Utiliser l'API REST S3

StorageGRID software

NetApp
December 03, 2025

Sommaire

Utiliser l’API REST S3

Versions et mises à jour prises en charge par l’API REST S3

StorageGRID prend en charge l’API Simple Storage Service (S3), qui est implémentée sous la forme d’un ensemble de services Web Representational State Transfer (REST).

La prise en charge de l’API REST S3 vous permet de connecter des applications orientées services développées pour les services Web S3 avec un stockage d’objets sur site qui utilise le système StorageGRID . Des modifications minimales sont requises dans l’utilisation actuelle des appels d’API REST S3 par une application cliente.

Versions prises en charge

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

Article	Version
Spécification de l’API S3	"Documentation Amazon Web Services (AWS) : Référence de l’API Amazon Simple Storage Service"
HTTP	1,1 Pour plus d’informations sur HTTP, consultez HTTP/1.1 (RFC 7230-35). "IETF RFC 2616 : Protocole de transfert hypertexte (HTTP/1.1)" **Remarque** : StorageGRID ne prend pas en charge le pipeline HTTP/1.1.

Mises à jour de la prise en charge de l’API REST S3

Libérer	Commentaires
11,9	• Ajout de la prise en charge des valeurs de somme de contrôle SHA-256 précalculées pour les requêtes suivantes et les en-têtes pris en charge. Vous pouvez utiliser cette fonctionnalité pour vérifier l'intégrité des objets téléchargés : ◦ Téléchargement complet en plusieurs parties : `x-amz-checksum-sha256` ◦ Créer un téléchargement multi-parties : `x-amz-checksum-algorithm` ◦ Obtenir l'objet : `x-amz-checksum-mode` ◦ HeadObject : `x-amz-checksum-mode` ◦ Liste des pièces ◦ PutObject : `x-amz-checksum-sha256` ◦ TéléchargerPartie : `x-amz-checksum-sha256` • Ajout de la possibilité pour l'administrateur de la grille de contrôler les paramètres de conservation et de conformité au niveau du locataire. Ces paramètres affectent les paramètres de verrouillage d'objet S3. ◦ Mode de conservation par défaut du bucket et mode de conservation des objets : Gouvernance ou Conformité, si autorisé par l'administrateur de la grille. ◦ Période de conservation par défaut du bucket et date de conservation de l'objet : doit être inférieure ou égale à ce qui est autorisé par la période de conservation maximale définie par l'administrateur de la grille. • Prise en charge améliorée pour `aws-chunked` encodage et streaming de contenu `x-amz-content-sha256` valeurs. Limites: ◦ Si présent, `chunk-signature` est facultatif et non validé ◦ Si présent, `x-amz-trailer` le contenu est ignoré
11,8	Mise à jour des noms des opérations S3 pour correspondre aux noms utilisés dans le "Documentation Amazon Web Services (AWS) : Référence de l'API Amazon Simple Storage Service" .
11,7	• Ajouté"Référence rapide : requêtes API S3 prises en charge" . • Ajout de la prise en charge de l'utilisation du mode GOUVERNANCE avec S3 Object Lock. • Ajout de la prise en charge spécifique à StorageGRID `x-ntap-sg-cgr-replication-status` en-tête de réponse pour les requêtes GET Object et HEAD Object. Cet en-tête fournit l'état de réplication d'un objet pour la réplication inter-grille. • Les requêtes SelectObjectContent prennent désormais en charge les objets Parquet.

Libérer	Commentaires
11,6	• Ajout de la prise en charge de l'utilisation du `partNumber` paramètre de requête dans les requêtes d'objet GET et d'objet HEAD. • Ajout de la prise en charge d'un mode de conservation par défaut et d'une période de conservation par défaut au niveau du bucket pour S3 Object Lock. • Ajout du support pour le `s3:object-lock-remaining-retention-days` clé de condition de politique pour définir la plage de périodes de conservation autorisées pour vos objets. • La taille maximale *recommandée* pour une seule opération d'objet PUT a été modifiée à 5 Gio (5 368 709 120 octets). Si vous avez des objets dont la taille est supérieure à 5 Gio, utilisez plutôt le téléchargement en plusieurs parties.
11,5	• Prise en charge ajoutée pour la gestion du chiffrement du bucket. • Ajout de la prise en charge du verrouillage d'objet S3 et des demandes de conformité héritées obsolètes. • Ajout de la prise en charge de l'utilisation de DELETE Multiple Objects sur des buckets versionnés. • Le `Content-MD5` l'en-tête de requête est désormais correctement pris en charge.
11,4	• Prise en charge ajoutée pour le balisage des buckets DELETE, GET et PUT. Les balises d'allocation des coûts ne sont pas prises en charge. • Pour les buckets créés dans StorageGRID 11.4, la restriction des noms de clés d'objet pour respecter les meilleures pratiques en matière de performances n'est plus nécessaire. • Ajout de la prise en charge des notifications de bucket sur le `s3:ObjectRestore:Post` type d'événement. • Les limites de taille AWS pour les pièces en plusieurs parties sont désormais appliquées. Chaque partie d'un téléchargement en plusieurs parties doit être comprise entre 5 Mio et 5 Gio. La dernière partie peut être inférieure à 5 Mio. • Ajout de la prise en charge de TLS 1.3
11,3	• Ajout de la prise en charge du chiffrement côté serveur des données d'objet avec des clés fournies par le client (SSE-C). • Prise en charge ajoutée pour les opérations de cycle de vie du bucket DELETE, GET et PUT (action d'expiration uniquement) et pour le `x-amz-expiration` en-tête de réponse. • Objet PUT mis à jour, Objet PUT - Copie et Téléchargement en plusieurs parties pour décrire l'impact des règles ILM qui utilisent le placement synchrone lors de l'ingestion. • Les chiffrements TLS 1.1 ne sont plus pris en charge.

Libérer	Commentaires
11,2	Prise en charge ajoutée pour la restauration d'objets POST à utiliser avec les pools de stockage cloud. Ajout de la prise en charge de l'utilisation de la syntaxe AWS pour l'ARN, les clés de condition de stratégie et les variables de stratégie dans les stratégies de groupe et de compartiment. Les stratégies de groupe et de compartiment existantes qui utilisent la syntaxe StorageGRID continueront d'être prises en charge. **Remarque :** les utilisations d'ARN/URN dans d'autres configurations JSON/XML, y compris celles utilisées dans les fonctionnalités StorageGRID personnalisées, n'ont pas changé.
11,1	Ajout de la prise en charge du partage de ressources inter-origines (CORS), du HTTP pour les connexions client S3 aux nœuds de grille et des paramètres de conformité sur les buckets.
11,0	Prise en charge ajoutée pour la configuration des services de plateforme (réplication CloudMirror, notifications et intégration de recherche Elasticsearch) pour les buckets. La prise en charge des contraintes d'emplacement de balisage d'objets pour les buckets et la cohérence disponible ont également été ajoutées.
10,4	Ajout de la prise en charge des modifications d'analyse ILM apportées au contrôle de version, aux mises à jour de la page Noms de domaine de point de terminaison, aux conditions et variables dans les politiques, aux exemples de politiques et à l'autorisation PutOverwriteObject.
10,3	Prise en charge ajoutée pour le contrôle de version.
10,2	Ajout de la prise en charge des stratégies d'accès aux groupes et aux buckets, ainsi que de la copie en plusieurs parties (Télécharger une partie - Copier).
10,1	Prise en charge ajoutée pour le téléchargement en plusieurs parties, les demandes de type hébergé virtuellement et l'authentification v4.
10,0	Prise en charge initiale de l'API REST S3 par le système StorageGRID . La version actuellement prise en charge de la *Référence API du service de stockage simple* est le 01/03/2006.

Référence rapide : requêtes API S3 prises en charge

Cette page résume la manière dont StorageGRID prend en charge les API Amazon Simple Storage Service (S3).

Cette page inclut uniquement les opérations S3 prises en charge par StorageGRID.

Pour voir la documentation AWS pour chaque opération, sélectionnez le lien dans l'en-tête.

Paramètres de requête URI courants et en-têtes de requête

Sauf indication contraire, les paramètres de requête URI courants suivants sont pris en charge :

- `versionId`(comme requis pour les opérations sur les objets)

Sauf indication contraire, les en-têtes de requête courants suivants sont pris en charge :

- `Authorization`
- `Connection`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Date`
- `Expect`
- `Host`
- `x-amz-date`

Informations connexes

- "Détails d'implémentation de l'API REST S3"
- "Référence de l'API Amazon Simple Storage Service : en-têtes de requête courants"

"Abandonner le téléchargement en plusieurs parties"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette requête, plus ce paramètre de requête URI supplémentaire :

- `uploadId`

Corps de la requête

Aucune

Documentation de StorageGRID

"Opérations pour les téléchargements en plusieurs parties"

"Téléchargement complet en plusieurs parties"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette requête, plus ce paramètre de requête URI supplémentaire :

- `uploadId`
- `x-amz-checksum-sha256`

Balises XML du corps de la requête

StorageGRID prend en charge ces balises XML de corps de requête :

- `ChecksumSHA256`
- `CompleteMultipartUpload`
- `ETag`
- `Part`
- `PartNumber`

Documentation de StorageGRID

"Téléchargement complet en plusieurs parties"

"Copier l'objet"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette demande, plus ces en-têtes supplémentaires :

- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-modified-since`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-server-side-encryption-customer-algorithm`
- `x-amz-copy-source-server-side-encryption-customer-key`
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`
- `x-amz-metadata-directive`
- `x-amz-object-lock-legal-hold`
- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-server-side-encryption`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-storage-class`
- `x-amz-tagging`
- `x-amz-tagging-directive`
- `x-amz-meta-<metadata-name>`

Corps de la requête

Aucune

Documentation de StorageGRID

"Copier l'objet"

"Créer un bucket"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette demande, plus ces en-têtes supplémentaires :

- `x-amz-bucket-object-lock-enabled`

Corps de la requête

StorageGRID prend en charge tous les paramètres du corps de la requête définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation de StorageGRID

"Opérations sur les godets"

"Créer un téléchargement multi-parties"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette demande, plus ces en-têtes supplémentaires :

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `Expires`
- `x-amz-checksum-algorithm`
- `x-amz-server-side-encryption`
- `x-amz-storage-class`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-tagging`
- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-object-lock-legal-hold`
- `x-amz-meta-<metadata-name>`

Corps de la requête

Aucune

Documentation de StorageGRID

"Créer un téléchargement multi-parties"

"Supprimer le bucket"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette demande.

Documentation de StorageGRID

"Opérations sur les godets"

"SupprimerBucketCors"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette demande.

Corps de la requête

Aucune

Documentation de StorageGRID

"Opérations sur les godets"

"Supprimer le chiffrement du bucket"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette demande.

Corps de la requête

Aucune

Documentation de StorageGRID

"Opérations sur les godets"

"Supprimer le cycle de vie du bucket"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette demande.

Corps de la requête

Aucune

Documentation de StorageGRID

- "Opérations sur les godets"
- "Créer une configuration du cycle de vie S3"

"Supprimer la politique de bucket"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette demande.

Corps de la requête

Aucune

Documentation de StorageGRID

"Opérations sur les godets"

"SupprimerBucketReplication"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette demande.

Corps de la requête

Aucune

Documentation de StorageGRID

"Opérations sur les godets"

"Supprimer le balisage du bucket"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette demande.

Corps de la requête

Aucune

Documentation de StorageGRID

"Opérations sur les godets"

"Supprimer l'objet"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette requête, plus cet en-tête de requête supplémentaire :

- `x-amz-bypass-governance-retention`

Corps de la requête

Aucune

Documentation de StorageGRID

"Opérations sur les objets"

"Supprimer les objets"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette requête, plus cet en-tête de requête supplémentaire :

- `x-amz-bypass-governance-retention`

Corps de la requête

StorageGRID prend en charge tous les paramètres du corps de la requête définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation de StorageGRID

"Opérations sur les objets"

"Supprimer l'étiquetage des objets"

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette demande.

Corps de la requête

Aucune

Documentation de StorageGRID

"Opérations sur les objets"

"ObtenirBucketAcl"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette demande.

Corps de la requête

Aucune

Documentation de StorageGRID

"Opérations sur les godets"

"ObtenirBucketCors"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette demande.

Corps de la requête

Aucune

Documentation de StorageGRID

"Opérations sur les godets"

"Obtenir le chiffrement du bucket"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette demande.

Corps de la requête

Aucune

Documentation de StorageGRID

"Opérations sur les godets"

"GetBucketLifecycleConfiguration"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette demande.

Corps de la requête

Aucune

Documentation de StorageGRID

- "Opérations sur les godets"
- "Créer une configuration du cycle de vie S3"

"Obtenir l'emplacement du bucket"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette demande.

Corps de la requête

Aucune

Documentation de StorageGRID

"Opérations sur les godets"

"Configuration de GetBucketNotification"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette demande.

Corps de la requête

Aucune

Documentation de StorageGRID

"Opérations sur les godets"

"Obtenir la politique de Bucket"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette demande.

Corps de la requête

Aucune

Documentation de StorageGRID

"Opérations sur les godets"

"Réplication GetBucket"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette demande.

Corps de la requête

Aucune

Documentation de StorageGRID

"Opérations sur les godets"

"Obtenir le balisage du bucket"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette demande.

Corps de la requête

Aucune

Documentation de StorageGRID

"Opérations sur les godets"

"Obtenir la gestion des versions du bucket"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette demande.

Corps de la requête

Aucune

Documentation de StorageGRID

"Opérations sur les godets"

"Obtenir l'objet"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette requête, plus ces paramètres de requête URI supplémentaires :

- `x-amz-checksum-mode`
- `partNumber`
- `response-cache-control`
- `response-content-disposition`

- `response-content-encoding`
- `response-content-language`
- `response-content-type`
- `response-expires`

Et ces en-têtes de requête supplémentaires :

- `Range`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `If-Match`
- `If-Modified-Since`
- `If-None-Match`
- `If-Unmodified-Since`

Corps de la requête

Aucune

Documentation de StorageGRID

"Obtenir l'objet"

"ObtenirObjectAcl"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette demande.

Corps de la requête

Aucune

Documentation de StorageGRID

"Opérations sur les objets"

"Obtenir la conservation légale de l'objet"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette demande.

Corps de la requête

Aucune

Documentation de StorageGRID

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

"Obtenir la configuration du verrouillage de l'objet"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette demande.

Corps de la requête

Aucune

Documentation de StorageGRID

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

"Obtenir la rétention d'objet"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette demande.

Corps de la requête

Aucune

Documentation de StorageGRID

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

"Obtenir l'étiquetage des objets"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette demande.

Corps de la requête

Aucune

Documentation de StorageGRID

"Opérations sur les objets"

"Tête de godet"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette demande.

Corps de la requête

Aucune

Documentation de StorageGRID

"Opérations sur les godets"

"HeadObject"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette demande, plus ces en-têtes supplémentaires :

- `x-amz-checksum-mode`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `If-Match`
- `If-Modified-Since`
- `If-None-Match`
- `If-Unmodified-Since`
- `Range`

Corps de la requête

Aucune

Documentation de StorageGRID

"HeadObject"

"Listes de seaux"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette demande.

Corps de la requête

Aucune

Documentation de StorageGRID

Opérations sur le service › ListBuckets

"ListeMultipartUploads"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette requête, plus ces paramètres supplémentaires :

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

Corps de la requête

Aucune

Documentation de StorageGRID

"ListeMultipartUploads"

"Liste d'objets"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette requête, plus ces paramètres supplémentaires :

- `delimiter`
- `encoding-type`
- `marker`
- `max-keys`
- `prefix`

Corps de la requête

Aucune

Documentation de StorageGRID

"Opérations sur les godets"

"ListObjectsV2"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette requête, plus ces paramètres supplémentaires :

- `continuation-token`
- `delimiter`
- `encoding-type`
- `fetch-owner`
- `max-keys`
- `prefix`
- `start-after`

Corps de la requête

Aucune

Documentation de StorageGRID

"Opérations sur les godets"

"ListObjectVersions"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette requête, plus ces paramètres supplémentaires :

- `delimiter`

- `encoding-type`
- `key-marker`
- `max-keys`
- `prefix`
- `version-id-marker`

Corps de la requête

Aucune

Documentation de StorageGRID

"Opérations sur les godets"

"Liste des pièces"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette requête, plus ces paramètres supplémentaires :

- `max-parts`
- `part-number-marker`
- `uploadId`

Corps de la requête

Aucune

Documentation de StorageGRID

"ListeMultipartUploads"

"PutBucketCors"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette demande.

Corps de la requête

StorageGRID prend en charge tous les paramètres du corps de la requête définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation de StorageGRID

"Opérations sur les godets"

"Cryptage PutBucket"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette demande.

Balises XML du corps de la requête

StorageGRID prend en charge ces balises XML de corps de requête :

- `ApplyServerSideEncryptionByDefault`
- `Rule`
- `ServerSideEncryptionConfiguration`
- `SSEAlgorithm`

Documentation de StorageGRID

"Opérations sur les godets"

"Configuration du cycle de vie de PutBucket"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette demande.

Balises XML du corps de la requête

StorageGRID prend en charge ces balises XML de corps de requête :

- `And`
- `Days`
- `Expiration`
- `ExpiredObjectDeleteMarker`
- `Filter`
- `ID`
- `Key`
- `LifecycleConfiguration`
- `NewerNoncurrentVersions`
- `NoncurrentDays`
- `NoncurrentVersionExpiration`
- `Prefix`
- `Rule`
- `Status`
- `Tag`
- `Value`

Documentation de StorageGRID

- "Opérations sur les godets"
- "Créer une configuration du cycle de vie S3"

"Configuration de PutBucketNotification"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette demande.

Balises XML du corps de la requête

StorageGRID prend en charge ces balises XML de corps de requête :

- `Event`
- `Filter`
- `FilterRule`
- `Id`
- `Name`
- `NotificationConfiguration`
- `Prefix`
- `S3Key`
- `Suffix`
- `Topic`
- `TopicConfiguration`
- `Value`

Documentation de StorageGRID

"Opérations sur les godets"

"Politique de PutBucket"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette demande.

Corps de la requête

Pour plus de détails sur les champs de corps JSON pris en charge, voir"Utiliser des politiques d'accès aux buckets et aux groupes" .

"Réplication de PutBucket"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette demande.

Balises XML du corps de la requête

- `Bucket`
- `Destination`
- `Prefix`
- `ReplicationConfiguration`

- `Rule`
- `Status`
- `StorageClass`

Documentation de StorageGRID

"Opérations sur les godets"

"Balisage de PutBucket"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette demande.

Corps de la requête

StorageGRID prend en charge tous les paramètres du corps de la requête définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation de StorageGRID

"Opérations sur les godets"

"Gestion des versions de PutBucket"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette demande.

Paramètres du corps de la requête

StorageGRID prend en charge ces paramètres de corps de requête :

- `VersioningConfiguration`
- `Status`

Documentation de StorageGRID

"Opérations sur les godets"

"Mettre l'objet"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette demande, plus ces en-têtes supplémentaires :

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `Expires`
- `x-amz-checksum-sha256`
- `x-amz-server-side-encryption`

- `x-amz-storage-class`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-tagging`
- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-object-lock-legal-hold`
- `x-amz-meta-<metadata-name>`

Corps de la requête

- Données binaires de l'objet

Documentation de StorageGRID

"Mettre l'objet"

"MettreObjetLegalHold"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette demande.

Corps de la requête

StorageGRID prend en charge tous les paramètres du corps de la requête définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation de StorageGRID

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

"Configuration de PutObjectLock"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette demande.

Corps de la requête

StorageGRID prend en charge tous les paramètres du corps de la requête définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation de StorageGRID

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

"PutObjectRetention"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette demande, plus cet en-tête supplémentaire :

- `x-amz-bypass-governance-retention`

Corps de la requête

StorageGRID prend en charge tous les paramètres du corps de la requête définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation de StorageGRID

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

"Balisage d'objets"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette demande.

Corps de la requête

StorageGRID prend en charge tous les paramètres du corps de la requête définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation de StorageGRID

"Opérations sur les objets"

"Restaurer l'objet"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette demande.

Corps de la requête

Pour plus de détails sur les champs de corps pris en charge, voir"Restaurer l'objet" .

"Sélectionner le contenu de l'objet"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette demande.

Corps de la requête

Pour plus de détails sur les champs de corps pris en charge, consultez les éléments suivants :

- "Utiliser S3 Select"
- "Sélectionner le contenu de l'objet"

"Télécharger une partie"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette requête, plus ces paramètres de requête URI supplémentaires :

- `partNumber`
- `uploadId`

Et ces en-têtes de requête supplémentaires :

- `x-amz-checksum-sha256`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`

Corps de la requête

- Données binaires de la pièce

Documentation de StorageGRID

"Télécharger une partie"

"TéléchargerPartCopy"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous lesparamètres et en-têtes communs pour cette requête, plus ces paramètres de requête URI supplémentaires :

- `partNumber`
- `uploadId`

Et ces en-têtes de requête supplémentaires :

- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-modified-since`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-range`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-copy-source-server-side-encryption-customer-algorithm`
- `x-amz-copy-source-server-side-encryption-customer-key`
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`

Corps de la requête

Aucune

Documentation de StorageGRID

"TéléchargerPartCopy"

Tester la configuration de l'API REST S3

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

Avant de commencer

- Vous avez téléchargé et installé l'AWS CLI depuis "aws.amazon.com/cli" .
- En option, vous avez"créé un point de terminaison d'équilibrage de charge" . Sinon, vous connaissez l'adresse IP du nœud de stockage auquel vous souhaitez vous connecter et le numéro de port à utiliser. Voir "Adresses IP et ports pour les connexions client" .
- Tu as"créé un compte locataire S3" .
- Vous vous êtes connecté au locataire et"créé une clé d'accès" .

Pour plus de détails sur ces étapes, voir"Configurer les connexions client" .

Étapes

1. Configurez les paramètres AWS CLI pour utiliser le compte que vous avez créé dans le système StorageGRID :
   a. Entrer en mode configuration : `aws configure`
   b. Saisissez l'ID de clé d'accès pour le compte que vous avez créé.
   c. Saisissez la clé d'accès secrète du compte que vous avez créé.
   d. Entrez la région par défaut à utiliser. Par exemple : `us-east-1` .
   e. Saisissez le format de sortie par défaut à utiliser ou appuyez sur **Entrée** pour sélectionner JSON.
2. Créer un bucket.

   Cet exemple suppose que vous avez configuré un point de terminaison d'équilibrage de charge pour utiliser l'adresse IP 10.96.101.17 et le port 10443.

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

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

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

3. Télécharger un objet.

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

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

4. Répertoriez le contenu du bucket pour vérifier que l'objet a été téléchargé.

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

5. Supprimer l'objet.

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

6. Supprimer le bucket.

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

Comment StorageGRID implémente l'API REST S3

Demandes clients conflictuelles

Les demandes client conflictuelles, telles que deux clients écrivant sur la même clé, sont résolues sur la base des « derniers gagnants ».

Le moment de l'évaluation des « dernières victoires » est basé sur le moment où le système StorageGRID termine une demande donnée, et non sur le moment où les clients S3 commencent une opération.

Valeurs de cohérence

La cohérence fournit un équilibre entre la disponibilité des objets et la cohérence de ces objets sur différents nœuds de stockage et sites. Vous pouvez modifier la cohérence selon les besoins de votre application.

Par défaut, StorageGRID garantit la cohérence de lecture après écriture pour les objets nouvellement créés. Tout GET suivant un PUT terminé avec succès pourra lire les données nouvellement écrites. Les écrasements d'objets existants, les mises à jour de métadonnées et les suppressions sont finalement cohérents. Les écrasements prennent généralement quelques secondes ou minutes pour se propager, mais peuvent prendre jusqu'à 15 jours.

Si vous souhaitez effectuer des opérations sur les objets avec une cohérence différente, vous pouvez :

- Spécifier une consistance pourchaque seau .
- Spécifier une consistance pourchaque opération API .
- Modifiez la cohérence par défaut de l'ensemble de la grille en effectuant l'une des tâches suivantes :

◦ Dans le gestionnaire de grille, accédez à **CONFIGURATION** > **Système** > **Paramètres de stockage** > **Cohérence par défaut**.

◦ .

> Une modification de la cohérence à l'échelle de la grille s'applique uniquement aux compartiments créés après la modification du paramètre. Pour déterminer les détails d'une modification, consultez le journal d'audit situé à l'adresse `/var/local/log` (rechercher **consistencyLevel**).

Valeurs de cohérence

La cohérence affecte la manière dont les métadonnées utilisées par StorageGRID pour suivre les objets sont distribuées entre les nœuds et, par conséquent, la disponibilité des objets pour les demandes des clients.

Vous pouvez définir la cohérence d'un bucket ou d'une opération API sur l'une des valeurs suivantes :

- **Tous** : Tous les nœuds reçoivent les données immédiatement, sinon la demande échouera.
- **Strong-global** : garantit la cohérence de lecture après écriture pour toutes les demandes client sur tous les sites.
- **Strong-site** : garantit la cohérence de lecture après écriture pour toutes les requêtes client au sein d'un site.
- **Lecture après nouvelle écriture** : (par défaut) Fournit une cohérence de lecture après écriture pour les nouveaux objets et une cohérence éventuelle pour les mises à jour d'objets. Offre des garanties de haute disponibilité et de protection des données. Recommandé dans la plupart des cas.
- **Disponible** : Fournit une cohérence éventuelle pour les nouveaux objets et les mises à jour d'objets. Pour les buckets S3, utilisez-les uniquement si nécessaire (par exemple, pour un bucket contenant des valeurs de journal rarement lues ou pour des opérations HEAD ou GET sur des clés qui n'existent pas). Non pris en charge pour les buckets S3 FabricPool .

Utiliser la cohérence « Lecture après nouvelle écriture » et « Disponible »

Lorsqu'une opération HEAD ou GET utilise la cohérence « Lecture après nouvelle écriture », StorageGRID effectue la recherche en plusieurs étapes, comme suit :

- Il recherche d'abord l'objet en utilisant une faible cohérence.
- Si cette recherche échoue, elle répète la recherche à la valeur de cohérence suivante jusqu'à ce qu'elle atteigne une cohérence équivalente au comportement de strong-global.

Si une opération HEAD ou GET utilise la cohérence « Lecture après nouvelle écriture » mais que l'objet n'existe pas, la recherche d'objet atteindra toujours une cohérence équivalente au comportement de strong-global. Étant donné que cette cohérence nécessite que plusieurs copies des métadonnées de l'objet soient disponibles sur chaque site, vous pouvez recevoir un nombre élevé d'erreurs de serveur interne 500 si deux ou plusieurs nœuds de stockage sur le même site ne sont pas disponibles.

À moins que vous n'ayez besoin de garanties de cohérence similaires à celles d'Amazon S3, vous pouvez éviter ces erreurs pour les opérations HEAD et GET en définissant la cohérence sur « Disponible ». Lorsqu'une opération HEAD ou GET utilise la cohérence « Disponible », StorageGRID fournit uniquement la cohérence éventuelle. Il ne réessaye pas une opération ayant échoué en augmentant la cohérence, il ne nécessite donc pas que plusieurs copies des métadonnées de l'objet soient disponibles.

Spécifier la cohérence pour le fonctionnement de l'API

Pour définir la cohérence d'une opération API individuelle, les valeurs de cohérence doivent être prises en charge pour l'opération et vous devez spécifier la cohérence dans l'en-tête de la demande. Cet exemple définit la cohérence sur « Strong-site » pour une opération GetObject.

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

Vous devez utiliser la même cohérence pour les opérations PutObject et GetObject.

Spécifier la cohérence du bucket

Pour définir la cohérence du bucket, vous pouvez utiliser le StorageGRID"Cohérence du seau PUT" demande. Ou vous pouvez"changer la consistance d'un seau" du gestionnaire locataire.

Lorsque vous définissez la cohérence d'un bucket, tenez compte des éléments suivants :

- La définition de la cohérence d'un bucket détermine la cohérence utilisée pour les opérations S3 effectuées sur les objets du bucket ou sur la configuration du bucket. Cela n'affecte pas les opérations sur le bucket lui-même.
- La cohérence d'une opération API individuelle remplace la cohérence du bucket.
- En général, les buckets doivent utiliser la cohérence par défaut, « Lecture après nouvelle écriture ». Si les requêtes ne fonctionnent pas correctement, modifiez le comportement du client de l'application si possible. Ou configurez le client pour spécifier la cohérence de chaque demande d'API. Définissez la consistance au niveau du seau uniquement en dernier recours.

Comment les règles de cohérence et de gestion des informations interagissent pour affecter la protection des données

Votre choix de cohérence et votre règle ILM affectent la manière dont les objets sont protégés. Ces paramètres peuvent interagir.

Par exemple, la cohérence utilisée lors du stockage d'un objet affecte le placement initial des métadonnées de l'objet, tandis que le comportement d'ingestion sélectionné pour la règle ILM affecte le placement initial des copies de l'objet. Étant donné que StorageGRID nécessite l'accès aux métadonnées d'un objet et à ses données pour répondre aux demandes des clients, la sélection de niveaux de protection correspondants pour la cohérence et le comportement d'ingestion peut fournir une meilleure protection initiale des données et des réponses système plus prévisibles.

Ce qui suit"options d'ingestion" sont disponibles pour les règles ILM :

Double engagement

StorageGRID effectue immédiatement des copies intermédiaires de l'objet et renvoie le succès au client. Les copies spécifiées dans la règle ILM sont réalisées lorsque cela est possible.

Strict

Toutes les copies spécifiées dans la règle ILM doivent être effectuées avant que le succès ne soit renvoyé au client.

Équilibré

StorageGRID tente de réaliser toutes les copies spécifiées dans la règle ILM lors de l'ingestion ; si cela n'est pas possible, des copies intermédiaires sont réalisées et le succès est renvoyé au client. Les copies spécifiées dans la règle ILM sont réalisées lorsque cela est possible.

Exemple de la manière dont la règle de cohérence et la règle ILM peuvent interagir

Supposons que vous ayez une grille à deux sites avec la règle ILM suivante et la cohérence suivante :

- **Règle ILM** : Créez deux copies d'objet, une sur le site local et une sur un site distant. Adoptez un comportement d'ingestion strict.
- **cohérence** : Global fort (les métadonnées de l'objet sont immédiatement distribuées à tous les sites).

Lorsqu'un client stocke un objet dans la grille, StorageGRID effectue les deux copies de l'objet et distribue les métadonnées aux deux sites avant de renvoyer le succès au client.

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

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

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

Versionnage d'objet

Vous pouvez définir l'état de version d'un bucket si vous souhaitez conserver plusieurs versions de chaque objet. L'activation du contrôle de version pour un bucket peut aider à protéger contre la suppression accidentelle d'objets et vous permet de récupérer et de restaurer des versions antérieures d'un objet.

Le système StorageGRID implémente le contrôle de version avec prise en charge de la plupart des fonctionnalités et avec certaines limitations. StorageGRID prend en charge jusqu'à 10 000 versions de chaque objet.

Le contrôle de version des objets peut être combiné avec la gestion du cycle de vie des informations StorageGRID (ILM) ou avec la configuration du cycle de vie du bucket S3. Vous devez activer explicitement le contrôle de version pour chaque bucket. Lorsque le contrôle de version est activé pour un bucket, chaque objet ajouté au bucket se voit attribuer un ID de version, généré par le système StorageGRID .

L'utilisation de l'authentification multifacteur (MFA) n'est pas prise en charge.

Le contrôle de version ne peut être activé que sur les buckets créés avec StorageGRID version 10.3 ou ultérieure.

ILM et gestion des versions

Les politiques ILM sont appliquées à chaque version d'un objet. Un processus d'analyse ILM analyse en continu tous les objets et les réévalue par rapport à la politique ILM actuelle. Toutes les modifications que vous apportez aux stratégies ILM sont appliquées à tous les objets précédemment ingérés. Cela inclut les versions précédemment ingérées si le contrôle de version est activé. L'analyse ILM applique de nouvelles modifications ILM aux objets précédemment ingérés.

Pour les objets S3 dans les compartiments activés pour le contrôle de version, la prise en charge du contrôle de version vous permet de créer des règles ILM qui utilisent « Heure non actuelle » comme heure de référence (sélectionnez **Oui** pour la question « Appliquer cette règle uniquement aux anciennes versions d'objet ? » dans"Étape 1 de l'assistant Créer une règle ILM"). Lorsqu'un objet est mis à jour, ses versions précédentes deviennent obsolètes. L'utilisation d'un filtre « Heure non actuelle » vous permet de créer des politiques qui réduisent l'impact sur le stockage des versions précédentes des objets.

Lorsque vous téléchargez une nouvelle version d'un objet à l'aide d'une opération de téléchargement en plusieurs parties, l'heure non actuelle de la version d'origine de l'objet reflète le moment où le téléchargement en plusieurs parties a été créé pour la nouvelle version, et non le moment où le téléchargement en plusieurs parties a été terminé. Dans des cas limités, l'heure non actuelle de la version originale peut être antérieure de plusieurs heures ou jours à l'heure de la version actuelle.

Informations connexes

- "Comment les objets versionnés S3 sont supprimés"
- "Règles et politiques ILM pour les objets versionnés S3 (exemple 4)" .

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

Si le paramètre global de verrouillage d'objet S3 est activé pour votre système StorageGRID , vous pouvez créer des buckets avec le verrouillage d'objet S3 activé. Vous pouvez spécifier la rétention par défaut pour chaque compartiment ou les paramètres de rétention pour chaque version d'objet.

Comment activer le verrouillage d'objet S3 pour un bucket

Si le paramètre global de verrouillage d'objet S3 est activé pour votre système StorageGRID , vous pouvez éventuellement activer le verrouillage d'objet S3 lorsque vous créez chaque bucket.

Le verrouillage d'objet S3 est un paramètre permanent qui ne peut être activé que lorsque vous créez un bucket. Vous ne pouvez pas ajouter ou désactiver le verrouillage d'objet S3 après la création d'un bucket.

Pour activer le verrouillage d'objet S3 pour un bucket, utilisez l'une de ces méthodes :

- Créez le bucket à l'aide du gestionnaire de locataires. Voir "Créer un bucket S3" .
- Créez le bucket à l'aide d'une requête CreateBucket avec le `x-amz-bucket-object-lock-enabled` en-tête de requête. Voir "Opérations sur les godets" .

S3 Object Lock nécessite le contrôle de version du bucket, qui est activé automatiquement lors de la création

du bucket. Vous ne pouvez pas suspendre le contrôle de version du bucket. Voir "Versionnage d'objet" .

Paramètres de conservation par défaut pour un bucket

Lorsque le verrouillage d'objet S3 est activé pour un compartiment, vous pouvez éventuellement activer la rétention par défaut pour le compartiment et spécifier un mode de rétention par défaut et une période de rétention par défaut.

Mode de rétention par défaut

- En mode CONFORMITÉ :
  - L'objet ne peut pas être supprimé tant que sa date de conservation n'est pas atteinte.
  - La date de conservation de l'objet peut être augmentée, mais elle ne peut pas être diminuée.
  - La date de conservation de l'objet ne peut pas être supprimée tant que cette date n'est pas atteinte.
- En mode GOUVERNANCE :
  - Les utilisateurs avec le `s3:BypassGovernanceRetention` l'autorisation peut utiliser le `x-amz-bypass-governance-retention: true` en-tête de demande pour contourner les paramètres de conservation.
  - Ces utilisateurs peuvent supprimer une version d'objet avant que sa date de conservation ne soit atteinte.
  - Ces utilisateurs peuvent augmenter, diminuer ou supprimer la date de conservation d'un objet.

Période de conservation par défaut

Chaque bucket peut avoir une période de conservation par défaut spécifiée en années ou en jours.

Comment définir la rétention par défaut pour un bucket

Pour définir la rétention par défaut d'un bucket, utilisez l'une de ces méthodes :

- Gérez les paramètres du bucket à partir du gestionnaire de locataires. Voir"Créer un bucket S3" et"Mettre à jour la conservation par défaut du verrouillage des objets S3" .
- Émettez une demande PutObjectLockConfiguration pour le bucket afin de spécifier le mode par défaut et le nombre de jours ou d'années par défaut.

Configuration de PutObjectLock

La demande PutObjectLockConfiguration vous permet de définir et de modifier le mode de conservation par défaut et la période de conservation par défaut pour un bucket sur lequel le verrouillage d'objet S3 est activé. Vous pouvez également supprimer les paramètres de conservation par défaut précédemment configurés.

Lorsque de nouvelles versions d'objet sont ingérées dans le bucket, le mode de rétention par défaut est appliqué si `x-amz-object-lock-mode` et `x-amz-object-lock-retain-until-date` ne sont pas spécifiés. La période de conservation par défaut est utilisée pour calculer la date de conservation si `x-amz-object-lock-retain-until-date` n'est pas spécifié.

Si la période de conservation par défaut est modifiée après l'ingestion d'une version d'objet, la date de conservation de la version d'objet reste la même et n'est pas recalculée à l'aide de la nouvelle période de conservation par défaut.

Vous devez avoir le `s3:PutBucketObjectLockConfiguration` autorisation, ou être un compte root, pour

terminer cette opération.

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

Exemple de demande

Cet exemple active le verrouillage d'objet S3 pour un bucket et définit le mode de conservation par défaut sur CONFORMITÉ et la période de conservation par défaut sur 6 ans.

```
PUT /bucket?object-lock HTTP/1.1
Accept-Encoding: identity
Content-Length: 308
Host: host
Content-MD5: request header
User-Agent: s3sign/1.0.0 requests/2.24.0 python/3.8.2
X-Amz-Date: date
X-Amz-Content-SHA256: authorization-string
Authorization: authorization-string

<ObjectLockConfiguration>
    <ObjectLockEnabled>Enabled</ObjectLockEnabled>
    <Rule>
        <DefaultRetention>
            <Mode>COMPLIANCE</Mode>
            <Years>6</Years>
        </DefaultRetention>
    </Rule>
</ObjectLockConfiguration>
```

Comment déterminer la rétention par défaut d'un bucket

Pour déterminer si le verrouillage d'objet S3 est activé pour un bucket et pour voir le mode de conservation par défaut et la période de conservation, utilisez l'une de ces méthodes :

- Afficher le bucket dans le gestionnaire de locataires. Voir "Afficher les buckets S3" .
- Émettez une demande GetObjectLockConfiguration.

Obtenir la configuration du verrouillage de l'objet

La demande GetObjectLockConfiguration vous permet de déterminer si le verrouillage d'objet S3 est activé pour un compartiment et, s'il est activé, de voir s'il existe un mode de conservation par défaut et une période de conservation configurés pour le compartiment.

Lorsque de nouvelles versions d'objet sont ingérées dans le bucket, le mode de rétention par défaut est appliqué si `x-amz-object-lock-mode` n'est pas spécifié. La période de conservation par défaut est utilisée pour calculer la date de conservation si `x-amz-object-lock-retain-until-date` n'est pas spécifié.

Vous devez avoir le `s3:GetBucketObjectLockConfiguration` autorisation, ou être un compte root, pour terminer cette opération.

Exemple de demande

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

Exemple de réponse

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

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

Comment spécifier les paramètres de conservation d'un objet

Un bucket avec S3 Object Lock activé peut contenir une combinaison d'objets avec et sans paramètres de conservation S3 Object Lock.

Les paramètres de conservation au niveau de l'objet sont spécifiés à l'aide de l'API REST S3. Les paramètres de rétention d'un objet remplacent tous les paramètres de rétention par défaut du compartiment.

Vous pouvez spécifier les paramètres suivants pour chaque objet :

- **Mode de conservation** : Soit CONFORMITÉ, soit GOUVERNANCE.
- **Retain-until-date** : une date spécifiant la durée pendant laquelle la version de l'objet doit être conservée par StorageGRID.

    - En mode CONFORMITÉ, si la date de conservation est dans le futur, l'objet peut être récupéré, mais il ne peut pas être modifié ou supprimé. La date de conservation peut être augmentée, mais cette date ne peut pas être diminuée ou supprimée.
    - En mode GOUVERNANCE, les utilisateurs disposant d'une autorisation spéciale peuvent contourner le paramètre de conservation jusqu'à la date. Ils peuvent supprimer une version d'objet avant l'expiration de sa période de conservation. Ils peuvent également augmenter, diminuer ou même supprimer la date de conservation.
- **Conservation légale** : L'application d'une conservation légale à une version d'objet verrouille immédiatement cet objet. Par exemple, vous pourriez avoir besoin de suspendre légalement un objet lié à une enquête ou à un litige juridique. Une conservation légale n'a pas de date d'expiration, mais reste en place jusqu'à ce qu'elle soit explicitement supprimée.

  Le paramètre de conservation légale d'un objet est indépendant du mode de conservation et de la date de conservation. Si une version d'objet est soumise à une suspension légale, personne ne peut supprimer cette version.

Pour spécifier les paramètres de verrouillage d'objet S3 lors de l'ajout d'une version d'objet à un bucket, émettez un"Mettre l'objet" ,"Copier l'objet" , ou"Créer un téléchargement multi-parties" demande.

Vous pouvez utiliser les éléments suivants :

- `x-amz-object-lock-mode`, qui peut être CONFORMITÉ ou GOUVERNANCE (sensible à la casse).

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

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

  Si la conservation légale est activée (sensible à la casse), l'objet est placé sous conservation légale. Si la retenue légale est désactivée, aucune retenue légale n'est placée. Toute autre valeur entraîne une erreur 400 Bad Request (InvalidArgument).

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

- Le `Content-MD5` l'en-tête de la demande est requis le cas échéant `x-amz-object-lock-*` l'en-tête de requête est présent dans la requête PutObject. `Content-MD5` n'est pas requis pour CopyObject ou CreateMultipartUpload.
- Si le compartiment n'a pas de verrouillage d'objet S3 activé et qu'un `x-amz-object-lock-*` l'en-tête de requête est présent, une erreur 400 Bad Request (InvalidRequest) est renvoyée.
- La requête PutObject prend en charge l'utilisation de `x-amz-storage-class: REDUCED_REDUNDANCY` pour correspondre au comportement d'AWS. Cependant, lorsqu'un objet est ingéré dans un bucket avec S3 Object Lock activé, StorageGRID effectuera toujours une ingestion à double validation.
- Une réponse de version GET ou HeadObject ultérieure inclura les en-têtes `x-amz-object-lock-mode` ,

`x-amz-object-lock-retain-until-date` , et `x-amz-object-lock-legal-hold` , si configuré et si l'expéditeur de la requête a le bon `s3:Get*` autorisations.

Vous pouvez utiliser le `s3:object-lock-remaining-retention-days` clé de condition de politique pour limiter les périodes de conservation minimales et maximales autorisées pour vos objets.

Comment mettre à jour les paramètres de conservation d'un objet

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

- `PutObjectLegalHold`

  Si la nouvelle valeur de conservation légale est activée, l'objet est placé sous une conservation légale. Si la valeur de maintien légal est OFF, le maintien légal est levé.

- `PutObjectRetention`
  - La valeur du mode peut être COMPLIANCE ou GOVERNANCE (sensible à la casse).
  - La valeur de conservation jusqu'à la date doit être au format `2020-08-10T21:46:00Z` . Les fractions de secondes sont autorisées, mais seuls 3 chiffres décimaux sont conservés (précision en millisecondes). Les autres formats ISO 8601 ne sont pas autorisés.
  - Si une version d'objet possède une date de conservation existante, vous ne pouvez que l'augmenter. La nouvelle valeur doit être dans le futur.

Comment utiliser le mode GOUVERNANCE

Les utilisateurs qui ont le `s3:BypassGovernanceRetention` l'autorisation peut contourner les paramètres de conservation actifs d'un objet qui utilise le mode GOUVERNANCE. Toutes les opérations DELETE ou PutObjectRetention doivent inclure le `x-amz-bypass-governance-retention:true` en-tête de requête. Ces utilisateurs peuvent effectuer ces opérations supplémentaires :

- Exécutez les opérations DeleteObject ou DeleteObjects pour supprimer une version d'objet avant l'expiration de sa période de conservation.

  Les objets faisant l'objet d'une suspension légale ne peuvent pas être supprimés. La retenue légale doit être désactivée.

- Exécutez des opérations PutObjectRetention qui modifient le mode de version d'un objet de GOUVERNANCE à CONFORMITÉ avant l'expiration de la période de conservation de l'objet.

  Le passage du mode CONFORMITÉ au mode GOUVERNANCE n'est jamais autorisé.

- Exécutez des opérations PutObjectRetention pour augmenter, diminuer ou supprimer la période de conservation d'une version d'objet.

Informations connexes

- "Gérer les objets avec S3 Object Lock"
- "Utilisez S3 Object Lock pour conserver les objets"
- "Guide de l'utilisateur d'Amazon Simple Storage Service : Verrouillage d'objets"

Créer une configuration du cycle de vie S3

Vous pouvez créer une configuration de cycle de vie S3 pour contrôler le moment où des objets spécifiques sont supprimés du système StorageGRID .

L'exemple simple de cette section illustre comment une configuration de cycle de vie S3 peut contrôler le moment où certains objets sont supprimés (expirés) de compartiments S3 spécifiques. L'exemple dans cette section est fourni à titre d'illustration uniquement. Pour plus de détails sur la création de configurations de cycle de vie S3, consultez "Guide de l'utilisateur d'Amazon Simple Storage Service : Gestion du cycle de vie des objets" . Notez que StorageGRID prend uniquement en charge les actions d'expiration ; il ne prend pas en charge les actions de transition.

Quelle est la configuration du cycle de vie

Une configuration de cycle de vie est un ensemble de règles appliquées aux objets dans des compartiments S3 spécifiques. Chaque règle spécifie quels objets sont concernés et quand ces objets expireront (à une date spécifique ou après un certain nombre de jours).

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

- Expiration : supprimez un objet lorsqu'une date spécifiée est atteinte ou lorsqu'un nombre de jours spécifié est atteint, à compter du moment où l'objet a été ingéré.
- NoncurrentVersionExpiration : supprimez un objet lorsqu'un nombre de jours spécifié est atteint, à compter du moment où l'objet est devenu non actuel.
- Filtre (préfixe, balise)
- Statut
- ID

Chaque objet suit les paramètres de conservation d'un cycle de vie de compartiment S3 ou d'une politique ILM. Lorsqu'un cycle de vie de compartiment S3 est configuré, les actions d'expiration du cycle de vie remplacent la stratégie ILM pour les objets correspondant au filtre de cycle de vie du compartiment. Les objets qui ne correspondent pas au filtre de cycle de vie du bucket utilisent les paramètres de conservation de la stratégie ILM. Si un objet correspond à un filtre de cycle de vie de compartiment et qu'aucune action d'expiration n'est explicitement spécifiée, les paramètres de conservation de la stratégie ILM ne sont pas utilisés et il est implicite que les versions d'objet sont conservées pour toujours. Voir "Exemples de priorités pour le cycle de vie du bucket S3 et la politique ILM" .

Par conséquent, un objet peut être supprimé de la grille même si les instructions de placement d'une règle ILM s'appliquent toujours à l'objet. Ou bien, un objet peut être conservé sur la grille même après l'expiration des instructions de placement ILM pour l'objet. Pour plus de détails, consultez la section "Comment ILM fonctionne tout au long de la vie d'un objet" .

> La configuration du cycle de vie du bucket peut être utilisée avec les buckets pour lesquels le verrouillage d'objet S3 est activé, mais la configuration du cycle de vie du bucket n'est pas prise en charge pour les buckets conformes hérités.

StorageGRID prend en charge l'utilisation des opérations de bucket suivantes pour gérer les configurations du cycle de vie :

- Supprimer le cycle de vie du bucket

- GetBucketLifecycleConfiguration
- Configuration du cycle de vie de PutBucket

Créer une configuration du cycle de vie

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

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

   > Les règles qui spécifient un nombre de jours sont relatives au moment où l'objet a été ingéré. Si la date actuelle dépasse la date d'ingestion plus le nombre de jours, certains objets peuvent être supprimés du bucket dès que la configuration du cycle de vie est appliquée.

3. La règle 3 s'applique uniquement aux objets qui correspondent au préfixe `category3` /. Le `Expiration` le paramètre spécifie que toutes les versions non actuelles des objets correspondants expireront 50 jours après être devenues non actuelles.

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

Appliquer la configuration du cycle de vie au bucket

Après avoir créé le fichier de configuration du cycle de vie, vous l'appliquez à un bucket en émettant une requête PutBucketLifecycleConfiguration.

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

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

Pour valider qu'une configuration de cycle de vie a été correctement appliquée au bucket, émettez une demande GetBucketLifecycleConfiguration. Par exemple:

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

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

Valider que l'expiration du cycle de vie du bucket s'applique à l'objet

Vous pouvez déterminer si une règle d'expiration dans la configuration du cycle de vie s'applique à un objet spécifique lors de l'émission d'une demande PutObject, HeadObject ou GetObject. Si une règle s'applique, la réponse comprend une `Expiration` paramètre qui indique quand l'objet expire et quelle règle d'expiration a été respectée.

> Étant donné que le cycle de vie du bucket remplace ILM, le `expiry-date` la date réelle à laquelle l'objet sera supprimé est indiquée. Pour plus de détails, consultez la section "Comment la rétention d'objet est déterminée" .

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

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

La réponse de réussite indique que l'objet expirera dans 100 jours (1er octobre 2020) et qu'il correspond à la règle 2 de la configuration du cycle de vie.

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

Par exemple, cette requête HeadObject a été utilisée pour obtenir des métadonnées pour le même objet dans le bucket testbucket.

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

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

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

Pour les buckets avec contrôle de version activé, le `x-amz-expiration` l'en-tête de réponse s'applique uniquement aux versions actuelles des objets.

Recommandations pour la mise en œuvre de l'API REST S3

Vous devez suivre ces recommandations lors de l'implémentation de l'API REST S3 à utiliser avec StorageGRID.

Recommandations pour les HEADs vers des objets inexistants

Si votre application vérifie régulièrement si un objet existe dans un chemin où vous ne vous attendez pas à ce que l'objet existe réellement, vous devez utiliser l'option « Disponible »."cohérence" . Par exemple, vous devez utiliser la cohérence « Disponible » si votre application HEAD un emplacement avant d'y effectuer un PUT.

Dans le cas contraire, si l'opération HEAD ne trouve pas l'objet, vous risquez de recevoir un nombre élevé d'erreurs de serveur interne 500 si deux ou plusieurs nœuds de stockage sur le même site ne sont pas disponibles ou si un site distant est inaccessible.

Vous pouvez définir la cohérence « Disponible » pour chaque bucket à l'aide de l'"Cohérence du seau PUT" demande, ou vous pouvez spécifier la cohérence dans l'en-tête de demande pour une opération API individuelle.

Recommandations pour les clés d'objet

Suivez ces recommandations pour les noms de clés d'objet, en fonction de la date de création initiale du bucket.

Buckets créés dans StorageGRID 11.4 ou version antérieure

- N’utilisez pas de valeurs aléatoires comme quatre premiers caractères des clés d’objet. Ceci est en contraste avec l’ancienne recommandation AWS pour les préfixes de clé. Utilisez plutôt des préfixes non aléatoires et non uniques, tels que `image` .
- Si vous suivez l’ancienne recommandation AWS d’utiliser des caractères aléatoires et uniques dans les préfixes de clé, préfixez les clés d’objet avec un nom de répertoire. C’est-à-dire, utilisez ce format :

  `mybucket/mydir/f8e3-image3132.jpg`

  Au lieu de ce format :

  `mybucket/f8e3-image3132.jpg`

Buckets créés dans StorageGRID 11.4 ou version ultérieure

Il n’est pas nécessaire de restreindre les noms de clés d’objet pour respecter les meilleures pratiques en matière de performances. Dans la plupart des cas, vous pouvez utiliser des valeurs aléatoires pour les quatre premiers caractères des noms de clés d’objet.

Une exception à cette règle est une charge de travail S3 qui supprime en continu tous les objets après une courte période de temps. Pour minimiser l’impact sur les performances de ce cas d’utilisation, faites varier une partie initiale du nom de la clé tous les plusieurs milliers d’objets avec quelque chose comme la date. Par exemple, supposons qu’un client S3 écrit généralement 2 000 objets/seconde et que la politique de cycle de vie ILM ou bucket supprime tous les objets après trois jours. Pour minimiser l’impact sur les performances, vous pouvez nommer les clés en utilisant un modèle comme celui-ci : `/mybucket/mydir/`*`yyyymmddhhmmss-random_UUID`*`.jpg`

Recommandations pour les « lectures de plage »

Si le"option globale pour compresser les objets stockés" est activé, les applications clientes S3 doivent éviter d’effectuer des opérations GetObject qui spécifient une plage d’octets à renvoyer. Ces opérations de « lecture de plage » sont inefficaces car StorageGRID doit décompresser efficacement les objets pour accéder aux octets demandés. Les opérations GetObject qui demandent une petite plage d’octets à partir d’un très grand objet sont particulièrement inefficaces ; par exemple, il est inefficace de lire une plage de 10 Mo à partir d’un objet compressé de 50 Go.

Si les plages sont lues à partir d’objets compressés, les demandes des clients peuvent expirer.

Si vous devez compresser des objets et que votre application cliente doit utiliser des lectures de plage, augmentez le délai d’expiration de lecture pour l’application.

Prise en charge de l’API REST Amazon S3

Détails d’implémentation de l’API REST S3

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

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

type chemin.

Gestion des dates

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

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

En-têtes de requête courants

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

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

En-têtes de réponse courants

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

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

Authentifier les demandes

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

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

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

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

Utiliser l'en-tête d'autorisation HTTP

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

Utiliser les paramètres de requête

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

Opérations sur le service

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

Opération	Mise en œuvre
Listes de seaux (anciennement nommé service GET)	Implémenté avec tous les comportements de l'API REST Amazon S3. Sous réserve de modifications sans préavis.
Utilisation du stockage GET	Le StorageGRID"Utilisation du stockage GET" La demande vous indique la quantité totale de stockage utilisée par un compte et pour chaque compartiment associé au compte. Il s'agit d'une opération sur le service avec un chemin de / et un paramètre de requête personnalisé(`?x-ntap-sg-usage`) ajouté.
OPTIONS /	Les applications clientes peuvent émettre `OPTIONS /` demandes adressées au port S3 sur un nœud de stockage, sans fournir les informations d'identification d'authentification S3, pour déterminer si le nœud de stockage est disponible. Vous pouvez utiliser cette demande pour la surveillance ou pour permettre aux équilibreurs de charge externes d'identifier quand un nœud de stockage est en panne.

Opérations sur les godets

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

Chaque grille peut contenir un maximum de 100 000 buckets.

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

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

Pour plus d'informations, voir les éléments suivants :

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

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

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

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

Opération	Mise en œuvre
Créer un bucket	Crée un nouveau bucket. En créant le bucket, vous devenez le propriétaire du bucket. • Les noms de bucket doivent respecter les règles suivantes : ◦ Doit être unique sur chaque système StorageGRID (pas seulement unique au sein du compte locataire). ◦ Doit être conforme au DNS. ◦ Doit contenir au moins 3 et pas plus de 63 caractères. ◦ Peut être une série d'une ou plusieurs étiquettes, avec des étiquettes adjacentes séparées par un point. Chaque étiquette doit commencer et se terminer par une lettre minuscule ou un chiffre et ne peut utiliser que des lettres minuscules, des chiffres et des traits d'union. ◦ Ne doit pas ressembler à une adresse IP au format texte. ◦ Ne doit pas utiliser de points dans les requêtes de style hébergé virtuellement. Les points entraîneront des problèmes avec la vérification du certificat générique du serveur. • Par défaut, les buckets sont créés dans le `us-east-1` région; cependant, vous pouvez utiliser le `LocationConstraint` élément de demande dans le corps de la demande pour spécifier une région différente. Lors de l'utilisation du `LocationConstraint` élément, vous devez spécifier le nom exact d'une région qui a été définie à l'aide du gestionnaire de grille ou de l'API de gestion de grille. Contactez votre administrateur système si vous ne connaissez pas le nom de la région à utiliser. **Remarque** : une erreur se produira si votre demande CreateBucket utilise une région qui n'a pas été définie dans StorageGRID. • Vous pouvez inclure le `x-amz-bucket-object-lock-enabled` en-tête de demande pour créer un bucket avec S3 Object Lock activé. Voir "Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3" . Vous devez activer le verrouillage d'objet S3 lorsque vous créez le bucket. Vous ne pouvez pas ajouter ou désactiver le verrouillage d'objet S3 après la création d'un bucket. S3 Object Lock nécessite le contrôle de version du bucket, qui est activé automatiquement lorsque vous créez le bucket.
Supprimer le bucket	Supprime le bucket.
SupprimerBucketCors	Supprime la configuration CORS pour le bucket.
Supprimer le chiffrement du bucket	Supprime le cryptage par défaut du bucket. Les objets chiffrés existants restent chiffrés, mais tous les nouveaux objets ajoutés au bucket ne sont pas chiffrés.
Supprimer le cycle de vie du bucket	Supprime la configuration du cycle de vie du bucket. Voir "Créer une configuration du cycle de vie S3" .

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

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

Opération	Mise en œuvre
PutBucketCors	Définit la configuration CORS pour un bucket afin que celui-ci puisse traiter les demandes inter-origines. Le partage de ressources inter-origines (CORS) est un mécanisme de sécurité qui permet aux applications Web clientes d'un domaine d'accéder aux ressources d'un domaine différent. Par exemple, supposons que vous utilisiez un bucket S3 nommé `images` pour stocker des graphiques. En définissant la configuration CORS pour le `images` bucket, vous pouvez autoriser l'affichage des images de ce bucket sur le site Web `http://www.example.com` .
Cryptage PutBucket	Définit l'état de cryptage par défaut d'un bucket existant. Lorsque le chiffrement au niveau du bucket est activé, tout nouvel objet ajouté au bucket est chiffré. StorageGRID prend en charge le chiffrement côté serveur avec des clés gérées par StorageGRID. Lors de la spécification de la règle de configuration de chiffrement côté serveur, définissez le `SSEAlgorithm` paramètre à `AES256` , et n'utilisez pas le `KMSMasterKeyID` paramètre. La configuration de chiffrement par défaut du bucket est ignorée si la demande de téléchargement d'objet spécifie déjà le chiffrement (c'est-à-dire si la demande inclut le `x-amz-server-side-encryption-*` en-tête de requête).
Configuration du cycle de vie de PutBucket (anciennement appelé cycle de vie du bucket PUT)	Crée une nouvelle configuration de cycle de vie pour le bucket ou remplace une configuration de cycle de vie existante. StorageGRID prend en charge jusqu'à 1 000 règles de cycle de vie dans une configuration de cycle de vie. Chaque règle peut inclure les éléments XML suivants : • Expiration (jours, date, ExpiredObjectDeleteMarker) • NoncurrentVersionExpiration (NewerNoncurrentVersions, NoncurrentDays) • Filtre (préfixe, balise) • Statut • ID StorageGRID ne prend pas en charge ces actions : • AbandonnerTéléchargement multi-parties incomplet • Transition Voir "Créer une configuration du cycle de vie S3" . Pour comprendre comment l'action Expiration dans un cycle de vie de bucket interagit avec les instructions de placement ILM, voir"Comment ILM fonctionne tout au long de la vie d'un objet" . **Remarque** : la configuration du cycle de vie du bucket peut être utilisée avec les buckets pour lesquels le verrouillage d'objet S3 est activé, mais la configuration du cycle de vie du bucket n'est pas prise en charge pour les buckets conformes hérités.

Opération	Mise en œuvre

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

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

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

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

Opérations sur les objets

Opérations sur les objets

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

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

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

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

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

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

Opération	Mise en œuvre
PutObjectRetention	"Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3"
Balisage d'objets	Utilise le `tagging` sous-ressource pour ajouter un ensemble de balises à un objet existant. **Limites des balises d'objet** Vous pouvez ajouter des balises aux nouveaux objets lorsque vous les téléchargez, ou vous pouvez les ajouter aux objets existants. StorageGRID et Amazon S3 prennent en charge jusqu'à 10 balises pour chaque objet. Les balises associées à un objet doivent avoir des clés de balise uniques. Une clé de balise peut contenir jusqu'à 128 caractères Unicode et les valeurs de balise peuvent contenir jusqu'à 256 caractères Unicode. La clé et les valeurs sont sensibles à la casse. **Mises à jour des balises et comportement d'ingestion** Lorsque vous utilisez PutObjectTagging pour mettre à jour les balises d'un objet, StorageGRID ne réingère pas l'objet. Cela signifie que l'option pour le comportement d'ingestion spécifiée dans la règle ILM correspondante n'est pas utilisée. Toutes les modifications apportées au placement des objets déclenchées par la mise à jour sont effectuées lorsque ILM est réévalué par les processus ILM d'arrière-plan normaux. Cela signifie que si la règle ILM utilise l'option Strict pour le comportement d'ingestion, aucune action n'est entreprise si les placements d'objets requis ne peuvent pas être effectués (par exemple, parce qu'un emplacement nouvellement requis n'est pas disponible). L'objet mis à jour conserve son emplacement actuel jusqu'à ce que le placement requis soit possible. **Résoudre les conflits** Les demandes client conflictuelles, telles que deux clients écrivant sur la même clé, sont résolues sur la base des « derniers gagnants ». Le moment de l'évaluation des « dernières victoires » est basé sur le moment où le système StorageGRID termine une demande donnée, et non sur le moment où les clients S3 commencent une opération. **Gestion des versions** Si le `versionId` le paramètre de requête n'est pas spécifié dans la requête, l'opération ajoute des balises à la version la plus récente de l'objet dans un bucket versionné. Si la version actuelle de l'objet est un marqueur de suppression, un statut « MethodNotAllowed » est renvoyé avec le `x-amz-delete-marker` en-tête de réponse défini sur `true` .
Sélectionner le contenu de l'objet	"Sélectionner le contenu de l'objet"

Utiliser S3 Select

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

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

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

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

Clauses

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

Types de données

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

Opérateurs

Opérateurs logiques

- ET
- PAS
- OU

Opérateurs de comparaison

- <
- >
- ⇐
- >=
- =
- =
- <>

- !=
- ENTRE
- DANS

Opérateurs de recherche de motifs

- COMME
- _
- %

opérateurs unitaires

- EST NUL
- N'EST PAS NUL

opérateurs mathématiques

- +
- -
- *
- /
- %

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

Fonctions d'agrégation

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

Fonctions conditionnelles

- CAS
- SE FONDRE
- NULLIF

Fonctions de conversion

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

Fonctions de date

- DATE_ADD
- DATE_DIFF

- EXTRAIT
- TO_STRING
- À_HORODATAGE
- UTCNOW

Fonctions de chaîne

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

Utiliser le cryptage côté serveur

Le chiffrement côté serveur vous permet de protéger vos données d'objet au repos. StorageGRID crypte les données lorsqu'il écrit l'objet et décrypte les données lorsque vous accédez à l'objet.

Si vous souhaitez utiliser le chiffrement côté serveur, vous pouvez choisir l'une des deux options mutuellement exclusives, en fonction de la manière dont les clés de chiffrement sont gérées :

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

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

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

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

Utiliser SSE

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

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

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

- "Mettre l'objet"

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

Utiliser SSE-C

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

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

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

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

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

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

- Vous devez utiliser https.

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

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

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

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

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

Informations connexes

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

Copier l'objet

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

Résoudre les conflits

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

Taille de l'objet

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

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

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

Caractères UTF-8 dans les métadonnées utilisateur

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

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

- Les requêtes réussissent si les métadonnées définies par l'utilisateur incluent des caractères UTF-8 échappés.

- StorageGRID ne renvoie pas le `x-amz-missing-meta` en-tête si la valeur interprétée du nom ou de la valeur de la clé inclut des caractères non imprimables.

En-têtes de requête pris en charge

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

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

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

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

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

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

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

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

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

  VoirEn-têtes de requête pour le chiffrement côté serveur

En-têtes de requête non pris en charge

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

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

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

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

Options de classe de stockage

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

- `STANDARD`

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

- `REDUCED_REDUNDANCY`

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

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

Utilisation de x-amz-copy-source dans CopyObject

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

Si la source et la destination correspondent, et que le `x-amz-metadata-directive` l'en-tête est spécifié

comme `REPLACE` , les métadonnées de l'objet sont mises à jour avec les valeurs de métadonnées fournies dans la demande. Dans ce cas, StorageGRID ne réingère pas l'objet. Cela a deux conséquences importantes :

- Vous ne pouvez pas utiliser CopyObject pour crypter un objet existant sur place ou pour modifier le cryptage d'un objet existant sur place. Si vous fournissez le `x-amz-server-side-encryption` en-tête ou le `x-amz-server-side-encryption-customer-algorithm` en-tête, StorageGRID rejette la demande et renvoie `XNotImplemented` .
- L'option pour le comportement d'ingestion spécifiée dans la règle ILM correspondante n'est pas utilisée. Toutes les modifications apportées au placement des objets déclenchées par la mise à jour sont effectuées lorsque ILM est réévalué par les processus ILM d'arrière-plan normaux.

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

En-têtes de requête pour le chiffrement côté serveur

Si tu"utiliser le cryptage côté serveur" , les en-têtes de requête que vous fournissez dépendent du fait que l'objet source est chiffré ou non et du fait que vous prévoyez de chiffrer l'objet cible.

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

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

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

Gestion des versions

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

Obtenir l'objet

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

GetObject et objets multipartites

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

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

Caractères UTF-8 dans les métadonnées utilisateur

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

En-tête de requête pris en charge

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

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

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

En-tête de requête non pris en charge

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

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

Gestion des versions

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

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

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

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

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

Comportement de GetObject pour les objets Cloud Storage Pool

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

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

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

Objets multipartites ou segmentés dans un pool de stockage cloud

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

Dans ces cas :

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

GetObject et réplication inter-grille

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

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

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

HeadObject

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

HeadObject et objets multipartites

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

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

Caractères UTF-8 dans les métadonnées utilisateur

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

définies par l'utilisateur ne renvoient pas le `x-amz-missing-meta` en-tête si le nom ou la valeur de la clé inclut des caractères non imprimables.

En-tête de requête pris en charge

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

- `x-amz-checksum-mode`

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

En-tête de requête non pris en charge

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

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

Gestion des versions

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

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

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

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

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

Réponses HeadObject pour les objets Cloud Storage Pool

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

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

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

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

Objet dans le pool de stockage cloud, mais pas encore passé à un état non récupérable	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"`
	
	Jusqu'à ce que l'objet soit transféré vers un état non récupérable, la valeur de `expiry-date` se déroule à une époque lointaine dans le futur. L'heure exacte de la transition n'est pas contrôlée par le système StorageGRID .

L'objet est passé à un état non récupérable, mais au moins une copie existe également sur la grille	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"`
	
	La valeur pour `expiry-date` se déroule à une époque lointaine dans le futur.
	
	Remarque : Si la copie sur la grille n'est pas disponible (par exemple, un nœud de stockage est en panne), vous devez émettre un"Restaurer l'objet" demandez à restaurer la copie à partir du pool de stockage cloud avant de pouvoir récupérer l'objet avec succès.

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

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

État de l'objet	Réponse à HeadObject

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

Objets multipartites ou segmentés dans le pool de stockage cloud

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

Réplication HeadObject et inter-grille

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

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

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

Mettre l'objet

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

Résoudre les conflits

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

opération.

Taille de l'objet

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

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

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

Taille des métadonnées utilisateur

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

Caractères UTF-8 dans les métadonnées utilisateur

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

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

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

Limites des balises d'objet

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

Propriété de l'objet

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

En-têtes de requête pris en charge

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

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

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

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

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

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

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

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

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

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

  > Une règle ILM ne peut pas utiliser à la fois une **heure de création définie par l'utilisateur** pour l'heure de référence et l'option d'ingestion équilibrée ou stricte. Une erreur est renvoyée lors de la création de la règle ILM.
- `x-amz-tagging`
- En-têtes de demande de verrouillage d'objet S3

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

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

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

    VoirEn-têtes de requête pour le chiffrement côté serveur

En-têtes de requête non pris en charge

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

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

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

Options de classe de stockage

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

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

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

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

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

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

- `REDUCED_REDUNDANCY`

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

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

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

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

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

En-têtes de requête pour le chiffrement côté serveur

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

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

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

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

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

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

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

Gestion des versions

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

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

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

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

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

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

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

Informations connexes

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

Restaurer l'objet

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

Type de demande pris en charge

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

Gestion des versions

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

Comportement de RestoreObject sur les objets du pool de stockage cloud

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

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

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

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

Sélectionner le contenu de l'objet

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

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

Avant de commencer

- Le compte locataire dispose de l'autorisation S3 Select.
- Tu as `s3:GetObject` autorisation pour l'objet que vous souhaitez interroger.
- L'objet que vous souhaitez interroger doit être dans l'un des formats suivants :
  - **CSV**. Peut être utilisé tel quel ou compressé dans des archives GZIP ou BZIP2.
  - **Parquet**. Exigences supplémentaires pour les objets Parquet :
    - S3 Select prend uniquement en charge la compression en colonnes à l'aide de GZIP ou Snappy. S3 Select ne prend pas en charge la compression d'objets entiers pour les objets Parquet.
    - S3 Select ne prend pas en charge la sortie Parquet. Vous devez spécifier le format de sortie au format CSV ou JSON.
    - La taille maximale du groupe de lignes non compressé est de 512 Mo.
    - Vous devez utiliser les types de données spécifiés dans le schéma de l'objet.
    - Vous ne pouvez pas utiliser les types logiques INTERVAL, JSON, LIST, TIME ou UUID.
- Votre expression SQL a une longueur maximale de 256 Ko.
- Tout enregistrement dans l'entrée ou les résultats a une longueur maximale de 1 Mio.

Exemple de syntaxe de requête CSV

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

Exemple de syntaxe de demande de parquet

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

Exemple de requête SQL

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

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

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

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

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

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

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

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

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

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

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

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

Opérations pour les téléchargements en plusieurs parties

Opérations pour les téléchargements en plusieurs parties

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

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

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

peuvent ne pas répondre aux exigences ILM actuelles une fois le téléchargement multipartie terminé. Toute pièce qui n'est pas placée correctement est mise en file d'attente pour une réévaluation ILM et déplacée vers l'emplacement correct ultérieurement.

    - Lors de l'évaluation de l'ILM pour une pièce, StorageGRID filtre sur la taille de la pièce, et non sur la taille de l'objet. Cela signifie que des parties d'un objet peuvent être stockées dans des emplacements qui ne répondent pas aux exigences ILM pour l'objet dans son ensemble. Par exemple, si une règle spécifie que tous les objets de 10 Go ou plus sont stockés sur DC1 tandis que tous les objets plus petits sont stockés sur DC2, chaque partie de 1 Go d'un téléchargement multipartie en 10 parties est stockée sur DC2 lors de l'ingestion. Cependant, lorsque l'ILM est évalué pour l'objet dans son ensemble, toutes les parties de l'objet sont déplacées vers DC1.

- Toutes les opérations de téléchargement en plusieurs parties prennent en charge StorageGRID"valeurs de cohérence" .
- Lorsqu'un objet est ingéré à l'aide d'un téléchargement en plusieurs parties, le"seuil de segmentation des objets (1 Gio)" n'est pas appliqué.
- Selon vos besoins, vous pouvez utiliser"chiffrement côté serveur" avec des téléchargements en plusieurs parties. Pour utiliser SSE (chiffrement côté serveur avec clés gérées par StorageGRID), vous incluez le `x-amz-server-side-encryption` en-tête de demande dans la demande CreateMultipartUpload uniquement. Pour utiliser SSE-C (chiffrement côté serveur avec clés fournies par le client), vous spécifiez les trois mêmes en-têtes de demande de clé de chiffrement dans la demande CreateMultipartUpload et dans chaque demande UploadPart ultérieure.

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

Téléchargement complet en plusieurs parties

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

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

Résoudre les conflits

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

En-têtes de requête pris en charge

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

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

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

- `STANDARD`

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

- `REDUCED_REDUNDANCY`

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

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

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

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

En-têtes de requête non pris en charge

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

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

Gestion des versions

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

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

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

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

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

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

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

"Dépanner les services de la plateforme" .

Créer un téléchargement multi-parties

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

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

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

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

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

devront peut-être être réalisées à des emplacements différents et les copies intermédiaires initiales devront peut-être être supprimées.

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

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

- `REDUCED_REDUNDANCY`

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

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

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

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

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

En-têtes de requête pris en charge

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- En-têtes de requête SSE :

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

    En-têtes de requête pour le chiffrement côté serveur

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

En-têtes de requête pour le chiffrement côté serveur

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

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

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

En-têtes de requête non pris en charge

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

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

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

Gestion des versions

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

ListeMultipartUploads

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

Les paramètres de requête suivants sont pris en charge :

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

- `Authorization`

Gestion des versions

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

Télécharger une partie

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

En-têtes de requête pris en charge

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

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

En-têtes de requête pour le chiffrement côté serveur

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

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

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

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

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

En-têtes de requête non pris en charge

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

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

Gestion des versions

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

TéléchargerPartCopy

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

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

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

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

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

En-têtes de requête pour le chiffrement côté serveur

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

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

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

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

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

Gestion des versions

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

Réponses d'erreur

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

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

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

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

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

Codes d'erreur personnalisés StorageGRID

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

Opérations personnalisées StorageGRID

Opérations personnalisées StorageGRID

Le système StorageGRID prend en charge les opérations personnalisées qui sont ajoutées à l'API REST S3.

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

Opération	Description
"Cohérence du bucket GET"	Renvoie la cohérence appliquée à un bucket particulier.
"Cohérence du seau PUT"	Définit la cohérence appliquée à un bucket particulier.
"Heure du dernier accès au bucket GET"	Renvoie si les dernières mises à jour de l'heure d'accès sont activées ou désactivées pour un bucket particulier.
"Heure du dernier accès au bucket PUT"	Vous permet d'activer ou de désactiver les mises à jour de l'heure du dernier accès pour un bucket particulier.
"SUPPRIMER la configuration de notification des métadonnées du bucket"	Supprime la configuration XML de notification de métadonnées associée à un bucket particulier.
"Configuration de la notification des métadonnées du bucket GET"	Renvoie la configuration XML de notification de métadonnées associée à un bucket particulier.
"Configuration des notifications de métadonnées du compartiment PUT"	Configure le service de notification de métadonnées pour un bucket.
"Utilisation du stockage GET"	Vous indique la quantité totale de stockage utilisée par un compte et pour chaque bucket associé au compte.
"Obsolète : CreateBucket avec paramètres de conformité"	Obsolète et non pris en charge : vous ne pouvez plus créer de nouveaux buckets avec la conformité activée.
"Obsolète : conformité du bucket GET"	Obsolète mais pris en charge : renvoie les paramètres de conformité actuellement en vigueur pour un bucket conforme hérité existant.
"Obsolète : conformité du compartiment PUT"	Obsolète mais pris en charge : vous permet de modifier les paramètres de conformité d'un bucket conforme hérité existant.

Cohérence du bucket GET

La demande de cohérence GET Bucket vous permet de déterminer la cohérence appliquée à un bucket particulier.

La cohérence par défaut est définie pour garantir la lecture après écriture des objets nouvellement créés.

Vous devez disposer de l'autorisation s3:GetBucketConsistency ou être root du compte pour terminer cette opération.

Exemple de demande

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

Réponse

Dans la réponse XML, `<Consistency>` renverra l'une des valeurs suivantes :

Cohérence	Description
tous	Tous les nœuds reçoivent les données immédiatement, sinon la demande échouera.
fort-mondial	Garantit la cohérence de lecture après écriture pour toutes les demandes client sur tous les sites.
site fort	Garantit la cohérence de lecture après écriture pour toutes les demandes client au sein d'un site.
lecture après nouvelle écriture	(Par défaut) Fournit une cohérence de lecture après écriture pour les nouveaux objets et une cohérence éventuelle pour les mises à jour d'objets. Offre des garanties de haute disponibilité et de protection des données. Recommandé dans la plupart des cas.
disponible	Assure une cohérence éventuelle pour les nouveaux objets et les mises à jour d'objets. Pour les buckets S3, utilisez-les uniquement si nécessaire (par exemple, pour un bucket contenant des valeurs de journal rarement lues ou pour des opérations HEAD ou GET sur des clés qui n'existent pas). Non pris en charge pour les buckets S3 FabricPool .

Exemple de réponse

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

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

Informations connexes

"Valeurs de cohérence"

Cohérence du seau PUT

La demande de cohérence PUT Bucket vous permet de spécifier la cohérence à appliquer aux opérations effectuées sur un bucket.

La cohérence par défaut est définie pour garantir la lecture après écriture des objets nouvellement créés.

Avant de commencer

Vous devez disposer de l'autorisation s3:PutBucketConsistency ou être root du compte pour terminer cette opération.

Demande

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

Cohérence	Description
tous	Tous les nœuds reçoivent les données immédiatement, sinon la demande échouera.
fort-mondial	Garantit la cohérence de lecture après écriture pour toutes les demandes client sur tous les sites.
site fort	Garantit la cohérence de lecture après écriture pour toutes les demandes client au sein d'un site.
lecture après nouvelle écriture	(Par défaut) Fournit une cohérence de lecture après écriture pour les nouveaux objets et une cohérence éventuelle pour les mises à jour d'objets. Offre des garanties de haute disponibilité et de protection des données. Recommandé dans la plupart des cas.

Cohérence	Description
disponible	Assure une cohérence éventuelle pour les nouveaux objets et les mises à jour d'objets. Pour les buckets S3, utilisez-les uniquement si nécessaire (par exemple, pour un bucket contenant des valeurs de journal rarement lues ou pour des opérations HEAD ou GET sur des clés qui n'existent pas). Non pris en charge pour les buckets S3 FabricPool .

Remarque : En général, vous devez utiliser la cohérence « Lecture après nouvelle écriture ». Si les requêtes ne fonctionnent pas correctement, modifiez le comportement du client de l'application si possible. Ou configurez le client pour spécifier la cohérence de chaque demande d'API. Définissez la consistance au niveau du seau uniquement en dernier recours.

Exemple de demande

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

Informations connexes

"Valeurs de cohérence"

Heure du dernier accès au bucket GET

La demande d'heure du dernier accès au bucket GET vous permet de déterminer si les mises à jour de l'heure du dernier accès sont activées ou désactivées pour les buckets individuels.

Vous devez disposer de l'autorisation s3:GetBucketLastAccessTime ou être root du compte pour terminer cette opération.

Exemple de demande

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

Exemple de réponse

Cet exemple montre que les mises à jour de l'heure du dernier accès sont activées pour le bucket.

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

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

Heure du dernier accès au bucket PUT

La demande d'heure du dernier accès au bucket PUT vous permet d'activer ou de désactiver les mises à jour de l'heure du dernier accès pour des buckets individuels. La désactivation des mises à jour de l'heure du dernier accès améliore les performances et constitue le paramètre par défaut pour tous les buckets créés avec la version 10.3.0 ou ultérieure.

Vous devez disposer de l'autorisation s3:PutBucketLastAccessTime pour un bucket ou être root du compte pour terminer cette opération.

> ⓘ À partir de la version 10.3 de StorageGRID , les mises à jour de l'heure du dernier accès sont désactivées par défaut pour tous les nouveaux buckets. Si vous disposez de buckets créés à l'aide d'une version antérieure de StorageGRID et que vous souhaitez appliquer le nouveau comportement par défaut, vous devez désactiver explicitement les mises à jour de l'heure du dernier accès pour chacun de ces buckets antérieurs. Vous pouvez activer ou désactiver les mises à jour de l'heure du dernier accès à l'aide de la demande d'heure du dernier accès au bucket PUT ou à partir de la page de détails d'un bucket dans le gestionnaire de locataires. Voir "Activer ou désactiver les mises à jour de l'heure du dernier accès" .

Si les mises à jour de l'heure du dernier accès sont désactivées pour un bucket, le comportement suivant est appliqué aux opérations sur le bucket :

- Les requêtes GetObject, GetObjectAcl, GetObjectTagging et HeadObject ne mettent pas à jour l'heure du dernier accès. L'objet n'est pas ajouté aux files d'attente pour l'évaluation de la gestion du cycle de vie des informations (ILM).
- Les requêtes CopyObject et PutObjectTagging qui mettent à jour uniquement les métadonnées mettent également à jour l'heure du dernier accès. L'objet est ajouté aux files d'attente pour l'évaluation ILM.
- Si les mises à jour de l'heure du dernier accès sont désactivées pour le bucket source, les demandes CopyObject ne mettent pas à jour l'heure du dernier accès pour le bucket source. L'objet qui a été copié n'est pas ajouté aux files d'attente pour l'évaluation ILM pour le bucket source. Cependant, pour la destination, les demandes CopyObject mettent toujours à jour l'heure du dernier accès. La copie de l'objet est ajoutée aux files d'attente pour l'évaluation ILM.
- Les demandes CompleteMultipartUpload mettent à jour l'heure du dernier accès. L'objet terminé est ajouté aux files d'attente pour l'évaluation ILM.

Exemples de demandes

Cet exemple active l'heure du dernier accès à un bucket.

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

Cet exemple désactive l'heure du dernier accès à un bucket.

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

SUPPRIMER la configuration de notification des métadonnées du bucket

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

Vous devez disposer de l'autorisation s3:DeleteBucketMetadataNotification pour un bucket ou être root du compte pour terminer cette opération.

Exemple de demande

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

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

Configuration de la notification des métadonnées du bucket GET

La demande de configuration de notification de métadonnées GET Bucket vous permet de récupérer le XML de configuration utilisé pour configurer l'intégration de la recherche pour des buckets individuels.

Vous devez disposer de l'autorisation s3:GetBucketMetadataNotification ou être root du compte pour terminer cette opération.

Exemple de demande

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

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

Réponse

Le corps de la réponse inclut la configuration de notification de métadonnées pour le bucket. La configuration de notification des métadonnées vous permet de déterminer comment le bucket est configuré pour l'intégration de la recherche. Autrement dit, il vous permet de déterminer quels objets sont indexés et à quels points de terminaison leurs métadonnées d'objet sont envoyées.

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

Chaque configuration de notification de métadonnées comprend une ou plusieurs règles. Chaque règle spécifie les objets auxquels elle s'applique et la destination vers laquelle StorageGRID doit envoyer les métadonnées de l'objet. Les destinations doivent être spécifiées à l'aide de l'URN d'un point de terminaison StorageGRID .

Nom	Description	Obligatoire
Configuration des notifications de métadonnées	Balise de conteneur pour les règles utilisées pour spécifier les objets et la destination des notifications de métadonnées. Contient un ou plusieurs éléments de règle.	Oui

Nom	Description	Obligatoire
Règle	Balise de conteneur pour une règle qui identifie les objets dont les métadonnées doivent être ajoutées à un index spécifié. Les règles avec des préfixes qui se chevauchent sont rejetées. Inclus dans l'élément MetadataNotificationConfiguration.	Oui
ID	Identifiant unique de la règle. Inclus dans l'élément Règle.	Non
Statut	Le statut peut être « Activé » ou « Désactivé ». Aucune action n'est entreprise pour les règles désactivées. Inclus dans l'élément Règle.	Oui
Préfixe	Les objets qui correspondent au préfixe sont affectés par la règle et leurs métadonnées sont envoyées à la destination spécifiée. Pour faire correspondre tous les objets, spécifiez un préfixe vide. Inclus dans l'élément Règle.	Oui
Destination	Balise de conteneur pour la destination d'une règle. Inclus dans l'élément Règle.	Oui

Nom	Description	Obligatoire
Urne	URN de la destination où les métadonnées de l'objet sont envoyées. Doit être l'URN d'un point de terminaison StorageGRID avec les propriétés suivantes : • `es`doit être le troisième élément. • L'URN doit se terminer par l'index et le type où les métadonnées sont stockées, sous la forme `domain-name/myindex/mytype` . Les points de terminaison sont configurés à l'aide de l'API Tenant Manager ou Tenant Management. Ils prennent la forme suivante : • `arn:aws:es:_region:account-ID_:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` Le point de terminaison doit être configuré avant que le XML de configuration ne soit soumis, sinon la configuration échouera avec une erreur 404. L'urne est incluse dans l'élément Destination.	Oui

Exemple de réponse

Le XML inclus entre le `<MetadataNotificationConfiguration></MetadataNotificationConfiguration>` Les balises montrent comment l'intégration avec un point de terminaison d'intégration de recherche est configurée pour le bucket. Dans cet exemple, les métadonnées de l'objet sont envoyées à un index Elasticsearch nommé `current` et le type nommé `2017` qui est hébergé dans un domaine AWS nommé `records` .

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

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

Informations connexes

"Utiliser un compte locataire"

Configuration des notifications de métadonnées du compartiment PUT

La demande de configuration de notification des métadonnées PUT Bucket vous permet d'activer le service d'intégration de recherche pour des buckets individuels. La configuration XML de notification de métadonnées que vous fournissez dans le corps de la demande spécifie les objets dont les métadonnées sont envoyées à l'index de recherche de destination.

Vous devez disposer de l'autorisation s3:PutBucketMetadataNotification pour un bucket ou être root du compte pour terminer cette opération.

Demande

La demande doit inclure la configuration de notification des métadonnées dans le corps de la demande. Chaque configuration de notification de métadonnées comprend une ou plusieurs règles. Chaque règle spécifie les objets auxquels elle s'applique et la destination vers laquelle StorageGRID doit envoyer les métadonnées de l'objet.

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

Les configurations dont les préfixes se chevauchent ne sont pas valides et sont rejetées lorsqu'elles sont soumises. Par exemple, une configuration qui incluait une règle pour les objets avec le préfixe `test` et une deuxième règle pour les objets avec le préfixe `test2` ne serait pas autorisé.

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

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

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

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

Nom	Description	Obligatoire
Statut	Le statut peut être « Activé » ou « Désactivé ». Aucune action n'est entreprise pour les règles désactivées. Inclus dans l'élément Règle.	Oui
Préfixe	Les objets qui correspondent au préfixe sont affectés par la règle et leurs métadonnées sont envoyées à la destination spécifiée. Pour faire correspondre tous les objets, spécifiez un préfixe vide. Inclus dans l'élément Règle.	Oui
Destination	Balise de conteneur pour la destination d'une règle. Inclus dans l'élément Règle.	Oui
Urne	URN de la destination où les métadonnées de l'objet sont envoyées. Doit être l'URN d'un point de terminaison StorageGRID avec les propriétés suivantes : • `es`doit être le troisième élément. • L'URN doit se terminer par l'index et le type où les métadonnées sont stockées, sous la forme `domain-name/myindex/mytype` . Les points de terminaison sont configurés à l'aide de l'API Tenant Manager ou Tenant Management. Ils prennent la forme suivante : • `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` Le point de terminaison doit être configuré avant que le XML de configuration ne soit soumis, sinon la configuration échouera avec une erreur 404. L'urne est incluse dans l'élément Destination.	Oui

Exemples de demandes

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

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

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

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

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

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

JSON généré par le service d'intégration de recherche

Lorsque vous activez le service d'intégration de recherche pour un bucket, un document JSON est généré et envoyé au point de terminaison de destination chaque fois que des métadonnées ou des balises d'objet sont ajoutées, mises à jour ou supprimées.

Cet exemple montre un exemple de JSON qui pourrait être généré lorsqu'un objet avec la clé `SGWS/Tagging.txt` est créé dans un bucket nommé `test` . Le `test` le bucket n'est pas versionné, donc le `versionId` la balise est vide.

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

Métadonnées d'objet incluses dans les notifications de métadonnées

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

Le nom du document inclut le nom du bucket, le nom de l'objet et l'ID de version s'il est présent.

Type	Nom de l'article	Description
Informations sur le bucket et l'objet	seau	Nom du seau
Informations sur le bucket et l'objet	clé	Nom de la clé de l'objet
Informations sur le bucket et l'objet	ID de version	Version de l'objet, pour les objets dans les buckets versionnés
Informations sur le bucket et l'objet	région	Région de bucket, par exemple `us-east-1`
Métadonnées du système	taille	Taille de l'objet (en octets) telle que visible par un client HTTP
Métadonnées du système	md5	Hachage d'objet
Métadonnées de l'utilisateur	métadonnées *`key:value`*	Toutes les métadonnées utilisateur pour l'objet, sous forme de paires clé-valeur

Type	Nom de l'article	Description
Mots-clés	balises *key:value*	Toutes les balises d'objet définies pour l'objet, sous forme de paires clé-valeur

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

Informations connexes

"Utiliser un compte locataire"

Demande d'utilisation du stockage GET

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

La quantité de stockage utilisée par un compte et ses buckets peut être obtenue par une requête ListBuckets modifiée avec le `x-ntap-sg-usage` paramètre de requête. L'utilisation du stockage du bucket est suivie séparément des requêtes PUT et DELETE traitées par le système. Il peut y avoir un certain délai avant que les valeurs d'utilisation correspondent aux valeurs attendues en fonction du traitement des demandes, en particulier si le système est soumis à une charge importante.

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

Vous devez disposer de l'autorisation s3:ListAllMyBuckets ou être root du compte pour terminer cette opération.

Exemple de demande

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

Exemple de réponse

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

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

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

Gestion des versions

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

Informations connexes

"Valeurs de cohérence"

Demandes de bucket obsolètes pour la conformité héritée

Demandes de bucket obsolètes pour la conformité héritée

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

Fonctionnalité de conformité obsolète

La fonctionnalité de conformité StorageGRID disponible dans les versions précédentes de StorageGRID est obsolète et a été remplacée par S3 Object Lock.

Si vous avez précédemment activé le paramètre de conformité global, le paramètre de verrouillage d'objet S3 global est activé dans StorageGRID 11.6. Vous ne pouvez plus créer de nouveaux buckets avec la conformité activée ; toutefois, si nécessaire, vous pouvez utiliser l'API REST StorageGRID S3 pour gérer tous les buckets conformes existants.

- "Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3"
- "Gérer les objets avec ILM"
- "Base de connaissances NetApp : Gestion des buckets compatibles hérités dans StorageGRID 11.5"

Demandes de conformité obsolètes :

- "Obsolète - Modifications de la demande PUT Bucket pour la conformité"

  L'élément XML SGCompliance est obsolète. Auparavant, vous pouviez inclure cet élément personnalisé StorageGRID dans le corps de la requête XML facultatif des requêtes PUT Bucket pour créer un bucket conforme.

- "Obsolète - Conformité du bucket GET"

  La demande de conformité GET Bucket est obsolète. Toutefois, vous pouvez continuer à utiliser cette demande pour déterminer les paramètres de conformité actuellement en vigueur pour un bucket conforme hérité existant.

- "Obsolète - Conformité du compartiment PUT"

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

Obsolète : CreateBucket demande des modifications pour la conformité

L'élément XML SGCompliance est obsolète. Auparavant, vous pouviez inclure cet élément personnalisé StorageGRID dans le corps de la requête XML facultatif des requêtes CreateBucket pour créer un bucket conforme.

> La fonctionnalité de conformité StorageGRID disponible dans les versions précédentes de StorageGRID est obsolète et a été remplacée par S3 Object Lock. Voir ce qui suit pour plus de détails :
>
> - "Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3"
> - "Base de connaissances NetApp : Gestion des buckets compatibles hérités dans StorageGRID 11.5"

Vous ne pouvez plus créer de nouveaux buckets avec la conformité activée. Le message d'erreur suivant est renvoyé si vous tentez d'utiliser les modifications de demande CreateBucket pour la conformité afin de créer un nouveau bucket conforme :

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

Obsolète : demande de conformité GET Bucket

La demande de conformité GET Bucket est obsolète. Toutefois, vous pouvez continuer à utiliser cette demande pour déterminer les paramètres de conformité actuellement en vigueur pour un bucket conforme hérité existant.

> La fonctionnalité de conformité StorageGRID disponible dans les versions précédentes de StorageGRID est obsolète et a été remplacée par S3 Object Lock. Voir ce qui suit pour plus de détails :
>
> - "Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3"
> - "Base de connaissances NetApp : Gestion des buckets compatibles hérités dans StorageGRID 11.5"

Vous devez disposer de l'autorisation s3:GetBucketCompliance ou être root du compte pour terminer cette opération.

Exemple de demande

Cet exemple de requête vous permet de déterminer les paramètres de conformité pour le bucket nommé `mybucket` .

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

Exemple de réponse

Dans la réponse XML, `<SGCompliance>` répertorie les paramètres de conformité en vigueur pour le bucket. Cet exemple de réponse montre les paramètres de conformité d'un bucket dans lequel chaque objet sera conservé pendant un an (525 600 minutes), à compter du moment où l'objet est ingéré dans la grille. Il n'y a actuellement aucune retenue légale sur ce bucket. Chaque objet sera automatiquement supprimé après un an.

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

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

Nom	Description
Durée de conservation (minutes)	Durée de la période de conservation des objets ajoutés à ce bucket, en minutes. La période de conservation commence lorsque l'objet est ingéré dans la grille.
Conservation légale	• Vrai : ce bucket est actuellement sous une suspension légale. Les objets de ce compartiment ne peuvent pas être supprimés tant que la conservation légale n'est pas levée, même si leur période de conservation a expiré. • Faux : Ce bucket n'est actuellement pas soumis à une suspension légale. Les objets de ce compartiment peuvent être supprimés lorsque leur période de conservation expire.
Suppression automatique	• Vrai : les objets de ce compartiment seront supprimés automatiquement à l'expiration de leur période de conservation, sauf si le compartiment est soumis à une suspension légale. • Faux : les objets de ce bucket ne seront pas supprimés automatiquement à l'expiration de la période de conservation. Vous devez supprimer ces objets manuellement si vous devez les supprimer.

Réponses d'erreur

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

Obsolète : demande de conformité du compartiment PUT

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

> La fonctionnalité de conformité StorageGRID disponible dans les versions précédentes de StorageGRID est obsolète et a été remplacée par S3 Object Lock. Voir ce qui suit pour plus de détails :
>
> - "Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3"
> - "Base de connaissances NetApp : Gestion des buckets compatibles hérités dans StorageGRID 11.5"

Vous devez disposer de l'autorisation s3:PutBucketCompliance ou être root du compte pour terminer cette opération.

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

Exemple de demande

Cet exemple de requête modifie les paramètres de conformité pour le bucket nommé `mybucket` . Dans cet exemple, les objets dans `mybucket` seront désormais conservés pendant deux ans (1 051 200 minutes) au lieu d'un an, à compter de la date d'ingestion de l'objet dans la grille. Il n'y a aucune retenue légale sur ce seau. Chaque objet sera automatiquement supprimé après deux ans.

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

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

Nom	Description
Durée de conservation (minutes)	Durée de la période de conservation des objets ajoutés à ce bucket, en minutes. La période de conservation commence lorsque l'objet est ingéré dans la grille. **Important** Lorsque vous spécifiez une nouvelle valeur pour RetentionPeriodMinutes, vous devez spécifier une valeur égale ou supérieure à la période de rétention actuelle du bucket. Une fois la période de conservation du bucket définie, vous ne pouvez pas diminuer cette valeur ; vous pouvez uniquement l'augmenter.
Conservation légale	• Vrai : ce bucket est actuellement sous une suspension légale. Les objets de ce compartiment ne peuvent pas être supprimés tant que la conservation légale n'est pas levée, même si leur période de conservation a expiré. • Faux : Ce bucket n'est actuellement pas soumis à une suspension légale. Les objets de ce compartiment peuvent être supprimés lorsque leur période de conservation expire.
Suppression automatique	• Vrai : les objets de ce compartiment seront supprimés automatiquement à l'expiration de leur période de conservation, sauf si le compartiment est soumis à une suspension légale. • Faux : les objets de ce bucket ne seront pas supprimés automatiquement à l'expiration de la période de conservation. Vous devez supprimer ces objets manuellement si vous devez les supprimer.

Cohérence des paramètres de conformité

Lorsque vous mettez à jour les paramètres de conformité d'un bucket S3 avec une demande de conformité PUT Bucket, StorageGRID tente de mettre à jour les métadonnées du bucket sur la grille. Par défaut, StorageGRID utilise la cohérence **Strong-global** pour garantir que tous les sites de centre de données et tous les nœuds de stockage contenant des métadonnées de bucket ont une cohérence de lecture après écriture pour les paramètres de conformité modifiés.

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

Si vous recevez cette réponse, vous devez contacter l'administrateur du réseau pour vous assurer que les services de stockage requis sont mis à disposition dès que possible. Si l'administrateur du réseau ne parvient pas à rendre disponibles suffisamment de nœuds de stockage sur chaque site, le support technique peut vous demander de réessayer la demande ayant échoué en forçant la cohérence **Strong-site**.

> Ne forcez jamais la cohérence **Strong-site** pour la conformité du bucket PUT, sauf si le support technique vous l'a demandé et si vous comprenez les conséquences potentielles de l'utilisation de ce niveau.

Lorsque la cohérence est réduite à **Strong-site**, StorageGRID garantit que les paramètres de conformité mis à jour auront une cohérence de lecture après écriture uniquement pour les demandes client au sein d'un site. Cela signifie que le système StorageGRID peut temporairement avoir plusieurs paramètres incohérents pour ce bucket jusqu'à ce que tous les sites et nœuds de stockage soient disponibles. Les paramètres incohérents peuvent entraîner un comportement inattendu et indésirable. Par exemple, si vous placez un bucket sous une suspension légale et que vous forcez une cohérence inférieure, les paramètres de conformité précédents du bucket (c'est-à-dire la suspension légale) peuvent continuer à être en vigueur sur certains sites de centres de données. Par conséquent, les objets que vous pensez être en attente légale peuvent être supprimés à l'expiration de leur période de conservation, soit par l'utilisateur, soit par la suppression automatique, si cette option est activée.

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

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

Réponses d'erreur

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

Informations connexes

"Obsolète : Modifications de la demande PUT Bucket pour la conformité"

Politiques d'accès aux buckets et aux groupes

Utiliser des politiques d’accès aux buckets et aux groupes

StorageGRID utilise le langage de stratégie Amazon Web Services (AWS) pour permettre aux locataires S3 de contrôler l’accès aux buckets et aux objets au sein de ces buckets. Le système StorageGRID implémente un sous-ensemble du langage de politique de l’API REST S3. Les politiques d’accès pour l’API S3 sont écrites en JSON.

Aperçu de la politique d’accès

Il existe deux types de politiques d’accès prises en charge par StorageGRID.

- **Stratégies de bucket**, qui sont gérées à l’aide des opérations API S3 GetBucketPolicy, PutBucketPolicy et DeleteBucketPolicy ou de l’API Tenant Manager ou Tenant Management. Les stratégies de bucket sont attachées aux buckets, elles sont donc configurées pour contrôler l’accès des utilisateurs du compte propriétaire du bucket ou d’autres comptes au bucket et aux objets qu’il contient. Une politique de bucket s’applique à un seul bucket et éventuellement à plusieurs groupes.
- **Stratégies de groupe**, qui sont configurées à l’aide de Tenant Manager ou de l’API Tenant Management. Les stratégies de groupe sont attachées à un groupe dans le compte, elles sont donc configurées pour permettre à ce groupe d’accéder à des ressources spécifiques appartenant à ce compte. Une stratégie de groupe s’applique à un seul groupe et éventuellement à plusieurs compartiments.

> Il n’y a aucune différence de priorité entre les politiques de groupe et de compartiment.

Les stratégies de bucket et de groupe StorageGRID suivent une grammaire spécifique définie par Amazon. À l’intérieur de chaque politique se trouve un ensemble d’énoncés de politique, et chaque énoncé contient les éléments suivants :

- ID de relevé (Sid) (facultatif)
- Effet
- Principal/Non principal
- Ressource/PasRessource
- Action/Pas d’action
- Condition (facultatif)

Les instructions de politique sont construites à l’aide de cette structure pour spécifier les autorisations : Accorder <Effet> pour autoriser/refuser à <Principal> d’effectuer <Action> sur <Ressource> lorsque <Condition> s’applique.

Chaque élément de politique est utilisé pour une fonction spécifique :

Élément	Description
Sid	L’élément Sid est facultatif. Le Sid est uniquement destiné à servir de description pour l’utilisateur. Il est stocké mais non interprété par le système StorageGRID .

Élément	Description
Effet	Utilisez l'élément Effet pour déterminer si les opérations spécifiées sont autorisées ou refusées. Vous devez identifier les opérations que vous autorisez (ou refusez) sur les buckets ou les objets à l'aide des mots-clés d'élément Action pris en charge.
Principal/Non principal	Vous pouvez autoriser les utilisateurs, les groupes et les comptes à accéder à des ressources spécifiques et à effectuer des actions spécifiques. Si aucune signature S3 n'est incluse dans la demande, l'accès anonyme est autorisé en spécifiant le caractère générique (*) comme principal. Par défaut, seul le root du compte a accès aux ressources appartenant au compte. Il vous suffit de spécifier l'élément Principal dans une stratégie de bucket. Pour les stratégies de groupe, le groupe auquel la stratégie est attachée est l'élément principal implicite.
Ressource/PasRessource	L'élément Ressource identifie les buckets et les objets. Vous pouvez autoriser ou refuser des autorisations sur des buckets et des objets à l'aide du nom de ressource Amazon (ARN) pour identifier la ressource.
Action/Pas d'action	Les éléments Action et Effet sont les deux composants des autorisations. Lorsqu'un groupe demande une ressource, l'accès à cette ressource lui est accordé ou refusé. L'accès est refusé à moins que vous n'attribuiez spécifiquement des autorisations, mais vous pouvez utiliser un refus explicite pour remplacer une autorisation accordée par une autre politique.
Condition	L'élément Condition est facultatif. Les conditions vous permettent de créer des expressions pour déterminer quand une politique doit être appliquée.

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

```
s3:*Object
```

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

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

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

```
"Principal":{"AWS":"*"}
```

Dans l'exemple suivant, l'instruction utilise les éléments Effet, Principal, Action et Ressource. Cet exemple montre une déclaration de politique de compartiment complète qui utilise l'effet « Autoriser » pour donner aux principaux, le groupe d'administrateurs `federated-group/admin` et le groupe financier `federated-group/finance` , autorisations pour effectuer l'action `s3:ListBucket` sur le seau nommé `mybucket` et l'action `s3:GetObject` sur tous les objets à l'intérieur de ce seau.

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

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

Cohérence des politiques

Par défaut, toutes les mises à jour que vous apportez aux stratégies de groupe sont finalement cohérentes. Lorsqu'une stratégie de groupe devient cohérente, les modifications peuvent prendre 15 minutes supplémentaires pour prendre effet, en raison de la mise en cache des stratégies. Par défaut, toutes les mises à jour que vous apportez aux stratégies de compartiment sont fortement cohérentes.

Si nécessaire, vous pouvez modifier les garanties de cohérence pour les mises à jour de la stratégie de compartiment. Par exemple, vous souhaiterez peut-être qu'une modification apportée à une stratégie de compartiment soit disponible en cas de panne du site.

Dans ce cas, vous pouvez soit définir le `Consistency-Control` en-tête dans la demande PutBucketPolicy, ou vous pouvez utiliser la demande de cohérence PUT Bucket. Lorsqu'une stratégie de compartiment devient cohérente, les modifications peuvent prendre 8 secondes supplémentaires pour prendre effet, en raison de la

mise en cache de la stratégie.

> Si vous définissez la cohérence sur une valeur différente pour contourner une situation temporaire, assurez-vous de redéfinir le paramètre au niveau du bucket sur sa valeur d'origine lorsque vous avez terminé. Dans le cas contraire, toutes les futures demandes de bucket utiliseront le paramètre modifié.

Utiliser l'ARN dans les déclarations de politique

Dans les déclarations de politique, l'ARN est utilisé dans les éléments Principal et Ressource.

- Utilisez cette syntaxe pour spécifier l'ARN de la ressource S3 :

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

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

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

Autres considérations :

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

  "Syntaxe URN RFC 2141"

  Le corps de la requête HTTP pour l'opération PutBucketPolicy doit être codé avec charset=UTF-8.

Spécifier les ressources dans une politique

Dans les instructions de politique, vous pouvez utiliser l'élément Ressource pour spécifier le compartiment ou l'objet pour lequel les autorisations sont accordées ou refusées.

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

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

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

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

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

Spécifier les principaux dans une politique

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

- Chaque déclaration de politique dans une politique de compartiment doit inclure un élément Principal. Les instructions de politique dans une politique de groupe n'ont pas besoin de l'élément Principal car le groupe est considéré comme le principal.
- Dans une politique, les mandants sont désignés par l'élément « Principal » ou « NotPrincipal » pour l'exclusion.
- Les identités basées sur un compte doivent être spécifiées à l'aide d'un ID ou d'un ARN :

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

- Cet exemple utilise l'ID de compte locataire 27233906934684427525, qui inclut la racine du compte et tous les utilisateurs du compte :

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

- Vous pouvez spécifier uniquement la racine du compte :

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

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

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

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

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

- Vous pouvez spécifier un principal anonyme :

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

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

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

  Par exemple, supposons qu'Alex quitte l'organisation et le nom d'utilisateur `Alex` est supprimé. Si un nouvel Alex rejoint l'organisation et se voit attribuer le même `Alex` nom d'utilisateur, le nouvel utilisateur peut hériter involontairement des autorisations accordées à l'utilisateur d'origine.

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

Spécifier les autorisations dans une politique

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

Les tableaux répertorient les autorisations qui s'appliquent aux buckets et les autorisations qui s'appliquent aux objets.

> Amazon S3 utilise désormais l'autorisation s3:PutReplicationConfiguration pour les actions PutBucketReplication et DeleteBucketReplication. StorageGRID utilise des autorisations distinctes pour chaque action, ce qui correspond à la spécification Amazon S3 d'origine.

> Une suppression est effectuée lorsqu'un put est utilisé pour écraser une valeur existante.

Autorisations qui s'appliquent aux buckets

Autorisations	Opérations de l'API REST S3	Personnalisé pour StorageGRID
s3:Créer un bucket	Créer un bucket	Oui. **Remarque** : À utiliser uniquement dans la stratégie de groupe.
s3 : Supprimer le bucket	Supprimer le bucket	
s3 : Supprimer la notification des métadonnées du bucket	SUPPRIMER la configuration de notification des métadonnées du bucket	Oui

Autorisations	Opérations de l'API REST S3	Personnalisé pour StorageGRID
s3 : Supprimer la politique de bucket	Supprimer la politique de bucket	
s3 : Supprimer la configuration de réplication	SupprimerBucketReplication	Oui, des autorisations distinctes pour PUT et DELETE
s3 : Obtenir l'Acl du bucket	ObtenirBucketAcl	
s3 : Obtenir la conformité du bucket	Conformité du bucket GET (obsolète)	Oui
s3 : GetBucketConsistency	Cohérence du bucket GET	Oui
s3:Obtenir le bucket CORS	ObtenirBucketCors	
s3 : Obtenir la configuration du chiffrement	Obtenir le chiffrement du bucket	
s3 : Obtenir l'heure du dernier accès au bucket	Heure du dernier accès au bucket GET	Oui
s3 : Obtenir l'emplacement du bucket	Obtenir l'emplacement du bucket	
s3 : GetBucketMetadataNotification	Configuration de la notification des métadonnées du bucket GET	Oui
s3 : Obtenir une notification de bucket	Configuration de GetBucketNotification	
s3 : GetBucketObjectLockConfiguration	Obtenir la configuration du verrouillage de l'objet	
s3 : Obtenir la politique du bucket	Obtenir la politique de Bucket	
s3 : Obtenir le balisage du bucket	Obtenir le balisage du bucket	
s3 : Obtenir la gestion des versions du bucket	Obtenir la gestion des versions du bucket	
s3 : Obtenir la configuration du cycle de vie	GetBucketLifecycleConfiguration	
s3 : Obtenir la configuration de réplication	Réplication GetBucket	

Autorisations	Opérations de l'API REST S3	Personnalisé pour StorageGRID
s3 : ListeTousMesSeaux	• Listes de seaux • Utilisation du stockage GET	Oui, pour l'utilisation du stockage GET. **Remarque** : À utiliser uniquement dans la stratégie de groupe.
s3:ListBucket	• Liste d'objets • Tête de godet • Restaurer l'objet	
s3 : ListBucketMultipartUploads	• ListeMultipartUploads • Restaurer l'objet	
s3 : ListBucketVersions	Versions du bucket GET	
s3 : PutBucketCompliance	Conformité du compartiment PUT (obsolète)	Oui
s3 : PutBucketConsistency	Cohérence du seau PUT	Oui
s3:PutBucketCORS	• SupprimerBucketCors† • PutBucketCors	
s3 : PutEncryptionConfiguration	• Supprimer le chiffrement du bucket • Cryptage PutBucket	
s3 : PutBucketLastAccessTime	Heure du dernier accès au bucket PUT	Oui
s3 : PutBucketMetadataNotification	Configuration des notifications de métadonnées du compartiment PUT	Oui
s3 : PutBucketNotification	Configuration de PutBucketNotification	
s3 : PutBucketObjectLockConfiguration	• CreateBucket avec le `x-amz-bucket-object-lock-enabled: true` en-tête de requête (nécessite également l'autorisation s3:CreateBucket) • Configuration de PutObjectLock	
s3 : PutBucketPolicy	Politique de PutBucket	

Autorisations	Opérations de l'API REST S3	Personnalisé pour StorageGRID
s3 : Mettre en place le balisage du bucket	• Supprimer le balisage du bucket† • Balisage de PutBucket	
s3 : PutBucketVersioning	Gestion des versions de PutBucket	
s3 : PutLifecycleConfiguration	• Supprimer le cycle de vie du bucket† • Configuration du cycle de vie de PutBucket	
s3 : PutReplicationConfiguration	Réplication de PutBucket	Oui, des autorisations distinctes pour PUT et DELETE

Autorisations qui s'appliquent aux objets

Autorisations	Opérations de l'API REST S3	Personnalisé pour StorageGRID
s3 : Abandonner le téléchargement en plusieurs parties	• Abandonner le téléchargement en plusieurs parties • Restaurer l'objet	
s3 : Contournement de la gouvernance et de la rétention	• Supprimer l'objet • Supprimer les objets • PutObjectRetention	
s3:Supprimer l'objet	• Supprimer l'objet • Supprimer les objets • Restaurer l'objet	
s3 : Supprimer le balisage d'objet	Supprimer l'étiquetage des objets	
s3 : Supprimer le balisage de version d'objet	DeleteObjectTagging (une version spécifique de l'objet)	
s3 : Supprimer la version de l'objet	DeleteObject (une version spécifique de l'objet)	

Autorisations	Opérations de l'API REST S3	Personnalisé pour StorageGRID
s3:Obtenir l'objet	• Obtenir l'objet • HeadObject • Restaurer l'objet • Sélectionner le contenu de l'objet	
s3:GetObjectAcl	ObtenirObjectAcl	
s3 : GetObjectLegalHold	Obtenir la conservation légale de l'objet	
s3 : Obtenir la rétention d'objet	Obtenir la rétention d'objet	
s3 : Obtenir le balisage des objets	Obtenir l'étiquetage des objets	
s3 : Obtenir le balisage de la version de l'objet	GetObjectTagging (une version spécifique de l'objet)	
s3 : Obtenir la version de l'objet	GetObject (une version spécifique de l'objet)	
s3 : ListeMultipartUploadParts	ListParts, RestoreObject	
s3:PutObject	• Mettre l'objet • Copier l'objet • Restaurer l'objet • Créer un téléchargement multi-parties • Téléchargement complet en plusieurs parties • Télécharger une partie • TéléchargerPartCopy	
s3 : PutObjectLegalHold	MettreObjetLegalHold	
s3 : PutObjectRetention	PutObjectRetention	
s3 : Mettre en place un balisage d'objet	Balisage d'objets	
s3 : Mettre en place la version de l'objet	PutObjectTagging (une version spécifique de l'objet)	

Autorisations	Opérations de l'API REST S3	Personnalisé pour StorageGRID
s3 : PutOverwriteObject	• Mettre l'objet • Copier l'objet • Balisage d'objets • Supprimer l'étiquetage des objets • Téléchargement complet en plusieurs parties	Oui
s3:RestoreObject	Restaurer l'objet	

Utiliser l'autorisation PutOverwriteObject

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

Les paramètres possibles pour cette autorisation incluent :

- **Autoriser**: Le client peut écraser un objet. Il s'agit du paramètre par défaut.
- **Refuser** : Le client ne peut pas écraser un objet. Lorsqu'elle est définie sur Refuser, l'autorisation PutOverwriteObject fonctionne comme suit :
  - Si un objet existant est trouvé sur le même chemin :
    - Les données de l'objet, les métadonnées définies par l'utilisateur ou le balisage de l'objet S3 ne peuvent pas être écrasés.
    - Toutes les opérations d'ingestion en cours sont annulées et une erreur est renvoyée.
    - Si le contrôle de version S3 est activé, le paramètre Refuser empêche les opérations PutObjectTagging ou DeleteObjectTagging de modifier le TagSet d'un objet et ses versions non actuelles.
  - Si aucun objet existant n'est trouvé, cette autorisation n'a aucun effet.
- Lorsque cette autorisation n'est pas présente, l'effet est le même que si Autoriser était défini.

> Si la stratégie S3 actuelle autorise l'écrasement et que l'autorisation PutOverwriteObject est définie sur Refuser, le client ne peut pas écraser les données d'un objet, les métadonnées définies par l'utilisateur ou le balisage d'un objet. De plus, si la case à cocher **Empêcher la modification du client** est sélectionnée (**CONFIGURATION** > **Paramètres de sécurité** > **Réseau et objets**), ce paramètre remplace le paramètre de l'autorisation PutOverwriteObject.

Spécifier les conditions dans une politique

Les conditions définissent quand une politique sera en vigueur. Les conditions sont constituées d'opérateurs et de paires clé-valeur.

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

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

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

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

Opérateurs de condition pris en charge

Les opérateurs de condition sont classés comme suit :

- Chaîne
- Numérique
- Booléen
- adresse IP
- Vérification nulle

Opérateurs de condition	Description
Chaîne égale	Compare une clé à une valeur de chaîne en fonction d'une correspondance exacte (sensible à la casse).
Chaîne non égale	Compare une clé à une valeur de chaîne en fonction d'une correspondance négative (sensible à la casse).
Chaîne égale à Ignorer la casse	Compare une clé à une valeur de chaîne en fonction d'une correspondance exacte (ignore la casse).
Chaîne non égale à ignorer la casse	Compare une clé à une valeur de chaîne en fonction d'une correspondance négative (ignore la casse).
Comme une chaîne	Compare une clé à une valeur de chaîne en fonction d'une correspondance exacte (sensible à la casse). Peut inclure les caractères génériques * et ?.
ChaînePasComme	Compare une clé à une valeur de chaîne en fonction d'une correspondance négative (sensible à la casse). Peut inclure les caractères génériques * et ?.

Opérateurs de condition	Description
NumériqueÉgal	Compare une clé à une valeur numérique en fonction d'une correspondance exacte.
NumériqueNonÉgal	Compare une clé à une valeur numérique en fonction d'une correspondance négative.
Numérique supérieur à	Compare une clé à une valeur numérique en fonction d'une correspondance « supérieure à ».
Numérique supérieur à égal	Compare une clé à une valeur numérique en fonction d'une correspondance « supérieure ou égale ».
NumériqueInférieurÀ	Compare une clé à une valeur numérique en fonction d'une correspondance « inférieure à ».
NumériqueInférieurÀÉgal	Compare une clé à une valeur numérique en fonction d'une correspondance « inférieure ou égale ».
Booléen	Compare une clé à une valeur booléenne en fonction d'une correspondance « vrai ou faux ».
Adresse IP	Compare une clé à une adresse IP ou à une plage d'adresses IP.
Pas d'adresse IP	Compare une clé à une adresse IP ou à une plage d'adresses IP en fonction d'une correspondance négative.
Nul	Vérifie si une clé de condition est présente dans le contexte de la demande actuelle.

Clés de condition prises en charge

Clés de condition	Actions	Description
aws:SourceIP	opérateurs IP	Sera comparé à l'adresse IP à partir de laquelle la demande a été envoyée. Peut être utilisé pour les opérations de bucket ou d'objet. **Remarque :** si la requête S3 a été envoyée via le service d'équilibrage de charge sur les nœuds d'administration et les nœuds de passerelle, elle sera comparée à l'adresse IP en amont du service d'équilibrage de charge. **Remarque** : si un équilibreur de charge tiers non transparent est utilisé, cela sera comparé à l'adresse IP de cet équilibreur de charge. N'importe lequel `X-Forwarded-For` l'en-tête sera ignoré car sa validité ne peut pas être vérifiée.
aws:nom d'utilisateur	Ressource/Identité	Sera comparé au nom d'utilisateur de l'expéditeur à partir duquel la demande a été envoyée. Peut être utilisé pour les opérations de bucket ou d'objet.
s3:délimiteur	s3:ListBucket et s3:Autorisations ListBucketVersions	Sera comparé au paramètre délimiteur spécifié dans une demande ListObjects ou ListObjectVersions.

Clés de condition	Actions	Description
s3:ExistingObjectTag/<clé-balise>	s3 : Supprimer le balisage d'objet s3 : Supprimer le balisage de version d'objet s3:Obtenir l'objet s3:GetObjectAcl 3 : Obtenir le balisage des objets s3 : Obtenir la version de l'objet s3 : ObtenirObjectVersion Acl s3 : Obtenir le balisage de la version de l'objet s3:PutObjectAcl s3 : Mettre en place un balisage d'objet s3:PutObjectVersionAcl s3 : Mettre en place la version de l'objet	Nécessitera que l'objet existant possède la clé et la valeur de balise spécifiques.
s3:max-clés	s3:ListBucket et s3:Autorisations ListBucketVersions	Sera comparé au paramètre max-keys spécifié dans une requête ListObjects ou ListObjectVersions.
s3 : jours de conservation restants pour le verrouillage d'objet	s3:PutObject	Comparable à la date de conservation spécifiée dans le `x-amz-object-lock-retain-until-date` en-tête de demande ou période de conservation par défaut calculée à partir du compartiment pour garantir que ces valeurs se situent dans la plage autorisée pour les demandes suivantes : • Mettre l'objet • Copier l'objet • Créer un téléchargement multi-parties

Clés de condition	Actions	Description
s3 : jours de conservation restants pour le verrouillage d'objet	s3 : PutObjectRetention	Compare la date de conservation spécifiée dans la demande PutObjectRetention pour garantir qu'elle se situe dans la plage autorisée.
s3:préfixe	s3:ListBucket et s3:Autorisations ListBucketVersions	Sera comparé au paramètre de préfixe spécifié dans une demande ListObjects ou ListObjectVersions.
s3:RequestObjectTag/<clé-balise>	s3:PutObject s3 : Mettre en place un balisage d'objet s3 : Mettre en place la version de l'objet	Nécessitera une clé et une valeur de balise spécifiques lorsque la demande d'objet inclut le balisage.

Spécifier les variables dans une politique

Vous pouvez utiliser des variables dans les politiques pour renseigner les informations de politique lorsqu'elles sont disponibles. Vous pouvez utiliser des variables de politique dans le `Resource` élément et dans les comparaisons de chaînes dans le `Condition` élément.

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

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

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

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

Variable	Description
`${aws:SourceIp}`	Utilise la clé SourceIp comme variable fournie.
`${aws:username}`	Utilise la clé du nom d'utilisateur comme variable fournie.
`${s3:prefix}`	Utilise la clé de préfixe spécifique au service comme variable fournie.

Variable	Description
`${s3:max-keys}`	Utilise la clé max-keys spécifique au service comme variable fournie.
`${*}`	Caractère spécial. Utilise le caractère comme un caractère * littéral.
`${?}`	Caractère spécial. Utilise le caractère comme un caractère ? littéral.
`${$}`	Caractère spécial. Utilise le caractère comme un caractère $ littéral.

Créer des politiques nécessitant un traitement spécial

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

Description de la politique	Type de politique	Comportement d'Amazon	Comportement de StorageGRID
Refuser toute autorisation sur le compte root	Seau	Valide et appliqué, mais le compte utilisateur root conserve l'autorisation pour toutes les opérations de stratégie de compartiment S3	Même
Se refuser toute autorisation d'utilisateur/groupe	Groupe	Valide et appliqué	Même
Autoriser un groupe de comptes étrangers à accorder n'importe quelle autorisation	Seau	Principal invalide	Valide, mais les autorisations pour toutes les opérations de stratégie de compartiment S3 renvoient une erreur 405 Méthode non autorisée lorsqu'elles sont autorisées par une stratégie
Autoriser un compte root ou un utilisateur étranger à accéder à n'importe quelle autorisation	Seau	Valide, mais les autorisations pour toutes les opérations de stratégie de compartiment S3 renvoient une erreur 405 Méthode non autorisée lorsqu'elles sont autorisées par une stratégie	Même

Description de la politique	Type de politique	Comportement d'Amazon	Comportement de StorageGRID
Accorder à tout le monde des autorisations pour toutes les actions	Seau	Valide, mais les autorisations pour toutes les opérations de stratégie de compartiment S3 renvoient une erreur 405 Méthode non autorisée pour la racine du compte étranger et les utilisateurs	Même
Refuser à tout le monde les autorisations pour toutes les actions	Seau	Valide et appliqué, mais le compte utilisateur root conserve l'autorisation pour toutes les opérations de stratégie de compartiment S3	Même
Le principal est un utilisateur ou un groupe inexistant	Seau	Principal invalide	Valide
La ressource est un bucket S3 inexistant	Groupe	Valide	Même
Principal est un groupe local	Seau	Principal invalide	Valide
La politique accorde à un compte non propriétaire (y compris les comptes anonymes) des autorisations pour placer des objets.	Seau	Valide. Les objets appartiennent au compte créateur et la politique de compartiment ne s'applique pas. Le compte créateur doit accorder des autorisations d'accès à l'objet à l'aide des listes de contrôle d'accès (ACL) d'objet.	Valide. Les objets appartiennent au compte propriétaire du bucket. La politique des seaux s'applique.

Protection WORM (écriture unique, lecture multiple)

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

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

- Depuis le Gestionnaire de grille, accédez à **CONFIGURATION** > **Sécurité** > **Paramètres de sécurité** > **Réseau et objets**, puis cochez la case **Empêcher la modification du client**.
- Appliquez les règles et politiques S3 suivantes :
  - Ajoutez une opération PutOverwriteObject DENY à la stratégie S3.
  - Ajoutez une opération DeleteObject DENY à la stratégie S3.

- Ajoutez une opération PutObject ALLOW à la stratégie S3.

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

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

Situation A : Écritures simultanées (non protégées)

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

Situation B : Écrasements séquentiels terminés (protégés contre)

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

Informations connexes

- "Comment les règles ILM de StorageGRID gèrent les objets"
- "Exemples de politiques de compartiment"
- "Exemples de stratégies de groupe"
- "Gérer les objets avec ILM"
- "Utiliser un compte locataire"

Exemples de politiques de compartiment

Utilisez les exemples de cette section pour créer des politiques d'accès StorageGRID pour les buckets.

Les stratégies de compartiment spécifient les autorisations d'accès pour le compartiment auquel la stratégie est attachée. Vous configurez une stratégie de bucket en utilisant l'API S3 PutBucketPolicy via l'un de ces outils :

- "Gestionnaire de locataires" .
- AWS CLI utilisant cette commande (reportez-vous à"Opérations sur les godets"):

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

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

Dans cet exemple, tout le monde, y compris les personnes anonymes, est autorisé à répertorier les objets du bucket et à effectuer des opérations GetObject sur tous les objets du bucket. Toutes les autres opérations seront refusées. Notez que cette politique peut ne pas être particulièrement utile car personne, à l'exception de la racine du compte, n'a l'autorisation d'écrire dans le bucket.

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

Exemple : autoriser tous les utilisateurs d'un compte à accéder pleinement à un bucket et tous les utilisateurs d'un autre compte à accéder en lecture seule à un bucket.

Dans cet exemple, toutes les personnes d'un compte spécifié sont autorisées à accéder pleinement à un compartiment, tandis que toutes les personnes d'un autre compte spécifié sont uniquement autorisées à répertorier le compartiment et à effectuer des opérations GetObject sur les objets du compartiment commençant par le `shared/` préfixe de clé d'objet.

Dans StorageGRID, les objets créés par un compte non propriétaire (y compris les comptes anonymes) appartiennent au compte propriétaire du bucket. La politique de bucket s'applique à ces objets.

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

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

Dans cet exemple, tout le monde, y compris les anonymes, est autorisé à répertorier le bucket et à effectuer des opérations GetObject sur tous les objets du bucket, tandis que seuls les utilisateurs appartenant au groupe `Marketing` dans le compte spécifié, un accès complet est autorisé.

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

Exemple : autoriser tout le monde à accéder en lecture et en écriture à un bucket si le client se trouve dans la plage d'adresses IP

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

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

Exemple : autoriser l'accès complet à un bucket exclusivement par un utilisateur fédéré spécifié

Dans cet exemple, l'utilisateur fédéré Alex est autorisé à accéder pleinement au `examplebucket` seau et ses objets. Tous les autres utilisateurs, y compris « root », se voient explicitement refuser toutes les opérations. Notez cependant que « root » ne se voit jamais refuser les autorisations pour Put/Get/DeleteBucketPolicy.

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

Exemple : autorisation PutOverwriteObject

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

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

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

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

Exemples de stratégies de groupe

Utilisez les exemples de cette section pour créer des politiques d'accès StorageGRID pour les groupes.

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

Exemple : définir une stratégie de groupe à l'aide de Tenant Manager

Lorsque vous ajoutez ou modifiez un groupe dans le gestionnaire de locataires, vous pouvez sélectionner une stratégie de groupe pour déterminer les autorisations d'accès S3 dont disposeront les membres de ce groupe. Voir "Créer des groupes pour un locataire S3" .

- **Pas d'accès S3** : option par défaut. Les utilisateurs de ce groupe n'ont pas accès aux ressources S3, sauf si l'accès est accordé avec une stratégie de compartiment. Si vous sélectionnez cette option, seul l'utilisateur root aura accès aux ressources S3 par défaut.
- **Accès en lecture seule** : les utilisateurs de ce groupe ont un accès en lecture seule aux ressources S3. Par exemple, les utilisateurs de ce groupe peuvent répertorier les objets et lire les données, les métadonnées et les balises des objets. Lorsque vous sélectionnez cette option, la chaîne JSON d'une stratégie de groupe en lecture seule apparaît dans la zone de texte. Vous ne pouvez pas modifier cette chaîne.
- **Accès complet** : les utilisateurs de ce groupe ont un accès complet aux ressources S3, y compris aux buckets. Lorsque vous sélectionnez cette option, la chaîne JSON d'une stratégie de groupe à accès complet apparaît dans la zone de texte. Vous ne pouvez pas modifier cette chaîne.
- **Atténuation des ransomwares** : cet exemple de politique s'applique à tous les compartiments de ce locataire. Les utilisateurs de ce groupe peuvent effectuer des actions courantes, mais ne peuvent pas supprimer définitivement les objets des buckets pour lesquels le contrôle de version des objets est activé.

  Les utilisateurs de Tenant Manager qui disposent de l'autorisation Gérer tous les compartiments peuvent remplacer cette stratégie de groupe. Limitez l'autorisation Gérer tous les compartiments aux utilisateurs de confiance et utilisez l'authentification multifacteur (MFA) lorsqu'elle est disponible.

- **Personnalisé** : les utilisateurs du groupe bénéficient des autorisations que vous spécifiez dans la zone de texte.

Exemple : autoriser le groupe à accéder à tous les compartiments

Dans cet exemple, tous les membres du groupe sont autorisés à accéder pleinement à tous les compartiments appartenant au compte locataire, sauf si cela est explicitement refusé par la politique de compartiment.

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

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

Dans cet exemple, tous les membres du groupe ont un accès en lecture seule aux ressources S3, sauf si cela est explicitement refusé par la politique de bucket. Par exemple, les utilisateurs de ce groupe peuvent répertorier les objets et lire les données d'objet, les métadonnées et les balises.

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

Exemple : autoriser les membres du groupe à accéder pleinement à leur « dossier » dans un compartiment

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

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

Opérations S3 suivies dans les journaux d'audit

Les messages d'audit sont générés par les services StorageGRID et stockés dans des fichiers journaux texte. Vous pouvez consulter les messages d'audit spécifiques à S3 dans le journal d'audit pour obtenir des détails sur les opérations de bucket et d'objet.

Opérations de bucket suivies dans les journaux d'audit

- Créer un bucket
- Supprimer le bucket
- Supprimer le balisage du bucket
- Supprimer les objets
- Obtenir le balisage du bucket
- Tête de godet
- Liste d'objets
- ListObjectVersions
- Conformité du compartiment PUT
- Balisage de PutBucket
- Gestion des versions de PutBucket

Opérations sur les objets suivies dans les journaux d'audit

- Téléchargement complet en plusieurs parties
- Copier l'objet
- Supprimer l'objet
- Obtenir l'objet
- HeadObject
- Mettre l'objet
- Restaurer l'objet
- Sélectionner un objet
- UploadPart (lorsqu'une règle ILM utilise une ingestion équilibrée ou stricte)
- UploadPartCopy (lorsqu'une règle ILM utilise une ingestion équilibrée ou stricte)

Informations connexes

- "Accéder au fichier journal d'audit"
- "Le client écrit des messages d'audit"
- "Le client lit les messages d'audit"

Informations sur le copyright

Informations sur les marques commerciales