Utilizza i Cloud Storage Pools

StorageGRID software

NetApp
January 14, 2026

Sommario

Utilizza i Cloud Storage Pools

Che 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, come Amazon S3 Glacier, S3 Glacier Deep Archive, Google Cloud 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 all'interno del sistema StorageGRID, un Cloud Storage Pool è composto da un bucket esterno (S3) o da un container (storage BLOB di Azure).

La 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.	Utilizzando l'opzione **ILM** > **Storage Pools** > **Cloud 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 storage all'interno di StorageGRID.	In un bucket Amazon S3, un container di storage BLOB di Azure o Google Cloud esterno al sistema StorageGRID. Se il Cloud Storage Pool è un bucket Amazon S3: • 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 S3 RestoreObject. • È possibile creare pool di storage cloud da utilizzare con AWS Commercial Cloud Services (C2S), che supporta l'AWS Secret Region. Se il pool di storage cloud è un container di storage Azure Blob, StorageGRID passa l'oggetto al Tier di archiviazione. **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 RestoreObject sugli oggetti nel Cloud Storage Pool possono essere interessate dal ciclo di vita configurato.
Cosa controlla il posizionamento degli oggetti?	Una regola ILM nei criteri ILM attivi.	Una regola ILM nei criteri ILM attivi.
Quale metodo di protezione dei dati viene utilizzato?	Replica o erasure coding.	Replica.
Quante copie di ciascun oggetto sono consentite?	Multiplo.	Una copia nel pool di storage cloud e, facoltativamente, una o più copie in StorageGRID. **Nota:** non è possibile memorizzare un oggetto in più di un Cloud Storage Pool alla volta.
Quali sono i vantaggi?	Gli oggetti sono rapidamente accessibili in qualsiasi momento.	Storage a basso costo. **Nota**: Non è possibile eseguire il tiering dei dati FabricPool nei pool di storage cloud.

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.

S3: Ciclo di vita di un oggetto Cloud Storage Pool

Questa procedura descrive le fasi del ciclo di vita di un oggetto memorizzato in un Cloud Storage Pool S3.

> "Glacier" si riferisce sia alla classe di storage Glacier che a quella Glacier Deep Archive, con una sola eccezione: La classe di storage Glacier Deep Archive non supporta il Tier di ripristino Expedited. È supportato solo il recupero in blocco o standard.

> Google Cloud Platform (GCP) supporta il recupero di oggetti dallo storage a lungo termine senza richiedere un'operazione POST-ripristino.

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 Cloud Storage Pool S3, l'applicazione client può recuperarlo utilizzando una richiesta GetObject S3 da StorageGRID, a meno che l'oggetto non sia stato spostato nello 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.

     > Per trasferire oggetti, è necessario creare una configurazione del ciclo di vita per il bucket S3 esterno e utilizzare una soluzione storage che implementi la classe di storage Glacier e supporti l'API S3 RestoreObject.

   - Durante la transizione, l'applicazione client può utilizzare una richiesta S3 HeadObject per monitorare lo stato dell'oggetto.
4. **Oggetto ripristinato dallo storage Glacier**

   Se un oggetto è stato spostato nello storage Glacier, l'applicazione client può emettere una richiesta S3 RestoreObject 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 sui nodi di storage all'interno di StorageGRID, non è necessario ripristinare l'oggetto da Glacier mediante una richiesta RestoreObject. La copia locale può essere recuperata direttamente, utilizzando una richiesta GetObject.

5. **Oggetto recuperato**

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

Azure: Ciclo di vita di un oggetto Cloud Storage Pool

Questa procedura descrive le fasi del ciclo di vita di un oggetto memorizzato in un Cloud Storage Pool di Azure.

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 Azure Cloud Storage Pool come posizione di posizionamento, StorageGRID sposta l'oggetto nel contenitore di storage BLOB di Azure esterno specificato dal Cloud Storage Pool.

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 spostato nel Tier Archive, l'applicazione client può emettere una richiesta S3 RestoreObject per ripristinare una copia recuperabile nell'Azure Cloud Storage Pool.

   Quando StorageGRID riceve il RestoreObject, trasferisce temporaneamente l'oggetto al livello di raffreddamento dell'archiviazione BLOB di Azure. Non appena viene raggiunta la data di scadenza nella richiesta RestoreObject, StorageGRID trasferisce nuovamente l'oggetto al livello Archive.

   Se una o più copie dell'oggetto sono presenti anche nei nodi di archiviazione all'interno di StorageGRID, non è necessario ripristinare l'oggetto dal livello di accesso di archiviazione mediante una richiesta RestoreObject. La copia locale può essere recuperata direttamente, utilizzando una richiesta GetObject.

5. **Oggetto recuperato**

   Una volta ripristinato un oggetto in Azure Cloud Storage Pool, l'applicazione client può emettere una richiesta GetObject per recuperare l'oggetto ripristinato.

Informazioni correlate

"UTILIZZARE L'API REST S3"

Quando utilizzare i Cloud Storage Pools

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

Eseguire il 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 la richiesta S3 RestoreObject 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.

Dati di Tier da StorageGRID a 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

È possibile configurare più endpoint del Cloud Storage Pool se si desidera eseguire il Tier o il backup dei dati degli oggetti in più 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 endpoint multipli del 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 gli oggetti dal bucket A nel pool di cloud storage A e gli oggetti dal bucket B nel pool di cloud storage B. oppure gli oggetti nel pool di cloud storage A per un certo periodo di tempo, quindi spostarli nel pool di cloud storage 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.
- 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.
- Gli oggetti con blocco oggetti S3 abilitato non possono essere posizionati nei pool di storage cloud.
- Le seguenti combinazioni di piattaforma, autenticazione e protocollo con blocco oggetto S3 non sono supportate per i pool di archiviazione cloud:
  - **Piattaforme**: Google Cloud Platform e Azure
  - **Tipi di autenticazione**: Accesso anonimo
  - **Protocollo**: HTTP

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 anche "configurare un proxy di archiviazione"consentire l'invio di 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, le regole e i criteri ILM vengono riconfigurati. 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

Le policy per il bucket S3 esterno utilizzato per un Cloud Storage Pool devono garantire a StorageGRID l'autorizzazione a spostare un oggetto nel bucket, ottenere lo stato di un oggetto, ripristinare un oggetto dallo storage Glacier quando necessario e altro ancora. Idealmente, StorageGRID dovrebbe avere accesso con controllo 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 dalle policy ILM attive 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.

Per trasferire oggetti da Cloud Storage Pool, è necessario creare la configurazione del ciclo di vita appropriata nel bucket S3 esterno e utilizzare una soluzione storage che implementi la classe di storage Glacier e supporti l'API S3 RestoreObject.

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.

Per trasferire oggetti in Cloud Storage Pool in S3 Glacier Deep Archive (invece di su Amazon S3 Glacier), specificare `<StorageClass>DEEP_ARCHIVE</StorageClass>` nel ciclo di vita del bucket. Tuttavia, tieni presente che non puoi utilizzare il `Expedited` livello per ripristinare gli oggetti 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 Cloud Storage Pool. Le operazioni del ciclo di vita potrebbero interferire con le operazioni del Cloud Storage Pool.

Informazioni correlate

"Creare un pool di storage cloud"

Confronto tra Cloud Storage Pools e la replica di 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?	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 conservare due copie in loco, puoi conservarne una all'interno di StorageGRID e inviarne una copia al pool di storage cloud.	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 viene configurato?	Definito allo stesso modo dei pool di storage, utilizzando Grid Manager o l'API Grid Management. Può essere selezionata 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?	• Qualsiasi infrastruttura S3 compatibile (incluso Amazon S3) • Tier Azure Blob Archive • Piattaforma Google Cloud (GCP)	• Qualsiasi infrastruttura S3 compatibile (incluso Amazon S3) • Piattaforma Google Cloud (GCP)

	Pool di cloud storage	Servizio di replica di CloudMirror
Qual è la causa dello spostamento degli oggetti nella destinazione?	Una o più regole ILM nei criteri ILM attivi. 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.
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 cloud storage sono 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 anche eliminato dal 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.

Creare un pool di storage cloud

Un Cloud Storage Pool specifica un singolo bucket esterno Amazon S3 o un altro provider compatibile con S3 o un container di storage BLOB di Azure.

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 (storage Amazon S3/GCP o Azure Blob) e le informazioni StorageGRID necessarie per accedere al bucket o al container esterno.

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.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Si dispone di "autorizzazioni di accesso richieste".
- È stata esaminata la "Considerazioni per i Cloud Storage Pools".
- Il bucket o contenitore esterno a cui fa riferimento il Cloud Storage Pool esiste già e si dispone di informazioni sull'endpoint di servizio.
- Per accedere al secchio o al contenitore, è informazioni sull'account per il tipo di autenticazionepossibile scegliere.

Fasi

1. Selezionare **ILM** > **Storage Pools** > **Cloud Storage Pools**.
2. Selezionare **Crea**, quindi immettere le seguenti informazioni:

Campo	Descrizione
Nome del pool di cloud storage	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	Quale cloud provider utilizzerai per questo Cloud Storage Pool: • **Amazon S3/GCP**: Selezionare questa opzione per Amazon S3, Commercial Cloud Services (C2S) S3, Google Cloud Platform (GCP) o altri provider compatibili con S3. • **Azure Blob Storage**
Bucket o container	Il nome del bucket S3 esterno o del container Azure. Non puoi modificare questo valore dopo il salvataggio del Cloud Storage Pool.

3. in base alla selezione del tipo di provider, immettere le informazioni sull'endpoint del servizio.

Amazon S3/GCP

a. Per il protocollo, selezionare HTTPS o HTTP.

> Non utilizzare connessioni HTTP per dati sensibili.

b. Inserire il nome host. Esempio:

`s3-aws-region.amazonaws.com`

c. Selezionare lo stile URL:

Opzione	Descrizione
Rilevamento automatico	Tentare di rilevare automaticamente lo stile URL da utilizzare, in base alle informazioni fornite. Ad esempio, se si specifica un indirizzo IP, StorageGRID utilizzerà un URL di tipo path. Selezionare questa opzione solo se non si conosce lo stile specifico da utilizzare.
Stile virtual-hosted	Utilizza un URL di tipo virtual-hosted per accedere al bucket. Gli URL in stile virtual-hosted includono il nome del bucket come parte del nome di dominio. Esempio: `https://bucket-name.s3.company.com/key-name`
Stile di percorso	Utilizzare un URL stile percorso per accedere al bucket. Gli URL stile percorso includono il nome del bucket alla fine Esempio: `https://s3.company.com/bucket-name/key-name` **Nota:** l'opzione URL stile percorso non è consigliata e sarà obsoleta in una release futura di StorageGRID.

d. Se si desidera, inserire il numero della porta o utilizzare la porta predefinita: 443 per HTTPS o 80 per HTTP.

Azure Blob Storage

a. Utilizzando uno dei seguenti formati, immettere l'URI per l'endpoint del servizio.

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

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

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

4. selezionare **Continue**. Quindi, selezionare il tipo di autenticazione e immettere le informazioni richieste per l'endpoint del Cloud Storage Pool:

Tasto di accesso

Per Amazon S3/GCP o altro provider compatibile con S3

a. **ID chiave di accesso**: Immettere l'ID della chiave di accesso per l'account proprietario del bucket esterno.
b. **Chiave di accesso segreta**: Immettere la chiave di accesso segreta.

Ruoli IAM ovunque

Per AWS IAM Roles Anywhere service

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

a. **AWS IAM Roles Anywhere Region**: Selezionare la regione per il Cloud Storage Pool. Ad esempio, `us-east-1`.
b. **Trust anchor URN**: Immettere l'URN dell'ancoraggio trust che convalida le richieste per le credenziali STS di breve durata. Può essere una CA principale o intermedia.
c. **URN profilo**: Immettere l'URN del profilo IAM Roles Anywhere che elenca i ruoli che possono essere assunti da chiunque sia attendibile.
d. **Role URN**: Inserire l'URN del ruolo IAM che può essere assunto da chiunque sia attendibile.
e. **Durata sessione**: Immettere la durata delle credenziali di protezione temporanee e della sessione ruolo. Immettere almeno 15 minuti e non più di 12 ore.
f. **Certificato CA del server** (opzionale): Uno o più certificati CA attendibili, in formato PEM, per la verifica del server IAM Roles Anywhere. Se omesso, il server non verrà verificato.
g. **Certificato dell'entità finale**: La chiave pubblica, in formato PEM, del certificato X509 firmato dall'ancoraggio trust. 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 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. **Certificato CA del server**: Selezionare **Sfoglia** e caricare il certificato CA utilizzato da StorageGRID per verificare il CAP server. Il certificato deve essere codificato PEM ed emesso da un'autorità di certificazione pubblica competente (CA).
c. **Certificato client**: Selezionare **Sfoglia** e caricare il certificato che StorageGRID utilizzerà per identificarsi nel CAP server. Il certificato client deve essere codificato PEM, rilasciato da un'autorità di certificazione pubblica (CA) appropriata e deve essere concesso l'accesso al conto C2S.
d. **Chiave privata client**: Selezionare **Sfoglia** e caricare la chiave privata codificata PEM per il certificato client.
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 **Password chiave privata client**.

Se il certificato client viene crittografato, utilizzare il formato tradizionale per la crittografia. Il formato crittografato PKCS n. 8 non è supportato.

Azure Blob Storage

Per l'archiviazione BLOB di Azure, solo chiave condivisa

a. **Nome account**: Immettere il nome dell'account di archiviazione proprietario del contenitore esterno
b. **Codice account**: Immettere la chiave segreta per l'account di archiviazione

È possibile utilizzare il portale Azure per trovare questi valori.

Anonimo

Non sono richieste informazioni aggiuntive.

5. Selezionare **continua**. Quindi scegliere il tipo di verifica del server che si desidera utilizzare:

Opzione	Descrizione
Utilizzare i certificati della CA principale nel sistema operativo del nodo di storage	Utilizzare i certificati Grid CA installati nel sistema operativo per proteggere le connessioni.
USA certificato CA personalizzato	Utilizzare un certificato CA personalizzato. Selezionare **Sfoglia** e caricare il certificato codificato PEM.
Non verificare il certificato	La selezione di questa opzione indica che le connessioni TLS al Cloud Storage Pool non sono sicure.

6. Selezionare **Salva**.

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

   - Convalida l'esistenza del bucket o del container e dell'endpoint del servizio e la possibilità di raggiungerli utilizzando le credenziali specificate.
   - Scrive un file marker nel bucket o nel container per identificarlo come pool di storage cloud. Non rimuovere mai questo file, che è 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 o il container specificato non esiste già, potrebbe essere visualizzato un errore.

7. Se si verifica un errore, consultare la sezione "Istruzioni per la risoluzione dei problemi dei Cloud Storage Pools", risolvere eventuali problemi, quindi provare a salvare nuovamente il Cloud Storage Pool.

Visualizzare i dettagli dei pool di storage cloud

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

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Si dispone di "autorizzazioni di accesso specifiche".

Fasi

1. Selezionare **ILM** > **Storage Pools** > **Cloud Storage Pools**.

   La tabella Cloud Storage Pools include le seguenti informazioni per ogni Cloud Storage Pool che include i nodi di storage:

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

2. Per visualizzare i dettagli di un pool di cloud storage specifico, selezionarne il nome.

   Viene visualizzata la pagina dei dettagli del pool.

3. Visualizzare la scheda **autenticazione** per informazioni sul tipo di autenticazione per questo Cloud Storage Pool e per modificare i dettagli di autenticazione.
4. Visualizzare la scheda **verifica server** per informazioni sui dettagli della verifica, modificare la verifica, scaricare un nuovo certificato o copiare il PEM del certificato.
5. Visualizzare la scheda **utilizzo ILM** per determinare se il Cloud Storage Pool è attualmente utilizzato in qualsiasi regola ILM o profilo di erasure coding.
6. In alternativa, andare alla pagina **regole ILM** "informazioni e gestione di eventuali regole"che utilizzano il Cloud Storage Pool.

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.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Si dispone di "autorizzazioni di accesso specifiche".
- È stata esaminata la "Considerazioni per i Cloud Storage Pools".

Fasi

1. Selezionare **ILM** > **Storage Pools** > **Cloud Storage Pools**.

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

2. Seleziona la casella di controllo per il Cloud Storage Pool che desideri modificare, quindi seleziona **azioni** > **Modifica**.

   In alternativa, selezionare il nome del pool di archiviazione cloud, quindi selezionare **Modifica**.

3. Come richiesto, modificare il nome del Cloud Storage Pool, l'endpoint del servizio, le credenziali di autenticazione o il metodo di verifica del certificato.

   > Non puoi 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 espandere la fisarmonica **Dettagli certificato** per rivedere il certificato attualmente in uso.

4. Selezionare **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 "Risoluzione dei problemi relativi ai pool di storage cloud", risolvere il problema, quindi riprovare a salvare il Cloud Storage Pool.

Rimuovere un pool di storage cloud

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

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Si dispone di "autorizzazioni di accesso richieste".

Se necessario, utilizzare ILM per spostare i dati dell'oggetto

Se il Cloud Storage Pool che si desidera rimuovere contiene dati a oggetti, è necessario utilizzare ILM per spostare i dati in una posizione diversa. Ad esempio, è possibile spostare i dati su nodi di storage nel proprio grid o su un pool di storage cloud diverso.

Fasi

1. Selezionare **ILM** > **Storage Pools** > **Cloud Storage Pools**.
2. Esaminare la colonna relativa all'utilizzo di ILM nella tabella per determinare se è possibile rimuovere il Cloud Storage Pool.

   Non puoi rimuovere un Cloud Storage Pool se viene utilizzato in una regola ILM o in un profilo di erasure coding.

3. Se si utilizza il Cloud Storage Pool, selezionare ***cloud storage pool name*** > **ILM usage**.
4. "Clonare ogni regola ILM" Che attualmente colloca gli oggetti nel pool di cloud storage da rimuovere.

5. Determinare dove si desidera spostare gli oggetti esistenti gestiti da ciascuna regola clonata.

   È possibile utilizzare uno o più pool di storage o un pool di storage cloud diverso.

6. Modificare ciascuna regola clonata.

   Per la fase 2 della creazione guidata regola ILM, selezionare la nuova posizione dal campo **copie at**.

7. "Creare un nuovo criterio ILM" e sostituire ciascuna delle vecchie regole con una regola clonata.
8. Attivare la nuova policy.
9. Attendere che ILM rimuova gli oggetti dal Cloud Storage Pool e li inseri nella nuova posizione.

Eliminare il pool di storage cloud

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

Prima di iniziare

- Sono state rimosse tutte le regole ILM che potrebbero aver utilizzato il pool.
- Hai confermato che il bucket S3 o il container Azure non contiene oggetti.

  Si verifica un errore se si tenta di rimuovere un Cloud Storage Pool se contiene oggetti. Vedere "Risolvere i problemi dei 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, che è denominato `x-ntap-sgws-cloud-pool-uuid`.

Fasi

1. Selezionare **ILM** > **Storage Pools** > **Cloud Storage Pools**.
2. Se la colonna ILM Usage (utilizzo ILM) indica che il Cloud Storage Pool non è in uso, selezionare la casella di controllo.
3. Selezionare **azioni** > **Rimuovi**.
4. Selezionare **OK**.

Risolvere i problemi dei pool di storage cloud

Utilizzare questi passaggi per la risoluzione dei problemi per risolvere gli errori che potrebbero verificarsi durante la creazione, la modifica o l'eliminazione di un pool di storage cloud.

Determinare se si è verificato un errore

StorageGRID esegue un semplice controllo dello stato di salute di ogni pool di cloud storage leggendo l'oggetto noto `x-ntap-sgws-cloud-pool-uuid` per assicurarsi che il pool di cloud storage sia accessibile e funzioni correttamente. Quando StorageGRID rileva un errore nell'endpoint, esegue un controllo di integrità ogni minuto da ogni nodo di storage. Quando l'errore viene risolto, i controlli dello stato si interrompono. Se un controllo di integrità rileva un problema, viene visualizzato un messaggio nella colonna ultimo errore della tabella Pool di archiviazione cloud nella pagina Pool di archiviazione.

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

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 Pools (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.

Controllare se un errore è stato risolto

Dopo aver risolto eventuali problemi sottostanti, è possibile determinare se l'errore è stato risolto. Dalla pagina Cloud Storage Pool, selezionare l'endpoint e selezionare **Clear error**. Un messaggio di conferma indica che StorageGRID ha eliminato l'errore per il pool di storage cloud.

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: Controllo dello stato di salute non riuscito. Errore dall'endpoint

Questo errore potrebbe verificarsi quando si attiva S3 Object Lock con conservazione predefinita per il bucket Amazon S3 dopo aver iniziato a utilizzare questo bucket per un Cloud Storage Pool. Questo errore si verifica quando l'operazione PUT non ha un'intestazione HTTP con un valore checksum payload come `Content-MD5` . Questo valore della testata è richiesto da AWS per le operazioni di INSERIMENTO nei bucket con blocco oggetti S3 abilitato.

Per risolvere questo problema, seguire i passaggi descritti in "Modifica di un pool di storage cloud" senza apportare modifiche. Questa azione attiva la convalida della configurazione del Cloud Storage Pool che rileva e aggiorna automaticamente il flag blocco oggetto S3 in una configurazione endpoint di Cloud Storage Pool.

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 contenitore include il `x-ntap-sgws-cloud-pool-uuid` file marcatore, ma quel file non ha il campo metadati con 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, provare a eseguire una delle seguenti operazioni:

- Se stai configurando un nuovo Cloud Storage Pool e il bucket contiene il `x-ntap-sgws-cloud-pool-uuid` file e le chiavi oggetto aggiuntive simili all'esempio seguente, crea un nuovo bucket e utilizza invece questo nuovo bucket.

  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, eliminarlo.

Se questi passaggi non si applicano al proprio scenario, contattare l'assistenza.

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

Questo errore potrebbe verificarsi nelle seguenti circostanze:

- Quando si tenta di creare o modificare un Cloud Storage Pool.
- Quando si seleziona una combinazione di piattaforma, autenticazione o protocollo non supportata con blocco oggetto S3 durante la configurazione di un nuovo Cloud Storage Pool. Vedere "Considerazioni per i Cloud Storage Pools".

Questo errore indica che un problema di connettività o di configurazione impedisce la scrittura di StorageGRID 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`, controllare che l'endpoint del servizio utilizzato per il Cloud Storage Pool non utilizzi HTTP per un contenitore o un bucket che richiede HTTPS.
- Se il messaggio di errore contiene `Get *url*: net/http: request canceled while waiting for connection`, verificare che la configurazione di rete consenta ai nodi di archiviazione di accedere all'endpoint del servizio utilizzato per il pool di archiviazione cloud.
- Se l'errore è dovuto a una piattaforma, autenticazione o protocollo non supportati, passare a una configurazione supportata con blocco oggetti S3 e provare a salvare nuovamente il nuovo 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 pool di cloud storage non include il `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:

- Segui le istruzioni per riportare gli oggetti in StorageGRID in "ciclo di vita di un oggetto Cloud Storage Pool".
- 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

È possibile che si verifichi questo errore se è stato 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 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 di archiviazione.

Errore: Il certificato X,509 non è valido

Questo errore potrebbe verificarsi quando si tenta di eliminare un pool di storage cloud. Questo errore si verifica quando l'autenticazione richiede un certificato X,509 per garantire la convalida del Cloud Storage Pool esterno corretto e il pool esterno è vuoto prima di eliminare la configurazione del Cloud Storage Pool.

Per risolvere il problema, attenersi alla seguente procedura:

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

Informazioni correlate

"Ciclo di vita di un oggetto Cloud Storage Pool"

Informazioni sul copyright

Informazioni sul marchio commerciale