Cloud Storage Pool Erstellen

StorageGRID

NetApp
April 10, 2024

This PDF was generated from https://docs.netapp.com/de-de/storagegrid-116/ilm/s3-authentication-details-for-cloud-storage-pool.html on April 10, 2024. Always check docs.netapp.com for the latest.

Inhalt

Erstellen Sie einen Cloud-Storage-Pool 1
S3: Angeben von Authentifizierungsdetails für einen Cloud Storage-Pool 2
C2S S3: Geben Sie die Authentifizierungsdetails für einen Cloud-Storage-Pool an 7
Azure: Geben Sie die Authentifizierungsdetails für einen Cloud Storage-Pool an 10

Erstellen Sie einen Cloud-Storage-Pool

Wenn Sie einen Cloud-Storage-Pool erstellen, geben Sie den Namen und den Standort des externen Buckets oder Containers an, den StorageGRID zum Speichern von Objekten, dem Cloud-Provider-Typ (Amazon S3 oder Azure Blob Storage) und den Informationen, die StorageGRID für den Zugriff auf den externen Bucket oder Container benötigt.

Was Sie benötigen

- Sie sind mit einem bei Grid Manager angemeldet Unterstützter Webbrowser.
- Sie haben spezifische Zugriffsberechtigungen.
- Sie haben die Richtlinien zur Konfiguration von Cloud-Speicherpools überprüft.
- Der externe Bucket oder Container, auf den der Cloud-Storage-Pool verweist, ist bereits vorhanden.
- Sie verfügen über alle Authentifizierungsinformationen, die für den Zugriff auf den Bucket oder Container erforderlich sind.

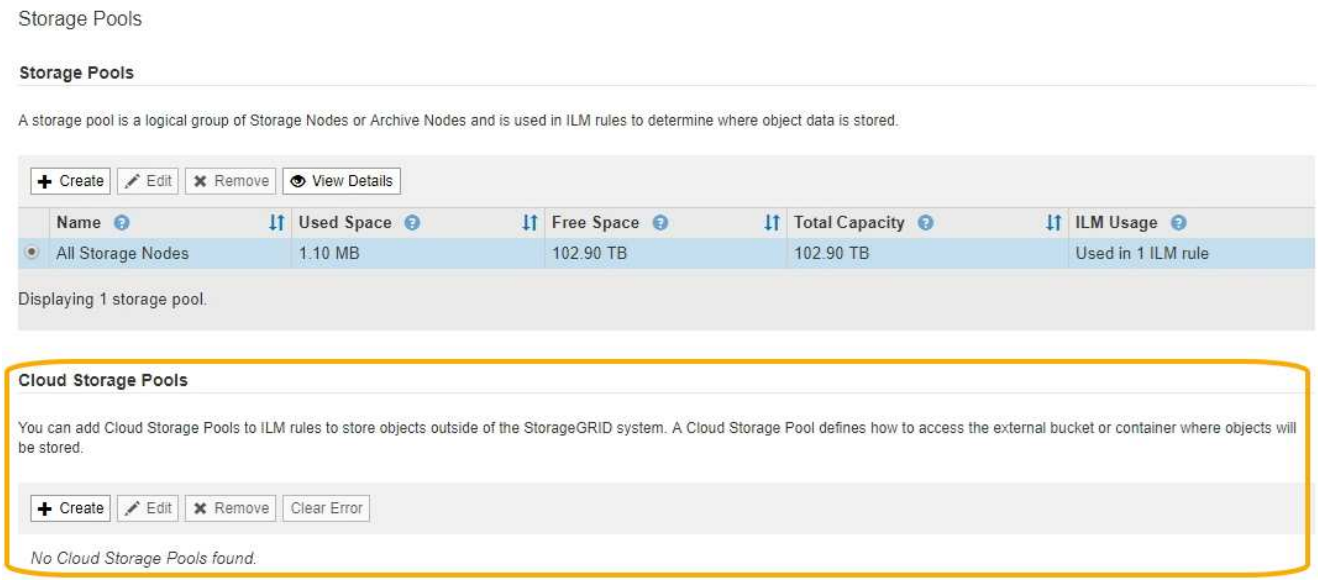
Über diese Aufgabe

Ein Cloud-Storage-Pool gibt einen einzelnen externen S3-Bucket oder Azure Blob-Storage-Container an. StorageGRID validiert den Cloud-Storage-Pool, sobald Sie ihn speichern. Sie müssen also sicherstellen, dass der im Cloud-Speicherpool angegebene Bucket oder Container vorhanden ist und erreichbar ist.

Schritte

1. Wählen Sie **ILM Storage Pools** aus.

   Die Seite Speicherpools wird angezeigt. Diese Seite enthält zwei Abschnitte: Speicherpools und Cloud-Speicherpools.



2. Wählen Sie im Abschnitt Cloud-Speicherpools der Seite **Erstellen** aus.

   Das Dialogfeld Cloud-Speicherpool erstellen wird angezeigt.

3. Geben Sie die folgenden Informationen ein:

Feld	Beschreibung
Anzeigename	Ein Name, der kurz den Cloud Storage Pool und dessen Zweck beschreibt. Verwenden Sie einen Namen, der leicht zu erkennen ist, wann Sie ILM-Regeln konfigurieren.
Art Des Anbieters	Welcher Cloud-Provider nutzen Sie für diesen Cloud-Storage-Pool? • **Amazon S3**: Wählen Sie diese Option für einen S3-, C2S S3- oder Google Cloud Platform (GCP)-Endpunkt. • * Azure Blob Storage* **Hinweis:** Wenn Sie einen Provider-Typ auswählen, werden unten auf der Seite die Abschnitte „Service Endpoint“, „Authentifizierung“ und „Server-Überprüfung“ angezeigt.
Bucket oder Container	Der Name des externen S3-Buckets oder Azure-Containers, der für den Cloud-Storage-Pool erstellt wurde. Der hier angegebene Name muss exakt mit dem Bucket oder Container-Namen übereinstimmen, oder die Erstellung von Cloud-Storage-Pool schlägt fehl. Sie können diesen Wert nicht ändern, nachdem der Cloud-Speicherpool gespeichert wurde.

4. Schließen Sie die Abschnitte „Service Endpoint“, „Authentifizierung“ und „Server-Verifizierung“ der Seite basierend auf dem ausgewählten Provider-Typ ab.
   - S3: Geben Sie Authentifizierungsdetails für einen Cloud Storage-Pool an
   - C2S S3: Geben Sie die Authentifizierungsdetails für einen Cloud-Storage-Pool an
   - Azure: Geben Sie die Authentifizierungsdetails für einen Cloud Storage-Pool an

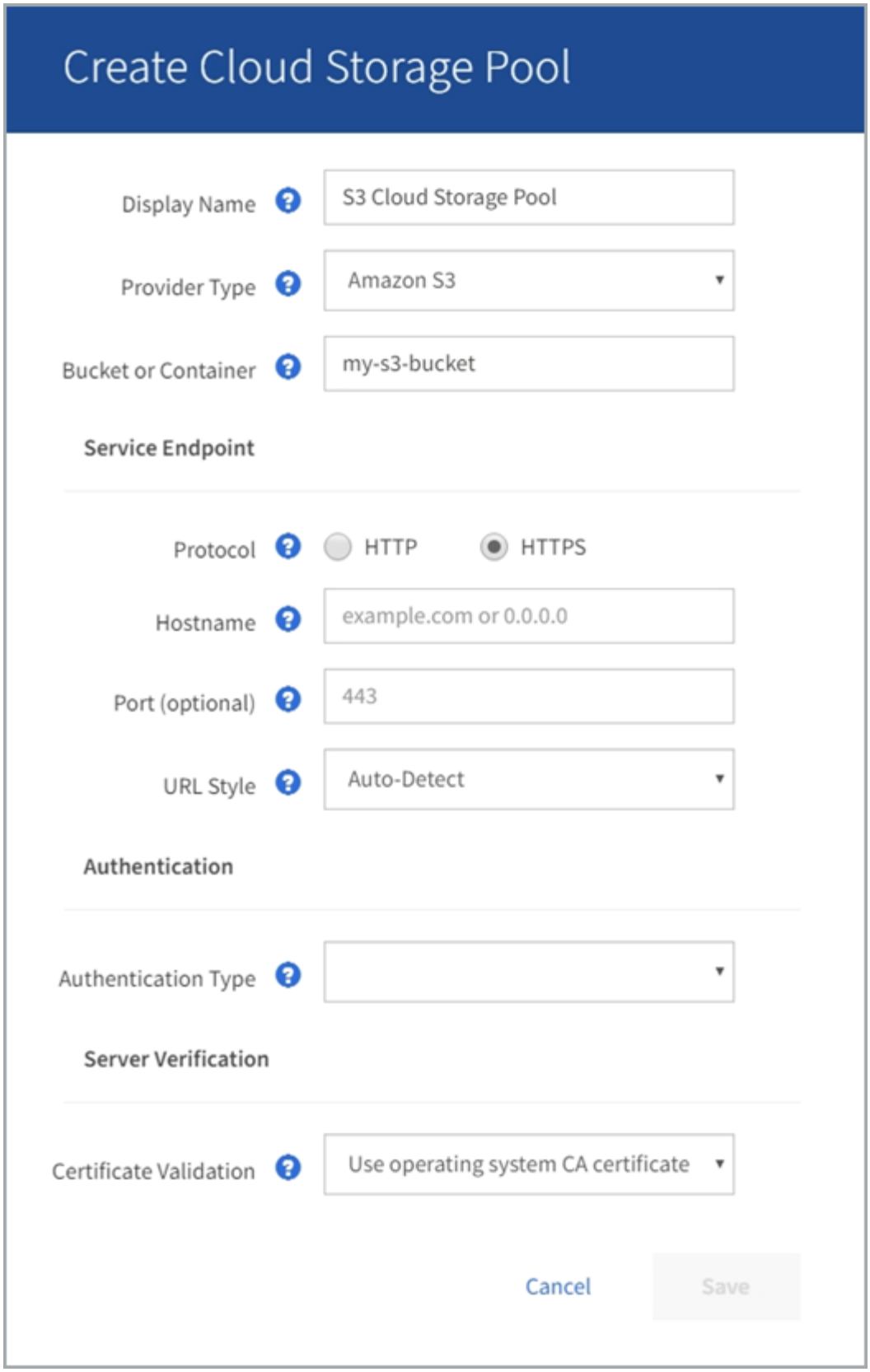
S3: Angeben von Authentifizierungsdetails für einen Cloud Storage-Pool

Wenn Sie einen Cloud Storage Pool für S3 erstellen, müssen Sie den

Authentifizierungstyp für den Cloud Storage Pool-Endpunkt auswählen. Sie können Anonymous angeben oder eine Zugriffsschlüssel-ID und einen geheimen Zugriffsschlüssel eingeben.

Was Sie benötigen

- Sie haben die Basisinformationen für den Cloud-Speicherpool eingegeben und als Provider-Typ **Amazon S3** angegeben.



- Wenn Sie die Authentifizierung für Zugriffsschlüssel verwenden, kennen Sie die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel für den externen S3-Bucket.

Schritte

1. Geben Sie im Abschnitt * Service Endpoint* folgende Informationen an:

a. Wählen Sie das Protokoll aus, das bei der Verbindung mit dem Cloud-Storage-Pool verwendet werden soll.

   Das Standardprotokoll ist HTTPS.

b. Geben Sie den Serverhostnamen oder die IP-Adresse des Cloud-Speicherpools ein.

   Beispiel:

   `s3-aws-region.amazonaws.com`

   > Geben Sie den Bucket-Namen nicht in dieses Feld ein. Sie fügen den Bucket-Namen in das Feld **Bucket oder Container** ein.

a. Geben Sie optional den Port an, der bei der Verbindung mit dem Cloud Storage Pool verwendet werden soll.

   Lassen Sie dieses Feld leer, um den Standardport Port 443 für HTTPS oder Port 80 für HTTP zu verwenden.

b. Wählen Sie den URL-Stil für den Cloud Storage Pool Bucket aus:

Option	Beschreibung
Virtual Hosted-Style	Verwenden Sie eine virtuelle gehostete URL, um auf den Bucket zuzugreifen. Virtuelle URLs im gehosteten Stil enthalten beispielsweise den Bucket-Namen als Teil des Domain-Namens `https://bucket-name.s3.company.com/key-name`.
Pfadstil	Verwenden Sie eine URL im Pfadstil, um auf den Bucket zuzugreifen. URLs im Pfadstil enthalten beispielsweise den Bucket-Namen am Ende `https://s3.company.com/bucket-name/key-name`. **Hinweis:** die URL im Pfadstil wird veraltet.
Automatische Erkennung	Versuchen Sie, basierend auf den bereitgestellten Informationen automatisch zu erkennen, welchen URL-Stil verwendet werden soll. Wenn Sie beispielsweise eine IP-Adresse angeben, verwendet StorageGRID eine URL im Pfadstil. Wählen Sie diese Option nur aus, wenn Sie nicht wissen, welcher Stil verwendet werden soll.

2. Wählen Sie im Abschnitt **Authentifizierung** den Authentifizierungstyp aus, der für den Cloud-Storage-Pool-Endpunkt erforderlich ist.

Option	Beschreibung
Zugriffsschlüssel	Für den Zugriff auf den Cloud Storage Pool-Bucket sind eine Zugriffsschlüssel-ID und ein geheimer Zugriffsschlüssel erforderlich.

Option	Beschreibung
Anonym	Jeder hat Zugriff auf den Cloud-Storage-Pool-Bucket. Eine Zugriffsschlüssel-ID und ein geheimer Zugriffsschlüssel sind nicht erforderlich.
KAPPE (C2S-Zugangsportal)	Wird nur für C2S S3 verwendet. Gehen Sie zu C2S S3: Angeben von Authentifizierungsdetails für einen Cloud-Storage-Pool.

3. Wenn Sie den Zugriffsschlüssel ausgewählt haben, geben Sie die folgenden Informationen ein:

Option	Beschreibung
Zugriffsschlüssel-ID	Zugriffsschlüssel-ID für das Konto, das den externen Bucket besitzt
Geheimer Zugriffsschlüssel	Der zugehörige Schlüssel für den geheimen Zugriff.

4. Wählen Sie im Abschnitt Server Verification die Methode aus, mit der das Zertifikat für TLS-Verbindungen zum Cloud Storage Pool validiert werden soll:

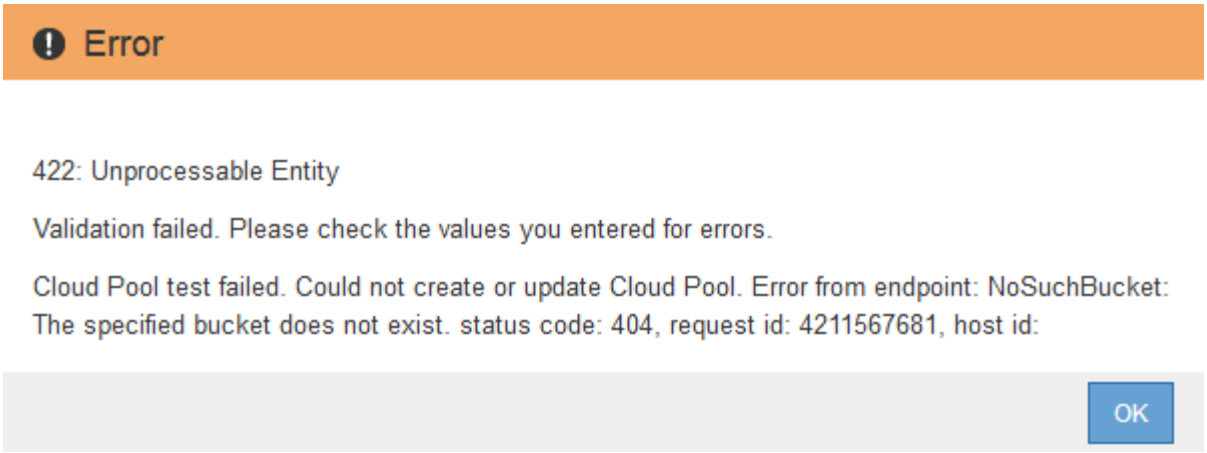
Option	Beschreibung
Verwenden Sie das CA-Zertifikat für das Betriebssystem	Verwenden Sie die auf dem Betriebssystem installierten Standard-Grid-CA-Zertifikate, um Verbindungen zu sichern.
Benutzerdefiniertes CA-Zertifikat verwenden	Verwenden Sie ein benutzerdefiniertes CA-Zertifikat. Wählen Sie **Select New** aus, und laden Sie das PEM-codierte CA-Zertifikat hoch.
Verifizieren Sie das Zertifikat nicht	Das für die TLS-Verbindung verwendete Zertifikat wird nicht verifiziert.

5. Wählen Sie **Speichern**.

Beim Speichern eines Cloud-Speicherpools führt StorageGRID Folgendes aus:

- Überprüft, ob der Bucket und der Service-Endpunkt vorhanden sind und ob sie mit den von Ihnen angegebenen Zugangsdaten erreicht werden können.
- Schreibt eine Markierungsdatei in den Bucket, um den Bucket als Cloud-Storage-Pool zu identifizieren. Entfernen Sie niemals diese Datei, die benannt ist `x-ntap-sgws-cloud-pool-uuid`.

Wenn die Validierung des Cloud-Storage-Pools fehlschlägt, erhalten Sie eine Fehlermeldung, die erklärt, warum die Validierung fehlgeschlagen ist. Möglicherweise wird ein Fehler gemeldet, wenn ein Zertifikatfehler vorliegt oder der angegebene Bucket nicht bereits vorhanden ist.



Siehe Anweisungen für Fehlerbehebung bei Cloud Storage Pools, Beheben Sie das Problem, und versuchen Sie dann erneut, den Cloud-Speicher-Pool zu speichern.

C2S S3: Geben Sie die Authentifizierungsdetails für einen Cloud-Storage-Pool an

Wenn Sie den S3-Service (Commercial Cloud Services, C2S) als Cloud-Storage-Pool verwenden möchten, müssen Sie C2S Access Portal (CAP) als Authentifizierungstyp konfigurieren, damit StorageGRID temporäre Anmeldedaten für den Zugriff auf den S3-Bucket in Ihrem C2S-Konto anfordern kann.

Was Sie benötigen

- Sie haben die Basisinformationen für einen Amazon S3 Cloud-Storage-Pool eingegeben, einschließlich des Service-Endpunkts.
- Sie kennen die vollständige URL, mit der StorageGRID temporäre Anmeldedaten vom CAP-Server erhalten wird, einschließlich aller erforderlichen und optionalen API-Parameter, die Ihrem C2S-Konto zugewiesen sind.
- Sie haben ein Server-CA-Zertifikat, das von einer entsprechenden Behörde ausgestellt wurde. StorageGRID verwendet dieses Zertifikat, um die Identität des CAP-Servers zu überprüfen. Das Server-CA-Zertifikat muss die PEM-Kodierung verwenden.
- Sie haben ein Clientzertifikat, das von einer entsprechenden Behörde ausgestellt wurde. StorageGRID verwendet dieses Zertifikat zur Identität des CAP-Servers. Das Clientzertifikat muss PEM-Kodierung verwenden und Zugriff auf Ihr C2S-Konto haben.
- Sie haben einen PEM-kodierten privaten Schlüssel für das Clientzertifikat.
- Wenn der private Schlüssel für das Clientzertifikat verschlüsselt ist, haben Sie die Passphrase zum Entschlüsseln.

Schritte

1. Wählen Sie im Abschnitt **Authentifizierung** im Dropdown-Menü **Authentifizierungstyp** die Option **CAP (C2S Access Portal)** aus.

   Die C2S-Authentifizierungsfelder werden angezeigt.

Create Cloud Storage Pool

Display Name: C2S Cloud Storage Pool

Provider Type: Amazon S3

Bucket or Container: my-c2s-bucket

Service Endpoint

Protocol: HTTP HTTPS

Hostname: s3-aws-region.amazonaws.com

Port (optional): 443

URL Style: Auto-Detect

Authentication

Authentication Type: CAP (C2S Access Portal)

Temporary Credentials URL: https://example.com/CAP/api/v1/cred

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. Geben Sie die folgenden Informationen an:
   a. Geben Sie unter **URL für temporäre Anmeldeinformationen** die vollständige URL ein, die StorageGRID zum Abrufen temporärer Anmeldeinformationen vom CAP-Server verwendet, einschließlich aller erforderlichen und optionalen API-Parameter, die Ihrem C2S-Konto zugewiesen sind.
   b. Wählen Sie für **Server CA-Zertifikat Wählen Sie Neu** aus, und laden Sie das PEM-codierte CA-Zertifikat hoch, das StorageGRID zur Überprüfung des CAP-Servers verwendet.
   c. Wählen Sie für **Clientzertifikat Wählen Sie Neu** aus, und laden Sie das PEM-kodierte Zertifikat, das StorageGRID zur Identifizierung verwendet, auf den CAP-Server hoch.
   d. Wählen Sie für **Client Private Key Select New** aus, und laden Sie den PEM-kodierten privaten Schlüssel für das Clientzertifikat hoch.

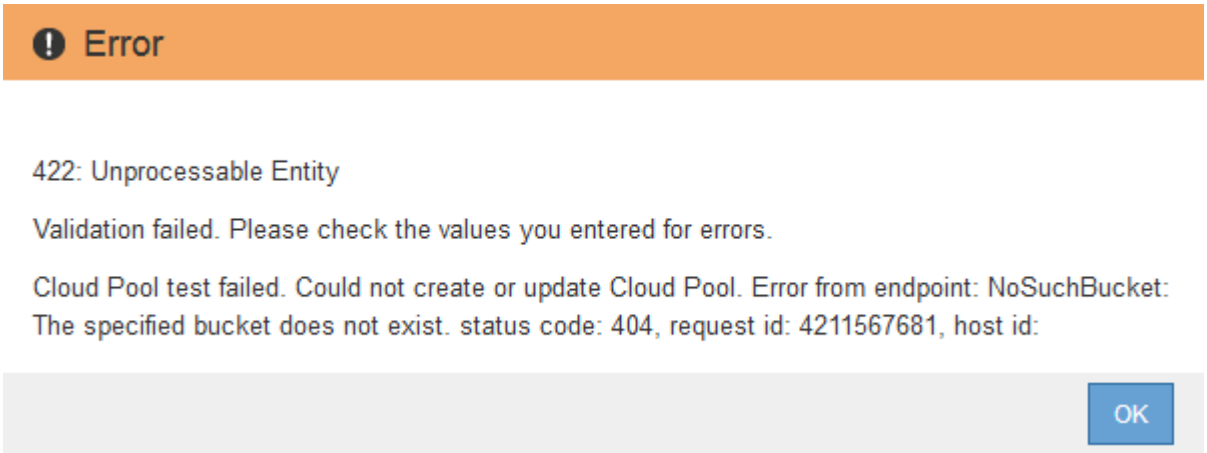
      Wenn der private Schlüssel verschlüsselt ist, muss das traditionelle Format verwendet werden. (Das verschlüsselte PKCS #8-Format wird nicht unterstützt.)

   e. Wenn der private Clientschlüssel verschlüsselt ist, geben Sie die Passphrase zum Entschlüsseln des privaten Clientschlüssels ein. Andernfalls lassen Sie das Feld **Client Private Key Passphrase** leer.
3. Geben Sie im Abschnitt Server-Überprüfung folgende Informationen an:
   a. Wählen Sie für **Zertifikatvalidierung** * Benutzerdefiniertes CA-Zertifikat verwenden* aus.
   b. Wählen Sie **Select New** aus, und laden Sie das PEM-codierte CA-Zertifikat hoch.
4. Wählen Sie **Speichern**.

Beim Speichern eines Cloud-Speicherpools führt StorageGRID Folgendes aus:

- Überprüft, ob der Bucket und der Service-Endpunkt vorhanden sind und ob sie mit den von Ihnen angegebenen Zugangsdaten erreicht werden können.
- Schreibt eine Markierungsdatei in den Bucket, um den Bucket als Cloud-Storage-Pool zu identifizieren. Entfernen Sie niemals diese Datei, die benannt ist `x-ntap-sgws-cloud-pool-uuid`.

Wenn die Validierung des Cloud-Storage-Pools fehlschlägt, erhalten Sie eine Fehlermeldung, die erklärt, warum die Validierung fehlgeschlagen ist. Möglicherweise wird ein Fehler gemeldet, wenn ein Zertifikatfehler vorliegt oder der angegebene Bucket nicht bereits vorhanden ist.



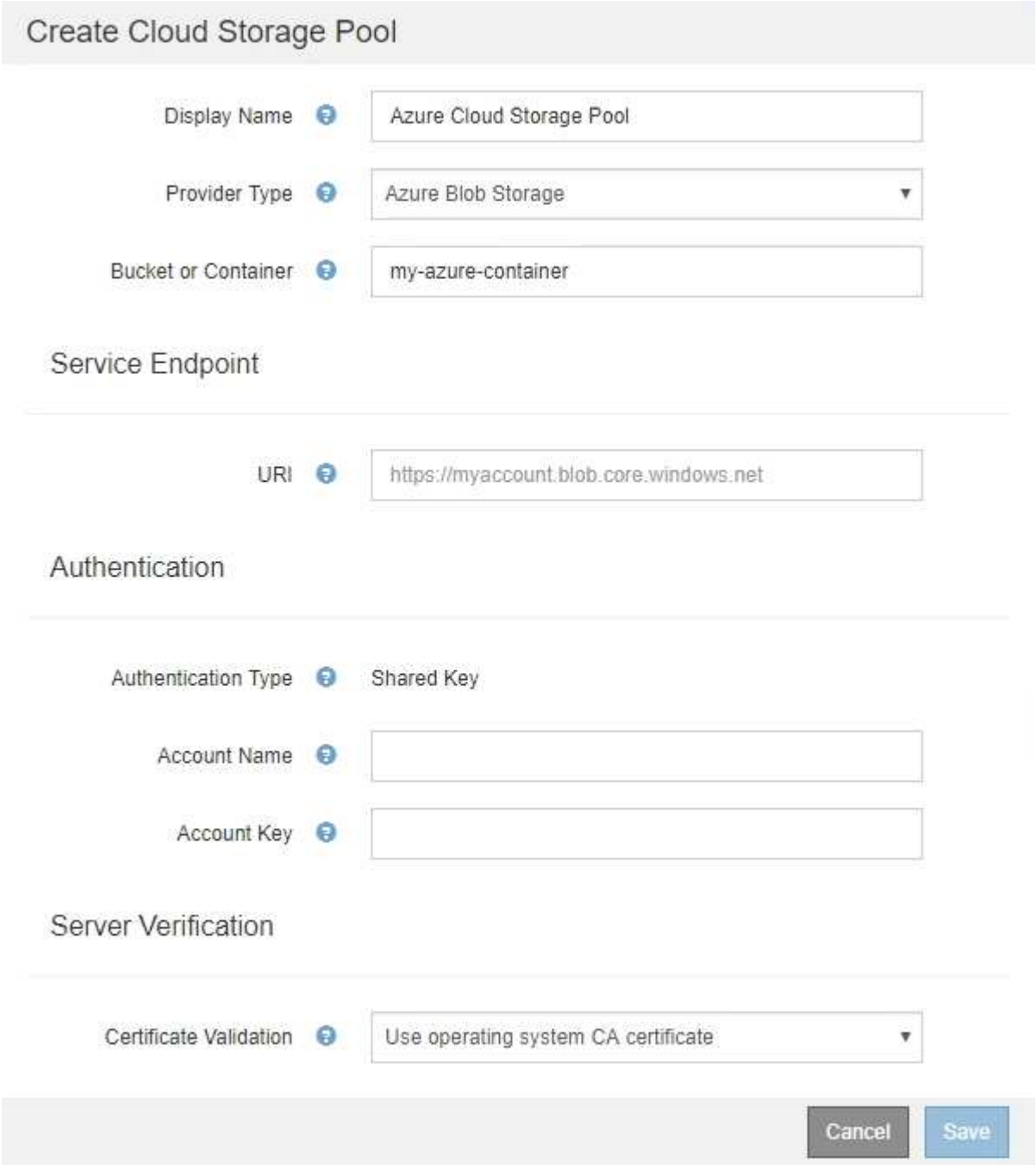
Siehe Anweisungen für Fehlerbehebung bei Cloud Storage Pools, Beheben Sie das Problem, und versuchen Sie dann erneut, den Cloud-Speicher-Pool zu speichern.

Azure: Geben Sie die Authentifizierungsdetails für einen Cloud Storage-Pool an

Wenn Sie einen Cloud Storage Pool für Azure Blob Storage erstellen, müssen Sie einen Kontonamen und Kontoschlüssel für den externen Container angeben, den StorageGRID zum Speichern von Objekten verwendet.

Was Sie benötigen

- Sie haben die Basisinformationen für den Cloud Storage Pool eingegeben und als Provider-Typ **Azure Blob Storage** angegeben. **Gemeinsamer Schlüssel** wird im Feld **Authentifizierungstyp** angezeigt.



- Sie kennen den Uniform Resource Identifier (URI) für den Zugriff auf den Blob-Storage-Container, der für den Cloud Storage Pool verwendet wird.

- Sie kennen den Namen des Speicherkontos und den geheimen Schlüssel. Im Azure-Portal finden Sie diese Werte.

Schritte

1. Geben Sie im Abschnitt **Service Endpoint** den Uniform Resource Identifier (URI) ein, der für den Zugriff auf den Blob-Storage-Container verwendet wird, der für den Cloud-Storage-Pool verwendet wird.

   Geben Sie den URI in einem der folgenden Formate an:

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

   Wenn Sie keinen Port angeben, wird standardmäßig der Port 443 für HTTPS-URIs verwendet, und Port 80 wird für HTTP-URIs verwendet. + * Beispiel-URI für Azure Blob Storage-Container*: `https://myaccount.blob.core.windows.net`

2. Geben Sie im Abschnitt **Authentifizierung** folgende Informationen an:

   a. Geben Sie für **Kontoname** den Namen des Blob-Speicherkontos ein, der den externen Service-Container besitzt.

   b. Geben Sie für **Kontenschlüssel** den geheimen Schlüssel für das Blob-Speicherkonto ein.

   > Für Azure-Endpunkte ist die Authentifizierung mit gemeinsamem Schlüssel erforderlich.

3. Wählen Sie im Abschnitt **Server Verification** die Methode aus, mit der das Zertifikat für TLS-Verbindungen zum Cloud-Speicherpool validiert werden soll:

Option	Beschreibung
Verwenden Sie das CA-Zertifikat für das Betriebssystem	Verwenden Sie zum Sichern der Verbindungen die auf dem Betriebssystem installierten Grid CA-Zertifikate.
Benutzerdefiniertes CA-Zertifikat verwenden	Verwenden Sie ein benutzerdefiniertes CA-Zertifikat. Wählen Sie **Select New** aus, und laden Sie das PEM-codierte Zertifikat hoch.
Verifizieren Sie das Zertifikat nicht	Das für die TLS-Verbindung verwendete Zertifikat wird nicht verifiziert.

4. Wählen Sie **Speichern**.

Beim Speichern eines Cloud-Speicherpools führt StorageGRID Folgendes aus:

- Überprüft, ob der Container und die URI vorhanden sind und ob sie mit den von Ihnen angegebenen Zugangsdaten erreicht werden können.
- Schreibt eine Markierungsdatei in den Container, um sie als Cloud-Storage-Pool zu identifizieren. Entfernen Sie niemals diese Datei, die benannt ist `x-ntap-sgws-cloud-pool-uuid`.

Wenn die Validierung des Cloud-Storage-Pools fehlschlägt, erhalten Sie eine Fehlermeldung, die erklärt, warum die Validierung fehlgeschlagen ist. Möglicherweise wird ein Fehler gemeldet, wenn ein Zertifikatfehler vorliegt oder der angegebene Container nicht bereits vorhanden ist.

Siehe Anweisungen für Fehlerbehebung bei Cloud Storage Pools, Beheben Sie das Problem, und versuchen Sie dann erneut, den Cloud-Speicher-Pool zu speichern.

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.