Utilisation de pools de stockage cloud

StorageGRID 11.5

NetApp
April 11, 2024

Sommaire

Utilisation de pools de stockage cloud

Vous pouvez utiliser les pools de stockage cloud pour déplacer des objets StorageGRID vers un emplacement de stockage externe, tel que le stockage S3 Glacier ou Microsoft Azure Blob. Le déplacement d'objets hors de la grille vous permet de bénéficier d'un Tier de stockage à faible coût pour un archivage à long terme.

- "Définition d'un pool de stockage cloud"
- "Cycle de vie d'un objet de pool de stockage cloud"
- "Quand utiliser les pools de stockage cloud"
- "Considérations relatives aux pools de stockage cloud"
- "Comparaison des pools de stockage cloud et de la réplication CloudMirror"
- "Création d'un pool de stockage cloud"
- "Modification d'un pool de stockage cloud"
- "Suppression d'un pool de stockage cloud"
- "Résolution des problèmes avec les pools de stockage cloud"

Définition d'un pool de stockage cloud

Un pool de stockage cloud permet d'utiliser des règles ILM pour déplacer des données d'objet en dehors de votre système StorageGRID. Par exemple, vous pouvez déplacer des objets peu utilisés vers un stockage cloud à moindre coût, comme Amazon S3 Glacier, S3 Glacier Deep Archive ou le Tier d'accès à l'archivage dans le stockage Microsoft Azure Blob. Vous pouvez également conserver une sauvegarde dans le cloud des objets StorageGRID pour améliorer la reprise d'activité.

Le pool de stockage cloud est similaire à celui d'un pool de stockage du point de vue ILM. Pour stocker des objets à l'un ou l'autre des emplacements, sélectionnez le pool lors de la création des instructions de placement pour une règle ILM. Toutefois, alors que les pools de stockage sont constitués de nœuds de stockage ou de nœuds d'archivage dans le système StorageGRID, un pool de stockage cloud est constitué d'un compartiment externe (S3) ou d'un conteneur (stockage Azure Blob Storage).

Le tableau suivant compare les pools de stockage avec les pools de stockage cloud et présente les similarités et les différences générales.

	Pool de stockage	**Pool de stockage cloud**
Comment est-elle créée ?	Utilisation de l'option **ILM** > **Storage pools** dans Grid Manager. Vous devez configurer les classes de stockage avant de pouvoir créer le pool de stockage.	Utilisation de l'option **ILM** > **Storage pools** dans Grid Manager. Vous devez configurer le compartiment ou le conteneur externe avant de pouvoir créer le pool de stockage cloud.
Combien de pools pouvez-vous créer ?	Illimitée.	Jusqu'à 10.

	Pool de stockage	Pool de stockage cloud
Où sont stockés les objets ?	Sur un ou plusieurs nœuds de stockage ou d'archivage dans StorageGRID.	Dans un compartiment Amazon S3 ou un conteneur de stockage Azure Blob externe au système StorageGRID. Si le pool de stockage cloud est un compartiment Amazon S3 : • Vous pouvez configurer un cycle de vie de compartiment pour la transition des objets vers un stockage à long terme à faible coût, comme Amazon S3 Glacier ou S3 Glacier Deep Archive. Le système de stockage externe doit prendre en charge la classe de stockage Glacier et l'API S3 POST-restauration objet. • Vous pouvez créer des pools de stockage cloud à utiliser avec AWS commercial Cloud Services (C2S), qui prend en charge la région secrète AWS. Si le pool de stockage cloud est un conteneur de stockage Azure Blob, StorageGRID transfère l'objet vers le Tier d'archivage. **Remarque :** en général, ne configurez pas la gestion du cycle de vie du stockage Azure Blob Storage pour le conteneur utilisé pour un pool de stockage cloud. Les opérations DE restauration POST-objet des objets dans le pool de stockage cloud peuvent être affectées par le cycle de vie configuré.
Quels sont les contrôles du placement des objets ?	Règle ILM de la politique ILM active.	Règle ILM de la politique ILM active.
Quelle est la méthode de protection des données utilisée ?	La réplication ou le code d'effacement.	La réplication.

	Pool de stockage	Pool de stockage cloud
Combien de copies de chaque objet sont autorisées ?	Plusieurs.	Une copie dans le pool de stockage cloud et, éventuellement, une ou plusieurs copies dans StorageGRID. **Remarque :** vous ne pouvez pas stocker un objet dans plusieurs pools de stockage cloud à un moment donné.
Quels sont les avantages ?	Les objets sont rapidement accessibles à tout moment.	Stockage à moindre coût

Cycle de vie d'un objet de pool de stockage cloud

Avant d'implémenter les pools de stockage cloud, vérifiez le cycle de vie des objets stockés dans chaque type de pool de stockage cloud.

Informations associées

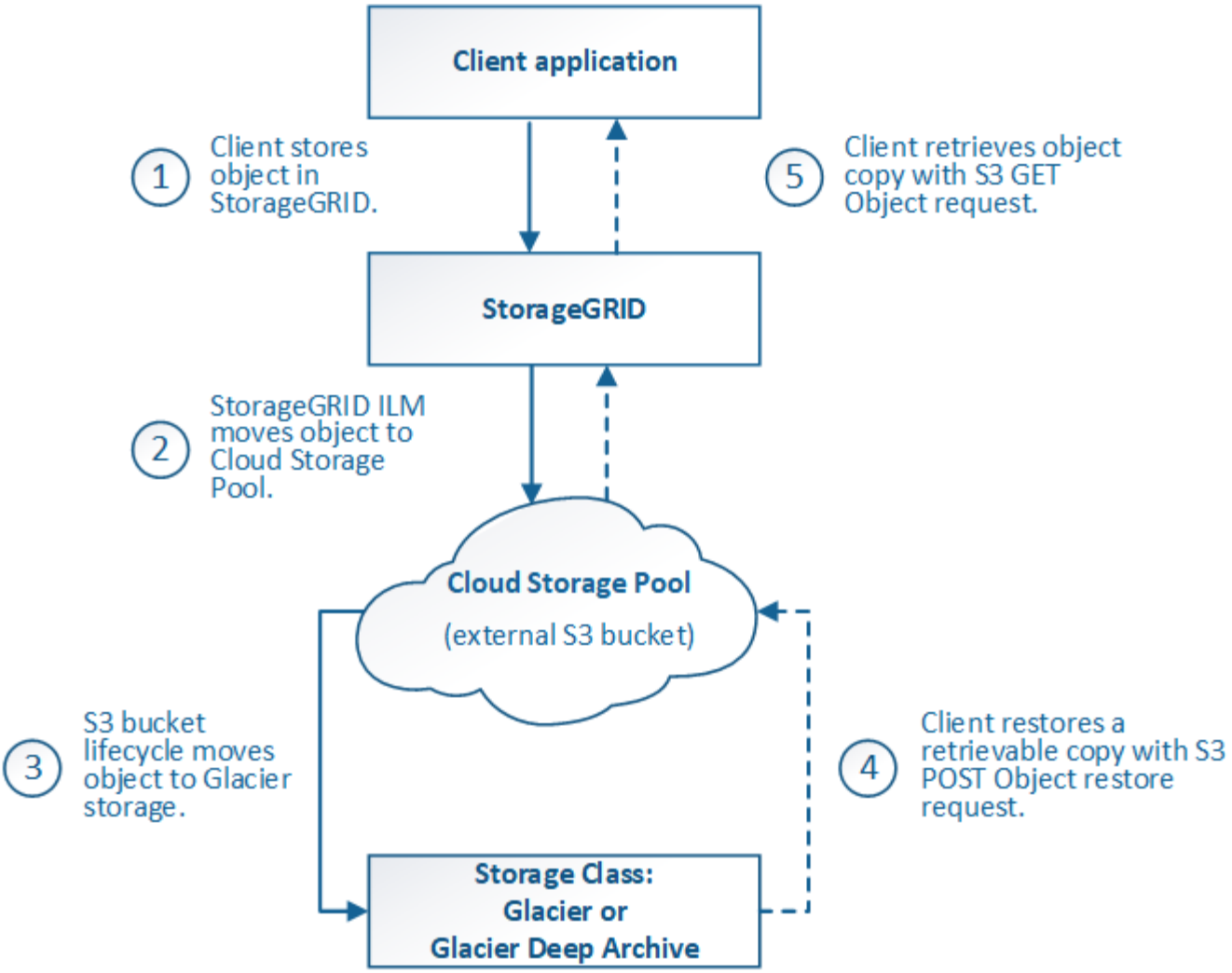
S3 : cycle de vie d'un objet de pool de stockage cloud

Azure : cycle de vie d'un objet de pool de stockage cloud]

S3 : cycle de vie d'un objet de pool de stockage cloud

La figure représente les étapes du cycle de vie d'un objet stocké dans un pool de stockage cloud S3.

> Dans la figure et les explications, « Glacier » désigne à la fois la classe de stockage Glacier et la classe de stockage Glacier Deep Archive, à une exception près : la classe de stockage Glacier Deep Archive ne prend pas en charge le niveau de restauration accéléré. Seule la récupération en bloc ou standard est prise en charge.



1. **Objet stocké dans StorageGRID**

   Pour démarrer le cycle de vie, une application client stocke un objet dans StorageGRID.

2. **Objet déplacé vers le pool de stockage cloud S3**
   - Lorsque l'objet est associé à une règle ILM utilisant un pool de stockage cloud S3 en tant qu'emplacement, StorageGRID déplace l'objet vers le compartiment S3 externe spécifié par le pool de stockage cloud.
   - Lorsque l'objet a été déplacé vers le pool de stockage cloud S3, l'application client peut la récupérer à l'aide d'une requête d'objet GET S3 de StorageGRID, à moins que l'objet n'ait été transféré vers le stockage Glacier.
3. **L'objet a été transféré vers Glacier (état non récupérable)**
   - L'objet peut également être transféré vers le stockage Glacier. Par exemple, un compartiment S3 externe peut utiliser la configuration du cycle de vie pour transférer un objet vers le stockage Glacier immédiatement ou après quelques jours.

> Si vous souhaitez effectuer la transition des objets, vous devez créer une configuration de cycle de vie pour le compartiment S3 externe. Pour ce faire, vous devez utiliser une solution de stockage implémentant la classe de stockage Glacier et prendre en charge l'API S3 POST-restauration objet.

> N’utilisez pas Cloud Storage pools pour les objets qui ont été ingérées par les clients Swift. Swift ne prend pas en charge les demandes DE restauration POST-objet. StorageGRID ne pourra donc pas récupérer d’objets Swift ayant été transférés vers le stockage Glacier S3. L’émission d’une demande d’objet GET Swift pour récupérer ces objets échouera (403 interdit).

- Lors de la transition, l’application client peut utiliser une requête objet TÊTE S3 pour contrôler l’état de l’objet.

4. **Objet restauré à partir du stockage Glacier**

   Lorsqu’un objet est transféré vers le stockage Glacier, l’application client peut émettre une demande de restauration APRÈS objet S3 pour restaurer une copie récupérable dans le pool de stockage cloud S3. La demande spécifie le nombre de jours pendant lesquels la copie doit être disponible dans le pool de stockage cloud et le Tier d’accès aux données à utiliser pour l’opération de restauration (accéléré, Standard ou en bloc). Lorsque la date d’expiration de la copie récupérable est atteinte, la copie est automatiquement renvoyée à un état non récupérable.

   > Si une ou plusieurs copies de l’objet existent également sur les nœuds de stockage dans StorageGRID, il n’est pas nécessaire de restaurer l’objet à partir de Glacier à l’aide d’une demande DE restauration POST-objet. En revanche, la copie locale peut être récupérée directement à l’aide d’une demande D’OBJET GET.

5. **Objet récupéré**

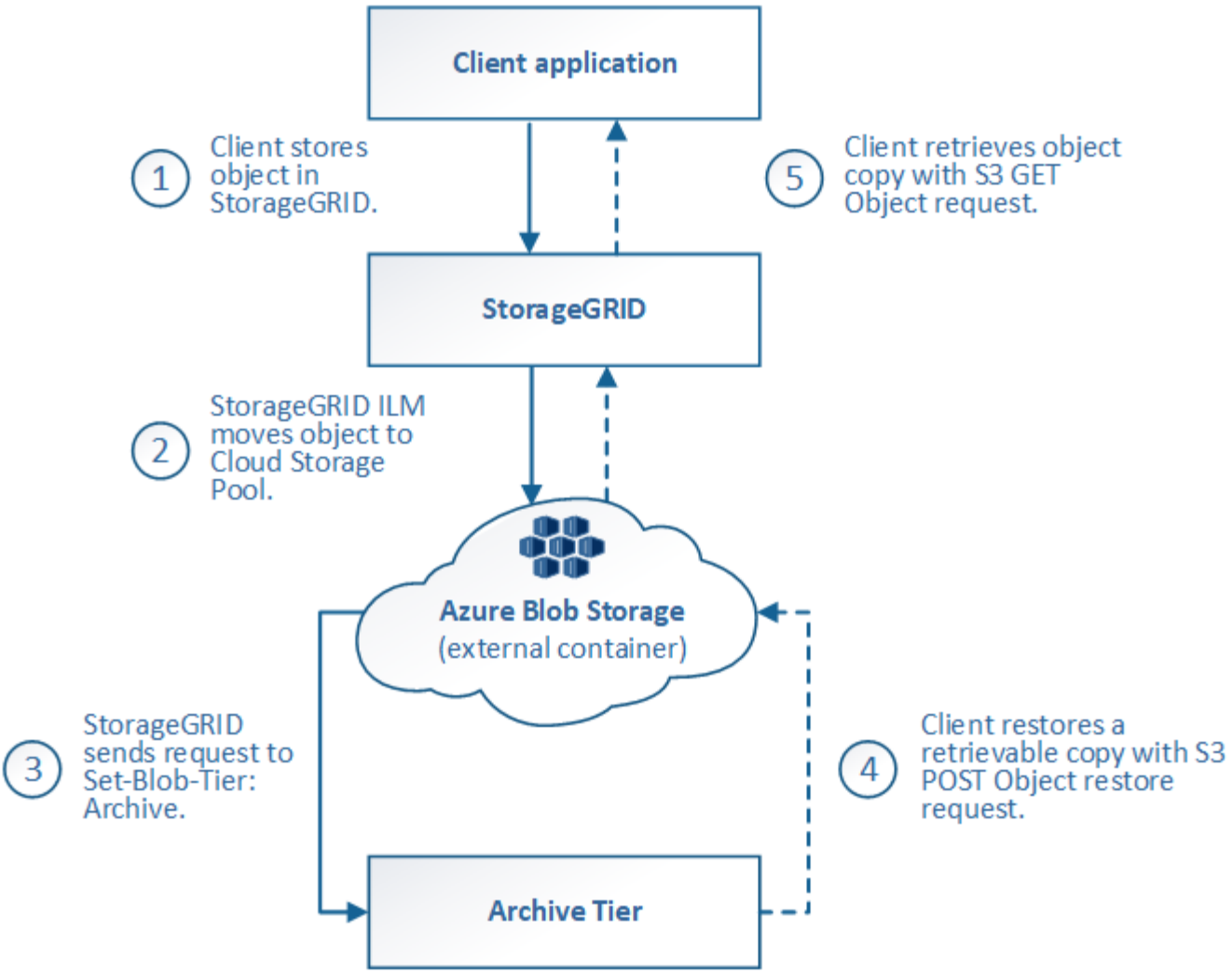
   Une fois qu’un objet a été restauré, l’application client peut émettre une requête GET Object pour récupérer l’objet restauré.

Informations associées

"Utilisation de S3"

Azure : cycle de vie d’un objet de pool de stockage cloud

La figure représente les étapes du cycle de vie d’un objet stocké dans un pool de stockage cloud Azure.



1. **Objet stocké dans StorageGRID**

   Pour démarrer le cycle de vie, une application client stocke un objet dans StorageGRID.

2. **Objet déplacé vers Azure Cloud Storage Pool**

   Lorsque l'objet est associé à une règle ILM utilisant un pool de stockage cloud Azure comme emplacement, StorageGRID déplace l'objet vers le conteneur de stockage Azure Blob externe spécifié par le pool de stockage cloud

   > N'utilisez pas Cloud Storage pools pour les objets qui ont été ingérées par les clients Swift. Swift ne prend pas en charge les demandes DE restauration POST-objet. StorageGRID ne pourra donc pas récupérer d'objets Swift ayant été transférés vers le niveau d'archivage du stockage Azure Blob Storage. L'émission d'une demande d'objet GET Swift pour récupérer ces objets échouera (403 interdit).

3. **L'objet a été transféré au niveau Archive (état non récupérable)**

   Immédiatement après le déplacement de l'objet vers le pool de stockage cloud Azure, StorageGRID transfère automatiquement l'objet vers le Tier d'archivage du stockage Azure Blob.

4. **Objet restauré à partir du niveau d'archive**

Si un objet a été migré vers le Tier d'archivage, l'application client peut lancer une demande de restauration S3 POST-objet pour restaurer une copie récupérable dans le pool de stockage cloud Azure.

Lorsqu'StorageGRID reçoit le POST-restauration d'objet, il transfère temporairement l'objet vers le Tier Azure Blob Storage Cool. Dès que la date d'expiration de la requête DE restauration POST-objet est atteinte, StorageGRID retransfère l'objet vers le niveau d'archivage.

> Si une ou plusieurs copies de l'objet existent également sur les nœuds de stockage dans StorageGRID, il n'est pas nécessaire de restaurer l'objet à partir du Tier d'accès Archive en émettant une demande de restauration POST-objet. En revanche, la copie locale peut être récupérée directement à l'aide d'une demande D'OBJET GET.

5. **Objet récupéré**

   Une fois qu'un objet a été restauré dans Azure Cloud Storage Pool, l'application client peut émettre une requête GET Object pour récupérer l'objet restauré.

Quand utiliser les pools de stockage cloud

Les pools de stockage cloud offrent des avantages significatifs dans plusieurs cas d'utilisation.

Sauvegarde des données StorageGRID dans un emplacement externe

Vous pouvez utiliser un pool de stockage cloud pour sauvegarder des objets StorageGRID dans un emplacement externe.

Si les copies dans StorageGRID sont inaccessibles, vous pouvez utiliser les données objet du pool de stockage cloud pour transmettre les requêtes des clients. Cependant, vous devrez peut-être émettre une demande de restauration S3 POST-objet pour accéder à la copie d'objet de sauvegarde dans le pool de stockage cloud.

Les données d'objet d'un pool de stockage cloud peuvent également être utilisées pour restaurer des données perdues à partir de StorageGRID en raison d'un volume de stockage ou d'une défaillance du nœud de stockage. Si la seule copie restante d'un objet se trouve dans un pool de stockage cloud, StorageGRID restaure temporairement l'objet et crée une nouvelle copie sur le nœud de stockage restauré.

Pour implémenter une solution de sauvegarde :

1. Créez un pool de stockage cloud unique.
2. Configurez une règle ILM pour stocker simultanément les copies d'objets sur les nœuds de stockage (en tant que copies répliquées ou avec code d'effacement) et une seule copie objet dans le pool de stockage cloud.
3. Ajoutez la règle à votre règle ILM. Ensuite, simuler et activer la règle.

Tiering des données du StorageGRID vers un emplacement externe

Vous pouvez utiliser un pool de stockage cloud pour stocker des objets en dehors du système StorageGRID. Supposons par exemple que vous disposez d'un grand nombre d'objets que vous devez conserver, mais que vous prévoyez d'accéder rarement à ces objets. Un pool de stockage cloud permet de classer les objets en fonction de leur coût de stockage et de libérer de l'espace dans StorageGRID.

Pour implémenter une solution de hiérarchisation :

1. Créez un pool de stockage cloud unique.
2. Configurez une règle ILM pour déplacer les objets rarement utilisés depuis les nœuds de stockage vers le pool de stockage cloud.
3. Ajoutez la règle à votre règle ILM. Ensuite, simuler et activer la règle.

Possibilité de gérer plusieurs terminaux cloud

Vous pouvez configurer plusieurs pools de stockage cloud si vous souhaitez hiérarchiser ou sauvegarder des données d'objet dans plusieurs clouds. Les filtres de vos règles ILM permettent de spécifier les objets qui sont stockés dans chaque pool de stockage cloud. Par exemple, vous pouvez stocker des objets à partir de certains locataires ou compartiments dans Amazon S3 Glacier et des objets à partir d'un autre locataire ou compartiments dans le stockage Azure Blob. Vous pouvez également déplacer des données entre Amazon S3 Glacier et le stockage Azure Blob. Si vous utilisez plusieurs pools de stockage cloud, n'oubliez pas qu'un objet ne peut être stocké que dans un seul pool de stockage cloud à la fois.

Pour implémenter plusieurs terminaux cloud :

1. Créez jusqu'à 10 pools de stockage cloud.
2. Configurez les règles ILM pour stocker les données d'objet appropriées au moment opportun dans chaque pool de stockage cloud. Stockez par exemple des objets à partir du compartiment A dans le pool de stockage cloud A et stockez des objets à partir du compartiment B dans le pool de stockage cloud B. Stockez les objets dans Cloud Storage Pool A pendant un certain temps, puis déplacez-les vers Cloud Storage Pool B.
3. Ajoutez les règles à votre politique ILM. Ensuite, simuler et activer la règle.

Considérations relatives aux pools de stockage cloud

Si vous envisagez d'utiliser un pool de stockage cloud pour déplacer les objets hors du système StorageGRID, vous devez étudier les critères de configuration et d'utilisation des pools de stockage cloud.

Considérations générales

- En général, le stockage d'archivage dans le cloud, comme Amazon S3 Glacier ou Azure Blob Storage, est un emplacement économique pour stocker les données d'objet. Mais le coût de la récupération des données à partir du stockage d'archivage dans le cloud est relativement élevé. Pour atteindre le coût global le plus bas, vous devez savoir quand et à quelle fréquence vous accéderez aux objets dans Cloud Storage Pool. L'utilisation d'un pool de stockage cloud est recommandée uniquement pour le contenu dont vous souhaitez accéder rarement.
- N'utilisez pas Cloud Storage pools pour les objets qui ont été ingérées par les clients Swift. Swift ne prend pas en charge les demandes DE restauration POST-objet. StorageGRID ne pourra donc pas récupérer d'objets Swift ayant été transférés vers le stockage Glacier S3 ou le Tier d'archivage du stockage Azure Blob Storage. L'émission d'une demande d'objet GET Swift pour récupérer ces objets échouera (403 interdit).
- L'utilisation de pools de stockage cloud avec FabricPool n'est pas prise en charge en raison de la latence ajoutée pour extraire un objet de la cible du pool de stockage cloud.

Informations requises pour la création d'un pool de stockage cloud

Avant de créer un pool de stockage cloud, vous devez créer un compartiment S3 externe ou le conteneur de stockage Azure Blob externe que vous utiliserez pour le pool de stockage cloud. Lorsque vous créez le pool de stockage cloud dans StorageGRID, vous devez spécifier les informations suivantes :

- Le type de fournisseur : stockage Amazon S3 ou Azure Blob.
- Si vous sélectionnez Amazon S3, que le pool de stockage cloud soit utilisé avec la région secrète AWS (**CAP (C2S Access Portal)**).
- Nom exact du godet ou du conteneur.
- Le terminal de service devait accéder au compartiment ou au conteneur.
- Pour accéder au compartiment ou au conteneur :
  - **S3** : en option, une clé d'accès et une clé secrète d'accès.
  - **C2S** : l'URL complète pour obtenir les informations d'identification temporaires du serveur CAP; un certificat d'autorité de certification de serveur, un certificat client, une clé privée pour le certificat client, et, si la clé privée est cryptée, la phrase de passe pour le déchiffrer.
  - **Stockage Azure Blob** : nom de compte et clé de compte. Ces informations d'identification doivent disposer d'une autorisation complète pour le conteneur.
- Un certificat d'autorité de certification personnalisé permet éventuellement de vérifier les connexions TLS avec le compartiment ou le conteneur.

Considérations relatives aux ports utilisés pour les pools de stockage cloud

Pour s'assurer que les règles ILM peuvent déplacer des objets vers et depuis le pool de stockage cloud spécifié, vous devez configurer le ou les réseaux contenant les nœuds de stockage du système. Vous devez vous assurer que les ports suivants peuvent communiquer avec le pool de stockage cloud.

Par défaut, les pools de stockage cloud utilisent les ports suivants :

- **80**: Pour les URI de point final commençant par http
- **443**: Pour les URI de point final qui commencent par https

Vous pouvez spécifier un autre port lorsque vous créez ou modifiez un pool de stockage cloud.

Si vous utilisez un serveur proxy non transparent, vous devez également configurer un proxy de stockage pour permettre l'envoi de messages vers des noeuds finaux externes, tels qu'un noeud final sur Internet.

Considérations relatives aux coûts

L'accès au stockage dans le cloud à l'aide d'un pool de stockage cloud requiert une connectivité réseau au cloud. Tenez compte des coûts de l'infrastructure réseau que vous utiliserez pour accéder au cloud et le provisionner de façon appropriée, en fonction de la quantité de données que vous prévoyez de déplacer entre StorageGRID et le cloud à l'aide du pool de stockage cloud.

Lorsque StorageGRID se connecte au terminal Cloud Storage Pool externe, plusieurs demandes de contrôle de la connectivité sont émises et les opérations nécessaires sont possibles. Un certain nombre de coûts supplémentaires seront associés à ces demandes, mais le coût de la surveillance d'un pool de stockage cloud ne doit être qu'une fraction du coût global du stockage d'objets dans S3 ou Azure.

Des coûts plus importants peuvent être encourus si vous devez déplacer des objets depuis un terminal externe

de pool de stockage dans le cloud vers StorageGRID. Les objets peuvent être redéplacés vers StorageGRID dans l'un ou l'autre de ces cas :

- La seule copie de l'objet se trouve dans un pool de stockage cloud et vous décidez de le stocker dans StorageGRID à la place. Dans ce cas, il vous suffit de reconfigurer les règles et les règles ILM. Lors de l'évaluation ILM, StorageGRID émet plusieurs demandes de récupération de l'objet à partir du pool de stockage cloud. StorageGRID crée ensuite le nombre spécifié de copies répliquées ou codées en local. Une fois que l'objet est de nouveau déplacé vers StorageGRID, la copie dans le pool de stockage cloud est supprimée.
- Les objets sont perdus en raison de la défaillance du nœud de stockage. Si la seule copie restante d'un objet se trouve dans un pool de stockage cloud, StorageGRID restaure temporairement l'objet et crée une nouvelle copie sur le nœud de stockage restauré.

> Lorsque les objets sont déplacés vers StorageGRID à partir d'un pool de stockage cloud, StorageGRID émet plusieurs requêtes vers le terminal de pool de stockage cloud pour chaque objet. Avant de déplacer un grand nombre d'objets, contactez le support technique pour obtenir de l'aide pour estimer le délai et les coûts associés.

S3 : autorisations requises pour le compartiment de pool de stockage cloud

La politique de compartiment pour le compartiment S3 externe utilisé pour un pool de stockage cloud doit autoriser StorageGRID à déplacer un objet vers le compartiment, à obtenir l'état d'un objet et à restaurer un objet à partir du stockage Glacier, le cas échéant, et bien plus encore. Dans l'idéal, StorageGRID doit disposer d'un accès total au compartiment (`s3:*`) ; Cependant, si ce n'est pas possible, la politique de compartiment doit accorder les autorisations S3 suivantes à StorageGRID :

- `s3:AbortMultipartUpload`
- `s3:DeleteObject`
- `s3:GetObject`
- `s3:ListBucket`
- `s3:ListBucketMultipartUploads`
- `s3:ListMultipartUploadParts`
- `s3:PutObject`
- `s3:RestoreObject`

S3 : considérations sur le cycle de vie du compartiment externe

Le déplacement des objets entre le StorageGRID et le compartiment S3 externe spécifié dans le pool de stockage cloud est contrôlé par les règles ILM et la politique ILM active dans StorageGRID. À l'inverse, la transition des objets à partir du compartiment S3 externe spécifié dans le pool de stockage cloud vers Amazon S3 Glacier ou S3 Glacier Deep Archive (ou vers une solution de stockage implémentant la classe de stockage Glacier) est contrôlée par la configuration du cycle de vie de ce compartiment.

Si vous souhaitez migrer des objets depuis le pool de stockage cloud, vous devez créer la configuration de cycle de vie appropriée sur un compartiment S3 externe. Vous devez d'autre part utiliser une solution de stockage implémentant la classe de stockage Glacier et prendre en charge l'API DE restauration POST-objet S3.

Supposons par exemple que vous souhaitiez que tous les objets déplacés d'StorageGRID vers le pool de

stockage cloud soient transférés immédiatement vers le stockage Amazon S3 Glacier. Vous devez créer une configuration de cycle de vie sur le compartiment S3 externe qui spécifie une seule action (**transition**) comme suit :

```
<LifecycleConfiguration>
  <Rule>
    <ID>Transition Rule</ID>
    <Filter>
       <Prefix></Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>0</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
  </Rule>
</LifecycleConfiguration>
```

Cette règle consiste à basculer tous les objets de compartiment vers Amazon S3 Glacier le jour de leur création (à savoir le jour où ils ont été déplacés d'StorageGRID vers le pool de stockage cloud).

> Lors de la configuration du cycle de vie du compartiment externe, n'utilisez jamais les actions **expiration** pour définir quand les objets arrivent à expiration. Les actions d'expiration entraînent la suppression des objets expirés par le système de stockage externe. Si vous tentez par la suite d'accéder à un objet expiré à partir de StorageGRID, l'objet supprimé est introuvable.

Pour migrer les objets du pool de stockage cloud vers l'archivage profond S3 Glacier (au lieu d'Amazon S3 Glacier), spécifiez `<StorageClass>DEEP_ARCHIVE</StorageClass>` pendant le cycle de vie du compartiment. Toutefois, sachez que vous ne pouvez pas utiliser le `Expedited` tiering pour restaurer des objets à partir d'une archive complète S3 Glacier.

Azure : considérations relatives au niveau d'accès

Lorsque vous configurez un compte de stockage Azure, vous pouvez définir le niveau d'accès par défaut sur chaud ou froid. Lorsque vous créez un compte de stockage à utiliser avec un pool de stockage cloud, vous devez utiliser le Tier actif comme niveau par défaut. Même si StorageGRID définit immédiatement le Tier sur Archive lors du déplacement d'objets vers le pool de stockage cloud, l'utilisation du paramètre par défaut de Hot garantit que vous ne serez pas facturé de frais de suppression anticipé pour les objets supprimés du Tier Cool avant le minimum de 30 jours.

Azure : gestion du cycle de vie non prise en charge

N'utilisez pas la fonctionnalité de gestion du cycle de vie du stockage Azure Blob Storage pour le conteneur utilisé avec un pool de stockage cloud. Toute interférence entre les opérations du cycle de vie du système Cloud Storage Pool.

Informations associées

"Création d'un pool de stockage cloud"

"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"

"Administrer StorageGRID"

Comparaison des pools de stockage cloud et de la réplication CloudMirror

Lorsque vous commencez à utiliser les pools de stockage cloud, il peut être utile d'étudier les similarités et les différences entre les pools de stockage cloud et le service de réplication StorageGRID CloudMirror.

	Pool de stockage cloud	**Service de réplication CloudMirror**
Quel est l'objectif principal ?	Un pool de stockage cloud agit comme cible d'archivage. La copie d'objet du pool de stockage cloud peut être la seule copie de l'objet ou une copie supplémentaire. Par exemple, au lieu de conserver deux copies sur site, vous ne pouvez conserver qu'une seule copie dans StorageGRID et envoyer une copie au pool de stockage cloud.	Le service de réplication CloudMirror permet à un locataire de répliquer automatiquement les objets depuis un compartiment dans StorageGRID (source) vers un compartiment S3 externe (destination). La réplication CloudMirror crée une copie indépendante d'un objet dans une infrastructure S3 indépendante.
Comment est-il configuré ?	Les pools de stockage cloud sont définis de la même manière que les pools de stockage, à l'aide de Grid Manager ou de l'API de gestion du grid. Un pool de stockage cloud peut être sélectionné comme emplacement dans une règle ILM. Lorsqu'un pool de stockage est constitué d'un groupe de nœuds de stockage, un pool de stockage cloud est défini à l'aide d'un terminal S3 ou Azure distant (adresse IP, identifiants, etc.).	Un utilisateur de locataire configure la réplication CloudMirror en définissant un terminal CloudMirror (adresse IP, identifiants, etc.) à l'aide du Gestionnaire des locataires ou de l'API S3. Une fois le terminal CloudMirror configuré, tous les compartiments appartenant à ce compte peuvent être configurés pour pointer vers le terminal CloudMirror.
Qui est responsable de sa configuration ?	En général, un administrateur grid	Généralement, un utilisateur locataire
Quelle est la destination ?	• Toute infrastructure S3 compatible (y compris Amazon S3) • Tier Azure Blob Archive	• Toute infrastructure S3 compatible (y compris Amazon S3)

	Pool de stockage cloud	Service de réplication CloudMirror
Pourquoi déplacer des objets vers la destination ?	Une ou plusieurs règles ILM de la politique ILM active. Les règles ILM définissent le déplacement des objets StorageGRID vers le pool de stockage cloud et le déplacement des objets.	Le fait d'ingérer un nouvel objet dans un compartiment source qui a été configuré avec un noeud final CloudMirror.les objets qui existaient dans le compartiment source avant que le compartiment n'ait été configuré avec le noeud final CloudMirror ne soient pas répliqués, à moins qu'ils ne soient modifiés.
Comment les objets sont-ils récupérés ?	Les applications doivent demander à StorageGRID de récupérer les objets qui ont été déplacés vers un pool de stockage cloud. Si la seule copie d'un objet a été transférée vers le stockage d'archivage, StorageGRID gère le processus de restauration de l'objet afin de pouvoir la récupérer.	Étant donné que la copie en miroir dans le compartiment de destination est une copie indépendante, les applications peuvent récupérer l'objet en effectuant des demandes vers StorageGRID ou vers la destination S3. Supposons, par exemple, que vous utilisiez la réplication CloudMirror pour mettre en miroir les objets dans une organisation partenaire. Le partenaire peut utiliser ses propres applications pour lire ou mettre à jour les objets directement à partir de la destination S3. Utiliser StorageGRID n'est pas nécessaire.
Pouvez-vous lire directement depuis la destination ?	Non Les objets déplacés vers un pool de stockage cloud sont gérés par StorageGRID. Les demandes de lecture doivent être dirigées vers StorageGRID (et StorageGRID sera responsable de la récupération à partir du pool de stockage cloud).	Oui, car la copie en miroir est une copie indépendante.
Que se passe-t-il si un objet est supprimé de la source ?	L'objet a également été supprimé dans le pool de stockage cloud.	L'action de suppression n'est pas répliquée. Un objet supprimé n'existe plus dans le compartiment StorageGRID, mais il continue d'exister dans le compartiment de destination. De même, les objets du compartiment de destination peuvent être supprimés sans affecter la source.
Comment accéder aux objets après un incident (le système StorageGRID n'est pas opérationnel) ?	Les nœuds StorageGRID défaillants doivent être récupérés. Au cours de ce processus, les copies des objets répliqués peuvent être restaurées à l'aide de copies dans le pool de stockage cloud.	Les copies d'objets de la destination CloudMirror sont indépendantes de StorageGRID, ce qui permet d'y accéder directement avant la restauration des nœuds StorageGRID.

Informations associées

"Administrer StorageGRID"

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.

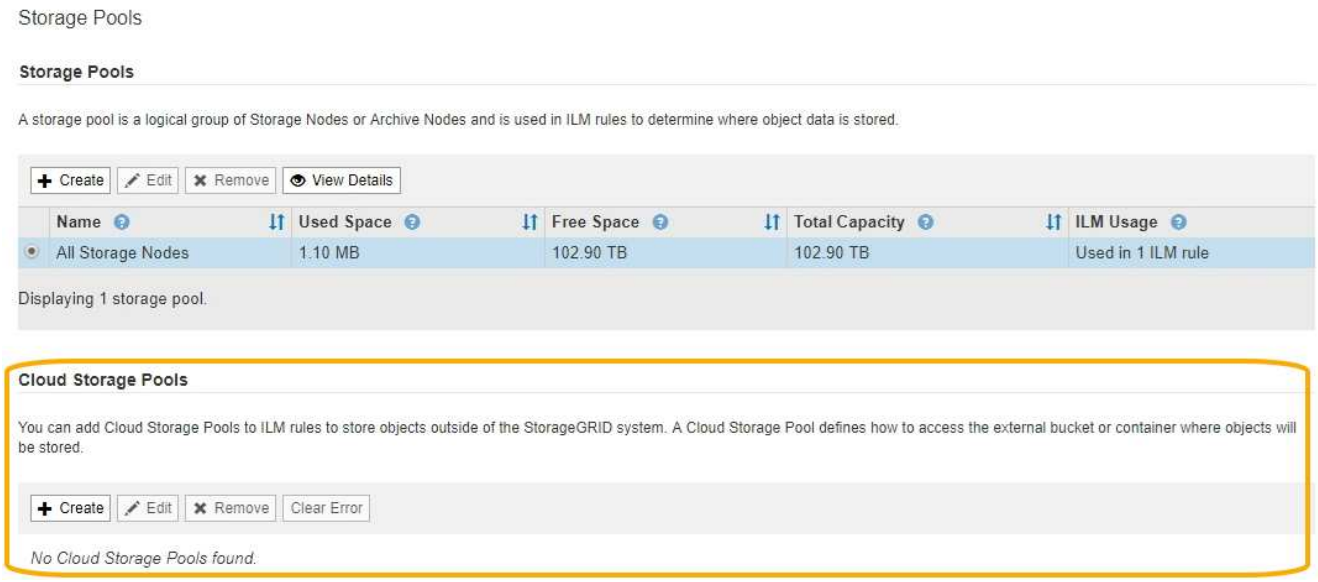
Description de la tâche

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.

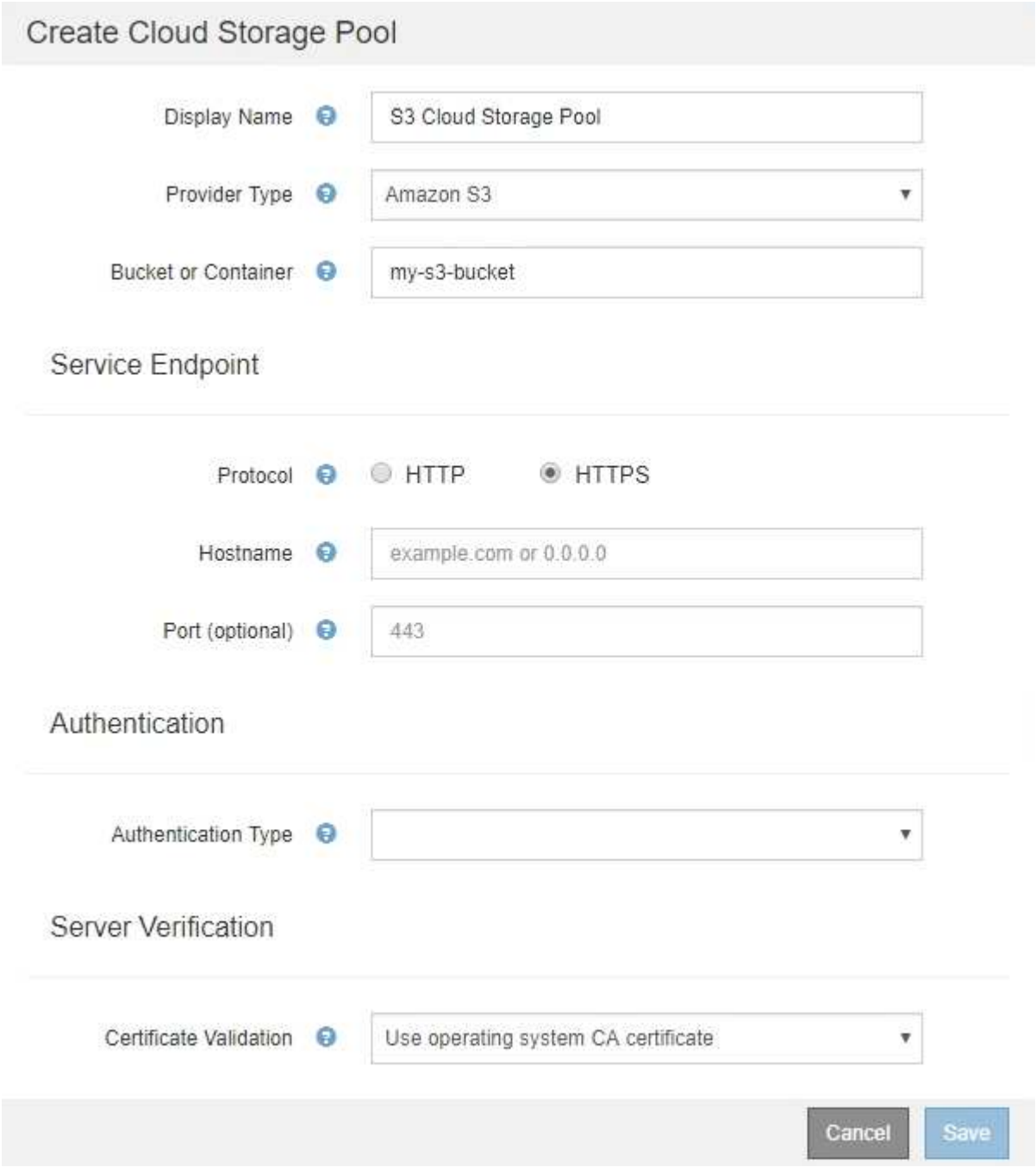
4. Complétez les sections point de terminaison de service, authentification et vérification du serveur de la page, en fonction du type de fournisseur sélectionné.
   - "S3 : spécification des détails d'authentification pour un pool de stockage cloud"
   - "C2S S3 : spécification des détails d'authentification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

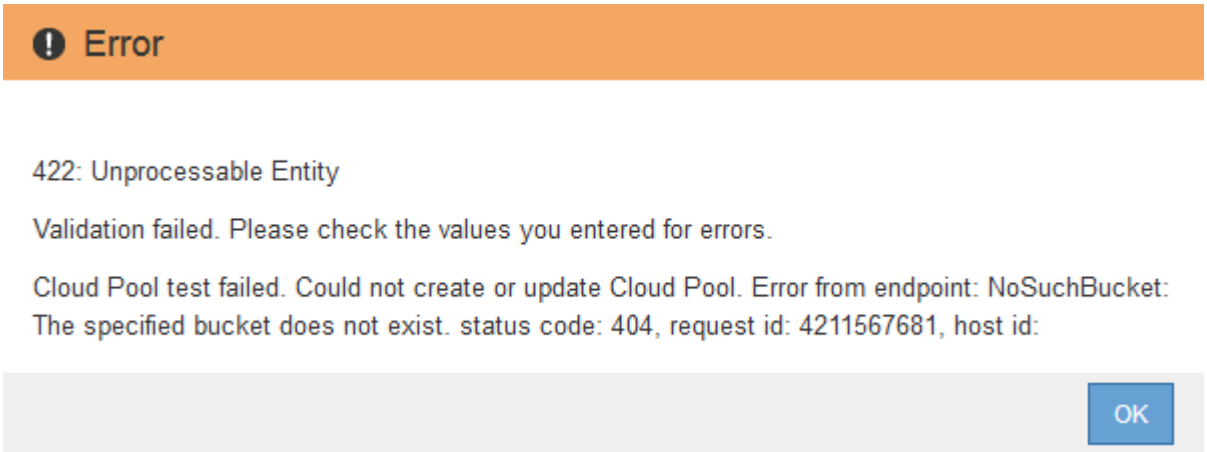
Option	Description
Utiliser le certificat CA du système d'exploitation	Utilisez les certificats CA par défaut installés sur le système d'exploitation pour sécuriser les connexions.
Utiliser un certificat d'autorité de certification personnalisé	Utilisez un certificat d'autorité de certification personnalisé. 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.

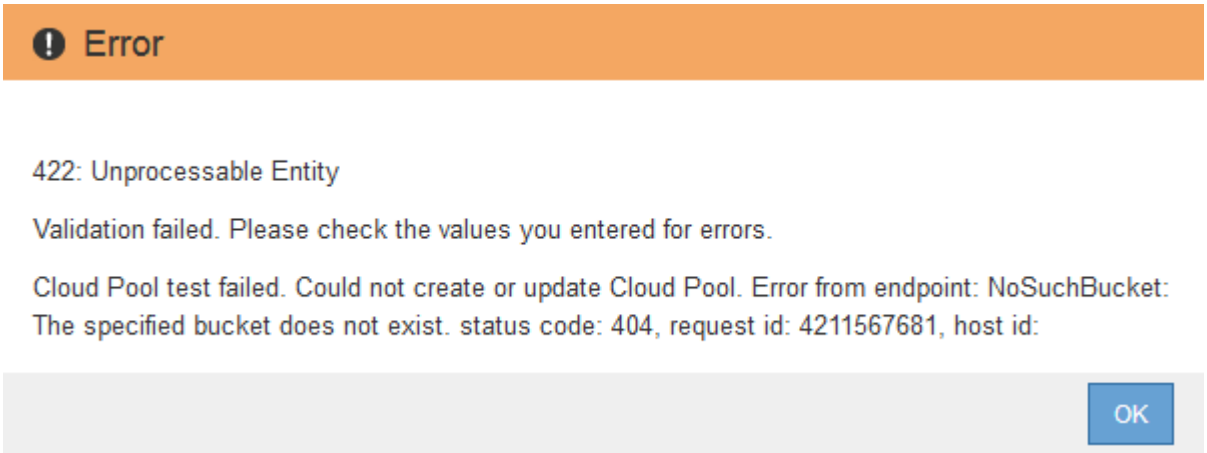
      Si la clé privée est cryptée, le format traditionnel doit être utilisé. (Le format crypté PKCS #8 n'est pas pris en charge.)

   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

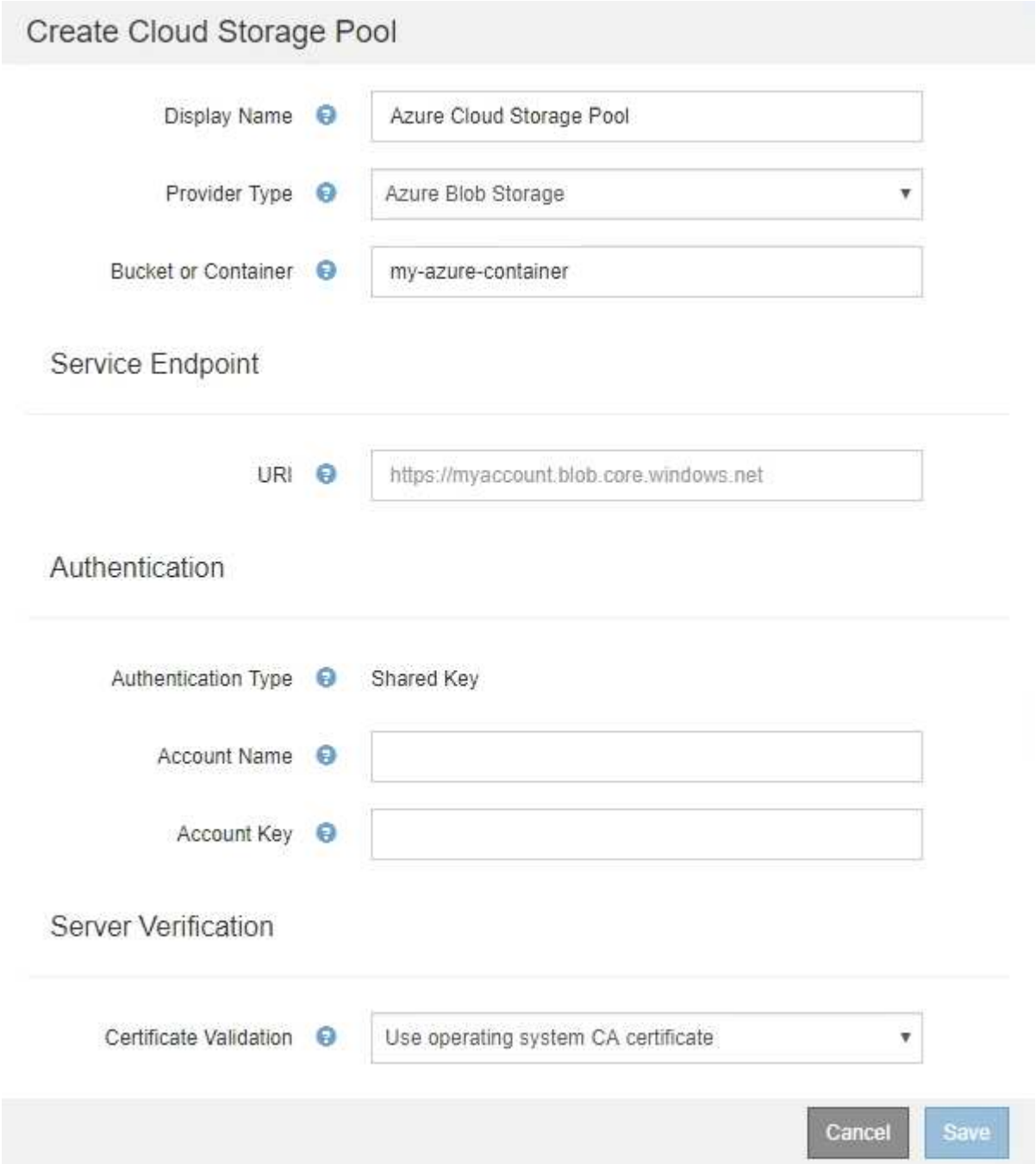
"Résolution des problèmes avec les pools de stockage cloud"

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"

Modification d'un pool de stockage cloud

Vous pouvez modifier un pool de stockage cloud pour en changer le nom, le terminal de service ou d'autres détails. Toutefois, vous ne pouvez pas modifier le compartiment S3 ou le conteneur Azure pour un pool de stockage cloud.

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.

Étapes

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

   La page Storage pools s'affiche. Le tableau Cloud Storage pools répertorie les pools de stockage cloud existants.

   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

	Pool Name	URI	Pool Type	Container	Used in ILM Rule	Last Error
◉	azure-endpoint	https://storagegrid.blob.core.windows.net	azure	azure-3	✔	
○	s3-endpoint	https://s3.amazonaws.com	s3	s3-1	✔	

   Displaying 2 pools.

2. Sélectionnez le bouton radio correspondant au pool de stockage cloud que vous souhaitez modifier.
3. Cliquez sur **Modifier**.
4. Si nécessaire, modifiez le nom d'affichage, le point de terminaison de service, les informations d'identification d'authentification ou la méthode de validation de certificat.

   > Vous ne pouvez pas modifier le type de fournisseur, le compartiment S3 ou le conteneur Azure pour un pool de stockage cloud.

   Si vous avez déjà téléchargé un certificat de serveur ou de client, vous pouvez sélectionner **Afficher actuel** pour vérifier le certificat actuellement utilisé.

5. Cliquez sur **Enregistrer**.

   Lorsque vous enregistrez un pool de stockage cloud, StorageGRID valide la présence du compartiment ou du conteneur et du terminal de service, et qu'ils peuvent être atteints à l'aide des identifiants que vous avez

spécifiés.

Si la validation du pool de stockage cloud échoue, un message d'erreur s'affiche. Par exemple, une erreur peut être signalée en cas d'erreur de certificat.

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

"Considérations relatives aux pools de stockage cloud"

"Résolution des problèmes avec les pools de stockage cloud"

Suppression d'un pool de stockage cloud

Vous pouvez supprimer un pool de stockage cloud qui n'est pas utilisé dans une règle ILM et qui ne contient pas de données d'objet.

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 avez confirmé que le compartiment S3 ou le conteneur Azure ne contient aucun objet. Une erreur se produit si vous tentez de supprimer un pool de stockage cloud s'il contient des objets. Voir « Dépannage des pools de stockage cloud ».

> Lorsque vous créez un pool de stockage cloud, StorageGRID écrit un fichier de marqueur vers le compartiment ou le conteneur pour l'identifier comme un pool de stockage cloud. Ne supprimez pas ce fichier, qui est nommé `x-ntap-sgws-cloud-pool-uuid`.

- Vous avez déjà supprimé toutes les règles ILM susceptibles d'avoir utilisé le pool.

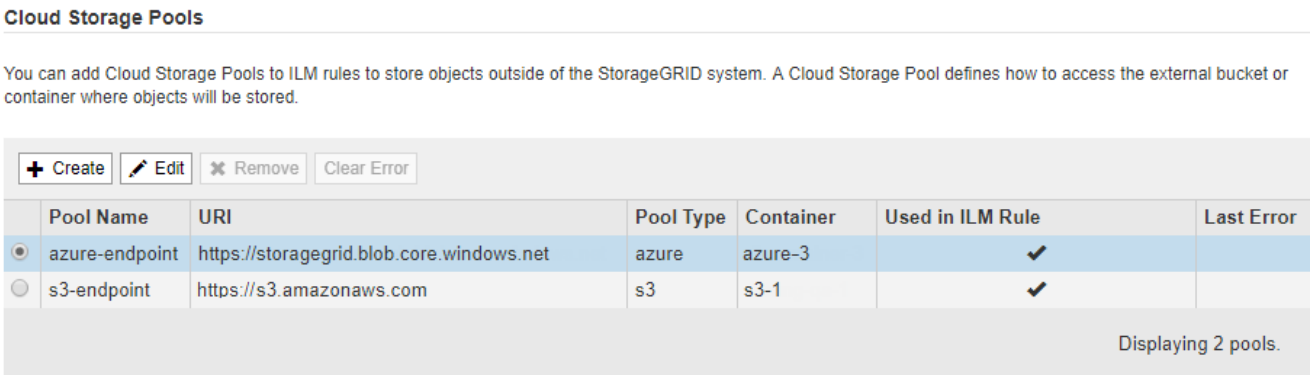
Étapes

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

   La page Storage pools s'affiche.

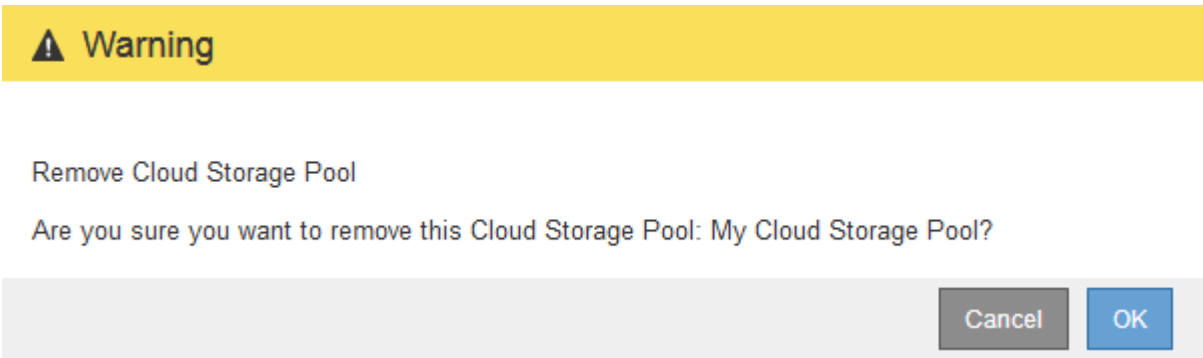
2. Sélectionnez le bouton radio d'un pool de stockage cloud qui n'est pas actuellement utilisé dans une règle ILM.

   Vous ne pouvez pas supprimer un pool de stockage cloud s'il est utilisé dans une règle ILM. Le bouton **Supprimer** est désactivé.



3. Cliquez sur **Supprimer**.

   Un avertissement de confirmation s'affiche.



4. Cliquez sur **OK**.

   Le pool de stockage cloud est supprimé.

Informations associées

"Résolution des problèmes avec les pools de stockage cloud"

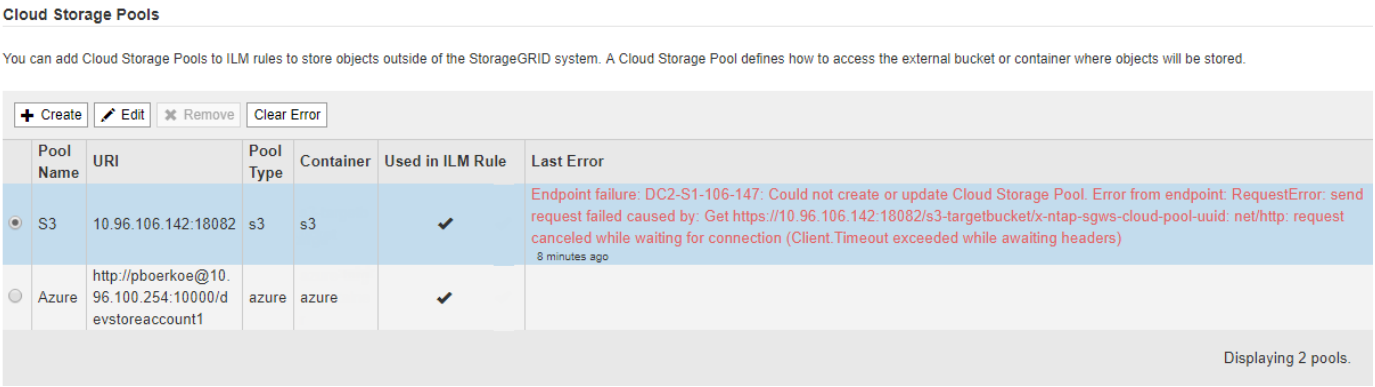
Résolution des problèmes avec les pools de stockage cloud

Si vous rencontrez des erreurs lors de la création, de la modification ou de la suppression d'un pool de stockage cloud, utilisez ces étapes de dépannage pour résoudre le problème.

Déterminer si une erreur s'est produite

StorageGRID effectue une vérification simple de l'état de santé de chaque pool de stockage cloud une fois par minute pour vérifier que celui-ci est accessible et qu'il fonctionne correctement. Si le contrôle de l'état de santé détecte un problème, un message s'affiche dans la colonne dernière erreur du tableau Cloud Storage pools sur la page Storage pools.

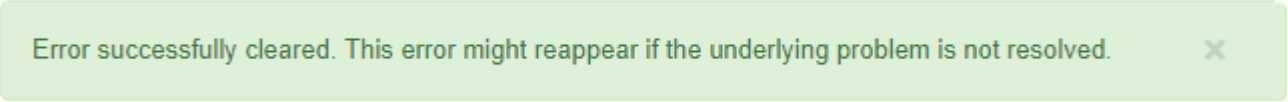
Le tableau indique la dernière erreur détectée pour chaque pool de stockage cloud et indique la durée de l'erreur.



En outre, une alerte **erreur** de connectivité de pool de stockage cloud est déclenchée si le contrôle d'intégrité détecte qu'une ou plusieurs nouvelles erreurs de pool de stockage cloud se sont produites au cours des 5 dernières minutes. Si vous recevez une notification par e-mail pour cette alerte, accédez à la page Storage Pool (sélectionnez **ILM** > **Storage pools**), examinez les messages d'erreur dans la colonne Last Error (dernière erreur) et reportez-vous aux instructions de dépannage ci-dessous.

Vérification de la résolution d'une erreur

Après avoir résolu les problèmes sous-jacents, vous pouvez déterminer si l'erreur a été résolue. Sur la page Cloud Storage Pool, sélectionnez le bouton radio du noeud final, puis cliquez sur **Effacer erreur**. Un message de confirmation indique que StorageGRID a résolu l'erreur pour le pool de stockage cloud.



Si le problème sous-jacent a été résolu, le message d'erreur ne s'affiche plus. Cependant, si le problème sous-jacent n'a pas été résolu (ou si une erreur différente est rencontrée), le message d'erreur s'affiche dans la colonne dernière erreur dans quelques minutes.

Erreur : ce pool de stockage cloud contient du contenu inattendu

Cette erreur peut se produire lorsque vous tentez de créer, modifier ou supprimer un pool de stockage cloud. Cette erreur se produit si le godet ou le conteneur inclut le `x-ntap-sgws-cloud-pool-uuid` Le fichier de marqueurs, mais ce fichier n'a pas l'UUID attendu.

En général, cette erreur s'affiche uniquement si vous créez un pool de stockage cloud et qu'une autre instance de StorageGRID utilise déjà le même pool de stockage cloud.

Essayez ces étapes pour corriger le problème :

- Assurez-vous que personne dans votre entreprise n'utilise également ce Cloud Storage Pool.
- Supprimez le `x-ntap-sgws-cloud-pool-uuid` Et essayez à nouveau de configurer le pool de stockage cloud.

Erreur : impossible de créer ou de mettre à jour le pool de stockage cloud. Erreur du noeud final

Cette erreur peut se produire lorsque vous tentez de créer ou de modifier un pool de stockage cloud. Cette erreur indique qu'un problème de connectivité ou de configuration empêche StorageGRID d'écrire dans le pool de stockage cloud.

Pour corriger le problème, consultez le message d'erreur du noeud final.

- Si le message d'erreur contient `Get *url*: EOF`, Vérifiez que le point de terminaison de service utilisé pour Cloud Storage Pool n'utilise pas le protocole HTTP pour un conteneur ou un compartiment qui nécessite HTTPS.
- Si le message d'erreur contient `Get *url*: net/http: request canceled while waiting for connection`, Vérifiez que la configuration réseau autorise les nœuds de stockage à accéder au terminal de service utilisé pour le pool de stockage cloud.
- Pour tous les autres messages d'erreur de point final, essayez un ou plusieurs des éléments suivants :
  - Créez un conteneur ou un compartiment externe avec le même nom que vous avez saisi pour le Cloud Storage Pool, et essayez à nouveau d'enregistrer le nouveau pool de stockage cloud.
  - Corrigez le nom de conteneur ou de compartiment que vous avez spécifié pour le pool de stockage cloud, et essayez de sauvegarder à nouveau le nouveau pool de stockage cloud.

Erreur : échec de l'analyse du certificat CA

Cette erreur peut se produire lorsque vous tentez de créer ou de modifier un pool de stockage cloud. L'erreur se produit si StorageGRID n'a pas pu analyser le certificat que vous avez saisi lors de la configuration du pool de stockage cloud.

Pour corriger le problème, vérifiez si le certificat CA que vous avez fourni ne présente pas de problèmes.

Erreur : un pool de stockage cloud associé à cet ID est introuvable

Cette erreur peut se produire lorsque vous essayez de modifier ou de supprimer un pool de stockage cloud. Cette erreur se produit si le noeud final renvoie une réponse 404, ce qui peut signifier l'un des éléments suivants :

- Les identifiants utilisés pour Cloud Storage Pool ne disposent pas d'une autorisation de lecture pour le compartiment.
- Le compartiment utilisé pour le pool de stockage cloud n'inclut pas la `x-ntap-sgws-cloud-pool-uuid` fichier de marqueur.

Essayez une ou plusieurs des étapes suivantes pour corriger le problème :

- Vérifiez que l'utilisateur associé à la clé d'accès configurée possède les autorisations requises.
- Modifiez le pool de stockage cloud avec des identifiants disposant des autorisations requises.
- Si les autorisations sont correctes, contactez l'assistance technique.

Erreur : impossible de vérifier le contenu du pool de stockage cloud. Erreur du noeud final

Cette erreur peut se produire lorsque vous tentez de supprimer un pool de stockage cloud. Cette erreur indique qu'un problème de connectivité ou de configuration empêche StorageGRID de lire le contenu du compartiment Cloud Storage Pool.

Pour corriger le problème, consultez le message d'erreur du noeud final.

Erreur : les objets ont déjà été placés dans ce compartiment

Cette erreur peut se produire lorsque vous tentez de supprimer un pool de stockage cloud. Vous ne pouvez pas supprimer un pool de stockage cloud si celui-ci contient des données déplacées par ILM, celles qui se trouvent dans le compartiment avant de configurer le pool de stockage cloud, ou celles qui ont été placées dans le compartiment par une autre source après la création du pool de stockage cloud.

Essayez une ou plusieurs des étapes suivantes pour corriger le problème :

- Suivez les instructions pour déplacer de nouveau des objets vers StorageGRID dans la section « cycle de vie d'un objet de pool de stockage cloud ».
- Si vous êtes certain que les objets restants n'ont pas été placés dans le pool de stockage cloud par ILM, supprimez manuellement les objets du compartiment.

> Ne supprimez jamais manuellement d'objets d'un pool de stockage cloud qui auraient pu y avoir été placés par ILM. Si vous tentez par la suite d'accéder à un objet supprimé manuellement à partir de StorageGRID, l'objet supprimé est introuvable.

Erreur : le proxy a rencontré une erreur externe lors de la tentative d'accès au pool de stockage cloud

Cette erreur peut se produire si vous avez configuré un proxy de stockage non transparent entre les nœuds de stockage et le terminal S3 externe utilisé pour le pool de stockage cloud. Cette erreur survient si le serveur proxy externe ne peut pas atteindre le terminal Cloud Storage Pool. Par exemple, il se peut que le serveur DNS ne puisse pas résoudre le nom d'hôte ou qu'il existe un problème de réseau externe.

Essayez une ou plusieurs des étapes suivantes pour corriger le problème :

- Vérifiez les paramètres de Cloud Storage Pool (**ILM** > **Storage pools**).
- Vérifiez la configuration réseau du serveur proxy de stockage.

Informations associées

"Cycle de vie d'un objet de pool de stockage cloud"