



Usa i Cloud Storage Pool

StorageGRID software

NetApp
July 23, 2026

Sommario

Usa i Cloud Storage Pool	1
Scopri i Cloud Storage Pool in StorageGRID	1
Ciclo di vita di un oggetto pool di storage cloud in StorageGRID	2
S3: Ciclo di vita di un oggetto Cloud Storage Pool	2
Azure: Ciclo di vita di un oggetto pool di storage cloud	3
Casi d'uso del Cloud Storage Pool in StorageGRID	4
Esegui il backup dei dati di StorageGRID in una posizione esterna	4
Sposta i dati di livello da StorageGRID a una posizione esterna	4
Gestisci più endpoint cloud	5
Requisiti e limiti del pool di storage cloud in StorageGRID	5
Considerazioni generali	5
Considerazioni sulle porte utilizzate per i Cloud Storage Pools	6
Considerazioni sui costi	6
S3: Autorizzazioni richieste per il bucket del Cloud Storage Pool	6
S3: Considerazioni sul ciclo di vita del bucket esterno	7
Azure: considerazioni per il tier Access	8
Azure: la gestione del ciclo di vita non è supportata	8
Pool di storage cloud e replica CloudMirror in StorageGRID	8
Crea un pool di storage cloud in StorageGRID	10
Visualizza i dettagli del pool di storage cloud in StorageGRID	14
Modifica un pool di storage cloud in StorageGRID	15
Rimuovere un Cloud Storage Pool in StorageGRID	16
Se necessario, usa ILM per spostare i dati degli oggetti	16
Elimina il pool di storage cloud	17
Risoluzione dei problemi dei pool di storage cloud in StorageGRID	17
\${post_edited_translations.segment}	17
Verifica se l'errore è stato risolto	18
Errore: Controllo di integrità non riuscito. Errore dall'endpoint	18
Errore: questo Cloud Storage Pool contiene contenuti imprevisti	18
Errore: Impossibile creare o aggiornare il Cloud Storage Pool. Errore dall'endpoint	19
Errore: impossibile analizzare il certificato CA	19
Errore: non è stato trovato un Cloud Storage Pool con questo ID	19
Errore: Impossibile verificare il contenuto del pool di storage cloud. Errore dall'endpoint	20
Errore: in questo bucket sono già stati inseriti oggetti	20
Errore: il proxy ha riscontrato un errore esterno durante il tentativo di raggiungere il Cloud Storage Pool	20
Errore: il certificato X.509 è fuori dal periodo di validità	20

Usa i Cloud Storage Pool

Scopri i Cloud Storage Pool in StorageGRID

Un pool di cloud storage ti permette di usare ILM per spostare i dati degli oggetti al di fuori del sistema StorageGRID. Ad esempio, potresti voler spostare oggetti a cui accedi raramente verso cloud storage a costo inferiore, come Amazon S3 Glacier, S3 Glacier Deep Archive, Google Cloud o il livello di accesso Archive in Microsoft Azure Blob storage. Oppure, potresti voler mantenere un backup cloud degli oggetti StorageGRID per migliorare il disaster recovery.

Dal punto di vista dell'ILM, un Cloud Storage Pool è simile a un pool di storage. Per archiviare oggetti in entrambe le posizioni, selezioni il pool quando crei le istruzioni di posizionamento per una regola ILM. Tuttavia, mentre i pool di storage sono costituiti da Storage Nodes all'interno del sistema StorageGRID, un Cloud Storage Pool è costituito da un bucket esterno (S3) o da un container (Azure Blob storage).

La tabella confronta i pool di storage con i Cloud Storage Pools e mostra le high-level somiglianze e differenze.

	Pool di storage	Pool di storage cloud
Come lo crei?	Utilizzando l'opzione ILM > Storage pools in Grid Manager.	Utilizzando l'opzione ILM > Storage pools > Cloud Storage Pools in Grid Manager. Devi configurare il bucket o il container esterno prima di poter creare il Cloud Storage Pool.
Quanti pool puoi creare?	Illimitato.	Fino a 10.
Dove sono memorizzati gli oggetti?	Su uno o più nodi di storage all'interno di StorageGRID.	In un bucket Amazon S3, in un container Azure Blob storage o in Google Cloud esterno al sistema StorageGRID. Se il pool di cloud storage è un bucket Amazon S3: • Puoi configurare facoltativamente un ciclo di vita del bucket per trasferire gli oggetti in storage a basso costo e a lungo termine, come Amazon S3 Glacier o S3 Glacier Deep Archive. Il sistema storage esterno deve supportare la classe di storage Glacier e l'API S3 RestoreObject. • Puoi creare Cloud Storage Pools da usare con AWS Commercial Cloud Services (C2S), che supportano la AWS Secret Region. Se il Cloud Storage Pool è un container Azure Blob storage, StorageGRID sposta l'oggetto al livello Archive. Nota: In generale, non configurare la gestione del ciclo di vita di Azure Blob storage per il container utilizzato per un Cloud Storage Pool. RestoreObject operazioni sugli oggetti nel Cloud Storage Pool possono essere influenzate dal ciclo di vita configurato.

	Pool di storage	Pool di storage cloud
Cosa controlla il posizionamento degli oggetti?	Una regola ILM nelle policy ILM attive.	Una regola ILM nelle policy ILM attive.
Quale metodo di protezione dei dati usi?	Replica o erasure coding.	Replicazione.
Quante copie di ciascun oggetto sono consentite?	Molteplici.	Una copia nel Cloud Storage Pool e, facoltativamente, una o più copie in StorageGRID. Nota: Non puoi archiviare un oggetto in più di un Cloud Storage Pool contemporaneamente.
Quali sono i vantaggi?	Gli oggetti sono accessibili rapidamente in qualsiasi momento.	Storage a basso costo. Nota: I dati di FabricPool non possono essere suddivisi in livelli nei Cloud Storage Pools.

Ciclo di vita di un oggetto pool di storage cloud in StorageGRID

Prima di implementare i Cloud Storage Pool, rivedi il ciclo di vita degli oggetti che sono archiviati in ciascun tipo di Cloud Storage Pool.

S3: Ciclo di vita di un oggetto Cloud Storage Pool

I passaggi descrivono le fasi del ciclo di vita di un oggetto archiviato in un S3 Cloud Storage Pool.



"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 Expedited. Sono supportati solo i recuperi Bulk o Standard.



La piattaforma Google Cloud (GCP) supporta il recupero di oggetti da storage a lungo termine senza richiedere un'operazione POST Restore.

1. Oggetto memorizzato in StorageGRID

Per avviare il ciclo di vita, un'applicazione client memorizza un oggetto in StorageGRID.

2. Oggetto spostato nel pool di storage cloud S3

- Quando l'oggetto viene identificato da una regola ILM che utilizza un S3 Cloud Storage Pool come posizione di collocazione, StorageGRID sposta l'oggetto nel bucket S3 esterno specificato dal Cloud

Storage Pool.

- Quando l'oggetto viene spostato nel pool di storage cloud S3, l'applicazione client può recuperarlo tramite una richiesta S3 GetObject da StorageGRID, a meno che l'oggetto non sia stato trasferito nello storage Glacier.

3. Oggetto trasferito in Glacier (stato non recuperabile)

- Facoltativamente, l'oggetto può essere trasferito 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 vuoi trasferire gli oggetti, devi creare una configurazione del ciclo di vita per il bucket S3 esterno e devi usare una soluzione storage che implementa la classe di storage Glacier e supporta l'API S3 RestoreObject.

- Durante la transizione, l'applicazione client può utilizzare una richiesta S3 HeadObject per monitorare lo stato dell'oggetto.

4. Oggetto ripristinato dallo storage Glacier

Se un oggetto è stato migrato allo storage Glacier, l'applicazione client può inviare una richiesta S3 RestoreObject per ripristinare una copia recuperabile nel pool di storage cloud S3. La richiesta specifica per quanti giorni la copia deve essere disponibile nel pool di storage cloud e il livello di accesso ai dati da utilizzare per l'operazione di ripristino (Expedited, Standard o Bulk). Quando viene raggiunta la data di scadenza della copia recuperabile, la copia viene automaticamente riportata a uno stato non recuperabile.



Se una o più copie dell'oggetto esistono anche sui nodi di storage all'interno di StorageGRID, non è necessario ripristinare l'oggetto da Glacier inviando una richiesta RestoreObject. Invece, la copia locale può essere recuperata direttamente tramite una richiesta GetObject.

5. Oggetto recuperato

Una volta ripristinato un oggetto, l'applicazione client può inviare una richiesta GetObject per recuperare l'oggetto ripristinato.

Azure: Ciclo di vita di un oggetto pool di storage cloud

I passaggi descrivono le fasi del ciclo di vita di un oggetto archiviato in un pool di storage cloud di Azure.

1. Oggetto memorizzato in StorageGRID

Per avviare il ciclo di vita, un'applicazione client memorizza un oggetto in StorageGRID.

2. Oggetto spostato nel pool di storage cloud di Azure

Quando l'oggetto viene abbinato a una regola ILM che utilizza un pool di storage cloud Azure come posizione di collocazione, StorageGRID sposta l'oggetto nel container Azure Blob storage esterno specificato dal Cloud Storage Pool.

3. Oggetto trasferito al livello Archivio (stato non recuperabile)

Subito dopo aver spostato l'oggetto nel pool di storage cloud di Azure, StorageGRID passa automaticamente l'oggetto al livello Archive di Azure Blob storage.

4. Oggetto ripristinato dal livello Archive

Se un oggetto è stato spostato nel livello Archivio, l'applicazione client può inviare una richiesta S3 RestoreObject per ripristinare una copia recuperabile nel pool di storage Azure Cloud Storage Pool.

Quando StorageGRID riceve la RestoreObject, sposta temporaneamente l'oggetto nel livello Cool di Azure Blob storage. Non appena viene raggiunta la data di scadenza nella richiesta RestoreObject, StorageGRID riporta l'oggetto al livello Archive.



Se una o più copie dell'oggetto esistono anche sui nodi di storage all'interno di StorageGRID, non è necessario ripristinare l'oggetto dal livello di accesso Archive inviando una richiesta RestoreObject. Invece, puoi recuperare direttamente la copia locale usando una richiesta GetObject.

5. Oggetto recuperato

Una volta che un oggetto è stato ripristinato nel pool di storage cloud di Azure, l'applicazione client può inviare una richiesta GetObject per recuperare l'oggetto ripristinato.

Informazioni correlate

["\\${post_edited_translations.segment}"](#)

Casi d'uso del Cloud Storage Pool in StorageGRID

Utilizzando i Cloud Storage Pools, puoi eseguire il backup o il tiering dei dati in una posizione esterna. Inoltre, puoi eseguire il backup o il tiering dei dati in più di un cloud.

Esegui il backup dei dati di StorageGRID in una posizione esterna

Puoi usare un Cloud Storage Pool per eseguire il backup degli oggetti StorageGRID in una posizione esterna.

Se le copie in StorageGRID non sono accessibili, puoi utilizzare i dati degli oggetti nel Cloud Storage Pool per soddisfare le richieste dei client. Tuttavia, potresti dover inviare una richiesta S3 RestoreObject per accedere alla copia di backup dell'oggetto nel Cloud Storage Pool.

I dati degli oggetti in un Cloud Storage Pool possono essere utilizzati anche per recuperare i dati persi da StorageGRID a causa di un errore del volume di storage o dello Storage Node. Se l'unica copia rimanente di un oggetto si trova in un Cloud Storage Pool, StorageGRID ripristina temporaneamente l'oggetto e crea una nuova copia sullo Storage Node ripristinato.

Per implementare una soluzione di backup:

1. Crea un singolo Cloud Storage Pool.
2. Configura una regola ILM che memorizza simultaneamente copie degli oggetti sui Storage Node (come copie replicate o con codifica di cancellazione) e una singola copia dell'oggetto nel Cloud Storage Pool.
3. Aggiungi la regola alla tua policy ILM. Poi, simula e attiva la policy.

Sposta i dati di livello da StorageGRID a una posizione esterna

Puoi usare un Cloud Storage Pool per memorizzare oggetti al di fuori del sistema StorageGRID. Ad esempio, supponi di avere un gran numero di oggetti che devi conservare, ma prevedi di accedervi raramente, se mai.

Puoi usare un Cloud Storage Pool per spostare gli oggetti in uno storage a costo inferiore e liberare spazio in StorageGRID.

Per implementare una soluzione di tiering:

1. Crea un singolo Cloud Storage Pool.
2. Configura una regola ILM che sposta gli oggetti usati raramente dai Storage Node al Cloud Storage Pool.
3. Aggiungi la regola alla tua policy ILM. Poi, simula e attiva la policy.

Gestisci più endpoint cloud

Puoi configurare più endpoint di Cloud Storage Pool se vuoi eseguire il tiering o il backup dei dati degli oggetti su più cloud. I filtri nelle tue regole ILM ti permettono di specificare quali oggetti vengono archiviati in ciascun Cloud Storage Pool. Ad esempio, potresti voler archiviare gli oggetti di alcuni tenant o bucket in Amazon S3 Glacier e gli oggetti di altri tenant o bucket in Azure Blob storage. Oppure, potresti voler spostare i dati tra Amazon S3 Glacier e Azure Blob storage.



Quando usi più endpoint di Cloud Storage Pool, tieni presente che un oggetto può essere archiviato in un solo Cloud Storage Pool alla volta.

Per implementare più endpoint cloud:

1. Crea fino a 10 Cloud Storage Pools.
2. Configura le regole ILM per archiviare i dati degli oggetti appropriati al momento opportuno in ciascun Cloud Storage Pool. Ad esempio, archivia gli oggetti del bucket A nel Cloud Storage Pool A e gli oggetti del bucket B nel Cloud Storage Pool B. Oppure, archivia gli oggetti nel Cloud Storage Pool A per un certo periodo di tempo e poi spostali nel Cloud Storage Pool B.
3. Aggiungi le regole alla tua policy ILM. Poi, simula e attiva la policy.

Requisiti e limiti del pool di storage cloud in StorageGRID

Se hai intenzione di usare un Cloud Storage Pool per spostare oggetti fuori dal sistema StorageGRID, devi esaminare le considerazioni per la configurazione e l'utilizzo dei Cloud Storage Pool.

Considerazioni generali

- In generale, l'archiviazione cloud di tipo archivio, come Amazon S3 Glacier o Azure Blob storage, è un posto economico dove memorizzare dati a oggetti. Tuttavia, i costi per recuperare i dati dall'archiviazione cloud di tipo archivio sono relativamente alti. Per ottenere il costo complessivo più basso, devi considerare quando e quanto spesso accederai agli oggetti nel Cloud Storage Pool. Si consiglia di usare un Cloud Storage Pool solo per contenuti a cui pensi di accedere raramente.
- L'uso di Cloud Storage Pool con FabricPool non è supportato a causa della latenza aggiuntiva per recuperare un oggetto dal target del Cloud Storage Pool.
- Gli oggetti con S3 Object Lock abilitato non possono essere inseriti nei Cloud Storage Pools.
- Le seguenti combinazioni di piattaforma, autenticazione e protocollo con S3 Object lock non sono supportate per i Cloud Storage Pools:
 - **Piattaforme:** Google Cloud Platform e Azure

- **Tipi di autenticazione:** Accesso anonimo
- **Protocollo:** HTTP

Considerazioni sulle porte utilizzate per i Cloud Storage Pools

Per garantire che le regole ILM possano spostare oggetti da e verso il Cloud Storage Pool specificato, devi configurare la rete o le reti che contengono i Storage Node del sistema. Devi assicurarti che le seguenti porte possano comunicare con il Cloud Storage Pool.

Per impostazione predefinita, i Cloud Storage Pools utilizzano le seguenti porte:

- **80:** Per gli URI degli endpoint che iniziano con http
- **443:** Per gli URI degli endpoint che iniziano con https

Puoi specificare una porta diversa quando crei o modifichi un Cloud Storage Pool.

Se usi un proxy server non trasparente, devi anche ["configurare un proxy storage"](#) consentire l'invio di messaggi a endpoint esterni, come un endpoint su internet.

Considerazioni sui costi

L'accesso allo storage nel cloud tramite un Cloud Storage Pool richiede la connettività di rete al cloud. Devi considerare il costo dell'infrastruttura di rete che userai per accedere al cloud e predisporla in modo appropriato, in base alla quantità di dati che prevedi di spostare tra StorageGRID e il cloud usando il Cloud Storage Pool.

Quando StorageGRID si connette all'endpoint esterno del Cloud Storage Pool, invia diverse richieste per monitorare la connettività e assicurarsi di poter eseguire le operazioni richieste. Sebbene queste richieste comportino dei costi aggiuntivi, il costo del monitoraggio di un Cloud Storage Pool dovrebbe rappresentare solo una piccola frazione del costo complessivo dell'archiviazione degli oggetti in S3 o Azure.

Potrebbero essere sostenuti costi più significativi se devi spostare oggetti da un endpoint esterno del Cloud Storage Pool a StorageGRID. Gli oggetti potrebbero essere spostati nuovamente in StorageGRID in uno di questi casi:

- L'unica copia dell'oggetto si trova in un Cloud Storage Pool e decidi di archiviare l'oggetto in StorageGRID invece. In questo caso, riconfiguri le tue regole e policy ILM. Quando avviene la valutazione ILM, StorageGRID invia più richieste per recuperare l'oggetto dal Cloud Storage Pool. StorageGRID crea quindi localmente il numero specificato di copie replicate o con codifica di cancellazione. Dopo che l'oggetto viene spostato di nuovo in StorageGRID, la copia nel Cloud Storage Pool viene eliminata.
- Gli oggetti vengono persi a causa di un errore del nodo di archiviazione. Se l'unica copia rimanente di un oggetto si trova in un Cloud Storage Pool, StorageGRID ripristina temporaneamente l'oggetto e crea una nuova copia sul nodo di archiviazione ripristinato.



Quando gli oggetti vengono spostati di nuovo su StorageGRID da un Cloud Storage Pool, StorageGRID invia più richieste all'endpoint del Cloud Storage Pool per ciascun oggetto. Prima di spostare un numero elevato di oggetti, contatta il supporto tecnico per ottenere aiuto nella stima dei tempi e dei costi associati.

S3: Autorizzazioni richieste per il bucket del Cloud Storage Pool

Le policy per il bucket S3 esterno utilizzato per un Cloud Storage Pool devono concedere a StorageGRID

l'autorizzazione a spostare un oggetto nel bucket, ottenere lo stato di un oggetto, ripristinare un oggetto da Glacier storage quando necessario e altro ancora. Idealmente, StorageGRID dovrebbe avere accesso con controllo completo al bucket (`s3:*`; tuttavia, se ciò non è possibile, la policy del bucket deve concedere le seguenti autorizzazioni S3 a StorageGRID:

- `s3:AbortMultipartUpload`
- `s3:DeleteObject`
- `s3:GetObject`
- `s3:ListBucket`
- `s3:ListBucketMultipartUploads`
- `s3:ListMultipartUploadParts`
- `s3:PutObject`
- `s3:RestoreObject`

S3: Considerazioni sul ciclo di vita del bucket esterno

Il movimento degli oggetti tra StorageGRID e il bucket S3 esterno specificato nel Cloud Storage Pool è controllato dalle regole ILM e dalle policy ILM attive in StorageGRID. Al contrario, il trasferimento degli oggetti dal bucket S3 esterno specificato nel Cloud Storage Pool ad Amazon S3 Glacier o S3 Glacier Deep Archive (o a una soluzione storage che implementa la classe di storage Glacier) è controllato dalla configurazione del ciclo di vita di quel bucket.

Se vuoi trasferire oggetti dal Cloud Storage Pool, devi creare la configurazione del ciclo di vita appropriata sul bucket S3 esterno e devi usare una soluzione storage che implementa la classe di storage Glacier e supporta l'API S3 `RestoreObject`.

Ad esempio, supponi di voler fare in modo che tutti gli oggetti spostati da StorageGRID al Cloud Storage Pool vengano trasferiti immediatamente in Amazon S3 Glacier storage. Dovresti creare una configurazione del ciclo di vita sul bucket S3 esterno che specifichi una sola azione (**Transition**) 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 sposterebbe tutti gli oggetti bucket su Amazon S3 Glacier il giorno stesso della loro creazione (ovvero, il giorno in cui vengono spostati da StorageGRID al Cloud Storage Pool).



Quando configuri il ciclo di vita del bucket esterno, non usare mai le azioni **Scadenza** per definire quando gli oggetti scadono. Le azioni di scadenza fanno sì che il sistema storage esterno elimini gli oggetti scaduti. Se in seguito provi ad accedere a un oggetto scaduto da StorageGRID, l'oggetto eliminato non verrà trovato.

Se vuoi migrare gli oggetti nel Cloud Storage Pool verso S3 Glacier Deep Archive (invece che verso Amazon S3 Glacier), specifica `<StorageClass>DEEP_ARCHIVE</StorageClass>` nel ciclo di vita del bucket. Tieni però presente che non puoi usare il livello `Expedited` per ripristinare oggetti da S3 Glacier Deep Archive.

Azure: considerazioni per il tier Access

Quando configuri un account di archiviazione Azure, puoi impostare il livello di accesso predefinito su Hot o Cool. Quando crei un account di archiviazione da usare con un Cloud Storage Pool, dovresti usare il livello Hot come livello predefinito. Anche se StorageGRID imposta immediatamente il livello su Archive quando sposta gli oggetti nel Cloud Storage Pool, usare l'impostazione predefinita Hot garantisce che non ti venga addebitato un costo di eliminazione anticipata per gli oggetti rimossi dal livello Cool prima dei 30 giorni minimi.

Azure: la gestione del ciclo di vita non è supportata

Non usare la gestione del ciclo di vita di Azure Blob storage per il container utilizzato con un Cloud Storage Pool. Le operazioni del ciclo di vita potrebbero interferire con le operazioni del Cloud Storage Pool.

Informazioni correlate

["\\${post_edited_translations.segment}"](#)

Pool di storage cloud e replica CloudMirror in StorageGRID

Quando inizi a utilizzare Cloud Storage Pools, potrebbe essere utile comprendere le somiglianze e le differenze tra Cloud Storage Pools e il servizio di replica CloudMirror di StorageGRID.

	Pool di storage cloud	servizio di replica CloudMirror
Qual è lo scopo principale?	Funge da destinazione di archiviazione. La copia dell'oggetto nel Cloud Storage Pool può essere l'unica copia dell'oggetto oppure una copia aggiuntiva. Cioè, invece di conservare due copie in sede, puoi conservarne una in StorageGRID e inviarne una al Cloud Storage Pool.	Consente a un tenant di replicare automaticamente gli oggetti da un bucket in StorageGRID (origine) a un bucket S3 esterno (destinazione). Crea una copia indipendente di un oggetto in un'infrastruttura S3 indipendente.
Come si configura?	Definito nello stesso modo dei pool di storage, usando il Grid Manager o la Grid Management API. Puoi selezionarlo come destinazione di posizionamento in una regola ILM. Mentre un pool di storage è costituito da un gruppo di Storage Node, un Cloud Storage Pool viene definito usando un endpoint S3 o Azure remoto (indirizzo IP, credenziali e così via).	Un utente tenant "configura la replica CloudMirror" definisce un endpoint CloudMirror (indirizzo IP, credenziali e così via) usando il Tenant Manager o l'API S3. Dopo che l'endpoint CloudMirror è stato configurato, qualsiasi bucket di proprietà di quell'account tenant può essere configurato per puntare all'endpoint CloudMirror.

	Pool di storage cloud	servizio di replica CloudMirror
Chi è responsabile della configurazione?	Di solito, un amministratore della grid	Di solito, un tenant
<code>\${post_edited_translations.segment}</code>	- Qualsiasi infrastruttura S3 compatibile (inclusi Amazon S3) - Livello Archive di Azure Blob <code>\${post_edited_translations.segment}</code>	- Qualsiasi infrastruttura S3 compatibile (inclusi Amazon S3) <code>\${post_edited_translations.segment}</code>
Cosa fa sì che gli oggetti vengano spostati verso la destinazione?	Una o più regole ILM nelle policy ILM attive. Le regole ILM definiscono quali oggetti StorageGRID sposta nel Cloud Storage Pool e quando gli oggetti vengono spostati.	L'azione di inserire un nuovo oggetto in un bucket di origine configurato con un endpoint CloudMirror. Gli oggetti già presenti nel bucket di origine prima che il bucket fosse configurato con l'endpoint CloudMirror non vengono replicati, a meno che non vengano modificati.
Come recuperi gli oggetti?	Le applicazioni devono inviare richieste a StorageGRID per recuperare gli oggetti che sono stati spostati in un Cloud Storage Pool. Se l'unica copia di un oggetto è stata trasferita nell'archivio, StorageGRID gestisce il processo di ripristino dell'oggetto in modo che possa essere recuperato.	Poiché la copia replicata nel bucket di destinazione è una copia indipendente, le applicazioni possono recuperare l'oggetto effettuando richieste sia a StorageGRID che alla destinazione S3. Ad esempio, supponi di usare la replica CloudMirror per replicare oggetti verso un'organizzazione partner. Il partner può usare le proprie applicazioni per leggere o aggiornare oggetti direttamente dalla destinazione S3. Non è necessario usare StorageGRID.
Puoi leggere direttamente dalla destinazione?	No. Gli oggetti spostati in un Cloud Storage Pool sono gestiti da StorageGRID. Le richieste di lettura devono essere indirizzate a StorageGRID (e StorageGRID sarà responsabile del recupero dal Cloud Storage Pool).	Sì, perché la copia speculare è una copia indipendente.
Cosa succede se un oggetto viene eliminato dalla sorgente?	L'oggetto viene inoltre eliminato dal Cloud Storage Pool.	L'azione di eliminazione non viene replicata. Un oggetto eliminato non esiste più nel bucket StorageGRID, ma continua a esistere nel bucket di destinazione. Allo stesso modo, gli oggetti nel bucket di destinazione possono essere eliminati senza influire sulla sorgente.

	Pool di storage cloud	servizio di replica CloudMirror
Come accedi agli oggetti dopo un disastro (StorageGRID non operativo)?	I nodi StorageGRID non funzionanti devono essere ripristinati. Durante questo processo, le copie degli oggetti replicati potrebbero essere ripristinate utilizzando le copie presenti nel Cloud Storage Pool.	Le copie degli oggetti nella destinazione CloudMirror sono indipendenti da StorageGRID, quindi puoi accedervi direttamente prima che i nodi StorageGRID vengano ripristinati.

Crea un pool di storage cloud in StorageGRID

Un cloud storage pool specifica un singolo bucket Amazon S3 esterno o un altro cloud provider compatibile con S3 oppure un container Azure Blob storage.

Quando crei un Cloud Storage Pool, specifichi il nome e la posizione del bucket o container esterno che StorageGRID userà per archiviare gli oggetti, il tipo di cloud provider (Amazon S3/GCP o Azure Blob storage) e le informazioni di cui StorageGRID ha bisogno per accedere al bucket o container esterno.

StorageGRID convalida il Cloud Storage Pool non appena lo salvi, quindi devi assicurarti che il bucket o container specificato nel Cloud Storage Pool esista e sia raggiungibile.

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Tu hai il ["autorizzazioni di accesso richieste"](#).
- Hai esaminato il ["Considerazioni sui Cloud Storage Pool"](#).
- Il bucket o container a cui fa riferimento il Cloud Storage Pool esiste già e hai il [informazioni sull'endpoint del servizio](#).
- Per accedere al bucket o container, hai l'[informazioni sull'account per il tipo di autenticazione](#) che sceglierai.

Passaggi

1. Seleziona **ILM > Storage pools > Cloud Storage Pools**.
2. Seleziona **Crea**, quindi inserisci le seguenti informazioni:

Campo	Descrizione
Nome del cloud storage pool	Un nome che descrive brevemente il Cloud Storage Pool e il suo scopo. Usa un nome che sia facile da identificare quando configuri le regole ILM.
Tipo di provider	Quale cloud provider utilizzerai per questo Cloud Storage Pool? • Amazon S3/GCP: Seleziona questa opzione per un Amazon S3, Commercial Cloud Services (C2S) S3, Google Cloud Platform (GCP) o un altro provider compatibile con S3. • Azure Blob Storage

Campo	Descrizione
Bucket o container	Il nome del bucket S3 esterno o container Azure. Non puoi modificare questo valore dopo che il Cloud Storage Pool è stato salvato.

3. In base al tipo di provider selezionato, inserisci le informazioni sull'endpoint del servizio.

Amazon S3/GCP

- a. Per il protocollo, seleziona HTTPS o HTTP.



Non usare connessioni HTTP per dati sensibili.

- b. Inserisci il nome host. Esempio:

`s3-aws-region.amazonaws.com`

- c. Seleziona lo stile URL:

Opzione	Descrizione
Rilevamento automatico	Tenta di rilevare automaticamente quale stile di URL utilizzare, in base alle informazioni fornite. Ad esempio, se specifichi un indirizzo IP, StorageGRID utilizzerà un URL in stile percorso. Seleziona questa opzione solo se non sai quale stile specifico utilizzare.
Stile virtual-hosted	Utilizza un URL in stile virtual-hosted per accedere al bucket. Gli URL in stile virtual-hosted includono il nome del bucket come parte del domain name. Esempio: <code>https://bucket-name.s3.company.com/key-name</code>
Stile path	Utilizza un URL in formato percorso per accedere al bucket. Gli URL in formato percorso includono il nome del bucket alla fine. Esempio: <code>https://s3.company.com/bucket-name/key-name</code> Nota: L'opzione URL in formato percorso non è consigliata e verrà deprecata in una versione futura di StorageGRID.

- d. Facoltativamente, inserisci il numero di porta oppure usa la porta predefinita: 443 per HTTPS o 80 per HTTP.

Azure Blob Storage

- a. Utilizzando uno dei seguenti formati, inserisci l'URI dell'endpoint del servizio.

- `https://host:port`
- `http://host:port`

Esempio: `https://myaccount.blob.core.windows.net:443`

Se non specifichi una porta, per impostazione predefinita viene utilizzata la porta 443 per HTTPS e la porta 80 per HTTP.

4. Seleziona **Continua**. Quindi seleziona il tipo di autenticazione e inserisci le informazioni richieste per l'endpoint del Cloud Storage Pool:

Chiave di accesso

Per Amazon S3/GCP o altri cloud provider compatibili con S3

- a. **ID chiave di accesso:** Inserisci l'ID della chiave di accesso per l'account che possiede il bucket esterno.
- b. **Chiave di accesso segreta:** Inserisci la chiave di accesso segreta.

IAM Roles Anywhere

Per il servizio AWS IAM Roles Anywhere

StorageGRID utilizza AWS Security Token Service (STS) per generare dinamicamente un token di breve durata per accedere alle risorse AWS.

- a. **Regione di AWS IAM Roles Anywhere:** Seleziona la regione per il pool di storage cloud. Ad esempio, `us-east-1`.
- b. **URN dell'ancora di fiducia:** Inserisci l'URN dell'ancora di fiducia che convalida le richieste di credenziali STS a breve termine. Può essere una CA root o intermedia.
- c. **URN del profilo:** Inserisci l'URN del profilo IAM Roles Anywhere che elenca i ruoli che possono essere assunti da chiunque sia considerato attendibile.
- d. **URN del ruolo:** Inserisci l'URN del ruolo IAM che può essere assunto da chiunque sia considerato affidabile.
- e. **Durata della sessione:** Inserisci la durata delle credenziali di sicurezza temporanee e della sessione del ruolo. Inserisci almeno 15 minuti e non più di 12 ore.
- f. **Certificato CA del server** (facoltativo): uno o più certificati CA attendibili, in formato PEM, per verificare il server IAM Roles Anywhere. Se omissso, il server non viene verificato.
- g. **Certificato dell'entità finale:** la chiave pubblica, in formato PEM, del certificato X509 firmato dall'ancora di fiducia. AWS IAM Roles Anywhere utilizza questa chiave per emettere un token STS.
- h. **Chiave privata dell'entità finale:** La chiave privata per il certificato dell'entità finale.

CAP (portale di accesso C2S)

Per il servizio Commercial Cloud Services (C2S) S3

- a. **URL delle credenziali temporanee:** Inserisci l'URL completo che StorageGRID userà per ottenere le credenziali temporanee dal server CAP, inclusi tutti i parametri API obbligatori e facoltativi assegnati al tuo account C2S.
- b. **Certificato CA del server:** Seleziona **Sfoglia** e carica il certificato CA che StorageGRID utilizzerà per verificare il server CAP. Il certificato deve essere codificato in formato PEM ed essere rilasciato da un'autorità di certificazione (CA) governativa appropriata.
- c. **Certificato client:** Seleziona **Sfoglia** e carica il certificato che StorageGRID utilizzerà per identificarsi al server CAP. Il certificato client deve essere codificato in formato PEM, rilasciato da un'autorità di certificazione (CA) governativa appropriata e deve consentire l'accesso al tuo account C2S.
- d. **Chiave privata del client:** Seleziona **Sfoglia** e carica la chiave privata codificata in formato PEM per il certificato client.
- e. Se la chiave privata del client è crittografata, inserisci la passphrase per decrittare la chiave privata del client. Altrimenti, lascia il campo **Passphrase della chiave privata del client** vuoto.



Se il certificato client deve essere crittografato, usa il formato tradizionale per la crittografia. Il formato crittografato PKCS #8 non è supportato.

Azure Blob Storage

Solo per Azure Blob Storage, solo Chiave condivisa

- Nome account:** Inserisci il nome dell'account di storage che possiede il container esterno
- Chiave account:** Inserisci la chiave segreta per l'account di storage

Puoi usare il portale di Azure per trovare questi valori.

Anonimo

Non sono richieste ulteriori informazioni.

5. Seleziona **Continua**. Quindi scegli il tipo di verifica del server che desideri utilizzare:

Opzione	Descrizione
Usa i certificati CA root in Storage Node OS	Usa i certificati Grid CA installati sul sistema operativo per proteggere le connessioni.
Usa un certificato CA personalizzato	Utilizza un certificato CA personalizzato. Seleziona Sfoggia e carica il certificato codificato in formato PEM.
Non verificare il certificato	Selezionando questa opzione, le connessioni TLS al pool di storage cloud non sono sicure.

6. Seleziona **Salva**.

Quando salvi un pool di storage cloud, StorageGRID esegue le seguenti operazioni:

- Verifica che il bucket o container e l'endpoint del servizio esistano e che siano raggiungibili utilizzando le credenziali che hai specificato.
- Scrive un file di marcatura nel bucket o container per identificarlo come Cloud Storage Pool. Non rimuovere mai questo file, che si chiama `x-ntap-sgws-cloud-pool-uuid`.

Se la convalida del pool di storage cloud non riesce, ricevi un messaggio di errore che spiega perché la convalida non è riuscita. Ad esempio, potrebbe essere segnalato un errore se c'è un problema con il certificato o se il bucket o container che hai specificato non esiste già.

7. Se si verifica un errore, consulta la ["Istruzioni per la risoluzione dei problemi relativi ai Cloud Storage Pools"](#) e risolvi eventuali problemi, poi prova a salvare di nuovo il Cloud Storage Pool.

Visualizza i dettagli del pool di storage cloud in StorageGRID

Puoi visualizzare i dettagli di un Cloud Storage Pool per determinare dove viene utilizzato e per vedere quali nodi e storage grades sono inclusi.

Prima di iniziare

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

Passaggi

1. Seleziona **ILM > Storage pools > Cloud Storage Pools**.

La tabella Cloud Storage Pools include le seguenti informazioni per ciascun Cloud Storage Pool che include Storage Nodes:

- **Nome:** Il nome visualizzato univoco del pool.
- **URI:** L'Uniform Resource Identifier del pool di cloud storage.
- **Tipo di provider:** Quale cloud provider viene utilizzato per questo Cloud Storage Pool.
- **Container:** Il nome del bucket utilizzato per il Cloud Storage Pool.
- **Utilizzo ILM:** Modalità di utilizzo attuale del pool. Un cloud storage pool potrebbe non essere utilizzato oppure potrebbe essere impiegato in una o più regole ILM, profili di erasure-coding o entrambi.
- **Ultimo errore:** L'ultimo errore rilevato durante un controllo di integrità di questo Cloud Storage Pool.

2. Per visualizzare i dettagli di uno specifico cloud storage pool, seleziona il suo nome.

Viene visualizzata la pagina dei dettagli del pool.

3. Consulta la scheda **Autenticazione** per scoprire il tipo di autenticazione per questo Cloud Storage Pool e per modificare i dettagli di autenticazione.
4. Consulta la scheda **Verifica server** per informazioni dettagliate sulla verifica, modificare la verifica, scaricare un nuovo certificato o copiare il PEM del certificato.
5. Consulta la scheda **Utilizzo ILM** per verificare se il Cloud Storage Pool viene attualmente utilizzato in qualche regola ILM o profilo di erasure-coding.
6. Facoltativamente, vai alla **pagina delle regole ILM** per ["scopri e gestisci qualsiasi regola"](#) che usano il Cloud Storage Pool.

Modifica un pool di storage cloud in StorageGRID

Puoi modificare un pool di storage cloud per cambiarne il nome, l'endpoint del servizio o altri dettagli; tuttavia, non puoi cambiare il bucket S3 o il container Azure per un pool di storage cloud.

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Hai ["autorizzazioni di accesso specifiche"](#).
- Hai esaminato il ["Considerazioni sui Cloud Storage Pool"](#).

Passaggi

1. Seleziona **ILM > Storage pools > Cloud Storage Pools**.

La tabella Cloud Storage Pools elenca i Cloud Storage Pools esistenti.

2. Seleziona la casella di controllo corrispondente al Cloud Storage Pool che vuoi modificare, poi seleziona

Azioni > Modifica.

In alternativa, seleziona il nome del Cloud Storage Pool, quindi seleziona **Modifica**.

3. Se necessario, modifica il nome del Cloud Storage Pool, l'endpoint del servizio, le credenziali per l'autenticazione o il metodo di verifica del certificato.



Non puoi cambiare il tipo di provider, il bucket S3 o il container Azure per un pool di storage cloud.

Se in precedenza hai caricato un certificato server o client, puoi espandere la sezione **Dettagli certificato** per visualizzare il certificato attualmente in uso.

4. Seleziona **Salva**.

Quando salvi un Cloud Storage Pool, StorageGRID verifica che il bucket o container e l'endpoint del servizio esistano e che siano raggiungibili utilizzando le credenziali che hai specificato.

Se la convalida del Cloud Storage Pool non riesce, viene visualizzato un messaggio di errore. Ad esempio, potrebbe essere segnalato un errore in caso di errore relativo al certificato.

Consulta le istruzioni per "[Risoluzione dei problemi relativi ai Cloud Storage Pools](#)", risolvi il problema e poi prova a salvare nuovamente il Cloud Storage Pool.

Rimuovere un Cloud Storage Pool in StorageGRID

Puoi rimuovere un Cloud Storage Pool se non viene utilizzato in una regola ILM e non contiene dati oggetto.

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "[browser web supportato](#)".
- Tu hai il "[autorizzazioni di accesso richieste](#)".

Se necessario, usa ILM per spostare i dati degli oggetti

Se il Cloud Storage Pool che vuoi rimuovere contiene dati oggetto, devi usare ILM per spostare i dati in una posizione diversa. Ad esempio, puoi spostare i dati nei Storage Node della tua grid o in un altro Cloud Storage Pool.

Passaggi

1. Seleziona **ILM > Storage pools > Cloud Storage Pools**.
2. Consulta la colonna Utilizzo ILM nella tabella per determinare se puoi rimuovere il Cloud Storage Pool.

Non puoi rimuovere un pool di storage cloud se viene utilizzato in una regola ILM o in un profilo di erasure coding.

3. Se stai utilizzando il Cloud Storage Pool, seleziona * *cloud storage pool name* * > **ILM usage**.
4. "[Clona ogni regola ILM](#)" che attualmente inserisce gli oggetti nel Cloud Storage Pool che vuoi rimuovere.
5. Determina dove vuoi spostare gli oggetti esistenti gestiti da ciascuna regola che hai clonato.

Puoi utilizzare uno o più pool di storage oppure un Cloud Storage Pool diverso.

6. Modifica ciascuna delle regole che hai clonato.

Per il passaggio 2 della procedura guidata Crea regola ILM, seleziona la nuova posizione dal campo **copies at**.

7. ["Crea una nuova policy ILM"](#) e sostituisci ciascuna delle vecchie regole con una regola clonata.

8. Attiva la nuova policy.

9. Attendi che ILM rimuova gli oggetti dal Cloud Storage Pool e li sposti nella nuova posizione.

Elimina il pool di storage cloud

Quando il Cloud Storage Pool è vuoto e non viene utilizzato in nessuna regola ILM, puoi eliminarlo.

Prima di iniziare

- Hai rimosso tutte le regole ILM che potrebbero aver utilizzato il pool.
- Hai confermato che il bucket S3 o il container Azure non contiene alcun oggetto.

Si verifica un errore se provi a rimuovere un pool di storage cloud se contiene oggetti. Vedi ["Risolvi i problemi dei pool di storage cloud"](#).



Quando crei un Cloud Storage Pool, StorageGRID scrive un file di marcatura nel bucket o container per identificarlo come Cloud Storage Pool. Non rimuovere questo file, che si chiama `x-ntap-sgws-cloud-pool-uuid`.

Passaggi

1. Seleziona **ILM > Storage pools > Cloud Storage Pools**.
2. Se nella colonna "Utilizzo ILM" viene indicato che il Cloud Storage Pool non è in uso, seleziona la casella di controllo.
3. Seleziona **Azioni > Rimuovi**.
4. Seleziona **OK**.

Risoluzione dei problemi dei pool di storage cloud in StorageGRID

Segui questi passaggi per la risoluzione dei problemi per risolvere gli errori che potresti incontrare durante la creazione, la modifica o l'eliminazione di un Cloud Storage Pool.

`${post_edited_translations.segment}`

StorageGRID esegue un semplice controllo di integrità su ogni Cloud Storage Pool leggendo l'oggetto noto `x-ntap-sgws-cloud-pool-uuid` per assicurarsi che il Cloud Storage Pool sia accessibile e funzioni correttamente. Quando StorageGRID rileva un errore sull'endpoint, esegue un controllo di integrità ogni minuto da ciascun Storage Node. Quando l'errore viene risolto, i controlli di integrità si interrompono. Se un controllo di integrità rileva un problema, viene mostrato un messaggio nella colonna Last error della tabella Cloud Storage Pools nella pagina Storage pools.

La tabella mostra l'errore più recente rilevato per ciascun Cloud Storage Pool e indica quanto tempo fa si è verificato l'errore.

Inoltre, viene attivato un avviso di **Errore di connettività del Cloud Storage Pool** se il controllo di integrità rileva che si sono verificati uno o più nuovi errori del Cloud Storage Pool negli ultimi 5 minuti. Se ricevi una notifica email per questo avviso, vai alla pagina Storage pools (seleziona **ILM > Storage pools**), esamina i messaggi di errore nella colonna Last error e fai riferimento alle linee guida per la risoluzione dei problemi riportate di seguito.

Verifica se l'errore è stato risolto

Dopo aver risolto eventuali problemi sottostanti, puoi verificare se l'errore è stato risolto. Dalla pagina Cloud Storage Pool, seleziona l'endpoint e seleziona **Cancella errore**. Un messaggio di conferma indica che StorageGRID ha cancellato l'errore per il Cloud Storage Pool.

Se il problema di fondo è stato risolto, il messaggio di errore non viene più visualizzato. Tuttavia, se il problema di fondo non è stato risolto (o se si verifica un errore diverso), il messaggio di errore verrà visualizzato nella colonna "Ultimo errore" entro pochi minuti.

Errore: Controllo di integrità non riuscito. Errore dall'endpoint

Potresti riscontrare questo errore quando abiliti S3 Object Lock con conservazione predefinita per il tuo bucket Amazon S3 dopo aver iniziato a utilizzarlo per un Cloud Storage Pool. Questo errore si verifica quando l'operazione PUT non ha un'intestazione HTTP con un valore di checksum del payload come `Content-MD5`. Questo valore di intestazione è richiesto da AWS per le operazioni PUT nei bucket con S3 Object Lock abilitato.

Per risolvere questo problema, segui i passaggi in ["Modifica un pool di archiviazione cloud"](#) senza apportare modifiche. Questa azione attiva la convalida della configurazione del Cloud Storage Pool che rileva e aggiorna automaticamente il flag S3 Object Lock sulla configurazione dell'endpoint del Cloud Storage Pool.

Errore: questo Cloud Storage Pool contiene contenuti imprevisti

Potresti riscontrare questo errore quando tenti di creare, modificare o eliminare un Cloud Storage Pool. Questo errore si verifica se il bucket o container include il `x-ntap-sgws-cloud-pool-uuid` file marker, ma quel file non ha il campo metadati con l'UUID previsto.

In genere, vedrai questo errore solo se stai creando un nuovo Cloud Storage Pool e un'altra istanza di StorageGRID sta già utilizzando lo stesso Cloud Storage Pool.

Prova uno di questi passaggi per risolvere il problema:

- Se stai configurando un nuovo Cloud Storage Pool e il bucket contiene il file `x-ntap-sgws-cloud-pool-uuid` e ulteriori chiavi di oggetti simili al seguente esempio, crea un nuovo bucket e usa questo nuovo bucket invece.

Esempio di chiave oggetto aggiuntiva: `my-bucket.3E64CF2C-B74D-4B7D-AFE7-AD28BC18B2F6.1727326606730410`

- Se il `x-ntap-sgws-cloud-pool-uuid` file è l'unico oggetto nel bucket, elimina questo file.

Se questi passaggi non si applicano al tuo caso, contatta il supporto.

Errore: Impossibile creare o aggiornare il Cloud Storage Pool. Errore dall'endpoint

Potresti riscontrare questo errore nelle seguenti circostanze:

- Quando provi a creare o modificare un Cloud Storage Pool.
- Quando selezioni una combinazione di piattaforma, autenticazione o protocollo non supportata con S3 Object Lock durante la configurazione di un nuovo Cloud Storage Pool. Vedi "[Considerazioni sui Cloud Storage Pool](#)".

Questo errore indica che un problema di connettività o di configurazione impedisce a StorageGRID di scrivere nel Cloud Storage Pool.

Per risolvere il problema, esamina il messaggio di errore proveniente dall'endpoint.

- Se il messaggio di errore contiene `Get url: EOF`, verifica che l'endpoint del servizio utilizzato per il Cloud Storage Pool non utilizzi HTTP per un container o un bucket che richiede HTTPS.
- Se il messaggio di errore contiene `Get url: net/http: request canceled while waiting for connection`, verifica che la configurazione di rete consenta ai nodi di Storage di accedere all'endpoint del servizio utilizzato per il Cloud Storage Pool.
- Se l'errore è dovuto a una piattaforma, un'autenticazione o un protocollo non supportati, passa a una configurazione supportata con S3 Object Lock e prova a salvare nuovamente il nuovo Cloud Storage Pool.
- Per tutti gli altri messaggi di errore dell'endpoint, prova una o più delle seguenti soluzioni:
 - Crea un container o un bucket esterno con lo stesso nome che hai inserito per il Cloud Storage Pool e prova a salvare nuovamente il nuovo Cloud Storage Pool.
 - Correggi il nome del container o del bucket che hai specificato per il Cloud Storage Pool e prova a salvare di nuovo il nuovo Cloud Storage Pool.

Errore: impossibile analizzare il certificato CA

Potresti riscontrare questo errore quando provi a creare o modificare un Cloud Storage Pool. L'errore si verifica se StorageGRID non riesce a interpretare il certificato che hai inserito durante la configurazione del Cloud Storage Pool.

Per risolvere il problema, controlla il certificato CA che hai fornito per eventuali problemi.

Errore: non è stato trovato un Cloud Storage Pool con questo ID

Potresti riscontrare questo errore quando tenti di modificare o eliminare un Cloud Storage Pool. Questo errore si verifica se l'endpoint restituisce una risposta 404, che può significare una delle seguenti:

- Le credenziali utilizzate per il Cloud Storage Pool non hanno il permesso di lettura per il bucket.
- Il bucket utilizzato per il Cloud Storage Pool non include il `x-ntap-sgws-cloud-pool-uuid` marker file.

Prova uno o più di questi passaggi per risolvere il problema:

- Controlla che l'utente associato alla chiave di accesso configurata abbia le autorizzazioni necessarie.
- Modifica il Cloud Storage Pool con credenziali che hanno le autorizzazioni richieste.
- Se le autorizzazioni sono corrette, contatta il supporto.

Errore: Impossibile verificare il contenuto del pool di storage cloud. Errore dall'endpoint

Potresti riscontrare questo errore quando tenti di eliminare un Cloud Storage Pool. Questo errore indica che un problema di connettività o di configurazione impedisce a StorageGRID di leggere il contenuto del bucket del Cloud Storage Pool.

Per risolvere il problema, esamina il messaggio di errore proveniente dall'endpoint.

Errore: in questo bucket sono già stati inseriti oggetti

Potresti riscontrare questo errore quando provi a eliminare un Cloud Storage Pool. Non puoi eliminare un Cloud Storage Pool se contiene dati che sono stati spostati lì da ILM, dati che erano nel bucket prima che tu configurassi il Cloud Storage Pool, o dati che sono stati inseriti nel bucket da un'altra origine dopo la creazione del Cloud Storage Pool.

Prova uno o più di questi passaggi per risolvere il problema:

- Segui le istruzioni per riportare gli oggetti in StorageGRID in "Ciclo di vita di un oggetto Cloud Storage Pool".
- Se sei certo che gli oggetti rimanenti non siano stati inseriti nel Cloud Storage Pool da ILM, elimina manualmente gli oggetti dal bucket.



Non eliminare mai manualmente oggetti da un Cloud Storage Pool che potrebbero essere stati inseriti da ILM. Se in seguito provi ad accedere a un oggetto eliminato manualmente da StorageGRID, l'oggetto eliminato non verrà trovato.

Errore: il proxy ha riscontrato un errore esterno durante il tentativo di raggiungere il Cloud Storage Pool

Potresti riscontrare questo errore se hai configurato un proxy di 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 proxy server esterno non riesce a raggiungere l'endpoint del Cloud Storage Pool. Ad esempio, il DNS server potrebbe non essere in grado di risolvere il nome host oppure potrebbe esserci un problema di rete esterno.

Prova uno o più di questi passaggi per risolvere il problema:

- Verifica le impostazioni del cloud storage pool (**ILM > storage pool**).
- Controlla la configurazione di rete del proxy server di storage.

Errore: il certificato X.509 è fuori dal periodo di validità

Potresti riscontrare questo errore quando provi a eliminare un Cloud Storage Pool. Questo errore si verifica quando l'autenticazione richiede un certificato X.509 per garantire che il Cloud Storage Pool esterno corretto venga convalidato e che il pool esterno sia vuoto prima che la configurazione del Cloud Storage Pool venga eliminata.

Prova questi passaggi per correggere il problema:

- Aggiorna il certificato configurato per l'autenticazione al Cloud Storage Pool.
- Assicurati che qualsiasi avviso di scadenza del certificato su questo Cloud Storage Pool sia risolto.

Informazioni correlate

["Ciclo di vita di un oggetto Cloud Storage Pool"](#)

Informazioni sul copyright

Copyright © 2026 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.