Création d'un pool de stockage cloud

StorageGRID 11.5

NetApp
April 11, 2024

Sommaire

Création d’un pool de stockage cloud

Lorsque vous créez un pool de stockage cloud, vous indiquez le nom et l’emplacement du compartiment ou du conteneur externe utilisé par StorageGRID pour stocker des objets, le type de fournisseur cloud (Amazon S3 ou Azure Blob Storage) et le StorageGRID service d’information doit accéder au compartiment ou au conteneur externe.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l’aide d’un navigateur pris en charge.
- Vous devez disposer d’autorisations d’accès spécifiques.
- Vous devez avoir lu les instructions sur la configuration des pools de stockage cloud.
- Le compartiment externe ou conteneur référencé par le pool de stockage cloud doit exister.
- Vous devez disposer de toutes les informations d’authentification requises pour accéder au compartiment ou au conteneur.

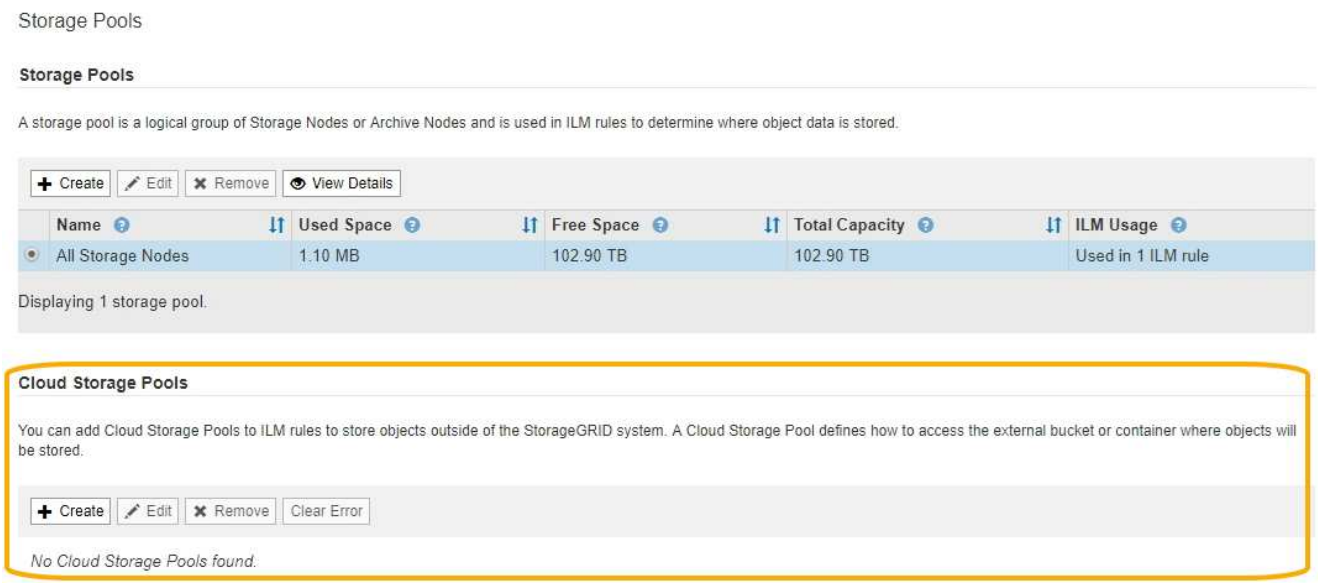
Description de la tâche

Un pool de stockage cloud spécifie un compartiment S3 externe unique ou un conteneur de stockage Azure Blob. StorageGRID valide le pool de stockage cloud dès que vous le sauvegardez. Vous devez donc vous assurer que le compartiment ou le conteneur spécifié dans le pool de stockage cloud est accessible et qu’il existe.

Étapes

1. Sélectionnez **ILM** > **pools de stockage**.

   La page Storage pools s’affiche. Cette page contient deux sections : les pools de stockage et les pools de stockage cloud.



2. Dans la section Cloud Storage pools (pools de stockage cloud) de la page, cliquez sur **Create** (Créer).

   La boîte de dialogue Créer un pool de stockage cloud s’affiche.

3. Saisissez les informations suivantes :

Champ	Description
Afficher le nom	Un nom qui décrit brièvement le pool de stockage cloud et son objectif. Nom facile à identifier lors de la configuration des règles ILM.
Type de fournisseur	Quel fournisseur de cloud utiliser pour ce pool de stockage cloud : • Amazon S3 (sélectionnez cette option pour un pool de stockage cloud S3 ou C2S S3) • Stockage Azure Blob Storage **Remarque :** lorsque vous sélectionnez un type de fournisseur, les sections point de terminaison de service, authentification et vérification du serveur s'affichent en bas de la page.
Godet ou conteneur	Nom du compartiment S3 externe ou du conteneur Azure créé pour le pool de stockage cloud. Le nom que vous indiquez ici doit correspondre exactement au nom du compartiment ou du conteneur, ou la création du pool de stockage cloud échoue. Vous ne pouvez pas modifier cette valeur après l'enregistrement du pool de stockage cloud.

4. Complétez les sections point de terminaison de service, authentification et vérification du serveur de la page, en fonction du type de fournisseur sélectionné.
   - "S3 : spécification des détails d'authentification pour un pool de stockage cloud"
   - "C2S S3 : spécification des détails d'authentification pour un pool de stockage cloud"
   - "Azure : spécification des détails d'authentification pour un pool de stockage cloud"

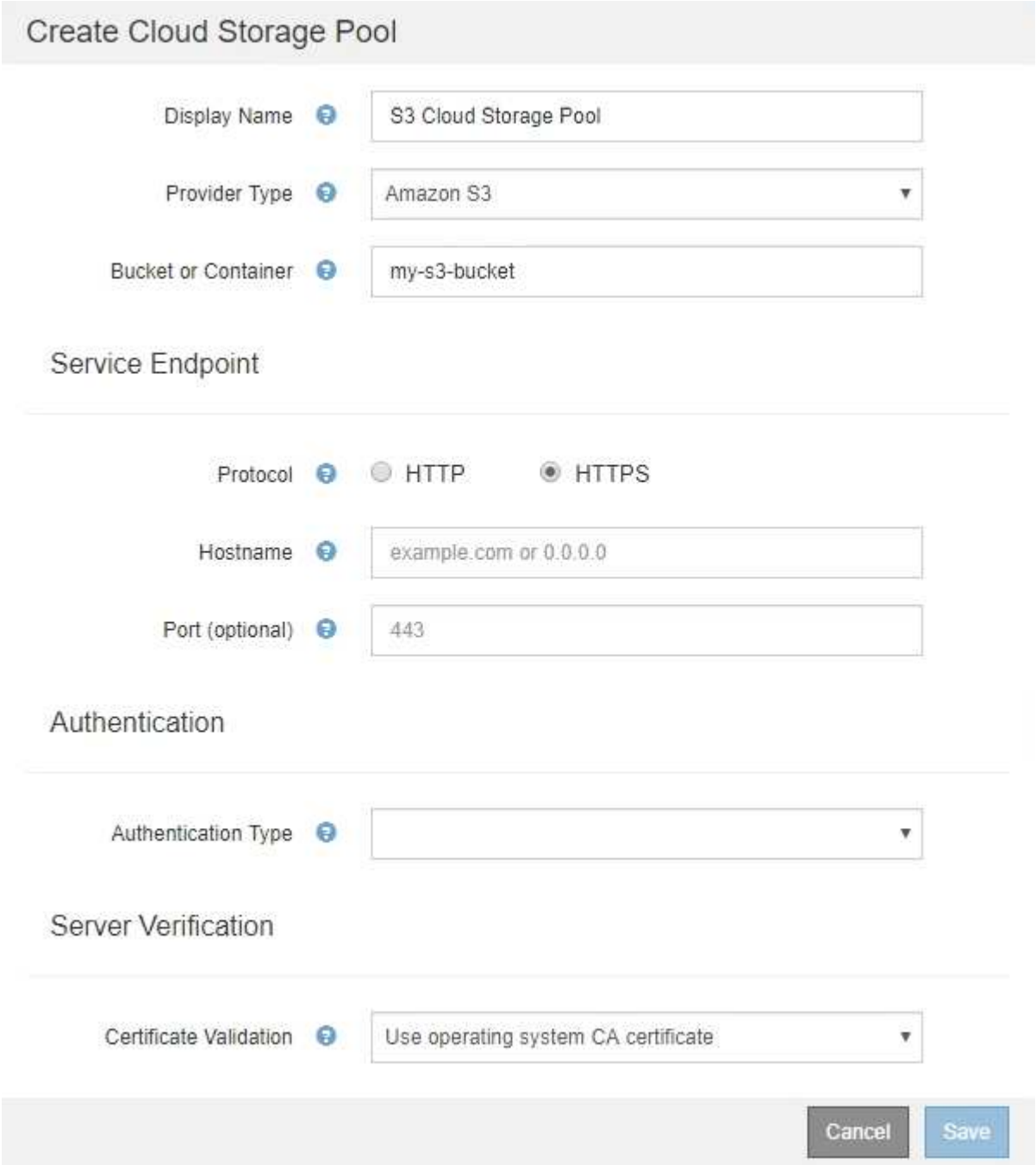
S3 : spécification des détails d'authentification pour un pool de stockage cloud

Lorsque vous créez un pool de stockage cloud pour S3, vous devez sélectionner le type d'authentification requis pour le terminal Cloud Storage Pool. Vous pouvez spécifier

Anonyme ou entrer un ID de clé d'accès et une clé d'accès secrète.

Ce dont vous avez besoin

- Vous devez avoir saisi les informations de base pour le pool de stockage cloud et spécifié **Amazon S3** comme type de fournisseur.



- Si vous utilisez l'authentification par clé d'accès, vous devez connaître l'ID de clé d'accès et la clé d'accès secrète pour le compartiment S3 externe.

Étapes

1. Dans la section **Service Endpoint**, fournissez les informations suivantes :

    a. Sélectionnez le protocole à utiliser lors de la connexion au pool de stockage cloud.

Le protocole par défaut est HTTPS.

b. Entrez le nom d'hôte ou l'adresse IP du serveur du pool de stockage cloud.

Par exemple :

`s3-aws-region.amazonaws.com`

> Ne pas inclure le nom de compartiment dans ce champ. Vous incluez le nom du compartiment dans le champ **godet ou conteneur**.

a. Spécifiez éventuellement le port à utiliser lors de la connexion au Cloud Storage Pool.

Laissez ce champ vide pour utiliser le port par défaut : port 443 pour HTTPS ou port 80 pour HTTP.

2. Dans la section **Authentication**, sélectionnez le type d'authentification requis pour le terminal Cloud Storage Pool.

Option	Description
Clé d'accès	Un ID de clé d'accès et une clé d'accès secrète sont nécessaires pour accéder au compartiment de pool de stockage cloud.
Anonyme	Tout le monde a accès au compartiment Cloud Storage Pool. Un ID de clé d'accès et une clé d'accès secrète ne sont pas nécessaires.
CAP (portail d'accès C2S)	Utilisé uniquement pour C2S S3. Accédez à "C2S S3 : spécification des détails d'authentification pour un pool de stockage cloud".

3. Si vous avez sélectionné clé d'accès, saisissez les informations suivantes :

Option	Description
ID de clé d'accès	ID de clé d'accès du compte propriétaire du compartiment externe.
Clé d'accès secrète	La clé d'accès secrète associée.

4. Dans la section Server Verification, sélectionnez la méthode à utiliser pour valider le certificat pour les connexions TLS au Cloud Storage Pool :

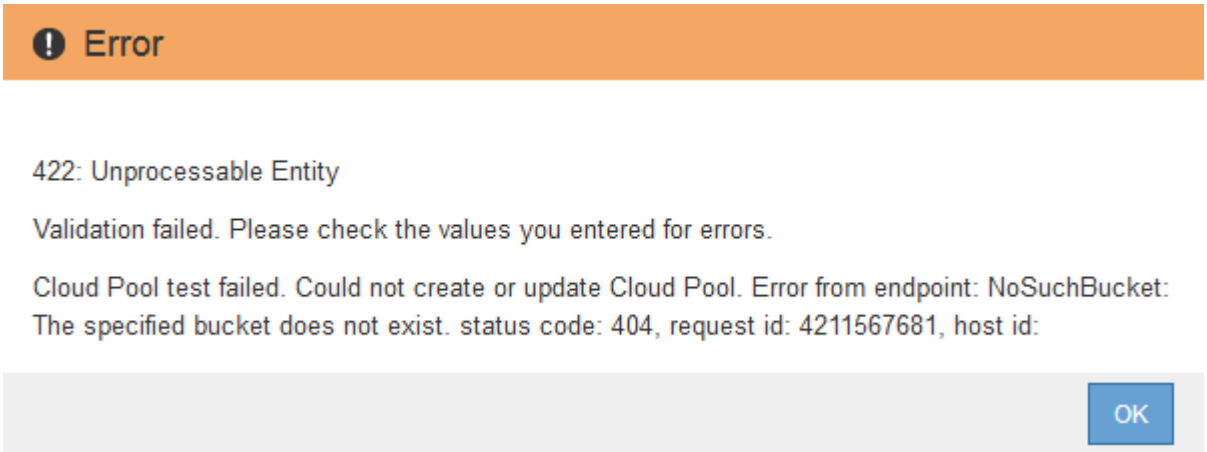
Option	Description
Utiliser le certificat CA du système d'exploitation	Utilisez les certificats CA par défaut installés sur le système d'exploitation pour sécuriser les connexions.
Utiliser un certificat d'autorité de certification personnalisé	Utilisez un certificat d'autorité de certification personnalisé. Cliquez sur **Sélectionner nouveau** et téléchargez le certificat d'autorité de certification codé PEM.
Ne vérifiez pas le certificat	Le certificat utilisé pour la connexion TLS n'est pas vérifié.

5. Cliquez sur **Enregistrer**.

Lorsque vous enregistrez un pool de stockage cloud, StorageGRID effectue les opérations suivantes :

- Valide la présence du compartiment et du point de terminaison de service et qu'ils peuvent être atteints à l'aide des identifiants que vous avez spécifiés.
- Écrit un fichier de marqueur dans le compartiment pour identifier le compartiment comme pool de stockage cloud. Ne supprimez jamais ce fichier nommé `x-ntap-sgws-cloud-pool-uuid`.

Si la validation du pool de stockage cloud échoue, un message d'erreur s'affiche indiquant pourquoi la validation a échoué. Par exemple, une erreur peut être signalée en cas d'erreur de certificat ou si le compartiment spécifié n'existe pas déjà.



Consultez les instructions de résolution des problèmes liés aux pools de stockage cloud, résolvez le problème, puis essayez à nouveau d'enregistrer le pool de stockage cloud.

Informations associées

"Résolution des problèmes avec les pools de stockage cloud"

C2S S3 : spécification des détails d'authentification pour un pool de stockage cloud

Pour utiliser le service S3 commercial Cloud Services (C2S) comme pool de stockage cloud, vous devez configurer C2S Access Portal (CAP) comme type d'authentification. StorageGRID peut ainsi demander des identifiants temporaires pour accéder au compartiment S3 de votre compte C2S.

Ce dont vous avez besoin

- Vous devez avoir saisi les informations de base d'un pool de stockage cloud Amazon S3, y compris le terminal du service.
- Vous devez connaître l'URL complète utilisée par StorageGRID pour obtenir des informations d'identification temporaires du serveur CAP, y compris tous les paramètres d'API obligatoires et facultatifs attribués à votre compte C2S.
- Vous devez disposer d'un certificat d'autorité de certification de serveur délivré par une autorité de certification du gouvernement (AC) appropriée. StorageGRID utilise ce certificat pour vérifier l'identité du serveur CAP. Le certificat d'autorité de certification du serveur doit utiliser le codage PEM.

- Vous devez avoir un certificat de client délivré par une autorité de certification gouvernementale (AC) appropriée. StorageGRID utilise ce certificat pour s'identifier lui-même au serveur CAP. Le certificat client doit utiliser le codage PEM et avoir reçu l'accès à votre compte C2S.
- Vous devez disposer d'une clé privée codée PEM pour le certificat client.
- Si la clé privée du certificat client est cryptée, vous devez disposer de la phrase de passe pour le déchiffrer.

Étapes

1. Dans la section **authentification**, sélectionnez **CAP (portail d'accès C2S)** dans la liste déroulante **Type d'authentification**.

   Les champs d'authentification CAP C2S s'affichent.

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. Fournissez les informations suivantes :
   a. Pour **URL d'informations d'identification temporaires**, entrez l'URL complète utilisée par StorageGRID pour obtenir des informations d'identification temporaires du serveur CAP, y compris tous les paramètres d'API obligatoires et facultatifs attribués à votre compte C2S.
   b. Pour **certificat d'autorité de certification serveur**, cliquez sur **Sélectionner nouveau** et téléchargez le certificat d'autorité de certification codé au PEM que StorageGRID utilisera pour vérifier le serveur CAP.
   c. Pour **certificat client**, cliquez sur **Sélectionner nouveau** et téléchargez le certificat codé au PEM que StorageGRID utilisera pour s'identifier au serveur CAP.
   d. Pour **clé privée client**, cliquez sur **Sélectionner nouveau** et téléchargez la clé privée codée PEM pour le certificat client.

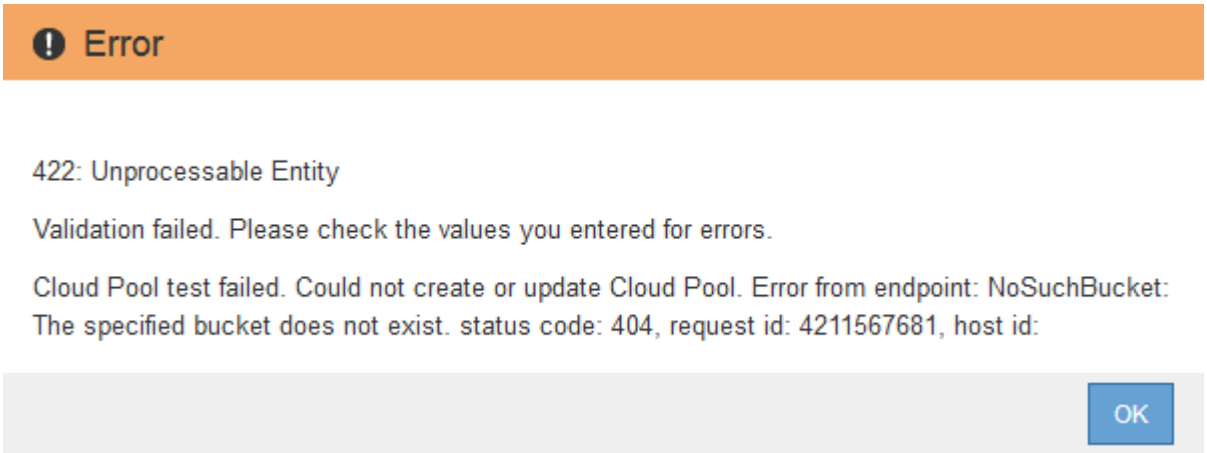
      Si la clé privée est cryptée, le format traditionnel doit être utilisé. (Le format crypté PKCS #8 n'est pas pris en charge.)

   e. Si la clé privée du client est cryptée, entrez la phrase de passe pour déchiffrer la clé privée du client. Sinon, laissez le champ **Mot de passe de clé privée client** vide.
3. Dans la section Vérification du serveur, fournissez les informations suivantes :
   a. Pour **validation de certificat**, sélectionnez **utiliser le certificat d'autorité de certification personnalisé**.
   b. Cliquez sur **Sélectionner nouveau** et téléchargez le certificat d'autorité de certification codé PEM.
4. Cliquez sur **Enregistrer**.

Lorsque vous enregistrez un pool de stockage cloud, StorageGRID effectue les opérations suivantes :

- Valide la présence du compartiment et du point de terminaison de service et qu'ils peuvent être atteints à l'aide des identifiants que vous avez spécifiés.
- Écrit un fichier de marqueur dans le compartiment pour identifier le compartiment comme pool de stockage cloud. Ne supprimez jamais ce fichier nommé `x-ntap-sgws-cloud-pool-uuid`.

Si la validation du pool de stockage cloud échoue, un message d'erreur s'affiche indiquant pourquoi la validation a échoué. Par exemple, une erreur peut être signalée en cas d'erreur de certificat ou si le compartiment spécifié n'existe pas déjà.



Consultez les instructions de résolution des problèmes liés aux pools de stockage cloud, résolvez le problème, puis essayez à nouveau d'enregistrer le pool de stockage cloud.

Informations associées

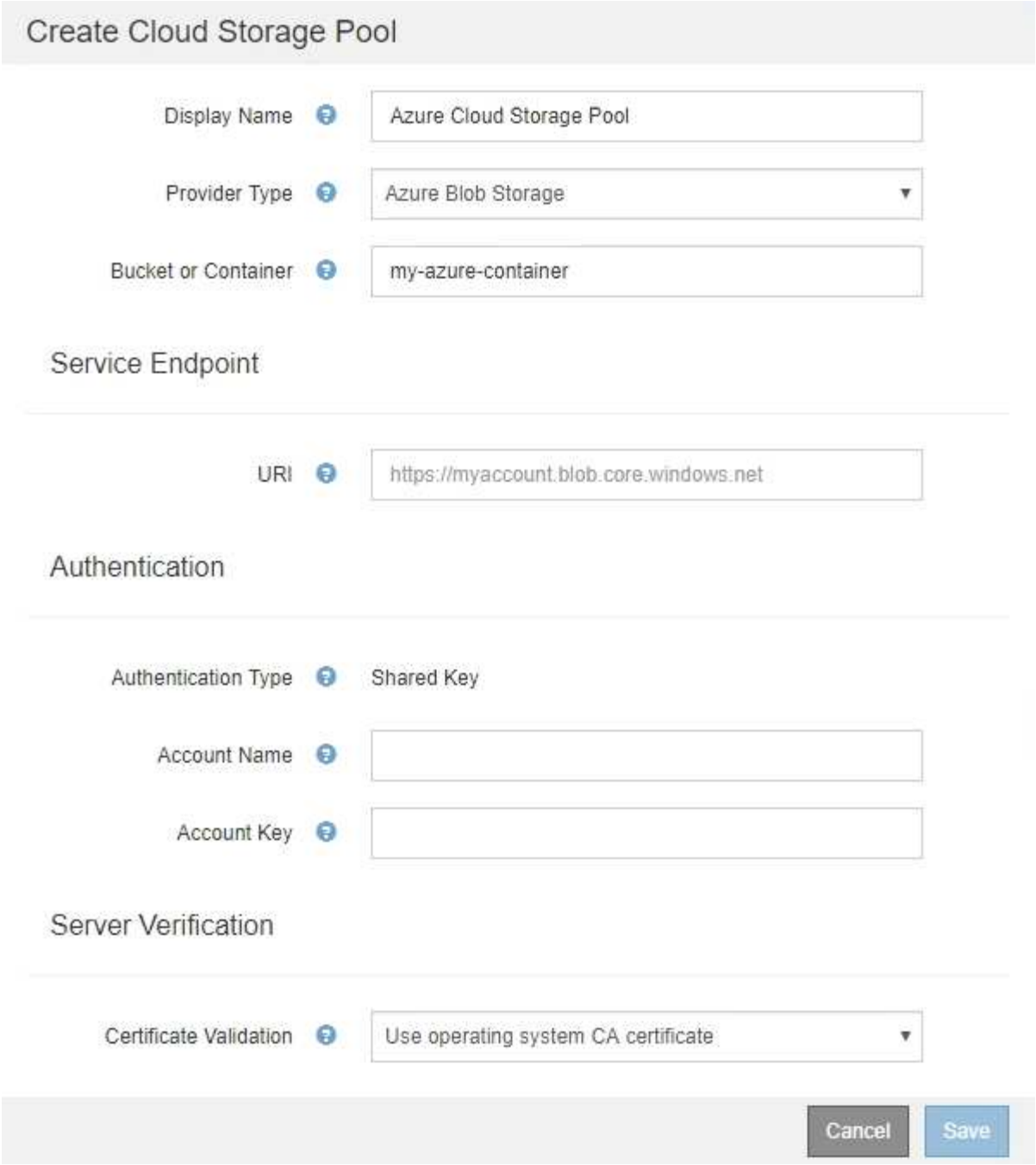
"Résolution des problèmes avec les pools de stockage cloud"

Azure : spécification des détails d'authentification pour un pool de stockage cloud

Lorsque vous créez un pool de stockage cloud pour le stockage Azure Blob, vous devez spécifier un nom de compte et une clé de compte pour le conteneur externe que StorageGRID utilisera pour stocker des objets.

Ce dont vous avez besoin

- Vous devez avoir saisi les informations de base pour le pool de stockage cloud et spécifier **Azure Blob Storage** comme type de fournisseur. **Clé partagée** apparaît dans le champ **Type d'authentification**.



- Vous devez connaître l'URI (Uniform Resource identifier) utilisé pour accéder au conteneur de stockage Blob utilisé pour le pool de stockage cloud.
- Vous devez connaître le nom du compte de stockage et la clé secrète. Utilisez le portail Azure pour trouver ces valeurs.

Étapes

1. Dans la section **Service Endpoint**, entrez l'URI (Uniform Resource identifier) utilisé pour accéder au conteneur de stockage Blob utilisé pour le pool de stockage cloud.

   Spécifiez l'URI dans l'un des formats suivants :

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

Si vous ne spécifiez pas de port, le port 443 est utilisé par défaut pour les URI HTTPS et le port 80 est utilisé pour les URI HTTP. + + **exemple d'URI pour conteneur de stockage Azure Blob** : `https://myaccount.blob.core.windows.net`

2. Dans la section **authentification**, fournissez les informations suivantes :

   a. Pour **Nom de compte**, entrez le nom du compte de stockage Blob qui possède le conteneur de services externes.

   b. Pour **clé de compte**, saisissez la clé secrète du compte de stockage Blob.

   > Pour les terminaux Azure, vous devez utiliser l'authentification Shared Key.

3. Dans la section **Vérification du serveur**, sélectionnez la méthode à utiliser pour valider le certificat pour les connexions TLS au pool de stockage cloud :

Option	Description
Utiliser le certificat CA du système d'exploitation	Utilisez les certificats CA par défaut installés sur le système d'exploitation pour sécuriser les connexions.
Utiliser un certificat d'autorité de certification personnalisé	Utilisez un certificat d'autorité de certification personnalisé. Cliquez sur **Sélectionner nouveau** et téléchargez le certificat codé PEM.
Ne vérifiez pas le certificat	Le certificat utilisé pour la connexion TLS n'est pas vérifié.

4. Cliquez sur **Enregistrer**.

Lorsque vous enregistrez un pool de stockage cloud, StorageGRID effectue les opérations suivantes :

- Valide que le conteneur et l'URI existent et qu'ils peuvent être atteints à l'aide des informations d'identification que vous avez spécifiées.
- Écrit un fichier de marqueur vers le conteneur pour l'identifier comme pool de stockage cloud. Ne supprimez jamais ce fichier nommé `x-ntap-sgws-cloud-pool-uuid`.

Si la validation du pool de stockage cloud échoue, un message d'erreur s'affiche indiquant pourquoi la validation a échoué. Par exemple, une erreur peut être signalée s'il y a une erreur de certificat ou si le conteneur spécifié n'existe pas déjà.

Consultez les instructions de résolution des problèmes liés aux pools de stockage cloud, résolvez le problème, puis essayez à nouveau d'enregistrer le pool de stockage cloud.

Informations associées

"Résolution des problèmes avec les pools de stockage cloud"