



Gérer les buckets S3

StorageGRID software

NetApp

December 03, 2025

Sommaire

Gérer les buckets S3	1
Créer un bucket S3	1
Accéder à l'assistant	1
Entrez les détails	1
Gérer les paramètres	2
Afficher les détails du godet	4
Appliquer une balise de stratégie ILM à un bucket	6
Gérer la politique de compartiment	7
Gérer la cohérence des buckets	8
Directives relatives à la cohérence des seaux	8
Modifier la cohérence du bucket	8
Que se passe-t-il lorsque vous modifiez les paramètres du bucket	9
Activer ou désactiver les mises à jour de l'heure du dernier accès	10
Modifier la version d'objet pour un bucket	12
Utilisez S3 Object Lock pour conserver les objets	13
Qu'est-ce que S3 Object Lock ?	13
Tâches de verrouillage d'objet S3	15
Exigences pour les buckets avec S3 Object Lock activé	15
Exigences relatives aux objets dans les compartiments avec le verrouillage d'objet S3 activé	16
Cycle de vie des objets dans les buckets avec S3 Object Lock activé	16
Puis-je toujours gérer les buckets conformes hérités ?	16
Mettre à jour la conservation par défaut du verrouillage des objets S3	17
Configurer le partage de ressources inter-origines (CORS)	18
Activer CORS pour un bucket	19
Modifier le paramètre CORS	19
Désactiver le paramètre CORS	20
Supprimer les objets dans le bucket	20
Supprimer le compartiment S3	23
Utiliser la console S3	24

Gérer les buckets S3

Créer un bucket S3

Vous pouvez utiliser Tenant Manager pour créer des compartiments S3 pour les données d'objet.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un [navigateur Web pris en charge](#) .
- Vous appartenez à un groupe d'utilisateurs disposant de l'accès Root ou Gérer tous les buckets [autorisation](#) . Ces autorisations remplacent les paramètres d'autorisations dans les stratégies de groupe ou de compartiment.



Les autorisations permettant de définir ou de modifier les propriétés de verrouillage d'objet S3 des compartiments ou des objets peuvent être accordées par [politique de compartiment](#) ou [politique de groupe](#) .

- Si vous prévoyez d'activer le verrouillage d'objet S3 pour un bucket, un administrateur de grille a activé le paramètre global de verrouillage d'objet S3 pour le système StorageGRID et vous avez examiné les exigences pour les buckets et objets de verrouillage d'objet S3.
- Si chaque locataire dispose de 5 000 buckets, chaque nœud de stockage de la grille dispose d'un minimum de 64 Go de RAM.



Chaque grille peut contenir un maximum de 100 000 buckets.

Accéder à l'assistant

Étapes

1. Sélectionnez **Afficher les buckets** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > Buckets**.
2. Sélectionnez **Créer un bucket**.

Entrez les détails

Étapes

1. Saisissez les détails du bucket.

Champ	Description
Nom du bucket	<p>Un nom pour le bucket qui respecte ces règles :</p> <ul style="list-style-type: none"> • Doit être unique sur chaque système StorageGRID (pas seulement unique au sein du compte locataire). • Doit être conforme au DNS. • Doit contenir au moins 3 et pas plus de 63 caractères. • Chaque étiquette doit commencer et se terminer par une lettre minuscule ou un chiffre et ne peut utiliser que des lettres minuscules, des chiffres et des traits d'union. • Ne doit pas contenir de points dans les demandes de style hébergé virtuellement. Les points entraîneront des problèmes avec la vérification du certificat générique du serveur. <p>Pour plus d'informations, consultez le "Documentation d'Amazon Web Services (AWS) sur les règles de dénomination des buckets" .</p> <p>Remarque : vous ne pouvez pas modifier le nom du bucket après l'avoir créé.</p>
Région	<p>La région du seau.</p> <p>Votre administrateur StorageGRID gère les régions disponibles. La région d'un bucket peut affecter la politique de protection des données appliquée aux objets. Par défaut, tous les buckets sont créés dans le <code>us-east-1</code> région.</p> <p>Remarque : vous ne pouvez pas modifier la région après avoir créé le bucket.</p>

2. Sélectionnez **Continuer**.

Gérer les paramètres

Étapes

1. Vous pouvez également activer le contrôle de version des objets pour le bucket.

Activez le contrôle de version des objets si vous souhaitez stocker chaque version de chaque objet dans ce bucket. Vous pouvez ensuite récupérer les versions précédentes d'un objet selon vos besoins. Vous devez activer le contrôle de version des objets si le bucket doit être utilisé pour la réplication inter-grille.

2. Si le paramètre global de verrouillage d'objet S3 est activé, activez éventuellement le verrouillage d'objet S3 pour que le bucket stocke les objets à l'aide d'un modèle WORM (écriture unique, lecture multiple).

Activez le verrouillage d'objet S3 pour un bucket uniquement si vous devez conserver des objets pendant une durée déterminée, par exemple pour répondre à certaines exigences réglementaires. S3 Object Lock est un paramètre permanent qui vous aide à empêcher la suppression ou l'écrasement d'objets pendant une durée déterminée ou indéfiniment.



Une fois le paramètre de verrouillage d'objet S3 activé pour un bucket, il ne peut pas être désactivé. Toute personne disposant des autorisations appropriées peut ajouter des objets à ce bucket qui ne peuvent pas être modifiés. Vous ne pourrez peut-être pas supprimer ces objets ni le bucket lui-même.

Si vous activez le verrouillage d'objet S3 pour un bucket, le contrôle de version du bucket est activé automatiquement.

3. Si vous avez sélectionné **Activer le verrouillage d'objet S3**, activez éventuellement la **Rétention par défaut** pour ce bucket.



Votre administrateur de réseau doit vous donner la permission de "[utiliser les fonctionnalités spécifiques de S3 Object Lock](#)".

Lorsque la **rétention par défaut** est activée, les nouveaux objets ajoutés au bucket seront automatiquement protégés contre la suppression ou l'écrasement. Le paramètre **Conservation par défaut** ne s'applique pas aux objets qui ont leurs propres périodes de conservation.

- a. Si la **Rétention par défaut** est activée, spécifiez un **Mode de rétention par défaut** pour le bucket.

Mode de rétention par défaut	Description
Gouvernance	<ul style="list-style-type: none">• Les utilisateurs avec le <code>s3:BypassGovernanceRetention</code> l'autorisation peut utiliser le <code>x-amz-bypass-governance-retention: true</code> en-tête de demande pour contourner les paramètres de conservation.• Ces utilisateurs peuvent supprimer une version d'objet avant que sa date de conservation ne soit atteinte.• Ces utilisateurs peuvent augmenter, diminuer ou supprimer la date de conservation d'un objet.
Conformité	<ul style="list-style-type: none">• L'objet ne peut pas être supprimé tant que sa date de conservation n'est pas atteinte.• La date de conservation de l'objet peut être augmentée, mais elle ne peut pas être diminuée.• La date de conservation de l'objet ne peut pas être supprimée tant que cette date n'est pas atteinte. <p>Remarque : votre administrateur de réseau doit vous autoriser à utiliser le mode de conformité.</p>

- b. Si la **Conservation par défaut** est activée, spécifiez la **Période de conservation par défaut** pour le bucket.

La **Période de conservation par défaut** indique la durée pendant laquelle les nouveaux objets ajoutés à ce bucket doivent être conservés, à compter du moment où ils sont ingérés. Spécifiez une valeur inférieure ou égale à la période de conservation maximale du locataire, telle que définie par l'administrateur de la grille.

Une période de conservation *maximale*, qui peut être une valeur comprise entre 1 jour et 100 ans, est définie lorsque l'administrateur de la grille crée le locataire. Lorsque vous définissez une période de conservation par défaut, elle ne peut pas dépasser la valeur définie pour la période de conservation maximale. Si nécessaire, demandez à votre administrateur de réseau d'augmenter ou de diminuer la période de conservation maximale.

4. Vous pouvez également sélectionner **Activer la limite de capacité**.

La limite de capacité est la capacité maximale disponible pour les objets de ce bucket. Cette valeur représente une quantité logique (taille de l'objet), et non une quantité physique (taille sur le disque).

Si aucune limite n'est définie, la capacité de ce bucket est illimitée. Consultez ["Utilisation de la limite de capacité"](#) pour plus d'informations.

5. Sélectionnez **Créer un bucket**.

Le bucket est créé et ajouté au tableau sur la page Buckets.

6. En option, sélectionnez **Accéder à la page des détails du bucket** pour ["afficher les détails du godet"](#) et effectuer une configuration supplémentaire.

Afficher les détails du godet

Vous pouvez afficher les buckets dans votre compte locataire.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Accès root, autorisation Gérer tous les buckets ou Afficher tous les buckets"](#). Ces autorisations remplacent les paramètres d'autorisation dans les stratégies de groupe ou de compartiment.

Étapes

1. Sélectionnez **Afficher les buckets** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > Buckets**.

La page Buckets apparaît.

2. Consultez le tableau récapitulatif pour chaque compartiment.

Selon vos besoins, vous pouvez trier les informations par colonne ou parcourir la liste en avant et en arrière.



Les valeurs de nombre d'objets, d'espace utilisé et d'utilisation affichées sont des estimations. Ces estimations sont affectées par le moment des ingestions, la connectivité réseau et l'état du nœud. Si le contrôle de version est activé pour les buckets, les versions d'objet supprimées sont incluses dans le nombre d'objets.

Nom

Le nom unique du bucket, qui ne peut pas être modifié.

Fonctionnalités activées

La liste des fonctionnalités activées pour le bucket.

Verrouillage d'objet S3

Si le verrouillage d'objet S3 est activé pour le bucket.

Cette colonne apparaît uniquement si le verrouillage d'objet S3 est activé pour la grille. Cette colonne affiche également des informations sur tous les buckets conformes hérités.

Région

La région du bucket, qui ne peut pas être modifiée. Cette colonne est masquée par défaut.

Nombre d'objets

Le nombre d'objets dans ce bucket. Si le contrôle de version est activé pour les buckets, les versions d'objet non actuelles sont incluses dans cette valeur.

Lorsque des objets sont ajoutés ou supprimés, cette valeur peut ne pas être mise à jour immédiatement.

Espace utilisé

La taille logique de tous les objets dans le bucket. La taille logique n'inclut pas l'espace réel requis pour les copies répliquées ou codées par effacement ou pour les métadonnées de l'objet.

La mise à jour de cette valeur peut prendre jusqu'à 10 minutes.

Usage

Le pourcentage utilisé de la limite de capacité du bucket, si elle a été définie.

La valeur d'utilisation est basée sur des estimations internes et peut être dépassée dans certains cas. Par exemple, StorageGRID vérifie la limite de capacité (si définie) lorsqu'un locataire commence à télécharger des objets et rejette les nouvelles ingestions dans ce bucket si le locataire a dépassé la limite de capacité. Cependant, StorageGRID ne prend pas en compte la taille du téléchargement actuel pour déterminer si la limite de capacité a été dépassée. Si des objets sont supprimés, un locataire peut être temporairement empêché de télécharger de nouveaux objets dans ce bucket jusqu'à ce que l'utilisation de la limite de capacité soit recalculée. Les calculs peuvent prendre 10 minutes ou plus.

Cette valeur indique la taille logique, et non la taille physique nécessaire pour stocker les objets et leurs métadonnées.

Capacité

Si défini, la limite de capacité du bucket.

Date de création

La date et l'heure de création du bucket. Cette colonne est masquée par défaut.

3. Pour afficher les détails d'un bucket spécifique, sélectionnez le nom du bucket dans le tableau.
 - a. Consultez les informations récapitulatives en haut de la page Web pour confirmer les détails du bucket, tels que la région et le nombre d'objets.
 - b. Affichez la barre d'utilisation de la limite de capacité. Si l'utilisation est de 100 % ou proche de 100 %, envisagez d'augmenter la limite ou de supprimer certains objets.
 - c. Si nécessaire, sélectionnez **Supprimer les objets dans le bucket** et **Supprimer le bucket**.



Portez une attention particulière aux avertissements qui s'affichent lorsque vous sélectionnez chacune de ces options. Pour plus d'informations, reportez-vous à :

- ["Supprimer tous les objets d'un bucket"](#)
- ["Supprimer un bucket"](#)(le seau doit être vide)

- d. Affichez ou modifiez les paramètres du bucket dans chacun des onglets selon vos besoins.
 - **Console S3** : Affichez les objets du bucket. Pour plus d'informations, reportez-vous à ["Utiliser la](#)

[console S3](#) .

- **Options du bucket** : afficher ou modifier les paramètres des options. Certains paramètres, tels que le verrouillage d'objet S3, ne peuvent pas être modifiés une fois le bucket créé.
 - ["Gérer la cohérence des buckets"](#)
 - ["Mises à jour de l'heure du dernier accès"](#)
 - ["Limite de capacité"](#)
 - ["Versionnage d'objet"](#)
 - ["Verrouillage d'objet S3"](#)
 - ["Rétention du bucket par défaut"](#)
 - ["Gérer la réplication inter-réseaux"](#)(si autorisé pour le locataire)
- **Services de la plateforme:**["Gérer les services de la plateforme"](#) (si autorisé pour le locataire)
- **Accès au bucket** : afficher ou modifier les paramètres des options. Vous devez disposer d'autorisations d'accès spécifiques.
 - Configurez ["Partage des ressources inter-origines \(CORS\)"](#) ainsi, le bucket et les objets qu'il contient seront accessibles aux applications Web dans d'autres domaines.
 - ["Contrôler l'accès des utilisateurs"](#) pour un bucket S3 et les objets dans ce bucket.

Appliquer une balise de stratégie ILM à un bucket

Choisissez une balise de stratégie ILM à appliquer à un bucket en fonction de vos besoins de stockage d'objets.

La politique ILM contrôle où les données de l'objet sont stockées et si elles sont supprimées après une certaine période. Votre administrateur de réseau crée des stratégies ILM et les attribue à des balises de stratégie ILM lors de l'utilisation de plusieurs stratégies actives.



Évitez de réaffecter fréquemment la balise de stratégie d'un bucket. Dans le cas contraire, des problèmes de performances pourraient survenir.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#) .
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Accès root, autorisation Gérer tous les buckets ou Afficher tous les buckets"](#) . Ces autorisations remplacent les paramètres d'autorisation dans les stratégies de groupe ou de compartiment.

Étapes

1. Sélectionnez **Afficher les buckets** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > Buckets**.

La page Buckets apparaît. Selon vos besoins, vous pouvez trier les informations par colonne ou parcourir la liste en avant et en arrière.

2. Sélectionnez le nom du bucket auquel vous souhaitez attribuer une balise de stratégie ILM.

Vous pouvez également modifier l'attribution de balise de stratégie ILM pour un bucket auquel une balise est déjà attribuée.



Les valeurs affichées pour le nombre d'objets et l'espace utilisé sont des estimations. Ces estimations sont affectées par le moment des ingestions, la connectivité réseau et l'état du nœud. Si le contrôle de version est activé pour les buckets, les versions d'objet supprimées sont incluses dans le nombre d'objets.

3. Dans l'onglet Options du compartiment, développez l'accordéon de balise de stratégie ILM. Cet accordéon n'apparaît que si votre administrateur de grille a activé l'utilisation de balises de stratégie personnalisées.
4. Lisez la description de chaque balise de stratégie pour déterminer quelle balise doit être appliquée au bucket.



La modification de la balise de politique ILM pour un bucket déclenchera la réévaluation ILM de tous les objets du bucket. Si la nouvelle politique conserve les objets pendant une durée limitée, les objets plus anciens seront supprimés.

5. Sélectionnez le bouton radio correspondant à la balise que vous souhaitez attribuer au bucket.
6. Sélectionnez **Enregistrer les modifications**. Une nouvelle balise de compartiment S3 sera définie sur le compartiment avec la clé `NTAP-SG-ILM-BUCKET-TAG` et la valeur du nom de la balise de politique ILM.



Assurez-vous que vos applications S3 ne remplacent pas ou ne suppriment pas accidentellement la nouvelle balise de compartiment. Si cette balise est omise lors de l'application d'un nouveau TagSet au bucket, les objets du bucket seront à nouveau évalués par rapport à la stratégie ILM par défaut.



Définissez et modifiez les balises de stratégie ILM à l'aide uniquement de Tenant Manager ou de l'API Tenant Manager où la balise de stratégie ILM est validée. Ne pas modifier le `NTAP-SG-ILM-BUCKET-TAG` Balise de stratégie ILM utilisant l'API S3 PutBucketTagging ou l'API S3 DeleteBucketTagging.



La modification de la balise de stratégie attribuée à un bucket a un impact temporaire sur les performances pendant que les objets sont réévalués à l'aide de la nouvelle stratégie ILM.

Gérer la politique de compartiment

Vous pouvez contrôler l'accès des utilisateurs à un compartiment S3 et aux objets de ce compartiment.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#) .
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Autorisation d'accès root"](#) . Les autorisations Afficher tous les compartiments et Gérer tous les compartiments permettent uniquement l'affichage.
- Vous avez vérifié que le nombre requis de nœuds de stockage et de sites est disponible. Si deux ou plusieurs nœuds de stockage ne sont pas disponibles sur un site, ou si un site n'est pas disponible, les modifications apportées à ces paramètres peuvent ne pas être disponibles.

Étapes

1. Sélectionnez **Buckets**, puis sélectionnez le bucket que vous souhaitez gérer.
2. Sur la page des détails du bucket, sélectionnez **Accès au bucket** > **Politique du bucket**.

3. Effectuez l'une des opérations suivantes :

- Saisissez une politique de compartiment en cochant la case **Activer la politique**. Saisissez ensuite une chaîne formatée JSON valide.

Chaque politique de compartiment a une limite de taille de 20 480 octets.

- Modifier une politique existante en modifiant la chaîne.
- Désactivez une politique en désélectionnant **Activer la politique**.

Pour des informations détaillées sur les politiques de bucket, y compris la syntaxe du langage et des exemples, voir "[Exemples de politiques de compartiment](#)".

Gérer la cohérence des buckets

Les valeurs de cohérence peuvent être utilisées pour spécifier la disponibilité des modifications des paramètres de bucket ainsi que pour fournir un équilibre entre la disponibilité des objets dans un bucket et la cohérence de ces objets sur différents nœuds de stockage et sites. Vous pouvez modifier les valeurs de cohérence pour qu'elles soient différentes des valeurs par défaut afin que les applications clientes puissent répondre à leurs besoins opérationnels.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un "[navigateur Web pris en charge](#)".
- Vous appartenez à un groupe d'utilisateurs qui possède le "[Gérer tous les buckets ou l'autorisation d'accès root](#)". Ces autorisations remplacent les paramètres d'autorisations dans les stratégies de groupe ou de compartiment.

Directives relatives à la cohérence des seaux

La cohérence du bucket est utilisée pour déterminer la cohérence des applications clientes affectant les objets dans ce bucket S3. En général, vous devez utiliser la cohérence **Lecture après nouvelle écriture** pour vos buckets.

Modifier la cohérence du bucket

Si la cohérence **Lecture après nouvelle écriture** ne répond pas aux exigences de l'application cliente, vous pouvez modifier la cohérence en définissant la cohérence du compartiment ou en utilisant le Consistency-Control en-tête. Le Consistency-Control l'en-tête remplace la cohérence du bucket.



Lorsque vous modifiez la cohérence d'un bucket, seuls les objets ingérés après la modification sont assurés de respecter le paramètre révisé.

Étapes

1. Sélectionnez **Afficher les buckets** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > Buckets**.
2. Sélectionnez le nom du bucket dans le tableau.

La page des détails du bucket apparaît.

3. Dans l'onglet **Options du bucket**, sélectionnez l'accordéon **.

4. Sélectionnez une cohérence pour les opérations effectuées sur les objets de ce bucket.
- **Tous** : Offre le plus haut niveau de cohérence. Tous les nœuds reçoivent les données immédiatement, sinon la demande échouera.
 - **Strong-global** : garantit la cohérence de lecture après écriture pour toutes les demandes client sur tous les sites.
 - **Strong-site** : garantit la cohérence de lecture après écriture pour toutes les requêtes client au sein d'un site.
 - **Lecture après nouvelle écriture** (par défaut) : assure la cohérence de lecture après écriture pour les nouveaux objets et la cohérence éventuelle pour les mises à jour d'objets. Offre des garanties de haute disponibilité et de protection des données. Recommandé dans la plupart des cas.
 - **Disponible** : Fournit une cohérence éventuelle pour les nouveaux objets et les mises à jour d'objets. Pour les buckets S3, utilisez-les uniquement si nécessaire (par exemple, pour un bucket contenant des valeurs de journal rarement lues ou pour des opérations HEAD ou GET sur des clés qui n'existent pas). Non pris en charge pour les buckets S3 FabricPool .
5. Sélectionnez **Enregistrer les modifications**.

Que se passe-t-il lorsque vous modifiez les paramètres du bucket

Les buckets ont plusieurs paramètres qui affectent le comportement des buckets et des objets qu'ils contiennent.

Les paramètres de bucket suivants utilisent une cohérence **forte** par défaut. Si deux ou plusieurs nœuds de stockage ne sont pas disponibles sur un site, ou si un site n'est pas disponible, les modifications apportées à ces paramètres peuvent ne pas être disponibles.

- "Suppression du bucket vide en arrière-plan"
- "Heure du dernier accès"
- "Cycle de vie du bucket"
- "Politique de compartiment"
- "Étiquetage des buckets"
- "Gestion des versions de buckets"
- "Verrouillage d'objet S3"
- "Chiffrement du bucket"



La valeur de cohérence pour le contrôle de version du bucket, le verrouillage d'objet S3 et le chiffrement du bucket ne peut pas être définie sur une valeur qui n'est pas fortement cohérente.

Les paramètres de compartiment suivants n'utilisent pas de cohérence forte et ont une plus grande disponibilité pour les modifications. Les modifications apportées à ces paramètres peuvent prendre un certain temps avant d'avoir un effet.

- "Configuration des services de la plateforme : intégration des notifications, de la réplication ou de la recherche"
- "Configuration CORS"
- Modifier la cohérence du bucket



Si la cohérence par défaut utilisée lors de la modification des paramètres de compartiment ne répond pas aux exigences de l'application cliente, vous pouvez modifier la cohérence à l'aide de l' `Consistency-Control` en-tête pour le ["API REST S3"](#) ou en utilisant le `reducedConsistency` ou `force` options dans le ["API de gestion des locataires"](#) .

Activer ou désactiver les mises à jour de l'heure du dernier accès

Lorsque les administrateurs de grille créent les règles de gestion du cycle de vie des informations (ILM) pour un système StorageGRID , ils peuvent éventuellement spécifier que l'heure du dernier accès d'un objet soit utilisée pour déterminer s'il faut déplacer cet objet vers un autre emplacement de stockage. Si vous utilisez un locataire S3, vous pouvez tirer parti de ces règles en activant les mises à jour de l'heure du dernier accès pour les objets d'un compartiment S3.

Ces instructions s'appliquent uniquement aux systèmes StorageGRID qui incluent au moins une règle ILM qui utilise l'option **Dernière heure d'accès** comme filtre avancé ou comme heure de référence. Vous pouvez ignorer ces instructions si votre système StorageGRID n'inclut pas une telle règle. Voir ["Utiliser l'heure du dernier accès dans les règles ILM"](#) pour plus de détails.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#) .
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Gérer tous les buckets ou l'autorisation d'accès root"](#) . Ces autorisations remplacent les paramètres d'autorisations dans les stratégies de groupe ou de compartiment.

À propos de cette tâche

L'**heure du dernier accès** est l'une des options disponibles pour l'instruction de placement **Heure de référence** pour une règle ILM. La définition de l'heure de référence d'une règle sur l'heure du dernier accès permet aux administrateurs de grille de spécifier que les objets doivent être placés dans certains emplacements de stockage en fonction du moment où ces objets ont été récupérés pour la dernière fois (lus ou visualisés).

Par exemple, pour garantir que les objets récemment consultés restent sur un stockage plus rapide, un administrateur de grille peut créer une règle ILM spécifiant les éléments suivants :

- Les objets récupérés au cours du mois dernier doivent rester sur les nœuds de stockage locaux.
- Les objets qui n'ont pas été récupérés au cours du mois dernier doivent être déplacés vers un emplacement hors site.

Par défaut, les mises à jour de l'heure du dernier accès sont désactivées. Si votre système StorageGRID inclut une règle ILM qui utilise l'option **Dernière heure d'accès** et que vous souhaitez que cette option s'applique aux objets de ce compartiment, vous devez activer les mises à jour de la dernière heure d'accès pour les compartiments S3 spécifiés dans cette règle.



La mise à jour de l'heure du dernier accès lors de la récupération d'un objet peut réduire les performances de StorageGRID , en particulier pour les petits objets.

Un impact sur les performances se produit avec les mises à jour de l'heure du dernier accès, car StorageGRID doit effectuer ces étapes supplémentaires à chaque fois que des objets sont récupérés :

- Mettre à jour les objets avec de nouveaux horodatages
- Ajoutez les objets à la file d'attente ILM afin qu'ils puissent être réévalués par rapport aux règles et politiques ILM actuelles

Le tableau résume le comportement appliqué à tous les objets du compartiment lorsque l'heure du dernier accès est désactivée ou activée.

Type de demande	Comportement si l'heure du dernier accès est désactivée (par défaut)		Comportement si l'heure du dernier accès est activée	
	Dernière heure d'accès mise à jour ?	Objet ajouté à la file d'attente d'évaluation ILM ?	Dernière heure d'accès mise à jour ?	Objet ajouté à la file d'attente d'évaluation ILM ?
Demande de récupération d'un objet, de sa liste de contrôle d'accès ou de ses métadonnées	Non	Non	Oui	Oui
Demande de mise à jour des métadonnées d'un objet	Oui	Oui	Oui	Oui
Demande de liste d'objets ou de versions d'objets	Non	Non	Non	Non
Demande de copie d'un objet d'un bucket à un autre	<ul style="list-style-type: none"> • Non, pour la copie source • Oui, pour la copie de destination 	<ul style="list-style-type: none"> • Non, pour la copie source • Oui, pour la copie de destination 	<ul style="list-style-type: none"> • Oui, pour la copie source • Oui, pour la copie de destination 	<ul style="list-style-type: none"> • Oui, pour la copie source • Oui, pour la copie de destination
Demande de finalisation d'un téléchargement en plusieurs parties	Oui, pour l'objet assemblé	Oui, pour l'objet assemblé	Oui, pour l'objet assemblé	Oui, pour l'objet assemblé

Étapes

1. Sélectionnez **Afficher les buckets** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > Buckets**.
2. Sélectionnez le nom du bucket dans le tableau.

La page des détails du bucket apparaît.

3. Dans l'onglet **Options du bucket**, sélectionnez l'accordéon **Dernières mises à jour de l'heure d'accès**.
4. Activer ou désactiver les mises à jour de l'heure du dernier accès.

5. Sélectionnez **Enregistrer les modifications**.

Modifier la version d'objet pour un bucket

Si vous utilisez un locataire S3, vous pouvez modifier l'état de contrôle de version des buckets S3.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Gérer tous les buckets ou l'autorisation d'accès root"](#). Ces autorisations remplacent les paramètres d'autorisations dans les stratégies de groupe ou de compartiment.
- Vous avez vérifié que le nombre requis de nœuds de stockage et de sites est disponible. Si deux ou plusieurs nœuds de stockage ne sont pas disponibles sur un site, ou si un site n'est pas disponible, les modifications apportées à ces paramètres peuvent ne pas être disponibles.

À propos de cette tâche

Vous pouvez activer ou suspendre le contrôle de version d'objet pour un bucket. Une fois que vous avez activé le contrôle de version pour un bucket, celui-ci ne peut pas revenir à un état non versionné. Cependant, vous pouvez suspendre le contrôle de version du bucket.

- Désactivé : le contrôle de version n'a jamais été activé
- Activé : le contrôle de version est activé
- Suspendu : le contrôle de version était précédemment activé et est suspendu

Pour plus d'informations, consultez les éléments suivants :

- ["Versionnage d'objet"](#)
- ["Règles et politiques ILM pour les objets versionnés S3 \(exemple 4\)"](#)
- ["Comment les objets sont supprimés"](#)

Étapes

1. Sélectionnez **Afficher les buckets** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > Buckets**.
2. Sélectionnez le nom du bucket dans le tableau.

La page des détails du bucket apparaît.

3. Dans l'onglet **Options du bucket**, sélectionnez l'accordéon **Versionnement d'objet**.
4. Sélectionnez un état de version pour les objets de ce bucket.

Le contrôle de version des objets doit rester activé pour un bucket utilisé pour la réplication inter-grille. Si le verrouillage d'objet S3 ou la conformité héritée est activé, les options **Versionnage d'objet** sont désactivées.

Option	Description
Activer le contrôle de version	<p>Activez le contrôle de version des objets si vous souhaitez stocker chaque version de chaque objet dans ce bucket. Vous pouvez ensuite récupérer les versions précédentes d'un objet selon vos besoins.</p> <p>Les objets qui étaient déjà dans le bucket seront versionnés lorsqu'ils seront modifiés par un utilisateur.</p>
Suspendre le contrôle de version	Suspendez le contrôle de version des objets si vous ne souhaitez plus que de nouvelles versions d'objets soient créées. Vous pouvez toujours récupérer toutes les versions d'objet existantes.

5. Sélectionnez **Enregistrer les modifications**.

Utilisez S3 Object Lock pour conserver les objets

Vous pouvez utiliser S3 Object Lock si les buckets et les objets doivent être conformes aux exigences réglementaires en matière de conservation.



Votre administrateur de grille doit vous donner l'autorisation d'utiliser des fonctionnalités spécifiques de S3 Object Lock.

Qu'est-ce que S3 Object Lock ?

La fonctionnalité StorageGRID S3 Object Lock est une solution de protection d'objets équivalente à S3 Object Lock dans Amazon Simple Storage Service (Amazon S3).

Lorsque le paramètre global de verrouillage d'objet S3 est activé pour un système StorageGRID, un compte de locataire S3 peut créer des buckets avec ou sans verrouillage d'objet S3 activé. Si le verrouillage d'objet S3 est activé pour un bucket, le contrôle de version du bucket est requis et est activé automatiquement.

Un bucket sans verrouillage d'objet S3 ne peut contenir que des objets sans paramètres de conservation spécifiés. Aucun objet ingéré n'aura de paramètres de rétention.

Un bucket avec verrouillage d'objet S3 peut contenir des objets avec et sans paramètres de rétention spécifiés par les applications clientes S3. Certains objets ingérés auront des paramètres de rétention.

Un bucket avec verrouillage d'objet S3 et rétention par défaut configuré peut contenir des objets téléchargés avec des paramètres de rétention spécifiés et de nouveaux objets sans paramètres de rétention. Les nouveaux objets utilisent le paramètre par défaut, car le paramètre de rétention n'a pas été configuré au niveau de l'objet.

En effet, tous les objets nouvellement ingérés ont des paramètres de rétention lorsque la rétention par défaut est configurée. Les objets existants sans paramètres de conservation d'objets restent inchangés.

Modes de rétention

La fonctionnalité de verrouillage d'objet StorageGRID S3 prend en charge deux modes de conservation pour appliquer différents niveaux de protection aux objets. Ces modes sont équivalents aux modes de rétention d'Amazon S3.

- En mode conformité :
 - L'objet ne peut pas être supprimé tant que sa date de conservation n'est pas atteinte.
 - La date de conservation de l'objet peut être augmentée, mais elle ne peut pas être diminuée.
 - La date de conservation de l'objet ne peut pas être supprimée tant que cette date n'est pas atteinte.
- En mode gouvernance :
 - Les utilisateurs disposant d'une autorisation spéciale peuvent utiliser un en-tête de contournement dans les demandes pour modifier certains paramètres de conservation.
 - Ces utilisateurs peuvent supprimer une version d'objet avant que sa date de conservation ne soit atteinte.
 - Ces utilisateurs peuvent augmenter, diminuer ou supprimer la date de conservation d'un objet.

Paramètres de conservation pour les versions d'objet

Si un compartiment est créé avec le verrouillage d'objet S3 activé, les utilisateurs peuvent utiliser l'application cliente S3 pour spécifier éventuellement les paramètres de conservation suivants pour chaque objet ajouté au compartiment :

- **Mode de conservation** : Soit la conformité, soit la gouvernance.
- **Date de conservation jusqu'à** : si la date de conservation jusqu'à d'une version d'objet est dans le futur, l'objet peut être récupéré, mais il ne peut pas être supprimé.
- **Conservation légale** : L'application d'une conservation légale à une version d'objet verrouille immédiatement cet objet. Par exemple, vous pourriez avoir besoin de suspendre légalement un objet lié à une enquête ou à un litige juridique. Une conservation légale n'a pas de date d'expiration, mais reste en place jusqu'à ce qu'elle soit explicitement supprimée. Les conservations légales sont indépendantes de la date de conservation.



Si un objet est sous conservation légale, personne ne peut supprimer l'objet, quel que soit son mode de conservation.

Pour plus de détails sur les paramètres de l'objet, voir ["Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3"](#) .

Paramètre de rétention par défaut pour les buckets

Si un bucket est créé avec le verrouillage d'objet S3 activé, les utilisateurs peuvent éventuellement spécifier les paramètres par défaut suivants pour le bucket :

- **Mode de conservation par défaut** : Conformité ou gouvernance.
- **Période de conservation par défaut** : durée pendant laquelle les nouvelles versions d'objet ajoutées à ce bucket doivent être conservées, à compter du jour de leur ajout.

Les paramètres de compartiment par défaut s'appliquent uniquement aux nouveaux objets qui ne disposent pas de leurs propres paramètres de conservation. Les objets de compartiment existants ne sont pas affectés lorsque vous ajoutez ou modifiez ces paramètres par défaut.

Voir ["Créer un bucket S3"](#) et ["Mettre à jour la conservation par défaut du verrouillage des objets S3"](#) .

Tâches de verrouillage d'objet S3

Les listes suivantes destinées aux administrateurs de grille et aux utilisateurs locataires contiennent les tâches de haut niveau pour l'utilisation de la fonctionnalité de verrouillage d'objet S3.

Administrateur de réseau

- Activez le paramètre de verrouillage d'objet S3 global pour l'ensemble du système StorageGRID .
- Assurez-vous que les politiques de gestion du cycle de vie de l'information (ILM) sont *conformes* ; c'est-à-dire qu'elles répondent aux ["exigences des buckets avec S3 Object Lock activé"](#) .
- Si nécessaire, autorisez un locataire à utiliser la conformité comme mode de conservation. Sinon, seul le mode Gouvernance est autorisé.
- Si nécessaire, définissez une période de conservation maximale pour un locataire.

Utilisateur locataire

- Passez en revue les considérations relatives aux buckets et aux objets avec S3 Object Lock.
- Si nécessaire, contactez l'administrateur de la grille pour activer le paramètre de verrouillage d'objet S3 global et définir les autorisations.
- Créez des buckets avec le verrouillage d'objet S3 activé.
- Vous pouvez également configurer les paramètres de conservation par défaut pour un bucket :
 - Mode de conservation par défaut : Gouvernance ou Conformité, si autorisé par l'administrateur du réseau.
 - Période de conservation par défaut : doit être inférieure ou égale à la période de conservation maximale définie par l'administrateur du réseau.
- Utilisez l'application client S3 pour ajouter des objets et éventuellement définir une conservation spécifique à l'objet :
 - Mode de rétention. Gouvernance ou conformité, si autorisée par l'administrateur du réseau.
 - Date de conservation : doit être inférieure ou égale à ce qui est autorisé par la période de conservation maximale définie par l'administrateur de la grille.

Exigences pour les buckets avec S3 Object Lock activé

- Si le paramètre global de verrouillage d'objet S3 est activé pour le système StorageGRID , vous pouvez utiliser le gestionnaire de locataires, l'API de gestion des locataires ou l'API REST S3 pour créer des buckets avec le verrouillage d'objets S3 activé.
- Si vous prévoyez d'utiliser S3 Object Lock, vous devez activer S3 Object Lock lorsque vous créez le bucket. Vous ne pouvez pas activer le verrouillage d'objet S3 pour un bucket existant.
- Lorsque le verrouillage d'objet S3 est activé pour un bucket, StorageGRID active automatiquement le contrôle de version pour ce bucket. Vous ne pouvez pas désactiver le verrouillage d'objet S3 ou suspendre le contrôle de version du bucket.
- Vous pouvez également spécifier un mode de conservation par défaut et une période de conservation pour chaque compartiment à l'aide du gestionnaire de locataires, de l'API de gestion des locataires ou de l'API REST S3. Les paramètres de conservation par défaut du bucket s'appliquent uniquement aux nouveaux objets ajoutés au bucket qui ne disposent pas de leurs propres paramètres de conservation. Vous pouvez remplacer ces paramètres par défaut en spécifiant un mode de conservation et une date de conservation pour chaque version d'objet lors de son téléchargement.
- La configuration du cycle de vie du bucket est prise en charge pour les buckets avec S3 Object Lock activé.

- La réplication CloudMirror n'est pas prise en charge pour les buckets avec S3 Object Lock activé.

Exigences relatives aux objets dans les compartiments avec le verrouillage d'objet S3 activé

- Pour protéger une version d'objet, vous pouvez spécifier des paramètres de rétention par défaut pour le compartiment ou spécifier des paramètres de rétention pour chaque version d'objet. Les paramètres de conservation au niveau de l'objet peuvent être spécifiés à l'aide de l'application cliente S3 ou de l'API REST S3.
- Les paramètres de conservation s'appliquent aux versions d'objet individuelles. Une version d'objet peut avoir à la fois une date de conservation et un paramètre de conservation légale, l'un mais pas l'autre, ou aucun des deux. La spécification d'une date de conservation ou d'un paramètre de conservation légale pour un objet protège uniquement la version spécifiée dans la demande. Vous pouvez créer de nouvelles versions de l'objet, tandis que la version précédente de l'objet reste verrouillée.

Cycle de vie des objets dans les buckets avec S3 Object Lock activé

Chaque objet enregistré dans un bucket avec S3 Object Lock activé passe par ces étapes :

1. Objet ingéré

Lorsqu'une version d'objet est ajoutée à un bucket sur lequel le verrouillage d'objet S3 est activé, les paramètres de rétention sont appliqués comme suit :

- Si des paramètres de conservation sont spécifiés pour l'objet, les paramètres au niveau de l'objet sont appliqués. Tous les paramètres de bucket par défaut sont ignorés.
- Si aucun paramètre de conservation n'est spécifié pour l'objet, les paramètres de compartiment par défaut sont appliqués, s'ils existent.
- Si aucun paramètre de conservation n'est spécifié pour l'objet ou le compartiment, l'objet n'est pas protégé par S3 Object Lock.

Si les paramètres de conservation sont appliqués, l'objet et toutes les métadonnées définies par l'utilisateur S3 sont protégés.

2. Conservation et suppression d'objets

Plusieurs copies de chaque objet protégé sont stockées par StorageGRID pendant la période de conservation spécifiée. Le nombre et le type exacts de copies d'objets ainsi que les emplacements de stockage sont déterminés par les règles de conformité des politiques ILM actives. La possibilité de supprimer un objet protégé avant que sa date de conservation ne soit atteinte dépend de son mode de conservation.

- Si un objet est sous conservation légale, personne ne peut supprimer l'objet, quel que soit son mode de conservation.

Puis-je toujours gérer les buckets conformes hérités ?

La fonctionnalité de verrouillage d'objet S3 remplace la fonctionnalité de conformité qui était disponible dans les versions précédentes de StorageGRID . Si vous avez créé des buckets conformes à l'aide d'une version précédente de StorageGRID, vous pouvez continuer à gérer les paramètres de ces buckets ; toutefois, vous ne pouvez plus créer de nouveaux buckets conformes. Pour les instructions, voir https://kb.netapp.com/Advice_and_Troubleshooting/Hybrid_Cloud_Infrastructure/StorageGRID/How_to_manage_legacy_Compliant_buckets_in_StorageGRID_11.5 [Base de connaissances NetApp : Gestion des

Mettre à jour la conservation par défaut du verrouillage des objets S3

Si vous avez activé le verrouillage d'objet S3 lors de la création du bucket, vous pouvez modifier le bucket pour modifier les paramètres de rétention par défaut. Vous pouvez activer (ou désactiver) la conservation par défaut et définir un mode de conservation par défaut et une période de conservation.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un [navigateur Web pris en charge](#) .
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Gérer tous les buckets ou l'autorisation d'accès root"](#) . Ces autorisations remplacent les paramètres d'autorisations dans les stratégies de groupe ou de compartiment.
- Le verrouillage des objets S3 est activé globalement pour votre système StorageGRID et vous avez activé le verrouillage des objets S3 lorsque vous avez créé le bucket. Voir ["Utilisez S3 Object Lock pour conserver les objets"](#) .

Étapes

1. Sélectionnez **Afficher les buckets** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > Buckets**.
2. Sélectionnez le nom du bucket dans le tableau.

La page des détails du bucket apparaît.

3. Dans l'onglet **Options du bucket**, sélectionnez l'accordéon **Verrouillage d'objet S3**.
4. En option, activez ou désactivez la **Rétention par défaut** pour ce bucket.

Les modifications apportées à ce paramètre ne s'appliquent pas aux objets déjà présents dans le bucket ni aux objets susceptibles d'avoir leurs propres périodes de conservation.

5. Si la **Rétention par défaut** est activée, spécifiez un **Mode de rétention par défaut** pour le bucket.

Mode de rétention par défaut	Description
Gouvernance	<ul style="list-style-type: none">• Les utilisateurs avec le <code>s3:BypassGovernanceRetention</code> l'autorisation peut utiliser le <code>x-amz-bypass-governance-retention: true</code> en-tête de demande pour contourner les paramètres de conservation.• Ces utilisateurs peuvent supprimer une version d'objet avant que sa date de conservation ne soit atteinte.• Ces utilisateurs peuvent augmenter, diminuer ou supprimer la date de conservation d'un objet.

Mode de rétention par défaut	Description
Conformité	<ul style="list-style-type: none"> • L'objet ne peut pas être supprimé tant que sa date de conservation n'est pas atteinte. • La date de conservation de l'objet peut être augmentée, mais elle ne peut pas être diminuée. • La date de conservation de l'objet ne peut pas être supprimée tant que cette date n'est pas atteinte. <p>Remarque : votre administrateur de réseau doit vous autoriser à utiliser le mode de conformité.</p>

6. Si la **Conservation par défaut** est activée, spécifiez la **Période de conservation par défaut** pour le bucket.

La **Période de conservation par défaut** indique la durée pendant laquelle les nouveaux objets ajoutés à ce bucket doivent être conservés, à compter du moment où ils sont ingérés. Spécifiez une valeur inférieure ou égale à la période de conservation maximale du locataire, telle que définie par l'administrateur de la grille.

Une période de conservation *maximale*, qui peut être une valeur comprise entre 1 jour et 100 ans, est définie lorsque l'administrateur de la grille crée le locataire. Lorsque vous définissez une période de conservation par défaut, elle ne peut pas dépasser la valeur définie pour la période de conservation maximale. Si nécessaire, demandez à votre administrateur de réseau d'augmenter ou de diminuer la période de conservation maximale.

7. Sélectionnez **Enregistrer les modifications**.

Configurer le partage de ressources inter-origines (CORS)

Vous pouvez configurer le partage de ressources inter-origines (CORS) pour un bucket S3 si vous souhaitez que ce bucket et les objets qu'il contient soient accessibles aux applications Web d'autres domaines.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un [navigateur Web pris en charge](#).
- Pour les demandes de configuration GET CORS, vous appartenez à un groupe d'utilisateurs qui possède le ["Autorisation de gérer tous les compartiments ou d'afficher tous les compartiments"](#). Ces autorisations remplacent les paramètres d'autorisations dans les stratégies de groupe ou de compartiment.
- Pour les demandes de configuration PUT CORS, vous appartenez à un groupe d'utilisateurs qui possède le ["Gérer toutes les autorisations des buckets"](#). Cette autorisation remplace les paramètres d'autorisations dans les stratégies de groupe ou de compartiment.
- Le ["Autorisation d'accès root"](#) donne accès à toutes les demandes de configuration CORS.

À propos de cette tâche

Le partage de ressources inter-origines (CORS) est un mécanisme de sécurité qui permet aux applications Web clientes d'un domaine d'accéder aux ressources d'un domaine différent. Par exemple, supposons que vous utilisiez un bucket S3 nommé *Images* pour stocker des graphiques. En configurant CORS pour le *Images* bucket, vous pouvez autoriser l'affichage des images de ce bucket sur le site Web

Activer CORS pour un bucket

Étapes

1. Utilisez un éditeur de texte pour créer le XML requis. Cet exemple montre le XML utilisé pour activer CORS pour un bucket S3. Spécifiquement:
 - Permet à n'importe quel domaine d'envoyer des requêtes GET au bucket
 - Autorise uniquement le `http://www.example.com` domaine pour envoyer des requêtes GET, POST et DELETE
 - Tous les en-têtes de requête sont autorisés

```
<CORSConfiguration
  xmlns="http://s3.amazonaws.com/doc/2020-10-22/">
  <CORSRule>
    <AllowedOrigin>*</AllowedOrigin>
    <AllowedMethod>GET</AllowedMethod>
    <AllowedHeader>*</AllowedHeader>
  </CORSRule>
  <CORSRule>
    <AllowedOrigin>http://www.example.com</AllowedOrigin>
    <AllowedMethod>GET</AllowedMethod>
    <AllowedMethod>POST</AllowedMethod>
    <AllowedMethod>DELETE</AllowedMethod>
    <AllowedHeader>*</AllowedHeader>
  </CORSRule>
</CORSConfiguration>
```

Pour plus d'informations sur le XML de configuration CORS, voir ["Documentation Amazon Web Services \(AWS\) : Guide de l'utilisateur d'Amazon Simple Storage Service"](#).

2. Sélectionnez **Afficher les buckets** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > Buckets**.
3. Sélectionnez le nom du bucket dans le tableau.

La page des détails du bucket apparaît.

4. Dans l'onglet **Accès au bucket**, sélectionnez l'accordéon **Partage de ressources inter-origines (CORS)**.
5. Cochez la case **Activer CORS**.
6. Collez le XML de configuration CORS dans la zone de texte.
7. Sélectionnez **Enregistrer les modifications**.

Modifier le paramètre CORS

Étapes

1. Mettez à jour le XML de configuration CORS dans la zone de texte ou sélectionnez **Effacer** pour recommencer.

2. Sélectionnez **Enregistrer les modifications**.

Désactiver le paramètre CORS

Étapes

1. Décochez la case **Activer CORS**.
2. Sélectionnez **Enregistrer les modifications**.

Supprimer les objets dans le bucket

Vous pouvez utiliser le gestionnaire de locataires pour supprimer les objets dans un ou plusieurs compartiments.

Considérations et exigences

Avant d'effectuer ces étapes, notez les points suivants :

- Lorsque vous supprimez les objets d'un bucket, StorageGRID supprime définitivement tous les objets et toutes les versions d'objets de chaque bucket sélectionné de tous les nœuds et sites de votre système StorageGRID . StorageGRID supprime également toutes les métadonnées d'objet associées. Vous ne pourrez pas récupérer ces informations.
- La suppression de tous les objets d'un bucket peut prendre des minutes, des jours, voire des semaines, en fonction du nombre d'objets, de copies d'objets et d'opérations simultanées.
- Si un seau a "[Verrouillage d'objet S3 activé](#)" , il pourrait rester dans l'état **Suppression d'objets : lecture seule** pendant *années*.



Un bucket qui utilise S3 Object Lock restera dans l'état **Suppression d'objets : lecture seule** jusqu'à ce que la date de conservation soit atteinte pour tous les objets et que toutes les conservations légales soient supprimées.

- Pendant la suppression des objets, l'état du bucket est **Suppression d'objets : lecture seule**. Dans cet état, vous ne pouvez pas ajouter de nouveaux objets au bucket.
- Lorsque tous les objets ont été supprimés, le bucket reste en état de lecture seule. Vous pouvez effectuer l'une des opérations suivantes :
 - Remettre le bucket en mode écriture et le réutiliser pour de nouveaux objets
 - Supprimer le bucket
 - Gardez le bucket en mode lecture seule pour réserver son nom pour une utilisation ultérieure
- Si le contrôle de version d'objet est activé pour un bucket, les marqueurs de suppression créés dans StorageGRID 11.8 ou version ultérieure peuvent être supprimés à l'aide des opérations Supprimer des objets dans le bucket.
- Si le contrôle de version d'objet est activé pour un bucket, l'opération de suppression d'objets ne supprimera pas les marqueurs de suppression créés dans StorageGRID 11.7 ou une version antérieure. Consultez les informations sur la suppression d'objets dans un bucket dans "[Comment les objets versionnés S3 sont supprimés](#)" .
- Si vous utilisez "[réplication inter-réseaux](#)" , notez ce qui suit :
 - L'utilisation de cette option ne supprime aucun objet du bucket sur l'autre grille.
 - Si vous sélectionnez cette option pour le bucket source, l'alerte **Échec de la réplication inter-grille** sera déclenchée si vous ajoutez des objets au bucket de destination sur l'autre grille. Si vous ne

pouvez pas garantir que personne n'ajoutera d'objets au seau sur l'autre grille, "[désactiver la réplication inter-grille](#)" pour ce bucket avant de supprimer tous les objets du bucket.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un "[navigateur Web pris en charge](#)".
- Vous appartenez à un groupe d'utilisateurs qui possède le "[Autorisation d'accès root](#)". Cette autorisation remplace les paramètres d'autorisations dans les stratégies de groupe ou de compartiment.

Étapes

1. Sélectionnez **Afficher les buckets** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > Buckets**.

La page Buckets apparaît et affiche tous les buckets S3 existants.

2. Utilisez le menu **Actions** ou la page de détails pour un bucket spécifique.

Menu Actions

- a. Cochez la case correspondant à chaque compartiment dont vous souhaitez supprimer des objets.
- b. Sélectionnez **Actions > Supprimer les objets dans le bucket**.

Page de détails

- a. Sélectionnez un nom de bucket pour afficher ses détails.
- b. Sélectionnez **Supprimer les objets dans le bucket**.

3. Lorsque la boîte de dialogue de confirmation s'affiche, vérifiez les détails, entrez **Oui** et sélectionnez **OK**.
4. Attendez que l'opération de suppression commence.

Après quelques minutes :

- Une bannière d'état jaune apparaît sur la page des détails du bucket. La barre de progression représente le pourcentage d'objets supprimés.
- **(lecture seule)** apparaît après le nom du bucket sur la page des détails du bucket.
- **(Suppression d'objets : lecture seule)** apparaît à côté du nom du bucket sur la page Buckets.

Buckets > my-bucket

my-bucket (read-only)


Region: us-east-1

Date created: 2022-12-14 10:09:50 MST

Object count: 3

View bucket contents in Experimental S3 Console

Delete bucket

 **All bucket objects are being deleted**

StorageGRID is deleting all copies of the objects in this bucket, which might take days or weeks. While objects are being deleted, the bucket is read only. To stop the operation, select **Stop deleting objects**. You cannot restore objects that have already been deleted.

0% (0 of 3 objects deleted)

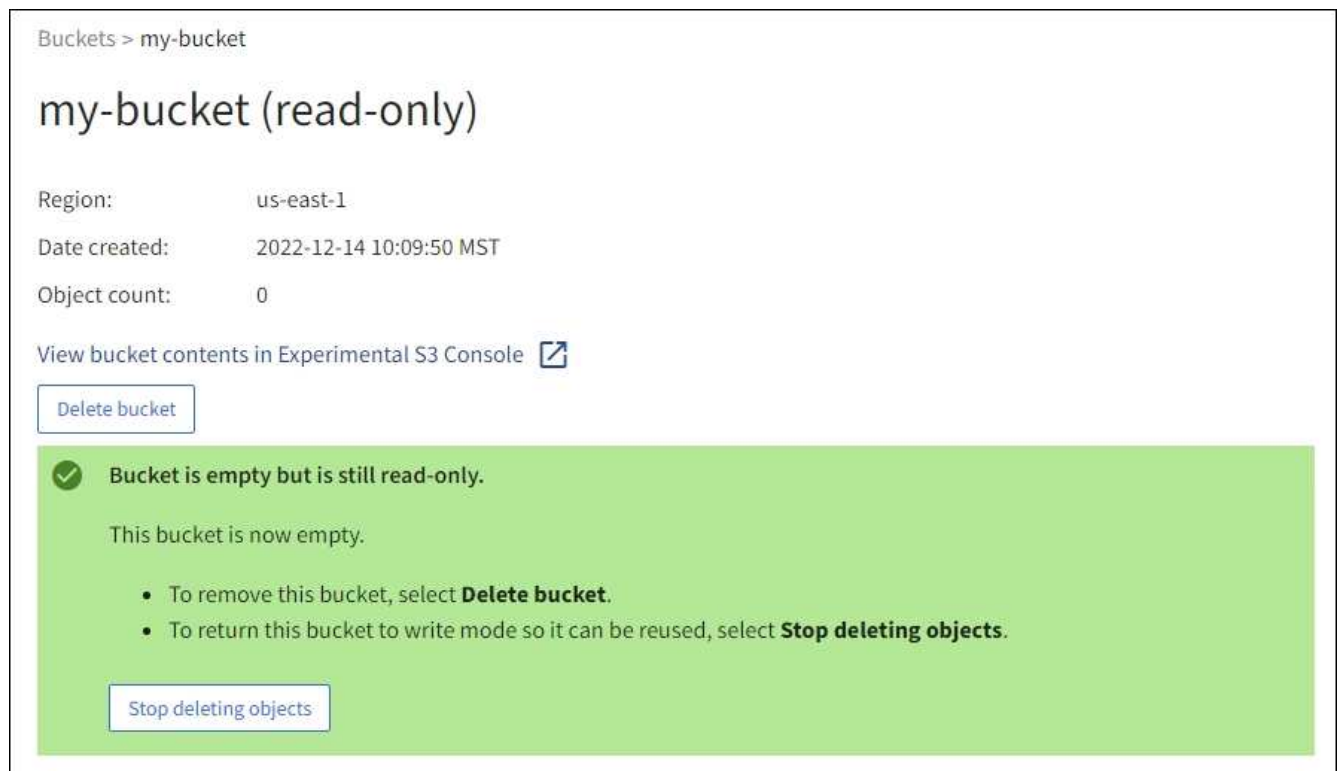
Stop deleting objects

5. Si nécessaire, pendant que l'opération est en cours, sélectionnez **Arrêter la suppression des objets** pour arrêter le processus. Ensuite, si vous le souhaitez, sélectionnez **Supprimer les objets dans le bucket** pour reprendre le processus.

Lorsque vous sélectionnez **Arrêter la suppression des objets**, le bucket revient en mode écriture ; cependant, vous ne pouvez pas accéder ni restaurer les objets qui ont été supprimés.

6. Attendez que l'opération soit terminée.

Lorsque le bucket est vide, la bannière d'état est mise à jour, mais le bucket reste en lecture seule.



7. Effectuez l'une des opérations suivantes :

- Quittez la page pour conserver le bucket en mode lecture seule. Par exemple, vous pouvez conserver un bucket vide en mode lecture seule pour réserver le nom du bucket pour une utilisation ultérieure.
- Supprimer le bucket. Vous pouvez sélectionner **Supprimer le bucket** pour supprimer un seul bucket ou revenir à la page Buckets et sélectionner **Actions > Supprimer** les buckets pour supprimer plusieurs buckets.



Si vous ne parvenez pas à supprimer un bucket versionné après la suppression de tous les objets, des marqueurs de suppression peuvent rester. Pour supprimer le bucket, vous devez supprimer tous les marqueurs de suppression restants.

- Remettez le bucket en mode écriture et réutilisez-le éventuellement pour de nouveaux objets. Vous pouvez sélectionner **Arrêter la suppression des objets** pour un seul bucket ou revenir à la page Buckets et sélectionner **Action > Arrêter la suppression des objets** pour plusieurs buckets.

Supprimer le compartiment S3

Vous pouvez utiliser le gestionnaire de locataires pour supprimer un ou plusieurs compartiments S3 vides.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un "[navigateur Web pris en charge](#)".
- Vous appartenez à un groupe d'utilisateurs qui possède le "[Gérer tous les buckets ou l'autorisation d'accès root](#)". Ces autorisations remplacent les paramètres d'autorisations dans les stratégies de groupe ou de compartiment.
- Les buckets que vous souhaitez supprimer sont vides. Si les buckets que vous souhaitez supprimer ne sont pas vides, "[supprimer des objets du bucket](#)".

À propos de cette tâche

Ces instructions décrivent comment supprimer un compartiment S3 à l'aide du gestionnaire de locataires. Vous pouvez également supprimer des compartiments S3 à l'aide de la ["API de gestion des locataires"](#) ou le ["API REST S3"](#).

Vous ne pouvez pas supprimer un compartiment S3 s'il contient des objets, des versions d'objet non actuelles ou des marqueurs de suppression. Pour plus d'informations sur la manière dont les objets versionnés S3 sont supprimés, consultez ["Comment les objets sont supprimés"](#).

Étapes

1. Sélectionnez **Afficher les buckets** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > Buckets**.

La page Buckets apparaît et affiche tous les buckets S3 existants.

2. Utilisez le menu **Actions** ou la page de détails pour un bucket spécifique.

Menu Actions

- a. Cochez la case correspondant à chaque compartiment que vous souhaitez supprimer.
- b. Sélectionnez **Actions > Supprimer les buckets**.

Page de détails

- a. Sélectionnez un nom de bucket pour afficher ses détails.
- b. Sélectionnez **Supprimer le bucket**.

3. Lorsque la boîte de dialogue de confirmation apparaît, sélectionnez **Oui**.

StorageGRID confirme que chaque bucket est vide, puis supprime chaque bucket. Cette opération peut prendre quelques minutes.

Si un bucket n'est pas vide, un message d'erreur s'affiche. Vous devez ["supprimer tous les objets et tous les marqueurs de suppression dans le bucket"](#) avant de pouvoir supprimer le bucket.

Utiliser la console S3

Vous pouvez utiliser la console S3 pour afficher et gérer les objets dans un bucket S3.

La console S3 vous permet de :

- Télécharger, renommer, copier, déplacer et supprimer des objets
- Afficher, rétablir, télécharger et supprimer les versions d'objets
- Rechercher des objets par préfixe
- Gérer les balises d'objet
- Afficher les métadonnées de l'objet
- Afficher, créer, renommer, copier, déplacer et supprimer des dossiers

La console S3 offre une expérience utilisateur améliorée pour les cas les plus courants. Il n'est pas conçu pour remplacer les opérations CLI ou API dans toutes les situations.



Si l'utilisation de la console S3 entraîne des opérations qui prennent trop de temps (par exemple, des minutes ou des heures), tenez compte des éléments suivants :

- Réduire le nombre d'objets sélectionnés
- Utiliser des méthodes non graphiques (API ou CLI) pour accéder à vos données

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#) .
- Si vous souhaitez gérer des objets, vous appartenez à un groupe d'utilisateurs disposant de l'autorisation d'accès Root. Vous pouvez également appartenir à un groupe d'utilisateurs disposant de l'autorisation Utiliser l'onglet Console S3 et de l'autorisation Afficher tous les buckets ou Gérer tous les buckets. Voir ["Autorisations de gestion des locataires"](#) .
- Une stratégie de groupe ou de compartiment S3 a été configurée pour l'utilisateur. Voir ["Utiliser des politiques d'accès aux buckets et aux groupes"](#) .
- Vous connaissez l'ID de la clé d'accès et la clé d'accès secrète de l'utilisateur. En option, vous disposez d'un `.csv` fichier contenant ces informations. Voir le ["instructions pour créer des clés d'accès"](#) .

Étapes

1. Sélectionnez **STOCKAGE > Compartiments > *nom du compartiment***.
2. Sélectionnez l'onglet Console S3.
3. Collez l'ID de la clé d'accès et la clé d'accès secrète dans les champs. Sinon, sélectionnez **Télécharger les clés d'accès** et sélectionnez votre `.csv` déposer.
4. Sélectionnez * Sign in*.
5. Le tableau des objets du bucket apparaît. Vous pouvez gérer les objets selon vos besoins.

Informations Complémentaires

- **Recherche par préfixe** : La fonction de recherche par préfixe recherche uniquement les objets commençant par un mot spécifique relatif au dossier actuel. La recherche n'inclut pas les objets qui contiennent le mot ailleurs. Cette règle s'applique également aux objets contenus dans les dossiers. Par exemple, une recherche de `folder1/folder2/somefile-` renverrait les objets qui sont dans le `folder1/folder2/` dossier et commencer par le mot `somefile-` .
- **Glisser-déposer** : vous pouvez glisser-déposer des fichiers du gestionnaire de fichiers de votre ordinateur vers la console S3. Cependant, vous ne pouvez pas télécharger de dossiers.
- **Opérations sur les dossiers** : Lorsque vous déplacez, copiez ou renommez un dossier, tous les objets du dossier sont mis à jour un par un, ce qui peut prendre du temps.
- **Suppression permanente lorsque le contrôle de version du bucket est désactivé** : lorsque vous écrasez ou supprimez un objet dans un bucket avec le contrôle de version désactivé, l'opération est permanente. Voir ["Modifier la version d'objet pour un bucket"](#) .

Informations sur le copyright

Copyright © 2025 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTEUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.