



Configurare e gestire

StorageGRID 11.5

NetApp
April 11, 2024

Sommario

- Configurare e gestire 1
- Amministrare StorageGRID 1
- Gestire gli oggetti con ILM 278
- Protezione avanzata del sistema 448
- Configurare StorageGRID per FabricPool 457

Configurare e gestire

Amministrare StorageGRID

Scopri come configurare il sistema StorageGRID.

- ["Amministrazione di un sistema StorageGRID"](#)
- ["Controllo dell'accesso amministratore a StorageGRID"](#)
- ["Configurazione dei server di gestione delle chiavi"](#)
- ["Gestione dei tenant"](#)
- ["Configurazione delle connessioni dei client S3 e Swift"](#)
- ["Gestione delle reti e delle connessioni StorageGRID"](#)
- ["Configurazione di AutoSupport"](#)
- ["Gestione dei nodi di storage"](#)
- ["Gestione dei nodi di amministrazione"](#)
- ["Gestione dei nodi di archiviazione"](#)
- ["Migrazione dei dati in StorageGRID"](#)

Amministrazione di un sistema StorageGRID

Seguire queste istruzioni per configurare e amministrare un sistema StorageGRID.

Queste istruzioni descrivono come utilizzare Grid Manager per configurare gruppi e utenti, creare account tenant per consentire alle applicazioni client S3 e Swift di memorizzare e recuperare oggetti, configurare e gestire reti StorageGRID, configurare AutoSupport, gestire le impostazioni dei nodi e molto altro ancora.



Le istruzioni per la gestione degli oggetti con le regole e le policy ILM (Information Lifecycle Management) sono state spostate in ["Gestire gli oggetti con ILM"](#).

Queste istruzioni sono destinate al personale tecnico che configurerà, amministrerà e supporterà un sistema StorageGRID dopo l'installazione.

Di cosa hai bisogno

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

Requisiti del browser Web

È necessario utilizzare un browser Web supportato.

Browser Web	Versione minima supportata
Google Chrome	87

Browser Web	Versione minima supportata
Microsoft Edge	87
Mozilla Firefox	84

Impostare la larghezza consigliata per la finestra del browser.

Larghezza del browser	Pixel
Minimo	1024
Ottimale	1280

Accesso a Grid Manager

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

Di cosa hai bisogno

- È necessario disporre delle credenziali di accesso.
- È necessario disporre dell'URL per Grid Manager.
- È necessario utilizzare un browser Web supportato.
- I cookie devono essere attivati nel browser Web.
- È necessario disporre di autorizzazioni di accesso specifiche.

A proposito di questa attività

Ogni sistema StorageGRID include un nodo di amministrazione primario e un numero qualsiasi di nodi di amministrazione non primari. Per gestire il sistema StorageGRID, è possibile accedere a Grid Manager da qualsiasi nodo amministrativo. Tuttavia, i nodi Admin non sono esattamente gli stessi:

- Le conferme di allarme (sistema legacy) eseguite su un nodo di amministrazione non vengono copiate in altri nodi di amministrazione. Per questo motivo, le informazioni visualizzate per gli allarmi potrebbero non apparire identiche su ciascun nodo di amministrazione.
- Alcune procedure di manutenzione possono essere eseguite solo dal nodo di amministrazione primario.

Se i nodi di amministrazione sono inclusi in un gruppo ad alta disponibilità (ha), la connessione viene eseguita utilizzando l'indirizzo IP virtuale del gruppo ha o un nome di dominio completo che viene mappato all'indirizzo IP virtuale. Il nodo di amministrazione primario deve essere selezionato come master preferito del gruppo, in modo che quando si accede a Grid Manager, si accede al nodo di amministrazione primario, a meno che il nodo di amministrazione primario non sia disponibile.

Fasi

1. Avviare un browser Web supportato.
2. Nella barra degli indirizzi del browser, immettere l'URL per Grid Manager:

`https://FQDN_or_Admin_Node_IP/`

dove *FQDN_or_Admin_Node_IP* È un nome di dominio completo o l'indirizzo IP di un nodo di amministrazione o l'indirizzo IP virtuale di un gruppo ha di nodi di amministrazione.

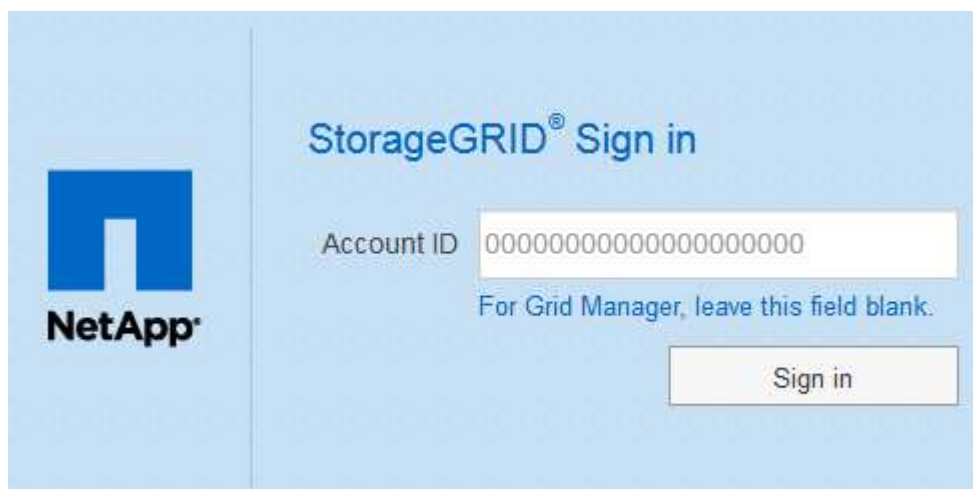
Se è necessario accedere a Grid Manager su una porta diversa da quella standard per HTTPS (443), immettere la seguente voce, dove *FQDN_or_Admin_Node_IP* È un nome di dominio completo o un indirizzo IP e porta è il numero di porta:

`https://FQDN_or_Admin_Node_IP:port/`

3. Se viene richiesto un avviso di protezione, installare il certificato utilizzando l'installazione guidata del browser.
4. Accedi a Grid Manager:
 - Se il sistema StorageGRID non utilizza il Single Sign-on (SSO):
 - i. Immettere il nome utente e la password per Grid Manager.
 - ii. Fare clic su **Accedi**.



- Se SSO è attivato per il sistema StorageGRID ed è la prima volta che si accede all'URL dal browser:
 - i. Fare clic su **Accedi**. È possibile lasciare vuoto il campo ID centro di costo.



- ii. Immettere le credenziali SSO standard nella pagina di accesso SSO dell'organizzazione. Ad esempio:

Sign in with your organizational account

someone@example.com

Password

Sign in

- Se SSO è abilitato per il sistema StorageGRID e si è precedentemente effettuato l'accesso a Grid Manager o a un account tenant:
 - i. Effettuare una delle seguenti operazioni:
 - Immettere **0** (l'ID account per Grid Manager) e fare clic su **Sign in** (Accedi).
 - Selezionare **Grid Manager** se compare nell'elenco degli account recenti e fare clic su **Sign in** (Accedi).



StorageGRID® Sign in

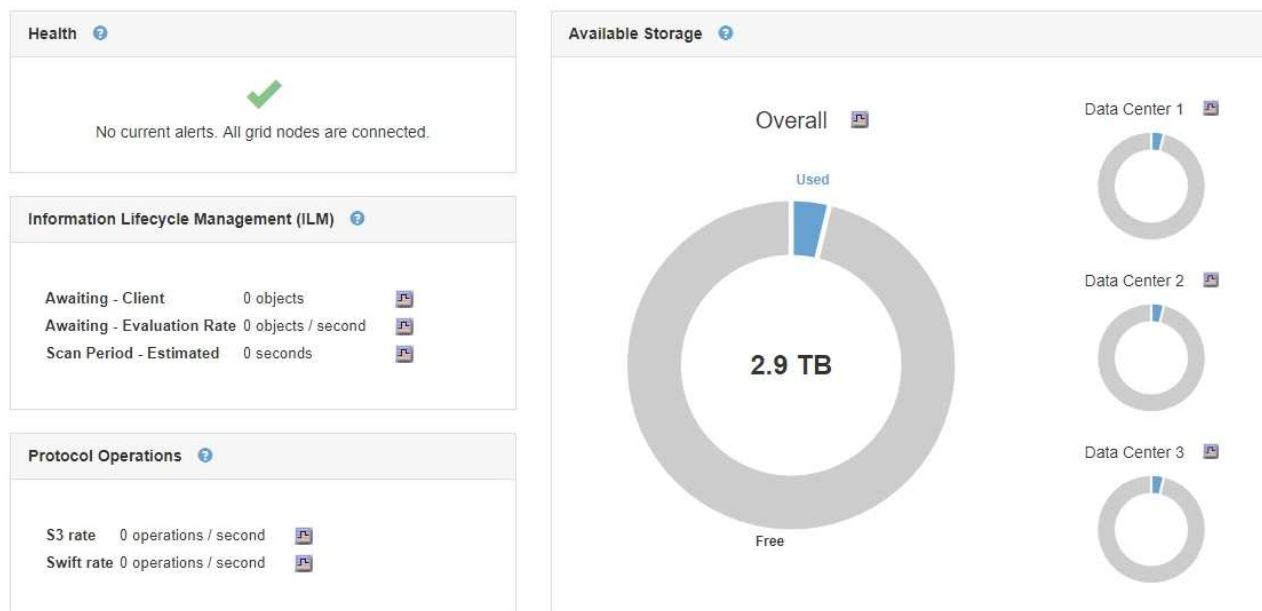
Recent Grid Manager

Account ID 0

Sign in

- ii. Accedi con le tue credenziali SSO standard nella pagina di accesso SSO della tua organizzazione. Una volta effettuato l'accesso, viene visualizzata la home page di Grid Manager, che include la dashboard. Per informazioni sulle informazioni fornite, consultare "visualizzazione della dashboard" nelle istruzioni per il monitoraggio e la risoluzione dei problemi di StorageGRID.

Dashboard



5. Se si desidera accedere a un altro nodo amministratore:

Opzione	Fasi
SSO non abilitato	<p>a. Nella barra degli indirizzi del browser, inserire il nome di dominio completo o l'indirizzo IP dell'altro nodo di amministrazione. Includere il numero di porta come richiesto.</p> <p>b. Immettere il nome utente e la password per Grid Manager.</p> <p>c. Fare clic su Accedi.</p>
SSO attivato	<p>Nella barra degli indirizzi del browser, inserire il nome di dominio completo o l'indirizzo IP dell'altro nodo di amministrazione.</p> <p>Se si è effettuato l'accesso a un nodo di amministrazione, è possibile accedere ad altri nodi di amministrazione senza dover effettuare nuovamente l'accesso. Tuttavia, se la sessione SSO scade, vengono richieste nuovamente le credenziali.</p> <p>Nota: SSO non è disponibile sulla porta limitata di Grid Manager. Se si desidera che gli utenti eseguano l'autenticazione con Single Sign-on, è necessario utilizzare la porta HTTPS predefinita (443).</p>

Informazioni correlate

["Requisiti del browser Web"](#)

["Controllo dell'accesso tramite firewall"](#)

["Configurazione dei certificati del server"](#)

["Configurazione del single sign-on"](#)

["Gestione dei gruppi di amministratori"](#)

["Gestione di gruppi ad alta disponibilità"](#)

["Utilizzare un account tenant"](#)

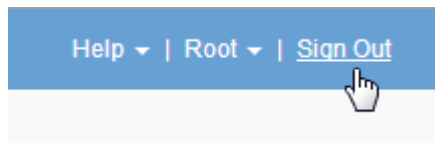
["Monitor risoluzione dei problemi"](#)

Disconnessione da Grid Manager

Una volta terminato l'utilizzo di Grid Manager, è necessario disconnettersi per garantire che gli utenti non autorizzati non possano accedere al sistema StorageGRID. La chiusura del browser potrebbe non disconnettersi dal sistema, in base alle impostazioni dei cookie del browser.

Fasi

1. Individuare il collegamento **Disconnetti** nell'angolo in alto a destra dell'interfaccia utente.



2. Fare clic su **Disconnetti**.

Opzione	Descrizione
SSO non in uso	<p>Si è disconnessi dal nodo di amministrazione.</p> <p>Viene visualizzata la pagina di accesso di Grid Manager.</p> <p>Nota: se si è effettuato l'accesso a più di un nodo Admin, è necessario disconnettersi da ciascun nodo.</p>

Opzione	Descrizione
SSO attivato	<p>Si è disconnessi da tutti i nodi di amministrazione ai quali si stava accedendo. Viene visualizzata la pagina di accesso a StorageGRID. Grid Manager è elencato come predefinito nell'elenco a discesa Recent Accounts (account recenti) e il campo account ID (ID account) mostra 0.</p> <p>Nota: se SSO è attivato e si è anche connessi al tenant Manager, è necessario disconnettersi dall'account tenant per disconnettersi da SSO.</p>

Informazioni correlate

["Configurazione del single sign-on"](#)

["Utilizzare un account tenant"](#)

Modifica della password

Gli utenti locali di Grid Manager possono modificare la propria password.

Di cosa hai bisogno

È necessario accedere a Grid Manager utilizzando un browser supportato.

A proposito di questa attività

Se si effettua l'accesso a StorageGRID come utente federato o se è attivato il Single Sign-on (SSO), non è possibile modificare la password in Grid Manager. È invece necessario modificare la password nell'origine dell'identità esterna, ad esempio Active Directory o OpenLDAP.

Fasi

1. Dall'interfaccia Grid Manager, selezionare **_nome_Modifica password**.
2. Inserire la password corrente.
3. Digitare una nuova password.

La password deve contenere almeno 8 e non più di 32 caratteri. Le password distinguono tra maiuscole e minuscole.

4. Immettere nuovamente la nuova password.
5. Fare clic su **Save** (Salva).

Modifica della passphrase di provisioning

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

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre delle autorizzazioni di manutenzione o di accesso root.
- È necessario disporre della passphrase di provisioning corrente.

A proposito di questa attività

La passphrase di provisioning è necessaria per molte procedure di installazione e manutenzione e per scaricare il pacchetto di ripristino. La passphrase di provisioning non è elencata in `Passwords.txt` file. Assicurarsi di documentare la passphrase di provisioning e conservarla in una posizione sicura.

Fasi

1. Selezionare **Configurazione controllo accessi Password griglia**.

NetApp® StorageGRID® Help ▾ | Root ▾ | Sign Out

Dashboard Alerts ▾ Nodes Tenants ILM ▾ Configuration ▾ Maintenance ▾ Support ▾

Grid Passwords
Change the provisioning passphrase and other passwords for your StorageGRID system.

Change Provisioning Passphrase

The provisioning passphrase is required for any installation, expansion, or maintenance procedure that makes changes to the grid topology. This passphrase is also required to download backups of the grid topology information and encryption keys for the StorageGRID system. After changing the provisioning passphrase, you must download a new Recovery Package.

Current Provisioning Passphrase

New Provisioning Passphrase

Confirm New Provisioning Passphrase

2. Inserire la passphrase di provisioning corrente.
3. Immettere la nuova passphrase. la passphrase deve contenere almeno 8 e non più di 32 caratteri. Le passphrase sono sensibili al maiuscolo/minuscolo.



Memorizzare la nuova passphrase di provisioning in una posizione sicura. È necessario per le procedure di installazione, espansione e manutenzione.

4. Immettere nuovamente la nuova passphrase e fare clic su **Save** (Salva).

Al termine della modifica della passphrase di provisioning, il sistema visualizza un banner verde di successo. La modifica dovrebbe richiedere meno di un minuto.

Dashboard

✓ Alerts ▾

Nodes

Tenants

ILM ▾

Configuration ▾

Maintenance ▾

Support ▾

Grid Passwords

Change the provisioning passphrase and other passwords for your StorageGRID system.

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

Change Provisioning Passphrase

The provisioning passphrase is required for any installation, expansion, or maintenance procedure that makes changes to the grid topology. This passphrase is also required to download backups of the grid topology information and encryption keys for the StorageGRID system. After changing the provisioning passphrase, you must download a new Recovery Package.

Current Provisioning Passphrase

New Provisioning Passphrase

Confirm New Provisioning Passphrase

Save

5. Selezionare il collegamento **Recovery Package page** all'interno del banner di successo.
6. Scarica il nuovo pacchetto di ripristino da Grid Manager. Selezionare **manutenzione pacchetto di ripristino** e inserire la nuova passphrase di provisioning.



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.

Modifica del timeout della sessione del browser

È possibile controllare se gli utenti di Grid Manager e Tenant Manager vengono disconnessi se rimangono inattivi per più di un certo periodo di tempo.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

A proposito di questa attività

Il valore predefinito del timeout di inattività della GUI è 900 secondi (15 minuti). Se la sessione del browser di un utente non è attiva per questo periodo di tempo, la sessione viene chiusa.

Se necessario, è possibile aumentare o diminuire il periodo di timeout impostando l'opzione di visualizzazione Timeout inattività GUI.

Se è attivato il Single Sign-on (SSO) e la sessione del browser di un utente va in timeout, il sistema si comporta come se l'utente abbia fatto clic su **Disconnetti** manualmente. L'utente deve immettere nuovamente le proprie credenziali SSO per accedere nuovamente a StorageGRID.

Il timeout della sessione utente può essere controllato anche da:



- Un timer StorageGRID separato, non configurabile, incluso per la sicurezza del sistema. Per impostazione predefinita, ogni token di autenticazione dell'utente scade 16 ore dopo l'accesso. Al termine dell'autenticazione, l'utente viene automaticamente disconnesso, anche se non viene raggiunto il valore per il timeout di inattività della GUI. Per rinnovare il token, l'utente deve effettuare nuovamente l'accesso.
- Impostazioni di timeout per il provider di identità, presupponendo che SSO sia abilitato per StorageGRID.

Fasi

1. Selezionare **Configurazione > Impostazioni di sistema > Opzioni di visualizzazione**.
2. Per **GUI Inactivity Timeout** (Timeout inattività GUI), immettere un periodo di timeout di almeno 60 secondi.

Impostare questo campo su 0 se non si desidera utilizzare questa funzionalità. Gli utenti vengono disconnessi 16 ore dopo l'accesso, quando scadono i token di autenticazione.



Display Options

Updated: 2017-03-09 20:36:53 MST

Current Sender

ADMIN-DC1-ADM1

Preferred Sender

ADMIN-DC1-ADM1

GUI Inactivity Timeout

900

Notification Suppress All



Apply Changes



3. Fare clic su **Applica modifiche**.

La nuova impostazione non influisce sugli utenti attualmente registrati. Gli utenti devono effettuare nuovamente l'accesso o aggiornare il browser per rendere effettiva la nuova impostazione di timeout.

Informazioni correlate

["Come funziona il single sign-on"](#)

["Utilizzare un account tenant"](#)

Visualizzazione delle informazioni sulla licenza StorageGRID

Se necessario, è possibile visualizzare le informazioni sulla licenza del sistema StorageGRID, ad esempio la capacità di storage massima del grid.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.

A proposito di questa attività

In caso di problemi con la licenza software per questo sistema StorageGRID, il pannello Stato del dashboard include un'icona Stato licenza e un collegamento **licenza**. Il numero indica il numero di problemi relativi alla licenza.

Dashboard



Fase

Per visualizzare la licenza, effettuare una delle seguenti operazioni:

- Dal pannello Health (Stato) della dashboard, fare clic sull'icona License status (Stato licenza) o sul collegamento **License** (licenza). Questo collegamento viene visualizzato solo in caso di problemi con la licenza.
- Selezionare **manutenzione sistema licenza**.

Viene visualizzata la pagina License (licenza) che fornisce le seguenti informazioni di sola lettura sulla licenza corrente:

- ID sistema StorageGRID, che è il numero di identificazione univoco per l'installazione di StorageGRID
- Numero di serie della licenza
- Capacità di storage concessa in licenza del grid
- Data di fine della licenza software
- Data di fine del contratto di assistenza
- Contenuto del file di testo della licenza



Per le licenze rilasciate prima di StorageGRID 10.3, la capacità dello storage concesso in licenza non è inclusa nel file di licenza e viene visualizzato il messaggio "vedere il contratto di licenza" invece di un valore.

Aggiornamento delle informazioni sulla licenza StorageGRID

È necessario aggiornare le informazioni di licenza per il sistema StorageGRID in qualsiasi momento in cui i termini della licenza cambiano. Ad esempio, è necessario aggiornare le informazioni sulla licenza se si acquista ulteriore capacità di storage per il grid.

Di cosa hai bisogno

- È necessario disporre di un nuovo file di licenza per l'applicazione al sistema StorageGRID.
- È necessario disporre di autorizzazioni di accesso specifiche.
- È necessario disporre della passphrase di provisioning.

Fasi

1. Selezionare **manutenzione sistema licenza**.
2. Inserire la passphrase di provisioning per il sistema StorageGRID nella casella di testo **Passphrase di provisioning**.
3. Fare clic su **Sfoglia**.
4. Nella finestra di dialogo Apri, individuare e selezionare il nuovo file di licenza (.txt), quindi fare clic su **Apri**.

Il nuovo file di licenza viene validato e visualizzato.

5. Fare clic su **Save** (Salva).

Utilizzando l'API Grid Management

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

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

Risorse di alto livello

L'API Grid Management 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 ulteriori informazioni, consulta le informazioni sull'utilizzo degli account tenant.
- `/private`: L'accesso è limitato agli utenti di Grid Manager e si basa sulle autorizzazioni di gruppo configurate. Queste API sono destinate esclusivamente all'uso interno e non sono documentate pubblicamente. Queste API sono inoltre soggette a modifiche senza preavviso.

Informazioni correlate

["Utilizzare un account tenant"](#)

["Prometheus: Nozioni di base sulle query"](#)

Operazioni API di Grid Management

L'API Grid Management organizza le operazioni API disponibili nelle seguenti sezioni.

- **Account** — operazioni per gestire gli account del tenant di storage, inclusa la creazione di nuovi account e il recupero dell'utilizzo dello storage per un determinato account.

- **Alarms** — operazioni per elencare gli allarmi correnti (sistema legacy) e restituire informazioni sullo stato della griglia, inclusi gli avvisi correnti e un riepilogo degli stati di connessione del nodo.
- **Alert-history** — operazioni sugli avvisi risolti.
- **Ricevitori di avvisi** — operazioni sui destinatari di notifiche di avvisi (e-mail).
- **Alert-rules** — operazioni sulle regole di allerta.
- **Silenzi di allerta** — operazioni su silenzi di allerta.
- **Alerts** — operazioni sugli avvisi.
- **Audit** — operazioni per elencare e aggiornare la configurazione dell'audit.
- **Auth** — operazioni per eseguire l'autenticazione della sessione utente.

L'API Grid Management supporta lo schema di autenticazione del token del bearer. Per effettuare l'accesso, inserisci 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 richieste API successive ("Authorization: Bearer *token*").



Se per il sistema StorageGRID è attivato il single sign-on, è necessario eseguire diversi passaggi per l'autenticazione. Vedere "autenticare l'API se è attivato il Single Sign-on".

Per informazioni su come migliorare la sicurezza dell'autenticazione, consultare "Protecting Against Cross-Site Request Fjery".

- **Certificati-client** — operazioni per configurare i certificati client in modo che sia possibile accedere in modo sicuro a StorageGRID utilizzando strumenti di monitoraggio esterni.
- **Config** — operazioni relative alla release del prodotto e alle versioni dell'API Grid Management. È possibile elencare la versione del prodotto e le principali versioni dell'API Grid Management supportate da tale release ed è possibile disattivare le versioni obsolete dell'API.
- **Disattivato-funzioni** — operazioni per visualizzare le funzioni che potrebbero essere state disattivate.
- **dns-servers** — operazioni per elencare e modificare i server DNS esterni configurati.
- **Nomi-dominio-endpoint** — operazioni per elencare e modificare i nomi di dominio degli endpoint.
- **Erasure-coding** — operazioni sui profili di codifica Erasure.
- **Espansione** — operazioni di espansione (a livello di procedura).
- **Expansion-node** — 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 Grid Network.
- **Grid-password** — operazioni per la gestione delle password grid.
- **Gruppi** — operazioni per gestire i gruppi di amministratori di griglia locali e recuperare i gruppi di amministratori di griglia federati da un server LDAP esterno.
- **Identity-source** — operazioni per configurare un'origine di identità esterna e sincronizzare manualmente le informazioni di utenti e gruppi federati.
- **ilm** — operazioni sulla gestione del ciclo di vita delle informazioni (ILM).
- **Licenza** — operazioni per recuperare e aggiornare la licenza StorageGRID.
- **Logs** — operazioni per la raccolta e il download dei file di log.

- **Metriche** — operazioni su metriche StorageGRID, incluse query metriche istantanee in un singolo punto nel tempo e query metriche di intervallo in un intervallo di tempo. L'API Grid Management utilizza lo strumento di monitoraggio dei sistemi Prometheus come origine dei dati back-end. Per informazioni sulla creazione di query Prometheus, visitare il sito Web Prometheus.



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

- **Node-Health** — operazioni sullo stato di salute del nodo.
- **ntp-servers** — operazioni per elencare o aggiornare server NTP (Network Time Protocol) esterni.
- **Objects** — operazioni su oggetti e metadati di oggetti.
- **Recovery** — operazioni per la procedura di recovery.
- **Recovery-package** — operazioni per scaricare il pacchetto di ripristino.
- **Regioni** — operazioni per visualizzare e creare regioni.
- **s3-Object-lock** — operazioni sulle impostazioni generali di blocco oggetti S3.
- **Certificato-server** — operazioni per visualizzare e aggiornare i certificati del server Grid Manager.
- **snmp** — operazioni sulla configurazione SNMP corrente.
- **Classi di traffico** — operazioni per le policy di classificazione del traffico.
- **Untrusted-client-network** — operazioni sulla configurazione Untrusted Client Network.
- **Utenti** — operazioni per visualizzare e gestire gli utenti di Grid Manager.

Invio di richieste API

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

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.



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

Fasi

1. Selezionare **Help API Documentation** dall'intestazione Grid Manager.
2. Selezionare l'operazione desiderata.

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

3. 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.

GET
/grid/groups Lists Grid Administrator Groups
🔒

Try it out

Name	Description
type string <small>(query)</small>	filter by group type Available values : local, federated <div style="border: 1px solid #ccc; padding: 2px; width: 100px; margin-top: 5px;">--</div>
limit integer <small>(query)</small>	maximum number of results Default value : 25 <div style="border: 1px solid #ccc; padding: 2px; width: 100px; margin-top: 5px;">25</div>
marker string <small>(query)</small>	marker-style pagination offset (value is Group's URN) <div style="border: 1px solid #ccc; padding: 2px; width: 100px; margin-top: 5px;">marker - marker-style pagination offset (value</div>
includeMarker boolean <small>(query)</small>	if set, the marker element is also returned <div style="border: 1px solid #ccc; padding: 2px; width: 100px; margin-top: 5px;">--</div>
order string <small>(query)</small>	pagination order (desc requires marker) Available values : asc, desc <div style="border: 1px solid #ccc; padding: 2px; width: 100px; margin-top: 5px;">--</div>

Responses
Response content type application/json

Code	Description
200	successfully retrieved Example Value Model <div style="background-color: #2e3436; color: #eeeeec; padding: 10px; font-family: monospace; font-size: 0.9em; margin-top: 5px;"> <pre> { "responseTime": "2021-03-29T14:22:19.673Z", "status": "success", "apiVersion": "3.3", "deprecated": false, "data": [{ "displayName": "Developers", </pre> </div>

4. Determinare se la richiesta richiede parametri aggiuntivi, ad esempio un ID utente o un gruppo. Quindi, ottenere questi valori. Potrebbe essere necessario emettere prima una richiesta API diversa per ottenere le informazioni necessarie.
5. Determinare se è necessario modificare il corpo della richiesta di esempio. In tal caso, fare clic su **Model** per conoscere i requisiti di ciascun campo.
6. Fare clic su **Provalo**.
7. Fornire i parametri richiesti o modificare il corpo della richiesta secondo necessità.
8. Fare clic su **Execute** (Esegui).
9. Esaminare il codice di risposta per determinare se la richiesta ha avuto esito positivo.

Versione dell'API Grid Management

L'API Grid Management utilizza il controllo delle versioni per supportare aggiornamenti senza interruzioni.

Ad esempio, questo URL di richiesta specifica la versione 3 dell'API.

```
https://hostname_or_ip_address/api/v3/authorize
```

La versione principale dell'API di gestione tenant viene bloccata quando vengono apportate modifiche **non compatibili** con le versioni precedenti. La versione minore dell'API di gestione tenant viene ridotta quando vengono apportate modifiche che **sono compatibili** con le versioni precedenti. Le modifiche compatibili includono l'aggiunta di nuovi endpoint o di nuove proprietà. Nell'esempio seguente viene illustrato il modo in cui la versione dell'API viene modificata in base al tipo di modifiche apportate.

Tipo di modifica all'API	Versione precedente	Nuova versione
Compatibile con le versioni precedenti	2.1	2.2
Non compatibile con versioni precedenti	2.1	3.0

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



È possibile utilizzare l'API Grid Management per configurare le versioni supportate. Per ulteriori informazioni, consultare la sezione "config" della documentazione dell'API Swagger. Disattivare il supporto per la versione precedente dopo aver aggiornato tutti i client API Grid Management per utilizzare la versione più recente.

Le richieste obsolete vengono contrassegnate come obsolete nei seguenti modi:

- L'intestazione della risposta è "Deprecated: True"
- Il corpo di risposta JSON include "deprecato": Vero
- Viene aggiunto un avviso obsoleto a nms.log. Ad esempio:

```
Received call to deprecated v1 API at POST "/api/v1/authorize"
```

Determinazione delle versioni API supportate nella release corrente

Utilizzare la seguente richiesta API per restituire un elenco delle versioni principali dell'API supportate:

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2019-01-10T20:41:00.845Z",
  "status": "success",
  "apiVersion": "3.0",
  "data": [
    2,
    3
  ]
}
```

Specifica di una versione API per una richiesta

È possibile specificare la versione dell'API utilizzando un parametro path (`/api/v3`) o un'intestazione (`Api-Version: 3`). Se si forniscono entrambi i valori, il valore dell'intestazione sovrascrive il valore del percorso.

```
curl https://[IP-Address]/api/v3/grid/accounts

curl -H "Api-Version: 3" https://[IP-Address]/api/grid/accounts
```

Protezione contro la contraffazione delle richieste (CSRF)

Puoi contribuire a proteggere dagli attacchi di cross-site request forgery (CSRF) 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 attivarla al momento dell'accesso.

Un utente malintenzionato in grado di inviare una richiesta a un sito diverso (ad esempio con UN HTTP Form POST) può causare l'esecuzione di determinate richieste utilizzando i cookie dell'utente che ha effettuato l'accesso.

StorageGRID aiuta a proteggere dagli attacchi CSRF utilizzando token CSRF. Se attivato, il contenuto di un cookie specifico deve corrispondere al contenuto di un'intestazione specifica o di un parametro POST-body specifico.

Per attivare 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 viene impostato con un valore casuale per l'accesso a Grid Manager e a. `AccountCsrfToken` Il cookie viene impostato con un valore casuale per l'accesso a Tenant Manager.

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

- Il `X-Csrf-Token` Header, con il valore dell'intestazione impostato sul valore del cookie del token CSRF.
- Per gli endpoint che accettano un corpo con codifica a modulo: A. `csrfToken` parametro del corpo della richiesta codificato dal modulo.

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



Anche le richieste che dispongono di un set di cookie token CSRF applicheranno "`Content-Type: application/json`" Intestazione per qualsiasi richiesta che prevede un corpo di richiesta JSON come protezione aggiuntiva contro gli attacchi CSRF.

Utilizzo dell'API se è attivato il single sign-on

Se per il sistema StorageGRID è stato attivato il Single Sign-on (SSO), non è possibile utilizzare le richieste API autenticate standard per accedere e disconnettersi dall'API di gestione griglia o dall'API di gestione tenant.

Accesso all'API se è attivato il Single Sign-on

Se è stato attivato il Single Sign-on (SSO), è necessario emettere una serie di richieste API per ottenere un token di autenticazione da ad FS valido per l'API Grid Management o l'API Tenant Management.

Di cosa hai bisogno

- Si conoscono il nome utente e la password SSO di un utente federated appartenente a un gruppo di utenti StorageGRID.
- Se si desidera accedere all'API di gestione tenant, si conosce l'ID account tenant.

A proposito di questa attività

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

- Il `storagegrid-ssoauth.py` Script Python, che si trova nella directory dei file di installazione di StorageGRID (`./rpms` Per Red Hat Enterprise Linux o CentOS, `./debs` Per Ubuntu o Debian, e `./vsphere` Per VMware).
- Un esempio di workflow di richieste di curl.

Il flusso di lavoro di arricciatura potrebbe andare in timeout se viene eseguito troppo lentamente. Potrebbe essere visualizzato l'errore: Impossibile trovare una `SubjectConfirmation` valida in questa risposta.



L'esempio di workflow di curl non protegge la password da essere vista da altri utenti.

Se si verifica un problema di codifica URL, potrebbe essere visualizzato l'errore: Versione SAML non supportata.

Fasi

1. Selezionare uno dei seguenti metodi per ottenere un token di autenticazione:
 - Utilizzare `storagegrid-ssoauth.py` Script Python. Passare alla fase 2.
 - USA richieste di curl. Passare alla fase 3.
2. Se si desidera utilizzare `storagegrid-ssoauth.py` Passare lo script all'interprete Python ed eseguirlo.

Quando richiesto, inserire i valori per i seguenti argomenti:

- Il nome utente SSO
- Il dominio in cui è installato StorageGRID
- L'indirizzo per StorageGRID
- Se si desidera accedere all'API di gestione tenant, inserire l'ID account tenant.

```
python3 /tmp/storagegrid-ssoauth.py
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. È ora possibile utilizzare il token per altre richieste, in modo simile a come si utilizzerebbe l'API se SSO non fosse utilizzato.

3. Se si desidera utilizzare le richieste di arricciamento, attenersi alla seguente procedura.
 - a. Dichiarare le variabili necessarie per 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 Grid Management, utilizzare 0 AS TENANTACCOUNTID.

- b. Per ricevere un URL di autenticazione firmato, inviare una richiesta DI 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 con codifica URL, ma non include il layer di codifica JSON aggiuntivo.

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

c. Salvare SAMLRequest dalla risposta per l'utilizzo nei comandi successivi.

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

d. Ottenere un URL completo che includa l'ID della richiesta del client da ad FS.

Un'opzione consiste nel richiedere il modulo di accesso utilizzando l'URL della risposta precedente.

```
curl
"https://$AD_FS_ADDRESS/ads/ls/?SAMLRequest=$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="/ads/ls/?
SAMLRequest=fZHRTOMwFIZfhh...UJikvo77sXPw%3D%3D&RelayState=12345&clie
nt-request-id=00000000-0000-0000-ee02-0080000000de" >
```

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

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

f. Inviare le credenziali all'azione del modulo della risposta precedente.

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

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



Se l'autenticazione a più fattori (MFA) è attivata per il 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=fZHRTomwFIZfhh...UJikvo
77sXPw%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. Salvare MSISAuth cookie dalla risposta.

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

h. Inviare una richiesta GET alla posizione specificata con i cookie del POST di autenticazione.

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

Le intestazioni delle risposte conterranno le informazioni della sessione di ad FS per un utilizzo successivo della disconnessione e il corpo della risposta conterrà la risposta SAML in un campo di forma 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
XFxVWx3bk1lMnFuUSUzZCUzZCYmJiYmXzE3MjAyZTA5LTNmMDgtNDRkZC04Yzg5LTQ3ND
UxYzA3ZjkzYw==; path=/adfs; HttpOnly; Secure
Set-Cookie: MSISAuthenticated=MTEvNy8yMDE4IDQ6MzI6NTkgUE0=;
path=/adfs; HttpOnly; Secure
Set-Cookie: MSISLoopDetectionCookie=MjAxOC0xMS0wNzoxNjoxMjAzMjQzZT4=;
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="PHNhbWxwOlJlc3Bvb3N...1scDpSZXNwb25zZT4=" /><input
type="hidden" name="RelayState" value="12345" />

```

- i. Salvare SAMLResponse dal campo nascosto:

```
export SAMLResponse='PHNhbWxwOlJlc3Bvb3N...1scDpSZXNwb25zZT4='
```

- j. Utilizzando il salvato SAMLResponse, Creare un StorageGRID/api/saml-response Richiesta di generazione di un token di autenticazione StorageGRID.

Per RelayState, Utilizzare l'ID account tenant o utilizzare 0 se si desidera accedere all'API Grid Management.

```

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. Salvare il token di autenticazione nella risposta con nome MYTOKEN.

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

Ora puoi utilizzare MYTOKEN Per le altre richieste, in modo simile a come si utilizza l'API se SSO non viene utilizzato.

Disconnettersi dall'API se è attivato il Single Sign-on

Se è stato attivato il Single Sign-on (SSO), è necessario emettere una serie di richieste API per disconnettersi dall'API Grid Management o dall'API Tenant Management.

A proposito di questa attività

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

Fasi

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

2. Salvare 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 API-only.

```
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 del bearer StorageGRID.

L'eliminazione del token portante StorageGRID funziona come senza SSO. Se cookie "sso=true" Non viene fornito, l'utente viene disconnesso da StorageGRID senza influire sullo stato SSO.

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

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

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

Utilizzo dei certificati di sicurezza StorageGRID

I certificati di sicurezza sono piccoli file di dati utilizzati per creare connessioni sicure e affidabili tra i componenti di StorageGRID e tra i componenti di StorageGRID e i sistemi esterni.

StorageGRID utilizza due tipi di certificati di sicurezza:

- **I certificati server** sono richiesti quando si utilizzano connessioni HTTPS. I certificati del server vengono utilizzati per stabilire connessioni sicure tra client e server, autenticando l'identità di un server nei suoi

client e fornendo un percorso di comunicazione sicuro per i dati. Il server e il client dispongono di una copia del certificato.

- **Certificati client** autenticano un'identità del client o dell'utente sul server, fornendo un'autenticazione più sicura rispetto alle sole password. I certificati client non crittografano i dati.

Quando un client si connette al server utilizzando 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 sulla copia del certificato. Se le firme corrispondono, il client avvia una sessione con il server utilizzando la stessa chiave pubblica.

StorageGRID funziona come server per alcune connessioni (come l'endpoint del bilanciamento del carico) o come client per altre connessioni (come il servizio di replica di CloudMirror).

Un'autorità di certificazione esterna (CA) può emettere certificati personalizzati pienamente conformi ai criteri di sicurezza delle informazioni dell'organizzazione. StorageGRID include anche un'autorità di certificazione (CA) incorporata che genera certificati CA interni durante l'installazione del sistema. Questi certificati CA interni vengono utilizzati, per impostazione predefinita, per proteggere il traffico StorageGRID interno. Sebbene sia possibile utilizzare i certificati CA interni per un ambiente non di produzione, la procedura consigliata per un ambiente di produzione consiste nell'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 devono essere quelli specificati per la verifica delle connessioni al server.
- Tutti i certificati personalizzati devono soddisfare le linee guida per la protezione avanzata del sistema per i certificati server.

"Protezione avanzata del sistema"

- StorageGRID supporta il raggruppamento di certificati da una CA in un singolo file (noto come bundle 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 di StorageGRID.

Certificato	Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Certificato del client di amministratore	Client	<p>Installato su ciascun client, consentendo a StorageGRID di autenticare l'accesso client esterno.</p> <ul style="list-style-type: none"> • Consente ai client esterni autorizzati di accedere al database StorageGRID Prometheus. • Consente il monitoraggio sicuro di StorageGRID utilizzando strumenti esterni. 	Configurazione controllo accessi certificati client	"Configurazione dei certificati client dell'amministratore"
Certificato di federazione delle identità	Server	<p>Autentica la connessione tra StorageGRID e un server di directory esterno, OpenLDAP o Oracle. Utilizzato per la federazione delle identità, che consente la gestione di gruppi di amministratori e utenti da parte di un sistema esterno.</p>	Configurazione controllo accessi Federazione identità	"Utilizzo della federazione delle identità"
Certificato SSO (Single Sign-on)	Server	<p>Autentica la connessione tra servizi di federazione Active Directory (ad FS) e StorageGRID utilizzata per le richieste SSO (Single Sign-on).</p>	Configurazione controllo accessi Single Sign-on	"Configurazione del single sign-on"

Certificato	Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Certificato del Key Management Server (KMS)	Server e client	Autentica la connessione tra StorageGRID e un KMS (Key Management Server) esterno, che fornisce chiavi di crittografia ai nodi appliance StorageGRID.	Configurazione Impostazioni di sistema Server di gestione delle chiavi	" Aggiunta di un server di gestione delle chiavi (KMS) "
Certificato di notifica degli avvisi via email	Server e client	<p>Autentica la connessione tra un server e-mail SMTP e StorageGRID utilizzato per le notifiche degli avvisi.</p> <ul style="list-style-type: none"> • Se le comunicazioni con il server SMTP richiedono TLS (Transport Layer Security), è necessario specificare il certificato CA del server di posta elettronica. • Specificare un certificato client solo se il server di posta SMTP richiede certificati client per l'autenticazione. 	Avvisi Configurazione e-mail	" Monitor risoluzione dei problemi "

Certificato	Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Certificato endpoint per il bilanciamento del carico	Server	<p>Autentica la connessione tra i client S3 o Swift e il servizio bilanciamento del carico StorageGRID sui nodi gateway o sui nodi di amministrazione. Quando si configura un endpoint di bilanciamento del carico, si carica o genera un certificato di bilanciamento del carico. Le applicazioni client utilizzano il certificato di bilanciamento del carico quando si effettua la connessione a StorageGRID per salvare e recuperare i dati degli oggetti.</p> <p>Nota: il certificato di bilanciamento del carico è il certificato più utilizzato durante il normale funzionamento StorageGRID.</p>	Configurazione Impostazioni di rete endpoint del bilanciamento del carico	<ul style="list-style-type: none"> • "Configurazione degli endpoint del bilanciamento del carico" • Creazione di un endpoint di bilanciamento del carico per FabricPool <p>"Configurare StorageGRID per FabricPool"</p>

Certificato	Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Certificato del server dell'interfaccia di gestione	Server	<p>Autentica la connessione tra i browser Web client e l'interfaccia di gestione di StorageGRID, consentendo agli utenti di accedere a Grid Manager e Tenant Manager senza avvisi di sicurezza.</p> <p>Questo certificato autentica anche le connessioni API Grid Management e API Tenant Management.</p> <p>È possibile utilizzare il certificato CA interno o caricare un certificato personalizzato.</p>	Configurazione Impostazioni di rete certificati server	<ul style="list-style-type: none"> • "Configurazione dei certificati del server" • "Configurazione di un certificato server personalizzato per Grid Manager e Tenant Manager"
Certificato endpoint Cloud Storage Pool	Server	<p>Autentica la connessione dal pool di storage cloud di StorageGRID a una posizione di storage esterna (ad esempio, lo storage S3 Glacier o Microsoft Azure Blob). Per ogni tipo di cloud provider è necessario un certificato diverso.</p>	ILM Storage Pools	"Gestire gli oggetti con ILM"
Certificato endpoint dei servizi di piattaforma	Server	<p>Autentica la connessione dal servizio della piattaforma StorageGRID a una risorsa di storage S3.</p>	Tenant Manager STORAGE (S3) endpoint dei servizi della piattaforma	"Utilizzare un account tenant"

Certificato	Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Object Storage API Service Endpoint Server Certificate	Server	Autentica le connessioni client protette S3 o Swift al servizio LDR (Local Distribution Router) su un nodo di storage o al servizio CLB (Connection Load Balancer) obsoleto su un nodo gateway.	Configurazione Impostazioni di rete endpoint del bilanciamento del carico	"Configurazione di un certificato server personalizzato per le connessioni al nodo di storage o al servizio CLB"

Esempio 1: Servizio di bilanciamento del carico

In questo esempio, StorageGRID agisce come server.

1. È possibile configurare un endpoint di bilanciamento del carico e caricare o generare un certificato server in StorageGRID.
2. È possibile configurare una connessione client S3 o Swift all'endpoint del bilanciamento del carico e caricare lo stesso certificato nel client.
3. Quando il client desidera salvare o recuperare i dati, si connette all'endpoint del bilanciamento del carico utilizzando 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 sulla 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 KMS (Key Management Server) esterno

In questo esempio, StorageGRID agisce come client.

1. Utilizzando il software del server di gestione delle chiavi esterno, è possibile configurare StorageGRID come client KMS e ottenere un certificato server con firma CA, un certificato client pubblico e la chiave privata per il certificato client.
2. Utilizzando Grid Manager, è possibile configurare un server KMS e caricare i certificati server e client e la chiave privata del client.
3. Quando un nodo StorageGRID necessita di una chiave di crittografia, effettua 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 può fidarsi di StorageGRID.
5. Il server KMS risponde utilizzando la connessione validata.

Controllo dell'accesso amministratore a StorageGRID

È possibile controllare l'accesso dell'amministratore al sistema StorageGRID aprendo o chiudendo le porte del firewall, gestendo utenti e gruppi di amministratori, configurando

SSO (Single Sign-on) e fornendo certificati client per consentire l'accesso esterno sicuro alle metriche StorageGRID.

- ["Controllo dell'accesso tramite firewall"](#)
- ["Utilizzo della federazione delle identità"](#)
- ["Gestione dei gruppi di amministratori"](#)
- ["Gestione degli utenti locali"](#)
- ["Utilizzo di SSO \(Single Sign-on\) per StorageGRID"](#)
- ["Configurazione dei certificati client dell'amministratore"](#)

Controllo dell'accesso tramite firewall

Quando si desidera controllare l'accesso tramite firewall, aprire o chiudere porte specifiche sul firewall esterno.

Controllo dell'accesso al 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, è possibile impedire ai tenant di connettersi a Grid Manager dal firewall, oltre a utilizzare altri metodi per controllare l'accesso al sistema.

Porta	Descrizione	Se la porta è aperta...
443	Porta HTTPS predefinita per i nodi di amministrazione	<p>I browser Web e i client API di gestione possono accedere a Grid Manager, Grid Management API, Tenant Manager e Tenant Management API.</p> <p>Nota: la porta 443 viene utilizzata anche per il traffico interno.</p>
8443	Porta Grid Manager limitata sui nodi di amministrazione	<ul style="list-style-type: none"> • I browser Web e i client API di gestione possono accedere a Grid Manager e all'API di Grid Management utilizzando HTTPS. • I browser Web e i client API di gestione non possono accedere a tenant Manager o all'API di gestione tenant. • Le richieste di contenuto interno verranno rifiutate.
9443	Porta limitata di Tenant Manager sui nodi di amministrazione	<ul style="list-style-type: none"> • I browser Web e i client API di gestione possono accedere a Tenant Manager e all'API di gestione tenant utilizzando HTTPS. • I browser Web e i client API di gestione non possono accedere a Grid Manager o all'API di Grid Management. • Le richieste di contenuto interno verranno rifiutate.



Single Sign-on (SSO) non è disponibile sulle porte limitate di Grid Manager o Tenant Manager. Se si desidera che gli utenti eseguano l'autenticazione con Single Sign-on, è necessario utilizzare la porta HTTPS predefinita (443).

Informazioni correlate

["Accesso a Grid Manager"](#)

["Creazione di un account tenant se StorageGRID non utilizza SSO"](#)

["Riepilogo: Indirizzi IP e porte per le connessioni client"](#)

["Gestione di reti client non attendibili"](#)

["Installare Ubuntu o Debian"](#)

["Installare VMware"](#)

["Installare Red Hat Enterprise Linux o CentOS"](#)

Utilizzo della federazione delle identità

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

Configurazione della federazione delle identità

È possibile configurare la federazione delle identità se si desidera che i gruppi amministrativi e gli utenti vengano gestiti in un altro sistema, ad esempio Active Directory, OpenLDAP o Oracle Directory Server.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.
- Se si prevede di attivare SSO (Single Sign-on), è necessario utilizzare Active Directory come origine dell'identità federata e ad FS come provider di identità. Consulta "requisiti per l'utilizzo del Single Sign-on".
- È necessario utilizzare Active Directory, OpenLDAP o Oracle Directory Server come provider di identità.



Se si desidera utilizzare un servizio LDAP v3 non presente nell'elenco, contattare il supporto tecnico.

- Se si intende utilizzare TLS (Transport Layer Security) per le comunicazioni con il server LDAP, il provider di identità deve utilizzare TLS 1.2 o 1.3.

A proposito di questa attività

È necessario configurare un'origine identità per Grid Manager se si desidera importare i seguenti tipi di gruppi federated:

- Gruppi di amministrazione. Gli utenti dei 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 la propria origine di identità. Gli utenti dei gruppi di tenant possono accedere al tenant manager ed eseguire le attività in base alle autorizzazioni assegnate al gruppo nel tenant manager.

Fasi

1. Selezionare **Configuration Access Control Identity Federation**.
2. Selezionare **Enable Identity Federation** (attiva federazione identità).

Vengono visualizzati i campi per la configurazione del server LDAP.

3. Nella sezione tipo di servizio LDAP, selezionare il tipo di servizio LDAP che si desidera configurare.

È possibile selezionare **Active Directory**, **OpenLDAP** o **Other**.



Se si seleziona **OpenLDAP**, è necessario configurare il server OpenLDAP. Consultare le linee guida per la configurazione di un server OpenLDAP.



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

4. Se si seleziona **Altro**, completare i campi nella sezione attributi LDAP.
 - **User Unique Name** (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`. Ogni valore dell'utente per l'attributo specificato deve essere un numero esadecimale a 32 cifre in formato a 16 byte o stringa, dove i trattini vengono ignorati.
 - **Group unique name** (Nome univoco 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 a 32 cifre nel formato a 16 byte o stringa, dove i trattini vengono ignorati.
5. Nella sezione Configure LDAP server (Configura server LDAP), immettere le informazioni richieste per il server LDAP e la connessione di rete.
 - **Nome host**: Nome host del server o indirizzo IP del server LDAP.
 - **Port** (porta): Porta utilizzata per la connessione al server LDAP.



La porta predefinita per STARTTLS è 389 e la porta predefinita per LDAPS è 636. Tuttavia, è possibile utilizzare qualsiasi porta purché il firewall sia configurato correttamente.

- **Username**: Percorso completo del nome distinto (DN) per l'utente che si connette al server LDAP.



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

L'utente specificato deve disporre dell'autorizzazione per elencare gruppi e utenti e per accedere ai

seguenti attributi:

- sAMAccountName oppure uid
 - objectGUID, entryUUID, o. nsuniqueid
 - cn
 - memberOf oppure isMemberOf
- **Password:** La password associata al nome utente.
 - **DN base gruppo:** Il percorso completo del nome distinto (DN) per una sottostruttura LDAP che si desidera cercare gruppi. Nell'esempio di Active Directory (riportato di seguito), 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 **Group unique name** devono essere univoci all'interno del **Group base DN** a cui appartengono.

- **User base DN:** Il percorso completo del nome distinto (DN) di una sottostruttura LDAP che si desidera cercare gli utenti.



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

6. Nella sezione **Transport Layer Security (TLS)**, selezionare un'impostazione di protezione.

- **Utilizzare STARTTLS (consigliato):** Utilizzare STARTTLS per proteggere le comunicazioni con il server LDAP. Questa è l'opzione consigliata.
- **Usa LDAPS:** L'opzione LDAPS (LDAP su SSL) utilizza TLS per stabilire una connessione al server LDAP. Questa opzione è supportata per motivi di compatibilità.
- **Non utilizzare TLS:** Il traffico di rete tra il sistema StorageGRID e il server LDAP non sarà protetto.



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

7. Se si seleziona STARTTLS o LDAPS, scegliere il certificato utilizzato per proteggere la connessione.

- **Usa certificato CA del sistema operativo:** Utilizzare il certificato CA predefinito installato sul sistema operativo per proteggere le connessioni.
- **Usa certificato CA personalizzato:** Utilizza un certificato di protezione personalizzato.

Se si seleziona questa impostazione, copiare e incollare il certificato di protezione personalizzato nella casella di testo del certificato CA.

8. Facoltativamente, selezionare **Test di connessione** per convalidare le impostazioni di connessione per il server LDAP.

Se la connessione è valida, nell'angolo superiore destro della pagina viene visualizzato un messaggio di conferma.

9. Se la connessione è valida, selezionare **Salva**.

La seguente schermata mostra valori di configurazione di esempio per un server LDAP che utilizza Active

Directory.

LDAP service type

Select the type of LDAP service you want to configure.

Active Directory OpenLDAP Other

Configure LDAP server (All fields are required)

Hostname **Port**

Username

Password

Group Base DN

User Base DN

Informazioni correlate

["Crittografia supportata per le connessioni TLS in uscita"](#)

["Requisiti per l'utilizzo del single sign-on"](#)

["Creazione di un account tenant"](#)

["Utilizzare un account tenant"](#)

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.

MemberOf e refint overlay

Gli overlay memberof e refint devono essere attivati. Per ulteriori informazioni, consultare le istruzioni per la manutenzione inversa dell'appartenenza al gruppo nella Guida per l'amministratore di OpenLDAP.

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, assicurarsi che i campi indicati nella guida per Nome utente siano indicizzati per ottenere prestazioni ottimali.

Consultare le informazioni sulla manutenzione inversa dell'appartenenza al gruppo nella Guida per l'amministratore di OpenLDAP.

Informazioni correlate

["Documentazione di OpenLDAP: Guida per l'amministratore della versione 2.4"](#)

Forzare la sincronizzazione con l'origine dell'identità

Il sistema StorageGRID sincronizza periodicamente gruppi e utenti federati dall'origine dell'identità. È possibile forzare l'avvio della sincronizzazione se si desidera attivare o limitare le autorizzazioni utente il più rapidamente possibile.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.
- L'origine dell'identità deve essere attivata.

Fasi

1. Selezionare **Configuration Access Control Identity Federation**.

Viene visualizzata la pagina Identity Federation. Il pulsante **Synchronize** si trova nella parte inferiore della pagina.

Synchronize

StorageGRID periodically synchronizes federated groups and users from the configured LDAP server. Clicking the button below will immediately start the synchronization process against the saved LDAP server.

Synchronize

2. Fare clic su **Sincronizza**.

Un messaggio di conferma indica che la sincronizzazione è stata avviata correttamente. Il processo di

sincronizzazione potrebbe richiedere del tempo a seconda dell'ambiente in uso.



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

Disattivazione della federazione delle identità

È possibile disattivare temporaneamente o permanentemente la federazione di identità per gruppi e utenti. Quando la federazione delle identità è disattivata, non vi è alcuna comunicazione tra StorageGRID e l'origine delle identità. Tuttavia, tutte le impostazioni configurate vengono conservate, consentendo di riabilitare facilmente la federazione delle identità in futuro.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

A proposito di questa attività

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

- Gli utenti federati non potranno accedere.
- Gli utenti federati che hanno effettuato l'accesso manterranno l'accesso al sistema StorageGRID fino alla scadenza della sessione, ma non potranno accedere dopo la scadenza della sessione.
- La sincronizzazione tra il sistema StorageGRID e l'origine dell'identità non viene eseguita e non vengono generati avvisi o allarmi per gli account che non sono stati sincronizzati.
- La casella di controllo **Enable Identity Federation** (Abilita federazione identità) è disattivata se Single Sign-on (SSO) è impostato su **Enabled** o **Sandbox Mode**. Lo stato SSO nella pagina Single Sign-on deve essere **Disabled** prima di poter disattivare la federazione delle identità.

Fasi

1. Selezionare **Configuration Access Control Identity Federation**.
2. Deselezionare la casella di controllo **Enable Identity Federation** (attiva federazione identità).
3. Fare clic su **Save** (Salva).

Informazioni correlate

["Disattivazione del single sign-on"](#)

Gestione dei gruppi di amministratori

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

Creazione di gruppi di amministratori

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

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.

- È necessario disporre di autorizzazioni di accesso specifiche.
- Se si intende importare un gruppo federated, è necessario che la federazione delle identità sia configurata e che il gruppo federated esista già nell'origine delle identità configurata.

Fasi

1. Selezionare **Configuration Access Control Admin Groups**.

Viene visualizzata la pagina Admin Groups (gruppi di amministratori) che elenca i gruppi di amministratori esistenti.

Admin Groups

Add and manage local and federated user groups, allowing member users to sign in to the Grid Manager. Set group permissions to control access to specific pages and features.

<input type="button" value="+ Add"/> <input type="button" value="Clone"/> <input type="button" value="Edit"/> <input type="button" value="x Remove"/>				
	Name	ID	Group Type	Access Mode
<input checked="" type="radio"/>	Flintstone	264083d0-23b5-3046-9bd4-88b7097731ab	Federated	Read-write
<input type="radio"/>	Simpson	cc8ad11f-68d0-f84a-af29-e7a6fcdc63a2	Federated	Read-only
<input type="radio"/>	ILM (read-only group)	88446141-9599-4543-b183-9c227ce7767a	Local	Read-only
<input type="radio"/>	API Developers	974b2faa-f9a1-4cfc-b364-914cdba2905f	Local	Read-write
<input type="radio"/>	ILM Admins (read-write)	a528c0c2-2417-4559-86ed-f0d2e31da820	Local	Read-write
<input type="radio"/>	Maintenance Users	7e3400ec-de8c-45a7-8bb8-e1496b362a8d	Local	Read-write


Group Type: Show rows per page

2. Selezionare **Aggiungi**.

Viene visualizzata la finestra di dialogo Add Group (Aggiungi gruppo).


Add Group

Create a new local group or import a group from the external identity source.













Group Type  Local Federated

Display Name

Unique Name 

Access Mode  Read-write Read-only

Management Permissions

- | | |
|--|---|
| <input type="checkbox"/> Root Access  | <input type="checkbox"/> Manage Alerts  |
| <input type="checkbox"/> Acknowledge Alarms  | <input type="checkbox"/> Grid Topology Page Configuration  |
| <input type="checkbox"/> Other Grid Configuration  | <input type="checkbox"/> Tenant Accounts  |
| <input type="checkbox"/> Change Tenant Root Password  | <input type="checkbox"/> Maintenance  |
| <input type="checkbox"/> Metrics Query  | <input type="checkbox"/> ILM  |
| <input type="checkbox"/> Object Metadata Lookup  | <input type="checkbox"/> Storage Appliance Administrator  |

Cancel

Save

- Per tipo di gruppo, selezionare **locale** se si desidera creare un gruppo che verrà utilizzato solo all'interno di StorageGRID oppure selezionare **Federato** se si desidera importare un gruppo dall'origine dell'identità.
- Se si seleziona **locale**, immettere un nome visualizzato per il gruppo. Il nome visualizzato è il nome visualizzato in Grid Manager. Ad esempio, "Maintenance Users" o "ILM Administrators."
- Immettere un nome univoco per il gruppo.
 - **Locale**: Immettere il nome univoco desiderato. Ad esempio, "ILM Administrators."
 - **Federated**: Immettere il nome del gruppo esattamente come appare nell'origine dell'identità configurata.
- Per **Access Mode**, selezionare se gli utenti del gruppo possono modificare le impostazioni ed eseguire operazioni in Grid Manager e nell'API Grid Management o se possono visualizzare solo impostazioni e funzionalità.
 - **Read-write** (valore predefinito): Gli utenti possono modificare le impostazioni ed eseguire le operazioni consentite dalle autorizzazioni di gestione.
 - **Sola lettura**: Gli utenti possono visualizzare solo le impostazioni e le funzionalità. Non possono apportare modifiche o eseguire operazioni nell'API Grid Manager o Grid Management. Gli utenti locali di sola lettura possono modificare le proprie password.



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

7. Selezionare una o più autorizzazioni di gestione.

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

8. Selezionare **Salva**.

Viene creato il nuovo gruppo. Se si tratta di un gruppo locale, è ora possibile aggiungere uno o più utenti. Se si tratta di un gruppo federated, l'origine identità gestisce gli utenti appartenenti al gruppo.

Informazioni correlate

["Gestione degli utenti locali"](#)

Autorizzazioni del gruppo di amministrazione

Quando si creano gruppi di utenti admin, 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 possono essere eseguite dall'utente.

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

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

- Accedi a Grid Manager
- Visualizza la dashboard
- Visualizzare le pagine dei nodi
- Monitorare la topologia della griglia
- Visualizzare gli avvisi correnti e risolti
- Visualizzazione degli allarmi correnti e storici (sistema legacy)
- Modifica della propria password (solo utenti locali)
- Visualizzare alcune informazioni nelle pagine Configurazione e manutenzione

Le sezioni seguenti descrivono le autorizzazioni che è possibile assegnare durante la creazione o la modifica di un gruppo amministrativo. Qualsiasi funzionalità non esplicitamente menzionata richiede l'autorizzazione Root Access.

Accesso root

Questa autorizzazione consente di accedere a tutte le funzioni di amministrazione della griglia.

Gestire gli avvisi

Questa autorizzazione consente di accedere alle opzioni per la gestione degli avvisi. Gli utenti devono disporre di questa autorizzazione per gestire silenzi, notifiche di avviso e regole di avviso.

Riconoscere gli allarmi (sistema legacy)

Questa autorizzazione consente di riconoscere e rispondere agli allarmi (sistema legacy). Tutti gli utenti che hanno effettuato l'accesso possono visualizzare gli allarmi correnti e storici.

Se si desidera che un utente monitori la topologia della griglia e riconosca solo gli allarmi, è necessario assegnare questa autorizzazione.

Configurazione della pagina Grid Topology (topologia griglia)

Questa autorizzazione consente di accedere alle seguenti opzioni di menu:

- Schede di configurazione disponibili nelle pagine di **supporto Strumenti topologia griglia**.
- Collegamento **Reset event count** (Ripristina conteggi eventi) nella scheda **Nodes Events** (nodi).

Altra configurazione della griglia

Questa autorizzazione consente di accedere a ulteriori opzioni di configurazione della griglia.



Per visualizzare queste opzioni aggiuntive, gli utenti devono disporre anche dell'autorizzazione Grid Topology Page Configuration.

- **Allarmi** (sistema legacy):
 - Allarmi globali
 - Configurazione e-mail legacy
- **ILM:**
 - Pool di storage
 - Storage Grades (gradi di storage)
- **Configurazione Impostazioni di rete**
 - Costo del collegamento
- **Configurazione Impostazioni di sistema:**
 - Opzioni di visualizzazione
 - Opzioni griglia
 - Opzioni di storage
- **Configurazione monitoraggio:**
 - Eventi
- **Supporto:**
 - AutoSupport

Account tenant

Questa autorizzazione consente di accedere alla pagina **tenant tenant account**.



La versione 1 dell'API Grid Management (obsoleta) utilizza questa autorizzazione per gestire i criteri di gruppo tenant, reimpostare le password di amministrazione di Swift e gestire le chiavi di accesso S3 dell'utente root.

Modificare la password principale del tenant

Questa autorizzazione consente di accedere all'opzione **Change Root Password** (Modifica password root) nella pagina Tenant Accounts (account tenant), consentendo di controllare chi può modificare la password per

l'utente root locale del tenant. Gli utenti che non dispongono di questa autorizzazione non possono visualizzare l'opzione **Change Root Password** (Modifica password root).



Prima di poter assegnare questa autorizzazione, è necessario assegnare al gruppo l'autorizzazione account tenant.

Manutenzione

Questa autorizzazione consente di accedere alle seguenti opzioni di menu:

- **Configurazione Impostazioni di sistema:**
 - Nomi di dominio*
 - Certificati server*
- **Configurazione monitoraggio:**
 - Audit*
- **Configurazione controllo accessi:**
 - Password di rete
- **Manutenzione attività di manutenzione**
 - Decommissionare
 - Espansione
 - Recovery (recupero)
- **Manutenzione rete:**
 - Server DNS*
 - Rete di rete*
 - Server NTP*
- **Manutenzione sistema:**
 - Licenza*
 - Pacchetto di ripristino
 - Aggiornamento software
- **Supporto Strumenti:**
 - Registri
- Gli utenti che non dispongono dell'autorizzazione di manutenzione possono visualizzare, ma non modificare, le pagine contrassegnate da un asterisco.

Query metriche

Questa autorizzazione consente di accedere alla pagina **Support Tools Metrics**. Questa autorizzazione consente inoltre di accedere alle query metriche Prometheus personalizzate utilizzando la sezione **metriche** dell'API Grid Management.

ILM

Questa autorizzazione consente di accedere alle seguenti opzioni del menu **ILM**:

- Erasure coding
- Regole
- Politiche
- Regioni



L'accesso alle opzioni di menu **ILM Storage Pools** e **ILM Storage Grades** è controllato dalle altre autorizzazioni Grid Configuration (Configurazione griglia) e Grid Topology Page Configuration (Configurazione pagina topologia griglia).

Object Metadata Lookup (Ricerca metadati oggetto)

Questa autorizzazione consente di accedere all'opzione di menu **ILM Object Metadata Lookup**.

Amministratore dell'appliance di storage

Questa autorizzazione consente di accedere al gestore di sistema e-Series SANtricity sulle appliance di storage tramite Grid Manager.

Interazione tra permessi e modalità di accesso

Per tutte le autorizzazioni, l'impostazione della modalità di accesso del gruppo determina se gli utenti possono modificare le impostazioni ed eseguire operazioni o se possono visualizzare solo le relative impostazioni e funzionalità. Se un utente appartiene a più gruppi e un gruppo è impostato su **sola lettura**, l'utente avrà accesso in sola lettura a tutte le impostazioni e funzionalità selezionate.

Disattivazione delle funzionalità dall'API Grid Management

È possibile utilizzare l'API di gestione griglia per disattivare completamente alcune funzionalità nel sistema StorageGRID. Quando una funzione viene disattivata, non è possibile assegnare a nessuno le autorizzazioni per eseguire le attività correlate a tale funzione.

A proposito di questa attività

Il sistema Disattivato consente di impedire l'accesso a determinate funzioni del sistema StorageGRID. La disattivazione di una funzione è l'unico modo per impedire all'utente root o agli utenti appartenenti a gruppi di amministrazione con l'autorizzazione di accesso root di utilizzare tale funzione.

Per comprendere come questa funzionalità potrebbe essere utile, considerare il seguente scenario:

L'azienda A è un provider di servizi che affitta la capacità di storage del proprio sistema StorageGRID creando account tenant. Per proteggere la sicurezza degli oggetti dei titolari di leasing, la Società A desidera garantire che i propri dipendenti non possano mai accedere a alcun account tenant dopo l'implementazione dell'account.

*L'azienda A è in grado di raggiungere questo obiettivo utilizzando il sistema Deactivate Features nell'API Grid Management. Disattivando completamente la funzione **Change tenant Root Password** in Grid Manager (sia l'interfaccia utente che l'API), la società A può garantire che nessun utente Admin, incluso l'utente root e gli utenti appartenenti a gruppi con l'autorizzazione Root Access, possa modificare la password per qualsiasi utente root dell'account tenant.*

Riattivazione delle funzioni disattivate

Per impostazione predefinita, è possibile utilizzare l'API Grid Management per riattivare una funzione disattivata. Tuttavia, se si desidera evitare che le funzioni disattivate vengano riattivate, è possibile disattivare

la funzione **ActivateFeatures**.



Impossibile riattivare la funzione **ActivateFeatures**. Se decidi di disattivare questa funzione, tieni presente che perderai in modo permanente la possibilità di riattivare qualsiasi altra funzione disattivata. È necessario contattare il supporto tecnico per ripristinare eventuali funzionalità perse.

Per ulteriori informazioni, consultare le istruzioni per l'implementazione delle applicazioni client S3 o Swift.

Fasi

1. Accedere alla documentazione Swagger per l'API di gestione griglia.
2. Individuare l'endpoint Deactivate Features.
3. Per disattivare una funzione, ad esempio **Change tenant Root Password**, inviare un corpo all'API come segue:

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

Al termine della richiesta, la funzione Cambia password principale tenant viene disattivata. L'autorizzazione per la gestione della password principale del tenant non viene più visualizzata nell'interfaccia utente e qualsiasi richiesta API che tenta di modificare la password root per un tenant non riuscirà con "403 Forbidden".

4. Per riattivare tutte le funzioni, inviare un corpo all'API come segue:

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

Una volta completata la richiesta, tutte le funzioni, inclusa la funzione Change tenant Root Password (Modifica password principale tenant), vengono riattivate. L'autorizzazione di gestione della password root del tenant viene ora visualizzata nell'interfaccia utente e tutte le richieste API che tentano di modificare la password root di un tenant avranno esito positivo, presupponendo che l'utente disponga dell'autorizzazione di gestione Root Access o Change tenant Root Password.



L'esempio precedente causa la riattivazione di *tutte* le funzioni disattivate. Se sono state disattivate altre funzioni che devono rimanere disattivate, è necessario specificarle esplicitamente nella richiesta PUT. Ad esempio, per riattivare la funzione Cambia password principale tenant e continuare a disattivare la funzione di conferma allarme, inviare la seguente richiesta PUT:

```
{ "grid": { "alarmAcknowledgment": true } }
```

Informazioni correlate

["Utilizzando l'API Grid Management"](#)

Modifica di un gruppo di amministratori

È possibile modificare un gruppo di amministratori per modificare le autorizzazioni associate al gruppo. Per i gruppi di amministratori locali, è anche possibile aggiornare il nome visualizzato.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

Fasi

1. Selezionare **Configuration Access Control Admin Groups**.
2. Selezionare il gruppo.

Se il sistema include più di 20 elementi, è possibile specificare quante righe vengono visualizzate su ogni pagina contemporaneamente. È quindi possibile utilizzare la funzione trova del browser per cercare un elemento specifico nelle righe attualmente visualizzate.

3. Fare clic su **Edit** (Modifica).
4. Se si desidera, per i gruppi locali, inserire il nome del gruppo che verrà visualizzato agli utenti, ad esempio "Maintenance Users".

Non è possibile modificare il nome univoco, ovvero il nome del gruppo interno.

5. In alternativa, modificare la modalità di accesso del gruppo.
 - **Read-write** (valore predefinito): Gli utenti possono modificare le impostazioni ed eseguire le operazioni consentite dalle autorizzazioni di gestione.
 - **Sola lettura**: Gli utenti possono visualizzare solo le impostazioni e le funzionalità. Non possono apportare modifiche o eseguire operazioni nell'API Grid Manager o Grid Management. Gli utenti locali di sola lettura possono modificare le proprie password.



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

6. Facoltativamente, aggiungere o rimuovere le autorizzazioni di gruppo.

Vedere le informazioni sulle autorizzazioni del gruppo di amministrazione.

7. Selezionare **Salva**.

Informazioni correlate

[Autorizzazioni del gruppo di amministrazione](#)

Eliminazione di un gruppo di amministratori

È possibile eliminare un gruppo di amministratori quando si desidera rimuovere il gruppo dal sistema e rimuovere tutte le autorizzazioni associate al gruppo. L'eliminazione di un gruppo di amministratori comporta la rimozione di tutti gli utenti admin dal gruppo, ma non l'eliminazione degli utenti admin.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

A proposito di questa attività

Quando elimini un gruppo, gli utenti assegnati a quel gruppo perderanno tutti i privilegi di accesso a Grid Manager, a meno che non ricevano privilegi da un altro gruppo.

Fasi

1. Selezionare **Configuration Access Control Admin Groups**.
2. Selezionare il nome del gruppo.

Se il sistema include più di 20 elementi, è possibile specificare quante righe vengono visualizzate su ogni pagina contemporaneamente. È quindi possibile utilizzare la funzione trova del browser per cercare un elemento specifico nelle righe attualmente visualizzate.

3. Selezionare **Rimuovi**.
4. Selezionare **OK**.

Gestione degli utenti locali

È possibile creare utenti locali e assegnarli a gruppi di amministratori locali per determinare a quali funzioni di Grid Manager possono accedere questi utenti.

Grid Manager include un utente locale predefinito, denominato "root". Sebbene sia possibile aggiungere e rimuovere utenti locali, non è possibile rimuovere l'utente root.



Se è stato attivato il Single Sign-on (SSO), gli utenti locali non possono accedere a StorageGRID.

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

Creazione di un utente locale

Se sono stati creati gruppi di amministratori locali, è possibile creare uno o più utenti locali e assegnare ciascun utente a uno o più gruppi. Le autorizzazioni del gruppo controllano le funzionalità di Grid Manager a cui l'utente può accedere.

A proposito di questa attività

È possibile creare solo utenti locali e assegnarli solo a gruppi di amministratori locali. Gli utenti federati e i gruppi federati vengono gestiti utilizzando l'origine dell'identità esterna.

Fasi

1. Selezionare **Configuration Access Control Admin Users**.
2. Fare clic su **Create** (Crea).
3. Immettere il nome visualizzato, il nome univoco e la password dell'utente.
4. Assegnare l'utente a uno o più gruppi che gestiscono le autorizzazioni di accesso.

L'elenco dei nomi dei gruppi viene generato dalla tabella Groups (gruppi).

5. Fare clic su **Save** (Salva).

Informazioni correlate

["Gestione dei gruppi di amministratori"](#)

Modifica dell'account di un utente locale

È possibile modificare l'account di un utente amministratore locale per aggiornare il nome visualizzato dell'utente o l'appartenenza al gruppo. È inoltre possibile impedire temporaneamente a un utente di accedere al sistema.

A proposito di questa attività

È possibile modificare solo gli utenti locali. I dettagli dell'utente federato vengono sincronizzati automaticamente con l'origine dell'identità esterna.

Fasi

1. Selezionare **Configuration Access Control Admin Users**.
2. Selezionare l'utente che si desidera modificare.

Se il sistema include più di 20 elementi, è possibile specificare quante righe vengono visualizzate su ogni pagina contemporaneamente. È quindi possibile utilizzare la funzione trova del browser per cercare un elemento specifico nelle righe attualmente visualizzate.

3. Fare clic su **Edit** (Modifica).
4. Facoltativamente, apportare modifiche al nome o all'appartenenza al gruppo.
5. Facoltativamente, per impedire all'utente di accedere temporaneamente al sistema, selezionare **Nega accesso**.
6. Fare clic su **Save** (Salva).

Le nuove impostazioni vengono applicate alla successiva disconnessione dell'utente e quindi all'accesso a Grid Manager.

Eliminazione di un account utente locale

È possibile eliminare gli account degli utenti locali che non richiedono più l'accesso a Grid Manager.

Fasi

1. Selezionare **Configuration Access Control Admin Users**.
2. Selezionare l'utente locale che si desidera eliminare.



Non è possibile eliminare l'utente locale root predefinito.

Se il sistema include più di 20 elementi, è possibile specificare quante righe vengono visualizzate su ogni pagina contemporaneamente. È quindi possibile utilizzare la funzione trova del browser per cercare un elemento specifico nelle righe attualmente visualizzate.

3. Fare clic su **Rimuovi**.
4. Fare clic su **OK**.

Modifica della password di un utente locale

Gli utenti locali possono modificare le proprie password utilizzando l'opzione **Change Password** (Modifica password) nel banner Grid Manager. Inoltre, gli utenti che hanno accesso alla pagina Admin Users possono modificare le password per altri utenti locali.

A proposito di questa attività

È possibile modificare le password solo per gli utenti locali. Gli utenti federati devono modificare le proprie password nell'origine dell'identità esterna.

Fasi

1. Selezionare **Configuration Access Control Admin Users**.
2. Nella pagina utenti, selezionare l'utente.

Se il sistema include più di 20 elementi, è possibile specificare quante righe vengono visualizzate su ogni pagina contemporaneamente. È quindi possibile utilizzare la funzione trova del browser per cercare un elemento specifico nelle righe attualmente visualizzate.

3. Fare clic su **Change Password** (Modifica password).
4. Immettere e confermare la password, quindi fare clic su **Save** (Salva).

Utilizzo di SSO (Single Sign-on) per StorageGRID

Il sistema StorageGRID supporta SSO (Single Sign-on) utilizzando lo standard SAML 2.0 (Security Assertion Markup Language 2.0). Quando SSO è attivato, 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.

- ["Come funziona il single sign-on"](#)
- ["Requisiti per l'utilizzo del single sign-on"](#)
- ["Configurazione del single sign-on"](#)

Come funziona il single sign-on

Prima di attivare SSO (Single Sign-on), esaminare in che modo i processi di accesso e disconnessione di StorageGRID vengono influenzati quando SSO è attivato.

Accesso quando SSO è attivato

Quando SSO è attivato e si accede a StorageGRID, si viene reindirizzati alla pagina SSO dell'organizzazione per convalidare le credenziali.

Fasi

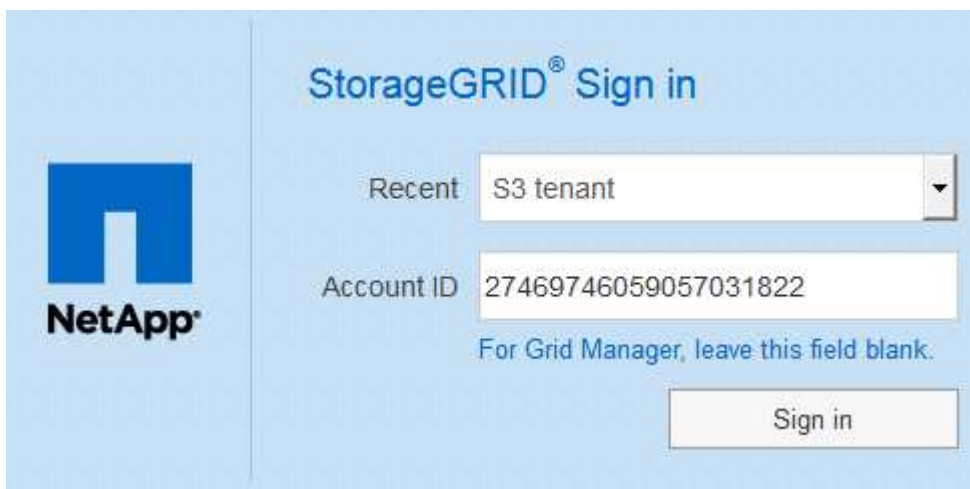
1. Immettere il nome di dominio completo o l'indirizzo IP di qualsiasi nodo di amministrazione StorageGRID in un browser Web.

Viene visualizzata la pagina di accesso a StorageGRID.

- Se si accede per la prima volta all'URL del browser, viene richiesto di inserire un ID account:



- Se in precedenza hai effettuato l'accesso a Grid Manager o al Tenant Manager, ti verrà richiesto di selezionare un account recente o di inserire un ID account:



La pagina di accesso a StorageGRID non viene visualizzata quando si inserisce l'URL completo di un account tenant (ovvero un nome di dominio completo o un indirizzo IP seguito da) `?accountId=20-digit-account-id`). Al contrario, si viene immediatamente reindirizzati alla pagina di accesso SSO dell'organizzazione, dove è possibile [Accedi con le tue credenziali SSO](#).

2. Indicare se si desidera accedere a Grid Manager o al tenant Manager:

- Per accedere a Grid Manager, lasciare vuoto il campo **account ID**, inserire **0** come ID account o selezionare **Grid Manager** se compare nell'elenco degli account recenti.
- Per accedere al tenant Manager, inserire l'ID account tenant di 20 cifre o selezionare un tenant in base al nome, se visualizzato nell'elenco degli account recenti.

3. Fare clic su **Accedi**

StorageGRID reindirizza l'utente alla pagina di accesso SSO della propria organizzazione. Ad esempio:

Sign in with your organizational account

[Sign in](#)

4. Accedi con le tue credenziali SSO.

Se le credenziali SSO sono corrette:

- a. Il provider di identità (IdP) fornisce una risposta di autenticazione a StorageGRID.
- b. StorageGRID convalida la risposta di autenticazione.
- c. Se la risposta è valida e l'utente appartiene a un gruppo federated con un'autorizzazione di accesso adeguata, l'utente ha effettuato l'accesso a Grid Manager o al tenant Manager, a seconda dell'account selezionato.

5. Se si dispone di autorizzazioni adeguate, è possibile accedere ad altri nodi di amministrazione o a Grid Manager o Tenant Manager.

Non è necessario immettere nuovamente le credenziali SSO.

Disconnessione quando SSO è attivato

Quando SSO è abilitato per StorageGRID, ciò che accade quando si effettua la disconnessione dipende da ciò che si effettua l'accesso e da dove si effettua la disconnessione.

Fasi

1. Individuare il collegamento **Disconnetti** nell'angolo in alto a destra dell'interfaccia utente.
2. Fare clic su **Disconnetti**.

Viene visualizzata la pagina di accesso a StorageGRID. Il menu a discesa **Recent Accounts** (account recenti) viene aggiornato per includere **Grid Manager** o il nome del tenant, in modo da poter accedere a queste interfacce utente più rapidamente in futuro.

Se hai effettuato l'accesso a...	E ti disconetterai da...	Sei disconnesso da...
Grid Manager su uno o più nodi di amministrazione	Grid Manager su qualsiasi nodo di amministrazione	Grid Manager su tutti i nodi di amministrazione
Tenant Manager su uno o più nodi di amministrazione	Tenant Manager su qualsiasi nodo di amministrazione	Tenant Manager su tutti i nodi di amministrazione

Se hai effettuato l'accesso a...	E ti disconnetterai da...	Sei disconnesso da...
Sia Grid Manager che tenant Manager	Grid Manager	Solo Grid Manager. Per disconnettersi da SSO, devi anche disconnetterti da Tenant Manager.



La tabella riassume ciò che accade quando si effettua la disconnessione se si utilizza una singola sessione del browser. Se hai effettuato l'accesso a StorageGRID in più sessioni del browser, devi disconnetterti separatamente da tutte le sessioni del browser.

Requisiti per l'utilizzo del single sign-on

Prima di attivare il Single Sign-on (SSO) per un sistema StorageGRID, esaminare i requisiti di questa sezione.



Single Sign-on (SSO) non è disponibile sulle porte limitate di Grid Manager o Tenant Manager. Se si desidera che gli utenti eseguano l'autenticazione con Single Sign-on, è necessario utilizzare la porta HTTPS predefinita (443).

Requisiti del provider di identità

Il provider di identità (IdP) per SSO deve soddisfare i seguenti requisiti:

- Una delle seguenti versioni di Active Directory Federation Service (ad FS):
 - AD FS 4.0, incluso in Windows Server 2016



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

- AD FS 3.0, incluso nell'aggiornamento di Windows Server 2012 R2 o superiore.
- Transport Layer Security (TLS) 1.2 o 1.3
- Microsoft .NET Framework, versione 3.5.1 o successiva

Requisiti dei certificati del server

StorageGRID utilizza un certificato del server di interfaccia di gestione su ciascun nodo di amministrazione per garantire l'accesso al gestore di griglia, al gestore del tenant, all'API di gestione del grid e all'API di gestione del tenant. Quando si configurano i trust delle parti di supporto SSO per StorageGRID in ad FS, il certificato del server viene utilizzato come certificato di firma per le richieste StorageGRID ad FS.

Se non è già stato installato un certificato server personalizzato per l'interfaccia di gestione, è necessario farlo ora. Quando si installa un certificato server personalizzato, viene utilizzato per tutti i nodi di amministrazione ed è possibile utilizzarlo in tutti i trust di StorageGRID.



Si sconsiglia di utilizzare il certificato server predefinito di un nodo di amministrazione nell'attendibilità della parte di base di ad FS. Se il nodo si guasta e viene ripristinato, viene generato un nuovo certificato server predefinito. Prima di poter accedere al nodo recuperato, è necessario aggiornare il trust della parte che si basa in ad FS con il nuovo certificato.

È possibile accedere al certificato del server di un nodo amministratore accedendo alla shell dei comandi del nodo e accedendo a `/var/local/mgmt-api` directory. Viene assegnato un nome a un certificato server personalizzato `custom-server.crt`. Il certificato server predefinito del nodo viene denominato `server.crt`.

Informazioni correlate

["Controllo dell'accesso tramite firewall"](#)

["Configurazione di un certificato server personalizzato per Grid Manager e Tenant Manager"](#)

Configurazione del single sign-on

Quando è attivato il 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 utilizzando il processo di accesso SSO implementato dall'organizzazione.

- ["Conferma che gli utenti federati possono effettuare l'accesso"](#)
- ["Utilizzo della modalità sandbox"](#)
- ["Creazione di trust per la parte di base in ad FS"](#)
- ["Verifica dei trust della parte di base"](#)
- ["Abilitazione del single sign-on"](#)
- ["Disattivazione del single sign-on"](#)
- ["Disattivare e riabilitare temporaneamente il Single Sign-on per un nodo di amministrazione"](#)

Conferma che gli utenti federati possono effettuare l'accesso

Prima di attivare il Single Sign-on (SSO), è necessario confermare che almeno un utente federato possa accedere a Grid Manager e a Tenant Manager per qualsiasi account tenant esistente.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.
- Si utilizza Active Directory come origine dell'identità federata e ad FS come provider di identità.

["Requisiti per l'utilizzo del single sign-on"](#)

Fasi

1. Se esistono account tenant, verificare che nessuno dei tenant utilizzi la propria origine di identità.



Quando si attiva SSO, un'origine identità configurata in Tenant Manager viene ignorata dall'origine identità configurata in Grid Manager. Gli utenti che appartengono all'origine dell'identità del tenant non potranno più accedere a meno che non dispongano di un account con l'origine dell'identità di Grid Manager.

- a. Accedi al tenant manager per ogni account tenant.

- b. Selezionare **Access Control Identity Federation**.
 - c. Verificare che la casella di controllo **Enable Identity Federation** (Abilita federazione identità) non sia selezionata.
 - d. In tal caso, verificare che i gruppi federated che potrebbero essere in uso per questo account tenant non siano più necessari, deselegionare la casella di controllo e fare clic su **Salva**.
2. Verificare che un utente federated possa accedere a Grid Manager:
 - a. Da Grid Manager, selezionare **Configuration Access Control Admin Groups**.
 - b. Assicursi che almeno un gruppo federated sia stato importato dall'origine dell'identità di Active Directory e che sia stata assegnata l'autorizzazione di accesso root.
 - c. Disconnettersi.
 - d. Confermare che è possibile accedere nuovamente a Grid Manager come utente nel gruppo federated.
 3. Se sono presenti account tenant, verificare che un utente federato che dispone dell'autorizzazione di accesso root possa effettuare l'accesso:
 - a. In Grid Manager, selezionare **tenant**.
 - b. Selezionare l'account tenant e fare clic su **Edit account** (Modifica account).
 - c. Se la casella di controllo **utilizza origine identità** è selezionata, deselegionare la casella e fare clic su **Salva**.

Edit Tenant Account

Tenant Details

Display Name

Uses Own Identity Source

Allow Platform Services

Storage Quota (optional) **GB** ▼

Cancel **Save**

Viene visualizzata la pagina account tenant.

- a. Selezionare l'account tenant, fare clic su **Accedi** e accedere all'account tenant come utente root locale.
- b. Da Tenant Manager, fare clic su **Access Control Groups**.
- c. Assicursi che almeno un gruppo federated di Grid Manager sia stato assegnato all'autorizzazione di accesso root per questo tenant.
- d. Disconnettersi.
- e. Confermare che è possibile accedere nuovamente al tenant come utente nel gruppo federated.

Informazioni correlate

["Requisiti per l'utilizzo del single sign-on"](#)

"Gestione dei gruppi di amministratori"

"Utilizzare un account tenant"

Utilizzo della modalità sandbox

È possibile utilizzare la modalità sandbox per configurare e testare i trust delle parti di base di Active Directory Federation Services (ad FS) prima di applicare il single sign-on (SSO) per gli utenti StorageGRID. Una volta attivato SSO, è possibile riabilitare la modalità sandbox per configurare o testare i trust delle parti di base nuove ed esistenti. La riattivazione della modalità sandbox disattiva temporaneamente SSO per gli utenti StorageGRID.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

A proposito di questa attività

Quando SSO è attivato e un utente tenta di accedere a un nodo amministratore, StorageGRID invia una richiesta di autenticazione ad FS. A sua volta, ad FS invia una risposta di autenticazione a StorageGRID, indicando se la richiesta di autorizzazione ha avuto esito positivo. Per le richieste riuscite, la risposta include un UUID (Universally Unique Identifier) per l'utente.

Per consentire a StorageGRID (il provider di servizi) e ad FS (il provider di identità) di comunicare in modo sicuro sulle richieste di autenticazione dell'utente, è necessario configurare alcune impostazioni in StorageGRID. Quindi, è necessario utilizzare ad FS per creare un trust per la parte di base per ogni nodo di amministrazione. Infine, è necessario tornare a StorageGRID per attivare SSO.

La modalità sandbox semplifica l'esecuzione di questa configurazione e il test di tutte le impostazioni prima di attivare SSO.



L'utilizzo della modalità sandbox è altamente consigliato, ma non strettamente necessario. Se si è pronti a creare trust di ad FS contando subito dopo aver configurato SSO in StorageGRID, inoltre, non è necessario testare i processi SSO e di logout singolo (SLO) per ciascun nodo di amministrazione, fare clic su **Enabled**, immettere le impostazioni StorageGRID, creare un trust per ciascun nodo di amministrazione in ad FS, quindi fare clic su **Save** per attivare SSO.

Fasi

1. Selezionare **Configuration Access Control Single Sign-on**.

Viene visualizzata la pagina Single Sign-on (accesso singolo), con l'opzione **Disabled** (Disattivato) 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 Active Directory come origine dell'identità federata. Consulta "requisiti per l'utilizzo del Single Sign-on".

2. Selezionare l'opzione **Sandbox Mode**.

Vengono visualizzate le impostazioni del provider di identità e della parte che si basa. Nella sezione Identity Provider, il campo **Service Type** è di sola lettura. Mostra il tipo di servizio di federazione delle identità in uso (ad esempio, Active Directory).

3. Nella sezione Identity Provider:

- a. Inserire il nome del servizio Federation, esattamente come appare in ad FS.



Per individuare il nome del servizio Federation, accedere a Gestione server Windows. Selezionare **Tools ad FS Management**. Dal menu Action (azione), selezionare **Edit Federation Service Properties** (Modifica proprietà servizio federazione). Il nome del servizio della federazione viene visualizzato nel secondo campo.

- b. Specificare se si desidera utilizzare TLS (Transport Layer Security) per proteggere la connessione quando il provider di identità invia le informazioni di configurazione SSO in risposta alle richieste StorageGRID.

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

Se si seleziona questa impostazione, copiare e incollare il certificato nella casella di testo **certificato CA**.

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

4. Nella sezione parte che si basa, specificare l'identificativo della parte che si desidera utilizzare per i nodi di amministrazione StorageGRID quando si configurano i trust della parte che si basa.

- Ad esempio, se la griglia dispone di un solo nodo di amministrazione e non si prevede di aggiungere altri nodi di amministrazione in futuro, immettere `SG` oppure `StorageGRID`.
- Se la griglia include più di un nodo di amministrazione, includere la stringa `[HOSTNAME]` nell'identificatore. Ad esempio, `SG-[HOSTNAME]`. In questo modo viene generata una tabella che include un identificativo di parte di base per ciascun nodo di amministrazione, in base al nome host del nodo. + **NOTA:** È necessario creare un trust per ciascun nodo amministrativo nel sistema StorageGRID. La disponibilità di un trust per ciascun nodo di amministrazione garantisce che gli utenti possano accedere e uscire in modo sicuro da qualsiasi nodo di amministrazione.

5. Fare clic su **Save** (Salva).

- Sul pulsante **Save** viene visualizzato un segno di spunta verde per alcuni secondi.



- Viene visualizzato il messaggio di conferma della modalità Sandbox, che conferma l'attivazione della modalità sandbox. È possibile utilizzare questa modalità mentre si utilizza ad FS per configurare un trust di parte per ciascun nodo di amministrazione e testare i processi di accesso singolo (SSO) e di logout singolo (SLO).

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

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.

Informazioni correlate

["Requisiti per l'utilizzo del single sign-on"](#)

Creazione di trust per la parte di base in ad FS

È necessario utilizzare Active Directory Federation Services (ad FS) per creare un trust di parte per ciascun nodo di amministrazione nel sistema. È possibile creare trust di parti che utilizzano i comandi PowerShell, importando metadati SAML da StorageGRID o immettendo i dati manualmente.

Creazione di un trust di parte che si basa utilizzando Windows PowerShell

È possibile utilizzare Windows PowerShell per creare rapidamente uno o più trust di parti.

Di cosa hai bisogno

- L'SSO è stato configurato in StorageGRID e si conoscono il nome di dominio completo (o l'indirizzo IP) e l'identificativo della parte di base per ciascun nodo amministratore del sistema.



È necessario creare un trust per ciascun nodo amministratore nel sistema StorageGRID. La disponibilità di un trust per ciascun nodo di amministrazione garantisce che gli utenti possano accedere e uscire in modo sicuro da qualsiasi nodo di amministrazione.

- Si dispone di esperienza nella creazione di trust di parti di supporto in ad FS o si dispone dell'accesso alla documentazione di Microsoft ad FS.
- Si sta utilizzando lo snap-in di gestione di ad FS e si appartiene al gruppo Administrators.

A proposito di questa attività

Queste istruzioni si applicano ad FS 4.0, incluso in Windows Server 2016. Se si utilizza ad FS 3.0, incluso in Windows 2012 R2, si noteranno lievi differenze nella procedura. In caso di domande, consultare la documentazione di Microsoft ad FS.

Fasi

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

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

- Per *Admin_Node_Identifier*, Immettere l'identificativo della parte di base 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, è necessario aggiornare o ricreare la fiducia della parte che si basa se tale indirizzo IP cambia).

3. Da Gestione server Windows, selezionare **Strumenti Gestione di ad FS**.

Viene visualizzato lo strumento di gestione di ad FS.

4. Selezionare **ad FS Trust di parte di base**.

Viene visualizzato l'elenco dei trust della parte che si basa.

5. Aggiungere un criterio di controllo degli accessi al trust della parte di base appena creato:

- a. Individuare la fiducia della parte di base appena creata.
- b. Fare clic con il pulsante destro del mouse sull'attendibilità e selezionare **Edit Access Control Policy** (Modifica policy di controllo degli accessi).
- c. Selezionare un criterio di controllo degli accessi.
- d. Fare clic su **Apply** (Applica), quindi su **OK**

6. Aggiungere una policy di emissione delle richieste di rimborso al nuovo Trust della parte di base creato:

- a. Individuare la fiducia della parte di base appena creata.
- b. Fare clic con il pulsante destro del mouse sull'attendibilità e selezionare **Edit claim issuance policy** (Modifica policy di emissione richiesta di rimborso).
- c. Fare clic su **Aggiungi regola**.
- d. Nella pagina Select Rule Template (Seleziona modello di regola), selezionare **Send LDAP Attributes**

as Claims (Invia attributi LDAP come richieste) dall'elenco e fare clic su **Next** (Avanti).

e. Nella pagina Configure Rule (Configura regola), immettere un nome da visualizzare per questa regola.

Ad esempio, da **objectGUID a ID nome**.

f. Per l'archivio attributi, selezionare **Active Directory**.

g. Nella colonna LDAP Attribute della tabella Mapping, digitare **objectGUID**.

h. Nella colonna Outgoing Claim Type (tipo di richiesta di rimborso in uscita) della tabella Mapping (mappatura), selezionare **Name ID** (ID nome) dall'elenco a discesa.

i. Fare clic su **fine**, quindi su **OK**.

7. Verificare che i metadati siano stati importati correttamente.

a. Fare clic con il pulsante destro del mouse sull'attendibilità della parte che si basa per aprirne le proprietà.

b. Verificare che i campi nelle schede **endpoint**, **identificatori** e **Firma** siano compilati.

Se i metadati non sono presenti, verificare che l'indirizzo dei metadati della federazione sia corretto o semplicemente inserire i valori manualmente.

8. Ripetere questa procedura per configurare un trust per tutti i nodi di amministrazione nel sistema StorageGRID.

9. Al termine, tornare a StorageGRID e. "[verificare tutti i trust delle parti di base](#)" per confermare che sono configurati correttamente.

Creazione di un trust per la parte che si basa importando metadati di federazione

È possibile importare i valori per ciascun trust di parte che si basa accedendo ai metadati SAML per ciascun nodo di amministrazione.

Di cosa hai bisogno

- L'SSO è stato configurato in StorageGRID e si conoscono il nome di dominio completo (o l'indirizzo IP) e l'identificativo della parte di base per ciascun nodo amministratore del sistema.



È necessario creare un trust per ciascun nodo amministratore nel sistema StorageGRID. La disponibilità di un trust per ciascun nodo di amministrazione garantisce che gli utenti possano accedere e uscire in modo sicuro da qualsiasi nodo di amministrazione.

- Si dispone di esperienza nella creazione di trust di parti di supporto in ad FS o si dispone dell'accesso alla documentazione di Microsoft ad FS.
- Si sta utilizzando lo snap-in di gestione di ad FS e si appartiene al gruppo Administrators.

A proposito di questa attività

Queste istruzioni si applicano ad FS 4.0, incluso in Windows Server 2016. Se si utilizza ad FS 3.0, incluso in Windows 2012 R2, si noteranno lievi differenze nella procedura. In caso di domande, consultare la documentazione di Microsoft ad FS.

Fasi

1. In Gestione server Windows, fare clic su **Strumenti**, quindi selezionare **Gestione di ad FS**.
2. In azioni, fare clic su **Aggiungi fiducia parte di base**.

3. Nella pagina di benvenuto, scegliere **Richieste di rimborso** e fare clic su **Avvia**.
4. Selezionare **Importa dati relativi alla parte che si basa pubblicati online o su una rete locale**.
5. In **Federation metadata address (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, è necessario aggiornare o ricreare la fiducia della parte che si basa se tale indirizzo IP cambia).

6. Completare la procedura guidata Trust Party, salvare il trust della parte che si basa e chiudere la procedura guidata.



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

7. Aggiungere una regola di richiesta di rimborso:
 - a. Fare clic con il pulsante destro del mouse sull'attendibilità e selezionare **Edit claim issuance policy** (Modifica policy di emissione richiesta di rimborso).
 - b. Fare clic su **Aggiungi regola**:
 - c. Nella pagina Select Rule Template (Seleziona modello di regola), selezionare **Send LDAP Attributes as Claims** (Invia attributi LDAP come richieste) dall'elenco e fare clic su **Next** (Avanti).
 - d. Nella pagina Configure Rule (Configura regola), immettere un nome da visualizzare per questa regola.

Ad esempio, da **objectGUID** a **ID nome**.
 - e. Per l'archivio attributi, selezionare **Active Directory**.
 - f. Nella colonna LDAP Attribute della tabella Mapping, digitare **objectGUID**.
 - g. Nella colonna Outgoing Claim Type (tipo di richiesta di rimborso in uscita) della tabella Mapping (mappatura), selezionare **Name ID** (ID nome) dall'elenco a discesa.
 - h. Fare clic su **fine**, quindi su **OK**.
8. Verificare che i metadati siano stati importati correttamente.
 - a. Fare clic con il pulsante destro del mouse sull'attendibilità della parte che si basa per aprirne le proprietà.
 - b. Verificare che i campi nelle schede **endpoint**, **identificatori** e **Firma** siano compilati.

Se i metadati non sono presenti, verificare che l'indirizzo dei metadati della federazione sia corretto o semplicemente inserire i valori manualmente.
9. Ripetere questa procedura per configurare un trust per tutti i nodi di amministrazione nel sistema StorageGRID.
10. Al termine, tornare a StorageGRID e **"verificare tutti i trust delle parti di base"** per confermare che sono configurati correttamente.

Creazione manuale di un trust per la parte che si basa

Se si sceglie di non importare i dati per i trust della parte di base, è possibile inserire i valori manualmente.

Di cosa hai bisogno

- L'SSO è stato configurato in StorageGRID e si conoscono il nome di dominio completo (o l'indirizzo IP) e l'identificativo della parte di base per ciascun nodo amministratore del sistema.



È necessario creare un trust per ciascun nodo amministratore nel sistema StorageGRID. La disponibilità di un trust per ciascun nodo di amministrazione garantisce che gli utenti possano accedere e uscire in modo sicuro da qualsiasi nodo di amministrazione.

- Si dispone del certificato personalizzato caricato per l'interfaccia di gestione di StorageGRID oppure si sa come accedere a un nodo amministratore dalla shell dei comandi.
- Si dispone di esperienza nella creazione di trust di parti di supporto in ad FS o si dispone dell'accesso alla documentazione di Microsoft ad FS.
- Si sta utilizzando lo snap-in di gestione di ad FS e si appartiene al gruppo Administrators.

A proposito di questa attività

Queste istruzioni si applicano ad FS 4.0, incluso in Windows Server 2016. Se si utilizza ad FS 3.0, incluso in Windows 2012 R2, si noteranno lievi differenze nella procedura. In caso di domande, consultare la documentazione di Microsoft ad FS.

Fasi

1. In Gestione server Windows, fare clic su **Strumenti**, quindi selezionare **Gestione di ad FS**.
2. In azioni, fare clic su **Aggiungi fiducia parte di base**.
3. Nella pagina di benvenuto, scegliere **Richieste di rimborso** e fare clic su **Avvia**.
4. Selezionare **inserire manualmente i dati relativi alla parte di base** e fare clic su **Avanti**.
5. Completare la procedura guidata Trust Party:

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

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

- b. Saltare il passaggio per configurare un certificato di crittografia token opzionale.
- c. Nella pagina Configure URL (Configura URL), selezionare la casella di controllo **Enable support for the SAML 2.0 WebSSO Protocol** (attiva supporto per il protocollo SAML 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, è necessario aggiornare o ricreare la fiducia della parte che si basa se tale indirizzo IP cambia).

- e. Nella pagina Configure Identifier (Configura identificatori), specificare l'identificativo della parte di base per lo stesso nodo di amministrazione:

```
Admin_Node_Identifier
```

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

- f. Rivedere le impostazioni, salvare l'attendibilità della parte che si basa e chiudere la procedura guidata.

Viene visualizzata la finestra di dialogo Edit Claim Issuance Policy (Modifica policy di emissione richieste di



Se la finestra di dialogo non viene visualizzata, fare clic con il pulsante destro del mouse sull'attendibilità e selezionare **Edit claim issuance policy** (Modifica policy di emissione richiesta di rimborso).

6. Per avviare la procedura guidata Claim Rule, fare clic su **Add Rule**:
 - a. Nella pagina Select Rule Template (Seleziona modello di regola), selezionare **Send LDAP Attributes as Claims** (Invia attributi LDAP come richieste) dall'elenco e fare clic su **Next** (Avanti).
 - b. Nella pagina Configure Rule (Configura regola), immettere un nome da visualizzare per questa regola.

Ad esempio, da **objectGUID a ID nome**.
 - c. Per l'archivio attributi, selezionare **Active Directory**.
 - d. Nella colonna LDAP Attribute della tabella Mapping, digitare **objectGUID**.
 - e. Nella colonna Outgoing Claim Type (tipo di richiesta di rimborso in uscita) della tabella Mapping (mappatura), selezionare **Name ID** (ID nome) dall'elenco a discesa.
 - f. Fare clic su **fine**, quindi su **OK**.
7. Fare clic con il pulsante destro del mouse sull'attendibilità della parte che si basa per aprirne le proprietà.
8. Nella scheda **Endpoint**, configurare l'endpoint per la disconnessione singola (SLO):
 - a. Fare clic su **Add SAML** (Aggiungi SAML).
 - b. Selezionare **Endpoint Type SAML Logout**.
 - c. Selezionare **binding Redirect**.
 - d. Nel campo **Trusted URL**, 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, è necessario aggiornare o ricreare la fiducia della parte che si basa se tale indirizzo IP cambia).

- a. Fare clic su **OK**.
9. Nella scheda **Firma**, specificare il certificato di firma per il trust della parte che si basa:
 - a. Aggiungere il certificato personalizzato:
 - Se si dispone del certificato di gestione personalizzato caricato su StorageGRID, selezionare il certificato.
 - Se non si dispone del certificato personalizzato, accedere al nodo di amministrazione, quindi passare a `/var/local/mgmt-api` Della directory Admin Node e aggiungere `custom-server.crt` file di certificato.

Nota: utilizzando il certificato predefinito del nodo di amministrazione (`server.crt`) non è consigliato. Se il nodo Admin non riesce, il certificato predefinito viene rigenerato quando si ripristina il nodo ed è necessario aggiornare il trust della parte che si basa.

- b. Fare clic su **Apply** (Applica), quindi su **OK**.

Le proprietà della parte di base vengono salvate e chiuse.

10. Ripetere questa procedura per configurare un trust per tutti i nodi di amministrazione nel sistema StorageGRID.
11. Al termine, tornare a StorageGRID e "[verificare tutti i trust delle parti di base](#)" per confermare che sono configurati correttamente.

Verifica dei trust della parte di base

Prima di imporre l'utilizzo del Single Sign-on (SSO) per StorageGRID, verificare che il Single Sign-on e il Single Logout (SLO) siano configurati correttamente. Se è stata creata un'attendibilità per ciascun nodo di amministrazione, confermare che è possibile utilizzare SSO e SLO per ciascun nodo di amministrazione.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.
- Sono stati configurati uno o più trust di parti di supporto in ad FS.

Fasi

1. Selezionare **Configuration Access Control Single Sign-on**.

Viene visualizzata la pagina Single Sign-on (accesso singolo), con l'opzione **Sandbox Mode** (modalità sandbox) selezionata.

2. Nelle istruzioni per la modalità sandbox, individuare il collegamento alla pagina di accesso del provider di identità.

L'URL deriva dal valore immesso nel campo **Federated Service Name**.

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.

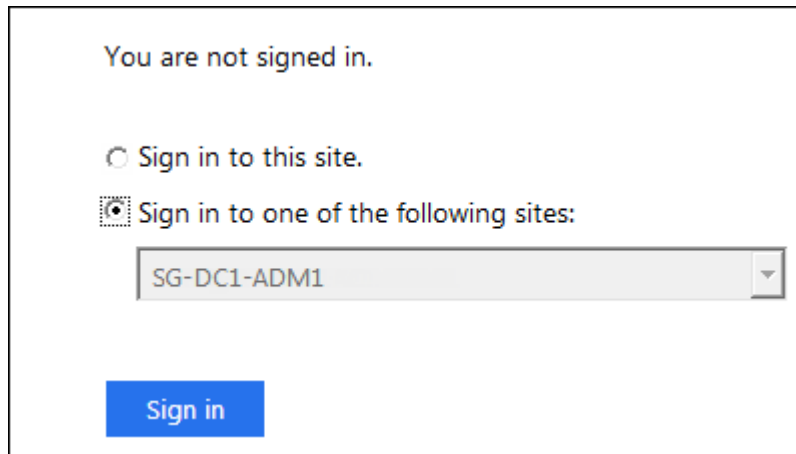
1. Use Active Directory Federation Services (AD FS) to create relying party trusts for StorageGRID. Create one trust for each Admin Node, using the relying party identifier(s) shown below.
2. Go to your identity provider's sign-on page: <https://ad2016.saml.sgws/adfs/ls/idpinitiatedsignon.htm>
3. From 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.

3. Fare clic sul collegamento oppure copiare e incollare l'URL in un browser per accedere alla pagina di

accesso del provider di identità.

4. Per confermare che è possibile utilizzare SSO per accedere a StorageGRID, selezionare **Accedi a uno dei seguenti siti**, selezionare l'identificativo della parte di base per il nodo di amministrazione principale e fare clic su **Accedi**.



The screenshot shows a login page with the text "You are not signed in." at the top. Below it, there are two radio button options: "Sign in to this site." (which is unselected) and "Sign in to one of the following sites:" (which is selected). Under the second option, there is a dropdown menu with "SG-DC1-ADM1" selected. At the bottom left, there is a blue "Sign in" button.

Viene richiesto di inserire il nome utente e la password.

5. Immettere il nome utente e la password federated.
 - Se le operazioni di accesso e disconnessione SSO hanno esito positivo, viene visualizzato un messaggio di esito positivo.

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

- Se l'operazione SSO non riesce, viene visualizzato un messaggio di errore. Risolvere il problema, eliminare i cookie del browser e riprovare.
6. Ripetere i passaggi precedenti per confermare che è possibile accedere a qualsiasi altro nodo Admin.

Se tutte le operazioni di accesso e disconnessione SSO hanno esito positivo, è possibile attivare SSO.

Abilitazione del single sign-on

Dopo aver utilizzato la modalità sandbox per testare tutti i trust di StorageGRID, sei pronto per attivare il single sign-on (SSO).

Di cosa hai bisogno

- È necessario aver importato almeno un gruppo federated dall'origine dell'identità e aver assegnato al gruppo le autorizzazioni di gestione di accesso root. È necessario confermare che almeno un utente federato disponga dell'autorizzazione di accesso root per Grid Manager e per il tenant Manager per gli account tenant esistenti.
- È necessario aver testato tutti i trust delle parti di base utilizzando la modalità sandbox.

Fasi

1. Selezionare **Configuration Access Control Single Sign-on**.

Viene visualizzata la pagina Single Sign-on (accesso singolo) con l'opzione **Sandbox Mode** (modalità sandbox) selezionata.

2. Impostare lo stato SSO su **Enabled**.
3. Fare clic su **Save** (Salva).

Viene visualizzato un messaggio di avviso.

Warning

Enable single sign-on

After you enable SSO, no local users—including the root user—will be able to sign in to the Grid Manager, the Tenant Manager, the Grid Management API, or the Tenant Management API.

Before proceeding, confirm the following:

- You have imported at least one federated group from the identity source and assigned Root Access management permissions to the group. You must 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.
- You have tested all relying party trusts using sandbox mode.

Are you sure you want to enable single sign-on?

Cancel

OK

4. Esaminare l'avviso e fare clic su **OK**.

Il Single Sign-on è ora attivato.



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.

Disattivazione del single sign-on

È possibile disattivare SSO (Single Sign-on) se non si desidera più utilizzare questa funzionalità. È necessario disattivare il Single Sign-on prima di poter disattivare la federazione delle identità.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

Fasi

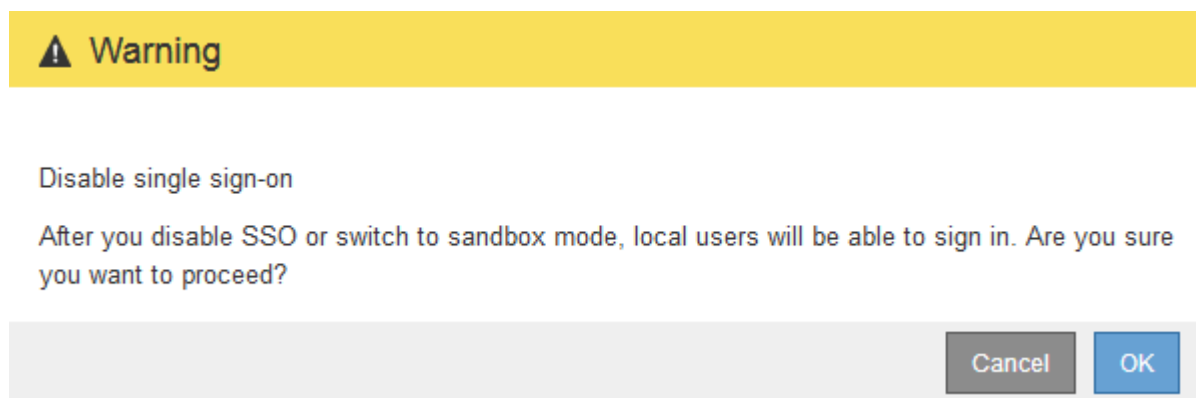
1. Selezionare **Configuration Access Control Single Sign-on**.

Viene visualizzata la pagina Single Sign-on (accesso singolo).

2. Selezionare l'opzione **Disabled**.

3. Fare clic su **Save** (Salva).

Viene visualizzato un messaggio di avviso che indica che gli utenti locali potranno accedere.



4. Fare clic su **OK**.

Al successivo accesso a StorageGRID, viene visualizzata la pagina di accesso a StorageGRID e sono necessari il nome utente e la password di un utente StorageGRID locale o federato.

Disattivare e riabilitare temporaneamente il Single Sign-on per un nodo di amministrazione

Se il sistema SSO (Single Sign-on) non funziona, potrebbe non essere possibile accedere a Grid Manager. In questo caso, è possibile disattivare e riabilitare temporaneamente SSO per un nodo di amministrazione. Per disattivare e riabilitare SSO, è necessario accedere alla shell dei comandi del nodo.

Di cosa hai bisogno

- È necessario disporre di autorizzazioni di accesso specifiche.
- È necessario disporre di `Passwords.txt` file.
- È necessario conoscere la password dell'utente root locale.

A proposito di questa attività

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



La disattivazione di SSO per un nodo di amministrazione non influisce sulle impostazioni SSO per qualsiasi altro nodo di amministrazione nella griglia. La casella di controllo **Enable SSO** (attiva SSO) nella pagina Single Sign-on (accesso singolo) di Grid Manager rimane selezionata e tutte le impostazioni SSO esistenti vengono mantenute, a meno che non vengano aggiornate.

Fasi

1. Accedere a un nodo amministratore:
 - a. Immettere il seguente comando: `ssh admin@Admin_Node_IP`
 - b. Immettere la password elencata in `Passwords.txt` file.
 - c. Immettere il seguente comando per passare a root: `su -`

d. Immettere la password elencata in `Passwords.txt` file.

Una volta effettuato l'accesso 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. Confermare che si desidera disattivare SSO.

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

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

Viene visualizzata la pagina di accesso di Grid Manager perché SSO è stato disattivato.

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

6. Se SSO è stato disattivato temporaneamente perché era necessario correggere la configurazione SSO:

a. Selezionare **Configuration Access Control Single Sign-on**.

b. Modificare le impostazioni SSO non corrette o non aggiornate.

c. Fare clic su **Save** (Salva).

Facendo clic su **Save** (Salva) dalla pagina Single Sign-on (accesso singolo), viene riattivata automaticamente l'SSO per l'intera griglia.

7. Se l'SSO è stato disattivato temporaneamente perché era necessario accedere a Grid Manager per un altro motivo:

a. Eseguire qualsiasi attività o attività da eseguire.

b. Fare clic su **Disconnetti** e chiudere Grid Manager.

c. Riabilitare SSO sul nodo di amministrazione. È possibile eseguire una delle seguenti operazioni:

▪ Eseguire il seguente comando: `enable-saml`

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

Confermare che si desidera attivare SSO.

Un messaggio indica che il Single Sign-on è attivato sul nodo.

◦ Riavviare il nodo Grid: `reboot`

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

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

Informazioni correlate

["Configurazione del single sign-on"](#)

Configurazione dei certificati client dell'amministratore

È possibile utilizzare i certificati client per consentire ai client esterni autorizzati di accedere al database StorageGRID Prometheus. I certificati client offrono un metodo sicuro per utilizzare strumenti esterni per monitorare StorageGRID.

Se si desidera accedere a StorageGRID utilizzando uno strumento di monitoraggio esterno, è necessario caricare o generare un certificato client utilizzando Grid Manager e copiare le informazioni del certificato nello strumento esterno.

Aggiunta di certificati client amministratore

Per aggiungere un certificato client, è possibile fornire il proprio certificato o generarne uno utilizzando Grid Manager.

Di cosa hai bisogno

- È necessario disporre dell'autorizzazione di accesso root.
- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario conoscere l'indirizzo IP o il nome di dominio del nodo di amministrazione.
- È necessario aver configurato il certificato del server dell'interfaccia di gestione StorageGRID e disporre del bundle CA corrispondente
- Se si desidera caricare il proprio certificato, la chiave pubblica e la chiave privata del certificato devono essere disponibili sul computer locale.

Fasi

1. In Grid Manager, selezionare **Configuration Access Control Client Certificates**.

Viene visualizzata la pagina certificati client.

Client Certificates

You can upload or generate one or more client certificates to allow StorageGRID to authenticate external client access.

+ Add Edit ✕ Remove		
Name	Allow Prometheus	Expiration Date
<i>No client certificates configured.</i>		

2. Selezionare **Aggiungi**.

Viene visualizzata la pagina carica certificato.

Upload Certificate

Name 

Allow Prometheus 

Certificate Details

Upload the public key for the client certificate.

Upload Client Certificate

Generate Client Certificate

Cancel


Save

3. Digitare un nome compreso tra 1 e 32 caratteri per il certificato.
4. Per accedere alle metriche Prometheus utilizzando lo strumento di monitoraggio esterno, selezionare la casella di controllo **Consenti Prometheus**.
5. Caricare o generare un certificato:
 - a. Per caricare un certificato, vai su [qui](#).
 - b. Per generare un certificato, andare [qui](#).
6. per caricare un certificato:
 - a. Selezionare **carica certificato client**.
 - b. Cercare la chiave pubblica per il certificato.

Dopo aver caricato la chiave pubblica per il certificato, i campi **metadati del certificato** e **PEM del certificato** vengono compilati.

Upload Certificate

Name  test-certificate-upload

Allow Prometheus 

Certificate Details

Upload the public key for the client certificate.

Upload Client Certificate

Generate Client Certificate

Uploaded file name: client (1).crt

Certificate metadata 

```
Subject DN: /C=US/ST=California/L=Sunnyvale/O=Example Co./OU=IT/CN=*.s3.example.com
Serial Number: 0D:0E:FC:16:75:B8:BE:3E:7D:47:4D:05:49:08:F3:7B:E8:4A:71:90
Issuer DN: /C=US/ST=California/L=Sunnyvale/O=Example Co./OU=IT/CN=*.s3.example.com
Issued On: 2020-06-19T22:11:56.000Z
Expires On: 2021-06-19T22:11:56.000Z
SHA-1 Fingerprint: 13:AA:D6:06:2B:90:FE:B7:7B:EB:1A:83:BE:C3:62:39:B7:A6:E7:F0
SHA-256 Fingerprint: 5C:29:06:6B:CF:81:50:B8:4F:A9:56:F7:A7:AB:3C:36:FA:3D:B7:32:A4:C9:74:85:2C:8D:E6:67:37:C3:AC:60
```

Certificate PEM 

```
-----BEGIN CERTIFICATE-----
MIIDmzCCAoQgAwIBAgIUUDQ78FnW4vj59R00FSQjze+hKcZAwDQYJKoZIhvcNAQEL
BQAwdDELMAkGA1UEBhMCVVMxZzARBgNVBAgMCkNhbg1mb3JuaWEuXzAQBgNVBAcM
CVN1bm55dmFzZTEUMBIGA1UECgwLRXhhbXBsZSBDby4xCzAJBgNVBAsMAk1UMRkw
FwYDQDDDBAqLnMzLmV4YW1wbGUuY29tMB4XDTEwMDYxOTIyMTE1N1oXDTEwMDYx
OTIyMTE1N1owDELMAkGA1UEBhMCVVMxZzARBgNVBAgMCkNhbg1mb3JuaWEuXzAQBg
NVBAcMNVN1bm55dmFzZTEUMBIGA1UECgwLRXhhbXBsZSBDby4xCzAJBgNVBAsMAk1UMRkw
FwYDQDDDBAqLnMzLmV4YW1wbGUuY29tMIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEAzVqq2MnjvVotLeStq1Co4coJmsQ2ygrhuwSza0bgMnjf
cwUgHNVFXGuGlzY/Tl37r3Dk5bu2fyGYAeJ6mqbQA6cE3yp0p5Hx7Cm/AWJknFw6
```

Copy certificate to clipboard


Cancel


Save

- a. Selezionare **Copia certificato negli Appunti** e incollare il certificato nello strumento di monitoraggio esterno.
 - b. Utilizzare uno strumento di modifica per copiare e incollare la chiave privata nello strumento di monitoraggio esterno.
 - c. Selezionare **Save** (Salva) per salvare il certificato in Grid Manager.
7. per generare un certificato:
- a. Selezionare **generate Client Certificate** (genera certificato client).
 - b. Immettere il nome di dominio o l'indirizzo IP del nodo di amministrazione.
 - c. Facoltativamente, immettere un oggetto X.509, denominato anche nome distinto (DN), per identificare l'amministratore proprietario del certificato.
 - d. Se si desidera, selezionare il numero di giorni in cui il certificato è valido. L'impostazione predefinita è 730 giorni.
 - e. Selezionare **generate**.

I campi **metadati del certificato**, **PEM del certificato** e **chiave privata del certificato** vengono compilati.

Upload Certificate

Name  test-certificate-generate

Allow Prometheus 

Certificate Details

Upload the public key for the client certificate.

Upload Client Certificate

Generate Client Certificate

Certificate metadata 

```
Subject DN: /CN=test.com
Serial Number: 08:F8:FB:76:B2:13:E4:DF:54:83:3D:35:56:6F:2A:03:53:B0:E2:0
A
Issuer DN: /CN=test.com
Issued On: 2020-11-20T22:44:46.000Z
Expires On: 2022-11-20T22:44:46.000Z
SHA-1 Fingerprint: 6E:DB:8C:F8:3E:20:68:E4:C6:42:52:5F:32:7E:E7:93:66:69:F3:3
D
SHA-256 Fingerprint: 73:D3:51:83:ED:D3:89:AD:7B:89:4C:AF:AE:34:76:B6:42:FE:0D:
EF:78:C0:A4:66:C2:EB:65:64:C3:D4:7A:B0
```

Certificate PEM 

```
-----BEGIN CERTIFICATE-----
MIICyzCCAhOgAwIBAgIUUCFj7dxITSN9Ugs01Vm8qA1Ow4gowDQYJKoZIhvcNAQEL
BQAwEwERMA8GA1UEAwIgdGVudC5jb20wHhcNMjA1MTIwMjI0NDQ2WjEwMTIw
MjI0NDQ2WjATMREwDwYDVQQDDAh0ZXN0LmNvbTCCASAwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAR02dS9mx2jFrGuBb22Mjcidf/tTcKxLtB9m+4vIwt1gvrR
XgHZ31B9YIqn/Vo729R2mNKKyBwkyQTkGCO2Ixvv0STBLEIWFb8S+TgcIeMyt1V1F
OseBWy402xxjnR3/X+AX+6s2WZIsVe+3CDjGu4ie0V/uVQxx4yA1T9SoKnjBmOa
LCVjL6iVnkUGB8GbkYUPeOaoMjeL6TN1QsoFv9VEB0xBKCP4D7FDbaIy2f9Ng8rS
FEOQoLN=N+XCasLO4D7j2qFqOVUpFJ3M0ohlx0n5pQ78Z5KfYwV=DKg6v52P8UBM
1o6GeuoFaW+dbpLZKp09N1V=VhghXe9AxxN8s+kCAwEAAAMXMBUwEwYDVR0RBBAw
```

Copy certificate to clipboard

Certificate private key 

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEArT20H2bHaM+sa4Fv2kyNyJ1/+1NwzEu0Eab7i8jC2KNC/BFe
AdneUH1ghCf9Wjvb1HaY0orIHCTJBOQYI5kjG+/RjMEb4h29sRx0Bw1gzK2VWUU7
OwF2jPg7bPFOOrf9f4Bf7n1ZkixV75IICMa7iJaRX+5VDPHjIDVP1KggelMGY5oe
JWmVqJWeRQYFI2uTJQ946qgyOwvpm2VDOgW/1UQHTEEoKngFeUNtojL2/02DmtJ8
Q8Cg=202x0JrMe7gFuNmoWo5hS8kUncw6iHXHSfm1Dvxnkp9jBw0MqDm/nY/xQEwW
jw266h9pb51ukt2k703VW0WGCfD7GDPE2yyQIDAQAABoIBAQCfEUfY4pE0Hqcv
2uEL6De4yXMTwg/3Gn+W8mvdgQB4xWEGQrk1kEUG+HTYrFJen6XX0vACDYAC/
Hh1Q67xDVpWRjdpUK0cr1W8ervsEmpBx99MqH9Y2UGw6Yub3UBJaqfDvja4Nvaon
MxaYJRFBLvAR7f2z2xXV5b0zRPA+rn0YCrslLct5Y0K73e0G8naTmwIdm2YM6EE
```

Copy private key to clipboard

 You will not be able to view the certificate private key after you close this dialog. To save the keys for future reference, copy and paste the values to another location.

Cancel Save

- Selezionare **Copia certificato negli Appunti** e incollare il certificato nello strumento di monitoraggio esterno.
- Selezionare **Copia chiave privata negli Appunti** e incollarla nello strumento di monitoraggio esterno.



Non sarà possibile visualizzare la chiave privata dopo aver chiuso la finestra di dialogo. Copiare la chiave in un luogo sicuro.

- Selezionare **Save** (Salva) per salvare il certificato in Grid Manager.

8. Configurare le seguenti impostazioni sullo strumento di monitoraggio esterno, ad esempio Grafana.

Un esempio di Grafana viene mostrato nella seguente schermata:

The screenshot shows the configuration interface for a Prometheus data source in Grafana. The source is named 'sg-prometheus' and is set to 'Default'. The 'HTTP' section is expanded, showing the 'URL' as 'https://admin-node.example.com:9091'. The 'Access' is set to 'Server (default)'. The 'Auth' section is also expanded, showing 'TLS Client Auth' and 'With CA Cert' are enabled. The 'TLS/SSL Auth Details' section is expanded, showing 'CA Cert' and 'ServerName' (admin-node.example.com) are highlighted.

a. **Nome:** Immettere un nome per la connessione.

StorageGRID non richiede queste informazioni, ma è necessario fornire un nome per verificare 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. Abilitare **TLS Client Authorization** e **with CA Certate**.
- d. Copiare e incollare il certificato del server dell'interfaccia di gestione o il bundle CA in **CA Certificate** in TLS/SSL Auth Details (Dettagli autorizzazione TLS/SSL).
- e. **ServerName**: Immettere il nome di dominio del nodo di amministrazione.

Il nome server deve corrispondere al nome di dominio così come appare nel certificato del server dell'interfaccia di gestione.

- f. Salvare e verificare 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 tool di monitoraggio esterno.

Per informazioni sulle metriche, consultare le istruzioni per il monitoraggio e la risoluzione dei problemi di StorageGRID.

Informazioni correlate

["Utilizzo dei certificati di sicurezza StorageGRID"](#)

["Configurazione di un certificato server personalizzato per Grid Manager e Tenant Manager"](#)

["Monitor risoluzione dei problemi"](#)

Modifica dei certificati client amministratore

È possibile modificare un certificato per modificarne il nome, attivare o disattivare l'accesso Prometheus o caricare un nuovo certificato quando quello corrente è scaduto.

Di cosa hai bisogno

- È necessario disporre dell'autorizzazione di accesso root.
- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario conoscere l'indirizzo IP o il nome di dominio del nodo di amministrazione.
- Se si desidera caricare un nuovo certificato e una nuova chiave privata, questi devono essere disponibili sul computer locale.

Fasi

1. Selezionare **Configurazione controllo accessi certificati client**.

Viene visualizzata la pagina certificati client. Vengono elencati i certificati esistenti.

Le date di scadenza del certificato sono elencate nella tabella. Se un certificato scade presto o è già scaduto, viene visualizzato un messaggio nella tabella e viene attivato un avviso.

	Name	Allow Prometheus	Expiration Date
<input type="radio"/>	test-certificate-upload	✓	2021-06-19 16:11:56 MDT
<input checked="" type="radio"/>	test-certificate-generate	✓	2022-08-20 09:42:00 MDT

Displaying 2 certificates.

2. Selezionare il pulsante di opzione a sinistra del certificato che si desidera modificare.
3. Selezionare **Modifica**.

Viene visualizzata la finestra di dialogo Modifica certificato.

Edit Certificate test-certificate-generate

Name

Allow Prometheus

Certificate Details

Upload the public key for the client certificate.

Upload Client Certificate
Generate Client Certificate

Certificate metadata

Subject DN: /CN=test.com
Serial Number: 0C:11:87:6C:1E:FD:13:16:F3:F2:06:D9:DA:6D:BC:CE:2A:A9:C3:53
Issuer DN: /CN=test.com
Issued On: 2020-11-23T15:53:33.000Z
Expires On: 2022-11-23T15:53:33.000Z
SHA-1 Fingerprint: AE:E6:70:A7:D3:C3:39:7A:09:F9:62:9B:81:8A:87:CD:43:16:89:A7
SHA-256 Fingerprint: 63:07:BF:FF:08:1E:84:F1:D4:67:C6:16:B0:35:26:00:C6:A3:13:11:7E:5E:9
0:EC:7A:7B:EF:23:14:55:3D:56

Certificate PEM

```
-----BEGIN CERTIFICATE-----
MIICyzCCAbOgAwIBAgIUDBGHbB79Exbz8gbZ2m28ziqpw1MwDQYJKoZIhvcNAQEL
BQAwEzERMA8GA1UEAwIdGVzdC5jb20wHhcNMjAxMTIzMTU1MzUzNjUzNjUzNjUz
MTU1MzUzNjUzATMREwYDQVQDDAhoZXR0eXN0LmNvbTCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBBAKdGfEeneCDFsLjvLnX9ow6oPrdU7m2EN6SS6xdVI155sCH+
hkwO5a2Mym7EhbNrfwOt2nMjQkcaKIrk8OAmutRgG6N1N12FIW0qYQouzFQ0QddLq
n7ymFw6w8a9zYSu7bLp84Yn0/LSDPk+h3Jio7Mrt2X70It52DRwFmbLNvEvYEtTS
h+FbNh885AIRO2eLxvC0IRij1bySe76wK+Wmc97HdxRSgyxIWk6BD47XC+d0rv55
wvtjc/41qc5xsE6Xm7s2yJg4VARx10y8Icwa9fz00+xPwIdC0NwXkpWJXeBnCoXx
YqQxbWzjz+iVLJqLTMxU8zTIT30zUgN00M82GJUCAwEAAaMKMBUwEwYDVR0RBAAw

```

Copy certificate to clipboard

Cancel Save

4. Apportare le modifiche desiderate al certificato.
5. Selezionare **Save** (Salva) per salvare il certificato in Grid Manager.
6. Se hai caricato un nuovo certificato:
 - a. Selezionare **Copia certificato negli Appunti** per incollare il certificato nello strumento di monitoraggio esterno.
 - b. Utilizzare uno strumento di modifica per copiare e incollare la nuova chiave privata nello strumento di monitoraggio esterno.

c. Salvare e verificare il certificato e la chiave privata nello strumento di monitoraggio esterno.

7. Se è stato generato un nuovo certificato:

a. Selezionare **Copia certificato negli Appunti** per incollare il certificato nello strumento di monitoraggio esterno.

b. Selezionare **Copia chiave privata negli Appunti** per incollare il certificato nello strumento di monitoraggio esterno.



Una volta chiusa la finestra di dialogo, non sarà possibile visualizzare o copiare la chiave privata. Copiare la chiave in un luogo sicuro.

c. Salvare e verificare il certificato e la chiave privata nello strumento di monitoraggio esterno.

Rimozione dei certificati del client amministratore

Se non hai più bisogno di un certificato, puoi rimuoverlo.

Di cosa hai bisogno

- È necessario disporre dell'autorizzazione di accesso root.
- È necessario accedere a Grid Manager utilizzando un browser supportato.

Fasi

1. Selezionare **Configurazione controllo accessi certificati client**.

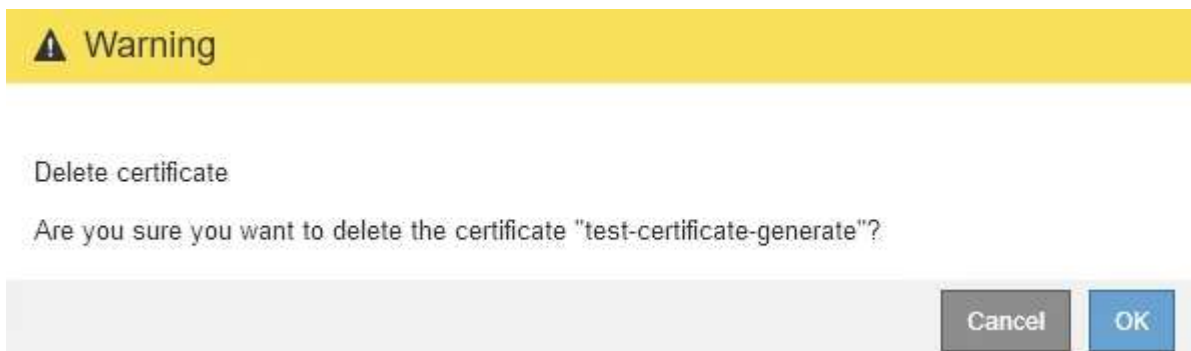
Viene visualizzata la pagina certificati client. Vengono elencati i certificati esistenti.

<input type="button" value="+ Add"/> <input type="button" value="✎ Edit"/> <input type="button" value="✕ Remove"/>		
Name	Allow Prometheus	Expiration Date
<input type="radio"/> test-certificate-upload	✓	2021-06-19 16:11:56 MDT
<input checked="" type="radio"/> test-certificate-generate	✓	2022-08-20 09:42:00 MDT
Displaying 2 certificates.		

2. Selezionare il pulsante di opzione a sinistra del certificato che si desidera rimuovere.

3. Selezionare **Rimuovi**.

Viene visualizzata una finestra di dialogo di conferma.



4. Selezionare **OK**.

Il certificato viene rimosso.

Configurazione dei server di gestione delle chiavi

È possibile configurare uno o più server di gestione delle chiavi (KMS) esterni per proteggere i dati su nodi appliance appositamente configurati.

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).

È possibile utilizzare uno o più server di gestione delle chiavi per gestire le chiavi di crittografia dei nodi di qualsiasi appliance StorageGRID con l'impostazione **crittografia dei nodi** attivata durante l'installazione. L'utilizzo di server di gestione delle chiavi con questi nodi appliance consente di proteggere i dati anche in caso di rimozione di un'appliance dal data center. Una volta crittografati i volumi dell'appliance, non è possibile accedere ai dati dell'appliance a meno che il nodo non sia in grado di comunicare con il KMS.



StorageGRID non crea o gestisce le chiavi esterne utilizzate per crittografare e decrittare i nodi dell'appliance. Se si intende 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 delle attività di gestione chiave non rientra nell'ambito di queste istruzioni. Per assistenza, consultare la documentazione relativa al server di gestione delle chiavi o contattare il supporto tecnico.

Analisi dei metodi di crittografia StorageGRID

StorageGRID offre una serie di opzioni per la crittografia dei dati. È necessario esaminare i metodi disponibili per determinare quali metodi soddisfano i requisiti di protezione dei dati.

La tabella fornisce un riepilogo generale dei metodi di crittografia disponibili in StorageGRID.

Opzione di crittografia	Come funziona	Valido per
Server di gestione delle chiavi (KMS) in Grid Manager	Configurare un server di gestione delle chiavi per il sito StorageGRID (Configurazione Impostazioni di sistema Server di gestione delle chiavi) e abilitare la crittografia dei nodi per l'appliance. Quindi, un nodo appliance si connette al KMS per richiedere una chiave di crittografia a chiave (KEK). Questa chiave crittografata e decrittata la chiave di crittografia dei dati (DEK) su ciascun volume.	Nodi appliance con Node Encryption attivato durante l'installazione. Tutti i dati dell'appliance sono protetti da perdite fisiche o rimozione dal data center. Può essere utilizzato con alcune appliance di storage e servizi StorageGRID.

Opzione di crittografia	Come funziona	Valido per
Protezione dei dischi in Gestione di sistema SANtricity	Se la funzione protezione disco è attivata per un'appliance di storage, è possibile utilizzare Gestione sistema di SANtricity per creare e gestire la chiave di sicurezza. La chiave è necessaria per accedere ai dati sui dischi protetti.	Appliance di storage con dischi FDE (Full Disk Encryption) o FIPS (Federal Information Processing Standard). Tutti i dati presenti sulle unità protette sono protetti da perdita fisica o rimozione dal data center. Non può essere utilizzato con alcune appliance di storage o con altre appliance di servizio. "Appliance di storage SG6000" "Appliance di storage SG5700" "Appliance di storage SG5600"
Opzione della griglia di crittografia degli oggetti memorizzati	L'opzione Stored Object Encryption può essere attivata in Grid Manager (Configuration System Settings Grid Options). Quando questa opzione è attivata, tutti i nuovi oggetti che non sono crittografati a livello di bucket o a livello di oggetto vengono crittografati durante l'acquisizione.	Dati degli oggetti S3 e Swift acquisiti di recente. Gli oggetti memorizzati esistenti non vengono crittografati. I metadati degli oggetti e altri dati sensibili non vengono crittografati. "Configurazione della crittografia degli oggetti memorizzati"
Crittografia bucket S3	Viene inviata una richiesta di crittografia PUT Bucket per abilitare la crittografia per il bucket. Tutti i nuovi oggetti non crittografati a livello di oggetto vengono crittografati durante l'acquisizione.	Solo dati S3 appena acquisiti. specificare la crittografia per il bucket. Gli oggetti bucket esistenti non vengono crittografati. I metadati degli oggetti e altri dati sensibili non vengono crittografati. "Utilizzare S3"
Crittografia a oggetti lato server (SSE) S3	Viene inviata una richiesta S3 per memorizzare un oggetto e includere <code>x-amz-server-side-encryption</code> intestazione della richiesta.	Solo i dati S3 appena acquisiti. specificare la crittografia per l'oggetto. I metadati degli oggetti e altri dati sensibili non vengono crittografati. StorageGRID gestisce le chiavi. "Utilizzare S3"

Opzione di crittografia	Come funziona	Valido per
Crittografia a oggetti S3 lato server con chiavi fornite dal cliente (SSE-C)	Viene inviata una richiesta S3 per memorizzare un oggetto e includere tre intestazioni di richiesta. <ul style="list-style-type: none"> • x-amz-server-side-encryption-customer-algorithm • x-amz-server-side-encryption-customer-key • x-amz-server-side-encryption-customer-key-MD5 	Solo i dati S3 appena acquisiti. specificare la crittografia per l'oggetto. I metadati degli oggetti e altri dati sensibili non vengono crittografati. Le chiavi vengono gestite al di fuori di StorageGRID. "Utilizzare S3"
Crittografia di un volume esterno o di un datastore	Se la piattaforma di implementazione lo supporta, si utilizza un metodo di crittografia esterno a StorageGRID per crittografare un intero volume o datastore.	Tutti i dati degli oggetti, i metadati e i dati di configurazione del sistema, presupponendo che ogni volume o datastore sia crittografato. Un metodo di crittografia esterno offre un controllo più rigoroso sugli algoritmi e sulle chiavi di crittografia. Può essere combinato con gli altri metodi elencati.
Crittografia degli oggetti al di fuori di StorageGRID	Si utilizza un metodo di crittografia esterno a StorageGRID per crittografare i dati degli oggetti e i metadati prima che vengano acquisiti in StorageGRID.	Solo dati a oggetti e metadati (i dati di configurazione del sistema non sono crittografati). Un metodo di crittografia esterno offre 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 gli sviluppatori: Protezione dei dati mediante crittografia lato client"

Utilizzo di più metodi di crittografia

A seconda dei requisiti, è possibile utilizzare più metodi di crittografia alla volta. Ad esempio:

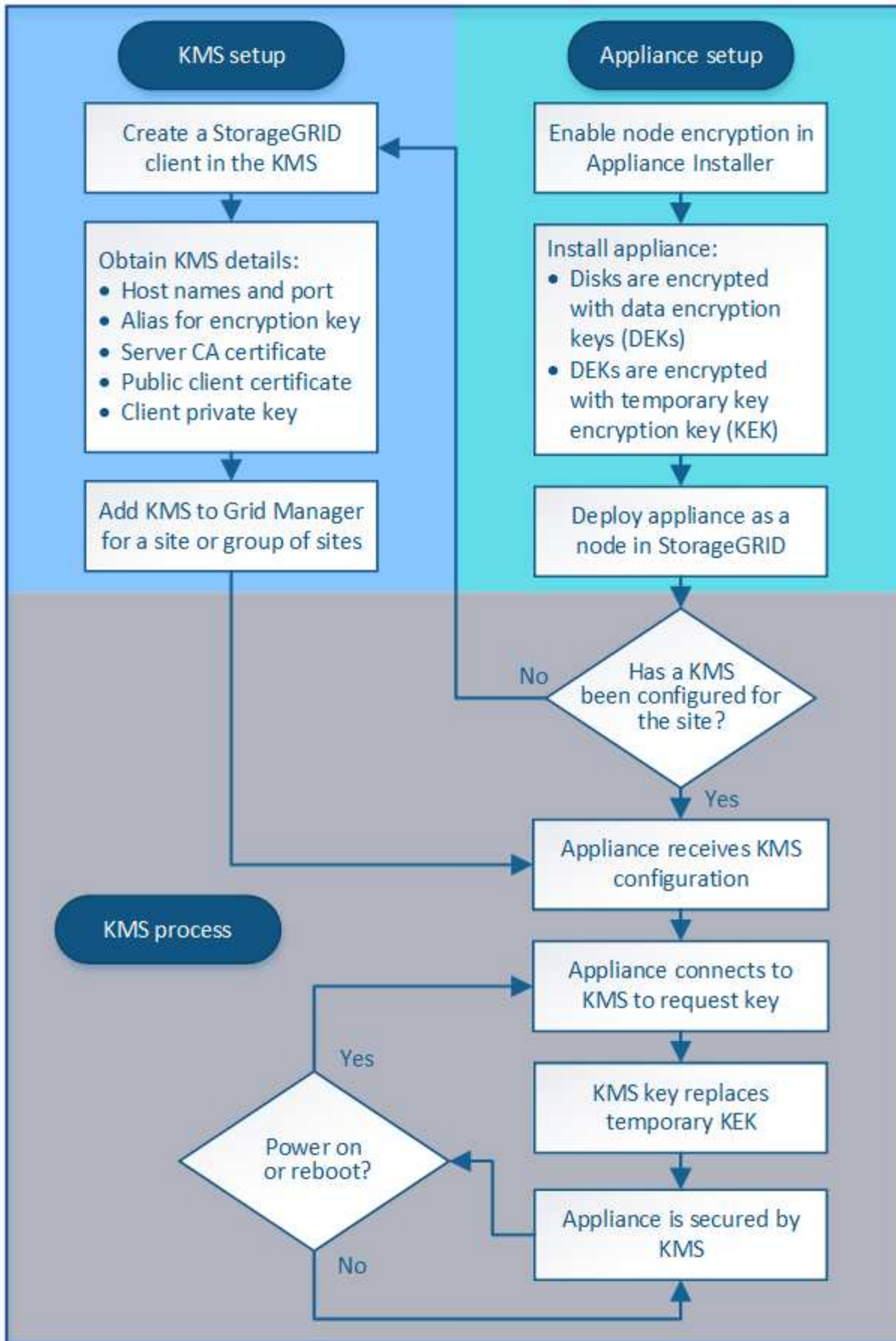
- È possibile utilizzare un KMS per proteggere i nodi dell'appliance e la funzione di sicurezza del disco di Gestione di sistema di SANtricity per "crittografare `din doppio`" i dati sulle unità con crittografia automatica delle stesse appliance.
- È possibile utilizzare un KMS per proteggere i dati sui nodi dell'appliance e l'opzione griglia crittografia oggetti memorizzati per crittografare tutti gli oggetti quando vengono acquisiti.

Se solo una piccola parte degli oggetti richiede la crittografia, prendere in considerazione il controllo della crittografia a livello di bucket o di singolo oggetto. L'abilitazione di più livelli di crittografia comporta un costo aggiuntivo per le performance.

Panoramica di KMS e configurazione dell'appliance

Prima di utilizzare un server di gestione delle chiavi (KMS) per proteggere i dati StorageGRID sui nodi appliance, è necessario completare due attività di configurazione: La configurazione di uno o più server KMS e l'abilitazione della crittografia dei nodi per i nodi appliance. Una volta completate queste due attività di configurazione, il processo di gestione delle chiavi viene eseguito automaticamente.

Il diagramma di flusso mostra i passaggi di alto livello per l'utilizzo di un KMS per proteggere i dati StorageGRID sui nodi dell'appliance.



Il diagramma di flusso mostra la configurazione di KMS e dell'appliance in parallelo; tuttavia, è possibile

configurare i server di gestione delle chiavi prima o dopo aver attivato la crittografia dei nodi per i nuovi nodi appliance, in base ai requisiti.

Configurazione del server di gestione delle chiavi (KMS)

La configurazione di un server di gestione delle chiavi include i seguenti passaggi di alto livello.

Fase	Fare riferimento a.
Accedere al software KMS e aggiungere un client per StorageGRID a ciascun cluster KMS o KMS.	"Configurazione di StorageGRID come client nel KMS"
Ottenere le informazioni richieste per il client StorageGRID sul KMS.	"Configurazione di StorageGRID come client nel KMS"
Aggiungere il KMS al Grid Manager, assegnarlo a un singolo sito o a un gruppo predefinito di siti, caricare i certificati richiesti e salvare la configurazione del KMS.	"Aggiunta di un server di gestione delle chiavi (KMS)"

Configurazione dell'apparecchio

La configurazione di un nodo appliance per l'utilizzo di KMS include i seguenti passaggi di alto livello.

1. Durante la fase di configurazione hardware dell'installazione dell'appliance, utilizzare il programma di installazione dell'appliance StorageGRID per attivare l'impostazione **crittografia del nodo** dell'appliance.



Non è possibile attivare l'impostazione **Node Encryption** dopo l'aggiunta di un'appliance alla griglia e non è possibile utilizzare la gestione delle chiavi esterne per le appliance che non dispongono della crittografia del 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 dei dati casuale (DEK), come segue:
 - I DEK vengono utilizzati 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 viene crittografato mediante una chiave di crittografia della chiave master (KEK). La chiave iniziale KEK è una chiave temporanea che crittografa i DEK fino a quando l'appliance non riesce a connettersi al KMS.
3. Aggiungere il nodo appliance a StorageGRID.

Per ulteriori informazioni, fare riferimento a quanto segue:

- ["SG100 SG1000 Services appliance"](#)
- ["Appliance di storage SG6000"](#)
- ["Appliance di storage SG5700"](#)
- ["Appliance di storage SG5600"](#)

Processo di crittografia per la gestione delle chiavi (si verifica automaticamente)

La crittografia per la gestione delle chiavi include i seguenti passaggi di alto livello che vengono eseguiti automaticamente.

1. Quando si installa un'appliance che ha attivato la crittografia dei nodi nella griglia, StorageGRID determina se esiste una configurazione KMS per il sito che contiene il nuovo nodo.
 - Se un KMS è già stato configurato per il sito, l'appliance riceve la configurazione KMS.
 - Se non è ancora stato configurato un KMS per il sito, i dati dell'appliance continuano a essere crittografati dalla KEK temporanea fino a quando 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 viene ora utilizzata per crittografare e decrittare i DEK per i volumi dell'appliance.



Tutti i dati che esistono prima che il nodo dell'appliance crittografato 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 fino a quando la chiave temporanea non viene sostituita dalla chiave di crittografia KMS.

4. Se l'appliance viene accesa o riavviata, si ricollega al KMS per richiedere la chiave. La chiave, che viene salvata nella memoria volatile, non può sopravvivere a una perdita di alimentazione o a un riavvio.

Considerazioni e requisiti per l'utilizzo di un server di gestione delle chiavi

Prima di configurare un KMS (Key Management Server) esterno, è necessario comprendere le considerazioni e i requisiti.

Quali sono i requisiti KMIP?

StorageGRID supporta KMIP versione 1.4.

["Key Management Interoperability Protocol Specification versione 1.4"](#)

Le comunicazioni tra i nodi dell'appliance e il KMS configurato utilizzano connessioni TLS sicure. StorageGRID supporta i seguenti cifrari TLS v1.2 per KMIP:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

È necessario assicurarsi che ogni nodo dell'appliance che utilizza la crittografia del nodo disponga dell'accesso di rete al cluster KMS o KMS configurato per il sito.

Le impostazioni del firewall di rete devono consentire a ciascun nodo dell'appliance di comunicare attraverso la porta utilizzata per le comunicazioni KMIP (Key Management Interoperability Protocol). La porta KMIP predefinita è 5696.

Quali appliance sono supportate?

È possibile utilizzare un server di gestione delle chiavi (KMS) per gestire le chiavi di crittografia per qualsiasi appliance StorageGRID nel grid con l'impostazione **crittografia nodo** attivata. Questa impostazione può essere attivata solo durante la fase di configurazione hardware dell'installazione dell'appliance mediante il

programma di installazione dell'appliance StorageGRID.



Non è possibile attivare la crittografia dei nodi dopo l'aggiunta di un'appliance alla griglia e non è possibile utilizzare la gestione delle chiavi esterne per le appliance che non hanno attivato la crittografia dei nodi.

È possibile utilizzare il KMS configurato per i seguenti appliance StorageGRID e nodi appliance:

Appliance	Tipo di nodo
Appliance di servizi SG1000	Nodo Admin o nodo gateway
Appliance di servizi SG100	Nodo Admin o nodo gateway
Appliance di storage SG6000	Nodo di storage
Appliance di storage SG5700	Nodo di storage
Appliance di storage SG5600	Nodo di storage

Non è possibile utilizzare il KMS configurato per i nodi software-based (non-appliance), inclusi i seguenti:

- Nodi implementati come macchine virtuali (VM)
- Nodi implementati all'interno di container Docker su host Linux

I nodi implementati su queste altre piattaforme possono utilizzare la crittografia all'esterno di StorageGRID a livello di datastore o disco.

Quando è necessario 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 tenant. Questo ordine garantisce che i nodi siano protetti prima che i dati degli oggetti siano memorizzati su di essi.

È possibile configurare i server di gestione delle chiavi in Grid Manager prima o dopo l'installazione dei nodi appliance.

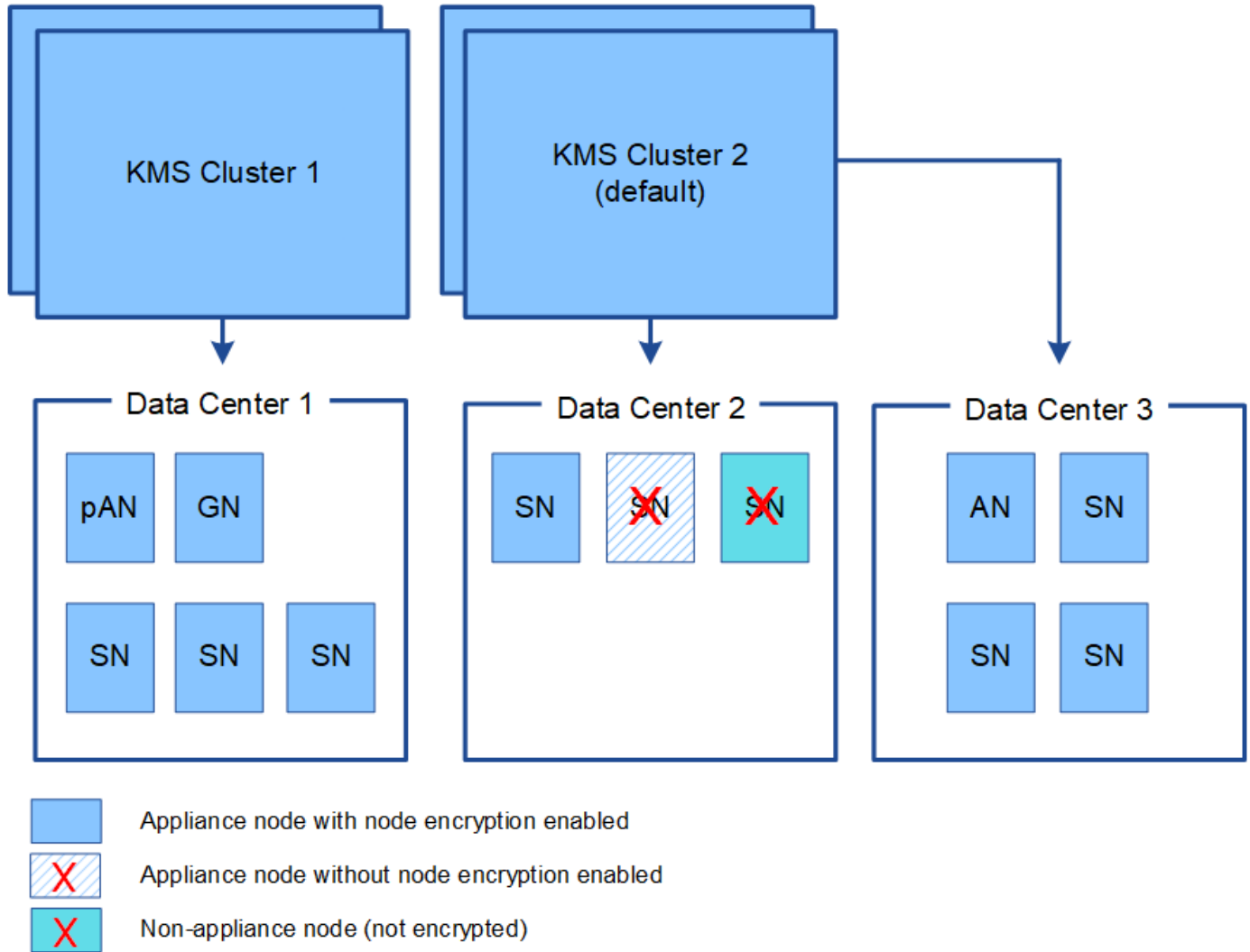
Quanti server di gestione delle chiavi sono necessari?

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'utilizzo di cluster KMS. Ogni cluster KMS contiene più server di gestione delle chiavi replicati che condividono le impostazioni di configurazione e le chiavi di crittografia. Si consiglia di utilizzare i cluster KMS per la gestione delle chiavi perché migliora le funzionalità di failover di una configurazione ad alta disponibilità.

Si supponga, ad esempio, che il sistema StorageGRID disponga di tre siti per data center. È possibile configurare un cluster KMS per fornire una chiave a tutti i nodi appliance nel data center 1 e un secondo cluster KMS per fornire una chiave a tutti i nodi 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.

Tenere presente che non è possibile utilizzare un KMS per i nodi non appliance o per i nodi appliance che non hanno attivato l'impostazione **Node Encryption** durante l'installazione.



Cosa succede quando si ruota una chiave?

Come Best practice per la sicurezza, è necessario ruotare periodicamente la chiave di crittografia utilizzata da ciascun KMS configurato.

Quando si ruota la chiave di crittografia, utilizzare il software KMS per eseguire la rotazione dall'ultima versione della chiave utilizzata a una nuova versione della stessa chiave. Non ruotare su una chiave completamente diversa.



Non tentare mai di ruotare una chiave modificando il nome della chiave (alias) per il KMS in Grid Manager. Al contrario, ruotare la chiave aggiornando la versione della chiave nel software KMS. Utilizzare lo stesso alias per le nuove chiavi utilizzato per le chiavi precedenti. Se si modifica l'alias della chiave per un KMS configurato, StorageGRID potrebbe non essere in grado di decrittare i dati.

Quando è disponibile la nuova versione della chiave:

- Viene distribuito automaticamente ai nodi appliance crittografati nel sito o nei siti associati al KMS. La distribuzione deve avvenire entro un'ora dalla rotazione della chiave.

- Se il nodo dell'appliance crittografato non è in linea quando viene distribuita la nuova versione della chiave, il nodo riceverà la nuova chiave non appena verrà riavviato.
- Se la nuova versione della chiave non può essere utilizzata per crittografare i volumi dell'appliance per qualsiasi motivo, viene attivato l'avviso **rotazione chiave di crittografia KMS non riuscita** per il nodo dell'appliance. Potrebbe essere necessario contattare il supporto tecnico per ottenere assistenza nella risoluzione di questo avviso.

È possibile riutilizzare un nodo appliance dopo averlo crittografato?

Se è necessario installare un'appliance crittografata in un altro sistema StorageGRID, è necessario prima decommissionare il nodo Grid per spostare i dati degli oggetti in un altro nodo. Quindi, è possibile utilizzare il programma di installazione dell'appliance StorageGRID per cancellare la configurazione KMS. La cancellazione della configurazione KMS disattiva l'impostazione **crittografia nodo** e rimuove l'associazione tra il nodo appliance e la configurazione KMS per il sito StorageGRID.



Senza l'accesso alla chiave di crittografia KMS, i dati che rimangono sull'appliance non possono più essere utilizzati e bloccati in modo permanente.

["SG100 SG1000 Services appliance"](#)

["Appliance di storage SG6000"](#)

["Appliance di storage SG5700"](#)

["Appliance di storage SG5600"](#)

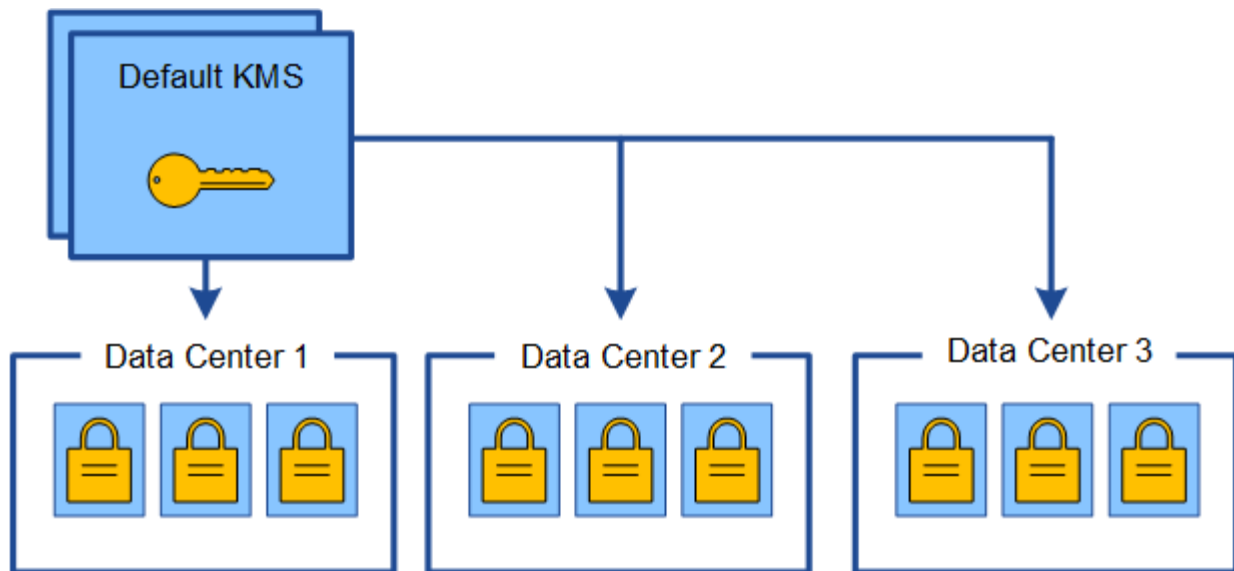
Considerazioni per la modifica del KMS per un sito

Ciascun server di gestione delle chiavi (KMS) o cluster KMS fornisce una chiave di crittografia a tutti i nodi appliance di un singolo sito o di 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 all'altro.

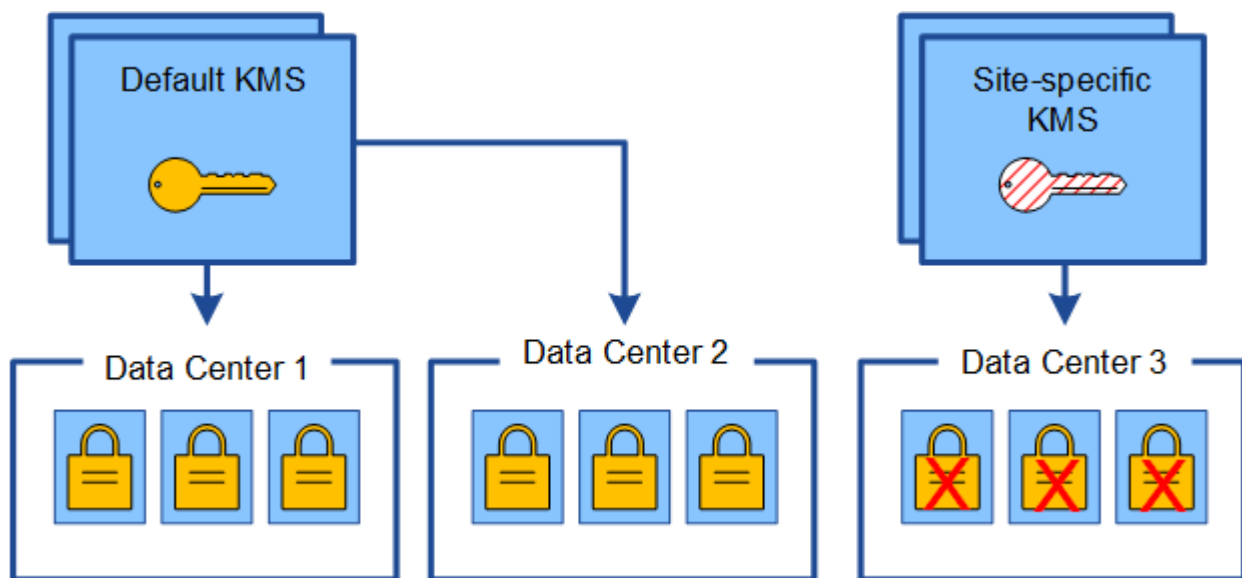
Se si modifica il KMS utilizzato per un sito, è necessario assicurarsi che i nodi appliance precedentemente crittografati in quel sito possano essere decifrati utilizzando la chiave memorizzata nel nuovo KMS. In alcuni casi, potrebbe essere necessario copiare la versione corrente della chiave di crittografia dal KMS originale al nuovo KMS. È necessario assicurarsi che il KMS disponga della chiave corretta per decrittare i nodi crittografati dell'appliance nel sito.

Ad esempio:

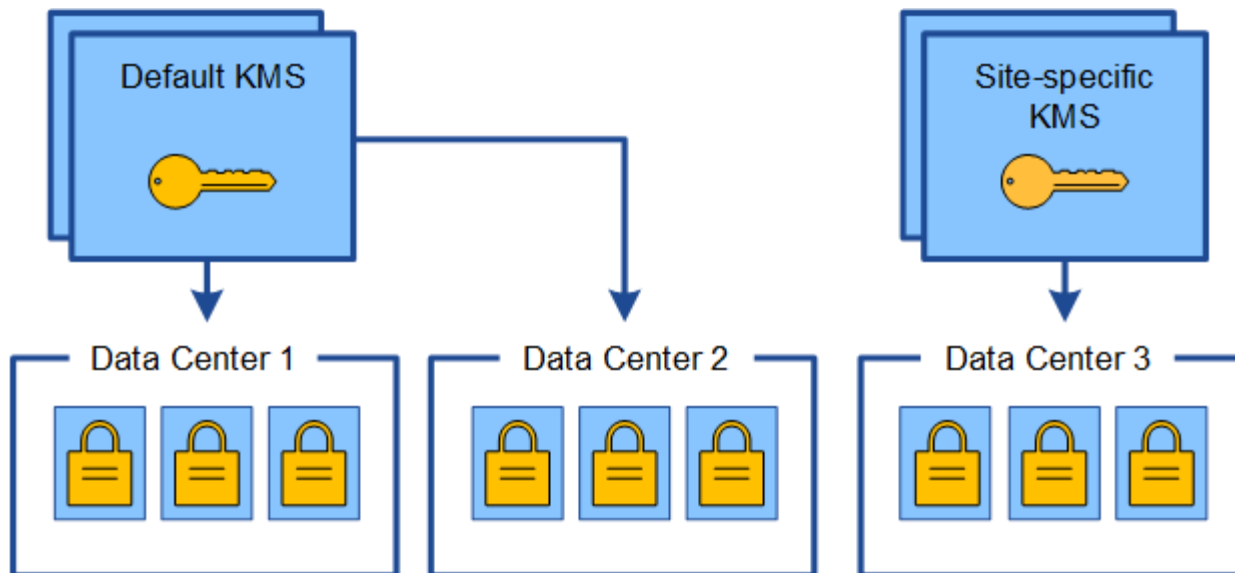
1. Inizialmente si configura un KMS predefinito che si applica a tutti i siti che non dispongono di un KMS dedicato.
2. Una volta salvato il KMS, tutti i nodi appliance con l'impostazione **Node Encryption** attivata si connettono al KMS e richiedono la chiave di crittografia. Questa chiave viene utilizzata per crittografare i nodi dell'appliance in tutti i siti. La stessa chiave deve essere utilizzata anche per decrittare tali appliance.



3. Si decide di aggiungere un KMS specifico del sito 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 decrittare 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 dispone ora della chiave corretta per decrittare i nodi dell'appliance nel data center 3, in modo che possa essere salvato in StorageGRID.



Casi di utilizzo per la modifica del KMS utilizzato per un sito

La tabella riassume i passaggi necessari per i casi più comuni di modifica del KMS per un sito.

Caso d'utilizzo per la modifica del KMS di un sito	Passaggi richiesti
<p>Si dispone di una o più voci KMS specifiche del sito e si desidera utilizzarne una come KMS predefinito.</p>	<p>Modificare il KMS specifico del sito. Nel campo Gestisci chiavi per, selezionare Siti non gestiti da un altro KMS (KMS predefinito). Il KMS specifico del sito verrà ora utilizzato come KMS predefinito. Si applica a tutti i siti che non dispongono di un KMS dedicato.</p> <p>"Modifica di un server di gestione delle chiavi (KMS)"</p>
<p>Si dispone di un KMS predefinito e si aggiunge un nuovo sito in un'espansione. Non si desidera utilizzare il KMS predefinito per il nuovo sito.</p>	<ol style="list-style-type: none"> 1. Se i nodi dell'appliance nel nuovo sito sono già stati crittografati con il 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, aggiungere il nuovo KMS e selezionare il sito. <p>"Aggiunta di un server di gestione delle chiavi (KMS)"</p>

Caso d'utilizzo per la modifica del KMS di un sito	Passaggi richiesti
Si desidera che il KMS di un sito utilizzi un server diverso.	<ol style="list-style-type: none"> 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, modificare la configurazione KMS esistente e inserire il nuovo nome host o indirizzo IP. <p>"Aggiunta di un server di gestione delle chiavi (KMS)"</p>

Configurazione di StorageGRID come client nel KMS

È necessario configurare StorageGRID come client per ogni server di gestione delle chiavi esterno o cluster KMS prima di poter aggiungere KMS a StorageGRID.

A proposito di questa attività

Queste istruzioni si applicano a Thales CipherTrust Manager k170v, versioni 2.0, 2.1 e 2.2. In caso di domande sull'utilizzo di un altro server di gestione delle chiavi con StorageGRID, contattare il supporto tecnico.

["Thales CipherTrust Manager"](#)

Fasi

1. Dal software KMS, creare un client StorageGRID per ogni cluster KMS o KMS che si intende utilizzare.

Ogni KMS gestisce una singola chiave di crittografia per i nodi delle appliance StorageGRID in un singolo sito o in un gruppo di siti.

2. Dal software KMS, creare una chiave di crittografia AES per ogni cluster KMS o KMS.

La chiave di crittografia deve essere esportabile.

3. Registrare le seguenti informazioni per ciascun cluster KMS o KMS.

Queste informazioni sono necessarie quando si aggiunge il KMS a StorageGRID.

- Nome host o indirizzo IP per ciascun server.
- Porta KMIP utilizzata dal KMS.
- Alias chiave per la chiave di crittografia nel KMS.



La chiave di crittografia deve già esistere nel KMS. StorageGRID non crea o gestisce chiavi KMS.

4. Per ogni cluster KMS o 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 con codifica 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 con Privacy Enhanced Mail (PEM) base-64.
- 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 connetterà.



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 del client pubblico rilasciato a StorageGRID dal KMS esterno e la chiave privata per il certificato del client.

Il certificato client consente a StorageGRID di autenticarsi nel KMS.

Aggiunta di un server di gestione delle chiavi (KMS)

Utilizzare la procedura guidata del server di gestione delle chiavi StorageGRID per aggiungere ogni cluster KMS o KMS.

Di cosa hai bisogno

- È necessario aver esaminato ["considerazioni e requisiti per l'utilizzo di un server di gestione delle chiavi"](#).
- Devi avere ["StorageGRID configurato come client nel KMS"](#) E devono essere disponibili le informazioni richieste per ciascun cluster KMS o KMS
- È necessario disporre dell'autorizzazione di accesso root.
- È necessario accedere a Grid Manager utilizzando un browser supportato.

A proposito di questa attività

Se possibile, configurare qualsiasi server di gestione delle chiavi specifico del sito prima di configurare un KMS predefinito che si applica a tutti i siti non gestiti da un altro KMS. Se si crea prima il KMS predefinito, tutte le appliance crittografate con nodo nella griglia verranno crittografate con il KMS predefinito. Se si desidera creare un KMS specifico del sito in un secondo momento, è necessario prima copiare la versione corrente della chiave di crittografia dal KMS predefinito al nuovo KMS.

["Considerazioni per la modifica del KMS per un sito"](#)

Fasi

1. ["Fase 1: Inserire i dettagli KMS"](#)
2. ["Fase 2: Caricare il certificato del server"](#)
3. ["Fase 3: Caricare i certificati client"](#)

Fase 1: Inserire i dettagli KMS

Nella fase 1 (inserire i dettagli KMS) della procedura guidata Add a Key Management Server (Aggiungi un server di gestione delle chiavi), vengono forniti i dettagli relativi al cluster KMS o KMS.

Fasi

1. Selezionare **Configuration System Settings Key Management Server**.

Viene visualizzata la pagina Key Management Server (Server di gestione chiavi) con la scheda Configuration Details (Dettagli configurazione) selezionata.

Key Management Server

If your StorageGRID system includes appliance nodes with node encryption enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID at rest.

Configuration Details

Encrypted Nodes

You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

Before adding a KMS:

- Ensure that the KMS is KMIP-compliant.
- Configure StorageGRID as a client in the KMS.
- Enable node encryption for each appliance during appliance installation. You cannot enable node encryption after an appliance is added to the grid and you cannot use a KMS for appliances that do not have node encryption enabled.

For complete instructions, see [administering StorageGRID](#).

KMS Display Name	Key Name	Manages keys for	Hostname	Certificate Status
No key management servers have been configured. Select Create.				

2. Selezionare **Crea**.

Viene visualizzata la fase 1 (immettere i dettagli KMS) della procedura guidata Add a Key Management Server (Aggiungi un server di gestione delle chiavi).

Add a Key Management Server

1 Enter KMS Details 2 Upload Server Certificate 3 Upload Client Certificates

Enter information about the external key management server (KMS) and the StorageGRID client you configured in that KMS. If you are configuring a KMS cluster, select + to add a hostname for each server in the cluster.

KMS Display Name

Key Name

Manages keys for

Port

Hostname

3. Immettere le seguenti informazioni per il KMS e il client StorageGRID configurati in tale KMS.

Campo	Descrizione
Nome visualizzato DI KMS	Un nome descrittivo per aiutarti a identificare questo KMS. Deve essere compreso tra 1 e 64 caratteri.
Key Name (Nome chiave)	L'alias esatto della chiave per il client StorageGRID nel KMS. Deve essere compreso tra 1 e 255 caratteri.
Gestisce le chiavi per	<p>Il sito StorageGRID che sarà associato a questo KMS. Se possibile, è necessario configurare qualsiasi server di gestione delle chiavi specifico del sito prima di configurare un KMS predefinito che si applica a tutti i siti non gestiti da un altro KMS.</p> <ul style="list-style-type: none"> • Selezionare un sito se il KMS gestirà le chiavi di crittografia per i nodi dell'appliance in un sito specifico. • Selezionare Siti non gestiti da un altro KMS (KMS predefinito) per configurare un KMS predefinito da applicare a tutti i siti che non dispongono di un KMS dedicato e a tutti i siti aggiunti nelle espansioni successive. <p>Nota: Quando si salva la configurazione KMS, si verifica Un errore di convalida se si seleziona un sito precedentemente crittografato dal KMS predefinito ma non si fornisce la versione corrente della chiave di crittografia originale al nuovo KMS.</p>
Porta	La porta utilizzata dal server KMS per le comunicazioni KMIP (Key Management Interoperability Protocol). Il valore predefinito è 5696, ovvero la porta standard KMIP.
Nome host	<p>Il nome di dominio completo o l'indirizzo IP del KMS.</p> <p>Nota: il campo 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 di un cluster KMS.</p>

4. Se si utilizza un cluster KMS, selezionare il segno più **+** per aggiungere un nome host per ciascun server nel cluster.
5. Selezionare **Avanti**.

Viene visualizzata la fase 2 (carica certificato server) della procedura guidata Add a Key Management Server (Aggiungi un server di gestione delle chiavi).

Fase 2: Caricare il certificato del server


Nella fase 2 (carica certificato server) della procedura guidata Add a Key Management Server (Aggiungi un server di gestione delle chiavi), viene caricato il certificato del server (o bundle di certificati) per il KMS. Il certificato del server consente al KMS esterno di autenticarsi su StorageGRID.

Fasi

1. Dal **passaggio 2 (carica certificato server)**, individuare la posizione del certificato server o del bundle di certificati salvato.

Add a Key Management Server

Upload a server certificate signed by the certificate authority (CA) on the external key management server (KMS) or a certificate bundle. The server certificate allows the KMS to authenticate itself to StorageGRID.

Server Certificate 

2. Caricare il file del certificato.

Vengono visualizzati i metadati del certificato del server.

Add a Key Management Server



Upload a server certificate signed by the certificate authority (CA) on the external key management server (KMS) or a certificate bundle. The server certificate allows the KMS to authenticate itself to StorageGRID.

Server Certificate ⓘ k170vCA.pem

Server Certificate Metadata

```
Server DN: /C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA
Serial Number: 71:CD:6D:72:53:B5:6D:0A:8C:69:13:0D:4D:D7:81:0E
Issue DN: /C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA
Issued On: 2020-10-15T21:12:45.000Z
Expires On: 2030-10-13T21:12:45.000Z
SHA-1 Fingerprint: EE:E4:6E:17:86:DF:56:B4:F5:AF:A2:3C:BD:56:6B:10:DB:B2:5A:79
```

Cancel

Back

Next



Se hai caricato un bundle di certificati, i metadati di ciascun certificato vengono visualizzati nella relativa scheda.

3. Selezionare **Avanti**.

Viene visualizzata la fase 3 (carica certificati client) della procedura guidata Add a Key Management Server (Aggiungi un server di gestione delle chiavi).

Fase 3: Caricare i certificati client

Nella fase 3 (carica certificati client) della procedura guidata Add a Key Management Server (Aggiungi un server di gestione delle chiavi), vengono caricati il certificato client e la chiave privata del certificato client. Il certificato client consente a StorageGRID di autenticarsi nel KMS.

Fasi

1. Dal **passaggio 3 (carica certificati client)**, individuare la posizione del certificato client.

Add a Key Management Server



Upload the client certificate and the client certificate private key. The client certificate is issued to StorageGRID by the external key management server (KMS), and it allows StorageGRID to authenticate itself to the KMS.

Client Certificate 

Client Certificate Private Key 

Cancel

Back

Save

2. Caricare il file di certificato del client.

Vengono visualizzati i metadati del certificato client.

3. Individuare la posizione della chiave privata per il certificato client.


4. Caricare il file della chiave privata.

Vengono visualizzati i metadati per il certificato client e la chiave privata del certificato client.

Add a Key Management Server



Upload the client certificate and the client certificate private key. The client certificate is issued to StorageGRID by the external key management server (KMS), and it allows StorageGRID to authenticate itself to the KMS.

Client Certificate  k170vClientCert.pem

```
Server DN: /CN=admin/UID=  
Serial Number: 7D:5A:8A:27:02:40:C8:F5:19:A1:28:22:E7:D6:E2:EB  
Issue DN: /C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA  
Issued On: 2020-10-15T23:31:49.000Z  
Expires On: 2022-10-15T23:31:49.000Z  
SHA-1 Fingerprint: A7:10:AC:39:85:42:80:8F:FF:62:AD:A1:BD:CF:4C:90:F3:E9:36:69
```

Client Certificate Private Key  k170vClientKey.pem

Cancel

Back

Save

5. Selezionare **Salva**.

Vengono verificate 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 nel 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 Server gestione chiavi viene visualizzato come Sconosciuto. Per ottenere lo stato effettivo di ciascun certificato, StorageGRID potrebbe impiegare fino a 30 minuti. È necessario aggiornare il browser Web per visualizzare lo stato corrente.

6. Se viene visualizzato un messaggio di errore quando si seleziona **Salva**, rivedere i dettagli del messaggio e selezionare **OK**.

Ad esempio, se un test di connessione non riesce, potrebbe essere visualizzato un errore 422: Unprocessable Entity.

7. Se si desidera salvare la configurazione corrente senza verificare la connessione esterna, selezionare **Force Save** (forza salvataggio).

Add a Key Management Server



Upload the client certificate and the client certificate private key. The client certificate is issued to StorageGRID by the external key management server (KMS), and it allows StorageGRID to authenticate itself to the KMS.

Client Certificate ⓘ k170vClientCert.pem

Server DN: /CN=admin/UID=
Serial Number: 7D:5A:8A:27:02:40:C8:F5:19:A1:28:22:E7:D6:E2:EB
Issue DN: /C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA
Issued On: 2020-10-15T23:31:49.000Z
Expires On: 2022-10-15T23:31:49.000Z
SHA-1 Fingerprint: A7:10:AC:39:85:42:80:8F:FF:62:AD:A1:BD:CF:4C:90:F3:E9:36:69

Client Certificate Private Key ⓘ k170vClientKey.pem

Select **Force Save** to save this KMS without testing the external connections. If there is an issue with the configuration, you might not be able to reboot any FDE-enabled appliance nodes at the affected site, and you might lose access to your data.

Cancel

Back

Force Save

Save



Selezionando **forza salvataggio** viene salvata la configurazione KMS, ma non viene eseguita una verifica della connessione esterna da ciascuna appliance a quel KMS. In caso di problemi con la configurazione, potrebbe non essere possibile riavviare i nodi dell'appliance che hanno attivato la crittografia dei nodi nel sito interessato. È possibile che l'accesso ai dati venga perso fino a quando i problemi non vengono risolti.

- Controllare l'avviso di conferma e selezionare **OK** se si desidera forzare il salvataggio della configurazione.

Warning

Confirm force-saving the KMS configuration

Are you sure you want to save this KMS without testing the external connections?

If there is an issue with the configuration, you might not be able to reboot any appliance nodes with node encryption enabled at the affected site, and you might lose access to your data.

Cancel

OK

La configurazione KMS viene salvata ma la connessione al KMS non viene verificata.

Visualizzazione dei dettagli di KMS

È possibile visualizzare informazioni su ciascun server di gestione delle chiavi (KMS) nel sistema StorageGRID, incluso lo stato corrente dei certificati server e client.

Fasi

1. Selezionare **Configuration System Settings Key Management Server**.

Viene visualizzata la pagina Key Management Server (Server di gestione delle chiavi). La scheda Dettagli configurazione mostra tutti i server di gestione delle chiavi configurati.

Key Management Server

If your StorageGRID system includes appliance nodes with node encryption enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID at rest.

Configuration Details

Encrypted Nodes

You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

Before adding a KMS:

- Ensure that the KMS is KMP-compliant.
- Configure StorageGRID as a client in the KMS.
- Enable node encryption for each appliance during appliance installation. You cannot enable node encryption after an appliance is added to the grid and you cannot use a KMS for appliances that do not have node encryption enabled.

For complete instructions, see [administering StorageGRID](#).

+ Create Edit Remove				
KMS Display Name	Key Name	Manages keys for	Hostname	Certificate Status
Default KMS	test	Sites not managed by another KMS (default KMS)	10.96.99.164	✓ All certificates are valid

2. Rivedere le informazioni nella tabella per ciascun KMS.

Campo	Descrizione
Nome visualizzato DI KMS	Il nome descrittivo del KMS.
Key Name (Nome chiave)	L'alias della chiave per il client StorageGRID nel KMS.
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) .

Campo	Descrizione
Nome host	<p>Il nome di dominio completo o l'indirizzo IP del KMS.</p> <p>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.</p> <p>Ad esempio: 10.10.10.10 and 10.10.10.11 oppure 10.10.10.10 and 2 others.</p> <p>Per visualizzare tutti i nomi host in un cluster, selezionare un KMS e quindi selezionare Edit.</p>
Stato del certificato	<p>Stato corrente del certificato del server, del certificato CA opzionale e del certificato del client: Valido, scaduto, in fase di scadenza o sconosciuto.</p> <p>Nota: potrebbero essere necessari 30 minuti per ottenere gli aggiornamenti dello stato del certificato da parte di StorageGRID. È necessario aggiornare il browser Web per visualizzare i valori correnti.</p>

- Se lo stato del certificato è sconosciuto, attendere fino a 30 minuti, quindi aggiornare il browser Web.



Subito dopo aver aggiunto un KMS, lo stato del certificato nella pagina Server gestione chiavi viene visualizzato come Sconosciuto. Per ottenere lo stato effettivo di ciascun certificato, StorageGRID potrebbe impiegare fino a 30 minuti. È necessario aggiornare il browser Web per visualizzare lo stato effettivo.

- Se la colonna Stato certificato indica che un certificato è scaduto o sta per scadere, risolvere il problema il prima possibile.

Consultare le azioni consigliate per gli avvisi **scadenza certificato CA KMS**, **scadenza certificato client KMS** e **scadenza certificato server KMS** nelle istruzioni per il monitoraggio e la risoluzione dei problemi di StorageGRID.



Per mantenere l'accesso ai dati, è necessario risolvere al più presto eventuali problemi di certificato.

Informazioni correlate

["Monitor risoluzione dei problemi"](#)

Visualizzazione dei nodi crittografati

È possibile visualizzare informazioni sui nodi appliance nel sistema StorageGRID per i quali è stata attivata l'impostazione **crittografia nodo**.

Fasi

1. Selezionare **Configuration System Settings Key Management Server**.

Viene visualizzata la pagina Key Management Server (Server di gestione delle chiavi). La scheda Dettagli configurazione mostra tutti i server di gestione delle chiavi configurati.

Key Management Server

If your StorageGRID system includes appliance nodes with node encryption enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID at rest.

Configuration Details Encrypted Nodes

You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

Before adding a KMS:

- Ensure that the KMS is KMP-compliant.
- Configure StorageGRID as a client in the KMS.
- Enable node encryption for each appliance during appliance installation. You cannot enable node encryption after an appliance is added to the grid and you cannot use a KMS for appliances that do not have node encryption enabled.

For complete instructions, see [administering StorageGRID](#).

+ Create	Edit	Remove			
KMS Display Name ?	Key Name ?	Manages keys for ?	Hostname ?	Certificate Status ?	
● Default KMS	test	Sites not managed by another KMS (default KMS)	10.96.99.164	✓ All certificates are valid	

2. Nella parte superiore della pagina, selezionare la scheda **nodi crittografati**.

Key Management Server

If your StorageGRID system includes appliance nodes with Full Disk Encryption (FDE) enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID data at rest.

Configuration Details **Encrypted Nodes**

You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

La scheda nodi crittografati elenca i nodi appliance nel sistema StorageGRID con l'impostazione **crittografia nodo** attivata.

Configuration Details Encrypted Nodes

Review the KMS status for all appliance nodes that have node encryption enabled. Address any issues immediately to ensure your data is fully protected. If no KMS exists for a site, select Configuration Details and add a KMS.

Nodes with Encryption Enabled

Node Name	Node Type	Site	KMS Display Name ?	Key UID ?	Status ?
SGA-010-096-104-67 🔗	Storage Node	Data Center 1	Default KMS	41b0...5c57	✓ Connected to KMS (2021-03-12 10:59:32 MST)

3. Esaminare le informazioni contenute nella tabella per ciascun nodo appliance.

Colonna	Descrizione
Nome del nodo	Il nome del nodo appliance.
Tipo di nodo	Il tipo di nodo: Storage, Admin o Gateway.
Sito	Il nome del sito StorageGRID in cui è installato il nodo.
Nome visualizzato DI KMS	Il nome descrittivo del KMS utilizzato per il nodo. Se non è elencato alcun KMS, selezionare la scheda Dettagli di configurazione per aggiungere un KMS. "Aggiunta di un server di gestione delle chiavi (KMS)"
UID chiave	ID univoco della chiave di crittografia utilizzata per crittografare e decrittare i dati sul nodo dell'appliance. Per visualizzare un intero UID chiave, spostare il cursore sulla cella. Un trattino (--) indica che l'UID della chiave non è noto, 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, l'indicatore data e ora viene aggiornato ogni 30 minuti. L'aggiornamento dello stato di connessione può richiedere alcuni minuti dopo le modifiche della configurazione KMS. Nota: per visualizzare i nuovi valori, è necessario aggiornare il browser Web.

4. Se la colonna Status (Stato) indica un problema KMS, risolverlo immediatamente.

Durante le normali operazioni KMS, lo stato sarà **connesso a KMS**. Se un nodo viene disconnesso dalla rete, viene visualizzato lo stato di connessione del nodo (amministrativamente inattivo o Sconosciuto).

Gli altri messaggi di stato corrispondono agli avvisi StorageGRID con gli stessi nomi:

- Impossibile caricare la configurazione KMS
- Errore di connettività KMS
- Nome chiave di crittografia KMS non trovato
- Rotazione della chiave di crittografia KMS non riuscita
- La chiave KMS non è riuscita a decrittare un volume dell'appliance
- KMS non è configurato vedere le azioni consigliate per questi avvisi nelle istruzioni per il monitoraggio e la risoluzione dei problemi di StorageGRID.



È necessario affrontare immediatamente qualsiasi problema per garantire la completa protezione dei dati.

Informazioni correlate

["Monitor risoluzione dei problemi"](#)

Modifica di un server di gestione delle chiavi (KMS)

Potrebbe essere necessario modificare la configurazione di un server di gestione delle chiavi, ad esempio, se un certificato sta per scadere.

Di cosa hai bisogno

- È necessario aver esaminato ["considerazioni e requisiti per l'utilizzo di un server di gestione delle chiavi"](#).
- Se si prevede di aggiornare il sito selezionato per un KMS, è necessario esaminare ["Considerazioni per la modifica del KMS per un sito"](#).
- È necessario disporre dell'autorizzazione di accesso root.
- È necessario accedere a Grid Manager utilizzando un browser supportato.

Fasi

1. Selezionare **Configuration System Settings Key Management Server**.

Viene visualizzata la pagina Key Management Server (Server di gestione delle chiavi) che mostra tutti i server di gestione delle chiavi configurati.

Key Management Server

If your StorageGRID system includes appliance nodes with node encryption enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID at rest.

Configuration Details

Encrypted Nodes

You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

Before adding a KMS:


- Ensure that the KMS is KMIP-compliant.
- Configure StorageGRID as a client in the KMS.
- Enable node encryption for each appliance during appliance installation. You cannot enable node encryption after an appliance is added to the grid and you cannot use a KMS for appliances that do not have node encryption enabled.

For complete instructions, see [administering StorageGRID](#).

+ Create	✎ Edit	🗑 Remove			
KMS Display Name ?	Key Name ?	Manages keys for ?	Hostname ?	Certificate Status ?	
<input checked="" type="radio"/> Default KMS	test	Sites not managed by another KMS (default KMS)	10.96.99.164	✔ All certificates are valid	

2. Selezionare il KMS che si desidera modificare e selezionare **Edit** (Modifica).
3. Se si desidera, aggiornare i dettagli nel **Passo 1 (Immetti dettagli KMS)** della procedura guidata Modifica un server di gestione delle chiavi.

Campo	Descrizione
Nome visualizzato DI KMS	Un nome descrittivo per aiutarti a identificare questo KMS. Deve essere compreso tra 1 e 64 caratteri.

Campo	Descrizione
Key Name (Nome chiave)	<p>L'alias esatto della chiave per il client StorageGRID nel KMS. Deve essere compreso tra 1 e 255 caratteri.</p> <p>È sufficiente modificare il nome della chiave solo in rari casi. Ad esempio, è necessario modificare il nome della chiave se l'alias viene rinominato in KMS o se tutte le versioni della chiave precedente sono state copiate nella cronologia delle versioni del nuovo alias.</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;">  <p>Non tentare mai di ruotare una chiave cambiando il nome della chiave (alias) per il KMS. Al contrario, ruotare la chiave aggiornando la versione della chiave nel software 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 si modifica l'alias della chiave per un KMS configurato, StorageGRID potrebbe non essere in grado di decrittare i dati.</p> <p>"Considerazioni e requisiti per l'utilizzo di un server di gestione delle chiavi"</p> </div>
Gestisce le chiavi per	<p>Se si sta modificando un KMS specifico del sito e non si dispone già di un KMS predefinito, selezionare Sites Not Managed by another KMS (default KMS) (Siti non gestiti da un altro KMS (default KMS)*). 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.</p> <p>Nota: se si modifica un KMS specifico del sito, non è possibile selezionare un altro sito. Se si sta modificando il KMS predefinito, non è possibile selezionare un sito specifico.</p>
Porta	<p>La porta utilizzata dal server KMS per le comunicazioni KMIP (Key Management Interoperability Protocol). Il valore predefinito è 5696, ovvero la porta standard KMIP.</p>
Nome host	<p>Il nome di dominio completo o l'indirizzo IP del KMS.</p> <p>Nota: il campo 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 di un cluster KMS.</p>

4. Se si sta configurando un cluster KMS, selezionare il segno più **+** per aggiungere un nome host per ciascun server nel cluster.
5. Selezionare **Avanti**.

Viene visualizzata la fase 2 (carica certificato server) della procedura guidata Modifica un server di gestione delle chiavi.

6. Se è necessario sostituire il certificato del server, selezionare **Sfogliare** e caricare il nuovo file.

7. Selezionare **Avanti**.

Viene visualizzata la fase 3 (carica 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 **Browse** (Sfogliare) e caricare i nuovi file.

9. Selezionare **Salva**.

Vengono testate le connessioni tra il server di gestione delle chiavi e tutti i nodi di appliance con crittografia a nodo nei siti interessati. Se tutte le connessioni dei nodi sono valide e la chiave corretta viene trovata nel 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, esaminare i dettagli del messaggio e selezionare **OK**.

Ad esempio, se il sito selezionato per questo KMS è già gestito da un altro KMS o se un test di connessione non ha avuto esito positivo, potrebbe essere visualizzato un errore 422: Unprocessable Entity.

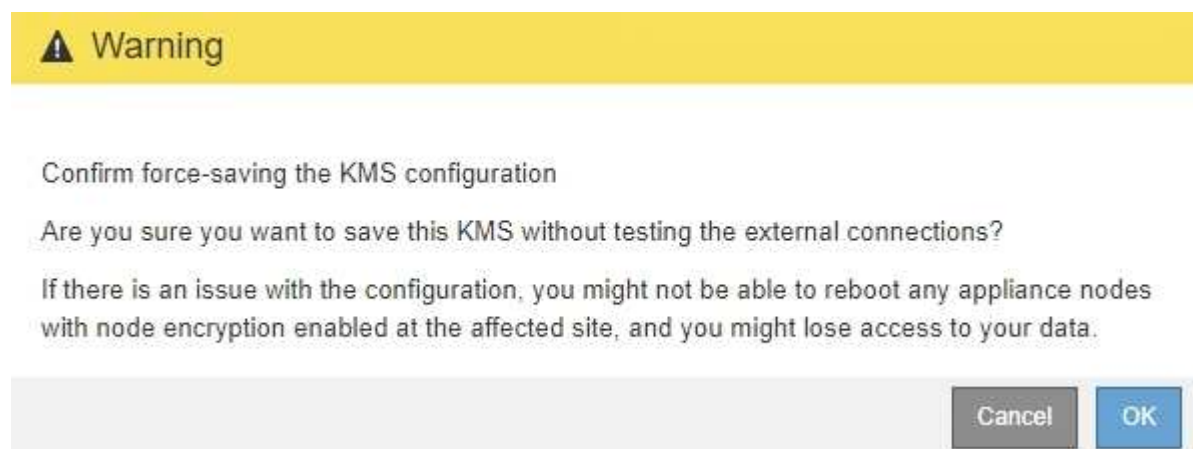
11. Se è necessario salvare la configurazione corrente prima di risolvere gli errori di connessione, selezionare **forza salvataggio**.



Selezionando **forza salvataggio** viene salvata la configurazione KMS, ma non viene eseguita una verifica della connessione esterna da ciascuna appliance a quel KMS. In caso di problemi con la configurazione, potrebbe non essere possibile riavviare i nodi dell'appliance che hanno attivato la crittografia dei nodi nel sito interessato. È possibile che l'accesso ai dati venga perso fino a quando i problemi non vengono risolti.

La configurazione KMS viene salvata.

12. Controllare l'avviso di conferma e selezionare **OK** se si desidera forzare il salvataggio della configurazione.



La configurazione KMS viene salvata ma la connessione al KMS non viene verificata.

Rimozione di un server di gestione delle chiavi (KMS)

In alcuni casi, potrebbe essere necessario rimuovere un server di gestione delle chiavi.

Ad esempio, è possibile rimuovere un KMS specifico del sito se il sito è stato decommissionato.

Di cosa hai bisogno

- È necessario aver esaminato "[considerazioni e requisiti per l'utilizzo di un server di gestione delle chiavi](#)".
- È necessario disporre dell'autorizzazione di accesso root.
- È necessario accedere a Grid Manager utilizzando un browser supportato.

A proposito di questa attività

È possibile rimuovere un KMS nei seguenti casi:

- È possibile rimuovere un KMS specifico del sito se il sito è stato decommissionato o se il sito non include nodi appliance con crittografia del nodo attivata.
- È possibile rimuovere il KMS predefinito se esiste già un KMS specifico del sito per ogni sito che ha nodi appliance con crittografia del nodo attivata.

Fasi

1. Selezionare **Configuration System Settings Key Management Server**.

Viene visualizzata la pagina Key Management Server (Server di gestione delle chiavi) che mostra tutti i server di gestione delle chiavi configurati.

Key Management Server

If your StorageGRID system includes appliance nodes with node encryption enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID at rest.

Configuration Details

Encrypted Nodes

You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

Before adding a KMS:

- Ensure that the KMS is KMIP-compliant.
- Configure StorageGRID as a client in the KMS.
- Enable node encryption for each appliance during appliance installation. You cannot enable node encryption after an appliance is added to the grid and you cannot use a KMS for appliances that do not have node encryption enabled.

For complete instructions, see [administering StorageGRID](#).

+ Create	✎ Edit	🗑 Remove			
KMS Display Name ?	Key Name ?	Manages keys for ?	Hostname ?	Certificate Status ?	
<input checked="" type="radio"/> Default KMS	test	Sites not managed by another KMS (default KMS)	10.96.99.164	✔ All certificates are valid	

2. Selezionare il pulsante di opzione relativo al KMS che si desidera rimuovere e selezionare **Remove** (Rimuovi).
3. Esaminare le considerazioni nella finestra di dialogo di avviso.

Warning

Delete KMS Configuration

You can only remove a KMS in these cases:

- You are removing a site-specific KMS for a site that has no appliance nodes with node encryption enabled.
- You are removing the default KMS, but a site-specific KMS already exists for each site with node encryption.

Are you sure you want to delete the Default KMS KMS configuration?

Cancel

OK

4. Selezionare **OK**.

La configurazione KMS viene rimossa.

Gestione dei tenant

In qualità di amministratore di grid, è possibile creare e gestire gli account tenant utilizzati dai client S3 e Swift per memorizzare e recuperare oggetti, monitorare l'utilizzo dello storage e gestire le azioni che i client sono in grado di eseguire utilizzando il sistema StorageGRID.

Quali sono gli account tenant

Gli account tenant consentono alle applicazioni client che utilizzano l'API REST di S3 (Simple Storage Service) o l'API DI Swift REST di memorizzare e recuperare oggetti su StorageGRID.

Ogni account tenant supporta l'utilizzo di un singolo protocollo, che viene specificato quando si crea l'account. Per memorizzare e recuperare oggetti in un sistema StorageGRID con entrambi i protocolli, è necessario creare due account tenant: Uno per i bucket S3 e gli oggetti e uno per i container Swift e gli oggetti. Ogni account tenant dispone di un proprio ID account, di gruppi e utenti autorizzati, di bucket o container e di oggetti.

Se si desidera separare gli oggetti memorizzati nel sistema da diverse entità, è possibile creare ulteriori account tenant. Ad esempio, è possibile configurare più account tenant in uno dei seguenti casi di utilizzo:

- **Caso d'utilizzo aziendale:** se si amministra un sistema StorageGRID in un'applicazione aziendale, è possibile separare lo storage a oggetti del grid dai diversi reparti dell'organizzazione. In questo caso, è possibile 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 semplicemente i bucket S3 e le policy bucket per separare gli oggetti tra i reparti di un'azienda. Non è necessario utilizzare account tenant. Per ulteriori informazioni, consultare le istruzioni per l'implementazione delle applicazioni client S3.

- **Caso d'utilizzo del provider di servizi:** se si amministra un sistema StorageGRID come provider di servizi, è possibile separare lo storage a oggetti della griglia dalle diverse entità che affitteranno lo storage sulla griglia. In questo caso, è necessario creare account tenant per la società A, la società B, la società C e così via.

Creazione e configurazione di account tenant

Quando si crea un account tenant, si specificano le seguenti informazioni:

- Visualizza il nome dell'account tenant.
- Quale protocollo client verrà utilizzato dall'account tenant (S3 o Swift).
- Per gli account tenant S3: Se l'account tenant dispone dell'autorizzazione per utilizzare i servizi della piattaforma con i bucket S3. Se si consente agli account tenant di utilizzare i servizi della piattaforma, è necessario assicurarsi che la griglia sia configurata per supportare il loro utilizzo. Vedere "Managing platform Services".
- Facoltativamente, una quota di storage per l'account tenant, ovvero il numero massimo di gigabyte, terabyte o petabyte disponibili per gli oggetti del tenant. Se la quota viene superata, il tenant non può creare nuovi oggetti.



La quota di storage di un tenant rappresenta una quantità logica (dimensione dell'oggetto), non una quantità fisica (dimensione sul disco).

- Se la federazione delle identità è attivata per il sistema StorageGRID, il gruppo federato dispone dell'autorizzazione di accesso root per configurare l'account tenant.
- Se l'SSO (Single Sign-on) non è in uso per il sistema StorageGRID, se l'account tenant utilizzerà la propria origine di identità o condividerà l'origine di identità della griglia e la password iniziale per l'utente root locale del tenant.

Una volta creato un account tenant, è possibile eseguire le seguenti attività:

- **Gestisci i servizi della piattaforma per il grid:** Se abiliti i servizi della piattaforma per gli account tenant, assicurati di comprendere come vengono inviati i messaggi dei servizi della piattaforma e i requisiti di rete che l'utilizzo dei servizi della piattaforma comporta nella tua implementazione StorageGRID.
- **Monitorare l'utilizzo dello storage di un account tenant:** Una volta che i tenant iniziano a utilizzare i propri account, è possibile utilizzare Grid Manager per monitorare la quantità di storage consumata da ciascun tenant.

Se sono state impostate le quote per i tenant, è possibile attivare l'avviso **quota elevata del tenant** per determinare se i tenant consumano le quote. Se attivato, questo avviso viene attivato quando un tenant utilizza il 90% della propria quota. Per ulteriori informazioni, consultare il riferimento agli avvisi nelle istruzioni per il monitoraggio e la risoluzione dei problemi di StorageGRID.

- **Configure client Operations** (Configura operazioni client): È possibile configurare se alcuni tipi di operazioni client sono vietate.

Configurazione dei tenant S3

Una volta creato un account tenant S3, gli utenti tenant possono accedere a tenant Manager per eseguire attività come le seguenti:

- Impostazione della federazione delle identità (a meno che l'origine delle identità non sia condivisa con la griglia) e creazione di gruppi e utenti locali

- Gestione delle chiavi di accesso S3
- Creazione e gestione di bucket S3
- Monitoraggio dell'utilizzo dello storage
- Utilizzo dei servizi della piattaforma (se abilitati)



Gli utenti del tenant S3 possono creare e gestire la chiave di accesso S3 e i bucket con Tenant Manager, ma devono utilizzare un'applicazione client S3 per acquisire e gestire gli oggetti.

Configurazione dei tenant Swift

Dopo la creazione di un account tenant Swift, l'utente root del tenant può accedere al tenant Manager per eseguire attività come le seguenti:

- Impostazione della federazione delle identità (a meno che l'origine delle identità non sia condivisa con la griglia) e creazione di gruppi e utenti locali
- Monitoraggio dell'utilizzo dello storage



Gli utenti Swift devono disporre dell'autorizzazione Root Access per accedere a Tenant Manager. Tuttavia, l'autorizzazione Root Access non consente agli utenti di autenticarsi nell'API SWIFT REST per creare container e acquisire oggetti. Gli utenti devono disporre dell'autorizzazione di amministratore Swift per autenticarsi nell'API DI Swift REST.

Informazioni correlate

["Utilizzare un account tenant"](#)

Creazione di un account tenant

È necessario creare almeno un account tenant per controllare l'accesso allo storage nel sistema StorageGRID.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

Fasi

1. Selezionare **tenant**.

Viene visualizzata la pagina account tenant che elenca gli account tenant esistenti.

Tenant Accounts

View information for each tenant account.

Note: 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 and select **View Details**.

+ Create View details Edit Actions Export to CSV Search by Name/ID

Display Name Space Used Quota Utilization Quota Object Count Sign in

No results found.

Show 20 rows per page

2. Selezionare **Crea**.

Viene visualizzata la pagina Create tenant account (Crea account tenant). I campi inclusi nella pagina dipendono dall'attivazione o meno di SSO (Single Sign-on) per il sistema StorageGRID.

- Se non viene utilizzato SSO, la pagina Create tenant account (Crea account tenant) è simile a questa.

Create Tenant Account

Tenant Details

Display Name

Protocol S3 Swift

Storage Quota (optional) GB

Authentication ?

Configure how the tenant account will be accessed.

Uses Own Identity Source

Specify a password for the tenant's local root user.

Username root

Password

Confirm Password

Cancel Save

- Se SSO è attivato, la pagina Create tenant account (Crea account tenant) è simile a questa.

Create Tenant Account

Tenant Details

Display Name	<input type="text" value="S3 tenant (SSO enabled)"/>
Protocol	<input checked="" type="radio"/> S3 <input type="radio"/> Swift
Allow Platform Services	<input checked="" type="checkbox"/>
Storage Quota (optional)	<input type="text"/> <input type="text" value="GB"/>

Authentication

Because single sign-on is enabled, the tenant must use the Grid Manager's identity federation service, and no local users can sign in. You must select an existing federated group to have the initial Root Access permission for the tenant.

Uses Own Identity Source	<input type="checkbox"/>	Single sign-on is enabled. The tenant cannot use its own identity source.
--------------------------	--------------------------	---

Root Access Group	<input type="text" value="qagrp"/>
-------------------	------------------------------------

Cancel

Save

Informazioni correlate

["Utilizzo della federazione delle identità"](#)

["Configurazione del single sign-on"](#)

Creazione di un account tenant se StorageGRID non utilizza SSO

Quando si crea un account tenant, specificare un nome, un protocollo client e, facoltativamente, una quota di storage. Se StorageGRID non utilizza SSO (Single Sign-on), è necessario specificare se l'account tenant utilizzerà la propria origine di identità e configurare la password iniziale per l'utente root locale del tenant.

A proposito di questa attività

Se l'account tenant utilizza l'origine dell'identità configurata per Grid Manager e si desidera concedere l'autorizzazione di accesso root per l'account tenant a un gruppo federato, è necessario aver importato tale gruppo federated in Grid Manager. Non è necessario assegnare alcuna autorizzazione Grid Manager a questo gruppo di amministratori. Consultare le istruzioni per ["gestione dei gruppi di amministratori"](#).

Fasi

1. Nella casella di testo **Display Name** (Nome visualizzato), immettere un nome visualizzato per l'account tenant.

I nomi visualizzati non devono essere univoci. Una volta creato, l'account tenant riceve un ID account univoco e numerico.

2. Selezionare il protocollo client che verrà utilizzato da questo account tenant, **S3** o **Swift**.
3. Per gli account tenant S3, mantenere la casella di controllo **Allow Platform Services** (Consenti servizi piattaforma) selezionata, a meno che non si desideri che il tenant non utilizzi i servizi della piattaforma per il bucket S3.

Se i servizi della piattaforma sono attivati, un tenant può utilizzare funzionalità, come la replica CloudMirror, che accedono ai servizi esterni. È possibile disattivare l'utilizzo di queste funzioni per limitare la quantità di larghezza di banda di rete o di altre risorse consumate dal tenant. Vedere "Managing platform Services".

4. Nella casella di testo **quota di storage**, immettere il numero massimo di gigabyte, terabyte o petabyte che si desidera rendere disponibili per gli oggetti del tenant. Quindi, selezionare le unità dall'elenco a discesa.

Lasciare vuoto questo campo se si desidera che il tenant abbia una quota illimitata.



La quota di storage di un tenant rappresenta una quantità logica (dimensione dell'oggetto), non una quantità fisica (dimensione sul disco). Le copie ILM e la codifica di cancellazione non contribuiscono alla quantità di quota utilizzata. Se la quota viene superata, l'account tenant non può creare nuovi oggetti.



Per monitorare l'utilizzo dello storage di ciascun account tenant, selezionare **Usage** (utilizzo). Gli account tenant possono anche monitorare il proprio utilizzo dello storage dalla dashboard in Tenant Manager o con l'API di gestione tenant. Si noti che i valori di utilizzo dello storage di un tenant potrebbero non essere aggiornati se i nodi sono isolati da altri nodi nella griglia. I totali verranno aggiornati al ripristino della connettività di rete.

5. Se il tenant gestirà i propri gruppi e utenti, attenersi alla seguente procedura.
 - a. Selezionare la casella di controllo **utilizza origine identità** (impostazione predefinita).



Se questa casella di controllo è selezionata e si desidera utilizzare la federazione di identità per gruppi e utenti tenant, il tenant deve configurare la propria origine di identità. Consultare le istruzioni per l'utilizzo degli account tenant.

- b. Specificare una password per l'utente root locale del tenant.
6. Se il tenant utilizza i gruppi e gli utenti configurati per Grid Manager, attenersi alla seguente procedura.
 - a. Deselezionare la casella di controllo **utilizza origine identità**.
 - b. Eseguire una o entrambe le operazioni seguenti:
 - Nel campo Root Access Group (Gruppo di accesso principale), selezionare un gruppo federated esistente da Grid Manager che deve disporre dell'autorizzazione di accesso principale iniziale per il tenant.



Se si dispone di autorizzazioni adeguate, quando si fa clic sul campo vengono elencati i gruppi federated esistenti di Grid Manager. In caso contrario, immettere il nome univoco del gruppo.

- Specificare una password per l'utente root locale del tenant.

7. Fare clic su **Save** (Salva).

Viene creato l'account tenant.

8. In alternativa, accedere al nuovo tenant. In caso contrario, passare al punto per [accesso al tenant in un secondo momento](#).

Se sei...	Eeguire questa operazione...
Accesso a Grid Manager su una porta con restrizioni	Fare clic su Restricted per ulteriori informazioni sull'accesso a questo account tenant. L'URL del tenant manager ha il seguente formato: <code>https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/</code> <ul style="list-style-type: none">• <i>FQDN_or_Admin_Node_IP</i> È un nome di dominio completo o l'indirizzo IP di un nodo amministratore• <i>port</i> è la porta solo tenant• <i>20-digit-account-id</i> È l'ID account univoco del tenant
Accesso a Grid Manager sulla porta 443 ma non è stata impostata una password per l'utente root locale	Fare clic su Accedi e immettere le credenziali per un utente nel gruppo federated di accesso root.
Accedendo a Grid Manager sulla porta 443, viene impostata una password per l'utente root locale	Passare alla fase successiva da a. accedi come root .

9. Accedi al tenant come root:
 - a. Dalla finestra di dialogo Configura account tenant, fare clic sul pulsante **Accedi come root**.

Configure Tenant Account

✓ Account S3 tenant created successfully.

If you are ready to configure this tenant account, sign in as the tenant's root user. Then, click the links below.

Sign in as root

- [Buckets](#) - Create and manage buckets.
- [Groups](#) - Manage user groups, and assign group permissions.
- [Users](#) - Manage local users, and assign users to groups.

Finish

Sul pulsante viene visualizzato un segno di spunta verde, a indicare che si è ora effettuato l'accesso all'account tenant come utente root.

Sign in as root ✓

a. Fare clic sui collegamenti per configurare l'account tenant.

Ciascun collegamento apre la pagina corrispondente in Tenant Manager. Per completare la pagina, consultare le istruzioni per l'utilizzo degli account tenant.

b. Fare clic su **fine**.

10. per accedere al tenant in un secondo momento:

Se si utilizza...	Eeguire una di queste operazioni...
Porta 443	<ul style="list-style-type: none">• Da Grid Manager, selezionare tenant e fare clic su Sign in (Accedi) a destra del nome del tenant.• Inserire l'URL del tenant in un browser Web: <code>https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/</code><ul style="list-style-type: none">◦ <i>FQDN_or_Admin_Node_IP</i> È un nome di dominio completo o l'indirizzo IP di un nodo amministratore◦ <i>20-digit-account-id</i> È l'ID account univoco del tenant

Se si utilizza...	Eseguire una di queste operazioni...
Una porta con restrizioni	<ul style="list-style-type: none"> • In Grid Manager, selezionare tenant e fare clic su Restricted. • Inserire l'URL del tenant in un browser Web: <pre>https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id</pre> <ul style="list-style-type: none"> ◦ <i>FQDN_or_Admin_Node_IP</i> È un nome di dominio completo o l'indirizzo IP di un nodo amministratore ◦ <i>port</i> è la porta limitata solo tenant ◦ <i>20-digit-account-id</i> È l'ID account univoco del tenant

Informazioni correlate

["Controllo dell'accesso tramite firewall"](#)

["Gestione dei servizi della piattaforma per gli account tenant S3"](#)

["Utilizzare un account tenant"](#)

Creazione di un account tenant se SSO è attivato

Quando si crea un account tenant, specificare un nome, un protocollo client e, facoltativamente, una quota di storage. Se SSO (Single Sign-on) è attivato per StorageGRID, specificare anche quale gruppo federato dispone dell'autorizzazione di accesso root per configurare l'account tenant.

Fasi

1. Nella casella di testo **Display Name** (Nome visualizzato), immettere un nome visualizzato per l'account tenant.

I nomi visualizzati non devono essere univoci. Una volta creato, l'account tenant riceve un ID account univoco e numerico.

2. Selezionare il protocollo client che verrà utilizzato da questo account tenant, **S3** o **Swift**.
3. Per gli account tenant S3, mantenere la casella di controllo **Allow Platform Services** (Consenti servizi piattaforma) selezionata, a meno che non si desideri che il tenant non utilizzi i servizi della piattaforma per i bucket S3.

Se i servizi della piattaforma sono attivati, un tenant può utilizzare funzionalità, come la replica CloudMirror, che accedono ai servizi esterni. È possibile disattivare l'utilizzo di queste funzioni per limitare la quantità di larghezza di banda di rete o di altre risorse consumate dal tenant. Vedere "Managing platform Services".

4. Nella casella di testo **quota di storage**, immettere il numero massimo di gigabyte, terabyte o petabyte che si desidera rendere disponibili per gli oggetti del tenant. Quindi, selezionare le unità dall'elenco a discesa.

Lasciare vuoto questo campo se si desidera che il tenant abbia una quota illimitata.



La quota di storage di un tenant rappresenta una quantità logica (dimensione dell'oggetto), non una quantità fisica (dimensione sul disco). Le copie ILM e la codifica di cancellazione non contribuiscono alla quantità di quota utilizzata. Se la quota viene superata, l'account tenant non può creare nuovi oggetti.



Per monitorare l'utilizzo dello storage di ciascun account tenant, selezionare **Usage** (utilizzo). Gli account tenant possono anche monitorare il proprio utilizzo dello storage dalla dashboard in Tenant Manager o con l'API di gestione tenant. Si noti che i valori di utilizzo dello storage di un tenant potrebbero non essere aggiornati se i nodi sono isolati da altri nodi nella griglia. I totali verranno aggiornati al ripristino della connettività di rete.

5. Si noti che la casella di controllo **utilizza origine identità** è deselezionata e disattivata.

Poiché SSO è attivato, il tenant deve utilizzare l'origine dell'identità configurata per Grid Manager. Nessun utente locale può accedere.

6. Nel campo **Root Access Group**, selezionare un gruppo federated esistente da Grid Manager per ottenere l'autorizzazione di accesso root iniziale per il tenant.



Se si dispone di autorizzazioni adeguate, quando si fa clic sul campo vengono elencati i gruppi federated esistenti di Grid Manager. In caso contrario, immettere il nome univoco del gruppo.

7. Fare clic su **Save** (Salva).

Viene creato l'account tenant. Viene visualizzata la pagina account tenant, che include una riga per il nuovo tenant.

8. Se si è un utente del gruppo Root Access, fare clic sul collegamento **Sign in** (Accedi) per accedere immediatamente al tenant Manager, dove è possibile configurare il tenant. In caso contrario, fornire l'URL del collegamento **Accedi** all'amministratore dell'account tenant. (L'URL di un tenant è il nome di dominio completo o l'indirizzo IP di qualsiasi nodo di amministrazione, seguito da `/?accountId=20-digit-account-id`.)



Se si fa clic su **Sign in** (accesso negato), ma non si appartiene al gruppo Root Access per l'account tenant, viene visualizzato un messaggio di accesso negato.

Informazioni correlate

["Configurazione del single sign-on"](#)

["Gestione dei servizi della piattaforma per gli account tenant S3"](#)

["Utilizzare un account tenant"](#)

Modifica della 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 dall'account.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.

- È necessario disporre di autorizzazioni di accesso specifiche.

A proposito di questa attività

Se il sistema StorageGRID è abilitato per il Single Sign-on (SSO), l'utente root locale non può accedere all'account tenant. Per eseguire le attività dell'utente root, gli utenti devono appartenere a un gruppo federated che disponga dell'autorizzazione di accesso root per il tenant.

Fasi

1. Selezionare **tenant**.

Viene visualizzata la pagina account tenant che elenca tutti gli account tenant esistenti.

Tenant Accounts

View information for each tenant account.

Note: 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 and select **View Details**.

	Display Name	Space Used	Quota Utilization	Quota	Object Count	Sign in
<input checked="" type="radio"/>	Account01	500.00 KB	0.00%	20.00 GB	100	
<input type="radio"/>	Account02	2.50 MB	0.01%	30.00 GB	500	
<input type="radio"/>	Account03	605.00 MB	4.03%	15.00 GB	31,000	
<input type="radio"/>	Account04	1.00 GB	10.00%	10.00 GB	200,000	
<input type="radio"/>	Account05	0 bytes	—	Unlimited	0	

Show 20 rows per page

2. Selezionare l'account tenant che si desidera modificare.

Se il sistema include più di 20 elementi, è possibile specificare quante righe vengono visualizzate su ogni pagina contemporaneamente. Utilizzare la casella di ricerca per cercare un account tenant in base al nome visualizzato o all'ID tenant.

Vengono attivati i pulsanti Visualizza dettagli, Modifica e azioni.

3. Dal menu a discesa **Actions** (azioni), selezionare **Change Root Password** (Modifica password root).

Change Root User Password - Account03

Username root

New Password

Confirm New Password

- Inserire la nuova password per l'account tenant.
- Selezionare **Salva**.

Informazioni correlate

["Controllo dell'accesso amministratore a StorageGRID"](#)

Modifica di un account tenant

È possibile modificare un account tenant per modificare il nome visualizzato, modificare l'impostazione dell'origine dell'identità, consentire o non consentire i servizi della piattaforma o immettere una quota di storage.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

Fasi

















- Selezionare **tenant**.

Viene visualizzata la pagina account tenant che elenca tutti gli account tenant esistenti.

Tenant Accounts

View information for each tenant account.

Note: 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 and select **View Details**.

	Display Name  	Space Used  	Quota Utilization  	Quota  	Object Count  	Sign in 
<input checked="" type="radio"/>	Account01	500.00 KB	0.00%	20.00 GB	100	
<input type="radio"/>	Account02	2.50 MB	0.01%	30.00 GB	500	
<input type="radio"/>	Account03	605.00 MB	4.03%	15.00 GB	31,000	
<input type="radio"/>	Account04	1.00 GB	10.00%	10.00 GB	200,000	
<input type="radio"/>	Account05	0 bytes	—	Unlimited	0	

Show rows per page

- Selezionare l'account tenant che si desidera modificare.

Se il sistema include più di 20 elementi, è possibile specificare quante righe vengono visualizzate su ogni pagina contemporaneamente. Utilizzare la casella di ricerca per cercare un account tenant in base al nome visualizzato o all'ID tenant.

- Selezionare **Modifica**.

Viene visualizzata la pagina Edit tenant account (Modifica account tenant). Questo esempio si intende per una griglia che non utilizza SSO (Single Sign-on). Questo account tenant non ha configurato la propria origine di identità.

Edit Tenant Account

Tenant Details

Display Name	<input type="text" value="Account03"/>
Allow Platform Services	<input checked="" type="checkbox"/>
Storage Quota (optional)	<input type="text" value="15"/> <input type="text" value="GB"/>
Uses Own Identity Source	<input checked="" type="checkbox"/>

4. Modificare i valori dei campi come richiesto.

- a. Modificare il nome visualizzato per questo account tenant.
- b. Modificare l'impostazione della casella di controllo **Allow Platform Services** (Consenti servizi piattaforma) per determinare se l'account tenant può utilizzare i servizi della piattaforma per i bucket S3.



Se si disattivano i servizi della piattaforma per un tenant che li sta già utilizzando, i servizi configurati per i 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 memorizzare oggetti nel bucket, ma le copie di tali oggetti non verranno più eseguite nel bucket S3 esterno configurato come endpoint.

- c. Per **quota di storage**, modificare il numero massimo di gigabyte, terabyte o petabyte disponibili per gli oggetti del tenant oppure lasciare vuoto il campo se si desidera che il tenant abbia una quota illimitata.

La quota di storage di un tenant rappresenta una quantità logica (dimensione dell'oggetto), non una quantità fisica (dimensione sul disco). Le copie ILM e la codifica di cancellazione non contribuiscono alla quantità di quota utilizzata.



Per monitorare l'utilizzo dello storage di ciascun account tenant, selezionare **Usage** (utilizzo). Gli account tenant possono anche monitorare il proprio utilizzo dalla dashboard in Tenant Manager o con l'API di gestione tenant. Si noti che i valori di utilizzo dello storage di un tenant potrebbero non essere aggiornati se i nodi sono isolati da altri nodi nella griglia. I totali verranno aggiornati al ripristino della connettività di rete.

- d. Modificare l'impostazione della casella di controllo **Use Own Identity Source** (utilizza origine identità propria) per determinare se l'account tenant utilizzerà la propria origine identità o l'origine identità configurata per Grid Manager.



Se la casella di controllo **utilizza origine identità** è:

- Disattivato e selezionato, il tenant ha già attivato la propria origine di identità. Un tenant deve disattivare l'origine dell'identità prima di poter utilizzare l'origine dell'identità configurata per Grid Manager.

- Disattivato e deselezionato, SSO è attivato per il sistema StorageGRID. Il tenant deve utilizzare l'origine dell'identità configurata per Grid Manager.

5. Selezionare **Salva**.

Informazioni correlate

["Gestione dei servizi della piattaforma per gli account tenant S3"](#)

["Utilizzare un account tenant"](#)

Eliminazione di un account tenant

È possibile eliminare un account tenant se si desidera rimuovere in modo permanente l'accesso del tenant al sistema.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.
- È necessario rimuovere tutti i bucket (S3), i container (Swift) e gli oggetti associati all'account tenant.

Fasi

1. Selezionare **tenant**.
2. Selezionare l'account tenant che si desidera eliminare.

Se il sistema include più di 20 elementi, è possibile specificare quante righe vengono visualizzate su ogni pagina contemporaneamente. Utilizzare la casella di ricerca per cercare un account tenant in base al nome visualizzato o all'ID tenant.

3. Dal menu a discesa **azioni**, selezionare **Rimuovi**.
4. Selezionare **OK**.

Informazioni correlate

["Controllo dell'accesso amministratore a StorageGRID"](#)

Gestione dei servizi della piattaforma per gli account tenant S3

Se si abilitano i servizi della piattaforma per gli account tenant S3, è necessario configurare il grid in modo che i tenant possano accedere alle risorse esterne necessarie per l'utilizzo di questi servizi.

- ["Quali sono i servizi della piattaforma"](#)
- ["Networking e porte per i servizi della piattaforma"](#)
- ["Erogazione per sito di messaggi relativi ai servizi della piattaforma"](#)
- ["Risoluzione dei problemi relativi ai servizi della piattaforma"](#)

Quali sono i servizi della piattaforma

I servizi della piattaforma includono la replica di CloudMirror, le notifiche degli eventi e il servizio di integrazione della ricerca.

Questi servizi consentono ai tenant di utilizzare le seguenti funzionalità con i bucket S3:

- **Replica di CloudMirror:** Il servizio di replica di StorageGRID CloudMirror viene utilizzato per eseguire il mirroring di oggetti specifici da un bucket StorageGRID a una destinazione esterna specificata.

Ad esempio, è possibile utilizzare la replica di CloudMirror per eseguire il mirroring di record specifici dei clienti in Amazon S3 e sfruttare i servizi AWS per eseguire analisi dei dati.



La replica di CloudMirror non è supportata se il bucket di origine ha attivato il blocco oggetti S3.

- **Notifiche:** Le notifiche degli eventi per bucket vengono utilizzate per inviare notifiche su azioni specifiche eseguite su oggetti a un servizio Amazon Simple Notification Service™ (SNS) esterno specificato.

Ad esempio, è possibile configurare gli avvisi da inviare agli amministratori in merito a ciascun oggetto aggiunto a un bucket, in cui gli oggetti rappresentano i file di registro associati a un evento di sistema critico.



Sebbene la notifica degli eventi possa essere configurata su un bucket con blocco oggetti S3 attivato, i metadati del blocco oggetti S3 (inclusi lo stato Mantiene fino alla data e conservazione legale) degli oggetti non saranno inclusi nei messaggi di notifica.

- **Search Integration service:** Il servizio di integrazione della ricerca viene utilizzato per inviare metadati di oggetti S3 a un indice Elasticsearch specificato, dove è possibile cercare o analizzare i metadati utilizzando il servizio esterno.

Ad esempio, è possibile configurare i bucket per inviare metadati di oggetti S3 a un servizio Elasticsearch remoto. È quindi possibile utilizzare Elasticsearch per eseguire ricerche tra bucket ed eseguire analisi sofisticate dei modelli presenti nei metadati degli oggetti.



Sebbene l'integrazione di Elasticsearch possa essere configurata su un bucket con S3 Object Lock attivato, i metadati S3 Object Lock (inclusi Retain until Date e Legal Hold status) degli oggetti non saranno inclusi nei messaggi di notifica.

I servizi della piattaforma offrono ai tenant la possibilità di utilizzare risorse di storage esterne, servizi di notifica e servizi di ricerca o analisi con i propri dati. Poiché la posizione di destinazione dei servizi della piattaforma è generalmente esterna alla distribuzione di StorageGRID, è necessario decidere se consentire ai tenant di utilizzare questi servizi. In tal caso, è necessario abilitare l'utilizzo dei servizi della piattaforma quando si creano o 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 proprie destinazioni.

Consigli per l'utilizzo dei servizi della piattaforma

Prima di utilizzare i servizi della piattaforma, è necessario conoscere i seguenti consigli:

- Non utilizzare più di 100 tenant attivi con richieste S3 che richiedono la replica CloudMirror, le notifiche e l'integrazione della ricerca. La presenza di più di 100 tenant attivi può rallentare le performance del client S3.
- Se in un bucket S3 nel sistema StorageGRID sono attivate sia la versione che la replica CloudMirror, è necessario attivare anche la versione del bucket S3 per l'endpoint di destinazione. Ciò consente alla replica di CloudMirror di generare versioni di oggetti simili sull'endpoint.

Informazioni correlate

["Utilizzare un account tenant"](#)

["Configurazione delle impostazioni del proxy di storage"](#)

["Monitor risoluzione dei problemi"](#)

Networking 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 attivati, il tenant può creare endpoint che fungono da destinazione per la replica CloudMirror, le notifiche di eventi o i messaggi di integrazione di ricerca dai bucket S3. Questi messaggi dei servizi della piattaforma vengono inviati dai nodi di storage che eseguono il servizio ADC agli endpoint di destinazione.

Ad esempio, i tenant potrebbero configurare i seguenti tipi di endpoint di destinazione:

- Cluster Elasticsearch ospitato localmente
- Applicazione locale che supporta la ricezione di messaggi SNS (Simple Notification Service)
- 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 inviati, è necessario configurare la rete o le reti contenenti i nodi di storage ADC. È necessario assicurarsi che le seguenti porte possano essere utilizzate per inviare messaggi di servizi della piattaforma agli endpoint di destinazione.

Per impostazione predefinita, i messaggi dei servizi della piattaforma vengono inviati alle seguenti porte:

- **80**: Per gli URI endpoint che iniziano con http
- **443**: Per gli URI endpoint che iniziano con https

I tenant possono specificare una porta diversa quando creano o modificano un endpoint.



Se si utilizza un'implementazione StorageGRID come destinazione della 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 dall'implementazione StorageGRID di destinazione sia specificata nell'endpoint.

Se si utilizza un server proxy non trasparente, è necessario configurare anche le impostazioni del proxy di storage per consentire l'invio dei messaggi a endpoint esterni, ad esempio un endpoint su Internet.

Informazioni correlate

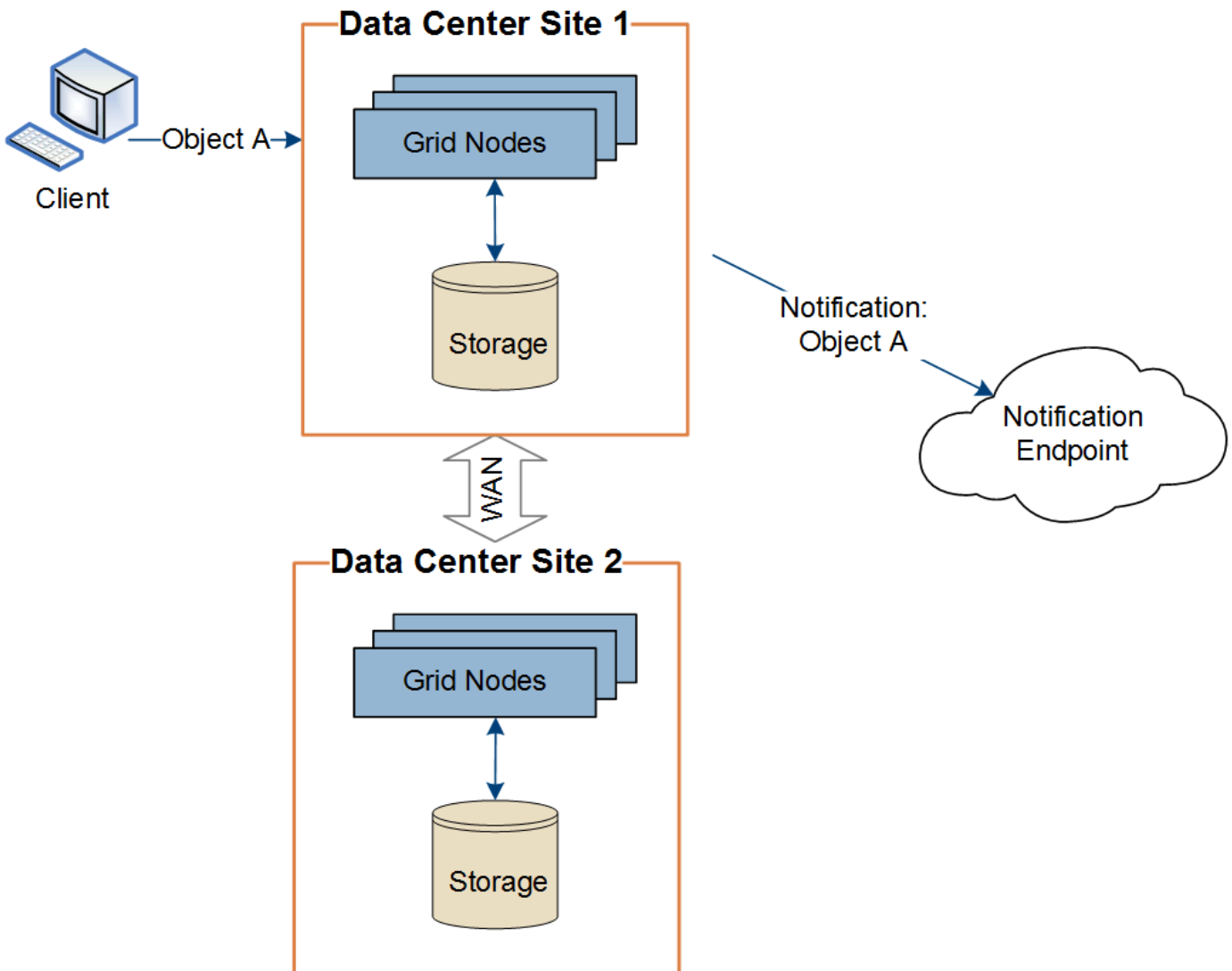
["Configurazione delle impostazioni del proxy di storage"](#)

["Utilizzare un account tenant"](#)

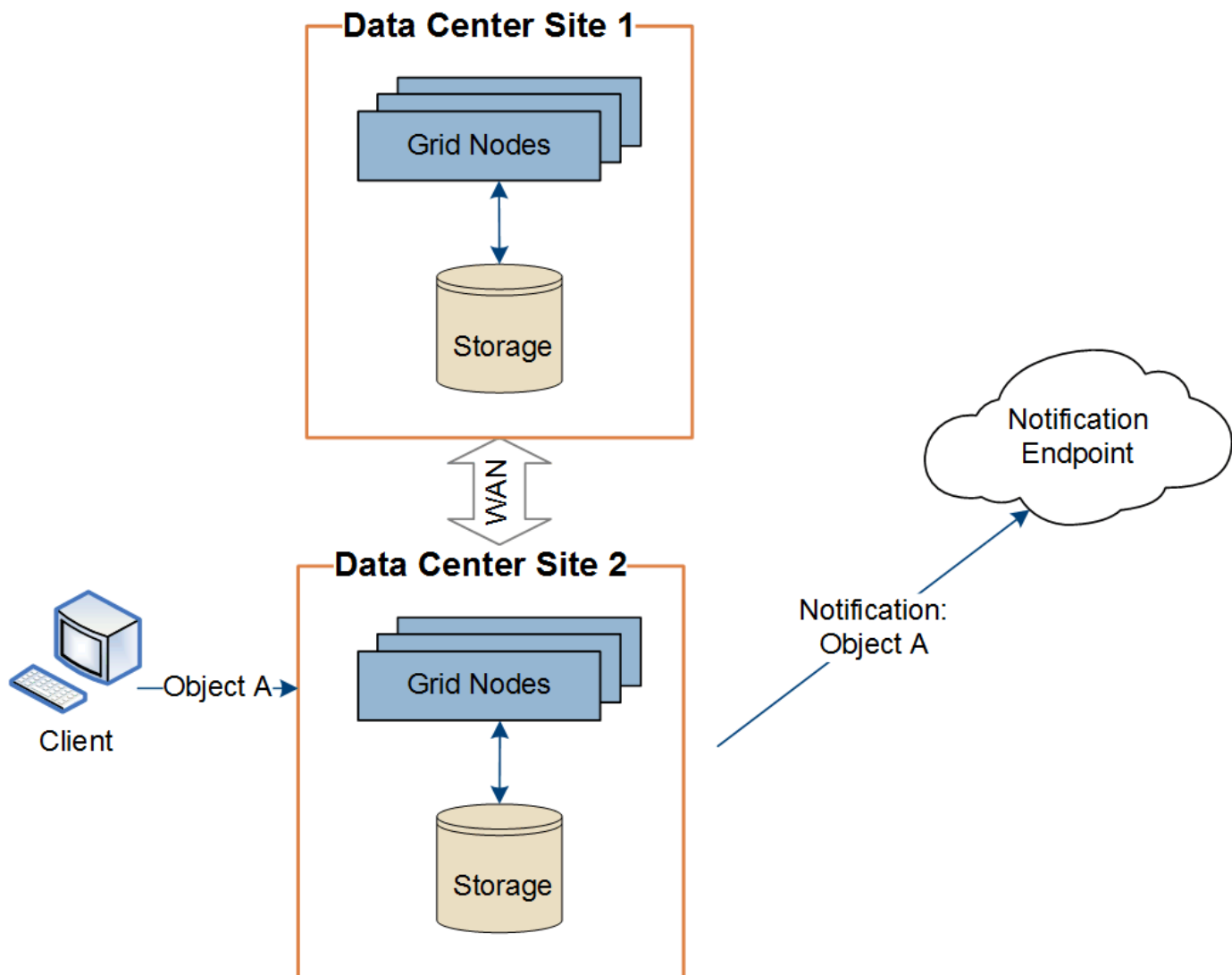
Erogazione per sito di messaggi relativi ai servizi della piattaforma

Tutte le operazioni dei servizi della piattaforma vengono eseguite in base al sito.

Cioè, se un tenant utilizza un client per eseguire un'operazione S3 API Create su un oggetto connettendosi a un nodo gateway nel sito 1 del data center, la notifica relativa a tale azione viene attivata e inviata dal sito 1 del data center.



Se il client esegue successivamente un'operazione di eliminazione 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 di ciascun sito sia configurata in modo che i messaggi dei servizi della piattaforma possano essere recapitati alle rispettive destinazioni.

Risoluzione dei problemi relativi ai servizi della piattaforma

Gli endpoint utilizzati nei servizi della piattaforma vengono creati e gestiti dagli utenti del tenant in Tenant Manager; tuttavia, se un tenant ha problemi nella configurazione o nell'utilizzo dei servizi della piattaforma, potrebbe essere 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 il 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 semplice argomento del servizio di notifica o un cluster Elasticsearch ospitato localmente o su AWS. Ogni endpoint include sia la posizione della risorsa esterna che le credenziali necessarie per accedere a tale risorsa.

Quando un tenant crea un endpoint, il sistema StorageGRID convalida che l'endpoint esiste e che può essere raggiunto utilizzando le credenziali specificate. La connessione all'endpoint viene convalidata da un nodo in ogni sito.

Se la convalida degli endpoint non riesce, viene visualizzato un messaggio di errore che spiega perché la convalida degli endpoint non è riuscita. L'utente tenant dovrebbe risolvere il problema, quindi provare a creare nuovamente l'endpoint.



La creazione dell'endpoint non riesce 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 Gestione tenant.



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 del tenant possono accedere alla pagina degli 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 per quanto tempo si è verificato l'errore. Errori che includono 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

<input type="checkbox"/>	Display name	Last error	Type	URI	URN
<input type="checkbox"/>	my-endpoint-2	2 hours ago	Search	http://10.96.104.30:9200	urn:sgws:es::mydomain/sveloso/_doc
<input type="checkbox"/>	my-endpoint-3	3 days ago	Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example1
<input type="checkbox"/>	my-endpoint-5	12 days ago	Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example3
<input type="checkbox"/>	my-endpoint-4		Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example2
<input type="checkbox"/>	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 della griglia o il supporto tecnico può utilizzare questo ID per individuare informazioni più dettagliate sull'errore nel file bycast.log.

Problemi relativi ai server proxy

Se è stato configurato un proxy di storage tra i nodi di storage e gli endpoint del servizio della piattaforma, potrebbero verificarsi errori se il servizio proxy non consente messaggi da StorageGRID. Per risolvere questi problemi, controllare le impostazioni del server proxy per assicurarsi che i messaggi relativi al servizio della piattaforma non siano bloccati.

Determinare se si è verificato un errore

Se si sono verificati errori degli endpoint negli ultimi 7 giorni, la dashboard di Tenant Manager visualizza un messaggio di avviso. È possibile accedere alla pagina Endpoint per ulteriori dettagli sull'errore.

Le operazioni del client non riescono

Alcuni problemi relativi ai servizi della piattaforma potrebbero causare il malfunzionamento delle operazioni client sul bucket S3. Ad esempio, le operazioni del client S3 non vengono eseguite correttamente se il servizio RSM (Replicated state Machine) interno viene arrestato o se sono presenti troppi messaggi dei servizi della piattaforma in coda per il recapito.

Per controllare lo stato dei servizi:

1. Selezionare **supporto > Strumenti > topologia griglia**.
2. Selezionare **Site Storage Node SSM Services**.

Errori degli endpoint ripristinabili e non ripristinabili

Una volta creati gli endpoint, gli errori di richiesta del servizio della piattaforma possono verificarsi per diversi motivi. Alcuni errori possono essere ripristinati con l'intervento dell'utente. Ad esempio, potrebbero verificarsi errori ripristinabili per i seguenti motivi:

- Le credenziali dell'utente sono state eliminate o scadute.
- Il bucket di destinazione non esiste.
- La notifica non può essere inviata.

Se StorageGRID rileva un errore ripristinabile, la richiesta di servizio della piattaforma verrà rievitata fino a quando non avrà esito positivo.

Altri errori non sono ripristinabili. Ad esempio, se l'endpoint viene cancellato, si verifica un errore irreversibile.

Se StorageGRID rileva un errore irreversibile dell'endpoint, l'allarme Eventi totali (SMTT) viene attivato in Gestione griglia. Per visualizzare l'allarme Total Events (Eventi totali):

1. Selezionare **nodi**.
2. Selezionare **Site Grid Node Events**.
3. Visualizza ultimo evento nella parte superiore della tabella.

I messaggi degli eventi sono elencati anche nella `/var/local/log/bycast-err.log`.

4. Seguire le indicazioni fornite nel contenuto degli allarmi SMTT per correggere il problema.
5. Fare clic su **Reset event count** (Ripristina conteggi eventi).
6. Notificare al tenant gli oggetti i cui messaggi dei servizi della piattaforma non sono stati recapitati.

7. Chiedere al tenant di riattivare la replica o la notifica non riuscita aggiornando i metadati o i tag dell'oggetto.

Il tenant può reinviare i valori esistenti per evitare modifiche indesiderate.

I messaggi dei servizi della piattaforma non possono essere inviati

Se la destinazione incontra un problema che impedisce l'accettazione dei 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 che StorageGRID non possa più autenticare il servizio di destinazione.

Se i messaggi dei servizi della piattaforma non possono essere inviati a causa di un errore irreversibile, l'allarme SMTT (Total Events) viene attivato in Grid Manager.

Performance più lente per le richieste di servizi della piattaforma

Il software StorageGRID potrebbe ridurre le richieste S3 in entrata per un bucket se la velocità con cui le richieste vengono inviate supera la velocità con cui l'endpoint di destinazione può ricevere le richieste. La limitazione si verifica solo quando è presente un backlog di richieste in attesa di essere inviate all'endpoint di destinazione.

L'unico effetto visibile è che l'esecuzione delle richieste S3 in entrata richiederà più tempo. Se si inizia a rilevare performance significativamente più lente, è necessario ridurre il tasso di acquisizione o utilizzare un endpoint con capacità superiore. Se il backlog delle richieste continua a crescere, le operazioni del client S3 (come LE richieste PUT) finiranno per fallire.

È più probabile che le richieste CloudMirror siano influenzate dalle performance dell'endpoint di destinazione, perché queste richieste comportano in genere un maggior numero di trasferimenti di dati rispetto alle richieste di integrazione della ricerca o di notifica degli eventi.

Le richieste di servizio della piattaforma non vengono soddisfatte

Per visualizzare il tasso di errore della richiesta per i servizi della piattaforma:

1. Selezionare **nodi**.
2. Selezionare **Site Platform Services**.
3. Visualizzare il grafico tasso di errore della richiesta.

Data Center 1



Avviso di servizi della piattaforma non disponibili

L'avviso **Platform Services unavailable** (servizi piattaforma non disponibili) indica che non è possibile eseguire operazioni di servizio della piattaforma in un sito perché sono in esecuzione o disponibili troppi nodi di storage 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 storage del sito includono il servizio RSM. (Il servizio RSM è presente sui nodi di storage che includono anche il servizio ADC). Quindi, assicurarsi che la maggior parte di questi nodi di storage sia in esecuzione e disponibile.



Se più di un nodo di storage che contiene il servizio RSM si guasta in un sito, si perdono le richieste di servizio della piattaforma in sospeso per quel sito.

Ulteriori linee guida per la risoluzione dei problemi per gli endpoint dei servizi della piattaforma

Per ulteriori informazioni sulla risoluzione dei problemi degli endpoint dei servizi della piattaforma, consultare le istruzioni per l'utilizzo degli account tenant.

["Utilizzare un account tenant"](#)

Informazioni correlate

["Monitor risoluzione dei problemi"](#)

["Configurazione delle impostazioni del proxy di storage"](#)

Configurazione delle connessioni dei client S3 e Swift

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

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

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



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

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

È possibile configurare le seguenti funzioni sul sistema StorageGRID:

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

È inoltre possibile abilitare l'utilizzo di HTTP per i client che si connettono a StorageGRID direttamente ai nodi

di storage o utilizzando il servizio CLB (obsoleto) ed è possibile configurare i nomi di dominio degli endpoint API S3 per i client S3.

Riepilogo: Indirizzi IP e porte per le connessioni client

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

A proposito di questa attività

Questa tabella riassume i diversi modi in cui i client possono connettersi a StorageGRID e gli indirizzi IP e le porte utilizzati per ciascun tipo di connessione. Le istruzioni descrivono come trovare queste informazioni in Grid Manager se gli endpoint del bilanciamento del carico e i gruppi ad alta disponibilità (ha) sono già configurati.

Dove viene stabilita la connessione	Servizio a cui si connette il client	Indirizzo IP	Porta
Gruppo HA	Bilanciamento del carico	Indirizzo IP virtuale di un gruppo ha	<ul style="list-style-type: none"> Porta endpoint del bilanciamento del carico
Gruppo HA	CLB Nota: il servizio CLB è obsoleto.	Indirizzo IP virtuale di un gruppo ha	Porte S3 predefinite: <ul style="list-style-type: none"> HTTPS: 8082 HTTP: 8084 Porte Swift predefinite: <ul style="list-style-type: none"> HTTPS:8083 HTTP:8085
Nodo Admin	Bilanciamento del carico	Indirizzo IP del nodo di amministrazione	<ul style="list-style-type: none"> Porta endpoint del bilanciamento del carico
Nodo gateway	Bilanciamento del carico	Indirizzo IP del nodo gateway	<ul style="list-style-type: none"> Porta endpoint del bilanciamento del carico

Dove viene stabilita la connessione	Servizio a cui si connette il client	Indirizzo IP	Porta
Nodo gateway	CLB Nota: il servizio CLB è obsoleto.	Indirizzo IP del nodo gateway Nota: per impostazione predefinita, le porte HTTP per CLB e LDR non sono attivate.	Porte S3 predefinite: • HTTPS: 8082 • HTTP: 8084 Porte Swift predefinite: • HTTPS:8083 • HTTP:8085
Nodo di storage	LDR	Indirizzo IP del nodo di storage	Porte S3 predefinite: • HTTPS: 18082 • HTTP: 18084 Porte Swift predefinite: • HTTPS: 18083 • HTTP:18085

Esempi

Per connettere un client S3 all'endpoint Load Balancer di un gruppo ha di nodi gateway, utilizzare un URL strutturato come mostrato di seguito:

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

Ad esempio, se l'indirizzo IP virtuale del gruppo ha è 192.0.2.5 e il numero di porta di un endpoint di bilanciamento del carico S3 è 10443, un client S3 potrebbe utilizzare il seguente URL per connettersi a StorageGRID:

- `https://192.0.2.5:10443`

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

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

Ad esempio, se l'indirizzo IP virtuale del gruppo ha è 192.0.2.6 e il numero di porta di un endpoint di bilanciamento del carico di Swift è 10444, un client Swift potrebbe utilizzare il seguente URL per connettersi a StorageGRID:

- `https://192.0.2.6:10444`

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

Fasi

1. Accedere a Grid Manager utilizzando un browser supportato.

2. Per trovare l'indirizzo IP di un nodo Grid:

- a. Selezionare **nodi**.
- b. Selezionare il nodo Admin, il nodo gateway o il nodo di storage a cui si desidera connettersi.
- c. Selezionare la scheda **Panoramica**.
- d. Nella sezione Node Information (informazioni sul nodo), annotare gli indirizzi IP del nodo.
- e. Fare clic su **Mostra altro** per visualizzare gli indirizzi IPv6 e le mappature dell'interfaccia.

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

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



Se si sta visualizzando un nodo Admin o un nodo Gateway e si tratta del nodo attivo di un gruppo ad alta disponibilità, l'indirizzo IP virtuale del gruppo ha viene visualizzato su eth2.

3. Per trovare l'indirizzo IP virtuale di un gruppo ad alta disponibilità:

- a. Selezionare **Configurazione > Impostazioni di 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 Load Balancer:

- a. Selezionare **Configuration > Network Settings > Load Balancer Endpoints**.

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

- b. Selezionare un endpoint e fare clic su **Edit endpoint** (Modifica endpoint).

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

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



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

Gestione del bilanciamento del carico

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

È possibile ottenere il bilanciamento del carico nel sistema StorageGRID nei seguenti modi:

- Utilizzare il servizio Load Balancer, installato nei nodi Admin e nei nodi Gateway. Il servizio Load Balancer fornisce il bilanciamento del carico di livello 7 ed esegue la terminazione TLS delle richieste dei client, ispeziona le richieste e stabilisce nuove connessioni sicure ai nodi di storage. Si tratta del meccanismo di bilanciamento del carico consigliato.
- Utilizzare il servizio Connection Load Balancer (CLB), installato solo sui nodi gateway. Il servizio CLB fornisce il bilanciamento del carico di livello 4 e supporta i costi di collegamento.



Il servizio CLB è obsoleto.

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

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

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

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

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

- Indirizzi IP virtuali (VIP) specifici ad alta disponibilità (ha)
- Interfacce di rete specifiche di nodi specifici

Considerazioni sulle porte

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

Se sono state rimappate delle porte, non è possibile utilizzare le stesse porte per configurare gli endpoint del bilanciamento del carico. È possibile creare endpoint utilizzando porte rimappate, ma tali endpoint verranno rimappati alle porte e al servizio CLB originali, non al servizio Load Balancer. Seguire le istruzioni riportate nelle istruzioni di ripristino e manutenzione per rimuovere i rimapper delle porte.



Il servizio CLB è obsoleto.

Disponibilità della CPU

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

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

Informazioni correlate

["Mantieni Ripristina"](#)

Configurazione degli endpoint del bilanciamento del carico

È possibile creare, modificare e rimuovere endpoint del bilanciamento del carico.

Creazione di endpoint per il bilanciamento del carico

Ogni endpoint del bilanciamento del carico specifica una porta, un protocollo di rete (HTTP o HTTPS) e un tipo di servizio (S3 o Swift). Se si crea un endpoint HTTPS, è necessario caricare o generare un certificato server.

Di cosa hai bisogno

- È necessario disporre dell'autorizzazione di accesso root.
- È necessario accedere a Grid Manager utilizzando un browser supportato.
- Se in precedenza sono state rimappate le porte che si intende utilizzare per il servizio Load Balancer, è necessario rimuovere i rimap.



Se sono state rimappate delle porte, non è possibile utilizzare le stesse porte per configurare gli endpoint del bilanciamento del carico. È possibile creare endpoint utilizzando porte rimappate, ma tali endpoint verranno rimappati alle porte e al servizio CLB originali, non al servizio Load Balancer. Seguire le istruzioni riportate nelle istruzioni di ripristino e manutenzione per rimuovere i rimapper delle porte.



Il servizio CLB è obsoleto.

Fasi

1. Selezionare **Configuration > Network Settings > Load Balancer Endpoints**.

Viene visualizzata la pagina endpoint del bilanciamento del carico.

Load Balancer Endpoints

Load balancer endpoints define Gateway Node and Admin Node ports that accept and load balance S3 and Swift requests to Storage Nodes. HTTPS endpoint certificates are configured per endpoint.

🕒 Changes to endpoints can take up to 15 minutes to be applied to all nodes.

[+ Add endpoint port](#) [✎ Edit endpoint](#) [✖ Remove endpoint port](#)

Display name	Port	Using HTTPS
No endpoints configured.		

2. Selezionare **Aggiungi endpoint**.

Viene visualizzata la finestra di dialogo Create Endpoint (Crea endpoint).

Create Endpoint

Display Name

Port

Protocol HTTP HTTPS

Endpoint Binding Mode Global HA Group VIPs Node Interfaces

3. Inserire un nome da visualizzare per l'endpoint, che verrà visualizzato nell'elenco della pagina endpoint del bilanciamento del carico.
4. Inserire un numero di porta o lasciare il numero di porta pre-compilato così com'è.

Se si immette il numero di porta 80 o 443, l'endpoint viene configurato solo sui nodi gateway, poiché queste porte sono riservate sui nodi Admin.



Le porte utilizzate da altri servizi di rete non sono consentite. Per un elenco delle porte utilizzate per le comunicazioni interne ed esterne, consultare le linee guida per il collegamento in rete.

5. Selezionare **HTTP** o **HTTPS** per specificare il protocollo di rete per questo endpoint.
6. Selezionare una modalità di binding degli endpoint.
 - **Globale** (impostazione predefinita): L'endpoint è accessibile su tutti i nodi Gateway e Admin sul numero di porta specificato.

Create Endpoint

Display Name

Port

Protocol HTTP HTTPS

Endpoint Binding Mode Global HA Group VIPs Node Interfaces

This endpoint is currently bound globally. All nodes will use this endpoint unless an endpoint with an overriding binding mode exists for a specific port.

- **Ha Group VIP**: L'endpoint è accessibile solo attraverso gli indirizzi IP virtuali definiti per i gruppi ha selezionati. Gli endpoint definiti in questa modalità possono riutilizzare lo stesso numero di porta, purché i gruppi ha definiti da tali endpoint non si sovrappongono tra loro.

Selezionare i gruppi ha con gli indirizzi IP virtuali in cui si desidera visualizzare l'endpoint.

Create Endpoint

Display Name

Port

Protocol HTTP HTTPS

Endpoint Binding Mode Global HA Group VIPs Node Interfaces

Name	Description	Virtual IP Addresses	Interfaces
<input type="checkbox"/> Group1		192.168.5.163	CO-REF-DC1-ADM1:eth0 (preferred Master)
<input type="checkbox"/> Group2		47.47.5.162	CO-REF-DC1-ADM1:eth2 (preferred Master)

Displaying 2 HA groups.

⚠ No HA groups selected. You must select one or more HA Groups; otherwise, this endpoint will act as a globally bound endpoint.

- **Node Interfaces:** L'endpoint è accessibile solo sui nodi designati e sulle interfacce di rete. Gli endpoint definiti in questa modalità possono riutilizzare lo stesso numero di porta purché tali interfacce non si sovrappongano l'una all'altra.

Selezionare le interfacce del nodo in cui si desidera visualizzare l'endpoint.

Create Endpoint

Display Name

Port

Protocol HTTP HTTPS

Endpoint Binding Mode Global HA Group VIPs Node Interfaces

Node	Interface
<input type="checkbox"/> CO-REF-DC1-ADM1	eth0
<input type="checkbox"/> CO-REF-DC1-ADM1	eth1
<input type="checkbox"/> CO-REF-DC1-ADM1	eth2
<input type="checkbox"/> CO-REF-DC1-GW1	eth0
<input type="checkbox"/> CO-REF-DC2-ADM1	eth0
<input type="checkbox"/> CO-REF-DC2-GW1	eth0

⚠ No node interfaces selected. You must select one or more node interfaces; otherwise, this endpoint will act as a globally bound endpoint.

7. Selezionare **Salva**.

Viene visualizzata la finestra di dialogo Edit Endpoint (Modifica endpoint).

8. Selezionare **S3** o **Swift** per specificare il tipo di traffico che verrà utilizzato dall'endpoint.

Edit Endpoint Unsecured Port A (port 10449)

Endpoint Service Configuration

Endpoint service type S3 Swift

9. Se si seleziona **HTTP**, selezionare **Save** (Salva).

Viene creato l'endpoint non protetto. La tabella nella pagina degli endpoint del bilanciamento del carico elenca il nome visualizzato, il numero di porta, il protocollo e l'ID dell'endpoint dell'endpoint.

10. Se si seleziona **HTTPS** e si desidera caricare un certificato, selezionare **carica certificato**.

Load Certificate

Upload the PEM-encoded custom certificate, private key, and CA bundle files.

Server Certificate

Certificate Private Key

CA Bundle

- a. Cercare il certificato del server e la chiave privata del certificato.

Per consentire ai client S3 di connettersi utilizzando un nome di dominio dell'endpoint S3 API, utilizzare un certificato con più domini o caratteri jolly che corrisponda a tutti i nomi di dominio che il client potrebbe utilizzare per connettersi alla griglia. Ad esempio, il certificato del server potrebbe utilizzare il nome di dominio `*.example.com`.

"Configurazione dei nomi di dominio degli endpoint S3 API"

- a. Se si desidera, cercare un bundle CA.
- b. Selezionare **Salva**.

Vengono visualizzati i dati del certificato con codifica PEM per l'endpoint.

11. Se si seleziona **HTTPS** e si desidera generare un certificato, selezionare **generate Certificate** (genera certificato).

Generate Certificate

Domain 1	<input type="text" value="*.s3.example.com"/>	+
IP 1	<input type="text" value="0.0.0.0"/>	+
Subject	<input type="text" value="/CN=StorageGRID"/>	
Days valid	<input type="text" value="730"/>	

a. Immettere un nome di dominio o un indirizzo IP.

È possibile utilizzare i caratteri jolly per rappresentare i nomi di dominio completi di tutti i nodi Admin e Gateway che eseguono il servizio Load Balancer. Ad esempio, *.sgws.foo.com utilizza il carattere jolly * per rappresentare gn1.sgws.foo.com e gn2.sgws.foo.com.

"Configurazione dei nomi di dominio degli endpoint S3 API"

a. Selezionare **+** Per aggiungere altri nomi di dominio o indirizzi IP.

Se si utilizzano gruppi ad alta disponibilità (ha), aggiungere i nomi di dominio e gli indirizzi IP degli virtuali ha.

b. Se si desidera, immettere un oggetto X.509, noto anche come nome distinto (DN), per identificare chi possiede il certificato.

c. Se si desidera, selezionare il numero di giorni in cui il certificato è valido. L'impostazione predefinita è 730 giorni.

d. Selezionare **generate**.

Vengono visualizzati i metadati del certificato e i dati del certificato con codifica PEM per l'endpoint.

12. Fare clic su **Save** (Salva).

Viene creato l'endpoint. La tabella nella pagina degli endpoint del bilanciamento del carico elenca il nome visualizzato, il numero di porta, il protocollo e l'ID dell'endpoint dell'endpoint.

Informazioni correlate

["Mantieni Ripristina"](#)

["Linee guida per la rete"](#)

["Gestione di gruppi ad alta disponibilità"](#)

["Gestione di reti client non attendibili"](#)

Modifica degli endpoint del bilanciamento del carico

Per un endpoint non protetto (HTTP), è possibile modificare il tipo di servizio dell'endpoint tra S3 e Swift. Per un endpoint protetto (HTTPS), è possibile modificare il tipo di servizio dell'endpoint e visualizzare o modificare il certificato di protezione.

Di cosa hai bisogno

- È necessario disporre dell'autorizzazione di accesso root.
- È necessario accedere a Grid Manager utilizzando un browser supportato.

Fasi

1. Selezionare **Configuration > Network Settings > Load Balancer Endpoints**.

Viene visualizzata la pagina endpoint del bilanciamento del carico. Gli endpoint esistenti sono elencati nella tabella.

Gli endpoint con certificati che scadranno a breve sono identificati nella tabella.

Load Balancer Endpoints

Load balancer endpoints define Gateway Node and Admin Node ports that accept and load balance S3 and Swift requests to Storage Nodes. HTTPS endpoint certificates are configured per endpoint.

<input type="button" value="+ Add endpoint"/> <input type="button" value="✎ Edit endpoint"/> <input type="button" value="✕ Remove endpoint"/>			
	Display name	Port	Using HTTPS
<input type="radio"/>	Unsecured Endpoint 5	10444	No
<input checked="" type="radio"/>	Secured Endpoint 1	10443	Yes
			Displaying 2 endpoints.

2. Selezionare l'endpoint che si desidera modificare.
3. Fare clic su **Edit endpoint** (Modifica endpoint).

Viene visualizzata la finestra di dialogo Edit Endpoint (Modifica endpoint).

Per un endpoint non protetto (HTTP), viene visualizzata solo la sezione Configurazione servizio endpoint della finestra di dialogo. Per un endpoint protetto (HTTPS), vengono visualizzate le sezioni Endpoint Service Configuration (Configurazione servizio endpoint) e Certificates (certificati) della finestra di dialogo, come illustrato nell'esempio seguente.

Rimozione degli endpoint del bilanciamento del carico

Se non hai più bisogno di un endpoint di bilanciamento del carico, puoi rimuoverlo.

Di cosa hai bisogno

- È necessario disporre dell'autorizzazione di accesso root.
- È necessario accedere a Grid Manager utilizzando un browser supportato.

Fasi

1. Selezionare **Configuration > Network Settings > Load Balancer Endpoints**.

Viene visualizzata la pagina endpoint del bilanciamento del carico. Gli endpoint esistenti sono elencati nella tabella.

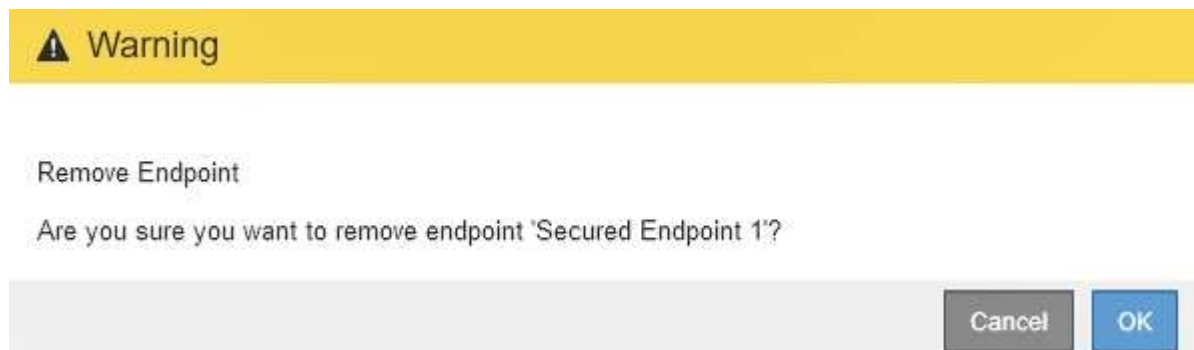
Load Balancer Endpoints

Load balancer endpoints define Gateway Node and Admin Node ports that accept and load balance S3 and Swift requests to Storage Nodes. HTTPS endpoint certificates are configured per endpoint.

<input type="button" value="+ Add endpoint"/> <input type="button" value="✎ Edit endpoint"/> <input type="button" value="✕ Remove endpoint"/>			
	Display name	Port	Using HTTPS
<input type="radio"/>	Unsecured Endpoint 5	10444	No
<input checked="" type="radio"/>	Secured Endpoint 1	10443	Yes
Displaying 2 endpoints.			

2. Selezionare il pulsante di opzione a sinistra dell'endpoint che si desidera rimuovere.
3. Fare clic su **Rimuovi endpoint**.

Viene visualizzata una finestra di dialogo di conferma.



4. Fare clic su **OK**.

L'endpoint viene rimosso.

Come funziona il bilanciamento del carico - servizio CLB

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

Il servizio CLB utilizza il bilanciamento del carico di livello 4 per distribuire le connessioni di rete TCP in entrata

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

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

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

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

Informazioni correlate

["Quali sono i costi di collegamento"](#)

["Aggiornamento dei costi di collegamento"](#)

Gestione di 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 esplicitamente.

Per impostazione predefinita, la rete client su ciascun nodo della griglia è *trusted*. Ovvero, per impostazione predefinita, StorageGRID considera attendibili le connessioni in entrata a ciascun nodo della griglia su tutte le porte esterne disponibili (vedere le informazioni sulle comunicazioni esterne nelle linee guida della rete).

È possibile ridurre la minaccia di attacchi ostili al sistema StorageGRID specificando che la rete client di ciascun nodo è *non attendibile*. Se la rete client di un nodo non è attendibile, il nodo accetta solo connessioni in entrata su porte esplicitamente configurate come endpoint del bilanciamento del carico.

Esempio 1: Il nodo gateway accetta solo richieste HTTPS S3

Si supponga che un nodo gateway rifiuti tutto il traffico in entrata sulla rete client, ad eccezione delle richieste HTTPS S3. Eseguire le seguenti operazioni generali:

1. Dalla pagina degli endpoint del bilanciamento del carico, configurare un endpoint del bilanciamento del carico per S3 su HTTPS sulla porta 443.
2. Nella pagina Untrusted Client Networks (reti client non attendibili), 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: Storage Node invia richieste di servizi della piattaforma S3

Si supponga di voler abilitare il traffico di servizio della piattaforma S3 in uscita da un nodo di storage, ma di voler impedire qualsiasi connessione in entrata a tale nodo di storage sulla rete client. Eseguire questa fase generale:

- Nella pagina Untrusted Client Networks (reti client non attendibili), indicare che la rete client sul nodo di storage non è attendibile.

Dopo aver salvato la configurazione, il nodo di storage non accetta più il traffico in entrata sulla rete client, ma continua a consentire le richieste in uscita ad Amazon Web Services.

Informazioni correlate

["Linee guida per la rete"](#)

["Configurazione degli endpoint del bilanciamento del carico"](#)

Specificare una rete client di un nodo non è attendibile

Se si utilizza una rete client, è possibile specificare se la rete client di ciascun nodo è attendibile o meno. È inoltre possibile specificare l'impostazione predefinita per i nuovi nodi aggiunti in un'espansione.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre dell'autorizzazione di accesso root.
- Se si desidera che un nodo Admin o un nodo gateway accetti il traffico in entrata solo su endpoint configurati esplicitamente, sono stati definiti gli endpoint del bilanciamento del carico.



Le connessioni client esistenti potrebbero non riuscire se gli endpoint del bilanciamento del carico non sono stati configurati.

Fasi

1. Selezionare **Configurazione Impostazioni di rete rete client non attendibile**.

Viene visualizzata la pagina Untrusted Client Networks (reti client non attendibili).

Questa pagina elenca tutti i nodi nel sistema StorageGRID. La colonna motivo non disponibile include una voce se la rete client del nodo deve essere attendibile.

Untrusted Client Networks

If you are using a Client Network, you can specify whether a node trusts inbound traffic from the Client Network. If the Client Network is untrusted, the node only accepts inbound traffic on ports configured as [load balancer endpoints](#).

Set New Node Default

This setting applies to new nodes expanded into the grid.

New Node Client Network Default Trusted Untrusted

Select Untrusted Client Network Nodes

Select nodes that should have untrusted Client Network enforcement.

<input type="checkbox"/>	Node Name	Unavailable Reason
<input type="checkbox"/>	DC1-ADM1	
<input type="checkbox"/>	DC1-G1	
<input type="checkbox"/>	DC1-S1	
<input type="checkbox"/>	DC1-S2	
<input type="checkbox"/>	DC1-S3	
<input type="checkbox"/>	DC1-S4	

Client Network untrusted on 0 nodes.

Save

- Nella sezione **Set New Node Default** (Imposta nuovo nodo predefinito), specificare l'impostazione predefinita quando si aggiungono nuovi nodi alla griglia in una procedura di espansione.
 - Trusted:** Quando un nodo viene aggiunto in un'espansione, la sua rete client è attendibile.
 - Untrusted:** Quando un nodo viene aggiunto in un'espansione, la sua rete client non è attendibile. Se necessario, tornare a questa pagina per modificare l'impostazione di un nuovo nodo specifico.



Questa impostazione non influisce sui nodi esistenti nel sistema StorageGRID.

- Nella sezione **Select untrusted Client Network Nodes** (Seleziona nodi di rete client non attendibili), selezionare i nodi che devono consentire le connessioni client solo su endpoint del bilanciamento del carico configurati esplicitamente.

È possibile selezionare o deselezionare la casella di controllo nel titolo per selezionare o deselezionare tutti i nodi.

- Fare clic su **Save** (Salva).

Le nuove regole del firewall vengono aggiunte e applicate immediatamente. Le connessioni client esistenti potrebbero non riuscire se gli endpoint del bilanciamento del carico non sono stati configurati.

Informazioni correlate

["Configurazione degli endpoint del bilanciamento del carico"](#)

Gestione di gruppi ad alta disponibilità

I gruppi ad alta disponibilità (ha) possono essere utilizzati per fornire connessioni dati ad alta disponibilità per i client S3 e Swift. I gruppi HA possono anche essere utilizzati per fornire connessioni altamente disponibili al Grid Manager e al tenant Manager.

- ["Che cos'è un gruppo ha"](#)
- ["Come vengono utilizzati i gruppi ha"](#)
- ["Opzioni di configurazione per i gruppi ha"](#)
- ["Creazione di un gruppo ad alta disponibilità"](#)
- ["Modifica di un gruppo ad alta disponibilità"](#)
- ["Rimozione di un gruppo ad alta disponibilità"](#)

Che cos'è un gruppo ha

I gruppi ad alta disponibilità utilizzano indirizzi IP virtuali (VIP) per fornire l'accesso di backup attivo ai servizi Gateway Node o Admin Node.

Un gruppo ha è costituito da una o più interfacce di rete sui nodi Admin e sui nodi Gateway. Quando si crea un gruppo ha, si selezionano le interfacce di rete appartenenti alla rete Grid (eth0) o alla rete client (eth2). Tutte le interfacce di un gruppo ha devono trovarsi all'interno della stessa subnet di rete.

Un gruppo ha mantiene uno o più indirizzi IP virtuali aggiunti all'interfaccia attiva del gruppo. Se l'interfaccia attiva non è più disponibile, gli indirizzi IP virtuali vengono spostati in un'altra interfaccia. Questo processo di failover richiede in genere solo pochi secondi ed è abbastanza rapido da consentire alle applicazioni client di avere un impatto minimo e può fare affidamento sui normali comportamenti di ripetizione per continuare a funzionare.

L'interfaccia attiva in un gruppo ha è designata come master. Tutte le altre interfacce sono designate come Backup. Per visualizzare queste designazioni, selezionare **Nodes Node Overview**.

DC1-ADM1 (Admin Node)

Node Information	
Name	DC1-ADM1
Type	Admin Node
ID	711b7b9b-8d24-4d9f-877a-be3fa3ac27e8
Connection State	✔ Connected
Software Version	11.4.0 (build 20200515.2346.8edcbbf)
HA Groups	Fabric Pools, Master
IP Addresses	192.168.2.208, 10.224.2.208, 47.47.2.208, 47.47.4.219 Show more

Quando si crea un gruppo ha, si specifica un'interfaccia come master preferito. Preferred Master è l'interfaccia

attiva a meno che non si verifichi un errore che causa la riassegnazione degli indirizzi VIP a un'interfaccia di backup. Una volta risolto il problema, gli indirizzi VIP vengono automaticamente riportati al Master preferito.

Il failover può essere attivato per uno dei seguenti motivi:

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



Il failover potrebbe non essere attivato da guasti di rete esterni al nodo che ospita l'interfaccia attiva. Allo stesso modo, il failover non viene attivato dal guasto del servizio CLB (obsoleto) o dei servizi per Grid Manager o il tenant Manager.

Se il gruppo ha include interfacce da più di due nodi, l'interfaccia attiva potrebbe spostarsi su qualsiasi altra interfaccia del nodo durante il failover.

Come vengono utilizzati i gruppi ha

È possibile utilizzare i gruppi ad alta disponibilità (ha) per diversi motivi.

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

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

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

Scopo del gruppo ha	Aggiungere nodi di questo tipo al gruppo ha
Accesso a Grid Manager	<ul style="list-style-type: none">• Nodo amministratore primario (Master preferito)• Nodi amministrativi non primari <p>Nota: il nodo di amministrazione primario deve essere il master preferito. Alcune procedure di manutenzione possono essere eseguite solo dal nodo di amministrazione primario.</p>
Accesso solo al tenant manager	<ul style="list-style-type: none">• Nodi di amministrazione primari o non primari
Accesso client S3 o Swift — Servizio Load Balancer	<ul style="list-style-type: none">• Nodi di amministrazione• Nodi gateway

Scopo del gruppo ha	Aggiungere nodi di questo tipo al gruppo ha
Accesso client S3 o Swift — Servizio CLB Nota: il servizio CLB è obsoleto.	<ul style="list-style-type: none"> • Nodi gateway

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

Il guasto dei servizi per Grid Manager o Tenant Manager non attiva il failover all'interno del gruppo ha.

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

Non è possibile eseguire alcune procedure di manutenzione quando il nodo di amministrazione primario non è disponibile. Durante il failover, è possibile utilizzare Grid Manager per monitorare il sistema StorageGRID.

Limitazioni dell'utilizzo di gruppi ha con il servizio CLB

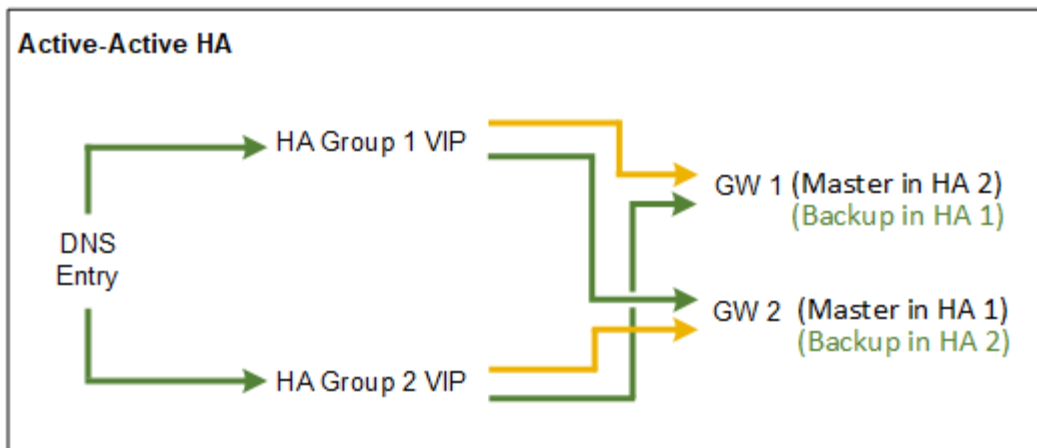
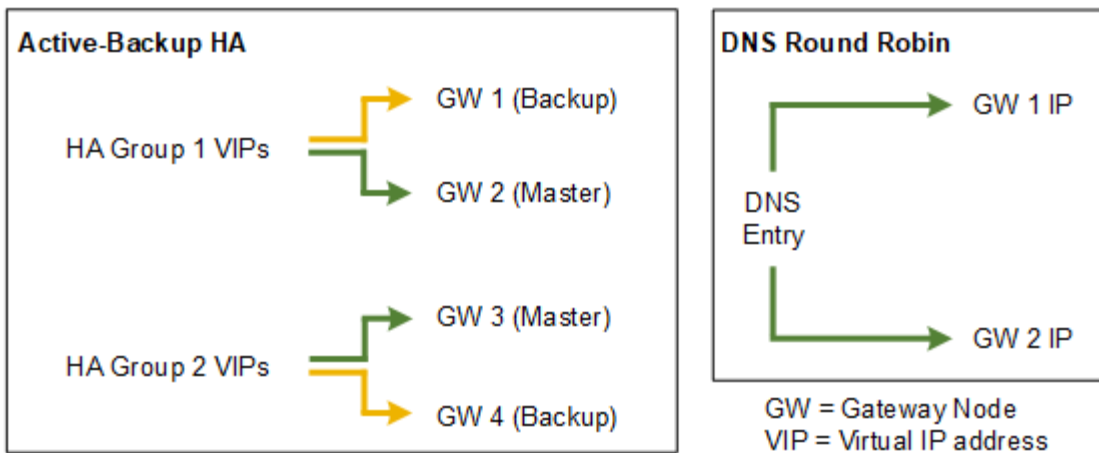
Il guasto del servizio CLB non attiva il failover all'interno del gruppo ha.



Il servizio CLB è obsoleto.

Opzioni di configurazione per i gruppi ha

I seguenti diagrammi forniscono esempi di diversi modi per configurare i gruppi ha. Ogni opzione presenta vantaggi e svantaggi.



Quando si creano più gruppi ha sovrapposti, come mostrato nell'esempio Active-Active ha, il throughput totale viene scalato in base al numero di nodi e gruppi ha. Con tre o più nodi e tre o più gruppi ha, puoi anche continuare le operazioni utilizzando uno qualsiasi dei VIP anche durante le procedure di manutenzione che richiedono di portare un nodo offline.

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

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

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

Creazione di un gruppo ad alta disponibilità

È possibile creare uno o più gruppi ad alta disponibilità (ha) per fornire un accesso altamente disponibile ai servizi sui nodi Admin o Gateway.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre dell'autorizzazione di accesso root.

A proposito di questa attività

Un'interfaccia deve soddisfare le seguenti condizioni per essere inclusa in un gruppo ha:

- L'interfaccia deve essere per un nodo gateway o un nodo amministratore.
- L'interfaccia deve appartenere alla Grid Network (eth0) o alla Client Network (eth2).
- L'interfaccia deve essere configurata con indirizzi IP fissi o statici, non con DHCP.

Fasi

1. Selezionare **Configurazione > Impostazioni di rete > gruppi ad alta disponibilità**.

Viene visualizzata la pagina High Availability Groups.

High Availability Groups

High availability (HA) groups allow multiple nodes to participate in an active-backup group. HA groups maintain virtual IP addresses on the active node and switch to a backup node automatically if a node fails.



2. Fare clic su **Create** (Crea).

Viene visualizzata la finestra di dialogo Crea gruppo ad alta disponibilità.

3. Digitare un nome e, se si desidera, una descrizione per il gruppo ha.
4. Fare clic su **Select Interfaces** (Seleziona interfacce).

Viene visualizzata la finestra di dialogo Add Interfaces to High Availability Group. La tabella elenca nodi, interfacce e subnet IPv4 idonee.

Add Interfaces to High Availability Group

Select interfaces to include in the HA group. All interfaces must be in the same network subnet.

Add to HA group	Node Name	Interface	IPv4 Subnet	Unavailable Reason
	g140-g1	eth0	172.16.0.0/21	This IP address is not in the same subnet as the selected interfaces
	g140-g1	eth2	47.47.0.0/21	This IP address is not in the same subnet as the selected interfaces
	g140-g2	eth0	172.16.0.0/21	This IP address is not in the same subnet as the selected interfaces
	g140-g2	eth2	47.47.0.0/21	This IP address is not in the same subnet as the selected interfaces
	g140-g3	eth0	172.16.0.0/21	This IP address is not in the same subnet as the selected interfaces
<input checked="" type="checkbox"/>	g140-g3	eth2	192.168.0.0/21	
	g140-g4	eth0	172.16.0.0/21	This IP address is not in the same subnet as the selected interfaces
<input checked="" type="checkbox"/>	g140-g4	eth2	192.168.0.0/21	

There are 2 interfaces selected.

Cancel

Apply

Se il relativo indirizzo IP è assegnato da DHCP, l'interfaccia non viene visualizzata nell'elenco.

5. Nella colonna **Aggiungi al gruppo ha**, selezionare la casella di controllo dell'interfaccia che si desidera aggiungere al gruppo ha.

Attenersi alle seguenti linee guida per la selezione delle interfacce:

- Selezionare almeno un'interfaccia.
- Se si seleziona più di un'interfaccia, tutte le interfacce devono trovarsi sulla rete griglia (eth0) o sulla rete client (eth2).
- Tutte le interfacce devono trovarsi nella stessa subnet o in subnet con un prefisso comune.

Gli indirizzi IP saranno limitati alla subnet più piccola (quella con il prefisso più grande).

- Se si selezionano interfacce su diversi tipi di nodi e si verifica un failover, solo i servizi comuni ai nodi selezionati saranno disponibili sugli IP virtuali.
 - Selezionare due o più nodi di amministrazione per la protezione ha di Grid Manager o di Tenant Manager.
 - Selezionare due o più nodi di amministrazione, nodi gateway o entrambi per la protezione ha del servizio Load Balancer.
 - Selezionare due o più nodi gateway per la protezione ha del servizio CLB.



Il servizio CLB è obsoleto.

Add Interfaces to High Availability Group

Select interfaces to include in the HA group. All interfaces must be in the same network subnet.

Add to HA group	Node Name	Interface	IPv4 Subnet	Unavailable Reason
<input checked="" type="checkbox"/>	DC1-ADM1	eth0	10.96.100.0/23	
<input checked="" type="checkbox"/>	DC1-G1	eth0	10.96.100.0/23	
<input checked="" type="checkbox"/>	DC2-ADM1	eth0	10.96.100.0/23	

There are 3 interfaces selected.

Attention: You have selected nodes of different types that run different services. If a failover occurs, only the services common to all node types will be available on the virtual IPs.

Cancel

Apply

6. Fare clic su **Apply** (Applica).

Le interfacce selezionate sono elencate nella sezione interfacce della pagina Crea gruppo ad alta disponibilità. Per impostazione predefinita, la prima interfaccia dell'elenco viene selezionata come Master preferito.

Create High Availability Group

High Availability Group

Name

Description

Interfaces

Select interfaces to include in the HA group. All interfaces must be in the same network subnet.

Select Interfaces

Node Name	Interface	IPv4 Subnet	Preferred Master
g140-g1	eth2	47.47.0.0/21	<input checked="" type="radio"/>
g140-g2	eth2	47.47.0.0/21	<input type="radio"/>

Displaying 2 interfaces.

Virtual IP Addresses

Virtual IP Subnet: 47.47.0.0/21. All virtual IP addresses must be within this subnet. There must be at least 1 and no more than 10 virtual IP addresses.

Virtual IP Address 1



Cancel

Save

- Se si desidera che un'interfaccia diversa sia la master preferita, selezionare tale interfaccia nella colonna **Master preferito**.

Preferred Master è l'interfaccia attiva a meno che non si verifichi un errore che causa la riassegnazione degli indirizzi VIP a un'interfaccia di backup.



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

- Nella sezione Virtual IP Addresses (indirizzi IP virtuali) della pagina, immettere da uno a 10 indirizzi IP virtuali per il gruppo ha. Fare clic sul segno più (+) Per aggiungere più indirizzi IP.

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

Gli indirizzi IPv4 devono trovarsi all'interno della subnet IPv4 condivisa da tutte le interfacce membri.

9. Fare clic su **Save** (Salva).

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

Informazioni correlate

["Installare Red Hat Enterprise Linux o CentOS"](#)

["Installare VMware"](#)

["Installare Ubuntu o Debian"](#)

["Gestione del bilanciamento del carico"](#)

Modifica di un gruppo ad alta disponibilità

È possibile modificare un gruppo ad alta disponibilità (ha) per modificarne nome e descrizione, aggiungere o rimuovere interfacce o aggiungere o aggiornare un indirizzo IP virtuale.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre dell'autorizzazione di accesso root.

A proposito di questa attività

Alcuni dei motivi per modificare un gruppo ha sono i seguenti:

- Aggiunta di un'interfaccia a un gruppo esistente. L'indirizzo IP dell'interfaccia deve trovarsi all'interno della stessa subnet delle altre interfacce già assegnate al gruppo.
- Rimozione di un'interfaccia da un gruppo ha. Ad esempio, non è possibile avviare una procedura di decommissionamento di un sito o di un nodo se in un gruppo ha viene utilizzata l'interfaccia di un nodo per Grid Network o Client Network.

Fasi

1. Selezionare **Configurazione > Impostazioni di rete > gruppi ad alta disponibilità**.

Viene visualizzata la pagina High Availability Groups.

High Availability Groups

High availability (HA) groups allow multiple nodes to participate in an active-backup group. HA groups maintain virtual IP addresses on the active node and switch to a backup node automatically if a node fails.

+ Create Edit Remove				
	Name	Description	Virtual IP Addresses	Interfaces
<input type="radio"/>	HA Group 1		47.47.4.219	g140-adm1:eth2 (preferred Master) g140-g1:eth2
<input type="radio"/>	HA Group 2		47.47.4.218 47.47.4.217	g140-g1:eth2 (preferred Master) g140-g2:eth2

Displaying 2 HA groups.

2. Selezionare il gruppo ha che si desidera modificare e fare clic su **Edit** (Modifica).

Viene visualizzata la finestra di dialogo Modifica gruppo ad alta disponibilità.

3. Facoltativamente, aggiornare il nome o la descrizione del gruppo.

4. Facoltativamente, fare clic su **Select Interfaces** (Seleziona interfacce) per modificare le interfacce per il gruppo ha.

Viene visualizzata la finestra di dialogo Add Interfaces to High Availability Group.

Add Interfaces to High Availability Group

Select interfaces to include in the HA group. All interfaces must be in the same network subnet.

Add to HA group	Node Name	Interface	IPv4 Subnet	Unavailable Reason
	g140-g1	eth0	172.16.0.0/21	This IP address is not in the same subnet as the selected interfaces
	g140-g1	eth2	47.47.0.0/21	This IP address is not in the same subnet as the selected interfaces
	g140-g2	eth0	172.16.0.0/21	This IP address is not in the same subnet as the selected interfaces
	g140-g2	eth2	47.47.0.0/21	This IP address is not in the same subnet as the selected interfaces
	g140-g3	eth0	172.16.0.0/21	This IP address is not in the same subnet as the selected interfaces
<input checked="" type="checkbox"/>	g140-g3	eth2	192.168.0.0/21	
	g140-g4	eth0	172.16.0.0/21	This IP address is not in the same subnet as the selected interfaces
<input checked="" type="checkbox"/>	g140-g4	eth2	192.168.0.0/21	

There are 2 interfaces selected.

Se il relativo indirizzo IP è assegnato da DHCP, l'interfaccia non viene visualizzata nell'elenco.

5. Selezionare o deselezionare le caselle di controllo per aggiungere o rimuovere interfacce.

Attenersi alle seguenti linee guida per la selezione delle interfacce:

- Selezionare almeno un'interfaccia.
- Se si seleziona più di un'interfaccia, tutte le interfacce devono trovarsi sulla rete griglia (eth0) o sulla rete client (eth2).
- Tutte le interfacce devono trovarsi nella stessa subnet o in subnet con un prefisso comune.

Gli indirizzi IP saranno limitati alla subnet più piccola (quella con il prefisso più grande).

- Se si selezionano interfacce su diversi tipi di nodi e si verifica un failover, solo i servizi comuni ai nodi selezionati saranno disponibili sugli IP virtuali.
 - Selezionare due o più nodi di amministrazione per la protezione ha di Grid Manager o di Tenant Manager.
 - Selezionare due o più nodi di amministrazione, nodi gateway o entrambi per la protezione ha del servizio Load Balancer.
 - Selezionare due o più nodi gateway per la protezione ha del servizio CLB.



Il servizio CLB è obsoleto.

6. Fare clic su **Apply** (Applica).

Le interfacce selezionate sono elencate nella sezione interfacce della pagina. Per impostazione predefinita, la prima interfaccia dell'elenco viene selezionata come Master preferito.

Edit High Availability Group 'HA Group - Admin Nodes'

High Availability Group

Name

Description

Interfaces

Select interfaces to include in the HA group. All interfaces must be in the same network subnet.

Node Name	Interface	IPv4 Subnet	Preferred Master
DC1-ADM1	eth0	10.96.100.0/23	<input checked="" type="radio"/>
DC2-ADM1	eth0	10.96.100.0/23	<input type="radio"/>

Displaying 2 interfaces.

Virtual IP Addresses

Virtual IP Subnet: 10.96.100.0/23. All virtual IP addresses must be within this subnet. There must be at least 1 and no more than 10 virtual IP addresses.

Virtual IP Address 1

7. Se si desidera che un'interfaccia diversa sia la master preferita, selezionare tale interfaccia nella colonna **Master preferito**.

Preferred Master è l'interfaccia attiva a meno che non si verifichi un errore che causa la riassegnazione degli indirizzi VIP a un'interfaccia di backup.



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

8. Facoltativamente, aggiornare gli indirizzi IP virtuali per il gruppo ha.

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

Gli indirizzi IPv4 devono trovarsi all'interno della subnet IPv4 condivisa da tutte le interfacce membri.

9. Fare clic su **Save** (Salva).

Il gruppo ha viene aggiornato.

Rimozione di un gruppo ad alta disponibilità

È possibile rimuovere un gruppo ad alta disponibilità (ha) che non si sta più utilizzando.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre dell'autorizzazione di accesso root.

Soprabout di questo compito

Se si rimuove un gruppo ha, qualsiasi client S3 o Swift configurato per utilizzare uno degli indirizzi IP virtuali del gruppo non sarà più in grado di connettersi a StorageGRID. Per evitare interruzioni del client, è necessario aggiornare tutte le applicazioni client S3 o Swift interessate prima di rimuovere un gruppo ha. Aggiornare ciascun client per la connessione utilizzando un altro indirizzo IP, ad esempio l'indirizzo IP virtuale di un gruppo ha diverso o l'indirizzo IP configurato per un'interfaccia durante l'installazione o utilizzando DHCP.

Fasi

1. Selezionare **Configurazione > Impostazioni di rete > gruppi ad alta disponibilità**.

Viene visualizzata la pagina High Availability Groups.

High Availability Groups

High availability (HA) groups allow multiple nodes to participate in an active-backup group. HA groups maintain virtual IP addresses on the active node and switch to a backup node automatically if a node fails.

<input type="button" value="+ Create"/> <input type="button" value="Edit"/> <input type="button" value="Remove"/>				
	Name	Description	Virtual IP Addresses	Interfaces
<input type="radio"/>	HA Group 1		47.47.4.219	g140-adm1:eth2 (preferred Master) g140-g1:eth2
<input type="radio"/>	HA Group 2		47.47.4.218 47.47.4.217	g140-g1:eth2 (preferred Master) g140-g2:eth2

Displaying 2 HA groups.

2. Selezionare il gruppo ha che si desidera rimuovere e fare clic su **Remove** (Rimuovi).

Viene visualizzato l'avviso Elimina gruppo ad alta disponibilità.

Warning

Delete High Availability Group

Are you sure you want to delete High Availability Group 'HA group 1'?

Cancel

OK

3. Fare clic su **OK**.

Il gruppo ha viene rimosso.

Configurazione dei nomi di dominio degli endpoint S3 API

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

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.
- Devi aver confermato che non è in corso un aggiornamento della griglia.



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

A proposito di questa attività

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

- Utilizzare Grid Manager per aggiungere i nomi di dominio degli endpoint S3 al sistema StorageGRID.
- Assicurarsi che il certificato utilizzato dal client per le connessioni HTTPS a StorageGRID sia firmato per tutti i nomi di dominio richiesti dal client.

Ad esempio, se l'endpoint è `s3.company.com`, È necessario assicurarsi che il certificato utilizzato per le connessioni HTTPS includa `s3.company.com` Endpoint e SAN (Subject alternative Name) con caratteri jolly dell'endpoint: `*.s3.company.com`.

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



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

Il certificato utilizzato da un client per le connessioni HTTPS dipende dal modo in cui il client si connette alla

griglia:

- Se un client si connette utilizzando il servizio Load Balancer, utilizza il certificato per uno specifico endpoint di bilanciamento del carico.



Ogni endpoint di bilanciamento del carico dispone di un proprio certificato e ciascun endpoint può essere configurato in modo da riconoscere nomi di dominio degli endpoint diversi.

- Se il client si connette a un nodo di storage o al servizio CLB su un nodo gateway, il client utilizza un certificato del server personalizzato Grid che è stato aggiornato per includere tutti i nomi di dominio endpoint richiesti.



Il servizio CLB è obsoleto.

Fasi

1. Selezionare **Configurazione Impostazioni di rete nomi di dominio**.

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

Endpoint Domain Names

Virtual Hosted-Style Requests

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

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

2. Utilizzando l'icona (+) per aggiungere altri campi, inserire l'elenco dei nomi di dominio degli endpoint API S3 nei campi **Endpoint**.

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

3. Fare clic su **Save** (Salva).
4. Assicurarsi che i certificati server utilizzati dai client corrispondano ai nomi di dominio degli endpoint richiesti.
 - Per i client che utilizzano il servizio Load Balancer, aggiornare il certificato associato all'endpoint del bilanciamento del carico a cui si connette il client.
 - Per i client che si connettono direttamente ai nodi di storage o che utilizzano il servizio CLB sui nodi gateway, aggiornare il certificato del server personalizzato per la griglia.
5. Aggiungere i record DNS necessari per garantire che le richieste dei nomi di dominio degli endpoint possano essere risolte.

Risultato

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

Informazioni correlate

["Utilizzare S3"](#)

["Visualizzazione degli indirizzi IP"](#)

["Creazione di un gruppo ad alta disponibilità"](#)

["Configurazione di un certificato server personalizzato per le connessioni al nodo di storage o al servizio CLB"](#)

["Configurazione degli endpoint del bilanciamento del carico"](#)

Abilitazione di HTTP per le comunicazioni client

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

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

A proposito di questa attività

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

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

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



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

Fasi

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

Network Options



3. Fare clic su **Save** (Salva).

Informazioni correlate

["Configurazione degli endpoint del bilanciamento del carico"](#)

["Utilizzare S3"](#)

["USA Swift"](#)

Controllare quali operazioni client sono consentite

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

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

A proposito di questa attività

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

• S3 REST API

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



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

• API REST Swift

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

Fasi

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

Network Options

Prevent Client Modification

Enable HTTP Connection

Network Transfer Encryption AES128-SHA AES256-SHA

3. Fare clic su **Save** (Salva).

Gestione delle reti e delle connessioni StorageGRID

È possibile utilizzare Grid Manager per configurare e gestire le reti e le connessioni StorageGRID.

Vedere ["Configurazione delle connessioni dei client S3 e Swift"](#) Per scoprire come connettere i client S3 o Swift.

- ["Linee guida per le reti StorageGRID"](#)
- ["Visualizzazione degli indirizzi IP"](#)
- ["Crittografia supportata per le connessioni TLS in uscita"](#)
- ["Modifica della crittografia del trasferimento di rete"](#)
- ["Configurazione dei certificati del server"](#)
- ["Configurazione delle impostazioni del proxy di storage"](#)
- ["Configurazione delle impostazioni del proxy amministratore"](#)
- ["Gestione delle policy di classificazione del traffico"](#)
- ["Quali sono i costi di collegamento"](#)

Linee guida per le reti StorageGRID

StorageGRID supporta fino a tre interfacce di rete per nodo di rete, consentendo di configurare la rete per ogni singolo nodo di rete in modo che corrisponda ai requisiti di sicurezza e accesso.



Per modificare o aggiungere una rete per un nodo griglia, consultare le istruzioni di ripristino e manutenzione. Per ulteriori informazioni sulla topologia di rete, consultare le istruzioni di rete.

Grid Network

Obbligatorio. La rete griglia viene utilizzata per tutto il traffico StorageGRID interno. Fornisce connettività tra tutti i nodi della rete, in tutti i siti e le subnet.

Admin Network (rete amministrativa)

Opzionale. La rete di amministrazione viene generalmente 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 client

Opzionale. La rete client è una rete aperta, generalmente utilizzata per fornire l'accesso alle applicazioni client S3 e Swift, 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 della griglia StorageGRID richiede un'interfaccia di rete dedicata, un indirizzo IP, una subnet mask e un gateway per ciascuna rete a cui è assegnato.
- Un nodo Grid non può avere più di un'interfaccia su una rete.
- È supportato un singolo gateway, per rete, per nodo di rete, che deve trovarsi sulla stessa sottorete del nodo. Se necessario, è possibile implementare un routing più complesso nel gateway.
- Su ciascun nodo, ogni rete viene mappata a una specifica interfaccia di rete.

Rete	Nome dell'interfaccia
Griglia	eth0
Admin (opzionale)	eth1
Client (opzionale)	eth2

- Se il nodo è collegato a un'appliance StorageGRID, vengono utilizzate porte specifiche per ciascuna rete. Per ulteriori informazioni, consultare le istruzioni di installazione dell'apparecchio.
- Il percorso predefinito viene generato automaticamente, per nodo. Se eth2 è attivato, 0.0.0.0/0 utilizza la rete client su eth2. Se eth2 non è abilitato, 0.0.0.0/0 utilizza Grid Network su eth0.
- La rete client non diventa operativa fino a quando il nodo grid non si è Unito alla griglia
- La rete amministrativa può essere configurata durante l'implementazione del nodo grid per consentire l'accesso all'interfaccia utente dell'installazione prima che la griglia sia completamente installata.

Informazioni correlate

["Mantieni Ripristina"](#)

["Linee guida per la rete"](#)

Visualizzazione degli 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 Grid dalla riga di comando ed eseguire varie procedure di manutenzione.

Di cosa hai bisogno

È necessario accedere a Grid Manager utilizzando un browser supportato.

A proposito di questa attività

Per informazioni sulla modifica degli indirizzi IP, consultare le istruzioni di ripristino e manutenzione.

Fasi

1. Selezionare **Nodes Grid Node Overview**.
2. Fare clic su **Mostra altri** a destra del titolo indirizzi IP.

Gli indirizzi IP per il nodo della griglia sono elencati in una tabella.

Node Information	
Name	SGA-lab11
Type	Storage Node
ID	0b583829-6659-4c6e-b2d0-31461d22ba67
Connection State	✔ Connected
Software Version	11.4.0 (build 20200527.0043.61839a2)
IP Addresses	192.168.4.138, 10.224.4.138, 169.254.0.1 Show less
Interface	IP Address
eth0	192.168.4.138
eth0	fd20:331:331:0:2a0:98ff:fea1:831d
eth0	fe80::2a0:98ff:fea1:831d
eth1	10.224.4.138
eth1	fd20:327:327:0:280:e5ff:fe43:a99c
eth1	fd20:8b1e:b255:8154:280:e5ff:fe43:a99c
eth1	fe80::280:e5ff:fe43:a99c
hic2	192.168.4.138
hic4	192.168.4.138
mtc1	10.224.4.138
mtc2	169.254.0.1

Informazioni correlate

["Mantieni Ripristina"](#)

Crittografia supportata per le connessioni TLS in uscita

Il sistema StorageGRID supporta un set limitato di suite di crittografia per le connessioni TLS (Transport Layer Security) ai sistemi esterni utilizzati per la federazione di identità e i pool di storage 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 storage cloud.

I cifrari TLS supportati per l'utilizzo con sistemi esterni sono stati selezionati per garantire la compatibilità con una vasta gamma di sistemi esterni. L'elenco è più grande dell'elenco di cifrature supportate per l'utilizzo con le applicazioni client S3 o Swift.



Le opzioni di configurazione TLS, quali versioni di protocollo, crittografia, algoritmi di scambio delle chiavi e algoritmi MAC, non sono configurabili in StorageGRID. Se hai richieste specifiche su queste impostazioni, contatta il tuo rappresentante NetApp.

Suite di crittografia TLS 1.2 supportate

Sono supportate le seguenti suite di crittografia TLS 1.2:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384

Suite di crittografia TLS 1.3 supportate

Sono supportate le seguenti suite di crittografia TLS 1.3:

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256

Modifica della crittografia del trasferimento di rete

Il sistema StorageGRID utilizza TLS (Transport Layer Security) per proteggere il traffico di controllo interno tra i nodi di rete. L'opzione Network Transfer Encryption (crittografia trasferimento di rete) imposta l'algoritmo utilizzato da TLS per crittografare il traffico di controllo tra i nodi della griglia. Questa impostazione non influisce sulla crittografia dei dati.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

A proposito di questa attività

Per impostazione predefinita, la crittografia del trasferimento di rete utilizza l'algoritmo AES256-SHA. Il traffico di controllo può anche essere crittografato utilizzando l'algoritmo AES128-SHA.

Fasi

1. Selezionare **Configurazione Impostazioni di sistema Opzioni griglia**.
2. Nella sezione Network Options (Opzioni di rete), impostare Network Transfer Encryption (crittografia trasferimento di rete) su **AES128-SHA** o **AES256-SHA** (impostazione predefinita).

Network Options



3. Fare clic su **Save** (Salva).

Configurazione dei certificati del server

È possibile personalizzare i certificati server utilizzati dal sistema StorageGRID.

Il sistema StorageGRID utilizza certificati di sicurezza per diversi scopi distinti:

- Management Interface Server Certificates: Utilizzato per proteggere l'accesso a Grid Manager, tenant Manager, Grid Management API e tenant Management API.
- Storage API Server Certificates: Utilizzato per proteggere l'accesso ai nodi di storage e ai nodi gateway, le applicazioni client API utilizzate per caricare e scaricare i dati degli oggetti.

È possibile utilizzare i certificati predefiniti creati durante l'installazione oppure sostituire uno o entrambi i tipi di certificati predefiniti con certificati personalizzati.

Tipi supportati di certificati server personalizzati

Il sistema StorageGRID supporta certificati server personalizzati crittografati con RSA o ECDSA (algoritmo di firma digitale a curva ellittica).

Per ulteriori informazioni su come StorageGRID protegge le connessioni client per l'API REST, consultare le guide all'implementazione di S3 o Swift.

Certificati per gli endpoint del bilanciamento del carico

StorageGRID gestisce separatamente i certificati utilizzati per gli endpoint del bilanciamento del carico. Per configurare i certificati di bilanciamento del carico, consultare le istruzioni per la configurazione degli endpoint di bilanciamento del carico.

Informazioni correlate

["Utilizzare S3"](#)

["USA Swift"](#)

["Configurazione degli endpoint del bilanciamento del carico"](#)

Configurazione di un certificato server personalizzato per Grid Manager e Tenant Manager

È possibile sostituire il certificato del server StorageGRID predefinito con un singolo certificato server personalizzato che consente agli utenti di accedere a Grid Manager e a Tenant Manager senza incontrare avvisi di sicurezza.

A proposito di questa attività

Per impostazione predefinita, ogni nodo amministrativo riceve un certificato firmato dalla CA della griglia. Questi certificati firmati dalla CA possono essere sostituiti da un singolo certificato server personalizzato comune e dalla chiave privata corrispondente.

Poiché per tutti i nodi di amministrazione viene utilizzato un singolo certificato server personalizzato, è necessario specificare il certificato come carattere jolly o certificato multidominio se i client devono verificare il nome host durante la connessione a Grid Manager e Tenant Manager. Definire il certificato personalizzato in modo che corrisponda a tutti i nodi Admin nella griglia.

È necessario completare la configurazione sul server e, a seconda dell'autorità di certificazione (CA) di origine in uso, gli utenti potrebbero dover installare il certificato CA di origine nel browser Web utilizzato per accedere a Grid Manager e a Tenant Manager.



Per garantire che le operazioni non vengano interrotte da un certificato del server guasto, l'avviso **scadenza del certificato del server per l'interfaccia di gestione** e l'allarme MCEP (Management Interface Certificate Expiry) legacy vengono attivati quando il certificato del server sta per scadere. In base alle esigenze, è possibile visualizzare il numero di giorni che devono essere trascorsi prima della scadenza del certificato di servizio corrente selezionando **supporto Strumenti topologia griglia**. Quindi, selezionare **Primary Admin Node CMN Resources**.



Se si accede a Grid Manager o Tenant Manager utilizzando un nome di dominio invece di un indirizzo IP, il browser mostra un errore di certificato senza l'opzione di ignorare se si verifica una delle seguenti condizioni:

- Il certificato del server dell'interfaccia di gestione personalizzata scade.
- Viene ripristinato il certificato del server di un'interfaccia di gestione personalizzata al certificato del server predefinito.

Fasi

1. Selezionare **Configurazione Impostazioni di rete certificati server**.
2. Nella sezione Management Interface Server Certificate (certificato server interfaccia di gestione), fare clic su **Install Custom Certificate** (Installa certificato personalizzato).
3. Caricare i file dei certificati del server richiesti:
 - **Server Certificate**: Il file di certificato del server personalizzato (.crt).
 - **Server Certificate Private Key** (chiave privata certificato server): Il file di chiave privata del certificato del server personalizzato (.key).



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

- **Bundle CA**: Un singolo file contenente i certificati di ciascuna CA intermedia. Il file deve contenere ciascuno dei file di certificato CA con codifica PEM, concatenati in ordine di catena del certificato.
4. Fare clic su **Save** (Salva).

I certificati server personalizzati vengono utilizzati per tutte le nuove connessioni client successive.

Selezionare una scheda per visualizzare informazioni dettagliate sul certificato del server StorageGRID predefinito o su un certificato firmato dalla CA caricato.



Dopo aver caricato un nuovo certificato, attendere fino a un giorno per eliminare eventuali avvisi relativi alla scadenza del certificato (o allarmi legacy).

5. Aggiornare la pagina per assicurarsi che il browser Web sia aggiornato.

Ripristino dei certificati server predefiniti per Grid Manager e Tenant Manager

È possibile ripristinare l'utilizzo dei certificati server predefiniti per Grid Manager e Tenant Manager.

Fasi

1. Selezionare **Configurazione Impostazioni di rete certificati server**.
2. Nella sezione Manage Interface Server Certificate (Gestisci certificato server interfaccia), fare clic su **Use Default Certificates** (Usa certificati predefiniti)
3. Fare clic su **OK** nella finestra di dialogo di conferma.

Quando si ripristinano i certificati del server predefiniti, i file dei certificati del server personalizzati configurati vengono cancellati e non possono essere ripristinati dal sistema. I certificati server predefiniti vengono utilizzati per tutte le nuove connessioni client successive.

4. Aggiornare la pagina per assicurarsi che il browser Web sia aggiornato.

Configurazione di un certificato server personalizzato per le connessioni al nodo di storage o al servizio CLB

È possibile sostituire il certificato del server utilizzato per le connessioni client S3 o Swift al nodo di storage o al servizio CLB (obsoleto) sul nodo gateway. Il certificato del server personalizzato sostitutivo è specifico dell'organizzazione.

A proposito di questa attività

Per impostazione predefinita, ogni nodo di storage viene emesso un certificato server X.509 firmato dalla CA della griglia. Questi certificati firmati dalla CA possono essere sostituiti da un singolo certificato server personalizzato comune e dalla chiave privata corrispondente.

Per tutti i nodi di storage viene utilizzato un singolo certificato server personalizzato, pertanto è necessario specificare il certificato come certificato wildcard o multi-dominio se i client devono verificare il nome host durante la connessione all'endpoint di storage. Definire il certificato personalizzato in modo che corrisponda a tutti i nodi di storage nella griglia.

Una volta completata la configurazione sul server, gli utenti potrebbero anche aver bisogno di installare il certificato CA principale nel client S3 o Swift API che utilizzeranno per accedere al sistema, a seconda dell'autorità di certificazione (CA) root in uso.



Per garantire che le operazioni non vengano interrotte da un certificato del server guasto, l'avviso **scadenza del certificato del server per gli endpoint API di storage** e l'allarme scadenza del certificato (SCEP) degli endpoint del servizio API di storage legacy vengono attivati quando il certificato del server root sta per scadere. In base alle esigenze, è possibile visualizzare il numero di giorni che devono essere trascorsi prima della scadenza del certificato di servizio corrente selezionando **supporto Strumenti topologia griglia**. Quindi, selezionare **Primary Admin Node CMN Resources**.

I certificati personalizzati vengono utilizzati solo se i client si connettono a StorageGRID utilizzando il servizio

CLB obsoleto sui nodi gateway o se si connettono direttamente ai nodi di storage. I client S3 o Swift che si connettono a StorageGRID utilizzando il servizio bilanciamento del carico sui nodi di amministrazione o gateway utilizzano il certificato configurato per l'endpoint del bilanciamento del carico.



L'avviso **scadenza del certificato endpoint del bilanciamento del carico** viene attivato per gli endpoint del bilanciamento del carico che scadranno a breve.

Fasi

1. Selezionare **Configurazione Impostazioni di rete certificati server**.
2. Nella sezione Object Storage API Service Endpoints Server Certificate, fare clic su **Install Custom Certificate** (Installa certificato personalizzato).
3. Caricare i file dei certificati del server richiesti:
 - **Server Certificate**: Il file di certificato del server personalizzato (.crt).
 - **Server Certificate Private Key** (chiave privata certificato server): Il file di chiave privata del certificato del server personalizzato (.key).



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

- **Bundle CA**: Un singolo file contenente i certificati di ciascuna CA intermedia. Il file deve contenere ciascuno dei file di certificato CA con codifica PEM, concatenati in ordine di catena del certificato.
4. Fare clic su **Save** (Salva).

Il certificato del server personalizzato viene utilizzato per tutte le nuove connessioni client API successive.

Selezionare una scheda per visualizzare informazioni dettagliate sul certificato del server StorageGRID predefinito o su un certificato firmato dalla CA caricato.



Dopo aver caricato un nuovo certificato, attendere fino a un giorno per eliminare eventuali avvisi relativi alla scadenza del certificato (o allarmi legacy).

5. Aggiornare la pagina per assicurarsi che il browser Web sia aggiornato.

Informazioni correlate

["Utilizzare S3"](#)

["USA Swift"](#)

["Configurazione dei nomi di dominio degli endpoint S3 API"](#)

Ripristino dei certificati server predefiniti per gli endpoint S3 e Swift REST API

È possibile ripristinare l'utilizzo dei certificati server predefiniti per gli endpoint S3 e Swift REST API.

Fasi

1. Selezionare **Configurazione Impostazioni di rete certificati server**.
2. Nella sezione Object Storage API Service Endpoints Server Certificate, fare clic su **Use Default Certificates** (Usa certificati predefiniti).

3. Fare clic su **OK** nella finestra di dialogo di conferma.

Quando si ripristinano i certificati server predefiniti per gli endpoint API dello storage a oggetti, i file di certificato del server personalizzati configurati vengono cancellati e non possono essere ripristinati dal sistema. I certificati server predefiniti vengono utilizzati per tutte le nuove connessioni client API successive.

4. Aggiornare la pagina per assicurarsi che il browser Web sia aggiornato.

Copia del certificato CA del sistema StorageGRID

StorageGRID utilizza un'autorità di certificazione (CA) interna per proteggere il traffico interno. Questo certificato non cambia se si caricano i propri certificati.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

A proposito di questa attività

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.

Fasi

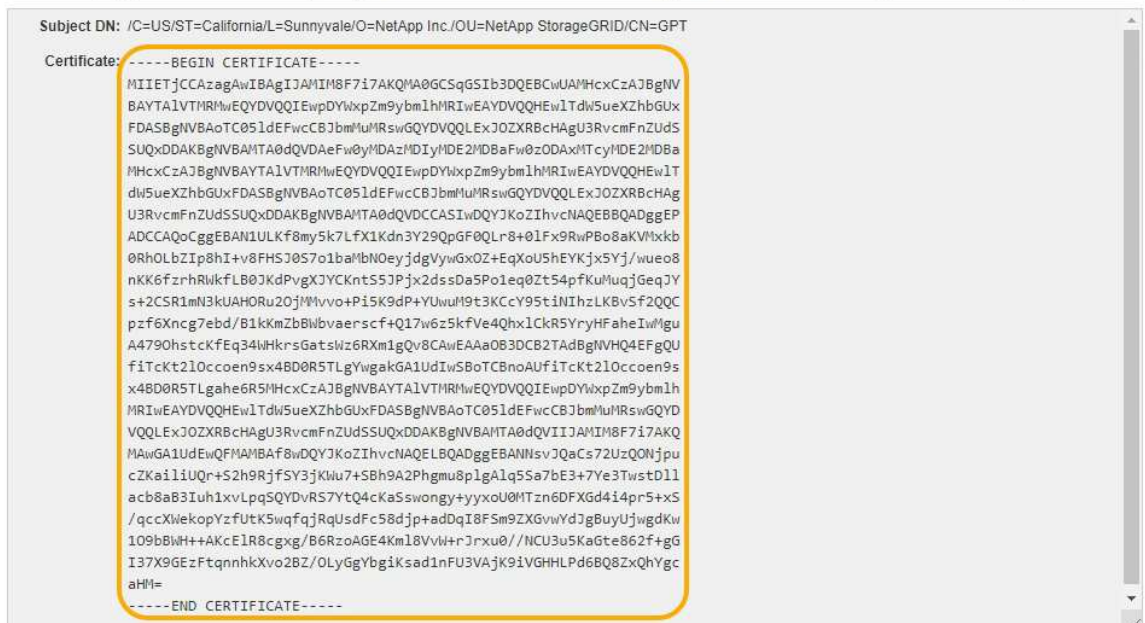
1. Selezionare **Configurazione Impostazioni di rete certificati server**.
2. Nella sezione **certificato CA interno**, selezionare tutto il testo del certificato.

È necessario includere -----BEGIN CERTIFICATE----- e -----END CERTIFICATE----- nella selezione.

Internal CA Certificate

StorageGRID uses an internal Certificate Authority (CA) to secure internal traffic. This certificate does not change if you upload your own certificates.

To export the internal CA certificate, copy all of the certificate text (starting with -----BEGIN CERTIFICATE and ending with END CERTIFICATE-----), and save it as a .pem file.



3. Fare clic con il pulsante destro del mouse sul testo selezionato e selezionare **Copia**.

4. Incollare il certificato copiato in un editor di testo.
5. Salvare il file con l'estensione `.pem`.

Ad esempio: `storagegrid_certificate.pem`

Configurazione dei certificati StorageGRID per FabricPool

Per i client S3 che eseguono una convalida rigorosa del nome host e non supportano la disattivazione della convalida rigorosa del nome host, ad esempio i client ONTAP che utilizzano FabricPool, è possibile generare o caricare un certificato server quando si configura l'endpoint del bilanciamento del carico.

Di cosa hai bisogno

- È necessario disporre di autorizzazioni di accesso specifiche.
- È necessario accedere a Grid Manager utilizzando un browser supportato.

A proposito di questa attività

Quando si crea un endpoint di bilanciamento 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 necessario utilizzare un certificato firmato da una CA nota. I certificati firmati da una CA possono essere ruotati senza interruzioni. Sono inoltre più sicuri perché offrono una migliore protezione contro gli attacchi man-in-the-middle.

La procedura riportata di seguito fornisce linee guida generali per i client S3 che utilizzano FabricPool. Per informazioni e procedure più dettagliate, consultare le istruzioni per la configurazione di StorageGRID per FabricPool.



Il servizio separato di bilanciamento del carico di connessione (CLB) sui nodi gateway è obsoleto e non è più consigliato per l'utilizzo con FabricPool.

Fasi

1. Facoltativamente, configurare un gruppo ad alta disponibilità (ha) da utilizzare per FabricPool.
2. Creare un endpoint di bilanciamento del carico S3 da utilizzare per FabricPool.

Quando si crea un endpoint di bilanciamento del carico HTTPS, viene richiesto di caricare il certificato del server, la chiave privata del certificato e il bundle CA.

3. Collega StorageGRID come Tier cloud in ONTAP.

Specificare la porta endpoint del bilanciamento del carico e il nome di dominio completo utilizzato nel certificato CA caricato. Quindi, fornire il certificato CA.



Se una CA intermedia ha emesso il certificato StorageGRID, è necessario fornire il certificato CA intermedio. Se il certificato StorageGRID è stato emesso direttamente dalla CA principale, è necessario fornire il certificato della CA principale.

Informazioni correlate

["Configurare StorageGRID per FabricPool"](#)

Creazione di un certificato server autofirmato per l'interfaccia di gestione

È possibile utilizzare uno script per generare un certificato server autofirmato per i client API di gestione che richiedono una convalida rigorosa del nome host.

Di cosa hai bisogno

- È necessario disporre di autorizzazioni di accesso specifiche.
- È necessario disporre di `Passwords.txt` file.

A proposito di questa attività

Negli ambienti di produzione, è necessario utilizzare un certificato firmato da un'autorità di certificazione nota (CA). I certificati firmati da una CA possono essere ruotati senza interruzioni. Sono inoltre più sicuri perché offrono una migliore protezione contro gli attacchi man-in-the-middle.

Fasi

1. Ottenere il nome di dominio completo (FQDN) di ciascun nodo di amministrazione.
2. Accedere al nodo di amministrazione principale:
 - a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
 - b. Immettere la password elencata in `Passwords.txt` file.
 - c. Immettere il seguente comando per passare a root: `su -`
 - d. Immettere la password elencata in `Passwords.txt` file.

Una volta effettuato l'accesso 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. Ad esempio, `*.ui.storagegrid.example.com` utilizza il carattere jolly `*` per rappresentare `admin1.ui.storagegrid.example.com` e `admin2.ui.storagegrid.example.com`.
- Impostare `--type` a `management` Per configurare il certificato 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. È possibile utilizzare `--days` argomento per eseguire l'override del periodo di validità predefinito.



Il periodo di validità di un certificato inizia quando `make-certificate` è eseguito. È necessario assicurarsi che il client API di gestione sia sincronizzato con la stessa origine temporale di StorageGRID; in caso contrario, il client potrebbe rifiutare il certificato.

```
$ sudo make-certificate --domains *.ui.storagegrid.example.com --type management --days 365
```

L'output risultante contiene il certificato pubblico necessario al client API di gestione.

4. Selezionare e copiare il certificato.

Includere i tag BEGIN e END nella selezione.

5. Disconnettersi dalla shell dei comandi. `$ exit`

6. Verificare che il certificato sia stato configurato:

a. Accedere a Grid Manager.

b. Selezionare **Configuration Server Certificates Management Interface Server Certificate**.

7. Configurare il client API di gestione in modo che utilizzi il certificato pubblico copiato. Includere i tag inizio e FINE.

Configurazione delle impostazioni del proxy di storage

Se si utilizzano servizi di piattaforma o Cloud Storage Pool, è possibile configurare un proxy non trasparente tra i nodi di storage e gli endpoint S3 esterni. Ad esempio, potrebbe essere necessario un proxy non trasparente per consentire l'invio dei messaggi dei servizi della piattaforma a endpoint esterni, ad esempio un endpoint su Internet.

Di cosa hai bisogno

- È necessario disporre di autorizzazioni di accesso specifiche.
- È necessario accedere a Grid Manager utilizzando un browser supportato.

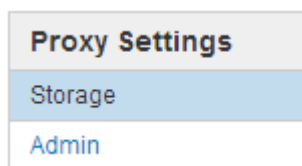
A proposito di questa attività

È possibile configurare le impostazioni per un singolo Storage Proxy.

Fasi

1. Selezionare **Configurazione Impostazioni di rete Impostazioni proxy**.

Viene visualizzata la pagina Storage Proxy Settings (Impostazioni proxy storage). Per impostazione predefinita, nel menu della barra laterale è selezionata l'opzione **Storage**.



2. Selezionare la casella di controllo **Enable Storage Proxy** (attiva proxy di storage).

Vengono visualizzati i campi per la configurazione di un proxy di storage.

Storage Proxy Settings

If you are using platform services or Cloud Storage Pools, you can configure a non-transparent proxy server between Storage Nodes and the external S3 endpoints.

Enable Storage Proxy

Protocol HTTP SOCKS5

Hostname

Port (optional)

3. Selezionare il protocollo per il proxy dello storage non trasparente.
4. Immettere il nome host o l'indirizzo IP del server proxy.
5. Facoltativamente, inserire la porta utilizzata per connettersi al server proxy.

È possibile lasciare vuoto questo campo se si utilizza la porta predefinita per il protocollo: 80 per HTTP o 1080 per SOCKS5.

6. Fare clic su **Save** (Salva).

Una volta salvato il proxy dello storage, è possibile configurare e testare i nuovi endpoint per i servizi della piattaforma o i pool di cloud storage.



Le modifiche del proxy possono richiedere fino a 10 minuti.

7. Controllare le impostazioni del server proxy per assicurarsi che i messaggi relativi al servizio della piattaforma da StorageGRID non vengano bloccati.

Al termine

Se è necessario disattivare un proxy di storage, deselezionare la casella di controllo **Enable Storage Proxy** (attiva proxy di storage) e fare clic su **Save** (Salva).

Informazioni correlate

["Networking e porte per i servizi della piattaforma"](#)

["Gestire gli oggetti con ILM"](#)

Configurazione delle impostazioni del proxy amministratore

Se si inviano messaggi AutoSupport utilizzando HTTP o HTTPS, è possibile configurare un server proxy non trasparente tra i nodi di amministrazione e il supporto tecnico (AutoSupport).

Di cosa hai bisogno

- È necessario disporre di autorizzazioni di accesso specifiche.
- È necessario accedere a Grid Manager utilizzando un browser supportato.

A proposito di questa attività

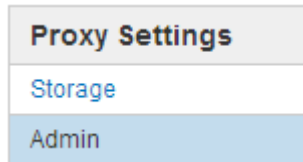
È possibile configurare le impostazioni per un singolo proxy Admin.

Fasi

1. Selezionare **Configurazione Impostazioni di rete Impostazioni proxy**.

Viene visualizzata la pagina Admin Proxy Settings (Impostazioni proxy amministratore). Per impostazione predefinita, nel menu della barra laterale è selezionata l'opzione **Storage**.

2. Dal menu della barra laterale, selezionare **Admin**.



3. Selezionare la casella di controllo **Enable Admin Proxy** (attiva proxy amministratore).

Admin Proxy Settings

If you send AutoSupport messages using HTTPS or HTTP, you can configure a non-transparent proxy server between Admin Nodes and technical support.

Enable Admin Proxy	<input checked="" type="checkbox"/>
Hostname	<input type="text" value="myproxy.example.com"/>
Port	<input type="text" value="8080"/>
Username (optional)	<input type="text" value="root"/>
Password (optional)	<input type="password" value="••••••"/>
<input type="button" value="Save"/>	

4. Immettere il nome host o l'indirizzo IP del server proxy.
5. Inserire la porta utilizzata per la connessione al server proxy.
6. Se si desidera, inserire il nome utente del proxy.

Lasciare vuoto questo campo se il server proxy non richiede un nome utente.

7. Se si desidera, inserire la password del proxy.

Lasciare vuoto questo campo se il server proxy non richiede una password.

8. Fare clic su **Save** (Salva).

Una volta salvato il proxy Admin, viene configurato il server proxy tra i nodi Admin e il supporto tecnico.



Le modifiche del proxy possono richiedere fino a 10 minuti.

9. Per disattivare il proxy, deselezionare la casella di controllo **Enable Admin Proxy** (attiva proxy amministratore) e fare clic su **Save** (Salva).

Informazioni correlate

["Specifica del protocollo per i messaggi AutoSupport"](#)

Gestione delle policy di classificazione del traffico

Per migliorare la qualità del servizio (QoS), è possibile creare policy di classificazione del traffico per identificare e monitorare diversi tipi di traffico di rete. Queste policy possono essere utili per la limitazione e il monitoraggio del traffico.

I criteri di classificazione del traffico vengono applicati agli endpoint del servizio bilanciamento del carico StorageGRID per i nodi gateway e i nodi di amministrazione. Per creare criteri di classificazione del traffico, è necessario aver già creato endpoint di bilanciamento del carico.

Regole corrispondenti e limiti opzionali

Ogni policy di classificazione del traffico contiene una o più regole corrispondenti per identificare il traffico di rete correlato a una o più delle seguenti entità:

- Bucket
- Tenant
- Subnet (subnet IPv4 contenente il client)
- Endpoint (endpoint del bilanciamento del carico)

StorageGRID monitora il traffico che corrisponde a qualsiasi regola all'interno del criterio in base agli obiettivi della regola. Qualsiasi traffico corrispondente a qualsiasi regola di un criterio viene gestito da tale criterio. Al contrario, è possibile impostare le regole in modo che corrispondano a tutto il traffico ad eccezione di un'entità specificata.

Facoltativamente, è possibile impostare limiti per una policy in base ai seguenti parametri:

- Larghezza di banda aggregata in
- Larghezza di banda aggregata in uscita
- Richieste di lettura simultanee
- Richieste di scrittura simultanee
- Larghezza di banda per richiesta in
- Larghezza di banda per richiesta in uscita
- Velocità richiesta di lettura
- Tasso di richieste di scrittura



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 di larghezza di banda aggregati potrebbero imporre un ulteriore impatto minore sulle performance sul traffico non limitato.

Limitazione del traffico

Una volta creati i criteri di classificazione del traffico, il traffico viene limitato in base al tipo di regole e limiti impostati. Per i limiti di larghezza di banda aggregati o per richiesta, le richieste vengono trasmesse in streaming alla velocità impostata. StorageGRID può applicare una sola velocità, quindi la corrispondenza di

policy più specifica, in base al tipo di matcher, è quella applicata. Per tutti gli altri tipi di limite, le richieste client vengono ritardate di 250 millisecondi e ricevono una risposta lenta di 503 per le richieste che superano qualsiasi limite di policy corrispondente.

In Grid Manager, è possibile visualizzare i diagrammi di traffico e verificare che i criteri stiano applicando i limiti di traffico previsti.

Utilizzo delle policy di classificazione del traffico con gli SLA

È possibile utilizzare le policy di classificazione del traffico insieme ai limiti di capacità e alla protezione dei dati per applicare gli SLA (Service-Level Agreement) che forniscono specifiche per capacità, protezione dei dati e performance.

I limiti di classificazione del traffico vengono implementati per bilanciamento del carico. Se il traffico viene distribuito simultaneamente tra più bilanciatori di carico, i tassi massimi totali sono un multiplo dei limiti di velocità specificati.

Nell'esempio riportato di seguito vengono illustrati tre livelli di uno SLA. È possibile creare criteri di classificazione del traffico per raggiungere gli obiettivi di performance di ciascun livello SLA.

Livello di servizio	Capacità	Protezione dei dati	Performance	Costo
Oro	1 PB di storage consentito	3 copia regola ILM	25 K richieste/sec Larghezza di banda di 5 GB/sec (40 Gbps)	€ al mese
Argento	250 TB di storage consentiti	2 copia regola ILM	10 K richieste/sec Larghezza di banda di 1.25 GB/sec (10 Gbps)	dollari al mese
Bronzo	100 TB di storage consentiti	2 copia regola ILM	5 K richieste/sec Larghezza di banda di 1 GB/sec (8 Gbps)	dollari al mese

Creazione di criteri di classificazione del traffico

È possibile creare criteri di classificazione del traffico se si desidera monitorare e, facoltativamente, limitare il traffico di rete per bucket, tenant, subnet IP o endpoint del bilanciamento del carico. Facoltativamente, è possibile impostare limiti per una policy in base alla larghezza di banda, al numero di richieste simultanee o alla velocità di richiesta.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre dell'autorizzazione di accesso root.
- È necessario aver creato tutti gli endpoint del bilanciamento del carico che si desidera associare.

- È necessario aver creato tutti i tenant che si desidera abbinare.

Fasi

1. Selezionare **Configurazione > Impostazioni di rete > classificazione del traffico**.

Viene visualizzata la pagina Criteri di classificazione del traffico.

Traffic Classification Policies

Traffic classification policies can be used to identify network traffic for metrics reporting and optional traffic limiting.


+ Create Edit Remove Metrics			
Name	Description	ID	
<i>No policies found.</i>			

2. Fare clic su **Create** (Crea).

Viene visualizzata la finestra di dialogo Crea policy di classificazione del traffico.

Create Traffic Classification Policy



Policy

Name 

Description

Matching Rules

Traffic that matches any rule is included in the policy.

Type	Inverse Match	Match Value
------	---------------	-------------

No matching rules found.

Limits (Optional)

Type	Value	Units
------	-------	-------

No limits found.

Cancel

Save

3. Nel campo **Nome**, immettere un nome per la policy.

Immettere un nome descrittivo per poter riconoscere il criterio.

4. Facoltativamente, aggiungere una descrizione per la policy nel campo **Descrizione**.

Ad esempio, descrivi a cosa si applica questa policy di classificazione del traffico e a cosa limiterà.

5. Creare una o più regole corrispondenti per il criterio.

Le regole corrispondenti controllano le entità interessate da questa policy di classificazione del traffico. Ad esempio, selezionare tenant se si desidera che questo criterio venga applicato al traffico di rete di un tenant specifico. In alternativa, selezionare Endpoint se si desidera applicare questo criterio al traffico di rete su un endpoint specifico del bilanciamento del carico.

- a. Fare clic su **Crea** nella sezione **regole corrispondenti**.

Viene visualizzata la finestra di dialogo Create Matching Rule (Crea regola corrispondente).

Create Matching Rule

Matching Rules

Type ⓘ -- Choose One -- ▾

Match Value ⓘ Choose type before providing match value

Inverse Match ⓘ

Cancel Apply

- b. Dal menu a discesa **Type**, selezionare il tipo di entità da includere nella regola di corrispondenza.
- c. Nel campo **valore di corrispondenza**, immettere un valore di corrispondenza in base al tipo di entità scelta.

- Bucket (bucket): Immettere il nome di un bucket.
- Bucket Regex (Regex bucket): Immettere un'espressione regolare che verrà utilizzata per far corrispondere un set di nomi di bucket.

L'espressione regolare non è ancorata. Utilizzare l'ancora `^` per trovare la corrispondenza all'inizio del nome del bucket e utilizzare l'ancora `$` per la corrispondenza alla fine del nome.

- CIDR: Immettere una subnet IPv4, nella notazione CIDR, che corrisponda alla subnet desiderata.
 - Endpoint: Selezionare un endpoint dall'elenco degli endpoint esistenti. Questi sono gli endpoint del bilanciamento del carico definiti nella pagina endpoint del bilanciamento del carico.
 - Tenant (tenant): Selezionare un tenant dall'elenco dei tenant esistenti. L'abbinamento dei tenant si basa sulla proprietà del bucket a cui si accede. L'accesso anonimo a un bucket corrisponde al tenant proprietario del bucket.
- d. Se si desidera far corrispondere tutto il traffico di rete *tranne* corrispondente al valore Type and Match appena definito, selezionare la casella di controllo **Inverse**. In caso contrario, lasciare deselezionata la casella di controllo.

Ad esempio, se si desidera che questo criterio venga applicato a tutti gli endpoint del bilanciamento del carico tranne uno, specificare l'endpoint del bilanciamento del carico da escludere e selezionare **inverso**.



Per un criterio contenente più adattatori in cui almeno uno è un adattatore inverso, fare attenzione a non creare un criterio che corrisponda a tutte le richieste.

- e. Fare clic su **Apply** (Applica).

La regola viene creata ed elencata nella tabella regole corrispondenti.

+ Create Edit Remove		
Type	Inverse Match	Match Value
Bucket Regex	✓	control-ld+


Displaying 1 matching rule.

Limits (Optional)


+ Create Edit Remove			
Type	Value	Type	Units
No limits found.			

Cancel Save

a. Ripetere questi passaggi per ogni regola che si desidera creare per il criterio.

 Il traffico che corrisponde a qualsiasi regola viene gestito dal criterio.

6. Facoltativamente, creare limiti per la policy.



 Anche se non si creano limiti, StorageGRID raccoglie le metriche in modo da poter monitorare il traffico di rete corrispondente alla policy.


a. Fare clic su **Crea** nella sezione **limiti**.


Viene visualizzata la finestra di dialogo Create Limit (Crea limite).

Create Limit

Limits (Optional)

Type  

Aggregate rate limits in use. Per-request rate limits are not available. 

Value 

Cancel Apply

b. Nell'elenco a discesa **tipo**, selezionare il tipo di limite che si desidera applicare al criterio.

Nell'elenco seguente, **in** si riferisce al traffico dai client S3 o Swift al bilanciamento del carico StorageGRID, mentre **out** si riferisce al traffico dal bilanciamento del carico ai client S3 o Swift.

- Larghezza di banda aggregata in
- Larghezza di banda aggregata in uscita
- Richieste di lettura simultanee
- Richieste di scrittura simultanee
- Larghezza di banda per richiesta in
- Larghezza di banda per richiesta in uscita
- Velocità richiesta di lettura
- Tasso di richieste di scrittura



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 di larghezza di banda aggregati potrebbero imporre un ulteriore impatto minore sulle performance sul 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 il traffico corrisponde a criteri aggiuntivi con limiti di larghezza di banda. StorageGRID implementa le corrispondenze “Best” per i limiti di larghezza di banda nel seguente ordine:

- Indirizzo IP esatto (/32 mask)
- Nome esatto del bucket
- Regex. Bucket
- Tenant
- Endpoint
- Corrispondenze CIDR non esatte (non /32)
- Corrispondenze inverse

c. Nel campo **valore**, immettere un valore numerico per il tipo di limite scelto.

Le unità previste vengono visualizzate quando si seleziona un limite.

d. Fare clic su **Apply** (Applica).

Il limite viene creato ed è elencato nella tabella dei limiti.

Type	Inverse Match	Match Value
<input checked="" type="radio"/> Bucket Regex	<input checked="" type="checkbox"/>	control-ld+

Displaying 1 matching rule.

Limits (Optional)

Type	Value	Units
<input checked="" type="radio"/> Aggregate Bandwidth Out	10000000000	Bytes/Second

Displaying 1 limit.

Cancel Save

e. Ripetere questi passaggi per ciascun limite che si desidera aggiungere al criterio.

Ad esempio, se si desidera creare un limite di larghezza di banda di 40 Gbps per un livello SLA, creare un limite di larghezza di banda aggregata in limite e un limite di larghezza di banda aggregato in uscita e impostare ciascuno su 40 Gbps.



Per convertire megabyte al secondo in gigabit al secondo, moltiplicare per otto. Ad esempio, 125 MB/s equivale a 1,000 Mbps o 1 Gbps.

7. Al termine della creazione di regole e limiti, fare clic su **Save** (Salva).

La policy viene salvata ed è elencata nella tabella Traffic Classification Policies (Criteri di classificazione del traffico).

Traffic Classification Policies

Traffic classification policies can be used to identify network traffic for metrics reporting and optional traffic limiting.

Name	Description	ID
<input type="radio"/> ERP Traffic Control	Manage ERP traffic into the grid	cd9afbc7-b85e-4208-b6f8-7e8a79e2c574
<input checked="" type="radio"/> Fabric Pools	Monitor Fabric Pools	223b0cbb-6968-4646-b32d-7665bddc894b

Displaying 2 traffic classification policies.

Il traffico dei client S3 e Swift viene ora gestito in base alle policy di classificazione del traffico. È possibile visualizzare i diagrammi di traffico e verificare che i criteri stiano applicando i limiti di traffico previsti.

Informazioni correlate

["Gestione del bilanciamento del carico"](#)

"Visualizzazione delle metriche del traffico di rete"

Modifica di una policy di classificazione del traffico

È possibile modificare un criterio di classificazione del traffico per modificarne il nome o la descrizione oppure per creare, modificare o eliminare eventuali regole o limiti per il criterio.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre dell'autorizzazione di accesso root.

Fasi

1. Selezionare **Configurazione > Impostazioni di rete > classificazione del traffico**.

Viene visualizzata la pagina Traffic Classification Policies (Criteri di classificazione del traffico) e i criteri esistenti sono elencati nella tabella.

Traffic Classification Policies

Traffic classification policies can be used to identify network traffic for metrics reporting and optional traffic limiting.

	Name	Description	ID
<input type="radio"/>	ERP Traffic Control	Manage ERP traffic into the grid	cd9afbc7-b85e-4208-b6f8-7e8a79e2c574
<input checked="" type="radio"/>	Fabric Pools	Monitor Fabric Pools	223b0cbb-6968-4646-b32d-7665bdc894b

Displaying 2 traffic classification policies.

2. Selezionare il pulsante di opzione a sinistra del criterio che si desidera modificare.
3. Fare clic su **Edit** (Modifica).

Viene visualizzata la finestra di dialogo Modifica policy di classificazione del traffico.

Edit Traffic Classification Policy "Fabric Pools"

Policy

Name 

Fabric Pools

Description (optional)

Monitor Fabric Pools

Matching Rules

Traffic that matches any rule is included in the policy.

 Create	 Edit	 Remove
Type	Inverse Match	Match Value
<input checked="" type="checkbox"/> CIDR		10.10.152.0/24
Displaying 1 matching rule.		

Limits (Optional)

 Create	 Edit	 Remove
Type	Value	Units
No limits found.		

Cancel

Save

4. Creare, modificare o rimuovere regole e limiti corrispondenti in base alle esigenze.
 - a. Per creare una regola o un limite corrispondente, fare clic su **Crea** e seguire le istruzioni per creare una regola o un limite.
 - b. Per modificare una regola o un limite corrispondente, selezionare il pulsante di opzione corrispondente alla regola o al limite, fare clic su **Edit** nella sezione **Matching Rules** (regole corrispondenti) o nella sezione **Limits** (limiti) e seguire le istruzioni per creare una regola o un limite.
 - c. Per rimuovere una regola o un limite corrispondente, selezionare il pulsante di opzione corrispondente alla regola o al limite e fare clic su **Rimuovi**. Quindi, fare clic su **OK** per confermare che si desidera rimuovere la regola o il limite.
5. Una volta creata o modificata una regola o un limite, fare clic su **Apply** (Applica).
6. Una volta terminata la modifica del criterio, fare clic su **Save** (Salva).

Le modifiche apportate alla policy vengono salvate e il traffico di rete viene gestito in base alle policy di classificazione del traffico. È possibile visualizzare i diagrammi di traffico e verificare che i criteri stiano applicando i limiti di traffico previsti.

Eliminazione di una policy di classificazione del traffico

Se non è più necessario un criterio di classificazione del traffico, è possibile eliminarlo.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre dell'autorizzazione di accesso root.

Fasi

1. Selezionare **Configurazione > Impostazioni di rete > classificazione del traffico**.

Viene visualizzata la pagina Traffic Classification Policies (Criteri di classificazione del traffico) e i criteri esistenti sono elencati nella tabella.

Traffic Classification Policies

Traffic classification policies can be used to identify network traffic for metrics reporting and optional traffic limiting.

Name	Description	ID
<input type="radio"/> ERP Traffic Control	Manage ERP traffic into the grid	cd9afbc7-b85e-4208-b6f8-7e8a79e2c574
<input checked="" type="radio"/> Fabric Pools	Monitor Fabric Pools	223b0cbb-6968-4646-b32d-7665bdc894b

Displaying 2 traffic classification policies.

2. Selezionare il pulsante di opzione a sinistra del criterio che si desidera eliminare.
3. Fare clic su **Rimuovi**.

Viene visualizzata la finestra di dialogo Avviso.



4. Fare clic su **OK** per confermare che si desidera eliminare il criterio.

La policy viene eliminata.

Visualizzazione delle metriche del traffico di rete

È possibile monitorare il traffico di rete visualizzando i grafici disponibili nella pagina Traffic Classification Policies (Criteri di classificazione del traffico).

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.

- È necessario disporre dell'autorizzazione di accesso root.

A proposito di questa attività

Per qualsiasi criterio di classificazione del traffico esistente, è possibile visualizzare le metriche per il servizio Load Balancer per determinare se il criterio limita correttamente il traffico nella rete. I dati nei grafici possono aiutare a determinare se è necessario modificare la policy.

Anche se non vengono impostati limiti per una policy di classificazione del traffico, vengono raccolte le metriche e i grafici forniscono informazioni utili per comprendere le tendenze del traffico.

Fasi

1. Selezionare **Configurazione > Impostazioni di rete > classificazione del traffico**.

Viene visualizzata la pagina Traffic Classification Policies (Criteri di classificazione del traffico) e i criteri esistenti sono elencati nella tabella.

Traffic Classification Policies

Traffic classification policies can be used to identify network traffic for metrics reporting and optional traffic limiting.

<input type="button" value="+ Create"/> <input type="button" value="✎ Edit"/> <input type="button" value="✕ Remove"/> <input type="button" value="📊 Metrics"/>			
	Name	Description	ID
<input type="radio"/>	ERP Traffic Control	Manage ERP traffic into the grid	cd9afbc7-b85e-4208-b6f8-7e8a79e2c574
<input checked="" type="radio"/>	Fabric Pools	Monitor Fabric Pools	223b0cbb-6968-4646-b32d-7665bdc894b

Displaying 2 traffic classification policies.

2. Selezionare il pulsante di opzione a sinistra della policy per la quale si desidera visualizzare le metriche.
3. Fare clic su **metriche**.

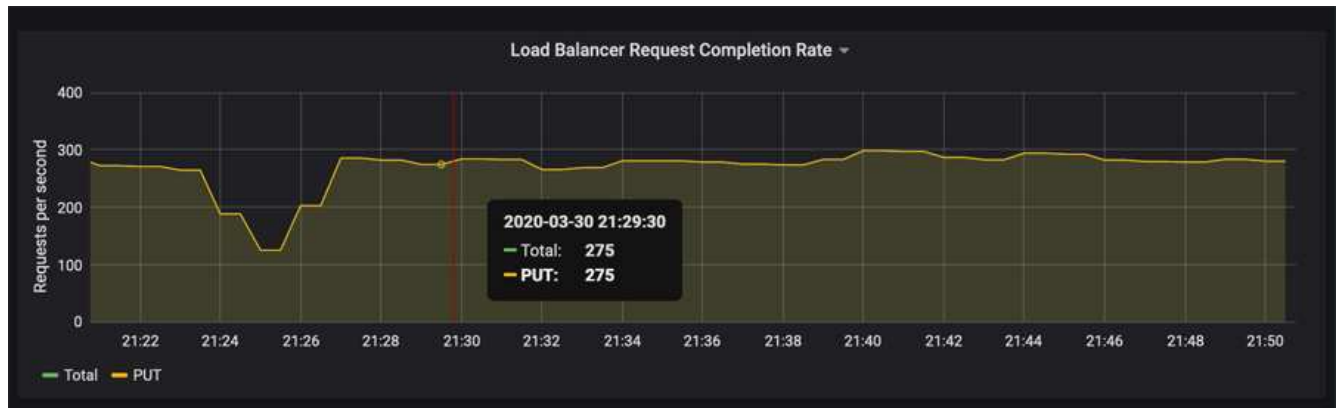
Viene visualizzata una nuova finestra del browser e i grafici della policy di classificazione del traffico. I grafici visualizzano le metriche solo per il traffico corrispondente al criterio selezionato.

È possibile selezionare altri criteri da visualizzare utilizzando l'elenco a discesa **policy**.

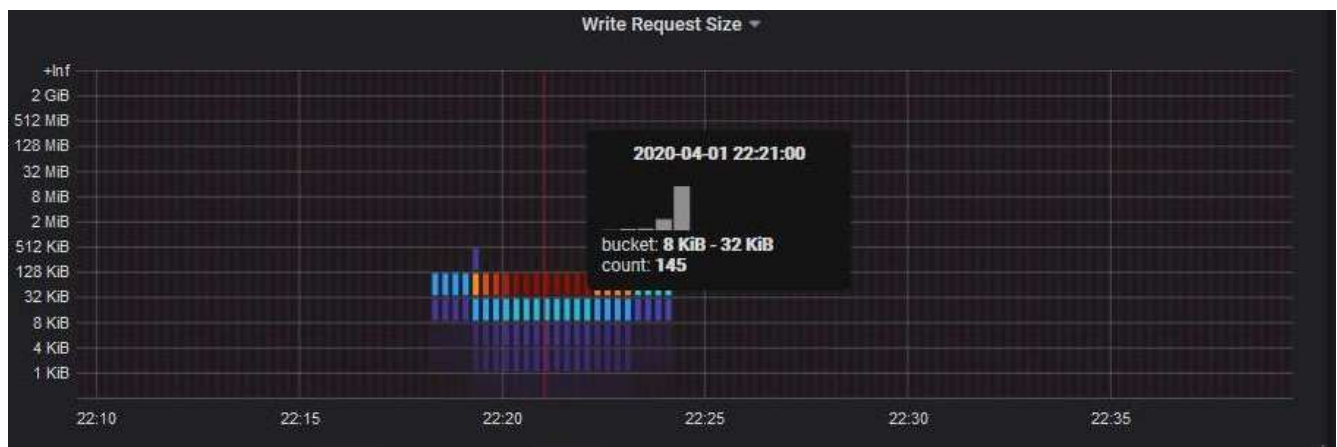


I grafici seguenti sono inclusi nella pagina Web.

- **Load Balancer Request Traffic:** Questo grafico fornisce una media mobile di 3 minuti del throughput dei dati trasmessi tra gli endpoint del bilanciamento del carico e i client che eseguono le richieste, in bit al secondo.
 - **Tasso di completamento della richiesta di bilanciamento del carico:** Questo grafico fornisce una media mobile di 3 minuti del numero di richieste completate al secondo, suddiviso per tipo di richiesta (GET, PUT, HEAD e DELETE). Questo valore viene aggiornato quando le intestazioni di una nuova richiesta sono state convalidate.
 - **Tasso di risposta agli errori:** Questo grafico fornisce una media mobile di 3 minuti del numero di risposte agli errori restituite ai client al secondo, suddiviso per codice di risposta agli errori.
 - **Durata media della richiesta (non errore):** Questo grafico fornisce una media mobile di 3 minuti delle durate della richiesta, suddivisa per tipo di richiesta (GET, PUT, HEAD e DELETE). Ogni durata della richiesta inizia quando un'intestazione di richiesta viene analizzata dal servizio Load Balancer e termina quando il corpo di risposta completo viene restituito al client.
 - **Write Request Rate by Object Size (velocità di richiesta di scrittura per dimensione oggetto):** Questa mappa termica fornisce una media mobile di 3 minuti della velocità di completamento delle richieste di scrittura in base alle dimensioni dell'oggetto. In questo contesto, le richieste di scrittura si riferiscono solo alle richieste PUT.
 - **Read Request Rate by Object Size (velocità richiesta di lettura per dimensione oggetto):** Questa mappa termica fornisce una media mobile di 3 minuti della velocità di completamento delle richieste di lettura in base alle dimensioni dell'oggetto. In questo contesto, le richieste di lettura si riferiscono solo alle richieste GET. I colori nella mappa termica indicano la frequenza relativa delle dimensioni di un oggetto all'interno di un singolo grafico. I colori più freddi (ad esempio, viola e blu) indicano tassi relativi inferiori, mentre i colori più caldi (ad esempio, arancione e rosso) indicano tassi relativi più elevati.
4. Posizionare il cursore su un grafico a linee per visualizzare una finestra a comparsa di valori su una parte specifica del grafico.



5. Spostare il cursore su una mappa termica per visualizzare una finestra a comparsa che mostra la data e l'ora del campione, le dimensioni degli oggetti aggregati nel conteggio e il numero di richieste al secondo durante tale periodo di tempo.



6. Utilizzare l'elenco a discesa **Policy** in alto a sinistra per selezionare un criterio diverso.

Vengono visualizzati i grafici relativi al criterio selezionato.

7. In alternativa, accedere ai grafici dal menu **supporto**.

- a. Selezionare **supporto Strumenti metriche**.
- b. Nella sezione **Grafana** della pagina, selezionare **Traffic Classification Policy**.
- c. Selezionare il criterio dall'elenco a discesa in alto a sinistra nella pagina.

Le policy di classificazione del traffico sono identificate dal loro ID. Gli ID policy sono elencati nella pagina Traffic Classification Policies.

8. Analizzare i grafici per determinare la frequenza con cui il criterio limita il traffico e se è necessario modificare il criterio.

Informazioni correlate

["Monitor risoluzione dei problemi"](#)

Quali sono i costi di collegamento

I costi di collegamento consentono di assegnare la priorità al sito del data center che fornisce un servizio richiesto quando esistono due o più siti del data center. È possibile

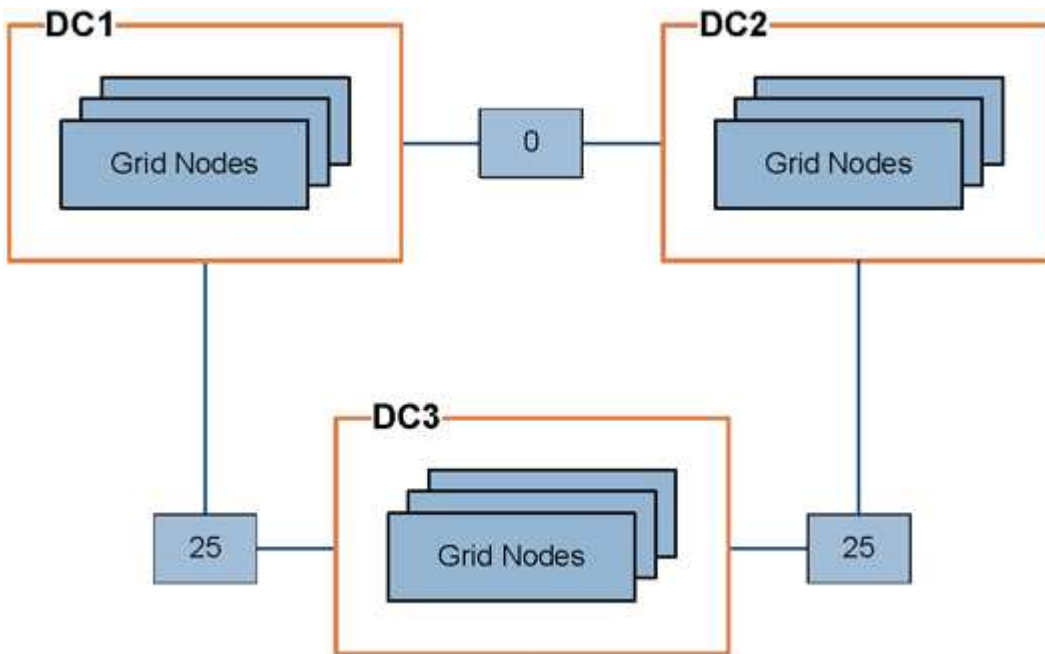
regolare i costi di collegamento in modo da riflettere la latenza tra i siti.

- I costi di collegamento vengono utilizzati per assegnare la priorità alla copia oggetto utilizzata per soddisfare i recuperi di oggetti.
- I costi di collegamento vengono utilizzati dall'API di gestione del grid e dall'API di gestione del tenant per determinare i servizi StorageGRID interni da utilizzare.
- I costi di collegamento vengono utilizzati dal servizio CLB sui nodi gateway per indirizzare le connessioni client.



Il servizio CLB è obsoleto.

Il diagramma mostra una griglia a tre siti con costi di collegamento configurati tra i siti:



- Il servizio CLB sui nodi gateway distribuisce in modo uguale le connessioni client a tutti i nodi di storage nello stesso sito del data center e a qualsiasi sito del data center con un costo di collegamento pari a 0.

Nell'esempio, un nodo gateway nel sito 1 del data center (DC1) distribuisce in modo uguale le connessioni client ai nodi di storage in DC1 e ai nodi di storage in DC2. Un nodo gateway in DC3 invia le connessioni client solo ai nodi di storage in DC3.

- Quando si recupera un oggetto che esiste come copie replicate multiple, StorageGRID recupera la copia nel data center che ha il costo di collegamento più basso.

Nell'esempio, se un'applicazione client in DC2 recupera un oggetto memorizzato sia in DC1 che in 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 di collegamento sono numeri relativi arbitrari senza unità di misura specifica. Ad esempio, un costo di collegamento di 50 viene utilizzato in modo meno preferenziale rispetto a un costo di collegamento di 25. La tabella mostra i costi di collegamento comunemente utilizzati.

Collegamento	Costo del collegamento	Note
Tra siti fisici di data center	25 (impostazione predefinita)	Data center connessi tramite un collegamento WAN.
Tra i siti del data center logico nella stessa posizione fisica	0	Data center logici nello stesso edificio fisico o campus connessi da una LAN.

Informazioni correlate

["Come funziona il bilanciamento del carico - servizio CLB"](#)

Aggiornamento dei costi di collegamento

È possibile aggiornare i costi di collegamento tra i siti del data center per riflettere la latenza tra i siti.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre dell'autorizzazione Grid Topology Page Configuration (Configurazione pagina topologia griglia).

Fasi

1. Selezionare **Configurazione Impostazioni di rete costo collegamento**.

Link Cost
Updated: 2021-03-29 12:28:41 EDT

Site Names (1 - 2 of 2)

Site ID	Site Name	Actions
10	Data Center 1	
20	Data Center 2	

Show 50 Records Per Page Previous « 1 » Next

Link Costs

Link Source	Link Destination	Actions
10	20	

2. Selezionare un sito in **link Source** (origine collegamento) e immettere un valore di costo compreso tra 0 e 100 in **link Destination** (destinazione collegamento).

Non è possibile modificare il costo del collegamento se l'origine è la stessa della destinazione.

Per annullare le modifiche, fare clic su **Ripristina**.

3. Fare clic su **Applica modifiche**.

Configurazione di AutoSupport

La funzione AutoSupport consente al sistema StorageGRID di inviare messaggi di stato e di stato al supporto tecnico. L'utilizzo di AutoSupport può accelerare notevolmente la determinazione e la risoluzione dei problemi. Il supporto tecnico può anche monitorare le esigenze di storage del sistema e aiutare a determinare se è necessario aggiungere nuovi nodi o siti. In alternativa, è possibile configurare i messaggi AutoSupport in modo che vengano inviati a una destinazione aggiuntiva.

Informazioni incluse nei messaggi AutoSupport


I messaggi AutoSupport includono informazioni quali:

- Versione del software StorageGRID
- Versione del sistema operativo
- Informazioni sugli attributi a livello di sistema e di posizione
- Avvisi e allarmi recenti (sistema legacy)
- Stato corrente di tutte le attività della griglia, inclusi i dati storici
- Informazioni sugli eventi elencate nella pagina **nodi nodo griglia Eventi**
- Utilizzo del database Admin Node
- Numero di oggetti persi o mancanti
- Impostazioni di configurazione della griglia
- Entità NMS
- Policy ILM attiva
- File delle specifiche della griglia con provisioning
- Metriche diagnostiche

È possibile attivare la funzione AutoSupport e le singole opzioni AutoSupport quando si installa StorageGRID per la prima volta oppure attivarle in un secondo momento. Se AutoSupport non è attivato, viene visualizzato un messaggio sul dashboard di gestione della griglia. Il messaggio include un collegamento alla pagina di configurazione di AutoSupport.

The AutoSupport feature is disabled. You should enable AutoSupport to allow StorageGRID to send health and status messages to technical support for proactive monitoring and troubleshooting.



È possibile selezionare il simbolo "X"  per chiudere il messaggio. Il messaggio non viene visualizzato fino a quando la cache del browser non viene cancellata, anche se AutoSupport rimane disattivato.

Utilizzando Active IQ

Active IQ è un consulente digitale basato sul cloud che sfrutta l'analisi predittiva e la saggezza della community della base installata di NetApp. Le valutazioni continue dei rischi, gli avvisi predittivi, le indicazioni

prescrittive e le azioni automatizzate consentono di prevenire i problemi prima che si verifichino, migliorando lo stato di salute del sistema e la disponibilità del sistema.

Se si desidera utilizzare le dashboard e le funzionalità di Active IQ sul sito del supporto, è necessario attivare AutoSupport.

["Documentazione di Active IQ Digital Advisor"](#)

Accesso alle impostazioni AutoSupport

Si configura AutoSupport utilizzando Gestione griglia (**supporto Strumenti AutoSupport**). La pagina **AutoSupport** contiene due schede: **Impostazioni** e **risultati**.

AutoSupport

The AutoSupport feature enables your StorageGRID system to send periodic and event-driven health and status messages to technical support to allow proactive monitoring and troubleshooting. StorageGRID AutoSupport also enables the use of Active IQ for predictive recommendations.

The screenshot shows the configuration interface for AutoSupport. At the top, there are two tabs: "Settings" (selected) and "Results". Below the tabs is a section titled "Protocol Details" with a sub-header "Protocol" and three radio button options: "HTTPS" (selected), "HTTP", and "SMTP". Below this is a dropdown menu for "NetApp Support Certificate Validation" with the selected option "Use NetApp support certificate". The next section is "AutoSupport Details" with three checkboxes: "Enable Weekly AutoSupport" (checked), "Enable Event-Triggered AutoSupport" (checked), and "Enable AutoSupport on Demand" (unchecked). Below this is "Additional AutoSupport Destination" with a checkbox "Enable Additional AutoSupport Destination" (unchecked). At the bottom, there are two buttons: "Save" and "Send User-Triggered AutoSupport".

Protocolli per l'invio di messaggi AutoSupport

È possibile scegliere uno dei tre protocolli per l'invio dei messaggi AutoSupport:

- HTTPS
- HTTP
- SMTP

Se si inviano messaggi AutoSupport utilizzando HTTPS o HTTP, è possibile configurare un server proxy non trasparente tra i nodi di amministrazione e il supporto tecnico.

Se si utilizza SMTP come protocollo per i messaggi AutoSupport, è necessario configurare un server di posta SMTP.

Opzioni AutoSupport

È possibile utilizzare qualsiasi combinazione delle seguenti opzioni per inviare messaggi AutoSupport al supporto tecnico:

- **Settimanale:** Invia automaticamente i messaggi AutoSupport una volta alla settimana. Impostazione predefinita: Enabled (attivato).
- **Evento attivato:** Invia automaticamente i messaggi AutoSupport ogni ora o quando si verificano eventi di sistema significativi. Impostazione predefinita: Enabled (attivato).
- **Su richiesta:** Consente al supporto tecnico di richiedere che il sistema StorageGRID invii automaticamente messaggi AutoSupport, utile quando si verifica un problema (richiede il protocollo di trasmissione HTTPS AutoSupport). Impostazione predefinita: Disattivata.
- **Attivato dall'utente:** Consente di inviare manualmente i messaggi AutoSupport in qualsiasi momento.

Informazioni correlate

["Supporto NetApp"](#)

Specifica del protocollo per i messaggi AutoSupport

È possibile utilizzare uno dei tre protocolli per l'invio di messaggi AutoSupport.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre dell'autorizzazione Root Access o Other Grid Configuration.
- Se si utilizza il protocollo HTTPS o HTTP per l'invio di messaggi AutoSupport, è necessario aver fornito l'accesso a Internet in uscita al nodo di amministrazione primario, direttamente o utilizzando un server proxy (non sono richieste connessioni in entrata).
- Se si utilizza il protocollo HTTPS o HTTP e si desidera utilizzare un server proxy, è necessario aver configurato un server proxy Admin.
- Se si utilizza SMTP come protocollo per i messaggi AutoSupport, è necessario aver configurato un server di posta SMTP. La stessa configurazione del server di posta viene utilizzata per le notifiche e-mail di allarme (sistema legacy).

A proposito di questa attività

I messaggi AutoSupport possono essere inviati utilizzando uno dei seguenti protocolli:

- **HTTPS:** Impostazione predefinita e consigliata per le nuove installazioni. Il protocollo HTTPS utilizza la porta 443. Se si desidera attivare la funzione AutoSupport on Demand, è necessario utilizzare il protocollo HTTPS.
- **HTTP:** Questo protocollo non è sicuro, a meno che non venga utilizzato in un ambiente attendibile in cui il server proxy converte in HTTPS durante l'invio di dati su Internet. Il protocollo HTTP utilizza la porta 80.
- **SMTP:** Utilizzare questa opzione se si desidera che i messaggi AutoSupport vengano inviati tramite e-mail. Se si utilizza il protocollo SMTP come protocollo per i messaggi AutoSupport, è necessario configurare un server di posta SMTP nella pagina Configurazione posta elettronica legacy (**supporto Allarmi (legacy) Configurazione posta elettronica legacy**).



SMTP era l'unico protocollo disponibile per i messaggi AutoSupport prima della release di StorageGRID 11.2. Se inizialmente è stata installata una versione precedente di StorageGRID, il protocollo selezionato potrebbe essere SMTP.

Il protocollo impostato viene utilizzato per l'invio di tutti i tipi di messaggi AutoSupport.

Fasi

1. Selezionare **supporto Strumenti AutoSupport**.

Viene visualizzata la pagina AutoSupport (Impostazioni) e viene selezionata la scheda **Settings** (Impostazioni).

2. Selezionare il protocollo che si desidera utilizzare per inviare messaggi AutoSupport.

The screenshot shows the 'Settings' tab selected. Under 'Protocol Details', the 'Protocol' is set to 'HTTPS'. The 'NetApp Support Certificate Validation' dropdown menu is open, showing three options: 'Use NetApp support certificate' (selected), 'Use NetApp support certificate', and 'Do not verify certificate'. Below this, there are checkboxes for 'Enable Weekly AutoSupport', 'Enable Event-Triggered AutoSupport', and 'Enable AutoSupport on Demand'. At the bottom, there are buttons for 'Save' and 'Send User-Triggered AutoSupport'.

3. Seleziona la tua scelta per **NetApp Support Certificate Validation**.

- USA certificato di supporto NetApp (impostazione predefinita): La convalida del certificato garantisce la sicurezza della trasmissione dei messaggi AutoSupport. Il certificato di supporto NetApp è già installato con il software StorageGRID.
- Non verificare il certificato: Selezionare questa opzione solo se si dispone di un buon motivo per non utilizzare la convalida del certificato, ad esempio quando si verifica un problema temporaneo con un certificato.

4. Selezionare **Salva**.

Tutti i messaggi settimanali, attivati dall'utente e attivati dagli eventi vengono inviati utilizzando il protocollo selezionato.

Informazioni correlate

["Configurazione delle impostazioni del proxy amministratore"](#)

Abilitazione di AutoSupport on-demand

AutoSupport on Demand può aiutare a risolvere i problemi sui quali il supporto tecnico sta lavorando attivamente. Attivando AutoSupport on Demand, il supporto tecnico può richiedere l'invio di messaggi AutoSupport senza richiedere alcun intervento da parte

dell'utente.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre dell'autorizzazione Root Access o Other Grid Configuration.
- È necessario aver attivato i messaggi AutoSupport settimanali.
- È necessario impostare il protocollo di trasporto su HTTPS.

A proposito di questa attività

Quando si attiva questa funzione, il supporto tecnico può richiedere che il sistema StorageGRID invii automaticamente messaggi AutoSupport. Il supporto tecnico può anche impostare l'intervallo di tempo di polling per le query AutoSupport on Demand.

Il supporto tecnico non può attivare o disattivare AutoSupport on Demand.

Fasi

1. Selezionare **supporto Strumenti AutoSupport**.

Viene visualizzata la pagina AutoSupport (Impostazioni) con la scheda **Settings** (Impostazioni) selezionata.

2. Selezionare il pulsante di opzione HTTPS nella sezione **Protocol Details** (Dettagli protocollo) della pagina.

The screenshot shows the 'Settings' tab of the AutoSupport configuration page. The 'Protocol Details' section has three radio buttons: 'HTTPS' (selected and highlighted), 'HTTP', and 'SMTP'. Below this is a dropdown menu for 'NetApp Support Certificate Validation' set to 'Use NetApp support certificate'. The 'AutoSupport Details' section contains three checkboxes: 'Enable Weekly AutoSupport' (checked and highlighted), 'Enable Event-Triggered AutoSupport' (unchecked), and 'Enable AutoSupport on Demand' (checked and highlighted). The 'Additional AutoSupport Destination' checkbox is unchecked. At the bottom, there are two buttons: 'Save' and 'Send User-Triggered AutoSupport'.

3. Selezionare la casella di controllo **Enable Weekly AutoSupport** (attiva impostazioni settimanali).
4. Selezionare la casella di controllo **attiva AutoSupport su richiesta**.
5. Selezionare **Salva**.

AutoSupport on Demand è attivato e il supporto tecnico può inviare richieste AutoSupport on Demand a StorageGRID.

Disattivazione dei messaggi AutoSupport settimanali

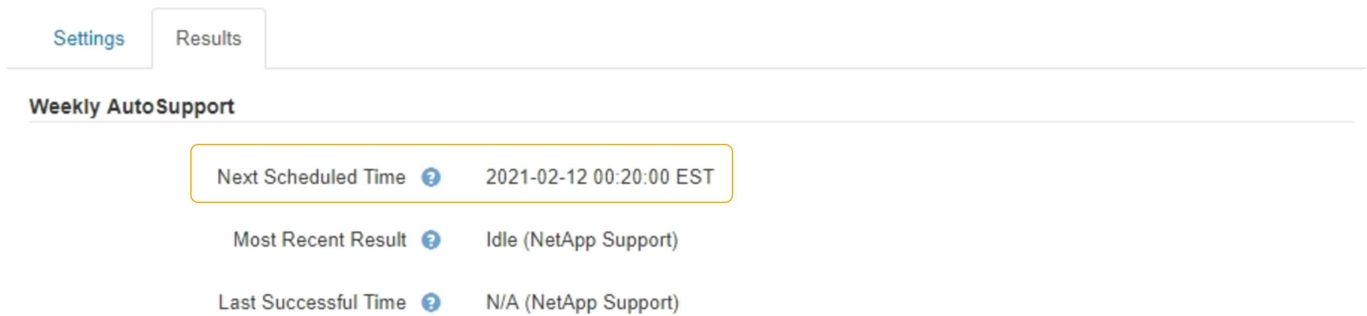
Per impostazione predefinita, il sistema StorageGRID è configurato per inviare un messaggio AutoSupport al supporto NetApp una volta alla settimana.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre dell'autorizzazione Root Access o Other Grid Configuration.

A proposito di questa attività

Per determinare quando viene inviato il messaggio AutoSupport settimanale, consultare la sezione **prossima ora pianificata** in **AutoSupport settimanale** nella pagina **AutoSupport risultati**.



The screenshot shows a web interface with two tabs: 'Settings' (selected) and 'Results'. Below the tabs is a section titled 'Weekly AutoSupport'. It contains three rows of information, each with a label, a help icon, and a value:

Next Scheduled Time	?	2021-02-12 00:20:00 EST
Most Recent Result	?	Idle (NetApp Support)
Last Successful Time	?	N/A (NetApp Support)

È possibile disattivare l'invio automatico di un messaggio AutoSupport in qualsiasi momento.

Fasi

1. Selezionare **supporto Strumenti AutoSupport**.

Viene visualizzata la pagina AutoSupport (Impostazioni) con la scheda **Settings** (Impostazioni) selezionata.

2. Deselezionare la casella di controllo **attiva AutoSupport settimanale**.

Settings
Results

Protocol Details

Protocol ? HTTPS HTTP SMTP

NetApp Support Certificate Validation ? Use NetApp support certificate ▼

AutoSupport Details

Enable Weekly AutoSupport ?

Enable Event-Triggered AutoSupport ?

AutoSupport On Demand can only be enabled when the protocol is HTTPS and Weekly AutoSupport is enabled. When you enable AutoSupport on Demand, technical support can request that your StorageGRID system send AutoSupport messages automatically.

Additional AutoSupport Destination

Enable Additional AutoSupport Destination ?

Save
Send User-Triggered AutoSupport

3. Selezionare **Salva**.

Disattivazione dei messaggi AutoSupport attivati dagli eventi

Per impostazione predefinita, il sistema StorageGRID è configurato per inviare un messaggio AutoSupport al supporto NetApp quando si verifica un avviso importante o un altro evento significativo del sistema.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre dell'autorizzazione Root Access o Other Grid Configuration.

A proposito di questa attività

È possibile disattivare i messaggi AutoSupport attivati da eventi in qualsiasi momento.



I messaggi AutoSupport attivati dagli eventi vengono eliminati anche quando si sopprimono le notifiche e-mail a livello di sistema. (Selezionare **Configurazione Impostazioni di sistema Opzioni di visualizzazione**. Quindi, selezionare **Notification Sopprimi tutto**.)

Fasi

1. Selezionare **supporto Strumenti AutoSupport**.

Viene visualizzata la pagina AutoSupport (Impostazioni) con la scheda **Settings** (Impostazioni) selezionata.

2. Deselezionare la casella di controllo **attiva AutoSupport attivato da eventi**.

Settings
Results

Protocol Details

Protocol ? HTTPS HTTP SMTP

NetApp Support Certificate Validation ? Use NetApp support certificate ▼

AutoSupport Details

Enable Weekly AutoSupport ?

Enable Event-Triggered AutoSupport ?

AutoSupport On Demand can only be enabled when the protocol is HTTPS and Weekly AutoSupport is enabled. When you enable AutoSupport on Demand, technical support can request that your StorageGRID system send AutoSupport messages automatically.

Additional AutoSupport Destination

Enable Additional AutoSupport Destination ?

Save
Send User-Triggered AutoSupport

3. Selezionare **Salva**.

Attivazione manuale di un messaggio AutoSupport

Per assistere il supporto tecnico nella risoluzione dei problemi relativi al sistema StorageGRID, è possibile attivare manualmente l'invio di un messaggio AutoSupport.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre dell'autorizzazione Root Access o Other Grid Configuration.

Fasi

1. Selezionare **supporto Strumenti AutoSupport**.

Viene visualizzata la pagina AutoSupport (Impostazioni) con la scheda **Settings** (Impostazioni) selezionata.

2. Selezionare **Invia AutoSupport attivato dall'utente**.

StorageGRID tenta di inviare un messaggio AutoSupport al supporto tecnico. Se il tentativo ha esito positivo, i valori **risultato più recente** e **tempo ultimo successo** nella scheda **risultati** vengono aggiornati. In caso di problemi, il valore **risultato più recente** viene aggiornato a "non riuscito" e StorageGRID non tenta di inviare nuovamente il messaggio AutoSupport.



Dopo aver inviato un messaggio AutoSupport attivato dall'utente, aggiornare la pagina AutoSupport del browser dopo 1 minuto per accedere ai risultati più recenti.

Aggiunta di una destinazione AutoSupport aggiuntiva

Quando si attiva AutoSupport, vengono inviati messaggi di stato e di salute al supporto NetApp. È possibile specificare una destinazione aggiuntiva per tutti i messaggi AutoSupport.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre dell'autorizzazione Root Access o Other Grid Configuration.

A proposito di questa attività

Per verificare o modificare il protocollo utilizzato per inviare messaggi AutoSupport, consultare le istruzioni per specificare un protocollo AutoSupport.



Non è possibile utilizzare il protocollo SMTP per inviare messaggi AutoSupport a una destinazione aggiuntiva.

"Specifica del protocollo per i messaggi AutoSupport"

Fasi

1. Selezionare **supporto Strumenti AutoSupport**.

Viene visualizzata la pagina AutoSupport (Impostazioni) con la scheda **Settings** (Impostazioni) selezionata.

2. Selezionare **Abilita destinazione AutoSupport aggiuntiva**.

Vengono visualizzati i campi destinazione AutoSupport aggiuntiva.

Additional AutoSupport Destination

Enable Additional AutoSupport Destination	<input checked="" type="checkbox"/>
Hostname	<input type="text" value="testbed.netapp.com"/>
Port	<input type="text" value="443"/>
Certificate Validation	<input type="text" value="Do not verify certificate"/>

You are not using a TLS certificate to secure the connection to the additional AutoSupport destination.

Save

Send User-Triggered AutoSupport

3. Immettere il nome host del server o l'indirizzo IP di un server di destinazione AutoSupport aggiuntivo.



È possibile inserire solo una destinazione aggiuntiva.

4. Inserire la porta utilizzata per la connessione a un server di destinazione AutoSupport aggiuntivo (l'impostazione predefinita è la porta 80 per HTTP o la porta 443 per HTTPS).
5. Per inviare i messaggi AutoSupport con la convalida del certificato, selezionare **Usa bundle CA**

personalizzato nell'elenco a discesa **convalida certificato**. Quindi, eseguire una delle seguenti operazioni:

- Utilizzare uno strumento di modifica per copiare e incollare tutto il contenuto di ciascun file di certificato CA con codifica PEM nel campo **bundle CA**, concatenato in ordine di catena del certificato. È necessario includere `-----BEGIN CERTIFICATE-----` e `-----END CERTIFICATE-----` nella selezione.

Additional AutoSupport Destination

Enable Additional AutoSupport Destination

Hostname

Port

Certificate Validation

CA Bundle

```
-----BEGIN CERTIFICATE-----
abcdefghijklmnop123456780ABCDEFGHIJKL
123456/7890ABCDEFabcdefghijklmnopklABCD
-----END CERTIFICATE-----
```

- Selezionare **Sfoggia**, individuare il file contenente i certificati, quindi selezionare **Apri** per caricare il file. La convalida del certificato garantisce la sicurezza della trasmissione dei messaggi AutoSupport.

6. Per inviare i messaggi AutoSupport senza convalida del certificato, selezionare **non verificare il certificato** nell'elenco a discesa **convalida certificato**.

Selezionare questa opzione solo se si dispone di un buon motivo per non utilizzare la convalida del certificato, ad esempio quando si verifica un problema temporaneo con un certificato.

Viene visualizzato un messaggio di attenzione: "Non si sta utilizzando un certificato TLS per proteggere la connessione alla destinazione AutoSupport aggiuntiva."

7. Selezionare **Salva**.

Tutti i messaggi AutoSupport futuri, generati da eventi e attivati dall'utente, verranno inviati alla destinazione aggiuntiva.

Invio di messaggi AutoSupport e-Series tramite StorageGRID

È possibile inviare messaggi AutoSupport di Gestione di sistema di e-Series SANtricity al supporto tecnico tramite un nodo di amministrazione StorageGRID anziché la porta di gestione dell'appliance di storage.

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un browser Web supportato.

- Si dispone dell'autorizzazione Storage Appliance Administrator o Root Access.



È necessario disporre del firmware SANtricity 8.70 o superiore per accedere a Gestione di sistema di SANtricity utilizzando Gestione griglia.

A proposito di questa attività

I messaggi AutoSupport di e-Series contengono informazioni dettagliate sull'hardware di storage e sono più specifici degli altri messaggi AutoSupport inviati dal sistema StorageGRID.

Configurare uno speciale indirizzo del server proxy in Gestore di sistema di SANtricity per fare in modo che i messaggi AutoSupport vengano trasmessi attraverso un nodo di amministrazione di StorageGRID senza utilizzare la porta di gestione dell'appliance. I messaggi AutoSupport trasmessi in questo modo rispettano le impostazioni del proxy di amministrazione e mittente preferite che potrebbero essere state configurate in Gestione griglia.

Se si desidera configurare il server proxy Admin in Grid Manager, consultare le istruzioni per la configurazione delle impostazioni del proxy Admin.

["Configurazione delle impostazioni del proxy amministratore"](#)



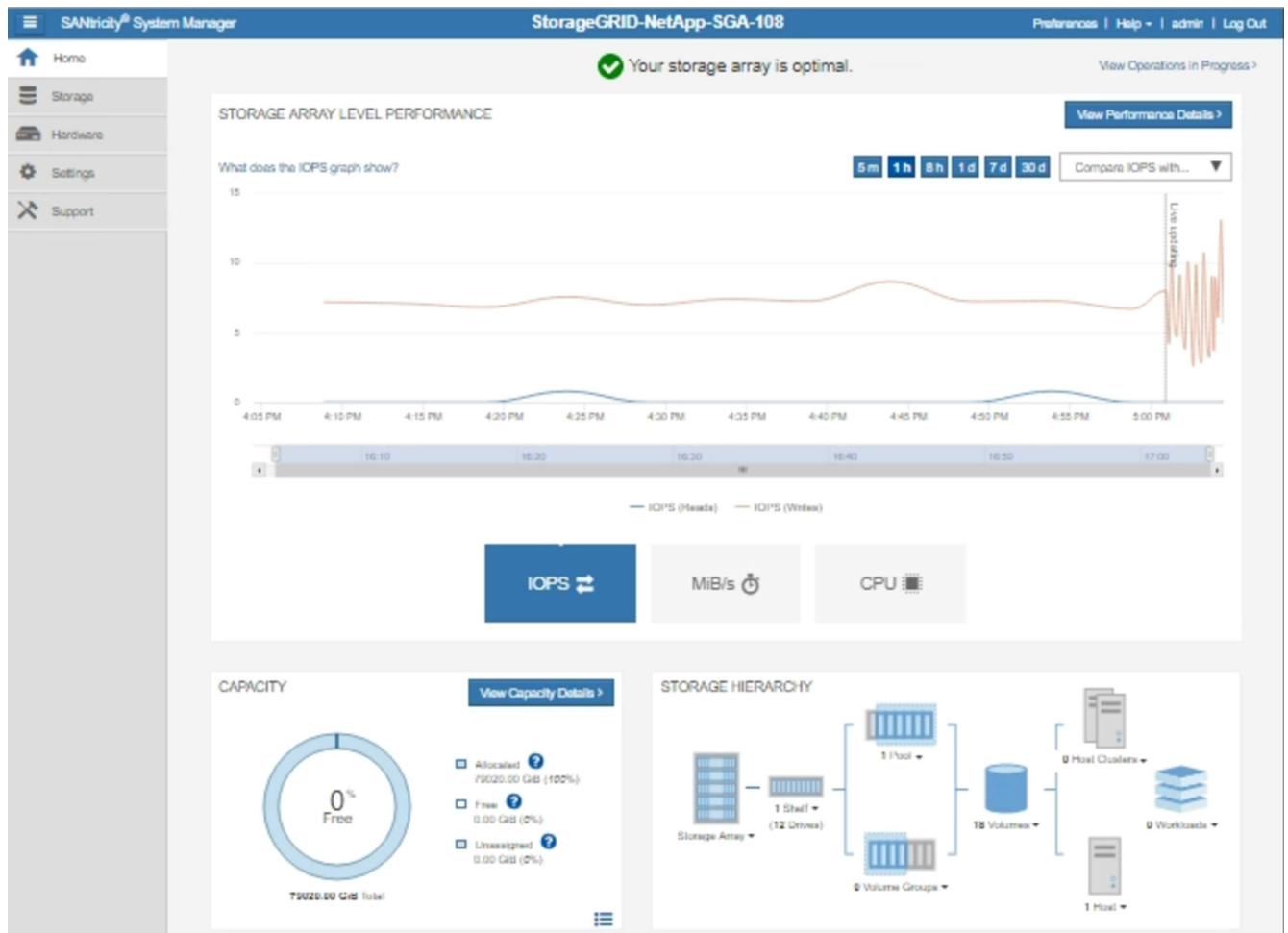
Questa procedura è valida solo per la configurazione di un server proxy StorageGRID per i messaggi AutoSupport e-Series. Per ulteriori informazioni sulla configurazione di e-Series AutoSupport, consultare il centro di documentazione di e-Series.

["Centro di documentazione dei sistemi NetApp e-Series"](#)

Fasi

1. In Grid Manager, selezionare **Nodes**.
2. Dall'elenco dei nodi a sinistra, selezionare il nodo dell'appliance di storage che si desidera configurare.
3. Selezionare **Gestore di sistema SANtricity**.

Viene visualizzata la home page di Gestore di sistema di SANtricity.



4. Selezionare **supporto Centro di supporto AutoSupport**.

Viene visualizzata la pagina AutoSupport Operations.

[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 erogazione AutoSupport**.

Viene visualizzata la pagina Configura metodo di erogazione AutoSupport.

Configure AutoSupport Delivery Method ✕

Select AutoSupport dispatch delivery method...

HTTPS
 HTTP
 Email

HTTPS delivery settings Show destination address

Connect to support team...

Directly ?
 via Proxy server ?

Host address ?

Port number ?

My proxy server requires authentication
 via Proxy auto-configuration script (PAC) ?

6. Selezionare **HTTPS** per il metodo di consegna.



Il certificato che abilita il protocollo HTTPS è preinstallato.

7. Selezionare **via Proxy server**.

8. Invio `tunnel-host` Per l'indirizzo **host**.

`tunnel-host` È l'indirizzo speciale per l'utilizzo di un nodo amministrativo per l'invio di messaggi AutoSupport e-Series.

9. Invio `10225` Per il numero di porta *.

`10225` È il numero di porta sul server proxy StorageGRID che riceve i messaggi AutoSupport dal controller e-Series nell'appliance.

10. Selezionare **verifica configurazione** per verificare l'instradamento e la configurazione del server proxy AutoSupport.

Se la risposta è corretta, viene visualizzato un messaggio in un banner verde: "la configurazione

AutoSupport è stata verificata”.

Se il test ha esito negativo, viene visualizzato un messaggio di errore su un banner rosso. Verificare le impostazioni DNS e la rete StorageGRID, assicurarsi che il nodo di amministrazione mittente preferito possa connettersi al sito di supporto NetApp e riprovare il test.

11. Selezionare **Salva**.

La configurazione viene salvata e viene visualizzato un messaggio di conferma: “AutoSupport delivery method has been configured”.

Risoluzione dei problemi relativi ai messaggi AutoSupport

Se un tentativo di inviare un messaggio AutoSupport non riesce, il sistema StorageGRID esegue diverse azioni a seconda del tipo di messaggio AutoSupport. Puoi controllare lo stato dei messaggi AutoSupport selezionando **supporto Strumenti AutoSupport risultati**.



I messaggi AutoSupport attivati dagli eventi vengono soppressi quando si sopprimono le notifiche e-mail a livello di sistema. (Selezionare **Configurazione Impostazioni di sistema Opzioni di visualizzazione**. Quindi, selezionare **Notification Sopprimi tutto**.)

Quando il messaggio AutoSupport non viene inviato, nella scheda **Results** della pagina **AutoSupport** viene visualizzato “Failed”.

AutoSupport

The AutoSupport feature enables your StorageGRID system to send periodic and event-driven health and status messages to technical support to allow proactive monitoring and troubleshooting. StorageGRID AutoSupport also enables the use of Active IQ for predictive recommendations.

Settings

Results

Weekly AutoSupport

Next Scheduled Time  2020-12-11 23:30:00 EST

Most Recent Result  Idle (NetApp Support)

Last Successful Time  N/A (NetApp Support)

Event-Triggered AutoSupport

Most Recent Result  N/A (NetApp Support)

Last Successful Time  N/A (NetApp Support)

User-Triggered AutoSupport

Most Recent Result  Failed (NetApp Support)

Last Successful Time  N/A (NetApp Support)

AutoSupport On Demand

AutoSupport On Demand messages are only sent to NetApp Support.

Most Recent Result  N/A (NetApp Support)

Last Successful Time  N/A (NetApp Support)

Errore settimanale del messaggio AutoSupport

Se un messaggio AutoSupport settimanale non viene inviato, il sistema StorageGRID esegue le seguenti operazioni:

1. Aggiorna l'attributo dei risultati più recenti in Riprova.
2. Tenta di inviare nuovamente il messaggio AutoSupport 15 volte ogni quattro minuti per un'ora.
3. Dopo un'ora di errori di invio, aggiorna l'attributo dei risultati più recenti su non riuscito.
4. Tenta di inviare nuovamente un messaggio AutoSupport all'ora successiva pianificata.
5. Mantiene la normale pianificazione AutoSupport se il messaggio non riesce perché il servizio NMS non è disponibile e se un messaggio viene inviato prima del termine di sette giorni.
6. Quando il servizio NMS è nuovamente disponibile, invia immediatamente un messaggio AutoSupport se non viene inviato alcun messaggio per almeno sette giorni.

Errore messaggio AutoSupport attivato dall'utente o attivato da evento

Se un messaggio AutoSupport attivato dall'utente o attivato da un evento non viene inviato, il sistema StorageGRID esegue le seguenti operazioni:

1. Visualizza un messaggio di errore se l'errore è noto. Ad esempio, se un utente seleziona il protocollo SMTP senza fornire le corrette impostazioni di configurazione dell'e-mail, viene visualizzato il seguente messaggio di errore: `AutoSupport messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`
2. Non tenta di inviare nuovamente il messaggio.
3. Registra l'errore in `nms.log`.

Se si verifica un errore e SMTP è il protocollo selezionato, verificare che il server e-mail del sistema StorageGRID sia configurato correttamente e che il server e-mail sia in esecuzione (**supporto Allarmi (legacy)** * Configurazione e-mail legacy*). Nella pagina AutoSupport potrebbe essere visualizzato il seguente messaggio di errore: `AutoSupport messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Informazioni su come configurare le impostazioni del server di posta elettronica in ["monitor amp; istruzioni per la risoluzione dei problemi"](#).

Correzione di un errore di messaggio AutoSupport

Se si verifica un errore e il protocollo SMTP è selezionato, verificare che il server e-mail del sistema StorageGRID sia configurato correttamente e che il server e-mail sia in esecuzione. Nella pagina AutoSupport potrebbe essere visualizzato il seguente messaggio di errore: `AutoSupport messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Informazioni correlate

["Monitor risoluzione dei problemi"](#)

Gestione dei nodi di storage

I nodi di storage forniscono servizi e capacità di storage su disco. La gestione dei nodi di storage comporta il monitoraggio della quantità di spazio utilizzabile su ciascun nodo, utilizzando le impostazioni di filigrana e applicando le impostazioni di configurazione del nodo di storage.

- ["Che cos'è un nodo di storage"](#)
- ["Gestione delle opzioni di storage"](#)
- ["Gestione dello storage dei metadati degli oggetti"](#)
- ["Configurazione delle impostazioni globali per gli oggetti memorizzati"](#)
- ["Impostazioni di configurazione del nodo di storage"](#)
- ["Gestione dei nodi di storage completi"](#)

Che cos'è un nodo di storage

I nodi di storage gestiscono e memorizzano i dati e i metadati degli oggetti. Ogni sistema StorageGRID deve avere almeno tre nodi di storage. Se si dispone di più siti, ogni sito

all'interno del sistema StorageGRID deve avere anche tre nodi di storage.

Un nodo di storage include i servizi e i processi necessari per memorizzare, spostare, verificare e recuperare i dati degli oggetti e i metadati sul disco. È possibile visualizzare informazioni dettagliate sui nodi di storage nella pagina **nodi**.

Che cos'è il servizio ADC

Il servizio ADC (Administrative Domain Controller) autentica i nodi della griglia e le relative connessioni tra loro. Il servizio ADC è ospitato su ciascuno dei primi tre nodi di storage di un sito.

Il servizio ADC mantiene le informazioni sulla topologia, inclusa la posizione e la disponibilità dei servizi. Quando un nodo della griglia richiede informazioni da un altro nodo della griglia o un'azione da eseguire da un altro nodo della griglia, contatta un servizio ADC per trovare il nodo della griglia migliore per elaborare la sua richiesta. Inoltre, il servizio ADC conserva una copia dei bundle di configurazione dell'implementazione StorageGRID, consentendo a qualsiasi nodo grid di recuperare le informazioni di configurazione correnti. È possibile visualizzare le informazioni ADC per un nodo di storage nella pagina topologia griglia (**supporto topologia griglia**).

Per facilitare le operazioni distribuite e islanded, ciascun servizio ADC sincronizza certificati, bundle di configurazione e informazioni sui servizi e sulla topologia con gli altri servizi ADC nel sistema StorageGRID.

In generale, tutti i nodi di rete mantengono una connessione ad almeno un servizio ADC. In questo modo, i nodi della griglia accedono sempre alle informazioni più recenti. Quando i nodi di rete si connettono, memorizzano nella cache i certificati degli altri nodi di rete, consentendo ai sistemi di continuare a funzionare con nodi di rete noti anche quando un servizio ADC non è disponibile. I nuovi nodi di rete possono stabilire connessioni solo utilizzando un servizio ADC.

La connessione di ciascun nodo di rete consente al servizio ADC di raccogliere informazioni sulla topologia. Queste informazioni sul nodo della griglia includono il carico della CPU, lo spazio su disco disponibile (se dotato di storage), i servizi supportati e l'ID del sito del nodo della griglia. Altri servizi richiedono al servizio ADC informazioni sulla topologia tramite query sulla topologia. Il servizio ADC risponde a ogni richiesta con le informazioni più recenti ricevute dal sistema StorageGRID.

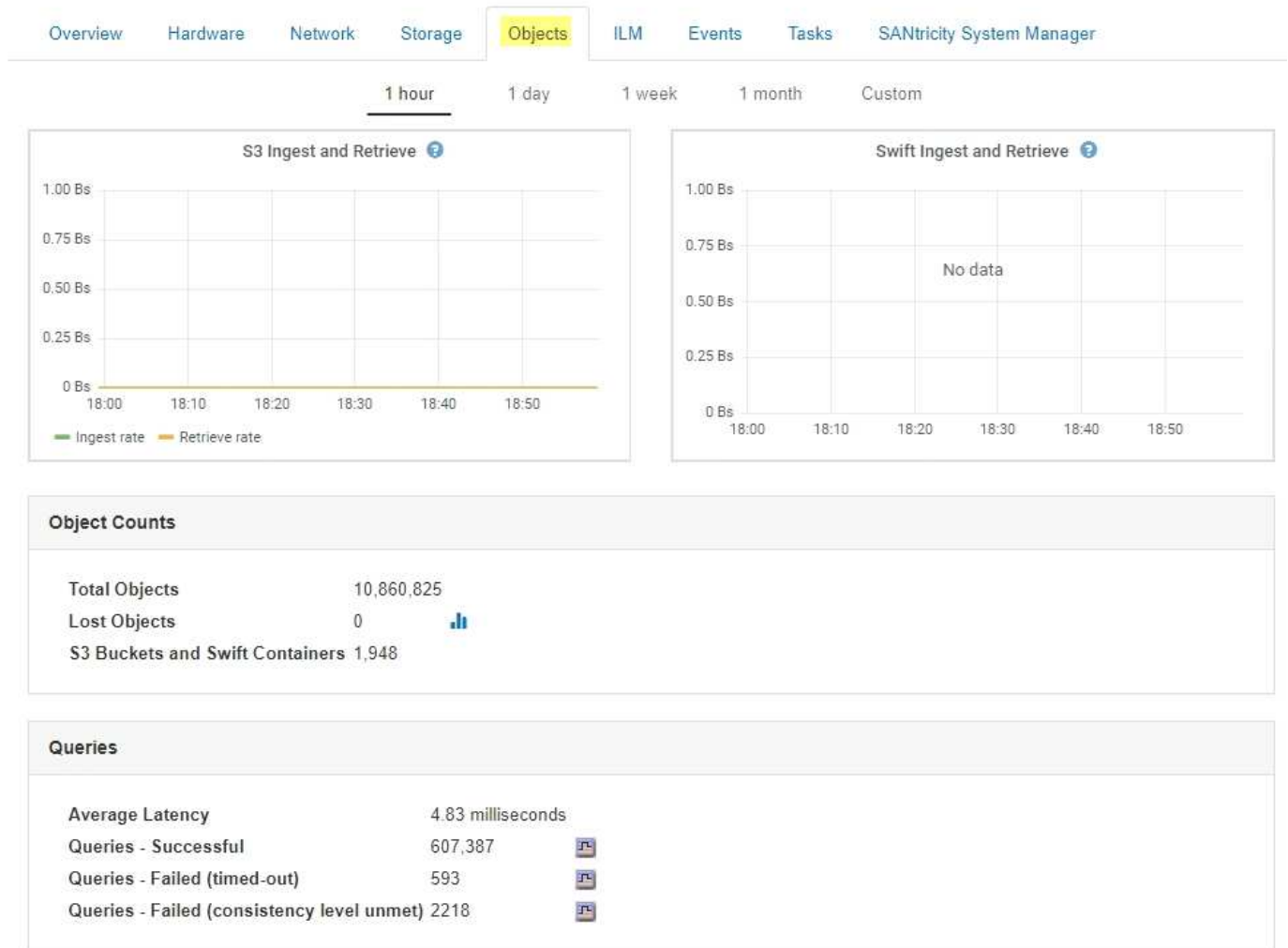
Che cos'è il servizio DDS

Ospitato da un nodo di storage, il servizio DDS (Distributed Data Store) si interfaccia con il database Cassandra per eseguire attività in background sui metadati degli oggetti memorizzati nel sistema StorageGRID.

Numero di oggetti

Il servizio DDS tiene traccia del numero totale di oggetti acquisiti nel sistema StorageGRID e del numero totale di oggetti acquisiti attraverso ciascuna delle interfacce supportate dal sistema (S3 o Swift).

È possibile visualizzare il numero totale di oggetti nella scheda oggetti della pagina nodi per qualsiasi nodo di storage.



Query

È possibile identificare il tempo medio necessario per eseguire una query sull'archivio di metadati tramite il servizio DDS specifico, il numero totale di query riuscite e il numero totale di query non riuscite a causa di un problema di timeout.

È possibile rivedere le informazioni sulle query per monitorare lo stato dell'archivio di metadati, Cassandra, che influisce sulle prestazioni di acquisizione e recupero del sistema. Ad esempio, se la latenza di una query media è lenta e il numero di query non riuscite a causa dei timeout è elevato, l'archivio di metadati potrebbe riscontrare un carico maggiore o eseguire un'altra operazione.

È inoltre possibile visualizzare il numero totale di query non riuscite a causa di errori di coerenza. Gli errori del livello di coerenza derivano da un numero insufficiente di archivi di metadati disponibili nel momento in cui viene eseguita una query attraverso il servizio DDS specifico.

È possibile utilizzare la pagina Diagnostics (Diagnostica) per ottenere ulteriori informazioni sullo stato corrente della griglia. Vedere ["Esecuzione della diagnostica"](#).

Garanzie e controlli di coerenza

StorageGRID garantisce la coerenza di lettura dopo scrittura per gli oggetti appena creati. Qualsiasi operazione GET successiva a un'operazione PUT completata con successo sarà in grado di leggere i dati

appena scritti. Le sovrascritture degli oggetti esistenti, gli aggiornamenti dei metadati e le eliminazioni rimangono alla fine coerenti.

Che cos'è il servizio LDR

Ospitato da ciascun nodo di storage, il servizio router di distribuzione locale (LDR) gestisce il trasporto dei contenuti per il sistema StorageGRID. Il trasporto dei contenuti comprende molte attività, tra cui storage dei dati, routing e gestione delle richieste. Il servizio LDR esegue la maggior parte del lavoro del sistema StorageGRID gestendo i carichi di trasferimento dei dati e le funzioni di traffico dei dati.

Il servizio LDR gestisce le seguenti attività:

- Query
- Attività ILM (Information Lifecycle Management)
- Eliminazione di oggetti
- Storage di dati a oggetti
- Trasferimenti di dati a oggetti da un altro servizio LDR (nodo di storage)
- Gestione dello storage dei dati
- Interfacce di protocollo (S3 e Swift)

Il servizio LDR gestisce inoltre la mappatura degli oggetti S3 e Swift sugli univoci "content handle" (UUID) assegnati dal sistema StorageGRID a ciascun oggetto acquisito.

Query

Le query LDR includono query per la posizione degli oggetti durante le operazioni di recupero e archiviazione. È possibile identificare il tempo medio necessario per eseguire una query, il numero totale di query riuscite e il numero totale di query non riuscite a causa di un problema di timeout.

È possibile rivedere le informazioni sulle query per monitorare lo stato dell'archivio di metadati, che influisce sulle prestazioni di acquisizione e recupero del sistema. Ad esempio, se la latenza di una query media è lenta e il numero di query non riuscite a causa dei timeout è elevato, l'archivio di metadati potrebbe riscontrare un carico maggiore o eseguire un'altra operazione.

È inoltre possibile visualizzare il numero totale di query non riuscite a causa di errori di coerenza. Gli errori del livello di coerenza derivano da un numero insufficiente di archivi di metadati disponibili nel momento in cui viene eseguita una query attraverso il servizio LDR specifico.

È possibile utilizzare la pagina Diagnostics (Diagnostica) per ottenere ulteriori informazioni sullo stato corrente della griglia. Vedere "[Esecuzione della diagnostica](#)".

Attività ILM

Le metriche ILM (Information Lifecycle Management) consentono di monitorare la velocità di valutazione degli oggetti per l'implementazione ILM. È possibile visualizzare queste metriche nella dashboard o nella scheda ILM della pagina nodi per ciascun nodo di storage.

Archivi di oggetti

Lo storage dei dati sottostante di un servizio LDR è diviso in un numero fisso di archivi a oggetti (noti anche come volumi di storage). Ogni archivio di oggetti è un punto di montaggio separato.

È possibile visualizzare gli archivi di oggetti per un nodo di storage nella scheda Storage della pagina Nodes.

Object Stores							
ID	Size	Available	Replicated Data	EC Data	Object Data (%)	Health	
0000	4.40 TB	1.35 TB	43.99 GB	0 bytes	1.00%	No Errors	
0001	1.97 TB	1.57 TB	44.76 GB	351.14 GB	20.09%	No Errors	
0002	1.97 TB	1.46 TB	43.29 GB	465.20 GB	25.81%	No Errors	
0003	1.97 TB	1.70 TB	43.51 GB	223.98 GB	13.58%	No Errors	
0004	1.97 TB	1.92 TB	44.03 GB	0 bytes	2.23%	No Errors	
0005	1.97 TB	1.46 TB	43.67 GB	463.36 GB	25.73%	No Errors	
0006	1.97 TB	1.92 TB	43.10 GB	1.61 GB	2.27%	No Errors	
0007	1.97 TB	1.35 TB	46.05 GB	575.24 GB	31.53%	No Errors	
0008	1.97 TB	1.81 TB	46.00 GB	112.84 GB	8.06%	No Errors	
0009	1.97 TB	1.57 TB	43.91 GB	352.72 GB	20.13%	No Errors	
000A	1.97 TB	1.70 TB	44.31 GB	226.81 GB	13.76%	No Errors	
000B	1.97 TB	1.92 TB	43.17 GB	780.07 MB	2.23%	No Errors	
000C	1.97 TB	1.58 TB	44.32 GB	339.56 GB	19.48%	No Errors	
000D	1.97 TB	1.82 TB	44.47 GB	107.34 GB	7.70%	No Errors	
000E	1.97 TB	1.68 TB	43.07 GB	241.70 GB	14.45%	No Errors	
000F	2.03 TB	1.50 TB	44.57 GB	475.47 GB	25.67%	No Errors	

Gli archivi di oggetti in un nodo di storage sono identificati da un numero esadecimale compreso tra 0000 e 002F, noto come ID del volume. Lo spazio è riservato nel primo archivio di oggetti (volume 0) per i metadati degli oggetti in un database Cassandra; qualsiasi spazio rimanente in tale volume viene utilizzato per i dati degli oggetti. Tutti gli altri archivi di oggetti vengono utilizzati esclusivamente per i dati degli oggetti, che includono copie replicate e frammenti con codifica di cancellazione.

Per garantire un utilizzo uniforme dello spazio per le copie replicate, i dati degli oggetti per un determinato oggetto vengono memorizzati in un archivio di oggetti in base allo spazio di storage disponibile. Quando uno o più archivi di oggetti riempiono la capacità, gli archivi di oggetti rimanenti continuano a memorizzare gli oggetti fino a quando non c'è più spazio nel nodo di storage.

Protezione dei metadati

I metadati degli oggetti sono informazioni correlate o una descrizione di un oggetto, ad esempio il tempo di modifica dell'oggetto o la posizione di storage. StorageGRID memorizza i metadati degli oggetti in un database Cassandra, che si interfaccia con il servizio LDR.

Per garantire la ridondanza e quindi la protezione contro la perdita, vengono conservate tre copie dei metadati degli oggetti in ogni sito. Le copie vengono distribuite in modo uniforme in tutti i nodi di storage di ogni sito. Questa replica non è configurabile ed è eseguita automaticamente.

["Gestione dello storage dei metadati degli oggetti"](#)

Gestione delle opzioni di storage

È possibile visualizzare e configurare le opzioni di storage utilizzando il menu Configuration (Configurazione) di Grid Manager. Le opzioni di storage includono le impostazioni di segmentazione degli oggetti e i valori correnti per le filigrane di storage. È inoltre possibile visualizzare le porte S3 e Swift utilizzate dal servizio CLB obsoleto sui

nodi gateway e dal servizio LDR sui nodi storage.

Per informazioni sulle assegnazioni delle porte, vedere ["Riepilogo: Indirizzi IP e porte per le connessioni client"](#).

Storage Options
Overview
Configuration



Storage Options Overview

Updated: 2019-03-22 12:49:16 MDT

Object Segmentation

Description	Settings
Segmentation	Enabled
Maximum Segment Size	1 GB

Storage Watermarks

Description	Settings
Storage Volume Read-Write Watermark	30 GB
Storage Volume Soft Read-Only Watermark	10 GB
Storage Volume Hard Read-Only Watermark	5 GB
Metadata Reserved Space	3,000 GB

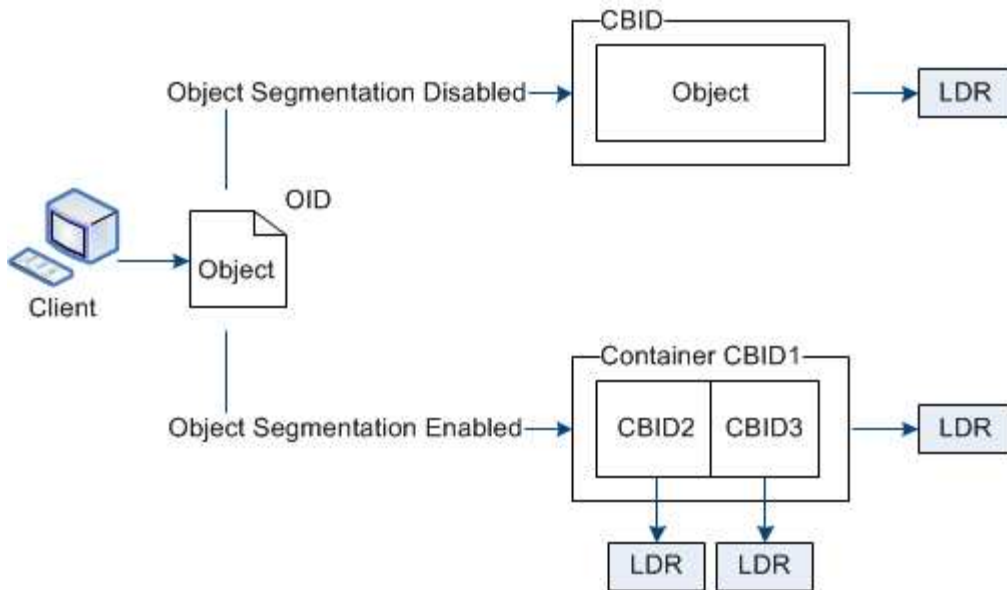
Ports

Description	Settings
CLB S3 Port	8082
CLB Swift Port	8083
LDR S3 Port	18082
LDR Swift Port	18083

Che cos'è la segmentazione degli oggetti

La segmentazione degli oggetti è il processo di suddivisione di un oggetto in un insieme di oggetti di dimensioni fisse più piccole per ottimizzare l'utilizzo dello storage e delle risorse per oggetti di grandi dimensioni. Il caricamento multiparte S3 crea anche oggetti segmentati, con un oggetto che rappresenta ciascuna parte.

Quando un oggetto viene acquisito nel sistema StorageGRID, il servizio LDR suddivide l'oggetto in segmenti e crea un container di segmenti che elenca le informazioni di intestazione di tutti i segmenti come contenuto.



Se il sistema StorageGRID include un nodo di archiviazione il cui tipo di destinazione è Tiering cloud — Servizio di storage semplice e il sistema di storage di archiviazione di destinazione è Amazon Web Services (AWS), la dimensione massima del segmento deve essere inferiore o uguale a 4.5 GiB (4,831,838,208 byte). Questo limite superiore garantisce che non venga superato il limite DI CINQUE GB DI AWS PUT. Le richieste ad AWS che superano questo valore non riescono.

Al momento del recupero di un container di segmenti, il servizio LDR assembla l'oggetto originale dai suoi segmenti e lo restituisce al client.

Il container e i segmenti non sono necessariamente memorizzati nello stesso nodo di storage. Container e segmenti possono essere memorizzati su qualsiasi nodo di storage.

Ogni segmento viene trattato dal sistema StorageGRID in modo indipendente e contribuisce al conteggio di attributi come oggetti gestiti e oggetti memorizzati. Ad esempio, se un oggetto memorizzato nel sistema StorageGRID viene suddiviso in due segmenti, il valore degli oggetti gestiti aumenta di tre dopo il completamento dell'acquisizione, come segue:

container di segmenti + segmento 1 + segmento 2 = tre oggetti memorizzati

È possibile migliorare le prestazioni durante la gestione di oggetti di grandi dimensioni garantendo che:

- Ciascun gateway e nodo di storage dispone di una larghezza di banda di rete sufficiente per il throughput richiesto. Ad esempio, configurare reti client e Grid separate su interfacce Ethernet a 10 Gbps.
- Vengono implementati un numero sufficiente di gateway e nodi storage per il throughput richiesto.
- Ogni nodo di storage dispone di prestazioni i/o su disco sufficienti per il throughput richiesto.

Quali sono le filigrane dei volumi di storage

StorageGRID utilizza le filigrane del volume di storage per consentire di monitorare la quantità di spazio utilizzabile disponibile sui nodi di storage. Se la quantità di spazio disponibile su un nodo è inferiore a un'impostazione di filigrana configurata, viene attivato l'allarme Storage Status (SST) per determinare se è necessario aggiungere nodi di storage.

Per visualizzare le impostazioni correnti delle filigrane Storage Volume, selezionare **Configurazione Opzioni**



Storage Options Overview

Updated: 2019-10-09 13:09:30 MDT

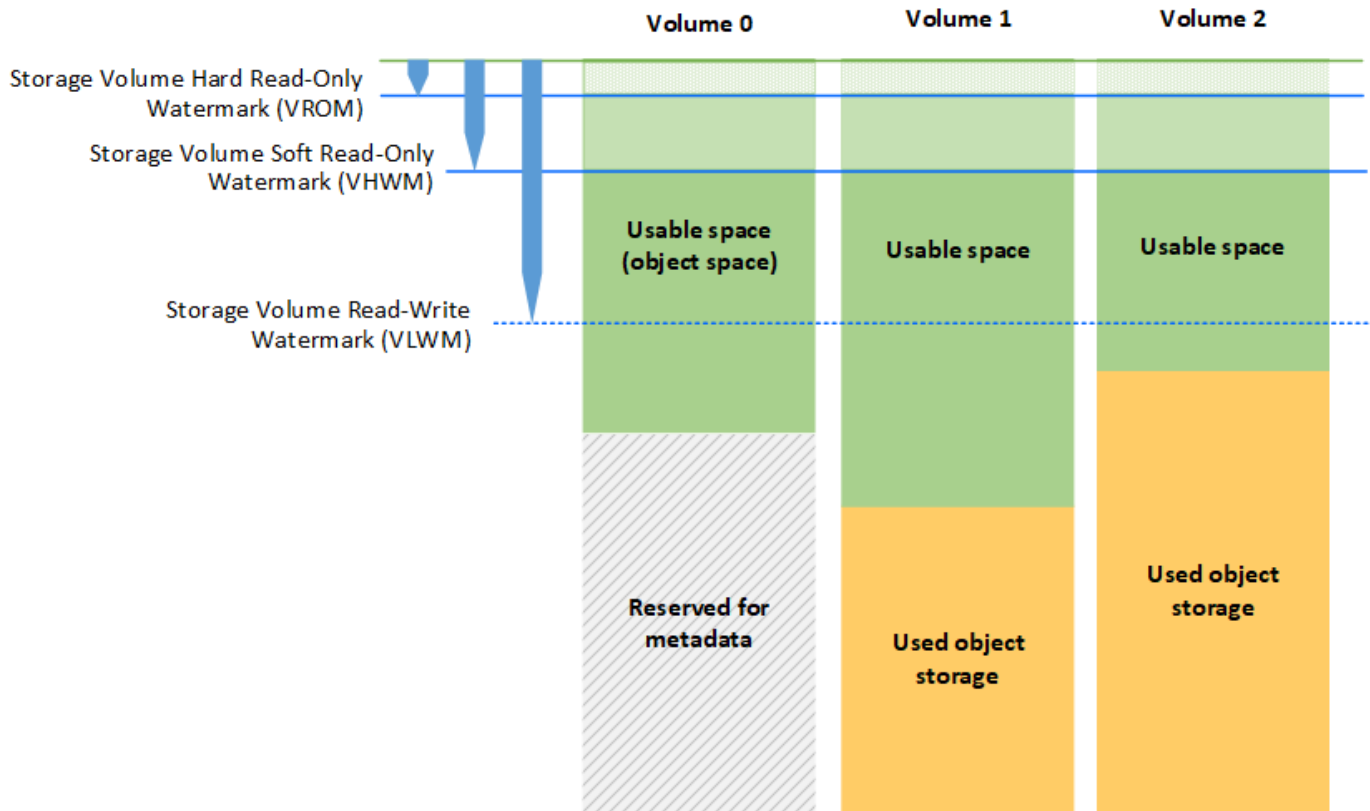
Object Segmentation

Description	Settings
Segmentation	Enabled
Maximum Segment Size	1 GB

Storage Watermarks

Description	Settings
Storage Volume Read-Write Watermark	30 GB
Storage Volume Soft Read-Only Watermark	10 GB
Storage Volume Hard Read-Only Watermark	5 GB
Metadata Reserved Space	3,000 GB

La figura seguente rappresenta un nodo di storage con tre volumi e mostra la posizione relativa delle tre filigrane del volume di storage. All'interno di ciascun nodo di storage, StorageGRID riserva spazio sul volume 0 per i metadati dell'oggetto; qualsiasi spazio rimanente su tale volume viene utilizzato per i dati dell'oggetto. Tutti gli altri volumi vengono utilizzati esclusivamente per i dati degli oggetti, che includono copie replicate e frammenti con codifica di cancellazione.



Le filigrane del volume di storage sono impostazioni predefinite a livello di sistema che indicano la quantità minima di spazio libero richiesta su ciascun volume nel nodo di storage per impedire a StorageGRID di modificare il comportamento di lettura/scrittura del nodo o di attivare un allarme. Tenere presente che tutti i volumi devono raggiungere il watermark prima che StorageGRID agisca. Se alcuni volumi hanno una quantità di spazio libero superiore al minimo richiesto, l'allarme non viene attivato e il comportamento di lettura/scrittura del nodo non cambia.

Filigrana di sola lettura software del volume di storage (VHWM)

Il watermark Storage Volume Soft Read-Only è il primo watermark a indicare che lo spazio utilizzabile di un nodo per i dati dell'oggetto sta diventando pieno. Questo watermark rappresenta la quantità di spazio libero che deve esistere su ogni volume in un nodo di storage per impedire al nodo di passare alla "modalità `soft Read-only`". La modalità di sola lettura morbida indica che il nodo di storage annuncia servizi di sola lettura al resto del sistema StorageGRID, ma soddisfa tutte le richieste di scrittura in sospeso.

Se la quantità di spazio libero su ciascun volume è inferiore all'impostazione di questo watermark, l'allarme Storage Status (SST) viene attivato al livello Notice e il nodo di storage passa alla modalità soft di sola lettura.

Ad esempio, si supponga che la filigrana Storage Volume Soft Read-Only sia impostata su 10 GB, che è il valore predefinito. Se su ciascun volume nel nodo di storage rimangono meno di 10 GB di spazio libero, l'allarme SST viene attivato a livello Notice e il nodo di storage passa alla modalità soft di sola lettura.

Filigrana di sola lettura (VROM) rigida del volume di storage

Il watermark di sola lettura hard del volume di storage è il watermark successivo per indicare che lo spazio utilizzabile di un nodo per i dati dell'oggetto sta diventando pieno. Questo watermark rappresenta la quantità di spazio libero che deve esistere su ogni volume in un nodo di storage per impedire al nodo di passare alla "modalità di sola lettura". La modalità hard Read-only significa che il nodo di storage è di sola lettura e non accetta più richieste di scrittura.

Se la quantità di spazio libero su ogni volume in un nodo di storage è inferiore all'impostazione di questo watermark, l'allarme Storage Status (SST) viene attivato al livello principale e il nodo di storage passa alla modalità hard Read-only.

Ad esempio, supponiamo che il watermark di sola lettura hard del volume di storage sia impostato su 5 GB, che è il valore predefinito. Se su ciascun volume di storage nel nodo di storage rimangono meno di 5 GB di spazio libero, l'allarme SSTS viene attivato al livello principale e il nodo di storage passa alla modalità hard Read-only.

Il valore della filigrana hard Read-only del volume di storage deve essere inferiore al valore della filigrana soft Read-only del volume di storage.

Filigrana di lettura/scrittura del volume di storage (VLWM)

Il watermark di lettura/scrittura del volume di storage si applica solo ai nodi di storage che sono passati alla modalità di sola lettura. Questo watermark determina quando il nodo di storage può diventare di nuovo in lettura/scrittura.

Ad esempio, supponiamo che un nodo di storage sia passato alla modalità hard Read-only. Se il watermark Read-Write del volume di storage è impostato su 30 GB (impostazione predefinita), lo spazio libero su ogni volume di storage nel nodo di storage deve aumentare da 5 GB a 30 GB prima che il nodo possa tornare in lettura-scrittura.

Il valore della filigrana Read-Write del volume di storage deve essere maggiore del valore della filigrana soft di sola lettura del volume di storage.

Informazioni correlate

["Gestione dei nodi di storage completi"](#)

Gestione dello storage dei metadati degli oggetti

La capacità dei metadati degli oggetti di un sistema StorageGRID controlla il numero massimo di oggetti che possono essere memorizzati in tale sistema. Per garantire che il sistema StorageGRID disponga di spazio sufficiente per memorizzare nuovi oggetti, è necessario comprendere dove e come StorageGRID memorizza i metadati degli oggetti.

Che cos'è il metadata a oggetti?

I metadati degli oggetti sono informazioni che descrivono un oggetto. StorageGRID utilizza i metadati degli oggetti per tenere traccia delle posizioni di tutti gli oggetti nella griglia e 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 o del container Swift, il nome o l'ID dell'account tenant, la dimensione logica dell'oggetto, la data

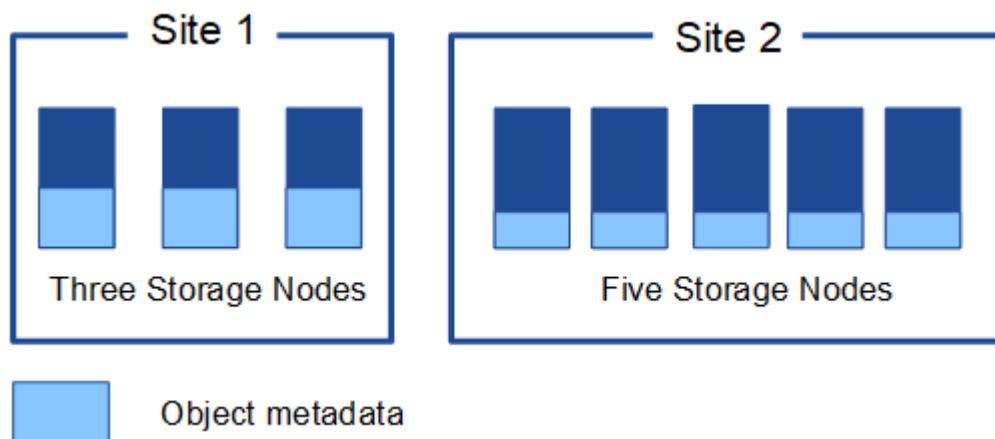
e l'ora in cui l'oggetto è stato creato per la prima volta, e la data e l'ora dell'ultima modifica dell'oggetto.

- Qualsiasi coppia di valori chiave metadati utente personalizzata associata all'oggetto.
- Per gli oggetti S3, qualsiasi coppia chiave-valore tag oggetto associata all'oggetto.
- Per le copie di oggetti replicate, la posizione di storage corrente di ciascuna copia.
- Per le copie di oggetti con codifica erasure, la posizione di storage 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 multiparte, identificatori di segmenti e dimensioni dei dati.

Come vengono memorizzati i metadati degli oggetti?

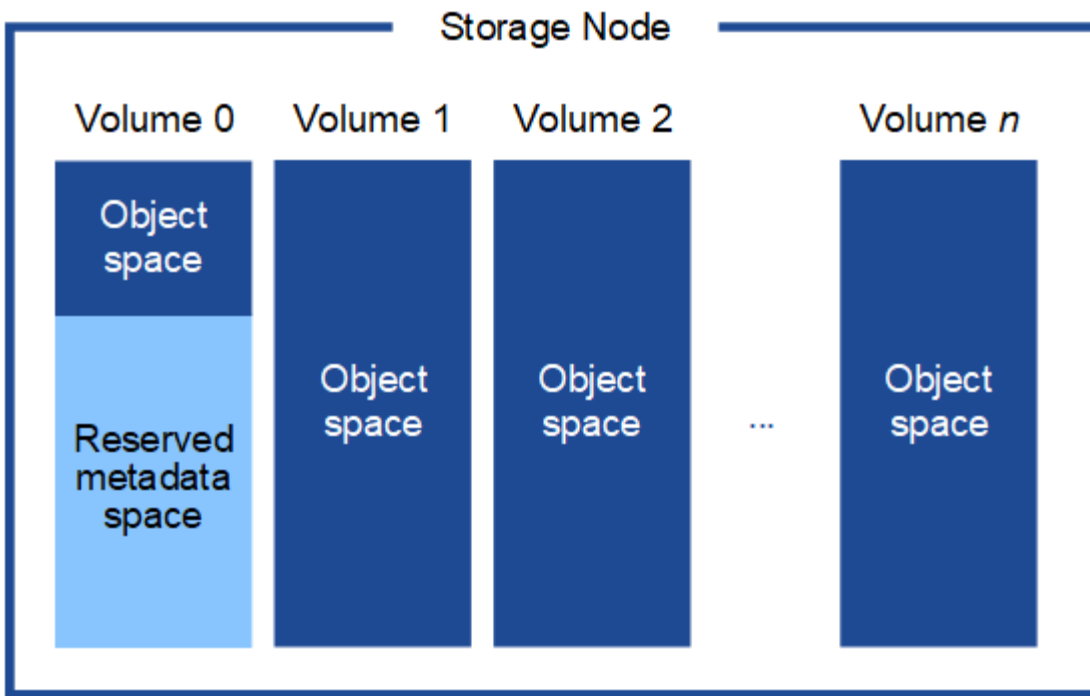
StorageGRID mantiene i metadati degli oggetti in un database Cassandra, che viene memorizzato indipendentemente dai dati degli oggetti. Per garantire la ridondanza e proteggere i metadati degli oggetti dalla perdita, StorageGRID memorizza tre copie dei metadati per tutti gli oggetti del sistema in ogni sito. Le tre copie dei metadati degli oggetti sono distribuite in modo uniforme in tutti i nodi di storage di ciascun sito.

Questa figura rappresenta i nodi di storage in due siti. Ogni sito ha la stessa quantità di metadati degli oggetti, che sono distribuiti in modo uguale tra i nodi di storage di quel sito.



Dove sono memorizzati i metadati degli oggetti?

Questa figura rappresenta i volumi di storage per un singolo nodo di storage.



Come mostrato nella figura, StorageGRID riserva spazio per i metadati degli oggetti sul volume di storage 0 di ciascun nodo di storage. Utilizza lo spazio riservato per memorizzare i metadati degli oggetti e per eseguire le operazioni essenziali del database. Qualsiasi spazio rimanente sul volume di storage 0 e tutti gli altri volumi di storage nel nodo di storage vengono utilizzati esclusivamente per i dati a oggetti (copie replicate e frammenti con codifica di cancellazione).

La quantità di spazio riservato ai metadati degli oggetti su un nodo di storage specifico dipende da una serie di fattori, descritti di seguito.

Impostazione spazio riservato metadati

L' *Metadata Reserved Space* 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 storage. Come mostrato nella tabella, il valore predefinito di questa impostazione per StorageGRID 11.5 si basa su quanto segue:

- La versione software utilizzata al momento dell'installazione iniziale di StorageGRID.
- La quantità di RAM su ciascun nodo di storage.

Versione utilizzata per l'installazione iniziale di StorageGRID	Quantità di RAM sui nodi di storage	Impostazione predefinita spazio riservato metadati per StorageGRID 11.5
11.5	128 GB o più su ciascun nodo di storage nella griglia	8 TB (8,000 GB)
	Meno di 128 GB su qualsiasi nodo di storage nel grid	3 TB (3,000 GB)
da 11.1 a 11.4	128 GB o più su ciascun nodo di storage in un sito qualsiasi	4 TB (4,000 GB)

Versione utilizzata per l'installazione iniziale di StorageGRID	Quantità di RAM sui nodi di storage	Impostazione predefinita spazio riservato metadati per StorageGRID 11.5
	Meno di 128 GB su qualsiasi nodo di storage in ogni sito	3 TB (3,000 GB)
11.0 o versioni precedenti	Qualsiasi importo	2 TB (2,000 GB)

Per visualizzare l'impostazione spazio riservato metadati per il sistema StorageGRID:

1. Selezionare **Configuration > System Settings > Storage Options**.
2. Nella tabella Storage Watermarks, individuare **Metadata Reserved Space**.



Storage Options Overview

Updated: 2021-02-23 11:58:33 MST

Object Segmentation

Description	Settings
Segmentation	Enabled
Maximum Segment Size	1 GB

Storage Watermarks

Description	Settings
Storage Volume Read-Write Watermark	30 GB
Storage Volume Soft Read-Only Watermark	10 GB
Storage Volume Hard Read-Only Watermark	5 GB
Metadata Reserved Space	8,000 GB

Nella schermata, il valore **Metadata Reserved Space** è 8,000 GB (8 TB). Questa è l'impostazione predefinita per una nuova installazione di StorageGRID 11.5 in cui ogni nodo di storage dispone di almeno 128 GB di RAM.

Spazio riservato effettivo per i metadati

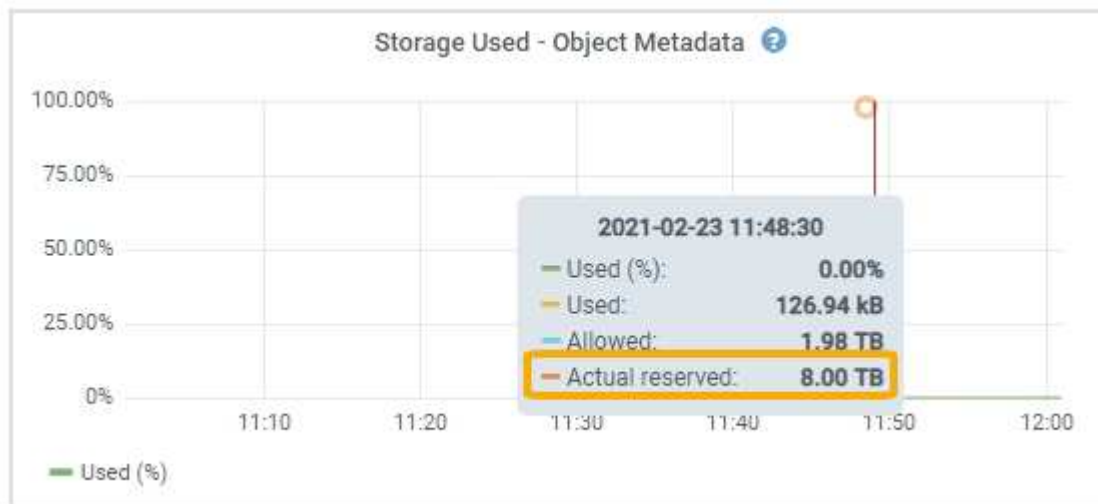
A differenza dell'impostazione spazio riservato metadati a livello di sistema, per ciascun nodo di storage viene determinato l' *spazio riservato effettivo* per i metadati dell'oggetto. Per qualsiasi nodo di storage, lo spazio riservato effettivo per i metadati dipende dalle dimensioni del volume 0 per il nodo e dall'impostazione **Metadata Reserved Space** a livello di sistema.

Dimensione del volume 0 per il nodo	Spazio riservato effettivo per i metadati
Meno di 500 GB (non in produzione)	10% del volume 0

Dimensione del volume 0 per il nodo	Spazio riservato effettivo per i metadati
500 GB o superiore	Il minore di questi valori: <ul style="list-style-type: none"> • Volume 0 • Impostazione spazio riservato metadati

Per visualizzare lo spazio riservato effettivo per i metadati su un nodo di storage specifico:

1. Da Grid Manager, selezionare **Nodes Storage Node**.
2. Selezionare la scheda **Storage**.
3. Posizionare il cursore sul grafico Storage used — Object Metadata (Storage utilizzato — metadati oggetto) e individuare il valore **Actual reserved** (riservato).



Nella schermata, il valore **effettivo riservato** è 8 TB. Questa schermata riguarda un nodo di storage di grandi dimensioni in una nuova installazione di StorageGRID 11.5. Poiché l'impostazione spazio riservato metadati a livello di sistema è inferiore al volume 0 per questo nodo di storage, lo spazio riservato effettivo per questo nodo corrisponde all'impostazione spazio riservato metadati.

Il valore **effettivo riservato** corrisponde a questa metrica Prometheus:

```
storagegrid_storage_utilization_metadata_reserved_bytes
```

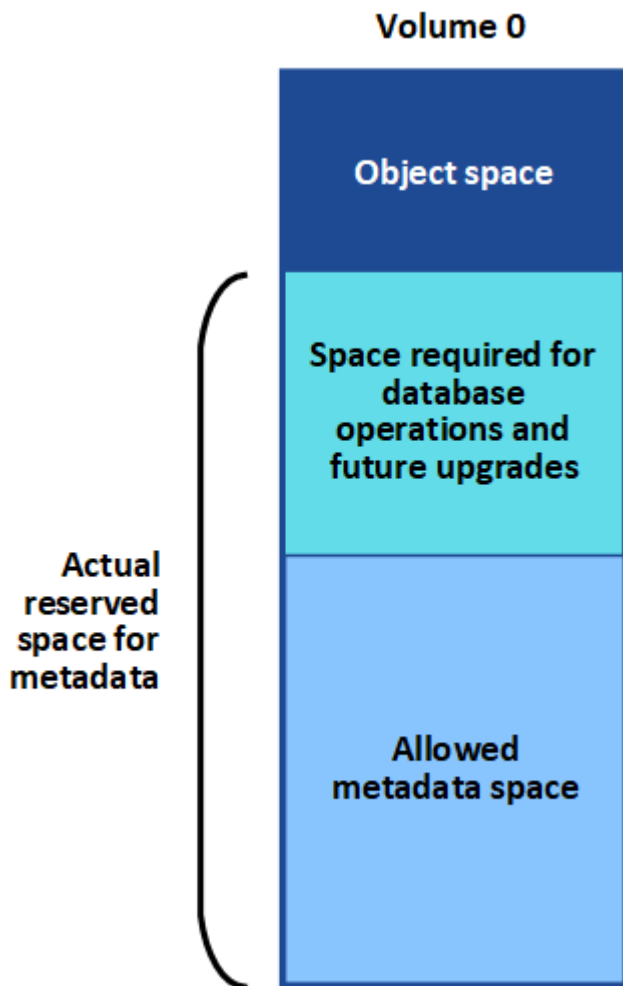
Esempio di spazio riservato effettivo dei metadati

Si supponga di installare un nuovo sistema StorageGRID utilizzando la versione 11.5. In questo esempio, si supponga che ogni nodo di storage abbia più di 128 GB di RAM e che il volume 0 del nodo di storage 1 (SN1) sia di 6 TB. In base a questi valori:

- L'opzione **Metadata Reserved Space** a livello di sistema è impostata su 8 TB. (Questo è il valore predefinito per una nuova installazione di StorageGRID 11.5 se ogni nodo di storage ha più di 128 GB di RAM).
- Lo spazio riservato effettivo per i metadati per SN1 è di 6 TB. (L'intero volume è riservato perché il volume 0 è più piccolo dell'impostazione **Metadata Reserved Space**).

Spazio consentito di metadati

Lo spazio riservato effettivo di ciascun nodo di storage per i metadati viene suddiviso nello spazio disponibile per i metadati dell'oggetto (il *spazio consentito per i metadati*) e nello spazio necessario per le operazioni essenziali del database (come la compattazione e la riparazione) e per i futuri aggiornamenti hardware e software. Lo spazio consentito per i metadati regola la capacità complessiva degli oggetti.



La tabella seguente riassume il modo in cui StorageGRID determina il valore dello spazio dei metadati consentito per un nodo di storage.

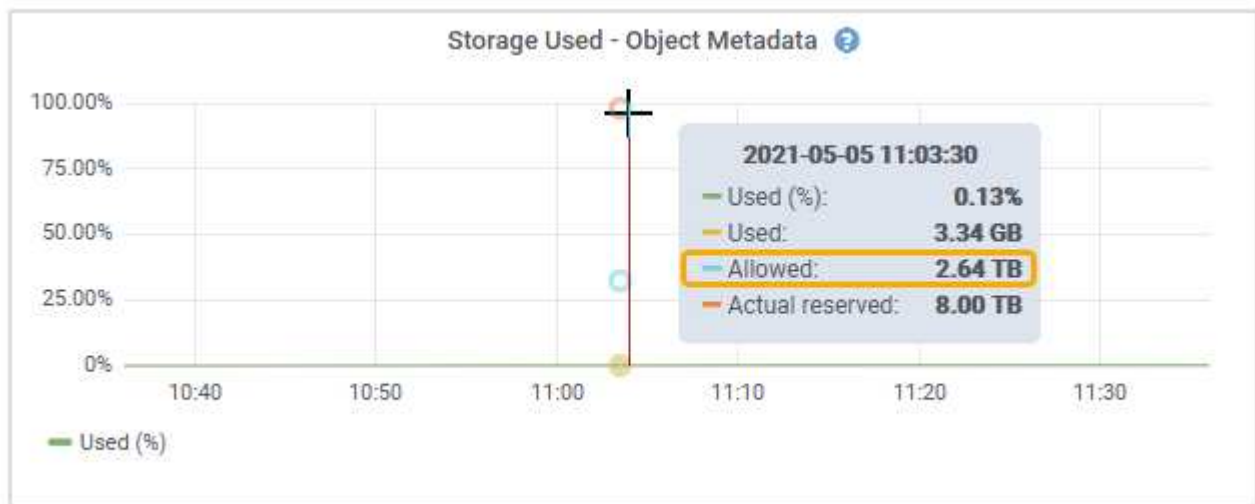
Spazio riservato effettivo per i metadati	Spazio consentito di metadati
4 TB o meno	60% dello spazio riservato effettivo per i metadati, fino a un massimo di 1.98 TB
Più di 4 TB	$(\text{Spazio riservato effettivo per i metadati} - 1 \text{ TB}) \times 60\%$, fino a un massimo di 2.64 TB



Se il sistema StorageGRID memorizza (o si prevede di memorizzare) più di 2.64 TB di metadati su qualsiasi nodo di storage, in alcuni casi lo spazio consentito per i metadati può essere aumentato. Se i nodi di storage hanno ciascuno più di 128 GB di RAM e spazio libero disponibile sul volume di storage 0, contattare il rappresentante NetApp. NetApp esaminerà i tuoi requisiti e, se possibile, aumenterà lo spazio di metadati consentito per ciascun nodo di storage.

Per visualizzare lo spazio di metadati consentito per un nodo di storage:

1. Da Grid Manager, selezionare **Node Storage Node**.
2. Selezionare la scheda **Storage**.
3. Posizionare il cursore del mouse sul grafico Storage used — Object Metadata (Storage utilizzato — metadati oggetto) e individuare il valore **Allowed** (consentito).



Nella schermata, il valore **Allowed** è 2.64 TB, ovvero il valore massimo per un nodo di storage il cui spazio riservato effettivo per i metadati è superiore a 4 TB.

Il valore **Allowed** corrisponde a questa metrica Prometheus:

```
storagegrid_storage_utilization_metadata_allowed_bytes
```

Esempio di spazio consentito per i metadati

Si supponga di installare un sistema StorageGRID utilizzando la versione 11.5. In questo esempio, si supponga che ogni nodo di storage abbia più di 128 GB di RAM e che il volume 0 del nodo di storage 1 (SN1) sia di 6 TB. In base a questi valori:

- L'opzione **Metadata Reserved Space** a livello di sistema è impostata su 8 TB. (Questo è il valore predefinito per StorageGRID 11.5 quando ogni nodo di storage ha più di 128 GB di RAM).
- Lo spazio riservato effettivo per i metadati per SN1 è di 6 TB. (L'intero volume è riservato perché il volume 0 è più piccolo dell'impostazione **Metadata Reserved Space**).
- Lo spazio consentito per i metadati su SN1 è di 2.64 TB. (Valore massimo per lo spazio riservato effettivo).

In che modo i nodi di storage di diverse dimensioni influiscono sulla capacità degli oggetti

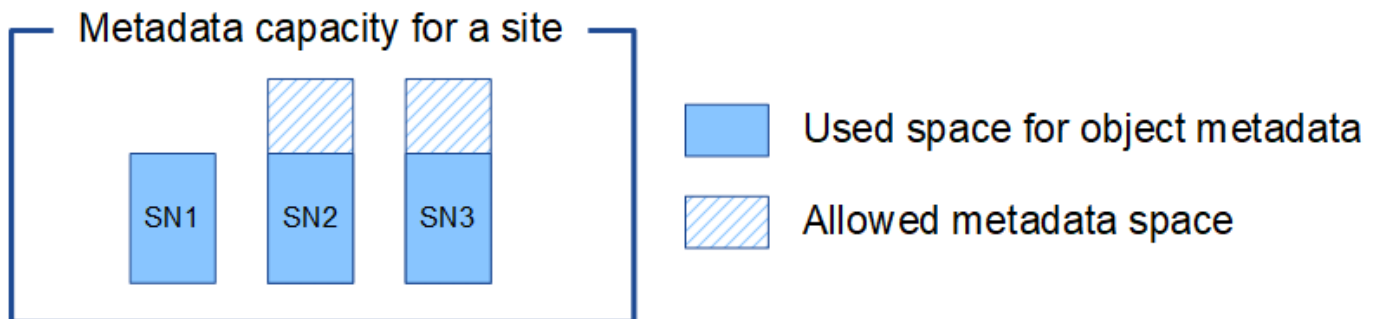
Come descritto in precedenza, StorageGRID distribuisce uniformemente i metadati degli oggetti nei nodi di storage di ciascun sito. Per questo motivo, se un sito contiene nodi di storage di dimensioni diverse, il nodo più piccolo del sito determina la capacità di metadati del sito.

Si consideri il seguente esempio:

- Si dispone di un grid a sito singolo contenente tre nodi di storage di dimensioni diverse.
- L'impostazione **Metadata Reserved Space** è 4 TB.
- I nodi di storage hanno i seguenti valori per lo spazio riservato effettivo dei metadati e per lo spazio consentito dei metadati.

Nodo di storage	Dimensione del volume 0	Spazio riservato effettivo dei metadati	Spazio consentito di metadati
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 in modo uniforme tra i nodi di storage di un sito, ciascun nodo di questo esempio può contenere solo 1.32 TB di metadati. Non è possibile utilizzare i 0.66 TB aggiuntivi di spazio consentito per i metadati 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.

Inoltre, poiché la capacità dei metadati degli oggetti controlla il numero massimo di oggetti, quando un nodo esaurisce la capacità dei metadati, la griglia è effettivamente piena.

Informazioni correlate

- Per informazioni su come monitorare la capacità dei metadati degli oggetti per ciascun nodo di storage:

["Monitor risoluzione dei problemi"](#)

- Per aumentare la capacità dei metadati degli oggetti per il sistema, è necessario aggiungere nuovi nodi di storage:

["Espandi il tuo grid"](#)

Configurazione delle impostazioni globali per gli oggetti memorizzati

È possibile utilizzare Opzioni griglia per configurare le impostazioni per tutti gli oggetti memorizzati nel sistema StorageGRID, inclusa la compressione degli oggetti memorizzati e la crittografia degli oggetti memorizzati. e l'hashing degli oggetti memorizzati.

- ["Configurazione della compressione degli oggetti memorizzati"](#)
- ["Configurazione della crittografia degli oggetti memorizzati"](#)
- ["Configurazione dell'hashing degli oggetti memorizzati"](#)

Configurazione della compressione degli oggetti memorizzati

È possibile utilizzare l'opzione Compress Stored Objects Grid per ridurre le dimensioni degli oggetti memorizzati in StorageGRID, in modo che gli oggetti consumino meno spazio di storage.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

A proposito di questa attività

Per impostazione predefinita, l'opzione Compress Stored Objects Grid (Comprimi oggetti memorizzati) è disattivata. Se si attiva questa opzione, StorageGRID tenta di comprimere ogni oggetto durante il salvataggio, utilizzando la compressione senza perdita di dati.



Se si modifica questa impostazione, l'applicazione della nuova impostazione richiede circa un minuto. Il valore configurato viene memorizzato nella cache per le prestazioni e la scalabilità.

Prima di attivare questa opzione, tenere presente quanto segue:

- Non attivare la compressione a meno che non si sappia che i dati memorizzati sono comprimibili.
- Le applicazioni che salvano oggetti in StorageGRID potrebbero comprimere gli oggetti prima di salvarli. Se un'applicazione client ha già compresso un oggetto prima di salvarlo in StorageGRID, l'attivazione della compressione degli oggetti memorizzati non ridurrà ulteriormente la dimensione di un oggetto.
- Non attivare la compressione se si utilizza NetApp FabricPool con StorageGRID.
- Se l'opzione Compress Stored Objects Grid è attivata, le applicazioni client S3 e Swift dovrebbero evitare di eseguire operazioni GET Object che specificano la restituzione di un intervallo di byte. Queste operazioni "range Read" sono inefficienti perché StorageGRID deve decomprimere efficacemente gli oggetti per accedere ai byte richiesti. LE operazioni GET Object che richiedono un piccolo intervallo 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 possono scadere.



Se è necessario comprimere gli oggetti e l'applicazione client deve utilizzare le letture dell'intervallo, aumentare il timeout di lettura per l'applicazione.

Fasi

1. Selezionare **Configurazione Impostazioni di sistema Opzioni griglia**.
2. Nella sezione Opzioni oggetto memorizzato, selezionare la casella di controllo **Comprimi oggetti memorizzati**.

Stored Object Options



3. Fare clic su **Save** (Salva).

Configurazione della crittografia degli oggetti memorizzati

È possibile crittografare gli oggetti memorizzati se si desidera garantire che i dati non possano essere recuperati in un formato leggibile se un archivio di oggetti viene compromesso. Per impostazione predefinita, gli oggetti non vengono crittografati.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

A proposito di questa attività

La crittografia degli oggetti memorizzati consente la crittografia di tutti i dati degli oggetti durante l'acquisizione tramite S3 o Swift. Quando si attiva l'impostazione, tutti gli oggetti inseriti di recente vengono crittografati, ma non vengono apportate modifiche agli oggetti memorizzati esistenti. Se si disattiva la crittografia, gli oggetti attualmente crittografati rimangono crittografati, ma gli oggetti appena acquisiti non vengono crittografati.



Se si modifica questa impostazione, l'applicazione della nuova impostazione richiede circa un minuto. Il valore configurato viene memorizzato nella cache per le prestazioni e la scalabilità.

Gli oggetti memorizzati possono essere crittografati utilizzando l'algoritmo di crittografia AES-128 o AES-256.

L'impostazione crittografia oggetti memorizzati si applica solo agli oggetti S3 che non sono stati crittografati mediante crittografia a livello di bucket o a livello di oggetto.

Fasi

1. Selezionare **Configurazione Impostazioni di sistema Opzioni griglia**.
2. Nella sezione Stored Object Options, impostare l'opzione Stored Object Encryption su **None** (Nessuna) (impostazione predefinita), **AES-128** o **AES-256**.

Stored Object Options

Compress Stored Objects ?

Stored Object Encryption None AES-128 AES-256

Stored Object Hashing SHA-1 SHA-256

3. Fare clic su **Save** (Salva).

Configurazione dell'hashing degli oggetti memorizzati

L'opzione di hashing degli oggetti memorizzati specifica l'algoritmo di hashing utilizzato per verificare l'integrità degli oggetti.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

A proposito di questa attività

Per impostazione predefinita, i dati degli oggetti vengono hash utilizzando l'algoritmo SHA-1. L'algoritmo SHA-256 richiede risorse CPU aggiuntive e generalmente non è consigliato per la verifica dell'integrità.



Se si modifica questa impostazione, l'applicazione della nuova impostazione richiede circa un minuto. Il valore configurato viene memorizzato nella cache per le prestazioni e la scalabilità.

Fasi

1. Selezionare **Configurazione Impostazioni di sistema Opzioni griglia**.
2. Nella sezione Stored Object Options, modificare l'hashing degli oggetti memorizzati in **SHA-1** (impostazione predefinita) o **SHA-256**.

Stored Object Options

Compress Stored Objects ?

Stored Object Encryption None AES-128 AES-256

Stored Object Hashing SHA-1 SHA-256

3. Fare clic su **Save** (Salva).

Impostazioni di configurazione del nodo di storage

Ogni nodo di storage utilizza una serie di impostazioni di configurazione e contatori.

Potrebbe essere necessario visualizzare le impostazioni correnti o reimpostare i contatori per cancellare gli allarmi (sistema precedente).



Ad eccezione di quando espressamente indicato nella documentazione, è necessario consultare il supporto tecnico prima di modificare le impostazioni di configurazione di Storage Node. Se necessario, è possibile reimpostare i contatori degli eventi per cancellare gli allarmi legacy.

Per accedere alle impostazioni di configurazione e ai contatori di un nodo di storage:

1. Selezionare **supporto > Strumenti > topologia griglia**.
2. Selezionare **Site Storage Node**.
3. Espandere il nodo di storage e selezionare il servizio o il componente.
4. Selezionare la scheda **Configurazione**.

Le seguenti tabelle riassumono le impostazioni di configurazione del nodo di storage.

LDR

Nome attributo	Codice	Descrizione
Stato HTTP	HSTE	Lo stato corrente del protocollo HTTP per S3, Swift e altro traffico StorageGRID interno: <ul style="list-style-type: none">• Offline: Non sono consentite operazioni e qualsiasi applicazione client che tenta di aprire una sessione HTTP al servizio LDR riceve un messaggio di errore. Le sessioni attive vengono normalmente chiuse.• Online: Il funzionamento continua normalmente
Avvio automatico HTTP	HTA	<ul style="list-style-type: none">• Se selezionata, lo stato del sistema al riavvio dipende dallo stato del componente LDR Storage. Se il componente LDR Storage è di sola lettura al riavvio, anche l'interfaccia HTTP è di sola lettura. Se il componente LDR Storage è Online, anche HTTP è Online. In caso contrario, l'interfaccia HTTP rimane in stato Offline.• Se l'opzione non è selezionata, l'interfaccia HTTP rimane offline fino a quando non viene attivata esplicitamente.

Data store LDR

Nome attributo	Codice	Descrizione
Ripristina conteggio oggetti persi	RCOR	Ripristina il contatore per il numero di oggetti persi su questo servizio.

Storage LDR

Nome attributo	Codice	Descrizione
Stato di storage — desiderato	SSD	<p>Un'impostazione configurabile dall'utente per lo stato desiderato del componente di storage. Il servizio LDR legge questo valore e tenta di corrispondere allo stato indicato da questo attributo. Il valore è persistente durante i riavvii.</p> <p>Ad esempio, è possibile utilizzare questa impostazione per forzare lo storage a diventare di sola lettura anche in presenza di ampio spazio di storage disponibile. Questo può essere utile per la risoluzione dei problemi.</p> <p>L'attributo può assumere uno dei seguenti valori:</p> <ul style="list-style-type: none">• Offline: Quando lo stato desiderato è offline, il servizio LDR porta il componente LDR Storage offline.• Sola lettura: Quando lo stato desiderato è di sola lettura, il servizio LDR sposta lo stato dello storage in sola lettura e interrompe l'accettazione del nuovo contenuto. Tenere presente che il contenuto potrebbe continuare a essere salvato nel nodo di storage per un breve periodo di tempo fino alla chiusura delle sessioni aperte.• Online: Lasciare il valore in Online durante le normali operazioni di sistema. Lo stato di storage — corrente del componente di storage viene impostato dinamicamente dal servizio in base alle condizioni del servizio LDR, ad esempio la quantità di spazio di storage a oggetti disponibile. Se lo spazio è basso, il componente diventa di sola lettura.
Timeout controllo stato di salute	STC	<p>Il limite di tempo in secondi entro il quale deve essere completato un test di controllo dello stato di salute per poter considerare un volume di storage integro. Modificare questo valore solo se richiesto dal supporto.</p>

Verifica LDR

Nome attributo	Codice	Descrizione
Ripristina numero oggetti mancanti	VCMI	<p>Ripristina il numero di oggetti mancanti rilevati (OMIS). Utilizzare solo al termine della verifica in primo piano. I dati degli oggetti replicati mancanti vengono ripristinati automaticamente dal sistema StorageGRID.</p>

Nome attributo	Codice	Descrizione
Verificare	FVOV	Selezionare gli archivi di oggetti su cui eseguire la verifica in primo piano.
Tasso di verifica	VPRI	Imposta la velocità con cui avviene la verifica in background. Vedere le informazioni sulla configurazione del tasso di verifica in background.
Ripristina numero oggetti corrotti	VCCR	Ripristinare il contatore per i dati degli oggetti replicati danneggiati rilevati durante la verifica in background. Questa opzione può essere utilizzata per eliminare la condizione di allarme OCOR (Corrupt Objects Detected). Per ulteriori informazioni, consultare le istruzioni per il monitoraggio e la risoluzione dei problemi di StorageGRID.
Elimina oggetti in quarantena	OQRT	<p>Eliminare gli oggetti corrotti dalla directory di quarantena, azzerare il numero di oggetti in quarantena e annullare l'allarme di rilevamento oggetti in quarantena (OQRT). Questa opzione viene utilizzata dopo il ripristino automatico degli oggetti corrotti da parte del sistema StorageGRID.</p> <p>Se viene attivato un allarme oggetti persi, il supporto tecnico potrebbe voler accedere agli oggetti in quarantena. In alcuni casi, gli oggetti in quarantena potrebbero essere utili per il ripristino dei dati o per il debug dei problemi sottostanti che hanno causato le copie degli oggetti corrotte.</p>

Codifica LDR Erasure

Nome attributo	Codice	Descrizione
Azzerare conteggio errori di scrittura	RSWF	Reimpostare il contatore per gli errori di scrittura dei dati degli oggetti con codifica erasure sul nodo di storage.
Il ripristino legge il numero di errori	RSRF	Reimpostare il contatore per gli errori di lettura dei dati degli oggetti con codifica erasure dal nodo di storage.
Ripristina Elimina numero di errori	RSDF	Reimpostare il contatore per gli errori di eliminazione dei dati degli oggetti con codifica erasure dal nodo di storage.
Ripristina numero copie corrotte rilevate	RSCC	Reimpostare il contatore per il numero di copie corrotte dei dati degli oggetti con codifica di cancellazione sul nodo di storage.

Nome attributo	Codice	Descrizione
Ripristina numero di frammenti corrotti rilevati	RSCD	Reimpostare il contatore per i frammenti corrotti di dati di oggetti con codifica di cancellazione sul nodo di storage.
Ripristina numero frammenti mancanti rilevati	RSMD	Reimpostare il contatore per i frammenti mancanti di dati di oggetti con codifica di cancellazione sul nodo di storage. Utilizzare solo al termine della verifica in primo piano.

Replica LDR

Nome attributo	Codice	Descrizione
Ripristina conteggio errori replica in entrata	RIC	Reimpostare il contatore per gli errori di replica in entrata. Questa opzione può essere utilizzata per cancellare l'allarme RIRF (Inbound Replication — Failed).
Ripristina conteggio errori replica in uscita	ROCR	Reimpostare il contatore per gli errori di replica in uscita. Questa opzione può essere utilizzata per cancellare l'allarme RORF (Outbound Replications — Failed).
Disattiva replica in entrata	DSIR	<p>Selezionare questa opzione per disattivare la replica in entrata come parte di una procedura di manutenzione o test. Lasciare deselezionato durante il normale funzionamento.</p> <p>Quando la replica in entrata è disattivata, gli oggetti possono essere recuperati dal nodo di storage per la copia in altre posizioni nel sistema StorageGRID, ma gli oggetti non possono essere copiati in questo nodo di storage da altre posizioni: Il servizio LDR è di sola lettura.</p>
Disattiva la replica in uscita	DSOR	<p>Selezionare questa opzione per disattivare la replica in uscita (incluse le richieste di contenuto per i retrievals HTTP) come parte di una procedura di manutenzione o test. Lasciare deselezionato durante il normale funzionamento.</p> <p>Quando la replica in uscita è disattivata, gli oggetti possono essere copiati in questo nodo di storage, ma non possono essere recuperati dal nodo di storage per essere copiati in altre posizioni nel sistema StorageGRID. Il servizio LDR è di sola scrittura.</p>

Informazioni correlate

["Monitor risoluzione dei problemi"](#)

Gestione dei nodi di storage completi

Man mano che i nodi di storage raggiungono la capacità, è necessario espandere il sistema StorageGRID con l'aggiunta di nuovo storage. Sono disponibili tre opzioni: Aggiunta di volumi di storage, aggiunta di shelf di espansione dello storage e aggiunta di nodi di storage.

Aggiunta di volumi di storage

Ciascun nodo di storage supporta un numero massimo di volumi di storage. Il valore massimo definito varia in base alla piattaforma. Se un nodo di storage contiene meno del numero massimo di volumi di storage, è possibile aggiungere volumi per aumentarne la capacità. Consultare le istruzioni per espandere un sistema StorageGRID.

Aggiunta di shelf di espansione dello storage

Alcuni nodi storage dell'appliance StorageGRID, come SG6060, possono supportare shelf di storage aggiuntivi. Se si dispone di appliance StorageGRID con funzionalità di espansione che non sono già state estese alla capacità massima, è possibile aggiungere shelf di storage per aumentare la capacità. Consultare le istruzioni per espandere un sistema StorageGRID.

Aggiunta di nodi di storage

È possibile aumentare la capacità dello storage aggiungendo nodi di storage. Quando si aggiunge lo storage, è necessario prendere in considerazione le regole ILM attualmente attive e i requisiti di capacità. Consultare le istruzioni per espandere un sistema StorageGRID.

Informazioni correlate

["Espandi il tuo grid"](#)

Gestione dei nodi di amministrazione

Ogni sito in un'implementazione StorageGRID può avere uno o più nodi di amministrazione.

- ["Che cos'è un nodo amministratore"](#)
- ["Utilizzo di più nodi di amministrazione"](#)
- ["Identificazione del nodo di amministrazione primario"](#)
- ["Selezione di un mittente preferito"](#)
- ["Visualizzazione dello stato delle notifiche e delle code"](#)
- ["Modalità di visualizzazione degli allarmi riconosciuti da Admin Node \(sistema legacy\)"](#)
- ["Configurazione dell'accesso al client di controllo"](#)

Che cos'è un nodo amministratore

I nodi di amministrazione forniscono servizi di gestione quali configurazione, monitoraggio e registrazione del sistema. Ogni grid deve avere un nodo di amministrazione primario e può avere un numero qualsiasi di nodi di amministrazione non primari per la ridondanza.

Quando si accede a Grid Manager o al tenant Manager, si sta effettuando la connessione a un nodo amministratore. È possibile connettersi a qualsiasi nodo amministratore e ciascun nodo amministratore visualizza una vista simile del sistema StorageGRID. Tuttavia, le procedure di manutenzione devono essere eseguite utilizzando il nodo di amministrazione primario.

I nodi di amministrazione possono anche essere utilizzati per bilanciare il carico del traffico dei client S3 e Swift.

I nodi di amministrazione ospitano i seguenti servizi:

- Servizio AMS
- Servizio CMN
- Servizio NMS
- Servizio Prometheus
- Servizi Load Balancer e High Availability (per supportare il traffico client S3 e Swift)

I nodi di amministrazione supportano anche la Management Application Program Interface (Mgmt-api) per elaborare le richieste provenienti dall'API Grid Management e dall'API Tenant Management.

Che cos'è il servizio AMS

Il servizio Audit Management System (AMS) tiene traccia dell'attività e degli eventi del sistema.

Che cos'è il servizio CMN

Il servizio CMN (Configuration Management Node) gestisce le configurazioni a livello di sistema di connettività e le funzionalità di protocollo necessarie a tutti i servizi. Inoltre, il servizio CMN viene utilizzato per eseguire e monitorare le attività della griglia. Esiste un solo servizio CMN per implementazione StorageGRID. Il nodo di amministrazione che ospita il servizio CMN è noto come nodo di amministrazione primario.

Che cos'è il servizio NMS

Il servizio del sistema di gestione della rete (NMS) alimenta le opzioni di monitoraggio, reporting e configurazione visualizzate tramite Grid Manager, l'interfaccia basata su browser del sistema StorageGRID.

Che cos'è il servizio Prometheus

Il servizio Prometheus raccoglie le metriche delle serie temporali dai servizi su tutti i nodi.

Informazioni correlate

["Utilizzando l'API Grid Management"](#)

["Utilizzare un account tenant"](#)

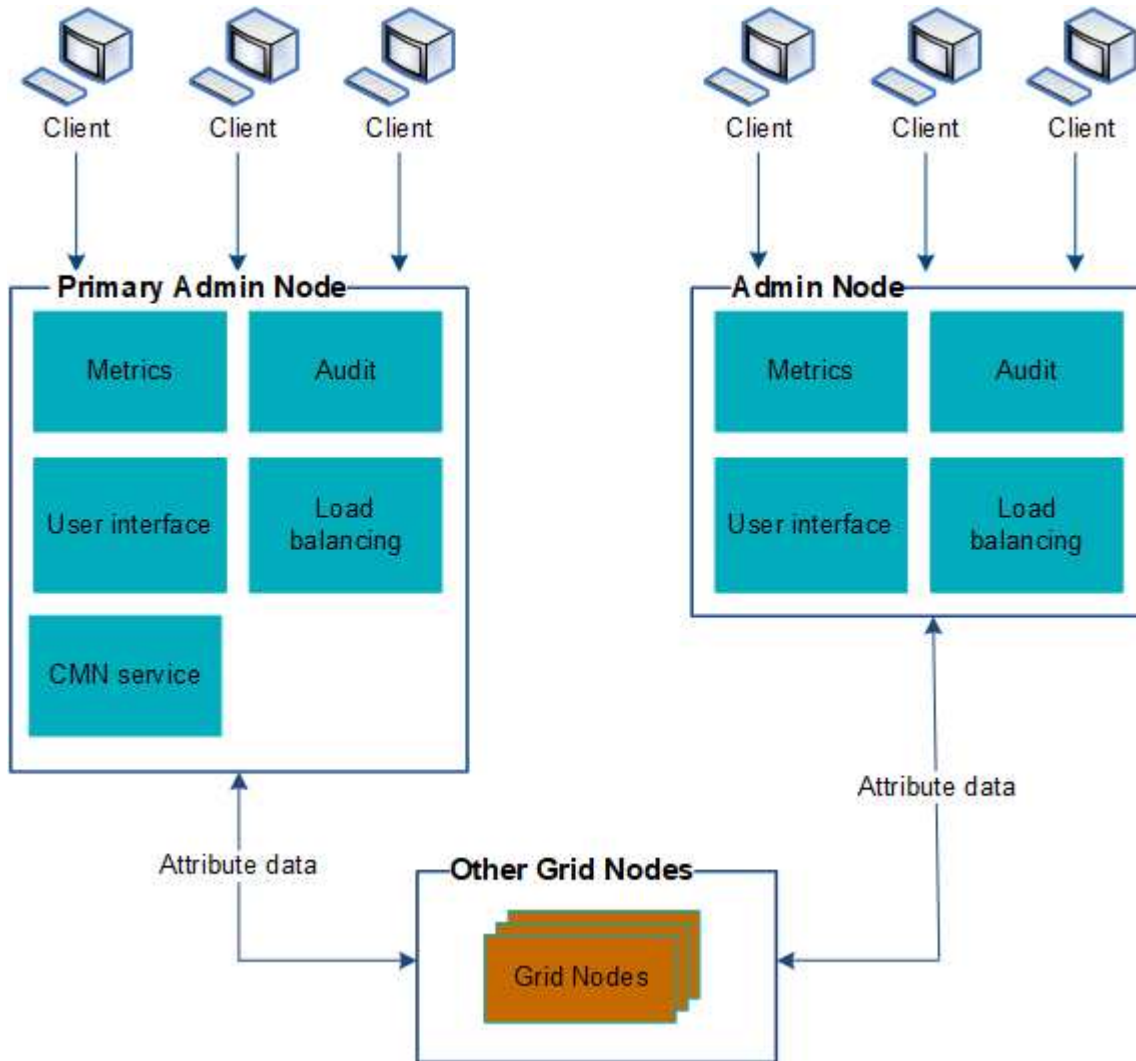
["Gestione del bilanciamento del carico"](#)

["Gestione di gruppi ad alta disponibilità"](#)

Utilizzo di più nodi di amministrazione

Un sistema StorageGRID può includere più nodi di amministrazione per consentire di monitorare e configurare continuamente il sistema StorageGRID anche in caso di guasto di un nodo di amministrazione.

Se un nodo amministratore non è più disponibile, l'elaborazione degli attributi continua, gli avvisi e gli allarmi (sistema legacy) vengono ancora attivati e le notifiche e-mail e i messaggi AutoSupport vengono ancora inviati. Tuttavia, la presenza di più nodi di amministrazione non fornisce la protezione di failover ad eccezione delle notifiche e dei messaggi AutoSupport. In particolare, le conferme di allarme effettuate da un nodo di amministrazione non vengono copiate in altri nodi di amministrazione.



Sono disponibili 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 Admin disponibile.
- Se un amministratore di sistema ha configurato un gruppo di nodi di amministrazione ad alta disponibilità, i client Web possono continuare ad accedere a Grid Manager o a Tenant Manager utilizzando l'indirizzo IP virtuale del gruppo ha.



Quando si utilizza un gruppo ha, l'accesso viene interrotto se il nodo di amministrazione master non riesce. Gli utenti devono effettuare nuovamente l'accesso dopo il failover dell'indirizzo IP virtuale del gruppo ha verso un altro nodo amministratore del gruppo.

Alcune attività di manutenzione possono essere eseguite solo utilizzando il nodo di amministrazione primario. In caso di guasto del nodo amministratore primario, è necessario ripristinarlo prima che il sistema StorageGRID funzioni nuovamente.

Informazioni correlate

["Gestione di gruppi ad alta disponibilità"](#)

Identificazione del nodo di amministrazione primario

Il nodo di amministrazione primario ospita il servizio CMN. Alcune procedure di manutenzione possono essere eseguite solo utilizzando il nodo di amministrazione primario.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

Fasi

1. Selezionare **supporto > Strumenti > topologia griglia**.
2. Selezionare **Site Admin Node**, quindi fare clic su **+** Per espandere la struttura della topologia e mostrare i servizi ospitati su questo nodo di amministrazione.

Il nodo di amministrazione primario ospita il servizio CMN.

3. Se questo nodo di amministrazione non ospita il servizio CMN, controllare gli altri nodi di amministrazione.

Selezione di un mittente preferito

Se l'implementazione di StorageGRID include più nodi di amministrazione, è possibile selezionare quale nodo di amministrazione deve essere il mittente preferito delle notifiche. Per impostazione predefinita, viene selezionato il nodo di amministrazione principale, ma qualsiasi nodo di amministrazione può essere il mittente preferito.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

A proposito di questa attività

La pagina **Configurazione Impostazioni di sistema Opzioni di visualizzazione** mostra quale nodo amministratore è attualmente selezionato come mittente preferito. Per impostazione predefinita, viene selezionato il nodo di amministrazione principale.

Nelle normali operazioni di sistema, solo il mittente preferito invia le seguenti notifiche:

- Messaggi AutoSupport
- Notifiche SNMP
- E-mail di avviso
- Email di allarme (sistema legacy)

Tuttavia, tutti gli altri nodi di amministrazione (mittenti in standby) monitorano il mittente preferito. Se viene rilevato un problema, anche un mittente in standby può inviare queste notifiche.

Sia il mittente preferito che il mittente in standby potrebbero inviare notifiche nei seguenti casi:

- Se i nodi di amministrazione diventano “islanded” l’uno dall’altro, sia il mittente preferito che i mittenti di standby tenteranno di inviare notifiche e potrebbero essere ricevute più copie delle notifiche.
- Dopo che un mittente in standby rileva problemi con il mittente preferito e inizia a inviare notifiche, il mittente preferito potrebbe riacquistare la capacità di inviare notifiche. In questo caso, potrebbero essere inviate notifiche duplicate. Il mittente in standby interrompe l’invio di notifiche quando non rileva più errori sul mittente preferito.



Quando si testano le notifiche di allarme e i messaggi AutoSupport, tutti i nodi di amministrazione inviano l’email di test. Quando si verificano le notifiche di avviso, è necessario accedere a ogni nodo amministratore per verificare la connettività.

Fasi

1. Selezionare **Configurazione > Impostazioni di sistema > Opzioni di visualizzazione**.
2. Dal menu Display Options (Opzioni di visualizzazione), selezionare **Options** (Opzioni).
3. Selezionare il nodo Admin che si desidera impostare come mittente preferito dall’elenco a discesa.



Display Options

Updated: 2017-08-30 16:31:10 MDT

Current Sender	ADMIN-DC1-ADM1
Preferred Sender	ADMIN-DC1-ADM1
GUI Inactivity Timeout	900
Notification Suppress All	<input type="checkbox"/>

Apply Changes

4. Fare clic su **Applica modifiche**.

L’Admin Node viene impostato come mittente preferito delle notifiche.


Visualizzazione dello stato delle notifiche e delle code



Il servizio NMS sui nodi di amministrazione invia notifiche al server di posta. È possibile visualizzare lo stato corrente del servizio NMS e le dimensioni della relativa coda di notifica nella pagina motore interfaccia.



Per accedere alla pagina Interface Engine, selezionare **Support Tools Grid Topology**. Infine, selezionare **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 %  

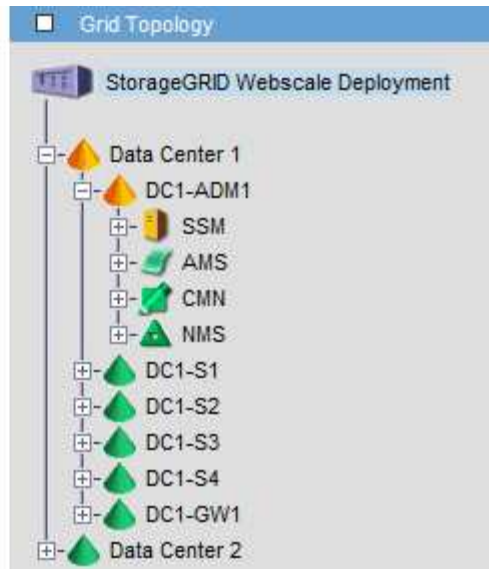
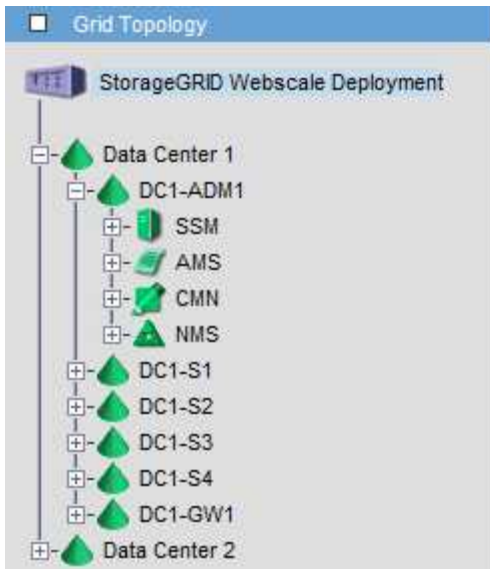
Active Connections: 5  

Le notifiche vengono elaborate tramite la coda di notifica 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, il tentativo più efficace di inviare nuovamente la notifica al server di posta continua per un periodo di 60 secondi. Se la notifica non viene inviata al server di posta dopo 60 secondi, la notifica viene interrotta dalla coda di notifica e viene eseguito un tentativo di invio della notifica successiva nella coda. Poiché le notifiche possono essere interrotte dalla coda delle notifiche senza essere inviate, è possibile che un allarme possa essere attivato senza l'invio di una notifica. Nel caso in cui una notifica venga interrotta dalla coda senza essere inviata, viene attivato l'allarme minore MINUTI (Stato notifica e-mail).

Modalità di visualizzazione degli allarmi riconosciuti da Admin Node (sistema legacy)

Quando si riconosce un allarme su un nodo di amministrazione, l'allarme confermato non viene copiato in nessun altro nodo di amministrazione. Poiché i riconoscimenti non vengono copiati in altri nodi di amministrazione, l'albero topologia griglia potrebbe non avere lo stesso aspetto per ciascun nodo di amministrazione.

Questa differenza può essere utile quando si connettono client web. I client Web possono avere viste diverse del sistema StorageGRID in base alle esigenze dell'amministratore.



Si noti che le notifiche vengono inviate dal nodo di amministrazione in cui si verifica la conferma.

Configurazione dell'accesso al client di controllo

Il nodo di amministrazione, tramite il servizio Audit Management System (AMS), registra tutti gli eventi di sistema controllati in un file di registro disponibile attraverso la condivisione dell'audit, che viene aggiunto a ciascun nodo di amministrazione al momento dell'installazione. Per un facile accesso ai registri di audit, è possibile configurare l'accesso client per le condivisioni di audit per CIFS e NFS.

Il sistema StorageGRID utilizza il riconoscimento positivo per impedire la perdita dei messaggi di audit prima che vengano scritti nel file di log. Un messaggio rimane in coda in un servizio fino a quando il servizio AMS o un servizio di inoltro di audit intermedio non ne ha riconosciuto il controllo.

Per ulteriori informazioni, consultare le istruzioni relative ai messaggi di audit.



Se hai la possibilità di utilizzare CIFS o NFS, scegli NFS.



L'esportazione dell'audit tramite CIFS/Samba è stata deprecata e verrà rimossa in una release futura di StorageGRID.

Informazioni correlate

["Che cos'è un nodo amministratore"](#)

["Esaminare i registri di audit"](#)

["Aggiornare il software"](#)

Configurazione dei client di audit per CIFS

La procedura utilizzata per configurare un client di audit dipende dal metodo di autenticazione: Windows Workgroup o Windows Active Directory (ad). Una volta aggiunta, la condivisione di controllo viene attivata automaticamente come condivisione di sola lettura.



L'esportazione dell'audit tramite CIFS/Samba è stata deprecata e verrà rimossa in una release futura di StorageGRID.

Informazioni correlate

["Aggiornare il software"](#)

Configurazione dei client di audit per Workgroup

Eseguire questa procedura per ogni nodo amministratore in un'implementazione StorageGRID da cui si desidera recuperare i messaggi di controllo.

Di cosa hai bisogno

- È necessario disporre di `Passwords.txt` File con la password dell'account root/admin (disponibile nel pacchetto).
- È necessario disporre di `Configuration.txt` File (disponibile in DETTO pacchetto).

A proposito di questa attività

L'esportazione dell'audit tramite CIFS/Samba è stata deprecata e verrà rimossa in una release futura di StorageGRID.

Fasi

1. Accedere al nodo di amministrazione principale:
 - a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
 - b. Immettere la password elencata in `Passwords.txt` file.
 - c. Immettere il seguente comando per passare a root: `su -`
 - d. Immettere la password elencata in `Passwords.txt` file.

Una volta effettuato l'accesso come root, il prompt cambia da `$` a `#`.

2. Verificare che tutti i servizi abbiano uno stato di esecuzione o verificato: `storagegrid-status`

Se tutti i servizi non sono in esecuzione o verificati, risolvere i problemi prima di continuare.

3. Tornare alla riga di comando, premere **Ctrl+C**.
4. Avviare l'utility di configurazione CIFS: `config_cifs.rb`

Shares	Authentication	Config
add-audit-share	set-authentication	validate-config
enable-disable-share	set-netbios-name	help
add-user-to-share	join-domain	exit
remove-user-from-share	add-password-server	
modify-group	remove-password-server	
	add-wins-server	
	remove-wins-server	

5. Impostare l'autenticazione per Windows Workgroup:

Se l'autenticazione è già stata impostata, viene visualizzato un messaggio di avviso. Se l'autenticazione è già stata impostata, passare alla fase successiva.

- Inserire: `set-authentication`
- Quando viene richiesto di installare Windows Workgroup o Active Directory, immettere: `workgroup`
- Quando richiesto, immettere un nome per il gruppo di lavoro: `workgroup_name`
- Quando richiesto, creare un nome NetBIOS significativo: `netbios_name`

oppure

Premere **Invio** per utilizzare il nome host del nodo di amministrazione come nome NetBIOS.

Lo script riavvia il server Samba e le modifiche vengono applicate. Questa operazione dovrebbe richiedere meno di un minuto. Dopo aver impostato l'autenticazione, aggiungere un client di audit.

- Quando richiesto, premere **Invio**.

Viene visualizzata l'utility di configurazione CIFS.

6. Aggiungere un client di audit:

- Inserire: `add-audit-share`



La condivisione viene aggiunta automaticamente in sola lettura.

- Quando richiesto, aggiungere un utente o un gruppo: `user`
- Quando richiesto, inserire il nome utente per l'audit: `audit_user_name`
- Quando richiesto, inserire una password per l'utente di controllo: `password`
- Quando richiesto, immettere nuovamente la stessa password per confermarla: `password`
- Quando richiesto, premere **Invio**.

Viene visualizzata l'utility di configurazione CIFS.



Non è necessario inserire una directory. Il nome della directory di controllo è predefinito.

7. Se più di un utente o gruppo è autorizzato ad accedere alla condivisione di controllo, aggiungere gli utenti aggiuntivi:

a. Inserire: `add-user-to-share`

Viene visualizzato un elenco numerato di condivisioni abilitate.

b. Quando richiesto, inserire il numero della condivisione audit-export: `share_number`

c. Quando richiesto, aggiungere un utente o un gruppo: `user`

oppure `group`

d. Quando richiesto, inserire il nome dell'utente o del gruppo di controllo: `audit_user` or `audit_group`

e. Quando richiesto, premere **Invio**.

Viene visualizzata l'utility di configurazione CIFS.

f. Ripetere questi passaggi secondari per ogni utente o gruppo aggiuntivo che ha accesso alla condivisione di controllo.

8. In alternativa, verificare la configurazione: `validate-config`

I servizi vengono controllati e visualizzati. È possibile ignorare i seguenti messaggi:

```
Can't find include file /etc/samba/includes/cifs-interfaces.inc
Can't find include file /etc/samba/includes/cifs-filesystem.inc
Can't find include file /etc/samba/includes/cifs-custom-config.inc
Can't find include file /etc/samba/includes/cifs-shares.inc
rlimit_max: increasing rlimit_max (1024) to minimum Windows limit
(16384)
```

a. Quando richiesto, premere **Invio**.

Viene visualizzata la configurazione del client di audit.

b. Quando richiesto, premere **Invio**.

Viene visualizzata l'utility di configurazione CIFS.

9. Chiudere l'utilità di configurazione CIFS: `exit`

10. Avviare il servizio Samba: `service smb start`

11. Se l'implementazione di StorageGRID è un singolo sito, passare alla fase successiva.

oppure

Facoltativamente, se l'implementazione di StorageGRID include nodi di amministrazione in altri siti, attivare questa condivisione di controllo come richiesto:

- a. Accedere in remoto al nodo di amministrazione di un sito:
 - i. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - ii. Immettere la password elencata in `Passwords.txt` file.
 - iii. Immettere il seguente comando per passare a root: `su -`
 - iv. Immettere la password elencata in `Passwords.txt` file.
- b. Ripetere la procedura per configurare la condivisione di controllo per ogni nodo amministrativo aggiuntivo.
- c. Chiudere l'accesso remoto sicuro alla shell nel nodo di amministrazione remoto: `exit`

12. Disconnettersi dalla shell dei comandi: `exit`

Informazioni correlate

["Aggiornare il software"](#)

Configurazione dei client di audit per Active Directory

Eseguire questa procedura per ogni nodo amministratore in un'implementazione StorageGRID da cui si desidera recuperare i messaggi di controllo.

Di cosa hai bisogno

- È necessario disporre di `Passwords.txt` File con la password dell'account root/admin (disponibile nel pacchetto).
- È necessario disporre del nome utente e della password di CIFS Active Directory.
- È necessario disporre di `Configuration.txt` File (disponibile in DETTO pacchetto).



L'esportazione dell'audit tramite CIFS/Samba è stata deprecata e verrà rimossa in una release futura di StorageGRID.

Fasi

1. Accedere al nodo di amministrazione principale:
 - a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
 - b. Immettere la password elencata in `Passwords.txt` file.
 - c. Immettere il seguente comando per passare a root: `su -`
 - d. Immettere la password elencata in `Passwords.txt` file.

Una volta effettuato l'accesso come root, il prompt cambia da `$` a `#`.

2. Verificare che tutti i servizi abbiano uno stato di esecuzione o verificato: `storagegrid-status`

Se tutti i servizi non sono in esecuzione o verificati, risolvere i problemi prima di continuare.

3. Tornare alla riga di comando, premere **Ctrl+C**.
4. Avviare l'utility di configurazione CIFS: `config_cifs.rb`

Shares	Authentication	Config
add-audit-share	set-authentication	validate-config
enable-disable-share	set-netbios-name	help
add-user-to-share	join-domain	exit
remove-user-from-share	add-password-server	
modify-group	remove-password-server	
	add-wins-server	
	remove-wins-server	

5. Impostare l'autenticazione per Active Directory: `set-authentication`

Nella maggior parte delle implementazioni, è necessario impostare l'autenticazione prima di aggiungere il client di audit. Se l'autenticazione è già stata impostata, viene visualizzato un messaggio di avviso. Se l'autenticazione è già stata impostata, passare alla fase successiva.

- Quando viene richiesto di installare Workgroup o Active Directory: `ad`
- Quando richiesto, inserire il nome del dominio `ad` (nome di dominio breve).
- Quando richiesto, inserire l'indirizzo IP o il nome host DNS del controller di dominio.
- Quando richiesto, inserire il nome completo del dominio.

Utilizzare lettere maiuscole.

- Quando viene richiesto di attivare il supporto winbind, digitare `y`.

Winbind viene utilizzato per risolvere le informazioni di utenti e gruppi dai server `ad`.

- Quando richiesto, inserire il nome NetBIOS.
- Quando richiesto, premere **Invio**.

Viene visualizzata l'utility di configurazione CIFS.

6. Unirsi al dominio:

- Se non è già stato avviato, avviare l'utility di configurazione CIFS: `config_cifs.rb`
- Unirsi al dominio: `join-domain`
- Viene richiesto di verificare se l'Admin Node è attualmente un membro valido del dominio. Se questo nodo di amministrazione non ha precedentemente aderito al dominio, immettere: `no`
- Quando richiesto, fornire il nome utente dell'amministratore: `administrator_username`

dove `administrator_username` È il nome utente di CIFS Active Directory, non il nome utente di StorageGRID.

- Quando richiesto, fornire la password dell'amministratore: `administrator_password`

erano `administrator_password` È il nome utente di CIFS Active Directory, non la password di

StorageGRID.

- f. Quando richiesto, premere **Invio**.

Viene visualizzata l'utility di configurazione CIFS.

7. Verificare di aver inserito correttamente il dominio:

- a. Unirsi al dominio: `join-domain`

- b. Quando viene richiesto di verificare se il server è attualmente un membro valido del dominio, immettere: `y`

Se viene visualizzato il messaggio "Join is OK," significa che l'accesso al dominio è stato eseguito correttamente. Se non si ottiene questa risposta, provare a impostare nuovamente l'autenticazione e ad accedere al dominio.

- c. Quando richiesto, premere **Invio**.

Viene visualizzata l'utility di configurazione CIFS.

8. Aggiungere un client di audit: `add-audit-share`

- a. Quando viene richiesto di aggiungere un utente o un gruppo, immettere: `user`

- b. Quando viene richiesto di inserire il nome utente per l'audit, inserire il nome utente per l'audit.

- c. Quando richiesto, premere **Invio**.

Viene visualizzata l'utility di configurazione CIFS.

9. Se più di un utente o gruppo è autorizzato ad accedere alla condivisione di controllo, aggiungere altri utenti: `add-user-to-share`

Viene visualizzato un elenco numerato di condivisioni abilitate.

- a. Inserire il numero della condivisione `audit-export`.

- b. Quando viene richiesto di aggiungere un utente o un gruppo, immettere: `group`

Viene richiesto il nome del gruppo di audit.

- c. Quando viene richiesto il nome del gruppo di audit, immettere il nome del gruppo di utenti di audit.

- d. Quando richiesto, premere **Invio**.

Viene visualizzata l'utility di configurazione CIFS.

- e. Ripetere questo passaggio per ogni utente o gruppo aggiuntivo che ha accesso alla condivisione di controllo.

10. In alternativa, verificare la configurazione: `validate-config`

I servizi vengono controllati e visualizzati. È possibile ignorare i seguenti messaggi:

- Impossibile trovare il file di inclusione `/etc/samba/includes/cifs-interfaces.inc`
- Impossibile trovare il file di inclusione `/etc/samba/includes/cifs-filesystem.inc`

- Impossibile trovare il file di inclusione `/etc/samba/includes/cifs-interfaces.inc`
- Impossibile trovare il file di inclusione `/etc/samba/includes/cifs-custom-config.inc`
- Impossibile trovare il file di inclusione `/etc/samba/includes/cifs-shares.inc`
- `Rlimit_max`: Aumento di `rlimit_max` (1024) al limite minimo di Windows (16384)



Non combinare l'impostazione 'security=ads' con il parametro 'password server'. (Per impostazione predefinita, Samba rileverà automaticamente il DC corretto da contattare).

- i. Quando richiesto, premere **Invio** per visualizzare la configurazione del client di controllo.
- ii. Quando richiesto, premere **Invio**.

Viene visualizzata l'utilità di configurazione CIFS.

11. Chiudere l'utilità di configurazione CIFS: `exit`

12. Se l'implementazione di StorageGRID è un singolo sito, passare alla fase successiva.

oppure

Facoltativamente, se l'implementazione di StorageGRID include nodi di amministrazione in altri siti, abilitare queste condivisioni di controllo come richiesto:

- a. Accedere in remoto al nodo di amministrazione di un sito:
 - i. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - ii. Immettere la password elencata in `Passwords.txt` file.
 - iii. Immettere il seguente comando per passare a root: `su -`
 - iv. Immettere la password elencata in `Passwords.txt` file.
- b. Ripetere questa procedura per configurare le condivisioni di controllo per ciascun nodo di amministrazione.
- c. Chiudere l'accesso remoto sicuro alla shell nel nodo di amministrazione: `exit`

13. Disconnettersi dalla shell dei comandi: `exit`

Informazioni correlate

["Aggiornare il software"](#)

Aggiunta di un utente o di un gruppo a una condivisione di audit CIFS

È possibile aggiungere un utente o un gruppo a una condivisione di audit CIFS integrata con l'autenticazione ad.

Di cosa hai bisogno

- È necessario disporre di `Passwords.txt` File con la password dell'account root/admin (disponibile nel pacchetto).
- È necessario disporre di `Configuration.txt` File (disponibile in DETTO pacchetto).

A proposito di questa attività

La seguente procedura riguarda una condivisione di controllo integrata con l'autenticazione ad.



L'esportazione dell'audit tramite CIFS/Samba è stata deprecata e verrà rimossa in una release futura di StorageGRID.

Fasi

1. Accedere al nodo di amministrazione principale:

- Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
- Immettere la password elencata in `Passwords.txt` file.
- Immettere il seguente comando per passare a root: `su -`
- Immettere la password elencata in `Passwords.txt` file.

Una volta effettuato l'accesso come root, il prompt cambia da `$` a `#`.

2. Verificare che tutti i servizi abbiano uno stato di esecuzione o verificato. Inserire: `storagegrid-status`

Se tutti i servizi non sono in esecuzione o verificati, risolvere i problemi prima di continuare.

3. Tornare alla riga di comando, premere **Ctrl+C**.

4. Avviare l'utility di configurazione CIFS: `config_cifs.rb`

```
-----  
| Shares                | Authentication          | Config                  |  
-----  
| add-audit-share       | set-authentication      | validate-config        |  
| enable-disable-share  | set-netbios-name       | help                   |  
| add-user-to-share     | join-domain            | exit                   |  
| remove-user-from-share| add-password-server    |                        |  
| modify-group          | remove-password-server |                        |  
|                       | add-wins-server        |                        |  
|                       | remove-wins-server     |                        |  
-----
```

5. Iniziare ad aggiungere un utente o un gruppo: `add-user-to-share`

Viene visualizzato un elenco numerato di condivisioni di controllo configurate.

6. Quando richiesto, inserire il numero per la condivisione dell'audit (audit-export): `audit_share_number`

Viene richiesto se si desidera concedere a un utente o a un gruppo l'accesso a questa condivisione di controllo.

7. Quando richiesto, aggiungere un utente o un gruppo: `user` oppure `group`

8. Quando viene richiesto il nome dell'utente o del gruppo per questa condivisione di audit ad, immettere il nome.

L'utente o il gruppo viene aggiunto in sola lettura per la condivisione di controllo sia nel sistema operativo

del server che nel servizio CIFS. La configurazione di Samba viene ricaricata per consentire all'utente o al gruppo di accedere alla condivisione del client di audit.

9. Quando richiesto, premere **Invio**.

Viene visualizzata l'utility di configurazione CIFS.

10. Ripetere questa procedura per ogni utente o gruppo che ha accesso alla condivisione di controllo.

11. In alternativa, verificare la configurazione: `validate-config`

I servizi vengono controllati e visualizzati. È possibile ignorare i seguenti messaggi:

- Impossibile trovare il file include `/etc/samba/includes/cifs-interfaces.inc`
- Impossibile trovare il file include `/etc/samba/includes/cifs-filesystem.inc`
- Impossibile trovare il file include `/etc/samba/includes/cifs-custom-config.inc`
- Impossibile trovare il file include `/etc/samba/includes/cifs-shares.inc`
 - i. Quando richiesto, premere **Invio** per visualizzare la configurazione del client di controllo.
 - ii. Quando richiesto, premere **Invio**.

12. Chiudere l'utilità di configurazione CIFS: `exit`

13. Determinare se è necessario attivare ulteriori condivisioni di audit, come segue:

- Se l'implementazione di StorageGRID è un singolo sito, passare alla fase successiva.
- Se l'implementazione di StorageGRID include nodi di amministrazione in altri siti, abilitare queste condivisioni di controllo come richiesto:
 - i. Accedere in remoto al nodo di amministrazione di un sito:
 - A. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - B. Immettere la password elencata in `Passwords.txt` file.
 - C. Immettere il seguente comando per passare a root: `su -`
 - D. Immettere la password elencata in `Passwords.txt` file.
 - ii. Ripetere questa procedura per configurare le condivisioni di controllo per ciascun nodo di amministrazione.
 - iii. Chiudere l'accesso remoto sicuro alla shell nel nodo di amministrazione remoto: `exit`

14. Disconnettersi dalla shell dei comandi: `exit`

Rimozione di un utente o di un gruppo da una condivisione di audit CIFS

Non è possibile rimuovere l'ultimo utente o gruppo autorizzato ad accedere alla condivisione di controllo.

Di cosa hai bisogno

- È necessario disporre di `Passwords.txt` File con le password dell'account root (disponibili in DETTO pacchetto).
- È necessario disporre di `Configuration.txt` File (disponibile in DETTO pacchetto).

A proposito di questa attività

L'esportazione dell'audit tramite CIFS/Samba è stata deprecata e verrà rimossa in una release futura di StorageGRID.

Fasi

1. Accedere al nodo di amministrazione principale:

- Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
- Immettere la password elencata in `Passwords.txt` file.
- Immettere il seguente comando per passare a root: `su -`
- Immettere la password elencata in `Passwords.txt` file.

Una volta effettuato l'accesso come root, il prompt cambia da `$` a `#`.

2. Avviare l'utility di configurazione CIFS: `config_cifs.rb`

```
-----  
| Shares                | Authentication          | Config                  |  
-----  
| add-audit-share       | set-authentication      | validate-config        |  
| enable-disable-share  | set-netbios-name       | help                   |  
| add-user-to-share     | join-domain            | exit                   |  
| remove-user-from-share | add-password-server    |                         |  
| modify-group          | remove-password-server |                         |  
|                       | add-wins-server        |                         |  
|                       | remove-wins-server     |                         |  
-----
```

3. Iniziare a rimuovere un utente o un gruppo: `remove-user-from-share`

Viene visualizzato un elenco numerato delle condivisioni di audit disponibili per il nodo di amministrazione. La condivisione dell'audit è etichettata `audit-export`.

4. Inserire il numero della condivisione di controllo: `audit_share_number`

5. Quando viene richiesto di rimuovere un utente o un gruppo: `user` oppure `group`

Viene visualizzato un elenco numerato di utenti o gruppi per la condivisione dell'audit.

6. Inserire il numero corrispondente all'utente o al gruppo che si desidera rimuovere: `number`

La condivisione di controllo viene aggiornata e l'utente o il gruppo non può più accedere alla condivisione di controllo. Ad esempio:

```
Enabled shares
 1. audit-export
Select the share to change: 1
Remove user or group? [User/group]: User
Valid users for this share
 1. audituser
 2. newaudituser
Select the user to remove: 1

Removed user "audituser" from share "audit-export".

Press return to continue.
```

7. Chiudere l'utilità di configurazione CIFS: `exit`
8. Se l'implementazione di StorageGRID include nodi di amministrazione in altri siti, disattivare la condivisione di controllo in ciascun sito secondo necessità.
9. Disconnettersi da ogni shell dei comandi al termine della configurazione: `exit`

Informazioni correlate

["Aggiornare il software"](#)

Modifica del nome di un utente o di un gruppo di condivisione dell'audit CIFS

È possibile modificare il nome di un utente o di un gruppo per una condivisione di audit CIFS aggiungendo un nuovo utente o gruppo ed eliminando quello precedente.

A proposito di questa attività

L'esportazione dell'audit tramite CIFS/Samba è stata deprecata e verrà rimossa in una release futura di StorageGRID.

Fasi

1. Aggiungere un nuovo utente o gruppo con il nome aggiornato alla condivisione di controllo.
2. Eliminare il vecchio nome utente o gruppo.

Informazioni correlate

["Aggiornare il software"](#)

["Aggiunta di un utente o di un gruppo a una condivisione di audit CIFS"](#)

["Rimozione di un utente o di un gruppo da una condivisione di audit CIFS"](#)

Verifica dell'integrazione dell'audit CIFS

La condivisione dell'audit è di sola lettura. I file di log devono essere letti dalle applicazioni del computer e la verifica non include l'apertura di un file. Si ritiene sufficiente verificare che i file di registro di controllo vengano visualizzati in una finestra di Esplora risorse. Dopo la verifica della connessione, chiudere tutte le finestre.

Configurazione del client di audit per NFS

La condivisione di controllo viene attivata automaticamente come condivisione di sola lettura.

Di cosa hai bisogno

- È necessario disporre di `Passwords.txt` File con la password root/admin (disponibile nel pacchetto).
- È necessario disporre di `Configuration.txt` File (disponibile in DETTO pacchetto).
- Il client di audit deve utilizzare NFS versione 3 (NFSv3).

A proposito di questa attività

Eseguire questa procedura per ogni nodo amministratore in un'implementazione StorageGRID da cui si desidera recuperare i messaggi di controllo.

Fasi

1. Accedere al nodo di amministrazione principale:

- Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
- Immettere la password elencata in `Passwords.txt` file.
- Immettere il seguente comando per passare a root: `su -`
- Immettere la password elencata in `Passwords.txt` file.

Una volta effettuato l'accesso come root, il prompt cambia da `$` a `#`.

2. Verificare che tutti i servizi abbiano uno stato di esecuzione o verificato. Inserire: `storagegrid-status`

Se alcuni servizi non sono elencati come in esecuzione o verificati, risolvere i problemi prima di continuare.

3. Tornare alla riga di comando. Premere **Ctrl+C**.

4. Avviare l'utilità di configurazione NFS. Inserire: `config_nfs.rb`

```
-----  
| Shares                | Clients                | Config                |  
-----  
| add-audit-share      | add-ip-to-share       | validate-config      |  
| enable-disable-share | remove-ip-from-share  | refresh-config       |  
|                       |                       | help                 |  
|                       |                       | exit                 |  
-----
```

5. Aggiungere il client di audit: `add-audit-share`

- Quando richiesto, inserire l'indirizzo IP o l'intervallo di indirizzi IP del client di controllo per la condivisione di controllo: `client_IP_address`
- Quando richiesto, premere **Invio**.

6. Se più di un client di audit è autorizzato ad accedere alla condivisione di audit, aggiungere l'indirizzo IP dell'utente aggiuntivo: `add-ip-to-share`

- a. Inserire il numero della condivisione di controllo: `audit_share_number`
- b. Quando richiesto, inserire l'indirizzo IP o l'intervallo di indirizzi IP del client di controllo per la condivisione di controllo: `client_IP_address`
- c. Quando richiesto, premere **Invio**.

Viene visualizzata l'utility di configurazione NFS.

- d. Ripetere questi passaggi secondari per ogni client di audit aggiuntivo che ha accesso alla condivisione di audit.

7. Se si desidera, verificare la configurazione.

- a. Immettere quanto segue: `validate-config`

I servizi vengono controllati e visualizzati.

- b. Quando richiesto, premere **Invio**.

Viene visualizzata l'utility di configurazione NFS.

- c. Chiudere l'utility di configurazione NFS: `exit`

8. Determinare se è necessario abilitare le condivisioni di audit in altri siti.

- Se l'implementazione di StorageGRID è un singolo sito, passare alla fase successiva.
- Se l'implementazione di StorageGRID include nodi di amministrazione in altri siti, abilitare queste condivisioni di controllo come richiesto:

- i. Accedere in remoto al nodo Admin del sito:

A. Immettere il seguente comando: `ssh admin@grid_node_IP`

B. Immettere la password elencata in `Passwords.txt` file.

C. Immettere il seguente comando per passare a root: `su -`

D. Immettere la password elencata in `Passwords.txt` file.

- ii. Ripetere questi passaggi per configurare le condivisioni di controllo per ogni nodo amministrativo aggiuntivo.

- iii. Chiudere l'accesso remoto sicuro alla shell nel nodo di amministrazione remoto. Inserire: `exit`

9. Disconnettersi dalla shell dei comandi: `exit`

Ai client di audit NFS viene concesso l'accesso a una condivisione di audit in base al proprio indirizzo IP. Concedere l'accesso alla condivisione di controllo a un nuovo client di audit NFS aggiungendo il proprio indirizzo IP alla condivisione oppure rimuovere un client di audit esistente rimuovendo il relativo indirizzo IP.

Aggiunta di un client di audit NFS a una condivisione di audit

Ai client di audit NFS viene concesso l'accesso a una condivisione di audit in base al proprio indirizzo IP. Concedere l'accesso alla condivisione di audit a un nuovo client di audit NFS aggiungendo il proprio indirizzo IP alla condivisione di audit.

Di cosa hai bisogno

- È necessario disporre di `Passwords.txt` File con la password dell'account root/admin (disponibile nel pacchetto).
- È necessario disporre di `Configuration.txt` File (disponibile in DETTO pacchetto).
- Il client di audit deve utilizzare NFS versione 3 (NFSv3).

Fasi

1. Accedere al nodo di amministrazione principale:

- Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
- Immettere la password elencata in `Passwords.txt` file.
- Immettere il seguente comando per passare a root: `su -`
- Immettere la password elencata in `Passwords.txt` file.

Una volta effettuato l'accesso come root, il prompt cambia da `$` a `#`.

2. Avviare l'utility di configurazione NFS: `config_nfs.rb`

```

-----
| Shares                | Clients                | Config                |
-----
| add-audit-share      | add-ip-to-share       | validate-config      |
| enable-disable-share | remove-ip-from-share  | refresh-config       |
|                       |                       | help                 |
|                       |                       | exit                 |
-----

```

3. Inserire: `add-ip-to-share`

Viene visualizzato un elenco di condivisioni di controllo NFS attivate nel nodo di amministrazione. La condivisione dell'audit è elencata come: `/var/local/audit/export`

4. Inserire il numero della condivisione di controllo: `audit_share_number`

5. Quando richiesto, inserire l'indirizzo IP o l'intervallo di indirizzi IP del client di controllo per la condivisione di controllo: `client_IP_address`

Il client di audit viene aggiunto alla condivisione di audit.

6. Quando richiesto, premere **Invio**.

Viene visualizzata l'utility di configurazione NFS.

7. Ripetere i passaggi per ogni client di audit da aggiungere alla condivisione di audit.

8. In alternativa, verificare la configurazione: `validate-config`

I servizi vengono controllati e visualizzati.

- Quando richiesto, premere **Invio**.

Viene visualizzata l'utility di configurazione NFS.

9. Chiudere l'utility di configurazione NFS: `exit`
10. Se l'implementazione di StorageGRID è un singolo sito, passare alla fase successiva.

In caso contrario, se l'implementazione di StorageGRID include nodi di amministrazione in altri siti, attivare facoltativamente queste condivisioni di controllo come richiesto:

- a. Accedere in remoto al nodo di amministrazione di un sito:
 - i. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - ii. Immettere la password elencata in `Passwords.txt` file.
 - iii. Immettere il seguente comando per passare a root: `su -`
 - iv. Immettere la password elencata in `Passwords.txt` file.
 - b. Ripetere questa procedura per configurare le condivisioni di controllo per ciascun nodo di amministrazione.
 - c. Chiudere l'accesso remoto sicuro alla shell nel nodo di amministrazione remoto: `exit`
11. Disconnettersi dalla shell dei comandi: `exit`

Verifica dell'integrazione dell'audit NFS

Dopo aver configurato una condivisione di audit e aggiunto un client di audit NFS, è possibile montare la condivisione del client di audit e verificare che i file siano disponibili dalla condivisione di audit.

Fasi

1. Verificare la connettività (o la variante per il sistema client) utilizzando l'indirizzo IP lato client del nodo di amministrazione che ospita il servizio AMS. Inserire: `ping IP_address`

Verificare che il server risponda, indicando la connettività.

2. Montare la condivisione di sola lettura dell'audit utilizzando un comando appropriato per il sistema operativo del client. Un comando Linux di esempio è (inserire su una riga):

```
mount -t nfs -o hard,intr Admin_Node_IP_address:/var/local/audit/export  
myAudit
```

Utilizzare l'indirizzo IP del nodo di amministrazione che ospita il servizio AMS e il nome di condivisione predefinito per il sistema di audit. Il punto di montaggio può essere qualsiasi nome selezionato dal client (ad esempio, `myAudit` nel comando precedente).

3. Verificare che i file siano disponibili dalla condivisione dell'audit. Inserire: `ls myAudit /*`

dove `myAudit` è il punto di montaggio della condivisione dell'audit. Dovrebbe essere presente almeno un file di log.

Rimozione di un client di audit NFS dalla condivisione di audit

Ai client di audit NFS viene concesso l'accesso a una condivisione di audit in base al

proprio indirizzo IP. È possibile rimuovere un client di audit esistente rimuovendo il relativo indirizzo IP.

Di cosa hai bisogno

- È necessario disporre di `Passwords.txt` File con la password dell'account root/admin (disponibile nel pacchetto).
- È necessario disporre di `Configuration.txt` File (disponibile in DETTO pacchetto).

A proposito di questa attività

Non è possibile rimuovere l'ultimo indirizzo IP consentito per accedere alla condivisione di controllo.

Fasi

1. Accedere al nodo di amministrazione principale:

- Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
- Immettere la password elencata in `Passwords.txt` file.
- Immettere il seguente comando per passare a root: `su -`
- Immettere la password elencata in `Passwords.txt` file.

Una volta effettuato l'accesso come root, il prompt cambia da `$` a `#`.

2. Avviare l'utility di configurazione NFS: `config_nfs.rb`

```
-----  
| Shares                | Clients                | Config                |  
-----  
| add-audit-share      | add-ip-to-share       | validate-config      |  
| enable-disable-share | remove-ip-from-share  | refresh-config       |  
|                       |                       | help                 |  
|                       |                       | exit                 |  
-----
```

3. Rimuovere l'indirizzo IP dalla condivisione dell'audit: `remove-ip-from-share`

Viene visualizzato un elenco numerato di condivisioni di controllo configurate sul server. La condivisione dell'audit è elencata come: `/var/local/audit/export`

4. Inserire il numero corrispondente alla condivisione di audit: `audit_share_number`

Viene visualizzato un elenco numerato di indirizzi IP autorizzati ad accedere alla condivisione dell'audit.

5. Inserire il numero corrispondente all'indirizzo IP che si desidera rimuovere.

La condivisione di audit viene aggiornata e l'accesso non è più consentito da alcun client di audit con questo indirizzo IP.

6. Quando richiesto, premere **Invio**.

Viene visualizzata l'utility di configurazione NFS.

7. Chiudere l'utility di configurazione NFS: `exit`
8. Se l'implementazione di StorageGRID è un'implementazione di più siti di data center con nodi amministrativi aggiuntivi negli altri siti, disattivare queste condivisioni di controllo secondo necessità:
 - a. Accedere in remoto al nodo di amministrazione di ciascun sito:
 - i. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - ii. Immettere la password elencata in `Passwords.txt` file.
 - iii. Immettere il seguente comando per passare a root: `su -`
 - iv. Immettere la password elencata in `Passwords.txt` file.
 - b. Ripetere questi passaggi per configurare le condivisioni di controllo per ogni nodo amministrativo aggiuntivo.
 - c. Chiudere l'accesso remoto sicuro alla shell nel nodo di amministrazione remoto: `exit`
9. Disconnettersi dalla shell dei comandi: `exit`

Modifica dell'indirizzo IP di un client di audit NFS

1. Aggiungere un nuovo indirizzo IP a una condivisione di audit NFS esistente.
2. Rimuovere l'indirizzo IP originale.

Informazioni correlate

["Aggiunta di un client di audit NFS a una condivisione di audit"](#)

["Rimozione di un client di audit NFS dalla condivisione di audit"](#)

Gestione dei nodi di archiviazione

In alternativa, è possibile implementare ciascun sito del data center del sistema StorageGRID con un nodo di archiviazione, che consente di connettersi a un sistema di storage di archiviazione esterno di destinazione, ad esempio Tivoli Storage Manager (TSM).

Dopo aver configurato le connessioni alla destinazione esterna, è possibile configurare il nodo di archiviazione in modo da ottimizzare le prestazioni del TSM, disattivare un nodo di archiviazione quando un server TSM si avvicina alla capacità o non è disponibile e configurare le impostazioni di replica e recupero. È inoltre possibile impostare allarmi personalizzati per il nodo di archiviazione.

- ["Che cos'è un nodo di archivio"](#)
- ["Configurazione delle connessioni del nodo di archiviazione allo storage di archiviazione"](#)
- ["Impostazione di allarmi personalizzati per il nodo di archiviazione"](#)
- ["Integrazione di Tivoli Storage Manager"](#)

Che cos'è un nodo di archivio

Il nodo di archiviazione fornisce un'interfaccia attraverso la quale è possibile indirizzare un sistema di storage di archiviazione esterno per lo storage a lungo termine dei dati a

oggetti. Il nodo di archiviazione monitora inoltre questa connessione e il trasferimento dei dati degli oggetti tra il sistema StorageGRID e il sistema di archiviazione esterno di destinazione.

The screenshot shows the StorageGRID WebScale Deployment interface. On the left, the Grid Topology tree is visible, with the node DC1-ARC1-98-165 highlighted. The main panel displays the Overview for this ARC node, showing various status indicators and node information.

Overview: ARC (DC1-ARC1-98-165) - ARC	
Updated: 2015-09-30 10:29:18 PDT	
ARC State:	Online
ARC Status:	No Errors
Tivoli Storage Manager State:	Online
Tivoli Storage Manager Status:	No Errors
Store State:	Online
Store Status:	No Errors
Retrieve State:	Online
Retrieve Status:	No Errors
Inbound Replication Status:	No Errors
Outbound Replication Status:	No Errors

Node Information	
Device Type:	Archive Node
Version:	10.2.0
Build:	20150928.2133.a27b3ab
Node ID:	19002524
Site ID:	10

I dati degli oggetti che non possono essere cancellati, ma a cui non si accede regolarmente, possono essere spostati in qualsiasi momento dai dischi rotanti di uno Storage Node e su uno storage di archiviazione esterno, come il cloud o il nastro. Questa archiviazione dei dati a oggetti viene eseguita attraverso la configurazione del nodo di archivio di un sito del data center e quindi la configurazione delle regole ILM in cui questo nodo di archivio viene selezionato come "destinazione" per le istruzioni di posizionamento del contenuto. Il nodo di archiviazione non gestisce i dati degli oggetti archiviati in sé; ciò viene ottenuto dal dispositivo di archiviazione esterno.



I metadati degli oggetti non vengono archiviati, ma rimangono nei nodi di storage.

Che cos'è il servizio ARC

Il servizio Archive Node's Archive (ARC) fornisce l'interfaccia di gestione che è possibile utilizzare per configurare le connessioni allo storage di archiviazione esterno, ad esempio su nastro, tramite il middleware TSM.

È il servizio ARC che interagisce con un sistema di storage di archiviazione esterno, inviando dati a oggetti per lo storage nearline ed eseguendo recuperi quando un'applicazione client richiede un oggetto archiviato. Quando un'applicazione client richiede un oggetto archiviato, un nodo di storage richiede i dati dell'oggetto al servizio ARC. Il servizio ARC invia una richiesta al sistema di storage di archiviazione esterno, che recupera i dati dell'oggetto richiesti e li invia al servizio ARC. Il servizio ARC verifica i dati dell'oggetto e li inoltra al nodo di storage, che a sua volta restituisce l'oggetto all'applicazione client richiedente.

Le richieste di dati a oggetti archiviati su nastro tramite il middleware TSM vengono gestite per garantire l'efficienza dei recuperi. Le richieste possono essere ordinate in modo che gli oggetti memorizzati in ordine sequenziale su nastro vengano richiesti nello stesso ordine sequenziale. Le richieste vengono quindi messe in coda per l'invio al dispositivo di storage. A seconda del dispositivo di archiviazione, è possibile elaborare contemporaneamente più richieste di oggetti su diversi volumi.

Configurazione delle connessioni del nodo di archiviazione allo storage di archiviazione

Quando si configura un nodo di archiviazione per la connessione a un archivio esterno, è necessario selezionare il tipo di destinazione.

Il sistema StorageGRID supporta l'archiviazione dei dati a oggetti nel cloud tramite un'interfaccia S3 o su nastro tramite il middleware TSM (Tivoli Storage Manager).



Una volta configurato il tipo di destinazione di archiviazione per un nodo di archiviazione, il tipo di destinazione non può essere modificato.

- ["Archiviazione nel cloud tramite l'API S3"](#)
- ["Archiviazione su nastro tramite middleware TSM"](#)
- ["Configurazione delle impostazioni di recupero del nodo di archiviazione"](#)
- ["Configurazione della replica del nodo di archiviazione"](#)

Archiviazione nel cloud tramite l'API S3

È possibile configurare un nodo di archiviazione per la connessione diretta ai servizi Web Amazon o a qualsiasi altro sistema in grado di interfacciarsi con il sistema StorageGRID tramite l'API S3.



Lo spostamento di oggetti da un nodo di archiviazione a un sistema storage di archiviazione esterno tramite l'API S3 è stato sostituito da pool di storage cloud ILM, che offrono maggiori funzionalità. L'opzione **Cloud Tiering - Simple Storage Service (S3)** è ancora supportata, ma potresti preferire implementare i Cloud Storage Pool.

Se stai utilizzando un nodo di archiviazione con l'opzione **Cloud Tiering - Simple Storage Service (S3)**, prendi in considerazione la migrazione degli oggetti a un pool di storage cloud. Consultare le istruzioni per la gestione degli oggetti con la gestione del ciclo di vita delle informazioni.

Informazioni correlate

["Gestire gli oggetti con ILM"](#)

Configurazione delle impostazioni di connessione per l'API S3

Se si sta effettuando la connessione a un nodo di archiviazione utilizzando l'interfaccia S3, è necessario configurare le impostazioni di connessione per l'API S3. Fino a quando queste impostazioni non vengono configurate, il servizio ARC rimane in uno stato di allarme principale in quanto non è in grado di comunicare con il sistema di storage di archiviazione esterno.



Lo spostamento di oggetti da un nodo di archiviazione a un sistema storage di archiviazione esterno tramite l'API S3 è stato sostituito da pool di storage cloud ILM, che offrono maggiori funzionalità. L'opzione **Cloud Tiering - Simple Storage Service (S3)** è ancora supportata, ma potresti preferire implementare i Cloud Storage Pool.

Se stai utilizzando un nodo di archiviazione con l'opzione **Cloud Tiering - Simple Storage Service (S3)**, prendi in considerazione la migrazione degli oggetti a un pool di storage cloud. Consultare le istruzioni per la gestione degli oggetti con la gestione del ciclo di vita delle informazioni.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.
- È necessario aver creato un bucket sul sistema storage di archiviazione di destinazione:
 - Il bucket deve essere dedicato a un singolo nodo di archiviazione. Non può essere utilizzato da altri nodi di archiviazione o altre applicazioni.
 - Il bucket deve avere la regione appropriata selezionata per la propria posizione.
 - Il bucket deve essere configurato con la versione sospesa.
- È necessario attivare la segmentazione degli oggetti e la dimensione massima dei segmenti deve essere inferiore o uguale a 4.5 GiB (4,831,838,208 byte). Le richieste API S3 che superano questo valore non avranno esito positivo se S3 viene utilizzato come sistema di storage di archiviazione esterno.


Fasi

1. Selezionare **supporto > Strumenti > topologia griglia**.
2. Selezionare **Archive Node ARC Target**.
3. Selezionare **Configurazione principale**.

Target Type: Cloud Tiering - Simple Storage Service (S3)

Cloud Tiering (S3) Account

Bucket Name:	<input type="text" value="name"/>
Region:	Virginia or Pacific Northwest (us-east-1)
Endpoint:	<input type="text" value="https://10.10.10.123:8082"/> <input type="checkbox"/> Use AWS
Endpoint Authentication:	<input type="checkbox"/>
Access Key:	<input type="text" value="ABCD123EFG45AB"/>
Secret Access Key:	<input type="password" value="•••••"/>
Storage Class:	Standard (Default)

Apply Changes 

4. Selezionare **Cloud Tiering - Simple Storage Service (S3)** dall'elenco a discesa Target Type (tipo di destinazione).



Le impostazioni di configurazione non sono disponibili fino a quando non si seleziona un tipo di destinazione.

5. Configurare l'account di cloud tiering (S3) attraverso il quale il nodo di archiviazione si conetterà al sistema di archiviazione esterno di destinazione in grado di supportare S3.

La maggior parte dei campi di questa pagina sono esplicativi. Di seguito vengono descritti i campi per i quali potrebbe essere necessario fornire assistenza.

- **Regione:** Disponibile solo se è selezionato **Usa AWS**. La regione selezionata deve corrispondere a quella del bucket.
- **Endpoint e Use AWS:** Per Amazon Web Services (AWS), selezionare **Use AWS**. **Endpoint** viene quindi compilato automaticamente con un URL dell'endpoint in base agli attributi Bucket Name e Region. Ad esempio:

`https://bucket.region.amazonaws.com`

Per una destinazione non AWS, inserire l'URL del sistema che ospita il bucket, incluso il numero di porta. Ad esempio:

`https://system.com:1080`

- **End Point Authentication:** Attivato per impostazione predefinita. Se la rete sul sistema di storage di archiviazione esterno è attendibile, deselegionare la casella di controllo per disattivare la verifica del

certificato SSL dell'endpoint e del nome host per il sistema di storage di archiviazione esterno di destinazione. Se un'altra istanza di un sistema StorageGRID è il dispositivo di archiviazione di destinazione e il sistema è configurato con certificati firmati pubblicamente, è possibile mantenere la casella di controllo selezionata.

- **Storage Class** (Classe di storage): Selezionare **Standard (predefinito)** per lo storage normale. Selezionare **Redundancy ridotta** solo per gli oggetti che possono essere ricreati facilmente. **Redundancy ridotta** offre storage a costi inferiori con minore affidabilità. Se il sistema storage di archiviazione di destinazione è un'altra istanza del sistema StorageGRID, **Classe storage** controlla quante copie intermedie dell'oggetto vengono eseguite al momento dell'acquisizione nel sistema di destinazione, se viene utilizzato il doppio commit quando vengono acquisiti oggetti.

6. Fare clic su **Applica modifiche**.

Le impostazioni di configurazione specificate vengono validate e applicate al sistema StorageGRID. Una volta configurata, la destinazione non può essere modificata.

Informazioni correlate

["Gestire gli oggetti con ILM"](#)

Modifica delle impostazioni di connessione per l'API S3

Una volta configurato il nodo di archiviazione per la connessione a un sistema di archiviazione esterno tramite l'API S3, è possibile modificare alcune impostazioni in caso di modifica della connessione.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

A proposito di questa attività

Se si modifica l'account Cloud Tiering (S3), è necessario assicurarsi che le credenziali di accesso dell'utente abbiano accesso in lettura/scrittura al bucket, inclusi tutti gli oggetti precedentemente acquisiti dal nodo di archiviazione nel bucket.

Fasi

1. Selezionare **supporto > Strumenti > topologia griglia**.
2. Selezionare **Archive Node ARC Target**.
3. Selezionare **Configurazione principale**.

Target Type: Cloud Tiering - Simple Storage Service (S3)

Cloud Tiering (S3) Account

Bucket Name:	<input type="text" value="name"/>
Region:	Virginia or Pacific Northwest (us-east-1)
Endpoint:	<input type="text" value="https://10.10.10.123:8082"/> <input type="checkbox"/> Use AWS
Endpoint Authentication:	<input type="checkbox"/>
Access Key:	<input type="text" value="ABCD123EFG45AB"/>
Secret Access Key:	<input type="password" value="•••••"/>
Storage Class:	Standard (Default)

Apply Changes 

4. Modificare le informazioni dell'account, se necessario.

Se si modifica la classe di storage, i nuovi dati dell'oggetto vengono memorizzati con la nuova classe di storage. L'oggetto esistente continua ad essere memorizzato nella classe di storage impostata al momento dell'acquisizione.



Nome bucket, Regione ed endpoint, utilizza i valori AWS e non può essere modificato.

5. Fare clic su **Applica modifiche**.

Modifica dello stato del servizio di tiering cloud

È possibile controllare la capacità di lettura e scrittura del nodo di archiviazione nel sistema storage di archiviazione esterno di destinazione che si connette attraverso l'API S3 modificando lo stato del servizio di tiering cloud.

Di cosa hai bisogno

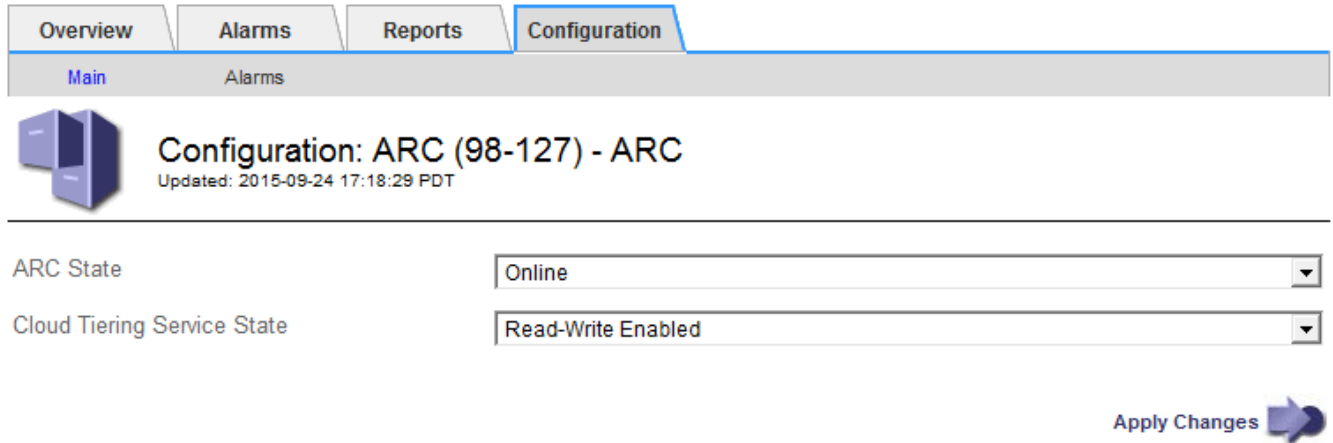
- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.
- Il nodo di archiviazione deve essere configurato.

A proposito di questa attività

È possibile disattivare il nodo di archiviazione modificando lo stato del servizio di tiering cloud in **Read-Write Disabled**.


Fasi

1. Selezionare **supporto > Strumenti > topologia griglia**.
2. Selezionare **Archive Node ARC**.
3. Selezionare **Configurazione principale**.



ARC State

Cloud Tiering Service State

Apply Changes 

4. Selezionare un **Cloud Tiering Service state**.
5. Fare clic su **Applica modifiche**.

Reimpostazione del numero di errori di archiviazione per la connessione API S3

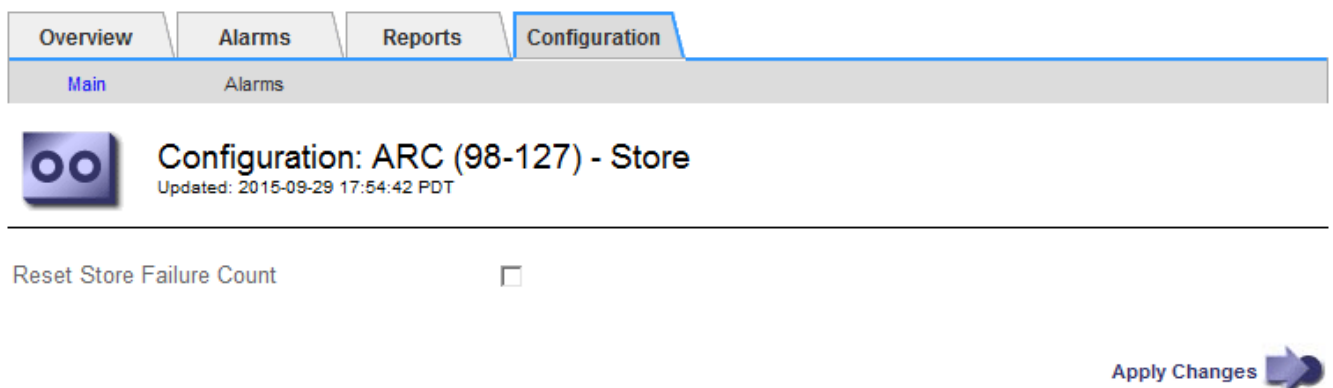
Se il nodo di archiviazione si connette a un sistema di storage di archiviazione tramite l'API S3, è possibile reimpostare il numero di errori di archiviazione, che può essere utilizzato per cancellare l'allarme ARVF (Store Failures).

Di cosa hai bisogno


- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

Fasi

1. Selezionare **supporto > Strumenti > topologia griglia**.
2. Selezionare **Archive Node ARC Store**.
3. Selezionare **Configurazione principale**.



Reset Store Failure Count

Apply Changes 

4. Selezionare **Reset Store Failure Count**.

5. Fare clic su **Applica modifiche**.

L'attributo Store Failures viene reimpostato su zero.

Migrazione di oggetti da Cloud Tiering - S3 a un Cloud Storage Pool

Se stai utilizzando la funzionalità **Cloud Tiering - Simple Storage Service (S3)** per tierare i dati degli oggetti in un bucket S3, prendi in considerazione la migrazione degli oggetti in un Cloud Storage Pool. I pool di cloud storage offrono un approccio scalabile che sfrutta tutti i nodi di storage nel sistema StorageGRID.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.
- Hai già memorizzato oggetti nel bucket S3 configurato per il Cloud Tiering.



Prima di migrare i dati degli oggetti, contatta il tuo rappresentante NetApp per conoscere e gestire i costi associati.

A proposito di questa attività

Dal punto di vista di ILM, un pool di storage cloud è simile a un pool di storage. Tuttavia, mentre i pool di storage sono costituiti da nodi di storage o nodi di archiviazione all'interno del sistema StorageGRID, un pool di storage cloud è costituito da un bucket S3 esterno.

Prima di migrare gli oggetti da Tier cloud - S3 a un pool di storage cloud, è necessario prima creare un bucket S3 e poi creare il pool di storage cloud in StorageGRID. Quindi, è possibile creare un nuovo criterio ILM e sostituire la regola ILM utilizzata per memorizzare gli oggetti nel bucket Cloud Tiering con una regola ILM clonata che memorizza gli stessi oggetti nel Cloud Storage Pool.



Quando gli oggetti vengono memorizzati in un pool di storage cloud, le copie di tali oggetti non possono essere memorizzate anche in StorageGRID. Se la regola ILM attualmente in uso per il Cloud Tiering è configurata per memorizzare oggetti in più posizioni contemporaneamente, considerare se si desidera eseguire questa migrazione facoltativa perché si perde tale funzionalità. Se si continua con questa migrazione, è necessario creare nuove regole invece di clonare quelle esistenti.

Fasi

1. Creare un pool di storage cloud.

Utilizza un nuovo bucket S3 per il Cloud Storage Pool per garantire che contenga solo i dati gestiti dal Cloud Storage Pool.

2. Individuare eventuali regole ILM nel criterio ILM attivo che causano l'archiviazione degli oggetti nel bucket Cloud Tiering.

3. Clonare ciascuna di queste regole.

4. Nelle regole clonate, modificare la posizione di posizionamento nel nuovo Cloud Storage Pool.

5. Salvare le regole clonate.

6. Creare una nuova policy che utilizzi le nuove regole.

7. Simulare e attivare la nuova policy.

Quando la nuova policy viene attivata e si verifica la valutazione ILM, gli oggetti vengono spostati dal bucket S3 configurato per il Cloud Tiering al bucket S3 configurato per il Cloud Storage Pool. Lo spazio utilizzabile sulla griglia non viene compromesso. Una volta spostati nel Cloud Storage Pool, gli oggetti vengono rimossi dal bucket Cloud Tiering.

Informazioni correlate

["Gestire gli oggetti con ILM"](#)

Archiviazione su nastro tramite middleware TSM

È possibile configurare un nodo di archiviazione in modo che utilizzi un server Tivoli Storage Manager (TSM) che fornisce un'interfaccia logica per l'archiviazione e il recupero dei dati degli oggetti su dispositivi di storage ad accesso casuale o sequenziale, incluse le librerie su nastro.

Il servizio ARC del nodo di archiviazione agisce come client per il server TSM, utilizzando Tivoli Storage Manager come middleware per la comunicazione con il sistema di storage di archiviazione.

Classi di gestione TSM

Le classi di gestione definite dal middleware TSM delineano il funzionamento delle operazioni di backup e archiviazione di TSM's e possono essere utilizzate per specificare le regole per il contenuto che vengono applicate dal server TSM. Tali regole funzionano indipendentemente dalla policy ILM del sistema StorageGRID e devono essere coerenti con il requisito del sistema StorageGRID che gli oggetti siano memorizzati in modo permanente e siano sempre disponibili per il recupero da parte del nodo di archiviazione. Dopo che i dati dell'oggetto sono stati inviati a un server TSM dal nodo di archiviazione, il ciclo di vita del TSM e le regole di conservazione vengono applicati mentre i dati dell'oggetto vengono memorizzati sul nastro gestito dal server TSM.

La classe di gestione TSM viene utilizzata dal server TSM per applicare regole per la posizione o la conservazione dei dati dopo che gli oggetti sono stati inviati al server TSM dal nodo di archiviazione. Ad esempio, gli oggetti identificati come backup del database (contenuto temporaneo che può essere sovrascritto con dati più recenti) potrebbero essere trattati in modo diverso rispetto ai dati dell'applicazione (contenuto fisso che deve essere conservato a tempo indeterminato).

Configurazione delle connessioni al middleware TSM

Prima che il nodo di archiviazione possa comunicare con il middleware Tivoli Storage Manager (TSM), è necessario configurare diverse impostazioni.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

A proposito di questa attività

Fino a quando queste impostazioni non vengono configurate, il servizio ARC rimane in uno stato di allarme principale in quanto non è in grado di comunicare con Tivoli Storage Manager.

Fasi

1. Selezionare **supporto > Strumenti > topologia griglia**.
2. Selezionare **Archive Node ARC Target**.
3. Selezionare **Configurazione principale**.

Configuration: ARC (DC1-ARC1-98-165) - Target
Updated: 2015-09-28 09:56:36 PDT

Target Type: Tivoli Storage Manager (TSM)

Tivoli Storage Manager State: Online

Target (TSM) Account

Server IP or Hostname: 10.10.10.123

Server Port: 1500

Node Name: ARC-USER

User Name: arc-user


Password: ●●●●●●

Management Class: sg-mgmtclass

Number of Sessions: 2

Maximum Retrieve Sessions: 1

Maximum Store Sessions: 1

Apply Changes 

4. Dall'elenco a discesa **Target Type** (tipo di destinazione), selezionare **Tivoli Storage Manager (TSM)**.
5. Per lo stato di **Tivoli Storage Manager**, selezionare **Offline** per impedire il recupero dal server middleware TSM.

Per impostazione predefinita, lo stato di Tivoli Storage Manager è impostato su Online, il che significa che il nodo di archiviazione è in grado di recuperare i dati degli oggetti dal server middleware TSM.

6. Completare le seguenti informazioni:
 - **Server IP (IP server) o Hostname (Nome host)**: Specificare l'indirizzo IP o il nome di dominio completo del server middleware TSM utilizzato dal servizio ARC. L'indirizzo IP predefinito è 127.0.0.1.
 - **Server Port** (porta server): Specificare il numero di porta sul server middleware TSM a cui si conatterà il servizio ARC. Il valore predefinito è 1500.
 - **Node Name** (Nome nodo): Specificare il nome del nodo di archiviazione. Immettere il nome (arco-utente) registrato sul server middleware TSM.
 - **User Name** (Nome utente): Specificare il nome utente utilizzato dal servizio ARC per accedere al server TSM. Immettere il nome utente predefinito (Arc-user) o l'utente amministrativo specificato per il nodo di archiviazione.
 - **Password**: Specificare la password utilizzata dal servizio ARC per accedere al server TSM.

- **Classe di gestione:** Specificare la classe di gestione predefinita da utilizzare se non viene specificata una classe di gestione quando l'oggetto viene salvato nel sistema StorageGRID o se la classe di gestione specificata non viene definita nel server middleware TSM.
- **Numero di sessioni:** Specificare il numero di unità nastro sul server middleware TSM dedicate al nodo di archiviazione. Il nodo di archiviazione crea contemporaneamente un massimo di una sessione per punto di montaggio più un piccolo numero di sessioni aggiuntive (meno di cinque).

È necessario modificare questo valore in modo che sia uguale al valore impostato per MAXNUMMP (numero massimo di punti di montaggio) quando il nodo di archiviazione è stato registrato o aggiornato. (Nel comando register, il valore predefinito di MAXNUMMP utilizzato è 1, se non viene impostato alcun valore).

È inoltre necessario modificare il valore di MAXSESSIONS per il server TSM con un numero pari almeno al numero di sessioni impostato per il servizio ARC. Il valore predefinito di MAXSESSIONS sul server TSM è 25.

- **Numero massimo di sessioni di recupero:** Specificare il numero massimo di sessioni che il servizio ARC può aprire al server middleware TSM per le operazioni di recupero. Nella maggior parte dei casi, il valore appropriato è numero di sessioni meno numero massimo di sessioni del negozio. Se è necessario condividere un'unità a nastro per lo storage e il recupero, specificare un valore uguale al numero di sessioni.
- **Numero massimo di sessioni di archiviazione:** Specificare il numero massimo di sessioni simultanee che il servizio ARC può aprire al server middleware TSM per le operazioni di archiviazione.

Questo valore deve essere impostato su uno, tranne quando il sistema storage di archiviazione di destinazione è pieno e possono essere eseguiti solo i recuperi. Impostare questo valore su zero per utilizzare tutte le sessioni per i recuperi.

7. Fare clic su **Applica modifiche**.

Ottimizzazione di un nodo di archiviazione per sessioni middleware TSM

È possibile ottimizzare le prestazioni di un nodo di archiviazione che si connette a Tivoli Server Manager (TSM) configurando le sessioni del nodo di archiviazione.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

A proposito di questa attività

In genere, il numero di sessioni simultanee che il nodo di archiviazione ha aperto al server middleware TSM viene impostato sul numero di unità a nastro dedicate dal server TSM al nodo di archiviazione. Un'unità a nastro viene allocata per lo storage, mentre le altre vengono allocate per il recupero. Tuttavia, nelle situazioni in cui un nodo di storage viene ricostruito dalle copie del nodo di archivio o il nodo di archivio opera in modalità di sola lettura, è possibile ottimizzare le prestazioni del server TSM impostando il numero massimo di sessioni di recupero sullo stesso numero di sessioni simultanee. Il risultato è che tutti i dischi possono essere utilizzati contemporaneamente per il recupero e, al massimo, uno di questi dischi può essere utilizzato anche per lo storage, se applicabile.


Fasi

1. Selezionare **supporto > Strumenti > topologia griglia**.
2. Selezionare **Archive Node ARC Target**.

3. Selezionare **Configurazione principale**.
4. Modificare **numero massimo di sessioni di recupero** in modo che sia uguale a **numero di sessioni**.

Overview Alarms Reports **Configuration**

Main Alarms

 **Configuration: ARC (DC1-ARC1-98-165) - Target**
Updated: 2015-09-28 09:56:36 PDT

Target Type:

Tivoli Storage Manager State:

Target (TSM) Account

Server IP or Hostname:

Server Port:

Node Name:

User Name:


Password:

Management Class:

Number of Sessions:

Maximum Retrieve Sessions:

Maximum Store Sessions:

Apply Changes 

5. Fare clic su **Applica modifiche**.

Configurazione dello stato di archiviazione e dei contatori per TSM

Se il nodo di archiviazione si connette a un server middleware TSM, è possibile configurare lo stato dell'archivio di un nodo di archiviazione su Online o Offline. È inoltre possibile disattivare l'archivio al primo avvio del nodo di archiviazione o ripristinare il conteggio degli errori rilevati per l'allarme associato.

Di cosa hai bisogno


- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

Fasi

1. Selezionare **supporto > Strumenti > topologia griglia**.
2. Selezionare **Archive Node ARC Store**.
3. Selezionare **Configurazione principale**.

Overview Alarms Reports **Configuration**


Main Alarms

 **Configuration: ARC (DC1-ARC1-98-165) - Store**
Updated: 2015-09-29 17:10:12 PDT

Store State

Archive Store Disabled on Startup

Reset Store Failure Count

Apply Changes 

4. Modificare le seguenti impostazioni, se necessario:

- Store state (Stato di archiviazione): Impostare lo stato del componente su:
 - Online: Il nodo di archiviazione è disponibile per elaborare i dati a oggetti per lo storage nel sistema di storage di archiviazione.
 - Offline: Il nodo di archiviazione non è disponibile per elaborare i dati degli oggetti per lo storage nel sistema di storage di archiviazione.
- Archivia archivio disattivata all'avvio: Se selezionato, il componente Archivia archivio rimane nello stato di sola lettura al riavvio. Utilizzato per disattivare in modo persistente lo storage nel sistema di storage di archiviazione di destinazione. Utile quando il sistema storage di archiviazione di destinazione non è in grado di accettare contenuti.
- Reset Store Failure Count (Ripristina numero di guasti del punto vendita): Consente di reimpostare il contatore per gli errori Questa opzione può essere utilizzata per cancellare l'allarme ARVF (Memorizza guasto).

5. Fare clic su **Applica modifiche**.

Informazioni correlate

["Gestione di un nodo di archiviazione quando il server TSM raggiunge la capacità"](#)

Gestione di un nodo di archiviazione quando il server TSM raggiunge la capacità

Il server TSM non ha modo di notificare al nodo di archiviazione quando il database TSM o lo storage dei supporti di archiviazione gestito dal server TSM si avvicina alla capacità. Il nodo di archiviazione continua ad accettare i dati dell'oggetto per il trasferimento al server TSM dopo che il server TSM ha interrotto l'accettazione del nuovo contenuto. Questo contenuto non può essere scritto su supporti gestiti dal server TSM. In questo caso, viene attivato un allarme. Questa situazione può essere evitata attraverso il monitoraggio proattivo del server TSM.

Di cosa hai bisogno

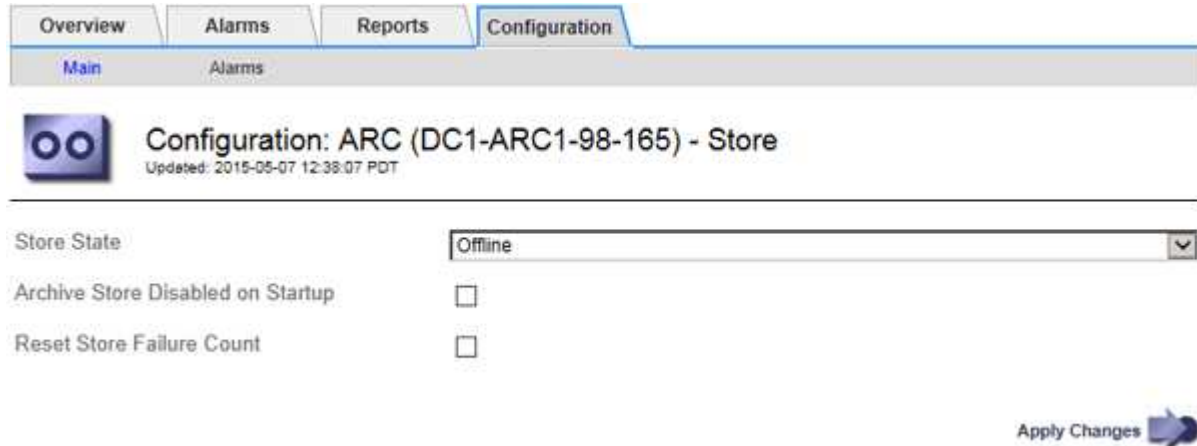
- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

A proposito di questa attività

Per impedire al servizio ARC di inviare ulteriore contenuto al server TSM, è possibile disattivare il nodo di archiviazione portando il componente **ARC Store** offline. Questa procedura può essere utile anche per prevenire gli allarmi quando il server TSM non è disponibile per la manutenzione.

Fasi

1. Selezionare **supporto > Strumenti > topologia griglia**.
2. Selezionare **Archive Node ARC Store**.
3. Selezionare **Configurazione principale**.



4. Modificare **Store state** in *Offline*.
5. Selezionare **Archivia archivio disabilitata all'avvio**.
6. Fare clic su **Applica modifiche**.

Impostazione di Archive Node su Read-only se il middleware TSM raggiunge la capacità

Se il server middleware TSM di destinazione raggiunge la capacità, il nodo di archiviazione può essere ottimizzato per eseguire solo i recuperi.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

Fasi

1. Selezionare **supporto > Strumenti > topologia griglia**.
2. Selezionare **Archive Node ARC Target**.
3. Selezionare **Configurazione principale**.
4. Impostare il numero massimo di sessioni di recupero in modo che sia uguale al numero di sessioni simultanee elencate in numero di sessioni.
5. Impostare il numero massimo di sessioni di memorizzazione su 0.



Se il nodo di archiviazione è di sola lettura, non è necessario modificare il numero massimo di sessioni di archiviazione su 0. Le sessioni del negozio non verranno create.

6. Fare clic su **Applica modifiche**.

Configurazione delle impostazioni di recupero del nodo di archiviazione

È possibile configurare le impostazioni di recupero per un nodo di archiviazione per impostare lo stato su Online o Offline, oppure reimpostare i conteggi degli errori rilevati per gli allarmi associati.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

Fasi

1. Selezionare **supporto > Strumenti > topologia griglia**.
2. Selezionare **nodo archivio ARC Recupera**.
3. Selezionare **Configurazione principale**.

Configuration: ARC (DC1-ARC1-98-165) - Retrieve
Updated: 2015-05-07 12:24:45 PDT

Retrieve State	Online
Reset Request Failure Count	<input type="checkbox"/>
Reset Verification Failure Count	<input type="checkbox"/>

Apply Changes

4. Modificare le seguenti impostazioni, se necessario:
 - **Stato di recupero:** Impostare lo stato del componente su:
 - Online: Il nodo Grid è disponibile per recuperare i dati degli oggetti dal dispositivo di archiviazione.
 - Offline: Il nodo Grid non è disponibile per recuperare i dati dell'oggetto.
 - Reset Request Failures Count (Ripristina numero di errori richiesta): Selezionare la casella di controllo per azzerare il contatore per gli errori della richiesta. Questa opzione può essere utilizzata per cancellare l'allarme ARRF (Request Failures).
 - Reset Verification Failure Count (Ripristina conteggio errori di verifica): Selezionare la casella di controllo per ripristinare il contatore per gli errori di verifica sui dati dell'oggetto recuperati. Questa opzione può essere utilizzata per cancellare l'allarme ARRV (Verification Failures) (errori di verifica).
5. Fare clic su **Applica modifiche**.

Configurazione della replica del nodo di archiviazione

È possibile configurare le impostazioni di replica per un nodo di archiviazione e disattivare la replica in entrata e in uscita oppure reimpostare i conteggi degli errori rilevati per gli allarmi associati.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

Fasi

1. Selezionare **supporto > Strumenti > topologia griglia**.
2. Selezionare **Archive Node ARC Replication**.
3. Selezionare **Configurazione principale**.

Configuration: ARC (DC1-ARC1-98-165) - Replication
Updated: 2015-05-07 12:21:53 PDT

Reset Inbound Replication Failure Count

Reset Outbound Replication Failure Count

Inbound Replication

Disable Inbound Replication

Outbound Replication

Disable Outbound Replication

Apply Changes

4. Modificare le seguenti impostazioni, se necessario:
 - **Reset Inbound Replication Failure Count** (Ripristina conteggio errori replica in entrata): Selezionare per reimpostare il contatore per gli errori di replica in entrata. Questa opzione può essere utilizzata per cancellare l'allarme RIRF (Inbound Replications — Failed).
 - **Reset Outbound Replication Failure Count** (Ripristina conteggio errori replica in uscita): Selezionare per reimpostare il contatore per gli errori di replica in uscita. Questa opzione può essere utilizzata per cancellare l'allarme RORF (Outbound Replications — Failed).
 - **Disable Inbound Replication** (Disattiva replica in entrata): Selezionare questa opzione per disattivare la replica in entrata come parte di una procedura di manutenzione o test. Lasciare deselezionato durante il normale funzionamento.

Quando la replica in entrata è disattivata, i dati degli oggetti possono essere recuperati dal servizio ARC per la replica in altre posizioni nel sistema StorageGRID, ma gli oggetti non possono essere replicati in questo servizio ARC da altre posizioni del sistema. Il servizio ARC è di sola lettura.

- **Disable Outbound Replication** (Disattiva replica in uscita): Selezionare la casella di controllo per disattivare la replica in uscita (incluse le richieste di contenuto per i recuperi HTTP) come parte di una procedura di manutenzione o test. Lasciare deselezionato durante il normale funzionamento.

Quando la replica in uscita è disattivata, i dati degli oggetti possono essere copiati in questo servizio ARC per soddisfare le regole ILM, ma i dati degli oggetti non possono essere recuperati dal servizio ARC per essere copiati in altre posizioni nel sistema StorageGRID. Il servizio ARC è di sola-scrittura.

5. Fare clic su **Applica modifiche**.

Impostazione di allarmi personalizzati per il nodo di archiviazione

È necessario stabilire allarmi personalizzati per gli attributi ARQL e ARRL utilizzati per monitorare la velocità e l'efficienza del recupero dei dati a oggetti dal sistema di storage di archiviazione da parte del nodo di archiviazione.

- ARQL: Lunghezza media della coda. Il tempo medio, in microsecondi, in cui i dati dell'oggetto vengono messi in coda per il recupero dal sistema di storage di archiviazione.
- ARRL: Latenza media della richiesta. Il tempo medio, in microsecondi, necessario al nodo di archiviazione per recuperare i dati degli oggetti dal sistema di storage di archiviazione.

I valori accettabili per questi attributi dipendono dalla configurazione e dall'utilizzo del sistema di storage di archiviazione. (Andare a **ARC Recupera Panoramica principale**.) I valori impostati per i timeout delle richieste e il numero di sessioni rese disponibili per le richieste di recupero sono particolarmente influenti.

Una volta completata l'integrazione, monitorare i recuperi dei dati dell'oggetto del nodo di archiviazione per stabilire i valori relativi ai tempi di recupero e alle lunghezze della coda normali. Quindi, creare allarmi personalizzati per ARQL e ARRL che si attiveranno in caso di condizioni operative anomale.

Informazioni correlate

["Monitor risoluzione dei problemi"](#)

Integrazione di Tivoli Storage Manager

Questa sezione include Best practice e informazioni sulla configurazione per l'integrazione di un nodo di archiviazione con un server Tivoli Storage Manager (TSM), inclusi i dettagli operativi del nodo di archiviazione che influiscono sulla configurazione del server TSM.

- ["Configurazione e funzionamento del nodo di archiviazione"](#)
- ["Best practice per la configurazione"](#)
- ["Completamento della configurazione del nodo di archiviazione"](#)

Configurazione e funzionamento del nodo di archiviazione

Il sistema StorageGRID gestisce il nodo di archiviazione come una posizione in cui gli oggetti vengono memorizzati a tempo indeterminato e sono sempre accessibili.

Quando viene acquisito un oggetto, le copie vengono eseguite in tutte le posizioni richieste, inclusi i nodi di archiviazione, in base alle regole di gestione del ciclo di vita delle informazioni (ILM) definite per il sistema StorageGRID. Il nodo di archiviazione funge da client per un server TSM e le librerie del client TSM vengono installate sul nodo di archiviazione mediante il processo di installazione del software StorageGRID. I dati dell'oggetto indirizzati al nodo di archiviazione per lo storage vengono salvati direttamente nel server TSM quando vengono ricevuti. Il nodo di archiviazione non esegue lo stage dei dati dell'oggetto prima di salvarli nel server TSM, né esegue l'aggregazione di oggetti. Tuttavia, il nodo di archiviazione può inviare più copie al server TSM in una singola transazione quando la velocità dei dati lo giustifica.

Dopo che il nodo di archiviazione ha salvato i dati dell'oggetto nel server TSM, i dati dell'oggetto vengono gestiti dal server TSM utilizzando i relativi criteri di conservazione/ciclo di vita. Questi criteri di conservazione devono essere definiti in modo da essere compatibili con il funzionamento del nodo di archiviazione. Ovvero, i dati degli oggetti salvati dal nodo di archiviazione devono essere memorizzati a tempo indeterminato e devono

essere sempre accessibili dal nodo di archiviazione, a meno che non vengano cancellati dal nodo di archiviazione.

Non esiste alcuna connessione tra le regole ILM del sistema StorageGRID e le policy di conservazione/ciclo di vita del server TSM. Ciascuno di essi opera indipendentemente dall'altro; tuttavia, quando ciascun oggetto viene acquisito nel sistema StorageGRID, è possibile assegnargli una classe di gestione TSM. Questa classe di gestione viene passata al server TSM insieme ai dati dell'oggetto. L'assegnazione di diverse classi di gestione a diversi tipi di oggetti consente di configurare il server TSM in modo che i dati degli oggetti siano memorizzati in diversi pool di storage o di applicare criteri di migrazione o conservazione diversi in base alle esigenze. Ad esempio, gli oggetti identificati come backup del database (contenuto temporaneo che può essere sovrascritto con dati più recenti) potrebbero essere trattati in modo diverso rispetto ai dati dell'applicazione (contenuto fisso che deve essere conservato a tempo indeterminato).

Il nodo di archiviazione può essere integrato con un server TSM nuovo o esistente; non richiede un server TSM dedicato. I server TSM possono essere condivisi con altri client, a condizione che il server TSM sia dimensionato in modo appropriato per il carico massimo previsto. TSM deve essere installato su un server o una macchina virtuale separato dal nodo di archiviazione.

È possibile configurare più di un nodo di archiviazione per la scrittura sullo stesso server TSM; tuttavia, questa configurazione è consigliata solo se i nodi di archiviazione scrivono set di dati diversi nel server TSM. La configurazione di più di un nodo di archivio per la scrittura sullo stesso server TSM non è consigliata quando ciascun nodo di archivio scrive copie degli stessi dati dell'oggetto nell'archivio. In quest'ultimo scenario, entrambe le copie sono soggette a un singolo punto di errore (il server TSM) per quelle che si suppone siano copie ridondanti indipendenti dei dati dell'oggetto.

I nodi di archiviazione non utilizzano il componente HSM (Hierarchical Storage Management) di TSM.

Best practice per la configurazione

Quando si esegue il dimensionamento e la configurazione del server TSM, è necessario applicare le Best practice per ottimizzarlo e utilizzarlo con il nodo di archiviazione.

Durante il dimensionamento e la configurazione del server TSM, è necessario considerare i seguenti fattori:

- Poiché il nodo di archiviazione non aggrega gli oggetti prima di salvarli nel server TSM, il database TSM deve essere dimensionato in modo da contenere riferimenti a tutti gli oggetti che verranno scritti nel nodo di archiviazione.
- Il software Archive Node non è in grado di tollerare la latenza necessaria per la scrittura di oggetti direttamente su nastro o su altri supporti rimovibili. Pertanto, il server TSM deve essere configurato con un pool di storage su disco per la memorizzazione iniziale dei dati salvati dal nodo di archiviazione ogni volta che si utilizzano supporti rimovibili.
- È necessario configurare i criteri di conservazione TSM per utilizzare la conservazione basata su eventi. Il nodo di archiviazione non supporta i criteri di conservazione TSM basati sulla creazione. Utilizzare le seguenti impostazioni consigliate di `retmin=0` e `retver=0` nel criterio di conservazione (che indica che la conservazione inizia quando il nodo di archiviazione attiva un evento di conservazione e viene mantenuta per 0 giorni dopo). Tuttavia, questi valori per `retmin` e `retver` sono facoltativi.

Il pool di dischi deve essere configurato per migrare i dati nel pool di nastri (ovvero, il pool di nastri deve essere il `NXTSTGPOOL` del pool di dischi). Il pool di nastri non deve essere configurato come pool di copie del pool di dischi con scrittura simultanea su entrambi i pool (ovvero, il pool di nastri non può essere un `COPYSTGPOOL` per il pool di dischi). Per creare copie non in linea dei nastri contenenti dati del nodo di archiviazione, configurare il server TSM con un secondo pool di nastri che è un pool di copie del pool di nastri utilizzato per i dati del nodo di archiviazione.

Completamento della configurazione del nodo di archiviazione

Il nodo di archiviazione non funziona dopo aver completato il processo di installazione. Prima che il sistema StorageGRID possa salvare gli oggetti nel nodo di archivio TSM, è necessario completare l'installazione e la configurazione del server TSM e configurare il nodo di archivio per comunicare con il server TSM.

Per ulteriori informazioni sull'ottimizzazione del recupero TSM e delle sessioni di archiviazione, consulta le informazioni sulla gestione dello storage di archiviazione.

- ["Gestione dei nodi di archiviazione"](#)

Fare riferimento alla seguente documentazione IBM, se necessario, durante la preparazione del server TSM per l'integrazione con il nodo di archiviazione in un sistema StorageGRID:

- ["Guida per l'installazione e l'utente dei driver di dispositivo su nastro IBM"](#)
- ["IBM Tape Device Drivers Programming Reference"](#)

Installazione di un nuovo server TSM

È possibile integrare il nodo di archiviazione con un server TSM nuovo o esistente. Se si sta installando un nuovo server TSM, seguire le istruzioni nella documentazione del TSM per completare l'installazione.



Un nodo di archiviazione non può essere co-ospitato con un server TSM.

Configurazione del server TSM

Questa sezione include istruzioni di esempio per la preparazione di un server TSM seguendo le Best practice del TSM.

Le seguenti istruzioni guidano l'utente nel processo di:

- Definizione di un pool di storage su disco e di un pool di storage su nastro (se necessario) sul server TSM
- Definizione di un criterio di dominio che utilizza la classe di gestione TSM per i dati salvati dal nodo di archiviazione e registrazione di un nodo per utilizzare questo criterio di dominio

Queste istruzioni sono fornite esclusivamente a scopo informativo; non sono intese a sostituire la documentazione del TSM o a fornire istruzioni complete e complete adatte a tutte le configurazioni. Le istruzioni specifiche per l'implementazione devono essere fornite da un amministratore TSM che abbia familiarità con i requisiti dettagliati e con la documentazione completa di TSM Server.

Definizione dei pool di storage su disco e nastro TSM

Il nodo di archiviazione scrive in un pool di dischi di storage. Per archiviare il contenuto su nastro, è necessario configurare il pool di storage su disco per spostare il contenuto in un pool di storage su nastro.

A proposito di questa attività

Per un server TSM, è necessario definire un pool di storage su nastro e un pool di storage su disco in Tivoli Storage Manager. Una volta definito il pool di dischi, creare un volume di dischi e assegnarlo al pool di dischi.

Non è necessario un pool di nastri se il server TSM utilizza lo storage solo-disco.

Prima di creare un pool di storage su nastro, è necessario completare una serie di passaggi sul server TSM. Creare una libreria di nastri e almeno un'unità nella libreria di nastri. Definire un percorso dal server alla libreria e dal server ai dischi, quindi definire una classe di dispositivi per i dischi. I dettagli di questi passaggi possono variare a seconda della configurazione hardware e dei requisiti di storage del sito. Per ulteriori informazioni, consultare la documentazione del TSM.

Il seguente set di istruzioni illustra il processo. Tenere presente che i requisiti del sito potrebbero essere diversi a seconda dei requisiti dell'implementazione. Per informazioni dettagliate sulla configurazione e istruzioni, consultare la documentazione del TSM.



È necessario accedere al server con privilegi amministrativi e utilizzare lo strumento `dsmacmc` per eseguire i seguenti comandi.

Fasi

1. Creare una libreria di nastri.

```
define library tapelibrary libtype=scsi
```

Dove *tapelibrary* è un nome arbitrario scelto per la libreria di nastri e il valore di *libtype* può variare a seconda del tipo di libreria di nastri.

2. Definire un percorso dal server alla libreria di nastri.

```
define path servername tapelibrary srctype=server desttype=library device=lib-devicename
```

- *servername* È il nome del server TSM
- *tapelibrary* è il nome della libreria di nastri definito
- *lib-devicename* è il nome del dispositivo per la libreria di nastri

3. Definire un disco per la libreria.

```
define drive tapelibrary drivename
```

- *drivename* è il nome che si desidera specificare per l'unità
- *tapelibrary* è il nome della libreria di nastri definito

A seconda della configurazione dell'hardware, potrebbe essere necessario configurare uno o più dischi aggiuntivi. Ad esempio, se il server TSM è collegato a uno switch Fibre Channel con due ingressi da una libreria di nastri, è possibile definire un'unità per ciascun ingresso.

4. Definire un percorso dal server all'unità definita.

```
define path servername drivename srctype=server desttype=drive  
library=tapelibrary device=drive-dname
```

- *drive-dname* è il nome del dispositivo per il disco
- *tapelibrary* è il nome della libreria di nastri definito

Ripetere l'operazione per ogni disco definito per la libreria di nastri, utilizzando un disco separato *drivename* e *drive-dname* per ciascun disco.

5. Definire una classe di dispositivi per i dischi.

```
define devclass DeviceClassName devtype=lto library=tapelibrary
format=tapetype
```

- *DeviceClassName* è il nome della classe device
- *lto* è il tipo di disco collegato al server
- *tapelibrary* è il nome della libreria di nastri definito
- *tapetype* è il tipo di nastro, ad esempio ultrium3

6. Aggiungere volumi su nastro all'inventario per la libreria.

```
checkin libvolume tapelibrary
```

tapelibrary è il nome della libreria di nastri definito.

7. Creare il pool di storage su nastro primario.

```
define stgpool SGWSTapePool DeviceClassName description=description
collocate=filespace maxscratch=XX
```

- *SGWSTapePool* È il nome del pool di storage su nastro del nodo di archiviazione. È possibile selezionare qualsiasi nome per il pool di storage su nastro (purché il nome utilizzi le convenzioni di sintassi previste dal server TSM).
- *DeviceClassName* è il nome della classe di dispositivi per la libreria di nastri.
- *description* È una descrizione del pool di storage che può essere visualizzato sul server TSM utilizzando `query stgpool` comando. Ad esempio: "Pool di storage su nastro per il nodo di archiviazione"
- *collocate=filespace* Specifica che il server TSM deve scrivere oggetti dallo stesso spazio di file in un singolo nastro.
- *XX* è uno dei seguenti:
 - Il numero di nastri vuoti nella libreria di nastri (nel caso in cui il nodo di archiviazione sia l'unica applicazione che utilizza la libreria).
 - Il numero di nastri allocati per l'utilizzo da parte del sistema StorageGRID (nei casi in cui la libreria di nastri è condivisa).

8. Su un server TSM, creare un pool di storage su disco. Nella console di amministrazione del server TSM, immettere

```
define stgpool SGWSDiskPool disk description=description
maxsize=maximum_file_size nextstgpool=SGWSTapePool highmig=percent_high
lowmig=percent_low
```

- *SGWSDiskPool* È il nome del pool di dischi del nodo di archiviazione. È possibile selezionare qualsiasi nome per il pool di storage su disco (purché il nome utilizzi le convenzioni di sintassi previste dal TSM).
- *description* È una descrizione del pool di storage che può essere visualizzato sul server TSM

utilizzando `query stgpool` comando. Ad esempio, "Disk storage pool for the Archive Node."

- `maximum_file_size` forza la scrittura diretta su nastro di oggetti di dimensioni superiori a tali, anziché la memorizzazione nella cache del pool di dischi. Si consiglia di impostare `maximum_file_size` A 10 GB.
- `nextstgpool=SGWSTapePool` Fa riferimento al pool di storage su disco al pool di storage su nastro definito per il nodo di archiviazione.
- `percent_high` imposta il valore in corrispondenza del quale il pool di dischi inizia la migrazione del contenuto nel pool di nastri. Si consiglia di impostare `percent_high` a 0 in modo che la migrazione dei dati inizi immediatamente
- `percent_low` imposta il valore in corrispondenza del quale la migrazione al pool di nastri viene interrotta. Si consiglia di impostare `percent_low` a 0 per eliminare il pool di dischi.

9. Su un server TSM, creare uno o più volumi di dischi e assegnarli al pool di dischi.

```
define volume SGWSDiskPool volume_name formatsize=size
```

- `SGWSDiskPool` è il nome del pool di dischi.
- `volume_name` è il percorso completo verso la posizione del volume (ad esempio, `/var/local/arc/stage6.dsm`) Sul server TSM in cui scrive il contenuto del pool di dischi in preparazione del trasferimento su nastro.
- `size` È la dimensione, in MB, del volume del disco.

Ad esempio, per creare un singolo volume di disco in modo che il contenuto di un pool di dischi occupi un singolo nastro, impostare il valore di `size` su 200000 quando il volume del nastro ha una capacità di 200 GB.

Tuttavia, potrebbe essere consigliabile creare più volumi di dischi di dimensioni inferiori, in quanto il server TSM può scrivere su ciascun volume del pool di dischi. Ad esempio, se la dimensione del nastro è di 250 GB, creare 25 volumi di dischi con una dimensione di 10 GB (10000) ciascuno.

Il server TSM preassegna lo spazio nella directory per il volume del disco. Il completamento di questa operazione può richiedere più di tre ore per un volume di disco da 200 GB.

Definizione di un criterio di dominio e registrazione di un nodo

È necessario definire un criterio di dominio che utilizzi la classe di gestione TSM per i dati salvati dal nodo di archiviazione, quindi registrare un nodo per utilizzare questo criterio di dominio.



I processi del nodo di archiviazione possono perdere memoria se la password del client per il nodo di archiviazione in Tivoli Storage Manager (TSM) scade. Assicurarsi che il server TSM sia configurato in modo che il nome utente/la password del client per il nodo di archiviazione non scada mai.

Quando si registra un nodo sul server TSM per l'utilizzo del nodo di archiviazione (o per l'aggiornamento di un nodo esistente), è necessario specificare il numero di punti di montaggio che il nodo può utilizzare per le operazioni di scrittura specificando il parametro `MAXNUMMP` nel comando `DEL NODO DI REGISTRO`. Il numero di punti di montaggio equivale in genere al numero di testine del disco a nastro allocate al nodo di archiviazione. Il numero specificato per `MAXNUMMP` sul server TSM deve essere grande almeno quanto il valore impostato per **ARC Target Configuration Main Maximum Store Sessions** per il nodo di archiviazione,

Che è impostato su un valore pari a 0 o 1, in quanto le sessioni dello store simultanee non sono supportate dal nodo di archiviazione.

Il valore di MAXSESSIONS impostato per il server TSM controlla il numero massimo di sessioni che possono essere aperte al server TSM da tutte le applicazioni client. Il valore di MAXSESSIONS specificato nel TSM deve essere almeno grande quanto il valore specificato per **ARC Target Configuration Main Number of Sessions** in Grid Manager per il nodo di archiviazione. Il nodo di archiviazione crea contemporaneamente al massimo una sessione per punto di montaggio più un piccolo numero (5) di sessioni aggiuntive.

Il nodo TSM assegnato al nodo di archiviazione utilizza una policy di dominio personalizzata `tsm-domain`. Il `tsm-domain` La policy di dominio è una versione modificata della policy di dominio "standard", configurata per la scrittura su nastro e con la destinazione dell'archivio impostata come pool di storage del sistema StorageGRID (`SGWSDiskPool`).



È necessario accedere al server TSM con privilegi amministrativi e utilizzare lo strumento `dsmacmc` per creare e attivare i criteri di dominio.

Creazione e attivazione dei criteri di dominio

È necessario creare un criterio di dominio e attivarlo per configurare il server TSM in modo da salvare i dati inviati dal nodo di archiviazione.

Fasi

1. Creare un criterio di dominio.

```
copy domain standard tsm-domain
```

2. Se non si utilizza una classe di gestione esistente, immettere una delle seguenti informazioni:

```
define policyset tsm-domain standard
```

```
define mgmtclass tsm-domain standard default
```

default è la classe di gestione predefinita per l'implementazione.

3. Creare un gruppo di copygroup nel pool di storage appropriato. Immettere (su una riga):

```
define copygroup tsm-domain standard default type=archive  
destination=SGWSDiskPool retinit=event retmin=0 retver=0
```

default È la classe di gestione predefinita per il nodo di archiviazione. I valori di `retinit`, `retmin`, e `retver` Sono stati scelti per riflettere il comportamento di conservazione attualmente utilizzato dal nodo di archiviazione



Non impostare `retinit a. retinit=create`. Impostazione `retinit=create` Impedisce al nodo di archiviazione di eliminare il contenuto, poiché gli eventi di conservazione vengono utilizzati per rimuovere il contenuto dal server TSM.

4. Assegnare la classe di gestione come predefinita.

```
assign defmgmtclass tsm-domain standard default
```

5. Impostare il nuovo set di criteri come attivo.

```
activate policyset tsm-domain standard
```

Ignorare l'avviso "no backup copy group" visualizzato quando si immette il comando Activate.

6. Registrare un nodo per utilizzare il nuovo set di criteri sul server TSM. Sul server TSM, immettere (su una riga):

```
register node arc-user arc-password passexp=0 domain=tsm-domain  
MAXNUMMP=number-of-sessions
```

Arc-user e Arc-password sono lo stesso nome e password del nodo client definiti nel nodo di archiviazione e il valore di MAXNUMMP è impostato sul numero di unità nastro riservate per le sessioni di archiviazione del nodo di archiviazione.



Per impostazione predefinita, la registrazione di un nodo crea un ID utente amministrativo con l'autorità del proprietario del client, con la password definita per il nodo.

Migrazione dei dati in StorageGRID

È possibile migrare grandi quantità di dati nel sistema StorageGRID utilizzando contemporaneamente il sistema StorageGRID per le operazioni quotidiane.

La sezione seguente è una guida alla comprensione e alla pianificazione di una migrazione di grandi quantità di dati nel sistema StorageGRID. Non si tratta di una guida generale alla migrazione dei dati e non include procedure dettagliate per l'esecuzione di una migrazione. Seguire le linee guida e le istruzioni di questa sezione per garantire che i dati vengano migrati in modo efficiente nel sistema StorageGRID senza interferire con le operazioni quotidiane e che i dati migrati vengano gestiti in modo appropriato dal sistema StorageGRID.

- ["Conferma della capacità del sistema StorageGRID"](#)
- ["Determinazione del criterio ILM per i dati migrati"](#)
- ["Impatto della migrazione sulle operazioni"](#)
- ["Pianificazione della migrazione dei dati"](#)
- ["Monitoraggio della migrazione dei dati"](#)
- ["Creazione di notifiche personalizzate per gli allarmi di migrazione"](#)

Conferma della capacità del sistema StorageGRID

Prima di migrare grandi quantità di dati nel sistema StorageGRID, verificare che il sistema StorageGRID disponga della capacità del disco necessaria per gestire il volume previsto.

Se il sistema StorageGRID include un nodo di archiviazione e una copia degli oggetti migrati è stata salvata nello storage nearline (come il nastro), assicurarsi che lo storage del nodo di archiviazione disponga di capacità sufficiente per il volume previsto dei dati migrati.

Nell'ambito della valutazione della capacità, esaminare il profilo dei dati degli oggetti che si intende migrare e calcolare la quantità di capacità del disco richiesta. Per ulteriori informazioni sul monitoraggio della capacità del disco del sistema StorageGRID, consultare le istruzioni per il monitoraggio e la risoluzione dei problemi di

StorageGRID.

Informazioni correlate

["Monitor risoluzione dei problemi"](#)

["Gestione dei nodi di storage"](#)

Determinazione del criterio ILM per i dati migrati

Il criterio ILM del sistema StorageGRID determina il numero di copie eseguite, le posizioni in cui vengono memorizzate e il periodo di conservazione delle copie. Un criterio ILM è costituito da un insieme di regole ILM che descrivono come filtrare gli oggetti e gestire i dati degli oggetti nel tempo.

A seconda del modo in cui vengono utilizzati i dati migrati e dei requisiti per i dati migrati, è possibile definire regole ILM univoche per i dati migrati che sono diverse dalle regole ILM utilizzate per le operazioni quotidiane. Ad esempio, se esistono requisiti normativi diversi per la gestione quotidiana dei dati rispetto ai dati inclusi nella migrazione, è possibile che si desideri un numero diverso di copie dei dati migrati su un diverso livello di storage.

È possibile configurare regole che si applicano esclusivamente ai dati migrati se è possibile distinguere in modo univoco tra i dati migrati e i dati oggetto salvati dalle operazioni quotidiane.

Se è possibile distinguere in modo affidabile tra i tipi di dati utilizzando uno dei criteri dei metadati, è possibile utilizzare questi criteri per definire una regola ILM che si applica solo ai dati migrati.

Prima di iniziare la migrazione dei dati, assicurarsi di aver compreso il criterio ILM del sistema StorageGRID e il modo in cui verrà applicato ai dati migrati e di aver apportato e verificato eventuali modifiche al criterio ILM.



Un criterio ILM specificato in modo non corretto può causare una perdita di dati irreversibile. Esaminare attentamente tutte le modifiche apportate a un criterio ILM prima di attivarlo per assicurarsi che il criterio funzioni come previsto.

Informazioni correlate

["Gestire gli oggetti con ILM"](#)

Impatto della migrazione sulle operazioni

Un sistema StorageGRID è progettato per fornire un funzionamento efficiente per lo storage e il recupero di oggetti e per fornire un'eccellente protezione contro la perdita di dati attraverso la creazione perfetta di copie ridondanti di dati a oggetti e metadati.

Tuttavia, la migrazione dei dati deve essere gestita con attenzione in base alle istruzioni di questo capitolo per evitare di avere un impatto sulle operazioni quotidiane del sistema o, in casi estremi, mettere i dati a rischio di perdita in caso di guasto nel sistema StorageGRID.

La migrazione di grandi quantità di dati pone un carico aggiuntivo sul sistema. Quando il sistema StorageGRID viene caricato pesantemente, risponde più lentamente alle richieste di archiviazione e recupero degli oggetti. Ciò può interferire con le richieste di archiviazione e recupero che sono parte integrante delle operazioni quotidiane. La migrazione può anche causare altri problemi operativi. Ad esempio, quando un nodo di storage si sta avvicinando alla capacità, il carico intermittente elevato dovuto all'acquisizione batch può causare il ciclo del nodo di storage tra sola lettura e lettura/scrittura, generando notifiche.

Se il carico pesante persiste, è possibile sviluppare code per varie operazioni che il sistema StorageGRID deve eseguire per garantire la ridondanza completa dei dati degli oggetti e dei metadati.

La migrazione dei dati deve essere gestita con attenzione in base alle linee guida del presente documento per garantire un funzionamento sicuro ed efficiente del sistema StorageGRID durante la migrazione. Durante la migrazione dei dati, acquisire oggetti in batch o ridurre continuamente l'acquisizione. Quindi, monitorare continuamente il sistema StorageGRID per assicurarsi che i vari valori degli attributi non vengano superati.

Pianificazione della migrazione dei dati

Evita la migrazione dei dati durante le ore di funzionamento principali. Limitare la migrazione dei dati a serate, fine settimana e altri periodi in cui l'utilizzo del sistema è basso.

Se possibile, non pianificare la migrazione dei dati durante i periodi di attività elevata. Tuttavia, se non è pratico evitare completamente il periodo di attività elevato, è sicuro procedere finché si monitorano attentamente gli attributi pertinenti e si interviene se superano i valori accettabili.

Informazioni correlate

["Monitoraggio della migrazione dei dati"](#)

Monitoraggio della migrazione dei dati

La migrazione dei dati deve essere monitorata e regolata in base alle necessità per garantire che i dati vengano inseriti in base alla policy ILM entro i tempi richiesti.

Questa tabella elenca gli attributi da monitorare durante la migrazione dei dati e i problemi che rappresentano.

Se si utilizzano criteri di classificazione del traffico con limiti di velocità per accelerare l'acquisizione, è possibile monitorare la velocità osservata insieme alle statistiche descritte nella tabella seguente e ridurre i limiti, se necessario.

Monitorare	Descrizione
Numero di oggetti in attesa di valutazione ILM	<ol style="list-style-type: none">1. Selezionare supporto > Strumenti > topologia griglia.2. Selezionare Deployment Overview Main.3. Nella sezione ILM Activity (attività ILM), monitorare il numero di oggetti visualizzati per i seguenti attributi:<ul style="list-style-type: none">◦ In attesa - tutti (XQUZ): Il numero totale di oggetti in attesa di valutazione ILM.◦ In attesa - Client (XCQZ): Il numero totale di oggetti in attesa di valutazione ILM dalle operazioni del client (ad esempio, acquisizione).4. Se il numero di oggetti visualizzato per uno di questi attributi supera 100,000, ridurre il tasso di acquisizione degli oggetti per ridurre il carico sul sistema StorageGRID.

Monitorare	Descrizione
Capacità di storage del sistema di archiviazione mirato	Se la policy ILM salva una copia dei dati migrati in un sistema storage di archiviazione di destinazione (nastro o cloud), monitorate la capacità del sistema storage di archiviazione di destinazione per garantire che vi sia una capacità sufficiente per i dati migrati.
Nodo di archivio ARC Memorizza	Se viene attivato un allarme per l'attributo Store Failures (ARVF) , il sistema storage di archiviazione di destinazione potrebbe aver raggiunto la capacità. Controllare il sistema storage di archiviazione di destinazione e risolvere eventuali problemi che hanno generato un allarme.

Creazione di notifiche personalizzate per gli allarmi di migrazione

È possibile che StorageGRID invii notifiche di avviso o notifiche di allarme (sistema legacy) all'amministratore di sistema responsabile del monitoraggio della migrazione se determinati valori superano le soglie consigliate.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.
- È necessario aver configurato le impostazioni e-mail per le notifiche di avviso (o allarme).

Fasi

1. Creare una regola di avviso personalizzata o un allarme personalizzato globale per ogni metrica Prometheus o attributo StorageGRID che si desidera monitorare durante la migrazione dei dati.

Gli avvisi vengono attivati in base ai valori delle metriche Prometheus. Gli allarmi vengono attivati in base ai valori degli attributi. Per ulteriori informazioni, consultare le istruzioni per il monitoraggio e la risoluzione dei problemi di StorageGRID.

2. Disattivare la regola di avviso personalizzata o l'allarme Global Custom al termine della migrazione dei dati.

Gli allarmi Global Custom hanno la precedenza su quelli predefiniti.

Informazioni correlate

["Monitor risoluzione dei problemi"](#)

Gestire gli oggetti con ILM

Scopri come gestire gli oggetti con le regole e le policy del ciclo di vita delle informazioni e come utilizzare S3 Object Lock per rispettare le normative per la conservazione degli oggetti.

- ["Gestione degli oggetti con la gestione del ciclo di vita delle informazioni"](#)
- ["Gestione degli oggetti con S3 Object Lock"](#)

- ["Esempio di regole e policy ILM"](#)

Gestione degli oggetti con la gestione del ciclo di vita delle informazioni

È possibile gestire gli oggetti in un sistema StorageGRID configurando le regole e le policy di Information Lifecycle Management (ILM). Le regole e i criteri ILM spiegano a StorageGRID come creare e distribuire copie di dati a oggetti e come gestirle nel tempo.

La progettazione e l'implementazione delle regole ILM e della policy ILM richiede 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 determinare come si desidera copiare, distribuire e memorizzare diversi tipi di oggetti.

- ["Come ILM opera per tutta la vita di un oggetto"](#)
- ["Che cos'è una policy ILM"](#)
- ["Che cos'è una regola ILM"](#)
- ["Creazione di livelli di storage, pool di storage, profili EC e regioni"](#)
- ["Creazione di una regola ILM"](#)
- ["Creazione di un criterio ILM"](#)
- ["Utilizzo delle regole ILM e delle policy ILM"](#)

Come ILM opera per tutta la vita di un oggetto

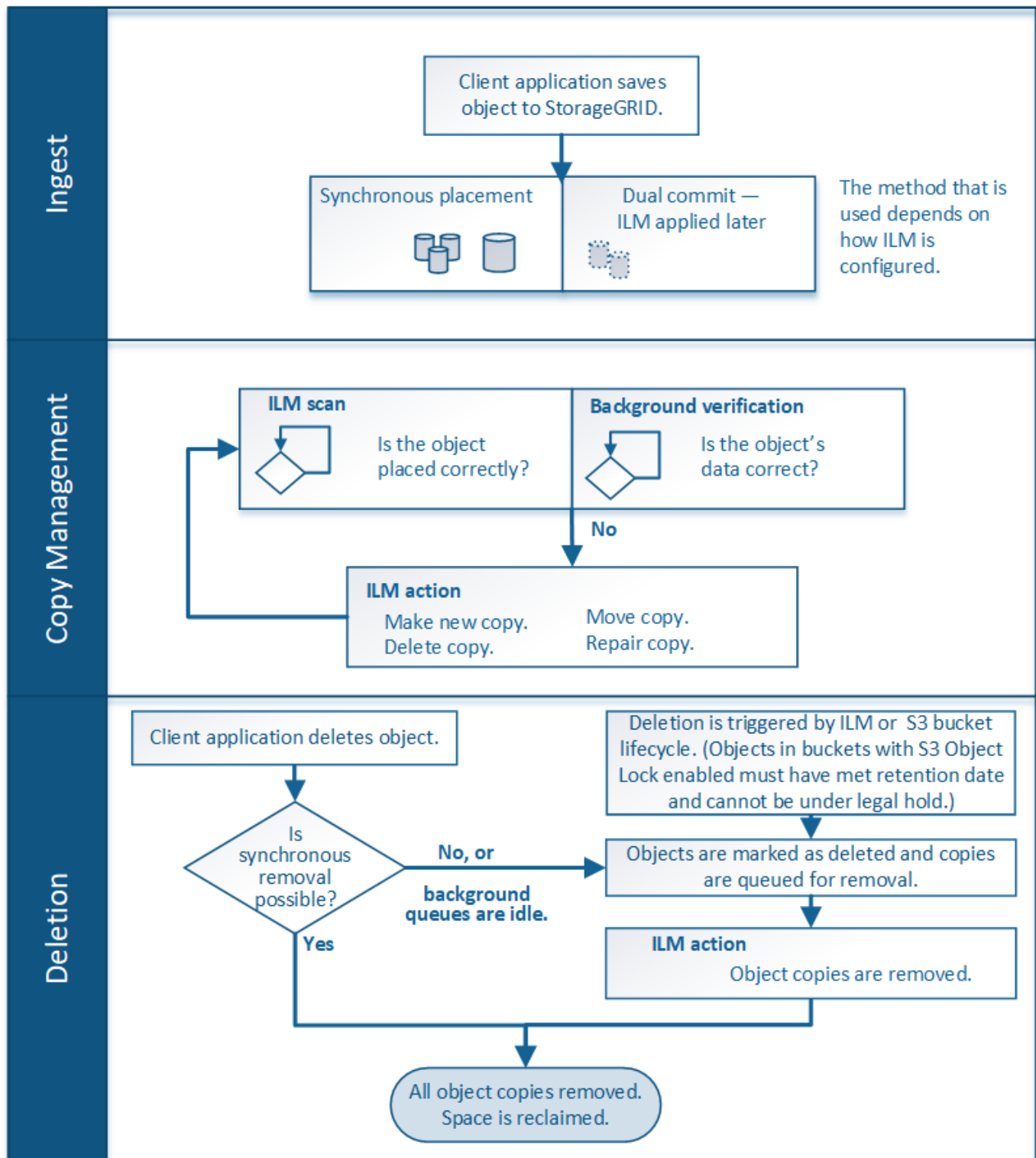
Comprendere come StorageGRID utilizza ILM per gestire gli oggetti in ogni fase della loro vita può aiutarti a progettare una policy più efficace.

- **Ingest:** L'acquisizione inizia quando un'applicazione client S3 o Swift stabilisce una connessione per salvare un oggetto nel sistema StorageGRID e viene completata quando StorageGRID restituisce un messaggio "Engest Successful" al client. I dati degli oggetti vengono protetti durante l'acquisizione applicando immediatamente le istruzioni ILM (posizionamento sincrono) o creando copie interinali e applicando ILM successivamente (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 di ILM, StorageGRID gestisce le posizioni degli oggetti e protegge gli oggetti dalla perdita.
 - Scansione e valutazione ILM: StorageGRID esegue una scansione continua dell'elenco di oggetti memorizzati nella griglia e verifica se le copie correnti soddisfano i requisiti ILM. Quando sono richiesti tipi, numeri o posizioni diversi di copie di oggetti, StorageGRID crea, elimina o sposta le copie in base alle necessità.
 - Verifica in background: StorageGRID esegue continuamente la verifica in background per verificare l'integrità dei dati dell'oggetto. Se viene rilevato un problema, StorageGRID crea automaticamente una nuova copia dell'oggetto o un frammento di oggetto erasure-coded sostitutivo in una posizione che soddisfa i requisiti ILM correnti. Consultare le istruzioni per il monitoraggio e la risoluzione dei problemi di StorageGRID.
- **Eliminazione oggetto:** La gestione di un oggetto termina quando tutte le copie vengono rimosse dal sistema StorageGRID. Gli oggetti possono essere rimossi in seguito a una richiesta di eliminazione da parte di un client o in seguito all'eliminazione da parte di ILM o all'eliminazione causata dalla scadenza di un ciclo di vita del bucket S3.



Gli oggetti in un bucket con S3 Object Lock abilitato non possono essere cancellati se sono in stato di conservazione legale o se è stata specificata una data di conservazione fino alla data, ma non ancora soddisfatta.

Il diagramma riassume il funzionamento di ILM durante l'intero ciclo di vita di un oggetto.



Informazioni correlate

["Monitor risoluzione dei problemi"](#)

Modalità di acquisizione degli oggetti

StorageGRID protegge gli oggetti durante l'acquisizione eseguendo il posizionamento sincrono o eseguendo il commit doppio, come specificato nella regola ILM che corrisponde agli oggetti.

Quando un client S3 o Swift memorizza un oggetto nella griglia, StorageGRID acquisisce l'oggetto utilizzando uno dei due metodi seguenti:

- **Posizionamento sincrono:** StorageGRID crea immediatamente tutte le copie degli oggetti necessarie per soddisfare i requisiti ILM. StorageGRID invia un messaggio "ingest Successful" al client al momento della creazione di tutte le copie.

Se StorageGRID non riesce a creare immediatamente tutte le copie degli oggetti (ad esempio, perché una posizione richiesta non è temporaneamente disponibile), invia un messaggio "ingest failed" al client. In alternativa, è possibile creare copie temporanee degli oggetti e valutare ILM in un secondo momento, a seconda della scelta effettuata al momento della creazione della regola ILM.

- **Doppio commit:** StorageGRID crea immediatamente due copie temporanee dell'oggetto, ciascuna su un nodo di storage diverso, e invia un messaggio "acquisizione riuscita" al client. StorageGRID inserisce quindi in coda l'oggetto per la valutazione ILM.

Quando StorageGRID esegue la valutazione ILM, verifica innanzitutto se le copie intermedie soddisfano le istruzioni di posizionamento della regola ILM. Ad esempio, le due copie intermedie potrebbero soddisfare le istruzioni di una regola ILM a due copie, ma non soddisferebbero le istruzioni di una regola di erasure coding. Se le copie intermedie non soddisfano le istruzioni ILM, StorageGRID crea nuove copie a oggetti ed elimina le copie temporanee non necessarie.

Se StorageGRID non riesce a creare due copie intermedie (ad esempio, se un problema di rete impedisce la creazione della seconda copia), StorageGRID non riprova. L'acquisizione non riesce.



I client S3 o Swift possono specificare che StorageGRID crea una singola copia provvisoria al momento dell'acquisizione specificando `REDUCED_REDUNDANCY` per la classe di storage. Per ulteriori informazioni, consultare le istruzioni per l'implementazione di un client S3 o Swift.

Per impostazione predefinita, StorageGRID utilizza il posizionamento sincrono per proteggere gli oggetti durante l'acquisizione.

Informazioni correlate

["Opzioni di protezione dei dati per l'acquisizione"](#)

["Utilizzare S3"](#)

["USA Swift"](#)

Opzioni di protezione dei dati per l'acquisizione

Quando si crea una regola ILM, si specifica una delle tre opzioni per la protezione degli oggetti in fase di acquisizione: Dual commit, balanced o strict. A seconda della scelta, StorageGRID esegue copie temporanee e mette in coda gli oggetti per la valutazione ILM in un secondo momento, oppure utilizza il posizionamento sincrono e crea

immediatamente copie per soddisfare i requisiti ILM.

Commit doppio

Quando si seleziona l'opzione doppio commit, StorageGRID esegue immediatamente copie temporanee degli oggetti su due nodi di storage diversi e restituisce un messaggio "ingest Successful" al client. L'oggetto viene messo in coda per la valutazione ILM e le copie che soddisfano le istruzioni di posizionamento della regola vengono eseguite in un secondo momento.

Quando utilizzare l'opzione Dual Commit

Utilizzare l'opzione Dual Commit in uno dei seguenti casi:

- Stai utilizzando regole ILM multi-sito e la latenza di acquisizione client è la tua principale considerazione. Quando si utilizza il doppio commit, è necessario assicurarsi che la griglia possa eseguire il lavoro aggiuntivo di creazione e rimozione delle copie a doppio commit se non soddisfano ILM. In particolare:
 - Il carico sulla griglia deve essere sufficientemente basso da impedire un backlog ILM.
 - La griglia deve avere risorse hardware in eccesso (IOPS, CPU, memoria, larghezza di banda della rete e così via).
- Si stanno utilizzando regole ILM multi-sito e la connessione WAN tra i siti in genere ha una latenza elevata o una larghezza di banda limitata. In questo scenario, l'utilizzo dell'opzione di commit doppio può contribuire a prevenire i timeout del client. Prima di scegliere l'opzione Dual Commit, è necessario testare l'applicazione client con carichi di lavoro realistici.

Rigoroso

Quando si seleziona l'opzione Strict, StorageGRID utilizza il posizionamento sincrono all'acquisizione e crea 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 storage richiesta non è temporaneamente disponibile. Il client deve riprovare l'operazione.

Quando utilizzare l'opzione Strict

Utilizzare l'opzione Strict se si dispone di un requisito operativo o normativo per memorizzare immediatamente gli oggetti solo nelle posizioni indicate nella regola ILM. Ad esempio, per soddisfare un requisito normativo, potrebbe essere necessario utilizzare l'opzione Strict e un filtro avanzato Location Constraint per garantire che gli oggetti non vengano mai memorizzati in un determinato data center.

["Esempio 5: Regole e policy ILM per un comportamento rigoroso di acquisizione"](#)

Bilanciato

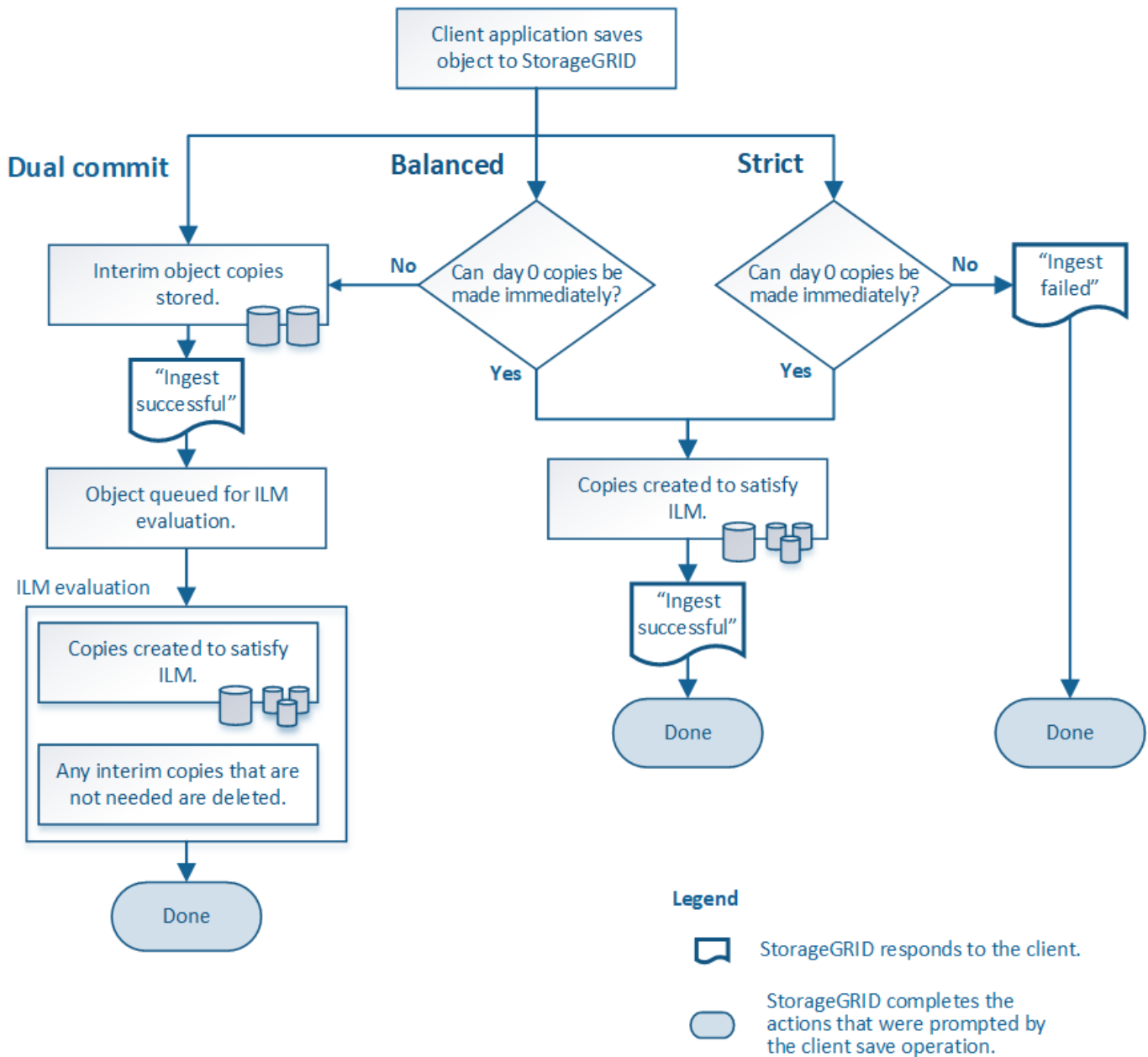
Quando si seleziona l'opzione Balanced (bilanciamento), StorageGRID utilizza anche il posizionamento sincrono all'acquisizione e crea immediatamente tutte le copie specificate nelle istruzioni di posizionamento della regola. In contrasto con l'opzione rigorosa, se StorageGRID non riesce a eseguire immediatamente tutte le copie, utilizza invece il doppio commit.

Quando utilizzare l'opzione Balanced (bilanciamento)

Utilizza l'opzione Balanced per ottenere la migliore combinazione di protezione dei dati, performance di grid e successo di acquisizione. Balanced (bilanciamento) è l'opzione predefinita nella creazione guidata regole ILM.

Diagramma di flusso di tre opzioni di acquisizione

Il diagramma di flusso mostra cosa accade quando gli oggetti vengono associati da una regola ILM che utilizza una di queste opzioni di acquisizione.



Informazioni correlate

["Modalità di acquisizione degli oggetti"](#)

Vantaggi, svantaggi e limitazioni delle opzioni di protezione dei dati

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 aiutare a decidere quale scegliere per una regola ILM.

Vantaggi delle opzioni bilanciate e rigorose

Rispetto al doppio commit, che crea copie intermedie durante l'acquisizione, le due opzioni di posizionamento sincrono possono offrire i seguenti vantaggi:

- **Maggiore sicurezza dei dati:** I dati degli oggetti sono immediatamente protetti come specificato nelle istruzioni di posizionamento della regola ILM, che possono essere configurate per la protezione da un'ampia varietà di condizioni di guasto, incluso il guasto di più di una posizione di storage. Il doppio commit può proteggere solo dalla perdita di una singola copia locale.
- **Operazione grid più efficiente:** Ogni oggetto viene elaborato una sola volta, man mano che viene acquisito. Poiché il sistema StorageGRID non deve tenere traccia o eliminare le copie temporanee, il carico di elaborazione è inferiore e lo spazio del database viene consumato meno.
- **(Balanced) Recommended (consigliato):** L'opzione Balanced (bilanciato) offre un'efficienza ILM ottimale. Si consiglia di utilizzare l'opzione Balanced (bilanciato) a meno che non sia richiesto un comportamento rigoroso di acquisizione o che la griglia soddisfi tutti i criteri per l'utilizzo di Dual Commit.
- **(Strict) certezze circa le posizioni degli oggetti:** L'opzione Strict garantisce che gli oggetti siano memorizzati immediatamente in base alle istruzioni di posizionamento nella regola ILM.

Svantaggi delle opzioni bilanciate e rigide

Rispetto al doppio commit, le opzioni bilanciate e rigide presentano alcuni svantaggi:

- **Ingest dei client più lunghi:** Le latenze di acquisizione dei client potrebbero essere più lunghe. Quando si utilizzano le opzioni bilanciate e rigorose, un messaggio "ingest Successful" (acquisizione riuscita) non viene restituito al client fino a quando non vengono creati e memorizzati tutti i frammenti con codifica di cancellazione o le copie replicate. Tuttavia, è molto probabile che i dati degli oggetti raggiungano il posizionamento finale molto più rapidamente.
- **(Strict) tassi più elevati di errore di acquisizione:** Con l'opzione Strict, l'acquisizione non riesce ogni volta che StorageGRID non è in grado di eseguire immediatamente tutte le copie specificate nella regola ILM. Se una posizione di storage richiesta è temporaneamente offline o se problemi di rete causano ritardi nella copia di oggetti tra siti, potrebbero verificarsi elevati tassi di errore di acquisizione.
- **(Strict) le posizioni di caricamento multiparte S3 potrebbero non essere quelle previste in alcune circostanze:** Con Strict, si prevede che gli oggetti vengano posizionati come descritto dalla regola ILM o che l'acquisizione non funzioni. Tuttavia, con un caricamento S3 multiparte, ILM viene valutato per ogni parte dell'oggetto così come è stato acquisito e per l'oggetto nel suo complesso al termine del caricamento multiparte. Nei seguenti casi, ciò potrebbe comportare posizionamenti diversi da quelli previsti:
 - **Se ILM cambia mentre è in corso un caricamento di più parti S3:** Poiché ogni parte viene posizionata in base alla regola attiva quando la parte viene inserita, alcune parti dell'oggetto potrebbero non soddisfare i requisiti ILM correnti al termine del caricamento di più parti. In questi casi, l'acquisizione dell'oggetto non ha esito negativo. Al contrario, qualsiasi parte non posizionata correttamente viene messa in coda per la rivalutazione ILM e spostata nella posizione corretta in un secondo momento.
 - **Quando le regole ILM filtrano sulla dimensione:** Quando si valuta ILM per una parte, StorageGRID filtra sulla dimensione della parte, non sulla dimensione dell'oggetto. Ciò significa che parti di un oggetto possono essere memorizzate 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 superiori sono memorizzati in DC1 mentre tutti gli oggetti più piccoli sono memorizzati in DC2, ogni parte da 1 GB di un caricamento multiparte da 10 parti viene memorizzata in DC2. Quando ILM viene valutato per l'oggetto, tutte le parti dell'oggetto vengono spostate in DC1.
- **(Strict) Ingest non ha esito negativo quando i tag degli oggetti o i metadati vengono aggiornati e non è possibile eseguire le nuove posizioni richieste:** Con Strict, si prevede che gli oggetti vengano

posizionati come descritto dalla regola ILM o che l'acquisizione non riesca. Tuttavia, quando si aggiornano metadati o tag per un oggetto già memorizzato nella griglia, l'oggetto non viene reinserito. Ciò significa che le modifiche al posizionamento degli oggetti che vengono attivate dall'aggiornamento non vengono apportate immediatamente. Le modifiche al posizionamento vengono apportate quando ILM viene rivalutato dai normali processi ILM in background. Se non è possibile apportare modifiche al posizionamento richieste (ad esempio, perché non è disponibile una nuova posizione richiesta), l'oggetto aggiornato mantiene la posizione corrente fino a quando non sono possibili modifiche al posizionamento.

Limitazioni al posizionamento degli oggetti con opzioni bilanciate o rigide

Le opzioni bilanciate o rigide non possono essere utilizzate per le regole ILM che hanno una delle seguenti istruzioni di posizionamento:

- Posizionamento in un pool di storage cloud al giorno 0.
- Posizionamento in un nodo di archivio al giorno 0.
- Posizionamenti in un pool di storage cloud o in un nodo di archivio quando la regola ha un tempo di creazione definito dall'utente come tempo di riferimento.

Queste restrizioni esistono perché StorageGRID non può eseguire copie in modo sincrono a un pool di storage cloud o a un nodo di archivio e un tempo di creazione definito dall'utente potrebbe risolversi fino al momento attuale.

Come interagiscono le regole ILM e i controlli di coerenza per influire sulla protezione dei dati

Sia la regola ILM che la scelta del controllo di coerenza influiscono sulla modalità di protezione degli oggetti. Queste impostazioni possono interagire.

Ad esempio, il comportamento di acquisizione selezionato per una regola ILM influisce sul posizionamento iniziale delle copie degli oggetti, mentre il controllo di coerenza utilizzato quando viene memorizzato un oggetto influisce sul posizionamento iniziale dei metadati degli oggetti. Poiché StorageGRID richiede l'accesso sia ai metadati di un oggetto che ai suoi dati per soddisfare le richieste dei client, la selezione dei livelli di protezione corrispondenti per il livello di coerenza e il comportamento di acquisizione può fornire una migliore protezione iniziale dei dati e risposte di sistema più prevedibili.

Ecco un breve riepilogo dei controlli di coerenza disponibili in StorageGRID:

- **All:** Tutti i nodi ricevono immediatamente i metadati dell'oggetto o la richiesta non riesce.
- **Strong-Global:** I metadati degli oggetti vengono distribuiti immediatamente a tutti i siti. Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client in tutti i siti.
- **Strong-Site:** I metadati degli oggetti vengono distribuiti immediatamente ad altri nodi del sito. Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client all'interno di un sito.
- **Read-after-new-write:** Fornisce coerenza di lettura dopo scrittura per nuovi oggetti ed eventuale coerenza per gli aggiornamenti degli oggetti. Offre alta disponibilità e garanzie di protezione dei dati.
- **Available** (eventuale coerenza per le operazioni HEAD): Si comporta come il livello di coerenza "read-after-new-write", ma fornisce solo una coerenza finale per le operazioni HEAD.



Prima di selezionare un livello di coerenza, leggere la descrizione completa di queste impostazioni nelle istruzioni per la creazione di un'applicazione client S3 o Swift. Prima di modificare il valore predefinito, è necessario comprendere i vantaggi e le limitazioni.

Esempio di come il controllo di coerenza e la regola ILM possono interagire

Si supponga di disporre di una griglia a due siti con la seguente regola ILM e la seguente impostazione del livello di coerenza:

- **ILM rule:** Creare due copie di oggetti, una nel sito locale e una in un sito remoto. Viene selezionato il comportamento rigoroso dell'acquisizione.
- **Livello di 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 degli oggetti e distribuisce i metadati a entrambi i siti prima di restituire il risultato al client.

L'oggetto è completamente protetto contro la perdita al momento dell'acquisizione del messaggio di successo. Ad esempio, se il sito locale viene perso poco dopo l'acquisizione, le copie dei dati dell'oggetto e dei metadati dell'oggetto rimangono nel sito remoto. L'oggetto è completamente recuperabile.

Se invece sono state utilizzate la stessa regola ILM e il livello di coerenza "strong-site", il client potrebbe ricevere un messaggio di successo dopo la replica dei dati dell'oggetto nel sito remoto, ma prima della distribuzione dei metadati dell'oggetto. 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 poco dopo l'acquisizione, i metadati dell'oggetto andranno persi. Impossibile recuperare l'oggetto.

L'interconnessione tra i livelli di coerenza e le regole ILM può essere complessa. Contattare NetApp per assistenza.

Informazioni correlate

["Che cos'è la replica"](#)

["Che cos'è la cancellazione dei codici"](#)

["Quali sono gli schemi di erasure coding"](#)

["Esempio 5: Regole e policy ILM per un comportamento rigoroso di acquisizione"](#)

["Utilizzare S3"](#)

["USA Swift"](#)

Modalità di archiviazione degli oggetti (replica o erasure coding)

StorageGRID è in grado di proteggere gli oggetti dalla perdita memorizzando copie replicate o copie codificate per la cancellazione. Specificare il tipo di copie da creare nelle istruzioni di posizionamento delle regole ILM.

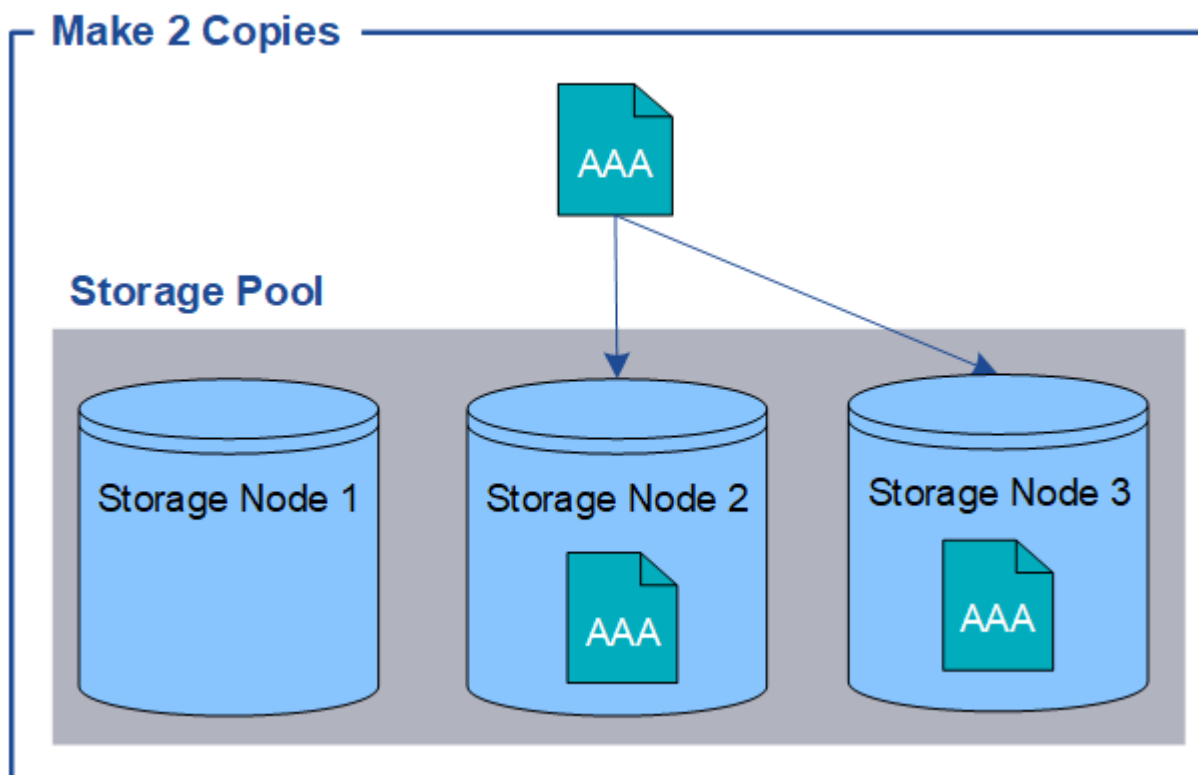
- ["Che cos'è la replica"](#)
- ["Perché non utilizzare la replica a copia singola"](#)
- ["Che cos'è la cancellazione dei codici"](#)
- ["Quali sono gli schemi di erasure coding"](#)
- ["Vantaggi, svantaggi e requisiti per l'erasure coding"](#)

Che cos'è la replica

La replica è uno dei due metodi utilizzati da StorageGRID per memorizzare i dati degli oggetti. Quando gli oggetti corrispondono a una regola ILM che utilizza la replica, il sistema crea copie esatte dei dati dell'oggetto e le memorizza nei nodi di storage o nei nodi di archivio.

Quando si configura una regola ILM per la creazione di copie replicate, specificare il numero di copie da creare, la posizione delle copie e la durata della memorizzazione delle copie in ciascuna posizione.

Nell'esempio seguente, la regola ILM specifica che due copie replicate di ciascun oggetto devono essere collocate in un pool di storage che contiene tre nodi di storage.



Quando StorageGRID associa gli oggetti a questa regola, crea due copie dell'oggetto, collocando ciascuna copia su un nodo di storage diverso nel pool di storage. Le due copie possono essere collocate su due dei tre nodi di storage disponibili. In questo caso, la regola ha posizionato le copie degli oggetti sui nodi di storage 2 e 3. Poiché sono presenti due copie, l'oggetto può essere recuperato in caso di guasto di uno qualsiasi dei nodi del pool di storage.



StorageGRID può memorizzare solo una copia replicata di un oggetto su un dato nodo di storage. Se la griglia include tre nodi di storage e si crea una regola ILM di 4 copie, verranno eseguite solo tre copie, una copia per ciascun nodo di storage. Viene attivato l'avviso **ILM placement unachievable** per indicare che la regola ILM non può essere applicata completamente.

Informazioni correlate

["Che cos'è un pool di storage"](#)

["Utilizzo di più pool di storage per la replica tra siti"](#)

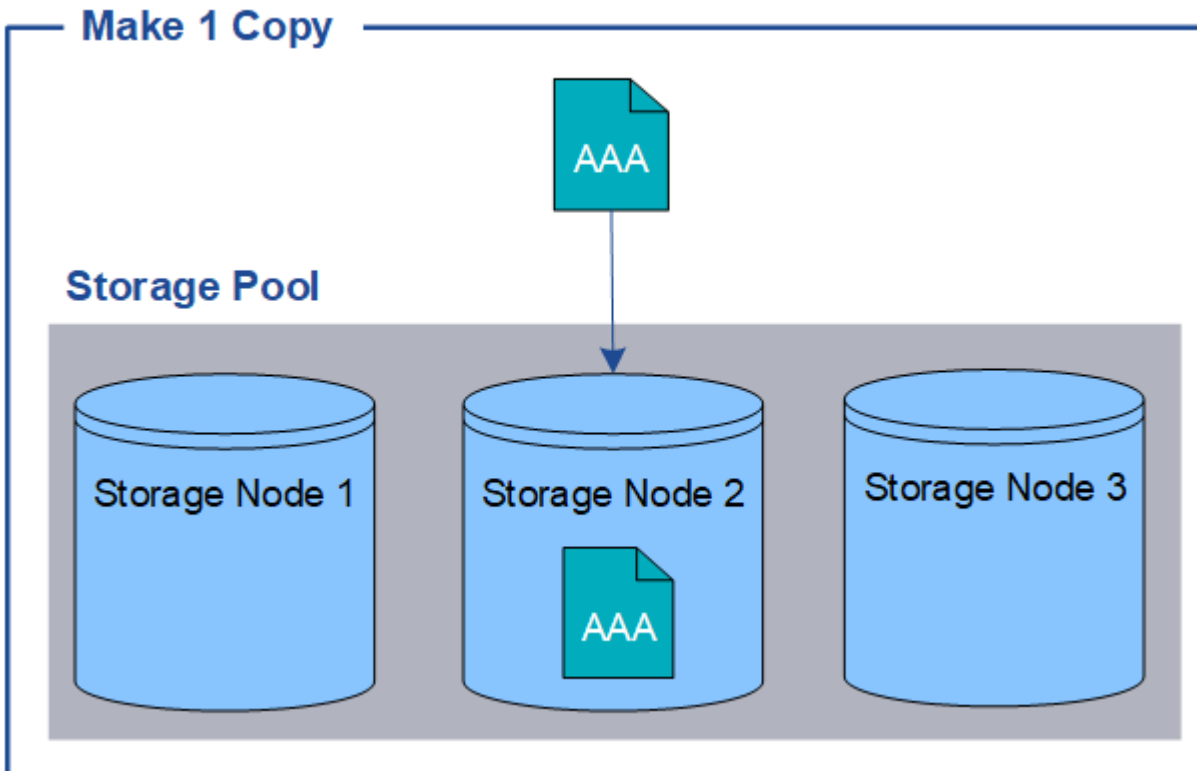
Perché non utilizzare la replica a copia singola

Quando si crea una regola ILM per creare copie replicate, è necessario specificare almeno due copie per un periodo di tempo qualsiasi nelle istruzioni di posizionamento.

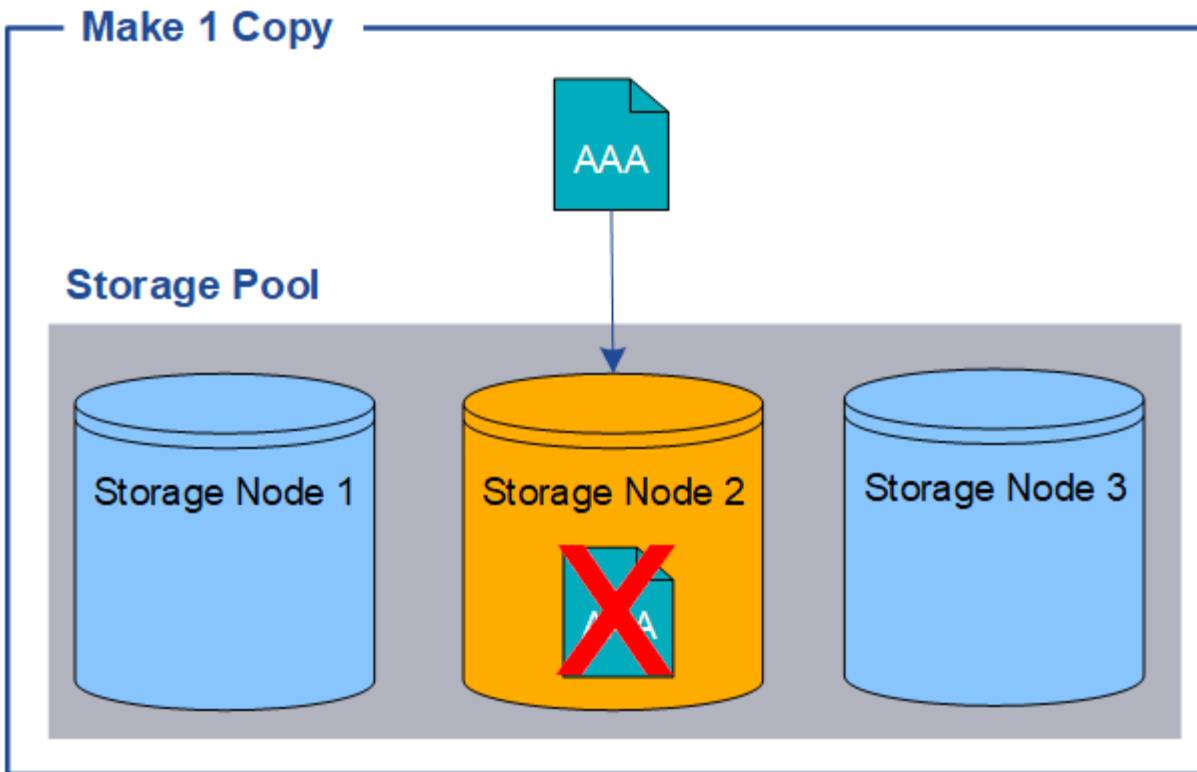


Non utilizzare una regola ILM che crea una sola copia replicata per qualsiasi periodo di tempo. Se esiste una sola copia replicata di un oggetto, quest'ultimo viene perso in caso di errore o errore significativo di un nodo di storage. Inoltre, durante le procedure di manutenzione, ad esempio gli aggiornamenti, si perde temporaneamente l'accesso all'oggetto.

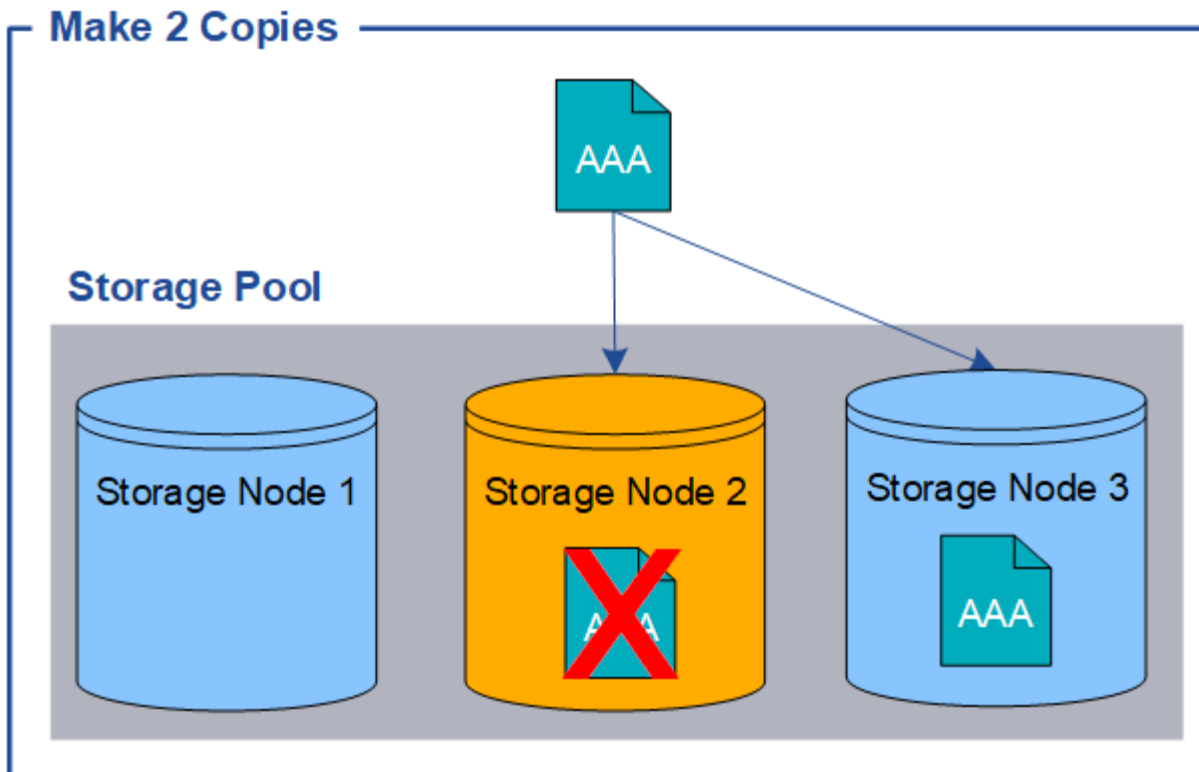
Nell'esempio seguente, la regola Make 1 Copy ILM specifica che una copia replicata di un oggetto deve essere inserita in un pool di storage che contiene tre nodi di storage. Quando viene acquisito un oggetto che corrisponde a questa regola, StorageGRID inserisce una singola copia su un solo nodo di storage.



Quando una regola ILM crea una sola copia replicata di un oggetto, l'oggetto diventa inaccessibile quando il nodo di storage non è disponibile. In questo esempio, l'accesso all'oggetto AAA viene temporaneamente perso ogni volta che il nodo di storage 2 non è in linea, ad esempio durante un aggiornamento o un'altra procedura di manutenzione. In caso di guasto del nodo di storage 2, l'oggetto AAA andrà perso completamente.



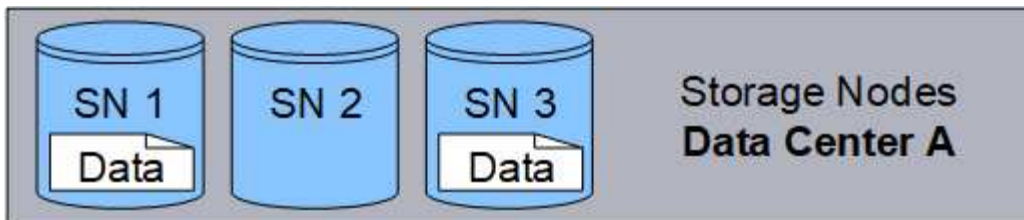
Per evitare di perdere i dati degli oggetti, è necessario eseguire almeno due copie di tutti gli oggetti che si desidera proteggere con la replica. Se esistono due o più copie, è comunque possibile accedere all'oggetto se un nodo di storage si guasta o non è in linea.



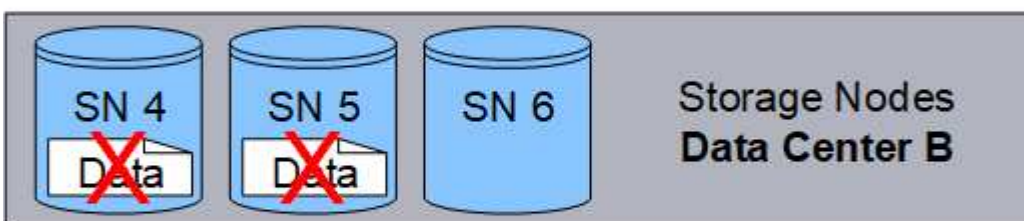
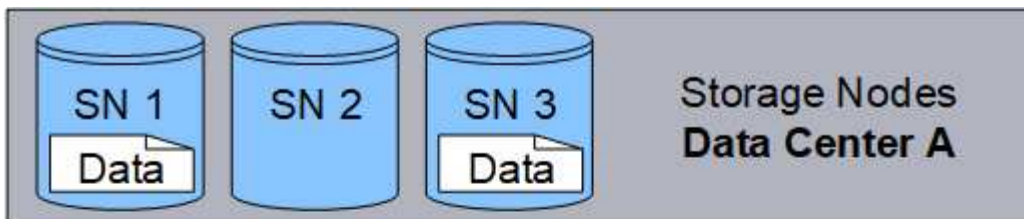
Che cos'è la cancellazione dei codici

Erasure coding è il secondo metodo utilizzato da StorageGRID per memorizzare i dati degli oggetti. Quando StorageGRID associa oggetti a una regola ILM configurata per creare copie con codifica di cancellazione, slice i dati degli oggetti in frammenti di dati, calcola ulteriori frammenti di parità e memorizza ogni frammento su un nodo di storage diverso. Quando si accede a un oggetto, questo viene riassembleato utilizzando i frammenti memorizzati. Se un dato o un frammento di parità viene corrotto o perso, l'algoritmo di erasure coding può ricreare quel frammento utilizzando un sottoinsieme dei dati rimanenti e dei frammenti di parità.

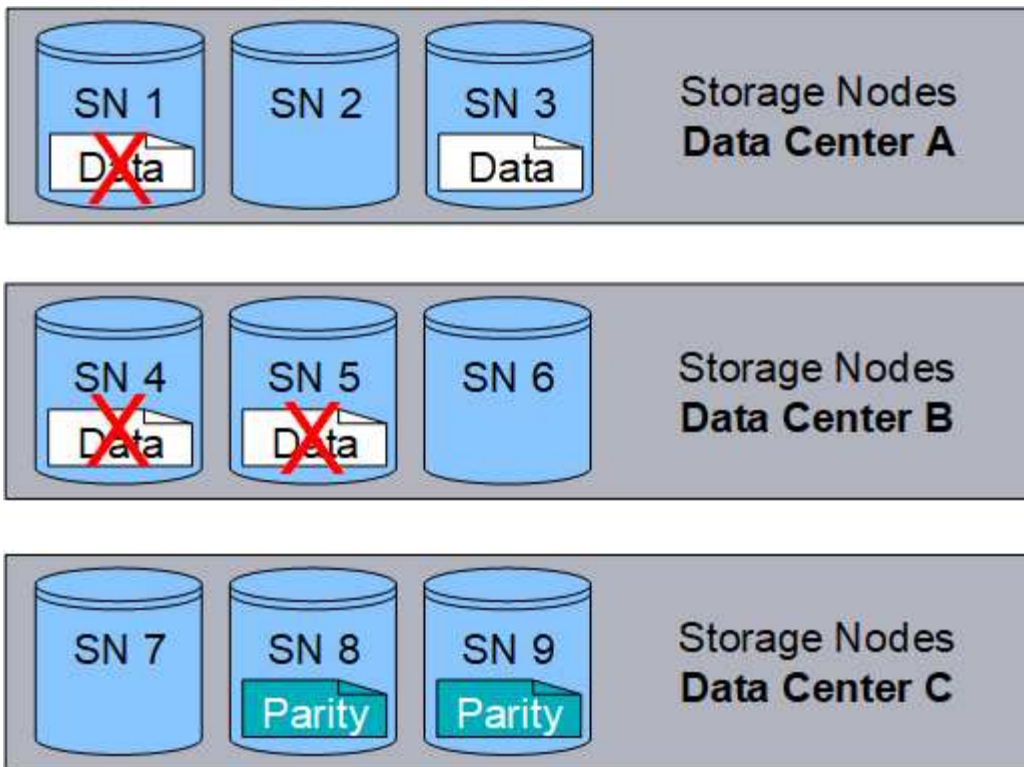
Nell'esempio seguente viene illustrato l'utilizzo di un algoritmo di erasure coding sui dati di un oggetto. In questo esempio, la regola ILM utilizza uno schema di erasure coding 4+2. Ciascun oggetto viene suddiviso in quattro frammenti di dati uguali e due frammenti di parità vengono calcolati dai dati dell'oggetto. Ciascuno dei sei frammenti viene memorizzato su un nodo diverso in tre siti del data center per fornire protezione dei dati in caso di guasti al nodo o perdita del sito.



Lo schema di erasure coding 4+2 richiede un minimo di nove nodi di storage, con tre nodi di storage in ciascuno dei tre siti diversi. Un oggetto può essere recuperato finché quattro dei sei frammenti (dati o parità) rimangono disponibili. È possibile perdere fino a due frammenti senza perdita dei dati dell'oggetto. In caso di perdita di un intero sito del data center, l'oggetto può comunque essere recuperato o riparato, purché tutti gli altri frammenti rimangano accessibili.



In caso di perdita di più di due nodi di storage, l'oggetto non può essere recuperato.



Informazioni correlate

["Che cos'è un pool di storage"](#)

["Quali sono gli schemi di erasure coding"](#)

["Configurazione dei profili di codifica Erasure"](#)

Quali sono gli schemi di erasure coding

Quando si configura il profilo Erasure coding per una regola ILM, si seleziona uno schema di erasure coding disponibile in base al numero di nodi e siti di storage che si intende utilizzare nel pool di storage. Gli schemi di erasure coding controllano il numero di frammenti di dati e il numero di frammenti di parità creati per ciascun oggetto.

Il sistema StorageGRID utilizza l'algoritmo di erasure coding Reed-Solomon. L'algoritmo suddivide un oggetto in k frammenti di dati e calcola m frammenti di parità. I frammenti $k + m = n$ sono distribuiti su n nodi di storage per fornire protezione dei dati. Un oggetto può sostenere fino a m frammenti persi o corrotti. k frammenti sono necessari per recuperare o riparare un oggetto.

Quando si configura un profilo di codifica Erasure, attenersi alle seguenti linee guida per i pool di storage:

- Il pool di storage deve includere tre o più siti, o esattamente un sito.



Non è possibile configurare un profilo di codifica Erasure se il pool di storage include due siti.

- [Schemi di erasure coding per pool di storage contenenti tre o più siti](#)
- [Schemi di erasure coding per pool di storage a sito singolo](#)

- Non utilizzare il pool di storage predefinito, tutti i nodi di storage o un pool di storage che include il sito

predefinito, tutti i siti.

- Il pool di storage deve includere almeno $k+m+1$ nodi di storage.

Il numero minimo di nodi di storage richiesto è $k+m$. Tuttavia, disporre di almeno un nodo di storage aggiuntivo può contribuire a prevenire gli errori di acquisizione o i backlog ILM se un nodo di storage richiesto non è temporaneamente disponibile.

L'overhead dello storage di uno schema di erasure coding viene calcolato dividendo il numero di frammenti di parità (m) per il numero di frammenti di dati (k). È possibile utilizzare l'overhead dello storage per calcolare la quantità di spazio su disco richiesta da ciascun oggetto con codifica di cancellazione:

$$\text{disk space} = \text{object size} + (\text{object size} * \text{storage overhead})$$

Ad esempio, se si memorizza un oggetto da 10 MB utilizzando lo schema 4+2 (con un overhead dello storage del 50%), l'oggetto consuma 15 MB di storage grid. Se si memorizza lo stesso oggetto da 10 MB utilizzando lo schema 6+2 (con un overhead dello storage del 33%), l'oggetto consuma circa 13.3 MB.

Seleziona lo schema di erasure coding con il valore totale più basso di $k+m$ che soddisfi le tue esigenze. gli schemi di erasure coding con un numero inferiore di frammenti sono in generale più efficienti dal punto di vista computazionale, in quanto vengono creati e distribuiti (o recuperati) meno frammenti per oggetto, possono mostrare performance migliori grazie alle maggiori dimensioni dei frammenti e possono richiedere l'aggiunta di un numero inferiore di nodi in un'espansione quando è necessario più storage. (Per informazioni sulla pianificazione di un'espansione dello storage, consultare le istruzioni relative all'espansione di StorageGRID).

Schemi di erasure coding per pool di storage contenenti tre o più siti

La seguente tabella descrive gli schemi di erasure coding attualmente supportati da StorageGRID per i pool di storage che includono tre o più siti. Tutti questi schemi offrono la protezione contro le perdite di sito. È possibile perdere un sito e l'oggetto sarà ancora accessibile.

Per gli schemi di erasure coding che forniscono la protezione contro la perdita di sito, il numero consigliato di nodi di storage nel pool di storage supera $k+m+1$ perché ogni sito richiede un minimo di tre nodi di storage.

Schema di erasure coding ($k+m$)	Numero minimo di siti implementati	Numero consigliato di nodi di storage in ogni sito	Numero totale consigliato di nodi di storage	Protezione contro le perdite di sito?	Overhead dello storage
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%

Schema di erasure coding ($k+m$)	Numero minimo di siti implementati	Numero consigliato di nodi di storage in ogni sito	Numero totale consigliato di nodi di storage	Protezione contro le perdite di sito?	Overhead dello storage
6+1	7	3	21	Sì	17%
7+5	3	5	15	Sì	71%



StorageGRID richiede un minimo di tre nodi di storage per sito. Per utilizzare lo schema 7+5, ogni sito richiede almeno quattro nodi di storage. Si consiglia di utilizzare cinque nodi di storage per sito.

Quando si seleziona uno schema di erasure coding che fornisce la protezione del sito, bilanciare 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.
- **Fault tolerance:** La tolleranza di errore viene aumentata con più segmenti di parità (ovvero, quando m ha un valore più elevato).
- **Traffico di rete:** Durante il ripristino da errori, l'utilizzo di uno schema con più frammenti (ovvero, un totale maggiore per $k+m$) crea più traffico di rete.
- **Overhead dello storage:** Gli schemi con overhead più elevato richiedono più spazio di storage per oggetto.

Ad esempio, quando si decide tra uno schema 4+2 e uno schema 6+3 (entrambi con un overhead dello storage del 50%), selezionare lo schema 6+3 se è richiesta una fault tolerance aggiuntiva. Selezionare lo schema 4+2 se le risorse di rete sono limitate. Se tutti gli altri fattori sono uguali, selezionare 4+2 perché il numero totale di frammenti è inferiore.



In caso di dubbi sul programma da utilizzare, selezionare 4+2 o 6+3 oppure contattare il supporto tecnico.

Schemi di erasure coding per pool di storage a sito singolo

Un pool di storage a sito singolo supporta tutti gli schemi di erasure coding definiti per tre o più siti, a condizione che il sito disponga di un numero sufficiente di nodi di storage.

Il numero minimo di nodi di storage richiesto è $k+m$, ma si consiglia un pool di storage con $k+m+1$ nodi di storage. Ad esempio, lo schema di erasure coding 2+1 richiede un pool di storage con almeno tre nodi di storage, ma si consiglia di utilizzare quattro nodi di storage.

Schema di erasure coding ($k+m$)	Numero minimo di nodi di storage	Numero consigliato di nodi di storage	Overhead dello storage
4+2	6	7	50%
6+2	8	9	33%

Schema di erasure coding ($k+m$)	Numero minimo di nodi di storage	Numero consigliato di nodi di storage	Overhead dello storage
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%

Informazioni correlate

["Espandi il tuo grid"](#)

Vantaggi, svantaggi e requisiti per l'erasure coding

Prima di decidere se utilizzare la replica o la cancellazione del codice per proteggere i dati degli oggetti dalla perdita, è necessario comprendere i vantaggi, gli svantaggi e i requisiti per la cancellazione del codice.

Vantaggi dell'erasure coding

Rispetto alla replica, l'erasure coding offre maggiore affidabilità, disponibilità ed efficienza dello storage.

- **Affidabilità:** L'affidabilità viene misurata in termini di tolleranza agli errori, ovvero il numero di guasti simultanei che possono essere sostenuti senza perdita di dati. Con la replica, più copie identiche vengono memorizzate su nodi diversi e tra siti diversi. Con la codifica erasure, un oggetto viene codificato in dati e frammenti di parità e distribuito su molti nodi e siti. Questa dispersione fornisce protezione da guasti sia a livello di sito che di nodo. Rispetto alla replica, l'erasure coding offre una maggiore affidabilità a costi di storage comparabili.
- **Disponibilità:** La disponibilità può essere definita come la capacità di recuperare oggetti se i nodi di storage si guastano o diventano inaccessibili. Rispetto alla replica, l'erasure coding offre una maggiore disponibilità a costi di storage comparabili.
- **Efficienza dello storage:** Per livelli simili di disponibilità e affidabilità, gli oggetti protetti tramite erasure coding consumano meno spazio su disco rispetto agli stessi oggetti se protetti tramite replica. Ad esempio, un oggetto da 10 MB replicato in due siti consuma 20 MB di spazio su disco (due copie), mentre un oggetto con codifica di cancellazione su tre siti con uno schema di codifica di cancellazione 6+3 consuma solo 15 MB di spazio su disco.



Lo spazio su disco per gli oggetti con codifica in cancellazione viene calcolato come dimensione dell'oggetto più l'overhead dello storage. La percentuale di overhead dello storage è il numero di frammenti di parità diviso per il numero di frammenti di dati.

Svantaggi della codifica erasure

Rispetto alla replica, l'erasure coding presenta i seguenti svantaggi:

- È necessario un maggior numero di nodi e siti di storage. Ad esempio, se si utilizza uno schema di erasure coding di 6+3, è necessario disporre di almeno tre nodi di storage in tre siti diversi. Al contrario, se si replicano semplicemente i dati degli oggetti, è necessario un solo nodo di storage per ogni copia.
- Aumento dei costi e della complessità delle espansioni dello storage. Per espandere un'implementazione che utilizza la replica, è sufficiente aggiungere capacità di storage in ogni posizione in cui vengono eseguite le copie a oggetti. Per espandere un'implementazione che utilizza il erasure coding, è necessario prendere in considerazione sia lo schema di erasure coding in uso sia la capacità dei nodi di storage esistenti. Ad esempio, se si attende che i nodi esistenti siano pieni al 100%, è necessario aggiungere almeno $k+m$ nodi di storage, ma se si espandono quando i nodi esistenti sono pieni al 70%, è possibile aggiungere due nodi per sito e massimizzare la capacità di storage utilizzabile. Per ulteriori informazioni, consulta le istruzioni per espandere StorageGRID.
- L'utilizzo di erasure coding in siti distribuiti geograficamente aumenta le latenze di recupero. I frammenti di oggetti per un oggetto che viene erasure coded e distribuito tra siti remoti richiedono più tempo per il recupero su connessioni WAN rispetto a un oggetto che viene replicato e disponibile localmente (lo stesso sito a cui si connette il client).
- Quando si utilizza il erasure coding in siti distribuiti geograficamente, il traffico di rete WAN è più elevato per recuperi e riparazioni, in particolare per oggetti recuperati di frequente o per riparazioni di oggetti su connessioni di rete WAN.
- Quando si utilizza l'erasure coding tra siti, il throughput massimo degli oggetti diminuisce drasticamente con l'aumentare della latenza di rete tra siti. Questa diminuzione è dovuta alla corrispondente diminuzione del throughput di rete TCP, che influisce sulla velocità con cui il sistema StorageGRID può memorizzare e recuperare frammenti di oggetti.
- Maggiore utilizzo delle risorse di calcolo.

Quando utilizzare la codifica di cancellazione

L'erasure coding è più adatto ai seguenti requisiti:

- Oggetti di dimensioni superiori a 1 MB.



A causa dell'overhead di gestione del numero di frammenti associati a una copia con codice erasure, non utilizzare la codifica erasure per oggetti di dimensioni pari o inferiori a 200 KB.

- Storage a lungo termine o a freddo per contenuti recuperati raramente.
- Elevata disponibilità e affidabilità dei dati.
- Protezione contro guasti completi del sito e dei nodi.
- Efficienza dello storage.
- Implementazioni a singolo sito che richiedono una protezione dei dati efficiente con una sola copia codificata in cancellazione anziché più copie replicate.
- Implementazioni multi-sito in cui la latenza tra siti è inferiore a 100 ms.

Informazioni correlate

["Espandi il tuo grid"](#)

Come viene determinata la conservazione degli oggetti

StorageGRID offre agli amministratori di grid e ai singoli utenti tenant opzioni per specificare la durata della memorizzazione degli 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 del tenant possono controllare per quanto tempo i propri oggetti vengono memorizzati in StorageGRID in tre modi principali:

- Se l'impostazione globale S3 Object Lock è attivata 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 e conservazione legale per ciascuna versione dell'oggetto aggiunta a quel bucket.
 - Una versione dell'oggetto sottoposta a blocco legale non può essere eliminata con alcun metodo.
 - Prima che venga raggiunta la data di conservazione di una versione a oggetti, tale versione non può essere eliminata da alcun metodo.
 - Gli oggetti nei bucket con S3 Object Lock abilitato vengono conservati da ILM "forever". 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.

"Gestione degli oggetti con S3 Object Lock"

- Gli utenti del tenant S3 possono aggiungere una configurazione del ciclo di vita ai bucket che specifica un'azione di scadenza. Se esiste un ciclo di vita del bucket, StorageGRID memorizza un oggetto fino a quando non viene soddisfatta la data o il numero di giorni specificati nell'azione di scadenza, a meno che il client non elimini prima l'oggetto.
- Un client S3 o Swift può emettere una richiesta di eliminazione degli oggetti. StorageGRID assegna sempre la priorità alle richieste di eliminazione dei client sul ciclo di vita del bucket S3 o ILM quando si determina se eliminare o conservare un oggetto.

Come gli amministratori della griglia controllano la conservazione degli oggetti

Gli amministratori della griglia utilizzano le istruzioni di posizionamento ILM per controllare la durata della memorizzazione degli oggetti. Quando un oggetto viene associato da una regola ILM, StorageGRID memorizza tali oggetti fino allo scadere dell'ultimo periodo di tempo della regola ILM. Gli oggetti vengono conservati a tempo indeterminato se viene specificato "forever" per le istruzioni di posizionamento.

Indipendentemente da chi controlla la durata della conservazione degli oggetti, le impostazioni ILM controllano i tipi di copie degli oggetti (replicate o codificate per la cancellazione) che vengono memorizzate e la posizione delle copie (nodi di storage, pool di storage cloud o nodi di archiviazione).

Come interagiscono il ciclo di vita del bucket S3 e ILM

L'azione Expiration (scadenza) in un ciclo di vita del bucket S3 sovrascrive sempre le impostazioni ILM. Di conseguenza, un oggetto potrebbe essere conservato sulla griglia anche dopo che sono scadute le istruzioni ILM per il posizionamento dell'oggetto.

Esempi di conservazione degli oggetti

Per comprendere meglio le interazioni tra blocco oggetti S3, impostazioni del ciclo di vita del bucket, richieste di eliminazione client e ILM, considerare gli esempi seguenti.

Esempio 1: Il ciclo di vita del bucket S3 mantiene gli oggetti più a lungo di ILM

ILM

Memorizzazione di 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 mantenuti più a lungo di quanto specificato da ILM, StorageGRID continua a utilizzare le istruzioni di posizionamento ILM per determinare il numero e il tipo di copie da memorizzare. In questo esempio, due copie dell'oggetto continueranno ad essere memorizzate in StorageGRID dai giorni 366 al 730.

Esempio 2: Il ciclo di vita del bucket S3 scade gli oggetti prima di ILM

ILM

Memorizzazione di due copie per 2 anni (730 giorni)

Ciclo di vita del bucket

Scadenza 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

Memorizzazione di due copie sui nodi di storage "forever"

Ciclo di vita del bucket

Scadenza degli oggetti in 2 anni (730 giorni)

Richiesta di eliminazione del client

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 oggetti S3

Retain-until-date per una versione a oggetti è 2026-03-31. Non è in vigore una conservazione a fini giudiziari.

Regola ILM conforme

Memorizzazione di due copie sui nodi di storage “forever”.

Richiesta di eliminazione del client

Pubblicato il 2024-03-31.

Risultato

StorageGRID non eliminerà la versione dell’oggetto perché la data di conservazione è ancora a 2 anni di distanza.

Informazioni correlate

["Gestione degli oggetti con S3 Object Lock"](#)

["Utilizzare S3"](#)

["Quali sono le istruzioni per il posizionamento delle regole ILM"](#)

Modalità di eliminazione degli oggetti

StorageGRID può eliminare gli oggetti in risposta diretta a una richiesta del client o automaticamente in conseguenza della scadenza di un ciclo di vita del bucket S3 o dei requisiti della policy ILM. La comprensione dei diversi modi in cui è possibile eliminare gli oggetti e del modo in cui StorageGRID gestisce le richieste di eliminazione può aiutare 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 del client, tutte le copie degli oggetti vengono rimosse immediatamente. Il client viene informato che l’eliminazione è stata eseguita correttamente dopo la rimozione delle copie.
- **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 dell’avvenuta eliminazione. Le copie degli oggetti vengono rimosse in seguito dall’elaborazione ILM in background.

Quando si eliminano gli oggetti, StorageGRID utilizza il metodo che ottimizza le performance di eliminazione, riduce al minimo i potenziali backlog di eliminazione e libera lo spazio più rapidamente.

La tabella riassume quando StorageGRID utilizza ciascun metodo.

Metodo di eliminazione	Se utilizzato
<p>Gli oggetti vengono messi in coda per l'eliminazione</p>	<p>Quando una delle seguenti condizioni è vera:</p> <ul style="list-style-type: none"> • L'eliminazione automatica degli oggetti è stata attivata da uno dei seguenti eventi: <ul style="list-style-type: none"> ◦ Viene raggiunta la data di scadenza o il numero di giorni nella configurazione del ciclo di vita di un bucket S3. ◦ È trascorso l'ultimo periodo di tempo specificato in una regola ILM. <p>Nota: gli oggetti in un bucket che ha attivato il blocco oggetti S3 non possono essere cancellati se sono in stato di conservazione legale o se è stato specificato un periodo di conservazione fino alla data, ma non ancora soddisfatto.</p> <ul style="list-style-type: none"> • Un client S3 o Swift richiede l'eliminazione e una o più di queste condizioni sono vere: <ul style="list-style-type: none"> ◦ Impossibile eliminare le copie entro 30 secondi, ad esempio perché una posizione dell'oggetto non è temporaneamente disponibile. ◦ Le code di eliminazione in background sono inattive.
<p>Gli oggetti vengono rimossi immediatamente (eliminazione sincrona)</p>	<p>Quando un client S3 o Swift effettua una richiesta di eliminazione e tutte le seguenti condizioni sono soddisfatte:</p> <ul style="list-style-type: none"> • Tutte le copie possono essere rimosse entro 30 secondi. • Le code di eliminazione in background contengono oggetti da elaborare.

Quando i client S3 o Swift effettuano richieste di eliminazione, StorageGRID inizia aggiungendo una serie di oggetti alla coda di eliminazione. Passa quindi all'eliminazione sincrona. Assicurarsi che la coda di eliminazione in background disponga di oggetti da elaborare consente a StorageGRID di elaborare le eliminazioni in modo più efficiente, in particolare per i client con bassa concorrenza, evitando al contempo i backlog di eliminazione dei client.

Comprendere l'impatto del modo in cui StorageGRID elimina gli oggetti

Il modo in cui StorageGRID elimina gli oggetti può influire sulle prestazioni del sistema:

- Quando StorageGRID esegue l'eliminazione sincrona, StorageGRID può impiegare fino a 30 secondi per restituire un risultato al client. Ciò significa che l'eliminazione può sembrare più lenta, anche se le copie vengono effettivamente rimosse più rapidamente di quanto non lo siano quando StorageGRID mette in coda gli oggetti per l'eliminazione.
- Se si stanno monitorando attentamente le prestazioni di eliminazione durante un'eliminazione in blocco, si potrebbe notare che la velocità di eliminazione sembra rallentare dopo l'eliminazione di un certo numero di oggetti. Questa modifica si verifica quando StorageGRID passa dall'accodamento di oggetti per l'eliminazione all'eliminazione sincrona. La riduzione apparente del tasso di eliminazione non significa che le copie degli oggetti vengano rimosse più lentamente. Al contrario, indica che, in media, lo spazio viene liberato più rapidamente.

Se si eliminano grandi quantità di oggetti e la priorità è liberare spazio rapidamente, considerare l'utilizzo di una richiesta client per eliminare gli oggetti piuttosto che eliminarli utilizzando 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.

Tenere presente che 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 la rimozione 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 dei client che per altri metodi).

Modalità di eliminazione degli oggetti con versione S3

Quando il controllo delle versioni è attivato per un bucket S3, StorageGRID segue il comportamento di Amazon S3 quando risponde alle richieste di eliminazione, sia che provengano da un client S3, dalla scadenza di un ciclo di vita del bucket S3 o dai requisiti della policy ILM.

Quando gli oggetti sono sottoposti a versione, le richieste di eliminazione degli oggetti non eliminano la versione corrente dell'oggetto e non liberano spazio. Invece, una richiesta di eliminazione di un oggetto crea semplicemente un indicatore di eliminazione come versione corrente dell'oggetto, rendendo la versione precedente dell'oggetto "non aggiornata".

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 quell'oggetto restituiscono 404 non trovato. Tuttavia, poiché i dati dell'oggetto non correnti non sono stati rimossi, le richieste che specificano una versione non corrente dell'oggetto possono avere successo.

Per liberare spazio durante l'eliminazione degli oggetti con versione, è necessario effettuare una delle seguenti operazioni:

- **S3 client request:** Specificare il numero di versione dell'oggetto nella richiesta S3 DELETE Object (DELETE /object?versionId=ID). Tenere presente che questa richiesta rimuove solo le copie degli oggetti per la versione specificata (le altre versioni occupano ancora spazio).
- **Ciclo di vita del bucket:** Utilizzare `NoncurrentVersionExpiration` azione nella configurazione del ciclo di vita del bucket. Quando viene raggiunto il numero di giorni non correnti specificato, StorageGRID rimuove in modo permanente tutte le copie delle versioni degli oggetti non correnti. Queste versioni degli oggetti non possono essere ripristinate.
- **ILM:** Aggiungi due regole ILM al tuo criterio ILM. Utilizzare **tempo non corrente** come tempo di riferimento nella prima regola per far corrispondere le versioni non correnti dell'oggetto. Utilizzare **Ingest Time** nella seconda regola per corrispondere alla versione corrente. La regola **ora non corrente** deve essere visualizzata nel criterio sopra la regola **ora di acquisizione**.

Informazioni correlate

["Utilizzare S3"](#)

["Esempio 4: Regole ILM e policy per gli oggetti con versione S3"](#)

Che cos'è una policy ILM

Un criterio ILM (Information Lifecycle Management) è un insieme ordinato di regole ILM che determina il modo in cui il sistema StorageGRID gestisce i dati degli oggetti nel tempo.

Come un criterio ILM valuta gli oggetti

Il criterio ILM attivo per il sistema StorageGRID controlla il posizionamento, la durata e la protezione dei dati di tutti gli oggetti.

Quando i client salvano gli oggetti in StorageGRID, gli oggetti vengono valutati in base all'insieme ordinato di regole ILM nel criterio attivo, come segue:

1. Se i filtri per la prima regola del criterio corrispondono a un oggetto, l'oggetto viene acquisito in base al comportamento di acquisizione di tale regola e memorizzato in base alle istruzioni di posizionamento di tale regola.
2. Se i filtri per la prima regola non corrispondono all'oggetto, l'oggetto viene valutato in base a ogni regola successiva nel criterio fino a quando non viene effettuata una corrispondenza.
3. Se nessuna regola corrisponde a un oggetto, vengono applicate le istruzioni di inserimento e posizionamento della regola predefinita nel criterio. La regola predefinita è l'ultima regola di un criterio e non può utilizzare alcun filtro.

Esempio di policy ILM

Questo esempio di policy ILM utilizza tre regole ILM.

Configure ILM Policy

Create a proposed policy by selecting and arranging rules. Then, save the policy and edit it later as required. Click Simulate to verify a saved policy using test objects. When you are ready, click Activate to make this policy the active ILM policy for the grid.

Name

Reason for change

Rules

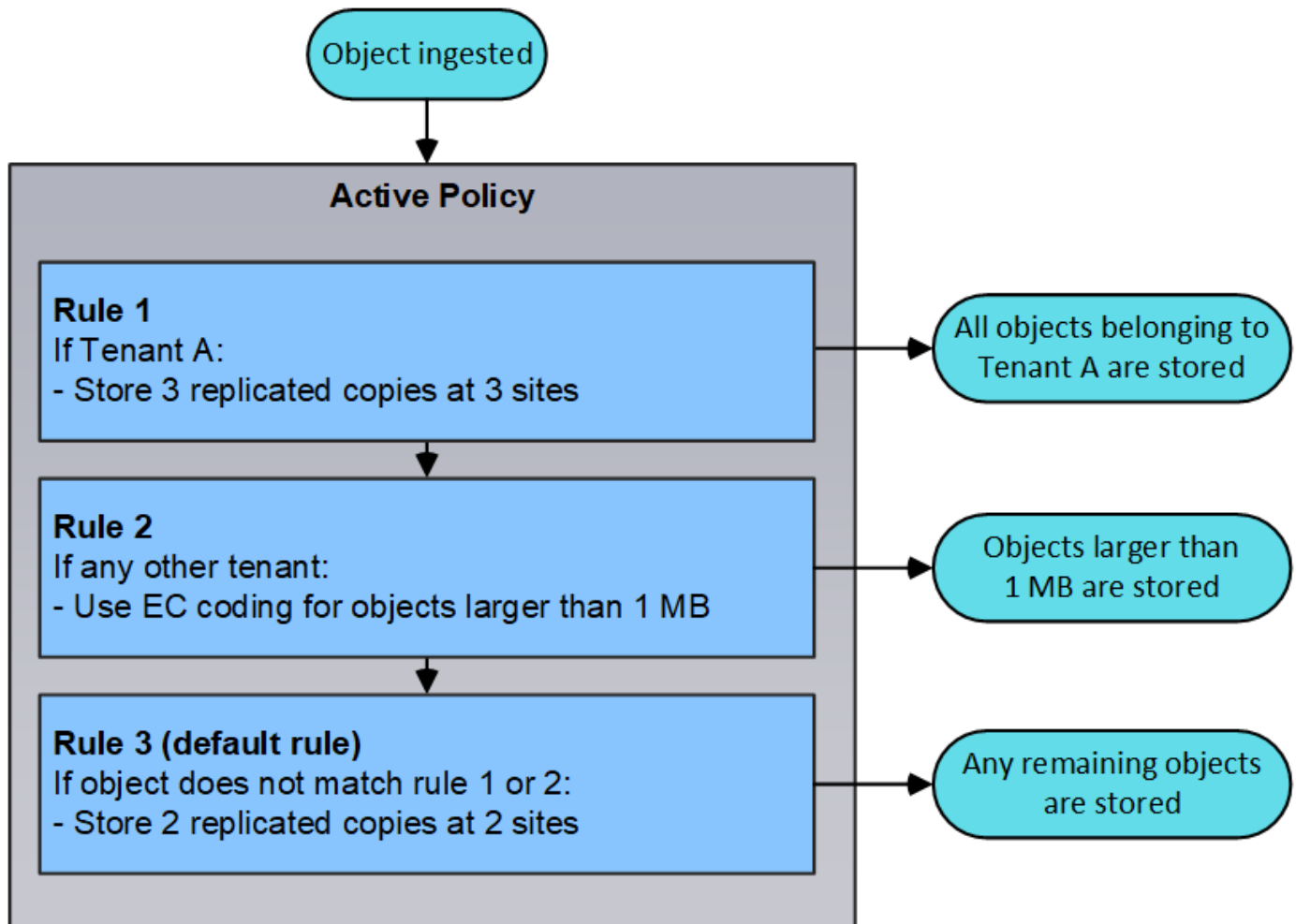
1. Select the rules you want to add to the policy.
2. Determine the order in which the rules will be evaluated by dragging and dropping the rows. The default rule will be automatically placed at the end of the policy and cannot be moved.

	Default	Rule Name	Tenant Account	Actions
		Rule 1: 3 replicated copies for Tenant A	Tenant A (58889986524346589742)	
		Rule 2: Erasure coding for objects greater than 1 MB	—	
	<input checked="" type="checkbox"/>	Rule 3: 2 copies 2 data centers (default)	—	

In questo esempio, la regola 1 corrisponde a tutti gli oggetti appartenenti al tenant A. Questi oggetti vengono memorizzati come tre copie replicate in tre siti. Gli oggetti appartenenti ad altri tenant non corrispondono alla regola 1, quindi vengono valutati in base alla regola 2.

La regola 2 corrisponde a tutti gli oggetti degli altri tenant, ma solo se sono più grandi di 1 MB. Questi oggetti più grandi vengono memorizzati utilizzando la codifica di cancellazione 6+3 in tre siti. La regola 2 non corrisponde a oggetti di dimensioni pari o inferiori a 1 MB, pertanto questi oggetti vengono valutati in base alla regola 3.

La regola 3 è l'ultima regola predefinita del criterio e non utilizza filtri. La regola 3 crea 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).



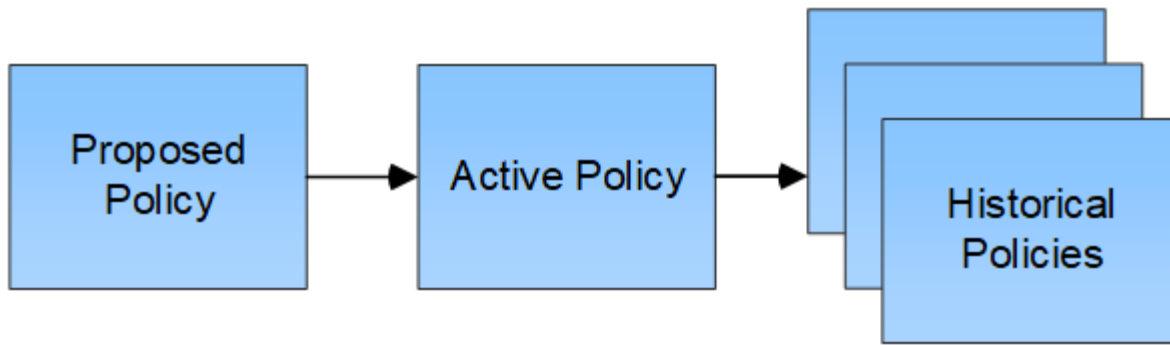
Quali sono le politiche proposte, attive e storiche

Ogni sistema StorageGRID deve disporre di un criterio ILM attivo. Un sistema StorageGRID potrebbe anche disporre di una policy ILM proposta e di un numero qualsiasi di policy storiche.

Quando si crea per la prima volta un criterio ILM, si crea un criterio proposto selezionando una o più regole ILM e ordinandole in un ordine specifico. Una volta simulata la policy proposta per confermarne il comportamento, attivarla per creare la policy attiva.

Quando si attiva un nuovo criterio ILM, StorageGRID utilizza tale criterio per gestire tutti gli oggetti, inclusi quelli esistenti e quelli appena acquisiti. Gli oggetti esistenti potrebbero essere spostati in nuove posizioni quando vengono implementate le regole ILM nel nuovo criterio.

L'attivazione della policy proposta fa sì che la policy precedentemente attiva diventi una policy storica. Impossibile eliminare i criteri ILM storici.



Informazioni correlate

["Creazione di un criterio ILM"](#)

Che cos'è una regola ILM

Per gestire gli oggetti, creare un set di regole ILM (Information Lifecycle Management) e organizzarle in un criterio ILM. Ogni oggetto acquisito nel sistema viene valutato in base al criterio attivo. Quando una regola del criterio corrisponde ai metadati di un oggetto, le istruzioni della regola determinano le azioni eseguite da StorageGRID per copiare e memorizzare tale oggetto.

Le regole ILM definiscono:

- Quali oggetti devono essere memorizzati. Una regola può essere applicata a tutti gli oggetti oppure è possibile specificare filtri per identificare gli oggetti a cui si applica una regola. Ad esempio, una regola può essere applicata solo agli oggetti associati a determinati account tenant, a specifici bucket S3 o a contenitori Swift o a specifici valori di metadati.
- Il tipo e la posizione di storage. Gli oggetti possono essere memorizzati nei nodi di storage, nei pool di storage cloud o nei nodi di archiviazione.
- Il tipo di copie a oggetti eseguite. Le copie possono essere replicate o codificate per la cancellazione.
- Per le copie replicate, il numero di copie eseguite.
- Per le copie codificate erasure, viene utilizzato lo schema di erasure coding.
- Il cambia nel tempo nella posizione di storage di un oggetto e nel tipo di copie.
- Modalità di protezione dei dati degli oggetti durante l'acquisizione degli oggetti nella griglia (posizionamento sincrono o doppio commit).

Si noti che i metadati degli oggetti non sono gestiti dalle regole ILM. I metadati degli oggetti vengono invece memorizzati in un database Cassandra in un archivio di metadati. Tre copie dei metadati degli oggetti vengono gestite automaticamente in ogni sito per proteggere i dati dalla perdita. Le copie sono distribuite uniformemente in tutti i nodi di storage.

Elementi di una regola ILM

Una regola ILM ha tre elementi:

- **Filtering Criteria:** 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 degli oggetti. Ciascuna regola può includere una sequenza di istruzioni di posizionamento per modificare il numero, il tipo e la posizione delle copie degli oggetti nel tempo. Quando scade il periodo di tempo per un posizionamento, le istruzioni nel posizionamento successivo vengono applicate automaticamente dalla valutazione ILM successiva.

- **Ingest Behavior:** Il comportamento di acquisizione di una regola definisce ciò che accade quando un client S3 o Swift salva un oggetto nella griglia. Il comportamento di acquisizione controlla se le copie degli oggetti vengono posizionate immediatamente in base alle istruzioni della regola o se vengono eseguite copie temporanee e le istruzioni di posizionamento vengono applicate in un secondo momento.

Esempio di regola ILM

Questo esempio di regola ILM si applica agli oggetti appartenenti al tenant A. Esegue due copie replicate di tali oggetti e memorizza ciascuna copia in un sito diverso. Le due copie vengono conservate “forever,” il che significa che StorageGRID non le eliminerà automaticamente. Al contrario, StorageGRID conserverà questi oggetti fino a quando non saranno cancellati da una richiesta di eliminazione del client o dalla scadenza di un ciclo di vita del bucket.

Questa regola utilizza l'opzione bilanciata per il comportamento di acquisizione: L'istruzione di posizionamento a due siti viene applicata non appena il tenant A salva un oggetto in StorageGRID, a meno che non sia possibile eseguire 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 intermedie sui nodi di storage nel sito 1. Non appena il sito 2 sarà disponibile, StorageGRID effettuerà la copia richiesta presso il sito.

Two copies at two sites for Tenant A

Description: Applies only to Tenant A

Ingest Behavior: Balanced

Tenant Accounts: Tenant A (34176783492629515782)

Reference Time: Ingest Time

Filtering Criteria:

Matches all objects.

Retention Diagram:

The diagram illustrates the retention policy for two sites, Site 1 and Site 2, starting from Day 0. A vertical line labeled 'Trigger' marks Day 0. Site 1 is represented by a horizontal bar with a blue segment extending to the right, labeled 'Forever'. Site 2 is represented by a horizontal bar with an orange segment extending to the right, also labeled 'Forever'. Both sites have a small cylinder icon representing a storage unit at the start of their respective bars.

Informazioni correlate

["Opzioni di protezione dei dati per l'acquisizione"](#)

"Che cos'è un pool di storage"

"Cos'è un pool di storage cloud"

"Modalità di archiviazione degli oggetti (replica o erasure coding)"

"Che cos'è il filtraggio delle regole ILM"

"Quali sono le istruzioni per il posizionamento delle regole ILM"

Che cos'è il 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 distinti e di grandi dimensioni. I filtri di base nella pagina Define Basics della procedura guidata Create ILM Rule consentono di applicare una regola a specifici account tenant, bucket S3 specifici o container Swift o entrambi.

Create ILM Rule Step 1 of 3: Define Basics

Name	<input type="text"/>
Description	<input type="text"/>
Tenant Accounts (optional)	<input type="text" value="Select tenant accounts or enter tenant IDs"/>
Bucket Name	<input type="text" value="matches all"/> <input type="button" value="Value"/>

[Advanced filtering...](#) (0 defined)

Questi filtri di base offrono un modo semplice per applicare regole diverse a un numero elevato di oggetti. Ad esempio, potrebbe essere necessario memorizzare i record finanziari della tua azienda per soddisfare i requisiti normativi, mentre potrebbe essere necessario memorizzare i dati del reparto di marketing per facilitare le operazioni quotidiane. Dopo aver creato account tenant separati per ciascun reparto o aver separato i dati dai 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.

La pagina **Advanced Filtering** della procedura guidata Create ILM Rule offre un controllo granulare. È possibile creare filtri per selezionare gli oggetti in base alle seguenti proprietà dell'oggetto:

- Tempo di acquisizione
- Ora dell'ultimo accesso
- Nome completo o parziale dell'oggetto (Key)
- Regione bucket S3 (vincolo di posizione)
- Dimensione dell'oggetto

- Metadati dell'utente
- Tag oggetti S3

È possibile filtrare gli oggetti in base a criteri molto specifici. Ad esempio, gli oggetti memorizzati dal reparto di imaging di un ospedale potrebbero essere utilizzati frequentemente quando hanno meno di 30 giorni e poco tempo dopo, mentre gli oggetti che contengono informazioni sulle visite dei pazienti potrebbero dover essere copiati nel reparto di fatturazione della sede centrale della rete sanitaria. È possibile creare filtri che identifichino ciascun tipo di oggetto in base al nome dell'oggetto, alle dimensioni, ai tag di oggetto S3 o a qualsiasi altro criterio pertinente, quindi creare regole separate per memorizzare ciascun set di oggetti in modo appropriato.

È inoltre possibile combinare filtri di base e avanzati in base alle esigenze in una singola regola. Ad esempio, il reparto marketing potrebbe voler memorizzare file di immagini di grandi dimensioni in modo diverso dai record dei vendor, mentre il reparto risorse umane potrebbe dover memorizzare i record del personale in un'area geografica specifica e le informazioni sulle policy a livello centrale. In questo caso, è possibile creare regole che filtrino in base all'account tenant per separare i record da ciascun reparto, utilizzando filtri avanzati in ciascuna regola per identificare il tipo specifico di oggetti a cui si applica la regola.

Quali sono le istruzioni per il posizionamento delle regole ILM

Le istruzioni di posizionamento determinano dove, quando e come vengono memorizzati 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 crea un'istruzione di posizionamento, si specifica quando si applica il posizionamento (il periodo di tempo), quale tipo di copie creare (replicate o codificate per la cancellazione) e dove memorizzare le copie (una o più posizioni di archiviazione). All'interno di una singola regola è possibile specificare più posizioni per un periodo di tempo e le istruzioni di posizionamento per più di un periodo di tempo:

- Per specificare più di un posizionamento degli oggetti durante un singolo periodo di tempo, fare clic sull'icona con il segno più **+** per aggiungere più di una riga per quel periodo di tempo.
- Per specificare il posizionamento degli oggetti per più di un periodo di tempo, fare clic sul pulsante **Add** (Aggiungi) per aggiungere il periodo di tempo successivo. Quindi, specificare una o più righe entro il periodo di tempo.

L'esempio mostra la pagina Definisci posizioni della procedura guidata Crea regola ILM.

Placements ⊕ ↑↓ Sort by start day

From day store days **Add** **Remove**

Type Location Copies **+** **x**

Specifying multiple storage pools might cause data to be stored at the same site if the pools overlap. See [Managing objects with information lifecycle management](#) for more information.

Type Location Copies **1** **+** **x**

From day store **Add** **Remove**

Type Location Copies Temporary location **2** **+** **x**

1	<p>La prima istruzione di posizionamento ha due righe per il primo anno:</p> <ol style="list-style-type: none"> 1. La prima riga crea due copie di oggetti replicate in due siti del data center. 2. La seconda riga crea una copia 6+3 con codifica di cancellazione utilizzando tre siti del data center.
2	<p>La seconda istruzione di posizionamento crea due copie archiviate dopo un anno e le conserva per sempre.</p>

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 finale di posizionamento continui per sempre o fino a quando non si richiede più alcuna copia oggetto.

Alla scadenza di ogni periodo di tempo previsto dalla regola, vengono applicate le istruzioni per il posizionamento dei contenuti per il periodo di tempo successivo. Vengono create nuove copie di oggetti e tutte le copie non necessarie vengono eliminate.

Creazione di livelli di storage, pool di storage, profili EC e regioni

Prima di poter creare le regole ILM per il sistema StorageGRID, è necessario definire le posizioni di archiviazione degli oggetti, determinare i tipi di copie desiderati e, facoltativamente, configurare le aree S3.

- ["Creazione e assegnazione dei gradi di storage"](#)
- ["Configurazione dei pool di storage"](#)
- ["Utilizzo dei Cloud Storage Pools"](#)
- ["Configurazione dei profili di codifica Erasure"](#)
- ["Configurazione delle regioni \(opzionale e solo S3\)"](#)

Creazione e assegnazione dei gradi di storage

I gradi di storage identificano il tipo di storage utilizzato da un nodo di storage. È possibile creare gradi di storage se si desidera che le regole ILM posizionino determinati oggetti su determinati nodi di storage, invece che su tutti i nodi del sito. Ad esempio, è possibile che alcuni oggetti vengano memorizzati nei nodi di storage più veloci, ad esempio le appliance di storage all-flash StorageGRID.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

A proposito di questa attività

Se si utilizzano più tipi di storage, è possibile creare un livello di storage per identificare ciascun tipo. La creazione dei gradi di storage consente di selezionare un tipo specifico di nodo di storage durante la configurazione dei pool di storage.

Se il livello di storage non è un problema (ad esempio, tutti i nodi di storage sono identici), è possibile saltare questa procedura e utilizzare il livello di storage predefinito di tutti i nodi di storage durante la configurazione dei pool di storage.


Quando si aggiunge un nuovo nodo di storage in un'espansione, tale nodo viene aggiunto al livello di storage predefinito di tutti i nodi di storage. Di conseguenza:

- Se una regola ILM utilizza un pool di storage con il grado All Storage Node, il nuovo nodo può essere utilizzato immediatamente dopo il completamento dell'espansione.
- Se una regola ILM utilizza un pool di storage con un livello di storage personalizzato, il nuovo nodo non verrà utilizzato fino a quando non si assegna manualmente il livello di storage personalizzato al nodo, come descritto di seguito.



Durante la creazione dei livelli di storage, non creare più livelli di storage del necessario. Ad esempio, non creare un livello di storage per ciascun nodo di storage. Assegnare invece ogni livello di storage a due o più nodi. I gradi di storage assegnati a un solo nodo possono causare backlog ILM se tale nodo non è più disponibile.

Fasi

1. Selezionare **ILM > Storage Grades**.
2. Creare un livello di storage:
 - a. Per ogni livello di storage da definire, fare clic su **Inserisci**  per aggiungere una riga e inserire un'etichetta per il livello di storage.

Impossibile modificare il livello di storage predefinito. È riservato ai nuovi nodi di storage aggiunti durante l'espansione del sistema StorageGRID.



Storage Grades

Updated: 2017-05-26 11:22:39 MDT

Storage Grade Definitions

Storage Grade	Label	Actions
0	Default	
1	<input type="text" value="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

- a. Per modificare un livello di storage esistente, fare clic su **Edit** (Modifica) e modificare l'etichetta secondo necessità.



Non è possibile eliminare i gradi di storage.

- b. Fare clic su **Applica modifiche**.

Questi livelli di storage sono ora disponibili per l'assegnazione ai nodi di storage.

3. Assegnare un livello di storage a un nodo di storage:

- a. Per il servizio LDR di ciascun nodo di storage, fare clic su **Edit** (Modifica) e selezionare un livello di storage dall'elenco.

Storage Grades



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 storage a un nodo di storage specifico una sola volta. Un nodo di storage recuperato dal guasto mantiene il livello di storage assegnato in precedenza. Non modificare questa assegnazione dopo l'attivazione del criterio ILM. Se l'assegnazione viene modificata, i dati vengono memorizzati in base al nuovo livello di storage.

- Fare clic su **Applica modifiche**.

Configurazione dei pool di storage

Quando si definisce una regola ILM, si utilizzano i pool di storage per specificare dove memorizzare gli oggetti. Prima di creare un pool di storage, è necessario rivedere le linee guida del pool di storage.

- ["Che cos'è un pool di storage"](#)
- ["Linee guida per la creazione di pool di storage"](#)
- ["Utilizzo di più pool di storage per la replica tra siti"](#)
- ["Utilizzo di un pool di storage come posizione temporanea \(obsoleto\)"](#)
- ["Creazione di un pool di storage"](#)
- ["Visualizzazione dei dettagli del pool di storage"](#)
- ["Modifica di un pool di storage"](#)
- ["Rimozione di un pool di storage"](#)

Che cos'è un pool di storage

Un pool di storage è un raggruppamento logico di nodi di storage o nodi di archivio. I pool di storage vengono configurati per determinare dove il sistema StorageGRID memorizza i dati a oggetti e il tipo di storage utilizzato.

I pool di storage hanno due attributi:

- **Storage grade:** Per i nodi di storage, le performance relative dello storage di backup.
- **Sito:** Il data center in cui verranno memorizzati gli oggetti.

I pool di storage vengono utilizzati nelle regole ILM per determinare dove sono memorizzati i dati degli oggetti. Quando si configurano le regole ILM per la replica, si selezionano uno o più pool di storage che includono nodi di storage o nodi di archivio. Quando si creano profili di codifica Erasure, si seleziona un pool di storage che include i nodi di storage.

Linee guida per la creazione di pool di storage

Per la configurazione e l'utilizzo dei pool di storage, attenersi alle seguenti linee guida.

Linee guida per tutti i pool di storage

- StorageGRID include un pool di storage predefinito, tutti i nodi di storage, che utilizza il sito predefinito, tutti i siti e il livello di storage predefinito, tutti i nodi di storage. Il pool di storage All Storage Node viene aggiornato automaticamente ogni volta che si aggiungono nuovi siti del data center.



Si sconsiglia di utilizzare il pool di storage All Storage Node o il sito All Sites perché questi elementi vengono aggiornati automaticamente per includere i nuovi siti aggiunti in un'espansione, il che potrebbe non essere il comportamento desiderato. Prima di utilizzare il pool di storage All Storage Node o il sito predefinito, rivedere attentamente le linee guida per le copie replicate e codificate per l'erasure.

- Le configurazioni del pool di storage sono il più semplici possibile. Non creare più pool di storage del necessario.
- Creare pool di storage con il maggior numero possibile di nodi. Ogni pool di storage deve contenere due o più nodi. Un pool di storage con nodi insufficienti può causare backlog ILM se un nodo diventa non disponibile.
- Evitare di creare o utilizzare pool di storage che si sovrappongono (contenenti uno o più degli stessi nodi). Se i pool di storage si sovrappongono, è possibile che più di una copia dei dati dell'oggetto venga salvata sullo stesso nodo.

Linee guida per i pool di storage utilizzati per le copie replicate

- Creare un pool di storage diverso per ciascun sito. Quindi, specificare uno o più pool di storage specifici del sito nelle istruzioni di posizionamento per ciascuna regola. L'utilizzo di un pool di storage per ciascun sito garantisce che le copie degli oggetti replicate vengano posizionate esattamente dove ci si aspetta (ad esempio, una copia di ogni oggetto in ogni sito per la protezione dalla perdita di sito).
- Se si aggiunge un sito in un'espansione, creare un nuovo pool di storage per il nuovo sito. Quindi, aggiornare le regole ILM per controllare quali oggetti sono memorizzati nel nuovo sito.
- In generale, non utilizzare il pool di storage predefinito, tutti i nodi di storage o qualsiasi pool di storage che includa il sito predefinito, tutti i siti.

Linee guida per i pool di storage utilizzati per le copie erasure-coded

- Non è possibile utilizzare i nodi di archiviazione per i dati con codifica erasure.
- Il numero di nodi e siti di storage contenuti nel pool di storage determina quali schemi di erasure coding sono disponibili.
- Se un pool di storage include solo due siti, non è possibile utilizzare tale pool di storage per la

cancellazione del codice. Non sono disponibili schemi di erasure coding per un pool di storage con due siti.

- In generale, non utilizzare il pool di storage predefinito, tutti i nodi di storage o qualsiasi pool di storage che includa il sito predefinito, tutti i siti in qualsiasi profilo di codifica Erasure.



Se la griglia include un solo sito, non è possibile utilizzare il pool di storage All Storage Node o il sito predefinito All Sites in un profilo di codifica Erasure. Questo comportamento impedisce che il profilo di codifica Erasure diventi non valido se viene aggiunto un secondo sito.

- Se si hanno requisiti di throughput elevati, la creazione di un pool di storage che include più siti non è consigliata se la latenza di rete tra 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 del throughput di rete TCP. La diminuzione del throughput influisce sui tassi massimi raggiungibili di acquisizione e recupero degli oggetti (quando si seleziona Strict o Balanced come comportamento Ingest) o può portare a backlog della coda ILM (quando viene selezionato Dual Commit come comportamento Ingest).
- Se possibile, un pool di storage deve includere un numero superiore al numero minimo di nodi di storage richiesto per lo schema di erasure coding selezionato. Ad esempio, se si utilizza uno schema di erasure coding 6+3, è necessario disporre di almeno nove nodi di storage. Tuttavia, si consiglia di disporre di almeno un nodo di storage aggiuntivo per sito.
- Distribuire i nodi di storage tra i siti nel modo più uniforme possibile. Ad esempio, per supportare uno schema di erasure coding 6+3, configurare un pool di storage che includa almeno tre nodi di storage in tre siti.

Linee guida per i pool di storage utilizzati per le copie archiviate

- Non è possibile creare un pool di storage che includa nodi di storage e nodi di archiviazione. Le copie archiviate richiedono un pool di storage che includa solo i nodi di archiviazione.
- Quando si utilizza un pool di storage che include nodi di archiviazione, è necessario mantenere almeno una copia replicata o codificata in cancellazione su un pool di storage che include nodi di storage.
- Se l'impostazione blocco oggetti S3 globale è attivata e si sta creando una regola ILM conforme, non è possibile utilizzare un pool di storage che include nodi di archiviazione. Vedere le istruzioni per la gestione degli oggetti con S3 Object Lock.
- Se il tipo di destinazione di un nodo di archiviazione è Cloud Tiering - Simple Storage Service (S3), il nodo di archiviazione deve trovarsi nel proprio pool di storage. Consultare le istruzioni per l'amministrazione di StorageGRID.

Informazioni correlate

["Che cos'è la replica"](#)

["Che cos'è la cancellazione dei codici"](#)

["Quali sono gli schemi di erasure coding"](#)

["Utilizzo di più pool di storage per la replica tra siti"](#)

["Utilizzo di un pool di storage come posizione temporanea \(obsoleto\)"](#)

["Gestione degli oggetti con S3 Object Lock"](#)

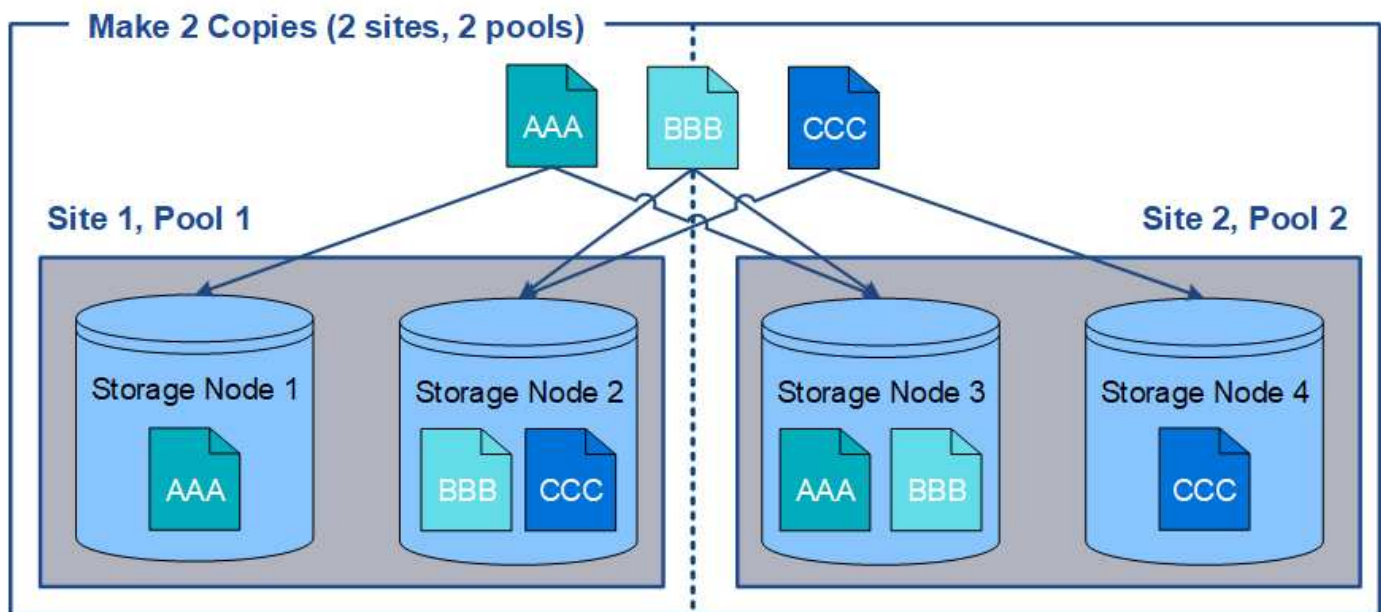
["Amministrare StorageGRID"](#)

Utilizzo di più pool di storage per la replica tra siti

Se l'implementazione di StorageGRID include più siti, è possibile attivare la protezione dalla perdita di sito creando un pool di storage per ciascun sito e specificando entrambi i pool di storage nelle istruzioni di posizionamento della regola. Ad esempio, se si configura una regola ILM per eseguire due copie replicate e specificare pool di storage in due siti, una copia di ciascun oggetto verrà posizionata in ciascun sito. Se si configura una regola per eseguire due copie e si specificano tre pool di storage, le copie vengono distribuite in modo da bilanciare l'utilizzo del disco tra i pool di storage, garantendo al contempo che le due copie vengano memorizzate in siti diversi.

Nell'esempio seguente viene illustrato cosa può accadere se una regola ILM inserisce copie di oggetti replicate in un singolo pool di storage contenente nodi di storage da due siti. Poiché il sistema utilizza i nodi disponibili nel pool di storage quando inserisce le copie replicate, potrebbe posizionare tutte le copie di alcuni oggetti all'interno di uno solo dei siti. In questo esempio, il sistema ha memorizzato due copie di Object AAA sui nodi di storage nel sito 1 e due copie di Object CCC sui nodi di storage nel sito 2. Solo il BBB oggetto è protetto se uno dei siti si guasta o diventa inaccessibile.

Al contrario, questo esempio illustra come vengono memorizzati gli oggetti quando si utilizzano più pool di storage. Nell'esempio, la regola ILM specifica che devono essere create due copie replicate di ciascun oggetto e che le copie devono essere distribuite in due pool di storage. Ogni pool di storage contiene tutti i nodi di storage in un sito. Poiché una copia di ciascun oggetto viene memorizzata in ogni sito, i dati dell'oggetto sono protetti da guasti o inaccessibilità del sito.



Quando si utilizzano più pool di storage, tenere presenti le seguenti regole:

- Se si creano n copie, è necessario aggiungere n o più pool di storage. Ad esempio, se una regola è configurata per eseguire tre copie, è necessario specificare tre o più pool di storage.
- Se il numero di copie corrisponde al numero di pool di storage, viene memorizzata una copia dell'oggetto in ciascun pool di storage.
- Se il numero di copie è inferiore al numero di pool di storage, il sistema distribuisce le copie per mantenere bilanciato l'utilizzo del disco tra i pool e garantire che due o più copie non vengano memorizzate nello

stesso pool di storage.

- Se i pool di storage si sovrappongono (contengono gli stessi nodi di storage), tutte le copie dell'oggetto potrebbero essere salvate in un solo sito. È necessario assicurarsi che i pool di storage selezionati non contengano gli stessi nodi di storage.

Utilizzo di un pool di storage come posizione temporanea (obsoleto)

Quando si crea una regola ILM con un posizionamento degli oggetti che include un singolo pool di storage, viene richiesto di specificare un secondo pool di storage da utilizzare come posizione temporanea.

Le posizioni temporanee sono state deprecate e verranno rimosse in una release futura. Non selezionare un pool di storage come posizione temporanea per una nuova regola ILM.



Se si seleziona il comportamento di acquisizione rigorosa (fase 3 della procedura guidata Crea regola ILM), la posizione temporanea viene ignorata.

Informazioni correlate

["Opzioni di protezione dei dati per l'acquisizione"](#)

Creazione di un pool di storage


Si creano pool di storage per determinare dove il sistema StorageGRID memorizza i dati a oggetti e il tipo di storage utilizzato. Ogni pool di storage include uno o più siti e uno o più tipi di storage.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.
- È necessario aver esaminato le linee guida per la creazione di pool di storage.

A proposito di questa attività

I pool di storage determinano la posizione in cui vengono memorizzati i dati degli oggetti. Il numero di pool di storage necessari dipende dal numero di siti nella griglia e dal tipo di copie desiderato: Replicate o con codifica di cancellazione.

- Per la replica e l'erasure coding a sito singolo, creare un pool di storage per ciascun sito. Ad esempio, se si desidera memorizzare copie di oggetti replicate in tre siti, creare tre pool di storage.
- Per la cancellazione del codice in tre o più siti, creare un pool di storage che includa una voce per ciascun sito. Ad esempio, se si desidera erasure gli oggetti del codice in tre siti, creare un pool di storage. Selezionare l'icona più  per aggiungere una voce per ciascun sito.



Non includere il sito All Sites predefinito in un pool di storage che verrà utilizzato in un profilo di codifica Erasure. Al contrario, aggiungere una voce separata al pool di storage per ogni sito che memorizzerà i dati codificati in cancellazione. Vedere [questo passo](#) ad esempio.

- Se si dispone di più storage di livello, non creare un pool di storage che includa diversi tipi di storage in un singolo sito.

["Linee guida per la creazione di pool di storage"](#)

Fasi

1. Selezionare **ILM > Storage Pools**.

Viene visualizzata la pagina Storage Pools (Pool di storage) che elenca tutti i pool di storage definiti.

Storage Pools

Storage Pools

A storage pool is a logical group of Storage Nodes or Archive Nodes and is used in ILM rules to determine where object data is stored.

Name	Used Space	Free Space	Total Capacity	ILM Usage
All Storage Nodes	1.10 MB	102.90 TB	102.90 TB	Used in 1 ILM rule

Displaying 1 storage pool.

Cloud Storage Pools

You can add Cloud Storage Pools to ILM rules to store objects outside of the StorageGRID system. A Cloud Storage Pool defines how to access the external bucket or container where objects will be stored.

Name	Used Space	Free Space	Total Capacity	ILM Usage
No Cloud Storage Pools found.				

L'elenco include il pool di storage predefinito del sistema, tutti i nodi di storage, che utilizza il sito predefinito del sistema, tutti i siti e il livello di storage predefinito, tutti i nodi di storage.



Poiché il pool di storage All Storage Node viene aggiornato automaticamente ogni volta che si aggiungono nuovi siti del data center, si sconsiglia di utilizzare questo pool di storage nelle regole ILM.

2. Per creare un nuovo pool di storage, selezionare **Crea**.

Viene visualizzata la finestra di dialogo Create Storage Pool (Crea pool di storage).

Create Storage Pool

- For replication and single-site erasure coding, create a storage pool for each site.
- For erasure coding at three or more sites, click + to add each site to a single storage pool.
- Do not add more than one storage grade for a single site.

Name

Site

Storage Grade

Viewing Storage Pool -

Site Name	Archive Nodes	Storage Nodes
-----------	---------------	---------------

3. Immettere un nome univoco per il pool di storage.

Utilizzare un nome facilmente identificabile quando si configurano i profili di codifica Erasure e le regole ILM.

4. Dall'elenco a discesa **Sito**, selezionare un sito per questo pool di storage.

Quando si seleziona un sito, il numero di nodi di storage e di nodi di archiviazione nella tabella viene aggiornato automaticamente.

5. Dall'elenco a discesa **Storage Grade**, selezionare il tipo di storage da utilizzare se una regola ILM utilizza questo pool di storage.

Il livello di storage predefinito di All Storage Node include tutti i nodi di storage nel sito selezionato. Il livello di storage dei nodi di archiviazione predefinito include tutti i nodi di archiviazione nel sito selezionato. Se sono stati creati altri gradi di storage per i nodi di storage nel grid, questi vengono elencati nell'elenco a discesa.

6. se si desidera utilizzare il pool di storage in un profilo di codifica Erasure multi-sito, selezionare **+** per aggiungere una voce per ciascun sito al pool di storage.

Create Storage Pool

- For replication and single-site erasure coding, create a storage pool for each site.
- For erasure coding at three or more sites, select + to add each site to a single storage pool.
- Do not select more than one storage grade for a single site.

Name:

Site:	<input type="text" value="Data Center 1"/>	Storage Grade:	<input type="text" value="All Storage Nodes"/>	<input type="button" value="x"/>
Site:	<input type="text" value="Data Center 2"/>	Storage Grade:	<input type="text" value="All Storage Nodes"/>	<input type="button" value="x"/>
Site:	<input type="text" value="Data Center 3"/>	Storage Grade:	<input type="text" value="All Storage Nodes"/>	<input type="button" value="+"/> <input type="button" value="x"/>

Viewing Storage Pool - All 3 Sites for Erasure Coding

Site Name	Archive Nodes	Storage Nodes
Data Center 1	0	3
Data Center 2	0	3
Data Center 3	0	3

You are creating a multi-site storage pool, which should not be used for replication or single-site erasure coding.

Cancel

Save



Non è possibile creare voci duplicate o creare un pool di storage che includa sia il livello di storage **Archive Node** che qualsiasi livello di storage che contenga i nodi di storage.

Viene visualizzato un avviso se si aggiungono più voci per un sito ma con diversi gradi di storage.

Per rimuovere una voce, selezionare **x**.

7. Quando si è soddisfatti delle selezioni effettuate, selezionare **Save** (Salva).

Il nuovo pool di storage viene aggiunto all'elenco.

Informazioni correlate

["Linee guida per la creazione di pool di storage"](#)

Visualizzazione dei dettagli del pool di storage

È possibile visualizzare i dettagli di un pool di storage per determinare dove viene utilizzato il pool di storage e per vedere quali nodi e gradi di storage sono inclusi.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

Fasi

1. Selezionare **ILM > Storage Pools**.

Viene visualizzata la pagina Storage Pools. In questa pagina sono elencati tutti i pool di storage definiti.

Storage Pools

Storage Pools

A storage pool is a logical group of Storage Nodes or Archive Nodes and is used in ILM rules to determine where object data is stored.

	Name	Used Space	Free Space	Total Capacity	ILM Usage
<input checked="" type="radio"/>	All Storage Nodes	1.88 MB	2.80 TB	2.80 TB	Used in 1 ILM rule
<input type="radio"/>	DC1	621.77 KB	932.42 GB	932.42 GB	Used in 2 ILM rules
<input type="radio"/>	DC2	675.82 KB	932.42 GB	932.42 GB	Used in 2 ILM rules
<input type="radio"/>	DC3	578.95 KB	932.42 GB	932.42 GB	Used in 1 ILM rule
<input type="radio"/>	All 3 Sites	1.88 MB	2.80 TB	2.80 TB	Used in 1 ILM rule and 1 EC profile
<input type="radio"/>	Archive	—	—	—	—

Displaying 6 storage pools.

Cloud Storage Pools

You can add Cloud Storage Pools to ILM rules to store objects outside of the StorageGRID system. A Cloud Storage Pool defines how to access the external bucket or container where objects will be stored.

	Name	Used Space	Free Space	Total Capacity	ILM Usage
No Cloud Storage Pools found.					

La tabella include le seguenti informazioni per ogni pool di storage che include i nodi di storage:

- **Name:** Il nome univoco del pool di storage.
- **Spazio utilizzato:** La quantità di spazio attualmente utilizzata per memorizzare gli oggetti nel pool di storage.

- **Spazio libero:** La quantità di spazio disponibile per memorizzare gli oggetti nel pool di storage.
- **Capacità totale:** La dimensione del pool di storage, che equivale alla quantità totale di spazio utilizzabile per i dati oggetto per tutti i nodi nel pool di storage .
- **ILM Usage:** Modalità di utilizzo del pool di storage. Un pool di storage potrebbe essere inutilizzato o utilizzato in una o più regole ILM, profili di codifica Erasure o entrambi.



Non è possibile rimuovere un pool di storage se è in uso.

2. Per visualizzare i dettagli relativi a uno specifico pool di storage, selezionare il relativo pulsante di opzione e selezionare **Visualizza dettagli**.

Viene visualizzato il modale Storage Pool Details (Dettagli pool di storage)

3. Visualizzare la scheda **nodi inclusi** per informazioni sui nodi di storage o di archivio inclusi nel pool di storage.

Storage Pool Details - DC1

Nodes Included

ILM Usage

Number of Nodes: 3
Storage Grade: All Storage Nodes

Node Name	Site Name	Used (%) ?	↑↓
DC1-S1	Data Center 1	0.000%	
DC1-S2	Data Center 1	0.000%	
DC1-S3	Data Center 1	0.000%	

Close

La tabella include le seguenti informazioni per ciascun nodo:

- Nome del nodo
- Nome del sito
- Utilizzato (%): Per i nodi di storage, la percentuale dello spazio utilizzabile totale per i dati dell'oggetto che è stato utilizzato. Questo valore non include i metadati degli oggetti.



Lo stesso valore utilizzato (%) viene mostrato anche nel grafico Storage Used - Object Data per ciascun nodo di storage (selezionare **Nodes > Storage Node > Storage**).

4. Selezionare la scheda **utilizzo ILM** per determinare se il pool di storage è attualmente utilizzato in qualsiasi regola ILM o profilo di codifica Erasure.

In questo esempio, il pool di storage DC1 viene utilizzato in tre regole ILM: Due regole che si trovano nel criterio ILM attivo e una regola che non si trova nel criterio attivo.

Storage Pool Details - DC1

Nodes Included


ILM Usage

ILM Rules Using the Storage Pool

The following ILM rules in the active ILM policy (Example ILM policy) use this storage pool.

- 3 copies for Account01
- 2 copies for smaller objects

1 ILM rule that is not in the active ILM policy uses this storage pool.

If you want to remove this storage pool, you must delete or edit every rule where it is used. Go to the [ILM Rules page](#) .

EC Profiles Using the Storage Pool

No Erasure Coding profiles use this storage pool.

Close



Non è possibile rimuovere un pool di storage se utilizzato in una regola ILM.

In questo esempio, il pool di storage di tutti e 3 i siti viene utilizzato in un profilo di codifica Erasure. A sua volta, il profilo di codifica Erasure viene utilizzato da una regola ILM nel criterio ILM attivo.

Storage Pool Details - All 3 Sites


Nodes Included

ILM Usage

ILM Rules Using the Storage Pool

The following ILM rules in the active ILM policy (Example ILM policy) use this storage pool.

- EC larger objects

If you want to remove this storage pool, you must delete or edit every rule where it is used. Go to the [ILM Rules page](#) .

EC Profiles Using the Storage Pool

The following Erasure Coding profiles use this storage pool.

Profile Name	Profile Status 
6 plus 3	Used in 1 ILM Rule

Close



Non è possibile rimuovere un pool di storage se utilizzato in un profilo di codifica Erasure.

5. Se si desidera, accedere alla pagina **ILM Rules** per informazioni e gestione delle regole che utilizzano il pool di storage.

Consultare le istruzioni per l'utilizzo delle regole ILM.

6. Una volta visualizzati i dettagli del pool di storage, selezionare **Chiudi**.

Informazioni correlate

["Utilizzo delle regole ILM e delle policy ILM"](#)

Modifica di un pool di storage

È possibile modificare un pool di storage per modificarne il nome o per aggiornare siti e gradi di storage.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.
- È necessario aver esaminato le linee guida per la creazione di pool di storage.
- Se si intende modificare un pool di storage utilizzato da una regola nel criterio ILM attivo, è necessario considerare come le modifiche influiranno sul posizionamento dei dati degli oggetti.

A proposito di questa attività

Se si aggiunge un nuovo livello di storage a un pool di storage utilizzato nel criterio ILM attivo, tenere presente che i nodi di storage nel nuovo livello di storage non verranno utilizzati automaticamente. Per forzare StorageGRID a utilizzare un nuovo livello di storage, è necessario attivare un nuovo criterio ILM dopo aver salvato il pool di storage modificato.

Fasi

1. Selezionare **ILM > Storage Pools**.

Viene visualizzata la pagina Storage Pools.

2. Selezionare il pulsante di opzione per il pool di storage che si desidera modificare.

Non è possibile modificare il pool di storage di tutti i nodi di storage.

3. Selezionare **Modifica**.

4. Se necessario, modificare il nome del pool di storage.

5. Se necessario, selezionare altri siti e livelli di storage.



Se il pool di storage viene utilizzato in un profilo di codifica Erasure e la modifica causerebbe l'invalidità dello schema di erasure coding, non sarà possibile modificare il livello di sito o storage. Ad esempio, se un pool di storage utilizzato in un profilo di codifica Erasure include attualmente un livello di storage con un solo sito, non è possibile utilizzare un livello di storage con due siti, poiché la modifica renderebbe lo schema di erasure-coding non valido.

6. Selezionare **Salva**.

Al termine

Se è stato aggiunto un nuovo livello di storage a un pool di storage utilizzato nel criterio ILM attivo, attivare un nuovo criterio ILM per forzare StorageGRID a utilizzare il nuovo livello di storage. Ad esempio, clonare il criterio ILM esistente e attivare il clone.

Rimozione di un pool di storage

È possibile rimuovere un pool di storage che non viene utilizzato.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

Fasi

1. Selezionare **ILM > Storage Pools**.

Viene visualizzata la pagina Storage Pools.

2. Esaminare la colonna ILM Usage nella tabella per determinare se è possibile rimuovere il pool di storage.

Non è possibile rimuovere un pool di storage se utilizzato in una regola ILM o in un profilo di codifica Erasure. Se necessario, selezionare **View Details > ILM Usage** (Visualizza dettagli* > **ILM Usage**) per determinare dove viene utilizzato un pool di storage.

3. Se il pool di storage che si desidera rimuovere non viene utilizzato, selezionare il pulsante di opzione.
4. Selezionare **Rimuovi**.
5. Selezionare **OK**.

Utilizzo dei Cloud Storage Pools

È possibile utilizzare i pool di storage cloud per spostare gli oggetti StorageGRID in una posizione di storage esterna, ad esempio lo storage S3 Glacier o Microsoft Azure Blob. Lo spostamento di oggetti all'esterno della griglia consente di sfruttare un Tier di storage a basso costo per l'archiviazione a lungo termine.

- ["Cos'è un pool di storage cloud"](#)
- ["Ciclo di vita di un oggetto Cloud Storage Pool"](#)
- ["Quando utilizzare i Cloud Storage Pools"](#)
- ["Considerazioni per i Cloud Storage Pools"](#)
- ["Confronto tra Cloud Storage Pools e la replica CloudMirror"](#)
- ["Creazione di un pool di storage cloud"](#)
- ["Modifica di un pool di storage cloud"](#)
- ["Rimozione di un pool di storage cloud"](#)
- ["Risoluzione dei problemi relativi ai pool di storage cloud"](#)

Cos'è un pool di storage cloud

Un pool di storage cloud consente di utilizzare ILM per spostare i dati degli oggetti all'esterno del sistema StorageGRID. Ad esempio, è possibile spostare gli oggetti con accesso non frequente in uno storage cloud a basso costo, ad esempio Amazon S3 Glacier, S3 Glacier Deep Archive o il Tier di accesso all'archivio nello storage Microsoft Azure Blob. In alternativa, è possibile mantenere un backup cloud degli oggetti

StorageGRID per migliorare il disaster recovery.

Dal punto di vista di ILM, un pool di storage cloud è simile a un pool di storage. Per memorizzare gli oggetti in entrambe le posizioni, selezionare il pool quando si creano le istruzioni di posizionamento per una regola ILM. Tuttavia, mentre i pool di storage sono costituiti da nodi di storage o nodi di archiviazione all'interno del sistema StorageGRID, un pool di storage cloud è costituito da un bucket esterno (S3) o da un container (storage blob Azure).

La seguente tabella confronta i pool di storage con i pool di storage cloud e mostra le analogie e le differenze di alto livello.

	Pool di storage	Pool di cloud storage
Come viene creato?	Utilizzando l'opzione ILM > Storage Pools in Grid Manager. È necessario impostare i gradi di storage prima di poter creare il pool di storage.	Utilizzando l'opzione ILM > Storage Pools in Grid Manager. È necessario configurare il bucket o il container esterno prima di poter creare il Cloud Storage Pool.
Quanti pool è possibile creare?	Senza limiti.	Fino a 10.

	Pool di storage	Pool di cloud storage
Dove sono memorizzati gli oggetti?	Su uno o più nodi di storage o nodi di archiviazione all'interno di StorageGRID.	<p>In un bucket Amazon S3 o in un container di storage Azure Blob esterno al sistema StorageGRID.</p> <p>Se il Cloud Storage Pool è un bucket Amazon S3:</p> <ul style="list-style-type: none"> • È possibile configurare un ciclo di vita del bucket per la transizione di oggetti a storage a lungo termine e a basso costo, come Amazon S3 Glacier o S3 Glacier Deep Archive. Il sistema di storage esterno deve supportare la classe di storage Glacier e l'API di ripristino degli oggetti S3 POST. • È possibile creare pool di storage cloud da utilizzare con AWS Commercial Cloud Services (C2S), che supporta l'AWS Secret Region. <p>Se il pool di storage cloud è un container di storage Azure Blob, StorageGRID passa l'oggetto al Tier di archiviazione.</p> <p>Nota: in generale, non configurare la gestione del ciclo di vita dello storage Azure Blob per il container utilizzato per un pool di storage cloud. Le operazioni DI ripristino POST-oggetto sugli oggetti nel Cloud Storage Pool possono essere influenzate dal ciclo di vita configurato.</p>
Cosa controlla il posizionamento degli oggetti?	Una regola ILM nel criterio ILM attivo.	Una regola ILM nel criterio ILM attivo.
Quale metodo di protezione dei dati viene utilizzato?	Replica o erasure coding.	Replica.
Quante copie di ciascun oggetto sono consentite?	Multiplo.	<p>Una copia nel pool di storage cloud e, facoltativamente, una o più copie in StorageGRID.</p> <p>Nota: non è possibile memorizzare un oggetto in più di un Cloud Storage Pool alla volta.</p>
Quali sono i vantaggi?	Gli oggetti sono rapidamente accessibili in qualsiasi momento.	Storage a basso costo.

Ciclo di vita di un oggetto Cloud Storage Pool

Prima di implementare i Cloud Storage Pool, esaminare il ciclo di vita degli oggetti memorizzati in ciascun tipo di Cloud Storage Pool.

Informazioni correlate

[S3: Ciclo di vita di un oggetto Cloud Storage Pool](#)

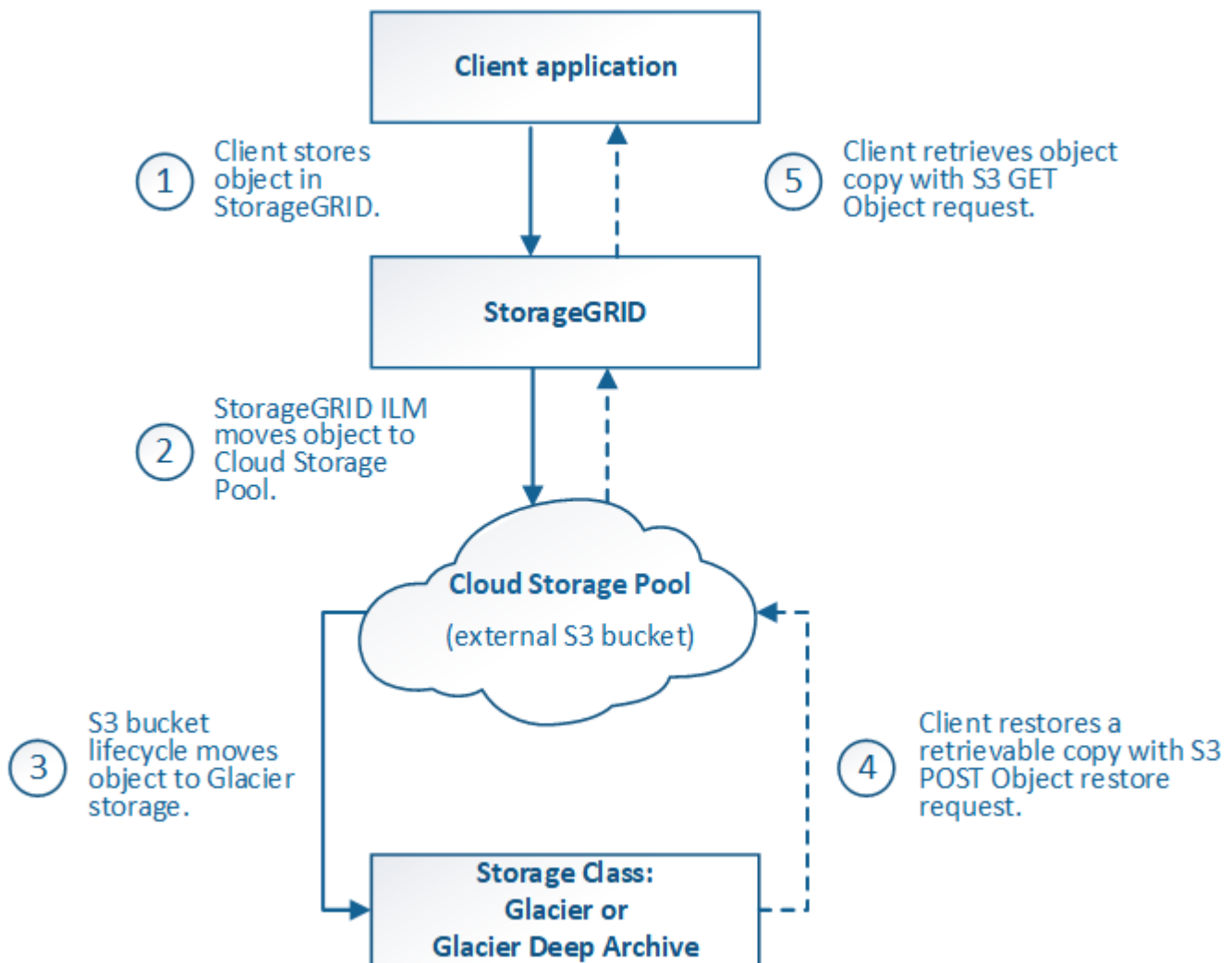
[Azure: Ciclo di vita di un oggetto Cloud Storage Pool\]](#)

S3: Ciclo di vita di un oggetto Cloud Storage Pool

La figura mostra le fasi del ciclo di vita di un oggetto memorizzato in un pool di storage cloud S3.



Nella figura e nelle spiegazioni, “Glacier” si riferisce sia alla classe di storage Glacier che alla classe di storage Glacier Deep Archive, con un’eccezione: La classe di storage Glacier Deep Archive non supporta il Tier di ripristino accelerato. È supportato solo il recupero in blocco o standard.



1. Oggetto memorizzato in StorageGRID

Per avviare il ciclo di vita, un'applicazione client memorizza un oggetto in StorageGRID.

2. Oggetto spostato in S3 Cloud Storage Pool

- Quando l'oggetto viene associato a una regola ILM che utilizza un pool di storage cloud S3 come posizione di posizionamento, StorageGRID sposta l'oggetto nel bucket S3 esterno specificato dal pool di storage cloud.
- Quando l'oggetto è stato spostato nel pool di storage cloud S3, l'applicazione client può recuperarlo utilizzando una richiesta di oggetti Get S3 da StorageGRID, a meno che l'oggetto non sia stato trasferito allo storage Glacier.

3. Oggetto in transizione a Glacier (stato non recuperabile)

- Facoltativamente, l'oggetto può essere passato allo 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 eseguire la transizione degli oggetti, è necessario creare una configurazione del ciclo di vita per il bucket S3 esterno e utilizzare una soluzione di storage che implementi la classe di storage Glacier e supporti l'API di ripristino degli oggetti S3 POST.



Non utilizzare i Cloud Storage Pools per oggetti che sono stati acquisiti dai client Swift. Swift non supporta le richieste DI ripristino DEGLI oggetti POST, pertanto StorageGRID non sarà in grado di recuperare oggetti Swift che sono stati trasferiti allo storage S3 Glacier. L'emissione di una richiesta Swift GET Object per recuperare questi oggetti non avrà esito positivo (403 proibita).

- Durante la transizione, l'applicazione client può utilizzare una richiesta di oggetto S3 HEAD per monitorare lo stato dell'oggetto.

4. Oggetto ripristinato dallo storage Glacier

Se un oggetto è stato passato allo storage Glacier, l'applicazione client può emettere una richiesta di ripristino dell'oggetto S3 POST per ripristinare una copia recuperabile nel Cloud Storage Pool S3. La richiesta specifica il numero di giorni in cui la copia deve essere disponibile nel Cloud Storage Pool e il Tier di accesso ai dati da utilizzare per l'operazione di ripristino (accelerato, Standard o in blocco). Una volta raggiunta la data di scadenza della copia recuperabile, la copia viene automaticamente riportata in uno stato non recuperabile.



Se una o più copie dell'oggetto esistono anche nei nodi di storage all'interno di StorageGRID, non è necessario ripristinare l'oggetto da Glacier inviando una richiesta DI ripristino DELL'oggetto POST. Invece, la copia locale può essere recuperata direttamente, utilizzando una richiesta DI oggetto GET.

5. Oggetto recuperato

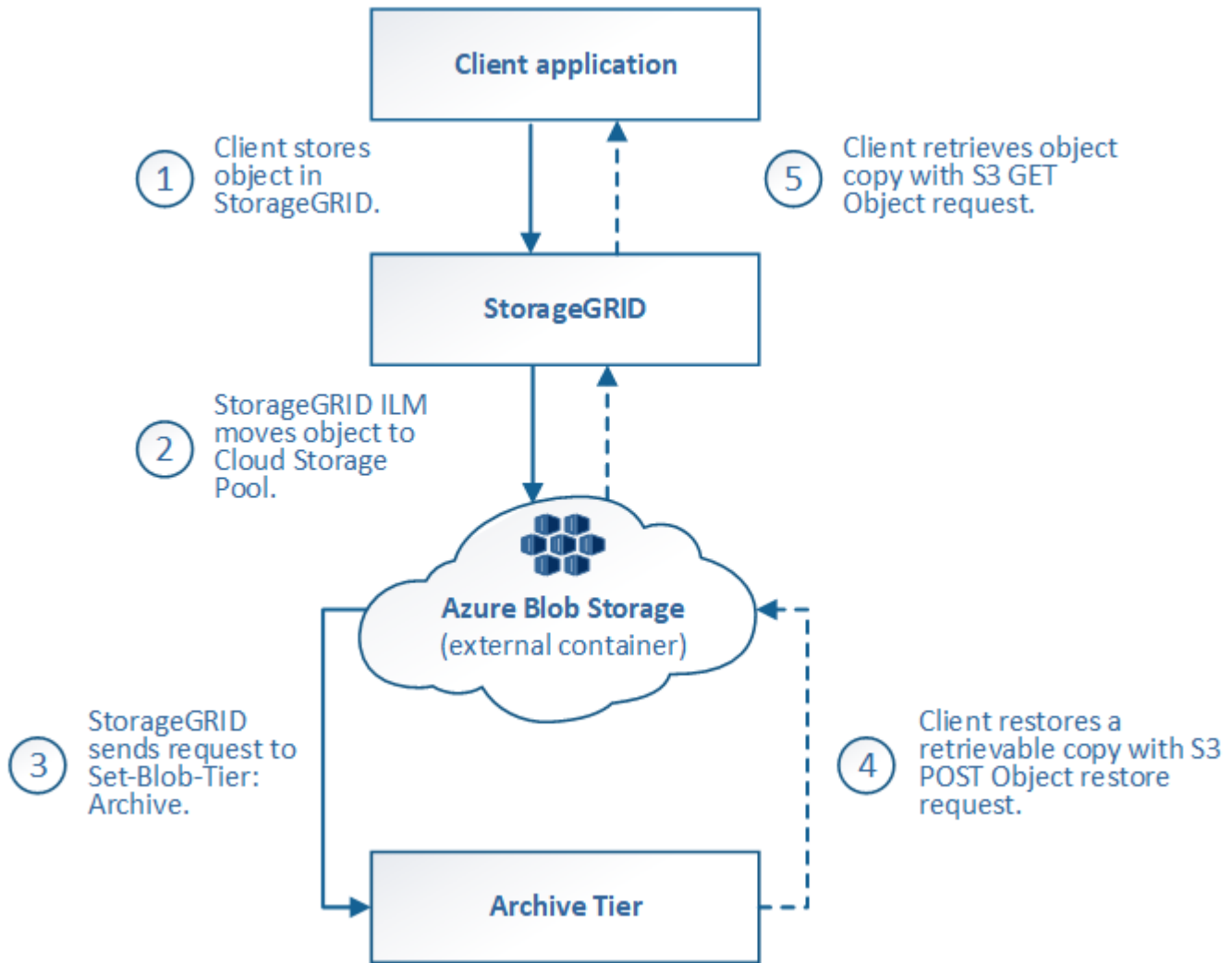
Una volta ripristinato un oggetto, l'applicazione client può inviare una richiesta DI RECUPERO dell'oggetto ripristinato.

Informazioni correlate

["Utilizzare S3"](#)

Azure: Ciclo di vita di un oggetto Cloud Storage Pool

La figura mostra le fasi del ciclo di vita di un oggetto memorizzato in un pool di storage Azure Cloud.



1. Oggetto memorizzato in StorageGRID

Per avviare il ciclo di vita, un'applicazione client memorizza un oggetto in StorageGRID.

2. Oggetto spostato in Azure Cloud Storage Pool

Quando l'oggetto viene associato a una regola ILM che utilizza un pool di storage cloud Azure come posizione di posizionamento, StorageGRID sposta l'oggetto nel contenitore di storage blob Azure esterno specificato dal pool di storage cloud



Non utilizzare i Cloud Storage Pools per oggetti che sono stati acquisiti dai client Swift. Swift non supporta le richieste DI ripristino POST-oggetto, pertanto StorageGRID non sarà in grado di recuperare oggetti Swift che sono stati trasferiti al Tier di archiviazione dello storage di Azure Blob. L'emissione di una richiesta Swift GET Object per recuperare questi oggetti non avrà esito positivo (403 proibita).

3. Oggetto sottoposto a transizione al Tier di archiviazione (stato non recuperabile)

Subito dopo aver spostato l'oggetto nel pool di storage cloud di Azure, StorageGRID passa

automaticamente l'oggetto al livello di archiviazione dello storage Blob di Azure.

4. Oggetto ripristinato dal Tier di archiviazione

Se un oggetto è stato passato al Tier Archive, l'applicazione client può emettere una richiesta di ripristino dell'oggetto S3 POST per ripristinare una copia recuperabile nel pool di storage di Azure Cloud.

Quando StorageGRID riceve il ripristino dell'oggetto POST, passa temporaneamente l'oggetto al livello di raffreddamento dello storage di Azure Blob. Non appena viene raggiunta la data di scadenza nella richiesta DI ripristino DELL'oggetto POST, StorageGRID riconsegna l'oggetto al livello di archiviazione.



Se una o più copie dell'oggetto esistono anche nei nodi di storage all'interno di StorageGRID, non è necessario ripristinare l'oggetto dal livello di accesso di archiviazione inviando una richiesta DI ripristino POST-oggetto. Invece, la copia locale può essere recuperata direttamente, utilizzando una richiesta DI oggetto GET.

5. Oggetto recuperato

Una volta ripristinato un oggetto in Azure Cloud Storage Pool, l'applicazione client può inviare una richiesta DI RECUPERO dell'oggetto ripristinato.

Quando utilizzare i Cloud Storage Pools

I pool di cloud storage possono offrire vantaggi significativi in diversi casi di utilizzo.

Backup dei dati StorageGRID in una posizione esterna

È possibile utilizzare un pool di storage cloud per eseguire il backup degli oggetti StorageGRID in una posizione esterna.

Se le copie in StorageGRID non sono accessibili, i dati dell'oggetto nel pool di storage cloud possono essere utilizzati per soddisfare le richieste dei client. Tuttavia, potrebbe essere necessario emettere una richiesta di ripristino S3 POST Object per accedere alla copia dell'oggetto di backup nel Cloud Storage Pool.

I dati dell'oggetto in un pool di storage cloud possono essere utilizzati anche per recuperare i dati persi da StorageGRID a causa di un guasto di un volume di storage o di un nodo di storage. Se l'unica copia rimanente di un oggetto si trova in un pool di storage cloud, StorageGRID ripristina temporaneamente l'oggetto e crea una nuova copia sul nodo di storage ripristinato.

Per implementare una soluzione di backup:

1. Creare un singolo pool di storage cloud.
2. Configurare una regola ILM che memorizzi simultaneamente le copie degli oggetti sui nodi di storage (come copie replicate o codificate in cancellazione) e una singola copia degli oggetti nel Cloud Storage Pool.
3. Aggiungere la regola al criterio ILM. Quindi, simulare e attivare la policy.

Tiering dei dati da StorageGRID a una posizione esterna

È possibile utilizzare un pool di storage cloud per memorizzare oggetti all'esterno del sistema StorageGRID. Si supponga, ad esempio, di disporre di un elevato numero di oggetti da conservare, ma si prevede di accedervi raramente, se mai. È possibile utilizzare un pool di storage cloud per tierare gli oggetti in modo da ridurre il costo dello storage e liberare spazio in StorageGRID.

Per implementare una soluzione di tiering:

1. Creare un singolo pool di storage cloud.
2. Configurare una regola ILM che sposti gli oggetti utilizzati raramente dai nodi di storage al Cloud Storage Pool.
3. Aggiungere la regola al criterio ILM. Quindi, simulare e attivare la policy.

Mantenere più endpoint cloud

Puoi configurare più Cloud Storage Pool se desideri eseguire il tiering o il backup dei dati degli oggetti in più di un cloud. I filtri nelle regole ILM consentono di specificare quali oggetti sono memorizzati in ciascun Cloud Storage Pool. Ad esempio, è possibile memorizzare oggetti di alcuni tenant o bucket in Amazon S3 Glacier e oggetti di altri tenant o bucket nello storage Azure Blob. In alternativa, puoi spostare i dati tra lo storage Amazon S3 Glacier e Azure Blob. Quando si utilizzano più Cloud Storage Pool, tenere presente che un oggetto può essere memorizzato in un solo Cloud Storage Pool alla volta.

Per implementare più endpoint cloud:

1. Crea fino a 10 pool di cloud storage.
2. Configurare le regole ILM in modo che memorizzino i dati dell'oggetto appropriati all'ora appropriata in ciascun Cloud Storage Pool. Ad esempio, memorizzare oggetti dal bucket A nel Cloud Storage Pool A e memorizzare oggetti dal bucket B nel Cloud Storage Pool B. Oppure, memorizzare gli oggetti nel Cloud Storage Pool A per un certo periodo di tempo e spostarli nel Cloud Storage Pool B.
3. Aggiungere le regole alla policy ILM. Quindi, simulare e attivare la policy.

Considerazioni per i Cloud Storage Pools

Se si prevede di utilizzare un pool di storage cloud per spostare oggetti fuori dal sistema StorageGRID, è necessario esaminare le considerazioni relative alla configurazione e all'utilizzo dei pool di storage cloud.

Considerazioni generali

- In generale, lo storage di archiviazione cloud, come Amazon S3 Glacier o Azure Blob, è un luogo conveniente per memorizzare i dati degli oggetti. Tuttavia, i costi per recuperare i dati dallo storage di archiviazione cloud sono relativamente elevati. Per ottenere il costo complessivo più basso, è necessario considerare quando e con quale frequenza accedere agli oggetti nel Cloud Storage Pool. L'utilizzo di un Cloud Storage Pool è consigliato solo per i contenuti ai quali si prevede di accedere con frequenza limitata.
- Non utilizzare i Cloud Storage Pools per oggetti che sono stati acquisiti dai client Swift. Swift non supporta le richieste DI ripristino POST-oggetto, pertanto StorageGRID non sarà in grado di recuperare oggetti Swift che sono stati trasferiti allo storage S3 Glacier o al Tier di archiviazione dello storage Blob Azure. L'emissione di una richiesta Swift GET Object per recuperare questi oggetti non avrà esito positivo (403 proibita).
- L'utilizzo dei pool di storage cloud con FabricPool non è supportato a causa della latenza aggiunta per recuperare un oggetto dalla destinazione del pool di storage cloud.

Informazioni necessarie per creare un pool di storage cloud

Prima di creare un Cloud Storage Pool, è necessario creare il bucket S3 esterno o il container di storage Azure Blob esterno da utilizzare per il Cloud Storage Pool. Quindi, quando si crea il pool di storage cloud in StorageGRID, è necessario specificare le seguenti informazioni:

- Il tipo di provider: Storage Amazon S3 o Azure Blob.
- Se si seleziona Amazon S3, specificare se il Cloud Storage Pool deve essere utilizzato con l'AWS Secret Region (**CAP (C2S Access Portal)**).
- Il nome esatto del bucket o del container.
- L'endpoint del servizio doveva accedere al bucket o al container.
- L'autenticazione necessaria per accedere al bucket o al container:
 - **S3**: Facoltativamente, un ID della chiave di accesso e una chiave di accesso segreta.
 - **C2S**: L'URL completo per ottenere le credenziali temporanee dal server CAP; un certificato CA del server, un certificato client, una chiave privata per il certificato client e, se la chiave privata è crittografata, la passphrase per la decrittografia.
 - **Azure Blob storage**: Un nome account e una chiave account. Queste credenziali devono disporre dell'autorizzazione completa per il container.
- Facoltativamente, un certificato CA personalizzato per verificare le connessioni TLS al bucket o al container.

Considerazioni sulle porte utilizzate per i pool di cloud storage

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 storage del sistema. È necessario assicurarsi che le seguenti porte possano comunicare con il Cloud Storage Pool.

Per impostazione predefinita, i Cloud Storage Pool utilizzano le seguenti porte:

- **80**: Per gli URI endpoint che iniziano con http
- **443**: Per gli URI 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 configurare anche un proxy di storage per consentire l'invio dei messaggi a endpoint esterni, ad esempio un endpoint su Internet.

Considerazioni sui costi

L'accesso allo storage nel cloud utilizzando un Cloud Storage Pool richiede la connettività di rete al cloud. Devi considerare il costo dell'infrastruttura di rete che utilizzerai per accedere al cloud e fornirlo in modo appropriato, in base alla quantità di dati che prevederai di spostare tra StorageGRID e il cloud utilizzando il pool di storage cloud.

Quando StorageGRID si connette all'endpoint esterno del pool di storage nel cloud, invia varie richieste per monitorare la connettività e garantire che possa eseguire le operazioni richieste. Anche se a queste richieste saranno associati costi aggiuntivi, il costo del monitoraggio di un pool di storage cloud dovrebbe essere solo una piccola frazione del costo complessivo di storage degli oggetti in S3 o Azure.

Se si devono spostare gli oggetti da un endpoint esterno del pool di cloud storage a StorageGRID, potrebbero verificarsi costi più significativi. Gli oggetti possono essere spostati di nuovo in StorageGRID in uno dei seguenti casi:

- L'unica copia dell'oggetto si trova in un pool di storage cloud e si decide di memorizzare l'oggetto in StorageGRID. In questo caso, è sufficiente riconfigurare le regole e le policy ILM. Quando si verifica la valutazione ILM, StorageGRID invia più richieste per recuperare l'oggetto dal pool di storage cloud. StorageGRID crea quindi localmente il numero specificato di copie replicate o codificate per la

cancellazione. Una volta spostato di nuovo l'oggetto in StorageGRID, la copia nel pool di storage cloud viene eliminata.

- Gli oggetti vengono persi a causa di un guasto al nodo di storage. Se l'unica copia rimanente di un oggetto si trova in un pool di storage cloud, StorageGRID ripristina temporaneamente l'oggetto e crea una nuova copia sul nodo di storage ripristinato.



Quando gli oggetti vengono spostati di nuovo in StorageGRID da un pool di storage cloud, StorageGRID invia più richieste all'endpoint del pool di storage cloud per ciascun oggetto. Prima di spostare un gran numero di oggetti, contattare il supporto tecnico per ottenere assistenza nella stima dei tempi e dei costi associati.

S3: Autorizzazioni richieste per il bucket Cloud Storage Pool

La policy del bucket per il bucket S3 esterno utilizzato per un pool di storage cloud deve concedere l'autorizzazione StorageGRID per spostare un oggetto nel bucket, ottenere lo stato di un oggetto, ripristinare un oggetto dallo storage Glacier quando richiesto e molto altro ancora. Idealmente, StorageGRID dovrebbe avere un accesso completo al bucket (`s3:*`); tuttavia, se ciò non è possibile, il criterio 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 pool di storage cloud è controllato dalle regole ILM e dalla policy ILM attiva 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 storage che implementa la classe di storage Glacier) è controllata dalla configurazione del ciclo di vita di tale bucket.

Se si desidera eseguire la transizione di oggetti dal Cloud Storage Pool, è necessario creare la configurazione del ciclo di vita appropriata sul bucket S3 esterno e utilizzare una soluzione di storage che implementa la classe di storage Glacier e supporta l'API S3 POST Object Restore.

Ad esempio, supponiamo che tutti gli oggetti spostati da StorageGRID al pool di storage cloud debbano essere trasferiti immediatamente allo storage Amazon S3 Glacier. 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 trasferirebbe tutti gli oggetti bucket al Glacier Amazon S3 il giorno in cui sono stati creati (ovvero il giorno in cui sono stati spostati da StorageGRID al pool di storage cloud).



Quando si configura il ciclo di vita del bucket esterno, non utilizzare mai le azioni **Expiration** per definire quando gli oggetti scadono. Le azioni di scadenza fanno sì che il sistema di storage esterno elimini gli oggetti scaduti. Se in seguito si tenta di accedere a un oggetto scaduto da StorageGRID, l'oggetto eliminato non viene trovato.

Se si desidera trasferire oggetti nel Cloud Storage Pool in S3 Glacier Deep Archive (invece di Amazon S3 Glacier), specificare `<StorageClass>DEEP_ARCHIVE</StorageClass>` nel ciclo di vita del bucket. Tuttavia, tenere presente che non è possibile utilizzare Expedited tier per ripristinare gli oggetti da S3 Glacier Deep Archive.

Azure: Considerazioni per il Tier di accesso

Quando si configura un account di storage Azure, è possibile impostare il Tier di accesso predefinito su Hot o Cool. Quando si crea un account storage da utilizzare con un Cloud Storage Pool, è necessario utilizzare l'hot Tier come Tier predefinito. Anche se StorageGRID imposta immediatamente il Tier per l'archiviazione quando sposta gli oggetti nel pool di storage cloud, l'utilizzo dell'impostazione predefinita di Hot garantisce che non venga addebitata una tariffa per l'eliminazione anticipata degli oggetti rimossi dal Tier Cool prima del minimo di 30 giorni.

Azure: Gestione del ciclo di vita non supportata

Non utilizzare la gestione del ciclo di vita dello storage Azure Blob per il container utilizzato con un pool di storage cloud. Le operazioni del ciclo di vita potrebbero interferire con le operazioni del Cloud Storage Pool.

Informazioni correlate

["Creazione di un pool di storage cloud"](#)

["S3: Specifica dei dettagli di autenticazione per un Cloud Storage Pool"](#)

["C2S S3: Specifica dei dettagli di autenticazione per un Cloud Storage Pool"](#)

["Azure: Specifica dei dettagli di autenticazione per un pool di storage cloud"](#)

Confronto tra Cloud Storage Pools e la replica CloudMirror

Quando si inizia a utilizzare i pool di storage cloud, potrebbe essere utile comprendere le analogie e le differenze tra i pool di storage cloud e il servizio di replica di StorageGRID CloudMirror.

	Pool di cloud storage	Servizio di replica di CloudMirror
Qual è lo scopo principale?	Un Cloud Storage Pool agisce come destinazione di archiviazione. La copia dell'oggetto nel Cloud Storage Pool può essere l'unica copia dell'oggetto oppure può essere una copia aggiuntiva. Ovvero, invece di mantenere due copie on-premise, puoi conservare una sola copia all'interno di StorageGRID e inviarne una copia al pool di storage cloud.	Il servizio di replica CloudMirror consente a un tenant di replicare automaticamente gli oggetti da un bucket in StorageGRID (origine) a un bucket S3 esterno (destinazione). La replica di CloudMirror crea una copia indipendente di un oggetto in un'infrastruttura S3 indipendente.
Come viene configurato?	I pool di cloud storage vengono definiti allo stesso modo dei pool di storage, utilizzando Grid Manager o l'API Grid Management. È possibile selezionare un Cloud Storage Pool come posizione di posizionamento in una regola ILM. Mentre un pool di storage è costituito da un gruppo di nodi di storage, un pool di storage cloud viene definito utilizzando un endpoint remoto S3 o Azure (indirizzo IP, credenziali e così via).	Un utente tenant configura la replica di CloudMirror definendo un endpoint CloudMirror (indirizzo IP, credenziali e così via) utilizzando Tenant Manager o l'API S3. Una volta configurato l'endpoint CloudMirror, qualsiasi bucket di proprietà dell'account tenant può essere configurato per puntare all'endpoint CloudMirror.
Chi è responsabile della sua configurazione?	In genere, un amministratore di rete	In genere, un utente tenant
Qual è la destinazione?	<ul style="list-style-type: none"> • Qualsiasi infrastruttura S3 compatibile (incluso Amazon S3) • Tier Azure Blob Archive 	<ul style="list-style-type: none"> • Qualsiasi infrastruttura S3 compatibile (incluso Amazon S3)
Qual è la causa dello spostamento degli oggetti nella destinazione?	Una o più regole ILM nel criterio ILM attivo. Le regole ILM definiscono gli oggetti che StorageGRID sposta nel pool di storage cloud e quando gli oggetti vengono spostati.	L'atto di inserire un nuovo oggetto in un bucket di origine configurato con un endpoint CloudMirror. Gli oggetti che esistevano nel bucket di origine prima della configurazione del bucket con l'endpoint CloudMirror non vengono replicati, a meno che non vengano modificati.

	Pool di cloud storage	Servizio di replica di CloudMirror
Come vengono recuperati gli oggetti?	Le applicazioni devono effettuare richieste a StorageGRID per recuperare gli oggetti spostati in un pool di storage cloud. Se l'unica copia di un oggetto è stata trasferita allo storage di archiviazione, StorageGRID gestisce il processo di ripristino dell'oggetto in modo che possa essere recuperato.	Poiché la copia mirrorata nel bucket di destinazione è una copia indipendente, le applicazioni possono recuperare l'oggetto inviando richieste a StorageGRID o alla destinazione S3. Si supponga, ad esempio, di utilizzare la replica CloudMirror per eseguire il mirroring degli oggetti in un'organizzazione partner. Il partner può utilizzare le proprie applicazioni per leggere o aggiornare gli oggetti direttamente dalla destinazione S3. Non è necessario utilizzare StorageGRID.
Puoi leggere direttamente dalla destinazione?	No Gli oggetti spostati in un pool di storage cloud vengono gestiti da StorageGRID. Le richieste di lettura devono essere indirizzate a StorageGRID (e StorageGRID sarà responsabile del recupero dal pool di storage cloud).	Sì, perché la copia mirrorata è una copia indipendente.
Cosa succede se un oggetto viene cancellato dall'origine?	L'oggetto viene eliminato anche nel Cloud Storage Pool.	L'azione di eliminazione non viene replicata. Un oggetto cancellato non esiste più nel bucket StorageGRID, ma continua ad esistere nel bucket di destinazione. Allo stesso modo, gli oggetti nel bucket di destinazione possono essere cancellati senza influire sull'origine.
Come si accede agli oggetti dopo un disastro (sistema StorageGRID non operativo)?	I nodi StorageGRID guasti devono essere ripristinati. Durante questo processo, le copie degli oggetti replicati potrebbero essere ripristinate utilizzando le copie nel Cloud Storage Pool.	Le copie degli oggetti nella destinazione CloudMirror sono indipendenti da StorageGRID, pertanto è possibile accedervi direttamente prima del ripristino dei nodi StorageGRID.

Informazioni correlate

["Amministrare StorageGRID"](#)

Creazione di un pool di storage cloud

Quando crei un pool di storage cloud, specifica il nome e la posizione del bucket o del container esterno che StorageGRID utilizzerà per memorizzare gli oggetti, il tipo di provider cloud (Amazon S3 o Azure Blob Storage) e le informazioni necessarie per accedere al bucket o al container esterno da parte di StorageGRID.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

- Devi aver esaminato le linee guida per la configurazione dei Cloud Storage Pools.
- Il bucket o il container esterno a cui fa riferimento il Cloud Storage Pool deve esistere.
- È necessario disporre di tutte le informazioni di autenticazione necessarie per accedere al bucket o al container.

A proposito di questa attività

Un Cloud Storage Pool specifica un singolo bucket S3 esterno o un container di storage Azure Blob. StorageGRID convalida il pool di storage cloud non appena viene salvato, quindi devi assicurarti che il bucket o il container specificato nel pool di storage cloud esista e sia raggiungibile.

Fasi

1. Selezionare **ILM > Storage Pools**.

Viene visualizzata la pagina Storage Pools. Questa pagina include due sezioni: Pool di storage e pool di storage cloud.

Storage Pools

Storage Pools

A storage pool is a logical group of Storage Nodes or Archive Nodes and is used in ILM rules to determine where object data is stored.

+ Create Edit Remove View Details

Name	Used Space	Free Space	Total Capacity	ILM Usage
All Storage Nodes	1.10 MB	102.90 TB	102.90 TB	Used in 1 ILM rule

Displaying 1 storage pool.

Cloud Storage Pools

You can add Cloud Storage Pools to ILM rules to store objects outside of the StorageGRID system. A Cloud Storage Pool defines how to access the external bucket or container where objects will be stored.

+ Create Edit Remove Clear Error

No Cloud Storage Pools found.

2. Nella sezione Cloud Storage Pools della pagina, fare clic su **Create** (Crea).

Viene visualizzata la finestra di dialogo Create Cloud Storage Pool (Crea pool di storage cloud).

Create Cloud Storage Pool

Display Name

Provider Type

Bucket or Container

Cancel Save

3. Inserire le seguenti informazioni:

Campo	Descrizione
Nome visualizzato	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 provider	<p>Quale cloud provider utilizzerai per questo Cloud Storage Pool:</p> <ul style="list-style-type: none"> • Amazon S3 (selezionare questa opzione per un pool di storage cloud S3 o C2S S3) • Azure Blob Storage <p>Nota: quando si seleziona un tipo di provider, nella parte inferiore della pagina vengono visualizzate le sezioni Service Endpoint, Authentication e Server Verification.</p>
Bucket o container	Il nome del bucket S3 esterno o del container Azure creato per il Cloud Storage Pool. Il nome specificato qui deve corrispondere esattamente al nome del bucket o del container, altrimenti la creazione del Cloud Storage Pool non avrà esito positivo. Non è possibile modificare questo valore dopo il salvataggio del Cloud Storage Pool.

4. Completare le sezioni Service Endpoint, Authentication e Server Verification della pagina, in base al tipo di provider selezionato.
- ["S3: Specifica dei dettagli di autenticazione per un Cloud Storage Pool"](#)
 - ["C2S S3: Specifica dei dettagli di autenticazione per un Cloud Storage Pool"](#)
 - ["Azure: Specifica dei dettagli di autenticazione per un pool di storage cloud"](#)

S3: Specifica dei dettagli di autenticazione per un Cloud Storage Pool

Quando si crea un Cloud Storage Pool per S3, è necessario selezionare il tipo di autenticazione richiesto per l'endpoint del Cloud Storage Pool. È possibile specificare Anonymous o immettere un ID della chiave di accesso e una chiave di accesso segreta.

Di cosa hai bisogno

- Devi aver inserito le informazioni di base per il Cloud Storage Pool e specificato **Amazon S3** come tipo di provider.

Create Cloud Storage Pool

Display Name ⓘ S3 Cloud Storage Pool

Provider Type ⓘ Amazon S3 ▼

Bucket or Container ⓘ my-s3-bucket

Service Endpoint

Protocol ⓘ HTTP HTTPS

Hostname ⓘ example.com or 0.0.0.0

Port (optional) ⓘ 443

Authentication

Authentication Type ⓘ ▼

Server Verification

Certificate Validation ⓘ Use operating system CA certificate ▼

Cancel

Save

- Se si utilizza l'autenticazione della chiave di accesso, è necessario conoscere l'ID della chiave di accesso e la chiave di accesso segreta per il bucket S3 esterno.

Fasi

1. Nella sezione **Service Endpoint**, fornire le seguenti informazioni:
 - a. Selezionare il protocollo da utilizzare per la connessione al Cloud Storage Pool.
Il protocollo predefinito è HTTPS.
 - b. Inserire il nome host del server o l'indirizzo IP del Cloud Storage Pool.

Ad esempio:



Non includere il nome del bucket in questo campo. Il nome del bucket viene incluso nel campo **bucket o container**.

- a. Facoltativamente, specificare la porta da utilizzare per la connessione al Cloud Storage Pool.

Lasciare vuoto questo campo per utilizzare la porta predefinita: Porta 443 per HTTPS o porta 80 per HTTP.

2. Nella sezione **Authentication**, selezionare il tipo di autenticazione richiesto per l'endpoint Cloud Storage Pool.

Opzione	Descrizione
Chiave di accesso	Per accedere al bucket Cloud Storage Pool sono necessari un ID della chiave di accesso e una chiave di accesso segreta.
Anonimo	Tutti hanno accesso al bucket Cloud Storage Pool. Non sono richiesti un ID della chiave di accesso e una chiave di accesso segreta.
CAP (portale di accesso C2S)	Utilizzato solo per C2S S3. Passare a. "C2S S3: Specifica dei dettagli di autenticazione per un Cloud Storage Pool" .

3. Se si seleziona Access Key (chiave di accesso), immettere le seguenti informazioni:

Opzione	Descrizione
ID chiave di accesso	L'ID della chiave di accesso per l'account proprietario del bucket esterno.
Chiave di accesso segreta	La chiave di accesso segreta associata.

4. Nella sezione verifica server, selezionare il metodo da utilizzare per convalidare il certificato per le connessioni TLS al Cloud Storage Pool:

Opzione	Descrizione
Utilizzare il certificato CA del sistema operativo	Utilizzare i certificati CA predefiniti installati nel sistema operativo per proteggere le connessioni.
USA certificato CA personalizzato	Utilizzare un certificato CA personalizzato. Fare clic su Select New (Seleziona nuovo) e caricare il certificato CA con codifica PEM.
Non verificare il certificato	Il certificato utilizzato per la connessione TLS non viene verificato.

5. Fare clic su **Save** (Salva).

Quando si salva un pool di storage cloud, StorageGRID esegue le seguenti operazioni:

- Convalida l'esistenza del bucket e dell'endpoint del servizio e la possibilità di raggiungerli utilizzando le credenziali specificate.
- Scrive un file di marker nel bucket per identificare il bucket come un Cloud Storage Pool. Non rimuovere mai questo file, denominato `x-ntap-sgws-cloud-pool-uuid`.

Se la convalida del Cloud Storage Pool non riesce, viene visualizzato un messaggio di errore che spiega perché la convalida non è riuscita. Ad esempio, se si verifica un errore nel certificato o se il bucket specificato non esiste già, potrebbe essere visualizzato un errore.

! Error

422: Unprocessable Entity

Validation failed. Please check the values you entered for errors.

Cloud Pool test failed. Could not create or update Cloud Pool. Error from endpoint: NoSuchBucket: The specified bucket does not exist. status code: 404, request id: 4211567681, host id:

OK

Consultare le istruzioni per la risoluzione dei problemi relativi ai pool di storage cloud, risolvere il problema, quindi provare a salvare nuovamente il pool di storage cloud.

Informazioni correlate

["Risoluzione dei problemi relativi ai pool di storage cloud"](#)

C2S S3: Specifica dei dettagli di autenticazione per un Cloud Storage Pool

Per utilizzare il servizio servizi cloud commerciali (C2S) S3 come pool di storage cloud, è necessario configurare il portale di accesso C2S (CAP) come tipo di autenticazione, in modo che StorageGRID possa richiedere credenziali temporanee per accedere al bucket S3 nel proprio account C2S.

Di cosa hai bisogno

- Devi aver inserito le informazioni di base per un pool di storage cloud Amazon S3, incluso l'endpoint del servizio.
- È necessario conoscere l'URL completo che StorageGRID utilizzerà per ottenere le credenziali temporanee dal server CAP, inclusi tutti i parametri API obbligatori e facoltativi assegnati all'account C2S.
- È necessario disporre di un certificato CA del server emesso da un'autorità di certificazione governativa (CA) appropriata. StorageGRID utilizza questo certificato per verificare l'identità del server CAP. Il certificato CA del server deve utilizzare la codifica PEM.
- È necessario disporre di un certificato client emesso da un'autorità di certificazione governativa (CA) appropriata. StorageGRID utilizza questo certificato per identificare se stesso nel server CAP. Il certificato client deve utilizzare la codifica PEM e deve avere ottenuto l'accesso all'account C2S.
- È necessario disporre di una chiave privata con codifica PEM per il certificato client.
- Se la chiave privata per il certificato client è crittografata, è necessario disporre della passphrase per decrittografare il certificato.

Fasi

1. Nella sezione **Authentication**, selezionare **CAP (C2S Access Portal)** dall'elenco a discesa **Authentication Type** (tipo di autenticazione).

Vengono visualizzati i campi DI autenticazione CAP C2S.

Create Cloud Storage Pool

Display Name ⓘ S3 Cloud Storage Pool

Provider Type ⓘ Amazon S3 ▼

Bucket or Container ⓘ my-s3-bucket

Service Endpoint

Protocol ⓘ HTTP HTTPS

Hostname ⓘ s3-aws-region.amazonaws.com

Port (optional) ⓘ 443

Authentication

Authentication Type ⓘ CAP (C2S Access Portal) ▼

Temporary Credentials URL ⓘ https://example.com/CAP/api/v1/credentials?agency=my

Server CA Certificate ⓘ

Client Certificate ⓘ

Client Private Key ⓘ

Client Private Key Passphrase (optional) ⓘ

Server Verification

Certificate Validation ⓘ Use operating system CA certificate ▼

Cancel

Save

2. Fornire le seguenti informazioni:

- a. Per **URL 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 all'account C2S.
- b. Per **certificato CA server**, fare clic su **Seleziona nuovo** e caricare il certificato CA con codifica PEM che StorageGRID utilizzerà per verificare il server CAP.
- c. Per **certificato client**, fare clic su **Seleziona nuovo** e caricare il certificato con codifica PEM che StorageGRID utilizzerà per identificarsi nel server CAP.
- d. Per **Client Private Key**, fare clic su **Select New** (Seleziona nuovo) e caricare la chiave privata con codifica PEM per il certificato del client.

Se la chiave privata è crittografata, è necessario utilizzare il formato tradizionale. (Il formato crittografato PKCS n. 8 non è supportato).

- e. Se la chiave privata del client è crittografata, immettere la passphrase per la decrittografia della chiave privata del client. In caso contrario, lasciare vuoto il campo **Client Private Key Passphrase** (Password chiave privata client).

3. Nella sezione verifica server, fornire le seguenti informazioni:

- a. Per **convalida certificato**, selezionare **Usa certificato CA personalizzato**.
- b. Fare clic su **Select New** (Seleziona nuovo) e caricare il certificato CA con codifica PEM.

4. Fare clic su **Save** (Salva).

Quando si salva un pool di storage cloud, StorageGRID esegue le seguenti operazioni:

- Convalida l'esistenza del bucket e dell'endpoint del servizio e la possibilità di raggiungerli utilizzando le credenziali specificate.
- Scrive un file di marker nel bucket per identificare il bucket come un Cloud Storage Pool. Non rimuovere mai questo file, denominato `x-ntap-sgws-cloud-pool-uuid`.

Se la convalida del Cloud Storage Pool non riesce, viene visualizzato un messaggio di errore che spiega perché la convalida non è riuscita. Ad esempio, se si verifica un errore nel certificato o se il bucket specificato non esiste già, potrebbe essere visualizzato un errore.

! Error

422: Unprocessable Entity

Validation failed. Please check the values you entered for errors.

Cloud Pool test failed. Could not create or update Cloud Pool. Error from endpoint: NoSuchBucket:
The specified bucket does not exist. status code: 404, request id: 4211567681, host id:

OK

Consultare le istruzioni per la risoluzione dei problemi relativi ai pool di storage cloud, risolvere il problema, quindi provare a salvare nuovamente il pool di storage cloud.

Informazioni correlate

Azure: Specifica dei dettagli di autenticazione per un pool di storage cloud

Quando si crea un pool di storage cloud per lo storage Azure Blob, è necessario specificare un nome account e una chiave account per il container esterno che StorageGRID utilizzerà per memorizzare gli oggetti.

Di cosa hai bisogno

- È necessario aver inserito le informazioni di base per il Cloud Storage Pool e specificato **Azure Blob Storage** come tipo di provider. Nel campo **Authentication Type** (tipo di autenticazione) viene visualizzato **Shared Key** (chiave condivisa).

Create Cloud Storage Pool

Display Name	<input type="text" value="Azure Cloud Storage Pool"/>
Provider Type	<input type="text" value="Azure Blob Storage"/>
Bucket or Container	<input type="text" value="my-azure-container"/>

Service Endpoint

URI	<input type="text" value="https://myaccount.blob.core.windows.net"/>
-----	--

Authentication

Authentication Type	Shared Key
Account Name	<input type="text"/>
Account Key	<input type="text"/>

Server Verification

Certificate Validation	<input type="text" value="Use operating system CA certificate"/>
------------------------	--

- È necessario conoscere l'URI (Uniform Resource Identifier) utilizzato per accedere al container di storage Blob utilizzato per il Cloud Storage Pool.
- È necessario conoscere il nome dell'account di storage e la chiave segreta. È possibile utilizzare il portale Azure per trovare questi valori.

Fasi

1. Nella sezione **Service Endpoint**, immettere l'URI (Uniform Resource Identifier) utilizzato per accedere al container di storage Blob utilizzato per il Cloud Storage Pool.

Specificare l'URI in uno dei seguenti formati:

- `https://host:port`
- `http://host:port`

Se non si specifica una porta, per impostazione predefinita viene utilizzata la porta 443 per gli URI HTTPS e la porta 80 per gli URI HTTP. + + + **URI di esempio per Azure Blob Storage Container:**

`https://myaccount.blob.core.windows.net`

2. Nella sezione **Authentication**, fornire le seguenti informazioni:
 - a. Per **Nome account**, immettere il nome dell'account di storage Blob proprietario del container di servizi esterno.
 - b. Per **account Key**, immettere la chiave segreta per l'account di storage Blob.



Per gli endpoint Azure, è necessario utilizzare l'autenticazione con chiave condivisa.

3. Nella sezione **verifica server**, selezionare il metodo da utilizzare per validare il certificato per le connessioni TLS al Cloud Storage Pool:

Opzione	Descrizione
Utilizzare il certificato CA del sistema operativo	Utilizzare i certificati CA predefiniti installati nel sistema operativo per proteggere le connessioni.
USA certificato CA personalizzato	Utilizzare un certificato CA personalizzato. Fare clic su Select New (Seleziona nuovo) e caricare il certificato con codifica PEM.
Non verificare il certificato	Il certificato utilizzato per la connessione TLS non viene verificato.

4. Fare clic su **Save** (Salva).

Quando si salva un pool di storage cloud, StorageGRID esegue le seguenti operazioni:

- Convalida l'esistenza del container e dell'URI e ne consente l'accesso utilizzando le credenziali specificate.
- Scrive un file marker nel container per identificarlo come pool di storage cloud. Non rimuovere mai questo file, denominato `x-ntap-sgws-cloud-pool-uuid`.

Se la convalida del Cloud Storage Pool non riesce, viene visualizzato un messaggio di errore che spiega perché la convalida non è riuscita. Ad esempio, se si verifica un errore nel certificato o se il contenitore specificato non esiste già, potrebbe essere visualizzato un errore.

Consultare le istruzioni per la risoluzione dei problemi relativi ai pool di storage cloud, risolvere il problema, quindi provare a salvare nuovamente il pool di storage cloud.

Informazioni correlate

["Risoluzione dei problemi relativi ai pool di storage cloud"](#)

Modifica di un pool di storage cloud

È possibile modificare un Cloud Storage Pool per modificarne il nome, l'endpoint del servizio o altri dettagli; tuttavia, non è possibile modificare il bucket S3 o il container Azure per un Cloud Storage Pool.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.
- Devi aver esaminato le linee guida per la configurazione dei Cloud Storage Pools.

Fasi

1. Selezionare **ILM > Storage Pools**.

Viene visualizzata la pagina Storage Pools. La tabella Cloud Storage Pools elenca i Cloud Storage Pools esistenti.

Cloud Storage Pools

You can add Cloud Storage Pools to ILM rules to store objects outside of the StorageGRID system. A Cloud Storage Pool defines how to access the external bucket or container where objects will be stored.

Pool Name	URI	Pool Type	Container	Used in ILM Rule	Last Error
<input checked="" type="radio"/> azure-endpoint	https://storagegrid.blob.core.windows.net	azure	azure-3	✓	
<input type="radio"/> s3-endpoint	https://s3.amazonaws.com	s3	s3-1	✓	

Displaying 2 pools.

2. Selezionare il pulsante di opzione per il Cloud Storage Pool che si desidera modificare.
3. Fare clic su **Edit** (Modifica).
4. Se necessario, modificare il nome visualizzato, l'endpoint del servizio, le credenziali di autenticazione o il metodo di convalida del certificato.



Non è possibile modificare il tipo di provider, il bucket S3 o il container Azure per un Cloud Storage Pool.

Se in precedenza è stato caricato un certificato server o client, è possibile selezionare **Visualizza attuale** per rivedere il certificato attualmente in uso.

5. Fare clic su **Save** (Salva).

Quando si salva un pool di storage cloud, StorageGRID convalida l'esistenza del bucket o del container e dell'endpoint del servizio e che è possibile raggiungerli utilizzando le credenziali specificate.

Se la convalida del Cloud Storage Pool non riesce, viene visualizzato un messaggio di errore. Ad esempio, se si verifica un errore del certificato, potrebbe essere visualizzato un errore.

Consultare le istruzioni per la risoluzione dei problemi relativi ai pool di storage cloud, risolvere il problema, quindi provare a salvare nuovamente il pool di storage cloud.

Informazioni correlate

["Considerazioni per i Cloud Storage Pools"](#)

["Risoluzione dei problemi relativi ai pool di storage cloud"](#)

Rimozione di un pool di storage cloud

È possibile rimuovere un Cloud Storage Pool che non viene utilizzato in una regola ILM e che non contiene dati oggetto.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.
- Hai confermato che il bucket S3 o il container Azure non contiene oggetti. Si verifica un errore se si tenta di rimuovere un Cloud Storage Pool se contiene oggetti. Consulta "risoluzione dei problemi relativi ai pool di storage cloud".



Quando crei un pool di storage cloud, StorageGRID scrive un file di marker nel bucket o nel container per identificarlo come pool di storage cloud. Non rimuovere questo file, denominato `x-ntap-sgws-cloud-pool-uuid`.

- Sono già state rimosse le regole ILM che potrebbero aver utilizzato il pool.

Fasi

1. Selezionare **ILM > Storage Pools**.

Viene visualizzata la pagina Storage Pools.

2. Selezionare il pulsante di opzione per un Cloud Storage Pool che non è attualmente utilizzato in una regola ILM.

Non è possibile rimuovere un pool di storage cloud se utilizzato in una regola ILM. Il pulsante **Remove** (Rimuovi) è disattivato.

Cloud Storage Pools

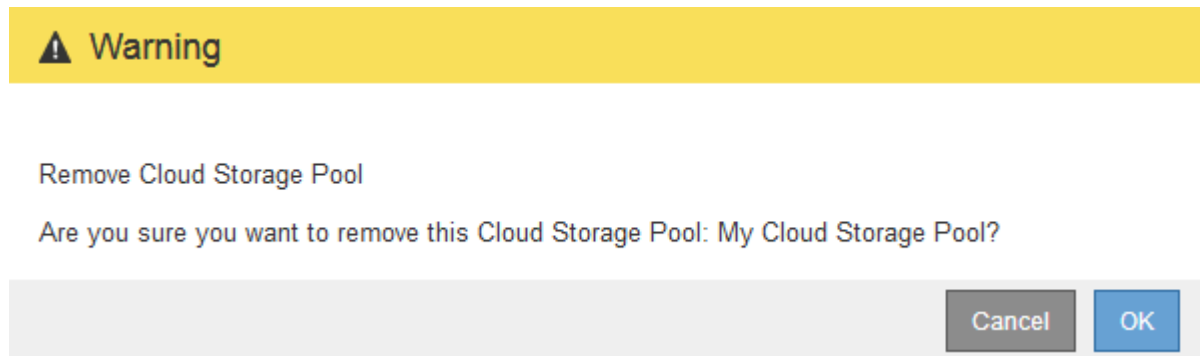
You can add Cloud Storage Pools to ILM rules to store objects outside of the StorageGRID system. A Cloud Storage Pool defines how to access the external bucket or container where objects will be stored.

Pool Name	URI	Pool Type	Container	Used in ILM Rule	Last Error
<input checked="" type="radio"/> azure-endpoint	https://storagegrid.blob.core.windows.net	azure	azure-3	✓	
<input type="radio"/> s3-endpoint	https://s3.amazonaws.com	s3	s3-1	✓	

Displaying 2 pools.

3. Fare clic su **Rimuovi**.

Viene visualizzato un avviso di conferma.



4. Fare clic su **OK**.

Il Cloud Storage Pool viene rimosso.

Informazioni correlate

["Risoluzione dei problemi relativi ai pool di storage cloud"](#)

Risoluzione dei problemi relativi ai pool di storage cloud

Se si verificano errori durante la creazione, la modifica o l'eliminazione di un pool di storage cloud, attenersi alla procedura di risoluzione dei problemi riportata di seguito per risolvere il problema.

Determinare se si è verificato un errore

StorageGRID esegue una semplice verifica dello stato di salute di ogni pool di storage cloud una volta al minuto per garantire che sia possibile accedere al pool di storage cloud e che funzioni correttamente. Se il controllo dello stato di salute rileva un problema, viene visualizzato un messaggio nella colonna Last Error (ultimo errore) della tabella Cloud Storage Pools (pool di storage cloud) della pagina Storage Pools (pool di storage).

La tabella mostra l'errore più recente rilevato per ciascun Cloud Storage Pool e indica quanto tempo fa si è verificato l'errore.

Cloud Storage Pools

You can add Cloud Storage Pools to ILM rules to store objects outside of the StorageGRID system. A Cloud Storage Pool defines how to access the external bucket or container where objects will be stored.

	Pool Name	URI	Pool Type	Container	Used in ILM Rule	Last Error
<input checked="" type="radio"/>	S3	10.96.106.142:18082	s3	s3	✓	Endpoint failure: DC2-S1-106-147: Could not create or update Cloud Storage Pool. Error from endpoint: RequestError: send request failed caused by: Get https://10.96.106.142:18082/s3-targetbucket/x-ntap-sgws-cloud-pool-uuid: net/http: request canceled while waiting for connection (Client.Timeout exceeded while awaiting headers) 8 minutes ago
<input type="radio"/>	Azure	http://pboerkoe@10.96.100.254:10000/d/evstoreaccount1	azure	azure	✓	

Displaying 2 pools.

Inoltre, un avviso di **errore di connettività del Cloud Storage Pool** viene attivato se il controllo dello stato di salute rileva che uno o più nuovi errori del Cloud Storage Pool si sono verificati negli ultimi 5 minuti. Se si

riceve una notifica via email per questo avviso, accedere alla pagina Storage Pool (selezionare **ILM > Storage Pools**), esaminare i messaggi di errore nella colonna Last Error (ultimo errore) e consultare le linee guida per la risoluzione dei problemi riportate di seguito.

Verifica della risoluzione di un errore

Dopo aver risolto eventuali problemi sottostanti, è possibile determinare se l'errore è stato risolto. Dalla pagina Cloud Storage Pool, selezionare il pulsante di opzione per l'endpoint e fare clic su **Clear Error**. Un messaggio di conferma indica che StorageGRID ha eliminato l'errore per il pool di storage cloud.

Error successfully cleared. This error might reappear if the underlying problem is not resolved.



Se il problema sottostante è stato risolto, il messaggio di errore non viene più visualizzato. Tuttavia, se il problema sottostante non è stato risolto (o se si verifica un errore diverso), il messaggio di errore viene visualizzato nella colonna Last Error (ultimo errore) entro pochi minuti.

Errore: Questo Cloud Storage Pool contiene contenuti imprevisti

Questo errore potrebbe verificarsi quando si tenta di creare, modificare o eliminare un pool di storage cloud. Questo errore si verifica se il bucket o il container include `x-ntap-sgws-cloud-pool-uuid` Il file marker, ma non ha l'UUID previsto.

In genere, questo errore viene visualizzato solo se si crea un nuovo pool di storage cloud e un'altra istanza di StorageGRID sta già utilizzando lo stesso pool di storage cloud.

Per risolvere il problema, attenersi alla seguente procedura:

- Assicurati che nessuno nella tua organizzazione stia utilizzando questo Cloud Storage Pool.
- Eliminare `x-ntap-sgws-cloud-pool-uuid` E provare a configurare nuovamente il Cloud Storage Pool.

Errore: Impossibile creare o aggiornare il Cloud Storage Pool. Errore dall'endpoint

Questo errore potrebbe verificarsi quando si tenta di creare o modificare un pool di storage cloud. Questo errore indica che alcuni problemi di connettività o configurazione impediscono a StorageGRID di scrivere nel pool di storage cloud.

Per risolvere il problema, esaminare il messaggio di errore dall'endpoint.

- Se il messaggio di errore contiene `Get url: EOF`, Verificare che l'endpoint del servizio utilizzato per il Cloud Storage Pool non utilizzi il protocollo HTTP per un container o 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 storage di accedere all'endpoint del servizio utilizzato per il Cloud Storage Pool.
- Per tutti gli altri messaggi di errore degli endpoint, provare una o più delle seguenti soluzioni:
 - Creare un container o bucket esterno con lo stesso nome immesso per il Cloud Storage Pool e provare a salvare di nuovo il nuovo Cloud Storage Pool.
 - Correggere il nome del container o bucket specificato per il Cloud Storage Pool e provare a salvare di nuovo il nuovo Cloud Storage Pool.

Errore: Impossibile analizzare il certificato CA

Questo errore potrebbe verificarsi quando si tenta di creare o modificare un pool di storage cloud. L'errore si verifica se StorageGRID non ha potuto analizzare il certificato inserito durante la configurazione del pool di storage cloud.

Per correggere il problema, controllare il certificato CA fornito per eventuali problemi.

Errore: Impossibile trovare un pool di storage cloud con questo ID

Questo errore potrebbe verificarsi quando si tenta di modificare o eliminare un pool di storage cloud. Questo errore si verifica se l'endpoint restituisce una risposta 404, il che può significare una delle seguenti:

- Le credenziali utilizzate per il 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 marker.

Provare una o più delle seguenti operazioni per risolvere il problema:

- Verificare che l'utente associato alla chiave di accesso configurata disponga delle autorizzazioni necessarie.
- Modificare il Cloud Storage Pool con le credenziali che dispongono delle autorizzazioni necessarie.
- Se le autorizzazioni sono corrette, contattare l'assistenza.

Errore: Impossibile controllare il contenuto del Cloud Storage Pool. Errore dall'endpoint

Questo errore potrebbe verificarsi quando si tenta di eliminare un pool di storage cloud. Questo errore indica che un problema di connettività o configurazione impedisce a StorageGRID di leggere il contenuto del bucket del pool di storage cloud.

Per risolvere il problema, esaminare il messaggio di errore dall'endpoint.

Errore: Gli oggetti sono già stati posizionati in questo bucket

Questo errore potrebbe verificarsi quando si tenta di eliminare un pool di storage cloud. Non è possibile eliminare un Cloud Storage Pool se contiene dati spostati 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.

Provare una o più delle seguenti operazioni per risolvere il problema:

- Seguire le istruzioni per lo spostamento degli oggetti in StorageGRID in "ciclo di vita di un oggetto pool di storage cloud".
- Se si è certi che ILM non abbia inserito gli oggetti rimanenti nel Cloud Storage Pool, eliminarli manualmente dal bucket.



Non eliminare mai manualmente oggetti da un Cloud Storage Pool che potrebbe essere stato collocato in tale posizione da ILM. Se in un secondo momento si tenta di accedere a un oggetto eliminato manualmente da StorageGRID, l'oggetto eliminato non viene trovato.

Errore: Il proxy ha rilevato un errore esterno durante il tentativo di raggiungere il Cloud Storage Pool

Questo errore potrebbe verificarsi se è stato configurato un proxy dello storage non trasparente tra i nodi di storage e l'endpoint S3 esterno utilizzato per il Cloud Storage Pool. 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 o potrebbe esserci un problema di rete esterno.

Provare una o più delle seguenti operazioni per risolvere il problema:

- Verificare le impostazioni del Cloud Storage Pool (**ILM > Storage Pools**).
- Controllare la configurazione di rete del server proxy dello storage.

Informazioni correlate

["Ciclo di vita di un oggetto Cloud Storage Pool"](#)

Configurazione dei profili di codifica Erasure

È possibile configurare i profili di codifica Erasure associando un pool di storage a uno schema di codifica erasure, ad esempio 6+3. Quindi, quando si configurano le istruzioni di posizionamento per una regola ILM, è possibile selezionare il profilo di codifica Erasure. Se un oggetto corrisponde alla regola, i frammenti di dati e parità vengono creati e distribuiti nelle posizioni di storage nel pool di storage in base allo schema di erasure coding.

- ["Creazione di un profilo di codifica Erasure"](#)
- ["Ridenominazione di un profilo di codifica Erasure"](#)
- ["Disattivazione di un profilo di codifica Erasure"](#)

Creazione di un profilo di codifica Erasure

Per creare un profilo di codifica Erasure, associare un pool di storage contenente nodi di storage a uno schema di codifica erasure. Questa associazione determina il numero di dati e di frammenti di parità creati e la posizione in cui il sistema distribuisce tali frammenti.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.
- È necessario aver creato un pool di storage che includa esattamente un sito o un pool di storage che includa tre o più siti. Non sono disponibili schemi di erasure coding per un pool di storage con solo due siti.

A proposito di questa attività

I pool di storage utilizzati nei profili di codifica Erasure devono includere esattamente un sito o tre o più siti. Se si desidera fornire la ridondanza del sito, il pool di storage deve avere almeno tre siti.



È necessario selezionare un pool di storage che contiene nodi di storage. Non è possibile utilizzare i nodi di archiviazione per i dati con codifica erasure.

Fasi

1. Selezionare **ILM > Erasure coding**.

Viene visualizzata la pagina Erasure Coding Profiles.

Erasure Coding Profiles

An Erasure Coding profile determines how many data and parity fragments are created and where those fragments are stored.

To create an Erasure Coding profile, select a [storage pool](#) and an erasure coding scheme. The storage pool must include Storage Nodes from exactly one site or from three or more sites. If you want to provide site redundancy, the storage pool must include nodes from at least three sites.

To deactivate an Erasure Coding profile that you no longer plan to use, first remove it from all ILM rules. Then, if the profile is still associated with object data, wait for those objects to be moved to new locations based on the new rules in the active ILM policy. Depending on the number of objects and the size of your StorageGRID system, it might take weeks or even months for the objects to be moved.

See [Managing objects with information lifecycle management](#) for important details.

+ Create ✎ Rename ⊘ Deactivate


Profile	Status	Storage Pool	Storage Nodes	Sites	Erasure Code	Storage Overhead (%)	Storage Node Redundancy	Site Redundancy
No Erasure Coding profiles found.								


2. Fare clic su **Create** (Crea).

Viene visualizzata la finestra di dialogo Create EC Profile (Crea profilo EC).

Create EC Profile

You cannot change the selected scheme and storage pool after saving the profile.

Profile Name 

Storage Pool 

Cancel Save

3. Immettere un nome univoco per il profilo di codifica Erasure.

I nomi dei profili di erasure coding 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.



Il nome del profilo di codifica Erasure viene aggiunto al nome del pool di storage nelle istruzioni di posizionamento per una regola ILM.

From day store Add Remove

Type Location Copies + x

Erasure Coding profile name →

Storage pool name →

4. Selezionare il pool di storage creato per questo profilo di codifica Erasure.



Se il grid attualmente include un solo sito, non è possibile utilizzare il pool di storage predefinito, tutti i nodi di storage o qualsiasi pool di storage che includa il sito predefinito, tutti i siti. Questo comportamento impedisce che il profilo di codifica Erasure diventi non valido se viene aggiunto un secondo sito.



Se un pool di storage include esattamente due siti, non è possibile utilizzare tale pool di storage per la cancellazione del codice. Non sono disponibili schemi di erasure coding per un pool di storage con due siti.

Quando si seleziona un pool di storage, viene visualizzato l'elenco degli schemi di erasure coding disponibili, in base al numero di nodi e siti di storage nel pool.

Create EC Profile

You cannot change the selected scheme and storage pool after saving the profile.

Profile Name

Storage Pool All 3 Sites ▼

9 Storage Nodes across 3 site(s)

Scheme

	Erasure Code	Storage Overhead (%)	Storage Node Redundancy	Site Redundancy
<input checked="" type="radio"/>	6+3	50%	3	Yes
<input type="radio"/>	2+1	50%	1	Yes
<input type="radio"/>	4+2	50%	2	Yes

Cancel

Save

Per ogni schema di erasure coding disponibile sono elencate le seguenti informazioni:

- **Erasure Code:** Il nome dello schema di erasure coding nel seguente formato: Frammenti di dati + frammenti di parità.
- **Overhead dello storage (%):** Lo storage aggiuntivo richiesto per i frammenti di parità in relazione alle dimensioni dei dati dell'oggetto. Overhead dello storage = numero totale di frammenti di parità / numero totale di frammenti di dati.
- **Ridondanza dei nodi di storage:** Il numero di nodi di storage che possono essere persi pur mantenendo la capacità di recuperare i dati degli oggetti.
- **Ridondanza del sito:** Se il codice di cancellazione selezionato consente di recuperare i dati dell'oggetto in caso di perdita di un sito.

Per supportare la ridondanza del sito, il pool di storage selezionato deve includere più siti, ciascuno con un numero sufficiente di nodi di storage per consentire la perdita di qualsiasi sito. Ad esempio, per supportare la ridondanza del sito utilizzando uno schema di erasure coding 6+3, il pool di storage selezionato deve includere almeno tre siti con almeno tre nodi di storage in ciascun sito.

I messaggi vengono visualizzati nei seguenti casi:

- Il pool di storage selezionato non fornisce ridondanza del sito. Il seguente messaggio è previsto

quando il pool di storage selezionato include un solo sito. È possibile utilizzare questo profilo di codifica Erasure nelle regole ILM per la protezione dai guasti dei nodi.

Scheme

	Erasure Code ?	Storage Overhead (%) ?	Storage Node Redundancy ?	Site Redundancy ?
<input checked="" type="radio"/>	2+1	50%	1	No

The selected storage pool and erasure coding scheme cannot protect object data from loss if a site is lost.

To provide site redundancy, the storage pool must have at least three sites.

- Il pool di storage selezionato non soddisfa i requisiti per qualsiasi schema di erasure coding. Ad esempio, il seguente messaggio è previsto quando il pool di storage selezionato include esattamente due siti. Se si desidera utilizzare la codifica erasure per proteggere i dati degli oggetti, è necessario selezionare un pool di storage con esattamente un sito o un pool di storage con tre o più siti.

Scheme

Erasure Code ?	Storage Overhead (%) ?	Storage Node Redundancy ?	Site Redundancy ?
----------------	------------------------	---------------------------	-------------------

No erasure coding schemes are supported for the selected storage pool because it contains two sites. You must select a storage pool that contains exactly one site or a storage pool that contains at least three sites.

- Il grid include un solo sito ed è stato selezionato il pool di storage predefinito, tutti i nodi di storage o qualsiasi pool di storage che includa il sito predefinito, tutti i siti.

Create EC Profile

You cannot change the selected scheme and storage pool after saving the profile.

Profile Name

Storage Pool

3 Storage Nodes across 1 site(s)

Scheme

Erasure Code	Storage Overhead (%)	Storage Node Redundancy	Site Redundancy
--------------	----------------------	-------------------------	-----------------

No erasure coding schemes are available for the selected storage pool. The storage pool includes the **All Sites** site, so it cannot be used in an Erasure Coding profile for a one-site grid.

Cancel

Save

- Lo schema di erasure coding e il pool di storage selezionati si sovrappongono a un altro profilo di codifica Erasure.

Create EC Profile

You cannot change the selected scheme and storage pool after saving the profile.

Profile Name

Storage Pool

9 Storage Nodes across 3 site(s)

Scheme

	Erasure Code	Storage Overhead (%)	Storage Node Redundancy	Site Redundancy
<input type="radio"/>	6+3	50%	3	Yes
<input checked="" type="radio"/>	2+1	50%	1	Yes
<input type="radio"/>	4+2	50%	2	Yes

The selected storage pool and erasure coding scheme overlap an existing Erasure Coding profile. Use caution if you apply this new profile to objects already protected by the other profile. When a new profile is applied to existing erasure-coded objects, entirely new erasure-coded fragments are created, which might cause resource issues.

Cancel

Save

In questo esempio, viene visualizzato un messaggio di avviso perché un altro profilo di codifica Erasure sta utilizzando lo schema 2+1 e il pool di storage per l'altro profilo utilizza anche uno dei siti nel pool di storage All 3 Sites.

Anche se non è possibile creare questo nuovo profilo, è necessario prestare molta attenzione quando si inizia a utilizzarlo nel criterio ILM. Se questo nuovo profilo viene applicato a oggetti con codifica in cancellazione già protetti dall'altro profilo, StorageGRID creerà un set completamente nuovo di frammenti di oggetti. Non riutilizza i frammenti 2+1 esistenti. I problemi relativi alle risorse potrebbero verificarsi quando si esegue la migrazione da un profilo di codifica Erasure all'altro, anche se gli schemi di codifica erasure sono gli stessi.

5. Se sono elencati più schemi di erasure coding, selezionare quello che si desidera utilizzare.

Quando si decide quale schema di erasure coding utilizzare, è necessario bilanciare la tolleranza agli errori (ottenuta con più segmenti di parità) con i requisiti di traffico di rete per le riparazioni (più frammenti equivalgono a più traffico di rete). Ad esempio, quando si decide tra uno schema 4+2 e uno schema 6+3, selezionare lo schema 6+3 se sono richieste ulteriori parità e tolleranza di errore. Selezionare lo schema 4+2 se le risorse di rete sono limitate per ridurre l'utilizzo della rete durante le riparazioni dei nodi.

6. Fare clic su **Save** (Salva).

Ridenominazione di un profilo di codifica Erasure

È possibile rinominare un profilo di codifica Erasure per rendere più evidente la funzione del profilo.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

Fasi

1. Selezionare **ILM > Erasure coding**.

Viene visualizzata la pagina Erasure Coding Profiles. I pulsanti **Rinomina** e **Disattiva** sono entrambi disattivati.

Profile	Status	Storage Pool	Storage Nodes	Sites	Erasure Code	Storage Overhead (%)	Storage Node Redundancy	Site Redundancy
DC1 2-1		DC1	3	1	2+1	50	1	No
DC2 2-1		DC2	3	1	2+1	50	1	No
DC3 2-1		DC3	3	1	2+1	50	1	No
All sites 6-3	Deactivated	All 3 Sites	9	3	6+3	50	3	Yes

2. Selezionare il profilo che si desidera rinominare.

I pulsanti **Rinomina** e **Disattiva** diventano abilitati.

3. Fare clic su **Rinomina**.

Viene visualizzata la finestra di dialogo Rename EC Profile (Rinomina profilo EC).

Rename EC Profile

Profile Name

4. Immettere un nome univoco per il profilo di codifica Erasure.

Il nome del profilo di codifica Erasure viene aggiunto al nome del pool di storage nelle istruzioni di posizionamento per una regola ILM.

From day store

Type Location Erasure Coding profile name

Storage pool name Copies



I nomi dei profili di erasure coding 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. Fare clic su **Save** (Salva).

Disattivazione di un profilo di codifica Erasure

Puoi disattivare un profilo di codifica Erasure se non intendi utilizzarlo e se il profilo non è attualmente utilizzato in nessuna regola ILM.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.
- Devi aver confermato che non sono in corso operazioni di riparazione dei dati codificati per la cancellazione o procedure di decommissionamento. Se si tenta di disattivare un profilo di codifica Erasure mentre è in corso una di queste operazioni, viene visualizzato un messaggio di errore.

A proposito di questa attività

Quando si disattiva un profilo di codifica Erasure, il profilo continua a essere visualizzato nella pagina Erasure Coding Profiles, ma il suo stato è **Disattivato**.

Profile	Status	Storage Pool	Storage Nodes	Sites	Erasure Code	Storage Overhead (%)	Storage Node Redundancy	Site Redundancy
DC1 2-1		DC1	3	1	2+1	50	1	No
DC2 2-1		DC2	3	1	2+1	50	1	No
DC3 2-1		DC3	3	1	2+1	50	1	No
All sites 6-3	Deactivated	All 3 Sites	9	3	6+3	50	3	Yes

Non è più possibile utilizzare un profilo di codifica Erasure disattivato. Un profilo disattivato non viene visualizzato quando si creano le istruzioni di posizionamento per una regola ILM. Non è possibile riattivare un profilo disattivato.

StorageGRID impedisce di disattivare un profilo di codifica Erasure se si verifica una delle seguenti condizioni:

- Il profilo di codifica Erasure è attualmente utilizzato in una regola ILM.
- Il profilo di codifica Erasure non viene più utilizzato in alcuna regola ILM, ma i dati degli oggetti e i frammenti di parità per il profilo esistono ancora.

Fasi

1. Selezionare **ILM > Erasure coding**.

Viene visualizzata la pagina Erasure Coding Profiles. I pulsanti **Rinomina** e **Disattiva** sono entrambi disattivati.


2. Controllare la colonna **Status** per verificare che il profilo di codifica Erasure che si desidera disattivare non sia utilizzato in alcuna regola ILM.

Non è possibile disattivare un profilo di codifica Erasure se utilizzato in qualsiasi regola ILM. Nell'esempio, il profilo **2_1 EC** viene utilizzato in almeno una regola ILM.

Profile	Status	Storage Pool	Storage Nodes	Sites	Erasure Code	Storage Overhead (%)	Storage Node Redundancy	Site Redundancy
2_1 EC Profile	Used In ILM Rule	DC1	3	1	2+1	50	1	No
Site 1 EC Profile	Deactivated	DC1	3	1	2+1	50	1	No

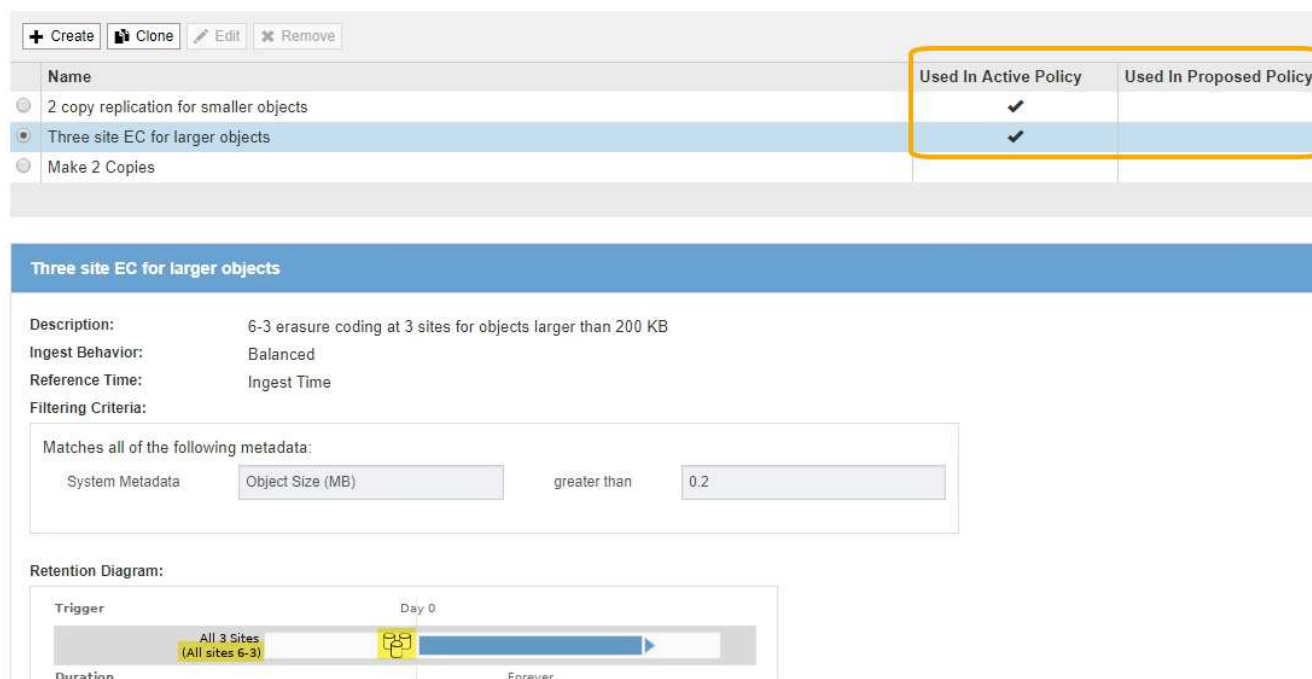
3. Se il profilo viene utilizzato in una regola ILM, attenersi alla seguente procedura:

- Selezionare **ILM > regole**.
- Per ciascuna regola elencata, selezionare il pulsante di opzione e consultare il diagramma di conservazione per determinare se la regola utilizza il profilo di codifica Erasure che si desidera disattivare.

Nell'esempio, la regola EC **tre siti per oggetti più grandi** utilizza un pool di storage denominato **tutti e 3 i siti** e il profilo di codifica Erasure **tutti i siti 6-3**. I profili di erasure coding sono rappresentati da questa icona: 

ILM Rules

Information lifecycle management (ILM) rules determine how and where object data is stored over time. Every object ingested into StorageGRID is evaluated against the ILM rules that make up the active ILM policy. Use this page to manage and view ILM rules. You cannot edit or remove an ILM rule that is used by an active or proposed ILM policy.



- a. Se la regola ILM utilizza il profilo di codifica Erasure che si desidera disattivare, determinare se la regola viene utilizzata nel criterio ILM attivo o in un criterio proposto.

Nell'esempio, la regola EC **tre siti per oggetti più grandi** viene utilizzata nel criterio ILM attivo.

- b. Completare i passaggi aggiuntivi della tabella, in base alla posizione in cui viene utilizzato il profilo di codifica Erasure.

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 necessari passaggi aggiuntivi. Continuare con questa procedura.	<i>nessuno</i>
In una regola ILM che non è mai stata utilizzata in alcun criterio ILM	<p>i. Modificare o eliminare tutte le regole ILM interessate. Se si modifica la regola, rimuovere tutte le posizioni che utilizzano il profilo di codifica Erasure.</p> <p>ii. Continuare con questa procedura.</p>	"Utilizzo delle regole ILM e delle policy 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 attualmente nel criterio ILM attivo	<ol style="list-style-type: none"> i. Clonare il criterio attivo. ii. Rimuovere la regola ILM che utilizza il profilo di codifica Erasure. iii. Aggiungere una o più nuove regole ILM per garantire la protezione degli oggetti. iv. Salvare, simulare e attivare la nuova policy. v. Attendere che il nuovo criterio venga applicato e che gli oggetti esistenti vengano spostati in nuove posizioni in base alle nuove regole aggiunte. <p>Nota: a seconda del numero di oggetti e delle dimensioni del sistema StorageGRID, potrebbero essere necessarie settimane o addirittura mesi per le operazioni ILM per spostare gli oggetti in nuove posizioni, in base alle nuove regole ILM.</p> <p>Sebbene sia possibile disattivare in modo sicuro un profilo di codifica Erasure mentre è ancora associato ai dati, l'operazione di disattivazione non riesce. Se il profilo non è ancora pronto per la disattivazione, viene visualizzato un messaggio di errore.</p> <ol style="list-style-type: none"> vi. Modificare o eliminare la regola rimossa dal criterio. Se si modifica la regola, rimuovere tutte le posizioni che utilizzano il profilo di codifica Erasure. vii. Continuare con questa procedura. 	<ul style="list-style-type: none"> • "Creazione di un criterio ILM" • "Utilizzo delle regole ILM e delle policy ILM"
In una regola ILM attualmente in un criterio ILM proposto	<ol style="list-style-type: none"> i. Modificare la policy proposta. ii. Rimuovere la regola ILM che utilizza il profilo di codifica Erasure. iii. Aggiungere una o più nuove regole ILM per garantire la protezione di tutti gli oggetti. iv. Salvare la policy proposta. v. Modificare o eliminare la regola rimossa dal criterio. Se si modifica la regola, rimuovere tutte le posizioni che utilizzano il profilo di codifica Erasure. vi. Continuare con questa procedura. 	<ul style="list-style-type: none"> • "Creazione di un criterio ILM" • "Utilizzo delle regole ILM e delle policy 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 si trova in una policy ILM storica	i. Modificare o eliminare la regola. Se si modifica la regola, rimuovere tutte le posizioni che utilizzano il profilo di codifica Erasure. (La regola verrà ora visualizzata come regola storica nella policy storica). ii. Continuare con questa procedura.	<ul style="list-style-type: none"> "Utilizzo delle regole ILM e delle policy ILM"

c. Aggiornare la pagina Erasure Coding Profiles 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 selezionare **Disattiva**.

Viene visualizzata la finestra di dialogo Disattiva profilo EC.



5. Se sei sicuro di voler disattivare il profilo, seleziona **Disattiva**.
- 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.
 - Se StorageGRID non è in grado di disattivare il profilo, viene visualizzato un messaggio di errore. Ad esempio, se i dati dell'oggetto sono ancora associati a questo profilo, viene visualizzato un messaggio di errore. Potrebbe essere necessario attendere alcune settimane prima di provare di nuovo il processo di disattivazione.

Configurazione delle regioni (opzionale e solo S3)

Le regole ILM possono filtrare gli oggetti in base alle aree in cui vengono creati i bucket S3, consentendo di memorizzare oggetti da diverse aree in diverse posizioni di storage. Se si desidera utilizzare un'area del bucket S3 come filtro in una regola, è necessario innanzitutto creare le regioni che possono essere utilizzate dai bucket nel sistema.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

A proposito di questa attività

Quando si crea un bucket S3, è possibile specificare che il bucket venga creato in un'area specifica. La specifica di una regione consente al bucket di essere geograficamente vicino ai propri utenti, in modo da ottimizzare la latenza, ridurre al minimo i costi e soddisfare i requisiti normativi.

Quando si crea una regola ILM, è possibile 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 nella regione US-West-2. È quindi possibile specificare che le copie di tali oggetti vengano collocate sui nodi di storage in un sito del data center all'interno di tale regione per ottimizzare la latenza.

Durante la configurazione delle regioni, attenersi alle seguenti linee guida:

- Per impostazione predefinita, tutti i bucket sono considerati come appartenenti alla regione US-East-1.
- È necessario creare le regioni utilizzando Grid Manager prima di poter specificare un'area non predefinita quando si creano i bucket utilizzando l'API Tenant Manager o Tenant Management o con l'elemento di richiesta LocationConstraint per le richieste API S3 PUT bucket. Si verifica un errore se una richiesta PUT bucket utilizza un'area non definita in StorageGRID.
- Quando si crea il bucket S3, è necessario utilizzare il nome esatto della regione. I nomi delle regioni distinguono tra maiuscole e minuscole e devono contenere almeno 2 e non più di 32 caratteri. I caratteri validi sono numeri, lettere e trattini.



EU non è considerato un alias per 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 attualmente utilizzata nel criterio ILM attivo o nel criterio ILM proposto.
- Se la regione utilizzata come filtro avanzato in una regola ILM non è valida, è comunque possibile aggiungere tale regola al criterio proposto. Tuttavia, si verifica un errore se si tenta di salvare o attivare la policy proposta. (Se si utilizza una regione come filtro avanzato in una regola ILM ma si elimina tale regione in un secondo momento o se si utilizza l'API Grid Management per creare una regola e specificare una regione non definita), potrebbe verificarsi un'area non valida.
- Se si elimina una regione dopo averla utilizzata per creare un bucket S3, sarà necessario aggiungerla nuovamente se si desidera utilizzare il filtro avanzato Location Constraint per trovare gli oggetti in tale bucket.

Fasi

1. Selezionare **ILM > regioni**.

Viene visualizzata la pagina regioni, con le regioni attualmente definite. **Regione 1** mostra la regione predefinita, `us-east-1`, che non può essere modificato o rimosso.

Regions (optional and S3 only)

Define any regions you want to use for the Location Constraint advanced filter in ILM rules. Then, use these exact names when creating S3 buckets. (Region names are case sensitive.)

Region 1

Region 2 + x

2. Per aggiungere una regione:

- Fare clic sull'icona di inserimento **+** a destra dell'ultima voce.
- Immettere il nome di una regione che si desidera utilizzare durante la creazione dei bucket S3.

Quando si crea il bucket S3 corrispondente, è necessario utilizzare il nome esatto della regione come elemento di richiesta LocationConstraint.

3. Per rimuovere una regione non utilizzata, fare clic sull'icona di eliminazione **x**.

Se si tenta di rimuovere una regione attualmente utilizzata nel criterio attivo o nel criterio proposto, viene visualizzato un messaggio di errore.

Error

422: Unprocessable Entity

Regions cannot be deleted if they are used by the active or the proposed ILM policy. In use:
us-test-3.

4. Una volta apportate le modifiche, fare clic su **Save** (Salva).

È ora possibile selezionare queste regioni dall'elenco **Location Constraint** nella pagina Advanced Filtering della creazione guidata regole ILM.

Informazioni correlate

["Utilizzo di filtri avanzati nelle regole ILM"](#)

Creazione di 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 regola ILM.

Prima di iniziare

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.
- Se si desidera specificare a quali account tenant si applica questa regola, è necessario disporre dell'autorizzazione account tenant o conoscere l'ID account per ciascun account.
- Se si desidera che la regola filtri gli oggetti sui metadati dell'ultimo accesso, gli ultimi aggiornamenti dell'ora di accesso devono essere attivati dal bucket per S3 o dal container per Swift.
- Se si creano copie replicate, è necessario aver configurato qualsiasi pool di storage o pool di cloud storage che si intende utilizzare.
- Se si stanno creando copie con codice erasure, è necessario aver configurato un profilo di codifica Erasure.
- È necessario avere familiarità con ["opzioni di protezione dei dati per l'acquisizione"](#).
- Se è necessario creare una regola conforme per l'utilizzo con il blocco oggetti S3, è necessario avere familiarità con ["Requisiti per il blocco oggetti S3"](#).



Per creare la regola ILM predefinita per un criterio, utilizzare questa procedura: ["Creazione di una regola ILM predefinita"](#).

A proposito di questa attività

Quando si creano regole ILM:

- Prendere in considerazione la topologia e le configurazioni dello storage del sistema StorageGRID.
- Considerare i tipi di copie di oggetti che si desidera eseguire (replicate o codificate per la cancellazione) e il numero di copie di ciascun oggetto richieste.
- Determinare i tipi di metadati degli oggetti utilizzati nelle applicazioni che si connettono al sistema StorageGRID. Le regole ILM filtrano gli oggetti in base ai metadati.
- Considerare dove si desidera che le copie a oggetti vengano collocate nel tempo.
- Decidere quale opzione utilizzare per l'opzione di protezione dei dati al momento dell'acquisizione (Balanced, Strict o Dual Commit)

Fasi

1. Selezionare **ILM > regole**.

Viene visualizzata la pagina ILM Rules (regole ILM), con la regola stock, fare 2 copie, selezionata.

ILM Rules

Information lifecycle management (ILM) rules determine how and where object data is stored over time. Every object ingested into StorageGRID is evaluated against the ILM rules that make up the active ILM policy. Use this page to manage and view ILM rules. You cannot edit or remove an ILM rule that is used by an active or proposed ILM policy.

+ Create Clone Edit Remove

Name	Used In Active Policy	Used In Proposed Policy
Make 2 Copies	✓	

Make 2 Copies

Ingest Behavior: Dual commit
Reference Time: Ingest Time
Filtering Criteria:
Matches all objects.

Retention Diagram:

The diagram shows two horizontal bars representing storage nodes. The top bar is labeled 'All Storage Nodes' and has a trigger icon at 'Day 0'. The bottom bar is also labeled 'All Storage Nodes' and has a trigger icon at 'Day 0'. Both bars have a duration of 'Forever'.



La pagina regole ILM appare leggermente diversa se l'impostazione globale di blocco oggetti S3 è stata attivata per il sistema StorageGRID. La tabella di riepilogo include una colonna **conforme** e i dettagli della regola selezionata includono un campo **conforme**.

2. Selezionare **Crea**.

Viene visualizzata la fase 1 (Definisci le basi) della procedura guidata Crea regola ILM. La pagina Definisci le basi consente di definire gli oggetti a cui si applica la regola.

Informazioni correlate

["Utilizzare S3"](#)

["USA Swift"](#)

["Configurazione dei profili di codifica Erasure"](#)

["Configurazione dei pool di storage"](#)

["Utilizzo dei Cloud Storage Pools"](#)

["Opzioni di protezione dei dati per l'acquisizione"](#)

["Gestione degli oggetti con S3 Object Lock"](#)

Fase 1 di 3: Definizione delle nozioni di base

Il passaggio 1 (Definisci le basi) della procedura guidata Crea regola ILM consente di definire i filtri di base e avanzati della regola.

A proposito di questa attività

Quando si valuta un oggetto rispetto a una 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 bucket, o filtri avanzati, come la dimensione dell'oggetto o i

metadati dell'utente.

Create ILM Rule Step 1 of 3: Define Basics

Name

Description

Tenant Accounts (optional)

Bucket Name Value

[Advanced filtering...](#) (0 defined)

Fasi

1. Immettere un nome univoco per la regola nel campo **Nome**.

È necessario immettere da 1 a 64 caratteri.

2. Se si desidera, inserire una breve descrizione per la regola nel campo **Descrizione**.

È necessario descrivere lo scopo o la funzione della regola in modo da poterne riconoscere in un secondo momento.

Name

Description

3. Facoltativamente, selezionare uno o più account tenant S3 o Swift a cui si applica questa regola. Se questa regola è applicabile a tutti i tenant, lasciare vuoto questo campo.

Se non si dispone dell'autorizzazione Root Access o dell'autorizzazione Tenant Accounts, non è possibile selezionare i tenant dall'elenco. Immettere invece l'ID tenant o più ID come stringa delimitata da virgole.

4. Facoltativamente, specificare i bucket S3 o i container Swift a cui si applica questa regola.

Se l'opzione **Match All** (corrispondenza totale) è selezionata (impostazione predefinita), la regola si applica a tutti i bucket S3 o a tutti i container Swift.

5. Se si desidera, selezionare **Advanced Filtering** (filtraggio avanzato) per specificare filtri aggiuntivi.

Se non si configura il filtraggio avanzato, la regola si applica a tutti gli oggetti che corrispondono ai filtri di base.



Se questa regola consente di creare copie con codifica in cancellazione, selezionare **Advanced Filtering** (filtraggio avanzato). Quindi, aggiungere il filtro avanzato **Object Size (MB)** e impostarlo su **maggiore di 0.2**. Il filtro delle dimensioni garantisce che gli oggetti di dimensioni pari o inferiori a 2 MB non vengano sottoposti a erasure coding.

6. Selezionare **Avanti**.

Viene visualizzato il punto 2 (definizione delle posizioni).

Informazioni correlate

["Che cos'è il filtraggio delle regole ILM"](#)

["Utilizzo di filtri avanzati nelle regole ILM"](#)

["Fase 2 di 3: Definizione delle posizioni"](#)

Utilizzo di filtri avanzati nelle regole ILM

Il filtraggio avanzato consente di creare regole ILM applicabili solo a oggetti specifici in base ai metadati. Quando si imposta il filtraggio avanzato per una regola, si seleziona il tipo di metadati che si desidera associare, si seleziona un operatore e si specifica un valore di metadati. Quando si valutano gli oggetti, la regola ILM viene applicata solo agli oggetti che hanno metadati corrispondenti al filtro avanzato.

La tabella mostra i tipi di metadati che è possibile specificare nei filtri avanzati, gli operatori che è possibile utilizzare per ogni tipo di metadati e i valori di metadati previsti.

Tipo di metadati	Operatori supportati	Valore dei metadati
Tempo di acquisizione (microsecondi)	<ul style="list-style-type: none">• uguale a• non uguale• inferiore a.• inferiore o uguale a.• maggiore di• maggiore di o uguale a.	Ora e data di acquisizione dell'oggetto. Nota: per evitare problemi di risorse quando si attiva un nuovo criterio ILM, è possibile utilizzare il filtro avanzato Ingest Time in qualsiasi regola che potrebbe modificare la posizione di un gran numero di oggetti esistenti. Impostare Ingest Time (tempo di acquisizione) su un valore maggiore o uguale al tempo approssimativo in cui il nuovo criterio verrà applicato per garantire che gli oggetti esistenti non vengano spostati inutilmente.
Chiave	<ul style="list-style-type: none">• uguale a• non uguale• contiene• non contiene• inizia con• non inizia con• termina con• non finisce con	Tutto o parte di una chiave oggetti S3 o Swift univoca. Ad esempio, è possibile associare gli oggetti che terminano con <code>.txt</code> oppure inizia con <code>test-object/</code> .

Tipo di metadati	Operatori supportati	Valore dei metadati
Tempo di ultimo accesso (microsecondi)	<ul style="list-style-type: none"> • uguale a • non uguale • inferiore a. • inferiore o uguale a. • maggiore di • maggiore di o uguale a. • esiste • non esiste 	<p>Ora e data dell'ultimo recupero dell'oggetto (letto o visualizzato).</p> <p>Nota: se si prevede di utilizzare l'ultimo tempo di accesso come filtro avanzato, è necessario abilitare gli ultimi aggiornamenti dell'ora di accesso per il bucket S3 o il container Swift.</p> <p>"Utilizzo dell'ultimo tempo di accesso nelle regole ILM"</p>
Vincolo di posizione (solo S3)	<ul style="list-style-type: none"> • uguale a • non uguale 	<p>La regione in cui è stato creato un bucket S3. Utilizzare ILM > regioni per definire le regioni visualizzate.</p> <p>Nota: Un valore di US-East-1 corrisponde agli oggetti nei bucket creati nella regione US-East-1 e agli oggetti nei bucket che non hanno alcuna regione specificata.</p> <p>"Configurazione delle regioni (opzionale e solo S3)"</p>
Dimensione oggetto (MB)	<ul style="list-style-type: none"> • uguale a • non uguale • inferiore a. • inferiore o uguale a. • maggiore di • maggiore di o uguale a. 	<p>Dimensione dell'oggetto in MB.</p> <p>Per filtrare le dimensioni degli oggetti inferiori a 1 MB, digitare un valore decimale. Ad esempio, impostare il filtro avanzato dimensione oggetto (MB) su maggiore di 0.2 per qualsiasi regola che crea copie con codifica di cancellazione. Questa impostazione garantisce che l'erasure coding non venga utilizzato per oggetti di dimensioni inferiori o pari a 200 KB.</p> <p>Nota: il tipo di browser e le impostazioni internazionali controllano se è necessario utilizzare un punto o una virgola come separatore decimale.</p>

Tipo di metadati	Operatori supportati	Valore dei metadati
Metadati dell'utente	<ul style="list-style-type: none"> • contiene • termina con • uguale a • esiste • non contiene • non finisce con • non uguale • non esiste • non inizia con • inizia con 	<p>Coppia key-value, dove User Metadata Name è la chiave e User Metadata Value è il valore.</p> <p>Ad esempio, per filtrare gli oggetti con metadati utente di <code>color=blue</code>, specificare <code>color</code> Per User Metadata Name, <code>equals</code> per l'operatore, e. <code>blue</code> Per valore metadati utente.</p> <p>Nota: i nomi dei metadati utente non distinguono tra maiuscole e minuscole; i valori dei metadati utente distinguono tra maiuscole e minuscole.</p>
Tag oggetto (solo S3)	<ul style="list-style-type: none"> • contiene • termina con • uguale a • esiste • non contiene • non finisce con • non uguale • non esiste • non inizia con • inizia con 	<p>Coppia Key-value, dove Object Tag Name è la chiave e Object Tag Value è il valore.</p> <p>Ad esempio, per filtrare gli oggetti che hanno un tag Object 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.</p> <p>Nota: i nomi dei tag degli oggetti e i valori dei tag degli oggetti fanno distinzione tra maiuscole e minuscole. È necessario inserire questi elementi esattamente come sono stati definiti per l'oggetto.</p>

Specifica di più tipi di metadati e valori

Quando si definisce il filtraggio 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, selezionare il tipo di metadati **Object Size** e specificare due valori di metadati.

- Il primo valore di metadati specifica oggetti superiori o uguali a 10 MB.
- Il secondo valore di metadati specifica gli oggetti inferiori o uguali a 100 MB.

Advanced Filtering

Use advanced filtering if you want a rule to apply only to specific objects. You can filter objects based on their system metadata, user metadata, or object tags (S3 only). When objects are evaluated, the rule is applied if the object's metadata matches the criteria in the advanced filter.

Objects between 10 and 100 MB

Matches all of the following metadata:

Object Size (MB)	greater than or equals	10	+	x	
Object Size (MB)	less than or equals	100	+	x	
+					x

Cancel

Remove Filters

Save

L'utilizzo di più voci consente di avere un controllo preciso su quali oggetti vengono associati. Nell'esempio seguente, la regola si applica agli oggetti che hanno un marchio A o un marchio B come valore dei metadati dell'utente camera_TYPE. Tuttavia, la regola si applica solo agli oggetti Brand B di dimensioni inferiori a 10 MB.

Advanced Filtering

Use advanced filtering if you want a rule to apply only to specific objects. You can filter objects based on their system metadata, user metadata, or object tags (S3 only). When objects are evaluated, the rule is applied if the object's metadata matches the criteria in the advanced filter.

Multiple filters

Matches all of the following metadata:

User Metadata	camera_type	equals	Brand A	+ x
---------------	-------------	--------	---------	-----

+ x

Or matches all of the following metadata:

User Metadata	camera_type	equals	Brand B	+ x
Object Size (MB)		less than or equals	10	+ x

+ x

Cancel Remove Filters Save

Informazioni correlate

["Utilizzo dell'ultimo tempo di accesso nelle regole ILM"](#)

["Configurazione delle regioni \(opzionale e solo S3\)"](#)

Fase 2 di 3: Definizione delle posizioni

Il passaggio 2 (definizione delle posizioni) della procedura guidata Crea regola ILM consente di definire le istruzioni di posizionamento che determinano la durata della memorizzazione degli oggetti, il tipo di copie (replicate o codificate per la cancellazione), la posizione di archiviazione e il numero di copie.

A proposito di questa attività

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 per sempre o fino a quando non sono più necessarie copie di oggetti.

Ogni istruzione di posizionamento può avere più righe se si desidera creare diversi tipi di copie o utilizzare posizioni diverse durante tale periodo di tempo.

Questa regola ILM di esempio crea due copie replicate per il primo anno. Ogni copia viene salvata in un pool di storage in un sito diverso. Dopo un anno, viene creata una copia 2+1 con codice di cancellazione e salvata in

un solo sito.

Create ILM Rule Step 2 of 3: Define Placements

Configure placement instructions to specify how you want objects matched by this rule to be stored.

Example rule

Two copies for one year, then EC forever

Reference Time

Placements Sort by start day

From day store for days Add Remove

Type Location Copies + x

Specifying multiple storage pools might cause data to be stored at the same site if the pools overlap. See [Managing objects with information lifecycle management](#) for more information.

From day store forever Add Remove

Type Location Copies + x

Retention Diagram Refresh

Trigger: Day 0, Year 1

Duration: 1 years, Forever

Cancel Back Next

Fasi

1. Per **Reference Time** (tempo di riferimento), selezionare il tipo di tempo da utilizzare per il calcolo dell'ora di inizio di un'istruzione di posizionamento.

Opzione	Descrizione
Tempo di acquisizione	L'ora in cui l'oggetto è stato acquisito.
Ora ultimo accesso	L'ora in cui l'oggetto è stato recuperato per l'ultima volta (letto o visualizzato). Nota: per utilizzare questa opzione, è necessario attivare gli aggiornamenti dell'ultimo tempo di accesso per il bucket S3 o il container Swift. "Utilizzo dell'ultimo tempo di accesso nelle regole ILM"

Opzione	Descrizione
Ora non corrente	<p>Il tempo in cui una versione dell'oggetto è diventata non aggiornata a causa dell'acquisizione di una nuova versione e della sua sostituzione come versione corrente.</p> <p>Nota: l'ora non corrente si applica solo agli oggetti S3 nei bucket abilitati per il controllo delle versioni.</p> <p>È possibile utilizzare questa opzione per ridurre l'impatto dello storage degli oggetti con versione filtrando le versioni degli oggetti non correnti. Vedere "esempio 4: Regole ILM e policy per gli oggetti con versione S3".</p>
Tempo di creazione definito dall'utente	Tempo specificato nei metadati definiti dall'utente.



Se si desidera creare una regola conforme, selezionare **Ingest Time**.

- Nella sezione **posizionamenti**, selezionare un'ora di inizio e una durata per il primo periodo di tempo.

Ad esempio, è possibile specificare dove memorizzare gli oggetti per il primo anno ("Ay 0 for 365 days `d`"). Almeno un'istruzione deve iniziare al giorno 0.

- Se si desidera creare copie replicate:

- Dall'elenco a discesa **tipo**, selezionare **replicato**.
- Nel campo **Location**, selezionare **Add Pool** per ciascun pool di storage che si desidera aggiungere.

Se si specifica un solo pool di storage, tenere presente che StorageGRID può memorizzare solo una copia replicata di un oggetto su un nodo di storage specifico. Se la griglia include tre nodi di storage e si seleziona 4 come numero di copie, verranno eseguite solo tre copie: Una copia per ciascun nodo di storage.



Viene attivato l'avviso **ILM placement unachievable** per indicare che la regola ILM non può essere applicata completamente.

Se si specificano più pool di storage, tenere presenti le seguenti regole:

- Il numero di copie non può essere superiore al numero di pool di storage.
- Se il numero di copie corrisponde al numero di pool di storage, viene memorizzata una copia dell'oggetto in ciascun pool di storage.
- Se il numero di copie è inferiore al numero di pool di storage, il sistema distribuisce le copie 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 storage si sovrappongono (contengono gli stessi nodi di storage), tutte le copie dell'oggetto potrebbero essere salvate in un solo sito. Per questo motivo, non specificare il pool di storage predefinito di tutti i nodi di storage e di un altro pool di storage.

Placements ⓘ Sort by start day

From day store Add Remove

Type Location Copies + x

Specifying multiple storage pools might cause data to be stored at the same site if the pools overlap. See [Managing objects with information lifecycle management](#) for more information.

c. Selezionare il numero di copie che si desidera eseguire.

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 mette i dati a rischio di perdita permanente. Se esiste una sola copia replicata di un oggetto durante un periodo di tempo, tale oggetto viene perso se un nodo di storage si guasta o presenta un errore significativo. Inoltre, durante le procedure di manutenzione, ad esempio gli aggiornamenti, si perde temporaneamente l'accesso all'oggetto.



Placements ⓘ Sort by start day

From day store Add Remove

Type Location Copies Temporary location + x

An ILM rule that creates only one replicated copy for any time period puts data at risk of permanent loss. [View additional details](#).

Per evitare questi rischi, effettuare una o più delle seguenti operazioni:

- Aumentare il numero di copie per il periodo di tempo.
- Fare clic sull'icona con il segno più **+** per creare copie aggiuntive durante il periodo di tempo. Quindi, selezionare un pool di storage diverso o un pool di storage cloud.
- Selezionare **erasure coded** per tipo, invece di **Replicated**. È possibile ignorare questo avviso se questa regola crea già più copie per tutti i periodi di tempo.

d. Se è stato specificato un solo pool di storage, ignorare il campo **posizione temporanea**.



Le posizioni temporanee sono obsolete e verranno rimosse in una release futura.

4. Se si desidera memorizzare oggetti in un pool di storage cloud:

a. Dall'elenco a discesa **tipo**, selezionare **replicato**.

b. Nel campo **Location**, selezionare **Add Pool** (Aggiungi pool). Quindi, selezionare un pool di storage cloud.

From day store Add Remove

Type Location Copies + x

Quando si utilizzano i Cloud Storage Pool, tenere presenti le seguenti 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

storage nelle stesse istruzioni di posizionamento.

Type Location Copies

If you want to use a Cloud Storage Pool, you must remove any other storage pools or Cloud Storage Pools from this placement instruction.

- È possibile memorizzare solo una copia di un oggetto in un determinato pool di storage cloud. Se si imposta **copie** su 2 o più, viene visualizzato un messaggio di errore.

Type Location Copies

The number of copies cannot be more than one when a Cloud Storage Pool is selected.

- Non è possibile memorizzare più copie di un oggetto contemporaneamente in un pool di storage cloud. Viene visualizzato un messaggio di errore se più posizioni che utilizzano un pool di storage cloud presentano date sovrapposte o se più righe nello stesso posizionamento utilizzano un pool di storage cloud.

Placements Sort by start day

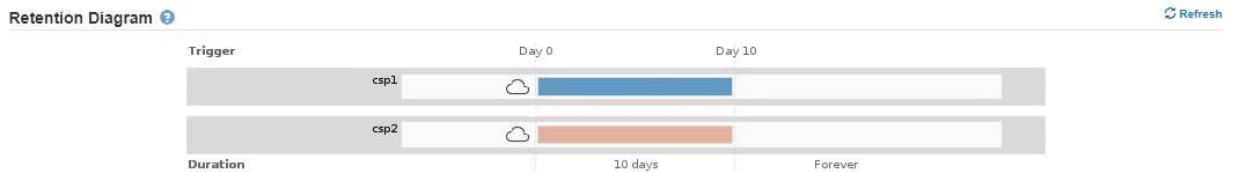
From day store for days

Type Location Copies

Type Location Copies

A rule cannot store more than one object copy in any Cloud Storage Pool at the same time. You must remove one of the Cloud Storage Pools (csp1, csp2) or use multiple placement instructions with dates that do not overlap. **Overlapping days:** 0-10.

To see the overlapping days on the Retention Diagram, click Refresh.



- È possibile memorizzare un oggetto in un pool di storage cloud nello stesso momento in cui l'oggetto viene memorizzato come copie replicate o erasure coded in StorageGRID. Tuttavia, come mostra questo esempio, è necessario includere più di una riga nelle istruzioni di posizionamento per il periodo di tempo, in modo da poter specificare il numero e i tipi di copie per ciascuna posizione.

Placements ?

From day store for days

Type Location Copies

Type Location Copies

5. Se si desidera creare una copia con codice di cancellazione:

a. Dall'elenco a discesa **tipo**, selezionare **erasure coded**.

Il numero di copie viene modificato in 1. Viene visualizzato un avviso se la regola non dispone di un filtro avanzato per ignorare oggetti di dimensioni pari o inferiori a 200 KB.

Do not use erasure coding for objects that are 200 KB or smaller. Select Back to return to Step 1. Then, use Advanced filtering to set the Object Size (MB) filter to "greater than 0.2".



Non utilizzare la codifica erasure per oggetti di dimensioni inferiori a 200 KB per evitare l'overhead di gestione di frammenti con codifica erasure molto piccoli.

b. Se viene visualizzato l'avviso relativo alle dimensioni dell'oggetto, attenersi alla seguente procedura per cancellarlo:

- i. Selezionare **Indietro** per tornare alla fase 1.
- ii. Selezionare **Advanced Filtering** (filtraggio avanzato).
- iii. Impostare il filtro dimensione oggetto (MB) su "maggiore di 0.2".

c. Selezionare la posizione di storage.

La posizione di storage per una copia con codice di cancellazione include il nome del pool di storage, seguito dal nome del profilo di codifica Erasure.

6. Facoltativamente, aggiungere periodi di tempo diversi o creare copie aggiuntive in posizioni diverse:

- Fare clic sull'icona più per creare copie aggiuntive in una posizione diversa durante lo stesso periodo di tempo.
- Fare clic su **Add** (Aggiungi) per aggiungere un periodo di tempo diverso alle istruzioni di posizionamento.



Gli oggetti vengono eliminati automaticamente alla fine del periodo di tempo finale, a meno che il periodo di tempo finale non termini con **forever**.

7. Fare clic su **Refresh** (Aggiorna) per aggiornare il diagramma di conservazione e confermare le istruzioni di posizionamento.

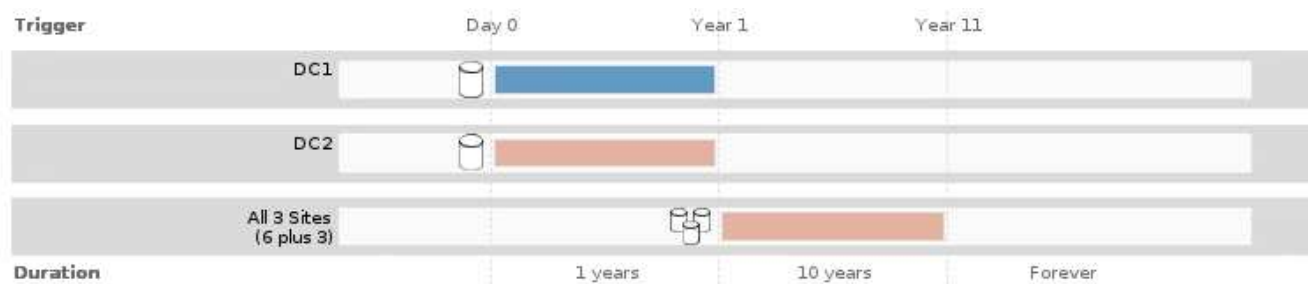
Ogni riga del diagramma indica dove e quando verranno collocate le copie degli oggetti. Il tipo di copia è rappresentato da una delle seguenti icone:

	Copia replicata
	Copia con codifica erasure



Copia del pool di cloud storage

In questo esempio, due copie replicate verranno salvate in due pool di storage (DC1 e DC2) per un anno. Quindi, una copia con codice di cancellazione verrà salvata per altri 10 anni, utilizzando uno schema di erasure coding 6+3 presso tre siti. Dopo 11 anni, gli oggetti verranno cancellati da StorageGRID.



8. Fare clic su **Avanti**.

Viene visualizzato il punto 3 (definire il comportamento di Ingest).

Informazioni correlate

["Quali sono le istruzioni per il posizionamento delle regole ILM"](#)

["Esempio 4: Regole ILM e policy per gli oggetti con versione S3"](#)

["Perché non utilizzare la replica a copia singola"](#)

["Gestione degli oggetti con S3 Object Lock"](#)

["Utilizzo di un pool di storage come posizione temporanea \(obsoleto\)"](#)

["Fase 3 di 3: Definizione del comportamento di acquisizione"](#)

Utilizzo dell'ultimo tempo di accesso nelle regole ILM

In una regola ILM, è possibile utilizzare l'ora dell'ultimo accesso come ora di riferimento. Ad esempio, è possibile lasciare oggetti che sono stati visualizzati negli ultimi tre mesi sui nodi di storage locali, mentre si spostano oggetti che non sono stati visualizzati di recente in una posizione off-site. È inoltre possibile utilizzare l'ora dell'ultimo accesso come filtro avanzato se si desidera che una regola ILM si applichi solo agli oggetti a cui è stato effettuato l'ultimo accesso in una data specifica.

A proposito di questa attività

Prima di utilizzare l'ultimo tempo di accesso in una regola ILM, esaminare le seguenti considerazioni:

- Quando si utilizza l'ultimo tempo di accesso come tempo di riferimento, tenere presente che la modifica dell'ultimo tempo di accesso per un oggetto non attiva una valutazione ILM immediata. Al contrario, le posizioni dell'oggetto vengono valutate e l'oggetto viene spostato come richiesto quando ILM in background valuta l'oggetto. Questa operazione potrebbe richiedere due settimane o più dopo l'accesso all'oggetto.

Tenere conto di questa latenza durante la creazione di regole ILM basate sull'ultimo tempo di accesso ed

evitare posizionamenti che utilizzano brevi periodi di tempo (meno di un mese).

- Quando si utilizza l'ultimo tempo di accesso come filtro avanzato o come tempo di riferimento, è necessario attivare gli ultimi aggiornamenti dell'ora di accesso per i bucket S3. È possibile utilizzare il tenant Manager o l'API di gestione tenant.



Gli ultimi aggiornamenti dell'orario di accesso sono sempre attivati per i container Swift, ma sono disattivati per impostazione predefinita per i bucket S3.



Tenere presente che l'attivazione degli ultimi aggiornamenti del tempo di accesso può ridurre le performance, soprattutto nei sistemi con oggetti di piccole dimensioni. L'impatto delle performance si verifica perché StorageGRID deve aggiornare gli oggetti con nuovi timestamp ogni volta che gli oggetti vengono recuperati.

La tabella seguente riassume se l'ora dell'ultimo accesso viene aggiornata per tutti gli oggetti nel bucket per diversi tipi di richieste.

Tipo di richiesta	Se l'ora dell'ultimo accesso viene aggiornata quando gli ultimi aggiornamenti dell'ora di accesso sono disattivati	Se l'ora dell'ultimo accesso viene aggiornata quando sono attivati gli ultimi aggiornamenti dell'ora di accesso
Richiesta di recuperare un oggetto, il relativo elenco di controllo degli accessi o i relativi metadati	No	Sì
Richiesta di aggiornamento dei metadati di un oggetto	Sì	Sì
Richiesta di copia di un oggetto da un bucket all'altro	<ul style="list-style-type: none">• No, per la copia di origine• Sì, per la copia di destinazione	<ul style="list-style-type: none">• Sì, per la copia di origine• Sì, per la copia di destinazione
Richiesta di completare un caricamento multiparte	Sì, per l'oggetto assemblato	Sì, per l'oggetto assemblato

Informazioni correlate

["Utilizzare S3"](#)

["Utilizzare un account tenant"](#)

Fase 3 di 3: Definizione del comportamento di acquisizione

Il passaggio 3 (Definisci comportamento di acquisizione) della procedura guidata Crea regola ILM consente di scegliere come proteggere gli oggetti filtrati da questa regola durante l'acquisizione.

A proposito di questa attività

StorageGRID può eseguire copie temporanee e mettere in coda gli oggetti per la valutazione ILM in un secondo momento, oppure può eseguire copie per soddisfare immediatamente le istruzioni di posizionamento della regola.

Select the data protection option to use when objects are ingested:

- Strict**
Always uses this rule's placements on ingest. Ingest fails when this rule's placements are not possible.
- Balanced**
Optimum ILM efficiency. Attempts this rule's placements on ingest. Creates interim copies when that is not possible.
- Dual commit**
Creates interim copies on ingest and applies this rule's placements later.

Cancel Back Save

Fasi

1. Selezionare l'opzione di protezione dei dati da utilizzare quando vengono acquisiti oggetti:

Opzione	Descrizione
Rigoroso	Utilizza sempre le posizioni di questa regola per l'acquisizione. L'acquisizione non riesce quando non è possibile eseguire il posizionamento di questa regola.
Bilanciato	Efficienza ILM ottimale. Tenta di inserire i posizionamenti di questa regola. Crea copie temporanee quando ciò non è possibile.
Commit doppio	Crea copie temporanee al momento dell'acquisizione e applica le posizioni di questa regola in un secondo momento.

Balanced offre una combinazione di sicurezza ed efficienza dei dati adatta nella maggior parte dei casi. Per soddisfare requisiti specifici, vengono generalmente utilizzati i requisiti Strict o Dual Commit.

Per ulteriori informazioni, consulta "quali sono le opzioni di protezione dei dati per l'acquisizione" e "vantaggi e svantaggi di ciascuna opzione di protezione dei dati".



Viene visualizzato un messaggio di errore se si seleziona l'opzione Strict (rigoroso) o Balanced (bilanciato) e la regola utilizza una delle seguenti posizioni:

- Un pool di storage cloud al giorno 0
- Un nodo di archivio al giorno 0
- Un Cloud Storage Pool o un nodo di archivio quando la regola utilizza un tempo di creazione definito dall'utente come tempo di riferimento

2. Fare clic su **Save** (Salva).

La regola ILM viene salvata. La regola non diventa attiva fino a quando non viene aggiunta a un criterio ILM e tale criterio non viene attivato.

Informazioni correlate

["Opzioni di protezione dei dati per l'acquisizione"](#)

["Vantaggi, svantaggi e limitazioni delle opzioni di protezione dei dati"](#)

"Esempio 5: Regole e policy ILM per un comportamento rigoroso di acquisizione"

"Creazione di un criterio ILM"

Creazione di una regola ILM predefinita

Ogni policy ILM deve disporre di una regola predefinita che non filtra gli oggetti. Prima di creare un criterio ILM, è necessario creare almeno una regola ILM che possa essere utilizzata come regola predefinita per il criterio.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

A proposito di questa attività

La regola predefinita è l'ultima regola da valutare in un criterio ILM, pertanto 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 del criterio.

In questo esempio di policy, la prima regola si applica solo agli oggetti appartenenti al tenant A. La regola predefinita, ultima, si applica agli oggetti appartenenti a tutti gli altri account tenant.

Default	Rule Name	Tenant Account	Actions
	Erasure Coding for Tenant A 	Tenant A (94793396288150002349)	✘
✓	2 Copies 2 Data Centers 	Ignore	✘

Quando si crea la regola predefinita, tenere presenti i seguenti requisiti:

- La regola predefinita viene automaticamente inserita come ultima regola nel criterio.
- La regola predefinita non può utilizzare filtri di base o avanzati.
- La regola predefinita dovrebbe creare copie replicate.



Non utilizzare una regola che crea copie con codice di cancellazione come regola predefinita per un criterio. Le regole di erasure coding devono utilizzare un filtro avanzato per evitare che oggetti più piccoli vengano sottoposti a erasure coding.

- In generale, la regola predefinita deve conservare gli oggetti per sempre.
- Se si utilizza (o si intende attivare) l'impostazione globale S3 Object Lock (blocco oggetto S3), la regola predefinita per il criterio attivo o proposto deve essere conforme.

Fasi

1. Selezionare **ILM** > **regole**.

Viene visualizzata la pagina ILM Rules (regole ILM).

2. Selezionare **Crea**.

Viene visualizzata la fase 1 (Definisci le basi) della procedura guidata Crea regola ILM.

3. Immettere un nome univoco per la regola nel campo **Nome**.
4. Se si desidera, inserire una breve descrizione per la regola nel campo **Descrizione**.
5. Lasciare vuoto il campo **account tenant**.

La regola predefinita deve essere applicata a tutti gli account tenant.

6. Lasciare vuoto il campo **Nome bucket**.

La regola predefinita deve essere applicata a tutti i bucket S3 e ai container Swift.

7. Non selezionare **Advanced Filtering**

La regola predefinita non può specificare alcun filtro.

8. Selezionare **Avanti**.

Viene visualizzato il punto 2 (definizione delle posizioni).

9. Specificare le istruzioni di posizionamento per la regola predefinita.

- La regola predefinita deve 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 un criterio. Le regole di erasure coding devono includere il filtro avanzato **Object Size (MB) maggiore di 0.2** per evitare che oggetti più piccoli vengano sottoposti a erasure coding.

- Se si utilizza (o si intende attivare) l'impostazione globale S3 Object Lock (blocco oggetto S3), la regola predefinita deve essere conforme:
 - Deve creare almeno due copie di oggetti replicate o una copia con codice di cancellazione.
 - Queste copie devono esistere nei nodi di storage per l'intera durata di ciascuna riga nelle istruzioni di posizionamento.
 - Impossibile salvare le copie degli oggetti in un pool di storage cloud.
 - Impossibile salvare le copie degli oggetti nei nodi di archiviazione.
 - Almeno una riga delle istruzioni di posizionamento deve iniziare al giorno 0, utilizzando l'ora di inizio come ora di riferimento.
 - Almeno una riga delle istruzioni di posizionamento deve essere "forever".

10. Fare clic su **Refresh** (Aggiorna) per aggiornare il diagramma di conservazione e confermare le istruzioni di posizionamento.
11. Fare clic su **Avanti**.

Viene visualizzato il punto 3 (definire il comportamento di Ingest).

12. Selezionare l'opzione di protezione dei dati da utilizzare quando vengono acquisiti oggetti e selezionare **Salva**.

Creazione di un criterio ILM

Quando si crea un criterio ILM, si inizia selezionando e ordinando le regole ILM. Quindi, verificare il comportamento della policy proposta simulandola rispetto agli oggetti precedentemente acquisiti. Quando si è soddisfatti del corretto funzionamento del criterio proposto, è possibile attivarlo per creare il criterio attivo.



Un criterio ILM non configurato correttamente può causare una perdita di dati non ripristinabile. Prima di attivare un criterio ILM, esaminare attentamente il criterio ILM e le relative regole ILM, quindi simulare il criterio ILM. Verificare sempre che la policy ILM funzioni come previsto.

Considerazioni per la creazione di un criterio ILM

- Utilizzare la policy integrata del sistema, Baseline 2 Copies Policy, solo nei sistemi di test. La regola Make 2 copies di questo criterio utilizza il pool di storage All Storage Node, che contiene tutti i siti. Se il sistema StorageGRID dispone di più siti, è possibile che due copie di un oggetto vengano posizionate sullo stesso sito.
- Durante la progettazione di un nuovo criterio, considerare tutti i diversi tipi di oggetti che potrebbero essere inseriti nella griglia. Assicurarsi che il criterio includa regole per la corrispondenza e posizionare questi oggetti secondo necessità.
- Mantenere la policy 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.
- Assicurarsi che le regole della policy siano nell'ordine corretto. Una volta attivato il criterio, gli oggetti nuovi ed esistenti vengono valutati dalle regole nell'ordine elencato, iniziando dall'inizio. Ad esempio, se la prima regola di un criterio corrisponde a un oggetto, tale regola non verrà valutata da altre regole.
- L'ultima regola in ogni policy ILM è la regola ILM predefinita, che non può utilizzare alcun filtro. Se un oggetto non è stato associato da un'altra regola, la regola predefinita controlla la posizione e il tempo di conservazione dell'oggetto.
- Prima di attivare un nuovo criterio, esaminare le modifiche apportate dal criterio al posizionamento degli oggetti esistenti. La modifica della posizione di un oggetto esistente potrebbe causare problemi di risorse temporanee quando i nuovi posizionamenti vengono valutati e implementati.

Informazioni correlate

["Che cos'è una policy ILM"](#)

["Esempio 6: Modifica di un criterio ILM"](#)

Creazione di una policy ILM proposta

È possibile creare un criterio ILM proposto da zero oppure clonare il criterio attivo corrente se si desidera iniziare con lo stesso insieme di regole.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.
- È necessario aver creato le regole ILM che si desidera aggiungere al criterio proposto. Se necessario, è possibile salvare una policy proposta, creare regole aggiuntive e quindi modificare la policy proposta per aggiungere le nuove regole.

- È necessario aver creato una regola ILM predefinita per il criterio che non contiene filtri.

"Creazione di una regola ILM predefinita"

A proposito di questa attività

I motivi tipici per la creazione di una policy ILM proposta includono:

- È stato aggiunto un nuovo sito ed è necessario utilizzare nuove regole ILM per posizionare gli oggetti in tale sito.
- Si sta smantellando un sito ed è necessario rimuovere tutte le regole che fanno riferimento al sito.
- È stato aggiunto un nuovo tenant con requisiti speciali per la protezione dei dati.
- Hai iniziato a utilizzare un Cloud Storage Pool.



Utilizzare la policy integrata del sistema, Baseline 2 Copies Policy, solo nei sistemi di test. La regola Make 2 copies di questo criterio utilizza il pool di storage All Storage Node, che contiene tutti i siti. Se il sistema StorageGRID dispone di più siti, è possibile che due copie di un oggetto vengano posizionate sullo stesso sito.



Se è stata attivata l'impostazione blocco oggetti S3 globale, i passaggi per la creazione di un criterio sono leggermente diversi. È necessario assicurarsi che il criterio ILM sia conforme ai requisiti dei bucket che hanno attivato il blocco oggetti S3.

"Creazione di un criterio ILM dopo l'attivazione del blocco oggetti S3"

Fasi

1. Selezionare **ILM > Policy**.

Viene visualizzata la pagina ILM Policies (Criteri ILM). Da questa pagina, è possibile esaminare l'elenco dei criteri proposti, attivi e storici; creare, modificare, oppure rimuovere una policy proposta, clonare la policy attiva o visualizzare i dettagli di qualsiasi policy.

ILM Policies

Review the proposed, active, and historical policies. You can create, edit, or delete a proposed policy; clone the active policy; or view the details for any policy.

+ Create Proposed Policy
📄 Clone
✎ Edit
✖ Remove

Policy Name	Policy State	Start Date	End Date
🔴 Baseline 2 Copies Policy	Active	2017-07-17 12:00:45 MDT	

Viewing Active Policy - Baseline 2 Copies Policy

Review the rules in this policy. If this is a proposed policy, click Simulate to verify the policy and then click Activate to make the policy active.

Rules are evaluated in order, starting from the top.

Rule Name	Default	Tenant Account
Make 2 Copies 🔗	✓	Ignore

Simulate
Activate

2. Determinare come si desidera creare il criterio ILM proposto.

Opzione	Fasi
Creare una nuova policy proposta senza regole già selezionate	<p>a. Se esiste attualmente un criterio ILM proposto, selezionarlo e fare clic su Rimuovi.</p> <p>Non è possibile creare una nuova policy proposta se esiste già una policy proposta.</p> <p>b. Fare clic su Crea policy proposta.</p>
Creare una policy proposta in base alla policy attiva	<p>a. Se esiste attualmente un criterio ILM proposto, selezionarlo e fare clic su Rimuovi.</p> <p>Non è possibile clonare il criterio attivo se esiste già un criterio proposto.</p> <p>b. Selezionare il criterio attivo dalla tabella.</p> <p>c. Fare clic su Clone.</p>
Modificare la policy proposta esistente	<p>a. Selezionare la policy proposta dalla tabella.</p> <p>b. Fare clic su Edit (Modifica).</p>

Viene visualizzata la finestra di dialogo Configure ILM Policy (Configura policy ILM).

Se si sta creando una nuova policy proposta, tutti i campi sono vuoti e non viene selezionata alcuna regola.

Configure ILM Policy

Create a proposed policy by selecting and arranging rules. Then, save the policy and edit it later as required. Click Simulate to verify a saved policy using test objects. When you are ready, click Activate to make this policy the active ILM policy for the grid.

Name

Reason for change

Rules

- Select the rules you want to add to the policy.
- 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

Default	Rule Name	Tenant Account	Actions
<i>No rules selected.</i>			

Cancel
Save

Se si esegue la clonazione del criterio attivo, il campo **Nome** mostra il nome del criterio attivo, aggiunto da un numero di versione (“v2” nell’esempio). Le regole utilizzate nel criterio attivo vengono selezionate e visualizzate nell’ordine corrente.

Name

Reason for change

3. Immettere un nome univoco per la policy proposta nel campo **Nome**.

Immettere almeno 1 e non più di 64 caratteri. Se si clonano i criteri attivi, è possibile utilizzare il nome corrente con il numero di versione aggiunto oppure immettere un nuovo nome.

4. Inserire il motivo della creazione di una nuova policy proposta nel campo **motivo della modifica**.

Immettere almeno 1 e non più di 128 caratteri.

5. Per aggiungere regole al criterio, selezionare **Seleziona regole**.

Viene visualizzata la finestra di dialogo Select Rules for Policy (Seleziona regole per policy), con tutte le regole definite elencate. Se si sta clonando un criterio:

- Vengono selezionate le regole utilizzate dal criterio che si sta clonando.
- Se il criterio da clonare utilizza regole senza filtri che non erano la regola predefinita, viene richiesto di rimuovere tutte le regole tranne una di queste.
- Se la regola predefinita utilizza un filtro, viene richiesto di selezionare una nuova regola predefinita.
- Se la regola predefinita non è l'ultima, un pulsante consente di spostarla alla fine del nuovo criterio.

Select Rules for Policy

Select Default Rule

This list shows the rules that do not use any filters. Select one rule to be the default rule for the policy. The default rule applies to any objects that do not match another rule in the policy and is always evaluated last. The default rule should retain objects forever.

Rule Name
<input checked="" type="radio"/> 2 copies at 2 data centers
<input type="radio"/> 2 copies at 2 data centers for 2 years
<input type="radio"/> Make 2 Copies

Select Other Rules

The other rules in a policy are evaluated before the default rule and must use at least one filter. Each rule in this list uses at least one filter (tenant account, bucket name, or an advanced filter, such as object size).

Rule Name	Tenant Account
<input type="checkbox"/> 1-site EC	—
<input type="checkbox"/> 3-site EC	—

6. Selezionare il nome di una regola o l'icona ulteriori dettagli per visualizzare le impostazioni relative a tale regola.

Questo esempio mostra i dettagli di una regola ILM che esegue due copie replicate in due siti.

Two-Site Replication for Other Tenants

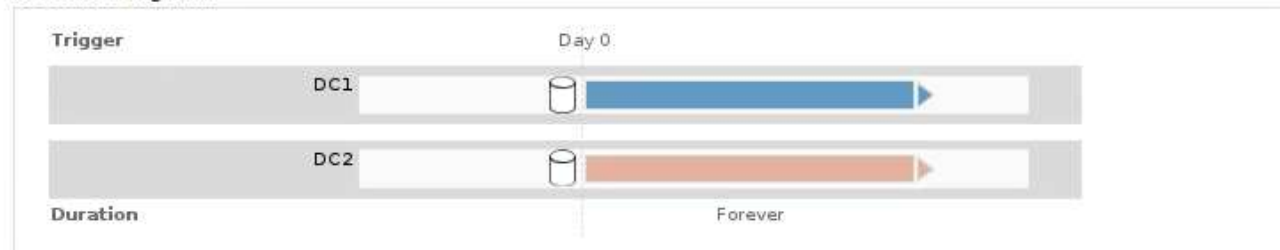
Description: Two-Site Replication for Other Tenants

Ingest Behavior: Balanced

Reference Time: Ingest Time

Filtering Criteria: Matches all objects.

Retention Diagram:



Close

7. Nella sezione **Select Default Rule** (Seleziona regola predefinita), selezionare una regola predefinita per il criterio proposto.

La regola predefinita si applica a tutti gli oggetti che non corrispondono a un'altra regola del criterio. La regola predefinita non può utilizzare alcun filtro e viene sempre valutata per ultima.



Se nella sezione Select Default Rule (Seleziona regola predefinita) non è elencata alcuna regola, uscire dalla pagina dei criteri ILM e creare una regola predefinita.

["Creazione di una regola ILM predefinita"](#)



Non utilizzare la regola di creazione di 2 copie come regola predefinita per un criterio. La regola Make 2 copies utilizza un singolo pool di storage, tutti i nodi di storage, che contiene tutti i siti. Se il sistema StorageGRID dispone di più siti, è possibile che due copie di un oggetto vengano posizionate sullo stesso sito.

8. Nella sezione **Seleziona altre regole**, selezionare le altre regole che si desidera includere nel criterio.

Le altre regole vengono valutate prima della regola predefinita e devono utilizzare almeno un filtro (account tenant, nome bucket o filtro avanzato, ad esempio la dimensione dell'oggetto).

9. Una volta selezionate le regole, selezionare **Apply** (Applica).

Vengono elencate le regole selezionate. La regola predefinita è alla fine, con le altre regole sopra di essa.

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

	Default	Rule Name	Tenant Account	Actions
⬇		3-site EC	Ignore	✘
⬇		1-site EC	Ignore	✘
	✓	2 copies at 2 data centers	Ignore	✘

Cancel **Save**

Viene visualizzato un avviso se la regola predefinita non conserva gli oggetti per sempre. Quando si attiva questo criterio, è necessario confermare che si desidera che StorageGRID elimini gli oggetti quando sono trascorse le istruzioni di posizionamento per la regola predefinita (a meno che un ciclo di vita del bucket non mantenga gli oggetti più a lungo).



	Default	Rule Name	Tenant Account	Actions
⬇		3-site EC	Ignore	✘
⬇		1-site EC	Ignore	✘
	✓	2 copies at 2 data centers for 2 years	Ignore	✘

The default ILM rule in this policy does not retain objects forever. Confirm this is the behavior you expect. Otherwise, any objects that are not matched by another rule will be deleted after 720 days.

10. Trascinare e rilasciare le righe per le regole non predefinite per determinare l'ordine in cui verranno valutate queste regole.

Non è possibile spostare la regola predefinita.



Verificare che le regole ILM siano nell'ordine corretto. Una volta attivato il criterio, gli oggetti nuovi ed esistenti vengono valutati dalle regole nell'ordine elencato, iniziando dall'inizio.

11. Se necessario, fare clic sull'icona di eliminazione ✘ Per eliminare le regole che non si desidera inserire nel criterio, oppure selezionare **Select Rules** (Seleziona regole) per aggiungere altre regole.
12. Al termine, selezionare **Salva**.

La pagina delle policy ILM viene aggiornata:

- Il criterio salvato viene visualizzato come proposto. Le policy proposte non hanno date di inizio e fine.
- I pulsanti **simulate** e **activate** sono abilitati.

ILM Policies

Review the proposed, active, and historical policies. You can create, edit, or delete a proposed policy; clone the active policy; or view the details for any policy.

[+ Create Proposed Policy](#) [Clone](#) [Edit](#) [Remove](#)

Policy Name	Policy State	Start Date	End Date
<input checked="" type="radio"/> Data Protection for Three Sites	Proposed		
<input type="radio"/> Data Protection for Two Sites	Active	2020-09-18 16:01:24 MDT	
<input type="radio"/> Baseline 2 Copies Policy	Historical	2020-09-17 21:32:57 MDT	2020-09-18 16:01:24 MDT

Viewing Proposed Policy - Data Protection for Three Sites

Before activating a new ILM policy:

- Review and carefully simulate the policy. Errors in an ILM policy can cause irreparable data loss.
- Review any changes to the placement of existing replicated and erasure-coded objects. Changing an existing object's location might result in temporary resource issues when the new placements are evaluated and implemented.

See [Managing objects with information lifecycle management](#) for more information.

This policy contains a rule that makes an erasure-coded copy. Confirm that at least one rule uses the Object Size advanced filter to prevent objects that are 200 KB or smaller from being erasure coded. See [Managing objects with information lifecycle management](#) for more information.

Review the rules in this policy. If this is a proposed policy, click Simulate to verify the policy and then click Activate to make the policy active.

Reason for change: Added a third site

Rules are evaluated in order, starting from the top.

Rule Name	Default	Tenant Account
One-Site Erasure Coding for Tenant A		Tenant A (20033011709864740158)
Three-Site Replication for Other Tenants	<input checked="" type="checkbox"/>	Ignore

[Simulate](#) [Activate](#)

13. Passare a. "Simulazione di un criterio ILM".

Informazioni correlate

["Che cos'è una policy ILM"](#)

["Gestione degli oggetti con S3 Object Lock"](#)

Creazione di un criterio ILM dopo l'attivazione del blocco oggetti S3

Se l'impostazione blocco oggetti S3 globale è attivata, i passaggi per la creazione di un criterio sono leggermente diversi. È necessario assicurarsi che il criterio ILM sia conforme ai requisiti dei bucket che hanno attivato il blocco oggetti S3.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.
- L'impostazione globale S3 Object Lock (blocco oggetti S3) deve essere già attivata per il sistema StorageGRID.



Se l'impostazione globale S3 Object Lock non è stata attivata, utilizzare le istruzioni generali per creare un criterio proposto.

["Creazione di una policy ILM proposta"](#)

- È necessario aver creato le regole ILM conformi e non conformi che si desidera aggiungere al criterio proposto. Se necessario, è possibile salvare una policy proposta, creare regole aggiuntive e quindi modificare la policy proposta per aggiungere le nuove regole.

"Esempio 7: Policy ILM conforme per il blocco oggetti S3"

- È necessario aver creato una regola ILM predefinita conforme per il criterio.

"Creazione di una regola ILM predefinita"

Fasi

1. Selezionare **ILM > Policy**.

Viene visualizzata la pagina ILM Policies (Criteri ILM). Se l'impostazione globale S3 Object Lock è attivata, la pagina ILM Policies (Criteri ILM) indica quali regole ILM sono conformi.

ILM Policies

Review the proposed, active, and historical policies. You can create, edit, or delete a proposed policy; clone the active policy; or view the details for any policy.

Policy Name	Policy State	Start Date	End Date
Baseline 2 Copies Policy	Active	2021-02-04 01:04:29 MST	

Rule Name	Default	Compliant	Tenant Account
Make 2 Copies	✓	✓	Ignore

2. Immettere un nome univoco per la policy proposta nel campo **Nome**.

Immettere almeno 1 e non più di 64 caratteri.

3. Inserire il motivo della creazione di una nuova policy proposta nel campo **motivo della modifica**.

Immettere almeno 1 e non più di 128 caratteri.

4. Per aggiungere regole al criterio, selezionare **Seleziona regole**.

Viene visualizzata la finestra di dialogo Select Rules for Policy (Seleziona regole per policy), con tutte le regole definite elencate.

- La sezione Select Default Rule (Seleziona regola predefinita) elenca le regole che possono essere quelle predefinite per un criterio conforme. Include regole conformi che non utilizzano filtri.
- La sezione Seleziona altre regole elenca le altre regole conformi e non compatibili che possono essere selezionate per questo criterio.

Select Rules for Policy

Select Default Rule

This list shows the rules that are compliant and do not use any filters. Select one rule to be the default rule for the policy. The default rule applies to any objects that do not match another rule in the policy and is always evaluated last.

	Rule Name
<input type="radio"/>	Default Compliant Rule: Two Copies Two Data Centers
<input type="radio"/>	Make 2 Copies

Select Other Rules

The other rules in a policy are evaluated before the default rule. If you need a different "default" rule for objects in non-compliant S3 buckets, select one non-compliant rule that does not use a filter. Any other rules in the policy must use at least one filter (tenant account, bucket name, or an advanced filter, such as object size).

	Rule Name	Compliant	Uses Filter	Is Selectable
<input type="checkbox"/>	Compliant Rule: EC for bank-records bucket - Bank of ABC	✓	✓	Yes
<input type="checkbox"/>	Non-Compliant Rule: Use Cloud Storage Pool			Yes

Cancel

Apply

5. Selezionare il nome di una regola o l'icona ulteriori dettagli per visualizzare le impostazioni relative a tale regola.
6. Nella sezione **Select Default Rule** (Seleziona regola predefinita), selezionare una regola predefinita per il criterio proposto.

La tabella di questa sezione elenca solo le regole conformi e non utilizzano filtri.



Se nella sezione Select Default Rule (Seleziona regola predefinita) non è elencata alcuna regola, uscire dalla pagina dei criteri ILM e creare una regola predefinita conforme.

["Creazione di una regola ILM predefinita"](#)



Non utilizzare la regola di creazione di 2 copie come regola predefinita per un criterio. La regola Make 2 copies utilizza un singolo pool di storage, tutti i nodi di storage, che contiene tutti i siti. Se si utilizza questa regola, sullo stesso sito potrebbero essere collocate più copie di un oggetto.

7. Nella sezione **Seleziona altre regole**, selezionare le altre regole che si desidera includere nel criterio.

- a. Se è necessaria una regola "default" diversa per gli oggetti nei bucket S3 non conformi, selezionare facoltativamente una regola non conforme che non utilizza un filtro.

Ad esempio, è possibile utilizzare un Cloud Storage Pool o un nodo di archiviazione per memorizzare gli oggetti nei bucket che non hanno attivato il blocco oggetti S3.



È possibile selezionare solo una regola non conforme che non utilizza un filtro. Non appena si seleziona una regola, la colonna **è selezionabile** mostra **No** per qualsiasi altra regola non conforme senza filtri.

- a. Selezionare qualsiasi altra regola conforme o non conforme che si desidera utilizzare nel criterio.

Le altre regole devono utilizzare almeno un filtro (account tenant, nome bucket o filtro avanzato, ad esempio la dimensione dell'oggetto).

8. Una volta selezionate le regole, selezionare **Apply** (Applica).

Vengono elencate le regole selezionate. La regola predefinita è alla fine, con le altre regole sopra di essa. Se è stata selezionata anche una regola "default" non conforme, tale regola viene aggiunta come seconda o ultima regola nel criterio.

In questo esempio, l'ultima regola, 2 copie 2 data center, è la regola predefinita: È conforme e non dispone di filtri. La seconda all'ultima regola, Cloud Storage Pool, non ha filtri ma non è conforme.

Configure ILM Policy

Create a proposed policy by selecting and arranging rules. Then, save the policy and edit it later as required. Click Simulate to verify a saved policy using test objects. When you are ready, click Activate to make this policy the active ILM policy for the grid.

Name

Reason for change

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 (and any non-compliant rule without a filter) will be automatically placed at the end of the policy and cannot be moved.

Default	Rule Name	Compliant	Tenant Account	Actions
	Compliant Rule: EC for bank-records bucket - Bank of ABC	✓	Bank of ABC (90767802913525281639)	✗
	Non-Compliant Rule: Use Cloud Storage Pool		Ignore	✗
✓	Default Compliant Rule: Two Copies Two Data Centers	✓	Ignore	✗

9. Trascinare e rilasciare le righe per le regole non predefinite per determinare l'ordine in cui verranno valutate queste regole.

Non è possibile spostare la regola predefinita o la regola "default" non conforme.



Verificare che le regole ILM siano nell'ordine corretto. Una volta attivato il criterio, gli oggetti nuovi ed esistenti vengono valutati dalle regole nell'ordine elencato, iniziando dall'inizio.

10. Se necessario, fare clic sull'icona di eliminazione ✗ Per eliminare le regole che non si desidera inserire nel criterio, oppure selezionare **Select Rules** (Seleziona regole) per aggiungere altre regole.

11. Al termine, selezionare **Salva**.

La pagina delle policy ILM viene aggiornata:

- Il criterio salvato viene visualizzato come proposto. Le policy proposte non hanno date di inizio e fine.
- I pulsanti **simulate** e **activate** sono abilitati.

ILM Policies

Review the proposed, active, and historical policies. You can create, edit, or delete a proposed policy; clone the active policy; or view the details for any policy.

+ Create Proposed Policy Clone Edit Remove

Policy Name	Policy State	Start Date	End Date
Compliant ILM Policy for S3 Object Lock	Proposed		
Compliant ILM Policy	Active	2021-02-05 16:22:53 MST	
Non-Compliant ILM policy	Historical	2021-02-05 15:17:05 MST	2021-02-05 16:22:53 MST
Baseline 2 Copies Policy	Historical	2021-02-04 21:35:52 MST	2021-02-05 15:17:05 MST

Viewing Proposed Policy - Compliant ILM Policy for S3 Object Lock

Before activating a new ILM policy:

- Review and carefully simulate the policy. Errors in an ILM policy can cause irreparable data loss.
- Review any changes to the placement of existing replicated and erasure-coded objects. Changing an existing object's location might result in temporary resource issues when the new placements are evaluated and implemented.

See [Managing objects with information lifecycle management](#) for more information.

This policy contains a rule that makes an erasure-coded copy. Confirm that at least one rule uses the Object Size advanced filter to prevent objects that are 200 KB or smaller from being erasure coded. See [Managing objects with information lifecycle management](#) for more information.

Review the rules in this policy. If this is a proposed policy, click Simulate to verify the policy and then click Activate to make the policy active.

Reason for change: Example policy

Rules are evaluated in order, starting from the top. The policy's default rule must be compliant.

Rule Name	Default	Compliant	Tenant Account
Compliant Rule: EC for bank-records bucket - Bank of ABC		✓	Bank of ABC (90767802913525281639)
Non-Compliant Rule: Use Cloud Storage Pool			Ignore
Default Compliant Rule: Two Copies Two Data Centers	✓	✓	Ignore

Simulate Activate

12. Passare a "Simulazione di un criterio ILM".

Simulazione di un criterio ILM

È necessario simulare una policy proposta sugli oggetti di test prima di attivare la policy e applicarla ai dati di produzione. La finestra di simulazione offre un ambiente standalone sicuro per le policy di test prima che vengano attivate e applicate ai dati nell'ambiente di produzione.

Di cosa hai bisogno


- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.
- È necessario conoscere il bucket S3/object-key o il container Swift/object-name per ciascun oggetto che si desidera sottoporre a test e che tali oggetti siano già stati acquisiti.

A proposito di questa attività

È necessario selezionare attentamente gli oggetti per i quali si desidera sottoporre a test il criterio proposto. Per simulare un criterio in maniera approfondita, è necessario testare almeno un oggetto per ciascun filtro in ogni regola.

Ad esempio, se un criterio include una regola per la corrispondenza degli oggetti nel bucket A e un'altra regola per la corrispondenza degli oggetti nel bucket B, è necessario selezionare almeno un oggetto dal bucket A e un oggetto dal bucket B per eseguire un test completo del criterio. Se il criterio include una regola predefinita per posizionare tutti gli altri oggetti, è necessario testare almeno un oggetto da un altro bucket.

Quando si simula un criterio, si applicano le seguenti considerazioni:

- Dopo aver apportato modifiche a un criterio, salvare il criterio proposto. Quindi, simulare il comportamento della policy proposta salvata.
- Quando si simula un criterio, le regole ILM del criterio filtrano gli oggetti di test, in modo da poter vedere quale regola è stata applicata a ciascun oggetto. Tuttavia, non vengono create copie di oggetti e non vengono posizionati oggetti. L'esecuzione di una simulazione non modifica in alcun modo i dati, le regole o i criteri.
- La pagina Simulation conserva gli oggetti testati fino alla chiusura, all'allontanamento o all'aggiornamento della pagina ILM Policies.
- Simulation restituisce il nome della regola corrispondente. Per determinare quale pool di storage o profilo di codifica Erasure è in vigore, è possibile visualizzare il diagramma di conservazione facendo clic sul nome della regola o sull'icona ulteriori dettagli .
- Se è attivata la versione S3, il criterio viene simulato solo rispetto alla versione corrente dell'oggetto.

Fasi

1. Selezionare e organizzare le regole e salvare la policy proposta.

La policy in questo esempio ha tre regole:

Nome regola	Filtro	Tipo di copie	Conservazione
X-men	<ul style="list-style-type: none"> • Tenant A. • Metadati dell'utente (serie=x-men) 	2 copie in due data center	2 anni
PNG	La chiave termina con .png	2 copie in due data center	5 anni
Due copie di due data center	<i>Nessuno</i>	2 copie in due data center	Per sempre

Viewing Proposed Policy - Example ILM policy

Before activating a new ILM policy:



- Review and carefully simulate the policy. Errors in an ILM policy can cause irreparable data loss.
- Review any changes to the placement of existing replicated and erasure-coded objects. Changing an existing object's location might result in temporary resource issues when the new placements are evaluated and implemented.

See [Managing objects with information lifecycle management](#) for more information.

Review the rules in this policy. If this is a proposed policy, click Simulate to verify the policy and then click Activate to make the policy active.

Reason for change: Example policy

Rules are evaluated in order, starting from the top.

Rule Name	Default	Tenant Account
X-men 		Tenant A (94793396288150002349)
PNGs 		Ignore
Two Copies at Two Data Centers 	✓	Ignore


Simulate
Activate

2. Fare clic su **simulate**.

Viene visualizzata la finestra di dialogo Simulation ILM Policy (Criteri ILM di Simulation).

3. Nel campo **oggetto**, immettere il bucket S3/object-key o il container Swift/object-name per un oggetto di test e fare clic su **simulate**.

Se si specifica un oggetto non acquisito, viene visualizzato un messaggio.



Object

Object 'photos/test' not found.

4. In **risultati di simulazione**, confermare che ogni oggetto è stato associato dalla regola corretta.




Nell'esempio, il `Havok.png` e `Warpath.jpg` Gli oggetti sono stati associati correttamente dalla regola X-MEN. Il `Fullsteam.png` oggetto, che non include `series=x-men` Metadati dell'utente, non corrispondenti alla regola X-MEN ma corrispondenti correttamente alla regola PNG. La regola predefinita non è stata utilizzata perché tutti e tre gli oggetti erano associati da altre regole.

Simulate ILM Policy - Demo

Simulates the active ILM policy or, if there is a proposed ILM policy, simulates the proposed ILM policy. Use this simulation to test the current configuration of ILM rules and determine whether ILM rules copy and place object data as intended.

Object

Simulation Results

Object	Rule Matched	Previous Match	
photos/Havok.png	X-men 		✘
photos/Warpath.jpg	X-men 		✘
photos/Fullsteam.png	PNGs 		✘

Esempi di simulazione delle policy ILM

Questi esempi mostrano come è possibile verificare le regole ILM simulando il criterio ILM prima di attivarlo.

Esempio 1: Verifica delle regole durante la simulazione di una policy ILM proposta

Questo esempio mostra come verificare le regole quando si simula un criterio proposto.

In questo esempio, la **policy ILM di esempio** viene simulata rispetto agli oggetti acquisiti in due bucket. La policy include tre regole, come segue:

- La prima regola, **due copie, due anni per bucket-a**, si applica solo agli oggetti nel bucket-a.
- La seconda regola, **EC objects > 1 MB**, si applica a tutti i bucket, ma ai filtri sugli oggetti superiori a 1 MB.
- La terza regola è quella predefinita e non include alcun filtro.

Viewing Proposed Policy - Example ILM policy

Before activating a new ILM policy:

- Review and carefully simulate the policy. Errors in an ILM policy can cause irreparable data loss.
- Review any changes to the placement of existing replicated and erasure-coded objects. Changing an existing object's location might result in temporary resource issues when the new placements are evaluated and implemented.

See [Managing objects with information lifecycle management](#) for more information.

This policy contains a rule that makes an erasure-coded copy. Confirm that at least one rule uses the Object Size advanced filter to prevent objects that are 200 KB or smaller from being erasure coded. See [Managing objects with information lifecycle management](#) for more information.

Review the rules in this policy. If this is a proposed policy, click Simulate to verify the policy and then click Activate to make the policy active.

Reason for change: Example policy

Rules are evaluated in order, starting from the top.

Rule Name	Default	Tenant Account
Two copies, two years for bucket-a		—
EC objects > 1 MB		—
Two copies, two data centers	✓	—

[Simulate](#) [Activate](#)

Fasi

1. Dopo aver aggiunto le regole e salvato il criterio, fare clic su **simulate**.

Viene visualizzata la finestra di dialogo Simula policy ILM.

2. Nel campo **oggetto**, immettere il bucket S3/object-key o il container Swift/object-name per un oggetto di test e fare clic su **simulate**.

Vengono visualizzati i risultati di Simulation, che mostrano quale regola del criterio corrisponde a ciascun oggetto testato.

Simulate ILM Policy - Example ILM policy

Simulates the active ILM policy or, if there is a proposed ILM policy, simulates the proposed ILM policy. Use this simulation to test the current configuration of ILM rules and determine whether ILM rules copy and place object data as intended.

Object: [Simulate](#)

Simulation Results

Object	Rule Matched	Previous Match	
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		✘

[Finish](#)

3. Verificare che ogni oggetto sia stato associato alla regola corretta.

In questo esempio:

- a. bucket-a/bucket-a object.pdf corrisponde correttamente alla prima regola, che filtra sugli oggetti in bucket-a.
- b. bucket-b/test object greater than 1 MB.pdf è in bucket-b, quindi non corrisponde alla prima regola. Al contrario, è stata associata correttamente dalla seconda regola, che filtra su oggetti

superiori a 1 MB.

- c. `bucket-b/test object less than 1 MB.pdf` i filtri non corrispondono alle prime due regole, quindi verranno posizionati in base alla regola predefinita, che non include filtri.

Esempio 2: Riordinamento delle regole durante la simulazione di una policy ILM proposta

Questo esempio mostra come è possibile riordinare le regole per modificare i risultati durante la simulazione di un criterio.

In questo esempio, viene simulata la policy **Demo**. Questo criterio, che ha lo scopo di trovare oggetti con metadati utente `series=x-men`, include tre regole, come segue:

- La prima regola, **PNG**, filtra i nomi delle chiavi che terminano `.png`.
- La seconda regola, **X-MEN**, si applica solo agli oggetti per il tenant 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.

Viewing Proposed Policy - Demo

Before activating a new ILM policy:

- Review and carefully simulate the policy. Errors in an ILM policy can cause irreparable data loss.
- Review any changes to the placement of existing replicated and erasure-coded objects. Changing an existing object's location might result in temporary resource issues when the new placements are evaluated and implemented.

See [Managing objects with information lifecycle management](#) for more information.

Review the rules in this policy. If this is a proposed policy, click Simulate to verify the policy and then click Activate to make the policy active.

Reason for change: new policy

Rules are evaluated in order, starting from the top.

Rule Name	Default	Tenant Account
PNGs		Ignore
X-men		Tenant A (24365814597594524591)
Two copies two data centers	✓	Ignore

[Simulate](#) [Activate](#)

Fasi

1. Dopo aver aggiunto le regole e salvato il criterio, fare clic su **simulate**.
2. Nel campo **oggetto**, immettere il bucket `S3/object-key` o il container `Swift/object-name` per un oggetto di test e fare clic su **simulate**.

Vengono visualizzati i risultati di Simulation, che indicano che il `Havok.png` L'oggetto è stato associato dalla regola **PNG**.

Simulate ILM Policy - Demo

Simulates the active ILM policy or, if there is a proposed ILM policy, simulates the proposed ILM policy. Use this simulation to test the current configuration of ILM rules and determine whether ILM rules copy and place object data as intended.

Object

Simulation Results

Object	Rule Matched	Previous Match	
photos/Havok.png	PNGs 		

Tuttavia, la regola che il `Havok.png` L'oggetto doveva essere testato come la regola **X-MEN**.

3. Per risolvere il problema, riordinare le regole.
 - a. Fare clic su **fine** per chiudere la pagina Simula policy ILM.
 - b. Fare clic su **Edit** (Modifica) per modificare il criterio.
 - c. Trascinare la regola **X-MEN** all'inizio dell'elenco.

Configure ILM Policy









Create a proposed policy by selecting and arranging rules. Then, save the policy and edit it later as required. Click Simulate to verify a saved policy using test objects. When you are ready, click Activate to make this policy the active ILM policy for the grid.

Name

Reason for change

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.

<input type="button" value="+ Select Rules"/>				
	Default	Rule Name	Tenant Account	Actions
		X-men 	Tenant A (48713995194927812566)	
		PNGs 	—	
	<input checked="" type="checkbox"/>	Two copies, two data centers 	—	

- d. Fare clic su **Save** (Salva).

4. Fare clic su **simulate**.



Gli oggetti precedentemente testati vengono rivalutati in base alla policy aggiornata e vengono visualizzati i risultati della nuova simulazione. Nell'esempio, la colonna Rule Matched mostra che il `Havok.png` L'oggetto ora corrisponde alla regola dei metadati X-MEN, come previsto. La colonna Previous Match (confronto precedente) mostra che la regola PNG ha trovato corrispondenza con l'oggetto nella simulazione precedente.

Simulate ILM Policy - Demo

Simulates the active ILM policy or, if there is a proposed ILM policy, simulates the proposed ILM policy. Use this simulation to test the current configuration of ILM rules and determine whether ILM rules copy and place object data as intended.

Object

Simulation Results

Object	Rule Matched	Previous Match	
photos/Havok.png	X-men 	PNGs 	



Se si rimane nella pagina Configura criteri, è possibile simulare nuovamente un criterio dopo aver apportato modifiche senza dover immettere nuovamente i nomi degli oggetti di test.

Esempio 3: Correzione di una regola durante la simulazione di una policy ILM proposta

Questo esempio mostra come simulare una policy, correggere una regola nella policy e continuare la simulazione.



In questo esempio, viene simulata la policy **Demo**. Questo criterio è destinato a trovare gli oggetti che hanno `series=x-men` metadati dell'utente. Tuttavia, si sono verificati risultati imprevisti durante la simulazione di questa policy rispetto a `Beast.jpg` oggetto. Invece di corrispondere alla regola dei metadati X-MEN, l'oggetto corrisponde alla regola predefinita, due copie di due data center.

Simulate ILM Policy - Demo

Simulates the active ILM policy or, if there is a proposed ILM policy, simulates the proposed ILM policy. Use this simulation to test the current configuration of ILM rules and determine whether ILM rules copy and place object data as intended.


Object

Simulation Results

Object	Rule Matched	Previous Match	
photos/Beast.jpg	Two copies two data centers 		

Quando un oggetto di test non corrisponde alla regola prevista nel criterio, è necessario esaminare ciascuna regola del criterio e correggere eventuali errori.

Fasi

1. Per ogni regola del criterio, visualizzare le impostazioni facendo clic sul nome della regola o sull'icona ulteriori dettagli  in qualsiasi finestra di dialogo in cui viene visualizzata la regola.
2. Esaminare l'account tenant della regola, il tempo di riferimento e i criteri di filtraggio.

In questo esempio, i metadati per la regola X-MEN includono un errore. Il valore dei metadati è stato immesso come "x-men1" invece di "x-men".

X-men

Ingest Behavior: Balanced
Tenant Account: 06846027571548027538
Reference Time: Ingest Time

Filtering Criteria:

Matches all of the following metadata:

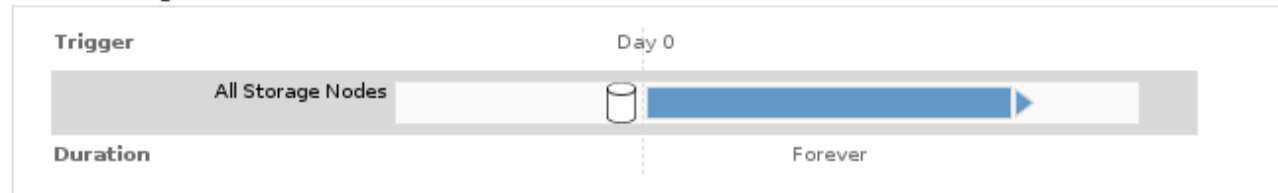
User Metadata

series

equals

x-men1

Retention Diagram:



Close

3. Per risolvere l'errore, correggere la regola come segue:

- Se la regola fa parte del criterio proposto, è possibile clonarla o rimuoverla dal criterio e modificarla.
- Se la regola fa parte del criterio attivo, è necessario clonarla. Non è possibile modificare o rimuovere una regola dal criterio attivo.

Opzione	Descrizione
Clonare la regola	<ol style="list-style-type: none">Selezionare ILM > regole.Selezionare la regola errata e fare clic su Clone.Modificare le informazioni non corrette e fare clic su Salva.Selezionare ILM > Policy.Selezionare la policy proposta e fare clic su Modifica.Fare clic su Seleziona regole.Selezionare la casella di controllo per la nuova regola, deselegionare la casella di controllo per la regola originale e fare clic su Applica.Fare clic su Save (Salva).

Opzione	Descrizione
Modifica della regola	i. Selezionare la policy proposta e fare clic su Modifica . ii. Fare clic sull'icona di eliminazione X Per rimuovere la regola errata, quindi fare clic su Salva . iii. Selezionare ILM > regole . iv. Selezionare la regola errata e fare clic su Modifica . v. Modificare le informazioni non corrette e fare clic su Salva . vi. Selezionare ILM > Policy . vii. Selezionare la policy proposta e fare clic su Modifica . viii. Selezionare la regola corretta, fare clic su Applica e fare clic su Salva .

4. Eseguire nuovamente la simulazione.



Poiché si è allontanati dalla pagina ILM Policies per modificare la regola, gli oggetti precedentemente immessi per la simulazione non vengono più visualizzati. È necessario immettere nuovamente i nomi degli oggetti.

In questo esempio, la regola corretta X-men corrisponde ora a `Beast.jpg` oggetto basato su `series=x-men` metadati dell'utente, come previsto.

Simulate ILM Policy - Demo

Simulates the active ILM policy or, if there is a proposed ILM policy, simulates the proposed ILM policy. Use this simulation to test the current configuration of ILM rules and determine whether ILM rules copy and place object data as intended.

Object

Simulation Results ?

Object	Rule Matched	Previous Match	
photos/Beast.jpg	X-men		X

Attivazione del criterio ILM

Dopo aver aggiunto le regole ILM a un criterio ILM proposto, aver simulato il criterio e aver confermato che si comporta come previsto, è possibile attivare il criterio proposto.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.
- È necessario aver salvato e simulato la policy ILM proposta.



Gli errori in un criterio 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 un nuovo criterio ILM, StorageGRID lo utilizza per gestire tutti gli oggetti, inclusi quelli esistenti e quelli acquisiti di recente. Prima di attivare un nuovo criterio ILM, esaminare le eventuali modifiche apportate al posizionamento degli oggetti replicati e codificati in cancellazione esistenti. La modifica della posizione di un oggetto esistente potrebbe causare problemi di risorse temporanee quando i nuovi posizionamenti vengono valutati e implementati.

A proposito di questa attività

Quando si attiva un criterio ILM, il sistema distribuisce il nuovo criterio a tutti i nodi. Tuttavia, il nuovo criterio attivo potrebbe non essere effettivo fino a quando tutti i nodi della griglia non saranno disponibili per ricevere il nuovo criterio. In alcuni casi, il sistema attende l'implementazione di una nuova policy attiva per garantire che gli oggetti Grid non vengano rimossi accidentalmente.

- Se si apportano modifiche alle policy che aumentano la ridondanza o la durata dei dati, tali modifiche vengono implementate immediatamente. Ad esempio, se si attiva un nuovo criterio che include una regola di tre copie invece di una regola di due copie, tale criterio verrà implementato immediatamente perché aumenta la ridondanza dei dati.
- Se si apportano modifiche alle policy che potrebbero ridurre la ridondanza o la durata dei dati, tali modifiche non verranno implementate fino a quando non saranno disponibili tutti i nodi della griglia. Ad esempio, se si attiva una nuova policy che utilizza una regola di due copie invece di una regola di tre copie, la nuova policy verrà contrassegnata come "Active", ma non avrà effetto fino a quando tutti i nodi non saranno online e disponibili.

Fasi

1. Quando si è pronti ad attivare una policy proposta, selezionarla nella pagina ILM Policies (Criteri ILM) e fare clic su **Activate** (attiva).

Viene visualizzato un messaggio di avviso che richiede di confermare l'attivazione della policy proposta.

Warning

Activate the proposed policy

Errors in an ILM policy can cause irreparable data loss. Review and test the policy carefully before activating. Are you sure you want to activate the proposed policy?

Cancel

OK

Se la regola predefinita per il criterio non mantiene gli oggetti per sempre, nel messaggio di avviso viene visualizzato un messaggio. In questo esempio, il diagramma di conservazione mostra che la regola predefinita elimina gli oggetti dopo 2 anni. È necessario digitare **2** nella casella di testo per riconoscere che gli oggetti non corrispondenti a un'altra regola del criterio verranno rimossi da StorageGRID dopo 2 anni.

⚠ Activate the proposed policy

Errors in an ILM policy can cause irreparable data loss. Review and test the policy carefully before activating.

The default rule in this policy does not retain objects forever. Confirm this is the behavior you want by referring to the retention diagram for the default rule:



Now, complete the following prompt:

Any objects that are not matched by another rule in this policy will be deleted after years.

Are you sure you want to activate the proposed policy?

Cancel

OK

2. Fare clic su **OK**.

Risultato

Quando viene attivata una nuova policy ILM:

- Il criterio viene visualizzato con lo stato policy attivo nella tabella della pagina Criteri ILM. La voce Data di inizio indica la data e l'ora di attivazione della policy.

ILM Policies

Review the proposed, active, and historical policies. You can create, edit, or delete a proposed policy; clone the active policy; or view the details for any policy.

Policy Name	Policy State	Start Date	End Date
<input checked="" type="radio"/> New Policy	Active	2017-07-20 18:49:53 MDT	
<input type="radio"/> Baseline 2 Copies Policy	Historical	2017-07-19 21:24:30 MDT	2017-07-20 18:49:53 MDT

- Il criterio precedentemente attivo viene visualizzato con lo stato del criterio storico. Le voci Data di inizio e Data di fine indicano quando il criterio è diventato attivo e quando non è più in vigore.

Informazioni correlate

["Esempio 6: Modifica di un criterio ILM"](#)

Verifica di un criterio ILM con la ricerca dei metadati degli oggetti

Dopo aver attivato un criterio ILM, è necessario acquisire oggetti di test rappresentativi nel sistema StorageGRID. Quindi, eseguire una ricerca dei metadati degli oggetti per confermare che le copie vengono eseguite come previsto e collocate nelle posizioni corrette.

Di cosa hai bisogno

- È necessario disporre di un identificatore di oggetto, che può essere uno dei seguenti:
 - **UUID**: Identificativo universalmente univoco dell'oggetto. Inserire l'UUID in tutte le lettere maiuscole.

- **CBID**: Identificatore univoco dell'oggetto all'interno di StorageGRID. È possibile ottenere il CBID di un oggetto dal log di audit. Inserire il CBID in tutte le lettere maiuscole.
- **S3 bucket e chiave oggetto**: Quando un oggetto viene acquisito tramite l'interfaccia S3, l'applicazione client utilizza una combinazione di bucket e chiave oggetto per memorizzare e identificare l'oggetto.
- **Swift container and object name**: Quando un oggetto viene acquisito tramite l'interfaccia Swift, l'applicazione client utilizza una combinazione di container e object name per memorizzare e identificare l'oggetto.

Fasi

1. Acquisire l'oggetto.
2. Selezionare **ILM > Object Metadata Lookup**.
3. Digitare l'identificativo dell'oggetto nel campo **Identifier**.

È possibile immettere UUID, CBID, S3 bucket/object-key o Swift container/object-name.

Object Metadata Lookup

Enter the identifier for any object stored in the grid to view its metadata.

Identifier

4. Fare clic su **Cerca**.

Vengono visualizzati i risultati della ricerca dei metadati dell'oggetto. In questa pagina sono elencati i seguenti tipi di informazioni:

- Metadati di sistema, tra cui l'ID oggetto (UUID), il nome dell'oggetto, il nome del contenitore, 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 dell'ultima modifica dell'oggetto.
- Qualsiasi coppia di valori chiave metadati utente personalizzata associata all'oggetto.
- Per gli oggetti S3, qualsiasi coppia chiave-valore tag oggetto associata all'oggetto.
- Per le copie di oggetti replicate, la posizione di storage corrente di ciascuna copia.
- Per le copie di oggetti con codifica erasure, la posizione di storage 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 multiparte, un elenco di segmenti di oggetti che include identificatori di segmenti e dimensioni dei dati. Per gli oggetti con più di 100 segmenti, vengono visualizzati solo i primi 100 segmenti.
- Tutti i metadati degli oggetti nel formato di storage interno non elaborato. Questi metadati raw includono metadati interni del sistema che non sono garantiti per la persistenza dalla release alla release.

Nell'esempio seguente vengono illustrati i risultati della ricerca dei metadati degli oggetti per un oggetto di test S3 memorizzato come due copie replicate.

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": "0x88230E7EC7C10416",
  "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
  "PPTH": "source",
  "META": {
    "BASE": {
      "PAWS": "2",

```

5. Verificare che l'oggetto sia memorizzato nella posizione o nelle posizioni corrette e che si tratti del tipo di copia corretto.



Se l'opzione Audit è attivata, è anche possibile monitorare il registro di audit per il messaggio ORLM Object Rules Met. Il messaggio di audit ORLM può fornire ulteriori 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. È necessario valutarlo da soli. Per ulteriori informazioni, vedere le informazioni relative ai messaggi di audit.

Informazioni correlate

["Esaminare i registri di audit"](#)

["Utilizzare S3"](#)

["USA Swift"](#)

Utilizzo delle regole ILM e delle policy ILM

Una volta create le regole ILM e un criterio ILM, è possibile continuare a utilizzarli, modificandone la configurazione man mano che cambiano i requisiti di storage.

Eliminazione di una regola ILM

Per mantenere gestibile l'elenco delle regole ILM correnti, eliminare eventuali regole ILM che non si intende utilizzare.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

Non è possibile eliminare una regola ILM se è attualmente utilizzata nel criterio attivo o nel criterio proposto. Se è necessario eliminare una regola ILM che utilizza un criterio, è necessario eseguire prima questa procedura:



1. Clonare il criterio attivo o modificare il criterio proposto.
2. Rimuovere la regola ILM dal criterio.
3. Salvare, simulare e attivare il nuovo criterio per assicurarsi che gli oggetti siano protetti come previsto.


Fasi

1. Selezionare **ILM > regole**.
2. Esaminare la voce della tabella relativa alla regola che si desidera rimuovere.

Verificare che la regola non sia utilizzata nel criterio ILM attivo o nel criterio ILM proposto.

3. Se la regola che si desidera rimuovere non è in uso, selezionare il pulsante di opzione e selezionare **Rimuovi**.
4. Selezionare **OK** per confermare che si desidera eliminare la regola ILM.

La regola ILM viene eliminata.

Se si elimina una regola utilizzata in un criterio storico, viene visualizzato  quando si visualizza il criterio, viene visualizzata un'icona che indica che la regola è diventata una regola storica.

Viewing Historical Policy - Example ILM policy

Review the rules in this policy. If this is a proposed policy, click Simulat

Reason for change: new policy

Rules are evaluated in order, starting from the top

Rule Name

Erasure code larger objects

2 copies 2 sites  

This is a historical ILM rule.
Historical rules are rules that
were included a policy and then
edited or deleted after the policy
became historical.



Informazioni correlate

["Creazione di un criterio ILM"](#)

Modifica di una regola ILM

Potrebbe essere necessario modificare una regola ILM per modificare un filtro o un'istruzione di posizionamento.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

A proposito di questa attività

Non è possibile modificare una regola se utilizzata nel criterio ILM proposto o nel criterio ILM attivo. È invece possibile clonare queste regole e apportare le modifiche necessarie alla copia clonata. Inoltre, non è possibile modificare la regola ILM (creare 2 copie) o le regole ILM create prima della versione 10.3 di StorageGRID.



Prima di aggiungere una regola modificata al criterio ILM attivo, tenere presente che una modifica alle istruzioni di posizionamento di un oggetto potrebbe causare un aumento del carico sul sistema.

Fasi

1. Selezionare **ILM > regole**.

Viene visualizzata la pagina ILM Rules (regole ILM). Questa pagina mostra tutte le regole disponibili e indica le regole utilizzate nel criterio attivo o nel criterio proposto.

ILM Rules

Information lifecycle management (ILM) rules determine how and where object data is stored over time. Every object ingested into the StorageGRID Webscale is evaluated against the ILM rules that make up the active ILM policy. Use this page to manage and view ILM rules. You cannot edit or remove an ILM rule that is used by an active or proposed ILM policy.

<input type="button" value="+ Create"/> <input type="button" value="Edit"/> <input type="button" value="Clone"/> <input type="button" value="Remove"/>			
	Name	Used In Active Policy	Used In Proposed Policy
<input type="radio"/>	Make 2 Copies	✓	✓
<input type="radio"/>	PNGs		✓
<input checked="" type="radio"/>	JPGs		
<input type="radio"/>	X-men		✓

2. Selezionare una regola non utilizzata e fare clic su **Modifica**.

Viene visualizzata la procedura guidata Edit ILM Rule (Modifica regola ILM).

Edit ILM Rule Step 1 of 3: Define Basics

Name:

Description:

Tenant Accounts (optional):


Bucket Name:

[Advanced filtering...](#) (0 defined)

3. Completare le pagine della procedura guidata Modifica regola ILM, seguendo la procedura per creare una regola ILM e utilizzare filtri avanzati, se necessario.

Quando si modifica una regola ILM, non è possibile modificarne il nome.

4. Fare clic su **Save** (Salva).

Se si modifica una regola utilizzata in un criterio storico, viene visualizzato  quando si visualizza il criterio, viene visualizzata un'icona che indica che la regola è diventata una regola storica.

Viewing Historical Policy - Example ILM policy

Review the rules in this policy. If this is a proposed policy, click Simulat

Reason for change: new policy

Rules are evaluated in order, starting from the top

Rule Name

Erasure code larger objects

2 copies 2 sites  

This is a historical ILM rule.
Historical rules are rules that
were included a policy and then
edited or deleted after the policy
became historical.



Informazioni correlate

["Creazione di una regola ILM"](#)

["Utilizzo di filtri avanzati nelle regole ILM"](#)

Clonazione di una regola ILM

Non è possibile modificare una regola se utilizzata nel criterio ILM proposto o nel criterio ILM attivo. È invece possibile clonare una regola e apportare le modifiche necessarie alla copia clonata. Quindi, se necessario, è possibile rimuovere la regola originale dal criterio proposto e sostituirla con la versione modificata. Non è possibile clonare una regola ILM se è stata creata utilizzando StorageGRID versione 10.2 o precedente.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

A proposito di questa attività

Prima di aggiungere una regola clonata al criterio ILM attivo, tenere presente che una modifica alle istruzioni di posizionamento di un oggetto potrebbe causare un aumento del carico sul sistema.

Fasi

1. Selezionare **ILM > regole**.

Viene visualizzata la pagina ILM Rules (regole ILM).

ILM Rules

Information lifecycle management (ILM) rules determine how and where object data is stored over time. Every object ingested into the StorageGRID Webscale is evaluated against the ILM rules that make up the active ILM policy. Use this page to manage and view ILM rules. You cannot edit or remove an ILM rule that is used by an active or proposed ILM policy.

<input type="button" value="+ Create"/> <input type="button" value="✎ Edit"/> <input type="button" value="📄 Clone"/> <input type="button" value="✕ Remove"/>			
	Name	Used In Active Policy	Used In Proposed Policy
<input type="radio"/>	Make 2 Copies	✓	✓
<input type="radio"/>	PNGs		✓
<input checked="" type="radio"/>	JPGs		
<input type="radio"/>	X-men		✓

2. Selezionare la regola ILM che si desidera clonare e fare clic su **Clone**.

Viene visualizzata la procedura guidata Create ILM Rule (Crea regola ILM).

3. Aggiornare la regola clonata seguendo la procedura per modificare una regola ILM e utilizzando filtri avanzati.

Quando si clonano una regola ILM, è necessario immettere un nuovo nome.

4. Fare clic su **Save** (Salva).

Viene creata la nuova regola ILM.

Informazioni correlate

["Utilizzo delle regole ILM e delle policy ILM"](#)

["Utilizzo di filtri avanzati nelle regole ILM"](#)

Visualizzazione della coda di attività del criterio ILM

È possibile visualizzare il numero di oggetti presenti nella coda da valutare in base al criterio ILM in qualsiasi momento. È possibile monitorare la coda di elaborazione ILM per determinare le prestazioni del sistema. Una coda di grandi dimensioni potrebbe indicare che il sistema non è in grado di tenere il passo con la velocità di acquisizione, che il carico dalle applicazioni client è troppo elevato o che esiste una condizione anomala.

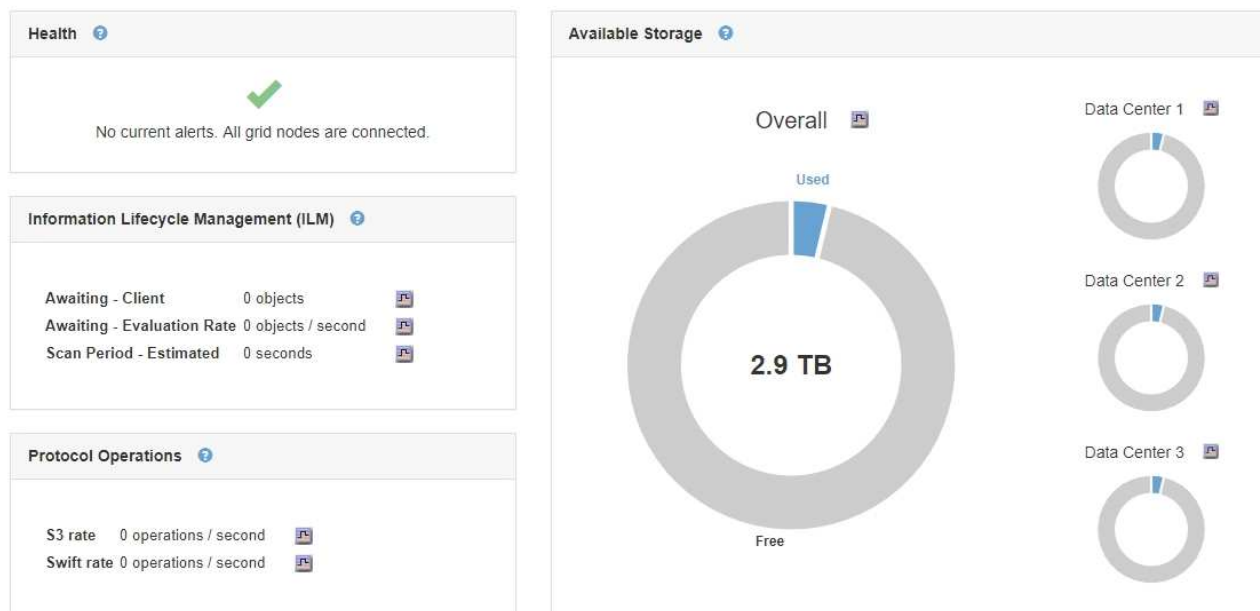
Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.


Fasi

1. Selezionare **Dashboard**.

Dashboard



2. Monitorare la sezione Information Lifecycle Management (ILM).

È possibile fare clic sul punto interrogativo  per visualizzare una descrizione degli elementi di questa sezione.

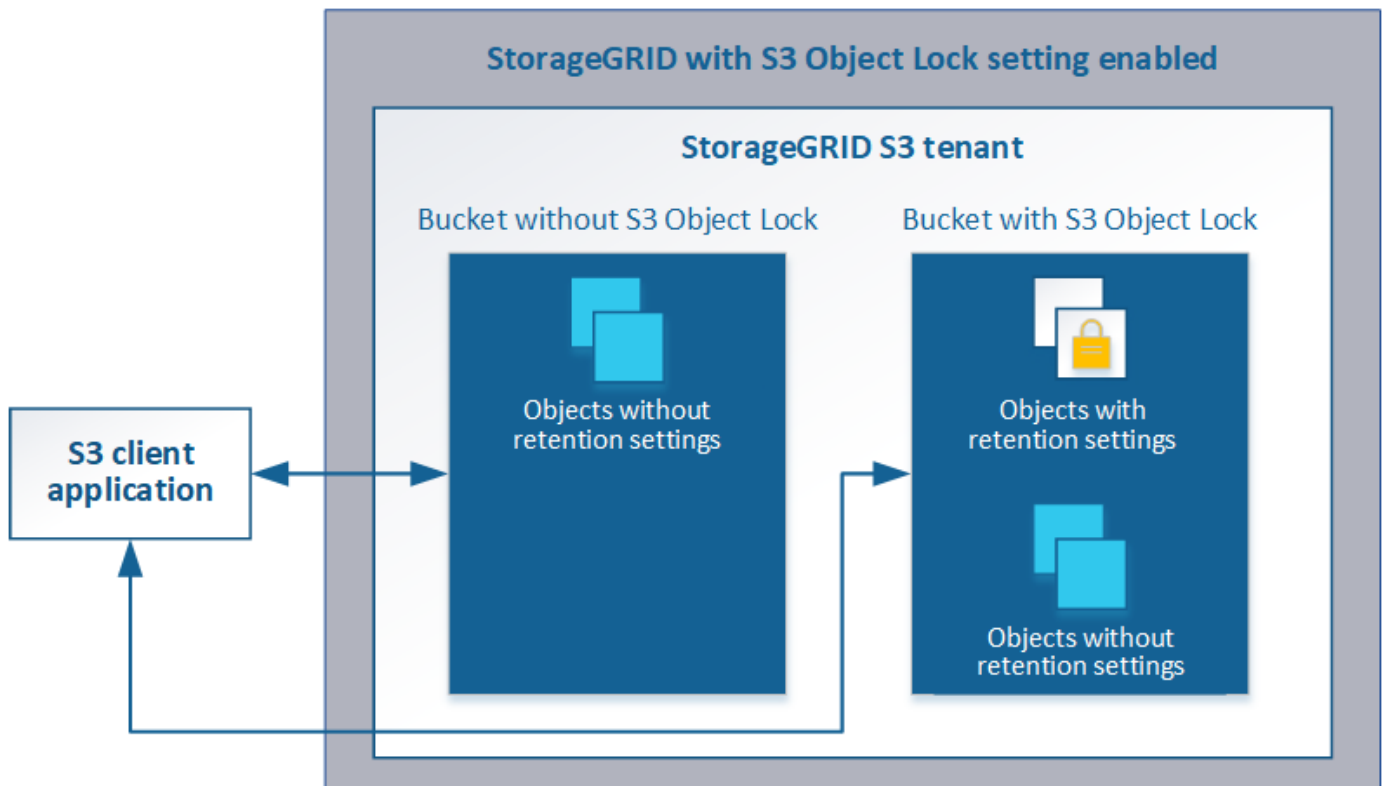
Gestione degli oggetti con S3 Object Lock

In qualità di amministratore di rete, è possibile attivare il blocco oggetti S3 per il sistema StorageGRID e implementare un criterio ILM conforme per garantire che gli oggetti in specifici bucket S3 non vengano cancellati o sovrascritti per un determinato periodo di tempo.

Che cos'è il blocco oggetti S3?

La funzione blocco oggetti StorageGRID S3 è una soluzione di protezione degli oggetti equivalente a blocco oggetti S3 in Amazon Simple Storage Service (Amazon S3).

Come mostrato nella figura, quando l'impostazione globale S3 Object Lock è attivata per un sistema StorageGRID, un account tenant S3 può creare bucket con o senza S3 Object Lock abilitato. Se un bucket ha S3 Object Lock attivato, le applicazioni client S3 possono specificare le impostazioni di conservazione per qualsiasi versione di oggetto in quel bucket. Una versione dell'oggetto deve avere le impostazioni di conservazione specificate per essere protetta da S3 Object Lock.



La funzione blocco oggetto StorageGRID S3 offre una singola modalità di conservazione equivalente alla modalità di conformità Amazon S3. Per impostazione predefinita, una versione dell'oggetto protetto non può essere sovrascritta o eliminata da alcun utente. La funzione blocco oggetti di StorageGRID S3 non supporta una modalità di governance e non consente agli utenti con autorizzazioni speciali di ignorare le impostazioni di conservazione o di eliminare gli oggetti protetti.

Se in un bucket è attivato il blocco oggetti S3, l'applicazione client S3 può specificare una o entrambe le seguenti impostazioni di conservazione a livello di oggetto durante la creazione o l'aggiornamento di un oggetto:

- **Mantieni-fino-data:** Se la data di conservazione di una versione dell'oggetto è futura, l'oggetto può essere recuperato, ma non può essere modificato o cancellato. Come richiesto, è possibile aumentare la data di conservazione di un oggetto fino alla data odierna, ma non è possibile diminuirla.
- **Conservazione legale:** L'applicazione di un blocco legale a una versione oggetto blocca immediatamente tale oggetto. Ad esempio, potrebbe essere necessario sospendere legalmente un oggetto correlato a un'indagine o a una controversia legale. Una conservazione a fini giudiziari non ha una data di scadenza, ma rimane attiva fino a quando non viene esplicitamente rimossa. Le conservazioni legali sono indipendenti dalla conservazione fino alla data odierna.

Per ulteriori informazioni su queste impostazioni, consultare "Using S3 Object lock" in ["Operazioni e limitazioni supportate dall'API REST S3"](#).

Confronto tra blocco oggetti S3 e conformità legacy

La funzionalità blocco oggetti S3 di StorageGRID 11.5 sostituisce la funzionalità di conformità disponibile nelle versioni precedenti di StorageGRID. Poiché la nuova funzione blocco oggetti S3 è conforme ai requisiti di Amazon S3, non è più compatibile con la funzionalità proprietaria di conformità StorageGRID, ora denominata "conformità legacy".

Se in precedenza è stata attivata l'impostazione di conformità globale, la nuova impostazione di blocco oggetti S3 globale viene attivata automaticamente quando si esegue l'aggiornamento a StorageGRID 11.5. Gli utenti del tenant non saranno più in grado di creare nuovi bucket con la conformità abilitata in StorageGRID 11.5; tuttavia, come richiesto, gli utenti del tenant possono continuare a utilizzare e gestire qualsiasi bucket compatibile esistente, che include l'esecuzione delle seguenti attività:

- Acquisizione di nuovi oggetti in un bucket esistente che ha abilitato la conformità legacy.
- Aumento del periodo di conservazione di un bucket esistente che ha abilitato la conformità legacy.
- Modifica dell'impostazione di eliminazione automatica per un bucket esistente che ha abilitato la conformità legacy.
- Mettere un blocco legale su un bucket esistente che ha abilitato la conformità legacy.
- Sollevare un blocco legale.

["Knowledge base di NetApp: Come gestire i bucket conformi alle versioni precedenti in StorageGRID 11.5"](#)

Se è stata utilizzata la funzionalità di conformità legacy in una versione precedente di StorageGRID, fare riferimento alla tabella seguente per informazioni sul confronto con la funzione blocco oggetti S3 di StorageGRID.

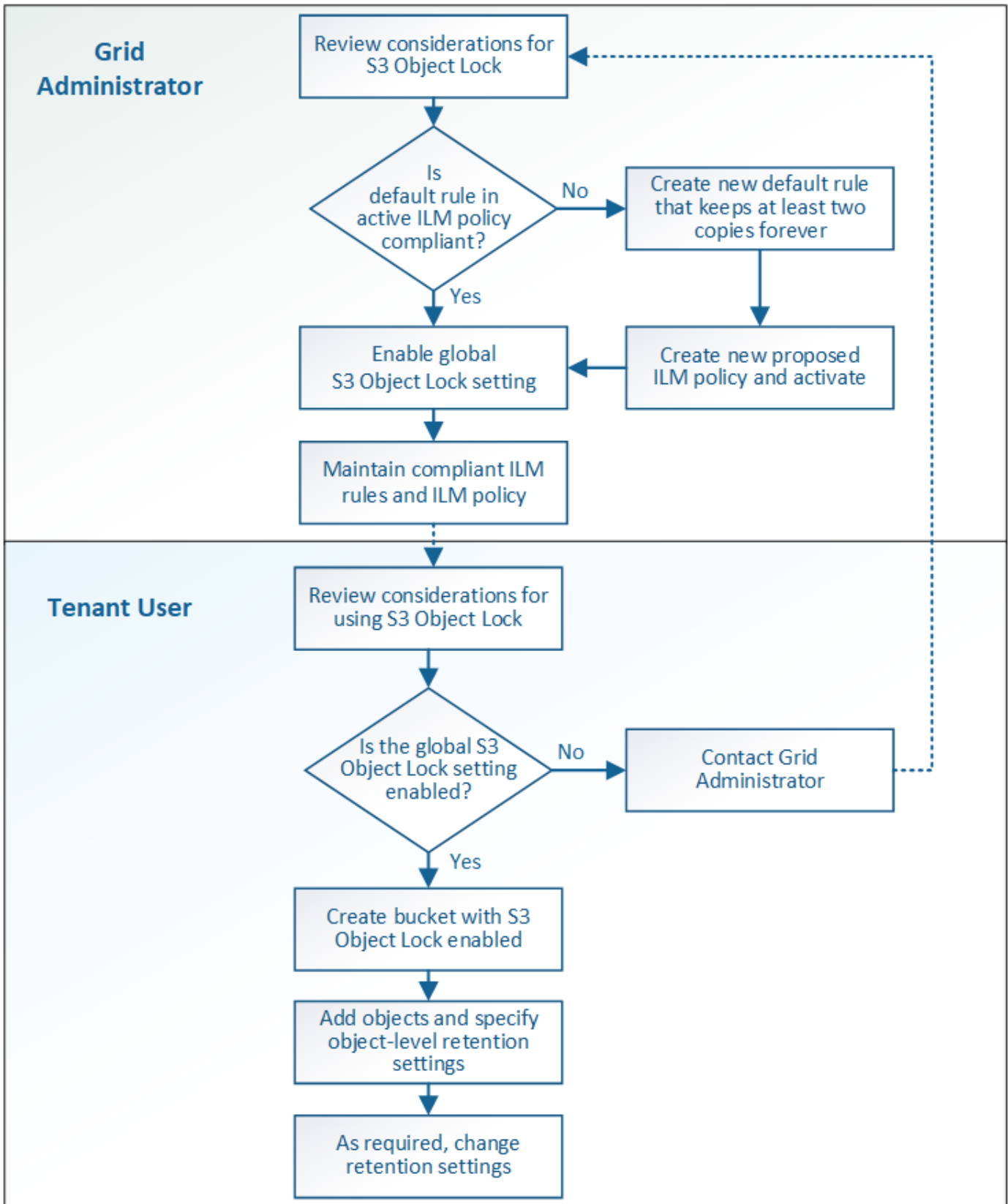
	Blocco oggetti S3 (nuovo)	Compliance (legacy)
In che modo la funzionalità è abilitata a livello globale?	Da Grid Manager, selezionare Configuration > System Settings > S3 Object Lock .	Non più supportato. Nota: se in precedenza è stata attivata l'impostazione di conformità globale, l'impostazione di blocco oggetti S3 globale viene attivata automaticamente quando si esegue l'aggiornamento a StorageGRID 11.5.
In che modo è abilitata la funzione per un bucket?	Gli utenti devono attivare il blocco oggetti S3 quando creano un nuovo bucket utilizzando Tenant Manager, l'API di gestione tenant o l'API REST S3.	Gli utenti non possono più creare nuovi bucket con la funzione Compliance abilitata; tuttavia, possono continuare ad aggiungere nuovi oggetti ai bucket Compliance esistenti.
La versione del bucket è supportata?	Sì. La versione del bucket è obbligatoria e viene attivata automaticamente quando il blocco oggetti S3 è attivato per il bucket.	No La funzionalità Compliance legacy non consente il controllo delle versioni del bucket.
Come viene impostata la conservazione degli oggetti?	Gli utenti possono impostare un periodo di conservazione fino alla data di scadenza per ciascuna versione dell'oggetto.	Gli utenti devono impostare un periodo di conservazione per l'intero bucket. Il periodo di conservazione si applica a tutti gli oggetti nel bucket.

	Blocco oggetti S3 (nuovo)	Compliance (legacy)
Un bucket può avere impostazioni predefinite per la conservazione e la conservazione legale?	No I bucket StorageGRID con blocco oggetti S3 attivato non hanno un periodo di conservazione predefinito. È invece possibile specificare una data di conservazione per ogni versione dell'oggetto.	Sì
È possibile modificare il periodo di conservazione?	Il periodo di conservazione fino alla data di una versione a oggetti può essere aumentato ma non ridotto.	Il periodo di conservazione del bucket può essere aumentato ma non ridotto.
Dove viene controllata la conservazione legale?	Gli utenti possono porre un blocco legale o revocare un blocco legale per qualsiasi versione di oggetto nel bucket.	Un blocco legale viene posizionato sul bucket e influisce su tutti gli oggetti nel bucket.
Quando è possibile eliminare gli oggetti?	Una versione dell'oggetto può essere eliminata dopo aver raggiunto la data di conservazione, presupponendo che l'oggetto non sia sottoposto a conservazione legale.	È possibile eliminare un oggetto dopo la scadenza del periodo di conservazione, presupponendo che il bucket non sia sottoposto a conservazione legale. Gli oggetti possono essere cancellati automaticamente o manualmente.
La configurazione del ciclo di vita del bucket è supportata?	Sì	No

Workflow per blocco oggetti S3

In qualità di amministratore della griglia, è necessario coordinare strettamente gli utenti tenant per garantire che gli oggetti siano protetti in modo da soddisfare i requisiti di conservazione.

Il diagramma del flusso di lavoro mostra i passaggi di alto livello per l'utilizzo di S3 Object Lock. Questi passaggi vengono eseguiti dall'amministratore della griglia e dagli utenti del tenant.



Task di amministrazione della griglia

Come mostra il diagramma del flusso di lavoro, un amministratore della griglia deve eseguire due attività di alto livello prima che gli utenti del tenant S3 possano utilizzare il blocco oggetti S3:

1. Creare almeno una regola ILM conforme e impostarla come regola predefinita nel criterio ILM attivo.
2. Attivare l'impostazione globale S3 Object Lock per l'intero sistema StorageGRID.

Attività utente tenant

Una volta attivata l'impostazione globale S3 Object Lock, i tenant possono eseguire le seguenti attività:

1. Creare bucket con S3 Object Lock attivato.
2. Aggiungere oggetti a tali bucket e specificare i periodi di conservazione a livello di oggetto e le impostazioni di conservazione a livello legale.
3. Se necessario, aggiornare un periodo di conservazione o modificare l'impostazione di conservazione legale per un singolo oggetto.

Informazioni correlate

["Utilizzare un account tenant"](#)

["Utilizzare S3"](#)

Requisiti per il blocco oggetti S3

È necessario esaminare i requisiti per l'attivazione dell'impostazione globale di blocco oggetti S3, i requisiti per la creazione di regole ILM e criteri ILM conformi e le restrizioni applicate da StorageGRID ai bucket e agli oggetti che utilizzano il blocco oggetti S3.

Requisiti per l'utilizzo dell'impostazione globale S3 Object Lock

- È necessario attivare l'impostazione globale S3 Object Lock utilizzando Grid Manager o l'API Grid Management prima che qualsiasi tenant S3 possa creare un bucket con S3 Object Lock attivato.
- L'attivazione dell'impostazione globale S3 Object Lock consente a tutti gli account tenant S3 di creare bucket con S3 Object Lock attivato.
- Dopo aver attivato l'impostazione globale S3 Object Lock (blocco oggetto S3), non è possibile disattivare l'impostazione.
- Non è possibile attivare il blocco oggetti S3 globale a meno che la regola predefinita nel criterio ILM attivo non sia *compliant* (ovvero, la regola predefinita deve essere conforme ai requisiti dei bucket con blocco oggetti S3 attivato).
- Quando l'impostazione blocco oggetto S3 globale è attivata, non è possibile creare un nuovo criterio ILM proposto o attivare un criterio ILM proposto esistente a meno che la regola predefinita del criterio non sia conforme. Una volta attivata l'impostazione globale S3 Object Lock, le pagine ILM Rules (regole ILM) e ILM Policies (Criteri ILM) indicano quali regole ILM sono conformi.

Nell'esempio seguente, la pagina ILM Rules (regole ILM) elenca tre regole che sono conformi ai bucket con S3 Object Lock abilitato.

Name	Compliant	Used In Active Policy	Used In Proposed Policy
Make 2 Copies	✓	✓	
Compliant Rule: EC for objects in bank-records bucket	✓		
2 copies 10 years, Archive forever			
2 Copies 2 Data Centers	✓		

Compliant Rule: EC for objects in bank-records bucket

Description: 2+1 EC at one site

Ingest Behavior: Balanced

Compliant: Yes

Tenant Accounts: Bank of ABC (94793396288150002349)

Bucket Name: equals 'bank-records'

Reference Time: Ingest Time

Requisiti per le regole ILM conformi

Se si desidera attivare l'impostazione blocco oggetti S3 globale, assicurarsi che la regola predefinita nel criterio ILM attivo sia conforme. Una regola conforme soddisfa i requisiti di entrambi i bucket con blocco oggetti S3 attivato e di tutti i bucket esistenti con conformità legacy attivata:

- Deve creare almeno due copie di oggetti replicate o una copia con codice di cancellazione.
- Queste copie devono esistere nei nodi di storage per l'intera durata di ciascuna riga nelle istruzioni di posizionamento.
- Impossibile salvare le copie degli oggetti in un pool di storage cloud.
- Impossibile salvare le copie degli oggetti nei nodi di archiviazione.
- Almeno una riga delle istruzioni di posizionamento deve iniziare al giorno 0, utilizzando **Ingest Time** come ora di riferimento.
- Almeno una riga delle istruzioni di posizionamento deve essere "forever".

Ad esempio, questa regola soddisfa i requisiti dei bucket con blocco oggetti S3 attivato. Memorizza due copie di oggetti replicate dall'ora di inizio (giorno 0) a "forever". Gli oggetti verranno memorizzati nei nodi di storage di due data center.

Compliant rule: 2 replicated copies at 2 sites

Description: 2 replicated copies on Storage Nodes from Day 0 to Forever

Ingest Behavior: Balanced

Compliant: Yes

Tenant Accounts: Bank of ABC (94793396288150002349)

Reference Time: Ingest Time

Filtering Criteria: Matches all objects.

Retention Diagram:

The diagram shows two horizontal bars representing retention periods. The top bar is labeled 'DC1' and the bottom bar is labeled 'DC2'. Both bars start at a point labeled 'Day 0' and extend to the right to a point labeled 'Forever'. A blue arrow points to the right from the 'Day 0' mark on the DC1 bar, and an orange arrow points to the right from the 'Day 0' mark on the DC2 bar.

Requisiti per le policy ILM attive e proposte

Quando l'impostazione blocco oggetto S3 globale è attivata, i criteri ILM attivi e proposti possono includere regole conformi e non conformi.

- La regola predefinita del criterio ILM attivo o proposto deve essere conforme.
- Le regole non conformi si applicano solo agli oggetti nei bucket che non hanno attivato il blocco oggetti S3 o che non hanno la funzione Compliance legacy attivata.
- Le regole conformi possono essere applicate agli oggetti in qualsiasi bucket; non è necessario attivare il blocco oggetti S3 o la conformità legacy per il bucket.

Un criterio ILM conforme potrebbe includere le seguenti tre regole:

1. Regola conforme che crea copie con codifica in cancellazione degli oggetti in un bucket specifico con blocco oggetti S3 attivato. Le copie EC vengono memorizzate nei nodi di storage dal giorno 0 a sempre.
2. Una regola non conforme che crea due copie di oggetti replicate sui nodi di storage per un anno, quindi sposta una copia di oggetti nei nodi di archivio e memorizza la copia per sempre. Questa regola si applica solo ai bucket che non hanno attivato il blocco oggetti S3 o la compliance legacy perché memorizza una sola copia dell'oggetto per sempre e utilizza i nodi di archiviazione.
3. Una regola predefinita e conforme che crea due copie di oggetti replicate sui nodi di storage dal giorno 0 a sempre. Questa regola si applica a qualsiasi oggetto in qualsiasi bucket che non è stato filtrato dalle prime due regole.

Requisiti per i bucket con S3 Object Lock attivato

- Se l'impostazione blocco oggetto S3 globale è attivata per il sistema StorageGRID, è possibile utilizzare Gestione tenant, API di gestione tenant o API REST S3 per creare bucket con blocco oggetto S3 attivato.

Questo esempio di Tenant Manager mostra un bucket con blocco oggetti S3 attivato.

Buckets

Create buckets and manage bucket settings.

1 bucket

Create bucket

Actions

<input type="checkbox"/>	Name	S3 Object Lock	Region	Object Count	Space Used	Date Created
<input type="checkbox"/>	bank-records	✓	us-east-1	0	0 bytes	2021-01-06 16:53:19 MST

← Previous 1 Next →

- Se si intende utilizzare il blocco oggetti S3, è necessario attivare il blocco oggetti S3 quando si crea il bucket. Non è possibile attivare il blocco oggetti S3 per un bucket esistente.
- La versione del bucket è richiesta con S3 Object Lock. Quando il blocco oggetti S3 è attivato per un bucket, StorageGRID attiva automaticamente il controllo delle versioni per quel bucket.
- Dopo aver creato un bucket con S3 Object Lock attivato, non è possibile disattivare S3 Object Lock o sospendere il controllo delle versioni per quel bucket.
- Un bucket StorageGRID con blocco oggetti S3 attivato non ha un periodo di conservazione predefinito. L'applicazione client S3 può invece specificare una data di conservazione e un'impostazione di conservazione legale per ogni versione di oggetto aggiunta a quel bucket.
- La configurazione del ciclo di vita del bucket è supportata per i bucket S3 Object Lifecycle.

- La replica di CloudMirror non è supportata per i bucket con blocco oggetti S3 attivato.

Requisiti per gli oggetti nei bucket con S3 Object Lock attivato

- L'applicazione client S3 deve specificare le impostazioni di conservazione per ciascun oggetto che deve essere protetto da S3 Object Lock.
- È possibile aumentare la data di conservazione per una versione a oggetti, ma non è mai possibile diminuire questo valore.
- Se si riceve la notifica di un'azione legale o di un'indagine normativa in sospeso, è possibile conservare le informazioni pertinenti ponendo un blocco legale su una versione dell'oggetto. Quando una versione dell'oggetto è sottoposta a un blocco legale, non è possibile eliminare tale oggetto da StorageGRID, anche se ha raggiunto la data di conservazione. Non appena la conservazione legale viene revocata, la versione dell'oggetto può essere eliminata se è stata raggiunta la data di conservazione.
- S3 Object Lock richiede l'utilizzo di bucket con versione. Le impostazioni di conservazione si applicano alle singole versioni di oggetti. Una versione a oggetti può avere un'impostazione di conservazione fino alla data e un'impostazione di conservazione legale, una ma non l'altra o nessuna delle due. La specifica di un'impostazione di conservazione fino a data o di conservazione legale per un oggetto 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 attivato

Ogni oggetto salvato in un bucket con S3 Object Lock attivato passa attraverso tre fasi:

1. Acquisizione oggetto

- Quando si aggiunge una versione dell'oggetto a un bucket con S3 Object Lock attivato, l'applicazione client S3 può specificare facoltativamente le impostazioni di conservazione per l'oggetto (conservazione fino alla data, conservazione legale o entrambe). StorageGRID genera quindi metadati per l'oggetto, che includono un UUID (Unique Object Identifier) e la data e l'ora di acquisizione.
- Dopo l'acquisizione di una versione a oggetti con impostazioni di conservazione, i relativi dati e i metadati S3 definiti dall'utente non possono essere modificati.
- StorageGRID memorizza i metadati dell'oggetto indipendentemente dai dati dell'oggetto. Conserva tre copie di tutti i metadati degli oggetti in ogni sito.

2. Conservazione degli oggetti

- StorageGRID memorizza più copie dell'oggetto. Il numero e il tipo esatti di copie e le posizioni di storage sono determinati dalle regole conformi nel criterio ILM attivo.

3. Eliminazione di oggetti

- È possibile eliminare un oggetto una volta raggiunta la data di conservazione.
- Non è possibile eliminare un oggetto sottoposto a conservazione a fini giudiziari.

Informazioni correlate

["Utilizzare un account tenant"](#)

["Utilizzare S3"](#)

["Confronto tra blocco oggetti S3 e conformità legacy"](#)

["Esempio 7: Policy ILM conforme per il blocco oggetti S3"](#)

["Esaminare i registri di audit"](#)

Abilitazione di S3 Object Lock a livello globale

Se un account tenant S3 deve rispettare i requisiti normativi durante il salvataggio dei dati degli oggetti, è necessario attivare il blocco oggetti S3 per l'intero sistema StorageGRID. L'attivazione dell'impostazione globale S3 Object Lock consente a qualsiasi utente del tenant S3 di creare e gestire bucket e oggetti con S3 Object Lock.

Di cosa hai bisogno

- È necessario disporre dell'autorizzazione di accesso root.
- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario aver esaminato il flusso di lavoro S3 Object Lock e comprendere le considerazioni.
- La regola predefinita nel criterio ILM attivo deve essere conforme.

["Creazione di una regola ILM predefinita"](#)

["Creazione di un criterio ILM"](#)

A proposito di questa attività

Un amministratore della griglia deve attivare l'impostazione globale S3 Object Lock per consentire agli utenti tenant di creare nuovi bucket con S3 Object Lock attivato. Una volta attivata, questa impostazione non può essere disattivata.



Se l'impostazione di conformità globale è stata attivata utilizzando una versione precedente di StorageGRID, la nuova impostazione blocco oggetti S3 viene attivata automaticamente quando si esegue l'aggiornamento a StorageGRID versione 11.5. È possibile continuare a utilizzare StorageGRID per gestire le impostazioni dei bucket conformi esistenti; tuttavia, non è più possibile creare nuovi bucket conformi.

["Knowledge base di NetApp: Come gestire i bucket conformi alle versioni precedenti in StorageGRID 11.5"](#)

Fasi

1. Selezionare **Configuration > System Settings > S3 Object Lock**.

Viene visualizzata la pagina S3 Object Lock Settings (Impostazioni blocco oggetti S3).

S3 Object Lock Settings

Enable S3 Object Lock for your entire StorageGRID system if S3 tenant accounts need to satisfy regulatory compliance requirements when saving object data. After this setting is enabled, it cannot be disabled.

S3 Object Lock

Before enabling S3 Object Lock, you must ensure that the default rule in the active ILM policy is compliant. A compliant rule satisfies the requirements of buckets with S3 Object Lock enabled.

- It must create at least two replicated object copies or one erasure-coded copy.
- These copies must exist on Storage Nodes for the entire duration of each line in the placement instructions.
- Object copies cannot be saved on Archive Nodes.
- At least one line of the placement instructions must start at day 0, using Ingest Time as the reference time.
- At least one line of the placement instructions must be "forever".

Enable S3 Object Lock

Apply

Se l'impostazione di conformità globale era stata attivata utilizzando una versione precedente di StorageGRID, la pagina contiene la seguente nota:

The S3 Object Lock setting replaces the legacy Compliance setting. When this setting is enabled, tenant users can create buckets with S3 Object Lock enabled. Tenants who previously created buckets for the legacy Compliance feature can manage their existing buckets, but can no longer create new buckets with legacy Compliance enabled. See [Managing objects with information lifecycle management](#) for information.

2. Selezionare **Enable S3 Object Lock** (attiva blocco oggetti S3).
3. Selezionare **Applica**.

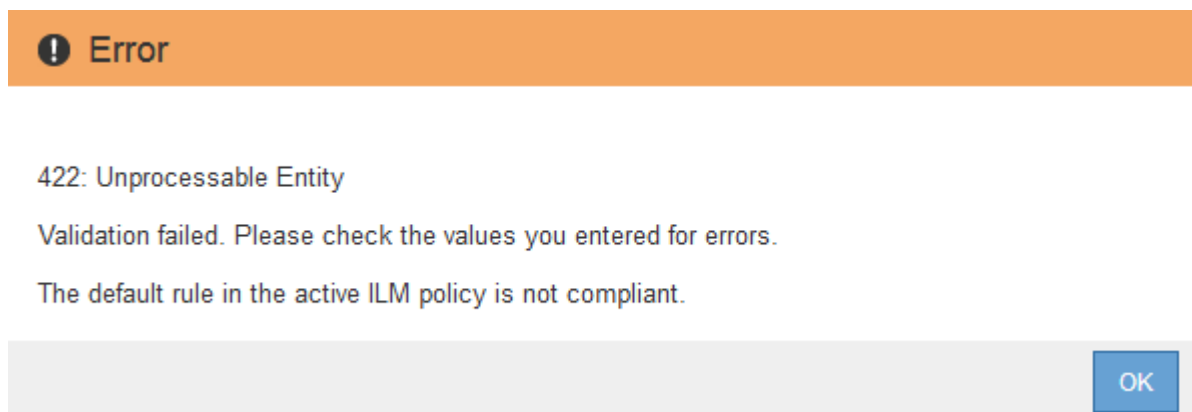
Viene visualizzata una finestra di dialogo di conferma che ricorda che non è possibile disattivare il blocco oggetti S3 dopo averlo attivato.



4. Se si è certi di voler abilitare in modo permanente il blocco oggetti S3 per l'intero sistema, selezionare **OK**.

Quando si seleziona **OK**:

- Se la regola predefinita nel criterio ILM attivo è conforme, il blocco oggetti S3 è ora attivato per l'intera griglia e non può essere disattivato.
- Se la regola predefinita non è conforme, viene visualizzato un errore che indica che è necessario creare e attivare un nuovo criterio ILM che include una regola conforme come regola predefinita. Selezionare **OK** e creare una nuova policy proposta, simularla e attivarla.



Al termine

Dopo aver attivato l'impostazione di blocco oggetti S3 globale, potrebbe essere necessario creare un nuovo criterio ILM. Una volta attivata l'impostazione, il criterio ILM può includere facoltativamente una regola predefinita conforme e una regola predefinita non conforme. Ad esempio, è possibile utilizzare una regola non conforme che non dispone di filtri per gli oggetti nei bucket che non hanno attivato il blocco oggetti S3.

Informazioni correlate

["Creazione di un criterio ILM dopo l'attivazione del blocco oggetti S3"](#)

["Creazione di una regola ILM"](#)

["Creazione di un criterio ILM"](#)

["Confronto tra blocco oggetti S3 e conformità legacy"](#)

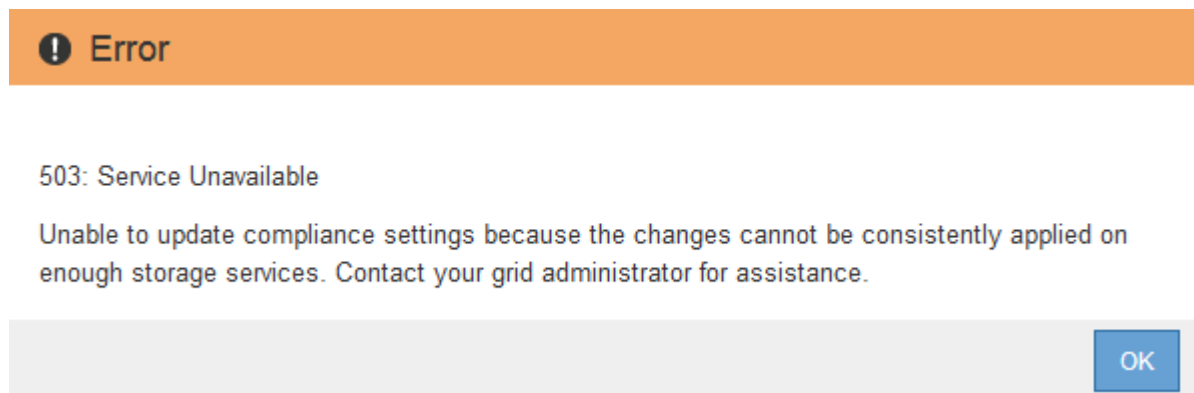
Risoluzione degli errori di coerenza durante l'aggiornamento della configurazione S3 Object Lock o Compliance legacy

Se un sito del data center o più nodi di storage in un sito non sono più disponibili, potrebbe essere necessario aiutare gli utenti del tenant S3 ad applicare le modifiche alla configurazione S3 Object Lock o Compliance legacy.

Gli utenti tenant che hanno bucket con S3 Object Lock (o Compliance legacy) abilitato possono modificare alcune impostazioni. Ad esempio, un utente tenant che utilizza il blocco oggetti S3 potrebbe dover mettere una versione dell'oggetto sotto il blocco legale.

Quando un utente tenant aggiorna le impostazioni di un bucket S3 o di una versione a oggetti, StorageGRID tenta di aggiornare immediatamente il bucket o i metadati dell'oggetto nella griglia. Se il sistema non è in grado di aggiornare i metadati perché un sito del data center o più nodi di storage non sono disponibili, viene visualizzato un messaggio di errore. In particolare:

- Gli utenti di tenant Manager visualizzano il seguente messaggio di errore:



- Gli utenti delle API di gestione tenant e gli utenti delle API S3 ricevono un codice di risposta di 503 Service Unavailable con testo simile.

Per risolvere questo errore, attenersi alla seguente procedura:

1. Tentare di rendere nuovamente disponibili tutti i nodi o i siti di storage il prima possibile.
2. Se non si riesce a rendere disponibile una quantità sufficiente di nodi di storage in ogni sito, contattare il supporto tecnico, che può aiutare a ripristinare i nodi e garantire che le modifiche vengano applicate in modo coerente in tutta la griglia.
3. Una volta risolto il problema sottostante, ricordare all'utente tenant di ripetere le modifiche alla configurazione.

Informazioni correlate

["Utilizzare un account tenant"](#)

"Utilizzare S3"

"Mantieni Ripristina"

Esempio di regole e policy ILM

Puoi utilizzare gli esempi di questa sezione come punto di partenza per le tue regole e policy ILM.

- ["Esempio 1: Regole ILM e policy per lo storage a oggetti"](#)
- ["Esempio 2: Regole ILM e policy per il filtraggio delle dimensioni degli oggetti EC"](#)
- ["Esempio 3: Regole e policy ILM per una migliore protezione dei file di immagine"](#)
- ["Esempio 4: Regole ILM e policy per gli oggetti con versione S3"](#)
- ["Esempio 5: Regole e policy ILM per un comportamento rigoroso di acquisizione"](#)
- ["Esempio 6: Modifica di un criterio ILM"](#)
- ["Esempio 7: Policy ILM conforme per il blocco oggetti S3"](#)

Esempio 1: Regole ILM e policy per lo storage a oggetti

È possibile utilizzare le seguenti regole e policy di esempio come punto di partenza per la definizione di un criterio ILM in modo da soddisfare i requisiti di protezione e conservazione degli oggetti.



Le seguenti regole e policy ILM sono solo esempi. Esistono diversi modi per configurare le regole ILM. Prima di attivare una nuova policy, simulare la policy proposta per confermare che funzionerà come previsto per proteggere il contenuto dalla perdita.

ILM regola 1 per esempio 1: Copia dei dati degli oggetti in due data center

Questa regola ILM di esempio copia i dati degli oggetti in pool di storage in due data center.

Definizione della regola	Valore di esempio
Pool di storage	Due pool di storage, ciascuno in diversi data center, denominati Storage Pool DC1 e Storage Pool DC2.
Nome regola	Due copie di due data center
Tempo di riferimento	Tempo di acquisizione
Posizionamento dei contenuti	Il giorno 0, conserva due copie replicate per sempre, una nello Storage Pool DC1 e una nello Storage Pool DC2.

Configure placement instructions to specify how you want objects matched by this rule to be stored.

Two Copies Two Data Centers

Reference Time Ingest Time ▼

Placements Sort by start day

From day store forever ▼ Add Remove

Type replicated ▼ Location Storage Pool DC1 × Storage Pool DC2 × Add Pool Copies 2 + ×

Specifying multiple storage pools might cause data to be stored at the same site if the pools overlap. See [Managing objects with information lifecycle management](#) for more information.

Retention Diagram Refresh

Cancel
Back
Next

ILM regola 2 per esempio 1: Erasure coding profile with bucket matching

Questa regola ILM di esempio utilizza un profilo di codifica Erasure e un bucket S3 per determinare dove e per quanto tempo l'oggetto viene memorizzato.

Definizione della regola	Valore di esempio
Erasure Coding Profile (erasure Coding Profile)	<ul style="list-style-type: none"> • Un pool di storage in tre data center (tutti e 3 i siti) • Utilizzare uno schema di erasure coding 6+3
Nome regola	EC per i record finanziari del bucket S3
Tempo di riferimento	Tempo di acquisizione
Posizionamento dei contenuti	Per gli oggetti nel bucket S3 denominati finance-records, creare una copia con codice di cancellazione nel pool specificato dal profilo di codifica Erasure. Conserva questa copia per sempre.

Configure placement instructions to specify how you want objects matched by this rule to be stored.

EC for S3 bucket finance-records

Reference Time Ingest Time ▼

Placements ⓘ ⇅ Sort by start day

From day store Add Remove

Type Location Copies + ✕

Retention Diagram ⓘ Refresh

The diagram shows a horizontal timeline starting at 'Day 0'. A trigger icon is placed at Day 0, with a label 'All 3 sites (6 plus 3)' above it. A blue bar extends to the right from Day 0, labeled 'Forever' below it. The x-axis is labeled 'Duration'.

Cancel Back Next

Policy ILM per esempio 1

Il sistema StorageGRID consente di progettare policy ILM sofisticate e complesse; tuttavia, in pratica, la maggior parte delle policy ILM è semplice.

Un tipico criterio ILM per una topologia multi-sito potrebbe includere regole ILM come le seguenti:

- Al momento dell'acquisizione, utilizzare la codifica di cancellazione 6+3 per memorizzare tutti gli oggetti appartenenti al bucket S3 denominato `finance-records` in tre data center.
- Se un oggetto non corrisponde alla prima regola ILM, utilizzare la regola ILM predefinita del criterio, due copie due data center, per memorizzare una copia di tale oggetto in due data center, DC1 e DC2.

Configure ILM Policy

Create a proposed policy by selecting and arranging rules. Then, save the policy and edit it later as required. Click Simulate to verify a saved policy using test objects. When you are ready, click Activate to make this policy the active ILM policy for the grid.

Name

Reason for change

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			
Default	Rule Name	Tenant Account	Actions
	EC for S3 bucket finance-records	Ignore	
<input checked="" type="checkbox"/>	Two Copies Two Data Centers	Ignore	

Esempio 2: Regole ILM e policy per il filtraggio delle dimensioni degli oggetti EC

È possibile utilizzare le seguenti regole e policy di esempio come punti di partenza per definire un criterio ILM che filtra in base alle dimensioni dell'oggetto per soddisfare i requisiti EC consigliati.



Le seguenti regole e policy ILM sono solo esempi. Esistono diversi modi per configurare le regole ILM. Prima di attivare una nuova policy, simulare la policy proposta per confermare che funzionerà come previsto per proteggere il contenuto dalla perdita.

ILM regola 1 per esempio 2: Utilizzare EC per tutti gli oggetti di dimensioni superiori a 200 KB

Questo esempio di cancellazione della regola ILM codifica tutti gli oggetti di dimensioni superiori a 200 KB (0.20 MB).

Definizione della regola	Valore di esempio
Nome regola	Solo oggetti EC > 200 KB
Tempo di riferimento	Tempo di acquisizione
Filtro avanzato per le dimensioni dell'oggetto	Dimensione oggetto (MB) maggiore di 0.20
Posizionamento dei contenuti	Creare una copia 2+1 con codifica per la cancellazione utilizzando tre siti

Advanced Filtering

Use advanced filtering if you want a rule to apply only to specific objects. You can filter objects based on their system metadata, user metadata, or object tags (S3 only). When objects are evaluated, the rule is applied if the object's metadata matches the criteria in the advanced filter.

EC only objects > 200 KB

Matches all of the following metadata:

Object Size (MB)	greater than	0.2	+ x
+ x			

Cancel Remove Filters Save

Le istruzioni di posizionamento specificano che una copia 2+1 con codice di cancellazione deve essere creata utilizzando tutti e tre i siti.

EC image files > 200 KB

Reference Time: Ingest Time

Placements Sort by start day

From day: 0 store: forever Add Remove

Type: erasure coded Location: All 3 sites (2 plus 1) Copies: 1 + x

Retention Diagram Refresh

The diagram shows a horizontal bar representing the retention period. The bar starts at 'Day 0' and is labeled 'All 3 sites (2 plus 1)'. The duration of the bar is 'Forever'. A 'Trigger' icon is shown at the start of the bar.

ILM regola 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 è la seconda regola del criterio. Poiché la regola ILM 1, ad esempio 2, filtra tutti gli oggetti di dimensioni superiori a 200 KB, la regola ILM 2, ad esempio 2, si applica solo agli oggetti di dimensioni inferiori o pari a 200 KB.

Definizione della regola	Valore di esempio
Nome regola	Due copie replicate
Tempo di riferimento	Tempo di acquisizione

Definizione della regola	Valore di esempio
Filtro avanzato per le dimensioni dell'oggetto	Nessuno
Posizionamento dei contenuti	Creare due copie replicate e salvarle in due data center, DC1 e DC2

Create ILM Rule Step 2 of 3: Define Placements

Configure placement instructions to specify how you want objects matched by this rule to be stored.

Two replicated copies

Reference Time:

Placements Sort by start day

From day: store:

Type: Location: Copies:

Specifying multiple storage pools might cause data to be stored at the same site if the pools overlap. See [Managing objects with information lifecycle management](#) for more information.

Retention Diagram Refresh

Critério ILM per esempio 2: Utilizzare EC per oggetti di dimensioni superiori a 200 KB

In questo esempio di policy, gli oggetti di dimensioni superiori a 200 KB vengono sottoposti a erasure coding. Vengono create due copie replicate di tutti gli altri oggetti.

Questo esempio di policy ILM include le seguenti regole ILM:

- Erasure coding di tutti gli oggetti di dimensioni superiori a 200 KB.
- Se un oggetto non corrisponde alla prima regola ILM, utilizzare la regola ILM predefinita per creare due copie replicate di tale oggetto. Poiché gli oggetti di dimensioni superiori a 200 KB sono stati filtrati dalla regola 1, la regola 2 si applica solo agli oggetti di dimensioni inferiori o pari a 200 KB.

Configure ILM Policy

Create a proposed policy by selecting and arranging rules. Then, save the policy and edit it later as required. Click Simulate to verify a saved policy using test objects. When you are ready, click Activate to make this policy the active ILM policy for the grid.

Name

Reason for change

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.

Default	Rule Name	Tenant Account	Actions
	EC only objects > 200 KB	Ignore	✘
✓	Two replicated copies	Ignore	✘

Esempio 3: Regole e policy ILM per una migliore protezione dei file di immagine

È possibile utilizzare le seguenti regole e policy di esempio per garantire che le immagini di dimensioni superiori a 200 KB vengano erasure coded e che vengano eseguite tre copie di immagini più piccole.



Le seguenti regole e policy ILM sono solo esempi. Esistono diversi modi per configurare le regole ILM. Prima di attivare una nuova policy, simulare la policy proposta per confermare che funzionerà come previsto per proteggere il contenuto dalla perdita.

ILM regola 1 per esempio 3: Utilizzare EC per file di immagine di dimensioni superiori a 200 KB

Questa regola ILM di esempio utilizza un filtro avanzato per eseguire la cancellazione di tutti i file di immagine di dimensioni superiori a 200 KB.

Definizione della regola	Valore di esempio
Nome regola	File immagine EC > 200 KB
Tempo di riferimento	Tempo di acquisizione
Filtro avanzato per i metadati utente	Il tipo di metadati utente equivale ai file di immagine
Filtro avanzato per le dimensioni dell'oggetto	Dimensione oggetto (MB) maggiore di 0.2

Definizione della regola	Valore di esempio
Posizionamento dei contenuti	Creare una copia 2+1 con codifica per la cancellazione utilizzando tre siti

Advanced Filtering

Use advanced filtering if you want a rule to apply only to specific objects. You can filter objects based on their system metadata, user metadata, or object tags (S3 only). When objects are evaluated, the rule is applied if the object's metadata matches the criteria in the advanced filter.

EC image files > 200 KB

Matches all of the following metadata:

User Metadata	type	equals	image	+ x
Object Size (MB)	greater than		0.2	+ x
+ x				

Cancel

Remove Filters

Save

Poiché questa regola è configurata come prima regola del criterio, l'istruzione di posizionamento della codifica di cancellazione si applica solo alle immagini di dimensioni superiori a 200 KB.

EC image files > 200 KB

Reference Time Ingest Time

Placements Sort by start day

From day store forever Add Remove

Type erasure coded Location All 3 sites (2 plus 1) Copies + x

Retention Diagram Refresh

Trigger Day 0

All 3 sites (2 plus 1)

Duration Forever

ILM regola 2 per esempio 3: Replica 3 copie per tutti i file immagine rimanenti

Questa regola ILM di esempio utilizza un filtro avanzato per specificare che i file di immagine devono essere replicati.

Definizione della regola	Valore di esempio
Nome regola	3 copie per i file di immagine
Tempo di riferimento	Tempo di acquisizione
Filtro avanzato per i metadati utente	Il tipo di metadati utente equivale ai file di immagine
Posizionamento dei contenuti	Creare 3 copie replicate in tutti i nodi di storage

Advanced Filtering

Use advanced filtering if you want a rule to apply only to specific objects. You can filter objects based on their system metadata, user metadata, or object tags (S3 only). When objects are evaluated, the rule is applied if the object's metadata matches the criteria in the advanced filter.

3 copies for image files

Matches all of the following metadata:

User Metadata type equals image + x

+ x

Cancel

Remove Filters

Save

Poiché la prima regola del criterio ha già trovato corrispondenza con file di immagine di dimensioni superiori a 200 KB, queste istruzioni di posizionamento si applicano solo ai file di immagine di dimensioni pari o inferiori a 200 KB.

3 copies for image files

Reference Time:

Placements Sort by start day

From day: store:

Type: Location: Copies:

Specifying multiple storage pools might cause data to be stored at the same site if the pools overlap. See [Managing objects with information lifecycle management](#) for more information.

Retention Diagram Refresh

Trigger: Day 0

Duration: Forever

Buttons: Cancel, Back, Next

Policy ILM per esempio 3: Migliore protezione per i file di immagine

In questo esempio, il criterio ILM utilizza tre regole ILM per creare un criterio che erasure i file immagine di dimensioni superiori a 200 KB (0.2 MB), crea copie replicate per i file immagine di dimensioni pari o inferiori a 200 KB e crea due copie replicate per i file non immagine.

Questo esempio di policy ILM include regole che eseguono le seguenti operazioni:

- Erasure coding tutti i file di immagine di dimensioni superiori a 200 KB.
- Creare tre copie dei file immagine rimanenti (ovvero, immagini di dimensioni pari o inferiori a 200 KB).
- Applicare la regola predefinita a tutti gli oggetti rimanenti (ovvero tutti i file non immagine).

Viewing Active Policy - Better protection for image files

Review the rules in this policy. If this is a proposed policy, click Simulate to verify the policy and then click Activate to make the policy active.

Reason for change: ILM policy for example 3

Rules are evaluated in order, starting from the top.

Rule Name	Default	Tenant Account
EC only objects > 200 KB		Ignore
3 copies for image files		Ignore
Make 2 Copies	✓	Ignore

Buttons: Simulate, Activate

Esempio 4: Regole ILM e policy per gli oggetti con versione S3

Se si dispone di un bucket S3 con la versione attivata, è possibile gestire le versioni degli oggetti non correnti includendo regole nella policy ILM che utilizzano **tempo non corrente** come tempo di riferimento.

Come illustrato in questo esempio, è possibile controllare la quantità di storage utilizzata dagli oggetti con versione utilizzando istruzioni di posizionamento diverse per le versioni degli oggetti non correnti.



Le seguenti regole e policy ILM sono solo esempi. Esistono diversi modi per configurare le regole ILM. Prima di attivare una nuova policy, simulare la policy proposta per confermare che funzionerà come previsto per proteggere il contenuto dalla perdita.



Se si creano criteri ILM per gestire le versioni degli oggetti non correnti, tenere presente che è necessario conoscere l'UUID o il CBID della versione dell'oggetto per simulare il criterio. Per trovare UUID e CBID di un oggetto, utilizzare Object Metadata Lookup (Ricerca metadati oggetto) mentre l'oggetto è ancora aggiornato.

Informazioni correlate

["Modalità di eliminazione degli oggetti con versione S3"](#)

["Verifica di un criterio ILM con la ricerca dei metadati degli oggetti"](#)

ILM regola 1 per esempio 4: Salva tre copie per 10 anni

Questa regola ILM di esempio memorizza una copia di ciascun oggetto in tre data center per 10 anni.

Questa regola si applica a tutti gli oggetti, indipendentemente dal fatto che siano con versione.

Definizione della regola	Valore di esempio
Pool di storage	Tre pool di storage, ciascuno in diversi data center, denominati DC1, DC2 e DC3.
Nome regola	Tre copie dieci anni
Tempo di riferimento	Tempo di acquisizione
Posizionamento dei contenuti	Il giorno 0, conserva tre copie replicate per 10 anni (3,652 giorni), una in DC1, una in DC2 e una in DC3. Alla fine dei 10 anni, eliminare tutte le copie dell'oggetto.

Configure placement instructions to specify how you want objects matched by this rule to be stored.

Three Copies Ten Years
 Save three copies for ten years

Reference Time Ingest Time

Placements ↑↓ Sort by start day

From day 0 store for 3652 days Add Remove

Type replicated Location DC1 × DC2 × DC3 × Add Pool Copies 3 + ×

Specifying multiple storage pools might cause data to be stored at the same site if the pools overlap. See [Managing objects with information lifecycle management](#) for more information.

Retention Diagram Refresh

Trigger Day 0 Day 3652

Duration 3652 days Forever

Cancel
Back
Next

ILM regola 2 per esempio 4: Salva due copie di 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 le versioni non correnti. Questa regola utilizza l'opzione **ora non corrente** per il tempo di riferimento.

In questo esempio, vengono memorizzate solo due copie delle versioni non correnti, che verranno memorizzate per due anni.

Definizione della regola	Valore di esempio
Pool di storage	Due pool di storage, ciascuno in diversi data center, denominati DC1 e DC2.
Nome regola	Versioni non correnti: Due copie per due anni
Tempo di riferimento	Ora non corrente
Posizionamento dei contenuti	Il giorno 0 relativo all'ora non corrente (ovvero, a partire dal giorno in cui la versione dell'oggetto diventa la versione non corrente), mantenere due copie replicate delle versioni dell'oggetto non correnti per 2 anni (730 giorni), una in DC1 e una in DC2. Alla fine di 2 anni, eliminare le versioni non aggiornate.

Noncurrent Versions: Two Copies Two Years
Save two copies of noncurrent versions for two years

Reference Time: ▾

Placements ⓘ ⇅ Sort by start day

From day: store for days Add Remove

Type: Location: Copies: + x

Specifying multiple storage pools might cause data to be stored at the same site if the pools overlap. See [Managing objects with information lifecycle management](#) for more information.

Retention Diagram ⓘ 🔄 Refresh

The diagram shows two horizontal bars representing retention periods. The top bar is labeled 'DC1' and has a blue segment from 'Day 0' to 'Year 2'. The bottom bar is labeled 'DC2' and has an orange segment from 'Day 0' to 'Year 2'. Below the bars, the duration is indicated as '2 years' and 'Forever'. A 'Trigger' icon is shown at 'Day 0' and 'Year 2'.

Policy ILM per esempio 4: Oggetti con versione S3

Se si desidera gestire le versioni precedenti di un oggetto in modo diverso dalla versione corrente, le regole che utilizzano **ora non corrente** come ora di riferimento devono essere visualizzate nel criterio ILM prima delle regole che si applicano alla versione corrente dell'oggetto.

Un criterio ILM per gli oggetti con versione S3 potrebbe includere regole ILM come le seguenti:

- Mantenere 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 dell'ora non corrente devono essere visualizzate nel criterio prima delle regole applicabili alla versione corrente dell'oggetto. In caso contrario, le versioni degli oggetti non correnti non verranno mai associate alla regola dell'ora non corrente.

- Al momento dell'acquisizione, creare tre copie replicate e memorizzare una copia in ciascuno dei tre data center. Conserva le copie della versione corrente dell'oggetto per 10 anni.

Configure ILM Policy

Create a proposed policy by selecting and arranging rules. Then, save the policy and edit it later as required. Click Simulate to verify a saved policy using test objects. When you are ready, click Activate to make this policy the active ILM policy for the grid.

Name

Reason for change

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.

Default	Rule Name	Tenant Account	Actions
	Noncurrent Versions: Two Copies Two Years	Ignore	
<input checked="" type="checkbox"/>	Three Copies Ten Years	Ignore	

The default ILM rule in this policy does not retain objects forever. Confirm this is the behavior you expect. Otherwise, any objects that are not matched by another rule will be deleted after 3652 days.

Quando si simula il criterio di esempio, si prevede che gli oggetti di test vengano valutati come segue:

- Qualsiasi versione dell'oggetto non corrente verrebbe associata dalla prima regola. Se una versione dell'oggetto non corrente ha più di 2 anni, viene eliminata in modo permanente da ILM (tutte le copie della versione non corrente vengono rimosse dalla griglia).



Per simulare versioni di oggetti non correnti, è necessario utilizzare UUID o CBID di tale versione. Mentre l'oggetto è ancora aggiornato, è possibile utilizzare Object Metadata Lookup (Ricerca metadati oggetto) per trovare UUID e CBID.

- La seconda regola corrisponde alla versione corrente dell'oggetto. Quando la versione corrente dell'oggetto è stata memorizzata per 10 anni, il processo ILM aggiunge un indicatore di eliminazione come versione corrente dell'oggetto e rende la versione precedente dell'oggetto "non aggiornata". La prossima volta che si verifica la valutazione ILM, questa versione non corrente corrisponde alla prima regola. Di conseguenza, la copia di DC3 viene eliminata e le due copie di DC1 e DC2 vengono conservate per altri 2 anni.

Informazioni correlate

["Verifica di un criterio ILM con la ricerca dei metadati degli oggetti"](#)

Esempio 5: Regole e policy ILM per un comportamento rigoroso di acquisizione

È possibile utilizzare un filtro di posizione e il rigoroso comportamento di acquisizione in una regola per impedire che gli oggetti vengano salvati in una determinata posizione del data center.

In questo esempio, un tenant con sede a Parigi non desidera memorizzare alcuni oggetti al di fuori dell'UE a causa di problemi normativi. Altri oggetti, inclusi tutti gli oggetti di altri account tenant, possono essere memorizzati nel data center di Parigi o nel data center statunitense.



Le seguenti regole e policy ILM sono solo esempi. Esistono diversi modi per configurare le regole ILM. Prima di attivare una nuova policy, simulare la policy proposta per confermare che funzionerà come previsto per proteggere il contenuto dalla perdita.

Informazioni correlate

["Modalità di acquisizione degli oggetti"](#)

["Fase 3 di 3: Definizione del comportamento di acquisizione"](#)

ILM regola 1 per esempio 5: Ingest rigoroso per garantire il data center di Parigi

Questa regola ILM di esempio utilizza il comportamento rigoroso dell'acquisizione per garantire che gli oggetti salvati da un tenant basato su Parigi nei bucket S3 con la regione impostata su ue-West-3 (Parigi) non vengano mai memorizzati 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
Account tenant	Tenant di Parigi
Filtraggio avanzato	Il vincolo di posizione equivale a eu-West-3
Pool di storage	DC1 (Parigi)
Nome regola	Un ingest rigoroso per garantire il data center di Parigi
Tempo di riferimento	Tempo di acquisizione
Posizionamento dei contenuti	Il giorno 0, conserva due copie replicate per sempre in DC1 (Parigi)
Comportamento di acquisizione	Rigoroso. Utilizza sempre le posizioni di questa regola per l'acquisizione. L'acquisizione non riesce se non è possibile memorizzare due copie dell'oggetto nel data center di Parigi.

Strict ingest to guarantee Paris data center

Description: Strict ingest to guarantee Paris data center
Ingest Behavior: Strict
Tenant Account: Paris tenant (25580610012441844135)
Reference Time: Ingest Time
Filtering Criteria:

Matches all of the following metadata:

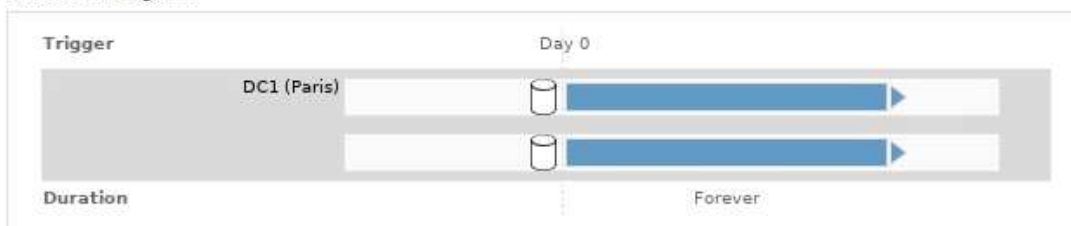
System Metadata

Location Constraint (S3 only)

equals

eu-west-3

Retention Diagram:



ILM regola 2 per esempio 5: Acquisizione bilanciata per altri oggetti

Questa regola ILM di esempio utilizza il comportamento di acquisizione bilanciata per fornire un'efficienza ILM ottimale per qualsiasi oggetto non associato alla prima regola. Verranno memorizzate due copie di tutti gli oggetti corrispondenti a questa regola: Una nel data center degli Stati Uniti e una nel data center di Parigi. Se la regola non può essere soddisfatta immediatamente, le copie temporanee vengono memorizzate in qualsiasi posizione disponibile.

Questa regola si applica agli oggetti che appartengono a qualsiasi tenant e a qualsiasi area.

Definizione della regola	Valore di esempio
Account tenant	Ignorare
Filtraggio avanzato	<i>Non specificato</i>
Pool di storage	DC1 (Parigi) e DC2 (Stati Uniti)
Nome regola	2 copie di 2 data center
Tempo di riferimento	Tempo di acquisizione
Posizionamento dei contenuti	Il giorno 0, conserva due copie replicate per sempre in due data center
Comportamento di acquisizione	Bilanciato. Gli oggetti che corrispondono a questa regola vengono posizionati in base alle istruzioni di posizionamento della regola, se possibile. In caso contrario, le copie temporanee vengono eseguite in qualsiasi ubicazione disponibile.

2 Copies 2 Data Centers

Description: 2 Copies 2 Data Centers

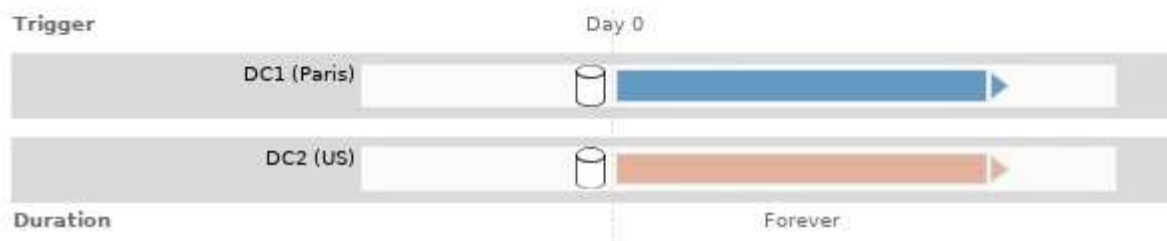
Ingest Behavior: Balanced

Reference Time: Ingest Time

Filtering Criteria:

Matches all objects.

Retention Diagram:



Policy ILM per esempio 5: Combinazione di comportamenti di acquisizione

Il criterio ILM di esempio include due regole che hanno comportamenti di acquisizione diversi.

Un criterio ILM che utilizza due diversi comportamenti di acquisizione potrebbe includere regole ILM come le seguenti:

- Memorizzare 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. Non eseguire l'acquisizione se il data center di Parigi non è disponibile.
- Memorizzare tutti gli altri oggetti (inclusi quelli che appartengono al tenant di Parigi ma che hanno una regione bucket diversa) nel data center statunitense e nel data center di Parigi. Se le istruzioni di posizionamento non possono essere soddisfatte, eseguire copie temporanee in qualsiasi ubicazione disponibile.

Configure ILM Policy

Create a proposed policy by selecting and arranging rules. Then, save the policy and edit it later as required. Click Simulate to verify a saved policy using test objects. When you are ready, click Activate to make this policy the active ILM policy for the grid.

Name

Reason for change

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.

Default	Rule Name	Tenant Account	Actions
	Strict ingest to guarantee Paris data center	Paris tenant (25580610012441844135)	
<input checked="" type="checkbox"/>	2 Copies 2 Data Centers	Ignore	

Quando si simula il criterio di esempio, si prevede che gli oggetti di test 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 memorizzati nel data center di Parigi. Poiché la prima regola utilizza un ingest rigoroso, questi oggetti non vengono mai memorizzati nel data center statunitense. Se i nodi di storage nel data center di Parigi non sono disponibili, l'acquisizione non riesce.
- Tutti gli altri oggetti sono abbinati dalla seconda regola, inclusi gli oggetti che appartengono al tenant di Parigi e che non hanno la regione del bucket S3 impostata su eu-West-3. Una copia di ciascun oggetto viene salvata in ciascun data center. Tuttavia, poiché la seconda regola utilizza l'acquisizione bilanciata, se un data center non è disponibile, vengono salvate due copie temporanee in qualsiasi posizione disponibile.

Esempio 6: Modifica di un criterio ILM

Potrebbe essere necessario creare e attivare una nuova policy ILM se la protezione dei dati deve cambiare o se si aggiungono nuovi siti.

Prima di modificare una policy, è necessario comprendere in che modo le modifiche apportate ai posizionamenti ILM possono influire temporaneamente sulle prestazioni generali di un sistema StorageGRID.

In questo esempio, è stato aggiunto un nuovo sito StorageGRID in un'espansione e il criterio ILM attivo deve essere rivisto per memorizzare i dati nel nuovo sito.



Le seguenti regole e policy ILM sono solo esempi. Esistono diversi modi per configurare le regole ILM. Prima di attivare una nuova policy, simulare la policy proposta per confermare che funzionerà come previsto per proteggere il contenuto dalla perdita.

In che modo la modifica di un criterio ILM influisce sulle performance

Quando si attiva un nuovo criterio ILM, le prestazioni del sistema StorageGRID potrebbero risentirne temporaneamente, soprattutto se le istruzioni di posizionamento nel nuovo criterio richiedono lo spostamento

di molti oggetti esistenti in nuove posizioni.



Quando si attiva un nuovo criterio ILM, StorageGRID lo utilizza per gestire tutti gli oggetti, inclusi quelli esistenti e quelli acquisiti di recente. Prima di attivare un nuovo criterio ILM, esaminare le eventuali modifiche apportate al posizionamento degli oggetti replicati e codificati in cancellazione esistenti. La modifica della posizione di un oggetto esistente potrebbe causare problemi di risorse temporanee quando i nuovi posizionamenti vengono valutati e implementati.

I tipi di modifiche ai criteri ILM che possono influire temporaneamente sulle prestazioni di StorageGRID includono:

- Applicazione di un profilo di codifica Erasure diverso agli oggetti con codifica erasure esistenti.



StorageGRID considera ogni profilo di codifica Erasure unico e non riutilizza i frammenti di codifica Erasure quando viene utilizzato un nuovo profilo.

- Modifica del tipo di copie richieste per gli oggetti esistenti; ad esempio, conversione di una grande percentuale di oggetti replicati in oggetti con codifica per la cancellazione.
- Spostamento di copie di oggetti esistenti in una posizione completamente diversa; ad esempio, spostamento di un numero elevato di oggetti da o verso un Cloud Storage Pool o da o verso un sito remoto.

Informazioni correlate

["Creazione di un criterio ILM"](#)

Policy ILM attiva ad 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.

ILM Policies

Review the proposed, active, and historical policies. You can create, edit, or delete a proposed policy; clone the active policy; or view the details for any policy.

Policy Name	Policy State	Start Date	End Date
<input checked="" type="radio"/> Data Protection for Two Sites	Active	2020-06-10 16:42:09 MDT	
<input type="radio"/> Baseline 2 Copies Policy	Historical	2020-06-09 21:48:34 MDT	2020-06-10 16:42:09 MDT

Viewing Active Policy - Data Protection for Two Sites

Review the rules in this policy. If this is a proposed policy, click Simulate to verify the policy and then click Activate to make the policy active.

Reason for change: Data Protection for Two Sites

Rules are evaluated in order, starting from the top.

Rule Name	Default	Tenant Account
One-Site Erasure Coding for Tenant A		Tenant A (49752734300032812036)
Two-Site Replication for Other Tenants	<input checked="" type="checkbox"/>	Ignore

[Simulate](#) [Activate](#)

In questa policy ILM, gli oggetti appartenenti al tenant A sono protetti da una codifica di cancellazione 2+1 in un singolo sito, mentre gli oggetti appartenenti a tutti gli altri tenant sono protetti in due siti utilizzando la replica a 2 copie.



La prima regola di questo esempio utilizza un filtro avanzato per garantire che la codifica erasure non venga utilizzata per oggetti di piccole dimensioni. Qualsiasi oggetto del tenant A di dimensioni inferiori a 200 KB sarà protetto dalla seconda regola, che utilizza la replica.

Regola 1: Erasure coding per un sito per il tenant A.

Definizione della regola	Valore di esempio
Nome regola	Codifica di cancellazione one-site per il tenant A.
Account tenant	Tenant A.
Pool di storage	Data center 1
Posizionamento dei contenuti	2+1 erasure coding in Data Center 1 dal giorno 0 a per sempre

Regola 2: Replica a due siti per altri tenant

Definizione della regola	Valore di esempio
Nome regola	Replica a due siti per altri tenant
Account tenant	Ignorare
Pool di storage	Data Center 1 e Data Center 2
Posizionamento dei contenuti	Due copie replicate dal giorno 0 all'infinito: Una copia nel data center 1 e una copia nel data center 2.

Policy ILM proposta per esempio 6: Protezione dei dati in tre siti

In questo esempio, il criterio ILM viene aggiornato per un sistema StorageGRID a tre siti.

Dopo aver eseguito un'espansione per aggiungere il nuovo sito, l'amministratore del grid ha creato due nuovi pool di storage: Un pool di storage per Data Center 3 e un pool di storage contenente tutti e tre i siti (non lo stesso del pool di storage predefinito di tutti i nodi di storage). Quindi, l'amministratore ha creato due nuove regole ILM e una nuova policy ILM proposta, progettata per proteggere i dati in tutti e tre i siti.

Before activating a new ILM policy:

- Review and carefully simulate the policy. Errors in an ILM policy can cause irreparable data loss.
- Review any changes to the placement of existing replicated and erasure-coded objects. Changing an existing object's location might result in temporary resource issues when the new placements are evaluated and implemented.

See [Managing objects with information lifecycle management](#) for more information.

This policy contains a rule that makes an erasure-coded copy. Confirm that at least one rule uses the Object Size advanced filter to prevent objects that are 200 KB or smaller from being erasure coded. See [Managing objects with information lifecycle management](#) for more information.

Review the rules in this policy. If this is a proposed policy, click Simulate to verify the policy and then click Activate to make the policy active.

Reason for change: Data Protection for Three Sites

Rules are evaluated in order, starting from the top.

Rule Name	Default	Tenant Account
Three-Site Erasure Coding for Tenant A 		Tenant A (49752734300032812036)
Three-Site Replication for Other Tenants 	✓	Ignore

Quando viene attivata questa nuova policy ILM, gli oggetti appartenenti al tenant A saranno protetti da una cancellazione 2+1 in tre siti, mentre gli oggetti appartenenti ad altri tenant (e gli oggetti più piccoli appartenenti al tenant A) saranno protetti in tre siti utilizzando la replica a 3 copie.

Regola 1: Erasure coding a tre siti per il tenant A.

Definizione della regola	Valore di esempio
Nome regola	Codifica di cancellazione a tre siti per il tenant A.
Account tenant	Tenant A.
Pool di storage	Tutti e 3 i data center (inclusi data center 1, data center 2 e data center 3)
Posizionamento dei contenuti	2+1 erasure coding in tutti e 3 i data center, dal giorno 0 fino all'eterno

Regola 2: Replica a tre siti per altri tenant

Definizione della regola	Valore di esempio
Nome regola	Replica a tre siti per altri tenant
Account tenant	Ignorare
Pool di storage	Data Center 1, Data Center 2 e Data Center 3
Posizionamento dei contenuti	Tre copie replicate dal giorno 0 a sempre: Una copia presso il data center 1, una copia presso il data center 2 e una copia presso il data center 3.

Attivazione della policy ILM proposta, ad esempio 6

Quando si attiva un nuovo criterio ILM proposto, gli oggetti esistenti potrebbero essere spostati in nuove posizioni oppure potrebbero essere create nuove copie degli oggetti per gli oggetti esistenti, in base alle istruzioni di posizionamento in qualsiasi regola nuova o aggiornata.



Gli errori in un criterio 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 un nuovo criterio ILM, StorageGRID lo utilizza per gestire tutti gli oggetti, inclusi quelli esistenti e quelli acquisiti di recente. Prima di attivare un nuovo criterio ILM, esaminare le eventuali modifiche apportate al posizionamento degli oggetti replicati e codificati in cancellazione esistenti. La modifica della posizione di un oggetto esistente potrebbe causare problemi di risorse temporanee quando i nuovi posizionamenti vengono valutati e implementati.

Cosa succede quando cambiano le istruzioni di erasure coding

Nella policy ILM attualmente attiva, per questo esempio, gli oggetti appartenenti al tenant A sono protetti utilizzando la codifica di cancellazione 2+1 nel data center 1. Nella nuova policy ILM proposta, gli oggetti appartenenti al tenant A verranno protetti utilizzando la codifica di cancellazione 2+1 nei data center 1, 2 e 3.

Quando viene attivato il nuovo criterio 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 memorizzato in un data center diverso.
- Gli oggetti esistenti appartenenti al tenant A vengono rivalutati durante il processo di scansione ILM in corso. Poiché le istruzioni di posizionamento di ILM utilizzano un nuovo profilo di codifica Erasure, vengono creati e distribuiti frammenti completamente nuovi con codifica erasure nei tre data center.



I frammenti 2+1 esistenti nel data center 1 non vengono riutilizzati. StorageGRID considera ogni profilo di codifica Erasure unico e non riutilizza i frammenti di codifica Erasure quando viene utilizzato un nuovo profilo.

Cosa succede quando cambiano le istruzioni di replica

Nel criterio ILM attualmente attivo per questo esempio, gli oggetti appartenenti ad altri tenant vengono protetti utilizzando due copie replicate nei pool di storage dei data center 1 e 2. Nella nuova policy ILM proposta, gli oggetti appartenenti ad altri tenant verranno protetti utilizzando tre copie replicate nei pool di storage dei data center 1, 2 e 3.

Quando viene attivato il nuovo criterio ILM, si verificano le seguenti operazioni ILM:

- Quando un tenant diverso dal tenant A acquisisce un nuovo oggetto, StorageGRID crea tre copie e salva una copia in ogni data center.
- Gli oggetti esistenti appartenenti a questi altri tenant vengono rivalutati durante il processo di scansione ILM in corso. Poiché le copie di oggetti esistenti nel data center 1 e nel data center 2 continuano a soddisfare i requisiti di replica della nuova regola ILM, StorageGRID deve creare solo una nuova copia dell'oggetto per il data center 3.

Impatto delle performance dell'attivazione di questa policy

Quando viene attivata la policy ILM proposta in questo esempio, le prestazioni generali di questo sistema StorageGRID saranno temporaneamente compromesse. Per creare nuovi frammenti erasure-coded per gli oggetti esistenti del tenant A e nuove copie replicate nel data center 3 per gli oggetti esistenti degli altri tenant saranno necessari livelli di risorse grid superiori al normale.

Come conseguenza della modifica del criterio ILM, le richieste di lettura e scrittura del client potrebbero temporaneamente riscontrare latenze superiori al normale. Le latenze torneranno ai livelli normali dopo che le istruzioni di posizionamento sono state completamente implementate nella griglia.

Per evitare problemi di risorse quando si attiva un nuovo criterio ILM, è possibile utilizzare il filtro avanzato Ingest Time in qualsiasi regola che potrebbe modificare la posizione di un gran numero di oggetti esistenti. Impostare Ingest Time (tempo di acquisizione) su un valore maggiore o uguale al tempo approssimativo in cui il nuovo criterio verrà applicato per garantire che gli oggetti esistenti non vengano spostati inutilmente.



Contattare il supporto tecnico se è necessario rallentare o aumentare la velocità di elaborazione degli oggetti dopo una modifica della policy ILM.

Esempio 7: Policy ILM conforme per il blocco oggetti S3

È possibile utilizzare il bucket S3, le regole ILM e il criterio ILM in questo esempio come punto di partenza quando si definisce un criterio ILM per soddisfare i requisiti di protezione e conservazione degli oggetti nei bucket con blocco oggetti S3 attivato.



Se hai utilizzato la funzionalità di conformità legacy nelle versioni precedenti di StorageGRID, puoi anche utilizzare questo esempio per gestire qualsiasi bucket esistente con la funzionalità di conformità legacy attivata.



Le seguenti regole e policy ILM sono solo esempi. Esistono diversi modi per configurare le regole ILM. Prima di attivare una nuova policy, simulare la policy proposta per confermare che funzionerà come previsto per proteggere il contenuto dalla perdita.

Informazioni correlate

["Gestione degli oggetti con S3 Object Lock"](#)

["Creazione di un criterio ILM"](#)

Esempio di bucket e oggetti per S3 Object Lock

In questo esempio, un account tenant S3 denominato Bank of ABC ha utilizzato il tenant Manager per creare un bucket con blocco oggetti S3 abilitato per memorizzare i record bancari critici.

Definizione del bucket	Valore di esempio
Nome account tenant	Banca di ABC
Nome bucket	banca-record
Area bucket	us-east-1 (impostazione predefinita)

Buckets

Create buckets and manage bucket settings.

1 bucket

Create bucket

Actions ▾

<input type="checkbox"/>	Name	S3 Object Lock	Region	Object Count	Space Used	Date Created
<input type="checkbox"/>	bank-records	✓	us-east-1	0	0 bytes	2021-01-06 16:53:19 MST

← Previous 1 Next →

Ogni versione di oggetto e oggetto aggiunta al bucket dei record bancari utilizzerà i seguenti valori per `retain-until-date` e `legal hold` impostazioni.

Impostazione per ciascun oggetto	Valore di esempio
<code>retain-until-date</code>	"2030-12-30T23:59:59Z" (30 dicembre 2030) Ogni versione dell'oggetto ha il proprio <code>retain-until-date</code> impostazione. Questa impostazione può essere aumentata, ma non ridotta.
<code>legal hold</code>	"OFF" (Non in vigore) È possibile mettere o revocare un blocco legale su qualsiasi versione oggetto in qualsiasi momento durante il periodo di conservazione. Se un oggetto è sottoposto a un blocco legale, non è possibile eliminarlo anche se <code>retain-until-date</code> è stato raggiunto.

ILM regola 1 per S3 Object Lock esempio: Erasure coding profile with bucket matching

Questa regola ILM di esempio si applica solo all'account tenant S3 denominato Bank of ABC. Corrisponde a qualsiasi oggetto in `bank-records` Quindi utilizza la codifica di cancellazione per memorizzare l'oggetto su nodi di storage in tre siti del data center utilizzando un profilo di codifica Erasure 6+3. Questa regola soddisfa i requisiti dei bucket con blocco oggetti S3 attivato: Una copia codificata in cancellazione viene conservata nei nodi di storage dal giorno 0 all'eterno, utilizzando l'ora di Ingest come ora di riferimento.

Definizione della regola	Valore di esempio
Nome regola	Compliant Rule (regola conforme): Oggetti EC nel bucket dei record bancari - Bank of ABC
Account tenant	Banca di ABC

Definizione della regola	Valore di esempio
Nome bucket	bank-records
Filtraggio avanzato	Dimensione oggetto (MB) maggiore di 0.20 Nota: questo filtro garantisce che la codifica erasure non venga utilizzata per oggetti di dimensioni pari o inferiori a 200 KB.

Create ILM Rule Step 1 of 3: Define Basics

Name

Description

Tenant Accounts (optional)

Bucket Name

[Advanced filtering...](#) (0 defined)

Cancel Next

Definizione della regola	Valore di esempio
Tempo di riferimento	Tempo di acquisizione
Posizionamenti	Dal giorno 0 memorizzare per sempre
Erasure Coding Profile (erasure Coding Profile)	<ul style="list-style-type: none"> • Creare una copia con codifica di cancellazione sui nodi di storage in tre siti del data center • Utilizza uno schema di erasure coding 6+3

Configure placement instructions to specify how you want objects matched by this rule to be stored.

Compliant Rule: EC objects in bank-record bucket - Bank of ABC

Reference Time Ingest Time

Placements Sort by start day

From day store Add Remove

Type Location Copies + x

Retention Diagram Refresh

The diagram shows a horizontal timeline starting at 'Day 0'. A grey bar labeled 'Three Data Centers (6 plus 3)' extends from Day 0 to the right. A blue arrow points to the right from the end of this bar, labeled 'Forever'. A vertical line marks 'Day 0' at the start of the bar.

Cancel Back Save

ILM regola 2 per S3 Object Lock esempio: Regola non conforme

Questa regola ILM di esempio memorizza inizialmente due copie di oggetti replicate sui nodi di storage. Dopo un anno, memorizza una copia su un Cloud Storage Pool per sempre. Poiché questa regola utilizza un Cloud Storage Pool, non è conforme e non si applica agli oggetti nei bucket con S3 Object Lock attivato.

Definizione della regola	Valore di esempio
Nome regola	Regola non conforme: Utilizza il pool di storage cloud
Account tenant	Non specificato
Nome bucket	Non specificato, ma si applica solo ai bucket che non hanno S3 Object Lock (o la funzione Compliance legacy) abilitato.
Filtraggio avanzato	Non specificato

Name

Description

Tenant Accounts (optional)

Bucket Name Value

Advanced filtering... (0 defined)

Cancel Next

Definizione della regola	Valore di esempio
Tempo di riferimento	Tempo di acquisizione
Posizionamenti	<ul style="list-style-type: none"> • Il giorno 0, conserva due copie replicate sui nodi di storage nel data center 1 e nel data center 2 per 365 giorni • Dopo 1 anno, conserva per sempre una copia replicata in un Cloud Storage Pool

ILM regola 3 per S3 Object Lock esempio: Regola predefinita

Questa regola ILM di esempio copia i dati degli oggetti in pool di storage in due data center. Questa regola di conformità è stata progettata per essere la regola predefinita nel criterio ILM. Non include alcun filtro e soddisfa i requisiti dei bucket con S3 Object Lock abilitato: Due copie di oggetti vengono conservate sui nodi di storage dal giorno 0 all'eterno, utilizzando Ingest come tempo di riferimento.

Definizione della regola	Valore di esempio
Nome regola	Default CompacCompacant Rule: Due copie di due data center
Account tenant	Non specificato
Nome bucket	Non specificato
Filtraggio avanzato	Non specificato

Create ILM Rule Step 1 of 3: Define Basics

Name

Description

Tenant Accounts (optional)

Bucket Name

[Advanced filtering...](#) (0 defined)

Cancel

Next

Definizione della regola	Valore di esempio
Tempo di riferimento	Tempo di acquisizione
Posizionamenti	Dal giorno 0 all'anno, conserva due copie replicate, una sui nodi di storage nel data center 1 e una sui nodi di storage nel data center 2.

Compliant Rule: Two Copies Two Data Centers

Reference Time:

Placements Sort by start day

From day: store:

Type: Location: Copies:

Specifying multiple storage pools might cause data to be stored at the same site if the pools overlap. See [Managing objects with information lifecycle management](#) for more information.

Retention Diagram Refresh

The diagram shows a horizontal timeline starting at 'Day 0'. Two horizontal bars represent the retention periods for 'Data Center 1' (blue) and 'Data Center 2' (orange). Both bars start at 'Day 0' and extend to the right, with the label 'Forever' at the end of the bars. A vertical line marks 'Day 0' as the 'Trigger' point.

Esempio di policy ILM conforme per S3 Object Lock

Per creare un criterio ILM che protegga efficacemente tutti gli oggetti del sistema, inclusi quelli nei bucket con S3 Object Lock attivato, è necessario selezionare le regole ILM che soddisfano i requisiti di storage per tutti gli oggetti. Quindi, è necessario simulare e attivare la policy proposta.

Aggiunta di regole al criterio

In questo esempio, il criterio ILM include tre regole ILM, nel seguente ordine:

1. Regola conforme che utilizza la codifica erasure per proteggere oggetti di dimensioni superiori a 200 KB in un bucket specifico con blocco oggetti S3 attivato. Gli oggetti vengono memorizzati nei nodi di storage dal giorno 0 a sempre.
2. Una regola non conforme che crea due copie di oggetti replicate sui nodi di storage per un anno e sposta una copia di oggetto in un pool di storage cloud per sempre. Questa regola non si applica ai bucket con blocco oggetti S3 attivato perché utilizza un pool di storage cloud.
3. La regola di conformità predefinita che crea due copie di oggetti replicate sui nodi di storage dal giorno 0 a per sempre.

Configure ILM Policy

Create a proposed policy by selecting and arranging rules. Then, save the policy and edit it later as required. Click Simulate to verify a saved policy using test objects. When you are ready, click Activate to make this policy the active ILM policy for the grid.

Name

Reason for change

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 (and any non-compliant rule without a filter) will be automatically placed at the end of the policy and cannot be moved.

+ Select Rules

Default	Rule Name	Compliant	Tenant Account	Actions
	Compliant Rule: EC for bank-records bucket - Bank of ABC	✓	Bank of ABC (90767802913525281639)	✕
	Non-Compliant Rule: Use Cloud Storage Pool		Ignore	✕
✓	Default Compliant Rule: Two Copies Two Data Centers	✓	Ignore	✕

Cancel

Save

Simulazione della policy proposta

Dopo aver aggiunto le regole nella policy proposta, aver scelto una regola di conformità predefinita e aver disposto le altre regole, è necessario simulare la policy testando gli oggetti dal bucket con S3 Object Lock abilitato e da altri bucket. Ad esempio, quando si simula il criterio di esempio, si prevede che gli oggetti di test vengano valutati come segue:

- La prima regola corrisponde solo agli oggetti di test di dimensioni superiori a 200 KB nei record bancari bucket per il tenant Bank of ABC.
- La seconda regola corrisponde a tutti gli oggetti in tutti i bucket non conformi per tutti gli altri account tenant.
- La regola predefinita corrisponde ai seguenti oggetti:
 - Oggetti di 200 KB o inferiori nei bucket bank-record per il tenant Bank of ABC.
 - Oggetti in qualsiasi altro bucket con S3 Object Lock attivato per tutti gli altri account tenant.

Attivazione del criterio

Quando si è completamente soddisfatti del fatto che il nuovo criterio protegga i dati degli oggetti come previsto, è possibile attivarlo.

Protezione avanzata del sistema

Scopri le impostazioni di sistema, le Best practice e i consigli per proteggere un sistema StorageGRID dalle minacce alla sicurezza.

- ["Protezione avanzata di un sistema StorageGRID"](#)
- ["Linee guida per la protezione avanzata degli aggiornamenti software"](#)

- ["Linee guida per la protezione avanzata delle reti StorageGRID"](#)
- ["Linee guida per la protezione avanzata dei nodi StorageGRID"](#)
- ["Linee guida per la protezione avanzata dei certificati server"](#)
- ["Altre linee guida per la protezione avanzata"\]](#)

Protezione avanzata di un sistema StorageGRID

La protezione avanzata del sistema è il processo che consente di eliminare il maggior numero possibile di rischi per la sicurezza da un sistema StorageGRID.

Questo documento fornisce una panoramica delle linee guida per la protezione avanzata specifiche di StorageGRID. Queste linee guida integrano le Best practice standard di settore per la protezione avanzata dei sistemi. Ad esempio, queste linee guida presuppongono l'utilizzo di password complesse per StorageGRID, l'utilizzo di HTTPS invece di HTTP e l'attivazione dell'autenticazione basata su certificato, se disponibile.

Durante l'installazione e la configurazione di StorageGRID, è possibile utilizzare queste linee guida per soddisfare qualsiasi obiettivo di sicurezza prescritto in termini di riservatezza, integrità e disponibilità del sistema informativo.

StorageGRID segue la *policy NetApp per la gestione delle vulnerabilità*. Le vulnerabilità segnalate vengono verificate e risolte in base al processo di risposta agli incidenti di sicurezza del prodotto.

Considerazioni generali per la protezione avanzata di un sistema StorageGRID

Quando si esegue la protezione avanzata di un sistema StorageGRID, è necessario considerare quanto segue:

- Quale delle tre reti StorageGRID è stata implementata? Tutti i sistemi StorageGRID devono utilizzare la rete griglia, ma è possibile utilizzare anche la rete di amministrazione, la rete client o entrambi. Ogni rete ha considerazioni di sicurezza diverse.
- Il tipo di piattaforme utilizzate per i singoli nodi nel sistema StorageGRID. I nodi StorageGRID possono essere implementati su macchine virtuali VMware, all'interno di un container Docker su host Linux o come appliance hardware dedicate. Ogni tipo di piattaforma dispone di un proprio set di Best practice per la protezione avanzata.
- Quanto sono affidabili gli account tenant. Se sei un provider di servizi con account tenant non attendibili, avrai problemi di sicurezza diversi rispetto all'utilizzo di tenant interni affidabili.
- Quali requisiti e convenzioni di sicurezza sono seguiti dalla tua organizzazione. Potrebbe essere necessario rispettare requisiti normativi o aziendali specifici.

Informazioni correlate

["Policy per la gestione delle vulnerabilità"](#)

Linee guida per la protezione avanzata degli aggiornamenti software

Per difenderti dagli attacchi, devi tenere aggiornato il tuo sistema StorageGRID e i servizi correlati.

Aggiornamenti al software StorageGRID

Se possibile, è necessario aggiornare il software StorageGRID alla versione principale più recente o alla

versione principale precedente. Mantenere aggiornato StorageGRID aiuta a ridurre il tempo di attivazione delle vulnerabilità note e l'area complessiva della superficie di attacco. Inoltre, le versioni più recenti di StorageGRID contengono spesso funzionalità di protezione avanzata che non sono incluse nelle versioni precedenti.

Quando è necessaria una correzione rapida, NetApp assegna la priorità alla creazione di aggiornamenti per le release più recenti. Alcune patch potrebbero non essere compatibili con le release precedenti.

Per scaricare le versioni più recenti di StorageGRID e gli aggiornamenti rapidi, accedere alla pagina di download del software StorageGRID. Per istruzioni dettagliate sull'aggiornamento del software StorageGRID, consultare le istruzioni per l'aggiornamento di StorageGRID. Per istruzioni sull'applicazione di una correzione rapida, consultare le istruzioni di ripristino e manutenzione.

Aggiornamenti a servizi esterni

I servizi esterni possono presentare vulnerabilità che influiscono indirettamente su StorageGRID. Devi assicurarti che i servizi da cui dipende StorageGRID siano sempre aggiornati. Questi servizi includono LDAP, KMS (o server KMIP), DNS e NTP.

Utilizza NetApp Interoperability Matrix Tool per ottenere un elenco delle versioni supportate.

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.

Utilizza NetApp Interoperability Matrix Tool per ottenere un elenco delle versioni supportate.

Upgrade a nodi Linux

Se i nodi StorageGRID utilizzano piattaforme host Linux, è necessario assicurarsi che gli aggiornamenti di sicurezza e del kernel siano applicati al sistema operativo host. Inoltre, è necessario applicare gli aggiornamenti del firmware all'hardware vulnerabile quando questi aggiornamenti diventano disponibili.

Utilizza NetApp Interoperability Matrix Tool per ottenere un elenco delle versioni supportate.

Informazioni correlate

["Download NetApp: StorageGRID"](#)

["Aggiornare il software"](#)

["Mantieni Ripristina"](#)

["Tool di matrice di interoperabilità NetApp"](#)

Linee guida per la protezione avanzata delle reti StorageGRID

Il sistema StorageGRID supporta fino a tre interfacce di rete per nodo di rete, consentendo di configurare la rete per ogni singolo nodo di rete in modo che corrisponda ai requisiti di sicurezza e accesso.

Linee guida per Grid Network

È necessario configurare una rete griglia per tutto il traffico StorageGRID interno. Tutti i nodi Grid si trovano sulla rete Grid e devono essere in grado di comunicare con tutti gli altri nodi.

Durante la configurazione della rete Grid, attenersi alle seguenti linee guida:

- Assicurarsi che la rete sia protetta da client non attendibili, ad esempio quelli su Internet aperto.
- Se possibile, utilizzare Grid Network esclusivamente per il traffico interno. Sia la rete di amministrazione che la rete client presentano ulteriori restrizioni firewall che bloccano il traffico esterno verso i servizi interni. È supportato l'utilizzo di Grid Network per il traffico client esterno, ma questo tipo di utilizzo offre meno livelli di protezione.
- Se l'implementazione di StorageGRID si estende su più data center, utilizzare una rete privata virtuale (VPN) o equivalente sulla rete grid per fornire una protezione aggiuntiva per il 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 generalmente utilizzata per le attività amministrative (dipendenti attendibili che utilizzano Grid Manager o SSH) e per la comunicazione con altri servizi attendibili come LDAP, DNS, NTP o KMS (o server KMIP). Tuttavia, StorageGRID non applica questo utilizzo internamente.

Se si utilizza la rete di amministrazione, attenersi alle seguenti linee guida:

- Bloccare tutte le porte di traffico interne sulla rete di amministrazione. Consultare l'elenco delle porte interne nella guida all'installazione della piattaforma in uso.
- Se i client non attendibili possono accedere alla rete di amministrazione, bloccare l'accesso a StorageGRID sulla rete di amministrazione con un firewall esterno.

Linee guida per la rete client

La rete client viene generalmente utilizzata per i tenant e per le comunicazioni con servizi esterni, come il servizio di replica CloudMirror o un altro servizio della piattaforma. Tuttavia, StorageGRID non applica questo utilizzo internamente.

Se si utilizza la rete client, attenersi alle seguenti linee guida:

- Bloccare tutte le porte di traffico interne sulla rete client. Consultare l'elenco delle porte interne nella guida all'installazione della piattaforma in uso.
- Accettare il traffico client in entrata solo su endpoint configurati esplicitamente. Consultare le informazioni sulla gestione delle reti client non attendibili nelle istruzioni per l'amministrazione di StorageGRID.

Informazioni correlate

["Linee guida per la rete"](#)

["Primer griglia"](#)

["Amministrare StorageGRID"](#)

["Installare Red Hat Enterprise Linux o CentOS"](#)

["Installare Ubuntu o Debian"](#)

["Installare VMware"](#)

Linee guida per la protezione avanzata dei nodi StorageGRID

I nodi StorageGRID possono essere implementati su macchine virtuali VMware, all'interno di un container Docker su host Linux o come appliance hardware dedicate. Ogni tipo di piattaforma e ogni tipo di nodo dispone di un proprio set di Best practice per la protezione avanzata.

Configurazione del firewall

Nell'ambito del processo di protezione avanzata del sistema, è necessario rivedere le configurazioni dei firewall esterni e modificarle in modo che il traffico venga accettato solo dagli indirizzi IP e dalle porte da cui è strettamente necessario.

I nodi in esecuzione sulle piattaforme VMware e sulle appliance StorageGRID utilizzano un firewall interno che viene gestito automaticamente. Sebbene questo firewall interno offra 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, consultare la guida all'installazione della piattaforma.

Virtualizzazione, container e hardware condiviso

Per tutti i nodi StorageGRID, evitare di eseguire StorageGRID sullo stesso hardware fisico del software non attendibile. Non presupporre che le protezioni dell'hypervisor impediscano al malware di accedere ai dati protetti da StorageGRID se StorageGRID e il malware esistono sullo stesso hardware fisico. Ad esempio, gli attacchi Meltdown e Spectre sfruttano le vulnerabilità critiche dei processori moderni e consentono ai programmi di rubare dati in memoria sullo stesso computer.

Disattivare i servizi inutilizzati

Per tutti i nodi StorageGRID, è necessario disattivare o bloccare l'accesso ai servizi inutilizzati. Ad esempio, se non si intende configurare l'accesso client alle condivisioni di controllo per CIFS o NFS, bloccare o disattivare l'accesso a questi servizi.

Proteggere i nodi durante l'installazione

Non consentire agli utenti non attendibili di accedere ai nodi StorageGRID sulla rete durante l'installazione dei nodi. I nodi non sono completamente sicuri fino a quando non si sono Uniti alla griglia.

Linee guida per i nodi di amministrazione

I nodi di amministrazione forniscono servizi di gestione quali configurazione, monitoraggio e registrazione del sistema. Quando si accede a Grid Manager o al tenant Manager, si sta effettuando la connessione a un nodo amministratore.

Seguire queste linee guida per proteggere i nodi di amministrazione nel sistema StorageGRID:

- Proteggere tutti i nodi di amministrazione da client non attendibili, ad esempio quelli su Internet aperto. Assicurarsi che nessun client non attendibile possa accedere a qualsiasi nodo Admin sulla rete Grid, sulla rete amministrativa o sulla rete client.
- I gruppi StorageGRID controllano l'accesso alle funzioni di gestione griglia e di gestione tenant. Concedere a ciascun gruppo di utenti le autorizzazioni minime richieste per il proprio ruolo e utilizzare la modalità di accesso in sola lettura per impedire agli utenti di modificare la configurazione.

- Quando si utilizzano gli endpoint del bilanciamento del carico StorageGRID, utilizzare i nodi gateway invece dei nodi di amministrazione per il traffico client non attendibile.
- Se si dispone di tenant non attendibili, non consentire loro di accedere direttamente al tenant Manager o all'API di gestione del tenant. I tenant non attendibili devono invece utilizzare un portale tenant o un sistema di gestione tenant esterno, che interagisce con l'API di gestione tenant.
- Se lo si desidera, utilizzare un proxy amministratore per un maggiore controllo sulle comunicazioni AutoSupport dai nodi di amministrazione al supporto NetApp. Consultare la procedura per la creazione di un proxy amministratore nelle istruzioni per l'amministrazione di StorageGRID.
- Facoltativamente, utilizzare le porte limitate 8443 e 9443 per separare le comunicazioni di Grid Manager e Tenant Manager. Bloccare la porta condivisa 443 e limitare le richieste del tenant alla porta 9443 per una protezione aggiuntiva.
- Facoltativamente, utilizzare nodi di amministrazione separati per gli amministratori di grid e gli utenti del tenant.

Per ulteriori informazioni, consultare le istruzioni per l'amministrazione di StorageGRID.

Linee guida per i nodi di storage

I nodi di storage gestiscono e memorizzano i dati e i metadati degli oggetti. Seguire queste linee guida per proteggere i nodi di storage nel sistema StorageGRID.

- Non abilitare i servizi in uscita per tenant non attendibili. Ad esempio, quando si crea l'account per un tenant non attendibile, non consentire al tenant di utilizzare la propria origine di identità e non consentire l'utilizzo dei servizi della piattaforma. Consultare la procedura per la creazione di un account tenant nelle istruzioni per l'amministrazione di StorageGRID.
- Utilizzare un bilanciamento del carico di terze parti per il traffico client non attendibile. Il bilanciamento del carico di terze parti offre un maggiore controllo e ulteriori livelli di protezione dagli attacchi.
- Se lo si desidera, utilizzare un proxy dello storage per un maggiore controllo sui pool di storage cloud e sulle comunicazioni dei servizi della piattaforma dai nodi di storage ai servizi esterni. Consultare la procedura per la creazione di un proxy di storage nelle istruzioni per l'amministrazione di StorageGRID.
- Se lo si desidera, connettersi a servizi esterni utilizzando la rete client. Quindi, selezionare **Configuration > Network Settings > Untrusted Client Network** e indicare che la rete client sul nodo di storage non è attendibile. Il nodo di storage non accetta più alcun traffico in entrata sulla rete client, ma continua a consentire le richieste in uscita per Platform Services.

Linee guida per i nodi gateway

I nodi gateway forniscono un'interfaccia opzionale per il bilanciamento del carico che le applicazioni client possono utilizzare per connettersi a StorageGRID. Attenersi alle seguenti linee guida per proteggere i nodi gateway nel sistema StorageGRID:

- Configurare e utilizzare gli endpoint del bilanciamento del carico invece di utilizzare il servizio CLB sui nodi gateway. Consultare la procedura per la gestione del bilanciamento del carico nelle istruzioni per l'amministrazione di StorageGRID.



Il servizio CLB è obsoleto.

- Utilizzare un bilanciamento del carico di terze parti tra il client e il nodo gateway o i nodi di storage per il traffico client non attendibile. Il bilanciamento del carico di terze parti offre un maggiore controllo e ulteriori livelli di protezione dagli attacchi. Se si utilizza un bilanciamento del carico di terze parti, il traffico di rete può comunque essere configurato in modo opzionale per passare attraverso un endpoint interno di

bilanciamento del carico o essere inviato direttamente ai nodi di storage.

- Se si utilizzano endpoint di bilanciamento del carico, è possibile che i client si connettano tramite la rete client. Quindi, selezionare **Configurazione > Impostazioni di rete > rete client non attendibile** e indicare che la rete client sul nodo gateway non è attendibile. Il nodo gateway accetta solo il traffico in entrata sulle porte esplicitamente configurate come endpoint del bilanciamento del carico.

Linee guida per i nodi dell'appliance hardware

Le appliance hardware StorageGRID sono progettate appositamente per l'utilizzo in un sistema StorageGRID. Alcune appliance possono essere utilizzate come nodi di storage. Altri appliance possono essere utilizzati come nodi di amministrazione o nodi gateway. È possibile combinare nodi appliance con nodi basati su software o implementare grid all-appliance completamente progettati.

Segui queste linee guida per proteggere i nodi dell'appliance hardware nel tuo sistema StorageGRID:

- Se l'appliance utilizza Gestione di sistema di SANtricity per la gestione del controller di storage, impedire ai client non attendibili di accedere a Gestione di sistema di SANtricity tramite la rete.
- Se l'appliance dispone di un BMC (Baseboard Management Controller), tenere presente che la porta di gestione BMC consente un accesso hardware di basso livello. Collegare la porta di gestione BMC solo a una rete di gestione interna sicura e affidabile. Se tale rete non è disponibile, lasciare la porta di gestione BMC disconnessa o bloccata, a meno che non venga richiesta una connessione BMC dal supporto tecnico.
- Se l'appliance supporta la gestione remota dell'hardware del controller su Ethernet utilizzando lo standard IPMI (Intelligent Platform Management Interface), bloccare il traffico non attendibile sulla porta 623.
- Se lo storage controller dell'appliance include dischi FDE o FIPS e la funzione di protezione del disco è attivata, utilizzare SANtricity per configurare le chiavi di protezione del disco.
- Per le appliance senza dischi FDE o FIPS, abilitare la crittografia dei nodi utilizzando un server di gestione delle chiavi (KMS).

Consultare le istruzioni di installazione e manutenzione dell'appliance hardware StorageGRID.

Informazioni correlate

["Installare Red Hat Enterprise Linux o CentOS"](#)

["Installare Ubuntu o Debian"](#)

["Installare VMware"](#)

["Amministrare StorageGRID"](#)

["Utilizzare un account tenant"](#)

["SG100 SG1000 Services appliance"](#)

["Appliance di storage SG5600"](#)

["Appliance di storage SG5700"](#)

["Appliance di storage SG6000"](#)

Linee guida per la protezione avanzata dei certificati server

È necessario sostituire i certificati predefiniti creati durante l'installazione con 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 con firma CA da utilizzare per l'autenticazione di StorageGRID.

In particolare, è necessario utilizzare certificati server personalizzati anziché i seguenti certificati predefiniti:

- **Management Interface Server Certificate:** Utilizzato per proteggere l'accesso a Grid Manager, Tenant Manager, Grid Management API e Tenant Management API.
- **Object Storage API Service Endpoints Server Certificate:** Utilizzato per proteggere l'accesso ai nodi di storage e ai nodi gateway, utilizzati dalle applicazioni client S3 e Swift per caricare e scaricare i dati degli oggetti.



StorageGRID gestisce separatamente i certificati utilizzati per gli endpoint del bilanciamento del carico. Per configurare i certificati di bilanciamento del carico, vedere i passaggi per la configurazione degli endpoint di bilanciamento del carico nelle istruzioni per l'amministrazione di StorageGRID.

Quando si utilizzano certificati server personalizzati, attenersi alle seguenti linee guida:

- I certificati devono avere un *subjectAltName* Che corrisponde alle voci DNS per StorageGRID. Per ulteriori informazioni, vedere la sezione 4.2.1.6, "Subject alternative Name," in ["RFC 5280: Certificato PKIX e profilo CRL"](#).
- Se possibile, evitare l'utilizzo di certificati con caratteri jolly. Un'eccezione a questa linea guida è il certificato per un endpoint di stile host virtuale S3, che richiede l'utilizzo di un carattere jolly se i nomi dei bucket non sono noti in anticipo.
- Quando è necessario utilizzare i caratteri jolly nei certificati, è necessario adottare ulteriori misure per ridurre i rischi. Utilizzare un modello con caratteri jolly come `*.s3.example.com` e non utilizzare ``s3.example.com` suffisso per altre applicazioni. Questo modello funziona anche con l'accesso S3 di tipo path, ad esempio `dc1-s1.s3.example.com/mybucket`.
- Impostare i tempi di scadenza del certificato su brevi (ad esempio, 2 mesi) e utilizzare l'API Grid Management per automatizzare la rotazione del certificato. Ciò è particolarmente importante per i certificati con caratteri jolly.

Inoltre, i client devono utilizzare un rigoroso controllo del nome host quando comunicano con StorageGRID.

Altre linee guida per la protezione avanzata

Oltre a seguire le linee guida per la protezione avanzata per reti e nodi StorageGRID, è necessario seguire le linee guida per la protezione avanzata per altre aree del sistema StorageGRID.

Registri e messaggi di audit

Proteggere sempre i log StorageGRID e l'output dei messaggi di controllo in modo sicuro. I registri e i messaggi di audit di StorageGRID forniscono informazioni preziose dal punto di vista del supporto e della disponibilità del sistema. Inoltre, le informazioni e i dettagli contenuti nei registri StorageGRID e nell'output dei

messaggi di audit sono generalmente di natura sensibile.

Per ulteriori informazioni sui registri StorageGRID, consultare le istruzioni per il monitoraggio e la risoluzione dei problemi. Per ulteriori informazioni sui messaggi di audit di StorageGRID, consultare le istruzioni per i messaggi di audit.

NetApp AutoSupport

La funzione AutoSupport di StorageGRID consente di monitorare in modo proattivo lo stato di salute del sistema e di inviare automaticamente messaggi e dettagli al supporto tecnico NetApp, al team di supporto interno della tua organizzazione o a un partner di supporto. Per impostazione predefinita, i messaggi AutoSupport al supporto tecnico NetApp vengono attivati quando si configura StorageGRID per la prima volta.

La funzione AutoSupport può essere disattivata. Tuttavia, NetApp consiglia di abilitare l'IT perché AutoSupport aiuta a velocizzare l'identificazione e la risoluzione dei problemi in caso di problemi nel sistema StorageGRID.

AutoSupport supporta HTTPS, HTTP e SMTP per i protocolli di trasporto. A causa della natura sensibile dei messaggi AutoSupport, NetApp consiglia vivamente di utilizzare HTTPS come protocollo di trasporto predefinito per l'invio di messaggi AutoSupport al supporto NetApp.

Facoltativamente, è possibile configurare un proxy amministratore per un maggiore controllo sulle comunicazioni AutoSupport dai nodi di amministrazione al supporto tecnico NetApp. Consultare la procedura per la creazione di un proxy amministratore nelle istruzioni per l'amministrazione di StorageGRID.

Cross-Origin Resource Sharing (CORS)

È possibile configurare Cross-Origin Resource Sharing (CORS) per un bucket S3 se si desidera che quel bucket e gli oggetti in quel bucket siano accessibili alle applicazioni web in altri domini. In generale, non abilitare il CORS a meno che non sia necessario. Se è richiesto un CORS, limitarlo alle origini attendibili.

Consultare la procedura per la configurazione di Cross-Origin Resource Sharing (CORS) nelle istruzioni per l'utilizzo degli account tenant.

Dispositivi di sicurezza esterni

Una soluzione di protezione avanzata completa deve affrontare i meccanismi di sicurezza esterni a StorageGRID. L'utilizzo di ulteriori dispositivi di infrastruttura per il filtraggio e la limitazione dell'accesso a StorageGRID è un metodo efficace per stabilire e mantenere una posizione di sicurezza rigorosa. 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 un bilanciamento del carico di terze parti. Il bilanciamento del carico di terze parti offre un maggiore controllo e ulteriori livelli di protezione dagli attacchi.

Informazioni correlate

["Monitor risoluzione dei problemi"](#)

["Esaminare i registri di audit"](#)

["Utilizzare un account tenant"](#)

["Amministrare StorageGRID"](#)

Configurare StorageGRID per FabricPool

Scopri come configurare StorageGRID come Tier cloud NetApp FabricPool.

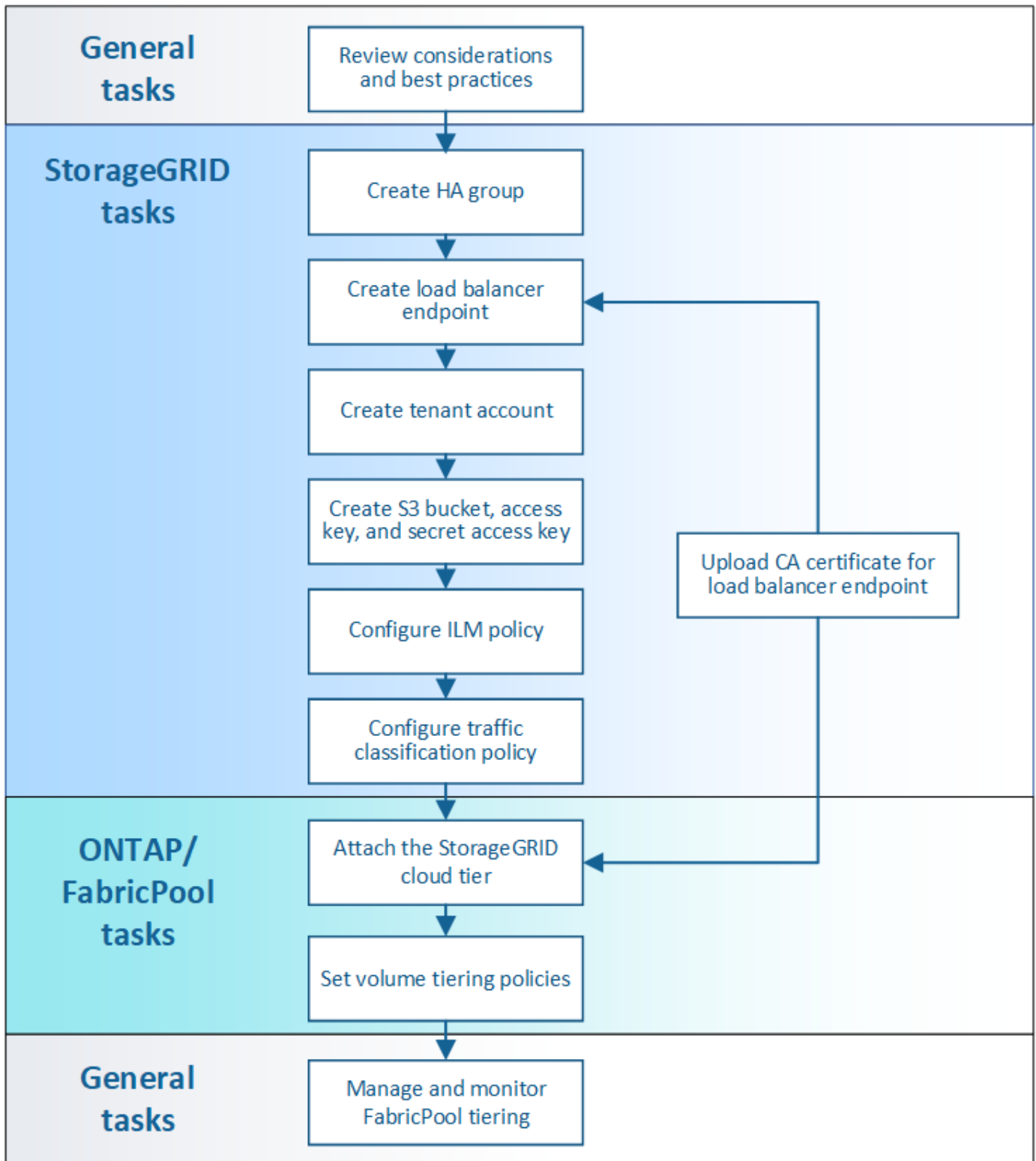
- ["Configurazione di StorageGRID per FabricPool"](#)
- ["Informazioni necessarie per collegare StorageGRID come Tier cloud"](#)
- ["Utilizzo della gestione del ciclo di vita delle informazioni StorageGRID con i dati FabricPool"](#)
- ["Creazione di una policy di classificazione del traffico per FabricPool"](#)
- ["Altre Best practice per StorageGRID e FabricPool"](#)

Configurazione di StorageGRID per FabricPool

Se si utilizza il software NetApp ONTAP, è possibile utilizzare NetApp FabricPool per eseguire il tiering dei dati inattivi o a freddo su un sistema di storage a oggetti NetApp StorageGRID.

Seguire queste istruzioni per:

- Ottieni una panoramica sulla configurazione di un sistema di storage a oggetti StorageGRID per l'utilizzo con FabricPool.
- Scopri come ottenere le informazioni che fornisci a ONTAP quando Aggiungi StorageGRID come Tier cloud FabricPool.
- Scopri le Best practice per la configurazione del criterio ILM (Information Lifecycle Management) di StorageGRID, di un criterio di classificazione del traffico StorageGRID e di altre opzioni StorageGRID per un carico di lavoro FabricPool.



Di cosa hai bisogno

Prima di utilizzare queste istruzioni:

- Decidere quale criterio di tiering dei volumi FabricPool utilizzare per eseguire il tiering dei dati ONTAP inattivi in StorageGRID.
- Pianificare e installare un sistema StorageGRID per soddisfare le esigenze di capacità e performance dello storage.

- Familiarizzare con il software di sistema StorageGRID, incluso il gestore del grid e il gestore del tenant.

Informazioni correlate

- ["TR-4598: Best practice FabricPool per ONTAP 9.8"](#)
- ["Centro documentazione di ONTAP 9"](#)

Che cos'è FabricPool

FabricPool è una soluzione di storage ibrido ONTAP che utilizza un aggregato flash dalle performance elevate come Tier delle performance e un archivio di oggetti come Tier del cloud. I dati in un FabricPool vengono memorizzati in un Tier in base all'accesso frequente o meno. L'utilizzo di un FabricPool consente di ridurre i costi dello storage senza compromettere le performance, l'efficienza o la protezione.

Non sono necessarie modifiche architetturali e puoi continuare a gestire il tuo ambiente di database e applicazioni dal sistema di storage centrale ONTAP.

Che cos'è lo storage a oggetti

Lo storage a oggetti è un'architettura di storage che gestisce i dati come oggetti, rispetto ad altre architetture di storage come lo storage a blocchi o a file. Gli oggetti vengono conservati all'interno di un singolo contenitore (ad esempio un bucket) e non vengono nidificati come file all'interno di una directory all'interno di altre directory. Sebbene lo storage a oggetti offra generalmente performance inferiori rispetto allo storage a blocchi o a file, è notevolmente più scalabile. I bucket StorageGRID possono contenere petabyte di dati.

Utilizzo di StorageGRID come livello cloud FabricPool

FabricPool può eseguire il tiering dei dati ONTAP a diversi provider di archivi di oggetti, tra cui StorageGRID. A differenza dei cloud pubblici che potrebbero impostare un numero massimo di IOPS (Input/Output Operations per Second) supportati a livello di bucket o container, le performance di StorageGRID sono scalabili in base al numero di nodi in un sistema. L'utilizzo di StorageGRID come livello cloud FabricPool ti consente di conservare i tuoi dati nel tuo cloud privato per ottenere le massime performance e il controllo completo sui tuoi dati.

Inoltre, non è necessaria una licenza FabricPool quando si utilizza StorageGRID come livello cloud.

Utilizzo di più cluster ONTAP con StorageGRID

Queste istruzioni descrivono come connettere StorageGRID a un singolo cluster ONTAP. Tuttavia, è possibile collegare lo stesso sistema StorageGRID a più cluster ONTAP.

L'unico requisito per il tiering dei dati da più cluster ONTAP a un singolo sistema StorageGRID è l'utilizzo di un bucket S3 diverso per ciascun cluster. In base ai tuoi requisiti, puoi utilizzare lo stesso gruppo ad alta disponibilità (ha), endpoint di bilanciamento del carico e account tenant per tutti i cluster, oppure puoi configurare ciascuno di questi elementi per ciascun cluster.

Informazioni necessarie per collegare StorageGRID come Tier cloud

Prima di poter collegare StorageGRID come livello cloud per FabricPool, è necessario eseguire alcune fasi di configurazione in StorageGRID e ottenere determinati valori.

A proposito di questa attività

La seguente tabella elenca le informazioni da fornire a ONTAP quando si collega StorageGRID come livello cloud per FabricPool. Gli argomenti di questa sezione spiegano come utilizzare il Gestore griglia e il Gestore tenant di StorageGRID per ottenere le informazioni necessarie.



I nomi esatti dei campi elencati e il processo utilizzato per inserire i valori richiesti in ONTAP dipendono dall'utilizzo dell'interfaccia CLI (creazione configurazione archivio oggetti aggregato di storage) o del gestore di sistema ONTAP (**Storage > aggregati e dischi > livello cloud**) di ONTAP.

Per ulteriori informazioni, fare riferimento a quanto segue:

- ["TR-4598: Best practice FabricPool per ONTAP 9.8"](#)
- ["Centro documentazione di ONTAP 9"](#)

Aeroporto ONTAP Field	Descrizione
Nome archivio oggetti	Qualsiasi nome univoco e descrittivo. Ad esempio, StorageGRID_Cloud_Tier.
Tipo di provider	StorageGRID (Gestore di sistema) o. SGWS (CLI).
Porta	La porta utilizzata da FabricPool per la connessione a StorageGRID. È possibile determinare il numero di porta da utilizzare quando si definisce l'endpoint del bilanciamento del carico di StorageGRID. "Creazione di un endpoint di bilanciamento del carico per FabricPool"
Nome del server	Nome di dominio completo (FQDN) per l'endpoint del bilanciamento del carico di StorageGRID. Ad esempio, s3.storagegrid.company.com. Tenere presente quanto segue: <ul style="list-style-type: none">• Il nome di dominio specificato deve corrispondere al nome di dominio sul certificato CA caricato per l'endpoint del bilanciamento del carico di StorageGRID.• Il record DNS per questo nome di dominio deve essere associato a ciascun indirizzo IP utilizzato per la connessione a StorageGRID. "Configurazione del server DNS per gli indirizzi IP StorageGRID"
Nome del container	Il nome del bucket StorageGRID che verrà utilizzato con questo cluster ONTAP. Ad esempio, fabricpool-bucket. Questo bucket viene creato nel tenant manager. Tenere presente quanto segue: <ul style="list-style-type: none">• Una volta creata la configurazione, non è possibile modificare il nome del bucket.• Il bucket non può avere la versione attivata.• È necessario utilizzare un bucket diverso per ogni cluster ONTAP che eseguirà il Tier dei dati in StorageGRID. "Creazione di un bucket S3 e ottenimento di una chiave di accesso"

Aeroporto ONTAP Field	Descrizione
Chiave di accesso e password segreta	<p>La chiave di accesso e la chiave di accesso segreta per l'account tenant StorageGRID.</p> <p>Questi valori vengono generati in Tenant Manager.</p> <p>"Creazione di un bucket S3 e ottenimento di una chiave di accesso"</p>
SSL	Deve essere attivato.
Certificato dell'archivio di oggetti	<p>Il certificato CA caricato al momento della creazione dell'endpoint del bilanciamento del carico di StorageGRID.</p> <p>Nota: se una CA intermedia ha emesso il certificato StorageGRID, è necessario fornire il certificato CA intermedio. Se il certificato StorageGRID è stato emesso direttamente dalla CA principale, è necessario fornire il certificato della CA principale.</p> <p>"Creazione di un endpoint di bilanciamento del carico per FabricPool"</p>

Al termine

Dopo aver ottenuto le informazioni StorageGRID richieste, puoi accedere a ONTAP per aggiungere StorageGRID come livello cloud, aggiungere il livello cloud come aggregato e impostare le policy di tiering dei volumi.

Best practice per il bilanciamento del carico

Prima di collegare StorageGRID come Tier cloud FabricPool, utilizza Gestione griglia StorageGRID per configurare almeno un endpoint di bilanciamento del carico.

Qual è il bilanciamento del carico

Quando i dati vengono suddivisi in livelli da FabricPool a un sistema StorageGRID, StorageGRID utilizza un sistema di bilanciamento del carico per gestire il carico di lavoro di acquisizione e recupero. Il bilanciamento del carico massimizza la velocità e la capacità di connessione distribuendo il carico di lavoro FabricPool su più nodi di storage.

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

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

Anche se il servizio bilanciamento del carico di StorageGRID è il meccanismo di bilanciamento del carico consigliato, potrebbe essere necessario integrare un bilanciamento del carico di terze parti. Per ulteriori informazioni, contatta il tuo account Representative NetApp o consulta il seguente report tecnico:

["Opzioni di bilanciamento del carico StorageGRID"](#)



Il servizio separato di bilanciamento del carico di connessione (CLB) sui nodi gateway è obsoleto e non è più consigliato per l'utilizzo con FabricPool.

Best practice per il bilanciamento del carico StorageGRID

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

È necessario configurare un endpoint del bilanciamento del carico StorageGRID per definire la porta che i nodi gateway e i nodi di amministrazione utilizzeranno per le richieste FabricPool in entrata e in uscita.

Best practice per il certificato endpoint del bilanciamento del carico

Quando si crea un endpoint di bilanciamento del carico da utilizzare con FabricPool, è necessario utilizzare HTTPS come protocollo. È quindi possibile caricare un certificato firmato da un'autorità di certificazione pubblica o privata oppure generare un certificato autofirmato. Il certificato consente a ONTAP di autenticarsi con StorageGRID.

Come procedura consigliata, è necessario utilizzare un certificato del server CA per proteggere la connessione. I certificati firmati da una CA possono essere ruotati senza interruzioni.

Quando si richiede un certificato CA per l'utilizzo con l'endpoint del bilanciamento del carico, assicurarsi che il nome di dominio sul certificato corrisponda al nome del server immesso in ONTAP per l'endpoint del bilanciamento del carico. Se possibile, utilizzare un carattere jolly (*) per consentire gli URL di tipo host virtuale. Ad esempio:

```
*.s3.storagegrid.company.com
```

Quando si aggiunge StorageGRID come livello cloud FabricPool, è necessario installare lo stesso certificato nel cluster ONTAP, nonché i certificati di autorità di certificazione (CA) root e subordinate.



StorageGRID utilizza i certificati del server per diversi scopi. Se ci si connette al servizio Load Balancer, non è necessario caricare il certificato del server degli endpoint del servizio API di storage a oggetti.

Per ulteriori informazioni sul certificato server per un endpoint di bilanciamento del carico:

- ["Gestione del bilanciamento del carico"](#)
- ["Linee guida per la protezione avanzata dei certificati server"](#)

Best practice per i gruppi ad alta disponibilità

Prima di collegare StorageGRID come livello cloud FabricPool, utilizza Gestione griglia StorageGRID per configurare un gruppo ad alta disponibilità (ha).

Che cos'è un gruppo ad alta disponibilità (ha)

Per garantire che il servizio bilanciamento del carico sia sempre disponibile per gestire i dati FabricPool, è

possibile raggruppare le interfacce di rete di più nodi di amministrazione e gateway in una singola entità, nota come gruppo ad alta disponibilità (ha). Se il nodo attivo nel gruppo non riesce, un altro nodo del gruppo può continuare a gestire il carico di lavoro.

Ogni gruppo ha fornisce un accesso altamente disponibile ai servizi condivisi sui nodi associati. Ad esempio, un gruppo ha costituito da tutti i nodi Admin fornisce un accesso altamente disponibile ad alcuni servizi di gestione di Admin Node e al servizio Load Balancer. Un gruppo ha costituito solo da nodi gateway o da nodi Admin e nodi gateway fornisce un accesso altamente disponibile al servizio Load Balancer condiviso.

Quando si crea un gruppo ha, si selezionano le interfacce di rete appartenenti alla rete Grid (eth0) o alla rete client (eth2). Tutte le interfacce di un gruppo ha devono trovarsi all'interno della stessa subnet di rete.

Un gruppo ha mantiene uno o più indirizzi IP virtuali aggiunti all'interfaccia attiva del gruppo. Se l'interfaccia attiva non è più disponibile, gli indirizzi IP virtuali vengono spostati in un'altra interfaccia. Questo processo di failover richiede in genere solo pochi secondi ed è abbastanza rapido da consentire alle applicazioni client di avere un impatto minimo e può fare affidamento sui normali comportamenti di ripetizione per continuare a funzionare.

Se si configura un gruppo ha di nodi per il bilanciamento del carico, FabricPool si connette agli indirizzi IP virtuali di quel gruppo ha.

Best practice per i gruppi ad alta disponibilità (ha)

Le Best practice per la creazione di un gruppo StorageGRID ha per FabricPool dipendono dal carico di lavoro, come segue:

- 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 l'interruzione del recupero dei dati.
- Se si prevede di utilizzare la policy di tiering del volume solo snapshot di FabricPool o Tier di performance locali non primari (ad esempio, ubicazioni per il disaster recovery o destinazioni NetApp SnapMirror®), è possibile configurare un gruppo ha con un solo nodo.

Queste istruzioni descrivono la configurazione di un gruppo ha per Active-Backup ha (un nodo è attivo e un nodo è il backup). Tuttavia, potrebbe essere preferibile utilizzare DNS Round Robin o Active-Active ha. Per ulteriori informazioni sui vantaggi di queste altre configurazioni ha, vedere "[Opzioni di configurazione per i gruppi ha](#)".

Configurazione del server DNS per gli indirizzi IP StorageGRID

Dopo aver configurato i gruppi ad alta disponibilità e gli endpoint del bilanciamento del carico, è necessario assicurarsi che il DNS (Domain Name System) del sistema ONTAP includa un record per associare il nome del server StorageGRID (Fully Qualified Domain Name) all'indirizzo IP che FabricPool utilizzerà per stabilire le connessioni.

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

- Se è stato configurato un gruppo ha, FabricPool si conatterà agli indirizzi IP virtuali di tale gruppo ha.
- Se non si utilizza un gruppo ha, FabricPool può connettersi al servizio bilanciamento del carico StorageGRID utilizzando l'indirizzo IP di qualsiasi nodo gateway o nodo amministratore.

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

Creazione di 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 costituito da una o più interfacce di rete su nodi di amministrazione, nodi gateway o entrambi.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre dell'autorizzazione di accesso root.

A proposito di questa attività

Ogni gruppo ha utilizza indirizzi IP virtuali (VIP) per fornire un accesso altamente disponibile ai servizi condivisi sui nodi associati.

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

Fasi

1. Selezionare **Configurazione > Impostazioni di rete > gruppi ad alta disponibilità**.
2. Selezionare una o più interfacce di rete. Le interfacce di rete devono appartenere alla stessa subnet della rete Grid (eth0) o della rete client (eth2).
3. Assegnare un nodo come master preferito.

Preferred Master è l'interfaccia attiva a meno che non si verifichi un errore che causa la riassegnazione degli indirizzi VIP a un'interfaccia di backup.

4. Inserire fino a dieci indirizzi IPv4 per il gruppo ha.

Gli indirizzi devono trovarsi all'interno della subnet IPv4 condivisa da tutte le interfacce membri.

Create High Availability Group

High Availability Group

Name

Description

Interfaces

Select interfaces to include in the HA group. All interfaces must be in the same network subnet.

Select Interfaces

Node Name	Interface	IPv4 Subnet	Preferred Master
DC1-ADM1	eth0	10.96.98.0/23	<input checked="" type="radio"/>
DC1-G1	eth0	10.96.98.0/23	<input type="radio"/>

Displaying 2 interfaces.

Virtual IP Addresses

Virtual IP Subnet: 10.96.98.0/23. All virtual IP addresses must be within this subnet. There must be at least 1 and no more than 10 virtual IP addresses.

Virtual IP Address 1



Cancel

Save

Creazione di un endpoint di bilanciamento del carico per FabricPool

Quando si configura StorageGRID per l'utilizzo con FabricPool, si configura un endpoint di bilanciamento del carico e si carica il certificato dell'endpoint di bilanciamento del carico, utilizzato per proteggere la connessione tra ONTAP e StorageGRID.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre dell'autorizzazione di accesso root.
- Sono disponibili i seguenti file:
 - Server Certificate (certificato server): Il file di certificato del server personalizzato.
 - Server Certificate Private Key (chiave privata certificato server): Il file di chiave privata del certificato del server personalizzato.

- **BUNDLE CA:** Un singolo file contenente i certificati di ciascuna CA (Intermediate Issuing Certificate Authority). Il file deve contenere ciascuno dei file di certificato CA con codifica PEM, concatenati in ordine di catena del certificato.

A proposito di questa attività

Per ulteriori informazioni su questa attività, vedere ["Configurazione degli endpoint del bilanciamento del carico"](#).

Fasi

1. Selezionare **Configuration > Network Settings > Load Balancer Endpoints**.

Create Endpoint

Display Name

Port

Protocol HTTP HTTPS

Endpoint Binding Mode Global HA Group VIPs Node Interfaces

2. Selezionare **Aggiungi endpoint**.
3. Inserire le seguenti informazioni.

Campo	Descrizione
Nome visualizzato	Un nome descrittivo per l'endpoint
Porta	<p>La porta StorageGRID che si desidera utilizzare per il bilanciamento del carico. Per impostazione predefinita, questo campo è 10433, ma è possibile inserire qualsiasi porta esterna non utilizzata. Se si immette 80 o 443, l'endpoint viene configurato solo sui nodi gateway, poiché queste porte sono riservate sui nodi Admin.</p> <p>Nota: le porte utilizzate da altri servizi di rete non sono consentite. Consulta l'elenco delle porte utilizzate per le comunicazioni interne ed esterne:</p> <p>"Riferimento porta di rete"</p> <p>Quando si collega StorageGRID come livello cloud FabricPool, è necessario fornire lo stesso numero di porta a ONTAP.</p>
Protocollo	Deve essere HTTPS .

Campo	Descrizione
Modalità di associazione degli endpoint	<p>Utilizzare l'impostazione Global (scelta consigliata) o limitare l'accessibilità di questo endpoint a una delle seguenti opzioni:</p> <ul style="list-style-type: none"> • Indirizzi IP virtuali (VIP) specifici ad alta disponibilità (ha). Utilizzare questa opzione solo se si richiedono livelli di isolamento dei carichi di lavoro molto più elevati. • Interfacce di rete specifiche di nodi specifici.

4. Selezionare **Salva**.

Viene visualizzata la finestra di dialogo Edit Endpoint (Modifica endpoint).

5. Per **Endpoint Service Type**, selezionare **S3**.

6. Selezionare **carica certificato** (consigliato), quindi selezionare il certificato del server, la chiave privata del certificato e il bundle CA.

Load Certificate

Upload the PEM-encoded custom certificate, private key, and CA bundle files.

Server Certificate

Certificate Private Key

CA Bundle

7. Selezionare **Salva**.

Creazione di un account tenant per FabricPool

È necessario creare un account tenant in Grid Manager per l'utilizzo con FabricPool.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

A proposito di questa attività

Gli account tenant consentono alle applicazioni client di memorizzare e recuperare oggetti su StorageGRID. Ogni account tenant dispone di un proprio ID account, gruppi e utenti autorizzati, bucket e oggetti.

È possibile utilizzare lo stesso account tenant per più cluster ONTAP. In alternativa, è possibile creare un account tenant dedicato per ciascun cluster ONTAP, in base alle esigenze.



Queste istruzioni presuppongono che sia stato configurato il Single Sign-on (SSO) per Grid Manager. Se non si utilizza SSO, seguire le istruzioni per "[Creazione di un account tenant se StorageGRID non utilizza SSO](#)".

Fasi

1. Selezionare **tenant**.
2. Selezionare **Crea**.
3. Immettere un nome da visualizzare per l'account tenant FabricPool.
4. Selezionare **S3**.
5. Lasciare selezionata la casella di controllo **Allow Platform Services** (Consenti servizi piattaforma) per abilitare l'utilizzo dei servizi della piattaforma.

Se i servizi della piattaforma sono attivati, un tenant può utilizzare funzionalità, come la replica CloudMirror, che accedono ai servizi esterni.

6. Lasciare vuoto il campo **quota di storage**.
7. Nel campo **Root Access Group**, selezionare un gruppo federated esistente da Grid Manager per ottenere l'autorizzazione di accesso root iniziale per il tenant.
8. Selezionare **Salva**.

Creazione di un bucket S3 e ottenimento di una chiave 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 si utilizzerà per FabricPool.

Di cosa hai bisogno

- È necessario aver creato un account tenant per l'utilizzo di FabricPool.

A proposito di questa attività

Queste istruzioni descrivono come utilizzare il gestore tenant StorageGRID per creare un bucket e ottenere le chiavi di accesso. È inoltre possibile eseguire queste attività utilizzando l'API di gestione dei tenant o l'API REST di StorageGRID S3.

Per saperne di più:

- "[Utilizzare un account tenant](#)"
- "[Utilizzare S3](#)"

Fasi

1. Accedi al tenant manager.

È possibile effettuare una delle seguenti operazioni:

- Dalla pagina account tenant in Grid Manager, selezionare il collegamento **Accedi** per il tenant e immettere le credenziali.
- Immettere l'URL dell'account tenant in un browser Web e le credenziali.

2. Creare un bucket S3 per i dati FabricPool.

È necessario creare un bucket unico per ogni cluster ONTAP che si intende utilizzare.

- a. Selezionare **STORAGE (S3) > Bucket**.
- b. Selezionare **Crea bucket**.
- c. Immettere il nome del bucket StorageGRID che si intende utilizzare con FabricPool. Ad esempio, `fabricpool-bucket`.



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

I nomi dei bucket devono essere conformi alle seguenti regole:

- Deve essere unico in ogni sistema StorageGRID (non solo univoco all'interno dell'account tenant).
 - Deve essere conforme al DNS.
 - Deve contenere almeno 3 e non più di 63 caratteri.
 - Può essere una serie di una o più etichette, con etichette adiacenti separate da un punto. Ogni etichetta deve iniziare e terminare con una lettera minuscola o un numero e può utilizzare solo lettere minuscole, numeri e trattini.
 - Non deve essere simile a un indirizzo IP formattato con testo.
 - Non utilizzare i periodi nelle richieste di stile ospitate virtuali. I punti causano problemi con la verifica del certificato con caratteri jolly del server.
- d. Selezionare la regione per questo bucket.

Per impostazione predefinita, tutti i bucket vengono creati in `us-east-1` regione.

Create bucket ✕

Enter bucket details

Enter the bucket's name and select the bucket's region.

Bucket name ?

Region ?

us-east-1▼

Cancel Create bucket

- a. Selezionare **Crea bucket**.

3. Creare una chiave di accesso e una chiave di accesso segreta.

- a. Selezionare **STORAGE (S3) > My access key**.
- b. Selezionare **Crea chiave**.
- c. Selezionare **Crea chiave di accesso**.
- d. Copiare l'ID della chiave di accesso e la chiave di accesso segreta in una posizione sicura oppure selezionare **Download .csv** per salvare un 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 creano una nuova chiave di accesso e una chiave di accesso segreta, ricordarsi di aggiornare immediatamente i valori corrispondenti in ONTAP per garantire che ONTAP possa memorizzare e recuperare i dati in StorageGRID senza interruzioni.

Utilizzo della gestione del ciclo di vita delle informazioni StorageGRID con i dati FabricPool

Se si utilizza FabricPool per eseguire il tiering dei dati in StorageGRID, è necessario comprendere i requisiti per la creazione di regole ILM (Information Lifecycle Management) di StorageGRID e una policy ILM per la gestione dei dati FabricPool. È necessario garantire che le regole ILM applicabili ai dati FabricPool non siano disgreganti.



FabricPool non conosce le regole o le policy ILM di StorageGRID. La perdita di dati può verificarsi se il criterio ILM di StorageGRID non è configurato correttamente.

Per saperne di più: ["Gestire gli oggetti con ILM"](#)

Linee guida ILM per i dati FabricPool

Consulta queste linee guida per assicurarti che le tue regole ILM e le policy ILM siano adatte ai dati FabricPool e ai tuoi requisiti di business. Se si utilizza già ILM di StorageGRID, potrebbe essere necessario aggiornare il criterio ILM attivo per soddisfare queste linee guida.

- Puoi utilizzare qualsiasi combinazione di regole di replica e erasure coding per proteggere i dati del livello cloud.

La Best practice consigliata consiste nell'utilizzare la codifica di cancellazione 2+1 all'interno di un sito per una protezione dei dati conveniente. L'erasure coding utilizza più CPU, ma una capacità di storage significativamente inferiore rispetto alla replica. Gli schemi 4+1 e 6+1 utilizzano una capacità inferiore rispetto a 2+1, ma a un costo di throughput inferiore e minore flessibilità quando si aggiungono nodi di storage durante l'espansione della griglia.

- Ogni regola applicata ai dati FabricPool deve utilizzare la codifica di cancellazione oppure creare almeno due copie replicate.



Una regola ILM che crea una sola copia replicata per qualsiasi periodo di tempo mette i dati a rischio di perdita permanente. Se esiste una sola copia replicata di un oggetto, quest'ultimo viene perso in caso di errore o errore significativo di un nodo di storage. Inoltre, durante le procedure di manutenzione, ad esempio gli aggiornamenti, si perde temporaneamente l'accesso all'oggetto.

- Non utilizzare una regola ILM che scadrà o eliminerà i dati del livello cloud di FabricPool. Impostare il periodo di conservazione in ogni regola ILM su "Perforever" per garantire che gli oggetti FabricPool non vengano eliminati da ILM StorageGRID.
- Non creare regole che spostino i dati del Tier cloud FabricPool dal bucket a un'altra posizione. Non è possibile utilizzare le regole ILM per archiviare i dati FabricPool su nastro utilizzando un nodo di archiviazione o utilizzare un pool di storage cloud per spostare i dati FabricPool su Glacier.



L'utilizzo dei pool di storage cloud con FabricPool non è supportato a causa della latenza aggiunta per recuperare un oggetto dalla destinazione del pool di storage cloud.

- A partire da ONTAP 9.8, è possibile creare tag a oggetti per semplificare la classificazione e l'ordinamento dei dati a più livelli. Ad esempio, è possibile impostare i tag solo sui volumi FabricPool collegati a StorageGRID. Quindi, quando si creano le regole ILM in StorageGRID, è possibile utilizzare il filtro avanzato tag oggetto per selezionare e inserire questi dati.

Esempio di policy ILM per i dati FabricPool

Utilizza questo semplice esempio di policy come punto di partenza per le tue regole e policy ILM.

In questo esempio si presuppone che si stiano progettando le regole ILM e una policy ILM per un sistema StorageGRID con quattro nodi di storage in un singolo 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 diversi modi per configurare le regole ILM. Prima di attivare una nuova policy, simulare la policy proposta per confermare che funzionerà come previsto per proteggere il contenuto dalla perdita.

Per saperne di più: ["Gestire gli oggetti con ILM"](#)

Fasi

1. Creare un pool di storage denominato **DEN**. Selezionare il sito di Denver.
2. Creare un profilo di codifica Erasure denominato **2 più 1**. Selezionare lo schema di erasure coding 2+1 e il pool di storage **DEN**.
3. Creare una regola ILM che si applica solo ai dati in `fabricpool-bucket`. Questa regola di esempio consente di creare copie codificate per la cancellazione.

Definizione della regola	Valore di esempio
Nome regola	2 più 1 erasure coding per i dati FabricPool

Definizione della regola	Valore di esempio
Nome bucket	fabricpool-bucket È anche possibile filtrare l'account tenant FabricPool.
Filtraggio avanzato	Dimensione oggetto (MB) maggiore di 0.2 MB. Nota: FabricPool scrive solo oggetti da 4 MB, ma è necessario aggiungere un filtro dimensione oggetto perché questa regola utilizza la codifica di cancellazione.
Tempo di riferimento	Tempo di acquisizione
Posizionamento	Dal giorno 0 memorizzare per sempre
Tipo	Codifica di cancellazione
Posizione	DEN (2 più 1)
Comportamento di acquisizione	Bilanciato

4. Creare una regola ILM che creerà due copie replicate di qualsiasi oggetto non corrispondente alla prima regola. Non selezionare un filtro di base (account tenant o nome bucket) o filtri avanzati.

Definizione della regola	Valore di esempio
Nome regola	Due copie replicate
Nome bucket	<i>nessuno</i>
Filtraggio avanzato	<i>nessuno</i>
Tempo di riferimento	Tempo di acquisizione
Posizionamento	Dal giorno 0 memorizzare per sempre
Tipo	Replicato
Posizione	DEN
Copie	2
Comportamento di acquisizione	Bilanciato

5. Creare una policy ILM proposta e selezionare le due regole. Poiché la regola di replica non utilizza alcun filtro, può essere l'ultima regola predefinita per il criterio.
6. Acquisire oggetti di test nella griglia.
7. Simulare il criterio con gli oggetti di test per verificare il comportamento.
8. Attivare il criterio.

Quando questo criterio è attivato, StorageGRID inserisce i dati degli oggetti come segue:

- I dati a più livelli di FabricPool in `fabricpool-bucket` verrà eseguito un erasure coding utilizzando lo schema di erasure coding 2+1. Due frammenti di dati e un frammento di parità verranno posizionati su tre diversi nodi di storage.
- Tutti gli oggetti in tutti gli altri bucket verranno replicati. Verranno create due copie e collocate su due diversi nodi di storage.
- Le copie replicate e codificate in cancellazione verranno conservate in StorageGRID fino a quando non verranno eliminate dal client S3. StorageGRID ILM non eliminerà mai questi elementi.

Creazione di una policy di classificazione del traffico per FabricPool

È possibile, in via opzionale, progettare una policy di classificazione del traffico StorageGRID per ottimizzare la qualità del servizio per il carico di lavoro FabricPool.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre dell'autorizzazione di accesso root.

A proposito di questa attività

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 StorageGRID, assicurarsi che il carico di lavoro FabricPool abbia la 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, le operazioni di lettura FabricPool sono più importanti per le priorità rispetto alle operazioni di scrittura.

Ad esempio, se altri client S3 utilizzano questo sistema StorageGRID, è necessario creare un criterio di classificazione del traffico. È possibile limitare il traffico di rete per gli altri bucket, tenant, subnet IP o endpoint del bilanciamento del carico.

- Come regola generale, non è necessario imporre limiti di qualità del servizio su qualsiasi carico di lavoro FabricPool; è necessario limitare solo gli altri carichi di lavoro.
- I limiti imposti su altri workload potrebbero dover essere ampi per tenere conto del comportamento sconosciuto di tali workload. I limiti imposti variano anche in base al dimensionamento e alle funzionalità del tuo grid e alla quantità di utilizzo prevista.

Per saperne di più: ["Gestione delle policy di classificazione del traffico"](#)

Fasi

1. Selezionare **Configurazione > Impostazioni di rete > classificazione del traffico**.
2. Inserire un nome e una descrizione.
3. Nella sezione regole corrispondenti, creare almeno una regola.
 - a. Selezionare **Crea**.
 - b. Selezionare **endpoint** e selezionare l'endpoint del bilanciamento del carico creato per FabricPool.

È inoltre possibile selezionare l'account o il bucket del tenant FabricPool.
 - c. Se si desidera che questo criterio di traffico limiti il traffico per gli altri endpoint, selezionare **corrispondenza inversa**.
4. Facoltativamente, creare uno o più limiti.



Anche se non sono stati impostati limiti per una policy di classificazione del traffico, vengono raccolte metriche in modo da poter comprendere le tendenze del traffico.

- a. Selezionare **Crea**.
- b. Selezionare il tipo di traffico che si desidera limitare e il limite da applicare.

Questo esempio di classificazione del traffico FabricPool elenca i tipi di traffico di rete che è possibile limitare e i tipi di valori che è possibile selezionare. I tipi di traffico e i valori di una policy effettiva si baserebbero sui requisiti specifici dell'utente.

Edit Traffic Classification Policy "FabricPool"

Policy

Name  FabricPool

Description (optional) Limit traffic other than FabricPool

Matching Rules

Traffic that matches any rule is included in the policy.

 Create  Edit  Remove

	Type	Inverse Match	Match Value
<input checked="" type="radio"/>	Endpoint	<input checked="" type="checkbox"/>	FabricPool (https 10443)

Displaying 1 matching rule.

Limits (Optional)

 Create  Edit  Remove

	Type	Value	Units
<input checked="" type="radio"/>	Concurrent Read Requests	50	Concurrent Requests
<input checked="" type="radio"/>	Concurrent Write Requests	15	Concurrent Requests
<input checked="" type="radio"/>	Read Request Rate	100	Requests/Second
<input checked="" type="radio"/>	Write Request Rate	25	Requests/Second
<input checked="" type="radio"/>	Per-Request Bandwidth In	2000000	Bytes/Second
<input checked="" type="radio"/>	Per-Request Bandwidth Out	10000000	Bytes/Second

Displaying 6 limits.

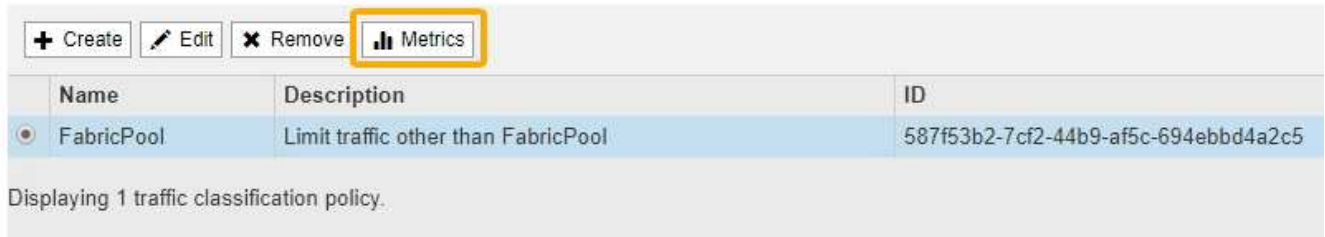
Cancel

Save

5. Dopo aver creato il criterio di classificazione del traffico, selezionare il criterio, quindi selezionare **metriche** per determinare se il criterio limita il traffico come previsto.

Traffic Classification Policies

Traffic classification policies can be used to identify network traffic for metrics reporting and optional traffic limiting.



Name	Description	ID
<input checked="" type="radio"/> FabricPool	Limit traffic other than FabricPool	587f53b2-7cf2-44b9-af5c-694ebbd4a2c5

Displaying 1 traffic classification policy.

Altre Best practice per StorageGRID e FabricPool

Quando si configura un sistema StorageGRID per l'utilizzo con FabricPool, evitare di impostare opzioni globali che potrebbero influire sul modo in cui i dati vengono salvati.

Crittografia degli oggetti

Durante la configurazione di StorageGRID, è possibile attivare l'impostazione globale **crittografia oggetti memorizzati** se è richiesta la crittografia dei dati per altri client StorageGRID (**Configurazione > Impostazioni di sistema > Opzioni griglia**). I dati a più livelli da FabricPool a StorageGRID sono già crittografati, pertanto l'attivazione dell'impostazione StorageGRID non è necessaria. Le chiavi di crittografia lato client sono di proprietà di ONTAP.

Compressione degli oggetti

Durante la configurazione di StorageGRID, non attivare l'impostazione globale **Comprimi oggetti memorizzati** (**Configurazione > Impostazioni di sistema > Opzioni griglia**). I dati a più livelli da FabricPool a StorageGRID sono già compressi. L'attivazione di **compress stored objects** non riduce ulteriormente la dimensione di un oggetto.

Livello di coerenza

Per i bucket FabricPool, il livello di coerenza consigliato è **Read-after-new-write**, che è l'impostazione predefinita per un nuovo bucket. Non modificare i bucket FabricPool per utilizzare **Available** o qualsiasi altro livello di coerenza.

Tiering FabricPool

Se il nodo StorageGRID utilizza lo storage assegnato da un sistema NetApp AFF, verificare che il volume non disponga di un criterio di tiering FabricPool attivato. Ad esempio, se un nodo StorageGRID è in esecuzione su un host VMware, assicurarsi che il volume che esegue il backup del datastore per il nodo StorageGRID non abbia un criterio di tiering FabricPool attivato. La disattivazione del tiering FabricPool per i volumi utilizzati con i nodi StorageGRID semplifica la risoluzione dei problemi e le operazioni di storage.



Non utilizzare mai FabricPool per eseguire il tiering dei dati relativi a StorageGRID su StorageGRID. Il tiering dei dati StorageGRID su StorageGRID aumenta la risoluzione dei problemi e la complessità operativa.

Informazioni sul copyright

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

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

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

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

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

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

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

Informazioni sul marchio commerciale

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