Utiliser StorageGRID

StorageGRID

NetApp
October 03, 2025

Sommaire

Utiliser StorageGRID . . . 1
- Utilisez un compte de locataire . . . 1
  - À l'aide du Gestionnaire de locataires . . . 1
  - Gestion de l'accès au système pour les utilisateurs locataires . . . 16
  - Gestion des comptes de locataires S3 . . . 38
  - Gestion des services de la plateforme S3 . . . 67
- Utilisation de S3 . . . 109
  - Prise en charge de l'API REST S3 . . . 109
  - Configuration des comptes et des connexions des locataires . . . 113
  - Comment StorageGRID implémente l'API REST S3 . . . 119
  - Opérations et limites prises en charge par l'API REST S3 . . . 126
  - Opérations des API REST StorageGRID S3 . . . 179
  - Règles d'accès au compartiment et au groupe . . . 202
  - Configuration de la sécurité pour l'API REST . . . 228
  - Surveillance et audit des opérations . . . 231
  - Avantages des connexions HTTP actives, inactives et simultanées . . . 234
- Utiliser Swift . . . 237
  - Prise en charge de l'API OpenStack Swift dans StorageGRID . . . 237
  - Configuration des comptes et des connexions des locataires . . . 241
  - Opérations prises en charge par l'API REST Swift . . . 245
  - Opérations de l'API REST StorageGRID Swift . . . 258
  - Configuration de la sécurité pour l'API REST . . . 263
  - Surveillance et audit des opérations . . . 266

Utiliser StorageGRID

Utilisez un compte de locataire

Découvrez comment utiliser un compte de locataire StorageGRID.

- "À l'aide du Gestionnaire de locataires"
- "Gestion de l'accès au système pour les utilisateurs locataires"
- "Gestion des comptes de locataires S3"
- "Gestion des services de la plateforme S3"

À l'aide du Gestionnaire de locataires

Le gestionnaire de locataires permet de gérer tous les aspects d'un compte de locataire StorageGRID.

Vous pouvez utiliser le gestionnaire des locataires pour surveiller l'utilisation du stockage d'un compte de locataire et gérer les utilisateurs avec une fédération des identités ou en créant des groupes et des utilisateurs locaux. Pour les comptes locataires S3, vous pouvez également gérer des clés S3, gérer des compartiments S3 et configurer les services de plateforme.

Utilisation d'un compte de locataire StorageGRID

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.

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

Il est possible d'utiliser des comptes de tenant pour isoler les objets stockés par différentes entités. 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. Il n'est pas nécessaire de créer des comptes de tenant distincts. Voir les instructions d'implémentation des applications client S3.

- **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.

Création de comptes de tenant

Les comptes de locataires sont créés par un administrateur grid StorageGRID à l'aide de Grid Manager. Lors de la création d'un compte de locataire, l'administrateur du grid spécifie les informations suivantes :

- Nom d'affichage du locataire (l'ID de compte du locataire est attribué automatiquement et ne peut pas être modifié).
- Si le compte de locataire utilise S3 ou Swift.
- Pour les comptes de locataire S3 : si le compte de locataire est autorisé à utiliser des services de plateforme. Si l'utilisation des services de plateforme est autorisée, la grille doit être configurée pour prendre en charge leur utilisation.
- Éventuellement, un quota de stockage pour le compte du locataire, soit le nombre maximal de gigaoctets, téraoctets ou pétaoctets disponibles pour les objets du locataire. Le quota de stockage d'un locataire représente une quantité logique (taille d'objet), et non une quantité physique (taille sur disque).
- Si la fédération des identités est activée pour le système StorageGRID, quel groupe fédéré a l'autorisation d'accès racine pour configurer le compte de tenant.
- Si l'authentification unique (SSO) n'est pas utilisée pour le système StorageGRID, que le compte de tenant utilise son propre référentiel d'identité ou partage le référentiel d'identité de la grille et le mot de passe initial de l'utilisateur racine local du locataire.

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.

Configuration des locataires S3

Une fois le compte de locataire S3 créé, vous pouvez accéder au Gestionnaire des locataires pour effectuer les tâches suivantes :

- Configuration de la fédération des identités (sauf si le référentiel d'identité est partagé avec la grille) ou création de groupes et d'utilisateurs locaux
- Gestion des clés d'accès S3
- Création et gestion des compartiments S3, notamment des compartiments conformes
- Utilisation des services de plate-forme (si activé)
- Contrôle de l'utilisation du stockage

> Vous pouvez créer et gérer des compartiments S3 avec le Gestionnaire des locataires. Toutefois, vous devez disposer de clés d'accès S3 et utiliser l'API REST S3 pour ingérer et gérer les objets.

Configuration des locataires Swift

Après la création d'un compte de locataire Swift, les utilisateurs disposant de l'autorisation accès racine peuvent accéder au Gestionnaire de locataires pour effectuer les tâches suivantes :

- Configuration de la fédération des identités (sauf si le référentiel d'identité est partagé avec la grille) et création de groupes et d'utilisateurs locaux
- Contrôle de l'utilisation du stockage

Les utilisateurs Swift doivent disposer de l'autorisation d'accès racine pour accéder au gestionnaire de locataires. Toutefois, l'autorisation accès racine ne permet pas aux utilisateurs de s'authentifier auprès de l'API REST Swift pour créer des conteneurs et ingérer des objets. Les utilisateurs doivent disposer de l'autorisation Administrateur Swift pour s'authentifier dans l'API REST de Swift.

Informations associées

"Administrer StorageGRID"

"Utilisation de S3"

"Utiliser Swift"

Navigateurs Web pris en charge

Vous devez utiliser un navigateur Web pris en charge.

Navigateur Web	Version minimale prise en charge
Google Chrome	87
Microsoft Edge	87
Mozilla Firefox	84

Vous devez régler la fenêtre du navigateur sur une largeur recommandée.

Largeur du navigateur	Pixels
Minimum	1024
Optimale	1280

Connexion au Gestionnaire de locataires

Pour accéder au Gestionnaire de locataires, entrez l'URL du locataire dans la barre d'adresse d'un navigateur Web pris en charge.

Ce dont vous avez besoin

- Vous devez disposer de vos identifiants de connexion.
- Vous devez disposer d'une URL pour accéder au Gestionnaire de locataires, telle que fournie par votre administrateur de grid. 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 contient toujours le nom de domaine complet (FQDN) ou l'adresse IP utilisée pour accéder à un nœud d'administration, et peut également inclure un numéro de port, l'ID de compte de locataire à 20 chiffres, ou les deux.

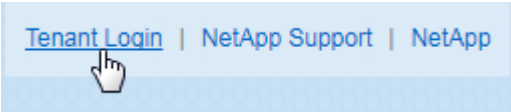
- Si l'URL n'inclut pas l'ID de compte à 20 chiffres du locataire, vous devez avoir cet ID de compte.
- Vous devez utiliser un navigateur Web pris en charge.
- Les cookies doivent être activés dans votre navigateur Web.
- Vous devez disposer d'autorisations d'accès spécifiques.

Étapes

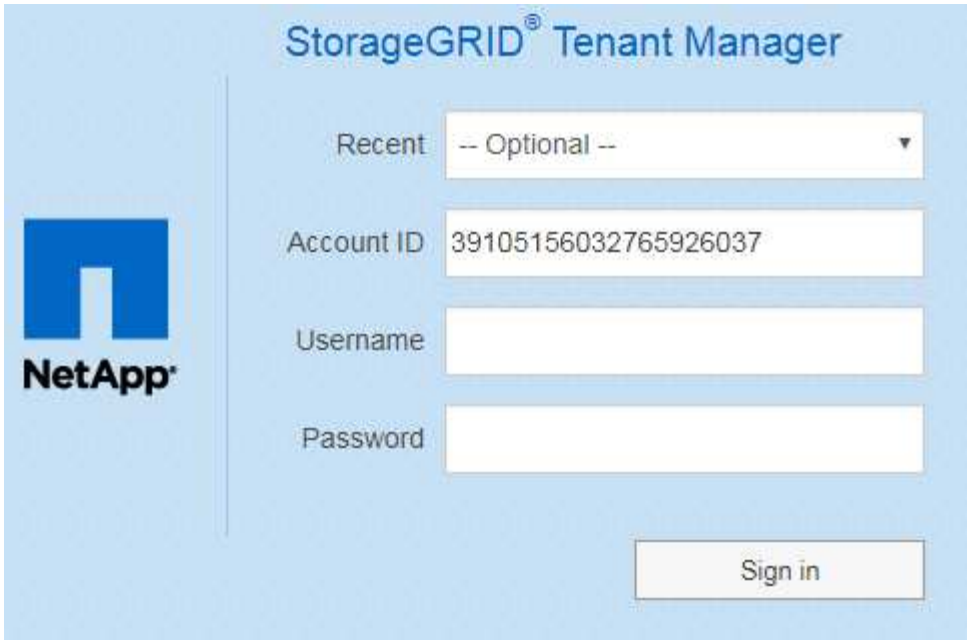
1. Lancez un navigateur Web pris en charge.
2. Dans la barre d'adresse du navigateur, entrez l'URL d'accès au Gestionnaire de locataires.
3. Si vous êtes invité à recevoir une alerte de sécurité, installez le certificat à l'aide de l'assistant d'installation du navigateur.
4. Connectez-vous au Gestionnaire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

   L'écran de connexion que vous voyez dépend de l'URL que vous avez saisie et de l'utilisation de SSO (Single Sign-on) par votre organisation. Vous verrez l'un des écrans suivants :

   - Page de connexion de Grid Manager. Cliquez sur le lien **tenant Login** dans le coin supérieur droit.

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



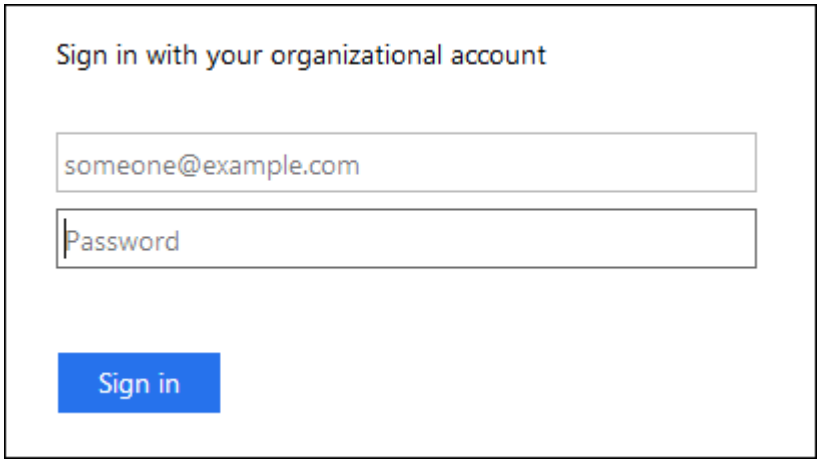
i. Si l'ID de compte à 20 chiffres du locataire ne s'affiche pas, sélectionnez le nom du compte du locataire s'il apparaît dans la liste des comptes récents ou saisissez l'ID du compte.

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

iii. Cliquez sur **connexion**.

Le tableau de bord de tenant Manager s'affiche.

◦ La page SSO de votre entreprise, si SSO est activé sur le grid. Par exemple :



Entrez vos informations d'identification SSO standard, puis cliquez sur **connexion**.

◦ 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. Cliquez sur **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 de tenant Manager s'affiche.

5. Si vous avez reçu un mot de passe initial de quelqu'un d'autre, modifiez votre mot de passe pour sécuriser votre compte. Sélectionnez ***username*** > **Modifier le mot de passe**.

> Si l'authentification SSO est activée pour le système StorageGRID, vous ne pouvez pas modifier votre mot de passe à partir du Gestionnaire de locataires.

Informations associées

"Administrer StorageGRID"

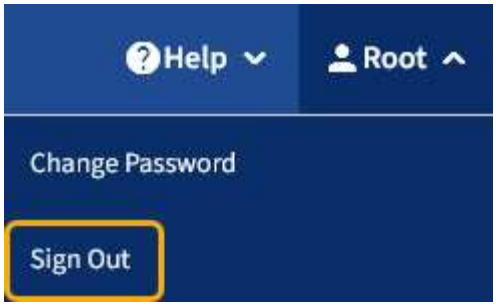
"Navigateurs Web pris en charge"

Déconnexion 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 **Déconnexion**.

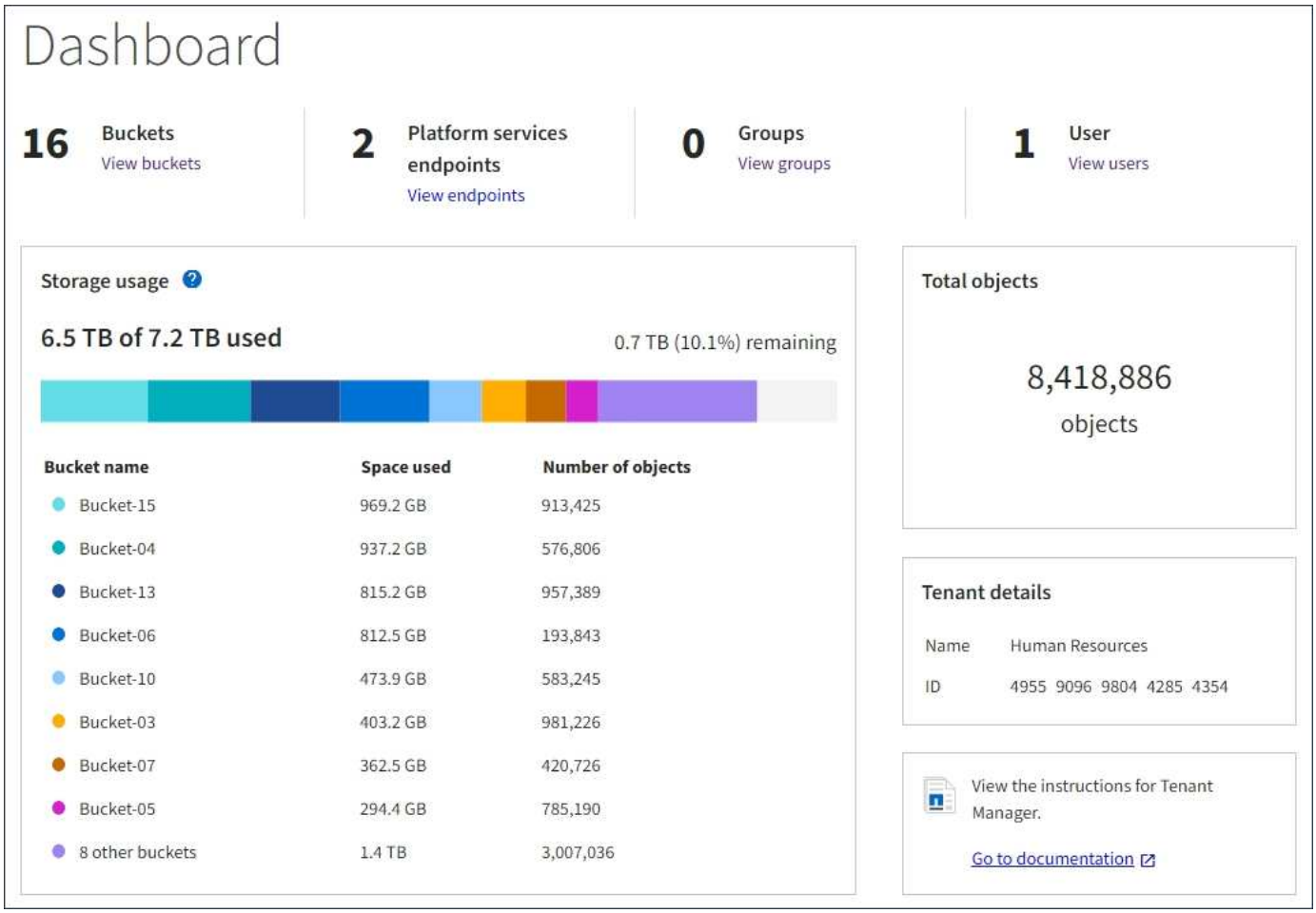
Option	Description
SSO non utilisé	Vous êtes déconnecté du nœud d'administration. La page de connexion au Gestionnaire de locataires s'affiche. **Remarque :** si vous vous êtes connecté à plusieurs nœuds d'administration, vous devez vous déconnecter de chaque nœud.
SSO activé	Vous êtes déconnecté de 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. **Remarque :** 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 de tenant Manager

Le tableau de bord de tenant Manager présente la configuration des comptes d'un locataire ainsi que la quantité d'espace utilisé par les objets dans les compartiments (S3) ou les conteneurs (Swift) du locataire. Si le locataire dispose d'un quota, le tableau de bord affiche la part du quota utilisée et la quantité restante. En cas d'erreurs liées au compte du locataire, les erreurs sont affichées sur 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.

Lorsque des objets ont été téléchargés, le Tableau de bord ressemble à l'exemple suivant :



Récapitulatif du compte de locataire

La partie supérieure du tableau de bord contient les informations suivantes :

- Le nombre de compartiments ou de conteneurs configurés, de groupes et d'utilisateurs
- Le nombre de terminaux de services de plate-forme, le cas échéant, ont été configurés

Vous pouvez sélectionner les liens pour afficher les détails.

La partie droite du tableau de bord contient les informations suivantes :

- Nombre total d'objets pour le locataire.

  Pour un compte S3, si aucun objet n'a été ingéré et que vous disposez de l'autorisation d'accès racine, les instructions relatives à la mise en route s'affichent au lieu du nombre total d'objets.

- Nom et ID du compte de locataire.
- Un lien vers la documentation StorageGRID.

Utilisation du stockage et des quotas

Le panneau utilisation du stockage contient les informations suivantes :

- Volume des données d'objet pour le locataire.

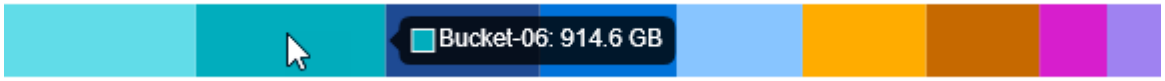
Cette valeur indique la quantité totale de données d'objet chargées et ne représente pas l'espace utilisé pour stocker les copies de ces objets et leurs métadonnées.

- 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 être temporairement empêché de charger de nouveaux objets jusqu'à ce que l'utilisation des quotas soit recalculée. Le calcul de l'utilisation des quotas peut prendre au moins 10 minutes.

- 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.

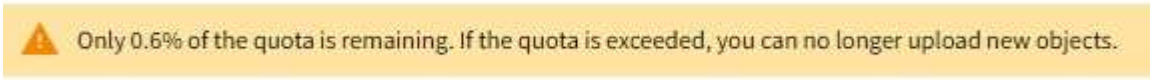
Bucket name	Space used	Number of objects
Bucket-02	944.7 GB	7,575
Bucket-09	899.6 GB	589,677
Bucket-15	889.6 GB	623,542
Bucket-06	846.4 GB	648,619
Bucket-07	730.8 GB	808,655
Bucket-04	700.8 GB	420,493
Bucket-11	663.5 GB	993,729
Bucket-03	656.9 GB	379,329
9 other buckets	2.3 TB	5,171,588

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.

Alertes d'utilisation des quotas

Si les alertes d'utilisation des quotas ont été activées dans Grid Manager, elles s'affichent 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. Pour plus d'informations, consultez la référence des alertes dans les instructions de surveillance et de dépannage de StorageGRID.

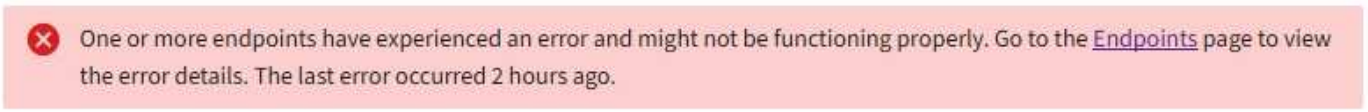


Si vous dépassez votre quota, vous ne pouvez pas télécharger de nouveaux objets.

Pour afficher des informations supplémentaires et gérer les règles et notifications relatives aux alertes, reportez-vous aux instructions de surveillance et de dépannage de StorageGRID.

Erreurs de point final

Si vous avez utilisé Grid Manager pour configurer un ou plusieurs terminaux pour les services de plateforme, le tableau de bord du Gestionnaire de locataires affiche une alerte si des erreurs de point final se sont produites au cours des sept derniers jours.



Pour afficher des détails sur une erreur de point final, sélectionnez noeuds finaux pour afficher la page noeuds finaux.

Informations associées

"Dépannage des erreurs de point final des services de plate-forme"

"Moniteur et amp ; dépannage"

Présentation 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 plateforme d'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.

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

Étapes

1. Connectez-vous au Gestionnaire de locataires.
2. Sélectionnez **aide** > **Documentation API** dans l'en-tête Gestionnaire de locataires.

Opérations d'API

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

- **Compte** — opérations sur le compte de locataire actuel, y compris l'obtention des 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 fournissez 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 »).

  Voir « protection contre la contrefaçon de demandes intersites » pour des informations sur l'amélioration de la sécurité de l'authentification.

  > Si l'authentification unique (SSO) est activée pour le système StorageGRID, vous devez effectuer différentes étapes pour l'authentification. Consultez la section « authentification dans l'API si l'authentification unique est activée » dans les instructions d'administration de StorageGRID.

- **Config** — opérations liées à la version du produit et aux versions de l'API tenant Management. Vous pouvez lister la version du produit ainsi que les versions principales de l'API prises en charge par cette version.
- **Conteneurs** — opérations sur des compartiments S3 ou des conteneurs Swift, comme suit :

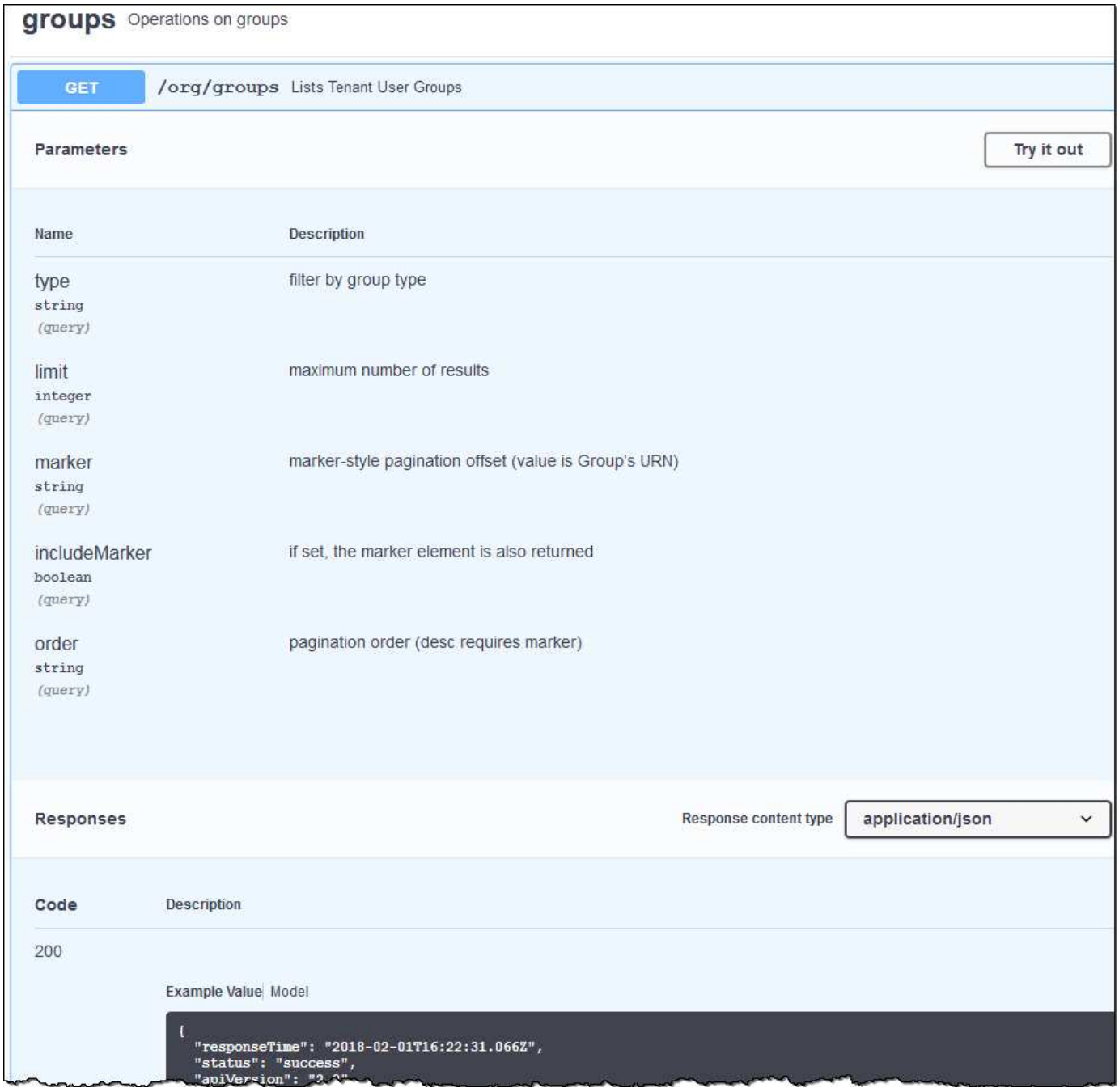
Protocole	L'autorisation permet
S3	• Création de compartiments conformes et non conformes • Modification des paramètres de conformité hérités • Définition du contrôle de cohérence pour les opérations effectuées sur les objets • Création, mise à jour et suppression de la configuration CORS d'un compartiment • Activation et désactivation des mises à jour de l'heure du dernier accès des objets • Gestion des paramètres de configuration des services de plateforme, y compris la réplication CloudMirror, les notifications et l'intégration de la recherche (notification-métadonnées) • Suppression de compartiments vides
SWIFT	Définition du niveau de cohérence utilisé pour les conteneurs

- **DESACTIVE-fonctions** — opérations pour afficher les fonctions qui pourraient avoir été 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.
- **Groupes** — opérations pour gérer des groupes de locataires locaux et extraire des groupes de locataires fédérés à partir d'un référentiel d'identité externe.
- **Identity-source** — opérations pour configurer un référentiel d'identité externe et synchroniser manuellement les informations de groupe et d'utilisateur fédérés.
- **Régions** — opérations pour déterminer les régions qui ont été configurées pour le système StorageGRID.
- **s3** — opérations pour gérer les clés d'accès S3 pour les utilisateurs locataires.
- **s3-Object-lock** — opérations pour déterminer comment le verrouillage d'objet S3 global (conformité) est configuré pour le système StorageGRID.
- **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.



Émission de requêtes API

Toutes les opérations d'API que vous effectuez à l'aide de la page Web API Docs 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. Cliquez sur 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 cliquer sur **modèle** pour connaître les exigences de chaque champ.

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

Informations associées

"Protection contre la contrefaçon de demandes intersites (CSRF)"

"Administrer StorageGRID"

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 3 de l'API.

```
https://hostname_or_ip_address/api/v3/authorize
```

La version majeure de l'API de gestion des locataires est incrémentée lorsque des modifications sont effectuées, qui sont ***non compatibles*** avec des versions antérieures. La version mineure de l'API de gestion des locataires est incrémentée lorsque des modifications sont effectuées que ***sont compatibles*** avec des versions antérieures. 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

Lors de la première installation du logiciel StorageGRID, seule la version la plus récente de l'API de gestion des locataires est activée. Cependant, lorsque StorageGRID est mis à niveau vers une nouvelle version de fonction, vous continuez à accéder à l'ancienne version de l'API pour au moins une version de StorageGRID.

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

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

Utilisez la requête d'API suivante pour renvoyer une liste des versions principales de l'API prises en charge :

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2019-01-10T20:41:00.845Z",
  "status": "success",
  "apiVersion": "3.0",
  "data": [
    2,
    3
  ]
}
```

Spécification d'une version d'API pour une requête

Vous pouvez spécifier la version de l'API à l'aide d'un paramètre de chemin d'accès (`/api/v3`) ou un en-tête (`Api-Version: 3`). Si vous indiquez les deux valeurs, la valeur de l'en-tête remplace la valeur du chemin d'accès.

```
curl https://[IP-Address]/api/v3/grid/accounts

curl -H "Api-Version: 3" 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 l' `csrfToken` paramètre à `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"
```

Si vrai, un `GridCsrfToken` Le cookie est défini avec une valeur aléatoire pour les connexions dans Grid Manager et dans `AccountCsrfToken` Le cookie est défini avec une valeur aléatoire pour les connexions au Gestionnaire de locataires.

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 :

- Le `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 par formulaire : a `csrfToken` paramètre corps de demande codé par formulaire.

Reportez-vous à la documentation en ligne de l'API pour obtenir des exemples et des détails supplémentaires.

> Les demandes disposant d'un jeu de cookies de jeton CSRF appliquent également le `"Content-Type: application/json"` En-tête pour toute demande qui attend un corps de requête JSON comme une protection supplémentaire contre les attaques CSRF.

Gestion de l'accès au système pour les utilisateurs locataires

Vous accordez aux utilisateurs l'accès à un compte de tenant en important des groupes à partir d'un référentiel d'identité fédéré et en attribuant des autorisations de gestion. Vous pouvez également créer des groupes et des utilisateurs de locataires locaux, sauf si l'authentification unique (SSO) est en vigueur pour l'ensemble du système StorageGRID.

- "Utilisation de la fédération des identités"
- "Gestion des groupes"
- "Gestion des utilisateurs locaux"

Utilisation de 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.

- "Configuration d'un référentiel d'identité fédéré"
- "Forcer la synchronisation avec le référentiel d'identité"
- "Désactivation de la fédération des identités"

Configuration d'un référentiel d'identité fédéré

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

Ce dont vous avez besoin

- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.
- Vous devez utiliser Active Directory, 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 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.

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.

Étapes

1. Sélectionnez **ACCESS MANAGEMENT** > **identity federation**.
2. Sélectionnez **Activer la fédération d'identités**.
3. Dans la section Type de service LDAP, sélectionnez **Active Directory**, **OpenLDAP** ou **Other**.

   Si vous sélectionnez **OpenLDAP**, configurez le serveur OpenLDAP. Reportez-vous aux instructions de configuration d'un serveur OpenLDAP.

   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.
   - **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. Dans la section configurer le serveur LDAP, entrez les informations de serveur LDAP et de connexion réseau requises.
   - **Nom d'hôte** : le nom d'hôte du serveur 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`
   - **Mot de passe** : mot de passe associé au nom d'utilisateur.
   - **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'utilisateur** : 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.
6. Dans la section **transport Layer Security (TLS)**, sélectionnez un paramètre de sécurité.
   - **Utilisez STARTTLS (recommandé)** : utilisez STARTTLS pour sécuriser les communications avec le serveur LDAP. Il s'agit de l'option recommandée.
   - **Utilisez LDAPS** : l'option LDAPS (LDAP sur SSL) utilise TLS pour établir une connexion au serveur LDAP. Cette option est prise en charge pour des raisons de compatibilité.
   - **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 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 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.

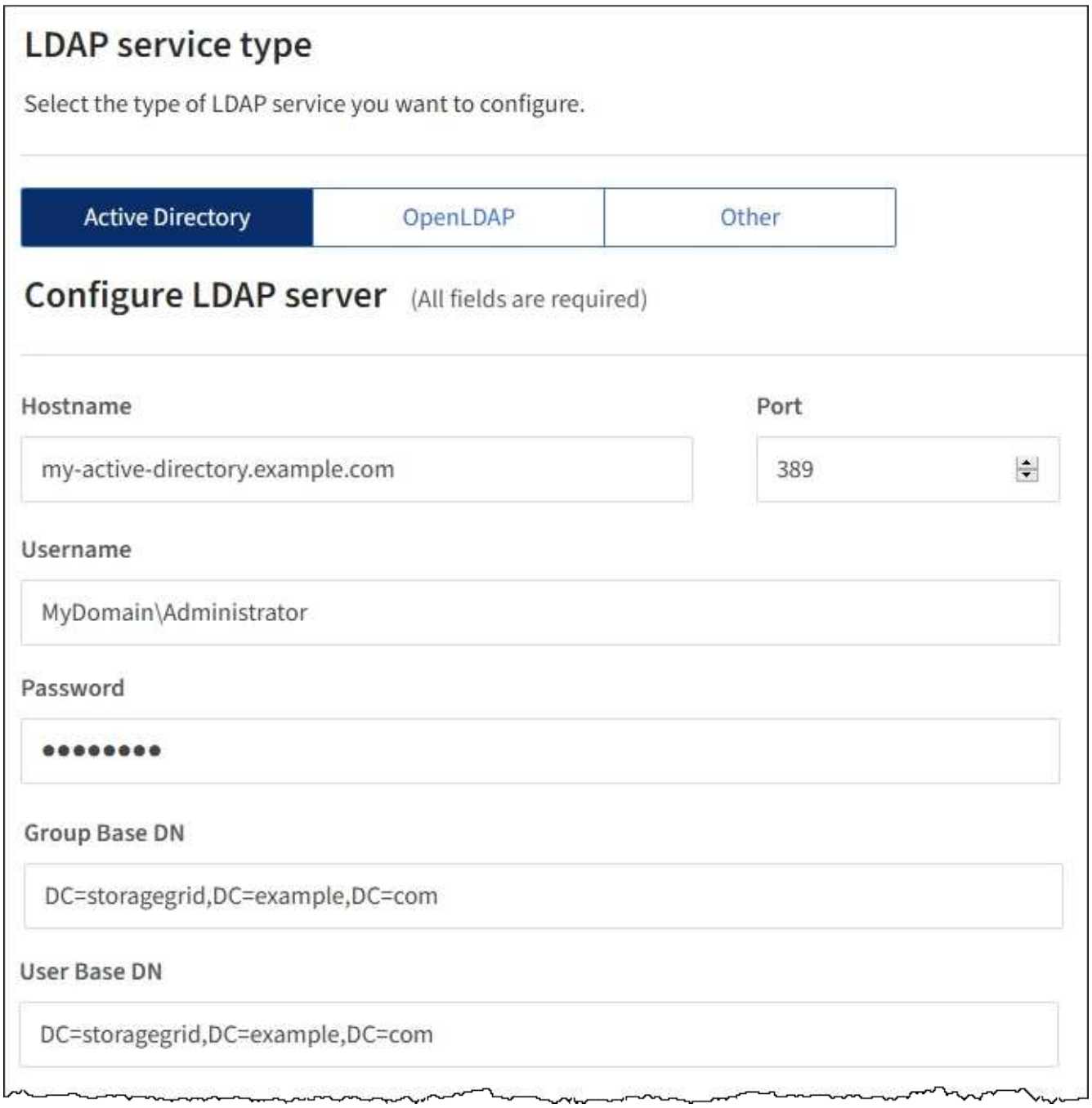
  Si vous sélectionnez ce paramètre, copiez et collez le certificat de sécurité personnalisé dans la zone de texte certificat de l'autorité de certification.

8. Sélectionnez **Tester la connexion** pour valider vos paramètres de connexion pour le serveur LDAP.

   Un message de confirmation s'affiche dans le coin supérieur droit de la page si la connexion est valide.

9. Si la connexion est valide, sélectionnez **Enregistrer**.

   La capture d'écran suivante montre des exemples de valeurs de configuration pour un serveur LDAP qui utilise Active Directory.



Informations associées

"Autorisations de gestion des locataires"

"Instructions de configuration d'un serveur OpenLDAP"

Instructions de configuration d'un serveur OpenLDAP

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

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 de l'adhésion inverse au groupe dans le Guide de l'administrateur pour OpenLDAP.

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'adhésion au groupe inverse dans le Guide de l'administrateur pour OpenLDAP.

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.

Ce dont vous avez besoin

- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.
- Le référentiel d'identité enregistré doit être activé.

Étapes

1. Sélectionnez **ACCESS MANAGEMENT** > **identity federation**.

   La page fédération des identités s'affiche. Le bouton **Sync Server** se trouve en haut à droite de la page.

   Si le référentiel d'identité enregistré n'est pas activé, le bouton **Sync Server** n'est pas actif.

2. Sélectionnez **serveur de synchronisation**.

   Un message de confirmation s'affiche pour indiquer que la synchronisation a démarré correctement.

Informations associées

"Autorisations de gestion des locataires"

Désactivation de la fédération des identités

Si vous avez configuré un service de fédération des identités pour ce locataire, vous pouvez désactiver temporairement ou définitivement la fédération des identités pour les groupes de locataires et les utilisateurs. Lorsque la fédération des identités est désactivée, il n'y a aucune communication entre le système 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.

Ce dont vous avez besoin

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

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 conserveront l'accès au compte du locataire 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.

Étapes

1. Sélectionnez **ACCESS MANAGEMENT** > **identity federation**.
2. Décochez la case **Activer la fédération d'identités**.
3. Sélectionnez **Enregistrer**.

Informations associées

"Autorisations de gestion des locataires"

Gestion des groupes

Vous attribuez des autorisations aux groupes d'utilisateurs pour contrôler les tâches que les utilisateurs peuvent effectuer. Vous pouvez importer des groupes fédérés à partir d'un référentiel d'identité, tel qu'Active Directory ou OpenLDAP, ou créer des groupes locaux.

> Si l'authentification unique est activée pour votre système StorageGRID, les utilisateurs locaux ne pourront pas se connecter au gestionnaire de locataires, même s'ils peuvent accéder aux ressources S3 et Swift, en fonction des autorisations de groupe.

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. L'application des modifications peut prendre jusqu'à 15 minutes à cause de la mise en cache.

Autorisations	Description
Accès racine	Donne un accès complet au gestionnaire des locataires et à l'API de gestion des locataires. **Remarque :** les utilisateurs de Swift doivent disposer de l'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 **Remarque :** les utilisateurs de Swift doivent disposer de l'autorisation Administrateur Swift pour effectuer toutes les opérations avec l'API REST Swift.
Gérez vos propres identifiants S3	Locataires S3 uniquement. 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
Gérer toutes les rubriques	• 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, indépendamment des règles du compartiment S3 ou du groupe. Les utilisateurs qui ne disposent pas de cette autorisation ne voient pas l'option de menu **seaux**. • Locataires Swift : permet aux utilisateurs Swift de contrôler le niveau de cohérence des conteneurs Swift à l'aide de l'API de gestion des locataires. **Remarque :** vous pouvez uniquement attribuer l'autorisation gérer toutes les rubriques aux groupes Swift à partir de l'API de gestion des locataires. Vous ne pouvez pas attribuer cette autorisation aux groupes Swift à l'aide du Gestionnaire de locataires.
Gérer les terminaux	Locataires S3 uniquement. Permet aux utilisateurs d'utiliser le Gestionnaire de locataires ou l'API de gestion des locataires pour créer ou modifier des terminaux, 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**.

Informations associées

"Utilisation de S3"

"Utiliser Swift"

Création de 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.

Ce dont vous avez besoin

- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur pris en charge.
- Vous devez appartenir à un groupe d'utilisateurs qui dispose de l'autorisation accès racine.
- Si vous envisagez d'importer un groupe fédéré, vous avez configuré la fédération des identités et le groupe fédéré existe déjà dans le référentiel d'identité configuré.

Étapes

1. Sélectionnez **ACCESS MANAGEMENT** > **Groups**.

2. Sélectionnez **Créer groupe**.
3. 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.

4. 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 `uid` attribut.
5. Sélectionnez **Continuer**.
6. Sélectionnez un mode d'accès. 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.
   - **Read-write** (valeur 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 effectuer d'opérations dans le Gestionnaire des locataires ou l'API de gestion des locataires. Les utilisateurs locaux en lecture seule peuvent modifier leurs propres mots de passe.
7. Sélectionnez les autorisations de groupe pour ce groupe.

   Reportez-vous aux informations sur les autorisations de gestion des locataires.

8. Sélectionnez **Continuer**.

9. Sélectionnez une stratégie de groupe pour déterminer quelles autorisations d'accès S3 seront attribuées aux membres de ce groupe.
   - **Pas d'accès 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.
   - **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.
   - **Custom** : les utilisateurs du groupe disposent des autorisations que vous spécifiez dans la zone de texte. Pour plus d'informations sur les règles de groupe, notamment la syntaxe du langage et des exemples, reportez-vous aux instructions de mise en œuvre d'une application client S3.
10. 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.

    Dans cet exemple, les membres du groupe sont uniquement autorisés à répertorier et accéder à un dossier correspondant à leur nom d'utilisateur (préfixe de clé) dans le champ 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.

11. Sélectionnez le bouton qui s'affiche, selon que vous créez un groupe fédéré ou local :

- Groupe fédéré : **Créer groupe**
- Groupe local : **Continuer**

Si vous créez un groupe local, STEP 4 (Ajouter des utilisateurs) apparaît après avoir sélectionné **Continuer**. Cette étape n'apparaît pas pour les groupes fédérés.

12. Cochez la case de chaque utilisateur que vous souhaitez ajouter au groupe, puis sélectionnez **Créer groupe**.

    Vous pouvez également enregistrer le groupe sans ajouter d'utilisateurs. Vous pouvez ajouter des utilisateurs au groupe ultérieurement ou sélectionner le groupe lorsque vous ajoutez de nouveaux utilisateurs.

13. Sélectionnez **Terminer**.

    Le groupe que vous avez créé apparaît dans la liste des groupes. L'application des modifications peut prendre jusqu'à 15 minutes à cause de la mise en cache.

Informations associées

"Autorisations de gestion des locataires"

"Utilisation de S3"

Création de 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.

Ce dont vous avez besoin

- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur pris en charge.
- Vous devez appartenir à un groupe d'utilisateurs qui dispose de l'autorisation accès racine.
- Si vous envisagez d'importer un groupe fédéré, vous avez configuré la fédération des identités et le groupe fédéré existe déjà dans le référentiel d'identité configuré.

Étapes

1. Sélectionnez **ACCESS MANAGEMENT** > **Groups**.

2. Sélectionnez **Créer groupe**.
3. 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.

4. 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 `uid` attribut.
5. Sélectionnez **Continuer**.
6. Sélectionnez un mode d'accès. 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.
   - **Read-write** (valeur 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 effectuer d'opérations dans le Gestionnaire des locataires ou l'API de gestion des locataires. Les utilisateurs locaux en lecture seule peuvent modifier leurs propres mots de passe.
7. Définissez l'autorisation Groupe.
   - Cochez la case **accès racine** si les utilisateurs doivent se connecter au Gestionnaire de locataires ou à l'API de gestion des locataires. (Valeur par défaut)
   - Désélectionnez la case **accès racine** si les utilisateurs n'ont pas besoin d'accéder au Gestionnaire de locataires ou à l'API de gestion des locataires. Par exemple, désélectionnez la case à cocher pour les

applications qui n'ont pas besoin d'accéder au locataire. Attribuez ensuite l'autorisation **Swift Administrator** pour permettre à ces utilisateurs de gérer des conteneurs et des objets.

8. Sélectionnez **Continuer**.
9. Cochez la case **Administrateur Swift** si l'utilisateur doit pouvoir utiliser l'API REST Swift.

   Les utilisateurs Swift doivent disposer de l'autorisation d'accès racine pour accéder au gestionnaire de locataires. Toutefois, l'autorisation accès racine ne permet pas aux utilisateurs de s'authentifier auprès de l'API REST Swift pour créer des conteneurs et ingérer des objets. Les utilisateurs doivent disposer de l'autorisation Administrateur Swift pour s'authentifier dans l'API REST de Swift.

10. Sélectionnez le bouton qui s'affiche, selon que vous créez un groupe fédéré ou local :
    - Groupe fédéré : **Créer groupe**
    - Groupe local : **Continuer**

      Si vous créez un groupe local, STEP 4 (Ajouter des utilisateurs) apparaît après avoir sélectionné **Continuer**. Cette étape n'apparaît pas pour les groupes fédérés.

11. Cochez la case de chaque utilisateur que vous souhaitez ajouter au groupe, puis sélectionnez **Créer groupe**.

    Vous pouvez également enregistrer le groupe sans ajouter d'utilisateurs. Vous pouvez ajouter des utilisateurs au groupe ultérieurement ou sélectionner le groupe lorsque vous créez de nouveaux utilisateurs.

12. Sélectionnez **Terminer**.

    Le groupe que vous avez créé apparaît dans la liste des groupes. L'application des modifications peut prendre jusqu'à 15 minutes à cause de la mise en cache.

Informations associées

"Autorisations de gestion des locataires"

"Utiliser Swift"

Affichage et modification des détails du groupe

Lorsque vous affichez les détails d'un groupe, vous pouvez modifier le nom d'affichage, les autorisations, les règles et les utilisateurs appartenant au groupe.

Ce dont vous avez besoin

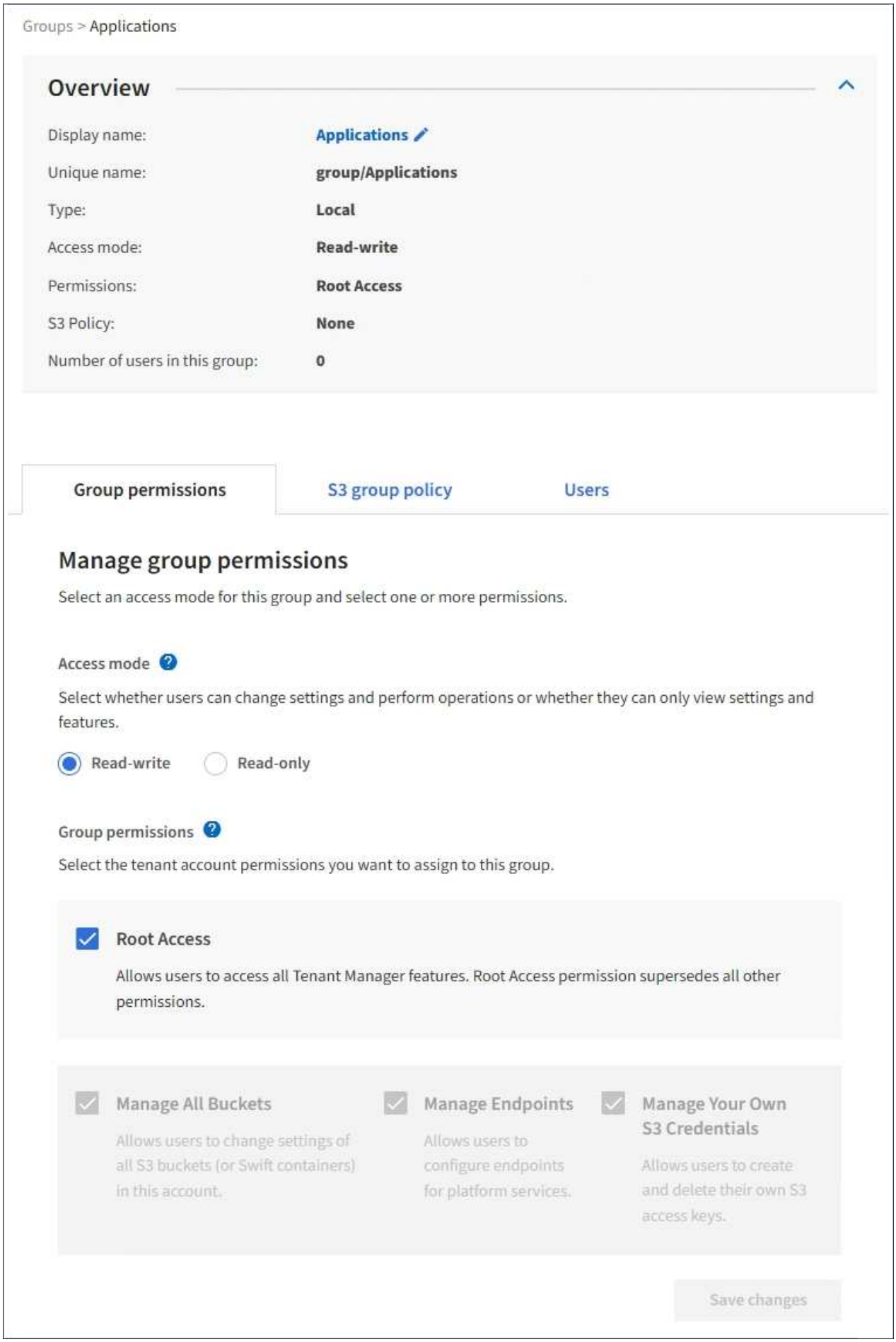
- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur pris en charge.
- Vous devez appartenir à un groupe d'utilisateurs qui dispose de l'autorisation accès racine.

Étapes

1. Sélectionnez **ACCESS MANAGEMENT** > **Groups**.
2. Sélectionnez le nom du groupe dont vous souhaitez afficher ou modifier les détails.

   Vous pouvez également sélectionner **actions** > **Afficher les détails du groupe**.

   La page des détails du groupe s'affiche. L'exemple suivant montre la page des détails du groupe S3.


Groups > Applications
Overview
Display name:
Applications
Unique name:
group/Applications
Type:
Local
Access mode:
Read-write
Permissions:
Root Access
S3 Policy:
None
Number of users in this group:
0
Group permissions
S3 group policy
Users
Manage group permissions
Select an access mode for this group and select one or more permissions.
Access mode
Select whether users can change settings and perform operations or whether they can only view settings and features.
Read-write
Read-only
Group permissions
Select the tenant account permissions you want to assign to this group.
Root Access
Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.
Manage All Buckets
Allows users to change settings of all S3 buckets (or Swift containers) in this account.
Manage Endpoints
Allows users to configure endpoints for platform services.
Manage Your Own S3 Credentials
Allows users to create and delete their own S3 access keys.
Save changes

3. Modifiez les paramètres du groupe selon vos besoins.

> Pour vous assurer que vos modifications sont enregistrées, sélectionnez **Enregistrer les modifications** après avoir effectué des modifications dans chaque section. Lorsque vos modifications sont enregistrées, un message de confirmation s'affiche dans le coin supérieur droit de la page.

   a. Vous pouvez également sélectionner le nom d'affichage ou l'icône de modification pour mettre à jour le nom d'affichage.

      Vous ne pouvez pas modifier le nom unique d'un groupe. Vous ne pouvez pas modifier le nom d'affichage d'un groupe fédéré.

   b. Si vous le souhaitez, mettez à jour les autorisations.

   c. Pour les règles de groupe, apportez les modifications appropriées à votre locataire S3 ou Swift.

      - Si vous modifiez un groupe pour un locataire S3, vous pouvez choisir une autre règle de groupe S3. Si vous sélectionnez une règle S3 personnalisée, mettez à jour la chaîne JSON si nécessaire.
      - Si vous modifiez un groupe pour un locataire Swift, vous pouvez sélectionner ou désélectionner la case à cocher **Administrateur Swift**.

        Pour plus d'informations sur l'autorisation de l'administrateur Swift, reportez-vous aux instructions de création de groupes pour un locataire Swift.

   d. Si vous le souhaitez, vous pouvez ajouter ou supprimer des utilisateurs.

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

   L'application des modifications peut prendre jusqu'à 15 minutes à cause de la mise en cache.

Informations associées

"Création de groupes pour un locataire S3"

"Création de groupes pour un locataire Swift"

Ajout d'utilisateurs à un groupe local

Vous pouvez ajouter des utilisateurs à un groupe local si nécessaire.

Ce dont vous avez besoin

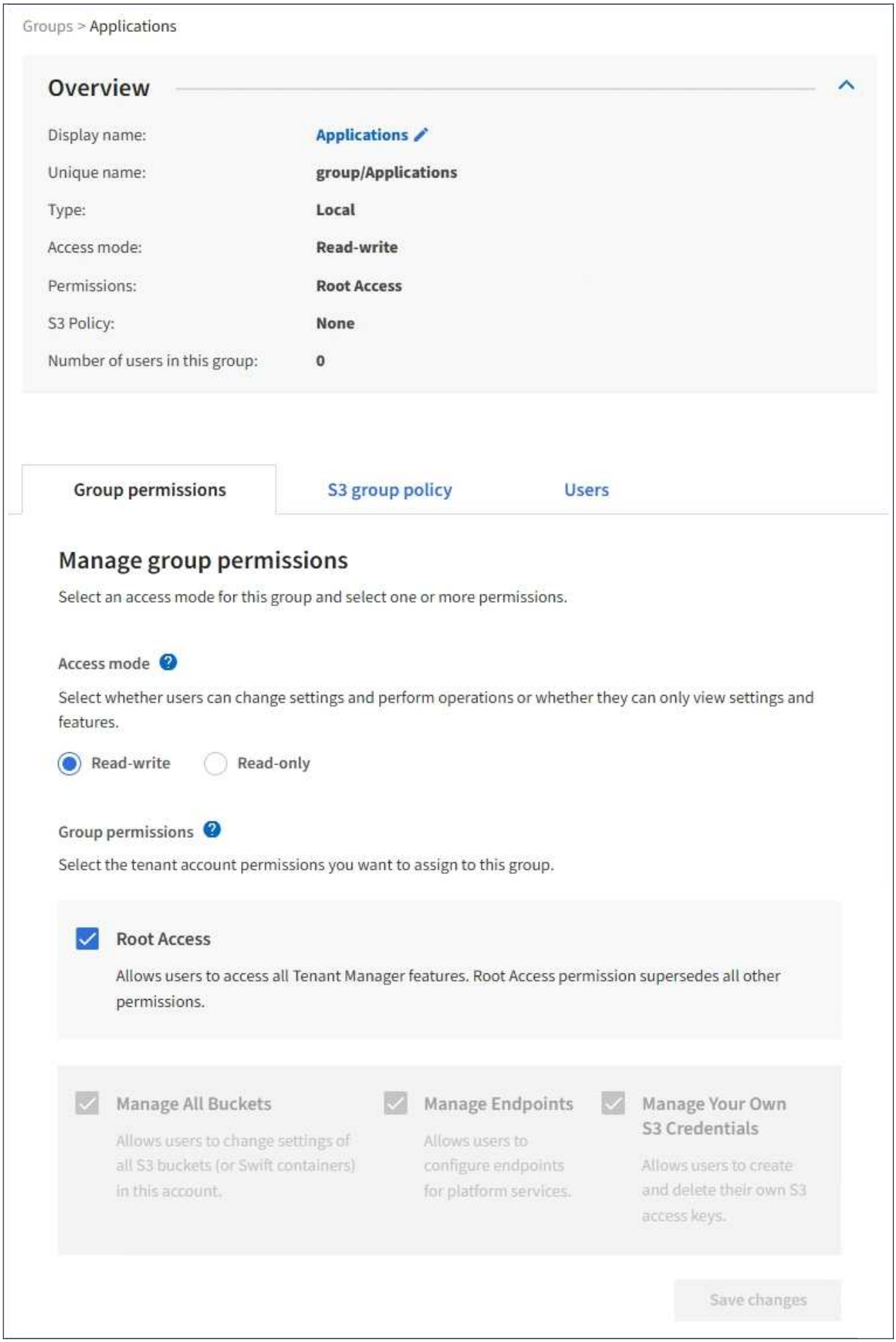
- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur pris en charge.
- Vous devez appartenir à un groupe d'utilisateurs qui dispose de l'autorisation accès racine.

Étapes

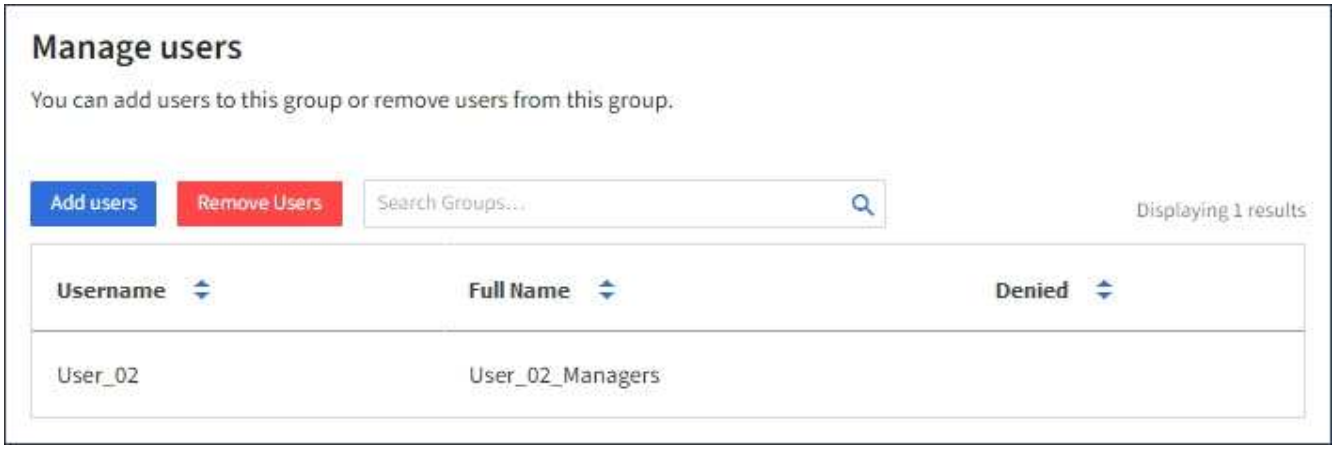
1. Sélectionnez **ACCESS MANAGEMENT** > **Groups**.
2. Sélectionnez le nom du groupe local auquel vous souhaitez ajouter des utilisateurs.

   Vous pouvez également sélectionner **actions** > **Afficher les détails du groupe**.

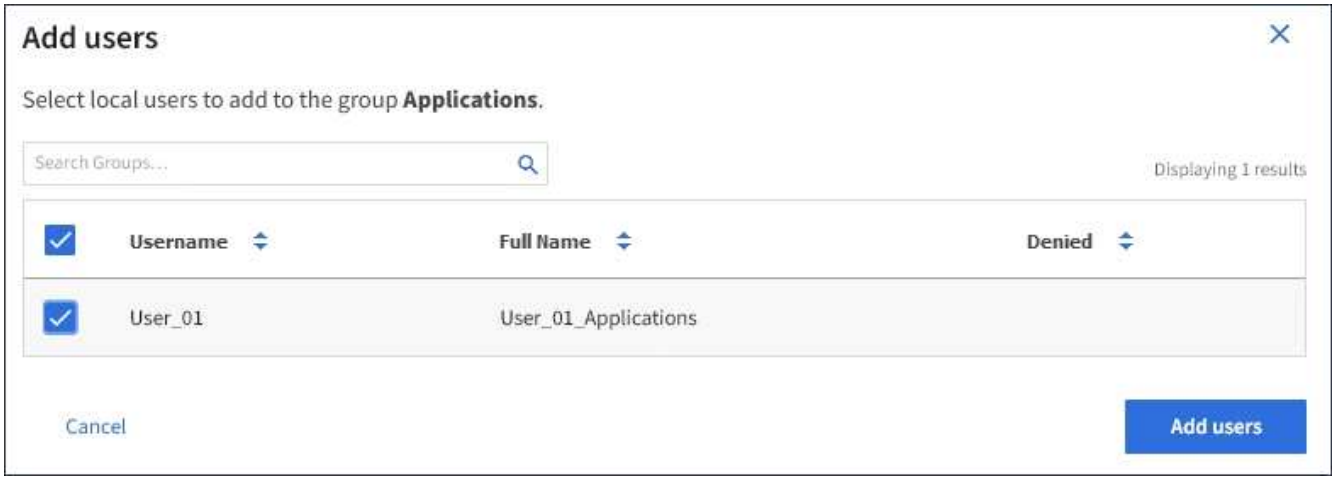
   La page des détails du groupe s'affiche.


Groups > Applications
Overview
Display name:
Applications
Unique name:
group/Applications
Type:
Local
Access mode:
Read-write
Permissions:
Root Access
S3 Policy:
None
Number of users in this group:
0
Group permissions
S3 group policy
Users
Manage group permissions
Select an access mode for this group and select one or more permissions.
Access mode
Select whether users can change settings and perform operations or whether they can only view settings and features.
Read-write
Read-only
Group permissions
Select the tenant account permissions you want to assign to this group.
Root Access
Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.
Manage All Buckets
Allows users to change settings of all S3 buckets (or Swift containers) in this account.
Manage Endpoints
Allows users to configure endpoints for platform services.
Manage Your Own S3 Credentials
Allows users to create and delete their own S3 access keys.
Save changes

3. Sélectionnez **gérer les utilisateurs**, puis **Ajouter des utilisateurs**.



4. Sélectionnez les utilisateurs que vous souhaitez ajouter au groupe, puis sélectionnez **Ajouter utilisateurs**.



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

Modification d'un nom de groupe

Vous pouvez modifier le nom d'affichage d'un groupe. Vous ne pouvez pas modifier le nom unique d'un groupe.

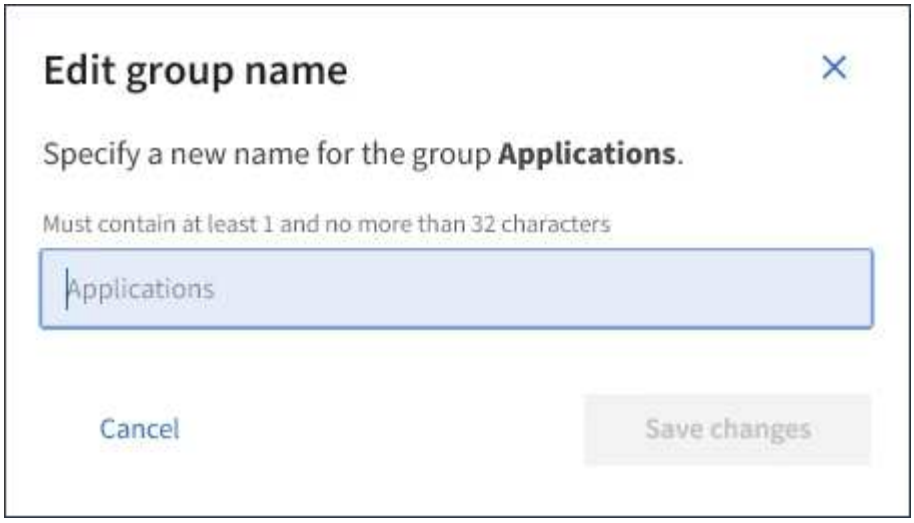
Ce dont vous avez besoin

- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur pris en charge.
- Vous devez appartenir à un groupe d'utilisateurs qui dispose de l'autorisation accès racine.

Étapes

1. Sélectionnez **ACCESS MANAGEMENT** > **Groups**.
2. Cochez la case du groupe dont vous souhaitez modifier le nom d'affichage.
3. Sélectionnez **actions** > **Modifier le nom du groupe**.

   La boîte de dialogue Modifier le nom du groupe s'affiche.



4. Si vous modifiez un groupe local, mettez à jour le nom d'affichage selon vos besoins.

   Vous ne pouvez pas modifier le nom unique d'un groupe. Vous ne pouvez pas modifier le nom d'affichage d'un groupe fédéré.

5. Sélectionnez **Enregistrer les modifications**.

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

Informations associées

"Autorisations de gestion des locataires"

Duplication d'un groupe

Vous pouvez créer de nouveaux groupes plus rapidement en dupliquant un groupe existant.

Ce dont vous avez besoin

- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur pris en charge.
- Vous devez appartenir à un groupe d'utilisateurs qui dispose de l'autorisation accès racine.

Étapes

1. Sélectionnez **ACCESS MANAGEMENT** > **Groups**.
2. Cochez la case correspondant au groupe que vous souhaitez dupliquer.
3. Sélectionnez **Dupliquer le groupe**. Pour plus d'informations sur la création d'un groupe, consultez les instructions de création de groupes pour un locataire S3 ou pour un locataire Swift.
4. 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.

5. 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 `uid` attribut.
6. Sélectionnez **Continuer**.
7. Si nécessaire, modifiez les autorisations pour ce groupe.
8. Sélectionnez **Continuer**.
9. Si nécessaire, si vous copiez un groupe pour un locataire S3, vous pouvez sélectionner une autre stratégie à partir des boutons d'option **Ajouter une stratégie S3**. Si vous avez sélectionné une règle personnalisée, mettez à jour la chaîne JSON si nécessaire.
10. Sélectionnez **Créer groupe**.

Informations associées

"Création de groupes pour un locataire S3"

"Création de groupes pour un locataire Swift"

"Autorisations de gestion des locataires"

Suppression d'un groupe

Vous pouvez supprimer un groupe du système. Les utilisateurs appartenant uniquement à ce groupe ne pourront plus se connecter au Gestionnaire de locataires ni utiliser le compte de tenant.

Ce dont vous avez besoin

- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur pris en charge.
- Vous devez appartenir à un groupe d'utilisateurs qui dispose de l'autorisation accès racine.

Étapes

1. Sélectionnez **ACCESS MANAGEMENT** > **Groups**.

2. Cochez les cases des groupes que vous souhaitez supprimer.
3. Sélectionnez **actions** > **Supprimer le groupe**.

   Un message de confirmation s'affiche.

4. Sélectionnez **Supprimer le groupe** pour confirmer la suppression des groupes indiqués dans le message de confirmation.

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

Informations associées

"Autorisations de gestion des locataires"

Gestion des 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.

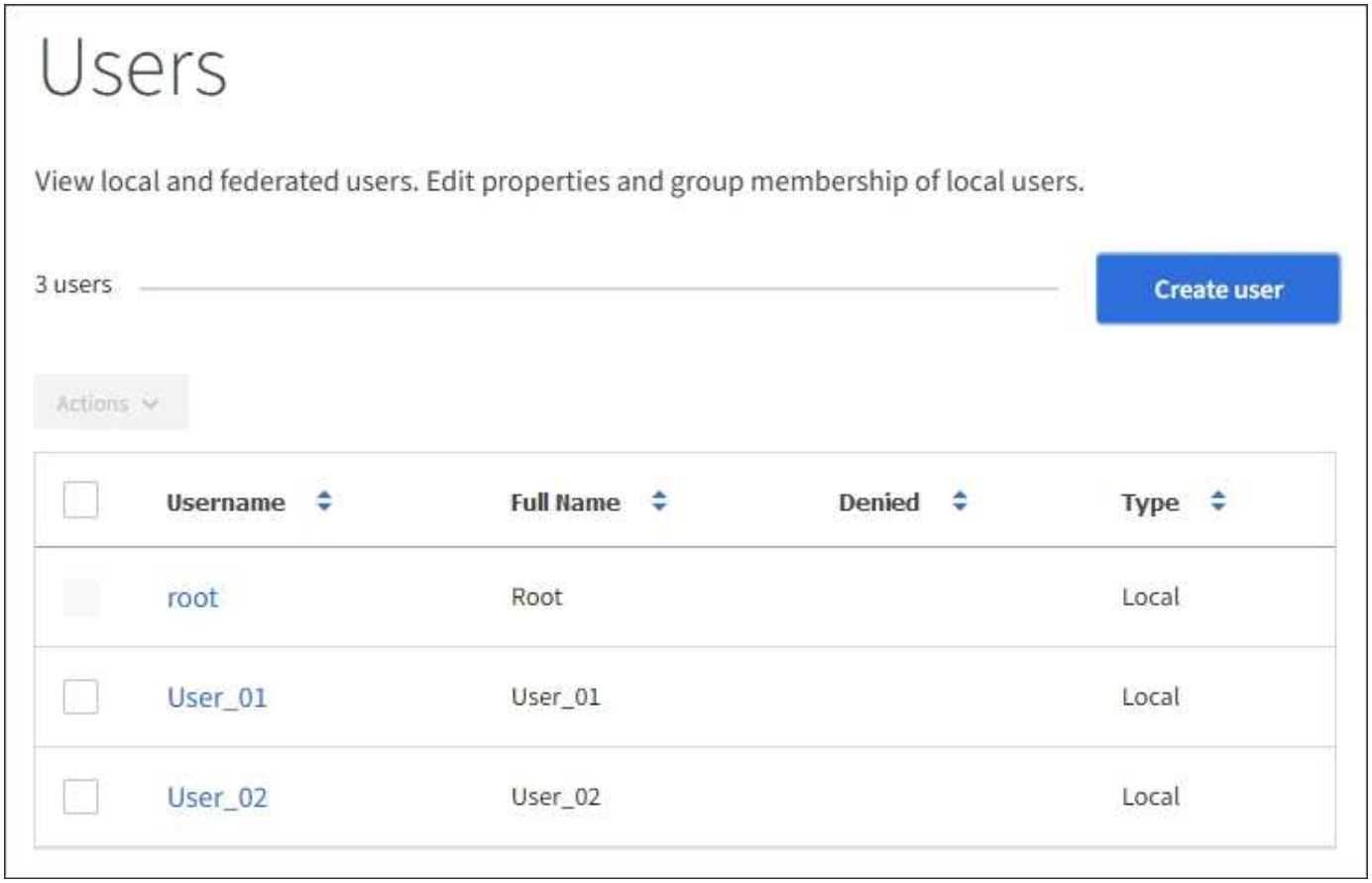
Ce dont vous avez besoin

- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur pris en charge.
- Vous devez appartenir à un groupe d'utilisateurs en lecture/écriture doté de l'autorisation accès racine.

> Si l'authentification unique 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, même s'ils peuvent utiliser les applications client S3 ou Swift pour accéder aux ressources du locataire en fonction des autorisations de groupe.

Accès à la page utilisateurs

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



Création d'utilisateurs locaux

Vous pouvez créer des utilisateurs locaux et les attribuer à un ou plusieurs groupes locaux pour contrôler leurs autorisations d'accès.

Les utilisateurs S3 qui n'appartiennent à aucun groupe ne disposent 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 n'appartenant à aucun groupe ne disposent d'autorisations de gestion ni d'un accès au conteneur Swift.

Étapes

1. Sélectionnez **Créer utilisateur**.
2. Renseignez les champs suivants.
   - **Nom complet** : le nom complet de cet utilisateur, par exemple le prénom et le nom de famille 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.
   - **Mot de passe** : mot de passe utilisé lorsque l'utilisateur ouvre une session.
   - **Confirmer le mot de passe** : saisissez le même mot de passe que celui que vous avez saisi dans le champ Mot de passe.

- **Refuser l'accès**: Si vous sélectionnez **Oui**, cet utilisateur ne peut pas se connecter au compte de tenant, même si l'utilisateur peut toujours appartenir à un ou plusieurs groupes.

  Par exemple, vous pouvez utiliser cette fonction pour suspendre temporairement la connexion d'un utilisateur.

3. Sélectionnez **Continuer**.
4. Attribuez l'utilisateur à un ou plusieurs groupes locaux.

   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.

5. Sélectionnez **Créer utilisateur**.

   L'application des modifications peut prendre jusqu'à 15 minutes à cause de la mise en cache.

Modification des détails de l'utilisateur

Lorsque vous modifiez les détails d'un utilisateur, vous pouvez modifier le nom complet et le mot de passe de l'utilisateur, ajouter l'utilisateur à différents groupes et empêcher l'utilisateur d'accéder au locataire.

Étapes

1. Dans la liste utilisateurs, sélectionnez le nom de l'utilisateur dont vous souhaitez afficher ou modifier les détails.

   Vous pouvez également cocher la case de l'utilisateur, puis sélectionner **actions** > **Afficher les détails de l'utilisateur**.

2. Apportez les modifications nécessaires aux paramètres utilisateur.
   a. Modifiez le nom complet de l'utilisateur selon vos besoins en sélectionnant le nom complet ou l'icône de modification Dans la section vue d'ensemble.

      Vous ne pouvez pas modifier le nom d'utilisateur.

   b. Dans l'onglet **Mot de passe**, modifiez le mot de passe de l'utilisateur si nécessaire.
   c. Dans l'onglet **Access**, permettez à l'utilisateur de se connecter (sélectionnez **non**) ou d'empêcher l'utilisateur de se connecter (sélectionnez **Oui**) selon les besoins.
   d. Dans l'onglet **groupes**, ajoutez l'utilisateur aux groupes ou supprimez l'utilisateur des groupes si nécessaire.
   e. Si nécessaire pour chaque section, sélectionnez **Enregistrer les modifications**.

      L'application des modifications peut prendre jusqu'à 15 minutes à cause de la mise en cache.

Duplication des utilisateurs locaux

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

Étapes

1. Dans la liste utilisateurs, sélectionnez l'utilisateur que vous souhaitez dupliquer.
2. Sélectionnez **Dupliquer l'utilisateur**.

3. Modifiez les champs suivants pour le nouvel utilisateur.
   - **Nom complet** : le nom complet de cet utilisateur, par exemple le prénom et le nom de famille 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.
   - **Mot de passe** : mot de passe utilisé lorsque l'utilisateur ouvre une session.
   - **Confirmer le mot de passe** : saisissez le même mot de passe que celui que vous avez saisi dans le champ Mot de passe.
   - **Refuser l'accès**: Si vous sélectionnez **Oui**, cet utilisateur ne peut pas se connecter au compte de tenant, même si l'utilisateur peut toujours appartenir à un ou plusieurs groupes.

     Par exemple, vous pouvez utiliser cette fonction pour suspendre temporairement la connexion d'un utilisateur.
4. Sélectionnez **Continuer**.
5. Sélectionnez un ou plusieurs groupes locaux.

   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.
6. Sélectionnez **Créer utilisateur**.

   L'application des modifications peut prendre jusqu'à 15 minutes à cause de la mise en cache.

Suppression d'utilisateurs locaux

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

À l'aide du Gestionnaire de locataires, vous pouvez supprimer des utilisateurs locaux, mais pas des utilisateurs fédérés. Vous devez utiliser le référentiel d'identité fédéré pour supprimer des utilisateurs fédérés.

Étapes

1. Dans la liste utilisateurs, cochez la case de l'utilisateur local que vous souhaitez supprimer.
2. Sélectionnez **actions** > **Supprimer l'utilisateur**.
3. Dans la boîte de dialogue de confirmation, sélectionnez **Supprimer l'utilisateur** pour confirmer que vous souhaitez supprimer l'utilisateur du système.

   L'application des modifications peut prendre jusqu'à 15 minutes à cause de la mise en cache.

Informations associées

"Autorisations de gestion des locataires"

Gestion des comptes de locataires S3

Vous pouvez utiliser le Gestionnaire des locataires pour gérer les clés d'accès S3 et créer et gérer des compartiments S3.

- "Gestion des clés d'accès S3"
- "Gestion des compartiments S3"

Gestion des clés d'accès S3

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

Description de la tâche

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

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

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

Création de vos propres clés d'accès S3

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

Ce dont vous avez besoin

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

Description de la tâche

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

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

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

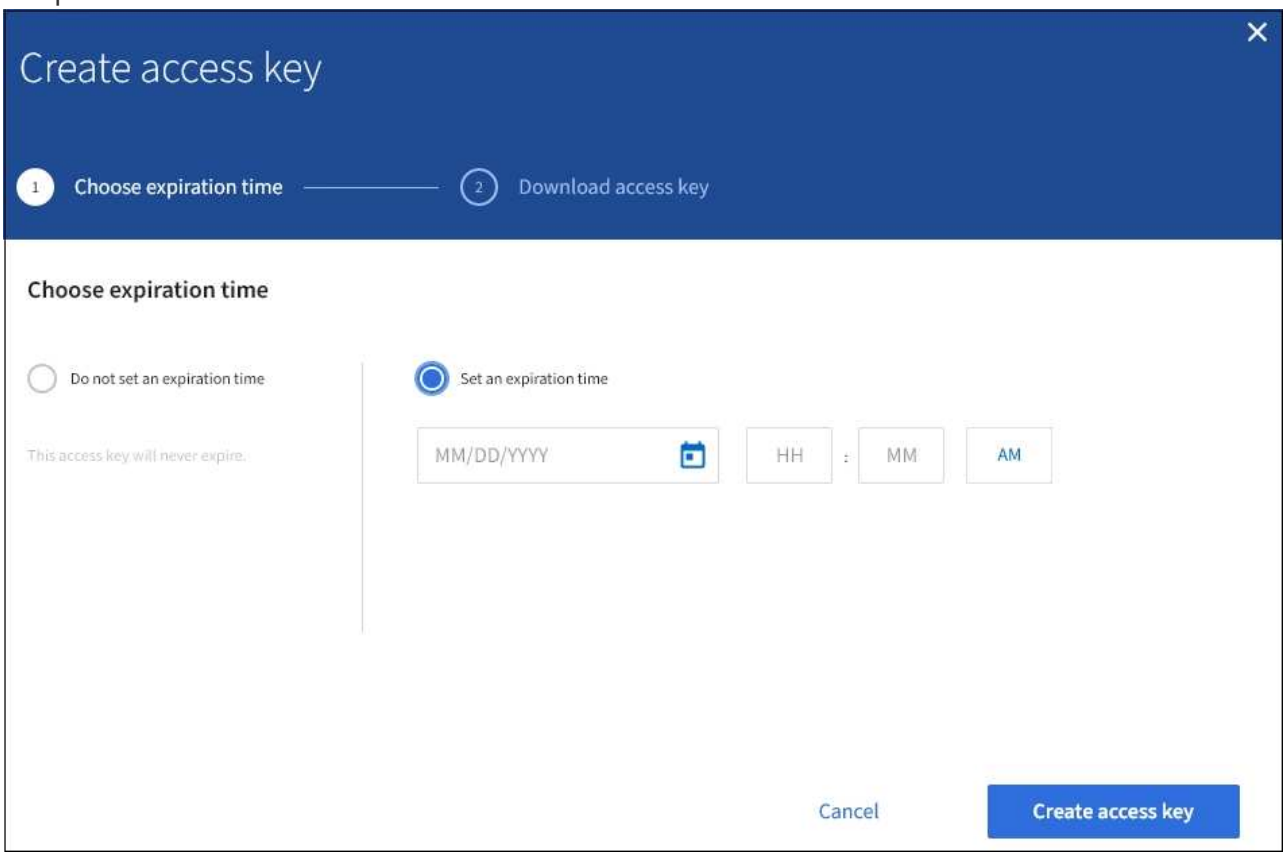
Vous pouvez accéder aux compartiments S3 et aux objets appartenant à votre compte à l'aide de l'ID de clé d'accès et de la clé secrète affichée pour votre compte dans le Gestionnaire des locataires. Pour cette raison, protégez les clés d'accès comme vous le feriez avec un mot de passe. Faites pivoter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

Étapes

1. Sélectionnez **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.

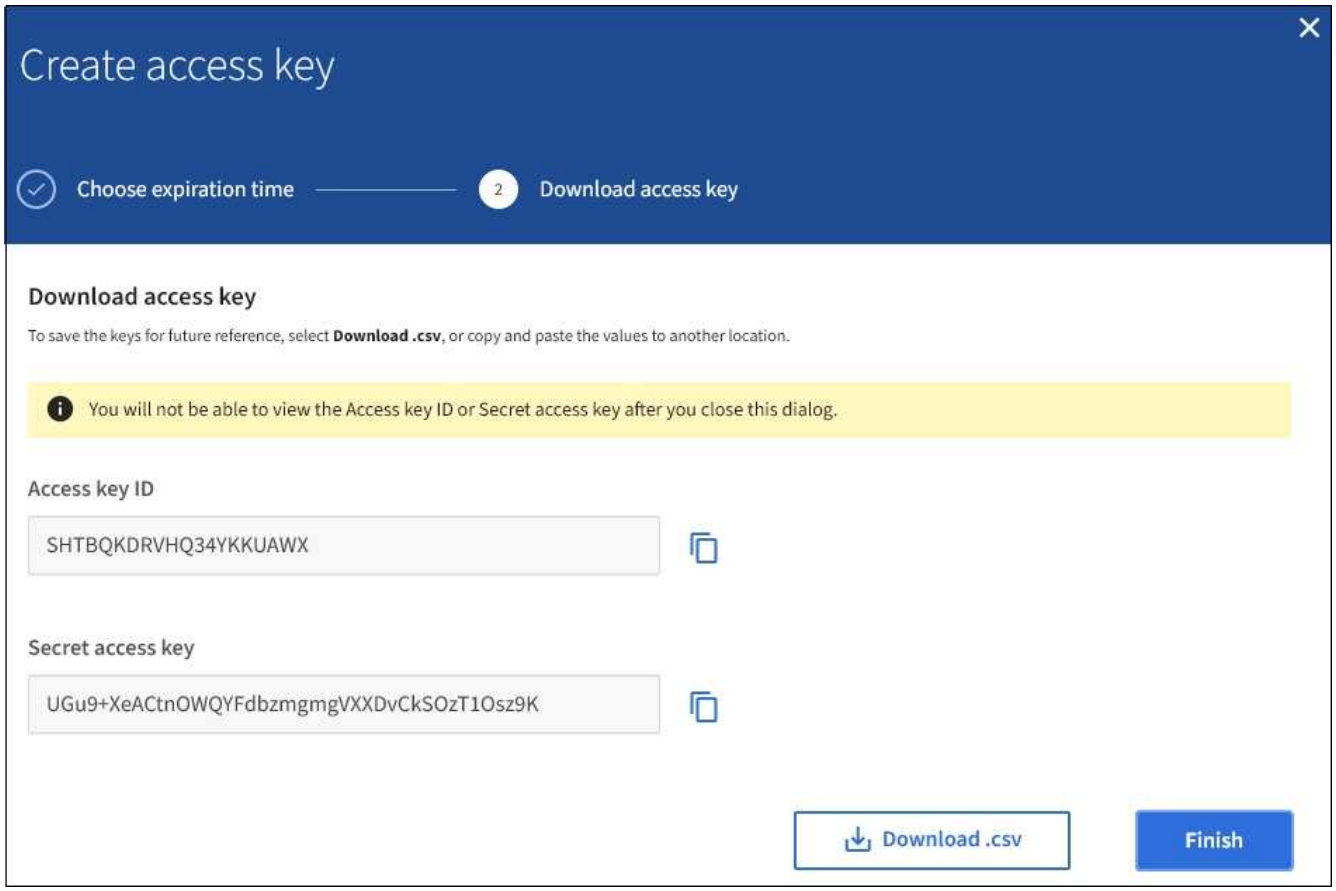


4. Sélectionnez **Créer une clé d'accès**.

   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.



6. Sélectionnez **Terminer**.

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

Informations associées

"Autorisations de gestion des locataires"

Affichage des clés d'accès S3

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

Ce dont vous avez besoin

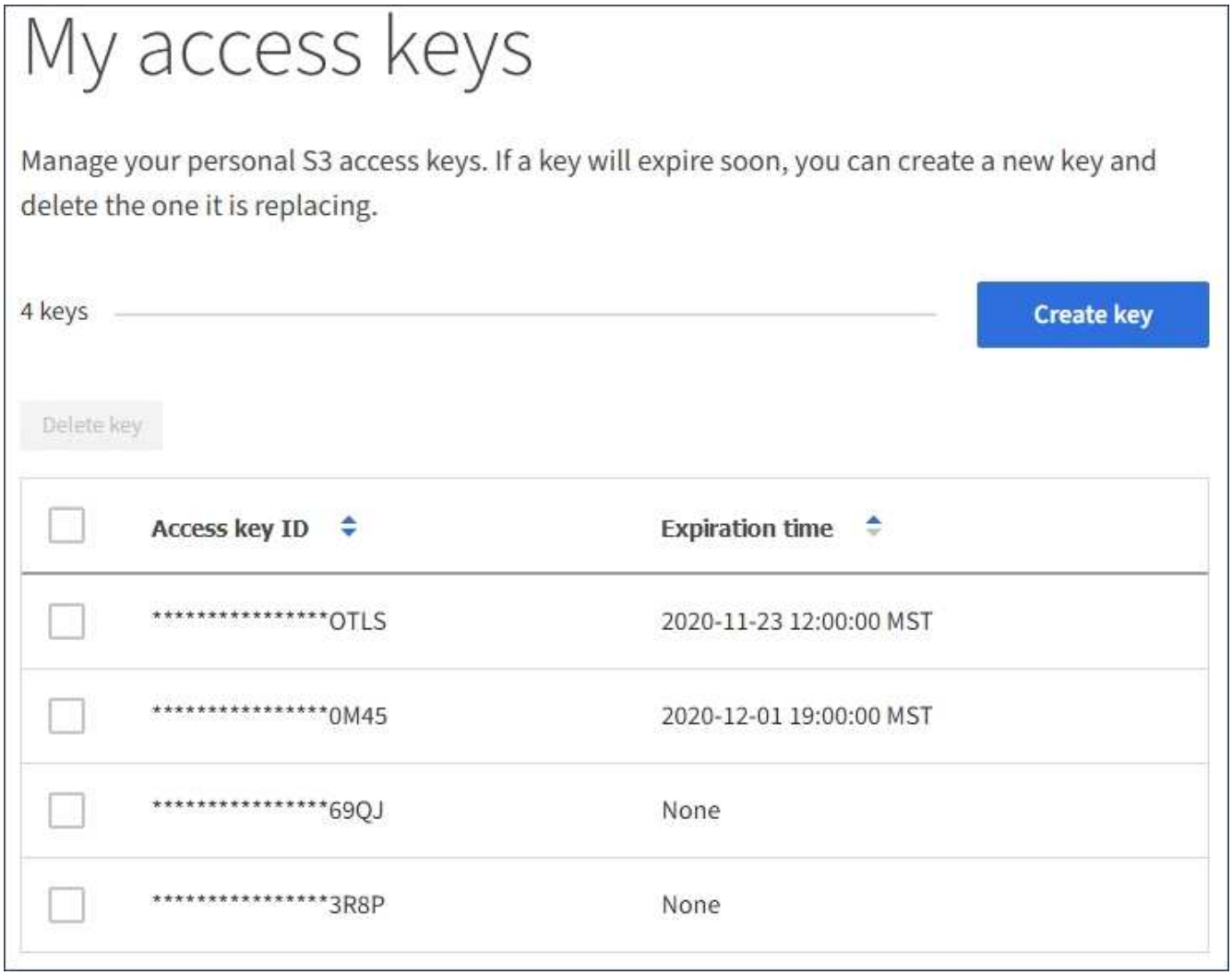
- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur pris en charge.
- Vous devez disposer de l'autorisation gérer vos propres informations d'identification S3.

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

Étapes

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

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



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

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

   Les clés expirées sont supprimées automatiquement.

Informations associées

"Création de vos propres clés d'accès S3"

"Suppression de vos propres clés d'accès S3"

Suppression de vos propres clés d'accès S3

Si vous utilisez un locataire S3 et que vous disposez des autorisations appropriées, vous pouvez supprimer vos propres clés d'accès S3. Une fois la clé d'accès supprimée, elle ne

peut plus être utilisée pour accéder aux objets et aux compartiments du compte du locataire.

Ce dont vous avez besoin

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

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

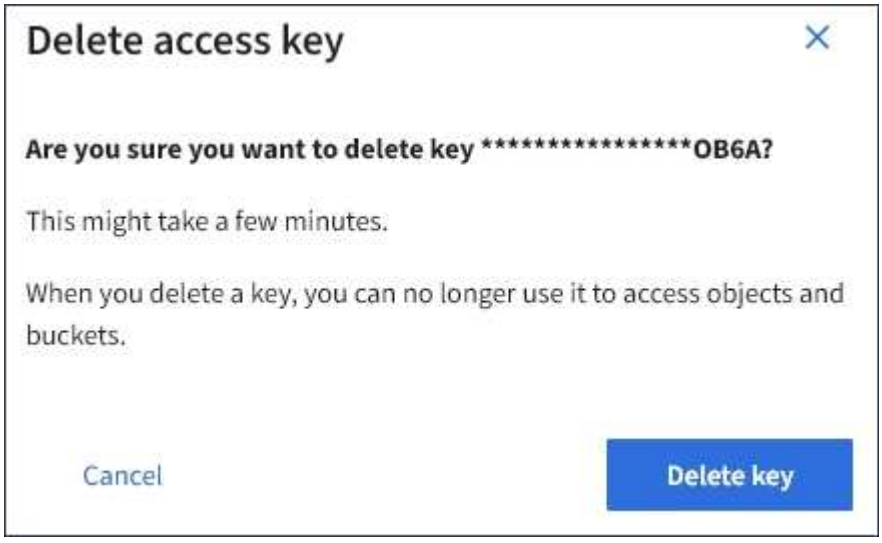
Étapes

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

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

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

   Une boîte de dialogue de confirmation s'affiche.



4. Sélectionnez **Supprimer la touche**.

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

Informations associées

"Autorisations de gestion des locataires"

Création des clés d'accès S3 d'un autre utilisateur

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

des compartiments et des objets.

Ce dont vous avez besoin

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

Description de la tâche

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

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

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

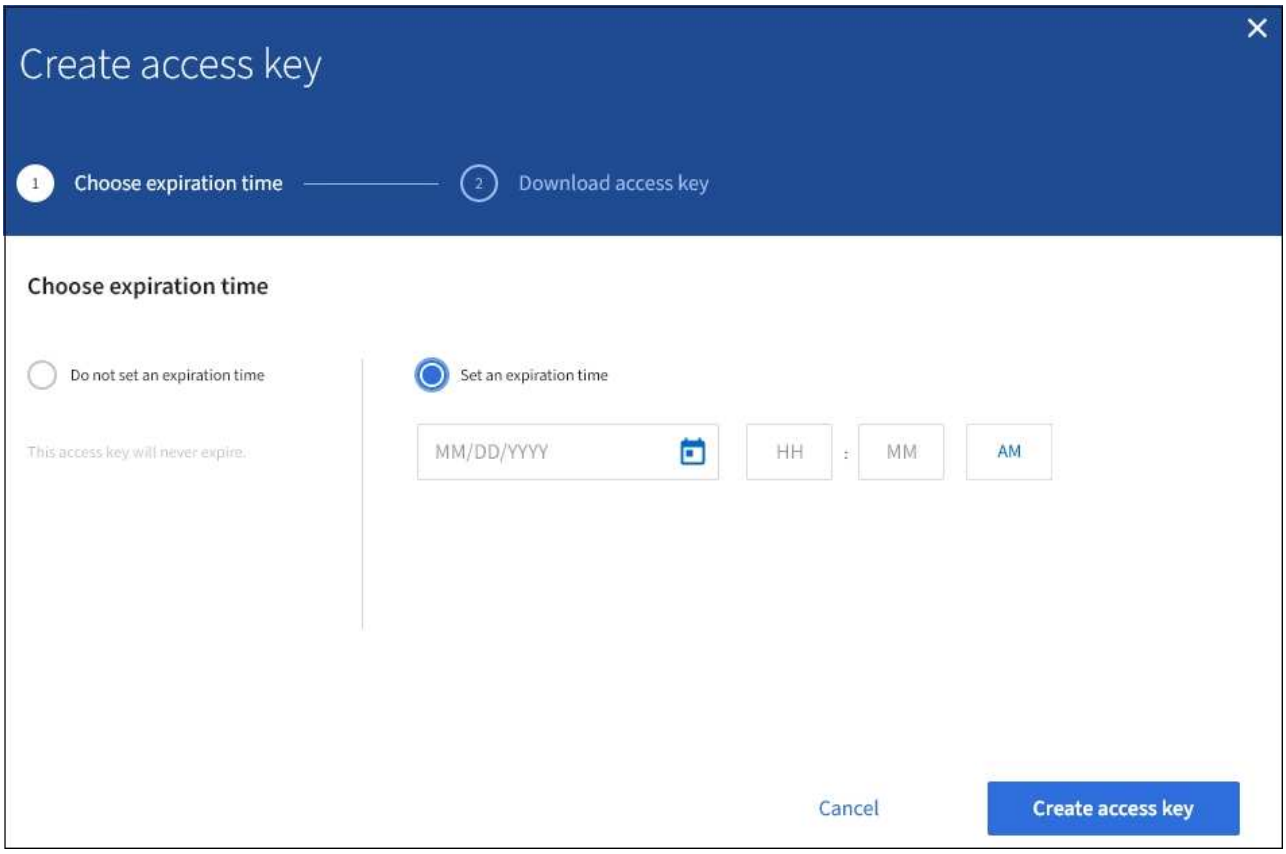
> Les compartiments S3 et les objets appartenant à un utilisateur sont accessibles à l'aide de l'ID de clé d'accès et de la clé secrète affichée pour cet utilisateur dans le Gestionnaire de locataires. Pour cette raison, protégez les clés d'accès comme vous le feriez avec un mot de passe. Faites pivoter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

Étapes

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

   La page de détails utilisateur s'affiche.

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

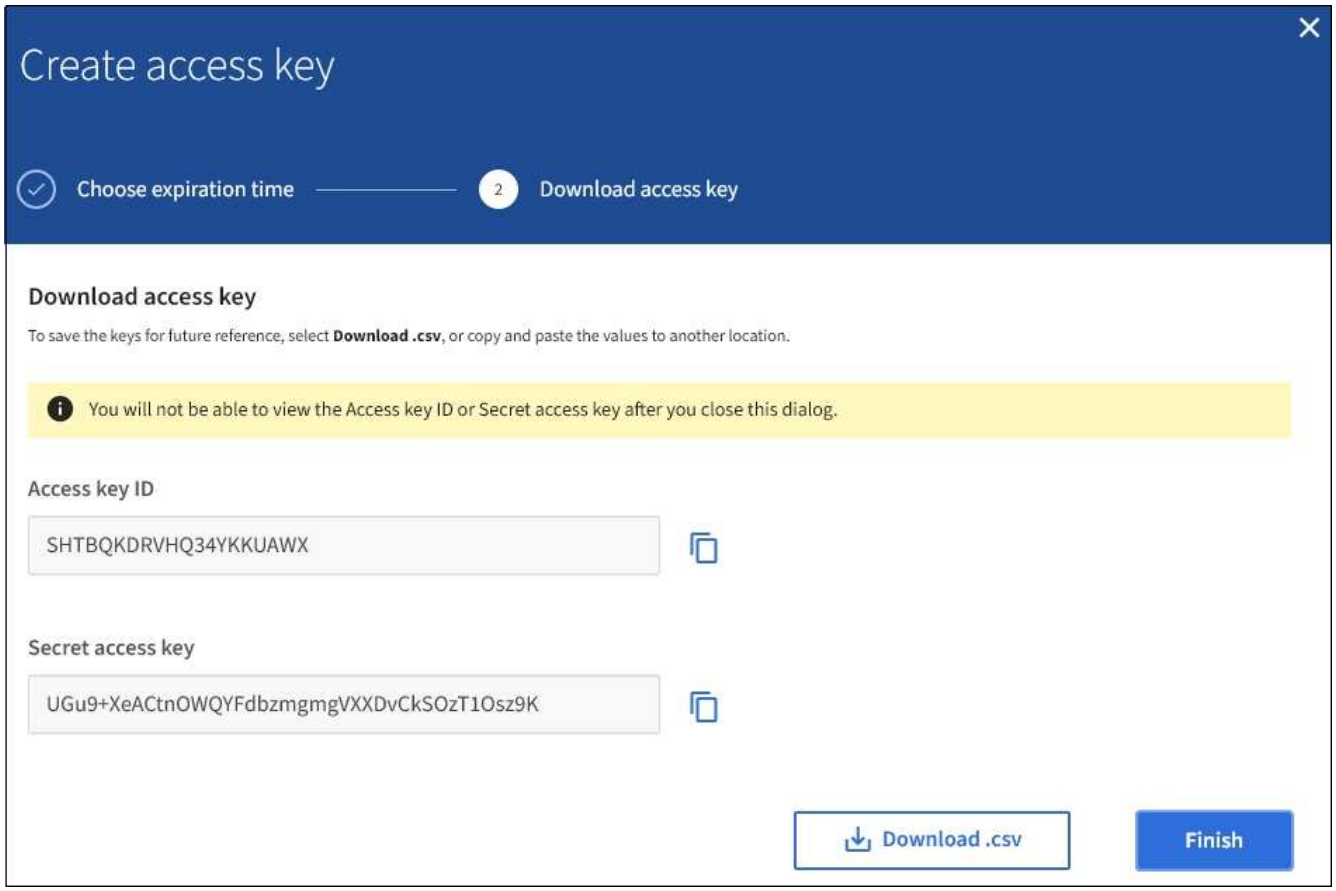


5. Sélectionnez **Créer une clé d'accès**.

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

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

   Ne fermez pas cette boîte de dialogue tant que vous n'avez pas copié ou téléchargé ces informations.



7. Sélectionnez **Terminer**.

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

Informations associées

"Autorisations de gestion des locataires"

Affichage des clés d'accès S3 d'un autre utilisateur

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

Ce dont vous avez besoin

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

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

Étapes

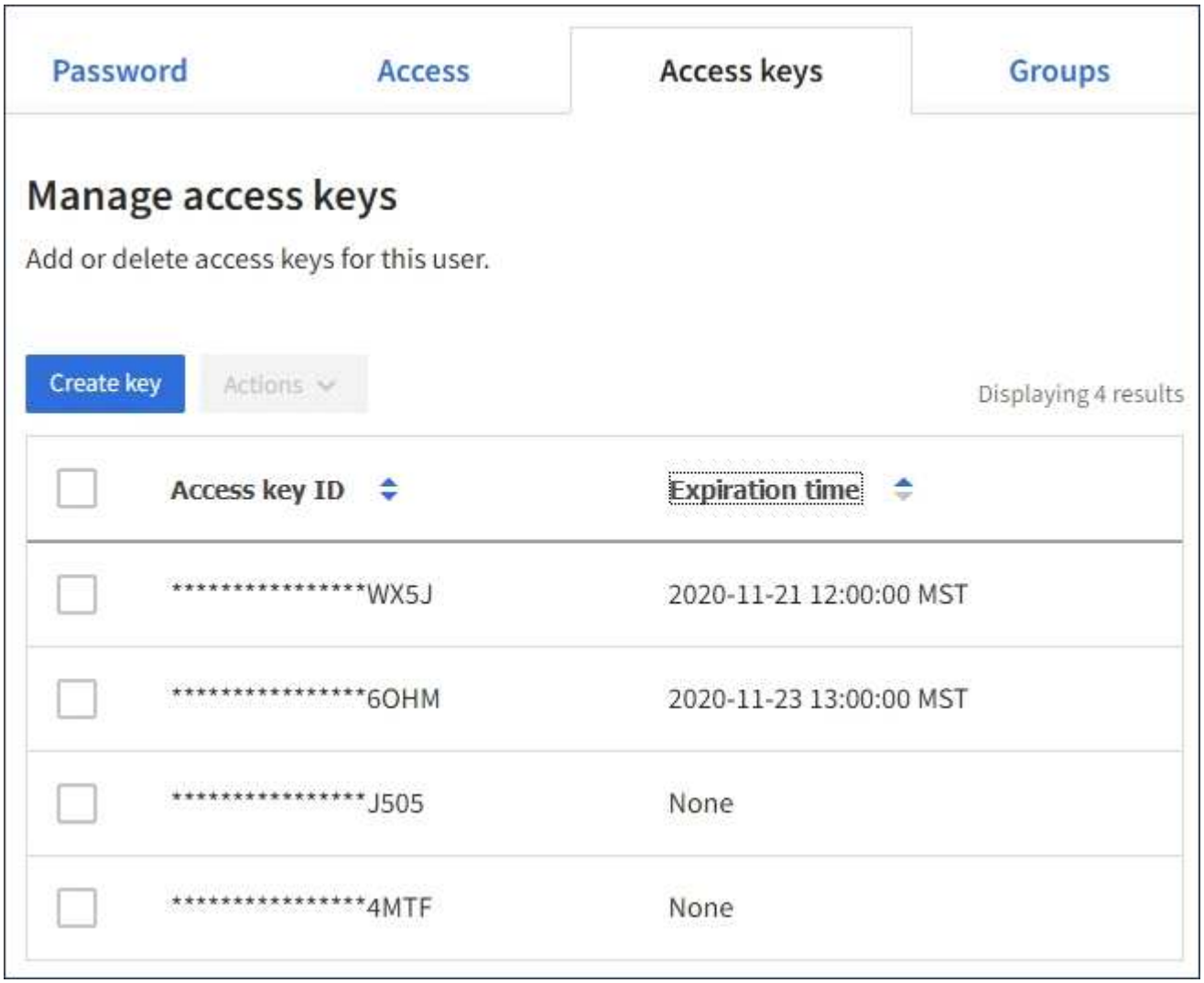
1. Sélectionnez **ACCESS MANAGEMENT** > **Users**.

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

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

   La page Détails de l'utilisateur s'affiche.

3. Sélectionnez **touches d'accès**.



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

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

   Les clés expirées sont supprimées automatiquement.

Informations associées

"Création des clés d'accès S3 d'un autre utilisateur"

"Suppression des clés d'accès S3 d'un autre utilisateur"

Suppression des clés d'accès S3 d'un autre utilisateur

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

Ce dont vous avez besoin

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

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

Étapes

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

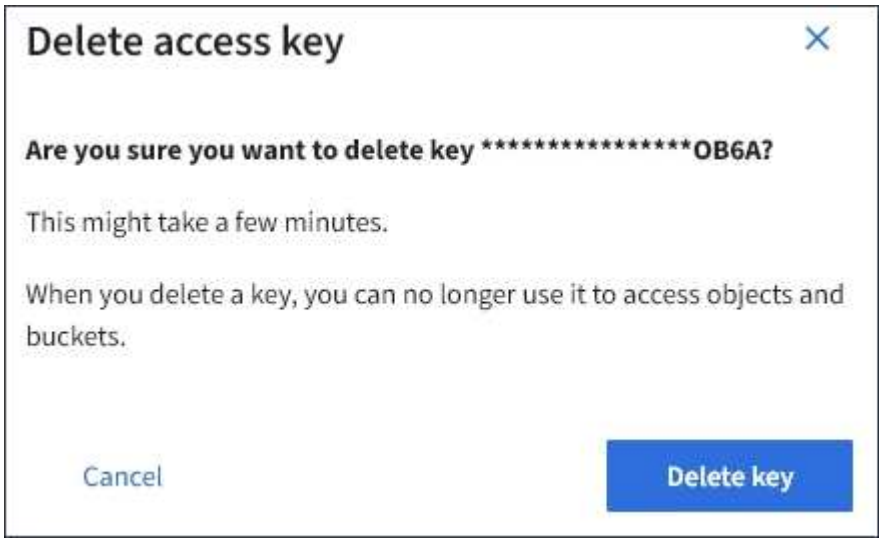
   La page utilisateurs s'affiche et répertorie les utilisateurs existants.

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

   La page Détails de l'utilisateur s'affiche.

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

   Une boîte de dialogue de confirmation s'affiche.



5. Sélectionnez **Supprimer la touche**.

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

Informations associées

"Autorisations de gestion des locataires"

Gestion des compartiments S3

Si vous utilisez un locataire S3 avec les autorisations appropriées, vous pouvez créer, afficher et supprimer des compartiments S3, mettre à jour les paramètres de niveau de cohérence, configurer le partage de ressources inter-origine (CORS), activer et désactiver les paramètres de mise à jour du dernier accès et gérer les services de la plateforme S3.

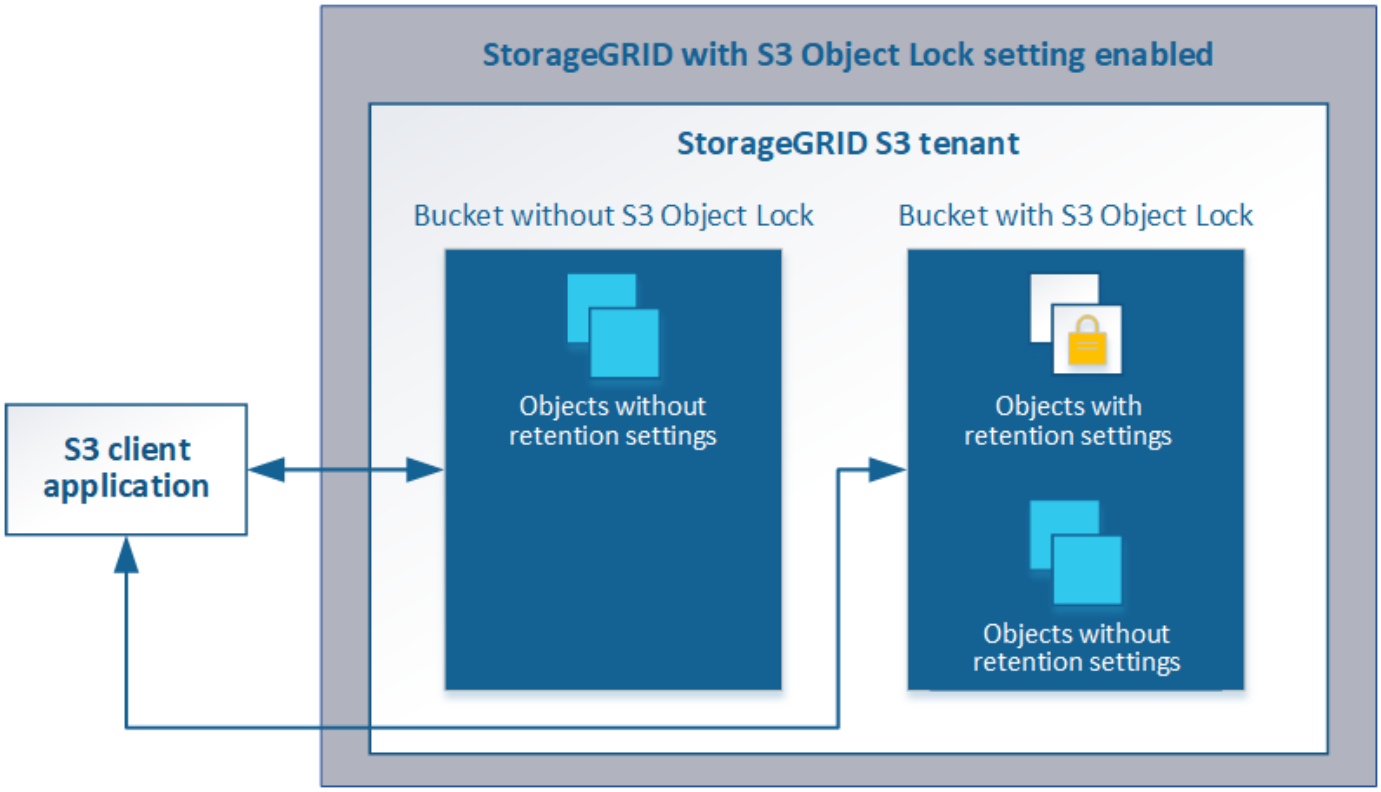
Utilisation du verrouillage d'objet S3

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

Qu'est-ce que le verrouillage objet S3 ?

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

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



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

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

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

Pour plus d'informations sur ces paramètres, consultez la section « utilisation du verrouillage d'objet S3 » dans "Opérations et limites prises en charge par l'API REST S3".

Gestion des compartiments conformes existants

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

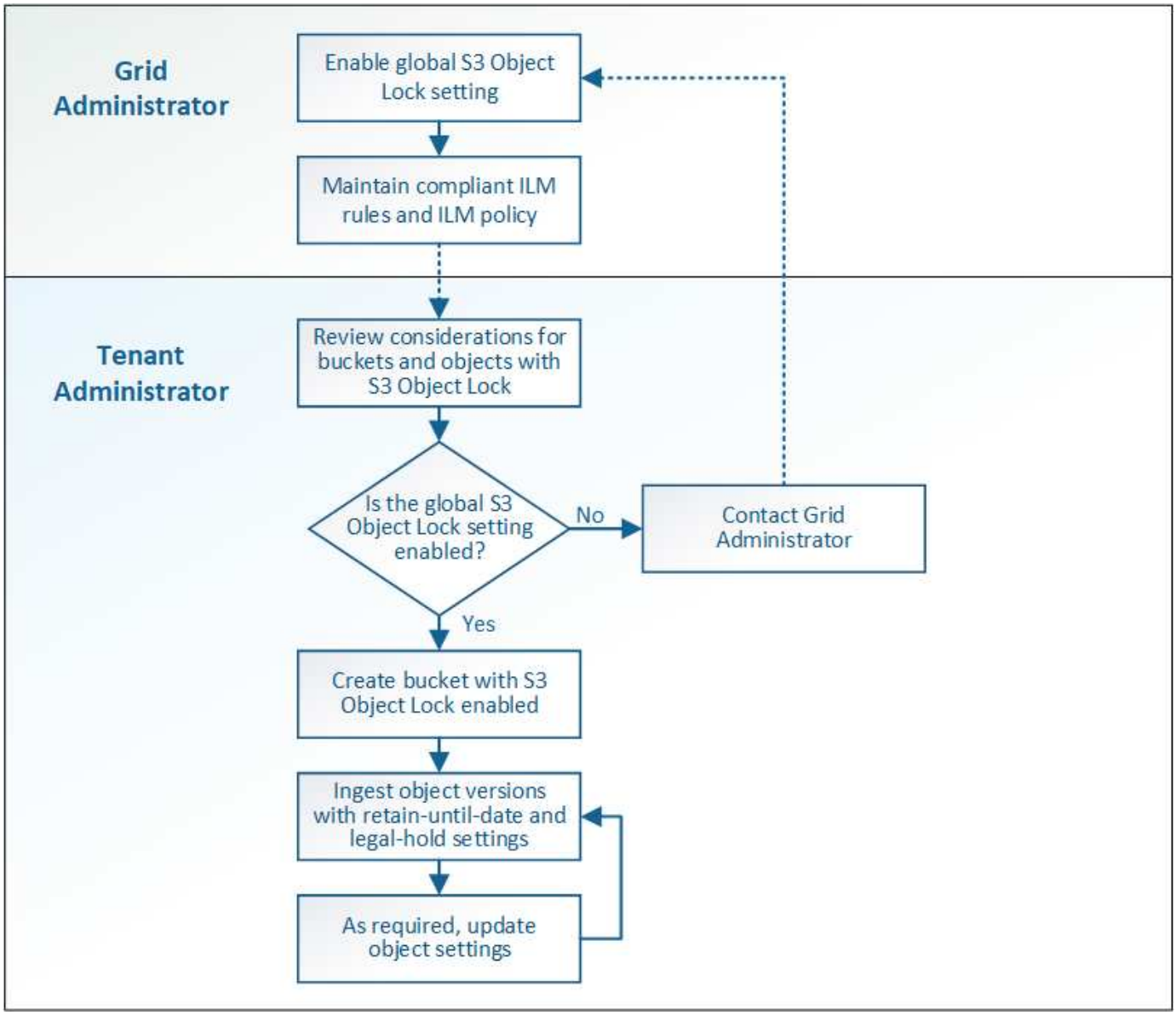
"Base de connaissances NetApp : comment gérer des compartiments conformes aux ancienne génération dans StorageGRID 11.5"

Workflow de verrouillage d'objet S3

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

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

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



Informations associées

"Gestion des objets avec ILM"

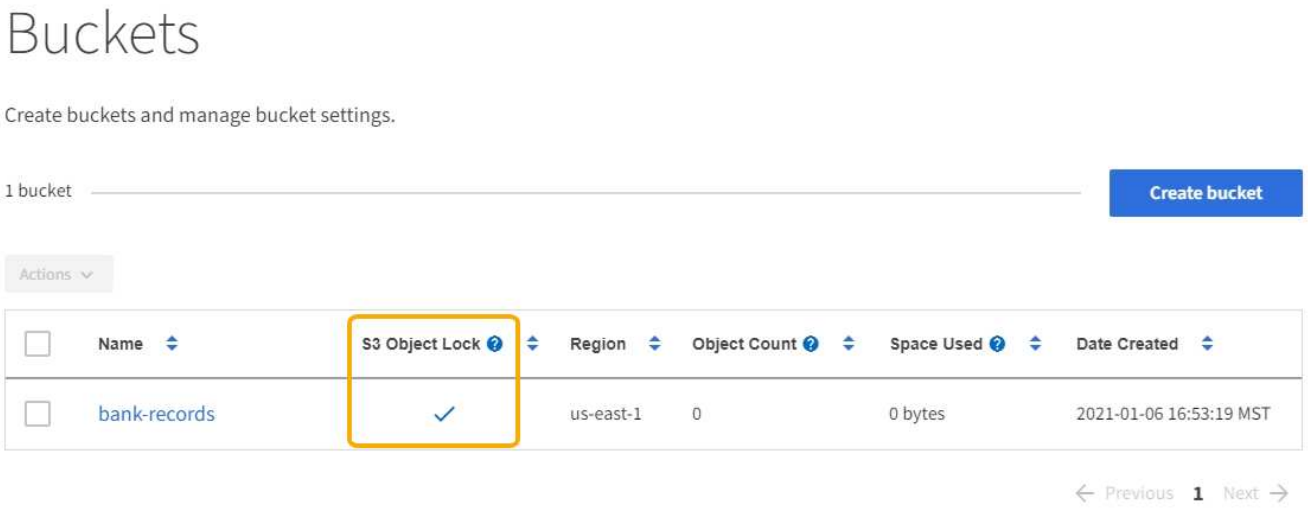
Conditions requises pour le verrouillage d'objet S3

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

Conditions requises pour les compartiments avec verrouillage objet S3 activé

- Si le paramètre global de verrouillage objet S3 est activé pour le système StorageGRID, vous pouvez utiliser le gestionnaire de locataires, l'API de gestion des locataires ou l'API REST S3 pour créer des compartiments avec le verrouillage objet S3 activé.

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



- Si vous prévoyez d'utiliser le verrouillage d'objet S3, vous devez activer le verrouillage d'objet S3 lors de la création du compartiment. Vous ne pouvez pas activer le verrouillage d'objet S3 pour un compartiment existant.
- Le contrôle de version de compartiment est requis avec le verrouillage d'objet S3. Lorsque le verrouillage d'objet S3 est activé pour un compartiment, StorageGRID active automatiquement le contrôle de version pour ce compartiment.
- Une fois que vous avez créé un compartiment avec le verrouillage d'objet S3 activé, vous ne pouvez pas désactiver le verrouillage d'objet S3 ou suspendre la gestion des versions pour ce compartiment.
- Un compartiment StorageGRID sur lequel le verrouillage d'objet S3 est activé ne dispose pas d'une période de conservation par défaut. À la place, l'application client S3 peut spécifier, éventuellement, une date de conservation et un paramètre de conservation légale pour chaque version d'objet ajoutée à ce compartiment.
- La configuration du cycle de vie des compartiments est prise en charge pour les compartiments de cycle de vie des objets S3.
- La réplication CloudMirror n'est pas prise en charge pour les compartiments avec le verrouillage objet S3 activé.

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

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

Cycle de vie des objets dans des compartiments avec verrouillage objet S3 activé

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

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

Création d'un compartiment S3

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

Ce dont vous avez besoin

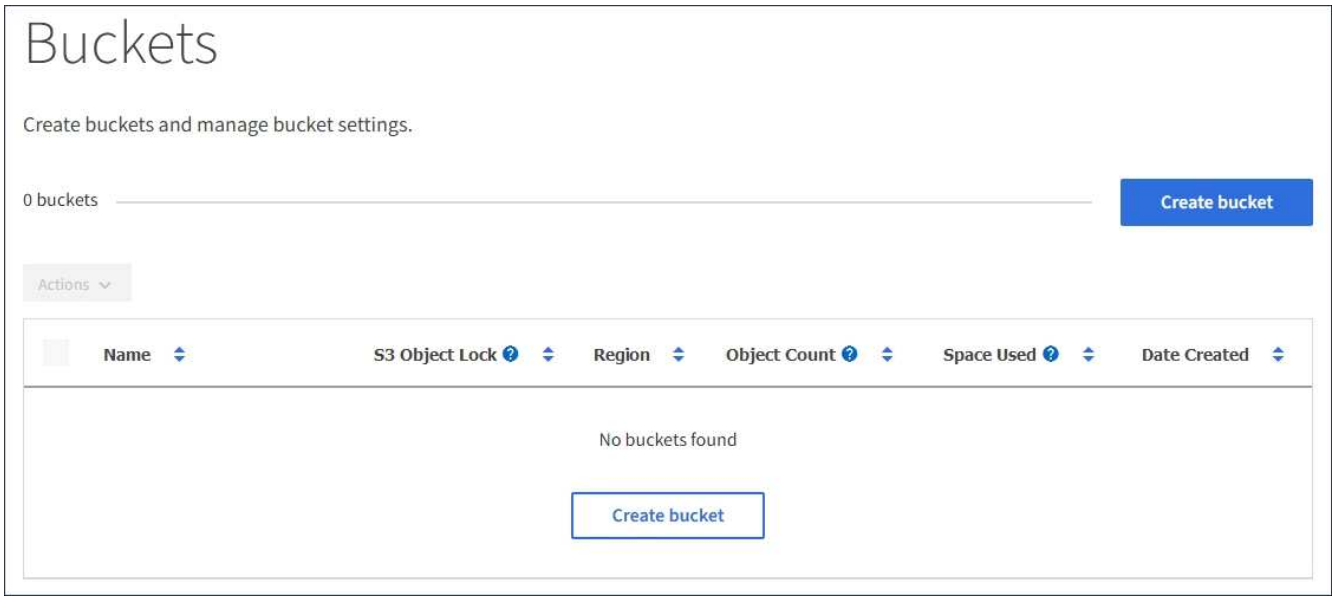
- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur pris en charge.
- Vous devez appartenir à un groupe d'utilisateurs possédant l'autorisation gérer toutes les rubriques ou accès racine. Ces autorisations remplacent les paramètres d'autorisations des stratégies de groupes ou de compartiments.
- Si vous prévoyez de créer un compartiment avec le verrouillage d'objet S3, le paramètre verrouillage d'objet S3 global doit avoir été activé pour le système StorageGRID et vous devez avoir vérifié les exigences relatives aux compartiments et objets de verrouillage d'objet S3.

  "Utilisation du verrouillage d'objet S3"

Étapes

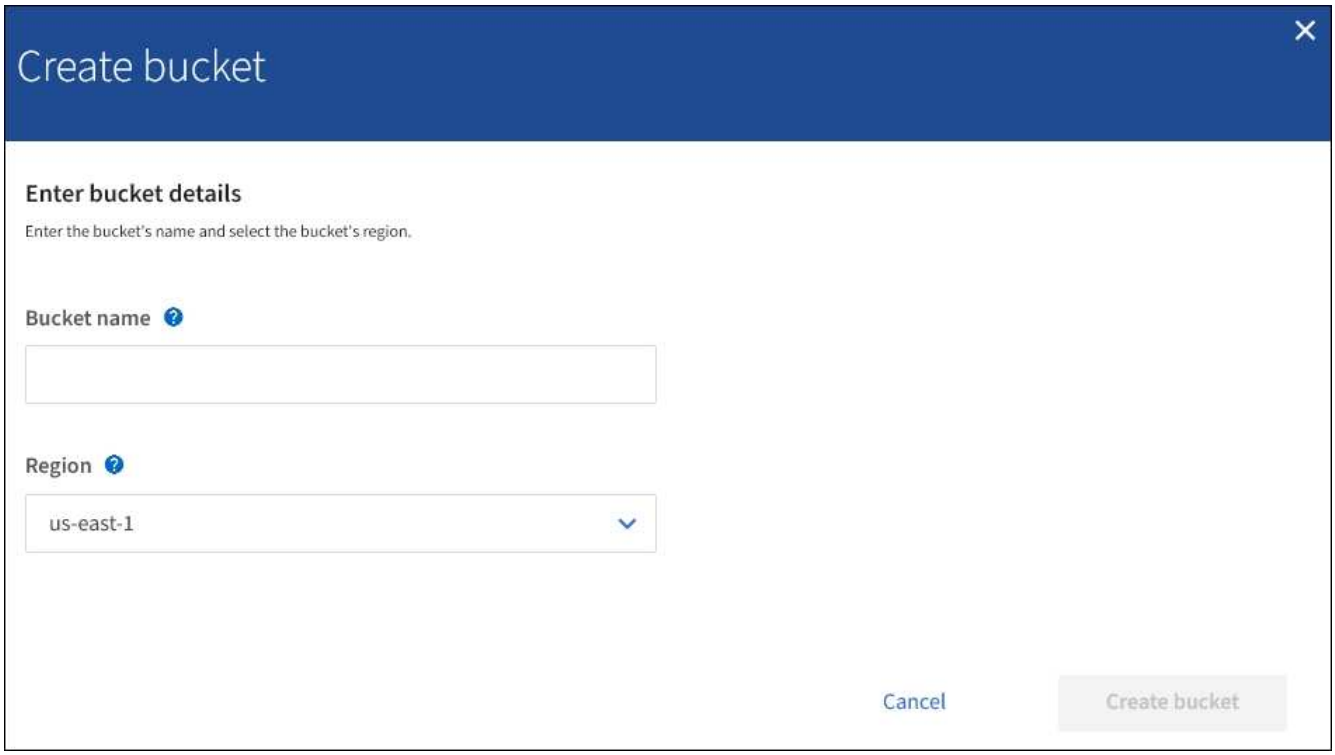
1. Sélectionnez **STOCKAGE (S3)** > **seaux**.

   La page rubriques s'affiche et répertorie les rubriques qui ont déjà été créées.



2. Sélectionnez **Créer un compartiment**.

   L'assistant Créer un compartiment s'affiche.



Si le paramètre global S3 Object Lock est activé, Create bucket inclut une deuxième étape de gestion du verrouillage d'objet S3 pour le compartiment.

3. Entrer un nom unique pour le compartiment.

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

   Les noms de compartiment doivent être conformes aux règles suivantes :

   - Il doit être unique sur chaque système StorageGRID (et pas seulement au sein du compte du locataire).
   - Doit être conforme DNS.
   - Doit contenir au moins 3 caractères et pas plus de 63 caractères.
   - 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.

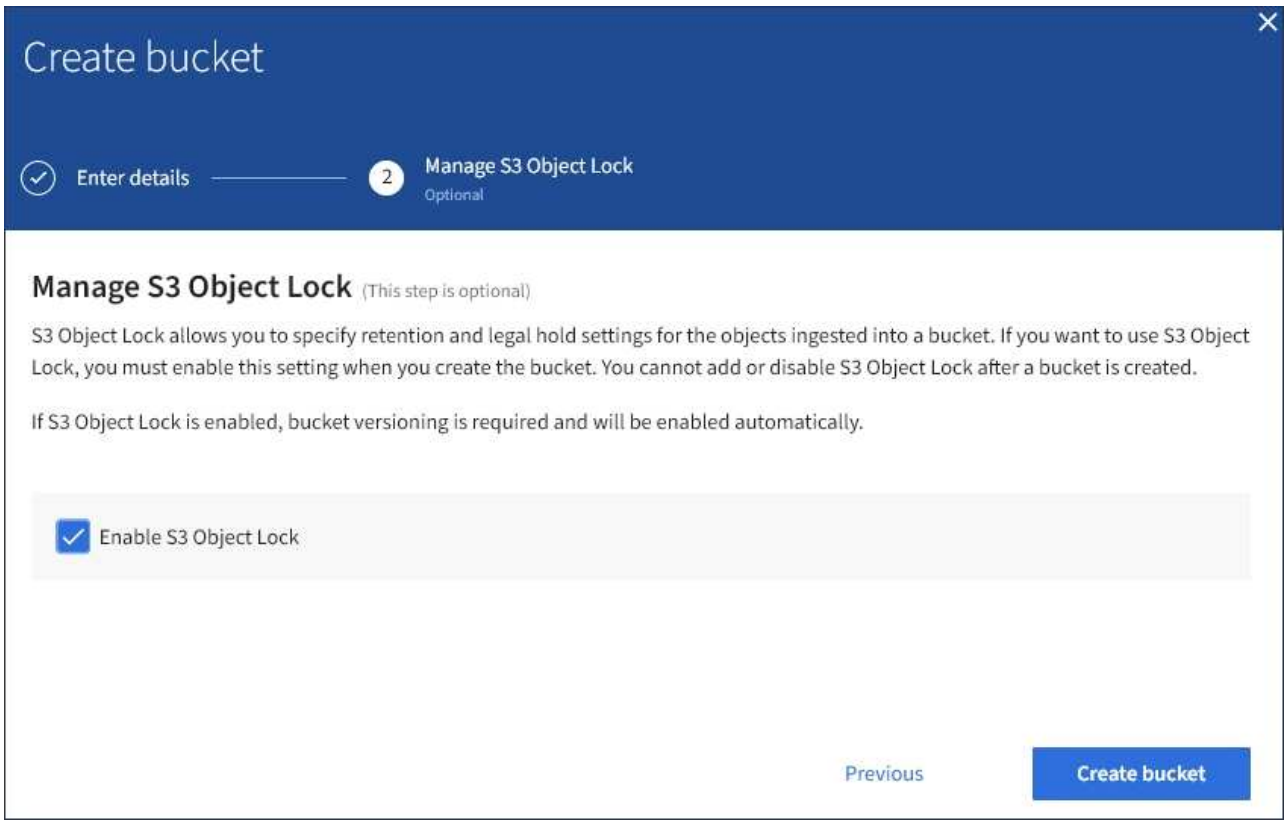
   Consultez la documentation Amazon Web Services (AWS) pour en savoir plus.

4. Sélectionnez la région de ce compartiment.

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

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

5. Sélectionnez **Créer un compartiment** ou **Continuer**.
   - Si le paramètre de verrouillage d'objet S3 global n'est pas activé, sélectionnez **Créer un compartiment**. Le godet est créé et ajouté au tableau sur la page godets.
   - Si le paramètre global de verrouillage d'objet S3 est activé, sélectionnez **Continuer**. L'étape 2, gérer le verrouillage d'objet S3 s'affiche.



6. Vous pouvez également cocher la case pour activer le verrouillage d'objet S3 pour ce compartiment.

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

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

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

7. Sélectionnez **Créer un compartiment**.

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

Informations associées

"Gestion des objets avec ILM"

"Présentation de l'API de gestion des locataires"

"Utilisation de S3"

Affichage des détails du compartiment S3

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

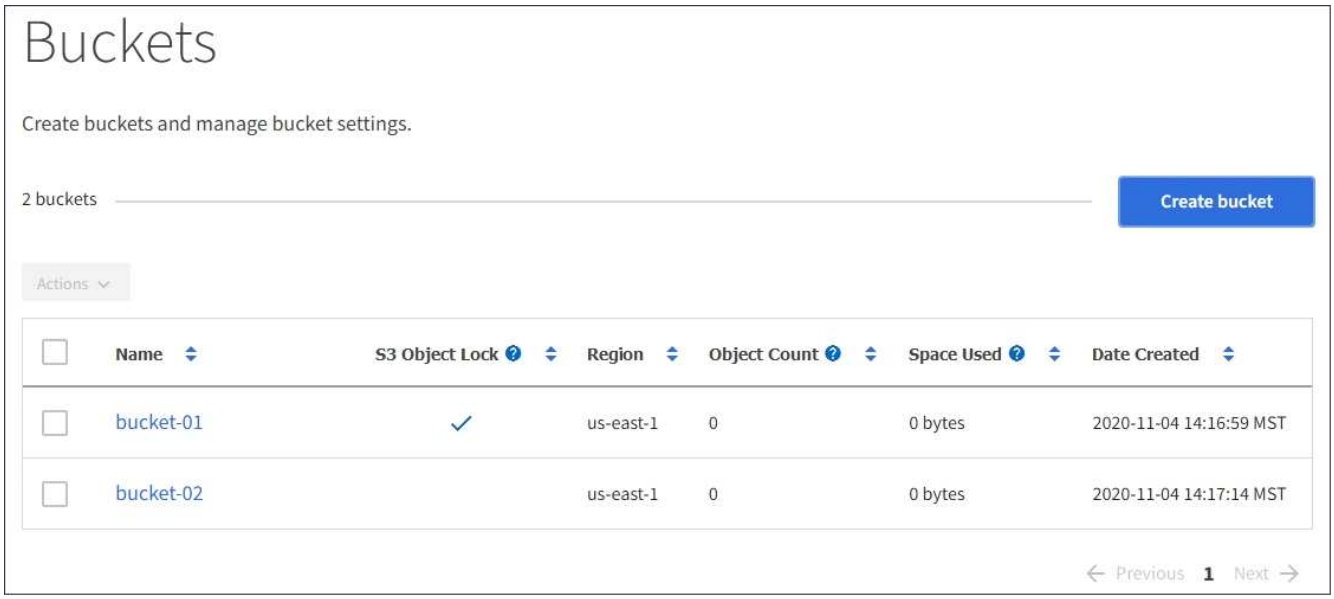
Ce dont vous avez besoin

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

Étapes

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

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



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

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

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

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

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

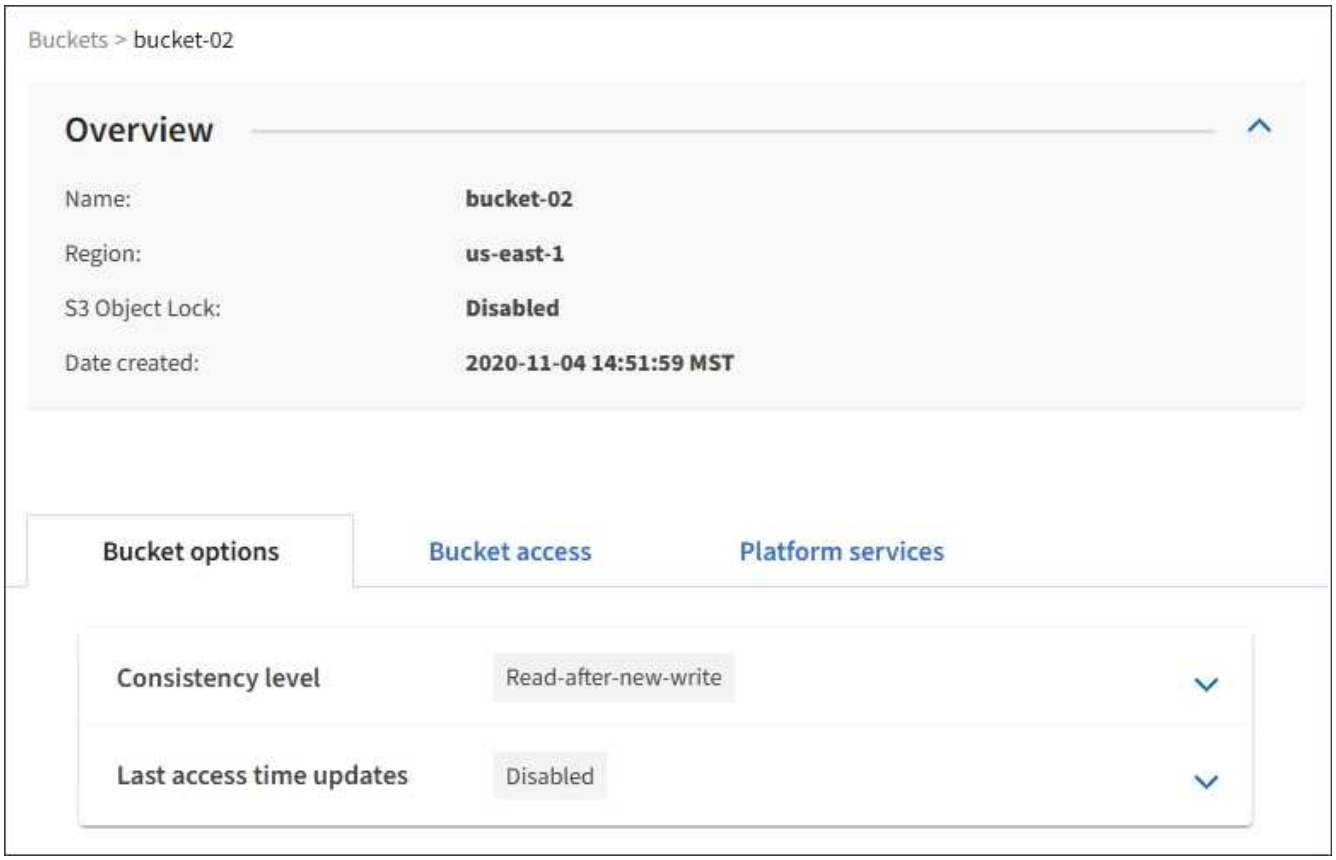
Les valeurs nombre d'objets et espace utilisé affichées sont des estimations. Ces estimations sont affectées par le moment de l'ingestion, la connectivité réseau et l'état des nœuds.

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

   La page des détails du compartiment s'affiche.

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

   Reportez-vous aux instructions de configuration de chaque paramètre ou service de plate-forme.



Informations associées

"Modification du niveau de cohérence"

"Activation ou désactivation des mises à jour de l'heure du dernier accès"

"Configuration du partage de ressources inter-origine (CORS)"

"Configuration de la réplication CloudMirror"

"Configuration des notifications d'événements"

"Configuration du service d'intégration de la recherche"

Modification du niveau de cohérence

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

Ce dont vous avez besoin

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

Description de la tâche

Le niveau de cohérence assure une reprise entre la disponibilité des objets et la cohérence de ces objets sur différents sites et nœuds de stockage. En général, vous devez utiliser le niveau de cohérence **Read-After-New-write** pour vos compartiments. Si le niveau de cohérence **Read-After-New-write** ne répond pas aux exigences de l'application client, vous pouvez modifier le niveau de cohérence en définissant le niveau de cohérence du compartiment ou en utilisant le `Consistency-Control` en-tête. Le `Consistency-Control` le cueilleur remplace le niveau de cohérence du godet.

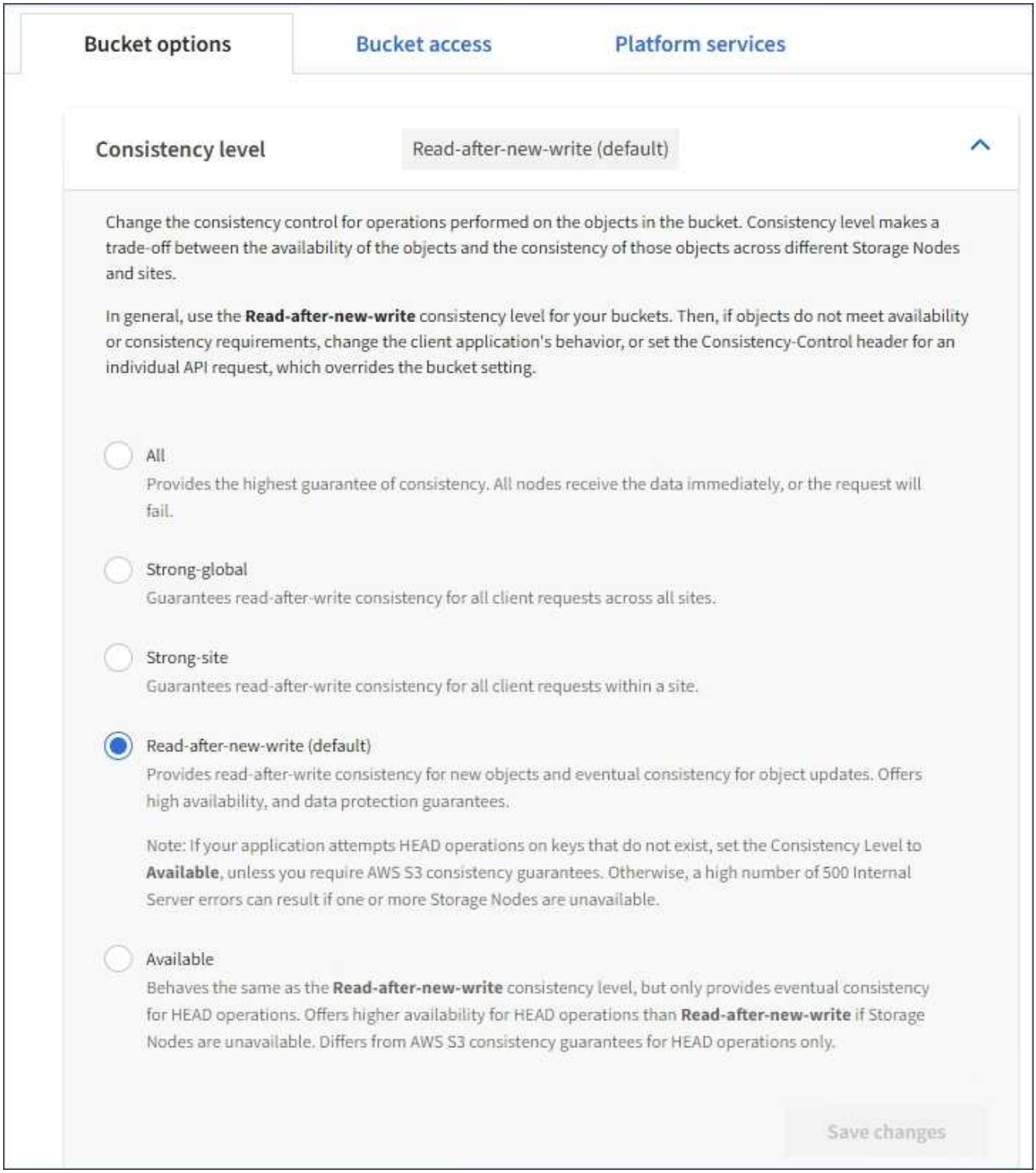
> Lorsque vous modifiez le niveau de cohérence d'un compartiment, seuls les objets ingérées après la modification sont garantis pour satisfaire le niveau révisé.

Étapes

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

   La page des détails du compartiment s'affiche.

3. Sélectionnez **Options de rubrique** > **niveau de cohérence**.



4. Sélectionnez un niveau de cohérence pour les opérations effectuées sur les objets de ce compartiment.

Niveau de cohérence	Description
Tout	Tous les nœuds reçoivent les données immédiatement, sinon la requête échoue.

Niveau de cohérence	Description
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 (par défaut)	Assure la cohérence de lecture après écriture pour les nouveaux objets et la cohérence des mises à jour d'objets. Offre une haute disponibilité et une protection des données garanties. Correspondance avec les garanties de cohérence Amazon S3. **Remarque :** si votre application tente D'effectuer DES opérations DE TÊTE sur des clés qui n'existent pas, définissez le niveau de cohérence sur **disponible**, à moins que vous n'ayez besoin des garanties de cohérence Amazon S3. Sinon, un nombre élevé de 500 erreurs de serveur interne peuvent se produire si un ou plusieurs nœuds de stockage ne sont pas disponibles.
Disponible (cohérence possible pour les opérations DE TÊTE)	Se comporte de la même manière que le niveau de cohérence **Read-After-New-write**, mais fournit uniquement une cohérence éventuelle pour les opérations HEAD. Offre une disponibilité plus élevée pour les opérations HEAD que **Read-After-New-write** si les nœuds de stockage ne sont pas disponibles. Diffère des garanties de cohérence Amazon S3 pour les opérations HEAD uniquement.

5. Sélectionnez **Enregistrer les modifications**.

Informations associées

"Autorisations de gestion des locataires"

Activation ou désactivation des mises à jour de l'heure du dernier accès

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

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

Ce dont vous avez besoin

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

Heure de dernier accès est l'une des options disponibles pour l'instruction de placement **temps de référence**

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

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

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

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

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

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

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

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

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

Type de demande	Comportement si l'heure du dernier accès est désactivée (par défaut)		Comportement si l'heure du dernier accès est activée	
	Heure du dernier accès mise à jour ?	Objet ajouté à la file d'attente d'évaluation ILM ?	Heure du dernier accès mise à jour ?	Objet ajouté à la file d'attente d'évaluation ILM ?
Demande de récupération d'un objet, de sa liste de contrôle d'accès ou de ses métadonnées	Non	Non	Oui.	Oui.
Demande de mise à jour des métadonnées d'un objet	Oui.	Oui.	Oui.	Oui.

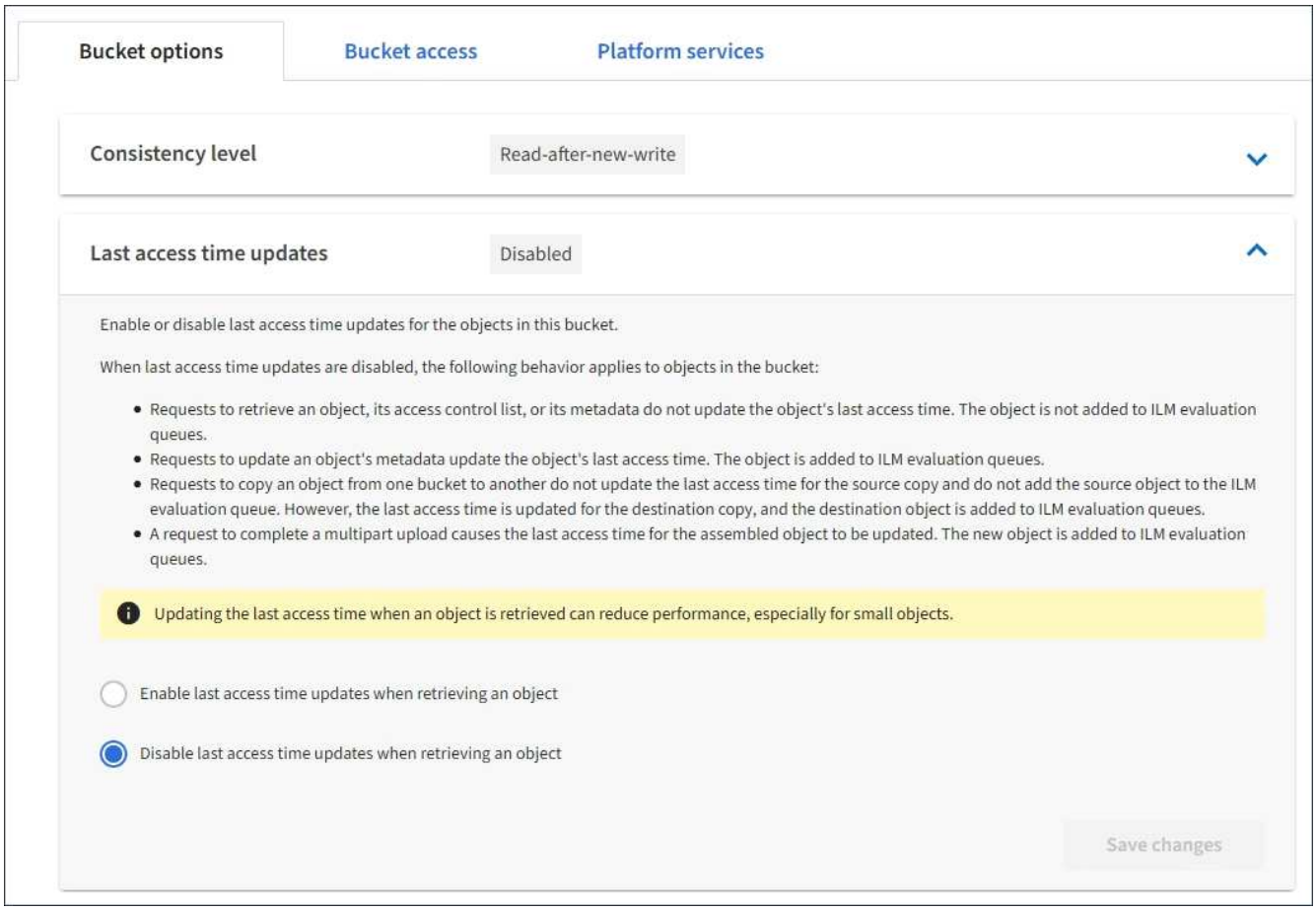
Demander de copier un objet d'un compartiment à un autre	• Non, pour la copie source • Oui, pour la copie de destination	• Non, pour la copie source • Oui, pour la copie de destination	• Oui, pour la copie source • Oui, pour la copie de destination	• Oui, pour la copie source • Oui, pour la copie de destination
Demander de terminer un téléchargement partitionné	Oui, pour l'objet assemblé	Oui, pour l'objet assemblé	Oui, pour l'objet assemblé	Oui, pour l'objet assemblé

Étapes

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

   La page des détails du compartiment s'affiche.

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



5. Sélectionnez **Enregistrer les modifications**.

Informations associées

"Autorisations de gestion des locataires"

"Gestion des objets avec ILM"

Configuration du partage de ressources inter-origine (CORS)

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

Ce dont vous avez besoin

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

Description de la tâche

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

Étapes

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

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

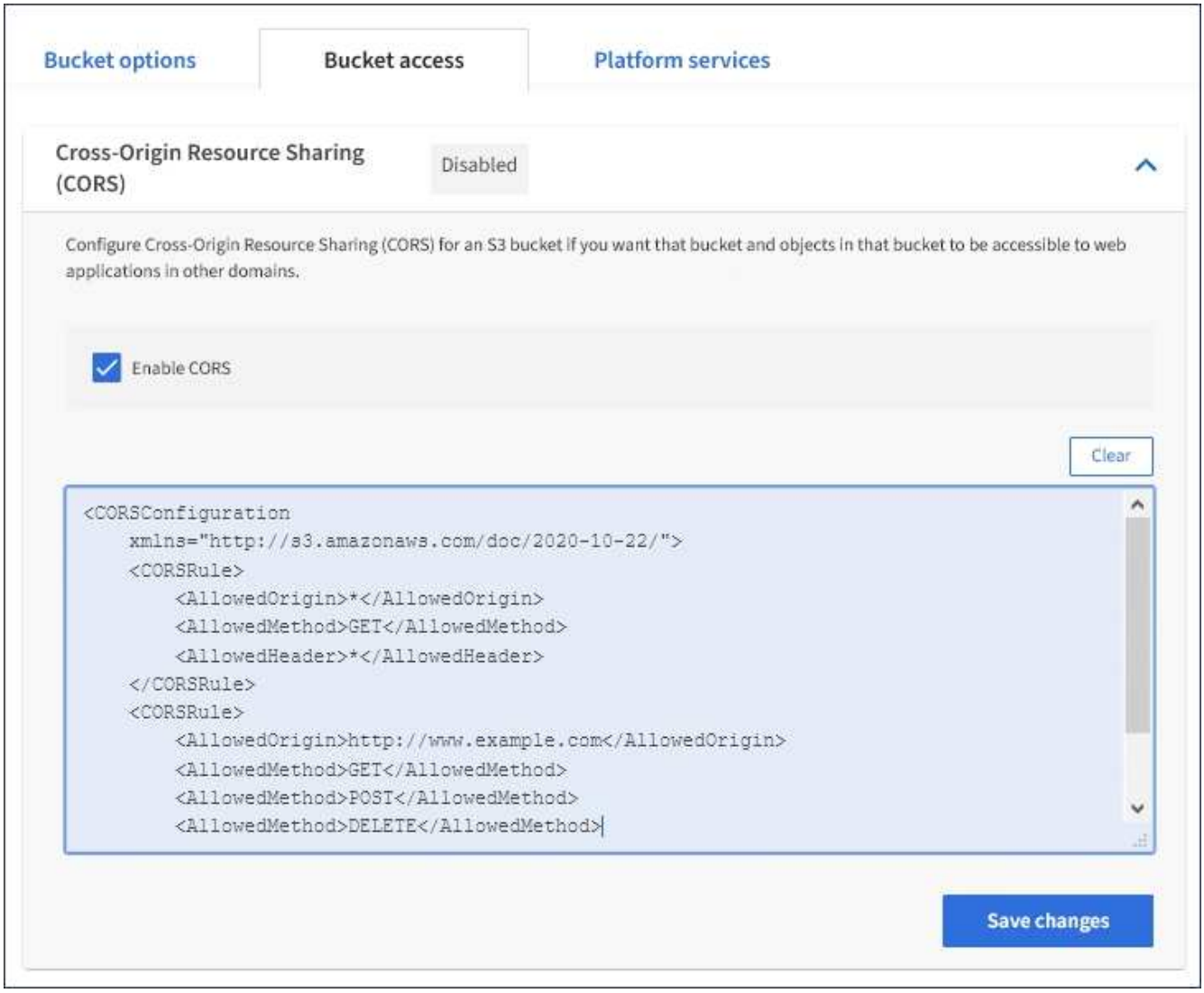
   ```
   <CORSConfiguration
       xmlns="http://s3.amazonaws.com/doc/2020-10-22/">
       <CORSRule>
           <AllowedOrigin>*</AllowedOrigin>
           <AllowedMethod>GET</AllowedMethod>
           <AllowedHeader>*</AllowedHeader>
       </CORSRule>
       <CORSRule>
           <AllowedOrigin>http://www.example.com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

   Pour plus d'informations sur le XML de configuration CORS, voir "Documentation Amazon Web Services (AWS) : guide du développeur Amazon simple Storage Service".

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

   La page des détails du compartiment s'affiche.

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



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

Suppression d'un compartiment S3

Vous pouvez utiliser le Gestionnaire de locataires pour supprimer un compartiment S3 vide.

Ce dont vous avez besoin

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

Description de la tâche

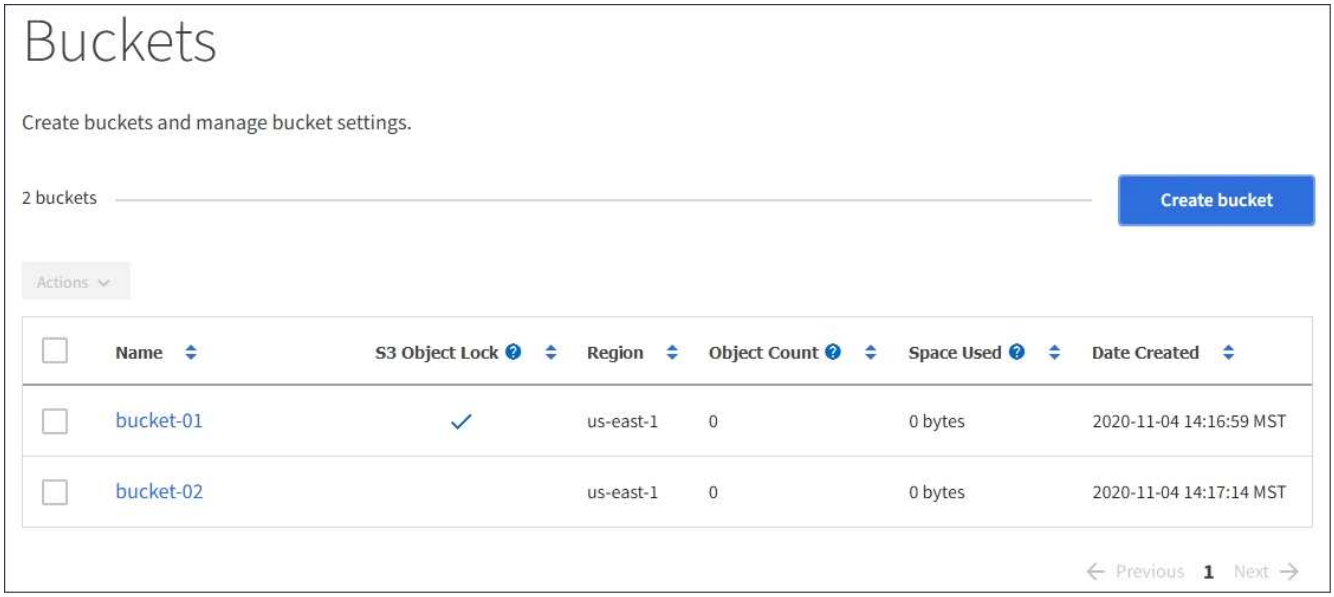
Ces instructions expliquent comment supprimer un compartiment S3 à l'aide du Gestionnaire des locataires. Vous pouvez également supprimer des compartiments S3 à l'aide de l'API de gestion des locataires ou de l'API REST S3.

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

Étapes

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

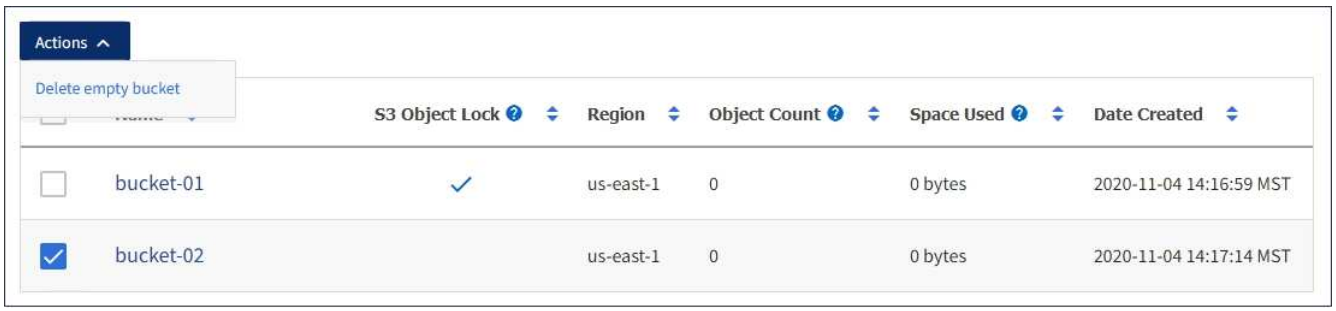
   La page compartiments s'affiche et affiche tous les compartiments S3 existants.



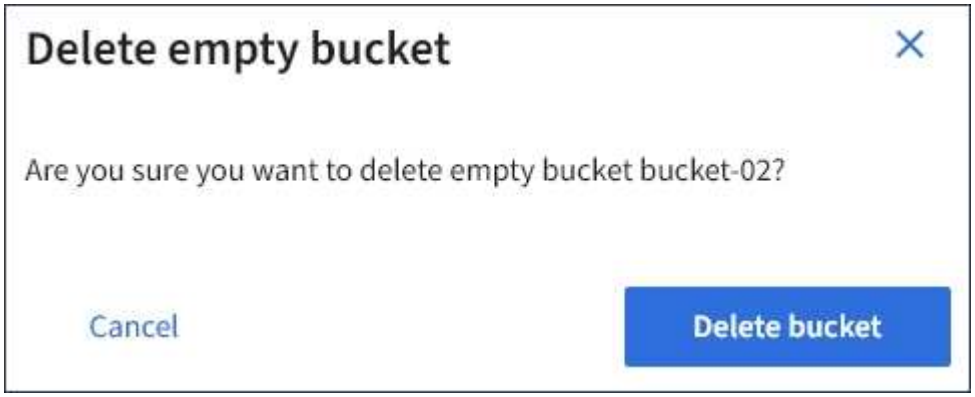
2. Cochez la case du compartiment vide que vous souhaitez supprimer.

   Le menu actions est activé.

3. Dans le menu actions, sélectionnez **Supprimer un compartiment vide**.



Un message de confirmation s'affiche.



4. Si vous êtes sûr de vouloir supprimer le compartiment, sélectionnez **Supprimer le compartiment**.

   L'StorageGRID confirme que le compartiment est vide avant de le supprimer. Cette opération peut prendre quelques minutes.

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

Informations associées

"Gestion des objets avec ILM"

Gestion des services de la plateforme S3

Si l'utilisation des services de plateforme est autorisée pour votre compte de locataire S3, vous pouvez utiliser des services de plateforme pour exploiter des services externes et configurer la réplication CloudMirror, les notifications et l'intégration de la recherche pour les compartiments S3.

- "Sont les services de plateforme"
- "Considérations relatives à l'utilisation des services de plate-forme"
- "Configuration des terminaux des services de plate-forme"
- "Configuration de la réplication CloudMirror"
- "Configuration des notifications d'événements"
- "À l'aide du service d'intégration de recherche"

Sont les services de plateforme

Les services de plateforme StorageGRID peuvent vous aider à mettre en œuvre une stratégie de cloud hybride.

Si l'utilisation des services de plateforme est autorisée pour votre compte de locataire, vous pouvez configurer les services suivants pour n'importe quel compartiment S3 :

- **Réplication CloudMirror** : le service de réplication StorageGRID CloudMirror permet la mise en miroir d'objets spécifiques d'un compartiment StorageGRID vers une destination externe spécifiée.

  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.

- **Notifications** : les notifications d'événements par compartiment sont utilisées pour envoyer des notifications sur des actions spécifiques effectuées sur des objets à un service externe Amazon simple notification Service™ (SNS) spécifié.

  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.

  > Bien que la notification d'événement puisse être configurée sur un compartiment avec l'option de verrouillage d'objet S3 activée, les métadonnées S3 Object Lock (conservation jusqu'à la date et état de conservation légale) des objets ne seront pas incluses dans les messages de notification.

- **Service d'intégration de recherche** : le service d'intégration de recherche est utilisé pour envoyer des métadonnées d'objet S3 à un index Elasticsearch spécifié où les métadonnées peuvent être recherchées ou analysées à l'aide du service externe.

  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.

  > Bien que l'intégration avec Elasticsearch puisse être configurée sur un compartiment avec l'option S3 Object Lock activée, les métadonnées S3 Object Lock (conservation jusqu'à la date et état de conservation légale) des objets ne seront pas incluses dans les messages de notification.

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 le service CloudMirror et les notifications sur un compartiment StorageGRID S3 afin de pouvoir mettre en miroir des objets spécifiques sur Amazon simple Storage Service, 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 plateforme communiquent avec des terminaux externes que vous configurez à l'aide du Gestionnaire de locataires ou de l'API de gestion des locataires. Chaque terminal représente une destination externe, par exemple un compartiment StorageGRID S3, un compartiment Amazon Web Services, un sujet SNS (simple notification Service) ou un cluster Elasticsearch hébergé localement, dans AWS ou ailleurs.

Après avoir créé un noeud final, 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 :

1. Si vous souhaitez que tous les objets dont les clés commencent par `/images` Pour la réplication vers un compartiment Amazon S3, vous devez ajouter une configuration de réplication dans le compartiment source.
2. Si vous souhaitez également envoyer des notifications lorsque ces objets sont stockés dans le compartiment, vous devez ajouter une configuration de notifications.
3. Enfin, si vous voulez indexer les métadonnées de ces objets, vous devez ajouter la configuration de notification de 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
Réplication CloudMirror	• RÉPLICATION des compartiments • RÉPLICATION des compartiments
Notifications	• GET Bucket notification • PUT Bucket notification
Intégration de la recherche	• CONFIGURATION DES notifications de métadonnées de compartiment • CONFIGURATION de notification des métadonnées de compartiment Ces opérations sont personnalisées pour StorageGRID.

Pour plus d'informations sur l'implémentation de ces API par StorageGRID, consultez les instructions relatives à l'implémentation des applications client S3.

Informations associées

"Utilisation de S3"

"Présentation du service de réplication CloudMirror"

"Présentation des notifications pour les compartiments"

"Présentation du service d'intégration de la recherche"

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

Présentation du service de réplication CloudMirror

Vous pouvez activer la réplication CloudMirror pour un compartiment S3 si vous souhaitez que StorageGRID réplique des objets spécifiés ajoutés au compartiment dans un ou plusieurs compartiments de destination.

La réplication CloudMirror fonctionne indépendamment de la règle ILM active 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.

Si vous activez la réplication CloudMirror pour un compartiment existant, seuls les nouveaux objets ajoutés à ce compartiment sont répliqués. Tout objet existant dans le compartiment n'est pas répliqué. 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 les objets vers une destination AWS S3, notez qu'Amazon S3 limite la taille des métadonnées définies par l'utilisateur dans chaque en-tête de demande PUT à 2 Ko. Si un objet possède des métadonnées définies par l'utilisateur supérieures à 2 Ko, cet objet ne sera pas répliqué.

Dans StorageGRID, vous pouvez répliquer les objets dans un compartiment unique vers plusieurs compartiments de destination. Pour ce faire, spécifiez la destination de chaque règle dans le XML de configuration de réplication. Vous ne pouvez pas répliquer un objet vers plusieurs compartiments à la fois.

En outre, vous pouvez configurer la réplication CloudMirror pour les compartiments avec version ou sans version, et spécifier un compartiment avec version ou sans version comme destination. 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.

Le comportement de suppression du service de réplication CloudMirror est identique au comportement de suppression du service CRR (Cross Region Replication) fourni par Amazon S3 — 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 multiversion, la suppression d'un objet du compartiment source ne réplique pas le marqueur de suppression vers le compartiment de destination ou supprime l'objet de destination.

Lors de la réplication des objets dans le compartiment de destination, StorageGRID les désigne par « duplicaas ». Un compartiment StorageGRID de destination ne réplique pas les objets marqués comme répliques, ce qui vous protège des boucles de réplication accidentelles. Ce marquage de réplication est interne à StorageGRID et ne vous empêche pas d'utiliser AWS CRR lorsque vous utilisez 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 réseaux.

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.

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.

Informations associées

"Configuration de la réplication CloudMirror"

Présentation des notifications pour les compartiments

Vous pouvez activer la notification des événements pour un compartiment S3 si vous souhaitez que StorageGRID envoie des notifications sur les événements spécifiés à un service Amazon simple notification Service (SNS) de destination.

Vous pouvez configurer les notifications d'événements en associant XML de configuration de notification à un compartiment source. Le XML de configuration de notification respecte les conventions S3 pour la configuration des notifications de compartiment, avec la rubrique SNS de destination spécifiée comme URN d'un terminal.

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.

Notre approche unique et notre 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 le `sequencer` Key dans le message d'événement pour déterminer l'ordre des événements pour un objet particulier, tel que décrit dans la documentation Amazon S3.

Notifications et messages pris en charge

La notification d'événements StorageGRID suit l'API Amazon S3 avec les limites suivantes :

- Vous ne pouvez pas configurer une 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 les autres, comme illustré dans le tableau :

Nom de la clé	Valeur ajoutée de StorageGRID
Source d'événements	`sgws:s3`

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

Informations associées

"Configuration des notifications d'événements"

Présentation du 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 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 mise à jour d'un objet ou de ses métadonnées. 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 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 sont générées sous la forme d'un document JSON nommé avec le nom de 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.

Les notifications sont générées et mises en file d'attente pour livraison chaque fois que :

- 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. Toutefois, les notifications ne sont pas envoyées 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.

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 *Interoperability Matrix Tool* pour déterminer les versions prises en charge par Elasticsearch.

Informations associées

"Matrice d'interopérabilité NetApp"

"XML de configuration pour l'intégration de la recherche"

"Métadonnées d'objet incluses dans les notifications de métadonnées"

"JSON généré par le service d'intégration de la recherche"

"Configuration du service d'intégration de la recherche"

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

Avant de mettre en œuvre des services de plateforme, examinez les recommandations et les considérations relatives à l'utilisation de ces services.

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.

Réflexion	Détails
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.
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 faire correspondre le comportement de suppression des services CRR et SNS d'AWS, les demandes de notification d'événements et CloudMirror ne sont pas envoyées lorsqu'un objet dans le compartiment source est supprimé en raison des règles ILM d'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.

Considérations relatives à l'utilisation du service de réplication CloudMirror

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

Taille de l'objet	La taille maximale des objets qui peuvent être répliqués sur un compartiment de destination par le service de réplication CloudMirror est de 5 To, ce qui est identique à la taille maximale d'objet prise en charge par StorageGRID.
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 demandes DE balisage d'objets PUT ou DELETE Object tagging 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'existe aucun moyen 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 demandes de balisage d'objets PUT ou SUPPRIME les demandes de balisage d'objets 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. En conséquence, le `ETag` la valeur de l'objet symétrique sera différente de la `ETag` valeur 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 chiffrés avec SSE-C. Si vous tentez 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	Si le compartiment S3 de destination pour la réplication CloudMirror est activé pour le verrouillage des objets S3, l'opération de réplication échoue avec une erreur AccessDenied.

Informations associées

"Utilisation de S3"

Configuration des terminaux des services de plate-forme

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 point final de services de plateforme, vous devez être un utilisateur locataire disposant de l'autorisation gérer les points de terminaison ou accès racine, dans une grille dont la mise en réseau a été configurée pour permettre aux nœuds de stockage d'accéder aux ressources de point final externes. Pour plus d'informations, contactez votre administrateur StorageGRID.

Qu'est-ce qu'un terminal de services de plate-forme

Lorsque vous créez un noeud final de services de plate-forme, vous spécifiez 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 S3, vous créez un terminal de services de plateforme qui inclut les informations et les identifiants requis par StorageGRID pour accéder au compartiment de destination sur AWS.

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 utiliser plusieurs points de terminaison comme cible, ce qui vous permet d'envoyer des notifications sur la création d'objet à une rubrique SNS et des notifications sur la suppression d'objet à une autre rubrique 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 SNS (simple notification Service). Les terminaux SQS (simple Queue Service) ou Lambda d'AWS ne sont pas pris en charge.

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"

Spécification de l'URN pour un terminal de services de plate-forme

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 créez 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 terminal de services de plateforme doit commencer par l'un ou l'autre `arn:aws` ou `urn:mysite`, comme suit:

- Si le service est hébergé sur AWS, utilisez `arn:aws`.
- Si le service est hébergé localement, utilisez `urn:mysite`

Par exemple, si vous spécifiez l'URN pour un terminal CloudMirror hébergé sur StorageGRID, il peut commencer par l'URN `urn:sgws`.

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

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

Par exemple, pour continuer à spécifier l'URN d'un terminal CloudMirror hébergé sur StorageGRID, vous devez ajouter `s3` pour 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	nom du compartiment
Notifications	nom-rubrique-sns
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

Pour les entités AWS, 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 indiqué 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 terminal CloudMirror hébergé sur StorageGRID, vous pouvez spécifier un URN valide

commençant par `urn:sgws`:

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

- Notifications :

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

- Intégration de la recherche :

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

> Pour les points de terminaison d'intégration de recherche hébergés localement, le `domain-name` L'élément peut être n'importe quelle chaîne tant que l'URN du terminal est unique.

Création d'un point final de services de plate-forme

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

Ce dont vous avez besoin

- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur pris en charge.
- Les services de plateforme doivent être activés pour votre compte de locataire par un administrateur StorageGRID.
- Vous devez appartenir à un groupe d'utilisateurs possédant l'autorisation gérer les noeuds finaux.
- La ressource référencée par le point final des services de plate-forme doit avoir été créée :
  - Réplication CloudMirror : compartiment S3
  - Notification d'événement : rubrique SNS
  - Notification de recherche : index Elasticsearch, si le cluster de destination n'est pas configuré pour créer automatiquement des index.
- Vous devez disposer 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)

    "Spécification de l'URN pour un terminal de services de plate-forme"

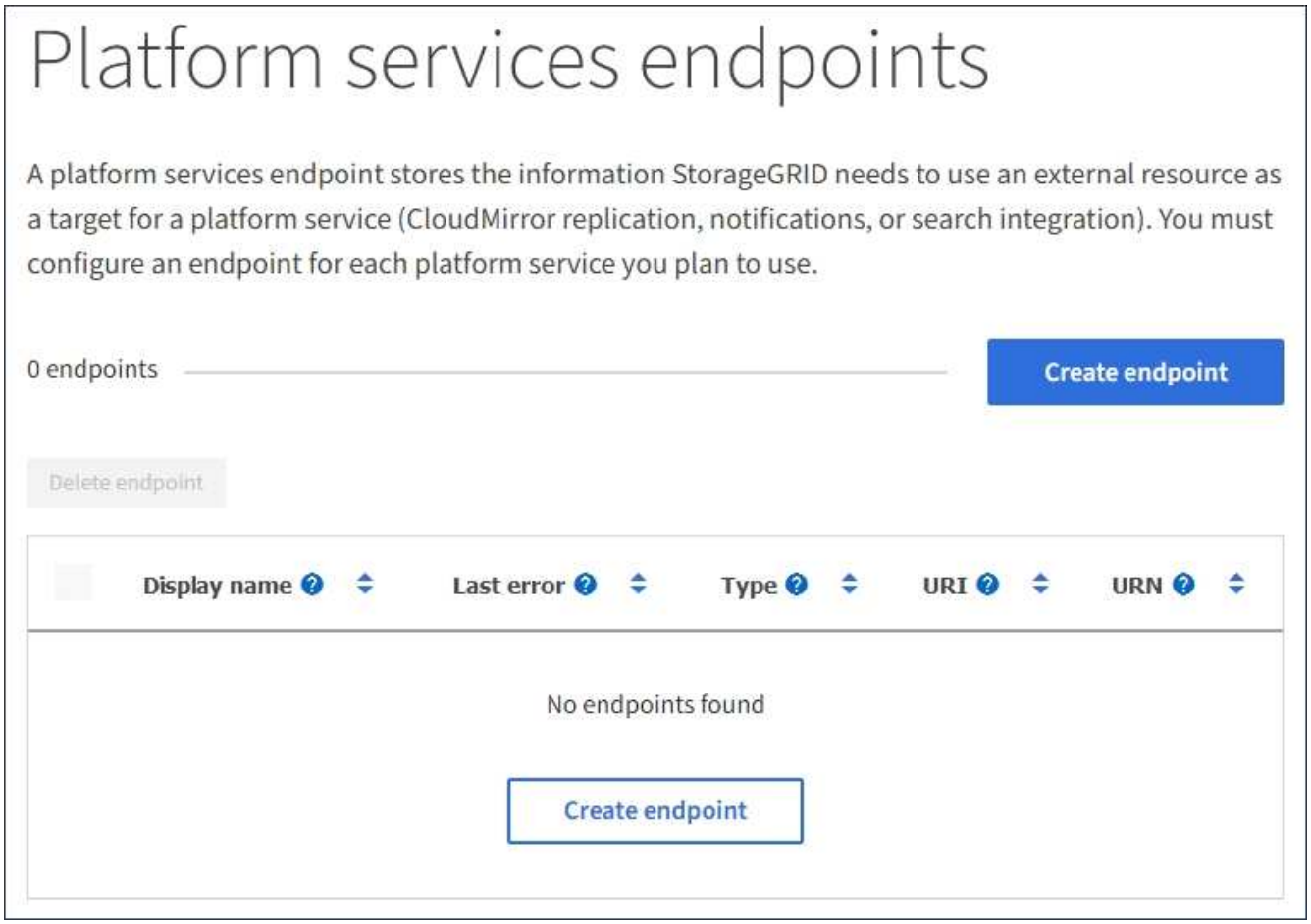
  - Informations d'authentification (si nécessaire) :
    - Clé d'accès : ID de clé d'accès et clé d'accès secrète

        - HTTP de base : nom d'utilisateur et mot de passe
    - Certificat de sécurité (en cas d'utilisation d'un certificat d'autorité de certification personnalisé)

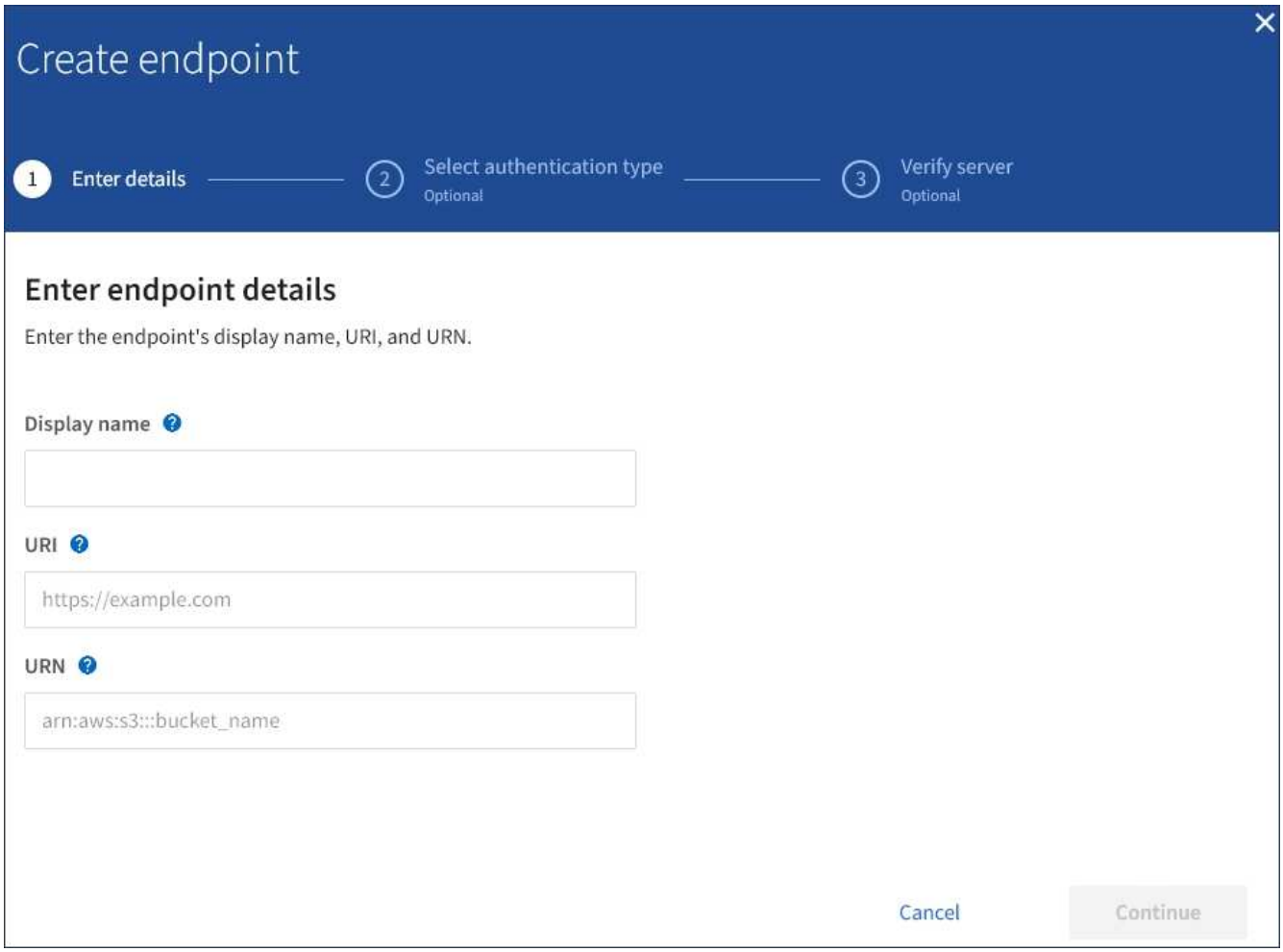
Étapes

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 s'affiche en regard du nom du noeud final lorsqu'il est répertorié sur la page noeuds finaux. Vous n'avez donc 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, le port 443 est utilisé pour les URI HTTPS et le port 80 est utilisé pour les URI HTTP.

   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, et `10443` représente le port défini dans le noeud final de l'équilibreur de charge.

> Lorsque cela est possible, vous devez vous connecter à un groupe haute disponibilité de nœuds d'équilibrage de la charge afin d'éviter un point de défaillance unique.

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

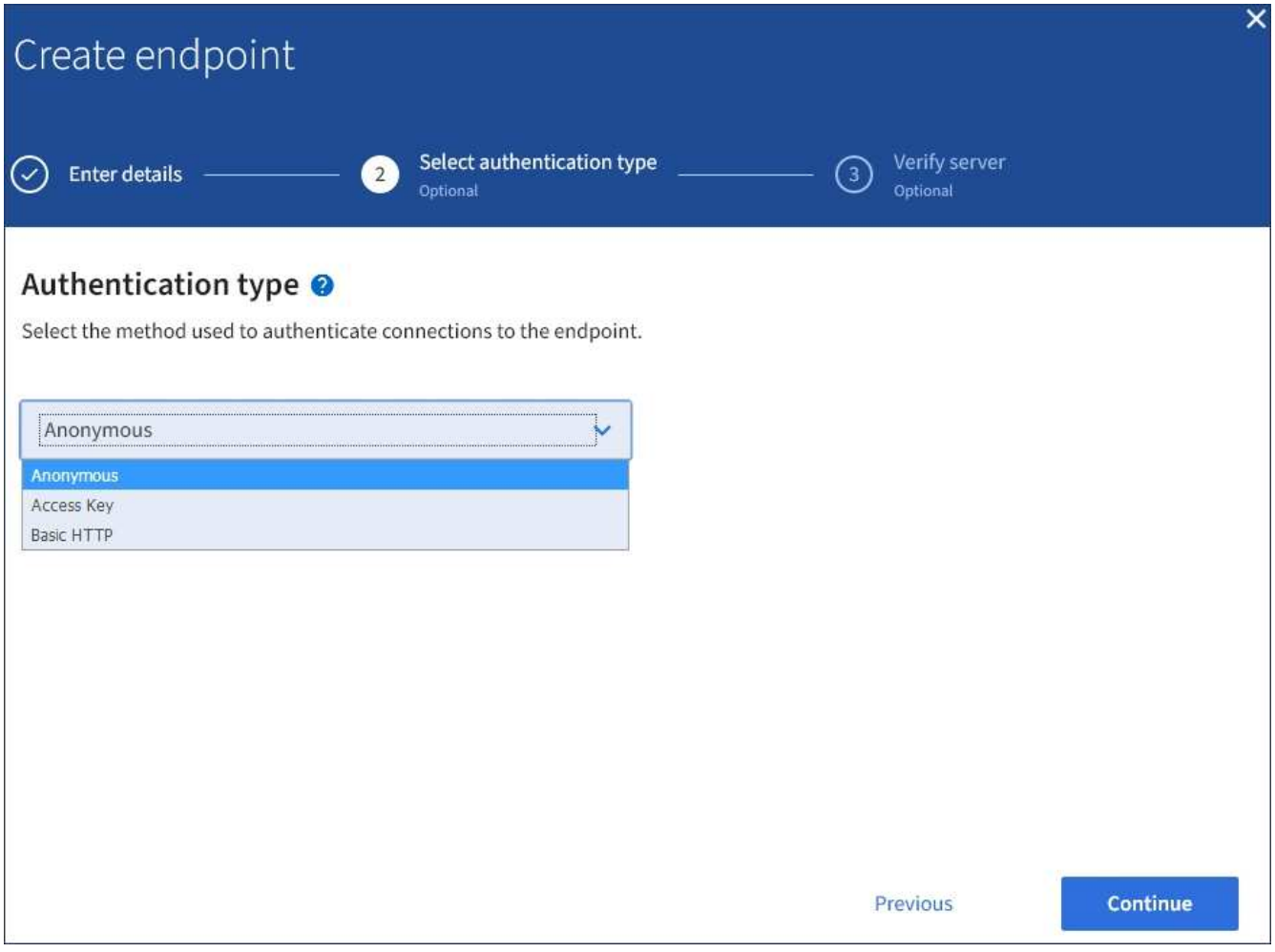
```
https://s3-aws-region.amazonaws.com
```

> 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 terminal après sa création.

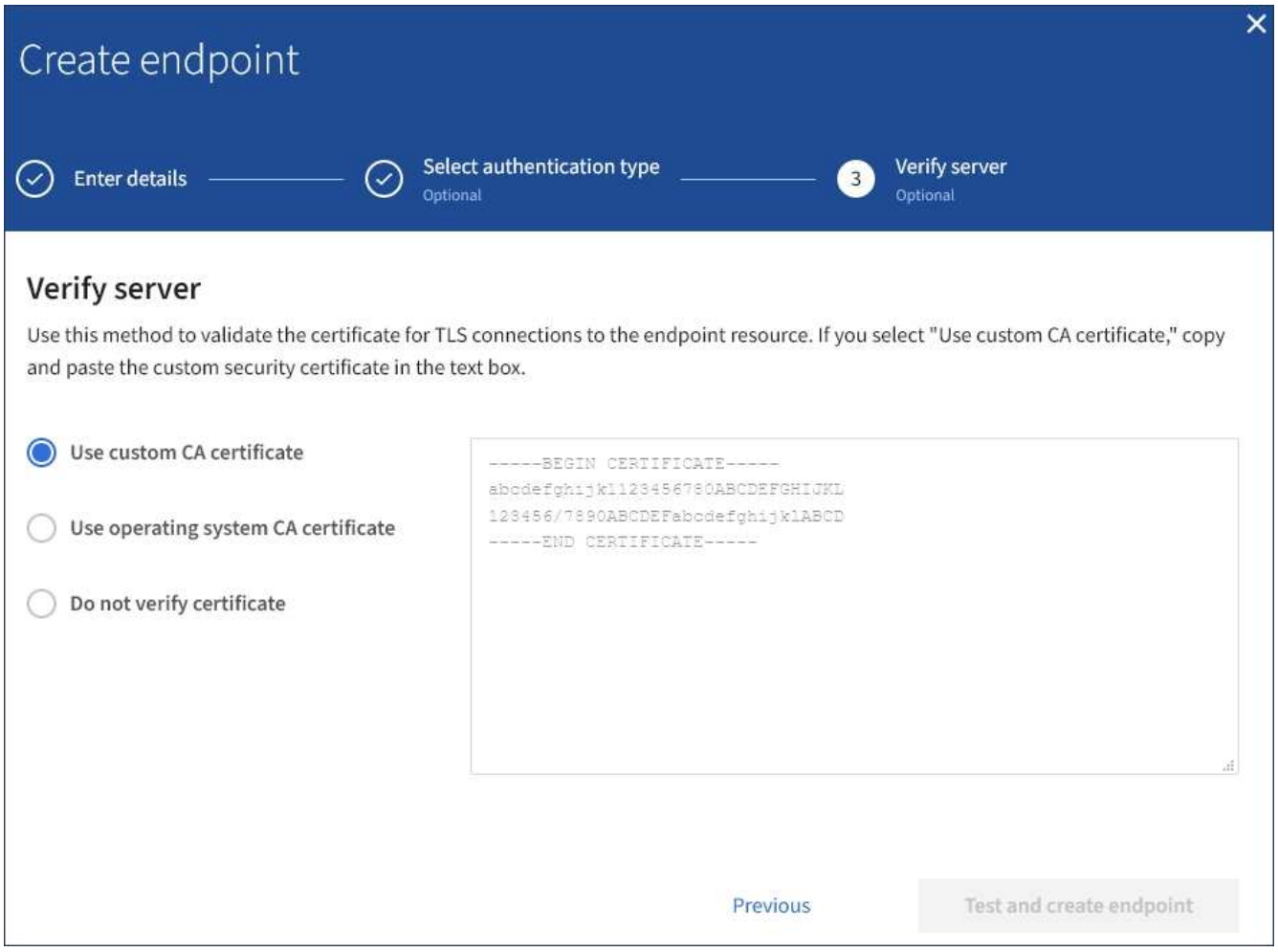
6. Sélectionnez **Continuer**.
7. Sélectionnez une valeur pour **Type d'authentification**, puis saisissez les informations d'identification requises.



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

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 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 de point final 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

"Spécification de l'URN pour un terminal de services de plate-forme"

"Configuration de la réplication CloudMirror"

"Configuration des notifications d'événements"

"Configuration du service d'intégration de la recherche"

Test de la connexion pour un point final de 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.

Ce dont vous avez besoin

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

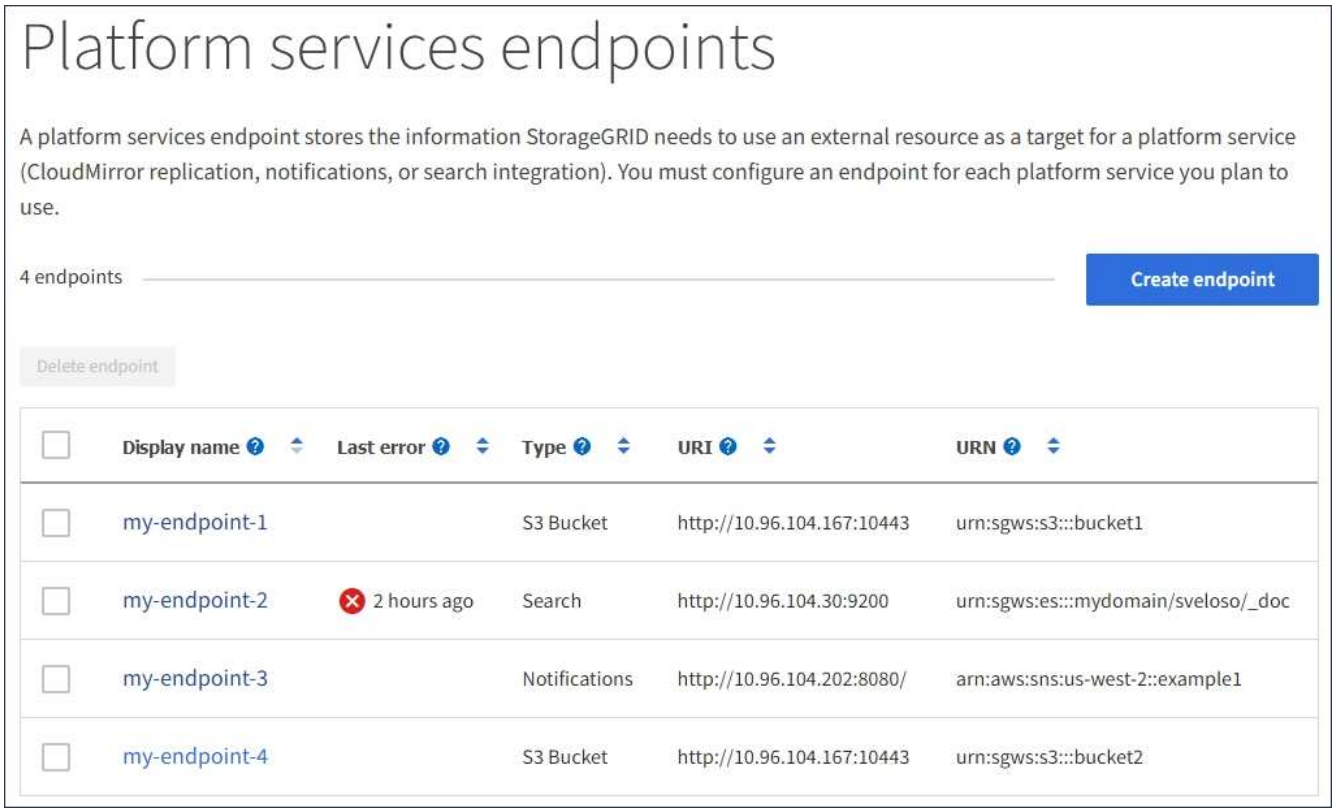
Description de la tâche

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

Étapes

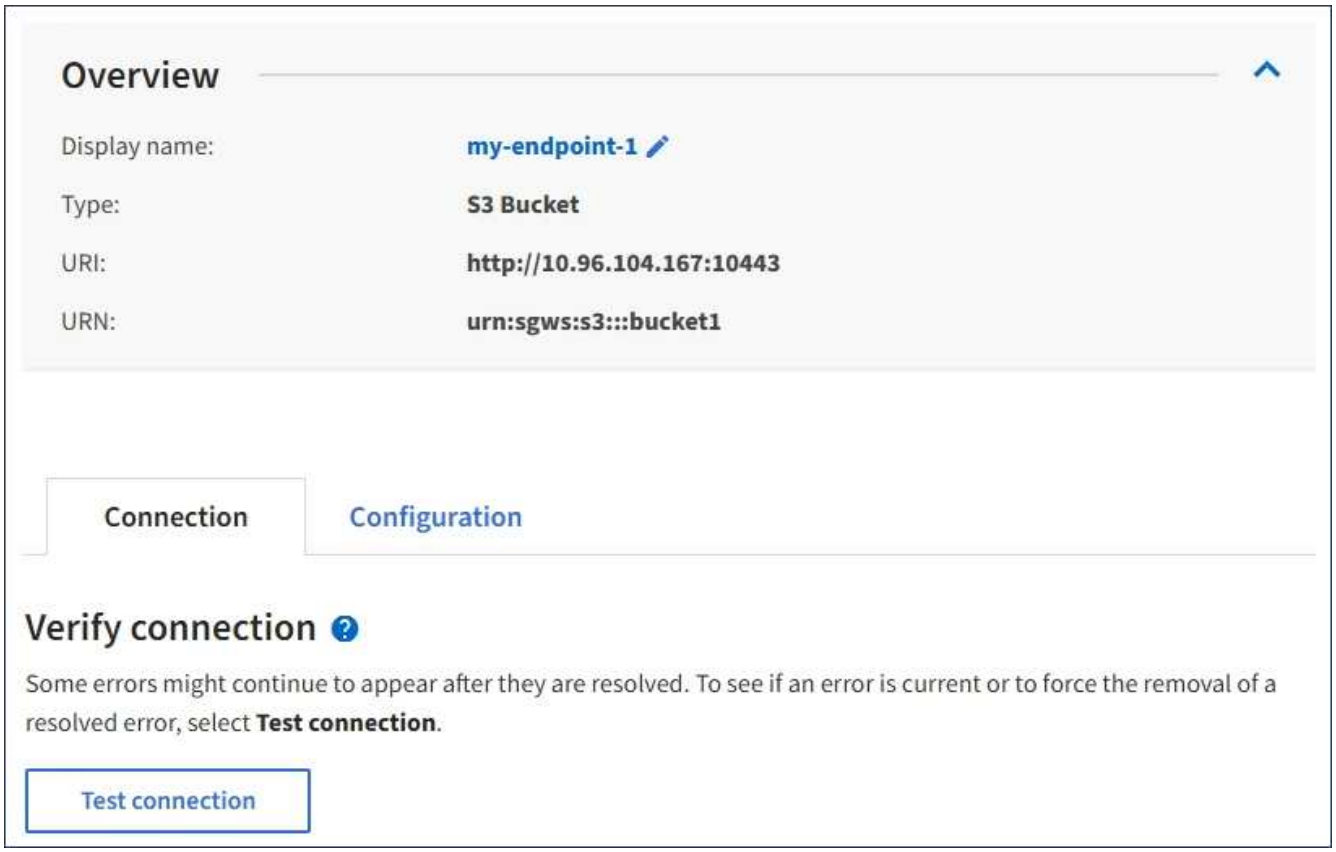
1. Sélectionnez **STORAGE (S3)** > **Platform services Endpoints**.

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**.

Modification d'un noeud final de 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 plateforme.

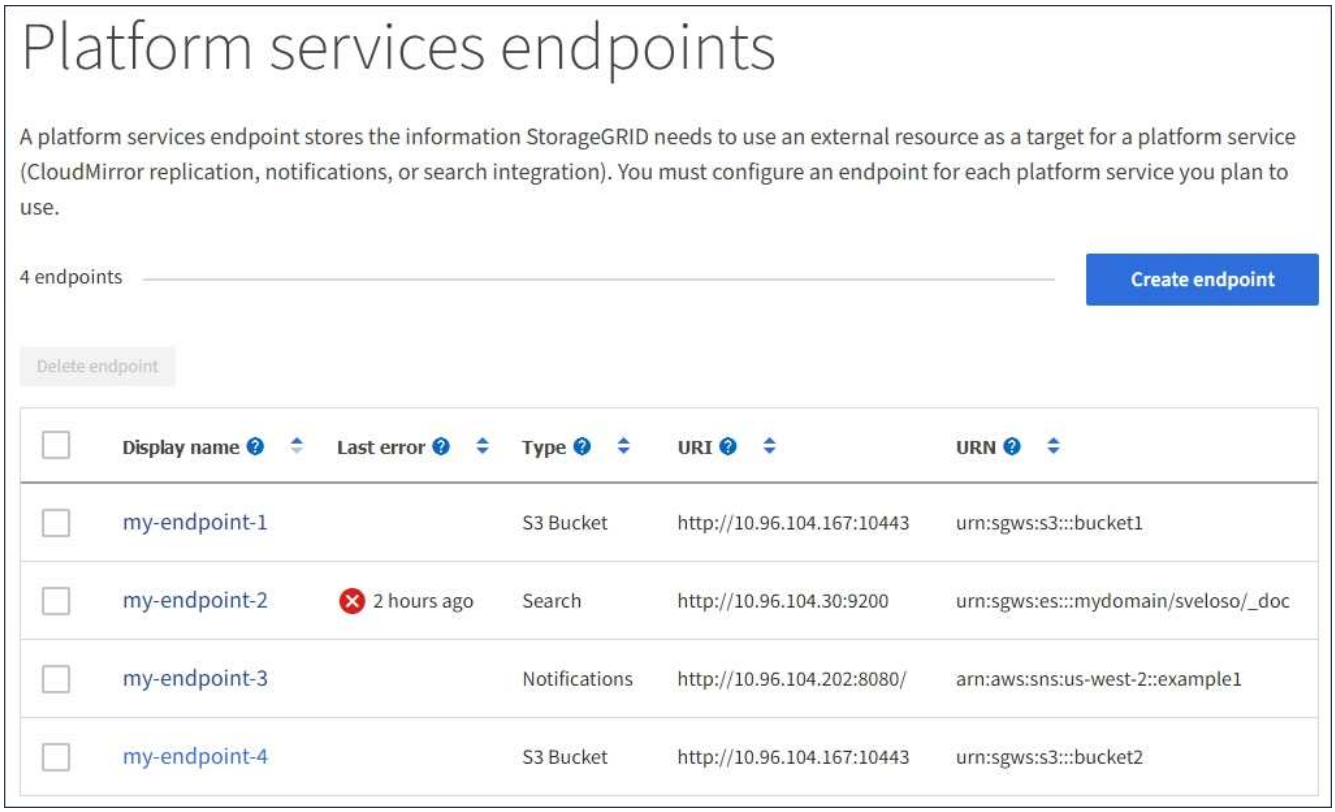
Ce dont vous avez besoin

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

Étapes

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

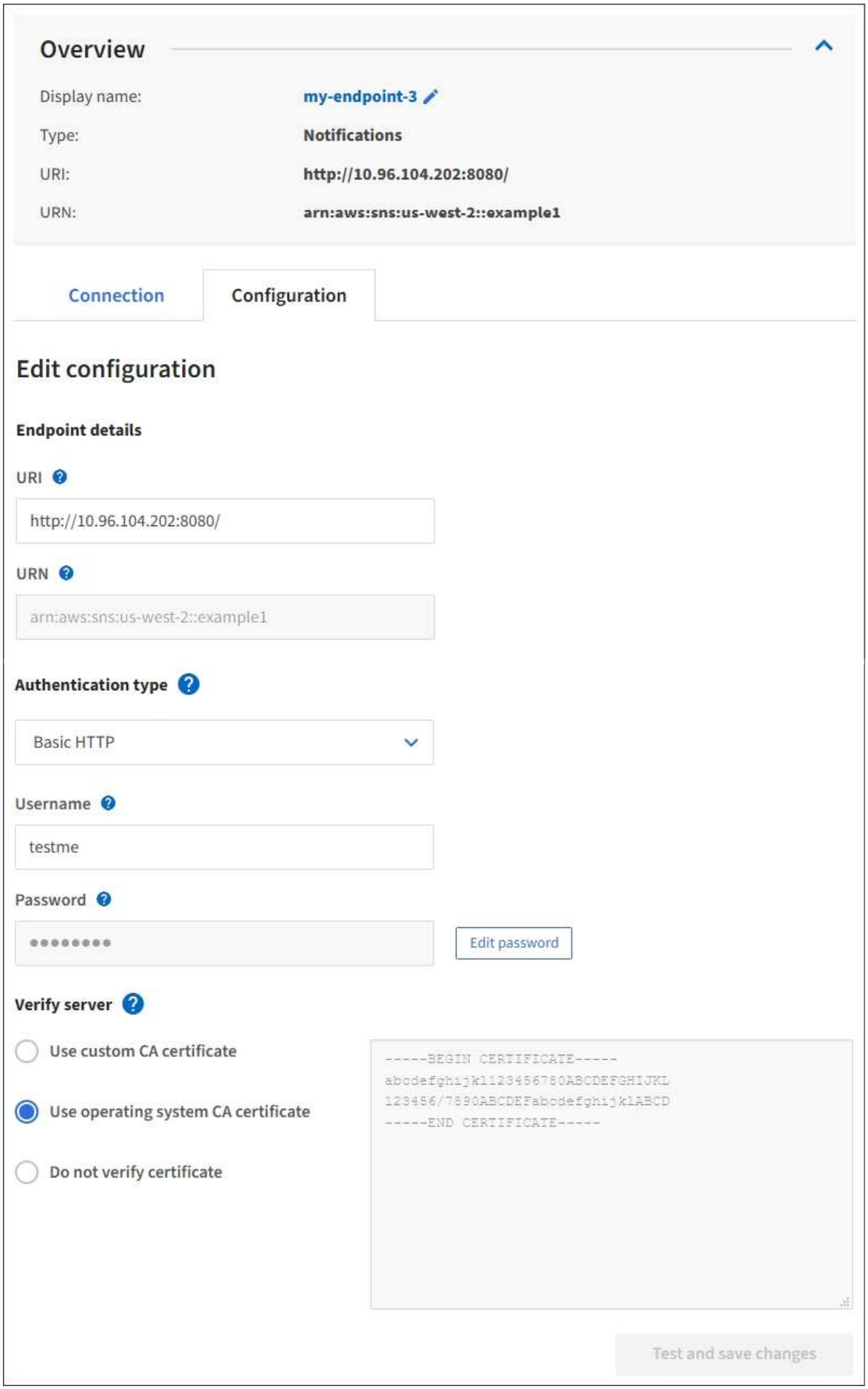
   La page noeuds finaux des services de plate-forme s'affiche et affiche la liste des noeuds finaux des services de plate-forme déjà configurés.



2. Sélectionnez le point final que vous souhaitez modifier.

   La page des détails du point final s'affiche.

3. Sélectionnez **Configuration**.


Overview
Display name:
my-endpoint-3
Type:
Notifications
URI:
http://10.96.104.202:8080/
URN:
arn:aws:sns:us-west-2::example1
Connection
Configuration
Edit configuration
Endpoint details
URI
http://10.96.104.202:8080/
URN
arn:aws:sns:us-west-2::example1
Authentication type
Basic HTTP
Username
testme
Password
Edit password
Verify server
Use custom CA certificate
Use operating system CA certificate
Do not verify certificate
-----BEGIN CERTIFICATE-----
abcdefghijkl123456780ABCDEFGHIJKL
123456/7890ABCDEFabcdefghijklABCD
-----END CERTIFICATE-----
Test and save changes

4. Modifiez la configuration du noeud final selon les besoins.

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

   a. Pour modifier le nom d'affichage du noeud final, sélectionnez l'icône d'édition .
   b. Modifiez l'URI si nécessaire.
   c. Si nécessaire, modifiez le type d'authentification.
      - Pour l'authentification HTTP de base, modifiez le nom d'utilisateur si nécessaire. Modifiez le mot de passe selon vos besoins en sélectionnant **Modifier le mot de passe** et en saisissant le nouveau mot de passe. Si vous devez annuler vos modifications, sélectionnez **Revert password edit**.
      - 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**.
   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**.

Informations associées

"Création d'un point final de services de plate-forme"

Suppression d'un noeud final de services de plate-forme

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

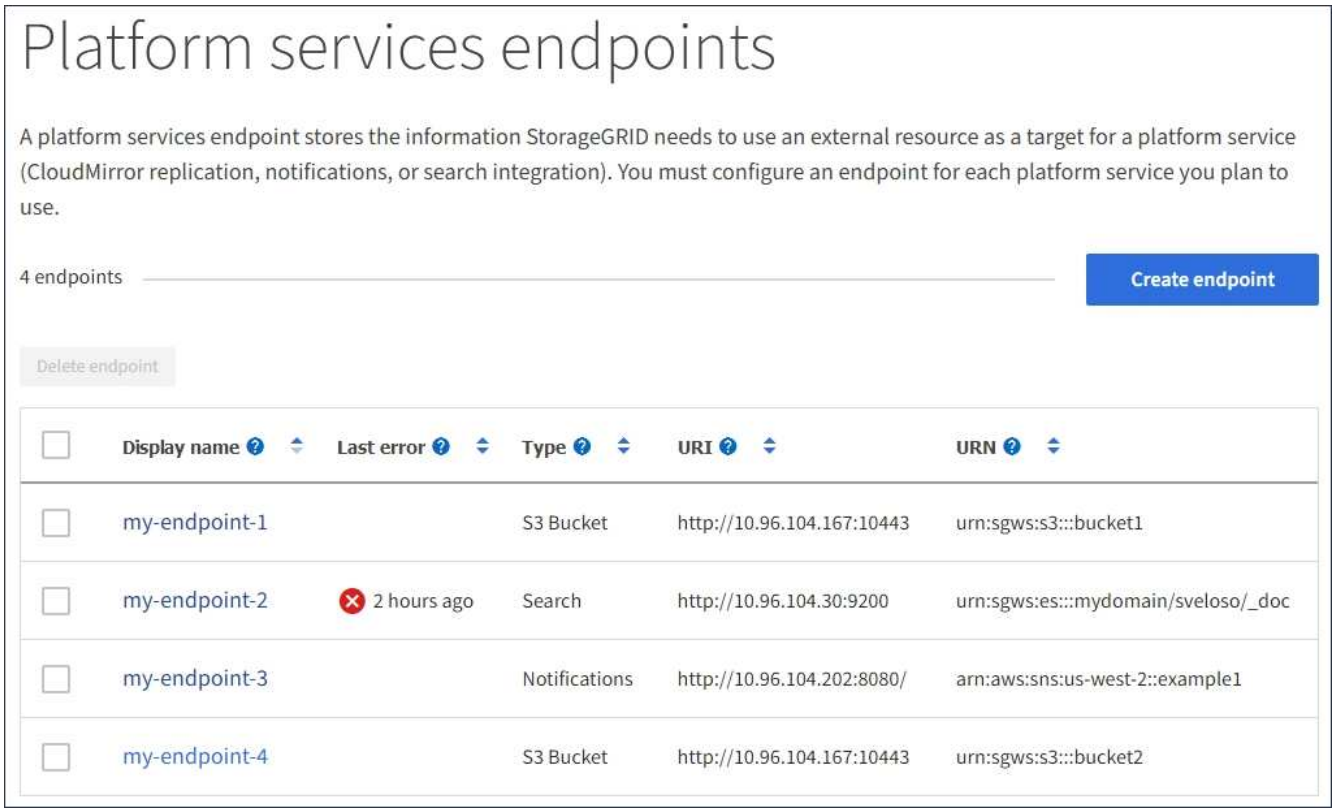
Ce dont vous avez besoin

- Vous devez être connecté au Gestionnaire de locataires à l'aide d'un navigateur pris en charge.
- Vous devez appartenir à un groupe d'utilisateurs qui dispose de l'autorisation **gérer les noeuds finaux** .

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.

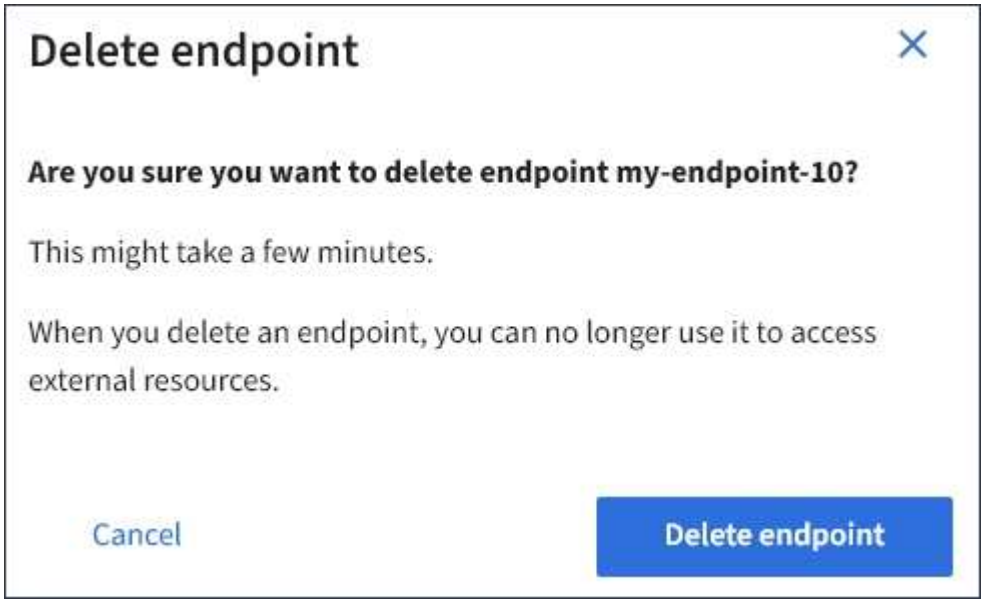


2. Cochez la case correspondant à chaque noeud final que vous souhaitez supprimer.

> 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.



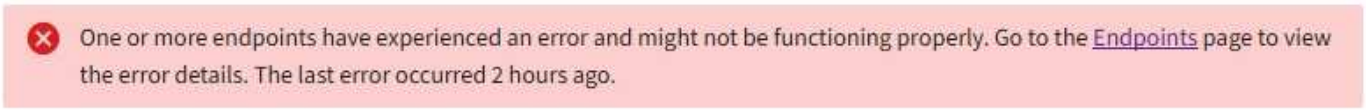
4. Sélectionnez **Supprimer le point final**.

Dépannage des erreurs de point final des services de plate-forme

En cas d'erreur lorsqu'StorageGRID tente de communiquer avec un point 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.

Déterminer si une erreur s'est produite

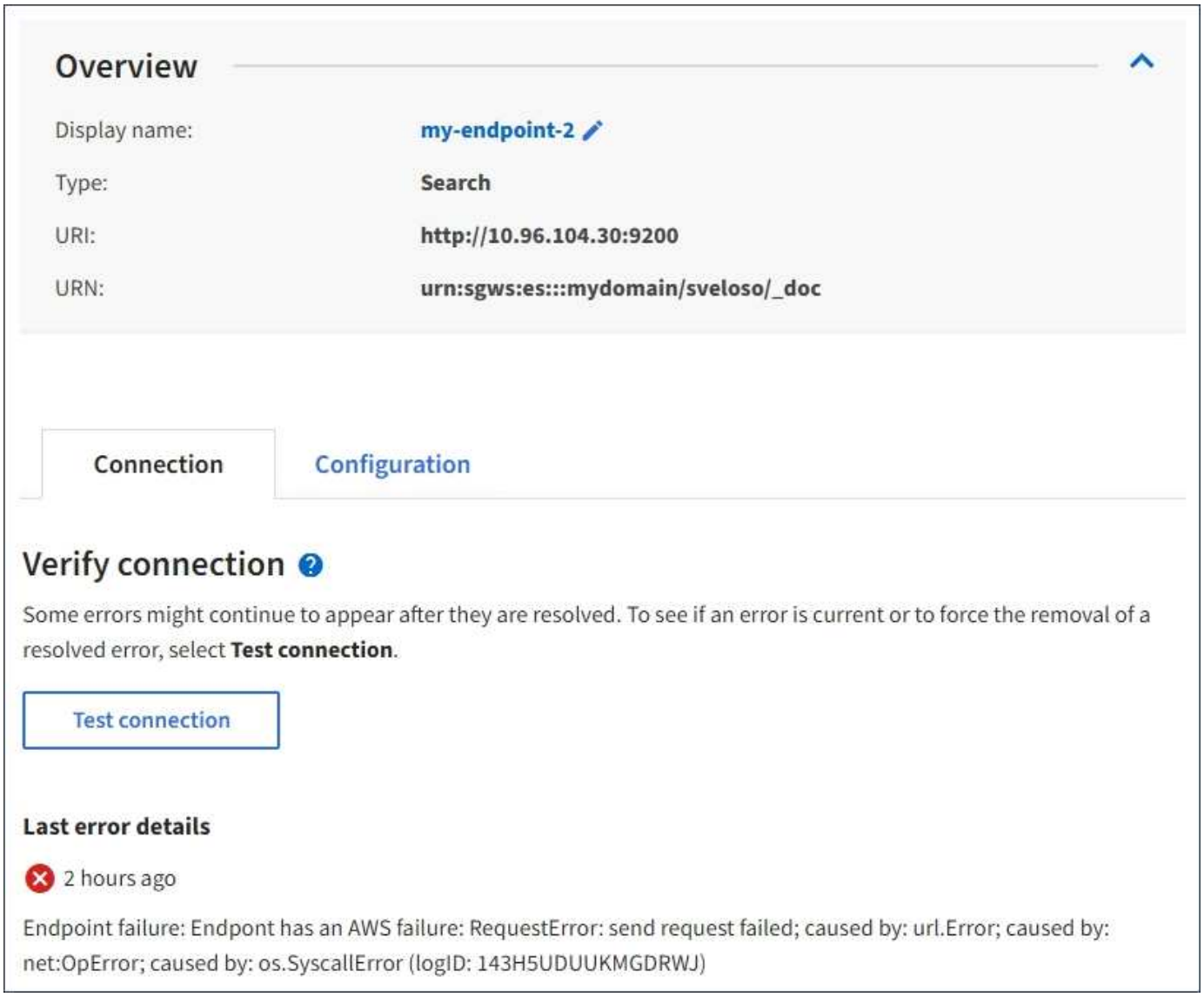
Si des erreurs de point de terminaison des services de plateforme se sont produites au cours des 7 derniers jours, le tableau de bord du gestionnaire des locataires affiche un message d'alerte. Vous pouvez accéder à la page noeuds finaux des services de plate-forme pour obtenir plus de détails sur l'erreur.



La même erreur qui s'affiche sur le tableau de bord s'affiche également en haut de la page noeuds finaux des services de plate-forme. 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. Erreurs incluant l'icône X rouge s'est produit au cours des 7 derniers jours.



Vérifier si une 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.

Résolution des 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 identifiants de point de terminaison ou l'accès de destination doivent être mis à jour", et les détails sont "AccessDenied" ou "InvalidAccessKeyId."".

Si vous devez modifier le noeud final pour résoudre une erreur : si vous sélectionnez **Test et enregistrer les modifications**, 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 (par exemple « 403 interdit »), vérifiez les autorisations associées aux identifiants du noeud final.

Dépannage des services de plateforme supplémentaires

Pour plus d'informations sur le dépannage des services de plate-forme, reportez-vous aux instructions d'administration de StorageGRID.

"Administrer StorageGRID"

Informations associées

"Création d'un point final de services de plate-forme"

"Test de la connexion pour un point final de services de plate-forme"

"Modification d'un noeud final de services de plate-forme"

Configuration de la réplication CloudMirror

Le service de réplication CloudMirror est l'un des trois services de plateforme StorageGRID. Vous pouvez utiliser la réplication CloudMirror pour répliquer automatiquement les objets dans un compartiment S3 externe.

Ce dont vous avez besoin

- Les services de plateforme doivent être activés pour votre compte de locataire par un administrateur StorageGRID.
- Vous devez avoir déjà créé un compartiment pour agir en tant que source de réplication.
- Le terminal que vous prévoyez d'utiliser comme destination pour la réplication CloudMirror doit déjà exister, et vous devez disposer de son URN.

- Vous devez appartenir à un groupe d'utilisateurs disposant de l'autorisation gérer toutes les rubriques ou accès racine, ce qui vous permet de gérer les paramètres de tous les compartiments S3 de votre compte locataire. 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 activer la réplication CloudMirror pour un compartiment, vous devez créer et appliquer un fichier XML de configuration de réplication de compartiment valide. Le XML de configuration de réplication 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.

Pour des informations générales sur la réplication des compartiments et sur la configuration de ce dernier, consultez la documentation Amazon sur la réplication inter-région (CRR). Pour plus d'informations sur la StorageGRID mise en œuvre de l'API de configuration de réplication des compartiments S3, reportez-vous aux instructions d'implémentation des applications client S3.

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 dans le compartiment ne le sont pas. 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 :

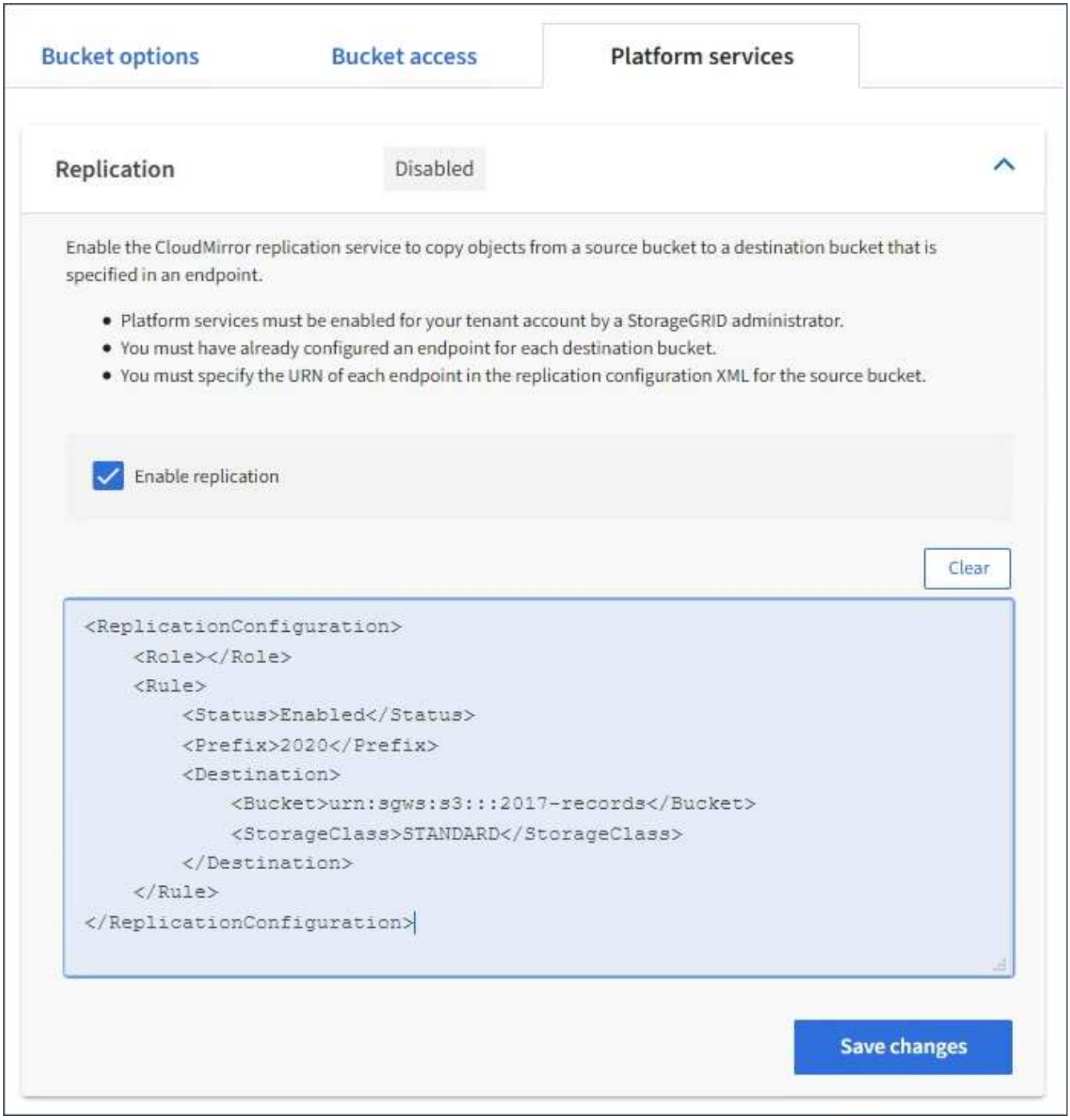
   - Notez que StorageGRID ne prend en charge que le V1 de la configuration de la réplication. Cela signifie que StorageGRID ne prend pas en charge l'utilisation de `Filter` Elément pour les règles, et suit les conventions V1 pour la suppression des versions d'objet. Pour plus d'informations, reportez-vous à la documentation Amazon sur la configuration de la réplication.
   - Utiliser l'URN d'un terminal du compartiment S3 comme destination.
   - Vous pouvez éventuellement ajouter le `<StorageClass>` et spécifiez l'un des éléments suivants :
     - `STANDARD`: La classe de stockage par défaut. Si vous ne spécifiez pas de classe de stockage lors du chargement d'un objet, le `STANDARD` la classe de stockage est utilisée.
     - `STANDARD_IA`: (Standard - accès peu fréquent.) Utilisez cette classe de stockage pour les données auxquelles vous accédez moins fréquemment, mais qui exige toujours un accès rapide lorsque cela est nécessaire.
     - `REDUCED_REDUNDANCY`: Utilisez cette classe de stockage pour les données non stratégiques reproductibles qui peuvent être stockées avec moins de redondance que le `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. 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** > **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

"Présentation du service de réplication CloudMirror"

"Utilisation de S3"

"Création d'un point final de services de plate-forme"

Configuration des notifications d'événements

Le service de notifications est l'un des trois services de plate-forme StorageGRID. Vous pouvez activer les notifications d'un compartiment pour envoyer des informations sur les événements spécifiés vers un service de destination qui prend en charge le service SNS (simple notification Service™) d'AWS.

Ce dont vous avez besoin

- Les services de plateforme doivent être activés pour votre compte de locataire par un administrateur StorageGRID.
- Vous devez avoir déjà créé un compartiment pour faire office de source de notifications.
- Le terminal que vous prévoyez d'utiliser comme destination pour les notifications d'événements doit déjà exister et vous devez disposer de son URN.
- Vous devez appartenir à un groupe d'utilisateurs disposant de l'autorisation gérer toutes les rubriques ou accès racine, ce qui vous permet de gérer les paramètres de tous les compartiments S3 de votre compte locataire. 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

Après avoir configuré les 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 SNS (simple notification Service) utilisée comme point final de destination. Pour activer les notifications pour un compartiment, vous devez créer et appliquer un XML de configuration de notification valide. Le XML de configuration de notification doit utiliser l'URN d'un terminal de notification d'événement pour chaque destination.

Pour obtenir des informations générales sur les notifications d'événements et leur configuration, consultez la documentation Amazon. Pour plus d'informations sur la façon dont StorageGRID implémente l'API de notification des compartiments S3, consultez les instructions pour l'implémentation des applications client S3.

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.

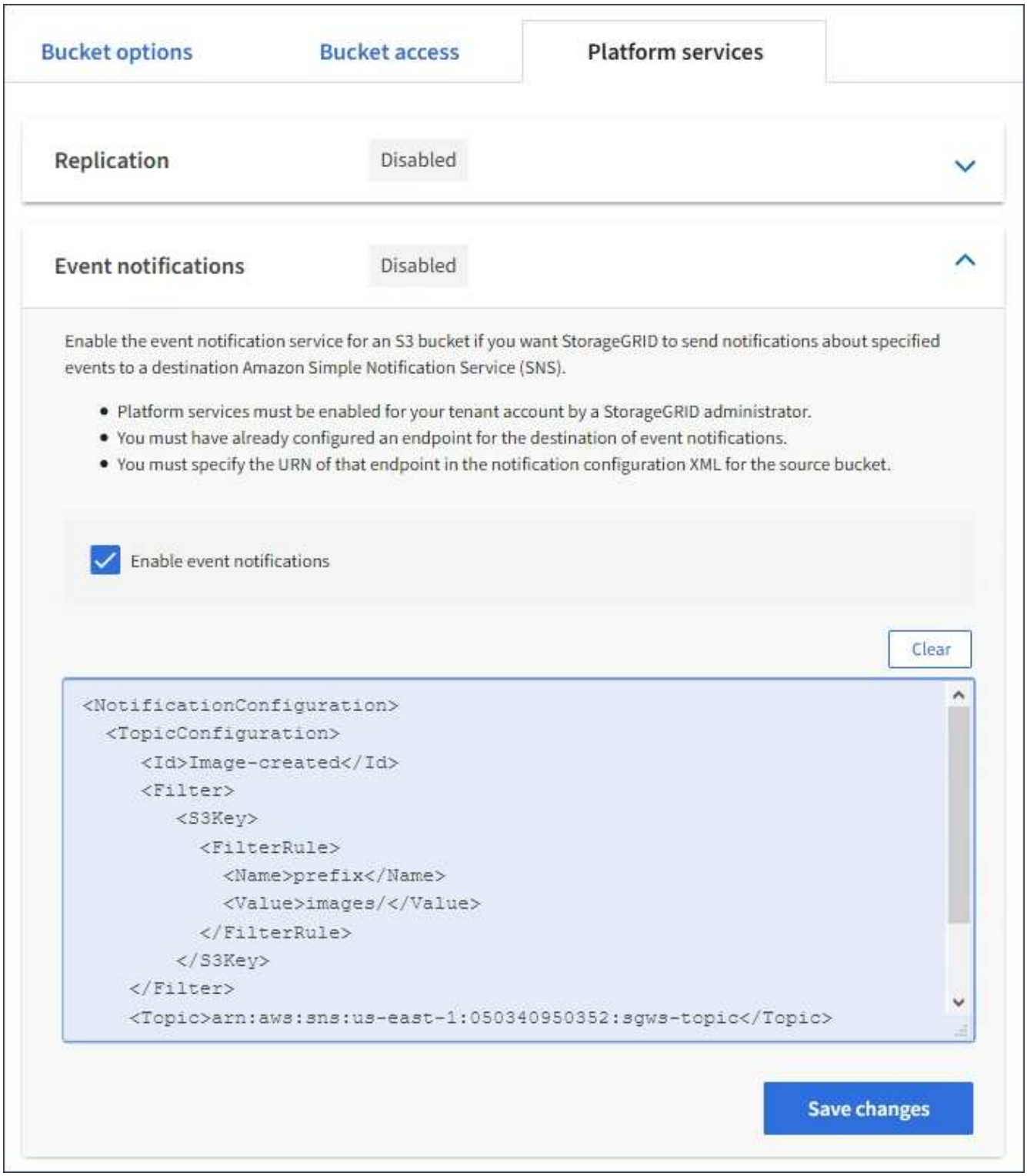
◦ Lors de la configuration du XML, utilisez l'URN d'un terminal de notification d'événements comme sujet de destination.

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

b. Confirmez qu'une notification a été envoyée à la rubrique SNS de destination.

Par exemple, si le sujet de votre destination est hébergé sur le service SNS (simple notification Service) d'AWS, vous pouvez configurer le service pour vous envoyer un e-mail une fois la notification envoyée.

```
{
   "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

"Présentation des notifications pour les compartiments"

"Utilisation de S3"

"Création d'un point final de services de plate-forme"

À l'aide du service d'intégration de recherche

Le service d'intégration de la recherche est l'un des trois services de plate-forme StorageGRID. Vous pouvez activer ce service pour envoyer des métadonnées d'objet à un index de recherche de destination chaque fois qu'un objet est créé ou supprimé, ou que ses métadonnées ou balises sont mises à jour.

Vous pouvez configurer l'intégration de la recherche à l'aide du Gestionnaire de locataires pour appliquer un code XML de configuration StorageGRID personnalisé à un compartiment.

> Comme le service d'intégration de recherche entraîne l'envoi des métadonnées d'objet vers une destination, son XML de configuration est appelé *metadata notification configuration XML*. Ce XML de configuration est différent de la configuration de *notification XML* utilisée pour activer les notifications d'événements.

Pour plus d'informations sur les opérations de l'API REST StorageGRID S3 personnalisées suivantes, reportez-vous aux instructions d'implémentation des applications client S3 :

- SUPPRIME la demande de configuration de notification des métadonnées de compartiment
- LIRE la demande de configuration de notification des métadonnées de compartiment
- PUT Bucket metadata notification configuration

Informations associées

"XML de configuration pour l'intégration de la recherche"

"Métadonnées d'objet incluses dans les notifications de métadonnées"

"JSON généré par le service d'intégration de la recherche"

"Configuration du service d'intégration de la recherche"

"Utilisation de S3"

XML de configuration pour l'intégration de la recherche

Le service d'intégration de recherche est configuré à l'aide d'un ensemble de règles contenues dans `<MetadataNotificationConfiguration>` et `</MetadataNotificationConfiguration>` balises. Chaque règle spécifie les objets auxquels la règle s'applique, et la destination vers laquelle StorageGRID doit envoyer les métadonnées de ces objets.

Les objets peuvent être filtrés sur le préfixe du nom de l'objet. Par exemple, vous pouvez envoyer les métadonnées pour les objets avec le préfixe `/images` à une destination et aux métadonnées pour les objets avec le préfixe `/videos` à un autre. Les configurations dont les préfixes se chevauchent ne sont pas valides et sont rejetées lors de leur envoi. 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 autorisé.

Les destinations doivent être spécifiées à l'aide de l'URN d'un terminal StorageGRID créé pour le service d'intégration de la recherche. Ces terminaux font référence à un index et à un type définis dans un cluster Elasticsearch.

```
<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.

Nom	Description	Obligatoire
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.
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.

Utilisez l'exemple de XML de configuration de notification de métadonnées pour apprendre à construire votre propre XML.

Configuration de notification des 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>
```

Configuration des notifications de métadonnées avec deux règles

Dans cet exemple, les métadonnées d'objet pour les objets qui correspondent au préfixe `/images` est envoyée à une destination, tandis que les métadonnées d'objet correspondent au préfixe `/videos` est envoyé 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>
```

Informations associées

"Utilisation de S3"

"JSON généré par le service d'intégration de la recherche"

"Configuration du service d'intégration de la recherche"

Configuration du service d'intégration de la recherche

Le service d'intégration de recherche envoie des métadonnées d'objet à un index de recherche de destination chaque fois qu'un objet est créé ou supprimé, ou que ses métadonnées ou balises sont mises à jour.

Ce dont vous avez besoin

- Les services de plateforme doivent être activés pour votre compte de locataire par un administrateur StorageGRID.
- Vous devez avoir déjà créé un compartiment S3 dont vous souhaitez indexer le contenu.
- Le terminal que vous prévoyez d'utiliser comme destination pour le service d'intégration de la recherche doit déjà exister et vous devez disposer de son URN.
- Vous devez appartenir à un groupe d'utilisateurs disposant de l'autorisation gérer toutes les rubriques ou accès racine, ce qui vous permet de gérer les paramètres de tous les compartiments S3 de votre compte locataire. 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. Vous devez mettre à jour ces objets existants pour vous assurer que leurs métadonnées sont ajoutées à l'index de recherche de destination.

Étapes

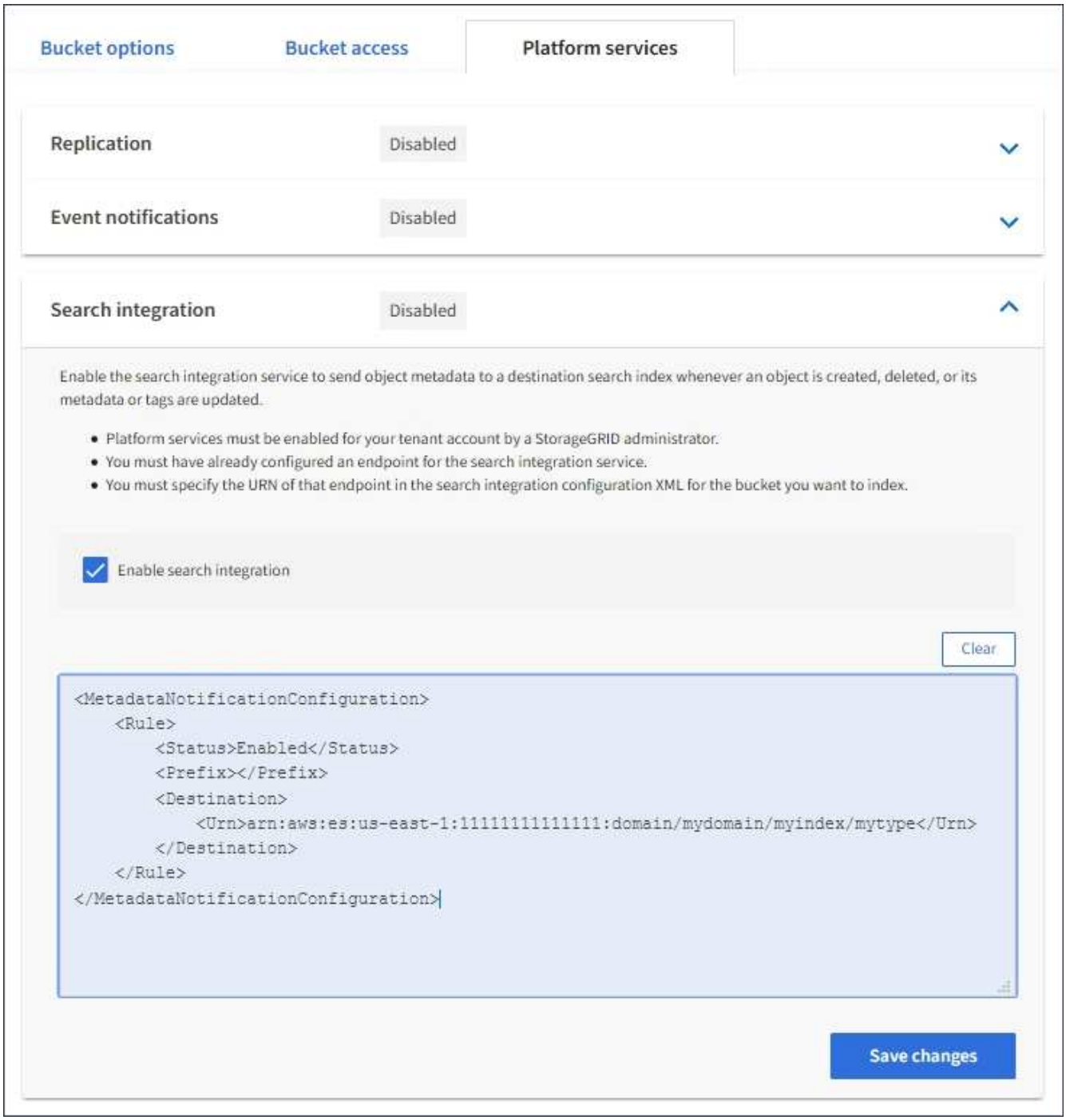
1. Utilisez un éditeur de texte pour créer le XML de notification de métadonnées requis pour activer l'intégration de la recherche.
   - Voir les informations sur le XML de configuration pour l'intégration de la recherche.
   - Lors de la configuration du XML, utilisez l'URN d'un noeud final d'intégration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

```
<MetadataNotificationConfiguration>
 <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
       <Urn>arn:aws:es:us-east-
1:11111111111111:domain/mydomain/myindex/mytype</Urn>
       </Destination>
 </Rule>
</MetadataNotificationConfiguration>
```

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 :

- Sélectionner **STORAGE (S3)** > **BAV** et désélectionner la case à cocher **Activer l'intégration de recherche**.
- 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.

Informations associées

"Présentation du service d'intégration de la recherche"

"XML de configuration pour l'intégration de la recherche"

"Utilisation de S3"

"Création d'un point final de services de plate-forme"

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 peut être généré lorsqu'un objet doté de la clé est associé `SGWS/Tagging.txt` est créé dans un compartiment nommé `test`. Le `test` le compartiment n'est pas multiversion `versionId` l'étiquette est 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 et description de l'élément
Informations sur les compartiments et les objets	`bucket`: Nom du compartiment
`key`: Nom de la clé d'objet	`versionID`: Version d'objet, pour les objets dans les compartiments multiversion
`region`: Région godet, 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`

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.

Utilisation de S3

Découvrez comment les applications client peuvent utiliser l'API S3 pour entrer en interface avec le système StorageGRID.

- "Prise en charge de l'API REST S3"
- "Configuration des comptes et des connexions des locataires"
- "Comment StorageGRID implémente l'API REST S3"
- "Opérations et limites prises en charge par l'API REST S3"
- "Opérations des API REST StorageGRID S3"
- "Règles d'accès au compartiment et au groupe"
- "Configuration de la sécurité pour l'API REST"
- "Surveillance et audit des opérations"
- "Avantages des connexions HTTP actives, inactives et simultanées"

Prise en charge de 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. Pour ce faire, des modifications mineures doivent être apportées à l'utilisation actuelle des appels de l'API REST S3 d'une application client.

- "Modifications apportées à la prise en charge de l'API REST S3"
- "Versions prises en charge"
- "La prise en charge des services de plateforme StorageGRID"

Modifications apportées à la prise en charge de l'API REST S3

Notez que des modifications ont été apportées à la prise en charge du système StorageGRID pour l'API REST S3.

Relâchez	Commentaires
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. • Le `Content-MD5` l'en-tête de 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 d'allocation de 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. • Ajout de la prise en charge des notifications de compartiment sur 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 et mise à jour de la liste des suites de chiffrement TLS prises en charge. • Le service CLB est obsolète.

Relâchez	Commentaires
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). • Ajout de la prise en charge des opérations DE SUPPRESSION, D'OBTENTION et DE REMPLACEMENT du cycle de vie des compartiments (action d'expiration uniquement) et pour le `x-amz-expiration` 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. • Liste mise à jour des suites de chiffrement TLS prises en charge. Les chiffrements TLS 1.1 ne sont plus pris en charge.
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 d'origine croisée (CORS), des connexions client HTTP pour S3 aux nœuds de grille et des paramètres de conformité aux 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 également de la prise en charge des contraintes d'emplacement de balisage d'objets pour les compartiments, ainsi que du paramètre de contrôle de 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.

Relâchez	Commentaires
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.

Versions prises en charge

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

Élément	Version
Spécification S3	*Simple Storage Service API Reference* 2006-03-01
HTTP	1.1 Pour plus d'informations sur HTTP, consultez le document HTTP/1.1 (RFC 7230-35). **Remarque**: StorageGRID ne prend pas en charge HTTP/1.1 pipeline.

Informations associées

"IETF RFC 2616 : Protocole de transfert hypertexte (HTTP/1.1)"

"Documentation Amazon Web Services (AWS) : référence de l'API Amazon simple Storage Service"

La prise en charge des services de plateforme StorageGRID

La plateforme StorageGRID permet aux comptes locataires d'StorageGRID d'utiliser des services tels qu'un compartiment S3 distant, un point de terminaison SNS (simple notification Service) ou un cluster Elasticsearch afin d'élargir les services fournis par un grid.

Le tableau suivant récapitule les services de plateforme disponibles et les API S3 utilisés pour les configurer.

Service de plateforme	Objectif	API S3 utilisée pour configurer le service
Réplication CloudMirror	Réplique les objets à partir d'un compartiment StorageGRID source vers le compartiment S3 distant configuré.	RÉPLICATION des compartiments
Notifications	Envoie des notifications sur les événements d'un compartiment StorageGRID source vers un point de terminaison SNS (simple notification Service) configuré.	PUT Bucket notification
Intégration de la recherche	Envoie les métadonnées d'objet des objets stockés dans un compartiment StorageGRID vers un index Elasticsearch configuré.	PUT Bucket metadata notification **Remarque :** il s'agit d'une API S3 personnalisée StorageGRID.

L'administrateur du grid doit activer les services de plateforme pour un compte de locataire avant de pouvoir les utiliser. Ensuite, un administrateur de tenant doit créer un noeud final qui représente le service distant dans le compte de tenant. Cette étape est requise avant la configuration d'un service.

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

Avant d'utiliser les services de plateforme, vous devez connaître les recommandations suivantes :

- NetApp recommande de ne pas autoriser plus de 100 locataires actifs avec les demandes S3 nécessitant la réplication CloudMirror, les notifications et l'intégration de la recherche. Avec plus de 100 locataires actifs, les performances des clients S3 sont plus lentes.
- Si un compartiment S3 est activé pour la gestion des versions et la réplication CloudMirror, NetApp recommande au terminal de destination d'activer le contrôle des versions du compartiment S3. Cela permet à la réplication CloudMirror de générer des versions d'objet similaires sur le noeud final.
- La réplication CloudMirror n'est pas prise en charge si le compartiment source est activé pour le verrouillage objet S3.
- La réplication CloudMirror échoue avec une erreur AccessDenied si la conformité héritée du compartiment de destination est activée.

Informations associées

"Utilisez un compte de locataire"

"Administrer StorageGRID"

"Opérations sur les compartiments"

"PUT Bucket metadata notification configuration"

Configuration des comptes et des connexions des locataires

Pour configurer StorageGRID pour accepter les connexions à partir des applications client, vous devez créer un ou plusieurs comptes de tenant et configurer les connexions.

Création et configuration des comptes de locataire S3

Un compte de locataire S3 est requis avant que les clients d'API S3 ne puissent stocker et récupérer des objets sur StorageGRID. Chaque compte de locataire possède son propre ID de compte, groupes et utilisateurs, ainsi que des conteneurs et des objets.

Les comptes de locataires S3 sont créés par un administrateur grid StorageGRID à l'aide de Grid Manager ou de l'API de gestion du grid. Lors de la création d'un compte de locataire S3, l'administrateur du grid spécifie les informations suivantes :

- Nom d'affichage du locataire (l'ID de compte du locataire est attribué automatiquement et ne peut pas être modifié).
- Indique si le compte locataire est autorisé à utiliser des services de plateforme. Si l'utilisation des services de plateforme est autorisée, la grille doit être configurée pour prendre en charge leur utilisation.
- Éventuellement, un quota de stockage pour le compte du locataire, soit le nombre maximal de gigaoctets, téraoctets ou pétaoctets disponibles pour les objets du locataire. Le quota de stockage d'un locataire représente une quantité logique (taille d'objet), et non une quantité physique (taille sur disque).
- Si la fédération des identités est activée pour le système StorageGRID, quel groupe fédéré a l'autorisation d'accès racine pour configurer le compte de tenant.
- Si l'authentification unique (SSO) n'est pas utilisée pour le système StorageGRID, que le compte de tenant utilise son propre référentiel d'identité ou partage le référentiel d'identité de la grille et le mot de passe initial de l'utilisateur racine local du locataire.

Une fois le compte de locataire S3 créé, les utilisateurs peuvent accéder au Gestionnaire des locataires pour effectuer les tâches suivantes :

- Configurez la fédération des identités (sauf si le référentiel d'identité est partagé avec la grille) et créez des groupes et des utilisateurs locaux
- Gestion des clés d'accès S3
- Créez et gérez des compartiments S3, notamment les compartiments où le verrouillage d'objet S3 est activé
- Utiliser les services de plate-forme (si activé)
- Contrôle de l'utilisation du stockage

> Les locataires S3 peuvent créer et gérer des compartiments S3 avec le Gestionnaire des locataires. Toutefois, ils doivent disposer de clés d'accès S3 et utiliser l'API REST S3 pour ingérer et gérer les objets.

Informations associées

"Administrer StorageGRID"

"Utilisez un compte de locataire"

Configuration des connexions client

Un administrateur du grid fait des choix de configuration qui affectent la façon dont les clients S3 se connectent à StorageGRID pour stocker et récupérer les données. Les informations spécifiques dont vous avez besoin pour établir une connexion dépendent de la configuration choisie.

Les applications client peuvent stocker ou récupérer des objets en se connectant à l'un des éléments suivants :

- Le service Load Balancer sur les nœuds d'administration ou de passerelle, ou, le cas échéant, l'adresse IP virtuelle d'un groupe de nœuds d'administration ou de nœuds de passerelle haute disponibilité
- Le service CLB sur les nœuds de passerelle ou, éventuellement, l'adresse IP virtuelle d'un groupe de nœuds de passerelle haute disponibilité

> Le service CLB est obsolète. Les clients configurés avant la version de StorageGRID 11.3 peuvent continuer à utiliser le service CLB sur les nœuds de passerelle. Toutes les autres applications client qui dépendent de StorageGRID pour fournir un équilibrage de la charge doivent se connecter à l'aide du service Load Balancer.

- Des nœuds de stockage, avec ou sans équilibreur de charge externe

Lors de la configuration de StorageGRID, un administrateur de la grille peut utiliser le gestionnaire de grille ou l'API de gestion de grille pour effectuer les étapes suivantes, qui sont toutes facultatives :

1. Configurez les noeuds finaux pour le service Load Balancer.

   Vous devez configurer les noeuds finaux pour utiliser le service Load Balancer. Le service Load Balancer sur les nœuds d'administration ou de passerelle distribue les connexions réseau entrantes des applications client aux nœuds de stockage. Lors de la création d'un terminal d'équilibrage de charge, l'administrateur StorageGRID spécifie un numéro de port, si le terminal accepte les connexions HTTP ou HTTPS, le type de client (S3 ou Swift) qui utilisera le terminal ainsi que le certificat à utiliser pour les connexions HTTPS (le cas échéant).

2. Configurer des réseaux clients non fiables.

   Si un administrateur StorageGRID configure le réseau client d'un nœud pour qu'il ne soit pas fiable, le nœud accepte uniquement les connexions entrantes sur le réseau client sur les ports explicitement configurés en tant que noeuds finaux d'équilibreur de charge.

3. Configurez les groupes haute disponibilité.

   Si l'administrateur crée un groupe haute disponibilité, les interfaces réseau de plusieurs nœuds d'administration ou nœuds de passerelle sont placées dans une configuration de sauvegarde active/active. Les connexions client sont établies à l'aide de l'adresse IP virtuelle du groupe haute disponibilité.

Pour plus d'informations sur chaque option, reportez-vous aux instructions d'administration de StorageGRID.

Informations associées

"Administrer StorageGRID"

Résumé : adresses IP et ports pour les connexions client

Les applications client se connectent à StorageGRID en utilisant l'adresse IP d'un nœud de grid et le numéro de port d'un service sur ce nœud. Si des groupes de haute disponibilité sont configurés, les applications client peuvent se connecter en utilisant l'adresse IP virtuelle du groupe de haute disponibilité.

Informations requises pour établir des connexions client

Le tableau récapitule les différentes façons dont les clients peuvent se connecter à StorageGRID ainsi que les adresses IP et les ports utilisés pour chaque type de connexion. Contactez votre administrateur StorageGRID pour en savoir plus ou consultez les instructions d'administration de StorageGRID pour obtenir une description de la recherche de ces informations dans le Gestionnaire de grille.

Là où la connexion est établie	Service auquel le client se connecte	Adresse IP	Port
Groupe HAUTE DISPONIBILITÉ	Équilibreur de charge	Adresse IP virtuelle d'un groupe haute disponibilité	• Port du terminal de l'équilibreur de charge
Groupe HAUTE DISPONIBILITÉ	CLB **Remarque :** le service CLB est obsolète.	Adresse IP virtuelle d'un groupe haute disponibilité	Ports S3 par défaut : • HTTPS: 8082 • HTTP : 8084
Nœud d'administration	Équilibreur de charge	Adresse IP du nœud d'administration	• Port du terminal de l'équilibreur de charge
Nœud de passerelle	Équilibreur de charge	Adresse IP du nœud de passerelle	• Port du terminal de l'équilibreur de charge
Nœud de passerelle	CLB **Remarque :** le service CLB est obsolète.	Adresse IP du nœud de passerelle **Remarque :** par défaut, les ports HTTP pour CLB et LDR ne sont pas activés.	Ports S3 par défaut : • HTTPS: 8082 • HTTP : 8084
Nœud de stockage	LDR	Adresse IP du nœud de stockage	Ports S3 par défaut : • HTTPS: 18082 • HTTP : 18084

Exemple

Pour connecter un client S3 au terminal Load Balancer d'un groupe HA de nœuds de passerelle, utilisez une URL structurée comme illustré ci-dessous :

- `https://VIP-of-HA-group:_LB-endpoint-port_`

Par exemple, si l'adresse IP virtuelle du groupe HA est 192.0.2.5 et le numéro de port d'un terminal S3 Load Balancer est 10443, un client S3 peut utiliser l'URL suivante pour vous connecter à StorageGRID :

- `https://192.0.2.5:10443`

Il est possible de configurer un nom DNS pour l'adresse IP que les clients utilisent pour se connecter à StorageGRID. Contactez votre administrateur réseau local.

Informations associées

"Administrer StorageGRID"

Choix d'utiliser des connexions HTTPS ou HTTP

Lorsque les connexions client sont effectuées à l'aide d'un noeud final Load Balancer, les connexions doivent être effectuées à l'aide du protocole (HTTP ou HTTPS) spécifié pour ce noeud final. Pour utiliser HTTP pour les connexions client aux nœuds de stockage ou au service CLB sur les nœuds de passerelle, vous devez activer son utilisation.

Par défaut, lorsque les applications client se connectent aux nœuds de stockage ou au service CLB sur les nœuds de passerelle, elles doivent utiliser le protocole HTTPS chiffré pour toutes les connexions. Vous pouvez également activer des connexions HTTP moins sécurisées en sélectionnant l'option de grille **Activer connexion HTTP** dans le Gestionnaire de grille. Par exemple, une application client peut utiliser HTTP lors du test de la connexion à un noeud de stockage dans un environnement non-production.

> Soyez prudent lorsque vous activez HTTP pour une grille de production car les demandes seront envoyées de manière non chiffrée.

> Le service CLB est obsolète.

Si l'option **Activer connexion HTTP** est sélectionnée, les clients doivent utiliser des ports HTTP différents de ceux qu'ils utilisent pour HTTPS. Voir les instructions d'administration de StorageGRID.

Informations associées

"Administrer StorageGRID"

"Avantages des connexions HTTP actives, inactives et simultanées"

Noms de domaine de terminaux pour les requêtes S3

Avant d'utiliser des noms de domaine S3 pour les demandes des clients, un administrateur StorageGRID doit configurer le système pour qu'il accepte les connexions qui utilisent les noms de domaine S3 dans les demandes de style d'accès S3 et de type hébergement virtuel S3.

Description de la tâche

Pour pouvoir utiliser des demandes de style hébergement virtuel S3, un administrateur grid doit effectuer les tâches suivantes :

- Utilisez le Gestionnaire de grille pour ajouter les noms de domaine de points de terminaison S3 au système StorageGRID.
- Vérifiez que le certificat utilisé par le client pour les connexions HTTPS à StorageGRID est signé pour tous les noms de domaine requis par le client.

  Par exemple, si le noeud final est `s3.company.com`, L'administrateur de la grille doit s'assurer que le certificat utilisé pour les connexions HTTPS inclut le `s3.company.com` Nom de l'alternative (SAN) de l'objet générique du noeud final et du noeud final : `*.s3.company.com`.

- Configurez le serveur DNS utilisé par le client pour inclure des enregistrements DNS qui correspondent aux noms de domaine de noeud final, y compris les enregistrements de caractères génériques requis.

Si le client se connecte à l'aide du service Load Balancer, le certificat que l'administrateur de la grille configure est le certificat du noeud final de l'équilibreur de charge utilisé par le client.

Chaque noeud final de l'équilibreur de charge possède son propre certificat et chaque noeud final peut être configuré pour reconnaître différents noms de domaine de point final.

Si le client connecte des nœuds de stockage ou au service CLB sur les nœuds de passerelle, le certificat que l'administrateur de la grille configure est le certificat de serveur personnalisé unique utilisé pour la grille.

Le service CLB est obsolète.

Pour plus d'informations, reportez-vous aux instructions d'administration de StorageGRID.

Une fois ces étapes terminées, vous pouvez utiliser des demandes de type hébergement virtuel (par exemple, `bucket.s3.company.com`).

Informations associées

"Administrer StorageGRID"

"Configuration de la sécurité pour l'API REST"

Test de la configuration de l'API REST S3

Vous pouvez utiliser l'interface de ligne de commande d'Amazon Web Services (AWS CLI) pour tester votre connexion au système et vérifier que vous pouvez lire et écrire des objets sur le système.

Ce dont vous avez besoin

- Vous devez avoir téléchargé et installé l'interface de ligne de commandes AWS depuis "aws.amazon.com/cli".
- Vous devez avoir créé un compte de locataire S3 dans le système StorageGRID.

Étapes

1. Configurez les paramètres Amazon Web Services pour utiliser le compte que vous avez créé dans le système StorageGRID :
   a. Passer en mode configuration : `aws configure`
   b. Entrez l'ID de clé d'accès AWS pour le compte que vous avez créé.
   c. Entrez la clé d'accès secret AWS 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.

   ```
   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
```

Comment StorageGRID implémente l'API REST S3

Une application client peut utiliser des appels d'API REST S3 pour se connecter à StorageGRID pour créer, supprimer et modifier des compartiments, ainsi que pour stocker et récupérer des objets.

- "Requêtes des clients en conflit"
- "Contrôles de cohérence"
- "Gestion des objets par les règles StorageGRID ILM"
- "Gestion des versions d'objet"
- "Recommandations pour l'implémentation de l'API REST S3"

Requêtes des clients en conflit

Les demandes contradictoires des clients, telles que deux clients qui écrivent sur la même clé, sont résolues sur la base des « derniers-victoires ».

Le calendrier de l'évaluation « derniers-victoires » est basé sur le moment où le système StorageGRID remplit une demande donnée et non sur le moment où les clients S3 commencent une opération.

Contrôles de cohérence

Les contrôles de cohérence assurent la reprise entre la disponibilité des objets et la cohérence de ces objets sur différents nœuds et sites de stockage, 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.

Pour effectuer des opérations d'objet à un niveau de cohérence différent, vous pouvez définir un contrôle de cohérence pour chaque compartiment ou pour chaque opération d'API.

Contrôles de cohérence

Le contrôle de cohérence affecte la façon dont les métadonnées utilisées par StorageGRID pour suivre les objets sont distribuées entre les nœuds, et donc la disponibilité des objets pour les requêtes client.

Vous pouvez définir le contrôle de cohérence pour une opération de compartiment ou API sur l'une des valeurs suivantes :

Contrôle de 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. Correspondance avec les garanties de cohérence Amazon S3. **Remarque :** si votre application utilise des demandes HEAD sur des objets qui n'existent pas, vous pouvez recevoir un nombre élevé de 500 erreurs de serveur interne si un ou plusieurs nœuds de stockage ne sont pas disponibles. Pour éviter ces erreurs, définissez le contrôle de cohérence sur « disponible », sauf si vous avez besoin de garanties de cohérence similaires à Amazon S3.

Contrôle de cohérence	Description
Disponible (cohérence possible pour les opérations DE TÊTE)	Se comporte de la même manière que le niveau de cohérence « entre la date et la nouvelle écriture », mais n'assure qu'une cohérence éventuelle pour les opérations DE TÊTE. Niveaux de disponibilité supérieurs à ceux de la « nouvelle écriture » en cas d'indisponibilité des nœuds de stockage Diffère des garanties de cohérence Amazon S3 pour les opérations HEAD uniquement.

Utilisation des contrôles de cohérence « en cas de nouvelle écriture » et « disponibles »

Lorsqu'une OPÉRATION EN TÊTE ou GET utilise le contrôle de cohérence « en cas de nouvelle écriture » ou QU'une opération GET utilise le contrôle de cohérence « disponible », 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 au niveau de cohérence suivant jusqu'à ce qu'elle atteigne le niveau de cohérence le plus élevé, « tous », qui nécessite la disponibilité de toutes les copies des métadonnées de l'objet.

Si une OPÉRATION HEAD ou GET utilise le contrôle de cohérence « read-after-New-write » mais que l'objet n'existe pas, la recherche d'objet atteint toujours le niveau de cohérence « All ». Comme ce niveau de cohérence requiert la disponibilité de toutes les copies des métadonnées de l'objet, vous pouvez recevoir un nombre élevé de 500 erreurs de serveur interne si un ou plusieurs nœuds de stockage sont indisponibles.

Sauf si vous avez besoin de garanties de cohérence similaires à Amazon S3, vous pouvez empêcher ces erreurs pour les opérations HEAD en définissant le contrôle de cohérence sur « disponible ». Lorsqu'une opération DE TÊTE utilise le contrôle de cohérence « disponible », StorageGRID n'offre qu'une cohérence éventuelle. Il ne réessaie pas l'échec d'une opération tant qu'elle n'atteint pas le niveau de cohérence « tous ». Il n'est donc pas nécessaire que toutes les copies des métadonnées de l'objet soient disponibles.

Spécification du contrôle de cohérence pour une opération d'API

Pour définir le contrôle de cohérence pour une opération API individuelle, les contrôles de cohérence doivent être pris en charge pour l'opération, et vous devez spécifier le contrôle de cohérence dans l'en-tête de la demande. Cet exemple définit le contrôle de cohérence sur "site de segmentation" pour une opération D'OBTENTION d'objet.

```
GET /bucket/object HTTP/1.1
Date: date
Authorization: <em>authorization name</em>
Host: <em>host</em>
Consistency-Control: strong-site
```

> Vous devez utiliser le même contrôle de cohérence pour les opérations PLACER l'objet et OBTENIR l'objet.

Spécification du contrôle de cohérence pour un compartiment

Pour définir le contrôle de cohérence du compartiment, vous pouvez utiliser la demande de cohérence StorageGRID PUT bucket et la demande DE cohérence GET bucket. Vous pouvez également utiliser le Gestionnaire de locataires ou l'API de gestion des locataires.

Lors du réglage des commandes de cohérence pour un godet, tenez compte des éléments suivants :

- La configuration du contrôle de cohérence d'un compartiment détermine quel contrôle de cohérence est utilisé pour les opérations S3 effectuées sur les objets dans le compartiment ou sur la configuration du compartiment. Cela n'affecte pas les opérations du compartiment lui-même.
- Le contrôle de cohérence d'une opération API individuelle remplace le contrôle de cohérence du compartiment.
- En général, les compartiments doivent utiliser le contrôle de cohérence par défaut, « en cas d'écriture ultérieure ». Si les demandes ne fonctionnent pas correctement, modifiez le comportement du client de l'application si possible. Ou configurez le client afin de spécifier le contrôle de cohérence pour chaque requête d'API. Réglez le contrôle de cohérence au niveau du godet uniquement en dernier recours.

Interaction des contrôles de cohérence et des règles ILM pour la protection des données

Le contrôle de cohérence et la règle ILM de votre choix affectent la protection des objets. Ces paramètres peuvent interagir.

Par exemple, le contrôle de cohérence utilisé 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. Étant donné que StorageGRID nécessite l'accès aux métadonnées d'un objet et à ses données pour répondre aux demandes client, la sélection de niveaux de protection correspondant au niveau de cohérence et au comportement d'ingestion permet d'améliorer la protection des données initiale et de mieux prévoir les réponses du système.

Les comportements d'ingestion suivants sont disponibles pour les règles ILM :

- **Strict** : toutes les copies spécifiées dans la règle ILM doivent être effectuées avant que le succès ne soit renvoyé au client.
- **Équilibré**: StorageGRID tente de faire toutes les copies spécifiées dans la règle ILM à l'entrée; si ce n'est pas possible, des copies intermédiaires sont faites et le succès est renvoyé au client. Les copies spécifiées dans la règle ILM sont effectuées lorsque cela est possible.
- **Double commit**: StorageGRID effectue immédiatement des copies intermédiaires de l'objet et retourne le succès au client. Les copies spécifiées dans la règle ILM sont effectuées lorsque cela est possible.

> Avant de sélectionner le comportement d'entrée d'une règle ILM, lisez la description complète de ces paramètres dans les instructions de gestion des objets avec la gestion du cycle de vie des informations.

Exemple d'interaction du contrôle de cohérence et de la règle ILM

Supposons que vous disposez d'une grille à deux sites avec la règle ILM suivante et le paramètre de niveau de cohérence suivant :

- **Règle ILM** : créez deux copies d'objet, une sur le site local et une sur un site distant. Le comportement d'entrée strict est sélectionné.
- **Niveau de cohérence**: "Sept-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 utilisez à la place la même règle ILM et le niveau de cohérence « sept-site », le client peut recevoir un message de réussite après la réplication des données d'objet sur le site distant, mais avant que les métadonnées d'objet ne soient distribuées sur ce site. 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. L'objet ne peut pas être récupéré.

L'interdépendance entre les niveaux de cohérence et les règles ILM peut être complexe. Contactez NetApp si vous avez besoin d'aide.

Informations associées

"Gestion des objets avec ILM"

"DEMANDE de cohérence des compartiments"

"PUT Bucket Consistency demandée"

Gestion des objets par les règles StorageGRID ILM

L'administrateur du grid crée des règles de gestion du cycle de vie des informations pour gérer les données d'objet ingérées sur le système StorageGRID à partir des applications client de l'API REST S3. Ces règles sont ensuite ajoutées à la règle ILM pour déterminer la façon dont et l'emplacement de stockage des données d'objet au fil du temps.

Les paramètres ILM déterminent les aspects suivants d'un objet :

- **Géographie**

  L'emplacement des données d'un objet, dans le système StorageGRID (pool de stockage) ou dans un pool de stockage cloud.

- **Grade de stockage**

  Type de stockage utilisé pour stocker les données d'objet : par exemple, Flash ou disque rotatif.

- * Protection contre les pertes*

  Le nombre de copies effectuées et les types de copies créées : réplication, code d'effacement, ou les deux.

- * Rétention*

  Évolution au fil du temps de la gestion des données d'un objet, de leur emplacement de stockage et de leur protection contre la perte.

- * Protection pendant l'ingestion*

  Méthode de protection des données d'objet lors de l'ingestion : placement synchrone (avec options

équilibrées ou strictes pour le comportement d'ingestion) ou copies intermédiaires (avec l'option de double validation).

Les règles ILM peuvent filtrer et sélectionner des objets. Pour les objets ingérées à l'aide du protocole S3, les règles ILM peuvent filtrer les objets en fonction des métadonnées suivantes :

- Compte de locataire
- Nom du compartiment
- Temps d'ingestion
- Clé
- Heure du dernier accès

> Par défaut, les mises à jour de l'heure du dernier accès sont désactivées pour tous les compartiments S3. Si votre système StorageGRID inclut une règle ILM utilisant l'option heure du dernier accès, vous devez activer les mises à jour de l'heure du dernier accès pour les compartiments S3 spécifiés dans cette règle. Vous pouvez activer les dernières mises à jour des temps d'accès à l'aide de la demande D'heure du dernier accès AU compartiment, de la case à cocher **S3 > seaux > configurer le dernier accès** dans le Gestionnaire de locataires ou à l'aide de l'API de gestion des locataires. Lors de l'activation des mises à jour du dernier accès, notez que les performances du StorageGRID peuvent être réduites, notamment dans les systèmes dotés d'objets de petite taille.

- Contrainte d'emplacement
- Taille de l'objet
- Métadonnées utilisateur
- Balise d'objet

Pour plus d'informations sur ILM, reportez-vous aux instructions de gestion des objets avec des informations relatives à la gestion du cycle de vie.

Informations associées

"Utilisez un compte de locataire"

"Gestion des objets avec ILM"

"DEMANDE de temps de dernier accès au compartiment"

Gestion des versions d'objet

Vous pouvez utiliser la gestion des versions pour conserver plusieurs versions d'un objet, ce qui vous protège contre la suppression accidentelle d'objets et vous permet d'extraire et de restaurer les 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 1,000 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 activer explicitement la gestion des versions pour chaque compartiment pour activer cette fonctionnalité. Chaque objet du

compartiment est associé à un ID de version, 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 des compartiments activés pour la gestion des versions, la prise en charge du contrôle de version vous permet de créer des règles ILM qui utilisent l'heure actuelle non sélectionnée comme heure de référence. Lorsqu'un objet est mis à jour, ses versions précédentes deviennent non actuelles. L'utilisation d'un filtre de temps non actuel vous permet de créer des règles qui réduisent l'impact sur le stockage des versions précédentes d'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.

Pour obtenir des informations sur la gestion du cycle de vie des objets avec la gestion du cycle de vie des informations, consultez les instructions de gestion des objets avec version S3.

Informations associées

"Gestion des objets avec ILM"

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 sur un chemin où vous ne vous attendez pas à ce que l'objet existe réellement, vous devez utiliser le contrôle de cohérence « disponible ». Par exemple, vous devez utiliser le contrôle de cohérence « disponible » si votre application dirige un emplacement avant DE LE PLACER.

Sinon, si l'opération HEAD ne trouve pas l'objet, vous pouvez recevoir un nombre élevé de 500 erreurs de serveur interne si un ou plusieurs nœuds de stockage ne sont pas disponibles.

Vous pouvez définir le contrôle de cohérence « disponible » pour chaque compartiment à l'aide de la demande DE cohérence PUT bucket, ou spécifier le contrôle de cohérence dans l'en-tête de demande pour une opération API individuelle.

Recommandations pour les clés d'objet

Pour les compartiments créés dans StorageGRID 11.4 ou version ultérieure, il n'est plus nécessaire de limiter les noms de clés d'objet afin de respecter les meilleures pratiques en matière de performances. Par exemple, vous pouvez maintenant utiliser des valeurs aléatoires pour les quatre premiers caractères des noms de clés d'objet.

Pour les compartiments créés dans les versions antérieures à StorageGRID 11.4, suivez les recommandations suivantes pour les noms de clés d'objet :

- Vous ne devez pas utiliser de valeurs aléatoires comme les quatre premiers caractères des clés d'objet. Cela contraste avec l'ancienne recommandation AWS pour les préfixes de clés. Au lieu de cela, vous devez utiliser des préfixes non aléatoires et non uniques, tels que `image`.
- Si vous suivez l'ancienne recommandation AWS pour utiliser des caractères aléatoires et uniques dans les préfixes de clés, vous devez préfixer les clés d'objet avec 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
  ```

Recommandations pour « plages de lectures »

Si l'option **Compress emmagased Objects** est sélectionnée (**Configuration** > **Grid Options**), les applications clientes S3 doivent éviter d'effectuer des opérations GET Object qui indiquent une plage d'octets à renvoyer. Ces opérations de « lecture à plage » sont inefficaces, car StorageGRID doit décompresser efficacement les objets pour accéder aux octets demandés. LES opérations GET Object qui demandent une petite plage d'octets provenant d'un objet très volumineux sont particulièrement inefficaces. Par exemple, il est très 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.

Informations associées

"Contrôles de cohérence"

"PUT Bucket Consistency demandée"

"Administrer StorageGRID"

Opérations et limites prises en charge par 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.

- "Authentification des demandes"
- "Opérations sur le service"
- "Opérations sur les compartiments"
- "Opérations personnalisées dans les compartiments"
- "Opérations sur les objets"
- "Opérations pour les téléchargements partitionnés"
- "Réponses d'erreur"

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 le `x-amz-date` En-tête de votre demande, elle remplace toute valeur spécifiée dans l'en-tête de la demande de date. Lors de l'utilisation de la signature AWS version 4, le `x-amz-date` l'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 courants définis par *simple Storage Service API Reference*, 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 : • La valeur SHA256 n'est pas calculée pour le corps de la demande. La valeur soumise par l'utilisateur est acceptée sans validation, comme si la valeur `UNSIGNED-PAYLOAD` avait été prévu pour le `x-amz-content-sha256` en-tête.
jeton de sécurité x-amz	Non mis en œuvre. Retours `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

Informations associées

"Documentation Amazon Web Services (AWS) : référence de l'API Amazon simple Storage Service"

Authentification des 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 : le protocole HTTP `Authorization` en-tête et utilisation des paramètres de requête.

Utilisation de l'en-tête autorisation HTTP

Le HTTP `Authorization` L'en-tête est utilisé par toutes les opérations de l'API S3 à l'exception des demandes anonymes lorsque la stratégie de compartiment l'autorise. Le `Authorization` en-tête contient toutes les informations de signature requises pour authentifier une demande.

Utilisation des 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 disposant de 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 restreint à une ressource par des tiers.

Opérations sur le service

Le système StorageGRID prend en charge les opérations suivantes sur ce service.

Fonctionnement	Mise en place
ACCÉDER au service	Mise en œuvre avec tout le comportement de l'API REST Amazon S3.
DÉCOUVREZ l'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. Il s'agit d'une opération sur le service avec un chemin de / et un paramètre de requête personnalisé (`?x-ntap-sg-usage`) ajouté.

Fonctionnement	Mise en place
OPTIONS /	Les applications client peuvent émettre `OPTIONS /` 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.

Informations associées

"DEMANDE d'utilisation du stockage"

Opérations sur les compartiments

Le système StorageGRID prend en charge un maximum de 1,000 compartiments pour chaque compte de locataire S3.

Les restrictions de noms de compartiment sont respectées dans les restrictions de région standard AWS, mais vous devez les restreindre davantage aux conventions de nommage DNS afin de prendre en charge les demandes de type hébergement virtuel S3.

"Documentation Amazon Web Services (AWS) : restrictions et limites des compartiments"

"Noms de domaine de terminaux pour la requête S3"

Les opérations GET Bucket (List Objects) et GET compartiment versions prennent en charge les contrôles de cohérence StorageGRID.

Vous pouvez vérifier si les mises à jour de l'heure du dernier accès sont activées ou désactivées pour les compartiments individuels.

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
SUPPRIMER le compartiment	Mise en œuvre avec tout le comportement de l'API REST Amazon S3.
SUPPRIMER les godets	Cette opération supprime la configuration CORS pour le compartiment.
SUPPRIMER le chiffrement du compartiment	Cette opération supprime le chiffrement par défaut du compartiment. Les objets chiffrés existants restent chiffrés, mais tous les nouveaux objets ajoutés au compartiment ne sont pas chiffrés.
SUPPRIMER le cycle de vie du compartiment	Cette opération supprime la configuration du cycle de vie du compartiment.

Fonctionnement	Mise en place
SUPPRIMER la règle de compartiment	Cette opération supprime la règle attachée au compartiment.
SUPPRIMER la réplication du compartiment	Cette opération supprime la configuration de réplication attachée au compartiment.
SUPPRIMER le balisage du compartiment	Cette opération utilise le `tagging` sous-ressource pour supprimer toutes les balises d'un compartiment.
GET Bucket (List Objects), version 1 et version 2	Cette opération renvoie une partie ou la totalité (jusqu'à 1,000) des objets dans un godet. La classe de stockage pour les objets peut avoir l'une ou l'autre des deux valeurs, même si l'objet a été ingéré avec le `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 qui ont le même préfixe, la réponse peut inclure une partie `CommonPrefixes` ne contenant pas de clés.
OBTENIR l'acl du compartiment	Cette opération renvoie une réponse positive et l'ID, le DisplayName et l'autorisation du propriétaire du compartiment, indiquant que le propriétaire a un accès complet au compartiment.
OBTENIR les godets	Cette opération renvoie le `cors` configuration du compartiment.
CHIFFREMENT des compartiments	Cette opération renvoie la configuration de cryptage par défaut pour le compartiment.
OPTIMISEZ le cycle de vie des compartiments	Cette opération retourne la configuration du cycle de vie du godet.
ACCÉDER à l'emplacement du compartiment	Cette opération renvoie la région définie à l'aide de `LocationConstraint` Élément dans la demande PUT Bucket. Si la région du godet est de `us-east-1`, une chaîne vide est renvoyée pour la région.

Fonctionnement	Mise en place
GET Bucket notification	Cette opération renvoie la configuration de notification attachée au compartiment.
OBTENIR les versions d'objet de compartiment	Avec accès EN LECTURE sur un godet, cette opération avec le `versions` sous-ressource répertorie les métadonnées de toutes les versions des objets dans le compartiment.
GET Bucket policy	Cette opération renvoie la politique attachée au godet.
RÉPLICATION des compartiments	Cette opération renvoie la configuration de réplication attachée au compartiment.
GET Bucket tagging	Cette opération utilise le `tagging` sous-ressource pour renvoyer toutes les balises d'un compartiment.
GESTION des versions des compartiments	Cette implémentation utilise le `versioning` sous-ressource pour retourner l'état de gestion des versions d'un compartiment. L'état de gestion des versions renvoyé indique si le compartiment est « non versionné » ou si le compartiment est de version « activé » ou « désactivé ».
OBTENIR la configuration de verrouillage d'objet	Cette opération détermine si le verrouillage d'objet S3 est activé pour un compartiment. "Utilisation du verrouillage d'objet S3"
Godet DE TÊTE	Cette opération détermine si un compartiment existe et que vous êtes autorisé à y accéder.

Fonctionnement	Mise en place
PLACER le godet	Cette opération crée un nouveau godet. 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 caractères et pas plus de 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 le `us-east-1` région ; cependant, vous pouvez utiliser le `LocationConstraint` élément de demande dans le corps de la demande pour spécifier une région différente. Lorsque vous utilisez le `LocationConstraint` Elément, 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 demande PUT Bucket utilise une région qui n'a pas été définie dans StorageGRID. • Vous pouvez inclure le `x-amz-bucket-object-lock-enabled` Demander l'en-tête pour créer un compartiment avec le verrouillage objet S3 activé. Vous devez activer le verrouillage d'objet S3 lors de la création du compartiment. Vous ne pouvez pas ajouter ou désactiver le verrouillage d'objet S3 après la création d'un compartiment. Le verrouillage objet S3 requiert la gestion des versions de compartiment, qui est activée automatiquement lors de la création du compartiment.

Fonctionnement	Mise en place
PLACEZ les godets	Cette opération définit la configuration du CORS pour un compartiment afin 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` le champ permet d'afficher les images de ce compartiment sur le site web `http://www.example.com`.
PUT Bucket Encryption	Cette opération définit l'état de cryptage 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 de cryptage côté serveur, définissez l' `SSEAlgorithm` paramètre à `AES256`, et n'utilisez pas le `KMSMasterKeyID` paramètre. La configuration de cryptage par défaut du compartiment est ignorée si la demande de téléchargement d'objet spécifie déjà le cryptage (c'est-à-dire, si la demande inclut le `x-amz-server-side-encryption-*` en-tête de demande).

Fonctionnement	Mise en place
CYCLE de vie des compartiments	Cette opération 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) • NonactuelVersionExp (Nontactut Days) • Filtre (préfixe, étiquette) • État • ID StorageGRID ne prend pas en charge les actions suivantes : • AbortIncompleMultipartUpload • ExpiredObjectDeleteMarker • Transition Pour comprendre comment l'action expiration dans un cycle de vie de compartiment interagit avec les instructions de placement ILM, reportez-vous à la section « fonctionnement de l'ILM tout au long de la vie d'un objet » dans les instructions de gestion des objets avec la gestion du cycle de vie des informations. **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

PUT Bucket notification	Cette opération configure les notifications pour le compartiment à l'aide du XML de configuration de notification inclus dans le corps de la demande. Vous devez connaître les détails d'implémentation suivants :
	
	• StorageGRID prend en charge les rubriques SNS (simple notification Service) comme destinations. Les terminaux SQS (simple Queue Service) ou Amazon Lambda 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, un `400 Bad Request` l'erreur est renvoyée avec le code `InvalidArgument`.
	
	• Vous ne pouvez pas configurer une 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 les autres, comme illustré dans la liste ci-dessous :
	• **EventSource**
	
	`sgws:s3`
	
	• **AwsRegion**
	
	non inclus
	
	• **x-amz-id-2**
	
	non inclus
	
	• **arn**
	
	`urn:sgws:s3:::bucket_name`

Fonctionnement	Mise en place
PUT Bucket policy	Cette opération définit la politique associée au compartiment.

Fonctionnement	Mise en place
RÉPLICATION des compartiments	Cette opération configure la réplication StorageGRID CloudMirror pour le compartiment à l'aide du 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` Elément pour les règles, et suit 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. • 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. 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`. • Il n'est pas nécessaire 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 le `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

Fonctionnement	Mise en place
PUT Bucket tagging	Cette opération utilise le `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
GESTION des versions du compartiment	Cette implémentation utilise le `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`.

Informations associées

"Documentation Amazon Web Services (AWS) : réplication entre régions"

"Contrôles de cohérence"

"DEMANDE DE dernier accès au compartiment"

"Règles d'accès au compartiment et au groupe"

"Utilisation du verrouillage d'objet S3"

"Opérations S3 suivies dans les journaux d'audit"

"Gestion des objets avec ILM"

"Utilisez un compte de locataire"

Création d'une configuration de 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 relative à la gestion du cycle de vie des objets dans le *Amazon simple Storage Service Developer Guide*. Notez que StorageGRID prend uniquement en charge les actions d'expiration, mais pas les actions de transition.

"Amazon simple Storage Service Developer Guide : gestion du cycle de vie des objets"

Qu'est-ce qu'une configuration de 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

Si vous appliquez une configuration de cycle de vie à un compartiment, les paramètres de cycle de vie du compartiment prévalent toujours sur les paramètres ILM de StorageGRID. StorageGRID utilise les paramètres d'expiration du compartiment et non ILM pour déterminer s'il faut supprimer ou conserver des objets spécifiques.

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, consultez la section « fonctionnement de ILM tout au long de la vie d'un objet » dans les instructions de gestion des objets avec la gestion du cycle de vie de l'information.

> 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 :

- SUPPRIMER le cycle de vie du compartiment
- OPTIMISEZ le cycle de vie des compartiments
- CYCLE de vie des compartiments

Création de la configuration du 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 un `key2` valeur de `tag2`. Le `Expiration` Le paramètre spécifie 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` le paramètre indique que les objets correspondant au filtre expirent 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 de correspondance expirera 50 jours après leur non-mise 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"
        }
    ]
}
```

Application d'une configuration de cycle de vie à un compartiment

Une fois que vous avez créé le fichier de configuration du cycle de vie, vous l'appliquez à un compartiment en émettant une demande DE cycle de vie PUT bucket.

Cette demande applique la configuration du cycle de vie dans le fichier exemple aux objets d'un compartiment nommé `testbucket`:godet

```
aws s3api --endpoint-url <StorageGRID endpoint> put-bucket-lifecycle-
configuration
--bucket testbucket --lifecycle-configuration file://bktjson.json
```

Pour vérifier qu'une configuration du cycle de vie a été appliquée avec succès au compartiment, émettez une demande GET Lifecycle. 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.

La validation de l'expiration du cycle de vie du compartiment s'applique à un 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 D'objet PUT, HEAD Object ou GET Object. Si une règle s'applique, la réponse comprend un `Expiration` paramètre qui indique quand l'objet expire et quelle règle d'expiration a été mise en correspondance.

> Le cycle de vie des compartiments ignore ILM, le `expiry-date` l'illustration représente la date réelle à laquelle l'objet sera supprimé. Pour plus de détails, reportez-vous à la section « détermination de la conservation des objets » dans les instructions d'administration de StorageGRID.

Par exemple, cette requête PUT Object a été émise le 22 juin 2020 et place un objet dans le `testbucket` godet.

```
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 demande d'objet TÊTE a été utilisée pour obtenir les métadonnées du même objet dans le compartiment test.

```
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": {}
}
```

Informations associées

"Opérations sur les compartiments"

"Gestion des objets avec ILM"

Opérations personnalisées dans les compartiments

Le système StorageGRID prend en charge les opérations de compartiment personnalisées, ajoutées à l'API REST S3 et propres au système.

Le tableau suivant répertorie les opérations de compartiment personnalisées prises en charge par StorageGRID.

Fonctionnement	Description	Pour en savoir plus
OPTIMISEZ la cohérence des compartiments	Renvoie le niveau de cohérence appliqué à un compartiment spécifique.	"DEMANDE de cohérence des compartiments"

Fonctionnement	Description	Pour en savoir plus
PRÉSERVER la cohérence du godet	Définit le niveau de cohérence appliqué à un compartiment spécifique.	"PUT Bucket Consistency demandée"
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.	"DEMANDE DE dernier accès au compartiment"
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.	"DEMANDE de temps de dernier accès au compartiment"
SUPPRIMEZ la configuration de notification des métadonnées de compartiment	Supprime le XML de configuration de notification de métadonnées associé à un compartiment spécifique.	"SUPPRIME la demande de configuration de notification des métadonnées de compartiment"
CONFIGURATION DES notifications de métadonnées de compartiment	Renvoie le XML de configuration de notification de métadonnées associé à un compartiment spécifique.	"LIRE la demande de configuration de notification des métadonnées de compartiment"
CONFIGURATION de notification des métadonnées de compartiment	Configure le service de notification des métadonnées pour un compartiment.	"PUT Bucket metadata notification configuration"
METTEZ les modifications du godet à des fins de conformité	Obsolète et non pris en charge : vous ne pouvez plus créer de compartiments avec conformité activée.	"Obsolète : METTEZ les modifications de la demande de compartiment à des fins de conformité"
ASSUREZ la conformité aux compartiments	Obsolète mais pris en charge : renvoie les paramètres de conformité actuellement en vigueur pour un compartiment compatible existant.	"Obsolète : RÉCUPÉRER la demande de conformité du compartiment"
METTEZ le godet en conformité	Obsolète mais pris en charge : permet de modifier les paramètres de conformité d'un compartiment compatible existant.	"Obsolète : PUT Bucket Compliance request"

Informations associées

"Opérations S3 suivies dans les journaux d'audit"

Opérations sur les objets

Cette section décrit la manière dont le système StorageGRID implémente les opérations de l'API REST S3 pour les objets.

- "Utilisation du verrouillage d'objet S3"
- "Utilisation du chiffrement côté serveur"
- "OBTENIR l'objet"
- "Objet TÊTE"
- "Restauration POST-objet"
- "PLACER l'objet"
- "PLACER l'objet - Copier"

Les conditions suivantes s'appliquent à toutes les opérations d'objet :

- Les contrôles de cohérence StorageGRID sont pris en charge par toutes les opérations sur les objets, à l'exception de ce qui suit :
  - OBTENIR l'ACL d'objet
  - `OPTIONS /`
  - METTRE l'objet en attente légale
  - CONSERVATION des objets
- Les demandes contradictoires des clients, telles que deux clients qui écrivent sur la même clé, sont résolues sur la base des « derniers-victoires ». Le moment de l'évaluation « derniers-victoires » est basé sur le moment où le système StorageGRID remplit une demande donnée et non sur le moment où 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 ingérées sur 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
SUPPRIMER l'objet	Authentification multifacteur (MFA) et en-tête de réponse `x-amz-mfa` ne sont pas pris en charge. Lors du traitement d'une requête DE SUPPRESSION d'objet, StorageGRID tente de supprimer immédiatement toutes les copies de l'objet des 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, si un emplacement est temporairement indisponible), StorageGRID met les copies en file d'attente pour suppression, puis indique que le client a réussi à les supprimer. **Gestion des versions** Pour supprimer une version spécifique, le demandeur doit être le propriétaire du compartiment et utiliser le `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 l' `versionId` sous-ressource sur un compartiment activé pour la version, il génère un marqueur de suppression. Le `versionId` pour le marqueur de suppression, est renvoyé à l'aide du `x-amz-version-id` en-tête de réponse, et le `x-amz-delete-marker` l'en-tête de réponse est renvoyé à `true`. • Si un objet est supprimé sans l' `versionId` sous-ressource sur un compartiment suspendu de version, elle entraîne la suppression permanente d'une version existante 'null' ou d'un marqueur de suppression 'null' et la génération d'un nouveau marqueur de suppression 'null'. Le `x-amz-delete-marker` l'en-tête de réponse est renvoyé à `true`. **Remarque** : dans certains cas, plusieurs marqueurs de suppression peuvent exister pour un objet.
SUPPRIMER plusieurs objets	Authentification multifacteur (MFA) et en-tête de réponse `x-amz-mfa` ne sont pas pris en charge. Plusieurs objets peuvent être supprimés dans le même message de demande.

Fonctionnement	Mise en place
SUPPRIMER le balisage d'objets	Utilise le `tagging` sous-ressource pour supprimer toutes les balises d'un objet. Mise en œuvre avec tout le comportement de l'API REST Amazon S3. **Gestion des versions** Si le `versionId` le paramètre query n'est pas spécifié dans la demande. 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, un état "methodNotAldue" est renvoyé avec l' `x-amz-delete-marker` réponse en-tête réglée sur `true`.
OBTENIR l'objet	"OBTENIR l'objet"
OBTENIR l'ACL d'objet	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.
OBTENIR la mise en attente légale de l'objet	"Utilisation du verrouillage d'objet S3"
OBTENIR la conservation des objets	"Utilisation du verrouillage d'objet S3"
OBTENIR le balisage d'objets	Utilise le `tagging` sous-ressource pour renvoyer toutes les balises d'un objet. Mise en œuvre avec tout le comportement de l'API REST Amazon S3 **Gestion des versions** Si le `versionId` le paramètre query n'est pas spécifié dans la demande, 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, un état "methodNotAldue" est renvoyé avec l' `x-amz-delete-marker` réponse en-tête réglée sur `true`.
Objet TÊTE	"Objet TÊTE"
Restauration POST-objet	"Restauration POST-objet"
PLACER l'objet	"PLACER l'objet"

Fonctionnement	Mise en place
PLACER l'objet - Copier	"PLACER l'objet - Copier"
METTRE l'objet en attente légale	"Utilisation du verrouillage d'objet S3"
CONSERVATION des objets	"Utilisation du verrouillage d'objet S3"
PUT Object tagging	Utilise le `tagging` sous-ressource pour ajouter un ensemble de balises à un objet existant. Mise en œuvre avec tout le comportement de l'API REST Amazon S3 **Mises à jour de balises et comportement d'entrée** Lorsque vous utilisez PUT Object tagging pour mettre à jour les balises d'un objet, StorageGRID ne réingérer 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. Cela signifie que si la règle ILM utilise l'option stricte pour le comportement d'ingestion, aucune action n'est effectuée si les placements d'objet requis ne peuvent pas être effectués (par exemple, car un nouvel emplacement requis 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 la base des « derniers-victoires ». Le moment de l'évaluation « derniers-victoires » est basé sur le moment où le système StorageGRID remplit une demande donnée et non sur le moment où les clients S3 commencent une opération. **Gestion des versions** Si le `versionId` le 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, un état "methodNotAldue" est renvoyé avec l' `x-amz-delete-marker` réponse en-tête réglée sur `true`.

Informations associées

"Contrôles de cohérence"

"Opérations S3 suivies dans les journaux d'audit"

Utilisation du verrouillage d'objet S3

Si le paramètre de verrouillage d'objet S3 global est activé pour votre système StorageGRID, vous pouvez créer des compartiments avec le verrouillage d'objet S3 activé, puis spécifier les paramètres de conservation à la date et de conservation légale pour chaque version d'objet que vous ajoutez à ce compartiment.

S3 Object Lock vous permet de spécifier des paramètres de niveau objet pour empêcher la suppression ou l'écrasement d'objets pendant une durée déterminée ou indéfiniment.

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

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. Vous pouvez utiliser l'une des méthodes suivantes :

- Créez le compartiment à l'aide du Gestionnaire des locataires.

  "Utilisez un compte de locataire"

- Créer le compartiment à l'aide d'une demande PUT bucket avec le `x-amz-bucket-object-lock_enabled` en-tête de demande.

  "Opérations sur les compartiments"

Une fois le compartiment créé, vous ne pouvez pas ajouter ou désactiver le verrouillage d'objet S3. Le verrouillage objet S3 requiert la gestion des versions de compartiment, qui est activée automatiquement lors de la création du compartiment.

Un compartiment avec l'option de verrouillage d'objet S3 activée peut contenir une combinaison d'objets avec et sans les paramètres de verrouillage d'objet S3. StorageGRID ne prend pas en charge la conservation par défaut des objets dans les compartiments de verrouillage d'objet S3. L'opération de compartiment DE configuration DE verrouillage d'objet N'est donc pas prise en charge.

Détermination de l'activation du verrouillage d'objet S3 pour un compartiment

Pour déterminer si le verrouillage d'objet S3 est activé, utilisez la demande OBTENIR la configuration du verrouillage d'objet.

"Opérations sur les compartiments"

Création d'un objet avec les paramètres de verrouillage d'objet S3

Pour spécifier les paramètres de verrouillage d'objet S3 lors de l'ajout d'une version d'objet dans un compartiment dont le verrouillage d'objet S3 est activé, exécutez un objet PUT, PLACER l'objet - copie ou lancez une demande de téléchargement de pièces multiples. Utiliser les en-têtes de demande suivants.

> Vous devez activer le verrouillage d'objet S3 lorsque vous créez un compartiment. Vous ne pouvez pas ajouter ou désactiver le verrouillage d'objet S3 après la création d'un compartiment.

- `x-amz-object-lock-mode`, Qui doit ÊTRE CONFORME (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 :

- Le `Content-MD5` l'en-tête de demande est requis le cas échéant `x-amz-object-lock-*` L'en-tête de la demande est présent dans la demande D'objet PUT. `Content-MD5` N'est pas nécessaire pour PLACER l'objet - Copier ou lancer le téléchargement de pièces multiples.
- Si le verrouillage d'objet S3 n'est pas activé dans le compartiment et qu'un `x-amz-object-lock-*` L'en-tête de la demande est présent, une erreur 400 Bad Request (InvalidRequest) est renvoyée.
- La requête PUT Object prend en charge l'utilisation de `x-amz-storage-class: REDUCED_REDUNDANCY` Pour correspondre au 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 DE la version D'objet GET ou HEAD inclura les en-têtes `x-amz-object-lock-mode`, `x-amz-object-lock-retain-until-date`, et `x-amz-object-lock-legal-hold`, si configuré et si l'expéditeur de la demande est correct `s3:Get*` autorisations.
- Une demande ultérieure DE SUPPRESSION de la version d'objet ou DE SUPPRESSION des versions d'objets échoue si elle est antérieure à la date de conservation ou si une mise en attente légale est activée.

Mise à jour des paramètres de verrouillage d'objet S3

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 :

- `PUT Object legal-hold`

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.

- `PUT Object retention`
  - La valeur du mode doit être CONFORME (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.

Informations associées

"Gestion des objets avec ILM"

"Utilisez un compte de locataire"

"PLACER l'objet"

"PLACER l'objet - Copier"

"Lancer le téléchargement de pièces multiples"

"Gestion des versions d'objet"

"Guide de l'utilisateur Amazon simple Storage Service : utilisation du verrouillage d'objets S3"

À l'aide du chiffrement 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.

Utilisation du 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 :

- PLACER l'objet
- PLACER l'objet - Copier
- Lancer le téléchargement de pièces multiples

Utilisation du 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 la barre de coupe doit être de `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 :

- OBTENIR l'objet
- Objet TÊTE
- PLACER l'objet
- PLACER l'objet - Copier
- Lancer le téléchargement de pièces multiples
- Télécharger la pièce
- Télécharger la pièce - Copier

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 en utilisant SSE-C. Pour des considérations de sécurité, vous devez envisager toute clé que vous envoyez accidentellement en utilisant http pour être 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 CloudMirror est configurée pour le compartiment, vous ne pouvez pas ingérer d'objets SSE-C. L'opération d'acquisition échoue.

Informations associées

"OBTENIR l'objet"

"Objet TÊTE"

"PLACER l'objet"

"PLACER l'objet - Copier"

"Lancer le téléchargement de pièces multiples"

"Télécharger la pièce"

"Télécharger la pièce - Copier"

"Guide pour les développeurs Amazon S3 : protection des données à l'aide du chiffrement côté serveur avec clés de chiffrement fournies par le client (SSE-C)"

OBTENIR l'objet

Vous pouvez utiliser la requête D'objet GET S3 pour récupérer un objet à partir d'un compartiment S3.

Le paramètre de demande de numéro de pièce n'est pas pris en charge

Le `partNumber` Le paramètre de demande n'est pas pris en charge pour les demandes D'objet GET. Vous ne pouvez pas effectuer de demande DE RÉCUPÉRATION pour récupérer une partie spécifique d'un objet partitionné. Une erreur 501 non implémentée est renvoyée avec le message suivant :

```
GET Object by partNumber is not implemented
```

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 cryptage 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 les clés fournies par le client pour sécuriser les données d'objet, consultez les considérations de la section « utilisation du cryptage côté serveur ».

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 D'OBTENTION d'un objet ayant échappé à l'UTF-8 dans les métadonnées définies par l'utilisateur ne renvoient pas le `x-amz-missing-meta` en-tête si le nom ou la valeur de la clé comporte des caractères non imprimables.

En-tête de demande non pris en charge

L'en-tête de demande suivant n'est pas pris en charge et renvoie `XNotImplemented`:

- `x-amz-website-redirect-location`

Gestion des versions

Si un `versionId` la sous-ressource n'est pas spécifiée, l'opération extrait la version la plus récente de l'objet dans un compartiment multiversion. Si la version actuelle de l'objet est un marqueur de suppression, un état « non trouvé » est renvoyé avec le `x-amz-delete-marker` réponse en-tête réglée sur `true`.

Comportement de L'objet GET pour les objets de pool de stockage cloud

Si un objet a été stocké dans un pool de stockage cloud (voir les instructions de gestion des objets avec gestion du cycle de vie des informations), le comportement d'une requête D'objet GET dépend de l'état de l'objet. Voir « objet TÊTE » pour plus de détails.

> Si un objet est stocké dans un pool de stockage cloud et qu'une ou plusieurs copies de cet objet existent également dans la grille, L'OBTENTION des demandes d'objet tente d'extraire les données de la grille avant de les récupérer depuis le pool de stockage cloud.

État de l'objet	Comportement de L'objet GET
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 demande DE restauration POST-objet pour restaurer l'objet à un état récupérable.
Objet en cours de restauration à partir d'un état non récupérable	`403 Forbidden`, `InvalidObjectState` Attendez que la demande DE restauration POST Object soit terminée.
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 demande GET Object peut retourner de manière incorrecte `200 OK` lorsque certaines parties de l'objet ont déjà été migrées à un état non récupérable ou lorsque certaines parties de l'objet n'ont pas encore été restaurées.

Dans ces cas :

- La demande GET Object peut renvoyer certaines données mais s'arrête à mi-chemin du transfert.
- Une requête GET Object suivante peut revenir `403 Forbidden`.

Informations associées

"À l'aide du chiffrement côté serveur"

"Gestion des objets avec ILM"

"Restauration POST-objet"

"Opérations S3 suivies dans les journaux d'audit"

Objet TÊTE

Vous pouvez utiliser la requête d'objet TÊTE S3 pour extraire les métadonnées à partir d'un objet sans y retourner. Si l'objet est stocké dans un pool de stockage cloud, vous

pouvez utiliser HEAD Object pour déterminer l'état de transition de l'objet.

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 cryptage 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 les clés fournies par le client pour sécuriser les données d'objet, consultez les considérations de la section « utilisation du cryptage côté serveur ».

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 DE TÊTE pour un objet ayant échappé à l'UTF-8 dans les métadonnées définies par l'utilisateur ne renvoient pas le `x-amz-missing-meta` en-tête si le nom ou la valeur de la clé comporte des caractères non imprimables.

En-tête de demande non pris en charge

L'en-tête de demande suivant n'est pas pris en charge et renvoie `XNotImplemented`:

- `x-amz-website-redirect-location`

En-têtes de réponse pour les objets Cloud Storage Pool

Si l'objet est stocké dans un pool de stockage cloud (voir les instructions de gestion des objets avec gestion du cycle de vie des informations), 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 TÊTE
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 à réponse spéciale n'est renvoyé.)

État de l'objet	Réponse à l'objet TÊTE

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 sur le point de passer un moment lointain dans le futur. 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 pour `expiry-date` est sur le point de passer un moment lointain dans le futur.
	
	Remarque : si la copie de la grille n'est pas disponible (par exemple, un nœud de stockage est en panne), vous devez émettre une demande DE restauration POST-objet pour restaurer la copie à partir du pool de stockage cloud avant de pouvoir extraire l'objet avec succès.

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 TÊTE

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 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 d'objet DE TÊTE peut revenir de manière incorrecte `x-amz-restore: ongoing-request="false"` lorsque certaines parties de l'objet ont déjà été migrées à un état non récupérable ou lorsque certaines parties de l'objet n'ont pas encore été restaurées.

Gestion des versions

Si un `versionId` la sous-ressource n'est pas spécifiée, l'opération extrait la version la plus récente de l'objet dans un compartiment multiversion. Si la version actuelle de l'objet est un marqueur de suppression, un état « non trouvé » est renvoyé avec le `x-amz-delete-marker` réponse en-tête réglée sur `true`.

Informations associées

"À l'aide du chiffrement côté serveur"

"Gestion des objets avec ILM"

"Restauration POST-objet"

"Opérations S3 suivies dans les journaux d'audit"

Restauration POST-objet

Vous pouvez utiliser la demande de restauration POST-objet 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 demandes DE restauration POST-objet pour restaurer un objet. Elle ne prend pas en charge le `SELECT` type de restauration. Sélectionnez demandes de retour `XNotImplemented`.

Gestion des versions

Spécifiez éventuellement `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 restauration POST-objet sur les objets de pool de stockage cloud

Si un objet a été stocké dans un pool de stockage cloud (voir les instructions de gestion des objets avec gestion du cycle de vie des informations), une demande de restauration POST-objet présente le comportement suivant, en fonction de l'état de l'objet. Voir « objet TÊTE » pour plus de détails.

> Si un objet est stocké dans un pool de stockage cloud et qu'une ou plusieurs copies de cet objet existent également dans la grille, il n'est pas nécessaire de le restaurer en émettant une demande de restauration POST-objet. En revanche, la copie locale peut être récupérée directement à l'aide d'une demande D'OBJET GET.

État de l'objet	Comportement de la restauration POST-objet
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 apportée. **Note**: Avant qu'un objet ait été transféré à un état non récupérable, vous ne pouvez pas le modifier `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 demande. À la fin de cette période, l'objet est renvoyé à un état non récupérable. Si vous le souhaitez, utilisez le `Tier` élément de demande pour déterminer la durée de la tâche de restauration (`Expedited`, `Standard`, ou `Bulk`). Si vous ne spécifiez pas `Tier`, le `Standard` le niveau est utilisé. **Attention** : si un objet a été transféré vers S3 Glacier Deep Archive ou si Cloud Storage Pool utilise Azure Blob Storage, vous ne pouvez pas le restaurer à l'aide de `Expedited` niveau. L'erreur suivante est renvoyée `403 Forbidden`, `InvalidTier`: `Retrieval option is not supported by this storage class`.
Objet en cours de restauration à partir d'un état non récupérable	`409 Conflict`, `RestoreAlreadyInProgress`

État de l'objet	Comportement de la restauration POST-objet
Objet entièrement restauré dans le pool de stockage cloud	`200 OK` **Remarque :** si un objet a été restauré à un état récupérable, vous pouvez le modifier `expiry-date` En réémettant la demande DE restauration POST Object avec une nouvelle valeur pour `Days`. La date de restauration est mise à jour par rapport à l'heure de la demande.

Informations associées

"Gestion des objets avec ILM"

"Objet TÊTE"

"Opérations S3 suivies dans les journaux d'audit"

PLACER l'objet

Vous pouvez utiliser la demande S3 PUT Object pour ajouter un objet à un compartiment.

Résolution des conflits

Les demandes contradictoires des clients, telles que deux clients qui écrivent sur la même clé, sont résolues sur la base des « derniers-victoires ». Le calendrier de l'évaluation « derniers-victoires » est basé sur le moment où le système StorageGRID remplit une demande donnée et non sur le moment où les clients S3 commencent une opération.

Taille de l'objet

StorageGRID prend en charge les objets pouvant atteindre 5 To.

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 demandes PUT, PUT Object-Copy, GET et HEAD sont satisfaites si les métadonnées définies par l'utilisateur incluent des caractères UTF-8 échappés.
- StorageGRID ne renvoie pas le `x-amz-missing-meta` en-tête si la valeur interprétée du nom ou de la valeur de la clé comprend 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` contre l'objet.
- `Content-Language`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Expires`
- `Transfer-Encoding`

  Le codage du transfert haché est pris en charge si `aws-chunked` la signature de charge utile est également utilisée.

- `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-<em>name</em>: <em>value</em>
  ```

  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` nom des métadonnées enregistrées lors de la création de l'objet. Par exemple :

```
x-amz-meta-creation-time: 1443399726
```

La valeur pour `creation-time` Est évaluée en secondes depuis le 1er janvier 1970.

> Une règle ILM ne peut pas utiliser à la fois un **temps de création défini par l'utilisateur** pour le temps de référence et les options équilibrées ou strictes pour le comportement d'ingestion. 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`

"Utilisation du verrouillage d'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`

"Opérations et limites prises en charge par l'API REST S3"

En-têtes de requête non pris en charge

Les en-têtes de requête suivants ne sont pas pris en charge :

- Le `x-amz-acl` l'en-tête de demande n'est pas pris en charge.
- Le `x-amz-website-redirect-location` l'en-tête de demande n'est pas pris en charge et renvoie `XNotImplemented`.

Options de classe de stockage

Le `x-amz-storage-class` l'en-tête de demande est pris en charge. Valeur soumise pour `x-amz-storage-class` StorageGRID protège les données d'objet lors de leur ingestion, mais pas le nombre de copies persistantes de l'objet stockées dans le système StorageGRID (déterminé par ILM).

Si la règle ILM correspondant à un objet ingéré utilise l'option stricte pour le comportement d'ingestion, le `x-amz-storage-class` la barre de coupe n'a aucun effet.

Les valeurs suivantes peuvent être utilisées pour `x-amz-storage-class`:

- `STANDARD` (Valeur 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). Lors de l'évaluation de l'ILM, StorageGRID détermine si ces copies intermédiaires initiales répondent aux instructions de placement de la règle. Autrement, de nouvelles copies d'objet peuvent être nécessaires à d'autres emplacements et les copies intermédiaires initiales peuvent être supprimées.

  - **Équilibré** : si la règle ILM spécifie l'option équilibrée et que StorageGRID ne peut pas immédiatement faire toutes les copies spécifiées dans la règle, StorageGRID effectue deux copies intermédiaires sur différents nœuds de stockage.

    Si StorageGRID peut immédiatement créer toutes les copies d'objet spécifiées dans la règle ILM (placement synchrone), l' `x-amz-storage-class` la barre de coupe 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 ne fait une copie provisoire que si le système ne peut pas immédiatement faire toutes les copies spécifiées dans la règle. Si StorageGRID peut effectuer un placement synchrone, cet en-tête n'a aucun effet. Le `REDUCED_REDUNDANCY` L'option est meilleure lorsque la règle ILM correspondant à l'objet crée une copie répliquée unique. Dans ce cas, utilisez `REDUCED_REDUNDANCY` élimine la création et la suppression inutiles d'une copie d'objet supplémentaire pour chaque opération d'ingestion.

  À l'aide du `REDUCED_REDUNDANCY` cette option n'est pas recommandée dans d'autres cas. `REDUCED_REDUNDANCY` augmente le risque de perte de données d'objet lors de l'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.

Attention: Avoir une seule copie répliquée pour une période donnée met les données en danger de perte permanente. 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.

Spécification `REDUCED_REDUNDANCY` l'impact sur le nombre de copies créées uniquement lors de l'ingestion d'un objet. Elle n'affecte pas le nombre de copies de l'objet lorsque celui-ci est évalué par la règle ILM active ; le stockage des données ne se produit pas à des niveaux de redondance inférieurs dans le système StorageGRID.

Remarque : si vous ingez un objet dans un compartiment avec le verrouillage d'objet S3 activé, le `REDUCED_REDUNDANCY` l'option est ignorée. Si vous ingez un objet dans un compartiment conforme d'ancienne génération, le `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`
- **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 cryptage pour le nouvel objet.
- `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le résumé MD5 de la clé de chiffrement du nouvel objet.

Attention : les clés de cryptage que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant. Avant d'utiliser les clés fournies par le client pour sécuriser les données d'objet, consultez les considérations de la section « utilisation du cryptage côté serveur ».

Remarque : si un objet est chiffré avec SSE ou SSE-C, les paramètres de chiffrement au niveau du godet ou de la grille sont ignorés.

Gestion des versions

Si le contrôle de version est activé pour un compartiment, un contrôle unique `versionId` est automatiquement généré pour la version de l'objet stocké. C'est ça `versionId` est également renvoyé dans la réponse en utilisant le `x-amz-version-id` en-tête de réponse.

Si la gestion des versions est suspendue, la version de l'objet est stockée avec un null `versionId` si une version nulle existe déjà, elle sera remplacée.

Informations associées

"Gestion des objets avec ILM"

"Opérations sur les compartiments"

"Opérations S3 suivies dans les journaux d'audit"

"À l'aide du chiffrement côté serveur"

"Configuration des connexions client"

PLACER l'objet - Copier

Vous pouvez utiliser la demande S3 PUT Object - copie pour créer une copie d'un objet déjà stocké dans S3. Une opération PUT Object - Copy est la même que l'exécution d'un GET puis D'un PUT.

Résolution des conflits

Les demandes contradictoires des clients, telles que deux clients qui écrivent sur la même clé, sont résolues sur la base des « derniers-victoires ». Le calendrier de l'évaluation « derniers-victoires » est basé sur le moment où le système StorageGRID remplit une demande donnée et non sur le moment où les clients S3 commencent une opération.

Taille de l'objet

StorageGRID prend en charge les objets pouvant atteindre 5 To.

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 le `x-amz-missing-meta` en-tête si la valeur interprétée du nom ou de la valeur de la clé comprend 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 permet de copier l'objet et les métadonnées associées.

  Vous pouvez spécifier `REPLACE` pour remplacer les métadonnées existantes lors de la copie de l'objet ou pour la mise à jour des 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` pour remplacer les balises existantes lors de la copie de l'objet ou pour 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`

"Utilisation du verrouillage d'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

"Demander des en-têtes pour le cryptage côté serveur"

En-têtes de requête non pris en charge

Les en-têtes de requête suivants ne sont pas pris en charge :

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- Expires
- x-amz-website-redirect-location

Options de classe de stockage

Le x-amz-storage-class L'en-tête de demande est pris en charge et affecte le nombre de copies d'objet créé par StorageGRID si la règle ILM correspondante spécifie le comportement d'ingestion de la double validation ou de l'équilibrage.

- 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 ingez un objet dans un compartiment avec l'option de verrouillage objet S3 activée, la REDUCED_REDUNDANCY l'option est ignorée. Si vous ingez un objet dans un compartiment conforme d'ancienne génération, le 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 PUT Object - Copy

Si le godet source et la clé, spécifiés dans le x-amz-copy-source en-tête diffèrent du compartiment de destination et de la clé, une copie des données de l'objet source est écrite sur la destination.

Si la source et la destination correspondent, et le `x-amz-metadata-directive` l'en-tête est spécifié comme `REPLACE`, les métadonnées de l'objet sont mises à jour avec les valeurs de métadonnées fournies dans la demande. Dans ce cas, StorageGRID ne réingère pas l'objet. Ceci a deux conséquences importantes :

- Vous ne pouvez pas utiliser METTRE l'objet - Copier pour crypter un objet existant en place ou pour modifier le chiffrement d'un objet existant. Si vous fournissez le `x-amz-server-side-encryption` en-tête ou le `x-amz-server-side-encryption-customer-algorithm` En-tête, StorageGRID rejette la demande et renvoie la requête `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.

  Cela signifie que si la règle ILM utilise l'option stricte pour le comportement d'ingestion, aucune action n'est effectuée si les placements d'objet requis ne peuvent pas être effectués (par exemple, car un nouvel emplacement requis 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 chiffrement 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 demande PUT Object - Copy, 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 cryptage pour l'objet cible.
  - `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le résumé MD5 de la nouvelle clé de chiffrement.

Attention : les clés de cryptage que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant. Avant d'utiliser les clés fournies par le client pour sécuriser les données d'objet, consultez les considérations de la section « utilisation du cryptage côté serveur ».

- Si vous souhaitez chiffrer l'objet cible (la copie) avec une clé unique gérée par StorageGRID (SSE), incluez cet en-tête dans la demande PUT Object - Copy :
  - `x-amz-server-side-encryption`

Remarque : le `server-side-encryption` la valeur de l'objet ne peut pas être mise à jour. Faites plutôt une copie avec un nouveau `server-side-encryption` valeur à l'aide de `x-amz-metadata-directive`: `REPLACE`.

Gestion des versions

Si le compartiment source est multiversion, vous pouvez utiliser le `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 l' `versionId` sous-ressource. Si le compartiment de destination est multiversion, la version générée est renvoyée dans le `x-amz-version-id` en-tête de réponse. Si le contrôle de version est suspendu pour le compartiment cible, alors `x-amz-version-id` renvoie une valeur « nulle ».

Informations associées

"Gestion des objets avec ILM"

"À l'aide du chiffrement côté serveur"

"Opérations S3 suivies dans les journaux d'audit"

"PLACER l'objet"

Opérations pour les téléchargements partitionnés

Cette section décrit comment StorageGRID prend en charge les opérations de téléchargement partitionné.

- "Répertorier les téléchargements partitionnés"
- "Lancer le téléchargement de pièces multiples"
- "Télécharger la pièce"
- "Télécharger la pièce - Copier"
- "Chargement de pièces multiples complet"

Les conditions et notes suivantes s'appliquent à toutes les opérations de téléchargement partitionné :

- Vous ne devez pas dépasser 1,000 téléchargements partitionnés simultanés dans un seul compartiment car les résultats des requêtes List Multipart Uploads pour ce compartiment pourraient 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. Comme chaque pièce est considérée comme un objet unique, l'utilisation de grandes tailles de pièce réduit la surcharge des métadonnées StorageGRID.
  - Pour les objets de moins de 5 Gio, envisagez l'utilisation de téléchargement non partitionné.
- Le ILM est évalué pour chaque partie d'un objet partitionné à l'ingestion et pour l'objet dans son ensemble, à la fin du téléchargement partitionné, si la règle ILM utilise le comportement d'entrée strict ou équilibré. Vous devez savoir comment cela affecte le positionnement de l'objet et de la pièce :
  - Si le téléchargement partitionné est en cours de modification du ILM, si le téléchargement partitionné et certaines parties de l'objet peuvent ne pas répondre aux exigences ILM actuelles. Toute pièce qui n'est pas placée correctement est mise en file d'attente pour la réévaluation ILM et est déplacée ultérieurement au bon emplacement.

    - Lors de l'évaluation d'ILM pour une pièce, StorageGRID filtre la taille de la pièce, et non la taille de l'objet. Cela signifie que certaines parties d'un objet peuvent être stockées à des emplacements ne respectant pas les exigences ILM de l'objet dans son ensemble. Par exemple, si une règle indique que tous les objets de 10 Go ou plus sont stockés dans DC1 alors que tous les objets plus petits sont stockés dans DC2, à l'acquisition chaque partie de 1 Go d'un téléchargement partitionné en 10 parties est stockée dans DC2. Lorsque ILM est évaluée pour l'ensemble de l'objet, toutes les parties de l'objet sont déplacées vers DC1.

- Toutes les opérations de téléchargement partitionné prennent en charge les contrôles de cohérence StorageGRID.
- Si nécessaire, vous pouvez utiliser le cryptage côté serveur avec des téléchargements partitionnés. Pour utiliser SSE (chiffrement côté serveur avec clés gérées par StorageGRID), vous avez accès au `x-amz-server-side-encryption` En-tête de demande dans la demande de téléchargement de pièces multiples uniquement. Pour utiliser SSE-C (chiffrement côté serveur avec clés fournies par le client), vous devez spécifier les trois mêmes en-têtes de demande de clé de chiffrement dans la demande de lancement de Multipart Upload et dans chaque demande de chargement de pièce suivante.

Fonctionnement	Mise en place
Liste des téléchargements partitionnés	Voir "Liste des téléchargements partitionnés"
Lancer le téléchargement de pièces multiples	Voir "Lancer le téléchargement de pièces multiples"
Télécharger la pièce	Voir "Télécharger la pièce"
Télécharger la pièce - Copier	Voir "Télécharger la pièce - Copier"
Chargement de pièces multiples complet	Voir "Chargement de pièces multiples complet"
Abandonner le téléchargement de pièces multiples	Mise en œuvre avec tout le comportement de l'API REST Amazon S3
Répertorier les pièces	Mise en œuvre avec tout le comportement de l'API REST Amazon S3

Informations associées

"Contrôles de cohérence"

"À l'aide du chiffrement côté serveur"

Liste des téléchargements partitionnés

L'opération List Multipart Uploads répertorie les téléchargements partitionnés en cours pour un compartiment.

Les paramètres de demande suivants sont pris en charge :

- `encoding-type`
- `max-uploads`

- `key-marker`
- `prefix`
- `upload-id-marker`

Le `delimiter` le paramètre de demande n'est pas pris en charge.

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. Lorsque l'opération de téléchargement multipart complète est exécutée, c'est-à-dire le point où les objets sont créés (et versionnés le cas échéant).

Lancer le téléchargement de pièces multiples

L'opération lancer le téléchargement de pièces multiples lance un téléchargement partitionné pour un objet et renvoie un ID de téléchargement.

Le `x-amz-storage-class` l'en-tête de demande est pris en charge. Valeur soumise pour `x-amz-storage-class` StorageGRID protège les données d'objet lors de leur ingestion, mais pas le nombre de copies persistantes de l'objet stockées dans le système StorageGRID (déterminé par ILM).

Si la règle ILM correspondant à un objet ingéré utilise l'option stricte pour le comportement d'ingestion, le `x-amz-storage-class` la barre de coupe n'a aucun effet.

Les valeurs suivantes peuvent être utilisées pour `x-amz-storage-class`:

- `STANDARD` (Valeur 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). Lors de l'évaluation de l'ILM, StorageGRID détermine si ces copies intermédiaires initiales répondent aux instructions de placement de la règle. Autrement, de nouvelles copies d'objet peuvent être nécessaires à d'autres emplacements et les copies intermédiaires initiales peuvent être supprimées.
  - **Équilibré** : si la règle ILM spécifie l'option équilibrée et que StorageGRID ne peut pas immédiatement faire toutes les copies spécifiées dans la règle, StorageGRID effectue deux copies intermédiaires sur différents nœuds de stockage.

    Si StorageGRID peut immédiatement créer toutes les copies d'objet spécifiées dans la règle ILM (placement synchrone), l' `x-amz-storage-class` la barre de coupe 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 ne fait une copie provisoire que si le système ne peut pas immédiatement faire toutes les copies spécifiées dans la règle. Si StorageGRID peut effectuer un placement synchrone, cet en-tête n'a aucun effet. Le `REDUCED_REDUNDANCY` L'option est meilleure lorsque la règle ILM correspondant à l'objet crée une copie répliquée unique. Dans ce cas, utilisez `REDUCED_REDUNDANCY` élimine la création et la

suppression inutiles d'une copie d'objet supplémentaire pour chaque opération d'ingestion.

À l'aide du `REDUCED_REDUNDANCY` cette option n'est pas recommandée dans d'autres cas. `REDUCED_REDUNDANCY` augmente le risque de perte de données d'objet lors de l'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.

Attention: Avoir une seule copie répliquée pour une période donnée met les données en danger de perte permanente. 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.

Spécification `REDUCED_REDUNDANCY` l'impact sur le nombre de copies créées uniquement lors de l'ingestion d'un objet. Elle n'affecte pas le nombre de copies de l'objet lorsque celui-ci est évalué par la règle ILM active ; le stockage des données ne se produit pas à des niveaux de redondance inférieurs dans le système StorageGRID.

Remarque : si vous ingez un objet dans un compartiment avec le verrouillage d'objet S3 activé, le `REDUCED_REDUNDANCY` l'option est ignorée. Si vous ingez un objet dans un compartiment conforme d'ancienne génération, le `REDUCED_REDUNDANCY` option renvoie une erreur. StorageGRID procède toujours à une récupération à double engagement afin de satisfaire les exigences de conformité.

Les en-têtes de requête suivants sont pris en charge :

- `Content-Type`
- `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` nom des métadonnées enregistrées lors de la création de l'objet. Par exemple :

  ```
  x-amz-meta-creation-time: 1443399726
  ```

  La valeur pour `creation-time` Est évaluée en secondes depuis le 1er janvier 1970.

  Ajout `creation-time` Comme les métadonnées définies par l'utilisateur n'sont pas autorisées si vous ajoutez un objet à un compartiment pour lequel la conformité héritée 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`

"Utilisation du verrouillage d'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`

"Opérations et limites prises en charge par l'API REST S3"

Pour plus d'informations sur le StorageGRID traitement des caractères UTF-8, reportez-vous à la documentation relative à L'objet PUT.

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 lancer le téléchargement multi-pièces si vous souhaitez crypter l'objet avec une clé unique gérée par StorageGRID. Ne spécifiez pas cet en-tête dans l'une des demandes de téléchargement d'article.
  - `x-amz-server-side-encryption`
- **SSE-C** : utilisez les trois en-têtes de la demande de téléchargement multipièces (et dans chaque demande de chargement ultérieure de pièce) si vous souhaitez 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 cryptage pour le nouvel objet.
  - `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le résumé MD5 de la clé de chiffrement du nouvel objet.

Attention : les clés de cryptage que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant. Avant d'utiliser les clés fournies par le client pour sécuriser les données d'objet, consultez les considérations de la section « utilisation du cryptage côté serveur ».

En-têtes de requête non pris en charge

L'en-tête de demande suivant n'est pas pris en charge et renvoie `XNotImplemented`

- `x-amz-website-redirect-location`

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 de

chargement multipièce complète est exécutée.

Informations associées

"Gestion des objets avec ILM"

"À l'aide du chiffrement côté serveur"

"PLACER l'objet"

Télécharger la pièce

L'opération de téléchargement de pièce 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 :

- `Content-Length`
- `Content-MD5`

Demander des en-têtes pour le cryptage côté serveur

Si vous avez spécifié le cryptage SSE-C pour lancer la demande de téléchargement multipièce, vous devez également inclure les en-têtes de requête suivants dans chaque demande de chargement de pièce :

- `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 de lancement de Multipart Upload.
- `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le même résumé MD5 que vous avez fourni dans la demande de lancement de Multipart Upload.

> 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 les clés fournies par le client pour sécuriser les données d'objet, consultez les considérations de la section « utilisation du 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 de chargement multipièce complète est exécutée.

Informations associées

"À l'aide du chiffrement côté serveur"

Télécharger la pièce - Copier

L'opération Télécharger la pièce - Copier télécharge une partie d'un objet en copiant les données d'un objet existant en tant que source de données.

L'opération Télécharger la pièce - copie est implémentée avec tout le comportement de l'API REST Amazon S3.

Cette requête lit et écrit les données de l'objet spécifiées dans `x-amz-copy-source-range` Dans le 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 lancer la demande de téléchargement multi-pièces, vous devez également inclure les en-têtes de requête suivants dans chaque pièce de téléchargement - demande de copie :

- `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 de lancement de Multipart Upload.
- `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le même résumé MD5 que vous avez fourni dans la demande de lancement de Multipart Upload.

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 demande de copie de pièce de téléchargement, 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 cryptage 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 les clés fournies par le client pour sécuriser les données d'objet, consultez les considérations de la section « utilisation du 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 de chargement multipièce complète est exécutée.

Chargement de pièces multiples complet

L'opération complète de téléchargement de pièces multiples termine un téléchargement partitionné d'un objet en assemblant les pièces précédemment téléchargées.

Résolution des conflits

Les demandes contradictoires des clients, telles que deux clients qui écrivent sur la même clé, sont résolues sur la base des « derniers-victoires ». Le calendrier de l'évaluation « derniers-victoires » est basé sur le moment où le système StorageGRID remplit une demande donnée et non sur le moment où les clients S3 commencent une opération.

Taille de l'objet

StorageGRID prend en charge les objets pouvant atteindre 5 To.

En-têtes de demande

Le `x-amz-storage-class` L'en-tête de demande est pris en charge et affecte le nombre de copies d'objet créé par StorageGRID si la règle ILM correspondante spécifie le comportement d'ingestion de la double validation ou de l'équilibrage.

- `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 ingez un objet dans un compartiment avec l'option de verrouillage objet S3 activée, la `REDUCED_REDUNDANCY` l'option est ignorée. Si vous ingez un objet dans un compartiment conforme d'ancienne génération, le `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.

> Le `ETag` La valeur renvoyée n'est pas une somme MD5 des données, mais suit l'implémentation de l'API Amazon S3 du `ETag` valeur pour les objets en plusieurs parties.

Gestion des versions

Cette opération termine un téléchargement partitionné. Si le contrôle de version est activé pour un compartiment, la version de l'objet est créée à la fin du téléchargement partitionné.

Si le contrôle de version est activé pour un compartiment, un contrôle unique `versionId` est automatiquement généré pour la version de l'objet stocké. C'est ça `versionId` est également renvoyé dans la réponse en utilisant le `x-amz-version-id` en-tête de réponse.

Si la gestion des versions est suspendue, la version de l'objet est stockée avec un null `versionId` si une version nulle existe déjà, elle sera remplacée.

> 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.

Dans ce cas, une alarme est déclenchée dans le gestionnaire de grille sur Total Events (SMTT). Le message « échec de publication des notifications pour la clé nom-zone » s'affiche pour le dernier objet dont la notification a échoué. (Pour afficher ce message, sélectionnez **Nodes** > ***Storage Node*** > **Events**. Afficher le dernier événement en haut du tableau.) Les messages d'événement sont également répertoriés dans le `/var/local/log/bycast-err.log`.

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.

Informations associées

"Gestion des objets avec ILM"

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

Nom	Statut HTTP
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
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

Nom	Statut HTTP
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
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
XMaxBucketPolicyLengthExcediéd é	Votre politique dépasse la longueur maximale autorisée pour la règle de gestion des compartiments.	400 demande erronée

Nom	Description	Statut HTTP
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 des API REST StorageGRID S3

Des opérations sont ajoutées à l'API REST S3 qui sont spécifiques à un système StorageGRID.

DEMANDE de cohérence des compartiments

La demande D'obtention de cohérence de godet vous permet de déterminer le niveau de cohérence appliqué à un compartiment particulier.

Les contrôles de cohérence par défaut garantissent la lecture après écriture des nouveaux objets.

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: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

Réponse

Dans le XML de réponse, `<Consistency>` renvoie l'une des valeurs suivantes :

Contrôle de cohérence	Description
tous	Tous les nœuds reçoivent les données immédiatement, sinon la requête échoue.

Contrôle de cohérence	Description
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. Correspondance avec les garanties de cohérence Amazon S3. **Remarque :** si votre application utilise des demandes HEAD sur des objets qui n'existent pas, vous pouvez recevoir un nombre élevé de 500 erreurs de serveur interne si un ou plusieurs nœuds de stockage ne sont pas disponibles. Pour éviter ces erreurs, définissez le contrôle de cohérence sur « disponible », sauf si vous avez besoin de garanties de cohérence similaires à Amazon S3.
Disponible (cohérence possible pour les opérations DE TÊTE)	Se comporte de la même manière que le niveau de cohérence « entre la date et la nouvelle écriture », mais n'assure qu'une cohérence éventuelle pour les opérations DE TÊTE. Niveaux de disponibilité supérieurs à ceux de la « nouvelle écriture » en cas d'indisponibilité des nœuds de stockage Diffère des garanties de cohérence Amazon S3 pour les opérations HEAD uniquement.

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

"Contrôles de cohérence"

PUT Bucket Consistency demandée

La demande de cohérence PUT bucket permet de spécifier le niveau de cohérence à appliquer aux opérations effectuées dans un compartiment.

Les contrôles de cohérence par défaut garantissent la lecture après écriture des nouveaux objets.

Pour effectuer cette opération, vous devez disposer de l'autorisation s3:PutBuckeConsistency, ou être root de compte.

Demande

Le `x-ntap-sg-consistency` le paramètre doit contenir l'une des valeurs suivantes :

Contrôle de 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. Correspondance avec les garanties de cohérence Amazon S3. **Remarque :** si votre application utilise des demandes HEAD sur des objets qui n'existent pas, vous pouvez recevoir un nombre élevé de 500 erreurs de serveur interne si un ou plusieurs nœuds de stockage ne sont pas disponibles. Pour éviter ces erreurs, définissez le contrôle de cohérence sur « disponible », sauf si vous avez besoin de garanties de cohérence similaires à Amazon S3.
Disponible (cohérence possible pour les opérations DE TÊTE)	Se comporte de la même manière que le niveau de cohérence « entre la date et la nouvelle écriture », mais n'assure qu'une cohérence éventuelle pour les opérations DE TÊTE. Niveaux de disponibilité supérieurs à ceux de la « nouvelle écriture » en cas d'indisponibilité des nœuds de stockage Diffère des garanties de cohérence Amazon S3 pour les opérations HEAD uniquement.

Remarque: en général, vous devez utiliser la valeur de contrôle de cohérence "entre les nouvelles écritures". Si les demandes ne fonctionnent pas correctement, modifiez le comportement du client de l'application si

possible. Ou configurez le client afin de spécifier le contrôle de cohérence pour chaque requête d'API. Réglez le contrôle de cohérence au niveau du godet uniquement en dernier recours.

Exemple de demande

```
PUT /bucket?x-ntap-sg-consistency=strong-global HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

Informations associées

"Contrôles de cohérence"

DEMANDE DE 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: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

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>
```

DEMANDE de temps de 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 D'heure du dernier accès AU compartiment, la case à cocher **S3 > seaux > Modifier le dernier paramètre d'accès** dans le Gestionnaire de locataires ou l'API de gestion des locataires.

Si les dernières mises à jour de temps d'accès sont désactivées pour un compartiment, les opérations suivantes sont appliquées sur le compartiment :

- LES demandes GET Object, GET Object ACL, GET Object Tagging et HEAD Object 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).
- PUT Object : les demandes de copie et DE BALISAGE d'objets QUI mettent à jour uniquement 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, PLACER l'objet - les demandes de copie 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, PLACER l'objet - demandes de copie toujours mettre à jour l'heure du dernier accès. La copie de l'objet est ajoutée aux files d'attente pour l'évaluation ILM.
- Terminer les demandes de téléchargement de pièces multiples mises à jour de l'heure de 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: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

Cet exemple désactive l'heure du dernier accès pour un compartiment.

```
PUT /bucket?x-ntap-sg-lastaccesstime=disabled HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

Informations associées

"Utilisez un compte de locataire"

SUPPRIME la demande de 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: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

LIRE la demande de configuration de notification des 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 demande récupère la configuration de notification des métadonnées pour le compartiment nommé `bucket`.

```
GET /bucket?x-ntap-sg-metadata-notification HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

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.
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.

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

XML inclus entre le `<MetadataNotificationConfiguration></MetadataNotificationConfiguration>` les balises indiquent comment l'intégration avec un terminal d'intégration de la recherche est configurée pour le compartiment. Dans cet exemple, les métadonnées d'objet sont envoyées à un index Elasticsearch nommé `current` et le type nommé `2017` 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"

PUT Bucket metadata notification configuration

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 les métadonnées pour les objets avec le préfixe `/images` à une destination et à des objets avec le préfixe `/videos` à un autre.

Les configurations dont les préfixes se chevauchent ne sont pas valides et sont rejetées lors de leur envoi. Par exemple, une configuration comprenant une règle pour les objets avec le préfixe `test` et une seconde règle pour les objets avec le préfixe `test2` ne serait pas autorisé.

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 de métadonnées est soumise, ou que 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.

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.

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: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>

<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 pour les objets qui correspondent au préfixe `/images` est envoyée à une destination, tandis que les métadonnées d'objet correspondent au préfixe `/videos` est envoyé à une seconde destination.

```
PUT /graphics?x-ntap-sg-metadata-notification HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>

<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>
```

Informations associées

"Utilisez un compte de locataire"

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 peut être généré lorsqu'un objet doté de la clé est associé `SGWS/Tagging.txt` est créé dans un compartiment nommé `test`. Le `test` le compartiment n'est pas multiversion `versionId` l'étiquette est 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	Zone de godet, 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	les 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

Remarque : pour les balises et les métadonnées d'utilisateur, StorageGRID transmet les dates et les chiffres à Elasticsearch sous forme de chaînes ou de 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.

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.

Le volume de stockage utilisé par un compte et ses compartiments peut être obtenu à l'aide d'une demande GET Service 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. Si la cohérence globale forte ne peut pas être atteinte, StorageGRID tente de récupérer les informations d'utilisation avec une cohérence site élevée.

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: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

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 à la `ObjectCount` et `DataBytes` valeurs dans la réponse. Les marqueurs de suppression ne sont pas ajoutés au `ObjectCount` total.

Informations associées

"Contrôles de cohérence"

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 automatiquement activé lorsque vous effectuez une mise à niveau vers StorageGRID 11.5. 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.

"Utilisation du verrouillage d'objet S3"

"Gestion des objets avec ILM"

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

Obsolète : METTEZ les modifications de la demande de compartiment 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.

> La fonctionnalité de conformité StorageGRID disponible dans les versions précédentes d'StorageGRID est obsolète et a été remplacée par le verrouillage d'objet S3.

"Utilisation du verrouillage d'objet S3"

"Gestion des objets avec ILM"

"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 s'affiche si vous tentez d'utiliser les modifications de demande DE MISE en godet pour la conformité afin de créer un nouveau compartiment conforme :

```
The Compliance feature is deprecated.
Contact your StorageGRID administrator if you need to create new Compliant
buckets.
```

Informations associées

"Gestion des objets avec ILM"

"Utilisez un compte de locataire"

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.

"Utilisation du verrouillage d'objet S3"

"Gestion des objets avec ILM"

"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 pour le compartiment nommé `mybucket`.

```
GET /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

Exemple de réponse

Dans le XML de réponse, `<SGCompliance>` le répertorie les paramètres de conformité utilisés 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: <em>date</em>
Connection: <em>connection</em>
Server: StorageGRID/11.1.0
x-amz-request-id: <em>request ID</em>
Content-Length: <em>length</em>
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.

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.

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`.

Informations associées

"Gestion des objets avec ILM"

"Utilisez un compte de locataire"

Obsolète : PUT Bucket Compliance request

La demande de conformité 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.

"Utilisation du verrouillage d'objet S3"

"Gestion des objets avec ILM"

"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, objets dans `mybucket` sera maintenant conservé pendant deux ans (1,051,200 minutes) au lieu d'un an, à partir de l'ingestion de l'objet dans le grid. 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: <em>date</em>
Authorization: <em>authorization name</em>
Host: <em>host</em>
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. **Attention:** lorsque vous spécifiez une nouvelle valeur pour RetentionPeriodMinutes, vous devez spécifier une valeur égale ou supérieure à la période de rétention actuelle du godet. Une fois la période de rétention du godet définie, vous ne pouvez pas la réduire ; vous pouvez uniquement l'augmenter.
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.

Nom	Description
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.

Niveau de cohérence des 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 le niveau de cohérence **Strong-global** pour garantir que tous les sites de data Center et tous les nœuds de stockage contenant des métadonnées de compartiment sont cohérents en lecture après écriture pour les paramètres de conformité modifiés.

Si StorageGRID ne peut pas atteindre le niveau de cohérence **Strong-global** car un site de centre de données ou plusieurs nœuds de stockage sur un site ne sont pas disponibles, 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 de la grille ne parvient pas à mettre suffisamment de nœuds de stockage sur chaque site, le support technique vous demandera peut-être de relancer la demande échouée en forçant le niveau de cohérence **site fort**.

> Ne forcez jamais le niveau de cohérence **site fort** pour la conformité DU godet DE MISE à moins que vous n'ayez été invité à le faire par le support technique et à moins que vous compreniez les conséquences possibles de l'utilisation de ce niveau.

Lorsque le niveau de cohérence est réduit à **strong-site**, StorageGRID garantit que les paramètres de conformité mis à jour auront une cohérence lecture-après-écriture uniquement pour les requêtes client 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 sous une obligation légale et que vous forcez un niveau de cohérence inférieur, 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 du niveau de cohérence **site fort**, réémettez la demande de conformité Put et incluez le `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 demande 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"

"Utilisez un compte de locataire"

"Gestion des objets avec ILM"

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.

- **Les règles de compartiment**, qui sont configurées à l'aide de la stratégie DE compartiment, DE LA règle DE compartiment PUT et DES opérations de L'API S3 de la politique de compartiment. 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.

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 un accès anonyme, qui accorde la permission à tous. Par exemple, vous définissez le caractère générique (*) comme valeur principale.

```
"Principal":"*"
```

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 les responsables, le groupe admin `federated-group/admin` et le groupe financier `federated-group/finance`, Autorisations d'exécution de l'action `s3:ListBucket` sur le compartiment nommé `mybucket` Et l'action `s3:GetObject` sur tous les objets à l'intérieur de ce godet.

```
{
  "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:iam:s3:::mybucket",
        "arn:aws:iam: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.

Informations associées

"Utilisez un compte de locataire"

Paramètres de contrôle de cohérence des règles

Par défaut, toutes les mises à jour apportées aux stratégies de groupe sont cohérentes. Une fois la stratégie de groupe cohérente, les modifications peuvent prendre 15 minutes supplémentaires à appliquer en raison de la mise en cache des règles. Par défaut, toutes les mises à jour effectuées sur les règles de compartiment sont

également cohérentes en définitive.

Si nécessaire, vous pouvez modifier les garanties de cohérence pour les mises à jour des règles de compartiment. Par exemple, il peut être intéressant de vouloir modifier cette règle afin qu'elle devienne effective dès que possible pour des raisons de sécurité.

Dans ce cas, vous pouvez définir le `Consistency-Control` L'en-tête de la demande de stratégie PUT Bucket ou vous pouvez utiliser la demande DE cohérence PUT Bucket. Lorsque vous modifiez le contrôle de cohérence pour cette demande, vous devez utiliser la valeur **All**, qui fournit la garantie la plus élevée de cohérence de lecture après écriture. Si vous spécifiez une autre valeur de contrôle de cohérence dans un en-tête pour la demande DE cohérence PUT Bucket, la demande sera rejetée. Si vous spécifiez une autre valeur pour une demande de stratégie PUT Bucket, la valeur sera ignorée. Une fois la règle de compartiment cohérente, les modifications peuvent prendre 8 secondes supplémentaires pour effet, grâce à la mise en cache des règles.

> Si vous définissez le niveau de cohérence sur **All** pour forcer une nouvelle stratégie de godet à devenir efficace plus tôt, veillez à remettre le contrôle au niveau du godet à sa valeur d'origine lorsque vous avez terminé. Sinon, toutes les futures demandes de rubrique utiliseront le paramètre **tous**.

Utilisation de l'ARN dans les instructions de stratégie

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 de stratégie PUT Bucket doit être codé avec charset=UTF-8.

Spécification des 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 politique, 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.

Informations associées

"Spécification des variables dans une règle"

Spécification des entités de base 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 d'une politique de groupe n'ont pas besoin de l'élément principal car le groupe est compris comme principal.
- Dans une politique, les principes sont indiqués par l'élément « principal » ou « notprincipal » 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 que Alex quitte l'entreprise et le nom d'utilisateur `Alex` est supprimé. Si un nouveau Alex rejoint l'organisation et est affecté de la même façon `Alex` nom d'utilisateur, le nouvel utilisateur peut hériter involontairement 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.

Définition des 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 opérations de réplication de compartiments PUT et DELETE. StorageGRID utilise des autorisations distinctes pour chaque action, qui correspond à la spécification Amazon S3 d'origine.

> Une SUPPRESSION est effectuée lorsqu'un PUT est utilisé pour remplacer une valeur existante.

Autorisations qui s'appliquent aux compartiments

Autorisations	OPÉRATIONS DES API REST S3	Personnalisée pour StorageGRID
s3:CreateBucket	PLACER le godet	
s3:DeleteBucket	SUPPRIMER le compartiment	
s3:DeleteBuckeMetadatanotification	SUPPRIMEZ la configuration de notification des métadonnées de compartiment	Oui.
s3:DeleteBucketPolicy	SUPPRIMER la règle de compartiment	
s3:DeleteReplicationConfiguration	SUPPRIMER la réplication du compartiment	Oui, séparer les autorisations pour PUT et DELETE*
s3:GetBucketAcl	OBTENIR l'ACL du compartiment	
s3:GetBuckeCompliance	GARANTIR la conformité des compartiments (obsolète)	Oui.
s3:persistance GetBucketConsistency	OPTIMISEZ la cohérence des compartiments	Oui.
s3:GetBucketCORS	OBTENIR les godets	
s3:GetEncryptionConfiguration	CHIFFREMENT des compartiments	
s3:GetBucketLastAccessTime	HEURE du dernier accès au compartiment	Oui.
s3:GetBucketLocation	ACCÉDER à l'emplacement du compartiment	
s3:GetBucketMetadatanotification	CONFIGURATION DES notifications de métadonnées de compartiment	Oui.
s3:GetBuckenotification	GET Bucket notification	
s3:GetBuckeObjectLockConfiguration	OBTENIR la configuration de verrouillage d'objet	
s3:GetBucketPolicy	GET Bucket policy	

Autorisations	OPÉRATIONS DES API REST S3	Personnalisée pour StorageGRID
s3:GetBucketTagging	GET Bucket tagging	
s3:GetBucketVersioning	GESTION des versions des compartiments	
s3:GetLifecyclConfiguration	OPTIMISEZ le cycle de vie des compartiments	
s3:GetReplicationTM	RÉPLICATION des compartiments	
s3:ListAllMyseaux	• ACCÉDER au service • DÉCOUVREZ l'utilisation du stockage	Oui, pour BÉNÉFICIER DE l'utilisation DU stockage
s3:ListBucket	• OBTENIR le compartiment (liste d'objets) • Godet DE TÊTE • Restauration POST-objet	
s3:ListBuckMultipartUploads	• Liste des téléchargements partitionnés • Restauration POST-objet	
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	• SUPPRIMER les godets† • PLACEZ les godets	
s3:PutEncryptionConfiguration	• SUPPRIMER le chiffrement du compartiment • PUT Bucket Encryption	
s3:PutBuckeLastAccessTime	METTRE l'heure du dernier accès au compartiment	Oui.

Autorisations	OPÉRATIONS DES API REST S3	Personnalisée pour StorageGRID
s3:PutBuckeMetadanotification	CONFIGURATION de notification des métadonnées de compartiment	Oui.
s3:PutBuckenotification	PUT Bucket notification	
s3:PutBuckObjectLockConfiguration	PLACEZ le godet avec le `x-amz-bucket-object-lock-enabled: true` En-tête de demande (nécessite également l'autorisation s3:CreateBucket)	
s3:PutBuckePolicy	PUT Bucket policy	
s3:PutBuckeTagging	• SUPPRIMER le marquage du compartiment† • PUT Bucket tagging	
s3:PutBuckeVersioning	GESTION des versions du compartiment	
s3:PutLifecyclConfiguration	• SUPPRIMER le cycle de vie du godet† • CYCLE de vie des compartiments	
s3:PutReplicationTM	RÉPLICATION des compartiments	Oui, séparer les autorisations pour PUT et DELETE*

Autorisations qui s'appliquent aux objets

Autorisations	OPÉRATIONS DES API REST S3	Personnalisée pour StorageGRID
s3:AbortMultipartUpload	• Abandonner le téléchargement de pièces multiples • Restauration POST-objet	
s3:DeleteObject	• SUPPRIMER l'objet • SUPPRIMER plusieurs objets • Restauration POST-objet	
s3:DeleteObjectTagging	SUPPRIMER le balisage d'objets	
s3:DeleteObjectVersionTagging	SUPPRIMER le balisage d'objets (une version spécifique de l'objet)	

Autorisations	OPÉRATIONS DES API REST S3	Personnalisée pour StorageGRID
s3:DeleteObjectVersion	SUPPRIMER l'objet (une version spécifique de l'objet)	
s3:GetObject	• OBTENIR l'objet • Objet TÊTE • Restauration POST-objet	
s3:GetObjectAcl	OBTENIR l'ACL d'objet	
s3:GetObjectLegalHold	OBTENIR la mise en attente légale de l'objet	
s3:GetObjectRetention	OBTENIR la conservation des objets	
s3:GetObjectTagging	OBTENIR le balisage d'objets	
s3:GetObjectVersionTagging	OBTENIR le balisage d'objets (une version spécifique de l'objet)	
s3:GetObjectVersion	OBTENIR objet (une version spécifique de l'objet)	
s3:ListMultipartUploadParts	Répertorier les pièces, POST-restauration d'objet	
s3:PutObject	• PLACER l'objet • PLACER l'objet - Copier • Restauration POST-objet • Lancer le téléchargement de pièces multiples • Chargement de pièces multiples complet • Télécharger la pièce • Télécharger la pièce - Copier	
s3:PutObjectLegalHold	METTRE l'objet en attente légale	
s3:PutObjectRetention	CONSERVATION des objets	
s3:PutObjectTagging	PLACER le balisage d'objets	

Autorisations	OPÉRATIONS DES API REST S3	Personnalisée pour StorageGRID
s3:PutObjectVersionTagging	PUT Object Tagging (une version spécifique de l'objet)	
s3:PutOverwriteObject	• PLACER l'objet • PLACER l'objet - Copier • PUT Object tagging • SUPPRIMER le balisage d'objets • Chargement de pièces multiples complet	Oui.
s3:RestoreObject	Restauration POST-objet	

Utilisation de 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, 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 PUT Object tagging ou DELETE Object tagging 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 politique S3 actuelle autorise le remplacement et que l'autorisation PutOverwriteObject est définie sur Deny, le client ne peut pas remplacer les données d'un objet, les métadonnées définies par l'utilisateur ou le balisage d'objets. En outre, si la case **empêcher modification client** est cochée (**Configuration** > **Options de grille**), ce paramètre remplace le paramètre de l'autorisation PutOverwriteObject.

Informations associées

"Exemples de règles de groupe S3"

Spécification de conditions dans une règle

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: {
     <em>condition_type</em>: {
          <em>condition_key</em>: <em>condition_values</em>
```

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).

Opérateurs de condition	Description
StringLike	Compare une clé à une valeur de chaîne en fonction de la correspondance exacte (sensible à la casse). Peut inclure * et ? caractères génériques.
StringNotLike	Compare une clé à une valeur de chaîne basée sur la correspondance niée (sensible à la casse). Peut inclure * et ? caractères génériques.
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 clé à une valeur numérique basée sur la comparaison « supérieure à ».
NumericGreaterThanEquals	Compare une clé à une valeur numérique basée sur la comparaison « supérieure ou égale ».
NumericLessThan	Compare une clé à une valeur numérique basée sur la comparaison « moins que ».
NumericLessThanEquals	Compare une clé à une valeur numérique basée sur la comparaison « inférieure à ou égale ».
BOOL	Compare une clé à une valeur booléenne basée sur la 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

Catégorie	Touches de condition applicables	Description
Opérateurs IP	aws:SourceIp	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. Toutes `X-Forwarded-For` le cueilleur sera ignoré car sa validité ne peut pas être vérifiée.
Ressource/identité	aws:nom d'utilisateur	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:ListBucket et S3:permissions ListBuckeVersions	s3:délimiteur	Compare avec le paramètre de délimiteur spécifié dans une demande GET Bucket ou GET Bucket Object versions.
S3:ListBucket et S3:permissions ListBuckeVersions	s3:touches max	Compare au paramètre max-keys spécifié dans une demande GET Bucket ou GET Bucket Object versions.
S3:ListBucket et S3:permissions ListBuckeVersions	s3:préfixe	Compare au paramètre de préfixe spécifié dans une demande GET Bucket ou GET Bucket Object versions.

Spécification des variables dans 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 règle dans le `Resource` comparaisons d'éléments et de chaînes dans `Condition` elément.

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 littéral ? caractère.
`${$}`	Caractère spécial. Utilise le caractère comme caractère littéral $.

Création de 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
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

Description de la politique	Type de règle	Comportement Amazon	Comportement de StorageGRID
La ressource est un compartiment S3 inexistant	Groupe	Valide	Identique
Principal est un groupe local	Godet	Principal non valide	Valide
La police accorde à un compte non propriétaire (y compris les comptes anonymes) des autorisations pour METTRE 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** > **Options de grille**, 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.
  - Ajouter une opération D'AUTORISATION PLACER l'objet à la règle S3.

> La définition de DeleteObject sur DENY dans une politique 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 règles 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 avec ILM"

"Création de règles nécessitant une gestion spéciale"

"Gestion des objets par les règles StorageGRID ILM"

"Exemples de règles de groupe S3"

Exemples de règles S3

Utilisez les exemples de cette section pour créer des règles d'accès StorageGRID pour les compartiments et les groupes.

Exemples de règles de compartiment S3

Les politiques de compartiment spécifient les autorisations d'accès pour le compartiment à lequel la politique est attachée. Les règles de compartiment sont configurées à l'aide de l'API S3 PutBuckPolicy.

Il est possible de configurer une politique de compartiment à l'aide de l'interface de ligne de commandes AWS, comme indiqué dans la commande suivante :

```
> aws s3api put-bucket-policy --bucket examplebucket --policy
<em>file://policy.json</em>
```

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 lister les objets dans le compartiment et à effectuer des opérations get Object sur tous les objets du compartiment. Toutes les autres opérations seront refusées. Notez que cette politique n'est peut-être pas particulièrement utile, car personne, à l'exception de la racine du compte, ne dispose d'autorisations pour 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 peut accéder intégralement à un compartiment, tandis que les utilisateurs d'un autre compte spécifié ne sont autorisés qu'à répertorier le compartiment et 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 GET Object sur tous les objets du compartiment, tandis que seuls les utilisateurs appartenant au groupe `Marketing` le compte spécifié est autorisé à accéder pleinement.

```
{
  "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 pleinement au `examplebucket` le godet et 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, le `Deny` Effet pour 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'objets 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/*"
    }
  ]
}
```

Informations associées

"Opérations sur les compartiments"

Exemples de règles de groupe S3

Les stratégies de groupe spécifient les autorisations d'accès pour le groupe auquel la stratégie est associée. Il n'y a pas de `Principal` élément de la politique car il est implicite. Les règles de groupe sont configurées à l'aide du Gestionnaire de locataires ou de l'API.

Exemple : définition de la stratégie de groupe à l'aide du Gestionnaire de tenant

Lorsque vous utilisez le Gestionnaire de locataires pour ajouter ou modifier un groupe, vous pouvez sélectionner la manière dont vous souhaitez créer la stratégie de groupe qui définit les autorisations d'accès S3 dont les membres de ce groupe auront, comme suit :

- **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.
- **Custom** : les utilisateurs du groupe disposent des autorisations que vous spécifiez dans la zone de texte.

  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.

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 : permettre aux membres du groupe d'accéder pleinement 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}/*"
    }
  ]
}
```

Informations associées

"Utilisez un compte de locataire"

"Utilisation de l'autorisation PutOverwriteObject"

"Protection WORM (Write-once, Read-many)"

Configuration de la sécurité pour l'API REST

Il est recommandé de passer en revue les mesures de sécurité mises en œuvre pour l'API REST et de comprendre comment sécuriser votre système.

Comment StorageGRID assure la sécurité pour l'API REST

Vous devez comprendre comment le système StorageGRID implémente la sécurité, l'authentification et l'autorisation pour l'API REST.

StorageGRID utilise les mesures de sécurité suivantes.

- Les communications client avec le service Load Balancer utilisent HTTPS si HTTPS est configuré pour le noeud final Load Balancer.

  Lorsque vous configurez un point final d'équilibreur de charge, HTTP peut éventuellement être activé. Par exemple, vous pouvez utiliser HTTP à des fins de test ou autres que la production. Pour plus d'informations, reportez-vous aux instructions d'administration de StorageGRID.

- Par défaut, StorageGRID utilise HTTPS pour les communications client avec les nœuds de stockage et le service CLB sur les nœuds de passerelle.

  HTTP peut éventuellement être activé pour ces connexions. Par exemple, vous pouvez utiliser HTTP à des fins de test ou autres que la production. Pour plus d'informations, reportez-vous aux instructions d'administration de StorageGRID.

  Le service CLB est obsolète.

- Les communications entre StorageGRID et le client sont chiffrées à l'aide de TLS.
- Les communications entre le service Load Balancer et les nœuds de stockage dans la grille sont cryptées que le terminal de l'équilibreur de charge soit configuré pour accepter les connexions HTTP ou HTTPS.
- Les clients doivent fournir des en-têtes d'authentification HTTP à StorageGRID pour effectuer des opérations d'API REST.

Certificats de sécurité et applications client

Les clients peuvent se connecter au service Load Balancer sur les nœuds de passerelle ou les nœuds d'administration, directement aux nœuds de stockage ou au service CLB sur les nœuds de passerelle.

Dans tous les cas, les applications client peuvent établir des connexions TLS à l'aide d'un certificat de serveur personnalisé chargé par l'administrateur de la grille ou d'un certificat généré par le système StorageGRID :

- Lorsque les applications client se connectent au service Load Balancer, elles le font à l'aide du certificat configuré pour le noeud final de l'équilibreur de charge spécifique utilisé pour établir la connexion. Chaque noeud final possède son propre certificat, qui est soit un certificat de serveur personnalisé chargé par l'administrateur de la grille, soit un certificat que l'administrateur de la grille a généré dans StorageGRID lors de la configuration du noeud final.
- Lorsque les applications client se connectent directement à un nœud de stockage ou au service CLB des nœuds de passerelle, elles utilisent soit les certificats de serveur générés par le système pour les nœuds de stockage lorsque le système StorageGRID a été installé (qui sont signés par l'autorité de certification du système), ou un seul certificat de serveur personnalisé fourni par un administrateur de grid pour la grille.

Les clients doivent être configurés pour approuver l'autorité de certification qui a signé le certificat qu'ils utilisent pour établir des connexions TLS.

Pour plus d'informations sur la configuration des noeuds finaux de l'équilibreur de charge et pour obtenir des instructions sur l'ajout d'un certificat de serveur personnalisé pour les connexions TLS directement aux noeuds de stockage ou au service CLB sur les noeuds de passerelle, reportez-vous aux instructions de la section Administration de StorageGRID.

Récapitulatif

Le tableau suivant montre comment les problèmes de sécurité sont implémentés dans les API REST S3 et Swift :

Problème de sécurité	Implémentation pour l'API REST
Sécurité de la connexion	TLS

Problème de sécurité	Implémentation pour l'API REST
Authentification du serveur	Certificat de serveur X.509 signé par l'autorité de certification du système ou certificat de serveur personnalisé fourni par l'administrateur
Authentification client	• S3 : compte S3 (ID de clé d'accès et clé d'accès secrète) • SWIFT : compte Swift (nom d'utilisateur et mot de passe)
Autorisation du client	• S3 : propriété des compartiments et toutes les règles de contrôle d'accès applicables • SWIFT : accès aux rôles d'administrateur

Informations associées

"Administrer StorageGRID"

Algorithmes de hachage et de cryptage pris en charge pour les bibliothèques TLS

Le système StorageGRID prend en charge un ensemble limité de suites de chiffrement que les applications clientes peuvent utiliser lors de l'établissement d'une session TLS (transport Layer Security).

Versions supportées de TLS

StorageGRID supporte TLS 1.2 et TLS 1.3.

SSLv3 et TLS 1.1 (ou versions antérieures) ne sont plus pris en charge.

Suites de chiffrement prises en charge

Version TLS	Nom IANA de la suite de chiffrement
1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
1.2	TLS_ECDHE_RSA_WITH_CHA20_POLY1305_SHA256
1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
1.3	TLS_AES_256_GCM_SHA384
1.3	TLS_CHA20_POLY1305_SHA256
1.3	TLS_AES_128_GCM_SHA256

Suites de chiffrement obsolètes

Les suites de chiffrement suivantes sont obsolètes. La prise en charge de ces chiffrements sera supprimée dans une prochaine version.

Nom IANA
TLS_RSA_WAS_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384

Informations associées

"Configuration des connexions client"

Surveillance et audit des opérations

Vous pouvez surveiller les charges de travail et l'efficacité des opérations client en visualisant les tendances de transaction pour l'ensemble du grid ou pour des nœuds spécifiques. Vous pouvez utiliser des messages d'audit pour surveiller les opérations et les transactions des clients.

- "Contrôle des taux d'entrée et de récupération des objets"
- "Accès aux journaux d'audit et vérification"

Contrôle des taux d'entrée et de récupération des objets

Vous pouvez surveiller les taux d'entrée et de récupération des objets, ainsi que les mesures relatives au nombre d'objets, aux requêtes et à la vérification. Vous pouvez afficher le nombre de tentatives de lecture, d'écriture et de modification d'objets du système StorageGRID ayant échoué et réussies par les applications client.

Étapes

1. Connectez-vous au Grid Manager à l'aide d'un navigateur pris en charge.
2. Dans le tableau de bord, recherchez la section opérations de protocole.

   Cette section récapitule le nombre d'opérations client effectuées par votre système StorageGRID. La moyenne des débits de protocole est calculée au cours des deux dernières minutes.

3. Sélectionnez **noeuds**.
4. Dans la page d'accueil noeuds (niveau de déploiement), cliquez sur l'onglet **Load Balancer**.

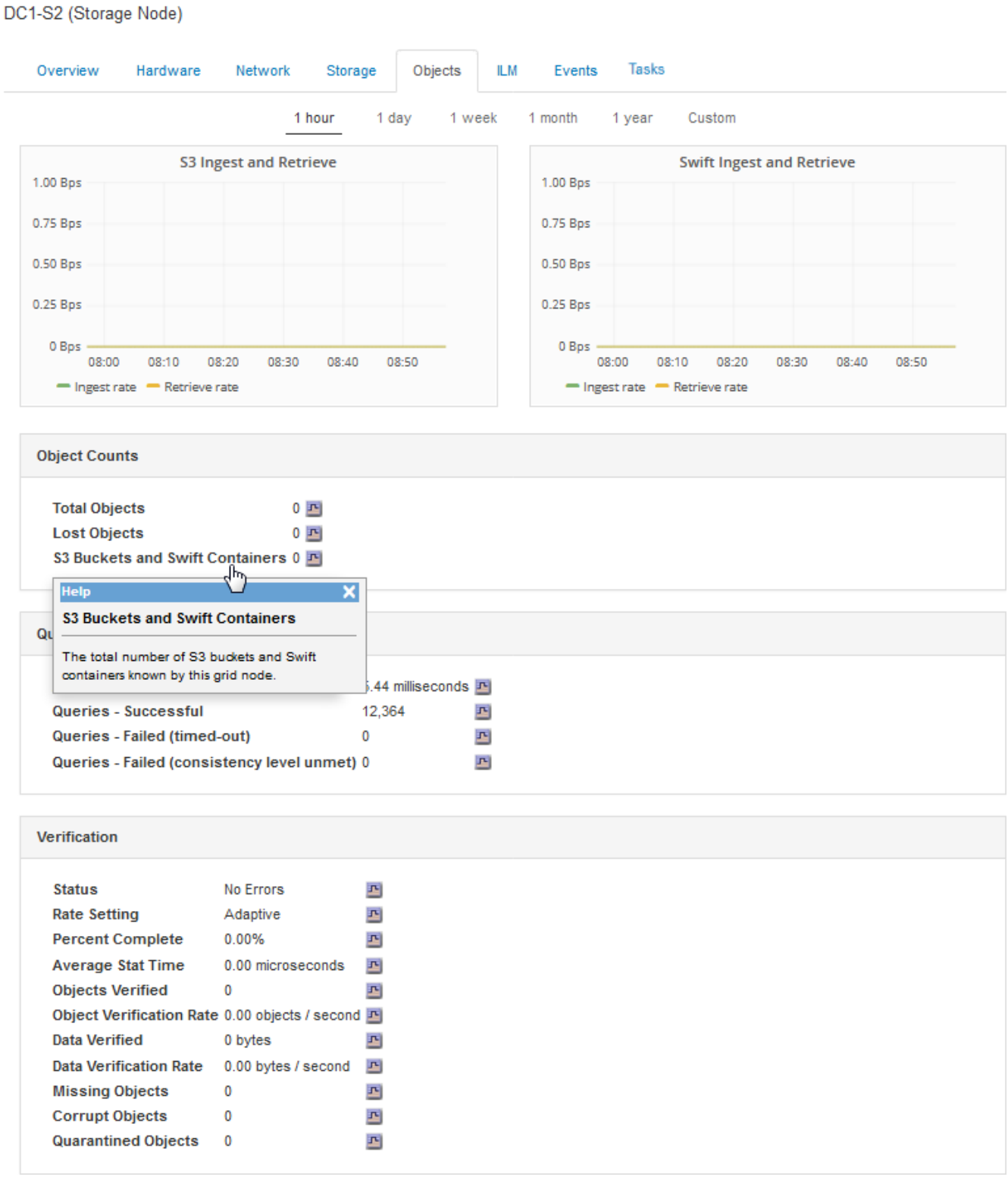
   Les graphiques présentent les tendances de tout le trafic client dirigé vers les terminaux d'équilibreur de charge dans la grille. Vous pouvez sélectionner un intervalle de temps en heures, jours, semaines, mois ou années, vous pouvez également appliquer un intervalle personnalisé.

5. Dans la page d'accueil noeuds (niveau de déploiement), cliquez sur l'onglet **objets**.

   Le graphique montre les taux d'entrée et de récupération de l'intégralité de votre système StorageGRID en octets par seconde et en octets totaux. Vous pouvez sélectionner un intervalle de temps en heures, jours, semaines, mois ou années, vous pouvez également appliquer un intervalle personnalisé.

6. Pour afficher les informations relatives à un noeud de stockage particulier, sélectionnez-le dans la liste de gauche, puis cliquez sur l'onglet **objets**.

   Le tableau affiche les taux d'entrée et de récupération de l'objet pour ce nœud de stockage. L'onglet inclut également des mesures pour le nombre d'objets, les requêtes et la vérification. Vous pouvez cliquer sur les étiquettes pour afficher les définitions de ces mesures.



7. Si vous voulez encore plus de détails :

a. Sélectionnez **support** > **Outils** > **topologie de grille**.
b. Sélectionnez ***site*** > **Présentation** > **main**.

   La section opérations d'API affiche un récapitulatif des informations sur l'ensemble de la grille.

c. Sélectionnez ***Storage Node*** > **LDR** > ***client application*** > **Présentation** > **main**

   La section opérations affiche un récapitulatif des informations sur le nœud de stockage sélectionné.

Accès aux journaux d'audit et vérification

Les messages d'audit sont générés par les services StorageGRID et stockés dans des fichiers journaux texte. Des messages d'audit spécifiques aux API dans les journaux d'audit fournissent des données stratégiques de sécurité, d'exploitation et de surveillance des performances qui vous aideront à évaluer l'état de votre système.

Ce dont vous avez besoin

- Vous devez disposer d'autorisations d'accès spécifiques.
- Vous devez avoir le `Passwords.txt` fichier.
- Vous devez connaître l'adresse IP d'un nœud d'administration.

Description de la tâche

Le fichier journal d'audit actif est nommé `audit.log`, Et il est stocké sur des nœuds d'administration.

Une fois par jour, le fichier audit.log actif est enregistré, et un nouveau `audit.log` le fichier est démarré. Le nom du fichier enregistré indique quand il a été enregistré, au format *`yyyy-mm-dd.txt`*.

Après un jour, le fichier enregistré est compressé et renommé, au format *`yyyy-mm-dd.txt.gz`*, qui conserve la date originale.

Cet exemple montre l'actif `audit.log` fichier du jour précédent (`2018-04-15.txt`), et le fichier compressé pour la veille (`2018-04-14.txt.gz`).

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

Étapes

1. Connectez-vous à un nœud d'administration :
   a. Saisissez la commande suivante :
      `ssh admin@`*`primary_Admin_Node_IP`*
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
2. Accédez au répertoire contenant les fichiers journaux d'audit :

```
cd /var/local/audit/export
```

3. Afficher le fichier journal d'audit actuel ou enregistré, selon les besoins.

Opérations S3 suivies dans les journaux d'audit

Plusieurs opérations de compartiment et les opérations d'objets sont suivies dans les journaux d'audit de StorageGRID.

Les opérations des compartiments sont suivies dans les journaux d'audit

- SUPPRIMER le compartiment
- SUPPRIMER le balisage du compartiment
- SUPPRIMER plusieurs objets
- OBTENIR le compartiment (liste d'objets)
- OBTENIR les versions d'objet de compartiment
- GET Bucket tagging
- Godet DE TÊTE
- PLACER le godet
- METTEZ le godet en conformité
- PUT Bucket tagging
- GESTION des versions du compartiment

Opérations d'objet suivies dans les journaux d'audit

- Chargement de pièces multiples complet
- Télécharger une pièce (lorsque la règle ILM utilise des comportements d'entrée stricts ou équilibrés)
- Télécharger une pièce : copie (lorsque la règle ILM utilise des comportements d'entrée stricts ou équilibrés)
- SUPPRIMER l'objet
- OBTENIR l'objet
- Objet TÊTE
- Restauration POST-objet
- PLACER l'objet
- PLACER l'objet - Copier

Informations associées

"Opérations sur les compartiments"

"Opérations sur les objets"

Avantages des connexions HTTP actives, inactives et simultanées

La configuration des connexions HTTP peut avoir un impact sur les performances du système StorageGRID. Les configurations varient selon que la connexion HTTP est active ou inactive ou si vous avez simultanément plusieurs connexions.

Vous pouvez identifier les avantages en termes de performances pour les types de connexions HTTP suivants :

- Connexions HTTP inactives
- Connexions HTTP actives
- Connexions HTTP simultanées

Informations associées

- "Avantages de maintenir les connexions HTTP inactives ouvertes"
- "Avantages des connexions HTTP actives"
- "Avantages des connexions HTTP simultanées"
- "Séparation des pools de connexions HTTP pour les opérations de lecture et d'écriture"

Avantages de maintenir les connexions HTTP inactives ouvertes

Vous devez maintenir les connexions HTTP ouvertes même lorsque les applications client sont inactives pour permettre aux applications client d'effectuer les transactions suivantes sur la connexion ouverte. En fonction des mesures du système et de l'expérience d'intégration, vous devez garder une connexion HTTP inactive ouverte pendant 10 minutes maximum. StorageGRID peut fermer automatiquement une connexion HTTP qui reste ouverte et inactive pendant plus de 10 minutes.

Les connexions HTTP ouvertes et inactives offrent les avantages suivants :

- Réduction de la latence entre le moment où le système StorageGRID détermine qu'il doit effectuer une transaction HTTP et le moment où le système StorageGRID peut effectuer la transaction

  La réduction de la latence constitue l'avantage principal, notamment pour la durée nécessaire à l'établissement des connexions TCP/IP et TLS.

- Augmentation de la vitesse de transfert des données en amorçant l'algorithme TCP/IP à démarrage lent avec des transferts effectués précédemment
- Notification instantanée de plusieurs classes de conditions de défaillance qui interrompent la connectivité entre l'application cliente et le système StorageGRID

Déterminer la durée d'ouverture d'une connexion inactive est un compromis entre les avantages du démarrage lent associés à la connexion existante et l'affectation idéale de la connexion aux ressources système internes.

Avantages des connexions HTTP actives

Pour les connexions directement aux nœuds de stockage ou au service CLB (obsolète) sur les nœuds de passerelle, vous devez limiter la durée d'une connexion HTTP active à un maximum de 10 minutes, même si la connexion HTTP effectue en continu des transactions.

La détermination de la durée maximale pendant laquelle une connexion doit être maintenue ouverte est un compromis entre les avantages de la persistance de connexion et l'allocation idéale de la connexion aux ressources système internes.

Pour les connexions client aux nœuds de stockage ou au service CLB, la limitation des connexions HTTP

actives offre les avantages suivants :

- Équilibrage optimal de la charge sur l'ensemble du système StorageGRID.

  Lors de l'utilisation du service CLB, vous devez empêcher les connexions TCP/IP de longue durée afin d'optimiser l'équilibrage de la charge sur le système StorageGRID. Vous devez configurer les applications client pour suivre la durée de chaque connexion HTTP et fermer la connexion HTTP après un délai défini afin que la connexion HTTP puisse être rétablie et rééquilibrée.

  Le service CLB équilibre la charge dans le système StorageGRID au moment où une application client établit une connexion HTTP. Avec le temps, une connexion HTTP pourrait ne plus être optimale au fur et à mesure que les besoins en équilibrage de la charge évoluent. Le système réalise son meilleur équilibrage de charge lorsque les applications client établissent une connexion HTTP distincte pour chaque transaction, mais cela annule les gains les plus importants associés aux connexions persistantes.

  Le service CLB est obsolète.

- Permet aux applications clientes de diriger des transactions HTTP vers des services LDR qui ont de l'espace disponible.
- Permet de démarrer les procédures de maintenance.

  Certaines procédures de maintenance ne démarrent qu'une fois toutes les connexions HTTP en cours terminées.

Pour les connexions client au service Load Balancer, limiter la durée des connexions ouvertes peut être utile pour permettre le démarrage rapide de certaines procédures de maintenance. Si la durée des connexions client n'est pas limitée, l'arrêt automatique des connexions actives peut prendre plusieurs minutes.

Avantages des connexions HTTP simultanées

Vous devez maintenir plusieurs connexions TCP/IP ouvertes au système StorageGRID pour permettre le parallélisme, ce qui augmente les performances. Le nombre optimal de connexions parallèles dépend de divers facteurs.

Les connexions HTTP simultanées offrent les avantages suivants :

- Latence réduite

  Les transactions peuvent commencer immédiatement au lieu d'attendre que d'autres transactions soient effectuées.

- Rendement accru

  Le système StorageGRID peut effectuer des transactions parallèles et augmenter le débit des transactions globales.

Les applications client doivent établir plusieurs connexions HTTP. Lorsqu'une application client doit effectuer une transaction, elle peut sélectionner et utiliser immédiatement toute connexion établie qui ne traite pas actuellement une transaction.

Le débit maximal de chaque topologie de chaque système StorageGRID est différent pour les transactions et les connexions simultanées, avant que les performances ne commencent à se dégrader. Le pic de débit dépend de facteurs tels que les ressources informatiques, les ressources réseau, les ressources de stockage

et les liaisons WAN. Des facteurs sont également pris en charge par le nombre de serveurs et de services, ainsi que par le nombre d'applications prises en charge par le système StorageGRID.

Les systèmes StorageGRID prennent souvent en charge plusieurs applications client. Vous devez garder cela à l'esprit lorsque vous déterminez le nombre maximal de connexions simultanées utilisées par une application client. Si l'application client se compose de plusieurs entités logicielles qui établissent chacune des connexions avec le système StorageGRID, vous devez ajouter toutes les connexions entre les entités. Vous devrez peut-être régler le nombre maximal de connexions simultanées dans les situations suivantes :

- La topologie du système StorageGRID affecte le nombre maximal de transactions et de connexions simultanées pris en charge par le système.
- Les applications client qui interagissent avec le système StorageGRID sur un réseau avec une bande passante limitée peuvent être contraintes de réduire le niveau de simultanéité pour s'assurer que les transactions individuelles sont effectuées dans un délai raisonnable.
- Lorsque de nombreuses applications client partagent le système StorageGRID, il peut être nécessaire de réduire le degré de simultanéité pour ne pas dépasser les limites du système.

Séparation des pools de connexions HTTP pour les opérations de lecture et d'écriture

Vous pouvez utiliser des pools séparés de connexions HTTP pour les opérations en lecture et écriture, et contrôler la proportion que vous souhaitez utiliser pour chacun d'eux. Le recours à des pools séparés de connexions HTTP vous permet de contrôler les transactions et d'équilibrer la charge plus efficacement.

Les applications client peuvent créer des chargements qui sont dominants par la récupération (lecture) ou dominants par le stockage (écriture). Grâce à des pools séparés de connexions HTTP pour les transactions en lecture et écriture, vous pouvez ajuster la quantité de chaque pool à dédier pour les transactions en lecture ou en écriture.

Utiliser Swift

Découvrez comment les applications client peuvent utiliser l'API OpenStack Swift pour interagir avec le système StorageGRID.

- "Prise en charge de l'API OpenStack Swift dans StorageGRID"
- "Configuration des comptes et des connexions des locataires"
- "Opérations prises en charge par l'API REST Swift"
- "Opérations de l'API REST StorageGRID Swift"
- "Configuration de la sécurité pour l'API REST"
- "Surveillance et audit des opérations"

Prise en charge de l'API OpenStack Swift dans StorageGRID

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

Élément	Version
Spécification SWIFT	OpenStack Swift Object Storage API v1 depuis novembre 2015
HTTP	1.1 pour plus d'informations sur HTTP, consultez le document HTTP/1.1 (RFC 7230-35). **Remarque**: StorageGRID ne prend pas en charge HTTP/1.1 pipeline.

Informations associées

"OpenStack : API de stockage objet"

Historique de la prise en charge de l'API Swift dans StorageGRID

Notez que des modifications ont été apportées à la prise en charge du système StorageGRID pour l'API REST Swift.

Relâchez	Commentaires
11.5	Suppression du contrôle de cohérence faible Le niveau de cohérence disponible sera utilisé à la place.
11.4	Ajout de la prise en charge de TLS 1.3 et mise à jour de la liste des suites de chiffrement TLS prises en charge. CLB est obsolète. Ajout d'une description de l'interrelation entre ILM et paramètre de cohérence.
11.3	Les opérations PUT mises à jour décrivent l'impact des règles ILM qui utilisent le placement synchrone à l'ingestion (options équilibrées et strictes pour le comportement d'ingestion). Ajout d'une description des connexions client qui utilisent des noeuds finaux d'équilibreur de charge ou des groupes de haute disponibilité. Liste mise à jour des suites de chiffrement TLS prises en charge. Les chiffrements TLS 1.1 ne sont plus pris en charge.
11.2	Modifications rédactionnelles mineures apportées au document
11.1	Ajout de la prise en charge de l'utilisation des connexions client HTTP pour Swift aux nœuds de la grille. Mise à jour des définitions des contrôles de cohérence.
11.0	Ajout de la prise en charge de 1,000 conteneurs pour chaque compte locataire.

Relâchez	Commentaires
10.3	Mises à jour administratives et corrections du document. Suppression des sections pour la configuration des certificats de serveur personnalisés.
10.2	Prise en charge initiale de l'API Swift par le système StorageGRID. La version actuellement prise en charge est l'API de stockage objet OpenStack Swift v1.

Comment StorageGRID implémente l'API REST Swift

Une application client peut utiliser les appels de l'API REST Swift pour se connecter aux nœuds de stockage et aux nœuds de passerelle afin de créer des conteneurs et de stocker et récupérer des objets. Les applications orientées services développées pour OpenStack Swift peuvent ainsi se connecter au stockage objet sur site fourni par le système StorageGRID.

Gestion des objets Swift

À l'entrée des objets Swift dans le système StorageGRID, ils sont gérés par les règles de gestion du cycle de vie des informations de la politique ILM active du système. Les règles et règles ILM déterminent la façon dont StorageGRID crée et distribue des copies de données d'objet ainsi que la façon dont elles gèrent ces copies au fil du temps. Par exemple, une règle ILM peut s'appliquer aux objets de conteneurs Swift spécifiques et peut spécifier que plusieurs copies d'objets seront enregistrées dans plusieurs data centers pendant un certain nombre d'années.

Contactez votre administrateur StorageGRID si vous avez besoin de savoir comment les règles et règles ILM du grid affectent les objets de votre compte de locataire Swift.

Requêtes des clients en conflit

Les demandes contradictoires des clients, telles que deux clients qui écrivent sur la même clé, sont résolues sur la base des « derniers-victoires ». Le calendrier de l'évaluation « derniers-victoires » est basé sur le moment où le système StorageGRID remplit une demande donnée et non sur le moment où les clients Swift démarrent une opération.

Garanties et contrôles de cohérence

Par défaut, StorageGRID fournit une cohérence de lecture après écriture pour les objets nouvellement créés et une cohérence éventuelle pour les mises à jour et les OPÉRATIONS HEAD d'objet. 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.

StorageGRID vous permet également de contrôler la cohérence par conteneur. Vous pouvez modifier le contrôle de cohérence pour assurer une reprise entre la disponibilité des objets et la cohérence de ces objets sur plusieurs nœuds et sites de stockage, selon les besoins de votre application.

Informations associées

"Gestion des objets avec ILM"

"DEMANDE DE cohérence du conteneur"

"REQUÊTE de cohérence du conteneur"

Recommandations pour la mise en œuvre de l'API REST Swift

Suivez ces recommandations lors de la mise en œuvre de l'API REST Swift pour une utilisation avec StorageGRID.

Recommandations pour les têtes à des objets inexistants

Si votre application vérifie régulièrement si un objet existe sur un chemin où vous ne vous attendez pas à ce que l'objet existe réellement, vous devez utiliser le contrôle de cohérence « disponible ». Par exemple, vous devez utiliser le contrôle de cohérence « disponible » si votre application effectue une opération DE TÊTE à un emplacement avant d'effectuer une opération DE MISE à cet emplacement.

Sinon, si l'opération HEAD ne trouve pas l'objet, vous pouvez recevoir un nombre élevé de 500 erreurs de serveur interne si un ou plusieurs nœuds de stockage ne sont pas disponibles.

Vous pouvez définir le contrôle de cohérence « disponible » pour chaque conteneur à l'aide de la demande DE cohérence DU conteneur PUT.

Recommandations pour les noms d'objet

Vous ne devez pas utiliser de valeurs aléatoires comme les quatre premiers caractères des noms d'objets. Au lieu de cela, vous devez utiliser des préfixes non aléatoires et non uniques, tels que l'image.

Si vous avez besoin d'utiliser des caractères aléatoires et uniques dans les préfixes de nom d'objet, vous devez préfixer les noms d'objet avec un nom de répertoire. C'est-à-dire, utilisez le format suivant :

```
mycontainer/mydir/f8e3-image3132.jpg
```

Au lieu de ce format :

```
mycontainer/f8e3-image3132.jpg
```

Recommandations pour « plages de lectures »

Si l'option **Compress emmagased Objects** est sélectionnée (**Configuration** > **Paramètres système** > **Grid Options**), les applications client Swift doivent éviter d'effectuer des opérations GET object spécifiant une plage d'octets à renvoyer. Ces opérations de « lecture à plage » sont inefficaces, car StorageGRID doit décompresser efficacement les objets pour accéder aux octets demandés. LES opérations GET Object qui demandent une petite plage d'octets provenant d'un objet très volumineux sont particulièrement inefficaces. Par exemple, il est très 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.

Informations associées

"DEMANDE DE cohérence du conteneur"

"REQUÊTE de cohérence du conteneur"

"Administrer StorageGRID"

Configuration des comptes et des connexions des locataires

Pour configurer StorageGRID pour accepter les connexions à partir des applications client, vous devez créer un ou plusieurs comptes de tenant et configurer les connexions.

Création et configuration de comptes de tenant Swift

Un compte de locataire Swift est requis pour que les clients de l'API Swift puissent stocker et récupérer des objets sur StorageGRID. Chaque compte de locataire possède son propre ID de compte, groupes et utilisateurs, ainsi que des conteneurs et des objets.

Les comptes de locataires Swift sont créés par un administrateur StorageGRID GRID à l'aide de Grid Manager ou de l'API de gestion du grid.

Lors de la création d'un compte de locataire Swift, l'administrateur du grid spécifie les informations suivantes :

- Nom d'affichage du locataire (l'ID de compte du locataire est attribué automatiquement et ne peut pas être modifié)
- Éventuellement, un quota de stockage pour le compte du locataire, soit le nombre maximal de gigaoctets, téraoctets ou pétaoctets disponibles pour les objets du locataire. Le quota de stockage d'un locataire représente une quantité logique (taille d'objet), et non une quantité physique (taille sur disque).
- Si l'authentification unique (SSO) n'est pas utilisée pour le système StorageGRID, que le compte de tenant utilise son propre référentiel d'identité ou partage le référentiel d'identité de la grille et le mot de passe initial de l'utilisateur racine local du locataire.
- Si SSO est activé, quel groupe fédéré dispose d'une autorisation d'accès racine pour configurer le compte locataire.

Après la création d'un compte de locataire Swift, les utilisateurs disposant de l'autorisation accès racine peuvent accéder au Gestionnaire de locataires pour effectuer les tâches suivantes :

- Configuration de la fédération des identités (sauf si le référentiel d'identité est partagé avec la grille) et création de groupes et d'utilisateurs locaux
- Contrôle de l'utilisation du stockage

> Les utilisateurs Swift doivent disposer de l'autorisation d'accès racine pour accéder au gestionnaire de locataires. Toutefois, l'autorisation accès racine ne permet pas aux utilisateurs de s'authentifier auprès de l'API REST Swift pour créer des conteneurs et ingérer des objets. Les utilisateurs doivent disposer de l'autorisation Administrateur Swift pour s'authentifier dans l'API REST de Swift.

Informations associées

"Administrer StorageGRID"

"Utilisez un compte de locataire"

"Terminaux API Swift pris en charge"

Configuration des connexions client

Un administrateur du grid fait des choix de configuration qui affectent la manière dont les clients Swift se connectent à StorageGRID pour stocker et récupérer les données. Les informations spécifiques dont vous avez besoin pour établir une connexion dépendent de la configuration choisie.

Les applications client peuvent stocker ou récupérer des objets en se connectant à l'un des éléments suivants :

- Le service Load Balancer sur les nœuds d'administration ou de passerelle, ou, le cas échéant, l'adresse IP virtuelle d'un groupe de nœuds d'administration ou de nœuds de passerelle haute disponibilité
- Le service CLB sur les nœuds de passerelle ou, éventuellement, l'adresse IP virtuelle d'un groupe de nœuds de passerelle haute disponibilité

> Le service CLB est obsolète. Les clients configurés avant la version de StorageGRID 11.3 peuvent continuer à utiliser le service CLB sur les nœuds de passerelle. Toutes les autres applications client qui dépendent de StorageGRID pour fournir un équilibrage de la charge doivent se connecter à l'aide du service Load Balancer.

- Des nœuds de stockage, avec ou sans équilibreur de charge externe

Lors de la configuration de StorageGRID, un administrateur de la grille peut utiliser le gestionnaire de grille ou l'API de gestion de grille pour effectuer les étapes suivantes, qui sont toutes facultatives :

1. Configurez les noeuds finaux pour le service Load Balancer.

   Vous devez configurer les noeuds finaux pour utiliser le service Load Balancer. Le service Load Balancer sur les nœuds d'administration ou de passerelle distribue les connexions réseau entrantes des applications client aux nœuds de stockage. Lors de la création d'un terminal d'équilibrage de charge, l'administrateur StorageGRID spécifie un numéro de port, si le terminal accepte les connexions HTTP ou HTTPS, le type de client (S3 ou Swift) qui utilisera le terminal ainsi que le certificat à utiliser pour les connexions HTTPS (le cas échéant).

2. Configurer des réseaux clients non fiables.

   Si un administrateur StorageGRID configure le réseau client d'un nœud pour qu'il ne soit pas fiable, le nœud accepte uniquement les connexions entrantes sur le réseau client sur les ports explicitement configurés en tant que noeuds finaux d'équilibreur de charge.

3. Configurez les groupes haute disponibilité.

   Si l'administrateur crée un groupe haute disponibilité, les interfaces réseau de plusieurs nœuds d'administration ou nœuds de passerelle sont placées dans une configuration de sauvegarde active/active. Les connexions client sont établies à l'aide de l'adresse IP virtuelle du groupe haute disponibilité.

Pour plus d'informations sur chaque option, reportez-vous aux instructions d'administration de StorageGRID.

Résumé : adresses IP et ports pour les connexions client

Les applications client se connectent à StorageGRID en utilisant l'adresse IP d'un nœud de grid et le numéro de port d'un service sur ce nœud. Si des groupes de haute disponibilité sont configurés, les applications client peuvent se connecter en utilisant l'adresse IP virtuelle du groupe de haute disponibilité.

Informations requises pour établir des connexions client

Le tableau récapitule les différentes façons dont les clients peuvent se connecter à StorageGRID ainsi que les adresses IP et les ports utilisés pour chaque type de connexion. Contactez votre administrateur StorageGRID pour en savoir plus ou consultez les instructions d'administration de StorageGRID pour obtenir une description de la recherche de ces informations dans le Gestionnaire de grille.

Là où la connexion est établie	Service auquel le client se connecte	Adresse IP	Port
Groupe HAUTE DISPONIBILITÉ	Équilibreur de charge	Adresse IP virtuelle d'un groupe haute disponibilité	• Port du terminal de l'équilibreur de charge
Groupe HAUTE DISPONIBILITÉ	CLB **Note:** le service CLB est obsolète.	Adresse IP virtuelle d'un groupe haute disponibilité	Ports Swift par défaut : • HTTPS: 8083 • HTTP : 8085
Nœud d'administration	Équilibreur de charge	Adresse IP du nœud d'administration	• Port du terminal de l'équilibreur de charge
Nœud de passerelle	Équilibreur de charge	Adresse IP du nœud de passerelle	• Port du terminal de l'équilibreur de charge
Nœud de passerelle	CLB **Note:** le service CLB est obsolète.	Adresse IP du nœud de passerelle **Remarque :** par défaut, les ports HTTP pour CLB et LDR ne sont pas activés.	Ports Swift par défaut : • HTTPS: 8083 • HTTP : 8085
Nœud de stockage	LDR	Adresse IP du nœud de stockage	Ports Swift par défaut : • HTTPS: 18083 • HTTP : 18085

Exemple

Pour connecter un client Swift au point de terminaison Load Balancer d'un groupe HA de nœuds de passerelle, utilisez une URL structurée comme indiqué ci-dessous :

- `https://VIP-of-HA-group:LB-endpoint-port`

Par exemple, si l'adresse IP virtuelle du groupe HA est 192.0.2.6 et que le numéro de port d'un noeud final Swift Load Balancer est 10444, un client Swift peut utiliser l'URL suivante pour se connecter à StorageGRID :

- `https://192.0.2.6:10444`

Il est possible de configurer un nom DNS pour l'adresse IP que les clients utilisent pour se connecter à StorageGRID. Contactez votre administrateur réseau local.

Choix d'utiliser des connexions HTTPS ou HTTP

Lorsque les connexions client sont effectuées à l'aide d'un noeud final Load Balancer, les connexions doivent être effectuées à l'aide du protocole (HTTP ou HTTPS) spécifié pour ce noeud final. Pour utiliser HTTP pour les connexions client aux nœuds de stockage ou au service CLB sur les nœuds de passerelle, vous devez activer son utilisation.

Par défaut, lorsque les applications client se connectent aux nœuds de stockage ou au service CLB sur les nœuds de passerelle, elles doivent utiliser le protocole HTTPS chiffré pour toutes les connexions. Vous pouvez également activer des connexions HTTP moins sécurisées en sélectionnant l'option de grille **Activer connexion HTTP** dans le Gestionnaire de grille. Par exemple, une application client peut utiliser HTTP lors du test de la connexion à un noeud de stockage dans un environnement non-production.

> Soyez prudent lorsque vous activez HTTP pour une grille de production car les demandes seront envoyées de manière non chiffrée.

> Le service CLB est obsolète.

Si l'option **Activer connexion HTTP** est sélectionnée, les clients doivent utiliser des ports HTTP différents de ceux qu'ils utilisent pour HTTPS. Voir les instructions d'administration de StorageGRID.

Informations associées

"Administrer StorageGRID"

Test de votre connexion dans la configuration de l'API Swift

Vous pouvez utiliser l'interface de ligne de commandes Swift pour tester votre connexion au système StorageGRID et vérifier que vous pouvez lire et écrire des objets sur le système.

Ce dont vous avez besoin

- Vous devez avoir téléchargé et installé python-swaftclient, le client de ligne de commande Swift.
- Vous devez disposer d'un compte de locataire Swift dans le système StorageGRID.

Description de la tâche

Si vous n'avez pas configuré la sécurité, vous devez ajouter le `--insecure` marquer pour chacune de ces commandes.

Étapes

1. Interrogez l'URL d'information pour votre déploiement StorageGRID Swift :

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/info
capabilities
```

   Cela suffit pour tester le fonctionnement de votre déploiement Swift. Pour tester davantage la configuration des comptes en stockant un objet, passez aux étapes supplémentaires.

2. Placer un objet dans le conteneur :

```
touch test_object
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
upload test_container test_object
--object-name test_object
```

3. Procurez-vous le conteneur pour vérifier l'objet :

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
list test_container
```

4. Supprimez l'objet :

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
delete test_container test_object
```

5. Supprimez le conteneur :

```
swift
-U `<_Tenant_Account_ID:Account_User_Name_>`
-K `<_User_Password_>`
-A `\https://<_FQDN_ | _IP_>:<_Port_>/auth/v1.0'
delete test_container
```

Informations associées

"Création et configuration de comptes de tenant Swift"

"Configuration de la sécurité pour l'API REST"

Opérations prises en charge par l'API REST Swift

Le système StorageGRID prend en charge la plupart des opérations dans l'API OpenStack Swift. Avant d'intégrer des clients de l'API REST Swift avec StorageGRID, consultez les informations d'implémentation pour les opérations des comptes, des

conteneurs et des objets.

Opérations prises en charge par StorageGRID

Les opérations de l'API Swift suivantes sont prises en charge :

- "Opérations sur le compte"
- "Opérations sur les conteneurs"
- "Opérations sur l'objet"

En-têtes de réponse courants pour toutes les opérations

Le système StorageGRID implémente toutes les en-têtes courants pour les opérations prises en charge, comme défini par l'API de stockage objet OpenStack Swift v1.

Informations associées

"OpenStack : API de stockage objet"

Terminaux API Swift pris en charge

StorageGRID prend en charge les points de terminaison de l'API Swift suivants : l'URL info, l'URL d'authentification et l'URL de stockage.

URL info

Vous pouvez déterminer les capacités et les limites de l'implémentation de StorageGRID Swift en émettant une demande GET à l'URL de base Swift avec le chemin /info.

```
https://FQDN | Node IP:Swift Port/info/
```

Dans la demande :

- *FQDN* est le nom de domaine complet.
- *Node IP* Est l'adresse IP du nœud de stockage ou du nœud de passerelle sur le réseau StorageGRID.
- *Swift Port* Est le numéro de port utilisé pour les connexions API Swift sur le nœud de stockage ou le nœud de passerelle.

Par exemple, l'URL d'information suivante demande des informations à un noeud de stockage avec l'adresse IP 10.99.106.103 et le port 18083.

```
https://10.99.106.103:18083/info/
```

La réponse inclut les fonctionnalités de l'implémentation Swift sous forme de dictionnaire JSON. Un outil client peut analyser la réponse JSON pour déterminer les fonctionnalités de l'implémentation et les utiliser comme contraintes pour les opérations de stockage ultérieures.

La mise en œuvre de StorageGRID de Swift permet un accès non authentifié à l'URL info.

URL d'authentification

Un client peut utiliser l'URL d'authentification Swift pour s'authentifier en tant qu'utilisateur de compte de locataire.

```
https://FQDN | Node IP:Swift Port/auth/v1.0/
```

Vous devez fournir l'ID de compte de tenant, le nom d'utilisateur et le mot de passe comme paramètres dans le `X-Auth-User` et `X-Auth-Key` en-têtes de demande, comme suit :

```
X-Auth-User: Tenant_Account_ID:Username

X-Auth-Key: Password
```

Dans les en-têtes de demande :

- *`Tenant_Account_ID`* Est l'ID de compte attribué par StorageGRID lors de la création du locataire Swift. Il s'agit du même ID de compte de locataire que celui utilisé sur la page de connexion du Gestionnaire de locataires.
- *`Username`* Est le nom d'un utilisateur locataire qui a été créé dans le Gestionnaire de tenant. Cet utilisateur doit appartenir à un groupe disposant de l'autorisation Administrateur Swift. L'utilisateur root du locataire ne peut pas être configuré pour utiliser l'API REST Swift.

  Si la fédération des identités est activée pour le compte de tenant, indiquez le nom d'utilisateur et le mot de passe de l'utilisateur fédéré à partir du serveur LDAP. Vous pouvez également indiquer le nom de domaine de l'utilisateur LDAP. Par exemple :

  ```
  X-Auth-User: Tenant_Account_ID:Username@Domain_Name
  ```

- *`Password`* est le mot de passe de l'utilisateur tenant. Les mots de passe utilisateur sont créés et gérés dans le Gestionnaire de locataires.

La réponse à une demande d'authentification réussie renvoie une URL de stockage et un jeton d'authentification, comme suit :

```
X-Storage-Url: https://FQDN | Node_IP:Swift_Port/v1/Tenant_Account_ID

X-Auth-Token: token

X-Storage-Token: token
```

Par défaut, le jeton est valide pendant 24 heures à compter de l'heure de génération.

Des jetons sont générés pour un compte de locataire spécifique. Un jeton valide pour un compte n'autorise pas un utilisateur à accéder à un autre compte.

URL du stockage

Une application client peut émettre des appels de l'API REST Swift pour exécuter des opérations de compte, conteneur et objet prises en charge sur un nœud de passerelle ou un nœud de stockage. Les demandes de stockage sont adressées à l'URL de stockage renvoyée dans la réponse d'authentification. La demande doit également inclure l'en-tête X-Auth-Token et la valeur renvoyée par la demande d'autorisation.

```
https://FQDN | IP:Swift_Port/v1/Tenant_Account_ID

[/container][/object]

X-Auth-Token: token
```

Certains en-têtes de réponse de stockage contenant des statistiques d'utilisation peuvent ne pas refléter les chiffres précis des objets récemment modifiés. L'affichage des nombres précis dans ces en-têtes peut prendre quelques minutes.

Les en-têtes de réponse suivants pour les opérations de compte et de conteneur sont des exemples de ceux qui contiennent des statistiques d'utilisation :

- `X-Account-Bytes-Used`
- `X-Account-Object-Count`
- `X-Container-Bytes-Used`
- `X-Container-Object-Count`

Informations associées

"Configuration des connexions client"

"Création et configuration de comptes de tenant Swift"

"Opérations sur le compte"

"Opérations sur les conteneurs"

"Opérations sur l'objet"

Opérations sur le compte

Les opérations de l'API Swift suivantes sont effectuées sur les comptes.

OBTENIR un compte

Cette opération récupère la liste de conteneurs associée aux statistiques d'utilisation du compte et du compte.

Le paramètre de demande suivant est requis :

- `Account`

L'en-tête de demande suivant est requis :

- `X-Auth-Token`

Les paramètres de requête pris en charge suivants sont facultatifs :

- `Delimiter`
- `End_marker`
- `Format`
- `Limit`
- `Marker`
- `Prefix`

Une exécution réussie renvoie les en-têtes suivants avec une réponse « HTTP/1.1 204 aucun contenu » si le

compte est trouvé et qu'aucun conteneur n'est vide, ou une réponse « HTTP/1.1 200 OK » si le compte est trouvé et que la liste de conteneurs n'est pas vide :

- `Accept-Ranges`
- `Content-Length`
- `Content-Type`
- `Date`
- `X-Account-Bytes-Used`
- `X-Account-Container-Count`
- `X-Account-Object-Count`
- `X-Timestamp`
- `X-Trans-Id`

Compte PRINCIPAL

Cette opération récupère les informations et les statistiques du compte à partir d'un compte Swift.

Le paramètre de demande suivant est requis :

- `Account`

L'en-tête de demande suivant est requis :

- `X-Auth-Token`

Une exécution réussie renvoie les en-têtes suivants avec une réponse « HTTP/1.1 204 No Content » :

- `Accept-Ranges`
- `Content-Length`
- `Date`
- `X-Account-Bytes-Used`
- `X-Account-Container-Count`
- `X-Account-Object-Count`
- `X-Timestamp`
- `X-Trans-Id`

Informations associées

"Les opérations Swift sont suivies dans les journaux d'audit"

Opérations sur les conteneurs

StorageGRID prend en charge un maximum de 1,000 conteneurs par compte Swift. Les opérations d'API Swift suivantes sont effectuées sur les conteneurs.

SUPPRIMER le conteneur

Cette opération supprime un conteneur vide d'un compte Swift dans un système StorageGRID.

Les paramètres de demande suivants sont requis :

- `Account`
- `Container`

L'en-tête de demande suivant est requis :

- `X-Auth-Token`

Une exécution réussie renvoie les en-têtes suivants avec une réponse "HTTP/1.1 204 No Content" :

- `Content-Length`
- `Content-Type`
- `Date`
- `X-Trans-Id`

CONTENEUR

Cette opération récupère la liste d'objets associée au conteneur, ainsi que les statistiques et métadonnées de conteneur dans un système StorageGRID.

Les paramètres de demande suivants sont requis :

- `Account`
- `Container`

L'en-tête de demande suivant est requis :

- `X-Auth-Token`

Les paramètres de requête pris en charge suivants sont facultatifs :

- `Delimiter`
- `End_marker`
- `Format`
- `Limit`
- `Marker`
- `Path`
- `Prefix`

Une exécution réussie renvoie les en-têtes suivants avec une réponse « HTTP/1.1 200 Success » ou « HTTP/1.1 204 No Content » :

- `Accept-Ranges`

- `Content-Length`
- `Content-Type`
- `Date`
- `X-Container-Bytes-Used`
- `X-Container-Object-Count`
- `X-Timestamp`
- `X-Trans-Id`

Conteneur DE TÊTE

Cette opération récupère les statistiques du conteneur et les métadonnées d'un système StorageGRID.

Les paramètres de demande suivants sont requis :

- `Account`
- `Container`

L'en-tête de demande suivant est requis :

- `X-Auth-Token`

Une exécution réussie renvoie les en-têtes suivants avec une réponse "HTTP/1.1 204 No Content" :

- `Accept-Ranges`
- `Content-Length`
- `Date`
- `X-Container-Bytes-Used`
- `X-Container-Object-Count`
- `X-Timestamp`
- `X-Trans-Id`

PLACER le conteneur

Cette opération crée un conteneur pour un compte dans un système StorageGRID.

Les paramètres de demande suivants sont requis :

- `Account`
- `Container`

L'en-tête de demande suivant est requis :

- `X-Auth-Token`

Une exécution réussie renvoie les en-têtes suivants avec une réponse « HTTP/1.1 201 created » ou « HTTP/1.1 202 Accepted » (si le conteneur existe déjà sous ce compte) :

- `Content-Length`
- `Date`
- `X-Timestamp`
- `X-Trans-Id`

Un nom de conteneur doit être unique dans le namespace StorageGRID. Si le conteneur existe sous un autre compte, l'en-tête suivant est renvoyé : « HTTP/1.1 409 Conflict ».

Informations associées

"Les opérations Swift sont suivies dans les journaux d'audit"

Opérations sur l'objet

Les opérations suivantes de l'API Swift sont effectuées sur des objets.

SUPPRIMER l'objet

Cette opération supprime le contenu et les métadonnées d'un objet du système StorageGRID.

Les paramètres de demande suivants sont requis :

- `Account`
- `Container`
- `Object`

L'en-tête de demande suivant est requis :

- `X-Auth-Token`

Une exécution réussie renvoie les en-têtes de réponse suivants avec un `HTTP/1.1 204 No Content` réponse :

- `Content-Length`
- `Content-Type`
- `Date`
- `X-Trans-Id`

Lors du traitement d'une requête DE SUPPRESSION d'objet, StorageGRID tente de supprimer immédiatement toutes les copies de l'objet des 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, si un emplacement est temporairement indisponible), StorageGRID met les copies en file d'attente pour suppression, puis indique que le client a réussi à les supprimer.

Pour plus d'informations sur la suppression des objets, reportez-vous aux instructions relatives à la gestion des objets avec la gestion du cycle de vie des informations.

OBJET GET

Cette opération récupère le contenu de l'objet et obtient ses métadonnées depuis un système StorageGRID.

Les paramètres de demande suivants sont requis :

- `Account`
- `Container`
- `Object`

L'en-tête de demande suivant est requis :

- `X-Auth-Token`

Les en-têtes de demande suivants sont facultatifs :

- `Accept-Encoding`
- `If-Match`
- `If-Modified-Since`
- `If-None-Match`
- `If-Unmodified-Since`
- `Range`

Une exécution réussie renvoie les en-têtes suivants avec un `HTTP/1.1 200 OK` réponse :

- `Accept-Ranges`
- `Content-Disposition`, retourné seulement si `Content-Disposition` les métadonnées ont été définies
- `Content-Encoding`, retourné seulement si `Content-Encoding` les métadonnées ont été définies
- `Content-Length`
- `Content-Type`
- `Date`
- `ETag`
- `Last-Modified`
- `X-Timestamp`
- `X-Trans-Id`

Objet TÊTE

Cette opération récupère les métadonnées et les propriétés d'un objet ingéré à partir d'un système StorageGRID.

Les paramètres de demande suivants sont requis :

- `Account`
- `Container`
- `Object`

L'en-tête de demande suivant est requis :

- `X-Auth-Token`

Une exécution réussie renvoie les en-têtes suivants avec une réponse "HTTP/1.1 200 OK" :

- `Accept-Ranges`
- `Content-Disposition`, retourné seulement si `Content-Disposition` les métadonnées ont été définies
- `Content-Encoding`, retourné seulement si `Content-Encoding` les métadonnées ont été définies
- `Content-Length`
- `Content-Type`
- `Date`
- `ETag`
- `Last-Modified`
- `X-Timestamp`
- `X-Trans-Id`

PLACER l'objet

Cette opération crée un nouvel objet avec des données et des métadonnées, ou remplace un objet existant par des données et des métadonnées dans un système StorageGRID.

StorageGRID prend en charge les objets pouvant atteindre 5 To.

> Les demandes contradictoires des clients, telles que deux clients qui écrivent sur la même clé, sont résolues sur la base des « derniers-victoires ». Le calendrier de l'évaluation « derniers-victoires » est basé sur le moment où le système StorageGRID remplit une demande donnée et non sur le moment où les clients Swift démarrent une opération.

Les paramètres de demande suivants sont requis :

- `Account`
- `Container`
- `Object`

L'en-tête de demande suivant est requis :

- `X-Auth-Token`

Les en-têtes de demande suivants sont facultatifs :

- `Content-Disposition`
- `Content-Encoding`

  N'utilisez pas de hachés `Content-Encoding` Si la règle ILM appliquée à un objet filtre les objets en

fonction de leur taille et utilise le placement synchrone à l'ingestion (options équilibrées ou strictes pour le comportement d'ingestion).

- `Transfer-Encoding`

  N'utilisez pas de compression ni de hachée `Transfer-Encoding` Si la règle ILM appliquée à un objet filtre les objets en fonction de leur taille et utilise le placement synchrone à l'ingestion (options équilibrées ou strictes pour le comportement d'ingestion).

- `Content-Length`

  Si une règle ILM filtre les objets par taille et utilise le placement synchrone lors de l'ingestion, vous devez spécifier `Content-Length`.

  > Si vous ne suivez pas ces directives pour `Content-Encoding`, `Transfer-Encoding`, et `Content-Length`, StorageGRID doit enregistrer l'objet avant de déterminer la taille de l'objet et d'appliquer la règle ILM. En d'autres termes, StorageGRID doit créer par défaut des copies intermédiaires d'un objet à l'entrée. C'est-à-dire que StorageGRID doit utiliser l'option de double validation pour le comportement d'ingestion.

  Pour plus d'informations sur le placement synchrone et les règles ILM, reportez-vous aux instructions relatives à la gestion des objets avec des informations relatives à la gestion du cycle de vie.

- `Content-Type`
- `ETag`
- `X-Object-Meta-<name\>` (métadonnées liées aux objets)

  Si vous souhaitez utiliser l'option **temps de création défini par l'utilisateur** comme temps de référence pour une règle ILM, vous devez stocker la valeur dans un en-tête défini par l'utilisateur nommé `X-Object-Meta-Creation-Time`. Par exemple :

  ```
  X-Object-Meta-Creation-Time: 1443399726
  ```

  Ce champ est évalué en secondes depuis le 1er janvier 1970.

- `X-Storage-Class: reduced_redundancy`

  Cet en-tête affecte le nombre de copies d'objet créées par StorageGRID si la règle ILM correspondant à l'objet ingéré spécifie le comportement d'ingestion de la double validation ou de l'équilibrage.

  - **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 ne fait une copie provisoire que si le système ne peut pas immédiatement faire toutes les copies spécifiées dans la règle. Si StorageGRID peut effectuer un placement synchrone, cet en-tête n'a aucun effet.

    Le `reduced_redundancy` L'en-tête est le plus utilisé lorsque la règle ILM correspondant à l'objet crée une copie répliquée unique. Dans ce cas, utilisez `reduced_redundancy` élimine la création et la suppression inutiles d'une copie d'objet supplémentaire pour chaque opération d'ingestion.

À l'aide du `reduced_redundancy` l'en-tête n'est pas recommandé dans d'autres cas, car il augmente le risque de perte de données d'objet lors de l'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.

Notez que la spécification `reduced_redundancy` l'impact sur le nombre de copies créées uniquement lors de l'ingestion d'un objet. Elle n'affecte pas le nombre de copies de l'objet lorsque celui-ci est évalué par la règle ILM active et n'entraîne pas le stockage des données avec des niveaux de redondance inférieurs dans le système StorageGRID.

Une exécution réussie renvoie les en-têtes suivants avec une réponse "HTTP/1.1 201 created" :

- `Content-Length`
- `Content-Type`
- `Date`
- `ETag`
- `Last-Modified`
- `X-Trans-Id`

Informations associées

"Gestion des objets avec ILM"

"Les opérations Swift sont suivies dans les journaux d'audit"

Demande D'OPTIONS

La demande D'OPTIONS vérifie la disponibilité d'un service Swift individuel. La demande D'OPTIONS est traitée par le nœud de stockage ou le nœud passerelle spécifié dans l'URL.

Méthode DES OPTIONS

Par exemple, les applications client peuvent émettre une demande D'OPTIONS vers le port Swift sur un nœud de stockage, sans fournir d'informations d'authentification Swift, 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.

Lorsqu'elle est utilisée avec l'URL info ou l'URL de stockage, la méthode OPTIONS renvoie une liste de verbes pris en charge pour l'URL donnée (par exemple, HEAD, GET, OPTIONS et PUT). La méthode D'OPTIONS ne peut pas être utilisée avec l'URL d'authentification.

Le paramètre de demande suivant est requis :

- `Account`

Les paramètres de demande suivants sont facultatifs :

- `Container`
- `Object`

Une exécution réussie renvoie les en-têtes suivants avec une réponse « HTTP/1.1 204 No Content ». La demande D'OPTIONS à l'URL de stockage ne nécessite pas que la cible existe.

- `Allow` (Une liste de verbes pris en charge pour l'URL donnée, par exemple, HEAD, GET, OPTIONS, Et PUT)
- `Content-Length`
- `Content-Type`
- `Date`
- `X-Trans-Id`

Informations associées

"Terminaux API Swift pris en charge"

Réponse aux erreurs des opérations de l'API Swift

La compréhension des réponses d'erreur possibles peut vous aider à résoudre les problèmes.

Les codes d'état HTTP suivants peuvent être renvoyés lorsque des erreurs se produisent au cours d'une opération :

Nom de l'erreur Swift	Statut HTTP
AccountNameToolong, ContainerNameToolong, HeaderTooBig, InvalidContainerName, InvalidRequest, InvalidURI, MetadaNameToolong, MetadaValueTooBig, MissingSecurityHeader, ObjectNameToolong, TooManyContainers, TooManyMetadaItems, TotalMetadaTooLarge	400 demande erronée
AccessDenied	403 interdit
ContainerNotEmpty, ContainerAlreadyExists	409 conflit
Erreur interne	500 erreur interne du serveur
InvalidRange	416 Plage demandée non satisfiable
MethodNotAlldue	405 méthode non autorisée

Nom de l'erreur Swift	Statut HTTP
MissingContentLength	411 longueur requise
NOTFOUND	404 introuvable
Note d'implémentation	501 non mis en œuvre
Pré-conditionFailed	412 Echec de la condition préalable
ResourceNotFound	404 introuvable
Non autorisé	401 non autorisé
Entité intraitableEntity	422 entité impossible à traiter

Opérations de l'API REST StorageGRID Swift

Des opérations sont ajoutées à l'API REST Swift qui sont spécifiques au système StorageGRID.

DEMANDE DE cohérence du conteneur

Le niveau de cohérence assure une reprise entre la disponibilité des objets et la cohérence de ces objets sur différents sites et nœuds de stockage. La demande DE cohérence DU conteneur GET vous permet de déterminer le niveau de cohérence appliqué à un conteneur particulier.

Demande

En-tête HTTP de demande	Description
`X-Auth-Token`	Spécifie le jeton d'authentification Swift pour le compte à utiliser pour la demande.
`x-ntap-sg-consistency`	Spécifie le type de demande, où `true` = COHÉRENCE GARANTIE entre les conteneurs, et `false` = CONTENEUR GET.
`Host`	Nom d'hôte auquel la demande est dirigée.

Exemple de demande

```
GET /v1/28544923908243208806/Swift container
X-Auth-Token: SGRD_3a877009a2d24cb1801587bfa9050f29
x-ntap-sg-consistency: true
Host: test.com
```

Réponse

En-tête HTTP de réponse	Description
`Date`	La date et l'heure de la réponse.
`Connection`	Indique si la connexion au serveur est ouverte ou fermée.
`X-Trans-Id`	Identifiant de transaction unique pour la demande.
`Content-Length`	Longueur du corps de réponse.
`x-ntap-sg-consistency`	Niveau de contrôle de cohérence appliqué au conteneur. Les valeurs suivantes sont prises en charge : • **Tous** : tous les nœuds reçoivent les données immédiatement ou la demande échouera. • **Forte-global**: Garantit la cohérence 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 de clients au sein d'un site. • **Lecture-après-nouvelle-écriture** : offre 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. **Remarque** : si votre application utilise des demandes HEAD sur des objets qui n'existent pas, vous pouvez recevoir un nombre élevé de 500 erreurs de serveur interne si un ou plusieurs nœuds de stockage ne sont pas disponibles. Pour éviter ces erreurs, utilisez le niveau « disponible ». • **Disponible** (cohérence éventuelle pour les opérations DE TÊTE) : se comporte de la même façon que le niveau de cohérence "entre les nouvelles écritures", mais ne fournit qu'une cohérence éventuelle pour les opérations DE TÊTE. Niveaux de disponibilité supérieurs à ceux de la « nouvelle écriture » en cas d'indisponibilité des nœuds de stockage

Exemple de réponse

```
HTTP/1.1 204 No Content
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
X-Trans-Id: 1936575373
Content-Length: 0
x-ntap-sg-consistency: strong-site
```

Informations associées

"Utilisez un compte de locataire"

REQUÊTE de cohérence du conteneur

La demande DE cohérence PUT dans le conteneur vous permet de spécifier le niveau de cohérence à appliquer aux opérations effectuées dans un conteneur. Par défaut, les nouveaux conteneurs sont créés à l'aide du niveau de cohérence « read-after-New-write ».

Demande

En-tête HTTP de demande	Description
`X-Auth-Token`	Jeton d'authentification Swift pour le compte à utiliser pour la demande.

En-tête HTTP de demande	Description
`x-ntap-sg-consistency`	Niveau de contrôle de cohérence à appliquer aux opérations sur le conteneur. Les valeurs suivantes sont prises en charge : • **Tous** : tous les nœuds reçoivent les données immédiatement ou la demande échouera. • **Forte-global**: Garantit la cohérence 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 de clients au sein d'un site. • **Lecture-après-nouvelle-écriture** : offre 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. **Remarque** : si votre application utilise des demandes HEAD sur des objets qui n'existent pas, vous pouvez recevoir un nombre élevé de 500 erreurs de serveur interne si un ou plusieurs nœuds de stockage ne sont pas disponibles. Pour éviter ces erreurs, utilisez le niveau « disponible ». • **Disponible** (cohérence éventuelle pour les opérations DE TÊTE) : se comporte de la même façon que le niveau de cohérence "entre les nouvelles écritures", mais ne fournit qu'une cohérence éventuelle pour les opérations DE TÊTE. Niveaux de disponibilité supérieurs à ceux de la « nouvelle écriture » en cas d'indisponibilité des nœuds de stockage
`Host`	Nom d'hôte auquel la demande est dirigée.

Interaction des contrôles de cohérence et des règles ILM pour la protection des données

Le contrôle de cohérence et la règle ILM de votre choix affectent la protection des objets. Ces paramètres peuvent interagir.

Par exemple, le contrôle de cohérence utilisé 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. Étant donné que StorageGRID nécessite l'accès aux métadonnées d'un objet et à ses données pour répondre aux demandes client, la sélection de niveaux de protection correspondant au niveau de cohérence et au comportement d'ingestion permet d'améliorer la protection des données initiale et de mieux prévoir les réponses du système.

Les comportements d'ingestion suivants sont disponibles pour les règles ILM :

- **Strict** : toutes les copies spécifiées dans la règle ILM doivent être effectuées avant que le succès ne soit renvoyé au client.
- **Équilibré**: StorageGRID tente de faire toutes les copies spécifiées dans la règle ILM à l'entrée; si ce n'est pas possible, des copies intermédiaires sont faites et le succès est renvoyé au client. Les copies spécifiées dans la règle ILM sont effectuées lorsque cela est possible.
- **Double commit**: StorageGRID effectue immédiatement des copies intermédiaires de l'objet et retourne le succès au client. Les copies spécifiées dans la règle ILM sont effectuées lorsque cela est possible.

> Avant de sélectionner le comportement d'entrée d'une règle ILM, lisez la description complète de ces paramètres dans les instructions de gestion des objets avec la gestion du cycle de vie des informations.

Exemple d'interaction du contrôle de cohérence et de la règle ILM

Supposons que vous disposez d'une grille à deux sites avec la règle ILM suivante et le paramètre de niveau de cohérence suivant :

- **Règle ILM** : créez deux copies d'objet, une sur le site local et une sur un site distant. Le comportement d'entrée strict est sélectionné.
- **Niveau de cohérence**: "Sept-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 utilisez à la place la même règle ILM et le niveau de cohérence "sept-site", le client peut recevoir un message de réussite après la réplication des données d'objet vers le site distant, mais avant que les métadonnées d'objet ne soient distribuées sur ce site. 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. L'objet ne peut pas être récupéré.

L'interdépendance entre les niveaux de cohérence et les règles ILM peut être complexe. Contactez NetApp si vous avez besoin d'aide.

Exemple de demande

```
PUT /v1/28544923908243208806/_Swift container_
X-Auth-Token: SGRD_3a877009a2d24cb1801587bfa9050f29
x-ntap-sg-consistency: strong-site
Host: test.com
```

Réponse

En-tête HTTP de réponse	Description
`Date`	La date et l'heure de la réponse.
`Connection`	Indique si la connexion au serveur est ouverte ou fermée.
`X-Trans-Id`	Identifiant de transaction unique pour la demande.
`Content-Length`	Longueur du corps de réponse.

Exemple de réponse

```
HTTP/1.1 204 No Content
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
X-Trans-Id: 1936575373
Content-Length: 0
```

Informations associées

"Utilisez un compte de locataire"

Configuration de la sécurité pour l'API REST

Il est recommandé de passer en revue les mesures de sécurité mises en œuvre pour l'API REST et de comprendre comment sécuriser votre système.

Comment StorageGRID assure la sécurité pour l'API REST

Vous devez comprendre comment le système StorageGRID implémente la sécurité, l'authentification et l'autorisation pour l'API REST.

StorageGRID utilise les mesures de sécurité suivantes.

- Les communications client avec le service Load Balancer utilisent HTTPS si HTTPS est configuré pour le noeud final Load Balancer.

  Lorsque vous configurez un point final d'équilibreur de charge, HTTP peut éventuellement être activé. Par exemple, vous pouvez utiliser HTTP à des fins de test ou autres que la production. Pour plus d'informations, reportez-vous aux instructions d'administration de StorageGRID.

- Par défaut, StorageGRID utilise HTTPS pour les communications client avec les nœuds de stockage et le service CLB sur les nœuds de passerelle.

  HTTP peut éventuellement être activé pour ces connexions. Par exemple, vous pouvez utiliser HTTP à des fins de test ou autres que la production. Pour plus d'informations, reportez-vous aux instructions d'administration de StorageGRID.

Le service CLB est obsolète.

- Les communications entre StorageGRID et le client sont chiffrées à l'aide de TLS.
- Les communications entre le service Load Balancer et les nœuds de stockage dans la grille sont cryptées que le terminal de l'équilibreur de charge soit configuré pour accepter les connexions HTTP ou HTTPS.
- Les clients doivent fournir des en-têtes d'authentification HTTP à StorageGRID pour effectuer des opérations d'API REST.

Certificats de sécurité et applications client

Les clients peuvent se connecter au service Load Balancer sur les nœuds de passerelle ou les nœuds d'administration, directement aux nœuds de stockage ou au service CLB sur les nœuds de passerelle.

Dans tous les cas, les applications client peuvent établir des connexions TLS à l'aide d'un certificat de serveur personnalisé chargé par l'administrateur de la grille ou d'un certificat généré par le système StorageGRID :

- Lorsque les applications client se connectent au service Load Balancer, elles le font à l'aide du certificat configuré pour le noeud final de l'équilibreur de charge spécifique utilisé pour établir la connexion. Chaque noeud final possède son propre certificat, qui est soit un certificat de serveur personnalisé chargé par l'administrateur de la grille, soit un certificat que l'administrateur de la grille a généré dans StorageGRID lors de la configuration du noeud final.
- Lorsque les applications client se connectent directement à un nœud de stockage ou au service CLB des nœuds de passerelle, elles utilisent soit les certificats de serveur générés par le système pour les nœuds de stockage lorsque le système StorageGRID a été installé (qui sont signés par l'autorité de certification du système), ou un seul certificat de serveur personnalisé fourni par un administrateur de grid pour la grille.

Les clients doivent être configurés pour approuver l'autorité de certification qui a signé le certificat qu'ils utilisent pour établir des connexions TLS.

Pour plus d'informations sur la configuration des noeuds finaux de l'équilibreur de charge et pour obtenir des instructions sur l'ajout d'un certificat de serveur personnalisé pour les connexions TLS directement aux noeuds de stockage ou au service CLB sur les noeuds de passerelle, reportez-vous aux instructions de la section Administration de StorageGRID.

Récapitulatif

Le tableau suivant montre comment les problèmes de sécurité sont implémentés dans les API REST S3 et Swift :

Problème de sécurité	Implémentation pour l'API REST
Sécurité de la connexion	TLS
Authentification du serveur	Certificat de serveur X.509 signé par l'autorité de certification du système ou certificat de serveur personnalisé fourni par l'administrateur
Authentification client	• S3 : compte S3 (ID de clé d'accès et clé d'accès secrète) • SWIFT : compte Swift (nom d'utilisateur et mot de passe)

Problème de sécurité	Implémentation pour l'API REST
Autorisation du client	• S3 : propriété des compartiments et toutes les règles de contrôle d'accès applicables • SWIFT : accès aux rôles d'administrateur

Informations associées

"Administrer StorageGRID"

Algorithmes de hachage et de cryptage pris en charge pour les bibliothèques TLS

Le système StorageGRID prend en charge un ensemble limité de suites de chiffrement que les applications clientes peuvent utiliser lors de l'établissement d'une session TLS (transport Layer Security).

Versions supportées de TLS

StorageGRID supporte TLS 1.2 et TLS 1.3.

SSLv3 et TLS 1.1 (ou versions antérieures) ne sont plus pris en charge.

Suites de chiffrement prises en charge

Version TLS	Nom IANA de la suite de chiffrement
1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_CHA20_POLY1305_SHA256	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
1.3	TLS_AES_256_GCM_SHA384
TLS_CHA20_POLY1305_SHA256	TLS_AES_128_GCM_SHA256

Suites de chiffrement obsolètes

Les suites de chiffrement suivantes sont obsolètes. La prise en charge de ces chiffrements sera supprimée dans une prochaine version.

Nom IANA
TLS_RSA_WAS_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384

Informations associées

"Configuration des connexions client"

Surveillance et audit des opérations

Vous pouvez surveiller les charges de travail et l'efficacité des opérations client en visualisant les tendances de transaction pour l'ensemble du grid ou pour des nœuds spécifiques. Vous pouvez utiliser des messages d'audit pour surveiller les opérations et les transactions des clients.

Contrôle des taux d'entrée et de récupération des objets

Vous pouvez surveiller les taux d'entrée et de récupération des objets, ainsi que les mesures relatives au nombre d'objets, aux requêtes et à la vérification. Vous pouvez afficher le nombre de tentatives de lecture, d'écriture et de modification d'objets du système StorageGRID ayant échoué et réussies par les applications client.

Étapes

1. Connectez-vous au Grid Manager à l'aide d'un navigateur pris en charge.
2. Dans le tableau de bord, recherchez la section opérations de protocole.

   Cette section récapitule le nombre d'opérations client effectuées par votre système StorageGRID. La moyenne des débits de protocole est calculée au cours des deux dernières minutes.

3. Sélectionnez **noeuds**.
4. Dans la page d'accueil noeuds (niveau de déploiement), cliquez sur l'onglet **Load Balancer**.

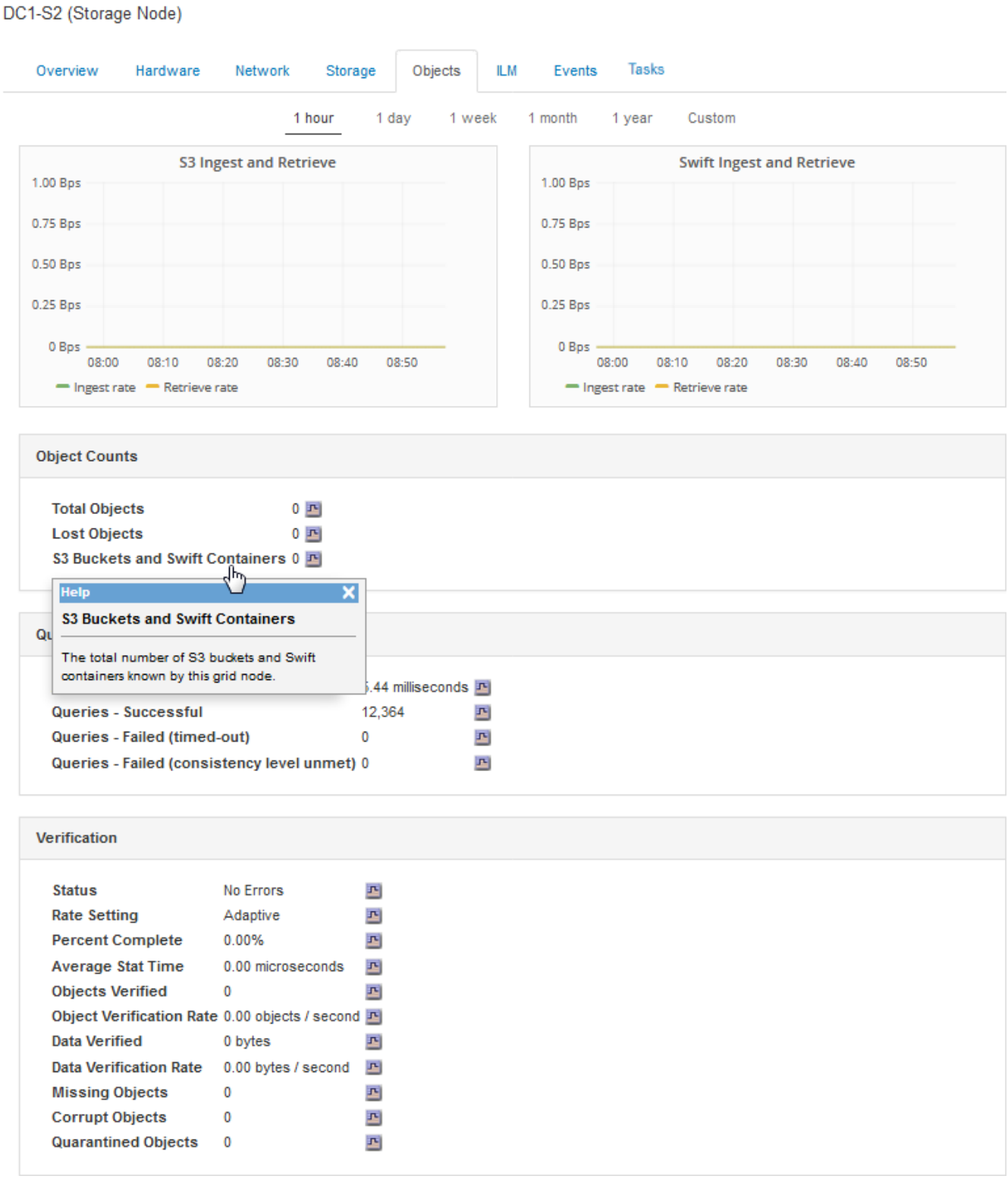
   Les graphiques présentent les tendances de tout le trafic client dirigé vers les terminaux d'équilibreur de charge dans la grille. Vous pouvez sélectionner un intervalle de temps en heures, jours, semaines, mois ou années, vous pouvez également appliquer un intervalle personnalisé.

5. Dans la page d'accueil noeuds (niveau de déploiement), cliquez sur l'onglet **objets**.

   Le graphique montre les taux d'entrée et de récupération de l'intégralité de votre système StorageGRID en octets par seconde et en octets totaux. Vous pouvez sélectionner un intervalle de temps en heures, jours, semaines, mois ou années, vous pouvez également appliquer un intervalle personnalisé.

6. Pour afficher les informations relatives à un noeud de stockage particulier, sélectionnez-le dans la liste de gauche, puis cliquez sur l'onglet **objets**.

   Le tableau affiche les taux d'entrée et de récupération de l'objet pour ce nœud de stockage. L'onglet inclut également des mesures pour le nombre d'objets, les requêtes et la vérification. Vous pouvez cliquer sur les étiquettes pour afficher les définitions de ces mesures.



7. Si vous voulez encore plus de détails :
   a. Sélectionnez **support** > **Outils** > **topologie de grille**.
   b. Sélectionnez ***site*** > **Présentation** > **main**.

      La section opérations d'API affiche un récapitulatif des informations sur l'ensemble de la grille.

   c. Sélectionnez ***Storage Node*** > **LDR** > ***client application*** > **Présentation** > **main**

La section opérations affiche un récapitulatif des informations sur le nœud de stockage sélectionné.

Accès aux journaux d'audit et vérification

Les messages d'audit sont générés par les services StorageGRID et stockés dans des fichiers journaux texte. Des messages d'audit spécifiques aux API dans les journaux d'audit fournissent des données stratégiques de sécurité, d'exploitation et de surveillance des performances qui vous aideront à évaluer l'état de votre système.

Ce dont vous avez besoin

- Vous devez disposer d'autorisations d'accès spécifiques.
- Vous devez avoir le `Passwords.txt` fichier.
- Vous devez connaître l'adresse IP d'un nœud d'administration.

Description de la tâche

Le fichier journal d'audit actif est nommé `audit.log`, Et il est stocké sur des nœuds d'administration.

Une fois par jour, le fichier audit.log actif est enregistré et un nouveau fichier audit.log est lancé. Le nom du fichier enregistré indique quand il a été enregistré, au format `yyyy-mm-dd.txt`.

Après un jour, le fichier enregistré est compressé et renommé, au format `yyyy-mm-dd.txt.gz`, qui conserve la date originale.

Cet exemple montre le fichier audit.log actif, le fichier de la veille (2018-04-15.txt) et le fichier compressé de la veille (`2018-04-14.txt.gz`).

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

Étapes

1. Connectez-vous à un nœud d'administration :
   a. Saisissez la commande suivante : `ssh admin@primary_Admin_Node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
2. Accédez au répertoire contenant les fichiers journaux d'audit :`cd /var/local/audit/export`
3. Afficher le fichier journal d'audit actuel ou enregistré, selon les besoins.

Informations associées

"Examiner les journaux d'audit"

Les opérations Swift sont suivies dans les journaux d'audit

Toutes les opérations réussies DE SUPPRESSION, D'OBTENTION, DE TÊTE, DE POST et DE PUT du stockage sont consignées dans le journal d'audit de StorageGRID. Les échecs ne sont pas consignés, ni les demandes d'info, d'auth ou D'OPTIONS.

Voir *compréhension des messages d'audit* pour plus de détails sur les informations suivies pour les opérations Swift suivantes.

Opérations sur le compte

- OBTENIR un compte
- Compte PRINCIPAL

Opérations sur les conteneurs

- SUPPRIMER le conteneur
- CONTENEUR
- Conteneur DE TÊTE
- PLACER le conteneur

Opérations sur l’objet

- SUPPRIMER l’objet
- OBJET GET
- Objet TÊTE
- PLACER l’objet

Informations associées

"Examiner les journaux d’audit"

"Opérations sur le compte"

"Opérations sur les conteneurs"

"Opérations sur l’objet"

Informations sur le copyright

Informations sur les marques commerciales