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

StorageGRID 11.5

NetApp
April 11, 2024

Sommaire

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

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

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

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

Traitement de la date

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

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

En-têtes de demande commune

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

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

En-têtes de réponse commune

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

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

Informations associées

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

Authentification des demandes

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

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

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

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

Utilisation de l'en-tête autorisation HTTP

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

Utilisation des paramètres de requête

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

Opérations sur le service

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

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

Informations associées

"DEMANDE d'utilisation du stockage"

Opérations sur les compartiments

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

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

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

"Noms de domaine de terminaux pour la requête S3"

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

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

compartiments individuels.

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

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

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

Fonctionnement	Mise en place
Godet DE TÊTE	Cette opération détermine si un compartiment existe et que vous êtes autorisé à y accéder.

Fonctionnement	Mise en place

PLACER le godet	Cette opération crée un nouveau godet. C'est en créant le compartiment que vous devenez le propriétaire.
	
	• Les noms de compartiment doivent être conformes aux règles suivantes :
	  ◦ Il doit être unique sur chaque système StorageGRID (et pas seulement au sein du compte du locataire).
	  ◦ Doit être conforme DNS.
	  ◦ Doit contenir au moins 3 caractères et pas plus de 63 caractères.
	  ◦ Peut être une série d'une ou plusieurs étiquettes, avec des étiquettes adjacentes séparées par un point. Chaque étiquette doit commencer et se terminer par une lettre ou un chiffre en minuscules et ne peut utiliser que des lettres minuscules, des chiffres et des tirets.
	  ◦ Ne doit pas ressembler à une adresse IP au format texte.
	  ◦ Ne doit pas utiliser de périodes dans des demandes de type hébergement virtuel. Les périodes provoquera des problèmes avec la vérification du certificat générique du serveur.
	• Par défaut, les compartiments sont créés dans le `us-east-1` région ; cependant, vous pouvez utiliser le `LocationConstraint` elément de demande dans le corps de la demande pour spécifier une région différente. Lorsque vous utilisez le `LocationConstraint` Elément, vous devez spécifier le nom exact d'une région qui a été définie à l'aide du gestionnaire de grille ou de l'API de gestion de grille. Contactez votre administrateur système si vous ne connaissez pas le nom de région que vous devez utiliser. **Remarque** : une erreur se produit si votre demande PUT Bucket utilise une région qui n'a pas été définie dans StorageGRID.
	• Vous pouvez inclure le `x-amz-bucket-object-lock-enabled` Demander l'en-tête pour créer un compartiment avec le verrouillage objet S3 activé.
	
	Vous devez activer le verrouillage d'objet S3 lors de la création du compartiment. Vous ne pouvez pas ajouter ou désactiver le verrouillage d'objet S3 après la création d'un compartiment. Le verrouillage objet S3 requiert la gestion des versions de compartiment, qui est activée automatiquement lors de la création du compartiment.

Fonctionnement	Mise en place
PLACEZ les godets	Cette opération définit la configuration du CORS pour un compartiment afin que le compartiment puisse traiter les demandes d'origine croisée. Le partage de ressources d'origine croisée (CORS) est un mécanisme de sécurité qui permet aux applications Web clientes d'un domaine d'accéder aux ressources d'un domaine différent. Supposons par exemple que vous utilisez un compartiment S3 nommé `images` pour stocker des graphiques. En définissant la configuration CORS pour le `images` le champ permet d'afficher les images de ce compartiment sur le site web `http://www.example.com`.
PUT Bucket Encryption	Cette opération définit l'état de cryptage par défaut d'un compartiment existant. Lorsque le chiffrement au niveau du compartiment est activé, tout nouvel objet ajouté au compartiment est chiffré.StorageGRID prend en charge le chiffrement côté serveur avec des clés gérées par StorageGRID. Lorsque vous spécifiez la règle de configuration de cryptage côté serveur, définissez l' `SSEAlgorithm` paramètre à `AES256`, et n'utilisez pas le `KMSMasterKeyID` paramètre. La configuration de cryptage par défaut du compartiment est ignorée si la demande de téléchargement d'objet spécifie déjà le cryptage (c'est-à-dire, si la demande inclut le `x-amz-server-side-encryption-*` en-tête de demande).

Fonctionnement	Mise en place
CYCLE de vie des compartiments	Cette opération crée une nouvelle configuration de cycle de vie pour le compartiment ou remplace une configuration de cycle de vie existante. StorageGRID prend en charge jusqu'à 1,000 règles de cycle de vie dans une configuration cycle de vie. Chaque règle peut inclure les éléments XML suivants : • Expiration (jours, date) • NonactuelVersionExp (Nontactut Days) • Filtre (préfixe, étiquette) • État • ID StorageGRID ne prend pas en charge les actions suivantes : • AbortIncompleMultipartUpload • ExpiredObjectDeleteMarker • Transition Pour comprendre comment l'action expiration dans un cycle de vie de compartiment interagit avec les instructions de placement ILM, reportez-vous à la section « fonctionnement de l'ILM tout au long de la vie d'un objet » dans les instructions de gestion des objets avec la gestion du cycle de vie des informations. **Remarque** : la configuration du cycle de vie des compartiments peut être utilisée avec des compartiments avec le verrouillage d'objet S3 activé, mais la configuration du cycle de vie des compartiments n'est pas prise en charge pour les compartiments conformes hérités.

Fonctionnement	Mise en place

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

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

Fonctionnement	Mise en place

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

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

Informations associées

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

"Contrôles de cohérence"

"DEMANDE DE dernier accès au compartiment"

"Règles d'accès au compartiment et au groupe"

"Utilisation du verrouillage d'objet S3"

"Opérations S3 suivies dans les journaux d'audit"

"Gestion des objets avec ILM"

"Utilisez un compte de locataire"

Création d'une configuration de cycle de vie S3

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

du système StorageGRID.

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

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

Qu'est-ce qu'une configuration de cycle de vie

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

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

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

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

Par conséquent, il est possible de supprimer un objet de la grille, même si les instructions de placement d'une règle ILM s'appliquent toujours à l'objet. Il est également possible de conserver un objet dans la grille même après l'expiration des instructions de placement ILM de l'objet. Pour plus de détails, consultez la section « fonctionnement de ILM tout au long de la vie d'un objet » dans les instructions de gestion des objets avec la gestion du cycle de vie de l'information.

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

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

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

Création de la configuration du cycle de vie

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

1. La règle 1 s'applique uniquement aux objets qui correspondent au préfixe `category1/` et qui ont un `key2` valeur de `tag2`. Le `Expiration` Le paramètre spécifie que les objets correspondant au filtre expireront à minuit le 22 août 2020.
2. La règle 2 s'applique uniquement aux objets qui correspondent au préfixe `category2/`. Le `Expiration` le paramètre indique que les objets correspondant au filtre expirent 100 jours après leur ingestion.

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

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

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

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

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

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

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

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

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

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

La validation de l'expiration du cycle de vie du compartiment s'applique à un objet

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

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

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

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

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

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

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

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

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

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

Informations associées

"Opérations sur les compartiments"

"Gestion des objets avec ILM"

Opérations personnalisées dans les compartiments

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

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

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

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

Informations associées

"Opérations S3 suivies dans les journaux d'audit"

Opérations sur les objets

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

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

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

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

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

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

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

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

Informations associées

"Contrôles de cohérence"

"Opérations S3 suivies dans les journaux d'audit"

Utilisation du verrouillage d'objet S3

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

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

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

Activation du verrouillage objet S3 pour un compartiment

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

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

  "Utilisez un compte de locataire"

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

  "Opérations sur les compartiments"

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

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

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

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

"Opérations sur les compartiments"

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

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

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

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

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

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

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

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

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

Mise à jour des paramètres de verrouillage d'objet S3

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

- `PUT Object legal-hold`

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

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

Informations associées

"Gestion des objets avec ILM"

"Utilisez un compte de locataire"

"PLACER l'objet"

"PLACER l'objet - Copier"

"Lancer le téléchargement de pièces multiples"

"Gestion des versions d'objet"

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

À l'aide du chiffrement côté serveur

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

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

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

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

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

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

Utilisation du SSE

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

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

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

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

Utilisation du SSE-C

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

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

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

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

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

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

- Vous devez utiliser https.

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

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

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

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

Informations associées

"OBTENIR l'objet"

"Objet TÊTE"

"PLACER l'objet"

"PLACER l'objet - Copier"

"Lancer le téléchargement de pièces multiples"

"Télécharger la pièce"

"Télécharger la pièce - Copier"

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

OBTENIR l'objet

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

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

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

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

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

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

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

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

Caractères UTF-8 dans les métadonnées utilisateur

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

En-tête de demande non pris en charge

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

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

Gestion des versions

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

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

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

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

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

Objets partitionnés ou segmentés dans un pool de stockage cloud

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

Dans ces cas :

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

Informations associées

"À l'aide du chiffrement côté serveur"

"Gestion des objets avec ILM"

"Restauration POST-objet"

"Opérations S3 suivies dans les journaux d'audit"

Objet TÊTE

Vous pouvez utiliser la requête d'objet TÊTE S3 pour extraire les métadonnées à partir

d'un objet sans y retourner. Si l'objet est stocké dans un pool de stockage cloud, vous pouvez utiliser HEAD Object pour déterminer l'état de transition de l'objet.

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

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

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

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

Caractères UTF-8 dans les métadonnées utilisateur

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

En-tête de demande non pris en charge

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

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

En-têtes de réponse pour les objets Cloud Storage Pool

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

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

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

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

État de l'objet	Réponse à l'objet TÊTE

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

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

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

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

État de l'objet	Réponse à l'objet TÊTE

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

Objets partitionnés ou segmentés dans un pool de stockage cloud

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

Gestion des versions

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

Informations associées

"À l'aide du chiffrement côté serveur"

"Gestion des objets avec ILM"

"Restauration POST-objet"

"Opérations S3 suivies dans les journaux d'audit"

Restauration POST-objet

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

Type de demande pris en charge

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

Gestion des versions

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

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

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

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

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

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

Informations associées

"Gestion des objets avec ILM"

"Objet TÊTE"

"Opérations S3 suivies dans les journaux d'audit"

PLACER l'objet

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

Résolution des conflits

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

Taille de l'objet

StorageGRID prend en charge les objets pouvant atteindre 5 To.

Taille des métadonnées utilisateur

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

Caractères UTF-8 dans les métadonnées utilisateur

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

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

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

valeur de la clé comprend des caractères non imprimables.

Limites des balises d'objet

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

Propriété de l'objet

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

En-têtes de demande pris en charge

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

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

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

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

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

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

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

  ```
  x-amz-meta-<em>name</em>: <em>value</em>
  ```

  Si vous souhaitez utiliser l'option **heure de création définie par l'utilisateur** comme heure de référence

pour une règle ILM, vous devez utiliser `creation-time` nom des métadonnées enregistrées lors de la création de l'objet. Par exemple :

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

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

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

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

"Utilisation du verrouillage d'objet S3"

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

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

En-têtes de requête non pris en charge

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

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

Options de classe de stockage

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

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

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

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

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

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

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

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

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

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

Demander des en-têtes pour le cryptage côté serveur

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

- **SSE**: Utilisez l'en-tête suivant si vous voulez chiffrer l'objet avec une clé unique gérée par StorageGRID.

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

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

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

Gestion des versions

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

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

Informations associées

"Gestion des objets avec ILM"

"Opérations sur les compartiments"

"Opérations S3 suivies dans les journaux d'audit"

"À l'aide du chiffrement côté serveur"

"Configuration des connexions client"

PLACER l'objet - Copier

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

Résolution des conflits

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

Taille de l’objet

StorageGRID prend en charge les objets pouvant atteindre 5 To.

Caractères UTF-8 dans les métadonnées utilisateur

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

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

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

En-têtes de demande pris en charge

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

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

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

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

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

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

"Utilisation du verrouillage d'objet S3"

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

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

En-têtes de requête non pris en charge

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

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

Options de classe de stockage

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

- `STANDARD`

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

- `REDUCED_REDUNDANCY`

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

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

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

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

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

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

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

Demander des en-têtes pour le cryptage côté serveur

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

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

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

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

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

Gestion des versions

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

Informations associées

"Gestion des objets avec ILM"

"À l'aide du chiffrement côté serveur"

"Opérations S3 suivies dans les journaux d'audit"

"PLACER l'objet"

Opérations pour les téléchargements partitionnés

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

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

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

- Vous ne devez pas dépasser 1,000 téléchargements partitionnés simultanés dans un seul compartiment car les résultats des requêtes List Multipart Uploads pour ce compartiment pourraient renvoyer des résultats incomplets.
- StorageGRID fait respecter les limites de taille d'AWS pour les pièces en plusieurs parties. Les clients S3 doivent respecter les consignes suivantes :
  - Chaque partie d'un téléchargement partitionné doit être comprise entre 5 Mio (5,242,880 octets) et 5 Gio (5,368,709,120 octets).
  - La dernière partie peut être inférieure à 5 Mio (5,242,880 octets).
  - En général, la taille des pièces doit être la plus grande possible. Par exemple, utilisez une taille de pièce de 5 Gio pour un objet de 100 Gio. Comme chaque pièce est considérée comme un objet unique, l'utilisation de grandes tailles de pièce réduit la surcharge des métadonnées StorageGRID.
  - Pour les objets de moins de 5 Gio, envisagez l'utilisation de téléchargement non partitionné.
- Le ILM est évalué pour chaque partie d'un objet partitionné à l'ingestion et pour l'objet dans son ensemble, à la fin du téléchargement partitionné, si la règle ILM utilise le comportement d'entrée strict ou équilibré.

Vous devez savoir comment cela affecte le positionnement de l'objet et de la pièce :

  - Si le téléchargement partitionné est en cours de modification du ILM, si le téléchargement partitionné et certaines parties de l'objet peuvent ne pas répondre aux exigences ILM actuelles. Toute pièce qui n'est pas placée correctement est mise en file d'attente pour la réévaluation ILM et est déplacée ultérieurement au bon emplacement.
  - Lors de l'évaluation d'ILM pour une pièce, StorageGRID filtre la taille de la pièce, et non la taille de l'objet. Cela signifie que certaines parties d'un objet peuvent être stockées à des emplacements ne respectant pas les exigences ILM de l'objet dans son ensemble. Par exemple, si une règle indique que tous les objets de 10 Go ou plus sont stockés dans DC1 alors que tous les objets plus petits sont stockés dans DC2, à l'acquisition chaque partie de 1 Go d'un téléchargement partitionné en 10 parties est stockée dans DC2. Lorsque ILM est évaluée pour l'ensemble de l'objet, toutes les parties de l'objet sont déplacées vers DC1.

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

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

Informations associées

"Contrôles de cohérence"

"À l'aide du chiffrement côté serveur"

Liste des téléchargements partitionnés

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

Les paramètres de demande suivants sont pris en charge :

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

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

Gestion des versions

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

Lancer le téléchargement de pièces multiples

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

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

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

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

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

    Si StorageGRID peut immédiatement créer toutes les copies d'objet spécifiées dans la règle ILM (placement synchrone), l' `x-amz-storage-class` la barre de coupe n'a aucun effet.
- `REDUCED_REDUNDANCY`
  - **Double commit** : si la règle ILM spécifie l'option de double validation pour le comportement d'ingestion, StorageGRID crée une copie intermédiaire unique lors de l'ingestion de l'objet (simple commit).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

"Utilisation du verrouillage d'objet S3"

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

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

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

Demander des en-têtes pour le cryptage côté serveur

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

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

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

En-têtes de requête non pris en charge

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

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

Gestion des versions

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

Informations associées

"Gestion des objets avec ILM"

"À l'aide du chiffrement côté serveur"

"PLACER l'objet"

Télécharger la pièce

L'opération de téléchargement de pièce télécharge une pièce dans un téléchargement partitionné pour un objet.

En-têtes de demande pris en charge

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

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

Demander des en-têtes pour le cryptage côté serveur

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

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

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

Gestion des versions

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

Informations associées

"À l'aide du chiffrement côté serveur"

Télécharger la pièce - Copier

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

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

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

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

- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-if-modified-since`

Demander des en-têtes pour le cryptage côté serveur

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

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

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

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

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

Gestion des versions

Le téléchargement partitionné est constitué de différentes opérations permettant de lancer le téléchargement, de répertorier les téléchargements, de télécharger des pièces, d'assembler les pièces téléchargées et de

terminer le téléchargement. Les objets sont créés (et versionnés le cas échéant) lorsque l'opération de chargement multipièce complète est exécutée.

Chargement de pièces multiples complet

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

Résolution des conflits

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

Taille de l'objet

StorageGRID prend en charge les objets pouvant atteindre 5 To.

En-têtes de demande

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

- `STANDARD`

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

- `REDUCED_REDUNDANCY`

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

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

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

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

Gestion des versions

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

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

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

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

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

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

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

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

Informations associées

"Gestion des objets avec ILM"

Réponses d'erreur

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

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

Nom	Statut HTTP
AccessDenied	403 interdit
BadDigest	400 demande erronée
BucketAlreadyExists	409 conflit
BucketNotEmpty	409 conflit

Nom	Statut HTTP
Corps entier	400 demande erronée
Erreur interne	500 erreur interne du serveur
InvalidAccessKeyId	403 interdit
Invalides	400 demande erronée
InvalidBucketName	400 demande erronée
InvalidBucketState	409 conflit
InvalidDigest	400 demande erronée
InvalidEncryptionAlgorithmError	400 demande erronée
Invalidpart	400 demande erronée
Ordre de pièce InvalidPartOrder	400 demande erronée
InvalidRange	416 Plage demandée non satisfiable
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

Nom	Statut HTTP
NoSuchBucket	404 introuvable
NoSuchKey	404 introuvable
NoSuchUpload	404 introuvable
Note d’implémentation	501 non mis en œuvre
NoSuchBucketPolicy	404 introuvable
ObjectLockNotConfigurationError	404 introuvable
Pré-conditionFailed	412 Echec de la condition préalable
RequestTimeTooSkewed	403 interdit
Disponibilité des services	503 Service indisponible
SignatureDoesNotMatch	403 interdit
TooManyseaux	400 demande erronée
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

Nom	Description	Statut HTTP
XMaxBucketPolicyLengthExcediéd é	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