Creating a Cloud Storage Pool

StorageGRID 11.5

NetApp
January 04, 2024

Table of Contents

Creating 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 must be signed in to the Grid Manager using a supported browser.
- You must have specific access permissions.
- You must have reviewed the guidelines for configuring Cloud Storage Pools.
- The external bucket or container referenced by the Cloud Storage Pool must exist.
- You must have all of the authentication information needed to access the bucket or container.

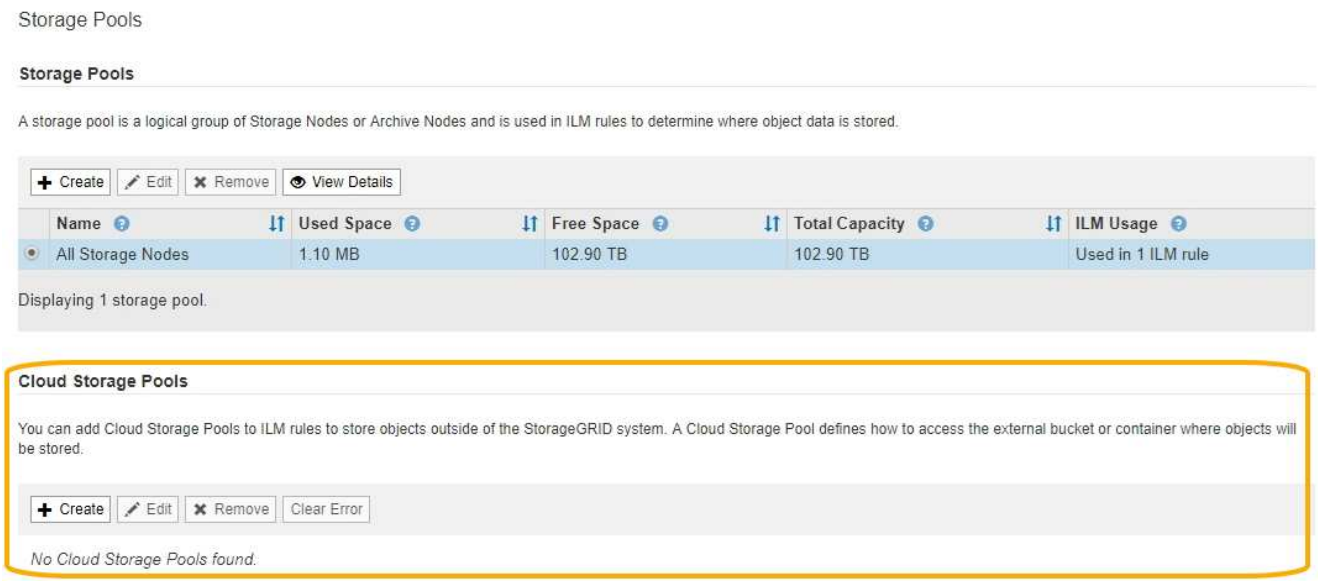
About this task

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.



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

   The Create Cloud Storage Pool dialog box appears.

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: • Amazon S3 (select this option for an S3 or C2S S3 Cloud Storage Pool) • Azure Blob Storage **Note:** When you select a Provider Type, the Service Endpoint, Authentication and Server Verification sections appear at the bottom on the page.
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.

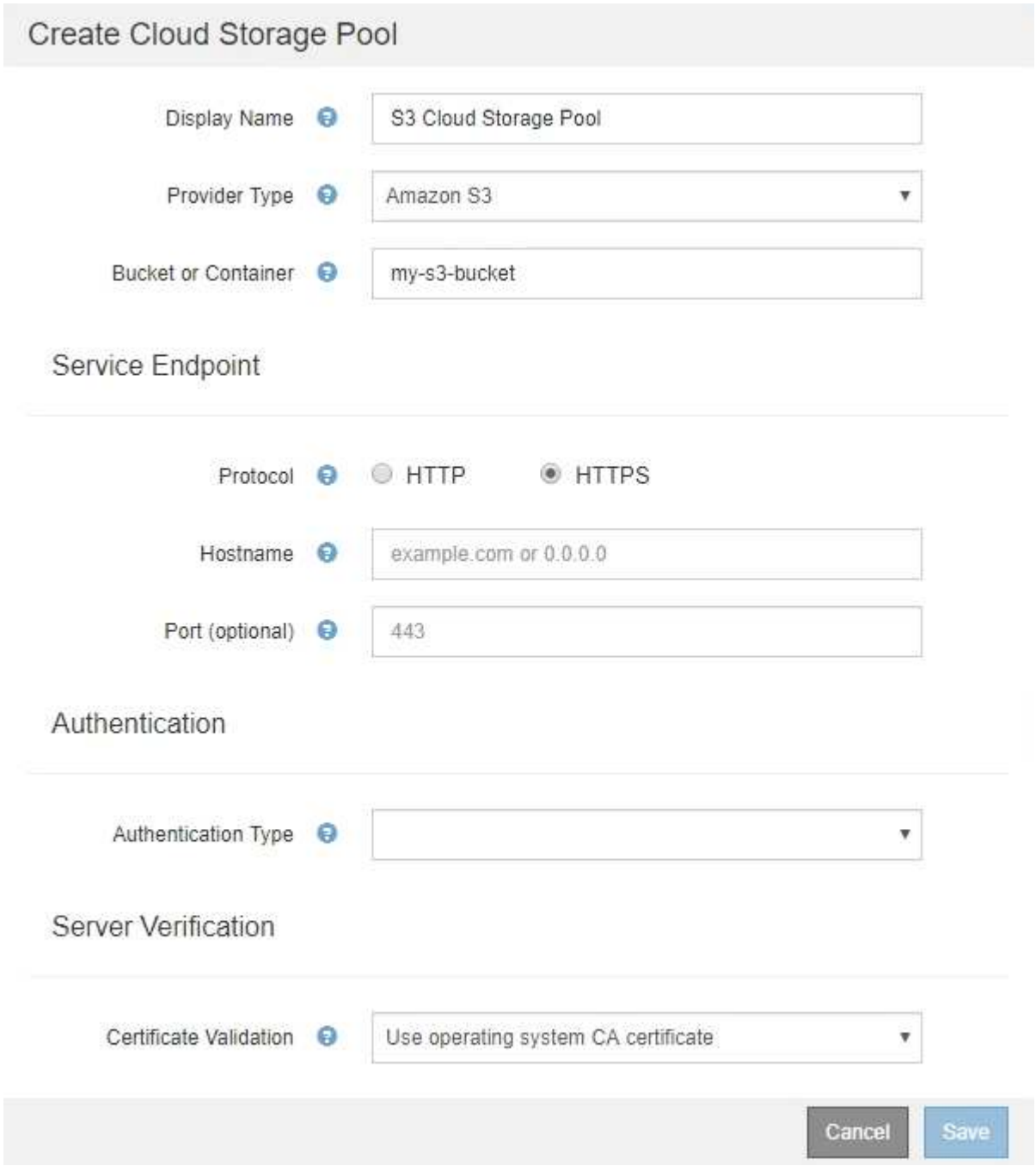
4. Complete the Service Endpoint, Authentication and Server Verification sections of the page, based on the selected provider type.
   - S3: Specifying authentication details for a Cloud Storage Pool
   - C2S S3: Specifying authentication details for a Cloud Storage Pool
   - Azure: Specifying authentication 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 must have entered the basic information for the Cloud Storage Pool and specified **Amazon S3** as the provider type.



- If you are using access key authentication, you must 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.

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.
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:

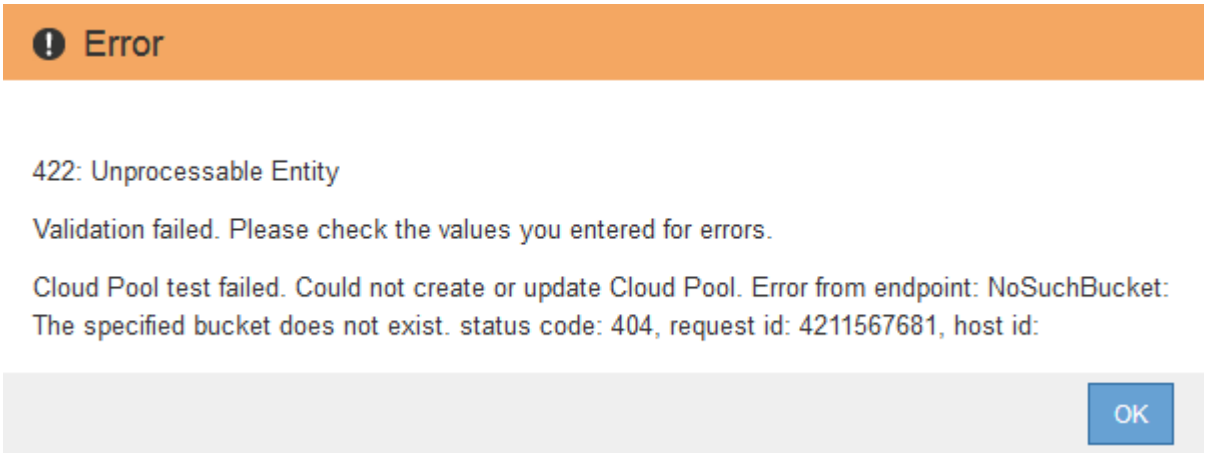
Option	Description
Use operating system CA certificate	Use the default CA certificates installed on the operating system to secure connections.
Use custom CA certificate	Use a custom CA certificate. Click **Select New**, and upload the PEM-encoded CA certificate.
Do not verify certificate	The certificate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

5. Click **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.



See the instructions for troubleshooting Cloud Storage Pools, resolve the issue, and then try saving the Cloud Storage Pool again.

Related information

Troubleshooting Cloud Storage Pools

C2S S3: Specifying 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

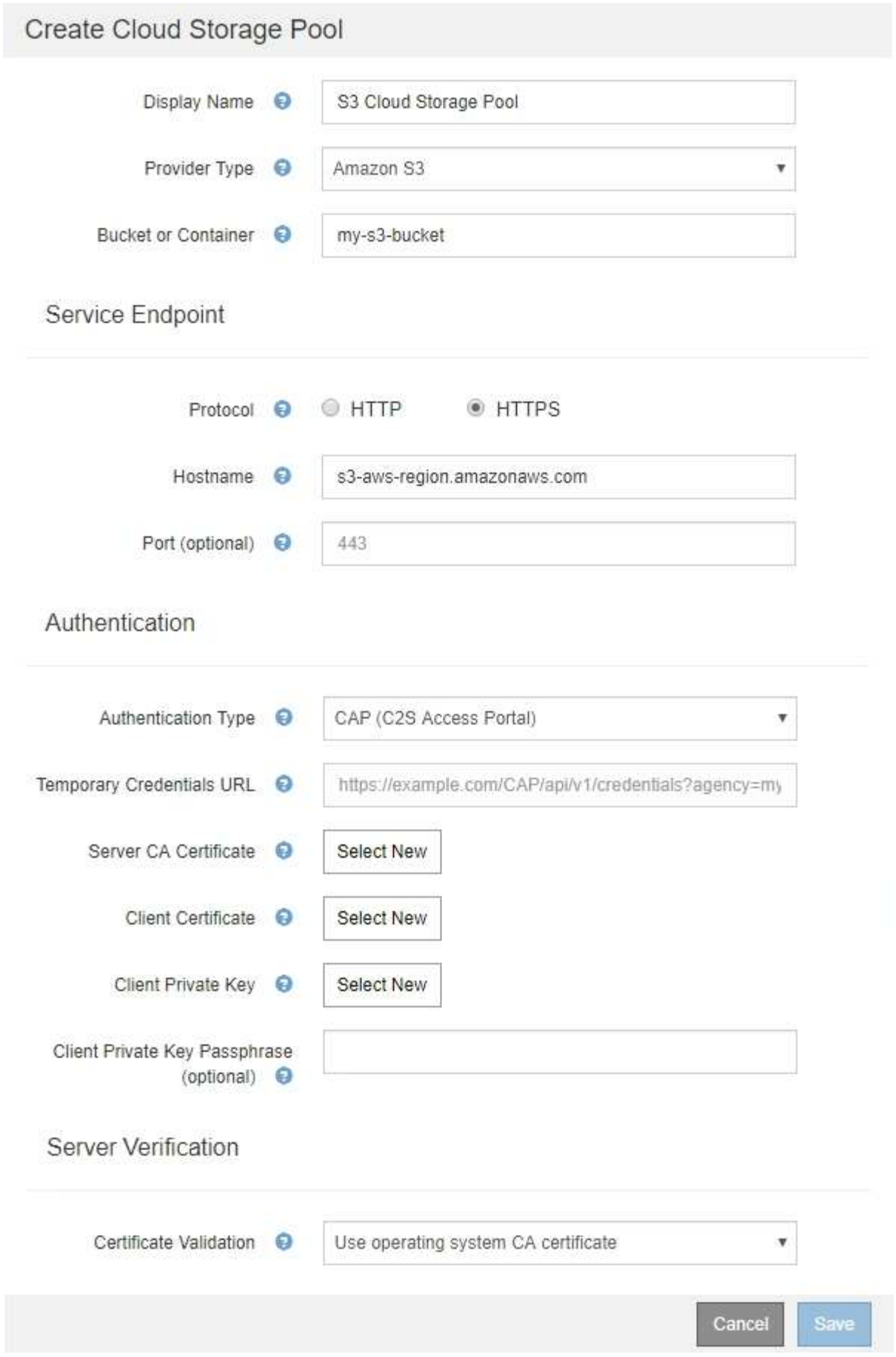
- You must have entered the basic information for an Amazon S3 Cloud Storage Pool, including the service endpoint.
- You must know the complete URL that StorageGRID will use to obtain temporary credentials from the CAP server, including all the required and optional API parameters assigned to your C2S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

- If the private key for the client certificate is encrypted, you must 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
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. 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**, click **Select New**, and upload the PEM-encoded CA certificate that StorageGRID will use to verify the CAP server.
    c. For **Client Certificate**, click **Select New**, and upload the PEM-encoded certificate that StorageGRID will use to identify itself to the CAP server.
    d. For **Client Private Key**, click **Select New**, and upload the PEM-encoded private key for the client certificate.

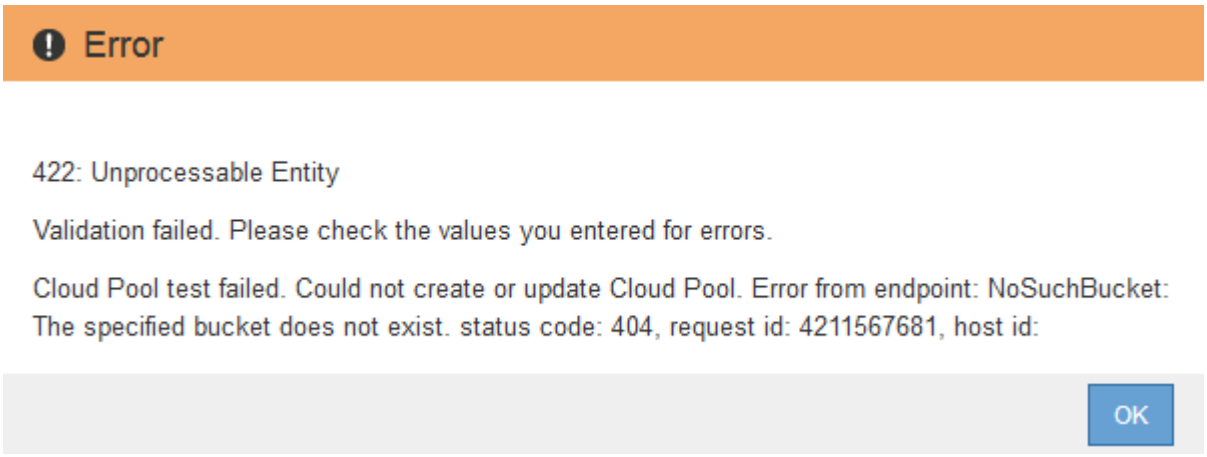
        If the private key is encrypted, the traditional format must be used. (PKCS #8 encrypted format is not supported.)

    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. Click **Select New**, and upload the PEM-encoded CA certificate.
4. Click **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.



See the instructions for troubleshooting Cloud Storage Pools, resolve the issue, and then try saving the Cloud Storage Pool again.

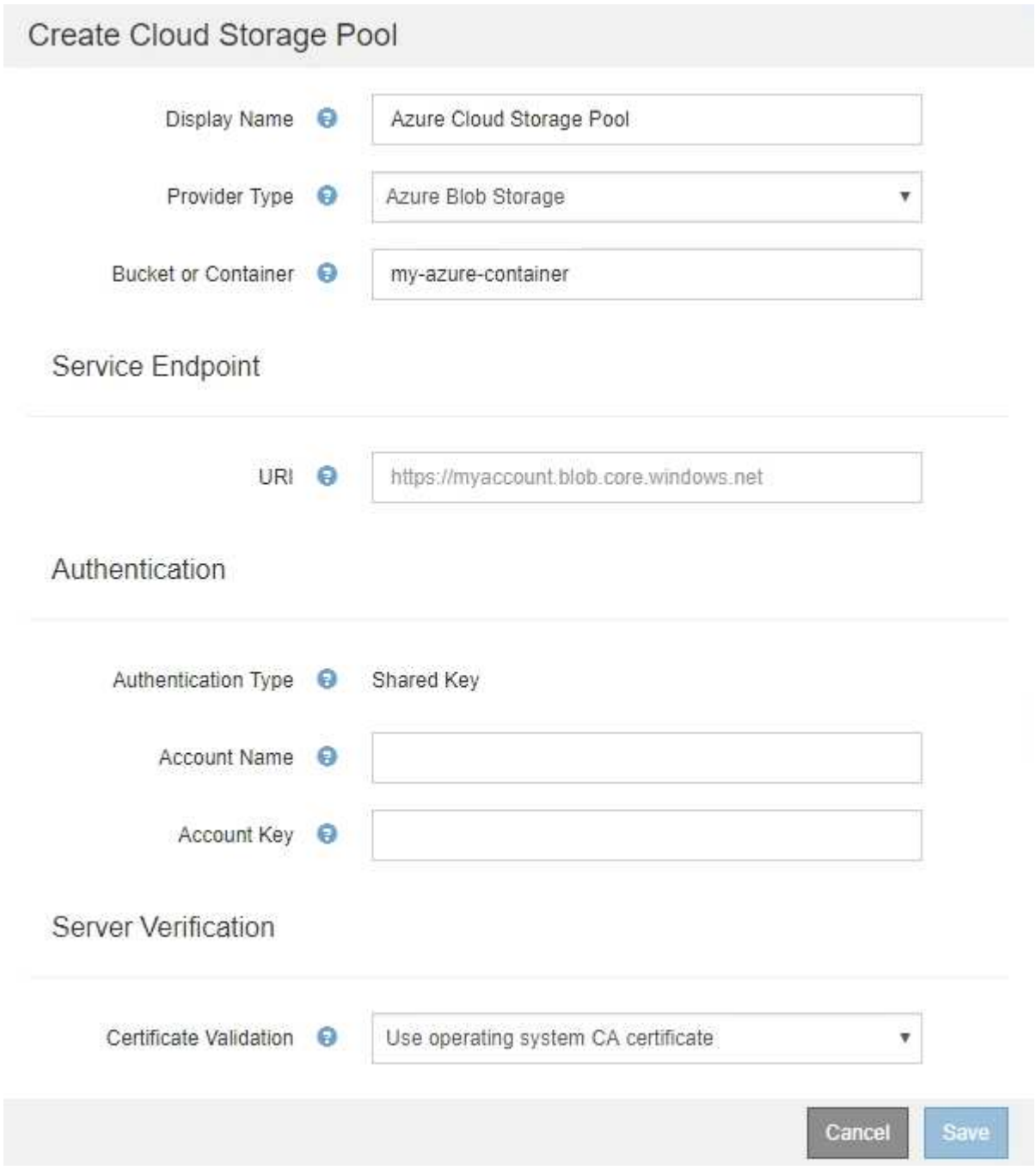
Related information

Azure: Specifying 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 must 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.



- You must know the Uniform Resource Identifier (URI) used to access the Blob storage container used for the Cloud Storage Pool.
- You must 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 default CA certificates installed on the operating system to secure connections.
Use custom CA certificate	Use a custom CA certificate. Click **Select New**, and upload the PEM-encoded certificate.
Do not verify certificate	The certificate used for the TLS connection is not verified.

4. Click **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.

Related information

Troubleshooting Cloud Storage Pools

Copyright information

Trademark information