



Prise en charge de l'API REST Amazon S3

StorageGRID software

NetApp
February 12, 2026

Sommaire

Prise en charge de l'API REST Amazon S3	1
Détails de l'implémentation de l'API REST S3	1
Traitement de la date	1
En-têtes de demande commune	1
En-têtes de réponse commune	1
Authentifier les demandes	2
Utilisez l'en-tête HTTP Authorization	2
Utiliser les paramètres de requête	2
Opérations sur le service	2
Opérations sur les compartiments	3
Opérations sur les objets	11
Opérations sur les objets	11
Utiliser S3 Select	16
Utilisez le cryptage côté serveur	18
Objet de copie	20
GetObject	24
Objet principal	26
PutObject	29
Objet de restauration	35
SelectObjectContent	36
Opérations pour les téléchargements partitionnés	40
Opérations pour les téléchargements partitionnés	40
CompleteMultipartUpload	41
CreateMultipartUpload	43
ListMultipartUploads	46
UploadPart	47
UploadPartCopy	48
Réponses d'erreur	49
Codes d'erreur de l'API S3 pris en charge	49
Codes d'erreur personnalisés StorageGRID	51

Prise en charge de l'API REST Amazon S3

Détails de l'implémentation de l'API REST S3

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

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

Traitement de la date

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

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

En-têtes de demande commune

Le système StorageGRID prend en charge les en-têtes de requête communs définis par "[Référence de l'API Amazon simple Storage Service : en-têtes de demande communs](#)", à une exception près.

En-tête de demande	Mise en place
Autorisation	<p>Prise en charge complète de la signature AWS version 2</p> <p>Prise en charge de la signature AWS version 4, à l'exception des cas suivants :</p> <ul style="list-style-type: none">Lorsque vous fournissez la valeur de somme de contrôle de charge utile réelle dans x-amz-content-sha256, la valeur est acceptée sans validation, comme si la valeur UNSIGNED-PAYLOAD avait été fournie pour l'en-tête. Lorsque vous fournissez une x-amz-content-sha256 valeur d'en-tête qui implique le aws-chunked STREAMING (par exemple, STREAMING-AWS4-HMAC-SHA256-PAYLOAD), les signatures des blocs ne sont pas vérifiées par rapport aux données des blocs.

En-têtes de réponse commune

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

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

Authentifier les demandes

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

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

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

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

Utilisez l'en-tête HTTP Authorization

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

Utiliser les paramètres de requête

Vous pouvez utiliser les paramètres de requête pour ajouter des informations d'authentification à une URL. Il s'agit de la présignature de l'URL, qui peut être utilisée pour accorder un accès temporaire à des ressources spécifiques. Les utilisateurs avec 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 limité tiers à une ressource.

Opérations sur le service

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

Fonctionnement	Mise en place
Listseaux (Anciennement appelé GET Service)	Mise en œuvre avec tout le comportement de l'API REST Amazon S3. D'être modifiées sans préavis.
DÉCOUVREZ l'utilisation du stockage	La demande StorageGRID " DÉCOUVREZ l'utilisation du stockage " 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 d'accès de / et un paramètre de requête personnalisée (?x-ntap-sg-usage) ajouté.

Fonctionnement	Mise en place
OPTIONS /	Les applications client peuvent émettre OPTIONS / des requêtes vers le port S3 d'un nœud de stockage, sans identifiants d'authentification S3, pour déterminer si le nœud de stockage est disponible. Vous pouvez utiliser cette requête pour la surveillance ou permettre aux équilibreurs de charge externes d'identifier lorsqu'un nœud de stockage est arrêté.

Opérations sur les compartiments

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

Chaque grille peut contenir un maximum de 100,000 compartiments.

Pour prendre en charge 5,000 compartiments, chaque nœud de stockage de la grille doit disposer d'au moins 64 Go de RAM.

Les restrictions relatives aux noms de compartiment respectent les restrictions régionales standard AWS, mais vous devez les restreindre à une nomenclature DNS pour prendre en charge les demandes de type hébergement virtuel S3.

Pour plus d'informations, reportez-vous aux sections suivantes :

- "[Guide de l'utilisateur d'Amazon simple Storage Service : quotas de compartiments, restrictions et limites](#)"
- "[Configuration des noms de domaine de terminaux 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 les compartiments individuels. Voir "[HEURE du dernier accès au compartiment](#)".

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

Fonctionnement	Mise en place
CreateBucket	<p>Crée un nouveau compartiment. C'est en créant le compartiment que vous devenez le propriétaire.</p> <ul style="list-style-type: none"> Les noms de compartiment doivent être conformes aux règles suivantes : <ul style="list-style-type: none"> Il doit être unique sur chaque système StorageGRID (et pas seulement au sein du compte du locataire). Doit être conforme DNS. Doit contenir au moins 3 et 63 caractères. Peut être une série d'une ou plusieurs étiquettes, avec des étiquettes adjacentes séparées par un point. Chaque étiquette doit commencer et se terminer par une lettre ou un chiffre en minuscules et ne peut utiliser que des lettres minuscules, des chiffres et des tirets. Ne doit pas ressembler à une adresse IP au format texte. Ne doit pas utiliser de périodes dans des demandes de type hébergement virtuel. Les périodes provoquera des problèmes avec la vérification du certificat générique du serveur. Par défaut, les compartiments sont créés dans la <code>us-east-1</code> région ; vous pouvez cependant utiliser <code>LocationConstraint</code> l'élément de demande du corps de la demande pour spécifier une région différente. Lorsque vous utilisez l' `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 région que vous devez utiliser. <p>Remarque : une erreur se produit si votre requête CreateBucket utilise une région qui n'a pas été définie dans StorageGRID.</p> <ul style="list-style-type: none"> Vous pouvez inclure l' `x-amz-bucket-object-lock-enabled` en-tête de demande pour créer un compartiment lorsque le verrouillage objet S3 est activé. Voir "Utilisez l'API REST S3 pour configurer le verrouillage objet S3". <p>Vous devez activer le verrouillage d'objet S3 lors de la création du compartiment. Une fois un compartiment créé, vous ne pouvez ni ajouter ni désactiver le verrouillage objet S3. Le verrouillage objet S3 requiert la gestion des versions de compartiment, qui est activée automatiquement lors de la création du compartiment.</p>
DeleteBucket	Supprime le godet.
DeleteBucketCors	Supprime la configuration CORS pour le godet.
DeleteBucketEncryption	Supprime le chiffrement par défaut du compartiment. Les objets chiffrés existants restent chiffrés, mais aucun nouvel objet ajouté au compartiment n'est chiffré.
DeleteBucketLifecycle	Supprime la configuration du cycle de vie du compartiment. Voir " Création de la configuration du cycle de vie S3 ".

Fonctionnement	Mise en place
DeleteBucketPolicy	Supprime la règle associée au compartiment.
DeleteBucketReplication	Supprime la configuration de réPLICATION attachée au compartiment.
DeleteBucketTagging	Utilise la <code>tagging</code> sous-ressource pour supprimer toutes les balises d'un compartiment. Attention : si une balise de stratégie ILM non définie par défaut est définie pour ce compartiment, une balise de compartiment sera affectée à cette <code>NTAP-SG-ILM-BUCKET-TAG</code> variable. N'émettez pas de demande <code>DeleteBucketTagging</code> s'il existe une <code>NTAP-SG-ILM-BUCKET-TAG</code> balise de compartiment. À la place, lancez une demande <code>PutBucketTagging</code> avec uniquement la <code>NTAP-SG-ILM-BUCKET-TAG</code> balise et sa valeur attribuée pour supprimer toutes les autres balises du compartiment. Ne pas modifier ou retirer l' <code>'NTAP-SG-ILM-BUCKET-TAG'</code> étiquette de godet.
GetBucketAcl	Renvoie une réponse positive et l'ID, DisplayName et l'autorisation du propriétaire du compartiment, indiquant que le propriétaire a un accès complet au compartiment.
GetBucketCors	Renvoie la <code>cors</code> configuration du compartiment.
GetBucketEncryption	Renvoie la configuration de chiffrement par défaut du compartiment.
GetBucketLifecycleConfiguration (Anciennement appelé cycle de vie du compartiment GET)	Renvoie la configuration du cycle de vie du compartiment. Voir " Création de la configuration du cycle de vie S3 ".
GetBucketLocation	Renvoie la région définie à l'aide de l' <code>LocationConstraint</code> élément dans la requête <code>CreateBucket</code> . Si la région du compartiment est, une chaîne vide est <code>'us-east-1'</code> renvoyée pour la région.
GetBucketNotificationConfiguration (Anciennement appelée notification GET Bucket)	Renvoie la configuration de notification associée au compartiment.
GetBucketPolicy	Renvoie la politique attachée au compartiment.
GetBucketReplication	Renvoie la configuration de réPLICATION attachée au compartiment.

Fonctionnement	Mise en place
GetBucketTagging	<p>Utilise la <code>tagging sous-ressource</code> pour renvoyer toutes les balises d'un compartiment.</p> <p>Attention : si une balise de stratégie ILM non définie par défaut est définie pour ce compartiment, une balise de compartiment sera affectée à cette <code>NTAP-SG-ILM-BUCKET-TAG</code> variable. Ne modifiez pas et ne supprimez pas cette balise.</p>
GetBucketVersioning	<p>Cette implémentation utilise la <code>versioning sous-ressource</code> pour renvoyer l'état de gestion des versions d'un compartiment.</p> <ul style="list-style-type: none"> • <i>Blank</i>: La gestion des versions n'a jamais été activée (le compartiment est « non versionné ») • Activé : la gestion des versions est activée • Suspendu : la gestion des versions a déjà été activée et est suspendue
GetObjectLockConfiguration	<p>Renvoie le mode de conservation par défaut du compartiment et la période de conservation par défaut, si elle est configurée.</p> <p>Voir "Utilisez l'API REST S3 pour configurer le verrouillage objet S3".</p>
Godet principal	<p>Détermine si un compartiment existe et que vous êtes autorisé à y accéder.</p> <p>Cette opération renvoie :</p> <ul style="list-style-type: none"> • <code>x-ntap-sg-bucket-id</code>: UUID du compartiment au format UUID. • <code>x-ntap-sg-trace-id</code>: ID de trace unique de la demande associée.

Fonctionnement	Mise en place
ListObjects et ListObjectsV2 (Anciennement appelé « GET Bucket »)	<p>Renvoie une partie ou la totalité (jusqu'à 1,000) des objets dans un compartiment. La classe de stockage des objets peut avoir l'une des deux valeurs, même si l'objet a été ingéré avec l' `REDUCED_REDUNDANCY` option de classe de stockage :</p> <ul style="list-style-type: none"> • STANDARD, Qui indique que l'objet est stocké dans un pool de stockage composé de nœuds de stockage. • GLACIER, Qui indique que l'objet a été déplacé vers le compartiment externe spécifié par le pool de stockage cloud. <p>Si le compartiment contient un grand nombre de clés supprimées dont le préfixe est identique, certains ne contiennent pas de CommonPrefixes clés.</p> <p>Pour les requêtes HeadObject et ListObject, StorageGRID renvoie les horodatages LastModified avec une précision différente tandis qu'AWS renvoie les horodatages avec la même précision, comme illustré dans les exemples suivants :</p> <ul style="list-style-type: none"> • Objet principal StorageGRID : « LastModified » : « 2024-09-26T16:43:24+00:00 » • Objet de liste StorageGRID : « LastModified » : « 2024-09-26T16:43:24.931000+00:00 » • AWS HeadObject : « LastModified » : « 2023-10-17T00:19:54+00:00 » • AWS ListObject : « LastModified » : « 2023-10-17T00:19:54+00:00 »
ListObjectVersions (Anciennement nommé OBTENIR les versions de l'objet compartiment)	Avec l'accès EN LECTURE sur un compartiment, cette opération associée à la versions sous-ressource liste les métadonnées de toutes les versions des objets du compartiment.
PutBucketCors	Définit la configuration CORS pour un compartiment de sorte que le compartiment puisse traiter les demandes d'origine croisée. Le partage de ressources d'origine croisée (CORS) est un mécanisme de sécurité qui permet aux applications Web clientes d'un domaine d'accéder aux ressources d'un domaine différent. Supposons, par exemple, que vous utilisez un compartiment S3 nommé images pour stocker des graphiques. En définissant la configuration CORS pour le images compartiment, vous pouvez autoriser l'affichage des images de ce compartiment sur le site Web http://www.example.com .

Fonctionnement	Mise en place
PutBucketEncryption	<p>Définit l'état de chiffrement par défaut d'un compartiment existant. Lorsque le chiffrement au niveau du compartiment est activé, tout nouvel objet ajouté au compartiment est chiffré. StorageGRID prend en charge le chiffrement côté serveur avec des clés gérées par StorageGRID. Lorsque vous spécifiez la règle de configuration du chiffrement côté serveur, définissez le SSEAlgorithm paramètre sur AES256 et n'utilisez pas le KMSMasterKeyID paramètre.</p> <p>La configuration de chiffrement par défaut du compartiment est ignorée si la demande de téléchargement d'objet spécifie déjà le chiffrement (c'est-à-dire si la demande inclut l' `x-amz-server-side-encryption-*` en-tête de la requête).</p>
PutBucketLifecycleConfiguration (Anciennement appelé cycle de vie du compartiment PUT)	<p>Crée une nouvelle configuration de cycle de vie pour le compartiment ou remplace une configuration de cycle de vie existante. StorageGRID prend en charge jusqu'à 1,000 règles de cycle de vie dans une configuration cycle de vie. Chaque règle peut inclure les éléments XML suivants :</p> <ul style="list-style-type: none"> • Expiration (jours, Date, ExpiredObjectDeleteMarker) • NoncurrentVersionExpiation (NewerNoncurrentVersions, NoncurrentDays) • Filtre (préfixe, étiquette) • État • ID <p>StorageGRID ne prend pas en charge les actions suivantes :</p> <ul style="list-style-type: none"> • AbortIncompleteMultipartUpload • Transition <p>Voir "Création de la configuration du cycle de vie S3". Pour comprendre comment l'action expiration d'un cycle de vie de compartiment interagit avec les instructions de placement ILM, reportez-vous à la section "Fonctionnement de ILM tout au long de la vie d'un objet".</p> <p>Remarque : la configuration du cycle de vie des compartiments peut être utilisée avec des compartiments avec le verrouillage d'objet S3 activé, mais la configuration du cycle de vie des compartiments n'est pas prise en charge pour les compartiments conformes hérités.</p>

Fonctionnement	Mise en place
PutBucketNotificationConfiguration (Anciennement appelée notification PUT Bucket)	<p>Configure les notifications pour le compartiment à l'aide du fichier XML de configuration de notification inclus dans le corps de la demande. Vous devez connaître les détails d'implémentation suivants :</p> <ul style="list-style-type: none"> StorageGRID prend en charge les rubriques Amazon Simple Notification Service (Amazon SNS), les rubriques Kafka ou les points de terminaison webhook comme destinations. Les points de terminaison Simple Queue Service (SQS) ou AWS Lambda ne sont pas pris en charge. La destination des notifications doit être spécifiée comme URN d'un terminal StorageGRID. Les terminaux peuvent être créés à l'aide du Gestionnaire de locataires ou de l'API de gestion des locataires. <p>Le noeud final doit exister pour que la configuration des notifications réussisse. Si le noeud final n'existe pas, une 400 Bad Request erreur est renvoyée avec le code InvalidArgument.</p> <ul style="list-style-type: none"> Vous ne pouvez pas configurer de notification pour les types d'événements suivants. Ces types d'événements sont non pris en charge. <ul style="list-style-type: none"> ◦ s3:ReducedRedundancyLostObject ◦ s3:ObjectRestore:Completed Les notifications d'événements envoyées par StorageGRID utilisent le format JSON standard, sauf qu'elles n'incluent pas certaines clés et utilisent des valeurs spécifiques pour d'autres, comme illustré dans la liste suivante : <ul style="list-style-type: none"> ◦ EventSource ◦ sgws:s3 ◦ AwsRegion ◦ non inclus ◦ x-amz-id-2 ◦ non inclus ◦ arn ◦ urn:sgws:s3:::bucket_name
PutBuckePolicy	Définit la politique attachée au bucket. Voir " Utilisez les règles d'accès au compartiment et au groupe " .

Fonctionnement	Mise en place
PutBucketReplication	<p>Configure "RéPLICATION StorageGRID CloudMirror" pour le compartiment à l'aide du fichier XML de configuration de réPLICATION fourni dans le corps de la demande. Pour la réPLICATION CloudMirror, vous devez connaître les détails d'implémentation suivants :</p> <ul style="list-style-type: none"> • StorageGRID ne prend en charge que le V1 de la configuration de la réPLICATION. Cela signifie que StorageGRID ne prend pas en charge l'utilisation de Filter l'élément pour les règles et respecte 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 des compartiments peut être configurée sur les compartiments avec ou sans version. • Vous pouvez spécifier un compartiment de destination différent dans chaque règle du XML de configuration de réPLICATION. Un compartiment source peut être répliqué sur plusieurs compartiments de destination. • Les compartiments de destination doivent être spécifiés en tant que URN des terminaux StorageGRID, tel que spécifié dans le Gestionnaire de locataires ou l'API de gestion des locataires. Voir "Configurez la réPLICATION CloudMirror". <p>Le noeud final doit exister pour que la configuration de réPLICATION réussisse. Si le noeud final n'existe pas, la demande échoue en tant que 400 Bad Request . le message d'erreur indique : <i>Unable to save the replication policy. The specified endpoint URN does not exist: URN.</i></p> <ul style="list-style-type: none"> • Vous n'avez pas besoin de spécifier un Role dans le XML de configuration. Cette valeur n'est pas utilisée par StorageGRID et sera ignorée si elle a été soumise. • Si vous omettez la classe de stockage du XML de configuration, StorageGRID utilise la STANDARD classe de stockage par défaut. • Si vous supprimez un objet du compartiment source ou que vous supprimez le compartiment source lui-même, le comportement de réPLICATION inter-région est le suivant : <ul style="list-style-type: none"> ◦ Si vous supprimez l'objet ou le compartiment avant sa réPLICATION, l'objet/le compartiment n'est pas réplié et vous n'êtes pas averti. ◦ Si vous supprimez l'objet ou le compartiment après sa réPLICATION, StorageGRID suit le comportement de suppression Amazon S3 standard pour la version V1 de la réPLICATION multi-région.

Fonctionnement	Mise en place
Étiquetage PutBucketTagging	<p>Utilise la tagging sous-ressource pour ajouter ou mettre à jour un ensemble de balises pour un compartiment. Lors de l'ajout de balises de compartiment, tenez compte des limites suivantes :</p> <ul style="list-style-type: none"> StorageGRID et Amazon S3 prennent en charge jusqu'à 50 balises pour chaque compartiment. Les étiquettes associées à un compartiment doivent avoir des clés d'étiquette uniques. Une clé de balise peut comporter jusqu'à 128 caractères Unicode. Les valeurs de balise peuvent comporter jusqu'à 256 caractères Unicode. Les clés et les valeurs sont sensibles à la casse <p>Attention : si une balise de stratégie ILM non définie par défaut est définie pour ce compartiment, une balise de compartiment sera affectée à cette NTAP-SG-ILM-BUCKET-TAG variable. Assurez-vous que la NTAP-SG-ILM-BUCKET-TAG balise de compartiment est incluse avec la valeur attribuée dans toutes les demandes PutBucketTagging. Ne modifiez pas et ne supprimez pas cette balise.</p> <p>Remarque : cette opération écrasera les balises actuelles du compartiment. Si des balises existantes sont omises de l'ensemble, ces balises seront supprimées pour le compartiment.</p>
PutBuckeVersioning	<p>Utilise la versioning sous-ressource pour définir l'état de gestion des versions d'un compartiment existant. Vous pouvez définir l'état de la gestion des versions à l'aide de l'une des valeurs suivantes :</p> <ul style="list-style-type: none"> Activé : permet la gestion des versions des objets dans le compartiment. Tous les objets ajoutés au compartiment reçoivent un ID de version unique. Suspendu : désactive la gestion des versions des objets dans le compartiment. Tous les objets ajoutés au compartiment reçoivent l'ID de version null .
PutObjectLockConfigurati on	<p>Configure ou supprime le mode de conservation par défaut du compartiment et la période de conservation par défaut.</p> <p>Si la période de conservation par défaut est modifiée, la conservation jusqu'à la date des versions d'objet existantes reste la même et n'est pas recalculée en utilisant la nouvelle période de conservation par défaut.</p> <p>Voir "Utilisez l'API REST S3 pour configurer le verrouillage objet S3" pour plus d'informations.</p>

Opérations sur les objets

Opérations sur les objets

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

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

- StorageGRID "valeurs de cohérence" sont pris en charge par toutes les opérations sur les objets, à l'exception des suivantes :
 - GetObjectAcl
 - OPTIONS /
 - PutObjectLegalHold
 - PutObjectRetention
 - SelectObjectContent
- Les demandes contradictoires des clients, telles que deux clients qui écrivent sur la même clé, sont résolues sur une base de « derniers-victoires ». La chronologie de l'évaluation « derniers-victoires » repose sur la date à laquelle le système StorageGRID termine une demande donnée et non sur la date à laquelle les clients S3 commencent une opération.
- Tous les objets d'un compartiment StorageGRID sont détenus par le propriétaire du compartiment, y compris les objets créés par un utilisateur anonyme ou par un autre compte.

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

Fonctionnement	Mise en place
DeleteObject	<p>L'authentification multifacteur (MFA) et l'en-tête de réponse <code>x-amz-mfa</code> ne sont pas pris en charge.</p> <p>Lors du traitement d'une requête 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 et indique que le client a réussi.</p> <p>Gestion des versions</p> <p>Pour supprimer une version spécifique, le demandeur doit être le propriétaire du compartiment et utiliser la <code>versionId</code> sous-ressource. L'utilisation de cette sous-ressource supprime définitivement la version. Si le <code>versionId</code> correspond à un marqueur de suppression, l'en-tête de réponse <code>x-amz-delete-marker</code> est renvoyé à <code>true</code>.</p> <ul style="list-style-type: none"> • Si un objet est supprimé sans la <code>versionId</code> sous-ressource sur un compartiment avec la gestion des versions activée, il génère un marqueur de suppression. Le <code>versionId</code> pour le marqueur de suppression est renvoyé à l'aide de <code>x-amz-version-id</code> l'en-tête de réponse et l'<code>x-amz-delete-marker</code> en-tête de réponse est renvoyé à <code>true</code>. • Si un objet est supprimé sans la <code>versionId</code> sous-ressource sur un compartiment avec la gestion des versions suspendue, il entraîne la suppression permanente d'une version 'null' existante ou d'un marqueur de suppression 'null', et la génération d'un nouveau marqueur de suppression 'null'. L'<code>x-amz-delete-marker</code> en-tête de réponse est renvoyé à <code>true</code>. <p>Remarque : dans certains cas, plusieurs marqueurs de suppression peuvent exister pour un objet.</p> <p>Reportez-vous à la section "Utilisez l'API REST S3 pour configurer le verrouillage objet S3" pour savoir comment supprimer des versions d'objets en mode GOUVERNANCE.</p>
DeleteObjects (Précédemment nommé, SUPPRIMER plusieurs objets)	<p>L'authentification multifacteur (MFA) et l'en-tête de réponse <code>x-amz-mfa</code> ne sont pas pris en charge.</p> <p>Plusieurs objets peuvent être supprimés dans le même message de demande.</p> <p>Reportez-vous à la section "Utilisez l'API REST S3 pour configurer le verrouillage objet S3" pour savoir comment supprimer des versions d'objets en mode GOUVERNANCE.</p>

Fonctionnement	Mise en place
DeleteObjectTagging	<p>Utilise la tagging sous-ressource pour supprimer toutes les balises d'un objet.</p> <p>Gestion des versions</p> <p>Si le <code>versionId</code> paramètre de requête n'est pas spécifié dans la requête, l'opération supprime toutes les balises de la version la plus récente de l'objet dans un compartiment versionné. Si la version actuelle de l'objet est un marqueur de suppression, l'état "MethodNotAllowed" est renvoyé avec l'<code>x-amz-delete-marker</code> en-tête de réponse défini sur <code>true</code>.</p>
GetObject	" GetObject "
GetObjectAcl	Si les informations d'identification d'accès nécessaires sont fournies pour le compte, l'opération renvoie une réponse positive ainsi que l'ID, le DisplayName et l'autorisation du propriétaire de l'objet, ce qui indique que le propriétaire dispose d'un accès complet à l'objet.
GetObjectLegalHold	" Utilisez l'API REST S3 pour configurer le verrouillage objet S3 "
GetObjectRetention	" Utilisez l'API REST S3 pour configurer le verrouillage objet S3 "
GetObjectTagging	<p>Utilise la tagging sous-ressource pour renvoyer toutes les balises d'un objet.</p> <p>Gestion des versions</p> <p>Si le <code>versionId</code> paramètre de requête n'est pas spécifié dans la requête, l'opération renvoie toutes les balises de la version la plus récente de l'objet dans un compartiment versionné. Si la version actuelle de l'objet est un marqueur de suppression, l'état "MethodNotAllowed" est renvoyé avec l'<code>x-amz-delete-marker</code> en-tête de réponse défini sur <code>true</code>.</p>
Objet principal	" Objet principal "
Objet de restauration	" Objet de restauration "
PutObject	" PutObject "
Objet de copie (Objet PUT précédemment nommé - Copier)	" Objet de copie "
PutObjectLegalHold	" Utilisez l'API REST S3 pour configurer le verrouillage objet S3 "

Fonctionnement	Mise en place
PutObjectRetention	"Utilisez l'API REST S3 pour configurer le verrouillage objet S3"
Marquage PutObject	<p>Utilise la tagging sous-ressource pour ajouter un ensemble de balises à un objet existant.</p> <p>Limites des balises d'objet</p> <p>Vous pouvez ajouter des balises à de nouveaux objets lorsque vous les téléchargez ou les ajouter à des objets existants. StorageGRID et Amazon S3 prennent en charge jusqu'à 10 balises pour chaque objet. Les balises associées à un objet doivent avoir des clés de balise uniques. Une clé de balise peut comporter jusqu'à 128 caractères Unicode et les valeurs de balise peuvent comporter jusqu'à 256 caractères Unicode. Les clés et les valeurs sont sensibles à la casse</p> <p>Mises à jour des balises et comportement d'ingestion</p> <p>Lorsque vous utilisez PutObjectTagging pour mettre à jour les balises d'un objet, StorageGRID ne réingère pas l'objet. Cela signifie que l'option de comportement d'ingestion spécifiée dans la règle ILM correspondante n'est pas utilisée. Tout changement au placement d'objet déclenché par la mise à jour est apporté lors de l'évaluation de ILM par des processus ILM en arrière-plan normaux.</p> <p>En d'autres termes, si la règle ILM utilise l'option strict pour le comportement d'ingestion, aucune action n'est entreprise si les placements d'objet requis ne peuvent pas être effectués (par exemple, parce qu'un nouvel emplacement n'est pas disponible). L'objet mis à jour conserve son emplacement actuel jusqu'à ce que le placement requis soit possible.</p> <p>Résolution des conflits</p> <p>Les demandes contradictoires des clients, telles que deux clients qui écrivent sur la même clé, sont résolues sur une base de « derniers-victoires ». La chronologie de l'évaluation « derniers-victoires » repose sur la date à laquelle le système StorageGRID termine une demande donnée et non sur la date à laquelle les clients S3 commencent une opération.</p> <p>Gestion des versions</p> <p>Si le <code>versionId</code> paramètre de requête n'est pas spécifié dans la requête, l'opération ajoute des balises à la version la plus récente de l'objet dans un compartiment versionné. Si la version actuelle de l'objet est un marqueur de suppression, l'état "MethodNotAllowed" est renvoyé avec l'<code>x-amz-delete-marker</code> en-tête de réponse défini sur <code>true</code>.</p>
SelectObjectContent	"SelectObjectContent"

Utiliser S3 Select

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



Les éléments non répertoriés ne sont pas pris en charge.

Pour la syntaxe, voir "[SelectObjectContent](#)". Pour plus d'informations sur S3 Select, reportez-vous au ["Documentation AWS pour S3 Select"](#).

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

Clauses

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

Types de données

- bool
- entier
- chaîne
- flottement
- décimale, numérique
- horodatage

Opérateurs

Opérateurs logiques

- ET
- PAS
- OU

Opérateurs de comparaison

- <
- >
- < ;=
- >=
- =
- =
- <>

- !=
- ENTRE
- DANS

Opérateurs de correspondance de répétition

- COMME
- _
- %

Opérateurs unitaires

- EST NULL
- N'EST PAS NULL

Opérateurs mathématiques

- +
- -
- *
- /
- %

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

Fonctions d'agrégation

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

Fonctions conditionnelles

- CASSE
- FUSIONNE
- NULLIF

Fonctions de conversion

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

Fonctions de date

- DATE_AJOUTER
- DATE_DIFF

- EXTRAIRE
- TO_STRING
- TO_TIMESTAMP
- CODE D'ARTICLE

Fonctions de chaîne

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

Utilisez le cryptage côté serveur

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

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

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

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



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



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

Utiliser SSE

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

x-amz-server-side-encryption

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

- "[PutObject](#)"

- "["Objet de copie"](#)
- "["CreateMultipartUpload"](#)

Utiliser SSE-C

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

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

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

- "["GetObject"](#)
- "["Objet principal"](#)
- "["PutObject"](#)
- "["Objet de copie"](#)
- "["CreateMultipartUpload"](#)
- "["UploadPart"](#)
- "["UploadPartCopy"](#)

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

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

- Vous devez utiliser https.
- 

StorageGRID rejette toute demande effectuée sur http lors de l'utilisation de SSE-C. Pour des raisons de sécurité, vous devez considérer que toute clé que vous envoyez accidentellement à l'aide de http est compromise. Mettez la clé au rebut et tournez-la selon les besoins.
- L'ETag dans la réponse n'est pas le MD5 des données objet.
 - Vous devez gérer le mappage des clés de chiffrement aux objets. StorageGRID ne stocke pas de clés de chiffrement. Vous êtes responsable du suivi de la clé de chiffrement que vous fournissez pour chaque objet.
 - Si le contrôle de version du compartiment est activé, chaque version d'objet doit disposer de sa propre clé de chiffrement. Vous êtes responsable du suivi de la clé de chiffrement utilisée pour chaque version d'objet.

- Comme vous gérez les clés de chiffrement côté client, vous devez également gérer d'autres dispositifs de protection, tels que la rotation des clés, côté client.



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

- Si la réPLICATION inter-grid ou CloudMirror est configurée pour le compartiment, vous ne pouvez pas acquérir d'objets SSE-C. L'opération d'acquisition échoue.

Informations associées

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

Objet de copie

Vous pouvez utiliser la requête CopyObject S3 pour créer une copie d'un objet déjà stocké dans S3. Une opération CopyObject est identique à l'exécution de GetObject suivie de PutObject.

Résoudre les conflits

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

Taille de l'objet

La taille recommandée maximale pour une opération PutObject unique est de 5 Gio (5,368,709,120 octets). Si vous avez des objets dont la valeur est supérieure à 5 Gio, utilisez la "[téléchargement partitionné](#)" valeur.

La taille supportée maximale pour une opération PutObject unique est de 5 Tio (5,497,558,138,880 octets).



Si vous avez mis à niveau à partir de StorageGRID 11.6 ou version antérieure, l'alerte PUT objet taille trop grande de S3 sera déclenchée si vous tentez de télécharger un objet dont la valeur dépasse 5 Gio. Si vous avez une nouvelle installation de StorageGRID 11.7 ou 11.8, l'alerte ne sera pas déclenchée dans ce cas. Toutefois, pour s'aligner sur la norme AWS S3, les futures versions d'StorageGRID ne prendront pas en charge le chargement d'objets de plus de 5 Gio.

Caractères UTF-8 dans les métadonnées utilisateur

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

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

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

de la clé contient des caractères non imprimables.

En-têtes de demande pris en charge

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

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

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

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

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

Si une demande est effectuée sans ces en-têtes, les paramètres de rétention par défaut du compartiment sont utilisés pour calculer le mode de version de l'objet et conserver jusqu'à la date. Voir "[Utilisez l'API REST S3 pour configurer le verrouillage objet S3](#)".

- En-têtes de demande SSE :

- x-amz-copy-source-server-side-encryption-customer-algorithm
- x-amz-copy-source-server-side-encryption-customer-key
- x-amz-copy-source-server-side-encryption-customer-key-MD5
- x-amz-server-side-encryption
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-algorithm

Voir [Demander des en-têtes pour le cryptage côté serveur](#)

En-têtes de requête non pris en charge

Les en-têtes de demande 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 celui-ci possède un checksum, StorageGRID ne copie pas cette valeur de checksum vers le nouvel objet. Ce comportement s'applique que vous essayez ou non d'utiliser x-amz-checksum-algorithm dans la demande d'objet.

- x-amz-website-redirect-location

Options de classe de stockage

L' `x-amz-storage-class` en-tête de requête est pris en charge et affecte le nombre de copies d'objet créées par StorageGRID si la règle ILM correspondante utilise la fonction Dual commit ou Balanced "option d'ingestion".

- STANDARD

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

- REDUCED_REDUNDANCY

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



Si vous acquérez un objet dans un compartiment avec le verrouillage d'objet S3 activé, l' `REDUCED_REDUNDANCY` option est ignorée. Si vous ingérer un objet dans un compartiment compatible hérité, l' `REDUCED_REDUNDANCY` option renvoie une erreur. StorageGRID procède toujours à une récupération à double engagement afin de satisfaire les exigences de conformité.

Utilisation de x-amz-copy-source dans CopyObject

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

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

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

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

Demander des en-têtes pour le cryptage côté serveur

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

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



Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant. Avant d'utiliser des clés fournies par le client pour sécuriser les données d'objet, consultez les considérations relatives à "utilisation du chiffrement 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 demande CopyObject :
 - x-amz-server-side-encryption



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

Gestion des versions

Si le compartiment source est versionné, vous pouvez utiliser l' `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 `versionId` sous-ressource. Si le compartiment de destination est versionné, la version générée est renvoyée dans l' `x-amz-version-id` en-tête de réponse. Si la gestion des versions est suspendue pour le compartiment cible, `x-amz-version-id` renvoie une valeur « null ».

GetObject

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

GetObject et objets multipièces

Vous pouvez utiliser le `partNumber` paramètre request pour extraire une partie spécifique d'un objet multi pièce ou segmenté. L' `x-amz-mp-parts-count` élément de réponse indique le nombre de parties de l'objet.

Vous pouvez définir `partNumber` la valeur 1 pour les objets segmentés/multi pièces et les objets non segmentés/non multi pièces ; cependant, l' `x-amz-mp-parts-count` élément de réponse est renvoyé uniquement pour les objets segmentés ou multi pièces.

Caractères UTF-8 dans les métadonnées utilisateur

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

En-tête de demande pris en charge

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

- **x-amz-checksum-mode:** Spécifiez ENABLED

L' `Range` en-tête n'est pas pris en charge `x-amz-checksum-mode` par 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 demande 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 aucune `versionId` sous-ressource n'est spécifiée, l'opération extrait la version la plus récente de l'objet dans un compartiment versionné. Si la version actuelle de l'objet est un marqueur de suppression, l'état « introuvable » est renvoyé avec l' `x-amz-delete-marker` en-tête de réponse défini sur `true`.

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

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

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

 Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant. Avant d'utiliser des clés fournies par le client pour sécuriser les données d'objet, consultez les considérations de la section "["Utilisez le cryptage côté serveur"](#).

Comportement de GetObject pour les objets de pool de stockage cloud

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 "[Objet principal](#)" 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 dans la grille, les requêtes GetObject tentent de récupérer les données de la grille avant de les extraire du pool de stockage cloud.

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

Objets partitionnés ou segmentés dans un pool de stockage cloud

Si vous avez téléchargé un objet partitionné ou si StorageGRID le divise en segments, StorageGRID détermine si l'objet est disponible dans le pool de stockage cloud en échantillonant un sous-ensemble de parties ou de segments de l'objet. Dans certains cas, une requête GetObject peut renvoyer de manière incorrecte 200 OK lorsque certaines parties de l'objet ont déjà été transférées à 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 certaines données, mais s'arrête à mi-chemin du transfert.
- Une requête GetObject suivante peut renvoyer 403 Forbidden.

GetObject et la réPLICATION inter-grille

Si vous utilisez "fédération des grilles" et "réPLICATION entre plusieurs grilles" est activé pour un compartiment, le client S3 peut vérifier l'état de réPLICATION d'un objet en émettant une requête GetObject. La réponse inclut l'en-tête de réponse spécifique à StorageGRID x-ntap-sg-cgr-replication-status, qui aura l'une des valeurs suivantes :

Grille	État de la réPLICATION
Source	<ul style="list-style-type: none">• TERMINÉ : la réPLICATION a réussi.• EN ATTENTE : l'objet n'a pas encore été répliqué.• ÉCHEC : la réPLICATION a échoué avec une défaillance permanente. L'utilisateur doit résoudre l'erreur.
Destination	RÉPLIQUE : l'objet a été répliqué à partir de la grille source.



StorageGRID ne prend pas en charge la x-amz-replication-status barre de coupe.

Objet principal

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

Objets en-tête et objets multiPièces

Vous pouvez utiliser partNumber le paramètre request pour extraire des métadonnées pour une partie spécifique d'un objet multiPièce ou segmenté. L' `x-amz-mp-parts-count` élément de réponse indique le nombre de parties de l'objet.

Vous pouvez définir partNumber la valeur 1 pour les objets segmentés/multiPièces et les objets non segmentés/non multiPièces ; cependant, l' `x-amz-mp-parts-count` élément de réponse est renvoyé uniquement pour les objets segmentés ou multiPièces.

Caractères UTF-8 dans les métadonnées utilisateur

StorageGRID n'analyse ni n'interprète pas les caractères UTF-8 qui se sont échappés dans les métadonnées

définies par l'utilisateur. Les demandes HEAD pour un objet avec des caractères UTF-8 échappés dans les métadonnées définies par l'utilisateur ne renvoient pas l' `x-amz-missing-meta` en-tête si le nom ou la valeur de la clé contient des caractères non imprimables.

En-tête de demande pris en charge

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

- x-amz-checksum-mode

Le partNumber paramètre et l' Range `en-tête 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 demande 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 aucune versionId sous-ressource n'est spécifiée, l'opération extrait la version la plus récente de l'objet dans un compartiment versionné. Si la version actuelle de l'objet est un marqueur de suppression, l'état « introuvable » est renvoyé avec l' x-amz-delete-marker`en-tête de réponse défini sur `true.

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

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

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

 Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant. Avant d'utiliser des clés fournies par le client pour sécuriser les données d'objet, consultez les considérations de la section "["Utilisez le cryptage côté serveur"](#).

HeadObject Responses for Cloud Storage Pool objects

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 lors de son déplacement vers Cloud Storage Pool, qui peut être migré vers un état non récupérable et restauré.

État de l'objet	Réponse à l'objet principal
Les objets sont ingéré dans StorageGRID mais pas encore évalués par ILM, ou objet stocké dans un pool de stockage traditionnel ou au moyen d'un code d'effacement	200 OK (Aucun en-tête de réponse spéciale n'est renvoyé.)
Objet dans Cloud Storage Pool, mais pas encore migré vers un état non récupérable	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"</p> <p>Jusqu'à ce que l'objet soit transféré à un état non récupérable, la valeur de expiry-date est définie sur un temps distant à l'avenir. L'heure exacte de la transition n'est pas contrôlée par le système StorageGRID.</p>
L'objet est passé à l'état non récupérable, mais il existe au moins une copie sur la grille	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"</p> <p>La valeur de expiry-date est définie sur un temps distant à l'avenir.</p> <p>Remarque : si la copie de la grille n'est pas disponible (par exemple, un nœud de stockage est en panne), vous devez émettre une "Objet de restauration" demande de restauration de la copie à partir du pool de stockage cloud avant de pouvoir récupérer l'objet.</p>
L'objet a été transféré à un état non récupérable et aucune copie n'existe sur la grille	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p>
Objet en cours de restauration à partir d'un état non récupérable	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>x-amz-restore: ongoing-request="true"</p>

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

Objets partitionnés ou segmentés dans Cloud Storage Pool

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

HeadObject et réPLICATION inter-grid

Si vous utilisez "fédération des grilles" et "réPLICATION entre plusieurs grilles" est activé pour un compartiment, le client S3 peut vérifier l'état de réPLICATION d'un objet en émettant une requête HeadObject. La réponse inclut l'en-tête de réponse spécifique à StorageGRID x-ntap-sg-cgr-rePLICATION-status, qui aura l'une des valeurs suivantes :

Grille	État de la réPLICATION
Source	<ul style="list-style-type: none"> TERMINÉ : la réPLICATION a réussi. EN ATTENTE : l'objet n'a pas encore été répliqué. ÉCHEC : la réPLICATION a échoué avec une défaillance permanente. L'utilisateur doit résoudre l'erreur.
Destination	RÉPLIQUE : l'objet a été répliqué à partir de la grille source.



StorageGRID ne prend pas en charge la x-amz-rePLICATION-status barre de coupe.

PutObject

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

Résoudre les conflits

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

Taille de l'objet

La taille recommandée maximale pour une opération PutObject unique est de 5 Gio (5,368,709,120 octets). Si vous avez des objets dont la valeur est supérieure à 5 Gio, utilisez la "[téléchargement partitionné](#)" valeur.

La taille supportée maximale pour une opération PutObject unique est de 5 Tio (5,497,558,138,880 octets).



Si vous avez mis à niveau à partir de StorageGRID 11.6 ou version antérieure, l'alerte PUT objet taille trop grande de S3 sera déclenchée si vous tentez de télécharger un objet dont la valeur dépasse 5 Gio. Si vous avez une nouvelle installation de StorageGRID 11.7 ou 11.8, l'alerte ne sera pas déclenchée dans ce cas. Toutefois, pour s'aligner sur la norme AWS S3, les futures versions d'StorageGRID ne prendront pas en charge le chargement d'objets de plus de 5 Gio.

Taille des métadonnées utilisateur

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

Caractères UTF-8 dans les métadonnées utilisateur

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

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

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

Limites des balises d'objet

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

Propriété de l'objet

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

En-têtes de demande pris en charge

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

- Cache-Control

- Content-Disposition

- Content-Encoding

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

- StorageGRID ne vérifie pas le chunk-signature par rapport aux données de bloc.
- StorageGRID ne vérifie pas la valeur que vous fournissez pour x-amz-decoded-content-length l'objet.

- Content-Language

- Content-Length

- Content-MD5

- Content-Type

- Expires

- Transfer-Encoding

Le codage de transfert avec chunked est pris en charge si aws-chunked la signature de charge est également utilisée.

- x-amz-checksum-sha256

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

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

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

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

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

La valeur de creation-time est évaluée 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'acquisition équilibrée ou stricte. Une erreur est renvoyée lors de la création de la règle ILM.

- x-amz-tagging
- En-têtes de requête de verrouillage d'objet S3
 - x-amz-object-lock-mode

- x-amz-object-lock-retain-until-date

- x-amz-object-lock-legal-hold

Si une demande est effectuée sans ces en-têtes, les paramètres de rétention par défaut du compartiment sont utilisés pour calculer le mode de version de l'objet et conserver jusqu'à la date. Voir ["Utilisez l'API REST S3 pour configurer le verrouillage objet S3"](#).

- En-têtes de demande SSE :

- x-amz-server-side-encryption

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

- x-amz-server-side-encryption-customer-key

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

Voir [Demander des en-têtes pour le cryptage côté serveur](#)

En-têtes de requête non pris en charge

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

- If-Match

- If-None-Match

- x-amz-acl

- x-amz-sdk-checksum-algorithm

- x-amz-trailer

- x-amz-website-redirect-location

L'`x-amz-website-redirect-location` en-tête renvoie `XNotImplemented.

Options de classe de stockage

L'`x-amz-storage-class` en-tête de la demande est pris en charge. La valeur fournie pour affecte la `x-amz-storage-class` façon dont StorageGRID protège les données d'objet lors de l'ingestion et non le nombre de copies persistantes de l'objet stockées dans le système StorageGRID (déterminé par la règle ILM).

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

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

- STANDARD (Par défaut)

- **Double commit** : si la règle ILM spécifie l'option de double validation pour le comportement d'ingestion, dès qu'un objet est ingéré, une seconde copie de cet objet est créée et distribuée à un autre nœud de stockage (double commit). Une fois la règle ILM évaluée, StorageGRID détermine si ces copies intermédiaires initiales répondent aux instructions de placement de la règle. Si ce n'est pas le cas, de nouvelles copies d'objet peuvent avoir besoin d'être effectuées à différents emplacements et

les copies intermédiaires initiales peuvent avoir besoin d'être supprimées.

- **Balanced** : si la règle ILM spécifie l'option équilibrée et que StorageGRID ne peut pas immédiatement effectuer 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'objet spécifiées dans la règle ILM (placement synchrone), l' `x-amz-storage-class` en-tête n'a aucun effet.

- **REDUCED_REDUNDANCY**

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

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

 Le fait d'avoir une seule copie répliquée pendant une période donnée présente un risque de perte permanente des données. Si une seule copie répliquée d'un objet existe, cet objet est perdu en cas de défaillance ou d'erreur importante d'un noeud de stockage. De plus, lors des procédures de maintenance telles que les mises à niveau, l'accès à l'objet est temporairement perdu.

Le fait de spécifier `REDUCED_REDUNDANCY` affecte uniquement le nombre de copies créées lors de la première ingestion d'un objet. Cela n'affecte pas le nombre de copies de l'objet effectuées lorsque l'objet est évalué par les règles ILM actives, et n'entraîne pas le stockage des données à des niveaux de redondance inférieurs dans le système StorageGRID.

 Si vous acquérez un objet dans un compartiment avec le verrouillage d'objet S3 activé, l' `REDUCED_REDUNDANCY` option est ignorée. Si vous ingérer un objet dans un compartiment compatible hérité, l' `REDUCED_REDUNDANCY` option renvoie une erreur. StorageGRID procède toujours à une récupération à double engagement afin de satisfaire les exigences de conformité.

Demander des en-têtes pour le cryptage côté serveur

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

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

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

Lorsque l' `x-amz-server-side-encryption` en-tête n'est pas inclus dans la demande PutObject, la grille

"paramètre de chiffrement d'objet stocké" est omise de la réponse PutObject.

- **SSE-C:** Utilisez les trois en-têtes si vous voulez chiffrer l'objet avec une clé unique que vous fournissez et gérez.

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

 Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant. Avant d'utiliser des clés fournies par le client pour sécuriser les données d'objet, consultez les considérations relatives à "[utilisation du chiffrement côté serveur](#)".

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

Gestion des versions

Si la gestion des versions est activée pour un compartiment, une unique `versionId` est automatiquement générée pour la version de l'objet stocké. Ceci `versionId` est également renvoyé dans la réponse à l'aide de l'``x-amz-version-id`` en-tête de réponse.

Si la gestion des versions est suspendue, la version de l'objet est stockée avec une valeur `versionId` NULL et si une version nulle existe déjà, elle sera écrasée.

Calculs de signature pour l'en-tête autorisation

Lorsque vous utilisez l'`Authorization` en-tête pour authentifier les requêtes, StorageGRID diffère d'AWS de la manière suivante :

- StorageGRID ne nécessite pas l'`host` inclusion d'en-têtes dans `CanonicalHeaders`.
- StorageGRID ne nécessite pas d'`Content-Type` être inclus dans `CanonicalHeaders`.
- StorageGRID ne nécessite pas l'`x-amz-*` inclusion d'en-têtes dans `CanonicalHeaders`.

 En règle générale, incluez toujours ces en-têtes dans `CanonicalHeaders` pour vous assurer 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 dans un seul bloc \(signature AWS version 4\)](#)" .

Informations associées

- "[Gestion des objets avec ILM](#)"
- "[Référence de l'API Amazon simple Storage Service : PutObject](#)"

Objet de restauration

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

Type de demande pris en charge

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

Gestion des versions

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

Comportement de `RestoreObject` sur les objets de pool de stockage cloud

Si un objet a été stocké dans un "[Pool de stockage cloud](#)", une requête `RestoreObject` a le comportement suivant, en fonction de l'état de l'objet. Voir "[Objet principal](#)" 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 dans la grille, il n'est pas nécessaire de restaurer l'objet en émettant une requête `RestoreObject`. À la place, la copie locale peut être récupérée directement à l'aide d'une requête `GetObject`.

État de l'objet	Comportement de <code>RestoreObject</code>
L'objet est ingéré dans StorageGRID mais pas encore évalué par ILM ou l'objet ne se trouve pas dans un pool de stockage cloud	403 Forbidden, InvalidObjectState
Objet dans Cloud Storage Pool, mais pas encore migré vers un état non récupérable	200 OK Aucune modification n'est effectuée. Remarque : avant qu'un objet ne soit transféré à un état non récupérable, vous ne pouvez pas modifier son <code>expiry-date</code> .

État de l'objet	Comportement de RestoreObject
L'objet a été transféré à un état non récupérable	<p>202 Accepted Restaure une copie récupérable de l'objet vers le pool de stockage cloud pendant le nombre de jours spécifié dans le corps de la requête. À la fin de cette période, l'objet est renvoyé à un état non récupérable.</p> <p>Vous pouvez également utiliser <code>Tier</code> l'élément de demande pour déterminer la durée de la tâche de restauration pour terminer (<code>Expedited</code>, <code>Standard</code> ou <code>Bulk</code>). Si vous ne spécifiez pas <code>Tier</code>, le Standard niveau est utilisé.</p> <p>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 du Expedited Tier. L'erreur suivante est renvoyée 403 Forbidden, InvalidTier: Retrieval option is not supported by this storage class.</p>
Objet en cours de restauration à partir d'un état non récupérable	409 Conflict, RestoreAlreadyInProgress
Objet entièrement restauré dans le pool de stockage cloud	<p>200 OK</p> <p>Note: si un objet a été restauré à un état récupérable, vous pouvez le modifier <code>expiry-date</code> en réémettant la requête <code>RestoreObject</code> avec une nouvelle valeur pour <code>Days</code>. La date de restauration est mise à jour par rapport à l'heure de la demande.</p>

SelectObjectContent

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

Pour plus d'informations, voir "[Référence de l'API Amazon simple Storage Service : SelectObjectContent](#)".

Avant de commencer

- Le compte de tenant dispose de l'autorisation S3 Select.
- Vous disposez de l'autorisation pour l'objet que vous `s3:GetObject` souhaitez interroger.
- L'objet que vous souhaitez interroger doit être dans l'un des formats suivants :
 - **CSV.** Peut être utilisé tel qu'il est ou compressé dans des archives GZIP ou BZIP2.
 - **Parquet.** Exigences supplémentaires pour les objets parquet :
 - S3 Select prend uniquement en charge la compression par colonne à l'aide de GZIP ou de 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 compressées est de 512 Mo.
 - Vous devez utiliser les types de données spécifiés dans le schéma de l'objet.

- Vous ne pouvez pas utiliser de types logiques D'INTERVALLE, de JSON, DE LISTE, DE TEMPS ou d'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 MIB.

Exemple de syntaxe de demande 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, 2010 populations, environ 2015 populations et le pourcentage de changement des données de recensement des États-Unis. Les enregistrements du fichier qui ne sont pas des États sont ignorés.

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

Les premières lignes du fichier à interroger, SUB-EST2020_ALL.csv, ressemblent 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, 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

```

Exemple d'utilisation de l'interface de ligne de commande AWS (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, change.csv, se 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 partitionnés

Opérations pour les téléchargements partitionnés

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

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

- Vous ne devez pas dépasser 1,000 téléchargements partitionnés simultanés vers un seul compartiment, car les résultats des requêtes ListMultipartUploads pour ce compartiment peuvent renvoyer des résultats incomplets.
- StorageGRID fait respecter les limites de taille d'AWS pour les pièces en plusieurs parties. Les clients S3 doivent respecter les consignes suivantes :
 - Chaque partie d'un téléchargement partitionné doit être comprise entre 5 Mio (5,242,880 octets) et 5 Gio (5,368,709,120 octets).
 - La dernière partie peut être inférieure à 5 Mio (5,242,880 octets).
 - En général, la taille des pièces doit être la plus grande possible. Par exemple, utilisez une taille de pièce de 5 Gio pour un objet de 100 Gio. Chaque pièce étant considérée comme un objet unique, l'utilisation de pièces de grande taille réduit la surcharge liée aux métadonnées StorageGRID.
 - Pour les objets de moins de 5 Gio, envisagez l'utilisation de téléchargement non partitionné.
- La gestion des règles ILM est évaluée pour chaque partie d'un objet en plusieurs parties lors de son ingestion et pour l'objet dans son ensemble lorsque le téléchargement partitionné est terminé, si la règle ILM utilise la méthode équilibrée ou stricte "[option d'ingestion](#)". Vous devez savoir comment cela affecte le positionnement de l'objet et de la pièce :

- Si des modifications sont apportées au ILM pendant un téléchargement partitionné S3, certaines parties de l'objet peuvent ne pas répondre aux exigences ILM actuelles une fois le téléchargement partitionné terminé. Toute pièce qui n'est pas correctement placée est mise en file d'attente pour une réévaluation ILM et déplacée vers l'emplacement correct ultérieurement.
 - Lors de l'évaluation d'ILM pour une pièce, StorageGRID filtre la taille de la pièce, et non la taille de l'objet. Ainsi, certaines parties d'un objet peuvent être stockées dans des emplacements qui ne respectent pas les exigences de la règle ILM pour l'ensemble de l'objet. Par exemple, si une règle indique que tous les objets de 10 Go ou plus sont stockés sur DC1 alors que tous les objets plus petits sont stockés sur DC2, chaque partie de 1 Go d'un téléchargement partitionné en 10 parties est stockée sur DC2 lors de l'ingestion. Cependant, lorsque 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 partitionné, le "Seuil de segmentation d'objet (1 Gio)" n'est pas appliqué.
 - Si nécessaire, vous pouvez l'utiliser "chiffrement côté serveur" avec les téléchargements partitionnés. Pour utiliser SSE (chiffrement côté serveur avec des clés gérées par StorageGRID), vous incluez l'en-tête `x-amz-server-side-encryption` dans la requête CreateMultipartUpload uniquement. Pour utiliser SSE-C (chiffrement côté serveur avec des clés fournies par le client), vous devez spécifier les trois mêmes en-têtes de requête de clé de chiffrement dans la demande CreateMultipartUpload et dans chaque demande UploadPart suivante.
 - Un objet téléchargé en plusieurs parties est inclus dans un "seau de branche" si l'ingestion a été initiée avant l'horodatage Avant du bucket de base, quel que soit le moment où le téléchargement est terminé.

Fonctionnement	Mise en place
AbortMultipartUpload	Mise en œuvre avec tout le comportement de l'API REST Amazon S3. D'être modifiées sans préavis.
CompleteMultipartUpload	Voir " CompleteMultipartUpload "
CreateMultipartUpload (Précédemment appelé lancer le téléchargement multipièce)	Voir " CreateMultipartUpload "
ListMultipartUploads	Voir " ListMultipartUploads "
ListParts	Mise en œuvre avec tout le comportement de l'API REST Amazon S3. D'être modifiées sans préavis.
UploadPart	Voir " UploadPart "
UploadPartCopy	Voir " UploadPartCopy "

CompleteMultipartUpload

L'opération CompleteMultipartUpload effectue un téléchargement partitionné d'un objet

en assemblant les pièces précédemment téléchargées.



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

Résoudre les conflits

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

En-têtes de demande pris en charge

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

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

L'`x-amz-storage-class` en-tête affecte le nombre de copies objet créées par StorageGRID si la règle ILM correspondante spécifie le "[Double allocation ou option d'ingestion équilibrée](#)".

- STANDARD

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

- REDUCED_REDUNDANCY

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



Si vous acquérez un objet dans un compartiment avec le verrouillage d'objet S3 activé, l'`'REDUCED_REDUNDANCY'` option est ignorée. Si vous ingérer un objet dans un compartiment compatible hérité, l'`'REDUCED_REDUNDANCY'` option renvoie une erreur. StorageGRID procède toujours à une récupération à double engagement afin de satisfaire les exigences de conformité.



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



La `ETag` valeur renvoyée n'est pas une somme MD5 des données, mais suit l'implémentation de l'API Amazon S3 de la `ETag` valeur pour les objets multipart.

En-têtes de requête non pris en charge

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

- `If-Match`

- If-None-Match
- x-amz-sdk-checksum-algorithm
- x-amz-trailer

Gestion des versions

Cette opération termine un téléchargement partitionné. Si la gestion des versions est activée pour un compartiment, la version de l'objet est créée une fois le téléchargement partitionné terminé.

Si la gestion des versions est activée pour un compartiment, une unique `versionId` est automatiquement générée pour la version de l'objet stocké. Ceci `versionId` est également renvoyé dans la réponse à l'aide de l'`x-amz-version-id` en-tête de réponse.

Si la gestion des versions est suspendue, la version de l'objet est stockée avec une valeur `versionId` NULL et si une version nulle existe déjà, elle sera écrasée.

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

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

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

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

Reportez-vous à la "[Résoudre les problèmes liés aux services de plateforme](#)".

CreateMultipartUpload

L'opération `CreateMultipartUpload` (précédemment appelée `Initiate Multipart Upload`) lance un téléchargement partitionné pour un objet et renvoie un ID de téléchargement.

L'`x-amz-storage-class` en-tête de la demande est pris en charge. La valeur fournie pour affecte la `x-amz-storage-class` façon dont StorageGRID protège les données d'objet lors de l'ingestion et non le nombre de copies persistantes de l'objet stockées dans le système StorageGRID (déterminé par la règle ILM).

Si la règle ILM correspondant à un objet ingéré utilise le paramètre strict "[option d'ingestion](#)", l'`x-amz-storage-class` en-tête n'a aucun effet.

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

- STANDARD (Par défaut)

- **Dual commit** : si la règle ILM spécifie l’option d’acquisition Dual commit, dès qu’un objet est ingéré, une deuxième copie de cet objet est créée et distribuée à un autre nœud de stockage (double commit). Une fois la règle ILM évaluée, StorageGRID détermine si ces copies intermédiaires initiales répondent aux instructions de placement de la règle. Si ce n’est pas le cas, de nouvelles copies d’objet peuvent avoir besoin d’être effectuées à différents emplacements et les copies intermédiaires initiales peuvent avoir besoin d’être supprimées.
- **Balanced** : si la règle ILM spécifie l’option équilibrée et que StorageGRID ne peut pas immédiatement effectuer 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’objet spécifiées dans la règle ILM (placement synchrone), l’`x-amz-storage-class` en-tête n’a aucun effet.

- REDUCED_REDUNDANCY

- **Dual commit** : si la règle ILM spécifie l’option Dual commit, StorageGRID crée une copie intermédiaire unique lorsque l’objet est ingéré (single commit).
- **Équilibré** : si la règle ILM spécifie l’option équilibrée, StorageGRID effectue une seule copie intermédiaire uniquement si le système ne peut pas immédiatement effectuer toutes les copies spécifiées dans la règle. Si StorageGRID peut effectuer un placement synchrone, cet en-tête n’a aucun effet. L’`REDUCED_REDUNDANCY` option est mieux utilisée lorsque la règle ILM qui correspond à l’objet crée une copie répliquée unique. Dans ce cas, l’utilisation de `REDUCED_REDUNDANCY` supprime la création et la suppression inutiles d’une copie d’objet supplémentaire pour chaque opération d’ingestion.

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

 Le fait d’avoir une seule copie répliquée pendant une période donnée présente un risque de perte permanente des données. Si une seule copie répliquée d’un objet existe, cet objet est perdu en cas de défaillance ou d’erreur importante d’un noeud de stockage. De plus, lors des procédures de maintenance telles que les mises à niveau, l’accès à l’objet est temporairement perdu.

Le fait de spécifier REDUCED_REDUNDANCY affecte uniquement le nombre de copies créées lors de la première ingestion d’un objet. Cela n’affecte pas le nombre de copies de l’objet effectuées lorsque l’objet est évalué par les règles ILM actives, et n’entraîne pas le stockage des données à des niveaux de redondance inférieurs dans le système StorageGRID.

 Si vous acquérez un objet dans un compartiment avec le verrouillage d’objet S3 activé, l’`REDUCED_REDUNDANCY` option est ignorée. Si vous ingérer un objet dans un compartiment compatible hérité, l’`REDUCED_REDUNDANCY` option renvoie une erreur. StorageGRID procède toujours à une récupération à double engagement afin de satisfaire les exigences de conformité.

En-têtes de demande pris en charge

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

- Content-Type

- `x-amz-checksum-algorithm`

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

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

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

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

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

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

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



L'ajout de `creation-time` métadonnées définies par l'utilisateur n'est pas autorisé si vous ajoutez un objet à un compartiment pour lequel la conformité des données existantes est activée. Une erreur sera renvoyée.

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

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

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

["Utilisez l'API REST S3 pour configurer le verrouillage objet S3"](#)

- En-têtes de demande SSE :

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

[Demander des en-têtes pour le cryptage côté serveur](#)



Pour plus d'informations sur la façon dont StorageGRID traite les caractères UTF-8, reportez-vous à la section ["PutObject"](#).

Demander des en-têtes pour le cryptage côté serveur

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

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

 Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant. Avant d'utiliser des clés fournies par le client pour sécuriser les données d'objet, consultez les considérations relatives à "[utilisation du chiffrement côté serveur](#)".

En-têtes de requête non pris en charge

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

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

L'`x-amz-website-redirect-location` en-tête renvoie `XNotImplemented.

Gestion des versions

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

ListMultipartUploads

L'opération ListMultipartUploads répertorie les téléchargements partitionnés en cours pour un compartiment.

Les paramètres de demande suivants sont pris en charge :

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

- upload-id-marker
- Host
- Date
- Authorization

Gestion des versions

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

UploadPart

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

En-têtes de demande pris en charge

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

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

Demander des en-têtes pour le cryptage côté serveur

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

- x-amz-server-side-encryption-customer-algorithm: Spécifiez AES256.
- x-amz-server-side-encryption-customer-key: Spécifiez la même clé de cryptage que celle que vous avez fournie dans la demande CreateMultipartUpload.
- x-amz-server-side-encryption-customer-key-MD5: Spécifiez le même résumé 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 des clés fournies par le client pour sécuriser les données d'objet, consultez les considérations de la section "[Utilisez 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 requête 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 demande suivants ne sont pas pris en charge :

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

Gestion des versions

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

UploadPartCopy

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

L'opération UploadPartCopy est implémentée avec tout comportement de l'API REST Amazon S3. D'être modifiées 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

Demander des en-têtes pour le cryptage côté serveur

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

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

Si l'objet source est crypté 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 décrypté puis copié :

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

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



Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant. Avant d'utiliser des clés fournies par le client pour sécuriser les données d'objet, consultez les considérations de la section "["Utilisez le cryptage côté serveur"](#)".

Gestion des versions

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

Réponses d'erreur

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

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

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

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

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

Codes d'erreur personnalisés StorageGRID

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

Informations sur le copyright

Copyright © 2026 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUSSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.