クラウドストレージプールを作成
StorageGRID

NetApp
April 10, 2024

目次

クラウドストレージプールを作成

クラウドストレージプールを作成 StorageGRID する際には、 StorageGRID がオブジェクトの格納に使用する外部バケットまたはコンテナの名前と場所、クラウドプロバイダのタイプ（ Amazon S3 または Azure Blob Storage ）、および外部のバケットまたはコンテナにアクセスするために必要な情報を指定します。

必要なもの

- を使用して Grid Manager にサインインします サポートされている Web ブラウザ。
- 特定のアクセス権限が必要です。
- クラウドストレージプールの設定に関するガイドラインを確認しておく必要があります。
- クラウドストレージプールに参照されている外部のバケットまたはコンテナがすでに存在します。
- バケットまたはコンテナへのアクセスに必要なすべての認証情報が必要です。

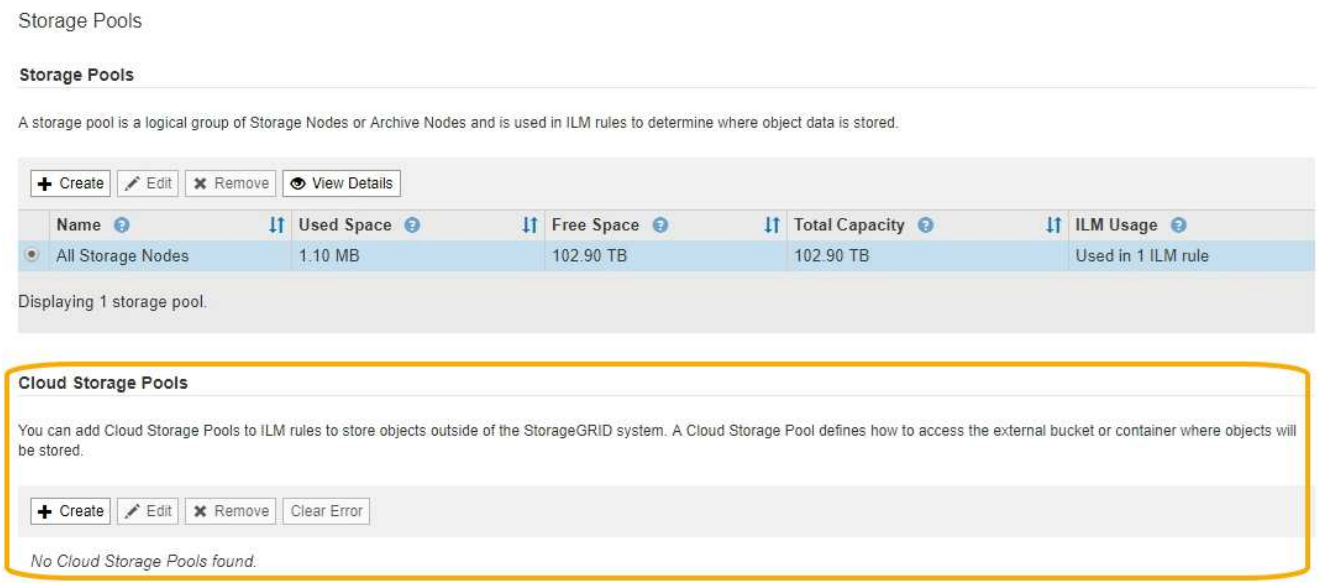
このタスクについて

クラウドストレージプールは、単一の外部の S3 バケットまたは Azure BLOB ストレージコンテナを指定します。クラウドストレージプールは保存後すぐに StorageGRID で検証されます。そのため、クラウドストレージプールに指定されたバケットまたはコンテナが存在し、アクセス可能であることを確認しておく必要があります。

手順

1. ILM * > * Storage pools * を選択します

   Storage Pools （ストレージプール）ページが表示されます。このページには、ストレージプールとクラウドストレージプールの 2 つのセクションがあります。



2. ページのクラウドストレージプールセクションで、 * 作成 * を選択します。

   Create Cloud Storage Pool （クラウドストレージプールの作成）ダイアログボックスが表示されます。

3. 次の情報を入力します。

フィールド	説明
表示名	クラウドストレージプールとその目的を簡単に説明する名前。ILM ルールを設定するときに識別しやすい名前を使用してください。
プロバイダタイプ	このクラウドストレージプールに使用するクラウドプロバイダ： • * Amazon S3 * ： S3 、 C2S S3 、または Google Cloud Platform （ GCP ）エンドポイントの場合は、このオプションを選択します。 • * Azure Blob Storage * ◦ 注： [プロバイダタイプ] を選択すると、ページの下部に [サービスエンドポイント] 、 [認証] 、および [サーバ検証] セクションが表示されます。
バケットまたはコンテナ	クラウドストレージプール用に作成された外部の S3 バケットまたは Azure コンテナの名前。バケットまたはコンテナの名前は正確に指定する必要があります。一致していないと、クラウドストレージプールの作成が失敗します。クラウドストレージプールの保存後にこの値を変更することはできません。

4. 選択したプロバイダータイプに基づいて、ページの [Service Endpoint] 、 [Authentication] 、および [Server Verification] セクションを完了します。
   - S3 ：クラウドストレージプールの認証情報を指定します
   - C2S S3 ：クラウドストレージプールの認証情報を指定します
   - Azure ：クラウドストレージプールの認証情報を指定します

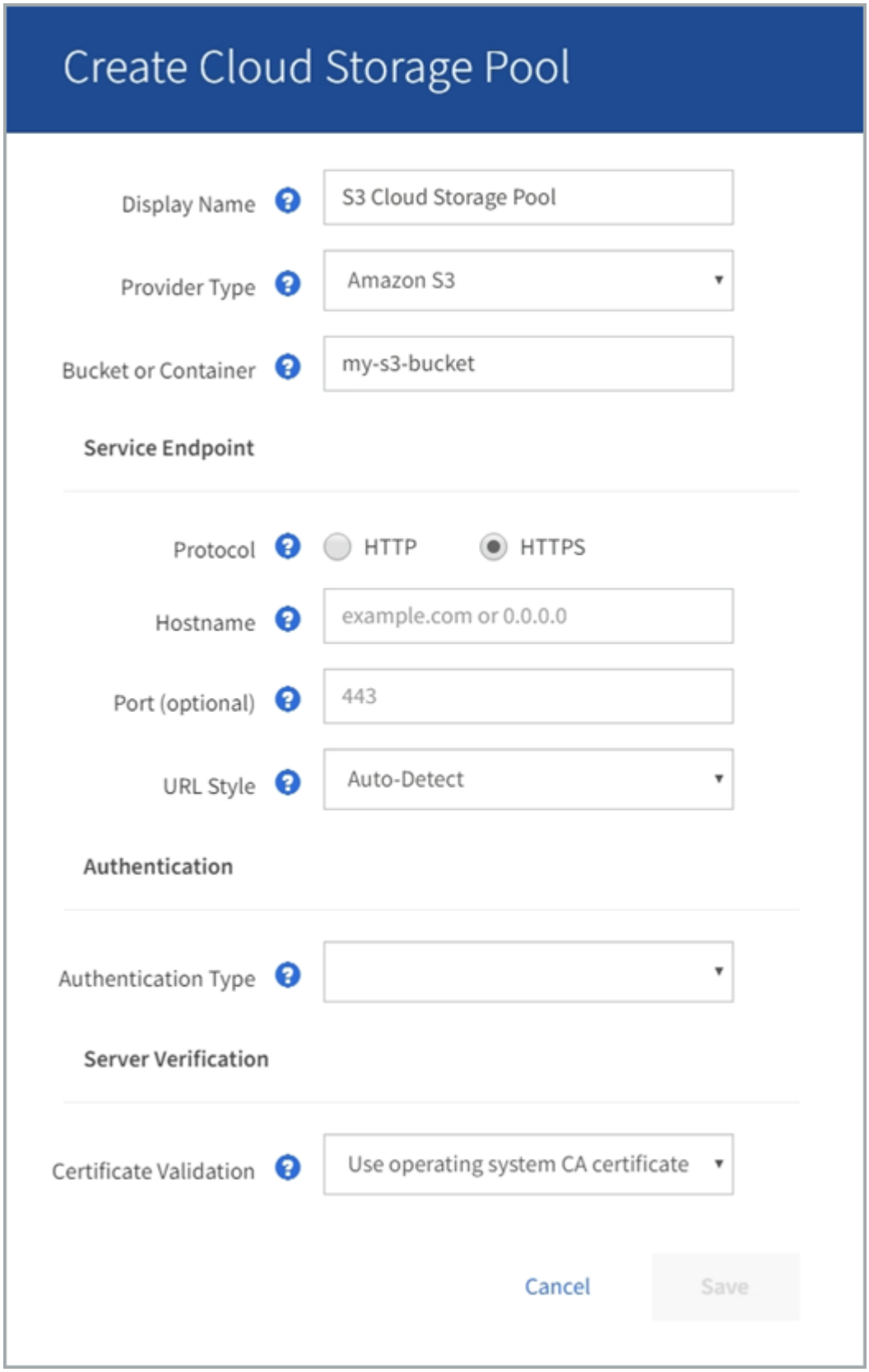
S3 ：クラウドストレージプールの認証情報の指定

S3 用のクラウドストレージプールを作成する場合は、クラウドストレージプールのエンドポイントで必要な認証のタイプを選択する必要があります。匿名を指定するか、アク

セスキー ID とシークレットアクセスキーを入力できます。

必要なもの

- クラウドストレージプールの基本情報を入力し、プロバイダタイプとして * Amazon S3 * を指定しておきます。



- アクセスキー認証を使用している場合は、外部の S3 バケットのアクセスキー ID とシークレットアクセスキーを確認しておきます。

手順

1. 「 * Service Endpoint * 」セクションで、次の情報を入力します。

   a. クラウドストレージプールに接続するときに使用するプロトコルを選択します。

      デフォルトのプロトコルは HTTPS です。

   b. クラウドストレージプールのサーバのホスト名または IP アドレスを入力します。

      例：

      s3-*aws-region*.amazonaws.com

      > バケット名はこのフィールドに含めないでください。バケット名は「 * Bucket 」フィールドまたは「 Container * 」フィールドに入力します。

   a. 必要に応じて、クラウドストレージプールへの接続時に使用するポートを指定します。

      デフォルトのポート（ HTTPS の場合はポート 443 、 HTTP の場合はポート 80 ）を使用する場合は、このフィールドを空白のままにします。

   b. クラウドストレージプールバケットの URL 形式を選択します。

オプション	説明
仮想ホスト形式	仮想ホスト形式の URL を使用してバケットにアクセスする。仮想ホスト形式の URL には、ドメイン名の一部としてバケット名が含まれます（例：「 + https://bucket-name.s3.company.com/key-name+` 」）。
パス形式	パス形式の URL を使用してバケットにアクセスします。パス形式の URL の末尾には、「 + https://s3.company.com/bucket-name/key-name+` 」のようにバケット名が含まれます。 • 注： * パス形式の URL は廃止されています。
自動検出	指定された情報に基づいて、使用する URL スタイルを自動的に検出します。たとえば、 IP アドレスを指定すると、 StorageGRID はパス形式の URL を使用します。使用するスタイルがわからない場合にのみ、このオプションを選択してください。

2. [* 認証 *] セクションで、クラウドストレージプールエンドポイントに必要な認証のタイプを選択します。

オプション	説明
アクセスキー	Cloud Storage Pool バケットにアクセスするには、アクセスキー ID とシークレットアクセスキーが必要です。

オプション	説明
匿名	すべてのユーザが Cloud Storage Pool バケットにアクセスできます。アクセスキー ID とシークレットアクセスキーは不要です。
CAP （ C2S Access Portal ）	C2S S3 にのみ使用されます。に進みます C2S S3 ：クラウドストレージプールの認証情報の指定。

3. アクセスキーを選択した場合は、次の情報を入力します。

オプション	説明
アクセスキー ID	外部バケットを所有するアカウントのアクセスキー ID 。
シークレットアクセスキー	関連付けられているシークレットアクセスキー。

4. Server Verification セクションで、クラウドストレージプールへの TLS 接続用の証明書を検証する方法を選択します。

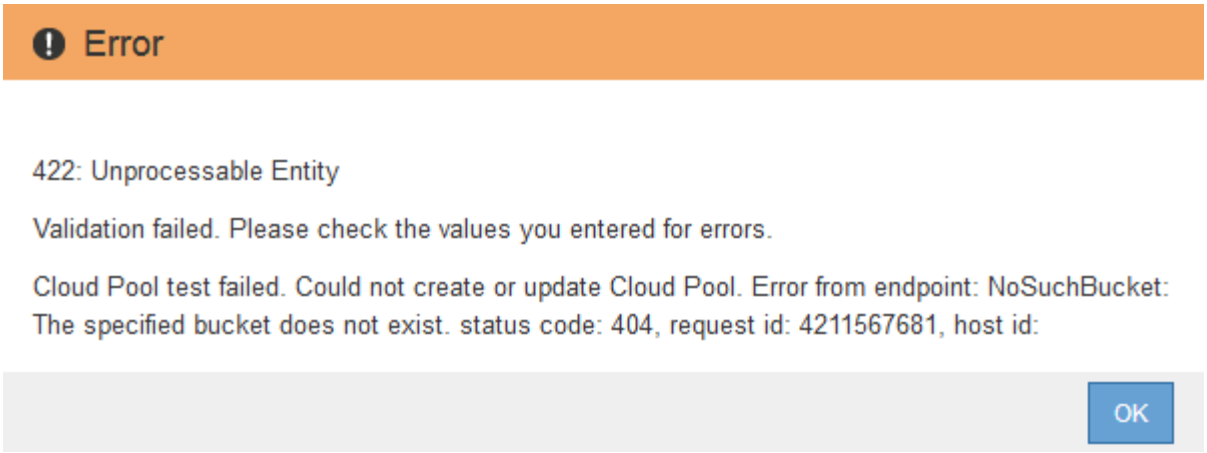
オプション	説明
オペレーティングシステムの CA 証明書を使用します	オペレーティングシステムにインストールされているデフォルトの Grid CA 証明書を使用して接続を保護します。
カスタム CA 証明書を使用する	カスタム CA 証明書を使用する。Select New * を選択し、 PEM でエンコードされた CA 証明書をアップロードします。
証明書を検証しないでください	TLS 接続に使用される証明書は検証されません。

5. [保存（ Save ）] を選択します。

クラウドストレージプールを保存すると、 StorageGRID では次の処理が実行されます。

- バケットとサービスエンドポイントが存在し、指定したクレデンシャルを使用してそれらにアクセスできることを検証します。
- バケットをクラウドストレージプールとして識別するために、バケットにマーカーファイルを書き込みます。このファイルは削除しないでください。「 x-ntap-sgws-cloud-pool-uuid 」という名前です。

クラウドストレージプールの検証に失敗すると、その理由を記載したエラーメッセージが表示されます。たとえば、証明書エラーが発生した場合や、指定したバケットが存在しない場合などにエラーが報告されます。



の手順を参照してください クラウドストレージプールのトラブルシューティングをクリックし、問題 を解決してから、クラウドストレージプールの保存を再度実行してください。

C2S S3 ：クラウドストレージプールの認証情報を指定します

Commercial クラウド サービス （ C2S ） S3 サービスをクラウドストレージプールとして使用するには、認証タイプとして C2S Access Portal （ CAP ）を設定し、StorageGRID が C2S アカウント内の S3 バケットにアクセスするための一時的なクレデンシャルを要求できるようにする必要があります。

必要なもの

- Amazon S3 クラウドストレージプールのサービスエンドポイントを含む基本情報を入力しておきます。
- StorageGRID が CAP サーバから一時的なクレデンシャルを取得するために使用する、 C2S アカウントに割り当てられている必須 / オプションの API パラメータをすべて含む完全な URL が必要です。
- 該当する公的認証局（ CA ）が発行したサーバ CA 証明書が必要です。StorageGRID は、この証明書を使用して CAP サーバの識別情報を確認します。サーバ CA 証明書は PEM エンコードを使用している必要があります。
- 該当する公的認証局（ CA ）が発行したクライアント証明書が必要です。StorageGRID は、この証明書を使用して CAP サーバに対して自身を識別します。クライアント証明書は PEM エンコードを使用し、C2S アカウントへのアクセスが許可されている必要があります。
- クライアント証明書の PEM でエンコードされた秘密鍵が必要です。
- クライアント証明書の秘密鍵が暗号化されている場合は、復号化用のパスフレーズが必要です。

手順

1. [* 認証] セクションで、 **[** 認証タイプ **]** ドロップダウンから ***CAP (C2S Access Portal)** を選択します。

   CAP C2S の認証フィールドが表示されます。

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. 次の情報を入力します。

   a. [*Temporary Credentials URL] には、 StorageGRID が CAP サーバから一時的なクレデンシャルを取得するために使用する完全な URL を入力します。これには、 C2S アカウントに割り当てられている必須およびオプションの API パラメータがすべて含まれます。

   b. Server CA Certificate* には、 * Select New* を選択し、 StorageGRID が CAP サーバの検証に使用する PEM でエンコードされた CA 証明書をアップロードします。

   c. * クライアント証明書 * の場合は、 * 新しい * を選択し、 StorageGRID が CAP サーバに対して自身を識別するために使用する PEM でエンコードされた証明書をアップロードします。

   d. * クライアント秘密鍵 * の場合は、 * 新規選択 * を選択し、クライアント証明書の PEM でエンコードされた秘密鍵をアップロードします。

      秘密鍵が暗号化されている場合は、従来の形式を使用する必要があります。（ PKCS #8 で暗号化された形式はサポートされていません）。

   e. クライアントの秘密鍵が暗号化されている場合は、クライアントの秘密鍵を復号化するためのパスフレーズを入力します。それ以外の場合は、 [* クライアント秘密キーのパスフレーズ *] フィールドを空白のままにします。

3. Server Verification セクションで、次の情報を指定します。

   a. 「 * 証明書の検証 * 」で、「 * カスタム CA 証明書を使用する * 」を選択します。

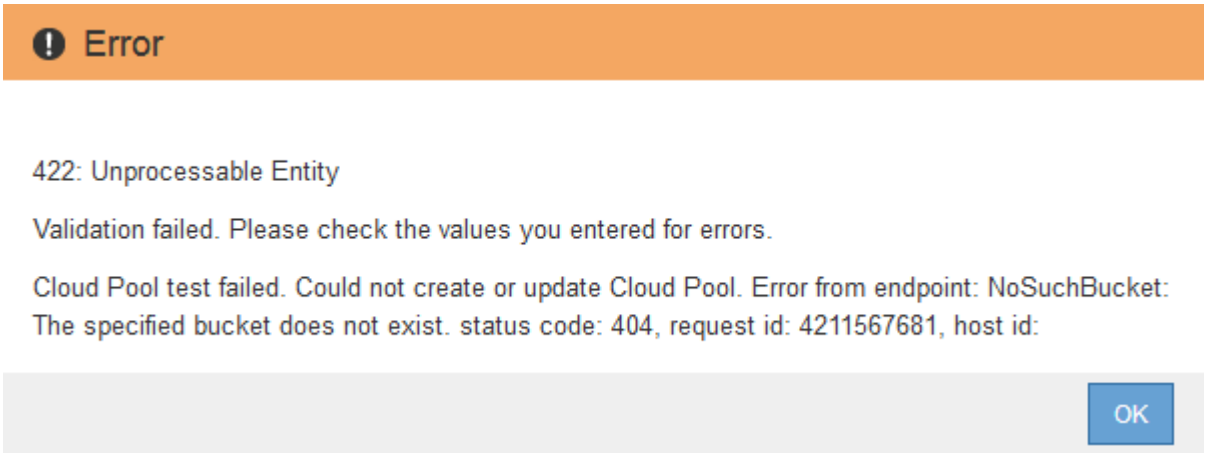
   b. Select New * を選択し、 PEM でエンコードされた CA 証明書をアップロードします。

4. [保存（ Save ）] を選択します。

クラウドストレージプールを保存すると、 StorageGRID では次の処理が実行されます。

- バケットとサービスエンドポイントが存在し、指定したクレデンシャルを使用してそれらにアクセスできることを検証します。
- バケットをクラウドストレージプールとして識別するために、バケットにマーカーファイルを書き込みます。このファイルは削除しないでください。「 x-ntap-sgws-cloud-pool-uuid 」という名前です。

クラウドストレージプールの検証に失敗すると、その理由を記載したエラーメッセージが表示されます。たとえば、証明書エラーが発生した場合や、指定したバケットが存在しない場合などにエラーが報告されます。



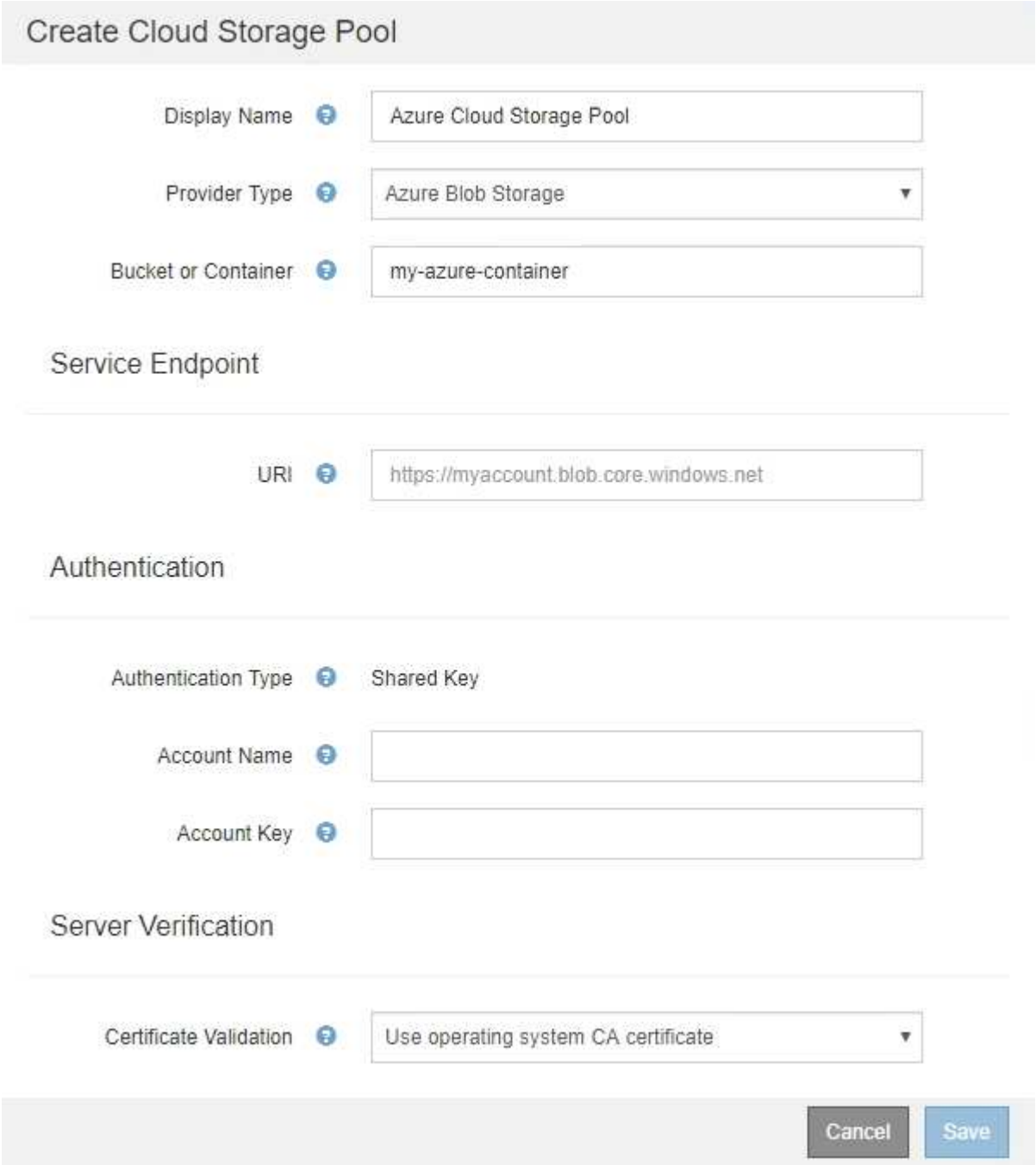
の手順を参照してください クラウドストレージプールのトラブルシューティングをクリックし、問題 を解決してから、クラウドストレージプールの保存を再度実行してください。

Azure ：クラウドストレージプールの認証情報を指定します

Azure BLOB ストレージ用のクラウドストレージプールを作成する場合は、StorageGRID がオブジェクトの格納に使用する外部コンテナのアカウント名とアカウントキーを指定する必要があります。

必要なもの

- クラウドストレージプールの基本情報を入力し、プロバイダタイプとして「 * Azure Blob Storage * 」を指定しておきます。**Authentication Type** フィールドに Shared Key* が表示されます。



- クラウドストレージプールに使用される BLOB ストレージコンテナへのアクセスに使用する Uniform Resource Identifier （ URI ）がわかっている。

- ストレージアカウントの名前とシークレットキーを確認しておきます。これらの値は Azure portal を使用して確認できます。

手順

1. 「 * サービスエンドポイント * 」セクションで、クラウドストレージプールに使用される BLOB ストレージコンテナへのアクセスに使用する Uniform Resource Identifier （ URI ）を入力します。

   次のいずれかの形式で指定します。

   - 「 + https://host:port+` 」と入力します
   - 「 + http://host:port+` 」と入力します

   ポートを指定しない場合、デフォルトでは HTTPS URI にはポート 443 が、 HTTP URI にはポート 80 が使用されます。*Azure BLOB ストレージコンテナの URI の例 *:`https://myaccount.blob.core.windows.net`

2. [* 認証 * （ * Authentication * ）] セクションで、次の情報を入力します。

   a. **Account Name** に、外部サービスコンテナを所有する BLOB ストレージアカウントの名前を入力します。

   b. 「 * Account Key * 」に、 BLOB ストレージアカウントのシークレットキーを入力します。

   Azure エンドポイントの場合は、共有キー認証を使用する必要があります。

3. [サーバ検証 *] セクションで、クラウドストレージプールへの TLS 接続用証明書の検証に使用する方法を選択します。

オプション	説明
オペレーティングシステムの CA 証明書を使用します	オペレーティングシステムにインストールされているグリッド CA 証明書を使用して接続を保護します。
カスタム CA 証明書を使用する	カスタム CA 証明書を使用する。Select New * を選択し、 PEM でエンコードされた証明書をアップロードします。
証明書を検証しないでください	TLS 接続に使用される証明書は検証されません。

4. [保存 （ Save ）] を選択します。

クラウドストレージプールを保存すると、 StorageGRID では次の処理が実行されます。

- コンテナと URI が存在し、指定したクレデンシャルを使用してアクセスできることを検証します。
- クラウドストレージプールとして識別するためにコンテナにマーカーファイルを書き込みます。このファイルは削除しないでください。「 x-ntap-sgws-cloud-pool-uuid 」という名前です。

クラウドストレージプールの検証に失敗すると、その理由を記載したエラーメッセージが表示されます。たとえば、証明書エラーが発生した場合や、指定したコンテナが存在しない場合などにエラーが報告されます。

の手順を参照してください クラウドストレージプールのトラブルシューティングをクリックし、問題 を解決してから、クラウドストレージプールの保存を再度実行してください。