Utiliser StorageGRID

StorageGRID 11.9

NetApp
November 08, 2024

Sommaire

Utilisez les locataires et clients StorageGRID

Utilisez un compte de locataire

Utilisez un compte de locataire

Un compte de locataire vous permet d'utiliser l'API REST S3 (simple Storage Service) ou l'API REST Swift pour stocker et récupérer des objets dans un système StorageGRID.

Qu'est-ce qu'un compte de locataire ?

Chaque compte de locataire possède ses propres groupes, utilisateurs, compartiments S3, conteneurs Swift et objets fédérés.

Les comptes de tenant peuvent être utilisés pour isoler les objets stockés par des entités différentes. Par exemple, vous pouvez utiliser plusieurs comptes locataires pour l'une de ces utilisations :

- **Utilisation en entreprise :** si le système StorageGRID est utilisé au sein d'une entreprise, le stockage objet de la grille peut être séparé par les différents services de l'organisation. Par exemple, il peut y avoir des comptes de tenant pour le service Marketing, le service Customer support, le service des ressources humaines, etc.

> Si vous utilisez le protocole client S3, vous pouvez également utiliser des compartiments S3 et des règles de compartiment pour isoler les objets entre les différents départements d'une entreprise. Vous n'avez pas besoin de créer des comptes de locataire distincts. Voir les instructions d'implémentation "Compartiments S3 et règles de compartiments" pour plus d'informations.

- **Cas d'utilisation du fournisseur de services :** si le système StorageGRID est utilisé par un fournisseur de services, le stockage objet de la grille peut être séparé par les différentes entités qui louent le stockage. Il peut s'agir, par exemple, de comptes de locataires pour la société A, la société B, la société C, etc.

Comment créer un compte de locataire

Les comptes de tenant sont créés par un "Administrateur du grid StorageGRID utilisant le gestionnaire de grille". Lors de la création d'un compte de locataire, l'administrateur de la grille spécifie ce qui suit :

- Informations de base comprenant le nom du locataire, le type de client (S3) et le quota de stockage facultatif.
- Autorisations pour le compte de locataire, par exemple si le compte de locataire peut utiliser les services de la plateforme S3, configurer son propre référentiel d'identité, utiliser S3 Select ou utiliser une connexion de fédération grid.
- Accès racine initial pour le locataire, selon que le système StorageGRID utilise des groupes et utilisateurs locaux, la fédération des identités ou l'authentification unique (SSO).

En outre, les administrateurs du grid peuvent activer le paramètre de verrouillage objet S3 pour le système StorageGRID si les comptes de locataires S3 doivent être conformes aux exigences réglementaires. Lorsque le verrouillage des objets S3 est activé, tous les comptes de locataires S3 peuvent créer et gérer des compartiments conformes.

Configurez les locataires S3

Après un "Le compte de locataire S3 est créé", vous pouvez accéder au gestionnaire de locataires pour effectuer des tâches telles que :

- Configurer la fédération des identités (sauf si le référentiel d'identité est partagé avec la grille)
- Gestion des groupes et des utilisateurs
- Utilisez la fédération grid pour le clone de compte et la réplication inter-grid
- Gestion des clés d'accès S3
- Création et gestion de compartiments S3
- Utilisez les services de plateforme S3
- Utiliser S3 Select
- Contrôle de l'utilisation du stockage

Bien que vous puissiez créer et gérer des compartiments S3 avec le gestionnaire des locataires, vous devez utiliser un "Client S3" ou "Console S3" pour ingérer et gérer les objets.

Comment se connecter et se déconnecter

Connectez-vous au Gestionnaire de locataires

Vous accédez au gestionnaire de locataires en entrant l'URL du locataire dans la barre d'adresse d'un "navigateur web pris en charge".

Avant de commencer

- Vous disposez de vos identifiants de connexion.
- Vous disposez d'une URL permettant d'accéder au gestionnaire de locataires, fournie par votre administrateur de grille. L'URL se présente comme l'un de ces exemples :

  ```
  https://FQDN_or_Admin_Node_IP/

  https://FQDN_or_Admin_Node_IP:port/

  https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id

  https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id
  ```

  L'URL inclut toujours un nom de domaine complet (FQDN), l'adresse IP d'un nœud d'administration ou l'adresse IP virtuelle d'un groupe haute disponibilité de nœuds d'administration. Il peut également inclure un numéro de port, l'ID de compte de locataire à 20 chiffres, ou les deux.

- Si l'URL n'inclut pas l'ID de compte à 20 chiffres du locataire, vous disposez de cet ID de compte.
- Vous utilisez un "navigateur web pris en charge".
- Les cookies sont activés dans votre navigateur Web.
- Vous appartenez à un groupe d'utilisateurs qui a "autorisations d'accès spécifiques".

Étapes

1. Lancez un "navigateur web pris en charge".

2. Dans la barre d’adresse du navigateur, entrez l’URL d’accès au Gestionnaire de locataires.
3. Si vous êtes invité à recevoir une alerte de sécurité, installez le certificat à l’aide de l’assistant d’installation du navigateur.
4. Connectez-vous au Gestionnaire de locataires.

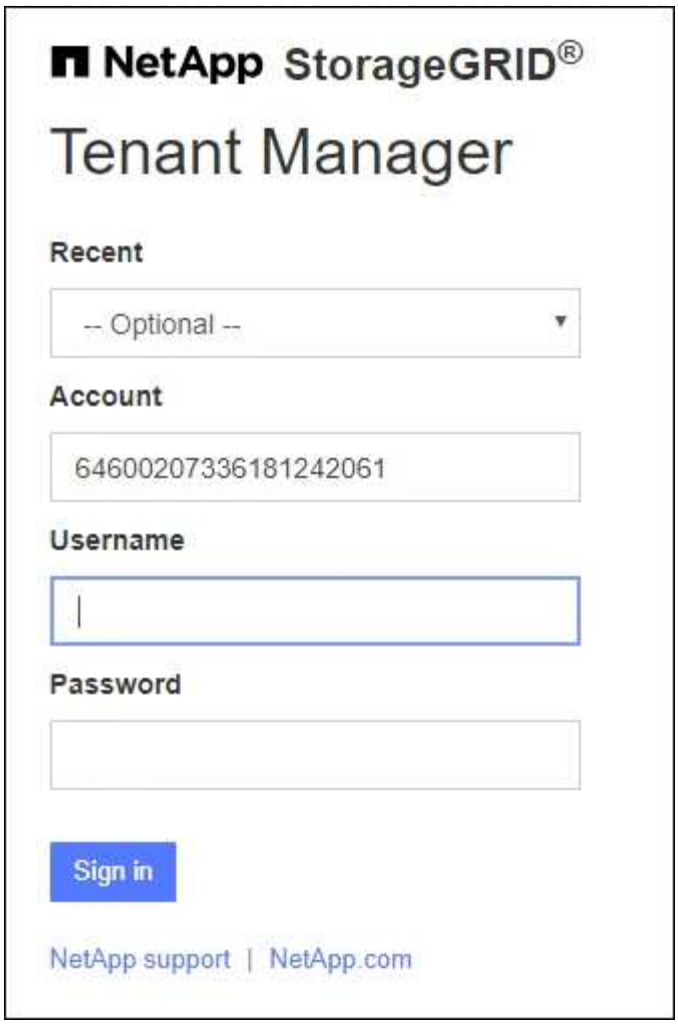
   L’écran d’ouverture de session qui s’affiche dépend de l’URL que vous avez saisie et de la configuration de l’authentification unique (SSO) pour StorageGRID.

Pas d'utilisation de SSO

Si StorageGRID n'utilise pas SSO, l'un des écrans suivants s'affiche :

- Page de connexion de Grid Manager. Sélectionnez le lien **tenant sign-in**.

- Page de connexion du Gestionnaire de locataires. Le champ **compte** est peut-être déjà renseigné, comme indiqué ci-dessous.



i. Si l'ID de compte à 20 chiffres du locataire ne s'affiche pas, sélectionnez le nom du compte du locataire s'il apparaît dans la liste des comptes récents ou saisissez l'ID du compte.

ii. Saisissez votre nom d'utilisateur et votre mot de passe.

iii. Sélectionnez **connexion**.

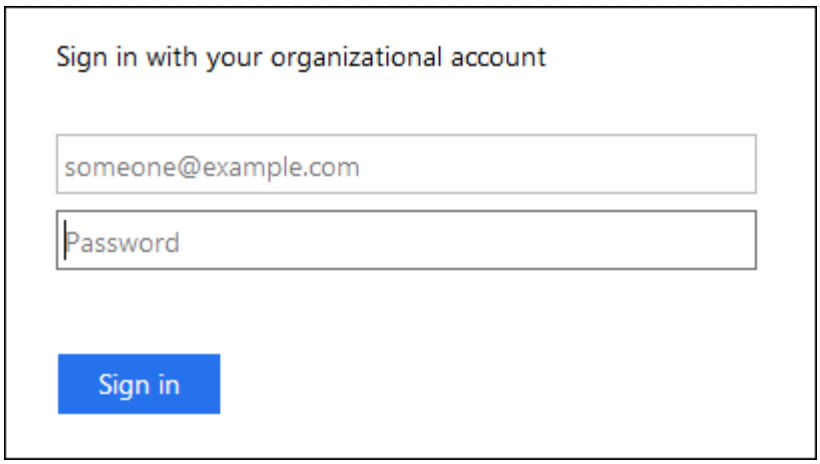
Le tableau de bord du gestionnaire de locataires s'affiche.

iv. Si vous avez reçu un mot de passe initial de la part d'une autre personne, sélectionnez ***username*** > **change password** pour sécuriser votre compte.

Utilisation de SSO

Si StorageGRID utilise SSO, l'un des écrans suivants s'affiche :

◦ La page SSO de votre organisation. Par exemple :



Entrez vos informations d'identification SSO standard et sélectionnez **se connecter**.

- Page de connexion SSO du Gestionnaire de locataires.

i. Si l'ID de compte à 20 chiffres du locataire ne s'affiche pas, sélectionnez le nom du compte du locataire s'il apparaît dans la liste des comptes récents ou saisissez l'ID du compte.

ii. Sélectionnez **connexion**.

iii. Connectez-vous à l'aide de vos identifiants SSO standard sur la page de connexion SSO de votre entreprise.

Le tableau de bord du gestionnaire de locataires s'affiche.

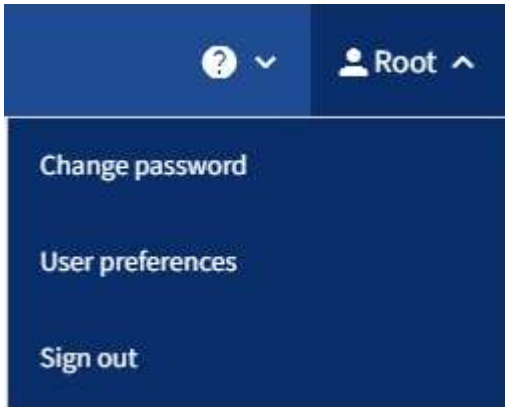
Déconnectez-vous du Gestionnaire de locataires

Lorsque vous avez terminé de travailler avec le Gestionnaire de locataires, vous devez

vous déconnecter pour vous assurer que les utilisateurs non autorisés ne peuvent pas accéder au système StorageGRID. La fermeture de votre navigateur risque de ne pas vous déconnecter du système, en fonction des paramètres des cookies du navigateur.

Étapes

1. Localisez la liste déroulante Nom d'utilisateur dans le coin supérieur droit de l'interface utilisateur.



2. Sélectionnez le nom d'utilisateur, puis sélectionnez **Déconnexion**.

   - Si SSO n'est pas utilisé :

     Vous êtes déconnecté du nœud d'administration. La page de connexion au Gestionnaire de locataires s'affiche.

     Si vous vous êtes connecté à plusieurs nœuds d'administration, vous devez vous déconnecter de chaque nœud.

   - Si SSO est activé :

     Vous êtes déconnecté de tous les nœuds d'administration auxquels vous accédiez. La page de connexion StorageGRID s'affiche. Le nom du compte de locataire que vous venez d'accéder est indiqué par défaut dans la liste déroulante **comptes récents** et le **ID de compte** du locataire s'affiche.

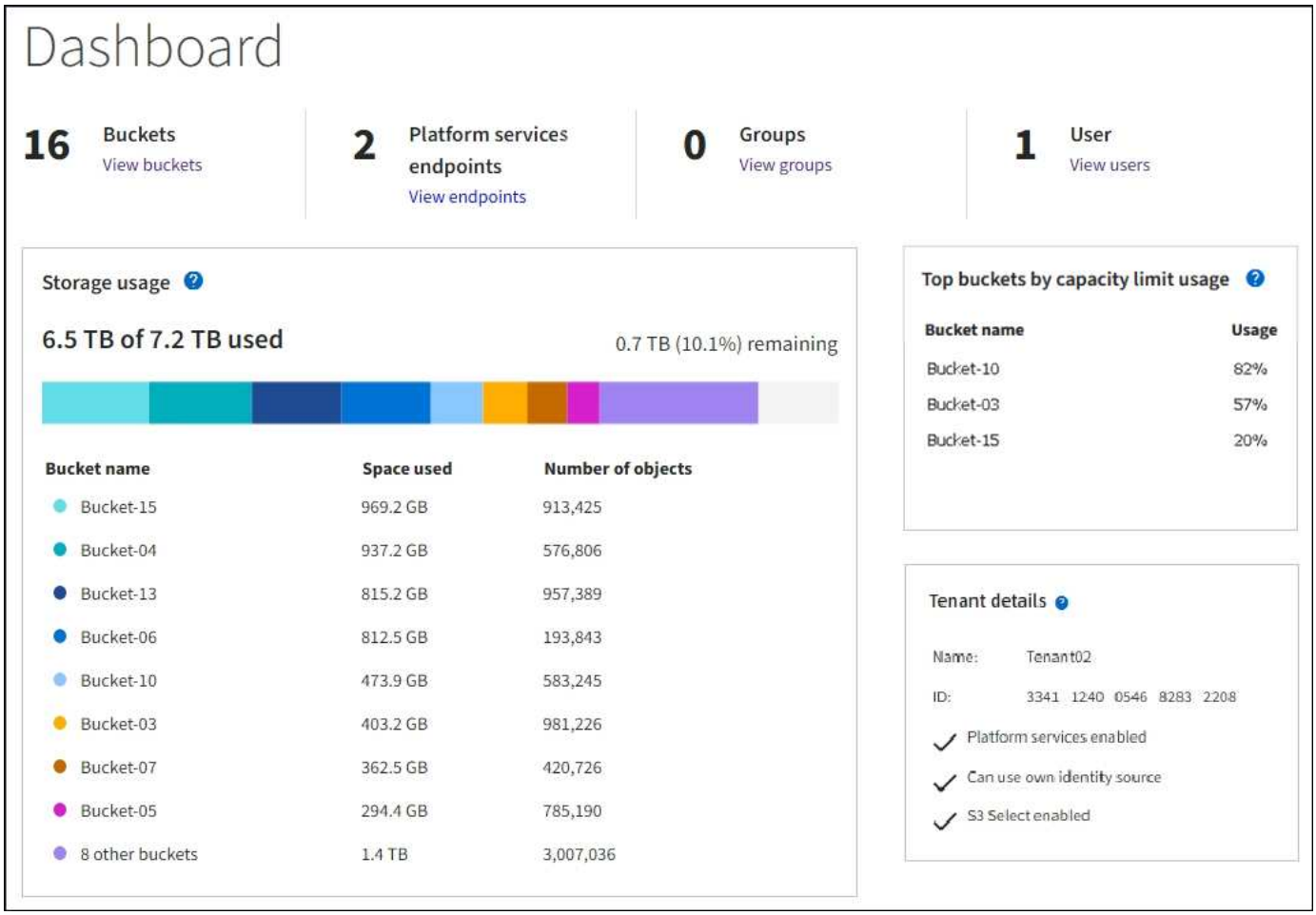
     Si SSO est activé et que vous êtes également connecté à Grid Manager, vous devez également vous déconnecter de Grid Manager pour vous déconnecter de SSO.

Présentation du tableau de bord du gestionnaire de locataires

Le tableau de bord du gestionnaire de locataires présente la configuration d'un compte de locataire et la quantité d'espace utilisée par les objets dans les compartiments du locataire (S3) ou les conteneurs (Swift). Si le locataire dispose d'un quota, le tableau de bord indique la part du quota utilisée et la quantité restante. En cas d'erreurs liées au compte de tenant, les erreurs s'affichent dans le tableau de bord.

Les valeurs espace utilisé sont des estimations. Ces estimations sont affectées par le moment de l'ingestion, la connectivité réseau et l'état des nœuds.

Une fois les objets téléchargés, le tableau de bord ressemble à l'exemple suivant :



Informations sur le compte locataire

Le haut du tableau de bord affiche le nombre de compartiments ou de conteneurs, de groupes et d'utilisateurs configurés. Il affiche également le nombre de noeuds finaux de services de plate-forme, s'ils ont été configurés. Sélectionnez les liens pour afficher les détails.

Selon votre configuration et les options dont vous disposez, le reste du tableau de bord affiche différentes combinaisons de consignes, d'utilisation du stockage, d'informations sur l'objet et de données sur le "autorisations de gestion des locataires"locataire.

Utilisation du stockage et des quotas

Le panneau utilisation du stockage contient les informations suivantes :

- Volume des données d'objet pour le locataire.

  Cette valeur indique la quantité totale de données d'objet chargées et ne représente pas l'espace utilisé pour stocker les copies de ces objets et leurs métadonnées.

- Si un quota est défini, la quantité totale d'espace disponible pour les données d'objet ainsi que la quantité et le pourcentage d'espace restant. Le quota limite la quantité de données d'objet pouvant être ingérées.

L'utilisation des quotas est basée sur des estimations internes et peut être dépassée dans certains cas. Par exemple, StorageGRID vérifie le quota lorsqu'un locataire commence à charger des objets et rejette les nouvelles ingère si le locataire a dépassé le quota. Cependant, StorageGRID ne prend pas en compte la taille du téléchargement actuel lors de la détermination du dépassement du quota. Si des objets sont supprimés, un locataire peut temporairement empêcher le téléchargement de nouveaux objets jusqu'au recalcul de l'utilisation du quota. Le calcul de l'utilisation des quotas peut prendre 10 minutes ou plus.

- Un graphique à barres qui représente les tailles relatives des grands godets ou conteneurs.

  Vous pouvez placer le curseur sur n'importe quel segment de graphique pour afficher l'espace total utilisé par ce compartiment ou ce conteneur.

- Pour correspondre au graphique à barres, une liste des plus grands seaux ou conteneurs, y compris la quantité totale de données d'objet et le nombre d'objets pour chaque godet ou conteneur.

Bucket name	Space used	Number of objects
Bucket-02	944.7 GB	7,575
Bucket-09	899.6 GB	589,677
Bucket-15	889.6 GB	623,542
Bucket-06	846.4 GB	648,619
Bucket-07	730.8 GB	808,655
Bucket-04	700.8 GB	420,493
Bucket-11	663.5 GB	993,729
Bucket-03	656.9 GB	379,329
9 other buckets	2.3 TB	5,171,588

  Si le locataire possède plus de neuf compartiments ou conteneurs, tous les autres compartiments ou conteneurs sont regroupés en une seule entrée au bas de la liste.

Pour modifier les unités des valeurs de stockage affichées dans le Gestionnaire de locataires, sélectionnez la liste déroulante utilisateur dans le coin supérieur droit du Gestionnaire de locataires, puis sélectionnez **Préférences utilisateur**.

Alertes d'utilisation des quotas

Si les alertes d'utilisation des quotas ont été activées dans Grid Manager, ces alertes apparaissent dans le gestionnaire de locataires lorsque le quota est faible ou dépassé, comme suit :

- Si 90 % ou plus du quota d'un locataire a été utilisé, l'alerte **usage du quota de locataire élevé** est déclenchée.

  Demandez à votre administrateur de grid d'augmenter le quota.

- Si vous dépassez votre quota, une notification vous indique que vous ne pouvez pas télécharger de nouveaux objets.

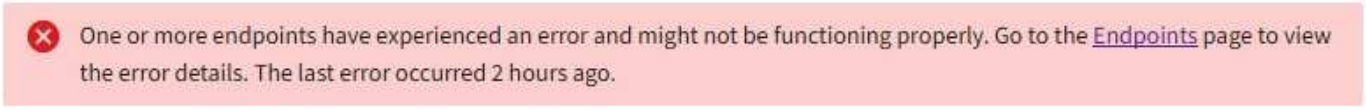
utilisation limitée de la capacité

Si vous avez défini une limite de capacité pour vos compartiments, le tableau de bord du gestionnaire de locataires affiche la liste des principaux compartiments par utilisation de la limite de capacité.

Si aucune limite n'est définie pour un godet, sa capacité est illimitée. Toutefois, si votre compte locataire dispose d'un quota de stockage total et que ce quota est atteint, vous ne pourrez pas ingérer davantage d'objets, quelle que soit la limite de capacité restante pour un compartiment.

Erreurs de point final

Si vous avez utilisé le gestionnaire de grille pour configurer un ou plusieurs points de terminaison pour les services de plateforme, le tableau de bord du gestionnaire de locataires affiche une alerte si des erreurs de point de terminaison se sont produites au cours des sept derniers jours.



Pour "erreurs de noeud final des services de plate-forme"afficher des détails sur , sélectionnez **noeuds finaux** pour afficher la page noeuds finaux.

API de gestion des locataires

Compréhension de l'API de gestion des locataires

Vous pouvez effectuer des tâches de gestion du système via l'API REST de gestion des locataires plutôt que dans l'interface utilisateur du gestionnaire de locataires. Par exemple, vous pouvez utiliser l'API pour automatiser les opérations ou créer plusieurs entités plus rapidement (par exemple, les utilisateurs).

L'API de gestion des locataires :

- Utilise la plate-forme API open source swagger. Swagger fournit une interface utilisateur intuitive qui permet aux développeurs et aux non-développeurs d'interagir avec l'API. L'interface utilisateur swagger fournit des détails complets et de la documentation pour chaque opération API.
- Utilise "gestion des versions pour prendre en charge les mises à niveau sans interruption".

Pour accéder à la documentation de swagger pour l'API de gestion des locataires :

1. Connectez-vous au Gestionnaire de locataires.
2. Dans le haut du Gestionnaire de locataires, sélectionnez l'icône d'aide et sélectionnez **documentation API**.

Opérations API

L'API de gestion des locataires organise les opérations API disponibles dans les sections suivantes :

- **Compte** : opérations sur le compte locataire actuel, y compris l'obtention d'informations sur l'utilisation du stockage.
- **Auth** : opérations pour effectuer l'authentification de session utilisateur.

  L'API de gestion des locataires prend en charge le schéma d'authentification par jeton Bearer. Pour une connexion locataire, vous devez fournir un nom d'utilisateur, un mot de passe et un ID de compte dans le corps JSON de la demande d'authentification (c'est-à-dire, `POST /api/v3/authorize`). Si l'utilisateur est authentifié, un jeton de sécurité est renvoyé. Ce token doit être fourni dans l'en-tête des requêtes API suivantes (« autorisation : jeton porteur »).

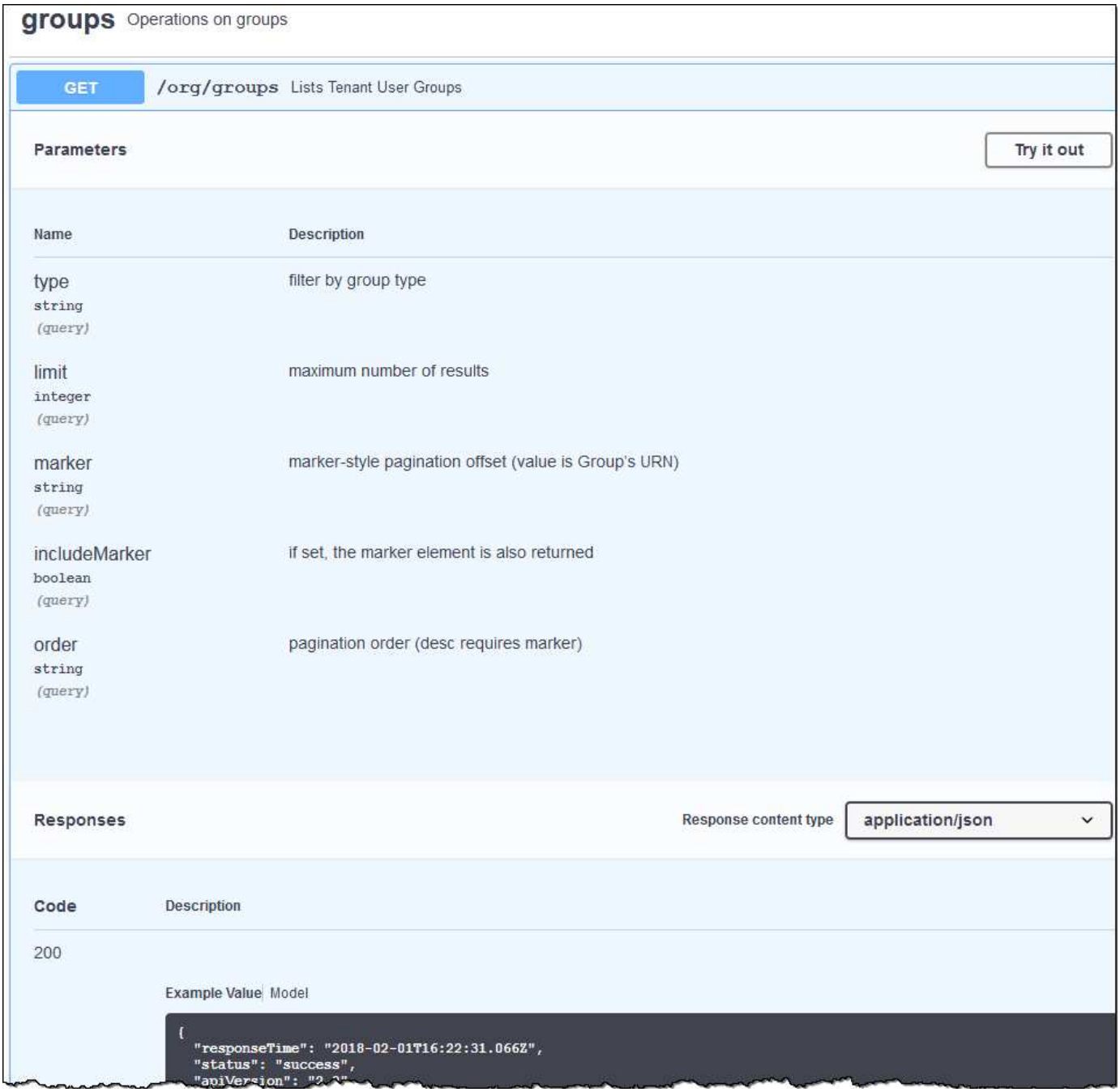
  Pour plus d'informations sur l'amélioration de la sécurité d'authentification, reportez-vous à la section "Protéger contre la contrefaçon de demandes intersites".

  > Si l'authentification unique (SSO) est activée pour le système StorageGRID, vous devez effectuer différentes étapes pour l'authentification. Voir la "Instructions d'utilisation de l'API de gestion de grille".

- **Config** : opérations liées à la version du produit et aux versions de l'API de gestion des locataires. Vous pouvez lister la version du produit ainsi que les versions principales de l'API prises en charge par cette version.
- **Conteneurs** : opérations sur les compartiments S3 ou les conteneurs Swift.
- **Désactivé-features** : opérations permettant d'afficher les fonctions qui auraient pu être désactivées.
- **Noeuds finaux** : opérations pour gérer un noeud final. Les terminaux permettent à un compartiment S3 d'utiliser un service externe pour la réplication StorageGRID CloudMirror, les notifications ou l'intégration de la recherche.
- **Grid-federation-connections** : opérations sur les connexions de fédération de grille et la réplication de grille transversale.
- **Groupes** : opérations de gestion des groupes de locataires locaux et de récupération des groupes de locataires fédérés à partir d'un référentiel d'identité externe.
- **Identity-source** : opérations permettant de configurer un référentiel d'identité externe et de synchroniser manuellement les informations relatives au groupe fédéré et à l'utilisateur.
- **ilm** : opérations sur les paramètres de gestion du cycle de vie de l'information (ILM).
- **Régions** : opérations permettant de déterminer quelles régions ont été configurées pour le système StorageGRID.
- **s3** : opérations de gestion des clés d'accès S3 pour les utilisateurs locataires.
- **s3-object-lock** : opérations sur les paramètres globaux de verrouillage d'objet S3, utilisées pour prendre en charge la conformité réglementaire.
- **Utilisateurs** : opérations pour afficher et gérer les utilisateurs locataires.

Détails de l'opération

Lorsque vous développez chaque opération d'API, vous pouvez voir son action HTTP, son URL de point final, une liste de tous les paramètres obligatoires ou facultatifs, un exemple du corps de la demande (si nécessaire) et les réponses possibles.



Émettre des requêtes API

> Toutes les opérations d'API que vous effectuez à l'aide de la page Web Documentation de l'API sont des opérations en direct. Veillez à ne pas créer, mettre à jour ou supprimer des données de configuration ou d'autres données par erreur.

Étapes

1. Sélectionnez l'action HTTP pour afficher les détails de la demande.
2. Déterminez si la demande nécessite des paramètres supplémentaires, tels qu'un ID de groupe ou d'utilisateur. Ensuite, obtenir ces valeurs. Vous devrez peut-être d'abord lancer une autre demande d'API pour obtenir les informations dont vous avez besoin.
3. Déterminez si vous devez modifier l'exemple de corps de la demande. Si c'est le cas, vous pouvez sélectionner **modèle** pour connaître les exigences de chaque champ.

4. Sélectionnez **essayez-le**.
5. Fournir tous les paramètres requis ou modifier le corps de la demande selon les besoins.
6. Sélectionnez **Exécuter**.
7. Vérifiez le code de réponse pour déterminer si la demande a réussi.

Gestion des versions de l'API de gestion des locataires

L'API de gestion des locataires utilise la gestion des versions pour prendre en charge les mises à niveau sans interruption.

Par exemple, cette URL de demande spécifie la version 4 de l'API.

`https://hostname_or_ip_address/api/v4/authorize`

La version majeure de l'API est incrémentée lorsque des modifications sont effectuées qui ne sont *pas compatibles* avec des versions plus anciennes. La version mineure de l'API est incrémentée lorsque des modifications qui sont *compatibles* avec des versions plus anciennes sont effectuées. Les modifications compatibles incluent l'ajout de nouveaux noeuds finaux ou de nouvelles propriétés.

L'exemple suivant illustre comment la version de l'API est incrémentée en fonction du type de modifications apportées.

Type de modification de l'API	Ancienne version	Nouvelle version
Compatible avec les versions plus anciennes	2,1	2,2
Non compatible avec les versions plus anciennes	2,1	3,0

Lorsque vous installez le logiciel StorageGRID pour la première fois, seule la version la plus récente de l'API est activée. Cependant, lorsque vous effectuez une mise à niveau vers une nouvelle version de StorageGRID, vous continuez à accéder à l'ancienne version de l'API pour au moins une version de StorageGRID.

> Vous pouvez configurer les versions prises en charge. Pour plus d'informations, reportez-vous à la section **config** de la documentation de l'API swagger"API de gestion du grid". Vous devez désactiver la prise en charge de l'ancienne version après avoir mis à jour tous les clients API pour utiliser la nouvelle version.

Les requêtes obsolètes sont marquées comme obsolètes de l'une des manières suivantes :

- L'en-tête de réponse est « obsolète : vrai »
- Le corps de la réponse JSON inclut « obsolète » : vrai
- Un avertissement obsolète est ajouté à nms.log. Par exemple :

```
Received call to deprecated v2 API at POST "/api/v2/authorize"
```

Identification des versions d'API prises en charge dans la version actuelle

Utilisez la `GET /versions` requête API pour renvoyer une liste des versions majeures de l'API prises en charge. Cette demande se trouve dans la section **config** de la documentation de l'API swagger.

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2023-06-27T22:13:50.750Z",
  "status": "success",
  "apiVersion": "4.0",
  "data": [
    2,
    3,
    4
  ]
}
```

Spécifiez une version API pour une demande

Vous pouvez spécifier la version de l'API à l'aide d'un paramètre de chemin d'accès (`/api/v4`) ou d'un en-tête (`Api-Version: 4`. Si vous indiquez les deux valeurs, la valeur de l'en-tête remplace la valeur du chemin d'accès.

```
curl https://[IP-Address]/api/v4/grid/accounts

curl -H "Api-Version: 4" https://[IP-Address]/api/grid/accounts
```

Protection contre la contrefaçon de demandes intersites (CSRF)

Vous pouvez vous protéger contre les attaques de contrefaçon de requêtes intersites (CSRF) contre StorageGRID en utilisant des jetons CSRF pour améliorer l'authentification qui utilise des cookies. Grid Manager et tenant Manager activent automatiquement cette fonction de sécurité ; les autres clients API peuvent choisir de l'activer lorsqu'ils se connectent.

Un attaquant pouvant déclencher une requête vers un autre site (par exemple avec UN POST de formulaire HTTP) peut créer certaines requêtes à l'aide des cookies de l'utilisateur connecté.

StorageGRID contribue à la protection contre les attaques CSRF en utilisant des jetons CSRF. Lorsque cette option est activée, le contenu d'un cookie spécifique doit correspondre au contenu d'un en-tête spécifique ou d'un paramètre DE CORPS POST spécifique.

Pour activer la fonction, définissez le `csrfToken` paramètre sur `true` pendant l'authentification. La valeur par défaut est `false`.

```
curl -X POST --header "Content-Type: application/json" --header "Accept:
application/json" -d "{
  \"username\": \"MyUserName\",
  \"password\": \"MyPassword\",
  \"cookie\": true,
  \"csrfToken\": true
}" "https://example.com/api/v3/authorize"
```

Lorsque la valeur est true, un `GridCsrfToken` cookie est défini avec une valeur aléatoire pour les connexions au gestionnaire de tenant et le `AccountCsrfToken` cookie est défini avec une valeur aléatoire pour les connexions au gestionnaire de tenant.

Si le cookie est présent, toutes les demandes pouvant modifier l'état du système (POST, PUT, PATCH, DELETE) doivent inclure l'une des options suivantes :

- L' `X-Csrf-Token`en-tête, avec la valeur de l'en-tête définie sur la valeur du cookie de jeton CSRF.
- Pour les noeuds finaux qui acceptent un corps codé en forme : un `csrfToken` paramètre de corps de requête codé en forme.

Pour configurer la protection CSRF, utilisez le ou le "API de gestion du grid""API de gestion des locataires".

> Les demandes qui ont un ensemble de cookies de token CSRF appliquent également l'en-tête « Content-Type: Application/json » pour toute demande qui attend un corps de requête JSON comme protection supplémentaire contre les attaques CSRF.

Utiliser les connexions de fédération de grille

Cloner des groupes de locataires et des utilisateurs

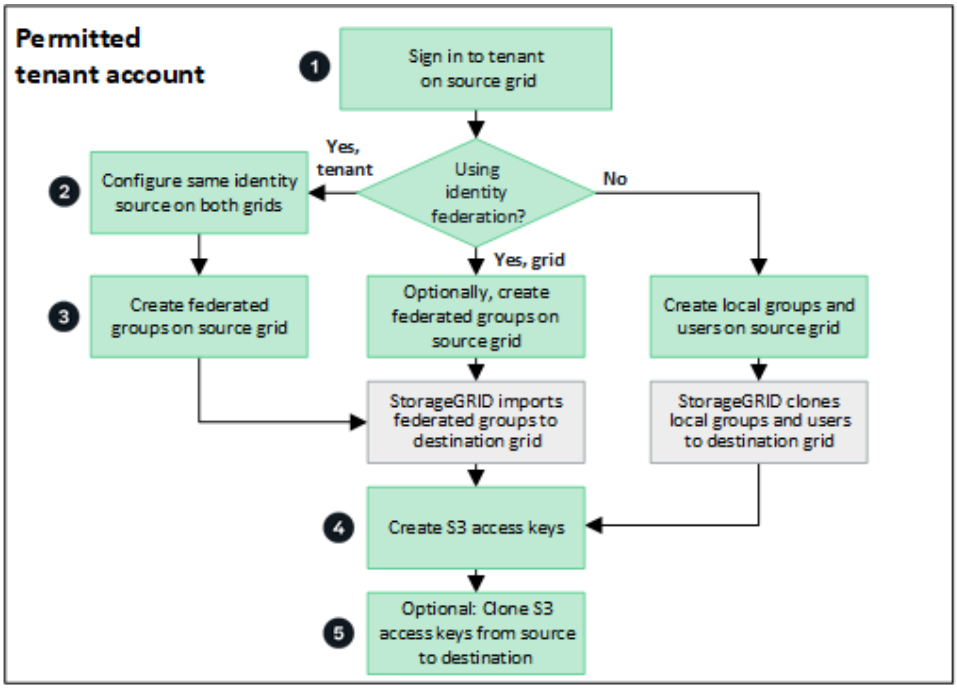
Si un locataire a été créé ou modifié pour utiliser une connexion de fédération de grille, ce dernier est répliqué d'un système StorageGRID (le locataire source) vers un autre système StorageGRID (le locataire de réplica). Une fois le tenant répliqué, tous les groupes et utilisateurs ajoutés au tenant source sont clonés dans le tenant de réplica.

Le système StorageGRID dans lequel le tenant est créé à l'origine est *source GRID* du tenant. Le système StorageGRID dans lequel le locataire est répliqué est la *grille de destination* du locataire. Les deux comptes de tenant possèdent les mêmes ID de compte, nom, description, quota de stockage et autorisations attribuées, mais le locataire de destination ne dispose pas initialement d'un mot de passe utilisateur root. Pour plus de détails, voir "Qu'est-ce que le clone de compte" et "Gérer les locataires autorisés".

Le clonage des informations de compte de locataire est requis pour les "réplication entre plusieurs grilles"objets de compartiment. Le fait de disposer des mêmes groupes de locataires et utilisateurs sur les deux grilles vous permet d'accéder aux compartiments et objets correspondants sur l'une ou l'autre grille.

Workflow des locataires pour le clone de compte

Si votre compte de locataire dispose de l'autorisation **utiliser la connexion de fédération de grille**, consultez le diagramme de flux de travail pour voir les étapes à suivre pour cloner des groupes, des utilisateurs et des clés d'accès S3.



Voici les principales étapes du flux de travail :

1 Connectez-vous au locataire

Connectez-vous au compte de locataire sur la grille source (la grille dans laquelle le locataire a été initialement créé).

2 Vous pouvez également configurer la fédération des identités

Si votre compte de tenant dispose de l'autorisation **utiliser son propre référentiel d'identité** pour utiliser des groupes et des utilisateurs fédérés, configurez le même référentiel d'identité (avec les mêmes paramètres) pour les comptes de tenant source et de destination. Les groupes et utilisateurs fédérés ne peuvent pas être clonés à moins que les deux grilles n'utilisent le même référentiel d'identité. Pour obtenir des instructions, reportez-vous à la section "Utiliser la fédération des identités".

3 Créer des groupes et des utilisateurs

Lorsque vous créez des groupes et des utilisateurs, commencez toujours par la grille source du locataire. Lorsque vous ajoutez un nouveau groupe, StorageGRID le clone automatiquement dans la grille de destination.

- Si la fédération des identités est configurée pour l'ensemble du système StorageGRID ou pour votre compte de locataire, "créer de nouveaux groupes de locataires" en important des groupes fédérés à partir du référentiel d'identité.
- Si vous n'utilisez pas la fédération des identités, "créer de nouveaux groupes locaux"puis "créer des utilisateurs locaux".

4 Création de clés d'accès S3

Vous pouvez "créez vos propres clés d'accès" ou "créez les clés d'accès d'un autre utilisateur"sur la grille source ou la grille de destination pour accéder aux compartiments de cette grille.

5 **Vous pouvez également cloner les clés d'accès S3**

Si vous avez besoin d'accéder à des compartiments avec les mêmes clés d'accès sur les deux grilles, créez les clés d'accès sur la grille source, puis utilisez l'API du gestionnaire de locataires pour les cloner manuellement dans la grille de destination. Pour obtenir des instructions, reportez-vous à la section "Cloner les clés d'accès S3 à l'aide de l'API".

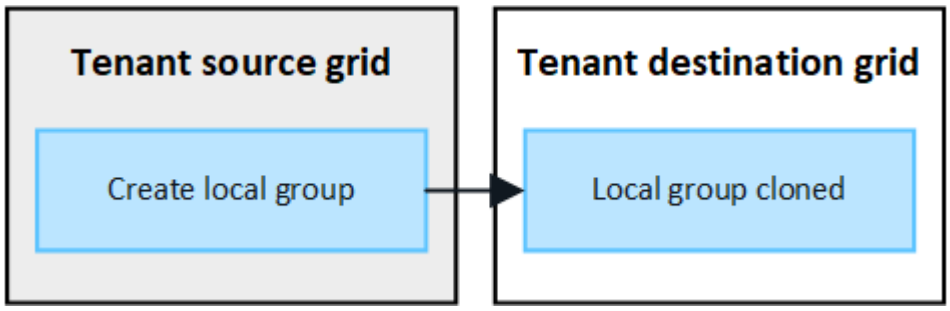
Comment les groupes, les utilisateurs et les clés d'accès S3 sont-ils clonés ?

Dans cette section, vous apprendrez comment les groupes, les utilisateurs et les clés d'accès S3 sont clonés entre la grille source des locataires et la grille de destination des locataires.

Les groupes locaux créés dans la grille source sont clonés

Une fois qu'un compte de locataire est créé et répliqué sur la grille de destination, StorageGRID clone automatiquement tous les groupes locaux que vous ajoutez à la grille source du locataire dans la grille de destination du locataire.

Le groupe d'origine et le clone disposent des mêmes mode d'accès, autorisations de groupe et règles de groupe S3. Pour obtenir des instructions, reportez-vous à la section "Créez des groupes pour les locataires S3".

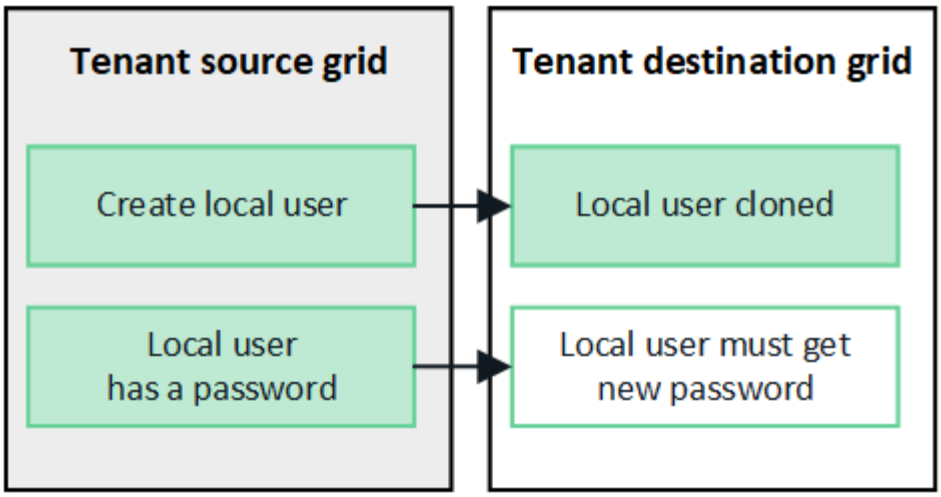


Tous les utilisateurs sélectionnés lors de la création d'un groupe local sur la grille source ne sont pas inclus lorsque le groupe est cloné dans la grille de destination. Pour cette raison, ne sélectionnez pas d'utilisateurs lorsque vous créez le groupe. Sélectionnez plutôt le groupe lorsque vous créez les utilisateurs.

Les utilisateurs locaux créés dans la grille source sont clonés

Lorsque vous créez un utilisateur local sur la grille source, StorageGRID le clone automatiquement dans la grille de destination. L'utilisateur d'origine et son clone ont tous les deux le même nom complet, le même nom d'utilisateur et le même paramètre **deny Access**. Les deux utilisateurs appartiennent également aux mêmes groupes. Pour obtenir des instructions, reportez-vous à la section "Gérez les utilisateurs locaux".

Pour des raisons de sécurité, les mots de passe des utilisateurs locaux ne sont pas clonés dans la grille de destination. Si un utilisateur local doit accéder au gestionnaire de locataires sur la grille de destination, l'utilisateur root du compte de locataire doit ajouter un mot de passe pour cet utilisateur sur la grille de destination. Pour obtenir des instructions, reportez-vous à la section "Gérez les utilisateurs locaux".

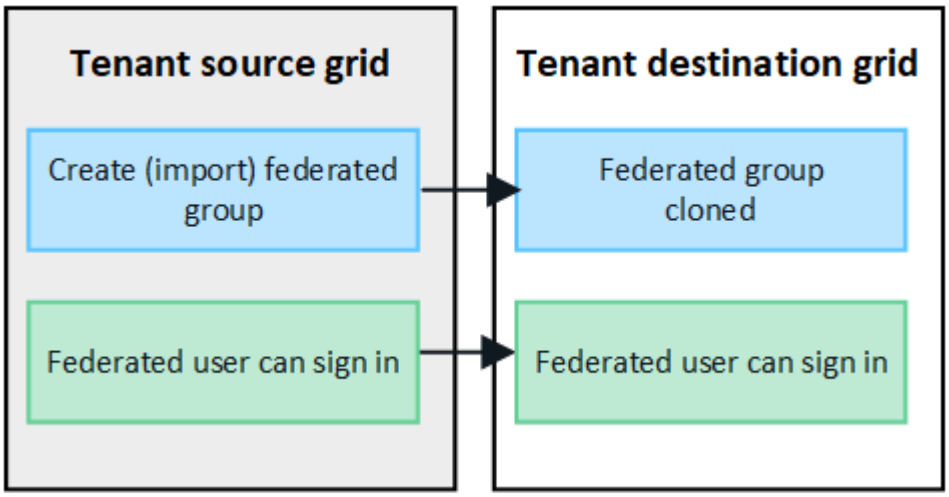


Les groupes fédérés créés dans la grille source sont clonés

En supposant que les conditions d'utilisation du clone de compte "authentification unique" "fédération des identités"soient remplies, les groupes fédérés que vous créez (importez) pour le locataire sur la grille source sont automatiquement clonés dans le locataire de la grille de destination.

Les deux groupes disposent des mêmes mode d'accès, autorisations de groupe et règles de groupe S3.

Une fois les groupes fédérés créés pour le locataire source et clonés dans le locataire de destination, les utilisateurs fédérés peuvent se connecter au locataire dans l'une ou l'autre des grilles.

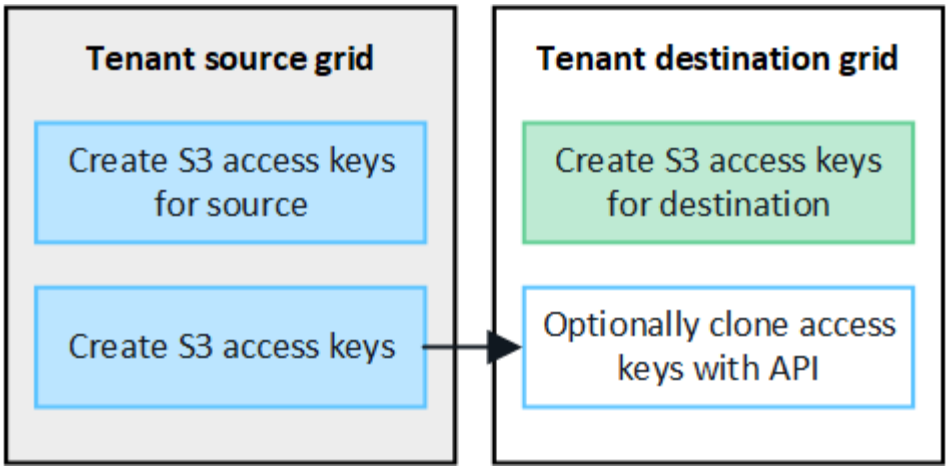


Les clés d'accès S3 peuvent être clonées manuellement

StorageGRID ne clone pas automatiquement les clés d'accès S3, car la sécurité est améliorée grâce à l'utilisation de clés différentes sur chaque grid.

Pour gérer les clés d'accès sur les deux grilles, vous pouvez effectuer l'une des opérations suivantes :

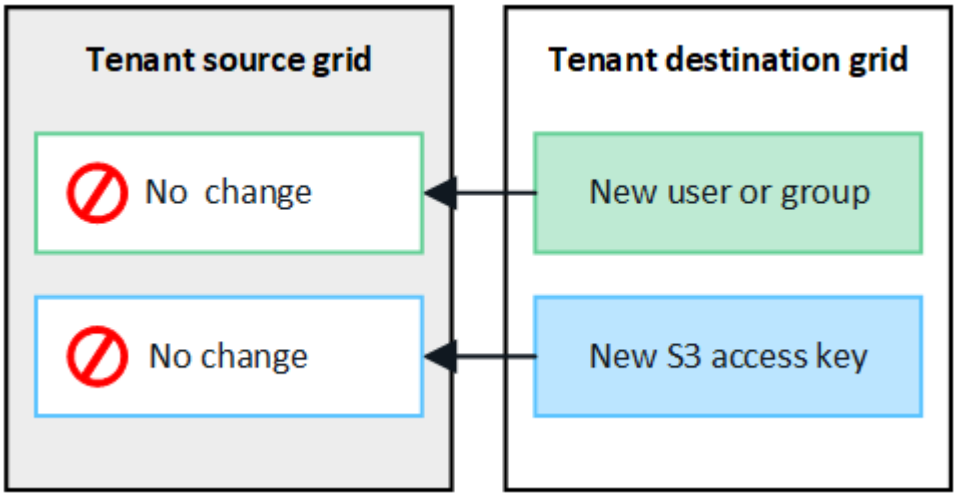
- Si vous n'avez pas besoin d'utiliser les mêmes touches pour chaque grille, vous pouvez "créez vos propres clés d'accès" ou "créez les clés d'accès d'un autre utilisateur" sur chaque grille.
- Si vous devez utiliser les mêmes clés sur les deux grilles, vous pouvez créer des clés sur la grille source, puis utiliser l'API du gestionnaire de locataires pour accéder manuellement "cloner les clés" à la grille de destination.



Lorsque vous clonez les clés d'accès S3 d'un utilisateur fédéré, ces deux clés sont clonées dans le locataire de destination.

Les groupes et utilisateurs ajoutés à la grille de destination ne sont pas clonés

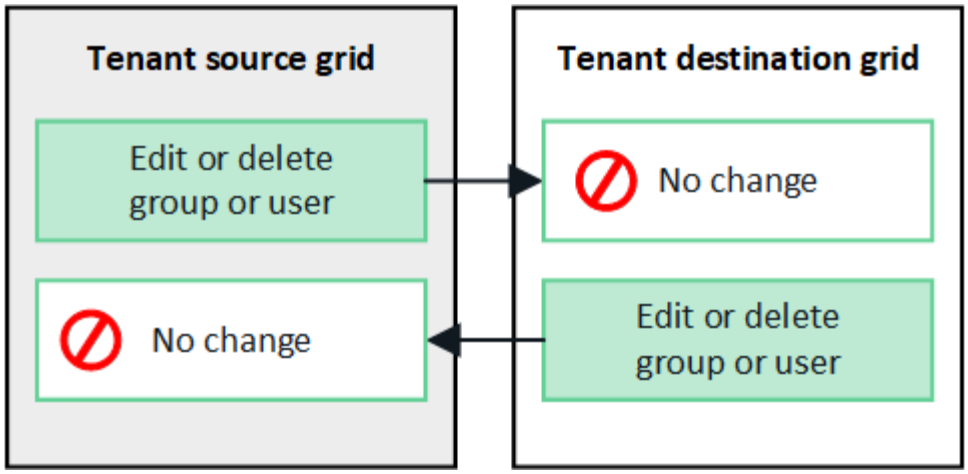
Le clonage s'effectue uniquement depuis la grille source du locataire vers la grille de destination du locataire. Si vous créez ou importez des groupes et des utilisateurs sur la grille de destination du locataire, StorageGRID ne les clonez pas dans la grille source du locataire.



Les groupes, utilisateurs et clés d'accès modifiés ou supprimés ne sont pas clonés

Le clonage a lieu uniquement lorsque vous créez de nouveaux groupes et utilisateurs.

Si vous modifiez ou supprimez des groupes, des utilisateurs ou des clés d'accès sur l'une ou l'autre grille, vos modifications ne seront pas clonées sur l'autre grille.



Cloner les clés d'accès S3 à l'aide de l'API

Si votre compte de locataire dispose de l'autorisation **utiliser la connexion de fédération grid**, vous pouvez utiliser l'API de gestion des locataires pour cloner manuellement les clés d'accès S3 du locataire de la grille source vers le locataire de la grille de destination.

Avant de commencer

- Le compte de tenant dispose de l'autorisation **utiliser la connexion de fédération de grille**.
- La connexion de fédération de grille a un **état de connexion** de **connecté**.
- Vous êtes connecté au gestionnaire de locataires sur la grille source du locataire à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Gérez vos propres informations d'identification S3 ou autorisations d'accès racine".
- Si vous clonez des clés d'accès pour un utilisateur local, l'utilisateur existe déjà sur les deux grilles.

> Lorsque vous clonez les clés d'accès S3 d'un utilisateur fédéré, ces deux clés sont ajoutées au locataire de destination.

Clonez vos propres clés d'accès

Vous pouvez cloner vos propres clés d'accès si vous devez accéder aux mêmes compartiments sur les deux grilles.

Étapes

1. À l'aide du gestionnaire de locataires sur la grille source "créez vos propres clés d'accès"et téléchargez le `.csv` fichier.
2. Dans le haut du Gestionnaire de locataires, sélectionnez l'icône d'aide et sélectionnez **documentation API**.
3. Dans la section **s3**, sélectionnez le noeud final suivant :

   ```
   POST /org/users/current-user/replicate-s3-access-key
   ```

4. Sélectionnez **essayez-le**.
5. Dans la zone de texte **body**, remplacez les entrées d'exemple pour **accesskey** et **secretAccessKey** par les valeurs du fichier **.csv** que vous avez téléchargé.

   Veillez à conserver les guillemets doubles autour de chaque chaîne.

6. Si la clé expire, remplacez l'exemple de **expire** par la date et l'heure d'expiration sous forme de chaîne au format de données ISO 8601 (par exemple, `2024-02-28T22:46:33-08:00`). Si la clé n'expire pas, entrez **null** comme valeur pour l'entrée **Expires** (ou supprimez la ligne **Expires** et la virgule précédente).
7. Sélectionnez **Exécuter**.
8. Vérifiez que le code de réponse du serveur est **204**, ce qui indique que la clé a été correctement clonée dans la grille de destination.

Cloner les clés d'accès d'un autre utilisateur

Vous pouvez cloner les clés d'accès d'un autre utilisateur s'il doit accéder aux mêmes compartiments sur les deux grilles.

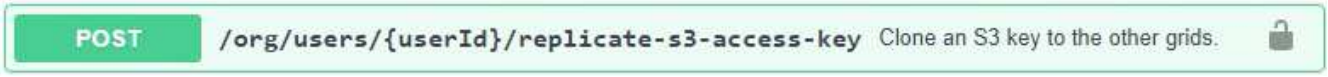
Étapes

1. À l'aide du gestionnaire de locataires sur la grille source "Créez les clés d'accès S3 de l'autre utilisateur"et téléchargez le `.csv` fichier.
2. Dans le haut du Gestionnaire de locataires, sélectionnez l'icône d'aide et sélectionnez **documentation API**.
3. Obtenez l'ID utilisateur. Vous aurez besoin de cette valeur pour cloner les clés d'accès des autres utilisateurs.
   a. Dans la section **Users**, sélectionnez le noeud final suivant :

      `GET /org/users`

   b. Sélectionnez **essayez-le**.
   c. Spécifiez les paramètres que vous souhaitez utiliser lors de la recherche d'utilisateurs.
   d. Sélectionnez **Exécuter**.
   e. Recherchez l'utilisateur dont vous souhaitez cloner les clés et copiez le numéro dans le champ **ID**.
4. Dans la section **s3**, sélectionnez le noeud final suivant :

   `POST /org/users/{userId}/replicate-s3-access-key`



5. Sélectionnez **essayez-le**.
6. Dans la zone de texte **userid**, collez l'ID utilisateur que vous avez copié.
7. Dans la zone de texte **body**, remplacez les entrées d'exemple pour **example Access key** et **secret Access key** par les valeurs du fichier **.csv** pour cet utilisateur.

   Veillez à conserver les guillemets doubles autour de la chaîne.

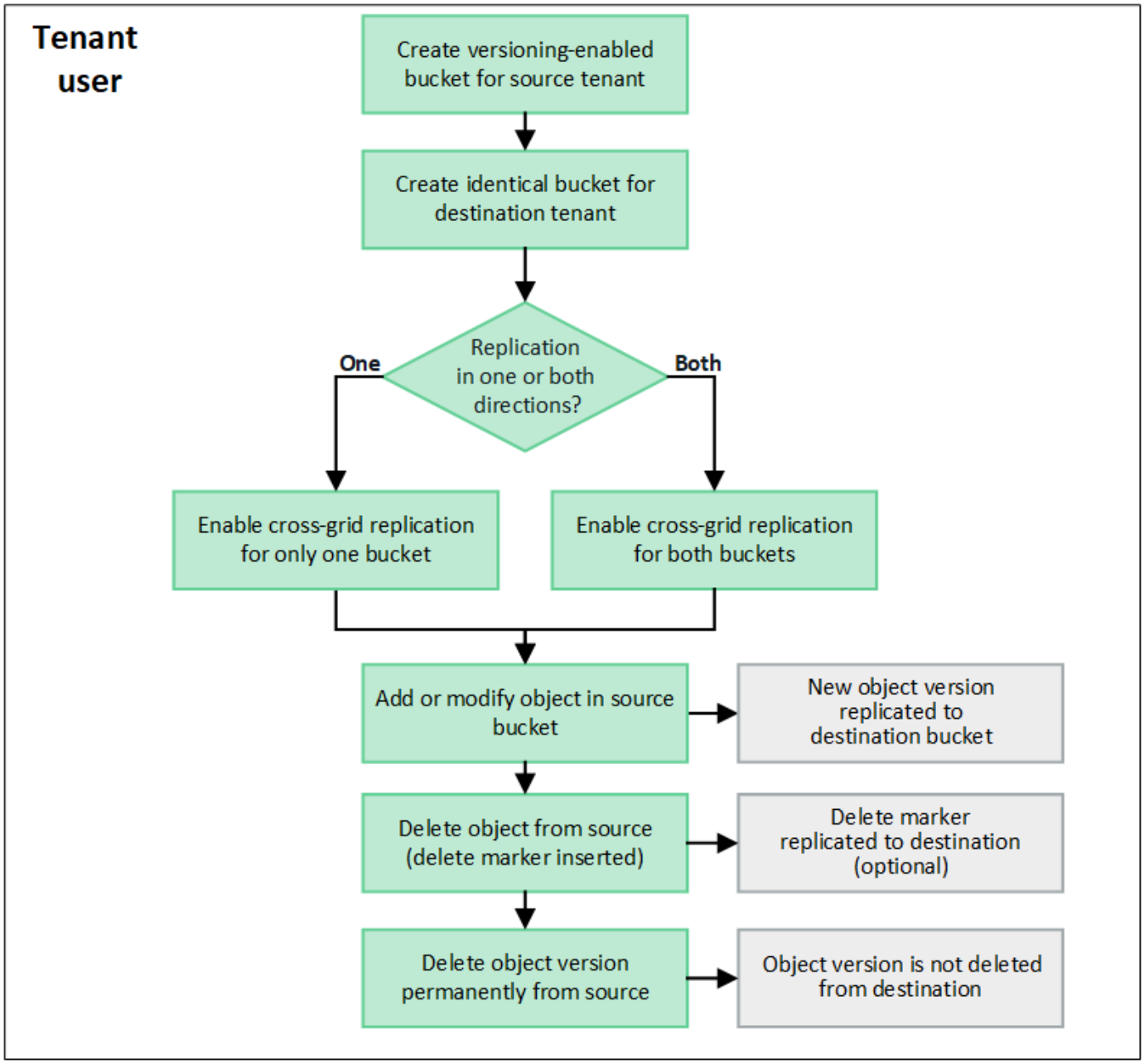
8. Si la clé expire, remplacez l'exemple de **expire** par la date et l'heure d'expiration sous forme de chaîne au format de données ISO 8601 (par exemple, `2023-02-28T22:46:33-08:00`). Si la clé n'expire pas, entrez **null** comme valeur pour l'entrée **Expires** (ou supprimez la ligne **Expires** et la virgule précédente).
9. Sélectionnez **Exécuter**.
10. Vérifiez que le code de réponse du serveur est **204**, ce qui indique que la clé a été correctement clonée dans la grille de destination.

Gérer la réplication entre les grilles

Si l'autorisation **utiliser la connexion de fédération de grille** a été attribuée à votre compte de locataire lors de sa création, vous pouvez utiliser la réplication multigrille pour répliquer automatiquement les objets entre les compartiments de la grille source du locataire et les compartiments de la grille de destination du locataire. La réplication inter-grille peut se produire dans une ou les deux directions.

Flux de production pour la réplication entre les grilles

Le diagramme de flux de travail récapitule les étapes que vous allez effectuer pour configurer la réplication inter-grille entre les compartiments sur deux grilles. Ces étapes sont décrites plus en détail ci-dessous.



Configurer la réplication entre les grilles

Avant de pouvoir utiliser la réplication multigrille, vous devez vous connecter aux comptes de locataires correspondants sur chaque grille et créer des compartiments identiques. Vous pouvez ensuite activer la réplication entre les grilles sur l'un ou l'autre des compartiments, ou sur les deux.

Avant de commencer

- Vous avez examiné les exigences relatives à la réplication intergrid. Voir "Qu'est-ce que la réplication cross-grid".
- Vous utilisez un "navigateur web pris en charge".
- Le compte de tenant possède l'autorisation **utiliser la connexion de fédération de grille** et des comptes de tenant identiques existent sur les deux grilles. Voir "Gérez les locataires autorisés pour la connexion de fédération de grille".
- L'utilisateur locataire auquel vous vous connectez, comme il existe déjà sur les deux grilles, et appartient à un groupe d'utilisateurs qui possède le "Autorisation d'accès racine".

- Si vous vous connectez à la grille de destination du locataire en tant qu'utilisateur local, l'utilisateur root du compte locataire a défini un mot de passe pour votre compte utilisateur sur cette grille.

Créer deux compartiments identiques

Dans un premier temps, connectez-vous aux comptes de locataires correspondants sur chaque grille et créez des compartiments identiques.

Étapes

1. En commençant à partir de l'une des grilles de la connexion de fédération de grille, créez un nouveau compartiment :
   a. Connectez-vous au compte de tenant à l'aide des informations d'identification d'un utilisateur de tenant qui existe sur les deux grilles.

      Si vous ne parvenez pas à vous connecter à la grille de destination du locataire en tant qu'utilisateur local, vérifiez que l'utilisateur root du compte locataire a défini un mot de passe pour votre compte utilisateur.

   b. Suivez les instructions à "Créer un compartiment S3".
   c. Dans l'onglet **gérer les paramètres d'objet**, sélectionnez **Activer la gestion des versions d'objet**.
   d. Si le verrouillage objet S3 est activé pour votre système StorageGRID, n'activez pas le verrouillage objet S3 pour le compartiment.
   e. Sélectionnez **Créer un compartiment**.
   f. Sélectionnez **Terminer**.
2. Répétez ces étapes pour créer un compartiment identique pour le même compte locataire sur l'autre grille de la connexion de fédération de grille.

   Selon les besoins, chaque godet peut utiliser une région différente.

Activer la réplication entre les grilles

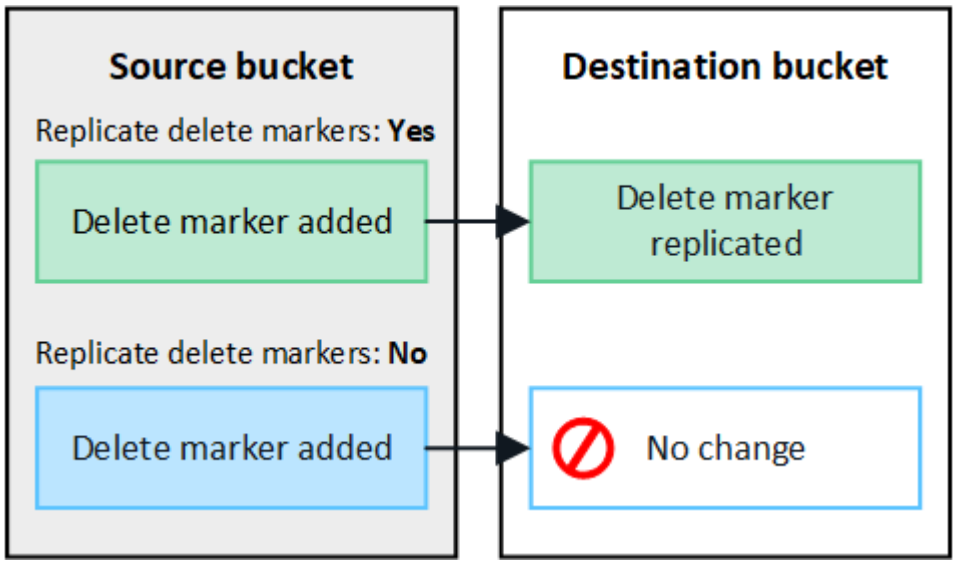
Vous devez effectuer ces étapes avant d'ajouter des objets à l'un ou l'autre compartiment.

Étapes

1. À partir d'une grille dont vous voulez répliquer les objets, activez "réplication multigrille dans une direction":
   a. Connectez-vous au compte du locataire pour le compartiment.
   b. Sélectionnez **Afficher les compartiments** dans le tableau de bord ou sélectionnez **STOCKAGE (S3)** > **compartiments**.
   c. Sélectionnez le nom du compartiment dans le tableau pour accéder à la page de détails du compartiment.
   d. Sélectionnez l'onglet **réplication multigrille**.
   e. Sélectionnez **Activer** et consultez la liste des exigences.
   f. Si toutes les exigences ont été satisfaites, sélectionnez la connexion de fédération de grille que vous souhaitez utiliser.
   g. Vous pouvez également modifier le paramètre **replicate delete markers** pour déterminer ce qui se passe sur la grille de destination si un client S3 envoie une demande de suppression à la grille source

qui n'inclut pas d'ID de version :

- **Yes** (par défaut) : un marqueur de suppression est ajouté au compartiment source et répliqué dans le compartiment de destination.
- **Non** : un marqueur de suppression est ajouté au compartiment source mais n'est pas répliqué dans le compartiment de destination.



> Si la demande de suppression inclut un ID de version, cette version de l'objet est définitivement supprimée du compartiment source. StorageGRID ne réplique pas les demandes de suppression qui incluent un ID de version, de sorte que la même version d'objet n'est pas supprimée de la destination.

Voir "Qu'est-ce que la réplication cross-grid" pour plus de détails.

a. Vous pouvez également modifier le paramètre de la catégorie d'audit **réplication multigrille** pour gérer le volume des messages d'audit :
   - **Erreur** (par défaut) : seules les demandes de réplication inter-grille en échec sont incluses dans la sortie d'audit.
   - **Normal** : toutes les demandes de réplication inter-grille sont incluses, ce qui augmente considérablement le volume de la sortie d'audit.

b. Vérifiez vos sélections. Vous ne pouvez pas modifier ces paramètres à moins que les deux compartiments ne soient vides.

c. Sélectionnez **Activer et tester**.

   Après quelques instants, un message de réussite s'affiche. Les objets ajoutés à ce compartiment seront désormais automatiquement répliqués sur l'autre grille. **La réplication multigrille** est affichée sous la forme d'une fonction activée sur la page de détails du compartiment.

2. Si vous le souhaitez, accédez au compartiment correspondant sur l'autre grille et "activez la réplication entre les grilles dans les deux sens".

Tester la réplication entre les grilles

Si la réplication inter-grid est activée pour un compartiment, vous devrez peut-être vérifier que la connexion et la réplication inter-grid fonctionnent correctement et que les compartiments source et de destination répondent

toujours à toutes les exigences (par exemple, la gestion des versions est toujours activée).

Avant de commencer

- Vous utilisez un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Autorisation d'accès racine".

Étapes

1. Connectez-vous au compte du locataire pour le compartiment.
2. Sélectionnez **Afficher les compartiments** dans le tableau de bord ou sélectionnez **STOCKAGE (S3)** > **compartiments**.
3. Sélectionnez le nom du compartiment dans le tableau pour accéder à la page de détails du compartiment.
4. Sélectionnez l'onglet **réplication multigrille**.
5. Sélectionnez **Tester la connexion**.

   Si la connexion est bonne, une bannière de réussite s'affiche. Sinon, un message d'erreur s'affiche, que vous et l'administrateur de la grille pouvez utiliser pour résoudre le problème. Pour plus de détails, voir "Dépanner les erreurs de fédération de grille".

6. Si la réplication inter-grille est configurée pour se produire dans les deux sens, allez dans le compartiment correspondant sur l'autre grille et sélectionnez **Tester la connexion** pour vérifier que la réplication inter-grille fonctionne dans l'autre sens.

Désactiver la réplication entre les grilles

Vous pouvez arrêter définitivement la réplication multigrille si vous ne souhaitez plus copier d'objets sur l'autre grille.

Avant de désactiver la réplication multigrille, notez ce qui suit :

- La désactivation de la réplication multigrille ne supprime pas les objets qui ont déjà été copiés entre les grilles. Par exemple, les objets de `my-bucket` la grille 1 qui ont été copiés sur `my-bucket` la grille 2 ne sont pas supprimés si vous désactivez la réplication inter-grille pour ce compartiment. Si vous souhaitez supprimer ces objets, vous devez les supprimer manuellement.
- Si la réplication inter-grid a été activée pour chacun des compartiments (c'est-à-dire si la réplication se produit dans les deux directions), vous pouvez désactiver la réplication inter-grid pour l'un ou les deux compartiments. Par exemple, vous pouvez désactiver la réplication d'objets de `my-bucket` sur la grille 1 vers `my-bucket` sur la grille 2, tout en continuant à répliquer des objets de `my-bucket` sur la grille 2 vers sur `my-bucket` la grille 1.
- Vous devez désactiver la réplication multigrille avant de pouvoir supprimer l'autorisation d'un locataire d'utiliser la connexion de fédération de grille. Voir "Gérer les locataires autorisés".
- Si vous désactivez la réplication inter-grid pour un compartiment contenant des objets, vous ne pourrez pas réactiver la réplication inter-grid à moins de supprimer tous les objets des compartiments source et de destination.

> ⚠ Vous ne pouvez pas réactiver la réplication sauf si les deux compartiments sont vides.

Avant de commencer

- Vous utilisez un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Autorisation d'accès racine".

Étapes

1. Depuis la grille dont vous ne souhaitez plus répliquer les objets, arrêtez la réplication inter-grid pour le compartiment :
   a. Connectez-vous au compte du locataire pour le compartiment.
   b. Sélectionnez **Afficher les compartiments** dans le tableau de bord ou sélectionnez **STOCKAGE (S3)** > **compartiments**.
   c. Sélectionnez le nom du compartiment dans le tableau pour accéder à la page de détails du compartiment.
   d. Sélectionnez l'onglet **réplication multigrille**.
   e. Sélectionnez **Désactiver la réplication**.
   f. Si vous êtes sûr de vouloir désactiver la réplication inter-grille pour ce compartiment, tapez **Yes** dans la zone de texte et sélectionnez **Disable**.

      Après quelques instants, un message de réussite s'affiche. Les nouveaux objets ajoutés à ce compartiment ne peuvent plus être automatiquement répliqués sur l'autre grille. **La réplication multigrille** n'est plus affichée comme fonction activée sur la page compartiments.
2. Si la réplication inter-grille a été configurée pour se produire dans les deux directions, allez dans le compartiment correspondant sur l'autre grille et arrêtez la réplication inter-grille dans l'autre direction.

Afficher les connexions de fédération de grille

Si votre compte de locataire dispose de l'autorisation **utiliser la connexion de fédération de grille**, vous pouvez afficher les connexions autorisées.

Avant de commencer

- Le compte de tenant dispose de l'autorisation **utiliser la connexion de fédération de grille**.
- Vous êtes connecté au gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Autorisation d'accès racine".

Étapes

1. Sélectionnez **STORAGE (S3)** > **Grid federation connections**.

   La page de connexion de fédération de grille s'affiche et comprend un tableau qui résume les informations suivantes :

Colonne	Description
Nom de la connexion	Les connexions de fédération de grille que ce locataire a l'autorisation d'utiliser.
Compartiments avec réplication inter-grid	Pour chaque connexion de fédération de grid, les compartiments de locataire pour lesquels la réplication inter-grid est activée. Les objets ajoutés à ces compartiments seront répliqués sur l'autre grille de la connexion.

Colonne	Description
Dernière erreur	Pour chaque connexion de fédération de grille, l'erreur la plus récente se produit, le cas échéant, lors de la réplication des données vers l'autre grille. Voir Effacez la dernière erreur.

2. Si vous le souhaitez, sélectionnez un nom de compartiment à "afficher les détails du compartiment".

efface la dernière erreur

Une erreur peut apparaître dans la colonne **dernière erreur** pour l'une des raisons suivantes :

- La version de l'objet source est introuvable.
- Le compartiment source est introuvable.
- Le compartiment de destination a été supprimé.
- Le compartiment de destination a été recréé par un autre compte.
- La gestion des versions du compartiment de destination est suspendue.
- Le compartiment de destination a été recréé par le même compte, mais il n'est plus versionné.

> Cette colonne affiche uniquement la dernière erreur de réplication inter-grille à se produire ; les erreurs précédentes qui se sont peut-être produites ne seront pas affichées.

Étapes

1. Si un message apparaît dans la colonne **dernière erreur**, affichez le texte du message.

   Par exemple, cette erreur indique que le compartiment de destination de la réplication inter-grid était dans un état non valide, probablement parce que la gestion de version a été suspendue ou que le verrouillage d'objet S3 a été activé.

2. Effectuez toutes les actions recommandées. Par exemple, si la gestion des versions a été suspendue dans le compartiment de destination pour la réplication inter-grid, réactivez la gestion des versions pour ce compartiment.
3. Sélectionnez la connexion dans le tableau.
4. Sélectionnez **Effacer erreur**.
5. Sélectionnez **Oui** pour effacer le message et mettre à jour l'état du système.

6. Patientez 5-6 minutes, puis ingérer un nouvel objet dans le compartiment. Vérifiez que le message d'erreur ne réapparaît pas.

> Pour vous assurer que le message d'erreur est effacé, attendez au moins 5 minutes après l'horodatage dans le message avant d'ingérer un nouvel objet.

7. Pour déterminer si des objets n'ont pas pu être répliqués en raison de l'erreur de compartiment, reportez-vous à la section "Identifier et réessayer les opérations de réplication ayant échoué".

Gestion des groupes et des utilisateurs

Utiliser la fédération des identités

L'utilisation de la fédération des identités accélère la configuration des groupes de locataires et des utilisateurs, et permet aux utilisateurs de se connecter au compte du locataire à l'aide des identifiants familiers.

Configurez la fédération des identités pour le gestionnaire des locataires

Vous pouvez configurer la fédération des identités pour le Gestionnaire de locataires si vous souhaitez que les groupes et les utilisateurs de locataires soient gérés dans un autre système, tel qu'Active Directory, Azure Active Directory (Azure AD), OpenLDAP ou Oracle Directory Server.

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Autorisation d'accès racine".
- Vous utilisez Active Directory, Azure AD, OpenLDAP ou Oracle Directory Server comme fournisseur d'identité.

> Si vous souhaitez utiliser un service LDAP v3 non répertorié, contactez le support technique.

- Si vous avez l'intention d'utiliser OpenLDAP, vous devez configurer le serveur OpenLDAP. Voir Instructions de configuration du serveur OpenLDAP.
- Si vous prévoyez d'utiliser TLS (transport Layer Security) pour les communications avec le serveur LDAP, le fournisseur d'identité doit utiliser TLS 1.2 ou 1.3. Voir "Chiffrement pris en charge pour les connexions TLS sortantes".

Description de la tâche

La configuration d'un service de fédération des identités pour votre locataire dépend de la configuration de votre compte locataire. Votre locataire peut partager le service de fédération des identités configuré pour Grid Manager. Si ce message s'affiche lorsque vous accédez à la page Fédération des identités, vous ne pouvez pas configurer un référentiel d'identité fédéré distinct pour ce locataire.

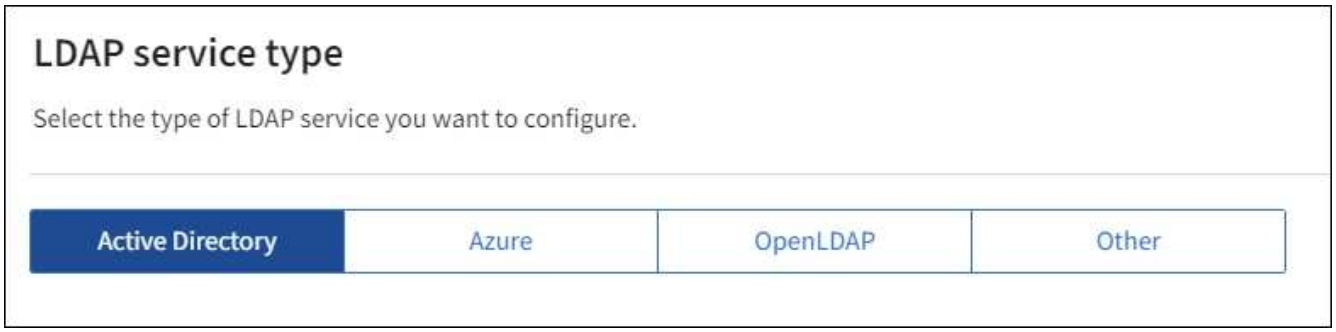
> This tenant account uses the LDAP server that is configured for the Grid Manager. Contact the grid administrator for information or to change this setting.

Entrez la configuration

Lorsque vous configurez la fédération Identify, vous fournissez les valeurs dont StorageGRID a besoin pour se connecter à un service LDAP.

Étapes

1. Sélectionnez **ACCESS MANAGEMENT** > **identity federation**.
2. Sélectionnez **Activer la fédération d'identités**.
3. Dans la section Type de service LDAP, sélectionnez le type de service LDAP que vous souhaitez configurer.



   Sélectionnez **autre** pour configurer les valeurs d'un serveur LDAP qui utilise Oracle Directory Server.

4. Si vous avez sélectionné **autre**, renseignez les champs de la section attributs LDAP. Dans le cas contraire, passez à l'étape suivante.
   - **Nom unique utilisateur** : nom de l'attribut qui contient l'identifiant unique d'un utilisateur LDAP. Cet attribut est équivalent à `sAMAccountName` pour Active Directory et `uid` pour OpenLDAP. Si vous configurez Oracle Directory Server, entrez `uid`.
   - **UUID d'utilisateur** : nom de l'attribut qui contient l'identifiant unique permanent d'un utilisateur LDAP. Cet attribut est équivalent à `objectGUID` pour Active Directory et `entryUUID` pour OpenLDAP. Si vous configurez Oracle Directory Server, entrez `nsuniqueid`. La valeur de chaque utilisateur pour l'attribut spécifié doit être un nombre hexadécimal à 32 chiffres au format 16 octets ou chaîne, où les tirets sont ignorés.
   - **Nom unique de groupe** : nom de l'attribut qui contient l'identifiant unique d'un groupe LDAP. Cet attribut est équivalent à `sAMAccountName` pour Active Directory et `cn` pour OpenLDAP. Si vous configurez Oracle Directory Server, entrez `cn`.
   - **UUID de groupe** : nom de l'attribut qui contient l'identificateur unique permanent d'un groupe LDAP. Cet attribut est équivalent à `objectGUID` pour Active Directory et `entryUUID` pour OpenLDAP. Si vous configurez Oracle Directory Server, entrez `nsuniqueid`. La valeur de chaque groupe pour l'attribut spécifié doit être un nombre hexadécimal à 32 chiffres au format 16 octets ou chaîne, où les tirets sont ignorés.
5. Pour tous les types de services LDAP, entrez les informations de connexion réseau et de serveur LDAP requises dans la section configurer le serveur LDAP.
   - **Nom d'hôte** : le nom de domaine complet (FQDN) ou l'adresse IP du serveur LDAP.
   - **Port** : port utilisé pour se connecter au serveur LDAP.

> ⓘ Le port par défaut de STARTTLS est 389 et le port par défaut de LDAPS est 636. Cependant, vous pouvez utiliser n'importe quel port tant que votre pare-feu est configuré correctement.

- **Nom d'utilisateur** : chemin complet du nom distinctif (DN) de l'utilisateur qui se connectera au serveur LDAP.

  Pour Active Directory, vous pouvez également spécifier le nom de connexion bas niveau ou le nom principal d'utilisateur.

  L'utilisateur spécifié doit être autorisé à répertorier les groupes et les utilisateurs et à accéder aux attributs suivants :

  - `sAMAccountName` ou `uid`
  - `objectGUID`, `entryUUID` ou `nsuniqueid`
  - `cn`
  - `memberOf` ou `isMemberOf`
  - **Active Directory** : `objectSid`, `primaryGroupID`, `userAccountControl` et `userPrincipalName`
  - **Azure**: `accountEnabled` Et `userPrincipalName`
- **Mot de passe** : mot de passe associé au nom d'utilisateur.

  > Si vous modifiez le mot de passe à l'avenir, vous devez le mettre à jour sur cette page.

- **DN de base de groupe** : chemin complet du nom distinctif (DN) pour une sous-arborescence LDAP que vous voulez rechercher des groupes. Dans l'exemple Active Directory (ci-dessous), tous les groupes dont le nom unique est relatif au DN de base (DC=storagegrid,DC=exemple,DC=com) peuvent être utilisés comme groupes fédérés.

  > Les valeurs **Nom unique de groupe** doivent être uniques dans le **DN de base de groupe** auquel elles appartiennent.

- **DN de base d'utilisateurs** : le chemin complet du nom distinctif (DN) d'une sous-arborescence LDAP que vous voulez rechercher des utilisateurs.

  > Les valeurs **Nom unique utilisateur** doivent être uniques dans le **DN de base utilisateur** auquel elles appartiennent.

- **Bind username format** (facultatif) : le nom d'utilisateur par défaut StorageGRID devrait utiliser si le modèle ne peut pas être déterminé automatiquement.

  Il est recommandé de fournir le format **Bind username** car il peut permettre aux utilisateurs de se connecter si StorageGRID ne parvient pas à se lier avec le compte de service.

  Entrez l'un des motifs suivants :

  - **Pattern UserPrincipalName (Active Directory et Azure)** : `[USERNAME]@*example*.com`
  - **Modèle de nom de connexion de niveau inférieur (Active Directory et Azure)** : `*example*\[USERNAME]`
  - **Motif de nom distinctif** : `CN=[USERNAME],CN=Users,DC=*example*,DC=com`

    Inclure **[NOM D'UTILISATEUR]** exactement comme écrit.

6. Dans la section transport Layer Security (TLS), sélectionnez un paramètre de sécurité.
   - **Utilisez STARTTLS** : utilisez STARTTLS pour sécuriser les communications avec le serveur LDAP. Il s'agit de l'option recommandée pour Active Directory, OpenLDAP ou autre, mais cette option n'est pas prise en charge pour Azure.
   - **Utilisez LDAPS** : l'option LDAPS (LDAP sur SSL) utilise TLS pour établir une connexion au serveur LDAP. Vous devez sélectionner cette option pour Azure.
   - **N'utilisez pas TLS** : le trafic réseau entre le système StorageGRID et le serveur LDAP ne sera pas sécurisé. Cette option n'est pas prise en charge pour Azure.

   > L'utilisation de l'option **ne pas utiliser TLS** n'est pas prise en charge si votre serveur Active Directory applique la signature LDAP. Vous devez utiliser STARTTLS ou LDAPS.

7. Si vous avez sélectionné STARTTLS ou LDAPS, choisissez le certificat utilisé pour sécuriser la connexion.
   - **Utilisez le certificat CA du système d'exploitation** : utilisez le certificat CA de la grille par défaut installé sur le système d'exploitation pour sécuriser les connexions.
   - **Utilisez un certificat d'autorité de certification personnalisé** : utilisez un certificat de sécurité personnalisé.

     Si vous sélectionnez ce paramètre, copiez et collez le certificat de sécurité personnalisé dans la zone de texte certificat de l'autorité de certification.

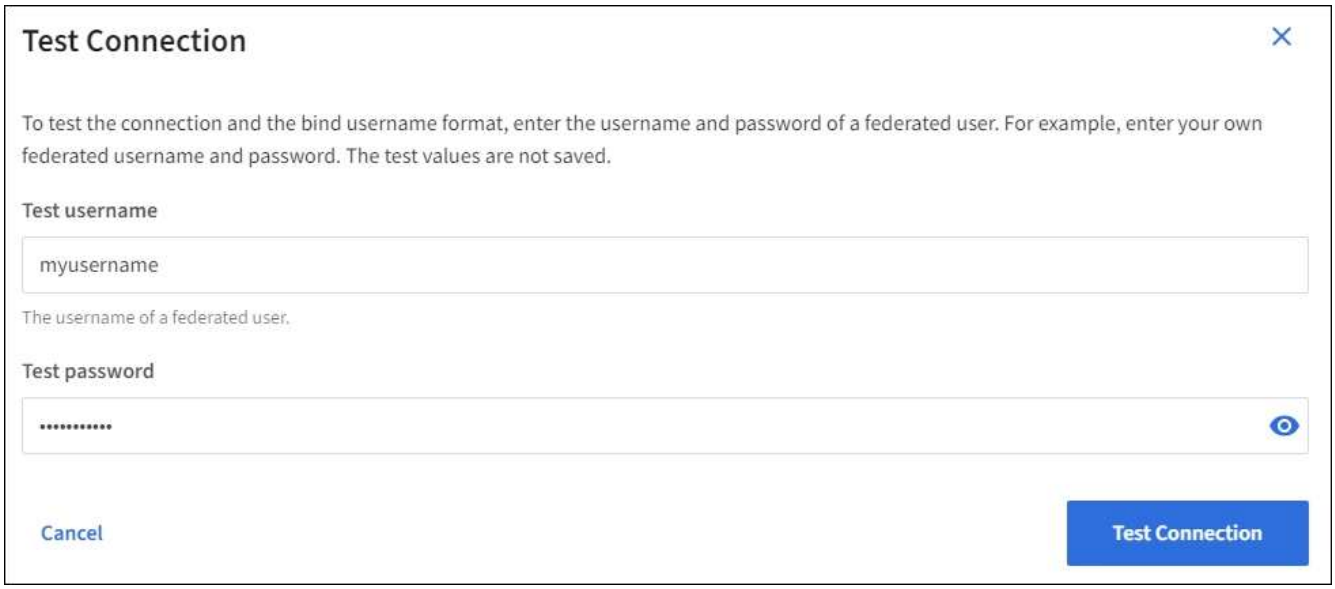
Testez la connexion et enregistrez la configuration

Après avoir saisi toutes les valeurs, vous devez tester la connexion avant de pouvoir enregistrer la configuration. StorageGRID vérifie les paramètres de connexion pour le serveur LDAP et le format de nom d'utilisateur BIND, si vous en avez fourni un.

Étapes

1. Sélectionnez **Tester la connexion**.
2. Si vous n'avez pas fourni de format de nom d'utilisateur de liaison :
   - Si les paramètres de connexion sont valides, le message « Test de connexion réussi » s'affiche. Sélectionnez **Enregistrer** pour enregistrer la configuration.
   - Si les paramètres de connexion ne sont pas valides, le message « Impossible d'établir la connexion de test » s'affiche. Sélectionnez **Fermer**. Ensuite, résolvez tout problème et testez à nouveau la connexion.
3. Si vous avez fourni un format de nom d'utilisateur BIND, entrez le nom d'utilisateur et le mot de passe d'un utilisateur fédéré valide.

   Par exemple, entrez votre nom d'utilisateur et votre mot de passe. N'incluez pas de caractères spéciaux dans le nom d'utilisateur, tels que @ ou /.



- Si les paramètres de connexion sont valides, le message « Test de connexion réussi » s'affiche. Sélectionnez **Enregistrer** pour enregistrer la configuration.
- Un message d'erreur s'affiche si les paramètres de connexion, le format du nom d'utilisateur de liaison ou le nom d'utilisateur et le mot de passe du test sont incorrects. Résolvez tout problème et testez à nouveau la connexion.

Forcer la synchronisation avec le référentiel d'identité

Le système StorageGRID synchronise régulièrement les groupes fédérés et les utilisateurs à partir du référentiel d'identité. Vous pouvez forcer la synchronisation à démarrer si vous souhaitez activer ou restreindre les autorisations utilisateur le plus rapidement possible.

Étapes

1. Accédez à la page fédération des identités.
2. Sélectionnez **serveur de synchronisation** en haut de la page.

   Le processus de synchronisation peut prendre un certain temps en fonction de votre environnement.

   L'alerte **échec de synchronisation de la fédération d'identités** est déclenchée en cas de problème de synchronisation des groupes fédérés et des utilisateurs à partir du référentiel d'identité.

Désactiver la fédération des identités

Vous pouvez désactiver temporairement ou définitivement la fédération des identités pour les groupes et les utilisateurs. Lorsque la fédération des identités est désactivée, il n'y a aucune communication entre StorageGRID et le référentiel d'identité. Cependant, tous les paramètres que vous avez configurés sont conservés, ce qui vous permet de réactiver facilement la fédération d'identités à l'avenir.

Description de la tâche

Avant de désactiver la fédération des identités, vous devez prendre connaissance des points suivants :

- Les utilisateurs fédérés ne pourront pas se connecter.
- Les utilisateurs fédérés qui sont actuellement connectés conservent l'accès au système StorageGRID

jusqu'à l'expiration de leur session, mais ils ne pourront pas se connecter après l'expiration de leur session.

- La synchronisation entre le système StorageGRID et le référentiel d'identité ne se fera pas et les alertes ne seront pas émises pour les comptes qui n'ont pas été synchronisés.
- La case **Activer la fédération d'identité** est désactivée si l'authentification unique (SSO) est définie sur **activé** ou **mode Sandbox**. Le statut SSO sur la page connexion unique doit être **désactivé** avant de pouvoir désactiver la fédération d'identités. Voir "Désactiver l'authentification unique".

Étapes

1. Accédez à la page fédération des identités.
2. Décochez la case **Activer la fédération d'identité**.

Instructions de configuration du serveur OpenLDAP

Si vous souhaitez utiliser un serveur OpenLDAP pour la fédération des identités, vous devez configurer des paramètres spécifiques sur le serveur OpenLDAP.

> Pour les référentiels d'identité qui ne sont pas ActiveDirectory ou Azure, StorageGRID ne bloquera pas automatiquement l'accès S3 aux utilisateurs désactivés en externe. Pour bloquer l'accès S3, supprimez les clés S3 de l'utilisateur ou supprimez l'utilisateur de tous les groupes.

Recouvrements de memberOf et de raffint

Les recouvrements de membre et de raffinage doivent être activés. Pour plus d'informations, reportez-vous aux instructions relatives à la maintenance des membres de groupe inversé dans le "Documentation OpenLDAP : version 2.4 - Guide de l'administrateur".

Indexation

Vous devez configurer les attributs OpenLDAP suivants avec les mots-clés d'index spécifiés :

- `olcDbIndex: objectClass eq`
- `olcDbIndex: uid eq,pres,sub`
- `olcDbIndex: cn eq,pres,sub`
- `olcDbIndex: entryUUID eq`

De plus, assurez-vous que les champs mentionnés dans l'aide pour le nom d'utilisateur sont indexés pour des performances optimales.

Reportez-vous aux informations sur la maintenance de l'appartenance à "Documentation OpenLDAP : version 2.4 - Guide de l'administrateur"un groupe inversé dans le .

Gestion des groupes de locataires

Créez des groupes pour un locataire S3

Vous pouvez gérer les autorisations des groupes d'utilisateurs S3 en important des groupes fédérés ou en créant des groupes locaux.

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Autorisation d'accès racine".
- Si vous prévoyez d'importer un groupe fédéré, vous avez "fédération des identités configurée"et le groupe fédéré existe déjà dans le référentiel d'identité configuré.
- Si votre compte de locataire dispose de l'autorisation **utiliser la connexion de fédération de grille**, vous avez examiné le flux de travail et les considérations pour "clonage de groupes de locataires et d'utilisateurs"et vous êtes connecté à la grille source du locataire.

Accédez à l'assistant de création de groupe

Pour la première étape, accédez à l'assistant de création de groupe.

Étapes

1. Sélectionnez **ACCESS MANAGEMENT** > **Groups**.
2. Si votre compte locataire dispose de l'autorisation **utiliser la connexion de fédération de grille**, vérifiez qu'une bannière bleue s'affiche, indiquant que les nouveaux groupes créés sur cette grille seront clonés sur le même locataire sur l'autre grille de la connexion. Si cette bannière n'apparaît pas, vous pouvez être connecté à la grille de destination du locataire.

3. Sélectionnez **Créer groupe**.

Choisissez un type de groupe

Vous pouvez créer un groupe local ou importer un groupe fédéré.

Étapes

1. Sélectionnez l'onglet **Groupe local** pour créer un groupe local ou sélectionnez l'onglet **Groupe fédéré** pour importer un groupe à partir du référentiel d'identité configuré précédemment.

   Si l'authentification unique (SSO) est activée pour votre système StorageGRID, les utilisateurs appartenant à des groupes locaux ne pourront pas se connecter au Gestionnaire de locataires, bien qu'ils puissent utiliser les applications client pour gérer les ressources du locataire, en fonction des autorisations de groupe.

2. Entrez le nom du groupe.
   - **Groupe local** : saisissez à la fois un nom d'affichage et un nom unique. Vous pouvez modifier le nom

d'affichage ultérieurement.

> Si votre compte de locataire dispose de l'autorisation **utiliser la connexion de fédération de grille**, une erreur de clonage se produit si le même **nom unique** existe déjà pour le locataire sur la grille de destination.

- **Groupe fédéré** : saisissez le nom unique. Pour Active Directory, le nom unique est le nom associé à l' `sAMAccountName`attribut. Pour OpenLDAP, le nom unique est le nom associé à l' `uid`attribut.

3. Sélectionnez **Continuer**.

Gérer les autorisations de groupe

Les autorisations de groupe contrôlent les tâches que les utilisateurs peuvent effectuer dans le Gestionnaire de locataires et l'API de gestion des locataires.

Étapes

1. Pour **Access mode**, sélectionnez l'une des options suivantes :
   - **Lecture-écriture** (par défaut) : les utilisateurs peuvent se connecter au gestionnaire de locataires et gérer la configuration du locataire.
   - **Lecture seule** : les utilisateurs peuvent uniquement afficher les paramètres et les fonctionnalités. Ils ne peuvent pas apporter de modifications ni exécuter d'opérations dans le gestionnaire de locataires ou l'API de gestion des locataires. Les utilisateurs locaux en lecture seule peuvent modifier leurs propres mots de passe.

> Si un utilisateur appartient à plusieurs groupes et qu'un groupe est défini sur lecture seule, l'utilisateur dispose d'un accès en lecture seule à tous les paramètres et fonctions sélectionnés.

2. Sélectionnez une ou plusieurs autorisations pour ce groupe.

   Voir "Autorisations de gestion des locataires".

3. Sélectionnez **Continuer**.

Définissez la règle de groupe S3

La stratégie de groupe détermine les autorisations d'accès S3 dont disposent les utilisateurs.

Étapes

1. Sélectionnez la stratégie que vous souhaitez utiliser pour ce groupe.

Stratégie de groupe	Description
Aucun accès à S3	Par défaut. Les utilisateurs de ce groupe n'ont pas accès aux ressources S3, sauf si l'accès est accordé avec une règle de compartiment. Si vous sélectionnez cette option, seul l'utilisateur root peut accéder aux ressources S3 par défaut.

Stratégie de groupe	Description
Accès en lecture seule	Les utilisateurs de ce groupe disposent d'un accès en lecture seule aux ressources S3. Par exemple, les utilisateurs de ce groupe peuvent afficher la liste des objets et lire les données d'objet, les métadonnées et les balises. Lorsque vous sélectionnez cette option, la chaîne JSON pour une stratégie de groupe en lecture seule s'affiche dans la zone de texte. Vous ne pouvez pas modifier cette chaîne.
Accès complet	Les utilisateurs de ce groupe bénéficient d'un accès complet aux ressources S3, y compris les compartiments. Lorsque vous sélectionnez cette option, la chaîne JSON pour une stratégie de groupe à accès complet s'affiche dans la zone de texte. Vous ne pouvez pas modifier cette chaîne.
Réduction des ransomwares	Cet exemple de règle s'applique à tous les compartiments de ce locataire. Les utilisateurs de ce groupe peuvent effectuer des actions courantes, mais ne peuvent pas supprimer définitivement des objets des compartiments pour lesquels la gestion des versions d'objet est activée. Les utilisateurs de tenant Manager disposant de l'autorisation **gérer tous les compartiments** peuvent remplacer cette stratégie de groupe. Limitez l'autorisation gérer tous les compartiments aux utilisateurs de confiance et utilisez l'authentification multifacteur (MFA), le cas échéant.
Personnalisées	Les utilisateurs du groupe se voient accorder les autorisations que vous spécifiez dans la zone de texte.

2. Si vous avez sélectionné **personnalisé**, entrez la stratégie de groupe. Chaque stratégie de groupe a une taille limite de 5,120 octets. Vous devez entrer une chaîne au format JSON valide.

   Pour plus d'informations sur les stratégies de groupe, notamment la syntaxe de la langue et des exemples, reportez-vous à la section "Exemples de stratégies de groupe".

3. Si vous créez un groupe local, sélectionnez **Continuer**. Si vous créez un groupe fédéré, sélectionnez **Créer groupe** et **Terminer**.

Ajouter des utilisateurs (groupes locaux uniquement)

Vous pouvez enregistrer le groupe sans ajouter d'utilisateurs, ou vous pouvez éventuellement ajouter des utilisateurs locaux qui existent déjà.

> Si votre compte de locataire dispose de l'autorisation **utiliser la connexion de fédération de grille**, tous les utilisateurs que vous sélectionnez lorsque vous créez un groupe local sur la grille source ne sont pas inclus lorsque le groupe est cloné dans la grille de destination. Pour cette raison, ne sélectionnez pas d'utilisateurs lorsque vous créez le groupe. Sélectionnez plutôt le groupe lorsque vous créez les utilisateurs.

Étapes

1. Vous pouvez également sélectionner un ou plusieurs utilisateurs locaux pour ce groupe.
2. Sélectionnez **Créer groupe** et **Terminer**.

   Le groupe que vous avez créé apparaît dans la liste des groupes.

   Si votre compte locataire dispose de l'autorisation **utiliser la connexion de fédération de grille** et que vous êtes sur la grille source du locataire, le nouveau groupe est cloné dans la grille de destination du locataire. **Succès** apparaît comme l'état **clonage** dans la section vue d'ensemble de la page de détails du groupe.

Créez des groupes pour un locataire Swift

Vous pouvez gérer les autorisations d'accès pour un compte de locataire Swift en important des groupes fédérés ou en créant des groupes locaux. Au moins un groupe doit disposer de l'autorisation Administrateur Swift, qui est requise pour gérer les conteneurs et les objets d'un compte de locataire Swift.

La prise en charge des applications du client Swift a été obsolète et sera supprimée dans une prochaine version.

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Autorisation d'accès racine".
- Si vous prévoyez d'importer un groupe fédéré, vous avez "fédération des identités configurée"et le groupe fédéré existe déjà dans le référentiel d'identité configuré.

Accédez à l'assistant de création de groupe

Étapes

Pour la première étape, accédez à l'assistant de création de groupe.

1. Sélectionnez **ACCESS MANAGEMENT** > **Groups**.
2. Sélectionnez **Créer groupe**.

Choisissez un type de groupe

Vous pouvez créer un groupe local ou importer un groupe fédéré.

Étapes

1. Sélectionnez l'onglet **Groupe local** pour créer un groupe local ou sélectionnez l'onglet **Groupe fédéré** pour importer un groupe à partir du référentiel d'identité configuré précédemment.

   Si l'authentification unique (SSO) est activée pour votre système StorageGRID, les utilisateurs appartenant à des groupes locaux ne pourront pas se connecter au Gestionnaire de locataires, bien qu'ils puissent utiliser les applications client pour gérer les ressources du locataire, en fonction des autorisations de groupe.

2. Entrez le nom du groupe.
   - **Groupe local** : saisissez à la fois un nom d'affichage et un nom unique. Vous pouvez modifier le nom d'affichage ultérieurement.

- **Groupe fédéré** : saisissez le nom unique. Pour Active Directory, le nom unique est le nom associé à l' `sAMAccountName`attribut. Pour OpenLDAP, le nom unique est le nom associé à l' `uid`attribut.

3. Sélectionnez **Continuer**.

Gérer les autorisations de groupe

Les autorisations de groupe contrôlent les tâches que les utilisateurs peuvent effectuer dans le Gestionnaire de locataires et l'API de gestion des locataires.

Étapes

1. Pour **Access mode**, sélectionnez l'une des options suivantes :
   - **Lecture-écriture** (par défaut) : les utilisateurs peuvent se connecter au gestionnaire de locataires et gérer la configuration du locataire.
   - **Lecture seule** : les utilisateurs peuvent uniquement afficher les paramètres et les fonctionnalités. Ils ne peuvent pas apporter de modifications ni exécuter d'opérations dans le gestionnaire de locataires ou l'API de gestion des locataires. Les utilisateurs locaux en lecture seule peuvent modifier leurs propres mots de passe.

   > Si un utilisateur appartient à plusieurs groupes et qu'un groupe est défini sur lecture seule, l'utilisateur dispose d'un accès en lecture seule à tous les paramètres et fonctions sélectionnés.

2. Cochez la case **accès racine** si les utilisateurs du groupe doivent se connecter à l'API tenant Manager ou tenant Management.
3. Sélectionnez **Continuer**.

Définissez la stratégie de groupe Swift

Les utilisateurs Swift ont besoin d'une autorisation d'administrateur pour s'authentifier auprès de l'API REST Swift afin de créer des conteneurs et d'ingérer des objets.

1. Cochez la case **Swift Administrator** si les utilisateurs du groupe doivent utiliser l'API REST Swift pour gérer les conteneurs et les objets.
2. Si vous créez un groupe local, sélectionnez **Continuer**. Si vous créez un groupe fédéré, sélectionnez **Créer groupe** et **Terminer**.

Ajouter des utilisateurs (groupes locaux uniquement)

Vous pouvez enregistrer le groupe sans ajouter d'utilisateurs, ou vous pouvez éventuellement ajouter des utilisateurs locaux qui existent déjà.

Étapes

1. Vous pouvez également sélectionner un ou plusieurs utilisateurs locaux pour ce groupe.

   Si vous n'avez pas encore créé d'utilisateurs locaux, vous pouvez ajouter ce groupe à l'utilisateur sur la page utilisateurs. Voir "Gérez les utilisateurs locaux".

2. Sélectionnez **Créer groupe** et **Terminer**.

   Le groupe que vous avez créé apparaît dans la liste des groupes.

Autorisations de gestion des locataires

Avant de créer un groupe de locataires, tenez compte des autorisations que vous souhaitez attribuer à ce groupe. Les autorisations de gestion des locataires déterminent les tâches que les utilisateurs peuvent effectuer à l'aide du Gestionnaire de locataires ou de l'API de gestion des locataires. Un utilisateur peut appartenir à un ou plusieurs groupes. Les autorisations sont cumulatives si un utilisateur appartient à plusieurs groupes.

Pour vous connecter au Gestionnaire de locataires ou utiliser l'API de gestion des locataires, les utilisateurs doivent appartenir à un groupe disposant d'au moins une autorisation. Tous les utilisateurs autorisés à se connecter peuvent effectuer les tâches suivantes :

- Afficher le tableau de bord
- Modifier son propre mot de passe (pour les utilisateurs locaux)

Pour toutes les autorisations, le paramètre mode d'accès du groupe détermine si les utilisateurs peuvent modifier les paramètres et effectuer des opérations ou s'ils ne peuvent afficher que les paramètres et les fonctions associés.

> Si un utilisateur appartient à plusieurs groupes et qu'un groupe est défini sur lecture seule, l'utilisateur dispose d'un accès en lecture seule à tous les paramètres et fonctions sélectionnés.

Vous pouvez attribuer les autorisations suivantes à un groupe. Notez que les locataires S3 et Swift disposent d'autorisations de groupe différentes.

Autorisations	Description	Détails
Accès racine	Donne un accès complet au gestionnaire des locataires et à l'API de gestion des locataires.	Les utilisateurs Swift doivent disposer d'une autorisation d'accès racine pour se connecter au compte du locataire.
Administrateur	Les locataires Swift uniquement. Fournit un accès complet aux conteneurs et objets Swift pour ce compte de locataire	Les utilisateurs Swift doivent disposer de l'autorisation d'administrateur Swift pour effectuer toute opération avec l'API REST Swift.
Gérez vos identifiants S3	Permet aux utilisateurs de créer et de supprimer leurs propres clés d'accès S3.	Les utilisateurs qui ne disposent pas de cette autorisation ne voient pas l'option de menu **STORAGE (S3)** > **My S3 Access keys**.

Autorisations	Description	Détails
Afficher tous les compartiments	**S3 tenants** : permet aux utilisateurs d'afficher toutes les configurations de compartiments et de compartiments. **Locataires Swift** : permet aux utilisateurs Swift d'afficher tous les conteneurs et configurations de conteneurs à l'aide de l'API de gestion des locataires.	Les utilisateurs qui ne disposent pas de l'autorisation Afficher tous les compartiments ou gérer tous les compartiments ne voient pas l'option de menu **compartiments**. Cette autorisation est remplacée par l'autorisation gérer tous les compartiments. Elle n'affecte pas les règles de compartiment S3 ou de groupe utilisées par les clients S3 ou la console S3. Vous pouvez uniquement attribuer cette autorisation à des groupes Swift à partir de l'API de gestion des locataires. Vous ne pouvez pas attribuer cette autorisation à des groupes Swift à l'aide du Gestionnaire de locataires.
Gestion de tous les compartiments	**Locataires S3** : permet aux utilisateurs d'utiliser le gestionnaire de locataires et l'API de gestion des locataires pour créer et supprimer des compartiments S3 et gérer les paramètres de tous les compartiments S3 du compte de locataire, indépendamment des règles de compartiment S3 ou de groupe. **Locataires Swift** : permet aux utilisateurs Swift de contrôler la cohérence des conteneurs Swift à l'aide de l'API de gestion des locataires.	Les utilisateurs qui ne disposent pas de l'autorisation Afficher tous les compartiments ou gérer tous les compartiments ne voient pas l'option de menu **compartiments**. Cette autorisation remplace l'autorisation Afficher tous les compartiments. Elle n'affecte pas les règles de compartiment S3 ou de groupe utilisées par les clients S3 ou la console S3. Vous pouvez uniquement attribuer cette autorisation à des groupes Swift à partir de l'API de gestion des locataires. Vous ne pouvez pas attribuer cette autorisation à des groupes Swift à l'aide du Gestionnaire de locataires.
Gestion des terminaux	Permet aux utilisateurs d'utiliser le gestionnaire de locataires ou l'API de gestion des locataires pour créer ou modifier des terminaux de service de plateforme, qui sont utilisés comme destination pour les services de plateforme StorageGRID.	Les utilisateurs qui ne disposent pas de cette autorisation ne voient pas l'option de menu **Platform Services Endpoints**.
Utilisez l'onglet de la console S3	Associé à l'autorisation Afficher tous les compartiments ou gérer tous les compartiments, permet aux utilisateurs d'afficher et de gérer des objets à partir de l'onglet de la console S3 de la page de détails d'un compartiment.	

Gérez vos groupes de locataires selon vos besoins pour afficher, modifier ou dupliquer un groupe, etc.

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Autorisation d'accès racine".

Afficher ou modifier un groupe

Vous pouvez afficher et modifier les informations de base et les détails de chaque groupe.

Étapes

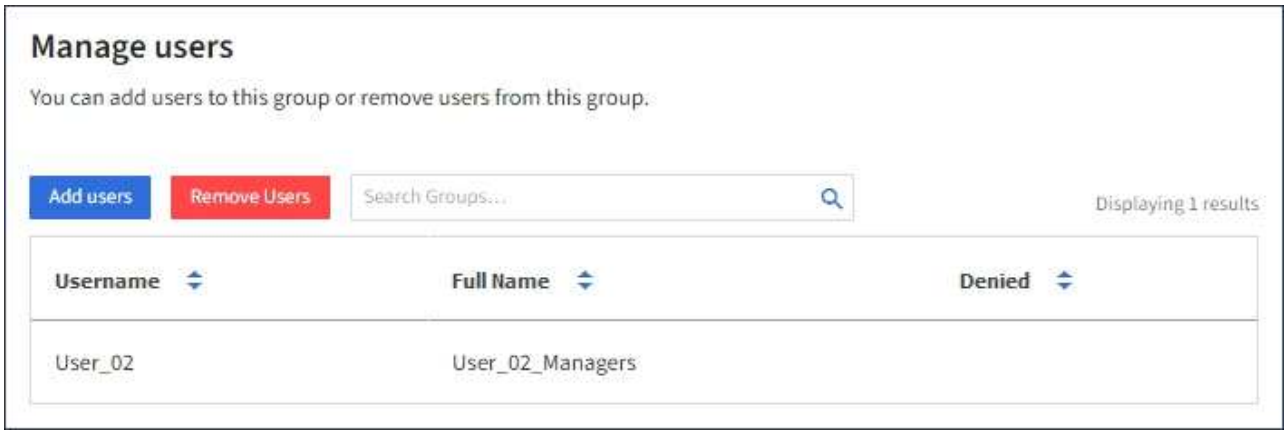
1. Sélectionnez **ACCESS MANAGEMENT** > **Groups**.
2. Consultez les informations fournies sur la page groupes, qui répertorie les informations de base pour tous les groupes locaux et fédérés pour ce compte de tenant.

   Si le compte de tenant dispose de l'autorisation **utiliser la connexion de fédération de grille** et que vous affichez des groupes sur la grille source du locataire :

   - Un message de bannière indique que si vous modifiez ou supprimez un groupe, vos modifications ne seront pas synchronisées avec l'autre grille.
   - Si nécessaire, un message de bannière indique si les groupes n'ont pas été clonés dans le locataire sur la grille de destination. Vous pouvez réessayez un clone de groupe que cela a échoué.
3. Si vous souhaitez modifier le nom du groupe :
   a. Cochez la case du groupe.
   b. Sélectionnez **actions** > **Modifier le nom du groupe**.
   c. Saisissez le nouveau nom.
   d. Sélectionnez **Enregistrer les modifications.**
4. Si vous souhaitez afficher plus de détails ou apporter des modifications supplémentaires, effectuez l'une des opérations suivantes :
   - Sélectionnez le nom du groupe.
   - Cochez la case du groupe et sélectionnez **actions** > **Afficher les détails du groupe**.
5. Consultez la section Présentation, qui présente les informations suivantes pour chaque groupe :
   - Nom d'affichage
   - Nom unique
   - Type
   - Mode d'accès
   - Autorisations
   - Règle S3
   - Nombre d'utilisateurs dans ce groupe
   - Champs supplémentaires si le compte de tenant dispose de l'autorisation **utiliser la connexion de fédération de grille** et que vous affichez le groupe sur la grille source du locataire :

- État de clonage, soit **succès** soit **échec**
- Une bannière bleue indiquant que si vous modifiez ou supprimez ce groupe, vos modifications ne seront pas synchronisées avec l'autre grille.

6. Modifiez les paramètres de groupe selon vos besoins. Voir "Créez des groupes pour un locataire S3" et "Créez des groupes pour un locataire Swift" pour plus de détails sur ce que vous devez saisir.
   a. Dans la section vue d'ensemble, modifiez le nom d'affichage en sélectionnant le nom ou l'icône d'édition .
   b. Dans l'onglet **autorisations de groupe**, mettez à jour les autorisations et sélectionnez **Enregistrer les modifications**.
   c. Dans l'onglet **Stratégie de groupe**, apportez les modifications nécessaires et sélectionnez **Enregistrer les modifications**.
      - Si vous modifiez un groupe S3, sélectionnez une règle de groupe S3 différente ou entrez la chaîne JSON pour une règle personnalisée, si nécessaire.
      - Si vous modifiez un groupe Swift, cochez ou décochez la case **Administrateur Swift**.
7. Pour ajouter un ou plusieurs utilisateurs locaux existants au groupe :
   a. Sélectionnez l'onglet utilisateurs.



   b. Sélectionnez **Ajouter des utilisateurs**.
   c. Sélectionnez les utilisateurs existants que vous souhaitez ajouter, puis sélectionnez **Ajouter des utilisateurs**.

      Un message de réussite s'affiche en haut à droite.

8. Pour supprimer des utilisateurs locaux du groupe :
   a. Sélectionnez l'onglet utilisateurs.
   b. Sélectionnez **Supprimer utilisateurs**.
   c. Sélectionnez les utilisateurs que vous souhaitez supprimer, puis sélectionnez **Supprimer utilisateurs**.

      Un message de réussite s'affiche en haut à droite.

9. Confirmez que vous avez sélectionné **Enregistrer les modifications** pour chaque section que vous avez modifiée.

Dupliquer le groupe

Vous pouvez dupliquer un groupe existant pour créer de nouveaux groupes plus rapidement.

> Si votre compte de locataire dispose de l'autorisation **utiliser la connexion de fédération de grille** et que vous dupliquez un groupe à partir de la grille source du locataire, le groupe dupliqué sera cloné dans la grille de destination du locataire.

Étapes

1. Sélectionnez **ACCESS MANAGEMENT** > **Groups**.
2. Cochez la case du groupe que vous souhaitez dupliquer.
3. Sélectionnez **actions** > **Dupliquer le groupe**.
4. Voir "Créez des groupes pour un locataire S3" ou "Créez des groupes pour un locataire Swift" pour plus de détails sur ce que vous devez saisir.
5. Sélectionnez **Créer groupe**.

Réessayez le clone de groupe

Pour réessayer un clone qui a échoué :

1. Sélectionnez chaque groupe indiquant *(échec du clonage)* sous le nom du groupe.
2. Sélectionnez **actions** > **groupes de clones**.
3. Consultez l'état de l'opération de clonage dans la page de détails de chaque groupe que vous êtes en train de cloner.

Pour plus d'informations, voir "Cloner des groupes de locataires et des utilisateurs".

Supprimer un ou plusieurs groupes

Vous pouvez supprimer un ou plusieurs groupes. Les utilisateurs qui appartiennent uniquement à un groupe supprimé ne pourront plus se connecter au gestionnaire de tenant ni utiliser le compte de tenant.

> Si votre compte de locataire dispose de l'autorisation **utiliser la connexion de fédération de grille** et que vous supprimez un groupe, StorageGRID ne supprimera pas le groupe correspondant sur l'autre grille. Si vous devez conserver ces informations synchronisées, vous devez supprimer le même groupe des deux grilles.

Étapes

1. Sélectionnez **ACCESS MANAGEMENT** > **Groups**.
2. Cochez la case correspondant à chaque groupe à supprimer.
3. Sélectionnez **actions** > **Supprimer groupe** ou **actions** > **Supprimer groupes**.

   Une boîte de dialogue de confirmation s'affiche.

4. Sélectionnez **Supprimer le groupe** ou **Supprimer les groupes**.

Gérez les utilisateurs locaux

Vous pouvez créer des utilisateurs locaux et les affecter à des groupes locaux pour

déterminer les fonctions auxquelles ces utilisateurs peuvent accéder. Le gestionnaire de locataires comprend un utilisateur local prédéfini, nommé « root ». Bien que vous puissiez ajouter et supprimer des utilisateurs locaux, vous ne pouvez pas supprimer l'utilisateur racine.

> Si l'authentification unique (SSO) est activée pour votre système StorageGRID, les utilisateurs locaux ne pourront pas se connecter au gestionnaire de locataires ou à l'API de gestion des locataires, bien qu'ils puissent utiliser des applications clientes pour accéder aux ressources du locataire, en fonction des autorisations de groupe.

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Autorisation d'accès racine".
- Si votre compte de locataire dispose de l'autorisation **utiliser la connexion de fédération de grille**, vous avez examiné le flux de travail et les considérations pour "clonage de groupes de locataires et d'utilisateurs"et vous êtes connecté à la grille source du locataire.

Créez un utilisateur local

Vous pouvez créer un utilisateur local et l'affecter à un ou plusieurs groupes locaux pour contrôler leurs autorisations d'accès.

Les utilisateurs S3 qui n'appartiennent à aucun groupe ne disposent pas d'autorisations de gestion ni de règles de groupe S3 qui leur sont appliquées. Il est possible que les utilisateurs bénéficient d'un accès par compartiment S3 accordé via une règle de compartiment.

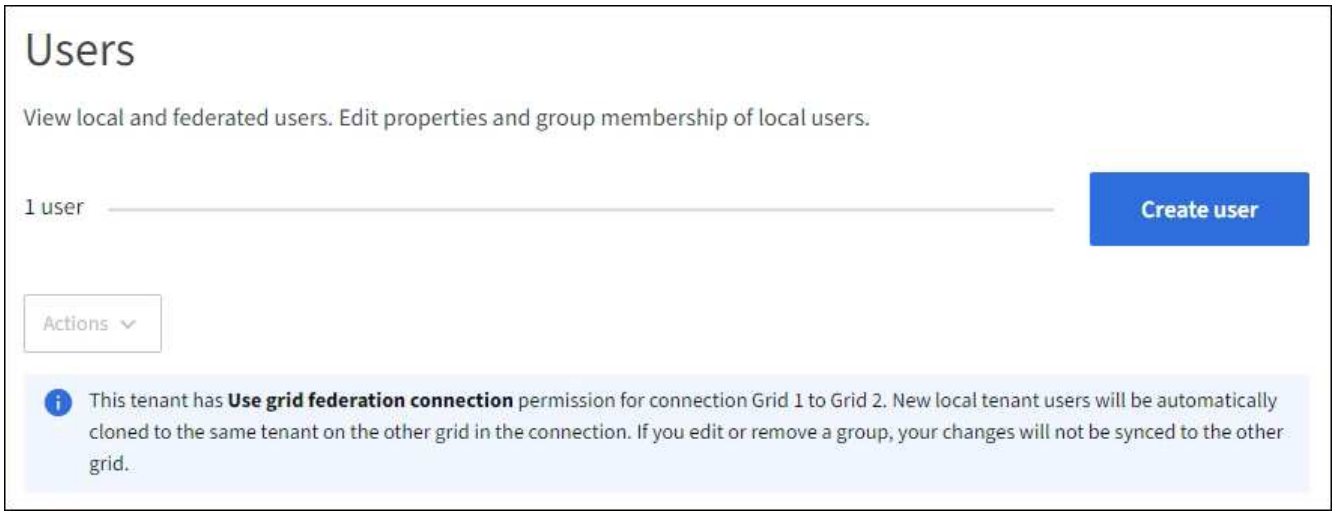
Les utilisateurs Swift qui n'appartiennent à aucun groupe ne disposent d'aucune autorisation de gestion ou d'un accès au conteneur Swift.

Accédez à l'assistant de création d'utilisateur

Étapes

1. Sélectionnez **ACCESS MANAGEMENT** > **Users**.

   Si votre compte de locataire dispose de l'autorisation **utiliser la connexion de fédération de grille**, une bannière bleue indique qu'il s'agit de la grille source du locataire. Tous les utilisateurs locaux que vous créez sur cette grille seront clonés dans l'autre grille de la connexion.



2. Sélectionnez **Créer utilisateur**.

Entrez les informations d'identification

Étapes

1. Pour l'étape **entrer les informations d'identification de l'utilisateur**, renseignez les champs suivants.

Champ	Description
Nom complet	Le nom complet de cet utilisateur, par exemple le prénom et le nom d'une personne ou le nom d'une application.
Nom d'utilisateur	Le nom que cet utilisateur utilisera pour se connecter. Les noms d'utilisateur doivent être uniques et ne peuvent pas être modifiés. **Remarque** : si votre compte locataire dispose de l'autorisation **utiliser la connexion de fédération de grille**, une erreur de clonage se produit si le même **Nom d'utilisateur** existe déjà pour le locataire sur la grille de destination.
Mot de passe et confirmer le mot de passe	Le mot de passe que l'utilisateur utilisera lors de sa connexion.
Refuser l'accès	Sélectionnez **Oui** pour empêcher cet utilisateur de se connecter au compte de tenant, même s'il appartient toujours à un ou plusieurs groupes. Par exemple, sélectionnez **Oui** pour suspendre temporairement la capacité d'un utilisateur à se connecter.

2. Sélectionnez **Continuer**.

Affecter à des groupes

Étapes

1. Attribuez l'utilisateur à un ou plusieurs groupes locaux pour déterminer les tâches qu'ils peuvent effectuer.

L'attribution d'un utilisateur à des groupes est facultative. Si vous le souhaitez, vous pouvez sélectionner des utilisateurs lorsque vous créez ou modifiez des groupes.

Les utilisateurs qui n'appartiennent à aucun groupe ne disposent d'aucune autorisation de gestion. Les autorisations sont cumulatives. Les utilisateurs disposent de toutes les autorisations pour tous les groupes auxquels ils appartiennent. Voir "Autorisations de gestion des locataires".

2. Sélectionnez **Créer utilisateur**.

   Si votre compte locataire dispose de l'autorisation **utiliser la connexion de fédération de grille** et que vous êtes sur la grille source du locataire, le nouvel utilisateur local est cloné dans la grille de destination du locataire. **Succès** apparaît comme l'état **clonage** dans la section vue d'ensemble de la page de détails de l'utilisateur.

3. Sélectionnez **Terminer** pour revenir à la page utilisateurs.

Afficher ou modifier un utilisateur local

Étapes

1. Sélectionnez **ACCESS MANAGEMENT** > **Users**.
2. Consultez les informations fournies sur la page utilisateurs, qui répertorie les informations de base pour tous les utilisateurs locaux et fédérés pour ce compte de tenant.

   Si le compte de tenant dispose de l'autorisation **utiliser la connexion de fédération de grille** et que vous affichez l'utilisateur sur la grille source du locataire :

   - Un message de bannière indique que si vous modifiez ou supprimez un utilisateur, vos modifications ne seront pas synchronisées avec l'autre grille.
   - Si nécessaire, un message de bannière indique si les utilisateurs n'ont pas été clonés dans le locataire sur la grille de destination. Vous pouvez réessayez un clone utilisateur qui a échoué.
3. Si vous souhaitez modifier le nom complet de l'utilisateur :
   a. Cochez la case de l'utilisateur.
   b. Sélectionnez **actions** > **Modifier le nom complet**.
   c. Saisissez le nouveau nom.
   d. Sélectionnez **Enregistrer les modifications.**
4. Si vous souhaitez afficher plus de détails ou apporter des modifications supplémentaires, effectuez l'une des opérations suivantes :
   - Sélectionnez le nom d'utilisateur.
   - Cochez la case de l'utilisateur et sélectionnez **actions** > **Afficher les détails de l'utilisateur**.
5. Consultez la section Présentation, qui présente les informations suivantes pour chaque utilisateur :
   - Nom complet
   - Nom d'utilisateur
   - Type d'utilisateur
   - Accès refusé
   - Mode d'accès
   - Appartenance à un groupe

- Champs supplémentaires si le compte de tenant dispose de l'autorisation **utiliser la connexion de fédération de grille** et que vous affichez l'utilisateur sur la grille source du locataire :
  - État de clonage, soit **succès** soit **échec**
  - Une bannière bleue indiquant que si vous modifiez cet utilisateur, vos modifications ne seront pas synchronisées avec l'autre grille.

6. Modifiez les paramètres utilisateur selon vos besoins. Voir Créer un utilisateur local pour plus de détails sur ce que vous devez saisir.
   a. Dans la section vue d'ensemble, modifiez le nom complet en sélectionnant le nom ou l'icône d'édition .

      Vous ne pouvez pas modifier le nom d'utilisateur.

   b. Dans l'onglet **Mot de passe**, modifiez le mot de passe de l'utilisateur et sélectionnez **Enregistrer les modifications**.
   c. Dans l'onglet **accès**, sélectionnez **non** pour permettre à l'utilisateur de se connecter ou sélectionnez **Oui** pour empêcher l'utilisateur de se connecter. Ensuite, sélectionnez **Enregistrer les modifications**.
   d. Dans l'onglet **clés d'accès**, sélectionnez **Créer une clé** et suivez les instructions pour "Création des clés d'accès S3 d'un autre utilisateur".
   e. Dans l'onglet **groupes**, sélectionnez **Modifier les groupes** pour ajouter l'utilisateur à des groupes ou supprimer l'utilisateur des groupes. Sélectionnez ensuite **Enregistrer les modifications**.
7. Confirmez que vous avez sélectionné **Enregistrer les modifications** pour chaque section que vous avez modifiée.

Dupliquer l'utilisateur local

Vous pouvez dupliquer un utilisateur local pour créer un nouvel utilisateur plus rapidement.

> Si votre compte locataire dispose de l'autorisation **utiliser la connexion de fédération de grille** et que vous dupliquez un utilisateur de la grille source du locataire, l'utilisateur dupliqué sera cloné dans la grille de destination du locataire.

Étapes

1. Sélectionnez **ACCESS MANAGEMENT** > **Users**.
2. Cochez la case correspondant à l'utilisateur que vous souhaitez dupliquer.
3. Sélectionnez **actions** > **Dupliquer utilisateur**.
4. Voir Créer un utilisateur local pour plus de détails sur ce que vous devez saisir.
5. Sélectionnez **Créer utilisateur**.

Réessayez le clone utilisateur

Pour réessayer un clone qui a échoué :

1. Sélectionnez chaque utilisateur qui indique *(échec du clonage)* sous le nom d'utilisateur.
2. Sélectionnez **actions** > **Cloner les utilisateurs**.
3. Consultez l'état de l'opération de clonage sur la page de détails de chaque utilisateur que vous êtes en train de cloner.

Pour plus d'informations, voir "Cloner des groupes de locataires et des utilisateurs".

Supprimez un ou plusieurs utilisateurs locaux

Vous pouvez supprimer définitivement un ou plusieurs utilisateurs locaux qui n'ont plus besoin d'accéder au compte de locataire StorageGRID.

> Si votre compte de tenant dispose de l'autorisation **utiliser la connexion de fédération de grille** et que vous supprimez un utilisateur local, StorageGRID ne supprimera pas l'utilisateur correspondant sur l'autre grille. Si vous devez conserver ces informations synchronisées, vous devez supprimer le même utilisateur des deux grilles.

> Vous devez utiliser le référentiel d'identité fédéré pour supprimer des utilisateurs fédérés.

Étapes

1. Sélectionnez **ACCESS MANAGEMENT** > **Users**.
2. Cochez la case correspondant à chaque utilisateur à supprimer.
3. Sélectionnez **actions** > **Supprimer utilisateur** ou **actions** > **Supprimer utilisateurs**.

   Une boîte de dialogue de confirmation s'affiche.
4. Sélectionnez **Supprimer utilisateur** ou **Supprimer utilisateurs**.

Gestion des clés d'accès 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.

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 du compte root S3 et de 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.

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Gérez vos propres informations d'identification S3 ou autorisations d'accès racine".

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 besoin de définir une heure 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 **STORAGE (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.

     > La date d'expiration peut être au maximum de cinq ans à compter de la date actuelle. La durée d'expiration peut être d'au moins une minute à partir de l'heure actuelle.

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 de clés après la fermeture de la boîte de dialogue.

6. Sélectionnez **Terminer**.

La nouvelle clé apparaît sur la page Mes clés d'accès.

7. Si votre compte de locataire dispose de l'autorisation **utiliser la connexion de fédération grid**, vous pouvez utiliser l'API de gestion des locataires pour cloner manuellement les clés d'accès S3 du locataire de la grille source vers le locataire de la grille de destination. Voir "Cloner les clés d'accès S3 à l'aide de l'API".

Affichez vos clés d'accès S3

Si vous utilisez un locataire S3 et que vous disposez de la "autorisation appropriée", 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 les clés" que vous n'utilisez plus.

> 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.

Avant de commencer

- 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 les informations d'identification Manage Your Own S3 "permission".

Étapes

1. Sélectionnez **STORAGE (S3)** > **Mes clés d'accès**.
2. À partir de la page Mes clés d'accès, triez toutes les clés d'accès existantes par **heure d'expiration** ou **ID de clé d'accès**.
3. Au besoin, créez de nouvelles clés ou supprimez 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.

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.

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous avez le "Gérez vos propres identifiants 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 **STORAGE (S3)** > **Mes clés d'accès**.
2. Sur la page Mes clés d'accès, cochez la case correspondant à chaque clé d'accès que vous souhaitez supprimer.
3. Sélectionnez **Supprimer la touche**.
4. Dans la boîte de dialogue de confirmation, sélectionnez **touche Suppr**.

   Un message de confirmation s'affiche dans le coin supérieur droit de la page.

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.

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Autorisation d'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 besoin de définir une heure 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 pas définir de délai 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.

   > La date d'expiration peut être au maximum de cinq ans à compter de la date actuelle. La durée d'expiration peut être d'au moins une minute à partir de l'heure actuelle.

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 de 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.

8. Si votre compte de locataire dispose de l'autorisation **utiliser la connexion de fédération grid**, vous pouvez utiliser l'API de gestion des locataires pour cloner manuellement les clés d'accès S3 du locataire de la grille source vers le locataire de la grille de destination. Voir "Cloner les clés d'accès S3 à l'aide de l'API".

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.

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous avez le "Autorisation d'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**.
2. Sur la page utilisateurs, sélectionnez l'utilisateur dont vous souhaitez afficher les clés d'accès S3.
3. Dans la page Détails de l'utilisateur, 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.

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous avez le "Autorisation d'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**.
2. Sur la page utilisateurs, sélectionnez l'utilisateur dont vous souhaitez gérer les clés d'accès S3.
3. Sur la page Détails de l'utilisateur, sélectionnez **touches d'accès**, puis cochez la case correspondant à chaque clé d'accès que vous souhaitez supprimer.
4. Sélectionnez **actions** > **Supprimer la touche sélectionnée**.
5. Dans la boîte de dialogue de confirmation, sélectionnez **touche Suppr**.

Un message de confirmation s'affiche dans le coin supérieur droit de la page.

Gestion des compartiments S3

Créer un compartiment S3

Vous pouvez utiliser le Gestionnaire des locataires pour créer des compartiments S3 pour les données d'objet.

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs disposant de l'accès racine ou de la fonction gérer tous les compartiments "permission". Ces autorisations remplacent les paramètres d'autorisations des stratégies de groupes ou de compartiments.

> Les autorisations permettant de définir ou de modifier les propriétés S3 Object Lock des compartiments ou des objets peuvent être accordées par "politique de compartiment ou règle de groupe".

- Si vous prévoyez d'activer le verrouillage objet S3 pour un compartiment, un administrateur du grid a activé le paramètre de verrouillage objet S3 global pour le système StorageGRID. Vous avez également passé en revue les exigences relatives aux compartiments et aux objets S3 Object Lock.
- Si chaque locataire dispose de 5,000 compartiments, chaque nœud de stockage de la grille dispose d'au moins 64 Go de RAM.

> Chaque grille peut contenir un maximum de 100,000 compartiments.

Accéder à l'assistant

Étapes

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

Entrez les détails

Étapes

1. Entrez les détails du compartiment.

Champ	Description
Nom du compartiment	Nom du compartiment conforme 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 et 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 contenir de périodes dans les demandes de type hébergement virtuel. Les périodes provoquera des problèmes avec la vérification du certificat générique du serveur. Pour plus d'informations, voir "Documentation Amazon Web Services (AWS) sur les règles d'attribution de nom de compartiment". **Remarque** : vous ne pouvez pas modifier le nom du compartiment après avoir créé le compartiment.
Région	La région du godet. 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 la `us-east-1` région. **Remarque** : vous ne pouvez pas modifier la région après avoir créé le compartiment.

2. Sélectionnez **Continuer**.

Gérer les paramètres

Étapes

1. 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. Vous devez activer la gestion des versions d'objet si le compartiment est utilisé pour la réplication entre plusieurs grilles.

2. Si le paramètre global S3 Object Lock est activé, activez éventuellement S3 Object Lock pour que le compartiment stocke des objets à l'aide d'un modèle WORM (Write-once-read-many).

   Activez le verrouillage des objets S3 pour un compartiment uniquement si vous devez conserver les objets pendant une durée fixe, par exemple, pour répondre à certaines exigences réglementaires. Le verrouillage objet S3 est un paramètre permanent qui vous permet d'empêcher la suppression ou l'écrasement d'objets pendant une durée fixe ou indéfiniment.

Une fois le paramètre S3 Object Lock activé pour un compartiment, il ne peut pas être désactivé. Toute personne disposant des autorisations appropriées peut ajouter à ce compartiment des objets qui ne peuvent pas être modifiés. Il se peut que vous ne puissiez pas supprimer ces objets ou le compartiment lui-même.

Si vous activez le verrouillage des objets S3 pour un compartiment, le contrôle de version des compartiments est automatiquement activé.

3. Si vous avez sélectionné **Activer le verrouillage d'objet S3**, vous pouvez activer **rétention par défaut** pour ce compartiment.

   Votre administrateur de grille doit vous donner l'autorisation de "Utiliser les fonctionnalités spécifiques du verrouillage objet S3".

   Lorsque **Default Retention** est activé, les nouveaux objets ajoutés au compartiment sont automatiquement protégés contre la suppression ou l'écrasement. Le paramètre **rétention par défaut** ne s'applique pas aux objets qui ont leurs propres périodes de rétention.

   a. Si **Default Retention** est activé, spécifiez un **mode de rétention par défaut** pour le compartiment.

Mode de rétention par défaut	Description
La gouvernance	• Les utilisateurs disposant de l' `s3:BypassGovernanceRetention`autorisation peuvent utiliser l' `x-amz-bypass-governance-retention: true`en-tête de la demande pour contourner les paramètres de rétention. • Ces utilisateurs peuvent supprimer une version d'objet avant d'atteindre sa date de conservation jusqu'à. • Ces utilisateurs peuvent augmenter, diminuer ou supprimer la date de conservation d'un objet.
La conformité	• L'objet ne peut pas être supprimé tant que sa date de conservation jusqu'à n'est pas atteinte. • La date de conservation de l'objet peut être augmentée, mais elle ne peut pas être réduite. • La date de conservation de l'objet jusqu'à ne peut pas être supprimée tant que cette date n'est pas atteinte. **Remarque** : votre administrateur de grille doit vous permettre d'utiliser le mode de conformité.

   b. Si **Default Retention** est activé, spécifiez la **période de rétention par défaut** pour le compartiment.

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

Une période de rétention *maximum*, qui peut être de 1 jour à 100 ans, est définie lorsque l'administrateur de la grille crée le locataire. Lorsque vous définissez une période de rétention *default*, elle ne peut pas dépasser la valeur définie pour la période de rétention maximale. Si nécessaire, demandez à votre

administrateur de grille d'augmenter ou de réduire la période de rétention maximale.

4. en option, sélectionnez **Enable Capacity limit**.

   La limite de capacité est la capacité maximale disponible pour les objets de ce compartiment. 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 godet est illimitée. Pour plus d'informations, reportez-vous à la section "Utilisation limitée de la capacité" .

5. Sélectionnez **Créer un compartiment**.

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

6. Si vous le souhaitez, sélectionnez **aller à la page des détails du compartiment** pour "afficher les détails du compartiment"effectuer une configuration supplémentaire.

Afficher les détails du compartiment

Vous pouvez afficher les compartiments de votre compte de locataire.

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Accès racine, gestion de tous les compartiments ou autorisation Afficher tous les compartiments". Ces autorisations remplacent les paramètres d'autorisation dans les stratégies de groupe ou de compartiment.

Étapes

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

   La page compartiments s'affiche.

2. Consultez le tableau récapitulatif pour chaque compartiment.

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

   > Les valeurs nombre d'objets, espace utilisé et utilisation 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.

   Nom

   Nom unique du compartiment, qui ne peut pas être modifié.

   Fonctionnalités activées

   Liste des fonctions activées pour le compartiment.

   Verrouillage d'objet S3

   Indique si le verrouillage d'objet S3 est activé pour le compartiment.

   Cette colonne apparaît uniquement si le verrouillage objet S3 est activé pour la grille. Cette colonne affiche également des informations pour tous les compartiments conformes existants.

Région

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

Nombre d'objets

Nombre d'objets dans ce compartiment. Si la gestion des versions des compartiments est activée, les versions d'objets non actuelles sont incluses dans cette valeur.

Lorsque des objets sont ajoutés ou supprimés, il est possible que cette valeur ne soit pas mise à jour immédiatement.

Espace utilisé

Taille logique de tous les objets du 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.

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

Du stockage

Pourcentage utilisé de la limite de capacité du godet, si un pourcentage a été défini.

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 elle est définie) lorsqu'un locataire commence à télécharger des objets et rejette de nouvelles ingests dans ce compartiment si le locataire a dépassé la limite de capacité. Cependant, StorageGRID ne prend pas en compte la taille du téléchargement actuel lorsqu'il détermine si la limite de capacité a été dépassée. En cas de suppression d'objets, un locataire peut temporairement empêcher le chargement de nouveaux objets dans ce compartiment 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 au stockage des objets et de leurs métadonnées.

Capacité

S'il est défini, la limite de capacité du godet.

Date de création

Date et heure de création du compartiment. Cette colonne est masquée par défaut.

3. Pour afficher les détails d'un compartiment spécifique, sélectionnez le nom du compartiment dans le tableau.
   a. Affichez le récapitulatif en haut de la page Web pour confirmer les détails du compartiment, tels que le nombre de régions et d'objets.
   b. Afficher 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. Au besoin, sélectionnez **Supprimer les objets dans le compartiment** et **Supprimer le compartiment**.

Soyez attentif aux mises en garde qui apparaissent lorsque vous sélectionnez chacune de ces options. Pour plus d'informations, se reporter à :

- "Supprime tous les objets d'un compartiment"
- "Supprimer un compartiment" (le godet doit être vide)

d. Afficher ou modifier les paramètres du compartiment dans chacun des onglets, selon les besoins.

- **S3 Console** : permet d'afficher les objets du compartiment. Pour plus d'informations, reportez-vous "Utiliser la console S3"à .
- **Options de compartiment** : afficher ou modifier les paramètres des options. Certains paramètres, tels que S3 Object Lock, ne peuvent pas être modifiés après la création du compartiment.
  - "Gestion de la cohérence des compartiments"
  - "Mises à jour de l'heure du dernier accès"
  - "Limite de capacité"
  - "Gestion des versions d'objet"
  - "Verrouillage d'objet S3"
  - "Rétention de compartiments par défaut"
  - "Gérer la réplication entre les grilles" (si autorisé pour le locataire)
- **Platform services**: "Gestion des services de plateforme" (Si autorisé pour le locataire)
- **Accès au compartiment** : afficher ou modifier les paramètres des options. Vous devez disposer d'autorisations d'accès spécifiques.
  - Configurer "Partage de ressources interorigine (CORS)" pour que le compartiment et les objets du compartiment soient accessibles aux applications Web d'autres domaines.
  - "Contrôler l'accès des utilisateurs" Pour un compartiment S3 et les objets dans ce compartiment.

Applique une balise de règle ILM à un compartiment

Vous pouvez choisir une balise de règle ILM à appliquer à un compartiment en fonction de vos besoins en stockage objet.

La politique ILM contrôle l'emplacement du stockage des données objet et leur suppression au bout d'une période donnée. Votre administrateur du grid crée des règles ILM et les attribue aux balises de règles ILM lors de l'utilisation de plusieurs règles actives.

> Évitez de fréquemment réaffecter le tag de stratégie d'un compartiment. Sinon, des problèmes de performances risquent de se produire.

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Accès racine, gestion de tous les compartiments ou autorisation Afficher tous les compartiments". Ces autorisations remplacent les paramètres d'autorisation dans les stratégies de groupe ou de compartiment.

Étapes

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

   La page compartiments s'affiche. Si nécessaire, vous pouvez trier les informations par colonne, ou vous pouvez avancer et revenir à la liste.

2. Sélectionnez le nom du compartiment auquel vous souhaitez attribuer une balise de règle ILM.

Vous pouvez également modifier l'affectation de balises de stratégie ILM pour un compartiment auquel une balise est déjà attribuée.

> 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. Dans l'onglet Options de compartiment, développez la balise de stratégie ILM accordéon. 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 compartiment.

> La modification de la balise de règle ILM d'un compartiment déclenche la réévaluation des règles ILM de tous les objets du compartiment. Si la nouvelle règle conserve des objets pendant une durée limitée, les objets plus anciens seront supprimés.

5. Sélectionnez le bouton radio correspondant à l'étiquette que vous souhaitez affecter au compartiment.
6. Sélectionnez **Enregistrer les modifications**. Une nouvelle balise de compartiment S3 sera définie dans le compartiment avec la clé `NTAP-SG-ILM-BUCKET-TAG` et la valeur du nom de la balise de règle ILM.

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

> Définissez et modifiez les balises de règles ILM à l'aide uniquement du gestionnaire de locataires ou de l'API du gestionnaire de locataires sur lequel la balise de règle ILM est validée. Ne modifiez pas la `NTAP-SG-ILM-BUCKET-TAG` balise de stratégie ILM à l'aide de l'API S3 PutBucketTagging ou de l'API S3 DeleteBuckeTagging.

> La modification de la balise de règle attribuée à un compartiment a un impact temporaire sur les performances, tandis que la réévaluation des objets est effectuée à l'aide de la nouvelle règle ILM.

Gestion de la règle de compartiment

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

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Autorisation d'accès racine". Les autorisations Afficher tous les compartiments et gérer tous les compartiments permettent uniquement l'affichage.
- Vous avez vérifié que le nombre de nœuds de stockage et de sites requis est disponible. Si deux nœuds de stockage ou plus ne sont pas disponibles dans un site, ou si un site n'est pas disponible, les modifications apportées à ces paramètres risquent de ne pas être disponibles.

Étapes

1. Sélectionnez **godets**, puis sélectionnez le compartiment que vous souhaitez gérer.
2. Sur la page de détails du compartiment, sélectionnez **accès au compartiment** > **Stratégie de compartiment**.
3. Effectuez l'une des opérations suivantes :
   - Entrez une stratégie de compartiment en cochant la case **Enable policy**. Entrez ensuite une chaîne au format JSON valide.

     Chaque politique de compartiment a une taille limite de 20,480 octets.
   - Modifiez une règle existante en modifiant la chaîne.
   - Désactivez une stratégie en désélectionnant **Activer la stratégie**.

Pour plus d'informations sur les règles de compartiment, notamment la syntaxe du langage et des exemples, reportez-vous à la section "Exemples de politiques de compartiments".

Gestion de la cohérence des compartiments

Les valeurs de cohérence peuvent être utilisées pour spécifier la disponibilité des modifications des paramètres de compartiment, ainsi que pour fournir un équilibre entre la disponibilité des objets au sein d'un compartiment et la cohérence de ces objets entre plusieurs 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 client puissent répondre à leurs besoins opérationnels.

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Gérez tous les compartiments ou l'autorisation d'accès racine". Ces autorisations remplacent les paramètres d'autorisations des stratégies de groupes ou de compartiments.

Instructions de cohérence des compartiments

La cohérence des compartiments détermine la cohérence des applications client qui affectent les objets au sein de ce compartiment S3. En général, vous devez utiliser la cohérence **Read-After-New-write** pour vos compartiments.

modifiez la cohérence des compartiments

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

> Lorsque vous modifiez la cohérence d'un compartiment, seuls les objets ingérés après la modification sont garantis pour respecter le paramètre révisé.

Étapes

1. Sélectionnez **Afficher les compartiments** dans le tableau de bord ou sélectionnez **STOCKAGE (S3)** > **compartiments**.
2. Sélectionnez le nom du compartiment dans la table.

La page des détails du compartiment s'affiche.

3. Dans l'onglet **Bucket options**, sélectionnez ** accordéon.
4. Sélectionnez une 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**.

Que se passe-t-il lorsque vous modifiez les paramètres de compartiment

Les compartiments ont plusieurs paramètres qui affectent le comportement des compartiments et des objets dans ces compartiments.

Les paramètres de compartiment suivants utilisent la cohérence **strong** par défaut. Si au moins deux nœuds de stockage ne sont disponibles dans aucun site, ou si un site n'est pas disponible, toute modification de ces paramètres peut ne pas être disponible.

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

> La valeur de cohérence pour la gestion des versions des compartiments, le verrouillage objet S3 et le chiffrement des compartiments ne peut pas être définie sur une valeur qui n'est pas parfaitement cohérente.

Les paramètres de compartiment suivants n'utilisent pas une cohérence élevée et offrent une plus grande disponibilité en cas de modification. Les modifications apportées à ces paramètres peuvent prendre un certain temps avant d'avoir un effet.

- "Configuration des services de plate-forme : intégration de notification, réplication ou recherche"
- "Configuration DE L'INFRASTRUCTURE CORS"

- Modifier la cohérence du compartiment

> Si la cohérence par défaut utilisée lors de la modification des paramètres de compartiment ne répond pas aux exigences de l'application client, vous pouvez modifier la cohérence à l'`Consistency-Control` aide de l'en-tête de "L'API REST S3"ou en utilisant les `reducedConsistency` options ou de `force`"API de gestion des locataires" .

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 **Last Access Time** 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 gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Gérez tous les compartiments ou l'autorisation d'accès racine". Ces autorisations remplacent les paramètres d'autorisations des stratégies de groupes ou de compartiments.

Description de la tâche

Last Access Time est l'une des options disponibles pour l'instruction de placement **Reference Time** 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 du moment où ces objets ont été récupérés (lus ou affichés) pour la dernière fois.

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.

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 **Last Access Time** 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
Demande de liste d'objets ou de versions d'objets	Non	Non	Non	Non
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 **Afficher les compartiments** dans le tableau de bord ou sélectionnez **STOCKAGE (S3)** > **compartiments**.
2. Sélectionnez le nom du compartiment dans la table.

   La page des détails du compartiment s'affiche.

3. Dans l'onglet **Bucket options**, sélectionnez l'accordéon **Last Access Time Updates**.
4. Activer ou désactiver les mises à jour des heures du dernier accès.
5. Sélectionnez **Enregistrer les modifications**.

Modifiez le contrôle de version d'objet pour un compartiment

Si vous utilisez un locataire S3, vous pouvez modifier l'état de gestion des versions des compartiments S3.

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Gérez tous les compartiments ou l'autorisation d'accès racine". Ces autorisations remplacent les paramètres d'autorisations des stratégies de groupes ou de compartiments.
- Vous avez vérifié que le nombre de nœuds de stockage et de sites requis est disponible. Si deux nœuds de stockage ou plus ne sont pas disponibles dans un site, ou si un site n'est pas disponible, les modifications apportées à ces paramètres risquent de ne pas être disponibles.

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 pour un compartiment, il 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

Pour plus d'informations, reportez-vous aux sections suivantes :

- "Gestion des versions d'objet"
- "Règles et règles ILM pour les objets avec version S3 (exemple 4)"
- "Comment supprimer les objets"

Étapes

1. Sélectionnez **Afficher les compartiments** dans le tableau de bord ou sélectionnez **STOCKAGE (S3)** > **compartiments**.
2. Sélectionnez le nom du compartiment dans la table.

   La page des détails du compartiment s'affiche.

3. Dans l'onglet **Bucket options**, sélectionnez l'accordéon **Object multiversion**.
4. Sélectionnez un état de gestion des versions pour les objets de ce compartiment.

   La gestion des versions d'objet doit rester activée pour un compartiment utilisé pour la réplication entre plusieurs grilles. 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**.

Utilisez le verrouillage d'objet S3 pour conserver les objets

Vous pouvez utiliser le verrouillage objet S3 si les compartiments et les objets doivent respecter les exigences réglementaires en matière de conservation des données.

> Votre administrateur de grille doit vous donner l'autorisation d'utiliser des fonctions spécifiques de verrouillage d'objet S3.

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).

Lorsque le paramètre de verrouillage objet S3 global est activé pour un système StorageGRID, un compte de locataire S3 peut créer des compartiments avec ou sans verrouillage objet S3 activé. Si le verrouillage objet S3 est activé pour un compartiment, la gestion des versions de compartiment est requise et elle est automatiquement activée.

Un compartiment sans S3 Object Lock ne peut contenir que des objets sans paramètres de rétention spécifiés. Aucun objet ingéré ne possède de paramètres de conservation.

Un compartiment avec S3 Object Lock peut contenir des objets avec et sans paramètres de conservation spécifiés par les applications client S3. Certains objets ingérés auront des paramètres de conservation.

Un compartiment avec le verrouillage d'objet S3 et la rétention par défaut configurés peut avoir téléchargé des objets 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 conservation lorsque la conservation par défaut est configurée. Les objets existants sans paramètres de conservation d'objet ne sont pas affectés.

Modes de rétention

La fonction 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 conservation Amazon S3.

- En mode conformité :
  - L'objet ne peut pas être supprimé tant que sa date de conservation jusqu'à n'est pas atteinte.
  - La date de conservation de l'objet peut être augmentée, mais elle ne peut pas être réduite.
  - La date de conservation de l'objet jusqu'à 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 d'atteindre sa date de conservation jusqu'à.
  - 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 objet S3 activé, les utilisateurs peuvent utiliser l'application client S3 pour spécifier éventuellement les paramètres de conservation suivants pour chaque objet ajouté au compartiment :

- **Mode de conservation** : conformité ou gouvernance.
- **Conserver-jusqu'à-date**: Si la date de conservation d'une version d'objet est dans le futur, l'objet peut être récupéré, mais il ne peut pas être supprimé.
- **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.

  > Si un objet fait l'objet d'une conservation légale, personne ne peut le supprimer, quel que soit son mode de conservation.

  Pour plus de détails sur les paramètres de l'objet, reportez-vous à la section "Utilisez l'API REST S3 pour configurer le verrouillage objet S3".

Paramètre de rétention par défaut pour les compartiments

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

- **Mode de rétention par défaut** : conformité ou gouvernance.
- **Période de rétention par défaut** : durée pendant laquelle les nouvelles versions d'objets ajoutées à ce compartiment doivent être conservées, à partir du jour où elles sont ajoutées.

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 compartiment S3" et "Mettre à jour la conservation par défaut du verrouillage d'objet S3".

Tâches de verrouillage d'objet S3

Les listes suivantes destinées aux administrateurs du grid et aux utilisateurs de locataires contiennent des tâches de haut niveau relatives à l'utilisation de la fonction S3 Object Lock.

Administrateur du grid

- 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 des informations (ILM) sont *conformes*; c'est-à"Exigences des compartiments avec le verrouillage objet S3 activé"-dire qu'elles respectent le .
- Si nécessaire, autorisez un locataire à utiliser le mode de conservation Compliance. Sinon, seul le mode gouvernance est autorisé.
- Si nécessaire, définissez une période de conservation maximale pour un locataire.

Utilisateur locataire

- Considérations relatives aux compartiments et aux objets avec le verrouillage d'objet S3
- Si nécessaire, contactez l'administrateur de la grille pour activer le paramètre global S3 Object Lock et définir les autorisations.
- Créez des compartiments avec le verrouillage d'objet S3 activé.
- Vous pouvez également configurer les paramètres de conservation par défaut d'un compartiment :
  - Mode de conservation par défaut : gouvernance ou conformité, si l'administrateur du grid l'autorise.
  - Période de conservation par défaut : doit être inférieure ou égale à la période de conservation maximale définie par l'administrateur du grid.
- Utilisez l'application client S3 pour ajouter des objets et définir éventuellement la conservation propre à l'objet :
  - Mode de rétention. Gouvernance ou conformité, si l'administrateur du grid l'autorise.
  - Conserver la date de fin : doit être inférieur ou égal à ce qui est autorisé par la période de conservation maximale définie par l'administrateur de la grille.

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.
- 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 objet S3 pour un compartiment existant.
- Lorsque le verrouillage d'objet S3 est activé pour un compartiment, StorageGRID active automatiquement le contrôle de version pour ce compartiment. Vous ne pouvez pas désactiver le verrouillage objet S3 ou suspendre la gestion des versions pour le compartiment.
- Vous pouvez également spécifier un mode de conservation et une période de conservation par défaut pour chaque compartiment à l'aide du gestionnaire des locataires, de l'API de gestion des locataires ou de l'API REST S3. Les paramètres de conservation par défaut du compartiment s'appliquent uniquement aux nouveaux objets ajoutés au compartiment 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 jusqu'à pour chaque version d'objet lors du téléchargement.
- La configuration du cycle de vie des compartiments est prise en charge pour les compartiments avec le verrouillage objet S3 activé.

- 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 une version d'objet, vous pouvez spécifier les paramètres de conservation par défaut du compartiment ou les paramètres de conservation pour chaque version d'objet. Les paramètres de conservation au niveau objet peuvent être spécifiés à l'aide de l'application client 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 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 lorsque le verrouillage objet S3 est activé passe par les étapes suivantes :

1. **Entrée d'objet**

   Lors de l'ajout d'une version d'objet à un compartiment pour lequel S3 Object Lock est activé, les paramètres de conservation sont appliqués comme suit :

   - Si des paramètres de rétention sont spécifiés pour l'objet, les paramètres de niveau objet sont appliqués. Tous les paramètres de compartiment 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 le verrouillage objet S3.

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

2. **Conservation et suppression d'objets**

   StorageGRID stocke plusieurs copies de chaque objet protégé pendant la période de conservation spécifiée. Le nombre et le type exacts de copies d'objet et d'emplacements de stockage sont déterminés par les règles de conformité dans les politiques ILM actives. La possibilité de supprimer un objet protégé avant d'atteindre sa date de conservation jusqu'à dépend de son mode de conservation.

   - Si un objet fait l'objet d'une conservation légale, personne ne peut le supprimer, quel que soit son mode de conservation.

Est-il toujours possible de gérer des compartiments existants conformes ?

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 obtenir des instructions, reportez-vous à la section "Base de connaissances NetApp : comment gérer des compartiments conformes aux ancienne génération dans StorageGRID 11.5".

Mettre à jour la conservation par défaut du verrouillage d'objet S3

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

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Gérez tous les compartiments ou l'autorisation d'accès racine". Ces autorisations remplacent les paramètres d'autorisations des stratégies de groupes ou de compartiments.
- 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 compartiment. Voir "Utilisez le verrouillage d'objet S3 pour conserver les objets".

Étapes

1. Sélectionnez **Afficher les compartiments** dans le tableau de bord ou sélectionnez **STOCKAGE (S3)** > **compartiments**.
2. Sélectionnez le nom du compartiment dans la table.

   La page des détails du compartiment s'affiche.

3. Dans l'onglet **Bucket options**, sélectionnez l'accordéon **S3 Object Lock**.
4. En option, activez ou désactivez **rétention par défaut** pour ce compartiment.

   Les modifications de ce paramètre ne s'appliquent pas aux objets qui se trouvent déjà dans le compartiment ni aux objets qui peuvent avoir leurs propres périodes de conservation.

5. Si **Default Retention** est activé, spécifiez un **mode de rétention par défaut** pour le compartiment.

Mode de rétention par défaut	Description
La gouvernance	• Les utilisateurs disposant de l' `s3:BypassGovernanceRetention`autorisation peuvent utiliser l' `x-amz-bypass-governance-retention: true`en-tête de la demande pour contourner les paramètres de rétention. • Ces utilisateurs peuvent supprimer une version d'objet avant d'atteindre sa date de conservation jusqu'à. • Ces utilisateurs peuvent augmenter, diminuer ou supprimer la date de conservation d'un objet.

Mode de rétention par défaut	Description
La conformité	• L'objet ne peut pas être supprimé tant que sa date de conservation jusqu'à n'est pas atteinte. • La date de conservation de l'objet peut être augmentée, mais elle ne peut pas être réduite. • La date de conservation de l'objet jusqu'à ne peut pas être supprimée tant que cette date n'est pas atteinte. **Remarque** : votre administrateur de grille doit vous permettre d'utiliser le mode de conformité.

6. Si **Default Retention** est activé, spécifiez la **période de rétention par défaut** pour le compartiment.

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

   Une période de rétention *maximum*, qui peut être de 1 jour à 100 ans, est définie lorsque l'administrateur de la grille crée le locataire. Lorsque vous définissez une période de rétention *default*, elle ne peut pas dépasser la valeur définie pour la période de rétention maximale. Si nécessaire, demandez à votre administrateur de grille d'augmenter ou de réduire la période de rétention maximale.

7. Sélectionnez **Enregistrer les modifications**.

Configurer le partage de ressources inter-sources (CORS)

Vous pouvez configurer le partage de ressources entre sources (CORS) pour un compartiment S3 si vous souhaitez que ce compartiment et ces objets soient accessibles aux applications web d'autres domaines.

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires 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 a le "Autorisation gérer tous les compartiments ou Afficher tous les compartiments". Ces autorisations remplacent les paramètres d'autorisations des stratégies de groupes ou de compartiments.
- Pour les demandes de configuration PUT CORS, vous appartenez à un groupe d'utilisateurs qui a le "Autorisations de gestion de tous les compartiments". Cette autorisation remplace les paramètres d'autorisations dans les stratégies de groupe ou de compartiment.
- Le "Autorisation d'accès racine" permet d'accéder à toutes les demandes de configuration CORS.

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 le `Images` compartiment, vous pouvez autoriser l'affichage des images de ce compartiment sur le site Web `http://www.example.com`.

Activer le CORS pour un godet

Étapes

1. Utilisez un éditeur de texte pour créer le fichier XML requis. Cet exemple montre le code XML utilisé pour activer le code commande pour un compartiment S3. Détails :
   - Permet à n'importe quel domaine d'envoyer des requêtes GET au compartiment
   - Autorise uniquement le `http://www.example.com` domaine à envoyer des requêtes GET, POST et DELETE
   - 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, reportez-vous àla section "Documentation Amazon Web Services (AWS) : guide de l'utilisateur d'Amazon simple Storage Service".

2. Sélectionnez **Afficher les compartiments** dans le tableau de bord ou sélectionnez **STOCKAGE (S3)** > **compartiments**.
3. Sélectionnez le nom du compartiment dans la table.

   La page des détails du compartiment s'affiche.

4. Dans l'onglet **Bucket Access**, sélectionnez l'accordéon **Cross-Origin Resource Sharing (CORS)**.
5. Cochez la case **Activer CORS**.
6. Collez le fichier 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**.

Supprime les objets du compartiment

Vous pouvez utiliser le Gestionnaire de locataires pour supprimer les objets d'une ou de plusieurs compartiments.

Considérations et exigences

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

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

> Un compartiment qui utilise le verrouillage d'objet S3 restera à 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 mises en suspens légales soient supprimées.

- Pendant la suppression des objets, l'état du compartiment est **Suppression d'objets : lecture seule**. Dans cet état, vous ne pouvez pas ajouter de nouveaux objets au compartiment.
- Une fois tous les objets supprimés, le compartiment reste à l'état en lecture seule. Vous pouvez effectuer l'une des opérations suivantes :
  - Ramener le compartiment en mode écriture et le réutiliser pour de nouveaux objets
  - Supprimez le compartiment
  - Conservez le compartiment en mode lecture seule pour réserver son nom pour une utilisation ultérieure
- Si la gestion des versions d'objet est activée dans un compartiment, les marqueurs de suppression créés dans StorageGRID 11.8 ou version ultérieure peuvent être supprimés à l'aide des opérations de suppression d'objets dans un compartiment.
- Si la gestion des versions d'objet est activée dans un compartiment, l'opération de suppression d'objets ne supprime pas les marqueurs de suppression créés dans StorageGRID 11.7 ou une version antérieure. Voir les informations sur la suppression d'objets dans un compartiment dans "Suppression d'objets avec version S3".
- Si vous utilisez "réplication entre plusieurs grilles", notez ce qui suit :
  - L'utilisation de cette option ne supprime aucun objet du compartiment de l'autre grille.
  - Si vous sélectionnez cette option pour le compartiment source, l'alerte **échec de réplication multigrille** est déclenchée si vous ajoutez des objets au compartiment de destination sur l'autre grille. Si vous ne pouvez pas garantir que personne n'ajoute d'objets au compartiment de l'autre grille avant de supprimer tous les objets "désactiver la réplication entre les grilles"du compartiment.

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Autorisation d'accès racine". Cette autorisation remplace les paramètres d'autorisations dans les stratégies de groupe ou de compartiment.

Étapes

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

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

2. Utilisez le menu **actions** ou la page de détails pour un compartiment spécifique.

   Menu actions

   a. Cochez la case correspondant à chaque compartiment dans lequel vous souhaitez supprimer des objets.

   b. Sélectionnez **actions** > **Supprimer les objets dans le compartiment**.

   Page de détails

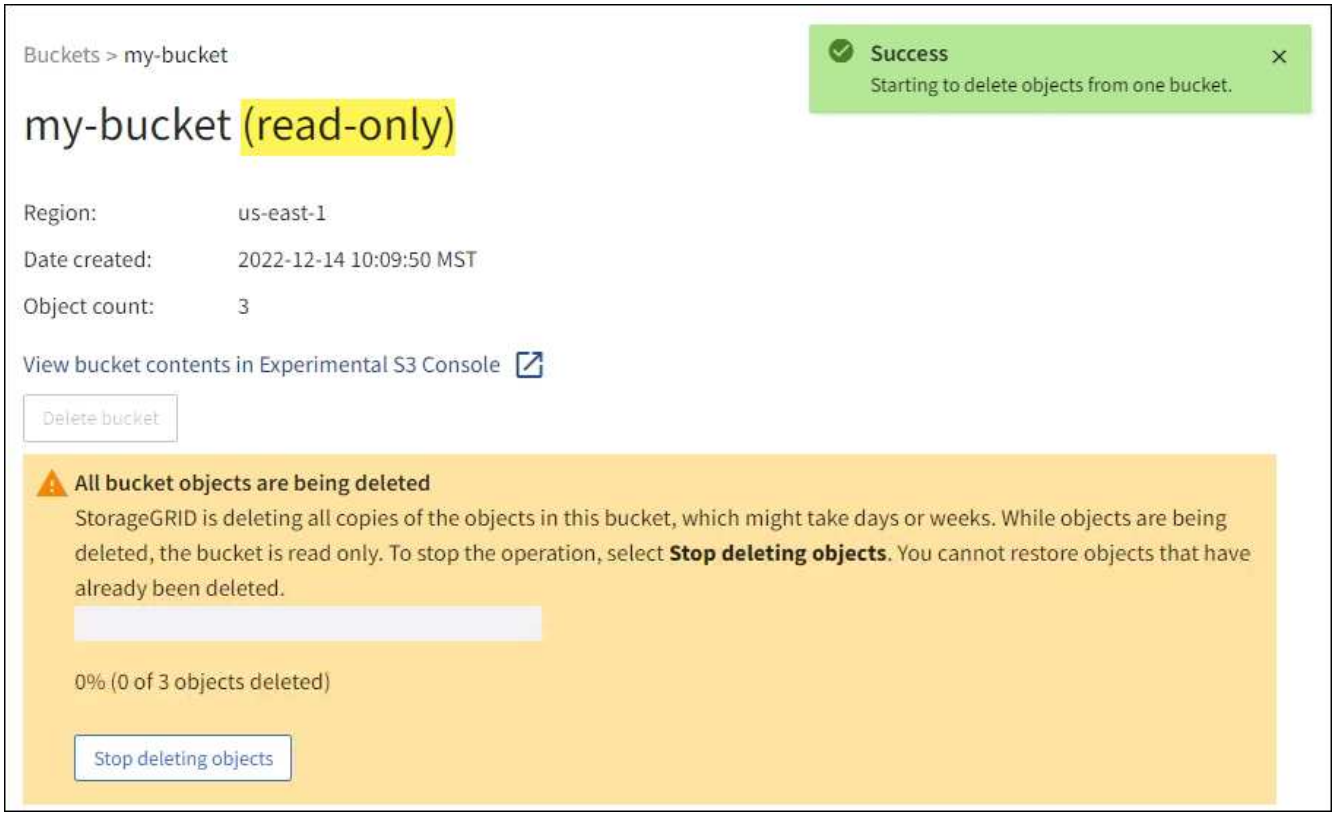
   a. Sélectionnez un nom de compartiment pour afficher ses détails.

   b. Sélectionnez **Supprimer les objets dans le compartiment**.

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.

   Au bout de quelques minutes :

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

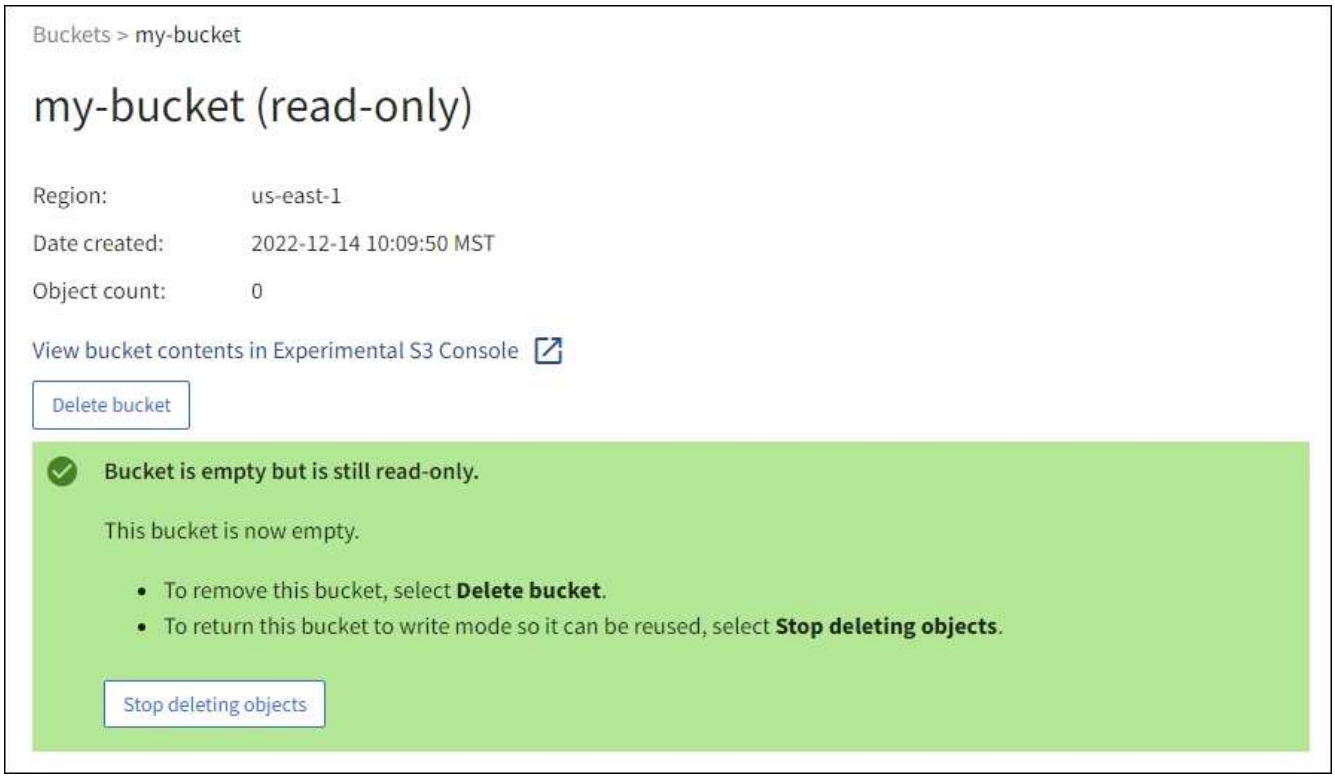


5. Si nécessaire pendant l'exécution de l'opération, sélectionnez **Arrêter la suppression d'objets** pour arrêter le processus. Sélectionnez ensuite **Supprimer les objets dans le compartiment** pour reprendre le processus.

   Lorsque vous sélectionnez **Arrêter la suppression d'objets**, le compartiment est remis en mode écriture ; cependant, vous ne pouvez pas accéder aux objets qui ont été supprimés ni les restaurer.

6. Attendez la fin de l'opération.

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



7. Effectuez l'une des opérations suivantes :
   - Quittez la page pour garder le compartiment en mode lecture seule. Par exemple, vous pouvez conserver un compartiment vide en mode lecture seule afin de réserver le nom du compartiment pour une utilisation ultérieure.
   - Supprimer le compartiment. Vous pouvez sélectionner **Supprimer un compartiment** pour supprimer un seul compartiment ou retourner à la page compartiments et sélectionner **actions** > **Supprimer** compartiments pour supprimer plusieurs compartiments.

     Si vous ne pouvez pas supprimer un compartiment multiversion après la suppression de tous les objets, les marqueurs de suppression peuvent rester. Pour supprimer le godet, vous devez supprimer tous les marqueurs de suppression restants.

   - Ramenez le compartiment en mode écriture et réutilisez-le éventuellement pour de nouveaux objets. Vous pouvez sélectionner **Arrêter la suppression d'objets** pour un seul compartiment ou revenir à la page compartiments et sélectionner **action** > **Arrêter la suppression d'objets** pour plusieurs compartiments.

Supprimez le compartiment S3

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

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Gérez tous les compartiments ou l'autorisation d'accès racine". Ces autorisations remplacent les paramètres d'autorisations des stratégies de groupes ou de compartiments.
- Les compartiments à supprimer sont vides. Si les rubriques que vous souhaitez supprimer sont *not* vides,

"supprimez des objets du compartiment".

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 de "API de gestion des locataires""L'API REST S3"la ou de la .

Vous ne pouvez pas supprimer un compartiment S3 s'il contient des objets, des versions d'objets non actuelles ou des marqueurs de suppression. Pour plus d'informations sur la suppression des objets avec version S3, reportez-vous à la section "Comment supprimer les objets".

Étapes

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

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

2. Utilisez le menu **actions** ou la page de détails pour un compartiment spécifique.

   Menu actions

   a. Cochez la case correspondant à chaque compartiment à supprimer.

   b. Sélectionnez **actions** > **Supprimer des compartiments**.

   Page de détails

   a. Sélectionnez un nom de compartiment pour afficher ses détails.

   b. Sélectionnez **Supprimer le compartiment**.

3. Lorsque la boîte de dialogue de confirmation s'affiche, sélectionnez **Oui**.

   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 "supprimez tous les objets et tous les marqueurs de suppression dans le compartiment" avant de pouvoir supprimer le compartiment.

Utiliser la console S3

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

Avec la console S3, vous pouvez :

- Télécharger, télécharger, renommer, copier, déplacer, et supprimer des objets
- Affichez, restaurez, téléchargez et supprimez des versions d'objet
- Recherche d'objets par préfixe
- Gérer les balises d'objet
- Afficher les métadonnées d'objet
- Afficher, créer, renommer, copier, déplacer, et supprimez des dossiers

La console S3 améliore l'expérience utilisateur dans les cas les plus courants. Elle n'a pas été conçue pour remplacer les opérations de l'interface de ligne de commande ou de l'API dans tous les cas.

Si les opérations sont trop longues avec la console S3 (en minutes ou en heures, par exemple), tenez compte des points suivants :

- Réduction du nombre d'objets sélectionnés
- Accédez à vos données à l'aide de méthodes non graphiques (API ou interface de ligne de commande)

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires 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 racine. Vous pouvez également appartenir à un groupe d'utilisateurs disposant de l'autorisation utiliser l'onglet de la console S3 et de l'autorisation Afficher tous les compartiments ou gérer tous les compartiments. Voir "Autorisations de gestion des locataires".
- Une règle de groupe S3 ou de compartiment a été configurée pour l'utilisateur. Voir "Utilisez les règles d'accès au compartiment et au groupe".
- Vous connaissez l'ID de clé d'accès de l'utilisateur et la clé d'accès secrète. Vous disposez éventuellement d'un `.csv` fichier contenant ces informations. Voir la "instructions pour la création de clés d'accès".

Étapes

1. Sélectionnez **STORAGE** > **Buckets** > ***bucket name***.
2. Sélectionnez l'onglet S3 Console.
3. Collez l'ID de clé d'accès et la clé d'accès secrète dans les champs. Sinon, sélectionnez **Télécharger les clés d'accès** et sélectionnez votre `.csv` fichier.
4. Sélectionnez **connexion**.
5. Le tableau des objets de compartiment s'affiche. Vous pouvez gérer les objets selon vos besoins.

Informations supplémentaires

- **Recherche par préfixe** : la fonction de recherche par préfixe recherche uniquement les objets commençant par un mot spécifique par rapport au dossier en cours. La recherche n'inclut pas les objets qui contiennent le mot ailleurs. Cette règle s'applique également aux objets dans les dossiers. Par exemple, une recherche de `folder1/folder2/somefile-` renvoie des objets se trouvant dans le `folder1/folder2/` dossier et commence par le mot `somefile-`.
- **Glisser-déposer** : vous pouvez faire glisser et 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 la gestion des versions de compartiment est désactivée** : lorsque vous écrasez ou supprimez un objet dans un compartiment avec la gestion des versions désactivée, l'opération est permanente. Voir "Modifiez le contrôle de version d'objet pour un compartiment".

Gérez les services de la plateforme S3

Services de plateforme S3

Présentation et éléments à prendre en compte pour les services de plateforme

Avant d'implémenter les services de plateforme, examinez la présentation et les considérations relatives à l'utilisation de ces services.

Pour plus d'informations sur S3, reportez-vous à "UTILISEZ L'API REST S3"la section .

Présentation des services de plateforme

Les services de plateforme StorageGRID vous aident à mettre en œuvre une stratégie de cloud hybride en vous permettant d'envoyer des notifications d'événements et des copies d'objets S3 et de métadonnées d'objet à des destinations externes.

L'emplacement cible des services de plateforme étant généralement externe à votre déploiement StorageGRID, les services de plateforme vous offrent la puissance et la flexibilité offertes par l'utilisation de ressources de stockage externes, de services de notification et de services de recherche ou d'analyse pour vos données.

Toute combinaison de services de plateforme peut être configurée pour un seul compartiment S3. Par exemple, vous pouvez configurer à la fois le "Service CloudMirror" et le "notifications" dans un compartiment StorageGRID S3 afin de mettre en miroir des objets spécifiques vers Amazon simple Storage Service (S3), tout en envoyant une notification sur chacun de ces objets à une application de surveillance tierce pour vous aider à suivre vos dépenses AWS.

L'utilisation des services de la plateforme doit être activée pour chaque compte de locataire par un administrateur StorageGRID à l'aide de Grid Manager ou de l'API de gestion du grid.

Configuration des services de plate-forme

Les services de plate-forme communiquent avec les noeuds finaux externes que vous configurez à l'aide du "Gestionnaire de locataires"ou du "API de gestion des locataires". Chaque terminal représente une destination externe, par exemple un compartiment StorageGRID S3, un compartiment Amazon Web Services, une rubrique Amazon SNS ou un cluster Elasticsearch hébergé localement, sur AWS ou ailleurs.

Après avoir créé un noeud final externe, vous pouvez activer un service de plate-forme pour un compartiment en ajoutant une configuration XML au compartiment. La configuration XML identifie les objets sur lesquels le compartiment doit agir, l'action que le compartiment doit effectuer et le point de terminaison que le compartiment doit utiliser pour le service.

Vous devez ajouter des configurations XML distinctes pour chaque service de plate-forme que vous souhaitez configurer. Par exemple :

- Si vous souhaitez que tous les objets dont les clés commencent par `/images` soient répliqués sur un compartiment Amazon S3, vous devez ajouter une configuration de réplication au compartiment source.
- Si vous souhaitez également envoyer des notifications lorsque ces objets sont stockés dans le compartiment, vous devez ajouter une configuration de notifications.
- Si vous souhaitez indexer les métadonnées de ces objets, vous devez ajouter la configuration de notification des métadonnées utilisée pour implémenter l'intégration de la recherche.

Le format du XML de configuration est régi par les API REST S3 utilisées pour mettre en œuvre les services de plateforme StorageGRID :

Service de plateforme	L'API REST S3	Reportez-vous à la section
Réplication CloudMirror	• GetBuckeReplication • PutBuckeReplication	• "Réplication CloudMirror" • "Opérations sur les compartiments"
Notifications	• GetBucketNotifationConfiguration • PutBucketNotifationConfiguration	• "Notifications" • "Opérations sur les compartiments"
Intégration de la recherche	• CONFIGURATION DES notifications de métadonnées de compartiment • CONFIGURATION de notification des métadonnées de compartiment	• "Intégration de la recherche" • "Opérations personnalisées StorageGRID"

Considérations relatives à l'utilisation des services de plate-forme

Réflexion	Détails
Surveillance des terminaux de destination	Vous devez surveiller la disponibilité de chaque point final de destination. Si la connexion au point final de destination est perdue pendant une période prolongée et qu'il existe un important retard de requêtes, les demandes client supplémentaires (telles QUE LES requêtes ENVOYÉES) à StorageGRID échoueront. Vous devez réessayer ces demandes ayant échoué lorsque le noeud final devient accessible.
Limitation du terminal de destination	Le logiciel StorageGRID peut canaliser les demandes S3 entrantes pour un compartiment si le taux d'envoi des demandes dépasse le taux à partir duquel le terminal de destination peut recevoir les demandes. La restriction ne se produit que lorsqu'il existe un arriéré de demandes en attente d'envoi vers le noeud final de destination. Le seul effet visible est que les requêtes S3 entrantes prennent plus de temps à s'exécuter. Si vous commencez à détecter les performances beaucoup plus lentes, vous devez réduire le taux d'entrée ou utiliser un terminal avec une capacité plus élevée. Si l'carnet de commandes des requêtes continue d'augmenter, les opérations S3 des clients (par EXEMPLE, LES requêtes PUT) finiront par échouer. Les demandes CloudMirror sont plus susceptibles d'être affectées par les performances du terminal de destination, car ces demandes impliquent généralement plus de transfert de données que les demandes d'intégration de recherche ou de notification d'événements.

Réflexion	Détails
Garanties de commande	StorageGRID garantit l'ordre des opérations sur un objet d'un site. Tant que toutes les opérations relatives à un objet se trouvent sur le même site, l'état final de l'objet (pour la réplication) sera toujours égal à l'état dans StorageGRID. StorageGRID tente également de commander des demandes lorsque des opérations sont effectuées sur des sites StorageGRID. Par exemple, si vous écrivez un objet initialement sur le site A, puis que vous le remplacez par un autre objet au niveau du site B, le dernier objet répliqué par CloudMirror vers le compartiment de destination n'est pas garanti que ce nouvel objet soit.
Suppressions d'objets basées sur des règles ILM	Pour correspondre au comportement de suppression des CRR AWS et Amazon simple notification Service, les requêtes CloudMirror et de notification d'événement ne sont pas envoyées lorsqu'un objet du compartiment source est supprimé en raison des règles ILM de StorageGRID. Par exemple, aucune demande de notification de CloudMirror ou d'événement n'est envoyée si une règle ILM supprime un objet au bout de 14 jours. Au contraire, les demandes d'intégration de la recherche sont envoyées lorsque les objets sont supprimés du fait de ILM.
À l'aide des terminaux Kafka	Pour les terminaux Kafka, le protocole TLS mutuel n'est pas pris en charge. Par conséquent, si vous avez `ssl.client.auth` défini sur `required` dans la configuration de votre courtier Kafka, cela peut entraîner des problèmes de configuration du terminal Kafka. L'authentification des terminaux Kafka utilise les types d'authentification suivants. Ces types sont différents de ceux utilisés pour l'authentification d'autres terminaux, tels qu'Amazon SNS, et nécessitent des informations d'identification de nom d'utilisateur et de mot de passe. • SASL/SIMPLE • SASL/SCRAM-SHA-256 • SASL/SCRAM-SHA-512 **Remarque :** les paramètres du proxy de stockage configuré ne s'appliquent pas aux noeuds finaux des services de la plateforme Kafka.

Considérations relatives à l'utilisation du service de réplication CloudMirror

Réflexion	Détails
État de la réplication	StorageGRID ne prend pas en charge la `x-amz-replication-status` barre de coupe.

Réflexion	Détails
Taille de l'objet	La taille maximale des objets qui peuvent être répliqués dans un compartiment de destination par le service de réplication CloudMirror est de 5 Tio, soit la même que la taille maximale de l'objet *pris en charge*. **Remarque** : la taille *recommandée* maximale pour une opération PutObject unique est de 5 Gio (5,368,709,120 octets). Si vos objets sont supérieurs à 5 Gio, utilisez le téléchargement partitionné.
Gestion des versions du compartiment et ID de version	Si le compartiment S3 source de StorageGRID est activé pour la gestion des versions, vous devez également activer la gestion des versions pour le compartiment de destination. Lors de l'utilisation du contrôle de version, notez que l'ordre des versions d'objet dans le compartiment de destination est meilleur effort et n'est pas garanti par le service CloudMirror, en raison des limites du protocole S3. **Remarque** : les ID de version du compartiment source dans StorageGRID ne sont pas liés aux ID de version du compartiment de destination.
Balisage des versions d'objets	Le service CloudMirror ne réplique pas les requêtes PutObjectTagging ou DeleteObjectTagging qui fournissent un ID de version, en raison des limitations du protocole S3. Étant donné que les ID de version de la source et de la destination ne sont pas liés, il n'est pas possible de s'assurer qu'une mise à jour de balise vers un ID de version spécifique sera répliquée. En revanche, le service CloudMirror réplique les requêtes PutObjectTagging ou DeleteObjectTagging qui ne spécifient pas d'ID de version. Ces demandes mettent à jour les balises pour la clé la plus récente (ou la dernière version si le compartiment est versionné). Les ings normaux avec des étiquettes (et non les mises à jour de marquage) sont également répliqués.
Téléchargements partitionnés et `ETag` valeurs	Lors de la mise en miroir d'objets qui ont été téléchargés à l'aide d'un téléchargement partitionné, le service CloudMirror ne conserve pas les pièces. Par conséquent, la `ETag` valeur de l'objet symétrique sera différente de celle `ETag` de l'objet d'origine.
Chiffrement des objets avec SSE-C (chiffrement côté serveur avec clés fournies par le client)	Le service CloudMirror ne prend pas en charge les objets cryptés avec SSE-C. si vous essayez d'ingérer un objet dans le compartiment source pour la réplication CloudMirror et que la demande inclut les en-têtes de requête SSE-C, l'opération échoue.
Compartiment avec verrouillage objet S3 activé	La réplication n'est pas prise en charge pour les compartiments source ou de destination lorsque le verrouillage d'objet S3 est activé.

Présentation du service de réplication CloudMirror

Vous pouvez activer la réplication CloudMirror pour un compartiment S3 si vous souhaitez que StorageGRID réplique les objets spécifiés ajoutés au compartiment vers

un ou plusieurs compartiments de destination externes.

Vous pouvez, par exemple, utiliser la réplication CloudMirror pour mettre en miroir des enregistrements client spécifiques dans Amazon S3, puis exploiter les services AWS pour analyser vos données.

> La réplication CloudMirror n'est pas prise en charge si le compartiment source est activé pour le verrouillage objet S3.

CloudMirror et ILM

La réplication CloudMirror fonctionne indépendamment des règles ILM actives de la grille. Le service CloudMirror réplique les objets au fur et à mesure qu'ils sont stockés dans le compartiment source et les fournit au compartiment de destination dès que possible. La livraison des objets répliqués est déclenchée lors de la réussite de l'acquisition de l'objet.

CloudMirror et réplication intergrille

La réplication CloudMirror présente des similarités et des différences importantes avec la fonction de réplication multigrille. Reportez-vous à la "Comparez la réplication entre les grilles et la réplication CloudMirror".

Compartiments CloudMirror et S3

La réplication CloudMirror est généralement configurée pour utiliser un compartiment S3 externe comme destination. Vous pouvez cependant également configurer la réplication afin d'utiliser un autre déploiement StorageGRID ou tout service compatible S3.

Compartiments existants

Lorsque vous activez la réplication CloudMirror pour un compartiment existant, seuls les nouveaux objets ajoutés à ce compartiment sont répliqués. Les objets existants dans le compartiment ne sont pas répliqués. Pour forcer la réplication d'objets existants, vous pouvez mettre à jour les métadonnées de l'objet existant en effectuant une copie d'objet.

> Si vous utilisez la réplication CloudMirror pour copier des objets vers une destination Amazon S3, sachez qu'Amazon S3 limite la taille des métadonnées définies par l'utilisateur dans chaque en-tête de la requête PUT à 2 Ko. Si un objet possède des métadonnées définies par l'utilisateur supérieures à 2 Ko, cet objet ne sera pas répliqué.

Compartiments de destination multiples

Pour répliquer des objets d'un compartiment unique vers plusieurs compartiments de destination, spécifiez la destination de chaque règle dans le XML de configuration de réplication. Vous ne pouvez pas répliquer un objet dans plusieurs compartiments en même temps.

Compartiments avec ou sans version

Vous pouvez configurer la réplication CloudMirror sur des compartiments avec ou sans version. Les compartiments de destination peuvent être avec ou sans version. Vous pouvez utiliser n'importe quelle combinaison de compartiments avec version et sans version. Par exemple, vous pouvez spécifier un compartiment avec version comme destination pour un compartiment source sans version, ou vice-versa. Vous pouvez également répliquer les compartiments sans version.

Suppression, boucles de réplication et événements

Comportement de suppression

Est identique au comportement de suppression du service Amazon S3, réplication interrégionale (CRR). La suppression d'un objet dans un compartiment source ne supprime jamais un objet répliqué dans la destination. Si le compartiment source et le compartiment de destination sont multiversion, le marqueur de suppression est répliqué. Si le compartiment de destination n'est pas versionné, la suppression d'un objet dans le compartiment source ne réplique pas le marqueur de suppression dans le compartiment de destination ni ne supprime l'objet de destination.

Protection contre les boucles de réplication

Comme les objets sont répliqués dans le compartiment de destination, StorageGRID les marque comme « réplicas ». Un compartiment StorageGRID de destination ne réplique pas les objets marqués comme répliques, ce qui vous protège contre les boucles de réplication accidentelles. Ce marquage de réplica est interne à StorageGRID et ne vous empêche pas d'utiliser AWS CRR lors de l'utilisation d'un compartiment Amazon S3 comme destination.

> ⓘ L'en-tête personnalisé utilisé pour marquer une réplique est `x-ntap-sg-replica`. Ce marquage empêche un miroir en cascade. StorageGRID prend en charge un CloudMirror bidirectionnel entre deux grilles.

Événements dans le compartiment de destination

L'unicité et l'ordre des événements dans le compartiment de destination ne sont pas garantis. Plusieurs copies identiques d'un objet source peuvent être livrées à la destination du fait des opérations effectuées pour garantir le succès de la livraison. Dans de rares cas, lorsque le même objet est mis à jour simultanément depuis deux sites StorageGRID ou plus, il peut ne pas correspondre au ordre d'événements du compartiment source.

Description des notifications pour les compartiments

Vous pouvez activer la notification d'événements pour un compartiment S3 si vous souhaitez que StorageGRID envoie des notifications sur des événements spécifiés à un cluster Kafka de destination ou à Amazon simple notification Service.

Par exemple, vous pouvez configurer l'envoi d'alertes aux administrateurs pour chaque objet ajouté à un compartiment, où les objets représentent les fichiers de journal associés à un événement système critique.

Les notifications d'événements sont créées au niveau du compartiment source, comme indiqué dans la configuration de la notification, et sont envoyées vers le compartiment de destination. Si un événement associé à un objet réussit, une notification concernant cet événement est créée et mise en file d'attente pour la livraison.

L'unicité et l'ordre des notifications ne sont pas garantis. Plusieurs notifications d'événement peuvent être envoyées vers la destination après les opérations effectuées pour garantir la réussite de la livraison. La livraison étant asynchrone, l'ordre dans le temps des notifications au niveau de la destination n'est pas garanti correspondant à l'ordre des événements dans le compartiment source, en particulier pour les opérations provenant de différents sites StorageGRID. Vous pouvez utiliser la `sequencer` clé du message d'événement pour déterminer l'ordre des événements pour un objet spécifique, comme décrit dans la documentation Amazon S3.

Les notifications d'événements StorageGRID suivent l'API Amazon S3 avec quelques restrictions.

- Les types d'événements suivants sont pris en charge :

- s3:ObjectCreated :
- s3:ObjectCreated:put
- s3:ObjectCreated:Post
- s3:ObjectCreated:Copier
- s3:ObjectCreated:CompleteMultipartUpload
- s3:objet Removed :
- s3:ObjectRemoved:Supprimer
- s3:ObjectRemoved:DeleteMarkerCreated
- s3:ObjectRestore:Post

- Les notifications d'événements envoyées par StorageGRID utilisent le format JSON standard, mais n'incluent pas certaines clés et utilisent des valeurs spécifiques pour d'autres, comme illustré dans le tableau :

Nom de la clé	Valeur ajoutée de StorageGRID
Source d'événements	`sgws:s3`
Région de l'awsRegion	*non inclus*
x-amz-id-2	*non inclus*
arn	`urn:sgws:s3:::bucket_name`

Comprendre le service d'intégration de la recherche

Si vous souhaitez utiliser un service externe de recherche et d'analyse de données pour vos métadonnées d'objet, vous pouvez activer l'intégration de la recherche pour un compartiment S3.

Le service d'intégration de la recherche est un service StorageGRID personnalisé qui envoie automatiquement et de manière asynchrone des métadonnées d'objet S3 vers un terminal de destination lors de la création ou de la suppression d'un objet ou de la mise à jour de ses métadonnées ou de ses balises. Vous pouvez ensuite utiliser des outils sophistiqués de recherche, d'analyse de données, de visualisation ou de machine learning proposés par le service de destination pour rechercher, analyser et obtenir des informations exploitables à partir de vos données d'objet.

Vous pouvez, par exemple, configurer des compartiments pour envoyer les métadonnées d'objet S3 vers un service Elasticsearch distant. Vous pouvez ensuite utiliser Elasticsearch pour effectuer des recherches dans des compartiments et effectuer des analyses sophistiquées des modèles présents dans les métadonnées de l'objet.

Même si l'intégration avec Elasticsearch peut être configurée dans un compartiment avec S3 Object Lock activé, les métadonnées S3 Object Lock (y compris la date de conservation jusqu'à et l'état de conservation légale) des objets ne seront pas incluses dans les métadonnées envoyées à Elasticsearch.

Étant donné que le service d'intégration de recherche envoie des métadonnées d'objet à une destination, son XML de configuration est appelé « XML de configuration de notification_métadonnées_ ». Ce XML de configuration est différent du XML de configuration de notification utilisé pour activer les notifications *événement*.

Intégration de la recherche et compartiments S3

Vous pouvez activer le service d'intégration de la recherche pour tout compartiment avec version ou sans version. L'intégration des recherches est configurée en associant le XML de configuration des notifications de métadonnées au compartiment qui spécifie les objets à utiliser et la destination des métadonnées de l'objet.

Les notifications de métadonnées sont générées sous la forme d'un document JSON nommé avec le nom du compartiment, le nom de l'objet et l'ID de version, le cas échéant. Chaque notification de métadonnées contient un ensemble standard de métadonnées système pour l'objet, en plus de toutes les balises de l'objet et de toutes les métadonnées utilisateur.

Pour les balises et les métadonnées d'utilisateur, StorageGRID transmet des dates et des chiffres à Elasticsearch en tant que chaînes ou notifications d'événement S3. Pour configurer Elasticsearch afin d'interpréter ces chaînes comme des dates ou des chiffres, suivez les instructions Elasticsearch pour un mappage dynamique des champs et un mappage des formats de date. Vous devez activer les mappages de champs dynamiques sur l'index avant de configurer le service d'intégration de la recherche. Une fois qu'un document est indexé, vous ne pouvez pas modifier les types de champ du document dans l'index.

Rechercher des notifications

Les notifications de métadonnées sont générées et mises en file d'attente pour être envoyées lorsque :

- Un objet est créé.
- Un objet est supprimé, notamment lorsque des objets sont supprimés suite au fonctionnement de la règle ILM de la grille.
- Les métadonnées ou les balises d'objet sont ajoutées, mises à jour ou supprimées. L'ensemble complet de métadonnées et de balises est toujours envoyé lors de la mise à jour, et pas seulement les valeurs modifiées.

Après avoir ajouté le XML de configuration de notification des métadonnées à un compartiment, des notifications sont envoyées pour tout nouvel objet que vous créez et pour tout objet que vous modifiez en mettant à jour ses données, métadonnées utilisateur ou balises. Cependant, aucune notification n'est envoyée pour les objets qui se trouvaient déjà dans le compartiment. Pour vous assurer que les métadonnées d'objet de tous les objets du compartiment sont envoyées à la destination, effectuez l'une des opérations suivantes :

- Configurez le service d'intégration de la recherche immédiatement après avoir créé le compartiment et avant d'ajouter des objets.
- Exécutez une action sur tous les objets déjà dans le compartiment pour déclencher un message de notification des métadonnées à envoyer à la destination.

Service d'intégration de la recherche et Elasticsearch

Le service d'intégration de recherche StorageGRID prend en charge un cluster Elasticsearch. Comme pour les autres services de plate-forme, la destination est spécifiée dans le noeud final dont l'URN est utilisé dans le XML de configuration du service. Utilisez le pour déterminer les "Matrice d'interopérabilité NetApp" versions de Elasticsearch prises en charge.

Gérez les terminaux des services de plateforme

Configurer les terminaux des services de plateforme

Avant de pouvoir configurer un service de plateforme pour un compartiment, vous devez configurer au moins un point de terminaison afin qu'il soit la destination du service de plateforme.

L'accès aux services de plateforme est activé par locataire par administrateur StorageGRID. Pour créer ou utiliser un noeud final de services de plate-forme, vous devez être un utilisateur locataire disposant de l'autorisation gérer les noeuds finaux ou accès racine, dans une grille dont la mise en réseau a été configurée pour permettre aux noeuds de stockage d'accéder aux ressources de noeuds finaux externes. Pour un seul locataire, vous pouvez configurer un maximum de 500 terminaux de services de plateforme. Pour plus d'informations, contactez votre administrateur StorageGRID.

Qu'est-ce qu'un terminal de services de plateforme ?

Un terminal de services de plateforme spécifie les informations dont StorageGRID a besoin pour accéder à la destination externe.

Par exemple, si vous souhaitez répliquer des objets à partir d'un compartiment StorageGRID vers un compartiment Amazon S3, vous créez un terminal des services de plateforme qui inclut les informations et les identifiants dont StorageGRID a besoin pour accéder au compartiment de destination sur Amazon.

Chaque type de service de plate-forme nécessite son propre terminal, vous devez donc configurer au moins un point final pour chaque service de plate-forme que vous prévoyez d'utiliser. Après avoir défini un noeud final de services de plate-forme, vous utilisez l'URN du noeud final comme destination dans le XML de configuration utilisé pour activer le service.

Vous pouvez utiliser le même point final que la destination pour plusieurs compartiments source. Par exemple, vous pouvez configurer plusieurs compartiments source pour envoyer les métadonnées d'objet vers le même point de terminaison d'intégration de la recherche, afin d'effectuer des recherches dans plusieurs compartiments. Vous pouvez également configurer un compartiment source pour qu'il utilise plusieurs terminaux comme cible, ce qui vous permet d'envoyer des notifications sur la création d'objets à une rubrique Amazon simple notification Service (Amazon SNS) et des notifications sur la suppression d'objets à une autre rubrique Amazon SNS.

Terminaux pour la réplication CloudMirror

StorageGRID prend en charge les terminaux de réplication qui représentent des compartiments S3. Ces compartiments peuvent être hébergés sur Amazon Web Services, sur le même déploiement StorageGRID, sur un autre service ou sur un autre déploiement à distance.

Terminaux pour les notifications

StorageGRID prend en charge les terminaux Amazon SNS et Kafka. Les terminaux SQS (simple Queue Service) ou Lambda d'AWS ne sont pas pris en charge.

Pour les terminaux Kafka, le protocole TLS mutuel n'est pas pris en charge. Par conséquent, si vous avez `ssl.client.auth` défini sur `required` dans la configuration de votre courtier Kafka, cela peut entraîner des problèmes de configuration du terminal Kafka.

Points d'extrémité du service d'intégration de la recherche

StorageGRID prend en charge des terminaux d'intégration de recherche représentant les clusters Elasticsearch. Ces clusters Elasticsearch peuvent se trouver dans un data Center local ou être hébergés dans un cloud AWS ou ailleurs.

Le point final de l'intégration de la recherche fait référence à un index et à un type Elasticsearch spécifiques. Vous devez créer l'index dans Elasticsearch avant la création du noeud final dans StorageGRID, sinon la création du noeud final échouera. Il n'est pas nécessaire de créer le type avant de créer le noeud final. StorageGRID crée le type si nécessaire lors de l'envoi de métadonnées d'objet au terminal.

Informations associées

"Administrer StorageGRID"

Spécifiez l'URN du terminal des services de plateforme

Lorsque vous créez un noeud final de services de plate-forme, vous devez spécifier un Nom de ressource unique (URN). Vous utiliserez l'URN pour référencer le noeud final lorsque vous créerez un XML de configuration pour le service de plate-forme. L'URN de chaque terminal doit être unique.

StorageGRID valide les terminaux de services de plateforme lors de leur création. Avant de créer un noeud final de services de plate-forme, vérifiez que la ressource spécifiée dans le noeud final existe et qu'elle peut être atteinte.

Éléments DE RETOUR

L'URN d'un noeud final de services de plate-forme doit commencer par ou `urn:mysite` par `arn:aws` , comme suit :

- Si le service est hébergé sur Amazon Web Services (AWS), utilisez `arn:aws`
- Si le service est hébergé sur Google Cloud Platform (GCP), utilisez `arn:aws`
- Si le service est hébergé localement, utilisez `urn:mysite`

Par exemple, si vous spécifiez l'URN d'un noeud final CloudMirror hébergé sur StorageGRID, l'URN peut commencer par `urn:sgws`.

L'élément suivant de l'URN spécifie le type de service de plateforme, comme suit :

Service	Type
Réplication CloudMirror	`s3`
Notifications	`sns` ou `kafka`
Intégration de la recherche	`es`

Par exemple, pour continuer à spécifier l'URN d'un noeud final CloudMirror hébergé sur StorageGRID, vous devez ajouter `s3` à obtenir `urn:sgws:s3`.

L'élément final de l'URN identifie la ressource cible spécifique au niveau de l'URI de destination.

Service	Ressource spécifique
Réplication CloudMirror	`bucket-name`
Notifications	`sns-topic-name` ou `kafka-topic-name`
Intégration de la recherche	`domain-name/index-name/type-name` **Remarque :** si le cluster Elasticsearch est **NOT** configuré pour créer automatiquement des index, vous devez créer l'index manuellement avant de créer le noeud final.

Urns pour les services hébergés sur AWS et GCP

Pour les entités AWS et GCP, l'URN complet est un ARN AWS valide. Par exemple :

- Réplication CloudMirror :

```
arn:aws:s3:::bucket-name
```

- Notifications :

```
arn:aws:sns:region:account-id:topic-name
```

- Intégration de la recherche :

```
arn:aws:es:region:account-id:domain/domain-name/index-name/type-name
```

> Pour un terminal d'intégration de recherche AWS, le `domain-name` doit inclure la chaîne littérale , `domain/`comme illustré ici.

Urnes pour des services hébergés localement

Lors de l'utilisation de services hébergés localement au lieu de services cloud, vous pouvez spécifier l'URN de toute façon qui crée un URN valide et unique, tant que l'URN inclut les éléments requis dans les troisième et dernière positions. Vous pouvez laisser les éléments indiqués en blanc facultatif, ou vous pouvez les spécifier de quelque manière que ce soit pour vous aider à identifier la ressource et à rendre l'URN unique. Par exemple :

- Réplication CloudMirror :

```
urn:mysite:s3:optional:optional:bucket-name
```

Pour un noeud final CloudMirror hébergé sur StorageGRID, vous pouvez spécifier un URN valide commençant par `urn:sgws`:

```
urn:sgws:s3:optional:optional:bucket-name
```

- Notifications :

  Spécifiez un point de terminaison Amazon simple notification Service :

  ```
  urn:mysite:sns:optional:optional:sns-topic-name
  ```

  Spécifiez un terminal Kafka :

  ```
  urn:mysite:kafka:optional:optional:kafka-topic-name
  ```

- Intégration de la recherche :

  ```
  urn:mysite:es:optional:optional:domain-name/index-name/type-name
  ```

  Pour les noeuds finaux d'intégration de recherche hébergés localement, l' `domain-name`élément peut être n'importe quelle chaîne tant que l'URN du noeud final est unique.

Créer un terminal de services de plate-forme

Vous devez créer au moins un noeud final du type correct avant d'activer un service de plate-forme.

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Les services de plateforme ont été activés pour votre compte de locataire par un administrateur StorageGRID.
- Vous appartenez à un groupe d'utilisateurs qui possède le "Gestion des noeuds finaux ou des autorisations d'accès racine".
- La ressource référencée par le noeud final des services de plate-forme a été créée :
  - Réplication CloudMirror : compartiment S3
  - Notification d'événements : Amazon simple notification Service (Amazon SNS) ou rubrique Kafka
  - Notification de recherche : index Elasticsearch, si le cluster de destination n'est pas configuré pour créer automatiquement des index.
- Vous disposez des informations relatives à la ressource de destination :
  - Hôte et port pour l'URI (Uniform Resource identifier)

Si vous prévoyez d'utiliser un compartiment hébergé sur un système StorageGRID comme point de terminaison pour la réplication CloudMirror, contactez l'administrateur de la grille pour déterminer les valeurs à saisir.

- Nom de ressource unique (URN)

  "Spécifiez l'URN du terminal des services de plateforme"

- Informations d'authentification (si nécessaire) :

  Rechercher les terminaux d'intégration

  Pour les terminaux d'intégration de recherche, vous pouvez utiliser les informations d'identification suivantes :

  - Clé d'accès : ID de clé d'accès et clé d'accès secrète
  - HTTP de base : nom d'utilisateur et mot de passe

  Terminaux de réplication CloudMirror

  Pour les terminaux de réplication CloudMirror, vous pouvez utiliser les informations d'identification suivantes :

  - Clé d'accès : ID de clé d'accès et clé d'accès secrète
  - CAP (C2S Access Portal) : URL d'informations d'identification temporaires, certificats de serveur et de client, clés client et phrase de passe de clé privée de client facultative.

  Terminaux Amazon SNS

  Pour les terminaux Amazon SNS, vous pouvez utiliser les informations d'identification suivantes :

  - Clé d'accès : ID de clé d'accès et clé d'accès secrète

  Les terminaux Kafka

  Pour les terminaux Kafka, vous pouvez utiliser les identifiants suivants :

  - SASL/PLAIN : nom d'utilisateur et mot de passe
  - SASL/SCRAM-SHA-256 : nom d'utilisateur et mot de passe
  - SASL/SCRAM-SHA-512 : nom d'utilisateur et mot de passe

- Certificat de sécurité (en cas d'utilisation d'un certificat d'autorité de certification personnalisé)

- Si les fonctions de sécurité de Elasticsearch sont activées, vous disposez du privilège Monitor cluster pour les tests de connectivité et du privilège write index ou des privilèges index and delete index pour les mises à jour de documents.

Étapes

1. Sélectionnez **STORAGE (S3)** > **Platform services Endpoints**. La page noeuds finaux des services de plate-forme s'affiche.
2. Sélectionnez **Créer un noeud final**.
3. Entrez un nom d'affichage pour décrire brièvement le point final et son objectif.

Le type de service de plate-forme pris en charge par le noeud final est affiché à côté du nom du noeud final lorsqu'il est répertorié sur la page noeuds finaux, de sorte que vous n'avez pas besoin d'inclure ces informations dans le nom.

4. Dans le champ **URI**, spécifiez l'identificateur de ressource unique (URI) du noeud final.

   Utilisez l'un des formats suivants :

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

   Si vous ne spécifiez pas de port, les ports par défaut suivants sont utilisés :

   - Port 443 pour les URI HTTPS et port 80 pour les URI HTTP (la plupart des terminaux)
   - Port 9092 pour les URI HTTPS et HTTP (terminaux Kafka uniquement)

   Par exemple, l'URI d'un compartiment hébergé sur StorageGRID peut être :

   ```
   https://s3.example.com:10443
   ```

   Dans cet exemple, `s3.example.com` représente l'entrée DNS pour l'adresse IP virtuelle (VIP) du groupe haute disponibilité StorageGRID (HA), et `10443` représente le port défini dans le noeud final de l'équilibreur de charge.

   > Si possible, vous devez vous connecter à un groupe haute disponibilité de nœuds d'équilibrage de la charge pour éviter un point de défaillance unique.

   De la même manière, l'URI d'un compartiment hébergé sur AWS peut être :

   ```
   https://s3-aws-region.amazonaws.com
   ```

   > Si le noeud final est utilisé pour le service de réplication CloudMirror, n'incluez pas le nom de compartiment dans l'URI. Vous incluez le nom du compartiment dans le champ **URN**.

5. Entrez le nom de ressource unique (URN) du noeud final.

   > Vous ne pouvez pas modifier l'URN d'un noeud final après sa création.

6. Sélectionnez **Continuer**.
7. Sélectionnez une valeur pour **Type d'authentification**.

Rechercher les terminaux d'intégration

Entrez ou téléchargez les informations d'identification d'un point final d'intégration de recherche.

Les informations d'identification que vous fournissez doivent disposer d'autorisations d'écriture pour la ressource de destination.

Type d'authentification	Description	Informations d'identification
Anonyme	Fournit un accès anonyme à la destination. Fonctionne uniquement pour les terminaux dont la sécurité est désactivée.	Pas d'authentification.
Clé d'accès	Utilise des identifiants de style AWS pour authentifier les connexions avec la destination.	• ID de clé d'accès • Clé d'accès secrète
HTTP de base	Utilise un nom d'utilisateur et un mot de passe pour authentifier les connexions à la destination.	• Nom d'utilisateur • Mot de passe

Terminaux de réplication CloudMirror

Entrez ou téléchargez les informations d'identification d'un point final de réplication CloudMirror.

Les informations d'identification que vous fournissez doivent disposer d'autorisations d'écriture pour la ressource de destination.

Type d'authentification	Description	Informations d'identification
Anonyme	Fournit un accès anonyme à la destination. Fonctionne uniquement pour les terminaux dont la sécurité est désactivée.	Pas d'authentification.
Clé d'accès	Utilise des identifiants de style AWS pour authentifier les connexions avec la destination.	• ID de clé d'accès • Clé d'accès secrète

Type d'authentification	Description	Informations d'identification
CAP (portail d'accès C2S)	Utilise des certificats et des clés pour authentifier les connexions à la destination.	• URL des informations d'identification temporaires • Certificat autorité de certification du serveur (téléchargement de fichiers PEM) • Certificat client (téléchargement de fichier PEM) • Clé privée client (téléchargement de fichiers PEM, format crypté OpenSSL ou format de clé privée non crypté) • Phrase de passe de clé privée du client (facultatif)

Terminaux Amazon SNS

Saisissez ou téléchargez les informations d'identification d'un terminal Amazon SNS.

Les informations d'identification que vous fournissez doivent disposer d'autorisations d'écriture pour la ressource de destination.

Type d'authentification	Description	Informations d'identification
Anonyme	Fournit un accès anonyme à la destination. Fonctionne uniquement pour les terminaux dont la sécurité est désactivée.	Pas d'authentification.
Clé d'accès	Utilise des identifiants de style AWS pour authentifier les connexions avec la destination.	• ID de clé d'accès • Clé d'accès secrète

Les terminaux Kafka

Entrez ou téléchargez les identifiants d'un terminal Kafka.

Les informations d'identification que vous fournissez doivent disposer d'autorisations d'écriture pour la ressource de destination.

Type d'authentification	Description	Informations d'identification
Anonyme	Fournit un accès anonyme à la destination. Fonctionne uniquement pour les terminaux dont la sécurité est désactivée.	Pas d'authentification.

Type d'authentification	Description	Informations d'identification
SASL/SIMPLE	Utilise un nom d'utilisateur et un mot de passe avec du texte brut pour authentifier les connexions à la destination.	• Nom d'utilisateur • Mot de passe
SASL/SCRAM-SHA-256	Utilise un nom d'utilisateur et un mot de passe à l'aide d'un protocole de réponse de vérification et d'un hachage SHA-256 pour authentifier les connexions à la destination.	• Nom d'utilisateur • Mot de passe
SASL/SCRAM-SHA-512	Utilise un nom d'utilisateur et un mot de passe à l'aide d'un protocole de réponse de vérification et d'un hachage SHA-512 pour authentifier les connexions à la destination.	• Nom d'utilisateur • Mot de passe

Sélectionnez **utiliser la délégation prise de l'authentification** si le nom d'utilisateur et le mot de passe proviennent d'un jeton de délégation obtenu à partir d'un cluster Kafka.

8. Sélectionnez **Continuer**.
9. Sélectionnez un bouton radio pour **Verify Server** pour choisir la manière dont la connexion TLS au noeud final est vérifiée.

Type de vérification du certificat	Description
Utiliser un certificat d'autorité de certification personnalisé	Utilisez un certificat de sécurité personnalisé. Si vous sélectionnez ce paramètre, copiez et collez le certificat de sécurité personnalisé dans la zone de texte **certificat CA**.
Utiliser le certificat CA du système d'exploitation	Utilisez le certificat d'autorité de certification Grid par défaut installé sur le système d'exploitation pour sécuriser les connexions.
Ne vérifiez pas le certificat	Le certificat utilisé pour la connexion TLS n'est pas vérifié. Cette option n'est pas sécurisée.

10. Sélectionnez **Test et Créer un noeud final**.
    - Un message de réussite s'affiche si le noeud final peut être atteint à l'aide des informations d'identification spécifiées. La connexion au noeud final est validée à partir d'un nœud sur chaque site.
    - Un message d'erreur s'affiche si la validation du noeud final échoue. Si vous devez modifier le noeud final pour corriger l'erreur, sélectionnez **Retour aux détails du noeud final** et mettez à jour les informations. Sélectionnez ensuite **Test et Créer un noeud final**.

> La création du terminal échoue si les services de plate-forme ne sont pas activés pour votre compte de locataire. Veuillez contacter votre administrateur StorageGRID.

Après avoir configuré un noeud final, vous pouvez utiliser son URN pour configurer un service de plate-forme.

Informations associées

- "Spécifiez l'URN du terminal des services de plateforme"
- "Configurez la réplication CloudMirror"
- "Configurer les notifications d'événements"
- "Configurez le service d'intégration de la recherche"

Tester la connexion pour le point final des services de plate-forme

Si la connexion à un service de plate-forme a changé, vous pouvez tester la connexion du noeud final pour vérifier que la ressource de destination existe et qu'elle peut être atteinte à l'aide des informations d'identification que vous avez spécifiées.

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Gestion des noeuds finaux ou des autorisations d'accès racine".

Description de la tâche

StorageGRID ne vérifie pas que les informations d'identification disposent des autorisations appropriées.

Étapes

1. Sélectionnez **STORAGE (S3)** > **Platform services Endpoints**.

   La page noeuds finaux des services de plate-forme s'affiche et affiche la liste des noeuds finaux des services de plate-forme déjà configurés.

2. Sélectionnez le noeud final dont vous souhaitez tester la connexion.

   La page des détails du point final s'affiche.

3. Sélectionnez **Tester la connexion**.
   - Un message de réussite s'affiche si le noeud final peut être atteint à l'aide des informations d'identification spécifiées. La connexion au noeud final est validée à partir d'un nœud sur chaque site.
   - Un message d'erreur s'affiche si la validation du noeud final échoue. Si vous devez modifier le noeud final pour corriger l'erreur, sélectionnez **Configuration** et mettez à jour les informations. Sélectionnez ensuite **Test et enregistrer les modifications**.

Modifier le point final des services de plate-forme

Vous pouvez modifier la configuration d'un point de terminaison de services de plate-forme pour modifier son nom, son URI ou d'autres détails. Par exemple, vous devrez peut-être mettre à jour les informations d'identification expirées ou modifier l'URI pour qu'il pointe vers un index Elasticsearch de sauvegarde pour le basculement. Vous ne pouvez pas modifier l'URN d'un terminal de services de plate-forme.

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".

- Vous appartenez à un groupe d'utilisateurs qui possède le "Gestion des noeuds finaux ou des autorisations d'accès racine".

Étapes

1. Sélectionnez **STORAGE (S3)** > **Platform services Endpoints**.

   La page noeuds finaux des services de plate-forme s'affiche et affiche la liste des noeuds finaux des services de plate-forme déjà configurés.

2. Sélectionnez le point final que vous souhaitez modifier.

   La page des détails du point final s'affiche.

3. Sélectionnez **Configuration**.
4. Modifiez la configuration du noeud final selon les besoins.

   Vous ne pouvez pas modifier l'URN d'un noeud final après sa création.

   a. Pour modifier le nom d'affichage du noeud final, sélectionnez l'icône de modification .
   b. Modifiez l'URI si nécessaire.
   c. Si nécessaire, modifiez le type d'authentification.
      - Pour l'authentification par clé d'accès, modifiez la clé selon vos besoins en sélectionnant **Modifier la clé S3** et en collant une nouvelle ID de clé d'accès et une nouvelle clé d'accès secrète. Si vous devez annuler vos modifications, sélectionnez **Revert S3 key edit**.
      - Pour l'authentification CAP (C2S Access Portal), modifiez l'URL des informations d'identification temporaires ou la phrase de passe de la clé privée du client facultative et téléchargez de nouveaux certificats et fichiers de clés selon les besoins.

        La clé privée du client doit être au format crypté OpenSSL ou au format de clé privée non crypté.

   d. Si nécessaire, modifiez la méthode de vérification du serveur.
5. Sélectionnez **Tester et enregistrer les modifications**.
   - Un message de réussite s'affiche si le noeud final peut être atteint à l'aide des informations d'identification spécifiées. La connexion au noeud final est vérifiée à partir d'un noeud sur chaque site.
   - Un message d'erreur s'affiche si la validation du noeud final échoue. Modifiez le noeud final pour corriger l'erreur, puis sélectionnez **Test et enregistrer les modifications**.

Supprimer le noeud final des services de plate-forme

Vous pouvez supprimer un noeud final si vous ne souhaitez plus utiliser le service de plate-forme associé.

Avant de commencer

- Vous êtes connecté au gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Gestion des noeuds finaux ou des autorisations d'accès racine".

Étapes

1. Sélectionnez **STORAGE (S3)** > **Platform services Endpoints**.

   La page noeuds finaux des services de plate-forme s'affiche et affiche la liste des noeuds finaux des services de plate-forme déjà configurés.

2. Cochez la case correspondant à chaque point final à supprimer.

   > Si vous supprimez un noeud final de services de plate-forme en cours d'utilisation, le service de plate-forme associé sera désactivé pour tous les compartiments qui utilisent le noeud final. Toutes les demandes qui n'ont pas encore été traitées seront supprimées. Toutes les nouvelles demandes seront toujours générées jusqu'à ce que vous modifiiez la configuration de compartiment pour ne plus référencer l'URN supprimé. StorageGRID signale ces demandes comme des erreurs irrécupérables.

3. Sélectionnez **actions** > **Supprimer le point final**.

   Un message de confirmation s'affiche.

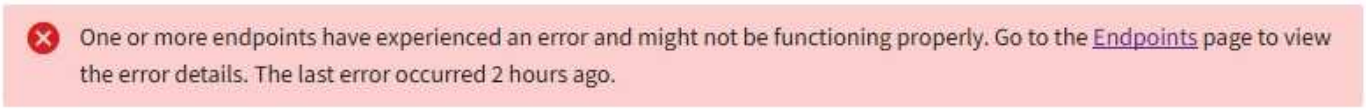
4. Sélectionnez **Supprimer le point final**.

Dépanner les erreurs de point final des services de plate-forme

Si une erreur se produit lorsque StorageGRID tente de communiquer avec un noeud final de services de plate-forme, un message s'affiche sur le tableau de bord. Sur la page noeuds finaux des services de plate-forme, la colonne dernière erreur indique il y a combien de temps l'erreur s'est produite. Aucune erreur ne s'affiche si les autorisations associées aux informations d'identification d'un noeud final sont incorrectes.

Déterminez si l'erreur s'est produite

Si des erreurs de noeud final de services de plateforme se sont produites au cours des 7 derniers jours, le tableau de bord du gestionnaire de locataires affiche un message d'alerte. Vous pouvez accéder à la page noeuds finaux des services de plate-forme pour obtenir plus de détails sur l'erreur.



La même erreur qui s'affiche sur le tableau de bord s'affiche également en haut de la page noeuds finaux Platform Services. Pour afficher un message d'erreur plus détaillé :

Étapes

1. Dans la liste des noeuds finaux, sélectionnez le noeud final qui contient l'erreur.
2. Sur la page des détails du noeud final, sélectionnez **connexion**. Cet onglet affiche uniquement l'erreur la plus récente pour un noeud final et indique il y a combien de temps l'erreur s'est produite. Des erreurs incluant l'icône X rouge se sont produites au cours des 7 derniers jours.

Vérifiez si l'erreur est toujours à jour

Certaines erreurs peuvent continuer à s'afficher dans la colonne **dernière erreur**, même après leur résolution. Pour voir si une erreur est active ou pour forcer la suppression d'une erreur résolue du tableau :

Étapes

1. Sélectionnez l'extrémité.

   La page des détails du point final s'affiche.

2. Sélectionnez **connexion** > **Tester la connexion**.

La sélection de **Test Connection** permet à StorageGRID de valider l'existence du noeud final des services de plate-forme et de l'atteindre avec les informations d'identification actuelles. La connexion au noeud final est validée à partir d'un nœud sur chaque site.

Résoudre les erreurs de point final

Vous pouvez utiliser le message **dernière erreur** sur la page des détails du noeud final pour déterminer ce qui est à l'origine de l'erreur. Certaines erreurs peuvent vous obliger à modifier le noeud final pour résoudre le problème. Par exemple, une erreur CloudMirroring peut se produire si StorageGRID ne parvient pas à accéder au compartiment S3 de destination, car il ne dispose pas des autorisations d'accès correctes ou si la clé d'accès a expiré. Le message est "les informations d'identification du noeud final ou l'accès à la destination doivent être mis à jour" et les détails sont "AccessDenied" ou "InvalidAccessKeyId".

Si vous devez modifier le noeud final pour résoudre une erreur, la sélection de **Test et enregistrer les modifications** fait que StorageGRID valide le noeud final mis à jour et confirme qu'il peut être atteint avec les informations d'identification actuelles. La connexion au noeud final est validée à partir d'un nœud sur chaque site.

Étapes

1. Sélectionnez l'extrémité.
2. Sur la page des détails du noeud final, sélectionnez **Configuration**.
3. Modifiez la configuration de point final selon vos besoins.
4. Sélectionnez **connexion** > **Tester la connexion**.

Identifiants de point de terminaison avec autorisations insuffisantes

Lorsque StorageGRID valide un terminal de services de plateforme, il confirme que les identifiants du terminal peuvent être utilisés pour contacter la ressource de destination et il vérifie les autorisations de base. Cependant, StorageGRID ne valide pas toutes les autorisations requises pour certaines opérations de services de plateforme. Pour cette raison, si vous recevez une erreur lors de la tentative d'utilisation d'un service de plate-forme (tel que « 403 interdit »), vérifiez les autorisations associées aux informations d'identification du noeud final.

Informations associées

- "Administration de StorageGRID ; dépannage des services de plate-forme"
- "Créer un terminal de services de plate-forme"
- "Tester la connexion pour le point final des services de plate-forme"
- "Modifier le point final des services de plate-forme"

Configurez la réplication CloudMirror

Pour activer la réplication de CloudMirror pour un compartiment, vous créez et appliquez un XML de configuration de réplication de compartiment valide.

Avant de commencer

- Les services de plateforme ont été activés pour votre compte de locataire par un administrateur StorageGRID.
- Vous avez déjà créé un compartiment qui servira de source de réplication.
- Le noeud final que vous prévoyez d'utiliser comme destination pour la réplication CloudMirror existe déjà, et vous avez son URN.
- Vous appartenez à un groupe d'utilisateurs qui possède le "Gérez tous les compartiments ou l'autorisation d'accès racine". Ces autorisations remplacent les paramètres d'autorisation des stratégies de groupe ou de compartiment lors de la configuration du compartiment à l'aide du Gestionnaire de locataires.

Description de la tâche

La réplication CloudMirror copie les objets à partir d'un compartiment source vers un compartiment de destination spécifié dans un terminal.

Pour des informations générales sur la réplication de compartiment et la configuration de celle-ci, reportez-vous à la section "Documentation d'Amazon simple Storage Service (S3) : réplication d'objets". Pour plus d'informations sur la manière dont StorageGRID implémente GetBuckeReplication, DeleteBuckeReplication et PutBuckeReplication, reportez-vous au "Opérations sur les compartiments".

> La réplication CloudMirror présente des similarités et des différences importantes avec la fonction de réplication multigrille. Pour en savoir plus, voir "Comparez la réplication entre les grilles et la réplication CloudMirror".

Notez les conditions et caractéristiques suivantes lors de la configuration de la réplication de CloudMirror :

- Lorsque vous créez et appliquez un XML de configuration de réplication de compartiment valide, il doit utiliser l'URN d'un terminal de compartiment S3 pour chaque destination.
- La réplication n'est pas prise en charge pour les compartiments source ou de destination lorsque le verrouillage d'objet S3 est activé.
- Si vous activez la réplication CloudMirror sur un compartiment qui contient des objets, les nouveaux objets ajoutés au compartiment sont répliqués, mais les objets existants du compartiment ne sont pas répliqués. Vous devez mettre à jour des objets existants pour déclencher la réplication.
- Si vous spécifiez une classe de stockage dans le fichier XML de configuration de réplication, StorageGRID utilise cette classe lors des opérations sur le terminal S3 de destination. Le noeud final de destination doit également prendre en charge la classe de stockage spécifiée. Veillez à suivre les recommandations fournies par le fournisseur du système de destination.

Étapes

1. Activer la réplication pour le compartiment source :
   - Utilisez un éditeur de texte pour créer le XML de configuration de réplication requis pour activer la réplication, comme spécifié dans l'API de réplication S3.
   - Lors de la configuration du XML :
     - Notez que StorageGRID ne prend en charge que le V1 de la configuration de la réplication. Cela signifie que StorageGRID ne prend pas en charge l'utilisation de `Filter` l'élément pour les règles et respecte les conventions V1 pour la suppression des versions d'objet. Pour plus d'informations, reportez-vous à la documentation Amazon sur la configuration de la réplication.
     - Utiliser l'URN d'un terminal du compartiment S3 comme destination.
     - Si vous le souhaitez, ajoutez l'élément et spécifiez l'une des options `<StorageClass>` suivantes :

- `STANDARD`: La classe de stockage par défaut. Si vous ne spécifiez pas de classe de stockage lorsque vous téléchargez un objet, la `STANDARD` classe de stockage est utilisée.
- `STANDARD_IA`: (Standard - accès peu fréquent.) Utilisez cette classe de stockage pour les données moins consultées, mais qui nécessitent un accès rapide en cas de besoin.
- `REDUCED_REDUNDANCY`: Utilisez cette classe de stockage pour les données non critiques et reproductibles qui peuvent être stockées avec moins de redondance que la `STANDARD` classe de stockage.

- Si vous spécifiez un `Role` dans le XML de configuration, il sera ignoré. Cette valeur n'est pas utilisée par StorageGRID.

```
<ReplicationConfiguration>
    <Role></Role>
    <Rule>
        <Status>Enabled</Status>
        <Prefix>2020</Prefix>
        <Destination>
           <Bucket>urn:sgws:s3:::2017-records</Bucket>
           <StorageClass>STANDARD</StorageClass>
         </Destination>
     </Rule>
</ReplicationConfiguration>
```

2. Sélectionnez **Afficher les compartiments** dans le tableau de bord ou sélectionnez **STOCKAGE (S3)** > **compartiments**.
3. Sélectionnez le nom du compartiment source.

   La page des détails du compartiment s'affiche.
4. Sélectionnez **Platform Services** > **Replication**.
5. Cochez la case **Activer la réplication**.
6. Collez le XML de configuration de réplication dans la zone de texte et sélectionnez **Enregistrer les modifications**.

> Les services de plateforme doivent être activés pour chaque compte de locataire par un administrateur StorageGRID à l'aide de Grid Manager ou de l'API de gestion du grid. Contactez votre administrateur StorageGRID si une erreur se produit lors de l'enregistrement du XML de configuration.

7. Vérifiez que la réplication est configurée correctement :
   a. Ajoutez un objet au compartiment source qui répond aux exigences de réplication telles que spécifiées dans la configuration de la réplication.

      Dans l'exemple présenté précédemment, les objets qui correspondent au préfixe « 2020 » sont répliqués.

   b. Confirmer que l'objet a été répliqué vers le compartiment de destination.

Pour les objets de petite taille, la réplication s'effectue rapidement.

Informations associées

"Créer un terminal de services de plate-forme"

Configurer les notifications d'événements

Vous activez les notifications pour un compartiment en créant un XML de configuration de notification et en utilisant le gestionnaire de locataires pour appliquer le XML à un compartiment.

Avant de commencer

- Les services de plateforme ont été activés pour votre compte de locataire par un administrateur StorageGRID.
- Vous avez déjà créé un compartiment qui sert de source de notifications.
- Le noeud final que vous avez l'intention d'utiliser comme destination pour les notifications d'événements existe déjà, et vous avez son URN.
- Vous appartenez à un groupe d'utilisateurs qui possède le "Gérez tous les compartiments ou l'autorisation d'accès racine". Ces autorisations remplacent les paramètres d'autorisation des stratégies de groupe ou de compartiment lors de la configuration du compartiment à l'aide du Gestionnaire de locataires.

Description de la tâche

Vous configurez les notifications d'événements en associant le XML de configuration de notification à un compartiment source. Le XML de configuration des notifications respecte les conventions S3 pour la configuration des notifications de compartiment. La rubrique Kafka ou Amazon SNS de destination est spécifiée comme URN d'un terminal.

Pour obtenir des informations générales sur les notifications d'événements et leur configuration, reportez-vous au "Documentation Amazon". Pour plus d'informations sur la manière dont StorageGRID implémente l'API de configuration des notifications de compartiment S3, reportez-vous au "Instructions d'implémentation des applications client S3".

Notez les exigences et caractéristiques suivantes lors de la configuration des notifications d'événement pour un compartiment :

- Lorsque vous créez et appliquez un XML de configuration de notification valide, il doit utiliser l'URN d'un noeud final de notification d'événement pour chaque destination.
- Bien que la notification d'événement puisse être configurée sur un compartiment avec le verrouillage objet S3 activé, les métadonnées de verrouillage objet S3 (y compris la date de conservation jusqu'à et l'état de conservation légale) des objets ne seront pas incluses dans les messages de notification.
- Après la configuration des notifications d'événements, chaque fois qu'un événement spécifié se produit pour un objet dans le compartiment source, une notification est générée et envoyée à la rubrique Amazon SNS ou Kafka utilisée comme terminal de destination.
- Si vous activez les notifications d'événements pour un compartiment contenant des objets, les notifications sont envoyées uniquement pour les actions qui sont effectuées après l'enregistrement de la configuration de notification.

Étapes

1. Activer les notifications pour le compartiment source :

- Utilisez un éditeur de texte pour créer le XML de configuration de notification requis pour activer les notifications d'événement, comme spécifié dans l'API de notification S3.
- Lors de la configuration du XML, utilisez l'URN d'un terminal de notification d'événements comme sujet de destination.

```
<NotificationConfiguration>
  <TopicConfiguration>
     <Id>Image-created</Id>
     <Filter>
        <S3Key>
          <FilterRule>
            <Name>prefix</Name>
            <Value>images/</Value>
          </FilterRule>
        </S3Key>
    </Filter>
    <Topic>arn:aws:sns:us-east-1:050340950352:sgws-topic</Topic>
    <Event>s3:ObjectCreated:*</Event>
   </TopicConfiguration>
 </NotificationConfiguration>
```

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

   La page des détails du compartiment s'affiche.

4. Sélectionnez **Platform Services** > **Event Notifications**.
5. Cochez la case **Activer les notifications d'événements**.
6. Collez le XML de configuration de notification dans la zone de texte, puis sélectionnez **Enregistrer les modifications**.

   Les services de plateforme doivent être activés pour chaque compte de locataire par un administrateur StorageGRID à l'aide de Grid Manager ou de l'API de gestion du grid. Contactez votre administrateur StorageGRID si une erreur se produit lors de l'enregistrement du XML de configuration.

7. Vérifiez que les notifications d'événements sont correctement configurées :

   a. Exécutez une action sur un objet du compartiment source qui répond aux exigences de déclenchement d'une notification telles qu'elles sont configurées dans le fichier XML de configuration.

      Dans cet exemple, une notification d'événement est envoyée chaque fois qu'un objet est créé avec le `images/` préfixe.

   b. Vérifiez qu'une notification a été envoyée à la rubrique Amazon SNS ou Kafka de destination.

      Par exemple, si votre sujet de destination est hébergé sur Amazon SNS, vous pouvez configurer le service pour qu'il vous envoie un e-mail lorsque la notification est remise.

```
{
   "Records":[
      {
         "eventVersion":"2.0",
         "eventSource":"sgws:s3",
         "eventTime":"2017-08-08T23:52:38Z",
         "eventName":"ObjectCreated:Put",
         "userIdentity":{
            "principalId":"11111111111111111"
         },
         "requestParameters":{
            "sourceIPAddress":"193.51.100.20"
         },
         "responseElements":{
            "x-amz-request-id":"122047343"
         },
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"Image-created",
            "bucket":{
               "name":"test1",
               "ownerIdentity":{
                  "principalId":"11111111111111111"
               },
               "arn":"arn:sgws:s3:::test1"
            },
            "object":{
               "key":"images/cat.jpg",
               "size":0,
               "eTag":"d41d8cd98f00b204e9800998ecf8427e",
               "sequencer":"14D90402421461C7"
            }
         }
      }
   ]
}
```


+
Si la notification est reçue dans la rubrique de destination, vous avez configuré votre compartiment source pour les notifications StorageGRID.

Informations associées

"Description des notifications pour les compartiments"

"UTILISEZ L'API REST S3"

"Créer un terminal de services de plate-forme"

Configurer le service d'intégration de la recherche

Vous activez l'intégration de la recherche pour un compartiment en créant un XML d'intégration de recherche et en utilisant le Gestionnaire de locataires pour appliquer le XML au compartiment.

Avant de commencer

- Les services de plateforme ont été activés pour votre compte de locataire par un administrateur StorageGRID.
- Vous avez déjà créé un compartiment S3 dont vous souhaitez indexer le contenu.
- Le noeud final que vous avez l'intention d'utiliser comme destination pour le service d'intégration de recherche existe déjà, et vous avez son URN.
- Vous appartenez à un groupe d'utilisateurs qui possède le "Gérez tous les compartiments ou l'autorisation d'accès racine". Ces autorisations remplacent les paramètres d'autorisation des stratégies de groupe ou de compartiment lors de la configuration du compartiment à l'aide du Gestionnaire de locataires.

Description de la tâche

Une fois que vous avez configuré le service d'intégration de recherche pour un compartiment source, la création d'un objet ou la mise à jour des métadonnées ou des balises d'un objet déclenche l'envoi des métadonnées d'objet vers le terminal de destination.

Si vous activez le service d'intégration de recherche pour un compartiment qui contient déjà des objets, les notifications de métadonnées ne sont pas automatiquement envoyées pour les objets existants. Mettez à jour ces objets existants pour vous assurer que leurs métadonnées sont ajoutées à l'index de recherche de destination.

Étapes

1. Activer l'intégration de la recherche pour un compartiment :
    - Utilisez un éditeur de texte pour créer le XML de notification de métadonnées requis pour activer l'intégration de la recherche.
    - Lors de la configuration du XML, utilisez l'URN d'un noeud final d'intégration de recherche comme destination.

      Les objets peuvent être filtrés sur le préfixe du nom de l'objet. Par exemple, vous pouvez envoyer des métadonnées pour les objets dont le préfixe est `images` donné à une destination, et des métadonnées pour les objets dont le préfixe est ajouté `videos` à une autre. Les configurations qui comportent des préfixes qui se chevauchent ne sont pas valides et sont rejetées lorsqu'elles sont soumises. Par exemple, une configuration qui inclut une règle pour les objets avec le préfixe `test` et une seconde règle pour les objets avec le préfixe `test2` n'est pas autorisée.

      Si nécessaire, reportez-vous à la Exemples pour le XML de configuration des métadonnées.

```
<MetadataNotificationConfiguration>
 <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
       <Urn>/Urn>
       </Destination>
 </Rule>
</MetadataNotificationConfiguration>
```

Éléments de la configuration de notification des métadonnées XML :

Nom	Description	Obligatoire
Configuration de la MetadaNotification Configuration	Balise de conteneur pour les règles utilisées pour spécifier les objets et la destination des notifications de métadonnées. Contient un ou plusieurs éléments de règle.	Oui
Règle	Balise de conteneur d'une règle qui identifie les objets dont les métadonnées doivent être ajoutées à un index spécifié. Les règles avec des préfixes qui se chevauchent sont rejetées. Inclus dans l'élément MetadaNotificationConfiguration.	Oui
ID	Identifiant unique de la règle. Inclus dans l'élément règle.	Non
État	L'état peut être « activé » ou « désactivé ». Aucune action n'est prise pour les règles désactivées. Inclus dans l'élément règle.	Oui
Préfixe	Les objets qui correspondent au préfixe sont affectés par la règle et leurs métadonnées sont envoyées à la destination spécifiée. Pour faire correspondre tous les objets, spécifiez un préfixe vide. Inclus dans l'élément règle.	Oui
Destination	Balise de conteneur pour la destination d'une règle. Inclus dans l'élément règle.	Oui

Nom	Description	Obligatoire
Urne	URN de la destination où les métadonnées d'objet sont envoyées. Doit être l'URN d'un terminal StorageGRID avec les propriétés suivantes : • `es` doit être le troisième élément. • L'URN doit se terminer par l'index et le type où les métadonnées sont stockées, sous la forme `domain-name/myindex/mytype`. Les terminaux sont configurés à l'aide du Gestionnaire de locataires ou de l'API de gestion des locataires. Ils se présentent sous la forme suivante : • `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` Le noeud final doit être configuré avant la soumission du XML de configuration, ou la configuration échouera avec une erreur 404. L'URNE est incluse dans l'élément destination.	Oui

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

   La page des détails du compartiment s'affiche.

4. Sélectionnez **Platform Services** > **Search Integration**
5. Cochez la case **Activer l'intégration de la recherche**.
6. Collez la configuration de notification de métadonnées dans la zone de texte, puis sélectionnez **Enregistrer les modifications**.

   > Les services de plateforme doivent être activés pour chaque compte de locataire par un administrateur StorageGRID à l'aide de l'API Grid Manager ou de gestion. Contactez votre administrateur StorageGRID si une erreur se produit lors de l'enregistrement du XML de configuration.

7. Vérifiez que le service d'intégration de la recherche est configuré correctement :
   a. Ajoutez un objet au compartiment source qui répond aux exigences relatives au déclenchement d'une notification de métadonnées comme spécifié dans le XML de configuration.

      Dans l'exemple présenté précédemment, tous les objets ajoutés au compartiment déclenchent une notification de métadonnées.

   b. Vérifiez qu'un document JSON contenant les métadonnées et les balises de l'objet a été ajouté à l'index de recherche spécifié dans le noeud final.

Une fois que vous avez terminé

Si nécessaire, vous pouvez désactiver l'intégration de la recherche pour un compartiment à l'aide de l'une des méthodes suivantes :

- Sélectionnez **STORAGE (S3)** > **Buckets** et décochez la case **Enable search Integration**.
- Si vous utilisez directement l'API S3, utilisez une demande de notification DE suppression des métadonnées du compartiment. Pour plus d'informations sur l'implémentation des applications client S3, reportez-vous aux instructions.

exemple : configuration de notification de métadonnées qui s'applique à tous les objets

Dans cet exemple, les métadonnées d'objet de tous les objets sont envoyées vers la même destination.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
           <Urn>urn:myes:es:::sgws-notifications/test1/all</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

Exemple : configuration des notifications de métadonnées avec deux règles

Dans cet exemple, les métadonnées d'objet des objets qui correspondent au préfixe `/images` sont envoyées à une destination, tandis que les métadonnées d'objet des objets correspondant au préfixe `/videos` sont envoyées à une seconde destination.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Images-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/images</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Videos-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/videos</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

Format de notification des métadonnées

Lorsque vous activez le service d'intégration de la recherche pour un compartiment, un document JSON est généré et envoyé au terminal de destination à chaque ajout, mise à jour ou suppression de métadonnées d'objet.

Cet exemple montre un exemple de fichier JSON qui pourrait être généré lors de la création d'un objet avec la clé `SGWS/Tagging.txt` dans un compartiment nommé `test`. Le `test` compartiment n'est pas versionné, la balise est donc `versionId` vide.

```
{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region":"us-east-1",
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}
```

Champs inclus dans le document JSON

Le nom du document inclut le nom du compartiment, le nom de l'objet et l'ID de version, le cas échéant.

Informations sur les compartiments et les objets

`bucket`: Nom du compartiment

`key`: Nom de clé d'objet

`versionID`: Version de l'objet, pour les objets dans les compartiments multiversion

`region`: Région du compartiment, par exemple `us-east-1`

Métadonnées de système

`size`: Taille de l'objet (en octets) visible par un client HTTP

`md5`: Hachage d'objet

Métadonnées d'utilisateur

`metadata`: Toutes les métadonnées utilisateur de l'objet, en tant que paires clé-valeur

`key:value`

Étiquettes

`tags`: Toutes les balises d'objet définies pour l'objet, en tant que paires clé-valeur

`key:value`

Affichage des résultats dans Elasticsearch

Pour les balises et les métadonnées d'utilisateur, StorageGRID transmet des dates et des chiffres à Elasticsearch en tant que chaînes ou notifications d'événement S3. Pour configurer Elasticsearch afin

d’interpréter ces chaînes comme des dates ou des chiffres, suivez les instructions Elasticsearch pour un mappage dynamique des champs et un mappage des formats de date. Activez les mappages de champs dynamiques sur l’index avant de configurer le service d’intégration de recherche. Une fois qu’un document est indexé, vous ne pouvez pas modifier les types de champ du document dans l’index.

UTILISEZ L’API REST S3

Versions et mises à jour prises en charge par l’API REST S3

StorageGRID prend en charge l’API simple Storage Service (S3), qui est implémentée en tant que ensemble de services web REST (Representational State Transfer).

La prise en charge de l’API REST S3 vous permet de connecter les applications orientées services développées pour les services web S3 avec un stockage objet sur site qui utilise le système StorageGRID. L’utilisation actuelle des appels de l’API REST S3 par une application client requiert des modifications minimales.

Versions prises en charge

StorageGRID prend en charge les versions spécifiques suivantes de S3 et HTTP.

Élément	Version
Spécification de l’API S3	"Documentation Amazon Web Services (AWS) : référence de l’API Amazon simple Storage Service"
HTTP	1,1 Pour plus d’informations sur HTTP, consultez le document HTTP/1.1 (RFC 7230-35). "IETF RFC 2616 : Protocole de transfert hypertexte (HTTP/1.1)" **Remarque**: StorageGRID ne prend pas en charge HTTP/1.1 pipeline.

Prise en charge des mises à jour de l’API REST S3

Relâchez	Commentaires
11,9	• Ajout de la prise en charge des valeurs de somme de contrôle SHA-256 pré-calculées pour les demandes suivantes et les en-têtes pris en charge. Vous pouvez utiliser cette fonction pour vérifier l'intégrité des objets téléchargés : ◦ Téléchargement CompleteMultipartUpload : `x-amz-checksum-sha256` ◦ CreateMultipartUpload : `x-amz-checksum-algorithm` ◦ GetObject : `x-amz-checksum-mode` ◦ Objet principal : `x-amz-checksum-mode` ◦ ListParts ◦ PutObject : `x-amz-checksum-sha256` ◦ UploadPart : `x-amz-checksum-sha256` • Ajout de la possibilité pour l'administrateur du grid de contrôler les paramètres de conservation et de conformité au niveau du locataire. Ces paramètres affectent les paramètres de verrouillage d'objet S3. ◦ Mode de conservation par défaut du compartiment et mode de conservation des objets : gouvernance ou conformité, si l'administrateur du grid l'autorise. ◦ La période de conservation par défaut du compartiment et la date de conservation de l'objet jusqu'au : doivent être inférieures ou égales à ce qui est autorisé par la période de conservation maximale définie par l'administrateur du grid. • Meilleure prise en charge de `aws-chunked` l'encodage de contenu et des valeurs de diffusion en continu `x-amz-content-sha256`. Limites : ◦ Le cas échéant, `chunk-signature` est facultatif et non validé ◦ S'il est présent, `x-amz-trailer` le contenu est ignoré
11,8	Mise à jour des noms des opérations S3 pour qu'ils correspondent aux noms utilisés dans le "Documentation Amazon Web Services (AWS) : référence de l'API Amazon simple Storage Service".
11,7	• Ajouté "Référence rapide : demandes d'API S3 prises en charge". • Ajout de la prise en charge du mode DE GOUVERNANCE avec S3 Object Lock. • Ajout de la prise en charge de l'en-TÊTE de réponse spécifique à StorageGRID `x-ntap-sg-cgr-replication-status` pour les requêtes GET Object et HEAD Object. Cet en-tête fournit l'état de réplication d'un objet pour la réplication inter-grid. • Les requêtes SelectObjectContent prennent désormais en charge les objets parquet.

Relâchez	Commentaires
11,6	• Ajout de la prise en charge de l'utilisation du `partNumber` paramètre de requête dans les requêtes GET Object et HEAD Object. • Ajout de la prise en charge d'un mode de conservation par défaut et d'une période de conservation par défaut au niveau du compartiment pour le verrouillage d'objet S3. • Ajout de la prise en charge de la `s3:object-lock-remaining-retention-days` clé de condition de règle pour définir la plage de périodes de conservation autorisées pour vos objets. • Modification de la taille *recommandée* maximale pour une opération objet PUT unique à 5 Gio (5,368,709,120 octets). Si vos objets sont supérieurs à 5 Gio, utilisez le téléchargement partitionné.
11,5	• Ajout de la prise en charge de la gestion du chiffrement de compartiment. • Ajout de la prise en charge des demandes de verrouillage d'objet S3 et des demandes de conformité héritées obsolètes. • Ajout de la prise en charge de L'utilisation DE LA SUPPRESSION de plusieurs objets sur les compartiments multiversion. • L' `Content-MD5`en-tête de la demande est désormais correctement pris en charge.
11,4	• Prise en charge accrue du balisage de compartiment, DE L'étiquetage DES compartiments ET DU balisage de compartiment. Les étiquettes de répartition des coûts ne sont pas prises en charge. • Pour les compartiments créés dans StorageGRID 11.4, il n'est plus nécessaire de limiter les noms de clés d'objet pour respecter les bonnes pratiques de performance. • Prise en charge supplémentaire des notifications de compartiment pour le `s3:ObjectRestore:Post` type d'événement. • Les limites de taille d'AWS pour les pièces partitionnés sont maintenant appliquées. Chaque partie d'un téléchargement partitionné doit être comprise entre 5 MIB et 5 Gio. La dernière partie peut être plus petite que 5 MIB. • Ajout de la prise en charge de TLS 1.3
11,3	• Ajout de la prise en charge du chiffrement côté serveur des données d'objet avec les clés fournies par le client (SSE-C). • Prise en charge supplémentaire des opérations de SUPPRESSION, d'OBTENTION et de MISE du cycle de vie du compartiment (action d'expiration uniquement) et de `x-amz-expiration` l'en-tête de réponse. • PUT Object mis à jour, PUT Object - copie et Multipart Upload pour décrire l'impact des règles ILM utilisant un placement synchrone à l'entrée. • Les chiffrements TLS 1.1 ne sont plus pris en charge.

Relâchez	Commentaires
11,2	Ajout de la prise en charge de la restauration POST-objet pour l'utilisation avec les pools de stockage cloud. Ajout de la prise en charge de l'utilisation de la syntaxe AWS pour ARN, des clés de condition de règle et des variables de règles de groupe et de compartiment Les règles de compartiment et de groupe qui utilisent la syntaxe StorageGRID restent prises en charge. **Remarque :** les utilisations de l'ARN/URN dans d'autres configurations JSON/XML, y compris celles utilisées dans les fonctions StorageGRID personnalisées, n'ont pas changé.
11,1	Ajout de la prise en charge du partage de ressources entre les sources (CORS), du protocole HTTP pour les connexions client S3 aux nœuds de grid et des paramètres de conformité dans les compartiments.
11,0	Ajout de la prise en charge de la configuration des services de plateforme (réplication CloudMirror, notifications et intégration de la recherche Elasticsearch) pour les compartiments Ajout de la prise en charge des contraintes d'emplacement du balisage d'objets pour les compartiments, ainsi que de la cohérence disponible.
10,4	Ajout de la prise en charge des modifications de l'analyse ILM sur la gestion des versions, mises à jour de la page noms de domaine de point final, conditions et variables dans les règles, exemples de règles et autorisation PutOverwriteObject.
10,3	Prise en charge ajoutée pour la gestion des versions.
10,2	Ajout de la prise en charge des règles d'accès de groupe et de compartiment, ainsi que de la copie multipart (Télécharger la pièce - copie).
10,1	Ajout de la prise en charge du téléchargement partitionné, des demandes de type hébergement virtuel et de l'authentification v4.
10,0	Prise en charge initiale de l'API REST S3 par le système StorageGRID.la version actuellement prise en charge de *simple Storage Service API Reference* est 2006-03-01.

Référence rapide : demandes d'API S3 prises en charge

Cette page explique comment StorageGRID prend en charge les API Amazon simple Storage Service (S3).

Cette page inclut uniquement les opérations S3 prises en charge par StorageGRID.

Pour afficher la documentation AWS pour chaque opération, sélectionnez le lien dans l'en-tête.

Paramètres de requête URI courants et en-têtes de requête

Sauf mention contraire, les paramètres de requête URI courants suivants sont pris en charge :

- `versionId` (comme requis pour les opérations d'objet)

Sauf mention contraire, les en-têtes de requête courants suivants sont pris en charge :

- `Authorization`
- `Connection`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Date`
- `Expect`
- `Host`
- `x-amz-date`

Informations associées

- "Détails de l'implémentation de l'API REST S3"
- "Référence de l'API Amazon simple Storage Service : en-têtes de demande communs"

"AbortMultipartUpload"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communséléments de cette demande, plus ce paramètre de requête URI supplémentaire :

- `uploadId`

Corps de la demande

Aucune

Documentation StorageGRID

"Opérations pour les téléchargements partitionnés"

"CompleteMultipartUpload"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communséléments de cette demande, plus ce paramètre de requête URI supplémentaire :

- `uploadId`
- `x-amz-checksum-sha256`

Demander des balises XML de corps

StorageGRID prend en charge les balises XML de corps de requête suivantes :

- `ChecksumSHA256`
- `CompleteMultipartUpload`

- `ETag`
- `Part`
- `PartNumber`

Documentation StorageGRID

"CompleteMultipartUpload"

"Objet de copie"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communséléments pour cette demande, plus les en-têtes supplémentaires suivants :

- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-modified-since`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-server-side-encryption-customer-algorithm`
- `x-amz-copy-source-server-side-encryption-customer-key`
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`
- `x-amz-metadata-directive`
- `x-amz-object-lock-legal-hold`
- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-server-side-encryption`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-storage-class`
- `x-amz-tagging`
- `x-amz-tagging-directive`
- `x-amz-meta-<metadata-name>`

Corps de la demande

Aucune

Documentation StorageGRID

"Objet de copie"

"CreateBucket"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communséléments pour cette demande, plus les en-têtes supplémentaires suivants :

- `x-amz-bucket-object-lock-enabled`

Corps de la demande

StorageGRID prend en charge tous les paramètres du corps de demande définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation StorageGRID

"Opérations sur les compartiments"

"CreateMultipartUpload"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communséléments pour cette demande, plus les en-têtes supplémentaires suivants :

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `Expires`
- `x-amz-checksum-algorithm`
- `x-amz-server-side-encryption`
- `x-amz-storage-class`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-tagging`
- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-object-lock-legal-hold`
- `x-amz-meta-<metadata-name>`

Corps de la demande

Aucune

Documentation StorageGRID

"CreateMultipartUpload"

"DeleteBucket"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous paramètres et en-têtes communsces éléments pour cette demande.

Documentation StorageGRID

"Opérations sur les compartiments"

"DeleteBuckeCors"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous paramètres et en-têtes communsces éléments pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

"Opérations sur les compartiments"

"DeleteBuckeEncryption"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous paramètres et en-têtes communsces éléments pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

"Opérations sur les compartiments"

"DeleteBuckeLifecycle"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous paramètres et en-têtes communsces éléments pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

- "Opérations sur les compartiments"
- "Création de la configuration du cycle de vie S3"

"DeleteBucketPolicy"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous paramètres et en-têtes communsces éléments pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

"Opérations sur les compartiments"

"DeleteBuckeReplication"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous paramètres et en-têtes communsces éléments pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

"Opérations sur les compartiments"

"DeleteBucketTagging"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous paramètres et en-têtes communsces éléments pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

"Opérations sur les compartiments"

"DeleteObject"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communséléments de cette demande, plus cet en-tête de demande supplémentaire :

- `x-amz-bypass-governance-retention`

Corps de la demande

Aucune

Documentation StorageGRID

"Opérations sur les objets"

"DeleteObjects"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communséléments de cette demande, plus cet en-tête de demande supplémentaire :

- `x-amz-bypass-governance-retention`

Corps de la demande

StorageGRID prend en charge tous les paramètres du corps de demande définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation StorageGRID

"Opérations sur les objets"

"DeleteObjectTagging"

StorageGRID prend en charge tous paramètres et en-têtes communsces éléments pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

"Opérations sur les objets"

"GetBucketAcl"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous paramètres et en-têtes communsces éléments pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

"Opérations sur les compartiments"

"GetBucketCors"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous paramètres et en-têtes communsces éléments pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

"Opérations sur les compartiments"

"GetBucketEncryption"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous paramètres et en-têtes communsces éléments pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

"Opérations sur les compartiments"

"GetBucketLifecycleConfiguration"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous paramètres et en-têtes communsces éléments pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

- "Opérations sur les compartiments"
- "Création de la configuration du cycle de vie S3"

"GetBuckeLocation"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous paramètres et en-têtes communsces éléments pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

"Opérations sur les compartiments"

"GetBucketNotifationConfiguration"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous paramètres et en-têtes communsces éléments pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

"Opérations sur les compartiments"

"GetBucketPolicy"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous paramètres et en-têtes communsces éléments pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

"Opérations sur les compartiments"

"GetBuckeReplication"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous paramètres et en-têtes communsces éléments pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

"Opérations sur les compartiments"

"GetBucketTagging"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous paramètres et en-têtes communsces éléments pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

"Opérations sur les compartiments"

"GetBucketVersioning"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous paramètres et en-têtes communsces éléments pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

"Opérations sur les compartiments"

"GetObject"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communséléments de cette demande, plus les paramètres de requête URI supplémentaires suivants :

- `x-amz-checksum-mode`
- `partNumber`
- `response-cache-control`
- `response-content-disposition`
- `response-content-encoding`
- `response-content-language`
- `response-content-type`
- `response-expires`

Et ces en-têtes de demande supplémentaires :

- `Range`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `If-Match`
- `If-Modified-Since`
- `If-None-Match`
- `If-Unmodified-Since`

Corps de la demande

Aucune

Documentation StorageGRID

"GetObject"

"GetObjectAcl"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous paramètres et en-têtes communsces éléments pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

"Opérations sur les objets"

"GetObjectLegalHold"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous paramètres et en-têtes communsces éléments pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

"Utilisez l'API REST S3 pour configurer le verrouillage objet S3"

"GetObjectLockConfiguration"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous paramètres et en-têtes communsces éléments pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

"Utilisez l'API REST S3 pour configurer le verrouillage objet S3"

"GetObjectRetention"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous paramètres et en-têtes communsces éléments pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

"Utilisez l'API REST S3 pour configurer le verrouillage objet S3"

"GetObjectTagging"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous paramètres et en-têtes communsces éléments pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

"Opérations sur les objets"

"Godet principal"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous paramètres et en-têtes communsces éléments pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

"Opérations sur les compartiments"

"Objet principal"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communséléments pour cette demande, plus les en-têtes supplémentaires suivants :

- `x-amz-checksum-mode`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `If-Match`
- `If-Modified-Since`
- `If-None-Match`
- `If-Unmodified-Since`
- `Range`

Corps de la demande

Aucune

Documentation StorageGRID

"Objet principal"

"Listseaux"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous paramètres et en-têtes communsces éléments pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

"Opérations sur le service et gt ; ListBuckets"

"ListMultipartUploads"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communséléments de cette demande, plus les paramètres supplémentaires suivants :

- `encoding-type`
- `key-marker`
- `max-uploads`
- `prefix`
- `upload-id-marker`

Corps de la demande

Aucune

Documentation StorageGRID

"ListMultipartUploads"

"ListObjects"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communséléments de cette demande, plus les paramètres supplémentaires suivants :

- `delimiter`
- `encoding-type`
- `marker`
- `max-keys`
- `prefix`

Corps de la demande

Aucune

Documentation StorageGRID

"Opérations sur les compartiments"

"ListObjectsV2"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communséléments de cette demande, plus les paramètres supplémentaires suivants :

- `continuation-token`
- `delimiter`
- `encoding-type`
- `fetch-owner`
- `max-keys`
- `prefix`
- `start-after`

Corps de la demande

Aucune

Documentation StorageGRID

"Opérations sur les compartiments"

"ListObjectVersions"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communséléments de cette demande, plus les paramètres supplémentaires suivants :

- `delimiter`
- `encoding-type`
- `key-marker`
- `max-keys`
- `prefix`
- `version-id-marker`

Corps de la demande

Aucune

Documentation StorageGRID

"Opérations sur les compartiments"

"ListParts"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communséléments de cette demande, plus les paramètres supplémentaires suivants :

- `max-parts`

- `part-number-marker`
- `uploadId`

Corps de la demande

Aucune

Documentation StorageGRID

"ListMultipartUploads"

"PutBucketCors"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous paramètres et en-têtes communsces éléments pour cette demande.

Corps de la demande

StorageGRID prend en charge tous les paramètres du corps de demande définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation StorageGRID

"Opérations sur les compartiments"

"PutBucketEncryption"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous paramètres et en-têtes communsces éléments pour cette demande.

Demander des balises XML de corps

StorageGRID prend en charge les balises XML de corps de requête suivantes :

- `ApplyServerSideEncryptionByDefault`
- `Rule`
- `ServerSideEncryptionConfiguration`
- `SSEAlgorithm`

Documentation StorageGRID

"Opérations sur les compartiments"

"PutBucketLifecycleConfiguration"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous paramètres et en-têtes communsces éléments pour cette demande.

Demander des balises XML de corps

StorageGRID prend en charge les balises XML de corps de requête suivantes :

- `And`
- `Days`
- `Expiration`

- `ExpiredObjectDeleteMarker`
- `Filter`
- `ID`
- `Key`
- `LifecycleConfiguration`
- `NewerNoncurrentVersions`
- `NoncurrentDays`
- `NoncurrentVersionExpiration`
- `Prefix`
- `Rule`
- `Status`
- `Tag`
- `Value`

Documentation StorageGRID

- "Opérations sur les compartiments"
- "Création de la configuration du cycle de vie S3"

"PutBucketNotifationConfiguration"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous paramètres et en-têtes communsces éléments pour cette demande.

Demander des balises XML de corps

StorageGRID prend en charge les balises XML de corps de requête suivantes :

- `Event`
- `Filter`
- `FilterRule`
- `Id`
- `Name`
- `NotificationConfiguration`
- `Prefix`
- `S3Key`
- `Suffix`
- `Topic`
- `TopicConfiguration`
- `Value`

Documentation StorageGRID

"Opérations sur les compartiments"

"PutBuckePolicy"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous paramètres et en-têtes communsces éléments pour cette demande.

Corps de la demande

Pour plus d'informations sur les champs de corps JSON pris en charge, reportez-vous à la section "Utilisez les règles d'accès au compartiment et au groupe".

"PutBuckeReplication"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous paramètres et en-têtes communsces éléments pour cette demande.

Demander des balises XML de corps

- `Bucket`
- `Destination`
- `Prefix`
- `ReplicationConfiguration`
- `Rule`
- `Status`
- `StorageClass`

Documentation StorageGRID

"Opérations sur les compartiments"

"Étiquetage PutBucketTagging"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous paramètres et en-têtes communsces éléments pour cette demande.

Corps de la demande

StorageGRID prend en charge tous les paramètres du corps de demande définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation StorageGRID

"Opérations sur les compartiments"

"PutBuckeVersioning"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous paramètres et en-têtes communsces éléments pour cette demande.

Demander les paramètres du corps

StorageGRID prend en charge les paramètres de corps de demande suivants :

- `VersioningConfiguration`
- `Status`

Documentation StorageGRID

"Opérations sur les compartiments"

"PutObject"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communséléments pour cette demande, plus les en-têtes supplémentaires suivants :

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `x-amz-checksum-sha256`
- `x-amz-server-side-encryption`
- `x-amz-storage-class`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-tagging`
- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-object-lock-legal-hold`
- `x-amz-meta-<metadata-name>`

Corps de la demande

- Données binaires de l'objet

Documentation StorageGRID

"PutObject"

"PutObjectLegalHold"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous paramètres et en-têtes communsces éléments pour cette demande.

Corps de la demande

StorageGRID prend en charge tous les paramètres du corps de demande définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation StorageGRID

"Utilisez l'API REST S3 pour configurer le verrouillage objet S3"

"PutObjectLockConfiguration"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous paramètres et en-têtes communsces éléments pour cette demande.

Corps de la demande

StorageGRID prend en charge tous les paramètres du corps de demande définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation StorageGRID

"Utilisez l'API REST S3 pour configurer le verrouillage objet S3"

"PutObjectRetention"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communséléments de cette demande, plus l'en-tête supplémentaire suivant :

- `x-amz-bypass-governance-retention`

Corps de la demande

StorageGRID prend en charge tous les paramètres du corps de demande définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation StorageGRID

"Utilisez l'API REST S3 pour configurer le verrouillage objet S3"

"Marquage PutObject"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous paramètres et en-têtes communsces éléments pour cette demande.

Corps de la demande

StorageGRID prend en charge tous les paramètres du corps de demande définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation StorageGRID

"Opérations sur les objets"

"Objet de restauration"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous paramètres et en-têtes communsces éléments pour cette demande.

Corps de la demande

Pour plus d'informations sur les champs de corps pris en charge, reportez-vous à la section "Objet de restauration".

"SelectObjectContent"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous paramètres et en-têtes communsces éléments pour cette demande.

Corps de la demande

Pour plus d'informations sur les champs de corps pris en charge, reportez-vous aux sections suivantes :

- "Utiliser S3 Select"
- "SelectObjectContent"

"UploadPart"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communséléments de cette demande, plus les paramètres de requête URI supplémentaires suivants :

- `partNumber`
- `uploadId`

Et ces en-têtes de demande supplémentaires :

- `x-amz-checksum-sha256`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`

Corps de la demande

- Données binaires de la pièce

Documentation StorageGRID

"UploadPart"

"UploadPartCopy"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communséléments de cette demande, plus les paramètres de requête URI supplémentaires suivants :

- `partNumber`
- `uploadId`

Et ces en-têtes de demande supplémentaires :

- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-modified-since`
- `x-amz-copy-source-if-none-match`

- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-range`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-copy-source-server-side-encryption-customer-algorithm`
- `x-amz-copy-source-server-side-encryption-customer-key`
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`

Corps de la demande

Aucune

Documentation StorageGRID

"UploadPartCopy"

Test de la configuration de l'API REST S3

Vous pouvez utiliser l'interface de ligne de commande d'Amazon Web Services pour tester votre connexion au système et vérifier que vous pouvez lire et écrire des objets.

Avant de commencer

- Vous avez téléchargé et installé l'interface de ligne de commande AWS à partir de "aws.amazon.com/cli".
- Si vous le souhaitez"créé un terminal d'équilibrage de charge", vous avez . Sinon, vous connaissez l'adresse IP du nœud de stockage auquel vous souhaitez vous connecter et le numéro de port à utiliser. Voir "Adresses IP et ports pour les connexions client".
- Vous avez "Compte de locataire S3 créé".
- Vous vous êtes connecté au locataire et "créé une clé d'accès"à .

Pour plus de détails sur ces étapes, reportez-vous "Configurer les connexions client"à la section .

Étapes

1. Configurez les paramètres de l'interface de ligne de commande AWS pour utiliser le compte que vous avez créé dans le système StorageGRID :
   a. Entrer en mode de configuration : `aws configure`
   b. Entrez l'ID de clé d'accès du compte que vous avez créé.
   c. Entrez la clé d'accès secrète pour le compte que vous avez créé.
   d. Entrez la région par défaut à utiliser. Par exemple `us-east-1`, .
   e. Entrez le format de sortie par défaut à utiliser ou appuyez sur **entrée** pour sélectionner JSON.
2. Créer un compartiment.

   Cet exemple suppose que vous avez configuré un noeud final d'équilibreur de charge pour utiliser l'adresse IP 10.96.101.17 et le port 10443.

```
aws s3api --endpoint-url https://10.96.101.17:10443
--no-verify-ssl create-bucket --bucket testbucket
```

Si le compartiment est créé avec succès, l'emplacement du compartiment est renvoyé, comme illustré dans l'exemple suivant :

```
"Location": "/testbucket"
```

3. Télécharger un objet.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
put-object --bucket testbucket --key s3.pdf --body C:\s3-
test\upload\s3.pdf
```

Si l'objet est téléchargé avec succès, un ETAG est renvoyé, qui est un hachage des données de l'objet.

4. Répertorier le contenu du compartiment pour vérifier que l'objet a été téléchargé.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
list-objects --bucket testbucket
```

5. Supprimez l'objet.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-object --bucket testbucket --key s3.pdf
```

6. Supprimer le compartiment.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-bucket --bucket testbucket
```

Implémentation de l'API REST S3 par StorageGRID

Requêtes des clients en conflit

Les demandes contradictoires des clients, telles que deux clients qui écrivent sur la même clé, sont résolues sur une base de « derniers-victoires ».

La chronologie de l'évaluation « derniers-victoires » repose sur la date à laquelle le système StorageGRID termine une demande donnée et non sur la date à laquelle les clients S3 commencent une opération.

Valeurs de cohérence

La cohérence assure un équilibre entre la disponibilité des objets et la cohérence de ces objets entre plusieurs nœuds de stockage et sites. Vous pouvez modifier la cohérence selon les besoins de votre application.

Par défaut, StorageGRID garantit la cohérence de lecture après écriture pour les nouveaux objets. Tout GET suivant un PUT réussi sera en mesure de lire les données nouvellement écrites. Les écrasements d'objets existants, les mises à jour de métadonnées et les suppressions sont cohérents. La propagation des écrasements ne prend généralement que quelques secondes ou minutes, mais peut prendre jusqu'à 15 jours.

Si vous souhaitez effectuer des opérations d'objet de manière différente, vous pouvez :

- Spécifiez une cohérence pour chaque godet.
- Spécifiez une cohérence pour Chaque opération d'API.
- Modifiez la cohérence par défaut à l'échelle de la grille en effectuant l'une des tâches suivantes :
  - Dans le Gestionnaire de grille, accédez à **CONFIGURATION** > **système** > **Paramètres de stockage** > **cohérence par défaut**.
  - .

> Une modification de la cohérence à l'échelle de la grille s'applique uniquement aux compartiments créés après la modification du paramètre. Pour déterminer les détails d'une modification, consultez le journal d'audit situé à l'adresse `/var/local/log` (recherchez **constencyLevel**).

Valeurs de cohérence

La cohérence affecte la façon dont les métadonnées utilisées par StorageGRID pour suivre les objets sont réparties entre les nœuds, et donc la disponibilité des objets pour les requêtes client.

Vous pouvez définir la cohérence d'une opération de compartiment ou d'API sur l'une des valeurs suivantes :

- **All** : tous les nœuds reçoivent immédiatement les données, sinon la demande échouera.
- **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.

Utilisez la cohérence « lecture après nouvelle écriture » et « disponible »

Lorsqu'une opération HEAD ou GET utilise la cohérence « Read-after-New-write », StorageGRID effectue la recherche en plusieurs étapes, comme suit :

- Il recherche tout d'abord l'objet à partir d'une faible cohérence.

- Si cette recherche échoue, elle répète la recherche à la valeur de cohérence suivante jusqu'à ce qu'elle atteigne une cohérence équivalente au comportement de Strong-global.

Si une opération HEAD ou GET utilise la cohérence « Read-after-New-write » mais que l'objet n'existe pas, la recherche d'objet atteint toujours une cohérence équivalente au comportement pour les opérations de type Strong-global. Cette cohérence exigeant la disponibilité de plusieurs copies des métadonnées d'objet sur chaque site, vous pouvez recevoir un nombre élevé d'erreurs de serveur interne 500 si deux nœuds de stockage ou plus sur le même site sont indisponibles.

À moins que vous ayez besoin de garanties de cohérence similaires à Amazon S3, vous pouvez empêcher ces erreurs pour les opérations HEAD et GET en définissant la cohérence sur « disponible ». Lorsqu'une opération HEAD ou GET utilise la cohérence « disponible », StorageGRID fournit uniquement la cohérence finale. Cette opération n'a pas abouti pour accroître la cohérence. Il n'est donc pas nécessaire que plusieurs copies des métadonnées de l'objet soient disponibles.

Indiquez la cohérence du fonctionnement de l'API

Pour définir la cohérence d'une opération d'API individuelle, les valeurs de cohérence doivent être prises en charge pour l'opération et vous devez spécifier la cohérence dans l'en-tête de la demande. Cet exemple définit la cohérence sur « site fort » pour une opération GetObject.

```
GET /bucket/object HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Consistency-Control: strong-site
```

> Vous devez utiliser la même cohérence pour les opérations PutObject et GetObject.

Spécifie la cohérence du compartiment

Pour définir la cohérence du compartiment, vous pouvez utiliser la requête StorageGRID"PRÉSERVER la cohérence du godet". Vous pouvez également "modifier la cohérence d'un compartiment"utiliser le Gestionnaire de locataires.

Lorsque vous définissez la cohérence d'un godet, tenez compte des points suivants :

- La cohérence d'un compartiment détermine la cohérence utilisée pour les opérations S3 exécutées sur les objets du compartiment ou sur la configuration du compartiment. Cela n'affecte pas les opérations du compartiment lui-même.
- La cohérence d'une opération d'API individuelle remplace la cohérence du compartiment.
- En général, les compartiments doivent utiliser la cohérence par défaut, « Read-after-New-write ». Si les demandes ne fonctionnent pas correctement, modifiez le comportement du client d'application si possible. Ou configurez le client de manière à spécifier la cohérence pour chaque requête d'API. Réglez la cohérence au niveau du godet uniquement en dernier recours.

[[comment les contrôles-cohérence-et-règles-ILM-interagissent]]Comment la cohérence et les règles ILM interagissent pour protéger les données

La cohérence et les règles ILM de votre choix affectent la protection des objets. Ces paramètres peuvent interagir.

Par exemple, la cohérence utilisée lorsqu'un objet est stocké affecte le placement initial des métadonnées d'objet, tandis que le comportement d'ingestion sélectionné pour la règle ILM affecte le placement initial des copies d'objet. Comme StorageGRID requiert l'accès aux métadonnées et aux données d'un objet pour répondre aux demandes des clients, le choix de niveaux de protection correspondants pour la cohérence et le comportement d'ingestion permet une meilleure protection initiale des données et des réponses système plus prévisibles.

Les éléments suivants "options d'ingestion" sont disponibles pour les règles ILM :

Double allocation
: StorageGRID effectue immédiatement des copies intermédiaires de l'objet et renvoie la réussite au client. Les copies spécifiées dans la règle ILM sont effectuées lorsque cela est possible.

Stricte
: Toutes les copies spécifiées dans la règle ILM doivent être effectuées avant que la réussite ne soit renvoyée au client.

Équilibré
: StorageGRID tente de faire toutes les copies spécifiées dans la règle ILM à l'entrée ; si cela n'est pas possible, des copies intermédiaires sont effectuées et le client est renvoyé avec succès. Les copies spécifiées dans la règle ILM sont effectuées lorsque cela est possible.

Exemple d'interaction entre la règle de cohérence et la règle ILM

Supposons que vous disposez d'un grid à deux sites avec la règle ILM suivante et la cohérence suivante :

- **Règle ILM** : créez deux copies d'objet, une sur le site local et une sur un site distant. Utiliser un comportement d'ingestion strict.
- **Cohérence** : fort-global (les métadonnées d'objet sont immédiatement distribuées à tous les sites).

Lorsqu'un client stocke un objet dans la grille, StorageGRID effectue à la fois des copies d'objet et distribue les métadonnées aux deux sites avant de rétablir la réussite du client.

L'objet est entièrement protégé contre la perte au moment du message d'ingestion. Par exemple, si le site local est perdu peu de temps après l'ingestion, des copies des données de l'objet et des métadonnées de l'objet existent toujours sur le site distant. L'objet est entièrement récupérable.

Si vous avez utilisé la même règle ILM et la même cohérence site forte, le client peut recevoir un message de réussite après la réplication des données de l'objet vers le site distant, mais avant la distribution des métadonnées de l'objet. Dans ce cas, le niveau de protection des métadonnées d'objet ne correspond pas au niveau de protection des données d'objet. Si le site local est perdu peu de temps après l'ingestion, les métadonnées d'objet sont perdues. Impossible de récupérer l'objet.

L'inter-relation entre la cohérence et les règles ILM peut être complexe. Contactez NetApp si vous avez besoin d'aide.

Gestion des versions d'objet

Vous pouvez définir l'état de gestion des versions d'un compartiment si vous souhaitez conserver plusieurs versions de chaque objet. L'activation de la gestion des versions pour un compartiment vous protège contre la suppression accidentelle d'objets et vous permet de récupérer et de restaurer des versions antérieures d'un objet.

Le système StorageGRID implémente la gestion des versions avec prise en charge de la plupart des fonctionnalités et avec certaines limites. StorageGRID prend en charge jusqu'à 10,000 versions de chaque objet.

Le contrôle de version d'objets peut être associé à la gestion du cycle de vie des informations (ILM) d'StorageGRID ou à la configuration du cycle de vie des compartiments S3. Vous devez explicitement activer la gestion des versions pour chaque compartiment. Lorsque la gestion des versions est activée pour un compartiment, un ID de version est attribué à chaque objet ajouté au compartiment, qui est généré par le système StorageGRID.

La suppression de l'authentification multifacteur (MFA) n'est pas prise en charge.

> Le contrôle de version ne peut être activé que pour les compartiments créés avec StorageGRID version 10.3 ou ultérieure.

ILM et gestion des versions

Les règles ILM sont appliquées à chaque version d'un objet. Un processus d'analyse ILM analyse en continu tous les objets, puis les évalue à nouveau en fonction de la règle ILM actuelle. Toute modification apportée aux règles ILM est appliquée à tous les objets précédemment ingérées. Ceci inclut les versions préalablement ingérées si la gestion des versions est activée. L'analyse ILM applique les modifications de l'ILM aux objets précédemment ingérées.

Pour les objets S3 dans les compartiments avec gestion des versions, la prise en charge de la gestion des versions vous permet de créer des règles ILM qui utilisent « Noncurrent Time » comme heure de référence (sélectionnez **Yes** pour la question « Apply this rule to Older object versions only? » "Étape 1 de l'assistant de création de règles ILM"(Appliquer cette règle aux versions d'objets plus anciennes uniquement ?) dans la section). Lorsqu'un objet est mis à jour, ses versions précédentes deviennent non actuelles. L'utilisation d'un filtre « Noncurrent Time » vous permet de créer des stratégies qui réduisent l'impact sur le stockage des versions précédentes des objets.

> Lorsque vous téléchargez une nouvelle version d'un objet à l'aide d'une opération de téléchargement partitionné, l'heure qui n'est pas à jour pour la version d'origine de l'objet correspond à la création du téléchargement partitionné pour la nouvelle version, et non à la fin du téléchargement partitionné. Dans des cas limités, l'heure non actuelle de la version d'origine peut être des heures ou des jours plus tôt que l'heure de la version actuelle.

Informations associées

- "Suppression d'objets avec version S3"
- "Règles et règles ILM pour les objets avec version S3 (exemple 4)".

Utilisez l'API REST S3 pour configurer le verrouillage objet S3

Si le paramètre global de verrouillage des objets S3 est activé pour votre système StorageGRID, vous pouvez créer des compartiments avec le verrouillage des objets S3 activé. Vous pouvez spécifier des paramètres de conservation par défaut pour chaque compartiment ou pour chaque version d'objet.

Activation du verrouillage objet S3 pour un compartiment

Si le paramètre global de verrouillage d'objet S3 est activé pour votre système StorageGRID, vous pouvez activer le verrouillage d'objet S3 lorsque vous créez chaque compartiment.

Le verrouillage objet S3 est un paramètre permanent qui ne peut être activé que lorsque vous créez un compartiment. Une fois un compartiment créé, vous ne pouvez ni ajouter ni désactiver le verrouillage objet S3.

Pour activer le verrouillage objet S3 pour un compartiment, utilisez l'une des méthodes suivantes :

- Créez le compartiment à l'aide du Gestionnaire des locataires. Voir "Créer un compartiment S3".
- Créez le compartiment à l'aide d'une demande CreateBucket avec l' `x-amz-bucket-object-lock-enabled`en-tête de la demande. Voir "Opérations sur les compartiments".

Le verrouillage objet S3 requiert la gestion des versions des compartiments, qui est automatiquement activée lors de la création du compartiment. Vous ne pouvez pas suspendre la gestion des versions pour le compartiment. Voir "Gestion des versions d'objet".

Paramètres de conservation par défaut d'un compartiment

Lorsque le verrouillage objet S3 est activé pour un compartiment, vous pouvez éventuellement activer la conservation par défaut du compartiment et spécifier un mode de conservation par défaut et une période de conservation par défaut.

Mode de rétention par défaut

- En mode CONFORMITÉ :
  - L'objet ne peut pas être supprimé tant que sa date de conservation jusqu'à n'est pas atteinte.
  - La date de conservation de l'objet peut être augmentée, mais elle ne peut pas être réduite.
  - La date de conservation de l'objet jusqu'à ne peut pas être supprimée tant que cette date n'est pas atteinte.
- En mode GOUVERNANCE :
  - Les utilisateurs disposant de l' `s3:BypassGovernanceRetention`autorisation peuvent utiliser l' `x-amz-bypass-governance-retention: true`en-tête de la demande pour contourner les paramètres de rétention.
  - Ces utilisateurs peuvent supprimer une version d'objet avant d'atteindre sa date de conservation jusqu'à.
  - Ces utilisateurs peuvent augmenter, diminuer ou supprimer la date de conservation d'un objet.

Période de conservation par défaut

Une période de conservation par défaut peut être spécifiée en années ou en jours pour chaque compartiment.

Comment définir la conservation par défaut d'un compartiment

Pour définir la rétention par défaut d'un compartiment, utilisez l'une des méthodes suivantes :

- Gérez les paramètres de compartiment depuis le gestionnaire de locataires. Voir "Créer un compartiment S3" et "Mettre à jour la conservation par défaut du verrouillage d'objet S3".
- Exécutez une demande PutObjectLockConfiguration pour que le compartiment indique le mode par défaut et le nombre de jours ou d'années par défaut.

PutObjectLockConfiguration

La demande PutObjectLockConfiguration vous permet de définir et de modifier le mode de rétention par défaut et la période de rétention par défaut pour un compartiment pour lequel S3 Object Lock est activé. Vous pouvez également supprimer les paramètres de conservation par défaut configurés précédemment.

Lorsque de nouvelles versions d'objet sont ingérées dans le compartiment, le mode de conservation par défaut est appliqué si `x-amz-object-lock-mode` et `x-amz-object-lock-retain-until-date` n'est pas spécifié. La période de conservation par défaut est utilisée pour calculer la date de conservation jusqu'à si `x-amz-object-lock-retain-until-date` n'est pas spécifiée.

Si la période de conservation par défaut est modifiée après l'ingestion d'une version d'objet, la conservation à la date de la version de l'objet reste la même et n'est pas recalculée en utilisant la nouvelle période de conservation par défaut.

Vous devez disposer de l' `s3:PutBucketObjectLockConfiguration`autorisation, ou être root, pour effectuer cette opération.

L' `Content-MD5`en-tête de la demande doit être spécifié dans la demande PUT.

Exemple de demande

Cet exemple active le verrouillage objet S3 pour un compartiment et définit le mode de conservation par défaut sur CONFORMITÉ et la période de conservation par défaut sur 6 ans.

```
PUT /bucket?object-lock HTTP/1.1
Accept-Encoding: identity
Content-Length: 308
Host: host
Content-MD5: request header
User-Agent: s3sign/1.0.0 requests/2.24.0 python/3.8.2
X-Amz-Date: date
X-Amz-Content-SHA256: authorization-string
Authorization: authorization-string

<ObjectLockConfiguration>
    <ObjectLockEnabled>Enabled</ObjectLockEnabled>
    <Rule>
        <DefaultRetention>
            <Mode>COMPLIANCE</Mode>
            <Years>6</Years>
        </DefaultRetention>
    </Rule>
</ObjectLockConfiguration>
```

Comment déterminer la conservation par défaut d'un compartiment

Pour déterminer si le verrouillage objet S3 est activé pour un compartiment et pour afficher le mode de conservation et la période de conservation par défaut, utilisez l'une des méthodes suivantes :

- Affichez le compartiment dans le gestionnaire de locataires. Voir "Afficher les compartiments S3".
- Émettre une demande GetObjectLockConfiguration.

GetObjectLockConfiguration

La demande GetObjectLockConfiguration vous permet de déterminer si le verrouillage d'objet S3 est activé pour un compartiment et, si ce dernier est activé, vérifiez s'il existe un mode de rétention et une période de rétention par défaut configurés pour le compartiment.

Lorsque de nouvelles versions d'objet sont ingérées dans le compartiment, le mode de conservation par défaut est appliqué si `x-amz-object-lock-mode` n'est pas spécifié. La période de conservation par défaut est utilisée pour calculer la date de conservation jusqu'à si `x-amz-object-lock-retain-until-date` n'est pas spécifiée.

Vous devez disposer de l' `s3:GetBucketObjectLockConfiguration`autorisation, ou être root, pour effectuer cette opération.

Exemple de demande

```
GET /bucket?object-lock HTTP/1.1
Host: host
Accept-Encoding: identity
User-Agent: aws-cli/1.18.106 Python/3.8.2 Linux/4.4.0-18362-Microsoft
botocore/1.17.29
x-amz-date: date
x-amz-content-sha256: authorization-string
Authorization: authorization-string
```

Exemple de réponse

```
HTTP/1.1 200 OK
x-amz-id-2:
iVmcB7OXXJRkRH1FiVq1151/T24gRfpwpuZrEG11Bb9ImOMAAe98oxSpXlknabA0LTvBYJpSIX
k=
x-amz-request-id: B34E94CACB2CEF6D
Date: Fri, 04 Sep 2020 22:47:09 GMT
Transfer-Encoding: chunked
Server: AmazonS3

<?xml version="1.0" encoding="UTF-8"?>
<ObjectLockConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
    <ObjectLockEnabled>Enabled</ObjectLockEnabled>
    <Rule>
        <DefaultRetention>
            <Mode>COMPLIANCE</Mode>
            <Years>6</Years>
        </DefaultRetention>
    </Rule>
</ObjectLockConfiguration>
```

Comment spécifier les paramètres de conservation d'un objet

Un compartiment lorsque le verrouillage objet S3 est activé peut contenir une combinaison d'objets avec ou sans paramètres de conservation du verrouillage objet S3.

Les paramètres de conservation au niveau objet sont spécifiés à l'aide de l'API REST S3. Les paramètres de conservation d'un objet remplacent les paramètres de conservation par défaut du compartiment.

Vous pouvez spécifier les paramètres suivants pour chaque objet :

- **Mode de conservation** : CONFORMITÉ ou GOUVERNANCE.
- **Conserver-jusqu'à-date** : une date spécifiant la durée pendant laquelle la version de l'objet doit être conservée par StorageGRID.
  - En mode CONFORMITÉ, si la date de conservation jusqu'à est dans le futur, l'objet peut être récupéré, mais il ne peut pas être modifié ou supprimé. La date de conservation jusqu'à peut être augmentée, mais cette date ne peut pas être réduite ou supprimée.
  - En mode GOUVERNANCE, les utilisateurs disposant d'une autorisation spéciale peuvent contourner le paramètre conserver jusqu'à la date. Ils peuvent supprimer une version d'objet avant la fin de sa période de conservation. Ils peuvent également augmenter, diminuer ou même supprimer la date de conservation jusqu'à.
- **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.

  Le paramètre de conservation légale d'un objet est indépendant du mode de conservation et de la date de conservation jusqu'à. Si une version d'objet est en attente légale, personne ne peut supprimer cette version.

Pour spécifier les paramètres de verrouillage d'objet S3 lors de l'ajout d'une version d'objet à un compartiment, émettez une "PutObject", "Objet de copie"ou "CreateMultipartUpload" une demande.

Vous pouvez utiliser les éléments suivants :

- `x-amz-object-lock-mode`, Qui peut être CONFORMITÉ ou GOUVERNANCE (sensible à la casse).

  > Si vous spécifiez `x-amz-object-lock-mode`, vous devez également spécifier `x-amz-object-lock-retain-until-date`.

- `x-amz-object-lock-retain-until-date`
  - La valeur conserver jusqu'à la date doit être au format `2020-08-10T21:46:00Z`. Les secondes fractionnaires sont autorisées, mais seuls 3 chiffres après la virgule sont conservés (précision des millisecondes). Les autres formats ISO 8601 ne sont pas autorisés.
  - La date de conservation doit être ultérieure.
- `x-amz-object-lock-legal-hold`

  Si la conservation légale est ACTIVÉE (sensible à la casse), l'objet est placé sous une obligation légale. Si la mise en attente légale est désactivée, aucune mise en attente légale n'est mise. Toute autre valeur entraîne une erreur 400 Bad Request (InvalidArgument).

Si vous utilisez l'un de ces en-têtes de demande, tenez compte des restrictions suivantes :

- L'`Content-MD5`en-tête de requête est requis si un `x-amz-object-lock-*` en-tête de requête est présent dans la requête PutObject. `Content-MD5` N'est pas nécessaire pour CopyObject ou CreateMultipartUpload.
- Si S3 Object Lock n'est pas activé dans le compartiment et qu'un `x-amz-object-lock-*` en-tête de requête est présent, une erreur 400 Bad Request (InvalidRequest) est renvoyée.
- La requête PutObject prend en charge l'utilisation de `x-amz-storage-class: REDUCED_REDUNDANCY` pour faire correspondre le comportement AWS. Cependant, lors de l'ingestion d'un objet dans un compartiment lorsque le verrouillage objet S3 est activé, StorageGRID effectue toujours une entrée à double validation.
- Une réponse ultérieure à la version GET ou HeadObject inclura les en-têtes `x-amz-object-lock-mode`, , `x-amz-object-lock-retain-until-date` et `x-amz-object-lock-legal-hold`, s'il est configuré et si l'expéditeur de la demande a les autorisations correctes `s3:Get*`.

Vous pouvez utiliser la `s3:object-lock-remaining-retention-days` clé de condition de règle pour limiter les périodes de conservation minimale et maximale autorisée pour vos objets.

Comment mettre à jour les paramètres de conservation d'un objet

Si vous devez mettre à jour les paramètres de conservation légale ou de conservation d'une version d'objet existante, vous pouvez effectuer les opérations de sous-ressource d'objet suivantes :

- `PutObjectLegalHold`

  Si la nouvelle valeur de conservation légale est ACTIVÉE, l'objet est placé sous une mise en attente légale. Si la valeur de retenue légale est OFF, la suspension légale est levée.

- `PutObjectRetention`
  - La valeur du mode peut être CONFORMITÉ ou GOUVERNANCE (sensible à la casse).
  - La valeur conserver jusqu'à la date doit être au format `2020-08-10T21:46:00Z`. Les secondes fractionnaires sont autorisées, mais seuls 3 chiffres après la virgule sont conservés (précision des millisecondes). Les autres formats ISO 8601 ne sont pas autorisés.
  - Si une version d'objet possède une date de conservation existante, vous pouvez uniquement l'augmenter. La nouvelle valeur doit être future.

Comment utiliser le mode GOUVERNANCE

Les utilisateurs disposant de cette `s3:BypassGovernanceRetention` autorisation peuvent contourner les paramètres de rétention actifs d'un objet qui utilise le mode de GOUVERNANCE. Toutes les opérations de SUPPRESSION ou de PutObjectRetention doivent inclure l' `x-amz-bypass-governance-retention:true`en-tête de la demande. Ces utilisateurs peuvent effectuer les opérations supplémentaires suivantes :

- Exécutez les opérations DeleteObject ou DeleteObjects pour supprimer une version d'objet avant que sa période de rétention ne soit écoulée.

  Impossible de supprimer les objets qui sont en attente légale. La mise en attente légale doit être désactivée.

- Exécutez des opérations PutObjectRetention qui changent le mode d'une version d'objet de GOUVERNANCE à CONFORMITÉ avant que la période de conservation de l'objet ne soit écoulée.

Le passage du mode DE CONFORMITÉ À LA GOUVERNANCE n'est jamais autorisé.

- Exécutez les opérations PutObjectRetention pour augmenter, diminuer ou supprimer la période de rétention d'une version d'objet.

Informations associées

- "Gestion des objets avec le verrouillage d'objets S3"
- "Utilisez le verrouillage d'objet S3 pour conserver les objets"
- "Guide de l'utilisateur d'Amazon simple Storage Service : verrouillage d'objets"

Création de la configuration du cycle de vie S3

Vous pouvez créer une configuration de cycle de vie S3 afin de contrôler la suppression d'objets spécifiques du système StorageGRID.

L'exemple simple de cette section illustre la façon dont une configuration du cycle de vie S3 peut contrôler la suppression de certains objets (expirés) dans des compartiments S3 spécifiques. L'exemple de cette section est fourni à titre d'illustration uniquement. Pour plus d'informations sur la création de configurations de cycle de vie S3, reportez-vous à la section "Guide de l'utilisateur d'Amazon simple Storage Service : gestion du cycle de vie des objets". Notez que StorageGRID prend uniquement en charge les actions d'expiration, mais pas les actions de transition.

La configuration du cycle de vie

La configuration du cycle de vie est un ensemble de règles appliquées aux objets dans des compartiments S3 spécifiques. Chaque règle indique quels objets sont affectés et quand ces objets vont expirer (à une date spécifique ou après un certain nombre de jours).

StorageGRID prend en charge jusqu'à 1,000 règles de cycle de vie dans une configuration cycle de vie. Chaque règle peut inclure les éléments XML suivants :

- Expiration : supprimez un objet lorsqu'une date spécifiée est atteinte ou lorsqu'un nombre de jours spécifié est atteint, à partir de l'ingestion de l'objet.
- NonactuelVersionExexpiration : supprimez un objet lorsque le nombre de jours spécifié est atteint, à partir de quand l'objet est devenu non courant.
- Filtre (préfixe, étiquette)
- État
- ID

Chaque objet respecte les paramètres de conservation du cycle de vie d'un compartiment S3 ou une règle ILM. Lorsqu'un cycle de vie d'un compartiment S3 est configuré, les actions d'expiration du cycle de vie remplacent la règle ILM pour les objets correspondant au filtre de cycle de vie du compartiment. Les objets qui ne correspondent pas au filtre de cycle de vie des compartiments utilisent les paramètres de conservation de la règle ILM. Si un objet correspond à un filtre de cycle de vie de compartiment et qu'aucune action d'expiration n'est explicitement spécifiée, les paramètres de conservation de la règle ILM ne sont pas utilisés et les versions d'objet sont conservées indéfiniment. Voir "Exemples de priorités pour le cycle de vie des compartiments S3 et les règles ILM".

Par conséquent, il est possible de supprimer un objet de la grille, même si les instructions de placement d'une règle ILM s'appliquent toujours à l'objet. Il est également possible de conserver un objet dans la grille même après l'expiration des instructions de placement ILM de l'objet. Pour plus de détails, voir "Fonctionnement de

ILM tout au long de la vie d'un objet".

> La configuration du cycle de vie des compartiments avec des compartiments dont le verrouillage objet S3 est activé, mais la configuration du cycle de vie des compartiments n'est pas prise en charge pour les compartiments conformes.

StorageGRID prend en charge les opérations suivantes des compartiments pour gérer les configurations du cycle de vie :

- DeleteBuckeLifecycle
- GetBucketLifecycleConfiguration
- PutBucketLifecycleConfiguration

Créer une configuration de cycle de vie

Comme première étape de la création de la configuration du cycle de vie, vous créez un fichier JSON qui inclut une ou plusieurs règles. Par exemple, ce fichier JSON contient trois règles, comme suit :

1. La règle 1 s'applique uniquement aux objets qui correspondent au préfixe `category1/` et qui ont une `key2` valeur de `tag2`. Le `Expiration` paramètre indique que les objets correspondant au filtre expireront à minuit le 22 août 2020.
2. La règle 2 s'applique uniquement aux objets qui correspondent au préfixe `category2/`. Le `Expiration` paramètre indique que les objets correspondant au filtre expireront 100 jours après leur ingestion.

   > Les règles spécifiant un nombre de jours sont relatives à l'ingestion de l'objet. Si la date actuelle dépasse la date d'ingestion et le nombre de jours, certains objets peuvent être supprimés du compartiment dès que la configuration de cycle de vie est appliquée.

3. La règle 3 s'applique uniquement aux objets qui correspondent au préfixe `category3/`. Le `Expiration` paramètre spécifie que toute version non actuelle des objets correspondants expirera 50 jours après qu'ils ne soient plus à jour.

```
{
    "Rules": [
        {
            "ID": "rule1",
            "Filter": {
                "And": {
                    "Prefix": "category1/",
                    "Tags": [
                        {
                            "Key": "key2",
                            "Value": "tag2"
                        }
                    ]
                }
            },
            "Expiration": {
                "Date": "2020-08-22T00:00:00Z"
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule2",
            "Filter": {
                "Prefix": "category2/"
            },
            "Expiration": {
                "Days": 100
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule3",
            "Filter": {
                "Prefix": "category3/"
            },
            "NoncurrentVersionExpiration": {
                "NoncurrentDays": 50
            },
            "Status": "Enabled"
        }
    ]
}
```

Appliquez la configuration du cycle de vie au compartiment

Après avoir créé le fichier de configuration du cycle de vie, vous l'appliquez à un compartiment en émettant une demande PutBucketLifecycleConfiguration.

Cette requête applique la configuration de cycle de vie du fichier d'exemple aux objets d'un compartiment nommé `testbucket`.

```
aws s3api --endpoint-url <StorageGRID endpoint> put-bucket-lifecycle-
configuration
--bucket testbucket --lifecycle-configuration file://bktjson.json
```

Pour vérifier qu'une configuration de cycle de vie a été correctement appliquée au compartiment, exécutez une demande GetBucketLifecycleConfiguration. Par exemple :

```
aws s3api --endpoint-url <StorageGRID endpoint> get-bucket-lifecycle-
configuration
 --bucket testbucket
```

Une réponse réussie répertorie la configuration de cycle de vie que vous venez d'appliquer.

Vérifiez que l'expiration du cycle de vie du compartiment s'applique à l'objet

Vous pouvez déterminer si une règle d'expiration dans la configuration de cycle de vie s'applique à un objet spécifique lors de l'émission d'une requête PutObject, HeadObject ou GetObject. Si une règle s'applique, la réponse inclut un `Expiration` paramètre qui indique quand l'objet expire et quelle règle d'expiration a été mise en correspondance.

> Étant donné que le cycle de vie d'un compartiment remplace ILM, la `expiry-date` date affichée est la date réelle à laquelle l'objet sera supprimé. Pour plus de détails, voir "Méthode de détermination de la conservation des objets".

Par exemple, cette requête PutObject a été émise le 22 juin 2020 et place un objet dans le `testbucket` compartiment.

```
aws s3api --endpoint-url <StorageGRID endpoint> put-object
--bucket testbucket --key obj2test2 --body bktjson.json
```

La réponse de réussite indique que l'objet expirera dans 100 jours (01 oct 2020) et qu'il correspond à la règle 2 de la configuration de cycle de vie.

```
{
      *"Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:49 GMT\", rule-
id=\"rule2\"",
      "ETag": "\"9762f8a803bc34f5340579d4446076f7\""
}
```

Par exemple, cette requête HeadObject a été utilisée pour obtenir les métadonnées du même objet dans le compartiment testbucket.

```
aws s3api --endpoint-url <StorageGRID endpoint> head-object
--bucket testbucket --key obj2test2
```

La réponse de réussite inclut les métadonnées de l'objet et indique que l'objet expirera dans 100 jours et qu'il correspond à la règle 2.

```
{
      "AcceptRanges": "bytes",
      *"Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:48 GMT\", rule-
id=\"rule2\"",
      "LastModified": "2020-06-23T09:07:48+00:00",
      "ContentLength": 921,
      "ETag": "\"9762f8a803bc34f5340579d4446076f7\""
      "ContentType": "binary/octet-stream",
      "Metadata": {}
}
```

Pour les compartiments avec gestion des versions, l' `x-amz-expiration`en-tête de réponse s'applique uniquement aux versions actuelles des objets.

Recommandations pour l'implémentation de l'API REST S3

Suivez ces recommandations lors de l'implémentation de l'API REST S3 pour une utilisation avec StorageGRID.

Recommandations pour les têtes à des objets inexistants

Si votre application vérifie régulièrement si un objet existe dans un chemin où vous ne vous attendez pas à ce que l'objet existe réellement, vous devez utiliser le "disponible" "la cohérence". Par exemple, vous devez utiliser la cohérence « disponible » si votre application se trouve en tête d'emplacement avant de la METTRE EN PLACE.

Sinon, si l'opération HEAD ne trouve pas l'objet, vous risquez de recevoir un nombre élevé d'erreurs de serveur interne 500 si deux nœuds de stockage ou plus sur le même site sont indisponibles ou si un site distant est inaccessible.

Vous pouvez définir la cohérence « disponible » pour chaque compartiment à l'aide de la "PRÉSERVER la

cohérence du godet" requête ou spécifier la cohérence dans l'en-tête de demande pour une opération d'API individuelle.

Recommandations pour les clés d'objet

Suivez ces recommandations pour les noms de clés d'objet, en fonction de la date de création du compartiment.

Compartiments créés dans StorageGRID 11.4 ou version antérieure

- N'utilisez pas de valeurs aléatoires comme les quatre premiers caractères des clés d'objet. Cela contraste avec l'ancienne recommandation AWS pour les préfixes de clés. Utilisez plutôt des préfixes non aléatoires et non uniques, tels que `image`.
- Si vous suivez les recommandations d'AWS pour utiliser des caractères aléatoires et uniques dans les préfixes de clés, préfixez les clés d'objet à l'aide d'un nom de répertoire. C'est-à-dire, utilisez le format suivant :

  ```
  mybucket/mydir/f8e3-image3132.jpg
  ```

  Au lieu de ce format :

  ```
  mybucket/f8e3-image3132.jpg
  ```

Compartiments créés dans StorageGRID 11.4 ou version ultérieure

Il n'est pas nécessaire de restreindre les noms de clés d'objet pour répondre aux bonnes pratiques de performances. Dans la plupart des cas, vous pouvez utiliser des valeurs aléatoires pour les quatre premiers caractères des noms de clé d'objet.

> À cela s'exception près un workload S3 qui supprime en continu tous les objets après une courte période de temps. Pour minimiser l'impact sur les performances de ce cas d'utilisation, il est possible de faire varier la première partie du nom de clé tous les mille objets avec une date comme la date. Supposons par exemple qu'un client S3 écrit généralement 2,000 objets/seconde et que la règle de cycle de vie ILM ou compartiment supprime tous les objets au bout de trois jours. Pour réduire l'impact sur les performances, vous pouvez nommer les clés comme suit : `/mybucket/mydir/`*`yyyymmddhhmmss-random_UUID`*`.jpg`

Recommandations pour les « lectures de plage »

Si "option globale pour compresser les objets stockés"est activé, les applications client S3 doivent éviter d'effectuer des opérations GetObject qui spécifient une plage d'octets. Ces opérations de « lecture de plage » sont inefficaces car StorageGRID doit décompresser efficacement les objets pour accéder aux octets demandés. Les opérations GetObject qui demandent une petite plage d'octets à partir d'un objet très volumineux sont particulièrement inefficaces ; par exemple, il est inefficace de lire une plage de 10 Mo à partir d'un objet compressé de 50 Go.

Si les plages sont lues à partir d'objets compressés, les demandes client peuvent être en attente.

> Si vous devez compresser des objets et que votre application client doit utiliser des lectures de plage, augmentez le délai de lecture de l'application.

Prise en charge de l'API REST Amazon S3

Détails de l'implémentation de l'API REST S3

Le système StorageGRID implémente l'API simple Storage Service (API version 2006-03-01) avec la prise en charge de la plupart des opérations et avec certaines limites. Vous devez connaître les détails d'implémentation lorsque vous intégrez des applications client de l'API REST S3.

Le système StorageGRID prend en charge les demandes de type hébergement virtuel et les demandes de type chemin d'accès.

Traitement de la date

L'implémentation StorageGRID de l'API REST S3 ne prend en charge que les formats de date HTTP valides.

Le système StorageGRID prend uniquement en charge les formats de date HTTP valides pour tous les en-têtes qui acceptent les valeurs de date. La partie heure de la date peut être spécifiée au format heure de Greenwich (GMT) ou au format heure coordonnée universelle (UTC) sans décalage de fuseau horaire (+0000 doit être spécifié). Si vous incluez l' `x-amz-date`en-tête dans votre demande, il remplace toute valeur spécifiée dans l'en-tête de la demande de date. Lors de l'utilisation de la signature AWS version 4, l' `x-amz-date`en-tête doit être présent dans la demande signée car l'en-tête de date n'est pas pris en charge.

En-têtes de demande commune

Le système StorageGRID prend en charge les en-têtes de requête communs définis par "Référence de l'API Amazon simple Storage Service : en-têtes de demande communs", à une exception près.

En-tête de demande	Mise en place
Autorisation	Prise en charge complète de la signature AWS version 2 Prise en charge de la signature AWS version 4, à l'exception des cas suivants : • Lorsque vous fournissez la valeur de somme de contrôle de charge utile réelle dans `x-amz-content-sha256`, la valeur est acceptée sans validation, comme si la valeur `UNSIGNED-PAYLOAD` avait été fournie pour l'en-tête. Lorsque vous fournissez une `x-amz-content-sha256` valeur d'en-tête qui implique le `aws-chunked` STREAMING (par exemple, STREAMING-AWS4-HMAC-SHA256-PAYLOAD), les signatures des blocs ne sont pas vérifiées par rapport aux données des blocs.
jeton de sécurité x-amz	Non mis en œuvre. Renvoie `XNotImplemented`.

En-têtes de réponse commune

Le système StorageGRID prend en charge tous les en-têtes de réponse courants définis par l'API *simple Storage Service Reference*, à une exception près.

En-tête de réponse	Mise en place
x-amz-id-2	Non utilisé

Authentifier les demandes

Le système StorageGRID prend en charge l'accès authentifié et anonyme aux objets à l'aide de l'API S3.

L'API S3 prend en charge la version 2 de Signature et la version 4 de Signature pour authentifier les requêtes API S3.

Les demandes authentifiées doivent être signées à l'aide de votre ID de clé d'accès et de votre clé secrète d'accès.

Le système StorageGRID prend en charge deux méthodes d'authentification : l'en-tête HTTP `Authorization` et l'utilisation des paramètres de requête.

Utilisez l'en-tête HTTP Authorization

L'en-tête HTTP `Authorization` est utilisé par toutes les opérations de l'API S3, à l'exception des requêtes anonymes lorsque cela est autorisé par la stratégie de compartiment. L' `Authorization`en-tête contient toutes les informations de signature requises pour authentifier une demande.

Utiliser les paramètres de requête

Vous pouvez utiliser les paramètres de requête pour ajouter des informations d'authentification à une URL. Il s'agit de la présignature de l'URL, qui peut être utilisée pour accorder un accès temporaire à des ressources spécifiques. Les utilisateurs avec l'URL présignée n'ont pas besoin de connaître la clé d'accès secrète pour accéder à la ressource, ce qui vous permet de fournir un accès limité tiers à une ressource.

Opérations sur le service

Le système StorageGRID prend en charge les opérations suivantes sur ce service.

Fonctionnement	Mise en place
Listseaux (Anciennement appelé GET Service)	Mise en œuvre avec tout le comportement de l'API REST Amazon S3. D'être modifiées sans préavis.
DÉCOUVREZ l'utilisation du stockage	La demande StorageGRID "DÉCOUVREZ l'utilisation du stockage"indique la quantité totale de stockage utilisée par un compte et pour chaque compartiment associé au compte. Il s'agit d'une opération sur le service avec un chemin d'accès de / et un paramètre de requête personnalisée (`?x-ntap-sg-usage`) ajouté.

Fonctionnement	Mise en place
OPTIONS /	Les applications client peuvent émettre `OPTIONS /` des requêtes vers le port S3 d'un nœud de stockage, sans identifiants d'authentification S3, pour déterminer si le nœud de stockage est disponible. Vous pouvez utiliser cette requête pour la surveillance ou permettre aux équilibreurs de charge externes d'identifier lorsqu'un nœud de stockage est arrêté.

Opérations sur les compartiments

Le système StorageGRID prend en charge un maximum de 5,000 compartiments pour chaque compte de locataire S3.

Chaque grille peut contenir un maximum de 100,000 compartiments.

Pour prendre en charge 5,000 compartiments, chaque nœud de stockage de la grille doit disposer d'au moins 64 Go de RAM.

Les restrictions relatives aux noms de compartiment respectent les restrictions régionales standard AWS, mais vous devez les restreindre à une nomenclature DNS pour prendre en charge les demandes de type hébergement virtuel S3.

Pour plus d'informations, reportez-vous aux sections suivantes :

- "Guide de l'utilisateur d'Amazon simple Storage Service : quotas de compartiments, restrictions et limites"
- "Configuration des noms de domaine de terminaux S3"

Les opérations ListObjects (GET Bucket) et ListObjectVersions (GET Bucket object versions) prennent en charge StorageGRID "valeurs de cohérence".

Vous pouvez vérifier si les mises à jour de l'heure du dernier accès sont activées ou désactivées pour les compartiments individuels. Voir "HEURE du dernier accès au compartiment".

Le tableau suivant décrit la façon dont StorageGRID implémente les opérations des compartiments de l'API REST S3. Pour effectuer l'une de ces opérations, les informations d'identification d'accès nécessaires doivent être fournies pour le compte.

Fonctionnement	Mise en place
CreateBucket	Crée un nouveau compartiment. C'est en créant le compartiment que vous devenez le propriétaire. • 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 et 63 caractères. ◦ Peut être une série d'une ou plusieurs étiquettes, avec des étiquettes adjacentes séparées par un point. 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 ressembler à une adresse IP au format texte. ◦ 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. • Par défaut, les compartiments sont créés dans la `us-east-1` région ; vous pouvez cependant utiliser `LocationConstraint` l'élément de demande du corps de la demande pour spécifier une région différente. Lorsque vous utilisez l' `LocationConstraint`élément, vous devez spécifier le nom exact d'une région qui a été définie à l'aide du Gestionnaire de grille ou de l'API de gestion de grille. Contactez votre administrateur système si vous ne connaissez pas le nom de région que vous devez utiliser. **Remarque** : une erreur se produit si votre requête CreateBucket utilise une région qui n'a pas été définie dans StorageGRID. • Vous pouvez inclure l' `x-amz-bucket-object-lock-enabled`en-tête de demande pour créer un compartiment lorsque le verrouillage objet S3 est activé. Voir "Utilisez l'API REST S3 pour configurer le verrouillage objet S3". Vous devez activer le verrouillage d'objet S3 lors de la création du compartiment. Une fois un compartiment créé, vous ne pouvez ni ajouter ni désactiver le verrouillage objet S3. Le verrouillage objet S3 requiert la gestion des versions de compartiment, qui est activée automatiquement lors de la création du compartiment.
DeleteBucket	Supprime le godet.
DeleteBuckeCors	Supprime la configuration CORS pour le godet.
DeleteBuckeEncryption	Supprime le chiffrement par défaut du compartiment. Les objets chiffrés existants restent chiffrés, mais aucun nouvel objet ajouté au compartiment n'est chiffré.
DeleteBuckeLifecycle	Supprime la configuration du cycle de vie du compartiment. Voir "Création de la configuration du cycle de vie S3".

Fonctionnement	Mise en place
DeleteBucketPolicy	Supprime la règle associée au compartiment.
DeleteBuckeReplication	Supprime la configuration de réplication attachée au compartiment.
DeleteBucketTagging	Utilise la `tagging` sous-ressource pour supprimer toutes les balises d'un compartiment. **Attention** : si une balise de stratégie ILM non définie par défaut est définie pour ce compartiment, une balise de compartiment sera affectée à cette `NTAP-SG-ILM-BUCKET-TAG` variable. N'émettez pas de demande DeleteBucketTagging s'il existe une `NTAP-SG-ILM-BUCKET-TAG` balise de compartiment. À la place, lancez une demande PutBucketTagging avec uniquement la `NTAP-SG-ILM-BUCKET-TAG` balise et sa valeur attribuée pour supprimer toutes les autres balises du compartiment. Ne pas modifier ou retirer l' `NTAP-SG-ILM-BUCKET-TAG`étiquette de godet.
GetBucketAcl	Renvoie une réponse positive et l'ID, DisplayName et l'autorisation du propriétaire du compartiment, indiquant que le propriétaire a un accès complet au compartiment.
GetBucketCors	Renvoie la `cors` configuration du compartiment.
GetBucketEncryption	Renvoie la configuration de chiffrement par défaut du compartiment.
GetBucketLifecycleConfiguration (Anciennement appelé cycle de vie du compartiment GET)	Renvoie la configuration du cycle de vie du compartiment. Voir "Création de la configuration du cycle de vie S3".
GetBuckeLocation	Renvoie la région définie à l'aide de l' `LocationConstraint`élément dans la requête `CreateBucket`. Si la région du compartiment est, une chaîne vide est `us-east-1` renvoyée pour la région.
GetBucketNotifationConfiguration (Anciennement appelée notification GET Bucket)	Renvoie la configuration de notification associée au compartiment.
GetBucketPolicy	Renvoie la politique attachée au compartiment.
GetBuckeReplication	Renvoie la configuration de réplication attachée au compartiment.

Fonctionnement	Mise en place
GetBucketTagging	Utilise la `tagging` sous-ressource pour renvoyer toutes les balises d'un compartiment. **Attention** : si une balise de stratégie ILM non définie par défaut est définie pour ce compartiment, une balise de compartiment sera affectée à cette `NTAP-SG-ILM-BUCKET-TAG` variable. Ne modifiez pas et ne supprimez pas cette balise.
GetBucketVersioning	Cette implémentation utilise la `versioning` sous-ressource pour renvoyer l'état de gestion des versions d'un compartiment. • *Blank*: La gestion des versions n'a jamais été activée (le compartiment est « non versionné ») • Activé : la gestion des versions est activée • Suspendu : la gestion des versions a déjà été activée et est suspendue
GetObjectLockConfiguration	Renvoie le mode de conservation par défaut du compartiment et la période de conservation par défaut, si elle est configurée. Voir "Utilisez l'API REST S3 pour configurer le verrouillage objet S3".
Godet principal	Détermine si un compartiment existe et que vous êtes autorisé à y accéder. Cette opération renvoie : • `x-ntap-sg-bucket-id`: UUID du compartiment au format UUID. • `x-ntap-sg-trace-id`: ID de trace unique de la demande associée.
ListObjects et ListObjectsV2 (Anciennement appelé « GET Bucket »)	Renvoie une partie ou la totalité (jusqu'à 1,000) des objets dans un compartiment. La classe de stockage des objets peut avoir l'une des deux valeurs, même si l'objet a été ingéré avec l' `REDUCED_REDUNDANCY`option de classe de stockage : • `STANDARD`, Qui indique que l'objet est stocké dans un pool de stockage composé de nœuds de stockage. • `GLACIER`, Qui indique que l'objet a été déplacé vers le compartiment externe spécifié par le pool de stockage cloud. Si le compartiment contient un grand nombre de clés supprimées dont le préfixe est identique, certains ne contiennent pas de `CommonPrefixes` clés.
ListObjectVersions (Anciennement nommé OBTENIR les versions de l'objet compartiment)	Avec l'accès EN LECTURE sur un compartiment, cette opération associée à la `versions` sous-ressource liste les métadonnées de toutes les versions des objets du compartiment.

Fonctionnement	Mise en place
PutBucketCors	Définit la configuration CORS pour un compartiment de sorte que le compartiment puisse traiter les demandes d'origine croisée. 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 définissant la configuration CORS pour le `images` compartiment, vous pouvez autoriser l'affichage des images de ce compartiment sur le site Web `http://www.example.com`.
PutBucketEncryption	Définit l'état de chiffrement par défaut d'un compartiment existant. Lorsque le chiffrement au niveau du compartiment est activé, tout nouvel objet ajouté au compartiment est chiffré.StorageGRID prend en charge le chiffrement côté serveur avec des clés gérées par StorageGRID. Lorsque vous spécifiez la règle de configuration du chiffrement côté serveur, définissez le `SSEAlgorithm` paramètre sur `AES256` et n'utilisez pas le `KMSMasterKeyID` paramètre. La configuration de chiffrement par défaut du compartiment est ignorée si la demande de téléchargement d'objet spécifie déjà le chiffrement (c'est-à-dire si la demande inclut l' `x-amz-server-side-encryption-*`en-tête de la requête).
PutBucketLifecycleConfiguration (Anciennement appelé cycle de vie du compartiment PUT)	Crée une nouvelle configuration de cycle de vie pour le compartiment ou remplace une configuration de cycle de vie existante. StorageGRID prend en charge jusqu'à 1,000 règles de cycle de vie dans une configuration cycle de vie. Chaque règle peut inclure les éléments XML suivants : • Expiration (jours, Date, ExpiredObjectDeleteMarker) • NoncurrentVersionExpiation (NewerNoncurrentVersions, NoncurrentDays) • Filtre (préfixe, étiquette) • État • ID StorageGRID ne prend pas en charge les actions suivantes : • AbortIncompleMultipartUpload • Transition Voir "Création de la configuration du cycle de vie S3". Pour comprendre comment l'action expiration d'un cycle de vie de compartiment interagit avec les instructions de placement ILM, reportez-vous à la section "Fonctionnement de ILM tout au long de la vie d'un objet". **Remarque** : la configuration du cycle de vie des compartiments peut être utilisée avec des compartiments avec le verrouillage d'objet S3 activé, mais la configuration du cycle de vie des compartiments n'est pas prise en charge pour les compartiments conformes hérités.

Fonctionnement	Mise en place

PutBucketNotifationConfiguration
 	
(Anciennement appelée notification PUT Bucket)
	Configure les notifications pour le compartiment à l'aide du fichier XML de configuration de notification inclus dans le corps de la demande. Vous devez connaître les détails d'implémentation suivants :
	
	• StorageGRID prend en charge Amazon simple notification Service (Amazon SNS) ou les rubriques Kafka en tant que destinations. Les points finaux SQS (simple Queue Service) ou Lambda d'Amazon ne sont pas pris en charge.
	• La destination des notifications doit être spécifiée comme URN d'un terminal StorageGRID. Les terminaux peuvent être créés à l'aide du Gestionnaire de locataires ou de l'API de gestion des locataires.
	
	Le noeud final doit exister pour que la configuration des notifications réussisse. Si le noeud final n'existe pas, une `400 Bad Request` erreur est renvoyée avec le code `InvalidArgument`.
	
	• Vous ne pouvez pas configurer de notification pour les types d'événements suivants. Ces types d'événements sont **non** pris en charge.
	◦ `s3:ReducedRedundancyLostObject`
	◦ `s3:ObjectRestore:Completed`
	• Les notifications d'événements envoyées par StorageGRID utilisent le format JSON standard, sauf qu'elles n'incluent pas certaines clés et utilisent des valeurs spécifiques pour d'autres, comme illustré dans la liste suivante :
	◦ **EventSource**
	
	`sgws:s3`
	
	◦ **AwsRegion**
	
	non inclus
	
	◦ **x-amz-id-2**
	
	non inclus
	
	◦ **arn**
	
	`urn:sgws:s3:::bucket_name`

PutBuckePolicy	Définit la règle attachée au compartiment. Voir "Utilisez les règles d'accès au compartiment et au groupe".

Fonctionnement	Mise en place
PutBuckeReplication	Configure "Réplication StorageGRID CloudMirror" pour le compartiment à l'aide du fichier XML de configuration de réplication fourni dans le corps de la demande. Pour la réplication CloudMirror, vous devez connaître les détails d'implémentation suivants : • StorageGRID ne prend en charge que le V1 de la configuration de la réplication. Cela signifie que StorageGRID ne prend pas en charge l'utilisation de `Filter` l'élément pour les règles et respecte les conventions V1 pour la suppression des versions d'objet. Pour plus de détails, voir "Guide de l'utilisateur d'Amazon simple Storage Service : configuration de la réplication". • La réplication des compartiments peut être configurée sur les compartiments avec ou sans version. • Vous pouvez spécifier un compartiment de destination différent dans chaque règle du XML de configuration de réplication. Un compartiment source peut être répliqué sur plusieurs compartiments de destination. • Les compartiments de destination doivent être spécifiés en tant que URN des terminaux StorageGRID, tel que spécifié dans le Gestionnaire de locataires ou l'API de gestion des locataires. Voir "Configurez la réplication CloudMirror". Le noeud final doit exister pour que la configuration de réplication réussisse. Si le noeud final n'existe pas, la demande échoue en tant que `400 Bad Request` . le message d'erreur indique : `Unable to save the replication policy. The specified endpoint URN does not exist: URN`. • Vous n'avez pas besoin de spécifier un `Role` dans le XML de configuration. Cette valeur n'est pas utilisée par StorageGRID et sera ignorée si elle a été soumise. • Si vous omettez la classe de stockage du XML de configuration, StorageGRID utilise la `STANDARD` classe de stockage par défaut. • Si vous supprimez un objet du compartiment source ou que vous supprimez le compartiment source lui-même, le comportement de réplication inter-région est le suivant : ◦ Si vous supprimez l'objet ou le compartiment avant sa réplication, l'objet/le compartiment n'est pas répliqué et vous n'êtes pas averti. ◦ Si vous supprimez l'objet ou le compartiment après sa réplication, StorageGRID suit le comportement de suppression Amazon S3 standard pour la version V1 de la réplication multi-région.

Fonctionnement	Mise en place
Étiquetage PutBucketTagging	Utilise la `tagging` sous-ressource pour ajouter ou mettre à jour un ensemble de balises pour un compartiment. Lors de l'ajout de balises de compartiment, tenez compte des limites suivantes : • StorageGRID et Amazon S3 prennent en charge jusqu'à 50 balises pour chaque compartiment. • Les étiquettes associées à un compartiment doivent avoir des clés d'étiquette uniques. Une clé de balise peut comporter jusqu'à 128 caractères Unicode. • Les valeurs de balise peuvent comporter jusqu'à 256 caractères Unicode. • Les clés et les valeurs sont sensibles à la casse **Attention** : si une balise de stratégie ILM non définie par défaut est définie pour ce compartiment, une balise de compartiment sera affectée à cette `NTAP-SG-ILM-BUCKET-TAG` variable. Assurez-vous que la `NTAP-SG-ILM-BUCKET-TAG` balise de compartiment est incluse avec la valeur attribuée dans toutes les demandes PutBucketTagging. Ne modifiez pas et ne supprimez pas cette balise. **Remarque** : cette opération écrasera les balises actuelles du compartiment. Si des balises existantes sont omises de l'ensemble, ces balises seront supprimées pour le compartiment.
PutBuckeVersioning	Utilise la `versioning` sous-ressource pour définir l'état de gestion des versions d'un compartiment existant. Vous pouvez définir l'état de la gestion des versions à l'aide de l'une des valeurs suivantes : • Activé : permet la gestion des versions des objets dans le compartiment. Tous les objets ajoutés au compartiment reçoivent un ID de version unique. • Suspendu : désactive la gestion des versions des objets dans le compartiment. Tous les objets ajoutés au compartiment reçoivent l'ID de version `null` .
PutObjectLockConfiguration	Configure ou supprime le mode de conservation par défaut du compartiment et la période de conservation par défaut. Si la période de conservation par défaut est modifiée, la conservation jusqu'à la date des versions d'objet existantes reste la même et n'est pas recalculée en utilisant la nouvelle période de conservation par défaut. Voir "Utilisez l'API REST S3 pour configurer le verrouillage objet S3" pour plus d'informations.

Opérations sur les objets

Opérations sur les objets

Cette section décrit la manière dont le système StorageGRID implémente les opérations de l'API REST S3 pour les objets.

Les conditions suivantes s'appliquent à toutes les opérations d'objet :

- StorageGRID "valeurs de cohérence"sont pris en charge par toutes les opérations sur les objets, à l'exception des opérations suivantes :
  - GetObjectAcl
  - `OPTIONS /`
  - PutObjectLegalHold
  - PutObjectRetention
  - SelectObjectContent
- Les demandes contradictoires des clients, telles que deux clients qui écrivent sur la même clé, sont résolues sur une base de « derniers-victoires ». La chronologie de l'évaluation « derniers-victoires » repose sur la date à laquelle le système StorageGRID termine une demande donnée et non sur la date à laquelle les clients S3 commencent une opération.
- Tous les objets d'un compartiment StorageGRID sont détenus par le propriétaire du compartiment, y compris les objets créés par un utilisateur anonyme ou par un autre compte.
- Les objets de données ingérés dans le système StorageGRID via Swift ne sont pas accessibles via S3.

Le tableau ci-dessous décrit la manière dont StorageGRID implémente les opérations sur les objets de l'API REST S3.

Fonctionnement	Mise en place
DeleteObject	L'authentification multifacteur (MFA) et l'en-tête de réponse `x-amz-mfa` ne sont pas pris en charge. Lors du traitement d'une requête DeleteObject, StorageGRID tente de supprimer immédiatement toutes les copies de l'objet de tous les emplacements stockés. En cas de succès, StorageGRID renvoie immédiatement une réponse au client. Si toutes les copies ne peuvent pas être supprimées dans les 30 secondes (par exemple, parce qu'un emplacement est temporairement indisponible), StorageGRID met les copies en file d'attente pour suppression et indique que le client a réussi. **Gestion des versions** Pour supprimer une version spécifique, le demandeur doit être le propriétaire du compartiment et utiliser la `versionId` sous-ressource. L'utilisation de cette sous-ressource supprime définitivement la version. Si le `versionId` correspond à un marqueur de suppression, l'en-tête de réponse `x-amz-delete-marker` est renvoyé à `true`. • Si un objet est supprimé sans la `versionId` sous-ressource sur un compartiment avec la gestion des versions activée, il génère un marqueur de suppression. Le `versionId` pour le marqueur de suppression est renvoyé à l'aide de `x-amz-version-id` l'en-tête de réponse et l' `x-amz-delete-marker`en-tête de réponse est renvoyé à `true. • Si un objet est supprimé sans la `versionId` sous-ressource sur un compartiment avec la gestion des versions suspendue, il entraîne la suppression permanente d'une version 'null' existante ou d'un marqueur de suppression 'null', et la génération d'un nouveau marqueur de suppression 'null'. L' `x-amz-delete-marker`en-tête de réponse est renvoyé à `true. **Remarque** : dans certains cas, plusieurs marqueurs de suppression peuvent exister pour un objet. Reportez-vous à la section "Utilisez l'API REST S3 pour configurer le verrouillage objet S3" pour savoir comment supprimer des versions d'objets en mode GOUVERNANCE.
DeleteObjects (Précédemment nommé, SUPPRIMER plusieurs objets)	L'authentification multifacteur (MFA) et l'en-tête de réponse `x-amz-mfa` ne sont pas pris en charge. Plusieurs objets peuvent être supprimés dans le même message de demande. Reportez-vous à la section "Utilisez l'API REST S3 pour configurer le verrouillage objet S3" pour savoir comment supprimer des versions d'objets en mode GOUVERNANCE.

Fonctionnement	Mise en place
DeleteObjectTagging	Utilise la `tagging` sous-ressource pour supprimer toutes les balises d'un objet. **Gestion des versions** Si le `versionId` paramètre de requête n'est pas spécifié dans la requête, l'opération supprime toutes les balises de la version la plus récente de l'objet dans un compartiment versionné. Si la version actuelle de l'objet est un marqueur de suppression, l'état "MethodNotAllowed" est renvoyé avec l' `x-amz-delete-marker`en-tête de réponse défini sur `true`.
GetObject	"GetObject"
GetObjectAcl	Si les informations d'identification d'accès nécessaires sont fournies pour le compte, l'opération renvoie une réponse positive ainsi que l'ID, le DisplayName et l'autorisation du propriétaire de l'objet, ce qui indique que le propriétaire dispose d'un accès complet à l'objet.
GetObjectLegalHold	"Utilisez l'API REST S3 pour configurer le verrouillage objet S3"
GetObjectRetention	"Utilisez l'API REST S3 pour configurer le verrouillage objet S3"
GetObjectTagging	Utilise la `tagging` sous-ressource pour renvoyer toutes les balises d'un objet. **Gestion des versions** Si le `versionId` paramètre de requête n'est pas spécifié dans la requête, l'opération renvoie toutes les balises de la version la plus récente de l'objet dans un compartiment versionné. Si la version actuelle de l'objet est un marqueur de suppression, l'état "MethodNotAllowed" est renvoyé avec l' `x-amz-delete-marker`en-tête de réponse défini sur `true`.
Objet principal	"Objet principal"
Objet de restauration	"Objet de restauration"
PutObject	"PutObject"
Objet de copie (Objet PUT précédemment nommé - Copier)	"Objet de copie"
PutObjectLegalHold	"Utilisez l'API REST S3 pour configurer le verrouillage objet S3"

Fonctionnement	Mise en place
PutObjectRetention	"Utilisez l'API REST S3 pour configurer le verrouillage objet S3"
Marquage PutObject	Utilise la `tagging` sous-ressource pour ajouter un ensemble de balises à un objet existant. **Limites des balises d'objet** Vous pouvez ajouter des balises à de nouveaux objets lorsque vous les téléchargez ou les ajouter à des objets existants. StorageGRID et Amazon S3 prennent en charge jusqu'à 10 balises pour chaque objet. Les balises associées à un objet doivent avoir des clés de balise uniques. Une clé de balise peut comporter jusqu'à 128 caractères Unicode et les valeurs de balise peuvent comporter jusqu'à 256 caractères Unicode. Les clés et les valeurs sont sensibles à la casse **Mises à jour des balises et comportement d'ingestion** Lorsque vous utilisez PutObjectTagging pour mettre à jour les balises d'un objet, StorageGRID ne réingère pas l'objet. Cela signifie que l'option de comportement d'ingestion spécifiée dans la règle ILM correspondante n'est pas utilisée. Tout changement au placement d'objet déclenché par la mise à jour est apporté lors de l'évaluation de ILM par des processus ILM en arrière-plan normaux. En d'autres termes, si la règle ILM utilise l'option strict pour le comportement d'ingestion, aucune action n'est entreprise si les placements d'objet requis ne peuvent pas être effectués (par exemple, parce qu'un nouvel emplacement n'est pas disponible). L'objet mis à jour conserve son emplacement actuel jusqu'à ce que le placement requis soit possible. **Résolution des conflits** Les demandes contradictoires des clients, telles que deux clients qui écrivent sur la même clé, sont résolues sur une base de « derniers-victoires ». La chronologie de l'évaluation « derniers-victoires » repose sur la date à laquelle le système StorageGRID termine une demande donnée et non sur la date à laquelle les clients S3 commencent une opération. **Gestion des versions** Si le `versionId` paramètre de requête n'est pas spécifié dans la requête, l'opération ajoute des balises à la version la plus récente de l'objet dans un compartiment versionné. Si la version actuelle de l'objet est un marqueur de suppression, l'état "MethodNotAllowed" est renvoyé avec l' `x-amz-delete-marker`en-tête de réponse défini sur `true`.
SelectObjectContent	"SelectObjectContent"

StorageGRID prend en charge les clauses, types de données et opérateurs Amazon S3 Select suivants pour le "Commande SelectObjectContent".

> Les éléments non répertoriés ne sont pas pris en charge.

Pour la syntaxe, voir "SelectObjectContent". Pour plus d'informations sur S3 Select, reportez-vous au "Documentation AWS pour S3 Select" .

Seuls les comptes de tenant dont S3 Select est activé peuvent émettre des requêtes SelectObjectContent. Voir la "Considérations et configuration requise pour l'utilisation de S3 Select".

Clauses

- SÉLECTIONNER la liste
- Clause FROM
- Clause WHERE
- Clause DE LIMITE

Types de données

- bool
- entier
- chaîne
- flottement
- décimale, numérique
- horodatage

Opérateurs

Opérateurs logiques

- ET
- PAS
- OU

Opérateurs de comparaison

- <
- >
- &lt ;=
- >=
- =
- =
- <>

- !=
- ENTRE
- DANS

Opérateurs de correspondance de répétition

- COMME
- _
- %

Opérateurs unitaires

- EST NULL
- N'EST PAS NULL

Opérateurs mathématiques

- +
- -
- *
- /
- %

StorageGRID suit la priorité de l'opérateur Amazon S3 Select.

Fonctions d'agrégation

- MOY()
- NOMBRE(*)
- MAX()
- MIN()
- SOMME()

Fonctions conditionnelles

- CASSE
- FUSIONNE
- NULLIF

Fonctions de conversion

- CAST (pour les types de données pris en charge)

Fonctions de date

- DATE_AJOUTER
- DATE_DIFF

- EXTRAIRE
- TO_STRING
- TO_TIMESTAMP
- CODE D'ARTICLE

Fonctions de chaîne

- CHAR_LENGTH, CARACTÈRE_LENGTH
- ABAISSEMENT
- SOUS-CHAÎNE
- GARNITURE
- SUPÉRIEUR

Utilisez le cryptage côté serveur

Le chiffrement côté serveur vous permet de protéger vos données au repos objet. StorageGRID crypte les données lors de leur écriture et décrypte les données lorsque vous accédez à l'objet.

Si vous souhaitez utiliser le chiffrement côté serveur, vous pouvez choisir l'une des deux options mutuellement exclusives, en fonction de la gestion des clés de cryptage :

- **SSE (chiffrement côté serveur avec clés gérées par StorageGRID)** : lorsque vous émettez une demande S3 pour stocker un objet, StorageGRID crypte l'objet avec une clé unique. Lorsque vous émettez une requête S3 pour récupérer l'objet, StorageGRID utilise la clé stockée pour décrypter l'objet.
- **SSE-C (chiffrement côté serveur avec clés fournies par le client)** : lorsque vous émettez une demande S3 pour stocker un objet, vous fournissez votre propre clé de chiffrement. Lorsque vous récupérez un objet, vous fournissez la même clé de chiffrement dans le cadre de votre demande. Si les deux clés de chiffrement correspondent, l'objet est décrypté et vos données d'objet sont renvoyées.

  StorageGRID gère toutes les opérations de cryptage et de décryptage des objets, mais vous devez gérer les clés de cryptage que vous fournissez.

> Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant.

> Si un objet est chiffré avec SSE ou SSE-C, tous les paramètres de chiffrement au niveau du godet ou de la grille sont ignorés.

Utiliser SSE

Pour chiffrer un objet avec une clé unique gérée par StorageGRID, utilisez l'en-tête de demande suivant :

```
x-amz-server-side-encryption
```

L'en-tête de demande SSE est pris en charge par les opérations d'objet suivantes :

- "PutObject"

- "Objet de copie"
- "CreateMultipartUpload"

Utiliser SSE-C

Pour crypter un objet avec une clé unique que vous gérez, vous utilisez trois en-têtes de requête :

En-tête de demande	Description
`x-amz-server-side-encryption-customer-algorithm`	Spécifiez l'algorithme de cryptage. La valeur de l'en-tête doit être `AES256`.
`x-amz-server-side-encryption-customer-key`	Spécifiez la clé de cryptage qui sera utilisée pour crypter ou décrypter l'objet. La valeur de la clé doit être codée en 256 bits, en base64.
`x-amz-server-side-encryption-customer-key-MD5`	Spécifiez le résumé MD5 de la clé de chiffrement selon la RFC 1321, qui est utilisé pour garantir que la clé de chiffrement a été transmise sans erreur. La valeur du résumé MD5 doit être codée en base64 à 128 bits.

Les en-têtes de demande SSE-C sont pris en charge par les opérations objet suivantes :

- "GetObject"
- "Objet principal"
- "PutObject"
- "Objet de copie"
- "CreateMultipartUpload"
- "UploadPart"
- "UploadPartCopy"

Considérations relatives au chiffrement côté serveur avec clés fournies par le client (SSE-C)

Avant d'utiliser SSE-C, tenez compte des points suivants :

- Vous devez utiliser https.

> StorageGRID rejette toute demande effectuée sur http lors de l'utilisation de SSE-C. pour des raisons de sécurité, vous devez considérer que toute clé que vous envoyez accidentellement à l'aide de http est compromise. Mettez la clé au rebut et tournez-la selon les besoins.

- L'ETag dans la réponse n'est pas le MD5 des données objet.
- Vous devez gérer le mappage des clés de chiffrement aux objets. StorageGRID ne stocke pas de clés de chiffrement. Vous êtes responsable du suivi de la clé de chiffrement que vous fournissez pour chaque objet.
- Si le contrôle de version du compartiment est activé, chaque version d'objet doit disposer de sa propre clé de chiffrement. Vous êtes responsable du suivi de la clé de chiffrement utilisée pour chaque version d'objet.

- Comme vous gérez les clés de chiffrement côté client, vous devez également gérer d'autres dispositifs de protection, tels que la rotation des clés, côté client.

> Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant.

- Si la réplication inter-grid ou CloudMirror est configurée pour le compartiment, vous ne pouvez pas acquérir d'objets SSE-C. L'opération d'acquisition échoue.

Informations associées

"Guide de l'utilisateur Amazon S3 : utilisation du chiffrement côté serveur avec des clés fournies par le client (SSE-C)"

Objet de copie

Vous pouvez utiliser la requête CopyObject S3 pour créer une copie d'un objet déjà stocké dans S3. Une opération CopyObject est identique à l'exécution de GetObject suivie de PutObject.

Résoudre les conflits

Les demandes contradictoires des clients, telles que deux clients qui écrivent sur la même clé, sont résolues sur une base de « derniers-victoires ». La chronologie de l'évaluation « derniers-victoires » repose sur la date à laquelle le système StorageGRID termine une demande donnée et non sur la date à laquelle les clients S3 commencent une opération.

Taille de l'objet

La taille *recommandée* maximale pour une opération PutObject unique est de 5 Gio (5,368,709,120 octets). Si vous avez des objets dont la valeur est supérieure à 5 Gio, utilisez la "téléchargement partitionné"valeur.

La taille *supportée* maximale pour une opération PutObject unique est de 5 Tio (5,497,558,138,880 octets).

> Si vous avez mis à niveau à partir de StorageGRID 11.6 ou version antérieure, l'alerte PUT objet taille trop grande de S3 sera déclenchée si vous tentez de télécharger un objet dont la valeur dépasse 5 Gio. Si vous avez une nouvelle installation de StorageGRID 11.7 ou 11.8, l'alerte ne sera pas déclenchée dans ce cas. Toutefois, pour s'aligner sur la norme AWS S3, les futures versions d'StorageGRID ne prendront pas en charge le chargement d'objets de plus de 5 Gio.

Caractères UTF-8 dans les métadonnées utilisateur

Si une requête inclut (non échappé) les valeurs UTF-8 dans le nom de clé ou la valeur des métadonnées définies par l'utilisateur, le comportement StorageGRID n'est pas défini.

StorageGRID n'analyse ni n'interprète pas les caractères UTF-8 qui se sont échappé dans le nom de clé ou la valeur des métadonnées définies par l'utilisateur. Les caractères UTF-8 échappés sont traités comme des caractères ASCII :

- Les requêtes réussissent si les métadonnées définies par l'utilisateur incluent des caractères UTF-8 échappés.
- StorageGRID ne renvoie pas l' `x-amz-missing-meta`en-tête si la valeur interprétée du nom ou de la valeur

de la clé contient des caractères non imprimables.

En-têtes de demande pris en charge

Les en-têtes de requête suivants sont pris en charge :

- `Content-Type`
- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-if-modified-since`
- `x-amz-meta-`, suivi d'une paire nom-valeur contenant des métadonnées définies par l'utilisateur
- `x-amz-metadata-directive`: La valeur par défaut est `COPY`, qui vous permet de copier l'objet et les métadonnées associées.

  Vous pouvez spécifier de `REPLACE` remplacer les métadonnées existantes lors de la copie de l'objet ou de mettre à jour les métadonnées de l'objet.

- `x-amz-storage-class`
- `x-amz-tagging-directive`: La valeur par défaut est `COPY`, qui vous permet de copier l'objet et toutes les balises.

  Vous pouvez spécifier `REPLACE` d'écraser les balises existantes lors de la copie de l'objet ou de mettre à jour les balises.

- En-têtes de demande de verrouillage d'objet S3 :
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

    Si une demande est effectuée sans ces en-têtes, les paramètres de rétention par défaut du compartiment sont utilisés pour calculer le mode de version de l'objet et conserver jusqu'à la date. Voir "Utilisez l'API REST S3 pour configurer le verrouillage objet S3".

- En-têtes de demande SSE :
  - `x-amz-copy-source-server-side-encryption-customer-algorithm`
  - `x-amz-copy-source-server-side-encryption-customer-key`
  - `x-amz-copy-source-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

Voir Demander des en-têtes pour le cryptage côté serveur

En-têtes de requête non pris en charge

Les en-têtes de demande suivants ne sont pas pris en charge :

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `Expires`
- `x-amz-checksum-algorithm`

  Lorsque vous copiez un objet, si celui-ci possède un checksum, StorageGRID ne copie pas cette valeur de checksum vers le nouvel objet. Ce comportement s'applique que vous essayiez ou non d'utiliser `x-amz-checksum-algorithm` dans la demande d'objet.

- `x-amz-website-redirect-location`

Options de classe de stockage

L' `x-amz-storage-class`en-tête de requête est pris en charge et affecte le nombre de copies d'objet créées par StorageGRID si la règle ILM correspondante utilise la fonction Dual commit ou Balanced "option d'ingestion".

- `STANDARD`

  (Valeur par défaut) Spécifie une opération d'ingestion à double validation lorsque la règle ILM utilise l'option de validation double, ou lorsque l'option équilibrée revient à créer des copies intermédiaires.

- `REDUCED_REDUNDANCY`

  Spécifie une opération d'entrée de validation unique lorsque la règle ILM utilise l'option Double allocation ou lorsque l'option équilibrée revient à créer des copies intermédiaires.

> Si vous acquérez un objet dans un compartiment avec le verrouillage d'objet S3 activé, l' `REDUCED_REDUNDANCY`option est ignorée. Si vous ingérer un objet dans un compartiment compatible hérité, l' `REDUCED_REDUNDANCY`option renvoie une erreur. StorageGRID procède toujours à une récupération à double engagement afin de satisfaire les exigences de conformité.

Utilisation de x-amz-copy-source dans CopyObject

Si le compartiment source et la clé, spécifiés dans l' `x-amz-copy-source`en-tête, sont différents du compartiment et de la clé de destination, une copie des données de l'objet source est écrite vers la destination.

Si la source et la destination correspondent et que l' `x-amz-metadata-directive`en-tête est spécifié comme `REPLACE`, les métadonnées de l'objet sont mises à jour avec les valeurs de métadonnées fournies dans la requête. Dans ce cas, StorageGRID ne réingère pas l'objet. Ceci a deux conséquences importantes :

- Vous ne pouvez pas utiliser CopyObject pour chiffrer un objet existant ou pour modifier le chiffrement d'un objet existant. Si vous fournissez l' `x-amz-server-side-encryption`en-tête ou l' `x-amz-server-side-encryption-customer-algorithm`en-tête, StorageGRID rejette la demande et renvoie `XNotImplemented`.
- L'option de comportement d'ingestion spécifiée dans la règle ILM correspondante n'est pas utilisée. Tout changement au placement d'objet déclenché par la mise à jour est apporté lors de l'évaluation de ILM par des processus ILM en arrière-plan normaux.

  En d'autres termes, si la règle ILM utilise l'option strict pour le comportement d'ingestion, aucune action n'est entreprise si les placements d'objet requis ne peuvent pas être effectués (par exemple, parce qu'un nouvel emplacement n'est pas disponible). L'objet mis à jour conserve son emplacement actuel jusqu'à ce que le placement requis soit possible.

Demander des en-têtes pour le cryptage côté serveur

Si vous "utilisez le chiffrement côté serveur", les en-têtes de requête que vous fournissez dépendent du cryptage de l'objet source et de l'intention de chiffrer l'objet cible.

- Si l'objet source est chiffré à l'aide d'une clé fournie par le client (SSE-C), vous devez inclure les trois en-têtes suivants dans la requête CopyObject, afin que l'objet puisse être décrypté puis copié :
  - `x-amz-copy-source-server-side-encryption-customer-algorithm`: Spécifiez `AES256`.
  - `x-amz-copy-source-server-side-encryption-customer-key`: Spécifiez la clé de chiffrement que vous avez fournie lors de la création de l'objet source.
  - `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Spécifiez le résumé MD5 que vous avez fourni lors de la création de l'objet source.
- Si vous souhaitez chiffrer l'objet cible (la copie) avec une clé unique que vous fournissez et gérez, incluez les trois en-têtes suivants :
  - `x-amz-server-side-encryption-customer-algorithm`: Spécifiez `AES256`.
  - `x-amz-server-side-encryption-customer-key`: Spécifiez une nouvelle clé de chiffrement pour l'objet cible.
  - `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le résumé MD5 de la nouvelle clé de chiffrement.

  > Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant. Avant d'utiliser des clés fournies par le client pour sécuriser les données d'objet, consultez les considérations relatives à "utilisation du chiffrement côté serveur".

- Si vous souhaitez crypter l'objet cible (la copie) avec une clé unique gérée par StorageGRID (SSE), incluez cet en-tête dans la demande CopyObject :
  - `x-amz-server-side-encryption`

  > La `server-side-encryption` valeur de l'objet ne peut pas être mise à jour. Au lieu de cela, faites une copie avec une nouvelle `server-side-encryption` valeur en utilisant `x-amz-metadata-directive`: `REPLACE`.

Gestion des versions

Si le compartiment source est versionné, vous pouvez utiliser l' `x-amz-copy-source`en-tête pour copier la dernière version d'un objet. Pour copier une version spécifique d'un objet, vous devez spécifier explicitement la version à copier à l'aide de la `versionId` sous-ressource. Si le compartiment de destination est versionné, la version générée est renvoyée dans l' `x-amz-version-id`en-tête de réponse. Si la gestion des versions est suspendue pour le compartiment cible, `x-amz-version-id` renvoie une valeur « null ».

GetObject

Vous pouvez utiliser la requête S3 GetObject pour récupérer un objet à partir d'un compartiment S3.

GetObject et objets multipièces

Vous pouvez utiliser le `partNumber` paramètre request pour extraire une partie spécifique d'un objet multipièce ou segmenté. L' `x-amz-mp-parts-count`élément de réponse indique le nombre de parties de l'objet.

Vous pouvez définir `partNumber` la valeur 1 pour les objets segmentés/multipièces et les objets non segmentés/non multipièces ; cependant, l' `x-amz-mp-parts-count`élément de réponse est renvoyé uniquement pour les objets segmentés ou multipièces.

Caractères UTF-8 dans les métadonnées utilisateur

StorageGRID n'analyse ni n'interprète pas les caractères UTF-8 qui se sont échappés dans les métadonnées définies par l'utilisateur. Les requêtes GET pour un objet avec des caractères UTF-8 échappés dans les métadonnées définies par l'utilisateur ne renvoient pas l' `x-amz-missing-meta`en-tête si le nom ou la valeur de la clé contient des caractères non imprimables.

En-tête de demande pris en charge

L'en-tête de demande suivant est pris en charge :

- `x-amz-checksum-mode`: Spécifiez `ENABLED`

  L' `Range`en-tête n'est pas pris en charge `x-amz-checksum-mode` par pour GetObject. Lorsque vous incluez `Range` dans la demande avec `x-amz-checksum-mode` activé, StorageGRID ne renvoie pas de valeur de somme de contrôle dans la réponse.

En-tête de demande non pris en charge

L'en-tête de requête suivant n'est pas pris en charge et renvoie `XNotImplemented`:

- `x-amz-website-redirect-location`

Gestion des versions

Si aucune `versionId` sous-ressource n'est spécifiée, l'opération extrait la version la plus récente de l'objet dans un compartiment versionné. Si la version actuelle de l'objet est un marqueur de suppression, l'état « introuvable » est renvoyé avec l' `x-amz-delete-marker`en-tête de réponse défini sur `true`.

En-têtes de demande pour chiffrement côté serveur avec clés de chiffrement fournies par le client (SSE-C)

Utilisez les trois en-têtes si l'objet est chiffré avec une clé unique que vous avez fournie.

- `x-amz-server-side-encryption-customer-algorithm`: Spécifiez `AES256`.
- `x-amz-server-side-encryption-customer-key`: Spécifiez votre clé de chiffrement pour l'objet.
- `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le résumé MD5 de la clé de chiffrement de l'objet.

> Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant. Avant d'utiliser des clés fournies par le client pour sécuriser les données d'objet, consultez les considérations de la section "Utilisez le cryptage côté serveur".

Comportement de GetObject pour les objets de pool de stockage cloud

Si un objet a été stocké dans un "Pool de stockage cloud", le comportement d'une requête GetObject dépend de l'état de l'objet. Voir "Objet principal" pour plus de détails.

> Si un objet est stocké dans un pool de stockage cloud et qu'une ou plusieurs copies de l'objet existent également dans la grille, les requêtes GetObject tentent de récupérer les données de la grille avant de les extraire du pool de stockage cloud.

État de l'objet	Comportement de GetObject
Les objets sont ingéré dans StorageGRID mais pas encore évalués par ILM, ou objet stocké dans un pool de stockage traditionnel ou au moyen d'un code d'effacement	`200 OK` Une copie de l'objet est récupérée.
Objet dans Cloud Storage Pool, mais pas encore migré vers un état non récupérable	`200 OK` Une copie de l'objet est récupérée.
L'objet a été transféré à un état non récupérable	`403 Forbidden, InvalidObjectState` Utilisez une "Objet de restauration" demande pour restaurer l'objet à un état récupérable.
Objet en cours de restauration à partir d'un état non récupérable	`403 Forbidden, InvalidObjectState` Attendez la fin de la demande RestoreObject.
Objet entièrement restauré dans le pool de stockage cloud	`200 OK` Une copie de l'objet est récupérée.

Objets partitionnés ou segmentés dans un pool de stockage cloud

Si vous avez téléchargé un objet partitionné ou si StorageGRID le divise en segments, StorageGRID détermine si l'objet est disponible dans le pool de stockage cloud en échantillonant un sous-ensemble de parties ou de segments de l'objet. Dans certains cas, une requête GetObject peut renvoyer de manière incorrecte `200 OK` lorsque certaines parties de l'objet ont déjà été transférées à un état non récupérable ou lorsque certaines parties de l'objet n'ont pas encore été restaurées.

Dans ces cas :

- La requête GetObject peut renvoyer certaines données, mais s'arrête à mi-chemin du transfert.
- Une requête GetObject suivante peut renvoyer `403 Forbidden`.

GetObject et la réplication inter-grille

Si vous utilisez "fédération des grilles" et "réplication entre plusieurs grilles" est activé pour un compartiment, le client S3 peut vérifier l'état de réplication d'un objet en émettant une requête GetObject. La réponse inclut l'en-tête de réponse spécifique à StorageGRID `x-ntap-sg-cgr-replication-status`, qui aura l'une des valeurs suivantes :

Grille	État de la réplication
Source	• **TERMINÉ** : la réplication a réussi. • **EN ATTENTE** : l'objet n'a pas encore été répliqué. • **ÉCHEC** : la réplication a échoué avec une défaillance permanente. L'utilisateur doit résoudre l'erreur.
Destination	**RÉPLIQUE** : l'objet a été répliqué à partir de la grille source.

> StorageGRID ne prend pas en charge la `x-amz-replication-status` barre de coupe.

Objet principal

Vous pouvez utiliser la requête S3 HeadObject pour extraire des métadonnées d'un objet sans renvoyer l'objet. Si l'objet est stocké dans un pool de stockage cloud, vous pouvez utiliser HeadObject pour déterminer l'état de transition de l'objet.

Objets en-tête et objets multipièces

Vous pouvez utiliser `partNumber` le paramètre request pour extraire des métadonnées pour une partie spécifique d'un objet multipièce ou segmenté. L' `x-amz-mp-parts-count`élément de réponse indique le nombre de parties de l'objet.

Vous pouvez définir `partNumber` la valeur 1 pour les objets segmentés/multipièces et les objets non segmentés/non multipièces ; cependant, l' `x-amz-mp-parts-count`élément de réponse est renvoyé uniquement pour les objets segmentés ou multipièces.

Caractères UTF-8 dans les métadonnées utilisateur

StorageGRID n'analyse ni n'interprète pas les caractères UTF-8 qui se sont échappés dans les métadonnées

définies par l'utilisateur. Les demandes HEAD pour un objet avec des caractères UTF-8 échappés dans les métadonnées définies par l'utilisateur ne renvoient pas l' `x-amz-missing-meta`en-tête si le nom ou la valeur de la clé contient des caractères non imprimables.

En-tête de demande pris en charge

L'en-tête de demande suivant est pris en charge :

- `x-amz-checksum-mode`

  Le `partNumber` paramètre et l' `Range`en-tête ne sont pas pris en charge avec `x-amz-checksum-mode` pour HeadObject. Lorsque vous les incluez dans la demande avec `x-amz-checksum-mode` activé, StorageGRID ne renvoie pas de valeur de somme de contrôle dans la réponse.

En-tête de demande non pris en charge

L'en-tête de requête suivant n'est pas pris en charge et renvoie `XNotImplemented`:

- `x-amz-website-redirect-location`

Gestion des versions

Si aucune `versionId` sous-ressource n'est spécifiée, l'opération extrait la version la plus récente de l'objet dans un compartiment versionné. Si la version actuelle de l'objet est un marqueur de suppression, l'état « introuvable » est renvoyé avec l' `x-amz-delete-marker`en-tête de réponse défini sur `true`.

En-têtes de demande pour chiffrement côté serveur avec clés de chiffrement fournies par le client (SSE-C)

Utilisez les trois en-têtes si l'objet est chiffré avec une clé unique que vous avez fournie.

- `x-amz-server-side-encryption-customer-algorithm`: Spécifiez `AES256`.
- `x-amz-server-side-encryption-customer-key`: Spécifiez votre clé de chiffrement pour l'objet.
- `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le résumé MD5 de la clé de chiffrement de l'objet.

> Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant. Avant d'utiliser des clés fournies par le client pour sécuriser les données d'objet, consultez les considérations de la section "Utilisez le cryptage côté serveur".

HeadObject Responses for Cloud Storage Pool objects

Si l'objet est stocké dans un "Pool de stockage cloud", les en-têtes de réponse suivants sont renvoyés :

- `x-amz-storage-class: GLACIER`
- `x-amz-restore`

Les en-têtes de réponse fournissent des informations sur l'état d'un objet lors de son déplacement vers Cloud Storage Pool, qui peut être migré vers un état non récupérable et restauré.

État de l'objet	Réponse à l'objet principal
Les objets sont ingéré dans StorageGRID mais pas encore évalués par ILM, ou objet stocké dans un pool de stockage traditionnel ou au moyen d'un code d'effacement	`200 OK` (Aucun en-tête de réponse spéciale n'est renvoyé.)

Objet dans Cloud Storage Pool, mais pas encore migré vers un état non récupérable	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"`
	
	Jusqu'à ce que l'objet soit transféré à un état non récupérable, la valeur de `expiry-date` est définie sur un temps distant à l'avenir. L'heure exacte de la transition n'est pas contrôlée par le système StorageGRID.

L'objet est passé à l'état non récupérable, mais il existe au moins une copie sur la grille	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"`
	
	La valeur de `expiry-date` est définie sur un temps distant à l'avenir.
	
	Remarque : si la copie de la grille n'est pas disponible (par exemple, un nœud de stockage est en panne), vous devez émettre une "Objet de restauration" demande de restauration de la copie à partir du pool de stockage cloud avant de pouvoir récupérer l'objet.

L'objet a été transféré à un état non récupérable et aucune copie n'existe sur la grille	`200 OK`
	
	`x-amz-storage-class: GLACIER`

Objet en cours de restauration à partir d'un état non récupérable	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="true"`

État de l'objet	Réponse à l'objet principal

Objet entièrement restauré dans le pool de stockage cloud	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2018 00:00:00 GMT"`
	
	Le `expiry-date` indique quand l'objet du pool de stockage cloud sera renvoyé à un état non récupérable.

Objets partitionnés ou segmentés dans Cloud Storage Pool

Si vous avez téléchargé un objet partitionné ou si StorageGRID le divise en segments, StorageGRID détermine si l'objet est disponible dans le pool de stockage cloud en échantillonnant un sous-ensemble de parties ou de segments de l'objet. Dans certains cas, une requête HeadObject peut être renvoyée de manière incorrecte `x-amz-restore: ongoing-request="false"` lorsque certaines parties de l'objet ont déjà été transférées à un état non récupérable ou lorsque certaines parties de l'objet n'ont pas encore été restaurées.

HeadObject et réplication inter-grid

Si vous utilisez "fédération des grilles" et "réplication entre plusieurs grilles" est activé pour un compartiment, le client S3 peut vérifier l'état de réplication d'un objet en émettant une requête HeadObject. La réponse inclut l'en-tête de réponse spécifique à StorageGRID `x-ntap-sg-cgr-replication-status`, qui aura l'une des valeurs suivantes :

Grille	État de la réplication
Source	• **TERMINÉ** : la réplication a réussi. • **EN ATTENTE** : l'objet n'a pas encore été répliqué. • **ÉCHEC** : la réplication a échoué avec une défaillance permanente. L'utilisateur doit résoudre l'erreur.
Destination	**RÉPLIQUE** : l'objet a été répliqué à partir de la grille source.

> StorageGRID ne prend pas en charge la `x-amz-replication-status` barre de coupe.

PutObject

Vous pouvez utiliser la demande S3 PutObject pour ajouter un objet à un compartiment.

Résoudre les conflits

Les demandes contradictoires des clients, telles que deux clients qui écrivent sur la même clé, sont résolues sur une base de « derniers-victoires ». La chronologie de l'évaluation « derniers-victoires » repose sur la date à laquelle le système StorageGRID termine une demande donnée et non sur la date à laquelle les clients S3 commencent une opération.

Taille de l'objet

La taille *recommandée* maximale pour une opération PutObject unique est de 5 Gio (5,368,709,120 octets). Si vous avez des objets dont la valeur est supérieure à 5 Gio, utilisez la "téléchargement partitionné"valeur.

La taille *supportée* maximale pour une opération PutObject unique est de 5 Tio (5,497,558,138,880 octets).

> Si vous avez mis à niveau à partir de StorageGRID 11.6 ou version antérieure, l'alerte PUT objet taille trop grande de S3 sera déclenchée si vous tentez de télécharger un objet dont la valeur dépasse 5 Gio. Si vous avez une nouvelle installation de StorageGRID 11.7 ou 11.8, l'alerte ne sera pas déclenchée dans ce cas. Toutefois, pour s'aligner sur la norme AWS S3, les futures versions d'StorageGRID ne prendront pas en charge le chargement d'objets de plus de 5 Gio.

Taille des métadonnées utilisateur

Amazon S3 limite la taille des métadonnées définies par l'utilisateur au sein de chaque en-tête de requête À 2 Ko. StorageGRID limite les métadonnées utilisateur à 24 Kio. La taille des métadonnées définies par l'utilisateur est mesurée en prenant la somme du nombre d'octets dans le codage UTF-8 de chaque clé et valeur.

Caractères UTF-8 dans les métadonnées utilisateur

Si une requête inclut (non échappé) les valeurs UTF-8 dans le nom de clé ou la valeur des métadonnées définies par l'utilisateur, le comportement StorageGRID n'est pas défini.

StorageGRID n'analyse ni n'interprète pas les caractères UTF-8 qui se sont échappé dans le nom de clé ou la valeur des métadonnées définies par l'utilisateur. Les caractères UTF-8 échappés sont traités comme des caractères ASCII :

- Les requêtes PutObject, CopyObject, GetObject et HeadObject réussissent si les métadonnées définies par l'utilisateur incluent des caractères UTF-8 échappés.
- StorageGRID ne renvoie pas l' `x-amz-missing-meta`en-tête si la valeur interprétée du nom ou de la valeur de la clé contient des caractères non imprimables.

Limites des balises d'objet

Vous pouvez ajouter des balises à de nouveaux objets lorsque vous les téléchargez ou les ajouter à des objets existants. StorageGRID et Amazon S3 prennent en charge jusqu'à 10 balises pour chaque objet. Les balises associées à un objet doivent avoir des clés de balise uniques. Une clé de balise peut comporter jusqu'à 128 caractères Unicode et les valeurs de balise peuvent comporter jusqu'à 256 caractères Unicode. Les clés et les valeurs sont sensibles à la casse

Propriété de l'objet

Dans StorageGRID, tous les objets sont détenus par le compte du propriétaire de compartiment, y compris les objets créés par un compte autre que le propriétaire ou un utilisateur anonyme.

En-têtes de demande pris en charge

Les en-têtes de requête suivants sont pris en charge :

- `Cache-Control`

- `Content-Disposition`
- `Content-Encoding`

  Lorsque vous spécifiez `aws-chunked` pour `Content-Encoding`StorageGRID, ne vérifie pas les éléments suivants :

  - StorageGRID ne vérifie pas le `chunk-signature` par rapport aux données de bloc.
  - StorageGRID ne vérifie pas la valeur que vous fournissez pour `x-amz-decoded-content-length` l'objet.
- `Content-Language`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Expires`
- `Transfer-Encoding`

  Le codage de transfert avec chunked est pris en charge si `aws-chunked` la signature de charge est également utilisée.
- `x-amz-checksum-sha256`
- `x-amz-meta-`, suivi d'une paire nom-valeur contenant des métadonnées définies par l'utilisateur.

  Lorsque vous spécifiez la paire nom-valeur pour les métadonnées définies par l'utilisateur, utilisez le format général suivant :

  ```
  x-amz-meta-name: value
  ```

  Si vous souhaitez utiliser l'option **heure de création définie par l'utilisateur** comme heure de référence pour une règle ILM, vous devez utiliser `creation-time` comme nom des métadonnées enregistrées lors de la création de l'objet. Par exemple :

  ```
  x-amz-meta-creation-time: 1443399726
  ```

  La valeur de `creation-time` est évaluée en secondes depuis le 1er janvier 1970.

  > Une règle ILM ne peut pas utiliser à la fois une **heure de création définie par l'utilisateur** pour l'heure de référence et l'option d'acquisition équilibrée ou stricte. Une erreur est renvoyée lors de la création de la règle ILM.

- `x-amz-tagging`
- En-têtes de requête de verrouillage d'objet S3
  - `x-amz-object-lock-mode`

- `x-amz-object-lock-retain-until-date`
- `x-amz-object-lock-legal-hold`

  Si une demande est effectuée sans ces en-têtes, les paramètres de rétention par défaut du compartiment sont utilisés pour calculer le mode de version de l'objet et conserver jusqu'à la date. Voir "Utilisez l'API REST S3 pour configurer le verrouillage objet S3".

- En-têtes de demande SSE :
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

    Voir Demander des en-têtes pour le cryptage côté serveur

En-têtes de requête non pris en charge

Les en-têtes de demande suivants ne sont pas pris en charge :

- `x-amz-acl`
- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`
- `x-amz-website-redirect-location`

L'`x-amz-website-redirect-location`en-tête renvoie `XNotImplemented`.

Options de classe de stockage

L'`x-amz-storage-class`en-tête de la demande est pris en charge. La valeur fournie pour affecte la `x-amz-storage-class` façon dont StorageGRID protège les données d'objet lors de l'ingestion et non le nombre de copies persistantes de l'objet stockées dans le système StorageGRID (déterminé par la règle ILM).

Si la règle ILM correspondant à un objet ingéré utilise l'option strict d'ingestion, l' `x-amz-storage-class`en-tête n'a aucun effet.

Les valeurs suivantes peuvent être utilisées pour `x-amz-storage-class`:

- `STANDARD` (Par défaut)
  - **Double commit** : si la règle ILM spécifie l'option de double validation pour le comportement d'ingestion, dès qu'un objet est ingéré, une seconde copie de cet objet est créée et distribuée à un autre nœud de stockage (double commit). Une fois la règle ILM évaluée, StorageGRID détermine si ces copies intermédiaires initiales répondent aux instructions de placement de la règle. Si ce n'est pas le cas, de nouvelles copies d'objet peuvent avoir besoin d'être effectuées à différents emplacements et les copies intermédiaires initiales peuvent avoir besoin d'être supprimées.
  - **Balanced** : si la règle ILM spécifie l'option équilibrée et que StorageGRID ne peut pas immédiatement effectuer toutes les copies spécifiées dans la règle, StorageGRID effectue deux copies intermédiaires

sur différents nœuds de stockage.

Si StorageGRID peut créer immédiatement toutes les copies d'objet spécifiées dans la règle ILM (placement synchrone), l' `x-amz-storage-class`en-tête n'a aucun effet.

- `REDUCED_REDUNDANCY`
  - **Double commit** : si la règle ILM spécifie l'option de double validation pour le comportement d'ingestion, StorageGRID crée une copie intermédiaire unique lors de l'ingestion de l'objet (simple commit).
  - **Équilibré** : si la règle ILM spécifie l'option équilibrée, StorageGRID effectue une seule copie intermédiaire uniquement si le système ne peut pas immédiatement effectuer toutes les copies spécifiées dans la règle. Si StorageGRID peut effectuer un placement synchrone, cet en-tête n'a aucun effet. L' `REDUCED_REDUNDANCY`option est mieux utilisée lorsque la règle ILM qui correspond à l'objet crée une copie répliquée unique. Dans ce cas, l'utilisation de `REDUCED_REDUNDANCY` supprime la création et la suppression inutiles d'une copie d'objet supplémentaire pour chaque opération d'ingestion.

  L'utilisation de cette `REDUCED_REDUNDANCY` option n'est pas recommandée dans d'autres circonstances. `REDUCED_REDUNDANCY` augmente le risque de perte des données d'objet lors de leur ingestion. Vous risquez par exemple de perdre des données si une seule copie est initialement stockée sur un nœud de stockage qui échoue avant l'évaluation du ILM.

> Le fait d'avoir une seule copie répliquée pendant une période donnée présente un risque de perte permanente des données. Si une seule copie répliquée d'un objet existe, cet objet est perdu en cas de défaillance ou d'erreur importante d'un noeud de stockage. De plus, lors des procédures de maintenance telles que les mises à niveau, l'accès à l'objet est temporairement perdu.

Le fait de spécifier `REDUCED_REDUNDANCY` affecte uniquement le nombre de copies créées lors de la première ingestion d'un objet. Cela n'affecte pas le nombre de copies de l'objet effectuées lorsque l'objet est évalué par les règles ILM actives, et n'entraîne pas le stockage des données à des niveaux de redondance inférieurs dans le système StorageGRID.

> Si vous acquérez un objet dans un compartiment avec le verrouillage d'objet S3 activé, l' `REDUCED_REDUNDANCY`option est ignorée. Si vous ingérer un objet dans un compartiment compatible hérité, l' `REDUCED_REDUNDANCY`option renvoie une erreur. StorageGRID procède toujours à une récupération à double engagement afin de satisfaire les exigences de conformité.

Demander des en-têtes pour le cryptage côté serveur

Vous pouvez utiliser les en-têtes de requête suivants pour crypter un objet avec un chiffrement côté serveur. Les options SSE et SSE-C sont mutuellement exclusives.

- **SSE**: Utilisez l'en-tête suivant si vous voulez chiffrer l'objet avec une clé unique gérée par StorageGRID.
  - `x-amz-server-side-encryption`

    Lorsque l' `x-amz-server-side-encryption`en-tête n'est pas inclus dans la demande PutObject, la grille "paramètre de chiffrement d'objet stocké"est omise de la réponse PutObject.
- **SSE-C**: Utilisez les trois en-têtes si vous voulez chiffrer l'objet avec une clé unique que vous fournissez et

gérez.

- `x-amz-server-side-encryption-customer-algorithm`: Spécifiez `AES256`.
- `x-amz-server-side-encryption-customer-key`: Spécifiez votre clé de chiffrement pour le nouvel objet.
- `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le résumé MD5 de la clé de chiffrement du nouvel objet.

> Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant. Avant d'utiliser des clés fournies par le client pour sécuriser les données d'objet, consultez les considérations relatives à "utilisation du chiffrement côté serveur".

> Si un objet est chiffré avec SSE ou SSE-C, tous les paramètres de chiffrement au niveau du godet ou de la grille sont ignorés.

Gestion des versions

Si la gestion des versions est activée pour un compartiment, une unique `versionId` est automatiquement générée pour la version de l'objet stocké. Ceci `versionId` est également renvoyé dans la réponse à l'aide de l' `x-amz-version-id`en-tête de réponse.

Si la gestion des versions est suspendue, la version de l'objet est stockée avec une valeur `versionId` NULL et si une version nulle existe déjà, elle sera écrasée.

Calculs de signature pour l'en-tête autorisation

Lorsque vous utilisez l' `Authorization`en-tête pour authentifier les requêtes, StorageGRID diffère d'AWS de la manière suivante :

- StorageGRID ne nécessite pas l' `host`inclusion d'en-têtes dans `CanonicalHeaders`.
- StorageGRID ne nécessite pas d' `Content-Type`être inclus dans `CanonicalHeaders`.
- StorageGRID ne nécessite pas l' `x-amz-*`inclusion d'en-têtes dans `CanonicalHeaders`.

> En règle générale, incluez toujours ces en-têtes dans `CanonicalHeaders` pour vous assurer qu'ils sont vérifiés. Cependant, si vous excluez ces en-têtes, StorageGRID ne renvoie pas d'erreur.

Pour plus de détails, reportez-vous à "Calculs de signature pour l'en-tête d'autorisation : transfert de charge utile dans un seul bloc (signature AWS version 4)" .

Informations associées

- "Gestion des objets avec ILM"
- "Référence de l'API Amazon simple Storage Service : PutObject"

Objet de restauration

Vous pouvez utiliser la requête objet de restauration S3 pour restaurer un objet stocké dans un pool de stockage cloud.

Type de demande pris en charge

StorageGRID ne prend en charge que les requêtes RestoreObject pour restaurer un objet. Il ne prend pas en charge le `SELECT` type de restauration. Sélectionnez demandes retour `XNotImplemented`.

Gestion des versions

Si vous le souhaitez, spécifiez `versionId` pour restaurer une version spécifique d'un objet dans un compartiment multiversion. Si vous ne spécifiez pas `versionId` , la version la plus récente de l'objet est restaurée

Comportement de RestoreObject sur les objets de pool de stockage cloud

Si un objet a été stocké dans un "Pool de stockage cloud", une requête RestoreObject a le comportement suivant, en fonction de l'état de l'objet. Voir "Objet principal" pour plus de détails.

> Si un objet est stocké dans un pool de stockage cloud et qu'une ou plusieurs copies de l'objet existent également dans la grille, il n'est pas nécessaire de restaurer l'objet en émettant une requête RestoreObject. À la place, la copie locale peut être récupérée directement à l'aide d'une requête GetObject.

État de l'objet	Comportement de RestoreObject
L'objet est ingéré dans StorageGRID mais pas encore évalué par ILM ou l'objet ne se trouve pas dans un pool de stockage cloud	`403 Forbidden`, `InvalidObjectState`
Objet dans Cloud Storage Pool, mais pas encore migré vers un état non récupérable	`200 OK` Aucune modification n'est effectuée. **Remarque** : avant qu'un objet ne soit transféré à un état non récupérable, vous ne pouvez pas modifier son `expiry-date`.
L'objet a été transféré à un état non récupérable	`202 Accepted` Restaure une copie récupérable de l'objet vers le pool de stockage cloud pendant le nombre de jours spécifié dans le corps de la requête. À la fin de cette période, l'objet est renvoyé à un état non récupérable. Vous pouvez également utiliser `Tier` l'élément de demande pour déterminer la durée de la tâche de restauration pour terminer (`Expedited`, , `Standard` ou `Bulk`). Si vous ne spécifiez pas `Tier` , le `Standard` niveau est utilisé. **Important** : si un objet a été transféré vers S3 Glacier Deep Archive ou si le pool de stockage cloud utilise le stockage Azure Blob, vous ne pouvez pas le restaurer à l'aide du `Expedited` Tier. L'erreur suivante est renvoyée `403 Forbidden`, `InvalidTier`: `Retrieval option is not supported by this storage class`.

État de l'objet	Comportement de RestoreObject
Objet en cours de restauration à partir d'un état non récupérable	`409 Conflict`, `RestoreAlreadyInProgress`
Objet entièrement restauré dans le pool de stockage cloud	`200 OK` **Note:** si un objet a été restauré à un état récupérable, vous pouvez le modifier `expiry-date` en réémettant la requête RestoreObject avec une nouvelle valeur pour `Days`. La date de restauration est mise à jour par rapport à l'heure de la demande.

SelectObjectContent

Vous pouvez utiliser la requête S3 SelectObjectContent pour filtrer le contenu d'un objet S3 à partir d'une instruction SQL simple.

Pour plus d'informations, voir "Référence de l'API Amazon simple Storage Service : SelectObjectContent".

Avant de commencer

- Le compte de tenant dispose de l'autorisation S3 Select.
- Vous disposez de l'autorisation pour l'objet que vous `s3:GetObject` souhaitez interroger.
- L'objet que vous souhaitez interroger doit être dans l'un des formats suivants :
  - **CSV**. Peut être utilisé tel qu'il est ou compressé dans des archives GZIP ou BZIP2.
  - **Parquet**. Exigences supplémentaires pour les objets parquet :
    - S3 Select prend uniquement en charge la compression par colonne à l'aide de GZIP ou de Snappy. S3 Select ne prend pas en charge la compression d'objets entiers pour les objets parquet.
    - S3 Select ne prend pas en charge la sortie parquet. Vous devez spécifier le format de sortie au format CSV ou JSON.
    - La taille maximale du groupe de lignes non compressées est de 512 Mo.
    - Vous devez utiliser les types de données spécifiés dans le schéma de l'objet.
    - Vous ne pouvez pas utiliser de types logiques D'INTERVALLE, de JSON, DE LISTE, DE TEMPS ou d'UUID.
- Votre expression SQL a une longueur maximale de 256 Ko.
- Tout enregistrement dans l'entrée ou les résultats a une longueur maximale de 1 MIB.

Exemple de syntaxe de demande CSV

```
POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns="http://s3.amazonaws.com/doc/2006-03-
01/">
   <Expression>string</Expression>
   <ExpressionType>string</ExpressionType>
   <RequestProgress>
      <Enabled>boolean</Enabled>
   </RequestProgress>
   <InputSerialization>
      <CompressionType>GZIP</CompressionType>
      <CSV>
         <AllowQuotedRecordDelimiter>boolean</AllowQuotedRecordDelimiter>
         <Comments>#</Comments>
         <FieldDelimiter>\t</FieldDelimiter>
         <FileHeaderInfo>USE</FileHeaderInfo>
         <QuoteCharacter>'</QuoteCharacter>
         <QuoteEscapeCharacter>\\</QuoteEscapeCharacter>
         <RecordDelimiter>\n</RecordDelimiter>
      </CSV>
   </InputSerialization>
   <OutputSerialization>
      <CSV>
         <FieldDelimiter>string</FieldDelimiter>
         <QuoteCharacter>string</QuoteCharacter>
         <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
         <QuoteFields>string</QuoteFields>
         <RecordDelimiter>string</RecordDelimiter>
      </CSV>
   </OutputSerialization>
   <ScanRange>
      <End>long</End>
      <Start>long</Start>
   </ScanRange>
</SelectObjectContentRequest>
```

Exemple de syntaxe de demande de parquet

```
POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns=http://s3.amazonaws.com/doc/2006-03-01/>
   <Expression>string</Expression>
   <ExpressionType>string</ExpressionType>
   <RequestProgress>
      <Enabled>boolean</Enabled>
   </RequestProgress>
   <InputSerialization>
      <CompressionType>GZIP</CompressionType>
      <PARQUET>
      </PARQUET>
   </InputSerialization>
   <OutputSerialization>
      <CSV>
         <FieldDelimiter>string</FieldDelimiter>
         <QuoteCharacter>string</QuoteCharacter>
         <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
         <QuoteFields>string</QuoteFields>
         <RecordDelimiter>string</RecordDelimiter>
      </CSV>
   </OutputSerialization>
   <ScanRange>
      <End>long</End>
      <Start>long</Start>
   </ScanRange>
</SelectObjectContentRequest>
```

Exemple de requête SQL

Cette requête obtient le nom de l'état, 2010 populations, environ 2015 populations et le pourcentage de changement des données de recensement des États-Unis. Les enregistrements du fichier qui ne sont pas des États sont ignorés.

```
SELECT STNAME, CENSUS2010POP, POPESTIMATE2015, CAST((POPESTIMATE2015 -
CENSUS2010POP) AS DECIMAL) / CENSUS2010POP * 100.0 FROM S3Object WHERE
NAME = STNAME
```

Les premières lignes du fichier à interroger, `SUB-EST2020_ALL.csv`, ressemblent à ceci :

```
SUMLEV,STATE,COUNTY,PLACE,COUSUB,CONCIT,PRIMGEO_FLAG,FUNCSTAT,NAME,STNAME,
CENSUS2010POP,
ESTIMATESBASE2010,POPESTIMATE2010,POPESTIMATE2011,POPESTIMATE2012,POPESTIM
ATE2013,POPESTIMATE2014,
POPESTIMATE2015,POPESTIMATE2016,POPESTIMATE2017,POPESTIMATE2018,POPESTIMAT
E2019,POPESTIMATE042020,
POPESTIMATE2020
040,01,000,00000,00000,00000,0,A,Alabama,Alabama,4779736,4780118,4785514,4
799642,4816632,4831586,
4843737,4854803,4866824,4877989,4891628,4907965,4920706,4921532
162,01,000,00124,00000,00000,0,A,Abbeville
city,Alabama,2688,2705,2699,2694,2645,2629,2610,2602,
2587,2578,2565,2555,2555,2553
162,01,000,00460,00000,00000,0,A,Adamsville
city,Alabama,4522,4487,4481,4474,4453,4430,4399,4371,
4335,4304,4285,4254,4224,4211
162,01,000,00484,00000,00000,0,A,Addison
town,Alabama,758,754,751,750,745,744,742,734,734,728,
725,723,719,717
```

Exemple d'utilisation d'AWS-CLI (CSV)

```
aws s3api select-object-content --endpoint-url https://10.224.7.44:10443
--no-verify-ssl  --bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.csv --expression-type SQL --input-serialization '{"CSV":
{"FileHeaderInfo": "USE", "Comments": "#", "QuoteEscapeCharacter": "\"",
"RecordDelimiter": "\n", "FieldDelimiter": ",", "QuoteCharacter": "\"",
"AllowQuotedRecordDelimiter": false}, "CompressionType": "NONE"}' --output
-serialization '{"CSV": {"QuoteFields": "ASNEEDED",
"QuoteEscapeCharacter": "#", "RecordDelimiter": "\n", "FieldDelimiter":
",", "QuoteCharacter": "\""}}' --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" changes.csv
```

Les premières lignes du fichier de sortie, `changes.csv`, ressemblent à ceci :

```
Alabama,4779736,4854803,1.570526070895965802295356898372629785 4
Alaska,710231,738430,3.970398363349389142405780654463125377 5
Arizona,6392017,6832810,6.895992297892824753125656580700583243 1
Arkansas,2915918,2979732,2.188470320495981025529524492801237894 9
California,37253956,38904296,4.429972483996062055798852610444914897 1
Colorado,5029196,5454328,8.453279609703022113276157859029554624 6
```

Exemple d'utilisation de l'interface de ligne de commande AWS (parquet)

```
aws s3api select-object-content  -endpoint-url https://10.224.7.44:10443
--bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.parquet --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" --expression-type
'SQL' --input-serialization '{"Parquet":{}}'  --output-serialization
'{"CSV": {}}' changes.csv
```

Les premières lignes du fichier de sortie, change.csv, se ressemblent à ceci :

```
Alabama,4779736,4854803,1.5705260708959658022953568983726297854
Alaska,710231,738430,3.9703983633493891424057806544631253775
Arizona,6392017,6832810,6.8959922978928247531256565807005832431
Arkansas,2915918,2979732,2.1884703204959810255295244928012378949
California,37253956,38904296,4.4299724839960620557988526104449148971
Colorado,5029196,5454328,8.4532796097030221132761578590295546246
```

Opérations pour les téléchargements partitionnés

Opérations pour les téléchargements partitionnés

Cette section décrit comment StorageGRID prend en charge les opérations de téléchargement partitionné.

Les conditions et notes suivantes s'appliquent à toutes les opérations de téléchargement partitionné :

- Vous ne devez pas dépasser 1,000 téléchargements partitionnés simultanés vers un seul compartiment, car les résultats des requêtes ListMultipartUploads pour ce compartiment peuvent renvoyer des résultats incomplets.
- StorageGRID fait respecter les limites de taille d'AWS pour les pièces en plusieurs parties. Les clients S3 doivent respecter les consignes suivantes :
  - Chaque partie d'un téléchargement partitionné doit être comprise entre 5 Mio (5,242,880 octets) et 5 Gio (5,368,709,120 octets).
  - La dernière partie peut être inférieure à 5 Mio (5,242,880 octets).
  - En général, la taille des pièces doit être la plus grande possible. Par exemple, utilisez une taille de pièce de 5 Gio pour un objet de 100 Gio. Chaque pièce étant considérée comme un objet unique, l'utilisation de pièces de grande taille réduit la surcharge liée aux métadonnées StorageGRID.
  - Pour les objets de moins de 5 Gio, envisagez l'utilisation de téléchargement non partitionné.
- La gestion des règles ILM est évaluée pour chaque partie d'un objet en plusieurs parties lors de son ingestion et pour l'objet dans son ensemble lorsque le téléchargement partitionné est terminé, si la règle ILM utilise la méthode équilibrée ou stricte "option d'ingestion". Vous devez savoir comment cela affecte le positionnement de l'objet et de la pièce :
  - Si des modifications sont apportées au ILM pendant un téléchargement partitionné S3, certaines

parties de l'objet peuvent ne pas répondre aux exigences ILM actuelles une fois le téléchargement partitionné terminé. Toute pièce qui n'est pas correctement placée est mise en file d'attente pour une réévaluation ILM et déplacée vers l'emplacement correct ultérieurement.

    - Lors de l'évaluation d'ILM pour une pièce, StorageGRID filtre la taille de la pièce, et non la taille de l'objet. Ainsi, certaines parties d'un objet peuvent être stockées dans des emplacements qui ne respectent pas les exigences de la règle ILM pour l'ensemble de l'objet. Par exemple, si une règle indique que tous les objets de 10 Go ou plus sont stockés sur DC1 alors que tous les objets plus petits sont stockés sur DC2, chaque partie de 1 Go d'un téléchargement partitionné en 10 parties est stockée sur DC2 lors de l'ingestion. Cependant, lorsque ILM est évalué pour l'objet dans son ensemble, toutes les parties de l'objet sont déplacées vers DC1.

- Toutes les opérations de téléchargement partitionné prennent en charge StorageGRID "valeurs de cohérence".
- Lorsqu'un objet est ingéré à l'aide d'un téléchargement partitionné, le "Seuil de segmentation d'objet (1 Gio)"n'est pas appliqué.
- Si nécessaire, vous pouvez l'utiliser "chiffrement côté serveur" avec les téléchargements partitionnés. Pour utiliser SSE (chiffrement côté serveur avec des clés gérées par StorageGRID), vous incluez l'en- `x-amz-server-side-encryption`tête de requête dans la requête CreateMultipartUpload uniquement. Pour utiliser SSE-C (chiffrement côté serveur avec des clés fournies par le client), vous devez spécifier les trois mêmes en-têtes de requête de clé de chiffrement dans la demande CreateMultipartUpload et dans chaque demande UploadPart suivante.

Fonctionnement	Mise en place
AbortMultipartUpload	Mise en œuvre avec tout le comportement de l'API REST Amazon S3. D'être modifiées sans préavis.
CompleteMultipartUpload	Voir "CompleteMultipartUpload"
CreateMultipartUpload (Précédemment appelé lancer le téléchargement multipièce)	Voir "CreateMultipartUpload"
ListMultipartUploads	Voir "ListMultipartUploads"
ListParts	Mise en œuvre avec tout le comportement de l'API REST Amazon S3. D'être modifiées sans préavis.
UploadPart	Voir "UploadPart"
UploadPartCopy	Voir "UploadPartCopy"

CompleteMultipartUpload

L'opération CompleteMultipartUpload effectue un téléchargement partitionné d'un objet en assemblant les pièces précédemment téléchargées.

StorageGRID prend en charge les valeurs non consécutives par ordre croissant pour le `partNumber` paramètre de requête avec CompleteMultipartUpload. Le paramètre peut commencer par n'importe quelle valeur.

Résoudre les conflits

Les demandes contradictoires des clients, telles que deux clients qui écrivent sur la même clé, sont résolues sur une base de « derniers-victoires ». La chronologie de l'évaluation « derniers-victoires » repose sur la date à laquelle le système StorageGRID termine une demande donnée et non sur la date à laquelle les clients S3 commencent une opération.

En-têtes de demande pris en charge

Les en-têtes de requête suivants sont pris en charge :

- `x-amz-checksum-sha256`
- `x-amz-storage-class`

  L' `x-amz-storage-class`en-tête affecte le nombre de copies objet créées par StorageGRID si la règle ILM correspondante spécifie le "Double allocation ou option d'ingestion équilibrée".

- `STANDARD`

  (Valeur par défaut) Spécifie une opération d'ingestion à double validation lorsque la règle ILM utilise l'option de validation double, ou lorsque l'option équilibrée revient à créer des copies intermédiaires.

- `REDUCED_REDUNDANCY`

  Spécifie une opération d'entrée de validation unique lorsque la règle ILM utilise l'option Double allocation ou lorsque l'option équilibrée revient à créer des copies intermédiaires.

  Si vous acquérez un objet dans un compartiment avec le verrouillage d'objet S3 activé, l' `REDUCED_REDUNDANCY`option est ignorée. Si vous ingérer un objet dans un compartiment compatible hérité, l' `REDUCED_REDUNDANCY`option renvoie une erreur. StorageGRID procède toujours à une récupération à double engagement afin de satisfaire les exigences de conformité.

Si un téléchargement partitionné n'est pas terminé dans les 15 jours, l'opération est marquée comme inactive et toutes les données associées sont supprimées du système.

La `ETag` valeur renvoyée n'est pas une somme MD5 des données, mais suit l'implémentation de l'API Amazon S3 de la `ETag` valeur pour les objets multipart.

En-têtes de requête non pris en charge

Les en-têtes de demande suivants ne sont pas pris en charge :

- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`

Gestion des versions

Cette opération termine un téléchargement partitionné. Si la gestion des versions est activée pour un compartiment, la version de l'objet est créée une fois le téléchargement partitionné terminé.

Si la gestion des versions est activée pour un compartiment, une unique `versionId` est automatiquement générée pour la version de l'objet stocké. Ceci `versionId` est également renvoyé dans la réponse à l'aide de l' `x-amz-version-id`en-tête de réponse.

Si la gestion des versions est suspendue, la version de l'objet est stockée avec une valeur `versionId` NULL et si une version nulle existe déjà, elle sera écrasée.

> Lorsque le contrôle de version est activé pour un compartiment, le fait de terminer un téléchargement partitionné crée toujours une nouvelle version, même si des téléchargements partitionnés simultanés sont terminés sur la même clé d'objet. Lorsque le contrôle de version n'est pas activé pour un compartiment, il est possible de lancer un téléchargement partitionné et de lancer un autre lancement de téléchargement partitionné et de le terminer d'abord sur la même clé d'objet. Pour les compartiments non versionnés, le téléchargement partitionné de la dernière version est prioritaire.

Échec de la réplication, de la notification ou de la notification des métadonnées

Si le compartiment dans lequel le téléchargement partitionné est configuré pour un service de plateforme, le téléchargement partitionné réussit même si l'action de réplication ou de notification associée échoue.

Un locataire peut déclencher la réplication ou la notification d'échec en mettant à jour les métadonnées ou les balises de l'objet. Un locataire peut soumettre à nouveau les valeurs existantes afin d'éviter toute modification non souhaitée.

Reportez-vous à la "Résoudre les problèmes liés aux services de plateforme".

CreateMultipartUpload

L'opération CreateMultipartUpload (précédemment appelée Initiate Multipart Upload) lance un téléchargement partitionné pour un objet et renvoie un ID de téléchargement.

L' `x-amz-storage-class`en-tête de la demande est pris en charge. La valeur fournie pour affecte la `x-amz-storage-class` façon dont StorageGRID protège les données d'objet lors de l'ingestion et non le nombre de copies persistantes de l'objet stockées dans le système StorageGRID (déterminé par la règle ILM).

Si la règle ILM correspondant à un objet ingéré utilise le paramètre strict "option d'ingestion", l' `x-amz-storage-class`en-tête n'a aucun effet.

Les valeurs suivantes peuvent être utilisées pour `x-amz-storage-class`:

- `STANDARD` (Par défaut)
  - **Dual commit** : si la règle ILM spécifie l'option d'acquisition Dual commit, dès qu'un objet est ingéré, une deuxième copie de cet objet est créée et distribuée à un autre nœud de stockage (double commit). Une fois la règle ILM évaluée, StorageGRID détermine si ces copies intermédiaires initiales répondent aux instructions de placement de la règle. Si ce n'est pas le cas, de nouvelles copies d'objet peuvent avoir besoin d'être effectuées à différents emplacements et les copies intermédiaires initiales peuvent avoir besoin d'être supprimées.

- **Balanced** : si la règle ILM spécifie l'option équilibrée et que StorageGRID ne peut pas immédiatement effectuer toutes les copies spécifiées dans la règle, StorageGRID effectue deux copies intermédiaires sur différents nœuds de stockage.

  Si StorageGRID peut créer immédiatement toutes les copies d'objet spécifiées dans la règle ILM (placement synchrone), l' `x-amz-storage-class`en-tête n'a aucun effet.

- `REDUCED_REDUNDANCY`

  - **Dual commit** : si la règle ILM spécifie l'option Dual commit, StorageGRID crée une copie intermédiaire unique lorsque l'objet est ingéré (single commit).
  - **Équilibré** : si la règle ILM spécifie l'option équilibrée, StorageGRID effectue une seule copie intermédiaire uniquement si le système ne peut pas immédiatement effectuer toutes les copies spécifiées dans la règle. Si StorageGRID peut effectuer un placement synchrone, cet en-tête n'a aucun effet. L' `REDUCED_REDUNDANCY`option est mieux utilisée lorsque la règle ILM qui correspond à l'objet crée une copie répliquée unique. Dans ce cas, l'utilisation de `REDUCED_REDUNDANCY` supprime la création et la suppression inutiles d'une copie d'objet supplémentaire pour chaque opération d'ingestion.

  L'utilisation de cette `REDUCED_REDUNDANCY` option n'est pas recommandée dans d'autres circonstances. `REDUCED_REDUNDANCY` augmente le risque de perte des données d'objet lors de leur ingestion. Vous risquez par exemple de perdre des données si une seule copie est initialement stockée sur un nœud de stockage qui échoue avant l'évaluation du ILM.

> Le fait d'avoir une seule copie répliquée pendant une période donnée présente un risque de perte permanente des données. Si une seule copie répliquée d'un objet existe, cet objet est perdu en cas de défaillance ou d'erreur importante d'un noeud de stockage. De plus, lors des procédures de maintenance telles que les mises à niveau, l'accès à l'objet est temporairement perdu.

Le fait de spécifier `REDUCED_REDUNDANCY` affecte uniquement le nombre de copies créées lors de la première ingestion d'un objet. Cela n'affecte pas le nombre de copies de l'objet effectuées lorsque l'objet est évalué par les règles ILM actives, et n'entraîne pas le stockage des données à des niveaux de redondance inférieurs dans le système StorageGRID.

> Si vous acquérez un objet dans un compartiment avec le verrouillage d'objet S3 activé, l' `REDUCED_REDUNDANCY`option est ignorée. Si vous ingérer un objet dans un compartiment compatible hérité, l' `REDUCED_REDUNDANCY`option renvoie une erreur. StorageGRID procède toujours à une récupération à double engagement afin de satisfaire les exigences de conformité.

En-têtes de demande pris en charge

Les en-têtes de requête suivants sont pris en charge :

- `Content-Type`
- `x-amz-checksum-algorithm`

  Actuellement, seule la valeur SHA256 pour `x-amz-checksum-algorithm` est prise en charge.

- `x-amz-meta-`, suivi d'une paire nom-valeur contenant des métadonnées définies par l'utilisateur

Lorsque vous spécifiez la paire nom-valeur pour les métadonnées définies par l'utilisateur, utilisez le format général suivant :

```
x-amz-meta-_name_: `value`
```

Si vous souhaitez utiliser l'option **heure de création définie par l'utilisateur** comme heure de référence pour une règle ILM, vous devez utiliser `creation-time` comme nom des métadonnées enregistrées lors de la création de l'objet. Par exemple :

```
x-amz-meta-creation-time: 1443399726
```

La valeur de `creation-time` est évaluée en secondes depuis le 1er janvier 1970.

> L'ajout de `creation-time` métadonnées définies par l'utilisateur n'est pas autorisé si vous ajoutez un objet à un compartiment pour lequel la conformité des données existantes est activée. Une erreur sera renvoyée.

- En-têtes de demande de verrouillage d'objet S3 :
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

    Si une demande est effectuée sans ces en-têtes, les paramètres de rétention par défaut du compartiment sont utilisés pour calculer la version de l'objet conserver jusqu'à la date.

"Utilisez l'API REST S3 pour configurer le verrouillage objet S3"

- En-têtes de demande SSE :
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

    Demander des en-têtes pour le cryptage côté serveur

> Pour plus d'informations sur la façon dont StorageGRID traite les caractères UTF-8, reportez-vous à la section "PutObject".

Demander des en-têtes pour le cryptage côté serveur

Vous pouvez utiliser les en-têtes de demande suivants pour crypter un objet partitionné avec un cryptage côté serveur. Les options SSE et SSE-C sont mutuellement exclusives.

- **SSE** : utilisez l'en-tête suivant dans la demande CreateMultipartUpload si vous souhaitez crypter l'objet

avec une clé unique gérée par StorageGRID. Ne spécifiez pas cet en-tête dans les demandes UploadPart.

  - `x-amz-server-side-encryption`

- **SSE-C** : utilisez ces trois en-têtes dans la demande CreateMultipartUpload (et dans chaque demande UploadPart suivante) si vous souhaitez crypter l'objet avec une clé unique que vous fournissez et gérez.
  - `x-amz-server-side-encryption-customer-algorithm`: Spécifiez `AES256`.
  - `x-amz-server-side-encryption-customer-key`: Spécifiez votre clé de chiffrement pour le nouvel objet.
  - `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le résumé MD5 de la clé de chiffrement du nouvel objet.

> Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant. Avant d'utiliser des clés fournies par le client pour sécuriser les données d'objet, consultez les considérations relatives à "utilisation du chiffrement côté serveur".

En-têtes de requête non pris en charge

L'en-tête de demande suivant n'est pas pris en charge :

- `x-amz-website-redirect-location`

  L'`x-amz-website-redirect-location`en-tête renvoie `XNotImplemented`.

Gestion des versions

Le téléchargement partitionné est constitué de différentes opérations permettant de lancer le téléchargement, de répertorier les téléchargements, de télécharger des pièces, d'assembler les pièces téléchargées et de terminer le téléchargement. Les objets sont créés (et versionnés le cas échéant) lorsque l'opération CompleteMultipartUpload est exécutée.

ListMultipartUploads

L'opération ListMultipartUploads répertorie les téléchargements partitionnés en cours pour un compartiment.

Les paramètres de demande suivants sont pris en charge :

- `encoding-type`
- `key-marker`
- `max-uploads`
- `prefix`
- `upload-id-marker`
- `Host`
- `Date`
- `Authorization`

Gestion des versions

Le téléchargement partitionné est constitué de différentes opérations permettant de lancer le téléchargement, de répertorier les téléchargements, de télécharger des pièces, d'assembler les pièces téléchargées et de terminer le téléchargement. Les objets sont créés (et versionnés le cas échéant) lorsque l'opération CompleteMultipartUpload est exécutée.

UploadPart

L'opération UploadPart télécharge une pièce dans un téléchargement partitionné pour un objet.

En-têtes de demande pris en charge

Les en-têtes de requête suivants sont pris en charge :

- `x-amz-checksum-sha256`
- `Content-Length`
- `Content-MD5`

Demander des en-têtes pour le cryptage côté serveur

Si vous avez spécifié le cryptage SSE-C pour la demande CreateMultipartUpload, vous devez également inclure les en-têtes de requête suivants dans chaque demande UploadPart :

- `x-amz-server-side-encryption-customer-algorithm`: Spécifiez `AES256`.
- `x-amz-server-side-encryption-customer-key`: Spécifiez la même clé de cryptage que celle que vous avez fournie dans la demande CreateMultipartUpload.
- `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le même résumé MD5 que celui que vous avez fourni dans la demande CreateMultipartUpload.

> Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant. Avant d'utiliser des clés fournies par le client pour sécuriser les données d'objet, consultez les considérations de la section "Utilisez le cryptage côté serveur".

Si vous avez spécifié une somme de contrôle SHA-256 lors de la demande CreateMultipartUpload, vous devez également inclure l'en-tête de requête suivant dans chaque demande UploadPart :

- `x-amz-checksum-sha256`: Spécifiez la somme de contrôle SHA-256 pour cette partie.

En-têtes de requête non pris en charge

Les en-têtes de demande suivants ne sont pas pris en charge :

- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`

Gestion des versions

Le téléchargement partitionné est constitué de différentes opérations permettant de lancer le téléchargement, de répertorier les téléchargements, de télécharger des pièces, d'assembler les pièces téléchargées et de terminer le téléchargement. Les objets sont créés (et versionnés le cas échéant) lorsque l'opération CompleteMultipartUpload est exécutée.

UploadPartCopy

L'opération UploadPartCopy télécharge une partie d'un objet en copiant les données d'un objet existant en tant que source de données.

L'opération UploadPartCopy est implémentée avec tout comportement de l'API REST Amazon S3. D'être modifiées sans préavis.

Cette requête lit et écrit les données d'objet spécifiées dans `x-amz-copy-source-range` au sein du système StorageGRID.

Les en-têtes de requête suivants sont pris en charge :

- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-if-modified-since`

Demander des en-têtes pour le cryptage côté serveur

Si vous avez spécifié le cryptage SSE-C pour la demande CreateMultipartUpload, vous devez également inclure les en-têtes de requête suivants dans chaque demande UploadPartCopy :

- `x-amz-server-side-encryption-customer-algorithm`: Spécifiez `AES256`.
- `x-amz-server-side-encryption-customer-key`: Spécifiez la même clé de cryptage que celle que vous avez fournie dans la demande CreateMultipartUpload.
- `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le même résumé MD5 que celui que vous avez fourni dans la demande CreateMultipartUpload.

Si l'objet source est crypté à l'aide d'une clé fournie par le client (SSE-C), vous devez inclure les trois en-têtes suivants dans la demande UploadPartCopy, afin que l'objet puisse être décrypté puis copié :

- `x-amz-copy-source-server-side-encryption-customer-algorithm`: Spécifiez `AES256`.
- `x-amz-copy-source-server-side-encryption-customer-key`: Spécifiez la clé de chiffrement que vous avez fournie lors de la création de l'objet source.
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Spécifiez le résumé MD5 que vous avez fourni lors de la création de l'objet source.

> Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant. Avant d'utiliser des clés fournies par le client pour sécuriser les données d'objet, consultez les considérations de la section "Utilisez le cryptage côté serveur".

Gestion des versions

Le téléchargement partitionné est constitué de différentes opérations permettant de lancer le téléchargement, de répertorier les téléchargements, de télécharger des pièces, d'assembler les pièces téléchargées et de terminer le téléchargement. Les objets sont créés (et versionnés le cas échéant) lorsque l'opération CompleteMultipartUpload est exécutée.

Réponses d'erreur

Le système StorageGRID prend en charge toutes les réponses d'erreur de l'API REST S3 standard qui s'appliquent. En outre, l'implémentation de StorageGRID ajoute plusieurs réponses personnalisées.

Codes d'erreur de l'API S3 pris en charge

Nom	Statut HTTP
AccessDenied	403 interdit
BadDigest	400 demande erronée
BucketAlreadyExists	409 conflit
BucketNotEmpty	409 conflit
Corps entier	400 demande erronée
Erreur interne	500 erreur interne du serveur
InvalidAccessKeyId	403 interdit
Invalides	400 demande erronée
InvalidBucketName	400 demande erronée
InvalidBucketState	409 conflit
InvalidDigest	400 demande erronée
InvalidEncryptionAlgorithmError	400 demande erronée
Invalidpart	400 demande erronée
Ordre de pièce InvalidPartOrder	400 demande erronée
InvalidRange	416 Plage demandée non satisfiable

Nom	Statut HTTP
InvalidRequest	400 demande erronée
InvalidStorageClass	400 demande erronée
InvalidTag	400 demande erronée
URI non valide	400 demande erronée
KeyToolong	400 demande erronée
MalformedXML	400 demande erronée
MetadaTooLarge	400 demande erronée
MethodNotAlldue	405 méthode non autorisée
MissingContentLength	411 longueur requise
Erreur MissingestBodyError	400 demande erronée
En-tête MissinécuritéSent	400 demande erronée
NoSuchBucket	404 introuvable
NoSuchKey	404 introuvable
NoSuchUpload	404 introuvable
Note d’implémentation	501 non mis en œuvre
NoSuchBucketPolicy	404 introuvable
ObjectLockNotConfigurationError	404 introuvable
Pré-conditionFailed	412 Echec de la condition préalable
RequestTimeTooSkewed	403 interdit
Disponibilité des services	503 Service indisponible
SignatureDoesNotMatch	403 interdit
TooManyseaux	400 demande erronée

Nom	Statut HTTP
UserKeyMustBeSpecified	400 demande erronée

Codes d'erreur personnalisés StorageGRID

Nom	Description	Statut HTTP
XBuckeLifecycleNotAlldue	La configuration du cycle de vie des compartiments n'est pas autorisée dans un compartiment conforme aux anciennes	400 demande erronée
XBuckePolicyParseException	Impossible d'analyser la politique de compartiment JSON.	400 demande erronée
XComplanceConflitt	Opération refusée en raison des paramètres de conformité hérités.	403 interdit
XComplanceReduceRAIDForbidden	La réduction de la redondance est interdite dans le compartiment conforme aux réglementations existantes	400 demande erronée
XMaxBucketPolicyLengthExcediédé	Votre politique dépasse la longueur maximale autorisée pour la règle de gestion des compartiments.	400 demande erronée
XMissingInternalRequestHeader	En-tête d'une demande interne manquant.	400 demande erronée
XNoSuchBucketCompliance	La conformité héritée n'est pas activée dans le compartiment spécifié.	404 introuvable
XNotAcceptable	La demande contient un ou plusieurs en-têtes Accept qui n'ont pas pu être satisfaits.	406 non acceptable
XNotImplementation	La demande que vous avez fournie implique une fonctionnalité qui n'est pas implémentée.	501 non mis en œuvre

Opérations personnalisées StorageGRID

Opérations personnalisées StorageGRID

Le système StorageGRID prend en charge les opérations personnalisées qui sont ajoutées à l'API REST S3.

Le tableau suivant répertorie les opérations personnalisées prises en charge par StorageGRID.

Fonctionnement	Description
"OPTIMISEZ la cohérence des compartiments"	Renvoie la cohérence appliquée à un compartiment particulier.
"PRÉSERVER la cohérence du godet"	Définit la cohérence appliquée à un compartiment spécifique.
"HEURE du dernier accès au compartiment"	Indique si les mises à jour de l'heure du dernier accès sont activées ou désactivées pour un compartiment spécifique.
"METTRE l'heure du dernier accès au compartiment"	Permet d'activer ou de désactiver les mises à jour de l'heure du dernier accès pour un compartiment spécifique.
"SUPPRIMEZ la configuration de notification des métadonnées de compartiment"	Supprime le XML de configuration de notification de métadonnées associé à un compartiment spécifique.
"CONFIGURATION DES notifications de métadonnées de compartiment"	Renvoie le XML de configuration de notification de métadonnées associé à un compartiment spécifique.
"CONFIGURATION de notification des métadonnées de compartiment"	Configure le service de notification des métadonnées pour un compartiment.
"DÉCOUVREZ l'utilisation du stockage"	Indique la quantité totale de stockage utilisée par un compte et par compartiment associé au compte.
"Obsolète : CreateBucket avec paramètres de conformité"	Obsolète et non pris en charge : vous ne pouvez plus créer de compartiments avec conformité activée.
"Obsolète : CONFORMITÉ DES compartiments"	Obsolète mais pris en charge : renvoie les paramètres de conformité actuellement en vigueur pour un compartiment compatible existant.
"Obsolète : conformité DES compartiments PUT"	Obsolète mais pris en charge : permet de modifier les paramètres de conformité d'un compartiment compatible existant.

OPTIMISEZ la cohérence des compartiments

La demande de cohérence GET Bucket vous permet de déterminer la cohérence appliquée à un compartiment spécifique.

La cohérence par défaut est définie pour garantir la lecture après écriture des objets nouvellement créés.

Pour effectuer cette opération, vous devez disposer de l'autorisation s3:GetBucketConsistency, ou être root de compte.

Exemple de demande

```
GET /bucket?x-ntap-sg-consistency HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Réponse

Dans le XML de réponse, `<Consistency>` renvoie l'une des valeurs suivantes :

La cohérence	Description
tous	Tous les nœuds reçoivent les données immédiatement, sinon la requête échoue.
forte croissance mondiale	Garantit une cohérence de lecture après écriture pour toutes les demandes client sur tous les sites.
site fort	Garantit la cohérence de lecture après écriture pour toutes les demandes client dans un site.
lecture-après-nouvelle-écriture	(Valeur par défaut) assure la cohérence en lecture après écriture des nouveaux objets et la cohérence des mises à jour des objets. Offre une haute disponibilité et une protection des données garanties. Recommandé dans la plupart des cas.
disponibilité	Assure la cohérence 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.

Exemple de réponse

```
HTTP/1.1 200 OK
Date: Fri, 18 Sep 2020 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/11.5.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<Consistency xmlns="http://s3.storagegrid.com/doc/2015-02-01/">read-after-new-write</Consistency>
```

Informations associées

"Valeurs de cohérence"

PRÉSERVER la cohérence du godet

La demande de cohérence PUT Bucket vous permet d'indiquer la cohérence à appliquer aux opérations effectuées sur un compartiment.

La cohérence par défaut est définie pour garantir la lecture après écriture des objets nouvellement créés.

Avant de commencer

Pour effectuer cette opération, vous devez disposer de l'autorisation s3:PutBuckeConsistency, ou être root de compte.

Demande

Le `x-ntap-sg-consistency` paramètre doit contenir l'une des valeurs suivantes :

La cohérence	Description
tous	Tous les nœuds reçoivent les données immédiatement, sinon la requête échoue.
forte croissance mondiale	Garantit une cohérence de lecture après écriture pour toutes les demandes client sur tous les sites.
site fort	Garantit la cohérence de lecture après écriture pour toutes les demandes client dans un site.
lecture-après-nouvelle-écriture	(Valeur par défaut) assure la cohérence en lecture après écriture des nouveaux objets et la cohérence des mises à jour des objets. Offre une haute disponibilité et une protection des données garanties. Recommandé dans la plupart des cas.

La cohérence	Description
disponibilité	Assure la cohérence 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.

Note: en général, vous devez utiliser la cohérence "lecture-après-nouvelle-écriture". Si les demandes ne fonctionnent pas correctement, modifiez le comportement du client d'application si possible. Ou configurez le client de manière à spécifier la cohérence pour chaque requête d'API. Réglez la cohérence au niveau du godet uniquement en dernier recours.

Exemple de demande

```
PUT /bucket?x-ntap-sg-consistency=strong-global HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Informations associées

"Valeurs de cohérence"

HEURE du dernier accès au compartiment

La demande D'heure de dernier accès À GET Bucket vous permet de déterminer si les dernières mises à jour de temps d'accès sont activées ou désactivées pour les compartiments individuels.

Pour effectuer cette opération, vous devez disposer de l'autorisation s3:GetBucketLastAccessTime, ou être root de compte.

Exemple de demande

```
GET /bucket?x-ntap-sg-lastaccesstime HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Exemple de réponse

Cet exemple montre que les mises à jour du temps de dernier accès sont activées pour le compartiment.

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/10.3.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<LastAccessTime xmlns="http://s3.storagegrid.com/doc/2015-02-01/">enabled
</LastAccessTime>
```

METTRE l'heure du dernier accès au compartiment

La demande d'heure de dernier accès AU compartiment PERMET d'activer ou de désactiver les mises à jour des temps de dernier accès pour chaque compartiment. La désactivation des mises à jour du temps d'accès précédent améliore les performances. Il s'agit du paramètre par défaut pour tous les compartiments créés avec la version 10.3.0, ou ultérieure.

Pour effectuer cette opération, vous devez disposer de l'autorisation s3:PutBuckLastAccessTime pour un compartiment ou être un compte root.

> ⓘ À partir de StorageGRID version 10.3, les mises à jour de l'heure du dernier accès sont désactivées par défaut pour tous les nouveaux compartiments. Si des compartiments ont été créés à l'aide d'une version antérieure de StorageGRID et que vous souhaitez faire correspondre le nouveau comportement par défaut, vous devez désactiver explicitement les mises à jour de la dernière heure d'accès pour chacune de ces rubriques précédentes. Vous pouvez activer ou désactiver les mises à jour de l'heure du dernier accès à l'aide de la demande PUT Bucket Last Access Time ou de la page de détails d'un compartiment dans le Gestionnaire de locataires. Voir "Activez ou désactivez les mises à jour de l'heure du dernier accès".

Si les dernières mises à jour de temps d'accès sont désactivées pour un compartiment, les opérations suivantes sont appliquées sur le compartiment :

- Les requêtes GetObject, GetObjectAcl, GetObjectTagging et HeadObject ne mettent pas à jour l'heure du dernier accès. L'objet n'est pas ajouté aux files d'attente pour l'évaluation de la gestion du cycle de vie des informations (ILM).
- Les requêtes CopyObject et PutObjectTagging qui ne mettent à jour que les métadonnées mettent également à jour l'heure du dernier accès. L'objet est ajouté aux files d'attente pour l'évaluation ILM.
- Si les mises à jour de l'heure du dernier accès sont désactivées pour le compartiment source, les requêtes CopyObject ne mettent pas à jour l'heure du dernier accès pour le compartiment source. L'objet copié n'est pas ajouté aux files d'attente pour l'évaluation ILM du compartiment source. Cependant, pour la destination, les requêtes CopyObject mettent toujours à jour l'heure du dernier accès. La copie de l'objet est ajoutée aux files d'attente pour l'évaluation ILM.
- CompleteMultipartUpload demande la mise à jour de l'heure du dernier accès. L'objet terminé est ajouté aux files d'attente pour l'évaluation ILM.

Exemples de demandes

Cet exemple permet d'activer le temps du dernier accès pour un compartiment.

```
PUT /bucket?x-ntap-sg-lastaccesstime=enabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Cet exemple désactive l'heure du dernier accès pour un compartiment.

```
PUT /bucket?x-ntap-sg-lastaccesstime=disabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

SUPPRIMEZ la configuration de notification des métadonnées de compartiment

La demande de configuration DE notification DE métadonnées DELETE Bucket vous permet de désactiver le service d'intégration de recherche pour les compartiments individuels en supprimant le XML de configuration.

Pour effectuer cette opération, vous devez disposer de l'autorisation s3:DeleteBuceMeteatanotification pour un compartiment, ou être un compte root.

Exemple de demande

Cet exemple montre la désactivation du service d'intégration de recherche pour un compartiment.

```
DELETE /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

CONFIGURATION DES notifications de métadonnées de compartiment

La demande de configuration DE notification DE métadonnées GET Bucket vous permet de récupérer le XML de configuration utilisé pour configurer l'intégration de la recherche pour chaque compartiment.

Pour effectuer cette opération, vous devez disposer de l'autorisation s3:GetBuckeMetadanotification, ou être root de compte.

Exemple de demande

Cette requête récupère la configuration de notification des métadonnées pour le compartiment nommé `bucket`.

```
GET /bucket?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Réponse

L'organe de réponse inclut la configuration de notification des métadonnées pour le compartiment. La configuration de notification des métadonnées vous permet de déterminer la configuration du compartiment pour l'intégration de la recherche. En d'autres termes, il vous permet de déterminer les objets à indexer et à quels terminaux leurs métadonnées d'objet sont envoyées.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>rule-status</Status>
        <Prefix>key-prefix</Prefix>
        <Destination>
           <Urn>arn:aws:es:_region:account-
ID_:domain/_mydomain/myindex/mytype_</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Rule-2</ID>
         ...
    </Rule>
     ...
</MetadataNotificationConfiguration>
```

Chaque configuration de notification de métadonnées comprend une ou plusieurs règles. Chaque règle indique les objets qu'elle s'applique ainsi que la destination à laquelle StorageGRID doit envoyer les métadonnées d'objet. Les destinations doivent être spécifiées à l'aide de l'URN d'un terminal StorageGRID.

Nom	Description	Obligatoire
Configuration de la MetadaNotificationConfiguration	Balise de conteneur pour les règles utilisées pour spécifier les objets et la destination des notifications de métadonnées. Contient un ou plusieurs éléments de règle.	Oui

Nom	Description	Obligatoire
Règle	Balise de conteneur d'une règle qui identifie les objets dont les métadonnées doivent être ajoutées à un index spécifié. Les règles avec des préfixes qui se chevauchent sont rejetées. Inclus dans l'élément MetadaNotificationConfiguration.	Oui
ID	Identifiant unique de la règle. Inclus dans l'élément règle.	Non
État	L'état peut être « activé » ou « désactivé ». Aucune action n'est prise pour les règles désactivées. Inclus dans l'élément règle.	Oui
Préfixe	Les objets qui correspondent au préfixe sont affectés par la règle et leurs métadonnées sont envoyées à la destination spécifiée. Pour faire correspondre tous les objets, spécifiez un préfixe vide. Inclus dans l'élément règle.	Oui
Destination	Balise de conteneur pour la destination d'une règle. Inclus dans l'élément règle.	Oui

Nom	Description	Obligatoire
Urne	URN de la destination où les métadonnées d'objet sont envoyées. Doit être l'URN d'un terminal StorageGRID avec les propriétés suivantes : • `es` doit être le troisième élément. • L'URN doit se terminer par l'index et le type où les métadonnées sont stockées, sous la forme `domain-name/myindex/mytype`. Les terminaux sont configurés à l'aide du Gestionnaire de locataires ou de l'API de gestion des locataires. Ils se présentent sous la forme suivante : • `arn:aws:es:_region:account-ID_:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` Le noeud final doit être configuré avant la soumission du XML de configuration, ou la configuration échouera avec une erreur 404. L'urne est incluse dans l'élément destination.	Oui

Exemple de réponse

Le XML inclus entre les `<MetadataNotificationConfiguration></MetadataNotificationConfiguration>` balises montre comment l'intégration avec un noeud final d'intégration de recherche est configurée pour le compartiment. Dans cet exemple, les métadonnées d'objet sont envoyées à un index Elasticsearch nommé `current` et type nommé `2017` qui est hébergé dans un domaine AWS nommé `records`.

```
HTTP/1.1 200 OK
Date: Thu, 20 Jul 2017 18:24:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/11.0.0
x-amz-request-id: 3832973499
Content-Length: 264
Content-Type: application/xml

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix>2017</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-
1:3333333:domain/records/current/2017</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

Informations associées

"Utilisez un compte de locataire"

CONFIGURATION de notification des métadonnées de compartiment

La demande de configuration DE notification DE métadonnées PUT compartiments vous permet d'activer le service d'intégration de la recherche pour chaque compartiment. Le XML de configuration de notification de métadonnées que vous fournissez dans le corps de la requête spécifie les objets dont les métadonnées sont envoyées à l'index de recherche de destination.

Pour effectuer cette opération, vous devez disposer de l'autorisation s3:PutBuckeMetadanotification pour un compartiment ou être un compte root.

Demande

La demande doit inclure la configuration de notification de métadonnées dans l'organisme de demande. Chaque configuration de notification de métadonnées comprend une ou plusieurs règles. Chaque règle spécifie les objets à lesquels elle s'applique, ainsi que la destination vers laquelle StorageGRID doit envoyer les métadonnées d'objet.

Les objets peuvent être filtrés sur le préfixe du nom de l'objet. Par exemple, vous pouvez envoyer des métadonnées pour les objets dont le préfixe est associé à une destination et pour `/images` les objets dont le préfixe est préfixe `/videos` à une autre.

Les configurations avec des préfixes qui se chevauchent ne sont pas valides et sont rejetées lorsqu'elles sont soumises. Par exemple, une configuration comprenant une règle pour les objets avec le préfixe et une seconde règle pour les objets avec `test` le préfixe `test2` ne serait pas autorisée.

Les destinations doivent être spécifiées à l'aide de l'URN d'un terminal StorageGRID. Le noeud final doit exister lorsque la configuration de notification des métadonnées est soumise, ou la demande échoue en tant que `400 Bad Request`. le message d'erreur indique : `Unable to save the metadata notification (search) policy. The specified endpoint URN does not exist: URN`.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>rule-status</Status>
        <Prefix>key-prefix</Prefix>
        <Destination>
           <Urn>arn:aws:es:region:account-
ID:domain/mydomain/myindex/mytype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Rule-2</ID>
         ...
    </Rule>
     ...
</MetadataNotificationConfiguration>
```

Le tableau décrit les éléments du XML de configuration de notification des métadonnées.

Nom	Description	Obligatoire
Configuration de la MetadaNotificationConfiguration	Balise de conteneur pour les règles utilisées pour spécifier les objets et la destination des notifications de métadonnées. Contient un ou plusieurs éléments de règle.	Oui
Règle	Balise de conteneur d'une règle qui identifie les objets dont les métadonnées doivent être ajoutées à un index spécifié. Les règles avec des préfixes qui se chevauchent sont rejetées. Inclus dans l'élément MetadaNotificationConfiguration.	Oui
ID	Identifiant unique de la règle. Inclus dans l'élément règle.	Non

Nom	Description	Obligatoire
État	L'état peut être « activé » ou « désactivé ». Aucune action n'est prise pour les règles désactivées. Inclus dans l'élément règle.	Oui
Préfixe	Les objets qui correspondent au préfixe sont affectés par la règle et leurs métadonnées sont envoyées à la destination spécifiée. Pour faire correspondre tous les objets, spécifiez un préfixe vide. Inclus dans l'élément règle.	Oui
Destination	Balise de conteneur pour la destination d'une règle. Inclus dans l'élément règle.	Oui
Urne	URN de la destination où les métadonnées d'objet sont envoyées. Doit être l'URN d'un terminal StorageGRID avec les propriétés suivantes : • `es` doit être le troisième élément. • L'URN doit se terminer par l'index et le type où les métadonnées sont stockées, sous la forme `domain-name/myindex/mytype`. Les terminaux sont configurés à l'aide du Gestionnaire de locataires ou de l'API de gestion des locataires. Ils se présentent sous la forme suivante : • `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` Le noeud final doit être configuré avant la soumission du XML de configuration, ou la configuration échouera avec une erreur 404. L'urne est incluse dans l'élément destination.	Oui

Exemples de demandes

Cet exemple montre l'activation de l'intégration de la recherche pour un compartiment. Dans cet exemple, les métadonnées d'objet de tous les objets sont envoyées vers la même destination.

```
PUT /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
           <Urn>urn:sgws:es:::sgws-notifications/test1/all</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

Dans cet exemple, les métadonnées d'objet des objets qui correspondent au préfixe `/images` sont envoyées à une destination, tandis que les métadonnées d'objet des objets correspondant au préfixe `/videos` sont envoyées à une seconde destination.

```
PUT /graphics?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Images-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/images</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Videos-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/videos</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

JSON généré par le service d'intégration de la recherche

Lorsque vous activez le service d'intégration de la recherche pour un compartiment, un document JSON est généré et envoyé au terminal de destination à chaque ajout, mise à jour ou suppression de métadonnées d'objet.

Cet exemple montre un exemple de fichier JSON qui pourrait être généré lors de la création d'un objet avec la clé `SGWS/Tagging.txt` dans un compartiment nommé `test`. Le `test` compartiment n'est pas versionné, la balise est donc `versionId` vide.

```
{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region":"us-east-1",
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}
```

Métadonnées d'objet incluses dans les notifications de métadonnées

Le tableau répertorie tous les champs inclus dans le document JSON qui est envoyé au noeud final de destination lorsque l'intégration de la recherche est activée.

Le nom du document inclut le nom du compartiment, le nom de l'objet et l'ID de version, le cas échéant.

Type	Nom de l'élément	Description
Informations sur les compartiments et les objets	godet	Nom du compartiment
Informations sur les compartiments et les objets	clé	Nom de clé d'objet
Informations sur les compartiments et les objets	ID de version	Version d'objet, pour les objets dans les compartiments multiversion
Informations sur les compartiments et les objets	région	Région de compartiment, par exemple `us-east-1`
Métadonnées de système	taille	Taille de l'objet (en octets) visible par un client HTTP
Métadonnées de système	md5	Hachage d'objets
Métadonnées d'utilisateur	métadonnées *`key:value`*	Toutes les métadonnées utilisateur pour l'objet, comme paires de clé-valeur

Type	Nom de l'élément	Description
Étiquettes	balises *key:value*	Toutes les balises d'objet définies pour l'objet, en tant que paires clé-valeur

> Pour les balises et les métadonnées d'utilisateur, StorageGRID transmet des dates et des chiffres à Elasticsearch en tant que chaînes ou notifications d'événement S3. Pour configurer Elasticsearch afin d'interpréter ces chaînes comme des dates ou des chiffres, suivez les instructions Elasticsearch pour un mappage dynamique des champs et un mappage des formats de date. Vous devez activer les mappages de champs dynamiques sur l'index avant de configurer le service d'intégration de la recherche. Une fois qu'un document est indexé, vous ne pouvez pas modifier les types de champ du document dans l'index.

Informations associées

"Utilisez un compte de locataire"

DEMANDE d'utilisation du stockage

La demande GET Storage usage vous indique la quantité totale de stockage utilisée par un compte et pour chaque compartiment associé au compte.

La quantité de stockage utilisée par un compte et ses compartiments peut être obtenue par une demande ListBuckets modifiée avec le `x-ntap-sg-usage` paramètre de requête. L'utilisation du stockage par compartiment est suivie séparément des demandes DE PUT et DELETE traitées par le système. Il peut y avoir un certain délai avant que les valeurs d'utilisation correspondent aux valeurs attendues en fonction du traitement des demandes, en particulier si le système est soumis à une charge importante.

Par défaut, StorageGRID tente de récupérer les informations d'utilisation à l'aide d'une cohérence globale forte. S'il est impossible d'obtenir une cohérence globale élevée, StorageGRID tente de récupérer les informations relatives à l'utilisation de façon cohérente sur les sites.

Pour effectuer cette opération, vous devez disposer de l'autorisation s3:ListAllMyseaux ou être root de compte.

Exemple de demande

```
GET /?x-ntap-sg-usage HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Exemple de réponse

Cet exemple montre un compte qui contient quatre objets et 12 octets de données dans deux compartiments. Chaque compartiment contient deux objets et six octets de données.

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 00:49:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/10.2.0
x-amz-request-id: 727237123
Content-Length: 427
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<UsageResult xmlns="http://s3.storagegrid.com/doc/2015-02-01">
<CalculationTime>2014-11-19T05:30:11.000000Z</CalculationTime>
<ObjectCount>4</ObjectCount>
<DataBytes>12</DataBytes>
<Buckets>
<Bucket>
<Name>bucket1</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
<Bucket>
<Name>bucket2</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
</Buckets>
</UsageResult>
```

Gestion des versions

Chaque version d'objet stockée contribuera aux `ObjectCount` valeurs et `DataBytes` dans la réponse. Les marqueurs de suppression ne sont pas ajoutés au `ObjectCount` total.

Informations associées

"Valeurs de cohérence"

Demandes de compartiment obsolètes pour la conformité des anciennes

Demandes de compartiment obsolètes pour la conformité des anciennes

Vous devrez peut-être utiliser l'API REST StorageGRID S3 pour gérer les compartiments qui ont été créés à l'aide de la fonctionnalité de conformité héritée.

Fonction de conformité obsolète

La fonctionnalité de conformité StorageGRID disponible dans les versions précédentes d'StorageGRID est obsolète et a été remplacée par le verrouillage d'objet S3.

Si vous avez précédemment activé le paramètre de conformité globale, le paramètre de verrouillage d'objet S3 global est activé dans StorageGRID 11.6. Vous ne pouvez plus créer de compartiments avec la conformité activée. Toutefois, si nécessaire, vous pouvez utiliser l'API REST StorageGRID S3 pour gérer tous les compartiments conformes existants.

- "Utilisez l'API REST S3 pour configurer le verrouillage objet S3"
- "Gestion des objets avec ILM"
- "Base de connaissances NetApp : comment gérer des compartiments conformes aux ancienne génération dans StorageGRID 11.5"

Demandes de conformité obsolètes :

- "Obsolète - METTRE les modifications de la demande de godet à des fins de conformité"

  L'élément XML SGCompliance est obsolète. Auparavant, vous pouviez inclure cet élément personnalisé StorageGRID dans le corps de demande XML facultatif de requêtes Put Bucket pour créer un compartiment conforme.

- "Obsolète : OBTENEZ la conformité des compartiments"

  La demande DE conformité DE GET Bucket est obsolète. Cependant, vous pouvez continuer à utiliser cette demande pour déterminer les paramètres de conformité actuellement en vigueur pour un compartiment compatible existant.

- "Obsolète : conformité DES compartiments PUT"

  La demande DE conformité DE PUT Bucket est obsolète. Cependant, vous pouvez continuer à utiliser cette demande pour modifier les paramètres de conformité d'un compartiment conforme existant. Par exemple, vous pouvez placer un compartiment existant en attente légale ou augmenter sa période de conservation.

Obsolète : CreateBucket demande des modifications pour la conformité

L'élément XML SGCompliance est obsolète. Auparavant, vous pouviez inclure cet élément personnalisé StorageGRID dans le corps de requête XML facultatif des requêtes CreateBucket pour créer un compartiment compatible.

> La fonctionnalité de conformité StorageGRID disponible dans les versions précédentes d'StorageGRID est obsolète et a été remplacée par le verrouillage d'objet S3. Pour plus d'informations, consultez les documents suivants :
>
> - "Utilisez l'API REST S3 pour configurer le verrouillage objet S3"
> - "Base de connaissances NetApp : comment gérer des compartiments conformes aux ancienne génération dans StorageGRID 11.5"

Vous ne pouvez plus créer de compartiments avec la fonctionnalité conformité activée. Le message d'erreur suivant est renvoyé si vous tentez d'utiliser les modifications de demande CreateBucket pour la conformité afin de créer un nouveau compartiment compatible :

```
The Compliance feature is deprecated.
Contact your StorageGRID administrator if you need to create new Compliant
buckets.
```

Obsolète : RÉCUPÉRER la demande de conformité du compartiment

La demande DE conformité DE GET Bucket est obsolète. Cependant, vous pouvez continuer à utiliser cette demande pour déterminer les paramètres de conformité actuellement en vigueur pour un compartiment compatible existant.

> La fonctionnalité de conformité StorageGRID disponible dans les versions précédentes d'StorageGRID est obsolète et a été remplacée par le verrouillage d'objet S3. Pour plus d'informations, consultez les documents suivants :
>
> - "Utilisez l'API REST S3 pour configurer le verrouillage objet S3"
> - "Base de connaissances NetApp : comment gérer des compartiments conformes aux ancienne génération dans StorageGRID 11.5"

Pour effectuer cette opération, vous devez disposer de l'autorisation s3:GetBucketCompliance ou être root de compte.

Exemple de demande

Cet exemple de demande vous permet de déterminer les paramètres de conformité du compartiment nommé `mybucket`.

```
GET /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Exemple de réponse

Dans le XML de réponse, `<SGCompliance>` répertorie les paramètres de conformité en vigueur pour le compartiment. Cet exemple de réponse montre les paramètres de conformité d'un compartiment dans lequel chaque objet sera conservé pendant un an (525,600 minutes), à partir de l'ingestion de l'objet dans la grille. Il n'y a actuellement aucune retenue légale sur ce godet. Chaque objet sera automatiquement supprimé après un an.

```
HTTP/1.1 200 OK
Date: date
Connection: connection
Server: StorageGRID/11.1.0
x-amz-request-id: request ID
Content-Length: length
Content-Type: application/xml

<SGCompliance>
  <RetentionPeriodMinutes>525600</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

Nom	Description
RetentionPeriodMinutes	Durée de conservation des objets ajoutés à ce compartiment, en minutes. La période de conservation commence lorsque l'objet est ingéré dans la grille.
LegalHold	• Vrai : ce compartiment est actuellement en attente légale. Les objets de ce compartiment ne peuvent pas être supprimés tant que la conservation légale n'est pas levée, même si leur période de conservation a expiré. • Faux : ce godet n'est pas actuellement en attente légale. Les objets de ce compartiment peuvent être supprimés à la fin de leur période de conservation.
Suppression automatique	• Vrai : les objets de ce compartiment sont automatiquement supprimés lors de leur expiration, à moins que le compartiment ne soit soumis à une obligation légale. • FALSE : les objets de ce compartiment ne sont pas supprimés automatiquement lorsque la période de conservation expire. Vous devez supprimer ces objets manuellement si vous devez les supprimer.

Réponses d'erreur

Si le compartiment n'a pas été créé pour être conforme, le code d'état HTTP de la réponse est `404 Not Found`, avec un code d'erreur S3 de `XNoSuchBucketCompliance`.

Obsolète : demande de conformité du compartiment PUT

La demande DE conformité DE PUT Bucket est obsolète. Cependant, vous pouvez continuer à utiliser cette demande pour modifier les paramètres de conformité d'un compartiment conforme existant. Par exemple, vous pouvez placer un compartiment existant en attente légale ou augmenter sa période de conservation.

La fonctionnalité de conformité StorageGRID disponible dans les versions précédentes d'StorageGRID est obsolète et a été remplacée par le verrouillage d'objet S3. Pour plus d'informations, consultez les documents suivants :

- "Utilisez l'API REST S3 pour configurer le verrouillage objet S3"
- "Base de connaissances NetApp : comment gérer des compartiments conformes aux ancienne génération dans StorageGRID 11.5"

Pour effectuer cette opération, vous devez disposer de l'autorisation s3:PutBuckCompliance, ou être root de compte.

Vous devez spécifier une valeur pour chaque champ des paramètres de conformité lors de l'émission d'une demande de conformité PUT Bucket.

Exemple de demande

Cet exemple de demande modifie les paramètres de conformité du compartiment nommé `mybucket`. Dans cet exemple, les objets dans `mybucket` seront conservés pendant deux ans (1,051,200 minutes) au lieu d'un an, à partir de la date d'ingestion de l'objet dans la grille. Il n'y a pas de retenue légale sur ce godet. Chaque objet sera automatiquement supprimé après deux ans.

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Content-Length: 152

<SGCompliance>
  <RetentionPeriodMinutes>1051200</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

Nom	Description
RetentionPeriodMinutes	Durée de conservation des objets ajoutés à ce compartiment, en minutes. La période de conservation commence lorsque l'objet est ingéré dans la grille. **Important** lorsque vous spécifiez une nouvelle valeur pour RetentionPeriodMinutes, vous devez spécifier une valeur égale ou supérieure à la période de rétention actuelle du compartiment. Une fois la période de rétention du compartiment définie, vous ne pouvez pas la réduire ; vous pouvez uniquement l'augmenter.

Nom	Description
LegalHold	• Vrai : ce compartiment est actuellement en attente légale. Les objets de ce compartiment ne peuvent pas être supprimés tant que la conservation légale n'est pas levée, même si leur période de conservation a expiré. • Faux : ce godet n'est pas actuellement en attente légale. Les objets de ce compartiment peuvent être supprimés à la fin de leur période de conservation.
Suppression automatique	• Vrai : les objets de ce compartiment sont automatiquement supprimés lors de leur expiration, à moins que le compartiment ne soit soumis à une obligation légale. • FALSE : les objets de ce compartiment ne sont pas supprimés automatiquement lorsque la période de conservation expire. Vous devez supprimer ces objets manuellement si vous devez les supprimer.

Cohérence pour les paramètres de conformité

Lorsque vous mettez à jour les paramètres de conformité d'un compartiment S3 avec une demande DE conformité PUT bucket, StorageGRID tente de mettre à jour les métadonnées du compartiment dans la grille. Par défaut, StorageGRID utilise la cohérence **strong-global** pour garantir que tous les sites de data Center et tous les nœuds de stockage contenant des métadonnées de compartiment disposent d'une cohérence de lecture après écriture pour les paramètres de conformité modifiés.

Si StorageGRID ne peut pas atteindre la cohérence **strong-global** car un site de centre de données ou plusieurs nœuds de stockage sur un site sont indisponibles, le code d'état HTTP de la réponse est `503 Service Unavailable`.

Si vous recevez cette réponse, vous devez contacter l'administrateur du grid pour vous assurer que les services de stockage requis sont disponibles dans les plus brefs délais. Si l'administrateur du grid ne parvient pas à rendre suffisamment de nœuds de stockage disponibles sur chaque site, le support technique peut vous demander de réessayer la demande en forçant la cohérence **strong-site**.

> Ne forcez jamais la cohérence **Strong-site** pour la conformité PUT bucket à moins que vous n'ayez été dirigé pour le faire par le support technique et à moins que vous ne compreniez les conséquences potentielles de l'utilisation de ce niveau.

Lorsque la cohérence est réduite à **strong-site**, StorageGRID garantit que les paramètres de conformité mis à jour auront une cohérence en lecture après écriture uniquement pour les demandes des clients au sein d'un site. Il est donc possible que le système StorageGRID dispose de plusieurs paramètres incohérents pour ce compartiment jusqu'à ce que tous les sites et nœuds de stockage soient disponibles. Les paramètres incohérents peuvent entraîner un comportement inattendu et indésirable. Par exemple, si vous placez un compartiment dans une conservation légale et que vous forcez une cohérence inférieure, les paramètres de conformité précédents du compartiment (c'est-à-dire la conservation légale) peuvent continuer à être en vigueur sur certains sites de data Center. Par conséquent, les objets qui, selon vous, sont en attente légale peuvent être supprimés à l'expiration de leur période de conservation, soit par l'utilisateur, soit par AutoDelete, si cette option est activée.

Pour forcer l'utilisation de la cohérence **strong-site**, relancez la demande de conformité PUT Bucket et incluez l' `Consistency-Control`en-tête de requête HTTP, comme suit :

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Consistency-Control: strong-site
```

Réponses d'erreur

- Si le compartiment n'a pas été créé pour être conforme, le code d'état HTTP de la réponse est `404 Not Found`.
- Si `RetentionPeriodMinutes` dans la requête est inférieure à la période de conservation actuelle du compartiment, le code d'état HTTP est `400 Bad Request`.

Informations associées

"Obsolète : METTEZ les modifications de la demande de compartiment à des fins de conformité"

Règles d'accès au compartiment et au groupe

Utilisez les règles d'accès au compartiment et au groupe

StorageGRID utilise le langage de règles Amazon Web Services (AWS) pour permettre aux locataires S3 de contrôler l'accès aux compartiments et aux objets dans ces compartiments. Le système StorageGRID implémente un sous-ensemble du langage de règles de l'API REST S3. Les règles d'accès de l'API S3 sont écrites au format JSON.

Présentation de la stratégie d'accès

Il existe deux types de politiques d'accès pris en charge par StorageGRID.

- **Stratégies de compartiment**, gérées à l'aide des opérations de l'API GetBucketPolicy, PutBuckePolicy et DeleteBuckePolicy S3 ou du gestionnaire de locataires ou de l'API de gestion des locataires. Les règles de compartiment sont liées aux compartiments. Elles sont donc configurées de façon à contrôler l'accès des utilisateurs du compte du propriétaire du compartiment ou d'autres comptes au compartiment et aux objets. Une politique de compartiment s'applique à un seul compartiment et peut-être à plusieurs groupes.
- **Stratégies de groupe**, qui sont configurées à l'aide du Gestionnaire de locataires ou de l'API de gestion des locataires. Les stratégies de groupe sont associées à un groupe du compte, de sorte qu'elles sont configurées de manière à permettre à ce groupe d'accéder à des ressources spécifiques appartenant à ce compte. Une stratégie de groupe s'applique à un seul groupe et peut-être plusieurs compartiments.

> ⓘ La priorité est la même entre les politiques de groupe et de compartiment.

Les règles de compartiment et de groupe StorageGRID respectent une grammaire spécifique définie par Amazon. À l'intérieur de chaque règle se trouve un ensemble d'énoncés de politique, et chaque instruction contient les éléments suivants :

- ID de déclaration (ID) (facultatif)
- Effet
- Principal/notPrincipal
- Ressource/NotResource
- Action/NotAction

- Condition (en option)

Les instructions de règles sont créées à l'aide de cette structure pour spécifier les autorisations : accorder <effet> pour autoriser/refuser <principal> d'exécuter <action> sur <ressource> lorsque <condition> s'applique.

Chaque élément de règle est utilisé pour une fonction spécifique :

Elément	Description
SID	L'élément Sid est facultatif. Le SID n'est destiné qu'à la description de l'utilisateur. Il est stocké mais non interprété par le système StorageGRID.
Effet	Utilisez l'élément d'effet pour déterminer si les opérations spécifiées sont autorisées ou refusées. Vous devez identifier les opérations que vous autorisez (ou refusez) les compartiments ou les objets à l'aide des mots clés action Element pris en charge.
Principal/notPrincipal	Vous pouvez autoriser les utilisateurs, groupes et comptes à accéder à des ressources spécifiques et à effectuer des actions spécifiques. Si aucune signature S3 n'est incluse dans la demande, l'accès anonyme est autorisé en spécifiant le caractère générique (*) comme principal. Par défaut, seul le root du compte peut accéder aux ressources qui lui sont propres. Il vous suffit de spécifier l'élément principal dans une stratégie de rubrique. Pour les stratégies de groupe, le groupe auquel la stratégie est associée est l'élément principal implicite.
Ressource/NotResource	L'élément ressource identifie les compartiments et les objets. Vous pouvez autoriser ou refuser des autorisations pour les compartiments et les objets en utilisant le nom de ressource Amazon (ARN) pour identifier la ressource.
Action/NotAction	Les éléments action et effet sont les deux composants des autorisations. Lorsqu'un groupe demande une ressource, l'accès à la ressource est accordé ou refusé. L'accès est refusé sauf si vous attribuez des autorisations spécifiques, mais vous pouvez utiliser le refus explicite pour remplacer une autorisation accordée par une autre stratégie.
Condition	L'élément condition est facultatif. Les conditions vous permettent de créer des expressions pour déterminer quand une stratégie doit être appliquée.

Dans l'élément action, vous pouvez utiliser le caractère générique (*) pour spécifier toutes les opérations ou un sous-ensemble d'opérations. Par exemple, cette action correspond à des autorisations telles que s3:GetObject, s3:PutObject et s3:DeleteObject.

```
s3:*Object
```

Dans l'élément ressource, vous pouvez utiliser les caractères génériques (*) et (?). Alors que l'astérisque (*) correspond à 0 caractères ou plus, le point d'interrogation (?) correspond à n'importe quel caractère.

Dans l'élément principal, les caractères génériques ne sont pas pris en charge, sauf pour définir l'accès anonyme, qui accorde l'autorisation à tout le monde. Par exemple, vous définissez le caractère générique (*) comme valeur principale.

```
"Principal":"*"
```

```
"Principal":{"AWS":"*"}
```

Dans l'exemple suivant, l'instruction utilise les éléments effet, principal, action et ressource. Cet exemple montre une instruction de stratégie de compartiment complète qui utilise l'effet « Autoriser » pour donner aux Principals, au groupe admin `federated-group/admin` et au groupe financier `federated-group/finance` , les autorisations d'effectuer l'action `s3:ListBucket` sur le compartiment nommé `mybucket` et l'action `s3:GetObject` sur tous les objets de ce compartiment.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::27233906934684427525:federated-group/admin",
          "arn:aws:iam::27233906934684427525:federated-group/finance"
        ]
      },
      "Action": [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::mybucket",
        "arn:aws:s3:::mybucket/*"
      ]
    }
  ]
}
```

La stratégie de compartiment a une taille limite de 20,480 octets et la stratégie de groupe a une taille limite de 5,120 octets.

Cohérence au niveau des règles

Par défaut, toutes les mises à jour apportées aux stratégies de groupe sont cohérentes. Lorsqu'une stratégie de groupe devient cohérente, les modifications peuvent prendre 15 minutes supplémentaires pour prendre

effet en raison de la mise en cache des règles. Par défaut, toutes les mises à jour des règles de compartiment sont fortement cohérentes.

Si nécessaire, vous pouvez modifier les garanties de cohérence pour les mises à jour des règles de compartiment. Par exemple, vous pouvez souhaiter qu'une modification de règle de compartiment soit disponible en cas de panne sur le site.

Dans ce cas, vous pouvez définir l' `Consistency-Control`en-tête dans la demande PutBucketPolicy ou utiliser la demande de cohérence PUT Bucket. Lorsqu'une règle de compartiment devient cohérente, les modifications peuvent prendre 8 secondes supplémentaires en raison de la mise en cache des règles.

> Si vous définissez la cohérence sur une valeur différente pour contourner une situation temporaire, assurez-vous de rétablir la valeur d'origine du paramètre de niveau du compartiment lorsque vous avez terminé. Dans le cas contraire, toutes les futures demandes de compartiment utiliseront le paramètre modifié.

Utilisez ARN dans les énoncés de politique

Dans les instructions de politique, le ARN est utilisé dans les éléments principal et ressource.

- Utilisez cette syntaxe pour spécifier la ressource S3 ARN :

```
arn:aws:s3:::bucket-name
arn:aws:s3:::bucket-name/object_key
```

- Utilisez cette syntaxe pour spécifier la ressource d'identité ARN (utilisateurs et groupes) :

```
arn:aws:iam::account_id:root
arn:aws:iam::account_id:user/user_name
arn:aws:iam::account_id:group/group_name
arn:aws:iam::account_id:federated-user/user_name
arn:aws:iam::account_id:federated-group/group_name
```

Autres considérations :

- Vous pouvez utiliser l'astérisque (*) comme caractère générique pour correspondre à zéro ou plus de caractères dans la clé d'objet.
- Les caractères internationaux, qui peuvent être spécifiés dans la clé d'objet, doivent être codés à l'aide de JSON UTF-8 ou de séquences d'échappement JSON \u. Le codage pourcentage n'est pas pris en charge.

  "Syntaxe RFC 2141 URN"

  Le corps de requête HTTP pour l'opération PutBucketPolicy doit être codé avec charset=UTF-8.

Spécifiez les ressources dans une stratégie

Dans les instructions de stratégie, vous pouvez utiliser l'élément ressource pour spécifier le compartiment ou l'objet pour lequel les autorisations sont autorisées ou refusées.

- Chaque instruction de stratégie nécessite un élément ressource. Dans une stratégie, les ressources sont signalées par l'élément `Resource`, ou, alternativement, `NotResource` pour exclusion.
- Vous spécifiez des ressources avec une ressource S3 ARN. Par exemple :

```
"Resource": "arn:aws:s3:::mybucket/*"
```

- Vous pouvez également utiliser des variables de règles à l'intérieur de la clé d'objet. Par exemple :

```
"Resource": "arn:aws:s3:::mybucket/home/${aws:username}/*"
```

- La valeur de ressource peut spécifier un compartiment qui n'existe pas encore lorsqu'une stratégie de groupe est créée.

Spécifiez les entités de gestion dans une stratégie

Utilisez l'élément principal pour identifier l'utilisateur, le groupe ou le compte locataire qui est autorisé/refusé l'accès à la ressource par l'instruction de stratégie.

- Chaque énoncé de politique dans une politique de rubrique doit inclure un élément principal. Les énoncés de politique dans une stratégie de groupe n'ont pas besoin de l'élément principal car le groupe est considéré comme le principal.
- Dans une police, les principaux sont désignés par l'élément « principal » ou par l'élément « noPrincipal » pour exclusion.
- Les identités basées sur les comptes doivent être spécifiées à l'aide d'un ID ou d'un ARN :

```
"Principal": { "AWS": "account_id"}
"Principal": { "AWS": "identity_arn" }
```

- Dans cet exemple, le compte locataire utilise l'ID 27233906934684427525, qui inclut le compte root et tous les utilisateurs du compte :

```
 "Principal": { "AWS": "27233906934684427525" }
```

- Vous pouvez spécifier uniquement la racine du compte :

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:root" }
```

- Vous pouvez spécifier un utilisateur fédéré spécifique (« Alex ») :

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
user/Alex" }
```

- Vous pouvez spécifier un groupe fédéré spécifique (« gestionnaires ») :

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
group/Managers"  }
```

- Vous pouvez spécifier un principal anonyme :

```
"Principal": "*"
```

- Pour éviter toute ambiguïté, vous pouvez utiliser l'UUID de l'utilisateur au lieu du nom d'utilisateur :

```
arn:aws:iam::27233906934684427525:user-uuid/de305d54-75b4-431b-adb2-
eb6b9e546013
```

  Par exemple, supposons qu'Alex quitte l'organisation et que le nom d'utilisateur `Alex` est supprimé. Si un nouveau Alex rejoint l'organisation et se voit attribuer le même `Alex` nom d'utilisateur, le nouvel utilisateur peut involontairement hériter des autorisations accordées à l'utilisateur d'origine.

- La valeur principale peut spécifier un nom de groupe/utilisateur qui n'existe pas encore lors de la création d'une stratégie de compartiment.

Spécifiez les autorisations dans une stratégie

Dans une stratégie, l'élément action est utilisé pour autoriser/refuser des autorisations à une ressource. Il existe un ensemble d'autorisations que vous pouvez spécifier dans une stratégie, qui sont désignées par l'élément « action » ou par « NotAction » pour exclusion. Chacun de ces éléments est associé à des opérations spécifiques d'API REST S3.

Le tableau répertorie les autorisations qui s'appliquent aux compartiments et aux autorisations qui s'appliquent aux objets.

> Amazon S3 utilise désormais l'autorisation s3:PutReplicationConfiguration pour les actions PutBuckeReplication et DeleteBuckeReplication. StorageGRID utilise des autorisations distinctes pour chaque action, qui correspond à la spécification Amazon S3 d'origine.

> Une suppression est effectuée lorsqu'une entrée est utilisée pour remplacer une valeur existante.

Autorisations qui s'appliquent aux compartiments

Autorisations	OPÉRATIONS DES API REST S3	Personnalisée pour StorageGRID
s3:CreateBucket	CreateBucket	Oui. **Remarque** : utiliser uniquement dans la stratégie de groupe.
s3:DeleteBucket	DeleteBucket	
s3:DeleteBuckeMetadatanotification	SUPPRIMEZ la configuration de notification des métadonnées de compartiment	Oui
s3:DeleteBucketPolicy	DeleteBucketPolicy	
s3:DeleteReplicationConfiguration	DeleteBuckeReplication	Oui, des autorisations séparées pour PUT et DELETE
s3:GetBucketAcl	GetBucketAcl	
s3:GetBuckeCompliance	GARANTIR la conformité des compartiments (obsolète)	Oui
s3:persistance GetBucketConsistency	OPTIMISEZ la cohérence des compartiments	Oui
s3:GetBucketCORS	GetBucketCors	
s3:GetEncryptionConfiguration	GetBucketEncryption	
s3:GetBucketLastAccessTime	HEURE du dernier accès au compartiment	Oui
s3:GetBucketLocation	GetBuckeLocation	
s3:GetBucketMetadatanotification	CONFIGURATION DES notifications de métadonnées de compartiment	Oui
s3:GetBuckenotification	GetBucketNotifationConfiguration	
s3:GetBuckeObjectLockConfiguration	GetObjectLockConfiguration	
s3:GetBucketPolicy	GetBucketPolicy	

Autorisations	OPÉRATIONS DES API REST S3	Personnalisée pour StorageGRID
s3:GetBucketTagging	GetBucketTagging	
s3:GetBucketVersioning	GetBucketVersioning	
s3:GetLifecyclConfiguration	GetBucketLifecycleConfiguration	
s3:GetReplicationTM	GetBuckeReplication	
s3:ListAllMyseaux	• Listseaux • DÉCOUVREZ l'utilisation du stockage	Oui, pour OBTENIR l'utilisation du stockage. **Remarque** : utiliser uniquement dans la stratégie de groupe.
s3:ListBucket	• ListObjects • Godet principal • Objet de restauration	
s3:ListBuckMultipartUploads	• ListMultipartUploads • Objet de restauration	
s3:ListBuckeVersions	OBTENIR les versions de compartiment	
s3:PutBuckeCompliance	MISE en conformité des compartiments (obsolète)	Oui
s3:persistance de PutBuckeConsistency	PRÉSERVER la cohérence du godet	Oui
s3:PutBuckeCORS	• DeleteBuckeCors† • PutBucketCors	
s3:PutEncryptionConfiguration	• DeleteBuckeEncryption • PutBucketEncryption	
s3:PutBuckeLastAccessTime	METTRE l'heure du dernier accès au compartiment	Oui
s3:PutBuckeMetadanotification	CONFIGURATION de notification des métadonnées de compartiment	Oui
s3:PutBuckenotification	PutBucketNotifationConfiguration	

Autorisations	OPÉRATIONS DES API REST S3	Personnalisée pour StorageGRID
s3:PutBuckObjectLockConfiguration	• CreateBucket avec l' `x-amz-bucket-object-lock-enabled: true`en-tête de requête (nécessite également l'autorisation s3:CreateBucket) • PutObjectLockConfiguration	
s3:PutBuckePolicy	PutBuckePolicy	
s3:PutBuckeTagging	• DeleteBucketTagging† • Étiquetage PutBucketTagging	
s3:PutBuckeVersioning	PutBuckeVersioning	
s3:PutLifecyclConfiguration	• DeleteBuckeLifecycle† • PutBucketLifecycleConfiguration	
s3:PutReplicationTM	PutBuckeReplication	Oui, des autorisations séparées pour PUT et DELETE

Autorisations qui s'appliquent aux objets

Autorisations	OPÉRATIONS DES API REST S3	Personnalisée pour StorageGRID
s3:AbortMultipartUpload	• AbortMultipartUpload • Objet de restauration	
s3:BipassGovernanceRetention	• DeleteObject • DeleteObjects • PutObjectRetention	
s3:DeleteObject	• DeleteObject • DeleteObjects • Objet de restauration	
s3:DeleteObjectTagging	DeleteObjectTagging	
s3:DeleteObjectVersionTagging	DeleteObjectTagging (une version spécifique de l'objet)	

Autorisations	OPÉRATIONS DES API REST S3	Personnalisée pour StorageGRID
s3:DeleteObjectVersion	DeleteObject (une version spécifique de l'objet)	
s3:GetObject	• GetObject • Objet principal • Objet de restauration • SelectObjectContent	
s3:GetObjectAcl	GetObjectAcl	
s3:GetObjectLegalHold	GetObjectLegalHold	
s3:GetObjectRetention	GetObjectRetention	
s3:GetObjectTagging	GetObjectTagging	
s3:GetObjectVersionTagging	GetObjectTagging (une version spécifique de l'objet)	
s3:GetObjectVersion	GetObject (une version spécifique de l'objet)	
s3:ListMultipartUploadParts	ListParts, RestoreObject	
s3:PutObject	• PutObject • Objet de copie • Objet de restauration • CreateMultipartUpload • CompleteMultipartUpload • UploadPart • UploadPartCopy	
s3:PutObjectLegalHold	PutObjectLegalHold	
s3:PutObjectRetention	PutObjectRetention	
s3:PutObjectTagging	Marquage PutObject	
s3:PutObjectVersionTagging	PutObjectTagging (une version spécifique de l'objet)	

Autorisations	OPÉRATIONS DES API REST S3	Personnalisée pour StorageGRID
s3:PutOverwriteObject	• PutObject • Objet de copie • Marquage PutObject • DeleteObjectTagging • CompleteMultipartUpload	Oui
s3:RestoreObject	Objet de restauration	

Utiliser l'autorisation PutOverwriteObject

L'autorisation s3:PutOverwriteObject est une autorisation StorageGRID personnalisée qui s'applique aux opérations qui créent ou mettent à jour des objets. Le paramètre de cette autorisation détermine si le client peut remplacer les données d'un objet, les métadonnées définies par l'utilisateur ou le balisage d'objets S3.

Les paramètres possibles pour cette autorisation sont les suivants :

- **Autoriser** : le client peut écraser un objet. Il s'agit du paramètre par défaut.
- **Deny** : le client ne peut pas écraser un objet. Lorsque cette option est définie sur Deny, l'autorisation PutOverwriteObject fonctionne comme suit :
  - Si un objet existant se trouve sur le même chemin :
    - Les données de l'objet, les métadonnées définies par l'utilisateur ou le balisage d'objets S3 ne peuvent pas être remplacés.
    - Toutes les opérations d'entrée en cours sont annulées et une erreur est renvoyée.
    - Si la gestion des versions S3 est activée, le paramètre deny empêche les opérations PutObjectTagging ou DeleteObjectTagging de modifier le TagSet d'un objet et ses versions non actuelles.
  - Si aucun objet existant n'est trouvé, cette autorisation n'a aucun effet.
- Lorsque cette autorisation n'est pas présente, l'effet est le même que si autorisation a été définie.

> Si la règle S3 actuelle autorise l'écrasement et que l'autorisation PutOverwriteObject est définie sur refuser, le client ne peut pas écraser les données d'un objet, les métadonnées définies par l'utilisateur ou le balisage d'objet. En outre, si la case **empêcher la modification du client** est cochée (**CONFIGURATION** > **Paramètres de sécurité** > **réseau et objets**), ce paramètre remplace le paramètre de l'autorisation PutOverwriteObject.

Spécifiez les conditions dans une stratégie

Les conditions définissent le moment où une police sera en vigueur. Les conditions sont constituées d'opérateurs et de paires de clé-valeur.

Les conditions utilisent des paires de clé-valeur pour l'évaluation. Un élément condition peut contenir plusieurs conditions, et chaque condition peut contenir plusieurs paires clé-valeur. Le bloc condition utilise le format suivant :

```
Condition: {
     condition_type: {
          condition_key: condition_values
```

Dans l'exemple suivant, la condition ipaddress utilise la clé condition SourceIp.

```
"Condition": {
    "IpAddress": {
      "aws:SourceIp": "54.240.143.0/24"
        ...
},
        ...
```

Opérateurs de condition pris en charge

Les opérateurs de condition sont classés comme suit :

- Chaîne
- Valeur numérique
- Booléen
- Adresse IP
- Vérification nulle

Opérateurs de condition	Description
Equals à jambes de chaîne	Compare une clé à une valeur de chaîne en fonction de la correspondance exacte (sensible à la casse).
Equals stringNotEquals	Compare une clé à une valeur de chaîne basée sur la correspondance niée (sensible à la casse).
StringEqualisIgnoreCase	Compare une clé à une valeur de chaîne basée sur la correspondance exacte (ignore case).
StringNotEqualisIgnoreCase	Compare une clé à une valeur de chaîne basée sur la correspondance nérée (ignore le cas).
StringLike	Compare une clé à une valeur de chaîne en fonction de la correspondance exacte (sensible à la casse). Peut inclure des caractères génériques * et ?.
StringNotLike	Compare une clé à une valeur de chaîne basée sur la correspondance niée (sensible à la casse). Peut inclure des caractères génériques * et ?.

Opérateurs de condition	Description
Valeurs numériques	Compare une touche à une valeur numérique en fonction de la correspondance exacte.
NumericNotEquals	Compare une touche à une valeur numérique basée sur la correspondance annulée.
NumericGreaterThan	Compare une touche à une valeur numérique basée sur une correspondance « supérieure à ».
NumericGreaterThanEquals	Compare une clé à une valeur numérique basée sur une correspondance « supérieure ou égale ».
NumericLessThan	Compare une clé à une valeur numérique basée sur une correspondance « inférieure à ».
NumericLessThanEquals	Compare une clé à une valeur numérique basée sur une correspondance « inférieure ou égale ».
BOOL	Compare une clé à une valeur booléenne basée sur une correspondance « vrai ou faux ».
Adresse IP	Compare une clé à une adresse IP ou une plage d'adresses IP.
Adresse de la note	Compare une clé à une adresse IP ou une plage d'adresses IP basée sur la correspondance annulée.
Nul	Vérifie si une clé condition est présente dans le contexte de demande actuel.

Touches de condition prises en charge

Touches condition	Actions	Description
aws:SourceIp	Opérateurs IP	Compare à l'adresse IP à partir de laquelle la demande a été envoyée. Peuvent être utilisées pour les opérations de compartiment ou d'objet. **Remarque :** si la requête S3 a été envoyée via le service Load Balancer sur les nœuds Admin et les passerelles, cela se compare à l'adresse IP en amont du service Load Balancer. **Remarque** : si un équilibreur de charge tiers non transparent est utilisé, il sera comparé à l'adresse IP de cet équilibreur de charge. N'importe quel `X-Forwarded-For` en-tête sera ignoré car sa validité ne peut pas être établie.

Touches condition	Actions	Description
aws:nom d'utilisateur	Ressource/identité	Compare le nom d'utilisateur de l'expéditeur à partir duquel la demande a été envoyée. Peuvent être utilisées pour les opérations de compartiment ou d'objet.
s3:délimiteur	s3:ListBucket et s3:permissions ListBuckeVersions	Compare avec le paramètre délimiteur spécifié dans une demande ListObjects ou ListObjectVersions.
s3:ExistingObjectTag/<tag-key>	s3:DeleteObjectTagging s3:DeleteObjectVersionTagging s3:GetObject s3:GetObjectAcl 3:GetObjectTagging s3:GetObjectVersion s3:GetObjectVersionAcl s3:GetObjectVersionTagging s3:PutObjectAcl s3:PutObjectTagging s3:PutObjectVersionAcl s3:PutObjectVersionTagging	Exige que l'objet existant ait la clé et la valeur de balise spécifiques.
s3:touches max	s3:ListBucket et s3:permissions ListBuckeVersions	Compare avec le paramètre max-keys spécifié dans une requête ListObjects ou ListObjectVersions.

Touches condition	Actions	Description
s3 :conservation des jours restants avec un verrouillage objet	s3:PutObject	Compare à la date de conservation jusqu'à spécifiée dans l'en-tête de la demande ou calculée à `x-amz-object-lock-retain-until-date` partir de la période de conservation par défaut du compartiment pour s'assurer que ces valeurs sont dans la plage autorisée pour les demandes suivantes : • PutObject • Objet de copie • CreateMultipartUpload
s3 :conservation des jours restants avec un verrouillage objet	s3:PutObjectRetention	Compare à la date de conservation jusqu'à spécifiée dans la demande PutObjectRetention pour s'assurer qu'elle se trouve dans la plage autorisée.
s3:préfixe	s3:ListBucket et s3:permissions ListBuckeVersions	Compare avec le paramètre de préfixe spécifié dans une requête ListObjects ou ListObjectVersions.
s3:RequestObjectTag/<tag-key>	s3:PutObject s3:PutObjectTagging s3:PutObjectVersionTagging	Nécessitera une clé de balise et une valeur spécifiques lorsque la demande d'objet inclut le balisage.

Spécifiez les variables d'une règle

Vous pouvez utiliser des variables dans les règles pour remplir les informations relatives aux règles lorsqu'elles sont disponibles. Vous pouvez utiliser des variables de règles dans l' `Resource`élément et dans des comparaisons de chaînes dans l' `Condition`élément.

Dans cet exemple, la variable `${aws:username}` fait partie de l'élément ressource :

```
"Resource": "arn:aws:s3:::bucket-name/home/${aws:username}/*"
```

Dans cet exemple, la variable `${aws:username}` fait partie de la valeur de condition dans le bloc condition :

```
"Condition": {
    "StringLike": {
      "s3:prefix": "${aws:username}/*"
        ...
},
        ...
```

Variable	Description
`${aws:SourceIp}`	Utilise la touche SourceIp comme variable fournie.
`${aws:username}`	Utilise la clé de nom d'utilisateur comme variable fournie.
`${s3:prefix}`	Utilise la clé de préfixe spécifique au service comme variable fournie.
`${s3:max-keys}`	Utilise la touche max-keys spécifique au service comme variable fournie.
`${*}`	Caractère spécial. Utilise le caractère comme caractère littéral *.
`${?}`	Caractère spécial. Utilise le caractère comme un caractère littéral ?.
`${$}`	Caractère spécial. Utilise le caractère comme caractère littéral $.

Créez des règles nécessitant une gestion spéciale

Parfois, une politique peut accorder des autorisations dangereuses pour la sécurité ou dangereuses pour les opérations continues, telles que le verrouillage de l'utilisateur racine du compte. L'implémentation de l'API REST StorageGRID S3 est moins restrictive lors de la validation des règles qu'Amazon, mais tout aussi stricte lors de l'évaluation des règles.

Description de la politique	Type de règle	Comportement Amazon	Comportement de StorageGRID
Refusez vous-même toutes les autorisations sur le compte racine	Godet	Valide et appliquée, mais le compte utilisateur root conserve les autorisations nécessaires pour toutes les opérations des règles de compartiment S3	Identique
Refusez vous-même les autorisations d'accès à l'utilisateur/au groupe	Groupe	Valide et appliquée	Identique
Autoriser un groupe de comptes étrangers toute autorisation	Godet	Principal non valide	Valide, mais les autorisations pour toutes les opérations de stratégie de compartiment S3 renvoient une erreur 405 méthode non autorisée lorsque cela est autorisé par une règle

Description de la politique	Type de règle	Comportement Amazon	Comportement de StorageGRID
Autoriser un utilisateur ou une racine de compte étranger à accorder toute autorisation	Godet	Valide, mais les autorisations pour toutes les opérations de stratégie de compartiment S3 renvoient une erreur 405 méthode non autorisée lorsque cela est autorisé par une règle	Identique
Autoriser tout le monde à autoriser toutes les actions	Godet	Valide, mais les autorisations pour toutes les opérations de politique de compartiment S3 renvoient une erreur 405 méthode non autorisée pour la racine du compte étranger et les utilisateurs	Identique
Refuser les autorisations de tous pour toutes les actions	Godet	Valide et appliquée, mais le compte utilisateur root conserve les autorisations nécessaires pour toutes les opérations des règles de compartiment S3	Identique
Le principal est un utilisateur ou un groupe inexistant	Godet	Principal non valide	Valide
La ressource est un compartiment S3 inexistant	Groupe	Valide	Identique
Principal est un groupe local	Godet	Principal non valide	Valide
La stratégie accorde à un compte non propriétaire (y compris les comptes anonymes) des autorisations de placer des objets.	Godet	Valide. Les objets sont détenus par le compte de créateur et la stratégie de compartiment ne s'applique pas. Le compte créateur doit accorder des autorisations d'accès à l'objet à l'aide des listes de contrôle d'accès d'objet.	Valide. Les objets sont la propriété du compte du propriétaire du compartiment. La politique de compartiment s'applique.

Protection WORM (Write-once, Read-many)

Vous pouvez créer des compartiments WORM (Write-once, Read-many) pour protéger les données, les métadonnées d'objet définies par l'utilisateur et le balisage d'objets S3. Vous configurez les compartiments WORM pour permettre la création de nouveaux objets et empêcher les écrasements ou la suppression de contenu existant. Utilisez l'une des approches décrites ici.

Pour vous assurer que les écrasements sont toujours refusés, vous pouvez :

- Dans le Gestionnaire de grille, accédez à **CONFIGURATION** > **sécurité** > **Paramètres de sécurité** > **réseau et objets**, puis cochez la case **empêcher la modification du client**.
- Appliquez les règles suivantes et les règles S3 :
  - Ajoutez une opération DE REFUS PutOverwriteObject à la règle S3.
  - Ajoutez une opération DE REFUS DeleteObject à la règle S3.
  - Ajoutez une opération PutObject ALLOW à la règle S3.

> La définition de DeleteObject sur REFUSER dans une règle S3 n'empêche pas ILM de supprimer des objets lorsqu'une règle telle que « zéro copie après 30 jours » existe.

> Même lorsque toutes ces règles et politiques sont appliquées, elles ne protègent pas contre les écritures simultanées (voir situation A). Ils protègent contre les écrasements séquentiels terminés (voir situation B).

Situation A: Écritures simultanées (non protégées contre)

```
/mybucket/important.doc
PUT#1 ---> OK
PUT#2 -------> OK
```

Situation B: Remplacements séquentiels terminés (protégés contre)

```
/mybucket/important.doc
PUT#1 -------> PUT#2 ---X (denied)
```

Informations associées

- "Gestion des objets par les règles StorageGRID ILM"
- "Exemples de politiques de compartiments"
- "Exemples de stratégies de groupe"
- "Gestion des objets avec ILM"
- "Utilisez un compte de locataire"

Exemples de politiques de compartiments

Utilisez les exemples de cette section pour créer des règles d'accès StorageGRID pour les compartiments.

Les politiques de compartiment spécifient les autorisations d'accès pour le compartiment à lequel la politique est attachée. Pour configurer une stratégie de compartiment, utilisez l'API PutBucketPolicy S3 au moyen de l'un des outils suivants :

- "Gestionnaire de locataires".

- CLI AWS utilisant cette commande (voir "Opérations sur les compartiments") :

```
> aws s3api put-bucket-policy --bucket examplebucket --policy
file://policy.json
```

Exemple : autoriser tout le monde à accéder en lecture seule à un compartiment

Dans cet exemple, tout le monde, y compris anonyme, est autorisé à répertorier les objets dans le compartiment et à effectuer des opérations GetObject sur tous les objets du compartiment. Toutes les autres opérations seront refusées. Notez que cette politique peut ne pas être particulièrement utile, car personne, à l'exception de la racine du compte, ne peut écrire dans le compartiment.

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadOnlyAccess",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:GetObject", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket","arn:aws:s3:::examplebucket/*"]
    }
  ]
}
```

Exemple : autoriser l'accès complet de tous les utilisateurs d'un compte et permettre à chacun d'un autre compte d'accéder en lecture seule à un compartiment

Dans cet exemple, tout le monde d'un compte spécifié est autorisé à accéder à un compartiment, tandis que tous les utilisateurs d'un autre compte spécifié sont uniquement autorisés à répertorier le compartiment et à effectuer des opérations GetObject sur les objets du compartiment en commençant par le `shared/` préfixe de clé d'objet.

> Dans StorageGRID, les objets créés par un compte autre que le propriétaire (y compris les comptes anonymes) sont détenus par le compte du propriétaire du compartiment. La politique de compartiment s'applique à ces objets.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "95390887230002558202"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::examplebucket/shared/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::examplebucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "shared/*"
        }
      }
    }
  ]
}
```

Exemple : autoriser tout le monde à accéder en lecture seule à un compartiment et à accéder entièrement au groupe spécifié

Dans cet exemple, tout le monde, y compris anonyme, est autorisé à répertorier le compartiment et à effectuer des opérations GetObject sur tous les objets du compartiment, alors que seuls les utilisateurs appartenant au groupe `Marketing` du compte spécifié ont un accès complet.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/Marketing"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": ["s3:ListBucket","s3:GetObject"],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}
```

Exemple : autoriser tout le monde à lire et à écrire l'accès à un compartiment si le client se trouve dans la plage IP

Dans cet exemple, tout le monde, y compris anonyme, est autorisé à répertorier le compartiment et à effectuer toutes les opérations objet sur tous les objets du compartiment, à condition que les demandes proviennent d'une plage IP spécifiée (54.240.143.0 à 54.240.143.255, sauf 54.240.143.188). Toutes les autres opérations seront refusées et toutes les demandes en dehors de la plage IP seront refusées.

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadWriteAccessIfInSourceIpRange",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:*Object", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket","arn:aws:s3:::examplebucket/*"],
      "Condition": {
        "IpAddress": {"aws:SourceIp": "54.240.143.0/24"},
        "NotIpAddress": {"aws:SourceIp": "54.240.143.188"}
      }
    }
  ]
}
```

Exemple : autoriser un accès complet à un compartiment exclusivement par un utilisateur fédéré spécifié

Dans cet exemple, l'utilisateur fédéré Alex est autorisé à accéder entièrement au `examplebucket` compartiment et à ses objets. Tous les autres utilisateurs, y compris « root », sont explicitement refusés à toutes les opérations. Notez toutefois que « root » n'est jamais refusé les autorisations de mettre/obtenir/DeleteBuckePolicy.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Deny",
      "NotPrincipal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}
```

Exemple : autorisation PutOverwriteObject

Dans cet exemple, l' `Deny`effet de PutOverwriteObject et DeleteObject garantit que personne ne peut écraser ou supprimer les données de l'objet, les métadonnées définies par l'utilisateur et le balisage d'objet S3.

```
{
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "s3:PutOverwriteObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion"
      ],
      "Resource": "arn:aws:s3:::wormbucket/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"

},
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::wormbucket"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"

},
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::wormbucket/*"
    }
  ]
}
```

Exemples de stratégies de groupe

Utilisez les exemples de cette section pour créer des stratégies d'accès StorageGRID pour les groupes.

Les stratégies de groupe spécifient les autorisations d'accès pour le groupe auquel la stratégie est associée. Il n'y a pas d' `Principal`élément dans la règle car elle est implicite. Les règles de groupe sont configurées à l'aide du Gestionnaire de locataires ou de l'API.

Exemple : définissez la stratégie de groupe à l'aide du Gestionnaire de locataires

Lorsque vous ajoutez ou modifiez un groupe dans le Gestionnaire de locataires, vous pouvez sélectionner une stratégie de groupe pour déterminer les autorisations d'accès S3 dont les membres de ce groupe auront accès. Voir "Créez des groupes pour un locataire S3".

- **Pas d'accès S3** : option par défaut. Les utilisateurs de ce groupe n'ont pas accès aux ressources S3, sauf si l'accès est accordé avec une règle de compartiment. Si vous sélectionnez cette option, seul l'utilisateur root peut accéder aux ressources S3 par défaut.
- **Accès en lecture seule** : les utilisateurs de ce groupe ont accès en lecture seule aux ressources S3. Par exemple, les utilisateurs de ce groupe peuvent afficher la liste des objets et lire les données d'objet, les métadonnées et les balises. Lorsque vous sélectionnez cette option, la chaîne JSON pour une stratégie de groupe en lecture seule s'affiche dans la zone de texte. Vous ne pouvez pas modifier cette chaîne.
- **Accès complet** : les utilisateurs de ce groupe ont accès aux ressources S3, y compris aux compartiments. Lorsque vous sélectionnez cette option, la chaîne JSON pour une stratégie de groupe à accès complet s'affiche dans la zone de texte. Vous ne pouvez pas modifier cette chaîne.
- **Atténuation des ransomware** : cet exemple de politique s'applique à tous les compartiments pour ce locataire. Les utilisateurs de ce groupe peuvent effectuer des actions courantes, mais ne peuvent pas supprimer définitivement des objets des compartiments pour lesquels la gestion des versions d'objet est activée.

  Les utilisateurs du Gestionnaire de locataires disposant de l'autorisation gérer tous les compartiments peuvent remplacer cette stratégie de groupe. Limitez l'autorisation gérer tous les compartiments aux utilisateurs de confiance et utilisez l'authentification multifacteur (MFA), le cas échéant.

- **Custom** : les utilisateurs du groupe disposent des autorisations que vous spécifiez dans la zone de texte.

Exemple : autoriser l'accès complet du groupe à toutes les rubriques

Dans cet exemple, tous les membres du groupe sont autorisés à accéder à tous les compartiments appartenant au compte du locataire, sauf s'ils sont explicitement refusés par la politique de compartiment.

```
{
  "Statement": [
    {
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

Exemple : autoriser l'accès en lecture seule du groupe à tous les compartiments

Dans cet exemple, tous les membres du groupe ont un accès en lecture seule aux ressources S3, à moins qu'ils ne soient explicitement refusés par la règle de compartiment. Par exemple, les utilisateurs de ce groupe peuvent afficher la liste des objets et lire les données d'objet, les métadonnées et les balises.

```
{
  "Statement": [
    {
      "Sid": "AllowGroupReadOnlyAccess",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

Exemple : autorisez les membres du groupe à accéder entièrement à leur « dossier » uniquement dans un compartiment

Dans cet exemple, les membres du groupe ne sont autorisés qu'à répertorier et accéder à leur dossier spécifique (préfixe de clé) dans le compartiment spécifié. Notez que les autorisations d'accès à partir d'autres stratégies de groupes et de la règle de compartiment doivent être prises en compte lors de la détermination de la confidentialité de ces dossiers.

```
{
  "Statement": [
    {
      "Sid": "AllowListBucketOfASpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::department-bucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "${aws:username}/*"
        }
      }
    },
    {
      "Sid": "AllowUserSpecificActionsOnlyInTheSpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:*Object",
      "Resource": "arn:aws:s3:::department-bucket/${aws:username}/*"
    }
  ]
}
```

Opérations S3 suivies dans les journaux d'audit

Les messages d'audit sont générés par les services StorageGRID et stockés dans des fichiers journaux texte. Vous pouvez consulter les messages d'audit spécifiques à S3 dans le journal d'audit pour obtenir des informations détaillées sur les opérations relatives aux compartiments et aux objets.

Les opérations des compartiments sont suivies dans les journaux d'audit

- CreateBucket
- DeleteBucket
- DeleteBucketTagging
- DeleteObjects
- GetBucketTagging
- Godet principal
- ListObjects
- ListObjectVersions
- METTEZ le godet en conformité
- Étiquetage PutBucketTagging
- PutBuckeVersioning

Opérations d'objet suivies dans les journaux d'audit

- CompleteMultipartUpload
- Objet de copie
- DeleteObject
- GetObject
- Objet principal
- PutObject
- Objet de restauration
- SelectObject
- UploadPart (lorsqu'une règle ILM utilise un ingestion équilibrée ou stricte)
- UploadPartCopy (lorsqu'une règle ILM utilise un ingestion équilibrée ou stricte)

Informations associées

- "Accéder au fichier journal d'audit"
- "Écrire des messages d'audit client"
- "Messages d'audit de lecture du client"

Utilisation de l'API REST Swift (fin de vie)

Utilisez l'API REST de Swift

La prise en charge de l'API Swift est arrivée en fin de vie et sera supprimée dans une prochaine version.

Les détails SWIFT ont été supprimés de cette version du site doc. Voir "StorageGRID 11.8 : utilisez l'API REST Swift".

Informations sur le copyright

Informations sur les marques commerciales