Utilisation des pools de stockage cloud

StorageGRID software

NetApp
January 14, 2026

Sommaire

Utilisation des pools de stockage cloud

Qu’est-ce qu’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 les objets rarement consultés vers un stockage cloud moins coûteux, comme Amazon S3 Glacier, S3 Glacier Deep Archive, Google Cloud ou le Tier d’accès Archive 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. Cependant, même si les pools de stockage sont constitués de nœuds de stockage dans le système StorageGRID, un pool de stockage cloud comprend un compartiment externe (S3) ou un conteneur (stockage Azure Blob).

Le tableau compare les pools de stockage aux pools de stockage cloud et montre les similarités et les différences de haut niveau.

	Pool de stockage	**Pool de stockage cloud**
Comment est-elle créée ?	Utilisation de l’option **ILM** > **Storage pools** dans Grid Manager.	Utilisation de l’option **ILM** > **Storage pools** > **Cloud 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 dans StorageGRID.	Dans un compartiment Amazon S3, un conteneur de stockage Azure Blob ou Google Cloud 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 RestoreObject S3. • 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 pour le conteneur utilisé pour un pool de stockage cloud. Les opérations RestoreObject sur les objets du pool de stockage cloud peuvent être affectées par le cycle de vie configuré.
Quels sont les contrôles du placement des objets ?	Règle ILM dans les politiques ILM actives.	Règle ILM dans les politiques ILM actives.
Quelle est la méthode de protection des données utilisée ?	La réplication ou le code d'effacement.	La réplication.
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 **Remarque** : les données FabricPool ne peuvent pas être hiérarchisées vers des pools de stockage cloud.

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.

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

Les étapes décrivent les étapes de cycle de vie d’un objet stocké dans un pool de stockage cloud S3.

> « Glacier » fait référence à la classe de stockage Glacier et Glacier Deep Archive, à une exception près : la classe de stockage Glacier Deep Archive ne prend pas en charge le niveau de restauration accélérée. Seule la récupération en bloc ou standard est prise en charge.

> Google Cloud Platform (GCP) prend en charge la récupération d’objets à partir d’un stockage à long terme sans nécessiter de POST-restauration.

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.
   - Une fois l’objet déplacé vers le pool de stockage cloud S3, l’application client peut le récupérer à l’aide d’une requête GetObject S3 de StorageGRID, sauf si l’objet a 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 d’objets, vous devez créer une configuration de cycle de vie pour le compartiment S3 externe et utiliser une solution de stockage qui implémente la classe de stockage Glacier et qui prend en charge l’API S3 RestoreObject.

   - Pendant la transition, l’application client peut utiliser une requête S3 HeadObject pour contrôler l’état de l’objet.
4. **Objet restauré à partir du stockage Glacier**

   Si un objet a été transféré vers le stockage Glacier, l’application client peut émettre une demande RestoreObject 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 en émettant une requête RestoreObject. À la place, la copie locale peut être récupérée directement à l'aide d'une requête GetObject.

5. **Objet récupéré**

   Une fois qu'un objet a été restauré, l'application client peut émettre une requête GetObject pour récupérer l'objet restauré.

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

Les étapes décrivent les étapes de 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 de placement, StorageGRID déplace l'objet vers le conteneur de stockage Azure Blob externe spécifié par le pool de stockage cloud.

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 transféré vers le niveau Archive, l'application client peut émettre une requête S3 RestoreObject pour restaurer une copie récupérable vers Azure Cloud Storage Pool.

   Lorsque StorageGRID reçoit l'objet RestoreObject, il le transfère temporairement vers le Tier Azure Blob Storage Cool. Dès que la date d'expiration de la requête RestoreObject est atteinte, StorageGRID ramène l'objet au niveau Archive.

   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 niveau d'accès aux archives en émettant une requête RestoreObject. À la place, la copie locale peut être récupérée directement à l'aide d'une requête GetObject.

5. **Objet récupéré**

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

Informations associées

"UTILISEZ L'API REST S3"

Quand utiliser les pools de stockage cloud

À l'aide des pools de stockage cloud, vous pouvez sauvegarder ou hiérarchiser les données vers un emplacement externe. En outre, vous pouvez sauvegarder ou déplacer des données vers plusieurs clouds.

Sauvegardez les 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 requête S3 RestoreObject 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.

Déplacez les données de 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 terminaux de pool de stockage cloud si vous souhaitez effectuer le Tiering ou la sauvegarde des données d'objet vers 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 de certains locataires ou compartiments dans Amazon S3 Glacier et des objets d'autres locataires ou compartiments dans le stockage Azure Blob. Vous pouvez également déplacer des données entre Amazon S3 Glacier et le stockage Azure Blob.

Lors de l'utilisation de plusieurs terminaux Cloud Storage Pool, 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. Par exemple, stockage des objets du compartiment A dans le pool de stockage cloud A, stockage des objets du compartiment B dans le pool de stockage cloud B. stockage cloud ou stockage des objets dans le pool de stockage cloud A pendant un certain temps, puis déplacement des objets vers le pool de stockage cloud 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.
- 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.
- Les objets avec le verrouillage d'objet S3 activé ne peuvent pas être placés dans les pools de stockage cloud.
- Les combinaisons de plateforme, d'authentification et de protocoles suivantes avec le verrouillage objet S3 ne sont pas prises en charge pour les pools de stockage cloud :
  - **Plateformes** : Google Cloud Platform et Azure
  - **Types d'authentification** : Accès anonyme
  - **Protocole** : HTTP

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"autoriser l'envoi de messages à des points finaux externes, tels qu'un point de terminaison 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, vous reconfigurez vos règles et votre règle 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

Les règles du compartiment S3 externe utilisé pour un pool de stockage cloud doivent accorder l'autorisation StorageGRID pour déplacer un objet vers le compartiment, obtenir l'état d'un objet, restaurer un objet depuis le stockage Glacier, le cas échéant, etc. Dans l'idéal, StorageGRID doit disposer d'un accès contrôle total au compartiment (`s3:*`). Toutefois, 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 d'objets entre StorageGRID et le compartiment S3 externe spécifié dans le pool de stockage cloud est contrôlé par des règles ILM et les règles ILM actives 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 effectuer la transition d'objets à partir de Cloud Storage Pool, vous devez créer la configuration de cycle de vie appropriée sur le compartiment S3 externe et utiliser une solution de stockage qui implémente la classe de stockage Glacier et prend en charge l'API S3 RestoreObject.

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.

Si vous souhaitez transférer des objets du pool de stockage cloud vers le service S3 Glacier Deep Archive (au lieu d'Amazon S3 Glacier), spécifiez le `<StorageClass>DEEP_ARCHIVE</StorageClass>` cycle de vie du compartiment. Cependant, notez que vous ne pouvez pas utiliser le `Expedited` Tier pour restaurer des objets à partir de S3 Glacier Deep Archive.

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 gestion du cycle de vie du stockage Azure Blob 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"

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 ?	Sert de cible d'archivage. La copie d'objet du pool de stockage cloud peut être la seule copie de l'objet ou une copie supplémentaire. Ainsi, au lieu de conserver deux copies sur site, vous pouvez conserver une copie dans StorageGRID et en envoyer une autre dans le pool de stockage cloud.	Permet à un locataire de répliquer automatiquement les objets à partir d'un compartiment dans StorageGRID (source) vers un compartiment S3 externe (destination). Crée une copie indépendante d'un objet dans une infrastructure S3 indépendante.
Comment est-il configuré ?	Défini de la même manière que les pools de stockage, à l'aide du gestionnaire de grille ou de l'API de gestion de grille. 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.).	Utilisateur 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

	Pool de stockage cloud	Service de réplication CloudMirror
Quelle est la destination ?	• Toute infrastructure S3 compatible (y compris Amazon S3) • Tier Azure Blob Archive • Google Cloud Platform (GCP)	• Toute infrastructure S3 compatible (y compris Amazon S3) • Google Cloud Platform (GCP)
Pourquoi déplacer des objets vers la destination ?	Une ou plusieurs règles ILM dans les politiques ILM actives. Les règles ILM définissent le déplacement des objets StorageGRID vers le pool de stockage cloud et le déplacement des objets.	Acte d'ingestion d'un nouvel objet dans un compartiment source configuré avec un terminal CloudMirror. Les objets qui existaient dans le compartiment source avant la configuration du compartiment avec le point de terminaison CloudMirror ne sont pas répliqués, sauf s'ils ont été 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 est également supprimé du 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.

	Pool de stockage cloud	Service de réplication CloudMirror
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.

Création d'un pool de stockage cloud

Un pool de stockage cloud désigne un compartiment Amazon S3 externe unique, un autre fournisseur compatible avec S3 ou un conteneur de stockage Azure Blob.

Lorsque vous créez un pool de stockage cloud, vous spécifiez le nom et l'emplacement du compartiment ou conteneur externe que StorageGRID utilisera pour stocker les objets, le type de fournisseur cloud (Amazon S3/GCP ou Azure Blob Storage), ainsi que les informations dont StorageGRID a besoin pour accéder au compartiment ou conteneur externe.

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.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur web pris en charge".
- Vous avez le "autorisations d'accès requises".
- Vous avez examiné le "Considérations relatives aux pools de stockage cloud".
- Le compartiment ou conteneur externe référencé par le pool de stockage cloud existe déjà, et vous disposez du informations sur le terminal de service.
- Pour accéder au godet ou au conteneur, vous avez le informations de compte pour le type d'authentificationchoix.

Étapes

1. Sélectionnez **ILM** > **Storage pools** > **Cloud Storage pools**.
2. Sélectionnez **Créer**, puis entrez les informations suivantes :

Champ	Description
Nom du pool de stockage cloud	Un nom qui décrit brièvement le pool de stockage cloud et son objectif. Nom facile à identifier lors de la configuration des règles ILM.

Champ	Description
Type de fournisseur	Quel fournisseur de cloud utiliser pour ce pool de stockage cloud : • **Amazon S3/GCP** : sélectionnez cette option pour Amazon S3, commercial Cloud Services (C2S) S3, Google Cloud Platform (GCP) ou un autre fournisseur compatible avec S3. • **Stockage Azure Blob**
Seau ou conteneur	Nom du compartiment S3 ou du conteneur Azure externe. Vous ne pouvez pas modifier cette valeur une fois le pool de stockage cloud enregistré.

3. en fonction de votre sélection de type de fournisseur, entrez les informations sur le noeud final du service.

Amazon S3/GCP

a. Pour le protocole, sélectionnez HTTPS ou HTTP.

> N'utilisez pas de connexions HTTP pour les données sensibles.

b. Entrez le nom d'hôte. Exemple :

`s3-aws-region.amazonaws.com`

c. Sélectionnez le style d'URL :

Option	Description
Détection automatique	Essayez de détecter automatiquement le style d'URL à utiliser, en fonction des informations fournies. Par exemple, si vous spécifiez une adresse IP, StorageGRID utilise une URL de style de chemin d'accès. Sélectionnez cette option uniquement si vous ne savez pas quel style spécifique utiliser.
De type hébergement virtuel	Utilisez une URL de type hébergement virtuel pour accéder au compartiment. Les URL de type hébergement virtuel incluent le nom de compartiment dans le nom de domaine. Exemple : `https://bucket-name.s3.company.com/key-name`
Style de trajectoire	Utilisez une URL de style de chemin d'accès pour accéder au compartiment. Les URL de type chemin d'accès incluent le nom du compartiment à la fin Exemple : `https://s3.company.com/bucket-name/key-name` **Note:** l'option URL de style chemin d'accès n'est pas recommandée et sera obsolète dans une future version de StorageGRID.

d. Vous pouvez également saisir le numéro de port ou utiliser le port par défaut : 443 pour HTTPS ou 80 pour HTTP.

Stockage Azure Blob Storage

a. À l'aide de l'un des formats suivants, entrez l'URI du point de terminaison de service.

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

Exemple : `https://myaccount.blob.core.windows.net:443`

Si vous ne spécifiez pas de port, le port 443 est utilisé par défaut pour HTTPS et le port 80 pour HTTP.

4. sélectionnez **continue**. Sélectionnez ensuite le type d'authentification et entrez les informations requises pour le terminal Cloud Storage Pool :

Touche d'accès

Pour Amazon S3/GCP ou tout autre fournisseur compatible avec S3

a. **ID de la clé d'accès** : saisissez l'ID de la clé d'accès du compte propriétaire du compartiment externe.
b. **Clé d'accès secrète** : saisissez la clé d'accès secrète.

Rôles IAM n'importe où

Pour le service AWS IAM Roles Anywhere

StorageGRID utilise AWS Security Token Service (STS) pour générer de manière dynamique un jeton de courte durée afin d'accéder aux ressources AWS.

a. **Région AWS IAM Roles Anywhere** : sélectionnez la région du pool de stockage cloud. Par exemple `us-east-1`, .
b. **Trust ancre URN** : saisissez l'URN de l'ancre de confiance qui valide les demandes d'informations d'identification STS à courte durée de vie. Peut être une AC racine ou intermédiaire.
c. **Profil URN** : saisissez l'URN du profil IAM Roles Anywhere qui répertorie les rôles qui sont présumés pour toute personne de confiance.
d. **Rôle URN** : saisissez l'URN du rôle IAM qui est assurable pour toute personne de confiance.
e. **Durée de la session** : saisissez la durée des informations d'identification de sécurité temporaires et de la session de rôle. Entrez au moins 15 minutes et au plus 12 heures.
f. **Certificat d'autorité de certification du serveur** (facultatif) : un ou plusieurs certificats d'autorité de certification approuvés, au format PEM, pour vérifier le serveur IAM Roles Anywhere. S'il est omis, le serveur ne sera pas vérifié.
g. **Certificat d'entité finale** : la clé publique, au format PEM, du certificat X509 signé par l'ancre de confiance. AWS IAM Roles Anywhere utilise cette clé pour émettre un jeton STS.
h. **Clé privée de l'entité finale** : clé privée du certificat de l'entité finale.

CAP (portail d'accès C2S)

Pour le service S3 de services cloud commerciaux (C2S)

a. **URL des informations d'identification temporaires** : saisissez l'URL complète que StorageGRID utilisera pour obtenir des informations d'identification temporaires du serveur CAP, y compris tous les paramètres d'API requis et facultatifs attribués à votre compte C2S.
b. **Certificat de l'autorité de certification du serveur** : sélectionnez **Parcourir** et téléchargez le certificat de l'autorité de certification que StorageGRID utilisera pour vérifier le serveur CAP. Le certificat doit être codé au format PEM et émis par une autorité de certification gouvernementale (AC) appropriée.
c. **Certificat client** : sélectionnez **Parcourir** et téléchargez le certificat que StorageGRID utilisera pour s'identifier sur le serveur CAP. Le certificat client doit être codé au format PEM, délivré par une autorité de certification gouvernementale (CA) appropriée et accordé l'accès à votre compte C2S.
d. **Clé privée client** : sélectionnez **Parcourir** et téléchargez la clé privée codée PEM pour le certificat client.
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 **phrase de passe de clé privée client** vide.

> Si le certificat client est crypté, utilisez le format traditionnel pour le chiffrement. Le format chiffré PKCS #8 n'est pas pris en charge.

Stockage Azure Blob Storage

Pour Azure Blob Storage, clé partagée uniquement

a. **Nom du compte** : saisissez le nom du compte de stockage qui possède le conteneur externe
b. **Clé de compte** : saisissez la clé secrète du compte de stockage

Utilisez le portail Azure pour trouver ces valeurs.

Anonyme

Aucune information supplémentaire n'est requise.

5. Sélectionnez **Continuer**. Choisissez ensuite le type de vérification du serveur que vous souhaitez utiliser :

Option	Description
Utilisez les certificats d'autorité de certification racine dans le système d'exploitation du nœud de stockage	Utilisez les certificats CA de la grille 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. Sélectionnez **Parcourir** et téléchargez le certificat codé PEM.
Ne vérifiez pas le certificat	Si vous sélectionnez cette option, les connexions TLS au pool de stockage cloud ne sont pas sécurisées.

6. Sélectionnez **Enregistrer**.

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

   - Vérifie que le compartiment ou le conteneur et le terminal de service existent et qu'ils peuvent être atteints à l'aide des informations d'identification que vous avez spécifiées.
   - Écrit un fichier de marqueur dans le compartiment ou le conteneur pour l'identifier en tant que pool de stockage cloud. Ne supprimez jamais ce fichier, qui est 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 ou le conteneur que vous avez spécifié n'existe pas déjà.

7. Si une erreur se produit, consultez le "Instructions de dépannage des pools de stockage cloud", résolvez les problèmes, puis essayez à nouveau d'enregistrer le pool de stockage cloud.

Afficher les détails du pool de stockage cloud

Vous pouvez afficher les détails d'un pool de stockage cloud pour déterminer où il est utilisé et voir quels nœuds et niveaux de stockage sont inclus.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur web pris en charge".
- Vous avez "autorisations d'accès spécifiques".

Étapes

1. Sélectionnez **ILM** > **Storage pools** > **Cloud Storage pools**.

   Le tableau pools de stockage cloud inclut les informations suivantes pour chaque pool de stockage cloud, y compris les nœuds de stockage :

   - **Nom** : le nom d'affichage unique du pool.
   - **URI** : l'identificateur de ressource uniforme du pool de stockage cloud.
   - **Type de fournisseur** : quel fournisseur de cloud est utilisé pour ce pool de stockage cloud.
   - **Container** : nom du compartiment utilisé pour le pool de stockage cloud.
   - **Utilisation ILM**: Comment le pool est actuellement utilisé. Un pool de stockage cloud peut être inutilisé ou être utilisé dans une ou plusieurs règles ILM, profils de code d'effacement, ou les deux.
   - **Dernière erreur** : dernière erreur détectée lors d'une vérification de l'intégrité de ce pool de stockage cloud.

2. Pour afficher les détails d'un pool de stockage cloud spécifique, sélectionnez son nom.

   La page de détails du pool s'affiche.

3. Consultez l'onglet **Authentication** pour en savoir plus sur le type d'authentification pour ce pool de stockage cloud et pour modifier les détails de l'authentification.
4. Consultez l'onglet **Vérification du serveur** pour en savoir plus sur les détails de la vérification, modifier la vérification, télécharger un nouveau certificat ou copier le certificat PEM.
5. Consultez l'onglet **ILM usage** pour déterminer si le pool de stockage cloud est actuellement utilisé dans des règles ILM ou des profils de code d'effacement.
6. Vous pouvez également accéder à la page **ILM rules** "découvrez et gérez toutes les règles"qui utilise le pool de stockage cloud.

Modifiez un pool de stockage cloud

Vous pouvez modifier un pool de stockage cloud pour modifier son nom, le point de terminaison de service ou d'autres informations. Cependant, vous ne pouvez pas modifier le compartiment S3 ou le conteneur Azure pour un pool de stockage cloud.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur web pris en charge".
- Vous avez "autorisations d'accès spécifiques".
- Vous avez examiné le "Considérations relatives aux pools de stockage cloud".

Étapes

1. Sélectionnez **ILM** > **Storage pools** > **Cloud Storage pools**.

   Le tableau Cloud Storage pools répertorie les pools de stockage cloud existants.

2. Cochez la case correspondant au pool de stockage cloud à modifier, puis sélectionnez **actions** > **Modifier**.

   Vous pouvez également sélectionner le nom du pool de stockage cloud, puis sélectionner **Modifier**.

3. Si nécessaire, modifiez le nom du pool de stockage cloud, le terminal du service, les paramètres d'authentification ou la méthode de vérification du 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 développer l'accordéon **Certificate Details** pour examiner le certificat actuellement utilisé.

4. Sélectionnez **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.

   Reportez-vous aux instructions de "Résolution des problèmes avec les pools de stockage cloud", résolvez le problème, puis essayez à nouveau d'enregistrer le pool de stockage cloud.

Supprimez un pool de stockage cloud

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

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur web pris en charge".
- Vous avez le "autorisations d'accès requises".

Si nécessaire, utilisez la règles ILM pour déplacer les données d'objet

Si le pool de stockage cloud que vous souhaitez supprimer contient des données d'objet, vous devez utiliser ILM pour déplacer les données vers un autre emplacement. Par exemple, vous pouvez déplacer les données vers des nœuds de stockage sur votre grille ou vers un autre pool de stockage cloud.

Étapes

1. Sélectionnez **ILM** > **Storage pools** > **Cloud Storage pools**.
2. Consultez la colonne utilisation ILM du tableau pour déterminer si vous pouvez supprimer le pool de stockage cloud.

   Vous ne pouvez pas supprimer un pool de stockage cloud s'il est utilisé dans une règle ILM ou dans un

profil de code d'effacement.

3. Si le pool de stockage cloud est utilisé, sélectionnez ***cloud Storage pool name*** > **ILM usage**.
4. "Clonez chaque règle ILM" Qui place actuellement les objets dans le pool de stockage cloud que vous souhaitez supprimer.
5. Déterminez l'emplacement où vous souhaitez déplacer les objets existants gérés par chaque règle clonée.

   Vous pouvez utiliser un ou plusieurs pools de stockage ou un autre pool de stockage cloud.

6. Editez chacune des règles que vous avez clonées.

   Pour l'étape 2 de l'assistant Créer une règle ILM, sélectionnez le nouvel emplacement dans le champ **copies AT**.

7. "Création d'une règle ILM" et remplacez chacune des anciennes règles par une règle clonée.
8. Activer la nouvelle règle.
9. Attendez que ILM supprime les objets du pool de stockage cloud et les place à un nouvel emplacement.

Supprimer le pool de stockage cloud

Lorsque le pool de stockage cloud est vide et qu'il n'est utilisé dans aucune règle ILM, vous pouvez le supprimer.

Avant de commencer

- Vous avez supprimé toutes les règles ILM qui auraient pu utiliser le pool.
- 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 "Résoudre les problèmes liés aux 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`.

Étapes

1. Sélectionnez **ILM** > **Storage pools** > **Cloud Storage pools**.
2. Si la colonne utilisation d'ILM indique que Cloud Storage Pool n'est pas utilisé, cochez la case.
3. Sélectionnez **actions** > **Supprimer**.
4. Sélectionnez **OK**.

Résoudre les problèmes liés aux pools de stockage cloud

Suivez ces étapes de dépannage pour résoudre les erreurs que vous pouvez rencontrer lors de la création, de la modification ou de la suppression d'un pool de stockage cloud.

Déterminez si une erreur s'est produite

StorageGRID effectue un simple contrôle de l'état de santé de chaque pool de stockage cloud en lisant l'objet

connu `x-ntap-sgws-cloud-pool-uuid` pour s'assurer que le pool de stockage cloud est accessible et qu'il fonctionne correctement. Lorsque StorageGRID rencontre une erreur sur le noeud final, il vérifie l'état de santé toutes les minutes depuis chaque noeud de stockage. Une fois l'erreur résolue, les vérifications de l'état de santé s'arrêtent. Si une vérification de l'état de santé détecte un problème, un message s'affiche dans la colonne dernière erreur du tableau pools de stockage cloud de la page pools de stockage cloud.

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 pools (sélectionnez **ILM** > **Storage pools**), consultez les messages d'erreur dans la colonne Last error (dernière erreur) et reportez-vous aux instructions de dépannage ci-dessous.

Vérifiez si une erreur a été résolue

Après avoir résolu les problèmes sous-jacents, vous pouvez déterminer si l'erreur a été résolue. Sur la page Cloud Storage Pool, sélectionnez le noeud final, puis sélectionnez **Clear error**. 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. Toutefois, 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 les minutes qui suivent.

Erreur : échec de la vérification de l'état de santé. Erreur du noeud final

Cette erreur peut se produire lorsque vous activez le verrouillage objet S3 avec conservation par défaut pour votre compartiment Amazon S3 après avoir commencé à utiliser ce compartiment pour un pool de stockage cloud. Cette erreur se produit lorsque l'opération PUT ne possède pas d'en-tête HTTP avec une valeur de somme de contrôle de charge telle que `Content-MD5`. Cette valeur d'en-tête est requise par AWS pour les opérations PUT dans des compartiments avec le verrouillage objet S3 activé.

Pour corriger ce problème, suivez les étapes de la section "Modifiez un pool de stockage cloud" sans apporter de modifications. Cette action déclenche la validation de la configuration de pool de stockage cloud qui détecte et met à jour automatiquement l'indicateur de verrouillage d'objet S3 sur une configuration de terminal de pool de stockage cloud.

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 compartiment ou le conteneur inclut le `x-ntap-sgws-cloud-pool-uuid` fichier de marqueur, mais que ce fichier ne possède pas le champ de métadonnées avec 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 l'une des étapes suivantes pour corriger le problème :

- Si vous configurez un nouveau pool de stockage cloud et que le compartiment contient le `x-ntap-sgws-cloud-pool-uuid` fichier et les clés d'objet supplémentaires, comme dans l'exemple suivant, créez un nouveau compartiment et utilisez ce nouveau compartiment.

  Exemple de clé d'objet supplémentaire : `my-bucket.3E64CF2C-B74D-4B7D-AFE7-`

`AD28BC18B2F6.1727326606730410`

- Si le `x-ntap-sgws-cloud-pool-uuid` fichier est le seul objet du compartiment, supprimez ce fichier.

Si ces étapes ne s'appliquent pas à votre scénario, contactez l'assistance.

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

Vous pouvez rencontrer cette erreur dans les circonstances suivantes :

- Lorsque vous essayez de créer ou de modifier un pool de stockage cloud.
- Lorsque vous sélectionnez une plateforme, une authentification ou une combinaison de protocoles non pris en charge avec S3 Object Lock lors de la configuration d'un nouveau pool de stockage cloud. Voir "Considérations relatives aux pools 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 terminal de service utilisé pour le pool de stockage cloud n'utilise pas 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 permet aux nœuds de stockage d'accéder au point de terminaison de service utilisé pour le pool de stockage cloud.
- Si l'erreur est due à une plateforme, une authentification ou un protocole non pris en charge, passez à une configuration prise en charge avec le verrouillage objet S3 et essayez à nouveau d'enregistrer le nouveau 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 le pool de stockage cloud ne disposent pas des autorisations de lecture pour le compartiment.

- Le compartiment utilisé pour le pool de stockage cloud n'inclut pas le `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 s'il contient des données qui y ont été déplacées par ILM, des données qui se trouvait dans le compartiment avant la configuration du pool de stockage cloud, ou des données 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 se produit si le serveur proxy externe ne parvient pas à 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.

Erreur : le certificat X.509 est hors période de validité

Cette erreur peut se produire lorsque vous tentez de supprimer un pool de stockage cloud. Cette erreur se produit lorsque l'authentification nécessite un certificat X.509 pour s'assurer que le pool de stockage cloud externe correct est validé et que le pool externe est vide avant la suppression de la configuration du pool de stockage cloud.

Essayez ces étapes pour corriger le problème :

- Mettez à jour le certificat configuré pour l'authentification vers le pool de stockage cloud.
- Assurez-vous que toute alerte d'expiration de certificat relative à ce pool de stockage cloud est résolue.

Informations associées

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