



Create Cloud Storage Pool

StorageGRID

NetApp
July 18, 2022

This PDF was generated from <https://docs.netapp.com/us-en/storagegrid-116/ilm/s3-authentication-details-for-cloud-storage-pool.html> on July 18, 2022. Always check docs.netapp.com for the latest.

Table of Contents

- Create a Cloud Storage Pool 1
 - S3: Specifying authentication details for a Cloud Storage Pool 2
 - C2S S3: Specify authentication details for a Cloud Storage Pool 6
 - Azure: Specify authentication details for a Cloud Storage Pool 9

Create a Cloud Storage Pool

When you create a Cloud Storage Pool, you specify the name and location of the external bucket or container that StorageGRID will use to store objects, the cloud provider type (Amazon S3 or Azure Blob Storage), and the information StorageGRID needs to access the external bucket or container.

What you'll need

- You are signed in to the Grid Manager using a [supported web browser](#).
- You have specific access permissions.
- You have reviewed the guidelines for configuring Cloud Storage Pools.
- The external bucket or container referenced by the Cloud Storage Pool already exists.
- You have all of the authentication information needed to access the bucket or container.

About this task

A Cloud Storage Pool specifies a single external S3 bucket or Azure Blob storage container. StorageGRID validates the Cloud Storage Pool as soon as you save it, so you must ensure that the bucket or container specified in the Cloud Storage Pool exists and is reachable.

Steps

1. Select **ILM > Storage pools**.

The Storage Pools page appears. This page includes two sections: Storage Pools and Cloud Storage Pools.

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. In the Cloud Storage Pools section of the page, select **Create**.

The Create Cloud Storage Pool dialog box appears.

Create Cloud Storage Pool

Display Name ?

Provider Type ?

Bucket or Container ?

Cancel

Save

3. Enter the following information:

Field	Description
Display Name	A name that briefly describes the Cloud Storage Pool and its purpose. Use a name that will be easy to identify when you configure ILM rules.
Provider Type	Which cloud provider you will use for this Cloud Storage Pool: <ul style="list-style-type: none"> • Amazon S3: Select this option for an S3, C2S S3, or Google Cloud Platform (GCP) endpoint. • Azure Blob Storage <p>Note: When you select a Provider Type, the Service Endpoint, Authentication and Server Verification sections appear at the bottom on the page.</p>
Bucket or Container	The name of the external S3 bucket or Azure container that was created for the Cloud Storage Pool. The name you specify here must exactly match the bucket or container's name or Cloud Storage Pool creation will fail. You cannot change this value after the Cloud Storage Pool is saved.

4. Complete the Service Endpoint, Authentication and Server Verification sections of the page, based on the selected provider type.
- [S3: Specify authentication details for a Cloud Storage Pool](#)
 - [C2S S3: Specify authentication details for a Cloud Storage Pool](#)
 - [Azure: Specify authentication details for a Cloud Storage Pool](#)

S3: Specifying authentication details for a Cloud Storage Pool

When you create a Cloud Storage Pool for S3, you must select the type of authentication that is required for the Cloud Storage Pool endpoint. You can specify Anonymous or enter an Access Key ID and Secret Access Key.

What you'll need

- You have entered the basic information for the Cloud Storage Pool and specified **Amazon S3** as the provider type.

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 ?

example.com or 0.0.0.0

Port (optional) ?

443

URL Style ?

Auto-Detect ▼

Authentication

Authentication Type ?

Server Verification

Certificate Validation ?

Use operating system CA certificate ▼

Cancel

Save

- If you are using access key authentication, you know the Access Key ID and Secret Access Key for the

external S3 bucket.

Steps

1. In the **Service Endpoint** section, provide the following information:

- a. Select which protocol to use when connecting to the Cloud Storage Pool.

The default protocol is HTTPS.

- b. Enter the server hostname or IP address of the Cloud Storage Pool.

For example:

`s3-aws-region.amazonaws.com`



Do not include the bucket name in this field. You include the bucket name in the **Bucket** or **Container** field.

- c. Optionally, specify the port that should be used when connecting to the Cloud Storage Pool.

Leave this field blank to use the default port: port 443 for HTTPS or port 80 for HTTP.

- d. Select the URL style for the Cloud Storage Pool bucket:

Option	Description
Virtual Hosted-Style	Use a virtual hosted-style URL to access the bucket. Virtual hosted-style URLs include the bucket name as part of the domain name, for example <code>https://bucket-name.s3.company.com/key-name</code> .
Path-Style	Use a path-style URL to access the bucket. Path-style URLs include the bucket name at the end, for example <code>https://s3.company.com/bucket-name/key-name</code> . Note: The path-style URL is being deprecated.
Auto-Detect	Attempt to automatically detect which URL style to use, based on the information provided. For example, if you specify an IP address, StorageGRID will use a path-style URL. Select this option only if you don't know which specific style to use.

2. In the **Authentication** section, select the type of authentication that is required for the Cloud Storage Pool endpoint.

Option	Description
Access Key	An Access Key ID and Secret Access Key are required to access the Cloud Storage Pool bucket.
Anonymous	Everyone has access to the Cloud Storage Pool bucket. An Access Key ID and Secret Access Key are not required.

Option	Description
CAP (C2S Access Portal)	Used for C2S S3 only. Go to C2S S3: Specifying authentication details for a Cloud Storage Pool .

3. If you selected Access Key, enter the following information:

Option	Description
Access Key ID	The Access Key ID for the account that owns the external bucket.
Secret Access Key	The associated Secret Access Key.

4. In the Server Verification section, select which method should be used to validate the certificate for TLS connections to the Cloud Storage Pool:

Option	Description
Use operating system CA certificate	Use the default Grid CA certificates installed on the operating system to secure connections.
Use custom CA certificate	Use a custom CA certificate. Select Select New , and upload the PEM-encoded CA certificate.
Do not verify certificate	The certificate used for the TLS connection is not verified.

5. Select **Save**.

When you save a Cloud Storage Pool, StorageGRID does the following:

- Validates that the bucket and the service endpoint exist and that they can be reached using the credentials that you specified.
- Writes a marker file to the bucket to identify the bucket as a Cloud Storage Pool. Never remove this file, which is named `x-ntap-sgws-cloud-pool-uuid`.

If Cloud Storage Pool validation fails, you receive an error message that explains why validation failed. For example, an error might be reported if there is a certificate error or if the bucket you specified does not already exist.

! 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

See the instructions for [troubleshooting Cloud Storage Pools](#), resolve the issue, and then try saving the Cloud Storage Pool again.

C2S S3: Specify authentication details for a Cloud Storage Pool

To use the Commercial Cloud Services (C2S) S3 service as a Cloud Storage Pool, you must configure C2S Access Portal (CAP) as the authentication type, so that StorageGRID can request temporary credentials to access the S3 bucket in your C2S account.

What you'll need

- You have entered the basic information for an Amazon S3 Cloud Storage Pool, including the service endpoint.
- You know the complete URL that StorageGRID will use to obtain temporary credentials from the CAP server, including all the required and optional API parameters assigned to your C2S account.
- You have a server CA certificate issued by an appropriate Government Certificate Authority (CA). StorageGRID uses this certificate to verify the identity of the CAP server. The server CA certificate must use PEM encoding.
- You have a client certificate issued by an appropriate Government Certificate Authority (CA). StorageGRID uses this certificate to identify itself to the CAP server. The client certificate must use PEM encoding and must have been granted access to your C2S account.
- You have a PEM-encoded private key for the client certificate.
- If the private key for the client certificate is encrypted, you have the passphrase for decrypting it.

Steps


1. In the **Authentication** section, select **CAP (C2S Access Portal)** from the **Authentication Type** drop-down.

The CAP C2S authentication fields appear.

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. Provide the following information:

- a. For **Temporary Credentials URL**, enter the complete URL that StorageGRID will use to obtain temporary credentials from the CAP server, including all the required and optional API parameters assigned to your C2S account.
- b. For **Server CA Certificate**, select **Select New**, and upload the PEM-encoded CA certificate that StorageGRID will use to verify the CAP server.
- c. For **Client Certificate**, select **Select New**, and upload the PEM-encoded certificate that StorageGRID will use to identify itself to the CAP server.
- d. For **Client Private Key**, select **Select New**, and upload the PEM-encoded private key for the client certificate.

If the private key is encrypted, the traditional format must be used. (PKCS #8 encrypted format is not supported.)

- e. If the client private key is encrypted, enter the passphrase for decrypting the client private key. Otherwise, leave the **Client Private Key Passphrase** field blank.

3. In the Server Verification section, provide the following information:

- a. For **Certificate Validation**, select **Use custom CA certificate**.
- b. Select **Select New**, and upload the PEM-encoded CA certificate.

4. Select **Save**.

When you save a Cloud Storage Pool, StorageGRID does the following:

- Validates that the bucket and the service endpoint exist and that they can be reached using the credentials that you specified.
- Writes a marker file to the bucket to identify the bucket as a Cloud Storage Pool. Never remove this file, which is named `x-ntap-sgws-cloud-pool-uuid`.

If Cloud Storage Pool validation fails, you receive an error message that explains why validation failed. For example, an error might be reported if there is a certificate error or if the bucket you specified does not already exist.

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

See the instructions for [troubleshooting Cloud Storage Pools](#), resolve the issue, and then try saving the Cloud Storage Pool again.

Azure: Specify authentication details for a Cloud Storage Pool

When you create a Cloud Storage Pool for Azure Blob storage, you must specify an account name and account key for the external container that StorageGRID will use to store objects.

What you'll need

- You have entered the basic information for the Cloud Storage Pool and specified **Azure Blob Storage** as the provider type. **Shared Key** appears in the **Authentication Type** field.

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

- You know the Uniform Resource Identifier (URI) used to access the Blob storage container used for the Cloud Storage Pool.

- You know the name of the storage account and the secret key. You can use the Azure portal to find these values.

Steps

1. In the **Service Endpoint** section, enter the Uniform Resource Identifier (URI) used to access the Blob storage container used for the Cloud Storage Pool.

Specify the URI in one of the following formats:

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

If you do not specify a port, by default port 443 is used for HTTPS URIs and port 80 is used for HTTP URIs.

Example URI for Azure Blob storage container:

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

2. In the **Authentication** section, provide the following information:
 - a. For **Account Name**, enter the name of the Blob storage account that owns the external service container.
 - b. For **Account Key**, enter the secret key for the Blob storage account.



For Azure endpoints, you must use Shared Key authentication.

3. In the **Server Verification** section, select which method should be used to validate the certificate for TLS connections to the Cloud Storage Pool:

Option	Description
Use operating system CA certificate	Use the Grid CA certificates installed on the operating system to secure connections.
Use custom CA certificate	Use a custom CA certificate. Select Select New , and upload the PEM-encoded certificate.
Do not verify certificate	The certificate used for the TLS connection is not verified.

4. Select **Save**.

When you save a Cloud Storage Pool, StorageGRID does the following:

- Validates that the container and the URI exist and that they can be reached using the credentials that you specified.
- Writes a marker file to the container to identify it as a Cloud Storage Pool. Never remove this file, which is named `x-ntap-sgws-cloud-pool-uuid`.

If Cloud Storage Pool validation fails, you receive an error message that explains why validation failed. For example, an error might be reported if there is a certificate error or if the container you specified does not already exist.

See the instructions for [troubleshooting Cloud Storage Pools](#), resolve the issue, and then try saving the Cloud Storage Pool again.

Copyright Information

Copyright © 2022 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system- without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.