Utilizzo dei Cloud Storage Pools

StorageGRID 11.5

NetApp
April 11, 2024

Sommario

Utilizzo dei Cloud Storage Pools

È possibile utilizzare i pool di storage cloud per spostare gli oggetti StorageGRID in una posizione di storage esterna, ad esempio lo storage S3 Glacier o Microsoft Azure Blob. Lo spostamento di oggetti all'esterno della griglia consente di sfruttare un Tier di storage a basso costo per l'archiviazione a lungo termine.

Cos'è un pool di storage cloud

Un pool di storage cloud consente di utilizzare ILM per spostare i dati degli oggetti all'esterno del sistema StorageGRID. Ad esempio, è possibile spostare gli oggetti con accesso non frequente in uno storage cloud a basso costo, ad esempio Amazon S3 Glacier, S3 Glacier Deep Archive o il Tier di accesso all'archivio nello storage Microsoft Azure Blob. In alternativa, è possibile mantenere un backup cloud degli oggetti StorageGRID per migliorare il disaster recovery.

Dal punto di vista di ILM, un pool di storage cloud è simile a un pool di storage. Per memorizzare gli oggetti in entrambe le posizioni, selezionare il pool quando si creano le istruzioni di posizionamento per una regola ILM. Tuttavia, mentre i pool di storage sono costituiti da nodi di storage o nodi di archiviazione all'interno del sistema StorageGRID, un pool di storage cloud è costituito da un bucket esterno (S3) o da un container (storage blob Azure).

La seguente tabella confronta i pool di storage con i pool di storage cloud e mostra le analogie e le differenze di alto livello.

	Pool di storage	**Pool di cloud storage**
Come viene creato?	Utilizzando l'opzione **ILM** > **Storage Pools** in Grid Manager. È necessario impostare i gradi di storage prima di poter creare il pool di storage.	Utilizzando l'opzione **ILM** > **Storage Pools** in Grid Manager. È necessario configurare il bucket o il container esterno prima di poter creare il Cloud Storage Pool.
Quanti pool è possibile creare?	Senza limiti.	Fino a 10.

	Pool di storage	Pool di cloud storage
Dove sono memorizzati gli oggetti?	Su uno o più nodi di storage o nodi di archiviazione all'interno di StorageGRID.	In un bucket Amazon S3 o in un container di storage Azure Blob 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 di ripristino degli oggetti S3 POST. • È possibile creare pool di storage cloud da utilizzare con AWS Commercial Cloud Services (C2S), che supporta l'AWS Secret Region. 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 DI ripristino POST-oggetto sugli oggetti nel Cloud Storage Pool possono essere influenzate dal ciclo di vita configurato.
Cosa controlla il posizionamento degli oggetti?	Una regola ILM nel criterio ILM attivo.	Una regola ILM nel criterio ILM attivo.
Quale metodo di protezione dei dati viene utilizzato?	Replica o erasure coding.	Replica.
Quante copie di ciascun oggetto sono consentite?	Multiplo.	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.

Ciclo di vita di un oggetto Cloud Storage Pool

Prima di implementare i Cloud Storage Pool, esaminare il ciclo di vita degli oggetti memorizzati in ciascun tipo di Cloud Storage Pool.

Informazioni correlate

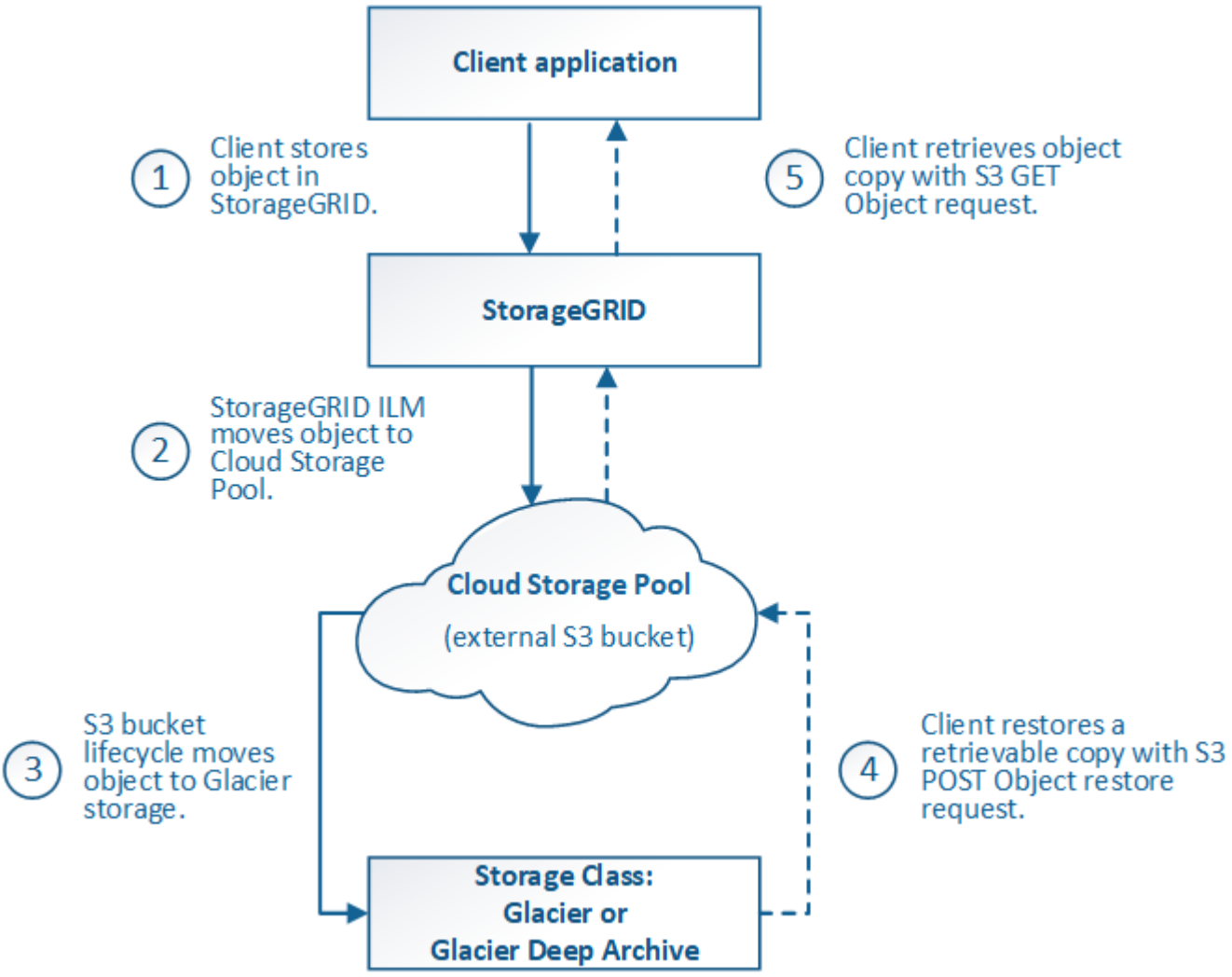
S3: Ciclo di vita di un oggetto Cloud Storage Pool

Azure: Ciclo di vita di un oggetto Cloud Storage Pool]

S3: Ciclo di vita di un oggetto Cloud Storage Pool

La figura mostra le fasi del ciclo di vita di un oggetto memorizzato in un pool di storage cloud S3.

> Nella figura e nelle spiegazioni, “Glacier” si riferisce sia alla classe di storage Glacier che alla classe di storage Glacier Deep Archive, con un’eccezione: La classe di storage Glacier Deep Archive non supporta il Tier di ripristino accelerato. È supportato solo il recupero in blocco o standard.



1. **Oggetto memorizzato in StorageGRID**

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

2. **Oggetto spostato in S3 Cloud Storage Pool**
   - Quando l'oggetto viene associato a una regola ILM che utilizza un pool di storage cloud S3 come posizione di posizionamento, StorageGRID sposta l'oggetto nel bucket S3 esterno specificato dal pool di storage cloud.
   - Quando l'oggetto è stato spostato nel pool di storage cloud S3, l'applicazione client può recuperarlo utilizzando una richiesta di oggetti Get S3 da StorageGRID, a meno che l'oggetto non sia stato trasferito allo storage Glacier.
3. **Oggetto in transizione a Glacier (stato non recuperabile)**
   - Facoltativamente, l'oggetto può essere passato allo storage Glacier. Ad esempio, il bucket S3 esterno potrebbe utilizzare la configurazione del ciclo di vita per trasferire un oggetto allo storage Glacier immediatamente o dopo un certo numero di giorni.

> Se si desidera eseguire la transizione degli oggetti, è necessario creare una configurazione del ciclo di vita per il bucket S3 esterno e utilizzare una soluzione di storage che implementi la classe di storage Glacier e supporti l'API di ripristino degli oggetti S3 POST.

> Non utilizzare i Cloud Storage Pools per oggetti che sono stati acquisiti dai client Swift. Swift non supporta le richieste DI ripristino DEGLI oggetti POST, pertanto StorageGRID non sarà in grado di recuperare oggetti Swift che sono stati trasferiti allo storage S3 Glacier. L'emissione di una richiesta Swift GET Object per recuperare questi oggetti non avrà esito positivo (403 proibita).

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

   Se un oggetto è stato passato allo storage Glacier, l'applicazione client può emettere una richiesta di ripristino dell'oggetto S3 POST per ripristinare una copia recuperabile nel Cloud Storage Pool S3. La richiesta specifica il numero di giorni in cui la copia deve essere disponibile nel Cloud Storage Pool e il Tier di accesso ai dati da utilizzare per l'operazione di ripristino (accelerato, Standard o in blocco). Una volta raggiunta la data di scadenza della copia recuperabile, la copia viene automaticamente riportata in uno stato non recuperabile.

> Se una o più copie dell'oggetto esistono anche nei nodi di storage all'interno di StorageGRID, non è necessario ripristinare l'oggetto da Glacier inviando una richiesta DI ripristino DELL'oggetto POST. Invece, la copia locale può essere recuperata direttamente, utilizzando una richiesta DI oggetto GET.

5. **Oggetto recuperato**

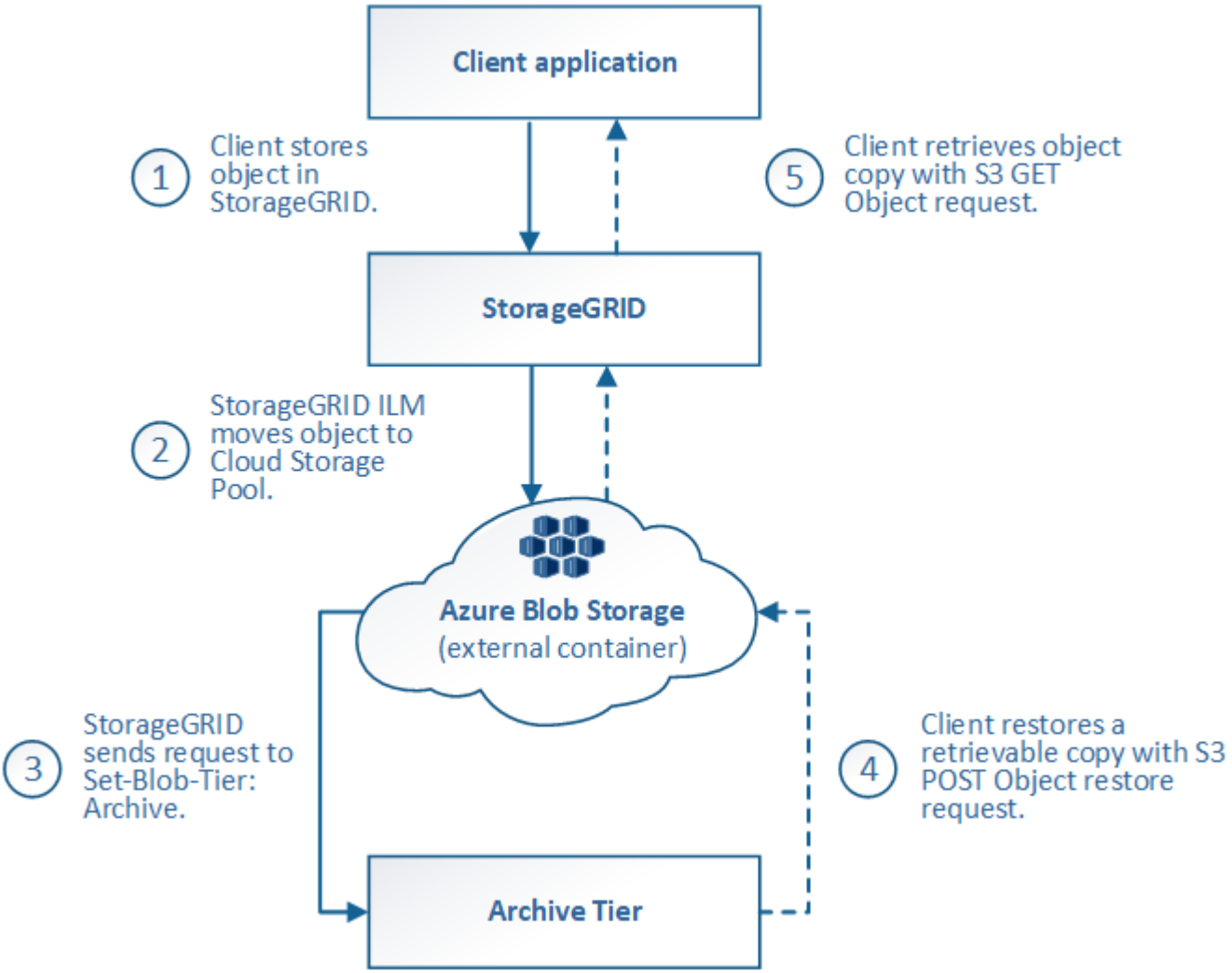
   Una volta ripristinato un oggetto, l'applicazione client può inviare una richiesta DI RECUPERO dell'oggetto ripristinato.

Informazioni correlate

"Utilizzare S3"

Azure: Ciclo di vita di un oggetto Cloud Storage Pool

La figura mostra le fasi del ciclo di vita di un oggetto memorizzato in un pool di storage Azure Cloud.



1. **Oggetto memorizzato in StorageGRID**

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

2. **Oggetto spostato in Azure Cloud Storage Pool**

   Quando l'oggetto viene associato a una regola ILM che utilizza un pool di storage cloud Azure come posizione di posizionamento, StorageGRID sposta l'oggetto nel contenitore di storage blob Azure esterno specificato dal pool di storage cloud

   > Non utilizzare i Cloud Storage Pools per oggetti che sono stati acquisiti dai client Swift. Swift non supporta le richieste DI ripristino POST-oggetto, pertanto StorageGRID non sarà in grado di recuperare oggetti Swift che sono stati trasferiti al Tier di archiviazione dello storage di Azure Blob. L'emissione di una richiesta Swift GET Object per recuperare questi oggetti non avrà esito positivo (403 proibita).

3. **Oggetto sottoposto a transizione al Tier di archiviazione (stato non recuperabile)**

   Subito dopo aver spostato l'oggetto nel pool di storage cloud di Azure, StorageGRID passa

automaticamente l'oggetto al livello di archiviazione dello storage Blob di Azure.

4. **Oggetto ripristinato dal Tier di archiviazione**

   Se un oggetto è stato passato al Tier Archive, l'applicazione client può emettere una richiesta di ripristino dell'oggetto S3 POST per ripristinare una copia recuperabile nel pool di storage di Azure Cloud.

   Quando StorageGRID riceve IL ripristino dell'oggetto POST, passa temporaneamente l'oggetto al livello di raffreddamento dello storage di Azure Blob. Non appena viene raggiunta la data di scadenza nella richiesta DI ripristino DELL'oggetto POST, StorageGRID riconsegna l'oggetto al livello di archiviazione.

   > Se una o più copie dell'oggetto esistono anche nei nodi di storage all'interno di StorageGRID, non è necessario ripristinare l'oggetto dal livello di accesso di archiviazione inviando una richiesta DI ripristino POST-oggetto. Invece, la copia locale può essere recuperata direttamente, utilizzando una richiesta DI oggetto GET.

5. **Oggetto recuperato**

   Una volta ripristinato un oggetto in Azure Cloud Storage Pool, l'applicazione client può inviare una richiesta DI RECUPERO dell'oggetto ripristinato.

Quando utilizzare i Cloud Storage Pools

I pool di cloud storage possono offrire vantaggi significativi in diversi casi di utilizzo.

Backup dei dati StorageGRID in una posizione esterna

È possibile utilizzare un pool di storage cloud per eseguire il backup degli oggetti StorageGRID in una posizione esterna.

Se le copie in StorageGRID non sono accessibili, i dati dell'oggetto nel pool di storage cloud possono essere utilizzati per soddisfare le richieste dei client. Tuttavia, potrebbe essere necessario emettere una richiesta di ripristino S3 POST Object per accedere alla copia dell'oggetto di backup nel Cloud Storage Pool.

I dati dell'oggetto in un pool di storage cloud possono essere utilizzati anche per recuperare i dati persi da StorageGRID a causa di un guasto di un volume di storage o di un nodo di storage. Se l'unica copia rimanente di un oggetto si trova in un pool di storage cloud, StorageGRID ripristina temporaneamente l'oggetto e crea una nuova copia sul nodo di storage ripristinato.

Per implementare una soluzione di backup:

1. Creare un singolo pool di storage cloud.
2. Configurare una regola ILM che memorizzi simultaneamente le copie degli oggetti sui nodi di storage (come copie replicate o codificate in cancellazione) e una singola copia degli oggetti nel Cloud Storage Pool.
3. Aggiungere la regola al criterio ILM. Quindi, simulare e attivare la policy.

Tiering dei dati da StorageGRID a una posizione esterna

È possibile utilizzare un pool di storage cloud per memorizzare oggetti all'esterno del sistema StorageGRID. Si supponga, ad esempio, di disporre di un elevato numero di oggetti da conservare, ma si prevede di accedervi raramente, se mai. È possibile utilizzare un pool di storage cloud per tierare gli oggetti in modo da ridurre il

costo dello storage e liberare spazio in StorageGRID.

Per implementare una soluzione di tiering:

1. Creare un singolo pool di storage cloud.
2. Configurare una regola ILM che sposti gli oggetti utilizzati raramente dai nodi di storage al Cloud Storage Pool.
3. Aggiungere la regola al criterio ILM. Quindi, simulare e attivare la policy.

Mantenere più endpoint cloud

Puoi configurare più Cloud Storage Pool se desideri eseguire il tiering o il backup dei dati degli oggetti in più di un cloud. I filtri nelle regole ILM consentono di specificare quali oggetti sono memorizzati in ciascun Cloud Storage Pool. Ad esempio, è possibile memorizzare oggetti di alcuni tenant o bucket in Amazon S3 Glacier e oggetti di altri tenant o bucket nello storage Azure Blob. In alternativa, puoi spostare i dati tra lo storage Amazon S3 Glacier e Azure Blob. Quando si utilizzano più Cloud Storage Pool, tenere presente che un oggetto può essere memorizzato in un solo Cloud Storage Pool alla volta.

Per implementare più endpoint cloud:

1. Crea fino a 10 pool di cloud storage.
2. Configurare le regole ILM in modo che memorizzino i dati dell'oggetto appropriati all'ora appropriata in ciascun Cloud Storage Pool. Ad esempio, memorizzare oggetti dal bucket A nel Cloud Storage Pool A e memorizzare oggetti dal bucket B nel Cloud Storage Pool B. Oppure, memorizzare gli oggetti nel Cloud Storage Pool A per un certo periodo di tempo e spostarli nel Cloud Storage Pool B.
3. Aggiungere le regole alla policy ILM. Quindi, simulare e attivare la policy.

Considerazioni per i Cloud Storage Pools

Se si prevede di utilizzare un pool di storage cloud per spostare oggetti fuori dal sistema StorageGRID, è necessario esaminare le considerazioni relative alla configurazione e all'utilizzo dei pool di storage cloud.

Considerazioni generali

- In generale, lo storage di archiviazione cloud, come Amazon S3 Glacier o Azure Blob, è un luogo conveniente per memorizzare i dati degli oggetti. Tuttavia, i costi per recuperare i dati dallo storage di archiviazione cloud sono relativamente elevati. Per ottenere il costo complessivo più basso, è necessario considerare quando e con quale frequenza accedere agli oggetti nel Cloud Storage Pool. L'utilizzo di un Cloud Storage Pool è consigliato solo per i contenuti ai quali si prevede di accedere con frequenza limitata.
- Non utilizzare i Cloud Storage Pools per oggetti che sono stati acquisiti dai client Swift. Swift non supporta le richieste DI ripristino POST-oggetto, pertanto StorageGRID non sarà in grado di recuperare oggetti Swift che sono stati trasferiti allo storage S3 Glacier o al Tier di archiviazione dello storage Blob Azure. L'emissione di una richiesta Swift GET Object per recuperare questi oggetti non avrà esito positivo (403 proibita).
- L'utilizzo dei pool di storage cloud con FabricPool non è supportato a causa della latenza aggiunta per recuperare un oggetto dalla destinazione del pool di storage cloud.

Informazioni necessarie per creare un pool di storage cloud

Prima di creare un Cloud Storage Pool, è necessario creare il bucket S3 esterno o il container di storage Azure Blob esterno da utilizzare per il Cloud Storage Pool. Quindi, quando si crea il pool di storage cloud in StorageGRID, è necessario specificare le seguenti informazioni:

- Il tipo di provider: Storage Amazon S3 o Azure Blob.
- Se si seleziona Amazon S3, specificare se il Cloud Storage Pool deve essere utilizzato con l'AWS Secret Region (**CAP (C2S Access Portal)**).
- Il nome esatto del bucket o del container.
- L'endpoint del servizio doveva accedere al bucket o al container.
- L'autenticazione necessaria per accedere al bucket o al container:
  - **S3**: Facoltativamente, un ID della chiave di accesso e una chiave di accesso segreta.
  - **C2S**: L'URL completo per ottenere le credenziali temporanee dal server CAP; un certificato CA del server, un certificato client, una chiave privata per il certificato client e, se la chiave privata è crittografata, la passphrase per la decrittografia.
  - **Azure Blob storage**: Un nome account e una chiave account. Queste credenziali devono disporre dell'autorizzazione completa per il container.
- Facoltativamente, un certificato CA personalizzato per verificare le connessioni TLS al bucket o al container.

Considerazioni sulle porte utilizzate per i pool di cloud storage

Per garantire che le regole ILM possano spostare oggetti da e verso il Cloud Storage Pool specificato, è necessario configurare la rete o le reti che contengono i nodi di storage del sistema. È necessario assicurarsi che le seguenti porte possano comunicare con il Cloud Storage Pool.

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

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

È possibile specificare una porta diversa quando si crea o si modifica un Cloud Storage Pool.

Se si utilizza un server proxy non trasparente, è necessario configurare anche un proxy di storage per consentire l'invio dei messaggi a endpoint esterni, ad esempio un endpoint su Internet.

Considerazioni sui costi

L'accesso allo storage nel cloud utilizzando un Cloud Storage Pool richiede la connettività di rete al cloud. Devi considerare il costo dell'infrastruttura di rete che utilizzerai per accedere al cloud e fornirlo in modo appropriato, in base alla quantità di dati che prevederai di spostare tra StorageGRID e il cloud utilizzando il pool di storage cloud.

Quando StorageGRID si connette all'endpoint esterno del pool di storage nel cloud, invia varie richieste per monitorare la connettività e garantire che possa eseguire le operazioni richieste. Anche se a queste richieste saranno associati costi aggiuntivi, il costo del monitoraggio di un pool di storage cloud dovrebbe essere solo una piccola frazione del costo complessivo di storage degli oggetti in S3 o Azure.

Se si devono spostare gli oggetti da un endpoint esterno del pool di cloud storage a StorageGRID, potrebbero

verificarsi costi più significativi. Gli oggetti possono essere spostati di nuovo in StorageGRID in uno dei seguenti casi:

- L'unica copia dell'oggetto si trova in un pool di storage cloud e si decide di memorizzare l'oggetto in StorageGRID. In questo caso, è sufficiente riconfigurare le regole e le policy ILM. Quando si verifica la valutazione ILM, StorageGRID invia più richieste per recuperare l'oggetto dal pool di storage cloud. StorageGRID crea quindi localmente il numero specificato di copie replicate o codificate per la cancellazione. Una volta spostato di nuovo l'oggetto in StorageGRID, la copia nel pool di storage cloud viene eliminata.
- Gli oggetti vengono persi a causa di un guasto al nodo di storage. Se l'unica copia rimanente di un oggetto si trova in un pool di storage cloud, StorageGRID ripristina temporaneamente l'oggetto e crea una nuova copia sul nodo di storage ripristinato.

> Quando gli oggetti vengono spostati di nuovo in StorageGRID da un pool di storage cloud, StorageGRID invia più richieste all'endpoint del pool di storage cloud per ciascun oggetto. Prima di spostare un gran numero di oggetti, contattare il supporto tecnico per ottenere assistenza nella stima dei tempi e dei costi associati.

S3: Autorizzazioni richieste per il bucket Cloud Storage Pool

La policy del bucket per il bucket S3 esterno utilizzato per un pool di storage cloud deve concedere l'autorizzazione StorageGRID per spostare un oggetto nel bucket, ottenere lo stato di un oggetto, ripristinare un oggetto dallo storage Glacier quando richiesto e molto altro ancora. Idealmente, StorageGRID dovrebbe avere un accesso completo al bucket (`s3:*`); tuttavia, se ciò non è possibile, il criterio bucket deve concedere le seguenti autorizzazioni S3 a StorageGRID:

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

S3: Considerazioni sul ciclo di vita del bucket esterno

Lo spostamento degli oggetti tra StorageGRID e il bucket S3 esterno specificato nel pool di storage cloud è controllato dalle regole ILM e dalla policy ILM attiva in StorageGRID. Al contrario, la transizione degli oggetti dal bucket S3 esterno specificato nel Cloud Storage Pool ad Amazon S3 Glacier o S3 Glacier Deep Archive (o a una soluzione di storage che implementa la classe di storage Glacier) è controllata dalla configurazione del ciclo di vita di tale bucket.

Se si desidera eseguire la transizione di oggetti dal Cloud Storage Pool, è necessario creare la configurazione del ciclo di vita appropriata sul bucket S3 esterno e utilizzare una soluzione di storage che implementa la classe di storage Glacier e supporta l'API S3 POST Object Restore.

Ad esempio, supponiamo che tutti gli oggetti spostati da StorageGRID al pool di storage cloud debbano essere trasferiti immediatamente allo storage Amazon S3 Glacier. Creare una configurazione del ciclo di vita sul

bucket S3 esterno che specifica una singola azione (**transizione**) come segue:

```
<LifecycleConfiguration>
  <Rule>
    <ID>Transition Rule</ID>
    <Filter>
       <Prefix></Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>0</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
  </Rule>
</LifecycleConfiguration>
```

Questa regola trasferirebbe tutti gli oggetti bucket al Glacier Amazon S3 il giorno in cui sono stati creati (ovvero il giorno in cui sono stati spostati da StorageGRID al pool di storage cloud).

> Quando si configura il ciclo di vita del bucket esterno, non utilizzare mai le azioni **Expiration** per definire quando gli oggetti scadono. Le azioni di scadenza fanno sì che il sistema di storage esterno elimini gli oggetti scaduti. Se in seguito si tenta di accedere a un oggetto scaduto da StorageGRID, l'oggetto eliminato non viene trovato.

Se si desidera trasferire oggetti nel Cloud Storage Pool in S3 Glacier Deep Archive (invece di Amazon S3 Glacier), specificare `<StorageClass>DEEP_ARCHIVE</StorageClass>` nel ciclo di vita del bucket. Tuttavia, tenere presente che non è possibile utilizzare `Expedited` tier per ripristinare gli oggetti da S3 Glacier Deep Archive.

Azure: Considerazioni per il Tier di accesso

Quando si configura un account di storage Azure, è possibile impostare il Tier di accesso predefinito su Hot o Cool. Quando si crea un account storage da utilizzare con un Cloud Storage Pool, è necessario utilizzare l'hot Tier come Tier predefinito. Anche se StorageGRID imposta immediatamente il Tier per l'archiviazione quando sposta gli oggetti nel pool di storage cloud, l'utilizzo dell'impostazione predefinita di Hot garantisce che non venga addebitata una tariffa per l'eliminazione anticipata degli oggetti rimossi dal Tier Cool prima del minimo di 30 giorni.

Azure: Gestione del ciclo di vita non supportata

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

Informazioni correlate

"Creazione di un pool di storage cloud"

"S3: Specifica dei dettagli di autenticazione per un Cloud Storage Pool"

"C2S S3: Specifica dei dettagli di autenticazione per un Cloud Storage Pool"

"Azure: Specifica dei dettagli di autenticazione per un pool di storage cloud"

"Amministrare StorageGRID"

Confronto tra Cloud Storage Pools e la replica CloudMirror

Quando si inizia a utilizzare i pool di storage cloud, potrebbe essere utile comprendere le analogie e le differenze tra i pool di storage cloud e il servizio di replica di StorageGRID CloudMirror.

	Pool di cloud storage	**Servizio di replica di CloudMirror**
Qual è lo scopo principale?	Un Cloud Storage Pool agisce come destinazione di archiviazione. La copia dell'oggetto nel Cloud Storage Pool può essere l'unica copia dell'oggetto oppure può essere una copia aggiuntiva. Ovvero, invece di mantenere due copie on-premise, puoi conservare una sola copia all'interno di StorageGRID e inviarne una copia al pool di storage cloud.	Il servizio di replica CloudMirror consente a un tenant di replicare automaticamente gli oggetti da un bucket in StorageGRID (origine) a un bucket S3 esterno (destinazione). La replica di CloudMirror crea una copia indipendente di un oggetto in un'infrastruttura S3 indipendente.
Come viene configurato?	I pool di cloud storage vengono definiti allo stesso modo dei pool di storage, utilizzando Grid Manager o l'API Grid Management. È possibile selezionare un Cloud Storage Pool come posizione di posizionamento in una regola ILM. Mentre un pool di storage è costituito da un gruppo di nodi di storage, un pool di storage cloud viene definito utilizzando un endpoint remoto S3 o Azure (indirizzo IP, credenziali e così via).	Un utente tenant configura la replica di CloudMirror definendo un endpoint CloudMirror (indirizzo IP, credenziali e così via) utilizzando Tenant Manager o l'API S3. Una volta configurato l'endpoint CloudMirror, qualsiasi bucket di proprietà dell'account tenant può essere configurato per puntare all'endpoint CloudMirror.
Chi è responsabile della sua configurazione?	In genere, un amministratore di rete	In genere, un utente tenant
Qual è la destinazione?	• Qualsiasi infrastruttura S3 compatibile (incluso Amazon S3) • Tier Azure Blob Archive	• Qualsiasi infrastruttura S3 compatibile (incluso Amazon S3)
Qual è la causa dello spostamento degli oggetti nella destinazione?	Una o più regole ILM nel criterio ILM attivo. Le regole ILM definiscono gli oggetti che StorageGRID sposta nel pool di storage cloud e quando gli oggetti vengono spostati.	L'atto di inserire un nuovo oggetto in un bucket di origine configurato con un endpoint CloudMirror.gli oggetti che esistevano nel bucket di origine prima della configurazione del bucket con l'endpoint CloudMirror non vengono replicati, a meno che non vengano modificati.

	Pool di cloud storage	Servizio di replica di CloudMirror
Come vengono recuperati gli oggetti?	Le applicazioni devono effettuare richieste a StorageGRID per recuperare gli oggetti spostati in un pool di storage cloud. Se l'unica copia di un oggetto è stata trasferita allo storage di archiviazione, StorageGRID gestisce il processo di ripristino dell'oggetto in modo che possa essere recuperato.	Poiché la copia mirrorata nel bucket di destinazione è una copia indipendente, le applicazioni possono recuperare l'oggetto inviando richieste a StorageGRID o alla destinazione S3. Si supponga, ad esempio, di utilizzare la replica CloudMirror per eseguire il mirroring degli oggetti in un'organizzazione partner. Il partner può utilizzare le proprie applicazioni per leggere o aggiornare gli oggetti direttamente dalla destinazione S3. Non è necessario utilizzare StorageGRID.
Puoi leggere direttamente dalla destinazione?	No Gli oggetti spostati in un pool di storage cloud vengono gestiti da StorageGRID. Le richieste di lettura devono essere indirizzate a StorageGRID (e StorageGRID sarà responsabile del recupero dal pool di storage cloud).	Sì, perché la copia mirrorata è una copia indipendente.
Cosa succede se un oggetto viene cancellato dall'origine?	L'oggetto viene eliminato anche nel Cloud Storage Pool.	L'azione di eliminazione non viene replicata. Un oggetto cancellato non esiste più nel bucket StorageGRID, ma continua ad esistere nel bucket di destinazione. Allo stesso modo, gli oggetti nel bucket di destinazione possono essere cancellati senza influire sull'origine.
Come si accede agli oggetti dopo un disastro (sistema StorageGRID non operativo)?	I nodi StorageGRID guasti devono essere ripristinati. Durante questo processo, le copie degli oggetti replicati potrebbero essere ripristinate utilizzando le copie nel Cloud Storage Pool.	Le copie degli oggetti nella destinazione CloudMirror sono indipendenti da StorageGRID, pertanto è possibile accedervi direttamente prima del ripristino dei nodi StorageGRID.

Informazioni correlate

"Amministrare StorageGRID"

Creazione di un pool di storage cloud

Quando crei un pool di storage cloud, specifica il nome e la posizione del bucket o del container esterno che StorageGRID utilizzerà per memorizzare gli oggetti, il tipo di provider cloud (Amazon S3 o Azure Blob Storage) e le informazioni necessarie per accedere al bucket o al container esterno da parte di StorageGRID.

Di cosa hai bisogno

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

- È necessario disporre di autorizzazioni di accesso specifiche.
- Devi aver esaminato le linee guida per la configurazione dei Cloud Storage Pools.
- Il bucket o il container esterno a cui fa riferimento il Cloud Storage Pool deve esistere.
- È necessario disporre di tutte le informazioni di autenticazione necessarie per accedere al bucket o al container.

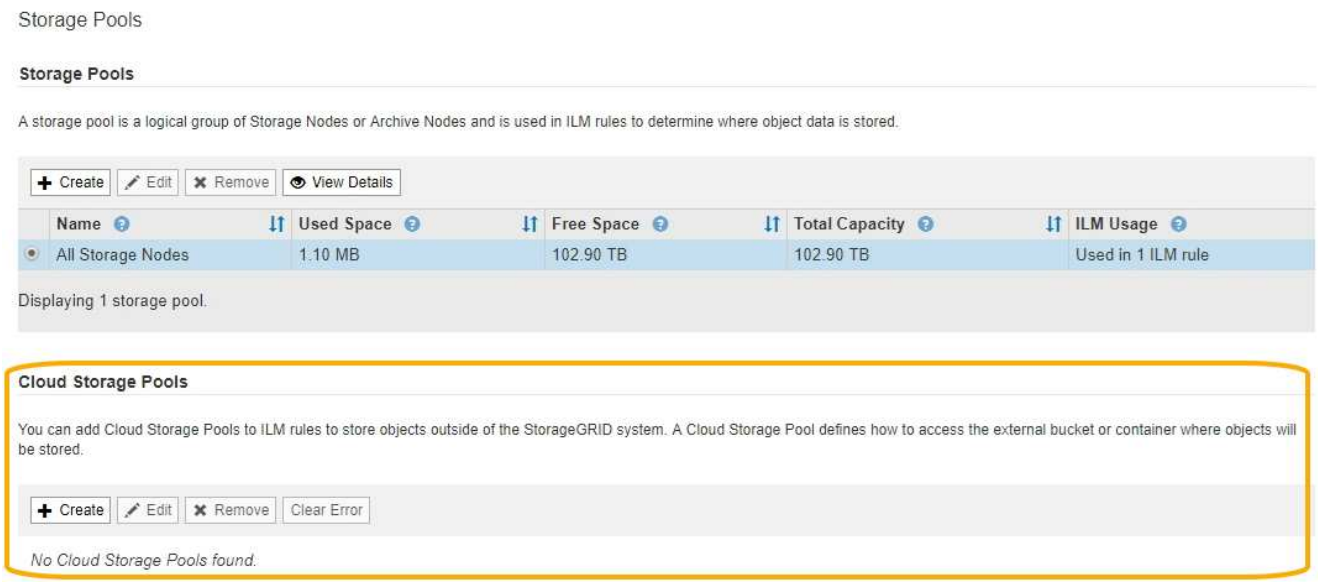
A proposito di questa attività

Un Cloud Storage Pool specifica un singolo bucket S3 esterno o un container di storage Azure Blob. StorageGRID convalida il pool di storage cloud non appena viene salvato, quindi devi assicurarti che il bucket o il container specificato nel pool di storage cloud esista e sia raggiungibile.

Fasi

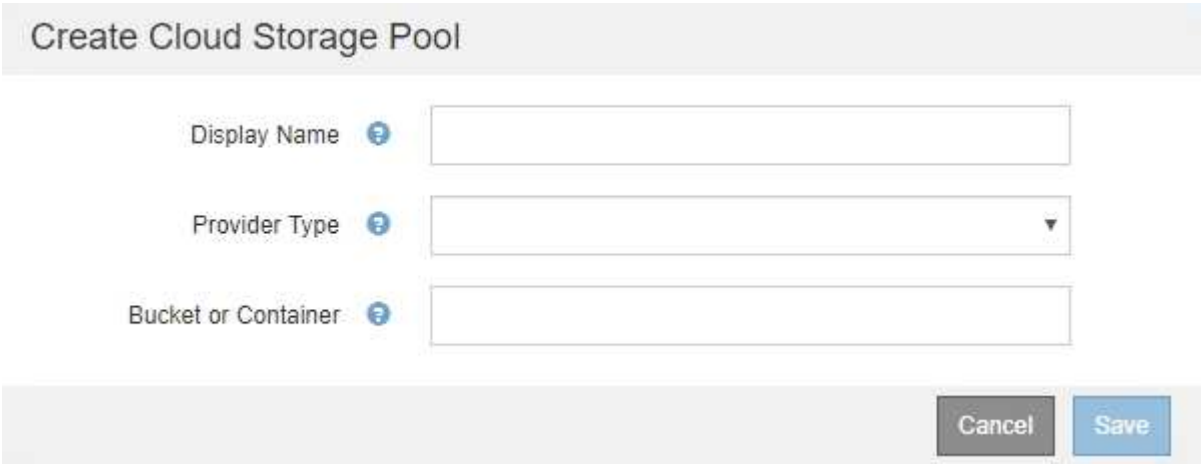
1. Selezionare **ILM** > **Storage Pools**.

   Viene visualizzata la pagina Storage Pools. Questa pagina include due sezioni: Pool di storage e pool di storage cloud.



2. Nella sezione Cloud Storage Pools della pagina, fare clic su **Create** (Crea).

   Viene visualizzata la finestra di dialogo Create Cloud Storage Pool (Crea pool di storage cloud).



3. Inserire le seguenti informazioni:

Campo	Descrizione
Nome visualizzato	Un nome che descrive brevemente il Cloud Storage Pool e il suo scopo. Utilizzare un nome che sia facile da identificare quando si configurano le regole ILM.
Tipo di provider	Quale cloud provider utilizzerai per questo Cloud Storage Pool: • Amazon S3 (selezionare questa opzione per un pool di storage cloud S3 o C2S S3) • Azure Blob Storage **Nota:** quando si seleziona un tipo di provider, nella parte inferiore della pagina vengono visualizzate le sezioni Service Endpoint, Authentication e Server Verification.
Bucket o container	Il nome del bucket S3 esterno o del container Azure creato per il Cloud Storage Pool. Il nome specificato qui deve corrispondere esattamente al nome del bucket o del container, altrimenti la creazione del Cloud Storage Pool non avrà esito positivo. Non è possibile modificare questo valore dopo il salvataggio del Cloud Storage Pool.

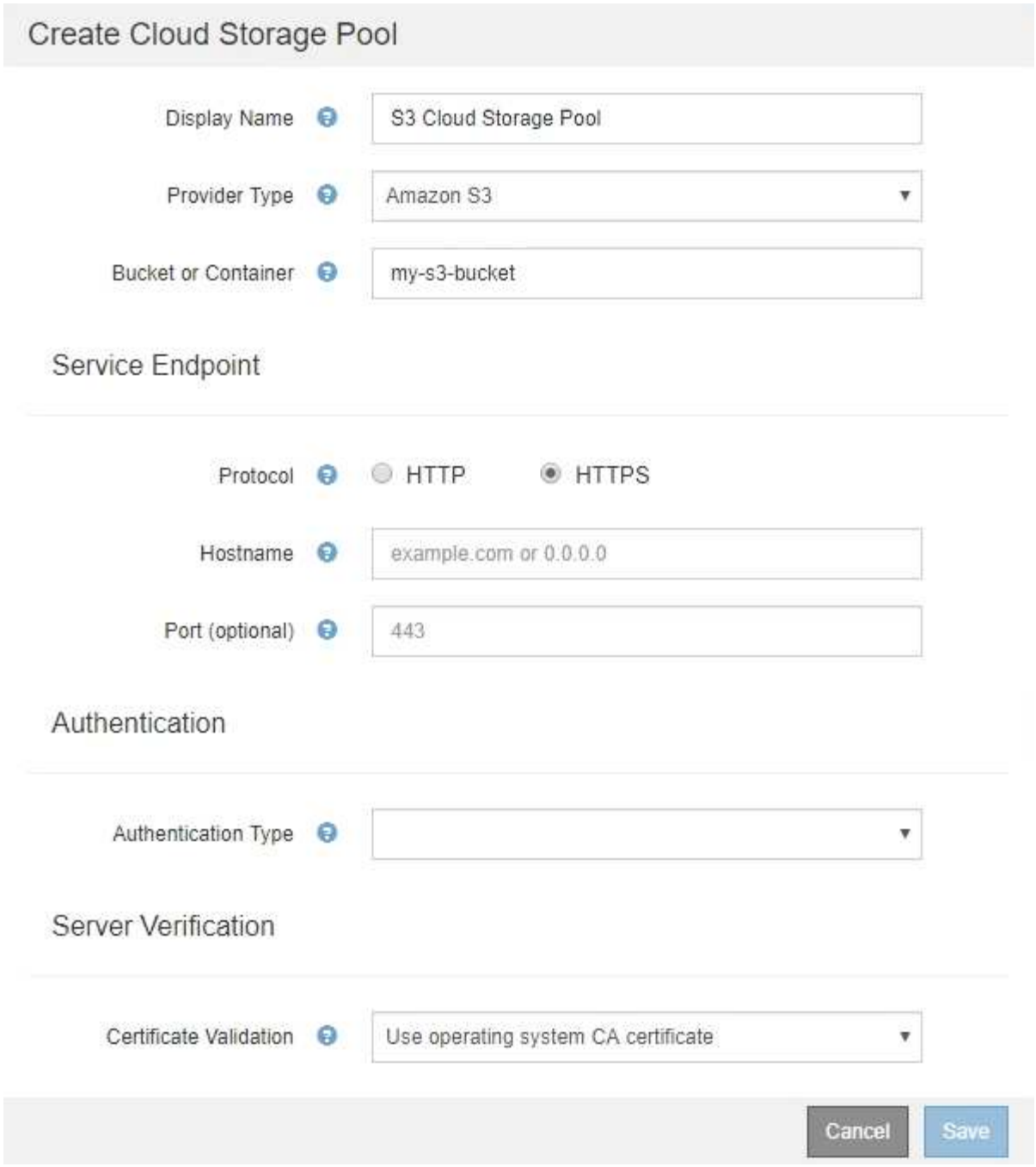
4. Completare le sezioni Service Endpoint, Authentication e Server Verification della pagina, in base al tipo di provider selezionato.
   - "S3: Specifica dei dettagli di autenticazione per un Cloud Storage Pool"
   - "C2S S3: Specifica dei dettagli di autenticazione per un Cloud Storage Pool"
   - "Azure: Specifica dei dettagli di autenticazione per un pool di storage cloud"

S3: Specifica dei dettagli di autenticazione per un Cloud Storage Pool

Quando si crea un Cloud Storage Pool per S3, è necessario selezionare il tipo di autenticazione richiesto per l'endpoint del Cloud Storage Pool. È possibile specificare Anonymous o immettere un ID della chiave di accesso e una chiave di accesso segreta.

Di cosa hai bisogno

- Devi aver inserito le informazioni di base per il Cloud Storage Pool e specificato **Amazon S3** come tipo di provider.



- Se si utilizza l'autenticazione della chiave di accesso, è necessario conoscere l'ID della chiave di accesso e la chiave di accesso segreta per il bucket S3 esterno.

Fasi

1. Nella sezione **Service Endpoint**, fornire le seguenti informazioni:

   a. Selezionare il protocollo da utilizzare per la connessione al Cloud Storage Pool.

      Il protocollo predefinito è HTTPS.

   b. Inserire il nome host del server o l'indirizzo IP del Cloud Storage Pool.

      Ad esempio:

`s3-aws-region.amazonaws.com`

> Non includere il nome del bucket in questo campo. Il nome del bucket viene incluso nel campo **bucket o container**.

a. Facoltativamente, specificare la porta da utilizzare per la connessione al Cloud Storage Pool.

   Lasciare vuoto questo campo per utilizzare la porta predefinita: Porta 443 per HTTPS o porta 80 per HTTP.

2. Nella sezione **Authentication**, selezionare il tipo di autenticazione richiesto per l'endpoint Cloud Storage Pool.

Opzione	Descrizione
Chiave di accesso	Per accedere al bucket Cloud Storage Pool sono necessari un ID della chiave di accesso e una chiave di accesso segreta.
Anonimo	Tutti hanno accesso al bucket Cloud Storage Pool. Non sono richiesti un ID della chiave di accesso e una chiave di accesso segreta.
CAP (portale di accesso C2S)	Utilizzato solo per C2S S3. Passare a. "C2S S3: Specifica dei dettagli di autenticazione per un Cloud Storage Pool".

3. Se si seleziona Access Key (chiave di accesso), immettere le seguenti informazioni:

Opzione	Descrizione
ID chiave di accesso	L'ID della chiave di accesso per l'account proprietario del bucket esterno.
Chiave di accesso segreta	La chiave di accesso segreta associata.

4. Nella sezione verifica server, selezionare il metodo da utilizzare per convalidare il certificato per le connessioni TLS al Cloud Storage Pool:

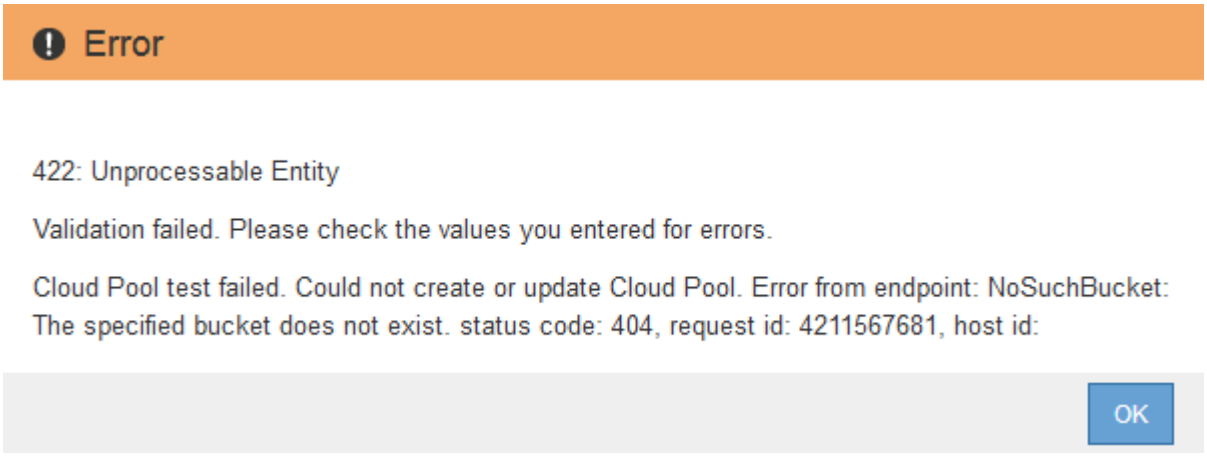
Opzione	Descrizione
Utilizzare il certificato CA del sistema operativo	Utilizzare i certificati CA predefiniti installati nel sistema operativo per proteggere le connessioni.
USA certificato CA personalizzato	Utilizzare un certificato CA personalizzato. Fare clic su **Select New** (Seleziona nuovo) e caricare il certificato CA con codifica PEM.
Non verificare il certificato	Il certificato utilizzato per la connessione TLS non viene verificato.

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

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

- Convalida l'esistenza del bucket e dell'endpoint del servizio e la possibilità di raggiungerli utilizzando le credenziali specificate.
- Scrive un file di marker nel bucket per identificare il bucket come un Cloud Storage Pool. Non rimuovere mai questo file, denominato `x-ntap-sgws-cloud-pool-uuid`.

Se la convalida del Cloud Storage Pool non riesce, viene visualizzato un messaggio di errore che spiega perché la convalida non è riuscita. Ad esempio, se si verifica un errore nel certificato o se il bucket specificato non esiste già, potrebbe essere visualizzato un errore.



Consultare le istruzioni per la risoluzione dei problemi relativi ai pool di storage cloud, risolvere il problema, quindi provare a salvare nuovamente il pool di storage cloud.

Informazioni correlate

"Risoluzione dei problemi relativi ai pool di storage cloud"

C2S S3: Specifica dei dettagli di autenticazione per un Cloud Storage Pool

Per utilizzare il servizio servizi cloud commerciali (C2S) S3 come pool di storage cloud, è necessario configurare il portale di accesso C2S (CAP) come tipo di autenticazione, in modo che StorageGRID possa richiedere credenziali temporanee per accedere al bucket S3 nel proprio account C2S.

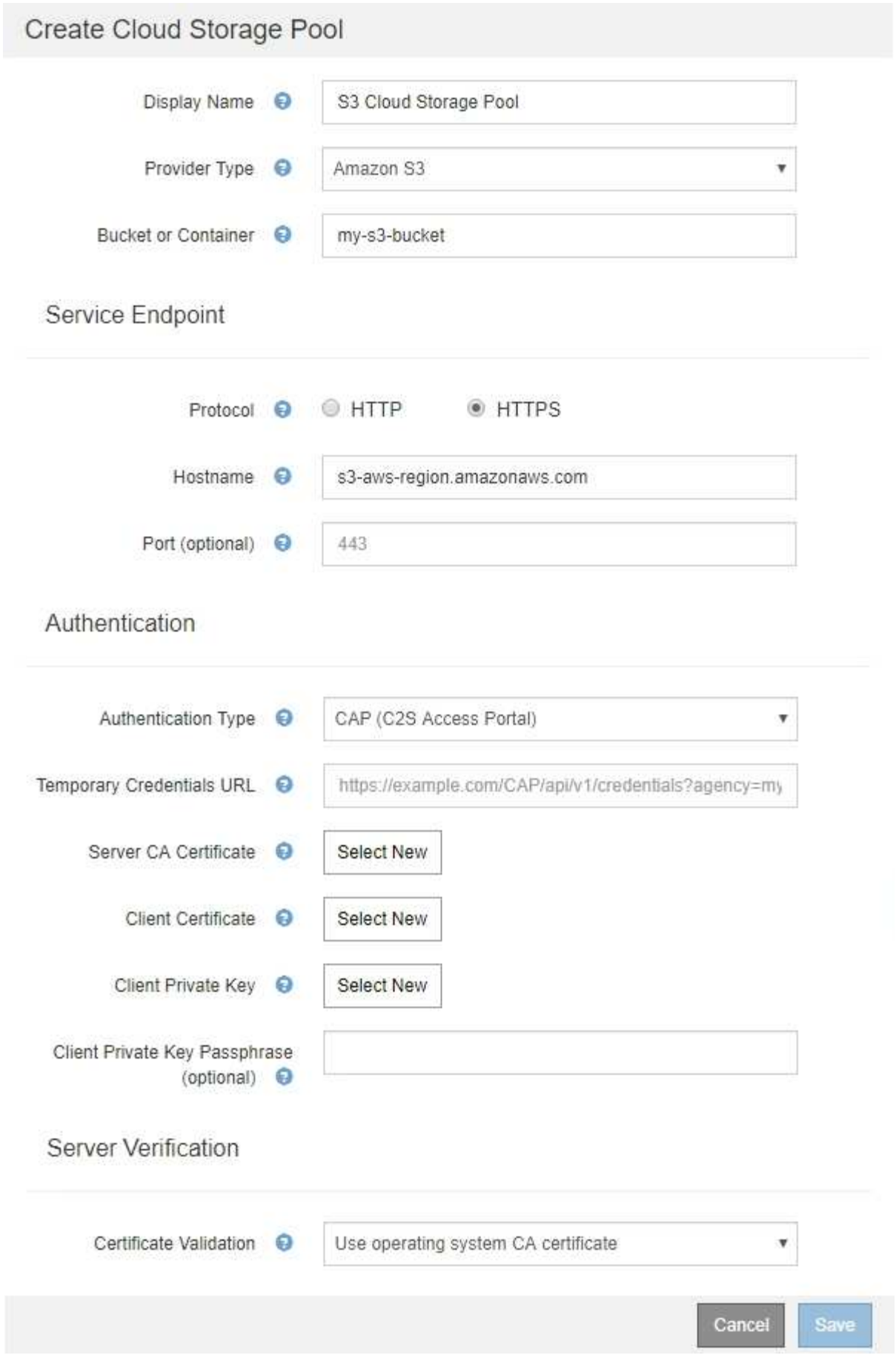
Di cosa hai bisogno

- Devi aver inserito le informazioni di base per un pool di storage cloud Amazon S3, incluso l'endpoint del servizio.
- È necessario conoscere l'URL completo che StorageGRID utilizzerà per ottenere le credenziali temporanee dal server CAP, inclusi tutti i parametri API obbligatori e facoltativi assegnati all'account C2S.
- È necessario disporre di un certificato CA del server emesso da un'autorità di certificazione governativa (CA) appropriata. StorageGRID utilizza questo certificato per verificare l'identità del server CAP. Il certificato CA del server deve utilizzare la codifica PEM.
- È necessario disporre di un certificato client emesso da un'autorità di certificazione governativa (CA) appropriata. StorageGRID utilizza questo certificato per identificare se stesso nel server CAP. Il certificato client deve utilizzare la codifica PEM e deve avere ottenuto l'accesso all'account C2S.
- È necessario disporre di una chiave privata con codifica PEM per il certificato client.
- Se la chiave privata per il certificato client è crittografata, è necessario disporre della passphrase per decrittografare il certificato.

Fasi

1. Nella sezione **Authentication**, selezionare **CAP (C2S Access Portal)** dall'elenco a discesa **Authentication Type** (tipo di autenticazione).

   Vengono visualizzati i campi DI autenticazione CAP C2S.


Create Cloud Storage Pool
Display Name
S3 Cloud Storage Pool
Provider Type
Amazon S3
Bucket or Container
my-s3-bucket
Service Endpoint
Protocol
HTTP
HTTPS
Hostname
s3-aws-region.amazonaws.com
Port (optional)
443
Authentication
Authentication Type
CAP (C2S Access Portal)
Temporary Credentials URL
https://example.com/CAP/api/v1/credentials?agency=my
Server CA Certificate
Select New
Client Certificate
Select New
Client Private Key
Select New
Client Private Key Passphrase (optional)
Server Verification
Certificate Validation
Use operating system CA certificate
Cancel
Save

2. Fornire le seguenti informazioni:
   a. Per **URL credenziali temporanee**, immettere l'URL completo che StorageGRID utilizzerà per ottenere le credenziali temporanee dal server CAP, inclusi tutti i parametri API obbligatori e facoltativi assegnati all'account C2S.
   b. Per **certificato CA server**, fare clic su **Seleziona nuovo** e caricare il certificato CA con codifica PEM che StorageGRID utilizzerà per verificare il server CAP.
   c. Per **certificato client**, fare clic su **Seleziona nuovo** e caricare il certificato con codifica PEM che StorageGRID utilizzerà per identificarsi nel server CAP.
   d. Per **Client Private Key**, fare clic su **Select New** (Seleziona nuovo) e caricare la chiave privata con codifica PEM per il certificato del client.

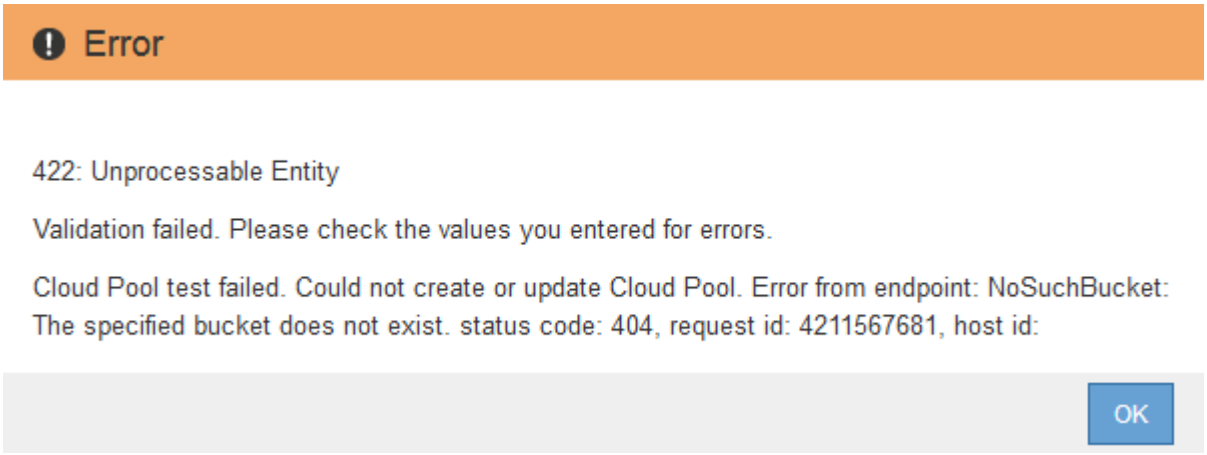
      Se la chiave privata è crittografata, è necessario utilizzare il formato tradizionale. (Il formato crittografato PKCS n. 8 non è supportato).

   e. Se la chiave privata del client è crittografata, immettere la passphrase per la decrittografia della chiave privata del client. In caso contrario, lasciare vuoto il campo **Client Private Key Passphrase** (Password chiave privata client).
3. Nella sezione verifica server, fornire le seguenti informazioni:
   a. Per **convalida certificato**, selezionare **Usa certificato CA personalizzato**.
   b. Fare clic su **Select New** (Seleziona nuovo) e caricare il certificato CA con codifica PEM.
4. Fare clic su **Save** (Salva).

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

- Convalida l'esistenza del bucket e dell'endpoint del servizio e la possibilità di raggiungerli utilizzando le credenziali specificate.
- Scrive un file di marker nel bucket per identificare il bucket come un Cloud Storage Pool. Non rimuovere mai questo file, denominato `x-ntap-sgws-cloud-pool-uuid`.

Se la convalida del Cloud Storage Pool non riesce, viene visualizzato un messaggio di errore che spiega perché la convalida non è riuscita. Ad esempio, se si verifica un errore nel certificato o se il bucket specificato non esiste già, potrebbe essere visualizzato un errore.



Consultare le istruzioni per la risoluzione dei problemi relativi ai pool di storage cloud, risolvere il problema, quindi provare a salvare nuovamente il pool di storage cloud.

Informazioni correlate

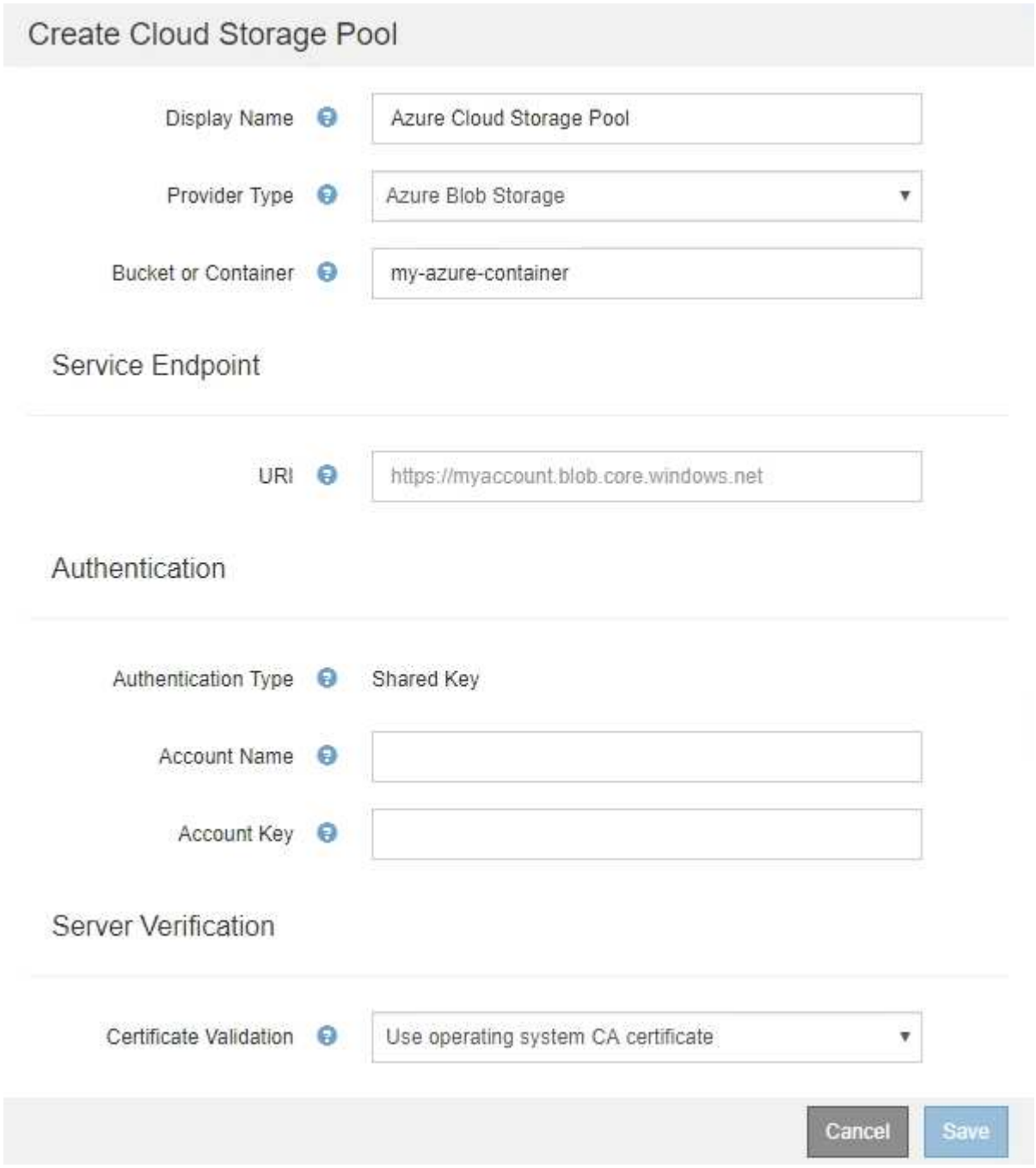
"Risoluzione dei problemi relativi ai pool di storage cloud"

Azure: Specifica dei dettagli di autenticazione per un pool di storage cloud

Quando si crea un pool di storage cloud per lo storage Azure Blob, è necessario specificare un nome account e una chiave account per il container esterno che StorageGRID utilizzerà per memorizzare gli oggetti.

Di cosa hai bisogno

- È necessario aver inserito le informazioni di base per il Cloud Storage Pool e specificato **Azure Blob Storage** come tipo di provider. Nel campo **Authentication Type** (tipo di autenticazione) viene visualizzato **Shared Key** (chiave condivisa).



- È necessario conoscere l'URI (Uniform Resource Identifier) utilizzato per accedere al container di storage Blob utilizzato per il Cloud Storage Pool.
- È necessario conoscere il nome dell'account di storage e la chiave segreta. È possibile utilizzare il portale Azure per trovare questi valori.

Fasi

1. Nella sezione **Service Endpoint**, immettere l'URI (Uniform Resource Identifier) utilizzato per accedere al container di storage Blob utilizzato per il Cloud Storage Pool.

   Specificare l'URI in uno dei seguenti formati:

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

   Se non si specifica una porta, per impostazione predefinita viene utilizzata la porta 443 per gli URI HTTPS e la porta 80 per gli URI HTTP. + + + **URI di esempio per Azure Blob Storage Container**: `https://myaccount.blob.core.windows.net`

2. Nella sezione **Authentication**, fornire le seguenti informazioni:

   a. Per **Nome account**, immettere il nome dell'account di storage Blob proprietario del container di servizi esterno.

   b. Per **account Key**, immettere la chiave segreta per l'account di storage Blob.

   Per gli endpoint Azure, è necessario utilizzare l'autenticazione con chiave condivisa.

3. Nella sezione **verifica server**, selezionare il metodo da utilizzare per validare il certificato per le connessioni TLS al Cloud Storage Pool:

Opzione	Descrizione
Utilizzare il certificato CA del sistema operativo	Utilizzare i certificati CA predefiniti installati nel sistema operativo per proteggere le connessioni.
USA certificato CA personalizzato	Utilizzare un certificato CA personalizzato. Fare clic su **Select New** (Seleziona nuovo) e caricare il certificato con codifica PEM.
Non verificare il certificato	Il certificato utilizzato per la connessione TLS non viene verificato.

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

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

- Convalida l'esistenza del container e dell'URI e ne consente l'accesso utilizzando le credenziali specificate.
- Scrive un file marker nel container per identificarlo come pool di storage cloud. Non rimuovere mai questo file, denominato `x-ntap-sgws-cloud-pool-uuid`.

Se la convalida del Cloud Storage Pool non riesce, viene visualizzato un messaggio di errore che spiega perché la convalida non è riuscita. Ad esempio, se si verifica un errore nel certificato o se il contenitore specificato non esiste già, potrebbe essere visualizzato un errore.

Consultare le istruzioni per la risoluzione dei problemi relativi ai pool di storage cloud, risolvere il problema, quindi provare a salvare nuovamente il pool di storage cloud.

Informazioni correlate

"Risoluzione dei problemi relativi ai pool di storage cloud"

Modifica di un pool di storage cloud

È possibile modificare un Cloud Storage Pool per modificarne il nome, l'endpoint del servizio o altri dettagli; tuttavia, non è possibile modificare il bucket S3 o il container Azure per un Cloud Storage Pool.

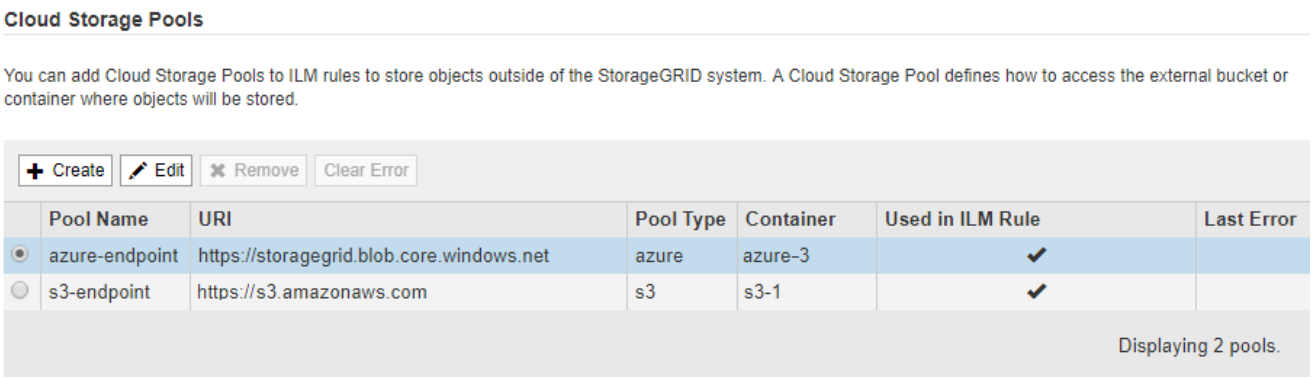
Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.
- Devi aver esaminato le linee guida per la configurazione dei Cloud Storage Pools.

Fasi

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

   Viene visualizzata la pagina Storage Pools. La tabella Cloud Storage Pools elenca i Cloud Storage Pools esistenti.



2. Selezionare il pulsante di opzione per il Cloud Storage Pool che si desidera modificare.
3. Fare clic su **Edit** (Modifica).
4. Se necessario, modificare il nome visualizzato, l'endpoint del servizio, le credenziali di autenticazione o il metodo di convalida del certificato.

   Non è possibile modificare il tipo di provider, il bucket S3 o il container Azure per un Cloud Storage Pool.

   Se in precedenza è stato caricato un certificato server o client, è possibile selezionare **Visualizza attuale** per rivedere il certificato attualmente in uso.

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

   Quando si salva un pool di storage cloud, StorageGRID convalida l'esistenza del bucket o del container e dell'endpoint del servizio e che è possibile raggiungerli utilizzando le credenziali specificate.

Se la convalida del Cloud Storage Pool non riesce, viene visualizzato un messaggio di errore. Ad esempio, se si verifica un errore del certificato, potrebbe essere visualizzato un errore.

Consultare le istruzioni per la risoluzione dei problemi relativi ai pool di storage cloud, risolvere il problema, quindi provare a salvare nuovamente il pool di storage cloud.

Informazioni correlate

"Considerazioni per i Cloud Storage Pools"

"Risoluzione dei problemi relativi ai pool di storage cloud"

Rimozione di un pool di storage cloud

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

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.
- Hai confermato che il bucket S3 o il container Azure non contiene oggetti. Si verifica un errore se si tenta di rimuovere un Cloud Storage Pool se contiene oggetti. Consulta “risoluzione dei problemi relativi ai pool di storage cloud”.

> Quando crei un pool di storage cloud, StorageGRID scrive un file di marker nel bucket o nel container per identificarlo come pool di storage cloud. Non rimuovere questo file, denominato `x-ntap-sgws-cloud-pool-uuid`.

- Sono già state rimosse le regole ILM che potrebbero aver utilizzato il pool.

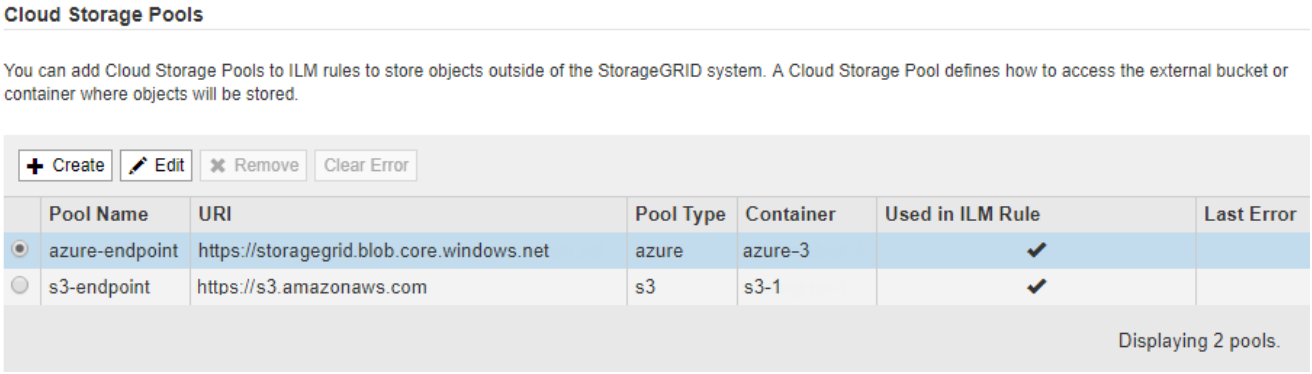
Fasi

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

   Viene visualizzata la pagina Storage Pools.

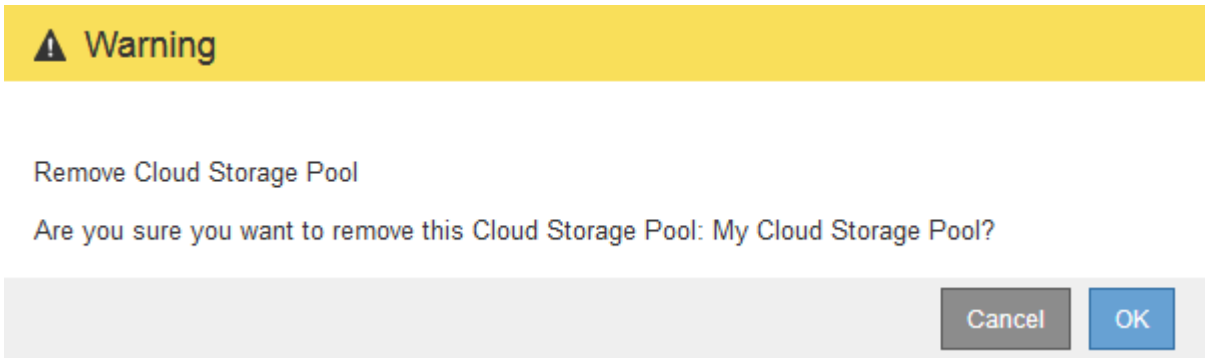
2. Selezionare il pulsante di opzione per un Cloud Storage Pool che non è attualmente utilizzato in una regola ILM.

   Non è possibile rimuovere un pool di storage cloud se utilizzato in una regola ILM. Il pulsante **Remove** (Rimuovi) è disattivato.



3. Fare clic su **Rimuovi**.

   Viene visualizzato un avviso di conferma.



4. Fare clic su **OK**.

   Il Cloud Storage Pool viene rimosso.

Informazioni correlate

"Risoluzione dei problemi relativi ai pool di storage cloud"

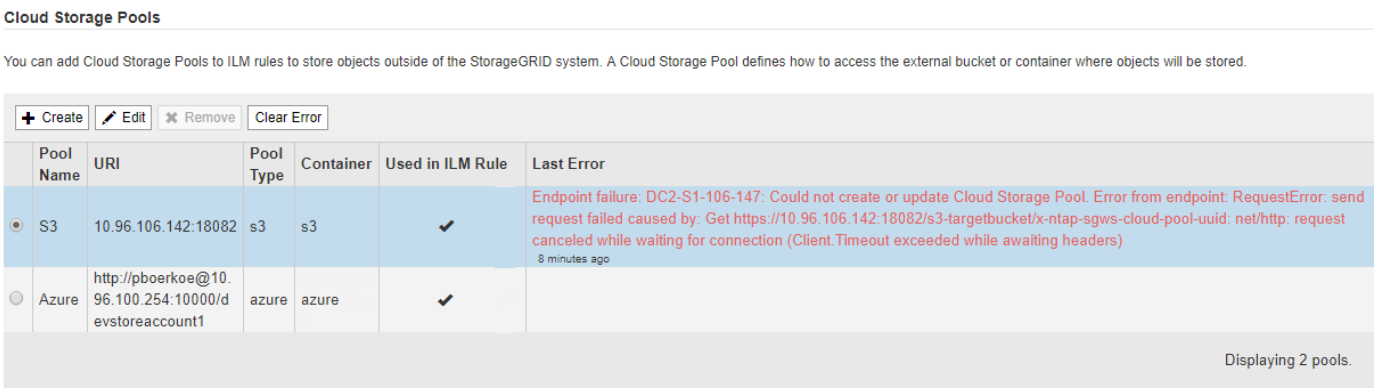
Risoluzione dei problemi relativi ai pool di storage cloud

Se si verificano errori durante la creazione, la modifica o l'eliminazione di un pool di storage cloud, attenersi alla procedura di risoluzione dei problemi riportata di seguito per risolvere il problema.

Determinare se si è verificato un errore

StorageGRID esegue una semplice verifica dello stato di salute di ogni pool di storage cloud una volta al minuto per garantire che sia possibile accedere al pool di storage cloud e che funzioni correttamente. Se il controllo dello stato di salute rileva un problema, viene visualizzato un messaggio nella colonna Last Error (ultimo errore) della tabella Cloud Storage Pools (pool di storage cloud) della pagina Storage Pools (pool di storage).

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

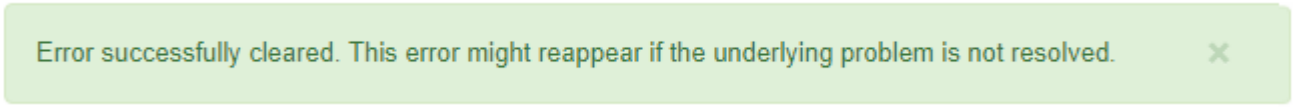


Inoltre, un avviso di **errore di connettività del Cloud Storage Pool** viene attivato se il controllo dello stato di

salute rileva che uno o più nuovi errori del Cloud Storage Pool si sono verificati negli ultimi 5 minuti. Se si riceve una notifica via email per questo avviso, accedere alla pagina Storage Pool (selezionare **ILM** > **Storage Pools**), esaminare i messaggi di errore nella colonna Last Error (ultimo errore) e consultare le linee guida per la risoluzione dei problemi riportate di seguito.

Verifica della risoluzione di un errore

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



Se il problema sottostante è stato risolto, il messaggio di errore non viene più visualizzato. Tuttavia, se il problema sottostante non è stato risolto (o se si verifica un errore diverso), il messaggio di errore viene visualizzato nella colonna Last Error (ultimo errore) entro pochi minuti.

Errore: Questo Cloud Storage Pool contiene contenuti imprevisti

Questo errore potrebbe verificarsi quando si tenta di creare, modificare o eliminare un pool di storage cloud. Questo errore si verifica se il bucket o il container include `x-ntap-sgws-cloud-pool-uuid` Il file marker, ma non ha l'UUID previsto.

In genere, questo errore viene visualizzato solo se si crea un nuovo pool di storage cloud e un'altra istanza di StorageGRID sta già utilizzando lo stesso pool di storage cloud.

Per risolvere il problema, attenersi alla seguente procedura:

- Assicurati che nessuno nella tua organizzazione stia utilizzando questo Cloud Storage Pool.
- Eliminare `x-ntap-sgws-cloud-pool-uuid` E provare a configurare nuovamente il Cloud Storage Pool.

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

Questo errore potrebbe verificarsi quando si tenta di creare o modificare un pool di storage cloud. Questo errore indica che alcuni problemi di connettività o configurazione impediscono a StorageGRID di scrivere nel pool di storage cloud.

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

- Se il messaggio di errore contiene `Get *url*: EOF`, Verificare che l'endpoint del servizio utilizzato per il Cloud Storage Pool non utilizzi il protocollo HTTP per un container o bucket che richiede HTTPS.
- Se il messaggio di errore contiene `Get *url*: net/http: request canceled while waiting for connection`, Verificare che la configurazione di rete consenta ai nodi di storage di accedere all'endpoint del servizio utilizzato per il Cloud Storage Pool.
- Per tutti gli altri messaggi di errore degli endpoint, provare una o più delle seguenti soluzioni:
  - Creare un container o bucket esterno con lo stesso nome immesso per il Cloud Storage Pool e provare a salvare di nuovo il nuovo Cloud Storage Pool.
  - Correggere il nome del container o bucket specificato per il Cloud Storage Pool e provare a salvare di nuovo il nuovo Cloud Storage Pool.

Errore: Impossibile analizzare il certificato CA

Questo errore potrebbe verificarsi quando si tenta di creare o modificare un pool di storage cloud. L'errore si verifica se StorageGRID non ha potuto analizzare il certificato inserito durante la configurazione del pool di storage cloud.

Per correggere il problema, controllare il certificato CA fornito per eventuali problemi.

Errore: Impossibile trovare un pool di storage cloud con questo ID

Questo errore potrebbe verificarsi quando si tenta di modificare o eliminare un pool di storage cloud. Questo errore si verifica se l'endpoint restituisce una risposta 404, il che può significare una delle seguenti:

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

Provare una o più delle seguenti operazioni per risolvere il problema:

- Verificare che l'utente associato alla chiave di accesso configurata disponga delle autorizzazioni necessarie.
- Modificare il Cloud Storage Pool con le credenziali che dispongono delle autorizzazioni necessarie.
- Se le autorizzazioni sono corrette, contattare l'assistenza.

Errore: Impossibile controllare il contenuto del Cloud Storage Pool. Errore dall'endpoint

Questo errore potrebbe verificarsi quando si tenta di eliminare un pool di storage cloud. Questo errore indica che un problema di connettività o configurazione impedisce a StorageGRID di leggere il contenuto del bucket del pool di storage cloud.

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

Errore: Gli oggetti sono già stati posizionati in questo bucket

Questo errore potrebbe verificarsi quando si tenta di eliminare un pool di storage cloud. Non è possibile eliminare un Cloud Storage Pool se contiene dati spostati da ILM, dati presenti nel bucket prima della configurazione del Cloud Storage Pool o dati inseriti nel bucket da un'altra origine dopo la creazione del Cloud Storage Pool.

Provare una o più delle seguenti operazioni per risolvere il problema:

- Seguire le istruzioni per lo spostamento degli oggetti in StorageGRID in "ciclo di vita di un oggetto pool di storage cloud".
- Se si è certi che ILM non abbia inserito gli oggetti rimanenti nel Cloud Storage Pool, eliminarli manualmente dal bucket.

> Non eliminare mai manualmente oggetti da un Cloud Storage Pool che potrebbe essere stato collocato in tale posizione da ILM. Se in un secondo momento si tenta di accedere a un oggetto eliminato manualmente da StorageGRID, l'oggetto eliminato non viene trovato.

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

Questo errore potrebbe verificarsi se è stato configurato un proxy dello storage non trasparente tra i nodi di storage e l'endpoint S3 esterno utilizzato per il Cloud Storage Pool. Questo errore si verifica se il server proxy esterno non riesce a raggiungere l'endpoint del Cloud Storage Pool. Ad esempio, il server DNS potrebbe non essere in grado di risolvere il nome host o potrebbe esserci un problema di rete esterno.

Provare una o più delle seguenti operazioni per risolvere il problema:

- Verificare le impostazioni del Cloud Storage Pool (**ILM** > **Storage Pools**).
- Controllare la configurazione di rete del server proxy dello storage.

Informazioni correlate

"Ciclo di vita di un oggetto Cloud Storage Pool"

Informazioni sul copyright

Informazioni sul marchio commerciale