



Creazione di un pool di storage cloud

StorageGRID 11.5

NetApp
April 11, 2024

Sommario

- Creazione di un pool di storage cloud 1
 - S3: Specifica dei dettagli di autenticazione per un Cloud Storage Pool 2
 - C2S S3: Specifica dei dettagli di autenticazione per un Cloud Storage Pool 5
 - Azure: Specifica dei dettagli di autenticazione per un pool di storage cloud 9

Creazione di un pool di storage cloud

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

Di cosa hai bisogno

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

A proposito di questa attività

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

Fasi

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

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

Storage Pools

Storage Pools

A storage pool is a logical group of Storage Nodes or Archive Nodes and is used in ILM rules to determine where object data is stored.

+ Create Edit Remove View Details

Name	Used Space	Free Space	Total Capacity	ILM Usage
All Storage Nodes	1.10 MB	102.90 TB	102.90 TB	Used in 1 ILM rule

Displaying 1 storage pool.

Cloud Storage Pools

You can add Cloud Storage Pools to ILM rules to store objects outside of the StorageGRID system. A Cloud Storage Pool defines how to access the external bucket or container where objects will be stored.

+ Create Edit Remove Clear Error

No Cloud Storage Pools found.


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

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

Create Cloud Storage Pool

Display Name 

Provider Type 

Bucket or Container 

3. Inserire le seguenti informazioni:

Campo	Descrizione
Nome visualizzato	Un nome che descrive brevemente il Cloud Storage Pool e il suo scopo. Utilizzare un nome che sia facile da identificare quando si configurano le regole ILM.
Tipo di provider	<p>Quale cloud provider utilizzerai per questo Cloud Storage Pool:</p> <ul style="list-style-type: none"> • Amazon S3 (selezionare questa opzione per un pool di storage cloud S3 o C2S S3) • Azure Blob Storage <p>Nota: quando si seleziona un tipo di provider, nella parte inferiore della pagina vengono visualizzate le sezioni Service Endpoint, Authentication e Server Verification.</p>
Bucket o container	Il nome del bucket S3 esterno o del container Azure creato per il Cloud Storage Pool. Il nome specificato qui deve corrispondere esattamente al nome del bucket o del container, altrimenti la creazione del Cloud Storage Pool non avrà esito positivo. Non è possibile modificare questo valore dopo il salvataggio del Cloud Storage Pool.

4. Completare le sezioni Service Endpoint, Authentication e Server Verification della pagina, in base al tipo di provider selezionato.

- ["S3: Specifica dei dettagli di autenticazione per un Cloud Storage Pool"](#)
- ["C2S S3: Specifica dei dettagli di autenticazione per un Cloud Storage Pool"](#)
- ["Azure: Specifica dei dettagli di autenticazione per un pool di storage cloud"](#)

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

Quando si crea un Cloud Storage Pool per S3, è necessario selezionare il tipo di

autenticazione richiesto per l'endpoint del Cloud Storage Pool. È possibile specificare Anonymous o immettere un ID della chiave di accesso e una chiave di accesso segreta.

Di cosa hai bisogno

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

Create Cloud Storage Pool

Display Name	<input type="text" value="S3 Cloud Storage Pool"/>
Provider Type	<input type="text" value="Amazon S3"/>
Bucket or Container	<input type="text" value="my-s3-bucket"/>

Service Endpoint

Protocol	<input type="radio"/> HTTP <input checked="" type="radio"/> HTTPS
Hostname	<input type="text" value="example.com or 0.0.0.0"/>
Port (optional)	<input type="text" value="443"/>

Authentication

Authentication Type	<input type="text"/>
---------------------	----------------------

Server Verification

Certificate Validation	<input type="text" value="Use operating system CA certificate"/>
------------------------	--

- 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.

Opzione	Descrizione
USA certificato CA personalizzato	Utilizzare un certificato CA personalizzato. Fare clic su Select New (Seleziona nuovo) e caricare il certificato CA con codifica PEM.
Non verificare il certificato	Il certificato utilizzato per la connessione TLS non viene verificato.

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

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

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

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

Error

422: Unprocessable Entity

Validation failed. Please check the values you entered for errors.

Cloud Pool test failed. Could not create or update Cloud Pool. Error from endpoint: NoSuchBucket: The specified bucket does not exist. status code: 404, request id: 4211567681, host id:

OK

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

Informazioni correlate

["Risoluzione dei problemi relativi ai pool di storage cloud"](#)

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

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

Di cosa hai bisogno

- Devi aver inserito le informazioni di base per un pool di storage cloud Amazon S3, incluso l'endpoint del

servizio.

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

Fasi

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

Vengono visualizzati i campi DI autenticazione CAP C2S.

Create Cloud Storage Pool

Display Name ⓘ S3 Cloud Storage Pool

Provider Type ⓘ Amazon S3 ▼

Bucket or Container ⓘ my-s3-bucket

Service Endpoint

Protocol ⓘ HTTP HTTPS

Hostname ⓘ s3-aws-region.amazonaws.com

Port (optional) ⓘ 443

Authentication

Authentication Type ⓘ CAP (C2S Access Portal) ▼

Temporary Credentials URL ⓘ https://example.com/CAP/api/v1/credentials?agency=my

Server CA Certificate ⓘ 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.

Error

422: Unprocessable Entity

Validation failed. Please check the values you entered for errors.

Cloud Pool test failed. Could not create or update Cloud Pool. Error from endpoint: NoSuchBucket:
The specified bucket does not exist. status code: 404, request id: 4211567681, host id:

OK

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

Informazioni correlate

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

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

Di cosa hai bisogno

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

Create Cloud Storage Pool

Display Name ⓘ Azure Cloud Storage Pool

Provider Type ⓘ Azure Blob Storage ▼

Bucket or Container ⓘ my-azure-container

Service Endpoint

URI ⓘ https://myaccount.blob.core.windows.net

Authentication

Authentication Type ⓘ Shared Key

Account Name ⓘ

Account Key ⓘ

Server Verification

Certificate Validation ⓘ Use operating system CA certificate ▼

Cancel

Save

- 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"](#)

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.