Prise en charge de l'API REST Amazon S3

StorageGRID software

NetApp
December 03, 2025

Sommaire

Prise en charge de l'API REST Amazon S3

Détails d'implémentation de l'API REST S3

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

Le système StorageGRID prend en charge à la fois les demandes de type hébergé virtuel et les demandes de type chemin.

Gestion des dates

L'implémentation StorageGRID de l'API REST S3 prend uniquement en charge 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 horaire de la date peut être spécifiée au format Greenwich Mean Time (GMT) ou au format Universal Coordinated Time (UTC) sans décalage de fuseau horaire (+0000 doit être spécifié). Si vous incluez le `x-amz-date` en-tête de votre demande, il remplace toute valeur spécifiée dans l'en-tête de la demande Date. Lors de l'utilisation d'AWS Signature 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 requête courants

Le système StorageGRID prend en charge les en-têtes de requête courants définis par "Référence de l'API Amazon Simple Storage Service : en-têtes de requête courants" , à une exception près.

En-tête de la requête	Mise en œuvre
Autorisation	Prise en charge complète d'AWS Signature Version 2 Prise en charge d'AWS Signature version 4, avec les exceptions suivantes : • Lorsque vous fournissez la valeur réelle de la somme de contrôle de la charge utile dans `x-amz-content-sha256` , la valeur est acceptée sans validation, comme si la valeur `UNSIGNED-PAYLOAD` avait été prévu pour l'en-tête. Lorsque vous fournissez un `x-amz-content-sha256` valeur d'en-tête qui implique `aws-chunked` en streaming (par exemple, STREAMING-AWS4-HMAC-SHA256-PAYLOAD), les signatures de bloc ne sont pas vérifiées par rapport aux données de bloc.
jeton de sécurité x-amz	Non implémenté. Retours `XNotImplemented` .

En-têtes de réponse courants

Le système StorageGRID prend en charge tous les en-têtes de réponse courants définis par la *Référence API du service de stockage simple*, à une exception près.

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

Authentifier les demandes

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

L'API S3 prend en charge les versions Signature 2 et Signature 4 pour l'authentification des requêtes API S3.

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

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

Utiliser l'en-tête d'autorisation HTTP

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

Utiliser les paramètres de requête

Vous pouvez utiliser des paramètres de requête pour ajouter des informations d'authentification à une URL. Ceci est connu sous le nom de 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 un tiers à une ressource.

Opérations sur le service

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

Opération	Mise en œuvre
Listes de seaux (anciennement nommé service GET)	Implémenté avec tous les comportements de l'API REST Amazon S3. Sous réserve de modifications sans préavis.

Opération	Mise en œuvre
Utilisation du stockage GET	Le StorageGRID"Utilisation du stockage GET" La demande 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 clientes peuvent émettre `OPTIONS /` demandes adressées au port S3 sur un nœud de stockage, sans fournir les informations d'identification d'authentification S3, pour déterminer si le nœud de stockage est disponible. Vous pouvez utiliser cette demande pour la surveillance ou pour permettre aux équilibreurs de charge externes d'identifier quand un nœud de stockage est en panne.

Opérations sur les godets

Le système StorageGRID prend en charge un maximum de 5 000 buckets pour chaque compte de locataire S3.

Chaque grille peut contenir un maximum de 100 000 buckets.

Pour prendre en charge 5 000 buckets, chaque nœud de stockage de la grille doit disposer d'un minimum de 64 Go de RAM.

Les restrictions de nom de bucket suivent les restrictions régionales standard AWS US, mais vous devez les restreindre davantage aux conventions de dénomination DNS pour prendre en charge les demandes de style hébergé virtuel S3.

Pour plus d'informations, voir les éléments suivants :

- "Guide de l'utilisateur d'Amazon Simple Storage Service : quotas, restrictions et limitations des buckets"
- "Configurer les noms de domaine des points de terminaison S3"

Les opérations ListObjects (GET Bucket) et ListObjectVersions (versions d'objet GET Bucket) prennent en charge StorageGRID"valeurs de cohérence" .

Vous pouvez vérifier si les mises à jour de l'heure du dernier accès sont activées ou désactivées pour des compartiments individuels. Voir "Heure du dernier accès au bucket GET" .

Le tableau suivant décrit comment StorageGRID implémente les opérations de bucket S3 REST API. Pour effectuer l'une de ces opérations, les informations d'accès nécessaires doivent être fournies pour le compte.

Opération	Mise en œuvre
Créer un bucket	Crée un nouveau bucket. En créant le bucket, vous devenez le propriétaire du bucket. • Les noms de bucket doivent respecter les règles suivantes : ◦ Doit être unique sur chaque système StorageGRID (pas seulement unique au sein du compte locataire). ◦ Doit être conforme au DNS. ◦ Doit contenir au moins 3 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 minuscule ou un chiffre et ne peut utiliser que des lettres minuscules, des chiffres et des traits d'union. ◦ Ne doit pas ressembler à une adresse IP au format texte. ◦ Ne doit pas utiliser de points dans les requêtes de style hébergé virtuellement. Les points entraîneront des problèmes avec la vérification du certificat générique du serveur. • Par défaut, les buckets sont créés dans le `us-east-1` région; cependant, vous pouvez utiliser le `LocationConstraint` élément de demande dans le corps de la demande pour spécifier une région différente. Lors de l'utilisation du `LocationConstraint` élément, vous devez spécifier le nom exact d'une région qui a été définie à l'aide du gestionnaire de grille ou de l'API de gestion de grille. Contactez votre administrateur système si vous ne connaissez pas le nom de la région à utiliser. **Remarque** : une erreur se produira si votre demande CreateBucket utilise une région qui n'a pas été définie dans StorageGRID. • Vous pouvez inclure le `x-amz-bucket-object-lock-enabled` en-tête de demande pour créer un bucket avec S3 Object Lock activé. Voir "Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3" . Vous devez activer le verrouillage d'objet S3 lorsque vous créez le bucket. Vous ne pouvez pas ajouter ou désactiver le verrouillage d'objet S3 après la création d'un bucket. S3 Object Lock nécessite le contrôle de version du bucket, qui est activé automatiquement lorsque vous créez le bucket.
Supprimer le bucket	Supprime le bucket.
SupprimerBucketCors	Supprime la configuration CORS pour le bucket.
Supprimer le chiffrement du bucket	Supprime le cryptage par défaut du bucket. Les objets chiffrés existants restent chiffrés, mais tous les nouveaux objets ajoutés au bucket ne sont pas chiffrés.
Supprimer le cycle de vie du bucket	Supprime la configuration du cycle de vie du bucket. Voir "Créer une configuration du cycle de vie S3" .

Opération	Mise en œuvre
Supprimer la politique de bucket	Supprime la politique attachée au bucket.
SupprimerBucketReplication	Supprime la configuration de réplication attachée au bucket.
Supprimer le balisage du bucket	Utilise le `tagging` sous-ressource pour supprimer toutes les balises d'un bucket. **Attention** : Si une balise de politique ILM non par défaut est définie pour ce compartiment, il y aura un `NTAP-SG-ILM-BUCKET-TAG` balise de bucket avec une valeur qui lui est attribuée. N'émettez pas de demande DeleteBucketTagging s'il y a un `NTAP-SG-ILM-BUCKET-TAG` étiquette de seau. Au lieu de cela, émettez une requête PutBucketTagging avec uniquement le `NTAP-SG-ILM-BUCKET-TAG` balise et sa valeur attribuée pour supprimer toutes les autres balises du bucket. Ne pas modifier ni supprimer le `NTAP-SG-ILM-BUCKET-TAG` étiquette de seau.
ObtenirBucketAcl	Renvoie une réponse positive et l'ID, le nom d'affichage et l'autorisation du propriétaire du bucket, indiquant que le propriétaire a un accès complet au bucket.
ObtenirBucketCors	Renvoie le `cors` configuration pour le bucket.
Obtenir le chiffrement du bucket	Renvoie la configuration de chiffrement par défaut pour le bucket.
GetBucketLifecycleConfiguration (anciennement appelé cycle de vie du bucket GET)	Renvoie la configuration du cycle de vie du bucket. Voir "Créer une configuration du cycle de vie S3" .
Obtenir l'emplacement du bucket	Renvoie la région qui a été définie à l'aide de `LocationConstraint` élément dans la requête CreateBucket. Si la région du bucket est `us-east-1` , une chaîne vide est renvoyée pour la région.
Configuration de GetBucketNotification (anciennement appelée notification GET Bucket)	Renvoie la configuration de notification attachée au bucket.
Obtenir la politique de Bucket	Renvoie la politique attachée au bucket.
Réplication GetBucket	Renvoie la configuration de réplication attachée au bucket.

Opération	Mise en œuvre
Obtenir le balisage du bucket	Utilise le `tagging` sous-ressource pour renvoyer toutes les balises d'un bucket. **Attention** : Si une balise de politique ILM non par défaut est définie pour ce compartiment, il y aura un `NTAP-SG-ILM-BUCKET-TAG` balise de bucket avec une valeur qui lui est attribuée. Ne pas modifier ni supprimer cette balise.
Obtenir la gestion des versions du bucket	Cette implémentation utilise le `versioning` sous-ressource pour renvoyer l'état de version d'un bucket. • *blank* : le contrôle de version n'a jamais été activé (le bucket est « Non versionné ») • Activé : le contrôle de version est activé • Suspendu : le contrôle de version était précédemment activé et est suspendu
Obtenir la configuration du verrouillage de l'objet	Renvoie le mode de conservation par défaut du bucket et la période de conservation par défaut, si configurés. Voir "Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3" .
Tête de godet	Détermine si un bucket existe et si vous avez l'autorisation d'y accéder. Cette opération renvoie : • `x-ntap-sg-bucket-id`: L'UUID du bucket au format UUID. • `x-ntap-sg-trace-id`: L'ID de trace unique de la demande associée.
ListObjects et ListObjectsV2 (anciennement nommé GET Bucket)	Renvoie tout ou partie (jusqu'à 1 000) des objets d'un bucket. La classe de stockage des objets peut avoir l'une des deux valeurs, même si l'objet a été ingéré avec le `REDUCED_REDUNDANCY` option de classe de stockage : • `STANDARD`, ce qui indique que l'objet est stocké dans un pool de stockage composé de nœuds de stockage. • `GLACIER`, ce qui indique que l'objet a été déplacé vers le bucket 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 certaines `CommonPrefixes` qui ne contiennent pas de clés.
ListObjectVersions (anciennement appelées versions d'objets GET Bucket)	Avec un accès en LECTURE sur un bucket, en utilisant cette opération avec le `versions` la sous-ressource répertorie les métadonnées de toutes les versions des objets dans le bucket.

Opération	Mise en œuvre
PutBucketCors	Définit la configuration CORS pour un bucket afin que celui-ci puisse traiter les demandes inter-origines. Le partage de ressources inter-origines (CORS) est un mécanisme de sécurité qui permet aux applications Web clientes d'un domaine d'accéder aux ressources d'un domaine différent. Par exemple, supposons que vous utilisiez un bucket S3 nommé `images` pour stocker des graphiques. En définissant la configuration CORS pour le `images` bucket, vous pouvez autoriser l'affichage des images de ce bucket sur le site Web `http://www.example.com` .
Cryptage PutBucket	Définit l'état de cryptage par défaut d'un bucket existant. Lorsque le chiffrement au niveau du bucket est activé, tout nouvel objet ajouté au bucket est chiffré. StorageGRID prend en charge le chiffrement côté serveur avec des clés gérées par StorageGRID. Lors de la spécification de la règle de configuration de chiffrement côté serveur, définissez le `SSEAlgorithm` paramètre à `AES256` , et n'utilisez pas le `KMSMasterKeyID` paramètre. La configuration de chiffrement par défaut du bucket est ignorée si la demande de téléchargement d'objet spécifie déjà le chiffrement (c'est-à-dire si la demande inclut le `x-amz-server-side-encryption-*` en-tête de requête).
Configuration du cycle de vie de PutBucket (anciennement appelé cycle de vie du bucket PUT)	Crée une nouvelle configuration de cycle de vie pour le bucket 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 de cycle de vie. Chaque règle peut inclure les éléments XML suivants : • Expiration (jours, date, ExpiredObjectDeleteMarker) • NoncurrentVersionExpiration (NewerNoncurrentVersions, NoncurrentDays) • Filtre (préfixe, balise) • Statut • ID StorageGRID ne prend pas en charge ces actions : • AbandonnerTéléchargement multi-parties incomplet • Transition Voir "Créer une configuration du cycle de vie S3" . Pour comprendre comment l'action Expiration dans un cycle de vie de bucket interagit avec les instructions de placement ILM, voir"Comment ILM fonctionne tout au long de la vie d'un objet" . **Remarque** : la configuration du cycle de vie du bucket peut être utilisée avec les buckets pour lesquels le verrouillage d'objet S3 est activé, mais la configuration du cycle de vie du bucket n'est pas prise en charge pour les buckets conformes hérités.

Opération	Mise en œuvre

Configuration de PutBucketNotification
 	
(anciennement appelée notification PUT Bucket)
	Configure les notifications pour le bucket à l'aide du XML de configuration de notification inclus dans le corps de la demande. Vous devez être conscient des détails de mise en œuvre suivants :
	
	• StorageGRID prend en charge les rubriques Amazon Simple Notification Service (Amazon SNS) ou Kafka comme destinations. Les points de terminaison Simple Queue Service (SQS) ou Amazon Lambda ne sont pas pris en charge.
	• La destination des notifications doit être spécifiée comme l'URN d'un point de terminaison StorageGRID . Les points de terminaison peuvent être créés à l'aide du gestionnaire de locataires ou de l'API de gestion des locataires.
	
	Le point de terminaison doit exister pour que la configuration des notifications réussisse. Si le point de terminaison n'existe pas, un `400 Bad Request` l'erreur est renvoyée avec le code `InvalidArgument` .
	
	• Vous ne pouvez pas configurer de notification pour les types d'événements suivants. Ces types d'événements ne sont **pas** pris en charge.
	◦ `s3:ReducedRedundancyLostObject`
	◦ `s3:ObjectRestore:Completed`
	• Les notifications d'événements envoyées depuis StorageGRID utilisent le format JSON standard, sauf qu'elles n'incluent pas certaines clés et utilisent des valeurs spécifiques pour d'autres, comme indiqué dans la liste suivante :
	◦ **Source de l'événement**
	
	`sgws:s3`
	
	◦ **awsRegion**
	
	non inclus
	
	◦ **x-amz-id-2**
	
	non inclus
	
	◦ **arn**
	
	`urn:sgws:s3:::bucket_name`

Politique de PutBucket	Définit la politique attachée au bucket. Voir "Utiliser des politiques d'accès aux buckets et aux groupes" .

Opération	Mise en œuvre
Réplication de PutBucket	Configure"Réplication StorageGRID CloudMirror" pour le bucket utilisant la configuration de réplication XML fournie dans le corps de la demande. Pour la réplication CloudMirror, vous devez connaître les détails d'implémentation suivants : • StorageGRID prend uniquement en charge la version V1 de la configuration de réplication. Cela signifie que StorageGRID ne prend pas en charge l'utilisation du `Filter` élément pour les règles et suit les conventions V1 pour la suppression des versions d'objet. Pour plus de détails, voir "Guide de l'utilisateur d'Amazon Simple Storage Service : Configuration de la réplication" . • La réplication de bucket peut être configurée sur des buckets versionnés ou non versionnés. • Vous pouvez spécifier un bucket de destination différent dans chaque règle du XML de configuration de réplication. Un bucket source peut être répliqué vers plusieurs buckets de destination. • Les buckets de destination doivent être spécifiés comme URN des points de terminaison StorageGRID comme spécifié dans le gestionnaire de locataires ou l'API de gestion des locataires. Voir "Configurer la réplication CloudMirror" . Le point de terminaison doit exister pour que la configuration de la réplication réussisse. Si le point de terminaison n'existe pas, la demande échoue en tant que `400 Bad Request` . Le message d'erreur indique : `Unable to save the replication policy. The specified endpoint URN does not exist: URN.` • Vous n'avez pas besoin de spécifier un `Role` dans la configuration XML. Cette valeur n'est pas utilisée par StorageGRID et sera ignorée si elle est 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 bucket source ou si vous supprimez le bucket source lui-même, le comportement de la réplication inter-région est le suivant : ◦ Si vous supprimez l'objet ou le bucket avant qu'il ne soit répliqué, l'objet/bucket n'est pas répliqué et vous n'en êtes pas averti. ◦ Si vous supprimez l'objet ou le compartiment après sa réplication, StorageGRID suit le comportement de suppression standard d'Amazon S3 pour la V1 de la réplication inter-régions.

Opération	Mise en œuvre
Balisage de PutBucket	Utilise le `tagging` sous-ressource pour ajouter ou mettre à jour un ensemble de balises pour un bucket. Lorsque vous ajoutez des balises de bucket, tenez compte des limitations suivantes : • StorageGRID et Amazon S3 prennent en charge jusqu'à 50 balises pour chaque compartiment. • Les balises associées à un bucket doivent avoir des clés de balise uniques. Une clé de balise peut comporter jusqu'à 128 caractères Unicode. • Les valeurs des balises peuvent contenir jusqu'à 256 caractères Unicode. • La clé et les valeurs sont sensibles à la casse. **Attention** : Si une balise de politique ILM non par défaut est définie pour ce compartiment, il y aura un `NTAP-SG-ILM-BUCKET-TAG` balise de bucket avec une valeur qui lui est attribuée. Assurez-vous que le `NTAP-SG-ILM-BUCKET-TAG` la balise de bucket est incluse avec la valeur attribuée dans toutes les requêtes PutBucketTagging. Ne pas modifier ni supprimer cette balise. **Remarque** : cette opération écrasera toutes les balises actuelles que le bucket possède déjà. Si des balises existantes sont omises de l'ensemble, ces balises seront supprimées pour le bucket.
Gestion des versions de PutBucket	Utilise le `versioning` sous-ressource pour définir l'état de version d'un bucket existant. Vous pouvez définir l'état de versionnage avec l'une des valeurs suivantes : • Activé : active le contrôle de version pour les objets du bucket. Tous les objets ajoutés au bucket reçoivent un ID de version unique. • Suspendu : désactive le contrôle de version pour les objets du bucket. Tous les objets ajoutés au bucket reçoivent l'ID de version `null` .
Configuration de PutObjectLock	Configure ou supprime le mode de conservation par défaut du bucket et la période de conservation par défaut. Si la période de conservation par défaut est modifiée, la date de conservation des versions d'objet existantes reste la même et n'est pas recalculée à l'aide de la nouvelle période de conservation par défaut. Voir"Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3" pour des informations détaillées.

Opérations sur les objets

Opérations sur les objets

Cette section décrit comment le système StorageGRID implémente les opérations API REST S3 pour les objets.

Les conditions suivantes s'appliquent à toutes les opérations sur les objets :

- StorageGRID"valeurs de cohérence" sont pris en charge par toutes les opérations sur les objets, à l'exception des suivantes :
  - ObtenirObjectAcl
  - `OPTIONS /`
  - MettreObjetLegalHold
  - PutObjectRetention
  - Sélectionner le contenu de l'objet
- Les demandes client conflictuelles, telles que deux clients écrivant sur la même clé, sont résolues sur la base des « derniers gagnants ». Le moment de l'évaluation des « dernières victoires » est basé sur le moment où le système StorageGRID termine une demande donnée, et non sur le moment où les clients S3 commencent une opération.
- Tous les objets d'un bucket StorageGRID appartiennent au propriétaire du bucket, y compris les objets créés par un utilisateur anonyme ou par un autre compte.
- Les objets de données ingérés dans le système StorageGRID via Swift ne sont pas accessibles via S3.

Le tableau suivant décrit comment StorageGRID implémente les opérations d'objet S3 REST API.

Opération	Mise en œuvre
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 demande DeleteObject, StorageGRID tente de supprimer immédiatement toutes les copies de l'objet de tous les emplacements stockés. En cas de succès, StorageGRID renvoie immédiatement une réponse au client. Si toutes les copies ne peuvent pas être supprimées dans les 30 secondes (par exemple, parce qu'un emplacement est temporairement indisponible), StorageGRID met les copies en file d'attente pour suppression, puis indique la réussite au client. **Gestion des versions** Pour supprimer une version spécifique, le demandeur doit être le propriétaire du bucket 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 défini sur `true` . • Si un objet est supprimé sans le `versionId` sous-ressource sur un bucket avec le contrôle de version activé, cela entraîne la génération d'un marqueur de suppression. Le `versionId` pour le marqueur de suppression est renvoyé en utilisant le `x-amz-version-id` en-tête de réponse et le `x-amz-delete-marker` l'en-tête de réponse est renvoyé défini sur `true` . • Si un objet est supprimé sans le `versionId` sous-ressource sur un bucket avec contrôle de version suspendu, cela entraîne une suppression permanente d'une version « null » déjà existante 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 défini sur `true` . **Remarque** : Dans certains cas, plusieurs marqueurs de suppression peuvent exister pour un objet. Voir"Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3" pour savoir comment supprimer des versions d'objets en mode GOUVERNANCE.
Supprimer les objets (précédemment nommé 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. Voir"Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3" pour savoir comment supprimer des versions d'objets en mode GOUVERNANCE.

Opération	Mise en œuvre
Supprimer l'étiquetage des objets	Utilise le `tagging` sous-ressource pour supprimer toutes les balises d'un objet. **Gestion des versions** Si le `versionId` si le paramètre de requête n'est pas spécifié dans la requête, l'opération supprime toutes les balises de la version la plus récente de l'objet dans un bucket versionné. Si la version actuelle de l'objet est un marqueur de suppression, un statut « MethodNotAllowed » est renvoyé avec le `x-amz-delete-marker` en-tête de réponse défini sur `true` .
Obtenir l'objet	"Obtenir l'objet"
ObtenirObjectAcl	Si les informations d'identification d'accès nécessaires sont fournies pour le compte, l'opération renvoie une réponse positive et l'ID, le nom d'affichage et l'autorisation du propriétaire de l'objet, indiquant que le propriétaire dispose d'un accès complet à l'objet.
Obtenir la conservation légale de l'objet	"Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3"
Obtenir la rétention d'objet	"Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3"
Obtenir l'étiquetage des objets	Utilise le `tagging` sous-ressource pour renvoyer toutes les balises d'un objet. **Gestion des versions** Si le `versionId` si le paramètre de requête n'est pas spécifié dans la requête, l'opération renvoie toutes les balises de la version la plus récente de l'objet dans un bucket versionné. Si la version actuelle de l'objet est un marqueur de suppression, un statut « MethodNotAllowed » est renvoyé avec le `x-amz-delete-marker` en-tête de réponse défini sur `true` .
HeadObject	"HeadObject"
Restaurer l'objet	"Restaurer l'objet"
Mettre l'objet	"Mettre l'objet"
Copier l'objet (précédemment nommé PUT Object - Copy)	"Copier l'objet"
MettreObjetLegalHold	"Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3"

Opération	Mise en œuvre
PutObjectRetention	"Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3"
Balisage d'objets	Utilise le `tagging` sous-ressource pour ajouter un ensemble de balises à un objet existant. **Limites des balises d'objet** Vous pouvez ajouter des balises aux nouveaux objets lorsque vous les téléchargez, ou vous pouvez les ajouter aux 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 contenir jusqu'à 128 caractères Unicode et les valeurs de balise peuvent contenir jusqu'à 256 caractères Unicode. La clé et les valeurs sont sensibles à la casse. **Mises à jour des balises et comportement d'ingestion** Lorsque vous utilisez PutObjectTagging pour mettre à jour les balises d'un objet, StorageGRID ne réingère pas l'objet. Cela signifie que l'option pour le comportement d'ingestion spécifiée dans la règle ILM correspondante n'est pas utilisée. Toutes les modifications apportées au placement des objets déclenchées par la mise à jour sont effectuées lorsque ILM est réévalué par les processus ILM d'arrière-plan normaux. Cela signifie que si la règle ILM utilise l'option Strict pour le comportement d'ingestion, aucune action n'est entreprise si les placements d'objets requis ne peuvent pas être effectués (par exemple, parce qu'un emplacement nouvellement requis n'est pas disponible). L'objet mis à jour conserve son emplacement actuel jusqu'à ce que le placement requis soit possible. **Résoudre les conflits** Les demandes client conflictuelles, telles que deux clients écrivant sur la même clé, sont résolues sur la base des « derniers gagnants ». Le moment de l'évaluation des « dernières victoires » est basé sur le moment où le système StorageGRID termine 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 bucket versionné. Si la version actuelle de l'objet est un marqueur de suppression, un statut « MethodNotAllowed » est renvoyé avec le `x-amz-delete-marker` en-tête de réponse défini sur `true` .
Sélectionner le contenu de l'objet	"Sélectionner le contenu de l'objet"

Utiliser S3 Select

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

> Tous les éléments non répertoriés ne sont pas pris en charge.

Pour la syntaxe, voir"Sélectionner le contenu de l'objet" . Pour plus d'informations sur S3 Select, consultez le "Documentation AWS pour S3 Select" .

Seuls les comptes locataires pour lesquels S3 Select est activé peuvent émettre des requêtes SelectObjectContent. Voir le"considérations et exigences pour l'utilisation de S3 Select" .

Clauses

- Liste SELECT
- Clause FROM
- Clause WHERE
- Clause LIMIT

Types de données

- booléen
- entier
- chaîne
- flotter
- décimal, numérique
- horodatage

Opérateurs

Opérateurs logiques

- ET
- PAS
- OU

Opérateurs de comparaison

- <
- >
- ⇐
- >=
- =
- =
- <>

- !=
- ENTRE
- DANS

Opérateurs de recherche de motifs

- COMME
- _
- %

opérateurs unitaires

- EST NUL
- N'EST PAS NUL

opérateurs mathématiques

- +
- -
- *
- /
- %

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

Fonctions d'agrégation

- MOYENNE()
- COMPTER(*)
- MAX()
- MIN()
- SOMME()

Fonctions conditionnelles

- CAS
- SE FONDRE
- NULLIF

Fonctions de conversion

- CAST (pour le type de données pris en charge)

Fonctions de date

- DATE_ADD
- DATE_DIFF

- EXTRAIT
- TO_STRING
- À_HORODATAGE
- UTCNOW

Fonctions de chaîne

- LONGUEUR_CARACTÈRE, LONGUEUR_CARACTÈRE
- INFÉRIEUR
- SOUS-CHAÎNE
- GARNITURE
- SUPÉRIEUR

Utiliser le cryptage côté serveur

Le chiffrement côté serveur vous permet de protéger vos données d'objet au repos. StorageGRID crypte les données lorsqu'il écrit l'objet 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 manière dont les clés de chiffrement sont gérées :

- **SSE (chiffrement côté serveur avec clés gérées par StorageGRID)** : lorsque vous émettez une demande S3 pour stocker un objet, StorageGRID chiffre l'objet avec une clé unique. Lorsque vous émettez une demande S3 pour récupérer l'objet, StorageGRID utilise la clé stockée pour déchiffrer 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 déchiffré et vos données d'objet sont renvoyées.

  Bien que StorageGRID gère toutes les opérations de chiffrement et de déchiffrement d'objets, vous devez gérer les clés de chiffrement que vous fournissez.

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

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

Utiliser SSE

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

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

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

- "Mettre l'objet"

- "Copier l'objet"
- "Créer un téléchargement multi-parties"

Utiliser SSE-C

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

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

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

- "Obtenir l'objet"
- "HeadObject"
- "Mettre l'objet"
- "Copier l'objet"
- "Créer un téléchargement multi-parties"
- "Télécharger une partie"
- "TéléchargerPartCopy"

Considérations relatives à l'utilisation du chiffrement côté serveur avec des clés fournies par le client (SSE-C)

Avant d'utiliser SSE-C, tenez compte des considérations suivantes :

- Vous devez utiliser https.

> StorageGRID rejette toute requête effectuée via http lors de l'utilisation de SSE-C. Pour des raisons de sécurité, il est important de considérer que toute clé envoyée accidentellement via http est compromise. Jetez la clé et faites-la tourner comme il convient.

- L'ETag dans la réponse n'est pas le MD5 des données de l'objet.
- Vous devez gérer le mappage des clés de chiffrement aux objets. StorageGRID ne stocke pas les clés de chiffrement. Vous êtes responsable du suivi de la clé de cryptage que vous fournissez pour chaque objet.
- Si votre bucket est compatible avec le contrôle de version, chaque version d'objet doit avoir sa propre clé de chiffrement. Vous êtes responsable du suivi de la clé de chiffrement utilisée pour chaque version d'objet.

- Étant donné que vous gérez les clés de chiffrement côté client, vous devez également gérer toutes les mesures de protection supplémentaires, telles que la rotation des clés, côté client.

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

- Si la réplication inter-grille ou la réplication CloudMirror est configurée pour le bucket, vous ne pouvez pas ingérer d'objets SSE-C. L'opération d'ingestion échouera.

Informations connexes

"Guide de l'utilisateur Amazon S3 : Utilisation du chiffrement côté serveur avec les clés fournies par le client (SSE-C)"

Copier l'objet

Vous pouvez utiliser la requête S3 CopyObject pour créer une copie d'un objet déjà stocké dans S3. Une opération CopyObject revient à exécuter GetObject suivi de PutObject.

Résoudre les conflits

Les demandes client conflictuelles, telles que deux clients écrivant sur la même clé, sont résolues sur la base des « derniers gagnants ». Le moment de l'évaluation des « dernières victoires » est basé sur le moment où le système StorageGRID termine une demande donnée, et non sur le moment où les clients S3 commencent une opération.

Taille de l'objet

La taille maximale *recommandée* pour une seule opération PutObject est de 5 Gio (5 368 709 120 octets). Si vous avez des objets dont la taille est supérieure à 5 Gio, utilisez"téléchargement en plusieurs parties" plutôt.

La taille maximale *prise en charge* pour une seule opération PutObject est de 5 Tio (5 497 558 138 880 octets).

> Si vous avez effectué une mise à niveau à partir de StorageGRID 11.6 ou d'une version antérieure, l'alerte S3 PUT La taille de l'objet est trop grande sera déclenchée si vous tentez de télécharger un objet dépassant 5 Gio. Si vous disposez d'une nouvelle installation de StorageGRID 11.7 ou 11.8, l'alerte ne sera pas déclenchée dans ce cas. Cependant, pour s'aligner sur la norme AWS S3, les futures versions de StorageGRID ne prendront pas en charge les téléchargements d'objets supérieurs à 5 Gio.

Caractères UTF-8 dans les métadonnées utilisateur

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

StorageGRID n'analyse ni n'interprète les caractères UTF-8 échappés inclus 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 inclut des caractères non imprimables.

En-têtes de requête pris en charge

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

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

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

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

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

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

    Si une demande est effectuée sans ces en-têtes, les paramètres de conservation par défaut du bucket sont utilisés pour calculer le mode de version de l'objet et la date de conservation. Voir "Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3" .

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

- `x-amz-server-side-encryption-customer-algorithm`

  Voir En-têtes de requête pour le chiffrement côté serveur

En-têtes de requête non pris en charge

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

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `Expires`
- `x-amz-checksum-algorithm`

  Lorsque vous copiez un objet, si l'objet source possède une somme de contrôle, StorageGRID ne copie pas cette valeur de somme de contrôle dans le nouvel objet. Ce comportement s'applique que vous essayiez ou non d'utiliser `x-amz-checksum-algorithm` dans la demande d'objet.

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

Options de classe de stockage

Le `x-amz-storage-class` L'en-tête de requête est pris en charge et affecte le nombre de copies d'objets créées par StorageGRID si la règle ILM correspondante utilise la validation double ou équilibrée"option d'ingestion" .

- `STANDARD`

  (Par défaut) Spécifie une opération d'ingestion à double validation lorsque la règle ILM utilise l'option Double validation ou lorsque l'option Équilibré revient à la création de copies intermédiaires.

- `REDUCED_REDUNDANCY`

  Spécifie une opération d'ingestion à validation unique lorsque la règle ILM utilise l'option de validation double ou lorsque l'option Équilibré revient à la création de copies intermédiaires.

> Si vous ingérez un objet dans un bucket avec le verrouillage d'objet S3 activé, le `REDUCED_REDUNDANCY` l'option est ignorée. Si vous ingérez un objet dans un bucket conforme hérité, le `REDUCED_REDUNDANCY` l'option renvoie une erreur. StorageGRID effectuera toujours une ingestion à double validation pour garantir que les exigences de conformité sont satisfaites.

Utilisation de x-amz-copy-source dans CopyObject

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

Si la source et la destination correspondent, et que 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. Cela a deux conséquences importantes :

- Vous ne pouvez pas utiliser CopyObject pour crypter un objet existant sur place ou pour modifier le cryptage d'un objet existant sur place. 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 `XNotImplemented` .
- L'option pour le comportement d'ingestion spécifiée dans la règle ILM correspondante n'est pas utilisée. Toutes les modifications apportées au placement des objets déclenchées par la mise à jour sont effectuées lorsque ILM est réévalué par les processus ILM d'arrière-plan normaux.

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

En-têtes de requête pour le chiffrement côté serveur

Si tu"utiliser le cryptage côté serveur" , les en-têtes de requête que vous fournissez dépendent du fait que l'objet source est chiffré ou non et du fait que vous prévoyez 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 CopyObject, afin que l'objet puisse être déchiffré puis copié :
  - `x-amz-copy-source-server-side-encryption-customer-algorithm`: Préciser `AES256` .
  - `x-amz-copy-source-server-side-encryption-customer-key`: Spécifiez la clé de chiffrement que vous avez fournie lors de la création de l'objet source.
  - `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Spécifiez le condensé MD5 que vous avez fourni lors de la création de l'objet source.
- Si vous souhaitez crypter 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`: Préciser `AES256` .
  - `x-amz-server-side-encryption-customer-key`:Spécifiez une nouvelle clé de chiffrement pour l'objet cible.
  - `x-amz-server-side-encryption-customer-key-MD5`:Spécifiez le condensé MD5 de la nouvelle clé de chiffrement.

  > Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant. Avant d'utiliser les clés fournies par le client pour sécuriser les données d'objet, examinez les considérations relatives"en utilisant le cryptage côté serveur" .
- Si vous souhaitez crypter l'objet cible (la copie) avec une clé unique gérée par StorageGRID (SSE), incluez cet en-tête dans la requête CopyObject :
  - `x-amz-server-side-encryption`

  > Le `server-side-encryption` la valeur de l'objet ne peut pas être mise à jour. Au lieu de cela, faites une copie avec un nouveau `server-side-encryption` valeur en utilisant `x-amz-metadata-directive` : `REPLACE` .

Gestion des versions

Si le bucket source est versionné, 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 la commande `versionId` sous-ressource. Si le bucket de destination est versionné, la version générée est renvoyée dans le `x-amz-version-id` en-tête de réponse. Si le contrôle de version est suspendu pour le bucket cible, alors `x-amz-version-id` renvoie une valeur « null ».

Obtenir l'objet

Vous pouvez utiliser la requête S3 GetObject pour récupérer un objet d'un bucket S3.

GetObject et objets multipartites

Vous pouvez utiliser le `partNumber` paramètre de requête pour récupérer une partie spécifique d'un objet en plusieurs parties ou segmenté. Le `x-amz-mp-parts-count` L'élément de réponse indique le nombre de parties que contient l'objet.

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

Caractères UTF-8 dans les métadonnées utilisateur

StorageGRID n'analyse ni n'interprète les caractères UTF-8 échappés dans les métadonnées définies par l'utilisateur. Les requêtes GET pour un objet avec des caractères UTF-8 échappés 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 inclut des caractères non imprimables.

En-tête de requête pris en charge

L'en-tête de requête suivant est pris en charge :

- `x-amz-checksum-mode`: Préciser `ENABLED`

  Le `Range` l'en-tête n'est pas pris en charge avec `x-amz-checksum-mode` pour GetObject. Lorsque vous incluez `Range` dans la demande avec `x-amz-checksum-mode` activé, StorageGRID ne renvoie pas de valeur de somme de contrôle dans la réponse.

En-tête de requête non pris en charge

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

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

Gestion des versions

Si un `versionId` la sous-ressource n'est pas spécifiée, l'opération récupère la version la plus récente de l'objet dans un bucket versionné. Si la version actuelle de l'objet est un marqueur de suppression, un statut « Non trouvé » est renvoyé avec le `x-amz-delete-marker` en-tête de réponse défini sur `true` .

En-têtes de requête pour le chiffrement côté serveur avec les 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`: Préciser `AES256` .
- `x-amz-server-side-encryption-customer-key`:Spécifiez votre clé de chiffrement pour l'objet.
- `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le condensé MD5 de la clé de chiffrement de l'objet.

> Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant. Avant d'utiliser les clés fournies par le client pour sécuriser les données d'objet, examinez les considérations dans"Utiliser le cryptage côté serveur" .

Comportement de GetObject pour les objets Cloud Storage Pool

Si un objet a été stocké dans un"Pool de stockage cloud" , le comportement d'une requête GetObject dépend de l'état de l'objet. Voir"HeadObject" pour plus de détails.

> Si un objet est stocké dans un pool de stockage cloud et qu'une ou plusieurs copies de l'objet existent également sur la grille, les requêtes GetObject tenteront de récupérer les données de la grille, avant de les récupérer du pool de stockage cloud.

État de l'objet	Comportement de GetObject
Objet ingéré dans StorageGRID mais pas encore évalué par ILM, ou objet stocké dans un pool de stockage traditionnel ou utilisant un codage d'effacement	`200 OK` Une copie de l'objet est récupérée.
Objet dans le pool de stockage cloud, mais pas encore passé à un état non récupérable	`200 OK` Une copie de l'objet est récupérée.
Objet passé à un état non récupérable	`403 Forbidden` , `InvalidObjectState` Utiliser un"Restaurer l'objet" demande de restauration de 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 RestoreObject soit terminée.
Objet entièrement restauré dans le pool de stockage cloud	`200 OK` Une copie de l'objet est récupérée.

Objets multipartites ou segmentés dans un pool de stockage cloud

Si vous avez téléchargé un objet en plusieurs parties ou si StorageGRID a divisé un objet volumineux en segments, StorageGRID détermine si l'objet est disponible dans le pool de stockage cloud en échantillonnant un sous-ensemble des parties ou des segments de l'objet. Dans certains cas, une requête GetObject peut renvoyer de manière incorrecte `200 OK` lorsque certaines parties de l'objet ont déjà été transférées vers un état non récupérable ou lorsque certaines parties de l'objet n'ont pas encore été restaurées.

Dans ces cas :

- La requête GetObject peut renvoyer des données mais s'arrêter à mi-chemin du transfert.
- Une requête GetObject ultérieure peut renvoyer `403 Forbidden`.

GetObject et réplication inter-grille

Si vous utilisez"fédération de réseau" et"réplication inter-réseaux" est activé pour un bucket, le client S3 peut vérifier l'état de réplication d'un objet en émettant une requête GetObject. La réponse inclut le StorageGRID spécifique `x-ntap-sg-cgr-replication-status` en-tête de réponse, qui aura l'une des valeurs suivantes :

Grille	État de réplication
Source	• **TERMINÉ** : La réplication a réussi. • **EN ATTENTE** : L'objet n'a pas encore été répliqué. • **ÉCHEC** : La réplication a échoué avec un échec permanent. Un utilisateur doit résoudre l'erreur.
Destination	**RÉPLIQUE** : L'objet a été répliqué à partir de la grille source.

> StorageGRID ne prend pas en charge le `x-amz-replication-status` en-tête.

HeadObject

Vous pouvez utiliser la requête S3 HeadObject pour récupérer les métadonnées d'un objet sans renvoyer l'objet lui-même. Si l'objet est stocké dans un pool de stockage cloud, vous pouvez utiliser HeadObject pour déterminer l'état de transition de l'objet.

HeadObject et objets multipartites

Vous pouvez utiliser le `partNumber` paramètre de demande pour récupérer les métadonnées d'une partie spécifique d'un objet en plusieurs parties ou segmenté. Le `x-amz-mp-parts-count` L'élément de réponse indique le nombre de parties que contient l'objet.

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

Caractères UTF-8 dans les métadonnées utilisateur

StorageGRID n'analyse ni n'interprète les caractères UTF-8 échappés dans les métadonnées définies par

l'utilisateur. Les requêtes HEAD pour un objet avec des caractères UTF-8 échappés 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 inclut des caractères non imprimables.

En-tête de requête pris en charge

L'en-tête de requête suivant est pris en charge :

- `x-amz-checksum-mode`

  Le `partNumber` paramètre et `Range` les en-têtes ne sont pas pris en charge avec `x-amz-checksum-mode` pour HeadObject. Lorsque vous les incluez dans la demande avec `x-amz-checksum-mode` activé, StorageGRID ne renvoie pas de valeur de somme de contrôle dans la réponse.

En-tête de requête non pris en charge

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

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

Gestion des versions

Si un `versionId` la sous-ressource n'est pas spécifiée, l'opération récupère la version la plus récente de l'objet dans un bucket versionné. Si la version actuelle de l'objet est un marqueur de suppression, un statut « Non trouvé » est renvoyé avec le `x-amz-delete-marker` en-tête de réponse défini sur `true` .

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

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

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

> Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant. Avant d'utiliser les clés fournies par le client pour sécuriser les données d'objet, examinez les considérations dans"Utiliser le cryptage côté serveur" .

Réponses HeadObject pour les objets Cloud Storage Pool

Si l'objet est stocké dans un"Pool de stockage cloud" , les en-têtes de réponse suivants sont renvoyés :

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

Les en-têtes de réponse fournissent des informations sur l'état d'un objet lorsqu'il est déplacé vers un pool de stockage cloud, éventuellement transféré vers un état non récupérable et restauré.

État de l'objet	Réponse à HeadObject
Objet ingéré dans StorageGRID mais pas encore évalué par ILM, ou objet stocké dans un pool de stockage traditionnel ou utilisant un codage d'effacement	`200 OK`(Aucun en-tête de réponse spécial n'est renvoyé.)

Objet dans le pool de stockage cloud, mais pas encore passé à 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 vers un état non récupérable, la valeur de `expiry-date` se déroule à une époque lointaine dans le futur. L'heure exacte de la transition n'est pas contrôlée par le système StorageGRID .

L'objet est passé à un état non récupérable, mais au moins une copie existe également sur la grille	`200 OK`
	
	`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` se déroule à une époque lointaine dans le futur.
	
	Remarque : Si la copie sur la grille n'est pas disponible (par exemple, un nœud de stockage est en panne), vous devez émettre un"Restaurer l'objet" demandez à restaurer la copie à partir du pool de stockage cloud avant de pouvoir récupérer l'objet avec succès.

L'objet est passé 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 HeadObject

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 dans le pool de stockage cloud sera renvoyé à un état non récupérable.

Objets multipartites ou segmentés dans le pool de stockage cloud

Si vous avez téléchargé un objet en plusieurs parties ou si StorageGRID a divisé un objet volumineux en segments, StorageGRID détermine si l'objet est disponible dans le pool de stockage cloud en échantillonnant un sous-ensemble des parties ou des segments de l'objet. Dans certains cas, une requête HeadObject peut renvoyer de manière incorrecte `x-amz-restore: ongoing-request="false"` lorsque certaines parties de l'objet ont déjà été transférées vers un état non récupérable ou lorsque certaines parties de l'objet n'ont pas encore été restaurées.

Réplication HeadObject et inter-grille

Si vous utilisez"fédération de réseau" et"réplication inter-réseaux" est activé pour un bucket, le client S3 peut vérifier l'état de réplication d'un objet en émettant une demande HeadObject. La réponse inclut le StorageGRID spécifique `x-ntap-sg-cgr-replication-status` en-tête de réponse, qui aura l'une des valeurs suivantes :

Grille	État de réplication
Source	• **TERMINÉ** : La réplication a réussi. • **EN ATTENTE** : L'objet n'a pas encore été répliqué. • **ÉCHEC** : La réplication a échoué avec un échec permanent. Un utilisateur doit résoudre l'erreur.
Destination	**RÉPLIQUE** : L'objet a été répliqué à partir de la grille source.

> ⓘ StorageGRID ne prend pas en charge le `x-amz-replication-status` en-tête.

Mettre l'objet

Vous pouvez utiliser la requête S3 PutObject pour ajouter un objet à un bucket.

Résoudre les conflits

Les demandes client conflictuelles, telles que deux clients écrivant sur la même clé, sont résolues sur la base des « derniers gagnants ». Le moment de l'évaluation des « dernières victoires » est basé sur le moment où le système StorageGRID termine une demande donnée, et non sur le moment où les clients S3 commencent une

opération.

Taille de l'objet

La taille maximale *recommandée* pour une seule opération PutObject est de 5 Gio (5 368 709 120 octets). Si vous avez des objets dont la taille est supérieure à 5 Gio, utilisez"téléchargement en plusieurs parties" plutôt.

La taille maximale *prise en charge* pour une seule opération PutObject est de 5 Tio (5 497 558 138 880 octets).

> Si vous avez effectué une mise à niveau à partir de StorageGRID 11.6 ou d'une version antérieure, l'alerte S3 PUT La taille de l'objet est trop grande sera déclenchée si vous tentez de télécharger un objet dépassant 5 Gio. Si vous disposez d'une nouvelle installation de StorageGRID 11.7 ou 11.8, l'alerte ne sera pas déclenchée dans ce cas. Cependant, pour s'aligner sur la norme AWS S3, les futures versions de StorageGRID ne prendront pas en charge les téléchargements d'objets supérieurs à 5 Gio.

Taille des métadonnées utilisateur

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

Caractères UTF-8 dans les métadonnées utilisateur

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

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

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

Limites des balises d'objet

Vous pouvez ajouter des balises aux nouveaux objets lorsque vous les téléchargez, ou vous pouvez les ajouter aux 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 contenir jusqu'à 128 caractères Unicode et les valeurs de balise peuvent contenir jusqu'à 256 caractères Unicode. La clé et les valeurs sont sensibles à la casse.

Propriété de l'objet

Dans StorageGRID, tous les objets appartiennent au compte propriétaire du bucket, y compris les objets créés par un compte non propriétaire ou un utilisateur anonyme.

En-têtes de requête pris en charge

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

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

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

  - StorageGRID ne vérifie pas le `chunk-signature` par rapport aux données du 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`

  L'encodage de transfert fragmenté est pris en charge si `aws-chunked` la signature de la charge utile est également utilisée.
- `x-amz-checksum-sha256`
- `x-amz-meta-`, suivi d'une paire nom-valeur contenant des métadonnées définies par l'utilisateur.

  Lors de la spécification de la paire nom-valeur pour les métadonnées définies par l'utilisateur, utilisez ce format général :

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

  Si vous souhaitez utiliser l'option **Heure de création définie par l'utilisateur** comme heure de référence pour une règle ILM, vous devez utiliser `creation-time` comme le nom des métadonnées qui enregistrent quand l'objet a été créé. Par exemple:

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

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

  > ⓘ Une règle ILM ne peut pas utiliser à la fois une **heure de création définie par l'utilisateur** pour l'heure de référence et l'option d'ingestion équilibrée ou stricte. Une erreur est renvoyée lors de la création de la règle ILM.

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

    Si une demande est effectuée sans ces en-têtes, les paramètres de conservation par défaut du bucket sont utilisés pour calculer le mode de version de l'objet et la date de conservation. Voir "Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3" .
- En-têtes de requête SSE :
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

    VoirEn-têtes de requête pour le chiffrement côté serveur

En-têtes de requête non pris en charge

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

- `x-amz-acl`
- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`
- `x-amz-website-redirect-location`

  Le `x-amz-website-redirect-location` retours d'en-tête `XNotImplemented` .

Options de classe de stockage

Le `x-amz-storage-class` l'en-tête de requête est pris en charge. La valeur soumise pour `x-amz-storage-class` affecte la manière dont StorageGRID protège les données de l'objet pendant l'ingestion et non le nombre de copies persistantes de l'objet stockées dans le système StorageGRID (qui est déterminé par ILM).

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

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

- `STANDARD`(Défaut)
  - **Double validation** : si la règle ILM spécifie l'option Double validation pour le comportement d'ingestion, dès qu'un objet est ingéré, une deuxième copie de cet objet est créée et distribuée à un autre nœud de stockage (double validation). Lorsque l'ILM est évalué, StorageGRID détermine si ces copies intermédiaires initiales satisfont aux instructions de placement de la règle. Si ce n'est pas le

cas, de nouvelles copies d'objets devront peut-être être réalisées à des emplacements différents et les copies intermédiaires initiales devront peut-être être supprimées.

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

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

- `REDUCED_REDUNDANCY`

  - * Double validation * : si la règle ILM spécifie l'option Double validation pour le comportement d'ingestion, StorageGRID crée une copie intermédiaire unique lorsque l'objet est ingéré (validation unique).
  - **Équilibré** : si la règle ILM spécifie l'option Équilibré, StorageGRID effectue une seule copie intermédiaire uniquement si le système ne peut pas effectuer immédiatement 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 mieux utilisée lorsque la règle ILM qui correspond à l'objet crée une seule copie répliquée. Dans ce cas, en utilisant `REDUCED_REDUNDANCY` élimine la création et la suppression inutiles d'une copie d'objet supplémentaire pour chaque opération d'ingestion.

  En utilisant le `REDUCED_REDUNDANCY` Cette option n'est pas recommandée dans d'autres circonstances. `REDUCED_REDUNDANCY` augmente le risque de perte de données d'objet lors de l'ingestion. Par exemple, vous risquez de perdre des données si la copie unique est initialement stockée sur un nœud de stockage qui échoue avant que l'évaluation ILM puisse avoir lieu.

> Le fait de n'avoir qu'une seule copie répliquée pendant une période donnée expose les données à un risque de perte permanente. Si une seule copie répliquée d'un objet existe, cet objet est perdu si un nœud de stockage échoue ou présente une erreur importante. Vous perdez également temporairement l'accès à l'objet pendant les procédures de maintenance telles que les mises à niveau.

Spécification `REDUCED_REDUNDANCY` affecte uniquement le nombre de copies créées lorsqu'un objet est ingéré pour la première fois. Cela n'affecte pas le nombre de copies de l'objet effectuées lorsque l'objet est évalué par les stratégies ILM actives et n'entraîne pas le stockage des données à des niveaux de redondance inférieurs dans le système StorageGRID .

> Si vous ingérez un objet dans un bucket avec le verrouillage d'objet S3 activé, le `REDUCED_REDUNDANCY` l'option est ignorée. Si vous ingérez un objet dans un bucket conforme hérité, le `REDUCED_REDUNDANCY` l'option renvoie une erreur. StorageGRID effectuera toujours une ingestion à double validation pour garantir que les exigences de conformité sont satisfaites.

En-têtes de requête pour le chiffrement côté serveur

Vous pouvez utiliser les en-têtes de requête suivants pour crypter un objet avec un cryptage côté serveur. Les options SSE et SSE-C s'excluent mutuellement.

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

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

Quand le `x-amz-server-side-encryption` l'en-tête n'est pas inclus dans la requête PutObject, la grille entière"paramètre de cryptage des objets stockés" est omis de la réponse PutObject.

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

> Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant. Avant d'utiliser les clés fournies par le client pour sécuriser les données d'objet, examinez les considérations relatives"en utilisant le cryptage côté serveur" .

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

Gestion des versions

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

Si le contrôle de version est suspendu, la version de l'objet est stockée avec une valeur nulle `versionId` et si une version nulle existe déjà, elle sera écrasée.

Calculs de signature pour l'en-tête d'autorisation

Lors de l'utilisation du `Authorization` en-tête pour authentifier les requêtes, StorageGRID diffère d'AWS des manières suivantes :

- StorageGRID ne nécessite pas `host` en-têtes à inclure dans `CanonicalHeaders` .
- StorageGRID ne nécessite pas `Content-Type` à inclure dans `CanonicalHeaders` .
- StorageGRID ne nécessite pas `x-amz-*` en-têtes à inclure dans `CanonicalHeaders` .

> En règle générale, incluez toujours ces en-têtes dans `CanonicalHeaders` pour garantir qu'ils sont vérifiés ; cependant, si vous excluez ces en-têtes, StorageGRID ne renvoie pas d'erreur.

Pour plus de détails, reportez-vous à "Calculs de signature pour l'en-tête d'autorisation : transfert de charge utile en un seul bloc (AWS Signature Version 4)" .

Informations connexes

- "Gérer les objets avec ILM"
- "Référence de l'API Amazon Simple Storage Service : PutObject"

Restaurer l'objet

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

Type de demande pris en charge

StorageGRID prend uniquement en charge les requêtes RestoreObject pour restaurer un objet. Il ne prend pas en charge le `SELECT` type de restauration. Sélectionnez les demandes de retour `XNotImplemented` .

Gestion des versions

En option, précisez `versionId` pour restaurer une version spécifique d'un objet dans un bucket versionné. Si vous ne précisez pas `versionId` , la version la plus récente de l'objet est restaurée

Comportement de RestoreObject sur les objets du pool de stockage cloud

Si un objet a été stocké dans un"Pool de stockage cloud" , une demande RestoreObject a le comportement suivant, en fonction de l'état de l'objet. Voir"HeadObject" pour plus de détails.

> Si un objet est stocké dans un pool de stockage cloud et qu'une ou plusieurs copies de l'objet existent également sur la grille, il n'est pas nécessaire de restaurer l'objet en émettant une demande RestoreObject. Au lieu de cela, la copie locale peut être récupérée directement, à l'aide d'une requête GetObject.

État de l'objet	Comportement de RestoreObject
Objet ingéré dans StorageGRID mais pas encore évalué par ILM, ou l'objet ne se trouve pas dans un pool de stockage cloud	`403 Forbidden` , `InvalidObjectState`
Objet dans le pool de stockage cloud, mais pas encore passé à un état non récupérable	`200 OK`Aucune modification n'est apportée. **Remarque** : Avant qu'un objet ne soit passé à un état non récupérable, vous ne pouvez pas modifier son `expiry-date` .

État de l'objet	Comportement de RestoreObject
Objet passé à un état non récupérable	`202 Accepted`Restaure une copie récupérable de l'objet dans 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 remis dans un état non récupérable. En option, utilisez le `Tier` élément de demande pour déterminer combien de temps la tâche de restauration prendra pour se terminer(`Expedited` , `Standard` , ou `Bulk`). Si vous ne précisez pas `Tier` , le `Standard` le niveau est utilisé. **Important** : Si un objet a été transféré vers S3 Glacier Deep Archive ou si le pool de stockage cloud utilise le stockage Azure Blob, vous ne pouvez pas le restaurer à l'aide de `Expedited` étage. 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`
Objet entièrement restauré dans le pool de stockage cloud	`200 OK` **Remarque :** si un objet a été restauré dans un état récupérable, vous pouvez modifier son `expiry-date` en réémettant la requête RestoreObject avec une nouvelle valeur pour `Days` . La date de restauration est mise à jour par rapport à l'heure de la demande.

Sélectionner le contenu de l'objet

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

Pour plus d'informations, voir "Référence de l'API Amazon Simple Storage Service : SelectObjectContent" .

Avant de commencer

- Le compte locataire dispose de l'autorisation S3 Select.
- Tu as `s3:GetObject` autorisation pour l'objet que vous souhaitez interroger.
- L'objet que vous souhaitez interroger doit être dans l'un des formats suivants :
  - **CSV**. Peut être utilisé tel quel ou compressé dans des archives GZIP ou BZIP2.
  - **Parquet**. Exigences supplémentaires pour les objets Parquet :
    - S3 Select prend uniquement en charge la compression en colonnes à l'aide de GZIP ou Snappy. S3 Select ne prend pas en charge la compression d'objets entiers pour les objets Parquet.
    - S3 Select ne prend pas en charge la sortie Parquet. Vous devez spécifier le format de sortie au format CSV ou JSON.
    - La taille maximale du groupe de lignes non compressé est de 512 Mo.
    - Vous devez utiliser les types de données spécifiés dans le schéma de l'objet.

        - Vous ne pouvez pas utiliser les types logiques INTERVAL, JSON, LIST, TIME ou UUID.
- Votre expression SQL a une longueur maximale de 256 Ko.
- Tout enregistrement dans l'entrée ou les résultats a une longueur maximale de 1 Mio.

Exemple de syntaxe de requête CSV

```
POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns="http://s3.amazonaws.com/doc/2006-03-
01/">
   <Expression>string</Expression>
   <ExpressionType>string</ExpressionType>
   <RequestProgress>
      <Enabled>boolean</Enabled>
   </RequestProgress>
   <InputSerialization>
      <CompressionType>GZIP</CompressionType>
      <CSV>
         <AllowQuotedRecordDelimiter>boolean</AllowQuotedRecordDelimiter>
         <Comments>#</Comments>
         <FieldDelimiter>\t</FieldDelimiter>
         <FileHeaderInfo>USE</FileHeaderInfo>
         <QuoteCharacter>'</QuoteCharacter>
         <QuoteEscapeCharacter>\\</QuoteEscapeCharacter>
         <RecordDelimiter>\n</RecordDelimiter>
      </CSV>
   </InputSerialization>
   <OutputSerialization>
      <CSV>
         <FieldDelimiter>string</FieldDelimiter>
         <QuoteCharacter>string</QuoteCharacter>
         <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
         <QuoteFields>string</QuoteFields>
         <RecordDelimiter>string</RecordDelimiter>
      </CSV>
   </OutputSerialization>
   <ScanRange>
      <End>long</End>
      <Start>long</Start>
   </ScanRange>
</SelectObjectContentRequest>
```

Exemple de syntaxe de demande de parquet

```
POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns=http://s3.amazonaws.com/doc/2006-03-01/>
   <Expression>string</Expression>
   <ExpressionType>string</ExpressionType>
   <RequestProgress>
      <Enabled>boolean</Enabled>
   </RequestProgress>
   <InputSerialization>
      <CompressionType>GZIP</CompressionType>
      <PARQUET>
      </PARQUET>
   </InputSerialization>
   <OutputSerialization>
      <CSV>
         <FieldDelimiter>string</FieldDelimiter>
         <QuoteCharacter>string</QuoteCharacter>
         <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
         <QuoteFields>string</QuoteFields>
         <RecordDelimiter>string</RecordDelimiter>
      </CSV>
   </OutputSerialization>
   <ScanRange>
      <End>long</End>
      <Start>long</Start>
   </ScanRange>
</SelectObjectContentRequest>
```

Exemple de requête SQL

Cette requête obtient le nom de l'État, les populations de 2010, les populations estimées de 2015 et le pourcentage de changement à partir des données du recensement américain. Les enregistrements du fichier qui ne sont pas des états sont ignorés.

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

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

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

Exemple d'utilisation d'AWS-CLI (CSV)

```
aws s3api select-object-content --endpoint-url https://10.224.7.44:10443
--no-verify-ssl  --bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.csv --expression-type SQL --input-serialization '{"CSV":
{"FileHeaderInfo": "USE", "Comments": "#", "QuoteEscapeCharacter": "\"",
"RecordDelimiter": "\n", "FieldDelimiter": ",", "QuoteCharacter": "\"",
"AllowQuotedRecordDelimiter": false}, "CompressionType": "NONE"}' --output
-serialization '{"CSV": {"QuoteFields": "ASNEEDED",
"QuoteEscapeCharacter": "#", "RecordDelimiter": "\n", "FieldDelimiter":
",", "QuoteCharacter": "\""}}' --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" changes.csv
```

Les premières lignes du fichier de sortie, `changes.csv` , ressemble à ceci :

```
Alabama,4779736,4854803,1.570526070895965802295356898372629785 4
Alaska,710231,738430,3.970398363349389142405780654463125377 5
Arizona,6392017,6832810,6.895992297892824753125656580700583243 1
Arkansas,2915918,2979732,2.188470320495981025529524492801237894 9
California,37253956,38904296,4.429972483996062055798852610444914897 1
Colorado,5029196,5454328,8.453279609703022113276157859029554624 6
```

Exemple d'utilisation d'AWS-CLI (Parquet)

```
aws s3api select-object-content  -endpoint-url https://10.224.7.44:10443
--bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.parquet --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" --expression-type
'SQL' --input-serialization '{"Parquet":{}}'  --output-serialization
'{"CSV": {}}' changes.csv
```

Les premières lignes du fichier de sortie, changes.csv, ressemblent à ceci :

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

Opérations pour les téléchargements en plusieurs parties

Opérations pour les téléchargements en plusieurs parties

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

Les conditions et notes suivantes s'appliquent à toutes les opérations de téléchargement en plusieurs parties :

- Vous ne devez pas dépasser 1 000 téléchargements multipartites simultanés vers un seul bucket, car les résultats des requêtes ListMultipartUploads pour ce bucket peuvent renvoyer des résultats incomplets.
- StorageGRID applique les limites de taille AWS pour les parties en plusieurs parties. Les clients S3 doivent suivre ces directives :
  - Chaque partie d'un téléchargement en plusieurs parties doit être comprise entre 5 Mio (5 242 880 octets) et 5 Gio (5 368 709 120 octets).
  - La dernière partie peut être inférieure à 5 Mio (5 242 880 octets).
  - En général, les tailles des pièces doivent être aussi grandes que possible. Par exemple, utilisez des tailles de partie de 5 Gio pour un objet de 100 Gio. Étant donné que chaque partie est considérée comme un objet unique, l'utilisation de grandes tailles de partie réduit la surcharge des métadonnées StorageGRID .
  - Pour les objets inférieurs à 5 Gio, envisagez plutôt d'utiliser un téléchargement non multipartite.
- L'ILM est évalué pour chaque partie d'un objet multipartite au fur et à mesure de son ingestion et pour l'objet dans son ensemble lorsque le téléchargement multipartite est terminé, si la règle ILM utilise l'option Équilibré ou Strict"option d'ingestion" . Vous devez être conscient de la manière dont cela affecte le placement des objets et des pièces :

    - Si l'ILM change pendant qu'un téléchargement multipartie S3 est en cours, certaines parties de l'objet peuvent ne pas répondre aux exigences ILM actuelles une fois le téléchargement multipartie terminé. Toute pièce qui n'est pas placée correctement est mise en file d'attente pour une réévaluation ILM et déplacée vers l'emplacement correct ultérieurement.
    - Lors de l'évaluation de l'ILM pour une pièce, StorageGRID filtre sur la taille de la pièce, et non sur la taille de l'objet. Cela signifie que des parties d'un objet peuvent être stockées dans des emplacements qui ne répondent pas aux exigences ILM pour l'objet dans son ensemble. Par exemple, si une règle spécifie que tous les objets de 10 Go ou plus sont stockés sur DC1 tandis que tous les objets plus petits sont stockés sur DC2, chaque partie de 1 Go d'un téléchargement multipartie en 10 parties est stockée sur DC2 lors de l'ingestion. Cependant, lorsque l'ILM est évalué pour l'objet dans son ensemble, toutes les parties de l'objet sont déplacées vers DC1.
- Toutes les opérations de téléchargement en plusieurs parties prennent en charge StorageGRID"valeurs de cohérence" .
- Lorsqu'un objet est ingéré à l'aide d'un téléchargement en plusieurs parties, le"seuil de segmentation des objets (1 Gio)" n'est pas appliqué.
- Selon vos besoins, vous pouvez utiliser"chiffrement côté serveur" avec des téléchargements en plusieurs parties. Pour utiliser SSE (chiffrement côté serveur avec clés gérées par StorageGRID), vous incluez le `x-amz-server-side-encryption` en-tête de demande dans la demande CreateMultipartUpload uniquement. Pour utiliser SSE-C (chiffrement côté serveur avec clés fournies par le client), vous spécifiez les trois mêmes en-têtes de demande de clé de chiffrement dans la demande CreateMultipartUpload et dans chaque demande UploadPart ultérieure.

Opération	Mise en œuvre
Abandonner le téléchargement en plusieurs parties	Implémenté avec tous les comportements de l'API REST Amazon S3. Sous réserve de modifications sans préavis.
Téléchargement complet en plusieurs parties	Voir"Téléchargement complet en plusieurs parties"
Créer un téléchargement multi-parties (anciennement appelé Initiate Multipart Upload)	Voir"Créer un téléchargement multi-parties"
ListeMultipartUploads	Voir"ListeMultipartUploads"
Liste des pièces	Implémenté avec tous les comportements de l'API REST Amazon S3. Sous réserve de modifications sans préavis.
Télécharger une partie	Voir"Télécharger une partie"
TéléchargerPartCopy	Voir"TéléchargerPartCopy"

Téléchargement complet en plusieurs parties

L'opération CompleteMultipartUpload termine un téléchargement en plusieurs parties d'un objet en assemblant les parties précédemment téléchargées.

StorageGRID prend en charge les valeurs non consécutives dans l'ordre croissant pour le `partNumber` paramètre de demande avec CompleteMultipartUpload. Le paramètre peut commencer par n'importe quelle valeur.

Résoudre les conflits

Les demandes client conflictuelles, telles que deux clients écrivant sur la même clé, sont résolues sur la base des « derniers gagnants ». Le moment de l'évaluation des « dernières victoires » est basé sur le moment où le système StorageGRID termine une demande donnée, et non sur le moment où les clients S3 commencent une opération.

En-têtes de requête pris en charge

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

- `x-amz-checksum-sha256`
- `x-amz-storage-class`

  Le `x-amz-storage-class` l'en-tête affecte le nombre de copies d'objets créées par StorageGRID si la règle ILM correspondante spécifie le"Option de double validation ou d'ingestion équilibrée" .

- `STANDARD`

  (Par défaut) Spécifie une opération d'ingestion à double validation lorsque la règle ILM utilise l'option Double validation ou lorsque l'option Équilibré revient à la création de copies intermédiaires.

- `REDUCED_REDUNDANCY`

  Spécifie une opération d'ingestion à validation unique lorsque la règle ILM utilise l'option de validation double ou lorsque l'option Équilibré revient à la création de copies intermédiaires.

  Si vous ingérez un objet dans un bucket avec le verrouillage d'objet S3 activé, le `REDUCED_REDUNDANCY` l'option est ignorée. Si vous ingérez un objet dans un bucket conforme hérité, le `REDUCED_REDUNDANCY` l'option renvoie une erreur. StorageGRID effectuera toujours une ingestion à double validation pour garantir que les exigences de conformité sont satisfaites.

Si un téléchargement en plusieurs parties 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 de la `ETag` valeur pour les objets en plusieurs parties.

En-têtes de requête non pris en charge

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

- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`

Gestion des versions

Cette opération termine un téléchargement en plusieurs parties. Si le contrôle de version est activé pour un bucket, la version de l'objet est créée une fois le téléchargement en plusieurs parties terminé.

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

Si le contrôle de version est suspendu, la version de l'objet est stockée avec une valeur nulle `versionId` et si une version nulle existe déjà, elle sera écrasée.

> Lorsque le contrôle de version est activé pour un bucket, l'exécution d'un téléchargement en plusieurs parties crée toujours une nouvelle version, même s'il existe des téléchargements en plusieurs parties simultanés effectués sur la même clé d'objet. Lorsque le contrôle de version n'est pas activé pour un bucket, il est possible de lancer un téléchargement en plusieurs parties, puis de lancer et de terminer un autre téléchargement en plusieurs parties sur la même clé d'objet. Sur les buckets non versionnés, le téléchargement en plusieurs parties qui se termine en dernier est prioritaire.

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

Si le bucket dans lequel le téléchargement en plusieurs parties se produit est configuré pour un service de plateforme, le téléchargement en plusieurs parties réussit même si l'action de réplication ou de notification associée échoue.

Un locataire peut déclencher la réplication ou la notification ayant échoué en mettant à jour les métadonnées ou les balises de l'objet. Un locataire peut soumettre à nouveau les valeurs existantes pour éviter d'apporter des modifications indésirables.

"Dépanner les services de la plateforme" .

Créer un téléchargement multi-parties

L'opération CreateMultipartUpload (précédemment nommée Initiate Multipart Upload) lance un téléchargement en plusieurs parties pour un objet et renvoie un ID de téléchargement.

Le `x-amz-storage-class` l'en-tête de requête est pris en charge. La valeur soumise pour `x-amz-storage-class` affecte la manière dont StorageGRID protège les données de l'objet pendant l'ingestion et non le nombre de copies persistantes de l'objet stockées dans le système StorageGRID (qui est déterminé par ILM).

Si la règle ILM correspondant à un objet ingéré utilise le Strict"option d'ingestion" , le `x-amz-storage-class` l'en-tête n'a aucun effet.

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

- `STANDARD`(Défaut)
  - **Double validation** : si la règle ILM spécifie l'option d'ingestion Double validation, dès qu'un objet est ingéré, une deuxième copie de cet objet est créée et distribuée à un autre nœud de stockage (double validation). Lorsque l'ILM est évalué, StorageGRID détermine si ces copies intermédiaires initiales

satisfont aux instructions de placement de la règle. Si ce n'est pas le cas, de nouvelles copies d'objets devront peut-être être réalisées à des emplacements différents et les copies intermédiaires initiales devront peut-être être supprimées.

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

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

- `REDUCED_REDUNDANCY`

  - **Double validation** : si la règle ILM spécifie l'option Double validation, StorageGRID crée une seule copie intermédiaire lorsque l'objet est ingéré (validation unique).
  - **Équilibré** : si la règle ILM spécifie l'option Équilibré, StorageGRID effectue une seule copie intermédiaire uniquement si le système ne peut pas effectuer immédiatement 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 mieux utilisée lorsque la règle ILM qui correspond à l'objet crée une seule copie répliquée. Dans ce cas, en utilisant `REDUCED_REDUNDANCY` élimine la création et la suppression inutiles d'une copie d'objet supplémentaire pour chaque opération d'ingestion.

  En utilisant le `REDUCED_REDUNDANCY` Cette option n'est pas recommandée dans d'autres circonstances. `REDUCED_REDUNDANCY` augmente le risque de perte de données d'objet lors de l'ingestion. Par exemple, vous risquez de perdre des données si la copie unique est initialement stockée sur un nœud de stockage qui échoue avant que l'évaluation ILM puisse avoir lieu.

> Le fait de n'avoir qu'une seule copie répliquée pendant une période donnée expose les données à un risque de perte permanente. Si une seule copie répliquée d'un objet existe, cet objet est perdu si un nœud de stockage échoue ou présente une erreur importante. Vous perdez également temporairement l'accès à l'objet pendant les procédures de maintenance telles que les mises à niveau.

Spécification `REDUCED_REDUNDANCY` affecte uniquement le nombre de copies créées lorsqu'un objet est ingéré pour la première fois. Cela n'affecte pas le nombre de copies de l'objet effectuées lorsque l'objet est évalué par les stratégies ILM actives et n'entraîne pas le stockage des données à des niveaux de redondance inférieurs dans le système StorageGRID .

> Si vous ingérez un objet dans un bucket avec le verrouillage d'objet S3 activé, le `REDUCED_REDUNDANCY` l'option est ignorée. Si vous ingérez un objet dans un bucket conforme hérité, le `REDUCED_REDUNDANCY` l'option renvoie une erreur. StorageGRID effectuera toujours une ingestion à double validation pour garantir que les exigences de conformité sont satisfaites.

En-têtes de requête pris en charge

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

- `Content-Type`
- `x-amz-checksum-algorithm`

  Actuellement, seule la valeur SHA256 pour `x-amz-checksum-algorithm` est pris en charge.

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

  Lors de la spécification de la paire nom-valeur pour les métadonnées définies par l'utilisateur, utilisez ce format général :

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

  Si vous souhaitez utiliser l'option **Heure de création définie par l'utilisateur** comme heure de référence pour une règle ILM, vous devez utiliser `creation-time` comme le nom des métadonnées qui enregistrent quand l'objet a été créé. Par exemple:

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

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

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

- En-têtes de demande de verrouillage d'objet S3 :

  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

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

  "Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3"

- En-têtes de requête SSE :

  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

    En-têtes de requête pour le chiffrement côté serveur

  > Pour plus d'informations sur la façon dont StorageGRID gère les caractères UTF-8, consultez"Mettre l'objet" .

En-têtes de requête pour le chiffrement côté serveur

Vous pouvez utiliser les en-têtes de requête suivants pour chiffrer un objet en plusieurs parties avec un chiffrement côté serveur. Les options SSE et SSE-C s'excluent mutuellement.

- **SSE** : utilisez l'en-tête suivant dans la demande CreateMultipartUpload si vous souhaitez chiffrer l'objet avec une clé unique gérée par StorageGRID. Ne spécifiez pas cet en-tête dans aucune des requêtes UploadPart.
  - `x-amz-server-side-encryption`
- **SSE-C** : utilisez ces trois en-têtes dans la demande CreateMultipartUpload (et dans chaque demande UploadPart ultérieure) si vous souhaitez crypter l'objet avec une clé unique que vous fournissez et gérez.
  - `x-amz-server-side-encryption-customer-algorithm`: Préciser `AES256` .
  - `x-amz-server-side-encryption-customer-key`:Spécifiez votre clé de chiffrement pour le nouvel objet.
  - `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le condensé MD5 de la clé de chiffrement du nouvel objet.

> Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant. Avant d'utiliser les clés fournies par le client pour sécuriser les données d'objet, examinez les considérations relatives"en utilisant le cryptage côté serveur" .

En-têtes de requête non pris en charge

L'en-tête de requête suivant n'est pas pris en charge :

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

  Le `x-amz-website-redirect-location` retours d'en-tête `XNotImplemented` .

Gestion des versions

Le téléchargement en plusieurs parties consiste en des opérations distinctes pour lancer le téléchargement, répertorier les téléchargements, télécharger des parties, assembler les parties téléchargées et terminer le téléchargement. Les objets sont créés (et versionnés si applicable) lorsque l'opération CompleteMultipartUpload est effectuée.

ListeMultipartUploads

L'opération ListMultipartUploads répertorie les téléchargements multipartites en cours pour un bucket.

Les paramètres de requête suivants sont pris en charge :

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

- `Authorization`

Gestion des versions

Le téléchargement en plusieurs parties consiste en des opérations distinctes pour lancer le téléchargement, répertorier les téléchargements, télécharger des parties, assembler les parties téléchargées et terminer le téléchargement. Les objets sont créés (et versionnés si applicable) lorsque l'opération CompleteMultipartUpload est effectuée.

Télécharger une partie

L'opération UploadPart télécharge une partie dans un téléchargement en plusieurs parties pour un objet.

En-têtes de requête pris en charge

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

- `x-amz-checksum-sha256`
- `Content-Length`
- `Content-MD5`

En-têtes de requête pour le chiffrement côté serveur

Si vous avez spécifié le chiffrement SSE-C pour la demande CreateMultipartUpload, vous devez également inclure les en-têtes de demande suivants dans chaque demande UploadPart :

- `x-amz-server-side-encryption-customer-algorithm`: Préciser `AES256` .
- `x-amz-server-side-encryption-customer-key`:Spécifiez la même clé de chiffrement que celle que vous avez fournie dans la demande CreateMultipartUpload.
- `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le même condensé MD5 que celui que vous avez fourni dans la demande CreateMultipartUpload.

> Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant. Avant d'utiliser les clés fournies par le client pour sécuriser les données d'objet, examinez les considérations dans"Utiliser le cryptage côté serveur" .

Si vous avez spécifié une somme de contrôle SHA-256 lors de la demande CreateMultipartUpload, vous devez également inclure l'en-tête de demande suivant dans chaque demande UploadPart :

- `x-amz-checksum-sha256`:Spécifiez la somme de contrôle SHA-256 pour cette partie.

En-têtes de requête non pris en charge

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

- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`

Gestion des versions

Le téléchargement en plusieurs parties consiste en des opérations distinctes pour lancer le téléchargement, répertorier les téléchargements, télécharger des parties, assembler les parties téléchargées et terminer le téléchargement. Les objets sont créés (et versionnés si applicable) lorsque l'opération CompleteMultipartUpload est effectuée.

TéléchargerPartCopy

L'opération UploadPartCopy télécharge une partie d'un objet en copiant les données d'un objet existant comme source de données.

L'opération UploadPartCopy est implémentée avec tout le comportement de l'API REST Amazon S3. Sous réserve de modifications sans préavis.

Cette requête lit et écrit les données d'objet spécifiées dans `x-amz-copy-source-range` au sein du système StorageGRID .

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

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

En-têtes de requête pour le chiffrement côté serveur

Si vous avez spécifié le chiffrement SSE-C pour la demande CreateMultipartUpload, vous devez également inclure les en-têtes de demande suivants dans chaque demande UploadPartCopy :

- `x-amz-server-side-encryption-customer-algorithm`: Préciser `AES256` .
- `x-amz-server-side-encryption-customer-key`:Spécifiez la même clé de chiffrement que celle que vous avez fournie dans la demande CreateMultipartUpload.
- `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le même condensé MD5 que celui que vous avez fourni dans la demande CreateMultipartUpload.

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

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

> Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant. Avant d'utiliser les clés fournies par le client pour sécuriser les données d'objet, examinez les considérations dans"Utiliser le cryptage côté serveur" .

Gestion des versions

Le téléchargement en plusieurs parties consiste en des opérations distinctes pour lancer le téléchargement, répertorier les téléchargements, télécharger des parties, assembler les parties téléchargées et terminer le téléchargement. Les objets sont créés (et versionnés si applicable) lorsque l'opération CompleteMultipartUpload est effectuée.

Réponses d'erreur

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

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

Nom	Statut HTTP
Accès refusé	403 Interdit
BadDigest	400 Mauvaise requête
BucketExisteDéjà	409 Conflit
Seau non vide	409 Conflit
Corps incomplet	400 Mauvaise requête
Erreur interne	Erreur interne du serveur 500
ID de clé d'accès non valide	403 Interdit
Argument invalide	400 Mauvaise requête
Nom de bucket invalide	400 Mauvaise requête
État du bucket invalide	409 Conflit
InvalidDigest	400 Mauvaise requête
Erreur d'algorithme de chiffrement invalide	400 Mauvaise requête
Partie invalide	400 Mauvaise requête
Commande de pièces invalide	400 Mauvaise requête
Plage invalide	416 Plage demandée non satisfaisante

Nom	Statut HTTP
Demande invalide	400 Mauvaise requête
Classe de stockage invalide	400 Mauvaise requête
Balise invalide	400 Mauvaise requête
URI invalide	400 Mauvaise requête
Clé trop longue	400 Mauvaise requête
XML malformé	400 Mauvaise requête
Métadonnées trop volumineuses	400 Mauvaise requête
Méthode non autorisée	Méthode 405 non autorisée
Longueur du contenu manquant	411 Longueur requise
Erreur de corps de demande manquante	400 Mauvaise requête
En-tête de sécurité manquant	400 Mauvaise requête
Aucun seau de ce type	404 non trouvé
Aucune clé de ce type	404 non trouvé
Aucun téléchargement de ce type	404 non trouvé
Non implémenté	501 non implémenté
Politique NoSuchBucket	404 non trouvé
Erreur de configuration de verrouillage d’objet non trouvée	404 non trouvé
Précondition échouée	412 Échec de la condition préalable
RequestTimeTooSkewed	403 Interdit
Service non disponible	Service 503 indisponible
La signature ne correspond pas	403 Interdit

Nom	Statut HTTP
Trop de seaux	400 Mauvaise requête
La clé utilisateur doit être spécifiée	400 Mauvaise requête

Codes d’erreur personnalisés StorageGRID

Nom	Description	Statut HTTP
XBucketLifecycleNon autorisé	La configuration du cycle de vie du bucket n’est pas autorisée dans un bucket conforme hérité	400 Mauvaise requête
Exception d’analyse de politique XBucket	Échec de l’analyse de la politique de bucket JSON reçue.	400 Mauvaise requête
Conflit de conformité X	Opération refusée en raison de paramètres de conformité hérités.	403 Interdit
XComplianceRéduitRedondanceInterdit	La redondance réduite n’est pas autorisée dans le bucket conforme hérité	400 Mauvaise requête
XMaxBucketPolicyLengthDépassé	Votre politique dépasse la durée maximale autorisée pour la politique de compartiment.	400 Mauvaise requête
En-tête de demande interne XMissing	Il manque un en-tête d’une requête interne.	400 Mauvaise requête
XNoSuchBucketCompliance	La conformité héritée n’est pas activée pour le bucket spécifié.	404 non trouvé
XNonAcceptable	La demande contient un ou plusieurs en-têtes d’acceptation qui n’ont pas pu être satisfaits.	406 Non acceptable
XNonImplémenté	La demande que vous avez fournie implique une fonctionnalité qui n’est pas implémentée.	501 non implémenté