Utilisation de S3

StorageGRID

NetApp
October 03, 2025

Sommaire

Utilisation de S3

Utiliser S3 : présentation

StorageGRID prend en charge l'API simple Storage Service (S3), qui est implémentée en tant que ensemble de services web REST (Representational State Transfer). La prise en charge de l'API REST S3 vous permet de connecter les applications orientées services développées pour les services web S3 avec un stockage objet sur site qui utilise le système StorageGRID. Pour ce faire, des modifications mineures doivent être apportées à l'utilisation actuelle des appels de l'API REST S3 d'une application client.

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

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

Relâchez	Commentaires
11.6	• Ajout de la prise en charge de l'utilisation du `partNumber` Paramètre de demande dans DEMANDES OBJET GET et objet TÊTE. • Ajout de la prise en charge d'un mode de conservation par défaut et d'une période de conservation par défaut au niveau du compartiment pour le verrouillage d'objet S3. • Prise en charge ajoutée de `s3:object-lock-remaining-retention-days` la touche condition de police permet de définir la plage de périodes de conservation autorisées pour vos objets. • La taille maximale *recommandée* pour une opération d'objet PUT unique est maintenant de 5 Gio (5,368,709,120 octets). Si vos objets sont supérieurs à 5 Gio, utilisez le téléchargement partitionné. ⓘ Dans StorageGRID 11.6, la taille maximale *supportée* pour une opération put Object est de 5 Tio (5,497,558,138,880 octets). Cependant, l'alerte **S3 PUT Object size trop importante** est déclenchée si vous tentez de télécharger un objet supérieur à 5 Gio.
11.5	• Ajout de la prise en charge de la gestion du chiffrement de compartiment. • Ajout de la prise en charge des demandes de verrouillage d'objet S3 et des demandes de conformité héritées obsolètes. • Ajout de la prise en charge de L'utilisation DE LA SUPPRESSION de plusieurs objets sur les compartiments multiversion. • Le `Content-MD5` l'en-tête de demande est désormais correctement pris en charge.

Relâchez	Commentaires
11.4	• Prise en charge accrue du balisage de compartiment, DE L'étiquetage DES compartiments ET DU balisage de compartiment. Les étiquettes d'allocation de coûts ne sont pas prises en charge. • Pour les compartiments créés dans StorageGRID 11.4, il n'est plus nécessaire de limiter les noms de clés d'objet pour respecter les bonnes pratiques de performance. • Ajout de la prise en charge des notifications de compartiment sur le `s3:ObjectRestore:Post` type d'événement. • Les limites de taille d'AWS pour les pièces partitionnés sont maintenant appliquées. Chaque partie d'un téléchargement partitionné doit être comprise entre 5 MIB et 5 Gio. La dernière partie peut être plus petite que 5 MIB. • Ajout de la prise en charge de TLS 1.3 et mise à jour de la liste des suites de chiffrement TLS prises en charge. • Le service CLB est obsolète.
11.3	• Ajout de la prise en charge du chiffrement côté serveur des données d'objet avec les clés fournies par le client (SSE-C). • Ajout de la prise en charge des opérations DE SUPPRESSION, D'OBTENTION et DE REMPLACEMENT du cycle de vie des compartiments (action d'expiration uniquement) et pour le `x-amz-expiration` en-tête de réponse. • PUT Object mis à jour, PUT Object - copie et Multipart Upload pour décrire l'impact des règles ILM utilisant un placement synchrone à l'entrée. • Liste mise à jour des suites de chiffrement TLS prises en charge. Les chiffrements TLS 1.1 ne sont plus pris en charge.
11.2	Ajout de la prise en charge de la restauration POST-objet pour l'utilisation avec les pools de stockage cloud. Ajout de la prise en charge de l'utilisation de la syntaxe AWS pour ARN, des clés de condition de règle et des variables de règles de groupe et de compartiment Les règles de compartiment et de groupe qui utilisent la syntaxe StorageGRID restent prises en charge. **Remarque :** les utilisations de l'ARN/URN dans d'autres configurations JSON/XML, y compris celles utilisées dans les fonctions StorageGRID personnalisées, n'ont pas changé.
11.1	Ajout de la prise en charge du partage de ressources d'origine croisée (CORS), des connexions client HTTP pour S3 aux nœuds de grille et des paramètres de conformité aux compartiments.
11.0	Ajout de la prise en charge de la configuration des services de plateforme (réplication CloudMirror, notifications et intégration de la recherche Elasticsearch) pour les compartiments Ajout également de la prise en charge des contraintes d'emplacement de balisage d'objets pour les compartiments, ainsi que du paramètre de contrôle de cohérence disponible.

Relâchez	Commentaires
10.4	Ajout de la prise en charge des modifications de l'analyse ILM sur la gestion des versions, mises à jour de la page noms de domaine de point final, conditions et variables dans les règles, exemples de règles et autorisation PutOverwriteObject.
10.3	Prise en charge ajoutée pour la gestion des versions.
10.2	Ajout de la prise en charge des règles d'accès de groupe et de compartiment, ainsi que de la copie multipart (Télécharger la pièce - copie).
10.1	Ajout de la prise en charge du téléchargement partitionné, des demandes de type hébergement virtuel et de l'authentification v4.
10.0	Prise en charge initiale de l'API REST S3 par le système StorageGRID.la version actuellement prise en charge de *simple Storage Service API Reference* est 2006-03-01.

Versions prises en charge

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

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

Informations associées

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

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

La prise en charge des services de plateforme StorageGRID

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

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

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

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

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

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

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

Informations associées

Utilisez le compte du locataire

Administrer StorageGRID

Opérations sur les compartiments

PUT Bucket metadata notification configuration

Configurez les comptes et les connexions des locataires

Pour configurer StorageGRID pour accepter les connexions à partir des applications

client, vous devez créer un ou plusieurs comptes de tenant et configurer les connexions.

Créez et configurez des comptes de locataire S3

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

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

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

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

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

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

Informations associées

Administrer StorageGRID

Utilisez le compte du locataire

Configuration des connexions client

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

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

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

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

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

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

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

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

2. Configurer des réseaux clients non fiables.

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

3. Configurez les groupes haute disponibilité.

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

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

Informations associées

Administrer StorageGRID

Résumé : adresses IP et ports pour les connexions client

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

Informations requises pour établir des connexions client

Le tableau récapitule les différentes façons dont les clients peuvent se connecter à StorageGRID ainsi que les

adresses IP et les ports utilisés pour chaque type de connexion. Contactez votre administrateur StorageGRID pour en savoir plus ou consultez les instructions d'administration de StorageGRID pour obtenir une description de la recherche de ces informations dans le Gestionnaire de grille.

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

Exemple

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

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

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

- `https://192.0.2.5:10443`

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

Informations associées

Administrer StorageGRID

Choisissez d'utiliser des connexions HTTPS ou HTTP

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

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

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

> Le service CLB est obsolète.

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

Informations associées

Administrer StorageGRID

Avantages des connexions HTTP actives, inactives et simultanées

Noms de domaine de terminaux pour les requêtes S3

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

Description de la tâche

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

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

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

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

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

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

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

Le service CLB est obsolète.

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

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

Informations associées

Administrer StorageGRID

Configuration de la sécurité pour l'API REST

Testez la configuration de l'API REST S3

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

Ce dont vous avez besoin

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

Étapes

1. Configurez les paramètres Amazon Web Services pour utiliser le compte que vous avez créé dans le système StorageGRID :
   a. Passer en mode configuration : `aws configure`
   b. Entrez l'ID de clé d'accès AWS pour le compte que vous avez créé.
   c. Entrez la clé d'accès secret AWS pour le compte que vous avez créé.
   d. Entrez la région par défaut à utiliser, par exemple US-East-1.
   e. Entrez le format de sortie par défaut à utiliser ou appuyez sur **entrée** pour sélectionner JSON.
2. Créer un compartiment.

```
aws s3api --endpoint-url https://10.96.101.17:10443
--no-verify-ssl create-bucket --bucket testbucket
```

Si le compartiment est créé avec succès, l'emplacement du compartiment est renvoyé, comme illustré dans l'exemple suivant :

```
"Location": "/testbucket"
```

1. Télécharger un objet.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
put-object --bucket testbucket --key s3.pdf --body C:\s3-
test\upload\s3.pdf
```

   Si l'objet est téléchargé avec succès, un ETAG est renvoyé, qui est un hachage des données de l'objet.

2. Répertorier le contenu du compartiment pour vérifier que l'objet a été téléchargé.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
list-objects --bucket testbucket
```

3. Supprimez l'objet.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-object --bucket testbucket --key s3.pdf
```

4. Supprimer le compartiment.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-bucket --bucket testbucket
```

Implémentation de l'API REST S3 par StorageGRID

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

Requêtes des clients en conflit

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

La chronologie de l'évaluation « derniers-victoires » repose sur la date à laquelle le système StorageGRID termine une demande donnée et non sur la date à laquelle les clients S3 commencent une opération.

Contrôles de cohérence

Les contrôles de cohérence assurent un équilibre entre la disponibilité des objets et la cohérence de ces objets entre plusieurs nœuds et sites de stockage, selon les exigences de votre application.

Par défaut, StorageGRID garantit la cohérence de lecture après écriture pour les nouveaux objets. Tout GET suivant un PUT réussi sera en mesure de lire les données nouvellement écrites. Les écrasements d'objets existants, les mises à jour de métadonnées et les suppressions sont cohérents. La propagation des écrasements ne prend généralement que quelques secondes ou minutes, mais peut prendre jusqu'à 15 jours.

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

Contrôles de cohérence

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

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

- **All** : tous les nœuds reçoivent immédiatement les données, sinon la demande échouera.
- **Forte-global**: Garantit la cohérence lecture-après-écriture pour toutes les demandes client sur tous les sites.
- **Site fort** : garantit la cohérence de lecture après écriture pour toutes les demandes de clients au sein d'un site.
- **Read-after-New-write**: (Par défaut) fournit la cohérence lecture-après-écriture pour les nouveaux objets et éventuellement la cohérence pour les mises à jour d'objets. Offre une haute disponibilité et une protection des données garanties. Recommandé dans la plupart des cas.
- **Disponible** : assure la cohérence finale pour les nouveaux objets et les mises à jour d'objets. Pour les compartiments S3, utilisez uniquement si nécessaire (par exemple, pour un compartiment qui contient des valeurs de journal rarement lues ou pour les opérations HEAD ou GET sur des clés qui n'existent pas). Non pris en charge pour les compartiments FabricPool S3.

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

Lorsqu'une OPÉRATION EN TÊTE ou GET utilise le contrôle de cohérence « en cas de nouvelle écriture », StorageGRID effectue la recherche en plusieurs étapes, comme suit :

- Il recherche tout d'abord l'objet à partir d'une faible cohérence.
- Si cette recherche échoue, elle répète la recherche au niveau de cohérence suivant jusqu'à ce qu'elle atteigne un niveau de cohérence équivalent au comportement de Strong-global.

Si une opération HEAD ou GET utilise le contrôle de cohérence « read-after-New-write », mais que l'objet n'existe pas, la recherche d'objets atteindra toujours un niveau de cohérence équivalent au comportement pour les groupes globaux forts. Ce niveau de cohérence exigeant la disponibilité de plusieurs copies des métadonnées d'objet sur chaque site, vous pouvez recevoir un nombre élevé d'erreurs de serveur interne 500 si un ou plusieurs nœuds de stockage sur le même site sont indisponibles.

À moins que vous n'ayez besoin de garanties de cohérence similaires à Amazon S3, vous pouvez empêcher ces erreurs de TÊTE et D'OBTENIR des opérations en définissant le contrôle de cohérence sur « disponible ». Lorsqu'une OPÉRATION DE TÊTE OU D'OBTENTION utilise le contrôle de cohérence « disponible », StorageGRID n'offre qu'une cohérence éventuelle. Elle n'essaie pas d'effectuer une opération ayant échoué à des niveaux de cohérence toujours plus élevés. Il n'est donc pas nécessaire que plusieurs copies des métadonnées de l'objet soient disponibles.

Spécifiez le contrôle de cohérence pour les opérations d'API

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

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

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

Contrôle de cohérence du compartiment

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

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

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

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

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

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

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

- **Strict** : toutes les copies spécifiées dans la règle ILM doivent être effectuées avant que le succès ne soit renvoyé au client.

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

> Avant de sélectionner le comportement d'ingestion d'une règle ILM, lisez la description complète de ces paramètres dans le Gestion des objets avec ILM.

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

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

- **Règle ILM** : créez deux copies d'objet, une sur le site local et une sur un site distant. Le comportement d'entrée strict est sélectionné.
- **Niveau de cohérence**: "Sept-global" (les métadonnées d'objet sont immédiatement distribuées à tous les sites).

Lorsqu'un client stocke un objet dans la grille, StorageGRID effectue à la fois des copies d'objet et distribue les métadonnées aux deux sites avant de rétablir la réussite du client.

L'objet est entièrement protégé contre la perte au moment du message d'ingestion. Par exemple, si le site local est perdu peu de temps après l'ingestion, des copies des données de l'objet et des métadonnées de l'objet existent toujours sur le site distant. L'objet est entièrement récupérable.

Si vous utilisez à la place la même règle ILM et le niveau de cohérence "sept-site", le client peut recevoir un message de réussite après la réplication des données d'objet vers le site distant, mais avant que les métadonnées d'objet ne soient distribuées sur ce site. Dans ce cas, le niveau de protection des métadonnées d'objet ne correspond pas au niveau de protection des données d'objet. Si le site local est perdu peu de temps après l'ingestion, les métadonnées d'objet sont perdues. L'objet ne peut pas être récupéré.

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

Informations associées

DEMANDE de cohérence des compartiments

PUT Bucket Consistency demandée

Gestion des objets par les règles StorageGRID ILM

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

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

- **Géographie**

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

de stockage cloud.

- **Grade de stockage**

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

- * Protection contre les pertes*

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

- * Rétention*

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

- * Protection pendant l'ingestion*

  Méthode de protection des données d'objet lors de l'ingestion : placement synchrone (avec options équilibrées ou strictes pour le comportement d'ingestion) ou copies intermédiaires (avec l'option de double validation).

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

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

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

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

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

Informations associées

Utilisez le compte du locataire

Gestion des objets avec ILM

DEMANDE de temps de dernier accès au compartiment

Gestion des versions d'objet

Vous pouvez utiliser la gestion des versions pour conserver plusieurs versions d'un objet, ce qui vous protège contre la suppression accidentelle d'objets et vous permet d'extraire et de restaurer les versions antérieures d'un objet.

Le système StorageGRID implémente la gestion des versions avec prise en charge de la plupart des fonctionnalités et avec certaines limites. StorageGRID prend en charge jusqu'à 1,000 versions de chaque objet.

Le contrôle de version d'objets peut être associé à la gestion du cycle de vie des informations (ILM) d'StorageGRID ou à la configuration du cycle de vie des compartiments S3. Vous devez activer explicitement la gestion des versions pour chaque compartiment pour activer cette fonctionnalité. Chaque objet du compartiment est associé à un ID de version, généré par le système StorageGRID.

La suppression de l'authentification multifacteur (MFA) n'est pas prise en charge.

> Le contrôle de version ne peut être activé que pour les compartiments créés avec StorageGRID version 10.3 ou ultérieure.

ILM et gestion des versions

Les règles ILM sont appliquées à chaque version d'un objet. Un processus d'analyse ILM analyse en continu tous les objets, puis les évalue à nouveau en fonction de la règle ILM actuelle. Toute modification apportée aux règles ILM est appliquée à tous les objets précédemment ingérées. Ceci inclut les versions préalablement ingérées si la gestion des versions est activée. L'analyse ILM applique les modifications de l'ILM aux objets précédemment ingérées.

Pour les objets S3 dans des compartiments activés pour la gestion des versions, la prise en charge du contrôle de version vous permet de créer des règles ILM qui utilisent l'heure actuelle non sélectionnée comme heure de référence. Lorsqu'un objet est mis à jour, ses versions précédentes deviennent non actuelles. L'utilisation d'un filtre de temps non actuel vous permet de créer des règles qui réduisent l'impact sur le stockage des versions précédentes d'objets.

> Lorsque vous téléchargez une nouvelle version d'un objet à l'aide d'une opération de téléchargement partitionné, l'heure qui n'est pas à jour pour la version d'origine de l'objet correspond à la création du téléchargement partitionné pour la nouvelle version, et non à la fin du téléchargement partitionné. Dans des cas limités, l'heure non actuelle de la version d'origine peut être des heures ou des jours plus tôt que l'heure de la version actuelle.

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

Informations associées

Gestion des objets avec ILM

Recommandations pour l'implémentation de l'API REST S3

Suivez ces recommandations lors de l'implémentation de l'API REST S3 pour une utilisation avec StorageGRID.

Recommandations pour les têtes à des objets inexistants

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

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

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

Recommandations pour les clés d'objet

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

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

- Vous ne devez pas utiliser de valeurs aléatoires comme les quatre premiers caractères des clés d'objet. Cela contraste avec l'ancienne recommandation AWS pour les préfixes de clés. Au lieu de cela, vous devez utiliser des préfixes non aléatoires et non uniques, tels que `image`.
- Si vous suivez l'ancienne recommandation AWS pour utiliser des caractères aléatoires et uniques dans les préfixes de clés, vous devez préfixer les clés d'objet avec un nom de répertoire. C'est-à-dire, utilisez le format suivant :

  ```
  mybucket/mydir/f8e3-image3132.jpg
  ```

  Au lieu de ce format :

  ```
  mybucket/f8e3-image3132.jpg
  ```

Recommandations pour « plages de lectures »

Si l'option **Compress Stored Objects** est sélectionnée (**CONFIGURATION système Grid options**), les applications client S3 doivent éviter d'effectuer des opérations GET Object qui indiquent une plage d'octets. Ces opérations de « lecture à plage » sont inefficaces, car StorageGRID doit décompresser efficacement les objets pour accéder aux octets demandés. LES opérations GET Object qui demandent une petite plage d'octets provenant d'un objet très volumineux sont particulièrement inefficaces. Par exemple, il est très inefficace de lire une plage de 10 Mo à partir d'un objet compressé de 50 Go.

Si les plages sont lues à partir d'objets compressés, les demandes client peuvent être en attente.

> Si vous devez compresser des objets et que votre application client doit utiliser des lectures de plage, augmentez le délai de lecture de l'application.

Informations associées

- Contrôles de cohérence
- PUT Bucket Consistency demandée
- Administrer StorageGRID

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

Le système StorageGRID implémente l'API simple Storage Service (API version 2006-03-01) avec la prise en charge de la plupart des opérations et avec certaines limites. Vous devez connaître les détails d'implémentation lorsque vous intégrez des applications client de l'API REST S3.

Le système StorageGRID prend en charge les demandes de type hébergement virtuel et les demandes de type chemin d'accès.

Traitement de la date

L'implémentation StorageGRID de l'API REST S3 ne prend en charge que les formats de date HTTP valides.

Le système StorageGRID prend uniquement en charge les formats de date HTTP valides pour tous les en-têtes qui acceptent les valeurs de date. La partie heure de la date peut être spécifiée au format heure de Greenwich (GMT) ou au format heure coordonnée universelle (UTC) sans décalage de fuseau horaire (+0000 doit être spécifié). Si vous incluez le `x-amz-date` En-tête de votre demande, elle remplace toute valeur spécifiée dans l'en-tête de la demande de date. Lors de l'utilisation de la signature AWS version 4, le `x-amz-date` l'en-tête doit être présent dans la demande signée car l'en-tête de date n'est pas pris en charge.

En-têtes de demande commune

Le système StorageGRID prend en charge les en-têtes de demande courants définis par le "Documentation Amazon Web Services (AWS) : référence de l'API Amazon simple Storage Service", à une exception près.

En-tête de demande	Mise en place
Autorisation	Prise en charge complète de la signature AWS version 2 Prise en charge de la signature AWS version 4, à l'exception des cas suivants : • La valeur SHA256 n'est pas calculée pour le corps de la demande. La valeur soumise par l'utilisateur est acceptée sans validation, comme si la valeur `UNSIGNED-PAYLOAD` avait été prévu pour le `x-amz-content-sha256` en-tête.

En-tête de demande	Mise en place
jeton de sécurité x-amz	Non mis en œuvre. Retours `XNotImplemented`.

En-têtes de réponse commune

Le système StorageGRID prend en charge tous les en-têtes de réponse courants définis par l'API *simple Storage Service Reference*, à une exception près.

En-tête de réponse	Mise en place
x-amz-id-2	Non utilisé

Authentifier les demandes

Le système StorageGRID prend en charge l'accès authentifié et anonyme aux objets à l'aide de l'API S3.

L'API S3 prend en charge la version 2 de Signature et la version 4 de Signature pour authentifier les requêtes API S3.

Les demandes authentifiées doivent être signées à l'aide de votre ID de clé d'accès et de votre clé secrète d'accès.

Le système StorageGRID prend en charge deux méthodes d'authentification : le protocole HTTP `Authorization` en-tête et utilisation des paramètres de requête.

Utilisez l'en-tête HTTP Authorization

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

Utiliser les paramètres de requête

Vous pouvez utiliser les paramètres de requête pour ajouter des informations d'authentification à une URL. Il s'agit de la présignature de l'URL, qui peut être utilisée pour accorder un accès temporaire à des ressources spécifiques. Les utilisateurs disposant de l'URL présignée n'ont pas besoin de connaître la clé d'accès secrète pour accéder à la ressource, ce qui vous permet de fournir un accès restreint à une ressource par des tiers.

Opérations sur le service

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

Fonctionnement	Mise en place
ACCÉDER au service	Mise en œuvre avec tout le comportement de l'API REST Amazon S3.

Fonctionnement	Mise en place
DÉCOUVREZ l'utilisation du stockage	La demande GET Storage usage vous indique la quantité totale de stockage utilisée par un compte et pour chaque compartiment associé au compte. Il s'agit d'une opération sur le service avec un chemin de / et un paramètre de requête personnalisé (`?x-ntap-sg-usage`) ajouté.
OPTIONS /	Les applications client peuvent émettre `OPTIONS /` Requêtes vers le port S3 d'un nœud de stockage, sans identifiants d'authentification S3, pour déterminer si le nœud de stockage est disponible. Vous pouvez utiliser cette requête pour la surveillance ou permettre aux équilibreurs de charge externes d'identifier lorsqu'un nœud de stockage est arrêté.

Informations associées

DEMANDE d'utilisation du stockage

Opérations sur les compartiments

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

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

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

Configurez les noms de domaine de terminaux API S3

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

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

Le tableau suivant décrit la façon dont StorageGRID implémente les opérations des compartiments de l'API REST S3. Pour effectuer l'une de ces opérations, les informations d'identification d'accès nécessaires doivent être fournies pour le compte.

Fonctionnement	Mise en place
SUPPRIMER le compartiment	Mise en œuvre avec tout le comportement de l'API REST Amazon S3.
SUPPRIMER les godets	Cette opération supprime la configuration CORS pour le compartiment.

Fonctionnement	Mise en place
SUPPRIMER le chiffrement du compartiment	Cette opération supprime le chiffrement par défaut du compartiment. Les objets chiffrés existants restent chiffrés, mais tous les nouveaux objets ajoutés au compartiment ne sont pas chiffrés.
SUPPRIMER le cycle de vie du compartiment	Cette opération supprime la configuration du cycle de vie du compartiment.
SUPPRIMER la règle de compartiment	Cette opération supprime la règle attachée au compartiment.
SUPPRIMER la réplication du compartiment	Cette opération supprime la configuration de réplication attachée au compartiment.
SUPPRIMER le balisage du compartiment	Cette opération utilise le `tagging` sous-ressource pour supprimer toutes les balises d'un compartiment.
GET Bucket (List Objects), version 1 et version 2	Cette opération renvoie une partie ou la totalité (jusqu'à 1,000) des objets dans un godet. La classe de stockage pour les objets peut avoir l'une ou l'autre des deux valeurs, même si l'objet a été ingéré avec le `REDUCED_REDUNDANCY` option de classe de stockage : • `STANDARD`, Qui indique que l'objet est stocké dans un pool de stockage composé de nœuds de stockage. • `GLACIER`, Qui indique que l'objet a été déplacé vers le compartiment externe spécifié par le pool de stockage cloud. Si le compartiment contient un grand nombre de clés supprimées qui ont le même préfixe, la réponse peut inclure une partie `CommonPrefixes` ne contenant pas de clés.
OBTENIR l'acl du compartiment	Cette opération renvoie une réponse positive et l'ID, le DisplayName et l'autorisation du propriétaire du compartiment, indiquant que le propriétaire a un accès complet au compartiment.
OBTENIR les godets	Cette opération renvoie le `cors` configuration du compartiment.
CHIFFREMENT des compartiments	Cette opération renvoie la configuration de cryptage par défaut pour le compartiment.
OPTIMISEZ le cycle de vie des compartiments	Cette opération retourne la configuration du cycle de vie du godet.
ACCÉDER à l'emplacement du compartiment	Cette opération renvoie la région définie à l'aide de `LocationConstraint` Élément dans la demande PUT Bucket. Si la région du godet est de `us-east-1`, une chaîne vide est renvoyée pour la région.

Fonctionnement	Mise en place
GET Bucket notification	Cette opération renvoie la configuration de notification attachée au compartiment.
OBTENIR les versions d'objet de compartiment	Avec accès EN LECTURE sur un godet, cette opération avec le `versions` sous-ressource répertorie les métadonnées de toutes les versions des objets dans le compartiment.
GET Bucket policy	Cette opération renvoie la politique attachée au godet.
RÉPLICATION des compartiments	Cette opération renvoie la configuration de réplication attachée au compartiment.
GET Bucket tagging	Cette opération utilise le `tagging` sous-ressource pour renvoyer toutes les balises d'un compartiment.
GESTION des versions des compartiments	Cette implémentation utilise le `versioning` sous-ressource pour retourner l'état de gestion des versions d'un compartiment. • *Blank*: La gestion des versions n'a jamais été activée (le compartiment est « non versionné ») • Activé : la gestion des versions est activée • Suspendu : la gestion des versions a déjà été activée et est suspendue
OBTENIR la configuration de verrouillage d'objet	Cette opération renvoie le mode de rétention par défaut du compartiment et la période de conservation par défaut, si configuré. Voir OBTENIR la configuration de verrouillage d'objet pour des informations détaillées.
Godet DE TÊTE	Cette opération détermine si un compartiment existe et que vous êtes autorisé à y accéder. Cette opération renvoie : • `x-ntap-sg-bucket-id`: L'UUID du godet au format UUID. • `x-ntap-sg-trace-id`: ID de trace unique de la demande associée.

Fonctionnement	Mise en place
PLACER le godet	Cette opération crée un nouveau godet. C'est en créant le compartiment que vous devenez le propriétaire. • Les noms de compartiment doivent être conformes aux règles suivantes : ◦ Il doit être unique sur chaque système StorageGRID (et pas seulement au sein du compte du locataire). ◦ Doit être conforme DNS. ◦ Doit contenir au moins 3 caractères et pas plus de 63 caractères. ◦ Peut être une série d'une ou plusieurs étiquettes, avec des étiquettes adjacentes séparées par un point. Chaque étiquette doit commencer et se terminer par une lettre ou un chiffre en minuscules et ne peut utiliser que des lettres minuscules, des chiffres et des tirets. ◦ Ne doit pas ressembler à une adresse IP au format texte. ◦ Ne doit pas utiliser de périodes dans des demandes de type hébergement virtuel. Les périodes provoquera des problèmes avec la vérification du certificat générique du serveur. • Par défaut, les compartiments sont créés dans le `us-east-1` région ; cependant, vous pouvez utiliser le `LocationConstraint` élément de demande dans le corps de la demande pour spécifier une région différente. Lorsque vous utilisez le `LocationConstraint` Elément, vous devez spécifier le nom exact d'une région qui a été définie à l'aide du gestionnaire de grille ou de l'API de gestion de grille. Contactez votre administrateur système si vous ne connaissez pas le nom de région que vous devez utiliser. **Remarque** : une erreur se produit si votre demande PUT Bucket utilise une région qui n'a pas été définie dans StorageGRID. • Vous pouvez inclure le `x-amz-bucket-object-lock-enabled` Demander l'en-tête pour créer un compartiment avec le verrouillage objet S3 activé. Voir Utilisez le verrouillage d'objet S3. Vous devez activer le verrouillage d'objet S3 lors de la création du compartiment. Vous ne pouvez pas ajouter ou désactiver le verrouillage d'objet S3 après la création d'un compartiment. Le verrouillage objet S3 requiert la gestion des versions de compartiment, qui est activée automatiquement lors de la création du compartiment.
PLACEZ les godets	Cette opération définit la configuration du CORS pour un compartiment afin que le compartiment puisse traiter les demandes d'origine croisée. Le partage de ressources d'origine croisée (CORS) est un mécanisme de sécurité qui permet aux applications Web clientes d'un domaine d'accéder aux ressources d'un domaine différent. Supposons par exemple que vous utilisez un compartiment S3 nommé `images` pour stocker des graphiques. En définissant la configuration CORS pour le `images` le champ permet d'afficher les images de ce compartiment sur le site web `http://www.example.com`.

Fonctionnement	Mise en place
PUT Bucket Encryption	Cette opération définit l'état de cryptage par défaut d'un compartiment existant. Lorsque le chiffrement au niveau du compartiment est activé, tout nouvel objet ajouté au compartiment est chiffré.StorageGRID prend en charge le chiffrement côté serveur avec des clés gérées par StorageGRID. Lorsque vous spécifiez la règle de configuration de cryptage côté serveur, définissez l' `SSEAlgorithm` paramètre à `AES256`, et n'utilisez pas le `KMSMasterKeyID` paramètre. La configuration de cryptage par défaut du compartiment est ignorée si la demande de téléchargement d'objet spécifie déjà le cryptage (c'est-à-dire, si la demande inclut le `x-amz-server-side-encryption-*` en-tête de demande).
CYCLE de vie des compartiments	Cette opération crée une nouvelle configuration de cycle de vie pour le compartiment ou remplace une configuration de cycle de vie existante. StorageGRID prend en charge jusqu'à 1,000 règles de cycle de vie dans une configuration cycle de vie. Chaque règle peut inclure les éléments XML suivants : • Expiration (jours, date) • NonactuelVersionExp (Nontactut Days) • Filtre (préfixe, étiquette) • État • ID StorageGRID ne prend pas en charge les actions suivantes : • AbortIncompleMultipartUpload • ExpiredObjectDeleteMarker • Transition Pour comprendre comment l'action expiration dans un cycle de vie de compartiment interagit avec les instructions de placement ILM, reportez-vous à la section « fonctionnement de l'ILM tout au long de la vie d'un objet » dans les instructions de gestion des objets avec la gestion du cycle de vie des informations. **Remarque** : la configuration du cycle de vie des compartiments peut être utilisée avec des compartiments avec le verrouillage d'objet S3 activé, mais la configuration du cycle de vie des compartiments n'est pas prise en charge pour les compartiments conformes hérités.

Fonctionnement	Mise en place

PUT Bucket notification	Cette opération configure les notifications pour le compartiment à l'aide du XML de configuration de notification inclus dans le corps de la demande. Vous devez connaître les détails d'implémentation suivants :
	
	• StorageGRID prend en charge les rubriques SNS (simple notification Service) comme destinations. Les terminaux SQS (simple Queue Service) ou Amazon Lambda ne sont pas pris en charge.
	• La destination des notifications doit être spécifiée comme URN d'un terminal StorageGRID. Les terminaux peuvent être créés à l'aide du Gestionnaire de locataires ou de l'API de gestion des locataires.
	
	Le noeud final doit exister pour que la configuration des notifications réussisse. Si le noeud final n'existe pas, un `400 Bad Request` l'erreur est renvoyée avec le code `InvalidArgument`.
	
	• Vous ne pouvez pas configurer une notification pour les types d'événements suivants. Ces types d'événements sont **non** pris en charge.
	
	◦ `s3:ReducedRedundancyLostObject`
	
	◦ `s3:ObjectRestore:Completed`
	
	• Les notifications d'événements envoyées par StorageGRID utilisent le format JSON standard, sauf qu'elles n'incluent pas certaines clés et utilisent des valeurs spécifiques pour les autres, comme illustré dans la liste ci-dessous :
	• **EventSource**
	
	`sgws:s3`
	
	• **AwsRegion**
	
	non inclus
	
	• **x-amz-id-2**
	
	non inclus
	
	• **arn**
	
	`urn:sgws:s3:::bucket_name`

PUT Bucket policy	Cette opération définit la politique associée au compartiment.

Fonctionnement	Mise en place
RÉPLICATION des compartiments	Cette opération configure la réplication StorageGRID CloudMirror pour le compartiment à l'aide du XML de configuration de réplication fourni dans le corps de la demande. Pour la réplication CloudMirror, vous devez connaître les détails d'implémentation suivants : • StorageGRID ne prend en charge que le V1 de la configuration de la réplication. Cela signifie que StorageGRID ne prend pas en charge l'utilisation de `Filter` Elément pour les règles, et suit les conventions V1 pour la suppression des versions d'objet. Pour plus d'informations, reportez-vous à la "Documentation Amazon S3 sur la configuration de la réplication". • La réplication des compartiments peut être configurée sur les compartiments avec ou sans version. • Vous pouvez spécifier un compartiment de destination différent dans chaque règle du XML de configuration de réplication. Un compartiment source peut être répliqué sur plusieurs compartiments de destination. • Les compartiments de destination doivent être spécifiés en tant que URN des terminaux StorageGRID, tel que spécifié dans le Gestionnaire de locataires ou l'API de gestion des locataires. Le noeud final doit exister pour que la configuration de réplication réussisse. Si le noeud final n'existe pas, la demande échoue en tant que `400 Bad Request`. Le message d'erreur indique : `Unable to save the replication policy. The specified endpoint URN does not exist: URN`. • Il n'est pas nécessaire de spécifier un `Role` Dans le XML de configuration. Cette valeur n'est pas utilisée par StorageGRID et sera ignorée si elle a été soumise. • Si vous omettez la classe de stockage du XML de configuration, StorageGRID utilise le `STANDARD` classe de stockage par défaut. • Si vous supprimez un objet du compartiment source ou que vous supprimez le compartiment source lui-même, le comportement de réplication inter-région est le suivant : ◦ Si vous supprimez l'objet ou le compartiment avant sa réplication, l'objet/le compartiment n'est pas répliqué et vous n'êtes pas averti. ◦ Si vous supprimez l'objet ou le compartiment après sa réplication, StorageGRID suit le comportement de suppression Amazon S3 standard pour la version V1 de la réplication multi-région.

Fonctionnement	Mise en place
PUT Bucket tagging	Cette opération utilise le `tagging` sous-ressource pour ajouter ou mettre à jour un ensemble de balises pour un compartiment. Lors de l'ajout de balises de compartiment, tenez compte des limites suivantes : • StorageGRID et Amazon S3 prennent en charge jusqu'à 50 balises pour chaque compartiment. • Les étiquettes associées à un compartiment doivent avoir des clés d'étiquette uniques. Une clé de balise peut comporter jusqu'à 128 caractères Unicode. • Les valeurs de balise peuvent comporter jusqu'à 256 caractères Unicode. • Les clés et les valeurs sont sensibles à la casse
GESTION des versions du compartiment	Cette implémentation utilise le `versioning` sous-ressource pour définir l'état de gestion des versions d'un compartiment existant. Vous pouvez définir l'état de la gestion des versions à l'aide de l'une des valeurs suivantes : • Activé : permet la gestion des versions des objets dans le compartiment. Tous les objets ajoutés au compartiment reçoivent un ID de version unique. • Suspendu : désactive la gestion des versions des objets dans le compartiment. Tous les objets ajoutés au compartiment reçoivent l'ID de version `null`.
CONFIGURATION du verrouillage de l'objet	Cette opération configure ou supprime le mode de conservation par défaut du compartiment et la période de conservation par défaut. Si la période de conservation par défaut est modifiée, la conservation jusqu'à la date des versions d'objet existantes reste la même et n'est pas recalculée en utilisant la nouvelle période de conservation par défaut. Voir CONFIGURATION du verrouillage de l'objet pour des informations détaillées.

Informations associées

Contrôles de cohérence

DEMANDE DE dernier accès au compartiment

Règles d'accès au compartiment et au groupe

Opérations S3 suivies dans les journaux d'audit

Gestion des objets avec ILM

Utilisez le compte du locataire

Création de la configuration du cycle de vie S3

Vous pouvez créer une configuration de cycle de vie S3 afin de contrôler la suppression d'objets spécifiques du système StorageGRID.

L'exemple simple de cette section illustre la façon dont une configuration du cycle de vie S3 peut contrôler la suppression de certains objets (expirés) dans des compartiments S3 spécifiques. L'exemple de cette section est fourni à titre d'illustration uniquement. Pour plus d'informations sur la création de configurations de cycle de vie S3, reportez-vous à la section "Amazon simple Storage Service Developer Guide : gestion du cycle de vie des objets". Notez que StorageGRID prend uniquement en charge les actions d'expiration, mais pas les actions de transition.

La configuration du cycle de vie

La configuration du cycle de vie est un ensemble de règles appliquées aux objets dans des compartiments S3 spécifiques. Chaque règle indique quels objets sont affectés et quand ces objets vont expirer (à une date spécifique ou après un certain nombre de jours).

StorageGRID prend en charge jusqu'à 1,000 règles de cycle de vie dans une configuration cycle de vie. Chaque règle peut inclure les éléments XML suivants :

- Expiration : supprimez un objet lorsqu'une date spécifiée est atteinte ou lorsqu'un nombre de jours spécifié est atteint, à partir de l'ingestion de l'objet.
- NonactuelVersionExexpiration : supprimez un objet lorsque le nombre de jours spécifié est atteint, à partir de quand l'objet est devenu non courant.
- Filtre (préfixe, étiquette)
- État
- ID

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

Par conséquent, il est possible de supprimer un objet de la grille, même si les instructions de placement d'une règle ILM s'appliquent toujours à l'objet. Il est également possible de conserver un objet dans la grille même après l'expiration des instructions de placement ILM de l'objet. Pour plus de détails, voir Fonctionnement de ILM tout au long de la vie d'un objet.

> La configuration du cycle de vie des compartiments avec des compartiments dont le verrouillage objet S3 est activé, mais la configuration du cycle de vie des compartiments n'est pas prise en charge pour les compartiments conformes.

StorageGRID prend en charge les opérations suivantes des compartiments pour gérer les configurations du cycle de vie :

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

Créer une configuration de cycle de vie

Comme première étape de la création de la configuration du cycle de vie, vous créez un fichier JSON qui inclut une ou plusieurs règles. Par exemple, ce fichier JSON contient trois règles, comme suit :

1. La règle 1 s'applique uniquement aux objets qui correspondent au préfixe `category1/` et qui ont un `key2` valeur de `tag2`. Le `Expiration` Le paramètre spécifie que les objets correspondant au filtre expireront à

minuit le 22 août 2020.

2. La règle 2 s'applique uniquement aux objets qui correspondent au préfixe `category2/`. Le `Expiration` le paramètre indique que les objets correspondant au filtre expirent 100 jours après leur ingestion.

   > Les règles spécifiant un nombre de jours sont relatives à l'ingestion de l'objet. Si la date actuelle dépasse la date d'ingestion et le nombre de jours, certains objets peuvent être supprimés du compartiment dès que la configuration de cycle de vie est appliquée.

3. La règle 3 s'applique uniquement aux objets qui correspondent au préfixe `category3/`. Le `Expiration` paramètre spécifie que toute version non actuelle des objets de correspondance expirera 50 jours après leur non-mise à jour.

```
{
    "Rules": [
        {
            "ID": "rule1",
            "Filter": {
                "And": {
                    "Prefix": "category1/",
                    "Tags": [
                        {
                            "Key": "key2",
                            "Value": "tag2"
                        }
                    ]
                }
            },
            "Expiration": {
                "Date": "2020-08-22T00:00:00Z"
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule2",
            "Filter": {
                "Prefix": "category2/"
            },
            "Expiration": {
                "Days": 100
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule3",
            "Filter": {
                "Prefix": "category3/"
            },
            "NoncurrentVersionExpiration": {
                "NoncurrentDays": 50
            },
            "Status": "Enabled"
        }
    ]
}
```

Appliquez la configuration du cycle de vie au compartiment

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

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

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

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

```
aws s3api --endpoint-url <StorageGRID endpoint> get-bucket-lifecycle-
configuration
 --bucket testbucket
```

Une réponse réussie répertorie la configuration de cycle de vie que vous venez d'appliquer.

Vérifiez que l'expiration du cycle de vie du compartiment s'applique à l'objet

Vous pouvez déterminer si une règle d'expiration dans la configuration de cycle de vie s'applique à un objet spécifique lors de l'émission d'une requête D'objet PUT, HEAD Object ou GET Object. Si une règle s'applique, la réponse comprend un `Expiration` paramètre qui indique quand l'objet expire et quelle règle d'expiration a été mise en correspondance.

> Le cycle de vie des compartiments ignore ILM, le `expiry-date` l'illustration représente la date réelle à laquelle l'objet sera supprimé. Pour plus de détails, voir Méthode de détermination de la conservation des objets.

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

```
aws s3api --endpoint-url <StorageGRID endpoint> put-object
--bucket testbucket --key obj2test2 --body bktjson.json
```

La réponse de réussite indique que l'objet expirera dans 100 jours (01 oct 2020) et qu'il correspond à la règle 2 de la configuration de cycle de vie.

```
{
      *"Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:49 GMT\", rule-
id=\"rule2\"",
      "ETag": "\"9762f8a803bc34f5340579d4446076f7\""
}
```

Par exemple, cette demande d'objet TÊTE a été utilisée pour obtenir les métadonnées du même objet dans le compartiment test.

```
aws s3api --endpoint-url <StorageGRID endpoint> head-object
--bucket testbucket --key obj2test2
```

La réponse de réussite inclut les métadonnées de l'objet et indique que l'objet expirera dans 100 jours et qu'il correspond à la règle 2.

```
{
      "AcceptRanges": "bytes",
      *"Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:48 GMT\", rule-
id=\"rule2\"",
      "LastModified": "2020-06-23T09:07:48+00:00",
      "ContentLength": 921,
      "ETag": "\"9762f8a803bc34f5340579d4446076f7\""
      "ContentType": "binary/octet-stream",
      "Metadata": {}
}
```

Utilisez la conservation de compartiment par défaut avec le verrouillage d'objet S3

Si le verrouillage objet S3 est activé pour un compartiment, vous pouvez spécifier un mode de conservation par défaut et une période de conservation par défaut qui est appliquée à chaque objet ajouté au compartiment.

- Le verrouillage objet S3 peut être activé ou désactivé pour un compartiment lors de la création du compartiment.
- Si le verrouillage objet S3 est activé pour un compartiment, vous pouvez configurer la conservation par défaut pour ce compartiment.
- La configuration de conservation par défaut spécifie :
  - Mode de rétention par défaut : StorageGRID ne prend en charge que le mode de « CONFORMITÉ ».
  - Durée de conservation par défaut en jours ou années.

OBTENIR la configuration de verrouillage d'objet

La demande GET Object Lock Configuration vous permet de déterminer si le verrouillage d'objet est activé pour un compartiment et, s'il est activé, de voir si un mode de rétention par défaut et une période de rétention

sont configurés pour le compartiment.

Lorsque de nouvelles versions d'objet sont ingérées sur le compartiment, le mode de conservation 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 de conservation si `x-amz-object-lock-retain-until-date` n'est pas spécifié.

Pour effectuer cette opération, vous devez disposer de l'autorisation s3:GetBucketObjectLockConfiguration, ou être root de compte.

Exemple de demande

```
GET /bucket?object-lock HTTP/1.1
Host: host
Accept-Encoding: identity
User-Agent: aws-cli/1.18.106 Python/3.8.2 Linux/4.4.0-18362-Microsoft
botocore/1.17.29
x-amz-date: date
x-amz-content-sha256: authorization string
Authorization: authorization string
```

Exemple de réponse

```
HTTP/1.1 200 OK
x-amz-id-2:
iVmcB7OXXJRkRH1FiVq1151/T24gRfpwpuZrEG11Bb9ImOMAAe98oxSpXlknabA0LTvBYJpSIX
k=
x-amz-request-id: B34E94CACB2CEF6D
Date: Fri, 04 Sep 2020 22:47:09 GMT
Transfer-Encoding: chunked
Server: AmazonS3

<?xml version="1.0" encoding="UTF-8"?>
<ObjectLockConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
    <ObjectLockEnabled>Enabled</ObjectLockEnabled>
    <Rule>
        <DefaultRetention>
            <Mode>COMPLIANCE</Mode>
            <Years>6</Years>
        </DefaultRetention>
    </Rule>
</ObjectLockConfiguration>
```

CONFIGURATION du verrouillage de l'objet

La demande DE configuration DE verrouillage D'objet PUT vous permet de modifier le mode de conservation par défaut et la période de conservation par défaut pour un compartiment dont le verrouillage d'objet est

activé. Vous pouvez également supprimer les paramètres de conservation par défaut configurés précédemment.

Lorsque de nouvelles versions d'objet sont ingérées sur le compartiment, le mode de conservation 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 de conservation 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 conservation à la date de la version de l'objet reste la même et n'est pas recalculée en utilisant la nouvelle période de conservation par défaut.

Pour effectuer cette opération, vous devez disposer de l'autorisation s3:PutBuckObjectLockConfiguration, ou être root de compte.

Le `Content-MD5` L'en-tête de demande doit être spécifié dans la demande PUT.

Exemple de demande

```
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>
```

Opérations personnalisées dans les compartiments

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

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

Fonctionnement	Description	Pour en savoir plus
OPTIMISEZ la cohérence des compartiments	Renvoie le niveau de cohérence appliqué à un compartiment spécifique.	DEMANDE de cohérence des compartiments
PRÉSERVER la cohérence du godet	Définit le niveau de cohérence appliqué à un compartiment spécifique.	PUT Bucket Consistency demandée
HEURE du dernier accès au compartiment	Indique si les mises à jour de l'heure du dernier accès sont activées ou désactivées pour un compartiment spécifique.	DEMANDE DE dernier accès au compartiment
METTRE l'heure du dernier accès au compartiment	Permet d'activer ou de désactiver les mises à jour de l'heure du dernier accès pour un compartiment spécifique.	DEMANDE de temps de dernier accès au compartiment
SUPPRIMEZ la configuration de notification des métadonnées de compartiment	Supprime le XML de configuration de notification de métadonnées associé à un compartiment spécifique.	SUPPRIME la demande de configuration de notification des métadonnées de compartiment
CONFIGURATION DES notifications de métadonnées de compartiment	Renvoie le XML de configuration de notification de métadonnées associé à un compartiment spécifique.	LIRE la demande de configuration de notification des métadonnées de compartiment
CONFIGURATION de notification des métadonnées de compartiment	Configure le service de notification des métadonnées pour un compartiment.	PUT Bucket metadata notification configuration
PUT Bucket with Compliance settings	Obsolète et non pris en charge : vous ne pouvez plus créer de compartiments avec conformité activée.	Obsolète : METTEZ le compartiment avec les paramètres de conformité
ASSUREZ la conformité aux compartiments	Obsolète mais pris en charge : renvoie les paramètres de conformité actuellement en vigueur pour un compartiment compatible existant.	Obsolète : RÉCUPÉRER la demande de conformité du compartiment
METTEZ le godet en conformité	Obsolète mais pris en charge : permet de modifier les paramètres de conformité d'un compartiment compatible existant.	Obsolète : PUT Bucket Compliance request

Informations associées

Opérations S3 suivies dans les journaux d'audit

Opérations sur les objets

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

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

- StorageGRID contrôles de cohérence sont prises en charge par toutes les opérations sur les objets, à l'exception de ce qui suit :
  - OBTENIR l'ACL d'objet
  - `OPTIONS /`
  - METTRE l'objet en attente légale
  - CONSERVATION des objets
  - SÉLECTIONNEZ contenu de l'objet
- Les demandes contradictoires des clients, telles que deux clients qui écrivent sur la même clé, sont résolues sur une base de « derniers-victoires ». La chronologie de l'évaluation « Latest-WINS » dépend de la date à laquelle le système StorageGRID remplit une demande donnée et non du moment où les clients S3 commencent une opération.
- Tous les objets d'un compartiment StorageGRID sont détenus par le propriétaire du compartiment, y compris les objets créés par un utilisateur anonyme ou par un autre compte.
- Les objets de données ingérées sur le système StorageGRID via Swift ne sont pas accessibles via S3.

Le tableau ci-dessous décrit la manière dont StorageGRID implémente les opérations sur les objets de l'API REST S3.

Fonctionnement	Mise en place
SUPPRIMER l'objet	Authentification multifacteur (MFA) et en-tête de réponse `x-amz-mfa` ne sont pas pris en charge. Lors du traitement d'une requête DE SUPPRESSION d'objet, StorageGRID tente de supprimer immédiatement toutes les copies de l'objet des emplacements stockés. En cas de succès, StorageGRID renvoie immédiatement une réponse au client. Si toutes les copies ne peuvent pas être supprimées dans les 30 secondes (par exemple, si un emplacement est temporairement indisponible), StorageGRID met les copies en file d'attente pour suppression, puis indique que le client a réussi à les supprimer. **Gestion des versions** Pour supprimer une version spécifique, le demandeur doit être le propriétaire du compartiment et utiliser le `versionId` sous-ressource. L'utilisation de cette sous-ressource supprime définitivement la version. Si le `versionId` correspond à un marqueur de suppression, l'en-tête de réponse `x-amz-delete-marker` est renvoyé à `true`. • Si un objet est supprimé sans l' `versionId` sous-ressource sur un compartiment activé pour la version, il génère un marqueur de suppression. Le `versionId` pour le marqueur de suppression, est renvoyé à l'aide du `x-amz-version-id` en-tête de réponse, et le `x-amz-delete-marker` l'en-tête de réponse est renvoyé à `true`. • Si un objet est supprimé sans l' `versionId` sous-ressource sur un compartiment suspendu de version, elle entraîne la suppression permanente d'une version existante 'null' ou d'un marqueur de suppression 'null' et la génération d'un nouveau marqueur de suppression 'null'. Le `x-amz-delete-marker` l'en-tête de réponse est renvoyé à `true`. **Remarque** : dans certains cas, plusieurs marqueurs de suppression peuvent exister pour un objet.
SUPPRIMER plusieurs objets	Authentification multifacteur (MFA) et en-tête de réponse `x-amz-mfa` ne sont pas pris en charge. Plusieurs objets peuvent être supprimés dans le même message de demande.

Fonctionnement	Mise en place
SUPPRIMER le balisage d'objets	Utilise le `tagging` sous-ressource pour supprimer toutes les balises d'un objet. Mise en œuvre avec tout le comportement de l'API REST Amazon S3. **Gestion des versions** Si le `versionId` le paramètre query n'est pas spécifié dans la demande. l'opération supprime toutes les balises de la version la plus récente de l'objet dans un compartiment versionné. Si la version actuelle de l'objet est un marqueur de suppression, un état "methodNotAldue" est renvoyé avec l' `x-amz-delete-marker` réponse en-tête réglée sur `true`.
OBTENIR l'objet	OBTENIR l'objet
OBTENIR l'ACL d'objet	Si les informations d'identification d'accès nécessaires sont fournies pour le compte, l'opération renvoie une réponse positive ainsi que l'ID, le DisplayName et l'autorisation du propriétaire de l'objet, ce qui indique que le propriétaire dispose d'un accès complet à l'objet.
OBTENIR la mise en attente légale de l'objet	Utilisez le verrouillage d'objet S3
OBTENIR la conservation des objets	Utilisez le verrouillage d'objet S3
OBTENIR le balisage d'objets	Utilise le `tagging` sous-ressource pour renvoyer toutes les balises d'un objet. Mise en œuvre avec tout le comportement de l'API REST Amazon S3 **Gestion des versions** Si le `versionId` le paramètre query n'est pas spécifié dans la demande, l'opération renvoie toutes les balises de la version la plus récente de l'objet dans un compartiment versionné. Si la version actuelle de l'objet est un marqueur de suppression, un état "methodNotAldue" est renvoyé avec l' `x-amz-delete-marker` réponse en-tête réglée sur `true`.
Objet TÊTE	Objet TÊTE
Restauration POST-objet	Restauration POST-objet
PLACER l'objet	PLACER l'objet
PLACER l'objet - Copier	PLACER l'objet - Copier

Fonctionnement	Mise en place
METTRE l'objet en attente légale	Utilisez le verrouillage d'objet S3
CONSERVATION des objets	Utilisez le verrouillage d'objet S3
PUT Object tagging	Utilise le `tagging` sous-ressource pour ajouter un ensemble de balises à un objet existant. Mise en œuvre avec tout le comportement de l'API REST Amazon S3 **Limites de balise d'objet** Vous pouvez ajouter des balises à de nouveaux objets lorsque vous les téléchargez ou les ajouter à des objets existants. StorageGRID et Amazon S3 prennent en charge jusqu'à 10 balises pour chaque objet. Les balises associées à un objet doivent avoir des clés de balise uniques. Une clé de balise peut comporter jusqu'à 128 caractères Unicode et les valeurs de balise peuvent comporter jusqu'à 256 caractères Unicode. Les clés et les valeurs sont sensibles à la casse **Mises à jour de balises et comportement d'entrée** Lorsque vous utilisez PUT Object tagging pour mettre à jour les balises d'un objet, StorageGRID ne réingérer pas l'objet. Cela signifie que l'option de comportement d'ingestion spécifiée dans la règle ILM correspondante n'est pas utilisée. Tout changement au placement d'objet déclenché par la mise à jour est apporté lors de l'évaluation de ILM par des processus ILM en arrière-plan normaux. Cela signifie que si la règle ILM utilise l'option stricte pour le comportement d'ingestion, aucune action n'est effectuée si les placements d'objet requis ne peuvent pas être effectués (par exemple, car un nouvel emplacement requis n'est pas disponible). L'objet mis à jour conserve son emplacement actuel jusqu'à ce que le placement requis soit possible. **Résolution des conflits** Les demandes contradictoires des clients, telles que deux clients qui écrivent sur la même clé, sont résolues sur une base de « derniers-victoires ». La chronologie de l'évaluation « Latest-WINS » dépend de la date à laquelle le système StorageGRID remplit une demande donnée et non du moment où les clients S3 commencent une opération. **Gestion des versions** Si le `versionId` le paramètre de requête n'est pas spécifié dans la requête, l'opération ajoute des balises à la version la plus récente de l'objet dans un compartiment versionné. Si la version actuelle de l'objet est un marqueur de suppression, un état "methodNotAldue" est renvoyé avec l' `x-amz-delete-marker` réponse en-tête réglée sur `true`.

Informations associées

Opérations S3 suivies dans les journaux d'audit

Utilisez le verrouillage d'objet S3

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

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

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

Activez le verrouillage objet S3 pour le compartiment

Si le paramètre global de verrouillage d'objet S3 est activé pour votre système StorageGRID, vous pouvez activer le verrouillage d'objet S3 lorsque vous créez chaque compartiment. Vous pouvez utiliser l'une des méthodes suivantes :

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

  Utilisez le compte du locataire

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

  Opérations sur les compartiments

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

Un compartiment avec l'option de verrouillage d'objet S3 activée peut contenir une combinaison d'objets avec et sans les paramètres de verrouillage d'objet S3. StorageGRID prend en charge les périodes de conservation par défaut pour les objets dans les compartiments de verrouillage d'objet S3 et prend en charge l'opération de compartiment DE configuration DE verrouillage d'objet. Le `s3:object-lock-remaining-retention-days` la touche condition de police définit les périodes de rétention minimum et maximum autorisées pour vos objets.

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

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

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

Pour spécifier les paramètres de verrouillage d'objet S3 lors de l'ajout d'une version d'objet dans un

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

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

- `x-amz-object-lock-mode`, Qui doit ÊTRE CONFORME (sensible à la casse).

  > Si vous spécifiez `x-amz-object-lock-mode`, vous devez également spécifier `x-amz-object-lock-retain-until-date`.

- `x-amz-object-lock-retain-until-date`
  - La valeur conserver jusqu'à la date doit être au format `2020-08-10T21:46:00Z`. Les secondes fractionnaires sont autorisées, mais seuls 3 chiffres après la virgule sont conservés (précision des millisecondes). Les autres formats ISO 8601 ne sont pas autorisés.
  - La date de conservation doit être ultérieure.
- `x-amz-object-lock-legal-hold`

  Si la conservation légale est ACTIVÉE (sensible à la casse), l'objet est placé sous une obligation légale. Si la mise en attente légale est désactivée, aucune mise en attente légale n'est mise. Toute autre valeur entraîne une erreur 400 Bad Request (InvalidArgument).

Si vous utilisez l'un de ces en-têtes de demande, tenez compte des restrictions suivantes :

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

Mettre à jour les paramètres de verrouillage d'objet S3

Si vous devez mettre à jour les paramètres de conservation légale ou de conservation d'une version d'objet existante, vous pouvez effectuer les opérations de sous-ressource d'objet suivantes :

- `PUT Object legal-hold`

  Si la nouvelle valeur de conservation légale est ACTIVÉE, l'objet est placé sous une mise en attente légale. Si la valeur de retenue légale est OFF, la suspension légale est levée.

- `PUT Object retention`
  - La valeur du mode doit être CONFORME (sensible à la casse).
  - La valeur conserver jusqu'à la date doit être au format `2020-08-10T21:46:00Z`. Les secondes fractionnaires sont autorisées, mais seuls 3 chiffres après la virgule sont conservés (précision des millisecondes). Les autres formats ISO 8601 ne sont pas autorisés.
  - Si une version d'objet possède une date de conservation existante, vous pouvez uniquement l'augmenter. La nouvelle valeur doit être future.

Informations associées

Gestion des objets avec ILM

Utilisez le compte du locataire

PLACER l'objet

PLACER l'objet - Copier

Lancer le téléchargement de pièces multiples

Gestion des versions d'objet

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

Utiliser S3 Select

StorageGRID prend en charge les clauses, types de données et opérateurs AWS S3 Select suivants pour le système Commande SelectObjectContent.

> Les éléments non répertoriés ne sont pas pris en charge.

Pour la syntaxe, voir SelectObjectContent. Pour plus d'informations sur S3 Select, consultez le "Documentation AWS pour S3 Select".

Seuls les comptes de tenant dont S3 Select est activé peuvent émettre des requêtes SelectObjectContent. Voir la Considérations et configuration requise pour l'utilisation de S3 Select.

Clauses

- SÉLECTIONNER la liste
- Clause FROM
- Clause WHERE
- Clause DE LIMITE

Types de données

- bool
- entier
- chaîne
- flottement

- décimale, numérique
- horodatage

Opérateurs

Opérateurs logiques

- ET
- PAS
- OU

Opérateurs de comparaison

* * * lt;= * gt;= * = * = * * != * ENTRE * DANS

Opérateurs de correspondance de répétition

- COMME
- _
- %

Opérateurs unitaires

- EST NULL
- N'EST PAS NULL

Opérateurs mathématiques

- +
- -
- *
- /
- %

StorageGRID suit la priorité de l'opérateur AWS S3 Select.

Fonctions d'agrégation

- MOY()
- NOMBRE(*)
- MAX()
- MIN()
- SOMME()

Fonctions conditionnelles

- CASSE

- FUSIONNE
- NULLIF

Fonctions de conversion

- CAST (pour les types de données pris en charge)

Fonctions de date

- DATE_AJOUTER
- DATE_DIFF
- EXTRAIRE
- TO_STRING
- TO_TIMESTAMP
- CODE D'ARTICLE

Fonctions de chaîne

- CHAR_LENGTH, CARACTÈRE_LENGTH
- ABAISSEMENT
- SOUS-CHAÎNE
- GARNITURE
- SUPÉRIEUR

Utilisez le cryptage côté serveur

Le chiffrement côté serveur vous permet de protéger vos données au repos objet. StorageGRID crypte les données lors de leur écriture et décrypte les données lorsque vous accédez à l'objet.

Si vous souhaitez utiliser le chiffrement côté serveur, vous pouvez choisir l'une des deux options mutuellement exclusives, en fonction de la gestion des clés de cryptage :

- **SSE (chiffrement côté serveur avec clés gérées par StorageGRID)** : lorsque vous émettez une demande S3 pour stocker un objet, StorageGRID crypte l'objet avec une clé unique. Lorsque vous émettez une requête S3 pour récupérer l'objet, StorageGRID utilise la clé stockée pour décrypter l'objet.
- **SSE-C (chiffrement côté serveur avec clés fournies par le client)** : lorsque vous émettez une demande S3 pour stocker un objet, vous fournissez votre propre clé de chiffrement. Lorsque vous récupérez un objet, vous fournissez la même clé de chiffrement dans le cadre de votre demande. Si les deux clés de chiffrement correspondent, l'objet est décrypté et vos données d'objet sont renvoyées.

  StorageGRID gère toutes les opérations de cryptage et de décryptage des objets, mais vous devez gérer les clés de cryptage que vous fournissez.

  > Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant.

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

Utiliser SSE

Pour chiffrer un objet avec une clé unique gérée par StorageGRID, utilisez l'en-tête de demande suivant :

```
x-amz-server-side-encryption
```

L'en-tête de demande SSE est pris en charge par les opérations d'objet suivantes :

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

Utiliser SSE-C

Pour crypter un objet avec une clé unique que vous gérez, vous utilisez trois en-têtes de requête :

En-tête de demande	Description
`x-amz-server-side-encryption-customer-algorithm`	Spécifiez l'algorithme de cryptage. La valeur de la barre de coupe doit être de `AES256`.
`x-amz-server-side-encryption-customer-key`	Spécifiez la clé de cryptage qui sera utilisée pour crypter ou décrypter l'objet. La valeur de la clé doit être codée en 256 bits, en base64.
`x-amz-server-side-encryption-customer-key-MD5`	Spécifiez le résumé MD5 de la clé de chiffrement selon la RFC 1321, qui est utilisé pour garantir que la clé de chiffrement a été transmise sans erreur. La valeur du résumé MD5 doit être codée en base64 à 128 bits.

Les en-têtes de demande SSE-C sont pris en charge par les opérations objet suivantes :

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

Considérations relatives au chiffrement côté serveur avec clés fournies par le client (SSE-C)

Avant d'utiliser SSE-C, tenez compte des points suivants :

- Vous devez utiliser https.

> StorageGRID rejette toute demande effectuée sur http en utilisant SSE-C. Pour des considérations de sécurité, vous devez envisager toute clé que vous envoyez accidentellement en utilisant http pour être compromise. Mettez la clé au rebut et tournez-la selon les besoins.

- L'ETag dans la réponse n'est pas le MD5 des données objet.
- Vous devez gérer le mappage des clés de chiffrement aux objets. StorageGRID ne stocke pas de clés de chiffrement. Vous êtes responsable du suivi de la clé de chiffrement que vous fournissez pour chaque objet.
- Si le contrôle de version du compartiment est activé, chaque version d'objet doit disposer de sa propre clé de chiffrement. Vous êtes responsable du suivi de la clé de chiffrement utilisée pour chaque version d'objet.
- Comme vous gérez les clés de chiffrement côté client, vous devez également gérer d'autres dispositifs de protection, tels que la rotation des clés, côté client.

> Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant.

- Si la réplication CloudMirror est configurée pour le compartiment, vous ne pouvez pas ingérer d'objets SSE-C. L'opération d'acquisition échoue.

Informations associées

OBTENIR l'objet

Objet TÊTE

PLACER l'objet

PLACER l'objet - Copier

Lancer le téléchargement de pièces multiples

Télécharger la pièce

Télécharger la pièce - Copier

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

OBTENIR l'objet

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

OBTENIR un objet et des objets partitionnés

Vous pouvez utiliser le `partNumber` paramètre de demande pour récupérer une partie spécifique d'un objet partitionné ou segmenté. Le `x-amz-mp-parts-count` l'élément de réponse indique le nombre de pièces dont dispose l'objet.

Vous pouvez définir `partNumber` à 1 pour les objets segmentés/multisegments et les objets non segmentés/non-partitionnés ; cependant, le `x-amz-mp-parts-count` l'élément de réponse n'est renvoyé que pour les objets segmentés ou partitionnés.

En-têtes de demande pour chiffrement côté serveur avec clés de chiffrement fournies par le client (SSE-C)

Utilisez les trois en-têtes si l'objet est chiffré avec une clé unique que vous avez fournie.

- `x-amz-server-side-encryption-customer-algorithm`: Spécifiez `AES256`.
- `x-amz-server-side-encryption-customer-key`: Spécifiez votre clé de cryptage pour l'objet.
- `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le résumé MD5 de la clé de chiffrement de l'objet.

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

Caractères UTF-8 dans les métadonnées utilisateur

StorageGRID n'analyse ni n'interprète pas les caractères UTF-8 qui se sont échappés dans les métadonnées définies par l'utilisateur. LES demandes D'OBTENTION d'un objet ayant échappé à l'UTF-8 dans les métadonnées définies par l'utilisateur ne renvoient pas le `x-amz-missing-meta` en-tête si le nom ou la valeur de la clé comporte des caractères non imprimables.

En-tête de demande non pris en charge

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

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

Gestion des versions

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

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

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

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

État de l'objet	Comportement de L'objet GET
Les objets sont ingéré dans StorageGRID mais pas encore évalués par ILM, ou objet stocké dans un pool de stockage traditionnel ou au moyen d'un code d'effacement	`200 OK` Une copie de l'objet est récupérée.
Objet dans Cloud Storage Pool, mais pas encore migré vers un état non récupérable	`200 OK` Une copie de l'objet est récupérée.
L'objet a été transféré à un état non récupérable	`403 Forbidden`, `InvalidObjectState` Utilisez une demande DE restauration POST-objet pour restaurer l'objet à un état récupérable.
Objet en cours de restauration à partir d'un état non récupérable	`403 Forbidden`, `InvalidObjectState` Attendez que la demande DE restauration POST Object soit terminée.
Objet entièrement restauré dans le pool de stockage cloud	`200 OK` Une copie de l'objet est récupérée.

Objets partitionnés ou segmentés dans un pool de stockage cloud

Si vous avez téléchargé un objet partitionné ou si StorageGRID le divise en segments, StorageGRID détermine si l'objet est disponible dans le pool de stockage cloud en échantillonant un sous-ensemble de parties ou de segments de l'objet. Dans certains cas, une demande GET Object peut retourner de manière incorrecte `200 OK` lorsque certaines parties de l'objet ont déjà été migrées à un état non récupérable ou lorsque certaines parties de l'objet n'ont pas encore été restaurées.

Dans ces cas :

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

Informations associées

Utilisez le cryptage côté serveur

Gestion des objets avec ILM

Restauration POST-objet

Opérations S3 suivies dans les journaux d'audit

Objet TÊTE

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

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

Objet TÊTE et objets multipart

Vous pouvez utiliser le `partNumber` paramètre de demande pour récupérer les métadonnées d'une partie spécifique d'un objet partitionné ou segmenté. Le `x-amz-mp-parts-count` l'élément de réponse indique le nombre de pièces dont dispose l'objet.

Vous pouvez définir `partNumber` à 1 pour les objets segmentés/multisegments et les objets non segmentés/non-partitionnés ; cependant, le `x-amz-mp-parts-count` l'élément de réponse n'est renvoyé que pour les objets segmentés ou partitionnés.

En-têtes de demande pour chiffrement côté serveur avec clés de chiffrement fournies par le client (SSE-C)

Utilisez les trois en-têtes si l'objet est chiffré avec une clé unique que vous avez fournie.

- `x-amz-server-side-encryption-customer-algorithm`: Spécifiez `AES256`.
- `x-amz-server-side-encryption-customer-key`: Spécifiez votre clé de cryptage pour l'objet.
- `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le résumé MD5 de la clé de chiffrement de l'objet.

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

Caractères UTF-8 dans les métadonnées utilisateur

StorageGRID n'analyse ni n'interprète pas les caractères UTF-8 qui se sont échappés dans les métadonnées définies par l'utilisateur. Les demandes DE TÊTE pour un objet ayant échappé à l'UTF-8 dans les métadonnées définies par l'utilisateur ne renvoient pas le `x-amz-missing-meta` en-tête si le nom ou la valeur de la clé comporte des caractères non imprimables.

En-tête de demande non pris en charge

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

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

En-têtes de réponse pour les objets Cloud Storage Pool

Si l'objet est stocké dans un pool de stockage cloud (voir les instructions de gestion des objets avec gestion du cycle de vie des informations), les en-têtes de réponse suivants sont renvoyés :

- `x-amz-storage-class: GLACIER`
- `x-amz-restore`

Les en-têtes de réponse fournissent des informations sur l'état d'un objet lors de son déplacement vers Cloud Storage Pool, qui peut être migré vers un état non récupérable et restauré.

État de l'objet	Réponse à l'objet TÊTE
Les objets sont ingéré dans StorageGRID mais pas encore évalués par ILM, ou objet stocké dans un pool de stockage traditionnel ou au moyen d'un code d'effacement	`200 OK` (Aucun en-tête à réponse spéciale n'est renvoyé.)

Objet dans Cloud Storage Pool, mais pas encore migré vers un état non récupérable	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"`
	
	Jusqu'à ce que l'objet soit transféré à un état non récupérable, la valeur de `expiry-date` est sur le point de passer un moment lointain dans le futur. L'heure exacte de la transition n'est pas contrôlée par le système StorageGRID.

L'objet est passé à l'état non récupérable, mais il existe au moins une copie sur la grille	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"`
	
	La valeur pour `expiry-date` est sur le point de passer un moment lointain dans le futur.
	
	Remarque : si la copie de la grille n'est pas disponible (par exemple, un nœud de stockage est en panne), vous devez émettre une demande DE restauration POST-objet pour restaurer la copie à partir du pool de stockage cloud avant de pouvoir extraire l'objet avec succès.

L'objet a été transféré à un état non récupérable et aucune copie n'existe sur la grille	`200 OK`
	
	`x-amz-storage-class: GLACIER`

Objet en cours de restauration à partir d'un état non récupérable	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="true"`

État de l'objet	Réponse à l'objet TÊTE

Objet entièrement restauré dans le pool de stockage cloud	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2018 00:00:00 GMT"`
	
	Le `expiry-date` Indique quand l'objet du pool de stockage cloud sera renvoyé à un état non récupérable.

Objets partitionnés ou segmentés dans Cloud Storage Pool

Si vous avez téléchargé un objet partitionné ou si StorageGRID le divise en segments, StorageGRID détermine si l'objet est disponible dans le pool de stockage cloud en échantillonant un sous-ensemble de parties ou de segments de l'objet. Dans certains cas, une requête d'objet DE TÊTE peut revenir de manière incorrecte `x-amz-restore: ongoing-request="false"` lorsque certaines parties de l'objet ont déjà été migrées à un état non récupérable ou lorsque certaines parties de l'objet n'ont pas encore été restaurées.

Gestion des versions

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

Informations associées

Utilisez le cryptage côté serveur

Gestion des objets avec ILM

Restauration POST-objet

Opérations S3 suivies dans les journaux d'audit

Restauration POST-objet

Vous pouvez utiliser la demande de restauration POST-objet S3 pour restaurer un objet stocké dans un pool de stockage cloud.

Type de demande pris en charge

StorageGRID ne prend en charge que les demandes DE restauration POST-objet pour restaurer un objet. Elle ne prend pas en charge le `SELECT` type de restauration. Sélectionnez demandes de retour `XNotImplemented`.

Gestion des versions

Spécifiez éventuellement `versionId` pour restaurer une version spécifique d'un objet dans un compartiment multiversion. Si vous ne spécifiez pas `versionId`, la version la plus récente de l'objet est restaurée

Comportement de restauration POST-objet sur les objets de pool de stockage cloud

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

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

État de l'objet	Comportement de la restauration POST-objet
L'objet est ingéré dans StorageGRID mais pas encore évalué par ILM ou l'objet ne se trouve pas dans un pool de stockage cloud	`403 Forbidden`, `InvalidObjectState`
Objet dans Cloud Storage Pool, mais pas encore migré vers un état non récupérable	`200 OK` Aucune modification n'est apportée. **Note**: Avant qu'un objet ait été transféré à un état non récupérable, vous ne pouvez pas le modifier `expiry-date`.
L'objet a été transféré à un état non récupérable	`202 Accepted` Restaure une copie récupérable de l'objet vers le pool de stockage cloud pendant le nombre de jours spécifié dans le corps de la demande. À la fin de cette période, l'objet est renvoyé à un état non récupérable. Si vous le souhaitez, utilisez le `Tier` élément de demande pour déterminer la durée de la tâche de restauration (`Expedited`, `Standard`, ou `Bulk`). Si vous ne spécifiez pas `Tier`, le `Standard` le niveau est utilisé. **Attention** : si un objet a été transféré vers S3 Glacier Deep Archive ou si Cloud Storage Pool utilise Azure Blob Storage, vous ne pouvez pas le restaurer à l'aide de `Expedited` niveau. L'erreur suivante est renvoyée `403 Forbidden`, `InvalidTier`: `Retrieval option is not supported by this storage class`.
Objet en cours de restauration à partir d'un état non récupérable	`409 Conflict`, `RestoreAlreadyInProgress`

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

Informations associées

Gestion des objets avec ILM

Objet TÊTE

Opérations S3 suivies dans les journaux d'audit

PLACER l'objet

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

Résoudre les conflits

Les demandes contradictoires des clients, telles que deux clients qui écrivent sur la même clé, sont résolues sur une base de « derniers-victoires ». La chronologie de l'évaluation « derniers-victoires » repose sur la date à laquelle le système StorageGRID termine une demande donnée et non sur la date à laquelle les clients S3 commencent une opération.

Taille de l'objet

La taille maximale *recommandée* pour une opération d'objet PUT unique est de 5 Gio (5,368,709,120 octets). Si vos objets sont supérieurs à 5 Gio, utilisez le téléchargement partitionné.

> Dans StorageGRID 11.6, la taille maximale *supportée* pour une opération put Object est de 5 Tio (5,497,558,138,880 octets). Cependant, l'alerte **S3 PUT Object size trop importante** est déclenchée si vous tentez de télécharger un objet supérieur à 5 Gio.

Taille des métadonnées utilisateur

Amazon S3 limite la taille des métadonnées définies par l'utilisateur au sein de chaque en-tête de requête À 2 Ko. StorageGRID limite les métadonnées utilisateur à 24 Kio. La taille des métadonnées définies par l'utilisateur est mesurée en prenant la somme du nombre d'octets dans le codage UTF-8 de chaque clé et valeur.

Caractères UTF-8 dans les métadonnées utilisateur

Si une requête inclut (non échappé) les valeurs UTF-8 dans le nom de clé ou la valeur des métadonnées définies par l'utilisateur, le comportement StorageGRID n'est pas défini.

StorageGRID n'analyse ni n'interprète pas les caractères UTF-8 qui se sont échappé dans le nom de clé ou la valeur des métadonnées définies par l'utilisateur. Les caractères UTF-8 échappés sont traités comme des caractères ASCII :

- LES demandes PUT, PUT Object-Copy, GET et HEAD sont satisfaites si les métadonnées définies par l'utilisateur incluent des caractères UTF-8 échappés.
- StorageGRID ne renvoie pas le `x-amz-missing-meta` en-tête si la valeur interprétée du nom ou de la valeur de la clé comprend des caractères non imprimables.

Limites des balises d'objet

Vous pouvez ajouter des balises à de nouveaux objets lorsque vous les téléchargez ou les ajouter à des objets existants. StorageGRID et Amazon S3 prennent en charge jusqu'à 10 balises pour chaque objet. Les balises associées à un objet doivent avoir des clés de balise uniques. Une clé de balise peut comporter jusqu'à 128 caractères Unicode et les valeurs de balise peuvent comporter jusqu'à 256 caractères Unicode. Les clés et les valeurs sont sensibles à la casse

Propriété de l'objet

Dans StorageGRID, tous les objets sont détenus par le compte du propriétaire de compartiment, y compris les objets créés par un compte autre que le propriétaire ou un utilisateur anonyme.

En-têtes de demande pris en charge

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

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`

  Lorsque vous spécifiez `aws-chunked` pour `Content-Encoding`StorageGRID ne vérifie pas les éléments suivants :

  - StorageGRID ne vérifie pas le `chunk-signature` par rapport aux données de bloc.
  - StorageGRID ne vérifie pas la valeur que vous fournissez pour `x-amz-decoded-content-length` contre l'objet.
- `Content-Language`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Expires`
- `Transfer-Encoding`

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

- `x-amz-meta-`, suivi d'une paire nom-valeur contenant des métadonnées définies par l'utilisateur.

  Lorsque vous spécifiez la paire nom-valeur pour les métadonnées définies par l'utilisateur, utilisez le format général suivant :

```
x-amz-meta-name: value
```

Si vous souhaitez utiliser l'option **heure de création définie par l'utilisateur** comme heure de référence pour une règle ILM, vous devez utiliser `creation-time` nom des métadonnées enregistrées lors de la création de l'objet. Par exemple :

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

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

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

- `x-amz-tagging`
- En-têtes de requête de verrouillage d'objet S3
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

    Si une demande est effectuée sans ces en-têtes, les paramètres de rétention par défaut du compartiment sont utilisés pour calculer la version de l'objet conserver jusqu'à la date.

  Utilisez le verrouillage d'objet S3
- En-têtes de demande SSE :
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

    Voir Demander des en-têtes pour le cryptage côté serveur

En-têtes de requête non pris en charge

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

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

Options de classe de stockage

Le `x-amz-storage-class` l'en-tête de demande est pris en charge. Valeur soumise pour `x-amz-storage-`

`class` StorageGRID protège les données d'objet lors de leur ingestion, mais pas le nombre de copies persistantes de l'objet stockées dans le système StorageGRID (déterminé par ILM).

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

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

- `STANDARD` (Valeur par défaut)
  - **Double commit** : si la règle ILM spécifie l'option de double validation pour le comportement d'ingestion, dès qu'un objet est ingéré, une seconde copie de cet objet est créée et distribuée à un autre nœud de stockage (double commit). Lors de l'évaluation de l'ILM, StorageGRID détermine si ces copies intermédiaires initiales répondent aux instructions de placement de la règle. Autrement, de nouvelles copies d'objet peuvent être nécessaires à d'autres emplacements et les copies intermédiaires initiales peuvent être supprimées.
  - **Équilibré** : si la règle ILM spécifie l'option équilibrée et que StorageGRID ne peut pas immédiatement faire toutes les copies spécifiées dans la règle, StorageGRID effectue deux copies intermédiaires sur différents nœuds de stockage.

    Si StorageGRID peut immédiatement créer toutes les copies d'objet spécifiées dans la règle ILM (placement synchrone), l' `x-amz-storage-class` la barre de coupe n'a aucun effet.

- `REDUCED_REDUNDANCY`
  - **Double commit** : si la règle ILM spécifie l'option de double validation pour le comportement d'ingestion, StorageGRID crée une copie intermédiaire unique lors de l'ingestion de l'objet (simple commit).
  - **Équilibré** : si la règle ILM spécifie l'option équilibrée, StorageGRID ne fait une copie provisoire que si le système ne peut pas immédiatement faire toutes les copies spécifiées dans la règle. Si StorageGRID peut effectuer un placement synchrone, cet en-tête n'a aucun effet. Le `REDUCED_REDUNDANCY` L'option est meilleure lorsque la règle ILM correspondant à l'objet crée une copie répliquée unique. Dans ce cas, utilisez `REDUCED_REDUNDANCY` élimine la création et la suppression inutiles d'une copie d'objet supplémentaire pour chaque opération d'ingestion.

  À l'aide du `REDUCED_REDUNDANCY` cette option n'est pas recommandée dans d'autres cas. `REDUCED_REDUNDANCY` augmente le risque de perte de données d'objet lors de l'ingestion. Vous risquez par exemple de perdre des données si une seule copie est initialement stockée sur un nœud de stockage qui échoue avant l'évaluation du ILM.

Attention: Avoir une seule copie répliquée pour une période donnée met les données en danger de perte permanente. Si une seule copie répliquée d'un objet existe, cet objet est perdu en cas de défaillance ou d'erreur importante d'un noeud de stockage. De plus, lors des procédures de maintenance telles que les mises à niveau, l'accès à l'objet est temporairement perdu.

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

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

Demander des en-têtes pour le cryptage côté serveur

Vous pouvez utiliser les en-têtes de requête suivants pour crypter un objet avec un chiffrement côté serveur. Les options SSE et SSE-C sont mutuellement exclusives.

- **SSE**: Utilisez l'en-tête suivant si vous voulez chiffrer l'objet avec une clé unique gérée par StorageGRID.
  - `x-amz-server-side-encryption`
- **SSE-C**: Utilisez les trois en-têtes si vous voulez chiffrer l'objet avec une clé unique que vous fournissez et gérez.
  - `x-amz-server-side-encryption-customer-algorithm`: Spécifiez `AES256`.
  - `x-amz-server-side-encryption-customer-key`: Spécifiez votre clé de cryptage pour le nouvel objet.
  - `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le résumé MD5 de la clé de chiffrement du nouvel objet.

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

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

Gestion des versions

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

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

Informations associées

Gestion des objets avec ILM

Opérations sur les compartiments

Opérations S3 suivies dans les journaux d'audit

Utilisez le cryptage côté serveur

Configuration des connexions client

PLACER l'objet - Copier

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

Résoudre les conflits

Les demandes contradictoires des clients, telles que deux clients qui écrivent sur la même clé, sont résolues sur une base de « derniers-victoires ». La chronologie de l'évaluation « derniers-victoires » repose sur la date

à laquelle le système StorageGRID termine une demande donnée et non sur la date à laquelle les clients S3 commencent une opération.

Taille de l'objet

La taille maximale *recommandée* pour une opération d'objet PUT unique est de 5 Gio (5,368,709,120 octets). Si vos objets sont supérieurs à 5 Gio, utilisez le téléchargement partitionné.

> Dans StorageGRID 11.6, la taille maximale *supportée* pour une opération put Object est de 5 Tio (5,497,558,138,880 octets). Cependant, l'alerte **S3 PUT Object size trop importante** est déclenchée si vous tentez de télécharger un objet supérieur à 5 Gio.

Caractères UTF-8 dans les métadonnées utilisateur

Si une requête inclut (non échappé) les valeurs UTF-8 dans le nom de clé ou la valeur des métadonnées définies par l'utilisateur, le comportement StorageGRID n'est pas défini.

StorageGRID n'analyse ni n'interprète pas les caractères UTF-8 qui se sont échappé dans le nom de clé ou la valeur des métadonnées définies par l'utilisateur. Les caractères UTF-8 échappés sont traités comme des caractères ASCII :

- Les requêtes réussissent si les métadonnées définies par l'utilisateur incluent des caractères UTF-8 échappés.
- StorageGRID ne renvoie pas le `x-amz-missing-meta` en-tête si la valeur interprétée du nom ou de la valeur de la clé comprend des caractères non imprimables.

En-têtes de demande pris en charge

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

- `Content-Type`
- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-if-modified-since`
- `x-amz-meta-`, suivi d'une paire nom-valeur contenant des métadonnées définies par l'utilisateur
- `x-amz-metadata-directive`: La valeur par défaut est `COPY`, qui permet de copier l'objet et les métadonnées associées.

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

- `x-amz-storage-class`
- `x-amz-tagging-directive`: La valeur par défaut est `COPY`, qui vous permet de copier l'objet et toutes les balises.

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

- En-têtes de demande de verrouillage d'objet S3 :
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

    Si une demande est effectuée sans ces en-têtes, les paramètres de rétention par défaut du compartiment sont utilisés pour calculer la version de l'objet conserver jusqu'à la date.

  Utilisez le verrouillage d'objet S3

- En-têtes de demande SSE :
  - `x-amz-copy-source-server-side-encryption-customer-algorithm`
  - `x-amz-copy-source-server-side-encryption-customer-key`
  - `x-amz-copy-source-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

    Voir Demander des en-têtes pour le cryptage côté serveur

En-têtes de requête non pris en charge

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

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

Options de classe de stockage

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

- `STANDARD`

  (Valeur par défaut) Spécifie une opération d'ingestion à double validation lorsque la règle ILM utilise l'option de validation double, ou lorsque l'option équilibrée revient à créer des copies intermédiaires.

- `REDUCED_REDUNDANCY`

Spécifie une opération d'entrée de validation unique lorsque la règle ILM utilise l'option Double allocation ou lorsque l'option équilibrée revient à créer des copies intermédiaires.

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

Utilisation de x-amz-copy-source dans PUT Object - Copy

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

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

- Vous ne pouvez pas utiliser METTRE l'objet - Copier pour crypter un objet existant en place ou pour modifier le chiffrement d'un objet existant. Si vous fournissez le `x-amz-server-side-encryption` en-tête ou le `x-amz-server-side-encryption-customer-algorithm` En-tête, StorageGRID rejette la demande et renvoie la requête `XNotImplemented`.
- L'option de comportement d'ingestion spécifiée dans la règle ILM correspondante n'est pas utilisée. Tout changement au placement d'objet déclenché par la mise à jour est apporté lors de l'évaluation de ILM par des processus ILM en arrière-plan normaux.

  Cela signifie que si la règle ILM utilise l'option stricte pour le comportement d'ingestion, aucune action n'est effectuée si les placements d'objet requis ne peuvent pas être effectués (par exemple, car un nouvel emplacement requis n'est pas disponible). L'objet mis à jour conserve son emplacement actuel jusqu'à ce que le placement requis soit possible.

Demander des en-têtes pour le cryptage côté serveur

Si vous utilisez le chiffrement côté serveur, les en-têtes de requête que vous fournissez dépendent du chiffrement de l'objet source et de l'intention de chiffrer l'objet cible.

- Si l'objet source est chiffré à l'aide d'une clé fournie par le client (SSE-C), vous devez inclure les trois en-têtes suivants dans la demande PUT Object - Copy, afin que l'objet puisse être décrypté puis copié :
  - `x-amz-copy-source-server-side-encryption-customer-algorithm` Spécifiez `AES256`.
  - `x-amz-copy-source-server-side-encryption-customer-key` Spécifiez la clé de chiffrement que vous avez fournie lors de la création de l'objet source.
  - `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Spécifiez le résumé MD5 que vous avez fourni lors de la création de l'objet source.
- Si vous souhaitez chiffrer l'objet cible (la copie) avec une clé unique que vous fournissez et gérez, incluez les trois en-têtes suivants :
  - `x-amz-server-side-encryption-customer-algorithm`: Spécifiez `AES256`.
  - `x-amz-server-side-encryption-customer-key`: Spécifiez une nouvelle clé de cryptage pour l'objet cible.

- `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le résumé MD5 de la nouvelle clé de chiffrement.

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

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

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

Gestion des versions

Si le compartiment source est multiversion, vous pouvez utiliser le `x-amz-copy-source` en-tête pour copier la dernière version d'un objet. Pour copier une version spécifique d'un objet, vous devez spécifier explicitement la version à copier à l'aide de l' `versionId` sous-ressource. Si le compartiment de destination est multiversion, la version générée est renvoyée dans le `x-amz-version-id` en-tête de réponse. Si le contrôle de version est suspendu pour le compartiment cible, alors `x-amz-version-id` renvoie une valeur « nulle ».

Informations associées

Gestion des objets avec ILM

Utilisez le cryptage côté serveur

Opérations S3 suivies dans les journaux d'audit

PLACER l'objet

SelectObjectContent

Vous pouvez utiliser la requête S3 SelectObjectContent pour filtrer le contenu d'un objet S3 à partir d'une instruction SQL simple.

Pour plus d'informations, reportez-vous au "Documentation AWS pour SelectObjectContent".

Ce dont vous avez besoin

- Le compte de tenant dispose de l'autorisation S3 Select.
- Vous avez `s3:GetObject` autorisation pour l'objet à interroger.
- L'objet que vous souhaitez interroger est au format CSV ou est un fichier compressé GZIP ou BZIP2 contenant un fichier au format CSV.
- Votre expression SQL a une longueur maximale de 256 Ko.
- Tout enregistrement dans l'entrée ou les résultats a une longueur maximale de 1 MIB.

Exemple de syntaxe de la demande

```
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 requête SQL

Cette requête obtient le nom de l'état, 2010 populations, environ 2015 populations et le pourcentage de changement des données de recensement des États-Unis. Les enregistrements du fichier qui ne sont pas des États sont ignorés.

```
SELECT STNAME, CENSUS2010POP, POPESTIMATE2015, CAST((POPESTIMATE2015 -
CENSUS2010POP) AS DECIMAL) / CENSUS2010POP * 100.0 FROM S3Object WHERE
NAME = STNAME
```

Les premières lignes du fichier à interroger, `SUB-EST2020_ALL.csv`, regardez comme ceci:

```
SUMLEV,STATE,COUNTY,PLACE,COUSUB,CONCIT,PRIMGEO_FLAG,FUNCSTAT,NAME,STNAME,
CENSUS2010POP,
ESTIMATESBASE2010,POPESTIMATE2010,POPESTIMATE2011,POPESTIMATE2012,POPESTIM
ATE2013,POPESTIMATE2014,
POPESTIMATE2015,POPESTIMATE2016,POPESTIMATE2017,POPESTIMATE2018,POPESTIMAT
E2019,POPESTIMATE042020,
POPESTIMATE2020
040,01,000,00000,00000,00000,0,A,Alabama,Alabama,4779736,4780118,4785514,4
799642,4816632,4831586,
4843737,4854803,4866824,4877989,4891628,4907965,4920706,4921532
162,01,000,00124,00000,00000,0,A,Abbeville
city,Alabama,2688,2705,2699,2694,2645,2629,2610,2602,
2587,2578,2565,2555,2555,2553
162,01,000,00460,00000,00000,0,A,Adamsville
city,Alabama,4522,4487,4481,4474,4453,4430,4399,4371,
4335,4304,4285,4254,4224,4211
162,01,000,00484,00000,00000,0,A,Addison
town,Alabama,758,754,751,750,745,744,742,734,734,728,
725,723,719,717
```

Exemple d'utilisation d'AWS-CLI

```
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`, regardez comme ceci:

```
Alabama,4779736,4854803,1.5705260708959658022953568983726297854
Alaska,710231,738430,3.9703983633493891424057806544631253775
Arizona,6392017,6832810,6.8959922978928247531256565807005832431
Arkansas,2915918,2979732,2.1884703204959810255295244928012378949
California,37253956,38904296,4.4299724839960620557988526104449148971
Colorado,5029196,5454328,8.4532796097030221132761578590295546246
```

Opérations pour les téléchargements partitionnés

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

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

- Vous ne devez pas dépasser 1,000 téléchargements partitionnés simultanés dans un seul compartiment car les résultats des requêtes List Multipart Uploads pour ce compartiment pourraient renvoyer des résultats incomplets.
- StorageGRID fait respecter les limites de taille d'AWS pour les pièces en plusieurs parties. Les clients S3 doivent respecter les consignes suivantes :
  - Chaque partie d'un téléchargement partitionné doit être comprise entre 5 Mio (5,242,880 octets) et 5 Gio (5,368,709,120 octets).
  - La dernière partie peut être inférieure à 5 Mio (5,242,880 octets).
  - En général, la taille des pièces doit être la plus grande possible. Par exemple, utilisez une taille de pièce de 5 Gio pour un objet de 100 Gio. Comme chaque pièce est considérée comme un objet unique, l'utilisation de grandes tailles de pièce réduit la surcharge des métadonnées StorageGRID.
  - Pour les objets de moins de 5 Gio, envisagez l'utilisation de téléchargement non partitionné.
- Le ILM est évalué pour chaque partie d'un objet partitionné à l'ingestion et pour l'objet dans son ensemble, à la fin du téléchargement partitionné, si la règle ILM utilise le comportement d'entrée strict ou équilibré. Vous devez savoir comment cela affecte le positionnement de l'objet et de la pièce :
  - Si le téléchargement partitionné est en cours de modification du ILM, si le téléchargement partitionné et certaines parties de l'objet peuvent ne pas répondre aux exigences ILM actuelles. Toute pièce qui n'est pas placée correctement est mise en file d'attente pour la réévaluation ILM et est déplacée ultérieurement au bon emplacement.
  - Lors de l'évaluation d'ILM pour une pièce, StorageGRID filtre la taille de la pièce, et non la taille de l'objet. Cela signifie que certaines parties d'un objet peuvent être stockées à des emplacements ne respectant pas les exigences ILM de l'objet dans son ensemble. Par exemple, si une règle indique que tous les objets de 10 Go ou plus sont stockés dans DC1 alors que tous les objets plus petits sont stockés dans DC2, à l'acquisition chaque partie de 1 Go d'un téléchargement partitionné en 10 parties est stockée dans DC2. Lorsque ILM est évaluée pour l'ensemble de l'objet, toutes les parties de l'objet sont déplacées vers DC1.
- Toutes les opérations de téléchargement partitionné prennent en charge les contrôles de cohérence StorageGRID.
- Si nécessaire, vous pouvez utiliser le cryptage côté serveur avec des téléchargements partitionnés. Pour utiliser SSE (chiffrement côté serveur avec clés gérées par StorageGRID), vous avez accès au `x-amz-server-side-encryption` En-tête de demande dans la demande de téléchargement de pièces multiples uniquement. Pour utiliser SSE-C (chiffrement côté serveur avec clés fournies par le client), vous

devez spécifier les trois mêmes en-têtes de demande de clé de chiffrement dans la demande de lancement de Multipart Upload et dans chaque demande de chargement de pièce suivante.

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

Informations associées

- Contrôles de cohérence
- Utilisez le cryptage côté serveur

Liste des téléchargements partitionnés

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

Les paramètres de demande suivants sont pris en charge :

- `encoding-type`
- `max-uploads`
- `key-marker`
- `prefix`
- `upload-id-marker`

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

Gestion des versions

Le téléchargement partitionné est constitué de différentes opérations permettant de lancer le téléchargement, de répertorier les téléchargements, de télécharger des pièces, d'assembler les pièces téléchargées et de terminer le téléchargement. Lorsque l'opération de téléchargement multipart complète est exécutée, c'est-à-dire le point où les objets sont créés (et versionnés le cas échéant).

Lancer le téléchargement de pièces multiples

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

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

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

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

- `STANDARD` (Valeur par défaut)
  - **Double commit** : si la règle ILM spécifie l'option de double validation pour le comportement d'ingestion, dès qu'un objet est ingéré, une seconde copie de cet objet est créée et distribuée à un autre nœud de stockage (double commit). Lors de l'évaluation de l'ILM, StorageGRID détermine si ces copies intermédiaires initiales répondent aux instructions de placement de la règle. Autrement, de nouvelles copies d'objet peuvent être nécessaires à d'autres emplacements et les copies intermédiaires initiales peuvent être supprimées.
  - **Équilibré** : si la règle ILM spécifie l'option équilibrée et que StorageGRID ne peut pas immédiatement faire toutes les copies spécifiées dans la règle, StorageGRID effectue deux copies intermédiaires sur différents nœuds de stockage.

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

  À l'aide du `REDUCED_REDUNDANCY` cette option n'est pas recommandée dans d'autres cas. `REDUCED_REDUNDANCY` augmente le risque de perte de données d'objet lors de l'ingestion. Vous risquez par exemple de perdre des données si une seule copie est initialement stockée sur un nœud de stockage qui échoue avant l'évaluation du ILM.

Attention: Avoir une seule copie répliquée pour une période donnée met les données en danger de perte permanente. Si une seule copie répliquée d'un objet existe, cet objet est perdu en cas de défaillance ou d'erreur importante d'un noeud de stockage. De plus, lors des procédures de maintenance telles que les mises à niveau, l'accès à l'objet est temporairement perdu.

Spécification `REDUCED_REDUNDANCY` l'impact sur le nombre de copies créées uniquement lors de l'ingestion d'un objet. Elle n'affecte pas le nombre de copies de l'objet lorsque celui-ci est évalué par la règle ILM active ;

le stockage des données ne se produit pas à des niveaux de redondance inférieurs dans le système StorageGRID.

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

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

- `Content-Type`
- `x-amz-meta-`, suivi d'une paire nom-valeur contenant des métadonnées définies par l'utilisateur

  Lorsque vous spécifiez la paire nom-valeur pour les métadonnées définies par l'utilisateur, utilisez le format général suivant :

  ```
  x-amz-meta-_name_: `value`
  ```

  Si vous souhaitez utiliser l'option **heure de création définie par l'utilisateur** comme heure de référence pour une règle ILM, vous devez utiliser `creation-time` nom des métadonnées enregistrées lors de la création de l'objet. Par exemple :

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

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

  > Ajout `creation-time` Comme les métadonnées définies par l'utilisateur n'sont pas autorisées si vous ajoutez un objet à un compartiment pour lequel la conformité héritée est activée. Une erreur sera renvoyée.

- En-têtes de demande de verrouillage d'objet S3 :
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

    Si une demande est effectuée sans ces en-têtes, les paramètres de rétention par défaut du compartiment sont utilisés pour calculer la version de l'objet conserver jusqu'à la date.

  Utilisation du verrouillage d'objet S3

- En-têtes de demande SSE :
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

Demander des en-têtes pour le cryptage côté serveur

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

Demander des en-têtes pour le cryptage côté serveur

Vous pouvez utiliser les en-têtes de demande suivants pour crypter un objet partitionné avec un cryptage côté serveur. Les options SSE et SSE-C sont mutuellement exclusives.

- **SSE** : utilisez l'en-tête suivant dans la demande lancer le téléchargement multi-pièces si vous souhaitez crypter l'objet avec une clé unique gérée par StorageGRID. Ne spécifiez pas cet en-tête dans l'une des demandes de téléchargement d'article.
  - `x-amz-server-side-encryption`
- **SSE-C** : utilisez les trois en-têtes de la demande de téléchargement multipièces (et dans chaque demande de chargement ultérieure de pièce) si vous souhaitez chiffrer l'objet avec une clé unique que vous fournissez et gérez.
  - `x-amz-server-side-encryption-customer-algorithm`: Spécifiez `AES256`.
  - `x-amz-server-side-encryption-customer-key`: Spécifiez votre clé de cryptage pour le nouvel objet.
  - `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le résumé MD5 de la clé de chiffrement du nouvel objet.

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

En-têtes de requête non pris en charge

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

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

Gestion des versions

Le téléchargement partitionné est constitué de différentes opérations permettant de lancer le téléchargement, de répertorier les téléchargements, de télécharger des pièces, d'assembler les pièces téléchargées et de terminer le téléchargement. Les objets sont créés (et versionnés le cas échéant) lorsque l'opération de chargement multipièce complète est exécutée.

Informations associées

Gestion des objets avec ILM

Utilisez le cryptage côté serveur

PLACER l'objet

Télécharger la pièce

L'opération de téléchargement de pièce télécharge une pièce dans un téléchargement

partitionné pour un objet.

En-têtes de demande pris en charge

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

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

Demander des en-têtes pour le cryptage côté serveur

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

- `x-amz-server-side-encryption-customer-algorithm`: Spécifiez `AES256`.
- `x-amz-server-side-encryption-customer-key`: Spécifiez la même clé de cryptage que celle que vous avez fournie dans la demande de lancement de Multipart Upload.
- `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le même résumé MD5 que vous avez fourni dans la demande de lancement de Multipart Upload.

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

Gestion des versions

Le téléchargement partitionné est constitué de différentes opérations permettant de lancer le téléchargement, de répertorier les téléchargements, de télécharger des pièces, d'assembler les pièces téléchargées et de terminer le téléchargement. Les objets sont créés (et versionnés le cas échéant) lorsque l'opération de chargement multipièce complète est exécutée.

Informations associées

Utilisez le cryptage côté serveur

Télécharger la pièce - Copier

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

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

Cette requête lit et écrit les données de l'objet spécifiées dans `x-amz-copy-source-range` Dans le système StorageGRID.

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

- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`

- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-if-modified-since`

Demander des en-têtes pour le cryptage côté serveur

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

- `x-amz-server-side-encryption-customer-algorithm`: Spécifiez `AES256`.
- `x-amz-server-side-encryption-customer-key`: Spécifiez la même clé de cryptage que celle que vous avez fournie dans la demande de lancement de Multipart Upload.
- `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le même résumé MD5 que vous avez fourni dans la demande de lancement de Multipart Upload.

Si l'objet source est chiffré à l'aide d'une clé fournie par le client (SSE-C), vous devez inclure les trois en-têtes suivants dans la demande de copie de pièce de téléchargement, afin que l'objet puisse être décrypté puis copié :

- `x-amz-copy-source-server-side-encryption-customer-algorithm`: Spécifiez `AES256`.
- `x-amz-copy-source-server-side-encryption-customer-key`: Spécifiez la clé de cryptage que vous avez fournie lors de la création de l'objet source.
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Spécifiez le résumé MD5 que vous avez fourni lors de la création de l'objet source.

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

Gestion des versions

Le téléchargement partitionné est constitué de différentes opérations permettant de lancer le téléchargement, de répertorier les téléchargements, de télécharger des pièces, d'assembler les pièces téléchargées et de terminer le téléchargement. Les objets sont créés (et versionnés le cas échéant) lorsque l'opération de chargement multipièce complète est exécutée.

Chargement de pièces multiples complet

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

Résoudre les conflits

Les demandes contradictoires des clients, telles que deux clients qui écrivent sur la même clé, sont résolues sur une base de « derniers-victoires ». La chronologie de l'évaluation « derniers-victoires » repose sur la date à laquelle le système StorageGRID termine une demande donnée et non sur la date à laquelle les clients S3 commencent une opération.

En-têtes de demande

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

- `STANDARD`

  (Valeur par défaut) Spécifie une opération d'ingestion à double validation lorsque la règle ILM utilise l'option de validation double, ou lorsque l'option équilibrée revient à créer des copies intermédiaires.

- `REDUCED_REDUNDANCY`

  Spécifie une opération d'entrée de validation unique lorsque la règle ILM utilise l'option Double allocation ou lorsque l'option équilibrée revient à créer des copies intermédiaires.

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

> Si un téléchargement partitionné n'est pas terminé dans les 15 jours, l'opération est marquée comme inactive et toutes les données associées sont supprimées du système.

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

Gestion des versions

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

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

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

> Lorsque le contrôle de version est activé pour un compartiment, le fait de terminer un téléchargement partitionné crée toujours une nouvelle version, même si des téléchargements partitionnés simultanés sont terminés sur la même clé d'objet. Lorsque le contrôle de version n'est pas activé pour un compartiment, il est possible de lancer un téléchargement partitionné et de lancer un autre lancement de téléchargement partitionné et de le terminer d'abord sur la même clé d'objet. Pour les compartiments non versionnés, le téléchargement partitionné de la dernière version est prioritaire.

Échec de la réplication, de la notification ou de la notification des métadonnées

Si le compartiment dans lequel le téléchargement partitionné est configuré pour un service de plateforme, le téléchargement partitionné réussit même si l'action de réplication ou de notification associée échoue.

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

Un locataire peut déclencher la réplication ou la notification d'échec en mettant à jour les métadonnées ou les balises de l'objet. Un locataire peut soumettre à nouveau les valeurs existantes afin d'éviter toute modification non souhaitée.

Informations associées

Gestion des objets avec ILM

Réponses d'erreur

Le système StorageGRID prend en charge toutes les réponses d'erreur de l'API REST S3 standard qui s'appliquent. En outre, l'implémentation de StorageGRID ajoute plusieurs réponses personnalisées.

Codes d'erreur de l'API S3 pris en charge

Nom	Statut HTTP
AccessDenied	403 interdit
BadDigest	400 demande erronée
BucketAlreadyExists	409 conflit
BucketNotEmpty	409 conflit
Corps entier	400 demande erronée
Erreur interne	500 erreur interne du serveur
InvalidAccessKeyId	403 interdit
Invalides	400 demande erronée
InvalidBucketName	400 demande erronée
InvalidBucketState	409 conflit
InvalidDigest	400 demande erronée
InvalidEncryptionAlgorithmError	400 demande erronée

Nom	Statut HTTP
Invalidpart	400 demande erronée
Ordre de pièce InvalidPartOrder	400 demande erronée
InvalidRange	416 Plage demandée non satisfiable
InvalidRequest	400 demande erronée
InvalidStorageClass	400 demande erronée
InvalidTag	400 demande erronée
URI non valide	400 demande erronée
KeyToolong	400 demande erronée
MalformedXML	400 demande erronée
MetadaTooLarge	400 demande erronée
MethodNotAlldue	405 méthode non autorisée
MissingContentLength	411 longueur requise
Erreur MissingestBodyError	400 demande erronée
En-tête MissinécuritéSent	400 demande erronée
NoSuchBucket	404 introuvable
NoSuchKey	404 introuvable
NoSuchUpload	404 introuvable
Note d’implémentation	501 non mis en œuvre
NoSuchBucketPolicy	404 introuvable
ObjectLockNotConfigurationError	404 introuvable
Pré-conditionFailed	412 Echec de la condition préalable
RequestTimeTooSkewed	403 interdit

Nom	Statut HTTP
Disponibilité des services	503 Service indisponible
SignatureDoesNotMatch	403 interdit
TooManyseaux	400 demande erronée
UserKeyMustBeSpecified	400 demande erronée

Codes d'erreur personnalisés StorageGRID

Nom	Description	Statut HTTP
XBuckeLifecycleNotAlldue	La configuration du cycle de vie des compartiments n'est pas autorisée dans un compartiment conforme aux anciennes	400 demande erronée
XBuckePolicyParseException	Impossible d'analyser la politique de compartiment JSON.	400 demande erronée
XComplanceConflitt	Opération refusée en raison des paramètres de conformité hérités.	403 interdit
XComplanceReduceRAIDForbidden	La réduction de la redondance est interdite dans le compartiment conforme aux réglementations existantes	400 demande erronée
XMaxBucketPolicyLengthExcediéé	Votre politique dépasse la longueur maximale autorisée pour la règle de gestion des compartiments.	400 demande erronée
XMissingInternalRequestHeader	En-tête d'une demande interne manquant.	400 demande erronée
XNoSuchBucketCompliance	La conformité héritée n'est pas activée dans le compartiment spécifié.	404 introuvable
XNotAcceptable	La demande contient un ou plusieurs en-têtes Accept qui n'ont pas pu être satisfaits.	406 non acceptable
XNotImplementation	La demande que vous avez fournie implique une fonctionnalité qui n'est pas implémentée.	501 non mis en œuvre

Opérations des API REST StorageGRID S3

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

- DEMANDE de cohérence des compartiments

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

- PUT Bucket Consistency demandée

  La demande de cohérence PUT bucket permet de spécifier le niveau de cohérence à appliquer aux opérations effectuées dans un compartiment.

- DEMANDE DE dernier accès au compartiment

  La demande D'heure de dernier accès À GET Bucket vous permet de déterminer si les dernières mises à jour de temps d'accès sont activées ou désactivées pour les compartiments individuels.

- DEMANDE de temps de dernier accès au compartiment

  La demande d'heure de dernier accès AU compartiment PERMET d'activer ou de désactiver les mises à jour des temps de dernier accès pour chaque compartiment. La désactivation des mises à jour du temps d'accès précédent améliore les performances. Il s'agit du paramètre par défaut pour tous les compartiments créés avec la version 10.3.0, ou ultérieure.

- SUPPRIME la demande de configuration de notification des métadonnées de compartiment

  La demande de configuration DE notification DE métadonnées DELETE Bucket vous permet de désactiver le service d'intégration de recherche pour les compartiments individuels en supprimant le XML de configuration.

- LIRE la demande de configuration de notification des métadonnées de compartiment

  La demande de configuration DE notification DE métadonnées GET Bucket vous permet de récupérer le XML de configuration utilisé pour configurer l'intégration de la recherche pour chaque compartiment.

- PUT Bucket metadata notification configuration

  La demande de configuration DE notification DE métadonnées PUT compartiments vous permet d'activer le service d'intégration de la recherche pour chaque compartiment. Le XML de configuration de notification de métadonnées que vous fournissez dans le corps de la requête spécifie les objets dont les métadonnées sont envoyées à l'index de recherche de destination.

- DEMANDE d'utilisation du stockage

  La demande GET Storage usage vous indique la quantité totale de stockage utilisée par un compte et pour chaque compartiment associé au compte.

- Demandes de compartiments obsolètes pour la conformité des anciennes

  Vous devrez peut-être utiliser l'API REST StorageGRID S3 pour gérer les compartiments qui ont été créés à l'aide de la fonctionnalité de conformité héritée.

DEMANDE de cohérence des compartiments

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

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

Pour effectuer cette opération, vous disposez de l'autorisation s3:GetBucketConsistency, ou d'un compte root.

Exemple de demande

```
GET /bucket?x-ntap-sg-consistency HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

Réponse

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

Contrôle de cohérence	Description
tous	Tous les nœuds reçoivent les données immédiatement, sinon la requête échoue.
forte croissance mondiale	Garantit une cohérence de lecture après écriture pour toutes les demandes client sur tous les sites.
site fort	Garantit la cohérence de lecture après écriture pour toutes les demandes client dans un site.
lecture-après-nouvelle-écriture	(Valeur par défaut) assure la cohérence en lecture après écriture des nouveaux objets et la cohérence des mises à jour des objets. Offre une haute disponibilité et une protection des données garanties. Le correspondance le plus étroite avec les garanties de cohérence Amazon S3. **Remarque :** si votre application utilise des demandes HEAD sur des objets qui n'existent pas, vous pouvez recevoir un nombre élevé de 500 erreurs de serveur interne si un ou plusieurs nœuds de stockage ne sont pas disponibles. Pour éviter ces erreurs, définissez le contrôle de cohérence sur « disponible », sauf si vous avez besoin de garanties de cohérence similaires à Amazon S3.

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

Exemple de réponse

```
HTTP/1.1 200 OK
Date: Fri, 18 Sep 2020 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/11.5.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<Consistency xmlns="http://s3.storagegrid.com/doc/2015-02-01/">read-after-
new-write</Consistency>
```

Informations associées

Contrôles de cohérence

PUT Bucket Consistency demandée

La demande de cohérence PUT bucket permet de spécifier le niveau de cohérence à appliquer aux opérations effectuées dans un compartiment.

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

Vous disposez de l'autorisation s3:PutBuckeConsistency, ou soyez root de compte, pour effectuer cette opération.

Demande

Le `x-ntap-sg-consistency` le paramètre doit contenir l'une des valeurs suivantes :

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

Contrôle de cohérence	Description
forte croissance mondiale	Garantit une cohérence de lecture après écriture pour toutes les demandes client sur tous les sites.
site fort	Garantit la cohérence de lecture après écriture pour toutes les demandes client dans un site.
lecture-après-nouvelle-écriture	(Valeur par défaut) assure la cohérence en lecture après écriture des nouveaux objets et la cohérence des mises à jour des objets. Offre une haute disponibilité et une protection des données garanties. Le correspondance le plus étroite avec les garanties de cohérence Amazon S3. **Remarque :** si votre application utilise des demandes HEAD sur des objets qui n'existent pas, vous pouvez recevoir un nombre élevé de 500 erreurs de serveur interne si un ou plusieurs nœuds de stockage ne sont pas disponibles. Pour éviter ces erreurs, définissez le contrôle de cohérence sur « disponible », sauf si vous avez besoin de garanties de cohérence similaires à Amazon S3.
Disponible (cohérence possible pour les opérations DE TÊTE)	Se comporte de la même manière que le niveau de cohérence « entre la date et la nouvelle écriture », mais n'assure qu'une cohérence éventuelle pour les opérations DE TÊTE. Niveaux de disponibilité supérieurs à ceux de la « nouvelle écriture » en cas d'indisponibilité des nœuds de stockage Diffère des garanties de cohérence Amazon S3 pour les opérations HEAD uniquement.

Remarque: en général, vous devez utiliser la valeur de contrôle de cohérence "entre les nouvelles écritures". Si les demandes ne fonctionnent pas correctement, modifiez le comportement du client de l'application si possible. Ou configurez le client afin de spécifier le contrôle de cohérence pour chaque requête d'API. Réglez le contrôle de cohérence au niveau du godet uniquement en dernier recours.

Exemple de demande

```
PUT /bucket?x-ntap-sg-consistency=strong-global HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

Informations associées

Contrôles de cohérence

DEMANDE DE dernier accès au compartiment

La demande D'heure de dernier accès À GET Bucket vous permet de déterminer si les dernières mises à jour de temps d'accès sont activées ou désactivées pour les compartiments individuels.

Vous disposez de l'autorisation s3:GetBucketLastAccessTime, ou d'un compte root, pour effectuer cette opération.

Exemple de demande

```
GET /bucket?x-ntap-sg-lastaccesstime HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

Exemple de réponse

Cet exemple montre que les mises à jour du temps de dernier accès sont activées pour le compartiment.

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/10.3.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<LastAccessTime xmlns="http://s3.storagegrid.com/doc/2015-02-01/">enabled
</LastAccessTime>
```

DEMANDE de temps de dernier accès au compartiment

La demande d'heure de dernier accès AU compartiment PERMET d'activer ou de désactiver les mises à jour des temps de dernier accès pour chaque compartiment. La désactivation des mises à jour du temps d'accès précédent améliore les performances. Il s'agit du paramètre par défaut pour tous les compartiments créés avec la version 10.3.0, ou ultérieure.

Pour terminer cette opération, vous disposez de l'autorisation s3:PutBuckLastAccessTime pour un compartiment, ou etre root pour un compte.

À partir de StorageGRID version 10.3, les mises à jour de l'heure du dernier accès sont désactivées par défaut pour tous les nouveaux compartiments. Si des compartiments ont été créés à l'aide d'une version antérieure de StorageGRID et que vous souhaitez faire correspondre le nouveau comportement par défaut, vous devez désactiver explicitement les mises à jour de la dernière heure d'accès pour chacune de ces rubriques précédentes. Vous pouvez activer ou désactiver les mises à jour de l'heure du dernier accès à l'aide de la demande D'heure du dernier accès AU compartiment, de la case **S3 seaux Modifier le dernier paramètre d'accès** dans le Gestionnaire de locataires ou de l'API de gestion des locataires.

Si les dernières mises à jour de temps d'accès sont désactivées pour un compartiment, les opérations suivantes sont appliquées sur le compartiment :

- LES demandes GET Object, GET Object ACL, GET Object Tagging et HEAD Object ne mettent pas à jour l'heure du dernier accès. L'objet n'est pas ajouté aux files d'attente pour l'évaluation de la gestion du cycle de vie des informations (ILM).
- PUT Object : les demandes de copie et DE BALISAGE d'objets QUI mettent à jour uniquement les métadonnées mettent également à jour l'heure du dernier accès. L'objet est ajouté aux files d'attente pour l'évaluation ILM.
- Si les mises à jour de l'heure du dernier accès sont désactivées pour le compartiment source, PLACER l'objet - les demandes de copie ne mettent pas à jour l'heure du dernier accès pour le compartiment source. L'objet copié n'est pas ajouté aux files d'attente pour l'évaluation ILM du compartiment source. Cependant, pour la destination, PLACER l'objet - demandes de copie toujours mettre à jour l'heure du dernier accès. La copie de l'objet est ajoutée aux files d'attente pour l'évaluation ILM.
- Terminer les demandes de téléchargement de pièces multiples mises à jour de l'heure de dernier accès. L'objet terminé est ajouté aux files d'attente pour l'évaluation ILM.

Exemples de demandes

Cet exemple permet d'activer le temps du dernier accès pour un compartiment.

```
PUT /bucket?x-ntap-sg-lastaccesstime=enabled HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

Cet exemple désactive l'heure du dernier accès pour un compartiment.

```
PUT /bucket?x-ntap-sg-lastaccesstime=disabled HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

Informations associées

Utilisez le compte du locataire

SUPPRIME la demande de configuration de notification des métadonnées de compartiment

La demande de configuration DE notification DE métadonnées DELETE Bucket vous permet de désactiver le service d'intégration de recherche pour les compartiments individuels en supprimant le XML de configuration.

Pour effectuer cette opération, vous disposez de l'autorisation s3:DeleteBucketMetadanotification pour un compartiment, ou être un compte root.

Exemple de demande

Cet exemple montre la désactivation du service d'intégration de recherche pour un compartiment.

```
DELETE /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

LIRE la demande de configuration de notification des métadonnées de compartiment

La demande de configuration DE notification DE métadonnées GET Bucket vous permet de récupérer le XML de configuration utilisé pour configurer l'intégration de la recherche pour chaque compartiment.

Pour terminer cette opération, vous disposez de l'autorisation s3:GetBuckeMetadatanotification, ou d'un compte root.

Exemple de demande

Cette demande récupère la configuration de notification des métadonnées pour le compartiment nommé `bucket`.

```
GET /bucket?x-ntap-sg-metadata-notification HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

Réponse

L'organe de réponse inclut la configuration de notification des métadonnées pour le compartiment. La configuration de notification des métadonnées vous permet de déterminer la configuration du compartiment pour l'intégration de la recherche. En d'autres termes, il vous permet de déterminer les objets à indexer et à quels terminaux leurs métadonnées d'objet sont envoyées.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>rule-status</Status>
        <Prefix>key-prefix</Prefix>
        <Destination>
           <Urn>arn:aws:es:_region:account-
ID_:domain/_mydomain/myindex/mytype_</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Rule-2</ID>
         ...
    </Rule>
     ...
</MetadataNotificationConfiguration>
```

Chaque configuration de notification de métadonnées comprend une ou plusieurs règles. Chaque règle indique les objets qu'elle s'applique ainsi que la destination à laquelle StorageGRID doit envoyer les métadonnées d'objet. Les destinations doivent être spécifiées à l'aide de l'URN d'un terminal StorageGRID.

Nom	Description	Obligatoire
Configuration de la MetadaNotificationConfiguration	Balise de conteneur pour les règles utilisées pour spécifier les objets et la destination des notifications de métadonnées. Contient un ou plusieurs éléments de règle.	Oui.
Règle	Balise de conteneur d'une règle qui identifie les objets dont les métadonnées doivent être ajoutées à un index spécifié. Les règles avec des préfixes qui se chevauchent sont rejetées. Inclus dans l'élément MetadaNotificationConfiguration.	Oui.
ID	Identifiant unique de la règle. Inclus dans l'élément règle.	Non

Nom	Description	Obligatoire
État	L'état peut être « activé » ou « désactivé ». Aucune action n'est prise pour les règles désactivées. Inclus dans l'élément règle.	Oui.
Préfixe	Les objets qui correspondent au préfixe sont affectés par la règle et leurs métadonnées sont envoyées à la destination spécifiée. Pour faire correspondre tous les objets, spécifiez un préfixe vide. Inclus dans l'élément règle.	Oui.
Destination	Balise de conteneur pour la destination d'une règle. Inclus dans l'élément règle.	Oui.

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

Exemple de réponse

XML inclus entre le `<MetadataNotificationConfiguration></MetadataNotificationConfiguration>` les balises indiquent comment l'intégration avec un terminal d'intégration de la recherche est configurée pour le compartiment. Dans cet exemple, les métadonnées d'objet sont envoyées à un index Elasticsearch nommé `current` et le type nommé `2017` Hébergé dans un domaine AWS nommé `records`.

```
HTTP/1.1 200 OK
Date: Thu, 20 Jul 2017 18:24:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/11.0.0
x-amz-request-id: 3832973499
Content-Length: 264
Content-Type: application/xml

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix>2017</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-
1:3333333:domain/records/current/2017</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

Informations associées

Utilisez le compte du locataire

PUT Bucket metadata notification configuration

La demande de configuration DE notification DE métadonnées PUT compartiments vous permet d'activer le service d'intégration de la recherche pour chaque compartiment. Le XML de configuration de notification de métadonnées que vous fournissez dans le corps de la requête spécifie les objets dont les métadonnées sont envoyées à l'index de recherche de destination.

Pour effectuer cette opération, vous disposez de l'autorisation s3:PutBuckeMetadanotification pour un compartiment ou être un compte root.

Demande

La demande doit inclure la configuration de notification de métadonnées dans l'organisme de demande. Chaque configuration de notification de métadonnées comprend une ou plusieurs règles. Chaque règle spécifie les objets à lesquels elle s'applique, ainsi que la destination vers laquelle StorageGRID doit envoyer les métadonnées d'objet.

Les objets peuvent être filtrés sur le préfixe du nom de l'objet. Par exemple, vous pouvez envoyer les métadonnées pour les objets avec le préfixe `/images` à une destination et à des objets avec le préfixe `/videos` à un autre.

Les configurations dont les préfixes se chevauchent ne sont pas valides et sont rejetées lors de leur envoi. Par exemple, une configuration comprenant une règle pour les objets avec le préfixe `test` et une seconde règle pour les objets avec le préfixe `test2` ne serait pas autorisé.

Les destinations doivent être spécifiées à l'aide de l'URN d'un terminal StorageGRID. Le noeud final doit exister lorsque la configuration de notification de métadonnées est soumise, ou que la demande échoue en tant que `400 Bad Request`. Le message d'erreur indique : `Unable to save the metadata notification (search) policy. The specified endpoint URN does not exist: URN`.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>rule-status</Status>
        <Prefix>key-prefix</Prefix>
        <Destination>
           <Urn>arn:aws:es:region:account-
ID:domain/mydomain/myindex/mytype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Rule-2</ID>
         ...
    </Rule>
     ...
</MetadataNotificationConfiguration>
```

Le tableau décrit les éléments du XML de configuration de notification des métadonnées.

Nom	Description	Obligatoire
Configuration de la MetadaNotificationConfiguration	Balise de conteneur pour les règles utilisées pour spécifier les objets et la destination des notifications de métadonnées. Contient un ou plusieurs éléments de règle.	Oui.
Règle	Balise de conteneur d'une règle qui identifie les objets dont les métadonnées doivent être ajoutées à un index spécifié. Les règles avec des préfixes qui se chevauchent sont rejetées. Inclus dans l'élément MetadaNotificationConfiguration.	Oui.
ID	Identifiant unique de la règle. Inclus dans l'élément règle.	Non

Nom	Description	Obligatoire
État	L'état peut être « activé » ou « désactivé ». Aucune action n'est prise pour les règles désactivées. Inclus dans l'élément règle.	Oui.
Préfixe	Les objets qui correspondent au préfixe sont affectés par la règle et leurs métadonnées sont envoyées à la destination spécifiée. Pour faire correspondre tous les objets, spécifiez un préfixe vide. Inclus dans l'élément règle.	Oui.
Destination	Balise de conteneur pour la destination d'une règle. Inclus dans l'élément règle.	Oui.

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

Exemples de demandes

Cet exemple montre l'activation de l'intégration de la recherche pour un compartiment. Dans cet exemple, les métadonnées d'objet de tous les objets sont envoyées vers la même destination.

```
PUT /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>

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

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

```
PUT /graphics?x-ntap-sg-metadata-notification HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>

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

JSON généré par le service d'intégration de la recherche

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

Cet exemple montre un exemple de fichier JSON qui peut être généré lorsqu'un objet doté de la clé est associé `SGWS/Tagging.txt` est créé dans un compartiment nommé `test`. Le `test` le compartiment n'est pas multiversion `versionId` l'étiquette est vide.

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

Métadonnées d'objet incluses dans les notifications de métadonnées

Le tableau répertorie tous les champs inclus dans le document JSON qui est envoyé au noeud final de destination lorsque l'intégration de la recherche est activée.

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

Type	Nom de l'élément	Description
Informations sur les compartiments et les objets	godet	Nom du compartiment
Informations sur les compartiments et les objets	clé	Nom de clé d'objet
Informations sur les compartiments et les objets	ID de version	Version d'objet, pour les objets dans les compartiments multiversion
Informations sur les compartiments et les objets	région	Zone de godet, par exemple `us-east-1`
Métadonnées de système	taille	Taille de l'objet (en octets) visible par un client HTTP
Métadonnées de système	md5	Hachage d'objets
Métadonnées d'utilisateur	les métadonnées *`key:value`*	Toutes les métadonnées utilisateur pour l'objet, comme paires de clé-valeur

Type	Nom de l'élément	Description
Étiquettes	balises *key:value*	Toutes les balises d'objet définies pour l'objet, en tant que paires clé-valeur

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

Informations associées

Utilisez le compte du locataire

DEMANDE d'utilisation du stockage

La demande GET Storage usage vous indique la quantité totale de stockage utilisée par un compte et pour chaque compartiment associé au compte.

Le volume de stockage utilisé par un compte et ses compartiments peut être obtenu à l'aide d'une demande GET Service modifiée avec le `x-ntap-sg-usage` paramètre de requête. L'utilisation du stockage par compartiment est suivie séparément des demandes DE PUT et DELETE traitées par le système. Il peut y avoir un certain délai avant que les valeurs d'utilisation correspondent aux valeurs attendues en fonction du traitement des demandes, en particulier si le système est soumis à une charge importante.

Par défaut, StorageGRID tente de récupérer les informations d'utilisation à l'aide d'une cohérence globale forte. Si la cohérence globale forte ne peut pas être atteinte, StorageGRID tente de récupérer les informations d'utilisation avec une cohérence site élevée.

Vous disposez de l'autorisation s3:ListAllMyseaux, ou soyez root de compte, pour effectuer cette opération.

Exemple de demande

```
GET /?x-ntap-sg-usage HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

Exemple de réponse

Cet exemple montre un compte qui contient quatre objets et 12 octets de données dans deux compartiments. Chaque compartiment contient deux objets et six octets de données.

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 00:49:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/10.2.0
x-amz-request-id: 727237123
Content-Length: 427
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<UsageResult xmlns="http://s3.storagegrid.com/doc/2015-02-01">
<CalculationTime>2014-11-19T05:30:11.000000Z</CalculationTime>
<ObjectCount>4</ObjectCount>
<DataBytes>12</DataBytes>
<Buckets>
<Bucket>
<Name>bucket1</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
<Bucket>
<Name>bucket2</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
</Buckets>
</UsageResult>
```

Gestion des versions

Chaque version d'objet stockée contribuera à la `ObjectCount` et `DataBytes` valeurs dans la réponse. Les marqueurs de suppression ne sont pas ajoutés au `ObjectCount` total.

Informations associées

Contrôles de cohérence

Demandes de compartiment obsolètes pour la conformité des anciennes

Vous devrez peut-être utiliser l'API REST StorageGRID S3 pour gérer les compartiments qui ont été créés à l'aide de la fonctionnalité de conformité héritée.

Fonction de conformité obsolète

La fonctionnalité de conformité StorageGRID disponible dans les versions précédentes d'StorageGRID est obsolète et a été remplacée par le verrouillage d'objet S3.

Si vous avez précédemment activé le paramètre de conformité globale, le paramètre de verrouillage d'objet S3 global est activé dans StorageGRID 11.6. Vous ne pouvez plus créer de compartiments avec la conformité

activée. Toutefois, si nécessaire, vous pouvez utiliser l'API REST StorageGRID S3 pour gérer tous les compartiments conformes existants.

- Utilisez le verrouillage d'objet S3
- Gestion des objets avec ILM
- "Base de connaissances NetApp : comment gérer des compartiments conformes aux ancienne génération dans StorageGRID 11.5"

Demandes de conformité obsolètes :

- Obsolète - METTRE les modifications de la demande de godet à des fins de conformité

  L'élément XML SGCompliance est obsolète. Auparavant, vous pouviez inclure cet élément personnalisé StorageGRID dans le corps de demande XML facultatif de requêtes Put Bucket pour créer un compartiment conforme.

- Obsolète : RÉCUPÉRER la demande de conformité du compartiment

  La demande DE conformité DE GET Bucket est obsolète. Cependant, vous pouvez continuer à utiliser cette demande pour déterminer les paramètres de conformité actuellement en vigueur pour un compartiment compatible existant.

- Obsolète - PUT Bucket Compliance request

  La demande de conformité PUT Bucket est obsolète. Cependant, vous pouvez continuer à utiliser cette demande pour modifier les paramètres de conformité d'un compartiment conforme existant. Par exemple, vous pouvez placer un compartiment existant en attente légale ou augmenter sa période de conservation.

Obsolète : METTEZ les modifications de la demande de compartiment à des fins de conformité

L'élément XML SGCompliance est obsolète. Auparavant, vous pouviez inclure cet élément personnalisé StorageGRID dans le corps de demande XML facultatif de requêtes Put Bucket pour créer un compartiment conforme.

> La fonctionnalité de conformité StorageGRID disponible dans les versions précédentes d'StorageGRID est obsolète et a été remplacée par le verrouillage d'objet S3.

Utilisez le verrouillage d'objet S3

Gestion des objets avec ILM

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

Vous ne pouvez plus créer de compartiments avec la fonctionnalité conformité activée. Le message d'erreur suivant s'affiche si vous tentez d'utiliser les modifications de demande DE MISE en godet pour la conformité afin de créer un nouveau compartiment conforme :

```
The Compliance feature is deprecated.
Contact your StorageGRID administrator if you need to create new Compliant
buckets.
```

Informations associées

Gestion des objets avec ILM

Utilisez le compte du locataire

Obsolète : RÉCUPÉRER la demande de conformité du compartiment

La demande DE conformité DE GET Bucket est obsolète. Cependant, vous pouvez continuer à utiliser cette demande pour déterminer les paramètres de conformité actuellement en vigueur pour un compartiment compatible existant.

> La fonctionnalité de conformité StorageGRID disponible dans les versions précédentes d'StorageGRID est obsolète et a été remplacée par le verrouillage d'objet S3.

Utilisez le verrouillage d'objet S3

Gestion des objets avec ILM

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

Vous disposez de l'autorisation s3:GetBucketCompliance, ou d'un compte root, pour effectuer cette opération.

Exemple de demande

Cet exemple de demande vous permet de déterminer les paramètres de conformité pour le compartiment nommé `mybucket`.

```
GET /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

Exemple de réponse

Dans le XML de réponse, `<SGCompliance>` le répertorie les paramètres de conformité utilisés pour le compartiment. Cet exemple de réponse montre les paramètres de conformité d'un compartiment dans lequel chaque objet sera conservé pendant un an (525,600 minutes), à partir de l'ingestion de l'objet dans la grille. Il n'y a actuellement aucune retenue légale sur ce godet. Chaque objet sera automatiquement supprimé après un an.

```
HTTP/1.1 200 OK
Date: <em>date</em>
Connection: <em>connection</em>
Server: StorageGRID/11.1.0
x-amz-request-id: <em>request ID</em>
Content-Length: <em>length</em>
Content-Type: application/xml

<SGCompliance>
  <RetentionPeriodMinutes>525600</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

Nom	Description
RetentionPeriodMinutes	Durée de conservation des objets ajoutés à ce compartiment, en minutes. La période de conservation commence lorsque l'objet est ingéré dans la grille.
LegalHold	• Vrai : ce compartiment est actuellement en attente légale. Les objets de ce compartiment ne peuvent pas être supprimés tant que la conservation légale n'est pas levée, même si leur période de conservation a expiré. • Faux : ce godet n'est pas actuellement en attente légale. Les objets de ce compartiment peuvent être supprimés à la fin de leur période de conservation.
Suppression automatique	• Vrai : les objets de ce compartiment sont automatiquement supprimés lors de leur expiration, à moins que le compartiment ne soit soumis à une obligation légale. • FALSE : les objets de ce compartiment ne sont pas supprimés automatiquement lorsque la période de conservation expire. Vous devez supprimer ces objets manuellement si vous devez les supprimer.

Réponses d'erreur

Si le compartiment n'a pas été créé pour être conforme, le code d'état HTTP de la réponse est `404 Not Found`, Avec un code d'erreur S3 de `XNoSuchBucketCompliance`.

Informations associées

Gestion des objets avec ILM

Utilisez le compte du locataire

Obsolète : PUT Bucket Compliance request

La demande de conformité PUT Bucket est obsolète. Cependant, vous pouvez continuer à utiliser cette demande pour modifier les paramètres de conformité d'un compartiment conforme existant. Par exemple, vous pouvez placer un compartiment existant en attente légale ou augmenter sa période de conservation.

> La fonctionnalité de conformité StorageGRID disponible dans les versions précédentes d'StorageGRID est obsolète et a été remplacée par le verrouillage d'objet S3.

Utilisez le verrouillage d'objet S3

Gestion des objets avec ILM

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

Vous disposez de l'autorisation s3:PutBuckeCompliance, ou d'un compte root, pour effectuer cette opération.

Vous devez spécifier une valeur pour chaque champ des paramètres de conformité lors de l'émission d'une demande de conformité PUT Bucket.

Exemple de demande

Cet exemple de demande modifie les paramètres de conformité du compartiment nommé `mybucket`. Dans cet exemple, objets dans `mybucket` sera maintenant conservé pendant deux ans (1,051,200 minutes) au lieu d'un an, à partir de l'ingestion de l'objet dans le grid. Il n'y a pas de retenue légale sur ce godet. Chaque objet sera automatiquement supprimé après deux ans.

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization name</em>
Host: <em>host</em>
Content-Length: 152

<SGCompliance>
  <RetentionPeriodMinutes>1051200</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

Nom	Description
RetentionPeriodMinutes	Durée de conservation des objets ajoutés à ce compartiment, en minutes. La période de conservation commence lorsque l'objet est ingéré dans la grille. **Attention:** lorsque vous spécifiez une nouvelle valeur pour RetentionPeriodMinutes, vous devez spécifier une valeur égale ou supérieure à la période de rétention actuelle du godet. Une fois la période de rétention du godet définie, vous ne pouvez pas la réduire ; vous pouvez uniquement l'augmenter.
LegalHold	• Vrai : ce compartiment est actuellement en attente légale. Les objets de ce compartiment ne peuvent pas être supprimés tant que la conservation légale n'est pas levée, même si leur période de conservation a expiré. • Faux : ce godet n'est pas actuellement en attente légale. Les objets de ce compartiment peuvent être supprimés à la fin de leur période de conservation.
Suppression automatique	• Vrai : les objets de ce compartiment sont automatiquement supprimés lors de leur expiration, à moins que le compartiment ne soit soumis à une obligation légale. • FALSE : les objets de ce compartiment ne sont pas supprimés automatiquement lorsque la période de conservation expire. Vous devez supprimer ces objets manuellement si vous devez les supprimer.

Niveau de cohérence des paramètres de conformité

Lorsque vous mettez à jour les paramètres de conformité d'un compartiment S3 avec une demande DE conformité PUT bucket, StorageGRID tente de mettre à jour les métadonnées du compartiment dans la grille. Par défaut, StorageGRID utilise le niveau de cohérence **Strong-global** pour garantir que tous les sites de data Center et tous les nœuds de stockage contenant des métadonnées de compartiment sont cohérents en lecture après écriture pour les paramètres de conformité modifiés.

Si StorageGRID ne peut pas atteindre le niveau de cohérence **Strong-global** car un site de centre de données ou plusieurs nœuds de stockage sur un site ne sont pas disponibles, le code d'état HTTP de la réponse est `503 Service Unavailable.`

Si vous recevez cette réponse, vous devez contacter l'administrateur du grid pour vous assurer que les services de stockage requis sont disponibles dans les plus brefs délais. Si l'administrateur de la grille ne parvient pas à mettre suffisamment de nœuds de stockage sur chaque site, le support technique vous demandera peut-être de relancer la demande échouée en forçant le niveau de cohérence **site fort**.

Ne forcez jamais le niveau de cohérence **site fort** pour la conformité DU godet DE MISE à moins que vous n'ayez été invité à le faire par le support technique et à moins que vous compreniez les conséquences possibles de l'utilisation de ce niveau.

Lorsque le niveau de cohérence est réduit à **strong-site**, StorageGRID garantit que les paramètres de conformité mis à jour auront une cohérence lecture-après-écriture uniquement pour les requêtes client au sein d'un site. Il est donc possible que le système StorageGRID dispose de plusieurs paramètres incohérents pour ce compartiment jusqu'à ce que tous les sites et nœuds de stockage soient disponibles. Les paramètres incohérents peuvent entraîner un comportement inattendu et indésirable. Par exemple, si vous placez un compartiment sous une obligation légale et que vous forcez un niveau de cohérence inférieur, les paramètres de conformité précédents du compartiment (c'est-à-dire la conservation légale) peuvent continuer à être en vigueur sur certains sites de data Center. Par conséquent, les objets qui, selon vous, sont en attente légale peuvent être supprimés à l'expiration de leur période de conservation, soit par l'utilisateur, soit par AutoDelete, si cette option est activée.

Pour forcer l'utilisation du niveau de cohérence **site fort**, réémettez la demande de conformité Put et incluez le `Consistency-Control` En-tête de requête HTTP, comme suit :

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Consistency-Control: strong-site
```

Réponses d'erreur

- Si le compartiment n'a pas été créé pour être conforme, le code d'état HTTP de la réponse est `404 Not Found`.
- Si `RetentionPeriodMinutes` Dans la demande est inférieure à la période de conservation actuelle du compartiment, le code d'état HTTP est `400 Bad Request`.

Informations associées

Obsolète : METTEZ les modifications de la demande de compartiment à des fins de conformité

Utilisez le compte du locataire

Gestion des objets avec ILM

Règles d'accès au compartiment et au groupe

StorageGRID utilise le langage de règles Amazon Web Services (AWS) pour permettre aux locataires S3 de contrôler l'accès aux compartiments et aux objets dans ces compartiments. Le système StorageGRID implémente un sous-ensemble du langage de règles de l'API REST S3. Les règles d'accès de l'API S3 sont écrites au format JSON.

Présentation de la stratégie d'accès

Il existe deux types de politiques d'accès pris en charge par StorageGRID.

- **Les règles de compartiment**, qui sont configurées à l'aide de la stratégie DE compartiment, DE LA règle DE compartiment PUT et DES opérations de L'API S3 de la politique de compartiment. Les règles de compartiment sont liées aux compartiments. Elles sont donc configurées de façon à contrôler l'accès des

utilisateurs du compte du propriétaire du compartiment ou d'autres comptes au compartiment et aux objets. Une politique de compartiment s'applique à un seul compartiment et peut-être à plusieurs groupes.

- **Stratégies de groupe**, qui sont configurées à l'aide du Gestionnaire de locataires ou de l'API de gestion des locataires. Les stratégies de groupe sont associées à un groupe du compte, de sorte qu'elles sont configurées de manière à permettre à ce groupe d'accéder à des ressources spécifiques appartenant à ce compte. Une stratégie de groupe s'applique à un seul groupe et peut-être plusieurs compartiments.

Les règles de compartiment et de groupe StorageGRID respectent une grammaire spécifique définie par Amazon. À l'intérieur de chaque règle se trouve un ensemble d'énoncés de politique, et chaque instruction contient les éléments suivants :

- ID de déclaration (ID) (facultatif)
- Effet
- Principal/notPrincipal
- Ressource/NotResource
- Action/NotAction
- Condition (en option)

Les instructions de règles sont créées à l'aide de cette structure pour spécifier les autorisations : accorder l'effet à Autoriser/refuser l'action sur la ressource lorsque la condition s'applique.

Chaque élément de règle est utilisé pour une fonction spécifique :

Elément	Description
SID	L'élément Sid est facultatif. Le SID n'est destiné qu'à la description de l'utilisateur. Il est stocké mais non interprété par le système StorageGRID.
Effet	Utilisez l'élément d'effet pour déterminer si les opérations spécifiées sont autorisées ou refusées. Vous devez identifier les opérations que vous autorisez (ou refusez) les compartiments ou les objets à l'aide des mots clés action Element pris en charge.
Principal/notPrincipal	Vous pouvez autoriser les utilisateurs, groupes et comptes à accéder à des ressources spécifiques et à effectuer des actions spécifiques. Si aucune signature S3 n'est incluse dans la demande, l'accès anonyme est autorisé en spécifiant le caractère générique (*) comme principal. Par défaut, seul le root du compte peut accéder aux ressources qui lui sont propres. Il vous suffit de spécifier l'élément principal dans une stratégie de rubrique. Pour les stratégies de groupe, le groupe auquel la stratégie est associée est l'élément principal implicite.
Ressource/NotResource	L'élément ressource identifie les compartiments et les objets. Vous pouvez autoriser ou refuser des autorisations pour les compartiments et les objets en utilisant le nom de ressource Amazon (ARN) pour identifier la ressource.

Elément	Description
Action/NotAction	Les éléments action et effet sont les deux composants des autorisations. Lorsqu'un groupe demande une ressource, l'accès à la ressource est accordé ou refusé. L'accès est refusé sauf si vous attribuez des autorisations spécifiques, mais vous pouvez utiliser le refus explicite pour remplacer une autorisation accordée par une autre stratégie.
Condition	L'élément condition est facultatif. Les conditions vous permettent de créer des expressions pour déterminer quand une stratégie doit être appliquée.

Dans l'élément action, vous pouvez utiliser le caractère générique (*) pour spécifier toutes les opérations ou un sous-ensemble d'opérations. Par exemple, cette action correspond à des autorisations telles que s3:GetObject, s3:PutObject et s3:DeleteObject.

```
s3:*Object
```

Dans l'élément ressource, vous pouvez utiliser les caractères génériques (*) et (?). Alors que l'astérisque (*) correspond à 0 caractères ou plus, le point d'interrogation (?) correspond à n'importe quel caractère.

Dans l'élément principal, les caractères génériques ne sont pas pris en charge sauf pour définir un accès anonyme, qui accorde la permission à tous. Par exemple, vous définissez le caractère générique (*) comme valeur principale.

```
"Principal":"*"
```

Dans l'exemple suivant, l'instruction utilise les éléments effet, principal, action et ressource. Cet exemple montre une instruction de stratégie de compartiment complète qui utilise l'effet « Autoriser » pour donner les responsables, le groupe admin `federated-group/admin` et le groupe financier `federated-group/finance`, Autorisations d'exécution de l'action `s3:ListBucket` sur le compartiment nommé `mybucket` Et l'action `s3:GetObject` sur tous les objets à l'intérieur de ce godet.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::27233906934684427525:federated-group/admin",
          "arn:aws:iam::27233906934684427525:federated-group/finance"
        ]
      },
      "Action": [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:iam:s3:::mybucket",
        "arn:aws:iam:s3:::mybucket/*"
      ]
    }
  ]
}
```

La stratégie de compartiment a une taille limite de 20,480 octets et la stratégie de groupe a une taille limite de 5,120 octets.

Informations associées

Utilisez le compte du locataire

Paramètres de contrôle de cohérence des règles

Par défaut, toutes les mises à jour apportées aux stratégies de groupe sont cohérentes. Une fois la stratégie de groupe cohérente, les modifications peuvent prendre 15 minutes supplémentaires à appliquer en raison de la mise en cache des règles. Par défaut, toutes les mises à jour effectuées sur les règles de compartiment sont également cohérentes en définitive.

Si nécessaire, vous pouvez modifier les garanties de cohérence pour les mises à jour des règles de compartiment. Par exemple, il peut être intéressant de vouloir modifier cette règle afin qu'elle devienne effective dès que possible pour des raisons de sécurité.

Dans ce cas, vous pouvez définir le `Consistency-Control` L'en-tête de la demande de stratégie PUT Bucket ou vous pouvez utiliser la demande DE cohérence PUT Bucket. Lorsque vous modifiez le contrôle de cohérence pour cette demande, vous devez utiliser la valeur **All**, qui fournit la garantie la plus élevée de cohérence de lecture après écriture. Si vous spécifiez une autre valeur de contrôle de cohérence dans un en-tête pour la demande DE cohérence PUT Bucket, la demande sera rejetée. Si vous spécifiez une autre valeur pour une demande de stratégie PUT Bucket, la valeur sera ignorée. Une fois la règle de compartiment cohérente, les modifications peuvent prendre 8 secondes supplémentaires pour effet, grâce à la mise en cache des règles.

Si vous définissez le niveau de cohérence sur **All** pour forcer une nouvelle stratégie de godet à devenir efficace plus tôt, veillez à remettre le contrôle au niveau du godet à sa valeur d'origine lorsque vous avez terminé. Sinon, toutes les futures demandes de rubrique utiliseront le paramètre **tous**.

Utilisez ARN dans les énoncés de politique

Dans les instructions de politique, le ARN est utilisé dans les éléments principal et ressource.

- Utilisez cette syntaxe pour spécifier la ressource S3 ARN :

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

- Utilisez cette syntaxe pour spécifier la ressource d'identité ARN (utilisateurs et groupes) :

```
arn:aws:iam::account_id:root
arn:aws:iam::account_id:user/user_name
arn:aws:iam::account_id:group/group_name
arn:aws:iam::account_id:federated-user/user_name
arn:aws:iam::account_id:federated-group/group_name
```

Autres considérations :

- Vous pouvez utiliser l'astérisque (*) comme caractère générique pour correspondre à zéro ou plus de caractères dans la clé d'objet.
- Les caractères internationaux, qui peuvent être spécifiés dans la clé d'objet, doivent être codés à l'aide de JSON UTF-8 ou de séquences d'échappement JSON \u. Le codage pourcentage n'est pas pris en charge.

  "Syntaxe RFC 2141 URN"

  Le corps de requête HTTP pour l'opération de stratégie PUT Bucket doit être codé avec charset=UTF-8.

Spécifiez les ressources dans une stratégie

Dans les instructions de stratégie, vous pouvez utiliser l'élément ressource pour spécifier le compartiment ou l'objet pour lequel les autorisations sont autorisées ou refusées.

- Chaque instruction de stratégie nécessite un élément ressource. Dans une politique, les ressources sont signalées par l'élément `Resource`, ou alternativement, `NotResource` pour exclusion.
- Vous spécifiez des ressources avec une ressource S3 ARN. Par exemple :

```
"Resource": "arn:aws:s3:::mybucket/*"
```

- Vous pouvez également utiliser des variables de règles à l'intérieur de la clé d'objet. Par exemple :

```
"Resource": "arn:aws:s3:::mybucket/home/${aws:username}/*"
```

- La valeur de ressource peut spécifier un compartiment qui n'existe pas encore lorsqu'une stratégie de groupe est créée.

Informations associées

Spécifiez les variables d'une règle

Spécifiez les entités de gestion dans une stratégie

Utilisez l'élément principal pour identifier l'utilisateur, le groupe ou le compte locataire qui est autorisé/refusé l'accès à la ressource par l'instruction de stratégie.

- Chaque énoncé de politique dans une politique de rubrique doit inclure un élément principal. Les énoncés de politique d'une politique de groupe n'ont pas besoin de l'élément principal car le groupe est compris comme principal.
- Dans une politique, les principes sont indiqués par l'élément « principal » ou « notprincipal » pour exclusion.
- Les identités basées sur les comptes doivent être spécifiées à l'aide d'un ID ou d'un ARN :

```
"Principal": { "AWS": "account_id"}
"Principal": { "AWS": "identity_arn" }
```

- Dans cet exemple, le compte locataire utilise l'ID 27233906934684427525, qui inclut le compte root et tous les utilisateurs du compte :

```
 "Principal": { "AWS": "27233906934684427525" }
```

- Vous pouvez spécifier uniquement la racine du compte :

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:root" }
```

- Vous pouvez spécifier un utilisateur fédéré spécifique (« Alex ») :

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
user/Alex" }
```

- Vous pouvez spécifier un groupe fédéré spécifique (« gestionnaires ») :

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
group/Managers"  }
```

- Vous pouvez spécifier un principal anonyme :

```
"Principal": "*"
```

- Pour éviter toute ambiguïté, vous pouvez utiliser l'UUID de l'utilisateur au lieu du nom d'utilisateur :

```
arn:aws:iam::27233906934684427525:user-uuid/de305d54-75b4-431b-adb2-
eb6b9e546013
```

  Par exemple, supposons que Alex quitte l'entreprise et le nom d'utilisateur `Alex` est supprimé. Si un nouveau Alex rejoint l'organisation et est affecté de la même façon `Alex` nom d'utilisateur, le nouvel utilisateur peut hériter involontairement des autorisations accordées à l'utilisateur d'origine.

- La valeur principale peut spécifier un nom de groupe/utilisateur qui n'existe pas encore lors de la création d'une stratégie de compartiment.

Spécifiez les autorisations dans une stratégie

Dans une stratégie, l'élément action est utilisé pour autoriser/refuser des autorisations à une ressource. Il existe un ensemble d'autorisations que vous pouvez spécifier dans une stratégie, qui sont désignées par l'élément « action » ou par « NotAction » pour exclusion. Chacun de ces éléments est associé à des opérations spécifiques d'API REST S3.

Le tableau répertorie les autorisations qui s'appliquent aux compartiments et aux autorisations qui s'appliquent aux objets.

> Amazon S3 utilise désormais l'autorisation s3:PutReplicationConfiguration pour les opérations de réplication de compartiments PUT et DELETE. StorageGRID utilise des autorisations distinctes pour chaque action, qui correspond à la spécification Amazon S3 d'origine.

> Une SUPPRESSION est effectuée lorsqu'un PUT est utilisé pour remplacer une valeur existante.

Autorisations qui s'appliquent aux compartiments

Autorisations	OPÉRATIONS DES API REST S3	Personnalisée pour StorageGRID
s3:CreateBucket	PLACER le godet	
s3:DeleteBucket	SUPPRIMER le compartiment	
s3:DeleteBuckeMetadatanotification	SUPPRIMEZ la configuration de notification des métadonnées de compartiment	Oui.

Autorisations	OPÉRATIONS DES API REST S3	Personnalisée pour StorageGRID
s3:DeleteBucketPolicy	SUPPRIMER la règle de compartiment	
s3:DeleteReplicationConfiguration	SUPPRIMER la réplication du compartiment	Oui, séparer les autorisations pour PUT et DELETE*
s3:GetBucketAcl	OBTENIR l'ACL du compartiment	
s3:GetBuckeCompliance	GARANTIR la conformité des compartiments (obsolète)	Oui.
s3:persistance GetBucketConsistency	OPTIMISEZ la cohérence des compartiments	Oui.
s3:GetBucketCORS	OBTENIR les godets	
s3:GetEncryptionConfiguration	CHIFFREMENT des compartiments	
s3:GetBucketLastAccessTime	HEURE du dernier accès au compartiment	Oui.
s3:GetBucketLocation	ACCÉDER à l'emplacement du compartiment	
s3:GetBucketMetadatanotification	CONFIGURATION DES notifications de métadonnées de compartiment	Oui.
s3:GetBuckenotification	GET Bucket notification	
s3:GetBuckeObjectLockConfiguration	OBTENIR la configuration de verrouillage d'objet	
s3:GetBucketPolicy	GET Bucket policy	
s3:GetBucketTagging	GET Bucket tagging	
s3:GetBucketVersioning	GESTION des versions des compartiments	
s3:GetLifecyclConfiguration	OPTIMISEZ le cycle de vie des compartiments	
s3:GetReplicationTM	RÉPLICATION des compartiments	

Autorisations	OPÉRATIONS DES API REST S3	Personnalisée pour StorageGRID
s3:ListAllMyseaux	• ACCÉDER au service • DÉCOUVREZ l'utilisation du stockage	Oui, pour BÉNÉFICIER DE l'utilisation DU stockage
s3:ListBucket	• OBTENIR le compartiment (liste d'objets) • Godet DE TÊTE • Restauration POST-objet	
s3:ListBuckMultipartUploads	• Liste des téléchargements partitionnés • Restauration POST-objet	
s3:ListBuckeVersions	OBTENIR les versions de compartiment	
s3:PutBuckeCompliance	MISE en conformité des compartiments (obsolète)	Oui.
s3:persistance de PutBuckeConsistency	PRÉSERVER la cohérence du godet	Oui.
s3:PutBuckeCORS	• SUPPRIMER les godets† • PLACEZ les godets	
s3:PutEncryptionConfiguration	• SUPPRIMER le chiffrement du compartiment • PUT Bucket Encryption	
s3:PutBuckeLastAccessTime	METTRE l'heure du dernier accès au compartiment	Oui.
s3:PutBuckeMetadanotification	CONFIGURATION de notification des métadonnées de compartiment	Oui.
s3:PutBuckenotification	PUT Bucket notification	

Autorisations	OPÉRATIONS DES API REST S3	Personnalisée pour StorageGRID
s3:PutBuckObjectLockConfiguration	• PLACEZ le godet avec le `x-amz-bucket-object-lock-enabled: true` En-tête de demande (nécessite également l'autorisation s3:CreateBucket) • CONFIGURATION du verrouillage de l'objet	
s3:PutBuckePolicy	PUT Bucket policy	
s3:PutBuckeTagging	• SUPPRIMER le marquage du compartiment† • PUT Bucket tagging	
s3:PutBuckeVersioning	GESTION des versions du compartiment	
s3:PutLifecyclConfiguration	• SUPPRIMER le cycle de vie du godet† • CYCLE de vie des compartiments	
s3:PutReplicationTM	RÉPLICATION des compartiments	Oui, séparer les autorisations pour PUT et DELETE*

Autorisations qui s'appliquent aux objets

Autorisations	OPÉRATIONS DES API REST S3	Personnalisée pour StorageGRID
s3:AbortMultipartUpload	• Abandonner le téléchargement de pièces multiples • Restauration POST-objet	
s3:DeleteObject	• SUPPRIMER l'objet • SUPPRIMER plusieurs objets • Restauration POST-objet	
s3:DeleteObjectTagging	SUPPRIMER le balisage d'objets	
s3:DeleteObjectVersionTagging	SUPPRIMER le balisage d'objets (une version spécifique de l'objet)	

Autorisations	OPÉRATIONS DES API REST S3	Personnalisée pour StorageGRID
s3:DeleteObjectVersion	SUPPRIMER l'objet (une version spécifique de l'objet)	
s3:GetObject	• OBTENIR l'objet • Objet TÊTE • Restauration POST-objet • SÉLECTIONNEZ contenu de l'objet	
s3:GetObjectAcl	OBTENIR l'ACL d'objet	
s3:GetObjectLegalHold	OBTENIR la mise en attente légale de l'objet	
s3:GetObjectRetention	OBTENIR la conservation des objets	
s3:GetObjectTagging	OBTENIR le balisage d'objets	
s3:GetObjectVersionTagging	OBTENIR le balisage d'objets (une version spécifique de l'objet)	
s3:GetObjectVersion	OBTENIR objet (une version spécifique de l'objet)	
s3:ListMultipartUploadParts	Répertorier les pièces, POST-restauration d'objet	
s3:PutObject	• PLACER l'objet • PLACER l'objet - Copier • Restauration POST-objet • Lancer le téléchargement de pièces multiples • Chargement de pièces multiples complet • Télécharger la pièce • Télécharger la pièce - Copier	
s3:PutObjectLegalHold	METTRE l'objet en attente légale	
s3:PutObjectRetention	CONSERVATION des objets	

Autorisations	OPÉRATIONS DES API REST S3	Personnalisée pour StorageGRID
s3:PutObjectTagging	PLACER le balisage d'objets	
s3:PutObjectVersionTagging	PUT Object Tagging (une version spécifique de l'objet)	
s3:PutOverwriteObject	• PLACER l'objet • PLACER l'objet - Copier • PUT Object tagging • SUPPRIMER le balisage d'objets • Chargement de pièces multiples complet	Oui.
s3:RestoreObject	Restauration POST-objet	

Utiliser l'autorisation PutOverwriteObject

L'autorisation s3:PutOverwriteObject est une autorisation StorageGRID personnalisée qui s'applique aux opérations qui créent ou mettent à jour des objets. Le paramètre de cette autorisation détermine si le client peut remplacer les données d'un objet, les métadonnées définies par l'utilisateur ou le balisage d'objets S3.

Les paramètres possibles pour cette autorisation sont les suivants :

- **Autoriser** : le client peut écraser un objet. Il s'agit du paramètre par défaut.
- **Deny** : le client ne peut pas écraser un objet. Lorsque cette option est définie sur Deny, l'autorisation PutOverwriteObject fonctionne comme suit :
  - Si un objet existant se trouve sur le même chemin :
    - Les données, les métadonnées définies par l'utilisateur ou le balisage d'objets S3 ne peuvent pas être remplacés.
    - Toutes les opérations d'entrée en cours sont annulées et une erreur est renvoyée.
    - Si la gestion des versions S3 est activée, le paramètre Deny empêche les opérations PUT Object tagging ou DELETE Object tagging de modifier le TagSet d'un objet et ses versions non actuelles.
  - Si aucun objet existant n'est trouvé, cette autorisation n'a aucun effet.
- Lorsque cette autorisation n'est pas présente, l'effet est le même que si autorisation a été définie.

> Si la politique S3 actuelle autorise le remplacement et que l'autorisation PutOverwriteObject est définie sur Deny, le client ne peut pas remplacer les données d'un objet, les métadonnées définies par l'utilisateur ou le balisage d'objets. En outre, si la case **empêcher modification client** est cochée (**CONFIGURATION système Options de grille**), ce paramètre remplace le paramètre de l'autorisation PutOverwriteObject.

Informations associées

Exemples de règles de groupe S3

Spécifiez les conditions dans une stratégie

Les conditions définissent le moment où une police sera en vigueur. Les conditions sont constituées d'opérateurs et de paires de clé-valeur.

Les conditions utilisent des paires de clé-valeur pour l'évaluation. Un élément condition peut contenir plusieurs conditions, et chaque condition peut contenir plusieurs paires clé-valeur. Le bloc condition utilise le format suivant :

```
Condition: {
     condition_type: {
          condition_key: condition_values
```

Dans l'exemple suivant, la condition ipaddress utilise la clé condition SourceIp.

```
"Condition": {
    "IpAddress": {
      "aws:SourceIp": "54.240.143.0/24"
        ...
},
        ...
```

Opérateurs de condition pris en charge

Les opérateurs de condition sont classés comme suit :

- Chaîne
- Valeur numérique
- Booléen
- Adresse IP
- Vérification nulle

Opérateurs de condition	Description
Equals à jambes de chaîne	Compare une clé à une valeur de chaîne en fonction de la correspondance exacte (sensible à la casse).
Equals stringNotEquals	Compare une clé à une valeur de chaîne basée sur la correspondance niée (sensible à la casse).
StringEqualisIgnoreCase	Compare une clé à une valeur de chaîne basée sur la correspondance exacte (ignore case).
StringNotEqualisIgnoreCase	Compare une clé à une valeur de chaîne basée sur la correspondance nérée (ignore le cas).

Opérateurs de condition	Description
StringLike	Compare une clé à une valeur de chaîne en fonction de la correspondance exacte (sensible à la casse). Peut inclure * et ? caractères génériques.
StringNotLike	Compare une clé à une valeur de chaîne basée sur la correspondance niée (sensible à la casse). Peut inclure * et ? caractères génériques.
Valeurs numériques	Compare une touche à une valeur numérique en fonction de la correspondance exacte.
NumericNotEquals	Compare une touche à une valeur numérique basée sur la correspondance annulée.
NumericGreaterThan	Compare une clé à une valeur numérique basée sur la comparaison « supérieure à ».
NumericGreaterThanEquals	Compare une clé à une valeur numérique basée sur la comparaison « supérieure ou égale ».
NumericLessThan	Compare une clé à une valeur numérique basée sur la comparaison « moins que ».
NumericLessThanEquals	Compare une clé à une valeur numérique basée sur la comparaison « inférieure à ou égale ».
BOOL	Compare une clé à une valeur booléenne basée sur la correspondance « vrai ou faux ».
Adresse IP	Compare une clé à une adresse IP ou une plage d'adresses IP.
Adresse de la note	Compare une clé à une adresse IP ou une plage d'adresses IP basée sur la correspondance annulée.
Nul	Vérifie si une clé condition est présente dans le contexte de demande actuel.

Touches de condition prises en charge

Catégorie	Touches de condition applicables	Description
Opérateurs IP	aws:SourceIp	Compare à l'adresse IP à partir de laquelle la demande a été envoyée. Peuvent être utilisées pour les opérations de compartiment ou d'objet. **Remarque :** si la requête S3 a été envoyée via le service Load Balancer sur les nœuds Admin et les passerelles, cela se compare à l'adresse IP en amont du service Load Balancer. **Remarque** : si un équilibreur de charge tiers non transparent est utilisé, il sera comparé à l'adresse IP de cet équilibreur de charge. Toutes `X-Forwarded-For` le cueilleur sera ignoré car sa validité ne peut pas être vérifiée.
Ressource/identité	aws:nom d'utilisateur	Compare le nom d'utilisateur de l'expéditeur à partir duquel la demande a été envoyée. Peuvent être utilisées pour les opérations de compartiment ou d'objet.
s3:ListBucket et s3:permissions ListBuckeVersions	s3:délimiteur	Compare avec le paramètre de délimiteur spécifié dans une demande GET Bucket ou GET Bucket Object versions.
s3:ListBucket et s3:permissions ListBuckeVersions	s3:touches max	Compare au paramètre max-keys spécifié dans une demande GET Bucket ou GET Bucket Object versions.
s3:ListBucket et s3:permissions ListBuckeVersions	s3:préfixe	Compare au paramètre de préfixe spécifié dans une demande GET Bucket ou GET Bucket Object versions.

Catégorie	Touches de condition applicables	Description
s3:PutObject	s3 :conservation des jours restants avec un verrouillage objet	Compare à la date de conservation spécifiée dans le `x-amz-object-lock-retain-until-date` demander l'en-tête ou calculé 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 demandes suivantes : • PLACER l'objet • PLACER l'objet - Copier • Lancer le téléchargement de pièces multiples
s3:PutObjectRetention	s3 :conservation des jours restants avec un verrouillage objet	Compare à la date de conservation spécifiée dans la demande DE conservation D'objet PUT pour s'assurer qu'elle se trouve dans la plage autorisée.

Spécifiez les variables d'une règle

Vous pouvez utiliser des variables dans les règles pour remplir les informations relatives aux règles lorsqu'elles sont disponibles. Vous pouvez utiliser des variables de règle dans le `Resource` comparaisons d'éléments et de chaînes dans `Condition` elément.

Dans cet exemple, la variable `${aws:username}` Fait partie de l'élément ressource :

```
"Resource": "arn:aws:s3:::bucket-name/home/${aws:username}/*"
```

Dans cet exemple, la variable `${aws:username}` fait partie de la valeur de condition dans le bloc condition :

```
"Condition": {
    "StringLike": {
      "s3:prefix": "${aws:username}/*"
        ...
},
        ...
```

Variable	Description
`${aws:SourceIp}`	Utilise la touche SourceIp comme variable fournie.

Variable	Description
`${aws:username}`	Utilise la clé de nom d'utilisateur comme variable fournie.
`${s3:prefix}`	Utilise la clé de préfixe spécifique au service comme variable fournie.
`${s3:max-keys}`	Utilise la touche max-keys spécifique au service comme variable fournie.
`${*}`	Caractère spécial. Utilise le caractère comme caractère littéral *.
`${?}`	Caractère spécial. Utilise le caractère comme littéral ? caractère.
`${$}`	Caractère spécial. Utilise le caractère comme caractère littéral $.

Créez des règles nécessitant une gestion spéciale

Parfois, une politique peut accorder des autorisations dangereuses pour la sécurité ou dangereuses pour les opérations continues, telles que le verrouillage de l'utilisateur racine du compte. L'implémentation de l'API REST StorageGRID S3 est moins restrictive lors de la validation des règles qu'Amazon, mais tout aussi stricte lors de l'évaluation des règles.

Description de la politique	Type de règle	Comportement Amazon	Comportement de StorageGRID
Refusez vous-même toutes les autorisations sur le compte racine	Godet	Valide et appliquée, mais le compte utilisateur root conserve les autorisations nécessaires pour toutes les opérations des règles de compartiment S3	Identique
Refusez vous-même les autorisations d'accès à l'utilisateur/au groupe	Groupe	Valide et appliquée	Identique
Autoriser un groupe de comptes étrangers toute autorisation	Godet	Principal non valide	Valide, mais les autorisations pour toutes les opérations de stratégie de compartiment S3 renvoient une erreur 405 méthode non autorisée lorsque cela est autorisé par une règle

Description de la politique	Type de règle	Comportement Amazon	Comportement de StorageGRID
Autoriser un utilisateur ou une racine de compte étranger à accorder toute autorisation	Godet	Valide, mais les autorisations pour toutes les opérations de stratégie de compartiment S3 renvoient une erreur 405 méthode non autorisée lorsque cela est autorisé par une règle	Identique
Autoriser tout le monde à autoriser toutes les actions	Godet	Valide, mais les autorisations pour toutes les opérations de politique de compartiment S3 renvoient une erreur 405 méthode non autorisée pour la racine du compte étranger et les utilisateurs	Identique
Refuser les autorisations de tous pour toutes les actions	Godet	Valide et appliquée, mais le compte utilisateur root conserve les autorisations nécessaires pour toutes les opérations des règles de compartiment S3	Identique
Le principal est un utilisateur ou un groupe inexistant	Godet	Principal non valide	Valide
La ressource est un compartiment S3 inexistant	Groupe	Valide	Identique
Principal est un groupe local	Godet	Principal non valide	Valide
La police accorde à un compte non propriétaire (y compris les comptes anonymes) des autorisations pour METTRE des objets	Godet	Valide. Les objets sont détenus par le compte de créateur et la stratégie de compartiment ne s'applique pas. Le compte créateur doit accorder des autorisations d'accès à l'objet à l'aide des listes de contrôle d'accès d'objet.	Valide. Les objets sont la propriété du compte du propriétaire du compartiment. La politique de compartiment s'applique.

Protection WORM (Write-once, Read-many)

Vous pouvez créer des compartiments WORM (Write-once, Read-many) pour protéger les données, les métadonnées d'objet définies par l'utilisateur et le balisage d'objets S3. Vous configurez les compartiments WORM pour permettre la création de nouveaux objets et empêcher les écrasements ou la suppression de contenu existant. Utilisez l'une des approches décrites ici.

Pour vous assurer que les écrasements sont toujours refusés, vous pouvez :

- Dans Grid Manager, allez à **CONFIGURATION système Options de grille**, puis cochez la case **empêcher modification client**.
- Appliquez les règles suivantes et les règles S3 :
  - Ajoutez une opération DE REFUS PutOverwriteObject à la règle S3.
  - Ajoutez une opération DE REFUS DeleteObject à la règle S3.
  - Ajouter une opération D'AUTORISATION PLACER l'objet à la règle S3.

> La définition de DeleteObject sur DENY dans une politique S3 n'empêche pas ILM de supprimer des objets lorsqu'une règle telle que « zéro copie après 30 jours » existe.

> Même lorsque toutes ces règles et règles sont appliquées, elles ne protègent pas contre les écritures simultanées (voir situation A). Ils protègent contre les écrasements séquentiels terminés (voir situation B).

Situation A: Écritures simultanées (non protégées contre)

```
/mybucket/important.doc
PUT#1 ---> OK
PUT#2 -------> OK
```

Situation B: Remplacements séquentiels terminés (protégés contre)

```
/mybucket/important.doc
PUT#1 -------> PUT#2 ---X (denied)
```

Informations associées

Gestion des objets avec ILM

Créez des règles nécessitant une gestion spéciale

Gestion des objets par les règles StorageGRID ILM

Exemples de règles de groupe S3

Exemples de règles S3

Utilisez les exemples de cette section pour créer des règles d'accès StorageGRID pour les compartiments et les groupes.

Exemples de règles de compartiment S3

Les politiques de compartiment spécifient les autorisations d'accès pour le compartiment à lequel la politique est attachée. Les règles de compartiment sont configurées à l'aide de l'API S3 PutBuckPolicy.

Il est possible de configurer une politique de compartiment à l'aide de l'interface de ligne de commandes AWS, comme indiqué dans la commande suivante :

```
> aws s3api put-bucket-policy --bucket examplebucket --policy
file://policy.json
```

Exemple : autoriser tout le monde à accéder en lecture seule à un compartiment

Dans cet exemple, tout le monde, y compris anonyme, est autorisé à lister les objets dans le compartiment et à effectuer des opérations get Object sur tous les objets du compartiment. Toutes les autres opérations seront refusées. Notez que cette politique n'est peut-être pas particulièrement utile, car personne, à l'exception de la racine du compte, ne dispose d'autorisations pour écrire dans le compartiment.

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadOnlyAccess",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:GetObject", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket","arn:aws:s3:::examplebucket/*"]
    }
  ]
}
```

Exemple : autoriser l'accès complet de tous les utilisateurs d'un compte et permettre à chacun d'un autre compte d'accéder en lecture seule à un compartiment

Dans cet exemple, tout le monde d'un compte spécifié peut accéder intégralement à un compartiment, tandis que les utilisateurs d'un autre compte spécifié ne sont autorisés qu'à répertorier le compartiment et effectuer des opérations GetObject sur les objets du compartiment en commençant par le `shared/` préfixe de clé d'objet.

> Dans StorageGRID, les objets créés par un compte autre que le propriétaire (y compris les comptes anonymes) sont détenus par le compte du propriétaire du compartiment. La politique de compartiment s'applique à ces objets.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "95390887230002558202"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::examplebucket/shared/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::examplebucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "shared/*"
        }
      }
    }
  ]
}
```

Exemple : autoriser tout le monde à accéder en lecture seule à un compartiment et à accéder entièrement au groupe spécifié

Dans cet exemple, tout le monde, y compris anonyme, est autorisé à répertorier le compartiment et à effectuer des opérations GET Object sur tous les objets du compartiment, tandis que seuls les utilisateurs appartenant au groupe `Marketing` le compte spécifié est autorisé à accéder pleinement.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/Marketing"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": ["s3:ListBucket","s3:GetObject"],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}
```

Exemple : autoriser tout le monde à lire et à écrire l'accès à un compartiment si le client se trouve dans la plage IP

Dans cet exemple, tout le monde, y compris anonyme, est autorisé à répertorier le compartiment et à effectuer toutes les opérations objet sur tous les objets du compartiment, à condition que les demandes proviennent d'une plage IP spécifiée (54.240.143.0 à 54.240.143.255, sauf 54.240.143.188). Toutes les autres opérations seront refusées et toutes les demandes en dehors de la plage IP seront refusées.

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadWriteAccessIfInSourceIpRange",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:*Object", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket","arn:aws:s3:::examplebucket/*"],
      "Condition": {
        "IpAddress": {"aws:SourceIp": "54.240.143.0/24"},
        "NotIpAddress": {"aws:SourceIp": "54.240.143.188"}
      }
    }
  ]
}
```

Exemple : autoriser un accès complet à un compartiment exclusivement par un utilisateur fédéré spécifié

Dans cet exemple, l'utilisateur fédéré Alex est autorisé à accéder pleinement au `examplebucket` le godet et ses objets. Tous les autres utilisateurs, y compris « root », sont explicitement refusés à toutes les opérations. Notez toutefois que « root » n'est jamais refusé les autorisations de mettre/obtenir/DeleteBuckePolicy.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Deny",
      "NotPrincipal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}
```

Exemple : autorisation PutOverwriteObject

Dans cet exemple, le `Deny` Effet pour PutOverwriteObject et DeleteObject garantit que personne ne peut écraser ou supprimer les données de l'objet, les métadonnées définies par l'utilisateur et le balisage d'objets S3.

```
{
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "s3:PutOverwriteObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion"
      ],
      "Resource": "arn:aws:s3:::wormbucket/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"

},
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::wormbucket"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"

},
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::wormbucket/*"
    }
  ]
}
```

Informations associées

Opérations sur les compartiments

Exemples de règles de groupe S3

Les stratégies de groupe spécifient les autorisations d'accès pour le groupe auquel la stratégie est associée. Il n'y a pas de `Principal` élément de la politique car il est implicite. Les règles de groupe sont configurées à l'aide du Gestionnaire de locataires ou de l'API.

Exemple : définissez la stratégie de groupe à l'aide du Gestionnaire de locataires

Lorsque vous utilisez le Gestionnaire de locataires pour ajouter ou modifier un groupe, vous pouvez sélectionner la manière dont vous souhaitez créer la stratégie de groupe qui définit les autorisations d'accès S3 dont les membres de ce groupe auront, comme suit :

- **Pas d'accès S3** : option par défaut. Les utilisateurs de ce groupe n'ont pas accès aux ressources S3, sauf si l'accès est accordé avec une règle de compartiment. Si vous sélectionnez cette option, seul l'utilisateur root peut accéder aux ressources S3 par défaut.
- **Accès en lecture seule** : les utilisateurs de ce groupe ont accès en lecture seule aux ressources S3. Par exemple, les utilisateurs de ce groupe peuvent afficher la liste des objets et lire les données d'objet, les métadonnées et les balises. Lorsque vous sélectionnez cette option, la chaîne JSON pour une stratégie de groupe en lecture seule s'affiche dans la zone de texte. Vous ne pouvez pas modifier cette chaîne.
- **Accès complet** : les utilisateurs de ce groupe ont accès aux ressources S3, y compris aux compartiments. Lorsque vous sélectionnez cette option, la chaîne JSON pour une stratégie de groupe à accès complet s'affiche dans la zone de texte. Vous ne pouvez pas modifier cette chaîne.
- **Custom** : les utilisateurs du groupe disposent des autorisations que vous spécifiez dans la zone de texte.

  Dans cet exemple, les membres du groupe ne sont autorisés qu'à répertorier et accéder à leur dossier spécifique (préfixe de clé) dans le compartiment spécifié.

Exemple : autoriser l'accès complet du groupe à toutes les rubriques

Dans cet exemple, tous les membres du groupe sont autorisés à accéder à tous les compartiments appartenant au compte du locataire, sauf s'ils sont explicitement refusés par la politique de compartiment.

```
{
  "Statement": [
    {
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

Exemple : autoriser l'accès en lecture seule du groupe à tous les compartiments

Dans cet exemple, tous les membres du groupe ont un accès en lecture seule aux ressources S3, à moins qu'ils ne soient explicitement refusés par la règle de compartiment. Par exemple, les utilisateurs de ce groupe peuvent afficher la liste des objets et lire les données d'objet, les métadonnées et les balises.

```
{
  "Statement": [
    {
      "Sid": "AllowGroupReadOnlyAccess",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

Exemple : permettre aux membres du groupe d'accéder pleinement à leur « dossier » uniquement dans un compartiment

Dans cet exemple, les membres du groupe ne sont autorisés qu'à répertorier et accéder à leur dossier spécifique (préfixe de clé) dans le compartiment spécifié. Notez que les autorisations d'accès à partir d'autres stratégies de groupes et de la règle de compartiment doivent être prises en compte lors de la détermination de la confidentialité de ces dossiers.

```
{
  "Statement": [
    {
      "Sid": "AllowListBucketOfASpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::department-bucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "${aws:username}/*"
        }
      }
    },
    {
      "Sid": "AllowUserSpecificActionsOnlyInTheSpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:*Object",
      "Resource": "arn:aws:s3:::department-bucket/${aws:username}/*"
    }
  ]
}
```

Informations associées

Utilisez le compte du locataire

Configuration de la sécurité pour l'API REST

Il est recommandé de passer en revue les mesures de sécurité mises en œuvre pour l'API REST et de comprendre comment sécuriser votre système.

Comment StorageGRID assure la sécurité des API REST

Vous devez comprendre comment le système StorageGRID implémente la sécurité, l'authentification et l'autorisation pour l'API REST.

StorageGRID utilise les mesures de sécurité suivantes.

- Les communications client avec le service Load Balancer utilisent HTTPS si HTTPS est configuré pour le noeud final Load Balancer.

  Lorsque vous configurez un point final d'équilibreur de charge, HTTP peut éventuellement être activé. Par exemple, vous pouvez utiliser HTTP à des fins de test ou autres que la production. Pour plus d'informations, reportez-vous aux instructions d'administration de StorageGRID.

- Par défaut, StorageGRID utilise HTTPS pour les communications client avec les nœuds de stockage et le service CLB sur les nœuds de passerelle.

  HTTP peut éventuellement être activé pour ces connexions. Par exemple, vous pouvez utiliser HTTP à des

fins de test ou autres que la production. Pour plus d'informations, reportez-vous aux instructions d'administration de StorageGRID.

Le service CLB est obsolète.

- Les communications entre StorageGRID et le client sont chiffrées à l'aide de TLS.
- Les communications entre le service Load Balancer et les nœuds de stockage dans la grille sont cryptées que le terminal de l'équilibreur de charge soit configuré pour accepter les connexions HTTP ou HTTPS.
- Les clients doivent fournir des en-têtes d'authentification HTTP à StorageGRID pour effectuer des opérations d'API REST.

Certificats de sécurité et applications client

Les clients peuvent se connecter au service Load Balancer sur les nœuds de passerelle ou les nœuds d'administration, directement aux nœuds de stockage ou au service CLB sur les nœuds de passerelle.

Dans tous les cas, les applications client peuvent établir des connexions TLS à l'aide d'un certificat de serveur personnalisé chargé par l'administrateur de la grille ou d'un certificat généré par le système StorageGRID :

- Lorsque les applications client se connectent au service Load Balancer, elles le font à l'aide du certificat configuré pour le noeud final de l'équilibreur de charge spécifique utilisé pour établir la connexion. Chaque noeud final possède son propre certificat, qui est soit un certificat de serveur personnalisé chargé par l'administrateur de la grille, soit un certificat que l'administrateur de la grille a généré dans StorageGRID lors de la configuration du noeud final.
- Lorsque les applications client se connectent directement à un nœud de stockage ou au service CLB des nœuds de passerelle, elles utilisent soit les certificats de serveur générés par le système pour les nœuds de stockage lorsque le système StorageGRID a été installé (qui sont signés par l'autorité de certification du système), ou un seul certificat de serveur personnalisé fourni par un administrateur de grid pour la grille.

Les clients doivent être configurés pour approuver l'autorité de certification qui a signé le certificat qu'ils utilisent pour établir des connexions TLS.

Pour plus d'informations sur la configuration des noeuds finaux de l'équilibreur de charge et pour obtenir des instructions sur l'ajout d'un certificat de serveur personnalisé pour les connexions TLS directement aux noeuds de stockage ou au service CLB sur les noeuds de passerelle, reportez-vous aux instructions de la section Administration de StorageGRID.

Récapitulatif

Le tableau suivant montre comment les problèmes de sécurité sont implémentés dans les API REST S3 et Swift :

Problème de sécurité	Implémentation pour l'API REST
Sécurité de la connexion	TLS
Authentification du serveur	Certificat de serveur X.509 signé par l'autorité de certification du système ou certificat de serveur personnalisé fourni par l'administrateur

Problème de sécurité	Implémentation pour l'API REST
Authentification client	• S3 : compte S3 (ID de clé d'accès et clé d'accès secrète) • SWIFT : compte Swift (nom d'utilisateur et mot de passe)
Autorisation du client	• S3 : propriété des compartiments et toutes les règles de contrôle d'accès applicables • SWIFT : accès aux rôles d'administrateur

Informations associées

Administrer StorageGRID

Algorithmes de hachage et de cryptage pris en charge pour les bibliothèques TLS

Le système StorageGRID prend en charge un ensemble limité de suites de chiffrement que les applications clientes peuvent utiliser lors de l'établissement d'une session TLS (transport Layer Security).

Versions supportées de TLS

StorageGRID supporte TLS 1.2 et TLS 1.3.

SSLv3 et TLS 1.1 (ou versions antérieures) ne sont plus pris en charge.

Suites de chiffrement prises en charge

Version TLS	Nom IANA de la suite de chiffrement
1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
1.2	TLS_ECDHE_RSA_WITH_CHA20_POLY1305_SHA256
1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
1.3	TLS_AES_256_GCM_SHA384
1.3	TLS_CHA20_POLY1305_SHA256
1.3	TLS_AES_128_GCM_SHA256

Suites de chiffrement obsolètes

Les suites de chiffrement suivantes sont obsolètes. La prise en charge de ces chiffrements sera supprimée dans une prochaine version.

Nom IANA
TLS_RSA_WAS_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384

Informations associées

Configuration des connexions client

Surveiller et auditer les opérations

Vous pouvez surveiller les charges de travail et l'efficacité des opérations client en visualisant les tendances de transaction pour l'ensemble du grid ou pour des nœuds spécifiques. Vous pouvez utiliser des messages d'audit pour surveiller les opérations et les transactions des clients.

Contrôler les taux d'entrée et de récupération des objets

Vous pouvez surveiller les taux d'entrée et de récupération des objets, ainsi que les mesures relatives au nombre d'objets, aux requêtes et à la vérification. Vous pouvez afficher le nombre de tentatives de lecture, d'écriture et de modification d'objets du système StorageGRID ayant échoué et réussies par les applications client.

Étapes

1. Connectez-vous au Grid Manager à l'aide d'un navigateur web pris en charge.
2. Dans le tableau de bord, recherchez la section opérations de protocole.

   Cette section récapitule le nombre d'opérations client effectuées par votre système StorageGRID. La moyenne des débits de protocole est calculée au cours des deux dernières minutes.

3. Sélectionnez **NOEUDS**.
4. Dans la page d'accueil noeuds (niveau de déploiement), cliquez sur l'onglet **Load Balancer**.

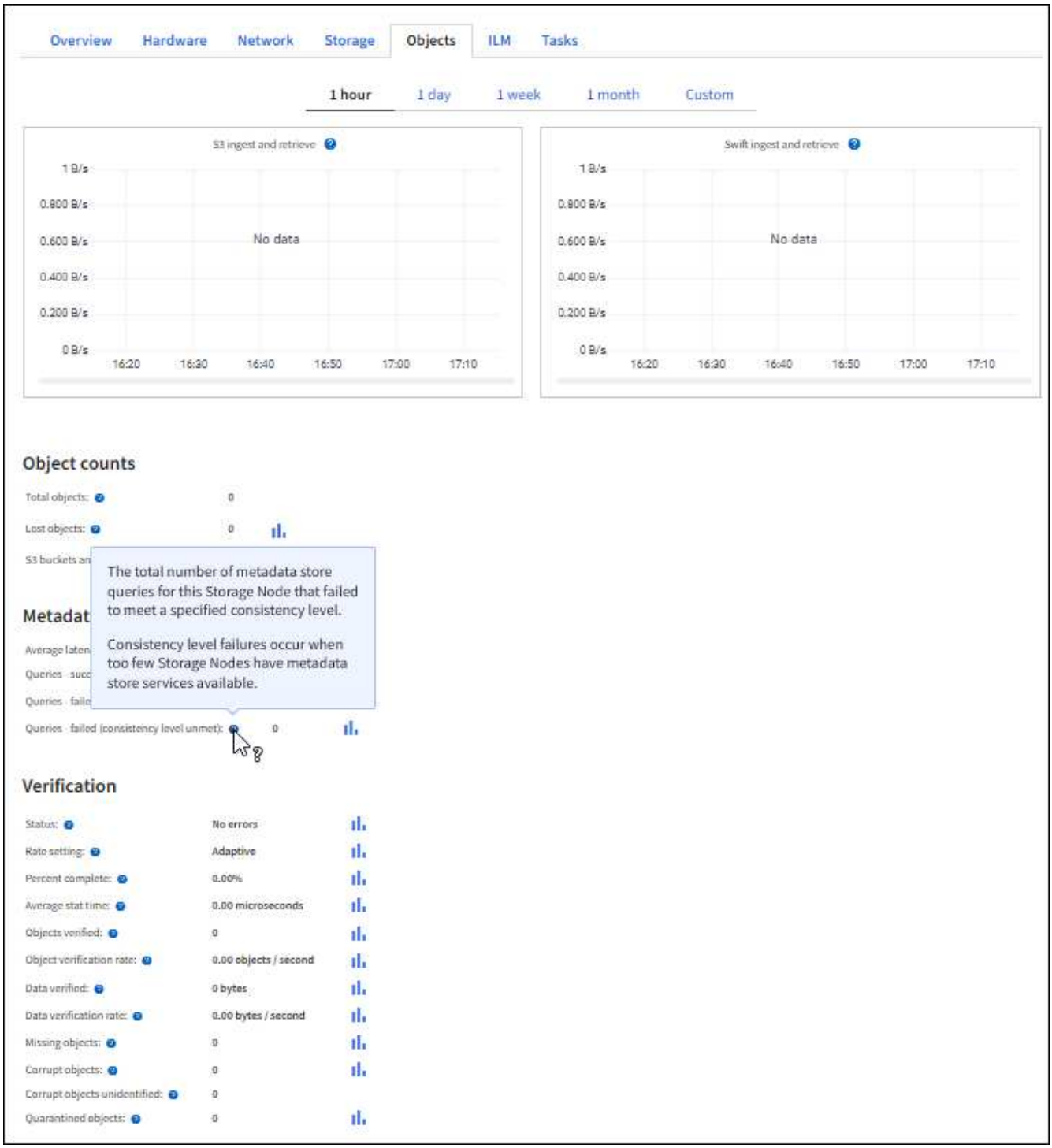
   Les graphiques présentent les tendances de tout le trafic client dirigé vers les terminaux d'équilibreur de charge dans la grille. Vous pouvez sélectionner un intervalle de temps en heures, jours, semaines, mois ou années, vous pouvez également appliquer un intervalle personnalisé.

5. Dans la page d'accueil noeuds (niveau de déploiement), cliquez sur l'onglet **objets**.

   Le graphique montre les taux d'entrée et de récupération de l'intégralité de votre système StorageGRID en octets par seconde et en octets totaux. Vous pouvez sélectionner un intervalle de temps en heures, jours, semaines, mois ou années, vous pouvez également appliquer un intervalle personnalisé.

6. Pour afficher les informations relatives à un noeud de stockage particulier, sélectionnez-le dans la liste de gauche, puis cliquez sur l'onglet **objets**.

   Le tableau affiche les taux d'entrée et de récupération de l'objet pour ce nœud de stockage. L'onglet inclut également des mesures pour le nombre d'objets, les requêtes et la vérification. Vous pouvez cliquer sur les étiquettes pour afficher les définitions de ces mesures.



7. Si vous voulez encore plus de détails :
   a. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
   b. Sélectionnez ***site* Présentation main**.

      La section opérations d'API affiche un récapitulatif des informations sur l'ensemble de la grille.

   c. Sélectionnez ***Storage Node* LDR *client application* Présentation main**

      La section opérations affiche un récapitulatif des informations sur le nœud de stockage sélectionné.

Examiner les journaux d'audit

Les messages d'audit sont générés par les services StorageGRID et stockés dans des fichiers journaux texte. Des messages d'audit spécifiques aux API dans les journaux d'audit fournissent des données stratégiques de sécurité, d'exploitation et de surveillance des performances qui vous aideront à évaluer l'état de votre système.

Ce dont vous avez besoin

- Vous disposez d'autorisations d'accès spécifiques.
- Vous avez le `Passwords.txt` fichier.
- Vous connaissez l'adresse IP d'un nœud d'administration.

Description de la tâche

Le fichier journal d'audit actif est nommé `audit.log`, Et il est stocké sur des nœuds d'administration.

Une fois par jour, le fichier audit.log actif est enregistré, et un nouveau `audit.log` le fichier est démarré. Le nom du fichier enregistré indique quand il a été enregistré, au format *`yyyy-mm-dd.txt`*.

Après un jour, le fichier enregistré est compressé et renommé, au format *`yyyy-mm-dd.txt.gz`*, qui conserve la date originale.

Cet exemple montre l'actif `audit.log` fichier du jour précédent (`2018-04-15.txt`), et le fichier compressé pour la veille (`2018-04-14.txt.gz`).

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

Étapes

1. Connectez-vous à un nœud d'administration :
   a. Saisissez la commande suivante : `ssh admin@primary_Admin_Node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
2. Accédez au répertoire contenant les fichiers journaux d'audit :

   ```
   cd /var/local/audit/export
   ```

3. Afficher le fichier journal d'audit actuel ou enregistré, selon les besoins.

Opérations S3 suivies dans les journaux d'audit

Plusieurs opérations de compartiment et les opérations d'objets sont suivies dans les journaux d'audit de StorageGRID.

Les opérations des compartiments sont suivies dans les journaux d'audit

- SUPPRIMER le compartiment
- SUPPRIMER le balisage du compartiment
- SUPPRIMER plusieurs objets
- OBTENIR le compartiment (liste d'objets)
- OBTENIR les versions d'objet de compartiment
- GET Bucket tagging
- Godet DE TÊTE
- PLACER le godet
- METTEZ le godet en conformité
- PUT Bucket tagging
- GESTION des versions du compartiment

Opérations d'objet suivies dans les journaux d'audit

- Chargement de pièces multiples complet
- Télécharger une pièce (lorsque la règle ILM utilise des comportements d'entrée stricts ou équilibrés)
- Télécharger une pièce : copie (lorsque la règle ILM utilise des comportements d'entrée stricts ou équilibrés)
- SUPPRIMER l'objet
- OBTENIR l'objet
- Objet TÊTE
- Restauration POST-objet
- PLACER l'objet
- PLACER l'objet - Copier

Informations associées

Opérations sur les compartiments

Opérations sur les objets

Avantages des connexions HTTP actives, inactives et simultanées

La configuration des connexions HTTP peut avoir un impact sur les performances du système StorageGRID. Les configurations varient selon que la connexion HTTP est active ou inactive ou si vous avez simultanément plusieurs connexions.

Vous pouvez identifier les avantages en termes de performances pour les types de connexions HTTP suivants :

- Connexions HTTP inactives
- Connexions HTTP actives

- Connexions HTTP simultanées

Avantages de maintenir les connexions HTTP inactives ouvertes

Vous devez maintenir les connexions HTTP ouvertes même lorsque les applications client sont inactives pour permettre aux applications client d'effectuer les transactions suivantes sur la connexion ouverte. En fonction des mesures du système et de l'expérience d'intégration, vous devez garder une connexion HTTP inactive ouverte pendant 10 minutes maximum. StorageGRID peut fermer automatiquement une connexion HTTP qui reste ouverte et inactive pendant plus de 10 minutes.

Les connexions HTTP ouvertes et inactives offrent les avantages suivants :

- Réduction de la latence entre le moment où le système StorageGRID détermine qu'il doit effectuer une transaction HTTP et le moment où le système StorageGRID peut effectuer la transaction

  La réduction de la latence constitue l'avantage principal, notamment pour la durée nécessaire à l'établissement des connexions TCP/IP et TLS.

- Augmentation de la vitesse de transfert des données en amorçant l'algorithme TCP/IP à démarrage lent avec des transferts effectués précédemment
- Notification instantanée de plusieurs classes de conditions de défaillance qui interrompent la connectivité entre l'application cliente et le système StorageGRID

Déterminer la durée d'ouverture d'une connexion inactive est un compromis entre les avantages du démarrage lent associés à la connexion existante et l'affectation idéale de la connexion aux ressources système internes.

Avantages des connexions HTTP actives

Pour les connexions directement aux nœuds de stockage ou au service CLB (obsolète) sur les nœuds de passerelle, vous devez limiter la durée d'une connexion HTTP active à un maximum de 10 minutes, même si la connexion HTTP effectue en continu des transactions.

La détermination de la durée maximale pendant laquelle une connexion doit être maintenue ouverte est un compromis entre les avantages de la persistance de connexion et l'allocation idéale de la connexion aux ressources système internes.

Pour les connexions client aux nœuds de stockage ou au service CLB, la limitation des connexions HTTP actives offre les avantages suivants :

- Équilibrage optimal de la charge sur l'ensemble du système StorageGRID.

  Lors de l'utilisation du service CLB, vous devez empêcher les connexions TCP/IP de longue durée afin d'optimiser l'équilibrage de la charge sur le système StorageGRID. Vous devez configurer les applications client pour suivre la durée de chaque connexion HTTP et fermer la connexion HTTP après un délai défini afin que la connexion HTTP puisse être rétablie et rééquilibrée.

  Le service CLB équilibre la charge dans le système StorageGRID au moment où une application client établit une connexion HTTP. Avec le temps, une connexion HTTP pourrait ne plus être optimale au fur et à mesure que les besoins en équilibrage de la charge évoluent. Le système réalise son meilleur équilibrage de charge lorsque les applications client établissent une connexion HTTP distincte pour chaque

transaction, mais cela annule les gains les plus importants associés aux connexions persistantes.

Le service CLB est obsolète.

- Permet aux applications clientes de diriger des transactions HTTP vers des services LDR qui ont de l'espace disponible.
- Permet de démarrer les procédures de maintenance.

  Certaines procédures de maintenance ne démarrent qu'une fois toutes les connexions HTTP en cours terminées.

Pour les connexions client au service Load Balancer, limiter la durée des connexions ouvertes peut être utile pour permettre le démarrage rapide de certaines procédures de maintenance. Si la durée des connexions client n'est pas limitée, l'arrêt automatique des connexions actives peut prendre plusieurs minutes.

Avantages des connexions HTTP simultanées

Vous devez maintenir plusieurs connexions TCP/IP ouvertes au système StorageGRID pour permettre le parallélisme, ce qui augmente les performances. Le nombre optimal de connexions parallèles dépend de divers facteurs.

Les connexions HTTP simultanées offrent les avantages suivants :

- Latence réduite

  Les transactions peuvent commencer immédiatement au lieu d'attendre que d'autres transactions soient effectuées.

- Rendement accru

  Le système StorageGRID peut effectuer des transactions parallèles et augmenter le débit des transactions globales.

Les applications client doivent établir plusieurs connexions HTTP. Lorsqu'une application client doit effectuer une transaction, elle peut sélectionner et utiliser immédiatement toute connexion établie qui ne traite pas actuellement une transaction.

Le débit maximal de chaque topologie de chaque système StorageGRID est différent pour les transactions et les connexions simultanées, avant que les performances ne commencent à se dégrader. Le pic de débit dépend de facteurs tels que les ressources informatiques, les ressources réseau, les ressources de stockage et les liaisons WAN. Des facteurs sont également pris en charge par le nombre de serveurs et de services, ainsi que par le nombre d'applications prises en charge par le système StorageGRID.

Les systèmes StorageGRID prennent souvent en charge plusieurs applications client. Vous devez garder cela à l'esprit lorsque vous déterminez le nombre maximal de connexions simultanées utilisées par une application client. Si l'application client se compose de plusieurs entités logicielles qui établissent chacune des connexions avec le système StorageGRID, vous devez ajouter toutes les connexions entre les entités. Vous devrez peut-être régler le nombre maximal de connexions simultanées dans les situations suivantes :

- La topologie du système StorageGRID affecte le nombre maximal de transactions et de connexions simultanées pris en charge par le système.
- Les applications client qui interagissent avec le système StorageGRID sur un réseau avec une bande

passante limitée peuvent être contraintes de réduire le niveau de simultanéité pour s'assurer que les transactions individuelles sont effectuées dans un délai raisonnable.

- Lorsque de nombreuses applications client partagent le système StorageGRID, il peut être nécessaire de réduire le degré de simultanéité pour ne pas dépasser les limites du système.

Séparation des pools de connexions HTTP pour les opérations de lecture et d'écriture

Vous pouvez utiliser des pools séparés de connexions HTTP pour les opérations en lecture et écriture, et contrôler la proportion que vous souhaitez utiliser pour chacun d'eux. Le recours à des pools séparés de connexions HTTP vous permet de contrôler les transactions et d'équilibrer la charge plus efficacement.

Les applications client peuvent créer des chargements qui sont dominants par la récupération (lecture) ou dominants par le stockage (écriture). Grâce à des pools séparés de connexions HTTP pour les transactions en lecture et écriture, vous pouvez ajuster la quantité de chaque pool à dédier pour les transactions en lecture ou en écriture.