Gestion des comptes de locataires S3

StorageGRID

NetApp
October 03, 2025

Sommaire

Gestion des comptes de locataires S3

Gestion des clés d'accès S3

Chaque utilisateur d'un compte de locataire S3 doit disposer d'une clé d'accès pour stocker et récupérer des objets dans le système StorageGRID. Une clé d'accès se compose d'un ID de clé d'accès et d'une clé d'accès secrète.

Description de la tâche

Les clés d'accès S3 peuvent être gérées de la manière suivante :

- Les utilisateurs disposant de l'autorisation **gérer vos propres informations d'identification S3** peuvent créer ou supprimer leurs propres clés d'accès S3.
- Les utilisateurs disposant de l'autorisation **Root Access** peuvent gérer les clés d'accès pour le compte racine S3 et tous les autres utilisateurs. Les clés d'accès racine offrent un accès complet à toutes les compartiments et objets du locataire, sauf si une règle de compartiment est explicitement désactivée.

StorageGRID prend en charge l'authentification Signature version 2 et Signature version 4. L'accès entre comptes n'est pas autorisé sauf si cette règle est explicitement activée par une règle de compartiment.

Créez vos propres clés d'accès S3

Si vous utilisez un locataire S3 et que vous disposez de l'autorisation appropriée, vous pouvez créer vos propres clés d'accès S3. Vous devez disposer d'une clé d'accès pour accéder à vos compartiments et objets dans le compte de locataire S3.

Ce dont vous avez besoin

- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur web pris en charge.
- Vous devez disposer de l'autorisation gérer vos propres informations d'identification S3. Voir Autorisations de gestion des locataires.

Description de la tâche

Vous pouvez créer une ou plusieurs clés d'accès S3 qui vous permettent de créer et de gérer des compartiments pour votre compte de locataire. Après avoir créé une nouvelle clé d'accès, mettez à jour l'application avec votre nouvel ID de clé d'accès et votre clé d'accès secrète. Pour des raisons de sécurité, ne créez pas plus de clés que nécessaire et supprimez les clés que vous n'utilisez pas. Si vous n'avez qu'une seule clé et que vous êtes sur le point d'expirer, créez une nouvelle clé avant l'expiration de l'ancienne, puis supprimez l'ancienne.

Chaque clé peut avoir une heure d'expiration spécifique ou pas d'expiration. Suivez les directives ci-dessous pour l'heure d'expiration :

- Définissez une durée d'expiration pour vos clés afin de limiter votre accès à une certaine période. La définition d'un délai d'expiration court peut vous aider à réduire le risque si votre ID de clé d'accès et votre clé secrète sont exposés accidentellement. Les clés expirées sont supprimées automatiquement.
- Si le risque de sécurité dans votre environnement est faible et que vous n'avez pas besoin de créer régulièrement de nouvelles clés, vous n'avez pas à définir de délai d'expiration pour vos clés. Si vous décidez plus tard de créer de nouvelles clés, supprimez les anciennes clés manuellement.

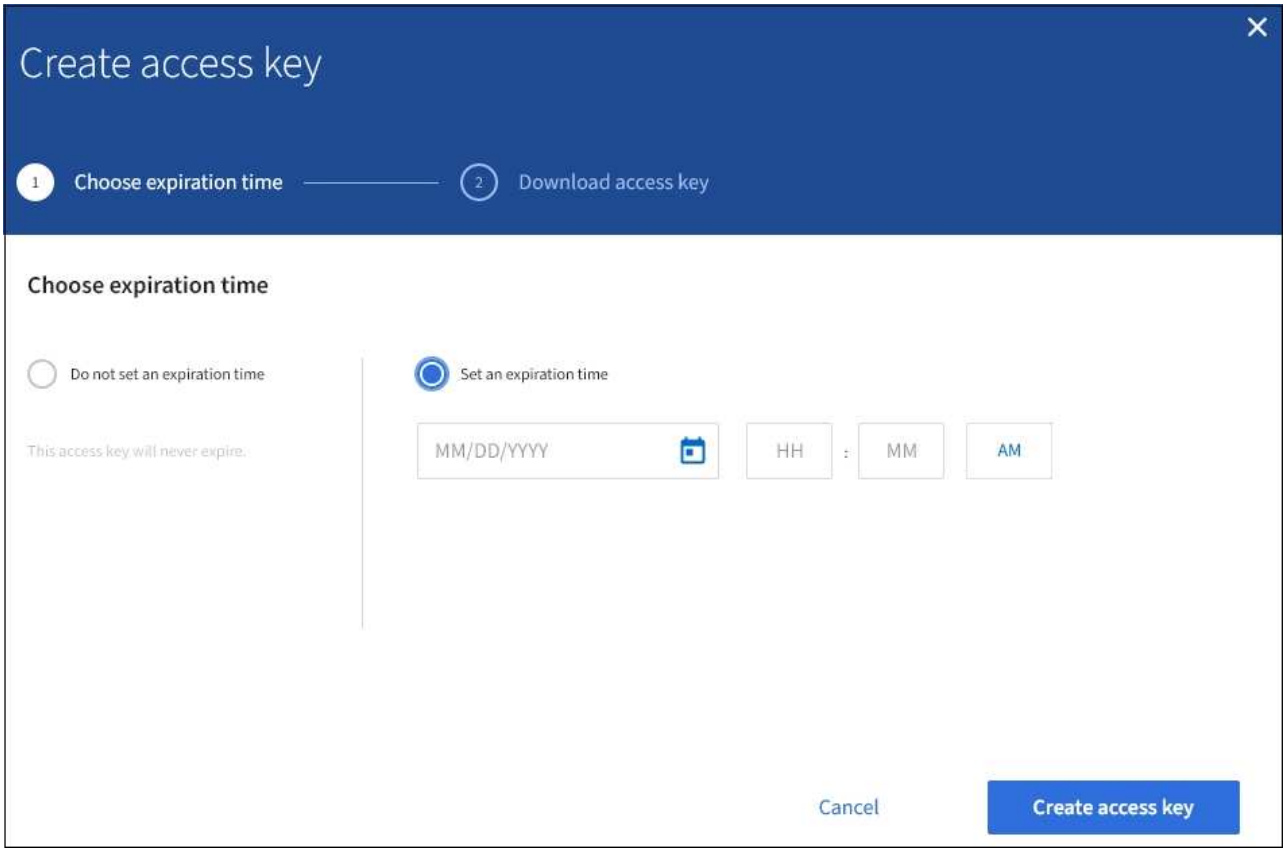
Vous pouvez accéder aux compartiments S3 et aux objets appartenant à votre compte à l'aide de l'ID de clé d'accès et de la clé secrète affichée pour votre compte dans le Gestionnaire des locataires. Pour cette raison, protégez les clés d'accès comme vous le feriez avec un mot de passe. Faites pivoter les clés d'accès régulièrement, supprimez les clés inutilisées de votre compte et ne les partagez jamais avec d'autres utilisateurs.

Étapes

1. Sélectionnez **STOCKAGE (S3) Mes clés d'accès**.

   La page Mes touches d'accès s'affiche et répertorie toutes les clés d'accès existantes.

2. Sélectionnez **Créer clé**.
3. Effectuez l'une des opérations suivantes :
   - Sélectionnez **ne définissez pas d'heure d'expiration** pour créer une clé qui n'expire pas. (Valeur par défaut)
   - Sélectionnez **définissez une heure d'expiration** et définissez la date et l'heure d'expiration.

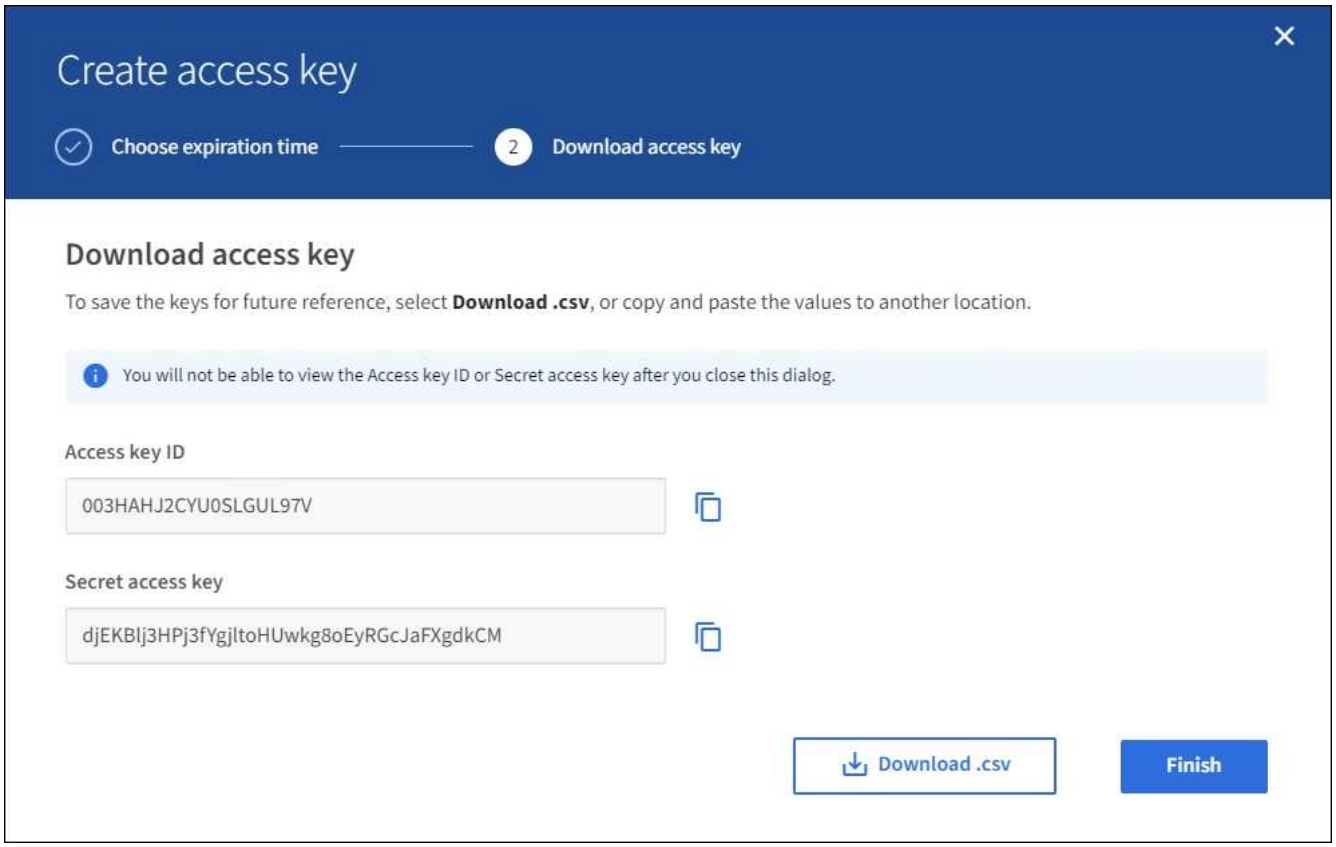


4. Sélectionnez **Créer une clé d'accès**.

   La boîte de dialogue Télécharger la clé d'accès s'affiche, avec la liste de votre ID de clé d'accès et de votre clé secrète d'accès.

5. Copiez l'ID de la clé d'accès et la clé secrète dans un emplacement sûr, ou sélectionnez **Download .csv** pour enregistrer un fichier de feuille de calcul contenant l'ID de la clé d'accès et la clé secrète d'accès.

Ne fermez pas cette boîte de dialogue tant que vous n'avez pas copié ou téléchargé ces informations. Vous ne pouvez pas copier ou télécharger des clés après la fermeture de la boîte de dialogue.



6. Sélectionnez **Terminer**.

   La nouvelle clé apparaît sur la page Mes clés d'accès. L'application des modifications peut prendre jusqu'à 15 minutes à cause de la mise en cache.

Affichez vos clés d'accès S3

Si vous utilisez un locataire S3 et que vous disposez des autorisations appropriées, vous pouvez afficher la liste de vos clés d'accès S3. Vous pouvez trier la liste en fonction de l'heure d'expiration afin de déterminer quelles clés vont bientôt expirer. Si nécessaire, vous pouvez créer de nouvelles clés ou supprimer des clés que vous n'utilisez plus.

Ce dont vous avez besoin

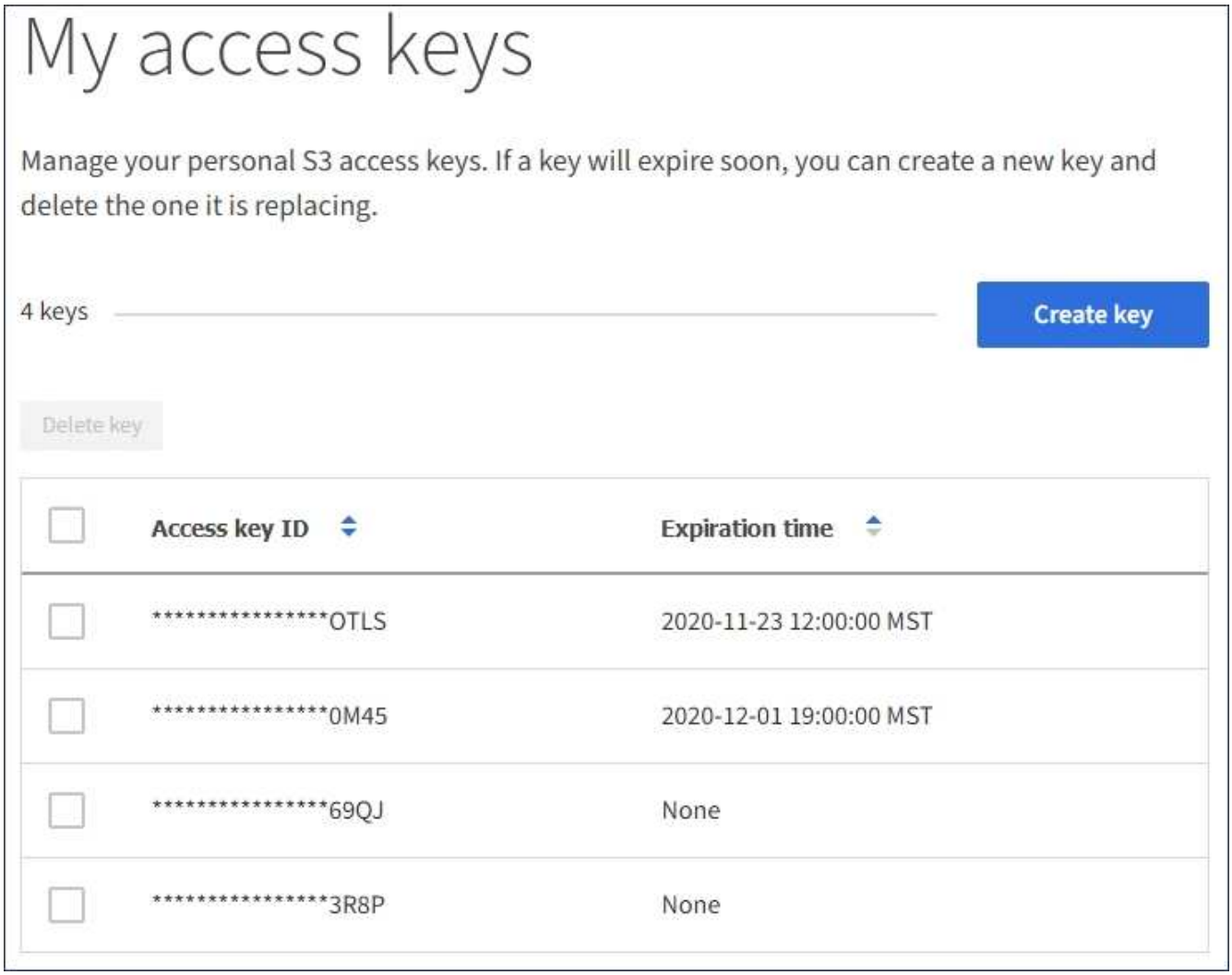
- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur web pris en charge.
- Vous devez disposer de l'autorisation gérer vos propres informations d'identification S3.

Vous pouvez accéder aux compartiments S3 et aux objets appartenant à votre compte à l'aide de l'ID de clé d'accès et de la clé secrète affichée pour votre compte dans le Gestionnaire des locataires. Pour cette raison, protégez les clés d'accès comme vous le feriez avec un mot de passe. Faites pivoter les clés d'accès régulièrement, supprimez les clés inutilisées de votre compte et ne les partagez jamais avec d'autres utilisateurs.

Étapes

1. Sélectionnez **STOCKAGE (S3) Mes clés d'accès**.

   La page Mes touches d'accès s'affiche et répertorie toutes les clés d'accès existantes.



2. Trier les clés par **heure d'expiration** ou **ID de clé d'accès**.
3. Si nécessaire, créez de nouvelles clés et supprimez manuellement les clés que vous n'utilisez plus.

   Si vous créez de nouvelles clés avant l'expiration des clés existantes, vous pouvez commencer à utiliser les nouvelles clés sans perdre temporairement l'accès aux objets du compte.

   Les clés expirées sont supprimées automatiquement.

Informations associées

Créez vos propres clés d'accès S3

Supprimez vos propres clés d'accès S3

Supprimez vos propres clés d'accès S3

Si vous utilisez un locataire S3 et que vous disposez des autorisations appropriées, vous

pouvez supprimer vos propres clés d'accès S3. Une fois la clé d'accès supprimée, elle ne peut plus être utilisée pour accéder aux objets et aux compartiments du compte du locataire.

Ce dont vous avez besoin

- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur web pris en charge.
- Vous devez disposer de l'autorisation gérer vos propres informations d'identification S3. Voir Autorisations de gestion des locataires.

> Vous pouvez accéder aux compartiments S3 et aux objets appartenant à votre compte à l'aide de l'ID de clé d'accès et de la clé secrète affichée pour votre compte dans le Gestionnaire des locataires. Pour cette raison, protégez les clés d'accès comme vous le feriez avec un mot de passe. Faites pivoter les clés d'accès régulièrement, supprimez les clés inutilisées de votre compte et ne les partagez jamais avec d'autres utilisateurs.

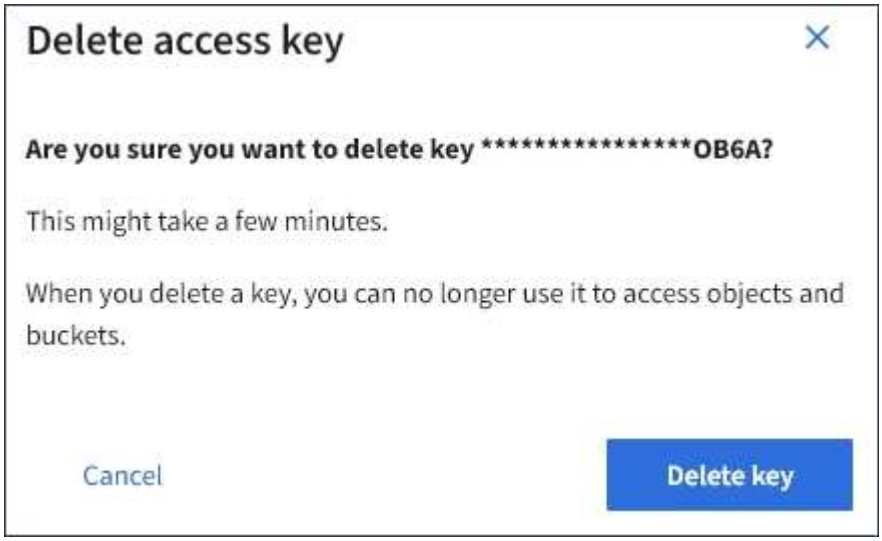
Étapes

1. Sélectionnez **STOCKAGE (S3) Mes clés d'accès**.

   La page Mes touches d'accès s'affiche et répertorie toutes les clés d'accès existantes.

2. Cochez la case correspondant à chaque clé d'accès que vous souhaitez supprimer.
3. Sélectionnez **Supprimer la touche**.

   Une boîte de dialogue de confirmation s'affiche.



4. Sélectionnez **Supprimer la touche**.

   Un message de confirmation s'affiche dans le coin supérieur droit de la page. L'application des modifications peut prendre jusqu'à 15 minutes à cause de la mise en cache.

Créez les clés d'accès S3 d'un autre utilisateur

Si vous utilisez un locataire S3 avec l'autorisation appropriée, vous pouvez créer des clés d'accès S3 pour d'autres utilisateurs, comme les applications qui ont besoin d'accéder à des compartiments et des objets.

Ce dont vous avez besoin

- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur web pris en charge.
- Vous devez disposer de l'autorisation accès racine.

Description de la tâche

Vous pouvez créer une ou plusieurs clés d'accès S3 pour les autres utilisateurs afin qu'ils puissent créer et gérer des compartiments pour leur compte de locataire. Après avoir créé une nouvelle clé d'accès, mettez à jour l'application avec le nouvel ID de clé d'accès et la clé d'accès secrète. Pour des raisons de sécurité, ne créez pas plus de clés que les besoins de l'utilisateur et supprimez les clés qui ne sont pas utilisées. Si vous n'avez qu'une seule clé et que vous êtes sur le point d'expirer, créez une nouvelle clé avant l'expiration de l'ancienne, puis supprimez l'ancienne.

Chaque clé peut avoir une heure d'expiration spécifique ou pas d'expiration. Suivez les directives ci-dessous pour l'heure d'expiration :

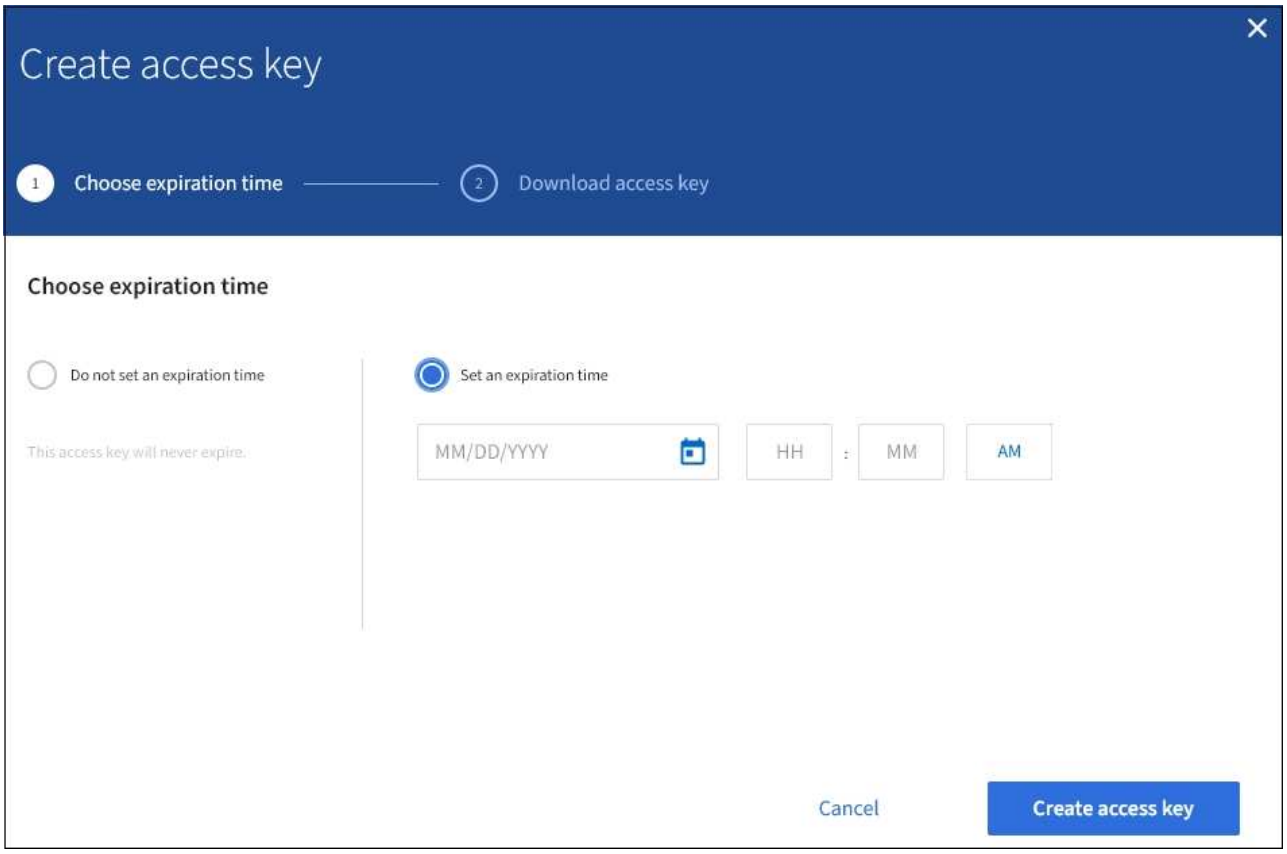
- Définissez un délai d'expiration pour les clés afin de limiter l'accès de l'utilisateur à une certaine période. La définition d'un délai d'expiration court peut aider à réduire le risque si l'ID de clé d'accès et la clé secrète sont exposés accidentellement. Les clés expirées sont supprimées automatiquement.
- Si le risque de sécurité dans votre environnement est faible et que vous n'avez pas besoin de créer régulièrement de nouvelles clés, vous n'avez pas à définir de délai d'expiration pour les clés. Si vous décidez plus tard de créer de nouvelles clés, supprimez les anciennes clés manuellement.

> Les compartiments S3 et les objets appartenant à un utilisateur sont accessibles à l'aide de l'ID de clé d'accès et de la clé secrète affichée pour cet utilisateur dans le Gestionnaire de locataires. Pour cette raison, protégez les clés d'accès comme vous le feriez avec un mot de passe. Faites pivoter les clés d'accès régulièrement, supprimez les clés inutilisées du compte et ne les partagez jamais avec d'autres utilisateurs.

Étapes

1. Sélectionnez **ACCESS MANAGEMENT Users**.
2. Sélectionnez l'utilisateur dont vous souhaitez gérer les clés d'accès S3.

   La page de détails utilisateur s'affiche.
3. Sélectionnez **touches d'accès**, puis **touche Créer**.
4. Effectuez l'une des opérations suivantes :
   - Sélectionnez **ne définissez pas d'heure d'expiration** pour créer une clé qui n'expire pas. (Valeur par défaut)
   - Sélectionnez **définissez une heure d'expiration** et définissez la date et l'heure d'expiration.

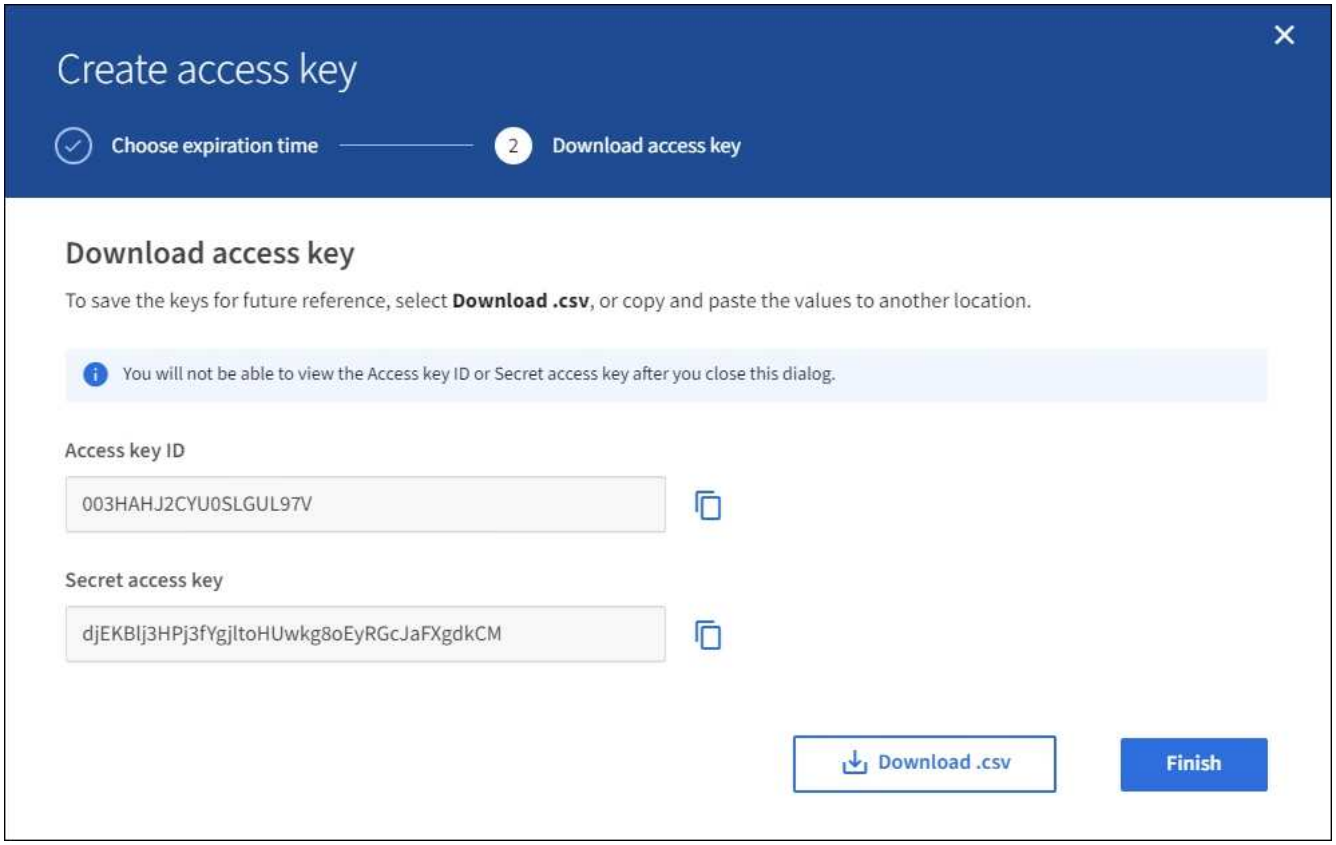


5. Sélectionnez **Créer une clé d'accès**.

   La boîte de dialogue Télécharger la clé d'accès s'affiche, avec la liste de l'ID de clé d'accès et de la clé secrète.

6. Copiez l'ID de la clé d'accès et la clé secrète dans un emplacement sûr, ou sélectionnez **Download .csv** pour enregistrer un fichier de feuille de calcul contenant l'ID de la clé d'accès et la clé secrète d'accès.

   Ne fermez pas cette boîte de dialogue tant que vous n'avez pas copié ou téléchargé ces informations. Vous ne pouvez pas copier ou télécharger des clés après la fermeture de la boîte de dialogue.



7. Sélectionnez **Terminer**.

   La nouvelle clé est répertoriée dans l'onglet touches d'accès de la page des détails de l'utilisateur. L'application des modifications peut prendre jusqu'à 15 minutes à cause de la mise en cache.

Informations associées

Autorisations de gestion des locataires

Afficher les clés d'accès S3 d'un autre utilisateur

Si vous utilisez un locataire S3 et que vous disposez des autorisations appropriées, vous pouvez afficher les clés d'accès S3 d'un autre utilisateur. Vous pouvez trier la liste par heure d'expiration pour déterminer quelles clés vont bientôt expirer. Au besoin, vous pouvez créer de nouvelles clés et supprimer des clés qui ne sont plus utilisées.

Ce dont vous avez besoin

- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur web pris en charge.
- Vous devez disposer de l'autorisation accès racine.

> Les compartiments S3 et les objets appartenant à un utilisateur sont accessibles à l'aide de l'ID de clé d'accès et de la clé secrète affichée pour cet utilisateur dans le Gestionnaire de locataires. Pour cette raison, protégez les clés d'accès comme vous le feriez avec un mot de passe. Faites pivoter les clés d'accès régulièrement, supprimez les clés inutilisées du compte et ne les partagez jamais avec d'autres utilisateurs.

Étapes

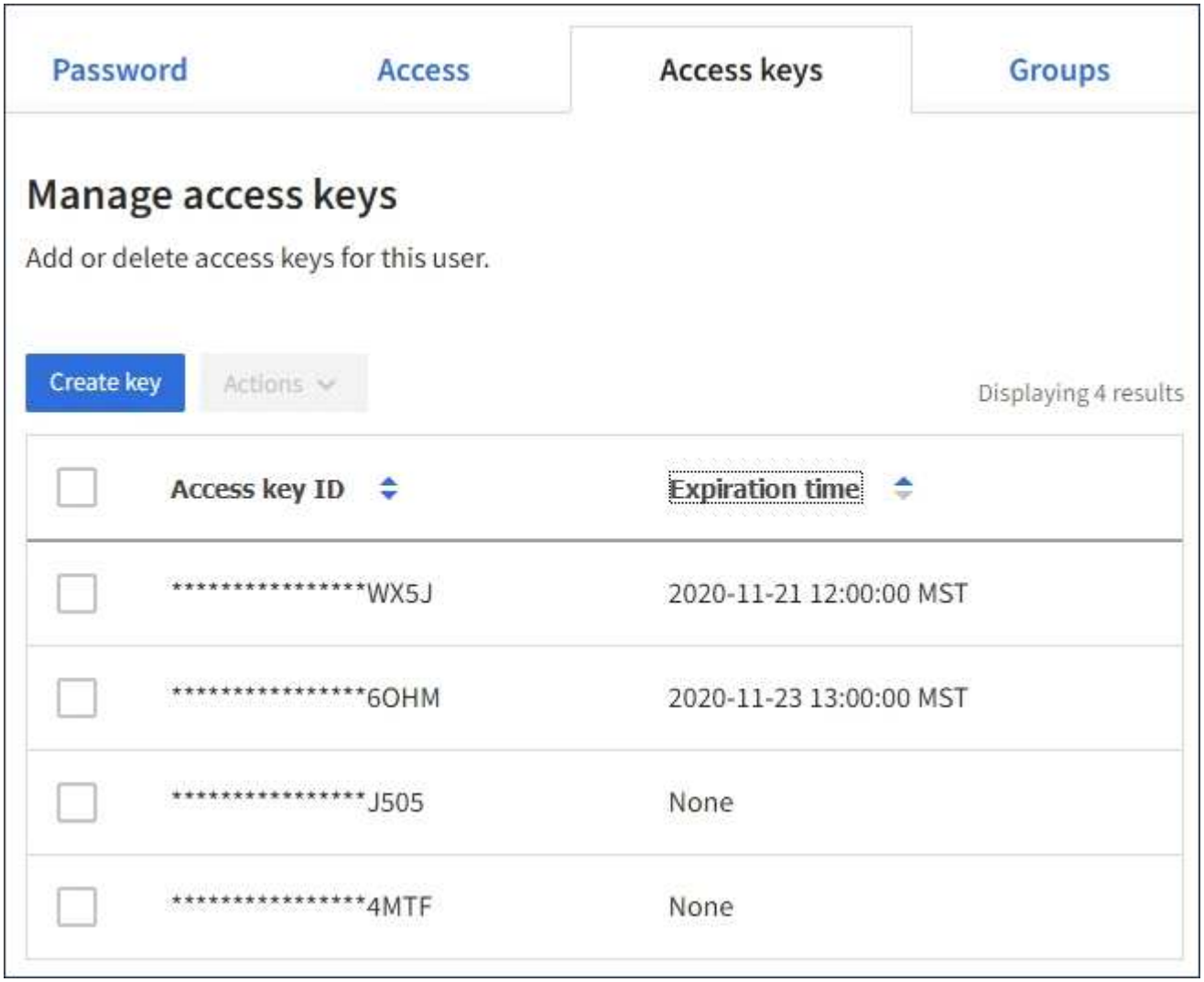
1. Sélectionnez **ACCESS MANAGEMENT Users**.

   La page utilisateurs s'affiche et répertorie les utilisateurs existants.

2. Sélectionnez l'utilisateur dont vous souhaitez afficher les clés d'accès S3.

   La page Détails de l'utilisateur s'affiche.

3. Sélectionnez **touches d'accès**.



4. Trier les clés par **heure d'expiration** ou **ID de clé d'accès**.
5. Si nécessaire, créez de nouvelles clés et supprimez manuellement les clés que le n'est plus utilisé.

   Si vous créez de nouvelles clés avant l'expiration des clés existantes, l'utilisateur peut commencer à utiliser les nouvelles clés sans perdre temporairement l'accès aux objets du compte.

   Les clés expirées sont supprimées automatiquement.

Informations associées

Créez les clés d'accès S3 d'un autre utilisateur

Supprimez les clés d'accès S3 d'un autre utilisateur

Supprimez les clés d'accès S3 d'un autre utilisateur

Si vous utilisez un locataire S3 et que vous disposez des autorisations appropriées, vous pouvez supprimer les clés d'accès S3 d'un autre utilisateur. Une fois la clé d'accès supprimée, elle ne peut plus être utilisée pour accéder aux objets et aux compartiments du compte du locataire.

Ce dont vous avez besoin

- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur web pris en charge.
- Vous devez disposer de l'autorisation accès racine. Voir Autorisations de gestion des locataires.

> Les compartiments S3 et les objets appartenant à un utilisateur sont accessibles à l'aide de l'ID de clé d'accès et de la clé secrète affichée pour cet utilisateur dans le Gestionnaire de locataires. Pour cette raison, protégez les clés d'accès comme vous le feriez avec un mot de passe. Faites pivoter les clés d'accès régulièrement, supprimez les clés inutilisées du compte et ne les partagez jamais avec d'autres utilisateurs.

Étapes

1. Sélectionnez **ACCESS MANAGEMENT Users**.

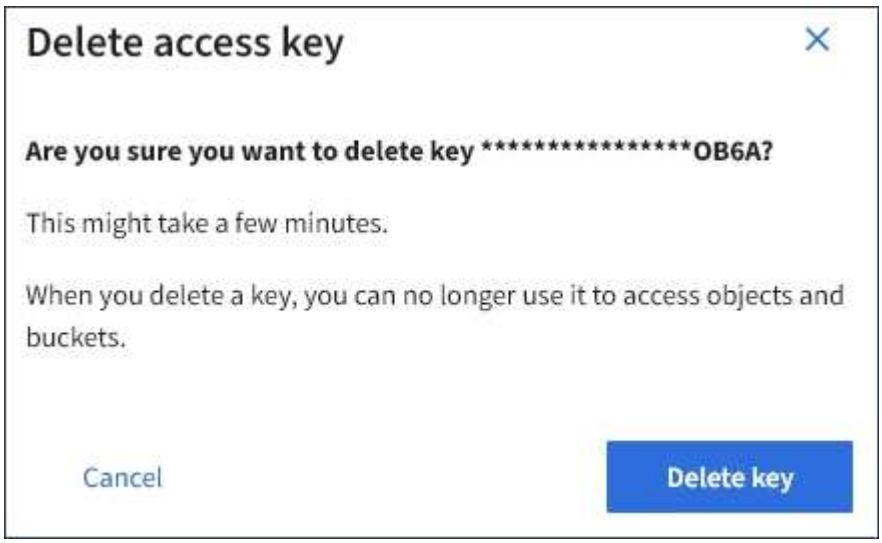
   La page utilisateurs s'affiche et répertorie les utilisateurs existants.

2. Sélectionnez l'utilisateur dont vous souhaitez gérer les clés d'accès S3.

   La page Détails de l'utilisateur s'affiche.

3. Sélectionnez **touches d'accès**, puis cochez la case pour chaque clé d'accès que vous souhaitez supprimer.
4. Sélectionnez **actions Supprimer la touche sélectionnée**.

   Une boîte de dialogue de confirmation s'affiche.



5. Sélectionnez **Supprimer la touche**.

   Un message de confirmation s'affiche dans le coin supérieur droit de la page. L'application des modifications peut prendre jusqu'à 15 minutes à cause de la mise en cache.

Gestion des compartiments S3

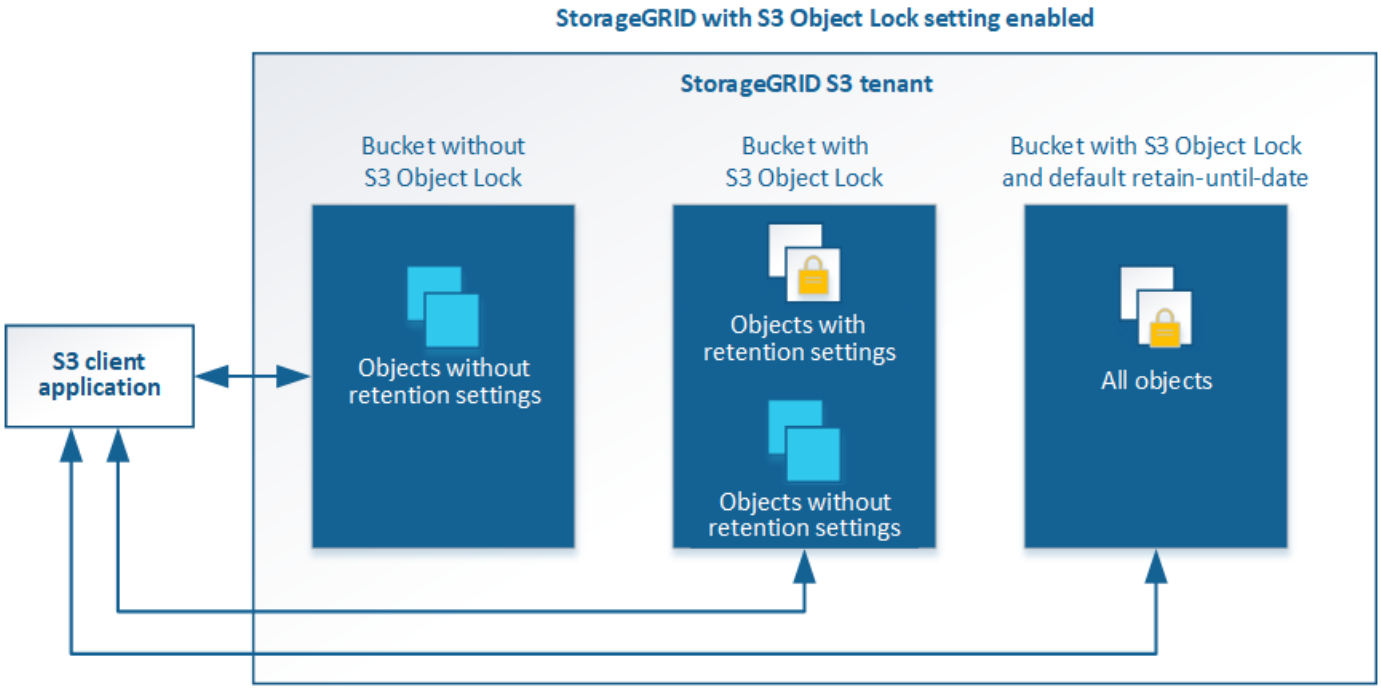
Utilisez la fonction de verrouillage d'objet S3 avec les locataires

Vous pouvez utiliser la fonctionnalité de verrouillage d'objet S3 dans StorageGRID si vos objets doivent être conformes aux exigences réglementaires en matière de conservation.

Qu'est-ce que le verrouillage objet S3 ?

La fonctionnalité de verrouillage objet StorageGRID S3 est une solution de protection des objets équivalente au verrouillage objet S3 dans Amazon simple Storage Service (Amazon S3).

Comme illustré dans la figure, lorsque le paramètre global de verrouillage d'objet S3 est activé pour un système StorageGRID, un compte de locataire S3 peut créer des compartiments avec ou sans verrouillage d'objet S3 activé. Si un compartiment est doté du verrouillage objet S3 activé, les applications client S3 peuvent éventuellement spécifier des paramètres de conservation pour toute version d'objet dans ce compartiment. Des paramètres de conservation doivent être spécifiés pour être protégés par le verrouillage d'objet S3.



La fonctionnalité de verrouillage d'objet StorageGRID S3 fournit un mode de conservation unique équivalent au mode de conformité Amazon S3. Par défaut, une version d'objet protégé ne peut être écrasée ou supprimée par aucun utilisateur. La fonction de verrouillage d'objet StorageGRID S3 ne prend pas en charge un mode de gouvernance et n'autorise pas les utilisateurs disposant d'autorisations spéciales à contourner les paramètres de rétention ou à supprimer des objets protégés.

Si un compartiment est doté de l'option de verrouillage des objets S3, l'application client S3 peut spécifier la ou les deux paramètres de conservation de niveau objet suivants lors de la création ou de la mise à jour d'un objet :

- **Conserver-jusqu'à-date** : si la date-à-jour d'une version d'objet est à l'avenir, l'objet peut être récupéré, mais ne peut pas être modifié ou supprimé. Si nécessaire, la date de conservation d'un objet peut être augmentée, mais cette date ne peut pas être réduite.

- **Mise en garde légale** : l'application d'une mise en garde légale à une version d'objet verrouille immédiatement cet objet. Par exemple, vous devrez peut-être mettre une obligation légale sur un objet lié à une enquête ou à un litige juridique. Une obligation légale n'a pas de date d'expiration, mais reste en place jusqu'à ce qu'elle soit explicitement supprimée. Les dispositions légales sont indépendantes de la date de conservation.

Vous pouvez également spécifiez un mode de conservation par défaut et la période de conservation par défaut pour le compartiment. Elles sont appliquées à chaque objet ajouté au compartiment qui ne spécifie pas ses propres paramètres de rétention.

Pour plus de détails sur ces paramètres, reportez-vous à la section Utilisez le verrouillage d'objet S3.

Gestion des compartiments conformes aux ancienne génération

La fonction de verrouillage d'objet S3 remplace la fonction de conformité disponible dans les versions StorageGRID précédentes. Si vous avez créé des compartiments conformes à l'aide d'une version précédente de StorageGRID, vous pouvez continuer à gérer les paramètres de ces compartiments. Toutefois, vous ne pouvez plus créer de compartiments conformes. Pour en savoir plus, consultez l'article de la base de connaissance NetApp.

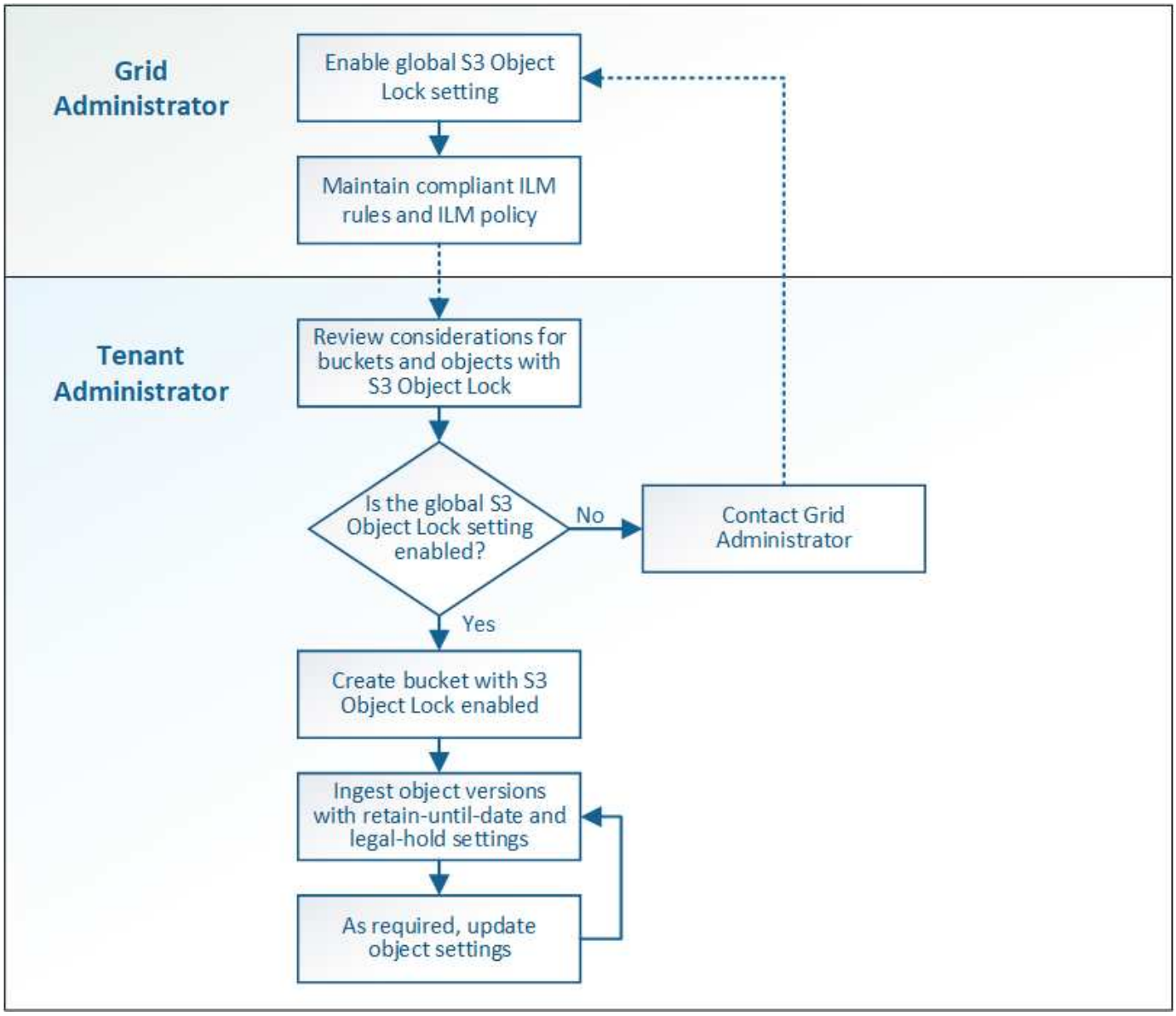
"Base de connaissances NetApp : comment gérer des compartiments conformes aux ancienne génération dans StorageGRID 11.5"

Workflow de verrouillage d'objet S3

Le schéma de workflow montre les étapes générales d'utilisation de la fonction de verrouillage d'objet S3 dans StorageGRID.

Avant de créer des compartiments avec le verrouillage d'objet S3 activé, l'administrateur de la grille doit activer le paramètre de verrouillage d'objet S3 global pour l'ensemble du système StorageGRID. L'administrateur du grid doit également s'assurer que La gestion du cycle de vie de l'information (ILM Est « conforme » ; il doit répondre aux exigences des compartiments lorsque le verrouillage d'objet S3 est activé. Pour plus d'informations, contactez votre administrateur de la grille ou consultez les instructions relatives à la gestion des objets avec la gestion du cycle de vie des informations.

Une fois que le paramètre de verrouillage d'objet S3 global a été activé, vous pouvez créer des compartiments avec le verrouillage d'objet S3 activé. Vous pouvez ensuite utiliser l'application client S3 pour spécifier les paramètres de conservation pour chaque version d'objet.



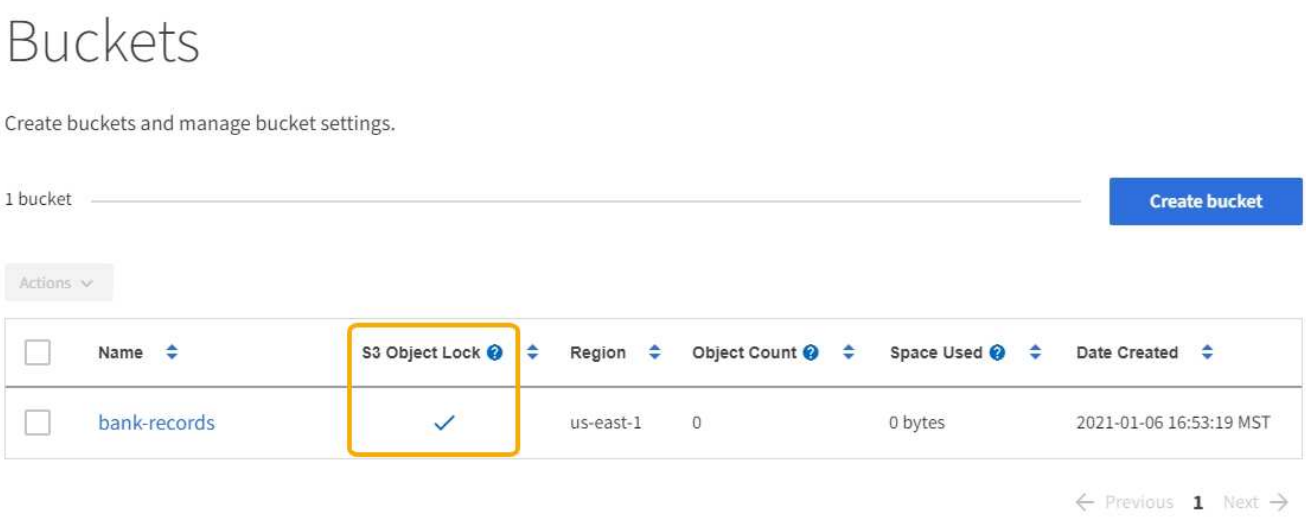
Conditions requises pour le verrouillage d'objet S3

Avant d'activer le verrouillage d'objet S3 pour un compartiment, vérifiez les exigences relatives aux compartiments et aux objets S3 Object Lock ainsi que le cycle de vie des objets dans des compartiments où le verrouillage d'objet S3 est activé.

Conditions requises pour les compartiments avec verrouillage objet S3 activé

- Si le paramètre global de verrouillage 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 compartiments avec le verrouillage objet S3 activé.

  Dans cet exemple, le gestionnaire des locataires affiche un compartiment avec le verrouillage objet S3 activé.



- Si vous prévoyez d'utiliser le verrouillage d'objet S3, vous devez activer le verrouillage d'objet S3 lors de la création du compartiment. Vous ne pouvez pas activer le verrouillage d'objet S3 pour un compartiment existant.
- Le contrôle de version de compartiment est requis avec le verrouillage d'objet S3. Lorsque le verrouillage d'objet S3 est activé pour un compartiment, StorageGRID active automatiquement le contrôle de version pour ce compartiment.
- Une fois que vous avez créé un compartiment avec le verrouillage d'objet S3 activé, vous ne pouvez pas désactiver le verrouillage d'objet S3 ou suspendre la gestion des versions pour ce compartiment.
- Vous pouvez également configurer la conservation par défaut d'un compartiment. Lors du téléchargement d'une version d'objet, la conservation par défaut est appliquée à la version de l'objet. Vous pouvez remplacer la valeur par défaut du compartiment en spécifiant un mode de rétention et une date de conservation dans la demande de téléchargement d'une version d'objet.
- La configuration du cycle de vie des compartiments est prise en charge pour les compartiments de cycle de vie des objets S3.
- La réplication CloudMirror n'est pas prise en charge pour les compartiments avec le verrouillage objet S3 activé.

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

- Pour protéger la version d'un objet, l'application client S3 doit configurer la conservation par défaut du compartiment ou spécifier les paramètres de conservation dans chaque demande de téléchargement.
- Vous pouvez augmenter la valeur de conservation jusqu'à la date d'une version d'objet, mais vous ne pouvez jamais la diminuer.
- Si vous êtes averti d'une action légale ou d'une enquête réglementaire en attente, vous pouvez conserver les informations pertinentes en plaçant une mise en garde légale sur une version d'objet. Lorsqu'une version d'objet est soumise à une conservation légale, cet objet ne peut pas être supprimé de StorageGRID, même si elle a atteint sa date de conservation. Dès que la mise en attente légale est levée, la version de l'objet peut être supprimée si la date de conservation a été atteinte.
- Le verrouillage d'objet S3 requiert l'utilisation de compartiments avec version. Les paramètres de conservation s'appliquent aux versions d'objet individuelles. Une version d'objet peut avoir à la fois un paramètre de conservation à la date et un paramètre de conservation légal, l'un mais pas l'autre, ou l'autre. La spécification d'un paramètre de conservation à la date ou d'un paramètre de conservation légal 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 des compartiments avec verrouillage objet S3 activé

Chaque objet enregistré dans un compartiment avec l'option de verrouillage d'objet S3 passe en trois étapes :

1. **Entrée d'objet**
   - Lorsque vous ajoutez une version d'objet dans un compartiment lorsque le verrouillage objet S3 est activé, l'application client S3 peut spécifier des paramètres de conservation pour l'objet (conservation à la date, conservation légale ou les deux). StorageGRID génère ensuite les métadonnées de cet objet, qui incluent un identificateur d'objet unique (UUID) et la date et l'heure d'ingestion.
   - Lors de l'ingestion d'une version d'objet avec paramètres de conservation, les données et les métadonnées S3 définies par l'utilisateur ne peuvent pas être modifiées.
   - StorageGRID stocke les métadonnées objet indépendamment des données de l'objet. Elle conserve trois copies de toutes les métadonnées d'objet sur chaque site.
2. **Rétention d'objet**
   - Plusieurs copies de l'objet sont stockées par StorageGRID. Le nombre et le type exacts de copies ainsi que les emplacements de stockage sont déterminés par les règles conformes de la politique ILM active.
3. **Suppression d'objet**
   - Un objet peut être supprimé lorsque sa date de conservation est atteinte.
   - Impossible de supprimer un objet en attente légale.

Créer un compartiment S3

Vous pouvez utiliser le Gestionnaire des locataires pour créer des compartiments S3 pour les données d'objet. Lorsque vous créez un compartiment, vous devez spécifier son nom et sa région. Si le paramètre global de verrouillage d'objet S3 est activé pour le système StorageGRID, vous pouvez activer le verrouillage d'objet S3 pour le compartiment.

Ce dont vous avez besoin

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un navigateur web pris en charge.
- Vous appartenez à un groupe d'utilisateurs possédant l'autorisation gérer toutes les rubriques ou accès racine. Ces autorisations remplacent les paramètres d'autorisations des stratégies de groupes ou de compartiments.

  > Les autorisations 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 règle de groupe.

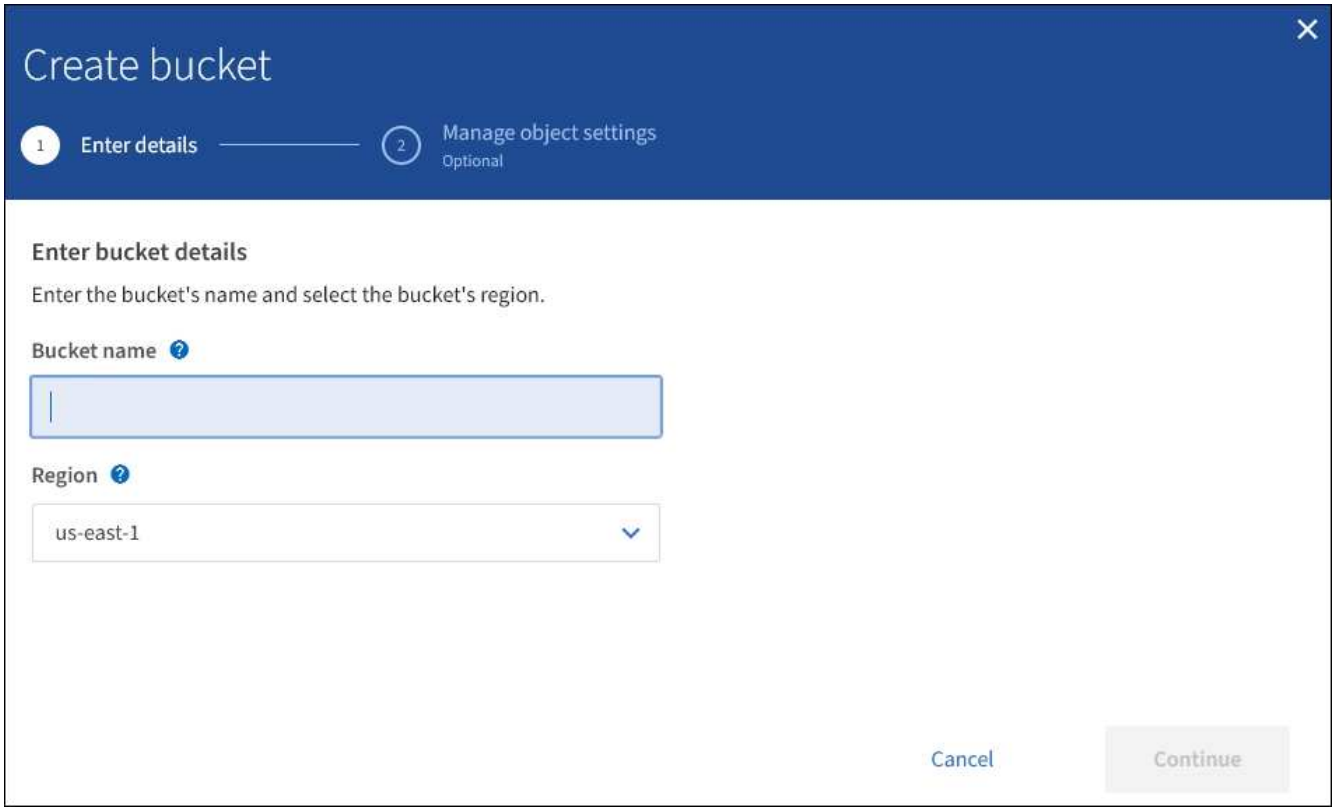
- Si vous prévoyez de créer un compartiment avec le verrouillage d'objet S3, vous avez activé le paramètre de verrouillage d'objet S3 global pour le système StorageGRID et vous avez examiné les exigences relatives aux compartiments et aux objets de verrouillage d'objet S3.

  Utilisez le verrouillage d'objet S3

Étapes

1. Sélectionnez **STOCKAGE (S3) seaux**.

2. Sélectionnez **Créer un compartiment**.



3. Entrer un nom unique pour le compartiment.

> Vous ne pouvez pas modifier le nom d'un compartiment après sa création.

Les noms de compartiment doivent être conformes aux règles suivantes :

- Il doit être unique sur chaque système StorageGRID (et pas seulement au sein du compte du locataire).
- Doit être conforme DNS.
- Doit contenir au moins 3 caractères et pas plus de 63 caractères.
- Chaque étiquette doit commencer et se terminer par une lettre ou un chiffre en minuscules et ne peut utiliser que des lettres minuscules, des chiffres et des tirets.
- Ne doit pas utiliser de périodes dans des demandes de type hébergement virtuel. Les périodes provoquera des problèmes avec la vérification du certificat générique du serveur.

> Pour plus d'informations, reportez-vous à la section "Documentation Amazon Web Services (AWS) sur les règles d'attribution de nom de compartiment".

4. Sélectionnez la région de ce compartiment.

L'administrateur StorageGRID gère les régions disponibles. Ce compartiment peut affecter la règle de protection des données appliquée aux objets. Par défaut, tous les compartiments sont créés dans le `us-east-1` région.

> Vous ne pouvez pas modifier la région après avoir créé le compartiment.

5. Sélectionnez **Continuer**.
6. Activez éventuellement le contrôle de version d'objet pour le compartiment.

   Activez la gestion des versions d'objet si vous souhaitez stocker chaque version de chaque objet dans ce compartiment. Vous pouvez ensuite récupérer les versions précédentes d'un objet si nécessaire.

7. Si la section verrouillage d'objet S3 s'affiche, activez éventuellement le verrouillage d'objet S3 pour le compartiment.

   > Vous ne pouvez pas activer ou désactiver le verrouillage d'objet S3 après la création du compartiment.

   La section verrouillage d'objet S3 s'affiche uniquement si le paramètre verrouillage d'objet S3 global est activé.

   Le verrouillage objet S3 doit être activé pour le compartiment avant qu'une application client S3 puisse spécifier des paramètres de conservation à une date et de conservation légale pour les objets ajoutés au compartiment.

   Si vous activez le verrouillage des objets S3 pour un compartiment, le contrôle de version des compartiments est automatiquement activé. Vous pouvez également spécifiez un mode de conservation par défaut et la période de conservation par défaut pour le compartiment qui sont appliquées à chaque objet ingéré dans le compartiment qui ne spécifie pas ses propres paramètres de conservation.

8. Sélectionnez **Créer un compartiment**.

   Le godet est créé et ajouté au tableau sur la page godets.

Informations associées

Gestion des objets avec ILM

Compréhension de l'API de gestion des locataires

Utilisation de S3

Affichez les détails du compartiment S3

Vous pouvez afficher la liste des compartiments et des paramètres de compartiment dans votre compte de locataire.

Ce dont vous avez besoin

- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur web pris en charge.

Étapes

1. Sélectionnez **STOCKAGE (S3) seaux**.

   La page rubriques s'affiche et répertorie toutes les rubriques du compte locataire.

2. Passer en revue les informations relatives à chaque godet.

   Si nécessaire, vous pouvez trier les informations par colonne, ou vous pouvez avancer et revenir à la liste.

   - Nom : nom unique du compartiment, qui ne peut pas être modifié.
   - Verrouillage de l'objet S3 : indique si le verrouillage de l'objet S3 est activé pour ce compartiment.

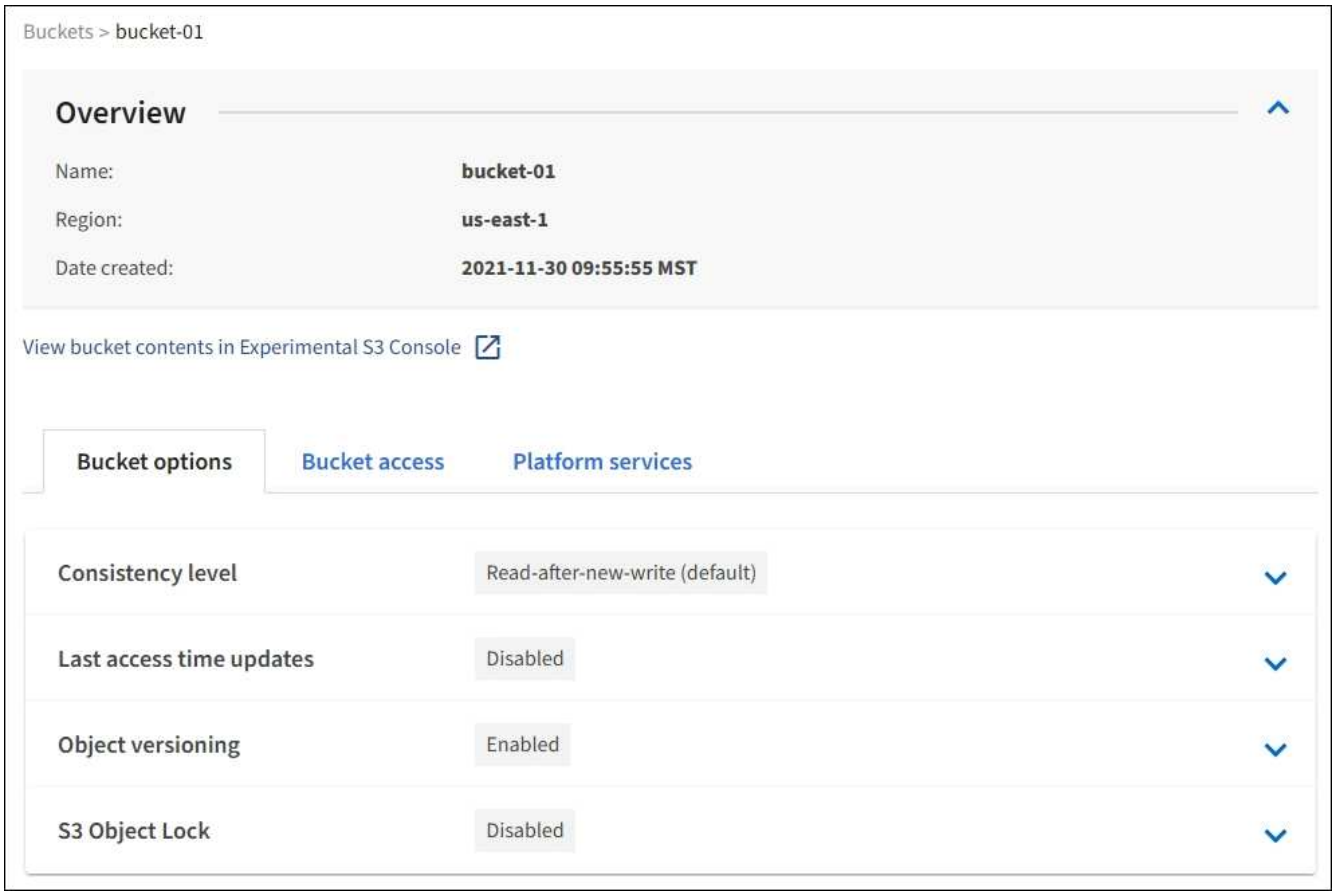
     Cette colonne n'est pas affichée si le paramètre de verrouillage d'objet S3 global est désactivé. Cette colonne affiche également des informations pour tous les compartiments conformes existants.

   - Région : région du godet, qui ne peut pas être modifiée.
   - Nombre d'objets : nombre d'objets dans ce compartiment.
   - Espace utilisé : taille logique de tous les objets de ce compartiment. La taille logique n'inclut pas l'espace réel requis pour les copies répliquées ou avec code d'effacement, ni pour les métadonnées d'objet.
   - Date de création : date et heure de création du compartiment.

   > Les valeurs nombre d'objets et espace utilisé affichées sont des estimations. Ces estimations sont affectées par le moment de l'ingestion, la connectivité réseau et l'état des nœuds. Si la gestion des versions des compartiments est activée, les versions des objets supprimés sont incluses dans le nombre d'objets.

3. Pour afficher et gérer les paramètres d'un compartiment, sélectionnez le nom du compartiment.

   La page des détails du compartiment vous permet d'afficher et de modifier les paramètres des options du compartiment, de l'accès au compartiment, et services de plateforme.



Modifiez le niveau de cohérence

Si vous utilisez un locataire S3, vous pouvez utiliser le gestionnaire des locataires ou l'API de gestion des locataires pour modifier le contrôle de cohérence pour les opérations effectuées sur les objets dans des compartiments S3.

Ce dont vous avez besoin

- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur web pris en charge.
- Vous devez appartenir à un groupe d'utilisateurs possédant l'autorisation gérer toutes les rubriques ou accès racine. Ces autorisations remplacent les paramètres d'autorisations des stratégies de groupes ou de compartiments. Voir Autorisations de gestion des locataires.

Description de la tâche

Le niveau de cohérence assure un équilibre entre la disponibilité des objets et la cohérence de ces objets entre plusieurs nœuds de stockage et sites. En général, vous devez utiliser le niveau de cohérence **Read-After-New-write** pour vos compartiments.

Si le niveau de cohérence **Read-After-New-write** ne répond pas aux exigences de l'application client, vous pouvez modifier le niveau de cohérence en définissant le niveau de cohérence du compartiment ou en utilisant le `Consistency-Control` en-tête. Le `Consistency-Control` le cueilleur remplace le niveau de cohérence du godet.

> Lorsque vous modifiez le niveau de cohérence d'un compartiment, seuls les objets ingérées après la modification sont garantis pour satisfaire le niveau révisé.

Étapes

1. Sélectionnez **STOCKAGE (S3) seaux**.
2. Sélectionnez le nom du compartiment dans la liste.

   La page des détails du compartiment s'affiche.

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

Activez ou désactivez les mises à jour de l'heure du dernier accès

Les administrateurs du grid créent les règles de gestion du cycle de vie des informations d'un système StorageGRID. Ils ont la possibilité de spécifier la date d'accès de dernier objet afin de déterminer si celui-ci doit être déplacé vers un autre emplacement de stockage. Si vous utilisez un locataire S3, vous pouvez activer ces règles en activant les mises à jour de l'heure du dernier accès pour les objets dans un compartiment S3.

Ces instructions s'appliquent uniquement aux systèmes StorageGRID qui incluent au moins une règle ILM utilisant l'option **dernier accès** dans ses instructions de placement. Vous pouvez ignorer ces instructions si votre système StorageGRID n'inclut pas une telle règle.

Ce dont vous avez besoin

- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur web pris en charge.
- Vous devez appartenir à un groupe d'utilisateurs possédant l'autorisation gérer toutes les rubriques ou accès racine. Ces autorisations remplacent les paramètres d'autorisations des stratégies de groupes ou de compartiments. Voir Autorisations de gestion des locataires.

Heure de dernier accès est l'une des options disponibles pour l'instruction de placement **temps de référence** pour une règle ILM. La définition de l'heure de référence d'une règle sur heure du dernier accès permet aux administrateurs de la grille de spécifier que les objets doivent être placés dans certains emplacements de stockage en fonction de la date de récupération de ces objets (lecture ou visualisation).

Par exemple, pour s'assurer que les objets récemment affichés restent dans un stockage plus rapide, un administrateur du grid peut créer une règle ILM spécifiant ce qui suit :

- 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 dernier mois doivent être déplacés vers un emplacement hors site.

Voir les instructions de gestion des objets avec la gestion du cycle de vie des informations.

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

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

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

- Mettre à jour les objets avec de nouveaux horodatages
- Ajoutez ces objets à la file d'attente ILM pour une réévaluation des règles et règles ILM actuelles

Le tableau récapitule 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	
	Heure du dernier accès mise à jour ?	Objet ajouté à la file d'attente d'évaluation ILM ?	Heure du dernier 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.
Demander de copier un objet d'un compartiment à un autre	• Non, pour la copie source • Oui, pour la copie de destination	• Non, pour la copie source • Oui, pour la copie de destination	• Oui, pour la copie source • Oui, pour la copie de destination	• Oui, pour la copie source • Oui, pour la copie de destination

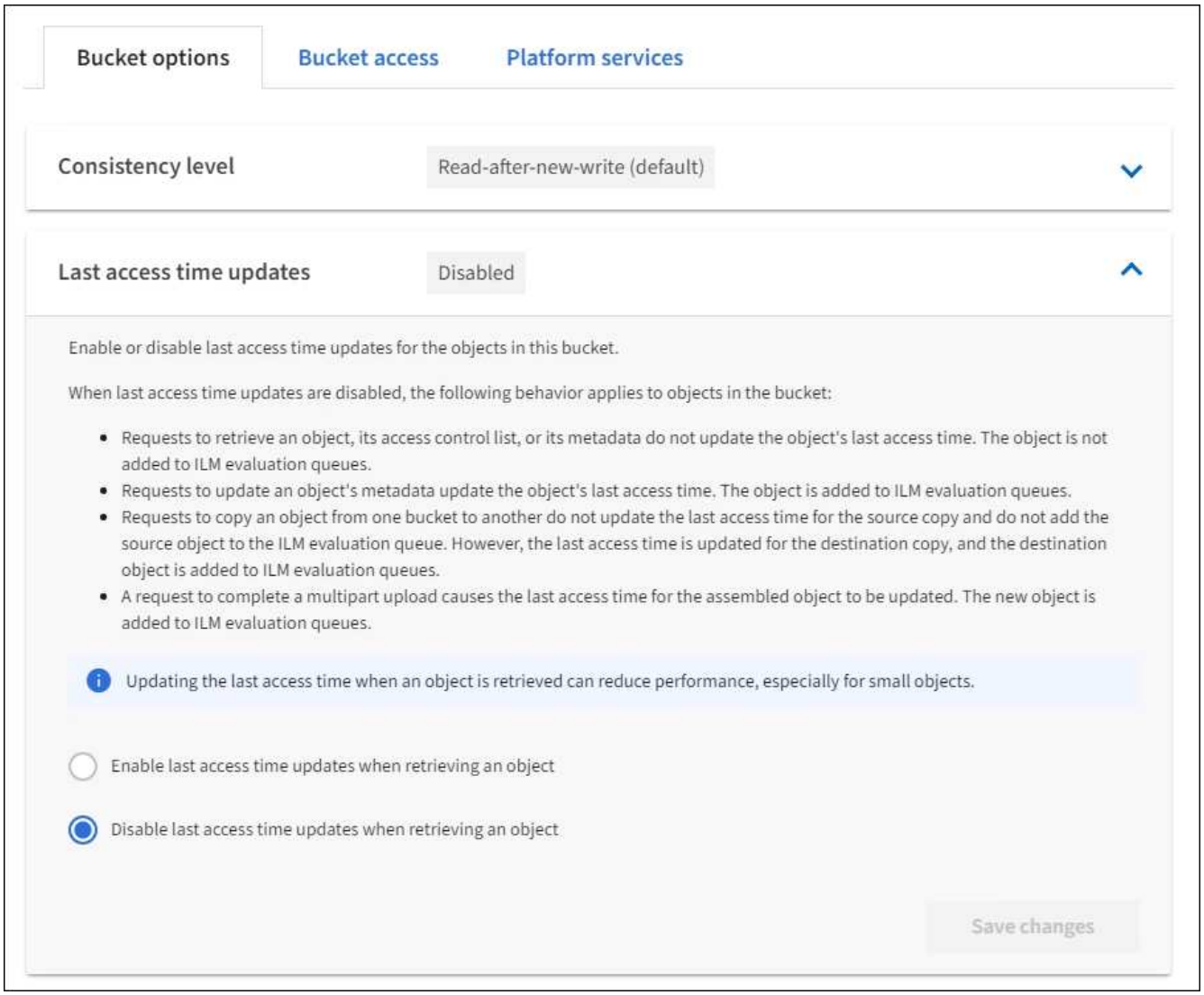
Demander de terminer un téléchargement partitionné	Oui, pour l'objet assemblé	Oui, pour l'objet assemblé	Oui, pour l'objet assemblé	Oui, pour l'objet assemblé

Étapes

1. Sélectionnez **STOCKAGE (S3) seaux**.
2. Sélectionnez le nom du compartiment dans la liste.

   La page des détails du compartiment s'affiche.

3. Sélectionnez **Options de rubrique mises à jour des dernières temps d'accès**.
4. Sélectionnez le bouton radio approprié pour activer ou désactiver les dernières mises à jour des heures d'accès.



5. Sélectionnez **Enregistrer les modifications**.

Informations associées

Autorisations de gestion des locataires

Gestion des objets avec ILM

Modifiez le contrôle de version d'objet pour un compartiment

Si vous utilisez un locataire S3, vous pouvez utiliser le Gestionnaire des locataires ou l'API de gestion des locataires pour modifier l'état des versions des compartiments S3.

Ce dont vous avez besoin

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un navigateur web pris en charge.
- Vous appartenez à un groupe d'utilisateurs possédant l'autorisation gérer toutes les rubriques ou accès racine. Ces autorisations remplacent les paramètres d'autorisations des stratégies de groupes ou de compartiments.

  Autorisations de gestion des locataires

Description de la tâche

Vous pouvez activer ou suspendre la gestion des versions d'objet pour un compartiment. Une fois que vous avez activé la gestion des versions d'un compartiment, celui-ci ne peut plus revenir à un état sans version. Toutefois, vous pouvez suspendre le contrôle de version du compartiment.

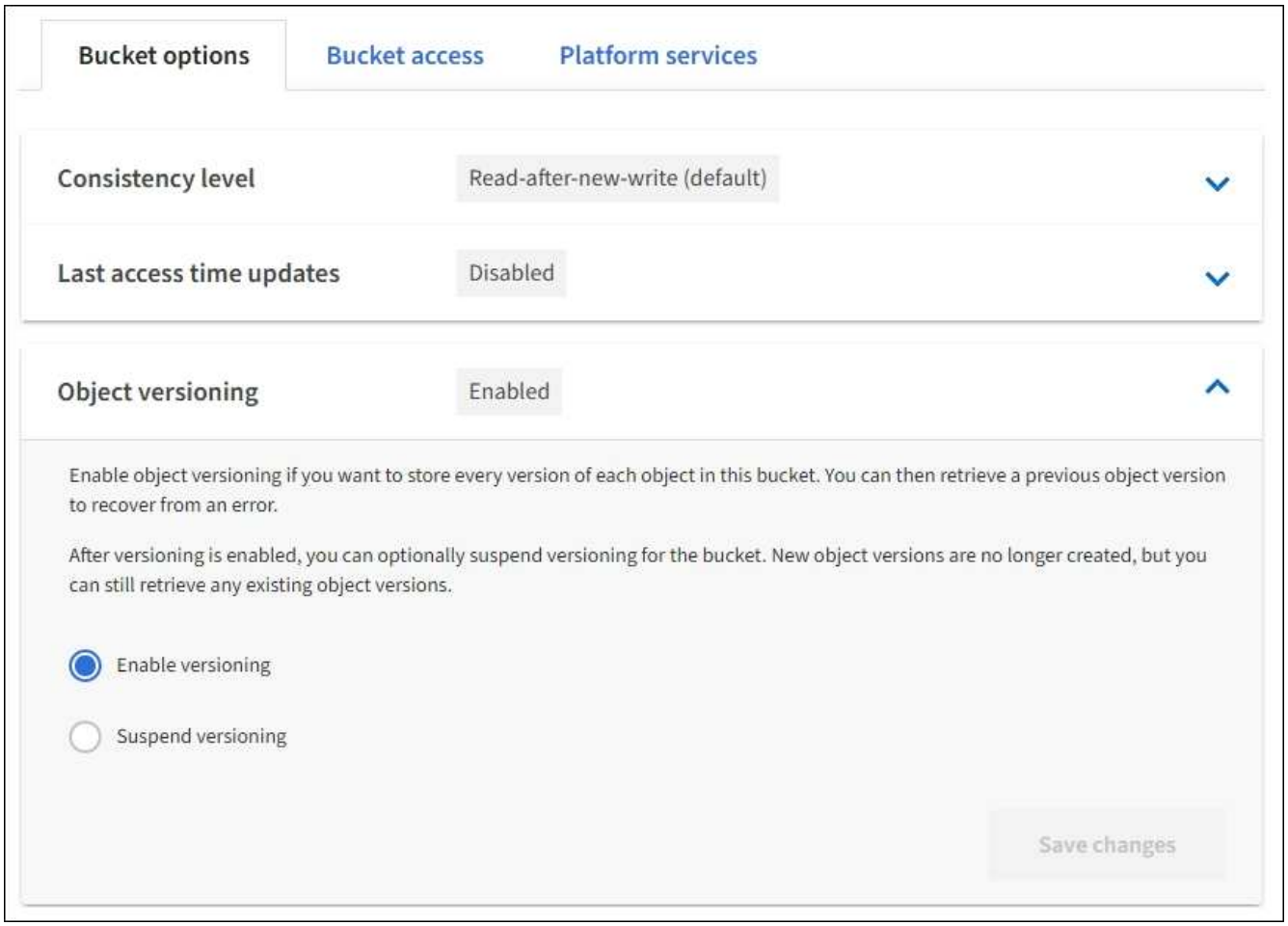
- Désactivé : le contrôle de version n'a jamais été activé
- Activé : la gestion des versions est activée
- Suspendu : la gestion des versions a déjà été activée et est suspendue

Gestion des versions d'objets S3

Règles et règles ILM pour les objets avec version S3 (exemple 4)

Étapes

1. Sélectionnez **STOCKAGE (S3) seaux**.
2. Sélectionnez le nom du compartiment dans la liste.
3. Sélectionnez **Options de rubrique gestion des versions d'objet**.



4. Sélectionnez un état de gestion des versions pour les objets de ce compartiment.

> Si le verrouillage d'objet S3 ou la conformité héritée est activée, les options **Object versionnage** sont désactivées.

Option	Description
Activez le contrôle des versions	Activez la gestion des versions d'objet si vous souhaitez stocker chaque version de chaque objet dans ce compartiment. Vous pouvez ensuite récupérer les versions précédentes d'un objet si nécessaire. Les objets qui se trouvent déjà dans le compartiment sont avec gestion de version lorsqu'ils sont modifiés par l'utilisateur.
Suspendre la gestion des versions	Suspendre la gestion des versions d'objet si vous ne souhaitez plus créer de nouvelles versions d'objet. Vous pouvez toujours récupérer toutes les versions d'objet existantes.

5. Sélectionnez **Enregistrer les modifications**.

Configurer le partage de ressources inter-origine (CORS)

Vous pouvez configurer le partage de ressources inter-origine (CORS) pour un

compartiment S3 si vous souhaitez que ce compartiment et les objets de ce compartiment soient accessibles aux applications Web dans d'autres domaines.

Ce dont vous avez besoin

- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur web pris en charge.
- Vous devez appartenir à un groupe d'utilisateurs possédant l'autorisation gérer toutes les rubriques ou accès racine. Ces autorisations remplacent les paramètres d'autorisations des stratégies de groupes ou de compartiments.

Description de la tâche

Le partage de ressources d'origine croisée (CORS) est un mécanisme de sécurité qui permet aux applications Web clientes d'un domaine d'accéder aux ressources d'un domaine différent. Supposons par exemple que vous utilisez un compartiment S3 nommé `Images` pour stocker des graphiques. En configurant CORS pour l'`Images` le champ permet d'afficher les images de ce compartiment sur le site web `http://www.example.com`.

Étapes

1. Utilisez un éditeur de texte pour créer le XML requis pour activer CORS.

   Cet exemple montre le code XML utilisé pour activer le code commande pour un compartiment S3. Ce XML permet à n'importe quel domaine d'envoyer des requêtes GET au compartiment, mais il n'autorise que le `http://www.example.com` Domaine pour envoyer des demandes POST et DE SUPPRESSION. Tous les en-têtes de demande sont autorisés.

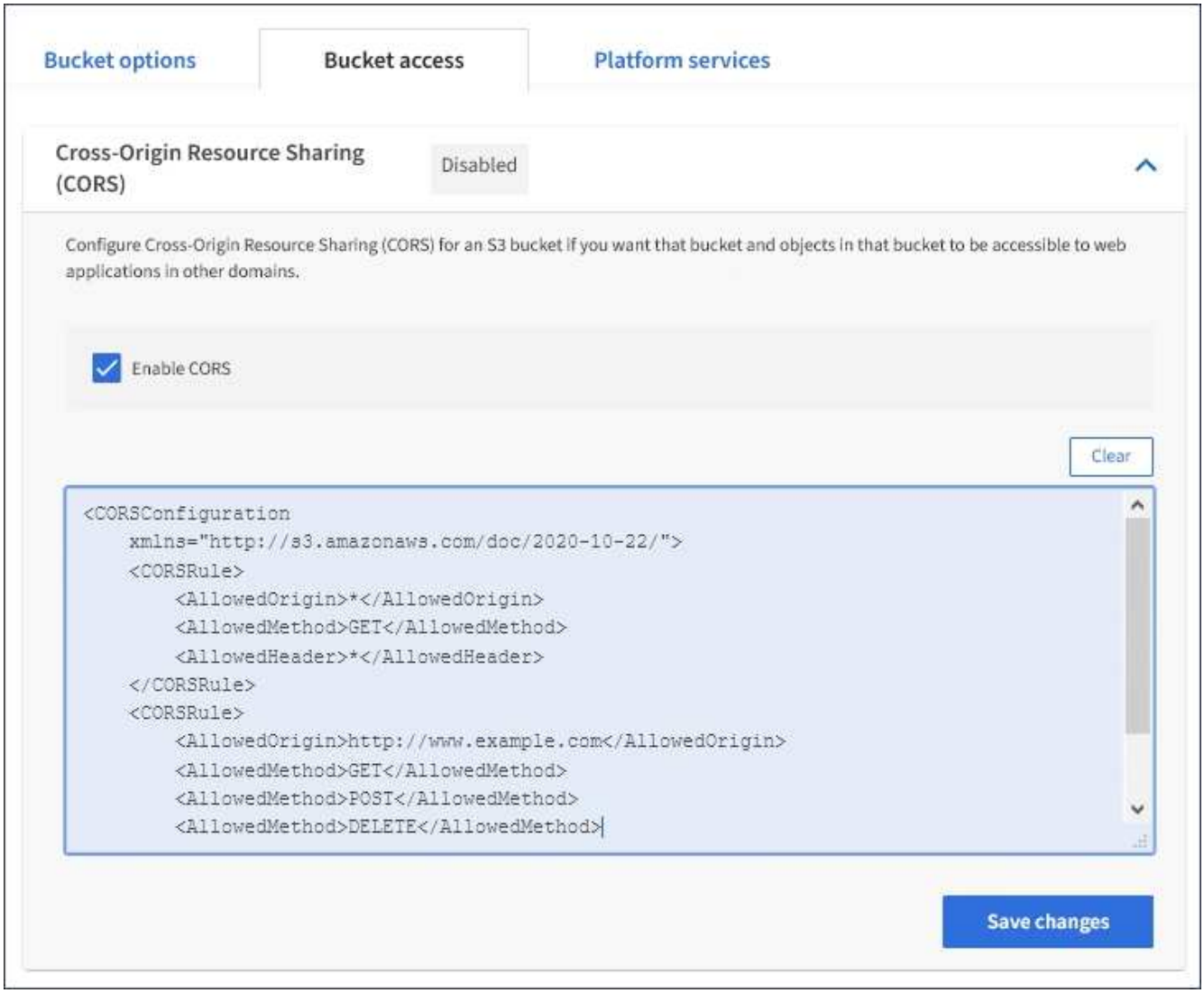
   ```
   <CORSConfiguration
       xmlns="http://s3.amazonaws.com/doc/2020-10-22/">
       <CORSRule>
           <AllowedOrigin>*</AllowedOrigin>
           <AllowedMethod>GET</AllowedMethod>
           <AllowedHeader>*</AllowedHeader>
       </CORSRule>
       <CORSRule>
           <AllowedOrigin>http://www.example.com</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 du développeur Amazon simple Storage Service".

2. Dans le Gestionnaire de locataires, sélectionnez **STORAGE (S3) seaux**.
3. Sélectionnez le nom du compartiment dans la liste.

   La page des détails du compartiment s'affiche.

4. Sélectionnez **accès au compartiment partage de ressources d'origine croisée (CORS)**.
5. Cochez la case **Activer CORS**.
6. Collez le code XML de configuration CORS dans la zone de texte, puis sélectionnez **Enregistrer les modifications**.



7. Pour modifier le paramètre CORS pour le compartiment, mettez à jour le code XML de configuration CORS dans la zone de texte ou sélectionnez **Clear** pour recommencer. Sélectionnez ensuite **Enregistrer les modifications**.
8. Pour désactiver CORS pour le compartiment, décochez la case **Activer CORS**, puis sélectionnez **Enregistrer les modifications**.

Supprimez le compartiment S3

Vous pouvez utiliser le Gestionnaire de locataires pour supprimer une ou plusieurs compartiments S3 vides.

Ce dont vous avez besoin

- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur web pris en charge.
- Vous devez appartenir à un groupe d'utilisateurs possédant l'autorisation gérer toutes les rubriques ou

accès racine. Ces autorisations remplacent les paramètres d'autorisations des stratégies de groupes ou de compartiments. Voir Autorisations de gestion des locataires.

- Les compartiments à supprimer sont vides.

Description de la tâche

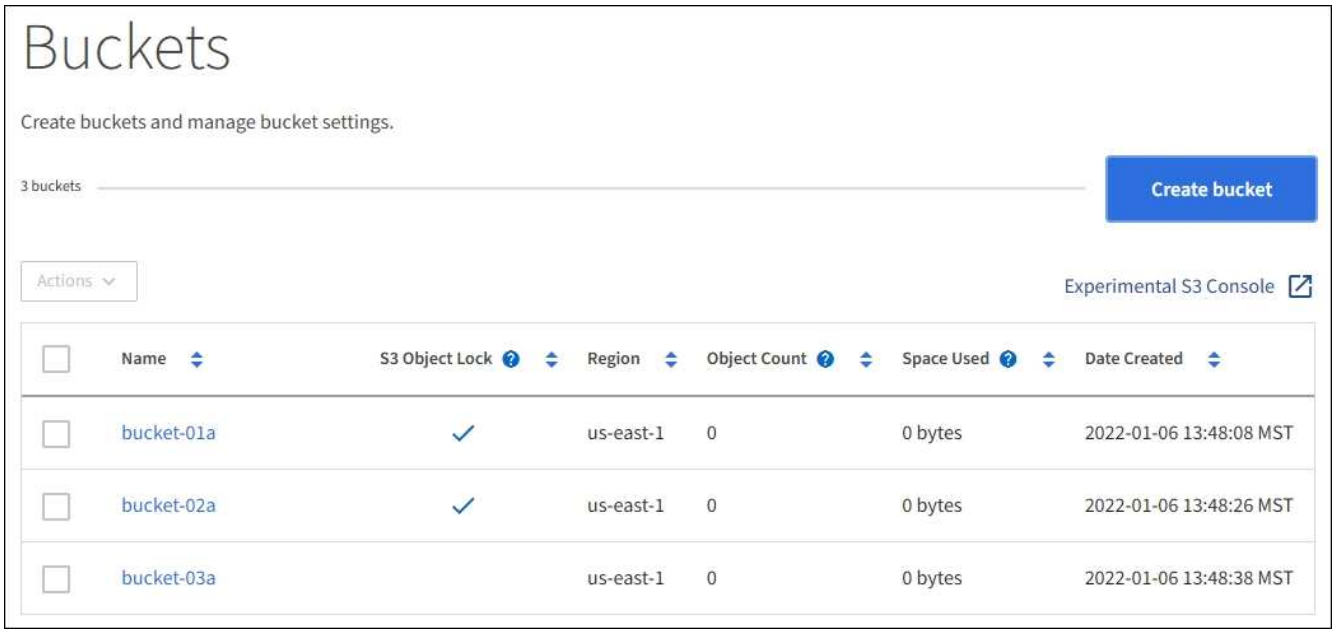
Ces instructions expliquent comment supprimer un compartiment S3 à l'aide du Gestionnaire des locataires. Vous pouvez également supprimer des compartiments S3 à l'aide du API de gestion des locataires ou le L'API REST S3.

Si ce compartiment contient des objets ou des versions d'objet non actuelles, vous ne pouvez pas le supprimer. Pour plus d'informations sur la suppression des objets avec version S3, consultez le instructions de gestion des objets avec gestion du cycle de vie des informations.

Étapes

1. Sélectionnez **STOCKAGE (S3) seaux**.

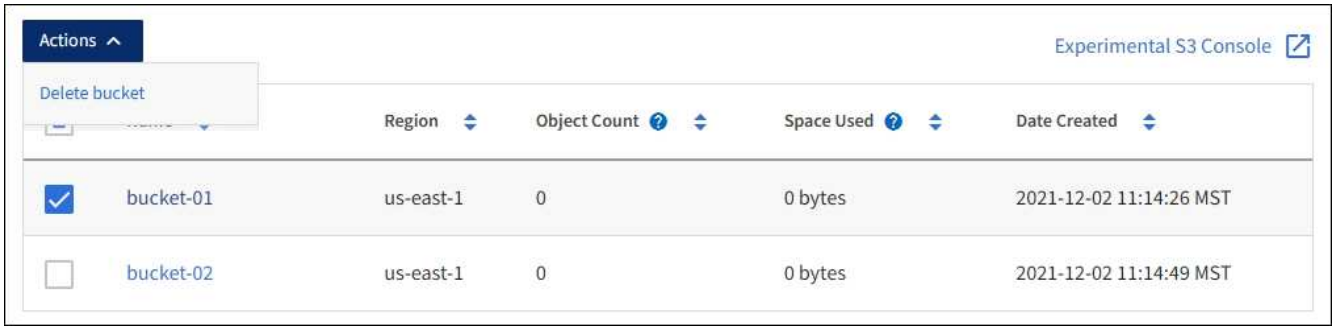
   La page compartiments s'affiche et affiche tous les compartiments S3 existants.



2. Cochez la case du compartiment vide que vous souhaitez supprimer. Vous pouvez sélectionner plusieurs compartiments à la fois.

   Le menu actions est activé.

3. Dans le menu actions, sélectionnez **Supprimer le compartiment** (ou **Supprimer les compartiments** si vous en avez choisi plusieurs).



4. Lorsque la boîte de dialogue de confirmation s'affiche, sélectionnez **Oui** pour supprimer tous les compartiments que vous avez choisis.

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

   Si un compartiment n'est pas vide, un message d'erreur s'affiche. Vous devez supprimer tous les objets avant de pouvoir supprimer un compartiment.

Utilisation de la console Experimental S3

Vous pouvez utiliser la console S3 pour afficher les objets d'un compartiment S3.

Vous pouvez également utiliser la console S3 pour :

- Ajouter et supprimer des objets, des versions d'objet et des dossiers
- Renommez les objets
- Déplacer et copier des objets entre des compartiments et des dossiers
- Gérer les balises d'objet
- Afficher les métadonnées d'objet
- Télécharger des objets

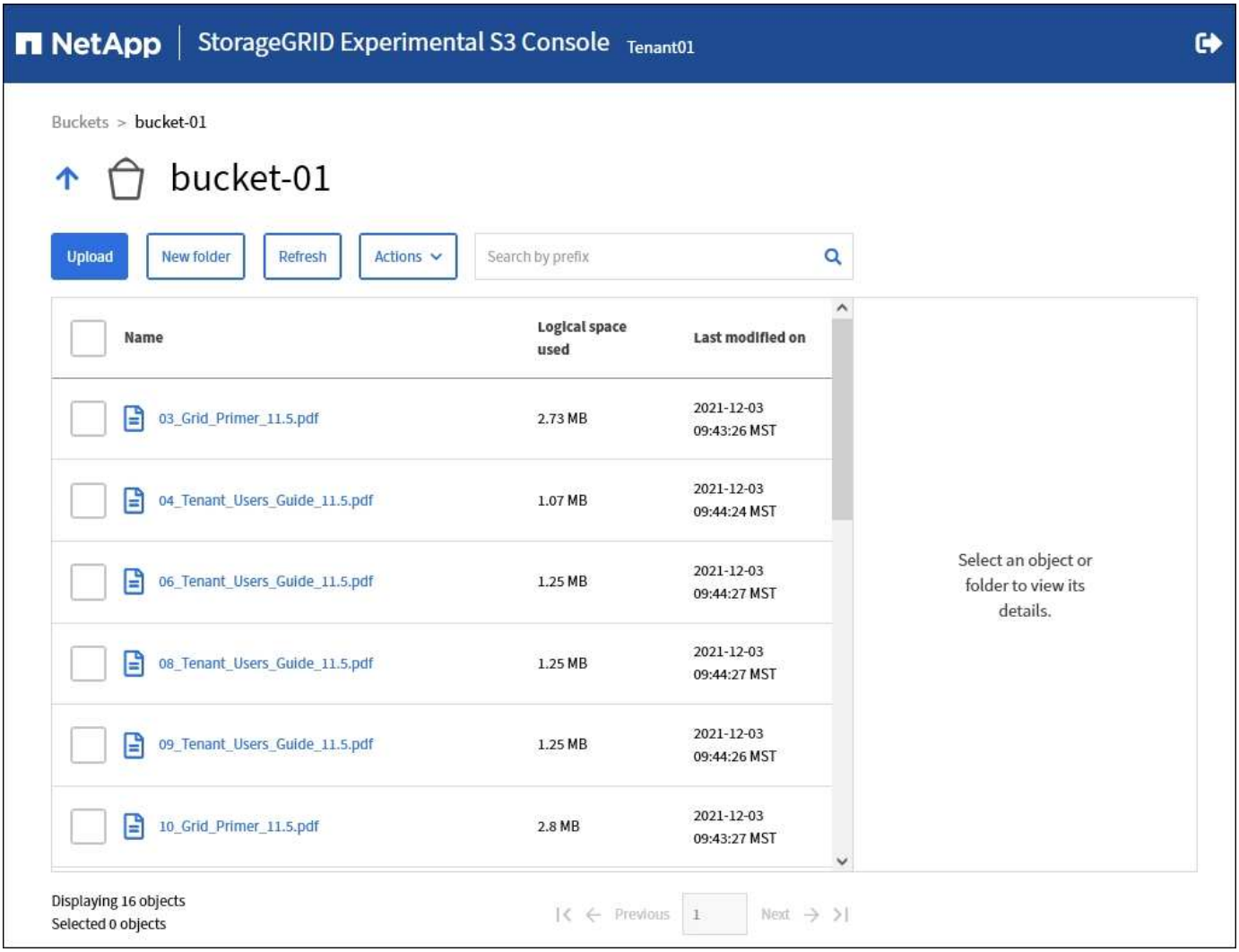
> La console S3 n'a pas été complètement testée et est marquée comme « expérimentale ». Il n'est pas destiné à la gestion en bloc des objets ou à une utilisation dans un environnement de production. Les locataires ne doivent utiliser la console S3 que lors de l'exécution de fonctions sur un petit nombre d'objets, par exemple lors du chargement d'objets pour simuler une nouvelle règle ILM, pour résoudre les problèmes d'ingestion ou via des grilles de validation technique ou non-production.

Ce dont vous avez besoin

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un navigateur web pris en charge.
- Vous disposez de l'autorisation gérer vos propres informations d'identification S3.
- Vous avez créé un compartiment.
- Vous connaissez l'ID de clé d'accès de l'utilisateur et la clé d'accès secrète. Si vous le souhaitez, vous avez un `.csv` fichier contenant ces informations. Voir la instructions pour la création de clés d'accès.

Étapes

1. Sélectionnez **godets**.
2. Sélectionnez Experimental S3 Console . Vous pouvez également accéder à ce lien à partir de la page des détails du compartiment.
3. Sur la page de connexion de la console Experimental S3, collez l'ID de clé d'accès et la clé secrète dans les champs. Sinon, sélectionnez **Télécharger les touches d'accès** et sélectionnez votre `.csv` fichier.
4. Sélectionnez **connexion**.
5. Gérez les objets selon vos besoins.


NetApp | StorageGRID Experimental S3 Console Tenant01
Buckets > bucket-01
bucket-01
Upload
New folder
Refresh
Actions
Search by prefix
Name
Logical space used
Last modified on
03_Grid_Primer_11.5.pdf
2.73 MB
2021-12-03 09:43:26 MST
04_Tenant_Users_Guide_11.5.pdf
1.07 MB
2021-12-03 09:44:24 MST
06_Tenant_Users_Guide_11.5.pdf
1.25 MB
2021-12-03 09:44:27 MST
08_Tenant_Users_Guide_11.5.pdf
1.25 MB
2021-12-03 09:44:27 MST
09_Tenant_Users_Guide_11.5.pdf
1.25 MB
2021-12-03 09:44:26 MST
10_Grid_Primer_11.5.pdf
2.8 MB
2021-12-03 09:43:27 MST
Select an object or folder to view its details.
Displaying 16 objects
Selected 0 objects
Previous
1
Next

Informations sur le copyright

Informations sur les marques commerciales