



Utilisez StorageGRID

StorageGRID software

NetApp
July 23, 2026

Sommaire

<code>\${post_edited_translations.segment}</code>	1
Utilisez un compte locataire	1
Utilisez un compte locataire StorageGRID	1
Comment se connecter et se déconnecter	2
Tableau de bord Tenant Manager dans StorageGRID	4
API de gestion des locataires	7
Utilisez les connexions de fédération de grille	12
Gérer les groupes et les utilisateurs	26
Gérer les clés d'accès S3	44
<code>\${post_edited_translations.segment}</code>	50
<code>\${post_edited_translations.segment}</code>	79
Utilisez l'API REST S3	113
Versions et mises à jour prises en charge de l'API REST StorageGRID S3	113
Requêtes S3 API prises en charge dans StorageGRID	117
Tester la configuration de l'API REST S3 de StorageGRID	136
Comment StorageGRID implémente l'API REST S3	137
<code>\${post_edited_translations.segment}</code>	153
Opérations personnalisées StorageGRID	205
<code>\${post_edited_translations.segment}</code>	228
Opérations S3 suivies dans les journaux d'audit de StorageGRID	255
Utilisez l'API REST Swift (fin de vie)	256
Prise en charge de l'API REST Swift dans StorageGRID	256

`${post_edited_translations.segment}`

Utilisez un compte locataire

Utilisez un compte locataire StorageGRID

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

Qu'est-ce qu'un compte locataire ?

Chaque compte locataire possède ses propres groupes fédérés ou locaux, utilisateurs, compartiments S3 et objets.

Les comptes locataires permettent de segmenter les objets stockés par différentes entités. Par exemple, plusieurs comptes locataires peuvent être utilisés dans les deux cas suivants :

- **Cas d'utilisation en entreprise** : si le système StorageGRID est utilisé au sein d'une entreprise, le stockage d'objets de la grille peut être cloisonné par les différents départements de l'organisation. Par exemple, il peut y avoir des comptes locataires pour le département Marketing, le département Support client, le département Ressources humaines, etc.



Si vous utilisez le protocole client S3, vous pouvez également utiliser les compartiments S3 et les stratégies de compartiment pour segmenter les objets entre les services d'une entreprise. Vous n'avez pas besoin de créer des comptes locataires distincts. Consultez les instructions de mise en œuvre "[Compartiments S3 et politiques de compartiment](#)" pour plus d'informations.

- **Cas d'utilisation du fournisseur de services** : si le système StorageGRID est utilisé par un fournisseur de services, le stockage d'objets de la grille peut être cloisonné selon les différentes entités qui louent le stockage. Par exemple, il peut y avoir des comptes locataires pour Company A, Company B, Company C, etc.

`${post_edited_translations.segment}`

Les comptes locataires sont créés par un "`${post_edited_translations.segment}`". Lors de la création d'un compte locataire, l'administrateur du grid spécifie les éléments suivants :

- Informations de base, notamment le nom du locataire, le type de client (S3) et le quota de stockage facultatif.
- Les autorisations du compte locataire, telles que la possibilité pour ce dernier d'utiliser les services de la plateforme S3, de configurer sa propre source d'identité, d'utiliser S3 Select ou d'utiliser une connexion de fédération de grille.
- L'accès racine initial du locataire, en fonction de la manière dont le système StorageGRID utilise les groupes et utilisateurs locaux, la fédération d'identités ou l'authentification unique (SSO).

De plus, les administrateurs de la grille peuvent activer le paramètre S3 Object Lock pour le système StorageGRID si les comptes locataires S3 doivent se conformer aux exigences réglementaires. Lorsque S3 Object Lock est activé, tous les comptes locataires S3 peuvent créer et gérer des compartiments conformes.

Configurer les locataires S3

Après un "[\\${post_edited_translations.segment}](#)", vous pouvez accéder au Gestionnaire de locataires pour effectuer des tâches telles que les suivantes :

- Configurer la fédération d'identités (sauf si la source d'identité est partagée avec la grille)
- Gérer les groupes et les utilisateurs
- Utilisez la fédération de grilles pour le clonage de comptes et la réplication inter-grilles
- Gérer les clés d'accès S3
- Créer et gérer des compartiments S3
- Utilisez les services de la plateforme S3
- Utilisez S3 Select
- Surveiller l'utilisation du stockage



Bien que vous puissiez créer et gérer des compartiments S3 avec le Tenant Manager, vous devez utiliser un "[Client S3](#)" ou "[Console S3](#)" pour ingérer et gérer des objets.

Comment se connecter et se déconnecter

Se connecter à StorageGRID Tenant Manager

Vous accédez au gestionnaire de locataires en saisissant l'URL du locataire dans la barre d'adresse d'un "[navigateur Web pris en charge](#)".

Avant de commencer

- Vous disposez de vos identifiants de connexion.
- Vous disposez d'une URL d'accès au Tenant Manager, fournie par votre administrateur de grid. L'URL ressemblera à l'un des exemples suivants :

```
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 comprend toujours un nom de domaine complet (FQDN), l'adresse IP d'un Admin Node ou l'adresse IP virtuelle d'un groupe HA d'Admin Nodes. Elle peut également inclure un numéro de port, l'ID de compte locataire à 20 chiffres, ou les deux.

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

Étapes

1. Lancez un "navigateur Web pris en charge".
2. Dans la barre d'adresse du navigateur, saisissez l'URL pour accéder à Tenant Manager.
3. \${post_edited_translations.segment}
4. Connectez-vous au Tenant Manager.

\${post_edited_translations.segment}

Ne pas utiliser l'authentification unique (SSO)

\${post_edited_translations.segment}

- Page de connexion de Grid Manager. Sélectionnez le lien **Tenant sign-in**.
- La page de connexion du Gestionnaire de locataires. Le champ **Compte** est peut-être déjà renseigné.
 - i. Si l'identifiant de compte à 20 chiffres du locataire n'est pas affiché, sélectionnez le nom du compte du locataire s'il apparaît dans la liste des comptes récents ou saisissez l'identifiant du compte.
 - ii. Saisissez votre nom d'utilisateur et votre mot de passe.
 - iii. Sélectionnez **Se connecter**.

Le tableau de bord du Tenant Manager s'affiche.

- iv. Si vous avez reçu un mot de passe initial de quelqu'un d'autre, sélectionnez **username > Change password** pour sécuriser votre compte.

Utilisation de l'authentification unique (SSO)

Si StorageGRID utilise l'authentification unique (SSO), l'un des écrans suivants apparaît :

- La page SSO de votre organisation.

Saisissez vos identifiants SSO standard et sélectionnez **Se connecter**.

- \${post_edited_translations.segment}
 - i. Si l'identifiant de compte à 20 chiffres du locataire n'est pas affiché, sélectionnez le nom du compte du locataire s'il apparaît dans la liste des comptes récents ou saisissez l'identifiant du compte.
 - ii. Sélectionnez **Se connecter**.
 - iii. Connectez-vous avec vos identifiants SSO habituels sur la page de connexion SSO de votre organisation.

Le tableau de bord du Tenant Manager s'affiche.

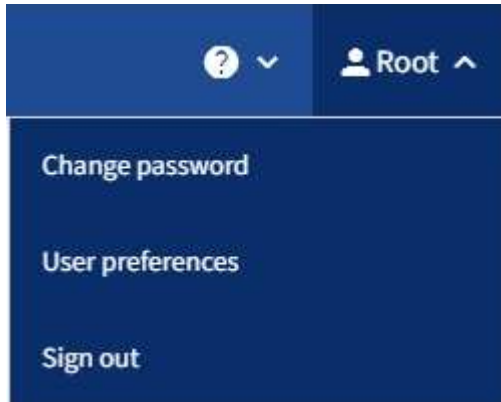
Déconnexion de StorageGRID Tenant Manager

Lorsque vous avez fini d'utiliser le Tenant Manager, vous devez vous déconnecter pour garantir que des utilisateurs non autorisés ne puissent pas accéder au système StorageGRID. La fermeture de votre navigateur peut ne pas vous déconnecter du

système, selon les paramètres de cookies du navigateur.

Étapes

1. `${post_edited_translations.segment}`



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

- `${post_edited_translations.segment}`

Vous êtes déconnecté du nœud d'administration. La page de connexion du Tenant Manager s'affiche.



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

- Si l'authentification unique (SSO) est activée :

Vous êtes déconnecté de tous les nœuds d'administration auxquels vous accédez. La page de connexion de StorageGRID s'affiche. Le nom du compte locataire auquel vous venez d'accéder est répertorié par défaut dans la liste déroulante **Comptes récents**, et l'**ID de compte** du locataire est affiché.



`${post_edited_translations.segment}`

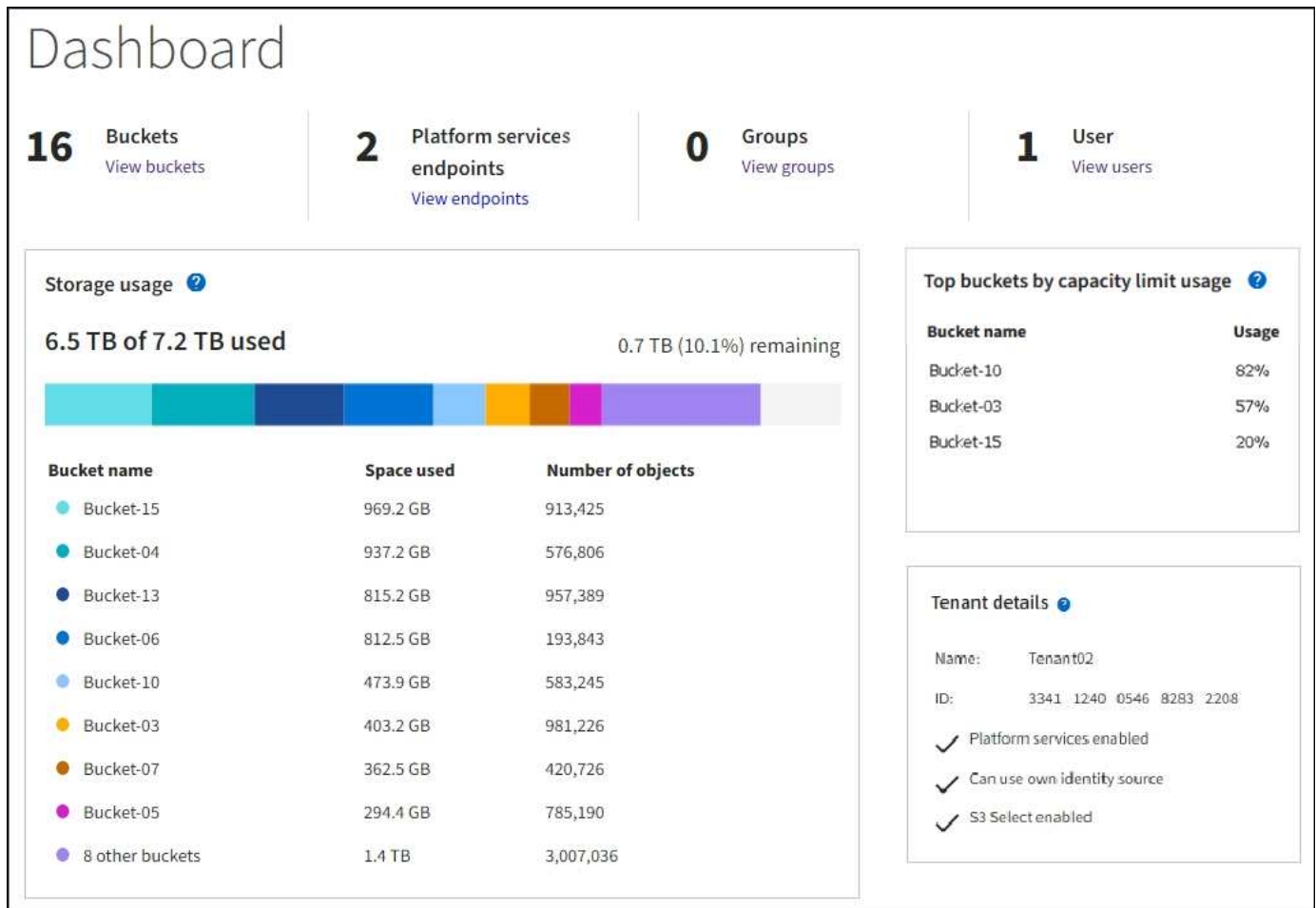
Tableau de bord Tenant Manager dans StorageGRID

Le tableau de bord du Tenant Manager fournit un aperçu de la configuration d'un compte de locataire et de l'espace utilisé par les objets dans les compartiments S3 du locataire. Si le locataire dispose d'un quota, le tableau de bord affiche la part du quota utilisée et la part restante. Si des erreurs sont liées au compte de locataire, elles s'affichent sur le tableau de bord.



La taille logique de tous les objets appartenant à ce locataire inclut les chargements multiparties incomplets et en cours. La taille n'inclut pas l'espace physique supplémentaire utilisé pour les politiques ILM. Les valeurs d'espace utilisé sont des estimations. Ces estimations sont influencées par le moment des ingestions, la connectivité réseau et l'état des nœuds.

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



Informations sur le compte du locataire

La partie supérieure du tableau de bord affiche le nombre de compartiments ou conteneurs, de groupes et d'utilisateurs configurés. Elle affiche également le nombre de points de terminaison des services de plateforme, si certains ont été configurés. Sélectionnez les liens pour afficher les détails.

Selon le "[autorisations de gestion des locataires](#)" dont vous disposez et les options que vous avez configurées, le reste du tableau de bord affiche différentes combinaisons de recommandations, d'utilisation du stockage, d'informations sur les objets et de détails sur les locataires.

``${post_edited_translations.segment}``

Le panneau d'utilisation du stockage contient les informations suivantes :

- ``${post_edited_translations.segment}``
``${post_edited_translations.segment}``
- Si un quota est défini, il indique 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 du quota est basée sur des estimations internes et peut être dépassée dans certains cas. Par exemple, StorageGRID vérifie le quota lorsqu'un client commence à charger des objets et refuse les nouvelles ingestions si le client a dépassé le quota. Cependant, StorageGRID ne prend pas en compte la taille du chargement en cours pour déterminer si le quota a été dépassé. Si des objets sont supprimés, un client peut être temporairement empêché de charger de nouveaux objets jusqu'à ce que l'utilisation du quota soit recalculée. Le calcul de l'utilisation du quota peut prendre 10 minutes ou plus.

- `${post_edited_translations.segment}`

Vous pouvez placer votre curseur sur n'importe quel segment du graphique pour afficher l'espace total consommé par ce compartiment ou conteneur.



- Pour correspondre au graphique à barres, une liste des plus grands compartiments ou conteneurs, incluant la quantité totale de données d'objets et le nombre d'objets pour chaque compartiment 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

`${post_edited_translations.segment}`



`${post_edited_translations.segment}`

`${post_edited_translations.segment}`

`${post_edited_translations.segment}`

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

`${post_edited_translations.segment}`

- `${post_edited_translations.segment}`

`${post_edited_translations.segment}`

`${post_edited_translations.segment}`

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

`${post_edited_translations.segment}`

`${post_edited_translations.segment}`



One or more endpoints have experienced an error and might not be functioning properly. Go to the [Endpoints](#) page to view the error details. The last error occurred 2 hours ago.

Pour afficher les détails concernant "`${post_edited_translations.segment}`", sélectionnez **Endpoints** pour afficher la page Endpoints.

API de gestion des locataires

Découvrez l'API de gestion des locataires StorageGRID

Vous pouvez effectuer des tâches de gestion système à l'aide de l'API REST Tenant Management plutôt qu'en utilisant l'interface utilisateur du Tenant Manager. Par exemple, vous pourriez vouloir utiliser l'API pour automatiser des opérations ou pour créer plusieurs entités, telles que des utilisateurs, plus rapidement.

`${post_edited_translations.segment}`

- Utilisez 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 de Swagger fournit des détails complets et de la documentation pour chaque opération d'API.
- Utilisez "`${post_edited_translations.segment}`".

`${post_edited_translations.segment}`

1. Connectez-vous au Tenant Manager.
2. En haut du Tenant Manager, sélectionnez l'icône d'aide et sélectionnez **API documentation**.

`${post_edited_translations.segment}`

`${post_edited_translations.segment}`

- `${post_edited_translations.segment}`
- **auth** : Opérations permettant d'authentifier la session utilisateur.

L'API de gestion des locataires prend en charge le schéma d'authentification par jeton Bearer. Pour la

connexion d'un locataire, vous fournissez un nom d'utilisateur, un mot de passe et un accountId dans le corps JSON de la demande d'authentification (c'est-à-dire `POST /api/v3/authorize`). Si l'utilisateur est authentifié avec succès, un jeton de sécurité est renvoyé. Ce jeton doit être fourni dans l'en-tête des demandes d'API ultérieures ("Authorization: Bearer token").

Pour obtenir des informations sur l'amélioration de la sécurité de l'authentification, consultez "[Protégez-vous contre la falsification de requêtes intersites](#)".



Si l'authentification unique (SSO) est activée pour le système StorageGRID, vous devez effectuer des étapes différentes pour vous authentifier. Voir le "[\\${post_edited_translations.segment}](#)".

- **config** : opérations relatives à la version du produit et aux versions de l'API de gestion des locataires. Vous pouvez lister la version du produit et les versions majeures de l'API prises en charge par cette version.
- `${post_edited_translations.segment}`
- **Fonctionnalités désactivées** : Opérations permettant d'afficher les fonctionnalités qui pourraient avoir été désactivées.
- **endpoints** : opérations de gestion d'un point de terminaison. Les points de terminaison permettent à un compartiment S3 d'utiliser un service externe pour la réplication CloudMirror de StorageGRID, les notifications ou l'intégration de la recherche.
- `${post_edited_translations.segment}`
- **Groupes** : Opérations permettant de gérer les groupes de locataires locaux et de récupérer les groupes de locataires fédérés à partir d'une source d'identité externe.
- **identity-source** : Opérations permettant de configurer une source d'identité externe et de synchroniser manuellement les informations de groupe et d'utilisateur fédérés.
- **ilm** : Opérations sur les paramètres de gestion du cycle de vie de l'information (ILM).
- `${post_edited_translations.segment}`
- `${post_edited_translations.segment}`
- `${post_edited_translations.segment}`
- **utilisateurs** : Opérations permettant de consulter et de gérer les utilisateurs locataires.

`${post_edited_translations.segment}`

`${post_edited_translations.segment}`

groups
Operations on groups

GET
/org/groups
Lists Tenant User Groups

Parameters
Try it out

Name	Description
type string (query)	filter by group type
limit integer (query)	maximum number of results
marker string (query)	marker-style pagination offset (value is Group's URN)
includeMarker boolean (query)	if set, the marker element is also returned
order string (query)	pagination order (desc requires marker)

Responses
Response content type
application/json

Code	Description
200	Example Value Model <pre>{ "responseTime": "2018-02-01T16:22:31.066Z", "status": "success", "apiVersion": "2.1" }</pre>

Émettre des requêtes API



Toute opération API effectuée via la page de documentation API est une opération en direct. Veuillez à ne pas créer, modifier ou supprimer par erreur des données de configuration ou autres.

Étapes

1. Sélectionnez l'action HTTP pour afficher les détails de la requête.
2. Déterminez si la requête nécessite des paramètres supplémentaires, tels qu'un identifiant de groupe ou d'utilisateur. Ensuite, obtenez ces valeurs. Vous devrez peut-être d'abord effectuer une autre requête API pour obtenir les informations dont vous avez besoin.
3. Déterminez si vous devez modifier le corps de la requête d'exemple. Le cas échéant, vous pouvez sélectionner **Modèle** pour connaître les exigences relatives à chaque champ.

4. Sélectionnez **Try it out**.
5. Fournissez les paramètres requis ou modifiez le corps de la requête selon les besoins.
6. Sélectionnez **Exécuter**.
7. Examinez le code de réponse pour déterminer si la requête a réussi.

Versionnage de l'API de gestion des locataires StorageGRID

L'API de gestion des locataires utilise le versionnage pour permettre des mises à niveau sans interruption de service.

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

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

La version majeure de l'API est mise à jour lorsque des modifications qui ne sont pas compatibles avec les versions précédentes sont apportées. La version mineure de l'API est mise à jour lorsque des modifications qui sont compatibles avec les versions précédentes sont apportées. Les modifications compatibles incluent l'ajout de nouveaux points de terminaison 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 antérieures	2,1	2,2
Non compatible avec les versions antérieures	2,1	3,0

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



Vous pouvez configurer les versions prises en charge. Consultez la section **config** de la documentation de l'API Swagger pour "[API de gestion de grille](#)" plus d'informations. Vous devez désactiver la prise en charge de l'ancienne version après avoir mis à jour tous les clients API vers la nouvelle version.

Les requêtes obsolètes sont marquées comme dépréciées de la manière suivante :

- L'en-tête de réponse est « `Deprecated: true` »
- Le corps de la réponse JSON inclut `"deprecated": true`
- Un avertissement de dépréciation est ajouté au fichier `nms.log`. Par exemple :

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

Déterminez quelles versions d'API sont prises en charge dans la version actuelle

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

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

Spécifiez une version d'API pour une requête

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

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

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

Protégez-vous contre la falsification de requêtes intersites (CSRF) dans StorageGRID

Vous pouvez contribuer à protéger StorageGRID contre les attaques de type Cross-Site Request Forgery (CSRF) en utilisant des jetons CSRF pour renforcer l'authentification qui utilise des cookies. Le Grid Manager et le Tenant Manager activent automatiquement cette fonctionnalité de sécurité ; les autres clients API peuvent choisir de l'activer ou non lors de leur connexion.

Un attaquant capable de déclencher une requête vers un autre site (par exemple avec un formulaire HTTP POST) peut faire en sorte que certaines requêtes soient effectuées en utilisant les cookies de l'utilisateur connecté.

StorageGRID contribue à la protection contre les attaques CSRF grâce à l'utilisation de jetons CSRF. Lorsqu'elle est activée, le contenu d'un cookie spécifique doit correspondre à celui d'un en-tête spécifique ou d'un paramètre spécifique du corps de la requête POST.

Pour activer cette fonctionnalité, définissez le paramètre `csrfToken` sur `true` lors de l'authentification. La valeur par défaut est `false`.

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

Lorsque cette option est activée, un `GridCsrfToken` cookie est défini avec une valeur aléatoire pour les connexions au Grid Manager, et le `AccountCsrfToken` cookie est défini avec une valeur aléatoire pour les connexions au Tenant Manager.

Si le cookie est présent, toutes les requêtes susceptibles de modifier l'état du système (POST, PUT, PATCH, DELETE) doivent inclure l'un des éléments suivants :

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

Pour configurer la protection CSRF, utilisez le ["API de gestion de grille"](#) ou le ["API de gestion des locataires"](#).



Les requêtes comportant un cookie de jeton CSRF défini appliqueront également l'en-tête "Content-Type: application/json" à toute requête attendant un corps de requête JSON, comme protection supplémentaire contre les attaques CSRF.

Utilisez les connexions de fédération de grille

Cloner les groupes de locataires et les utilisateurs dans StorageGRID

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

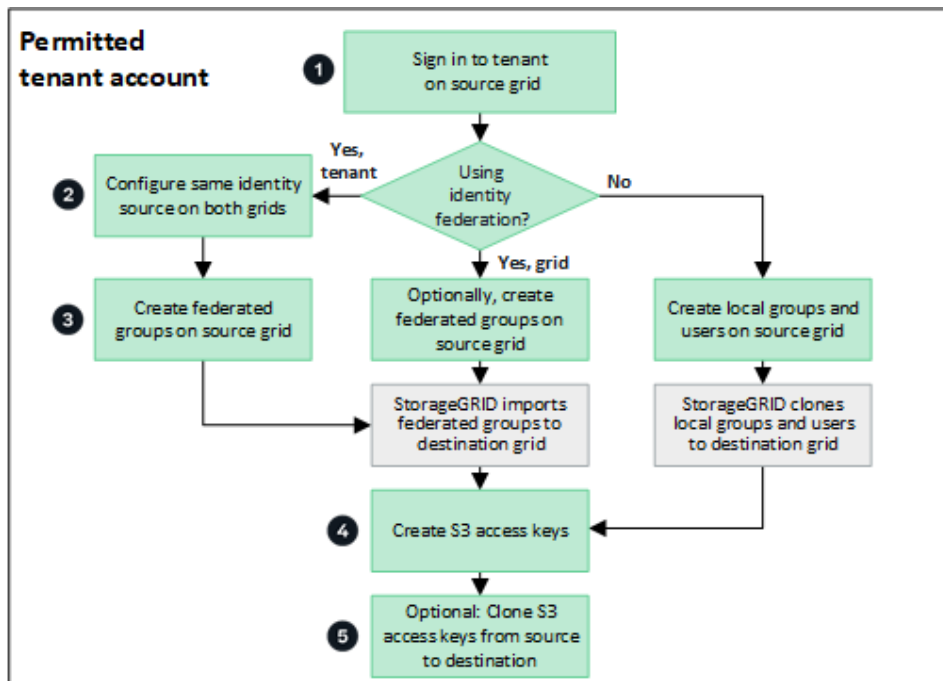
Le système StorageGRID dans lequel le locataire est initialement créé est la *grille source* du locataire. Le système StorageGRID dans lequel le locataire est répliqué est la *grille de destination* du locataire. Les deux comptes de locataire possèdent les mêmes ID de compte, nom, description, quota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

Le clonage des informations de compte locataire est nécessaire pour ["réplication inter-grilles"](#) des objets de compartiment. Avoir les mêmes groupes de locataires et utilisateurs sur les deux grilles garantit que vous pouvez accéder aux compartiments et objets correspondants sur l'une ou l'autre grille.

`${post_edited_translations.segment}`

Si votre compte locataire dispose de l'autorisation **Utiliser la connexion de fédération de grille**, consultez le diagramme de flux de travail pour voir les étapes que vous effectuerez pour cloner les groupes, les utilisateurs

et les clés d'accès S3.



`${post_edited_translations.segment}`

1

Se connecter au locataire

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

2

Configurez éventuellement la fédération d'identité

Si votre compte locataire dispose de l'autorisation **Utiliser sa propre source d'identité** pour utiliser les groupes et utilisateurs fédérés, configurez la même source d'identité (avec les mêmes paramètres) pour les comptes locataires source et de destination. Les groupes et utilisateurs fédérés ne peuvent pas être clonés à moins que les deux grilles n'utilisent la même source d'identité. Pour obtenir des instructions, consultez ["Utilisez la fédération d'identités"](#).

3

Créer des groupes et des utilisateurs

Lors de la création de groupes et d'utilisateurs, commencez toujours par la grille source du locataire. Lorsque vous ajoutez un nouveau groupe, StorageGRID le clone automatiquement sur la grille de destination.

- Si la fédération d'identité est configurée pour l'ensemble du système StorageGRID ou pour votre compte locataire, ["créer de nouveaux groupes de locataires"](#) en important des groupes fédérés depuis la source d'identité.
- Si vous n'utilisez pas la fédération d'identités, `"${post_edited_translations.segment}"` puis `"${post_edited_translations.segment}"`.

4

Créer des clés d'accès S3

Vous pouvez ["Créez vos propres clés d'accès"](#) ou ["créer les clés d'accès d'un autre utilisateur"](#) sur la grille source ou la grille de destination pour accéder aux compartiments de cette grille.

5

En option, clonez les clés d'accès S3

Si vous devez accéder à des compartiments avec les mêmes clés d'accès sur les deux grilles, créez les clés d'accès sur la grille source, puis utilisez l'API Tenant Manager pour les cloner manuellement sur la grille de destination. Pour obtenir des instructions, consultez ["Cloner les clés d'accès S3 à l'aide de l'API"](#).

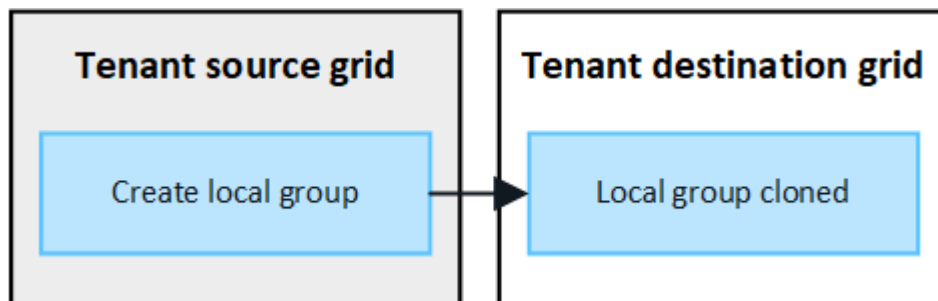
`${post_edited_translations.segment}`

Consultez cette section pour comprendre comment les groupes, les utilisateurs et les clés d'accès S3 sont clonés entre la grille source du locataire et la grille de destination du locataire.

Les groupes locaux créés sur la grille source sont clonés

`${post_edited_translations.segment}`

Le groupe d'origine et son clone possèdent le même mode d'accès, les mêmes autorisations de groupe et la même stratégie de groupe S3. Pour obtenir des instructions, consultez ["Créer des groupes pour le locataire S3"](#).

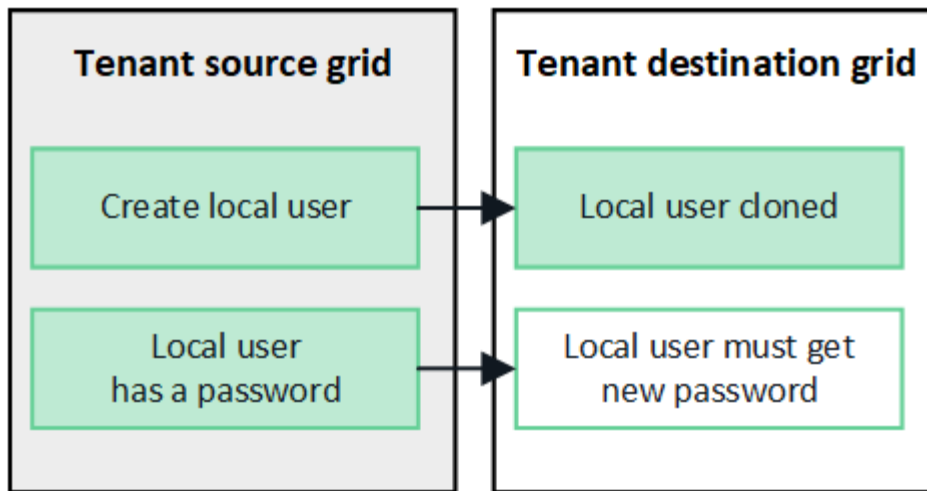


Tous les utilisateurs que vous sélectionnez lorsque vous créez un groupe local sur la grille source ne sont pas inclus lorsque le groupe est cloné sur la grille de destination. Pour cette raison, ne sélectionnez pas d'utilisateurs lorsque vous créez le groupe. Sélectionnez plutôt le groupe lorsque vous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

`${post_edited_translations.segment}`

Lorsque vous créez un nouvel utilisateur local sur la grille source, StorageGRID clone automatiquement cet utilisateur sur la grille de destination. L'utilisateur d'origine et son clone possèdent le même nom complet, le même nom d'utilisateur et le même paramètre **Deny access**. Les deux utilisateurs appartiennent également aux mêmes groupes. Pour obtenir des instructions, consultez ["Gérer les utilisateurs"](#).

Pour des raisons de sécurité, les mots de passe des utilisateurs locaux ne sont pas dupliqués sur la grille de destination. Si un utilisateur local doit accéder à Tenant Manager sur la grille de destination, l'utilisateur root du compte locataire doit ajouter un mot de passe pour cet utilisateur sur la grille de destination. Pour obtenir des instructions, consultez ["Gérer les utilisateurs"](#).

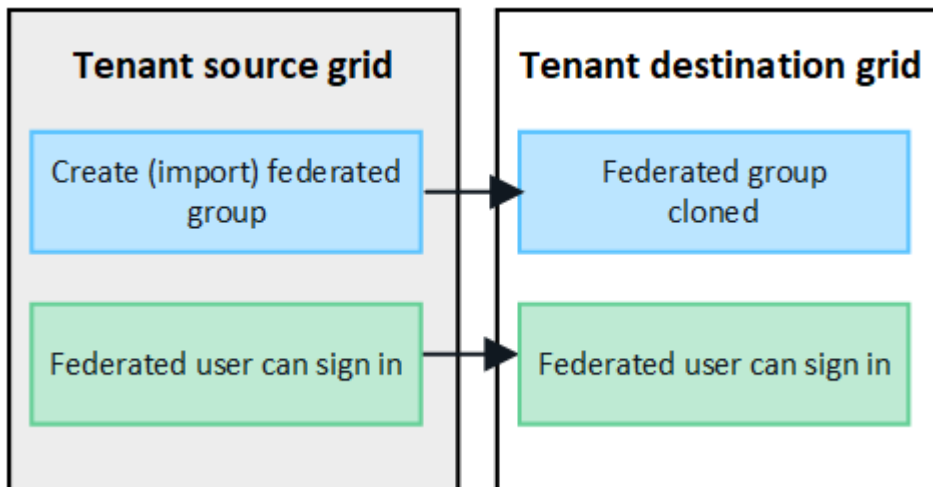


`${post_edited_translations.segment}`

Si les conditions requises pour utiliser le clonage de compte avec "authentification unique" et "fédération d'identité" sont remplies, les groupes fédérés que vous créez (importez) pour le locataire sur la grille source sont automatiquement clonés vers le locataire sur la grille de destination.

`${post_edited_translations.segment}`

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

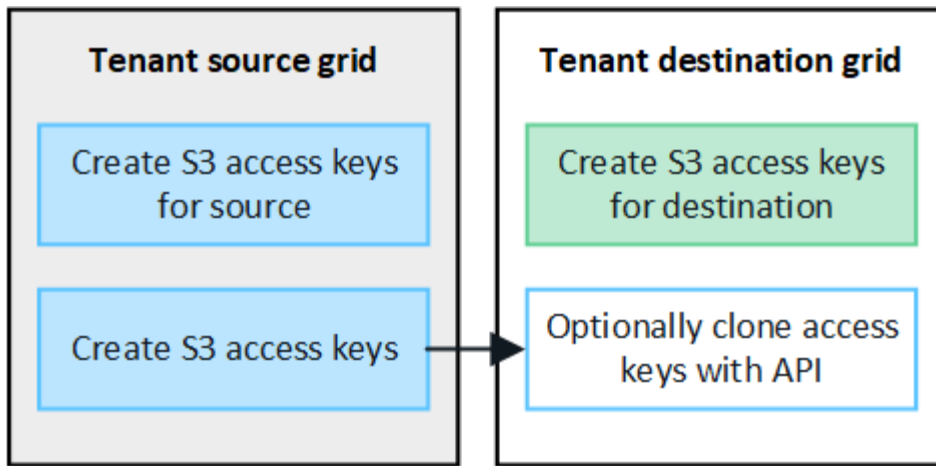


Les clés d'accès S3 peuvent être clonées manuellement

`${post_edited_translations.segment}`

`${post_edited_translations.segment}`

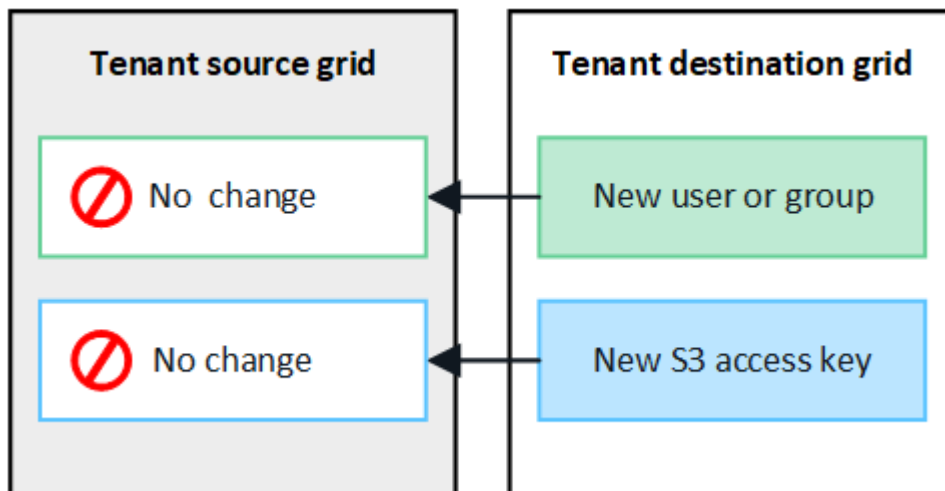
- Si vous n'avez pas besoin d'utiliser les mêmes clés pour chaque grille, vous pouvez "Créez vos propres clés d'accès" ou "créer les clés d'accès d'un autre utilisateur" sur chaque grille.
- Si vous devez utiliser les mêmes clés sur les deux grilles, vous pouvez créer des clés sur la grille source, puis utiliser l'API du Gestionnaire de locataires pour les "`${post_edited_translations.segment}`" manuellement vers la grille de destination.



Lorsque vous clonez les clés d'accès S3 d'un utilisateur fédéré, l'utilisateur et les clés d'accès S3 sont clonés dans le locataire de destination.

`#{post_edited_translations.segment}`

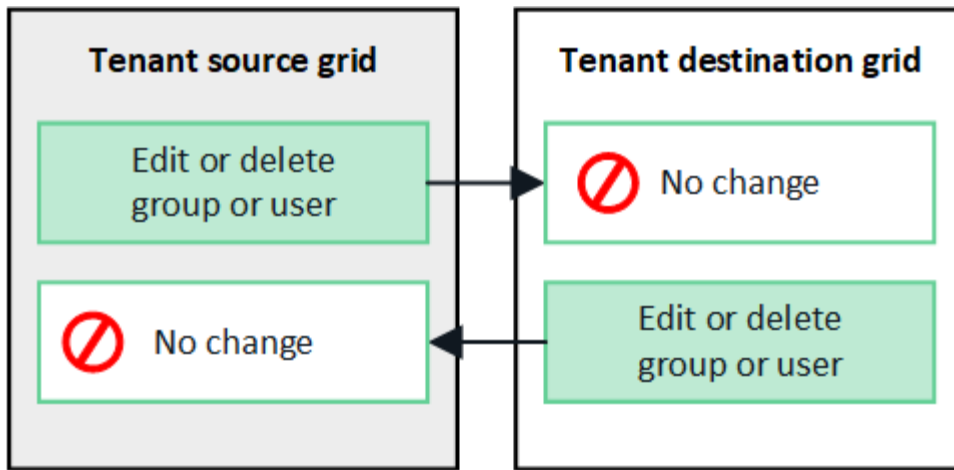
Le clonage s'effectue uniquement de la grille source du locataire vers la grille de destination du locataire. Si vous créez ou importez des groupes et des utilisateurs sur la grille de destination du locataire, StorageGRID ne clonera pas ces éléments en retour vers la grille source du locataire.



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

Le clonage n'a lieu que lorsque vous créez de nouveaux groupes et utilisateurs.

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



Cloner les clés d'accès S3 entre les grilles StorageGRID à l'aide de l'API de gestion des locataires

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

Avant de commencer

- `${post_edited_translations.segment}`
- `${post_edited_translations.segment}`
- Vous êtes connecté au Tenant Manager sur la grille source du locataire à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs qui possède le `"${post_edited_translations.segment}"`.
- `${post_edited_translations.segment}`



Lorsque vous clonez les clés d'accès S3 d'un utilisateur fédéré, l'utilisateur et les clés d'accès S3 sont ajoutés au locataire de destination.

`${post_edited_translations.segment}`

`${post_edited_translations.segment}`

Étapes

1. Utilisez le Tenant Manager sur la grille source, ["Créez vos propres clés d'accès"](#) et téléchargez le `.csv` fichier.
2. En haut du Tenant Manager, sélectionnez l'icône d'aide et sélectionnez **API documentation**.
3. Dans la section **s3**, sélectionnez le point de terminaison suivant :

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

POST

`/org/users/current-user/replicate-s3-access-key` Clone the current user's S3 key to the other grids.



4. Sélectionnez **Try it out**.

5. Dans la zone de texte **body**, remplacez les exemples d'entrées pour **accessKey** et **secretAccessKey** par les valeurs du fichier **.csv** que vous avez téléchargé.

Veillez à conserver les guillemets doubles autour de chaque chaîne de caractères.



6. Si la clé doit expirer, remplacez l'entrée d'exemple pour **expires** par la date et l'heure d'expiration sous la forme d'une chaîne au format de date et d'heure ISO 8601 (par exemple, 2024-02-28T22:46:33-08:00). Si la clé ne doit pas expirer, saisissez **null** comme valeur pour l'entrée **expires** (ou supprimez la ligne **Expires** et la virgule qui la précède).

7. Sélectionnez **Exécuter**.

8. `${post_edited_translations.segment}`

Cloner les clés d'accès d'un autre utilisateur

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

Étapes

1. À l'aide du Tenant Manager sur la grille source, `"${post_edited_translations.segment}"` et téléchargez le fichier **.csv**.
2. En haut du Tenant Manager, sélectionnez l'icône d'aide et sélectionnez **API documentation**.
3. Récupérez l'identifiant de l'utilisateur. Vous aurez besoin de cette valeur pour cloner les clés d'accès de l'autre utilisateur.

- a. `${post_edited_translations.segment}`

```
GET /org/users
```

- b. Sélectionnez **Try it out**.

- c. `${post_edited_translations.segment}`

- d. Sélectionnez **Exécuter**.

- e. `${post_edited_translations.segment}`

4. Dans la section **s3**, sélectionnez le point de terminaison suivant :

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



5. Sélectionnez **Try it out**.

6. Dans la zone de texte **userId**, collez l'identifiant utilisateur que vous avez copié.
7. Dans la zone de texte **corps**, remplacez les exemples d'entrées pour **example access key** et **secret access key** par les valeurs du fichier **.csv** pour cet utilisateur.

Veillez à conserver les guillemets doubles autour de la chaîne de caractères.

8. Si la clé doit expirer, remplacez l'exemple d'entrée pour **expires** par la date et l'heure d'expiration sous forme de chaîne au format date-heure ISO 8601 (par exemple, 2023-02-28T22:46:33-08:00). Si la clé ne doit pas expirer, saisissez **null** comme valeur pour l'entrée **expires** (ou supprimez la ligne **Expires** et la virgule précédente).
9. Sélectionnez **Exécuter**.
10. `${post_edited_translations.segment}`

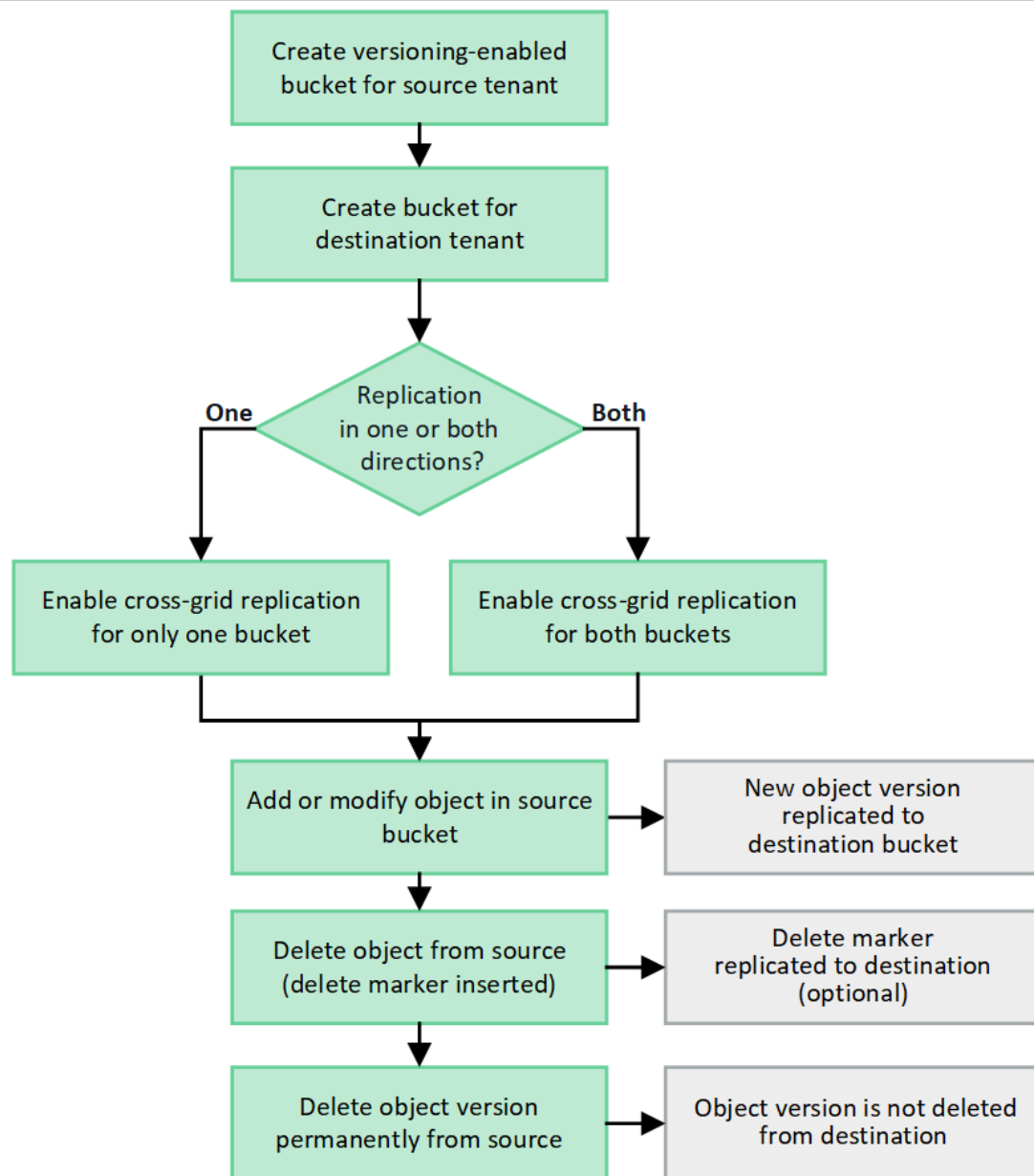
Gérer la réplication inter-grilles dans StorageGRID

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

Flux de travail pour la réplication inter-grilles

Le diagramme de flux de travail résume les étapes à suivre pour configurer la réplication inter-grilles entre les compartiments de deux grilles. Ces étapes sont décrites plus en détail ci-dessous.

Tenant user



Configurer la réplication inter-grilles

Avant de pouvoir utiliser la réplication inter-grilles, vous devez vous connecter aux comptes locataires correspondants sur chaque grille et créer deux compartiments. Ensuite, vous pouvez activer la réplication inter-grilles sur l'un ou les deux compartiments.

Avant de commencer

- Vous avez pris connaissance des exigences relatives à la réplication inter-grilles. Veuillez vous référer à ["Qu'est-ce que la réplication inter-grilles"](#).
- Vous utilisez un ["navigateur Web pris en charge"](#).
- Le compte locataire dispose de l'autorisation **Utiliser la connexion de fédération de grilles**, et des comptes locataires identiques existent sur les deux grilles. Voir ["Gérer les locataires autorisés pour la connexion à la fédération de grid"](#).
- L'utilisateur locataire avec lequel vous vous connectez existe déjà sur les deux grilles et appartient à un groupe d'utilisateurs qui possède le ["Autorisation d'accès root"](#).

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

Créez deux compartiments

Dans un premier temps, connectez-vous aux comptes locataires correspondants sur chaque grille et créez un compartiment sur chaque grille.

Étapes

1. À partir de l'une ou l'autre des grilles de la connexion de fédération de grilles, créez un nouveau compartiment :
 - a. Connectez-vous au compte locataire en utilisant les identifiants d'un utilisateur locataire qui existe sur les deux grilles.

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

- b. Suivez les instructions pour "[créer un compartiment S3](#)".



Les noms des compartiments et les régions peuvent être différents sur chaque grille.

- c. Dans l'onglet **Gérer les paramètres de l'objet**, sélectionnez **Activer le versionnage des objets**.
 - d. Si le verrouillage d'objet S3 est activé pour votre système StorageGRID, reportez-vous à "[Réplication inter-grilles avec S3 Object Lock](#)".
 - e. Sélectionnez **Créer un compartiment**.
 - f. Sélectionnez **Terminer**.
2. Répétez ces étapes pour créer un compartiment pour le même compte locataire sur l'autre grille dans la connexion de fédération de grilles.



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

Activer la réplication inter-grilles

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

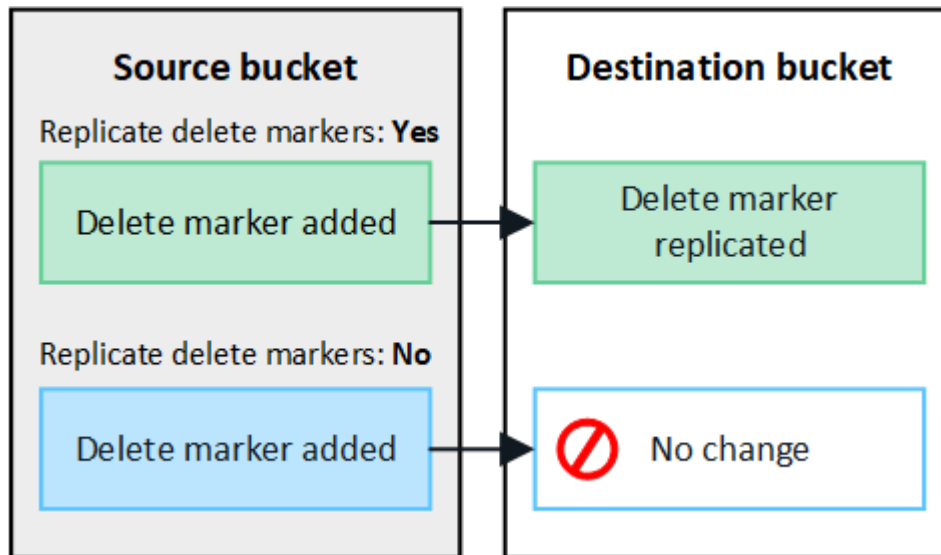
Étapes

1. À partir d'une grille dont vous souhaitez répliquer les objets, activez "[réplication inter-grilles dans une direction](#)" :
 - a. Connectez-vous au compte locataire pour le compartiment.
 - b. Sélectionnez **Afficher les compartiments** depuis le tableau de bord, ou sélectionnez **STOCKAGE (S3) > Compartiments**.
 - c. Sélectionnez le nom du compartiment dans le tableau pour accéder à la page de détails du compartiment.
 - d. Sélectionnez l'onglet **Réplication inter-grilles**.
 - e. Sélectionnez **Activer** et consultez la liste des exigences.
 - f. Si toutes les conditions requises sont remplies, sélectionnez la connexion de fédération de grille que

vous souhaitez utiliser.

g. Vous pouvez également modifier le paramètre **Répliquer les marqueurs de suppression** pour déterminer ce qui se passe sur la grille de destination si un client S3 envoie une requête de suppression à la grille source sans inclure d'ID de version :

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



Si la requête de suppression inclut un ID de version, cette version de l'objet est définitivement supprimée du compartiment source. StorageGRID ne réplique pas les requêtes de suppression qui incluent un ID de version, donc la même version de l'objet n'est pas supprimée de la destination.

Consultez ["Qu'est-ce que la réplification inter-grilles"](#) pour plus de détails.

- a. Vous pouvez également modifier le paramètre de la catégorie d'audit **Réplication inter-grilles** pour gérer le volume des messages d'audit :
 - **Erreur** (par défaut) : Seules les demandes de réplification inter-grilles ayant échoué sont incluses dans la sortie d'audit.
 - **Normal** : Toutes les demandes de réplification inter-grilles sont incluses, ce qui augmente considérablement le volume de la sortie d'audit.
- b. Veuillez vérifier vos sélections. Vous ne pouvez pas modifier ces paramètres à moins que les deux compartiments ne soient vides.
- c. Sélectionnez **Activer et tester**.

Après quelques instants, un message de réussite s'affiche. Les objets ajoutés à ce compartiment sont désormais automatiquement répliqués sur l'autre grille. **La réplification inter-grilles** s'affiche en tant que fonctionnalité activée sur la page des détails du compartiment.

2. Vous pouvez également vous rendre dans le compartiment correspondant sur l'autre grille et ["activer la réplification inter-grilles dans les deux sens"](#).

Tester la réplication entre les grilles

Si la réplication inter-grilles est activée pour un compartiment, vous devrez peut-être vérifier que la connexion et la réplication inter-grilles fonctionnent correctement et que les compartiments source et de destination répondent toujours à toutes les exigences (par exemple, le versionnage est toujours activé).

Avant de commencer

- Vous utilisez un ["navigateur Web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Autorisation d'accès root"](#).

Étapes

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

Si la connexion est saine, une bannière de réussite s'affiche. Dans le cas contraire, un message d'erreur apparaît, que vous et l'administrateur du grid pouvez utiliser pour résoudre le problème. Pour plus de détails, consultez ["Dépanner les erreurs de fédération de grille"](#).

6. Si la réplication inter-grilles est configurée pour fonctionner dans les deux sens, accédez au compartiment correspondant sur l'autre grille et sélectionnez **Tester la connexion** pour vérifier que la réplication inter-grilles fonctionne dans l'autre sens.

Désactiver la réplication inter-grilles

Vous pouvez arrêter définitivement la réplication inter-grilles si vous ne souhaitez plus copier des objets vers l'autre grille.

Avant de désactiver la réplication inter-grilles, notez les points suivants :

- La désactivation de la réplication inter-grilles ne supprime pas les objets déjà copiés entre les grilles. Par exemple, les objets dans `my-bucket` sur la grille 1 qui ont été copiés vers `my-bucket` sur la grille 2 ne sont pas supprimés si vous désactivez la réplication inter-grilles pour ce compartiment. Si vous souhaitez supprimer ces objets, vous devez les retirer manuellement.
- Si la réplication inter-grilles était activée pour chaque compartiment (c'est-à-dire si la réplication s'effectue dans les deux sens), vous pouvez désactiver la réplication inter-grilles pour l'un ou l'autre compartiment, voire pour les deux. Par exemple, vous pourriez vouloir désactiver la réplication des objets de `my-bucket` sur la grille 1 vers `my-bucket` sur la grille 2, tout en continuant à répliquer les objets de `my-bucket` sur la grille 2 vers `my-bucket` sur la grille 1.
- Vous devez désactiver la réplication inter-grilles avant de pouvoir supprimer l'autorisation d'un locataire à utiliser la connexion de fédération de grilles. Consultez ["Gérer les locataires autorisés"](#).
- Si vous désactivez la réplication inter-grilles pour un compartiment contenant des objets, vous ne pourrez pas réactiver la réplication inter-grilles à moins de supprimer tous les objets des compartiments source et de destination.



Vous ne pouvez pas réactiver la réplication à moins que les deux compartiments soient vides.

Avant de commencer

- Vous utilisez un ["navigateur Web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Autorisation d'accès root"](#).

Étapes

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

Après quelques instants, un message de réussite s'affiche. Les nouveaux objets ajoutés à ce compartiment ne peuvent plus être répliqués automatiquement sur l'autre grille. La **réplication inter-grilles** n'est plus affichée en tant que fonctionnalité activée sur la page Buckets.

2. Si la réplication inter-grilles a été configurée pour s'effectuer dans les deux sens, accédez au compartiment correspondant sur l'autre grille et arrêtez la réplication inter-grilles dans l'autre sens.

Afficher les connexions de fédération de grilles dans StorageGRID

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

Avant de commencer

- `${post_edited_translations.segment}`
- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Autorisation d'accès root"](#).

Étapes

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

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

Colonne	Description
Nom de la connexion	Les connexions de fédération de grid que ce locataire est autorisé à utiliser.

Colonne	Description
Buckets avec réplique inter-grille	Pour chaque connexion de fédération de grilles, les compartiments locataires pour lesquels la réplique inter-grilles est activée. Les objets ajoutés à ces compartiments seront répliqués sur l'autre grille de la connexion.
Dernière erreur	Pour chaque connexion de fédération de grilles, l'erreur la plus récente survenue, le cas échéant, lors de la réplique des données vers l'autre grille. Voir Effacez la dernière erreur .

2. Vous pouvez également sélectionner un nom de compartiment à `"${post_edited_translations.segment}"`.

Effacer la dernière erreur

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

- La version de l'objet source est introuvable.
- Le compartiment source est introuvable.
- Le compartiment de destination a été supprimé.
- Le compartiment de destination a été recréé par un compte différent.
- Le versionnage du bucket de destination est suspendu.
- Le compartiment de destination a été recréé par le même compte, mais il n'est plus versionné.



Cette colonne n'affiche que la dernière erreur de réplique inter-grilles survenue ; les erreurs précédentes qui auraient pu se produire ne seront pas affichées.

Étapes

1. Si un message apparaît dans la colonne **Dernière erreur**, consultez le texte du message.

Par exemple, cette erreur indique que le compartiment de destination pour la réplique inter-grilles était dans un état invalide, possiblement parce que le versionnage était suspendu ou que le S3 Object Lock était activé.

Grid federation connections

Displaying one result

Connection name	Buckets with cross-grid replication	Last error
Grid 1-Grid 2	my-cgr-bucket	2022-12-07 16:02:20 MST Cross-grid replication has encountered an error. Failed to send cross-grid replication request from source bucket 'my-cgr-bucket' to destination bucket 'my-cgr-bucket'. Error code: DestinationRequestError. Detail: InvalidBucketState. Confirm that the source and destination buckets have object versioning enabled and S3 Object Lock disabled. (logID 4791585492825418592)

2. Effectuez les actions recommandées. Par exemple, si le versionnage a été suspendu sur le compartiment de destination pour la réplique inter-grilles, réactivez le versionnage pour ce compartiment.

3. Sélectionnez la connexion dans le tableau.
4. Sélectionnez **Effacer l'erreur**.
5. Sélectionnez **Oui** pour effacer le message et mettre à jour l'état du système.
6. Attendez 5 à 6 minutes, puis ajoutez un nouvel objet au bucket. Vérifiez que le message d'erreur ne réapparaît pas.



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

7. Pour déterminer si des objets n'ont pas pu être répliqués en raison de l'erreur de compartiment, consultez ["Identifier et réessayer les opérations de réplication ayant échoué"](#).

Gérer les groupes et les utilisateurs

Utilisez la fédération d'identité dans StorageGRID

`${post_edited_translations.segment}`

Configurer la fédération d'identité pour Tenant Manager

Vous pouvez configurer la fédération d'identité pour le Tenant Manager si vous souhaitez que les groupes et utilisateurs de locataires soient gérés dans un autre système tel que Active Directory, Microsoft Entra ID, OpenLDAP ou Oracle Directory Server.

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Autorisation d'accès root"](#).
- Vous utilisez Active Directory, Microsoft Entra ID, OpenLDAP ou Oracle Directory Server comme fournisseur d'identité.



Si vous souhaitez utiliser un service LDAP v3 qui n'est pas répertorié, contactez le support technique.

- Si vous prévoyez d'utiliser OpenLDAP, vous devez configurer le serveur OpenLDAP. Voir [Instructions pour la configuration du serveur OpenLDAP](#).
- Si vous prévoyez d'utiliser le protocole Transport Layer Security (TLS) pour les communications avec le serveur LDAP, le fournisseur d'identité doit utiliser TLS 1.2 ou 1.3. Voir ["Chiffrements pris en charge pour les connexions TLS sortantes"](#).

À propos de cette tâche

La possibilité de configurer un service de fédération des identités pour votre locataire dépend de la manière dont votre compte de locataire a été configuré. Votre locataire peut partager le service de fédération des identités qui a été configuré pour le Grid Manager. Si vous voyez ce message lorsque vous accédez à la page Fédération des identités, vous ne pouvez pas configurer de source d'identité fédérée distincte 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.

`${post_edited_translations.segment}`

`${post_edited_translations.segment}`

Étapes

1. Sélectionnez **Gestion des accès > Fédération d'identités**.
2. Sélectionnez **Activer la fédération d'identités**.
3. Dans la section « Type de service LDAP », sélectionnez le type de service LDAP que vous souhaitez configurer.

LDAP service type

Select the type of LDAP service you want to configure.

Active Directory	Entra ID	OpenLDAP	Other
------------------	----------	----------	-------

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

4. Si vous avez sélectionné **Autre**, complétez les champs de la section Attributs LDAP. Sinon, passez à l'étape suivante.
 - **Nom unique de l'utilisateur** : le 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, saisissez `uid`.
 - **UUID utilisateur** : le 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, saisissez `nsuniqueid`. La valeur de chaque utilisateur pour l'attribut spécifié doit être un nombre hexadécimal de 32 chiffres, au format 16 octets ou chaîne, les traits d'union étant ignorés.
 - **Nom unique du groupe** : le 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, saisissez `cn`.
 - **UUID de groupe** : le nom de l'attribut qui contient l'identifiant 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, saisissez `nsuniqueid`. La valeur de chaque groupe pour l'attribut spécifié doit être un nombre hexadécimal de 32 chiffres, au format 16 octets ou chaîne de caractères, où les tirets sont ignorés.
5. Pour tous les types de services LDAP, saisissez les informations requises concernant le serveur LDAP et la connexion réseau dans la section Configurer le serveur LDAP.
 - **Nom d'hôte** : Le nom de domaine complet (FQDN) ou l'adresse IP du serveur LDAP.
 - **Port** : Le port utilisé pour se connecter au serveur LDAP.



Le port par défaut pour STARTTLS est 389, et le port par défaut pour LDAPS est 636. Cependant, vous pouvez utiliser n'importe quel port à condition que votre pare-feu soit correctement configuré.

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

Pour Active Directory, vous pouvez également spécifier le nom d'ouverture de session de niveau inférieur ou le User Principal Name.

L'utilisateur spécifié doit avoir l'autorisation de lister les groupes et les utilisateurs et d'accéder aux attributs suivants :

- sAMAccountName ou uid
- objectGUID, entryUUID, ou nsuniqueid
- cn
- memberOf ou isMemberOf
- **Active Directory** : objectSid, primaryGroupID, userAccountControl, et userPrincipalName
- **Entra ID** : accountEnabled et userPrincipalName

- **Mot de passe** : le mot de passe associé au nom d'utilisateur.



Si vous modifiez le mot de passe ultérieurement, vous devez le mettre à jour sur cette page.

- **DN de base du groupe** : le chemin complet du nom unique (DN) d'une sous-arborescence LDAP dans laquelle vous souhaitez 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=example,DC=com) peuvent être utilisés comme groupes fédérés.



Les valeurs du **nom unique du groupe** doivent être uniques au sein du **DN de base du groupe** auquel elles appartiennent.

- **DN de base utilisateur** : Le chemin complet du nom unique (DN) d'une sous-arborescence LDAP dans laquelle vous souhaitez rechercher des utilisateurs.



Les valeurs du **nom unique de l'utilisateur** doivent être uniques au sein du **DN de base utilisateur** auquel elles appartiennent.

- **Format du nom d'utilisateur de liaison** (facultatif) : Modèle de nom d'utilisateur par défaut que StorageGRID doit utiliser si le modèle ne peut pas être déterminé automatiquement.

Il est recommandé de fournir le **format du nom d'utilisateur de liaison** car cela peut permettre aux utilisateurs de se connecter si StorageGRID ne parvient pas à se lier au compte de service.

Saisissez l'un de ces modèles :

- **UserPrincipalName modèle (AD et Entra ID)**: [USERNAME]@example.com
- **Modèle de nom d'ouverture de session de niveau inférieur (AD et Entra ID)** : example\[USERNAME]
- **Modèle de nom unique** : CN=[USERNAME],CN=Users,DC=example,DC=com

Incluez **[USERNAME]** exactement comme écrit.

6. Dans la section Transport Layer Security (TLS), sélectionnez un paramètre de sécurité.

- **Utiliser STARTTLS** : Utilisez STARTTLS pour sécuriser les communications avec le serveur LDAP. Cette option est recommandée pour Active Directory, OpenLDAP ou Autre, mais cette option n'est pas prise en charge pour Microsoft Entra ID.
- **Utiliser LDAPS** : L'option LDAPS (LDAP sur SSL) utilise TLS pour établir une connexion au serveur LDAP. Vous devez sélectionner cette option pour Microsoft Entra ID.
- **N'utilisez pas TLS** : le trafic réseau entre le système StorageGRID et le serveur LDAP ne sera pas sécurisé. Cette option n'est pas prise en charge pour Microsoft Entra ID.



L'option « Ne pas utiliser TLS » n'est pas prise en charge si votre serveur Active Directory impose 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.

- **Utiliser le certificat CA du système d'exploitation** : Utilisez le certificat CA Grid 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 du certificat d'autorité de certification.

Testez la connexion et enregistrez la configuration

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

Étapes

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

Par exemple, saisissez votre propre nom d'utilisateur et votre mot de passe. N'incluez aucun caractère spécial dans le nom d'utilisateur, tel que @ ou /.

Test Connection

To test the connection and the bind username format, enter the username and password of a federated user. For example, enter your own federated username and password. The test values are not saved.

Test username

The username of a federated user.

Test password

Cancel

Test Connection

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

Forcer la synchronisation avec la source d'identité

Le système StorageGRID synchronise périodiquement les groupes fédérés et les utilisateurs à partir de la source d'identité. Vous pouvez forcer le démarrage de la synchronisation si vous souhaitez activer ou restreindre les autorisations des utilisateurs le plus rapidement possible.

Étapes

1. Accédez à la page de fédération d'identités.
2. Sélectionnez **Sync server** en haut de la page.

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



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

Désactivez la fédération d'identités

Vous pouvez désactiver temporairement ou définitivement la fédération d'identités pour les groupes et les utilisateurs. Lorsque la fédération d'identités est désactivée, il n'y a aucune communication entre StorageGRID et la source d'identités. Toutefois, les paramètres que vous avez configurés sont conservés, ce qui vous permet de réactiver facilement la fédération d'identités ultérieurement.

À propos de cette tâche

Avant de désactiver la fédération d'identités, vous devez prendre en compte les points suivants :

- Les utilisateurs fédérés ne pourront pas se connecter.
- Les utilisateurs fédérés actuellement connectés conserveront l'accès au système StorageGRID jusqu'à

l'expiration de leur session, mais ils ne pourront plus se connecter après l'expiration de celle-ci.

- La synchronisation entre le système StorageGRID et la source d'identité n'aura pas lieu et aucune alerte ne sera émise pour les comptes qui n'ont pas été synchronisés.
- La case à cocher **Activer la fédération d'identités** est désactivée si le statut de l'authentification unique (SSO) est **Activé** ou **Mode bac à sable**. Le statut SSO sur la page d'authentification unique doit être **Désactivé** avant que vous puissiez désactiver la fédération d'identités. Voir "[Désactivez l'authentification unique](#)".

Étapes

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

Instructions pour la configuration du serveur OpenLDAP

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



Pour les sources d'identité autres qu'Active Directory ou Microsoft Entra ID, StorageGRID ne bloque pas automatiquement l'accès S3 aux utilisateurs désactivés en externe. Pour bloquer l'accès S3, supprimez les clés S3 de l'utilisateur ou retirez l'utilisateur de tous les groupes.

Overlays Memberof et refint

Les superpositions memberof et refint doivent être activées. Pour plus d'informations, consultez les instructions relatives à la gestion des appartenances aux groupes inversées dans le "[Documentation OpenLDAP : Guide de l'administrateur version 2.4](#)".

Indexage

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.

Consultez les informations relatives à la gestion des appartenances aux groupes inversés dans le "[Documentation OpenLDAP : Guide de l'administrateur version 2.4](#)".

`#{post_edited_translations.segment}`

Créez des groupes pour un locataire S3 dans StorageGRID

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

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Autorisation d'accès root"](#).
- Si vous prévoyez d'importer un groupe fédéré, vous avez ["fédération d'identité configurée"](#), et le groupe fédéré existe déjà dans la source d'identité configurée.
- Si votre compte locataire dispose de l'autorisation **Utiliser la connexion de fédération de grille**, vous avez examiné le flux de travail et les considérations pour ["clonage des groupes de locataires et des utilisateurs"](#), et vous êtes connecté à la grille source du locataire.

`${post_edited_translations.segment}`

Pour commencer, accédez à l'assistant de création de groupe.

Étapes

1. Sélectionnez **Gestion des accès > Groupes**.
2. Si votre compte locataire dispose de l'autorisation **Utiliser la connexion de fédération de grilles**, vérifiez qu'une bannière bleue s'affiche, indiquant que les nouveaux groupes créés sur cette grille seront clonés sur le même locataire dans l'autre grille de la connexion. Si cette bannière n'apparaît pas, vous êtes peut-être connecté à la grille de destination du locataire.

Groups

Create and manage local and federated groups. Set group permissions to control access to specific pages and features.

Create group

Actions ▾

Search groups by name

No results

This tenant has **Use grid federation connection** permission for connection Grid 1 to Grid 2. New tenant groups will be automatically cloned to the same tenant on the other grid in the connection. If you edit or remove a group, your changes will not be synced to the other grid.

☐	Name ▾	ID ▾	Type ▾	Access mode ▾
No groups found				
Create group				

3. Sélectionnez **Créer un groupe**.

Choisissez un type de groupe

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

Étapes

1. Sélectionnez l'onglet **Groupe local** pour créer un groupe local, ou sélectionnez l'onglet **Groupe fédéré** pour importer un groupe à partir de la source d'identité précédemment configurée.

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

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



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

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

3. Sélectionnez **Continue**.

Gérer les autorisations de groupe

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

Étapes

1. Pour le **mode d'accès**, sélectionnez l'une des options suivantes :
 - **Lecture-écriture** (par défaut) : Les utilisateurs peuvent se connecter à Tenant Manager et gérer la configuration du locataire.
 - **Lecture seule** : Les utilisateurs peuvent uniquement consulter les paramètres et les fonctionnalités. Ils ne peuvent apporter aucune modification ni effectuer d'opérations dans le Tenant Manager ou l'API Tenant Management. Les utilisateurs locaux en lecture seule peuvent changer leur propre mot de passe.



Si un utilisateur appartient à plusieurs groupes et que l'un de ces groupes est configuré en lecture seule, l'utilisateur aura un accès en lecture seule à tous les paramètres et fonctionnalités sélectionnés.

2. Sélectionnez une ou plusieurs autorisations pour ce groupe.

Voir "[\\${post_edited_translations.segment}](#)".

3. Sélectionnez **Continue**.

Définir la stratégie de groupe S3

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

Étapes

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

stratégie de groupe	Description
Aucun accès S3	Par défaut. Les utilisateurs de ce groupe n'ont pas accès aux ressources S3, à moins que l'accès ne soit accordé par une politique de compartiment. Si vous sélectionnez cette option, seul l'utilisateur root aura accès aux ressources S3 par défaut.

stratégie de groupe	Description
Accès en lecture seule	Les utilisateurs de ce groupe disposent d'un accès en lecture seule aux ressources S3. Par exemple, les utilisateurs de ce groupe peuvent lister les 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 apparaît dans la zone de texte. Vous ne pouvez pas modifier cette chaîne.
Accès complet	Les utilisateurs de ce groupe disposent d'un accès complet aux ressources S3, y compris les compartiments. Lorsque vous sélectionnez cette option, la chaîne JSON d'une stratégie de groupe d'accès complet s'affiche dans la zone de texte. Vous ne pouvez pas modifier cette chaîne.
Atténuation des ransomwares	Cet exemple de politique s'applique à tous les compartiments de ce locataire. Les utilisateurs de ce groupe peuvent effectuer des actions courantes, mais ne peuvent pas supprimer définitivement des objets des compartiments pour lesquels le versionnement d'objets est activé. Les utilisateurs Tenant Manager disposant de l'autorisation Manage all buckets peuvent ignorer cette stratégie de groupe. Limitez l'autorisation Manage all buckets aux utilisateurs de confiance et utilisez l'authentification multifacteur (MFA) lorsque disponible.
Personnalisé	<code>\${post_edited_translations.segment}</code>

- Si vous avez sélectionné **Custom**, saisissez la stratégie de groupe. Chaque stratégie de groupe est limitée à une taille de 5 120 octets. Vous devez saisir une chaîne au format JSON valide.

Pour obtenir des informations détaillées sur les politiques de groupe, y compris la syntaxe du langage et des exemples, consultez ["Exemples de stratégies de groupe"](#).

- Si vous créez un groupe local, sélectionnez **Continuer**. Si vous créez un groupe fédéré, sélectionnez **Créer un groupe** puis **Terminer**.

Ajouter des utilisateurs (groupes locaux uniquement)

`${post_edited_translations.segment}`



Si votre compte locataire dispose de l'autorisation **Utiliser la connexion de fédération de grille**, les utilisateurs que vous sélectionnez lors de la création d'un groupe local sur la grille source ne sont pas inclus lorsque le groupe est cloné sur le cluster de destination. Pour cette raison, ne sélectionnez pas d'utilisateurs lors de la création du groupe. Sélectionnez plutôt le groupe lors de la création des utilisateurs.

Étapes

- Facultativement, sélectionnez un ou plusieurs utilisateurs locaux pour ce groupe.
- Sélectionnez **Créer un groupe** et **Terminer**.

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

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

Autorisations de gestion des locataires StorageGRID

Avant de créer un groupe de locataires, réfléchissez aux autorisations que vous souhaitez lui attribuer. Les autorisations de gestion des locataires déterminent les tâches que les utilisateurs peuvent effectuer à l'aide du Tenant Manager 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 se connecter au Tenant Manager ou utiliser l'API Tenant Management, 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
- `${post_edited_translations.segment}`

Pour toutes les autorisations, le paramètre de mode d'accès du groupe détermine si les utilisateurs peuvent modifier les paramètres et effectuer des opérations ou s'ils peuvent uniquement consulter les paramètres et fonctionnalités associés.



Si un utilisateur appartient à plusieurs groupes et que l'un de ces groupes est configuré en lecture seule, l'utilisateur aura un accès en lecture seule à tous les paramètres et fonctionnalités sélectionnés.

`${post_edited_translations.segment}`

Autorisation	Description	Détails
Accès root	Offre un accès complet au Tenant Manager et à l'API Tenant Management.	
Gérez vos propres identifiants S3	<code>\${post_edited_translations.segment}</code>	Les utilisateurs qui ne disposent pas de cette autorisation ne voient pas l'option de menu STOCKAGE (S3) > Mes clés d'accès S3 .
<code>\${post_edited_translations.segment}</code>	<code>\${post_edited_translations.segment}</code>	<code>\${post_edited_translations.segment}</code> Cette autorisation est remplacée par l'autorisation Gérer tous les compartiments. Elle n'affecte pas les politiques de groupe ou de compartiment S3 utilisées par les clients S3 ou la console S3.

Autorisation	Description	Détails
<code>\$_post_edited_translations.segment</code>	Permet aux utilisateurs d'utiliser le Tenant Manager et l'API Tenant Management pour créer et supprimer des compartiments S3 et gérer les paramètres de tous les compartiments S3 du compte locataire, indépendamment des stratégies de compartiment S3 ou de groupe.	<code>\$_post_edited_translations.segment</code> Cette autorisation remplace l'autorisation Afficher tous les compartiments. Elle n'affecte pas les politiques de compartiment ou de groupe S3 utilisées par les clients S3 ou la S3 Console.
Gérer les points de terminaison	Permet aux utilisateurs d'utiliser le Tenant Manager ou l'API de gestion des locataires pour créer ou modifier des points de terminaison de services de plateforme, qui sont utilisés comme destination pour les services de plateforme StorageGRID.	Les utilisateurs qui ne disposent pas de cette autorisation ne voient pas l'option de menu Points de terminaison des services de la plateforme .
<code>\$_post_edited_translations.segment</code>	<code>\$_post_edited_translations.segment</code>	

Gérer les groupes de locataires StorageGRID

`$_post_edited_translations.segment`

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un "navigateur Web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Autorisation d'accès root".

`$_post_edited_translations.segment`

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

Étapes

1. Sélectionnez **Gestion des accès > Groupes**.
2. `$_post_edited_translations.segment`

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

- `$_post_edited_translations.segment`
 - Au besoin, un message de bannière indique si des groupes n'ont pas été clonés sur le locataire de la grille de destination. Vous pouvez `$_post_edited_translations.segment` qui ont échoué.
3. `$_post_edited_translations.segment`
 - a. Cochez la case correspondant au groupe.
 - b. Sélectionnez **Actions > Modifier le nom du groupe**.
 - c. Saisissez le nouveau nom.
 - d. `$_post_edited_translations.segment`

4. `{post_edited_translations.segment}`
 - `{post_edited_translations.segment}`
 - Sélectionnez la case à cocher du groupe, puis sélectionnez **Actions > Afficher les détails du groupe**.
5. `{post_edited_translations.segment}`
 - Nom d'affichage
 - Nom unique
 - Type
 - Mode d'accès
 - Autorisations
 - `{post_edited_translations.segment}`
 - `{post_edited_translations.segment}`
 - `{post_edited_translations.segment}`
 - `{post_edited_translations.segment}`
 - `{post_edited_translations.segment}`
6. Modifiez les paramètres de groupe selon vos besoins. Reportez-vous à "[Créer des groupes pour un locataire S3](#)" pour obtenir des détails sur les informations à saisir.
 - a. Dans la section Vue d'ensemble, modifiez le nom d'affichage en sélectionnant le nom ou l'icône de modification .
 - b. Dans l'onglet **Autorisations du groupe**, mettez à jour les autorisations et sélectionnez **Enregistrer les modifications**.
 - c. `{post_edited_translations.segment}`
`{post_edited_translations.segment}`
7. Pour ajouter un ou plusieurs utilisateurs locaux existants au groupe :
 - a. `{post_edited_translations.segment}`



- b. `{post_edited_translations.segment}`
- c. `{post_edited_translations.segment}`

Un message de confirmation apparaît en haut à droite.

8. `{post_edited_translations.segment}`
 - a. `{post_edited_translations.segment}`

- b. `${post_edited_translations.segment}`
- c. `${post_edited_translations.segment}`

Un message de confirmation apparaît en haut à droite.

9. `${post_edited_translations.segment}`

`${post_edited_translations.segment}`

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



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

Étapes

1. Sélectionnez **Gestion des accès > Groupes**.
2. `${post_edited_translations.segment}`
3. Sélectionnez **Actions > Dupliquer le groupe**.
4. Reportez-vous à "[Créer des groupes pour un locataire S3](#)" pour plus de détails sur les informations à saisir.
5. Sélectionnez **Créer un groupe**.

Réessayer le clonage du groupe

`${post_edited_translations.segment}`

1. Sélectionnez chaque groupe qui indique (*Échec du clonage*) sous le nom du groupe.
2. Sélectionnez **Actions > Clone groups**.
3. Consultez l'état de l'opération de clonage sur la page de détails de chaque groupe que vous clonez.

Pour plus d'informations, voir "[Cloner les groupes de locataires et les utilisateurs](#)".

Supprimer un ou plusieurs groupes

Vous pouvez supprimer un ou plusieurs groupes. Tous les utilisateurs qui appartiennent uniquement à un groupe supprimé ne pourront plus se connecter au Gestionnaire de locataires ni utiliser le compte de locataire.



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

Étapes

1. Sélectionnez **Gestion des accès > Groupes**.
2. Cochez la case pour chaque groupe que vous souhaitez supprimer.
3. Sélectionnez **Actions > Supprimer le groupe** ou **Actions > Supprimer les groupes**.

Une boîte de dialogue de confirmation apparaît.

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

Configurez AssumeRole

Avant de commencer

Vous devez être administrateur pour configurer AssumeRole.

À propos de cette tâche

Pour configurer AssumeRole, créez le groupe cible à assumer, si le groupe n'existe pas déjà. Modifiez la politique S3 du groupe pour spécifier les actions autorisées pour assumer ce groupe. Modifiez la politique de confiance S3 du groupe pour spécifier les utilisateurs de confiance autorisés à assumer le groupe avec l'API AssumeRole.

Les informations d'identification de sécurité temporaires créées lors de l'adoption de ce groupe sont valides pour une durée limitée. La session dure entre 15 minutes et 12 heures, et la durée par défaut est d'une heure. Lorsque vous retirez l'utilisateur de la stratégie d'approbation S3 du groupe, l'utilisateur ne peut plus adopter ce groupe.

Étapes

- Sélectionnez **Gestion des accès > Groupes**.
- Cliquez sur le nom du groupe.
- Sélectionnez l'onglet **Stratégie de confiance S3**.
- Ajoutez votre politique de confiance S3, y compris une liste d'utilisateurs pouvant effectuer AssumeRole.
- Sélectionnez **Save changes**.
- Sélectionnez l'onglet **Stratégie de groupe S3**.
- `${post_edited_translations.segment}`
- Sélectionnez **Save changes**.

Exemple d'une AssumeRole politique de confiance S3

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Principal": {
        "AWS": [
          "urn:sgws:identity::1234567890:user/user1",
          "arn:aws:iam::1234567890:user/user2"
        ]
      }
    }
  ]
}
```

Une fois la configuration terminée, les utilisateurs listés dans la stratégie d'approbation S3 peuvent effectuer

AssumeRole et recevoir des informations d'identification. Les autorisations finales sont déterminées par la stratégie de groupe, la stratégie de compartiment et la stratégie de session. Pour plus d'informations, consultez ["Utilisez les politiques d'accès"](#).

Gérer les utilisateurs locataires de StorageGRID

Vous pouvez créer des utilisateurs locaux et les affecter à des groupes locaux afin de définir les fonctionnalités auxquelles ces utilisateurs peuvent accéder. Vous pouvez également importer des utilisateurs fédérés. Le Tenant Manager inclut un utilisateur local prédéfini, nommé « root ». Bien que vous puissiez ajouter et supprimer des utilisateurs locaux, vous ne pouvez pas supprimer l'utilisateur root.



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

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Autorisation d'accès root"](#).
- Si votre compte locataire dispose de l'autorisation **Utiliser la connexion de fédération de grille**, vous avez examiné le flux de travail et les considérations pour ["clonage des groupes de locataires et des utilisateurs"](#), et vous êtes connecté à la grille source du locataire.

`${post_edited_translations.segment}`

`${post_edited_translations.segment}`

Les utilisateurs S3 qui n'appartiennent à aucun groupe ne disposent pas d'autorisations de gestion et aucune politique de groupe S3 ne leur est appliquée. Ces utilisateurs peuvent disposer d'un accès aux compartiments S3 accordé via une politique de compartiment.

Accédez à l'assistant de création d'utilisateur

Étapes

1. `${post_edited_translations.segment}`

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

Users

View local and federated users. Edit properties and group membership of local users.

[Create local user](#) [Import federated users](#) [Actions](#)

Displaying one result

Username

Full name

Denied access

Type

root

Root

No

Local

[Previous](#) [Next](#)

2. Sélectionnez **Créer un utilisateur**.

Saisissez vos identifiants

Étapes

1. `${post_edited_translations.segment}`

Champ	Description
<code>\${post_edited_translations.segment}</code>	Le nom complet de cet utilisateur, par exemple, le prénom et le nom d'une personne ou le nom d'une application.
Nom d'utilisateur	<code>\${post_edited_translations.segment}</code> <code>\${post_edited_translations.segment}</code>
Mot de passe et confirmation du mot de passe	<code>\${post_edited_translations.segment}</code>
<code>\${post_edited_translations.segment}</code>	Sélectionnez Oui pour empêcher cet utilisateur de se connecter au compte locataire, même s'il peut encore appartenir à un ou plusieurs groupes. <code>\${post_edited_translations.segment}</code>

2. Sélectionnez **Continuer**.

Attribuer aux groupes

Étapes

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

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

Les utilisateurs qui n'appartiennent à aucun groupe ne disposeront d'aucune autorisation de gestion. Les autorisations sont cumulatives. Les utilisateurs disposeront de toutes les autorisations pour tous les groupes auxquels ils appartiennent. Voir "`${post_edited_translations.segment}`".

2. Sélectionnez **Créer un utilisateur**.

Si votre compte locataire dispose de l'autorisation **Utiliser la connexion de fédération de grille** et que vous vous trouvez sur la grille source du locataire, le nouvel utilisateur local est cloné sur la grille de destination du locataire. **Succès** apparaît en tant que **Statut de clonage** dans la section Aperçu de la page des détails de l'utilisateur.

3. `#{post_edited_translations.segment}`

`#{post_edited_translations.segment}`

Étapes

1. `#{post_edited_translations.segment}`

- Consultez les informations fournies sur la page Utilisateurs, qui répertorie les informations de base pour tous les utilisateurs locaux et fédérés de ce compte locataire.

`#{post_edited_translations.segment}`

- `#{post_edited_translations.segment}`
- Au besoin, un message de bannière indique si des utilisateurs n'ont pas été clonés vers le locataire sur la grille de destination. Vous pouvez [#{post_edited_translations.segment}](#).

3. `#{post_edited_translations.segment}`

- Cochez la case pour l'utilisateur.
- Sélectionnez **Actions > Modifier le nom complet**.
- Saisissez le nouveau nom.
- `#{post_edited_translations.segment}`

4. `#{post_edited_translations.segment}`

- Sélectionnez le nom d'utilisateur.
- `#{post_edited_translations.segment}`

5. `#{post_edited_translations.segment}`

- `#{post_edited_translations.segment}`
- Nom d'utilisateur
- `#{post_edited_translations.segment}`
- `#{post_edited_translations.segment}`
- Mode d'accès
- Adhésion au groupe
- `#{post_edited_translations.segment}`
 - `#{post_edited_translations.segment}`
 - Une bannière bleue indique que si vous modifiez cet utilisateur, vos modifications ne seront pas synchronisées avec l'autre grille.

- Modifiez les paramètres utilisateur selon vos besoins. Consultez [#{post_edited_translations.segment}](#) pour obtenir des détails sur les informations à saisir.

- Dans la section Vue d'ensemble, modifiez le nom complet en sélectionnant le nom ou l'icône de modification .

Vous ne pouvez pas changer le nom d'utilisateur.

- b. `#{post_edited_translations.segment}`
 - c. Dans l'onglet **Accès**, sélectionnez **Non** pour autoriser l'utilisateur à se connecter ou **Oui** pour l'empêcher de se connecter. Ensuite, sélectionnez **Enregistrer les modifications**.
 - d. Dans l'onglet **Touches d'accès**, sélectionnez **Créer une clé** et suivez les instructions pour "[création des clés d'accès S3 d'un autre utilisateur](#)".
 - e. Dans l'onglet **Groupes**, sélectionnez **Modifier les groupes** pour ajouter l'utilisateur à des groupes ou le retirer de groupes. Ensuite, sélectionnez **Enregistrer les modifications**.
7. `#{post_edited_translations.segment}`

Importer les utilisateurs fédérés

Vous pouvez importer un ou plusieurs utilisateurs fédérés, jusqu'à un maximum de 100 utilisateurs, directement dans la page Utilisateurs.

Étapes

1. `#{post_edited_translations.segment}`
2. Sélectionnez **Importer les utilisateurs fédérés**.
3. Saisissez l'UUID ou le nom d'utilisateur d'un ou de plusieurs utilisateurs fédérés.

Pour plusieurs entrées, ajoutez chaque UUID ou nom d'utilisateur sur une nouvelle ligne.

4. Sélectionnez **Importer**.

Si l'importation dans le champ Utilisateurs échoue pour un ou plusieurs utilisateurs, procédez comme suit :

- a. Développez **Utilisateurs non importés** et sélectionnez **Copier les utilisateurs**.
- b. Réessayez l'importation en sélectionnant **Précédent** et en collant les utilisateurs copiés dans la boîte de dialogue **Import federated users**.

Après la fermeture de la boîte de dialogue **Importer les utilisateurs fédérés**, les informations des utilisateurs fédérés s'affichent sur la page Utilisateurs pour les utilisateurs importés avec succès.

`#{post_edited_translations.segment}`

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



`#{post_edited_translations.segment}`

Étapes

1. `#{post_edited_translations.segment}`
2. Cochez la case correspondant à l'utilisateur que vous souhaitez dupliquer.
3. `#{post_edited_translations.segment}`
4. Consultez [#{post_edited_translations.segment}](#) pour obtenir des détails sur les informations à saisir.
5. Sélectionnez **Créer un utilisateur**.

`${post_edited_translations.segment}`

`${post_edited_translations.segment}`

1. `${post_edited_translations.segment}`
2. Sélectionnez **Actions** > **Cloner les utilisateurs**.
3. Consultez l'état de l'opération de clonage depuis la page de détails de chaque utilisateur que vous clonez.

Pour plus d'informations, voir "[Cloner les groupes de locataires et les utilisateurs](#)".

`${post_edited_translations.segment}`

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



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



`${post_edited_translations.segment}`

Étapes

1. `${post_edited_translations.segment}`
2. `${post_edited_translations.segment}`
3. Sélectionnez **Actions** > **Supprimer l'utilisateur** ou **Actions** > **Supprimer les utilisateurs**.

Une boîte de dialogue de confirmation apparaît.

4. Sélectionnez **Supprimer l'utilisateur** ou **Supprimer les utilisateurs**.

Gérer les clés d'accès S3

Gérer les clés d'accès S3 dans StorageGRID

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

Les clés d'accès S3 peuvent être gérées comme suit :

- Les utilisateurs disposant de l'autorisation **Gérer vos propres informations d'identification S3** peuvent créer ou supprimer leurs propres clés d'accès S3.
- Les utilisateurs disposant de l'autorisation **Root access** peuvent gérer les clés d'accès du compte racine S3 et de tous les autres utilisateurs. Les clés d'accès racine offrent un accès complet à tous les compartiments et objets pour le locataire, sauf si elles sont explicitement désactivées par une stratégie de compartiment.

StorageGRID prend en charge l'authentification Signature Version 2 et Signature Version 4. L'accès inter-comptes n'est pas autorisé, sauf s'il est explicitement activé par une stratégie de compartiment.

Créez vos propres clés d'accès S3 dans StorageGRID

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

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs qui possède le `"${post_edited_translations.segment}"`.

À propos de cette tâche

Vous pouvez créer une ou plusieurs clés d'accès S3 qui vous permettent de créer et de gérer des compartiments pour votre compte 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 celles que vous n'utilisez pas. Si vous ne disposez que d'une seule clé et qu'elle est sur le point d'expirer, créez-en une nouvelle avant l'expiration de l'ancienne, puis supprimez l'ancienne.

Chaque clé peut avoir une date d'expiration spécifique ou ne pas avoir d'expiration. Suivez ces directives concernant la durée d'expiration :

- Définissez un délai d'expiration pour vos clés afin de limiter votre accès à une période donnée. Définir un délai d'expiration court peut aider à réduire les risques si votre ID de clé d'accès et votre clé d'accès secrète sont accidentellement exposés. 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 périodiquement de nouvelles clés, vous n'avez pas besoin de définir de délai d'expiration pour vos clés. Si vous décidez ultérieurement de créer de nouvelles clés, supprimez manuellement les anciennes clés.



Les compartiments et objets S3 appartenant à votre compte sont accessibles à l'aide de l'ID de clé d'accès et de la clé d'accès secrète affichés pour votre compte dans le Tenant Manager. Pour cette raison, protégez les clés d'accès comme vous le feriez pour un mot de passe. Effectuez une rotation régulière des clés d'accès, supprimez toutes les clés inutilisées de votre compte et ne les partagez jamais avec d'autres utilisateurs.

Étapes

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

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

2. Sélectionnez **Créer une clé**.

3. Effectuez l'une des opérations suivantes :

- Sélectionnez **Ne pas définir de date d'expiration** pour créer une clé qui n'expirera pas. (Par défaut)
- Sélectionnez **Définir une date d'expiration**, puis indiquez la date et l'heure d'expiration.



La date d'expiration peut être fixée à un maximum de cinq ans à compter de la date actuelle. L'heure d'expiration peut être fixée à un minimum d'une minute à compter de l'heure actuelle.

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

La boîte de dialogue « Download access key » s'affiche, indiquant votre access key ID et votre secret access key.

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



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

6. Sélectionnez **Terminer**.

La nouvelle clé est répertoriée sur la page My access keys.

7. Si votre compte locataire dispose de l'autorisation **Utiliser la connexion de fédération de grille**, vous pouvez éventuellement utiliser l'API Tenant Management pour cloner manuellement les clés d'accès S3 du locataire de la grille source vers le locataire de la grille de destination. Voir "[Cloner les clés d'accès S3 à l'aide de l'API](#)".

Consultez vos clés d'accès S3 dans StorageGRID

Si vous utilisez un locataire S3 et que vous disposez de "[autorisation appropriée](#)", vous pouvez afficher la liste de vos clés d'accès S3. Vous pouvez trier la liste par date d'expiration afin de déterminer quelles clés vont bientôt expirer. Au besoin, vous pouvez "[\\${post_edited_translations.segment}](#)" ou "[\\${post_edited_translations.segment}](#)" que vous n'utilisez plus.



Les compartiments et objets S3 appartenant à votre compte sont accessibles à l'aide de l'ID de clé d'accès et de la clé d'accès secrète affichés pour votre compte dans le Tenant Manager. Pour cette raison, protégez les clés d'accès comme vous le feriez pour un mot de passe. Effectuez une rotation régulière des clés d'accès, supprimez toutes les clés inutilisées de votre compte et ne les partagez jamais avec d'autres utilisateurs.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un "[navigateur Web pris en charge](#)".
- Vous appartenez à un groupe d'utilisateurs qui possède l'autorisation Gérer vos propres informations d'identification S3 "[\\${post_edited_translations.segment}](#)".

Étapes

1. Sélectionnez **STOCKAGE (S3) > Mes clés d'accès**.
2. [\\${post_edited_translations.segment}](#)
3. [\\${post_edited_translations.segment}](#)

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

Les clés expirées sont supprimées automatiquement.

Supprimez vos propres clés d'accès S3 dans StorageGRID

Si vous utilisez un tenant S3 et que vous disposez des autorisations nécessaires, vous pouvez supprimer vos propres clés d'accès S3. Après la suppression d'une clé d'accès, elle ne peut plus être utilisée pour accéder aux objets et aux compartiments du compte du tenant.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous avez le ["Gérez vos propres autorisations d'identifiants S3"](#).



Les compartiments et objets S3 appartenant à votre compte sont accessibles à l'aide de l'ID de clé d'accès et de la clé d'accès secrète affichés pour votre compte dans le Tenant Manager. Pour cette raison, protégez les clés d'accès comme vous le feriez pour un mot de passe. Effectuez une rotation régulière des clés d'accès, supprimez toutes les clés inutilisées de votre compte et ne les partagez jamais avec d'autres utilisateurs.

Étapes

1. Sélectionnez **STOCKAGE (S3) > Mes clés d'accès**.
2. `${post_edited_translations.segment}`
3. Sélectionnez la touche **Delete key**.
4. Dans la boîte de dialogue de confirmation, sélectionnez **Delete key**.

Un message de confirmation apparaît dans le coin supérieur droit de la page.

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

Si vous utilisez un locataire S3 et que vous disposez des autorisations appropriées, vous pouvez créer des clés d'accès S3 pour d'autres utilisateurs, comme des applications qui ont besoin d'accéder aux compartiments et aux objets.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Autorisation d'accès root"](#).

À propos de cette tâche

Vous pouvez créer une ou plusieurs clés d'accès S3 pour d'autres utilisateurs afin qu'ils puissent créer et gérer des compartiments pour leur compte locataire. Après avoir créé une nouvelle clé d'accès, mettez à jour l'application avec le nouvel ID de clé d'accès et la nouvelle clé d'accès secrète. Par mesure de sécurité, ne créez pas plus de clés que nécessaire et supprimez celles qui ne sont pas utilisées. Si vous ne possédez qu'une seule clé et qu'elle est sur le point d'expirer, créez-en une nouvelle avant l'expiration de l'ancienne, puis supprimez cette dernière.

Chaque clé peut avoir une date d'expiration spécifique ou ne pas avoir d'expiration. Suivez ces directives concernant la durée d'expiration :

- Définissez une date d'expiration pour les clés afin de limiter l'accès de l'utilisateur à une période donnée. La définition d'une date d'expiration courte peut aider à réduire les risques si l'ID de clé d'accès et la clé d'accès secrète sont accidentellement exposés. 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, il n'est pas nécessaire de définir une date d'expiration pour les clés. Si vous décidez ultérieurement de créer de nouvelles clés, supprimez les anciennes clés manuellement.



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

Étapes

1. `${post_edited_translations.segment}`
2. Sélectionnez l'utilisateur dont vous souhaitez gérer les clés d'accès S3.

La page de détails de l'utilisateur s'affiche.

3. Sélectionnez **Access keys**, puis sélectionnez **Create key**.
4. Effectuez l'une des opérations suivantes :
 - Sélectionnez **Ne pas définir de date d'expiration** pour créer une clé qui n'expire pas. (Par défaut)
 - Sélectionnez **Définir une date d'expiration**, puis indiquez la date et l'heure d'expiration.



La date d'expiration peut être fixée à un maximum de cinq ans à compter de la date actuelle. L'heure d'expiration peut être fixée à un minimum d'une minute à compter de l'heure actuelle.

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

`${post_edited_translations.segment}`

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



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

7. Sélectionnez **Terminer**.

La nouvelle clé est répertoriée dans l'onglet Clés d'accès de la page de détails de l'utilisateur.

8. Si votre compte locataire dispose de l'autorisation **Utiliser la connexion de fédération de grille**, vous pouvez éventuellement utiliser l'API Tenant Management pour cloner manuellement les clés d'accès S3 du locataire de la grille source vers le locataire de la grille de destination. Voir "[Cloner les clés d'accès S3 à l'aide de l'API](#)".

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

Si vous utilisez un tenant S3 et que vous disposez des autorisations nécessaires, vous pouvez consulter les clés d'accès S3 d'un autre utilisateur. Vous pouvez trier la liste par date d'expiration afin de déterminer quelles clés expireront bientôt. Au besoin, vous

pouvez créer de nouvelles clés et supprimer les clés qui ne sont plus utilisées.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous disposez de ["Autorisation d'accès root"](#).



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

Étapes

1. `${post_edited_translations.segment}`
2. Sur la page Utilisateurs, sélectionnez l'utilisateur dont vous souhaitez consulter les clés d'accès S3.
3. `${post_edited_translations.segment}`
4. Triez les clés par **heure d'expiration** ou **ID de clé d'accès**.
5. `${post_edited_translations.segment}`

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 connexes

- ["Créer les clés d'accès S3 d'un autre utilisateur"](#)
- ["\\${post_edited_translations.segment}"](#)

Supprimer les clés d'accès S3 d'un autre utilisateur dans StorageGRID

Si vous utilisez un tenant S3 et que vous disposez des autorisations nécessaires, vous pouvez supprimer les clés d'accès S3 d'un autre utilisateur. Après la suppression d'une clé d'accès, elle ne peut plus être utilisée pour accéder aux objets et aux compartiments du compte du tenant.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous disposez de ["Autorisation d'accès root"](#).



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

Étapes

1. `${post_edited_translations.segment}`

2. `${post_edited_translations.segment}`
3. Sur la page Détails de l'utilisateur, sélectionnez **Clés d'accès**, puis cochez la case correspondant à chaque clé d'accès que vous souhaitez supprimer.
4. `${post_edited_translations.segment}`
5. Dans la boîte de dialogue de confirmation, sélectionnez **Delete key**.

Un message de confirmation apparaît dans le coin supérieur droit de la page.

`${post_edited_translations.segment}`

Créez un compartiment StorageGRID S3

`${post_edited_translations.segment}`

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs disposant des droits d'accès racine ou de gestion de tous les compartiments `"${post_edited_translations.segment}"`. Ces autorisations prévalent sur les paramètres d'autorisation définis dans les stratégies de groupe ou de compartiment.



Les autorisations permettant de définir ou de modifier les propriétés S3 Object Lock des compartiments ou des objets peuvent être accordées par `"${post_edited_translations.segment}"`.

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



Chaque grille peut comporter un maximum de 100 000 compartiments, y compris ["seaux de branches"](#).

Accédez à l'assistant

Étapes

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

Saisissez les détails

Étapes

1. `${post_edited_translations.segment}`

Champ	Description
Nom du compartiment	Un nom pour le seau qui respecte ces règles : • Doit être unique dans chaque système StorageGRID (et pas seulement unique au sein du compte du locataire). • Doit être conforme au DNS. • Doit contenir au moins 3 et au plus 63 caractères. • <code>\${post_edited_translations.segment}</code> • Ne doit pas contenir de points dans les requêtes de type hébergement virtuel. Les points entraîneront des problèmes lors de la vérification du certificat générique du serveur. Pour plus d'informations, consultez le "<code>\${post_edited_translations.segment}</code>". <code>\${post_edited_translations.segment}</code>
Région	La région du compartiment. Votre administrateur StorageGRID gère les régions disponibles. La région d'un compartiment peut affecter la politique de protection des données appliquée aux objets. Par défaut, tous les compartiments sont créés dans la région <code>us-east-1</code>. Si la région par défaut est configurée sur une région autre que <code>us-east-1</code>, cette autre région est initialement sélectionnée dans la liste déroulante. <code>\${post_edited_translations.segment}</code>

2. Sélectionnez **Continue**.

Gérer les paramètres

Étapes

1. `${post_edited_translations.segment}`

Activez le versionnement d'objets si vous souhaitez stocker chaque version de chaque objet dans ce compartiment. Vous pouvez ensuite récupérer les versions précédentes d'un objet selon vos besoins.

Vous devez activer le versionnage des objets si :

- `${post_edited_translations.segment}`
- Vous souhaitez créer un "**bucket de branche**" à partir de ce bucket.

2. `${post_edited_translations.segment}`

Activez S3 Object Lock pour un compartiment uniquement si vous devez conserver des objets pendant une période définie, par exemple pour répondre à certaines exigences réglementaires. S3 Object Lock est un paramètre permanent qui vous permet d'empêcher la suppression ou la réécriture d'objets pendant une période définie ou indéfiniment.



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

Si vous activez le verrouillage d'objet S3 pour un compartiment, le versionnage du compartiment est activé automatiquement.

3. `${post_edited_translations.segment}`



Votre administrateur de la grille doit vous donner l'autorisation de `"${post_edited_translations.segment}"`.

Lorsque la **Rétention par défaut** est activée, les nouveaux objets ajoutés au compartiment seront automatiquement protégés contre la suppression ou la réécriture. Le paramètre **Rétention par défaut** ne s'applique pas aux objets qui possèdent leurs propres périodes de rétention.

a. `${post_edited_translations.segment}`

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

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

La **période de rétention par défaut** indique la durée pendant laquelle les nouveaux objets ajoutés à ce compartiment doivent être conservés, à compter de leur ingestion. Spécifiez une valeur inférieure ou égale à la période de rétention maximale pour le locataire, telle que définie par l'administrateur de la grille.

Une période de conservation *maximale*, qui peut être une valeur allant de 1 jour à 100 ans, est définie lorsque l'administrateur de la grille crée le locataire. Lorsque vous définissez une période de conservation *par défaut*, elle ne peut pas dépasser la valeur définie pour la période de conservation maximale. Si

nécessaire, demandez à votre administrateur de la grille d'augmenter ou de diminuer la période de conservation maximale.

4. `${post_edited_translations.segment}`

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

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

5. `${post_edited_translations.segment}`

La limite du nombre d'objets est le nombre maximal d'objets que ce compartiment peut contenir. Cette valeur représente une quantité logique (nombre d'objets). Si aucune limite n'est définie, le nombre d'objets est illimité.

6. Sélectionnez **Créer un compartiment**.

Le compartiment est créé et ajouté au tableau de la page Buckets.

7. Vous pouvez également sélectionner **Accéder à la page de détails du compartiment** pour `"${post_edited_translations.segment}"` et effectuer une configuration supplémentaire.

Vous pouvez également ["créer des compartiments de branche"](#) au besoin.

Afficher les détails du compartiment S3 dans StorageGRID

Vous pouvez consulter les compartiments dans votre compte locataire.

Avant de commencer

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

Étapes

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

`${post_edited_translations.segment}`

2. `${post_edited_translations.segment}`

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



Les valeurs affichées pour le nombre d'objets, l'espace utilisé et l'utilisation sont des estimations. Ces estimations sont affectées par le moment des ingestions, la connectivité réseau et l'état des nœuds. Si les compartiments ont le versionnage activé, les versions d'objets supprimées sont incluses dans le nombre d'objets.

Nom

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

`${post_edited_translations.segment}`

La liste des fonctionnalités activées pour le compartiment.

Verrouillage d'objet S3

`${post_edited_translations.segment}`

Cette colonne s'affiche uniquement si le verrouillage des objets S3 est activé pour la grille. Cette colonne présente également des informations sur les anciens compartiments Compliant.

Région

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

`${post_edited_translations.segment}`

Le nombre d'objets dans ce compartiment. Si le versionnement est activé pour les compartiments, les versions d'objet non actuelles sont incluses dans cette valeur.

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

Espace utilisé

La taille logique de tous les objets du compartiment. La taille logique n'inclut pas l'espace réel requis pour les copies répliquées ou codées par effacement, ni pour les métadonnées d'objet.

`${post_edited_translations.segment}`

`${post_edited_translations.segment}`

`${post_edited_translations.segment}`

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

`${post_edited_translations.segment}`

Capacité

Si cette option est activée, la limite de capacité du compartiment.

`${post_edited_translations.segment}`

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

3. Pour afficher les détails d'un compartiment spécifique, sélectionnez le nom du compartiment dans le tableau.
 - a. Consultez les informations récapitulatives en haut de la page Web pour confirmer les détails du compartiment, tels que la région et le nombre d'objets.

- b. Consultez les barres d'utilisation de la limite de capacité et d'utilisation de la limite du nombre d'objets. Si l'utilisation est de 100 % ou proche de 100 %, envisagez d'augmenter la limite ou de supprimer certains objets.
- c. `${post_edited_translations.segment}`



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

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

- d. `${post_edited_translations.segment}`

- **S3 Console** : affichez les objets du compartiment. Pour plus d'informations, reportez-vous à ["Utilisez la console S3"](#).
- **Options du compartiment** : Consultez ou modifiez les paramètres des options. Certains paramètres, comme S3 Object Lock, ne peuvent pas être modifiés après la création du compartiment.
 - `"${post_edited_translations.segment}"`
 - `"${post_edited_translations.segment}"`
 - "Limite de capacité"
 - "Limite du nombre d'objets"
 - "Versionnage d'objets"
 - "Verrouillage d'objet S3"
 - `"${post_edited_translations.segment}"`
 - ["Gérer la réplication inter-grilles"](#) (si autorisé pour le locataire)
- **Services de plateforme** : ["Gérer les services de plateforme"](#) (s'ils sont autorisés pour le locataire)
- **Accès au bucket** : afficher ou modifier les paramètres d'option. Vous devez disposer d'autorisations d'accès spécifiques.
 - Configurez ["CORS pour les compartiments et les objets"](#) pour que le compartiment et les objets du compartiment soient accessibles aux applications web d'autres domaines.
 - `"${post_edited_translations.segment}"` pour un compartiment S3 et les objets de ce compartiment.
- **Branches** : affichez la liste des compartiments de branche pour le compartiment. ["Créer un nouveau compartiment de branche ou gérer les compartiments de branche"](#).

Découvrez les compartiments de branche StorageGRID

`${post_edited_translations.segment}`

Vous créez un compartiment de branche à partir d'un compartiment existant. Après avoir créé un compartiment de branche, le compartiment d'origine à partir duquel il a été créé est appelé le *compartiment de base*. De plus, vous pouvez créer un compartiment de branche à partir d'un autre compartiment de branche.

Un compartiment de branche fournit un accès aux données protégées, mais ne sert pas de sauvegarde. Pour continuer à protéger les données, utilisez ces fonctionnalités sur les compartiments de base :

- "Verrouillage d'objet S3"
- "Réplication inter-grilles" pour les compartiments de base
- "\${post_edited_translations.segment}" pour les compartiments versionnés afin de nettoyer les anciennes versions d'objets

`${post_edited_translations.segment}`

- Vous pouvez accéder aux objets des compartiments de succursale en utilisant "Console S3 pour télécharger des objets".
- Lorsque les clients accèdent aux objets dans un bucket de branche, ce sont les "\${post_edited_translations.segment}" du bucket de branche, plutôt que les politiques du bucket de base, qui déterminent si l'accès est accordé ou refusé.
- Les objets créés dans un compartiment de base sont évalués en fonction de la manière dont "Règles ILM" s'appliquent au compartiment de base. Les objets créés dans un compartiment de branche sont évalués en fonction de la manière dont les règles ILM s'appliquent au compartiment de branche.
- `${post_edited_translations.segment}`
- `${post_edited_translations.segment}`

Exemples d'utilisation des compartiments de branche

- `${post_edited_translations.segment}`
- Vous enregistrez des données dans un compartiment versionné. Une vulnérabilité accidentelle a entraîné l'ingestion de nombreux objets indésirables après l'instant *T*. Vous pouvez créer un compartiment de branche pour la valeur temporelle Before, *T*, et rediriger les opérations des clients vers ce compartiment de branche. Ainsi, seuls les objets ingérés avant la valeur temporelle Before *T* sont exposés aux clients.

Opérations sur les objets dans les compartiments de branche

- Une opération PUT object sur un bucket de branche crée un objet dans la branche.
- Une opération GET sur un bucket de branche récupère un objet de la branche. Si l'objet n'existe pas dans le bucket de branche, il est récupéré depuis le bucket de base.
- La suppression d'objets dans les compartiments de branche s'effectue comme suit :

Opération	Cible	Résultat	<code>\${post_edited_translations.segment}</code>	<code>\${post_edited_translations.segment}</code>
<code>\${post_edited_translations.segment}</code>	<code>\${post_edited_translations.segment}</code>	Le marqueur de suppression est créé uniquement pour le compartiment de base	<code>\${post_edited_translations.segment}</code>	HEAD/GET renvoie Objet existe, et des versions spécifiques restent accessibles Le marqueur de suppression aurait été créé après le <code>beforeTime</code> du compartiment de branche.

Opération	Cible	Résultat	<code>\${post_edited_translations.segment}</code>	<code>\${post_edited_translations.segment}</code>
Supprimer avec l'ID de version	<code>\${post_edited_translations.segment}</code>	<code>\${post_edited_translations.segment}</code>	<code>\${post_edited_translations.segment}</code>	<code>\${post_edited_translations.segment}</code>
<code>\${post_edited_translations.segment}</code>	<code>\${post_edited_translations.segment}</code>	Le marqueur de suppression est créé uniquement pour le compartiment de branche	<code>\${post_edited_translations.segment}</code>	HEAD/GET renvoie Objet n'existe pas
Supprimer avec l'ID de version	<code>\${post_edited_translations.segment}</code>	La version spécifique de l'objet est supprimée uniquement pour le compartiment de branche	HEAD/GET renvoie une version spécifique de l'objet (l'objet de base du bucket n'est pas affecté)	<code>\${post_edited_translations.segment}</code>

Voir aussi "`${post_edited_translations.segment}`".

Gérer les compartiments de branche StorageGRID

`${post_edited_translations.segment}`

Avant de commencer

- Vous vous êtes connecté au Tenant Manager à l'aide d'un "navigateur Web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui dispose de l'accès Root ou "`${post_edited_translations.segment}`". Ces autorisations remplacent les paramètres d'autorisation dans les politiques de groupe ou de compartiment.
- Le bucket de base à partir duquel vous souhaitez créer une branche possède "versionnage activé".
- `${post_edited_translations.segment}`

À propos de cette tâche

`${post_edited_translations.segment}`

- Les autorisations permettant de définir les propriétés de verrouillage d'objets S3 des compartiments ou des objets peuvent être accordées par "`${post_edited_translations.segment}`".
- Si vous suspendez le versionnage sur le compartiment principal, le contenu du compartiment principal ne sera plus visible dans ses compartiments secondaires.



`${post_edited_translations.segment}`

Créer un bucket de branche

Étapes

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

2. `${post_edited_translations.segment}`
3. Sur la page de détails du compartiment, sélectionnez **Branches** > **Créer un compartiment de branche**.

Le bouton **Créer un compartiment de branche** est désactivé si le compartiment de base n'a pas le versionnage activé.

Saisissez les détails

Étapes

1. Saisissez les détails du compartiment de branche.

Champ	Description
<code>\${post_edited_translations.segment}</code>	<code>\${post_edited_translations.segment}</code> • Doit être unique dans chaque système StorageGRID (et pas seulement unique au sein du compte du locataire). • Doit être conforme au DNS. • Doit contenir au moins 3 et au plus 63 caractères. • <code>\${post_edited_translations.segment}</code> • Ne doit pas contenir de points dans les requêtes de type hébergement virtuel. Les points entraîneront des problèmes lors de la vérification du certificat générique du serveur. Pour plus d'informations, consultez le "<code>\${post_edited_translations.segment}</code>". Remarque : Vous ne pouvez pas modifier le nom après avoir créé le compartiment de branche.
<code>\${post_edited_translations.segment}</code>	<code>\${post_edited_translations.segment}</code> <code>\${post_edited_translations.segment}</code>
Avant l'heure	L'heure limite pour que les versions d'objets créées dans le compartiment de base soient accessibles depuis le compartiment de branche. Le compartiment de branche permet d'accéder aux versions d'objets créées avant l'heure Before time. La date et l'heure « Avant » doivent être une date et une heure passées. Il ne peut pas s'agir d'une date future.
Type de compartiment de branche	• <code>\${post_edited_translations.segment}</code> • Lecture seule : Vous ne pouvez pas modifier les objets dans le compartiment de la branche. Remarque : vous ne pouvez définir le type de bucket de branche sur lecture seule que si le bucket de branche est vide. Si le type d'un bucket de branche existant est défini sur lecture-écriture et que vous n'y avez pas écrit, vous pouvez modifier le type en lecture seule.

2. Sélectionnez **Continue**.

`${post_edited_translations.segment}`

Les paramètres d'objet d'un compartiment de branche n'affectent pas les versions d'objet dans le compartiment de base.

Étapes

1. Si le paramètre global S3 Object Lock est activé, vous pouvez également activer S3 Object Lock pour le compartiment de branche. Pour activer S3 Object Lock, le compartiment de branche doit être un compartiment en lecture-écriture.

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



Une fois le paramètre de verrouillage des objets S3 activé pour un compartiment, il ne peut pas être désactivé. Toute personne disposant des autorisations appropriées peut ajouter des objets au compartiment de la branche qui ne peuvent pas être modifiés. Il se peut que vous ne puissiez pas supprimer ces objets ni le compartiment de la branche lui-même.

2. Si vous avez sélectionné **Activer le verrouillage des objets S3**, vous pouvez également activer **Rétention par défaut** pour le compartiment de branche.



Votre administrateur de la grille doit vous donner l'autorisation de `"${post_edited_translations.segment}"`.

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

- a. Si la **rétention par défaut** est activée, spécifiez un **mode de rétention par défaut** pour le compartiment de branche.

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

Mode de rétention par défaut	Description
Conformité	• L'objet ne peut pas être supprimé tant que sa date de conservation n'est pas atteinte. • La date de conservation de l'objet peut être augmentée, mais elle ne peut pas être diminuée. • La date de conservation de l'objet ne peut pas être supprimée avant que cette date ne soit atteinte. Remarque : Votre administrateur de grille doit vous autoriser à utiliser le mode de conformité.

b. `${post_edited_translations.segment}`

La **période de rétention par défaut** indique la durée pendant laquelle les nouveaux objets ajoutés au compartiment de succursale doivent être conservés, à compter de leur ingestion. Spécifiez une valeur inférieure ou égale à la période de rétention maximale pour le locataire, telle que définie par l'administrateur du grid.

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

3. `${post_edited_translations.segment}`

La limite de capacité correspond à la capacité maximale disponible pour le compartiment de branche. Cette valeur représente une taille logique (taille de l'objet), et non une taille physique (taille sur le disque).

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



`${post_edited_translations.segment}`

4. Vous pouvez éventuellement sélectionner **Activer la limite du nombre d'objets**.

La limite du nombre d'objets est le nombre maximal d'objets que le compartiment de succursale peut contenir. Cette valeur représente une quantité logique (nombre d'objets). Si aucune limite n'est définie, le nombre d'objets est illimité.



`${post_edited_translations.segment}`

5. Sélectionnez **Créer un compartiment**.

`${post_edited_translations.segment}`

6. Vous pouvez également sélectionner **Accéder à la page de détails du compartiment** pour `"${post_edited_translations.segment}"` et effectuer une configuration supplémentaire.

Sur la page de détails du compartiment, certaines options de configuration relatives à la modification des objets sont désactivées pour les compartiments en lecture seule.

Appliquer une étiquette de stratégie ILM à un compartiment StorageGRID

Choisissez une étiquette de stratégie ILM à appliquer à un compartiment en fonction de vos exigences de stockage d'objets.

La politique ILM contrôle l'emplacement de stockage des données d'objet et leur suppression après une certaine période. Votre administrateur de grille crée des politiques ILM et les assigne à des balises de politique ILM lorsqu'il utilise plusieurs politiques actives.



Évitez de réattribuer fréquemment l'étiquette de stratégie d'un compartiment. Sinon, des problèmes de performance pourraient survenir.

Avant de commencer

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

Étapes

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

La page « Buckets » s'affiche. Selon vos besoins, vous pouvez trier les informations par n'importe quelle colonne ou avancer et reculer dans la liste page par page.

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

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



Les valeurs affichées pour le nombre d'objets et l'espace utilisé sont des estimations. Ces estimations sont affectées par le moment des ingestions, la connectivité réseau et l'état des nœuds. Si le versionnage est activé pour les compartiments, les versions d'objets supprimées sont incluses dans le nombre d'objets.

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



Modifier l'étiquette de stratégie ILM d'un compartiment entraînera une réévaluation ILM de tous les objets de ce compartiment. Si la nouvelle stratégie conserve les objets pendant une durée limitée, les objets les plus anciens seront supprimés.

5. `${post_edited_translations.segment}`
6. Sélectionnez **Enregistrer les modifications**. Une nouvelle étiquette de compartiment S3 sera créée sur le compartiment avec la clé `NTAP-SG-ILM-BUCKET-TAG` et la valeur du nom de l'étiquette de stratégie ILM.



Veillez à ce que vos applications S3 ne remplacent ni ne suppriment accidentellement la nouvelle balise de compartiment. Si cette balise est omise lors de l'application d'un nouveau TagSet au compartiment, les objets du compartiment seront à nouveau évalués selon la stratégie ILM par défaut.



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



`${post_edited_translations.segment}`

Gérer la politique du compartiment StorageGRID

`${post_edited_translations.segment}`

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs qui possède les ["Autorisation d'accès root"](#). Les autorisations « View all buckets » et « Manage all buckets » permettent uniquement la consultation.
- Vous avez vérifié que le nombre requis de nœuds de stockage et de sites est disponible. Si deux nœuds de stockage ou plus ne sont pas disponibles dans un site, ou si un site n'est pas disponible, les modifications de ces paramètres peuvent ne pas être disponibles.

Étapes

1. `${post_edited_translations.segment}`
2. `${post_edited_translations.segment}`
3. Effectuez l'une des opérations suivantes :
 - Définissez une stratégie de compartiment en cochant la case **Activer la stratégie**. Saisissez ensuite une chaîne au format JSON valide.

`${post_edited_translations.segment}`
 - Modifiez une politique existante en modifiant la chaîne.
 - `${post_edited_translations.segment}`

Pour obtenir des informations détaillées sur les politiques de compartiment, y compris la syntaxe du langage et des exemples, consultez ["\\${post_edited_translations.segment}"](#).

Gérer la cohérence des buckets StorageGRID

Les valeurs de cohérence peuvent être utilisées pour spécifier la disponibilité des modifications des paramètres de compartiment, ainsi que pour assurer un équilibre entre la disponibilité des objets au sein d'un compartiment et la cohérence de ces objets sur différents Storage Nodes et sites. Vous pouvez modifier les valeurs de cohérence afin qu'elles diffèrent des valeurs par défaut pour permettre aux applications clientes de répondre à leurs besoins opérationnels.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs qui dispose de la ["Gérer tous les compartiments ou autorisation d'accès Root"](#). Ces autorisations remplacent les paramètres d'autorisation des politiques de groupe ou de compartiment.

`${post_edited_translations.segment}`

La cohérence du compartiment est utilisée pour déterminer la cohérence pour les applications clientes affectant les objets au sein de ce compartiment S3. En général, vous devriez utiliser la cohérence **Read-after-new-write** pour vos compartiments.

`${post_edited_translations.segment}`

Si la cohérence **Read-after-new-write** ne répond pas aux exigences de l'application cliente, vous pouvez la modifier en configurant la cohérence du compartiment ou en utilisant l' `Consistency-Control` header. L' `Consistency-Control` header remplace la cohérence du compartiment.



`${post_edited_translations.segment}`

Étapes

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

2. Sélectionnez le nom du compartiment dans le tableau.

`${post_edited_translations.segment}`

3. Dans l'onglet **Options du seau**, sélectionnez l'*** accordion.

4. `${post_edited_translations.segment}`

- **Tous** : Garantit le plus haut niveau de cohérence. Tous les nœuds reçoivent les données immédiatement, ou la requête échouera.
- **Strong-global** : Garantit la cohérence de lecture après écriture pour toutes les requêtes client sur tous les sites.
- **Site robuste** : Garantit la cohérence de lecture après écriture pour toutes les requêtes client au sein d'un site.
- **Read-after-new-write** (par défaut) : assure la cohérence lecture-après-écriture pour les nouveaux objets et la cohérence à terme pour les mises à jour d'objets. Offre des garanties de haute disponibilité et de protection des données. Recommandé dans la plupart des cas.
- **Disponible** : Garantit la cohérence éventuelle pour les nouveaux objets et les mises à jour d'objets. Pour les compartiments S3, utilisez cette fonctionnalité uniquement en cas de besoin (par exemple, pour un compartiment contenant des valeurs de journaux rarement lues, ou pour les opérations HEAD ou GET sur des clés qui n'existent pas). Non pris en charge pour les compartiments S3 FabricPool.

5. Sélectionnez **Save changes**.

`${post_edited_translations.segment}`

`${post_edited_translations.segment}`

Les paramètres de compartiment suivants utilisent la cohérence **forte** par défaut. Si deux nœuds de stockage ou plus ne sont pas disponibles sur un site, ou si un site n'est pas disponible, les modifications apportées à

ces paramètres peuvent ne pas être disponibles.

- ["Suppression en arrière-plan du compartiment vide"](#)
- ["\\${post_edited_translations.segment}"](#)
- ["Cycle de vie du bucket"](#)
- ["Politique de compartiment"](#)
- ["Étiquetage de compartiments"](#)
- ["\\${post_edited_translations.segment}"](#)
- ["Verrouillage d'objet S3"](#)
- ["Chiffrement du compartiment"](#)



[\\${post_edited_translations.segment}](#)

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

- ["Configuration des services de plateforme : notification, réplication ou intégration de recherche"](#)
- ["Configurer StorageGRID CORS pour les compartiments et les objets"](#)
- [Modifier la cohérence du compartiment](#)



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

Activer ou désactiver les mises à jour du temps d'accès dans StorageGRID

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

Ces instructions s'appliquent uniquement aux systèmes StorageGRID qui incluent au moins une règle ILM utilisant l'option **Dernier temps d'accès** comme filtre avancé ou comme temps de référence. Vous pouvez ignorer ces instructions si votre système StorageGRID ne comporte pas de règle de ce type. Voir ["Utilisez le temps d'accès dans les règles ILM"](#) pour plus de détails.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs qui dispose de la ["Gérer tous les compartiments ou autorisation d'accès Root"](#). Ces autorisations remplacent les paramètres d'autorisation des politiques de groupe ou de compartiment.

À propos de cette tâche

Le **dernier temps d'accès** est l'une des options disponibles pour l'instruction de placement **Heure de référence** d'une règle ILM. Définir l'Heure de référence d'une règle sur Dernier temps d'accès permet aux administrateurs de la grille de spécifier que les objets soient placés dans certains emplacements de stockage en fonction du moment où ces objets ont été récupérés (lus ou consultés) pour la dernière fois.

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

- `${post_edited_translations.segment}`
- Les objets qui n'ont pas été récupérés au cours du mois écoulé doivent être déplacés vers un site externe.

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



`${post_edited_translations.segment}`

`${post_edited_translations.segment}`

- Mettre à jour les objets avec de nouveaux horodatages
- `${post_edited_translations.segment}`

Le tableau récapitule le comportement appliqué à tous les objets du compartiment lorsque le temps d'accès est désactivé ou activé.

Type de demande	Comportement si le temps d'accès est désactivé (par défaut)		<code>\${post_edited_translations.segment}</code>	
	<code>\${post_edited_translations.segment}</code>	Objet ajouté à la file d'attente d'évaluation ILM ?	<code>\${post_edited_translations.segment}</code>	Objet ajouté à la file d'attente d'évaluation ILM ?
<code>\${post_edited_translations.segment}</code>	Non	Non	Non	Non
Demande de récupération d'un objet, de sa liste de contrôle d'accès ou de ses métadonnées	Non	Non	Oui	Oui
Demande de mise à jour des métadonnées d'un objet	Oui	Oui	Oui	Oui

Demande de liste d'objets ou de versions d'objets	Non	Non	Non	Non
Demande de copie d'un objet d'un bucket à un autre	• 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
Demande de finalisation d'un téléchargement en plusieurs parties	Oui, pour l'objet assemblé	Oui, pour l'objet assemblé	Oui, pour l'objet assemblé	Oui, pour l'objet assemblé

Étapes

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

`${post_edited_translations.segment}`

3. `${post_edited_translations.segment}`
4. `${post_edited_translations.segment}`
5. Sélectionnez **Save changes**.

Modifier le versionnage des objets pour un compartiment S3 dans StorageGRID

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

Avant de commencer

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

À propos de cette tâche

Vous pouvez activer ou suspendre le versionnement d'objets pour un compartiment. Après avoir activé le versionnement pour un compartiment, celui-ci ne peut plus revenir à un état non versionné. Toutefois, vous pouvez suspendre le versionnement pour ce compartiment.

- `${post_edited_translations.segment}`
- Activé : Le versionnage est activé

- Suspendu : le versionnage était précédemment activé et est suspendu

Pour plus d'informations, consultez les documents suivants :

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

Étapes

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

`${post_edited_translations.segment}`

3. `${post_edited_translations.segment}`
4. `${post_edited_translations.segment}`

Le versionnage des objets doit rester activé pour un compartiment utilisé pour la réplique inter-grilles. Si S3 Object Lock ou la conformité héritée est activé, les options **Object versioning** sont désactivées.

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

5. Sélectionnez **Save changes**.

Utilisez S3 Object Lock pour conserver les objets dans StorageGRID

Vous pouvez utiliser S3 Object Lock si les compartiments et les objets doivent se conformer aux exigences réglementaires en matière de conservation.



`${post_edited_translations.segment}`

Qu'est-ce que le S3 Object Lock ?

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

Lorsque le paramètre global de verrouillage des objets S3 est activé pour un système StorageGRID, un compte locataire S3 peut créer des compartiments avec ou sans verrouillage des objets S3 activé. Si un compartiment a le verrouillage des objets S3 activé, le versionnage du compartiment est requis et est activé

automatiquement.

Un bucket sans S3 Object Lock ne peut contenir que des objets sans paramètres de rétention spécifiés. Aucun objet ingéré ne disposera de paramètres de rétention.

Un compartiment avec S3 Object Lock peut contenir des objets avec ou sans paramètres de rétention définis par les applications clientes S3. Certains objets ingérés auront des paramètres de rétention.

Un compartiment avec S3 Object Lock et une rétention par défaut configurée peut contenir des objets chargés avec des paramètres de rétention spécifiés et de nouveaux objets sans paramètres de rétention. Les nouveaux objets utilisent le paramètre par défaut, car la rétention n'a pas été configurée au niveau de l'objet.

En pratique, tous les nouveaux objets ingérés se voient attribuer des paramètres de rétention lorsque la rétention par défaut est configurée. Les objets existants sans paramètres de rétention d'objet restent inchangés.

Modes de rétention

La fonctionnalité StorageGRID S3 Object Lock prend en charge deux modes de rétention pour appliquer différents niveaux de protection aux objets. Ces modes sont équivalents aux modes de rétention Amazon S3.

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

Paramètres de conservation des versions d'objets

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

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



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

Pour plus de détails sur les paramètres de l'objet, voir ["Utilisez l'API REST S3 pour configurer S3 Object Lock"](#).

Paramètre de rétention par défaut pour les compartiments

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

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

Les paramètres par défaut des compartiments s'appliquent uniquement aux nouveaux objets qui ne possèdent pas leurs propres paramètres de rétention. Les objets existants dans les compartiments ne sont pas affectés lorsque vous ajoutez ou modifiez ces paramètres par défaut.

Voir ["Créez un compartiment S3"](#) et ["Mettre à jour la rétention par défaut de S3 Object Lock"](#).

`${post_edited_translations.segment}`

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

Administrateur de grille

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

Utilisateur locataire

- Examinez les points à prendre en compte pour les compartiments et les objets avec S3 Object Lock.
- Au besoin, contactez l'administrateur de la grille pour activer le paramètre de verrouillage global S3 Object Lock et définir les autorisations.
- Créez des compartiments avec la fonctionnalité S3 Object Lock activée.
- Vous pouvez également configurer les paramètres de rétention par défaut d'un compartiment :
 - Mode de rétention par défaut : Gouvernance ou Conformité, si autorisé par l'administrateur du grid.
 - Durée de conservation par défaut : doit être inférieure ou égale à la durée de conservation maximale définie par l'administrateur du grid.
- Utilisez l'application cliente S3 pour ajouter des objets et, éventuellement, définir une durée de conservation spécifique à chaque objet :
 - Mode de conservation. Gouvernance ou conformité, si autorisé par l'administrateur du grid.
 - À conserver jusqu'à cette date : doit être inférieure ou égale à la durée de conservation maximale autorisée par l'administrateur du grid.

Exigences pour les compartiments avec S3 Object Lock activé

- Si le paramètre global S3 Object Lock est activé pour le système StorageGRID, vous pouvez utiliser le Tenant Manager, l'API de gestion des locataires ou l'API REST S3 pour créer des compartiments avec S3 Object Lock activé.
- Si vous prévoyez d'utiliser S3 Object Lock, vous devez activer S3 Object Lock lors de la création du compartiment. Vous ne pouvez pas activer S3 Object Lock pour un compartiment existant.
- Lorsque le verrouillage d'objets S3 est activé pour un compartiment, StorageGRID active automatiquement le versionnage pour ce compartiment. Vous ne pouvez pas désactiver le verrouillage d'objets S3 ni suspendre le versionnage pour ce compartiment.
- Vous pouvez, si vous le souhaitez, spécifier un mode de conservation par défaut et une période de conservation pour chaque compartiment à l'aide du Tenant Manager, de l'API de gestion des locataires ou de l'API REST S3. Les paramètres de conservation par défaut du compartiment s'appliquent uniquement aux nouveaux objets ajoutés au compartiment qui n'ont pas leurs propres paramètres de conservation. Vous pouvez remplacer ces paramètres par défaut en spécifiant un mode de conservation et une date de conservation jusqu'à pour chaque version d'objet lors de son chargement.
- La configuration du cycle de vie des compartiments est prise en charge pour les compartiments avec S3 Object Lock activé.
- La réplication CloudMirror n'est pas prise en charge pour les compartiments avec le verrouillage d'objet S3 activé.

Exigences relatives aux objets dans les compartiments avec S3 Object Lock activé

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

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

Chaque objet enregistré dans un compartiment avec le verrouillage d'objet S3 activé passe par les étapes suivantes :

1. Ingestion d'objet

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

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

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

2. Conservation et suppression des objets

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

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

Puis-je encore gérer les anciens compartiments conformes ?

La fonctionnalité S3 Object Lock remplace la fonctionnalité de conformité qui était disponible dans les versions précédentes de StorageGRID. 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 nouveaux compartiments conformes. Pour obtenir des instructions, consultez ["Base de connaissances NetApp : Comment gérer les compartiments conformes hérités dans StorageGRID 11.5"](#).

Mettre à jour la rétention par défaut du verrouillage d'objet S3 dans StorageGRID

Si vous avez activé S3 Object Lock lors de la création du compartiment, vous pouvez modifier le compartiment pour changer les paramètres de rétention par défaut. Vous pouvez activer (ou désactiver) la rétention par défaut et définir un mode de rétention par défaut ainsi qu'une période de rétention.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs qui dispose de la ["Gérer tous les compartiments ou autorisation d'accès Root"](#). Ces autorisations remplacent les paramètres d'autorisation des politiques de groupe ou de compartiment.
- Le verrouillage d'objets S3 est activé globalement pour votre système StorageGRID, et vous avez activé le verrouillage d'objets S3 lors de la création du compartiment. Voir ["\\${post_edited_translations.segment}"](#).

Étapes

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

[\\${post_edited_translations.segment}](#)

3. [\\${post_edited_translations.segment}](#)

4. Vous pouvez activer ou désactiver la **conservation par défaut** pour ce compartiment.

[\\${post_edited_translations.segment}](#)

5. [\\${post_edited_translations.segment}](#)

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

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

La **période de rétention par défaut** indique la durée pendant laquelle les nouveaux objets ajoutés à ce compartiment doivent être conservés, à compter de leur ingestion. Spécifiez une valeur inférieure ou égale à la période de rétention maximale pour le locataire, telle que définie par l'administrateur de la grille.

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

7. Sélectionnez **Save changes**.

Configurer CORS pour les compartiments S3 dans StorageGRID

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

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#).
- Pour les requêtes de configuration GET CORS, vous appartenez à un groupe d'utilisateurs qui possède la ["Autorisation de gérer tous les compartiments ou d'afficher tous les compartiments"](#). Ces autorisations prévalent sur les paramètres d'autorisation dans les politiques de groupe ou de compartiment.
- Pour les requêtes de configuration PUT CORS, vous appartenez à un groupe d'utilisateurs disposant de l'["{\\$post_edited_translations.segment}"](#). Cette autorisation remplace les paramètres d'autorisation définis dans les stratégies de groupe ou de compartiment.

- Le "[Autorisation d'accès root](#)" permet d'accéder à toutes les requêtes de configuration CORS.

À propos de cette tâche

Le partage de ressources entre origines multiples (CORS) est un mécanisme de sécurité qui permet aux applications web clientes d'un domaine d'accéder aux ressources d'un autre domaine. Par exemple, supposez que vous utilisiez un compartiment S3 nommé `Images` pour stocker des graphiques. En configurant le CORS pour le compartiment `Images`, vous pouvez autoriser l'affichage des images de ce compartiment sur le site web `http://www.example.com`.

Activer CORS pour un bucket

Étapes

1. Utilisez un éditeur de texte pour créer le XML requis. Cet exemple montre le XML utilisé pour activer le CORS pour un compartiment S3. Plus précisément :
 - Autorise tout domaine à envoyer des requêtes GET au compartiment
 - Autorise uniquement le `http://www.example.com` domaine à envoyer des requêtes GET, POST et DELETE
 - Tous les en-têtes de requête sont autorisés

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

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

2. Sélectionnez **Afficher les compartiments** depuis le tableau de bord, ou sélectionnez **STOCKAGE (S3) > Compartiments**.
3. Sélectionnez le nom du compartiment dans le tableau.
`${post_edited_translations.segment}`
4. Dans l'onglet **Accès au compartiment**, sélectionnez l'accordéon **Partage de ressources entre origines (CORS)**.
5. Sélectionnez la case à cocher **Activer CORS**.

6. Collez le code XML de configuration CORS dans la zone de texte.

7. Sélectionnez **Save changes**.

Modifier les paramètres CORS

Étapes

1. Mettez à jour le fichier XML de configuration CORS dans la zone de texte, ou sélectionnez **Clear** pour recommencer.
2. Sélectionnez **Save changes**.

Désactiver le paramètre CORS

Étapes

1. Décochez la case **Enable CORS**.
2. Sélectionnez **Save changes**.

Informations connexes

["Configurer StorageGRID CORS pour une interface de gestion"](#)

Supprimer des objets d'un compartiment StorageGRID S3

`${post_edited_translations.segment}`

`${post_edited_translations.segment}`

`${post_edited_translations.segment}`

- Lorsque vous supprimez des objets dans un bucket, StorageGRID supprime définitivement tous les objets et toutes les versions d'objet dans chaque bucket sélectionné, de tous les nœuds et sites de votre système StorageGRID. StorageGRID supprime également toutes les métadonnées associées à ces objets. Vous ne pourrez pas récupérer ces informations.
- `${post_edited_translations.segment}`
- Si un compartiment comporte ["Verrouillage d'objet S3 activé"](#), il peut rester dans l'état **Deleting objects: read-only** pendant des *années*.



`${post_edited_translations.segment}`

- Pendant la suppression d'objets, l'état du compartiment est **Suppression d'objets : lecture seule**. Dans cet état, vous ne pouvez pas ajouter de nouveaux objets au compartiment.
- Lorsque tous les objets ont été supprimés, le compartiment reste à l'état de lecture seule. Vous pouvez effectuer l'une des actions suivantes :
 - Remettez le bucket en mode écriture et réutilisez-le pour de nouveaux objets
 - Supprimez le compartiment
 - Conservez le bucket en mode lecture seule pour réserver son nom pour une utilisation ultérieure
- Si le versionnage des objets est activé pour un compartiment, les marqueurs de suppression créés dans StorageGRID 11.8 ou une version ultérieure peuvent être supprimés à l'aide des opérations Delete objects in bucket.
- Si le versionnement d'objets est activé sur un compartiment, l'opération de suppression d'objets ne retirera pas les marqueurs de suppression créés dans StorageGRID 11.7 ou version antérieure. Consultez les

informations relatives à la suppression d'objets dans un compartiment dans "\${post_edited_translations.segment}".

- Si vous utilisez "réplication inter-grilles", veuillez noter ce qui suit :
 - "\${post_edited_translations.segment}"
 - Si vous sélectionnez cette option pour le compartiment source, l'alerte **Échec de la réplication inter-grilles** sera déclenchée si vous ajoutez des objets au compartiment de destination sur l'autre grille. Si vous ne pouvez pas garantir que personne n'ajoutera d'objets au compartiment sur l'autre grille, "désactiver la réplication inter-grilles" pour ce compartiment avant de supprimer tous les objets du compartiment.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un "navigateur Web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui dispose de "Autorisation d'accès root". Cette autorisation remplace les paramètres d'autorisation définis dans les stratégies de groupe ou de compartiment.

Étapes

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

La page « Buckets » s'affiche et présente tous les buckets S3 existants.

2. "\${post_edited_translations.segment}"

Menu Actions

- a. Cochez la case correspondant à chaque compartiment dont vous souhaitez supprimer des objets.
- b. "\${post_edited_translations.segment}"

Page de détails

- a. Sélectionnez un nom de compartiment pour afficher ses détails.
- b. Sélectionnez **Supprimer les objets du compartiment**.

3. Lorsque la boîte de dialogue de confirmation apparaît, vérifiez les détails, saisissez **Yes** et sélectionnez **OK**.

4. "\${post_edited_translations.segment}"

"\${post_edited_translations.segment}"

- Une bannière jaune s'affiche sur la page de détails du compartiment. La barre de progression indique le pourcentage d'objets supprimés.
- **(lecture seule)** apparaît après le nom du compartiment sur la page de détails du compartiment.
- "\${post_edited_translations.segment}"

Buckets > my-bucket

my-bucket (read-only)

Region: us-east-1
Date created: 2022-12-14 10:09:50 MST
Object count: 3

[View bucket contents in Experimental S3 Console](#)

[Delete bucket](#)

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

0% (0 of 3 objects deleted)

[Stop deleting objects](#)

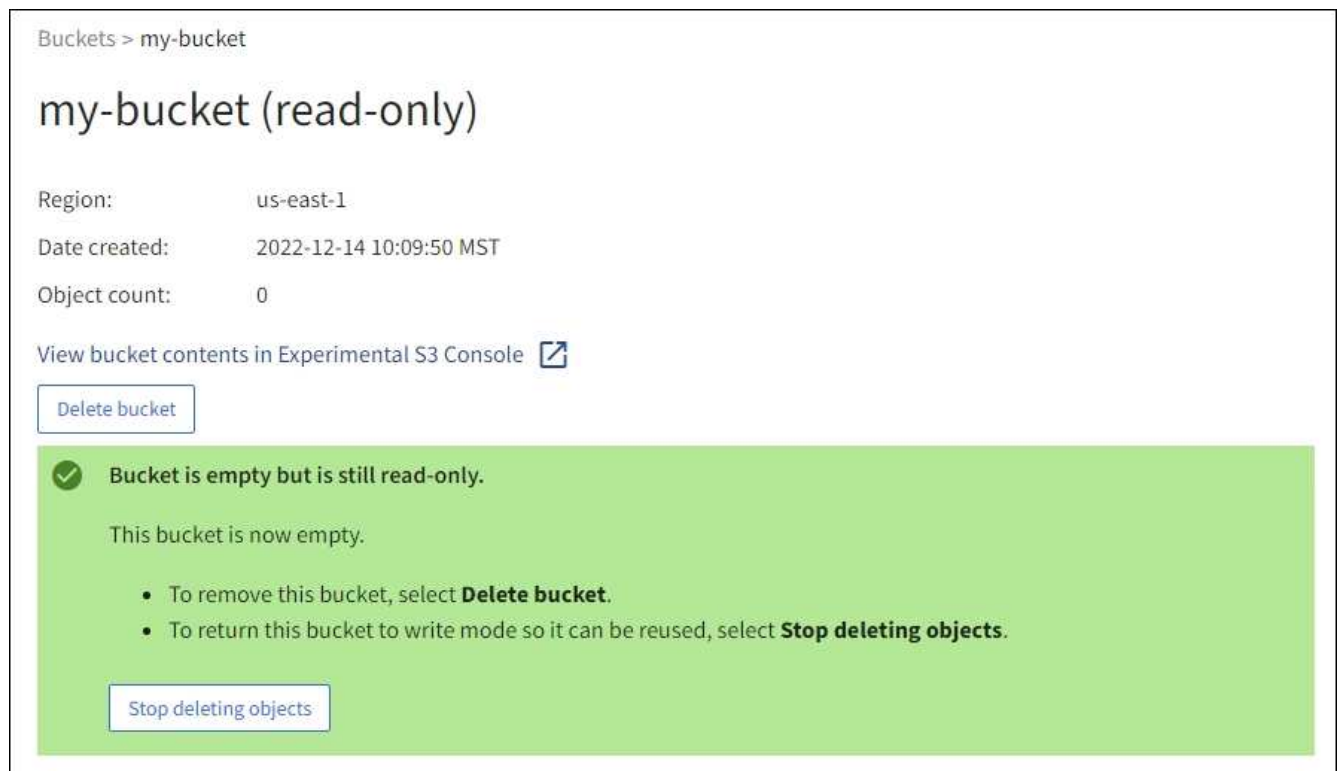
Success
Starting to delete objects from one bucket.

5. Au besoin, pendant que l'opération est en cours, sélectionnez **Arrêter la suppression d'objets** pour interrompre le processus. Ensuite, si vous le souhaitez, sélectionnez **Supprimer les objets du compartiment** pour reprendre le processus.

`${post_edited_translations.segment}`

6. Attendez que l'opération soit terminée.

`${post_edited_translations.segment}`



7. Effectuez l'une des opérations suivantes :

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



Si vous ne parvenez pas à supprimer un compartiment versionné après la suppression de tous les objets, il est possible que des marqueurs de suppression subsistent. Pour supprimer le compartiment, vous devez supprimer tous les marqueurs de suppression restants.

- Remettez le compartiment en mode écriture et, si vous le souhaitez, réutilisez-le pour de nouveaux objets. Vous pouvez sélectionner **Arrêter la suppression d'objets** pour un seul compartiment ou revenir à la page Compartiments et sélectionner **Action > Arrêter la suppression d'objets** pour plusieurs compartiments.

Supprimer un compartiment StorageGRID S3

Vous pouvez utiliser le Tenant Manager pour supprimer un ou plusieurs compartiments S3 vides.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un "navigateur Web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui dispose de la "Gérer tous les compartiments ou autorisation d'accès Root". Ces autorisations remplacent les paramètres d'autorisation des politiques de groupe ou de compartiment.

- Les compartiments que vous souhaitez supprimer sont vides. Si les compartiments que vous souhaitez supprimer ne sont *pas* vides, "[supprimer des objets du compartiment](#)".

À propos de cette tâche

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

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

Étapes

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

La page « Buckets » s'affiche et présente tous les buckets S3 existants.

2. `#{post_edited_translations.segment}`

Menu Actions

- a. Cochez la case correspondant à chaque compartiment que vous souhaitez supprimer.
- b. `#{post_edited_translations.segment}`

Page de détails

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

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

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

Si un compartiment n'est pas vide, un message d'erreur s'affiche. Vous devez "[#{post_edited_translations.segment}](#)" avant de pouvoir supprimer le compartiment.

Utilisez la console S3 dans StorageGRID

`#{post_edited_translations.segment}`

`#{post_edited_translations.segment}`

- Téléverser, télécharger, renommer, copier, déplacer et supprimer des objets
- Afficher, restaurer, télécharger et supprimer les versions d'objets
- `#{post_edited_translations.segment}`
- `#{post_edited_translations.segment}`
- `#{post_edited_translations.segment}`
- `#{post_edited_translations.segment}`

La console S3 offre une expérience utilisateur améliorée dans la plupart des cas. Elle n'est pas conçue pour remplacer les opérations de ligne de commande ou d'API dans toutes les situations.



Si l'utilisation de la console S3 entraîne des opérations trop longues (par exemple, minutes ou heures), envisagez :

- Réduction du nombre d'objets sélectionnés
- `${post_edited_translations.segment}`

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#).
- Si vous souhaitez gérer des objets, vous devez appartenir à un groupe d'utilisateurs disposant de l'autorisation d'accès Root. Alternativement, vous devez appartenir à un groupe d'utilisateurs disposant de l'autorisation Utiliser l'onglet Console S3 et soit de l'autorisation Afficher tous les compartiments, soit de l'autorisation Gérer tous les compartiments. Voir ["\\${post_edited_translations.segment}"](#).
- Une stratégie de groupe ou de compartiment S3 a été configurée pour l'utilisateur. Voir ["Utilisez les stratégies d'accès aux compartiments et aux groupes"](#).
- Vous connaissez l'identifiant de clé d'accès et la clé d'accès secrète de l'utilisateur. Vous disposez éventuellement d'un fichier `.csv` contenant ces informations. Voir le ["\\${post_edited_translations.segment}"](#).

Étapes

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

Informations complémentaires

- **Recherche par préfixe** : la fonction de recherche par préfixe recherche uniquement les objets qui commencent par un mot spécifique par rapport au dossier actuel. La recherche n'inclut pas les objets qui contiennent le mot ailleurs. Cette règle s'applique également aux objets situés dans des dossiers. Par exemple, une recherche de `folder1/folder2/somefile-` renverrait les objets qui se trouvent dans le dossier `folder1/folder2/` et commencent par le mot `somefile-`.
- **Glisser-déposer** : vous pouvez glisser-déposer des fichiers depuis le gestionnaire de fichiers de votre ordinateur vers S3 Console. Toutefois, vous ne pouvez pas importer de dossiers.
- `${post_edited_translations.segment}`
- **Suppression définitive lorsque le versionnage du compartiment est désactivé** : Lorsque vous écrasez ou supprimez un objet dans un compartiment dont le versionnage est désactivé, l'opération est définitive. Voir ["\\${post_edited_translations.segment}"](#).

`${post_edited_translations.segment}`

Services de la plateforme S3

Découvrez les services de plateforme pour StorageGRID

Avant de mettre en œuvre les services de la plateforme, consultez la présentation et les points à prendre en compte pour utiliser ces services.

Pour plus d'informations sur S3, voir ["Utilisez l'API REST S3"](#).

Aperçu des services de la plateforme

`${post_edited_translations.segment}`

Étant donné que l'emplacement cible des services de plateforme est généralement externe à votre déploiement StorageGRID, ces services vous offrent la puissance et la flexibilité liées à l'utilisation de ressources de stockage externes, de services de notification et de services de recherche ou d'analyse pour vos données.

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



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

Comment les services de la plateforme sont configurés

Les services de la plateforme communiquent avec des points de terminaison externes que vous configurez à l'aide de l'["Gestionnaire de locataires"](#) ou de l'["API de gestion des locataires"](#). Chaque point de terminaison représente une destination externe, telle qu'un compartiment StorageGRID S3, un compartiment Amazon Web Services, un sujet Amazon SNS, un point de terminaison webhook ou un cluster Elasticsearch hébergé localement, sur AWS ou ailleurs.

Après avoir créé un point de terminaison externe, vous pouvez activer un service de plateforme 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 plateforme que vous souhaitez configurer. Par exemple :

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

`${post_edited_translations.segment}`

Service de plateforme	API REST S3	Consultez
Réplication CloudMirror	• GetBucketReplication • PutBucketReplication	• "Réplication CloudMirror" • "Opérations sur les compartiments"
Notifications	• GetBucketNotificationConfiguration • PutBucketNotificationConfiguration	• "Notifications" • "Opérations sur les compartiments"
Intégration de la recherche	• Obtenir la configuration de notification des métadonnées du bucket • Configuration de notification des métadonnées du compartiment PUT	• "Intégration de la recherche" • "Opérations personnalisées StorageGRID"

Considérations relatives à l'utilisation des services de plateforme

<code>\${post_edited_translation.segment}</code>	Détails
Surveillance du point de terminaison de destination	Vous devez surveiller la disponibilité de chaque point de terminaison de destination. Si la connectivité au point de terminaison de destination est perdue pendant une période prolongée et qu'un important arriéré de requêtes existe, les requêtes client supplémentaires (telles que les requêtes PUT) adressées à StorageGRID échoueront. Vous devez réessayer ces requêtes ayant échoué lorsque le point de terminaison devient accessible.
Limitation du débit du point de terminaison de destination	Le logiciel StorageGRID peut limiter le nombre de requêtes S3 entrantes pour un compartiment si le débit d'envoi des requêtes dépasse le débit auquel le point de terminaison de destination peut les recevoir. La limitation ne se produit que lorsqu'il y a un retard d'envoi des requêtes en attente vers le point de terminaison de destination. Le seul effet visible est un allongement du temps d'exécution des requêtes S3 entrantes. Si vous constatez un ralentissement significatif des performances, vous devez réduire le débit d'ingestion ou utiliser un point de terminaison offrant une capacité supérieure. Si le nombre de requêtes en attente continue d'augmenter, les opérations S3 côté client (telles que les requêtes PUT) finiront par échouer. CloudMirror Les requêtes sont plus susceptibles d'être affectées par les performances du point de terminaison de destination, car elles impliquent généralement plus de transfert de données que les requêtes d'intégration de recherche ou de notification d'événements.

<code>\${post_edited_translations.segment}</code>	Détails
Garanties de commande	StorageGRID garantit l'ordre des opérations sur un objet au sein d'un site. Tant que toutes les opérations sur un objet sont effectuées au sein du même site, l'état final de l'objet (pour la réplication) sera toujours égal à l'état dans StorageGRID. StorageGRID s'efforce d'ordonner les requêtes lors d'opérations effectuées sur plusieurs sites StorageGRID. Par exemple, si vous écrivez initialement un objet sur le site A, puis que vous écrasez ultérieurement le même objet sur le site B, l'objet final répliqué par CloudMirror dans le compartiment de destination n'est pas garanti d'être la version la plus récente.
Suppressions d'objets pilotées par ILM	Pour correspondre au comportement de suppression d'AWS CRR et d'Amazon Simple Notification Service, les requêtes CloudMirror et de notification d'événement ne sont pas envoyées lorsqu'un objet du compartiment source est supprimé en raison des règles ILM de StorageGRID. Par exemple, aucune requête CloudMirror ou de notification d'événement n'est envoyée si une règle ILM supprime un objet après 14 jours. En revanche, les demandes d'intégration de recherche sont envoyées lorsque des objets sont supprimés en raison de l'ILM.
Utilisation des points de terminaison Kafka	Pour les points de terminaison Kafka, le protocole Mutual TLS n'est pas pris en charge. Par conséquent, si vous avez <code>ssl.client.auth</code> défini sur <code>required</code> dans la configuration de votre broker Kafka, cela peut entraîner des problèmes de configuration des points de terminaison Kafka. L'authentification des points de terminaison Kafka utilise les types d'authentification suivants. Ces types diffèrent de ceux utilisés pour l'authentification d'autres points de terminaison, tels que Amazon SNS, et nécessitent des identifiants de nom d'utilisateur et de mot de passe. • SASL/PLAIN • SASL/SCRAM-SHA-256 • <code>\${post_edited_translations.segment}</code> <code>\${post_edited_translations.segment}</code>

Considérations relatives à l'utilisation du service de réplication CloudMirror

<code>\${post_edited_translations.segment}</code>	Détails
État de la réplication	StorageGRID ne prend pas en charge l'`x-amz-replication-status` en-tête.

<code>\${post_edited_translations.segment}</code>	Détails
Taille de l'objet	La taille maximale des objets pouvant être répliqués dans un compartiment de destination par le service de réplication CloudMirror est de 5 Tio, ce qui correspond à la taille maximale des objets <i>pris en charge</i>. Note : la taille maximale <i>recommandée</i> pour une opération PutObject unique est de 5 Gio (5 368 709 120 octets). Si vous avez des objets d'une taille supérieure à 5 Gio, utilisez plutôt le chargement partitionné.
Gestion des versions de compartiments et identifiants de version	<code>\${post_edited_translations.segment}</code> Lors de l'utilisation du versionnage, veuillez noter que l'ordre des versions d'objets dans le compartiment de destination est déterminé au mieux et n'est pas garanti par le CloudMirror service, en raison des limitations du protocole S3. <code>\${post_edited_translations.segment}</code>
<code>\${post_edited_translations.segment}</code>	Le service CloudMirror ne réplique pas les requêtes PutObjectTagging ou DeleteObjectTagging qui fournissent un ID de version, en raison des limites du protocole S3. Les ID de version de la source et de la destination n'étant pas liés, il est impossible de garantir qu'une mise à jour de balise pour un ID de version spécifique sera répliquée. En revanche, le service CloudMirror réplique les requêtes PutObjectTagging ou DeleteObjectTagging qui ne spécifient pas d'identifiant de version. Ces requêtes mettent à jour les balises pour la clé la plus récente (ou la version la plus récente si le compartiment est versionné). Les ingestions normales avec balises (et non des mises à jour de balises) sont également répliquées.
Téléversements en plusieurs parties et ETag valeurs	Lors de la duplication d'objets téléchargés en plusieurs parties, le CloudMirror service ne conserve pas les différentes parties. Par conséquent, la valeur ETag de l'objet dupliqué sera différente de la valeur ETag de l'objet original.
Objets chiffrés 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 requête inclut les en-têtes SSE-C, l'opération échoue.
Compartiment avec S3 Object Lock activé	<code>\${post_edited_translations.segment}</code>

Découvrez le service de réplication CloudMirror StorageGRID

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

Par exemple, vous pouvez utiliser la réplication CloudMirror pour dupliquer des enregistrements clients spécifiques dans Amazon S3, puis exploiter les services AWS pour effectuer des analyses sur vos données.



CloudMirror la réplication n'est pas prise en charge si le compartiment source a le verrouillage d'objet S3 activé.

CloudMirror et ILM

CloudMirror replication fonctionne indépendamment des politiques ILM actives de la grille. Le service CloudMirror réplique les objets dès qu'ils sont stockés dans le compartiment source et les transfère vers le compartiment de destination dès que possible. La livraison des objets répliqués est déclenchée lorsque l'ingestion de l'objet réussit.

CloudMirror et réplication inter-grilles

La réplication CloudMirror présente des similitudes et des différences importantes avec la fonctionnalité de réplication inter-grilles. Consultez ["Comparez la réplication inter-grilles et la réplication CloudMirror"](#).

CloudMirror et les compartiments S3

CloudMirror replication est généralement configurée pour utiliser un compartiment S3 externe comme destination. Toutefois, vous pouvez également configurer la réplication pour utiliser un autre déploiement StorageGRID ou tout service compatible S3.

Buckets existants

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



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

`${post_edited_translations.segment}`

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

`${post_edited_translations.segment}`

Vous pouvez configurer la réplication CloudMirror sur des compartiments versionnés ou non versionnés. Les compartiments de destination peuvent être versionnés ou non versionnés. Vous pouvez utiliser n'importe quelle combinaison de compartiments versionnés et non versionnés. Par exemple, vous pouvez spécifier un compartiment versionné comme destination pour un compartiment source non versionné, ou inversement. Vous pouvez également répliquer entre des compartiments non versionnés.

`${post_edited_translations.segment}`

Comportement de suppression

Est identique au comportement de suppression du service Amazon S3, Cross-Region Replication (CRR). La suppression d'un objet dans un compartiment source ne supprime jamais un objet répliqué dans la destination. Si les compartiments source et de destination sont tous deux versionnés, le marqueur de suppression est répliqué. Si le compartiment de destination n'est pas versionné, la suppression d'un objet dans le compartiment source ne réplique pas le marqueur de suppression dans le compartiment de

destination et ne supprime pas l'objet de destination.

`${post_edited_translations.segment}`

Lors de la réplication des objets vers le compartiment de destination, StorageGRID les marque comme « répliques ». Un compartiment StorageGRID de destination ne répliquera pas à nouveau les objets marqués comme répliques, vous protégeant ainsi des boucles de réplication accidentelles. Ce marquage des répliques est interne à StorageGRID et ne vous empêche pas de tirer parti d'AWS CRR lorsque vous utilisez un compartiment Amazon S3 comme destination.



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

Événements dans le compartiment de destination

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

Découvrez les notifications d'événements StorageGRID pour les compartiments S3

Vous pouvez activer la notification d'événements pour un compartiment S3 si vous souhaitez que StorageGRID envoie des notifications concernant des événements spécifiques à un cluster Kafka de destination, un point de terminaison webhook ou Amazon Simple Notification Service.

Par exemple, vous pouvez configurer des alertes pour qu'elles soient envoyées aux administrateurs concernant chaque objet ajouté à un compartiment, où les objets représentent des fichiers journaux associés à un événement système critique.

Les notifications d'événements sont créées dans le compartiment source, conformément à la configuration des notifications, et sont transmises à la destination. Si un événement associé à un objet réussit, une notification concernant cet événement est créée et mise en file d'attente pour la livraison.

L'unicité et l'ordre des notifications ne sont pas garantis. Plusieurs notifications d'un même événement peuvent être envoyées à destination suite aux opérations mises en œuvre pour assurer la réussite de la livraison. De plus, la livraison étant asynchrone, l'ordre temporel des notifications à destination n'est pas garanti pour correspondre à l'ordre des événements sur le compartiment source, en particulier pour les opérations provenant de différents sites StorageGRID. Vous pouvez utiliser la clé `sequencer` dans le message d'événement pour déterminer l'ordre des événements pour un objet particulier, comme décrit dans la documentation Amazon S3.

Les notifications d'événements StorageGRID suivent l'API Amazon S3 avec certaines limitations.

- `${post_edited_translations.segment}`
 - `s3:ObjectCreated:`
 - `s3:ObjectCreated:Put`
 - `s3:ObjectCreated:Post`
 - `s3:ObjectCreated:Copie`

- s3:ObjectCreated:CompleteMultipartUpload
- s3:ObjectRemoved:
- s3:ObjectRemoved:Supprimer
- s3:ObjectRemoved:DeleteMarkerCreated
- s3:ObjectRestore:Post
- Les notifications d'événements envoyées depuis StorageGRID utilisent le format JSON standard, mais n'incluent pas certaines clés et utilisent des valeurs spécifiques pour d'autres, comme indiqué dans le tableau :

Nom de la clé	Valeur StorageGRID
eventSource	sgws:s3
awsRegion	<i>non inclus</i>
\${post_edited_translations.segment}	<i>non inclus</i>
arn	urn:sgws:s3:::bucket_name

Découvrez le service d'intégration de recherche StorageGRID

Vous pouvez activer l'intégration de la recherche pour un compartiment S3 si vous souhaitez utiliser un service externe de recherche et d'analyse de données pour les métadonnées de vos objets.

Le service d'intégration de la recherche est un service StorageGRID personnalisé qui envoie automatiquement et de manière asynchrone les métadonnées d'objet S3 à un point de terminaison de destination chaque fois qu'un objet est créé ou supprimé, ou que ses métadonnées ou ses balises sont mises à jour. Vous pouvez ensuite utiliser des outils sophistiqués de recherche, d'analyse de données, de visualisation ou d'apprentissage automatique fournis par le service de destination pour rechercher, analyser et tirer des enseignements de vos données d'objet.

Par exemple, vous pouvez configurer vos compartiments pour envoyer les métadonnées des objets S3 à un service Elasticsearch distant. Vous pouvez ensuite utiliser Elasticsearch pour effectuer des recherches dans vos compartiments et réaliser des analyses sophistiquées des tendances présentes dans les métadonnées de vos objets.

`${post_edited_translations.segment}`



Étant donné que le service d'intégration de recherche entraîne l'envoi des métadonnées des objets vers une destination, son fichier XML de configuration est appelé « *metadata* notification configuration XML ». Ce fichier XML de configuration est différent du « notification configuration XML » utilisé pour activer les notifications *event*.

`${post_edited_translations.segment}`

Vous pouvez activer le service d'intégration de recherche pour tout compartiment, versionné ou non. L'intégration de recherche est configurée en associant une configuration XML de notification des métadonnées

au compartiment, qui spécifie les objets concernés et la destination des métadonnées des objets.

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



Pour les balises et les métadonnées utilisateur, StorageGRID transmet les dates et les nombres à Elasticsearch sous forme de chaînes de caractères ou de notifications d'événements S3. Pour configurer Elasticsearch afin qu'il interprète ces chaînes comme des dates ou des nombres, suivez les instructions Elasticsearch pour le mappage dynamique des champs et le mappage des formats de date. Vous devez activer le mappage dynamique des champs sur l'index avant de configurer le service d'intégration de recherche. Après l'indexation d'un document, vous ne pouvez plus modifier les types de champs du document dans l'index.

`${post_edited_translations.segment}`

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

- Un objet est créé.
- `${post_edited_translations.segment}`
- Les métadonnées ou étiquettes des objets sont ajoutées, mises à jour ou supprimées. L'ensemble complet des métadonnées et des étiquettes est toujours envoyé lors d'une mise à jour, pas seulement les valeurs modifiées.

Après avoir ajouté un fichier 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, ses métadonnées utilisateur ou ses balises. Cependant, aucune notification n'est envoyée pour les objets qui étaient déjà présents dans le compartiment. Pour garantir que les métadonnées des objets pour tous les objets du compartiment sont envoyées à la destination, vous devez effectuer l'une des actions suivantes :

- Configurez le service d'intégration de recherche immédiatement après la création du compartiment et avant d'y ajouter des objets.
- Effectuez une action sur tous les objets déjà présents dans le compartiment qui déclenchera l'envoi d'un message de notification de métadonnées à la destination.

`${post_edited_translations.segment}`

Le service d'intégration de recherche StorageGRID prend en charge un cluster Elasticsearch comme destination. Comme pour les autres services de plateforme, la destination est spécifiée dans le point de terminaison dont l'URN est utilisé dans le XML de configuration du service. Utilisez le "[Outil NetApp Interoperability Matrix Tool](#)" pour déterminer les versions d'Elasticsearch prises en charge.

Gérer les points de terminaison des services de plateforme

Configurez les points de terminaison des services de plateforme dans StorageGRID

Avant de pouvoir configurer un service de plateforme pour un compartiment, vous devez configurer au moins un point de terminaison comme destination du service de plateforme.

L'accès aux services de la plateforme est activé pour chaque locataire par un administrateur StorageGRID.

Pour créer ou utiliser un point de terminaison de services de plateforme, vous devez être un utilisateur locataire disposant de l'autorisation Gérer les points de terminaison ou d'un accès Root, dans une grille dont le réseau a été configuré pour permettre aux nœuds de stockage d'accéder aux ressources de points de terminaison externes. Pour un seul locataire, vous pouvez configurer un maximum de 500 points de terminaison de services de plateforme. Contactez votre administrateur StorageGRID pour plus d'informations.

Qu'est-ce qu'un point de terminaison de services de plateforme ?

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

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

Chaque type de service de plateforme requiert son propre point de terminaison, vous devez donc configurer au moins un point de terminaison pour chaque service de plateforme que vous prévoyez d'utiliser. Après avoir défini un point de terminaison de service de plateforme, vous utilisez l'URN du point de terminaison comme destination dans le fichier XML de configuration utilisé pour activer le service.

Vous pouvez utiliser le même point de terminaison comme destination pour plusieurs compartiments sources. Par exemple, vous pouvez configurer plusieurs compartiments sources pour envoyer les métadonnées des objets au même point de terminaison d'intégration de recherche afin de pouvoir effectuer des recherches sur plusieurs compartiments. Vous pouvez également configurer un compartiment source pour utiliser plusieurs points de terminaison comme cibles, ce qui vous permet, par exemple, d'envoyer des notifications concernant la création d'objets à une rubrique Amazon Simple Notification Service (Amazon SNS) et des notifications concernant la suppression d'objets à une seconde rubrique Amazon SNS.

Points d'extrémité pour la réplication CloudMirror

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

Points de terminaison pour les notifications

StorageGRID prend en charge les points de terminaison Amazon SNS, Kafka et webhook. Les points de terminaison Simple Queue Service (SQS) et AWS Lambda ne sont pas pris en charge.

Pour les points de terminaison Kafka, l'authentification TLS mutuelle n'est pas prise en charge. Par conséquent, si vous avez `ssl.client.auth` défini sur `required` dans la configuration de votre broker Kafka, cela peut entraîner des problèmes de configuration des points de terminaison Kafka.

Points de terminaison pour le service d'intégration de recherche

StorageGRID prend en charge les points de terminaison d'intégration de recherche qui représentent des clusters Elasticsearch. Ces clusters Elasticsearch peuvent se trouver dans un centre de données local ou être hébergés dans un cloud AWS ou ailleurs.

Le point de terminaison d'intégration de recherche fait référence à un index et un type Elasticsearch spécifiques. Vous devez créer l'index dans Elasticsearch avant de créer le point de terminaison dans StorageGRID, sinon la création du point de terminaison échouera. Vous n'avez pas besoin de créer le type avant de créer le point de terminaison. StorageGRID créera le type si nécessaire lorsqu'il enverra les métadonnées de l'objet au point de terminaison.

Informations connexes

"Administrer StorageGRID"

Spécifiez un URN pour un point de terminaison des services de plateforme StorageGRID

Lorsque vous créez un point de terminaison de services de plateforme, vous devez spécifier un nom de ressource unique (URN). Vous utiliserez l'URN pour référencer le point de terminaison lorsque vous créerez un XML de configuration pour le service de plateforme. L'URN de chaque point de terminaison doit être unique.

StorageGRID valide les points de terminaison des services de plateforme lors de leur création. Avant de créer un point de terminaison des services de plateforme, vérifiez que la ressource spécifiée dans le point de terminaison existe et qu'elle est accessible.

`${post_edited_translations.segment}`

L'URN d'un point de terminaison de services de plateforme doit commencer par `arn:aws` ou `urn:mysite`, comme suit :

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

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

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

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

Par exemple, pour continuer à spécifier l'URN d'un point de terminaison CloudMirror hébergé sur StorageGRID, vous ajouteriez `s3` pour obtenir `urn:sgws:s3`.

Pour la plupart des points de terminaison, l'élément final de l'URN identifie la ressource cible spécifique à l'URI de destination, par exemple, `sns-topic-name`.

Pour les points de terminaison webhook, la ressource cible est l'URI de destination elle-même.

Service	<code>\${post_edited_translations.segment}</code>
Réplication CloudMirror	bucket-name

Service	<code>\${post_edited_translations.segment}</code>
Notifications	sns-topic-name ou kafka-topic-name <code>\${post_edited_translations.segment}</code>
Intégration de la recherche	domain-name/index-name/type-name Remarque : Si le cluster Elasticsearch n'est pas configuré pour créer automatiquement les index, vous devez créer l'index manuellement avant de créer le point de terminaison.

URNs pour les services hébergés sur AWS et GCP

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

- Réplication CloudMirror :

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

- `${post_edited_translations.segment}`

```
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 point de terminaison d'intégration de recherche AWS, le domain-name doit inclure la chaîne littérale `domain/`, comme illustré ici.

URN pour les services hébergés localement

Lorsque vous utilisez des services hébergés localement plutôt que des services cloud, vous pouvez spécifier l'URN de toute manière qui crée une URN valide et unique, à condition que l'URN inclue les éléments requis en troisième et dernière position. Vous pouvez laisser les éléments indiqués comme optionnels vides, ou les spécifier de toute manière qui vous aide à identifier la ressource et à rendre l'URN unique. Par exemple :

- Réplication CloudMirror :

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

Pour un point de terminaison CloudMirror hébergé sur StorageGRID, vous pouvez spécifier un URN valide qui commence par `urn:sgws :`

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

- `${post_edited_translations.segment}`

Spécifiez un point de terminaison Amazon Simple Notification Service :

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

Spécifiez un point de terminaison Kafka :

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

`${post_edited_translations.segment}`

```
urn:mystore:webhook:optional:optional:webhook-name
```

- Intégration de la recherche :

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



Pour les points de terminaison d'intégration de la recherche hébergés localement, l'élément `domain-name` peut être n'importe quelle chaîne, à condition que l'URN du point de terminaison soit unique.

Créer un point de terminaison de services de plateforme StorageGRID

`${post_edited_translations.segment}`

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#).
- `${post_edited_translations.segment}`
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Gérer les autorisations d'accès aux points de terminaison ou à l'accès root"](#).
- La ressource référencée par le point de terminaison des services de plateforme a été créée :
 - CloudMirror replication : compartiment S3
 - `${post_edited_translations.segment}`
 - `${post_edited_translations.segment}`
- Vous disposez des informations concernant la ressource de destination :
 - `${post_edited_translations.segment}`



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 que vous devez saisir.

- `${post_edited_translations.segment}`

"Spécifiez l'URN du point de terminaison des services de plateforme"

- Informations d'authentification (si nécessaire) :

`${post_edited_translations.segment}`

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

- `${post_edited_translations.segment}`
- `${post_edited_translations.segment}`

CloudMirror endpoints de réplication

Pour les points de terminaison de réplication CloudMirror, vous pouvez utiliser les identifiants suivants :

- `${post_edited_translations.segment}`
- `${post_edited_translations.segment}`

`${post_edited_translations.segment}`

Pour les points de terminaison Amazon SNS, vous pouvez utiliser les informations d'identification suivantes :

- `${post_edited_translations.segment}`

`${post_edited_translations.segment}`

`${post_edited_translations.segment}`

- `${post_edited_translations.segment}`
- `${post_edited_translations.segment}`
- `${post_edited_translations.segment}`

- Certificat de sécurité (si une vérification du certificat est requise)

- `${post_edited_translations.segment}`

Étapes

1. Sélectionnez **STOCKAGE (S3) > Points de terminaison des services de plateforme**. La page Points de terminaison des services de plateforme s'affiche.
2. Sélectionnez **Créer un point de terminaison**.
3. `${post_edited_translations.segment}`

`${post_edited_translations.segment}`

4. Dans le champ **URI**, spécifiez l'identifiant unique de ressource (URI) de l'endpoint.

Utilisez l'un des formats suivants :

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

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

- Port 443 pour les URI HTTPS et port 80 pour les URI HTTP (la plupart des points de terminaison)
- `${post_edited_translations.segment}`

`${post_edited_translations.segment}`

```
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 (HA) StorageGRID, et `10443` représente le port défini dans le point de terminaison de l'équilibreur de charge.



Dans la mesure du possible, vous devez vous connecter à un groupe HA de nœuds d'équilibrage de charge afin d'éviter un point de défaillance unique.

De même, l'URI d'un compartiment hébergé sur AWS pourrait être :

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



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

5. `${post_edited_translations.segment}`



Vous ne pouvez pas modifier l'URN d'un point de terminaison après sa création.

6. Sélectionnez **Continue**.

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



Si vous souhaitez une authentification pour les points de terminaison de webhook, configurez Mutual Transport Layer Security (mTLS) dans [Étape 9](#).

`${post_edited_translations.segment}`

`${post_edited_translations.segment}`

`${post_edited_translations.segment}`

Type d'authentification	Description	Informations d'identification
Anonyme	Fournit un accès anonyme à la destination. Fonctionne uniquement pour les endpoints dont la sécurité est désactivée.	<code>\${post_edited_translations.segment}</code>
<code>\${post_edited_translations.segment}</code>	<code>\${post_edited_translations.segment}</code>	• ID de la clé d'accès • <code>\${post_edited_translations.segment}</code>
<code>\${post_edited_translations.segment}</code>	Utilise un nom d'utilisateur et un mot de passe pour authentifier les connexions à la destination.	• Nom d'utilisateur • Mot de passe

CloudMirror endpoints de réplication

Saisissez ou téléversez les informations d'identification pour un point de terminaison de réplication CloudMirror.

`${post_edited_translations.segment}`

Type d'authentification	Description	Informations d'identification
Anonyme	Fournit un accès anonyme à la destination. Fonctionne uniquement pour les endpoints dont la sécurité est désactivée.	<code>\${post_edited_translations.segment}</code>
<code>\${post_edited_translations.segment}</code>	<code>\${post_edited_translations.segment}</code>	• ID de la clé d'accès • <code>\${post_edited_translations.segment}</code>

Type d'authentification	Description	Informations d'identification
<code>\${post_edited_translations.segment}</code>	Utilise des certificats et des clés pour authentifier les connexions à la destination.	<code>\${post_edited_translations.segment}</code> - Certificat CA du serveur (téléversement de fichier PEM) <code>\${post_edited_translations.segment}</code> <code>\${post_edited_translations.segment}</code> - Phrase secrète de la clé privée du client (facultatif)

`${post_edited_translations.segment}`

Saisissez ou téléchargez les informations d'identification pour un point de terminaison Amazon SNS.

`${post_edited_translations.segment}`

Type d'authentification	Description	Informations d'identification
Anonyme	Fournit un accès anonyme à la destination. Fonctionne uniquement pour les endpoints dont la sécurité est désactivée.	<code>\${post_edited_translations.segment}</code>
<code>\${post_edited_translations.segment}</code>	<code>\${post_edited_translations.segment}</code>	- ID de la clé d'accès <code>\${post_edited_translations.segment}</code>

`${post_edited_translations.segment}`

Saisissez ou téléchargez les identifiants pour un point de terminaison Kafka.

`${post_edited_translations.segment}`

Type d'authentification	Description	Informations d'identification
Anonyme	Fournit un accès anonyme à la destination. Fonctionne uniquement pour les endpoints dont la sécurité est désactivée.	<code>\${post_edited_translations.segment}</code>

Type d'authentification	Description	Informations d'identification
SASL/PLAIN	Utilise un nom d'utilisateur et un mot de passe en clair pour authentifier les connexions à la destination.	- Nom d'utilisateur - Mot de passe
SASL/SCRAM-SHA-256	Utilise un nom d'utilisateur et un mot de passe avec un protocole de défi-réponse et le hachage SHA-256 pour authentifier les connexions à la destination.	- Nom d'utilisateur - Mot de passe
<code>\${post_edited_translations.segment}</code>	<code>\${post_edited_translations.segment}</code>	- Nom d'utilisateur - Mot de passe

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

8. Sélectionnez **Continue**.
9. Sélectionnez un bouton radio pour **Vérifier les certificats** afin de choisir comment la connexion TLS au point de terminaison est vérifiée.

`${post_edited_translations.segment}`

Vérifiez la connexion TLS pour l'intégration Search, la réplication CloudMirror, Amazon SNS ou les points de terminaison Kafka.

Type de vérification de certificat	Description
TLS	<code>\${post_edited_translations.segment}</code>
Désactivées	La vérification du certificat est désactivée. Cette option n'est pas sécurisée.
Utilisez un certificat d'autorité de certification personnalisé	Le certificat d'autorité de certification personnalisé est utilisé pour vérifier l'identité du serveur lors de la connexion au point de terminaison.
<code>\${post_edited_translations.segment}</code>	Utilisez le certificat d'autorité de certification Grid par défaut installé sur le système d'exploitation pour sécuriser les connexions.

Points de terminaison Webhook uniquement

Vérifiez la connexion TLS pour les points de terminaison webhook.

Type de vérification de certificat	Description
TLS	<code>\${post_edited_translations.segment}</code>
mTLS	<code>\${post_edited_translations.segment}</code>
Désactivées	La vérification du certificat est désactivée. Cette option n'est pas sécurisée.
Utilisez un certificat d'autorité de certification personnalisé	Le certificat d'autorité de certification personnalisé est utilisé pour vérifier l'identité du serveur lors de la connexion au point de terminaison.

`${post_edited_translations.segment}`

Type de vérification de certificat	Description
<code>\${post_edited_translations.segment}</code>	Désactive la vérification du certificat du serveur, ce qui signifie que l'identité du serveur n'est pas vérifiée. Cette option n'est pas sécurisée.
Certificat client	<code>\${post_edited_translations.segment}</code>

Type de vérification de certificat	Description
Clé privée du client	La clé privée du certificat client. Si elle est chiffrée, elle doit utiliser le format traditionnel PKCS #1 (le format PKCS #8 n'est pas pris en charge).
Phrase secrète de la clé privée du client	La phrase de passe pour déchiffrer la clé privée du client. Si la clé privée n'est pas chiffrée, laissez ce champ vide.

10. Sélectionnez **Tester et créer un point de terminaison**.

- Un message de confirmation s'affiche si le point de terminaison est accessible avec les informations d'identification spécifiées. La connexion au point de terminaison est validée depuis un nœud sur chaque site.
- Un message d'erreur s'affiche si la validation du point de terminaison échoue. Si vous devez modifier le point de terminaison pour corriger l'erreur, sélectionnez **Retourner aux détails du point de terminaison** et mettez à jour les informations. Ensuite, sélectionnez **Tester et créer le point de terminaison**.



La création du point de terminaison échoue si les services de la plateforme ne sont pas activés pour votre compte locataire. Contactez votre administrateur StorageGRID.

Après avoir configuré un point de terminaison, vous pouvez utiliser son URN pour configurer un service de plateforme.

Informations connexes

- ["Spécifiez l'URN du point de terminaison des services de plateforme"](#)
- ["Configurer la réplication CloudMirror"](#)
- ["Configurer les notifications d'événements"](#)
- ["\\${post_edited_translations.segment}"](#)

Tester la connexion pour un point de terminaison des services de plateforme StorageGRID

[\\${post_edited_translations.segment}](#)

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Gérer les autorisations d'accès aux points de terminaison ou à l'accès root"](#).

À propos de cette tâche

StorageGRID ne vérifie pas que les identifiants disposent des autorisations appropriées.

Étapes

1. Sélectionnez **STORAGE (S3) > Points de terminaison des services de plateforme**.

La page des points de terminaison des services de la plateforme s'affiche et présente la liste des points de terminaison des services de la plateforme déjà configurés.

2. `${post_edited_translations.segment}`

`${post_edited_translations.segment}`

3. Sélectionnez **Test connection**.

- Un message de confirmation s'affiche si le point de terminaison est accessible avec les informations d'identification spécifiées. La connexion au point de terminaison est validée depuis un nœud sur chaque site.
- Un message d'erreur s'affiche si la validation du point de terminaison échoue. Si vous devez modifier le point de terminaison pour corriger l'erreur, sélectionnez **Configuration** et mettez à jour les informations. Ensuite, sélectionnez **Tester et enregistrer les modifications**.

Modifier un point de terminaison de services de plateforme dans StorageGRID

Vous pouvez modifier la configuration d'un point de terminaison de services de plateforme pour en changer le nom, l'URI ou d'autres détails. Par exemple, vous pourriez avoir besoin de mettre à jour des informations d'identification expirées ou de modifier l'URI pour qu'elle pointe vers un index Elasticsearch de secours en cas de basculement. Vous ne pouvez pas modifier l'URN d'un point de terminaison de services de plateforme.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Gérer les autorisations d'accès aux points de terminaison ou à l'accès root"](#).

Étapes

1. Sélectionnez **STORAGE (S3) > Points de terminaison des services de plateforme**.

La page des points de terminaison des services de la plateforme s'affiche et présente la liste des points de terminaison des services de la plateforme déjà configurés.

2. Sélectionnez le point de terminaison que vous souhaitez modifier.

`${post_edited_translations.segment}`

3. `${post_edited_translations.segment}`

4. `${post_edited_translations.segment}`



Vous ne pouvez pas modifier l'URN d'un point de terminaison après sa création.

a. Pour modifier le nom d'affichage du point de terminaison, sélectionnez l'icône de modification .

b. `${post_edited_translations.segment}`

c. Modifiez le type d'authentification si nécessaire.

- Pour l'authentification par clé d'accès, modifiez la clé si nécessaire en sélectionnant **Modifier la clé S3** et en collant un nouvel ID de clé d'accès et une nouvelle clé d'accès secrète. Si vous devez annuler vos modifications, sélectionnez **Annuler la modification de la clé S3**.
- Pour l'authentification CAP (C2S Access Portal), modifiez l'URL des informations d'identification temporaires ou la phrase secrète facultative de la clé privée du client et téléchargez de nouveaux fichiers de certificat et de clé selon les besoins.



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

d. `${post_edited_translations.segment}`

5. Sélectionnez **Tester et enregistrer les modifications**.

- Un message de réussite s'affiche si le point de terminaison peut être atteint à l'aide des identifiants spécifiés. La connexion au point de terminaison est vérifiée depuis un nœud sur chaque site.
- Un message d'erreur s'affiche si la validation du point de terminaison échoue. Modifiez le point de terminaison pour corriger l'erreur, puis sélectionnez **Tester et enregistrer les modifications**.

Supprimer un point de terminaison des services de plateforme StorageGRID

`${post_edited_translations.segment}`

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Gérer les autorisations d'accès aux points de terminaison ou à l'accès root"](#).

Étapes

1. Sélectionnez **STORAGE (S3) > Points de terminaison des services de plateforme**.

La page des points de terminaison des services de la plateforme s'affiche et présente la liste des points de terminaison des services de la plateforme déjà configurés.

2. Cochez la case correspondant à chaque point de terminaison que vous souhaitez supprimer.



Si vous supprimez un point de terminaison de services de plateforme en cours d'utilisation, le service de plateforme associé sera désactivé pour tous les compartiments qui utilisent ce point de terminaison. Toutes les requêtes qui n'ont pas encore été terminées seront abandonnées. Les nouvelles requêtes continueront d'être générées jusqu'à ce que vous modifiez la configuration de votre compartiment pour ne plus faire référence à l'URN supprimé. StorageGRID signalera ces requêtes comme des erreurs irrécupérables.

3. `${post_edited_translations.segment}`

`${post_edited_translations.segment}`

4. `${post_edited_translations.segment}`

Dépanner les erreurs de point de terminaison des services de plateforme StorageGRID

Si une erreur se produit lorsque StorageGRID tente de communiquer avec un point de terminaison des services de plateforme, un message s'affiche sur le tableau de bord. Sur la page Points de terminaison des services de plateforme, la colonne Dernière erreur indique depuis combien de temps l'erreur s'est produite. Aucune erreur ne s'affiche si les autorisations associées aux identifiants d'un point de terminaison sont incorrectes.

`#{post_edited_translations.segment}`

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 de locataires affiche un message d'alerte. Vous pouvez accéder à la page Points de terminaison des services de plateforme pour obtenir plus de détails sur l'erreur.

 One or more endpoints have experienced an error and might not be functioning properly. Go to the [Endpoints](#) page to view the error details. The last error occurred 2 hours ago.

La même erreur que celle qui s'affiche sur le tableau de bord apparaît également en haut de la page des points de terminaison des services de plateforme. Pour afficher un message d'erreur plus détaillé :

Étapes

1. `#{post_edited_translations.segment}`
2. Sur la page de détails du point de terminaison, sélectionnez **Connection**. Cet onglet affiche uniquement l'erreur la plus récente pour un point de terminaison et indique depuis combien de temps elle s'est produite. Les erreurs comportant l'icône X rouge  se sont produites au cours des 7 derniers jours.

`#{post_edited_translations.segment}`

Certaines erreurs peuvent continuer à apparaître dans la colonne **Dernière erreur** même après leur résolution. Pour vérifier si une erreur est toujours d'actualité ou pour forcer la suppression d'une erreur résolue du tableau :

Étapes

1. Sélectionnez le point de terminaison.

`#{post_edited_translations.segment}`
2. Sélectionnez **Connexion > Tester la connexion**.

La sélection de **Tester la connexion** permet à StorageGRID de valider que le point de terminaison des services de plateforme existe et qu'il est accessible avec les identifiants actuels. La connexion au point de terminaison est validée depuis un nœud sur chaque site.

Résoudre les erreurs de point de terminaison

Vous pouvez utiliser le message **Dernière erreur** sur la page de détails du point de terminaison pour vous aider à déterminer la cause de l'erreur. Certaines erreurs peuvent nécessiter que vous modifiez le point de terminaison pour résoudre le problème. Par exemple, une erreur CloudMirroring peut se produire si StorageGRID ne parvient pas à accéder au compartiment S3 de destination parce qu'il ne dispose pas des autorisations d'accès appropriées ou que la clé d'accès a expiré. Le message est « Either the endpoint credentials or the destination access needs to be updated, » et les détails sont « AccessDenied » ou « InvalidAccessKeyId. »

Si vous devez modifier le point de terminaison pour résoudre une erreur, la sélection de **Tester et enregistrer les modifications** amène StorageGRID à valider le point de terminaison mis à jour et à confirmer qu'il est accessible avec les informations d'identification actuelles. La connexion au point de terminaison est validée depuis un nœud sur chaque site.

Étapes

1. Sélectionnez le point de terminaison.
2. Sur la page de détails du point de terminaison, sélectionnez **Configuration**.
3. Modifiez la configuration du point de terminaison selon vos besoins.
4. Sélectionnez **Connexion > Tester la connexion**.

Informations d'identification du point de terminaison avec des autorisations insuffisantes

Lorsque StorageGRID valide un point de terminaison de service de plateforme, il vérifie que les informations d'identification de ce point de terminaison permettent de contacter la ressource de destination et effectue un contrôle d'autorisations de base. Toutefois, StorageGRID ne valide pas toutes les autorisations requises pour certaines opérations des services de plateforme. Par conséquent, si vous recevez une erreur lors de la tentative d'utilisation d'un service de plateforme (par exemple, "403 Forbidden"), vérifiez les autorisations associées aux informations d'identification du point de terminaison.

Informations connexes

- [Administrer StorageGRID > Dépanner les services de plateforme](#)
- ["Créer un point de terminaison de services de plateforme"](#)
- ["\\${post_edited_translations.segment}"](#)
- ["Modifier le point de terminaison des services de plateforme"](#)

Configurez la réplication CloudMirror dans StorageGRID

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

Avant de commencer

- ["\\${post_edited_translations.segment}"](#)
- ["\\${post_edited_translations.segment}"](#)
- Le point de terminaison que vous prévoyez d'utiliser comme destination pour la réplication CloudMirror existe déjà, et vous disposez de son URN.
- Vous appartenez à un groupe d'utilisateurs qui dispose de la ["Gérer tous les compartiments ou autorisation d'accès Root"](#). Ces autorisations prévalent sur les paramètres d'autorisation des politiques de groupe ou de compartiment lors de la configuration du compartiment à l'aide du Tenant Manager.

À propos de cette tâche

CloudMirror réplique des copies d'objets d'un compartiment source vers un compartiment de destination spécifié dans un point de terminaison.

Pour obtenir des informations générales sur la réplication de compartiment et sa configuration, consultez ["\\${post_edited_translations.segment}"](#). Pour en savoir plus sur la façon dont StorageGRID implémente GetBucketReplication, DeleteBucketReplication et PutBucketReplication, consultez le ["Opérations sur les compartiments"](#).



La réplication CloudMirror présente d'importantes similitudes et différences avec la fonctionnalité de réplication inter-grille. Pour en savoir plus, consultez ["Comparez la réplication inter-grilles et la réplication CloudMirror"](#).

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

- Lorsque vous créez et appliquez un fichier XML de configuration de réplication de compartiment valide, il doit utiliser l'URN d'un point de terminaison de compartiment S3 pour chaque destination.
- `${post_edited_translations.segment}`
- 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 sont pas répliqués. Vous devez mettre à jour les 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 point de terminaison S3 de destination. Le point de terminaison de destination doit également prendre en charge la classe de stockage spécifiée. Veillez à suivre toutes les recommandations fournies par le fournisseur du système de destination.

Étapes

1. `${post_edited_translations.segment}`

- Utilisez un éditeur de texte pour créer le fichier XML de configuration de réplication requis pour activer la réplication, comme spécifié dans l'API de réplication S3.
- `${post_edited_translations.segment}`
 - Notez que StorageGRID ne prend en charge que la version 1 de la configuration de réplication. Cela signifie que StorageGRID ne prend pas en charge l'utilisation de l'élément `Filter` pour les règles et suit les conventions de la version 1 pour la suppression des versions d'objets. Consultez la documentation Amazon relative à la configuration de réplication pour plus de détails.
 - `${post_edited_translations.segment}`
 - Ajoutez éventuellement l'élément `<StorageClass>` et spécifiez l'un des éléments suivants :
 - **STANDARD** : la classe de stockage par défaut. Si vous ne spécifiez pas de classe de stockage lorsque vous transférez un objet, la classe de stockage **STANDARD** est utilisée.
 - **STANDARD_IA** : (Standard - accès peu fréquent.) Utilisez cette classe de stockage pour les données consultées moins fréquemment, mais qui nécessitent tout de même un accès rapide en cas de besoin.
 - **REDUCED_REDUNDANCY** : Utilisez cette classe de stockage pour les données non critiques et reproductibles qui peuvent être stockées avec moins de redondance que la classe de stockage **STANDARD**.
 - Si vous spécifiez un `Role` dans le XML de configuration, il sera ignoré. Cette valeur n'est pas utilisée par StorageGRID.

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

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

`${post_edited_translations.segment}`

4. `${post_edited_translations.segment}`
5. `${post_edited_translations.segment}`
6. `${post_edited_translations.segment}`



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

7. `${post_edited_translations.segment}`
 - a. `${post_edited_translations.segment}`
`${post_edited_translations.segment}`
 - b. Confirmez que l'objet a été répliqué dans le compartiment de destination.

Pour les petits objets, la réplication se fait rapidement.

Informations connexes

["Créer un point de terminaison de services de plateforme"](#)

Configurez les notifications d'événements dans StorageGRID

Vous activez les notifications pour un compartiment en créant un fichier XML de configuration de notification et en utilisant le Tenant Manager pour appliquer le fichier XML à un compartiment.

Avant de commencer

- `${post_edited_translations.segment}`
- Vous avez déjà créé un compartiment qui servira de source de notifications.
- Le point de terminaison que vous souhaitez utiliser comme destination pour les notifications d'événements existe déjà, et vous disposez de son URN.
- Vous appartenez à un groupe d'utilisateurs qui dispose de la ["Gérer tous les compartiments ou autorisation d'accès Root"](#). Ces autorisations prévalent sur les paramètres d'autorisation des politiques de groupe ou de compartiment lors de la configuration du compartiment à l'aide du Tenant Manager.

À propos de cette tâche

Vous configurez les notifications d'événements en associant un fichier XML de configuration de notification à un compartiment source. Le fichier XML de configuration de notification suit les conventions S3 pour la configuration des notifications de compartiment, avec la destination (rubrique Amazon SNS, rubrique Kafka ou point de terminaison webhook) spécifiée comme l'URN d'un point de terminaison.

Pour obtenir des informations générales sur les notifications d'événements et leur configuration, consultez la

"[Documentation Amazon](#)". Pour des informations sur la manière dont StorageGRID implémente l'API de configuration des notifications de compartiment S3, consultez la "[Instructions pour la mise en œuvre des applications clientes S3](#)".

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

- Lorsque vous créez et appliquez un fichier XML de configuration de notification valide, celui-ci doit utiliser l'URN d'un point de terminaison de notification d'événement pour chaque destination.
- Bien que la notification d'événements puisse être configurée sur un compartiment avec S3 Object Lock activé, les métadonnées S3 Object Lock (y compris Retain Until Date et Legal Hold status) des objets ne seront pas incluses dans les messages de notification.
- Une fois les notifications d'événements configurées, lorsqu'un événement spécifié se produit pour un objet dans le compartiment source, une notification est générée et envoyée au sujet Amazon SNS, au sujet Kafka ou au point de terminaison webhook utilisé comme destination.
- Si vous activez les notifications d'événements pour un compartiment contenant des objets, les notifications ne sont envoyées que pour les actions effectuées après l'enregistrement de la configuration des notifications.

Étapes

1. Activez les notifications pour votre compartiment source :
 - Utilisez un éditeur de texte pour créer le fichier XML de configuration des notifications requis pour activer les notifications d'événements, comme spécifié dans l'API de notification S3.
 - Lors de la configuration du fichier XML, utilisez l'URN d'un point de terminaison de notifications 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 Tenant Manager, sélectionnez **STORAGE (S3) > Buckets**.
3. Sélectionnez le nom du compartiment source.

`${post_edited_translations.segment}`

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



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

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

- a. Effectuez une action sur un objet dans le compartiment source qui répond aux exigences pour déclencher une notification, comme configuré dans le fichier XML de configuration.

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

- b. Confirmez qu'une notification a été remise au sujet Amazon SNS, au sujet Kafka ou au point de terminaison webhook de destination.

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

```

{
  "Records": [
    {
      "eventVersion": "2.0",
      "eventSource": "sgws:s3",
      "eventTime": "2017-08-08T23:52:38Z",
      "eventName": "ObjectCreated:Put",
      "userIdentity": {
        "principalId": "11111111111111111111"
      },
      "requestParameters": {
        "sourceIPAddress": "193.51.100.20"
      },
      "responseElements": {
        "x-amz-request-id": "122047343"
      },
      "s3": {
        "s3SchemaVersion": "1.0",
        "configurationId": "Image-created",
        "bucket": {
          "name": "test1",
          "ownerIdentity": {
            "principalId": "11111111111111111111"
          },
          "arn": "arn:sgws:s3:::test1"
        },
        "object": {
          "key": "images/cat.jpg",
          "size": 0,
          "eTag": "d41d8cd98f00b204e9800998ecf8427e",
          "sequencer": "14D90402421461C7"
        }
      }
    }
  ]
}

```

+

Si la notification est reçue sur le sujet de destination, vous avez correctement configuré votre compartiment source pour les notifications StorageGRID.

Informations connexes

- ["Comprendre les notifications pour les compartiments"](#)
- ["Utilisez l'API REST S3"](#)

- ["Créer un point de terminaison de services de plateforme"](#)

Configurez le service d'intégration de recherche dans StorageGRID

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

Avant de commencer

- `${post_edited_translations.segment}`
- Vous avez déjà créé un compartiment S3 dont vous souhaitez indexer le contenu.
- Le point de terminaison que vous souhaitez utiliser comme destination pour le service d'intégration de recherche existe déjà, et vous disposez de son URN.
- Vous appartenez à un groupe d'utilisateurs qui dispose de la ["Gérer tous les compartiments ou autorisation d'accès Root"](#). Ces autorisations prévalent sur les paramètres d'autorisation des politiques de groupe ou de compartiment lors de la configuration du compartiment à l'aide du Tenant Manager.

À propos de cette tâche

Une fois le service d'intégration de recherche configuré 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 de l'objet au point de terminaison de destination.

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

Étapes

1. Activer l'intégration de la recherche pour un compartiment :

- Utilisez un éditeur de texte pour créer le fichier XML de notification des métadonnées requis pour activer l'intégration de la recherche.
- Lors de la configuration du fichier XML, utilisez l'URN d'un point de terminaison d'intégration de recherche comme destination.

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

Au besoin, reportez-vous au [Exemples pour la configuration des métadonnées XML](#).

```

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

```

Éléments du fichier XML de configuration des notifications de métadonnées :

Nom	Description	Obligatoire
MetadataNotificationConfiguration	Balise 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 conteneur pour une règle qui identifie les objets dont les métadonnées doivent être ajoutées à un index spécifié. Les règles comportant des préfixes qui se chevauchent sont rejetées. Inclus dans l'élément MetadataNotificationConfiguration.	Oui
ID	Identifiant unique de la règle. Inclus dans l'élément Rule.	Non
Statut	Le statut peut être « Activé » ou « Désactivé ». Aucune action n'est entreprise pour les règles désactivées. Inclus dans l'élément Rule.	Oui
Préfixe	Les objets correspondant au préfixe sont concernés 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 Rule.	Oui
Destination	Étiquette conteneur pour la destination d'une règle. Inclus dans l'élément Rule.	Oui

Nom	Description	Obligatoire
Urn	URN de la destination où les métadonnées de l'objet sont envoyées. Doit être l'URN d'un point de terminaison StorageGRID possédant 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 <code>domain-name/myindex/mytype</code>. Les points de terminaison sont configurés à l'aide du Gestionnaire de locataires ou de l'API de gestion des locataires. Ils se présentent sous la forme suivante : • <code>arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype</code> • <code>urn:mysite:es:::mydomain/myindex/mytype</code> Le point de terminaison doit être configuré avant la soumission du fichier XML de configuration, sinon la configuration échouera avec une erreur 404. L'URN est inclus dans l'élément Destination.	Oui

2. Dans le Tenant Manager, sélectionnez **STORAGE (S3) > Buckets**.

3. Sélectionnez le nom du compartiment source.

```
{post_edited_translations.segment}
```

4. Sélectionnez **Services de plateforme > Intégration de recherche**

5. Cochez la case **Activer l'intégration de la recherche**.

6. Collez la configuration de notification des métadonnées dans la zone de texte, puis sélectionnez **Enregistrer les modifications**.



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

7. Vérifiez que le service d'intégration de recherche est correctement configuré :

- Ajoutez un objet au compartiment source qui répond aux exigences de déclenchement d'une notification de métadonnées, comme spécifié dans le fichier XML de configuration.

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

- Confirmez qu'un document JSON contenant les métadonnées et les balises de l'objet a été ajouté à l'index de recherche spécifié dans le point de terminaison.

Après avoir terminé

Si nécessaire, vous pouvez désactiver l'intégration de recherche pour un compartiment en utilisant l'une des méthodes suivantes :

- Sélectionnez **STOCKAGE (S3) > Buckets** et décochez la case **Activer l'intégration de recherche**.
- Si vous utilisez directement l'API S3, utilisez une requête de notification de métadonnées DELETE Bucket. Consultez les instructions pour la mise en œuvre des applications clientes S3.

Exemple : Configuration de notification des métadonnées qui s'applique à tous les objets

Dans cet exemple, les métadonnées de tous les objets sont envoyées à la même destination.

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

Exemple : Configuration des notifications de métadonnées avec deux règles

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

```

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Images-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/images</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Videos-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/videos</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-west-1:2222222:domain/es-
domain/graphics/videotype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>

```

Format de notification des métadonnées

`${post_edited_translations.segment}`

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

```

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

```

Champs inclus dans le document JSON

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

Informations sur le bucket et l'objet

`bucket` : Nom du compartiment

`key`: Nom de la clé de l'objet

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

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

Métadonnées système

`size`: Taille de l'objet (en octets) telle qu'elle est visible pour un client HTTP

`md5`: Hachage d'objet

Métadonnées utilisateur

`metadata`: Toutes les métadonnées utilisateur de l'objet, sous forme de paires clé-valeur

`key:value`

Étiquettes

`tags`: Toutes les étiquettes d'objet définies pour l'objet, sous forme de paires clé-valeur

`key:value`

Comment afficher les résultats dans Elasticsearch

Pour les balises et les métadonnées utilisateur, StorageGRID transmet les dates et les nombres à Elasticsearch sous forme de chaînes ou de notifications d'événements S3. Pour configurer Elasticsearch afin qu'il interprète ces chaînes comme des dates ou des nombres, suivez les instructions Elasticsearch concernant le mappage dynamique des champs et le mappage des formats de date. Activez le mappage dynamique des champs sur l'index avant de configurer le service d'intégration de recherche. Après l'indexation d'un document, vous ne pouvez plus modifier les types de champs du document dans l'index.

Utilisez l'API REST S3

Versions et mises à jour prises en charge de l'API REST StorageGRID S3

StorageGRID prend en charge l'API Simple Storage Service (S3), qui est implémentée sous la forme d'un ensemble de services web REST (Representational State Transfer).

La prise en charge de l'API REST S3 vous permet de connecter des applications orientées services développées pour les services web S3 à un stockage d'objets sur site utilisant le système StorageGRID. Seules des modifications minimales sont nécessaires dans l'utilisation actuelle des appels à l'API REST S3 par l'application cliente.

Versions prises en charge

StorageGRID prend en charge les versions spécifiques suivantes de STS, S3 et HTTP :

Article	Version
Spécification de l'API STS AssumeRole	"Documentation Amazon Web Services (AWS) : Référence de l'API Amazon Assumerole" Pour plus d'informations sur AssumeRole, veuillez consulter "Configurez AssumeRole".
Spécification de l'API S3	"Documentation AWS : Référence de l'API Amazon Simple Storage Service"
HTTP	1,1 Pour plus d'informations sur HTTP, voir HTTP/1.1 (RFCs 7230-35). "IETF RFC 2616 : Protocole de transfert hypertexte (HTTP/1.1)" Remarque : StorageGRID ne prend pas en charge le pipelining HTTP/1.1.

Mises à jour de la prise en charge de l'API REST S3

Version	Commentaires
12,0	• Ajout de la prise en charge du partage de ressources entre origines (CORS) pour une interface de gestion, permettant à un autre domaine d'accéder aux données de StorageGRID à l'aide des API de gestion. "En savoir plus". • Ajout de la prise en charge de STS AssumeRole et des stratégies de session. Voir "un exemple de politique de session". Vous pouvez configurer AssumeRole dans les groupes de locataires.

Version	Commentaires
11,9	• Ajout de la prise en charge des valeurs de somme de contrôle SHA-256 précalculées pour les requêtes et en-têtes suivants. Vous pouvez utiliser cette fonctionnalité pour vérifier l'intégrité des objets téléchargés : ◦ CompleteMultipartUpload: x-amz-checksum-sha256 ◦ CreateMultipartUpload: x-amz-checksum-algorithm ◦ GetObject: x-amz-checksum-mode ◦ HeadObject: x-amz-checksum-mode ◦ ListParts ◦ PutObject: x-amz-checksum-sha256 ◦ UploadPart: x-amz-checksum-sha256 • Ajout de la possibilité pour l'administrateur de la grille de contrôler les paramètres de rétention et de conformité au niveau du locataire. Ces paramètres affectent les paramètres S3 Object Lock. ◦ Mode de rétention par défaut du compartiment et mode de rétention des objets : Gouvernance ou Conformité, si autorisé par l'administrateur de la grille. ◦ Période de rétention par défaut du compartiment et date de conservation de l'objet : doit être inférieure ou égale à la période de rétention maximale autorisée par l'administrateur de la grille. • Amélioration de la prise en charge de <code>aws-chunked</code> l'encodage du contenu et de la diffusion en continu des valeurs <code>x-amz-content-sha256</code>. Limitations : ◦ Si présent, <code>chunk-signature</code> est facultatif et n'est pas validé ◦ Si présent, <code>x-amz-trailer</code> le contenu est ignoré
11,8	Les noms des opérations S3 ont été mis à jour pour correspondre aux noms utilisés dans le "Documentation Amazon Web Services (AWS) : Référence de l'API Amazon Simple Storage Service".
11,7	• Ajouté "Référence rapide : Requêtes API S3 prises en charge". • Ajout de la prise en charge de l'utilisation du mode GOVERNANCE avec S3 Object Lock. • Ajout de la prise en charge de l'en-tête de réponse spécifique à StorageGRID <code>x-ntap-sg-cgr-replication-status</code> pour les requêtes GET Object et HEAD Object. Cet en-tête indique l'état de réplication d'un objet pour la réplication inter-grilles. • SelectObjectContent prend désormais en charge les objets Parquet.

Version	Commentaires
11,6	• Ajout de la prise en charge de l'utilisation du <code>partNumber</code> paramètre de requête dans les requêtes GET Object et HEAD Object. • Ajout de la prise en charge d'un mode de rétention par défaut et d'une période de rétention par défaut au niveau du compartiment pour S3 Object Lock. • Ajout de la prise en charge de la <code>`s3:object-lock-remaining-retention-days`</code> clé de condition de stratégie pour définir la plage des périodes de conservation autorisées pour vos objets. • La taille maximale <i>recommandée</i> pour une opération PUT Object unique est désormais de 5 Gio (5 368 709 120 octets). Si vous avez des objets d'une taille supérieure à 5 Gio, utilisez plutôt le chargement partitionné.
11,5	• Ajout de la prise en charge de la gestion du chiffrement des compartiments. • Ajout de la prise en charge de S3 Object Lock et suppression des anciennes requêtes de conformité. • Ajout de la prise en charge de l'utilisation de DELETE Multiple Objects sur les compartiments versionnés. • L' <code>`Content-MD5`</code> en-tête de requête est désormais correctement pris en charge.
11,4	• Ajout de la prise en charge de DELETE Bucket tagging, GET Bucket tagging et PUT Bucket tagging. Les balises 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 type d'événement <code>s3:ObjectRestore:Post</code>. • Les limites de taille AWS pour les chargements en plusieurs parties sont désormais appliquées. Chaque partie d'un chargement en plusieurs parties doit avoir une taille comprise entre 5 MiB et 5 GiB. La dernière partie peut être inférieure à 5 MiB. • Ajout de la prise en charge de TLS 1.3
11,3	• Ajout de la prise en charge du chiffrement côté serveur des données d'objet avec des clés fournies par le client (SSE-C). • Ajout de la prise en charge des opérations DELETE, GET et PUT du cycle de vie des compartiments (action d'expiration uniquement) et de l'en-tête de réponse <code>x-amz-expiration</code>. • Mise à jour de PUT Object, PUT Object - Copy et Multipart Upload pour décrire l'impact des règles ILM qui utilisent un placement synchrone à l'ingestion. • Les chiffrements TLS 1.1 ne sont plus pris en charge.

Version	Commentaires
11,2	Ajout de la prise en charge de la restauration d'objets POST pour une utilisation avec les Cloud Storage Pools. Ajout de la prise en charge de l'utilisation de la syntaxe AWS pour les ARN, les clés de condition de stratégie et les variables de stratégie dans les stratégies de groupe et de compartiment. Les stratégies de groupe et de compartiment existantes qui utilisent la syntaxe StorageGRID continueront d'être prises en charge. Remarque : Les utilisations des ARN/URN dans d'autres configurations JSON/XML, y compris celles utilisées dans les fonctionnalités personnalisées de StorageGRID, n'ont pas changé.
11,1	Ajout de la prise en charge du partage de ressources entre origines (CORS), du protocole HTTP pour les connexions client S3 aux nœuds de la grille et des paramètres de conformité sur les compartiments.
11,0	Ajout de la prise en charge de la configuration des services de plateforme (CloudMirror replication, notifications et intégration de la recherche Elasticsearch) pour les compartiments. Ajout également de la prise en charge des contraintes de localisation des balises d'objets pour les compartiments et de la cohérence Available.
10,4	Ajout de la prise en charge des modifications de versionnement de l'analyse ILM, des mises à jour de la page Noms de domaine des points de terminaison, des conditions et des variables dans les politiques, des exemples de politiques et de l'autorisation PutOverwriteObject.
10,3	Ajout de la prise en charge du versionnage.
10,2	Ajout de la prise en charge des politiques d'accès aux groupes et aux compartiments, ainsi que de la copie en plusieurs parties (Upload Part - Copy).
10,1	Ajout de la prise en charge du téléchargement en plusieurs parties, des requêtes 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 la <i>Référence de l'API Simple Storage Service</i> est 2006-03-01.

Requêtes S3 API prises en charge dans StorageGRID

Cette page résume comment StorageGRID prend en charge les API Amazon Simple Storage Service (S3).

Cette page ne comprend que les opérations S3 prises en charge par StorageGRID.



Pour consulter la documentation AWS relative à chaque opération, sélectionnez le lien dans l'en-tête.

Paramètres de requête URI et en-têtes de requête courants

Sauf indication contraire, les paramètres de requête URI courants suivants sont pris en charge :

- `versionId` (comme requis pour les opérations sur les objets)

`${post_edited_translations.segment}`

- `Authorization`
- `Connection`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Date`
- `Expect`
- `Host`
- `x-amz-date`

Informations connexes

- ["Détails de l'implémentation de l'API REST S3"](#)
- ["Référence de l'API Amazon Simple Storage Service : En-têtes de requête courants"](#)

"AbortMultipartUpload"

`${post_edited_translations.segment}`

StorageGRID prend en charge toutes les [paramètres et en-têtes communs](#) pour cette requête, ainsi que ce paramètre de requête URI supplémentaire :

- `uploadId`

Corps de la requête

Aucune

Documentation StorageGRID

["\\${post_edited_translations.segment}"](#)

"CompleteMultipartUpload"

`${post_edited_translations.segment}`

StorageGRID prend en charge toutes les [paramètres et en-têtes communs](#) pour cette requête, ainsi que ce paramètre de requête URI supplémentaire :

- `uploadId`
- `x-amz-checksum-sha256`

Balises XML du corps de la requête

`${post_edited_translations.segment}`

- ChecksumSHA256
- CompleteMultipartUpload
- ETag
- Part
- PartNumber

Documentation StorageGRID

"CompleteMultipartUpload"

"CopyObject"

`${post_edited_translations.segment}`

StorageGRID prend en charge toutes [paramètres et en-têtes communs](#) pour cette requête, ainsi que les en-têtes supplémentaires suivants :

- x-amz-copy-source
- x-amz-copy-source-if-match
- x-amz-copy-source-if-modified-since
- x-amz-copy-source-if-none-match
- x-amz-copy-source-if-unmodified-since
- x-amz-copy-source-server-side-encryption-customer-algorithm
- x-amz-copy-source-server-side-encryption-customer-key
- x-amz-copy-source-server-side-encryption-customer-key-MD5
- x-amz-metadata-directive
- x-amz-object-lock-legal-hold
- x-amz-object-lock-mode
- x-amz-object-lock-retain-until-date
- x-amz-server-side-encryption
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-storage-class
- x-amz-tagging
- x-amz-tagging-directive
- x-amz-meta-<metadata-name>

Corps de la requête

Aucune

Documentation StorageGRID

"CopyObject"

"CreateBucket"

`${post_edited_translations.segment}`

StorageGRID prend en charge toutes [paramètres et en-têtes communs](#) pour cette requête, ainsi que les en-têtes supplémentaires suivants :

- `x-amz-bucket-object-lock-enabled`

Corps de la requête

StorageGRID prend en charge tous les paramètres du corps de requête définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation StorageGRID

"Opérations sur les compartiments"

"CreateMultipartUpload"

`${post_edited_translations.segment}`

StorageGRID prend en charge toutes [paramètres et en-têtes communs](#) pour cette requête, ainsi que les en-têtes supplémentaires suivants :

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `Expires`
- `x-amz-checksum-algorithm`
- `x-amz-server-side-encryption`
- `x-amz-storage-class`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-tagging`
- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-object-lock-legal-hold`
- `x-amz-meta-<metadata-name>`

Corps de la requête

Aucune

Documentation StorageGRID

["CreateMultipartUpload"](#)

"DeleteBucket"

`${post_edited_translations.segment}`

StorageGRID prend en charge toutes les [paramètres et en-têtes communs](#) pour cette demande.

Documentation StorageGRID

["Opérations sur les compartiments"](#)

"DeleteBucketCors"

`${post_edited_translations.segment}`

StorageGRID prend en charge toutes les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

Aucune

Documentation StorageGRID

["Opérations sur les compartiments"](#)

"DeleteBucketEncryption"

`${post_edited_translations.segment}`

StorageGRID prend en charge toutes les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

Aucune

Documentation StorageGRID

["Opérations sur les compartiments"](#)

"DeleteBucketLifecycle"

`${post_edited_translations.segment}`

StorageGRID prend en charge toutes les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

Aucune

Documentation StorageGRID

- ["Opérations sur les compartiments"](#)
- ["Créer une configuration de cycle de vie S3"](#)

"DeleteBucketPolicy"

`${post_edited_translations.segment}`

StorageGRID prend en charge toutes les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

Aucune

Documentation StorageGRID

["Opérations sur les compartiments"](#)

"DeleteBucketReplication"

`${post_edited_translations.segment}`

StorageGRID prend en charge toutes les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

Aucune

Documentation StorageGRID

["Opérations sur les compartiments"](#)

"DeleteBucketTagging"

`${post_edited_translations.segment}`

StorageGRID prend en charge toutes les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

Aucune

Documentation StorageGRID

["Opérations sur les compartiments"](#)

"DeleteObject"

`${post_edited_translations.segment}`

StorageGRID prend en charge toutes [paramètres et en-têtes communs](#) pour cette requête, ainsi que cet en-tête de requête supplémentaire :

- `x-amz-bypass-governance-retention`

Corps de la requête

Aucune

Documentation StorageGRID

["Opérations sur les objets"](#)

"DeleteObjects"

`${post_edited_translations.segment}`

StorageGRID prend en charge toutes [paramètres et en-têtes communs](#) pour cette requête, ainsi que cet en-tête de requête supplémentaire :

- `x-amz-bypass-governance-retention`

Corps de la requête

StorageGRID prend en charge tous les paramètres du corps de requête définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation StorageGRID

["Opérations sur les objets"](#)

"DeleteObjectTagging"

StorageGRID prend en charge toutes les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

Aucune

Documentation StorageGRID

["Opérations sur les objets"](#)

"GetBucketAcl"

`${post_edited_translations.segment}`

StorageGRID prend en charge toutes les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

Aucune

Documentation StorageGRID

["Opérations sur les compartiments"](#)

"GetBucketCors"

`${post_edited_translations.segment}`

StorageGRID prend en charge toutes les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

Aucune

Documentation StorageGRID

["Opérations sur les compartiments"](#)

"GetBucketEncryption"

`${post_edited_translations.segment}`

StorageGRID prend en charge toutes les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

Aucune

Documentation StorageGRID

["Opérations sur les compartiments"](#)

"GetBucketLifecycleConfiguration"

`${post_edited_translations.segment}`

StorageGRID prend en charge toutes les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

Aucune

Documentation StorageGRID

- ["Opérations sur les compartiments"](#)
- ["Créer une configuration de cycle de vie S3"](#)

"GetBucketLocation"

`${post_edited_translations.segment}`

StorageGRID prend en charge toutes les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

Aucune

Documentation StorageGRID

["Opérations sur les compartiments"](#)

"GetBucketNotificationConfiguration"

`${post_edited_translations.segment}`

StorageGRID prend en charge toutes les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

Aucune

Documentation StorageGRID

["Opérations sur les compartiments"](#)

"GetBucketPolicy"

`${post_edited_translations.segment}`

StorageGRID prend en charge toutes les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

Aucune

Documentation StorageGRID

["Opérations sur les compartiments"](#)

"GetBucketReplication"

`${post_edited_translations.segment}`

StorageGRID prend en charge toutes les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

Aucune

Documentation StorageGRID

["Opérations sur les compartiments"](#)

"GetBucketTagging"

`${post_edited_translations.segment}`

StorageGRID prend en charge toutes les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

Aucune

Documentation StorageGRID

["Opérations sur les compartiments"](#)

"GetBucketVersioning"

`${post_edited_translations.segment}`

StorageGRID prend en charge toutes les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

Aucune

Documentation StorageGRID

["Opérations sur les compartiments"](#)

"GetObject"

`${post_edited_translations.segment}`

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette requête, ainsi que ces paramètres de requête URI supplémentaires :

- x-amz-checksum-mode
- partNumber
- response-cache-control
- response-content-disposition
- response-content-encoding
- response-content-language
- response-content-type
- response-expires

Et ces en-têtes de requête supplémentaires :

- Range
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- If-Match
- If-Modified-Since

- If-None-Match
- If-Unmodified-Since

Corps de la requête

Aucune

Documentation StorageGRID

["GetObject"](#)

"GetObjectAcl"

`${post_edited_translations.segment}`

StorageGRID prend en charge toutes les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

Aucune

Documentation StorageGRID

["Opérations sur les objets"](#)

"GetObjectLegalHold"

`${post_edited_translations.segment}`

StorageGRID prend en charge toutes les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

Aucune

Documentation StorageGRID

["Utilisez l'API REST S3 pour configurer S3 Object Lock"](#)

"GetObjectLockConfiguration"

`${post_edited_translations.segment}`

StorageGRID prend en charge toutes les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

Aucune

Documentation StorageGRID

["Utilisez l'API REST S3 pour configurer S3 Object Lock"](#)

"GetObjectRetention"

`${post_edited_translations.segment}`

StorageGRID prend en charge toutes les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

Aucune

Documentation StorageGRID

"Utilisez l'API REST S3 pour configurer S3 Object Lock"

"GetObjectTagging"

`${post_edited_translations.segment}`

StorageGRID prend en charge toutes les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

Aucune

Documentation StorageGRID

["Opérations sur les objets"](#)

"HeadBucket"

`${post_edited_translations.segment}`

StorageGRID prend en charge toutes les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

Aucune

Documentation StorageGRID

["Opérations sur les compartiments"](#)

"HeadObject"

`${post_edited_translations.segment}`

StorageGRID prend en charge toutes [paramètres et en-têtes communs](#) pour cette requête, ainsi que les en-têtes supplémentaires suivants :

- x-amz-checksum-mode
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- If-Match
- If-Modified-Since
- If-None-Match
- If-Unmodified-Since
- Range

Corps de la requête

Aucune

Documentation StorageGRID

["HeadObject"](#)

"ListBuckets"

`${post_edited_translations.segment}`

StorageGRID prend en charge toutes les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

Aucune

Documentation StorageGRID

[Opérations sur le service](#) › [ListBuckets](#)

"ListMultipartUploads"

`${post_edited_translations.segment}`

StorageGRID prend en charge toutes les [paramètres et en-têtes communs](#) pour cette requête, ainsi que les paramètres supplémentaires suivants :

- `encoding-type`
- `key-marker`
- `max-uploads`
- `prefix`
- `upload-id-marker`

Corps de la requête

Aucune

Documentation StorageGRID

["ListMultipartUploads"](#)

"ListObjects"

`${post_edited_translations.segment}`

StorageGRID prend en charge toutes les [paramètres et en-têtes communs](#) pour cette requête, ainsi que les paramètres supplémentaires suivants :

- `delimiter`
- `encoding-type`
- `marker`
- `max-keys`
- `prefix`

Corps de la requête

Aucune

Documentation StorageGRID

["Opérations sur les compartiments"](#)

"ListObjectsV2"

`${post_edited_translations.segment}`

StorageGRID prend en charge toutes les [paramètres et en-têtes communs](#) pour cette requête, ainsi que les paramètres supplémentaires suivants :

- continuation-token
- delimiter
- encoding-type
- fetch-owner
- max-keys
- prefix
- start-after

Corps de la requête

Aucune

Documentation StorageGRID

["Opérations sur les compartiments"](#)

"ListObjectVersions"

`${post_edited_translations.segment}`

StorageGRID prend en charge toutes les [paramètres et en-têtes communs](#) pour cette requête, ainsi que les paramètres supplémentaires suivants :

- delimiter
- encoding-type
- key-marker
- max-keys
- prefix
- version-id-marker

Corps de la requête

Aucune

Documentation StorageGRID

["Opérations sur les compartiments"](#)

"ListParts"

`${post_edited_translations.segment}`

StorageGRID prend en charge toutes les [paramètres et en-têtes communs](#) pour cette requête, ainsi que les paramètres supplémentaires suivants :

- max-parts

- part-number-marker
- uploadId

Corps de la requête

Aucune

Documentation StorageGRID

["ListMultipartUploads"](#)

"PutBucketCors"

`${post_edited_translations.segment}`

StorageGRID prend en charge toutes les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

StorageGRID prend en charge tous les paramètres du corps de requête définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation StorageGRID

["Opérations sur les compartiments"](#)

"PutBucketEncryption"

`${post_edited_translations.segment}`

StorageGRID prend en charge toutes les [paramètres et en-têtes communs](#) pour cette demande.

Balises XML du corps de la requête

`${post_edited_translations.segment}`

- ApplyServerSideEncryptionByDefault
- Rule
- ServerSideEncryptionConfiguration
- SSEAlgorithm

Documentation StorageGRID

["Opérations sur les compartiments"](#)

"PutBucketLifecycleConfiguration"

`${post_edited_translations.segment}`

StorageGRID prend en charge toutes les [paramètres et en-têtes communs](#) pour cette demande.

Balises XML du corps de la requête

`${post_edited_translations.segment}`

- And
- Days
- Expiration

- ExpiredObjectDeleteMarker
- Filter
- ID
- Key
- LifecycleConfiguration
- NewerNoncurrentVersions
- NoncurrentDays
- NoncurrentVersionExpiration
- Prefix
- Rule
- Status
- Tag
- Value

Documentation StorageGRID

- ["Opérations sur les compartiments"](#)
- ["Créer une configuration de cycle de vie S3"](#)

"PutBucketNotificationConfiguration"

`${post_edited_translations.segment}`

StorageGRID prend en charge toutes les [paramètres et en-têtes communs](#) pour cette demande.

Balises XML du corps de la requête

`${post_edited_translations.segment}`

- Event
- Filter
- FilterRule
- Id
- Name
- NotificationConfiguration
- Prefix
- S3Key
- Suffix
- Topic
- TopicConfiguration
- Value

Documentation StorageGRID

["Opérations sur les compartiments"](#)

"PutBucketPolicy"

`${post_edited_translations.segment}`

StorageGRID prend en charge toutes les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

Pour plus de détails sur les champs du corps JSON pris en charge, voir ["Utilisez les stratégies d'accès aux compartiments et aux groupes"](#).

"PutBucketReplication"

`${post_edited_translations.segment}`

StorageGRID prend en charge toutes les [paramètres et en-têtes communs](#) pour cette demande.

Balises XML du corps de la requête

- Bucket
- Destination
- Prefix
- ReplicationConfiguration
- Rule
- Status
- StorageClass

Documentation StorageGRID

["Opérations sur les compartiments"](#)

"PutBucketTagging"

`${post_edited_translations.segment}`

StorageGRID prend en charge toutes les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

StorageGRID prend en charge tous les paramètres du corps de requête définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation StorageGRID

["Opérations sur les compartiments"](#)

"PutBucketVersioning"

`${post_edited_translations.segment}`

StorageGRID prend en charge toutes les [paramètres et en-têtes communs](#) pour cette demande.

Paramètres du corps de la requête

StorageGRID prend en charge les paramètres de corps de requête suivants :

- VersioningConfiguration
- Status

Documentation StorageGRID

"Opérations sur les compartiments"

"PutObject"

`${post_edited_translations.segment}`

StorageGRID prend en charge toutes [paramètres et en-têtes communs](#) pour cette requête, ainsi que les en-têtes supplémentaires suivants :

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- Expires
- x-amz-checksum-sha256
- x-amz-server-side-encryption
- x-amz-storage-class
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-tagging
- x-amz-object-lock-mode
- x-amz-object-lock-retain-until-date
- x-amz-object-lock-legal-hold
- x-amz-meta-<metadata-name>

Corps de la requête

- Données binaires de l'objet

Documentation StorageGRID

"PutObject"

"PutObjectLegalHold"

`${post_edited_translations.segment}`

StorageGRID prend en charge toutes les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

StorageGRID prend en charge tous les paramètres du corps de requête définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation StorageGRID

"Utilisez l'API REST S3 pour configurer S3 Object Lock"

"PutObjectLockConfiguration"

`${post_edited_translations.segment}`

StorageGRID prend en charge toutes les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

StorageGRID prend en charge tous les paramètres du corps de requête définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation StorageGRID

"Utilisez l'API REST S3 pour configurer S3 Object Lock"

"PutObjectRetention"

`${post_edited_translations.segment}`

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette requête, ainsi que cet en-tête supplémentaire :

- `x-amz-bypass-governance-retention`

Corps de la requête

StorageGRID prend en charge tous les paramètres du corps de requête définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation StorageGRID

"Utilisez l'API REST S3 pour configurer S3 Object Lock"

"PutObjectTagging"

`${post_edited_translations.segment}`

StorageGRID prend en charge toutes les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

StorageGRID prend en charge tous les paramètres du corps de requête définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation StorageGRID

"Opérations sur les objets"

"RestoreObject"

`${post_edited_translations.segment}`

StorageGRID prend en charge toutes les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

Pour plus de détails sur les champs de corps pris en charge, voir ["RestoreObject"](#).

"SelectObjectContent"

`${post_edited_translations.segment}`

StorageGRID prend en charge toutes les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

Pour plus de détails sur les champs du corps pris en charge, consultez les informations suivantes :

- ["Utilisez S3 Select"](#)
- ["SelectObjectContent"](#)

"UploadPart"

`${post_edited_translations.segment}`

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette requête, ainsi que ces paramètres de requête URI supplémentaires :

- `partNumber`
- `uploadId`

Et ces en-têtes de requête supplémentaires :

- `x-amz-checksum-sha256`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`

Corps de la requête

- `${post_edited_translations.segment}`

Documentation StorageGRID

["UploadPart"](#)

["UploadPartCopy"](#)

`${post_edited_translations.segment}`

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette requête, ainsi que ces paramètres de requête URI supplémentaires :

- `partNumber`
- `uploadId`

Et ces en-têtes de requête supplémentaires :

- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-modified-since`
- `x-amz-copy-source-if-none-match`

- x-amz-copy-source-if-unmodified-since
- x-amz-copy-source-range
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-copy-source-server-side-encryption-customer-algorithm
- x-amz-copy-source-server-side-encryption-customer-key
- x-amz-copy-source-server-side-encryption-customer-key-MD5

Corps de la requête

Aucune

Documentation StorageGRID

["UploadPartCopy"](#)

Tester la configuration de l'API REST S3 de StorageGRID

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

Avant de commencer

- Vous avez téléchargé et installé l'AWS CLI depuis ["aws.amazon.com/cli"](https://aws.amazon.com/cli).
- Vous pouvez éventuellement ["a créé un point de terminaison d'équilibrage de charge"](#). Sinon, vous connaissez l'adresse IP du Storage Node auquel vous souhaitez vous connecter ainsi que le numéro de port à utiliser. Voir ["Adresses IP et ports pour les connexions client"](#).
- Vous avez ["a créé un compte locataire S3"](#).
- Vous vous êtes connecté au locataire et ["a créé une clé d'accès"](#).

Pour plus de détails sur ces étapes, voir ["Configurer les connexions client"](#).

Étapes

1. Configurez les paramètres de l'interface de ligne de commande AWS (AWS CLI) pour utiliser le compte que vous avez créé dans le système StorageGRID :
 - a. Entrez en mode de configuration : `aws configure`
 - b. Saisissez l'identifiant de la clé d'accès du compte que vous avez créé.
 - c. Saisissez la clé d'accès secrète du compte que vous avez créé.
 - d. Saisissez la région par défaut à utiliser. Par exemple, `us-east-1`.
 - e. Saisissez le format de sortie par défaut à utiliser, ou appuyez sur **Entrée** pour sélectionner JSON.
2. Créez un compartiment.

Cet exemple suppose que vous avez configuré un point de terminaison d'équilibrage de charge pour utiliser l'adresse IP 10.96.101.17 et le port 10443.

```
aws s3api --endpoint-url https://10.96.101.17:10443
--no-verify-ssl create-bucket --bucket testbucket
```

Si le compartiment est créé avec succès, son emplacement est renvoyé, comme illustré dans l'exemple suivant :

```
"Location": "/testbucket"
```

3. Téléchargez 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. Répertoriez le contenu du bucket 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. Supprimez 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

Comment l'API REST StorageGRID S3 résout les requêtes client conflictuelles

Les requêtes conflictuelles des clients, telles que deux clients écrivant sur la même clé, sont résolues selon le principe du « dernier arrivé, dernier servi ».

Le moment de l'évaluation « latest-wins » est basé sur le moment où le système StorageGRID termine une requête donnée, et non sur le moment où les clients S3 commencent une opération.

Comment l'API REST StorageGRID S3 équilibre la disponibilité et la cohérence

La cohérence assure un équilibre entre la disponibilité des objets et leur cohérence sur différents nœuds de stockage et sites. Vous pouvez modifier la cohérence selon les besoins de votre application.

Par défaut, StorageGRID garantit la cohérence en lecture après écriture pour les objets nouvellement créés. Toute requête GET suivant une requête PUT réussie pourra lire les données nouvellement écrites. Les écrasements d'objets existants, les mises à jour de métadonnées et les suppressions sont finalement cohérents.

Si vous souhaitez effectuer des opérations sur les objets avec un niveau de cohérence différent, vous pouvez :

- Spécifiez une cohérence pour [chaque compartiment](#).
- Spécifiez une consistance pour [chaque opération API](#).
- Modifiez la cohérence globale par défaut de la grille en effectuant l'une des tâches suivantes :
 - Dans le Gestionnaire de grille, accédez à **Configuration > Système > Paramètres de stockage > Cohérence par défaut des compartiments**.
 - .



Une modification de la cohérence globale de la grille s'applique uniquement aux compartiments créés après la modification du paramètre. Pour connaître les détails d'une modification, consultez le journal des audits situé à `/var/local/log` (recherchez **consistencyLevel**).

Valeurs de cohérence

La cohérence influe sur la manière dont les métadonnées que StorageGRID utilise pour le suivi des objets sont distribuées entre les nœuds. La cohérence influe sur la disponibilité des objets pour les requêtes client.

Vous pouvez définir la cohérence d'un compartiment ou d'une opération d'API sur l'une des valeurs suivantes :

- **Tous** : Tous les nœuds reçoivent immédiatement les métadonnées de l'objet ou la requête échouera.
- **Forte-globale** : Garantit la cohérence de lecture après écriture pour toutes les requêtes client sur tous les sites. Lorsque la sémantique de quorum est configurée, les comportements suivants s'appliquent :
 - Permet une tolérance aux pannes de site pour les requêtes client lorsque les grilles comportent trois sites ou plus. Les grilles à deux sites n'ont pas de tolérance aux pannes de site.
 - Les opérations S3 suivantes ne pourront pas aboutir si l'un des sites est hors service :
 - DeleteBucketEncryption
 - PutBucketBranch
 - PutBucketEncryption
 - PutBucketVersioning
 - PutObjectLegalHold
 - PutObjectLockConfiguration
 - PutObjectRetention

Si nécessaire, vous pouvez ["Configurer la sémantique de quorum de StorageGRID pour une cohérence](#)

globale forte".

- **Strong-site** : les métadonnées des objets sont immédiatement distribuées aux autres nœuds du site. Garantit la cohérence lecture-après-écriture pour toutes les requêtes client au sein du site.
- **Lecture après nouvelle écriture** : Garantit la cohérence en lecture après écriture pour les nouveaux objets et la cohérence éventuelle pour les mises à jour d'objets. Offre une haute disponibilité et des garanties de protection des données. Recommandé dans la plupart des cas.
- **Disponible** : Garantit la cohérence éventuelle pour les nouveaux objets et les mises à jour d'objets. Pour les compartiments S3, utilisez cette fonctionnalité uniquement en cas de besoin (par exemple, pour un compartiment contenant des valeurs de journaux rarement lues, ou pour les opérations HEAD ou GET sur des clés qui n'existent pas). Non pris en charge pour les compartiments S3 FabricPool.

Utilisez la cohérence « Lecture après nouvelle écriture » et « Disponible »

Lorsqu'une opération HEAD ou GET utilise la cohérence « Read-after-new-write », StorageGRID effectue la recherche en plusieurs étapes, comme suit :

- Il commence par rechercher l'objet avec un niveau de cohérence faible.
- Si cette recherche échoue, elle est répétée à la valeur de cohérence suivante jusqu'à atteindre une cohérence équivalente au comportement pour strong-global.

Si une opération HEAD ou GET utilise la cohérence « Lecture après nouvelle écriture » mais que l'objet n'existe pas, la recherche d'objet atteindra toujours un niveau de cohérence équivalent à celui du comportement pour strong-global. Parce que cette cohérence nécessite que plusieurs copies des métadonnées de l'objet soient disponibles sur chaque site, vous pouvez recevoir un nombre élevé d'erreurs 500 Internal Server Error si deux nœuds de stockage ou plus du même site sont indisponibles.

Sauf si vous exigez des garanties de cohérence similaires à celles d'Amazon S3, vous pouvez éviter ces erreurs pour les opérations HEAD et GET en définissant la cohérence sur « Disponible ». Lorsqu'une opération HEAD ou GET utilise la cohérence « Disponible », StorageGRID assure uniquement une cohérence éventuelle. Il ne retente pas une opération ayant échoué en cas de cohérence croissante, il n'est donc pas nécessaire que plusieurs copies des métadonnées de l'objet soient disponibles.

Spécifiez la cohérence pour l'opération API

Pour définir la cohérence d'une opération API individuelle, les valeurs de cohérence doivent être prises en charge pour l'opération, et vous devez spécifier la cohérence dans l'en-tête de la requête. Cet exemple définit la cohérence sur « Strong-site » pour une opération GetObject.

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



Vous devez utiliser la même cohérence pour les opérations PutObject et GetObject.

Spécifiez la cohérence du compartiment

Pour définir la cohérence d'un compartiment, vous pouvez utiliser la requête "[Cohérence PUT Bucket](#)" StorageGRID. Ou vous pouvez "[modifier la cohérence d'un bucket](#)" depuis le Tenant Manager.

Lors du réglage de la consistance d'un bucket, tenez compte des points suivants :

- La configuration de la cohérence d'un compartiment détermine le type de cohérence utilisé pour les opérations S3 effectuées sur les objets contenus dans le compartiment ou sur la configuration du compartiment. Elle n'affecte pas les opérations sur le compartiment lui-même.
- La cohérence d'une opération API individuelle prime sur la cohérence du compartiment.
- En règle générale, les buckets doivent utiliser la cohérence par défaut « Lecture après nouvelle écriture ». Si les requêtes ne fonctionnent pas correctement, modifiez le comportement du client applicatif si possible. Ou, configurez le client pour spécifier la cohérence pour chaque requête API. Définissez la cohérence au niveau du bucket uniquement en dernier recours.

Comment les règles de cohérence et les règles ILM interagissent pour affecter la protection des données

Le niveau de cohérence choisi et la règle ILM influent tous deux sur la manière dont les objets sont protégés. Ces paramètres peuvent interagir.

Par exemple, la cohérence utilisée lors du stockage d'un objet influe sur l'emplacement initial de ses métadonnées, tandis que le comportement d'ingestion sélectionné pour la règle ILM influe sur l'emplacement initial des copies de l'objet. Parce que StorageGRID nécessite l'accès à la fois aux métadonnées d'un objet et à ses données pour répondre aux requêtes client, le choix de niveaux de protection identiques pour la cohérence et le comportement d'ingestion peut offrir une meilleure protection des données initiale et des réponses système plus prévisibles.

Les ["options d'ingestion"](#) règles ILM suivantes sont disponibles :

Double engagement

StorageGRID crée immédiatement des copies intermédiaires de l'objet et renvoie la confirmation au client. Les copies spécifiées dans la règle ILM sont effectuées lorsque cela est possible.

Strict

Toutes les copies spécifiées dans la règle ILM doivent être effectuées avant que la réussite ne soit renvoyée au client.

Équilibré

StorageGRID tente de créer toutes les copies spécifiées dans la règle ILM lors de l'ingestion ; si cela s'avère impossible, des copies intermédiaires sont créées et un message de succès est renvoyé au client. Les copies spécifiées dans la règle ILM sont créées dès que possible.

Exemple de la façon dont la cohérence et la règle ILM peuvent interagir

Supposons que vous ayez une grille à trois sites avec la règle ILM suivante et la cohérence suivante :

- **Règle ILM** : Créez trois copies de l'objet, une sur le site local et une sur chaque site distant. Utilisez le comportement d'ingestion strict.
- **Cohérence** : Forte et globale (les métadonnées de l'objet sont immédiatement distribuées à plusieurs sites).

Lorsqu'un client stocke un objet dans la grille, StorageGRID effectue trois copies de l'objet et distribue les métadonnées à plusieurs sites avant de renvoyer un message de succès au client.

L'objet est intégralement protégé contre toute perte dès la confirmation de son ingestion. Par exemple, si le site local est perdu peu après l'ingestion, des copies des données de l'objet et des métadonnées de l'objet existent toujours sur les sites distants. L'objet est entièrement récupérable depuis les autres sites.

Si vous utilisiez la même règle ILM et la cohérence forte des sites, le client pourrait recevoir un message de succès après la réplication des données d'objet sur les sites distants, mais avant la distribution des métadonnées d'objet. Dans ce cas, le niveau de protection des métadonnées d'objet ne correspond pas au niveau de protection des données d'objet. Si le site local est perdu peu après l'ingestion, les métadonnées d'objet sont perdues. L'objet ne peut pas être récupéré.

L'interaction entre la cohérence et les règles ILM peut être complexe. Contactez NetApp si vous avez besoin d'assistance.

Comment StorageGRID utilise le versionnage des objets

Vous pouvez configurer le versionnage d'un compartiment si vous souhaitez conserver plusieurs versions de chaque objet. L'activation du versionnage pour un compartiment peut vous aider à vous prémunir contre la suppression accidentelle d'objets et vous permet de récupérer et de restaurer des versions antérieures d'un objet.

Le système StorageGRID implémente le versionnage et prend en charge la plupart des fonctionnalités, avec toutefois certaines limitations. StorageGRID prend en charge jusqu'à 10 000 versions de chaque objet.

Le versionnage des objets peut être combiné avec la gestion du cycle de vie des informations (ILM) de StorageGRID ou avec la configuration du cycle de vie des compartiments S3. Vous devez activer explicitement le versionnage pour chaque compartiment. Lorsque le versionnage est activé pour un compartiment, chaque objet ajouté au compartiment se voit attribuer un ID de version, qui est généré par le système StorageGRID.

L'utilisation de la suppression MFA (authentification multifacteur) n'est pas prise en charge.



Le versionnage ne peut être activé que sur les compartiments créés avec StorageGRID version 10.3 ou ultérieure.

ILM et gestion des versions

Les politiques ILM sont appliquées à chaque version d'un objet. Un processus d'analyse ILM examine en continu tous les objets et les réévalue par rapport à la politique ILM en vigueur. Toute modification apportée aux politiques ILM est appliquée à tous les objets précédemment importés. Cela inclut les versions précédemment importées si le versionnage est activé. L'analyse ILM applique les nouvelles modifications ILM aux objets précédemment importés.

Pour les objets S3 dans des compartiments avec versionnage activé, la prise en charge du versionnage vous permet de créer des règles ILM qui utilisent « Heure non actuelle » comme heure de référence (sélectionnez **Oui** à la question « Appliquer cette règle uniquement aux anciennes versions de l'objet ? » dans "[Étape 1 de l'assistant de création d'une règle ILM](#)"). Lorsqu'un objet est mis à jour, ses versions précédentes deviennent non actuelles. L'utilisation d'un filtre « Heure non actuelle » vous permet de créer des stratégies qui réduisent l'impact sur le stockage des versions précédentes des objets.



Lorsque vous chargez une nouvelle version d'un objet à l'aide d'une opération de chargement en plusieurs parties, l'horodatage de non-actualité de la version originale de l'objet correspond au moment où le chargement en plusieurs parties a été créé pour la nouvelle version, et non au moment où le chargement en plusieurs parties a été terminé. Dans certains cas limités, l'horodatage de non-actualité de la version originale peut être antérieur de plusieurs heures, voire de plusieurs jours, à celui de la version actuelle.

Informations connexes

- "\${post_edited_translations.segment}"
- "Règles et politiques ILM pour les objets versionnés S3 (Exemple 4)".

Utilisez l'API REST S3 pour configurer StorageGRID S3 Object Lock

Si le paramètre global S3 Object Lock est activé pour votre système StorageGRID, vous pouvez créer des compartiments avec S3 Object Lock activé. Vous pouvez spécifier une rétention par défaut pour chaque compartiment ou des paramètres de rétention pour chaque version d'objet.

`${post_edited_translations.segment}`

Si le paramètre de verrouillage global des objets S3 est activé pour votre système StorageGRID, vous pouvez éventuellement activer le verrouillage des objets S3 lors de la création de chaque compartiment.

Le verrouillage d'objet S3 est un paramètre permanent qui ne peut être activé que lors de la création d'un compartiment. Vous ne pouvez pas ajouter ni désactiver le verrouillage d'objet S3 après la création d'un compartiment.

`${post_edited_translations.segment}`

- Créez le compartiment à l'aide du Tenant Manager. Voir "[Créer un compartiment S3](#)".
- Créez le compartiment à l'aide d'une requête CreateBucket avec l'`x-amz-bucket-object-lock-enabled` en-tête de requête. Voir "[Opérations sur les compartiments](#)".

S3 Object Lock requiert le versionnement du compartiment, qui est activé automatiquement lors de la création du compartiment. Vous ne pouvez pas suspendre le versionnement pour le compartiment. Voir "[Versionnage d'objets](#)".

`${post_edited_translations.segment}`

Lorsque le verrouillage d'objet S3 est activé pour un compartiment, vous pouvez éventuellement activer la rétention par défaut pour le compartiment et spécifier un mode de rétention par défaut et une période de rétention par défaut.

Mode de rétention par défaut

- En mode CONFORMITÉ :
 - L'objet ne peut pas être supprimé tant que sa date de conservation n'est pas atteinte.
 - La date de conservation de l'objet peut être augmentée, mais elle ne peut pas être diminuée.
 - La date de conservation de l'objet ne peut pas être supprimée avant que cette date ne soit atteinte.
- En mode GOUVERNANCE :
 - Les utilisateurs disposant de l'`s3:BypassGovernanceRetention` autorisation peuvent utiliser l'`x-amz-bypass-governance-retention: true` en-tête de requête pour contourner les paramètres de rétention.
 - Ces utilisateurs peuvent supprimer une version d'objet avant que sa date de conservation ne soit atteinte.
 - Ces utilisateurs peuvent augmenter, diminuer ou supprimer la date de conservation d'un objet.

Période de conservation par défaut

`${post_edited_translations.segment}`

Comment définir la rétention par défaut pour un compartiment

`${post_edited_translations.segment}`

- Gérez les paramètres du compartiment depuis le Gestionnaire de locataires. Voir "[Créez un compartiment S3](#)" et "[Mettre à jour la rétention par défaut du verrouillage d'objet S3](#)".
- Envoyez une requête `PutObjectLockConfiguration` pour le compartiment afin de spécifier le mode par défaut et le nombre de jours ou d'années par défaut.

PutObjectLockConfiguration

La requête `PutObjectLockConfiguration` vous permet de définir et de modifier le mode de rétention par défaut et la période de rétention par défaut pour un compartiment ayant le verrouillage d'objets S3 activé. Vous pouvez également supprimer les paramètres de rétention par défaut précédemment configurés.

Lors de l'ingestion de nouvelles versions d'objets dans le compartiment, le mode de rétention par défaut est appliqué si `x-amz-object-lock-mode` et `x-amz-object-lock-retain-until-date` ne sont pas spécifiés. La période de rétention par défaut est utilisée pour calculer la date limite de rétention si `x-amz-object-lock-retain-until-date` n'est pas spécifié.

Si la période de conservation par défaut est modifiée après l'ingestion d'une version d'objet, la date de fin de conservation de la version d'objet reste la même et n'est pas recalculée en utilisant la nouvelle période de conservation par défaut.

Vous devez disposer de l'`s3:PutBucketObjectLockConfiguration` autorisation, ou être `account root`, pour effectuer cette opération.

L'`Content-MD5` en-tête de requête doit être spécifié dans la requête `PUT`.

Exemple de requête

Cet exemple active le verrouillage d'objet S3 pour un compartiment et définit le mode de rétention par défaut sur `COMPLIANCE` et la période de rétention par défaut sur 6 ans.

```

PUT /bucket?object-lock HTTP/1.1
Accept-Encoding: identity
Content-Length: 308
Host: host
Content-MD5: request header
User-Agent: s3sign/1.0.0 requests/2.24.0 python/3.8.2
X-Amz-Date: date
X-Amz-Content-SHA256: authorization-string
Authorization: authorization-string

<ObjectLockConfiguration>
  <ObjectLockEnabled>Enabled</ObjectLockEnabled>
  <Rule>
    <DefaultRetention>
      <Mode>COMPLIANCE</Mode>
      <Years>6</Years>
    </DefaultRetention>
  </Rule>
</ObjectLockConfiguration>

```

`${post_edited_translations.segment}`

Pour déterminer si le verrouillage d'objet S3 est activé pour un compartiment et pour afficher le mode de rétention et la période de rétention par défaut, utilisez l'une de ces méthodes :

- Consultez le compartiment dans le Gestionnaire de locataires. Voir ["Afficher les compartiments S3"](#).
- Envoyez une demande `GetObjectLockConfiguration`.

GetObjectLockConfiguration

La requête `GetObjectLockConfiguration` vous permet de déterminer si S3 Object Lock est activé pour un compartiment et, s'il est activé, de voir si un mode de rétention et une période de rétention par défaut sont configurés pour le compartiment.

Lorsque de nouvelles versions d'objets sont ingérées dans le compartiment, le mode de rétention par défaut est appliqué si `x-amz-object-lock-mode` n'est pas spécifié. La période de rétention par défaut est utilisée pour calculer la date limite de conservation si `x-amz-object-lock-retain-until-date` n'est pas spécifié.

Vous devez disposer de l'autorisation `s3:GetBucketObjectLockConfiguration`, ou être `account root`, pour effectuer cette opération.

Exemple de requête

```
GET /bucket?object-lock HTTP/1.1
Host: host
Accept-Encoding: identity
User-Agent: aws-cli/1.18.106 Python/3.8.2 Linux/4.4.0-18362-Microsoft
botocore/1.17.29
x-amz-date: date
x-amz-content-sha256: authorization-string
Authorization: authorization-string
```

Exemple de réponse

```
HTTP/1.1 200 OK
x-amz-id-2:
iVmcB7OXXJRkRH1FiVq1151/T24gRfpwpuZrEG11Bb9ImOMAAe98oxSpX1knabA0LTvBYJpSIX
k=
x-amz-request-id: B34E94CACB2CEF6D
Date: Fri, 04 Sep 2020 22:47:09 GMT
Transfer-Encoding: chunked
Server: AmazonS3

<?xml version="1.0" encoding="UTF-8"?>
<ObjectLockConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <ObjectLockEnabled>Enabled</ObjectLockEnabled>
  <Rule>
    <DefaultRetention>
      <Mode>COMPLIANCE</Mode>
      <Years>6</Years>
    </DefaultRetention>
  </Rule>
</ObjectLockConfiguration>
```

`${post_edited_translations.segment}`

Un compartiment avec le verrouillage d'objets S3 activé peut contenir une combinaison d'objets avec et sans paramètres de rétention de verrouillage d'objets S3.

Les paramètres de rétention au niveau de l'objet sont définis à l'aide de l'API REST S3. Les paramètres de rétention d'un objet remplacent tous les paramètres de rétention par défaut du compartiment.

Vous pouvez spécifier les paramètres suivants pour chaque objet :

- **Mode de rétention** : soit COMPLIANCE, soit GOVERNANCE.
- **Retain-until-date** : une date spécifiant la durée pendant laquelle la version de l'objet doit être conservée par StorageGRID.
 - En mode COMPLIANCE, si la date de conservation est dans le futur, l'objet peut être récupéré, mais il ne peut pas être modifié ou supprimé. La date de conservation peut être augmentée, mais cette date

ne peut pas être diminuée ou supprimée.

- En mode GOVERNANCE, les utilisateurs disposant d'une autorisation spéciale peuvent contourner le paramètre retain-until-date. Ils peuvent supprimer une version d'objet avant l'expiration de sa période de conservation. Ils peuvent également augmenter, diminuer ou même supprimer le retain-until-date.
- **Conservation légale** : L'application d'une conservation légale à une version d'objet verrouille immédiatement cet objet. Par exemple, vous pourriez avoir besoin d'appliquer une conservation légale à un objet lié à une enquête ou à un litige. Une conservation légale n'a pas de date d'expiration, mais reste en place jusqu'à ce qu'elle soit explicitement levée.

Le paramètre de conservation légale d'un objet est indépendant du mode de conservation et de la date limite de conservation. Si une version d'un objet est soumise à une conservation légale, personne ne peut supprimer cette version.

Pour spécifier les paramètres de S3 Object Lock lors de l'ajout d'une version d'objet à un compartiment, émettez une requête "PutObject", "CopyObject" ou "CreateMultipartUpload".

`${post_edited_translations.segment}`

- `x-amz-object-lock-mode`, qui peut être COMPLIANCE ou GOVERNANCE (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 de conservation jusqu'à la date doit être au format `2020-08-10T21:46:00Z`. Les fractions de seconde sont autorisées, mais seules trois décimales sont conservées (précision à la milliseconde). Les autres formats ISO 8601 ne sont pas autorisés.
 - `${post_edited_translations.segment}`
- `x-amz-object-lock-legal-hold`

Si la conservation légale est ON (sensible à la casse), l'objet est placé sous conservation légale. Si la conservation légale est OFF, aucune conservation légale n'est appliquée. Toute autre valeur entraîne une erreur 400 Bad Request (InvalidArgument).

Si vous utilisez l'un de ces en-têtes de requête, tenez compte des restrictions suivantes :

- L'`Content-MD5` en-tête de requête est requis si un `x-amz-object-lock-\*` en-tête de requête est présent dans la requête PutObject. `Content-MD5` n'est pas requis pour CopyObject ou CreateMultipartUpload.
- Si le compartiment n'a pas activé S3 Object Lock et qu'un en-tête de requête `x-amz-object-lock-*` est présent, une erreur 400 Bad Request (InvalidRequest) est renvoyée.
- La requête PutObject prend en charge l'utilisation de `x-amz-storage-class: REDUCED_REDUNDANCY` pour correspondre au comportement d'AWS. Toutefois, lorsqu'un objet est ingéré dans un compartiment avec S3 Object Lock activé, StorageGRID effectue toujours une ingestion dual-commit.
- Une réponse GET ou HeadObject de version ultérieure inclura les en-têtes `x-amz-object-lock-mode`, `x-amz-object-lock-retain-until-date` et `x-amz-object-lock-legal-hold`, s'ils sont configurés et si l'expéditeur de la requête dispose des autorisations `s3:Get*` correctes.

Vous pouvez utiliser la clé de condition de politique `s3:object-lock-remaining-retention-days` pour limiter les périodes de rétention minimales et maximales autorisées pour vos objets.

`${post_edited_translations.segment}`

`${post_edited_translations.segment}`

- `PutObjectLegalHold`

Si la nouvelle valeur de conservation légale est ON, l'objet est placé sous conservation légale. Si la valeur de conservation légale est OFF, la conservation légale est levée.

- `PutObjectRetention`
 - La valeur du mode peut être COMPLIANCE ou GOVERNANCE (sensible à la casse).
 - La valeur de conservation jusqu'à la date doit être au format `2020-08-10T21:46:00Z`. Les fractions de seconde sont autorisées, mais seules trois décimales sont conservées (précision à la milliseconde). Les autres formats ISO 8601 ne sont pas autorisés.
 - Si une version d'objet possède déjà une date de conservation (retain-until), vous pouvez uniquement l'augmenter. La nouvelle valeur doit être dans le futur.

Comment utiliser le mode GOVERNANCE

Les utilisateurs qui disposent de l'autorisation `s3:BypassGovernanceRetention` peuvent contourner les paramètres de rétention active d'un objet qui utilise le mode GOVERNANCE. Toutes les opérations DELETE ou `PutObjectRetention` doivent inclure l'en-tête de requête `x-amz-bypass-governance-retention:true`. Ces utilisateurs peuvent effectuer ces opérations supplémentaires :

- Exécutez les opérations `DeleteObject` ou `DeleteObjects` pour supprimer une version d'objet avant que sa période de rétention ne soit écoulée.

Les objets soumis à une conservation légale ne peuvent pas être supprimés. La conservation légale doit être désactivée.

- Effectuez des opérations `PutObjectRetention` qui modifient le mode d'une version d'objet de GOVERNANCE à COMPLIANCE avant que la période de rétention de l'objet ne soit écoulée.

Il est strictement interdit de passer du mode COMPLIANCE au mode GOVERNANCE.

- Effectuez des opérations `PutObjectRetention` pour augmenter, diminuer ou supprimer la période de conservation d'une version d'objet.

Informations connexes

- ["Gérez les objets avec S3 Object Lock"](#)
- `"${post_edited_translations.segment}"`
- ["Guide de l'utilisateur Amazon Simple Storage Service : Verrouillage des objets"](#)

Découvrez la configuration du cycle de vie S3 pour StorageGRID

Vous pouvez créer une configuration de cycle de vie S3 pour contrôler le moment où des objets spécifiques sont supprimés du système StorageGRID.

L'exemple simple présenté dans cette section illustre comment une configuration de cycle de vie S3 peut contrôler la suppression (expiration) de certains objets dans des compartiments S3 spécifiques. L'exemple de cette section est fourni uniquement à des fins d'illustration. Pour des informations complètes sur la création de configurations de cycle de vie S3, consultez ["Guide de l'utilisateur Amazon Simple Storage Service : gestion](#)

[du cycle de vie des objets](#)". Notez que StorageGRID prend uniquement en charge les actions d'expiration ; il ne prend pas en charge les actions de transition.

Ce qu'est la configuration du cycle de vie

Une configuration de cycle de vie est un ensemble de règles appliquées aux objets dans des compartiments S3 spécifiques. Chaque règle spécifie quels objets sont concernés et quand ces objets expireront (à une date précise ou après un certain nombre de jours).

StorageGRID prend en charge jusqu'à 1 000 règles de cycle de vie dans une configuration de cycle de vie. Chaque règle peut inclure les éléments XML suivants :

- Expiration : Supprimer un objet lorsqu'une date spécifiée est atteinte ou lorsqu'un nombre de jours spécifié est atteint, à compter de la date d'ingestion de l'objet.
- NoncurrentVersionExpiration : Supprimez un objet lorsqu'un nombre de jours spécifié est atteint, à compter du moment où l'objet est devenu non actuel.
- Filtrer (Préfixe, Tag)
- Statut
- ID

Chaque objet suit les paramètres de rétention définis soit par le cycle de vie d'un compartiment S3, soit par une stratégie ILM. Lorsqu'un cycle de vie de compartiment S3 est configuré, les actions d'expiration de ce cycle de vie prévalent sur la stratégie ILM pour les objets correspondant au filtre de cycle de vie du compartiment. Les objets qui ne correspondent pas au filtre de cycle de vie du compartiment utilisent les paramètres de rétention de la stratégie ILM. Si un objet correspond à un filtre de cycle de vie de compartiment et qu'aucune action d'expiration n'est explicitement spécifiée, les paramètres de rétention de la stratégie ILM ne sont pas utilisés et il est sous-entendu que les versions de l'objet sont conservées indéfiniment. Voir ["Exemples de priorités pour le cycle de vie d'un compartiment S3 et la politique ILM"](#).

Par conséquent, un objet peut être retiré de la grille même si les instructions de placement d'une règle ILM s'appliquent toujours à cet objet. Ou, un objet peut être conservé sur la grille même après l'expiration de toutes les instructions de placement ILM le concernant. Pour plus de détails, voir ["Comment l'ILM fonctionne tout au long du cycle de vie d'un objet"](#).



La configuration du cycle de vie des compartiments peut être utilisée avec les compartiments dont le S3 Object Lock est activé, mais la configuration du cycle de vie des compartiments n'est pas prise en charge pour les anciens compartiments Compliant.

StorageGRID prend en charge l'utilisation des opérations de compartiment suivantes pour gérer les configurations de cycle de vie :

- DeleteBucketLifecycle
- GetBucketLifecycleConfiguration
- PutBucketLifecycleConfiguration

Créer une configuration de cycle de vie

La première étape de la création d'une configuration de cycle de vie consiste à créer un fichier JSON contenant une ou plusieurs règles. Par exemple, ce fichier JSON contient trois règles, comme suit :

1. La règle 1 s'applique uniquement aux objets qui correspondent au préfixe `category1/` et qui ont une valeur de `key2 tag2`. Le paramètre `Expiration` 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` paramètre spécifie que les objets correspondant au filtre expireront 100 jours après leur ingestion.



Les règles qui spécifient un nombre de jours sont relatives à la date d'ingestion de l'objet. Si la date actuelle est postérieure à la date d'ingestion plus le nombre de jours, certains objets peuvent être supprimés du compartiment dès l'application de la configuration du cycle de vie.

3. La règle 3 s'applique uniquement aux objets qui correspondent au préfixe `category3/`. Le `Expiration` paramètre spécifie que toutes les versions non actuelles des objets correspondants expireront 50 jours après qu'elles soient devenues non actuelles.

```

{
  "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"
    }
  ]
}

```

Appliquer la configuration du cycle de vie au compartiment

Après avoir créé le fichier de configuration du cycle de vie, vous l'appliquez à un compartiment en émettant une requête `PutBucketLifecycleConfiguration`.

Cette requête applique la configuration de cycle de vie du fichier d'exemple aux objets d'un compartiment nommé `testbucket`.

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

Pour vérifier qu'une configuration de cycle de vie a bien été appliquée au compartiment, envoyez une requête `GetBucketLifecycleConfiguration`. Par exemple :

```
aws s3api --endpoint-url <StorageGRID endpoint> get-bucket-lifecycle-configuration
--bucket testbucket
```

Une réponse réussie répertorie la configuration du cycle de vie que vous venez d'appliquer.

Vérifiez que l'expiration du cycle de vie du compartiment s'applique à l'objet

Vous pouvez déterminer si une règle d'expiration dans la configuration du cycle de vie s'applique à un objet spécifique lors de l'émission d'une requête `PutObject`, `HeadObject` ou `GetObject`. Si une règle s'applique, la réponse inclut un `Expiration` paramètre qui indique quand l'objet expire et quelle règle d'expiration a été appliquée.



Étant donné que le cycle de vie du bucket remplace ILM, la ``expiry-date`` date affichée correspond à la date réelle à laquelle l'objet sera supprimé. Pour plus de détails, consultez ["Comment la rétention d'objet est déterminée"](#).

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

```
aws s3api --endpoint-url <StorageGRID endpoint> put-object
--bucket testbucket --key obj2test2 --body bktjson.json
```

La réponse positive indique que l'objet expirera dans 100 jours (01 Oct 2020) et qu'il correspond à la règle 2 de la configuration du cycle de vie.

```
{
  "Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:49 GMT\", rule-id=\"rule2\"",
  "ETag": "\"9762f8a803bc34f5340579d4446076f7\""
}
```

Par exemple, cette requête HeadObject a été utilisée pour obtenir les métadonnées du même objet dans le compartiment testbucket.

```
aws s3api --endpoint-url <StorageGRID endpoint> head-object
--bucket testbucket --key obj2test2
```

La réponse de succès inclut les métadonnées de l'objet et indique que l'objet expirera dans 100 jours et qu'il correspond à la Rule 2.

```
{
  "AcceptRanges": "bytes",
  *Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:48 GMT\", rule-
id=\"rule2\"",
  "LastModified": "2020-06-23T09:07:48+00:00",
  "ContentLength": 921,
  "ETag": "\"9762f8a803bc34f5340579d4446076f7\"",
  "ContentType": "binary/octet-stream",
  "Metadata": {}
}
```



Pour les compartiments compatibles avec le versionnage, l'`x-amz-expiration` en-tête de réponse s'applique uniquement aux versions actuelles des objets.

Recommandations pour la mise en œuvre de l'API REST S3 avec StorageGRID

`${post_edited_translations.segment}`

`${post_edited_translations.segment}`

Si votre application vérifie régulièrement si un objet existe dans un chemin où vous ne vous attendez pas à ce que l'objet existe réellement, vous devez utiliser le niveau « Available » ["cohérence"](#). Par exemple, vous devez utiliser la cohérence « Available » si votre application effectue une requête HEAD sur un emplacement avant d'y effectuer un PUT.

Sinon, si l'opération HEAD ne trouve pas l'objet, vous pourriez recevoir un grand nombre d'erreurs 500 Internal Server errors si deux ou plusieurs Storage Nodes du même site sont indisponibles ou si un site distant est inaccessible.

Vous pouvez définir la cohérence « Disponible » pour chaque compartiment à l'aide de la requête ["Cohérence PUT Bucket"](#), ou vous pouvez spécifier la cohérence dans l'en-tête de requête pour une opération API individuelle.

Recommandations concernant les clés d'objet

Suivez ces recommandations pour les noms de clés d'objet, en fonction du moment où le compartiment a été créé pour la première fois.

Compartiments créés dans StorageGRID 11.4 ou une version antérieure

- N'utilisez pas de valeurs aléatoires comme premiers quatre caractères des clés d'objet. Ceci contraste avec l'ancienne recommandation d'AWS concernant les préfixes de clés. Utilisez plutôt des préfixes non aléatoires et non uniques, tels que `image`.
- Si vous suivez l'ancienne recommandation d'AWS d'utiliser des caractères aléatoires et uniques dans les préfixes de clés, préfixez les clés d'objet avec un nom de répertoire. C'est-à-dire, utilisez ce format :

```
mybucket/mydir/f8e3-image3132.jpg
```

Au lieu de ce format :

```
mybucket/f8e3-image3132.jpg
```

`${post_edited_translations.segment}`

Il n'est pas nécessaire de restreindre les noms de clés d'objets pour respecter les bonnes pratiques en matière de performances. Dans la plupart des cas, vous pouvez utiliser des valeurs aléatoires pour les quatre premiers caractères des noms de clés d'objets.



Une exception à cela est une charge de travail S3 qui supprime continuellement tous les objets après une courte période. Pour minimiser l'impact sur les performances pour ce cas d'utilisation, faites varier la partie initiale du nom de la clé tous les quelques milliers d'objets avec un élément tel que la date. Par exemple, supposez qu'un client S3 écrive généralement 2 000 objets/seconde et que la politique ILM ou de cycle de vie du compartiment supprime tous les objets après trois jours. Pour minimiser l'impact sur les performances, vous pouvez nommer les clés en utilisant un modèle comme celui-ci : `/mybucket/mydir/yyyymmddhhmmss-random_UUID.jpg`

`${post_edited_translations.segment}`

Si la "[option globale pour compresser les objets stockés](#)" est activée, les applications clientes S3 doivent éviter d'effectuer des opérations `GetObject` qui spécifient le retour d'une plage d'octets. Ces opérations de « lecture par plage » sont inefficaces car `StorageGRID` doit effectivement décompresser les objets pour accéder aux octets demandés. Les opérations `GetObject` qui demandent une petite plage d'octets à partir d'un objet très volumineux sont particulièrement inefficaces ; par exemple, il est inefficace de lire une plage de 10 Mo à partir d'un objet compressé de 50 Go.

Si les plages sont lues à partir d'objets compressés, les requêtes client peuvent expirer.



Si vous devez compresser des objets et que votre application cliente doit utiliser des lectures par plage, augmentez le délai d'expiration de lecture pour l'application.

`${post_edited_translations.segment}`

Opérations prises en charge et limitations de l'API REST S3 dans `StorageGRID`

Le système `StorageGRID` implémente l'API Simple Storage Service (version 2006-03-01) et prend en charge la plupart des opérations, avec toutefois certaines limitations. Vous devez comprendre les détails d'implémentation lorsque vous intégrez des applications clientes de l'API REST S3.

`${post_edited_translations.segment}`

`${post_edited_translations.segment}`

`${post_edited_translations.segment}`

Le système StorageGRID prend en charge uniquement les formats de date HTTP valides pour tous les en-têtes qui acceptent des valeurs de date. La partie heure de la date peut être spécifiée au format GMT (Greenwich Mean Time) ou au format UTC (Universal Coordinated Time) sans décalage de fuseau horaire (+0000 doit être spécifié). Si vous incluez l'en-tête `x-amz-date` dans votre requête, il remplace toute valeur spécifiée dans l'en-tête de requête `Date`. Lors de l'utilisation d'AWS Signature Version 4, l'en-tête `x-amz-date` doit être présent dans la requête signée car l'en-tête de date n'est pas pris en charge.

En-têtes de requête courants

Le système StorageGRID prend en charge les en-têtes de requête communs définis par "[Référence de l'API Amazon Simple Storage Service : En-têtes de requête courants](#)", à une exception près.

En-tête de requête	Mise en œuvre
Autorisation	<code>\${post_edited_translations.segment}</code> <code>\${post_edited_translations.segment}</code> Lorsque vous fournissez la valeur réelle de la somme de contrôle de la charge utile dans <code>x-amz-content-sha256</code>, la valeur est acceptée sans validation, comme si la valeur <code>UNSIGNED-PAYLOAD</code> avait été fournie pour l'en-tête. Lorsque vous fournissez une valeur d'en-tête <code>x-amz-content-sha256</code> qui implique <code>aws-chunked</code> le streaming (par exemple, <code>STREAMING-AWS4-HMAC-SHA256-PAYLOAD</code>), les signatures de tronçon ne sont pas vérifiées par rapport aux données de tronçon.

`${post_edited_translations.segment}`

Le système StorageGRID prend en charge tous les en-têtes de réponse courants définis par la *Référence de l'API Simple Storage Service*, à une exception près.

<code>\${post_edited_translations.segment}</code>	Mise en œuvre
<code>\${post_edited_translations.segment}</code>	<code>\${post_edited_translations.segment}</code>

Comment l'API REST StorageGRID S3 authentifie les requêtes

Le système StorageGRID prend en charge l'accès authentifié et l'accès anonyme aux objets via l'API S3.

L'API S3 prend en charge la Signature version 2 et la Signature version 4 pour l'authentification des requêtes API S3.

Les requêtes authentifiées doivent être signées à l'aide de votre identifiant de clé d'accès et de votre clé d'accès secrète.

Le système StorageGRID prend en charge deux méthodes d'authentification : l'en-tête HTTP `Authorization` et l'utilisation des paramètres de requête.

Utilisez l'en-tête d'autorisation HTTP

L'`Authorization`en-tête HTTP est utilisé par toutes les opérations de l'API S3, à l'exception des requêtes anonymes autorisées par la politique du compartiment. L'`Authorization`en-tête contient toutes les informations de signature requises pour authentifier une requête.

Utilisez les paramètres de requête

Vous pouvez utiliser des paramètres de requête pour ajouter des informations d'authentification à une URL. Cela s'appelle la pré-signature de l'URL, ce qui peut être utilisé pour accorder un accès temporaire à des ressources spécifiques. Les utilisateurs disposant de l'URL pré-signée n'ont pas besoin de connaître la clé d'accès secrète pour accéder à la ressource, ce qui vous permet de fournir à des tiers un accès restreint à une ressource.

Opérations de service prises en charge dans StorageGRID

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

Opération	Mise en œuvre
ListBuckets (anciennement nommé GET Service)	Implémenté avec l'ensemble du comportement de l'API REST Amazon S3. Sous réserve de modifications sans préavis.
Obtenir l'utilisation du stockage	La requête " Obtenir l'utilisation du stockage " StorageGRID indique la capacité totale de stockage utilisée par un compte, ainsi que 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.
OPTIONS /	Les applications clientes peuvent envoyer `OPTIONS /` des requêtes au port S3 d'un nœud de stockage, sans fournir de paramètres d'authentification S3, afin de déterminer si le nœud de stockage est disponible. Vous pouvez utiliser cette requête pour la surveillance ou pour permettre aux équilibres de charge externes d'identifier lorsqu'un nœud de stockage est hors service.

Opérations sur les compartiments S3 et détails d'implémentation dans StorageGRID

Le système StorageGRID prend en charge un maximum de 5 000 compartiments pour chaque compte locataire S3.

Chaque grille peut comporter un maximum de 100 000 compartiments.

Pour prendre en charge 5 000 compartiments, chaque nœud de stockage de la grille doit disposer d'un minimum de 64 Go de RAM.

Les restrictions relatives aux noms de compartiments suivent les restrictions de la région standard AWS US,

mais vous devez les restreindre davantage aux conventions de nommage DNS pour prendre en charge les requêtes de type hébergement virtuel S3.

Pour plus d'informations, veuillez consulter les documents suivants :

- ["Guide de l'utilisateur d'Amazon Simple Storage Service : Quotas, restrictions et limitations des compartiments"](#)
- ["Configurer les noms de domaine des points de terminaison S3"](#)

Les opérations ListObjects (GET Bucket) et ListObjectVersions (GET Bucket object versions) prennent en charge StorageGRID ["valeurs de cohérence"](#).

Vous pouvez vérifier si les mises à jour du temps d'accès sont activées ou désactivées pour chaque compartiment. Voir ["Obtenir le temps d'accès du compartiment"](#).

Le tableau suivant décrit comment StorageGRID implémente les opérations sur les compartiments de l'API REST S3. Pour effectuer l'une de ces opérations, les identifiants d'accès nécessaires doivent être fournis pour le compte.

Opération	Mise en œuvre
CreateBucket	Crée un nouveau compartiment. En créant le compartiment, vous en devenez le propriétaire. • Les noms des compartiments doivent respecter les règles suivantes : ◦ Doit être unique dans chaque système StorageGRID (et pas seulement unique au sein du compte du locataire). ◦ Doit être conforme au DNS. ◦ Doit contenir au moins 3 et au plus 63 caractères. ◦ Peut être une série d'une ou plusieurs étiquettes, les étiquettes adjacentes étant séparées par un point. Chaque étiquette doit commencer et se terminer par une lettre minuscule ou un chiffre et ne peut utiliser que des lettres minuscules, des chiffres et des traits d'union. ◦ Ne doit pas ressembler à une adresse IP au format texte. ◦ Il est déconseillé d'utiliser des points dans les requêtes hébergées virtuellement. Les points peuvent entraîner des problèmes lors de la vérification du certificat générique du serveur. • Par défaut, les compartiments sont créés dans la <code>us-east-1</code> région ; cependant, vous pouvez utiliser l' <code>LocationConstraint</code> élément dans le corps de la requête pour spécifier une autre région. Lorsque vous utilisez l' <code>LocationConstraint</code> élément, vous devez indiquer le nom exact d'une région qui a été définie à l'aide de Grid Manager ou de l'API Grid Management. Contactez votre administrateur système si vous ne connaissez pas le nom de la région à utiliser. Remarque : Une erreur se produira si votre requête CreateBucket utilise une région qui n'a pas été définie dans StorageGRID. • Vous pouvez inclure l' <code>'x-amz-bucket-object-lock-enabled'</code> en-tête de requête pour créer un compartiment avec S3 Object Lock activé. Voir "Utilisez l'API REST S3 pour configurer S3 Object Lock". Vous devez activer S3 Object Lock lors de la création du compartiment. Vous ne pouvez pas ajouter ni désactiver S3 Object Lock après la création d'un compartiment. S3 Object Lock nécessite le versionnage du compartiment, qui est activé automatiquement lors de la création du compartiment.
DeleteBucket	Supprime le compartiment.
DeleteBucketCors	Supprime la configuration CORS du compartiment.
DeleteBucketEncryption	Supprime le chiffrement par défaut du compartiment. Les objets chiffrés existants restent chiffrés, mais les nouveaux objets ajoutés au compartiment ne sont pas chiffrés.
DeleteBucketLifecycle	Supprime la configuration du cycle de vie du compartiment. Voir "Créer une configuration de cycle de vie S3" .

Opération	Mise en œuvre
DeleteBucketPolicy	Supprime la stratégie associée au compartiment.
DeleteBucketReplication	Supprime la configuration de réplication associée au compartiment.
DeleteBucketTagging	Utilise la sous-ressource <code>tagging</code> pour supprimer toutes les balises d'un compartiment. Attention : Si une balise de règle de configuration ILM non par défaut est définie pour ce compartiment, il y aura une balise <code>NTAP-SG-ILM-BUCKET-TAG</code> de compartiment avec une valeur qui lui est attribuée. N'émettez pas de requête <code>DeleteBucketTagging</code> s'il existe une balise <code>NTAP-SG-ILM-BUCKET-TAG</code> de compartiment. Émettez plutôt une requête <code>PutBucketTagging</code> contenant uniquement la balise <code>NTAP-SG-ILM-BUCKET-TAG</code> et sa valeur attribuée afin de supprimer toutes les autres balises du compartiment. Ne modifiez ni ne supprimez la balise <code>NTAP-SG-ILM-BUCKET-TAG</code> de compartiment.
GetBucketAcl	Renvoie une réponse positive ainsi que l'ID, <code>DisplayName</code> et la permission du propriétaire du compartiment, indiquant que ce dernier dispose d'un accès complet au compartiment.
GetBucketCors	Renvoie la `cors` configuration du compartiment.
GetBucketEncryption	Renvoie la configuration de chiffrement par défaut du compartiment.
GetBucketLifecycleConfiguration (anciennement nommé GET Bucket lifecycle)	Renvoie la configuration du cycle de vie du compartiment. Voir " Créer une configuration de cycle de vie S3 ".
GetBucketLocation	Renvoie la région qui a été définie à l'aide de l'élément <code>LocationConstraint</code> dans la requête <code>CreateBucket</code> . Si la région du compartiment est <code>us-east-1</code> , une chaîne vide est renvoyée pour la région.
GetBucketNotificationConfiguration (anciennement nommé GET Bucket notification)	Renvoie la configuration de notification associée au compartiment.
GetBucketPolicy	Renvoie la règle de configuration associée au compartiment.
GetBucketReplication	Renvoie la configuration de réplication associée au compartiment.

Opération	Mise en œuvre
GetBucketTagging	Utilise la <code>tagging</code> sous-ressource pour renvoyer toutes les balises d'un compartiment. Attention : Si une étiquette de règle ILM non par défaut est définie pour ce compartiment, il y aura une étiquette de compartiment <code>NTAP-SG-ILM-BUCKET-TAG</code> avec une valeur qui lui est attribuée. Ne modifiez ni ne supprimez cette étiquette.
GetBucketVersioning	Cette implémentation utilise la <code>versioning</code> sous-ressource pour renvoyer l'état de versionnage d'un compartiment. • <i>blank</i>: Le versionnage n'a jamais été activé (bucket est "Non versionné") • Activé : Le versionnage est activé • Suspendu : le versionnage était précédemment activé et est suspendu
GetObjectLockConfiguration	Renvoie le mode de rétention par défaut et la période de rétention par défaut du compartiment, si configurés. Voir "Utilisez l'API REST S3 pour configurer S3 Object Lock".
HeadBucket	Détermine si un compartiment existe et si vous avez l'autorisation d'y accéder. Cette opération renvoie : • <code>x-ntap-sg-bucket-id</code>: L'UUID du compartiment au format UUID. • <code>x-ntap-sg-trace-id</code> : L'identifiant de suivi unique de la requête associée.

Opération	Mise en œuvre
ListObjects et ListObjectsV2 (anciennement nommé GET Bucket)	Renvoie tout ou partie (jusqu'à 1 000) des objets d'un compartiment. La classe de stockage des objets peut prendre l'une ou l'autre de deux valeurs, même si l'objet a été ingéré avec l'option de classe de stockage <code>REDUCED_REDUNDANCY</code> : • <code>STANDARD</code>, ce qui indique que l'objet est stocké dans un pool de stockage composé de Storage Nodes. • <code>GLACIER</code>, ce qui indique que l'objet a été déplacé vers le compartiment externe spécifié par le Cloud Storage Pool. Si le compartiment contient un grand nombre de clés supprimées ayant le même préfixe, la réponse peut inclure certaines <code>CommonPrefixes</code> qui ne contiennent pas de clés. Pour les requêtes <code>HeadObject</code> et <code>ListObject</code>, StorageGRID renvoie les horodatages <code>LastModified</code> avec une précision différente, tandis qu'AWS renvoie les horodatages avec la même précision, comme le montrent les exemples suivants : • StorageGRID <code>HeadObject</code>: "LastModified": "2024-09-26T16:43:24+00:00" • StorageGRID <code>ListObject</code> : « LastModified » : « 2024-09-26T16:43:24.931000+00:00 » • AWS <code>HeadObject</code>: "LastModified": "2023-10-17T00:19:54+00:00" • AWS <code>ListObject</code>: "LastModified": "2023-10-17T00:19:54+00:00"
ListObjectVersions (anciennement nommé GET Bucket Object versions)	Avec un accès en lecture sur un compartiment, l'utilisation de cette opération avec la <code>versions</code> sous-ressource répertorie les métadonnées de toutes les versions des objets dans le compartiment.
PutBucketCors	Définit la configuration CORS d'un compartiment afin que celui-ci puisse traiter des requêtes inter-origines. Le partage de ressources inter-origines (CORS) est un mécanisme de sécurité qui permet aux applications web clientes d'un domaine d'accéder aux ressources d'un domaine différent. Par exemple, supposons que vous utilisiez un compartiment S3 nommé <code>images</code> pour stocker des graphiques. En définissant la configuration CORS pour le compartiment <code>images</code>, vous pouvez autoriser l'affichage des images de ce compartiment sur le site web <code>http://www.example.com</code>.

Opération	Mise en œuvre
PutBucketEncryption	Définit l'état de chiffrement par défaut d'un compartiment existant. Lorsque le chiffrement au niveau du compartiment est activé, tout nouvel objet ajouté au compartiment est chiffré. StorageGRID prend en charge le chiffrement côté serveur avec des clés gérées par StorageGRID. Lors de la spécification de la règle de configuration du chiffrement côté serveur, définissez le paramètre <code>SSEAlgorithm</code> sur <code>AES256</code>, et n'utilisez pas le paramètre <code>KMSMasterKeyID</code>. La configuration de chiffrement par défaut du compartiment est ignorée si la requête de téléchargement d'objet spécifie déjà un chiffrement (c'est-à-dire si la requête inclut l'`x-amz-server-side-encryption-` en-tête de requête).
PutBucketLifecycleConfiguration (anciennement nommé PUT Bucket lifecycle)	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 règle de configuration. Chaque règle peut inclure les éléments XML suivants : • Expiration (Jours, Date, ExpiredObjectDeleteMarker) • NoncurrentVersionExpiration (NewerNoncurrentVersions, NoncurrentDays) • Filtrer (Préfixe, Tag) • Statut • ID StorageGRID ne prend pas en charge ces actions : • AbortIncompleteMultipartUpload • Transition Voir "Créer une configuration de cycle de vie S3". Pour comprendre comment l'action d'expiration dans un cycle de vie de compartiment interagit avec les instructions de placement ILM, voir "Comment l'ILM fonctionne tout au long du cycle de vie d'un objet". Remarque : La configuration du cycle de vie des compartiments peut être utilisée avec les compartiments dont le S3 Object Lock est activé, mais la configuration du cycle de vie des compartiments n'est pas prise en charge pour les anciens compartiments Compliant.

Opération	Mise en œuvre
PutBucketNotificationConfiguration (anciennement nommé PUT Bucket notification)	Configure les notifications pour le compartiment à l'aide du fichier XML de configuration des notifications inclus dans le corps de la requête. Veuillez prendre en compte les détails d'implémentation suivants : • StorageGRID prend en charge les sujets Amazon Simple Notification Service (Amazon SNS), les sujets Kafka ou les points de terminaison webhook comme destinations. Les points de terminaison Simple Queue Service (SQS) ou AWS Lambda ne sont pas pris en charge. • La destination des notifications doit être spécifiée comme l'URN d'un point de terminaison StorageGRID. Les points de terminaison peuvent être créés à l'aide du Tenant Manager ou de l'API Tenant Management. Le point de terminaison doit exister pour que la configuration des notifications réussisse. Si le point de terminaison n'existe pas, une 400 Bad Request erreur est renvoyée avec le code <code>InvalidArgument</code>. • Il est impossible de configurer une notification pour les types d'événements suivants. Ces types d'événements ne sont pas pris en charge. ◦ <code>s3:ReducedRedundancyLostObject</code> ◦ <code>s3:ObjectRestore:Completed</code> • Les notifications d'événements envoyées par StorageGRID utilisent le format JSON standard, à l'exception de certaines clés qui ne sont pas incluses et d'autres qui utilisent des valeurs spécifiques, comme indiqué dans la liste suivante : ◦ eventSource <code>sgws:s3</code> ◦ awsRegion non inclus ◦ x-amz-id-2 non inclus ◦ arn <code>urn:sgws:s3:::bucket_name</code>
PutBucketPolicy	Définit la politique associée au compartiment. Voir "Utilisez les stratégies d'accès aux compartiments et aux groupes" .

Opération	Mise en œuvre
PutBucketReplication	Configure "Réplication CloudMirror StorageGRID" pour le compartiment à l'aide du fichier XML de configuration de réplication fourni dans le corps de la requête. Pour la réplication CloudMirror, veuillez prendre en compte les détails d'implémentation suivants : • StorageGRID ne prend en charge que la version 1 de la configuration de réplication. Cela signifie que StorageGRID ne prend pas en charge l'utilisation de l'élément <code>Filter</code> pour les règles et suit les conventions de la version 1 pour la suppression des versions d'objets. Pour plus de détails, consultez "Guide de l'utilisateur Amazon Simple Storage Service : configuration de la réplication". • La réplication des compartiments peut être configurée sur des compartiments versionnés ou non versionnés. • Vous pouvez spécifier un compartiment de destination différent dans chaque règle du fichier XML de configuration de réplication. Un compartiment source peut répliquer vers plusieurs compartiments de destination. • Les compartiments de destination doivent être spécifiés comme l'URN des points de terminaison StorageGRID, tels que définis dans le Tenant Manager ou l'API Tenant Management. Voir "Configurer la réplication CloudMirror". Le point de terminaison doit exister pour que la configuration de la réplication réussisse. Si le point de terminaison n'existe pas, la requête échoue en tant que 400 Bad Request. Le message d'erreur indique : <code>Unable to save the replication policy. The specified endpoint URN does not exist: URN.</code> • Il n'est pas nécessaire de spécifier un <code>Role</code> dans le fichier XML de configuration. Cette valeur n'est pas utilisée par StorageGRID et sera ignorée si elle est soumise. • Si vous omettez la classe de stockage dans le fichier XML de configuration, StorageGRID utilise la classe de stockage <code>STANDARD</code> par défaut. • Si vous supprimez un objet du compartiment source ou si vous supprimez le compartiment source lui-même, le comportement de la réplication interrégionale est le suivant : ◦ Si vous supprimez l'objet ou le compartiment avant qu'il n'ait été répliqué, l'objet/compartiment n'est pas répliqué et vous n'êtes pas notifié. ◦ Si vous supprimez l'objet ou le compartiment après sa réplication, StorageGRID suit le comportement de suppression standard d'Amazon S3 pour la version 1 de la réplication interrégionale.

Opération	Mise en œuvre
PutBucketTagging	Utilise la <code>tagging</code> sous-ressource pour ajouter ou mettre à jour un ensemble d'étiquettes pour un compartiment. Lors de l'ajout d'étiquettes de compartiment, tenez compte des limitations suivantes : • StorageGRID et Amazon S3 prennent tous deux en charge jusqu'à 50 balises par compartiment. • Les étiquettes associées à un compartiment doivent avoir des clés d'étiquette uniques. Une clé d'étiquette peut comporter jusqu'à 128 caractères Unicode. • Les valeurs des balises peuvent comporter jusqu'à 256 caractères Unicode. • Les clés et les valeurs sont sensibles à la casse. Attention : Si une balise de stratégie ILM non standard est définie pour ce compartiment, il y aura une balise <code>NTAP-SG-ILM-BUCKET-TAG</code> de compartiment avec une valeur qui lui est attribuée. Assurez-vous que la balise <code>NTAP-SG-ILM-BUCKET-TAG</code> de compartiment est incluse avec la valeur attribuée dans toutes les requêtes PutBucketTagging. Ne modifiez ni ne supprimez cette balise. Remarque : Cette opération écrasera toutes les étiquettes existantes du compartiment. Si des étiquettes existantes sont omises de l'ensemble, ces étiquettes seront supprimées du compartiment.
PutBucketVersioning	Utilise la <code>versioning</code> sous-ressource pour définir l'état de versionnage d'un compartiment existant. Vous pouvez définir l'état de versionnage avec l'une des valeurs suivantes : • Activé : active le versionnage des objets du compartiment. Tous les objets ajoutés au compartiment reçoivent un identifiant de version unique. • Suspendu : désactive le versionnage des objets du compartiment. Tous les objets ajoutés au compartiment reçoivent l'ID de version <code>null</code>.
PutObjectLockConfiguration	Configure ou supprime le mode de rétention par défaut et la période de rétention par défaut du compartiment. Si la période de conservation par défaut est modifiée, la date limite de conservation des versions d'objets existantes reste la même et n'est pas recalculée en fonction de la nouvelle période de conservation par défaut. Voir "Utilisez l'API REST S3 pour configurer S3 Object Lock" pour plus d'informations.

Opérations sur les objets

Comment StorageGRID implémente les opérations de l'API REST S3 pour les objets

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

Les conditions suivantes s'appliquent à toutes les opérations sur les objets :

- StorageGRID "**valeurs de cohérence**" est pris en charge par toutes les opérations sur les objets, à l'exception des suivantes :
 - GetObjectAcl
 - OPTIONS /
 - PutObjectLegalHold
 - PutObjectRetention
 - SelectObjectContent
- Les requêtes clients conflictuelles, comme par exemple deux clients écrivant sur la même clé, sont résolues selon le principe du « latest-wins ». Le moment de l'évaluation du « latest-wins » est déterminé par la date à laquelle le système StorageGRID termine une requête donnée, et non par la date à laquelle les clients S3 commencent une opération.
- Tous les objets dans un StorageGRID bucket sont la propriété du propriétaire du bucket, y compris les objets créés par un utilisateur anonyme ou par un autre compte.

Le tableau suivant décrit comment StorageGRID implémente les opérations d'objet de l'API REST S3.

Opération	Mise en œuvre
DeleteObject	Lors du traitement d'une requête DeleteObject, StorageGRID tente de supprimer immédiatement toutes les copies de l'objet de tous les emplacements de stockage. En cas de succès, StorageGRID renvoie immédiatement une réponse au client. Si toutes les copies ne peuvent pas être supprimées dans un délai de 30 secondes (par exemple, si un emplacement est temporairement indisponible), StorageGRID met les copies en file d'attente pour suppression, puis indique la réussite de l'opération au client. Restrictions • L'authentification multifacteur (MFA) et l'en-tête de réponse <code>x-amz-mfa</code> ne sont pas pris en charge. • Les <code>If-None</code> et <code>If-None-Match</code> en-têtes sont acceptés mais non fonctionnels. Versionnage Pour supprimer une version spécifique, le demandeur doit être le propriétaire du compartiment et utiliser la sous-ressource <code>versionId</code>. L'utilisation de cette sous-ressource supprime définitivement la version. Si la <code>versionId</code> correspond à un marqueur de suppression, l'en-tête de réponse <code>x-amz-delete-marker</code> est renvoyé avec la valeur <code>true</code>. • Si un objet est supprimé sans la <code>versionId</code> sous-ressource sur un compartiment avec le versionnage activé, cela entraîne la génération d'un marqueur de suppression. L'<code>versionId</code> du marqueur de suppression est renvoyé via l'en-tête de réponse <code>x-amz-version-id</code>, et l'en-tête de réponse <code>x-amz-delete-marker</code> est renvoyé avec la valeur <code>true</code>. • Si un objet est supprimé sans la <code>versionId</code> sous-ressource sur un compartiment dont le versionnage est suspendu, cela entraîne la suppression définitive d'une version « null » existante ou d'un marqueur de suppression « null », ainsi que la génération d'un nouveau marqueur de suppression « null ». L'en-tête de réponse <code>x-amz-delete-marker</code> est renvoyé avec la valeur <code>true</code>. Remarque : Dans certains cas, plusieurs marqueurs de suppression peuvent exister pour un objet. Consultez "Utilisez l'API REST S3 pour configurer S3 Object Lock" pour savoir comment supprimer les versions d'objets en mode GOUVERNANCE.

Opération	Mise en œuvre
DeleteObjects (anciennement nommé DELETE Multiple Objects)	L'authentification multifacteur (MFA) et l'en-tête de réponse <code>x-amz-mfa</code> ne sont pas pris en charge. Plusieurs objets peuvent être supprimés dans le même message de requête. Consultez "Utilisez l'API REST S3 pour configurer S3 Object Lock" pour savoir comment supprimer les versions d'objets en mode GOUVERNANCE.
DeleteObjectTagging	Utilise la <code>tagging</code> sous-ressource pour supprimer toutes les balises d'un objet. Versionnage Si le <code>versionId</code> paramètre de requête n'est pas spécifié dans la requête, l'opération supprime toutes les balises de la version la plus récente de l'objet dans un compartiment versionné. Si la version actuelle de l'objet est un marqueur de suppression, un statut <code>"MethodNotAllowed"</code> est renvoyé avec l' <code>x-amz-delete-marker</code> en-tête de réponse défini sur <code>true</code>.
GetObject	"GetObject"
GetObjectAcl	Si les informations d'identification nécessaires sont fournies pour le compte, l'opération renvoie une réponse positive ainsi que l'ID, <code>DisplayName</code> et l'autorisation du propriétaire de l'objet, indiquant que ce dernier dispose d'un accès complet à l'objet.
GetObjectLegalHold	"Utilisez l'API REST S3 pour configurer S3 Object Lock"
GetObjectRetention	"Utilisez l'API REST S3 pour configurer S3 Object Lock"
GetObjectTagging	Utilise la <code>tagging</code> sous-ressource pour renvoyer toutes les balises d'un objet. Versionnage Si le <code>versionId</code> paramètre de requête n'est pas spécifié dans la requête, l'opération renvoie toutes les balises de la version la plus récente de l'objet dans un compartiment versionné. Si la version actuelle de l'objet est un marqueur de suppression, un statut <code>"MethodNotAllowed"</code> est renvoyé avec l' <code>x-amz-delete-marker</code> en-tête de réponse défini sur <code>true</code>.
HeadObject	"HeadObject"
RestoreObject	"RestoreObject"

Opération	Mise en œuvre
PutObject	"PutObject"
CopyObject (anciennement nommé PUT Object - Copy)	"CopyObject"
PutObjectLegalHold	"Utilisez l'API REST S3 pour configurer S3 Object Lock"
PutObjectRetention	"Utilisez l'API REST S3 pour configurer S3 Object Lock"

Opération	Mise en œuvre
PutObjectTagging	Utilise la <code>tagging</code> sous-ressource pour ajouter un ensemble de balises à un objet existant. Limites des balises d'objet Vous pouvez ajouter des balises aux nouveaux objets lors de leur chargement, ou vous pouvez les ajouter à des objets existants. StorageGRID et Amazon S3 prennent en charge jusqu'à 10 balises par objet. Les balises associées à un objet doivent avoir des clés de balise uniques. Une clé de balise peut comporter jusqu'à 128 caractères Unicode et les valeurs de balise peuvent comporter jusqu'à 256 caractères Unicode. Les clés et les valeurs sont sensibles à la casse. Mises à jour des balises et comportement d'ingestion Lorsque vous utilisez PutObjectTagging pour mettre à jour les balises d'un objet, StorageGRID ne réingère pas l'objet. Cela signifie que l'option de comportement d'ingestion spécifiée dans la règle ILM correspondante n'est pas utilisée. Toute modification du placement de l'objet déclenchée par la mise à jour est effectuée lorsque l'ILM est réévalué par les processus ILM d'arrière-plan habituels. Cela signifie que si la règle ILM utilise l'option Strict pour le comportement d'ingestion, aucune action n'est entreprise si les emplacements d'objets requis ne peuvent pas être effectués (par exemple, parce qu'un emplacement nouvellement requis est indisponible). L'objet mis à jour conserve son emplacement actuel jusqu'à ce que l'emplacement requis soit possible. Résolution des conflits Les requêtes clients conflictuelles, comme par exemple deux clients écrivant sur la même clé, sont résolues selon le principe du « latest-wins ». Le moment de l'évaluation du « latest-wins » est déterminé par la date à laquelle le système StorageGRID termine une requête donnée, et non par la date à laquelle les clients S3 commencent une opération. Versionnage Si le <code>versionId</code> 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 statut "MethodNotAllowed" est renvoyé avec l' <code>x-amz-delete-marker</code> en-tête de réponse défini sur <code>true</code>.
SelectObjectContent	"SelectObjectContent"

Opérations Amazon S3 Select prises en charge dans StorageGRID

StorageGRID prend en charge les clauses, les types de données et les opérateurs Amazon S3 Select suivants pour le "commande `SelectObjectContent`".



Les articles non répertoriés ne sont pas pris en charge.

Pour la syntaxe, consultez ["SelectObjectContent"](#). Pour plus d'informations sur S3 Select, consultez le ["Documentation AWS pour S3 Select"](#).

Seuls les comptes locataires pour lesquels S3 Select est activé peuvent émettre des requêtes SelectObjectContent. Consultez ["Considérations et exigences relatives à l'utilisation de S3 Select"](#).

`${post_edited_translations.segment}`

- `${post_edited_translations.segment}`
- `${post_edited_translations.segment}`
- clause WHERE
- `${post_edited_translations.segment}`

`${post_edited_translations.segment}`

- bool
- `${post_edited_translations.segment}`
- chaîne
- flottant
- `${post_edited_translations.segment}`
- horodatage

`${post_edited_translations.segment}`

`${post_edited_translations.segment}`

- ET
- PAS
- `${post_edited_translations.segment}`

Opérateurs de comparaison

- <
- >
- <=
- `${post_edited_translations.segment}`
- =
- =
- <>
- !=
- `${post_edited_translations.segment}`
- DANS

`${post_edited_translations.segment}`

- `${post_edited_translations.segment}`
- `${post_edited_translations.segment}`
- `${post_edited_translations.segment}`

Opérateurs unitaires

- IS NULL
- `${post_edited_translations.segment}`

`${post_edited_translations.segment}`

- +
- -
- *
- /
- `${post_edited_translations.segment}`

`${post_edited_translations.segment}`

`${post_edited_translations.segment}`

- `${post_edited_translations.segment}`
- COUNT(*)
- `${post_edited_translations.segment}`
- `${post_edited_translations.segment}`
- `${post_edited_translations.segment}`

`${post_edited_translations.segment}`

- `${post_edited_translations.segment}`
- `${post_edited_translations.segment}`
- `${post_edited_translations.segment}`

`${post_edited_translations.segment}`

- `${post_edited_translations.segment}`

Fonctions de date

- `${post_edited_translations.segment}`
- DATE_DIFF
- EXTRAIT
- `${post_edited_translations.segment}`
- `${post_edited_translations.segment}`

- `${post_edited_translations.segment}`

Fonctions de chaînes de caractères

- `CHAR_LENGTH`, `CHARACTER_LENGTH`
- `INFÉRIEUR`
- `${post_edited_translations.segment}`
- `TRIM`
- `${post_edited_translations.segment}`

Comment StorageGRID utilise le chiffrement côté serveur

Le chiffrement côté serveur vous permet de protéger vos données au repos. StorageGRID chiffre les données lors de l'écriture de l'objet et les déchiffre lorsque vous y accédez.

Si vous souhaitez utiliser le chiffrement côté serveur, vous pouvez choisir l'une des deux options mutuellement exclusives, selon la manière dont les clés de chiffrement sont gérées :

- **SSE (chiffrement côté serveur avec des clés gérées par StorageGRID)** : Lorsque vous effectuez une requête S3 pour stocker un objet, StorageGRID chiffre cet objet à l'aide d'une clé unique. Lorsque vous effectuez une requête S3 pour récupérer l'objet, StorageGRID utilise la clé stockée pour le déchiffrer.
- **SSE-C (chiffrement côté serveur avec clés fournies par le client)** : Lorsque vous envoyez une requête 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 votre requête. Si les deux clés de chiffrement correspondent, l'objet est déchiffré et vos données d'objet sont renvoyées.

Bien que StorageGRID gère toutes les opérations de chiffrement et de déchiffrement des objets, vous devez gérer les clés de chiffrement 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 compartiment ou de la grille sont ignorés.

Utilisez SSE

Pour chiffrer un objet avec une clé unique gérée par StorageGRID, vous utilisez l'en-tête de requête suivant :

`x-amz-server-side-encryption`

`${post_edited_translations.segment}`

- `"PutObject"`
- `"CopyObject"`
- `"CreateMultipartUpload"`

Utilisez SSE-C

`${post_edited_translations.segment}`

En-tête de requête	Description
<code>x-amz-server-side-encryption-customer-algorithm</code>	Spécifiez l'algorithme de chiffrement. La valeur de l'en-tête doit être AES256.
<code>x-amz-server-side-encryption-customer-key</code>	Spécifiez la clé de chiffrement qui sera utilisée pour chiffrer ou déchiffrer l'objet. La valeur de la clé doit être de 256 bits, encodée en base64.
<code>x-amz-server-side-encryption-customer-key-MD5</code>	Spécifiez le condensé MD5 de la clé de chiffrement conformément à la norme RFC 1321, qui est utilisé pour s'assurer que la clé de chiffrement a été transmise sans erreur. La valeur du condensé MD5 doit être encodée en base64 sur 128 bits.

`${post_edited_translations.segment}`

- ["GetObject"](#)
- ["HeadObject"](#)
- ["PutObject"](#)
- ["CopyObject"](#)
- ["CreateMultipartUpload"](#)
- ["UploadPart"](#)
- ["UploadPartCopy"](#)

Considérations relatives à l'utilisation du chiffrement côté serveur avec des clés fournies par le client (SSE-C)

Avant d'utiliser SSE-C, veuillez prendre en compte les points suivants :

- `${post_edited_translations.segment}`



StorageGRID rejette toutes les requêtes effectuées via http lors de l'utilisation de SSE-C. Pour des raisons de sécurité, vous devez considérer comme compromise toute clé que vous auriez envoyée accidentellement via http. Mettez la clé au rebut et procédez à sa rotation selon les besoins.

- L'ETag dans la réponse n'est pas le MD5 des données de l'objet.
- Vous devez gérer le mappage des clés de chiffrement aux objets. StorageGRID ne stocke pas les clés de chiffrement. Vous êtes responsable du suivi de la clé de chiffrement que vous fournissez pour chaque objet.
- Si le versionnement est activé pour votre compartiment, 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.
- Étant donné que vous gérez les clés de chiffrement côté client, vous devez également gérer toutes les

mesures de sécurité supplémentaires, telles que la rotation des clés, côté client.



Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant.

- Si la réplication inter-grilles ou la réplication CloudMirror est configurée pour le compartiment, vous ne pouvez pas ingérer d'objets SSE-C. L'opération d'ingestion échouera.

Informations connexes

["\\${post_edited_translations.segment}"](#)

Créer une copie d'un objet dans StorageGRID avec la requête S3 CopyObject

Vous pouvez utiliser la requête S3 CopyObject pour créer une copie d'un objet déjà stocké dans S3. Une opération CopyObject équivaut à effectuer GetObject suivi de PutObject.

Résoudre les conflits

Les requêtes clients conflictuelles, comme par exemple deux clients écrivant sur la même clé, sont résolues selon le principe du « latest-wins ». Le moment de l'évaluation du « latest-wins » est déterminé par la date à laquelle le système StorageGRID termine une requête donnée, et non par la date à laquelle les clients S3 commencent une opération.

Taille de l'objet

La taille maximale *recommandée* pour une seule opération PutObject est de 5 Gio (5 368 709 120 octets). Si vous avez des objets de plus de 5 Gio, utilisez plutôt ["téléchargement en plusieurs parties"](#).

La taille maximale *prise en charge* pour une seule opération PutObject est de 5 Tio (5 497 558 138 880 octets).



Si vous avez effectué une mise à niveau depuis StorageGRID 11.6 ou une version antérieure, l'alerte « Taille de l'objet S3 trop volumineux lors de la commande PUT » sera déclenchée si vous tentez de télécharger un objet dépassant 5 Gio. Si vous disposez d'une nouvelle installation de StorageGRID 11.7 ou 11.8, l'alerte ne sera pas déclenchée dans ce cas. Cependant, afin de s'aligner sur la norme AWS S3, les prochaines versions de StorageGRID ne prendront plus en charge le téléchargement d'objets de plus de 5 Gio.

Caractères UTF-8 dans les métadonnées utilisateur

Si une requête inclut des valeurs UTF-8 (non échappées) dans le nom de clé ou la valeur des métadonnées définies par l'utilisateur, le comportement de StorageGRID est indéfini.

StorageGRID n'analyse ni n'interprète les caractères UTF-8 échappés inclus dans le nom ou la valeur de la clé des métadonnées définies par l'utilisateur. Les caractères UTF-8 échappés sont traités comme des caractères ASCII :

- Les requêtes aboutissent si les métadonnées définies par l'utilisateur incluent des caractères UTF-8 échappés.
- StorageGRID ne renvoie pas l'`x-amz-missing-meta` en-tête si la valeur interprétée du nom ou de la valeur de la clé contient des caractères non imprimables.

En-têtes de requête 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, ce qui vous permet de copier l'objet et les métadonnées associées.

Vous pouvez spécifier REPLACE pour écraser les métadonnées existantes lors de la copie de l'objet, ou pour mettre à jour les métadonnées de l'objet.

- x-amz-storage-class
- x-amz-tagging-directive : La valeur par défaut est COPY, ce qui vous permet de copier l'objet et toutes ses balises.

Vous pouvez spécifier REPLACE d'écraser les balises existantes lors de la copie de l'objet, ou de mettre à jour les balises.

- En-têtes de requête S3 Object Lock :
 - x-amz-object-lock-mode
 - x-amz-object-lock-retain-until-date
 - x-amz-object-lock-legal-hold

Si une requête est effectuée sans ces en-têtes, les paramètres de rétention par défaut du compartiment sont utilisés pour calculer le mode de version de l'objet et la date de rétention jusqu'à la date limite. Voir ["Utilisez l'API REST S3 pour configurer S3 Object Lock"](#).

- En-têtes de requête SSE :
 - x-amz-copy-source-server-side-encryption-customer-algorithm
 - x-amz-copy-source-server-side-encryption-customer-key
 - x-amz-copy-source-server-side-encryption-customer-key-MD5
 - x-amz-server-side-encryption
 - x-amz-server-side-encryption-customer-key-MD5
 - x-amz-server-side-encryption-customer-key
 - x-amz-server-side-encryption-customer-algorithm

Voir [En-têtes de requête pour le chiffrement 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
- If-Match

Le If-Match header est accepté mais non fonctionnel.

- If-None-Match

Le If-None-Match header est accepté mais non fonctionnel.

- x-amz-checksum-algorithm

Lors de la copie d'un objet, si l'objet source possède une somme de contrôle, StorageGRID ne copie pas cette valeur de somme de contrôle dans le nouvel objet. Ce comportement s'applique que vous tentiez ou non d'utiliser x-amz-checksum-algorithm dans la requête d'objet.

- x-amz-website-redirect-location

Options de classe de stockage

L'`x-amz-storage-class`en-tête de requête est pris en charge et influe sur le nombre de copies d'objets que StorageGRID crée si la règle ILM correspondante utilise la validation double ou équilibrée ["option d'ingestion"](#).

- STANDARD

(Par défaut) Spécifie une opération d'ingestion à double validation lorsque la règle ILM utilise l'option Dual commit, ou lorsque l'option Balanced revient à créer des copies intermédiaires.

- REDUCED_REDUNDANCY

Spécifie une opération d'ingestion à validation unique lorsque la règle ILM utilise l'option de double validation, ou lorsque l'option équilibrée revient à créer des copies intermédiaires.



Si vous ingérez un objet dans un compartiment avec S3 Object Lock activé, l'`REDUCED\_REDUNDANCY`option est ignorée. Si vous ingérez un objet dans un compartiment Compliant hérité, l'`REDUCED\_REDUNDANCY`option renvoie une erreur. StorageGRID effectuera toujours une double validation à l'ingestion pour garantir le respect des exigences de conformité.

Utilisation de x-amz-copy-source dans CopyObject

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

destination.

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

- Vous ne pouvez pas utiliser `CopyObject` pour chiffrer un objet existant sur place, ni pour modifier le chiffrement d'un objet existant sur place. Si vous fournissez l'`x-amz-server-side-encryption` en-tête ou l'`x-amz-server-side-encryption-customer-algorithm` en-tête, StorageGRID rejette la requête et renvoie `XNotImplemented`.
- L'option de comportement d'ingestion spécifiée dans la règle ILM correspondante n'est pas utilisée. Toute modification du placement des objets déclenchée par la mise à jour est effectuée lorsque l'ILM est réévalué par les processus ILM d'arrière-plan normaux.

Cela signifie que si la règle ILM utilise l'option `Strict` pour le comportement d'ingestion, aucune action n'est entreprise si les emplacements d'objets requis ne peuvent pas être effectués (par exemple, parce qu'un emplacement nouvellement requis est indisponible). L'objet mis à jour conserve son emplacement actuel jusqu'à ce que l'emplacement requis soit possible.

En-têtes de requête pour le chiffrement côté serveur

Si vous "[utiliser le chiffrement côté serveur](#)", les en-têtes de requête que vous fournissez dépendent du chiffrement de l'objet source et de votre intention de chiffrer l'objet cible.

- Si l'objet source est chiffré à l'aide d'une clé fournie par le client (SSE-C), vous devez inclure les trois en-têtes suivants dans la requête `CopyObject`, afin que l'objet puisse être déchiffré puis copié :
 - `x-amz-copy-source-server-side-encryption-customer-algorithm`: Précisez `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 condensé 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`: Précisez `AES256`.
 - `x-amz-server-side-encryption-customer-key`: Spécifiez une nouvelle clé de chiffrement pour l'objet cible.
 - `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le condensé MD5 de la nouvelle clé de chiffrement.



Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant. Avant d'utiliser des clés fournies par le client pour sécuriser les données d'objet, examinez les considérations pour "[utilisation du chiffrement 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 requête `CopyObject` :
 - `x-amz-server-side-encryption`



La `server-side-encryption` valeur de l'objet ne peut pas être mise à jour. Créez plutôt une copie avec une nouvelle `server-side-encryption` valeur en utilisant `x-amz-metadata-directive: REPLACE`.

Versionnage

Si le compartiment source est versionné, vous pouvez utiliser l'en-tête `x-amz-copy-source` pour copier la dernière version d'un objet. Pour copier une version spécifique d'un objet, vous devez spécifier explicitement la version à copier à l'aide de la sous-ressource `versionId`. Si le compartiment de destination est versionné, la version générée est renvoyée dans l'en-tête de réponse `x-amz-version-id`. Si le versionnement est suspendu pour le compartiment cible, alors `x-amz-version-id` renvoie une valeur "null".

Récupérer un objet depuis un bucket dans StorageGRID avec la requête `GetObject`

Vous pouvez utiliser la requête S3 `GetObject` pour récupérer un objet depuis un compartiment S3.

`GetObject` et objets multipart

Vous pouvez utiliser le `partNumber` paramètre de requête pour récupérer une partie spécifique d'un objet multipart ou segmenté. L'élément de réponse `x-amz-mp-parts-count` indique combien de parties l'objet possède.

Vous pouvez définir `partNumber` à 1 pour les objets segmentés/multipart et les objets non segmentés/non multipart ; cependant, l'élément de réponse `x-amz-mp-parts-count` n'est renvoyé que pour les objets segmentés ou multipart.

Caractères UTF-8 dans les métadonnées utilisateur

StorageGRID n'analyse ni n'interprète les caractères UTF-8 échappés dans les métadonnées définies par l'utilisateur. Les requêtes GET concernant un objet dont les métadonnées définies par l'utilisateur contiennent des caractères UTF-8 échappés ne renvoient pas l'élément de réponse `x-amz-missing-meta` si le nom ou la valeur de la clé inclut des caractères non imprimables.

En-tête de requête pris en charge

L'en-tête de requête suivant est pris en charge :

- `x-amz-checksum-mode`: Spécifiez `ENABLED`

L'élément de réponse `Range` n'est pas pris en charge avec `x-amz-checksum-mode` pour `GetObject`. Lorsque vous incluez `Range` dans la requête avec `x-amz-checksum-mode` activé, StorageGRID ne renvoie pas de valeur de somme de contrôle dans la réponse.

En-tête de requête non pris en charge

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

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

Versionnage

Si aucune `versionId` sous-ressource n'est spécifiée, l'opération récupère 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 statut « Not Found » est renvoyé avec l' `x-amz-delete-marker` en-tête de réponse défini sur `true`.

En-têtes de requête pour le chiffrement côté serveur avec des 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`: Précisez AES256.
- `x-amz-server-side-encryption-customer-key`: Spécifiez votre clé de chiffrement pour l'objet.
- `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le condensé MD5 de la clé de chiffrement de l'objet.



Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant. Avant d'utiliser des clés fournies par le client pour sécuriser les données d'objet, examinez les considérations dans ["Utilisez le chiffrement côté serveur"](#).

Comportement de `GetObject` pour les objets Cloud Storage Pool

Si un objet a été stocké dans un ["Pool de stockage cloud"](#), le comportement d'une requête `GetObject` dépend de l'état de l'objet. Voir ["HeadObject"](#) pour plus de détails.



Si un objet est stocké dans un Cloud Storage Pool et qu'une ou plusieurs copies de cet objet existent également sur la grille, les requêtes `GetObject` tenteront de récupérer les données à partir de la grille avant de les récupérer à partir du Cloud Storage Pool.

État de l'objet	Comportement de <code>GetObject</code>
Objet ingéré dans StorageGRID mais pas encore évalué par ILM, ou objet stocké dans un pool de stockage traditionnel ou utilisant le code d'effacement	200 OK Une copie de l'objet est récupérée.
Objet présent dans le pool de stockage cloud mais n'ayant pas encore été transféré dans un état non récupérable	200 OK Une copie de l'objet est récupérée.
L'objet est passé dans un état non récupérable	403 Forbidden, InvalidObjectState Utilisez une "RestoreObject" demande pour restaurer l'objet à un état récupérable.
Objet en cours de restauration à partir d'un état non récupérable	403 Forbidden, InvalidObjectState Attendez que la requête <code>RestoreObject</code> soit terminée.

État de l'objet	Comportement de GetObject
Objet entièrement restauré dans le Cloud Storage Pool	200 OK Une copie de l'objet est récupérée.

Objets multipartites ou segmentés dans un Cloud Storage Pool

Si vous avez importé un objet multipart ou si StorageGRID a divisé un objet volumineux en segments, StorageGRID détermine si l'objet est disponible dans le Cloud Storage Pool en échantillonnant un sous-ensemble des parties ou segments de l'objet. Dans certains cas, une requête GetObject peut renvoyer 200 OK de façon incorrecte lorsque certaines parties de l'objet ont déjà été transférées dans un état non récupérable ou lorsque certaines parties de l'objet n'ont pas encore été restaurées.

Dans ces cas :

- La requête GetObject peut renvoyer des données mais s'interrompre en cours de transfert.
- Une requête GetObject ultérieure pourrait renvoyer 403 Forbidden.

GetObject et réplication inter-grilles

Si vous utilisez "fédération de grid" et "réplication inter-grilles" est activé pour un compartiment, le client S3 peut vérifier l'état de réplication d'un objet en envoyant une requête GetObject. La réponse inclut l'en-tête de réponse spécifique à StorageGRID `x-ntap-sg-cgr-replication-status`, qui aura l'une des valeurs suivantes :

Grid	État de la réplication
Source	• TERMINÉ : La réplication a réussi. • EN ATTENTE : L'objet n'a pas encore été répliqué. • ÉCHEC : La réplication a échoué de manière permanente. Un utilisateur doit résoudre l'erreur.
Destination	REPLICA : L'objet a été répliqué à partir de la grille source.



StorageGRID ne prend pas en charge l'`x-amz-replication-status` en-tête.

Récupérer les métadonnées d'un objet dans StorageGRID avec la requête S3 HeadObject

Vous pouvez utiliser la requête S3 HeadObject pour récupérer les métadonnées d'un objet sans renvoyer l'objet lui-même. Si l'objet est stocké dans un Cloud Storage Pool, vous pouvez utiliser HeadObject pour déterminer l'état de transition de l'objet.

HeadObject et objets multipart

Vous pouvez utiliser le `partNumber` paramètre de requête pour récupérer les métadonnées d'une partie spécifique d'un objet multipart ou segmenté. L'`x-amz-mp-parts-count` élément de réponse indique combien de parties l'objet possède.

Vous pouvez définir `partNumber` à 1 pour les objets segmentés/multipart et les objets non segmentés/non multipart ; cependant, l'élément de réponse `x-amz-mp-parts-count` n'est renvoyé que pour les objets segmentés ou multipart.

Caractères UTF-8 dans les métadonnées utilisateur

StorageGRID n'analyse ni n'interprète les caractères UTF-8 échappés dans les métadonnées définies par l'utilisateur. Les requêtes HEAD concernant un objet dont les métadonnées définies par l'utilisateur contiennent des caractères UTF-8 échappés ne renvoient pas l'en-tête `x-amz-missing-meta` si le nom ou la valeur de la clé inclut des caractères non imprimables.

En-tête de requête pris en charge

L'en-tête de requête suivant est pris en charge :

- `x-amz-checksum-mode`

Le `partNumber` paramètre et `Range` l'en-tête ne sont pas pris en charge avec `x-amz-checksum-mode` pour `HeadObject`. Lorsque vous les incluez dans la requête avec `x-amz-checksum-mode` activé, StorageGRID ne renvoie pas de valeur de somme de contrôle dans la réponse.

En-tête de requête non pris en charge

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

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

Versionnage

Si aucune `versionId` sous-ressource n'est spécifiée, l'opération récupère 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 statut « Not Found » est renvoyé avec l' `x-amz-delete-marker` en-tête de réponse défini sur `true`.

En-têtes de requête pour le chiffrement côté serveur avec des clés de chiffrement fournies par le client (SSE-C)

Utilisez ces trois en-têtes si l'objet est chiffré avec une clé unique que vous avez fournie.

- `x-amz-server-side-encryption-customer-algorithm`: Précisez AES256.
- `x-amz-server-side-encryption-customer-key`: Spécifiez votre clé de chiffrement pour l'objet.
- `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le condensé MD5 de la clé de chiffrement de l'objet.



Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant. Avant d'utiliser des clés fournies par le client pour sécuriser les données d'objet, examinez les considérations dans ["Utilisez le chiffrement côté serveur"](#).

HeadObject réponses pour les objets Cloud Storage Pool

Si l'objet est stocké dans un ["Pool de stockage cloud"](#), les en-têtes de réponse suivants sont renvoyés :

- `x-amz-storage-class: GLACIER`
- `x-amz-restore`

Les en-têtes de réponse fournissent des informations sur l'état d'un objet lorsqu'il est déplacé vers un Cloud Storage Pool, éventuellement transféré vers un état non récupérable, puis restauré.

État de l'objet	Réponse à HeadObject
Objet ingéré dans StorageGRID mais pas encore évalué par ILM, ou objet stocké dans un pool de stockage traditionnel ou utilisant le code d'effacement	200 OK (Aucun en-tête de réponse spécial n'est renvoyé.)
Objet présent dans le pool de stockage cloud mais n'ayant pas encore été transféré dans un état non récupérable	200 OK <code>x-amz-storage-class: GLACIER</code> <code>x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"</code> Jusqu'à ce que l'objet soit passé à un état non récupérable, la valeur pour <code>expiry-date</code> est définie à une date lointaine dans le futur. L'heure exacte de la transition n'est pas contrôlée par le système StorageGRID.
L'objet est passé à un état non récupérable, mais au moins une copie existe également sur la grille	200 OK <code>x-amz-storage-class: GLACIER</code> <code>x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"</code> La valeur de <code>expiry-date</code> est fixée à une date future lointaine. Remarque : Si la copie sur la grille n'est pas disponible (par exemple, si un nœud de stockage est hors service), vous devez émettre une demande "RestoreObject" pour restaurer la copie à partir du Cloud Storage Pool avant de pouvoir récupérer l'objet.
L'objet est passé à un état irrécupérable et aucune copie n'existe sur la grille	200 OK <code>x-amz-storage-class: GLACIER</code>

État de l'objet	Réponse à HeadObject
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"
Objet entièrement restauré dans le Cloud Storage Pool	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 Cloud Storage Pool sera renvoyé à un état non récupérable.

Objets multipartites ou segmentés dans le Cloud Storage Pool

Si vous avez importé un objet multipart ou si StorageGRID a divisé un objet volumineux en segments, StorageGRID détermine si l'objet est disponible dans le Cloud Storage Pool en échantillonnant un sous-ensemble des parties ou segments de l'objet. Dans certains cas, une requête HeadObject peut renvoyer `x-amz-restore: ongoing-request="false"` de façon incorrecte lorsque certaines parties de l'objet ont déjà été transférées dans un état non récupérable ou lorsque certaines parties de l'objet n'ont pas encore été restaurées.

HeadObject et réplication inter-grilles

Si vous utilisez "fédération de grid" et "réplication inter-grilles" est activé pour un compartiment, le client S3 peut vérifier l'état de réplication d'un objet en envoyant une requête HeadObject. La réponse inclut l'en-tête de réponse spécifique à StorageGRID `x-ntap-sg-cgr-replication-status`, qui aura l'une des valeurs suivantes :

Grid	État de la réplication
Source	• TERMINÉ : La réplication a réussi. • EN ATTENTE : L'objet n'a pas encore été répliqué. • ÉCHEC : La réplication a échoué de manière permanente. Un utilisateur doit résoudre l'erreur.
Destination	REPLICA : L'objet a été répliqué à partir de la grille source.



StorageGRID ne prend pas en charge l'`x-amz-replication-status` en-tête.

Ajouter un objet à un compartiment dans StorageGRID avec la requête S3 PutObject

Vous pouvez utiliser la requête S3 PutObject pour ajouter un objet à un compartiment.

Résoudre les conflits

Les requêtes clients conflictuelles, comme par exemple deux clients écrivant sur la même clé, sont résolues selon le principe du « latest-wins ». Le moment de l'évaluation du « latest-wins » est déterminé par la date à laquelle le système StorageGRID termine une requête donnée, et non par la date à laquelle les clients S3 commencent une opération.

Taille de l'objet

La taille maximale *recommandée* pour une seule opération PutObject est de 5 Gio (5 368 709 120 octets). Si vous avez des objets de plus de 5 Gio, utilisez plutôt ["téléchargement en plusieurs parties"](#).

La taille maximale *prise en charge* pour une seule opération PutObject est de 5 Tio (5 497 558 138 880 octets).



Si vous avez effectué une mise à niveau depuis StorageGRID 11.6 ou une version antérieure, l'alerte « Taille de l'objet S3 trop volumineux lors de la commande PUT » sera déclenchée si vous tentez de télécharger un objet dépassant 5 Gio. Si vous disposez d'une nouvelle installation de StorageGRID 11.7 ou 11.8, l'alerte ne sera pas déclenchée dans ce cas. Cependant, afin de s'aligner sur la norme AWS S3, les prochaines versions de StorageGRID ne prendront plus en charge le téléchargement d'objets de plus de 5 Gio.

Taille des métadonnées utilisateur

Amazon S3 limite la taille des métadonnées définies par l'utilisateur au sein de chaque en-tête de requête PUT à 2 Ko. StorageGRID limite les métadonnées utilisateur à 24 Kio. La taille des métadonnées définies par l'utilisateur est mesurée en faisant la somme du nombre d'octets dans l'encodage UTF-8 de chaque clé et valeur.

Caractères UTF-8 dans les métadonnées utilisateur

Si une requête inclut des valeurs UTF-8 (non échappées) dans le nom de clé ou la valeur des métadonnées définies par l'utilisateur, le comportement de StorageGRID est indéfini.

StorageGRID n'analyse ni n'interprète les caractères UTF-8 échappés inclus dans le nom ou la valeur de la clé des métadonnées définies par l'utilisateur. Les caractères UTF-8 échappés sont traités comme des caractères ASCII :

- PutObject, CopyObject, GetObject, et HeadObject réussissent si les métadonnées définies par l'utilisateur incluent des caractères UTF-8 échappés.
- StorageGRID ne renvoie pas l'`x-amz-missing-meta` en-tête si la valeur interprétée du nom ou de la valeur de la clé contient des caractères non imprimables.

Limites des balises d'objet

Vous pouvez ajouter des balises aux nouveaux objets lors de leur chargement, ou vous pouvez les ajouter à des objets existants. StorageGRID et Amazon S3 prennent en charge jusqu'à 10 balises par 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 appartiennent au compte propriétaire du compartiment, y compris les objets créés par un compte autre que celui du propriétaire ou par un utilisateur anonyme.

En-têtes de requête 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-EncodingStorageGRID`, ce dernier ne vérifie pas les éléments suivants :

- StorageGRID ne vérifie pas les `chunk-signature` par rapport aux données du bloc.
- StorageGRID ne vérifie pas la valeur que vous fournissez `x-amz-decoded-content-length` par rapport à l'objet.

- Content-Language
- Content-Length
- Content-MD5
- Content-Type
- Expires
- Transfer-Encoding

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

- `x-amz-checksum-sha256`
- `x-amz-meta-`, suivie d'une paire nom-valeur contenant des métadonnées définies par l'utilisateur.

Lors de la spécification de la paire nom-valeur pour les métadonnées définies par l'utilisateur, utilisez ce format général :

```
x-amz-meta-name: value
```

Si vous souhaitez utiliser l'option **Heure de création définie par l'utilisateur** comme heure de référence pour une règle ILM, vous devez utiliser `creation-time` comme nom des métadonnées qui enregistrent la date de 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 simultanément une **date de création définie par l'utilisateur** comme date de référence et l'option d'ingestion Équilibrée ou Stricte. Une erreur est renvoyée lors de la création de la règle ILM.

- `x-amz-tagging`
- En-têtes de requête S3 Object Lock
 - `x-amz-object-lock-mode`
 - `x-amz-object-lock-retain-until-date`
 - `x-amz-object-lock-legal-hold`

Si une requête est effectuée sans ces en-têtes, les paramètres de rétention par défaut du compartiment sont utilisés pour calculer le mode de version de l'objet et la date de rétention jusqu'à la date limite. Voir ["Utilisez l'API REST S3 pour configurer S3 Object Lock"](#).

- En-têtes de requête SSE :
 - `x-amz-server-side-encryption`
 - `x-amz-server-side-encryption-customer-key-MD5`
 - `x-amz-server-side-encryption-customer-key`
 - `x-amz-server-side-encryption-customer-algorithm`

Voir [En-têtes de requête pour le chiffrement côté serveur](#)

En-têtes de requête non pris en charge

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

- `If-Match`

Le `If-Match` header est accepté mais non fonctionnel.

- `If-None-Match`

Le `If-None-Match` header est accepté mais non fonctionnel.

- `x-amz-acl`
- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`
- `x-amz-website-redirect-location`

L'`x-amz-website-redirect-location` en-tête renvoie ``XNotImplemented`.

Options de classe de stockage

L'`x-amz-storage-class` en-tête de requête est pris en charge. La valeur soumise pour `x-amz-storage-class` influe sur la manière dont StorageGRID protège les données d'objet lors de l'ingestion, et non sur le nombre de copies persistantes de l'objet stockées dans le système StorageGRID (ce nombre étant déterminé par ILM).

Si la règle ILM correspondant à un objet ingéré utilise l'option d'ingestion stricte, l'`x-amz-storage-class` en-tête n'a aucun effet.

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

- **STANDARD (Défaut)**
 - **Double validation** : Si la règle ILM spécifie l'option « Double validation » pour le comportement d'ingestion, dès qu'un objet est ingéré, une seconde copie de cet objet est créée et distribuée sur un nœud de stockage différent (double validation). Lors de l'évaluation de l'ILM, StorageGRID détermine si ces copies intermédiaires initiales respectent les instructions de placement de la règle. Si ce n'est pas le cas, il peut être nécessaire de créer de nouvelles copies de l'objet à d'autres emplacements et de supprimer les copies intermédiaires initiales.
 - **Équilibré** : Si la règle ILM spécifie l'option Équilibré et StorageGRID ne peut pas effectuer immédiatement toutes les copies spécifiées dans la règle, StorageGRID effectue deux copies intermédiaires sur différents nœuds de stockage.

Si StorageGRID peut créer immédiatement toutes les copies d'objets spécifiées dans la règle ILM (placement synchrone), l'`x-amz-storage-class` en-tête n'a aucun effet.

- **REDUCED_REDUNDANCY**
 - **Double validation** : Si la règle ILM spécifie l'option de double validation pour le comportement d'ingestion, StorageGRID crée une seule copie intermédiaire lors de l'ingestion de l'objet (validation unique).
 - **Équilibré** : Si la règle ILM spécifie l'option Équilibré, StorageGRID crée une seule copie intermédiaire uniquement si le système ne peut pas créer immédiatement toutes les copies spécifiées dans la règle. Si StorageGRID peut effectuer un placement synchrone, cet en-tête est sans effet. L'option `REDUCED_REDUNDANCY` est particulièrement utile lorsque la règle ILM correspondant à l'objet crée une seule copie répliquée. Dans ce cas, utiliser `REDUCED_REDUNDANCY` évite la création et la suppression inutiles d'une copie supplémentaire de l'objet pour chaque opération d'ingestion.

L'utilisation de l'option `REDUCED_REDUNDANCY` est déconseillée dans d'autres circonstances. Elle augmente le risque de perte de données lors de l'ingestion. Par exemple, vous pourriez perdre des données si la copie unique est initialement stockée sur un Storage Node qui tombe en panne avant que l'évaluation ILM puisse avoir lieu.



Le fait de ne disposer que d'une seule copie répliquée pour une période donnée expose les données à un risque de perte définitive. Si une seule copie répliquée d'un objet existe, cet objet est perdu en cas de panne ou d'erreur grave d'un Storage Node. Vous perdez également temporairement l'accès à l'objet lors des procédures de maintenance telles que les mises à niveau.

La spécification de `REDUCED_REDUNDANCY` n'affecte que le nombre de copies créées lors de la première ingestion d'un objet. Elle n'affecte pas le nombre de copies de l'objet créées lors de l'évaluation de l'objet par les politiques ILM actives et n'entraîne pas le stockage des données à des niveaux de redondance inférieurs dans le système StorageGRID.



Si vous ingérez un objet dans un compartiment avec S3 Object Lock activé, l'option `REDUCED_REDUNDANCY` est ignorée. Si vous ingérez un objet dans un compartiment Compliant hérité, l'option `REDUCED_REDUNDANCY` renvoie une erreur. StorageGRID effectuera toujours une double validation à l'ingestion pour garantir le respect des exigences de conformité.

En-têtes de requête pour le chiffrement côté serveur

Vous pouvez utiliser les en-têtes de requête suivants pour chiffrer un objet avec le chiffrement côté serveur. Les options SSE et SSE-C sont incompatibles.

- **SSE** : Utilisez l'en-tête suivant si vous souhaitez chiffrer l'objet avec une clé unique gérée par StorageGRID.

- `x-amz-server-side-encryption`

Lorsque l'en-tête `x-amz-server-side-encryption` n'est pas inclus dans la requête `PutObject`, le "paramètre de chiffrement des objets stockés" à l'échelle de la grille est omis de la réponse `PutObject`.

- `${post_edited_translations.segment}`

- `x-amz-server-side-encryption-customer-algorithm`: Précisez AES256.
 - `x-amz-server-side-encryption-customer-key`: Spécifiez votre clé de chiffrement pour le nouvel objet.
 - `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le condensé MD5 de la clé de chiffrement du nouvel objet.



Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant. Avant d'utiliser des clés fournies par le client pour sécuriser les données d'objet, examinez les considérations pour ["utilisation du chiffrement côté serveur"](#).



Si un objet est chiffré avec SSE ou SSE-C, tous les paramètres de chiffrement au niveau du compartiment ou de la grille sont ignorés.

Versionnage

Si le versionnage est activé pour un compartiment, un identifiant unique `versionId` est automatiquement généré pour la version de l'objet stocké. Cet identifiant `versionId` est également renvoyé dans la réponse via l' `x-amz-version-id` en-tête de réponse.

Si le versionnage est suspendu, la version de l'objet est stockée avec une valeur nulle `versionId` et si une version nulle existe déjà, elle sera écrasée.

`${post_edited_translations.segment}`

Lors de l'utilisation de l' `Authorization` en-tête pour authentifier les requêtes, StorageGRID diffère d'AWS de la manière suivante :

- StorageGRID n'exige pas que les `host` en-têtes soient inclus dans `CanonicalHeaders`.
- StorageGRID n'a pas besoin que `Content-Type` soit inclus dans `CanonicalHeaders`.
- StorageGRID n'exige pas que les `x-amz-*` en-têtes soient inclus dans `CanonicalHeaders`.



En bonne pratique, incluez toujours ces en-têtes `CanonicalHeaders` afin de garantir leur vérification ; toutefois, si vous les excluez, StorageGRID ne renvoie pas d'erreur.

Pour plus de détails, consultez ["Calculs de signature pour l'en-tête d'autorisation : transfert de la charge utile"](#)

en un seul bloc (AWS Signature Version 4)".

Informations connexes

- "Gérez les objets avec ILM"
- "Référence de l'API Amazon Simple Storage Service : PutObject"

Restaurez un objet dans StorageGRID avec la requête S3 RestoreObject

Vous pouvez utiliser la requête S3 RestoreObject pour restaurer un objet stocké dans un Cloud Storage Pool.

Type de requête pris en charge

StorageGRID prend uniquement en charge les requêtes RestoreObject pour restaurer un objet. Il ne prend pas en charge le type de restauration SELECT. Les requêtes Select renvoient XNotImplemented.

Versionnage

Vous pouvez, si vous le souhaitez, spécifier versionId une version particulière d'un objet dans un compartiment versionné. Si vous ne spécifiez versionId, la version la plus récente de l'objet est restaurée.

Comportement de RestoreObject sur les objets du Cloud Storage Pool

Si un objet a été stocké dans un "Pool de stockage cloud", une requête RestoreObject présente le comportement suivant, en fonction de l'état de l'objet. Consultez "HeadObject" pour plus de détails.



Si un objet est stocké dans un Cloud Storage Pool et qu'une ou plusieurs copies de l'objet existent également sur la grille, il n'est pas nécessaire de restaurer l'objet en émettant une requête RestoreObject. À la place, la copie locale peut être récupérée directement à l'aide d'une requête GetObject.

État de l'objet	Comportement de RestoreObject
Objet ingéré dans StorageGRID mais pas encore évalué par ILM, ou l'objet ne se trouve pas dans un Cloud Storage Pool	403 Forbidden, InvalidObjectState
Objet présent dans le pool de stockage cloud mais n'ayant pas encore été transféré dans un état non récupérable	200 OK Aucune modification n'est apportée. Remarque : Avant qu'un objet ne soit passé à un état non récupérable, vous ne pouvez pas modifier son expiry-date.

État de l'objet	Comportement de RestoreObject
L'objet est passé dans un état non récupérable	202 Accepted Restaure une copie récupérable de l'objet dans le Cloud Storage Pool pour le nombre de jours spécifié dans le corps de la requête. À l'issue de cette période, l'objet est renvoyé à un état non récupérable. Vous pouvez éventuellement utiliser l'<code>Tier`</code>élément de requête pour déterminer combien de temps la tâche de restauration prendra pour se terminer (<code>`Expedited</code>, <code>Standard</code>, ou <code>Bulk</code>). Si vous ne spécifiez pas <code>Tier</code>, le <code>`Standard`</code> niveau est utilisé. Important : Si un objet a été transféré vers S3 Glacier Deep Archive ou si le Cloud Storage Pool utilise le stockage Azure Blob, vous ne pouvez pas le restaurer à l'aide du niveau <code>Expedited</code>. L'erreur suivante est renvoyée <code>403 Forbidden, InvalidTier: Retrieval option is not supported by this storage class.</code>
Objet en cours de restauration à partir d'un état non récupérable	409 Conflict, RestoreAlreadyInProgress
Objet entièrement restauré dans le Cloud Storage Pool	200 OK Remarque : Si un objet a été restauré à un état récupérable, vous pouvez modifier son <code>expiry-date</code> en réémettant la requête <code>RestoreObject</code> avec une nouvelle valeur pour <code>Days</code>. La date de restauration est mise à jour par rapport à l'heure de la requête.

Filtrer les données d'objets dans StorageGRID avec la requête S3 SelectObjectContent

Vous pouvez utiliser la requête S3 SelectObjectContent pour filtrer le contenu d'un objet S3 en fonction d'une instruction SQL simple.

Pour plus d'informations, consultez ["Référence de l'API Amazon Simple Storage Service : SelectObjectContent"](#).

Avant de commencer

- `${post_edited_translations.segment}`
- Vous disposez `s3:GetObject` des autorisations nécessaires pour l'objet que vous souhaitez interroger.
- L'objet que vous souhaitez interroger doit être dans l'un des formats suivants :
 - **CSV.** Peut être utilisé tel quel ou compressé dans des archives GZIP ou BZIP2.
 - **Parquet.** Exigences supplémentaires pour les objets Parquet :
 - S3 Select prend uniquement en charge la compression par colonnes via GZIP ou Snappy. S3 Select ne prend pas en charge la compression de l'objet entier pour les objets Parquet.
 - S3 Select ne prend pas en charge la sortie Parquet. Vous devez spécifier le format de sortie comme CSV ou JSON.
 - La taille maximale d'un groupe de lignes non compressé est de 512 Mo.

- Vous devez utiliser les types de données spécifiés dans le schéma de l'objet.
- Vous ne pouvez pas utiliser les types logiques INTERVAL, JSON, LIST, TIME ou UUID.
- Votre expression SQL a une longueur maximale de 256 Ko.
- \${post_edited_translations.segment}

Exemple de syntaxe de requête CSV

```
POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Expression>string</Expression>
  <ExpressionType>string</ExpressionType>
  <RequestProgress>
    <Enabled>boolean</Enabled>
  </RequestProgress>
  <InputSerialization>
    <CompressionType>GZIP</CompressionType>
    <CSV>
      <AllowQuotedRecordDelimiter>boolean</AllowQuotedRecordDelimiter>
      <Comments>#</Comments>
      <FieldDelimiter>\t</FieldDelimiter>
      <FileHeaderInfo>USE</FileHeaderInfo>
      <QuoteCharacter>'</QuoteCharacter>
      <QuoteEscapeCharacter>\\</QuoteEscapeCharacter>
      <RecordDelimiter>\n</RecordDelimiter>
    </CSV>
  </InputSerialization>
  <OutputSerialization>
    <CSV>
      <FieldDelimiter>string</FieldDelimiter>
      <QuoteCharacter>string</QuoteCharacter>
      <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
      <QuoteFields>string</QuoteFields>
      <RecordDelimiter>string</RecordDelimiter>
    </CSV>
  </OutputSerialization>
  <ScanRange>
    <End>long</End>
    <Start>long</Start>
  </ScanRange>
</SelectObjectContentRequest>
```

Exemple de syntaxe de requête Parquet

```
POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns=http://s3.amazonaws.com/doc/2006-03-01/>
  <Expression>string</Expression>
  <ExpressionType>string</ExpressionType>
  <RequestProgress>
    <Enabled>boolean</Enabled>
  </RequestProgress>
  <InputSerialization>
    <CompressionType>GZIP</CompressionType>
    <PARQUET>
    </PARQUET>
  </InputSerialization>
  <OutputSerialization>
    <CSV>
      <FieldDelimiter>string</FieldDelimiter>
      <QuoteCharacter>string</QuoteCharacter>
      <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
      <QuoteFields>string</QuoteFields>
      <RecordDelimiter>string</RecordDelimiter>
    </CSV>
  </OutputSerialization>
  <ScanRange>
    <End>long</End>
    <Start>long</Start>
  </ScanRange>
</SelectObjectContentRequest>
```

Exemple de requête SQL

Cette requête récupère le nom de l'État, la population de 2010, la population estimée de 2015 et le pourcentage de variation à partir des données de recensement des États-Unis. Les enregistrements du fichier qui ne sont pas des États sont ignorés.

```
SELECT STNAME, CENSUS2010POP, POPESTIMATE2015, CAST((POPESTIMATE2015 -
CENSUS2010POP) AS DECIMAL) / CENSUS2010POP * 100.0 FROM S3Object WHERE
NAME = STNAME
```

Les premières lignes du fichier à interroger, SUB-EST2020_ALL.csv, se présentent ainsi :

```
SUMLEV, STATE, COUNTY, PLACE, COUSUB, CONCIT, PRIMGEO_FLAG, FUNCSTAT, NAME, STNAME,
CENSUS2010POP,
ESTIMATESBASE2010, POPESTIMATE2010, POPESTIMATE2011, POPESTIMATE2012, POPESTIM
ATE2013, POPESTIMATE2014,
POPESTIMATE2015, POPESTIMATE2016, POPESTIMATE2017, POPESTIMATE2018, POPESTIMAT
E2019, POPESTIMATE042020,
POPESTIMATE2020
040,01,000,00000,00000,00000,0,A,Alabama,Alabama,4779736,4780118,4785514,4
799642,4816632,4831586,
4843737,4854803,4866824,4877989,4891628,4907965,4920706,4921532
162,01,000,00124,00000,00000,0,A,Abbeville
city,Alabama,2688,2705,2699,2694,2645,2629,2610,2602,
2587,2578,2565,2555,2555,2553
162,01,000,00460,00000,00000,0,A,Adamsville
city,Alabama,4522,4487,4481,4474,4453,4430,4399,4371,
4335,4304,4285,4254,4224,4211
162,01,000,00484,00000,00000,0,A,Addison
town,Alabama,758,754,751,750,745,744,742,734,734,728,
725,723,719,717
```

`${post_edited_translations.segment}`

```
aws s3api select-object-content --endpoint-url https://10.224.7.44:10443
--no-verify-ssl --bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.csv --expression-type SQL --input-serialization '{"CSV":
{"FileHeaderInfo": "USE", "Comments": "#", "QuoteEscapeCharacter": "\"",
"RecordDelimiter": "\n", "FieldDelimiter": ",", "QuoteCharacter": "\"",
"AllowQuotedRecordDelimiter": false}, "CompressionType": "NONE"}' --output
-serialization '{"CSV": {"QuoteFields": "ASNEEDED",
"QuoteEscapeCharacter": "#", "RecordDelimiter": "\n", "FieldDelimiter":
",", "QuoteCharacter": "\""}}' --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" changes.csv
```

Les premières lignes du fichier de sortie, `changes.csv`, ressemblent à ceci :

```
Alabama,4779736,4854803,1.5705260708959658022953568983726297854
Alaska,710231,738430,3.9703983633493891424057806544631253775
Arizona,6392017,6832810,6.8959922978928247531256565807005832431
Arkansas,2915918,2979732,2.1884703204959810255295244928012378949
California,37253956,38904296,4.4299724839960620557988526104449148971
Colorado,5029196,5454328,8.4532796097030221132761578590295546246
```

`${post_edited_translations.segment}`

```
aws s3api select-object-content --endpoint-url https://10.224.7.44:10443
--bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.parquet --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" --expression-type
'SQL' --input-serialization '{"Parquet":{}}' --output-serialization
'{"CSV":{}}' changes.csv
```

Les premières lignes du fichier de sortie, changes.csv, ressemblent à ceci :

```
Alabama,4779736,4854803,1.5705260708959658022953568983726297854
Alaska,710231,738430,3.9703983633493891424057806544631253775
Arizona,6392017,6832810,6.8959922978928247531256565807005832431
Arkansas,2915918,2979732,2.1884703204959810255295244928012378949
California,37253956,38904296,4.4299724839960620557988526104449148971
Colorado,5029196,5454328,8.4532796097030221132761578590295546246
```

`${post_edited_translations.segment}`

Opérations de chargement multiparties prises en charge dans StorageGRID

Cette section décrit comment StorageGRID prend en charge les opérations de chargement en plusieurs parties.

Les conditions et remarques suivantes s'appliquent à toutes les opérations de téléchargement en plusieurs parties :

- Vous ne devez pas dépasser 1 000 chargements multiparties simultanés vers un seul compartiment, car les résultats des requêtes ListMultipartUploads pour ce compartiment pourraient être incomplets.
- StorageGRID applique les limites de taille AWS pour les parties multipart. Les clients S3 doivent respecter les consignes suivantes :
 - Chaque partie d'un téléchargement en plusieurs parties 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 règle générale, la taille des parties doit être aussi grande que possible. Par exemple, utilisez des parties de 5 Gio pour un objet de 100 Gio. Comme chaque partie est considérée comme un objet unique, l'utilisation de grandes tailles de parties réduit la surcharge des métadonnées StorageGRID.
 - Pour les objets de moins de 5 Gio, envisagez d'utiliser le téléchargement non multipart à la place.
- L'ILM est évalué pour chaque partie d'un objet multipartie lors de son ingestion, puis pour l'objet dans son ensemble une fois le chargement multipartie terminé, si la règle ILM utilise le mode Balanced ou Strict ["option d'ingestion"](#). Vous devez être conscient de la façon dont cela affecte le placement des objets et des parties :
 - Si les paramètres ILM sont modifiés pendant un chargement multipartie vers S3, certaines parties de

l'objet risquent de ne plus respecter les exigences ILM en vigueur une fois le chargement terminé. Toute partie qui n'est pas placée correctement est mise en file d'attente pour une réévaluation ILM et déplacée ultérieurement vers l'emplacement correct.

- Lors de l'évaluation ILM d'une partie, StorageGRID filtre sur la taille de la partie, et non sur celle de l'objet. Cela signifie que des parties d'un objet peuvent être stockées dans des emplacements ne répondant pas aux exigences ILM de l'objet dans son ensemble. Par exemple, si une règle spécifie que tous les objets de 10 Go ou plus sont stockés à DC1 tandis que tous les objets plus petits sont stockés à DC2, chaque partie de 1 Go d'un chargement multipartie en 10 parties est stockée à DC2 lors de l'ingestion. Cependant, lors de l'évaluation ILM de l'objet dans son ensemble, toutes les parties de l'objet sont déplacées vers DC1.
- Toutes les opérations de téléchargement en plusieurs parties prennent en charge StorageGRID ["valeurs de cohérence"](#).
- Lorsqu'un objet est ingéré à l'aide d'un téléchargement multipart, le ["seuil de segmentation d'objet \(1 Gio\)"](#) n'est pas appliqué.
- Selon les besoins, vous pouvez utiliser ["chiffrement côté serveur"](#) avec les chargements en plusieurs parties. Pour utiliser SSE (chiffrement côté serveur avec des clés gérées par StorageGRID), vous devez inclure l'`x-amz-server-side-encryption` en-tête de requête uniquement dans la requête `CreateMultipartUpload`. Pour utiliser SSE-C (chiffrement côté serveur avec des clés fournies par le client), vous devez spécifier les mêmes trois en-têtes de requête de clé de chiffrement dans la requête `CreateMultipartUpload` et dans chaque requête `UploadPart` suivante.
- Un objet téléchargé en plusieurs parties est inclus dans un ["bucket de branche"](#) si l'ingestion a été initiée avant l'horodatage Before du compartiment de base, quelle que soit la date de fin du téléchargement.

Opération	Mise en œuvre
<code>AbortMultipartUpload</code>	Implémenté avec l'ensemble du comportement de l'API REST Amazon S3. Sous réserve de modifications sans préavis.
<code>CompleteMultipartUpload</code>	Voir "CompleteMultipartUpload"
<code>CreateMultipartUpload</code> (anciennement nommé <code>Initiate Multipart Upload</code>)	Voir "CreateMultipartUpload"
<code>ListMultipartUploads</code>	Voir "ListMultipartUploads"
<code>ListParts</code>	Implémenté avec l'ensemble du comportement de l'API REST Amazon S3. Sous réserve de modifications sans préavis.
<code>UploadPart</code>	Voir "UploadPart"
<code>UploadPartCopy</code>	Voir "UploadPartCopy"

Comment l'API REST S3 de StorageGRID effectue les chargements en plusieurs parties

L'opération `CompleteMultipartUpload` finalise le chargement en plusieurs parties d'un objet en assemblant les parties précédemment chargées.



StorageGRID prend en charge les valeurs non consécutives par ordre croissant pour le paramètre de requête `partNumber` avec `CompleteMultipartUpload`. Le paramètre peut commencer par n'importe quelle valeur.

Résoudre les conflits

Les requêtes clients conflictuelles, comme par exemple deux clients écrivant sur la même clé, sont résolues selon le principe du « latest-wins ». Le moment de l'évaluation du « latest-wins » est déterminé par la date à laquelle le système StorageGRID termine une requête donnée, et non par la date à laquelle les clients S3 commencent une opération.

En-têtes de requête pris en charge

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

- `x-amz-checksum-sha256`
- `x-amz-storage-class`

L'`x-amz-storage-class`en-tête affecte le nombre de copies d'objets que StorageGRID crée si la règle ILM correspondante spécifie le "[Option de double validation ou d'ingestion équilibrée](#)".

- `STANDARD`

(Par défaut) Spécifie une opération d'ingestion à double validation lorsque la règle ILM utilise l'option `Dual commit`, ou lorsque l'option `Balanced` revient à créer des copies intermédiaires.

- `REDUCED_REDUNDANCY`

Spécifie une opération d'ingestion à validation unique lorsque la règle ILM utilise l'option de double validation, ou lorsque l'option équilibrée revient à créer des copies intermédiaires.



Si vous ingérez un objet dans un compartiment avec S3 Object Lock activé, l'`REDUCED\_REDUNDANCY`option est ignorée. Si vous ingérez un objet dans un compartiment Compliant hérité, l'`REDUCED\_REDUNDANCY`option renvoie une erreur. StorageGRID effectuera toujours une double validation à l'ingestion pour garantir le respect des exigences de conformité.



Si un chargement en plusieurs parties n'est pas terminé dans un délai de 15 jours, l'opération est marquée comme inactive et toutes les données associées sont supprimées du système.



La `ETag`valeur renvoyée n'est pas une somme MD5 des données, mais suit l'implémentation de l'API Amazon S3 de la `ETag`valeur pour les objets multipart.

En-têtes de requête non pris en charge

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

- `If-Match`

Le `If-Match` header est accepté mais non fonctionnel.

- If-None-Match

Le If-None-Match header est accepté mais non fonctionnel.

- x-amz-sdk-checksum-algorithm
- x-amz-trailer

Versionnage

Cette opération finalise un chargement en plusieurs parties. Si le versionnage est activé pour un compartiment, la version de l'objet est créée après la finalisation du chargement en plusieurs parties.

Si le versionnage est activé pour un compartiment, un identifiant unique `versionId` est automatiquement généré pour la version de l'objet stocké. Cet identifiant `versionId` est également renvoyé dans la réponse via l' `x-amz-version-id` en-tête de réponse.

Si le versionnage est suspendu, la version de l'objet est stockée avec une valeur nulle `versionId` et si une version nulle existe déjà, elle sera écrasée.



Lorsque le versionnage est activé pour un bucket, la finalisation d'un chargement multipart crée toujours une nouvelle version, même si des chargements multipart simultanés sont finalisés sur la même clé d'objet. Lorsque le versionnage n'est pas activé pour un bucket, il est possible d'initier un chargement multipart, puis qu'un autre chargement multipart soit initié et finalisé en premier sur la même clé d'objet. Sur les buckets non versionnés, le chargement multipart finalisé en dernier prévaut.

Échec de la réplication, de la notification ou de la notification des métadonnées

Si le compartiment dans lequel s'effectue le chargement en plusieurs parties est configuré pour un service de plateforme, le chargement en plusieurs parties réussit même si l'action de réplication ou de notification associée échoue.

Un locataire peut déclencher l'échec de la réplication ou la notification 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 indésirable.

Consultez ["Dépannage des services de plateforme"](#).

En-têtes et options des requêtes S3 CreateMultipartUpload dans StorageGRID

L'opération CreateMultipartUpload (anciennement appelée Initiate Multipart Upload) lance un téléchargement en plusieurs parties pour un objet et renvoie un ID de téléchargement.

L' `x-amz-storage-class` en-tête de requête est pris en charge. La valeur soumise pour `x-amz-storage-class` influe sur la manière dont StorageGRID protège les données d'objet lors de l'ingestion, et non sur le nombre de copies persistantes de l'objet stockées dans le système StorageGRID (ce nombre étant déterminé par ILM).

Si la règle ILM correspondant à un objet ingéré utilise l'option Strict ["option d'ingestion"](#), l' `x-amz-storage-class` en-tête n'a aucun effet.

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

- **STANDARD (Défaut)**
 - **Double validation** : Si la règle ILM spécifie l'option d'ingestion « Double validation », dès qu'un objet est ingéré, une seconde copie de cet objet est créée et distribuée sur un nœud de stockage différent (double validation). Lors de l'évaluation de l'ILM, StorageGRID détermine si ces copies intermédiaires initiales respectent les instructions de placement de la règle. Si ce n'est pas le cas, il peut être nécessaire de créer de nouvelles copies de l'objet à d'autres emplacements et de supprimer les copies intermédiaires initiales.
 - **Équilibré** : Si la règle ILM spécifie l'option Équilibré et StorageGRID ne peut pas effectuer immédiatement toutes les copies spécifiées dans la règle, StorageGRID effectue deux copies intermédiaires sur différents nœuds de stockage.

Si StorageGRID peut créer immédiatement toutes les copies d'objets spécifiées dans la règle ILM (placement synchrone), l'`x-amz-storage-class` en-tête n'a aucun effet.

- **REDUCED_REDUNDANCY**
 - **Double validation** : Si la règle ILM spécifie l'option Double validation, StorageGRID crée une seule copie intermédiaire lors de l'ingestion de l'objet (validation unique).
 - **Équilibré** : Si la règle ILM spécifie l'option Équilibré, StorageGRID crée une seule copie intermédiaire uniquement si le système ne peut pas créer immédiatement toutes les copies spécifiées dans la règle. Si StorageGRID peut effectuer un placement synchrone, cet en-tête est sans effet. L'`'REDUCED_REDUNDANCY'` option est particulièrement utile lorsque la règle ILM correspondant à l'objet crée une seule copie répliquée. Dans ce cas, utiliser `'REDUCED_REDUNDANCY'` évite la création et la suppression inutiles d'une copie supplémentaire de l'objet pour chaque opération d'ingestion.

L'utilisation de l'`'REDUCED_REDUNDANCY'` option est déconseillée dans d'autres circonstances. `'REDUCED_REDUNDANCY'` Elle augmente le risque de perte de données lors de l'ingestion. Par exemple, vous pourriez perdre des données si la copie unique est initialement stockée sur un Storage Node qui tombe en panne avant que l'évaluation ILM puisse avoir lieu.



Le fait de ne disposer que d'une seule copie répliquée pour une période donnée expose les données à un risque de perte définitive. Si une seule copie répliquée d'un objet existe, cet objet est perdu en cas de panne ou d'erreur grave d'un Storage Node. Vous perdez également temporairement l'accès à l'objet lors des procédures de maintenance telles que les mises à niveau.

La spécification de `REDUCED_REDUNDANCY` n'affecte que le nombre de copies créées lors de la première ingestion d'un objet. Elle n'affecte pas le nombre de copies de l'objet créées lors de l'évaluation de l'objet par les politiques ILM actives et n'entraîne pas le stockage des données à des niveaux de redondance inférieurs dans le système StorageGRID.



Si vous ingérez un objet dans un compartiment avec S3 Object Lock activé, l'`'REDUCED_REDUNDANCY'` option est ignorée. Si vous ingérez un objet dans un compartiment Compliant hérité, l'`'REDUCED_REDUNDANCY'` option renvoie une erreur. StorageGRID effectuera toujours une double validation à l'ingestion pour garantir le respect des exigences de conformité.

En-têtes de requête pris en charge

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

- Content-Type
- x-amz-checksum-algorithm

Actuellement, seule la valeur SHA256 pour x-amz-checksum-algorithm est prise en charge.

- x-amz-meta-, suivi d'une paire nom-valeur contenant des métadonnées définies par l'utilisateur

Lors de la spécification de la paire nom-valeur pour les métadonnées définies par l'utilisateur, utilisez ce format général :

```
x-amz-meta-_name_: `value`
```

Si vous souhaitez utiliser l'option **Heure de création définie par l'utilisateur** comme heure de référence pour une règle ILM, vous devez utiliser `creation-time` comme nom des métadonnées qui enregistrent la date de 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.



L'ajout `creation-time` en tant que métadonnées définies par l'utilisateur n'est pas autorisé si vous ajoutez un objet à un compartiment avec la conformité héritée activée. Une erreur sera renvoyée.

- En-têtes de requête S3 Object Lock :

- x-amz-object-lock-mode
- x-amz-object-lock-retain-until-date
- x-amz-object-lock-legal-hold

Si une requête est effectuée sans ces en-têtes, les paramètres de rétention par défaut du compartiment sont utilisés pour calculer la date de rétention jusqu'à la version de l'objet.

["Utilisez l'API REST S3 pour configurer S3 Object Lock"](#)

- En-têtes de requête 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

[En-têtes de requête pour le chiffrement côté serveur](#)



Pour plus d'informations sur la façon dont StorageGRID gère les caractères UTF-8, consultez ["PutObject"](#).

En-têtes de requête pour le chiffrement côté serveur

Vous pouvez utiliser les en-têtes de requête suivants pour chiffrer un objet multipartite avec le chiffrement côté serveur. Les options SSE et SSE-C sont mutuellement exclusives.

- **SSE** : Utilisez l'en-tête suivant dans la requête `CreateMultipartUpload` si vous souhaitez chiffrer l'objet avec une clé unique gérée par StorageGRID. Ne spécifiez pas cet en-tête dans aucune des requêtes `UploadPart`.

- `x-amz-server-side-encryption`

- **SSE-C** : Utilisez ces trois en-têtes dans la requête `CreateMultipartUpload` (et dans chaque requête `UploadPart` suivante) si vous souhaitez chiffrer l'objet avec une clé unique que vous fournissez et gérez.

- `x-amz-server-side-encryption-customer-algorithm`: Précisez AES256.

- `x-amz-server-side-encryption-customer-key`: Spécifiez votre clé de chiffrement pour le nouvel objet.

- `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le condensé MD5 de la clé de chiffrement du nouvel objet.



Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant. Avant d'utiliser des clés fournies par le client pour sécuriser les données d'objet, examinez les considérations pour ["utilisation du chiffrement côté serveur"](#).

En-têtes de requête non pris en charge

L'en-tête de requête suivant n'est pas pris en charge :

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

L'`x-amz-website-redirect-location` en-tête renvoie ``XNotImplemented`.

Versionnage

Le chargement en plusieurs parties comprend des opérations distinctes pour lancer le chargement, lister les chargements, charger les différentes parties, assembler les parties chargées et finaliser le chargement. Les objets sont créés (et versionnés le cas échéant) lorsque l'opération `CompleteMultipartUpload` est effectuée.

Fonctionnement S3 `ListMultipartUploads` et paramètres pris en charge dans StorageGRID

L'opération `ListMultipartUploads` répertorie les chargements multipart en cours pour un compartiment.

Les paramètres de requête suivants sont pris en charge :

- `encoding-type`
- `key-marker`

- max-uploads
- prefix
- upload-id-marker
- Host
- Date
- Authorization

Versionnage

Le chargement en plusieurs parties comprend des opérations distinctes pour lancer le chargement, lister les chargements, charger les différentes parties, assembler les parties chargées et finaliser le chargement. Les objets sont créés (et versionnés le cas échéant) lorsque l'opération CompleteMultipartUpload est effectuée.

En-têtes de requête pris en charge et non pris en charge pour les opérations S3 UploadPart dans StorageGRID

L'opération UploadPart télécharge une partie dans un chargement multipart pour un objet.

En-têtes de requête pris en charge

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

- x-amz-checksum-sha256
- Content-Length
- Content-MD5

En-têtes de requête pour le chiffrement côté serveur

Si vous avez spécifié le chiffrement SSE-C pour la requête CreateMultipartUpload, vous devez également inclure les en-têtes de requête suivants dans chaque requête UploadPart :

- x-amz-server-side-encryption-customer-algorithm: Précisez AES256.
- x-amz-server-side-encryption-customer-key: Spécifiez la même clé de chiffrement que celle que vous avez fournie dans la requête CreateMultipartUpload.
- x-amz-server-side-encryption-customer-key-MD5 : Veuillez indiquer le même condensé MD5 que celui que vous avez fourni dans la requête CreateMultipartUpload.



Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant. Avant d'utiliser des clés fournies par le client pour sécuriser les données d'objet, examinez les considérations dans ["Utilisez le chiffrement côté serveur"](#).

Si vous avez spécifié une somme de contrôle SHA-256 lors de la requête CreateMultipartUpload, vous devez également inclure l'en-tête de requête suivant dans chaque requête UploadPart :

- x-amz-checksum-sha256: Spécifiez la somme de contrôle SHA-256 pour cette partie.

En-têtes de requête non pris en charge

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

- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`

Versionnage

Le chargement en plusieurs parties comprend des opérations distinctes pour lancer le chargement, lister les chargements, charger les différentes parties, assembler les parties chargées et finaliser le chargement. Les objets sont créés (et versionnés le cas échéant) lorsque l'opération `CompleteMultipartUpload` est effectuée.

Chargez une partie d'un objet dans StorageGRID avec l'opération S3 `UploadPartCopy`

L'opération `UploadPartCopy` téléverse une partie d'un objet en copiant les données d'un objet existant comme source de données.

L'opération `UploadPartCopy` est implémentée avec l'ensemble du comportement de l'API REST Amazon S3. Sous réserve de modifications sans préavis.

Cette requête lit et écrit les données de l'objet spécifié dans `x-amz-copy-source-range` 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`

En-têtes de requête pour le chiffrement côté serveur

Si vous avez spécifié le chiffrement SSE-C pour la requête `CreateMultipartUpload`, vous devez également inclure les en-têtes de requête suivants dans chaque requête `UploadPartCopy` :

- `x-amz-server-side-encryption-customer-algorithm`: Précisez AES256.
- `x-amz-server-side-encryption-customer-key`: Spécifiez la même clé de chiffrement que celle que vous avez fournie dans la requête `CreateMultipartUpload`.
- `x-amz-server-side-encryption-customer-key-MD5` : Veuillez indiquer le même condensé MD5 que celui que vous avez fourni dans la requête `CreateMultipartUpload`.

Si l'objet source est chiffré à l'aide d'une clé fournie par le client (SSE-C), vous devez inclure les trois en-têtes suivants dans la requête `UploadPartCopy`, afin que l'objet puisse être déchiffré puis copié :

- `x-amz-copy-source-server-side-encryption-customer-algorithm`: Précisez 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 condensé MD5

que vous avez fourni lors de la création de l'objet source.



Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant. Avant d'utiliser des clés fournies par le client pour sécuriser les données d'objet, examinez les considérations dans ["Utilisez le chiffrement côté serveur"](#).

Versionnage

Le chargement en plusieurs parties comprend des opérations distinctes pour lancer le chargement, lister les chargements, charger les différentes parties, assembler les parties chargées et finaliser le chargement. Les objets sont créés (et versionnés le cas échéant) lorsque l'opération CompleteMultipartUpload est effectuée.

Réponses d'erreur de l'API REST StorageGRID S3

Le système StorageGRID prend en charge toutes les réponses d'erreur standard de l'API REST S3 qui s'appliquent. De plus, l'implémentation StorageGRID ajoute plusieurs réponses personnalisées.

Codes d'erreur de l'API S3 pris en charge

Nom	statut HTTP
AccessDenied	403 Interdit
BadDigest	400 Mauvaise requête
BucketAlreadyExists	409 Conflit
BucketNotEmpty	409 Conflit
IncompleteBody	400 Mauvaise requête
InternalServerError	Erreur interne du serveur 500
InvalidAccessKeyId	403 Interdit
InvalidArgument	400 Mauvaise requête
InvalidBucketName	400 Mauvaise requête
InvalidBucketState	409 Conflit
InvalidDigest	400 Mauvaise requête
InvalidEncryptionAlgorithmError	400 Mauvaise requête
InvalidPart	400 Mauvaise requête

Nom	statut HTTP
InvalidPartOrder	400 Mauvaise requête
InvalidRange	416 Plage demandée non satisfaisable
InvalidRequest	400 Mauvaise requête
InvalidStorageClass	400 Mauvaise requête
InvalidTag	400 Mauvaise requête
URI invalide	400 Mauvaise requête
KeyTooLong	400 Mauvaise requête
XML malformé	400 Mauvaise requête
MetadataTooLarge	400 Mauvaise requête
MethodNotAllowed	405 Méthode non autorisée
MissingContentLength	411 Longueur requise
MissingRequestBodyError	400 Mauvaise requête
MissingSecurityHeader	400 Mauvaise requête
NoSuchBucket	404 Introuvable
NoSuchKey	404 Introuvable
NoSuchUpload	404 Introuvable
NotImplemented	501 Non implémenté
NoSuchBucketPolicy	404 Introuvable
ObjectLockConfigurationNotFoundError	404 Introuvable
PreconditionFailed	412 Précondition non remplie
RequestTimeTooSkewed	403 Interdit
ServiceUnavailable	503 Service indisponible

Nom	statut HTTP
SignatureDoesNotMatch	403 Interdit
TooManyBuckets	400 Mauvaise requête
UserKeyMustBeSpecified	400 Mauvaise requête

Codes d'erreur personnalisés StorageGRID

Nom	Description	statut HTTP
XBucketLifecycleNotAllowed	La configuration du cycle de vie du bucket n'est pas autorisée dans un bucket Compliant hérité	400 Mauvaise requête
Exception d'analyse de la politique de compartiment	Échec de l'analyse du JSON de la politique de compartiment reçue.	400 Mauvaise requête
XComplianceConflict	Opération refusée en raison de paramètres de conformité hérités.	403 Interdit
XComplianceReducedRedundancyForbidden	La redondance réduite n'est pas autorisée dans le compartiment Compliant hérité	400 Mauvaise requête
XMaxBucketPolicyLengthExceeded	Votre stratégie dépasse la longueur maximale autorisée pour une stratégie de compartiment.	400 Mauvaise requête
XMissingInternalRequestHeader	En-tête manquant d'une requête interne.	400 Mauvaise requête
XNoSuchBucketCompliance	Le compartiment spécifié n'a pas la conformité héritée activée.	404 Introuvable
XNotAcceptable	La requête contient un ou plusieurs en-têtes Accept qui n'ont pas pu être satisfaits.	406 Non acceptable
XNotImplemented	La demande que vous avez fournie implique une fonctionnalité qui n'est pas implémentée.	501 Non implémenté

Opérations personnalisées StorageGRID

Opérations personnalisées de compartiment prises en charge dans StorageGRID

Le système StorageGRID prend en charge les opérations personnalisées qui sont

ajoutées à l'API REST S3.

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

Opération	Description
"Cohérence du bucket GET"	Renvoie la cohérence appliquée à un compartiment particulier.
"Cohérence PUT Bucket"	Définit la cohérence appliquée à un compartiment particulier.
"Obtenir le temps d'accès du compartiment"	Indique si les mises à jour du temps d'accès sont activées ou désactivées pour un compartiment donné.
"PUT temps d'accès du dernier accès au compartiment"	Permet d'activer ou de désactiver les mises à jour du temps d'accès pour un compartiment particulier.
"SUPPRIMER la configuration de notification des métadonnées du compartiment"	Supprime le fichier XML de configuration des notifications de métadonnées associé à un compartiment particulier.
"Obtenir la configuration de notification des métadonnées du bucket"	Renvoie le fichier XML de configuration des notifications de métadonnées associé à un compartiment particulier.
"Configuration de notification des métadonnées du compartiment PUT"	Configure le service de notification des métadonnées pour un compartiment.
"Obtenir l'utilisation du stockage"	Indique la capacité totale de stockage utilisée par un compte et pour chaque compartiment associé au compte.
"Déprécié : CreateBucket avec paramètres de conformité"	Obsolète et non pris en charge : vous ne pouvez plus créer de nouveaux compartiments avec la conformité activée.
"Obsolète : GET Bucket compliance"	Déprécié mais toujours pris en charge : renvoie les paramètres de conformité actuellement en vigueur pour un compartiment Compliant hérité existant.
"Obsolète : PUT Bucket compliance"	Obsolète mais pris en charge : permet de modifier les paramètres de conformité d'un compartiment Compliant hérité existant.

Récupérez le niveau de cohérence du compartiment dans StorageGRID avec la requête GET Bucket consistency

La requête GET Bucket consistency vous permet de déterminer la cohérence appliquée à un bucket particulier.

La cohérence par défaut est définie pour garantir la lecture après écriture des objets nouvellement créés.

Vous devez disposer de l'autorisation `s3:GetBucketConsistency`, ou être administrateur du compte, pour effectuer cette opération.

Exemple de requête

```
GET /bucket?x-ntap-sg-consistency HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Réponse

Dans la réponse XML, `<Consistency>` renverra l'une des valeurs suivantes :

Cohérence	Description
tous	Tous les nœuds reçoivent les données immédiatement, ou la requête échouera.
fort-mondial	Garantit la cohérence en lecture après écriture pour toutes les requêtes client sur tous les sites.
site fort	Garantit la cohérence des données en lecture après écriture pour toutes les requêtes client au sein d'un site.
lecture après une nouvelle écriture	(Par défaut) Assure la cohérence en lecture après écriture pour les nouveaux objets et la cohérence éventuelle pour les mises à jour d'objets. Offre une haute disponibilité et des garanties de protection des données. Recommandé dans la plupart des cas.
disponible	Garantit la cohérence éventuelle des nouveaux objets et des mises à jour d'objets. Pour les compartiments S3, utilisez cette fonctionnalité uniquement lorsque cela est nécessaire (par exemple, pour un compartiment contenant des valeurs de journal rarement lues, ou pour les opérations HEAD ou GET sur des clés qui n'existent pas). Non pris en charge pour les compartiments S3 FabricPool.

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 connexes

"Cohérence"

Spécifiez les niveaux de cohérence dans StorageGRID avec la requête PUT Bucket consistency

`${post_edited_translations.segment}`

La cohérence par défaut est définie pour garantir la lecture après écriture des objets nouvellement créés.

Avant de commencer

Vous devez disposer de l'autorisation `s3:PutBucketConsistency`, ou être le compte racine, pour effectuer cette opération.

Demande

Le paramètre `x-ntap-sg-consistency` doit contenir l'une des valeurs suivantes :

Cohérence	Description
tous	Tous les nœuds reçoivent les données immédiatement, ou la requête échouera.
fort-mondial	Garantit la cohérence en lecture après écriture pour toutes les requêtes client sur tous les sites.
site fort	Garantit la cohérence des données en lecture après écriture pour toutes les requêtes client au sein d'un site.
lecture après une nouvelle écriture	(Par défaut) Assure la cohérence en lecture après écriture pour les nouveaux objets et la cohérence éventuelle pour les mises à jour d'objets. Offre une haute disponibilité et des garanties de protection des données. Recommandé dans la plupart des cas.

Cohérence	Description
disponible	Garantit la cohérence éventuelle des nouveaux objets et des mises à jour d'objets. Pour les compartiments S3, utilisez cette fonctionnalité uniquement lorsque cela est nécessaire (par exemple, pour un compartiment contenant des valeurs de journal rarement lues, ou pour les opérations HEAD ou GET sur des clés qui n'existent pas). Non pris en charge pour les compartiments S3 FabricPool.

Remarque : En général, vous devez utiliser la cohérence « Lecture après nouvelle écriture ». Si les requêtes ne fonctionnent pas correctement, modifiez le comportement du client applicatif si possible. Ou configurez le client pour spécifier la cohérence pour chaque requête API. Définissez la cohérence au niveau du compartiment uniquement en dernier recours.

Exemple de requête

```
PUT /bucket?x-ntap-sg-consistency=strong-global HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Informations connexes

["Cohérence"](#)

Récupérez l'état de la dernière date d'accès au bucket dans StorageGRID avec la requête GET Bucket last access time

La requête GET Bucket last access time vous permet de déterminer si les mises à jour du temps d'accès sont activées ou désactivées pour chaque compartiment.

Vous devez disposer de l'autorisation s3:GetBucketLastAccessTime, ou être administrateur du compte, pour effectuer cette opération.

Exemple de requête

```
GET /bucket?x-ntap-sg-lastaccesstime HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Exemple de réponse

Cet exemple montre que les mises à jour du dernier temps d'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>
```

Activer et désactiver les mises à jour du temps d'accès dans StorageGRID avec la requête PUT Bucket last access time

La requête PUT Bucket last access time vous permet d'activer ou de désactiver les mises à jour du temps d'accès pour les compartiments individuels. La désactivation des mises à jour du temps d'accès améliore les performances et constitue le paramètre par défaut pour tous les compartiments créés avec la version 10.3.0 ou ultérieure.

Vous devez disposer de l'autorisation `s3:PutBucketLastAccessTime` pour un compartiment, ou être root du compte, pour effectuer cette opération.



À partir de la version 10.3 de StorageGRID, les mises à jour du temps d'accès sont désactivées par défaut pour tous les nouveaux compartiments. Si vous avez des compartiments créés avec une version antérieure de StorageGRID et que vous souhaitez adopter le nouveau comportement par défaut, vous devez explicitement désactiver les mises à jour du temps d'accès pour chacun de ces compartiments. Vous pouvez activer ou désactiver les mises à jour du temps d'accès à l'aide de la requête PUT Bucket last access time ou depuis la page de détails d'un compartiment dans le Tenant Manager. Voir ["Activer ou désactiver la mise à jour du temps d'accès"](#).

`${post_edited_translations.segment}`

- `GetObject`, `GetObjectAcl`, `GetObjectTagging`, et `HeadObject` ne mettent pas à jour le temps d'accès. L'objet n'est pas ajouté aux files d'attente pour l'évaluation de la gestion du cycle de vie de l'information (ILM).
- Les requêtes `CopyObject` et `PutObjectTagging` qui mettent à jour uniquement les métadonnées mettent également à jour le temps d'accès. L'objet est ajouté aux files d'attente pour l'évaluation ILM.
- Si les mises à jour du temps d'accès sont désactivées pour le compartiment source, les requêtes `CopyObject` ne mettent pas à jour le temps d'accès pour le compartiment source. L'objet copié n'est pas ajouté aux files d'attente pour l'évaluation ILM du compartiment source. Cependant, pour la destination, les requêtes `CopyObject` mettent toujours à jour le temps d'accès. La copie de l'objet est ajoutée aux files d'attente pour l'évaluation ILM.
- `CompleteMultipartUpload` les requêtes mettent à jour le temps d'accès. L'objet finalisé est ajouté aux files d'attente pour l'évaluation ILM.

Exemples de requêtes

Cet exemple active le dernier temps d'accès pour un compartiment.

```
PUT /bucket?x-ntap-sg-lastaccesstime=enabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Cet exemple désactive le temps d'accès pour un compartiment.

```
PUT /bucket?x-ntap-sg-lastaccesstime=disabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Désactivez le service d'intégration de recherche avec la requête DELETE Bucket metadata notification configuration dans StorageGRID

La requête de configuration de notification de métadonnées DELETE Bucket vous permet de désactiver le service d'intégration de recherche pour des compartiments individuels en supprimant le fichier XML de configuration.

Vous devez disposer de l'autorisation s3:DeleteBucketMetadataNotification pour un compartiment, ou être root du compte, pour effectuer cette opération.

Exemple de requête

Cet exemple montre comment désactiver le service d'intégration de recherche pour un compartiment.

```
DELETE /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Configurez l'intégration de la recherche dans StorageGRID avec la requête de configuration de notification des métadonnées du compartiment GET

La requête de configuration de notification des métadonnées GET Bucket vous permet de récupérer le fichier XML de configuration utilisé pour configurer l'intégration de la recherche pour des compartiments individuels.

Vous devez disposer de l'autorisation s3:GetBucketMetadataNotification, ou être administrateur du compte, pour effectuer cette opération.

Exemple de requête

Cette requête récupère la configuration de notification des métadonnées pour le compartiment nommé bucket.

```
GET /bucket?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Réponse

Le corps de la réponse inclut la configuration de notification des métadonnées du compartiment. La configuration de notification des métadonnées vous permet de déterminer comment le compartiment est configuré pour l'intégration à la recherche. Autrement dit, elle vous permet de déterminer quels objets sont indexés et vers quels points de terminaison les métadonnées de leurs objets 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 spécifie les objets auxquels elle s'applique et la destination où StorageGRID doit envoyer les métadonnées des objets. Les destinations doivent être spécifiées à l'aide de l'URN d'un point de terminaison StorageGRID.

Nom	Description	Obligatoire
MetadataNotificationConfi guration	Balise conteneur pour les règles utilisées pour spécifier les objets et la destination des notifications de métadonnées. Contient un ou plusieurs éléments de règle.	Oui

Nom	Description	Obligatoire
Règle	Balise conteneur pour une règle qui identifie les objets dont les métadonnées doivent être ajoutées à un index spécifié. Les règles comportant des préfixes qui se chevauchent sont rejetées. Inclus dans l'élément <code>MetadataNotificationConfiguration</code>.	Oui
ID	Identifiant unique de la règle. Inclus dans l'élément <code>Rule</code>.	Non
Statut	Le statut peut être « Activé » ou « Désactivé ». Aucune action n'est entreprise pour les règles désactivées. Inclus dans l'élément <code>Rule</code>.	Oui
Préfixe	Les objets correspondant au préfixe sont concernés 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 <code>Rule</code>.	Oui
Destination	Étiquette conteneur pour la destination d'une règle. Inclus dans l'élément <code>Rule</code>.	Oui

Nom	Description	Obligatoire
Urn	URN de la destination où les métadonnées de l'objet sont envoyées. Doit être l'URN d'un point de terminaison StorageGRID possédant 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 <code>domain-name/myindex/mytype</code>. Les points de terminaison sont configurés à l'aide du Gestionnaire de locataires ou de l'API de gestion des locataires. Ils se présentent sous la forme suivante : • <code>arn:aws:es:_region:account-ID_:domain/mydomain/myindex/mytype</code> • <code>urn:mysite:es:::mydomain/myindex/mytype</code> Le point de terminaison doit être configuré avant la soumission du fichier XML de configuration, sinon la configuration échouera avec une erreur 404. Urn est inclus dans l'élément Destination.	Oui

Exemple de réponse

Le code XML inclus entre les

`<MetadataNotificationConfiguration></MetadataNotificationConfiguration>` balises montre comment l'intégration avec un point de terminaison d'intégration de recherche est configurée pour le compartiment. Dans cet exemple, les métadonnées de l'objet sont envoyées à un index Elasticsearch nommé `current` et de type nommé `2017` qui est hébergé dans un domaine AWS nommé `records`.

```
HTTP/1.1 200 OK
Date: Thu, 20 Jul 2017 18:24:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/11.0.0
x-amz-request-id: 3832973499
Content-Length: 264
Content-Type: application/xml

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>Enabled</Status>
    <Prefix>2017</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-
1:3333333:domain/records/current/2017</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

Informations connexes

["Utilisez un compte locataire"](#)

Activez le service d'intégration de recherche dans StorageGRID avec la requête de configuration de notification des métadonnées du compartiment PUT

La requête PUT de configuration de notification des métadonnées de compartiment permet d'activer le service d'intégration de recherche pour des compartiments individuels. Le fichier XML de configuration de notification des métadonnées fourni dans le corps de la requête spécifie les objets dont les métadonnées sont envoyées à l'index de recherche de destination.

Vous devez disposer de l'autorisation `s3:PutBucketMetadataNotification` pour un compartiment, ou être root du compte, pour effectuer cette opération.

Demande

La requête doit inclure la configuration de notification des métadonnées dans son corps. Chaque configuration de notification des métadonnées comprend une ou plusieurs règles. Chaque règle spécifie les objets auxquels elle s'applique et la destination où StorageGRID doit envoyer les métadonnées des objets.

Il est possible de filtrer les objets en fonction du préfixe de leur nom. Par exemple, vous pouvez envoyer les métadonnées des objets avec le préfixe `/images` vers une destination, et les objets avec le préfixe `/videos` vers une autre.

Les configurations comportant des préfixes qui se chevauchent ne sont pas valides et sont rejetées lors de leur soumission. Par exemple, une configuration incluant une règle pour les objets ayant le préfixe `test` et une autre règle pour les objets ayant le préfixe `test2` ne serait pas autorisée.

Les destinations doivent être spécifiées à l'aide de l'URN d'un point de terminaison StorageGRID. Le point de terminaison doit exister lors de la soumission de la configuration de notification des métadonnées, sinon la requête 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 fichier XML de configuration des notifications de métadonnées.

Nom	Description	Obligatoire
MetadataNotificationConfi guration	Balise 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 conteneur pour une règle qui identifie les objets dont les métadonnées doivent être ajoutées à un index spécifié. Les règles comportant des préfixes qui se chevauchent sont rejetées. Inclus dans l'élément MetadataNotificationConfiguration.	Oui
ID	Identifiant unique de la règle. Inclus dans l'élément Rule.	Non

Nom	Description	Obligatoire
Statut	Le statut peut être « Activé » ou « Désactivé ». Aucune action n'est entreprise pour les règles désactivées. Inclus dans l'élément Rule.	Oui
Préfixe	Les objets correspondant au préfixe sont concernés 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 Rule.	Oui
Destination	Étiquette conteneur pour la destination d'une règle. Inclus dans l'élément Rule.	Oui
Urn	URN de la destination où les métadonnées de l'objet sont envoyées. Doit être l'URN d'un point de terminaison StorageGRID possédant 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 <code>domain-name/myindex/mytype</code>. Les points de terminaison sont configurés à l'aide du Gestionnaire de locataires ou de l'API de gestion des locataires. Ils se présentent sous la forme suivante : • <code>arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype</code> • <code>urn:mysite:es:::mydomain/myindex/mytype</code> Le point de terminaison doit être configuré avant la soumission du fichier XML de configuration, sinon la configuration échouera avec une erreur 404. Urn est inclus dans l'élément Destination.	Oui

Exemples de requêtes

Cet exemple illustre l'activation de l'intégration de la recherche pour un compartiment. Dans cet exemple, les métadonnées de tous les objets sont envoyées à la même destination.

```
PUT /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

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

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

```

PUT /graphics?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Images-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/images</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-1:33333333:domain/es-
domain/graphics/imagetype</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Videos-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/videos</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>

```

JSON généré par le service d'intégration de recherche

```

${post_edited_translations.segment}

```

Cet exemple montre un exemple du JSON qui pourrait être généré lorsqu'un objet avec la clé `SGWS/Tagging.txt` est créé dans un compartiment nommé `test`. Le compartiment `test` n'est pas versionné, la balise `versionId` est donc 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 point de terminaison de destination lorsque l'intégration de la recherche est activée.

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

Type	Nom de l'article	Description
Informations sur le bucket et l'objet	bucket	Nom du compartiment
Informations sur le bucket et l'objet	<code>\${post_edited_translations.segment}</code>	Nom de la clé de l'objet
Informations sur le bucket et l'objet	versionID	Version de l'objet, pour les objets dans des compartiments versionnés
Informations sur le bucket et l'objet	région	Région de compartiment, par exemple <code>us-east-1</code>
Métadonnées système	taille	<code>\${post_edited_translations.segment}</code>
Métadonnées système	md5	<code>\${post_edited_translations.segment}</code>
Métadonnées utilisateur	métadonnées <i>key:value</i>	Toutes les métadonnées utilisateur de l'objet, sous forme de paires clé-valeur

Type	Nom de l'article	Description
Étiquettes	balises <i>key:value</i>	Toutes les étiquettes d'objet définies pour l'objet, sous forme de paires clé-valeur



Pour les balises et les métadonnées utilisateur, StorageGRID transmet les dates et les nombres à Elasticsearch sous forme de chaînes de caractères ou de notifications d'événements S3. Pour configurer Elasticsearch afin qu'il interprète ces chaînes comme des dates ou des nombres, suivez les instructions Elasticsearch pour le mappage dynamique des champs et le mappage des formats de date. Vous devez activer le mappage dynamique des champs sur l'index avant de configurer le service d'intégration de recherche. Après l'indexation d'un document, vous ne pouvez plus modifier les types de champs du document dans l'index.

Informations connexes

["Utilisez un compte locataire"](#)

Récupérez l'utilisation du stockage du compte et du bucket dans StorageGRID avec la requête GET Storage Usage

La requête GET Storage Usage vous indique la quantité totale de stockage utilisée par un compte, ainsi que pour chaque compartiment associé à ce compte.

La quantité de stockage utilisée par un compte et ses buckets peut être obtenue par une requête ListBuckets modifiée avec le paramètre de requête `x-ntap-sg-usage`. L'utilisation du stockage des buckets est suivie séparément des requêtes PUT et DELETE traitées par le système. Il peut y avoir un certain délai avant que les valeurs d'utilisation ne correspondent aux valeurs attendues en fonction du traitement des requêtes, en particulier si le système est fortement sollicité.

Par défaut, StorageGRID tente de récupérer les informations d'utilisation en utilisant une cohérence globale forte. Si une cohérence globale forte ne peut pas être atteinte, StorageGRID tente de récupérer les informations d'utilisation avec une cohérence site forte.

Vous devez disposer de l'autorisation `s3:ListAllMyBuckets`, ou être root du compte, pour effectuer cette opération.

Exemple de requête

```
GET /?x-ntap-sg-usage HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Exemple de réponse

Cet exemple illustre un compte contenant quatre objets et 12 octets de données répartis 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>
```

Versionnage

Chaque version d'objet stockée contribuera aux valeurs `ObjectCount` et `DataBytes` dans la réponse. Les marqueurs de suppression ne sont pas ajoutés au total `ObjectCount`.

Informations connexes

["Cohérence"](#)

`${post_edited_translations.segment}`

Requêtes de compartiment obsolètes pour la conformité StorageGRID héritée

Vous pourriez avoir besoin d'utiliser l'API REST S3 de StorageGRID pour gérer les compartiments créés à l'aide de l'ancienne fonctionnalité de conformité.

Fonctionnalité de conformité obsolète

La fonctionnalité de conformité StorageGRID, disponible dans les versions précédentes de StorageGRID, est obsolète et a été remplacée par S3 Object Lock.

Si vous aviez précédemment activé le paramètre de conformité global, le paramètre de verrouillage global des objets S3 est activé dans StorageGRID 11.6. Vous ne pouvez plus créer de nouveaux compartiments avec la conformité activée ; cependant, si nécessaire, vous pouvez utiliser l'API REST S3 de StorageGRID pour gérer tout compartiment conforme existant.

- ["Utilisez l'API REST S3 pour configurer S3 Object Lock"](#)
- ["Gérez les objets avec ILM"](#)
- ["Base de connaissances NetApp : Comment gérer les compartiments conformes hérités dans StorageGRID 11.5"](#)

Demandes de conformité obsolètes :

- ["Déprécié - Modifications des requêtes PUT Bucket pour la conformité"](#)

L'élément XML SGCompliance est obsolète. Auparavant, vous pouviez inclure cet élément personnalisé StorageGRID dans le corps de la requête XML facultatif des requêtes PUT Bucket pour créer un bucket conforme.

- ["Obsolète - GET Bucket compliance"](#)

La requête GET Bucket compliance est obsolète. Cependant, vous pouvez continuer à utiliser cette requête pour déterminer les paramètres de conformité actuellement en vigueur pour un bucket Compliant existant.

- ["Obsolète - PUT Bucket compliance"](#)

La requête PUT Bucket compliance est obsolète. Cependant, vous pouvez continuer à utiliser cette requête pour modifier les paramètres de conformité d'un compartiment Compliant existant. Par exemple, vous pouvez placer un compartiment existant en rétention légale ou augmenter sa période de conservation.

Élément SGCompliance obsolète dans StorageGRID

L'élément XML SGCompliance est obsolète. Auparavant, vous pouviez inclure cet élément personnalisé StorageGRID dans le corps XML facultatif des requêtes CreateBucket pour créer un compartiment conforme.



La fonctionnalité de conformité StorageGRID, disponible dans les versions précédentes de StorageGRID, est obsolète et a été remplacée par S3 Object Lock. Pour plus de détails, consultez ce qui suit :

- ["Utilisez l'API REST S3 pour configurer S3 Object Lock"](#)
- ["Base de connaissances NetApp : Comment gérer les compartiments conformes hérités dans StorageGRID 11.5"](#)

Vous ne pouvez plus créer de nouveaux compartiments avec la conformité activée. Le message d'erreur suivant est renvoyé si vous tentez d'utiliser les modifications de la requête CreateBucket 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.

Requête GET Bucket compliance obsolète dans StorageGRID

La requête GET Bucket compliance est obsolète. Cependant, vous pouvez continuer à utiliser cette requête pour déterminer les paramètres de conformité actuellement en vigueur pour un bucket Compliant existant.



La fonctionnalité de conformité StorageGRID, disponible dans les versions précédentes de StorageGRID, est obsolète et a été remplacée par S3 Object Lock. Pour plus de détails, consultez ce qui suit :

- ["Utilisez l'API REST S3 pour configurer S3 Object Lock"](#)
- ["Base de connaissances NetApp : Comment gérer les compartiments conformes hérités dans StorageGRID 11.5"](#)

Vous devez disposer de l'autorisation `s3:GetBucketCompliance`, ou être root du compte, pour effectuer cette opération.

Exemple de requête

Cette requête d'exemple vous permet de déterminer les paramètres de conformité du compartiment nommé `mybucket`.

```
GET /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Exemple de réponse

Dans la réponse XML, `<SGCompliance>` répertorie les paramètres de conformité en vigueur pour le compartiment. Cet exemple de réponse montre les paramètres de conformité d'un compartiment dans lequel chaque objet sera conservé pendant un an (525 600 minutes), à partir de son ingestion dans la grille. Il n'y a actuellement aucune restriction légale sur ce compartiment. Chaque objet sera automatiquement supprimé après un an.

```

HTTP/1.1 200 OK
Date: date
Connection: connection
Server: StorageGRID/11.1.0
x-amz-request-id: request ID
Content-Length: length
Content-Type: application/xml

<SGCompliance>
  <RetentionPeriodMinutes>525600</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>

```

Nom	Description
RetentionPeriodMinutes	La durée de la période de conservation des objets ajoutés à ce compartiment, en minutes. La période de conservation commence lorsque l'objet est ingérée dans la grille.
LegalHold	• Vrai : Ce compartiment fait actuellement l'objet d'une rétention légale. Les objets dans ce compartiment ne peuvent pas être supprimés tant que la rétention légale n'est pas levée, même si leur période de conservation est expirée. • Faux : ce compartiment n'est actuellement soumis à aucune restriction légale. Les objets de ce compartiment peuvent être supprimés à l'expiration de leur période de conservation.
AutoDelete	• Vrai : les objets dans ce compartiment seront automatiquement supprimés à l'expiration de leur période de conservation, sauf si le compartiment fait l'objet d'une rétention légale. • Faux : les objets de ce compartiment ne seront pas supprimés automatiquement à l'expiration de la période de rétention. 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.

Requête PUT Bucket compliance obsolète dans StorageGRID

La requête PUT Bucket compliance est obsolète. Cependant, vous pouvez continuer à utiliser cette requête pour modifier les paramètres de conformité d'un compartiment Compliant existant. Par exemple, vous pouvez placer un compartiment existant en rétention légale ou augmenter sa période de conservation.



La fonctionnalité de conformité StorageGRID, disponible dans les versions précédentes de StorageGRID, est obsolète et a été remplacée par S3 Object Lock. Pour plus de détails, consultez ce qui suit :

- ["Utilisez l'API REST S3 pour configurer S3 Object Lock"](#)
- ["Base de connaissances NetApp : Comment gérer les compartiments conformes hérités dans StorageGRID 11.5"](#)

Vous devez disposer de l'autorisation `s3:PutBucketCompliance`, ou être root du compte, pour effectuer cette opération.

Vous devez spécifier une valeur pour chaque champ des paramètres de conformité lors de l'émission d'une requête de conformité PUT Bucket.

Exemple de requête

Cette requête d'exemple modifie les paramètres de conformité du compartiment nommé `mybucket`. Dans cet exemple, les objets dans `mybucket` seront désormais conservés pendant deux ans (1 051 200 minutes) au lieu d'un an, à compter de leur ingestion dans la grille. Ce compartiment n'est soumis à aucune restriction légale. Chaque objet sera automatiquement supprimé après deux ans.

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Content-Length: 152

<SGCompliance>
  <RetentionPeriodMinutes>1051200</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

Nom	Description
RetentionPeriodMinutes	La durée de la période de conservation des objets ajoutés à ce compartiment, en minutes. La période de conservation commence lorsque l'objet est ingérée dans la grille. Important Lorsque vous définissez une nouvelle valeur pour <code>RetentionPeriodMinutes</code>, vous devez indiquer une valeur supérieure ou égale à la période de rétention actuelle du compartiment. Une fois la période de rétention du compartiment définie, vous ne pouvez plus diminuer cette valeur ; vous pouvez seulement l'augmenter.

Nom	Description
LegalHold	• Vrai : Ce compartiment fait actuellement l'objet d'une rétention légale. Les objets dans ce compartiment ne peuvent pas être supprimés tant que la rétention légale n'est pas levée, même si leur période de conservation est expirée. • Faux : ce compartiment n'est actuellement soumis à aucune restriction légale. Les objets de ce compartiment peuvent être supprimés à l'expiration de leur période de conservation.
AutoDelete	• Vrai : les objets dans ce compartiment seront automatiquement supprimés à l'expiration de leur période de conservation, sauf si le compartiment fait l'objet d'une rétention légale. • Faux : les objets de ce compartiment ne seront pas supprimés automatiquement à l'expiration de la période de rétention. Vous devez supprimer ces objets manuellement si vous devez les supprimer.

Cohérence des paramètres de conformité

Lorsque vous mettez à jour les paramètres de conformité d'un compartiment S3 à l'aide d'une requête PUT Bucket compliance, StorageGRID tente de mettre à jour les métadonnées du compartiment sur l'ensemble de la grille. Par défaut, StorageGRID utilise la cohérence **Strong-global** pour garantir que tous les sites de centres de données et tous les nœuds de stockage contenant des métadonnées de compartiment bénéficient d'une cohérence en lecture après écriture pour les paramètres de conformité modifiés.

Si StorageGRID ne peut pas atteindre la cohérence **Strong-global** parce qu'un site de centre de données ou plusieurs Storage Nodes d'un site sont indisponibles, le code d'état HTTP de la réponse est 503 `Service Unavailable`.

Si vous recevez cette réponse, vous devez contacter l'administrateur du grid pour vous assurer que les services de stockage requis sont disponibles dans les plus brefs délais. Si l'administrateur du grid ne parvient pas à rendre disponibles suffisamment de Storage Nodes sur chaque site, le support technique pourrait vous demander de relancer la requête ayant échoué en forçant la cohérence **Strong-site**.



N'imposez jamais la cohérence **Strong-site** pour la conformité du compartiment PUT, sauf si le support technique vous l'a demandé et si vous comprenez les conséquences potentielles de l'utilisation de ce niveau.

Lorsque la cohérence est réduite à **Strong-site**, StorageGRID garantit que les paramètres de conformité mis à jour offriront une cohérence de lecture après écriture uniquement pour les requêtes client au sein d'un site. Cela signifie que le système StorageGRID peut temporairement avoir plusieurs paramètres incohérents pour ce bucket, 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 bucket sous conservation légale et que vous forcez une cohérence inférieure, les paramètres de conformité précédents du bucket (c'est-à-dire conservation légale désactivée) peuvent continuer à être en vigueur sur certains sites de centres de données. En conséquence, des objets que vous pensez être sous conservation légale peuvent être supprimés à l'expiration de leur période de rétention, soit par l'utilisateur, soit par AutoDelete, si cette option est activée.

Pour forcer l'utilisation de la cohérence **Strong-site**, réenvoyez la requête de conformité PUT Bucket et incluez l'`Consistency-Control` en-tête de requête HTTP, comme suit :

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Consistency-Control: strong-site
```

Réponses d'erreur

- Si le compartiment n'a pas été créé pour être conforme, le code d'état HTTP de la réponse est 404 Not Found.
- Si `RetentionPeriodMinutes` dans la requête est inférieur à la période de rétention actuelle du compartiment, le code d'état HTTP est 400 Bad Request.

Informations connexes

["Déprécié : Modifications des requêtes PUT Bucket pour conformité"](#)

`${post_edited_translations.segment}`

Comment StorageGRID utilise les politiques AWS pour contrôler l'accès aux compartiments et objets S3

StorageGRID utilise le langage de stratégie Amazon Web Services (AWS) pour permettre aux locataires S3 de contrôler l'accès aux compartiments et aux objets au sein de ces compartiments. Le système StorageGRID implémente un sous-ensemble du langage de stratégie de l'API REST S3. Les stratégies d'accès pour l'API S3 sont écrites en JSON.

Aperçu de la politique d'accès

StorageGRID prend en charge trois types de politiques d'accès :

- Les **stratégies de compartiment**, qui sont gérées à l'aide des opérations d'API S3 `GetBucketPolicy`, `PutBucketPolicy` et `DeleteBucketPolicy`, ou du Gestionnaire de locataires ou de l'API de gestion des locataires. Les stratégies de compartiment sont rattachées aux compartiments. Elles sont donc configurées pour contrôler l'accès au compartiment et aux objets qu'il contient par les utilisateurs du compte propriétaire du compartiment ou d'autres comptes. Une stratégie de compartiment s'applique à un seul compartiment et potentiellement à plusieurs groupes.
- **Politiques de groupe**, qui sont configurées à l'aide du Tenant Manager ou de l'API Tenant Management. Les politiques de groupe sont associées à un groupe du compte, elles sont donc configurées pour autoriser ce groupe à accéder à des ressources spécifiques détenues par ce compte. Une politique de groupe s'applique à un seul groupe et éventuellement à plusieurs compartiments.
- **Politiques de session**, qui sont incluses dans une demande `AssumeRole`. Les politiques de session ne s'appliquent qu'à la session donnée, définissant plus précisément les autorisations dont l'utilisateur dispose, en plus de celles accordées par la politique de groupe et de compartiment.



`${post_edited_translations.segment}`

Les politiques de compartiment et de groupe StorageGRID suivent une grammaire spécifique définie par Amazon. Chaque politique contient un tableau d'instructions de stratégie, et chaque instruction contient les éléments suivants :

- `${post_edited_translations.segment}`

- `${post_edited_translations.segment}`
- Principal/NotPrincipal
- Ressource/NotResource
- Action/NotAction
- Condition (facultative)

Les instructions de stratégie sont construites à l'aide de cette structure pour spécifier les autorisations :
 Accorder <Effect> pour autoriser/refuser à <Principal> d'effectuer <Action> sur <Resource> lorsque
 <Condition> s'applique.

`${post_edited_translations.segment}`

Élément	Description
Sid	L'élément Sid est facultatif. Le Sid est uniquement destiné à servir de description pour l'utilisateur. Il est stocké mais n'est pas interprété par le système StorageGRID.
<code>\${post_edited_translations.segment}</code>	Utilisez l'élément Effect pour déterminer si les opérations spécifiées sont autorisées ou refusées. Vous devez identifier les opérations que vous autorisez (ou refusez) sur les compartiments ou les objets à l'aide des mots-clés de l'élément Action pris en charge.
Principal/NotPrincipal	Vous pouvez autoriser des utilisateurs, des groupes et des comptes à accéder à des ressources spécifiques et à effectuer des actions spécifiques. Si aucune signature S3 n'est incluse dans la requête, l'accès anonyme est autorisé en spécifiant le caractère générique (*) comme principal. Par défaut, seul le compte racine a accès aux ressources dont il est propriétaire. Il vous suffit de spécifier l'élément Principal dans une stratégie de compartiment. Pour les stratégies de groupe, le groupe auquel la stratégie est rattachée constitue l'élément Principal implicite.
Ressource/NotResource	L'élément Resource identifie les compartiments et les objets. Vous pouvez autoriser ou refuser des autorisations aux compartiments et aux objets en utilisant l'ARN (Amazon Resource Name) pour identifier la ressource.
Action/NotAction	Les éléments Action et Effect sont les deux composants des autorisations. Lorsqu'un groupe demande une ressource, l'accès à celle-ci lui est accordé ou refusé. L'accès est refusé à moins que vous n'attribuez spécifiquement des autorisations, mais vous pouvez utiliser un refus explicite pour remplacer une autorisation accordée par une autre règle.
Condition	L'élément Condition est facultatif. Les conditions permettent de créer des expressions pour déterminer quand une règle 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 permissions telles que `s3:GetObject`, `s3:PutObject` et `s3:DeleteObject`.

```
s3:*Object
```

Dans l'élément `Resource`, vous pouvez utiliser les caractères génériques `()` et `(?)`. L'**astérisque** `()` correspond à zéro ou plusieurs caractères, tandis que le point d'interrogation `(?)` correspond à n'importe quel caractère.

Dans l'élément `Principal`, les caractères génériques ne sont pas pris en charge, sauf pour définir l'accès anonyme, qui accorde l'autorisation à tous. Par exemple, vous définissez le caractère générique `(*)` comme valeur de `Principal`.

```
"Principal": "*" 
```

```
"Principal": { "AWS": "*" }
```

Dans l'exemple suivant, l'instruction utilise les éléments `Effect`, `Principal`, `Action` et `Resource`. Cet exemple présente une instruction de stratégie de compartiment complète qui utilise l'effet « Allow » pour accorder aux Principals, le groupe admin `federated-group/admin` et le groupe finance `federated-group/finance`, les autorisations d'effectuer l'Action `s3:ListBucket` sur le compartiment nommé `mybucket` et l'Action `s3:GetObject` sur tous les objets à l'intérieur de ce compartiment.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::27233906934684427525:federated-group/admin",
          "arn:aws:iam::27233906934684427525:federated-group/finance"
        ]
      },
      "Action": [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::mybucket",
        "arn:aws:s3:::mybucket/*"
      ]
    }
  ]
}
```

`${post_edited_translations.segment}`

`${post_edited_translations.segment}`

Par défaut, toutes les mises à jour que vous apportez aux règles de groupe sont cohérentes à terme. Lorsqu'une règle de groupe devient cohérente, l'application des modifications peut prendre 15 minutes supplémentaires en raison de la mise en cache des règles. Par défaut, toutes les mises à jour que vous apportez aux règles de compartiment sont fortement cohérentes.

Vous pouvez, si nécessaire, modifier les garanties de cohérence pour les mises à jour des règles d'accès du compartiment. Par exemple, vous pouvez souhaiter qu'une modification d'une règle d'accès de compartiment soit disponible lors d'une panne de site.

Dans ce cas, vous pouvez soit définir l'en-tête `Consistency-Control` dans la requête `PutBucketPolicy`, soit utiliser la requête de cohérence `PUT Bucket`. Lorsqu'une politique de compartiment devient cohérente, la prise d'effet des modifications peut prendre 8 secondes supplémentaires en raison de la mise en cache des politiques.



Si vous modifiez la cohérence pour contourner un problème temporaire, veillez à rétablir la valeur d'origine du paramètre au niveau du compartiment une fois la modification terminée. Sinon, toutes les requêtes ultérieures au compartiment utiliseront le paramètre modifié.

`${post_edited_translations.segment}`

Une règle de session est une règle d'accès qui restreint temporairement les autorisations disponibles lors d'une session spécifique, par exemple lorsqu'un utilisateur assume un groupe. Une règle de session ne peut autoriser qu'un sous-ensemble d'autorisations et ne peut pas accorder d'autorisations supplémentaires. Le groupe lui-même peut disposer d'autorisations plus larges.

`${post_edited_translations.segment}`

`${post_edited_translations.segment}`

- `${post_edited_translations.segment}`

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

- Utilisez cette syntaxe pour spécifier l'ARN de la ressource d'identité (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
```

`${post_edited_translations.segment}`

- `${post_edited_translations.segment}`

- Les caractères internationaux, qui peuvent être spécifiés dans la clé d'objet, doivent être encodés à l'aide de JSON UTF-8 ou de séquences d'échappement JSON \u. L'encodage en pourcentage n'est pas pris en charge.

`"${post_edited_translations.segment}"`

Le corps de la requête HTTP pour l'opération PutBucketPolicy doit être encodé avec charset=UTF-8.

Spécifiez les ressources dans une règle

`${post_edited_translations.segment}`

- Chaque énoncé de politique requiert un élément Resource. Dans une politique, les ressources sont désignées par l'élément Resource, ou alternativement, NotResource pour l'exclusion.
- Vous spécifiez les ressources avec un ARN de ressource S3. Par exemple :

```
"Resource": "arn:aws:s3:::mybucket/*"
```

- Vous pouvez également utiliser des variables de stratégie dans la clé de l'objet. Par exemple :

```
"Resource": "arn:aws:s3:::mybucket/home/${aws:username}/*"
```

- La valeur de la ressource peut spécifier un compartiment qui n'existe pas encore lors de la création d'une stratégie de groupe.

`${post_edited_translations.segment}`

`${post_edited_translations.segment}`

- Chaque déclaration de stratégie dans une stratégie de compartiment doit inclure un élément Principal. Les déclarations de stratégie dans une stratégie de groupe n'ont pas besoin de l'élément Principal car le groupe est considéré comme le principal.
- Dans une politique, les principaux sont désignés par l'élément "Principal" ou, alternativement, "NotPrincipal" pour l'exclusion.
- Les identités basées sur un compte doivent être spécifiées à l'aide d'un ID ou d'un ARN :

```
"Principal": { "AWS": "account_id" }
"Principal": { "AWS": "identity_arn" }
```

- `${post_edited_translations.segment}`

```
"Principal": { "AWS": "27233906934684427525" }
```

- Vous pouvez spécifier uniquement le compte racine :

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:root" }
```

- `${post_edited_translations.segment}`

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-user/Alex" }
```

- Vous pouvez spécifier un groupe fédéré particulier (« Managers ») :

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-group/Managers" }
```

- `${post_edited_translations.segment}`

```
"Principal": "*" 
```

- Pour éviter toute ambiguïté, vous pouvez utiliser l'UUID de l'utilisateur au lieu du nom d'utilisateur :

```
arn:aws:iam::27233906934684427525:user-uuid/de305d54-75b4-431b-adb2-eb6b9e546013
```

Par exemple, supposons qu'Alex quitte l'organisation et que le nom d'utilisateur `Alex` soit supprimé. Si un nouvel Alex rejoint l'organisation et qu'on lui attribue le même `Alex` nom d'utilisateur, le nouvel utilisateur pourrait 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 règle de compartiment.

`${post_edited_translations.segment}`

Dans une stratégie, l'élément Action est utilisé pour autoriser ou refuser des autorisations sur une ressource. Il existe un ensemble d'autorisations que vous pouvez spécifier dans une stratégie, qui sont désignées par l'élément "Action" ou, alternativement, "NotAction" pour l'exclusion. Chacun de ces éléments correspond à des opérations d'API REST S3 spécifiques.

Les tableaux répertorient les autorisations qui s'appliquent aux compartiments et les autorisations qui s'appliquent aux objets.



Amazon S3 utilise désormais l'autorisation `s3:PutReplicationConfiguration` pour les actions `PutBucketReplication` et `DeleteBucketReplication`. StorageGRID utilise des autorisations distinctes pour chaque action, ce qui correspond à la spécification Amazon S3 d'origine.



`${post_edited_translations.segment}`

Autorisations applicables aux compartiments

Autorisations	<code>\${post_edited_translations.segment}</code>	<code>\${post_edited_translations.segment}</code>
s3:CreateBucket	CreateBucket	Oui. Remarque : À utiliser uniquement dans la stratégie de groupe.
s3>DeleteBucket	DeleteBucket	
s3>DeleteBucketMetadataNotification	SUPPRIMER la configuration de notification des métadonnées du compartiment	Oui
s3>DeleteBucketPolicy	DeleteBucketPolicy	
s3>DeleteReplicationConfiguration	DeleteBucketReplication	Oui, des autorisations distinctes pour PUT et DELETE
s3:GetBucketAcl	GetBucketAcl	
s3:GetBucketCompliance	GET Bucket compliance (obsolète)	Oui
s3:GetBucketConsistency	Cohérence du bucket GET	Oui
<code>\${post_edited_translations.segment}</code>	GetBucketCors	
s3:GetEncryptionConfiguration	GetBucketEncryption	
s3:GetBucketLastAccessTime	Obtenir le temps d'accès du compartiment	Oui
s3:GetBucketLocation	GetBucketLocation	
s3:GetBucketMetadataNotification	Obtenir la configuration de notification des métadonnées du bucket	Oui
s3:GetBucketNotification	GetBucketNotificationConfiguration	
s3:GetBucketObjectLockConfiguration	GetObjectLockConfiguration	
s3:GetBucketPolicy	GetBucketPolicy	

Autorisations	<code>\${post_edited_translations.segment}</code>	<code>\${post_edited_translations.segment}</code>
s3:GetBucketTagging	GetBucketTagging	
s3:GetBucketVersioning	GetBucketVersioning	
s3:GetLifecycleConfiguration	GetBucketLifecycleConfiguration	
s3:GetReplicationConfiguration	GetBucketReplication	
s3:ListAllMyBuckets	- ListBuckets - Obtenir l'utilisation du stockage	<code>\${post_edited_translations.segment}</code> Remarque : À utiliser uniquement dans la stratégie de groupe.
s3:ListBucket	- ListObjects - HeadBucket - RestoreObject	
s3:ListBucketMultipartUploads	- ListMultipartUploads - RestoreObject	
s3:ListBucketVersions	<code>\${post_edited_translations.segment}</code>	
s3:PutBucketCompliance	<code>\${post_edited_translations.segment}</code>	Oui
s3:PutBucketConsistency	Cohérence PUT Bucket	Oui
s3:PutBucketCORS	- DeleteBucketCors† - PutBucketCors	
s3:PutEncryptionConfiguration	- DeleteBucketEncryption - PutBucketEncryption	
s3:PutBucketLastAccessTime	PUT temps d'accès du dernier accès au compartiment	Oui
s3:PutBucketMetadataNotification	Configuration de notification des métadonnées du compartiment PUT	Oui
s3:PutBucketNotification	PutBucketNotificationConfiguration	

Autorisations	<code>\${post_edited_translations.segment}</code>	<code>\${post_edited_translations.segment}</code>
s3:PutBucketObjectLockConfiguration	- CreateBucket avec l'en-tête de requête <code>x-amz-bucket-object-lock-enabled: true</code> (requiert également l'autorisation s3:CreateBucket) - PutObjectLockConfiguration	
s3:PutBucketPolicy	PutBucketPolicy	
s3:PutBucketTagging	- DeleteBucketTagging† - PutBucketTagging	
s3:PutBucketVersioning	PutBucketVersioning	
s3:PutLifecycleConfiguration	- DeleteBucketLifecycle† - PutBucketLifecycleConfiguration	
s3:PutReplicationConfiguration	PutBucketReplication	Oui, des autorisations distinctes pour PUT et DELETE

`${post_edited_translations.segment}`

Autorisations	<code>\${post_edited_translations.segment}</code>	<code>\${post_edited_translations.segment}</code>
s3:AbortMultipartUpload	- AbortMultipartUpload - RestoreObject	
s3:BypassGovernanceRetention	- DeleteObject - DeleteObjects - PutObjectRetention	
s3>DeleteObject	- DeleteObject - DeleteObjects - RestoreObject	
s3>DeleteObjectTagging	DeleteObjectTagging	
s3>DeleteObjectVersionTagging	DeleteObjectTagging (une version spécifique de l'objet)	

Autorisations	<code>\${post_edited_translations.segment}</code>	<code>\${post_edited_translations.segment}</code>
s3:DeleteObjectVersion	DeleteObject (une version spécifique de l'objet)	
s3:GetObject	• GetObject • HeadObject • RestoreObject • SelectObjectContent	
s3:GetObjectAcl	GetObjectAcl	
s3:GetObjectLegalHold	GetObjectLegalHold	
s3:GetObjectRetention	GetObjectRetention	
s3:GetObjectTagging	GetObjectTagging	
s3:GetObjectVersionTagging	GetObjectTagging (une version spécifique de l'objet)	
s3:GetObjectVersion	GetObject (une version spécifique de l'objet)	
s3:ListMultipartUploadParts	ListParts, RestoreObject	
s3:PutObject	• PutObject • CopyObject • RestoreObject • CreateMultipartUpload • CompleteMultipartUpload • UploadPart • UploadPartCopy	
s3:PutObjectLegalHold	PutObjectLegalHold	
s3:PutObjectRetention	PutObjectRetention	
s3:PutObjectTagging	PutObjectTagging	
s3:PutObjectVersionTagging	PutObjectTagging (une version spécifique de l'objet)	

Autorisations	<code>\${post_edited_translations.segment}</code>	<code>\${post_edited_translations.segment}</code>
s3:PutOverwriteObject	• PutObject • CopyObject • PutObjectTagging • DeleteObjectTagging • CompleteMultipartUpload	Oui
s3:RestoreObject	RestoreObject	

Utilisez l'autorisation PutOverwriteObject

L'autorisation s3:PutOverwriteObject est une autorisation StorageGRID personnalisée qui s'applique aux opérations de création ou de mise à jour d'objets. Le paramétrage de cette autorisation détermine si le client peut écraser les données d'un objet, les métadonnées définies par l'utilisateur ou le balisage d'objet S3.

`${post_edited_translations.segment}`

- **Autoriser** : le client peut écraser un objet. Il s'agit du paramètre par défaut.
- **Deny** : le client ne peut pas écraser un objet. Lorsqu'elle est définie sur Deny, l'autorisation PutOverwriteObject fonctionne comme suit :
 - Si un objet existant est trouvé au même chemin :
 - Les données de l'objet, les métadonnées définies par l'utilisateur ou le balisage de l'objet S3 ne peuvent pas être écrasés.
 - Toute opération d'ingestion en cours est annulée et une erreur est renvoyée.
 - Si le versionnement S3 est activé, le paramètre Deny empêche les opérations PutObjectTagging ou DeleteObjectTagging de modifier le TagSet pour un objet et ses versions non actuelles.
 - `${post_edited_translations.segment}`
- Lorsque cette autorisation est absente, l'effet est le même que si l'option Allow était activée.



Si la politique S3 actuelle autorise l'écrasement et que l'autorisation PutOverwriteObject est définie sur Deny, le client ne peut pas écraser les données d'un objet, ses métadonnées définies par l'utilisateur ou son balisage d'objet. De plus, si la case à cocher **Empêcher la modification par le client** est sélectionnée (**Configuration > Paramètres de sécurité > Réseau et objets**), ce paramètre remplace le paramètre de l'autorisation PutOverwriteObject.

`${post_edited_translations.segment}`

Les conditions définissent quand une politique sera en vigueur. Les conditions se composent d'opérateurs et de paires clé-valeur.

Les conditions utilisent des paires clé-valeur pour l'évaluation. Un élément Condition peut contenir plusieurs conditions, et chaque condition peut contenir plusieurs paires clé-valeur. Le bloc de condition utilise le format suivant :

```
Condition: {
  condition_type: {
    condition_key: condition_values
```

Dans l'exemple suivant, la condition IpAddress utilise la clé de condition SourceIp.

```
"Condition": {
  "IpAddress": {
    "aws:SourceIp": "54.240.143.0/24"
    ...
  },
  ...
```

`${post_edited_translations.segment}`

`${post_edited_translations.segment}`

- Chaîne
- Numérique
- `${post_edited_translations.segment}`
- Adresse IP
- `${post_edited_translations.segment}`

<code>\${post_edited_translations.segment}</code>	Description
StringEquals	<code>\${post_edited_translations.segment}</code>
StringNotEquals	Compare une clé à une valeur de chaîne en fonction d'une correspondance négative (sensible à la casse).
StringEqualsIgnoreCase	Compare une clé à une valeur de chaîne en fonction d'une correspondance exacte (ignore la casse).
StringNotEqualsIgnoreCase	<code>\${post_edited_translations.segment}</code>
StringLike	Compare une clé à une valeur de chaîne de caractères en fonction d'une correspondance exacte (sensible à la casse). Peut inclure les caractères génériques * et ?.
StringNotLike	Compare une clé à une valeur de chaîne sur la base d'une correspondance inversée (sensible à la casse). Peut inclure les caractères génériques * et ?.

<code>\${post_edited_translations.segment}</code>	Description
NumericEquals	Compare une clé à une valeur numérique en fonction d'une correspondance exacte.
NumericNotEquals	<code>\${post_edited_translations.segment}</code>
NumericGreaterThan	<code>\${post_edited_translations.segment}</code>
NumericGreaterThanEquals	Compare une clé à une valeur numérique en fonction d'une correspondance « supérieur ou égal à ».
NumericLessThan	Compare une clé à une valeur numérique en fonction de la correspondance « inférieur à ».
NumericLessThanEquals	<code>\${post_edited_translations.segment}</code>
<code>\${post_edited_translations.segment}</code>	<code>\${post_edited_translations.segment}</code>
IpAddress	<code>\${post_edited_translations.segment}</code>
NotIpAddress	Compare une clé à une adresse IP ou à une plage d'adresses IP en se basant sur une correspondance négative.
<code>\${post_edited_translations.segment}</code>	Vérifie si une clé de condition est présente dans le contexte de la requête actuelle.
IfExists	Ajouté à tout opérateur de condition, à l'exception de la condition Null, pour vérifier l'absence de cette clé de condition. Renvoie TRUE si la clé de condition n'est pas présente.

Clés de condition prises en charge

Clés de condition	Actions	Description
aws:SourceIp	opérateurs IP	Sera comparée à l'adresse IP à partir de laquelle la requête a été envoyée. Peut être utilisé pour les opérations sur les compartiments ou les objets. <code>\${post_edited_translations.segment}</code> Remarque : Si un équilibreur de charge tiers non transparent est utilisé, la comparaison portera sur l'adresse IP de cet équilibreur. Tout en-tête X-Forwarded-For sera ignoré, car sa validité ne peut être vérifiée.

Clés de condition	Actions	Description
<code>\${post_edited_translation.s.segment}</code>	<code>\${post_edited_translation.s.segment}</code>	Sera comparé au nom d'utilisateur de l'expéditeur à partir duquel la requête a été envoyée. Peut être utilisé pour les opérations sur les compartiments ou les objets.
s3: délimiteur	s3:ListBucket et Autorisations s3 : ListBucketVersions	Sera comparé au paramètre délimiteur spécifié dans une requête ListObjects ou ListObjectVersions.
s3:ExistingObjectTag/<tag-key>	s3:DeleteObjectTagging s3:DeleteObjectVersionTagging s3:GetObject s3:GetObjectAcl s3:GetObjectTagging s3:GetObjectVersion s3:GetObjectVersionAcl s3:GetObjectVersionTagging s3:PutObjectAcl s3:PutObjectTagging s3:PutObjectVersionAcl s3:PutObjectVersionTagging	Nécessitera que l'objet existant possède la clé et la valeur de balise spécifiques.
s3:max-keys	s3:ListBucket et Autorisations s3 : ListBucketVersions	Sera comparé au paramètre max-keys spécifié dans une requête ListObjects ou ListObjectVersions.
s3:object-lock-mode	s3:PutObject	Compare avec le <code>object-lock-mode</code> développé à partir de l'en-tête de requête dans la requête PutObject, CopyObject et CreateMultipartUpload.
s3:object-lock-mode	s3:PutObjectRetention	Comparé à l'élément <code>object-lock-mode</code> développé à partir du corps XML dans la requête PutObjectRetention.

Clés de condition	Actions	Description
<code>\${post_edited_translation s.segment}</code>	s3:PutObject	Compare à la date de conservation obligatoire spécifiée dans l'en-tête de requête <code>x-amz-object-lock-retain-until-date</code> ou calculée à partir de la période de rétention par défaut du compartiment pour s'assurer que ces valeurs se situent dans la plage autorisée pour les requêtes suivantes : • PutObject • CopyObject • CreateMultipartUpload
<code>\${post_edited_translation s.segment}</code>	s3:PutObjectRetention	Compare à la date de conservation limite spécifiée dans la requête PutObjectRetention pour s'assurer qu'elle s'inscrit dans la plage autorisée.
<code>\${post_edited_translation s.segment}</code>	s3:ListBucket et Autorisations s3 : ListBucketVersions	Sera comparé au paramètre de préfixe spécifié dans une requête ListObjects ou ListObjectVersions.
<code>s3:RequestObjectTag/<tag-key></code>	s3:PutObject s3:PutObjectTagging s3:PutObjectVersionTagging	Une clé et une valeur d'étiquette spécifiques seront requises lorsque la requête d'objet inclut un balisage.
<code>s3:x-amz-server-side-encryption-customer-algorithm</code>	s3:PutObject	Compare à la <code>sse-customer-algorithm</code> ou à la <code>copy-source-sse-customer-algorithm</code> valeur développée à partir de l'en-tête de la requête dans la demande PutObject, CopyObject, CreateMultipartUpload, UploadPart, UploadPartCopy et CompleteMultipartUpload.

Spécifiez les variables dans une politique

Vous pouvez utiliser des variables dans les politiques pour renseigner les informations de politique lorsqu'elles sont disponibles. Vous pouvez utiliser des variables de politique dans l'`Resource` élément et dans les comparaisons de chaînes dans l'`Condition` élément.

Dans cet exemple, la variable `${aws:username}` fait partie de l'élément Resource :

```
"Resource": "arn:aws:s3:::bucket-name/home/${aws:username}/*"
```

Dans cet exemple, la variable `${aws:username}` fait partie de la valeur de la condition dans le bloc de condition :

```

"Condition": {
  "StringLike": {
    "s3:prefix": "${aws:username}/*"
    ...
  },
  ...
}

```

Variable	Description
<code>\${aws:SourceIp}</code>	Utilise la clé SourceIp comme variable fournie.
<code>\${aws:username}</code>	<code>\${post_edited_translations.segment}</code>
<code>\${s3:prefix}</code>	Utilise la clé de préfixe spécifique au service comme variable fournie.
<code>\${s3:max-keys}</code>	Utilise la clé max-keys spécifique au service comme variable fournie.
<code>\${*}</code>	Caractère spécial. Utilise le caractère comme un caractère * littéral.
<code>\${?}</code>	Caractère spécial. Utilise le caractère en tant que caractère ? littéral.
<code>\${\$}</code>	Caractère spécial. Utilise le caractère comme un symbole \$ littéral.

`${post_edited_translations.segment}`

Il arrive qu'une politique accorde des autorisations dangereuses pour la sécurité ou la continuité des opérations, comme le blocage de l'utilisateur racine du compte. L'implémentation de l'API REST S3 de StorageGRID est moins restrictive lors de la validation des politiques qu'Amazon, mais tout aussi stricte lors de leur évaluation.

Description de la politique	Type de stratégie	Comportement d'Amazon	Comportement de StorageGRID
Refusez-vous toute autorisation sur le compte racine	Bucket	Valide et appliquée, mais le compte utilisateur root conserve l'autorisation pour toutes les opérations de stratégie de compartiment S3	Même
Refuser à soi-même toutes les autorisations à l'utilisateur/groupe	Groupe	<code>\${post_edited_translations.segment}</code>	Même
<code>\${post_edited_translations.segment}</code>	Bucket	Principal invalide	<code>\${post_edited_translations.segment}</code>

Description de la politique	Type de stratégie	Comportement d'Amazon	Comportement de StorageGRID
<code>\${post_edited_translations.segment}</code>	Bucket	<code>\${post_edited_translations.segment}</code>	Même
Autoriser à tous les autorisations pour toutes les actions	Bucket	Valide, mais les autorisations pour toutes les opérations de stratégie de compartiment S3 renvoient une erreur 405 Method Not Allowed pour le compte racine et les utilisateurs du compte externe.	Même
Refuser à tous l'autorisation d'effectuer toutes les actions	Bucket	Valide et appliquée, mais le compte utilisateur root conserve l'autorisation pour toutes les opérations de stratégie de compartiment S3	Même
<code>\${post_edited_translations.segment}</code>	Bucket	Principal invalide	<code>\${post_edited_translations.segment}</code>
La ressource est un compartiment S3 inexistant	Groupe	<code>\${post_edited_translations.segment}</code>	Même
Le principal est un groupe local	Bucket	Principal invalide	<code>\${post_edited_translations.segment}</code>
Cette politique accorde à un compte non propriétaire (y compris les comptes anonymes) l'autorisation de placer des objets.	Bucket	Valide. Les objets appartiennent au compte créateur, et la politique de compartiment ne s'applique pas. Le compte créateur doit accorder des autorisations d'accès pour l'objet à l'aide des ACL d'objet.	Valide. Les objets appartiennent au compte du propriétaire du compartiment. La politique de compartiment s'applique.

`${post_edited_translations.segment}`

Vous pouvez créer des compartiments WORM (write-once-read-many) afin de protéger les données, les métadonnées d'objet définies par l'utilisateur et le balisage d'objet S3. Vous configurez les compartiments WORM pour autoriser la création de nouveaux objets et empêcher la surécriture ou la suppression du contenu existant. Utilisez l'une des approches décrites ici.

Pour garantir que les écrasements soient toujours refusés, vous pouvez :

- Dans le Grid Manager, accédez à **Configuration > Sécurité > Paramètres de sécurité > Réseau et objets**, et cochez la case **Prevent client modification**.
- Appliquez les règles et politiques S3 suivantes :

- Ajoutez une opération DENY PutOverwriteObject à la stratégie S3.
- Ajoutez une opération DENY DeleteObject à la stratégie S3.
- Ajoutez une opération PutObject ALLOW à la stratégie S3.



Le paramètre DeleteObject sur REFUSER dans une stratégie S3 n'empêche pas ILM de supprimer des objets lorsqu'une règle telle que « zéro copie après 30 jours » existe.



Même en appliquant toutes ces règles et politiques, elles ne protègent pas contre les écritures simultanées (voir Situation A). Elles protègent en revanche contre les écrasements séquentiels complets (voir Situation B).

`${post_edited_translations.segment}`

```
/mybucket/important.doc
PUT#1 ---> OK
PUT#2 -----> OK
```

Situation B : Écrasements séquentiels terminés (protégés)

```
/mybucket/important.doc
PUT#1 -----> PUT#2 ---X (denied)
```

Informations connexes

- ["Comment les règles ILM de StorageGRID gèrent les objets"](#)
- ["\\${post_edited_translations.segment}"](#)
- ["Exemples de stratégies de groupe"](#)
- ["\\${post_edited_translations.segment}"](#)
- ["Gérez les objets avec ILM"](#)
- ["Utilisez un compte locataire"](#)

Exemple de stratégie de session de l'API REST StorageGRID S3

Utilisez l'exemple suivant pour créer une stratégie de session StorageGRID.

Exemple : Configurer une stratégie de session autorisant la récupération d'objets

Dans cet exemple, le principal de la session est uniquement autorisé à récupérer des objets du bucket1. Toutes les autres actions sont implicitement refusées, sauf pour les actions spécifiques à StorageGRID, telles que l'utilisation de la permission `"s3:PutOverwriteObject"`. La politique de session peut être fournie sous forme de fichier JSON lors de l'appel à l'API AssumeRole.

```
{
  "Statement": [
    {
      "Action": "s3:GetObject",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::bucket1/*"
    }
  ]
}
```

Exemples de stratégie de compartiment de l'API REST StorageGRID S3

Utilisez les exemples de cette section pour créer des politiques d'accès StorageGRID pour les compartiments.

Les stratégies de compartiment définissent les autorisations d'accès pour le compartiment auquel la stratégie est associée. Vous configurez une stratégie de compartiment à l'aide de l'API S3 PutBucketPolicy via l'un de ces outils :

- ["Gestionnaire de locataires"](#).
- AWS CLI en utilisant cette commande (voir ["Opérations sur les compartiments"](#)) :

```
> aws s3api put-bucket-policy --bucket examplebucket --policy
file://policy.json
```

Exemple : Autoriser tout le monde à accéder en lecture seule à un compartiment

Dans cet exemple, tout le monde, y compris les utilisateurs anonymes, est autorisé à lister les objets du compartiment et à effectuer des opérations GetObject sur tous les objets du compartiment. Toutes les autres opérations seront refusées. Notez que cette politique peut s'avérer peu utile, car seul le compte racine dispose des autorisations d'écriture 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 à tous les utilisateurs d'un compte un accès complet, et à tous les utilisateurs d'un autre compte un accès en lecture seule à un compartiment

Dans cet exemple, tous les membres d'un compte spécifié bénéficient d'un accès complet à un compartiment, tandis que tous les membres d'un autre compte spécifié sont uniquement autorisés à lister le compartiment et à effectuer des opérations GetObject sur les objets du compartiment commençant par le préfixe de clé de l'objet `shared/`.



Dans StorageGRID, les objets créés par un compte autre que le propriétaire (y compris les comptes anonymes) appartiennent au compte propriétaire du compartiment. La politique du 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 accorder un accès complet à un groupe spécifique

Dans cet exemple, tout le monde, y compris les utilisateurs anonymes, est autorisé à lister le compartiment et à effectuer des opérations GetObject sur tous les objets du compartiment, tandis que seuls les utilisateurs appartenant au groupe Marketing dans le compte spécifié bénéficient d'un accès complet.

```

{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/Marketing"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": ["s3:ListBucket", "s3:GetObject"],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}

```

Exemple : Autoriser à tous la lecture et l'écriture dans un bucket si le client se trouve dans la plage d'adresses IP

Dans cet exemple, toute personne, y compris anonyme, est autorisée à lister le bucket et à effectuer des opérations sur tous les objets du bucket, à condition que les requêtes proviennent d'une plage d'adresses 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 requêtes en dehors de la plage d'adresses 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 l'accès complet à un compartiment exclusivement à un utilisateur fédéré spécifié

Dans cet exemple, l'utilisateur fédéré Alex bénéficie d'un accès complet au `examplebucket` bucket et à ses objets. Tous les autres utilisateurs, y compris 'root', se voient explicitement refuser toutes les opérations. Notez cependant que 'root' ne se voit jamais refuser les autorisations de Put/Get/DeleteBucketPolicy.

```

{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Deny",
      "NotPrincipal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}

```

Exemple : autorisation PutOverwriteObject

Dans cet exemple, l'`Deny` effet 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 de l'objet S3.

```

{
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "s3:PutOverwriteObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion"
      ],
      "Resource": "arn:aws:s3:::wormbucket/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::wormbucket"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"
      },
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::wormbucket/*"
    }
  ]
}

```

Exemples de stratégie de groupe pour l'API REST S3 de StorageGRID

Utilisez les exemples de cette section pour créer des politiques d'accès StorageGRID pour les groupes.

Les stratégies de groupe définissent les autorisations d'accès du groupe auquel la stratégie est associée. Il n'y a pas d'Principal élément dans la stratégie car il est implicite. Les stratégies de groupe sont configurées à l'aide du Tenant Manager ou de l'API.

Exemple : Définir une stratégie de groupe à l'aide de Tenant Manager

Lorsque vous ajoutez ou modifiez un groupe dans le Tenant Manager, vous pouvez sélectionner une stratégie de groupe pour déterminer les autorisations d'accès S3 dont disposeront les membres de ce groupe. Voir ["Créer des groupes pour un locataire S3"](#).

- **Accès S3 interdit** : Option par défaut. Les utilisateurs de ce groupe n'ont pas accès aux ressources S3, sauf si l'accès est accordé par une stratégie de compartiment. Si vous sélectionnez cette option, seul l'utilisateur racine aura accès aux ressources S3 par défaut.
- **Accès en lecture seule** : Les utilisateurs de ce groupe disposent d'un accès en lecture seule aux ressources S3. Par exemple, les utilisateurs de ce groupe peuvent lister les objets et lire les données des objets, les métadonnées et les balises. Lorsque vous sélectionnez cette option, la chaîne JSON pour une stratégie de groupe en lecture seule apparaît dans la zone de texte. Vous ne pouvez pas modifier cette chaîne.
- **Accès complet** : Les utilisateurs de ce groupe disposent d'un accès complet aux ressources S3, y compris les compartiments. Lorsque vous sélectionnez cette option, la chaîne JSON de la stratégie de groupe d'accès complet s'affiche dans la zone de texte. Vous ne pouvez pas modifier cette chaîne.
- **Mesures de protection contre les ransomwares** : Cette stratégie s'applique à tous les compartiments de ce locataire. Les utilisateurs de ce groupe peuvent effectuer des actions courantes, mais ne peuvent pas supprimer définitivement d'objets des compartiments pour lesquels le versionnage des objets est activé.

Les utilisateurs de Tenant Manager disposant de l'autorisation « Manage all buckets » peuvent ignorer cette stratégie de groupe. Limitez l'autorisation « Manage all buckets » aux utilisateurs de confiance et utilisez l'authentification multifacteur (MFA) lorsque cela est possible.

- **Personnalisé** : Les utilisateurs du groupe reçoivent les autorisations que vous spécifiez dans la zone de texte.

Exemple : Accorder au groupe un accès complet à tous les compartiments

Dans cet exemple, tous les membres du groupe sont autorisés à accéder pleinement à tous les compartiments appartenant au compte du locataire, sauf interdiction explicite par la politique du 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 disposent d'un accès en lecture seule aux ressources S3, sauf interdiction explicite dans la stratégie du compartiment. Par exemple, les utilisateurs de ce groupe peuvent lister les objets et consulter les données, métadonnées et étiquettes des objets.

```

{
  "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 : Accorder aux membres d'un groupe un accès complet uniquement à leur « dossier » dans un compartiment

Dans cet exemple, les membres du groupe sont uniquement autorisés à consulter et à accéder à leur dossier spécifique (préfixe de clé) dans le compartiment indiqué. Notez que les autorisations d'accès provenant d'autres stratégies de groupe et de la stratégie du compartiment doivent être prises en compte pour déterminer la confidentialité de ces dossiers.

```

{
  "Statement": [
    {
      "Sid": "AllowListBucketOfASpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::department-bucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "${aws:username}/*"
        }
      }
    },
    {
      "Sid": "AllowUserSpecificActionsOnlyInTheSpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:*Object",
      "Resource": "arn:aws:s3:::department-bucket/${aws:username}/*"
    }
  ]
}

```

Opérations S3 suivies dans les journaux d'audit de StorageGRID

Les services StorageGRID génèrent des messages d'audit et les enregistrent dans des fichiers journaux texte. Vous pouvez consulter les messages d'audit spécifiques à S3 dans le journal des audits pour obtenir des détails sur les opérations de compartiment et d'objet.

`${post_edited_translations.segment}`

- CreateBucket
- DeleteBucket
- DeleteBucketTagging
- DeleteObjects
- GetBucketTagging
- HeadBucket
- ListObjects
- ListObjectVersions
- Conformité PUT Bucket
- PutBucketTagging
- PutBucketVersioning

Opérations sur les objets suivies dans les journaux des audits

- CompleteMultipartUpload
- CopyObject
- DeleteObject
- GetObject
- HeadObject
- PutObject
- RestoreObject
- SelectObject
- UploadPart (lorsqu'une règle ILM utilise l'ingestion équilibrée ou stricte)
- UploadPartCopy (lorsqu'une règle ILM utilise l'ingestion équilibrée ou stricte)

Informations connexes

- ["Accéder au fichier journal des audits"](#)
- ["\\${post_edited_translations.segment}"](#)
- ["Messages de journal des audits lus par le client"](#)

Utilisez l'API REST Swift (fin de vie)

Prise en charge de l'API REST Swift dans StorageGRID

La prise en charge de l'API Swift a atteint sa fin de vie et sera supprimée dans une prochaine version.



Les détails concernant Swift ont été supprimés de cette version du site de documentation. Voir ["StorageGRID 11.8 : Utilisez l'API REST Swift"](#).

Informations sur le copyright

Copyright © 2026 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

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

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

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

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

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

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

Informations sur les marques commerciales

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