



## **UTILISEZ L'API REST S3**

StorageGRID software

NetApp  
January 14, 2026

# Sommaire

UTILISEZ L'API REST S3 .....	1
Versions et mises à jour prises en charge par l'API REST S3 .....	1
Versions prises en charge .....	1
Prise en charge des mises à jour de l'API REST S3 .....	1
Référence rapide : demandes d'API S3 prises en charge .....	4
Paramètres de requête URI courants et en-têtes de requête .....	5
"AbortMultipartUpload" .....	5
"CompleteMultipartUpload" .....	5
"Objet de copie" .....	6
"CreateBucket" .....	7
"CreateMultipartUpload" .....	7
"DeleteBucket" .....	8
"DeleteBucketCors" .....	8
"DeleteBucketEncryption" .....	8
"DeleteBucketLifecycle" .....	8
"DeleteBucketPolicy" .....	9
"DeleteBucketReplication" .....	9
"DeleteBucketTagging" .....	9
"DeleteObject" .....	9
"DeleteObjects" .....	10
"DeleteObjectTagging" .....	10
"GetBucketAcl" .....	10
"GetBucketCors" .....	10
"GetBucketEncryption" .....	11
"GetBucketLifecycleConfiguration" .....	11
"GetBucketLocation" .....	11
"GetBucketNotificationConfiguration" .....	11
"GetBucketPolicy" .....	11
"GetBucketReplication" .....	12
"GetBucketTagging" .....	12
"GetBucketVersioning" .....	12
"GetObject" .....	12
"GetObjectAcl" .....	13
"GetObjectLegalHold" .....	13
"GetObjectLockConfiguration" .....	14
"GetObjectRetention" .....	14
"GetObjectTagging" .....	14
"Godet principal" .....	14
"Objet principal" .....	14
"Listseaux" .....	15
"ListMultipartUploads" .....	15
"ListObjects" .....	16
"ListObjectsV2" .....	16

"ListObjectVersions" . . . . .	16
"ListParts" . . . . .	17
"PutBucketCors" . . . . .	17
"PutBucketEncryption" . . . . .	17
"PutBucketLifecycleConfiguration" . . . . .	18
"PutBucketNotificationConfiguration" . . . . .	19
"PutBucketPolicy" . . . . .	19
"PutBuckeReplication" . . . . .	19
"Étiquetage PutBucketTagging" . . . . .	20
"PutBuckeVersioning" . . . . .	20
"PutObject" . . . . .	20
"PutObjectLegalHold" . . . . .	21
"PutObjectLockConfiguration" . . . . .	21
"PutObjectRetention" . . . . .	21
"Marquage PutObject" . . . . .	22
"Objet de restauration" . . . . .	22
"SelectObjectContent" . . . . .	22
"UploadPart" . . . . .	22
"UploadPartCopy" . . . . .	23
Test de la configuration de l'API REST S3 . . . . .	24
Implémentation de l'API REST S3 par StorageGRID . . . . .	25
Requêtes des clients en conflit . . . . .	25
La cohérence . . . . .	25
Gestion des versions d'objet . . . . .	28
Utilisez l'API REST S3 pour configurer le verrouillage objet S3 . . . . .	29
Création de la configuration du cycle de vie S3 . . . . .	35
Recommandations pour l'implémentation de l'API REST S3 . . . . .	39
Prise en charge de l'API REST Amazon S3 . . . . .	41
Détails de l'implémentation de l'API REST S3 . . . . .	41
Authentifier les demandes . . . . .	42
Opérations sur le service . . . . .	42
Opérations sur les compartiments . . . . .	43
Opérations sur les objets . . . . .	51
Opérations pour les téléchargements partitionnés . . . . .	80
Réponses d'erreur . . . . .	89
Opérations personnalisées StorageGRID . . . . .	91
Opérations personnalisées StorageGRID . . . . .	91
OPTIMISEZ la cohérence des compartiments . . . . .	92
PRÉSERVER la cohérence du godet . . . . .	94
HEURE du dernier accès au compartiment . . . . .	95
METTRE l'heure du dernier accès au compartiment . . . . .	96
SUPPRIMEZ la configuration de notification des métadonnées de compartiment . . . . .	97
CONFIGURATION DES notifications de métadonnées de compartiment . . . . .	97
CONFIGURATION de notification des métadonnées de compartiment . . . . .	101
DEMANDE d'utilisation du stockage . . . . .	107

Demandes de compartiment obsolètes pour la conformité des anciennes . . . . .	108
Gérer les politiques d'accès . . . . .	114
Utiliser les politiques d'accès . . . . .	114
Exemple de politique de session . . . . .	132
Exemples de politiques de compartiments . . . . .	132
Exemples de stratégies de groupe . . . . .	138
Opérations S3 suivies dans les journaux d'audit . . . . .	141
Les opérations des compartiments sont suivies dans les journaux d'audit . . . . .	141
Opérations d'objet suivies dans les journaux d'audit . . . . .	142

# UTILISEZ 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 en tant que ensemble de services web REST (Representational State Transfer).

La prise en charge de l'API REST S3 vous permet de connecter les applications orientées services développées pour les services web S3 avec un stockage objet sur site qui utilise le système StorageGRID. L'utilisation actuelle des appels de l'API REST S3 par une application client requiert des modifications minimales.

### Versions prises en charge

StorageGRID prend en charge les versions spécifiques suivantes de STS, S3 et HTTP :

Élément	Version
Spécification de l'API STS AssumeRole	<a href="#">"Documentation Amazon Web Services (AWS) : Référence de l'API Amazon Assumerole"</a>  Pour plus d'informations sur AssumeRole, reportez-vous à <a href="#">"Configurer AssumeRole"</a> .
Spécification de l'API S3	<a href="#">"Documentation AWS : Référence de l'API Amazon Simple Storage Service"</a>
HTTP	1,1  Pour plus d'informations sur HTTP, consultez le document HTTP/1.1 (RFC 7230-35).  <a href="#">"IETF RFC 2616 : Protocole de transfert hypertexte (HTTP/1.1)"</a>  <b>Remarque:</b> StorageGRID ne prend pas en charge HTTP/1.1 pipeline.

### Prise en charge des mises à jour de l'API REST S3

Relâchez	Commentaires
12,0	<ul style="list-style-type: none"><li>Ajout de la prise en charge du partage de ressources inter-origines (CORS) pour une interface de gestion, qui permet à un autre domaine d'accéder aux données dans StorageGRID à l'aide des API de gestion. <a href="#">"En savoir plus &gt;"</a> .</li><li>Ajout de la prise en charge de STS AssumeRole et de la politique de session. Voir <a href="#">"un exemple de politique de session"</a> . Vous pouvez configurer AssumeRole sous les groupes de locataires.</li></ul>

Relâchez	Commentaires
11,9	<ul style="list-style-type: none"> <li>• Ajout de la prise en charge des valeurs de somme de contrôle SHA-256 pré-calculées pour les demandes suivantes et les en-têtes pris en charge. Vous pouvez utiliser cette fonction pour vérifier l'intégrité des objets téléchargés : <ul style="list-style-type: none"> <li>◦ Téléchargement CompleteMultipartUpload : <code>x-amz-checksum-sha256</code></li> <li>◦ CreateMultipartUpload : <code>x-amz-checksum-algorithm</code></li> <li>◦ GetObject : <code>x-amz-checksum-mode</code></li> <li>◦ Objet principal : <code>x-amz-checksum-mode</code></li> <li>◦ ListParts</li> <li>◦ PutObject : <code>x-amz-checksum-sha256</code></li> <li>◦ UploadPart : <code>x-amz-checksum-sha256</code></li> </ul> </li> <li>• Ajout de la possibilité pour l'administrateur du grid de contrôler les paramètres de conservation et de conformité au niveau du locataire. Ces paramètres affectent les paramètres de verrouillage d'objet S3. <ul style="list-style-type: none"> <li>◦ Mode de conservation par défaut du compartiment et mode de conservation des objets : gouvernance ou conformité, si l'administrateur du grid l'autorise.</li> <li>◦ La période de conservation par défaut du compartiment et la date de conservation de l'objet jusqu'au : doivent être inférieures ou égales à ce qui est autorisé par la période de conservation maximale définie par l'administrateur du grid.</li> </ul> </li> <li>• Meilleure prise en charge de <code>aws-chunked</code> l'encodage de contenu et des valeurs de diffusion en continu <code>x-amz-content-sha256</code>. Limites : <ul style="list-style-type: none"> <li>◦ Le cas échéant, <code>chunk-signature</code> est facultatif et non validé</li> <li>◦ S'il est présent, <code>x-amz-trailer</code> le contenu est ignoré</li> </ul> </li> </ul>
11,8	Mise à jour des noms des opérations S3 pour qu'ils correspondent aux noms utilisés dans le <a href="#">"Documentation Amazon Web Services (AWS) : référence de l'API Amazon simple Storage Service"</a> .
11,7	<ul style="list-style-type: none"> <li>• Ajouté <a href="#">"Référence rapide : demandes d'API S3 prises en charge"</a>.</li> <li>• Ajout de la prise en charge du mode DE GOUVERNANCE avec S3 Object Lock.</li> <li>• Ajout de la prise en charge de l'en-TÊTE de réponse spécifique à StorageGRID <code>x-ntap-sg-cgr-replication-status</code> pour les requêtes GET Object et HEAD Object. Cet en-tête fournit l'état de réplication d'un objet pour la réplication inter-grid.</li> <li>• Les requêtes SelectObjectContent prennent désormais en charge les objets parquet.</li> </ul>

Relâchez	Commentaires
11,6	<ul style="list-style-type: none"> <li>• Ajout de la prise en charge de l'utilisation du <code>partNumber</code> paramètre de requête dans les requêtes GET Object et HEAD Object.</li> <li>• Ajout de la prise en charge d'un mode de conservation par défaut et d'une période de conservation par défaut au niveau du compartiment pour le verrouillage d'objet S3.</li> <li>• Ajout de la prise en charge de la <code>s3:object-lock-remaining-retention-days</code> clé de condition de règle pour définir la plage de périodes de conservation autorisées pour vos objets.</li> <li>• Modification de la taille recommandée maximale pour une opération objet PUT unique à 5 Gio (5,368,709,120 octets). Si vos objets sont supérieurs à 5 Gio, utilisez le téléchargement partitionné.</li> </ul>
11,5	<ul style="list-style-type: none"> <li>• Ajout de la prise en charge de la gestion du chiffrement de compartiment.</li> <li>• Ajout de la prise en charge des demandes de verrouillage d'objet S3 et des demandes de conformité héritées obsolètes.</li> <li>• Ajout de la prise en charge de L'utilisation DE LA SUPPRESSION de plusieurs objets sur les compartiments multiversion.</li> <li>• L' `Content-MD5` en-tête de la demande est désormais correctement pris en charge.</li> </ul>
11,4	<ul style="list-style-type: none"> <li>• Prise en charge accrue du balisage de compartiment, DE L'étiquetage DES compartiments ET DU balisage de compartiment. Les étiquettes de répartition des coûts ne sont pas prises en charge.</li> <li>• Pour les compartiments créés dans StorageGRID 11.4, il n'est plus nécessaire de limiter les noms de clés d'objet pour respecter les bonnes pratiques de performance.</li> <li>• Prise en charge supplémentaire des notifications de compartiment pour le <code>s3:ObjectRestore:Post</code> type d'événement.</li> <li>• Les limites de taille d'AWS pour les pièces partitionnées sont maintenant appliquées. Chaque partie d'un téléchargement partitionné doit être comprise entre 5 MIB et 5 Gio. La dernière partie peut être plus petite que 5 MIB.</li> <li>• Ajout de la prise en charge de TLS 1.3</li> </ul>
11,3	<ul style="list-style-type: none"> <li>• Ajout de la prise en charge du chiffrement côté serveur des données d'objet avec les clés fournies par le client (SSE-C).</li> <li>• Prise en charge supplémentaire des opérations de SUPPRESSION, d'OBTENTION et de MISE du cycle de vie du compartiment (action d'expiration uniquement) et de <code>x-amz-expiration</code> l'en-tête de réponse.</li> <li>• PUT Object mis à jour, PUT Object - copie et Multipart Upload pour décrire l'impact des règles ILM utilisant un placement synchrone à l'entrée.</li> <li>• Les chiffrements TLS 1.1 ne sont plus pris en charge.</li> </ul>

Relâchez	Commentaires
11,2	<p>Ajout de la prise en charge de la restauration POST-objet pour l'utilisation avec les pools de stockage cloud. Ajout de la prise en charge de l'utilisation de la syntaxe AWS pour ARN, des clés de condition de règle et des variables de règles de groupe et de compartiment Les règles de compartiment et de groupe qui utilisent la syntaxe StorageGRID restent prises en charge.</p> <p><b>Remarque :</b> les utilisations de l'ARN/URN dans d'autres configurations JSON/XML, y compris celles utilisées dans les fonctions StorageGRID personnalisées, n'ont pas changé.</p>
11,1	Ajout de la prise en charge du partage de ressources entre les sources (CORS), du protocole HTTP pour les connexions client S3 aux nœuds de grid et des paramètres de conformité dans les compartiments.
11,0	Ajout de la prise en charge de la configuration des services de plateforme (réplication CloudMirror, notifications et intégration de la recherche Elasticsearch) pour les compartiments Ajout de la prise en charge des contraintes d'emplacement du balisage d'objets pour les compartiments, ainsi que de la cohérence disponible.
10,4	Ajout de la prise en charge des modifications de l'analyse ILM sur la gestion des versions, mises à jour de la page noms de domaine de point final, conditions et variables dans les règles, exemples de règles et autorisation PutOverwriteObject.
10,3	Prise en charge ajoutée pour la gestion des versions.
10,2	Ajout de la prise en charge des règles d'accès de groupe et de compartiment, ainsi que de la copie multipart (Télécharger la pièce - copie).
10,1	Ajout de la prise en charge du téléchargement partitionné, des demandes de type hébergement virtuel et de l'authentification v4.
10,0	Prise en charge initiale de l'API REST S3 par le système StorageGRID . La version actuellement prise en charge de la <i>Référence API du service de stockage simple</i> est 2006-03-01.

## Référence rapide : demandes d'API S3 prises en charge

Cette page explique comment StorageGRID prend en charge les API Amazon simple Storage Service (S3).

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



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

## Paramètres de requête URI courants et en-têtes de requête

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

- `versionId` (comme requis pour les opérations d'objet)

Sauf mention 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 associées

- ["Détails de l'implémentation de l'API REST S3"](#)
- ["Référence de l'API Amazon simple Storage Service : en-têtes de demande communs"](#)

## "AbortMultipartUpload"

### Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#)éléments de cette demande, plus ce paramètre de requête URI supplémentaire :

- `uploadId`

### Corps de la demande

Aucune

### Documentation StorageGRID

["Opérations pour les téléchargements partitionnés"](#)

## "CompleteMultipartUpload"

### Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#)éléments de cette demande, plus ce paramètre de requête URI supplémentaire :

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

### Demander des balises XML de corps

StorageGRID prend en charge les balises XML de corps de requête suivantes :

- ChecksumSHA256
- CompleteMultipartUpload
- ETag
- Part
- PartNumber

## Documentation StorageGRID

### ["CompleteMultipartUpload"](#)

#### **"Objet de copie"**

##### **Paramètres de requête URI et en-têtes de requête**

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#)éléments pour cette demande, plus les en-têtes supplémentaires suivants :

- 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 demande**

Aucune

## Documentation StorageGRID

### "Objet de copie"

## "CreateBucket"

### Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#)éléments pour cette demande, plus les en-têtes supplémentaires suivants :

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

### Corps de la demande

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

## Documentation StorageGRID

### "Opérations sur les compartiments"

## "CreateMultipartUpload"

### Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#)éléments pour cette demande, plus les en-têtes supplémentaires suivants :

- 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 demande

Aucune

#### **Documentation StorageGRID**

["CreateMultipartUpload"](#)

### **["DeleteBucket"](#)**

#### **Paramètres de requête URI et en-têtes de requête**

StorageGRID prend en charge tous [paramètres et en-têtes communs](#)ces éléments pour cette demande.

#### **Documentation StorageGRID**

["Opérations sur les compartiments"](#)

### **["DeleteBucketCors"](#)**

#### **Paramètres de requête URI et en-têtes de requête**

StorageGRID prend en charge tous [paramètres et en-têtes communs](#)ces éléments pour cette demande.

#### **Corps de la demande**

Aucune

#### **Documentation StorageGRID**

["Opérations sur les compartiments"](#)

### **["DeleteBucketEncryption"](#)**

#### **Paramètres de requête URI et en-têtes de requête**

StorageGRID prend en charge tous [paramètres et en-têtes communs](#)ces éléments pour cette demande.

#### **Corps de la demande**

Aucune

#### **Documentation StorageGRID**

["Opérations sur les compartiments"](#)

### **["DeleteBucketLifecycle"](#)**

#### **Paramètres de requête URI et en-têtes de requête**

StorageGRID prend en charge tous [paramètres et en-têtes communs](#)ces éléments pour cette demande.

#### **Corps de la demande**

Aucune

#### **Documentation StorageGRID**

- ["Opérations sur les compartiments"](#)
- ["Création de la configuration du cycle de vie S3"](#)

## "DeleteBucketPolicy"

### Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#)ces éléments pour cette demande.

### Corps de la demande

Aucune

### Documentation StorageGRID

["Opérations sur les compartiments"](#)

## "DeleteBucketReplication"

### Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#)ces éléments pour cette demande.

### Corps de la demande

Aucune

### Documentation StorageGRID

["Opérations sur les compartiments"](#)

## "DeleteBucketTagging"

### Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#)ces éléments pour cette demande.

### Corps de la demande

Aucune

### Documentation StorageGRID

["Opérations sur les compartiments"](#)

## "DeleteObject"

### Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#)éléments de cette demande, plus cet en-tête de demande supplémentaire :

- x-amz-bypass-governance-retention

### Corps de la demande

Aucune

### Documentation StorageGRID

["Opérations sur les objets"](#)

## "DeleteObjects"

### Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#)éléments de cette demande, plus cet en-tête de demande supplémentaire :

- x-amz-bypass-governance-retention

### Corps de la demande

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

### Documentation StorageGRID

["Opérations sur les objets"](#)

## "DeleteObjectTagging"

StorageGRID prend en charge tous [paramètres et en-têtes communs](#)ces éléments pour cette demande.

### Corps de la demande

Aucune

### Documentation StorageGRID

["Opérations sur les objets"](#)

## "GetBucketAcl"

### Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#)ces éléments pour cette demande.

### Corps de la demande

Aucune

### Documentation StorageGRID

["Opérations sur les compartiments"](#)

## "GetBucketCors"

### Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#)ces éléments pour cette demande.

### Corps de la demande

Aucune

### Documentation StorageGRID

["Opérations sur les compartiments"](#)

## "GetBucketEncryption"

### Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#)ces éléments pour cette demande.

### Corps de la demande

Aucune

### Documentation StorageGRID

["Opérations sur les compartiments"](#)

## "GetBucketLifecycleConfiguration"

### Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#)ces éléments pour cette demande.

### Corps de la demande

Aucune

### Documentation StorageGRID

- ["Opérations sur les compartiments"](#)
- ["Création de la configuration du cycle de vie S3"](#)

## "GetBucketLocation"

### Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#)ces éléments pour cette demande.

### Corps de la demande

Aucune

### Documentation StorageGRID

["Opérations sur les compartiments"](#)

## "GetBucketNotificationConfiguration"

### Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#)ces éléments pour cette demande.

### Corps de la demande

Aucune

### Documentation StorageGRID

["Opérations sur les compartiments"](#)

## "GetBucketPolicy"

### Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#)ces éléments pour cette demande.

## **Corps de la demande**

Aucune

## **Documentation StorageGRID**

"Opérations sur les compartiments"

## **"GetBucketReplication"**

### **Paramètres de requête URI et en-têtes de requête**

StorageGRID prend en charge tous [paramètres et en-têtes communs](#)ces éléments pour cette demande.

## **Corps de la demande**

Aucune

## **Documentation StorageGRID**

"Opérations sur les compartiments"

## **"GetBucketTagging"**

### **Paramètres de requête URI et en-têtes de requête**

StorageGRID prend en charge tous [paramètres et en-têtes communs](#)ces éléments pour cette demande.

## **Corps de la demande**

Aucune

## **Documentation StorageGRID**

"Opérations sur les compartiments"

## **"GetBucketVersioning"**

### **Paramètres de requête URI et en-têtes de requête**

StorageGRID prend en charge tous [paramètres et en-têtes communs](#)ces éléments pour cette demande.

## **Corps de la demande**

Aucune

## **Documentation StorageGRID**

"Opérations sur les compartiments"

## **"GetObject"**

### **Paramètres de requête URI et en-têtes de requête**

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#)éléments de cette demande, plus les paramètres de requête URI supplémentaires suivants :

- 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 demande 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 demande**

Aucune

#### **Documentation StorageGRID**

["GetObject"](#)

### **"GetObjectAcl"**

#### **Paramètres de requête URI et en-têtes de requête**

StorageGRID prend en charge tous [paramètres et en-têtes communs](#)ces éléments pour cette demande.

#### **Corps de la demande**

Aucune

#### **Documentation StorageGRID**

["Opérations sur les objets"](#)

### **"GetObjectLegalHold"**

#### **Paramètres de requête URI et en-têtes de requête**

StorageGRID prend en charge tous [paramètres et en-têtes communs](#)ces éléments pour cette demande.

#### **Corps de la demande**

Aucune

#### **Documentation StorageGRID**

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

## "GetObjectLockConfiguration"

### Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#)ces éléments pour cette demande.

### Corps de la demande

Aucune

### Documentation StorageGRID

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

## "GetObjectRetention"

### Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#)ces éléments pour cette demande.

### Corps de la demande

Aucune

### Documentation StorageGRID

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

## "GetObjectTagging"

### Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#)ces éléments pour cette demande.

### Corps de la demande

Aucune

### Documentation StorageGRID

["Opérations sur les objets"](#)

## "Godet principal"

### Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#)ces éléments pour cette demande.

### Corps de la demande

Aucune

### Documentation StorageGRID

["Opérations sur les compartiments"](#)

## "Objet principal"

### Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#)éléments pour cette demande, plus les en-têtes supplémentaires suivants :

- 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 demande**

Aucune

#### **Documentation StorageGRID**

["Objet principal"](#)

### **"Listseaux"**

#### **Paramètres de requête URI et en-têtes de requête**

StorageGRID prend en charge tous [paramètres et en-têtes communs](#)ces éléments pour cette demande.

#### **Corps de la demande**

Aucune

#### **Documentation StorageGRID**

["Opérations sur le service et > ; ListBuckets"](#)

### **"ListMultipartUploads"**

#### **Paramètres de requête URI et en-têtes de requête**

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#)éléments de cette demande, plus les paramètres supplémentaires suivants :

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

#### **Corps de la demande**

Aucune

#### **Documentation StorageGRID**

["ListMultipartUploads"](#)

## "ListObjects"

### Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs éléments de cette demande, plus les paramètres supplémentaires suivants :

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

### Corps de la demande

Aucune

### Documentation StorageGRID

["Opérations sur les compartiments"](#)

## "ListObjectsV2"

### Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs éléments de cette demande, plus les paramètres supplémentaires suivants :

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

### Corps de la demande

Aucune

### Documentation StorageGRID

["Opérations sur les compartiments"](#)

## "ListObjectVersions"

### Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs éléments de cette demande, plus les paramètres supplémentaires suivants :

- delimiter

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

#### **Corps de la demande**

Aucune

#### **Documentation StorageGRID**

["Opérations sur les compartiments"](#)

### **"ListParts"**

#### **Paramètres de requête URI et en-têtes de requête**

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#)éléments de cette demande, plus les paramètres supplémentaires suivants :

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

#### **Corps de la demande**

Aucune

#### **Documentation StorageGRID**

["ListMultipartUploads"](#)

### **"PutBucketCors"**

#### **Paramètres de requête URI et en-têtes de requête**

StorageGRID prend en charge tous [paramètres et en-têtes communs](#)ces éléments pour cette demande.

#### **Corps de la demande**

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

#### **Documentation StorageGRID**

["Opérations sur les compartiments"](#)

### **"PutBucketEncryption"**

#### **Paramètres de requête URI et en-têtes de requête**

StorageGRID prend en charge tous [paramètres et en-têtes communs](#)ces éléments pour cette demande.

#### **Demandeur des balises XML de corps**

StorageGRID prend en charge les balises XML de corps de requête suivantes :

- ApplyServerSideEncryptionByDefault
- Rule
- ServerSideEncryptionConfiguration
- SSEAlgorithm

## Documentation StorageGRID

["Opérations sur les compartiments"](#)

## "PutBucketLifecycleConfiguration"

### Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#)ces éléments pour cette demande.

### Demander des balises XML de corps

StorageGRID prend en charge les balises XML de corps de requête suivantes :

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

## Documentation StorageGRID

- ["Opérations sur les compartiments"](#)
- ["Création de la configuration du cycle de vie S3"](#)

## "PutBucketNotificationConfiguration"

### Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#)ces éléments pour cette demande.

### Demander des balises XML de corps

StorageGRID prend en charge les balises XML de corps de requête suivantes :

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

### Documentation StorageGRID

["Opérations sur les compartiments"](#)

## "PutBucketPolicy"

### Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#)ces éléments pour cette demande.

### Corps de la demande

Pour plus de détails sur les champs de corps JSON pris en charge, voir "[Utilisez les règles d'accès au compartiment et au groupe](#)".

## "PutBucketReplication"

### Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#)ces éléments pour cette demande.

### Demander des balises XML de corps

- Bucket
- Destination
- Prefix
- ReplicationConfiguration

- Rule
- Status
- StorageClass

## Documentation StorageGRID

["Opérations sur les compartiments"](#)

## "Étiquetage PutBucketTagging"

### Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#)ces éléments pour cette demande.

### Corps de la demande

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

## Documentation StorageGRID

["Opérations sur les compartiments"](#)

## "PutBucketVersioning"

### Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous [paramètres et en-têtes communs](#)ces éléments pour cette demande.

### Demander les paramètres du corps

StorageGRID prend en charge les paramètres de corps de demande suivants :

- VersioningConfiguration
- Status

## Documentation StorageGRID

["Opérations sur les compartiments"](#)

## "PutObject"

### Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#)éléments pour cette demande, plus les en-têtes supplémentaires suivants :

- 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 demande**

- Données binaires de l'objet

#### **Documentation StorageGRID**

["PutObject"](#)

### ["PutObjectLegalHold"](#)

#### **Paramètres de requête URI et en-têtes de requête**

StorageGRID prend en charge tous [paramètres et en-têtes communs](#)ces éléments pour cette demande.

#### **Corps de la demande**

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

#### **Documentation StorageGRID**

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

### ["PutObjectLockConfiguration"](#)

#### **Paramètres de requête URI et en-têtes de requête**

StorageGRID prend en charge tous [paramètres et en-têtes communs](#)ces éléments pour cette demande.

#### **Corps de la demande**

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

#### **Documentation StorageGRID**

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

### ["PutObjectRetention"](#)

#### **Paramètres de requête URI et en-têtes de requête**

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#)éléments de cette demande, plus l'en-tête supplémentaire suivant :

- x-amz-bypass-governance-retention

### **Corps de la demande**

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

### **Documentation StorageGRID**

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

## **"Marquage PutObject"**

### **Paramètres de requête URI et en-têtes de requête**

StorageGRID prend en charge tous [paramètres et en-têtes communs](#)ces éléments pour cette demande.

### **Corps de la demande**

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

### **Documentation StorageGRID**

["Opérations sur les objets"](#)

## **"Objet de restauration"**

### **Paramètres de requête URI et en-têtes de requête**

StorageGRID prend en charge tous [paramètres et en-têtes communs](#)ces éléments pour cette demande.

### **Corps de la demande**

Pour plus d'informations sur les champs de corps pris en charge, reportez-vous à la section ["Objet de restauration"](#).

## **"SelectObjectContent"**

### **Paramètres de requête URI et en-têtes de requête**

StorageGRID prend en charge tous [paramètres et en-têtes communs](#)ces éléments pour cette demande.

### **Corps de la demande**

Pour plus d'informations sur les champs de corps pris en charge, reportez-vous aux sections suivantes :

- ["Utiliser S3 Select"](#)
- ["SelectObjectContent"](#)

## **"UploadPart"**

### **Paramètres de requête URI et en-têtes de requête**

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#)éléments de cette demande, plus les paramètres de requête URI supplémentaires suivants :

- partNumber
- uploadId

Et ces en-têtes de demande 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 demande**

- Données binaires de la pièce

#### **Documentation StorageGRID**

["UploadPart"](#)

### **"UploadPartCopy"**

#### **Paramètres de requête URI et en-têtes de requête**

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) éléments de cette demande, plus les paramètres de requête URI supplémentaires suivants :

- partNumber
- uploadId

Et ces en-têtes de demande 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 demande**

Aucune

#### **Documentation StorageGRID**

["UploadPartCopy"](#)

# Test de la configuration de l'API REST S3

Vous pouvez utiliser l'interface de ligne de commande d'Amazon Web Services 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'interface de ligne de commande AWS à partir de "[aws.amazon.com/cli](https://aws.amazon.com/cli)".
- Si vous le souhaitez "[crée un terminal d'équilibrage de charge](#)", vous avez . 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](#)".
- Vous avez "[Compte de locataire S3 créé](#)".
- Vous vous êtes connecté au locataire et "[crée une clé d'accès](#)" à .

Pour plus de détails sur ces étapes, reportez-vous "[Configurer les connexions client](#)" à la section .

## Étapes

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

Cet exemple suppose que vous avez configuré un noeud final 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 compartiment est créé avec succès, l'emplacement du compartiment est renvoyé, comme illustré 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. Répertorier le contenu du compartiment pour vérifier que l'objet a été téléchargé.

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

5. Supprimez 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 compartiment.

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

## Implémentation de l'API REST S3 par StorageGRID

### Requêtes des clients en conflit

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

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

### La cohérence

La cohérence assure un équilibre entre la disponibilité des objets et la cohérence de ces objets entre plusieurs 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.

Si vous souhaitez effectuer des opérations d'objet de manière différente, vous pouvez :

- Spécifier une consistance pour [chaque godet](#) .
- Spécifiez une cohérence pour [Chaque opération d'API](#).
- Modifiez la cohérence par défaut à l'échelle de la grille en effectuant l'une des tâches suivantes :
  - Dans le gestionnaire de grille, accédez à **Configuration > Système > Paramètres de stockage > Cohérence du bucket 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` (recherchez **constencyLevel**).

## Valeurs de cohérence

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

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

- **All** : tous les nœuds reçoivent immédiatement les métadonnées de l'objet ou la demande échoue.
- **Strong-global** : garantit la cohérence de lecture après écriture pour toutes les demandes client sur tous les sites. Lorsque la sémantique du quorum est configurée, les comportements suivants s'appliquent :
  - Permet une tolérance aux pannes de site pour les demandes des clients lorsque les grilles comportent trois sites ou plus. Les réseaux à deux sites n'auront pas de tolérance aux pannes de site.
  - Les opérations S3 suivantes ne réussiront pas avec un site en panne :
    - DeleteBucketEncryption
    - MettreBucketBranch
    - PutBucketEncryption
    - PutBucketVersioning
    - PutObjectLegalHold
    - PutObjectLockConfiguration
    - PutObjectRetention

Si nécessaire, vous pouvez "[configurer la sémantique du quorum StorageGRID pour une cohérence globale forte](#)".

- **Strong-site** : les métadonnées de l'objet sont immédiatement distribuées à d'autres nœuds du site. Garantit la cohérence de lecture après écriture pour toutes les demandes client dans un site.
- **Read-After-New-write** : fournit une cohérence lecture-après-écriture pour les nouveaux objets et une cohérence éventuelle pour les mises à jour d'objets. Offre une haute disponibilité et une protection des données garanties. Recommandé dans la plupart des cas.
- **Disponible** : assure la cohérence finale pour les nouveaux objets et les mises à jour d'objets. Pour les compartiments S3, utilisez uniquement si nécessaire (par exemple, pour un compartiment qui contient des valeurs de journal rarement lues ou pour les opérations HEAD ou GET sur des clés qui n'existent pas). Non pris en charge pour les compartiments FabricPool S3.

## Utilisez la cohérence « lecture après nouvelle écriture » et « disponible »

Lorsqu'une opération HEAD ou GET utilise la cohérence « Read-after-New-write », StorageGRID effectue la recherche en plusieurs étapes, comme suit :

- Il recherche tout d'abord l'objet à partir d'une faible cohérence.
- Si cette recherche échoue, elle répète la recherche 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 « Read-after-New-write » mais que l'objet n'existe pas, la recherche d'objet atteint toujours une cohérence équivalente au comportement pour les opérations de type Strong-global. Cette cohérence exigeant la disponibilité de plusieurs copies des métadonnées d'objet sur chaque site, vous pouvez recevoir un nombre élevé d'erreurs de serveur interne 500 si deux nœuds de stockage ou plus sur le même site sont indisponibles.

À moins que vous ayez besoin de garanties de cohérence similaires à Amazon S3, vous pouvez empêcher 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 finale. Cette opération n'a pas abouti pour accroître la cohérence. Il n'est donc pas nécessaire que plusieurs copies des métadonnées de l'objet soient disponibles.

### Indiquez la cohérence du fonctionnement de l'API

Pour définir la cohérence d'une opération d'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 « site fort » 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 compartiment, vous pouvez utiliser la requête StorageGRID "[PRÉSERVER la cohérence du godet](#)". Vous pouvez également "[modifier la cohérence d'un compartiment](#)" utiliser le Gestionnaire de locataires.

Lorsque vous définissez la cohérence d'un godet, tenez compte des points suivants :

- La cohérence d'un compartiment détermine la cohérence utilisée pour les opérations S3 exécutées sur les objets du compartiment ou sur la configuration du compartiment. Cela n'affecte pas les opérations du compartiment lui-même.
- La cohérence d'une opération d'API individuelle remplace la cohérence du compartiment.
- En général, les compartiments doivent utiliser la cohérence par défaut, « Read-after-New-write ». Si les demandes ne fonctionnent pas correctement, modifiez le comportement du client d'application si possible. Ou configurez le client de manière à spécifier la cohérence pour chaque requête d'API. Réglez la cohérence au niveau du godet uniquement en dernier recours.

### Comment les règles de cohérence et les règles ILM interagissent pour affecter la protection des données

La cohérence et les règles ILM de votre choix affectent la protection des objets. Ces paramètres peuvent interagir.

Par exemple, la cohérence utilisée lorsqu'un objet est stocké affecte le placement initial des métadonnées d'objet, tandis que le comportement d'ingestion sélectionné pour la règle ILM affecte le placement initial des

copies d'objet. Comme StorageGRID requiert l'accès aux métadonnées et aux données d'un objet pour répondre aux demandes des clients, le choix de niveaux de protection correspondants pour la cohérence et le comportement d'ingestion permet une meilleure protection initiale des données et des réponses système plus prévisibles.

Les éléments suivants "[options d'ingestion](#)" sont disponibles pour les règles ILM :

#### **Double allocation**

StorageGRID effectue immédiatement des copies intermédiaires de l'objet et renvoie la réussite au client.

Les copies spécifiées dans la règle ILM sont effectuées lorsque cela est possible.

#### **Stricte**

Toutes les copies spécifiées dans la règle ILM doivent être effectuées avant que la réussite ne soit renvoyée au client.

#### **Équilibré**

StorageGRID tente de faire toutes les copies spécifiées dans la règle ILM à l'entrée ; si cela n'est pas possible, des copies intermédiaires sont effectuées et le client est renvoyé avec succès. Les copies spécifiées dans la règle ILM sont effectuées lorsque cela est possible.

### **Exemple d'interaction entre la règle de cohérence et la règle ILM**

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

- **Règle ILM** : Créez trois copies d'objet, une sur le site local et une sur chaque site distant. Adoptez un comportement d'ingestion strict.
- **Cohérence** : Forte-globale (les métadonnées de l'objet sont immédiatement distribuées sur plusieurs sites).

Lorsqu'un client stocke un objet dans la grille, StorageGRID effectue les trois copies de l'objet et distribue les métadonnées à plusieurs sites avant de renvoyer l'opération 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 les sites distants. L'objet est entièrement récupérable sur les autres sites.

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 les sites distants, 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'inter-relation entre la cohérence et les règles ILM peut être complexe. Contactez NetApp si vous avez besoin d'aide.

### **Gestion des versions d'objet**

Vous pouvez définir l'état de gestion des versions d'un compartiment si vous souhaitez conserver plusieurs versions de chaque objet. L'activation de la gestion des versions pour un compartiment vous protège contre la suppression accidentelle d'objets et vous permet de récupérer et de restaurer des versions antérieures d'un objet.

Le système StorageGRID implémente la gestion des versions avec prise en charge de la plupart des

fonctionnalités et avec certaines limites. StorageGRID prend en charge jusqu'à 10,000 versions de chaque objet.

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

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



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

## ILM et gestion des versions

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

Pour les objets S3 dans les compartiments avec gestion des versions, la prise en charge de la gestion des versions vous permet de créer des règles ILM qui utilisent « Noncurrent Time » comme heure de référence (électionnez **Yes** pour la question « Apply this rule to Older object versions only? » ["Étape 1 de l'assistant de création de règles ILM"](#)(Appliquer cette règle aux versions d'objets plus anciennes uniquement ?) dans la section ). Lorsqu'un objet est mis à jour, ses versions précédentes deviennent non actuelles. L'utilisation d'un filtre « Noncurrent Time » vous permet de créer des stratégies 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 partitionné, l'heure qui n'est pas à jour pour la version d'origine de l'objet correspond à la création du téléchargement partitionné pour la nouvelle version, et non à la fin du téléchargement partitionné. Dans des cas limités, l'heure non actuelle de la version d'origine peut être des heures ou des jours plus tôt que l'heure de la version actuelle.

## Informations associées

- ["Suppression d'objets avec version S3"](#)
- ["Règles et règles ILM pour les objets avec version S3 \(exemple 4\)"](#).

## Utilisez l'API REST S3 pour configurer le verrouillage objet S3

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

### Activation du verrouillage objet S3 pour un compartiment

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

Le verrouillage objet S3 est un paramètre permanent qui ne peut être activé que lorsque vous créez un compartiment. Une fois un compartiment créé, vous ne pouvez ni ajouter ni désactiver le verrouillage objet S3.

Pour activer le verrouillage objet S3 pour un compartiment, utilisez l'une des méthodes suivantes :

- Créez le compartiment à l'aide du Gestionnaire des locataires. Voir "[Créer un compartiment S3](#)".
- Créez le compartiment à l'aide d'une demande CreateBucket avec l' `x-amz-bucket-object-lock-enabled` en-tête de la demande. Voir "[Opérations sur les compartiments](#)".

Le verrouillage objet S3 requiert la gestion des versions des compartiments, qui est automatiquement activée lors de la création du compartiment. Vous ne pouvez pas suspendre la gestion des versions pour le compartiment. Voir "[Gestion des versions d'objet](#)".

## Paramètres de conservation par défaut d'un compartiment

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

### Mode de rétention par défaut

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

### Période de conservation par défaut

Une période de conservation par défaut peut être spécifiée en années ou en jours pour chaque compartiment.

## Comment définir la conservation par défaut d'un compartiment

Pour définir la rétention par défaut d'un compartiment, utilisez l'une des méthodes suivantes :

- Gérez les paramètres de compartiment depuis le gestionnaire de locataires. Voir "[Créer un compartiment S3](#)" et "[Mettre à jour la conservation par défaut du verrouillage d'objet S3](#)".
- Exécutez une demande PutObjectLockConfiguration pour que le compartiment indique le mode par défaut et le nombre de jours ou d'années par défaut.

### PutObjectLockConfiguration

La demande PutObjectLockConfiguration vous permet de définir et de modifier le mode de rétention par défaut et la période de rétention par défaut pour un compartiment pour lequel S3 Object Lock est activé. Vous pouvez également supprimer les paramètres de conservation par défaut configurés précédemment.

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

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

Vous devez disposer de l'``s3:PutBucketObjectLockConfiguration`` autorisation, ou être root, pour effectuer cette opération.

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

### Exemple de demande

Cet exemple active le verrouillage objet S3 pour un compartiment 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 conservation par défaut d'un compartiment

Pour déterminer si le verrouillage objet S3 est activé pour un compartiment et pour afficher le mode de conservation et la période de conservation par défaut, utilisez l'une des méthodes suivantes :

- Affichez le compartiment dans le gestionnaire de locataires. Voir "[Afficher les compartiments S3](#)".
- Émettre une demande `GetObjectLockConfiguration`.

## GetObjectLockConfiguration

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

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

Vous devez disposer de l'`s3:GetBucketObjectLockConfiguration` autorisation, ou être root, pour effectuer 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:
iVmcB70XXJRkRH1FiVq1151/T24gRfpwpuZrEG11Bb9ImOMAAe98oxSpX1knabA0LTvBYJpSIX
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 compartiment lorsque le verrouillage objet S3 est activé peut contenir une combinaison d'objets avec ou sans paramètres de conservation du verrouillage objet S3.

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

Vous pouvez spécifier les paramètres suivants pour chaque objet :

- **Mode de conservation** : CONFORMITÉ ou GOUVERNANCE.
- **Conserver-jusqu'à-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 jusqu'à est dans le futur, l'objet peut être récupéré, mais il ne peut pas être modifié ou supprimé. La date de conservation jusqu'à peut être augmentée, mais cette date ne peut pas être réduite ou supprimée.
  - En mode GOUVERNANCE, les utilisateurs disposant d'une autorisation spéciale peuvent contourner le paramètre conserver jusqu'à la date. Ils peuvent supprimer une version d'objet avant la fin de sa période de conservation. Ils peuvent également augmenter, diminuer ou même supprimer la date de conservation jusqu'à.
- **Mise en garde légale** : l'application d'une mise en garde légale à une version d'objet verrouille immédiatement cet objet. Par exemple, vous devrez peut-être mettre une obligation légale sur un objet lié à une enquête ou à un litige juridique. Une obligation 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 jusqu'à. Si une version d'objet est en attente 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 compartiment, émettez une "["PutObject"](#)", "["Objet de copie"](#)" ou "["CreateMultipartUpload"](#)" une demande.

Vous pouvez utiliser les éléments suivants :

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



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

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

- La valeur conserver jusqu'à la date doit être au format 2020-08-10T21:46:00Z. Les secondes fractionnaires sont autorisées, mais seuls 3 chiffres après la virgule sont conservés (précision des millisecondes). Les autres formats ISO 8601 ne sont pas autorisés.

- La date de conservation doit être ultérieure.

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

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

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

- L'Content-MD5 en-tête de requête est requis si un `x-amz-object-lock-\*` en-tête de requête est présent dans la requête PutObject. Content-MD5 N'est pas nécessaire pour CopyObject ou CreateMultipartUpload.
- Si S3 Object Lock n'est pas activé dans le compartiment et qu'un x-amz-object-lock-\* 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 faire correspondre le comportement AWS. Cependant, lors de l'ingestion d'un objet dans un compartiment lorsque le verrouillage objet S3 est activé, StorageGRID effectue toujours une entrée à double validation.
- Une réponse ultérieure à la version GET ou HeadObject inclura les en-têtes x-amz-object-lock-mode, x-amz-object-lock-retain-until-date et x-amz-object-lock-legal-hold, s'il est configuré et si l'expéditeur de la demande a les autorisations correctes s3:Get\*.

Vous pouvez utiliser la s3:object-lock-remaining-retention-days clé de condition de règle pour limiter les périodes de conservation minimale et maximale autorisée 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 conservation d'une version d'objet existante, vous pouvez effectuer les opérations de sous-ressource d'objet suivantes :

- PutObjectLegalHold

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

- PutObjectRetention

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

### Comment utiliser le mode GOUVERNANCE

Les utilisateurs disposant de cette s3:BypassGovernanceRetention autorisation peuvent contourner les paramètres de rétention actifs d'un objet qui utilise le mode de GOUVERNANCE. Toutes les opérations de SUPPRESSION ou de PutObjectRetention doivent inclure l' `x-amz-bypass-governance-retention:true` en-tête de la demande. Ces utilisateurs peuvent effectuer les opérations supplémentaires suivantes :

- Exécutez les opérations DeleteObject ou DeleteObjects pour supprimer une version d'objet avant que sa période de rétention ne soit écoulée.

Impossible de supprimer les objets qui sont en attente légale. La mise en attente légale doit être désactivée.

- Exécutez des opérations PutObjectRetention qui changent le mode d'une version d'objet de GOUVERNANCE à CONFORMITÉ avant que la période de conservation de l'objet ne soit écoulée.

Le passage du mode DE CONFORMITÉ À LA GOUVERNANCE n'est jamais autorisé.

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

#### Informations associées

- ["Gestion des objets avec le verrouillage d'objets S3"](#)
- ["Utilisez le verrouillage d'objet S3 pour conserver les objets"](#)
- ["Guide de l'utilisateur d'Amazon simple Storage Service : verrouillage d'objets"](#)

## Création de la configuration du cycle de vie S3

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

L'exemple simple de cette section illustre la façon dont une configuration du cycle de vie S3 peut contrôler la suppression de certains objets (expirés) dans des compartiments S3 spécifiques. L'exemple de cette section est fourni à titre d'illustration uniquement. Pour plus d'informations sur la création de configurations de cycle de vie S3, reportez-vous à la section ["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, mais pas les actions de transition.

### La configuration du cycle de vie

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

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

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

Chaque objet respecte les paramètres de conservation du cycle de vie d'un compartiment S3 ou une règle ILM. Lorsqu'un cycle de vie d'un compartiment S3 est configuré, les actions d'expiration du cycle de vie remplacent la règle 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 des compartiments utilisent les paramètres de conservation de la règle 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 règle ILM ne sont pas utilisés et les versions d'objet sont conservées indéfiniment. Voir ["Exemples de priorités pour le cycle de vie des compartiments S3 et les règles ILM"](#).

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

## ILM tout au long de la vie d'un objet".



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

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

- DeleteBucketLifecycle
- GetBucketLifecycleConfiguration
- PutBucketLifecycleConfiguration

### Créer une configuration de cycle de vie

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

1. La règle 1 s'applique uniquement aux objets qui correspondent au préfixe `category1/` et qui ont une `key2` valeur de `tag2`. Le `Expiration` paramètre indique 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` paramètre indique que les objets correspondant au filtre expireront 100 jours après leur ingestion.



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

3. La règle 3 s'applique uniquement aux objets qui correspondent au préfixe `category3/`. Le `Expiration` paramètre spécifie que toute version non actuelle des objets correspondants expirera 50 jours après qu'ils ne soient plus à jour.

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

## Appliquez la configuration du cycle de vie au compartiment

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

Cette requête applique la configuration de cycle de vie du fichier d'exemple aux objets d'un compartiment nommé testbucket.

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

Pour vérifier qu'une configuration de cycle de vie a été correctement appliquée au compartiment, exécutez une demande GetBucketLifecycleConfiguration. Par exemple :

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

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

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

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



Étant donné que le cycle de vie d'un compartiment remplace ILM, la `expiry-date` date affichée est la date réelle à laquelle l'objet sera supprimé. Pour plus de détails, voir ["Méthode de détermination de la conservation des objets"](#).

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

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

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

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

Par exemple, cette requête HeadObject a été utilisée pour obtenir les métadonnées du même objet dans le compartiment 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 compartiments avec gestion des versions, l'`x-amz-expiration` en-tête de réponse s'applique uniquement aux versions actuelles des objets.

## Recommandations pour l'implémentation de l'API REST S3

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

### Recommandations pour les têtes à des objets inexistantes

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 ». ["la cohérence"](#). Par exemple, vous devez utiliser la cohérence « Disponible » si votre application HEAD un emplacement avant d'y effectuer un PUT.

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

Vous pouvez définir la cohérence « disponible » pour chaque compartiment à l'aide de la ["PRÉSERVER la cohérence du godet"](#) requête ou spécifier la cohérence dans l'en-tête de demande pour une opération d'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 du compartiment.

### Compartiments créés dans StorageGRID 11.4 ou version antérieure

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

`mybucket/mydir/f8e3-image3132.jpg`

Au lieu de ce format :

`mybucket/f8e3-image3132.jpg`

### Compartiments créés dans StorageGRID 11.4 ou version ultérieure

Il n'est pas nécessaire de restreindre les noms de clés d'objet pour répondre aux bonnes pratiques de performances. Dans la plupart des cas, vous pouvez utiliser des valeurs aléatoires pour les quatre premiers caractères des noms de clé d'objet.

À cela s'exception près un workload 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, il est possible de faire varier la première partie du nom de clé tous les mille objets avec une date comme la date. Supposons par exemple qu'un client S3 écrit généralement 2,000 objets/seconde et que la règle de cycle de vie ILM ou compartiment supprime tous les objets au bout de trois jours. Pour réduire l'impact sur les performances, vous pouvez nommer les clés comme suit : `/mybucket/mydir/yyyymmddhhmmss-random_UUID.jpg`

## Recommandations pour les « lectures de plage »

Si ["option globale pour compresser les objets stockés"](#) est activé, les applications client S3 doivent éviter d'effectuer des opérations `GetObject` qui spécifient une plage d'octets. 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 objet très volumineux 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 client peuvent être en attente.

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

# Prise en charge de l'API REST Amazon S3

## Détails de l'implémentation de l'API REST S3

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

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

### Traitement de la date

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

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

### En-têtes de demande commune

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

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

### En-têtes de réponse commune

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

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

## Authentifier les demandes

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

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

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

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

### Utilisez l'en-tête HTTP Authorization

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

### Utiliser les paramètres de requête

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

## Opérations sur le service

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

Fonctionnement	Mise en place
Listseaux  (Anciennement appelé GET Service)	Mise en œuvre avec tout le comportement de l'API REST Amazon S3. D'être modifiées sans préavis.
DÉCOUVREZ l'utilisation du stockage	La demande StorageGRID " <a href="#">DÉCOUVREZ l'utilisation du stockage</a> " indique la quantité totale de stockage utilisée par un compte et pour chaque compartiment associé au compte. Il s'agit d'une opération sur le service avec un chemin d'accès de / et un paramètre de requête personnalisée (?x-ntap-sg-usage) ajouté.

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

## Opérations sur les compartiments

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

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

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

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

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

- ["Guide de l'utilisateur d'Amazon simple Storage Service : quotas de compartiments, restrictions et limites"](#)
- ["Configuration des noms de domaine de terminaux S3"](#)

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

Vous pouvez vérifier si les mises à jour de l'heure du dernier accès sont activées ou désactivées pour les compartiments individuels. Voir ["HEURE du dernier accès au compartiment"](#).

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

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

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

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

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

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

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

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

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

## Opérations sur les objets

### Opérations sur les objets

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

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

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

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

Fonctionnement	Mise en place
DeleteObject  (Précédemment nommé, SUPPRIMER plusieurs objets)	<p>L'authentification multifacteur (MFA) et l'en-tête de réponse <code>x-amz-mfa</code> ne sont pas pris en charge.</p> <p>Lors du traitement d'une requête DeleteObject, StorageGRID tente de supprimer immédiatement toutes les copies de l'objet de tous les emplacements stockés. En cas de succès, StorageGRID renvoie immédiatement une réponse au client. Si toutes les copies ne peuvent pas être supprimées dans les 30 secondes (par exemple, parce qu'un emplacement est temporairement indisponible), StorageGRID met les copies en file d'attente pour suppression et indique que le client a réussi.</p> <p><b>Gestion des versions</b></p> <p>Pour supprimer une version spécifique, le demandeur doit être le propriétaire du compartiment et utiliser la <code>versionId</code> sous-ressource. L'utilisation de cette sous-ressource supprime définitivement la version. Si le <code>versionId</code> correspond à un marqueur de suppression, l'en-tête de réponse <code>x-amz-delete-marker</code> est renvoyé à <code>true</code>.</p> <ul style="list-style-type: none"> <li>Si un objet est supprimé sans la <code>versionId</code> sous-ressource sur un compartiment avec la gestion des versions activée, il génère un marqueur de suppression. Le <code>versionId</code> pour le marqueur de suppression est renvoyé à l'aide de <code>x-amz-version-id</code> l'en-tête de réponse et l'<code>x-amz-delete-marker</code> en-tête de réponse est renvoyé à <code>true</code>.</li> <li>Si un objet est supprimé sans la <code>versionId</code> sous-ressource sur un compartiment avec la gestion des versions suspendue, il entraîne la suppression permanente d'une version 'null' existante ou d'un marqueur de suppression 'null', et la génération d'un nouveau marqueur de suppression 'null'. L'<code>x-amz-delete-marker</code> en-tête de réponse est renvoyé à <code>true</code>.</li> </ul> <p><b>Remarque</b> : dans certains cas, plusieurs marqueurs de suppression peuvent exister pour un objet.</p> <p>Reportez-vous à la section "<a href="#">Utilisez l'API REST S3 pour configurer le verrouillage objet S3</a>" pour savoir comment supprimer des versions d'objets en mode GOUVERNANCE.</p>
	<p>L'authentification multifacteur (MFA) et l'en-tête de réponse <code>x-amz-mfa</code> ne sont pas pris en charge.</p> <p>Plusieurs objets peuvent être supprimés dans le même message de demande.</p> <p>Reportez-vous à la section "<a href="#">Utilisez l'API REST S3 pour configurer le verrouillage objet S3</a>" pour savoir comment supprimer des versions d'objets en mode GOUVERNANCE.</p>

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

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

## Utiliser S3 Select

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



Les éléments non répertoriés ne sont pas pris en charge.

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

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

### Clauses

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

### Types de données

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

### Opérateurs

#### Opérateurs logiques

- ET
- PAS
- OU

#### Opérateurs de comparaison

- <
- >
- &lt ;=
- >=
- =
- =
- <>

- !=
- ENTRE
- DANS

### Opérateurs de correspondance de répétition

- COMME
- \_
- %

### Opérateurs unitaires

- EST NULL
- N'EST PAS NULL

### Opérateurs mathématiques

- +
- -
- \*
- /
- %

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

### Fonctions d'agrégation

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

### Fonctions conditionnelles

- CASSE
- FUSIONNE
- NULLIF

### Fonctions de conversion

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

### Fonctions de date

- DATE\_AJOUTER
- DATE\_DIFF

- EXTRAIRE
- TO\_STRING
- TO\_TIMESTAMP
- CODE D'ARTICLE

#### Fonctions de chaîne

- CHAR\_LENGTH, CARACTÈRE\_LENGTH
- ABAISSEMENT
- SOUS-CHAÎNE
- GARNITURE
- SUPÉRIEUR

#### Utilisez le cryptage côté serveur

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

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

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

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



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



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

#### Utiliser SSE

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

`x-amz-server-side-encryption`

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

- ["PutObject"](#)

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

## Utiliser SSE-C

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

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

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

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

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

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

- Vous devez utiliser https.



StorageGRID rejette toute demande effectuée sur http lors de l'utilisation de SSE-C. Pour des raisons de sécurité, vous devez considérer que toute clé que vous envoyez accidentellement à l'aide de http est compromise. Mettez la clé au rebut et tournez-la selon les besoins.

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

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



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

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

## Informations associées

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

## Objet de copie

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

## Résoudre les conflits

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

## Taille de l'objet

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

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



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

## Caractères UTF-8 dans les métadonnées utilisateur

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

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

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

de la clé contient des caractères non imprimables.

#### En-têtes de demande pris en charge

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

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

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

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

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

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

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

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

- En-têtes de demande SSE :

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

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

### En-têtes de requête non pris en charge

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

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

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

- x-amz-website-redirect-location

### Options de classe de stockage

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

- STANDARD

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

- REDUCED\_REDUNDANCY

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



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

### Utilisation de x-amz-copy-source dans CopyObject

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

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

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

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

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

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

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



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

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



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

## Gestion des versions

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

## GetObject

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

### GetObject et objets multipièces

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

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

### Caractères UTF-8 dans les métadonnées utilisateur

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

### En-tête de demande pris en charge

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

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

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

### En-tête de demande non pris en charge

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

- **x-amz-website-redirect-location**

## Gestion des versions

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

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

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

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



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

## Comportement de GetObject pour les objets de pool de stockage cloud

Si un objet a été stocké dans un "[Pool de stockage cloud](#)", le comportement d'une requête GetObject dépend de l'état de l'objet. Voir "[Objet principal](#)" pour plus de détails.



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

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

## Objets partitionnés ou segmentés dans un pool de stockage cloud

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

Dans ces cas :

- La requête GetObject peut renvoyer certaines données, mais s'arrête à mi-chemin du transfert.
- Une requête GetObject suivante peut renvoyer 403 Forbidden.

## GetObject et la réplication inter-grille

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

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



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

## Objet principal

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

## Objets en-tête et objets multi pièces

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

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

## Caractères UTF-8 dans les métadonnées utilisateur

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

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

#### En-tête de demande pris en charge

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

- x-amz-checksum-mode

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

#### En-tête de demande non pris en charge

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

- x-amz-website-redirect-location

#### Gestion des versions

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

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

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

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

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

#### HeadObject Responses for Cloud Storage Pool objects

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

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

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

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

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

## Objets partitionnés ou segmentés dans Cloud Storage Pool

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

### HeadObject et réplication inter-grid

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

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



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

### PutObject

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

#### Résoudre les conflits

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

## Taille de l'objet

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

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



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

## Taille des métadonnées utilisateur

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

## Caractères UTF-8 dans les métadonnées utilisateur

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

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

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

## Limites des balises d'objet

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

## Propriété de l'objet

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

## En-têtes de demande pris en charge

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

- Cache-Control
- Content-Disposition

- Content-Encoding

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

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

- Content-Language

- Content-Length

- Content-MD5

- Content-Type

- Expires

- Transfer-Encoding

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

- `x-amz-checksum-sha256`
- `x-amz-meta-`, suivi d'une paire nom-valeur contenant des métadonnées définies par l'utilisateur.

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

`x-amz-meta-name: value`

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

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

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



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

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

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

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

- En-têtes de demande SSE :

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

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

#### En-têtes de requête non pris en charge

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

- If-Match
- If-None-Match
- x-amz-acl
- x-amz-sdk-checksum-algorithm
- x-amz-trailer
- x-amz-website-redirect-location

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

#### Options de classe de stockage

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

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

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

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

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

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

- **REDUCED\_REDUNDANCY**

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

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

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

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

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

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

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

- **SSE**: Utilisez l’en-tête suivant si vous voulez chiffrer l’objet avec une clé unique gérée par StorageGRID.
  - `x-amz-server-side-encryption`

Lorsque l’`x-amz-server-side-encryption`en-tête n’est pas inclus dans la demande PutObject, la grille "paramètre de chiffrement d’objet stocké" est omise de la réponse PutObject.

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



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



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

## Gestion des versions

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

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

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

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

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



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

Pour plus de détails, reportez-vous à ["Calculs de signature pour l'en-tête d'autorisation : transfert de charge utile dans un seul bloc \(signature AWS version 4\)"](#).

## Informations associées

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

## Objet de restauration

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

## Type de demande pris en charge

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

## Gestion des versions

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

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

Si un objet a été stocké dans un "[Pool de stockage cloud](#)", une requête `RestoreObject` a le comportement suivant, en fonction de l'état de l'objet. Voir "[Objet principal](#)" pour plus de détails.

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

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

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

## SelectObjectContent

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

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

### Avant de commencer

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

### Exemple de syntaxe de demande CSV

```

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

```

#### Exemple de syntaxe de demande de parquet

```

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

```

#### Exemple de requête SQL

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

```

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

```

Les premières lignes du fichier à interroger, SUB-EST2020\_ALL.csv, ressemblent à ceci :

```

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

```

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

```

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

```

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

```

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

```

## Exemple d'utilisation de l'interface de ligne de commande AWS (parquet)

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

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

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

## Opérations pour les téléchargements partitionnés

### Opérations pour les téléchargements partitionnés

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

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

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

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

- Lors de l'évaluation d'ILM pour une pièce, StorageGRID filtre la taille de la pièce, et non la taille de l'objet. Ainsi, certaines parties d'un objet peuvent être stockées dans des emplacements qui ne respectent pas les exigences de la règle ILM pour l'ensemble de l'objet. Par exemple, si une règle indique que tous les objets de 10 Go ou plus sont stockés sur DC1 alors que tous les objets plus petits sont stockés sur DC2, chaque partie de 1 Go d'un téléchargement partitionné en 10 parties est stockée sur DC2 lors de l'ingestion. Cependant, lorsque ILM est évalué pour l'objet dans son ensemble, toutes les parties de l'objet sont déplacées vers DC1.
- Toutes les opérations de téléchargement en plusieurs parties prennent en charge StorageGRID "valeurs de cohérence".
- Lorsqu'un objet est ingéré à l'aide d'un téléchargement partitionné, le "[Seuil de segmentation d'objet \(1 Gio\)](#)" n'est pas appliqué.
- Si nécessaire, vous pouvez l'utiliser "[chiffrement côté serveur](#)" avec les téléchargements partitionnés. Pour utiliser SSE (chiffrement côté serveur avec des clés gérées par StorageGRID), vous incluez l'en-`x-amz-server-side-encryption` tête de requête dans la requête CreateMultipartUpload uniquement. Pour utiliser SSE-C (chiffrement côté serveur avec des clés fournies par le client), vous devez spécifier les trois mêmes en-têtes de requête de clé de chiffrement dans la demande CreateMultipartUpload et dans chaque demande UploadPart suivante.
- Un objet téléchargé en plusieurs parties est inclus dans un "[seau de branche](#)" si l'ingestion a été initiée avant l'horodatage Avant du bucket de base, quel que soit le moment où le téléchargement est terminé.

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

### CompleteMultipartUpload

L'opération CompleteMultipartUpload effectue un téléchargement partitionné d'un objet en assemblant les pièces précédemment téléchargées.



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

## Résoudre les conflits

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

### En-têtes de demande pris en charge

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

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

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

- STANDARD

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

- REDUCED\_REDUNDANCY

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



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



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



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

### En-têtes de requête non pris en charge

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

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

- `x-amz-trailer`

## Gestion des versions

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

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

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

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

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

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

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

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

## CreateMultipartUpload

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

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

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

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

- STANDARD (Par défaut)
  - **Dual commit** : si la règle ILM spécifie l'option d'acquisition Dual commit, dès qu'un objet est ingéré, une deuxième copie de cet objet est créée et distribuée à un autre nœud de stockage (double commit). Une fois la règle ILM évaluée, StorageGRID détermine si ces copies intermédiaires initiales répondent aux instructions de placement de la règle. Si ce n'est pas le cas, de nouvelles copies d'objet peuvent

avoir besoin d'être effectuées à différents emplacements et les copies intermédiaires initiales peuvent avoir besoin d'être supprimées.

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

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

- **REDUCED\_REDUNDANCY**

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

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

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

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

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

#### En-têtes de demande pris en charge

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

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

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

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

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

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

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

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

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



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

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

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

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

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

- En-têtes de demande SSE :

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

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



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

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

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

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



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

#### En-têtes de requête non pris en charge

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

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

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

#### Gestion des versions

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

#### ListMultipartUploads

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

Les paramètres de demande suivants sont pris en charge :

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

## Gestion des versions

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

## UploadPart

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

### En-têtes de demande pris en charge

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

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

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

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

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

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

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

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

### En-têtes de requête non pris en charge

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

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

## Gestion des versions

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

## UploadPartCopy

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

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

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

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

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

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

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

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

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

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

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

## Gestion des versions

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

## Réponses d'erreur

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

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

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

<b>Nom</b>	<b>Statut HTTP</b>
InvalidRequest	400 demande erronée
InvalidStorageClass	400 demande erronée
InvalidTag	400 demande erronée
URI non valide	400 demande erronée
KeyToolong	400 demande erronée
MalformedXML	400 demande erronée
MetadaTooLarge	400 demande erronée
MethodNotAlldue	405 méthode non autorisée
MissingContentLength	411 longueur requise
Erreur MissingestBodyError	400 demande erronée
En-tête MissinécuritéSent	400 demande erronée
NoSuchBucket	404 introuvable
NoSuchKey	404 introuvable
NoSuchUpload	404 introuvable
Note d'implémentation	501 non mis en œuvre
NoSuchBucketPolicy	404 introuvable
ObjectLockNotConfigurationError	404 introuvable
Pré-conditionFailed	412 Echec de la condition préalable
RequestTimeTooSkewed	403 interdit
Disponibilité des services	503 Service indisponible
SignatureDoesNotMatch	403 interdit
TooManyseaux	400 demande erronée

Nom	Statut HTTP
UserKeyMustBeSpecified	400 demande erronée

## Codes d'erreur personnalisés StorageGRID

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

## Opérations 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.

Fonctionnement	Description
"OPTIMISEZ la cohérence des compartiments"	Renvoie la cohérence appliquée à un compartiment particulier.
"PRÉSERVER la cohérence du godet"	Définit la cohérence appliquée à un compartiment spécifique.
"HEURE du dernier accès au compartiment"	Indique si les mises à jour de l'heure du dernier accès sont activées ou désactivées pour un compartiment spécifique.
"METTRE l'heure du dernier accès au compartiment"	Permet d'activer ou de désactiver les mises à jour de l'heure du dernier accès pour un compartiment spécifique.
"SUPPRIMEZ la configuration de notification des métadonnées de compartiment"	Supprime le XML de configuration de notification de métadonnées associé à un compartiment spécifique.
"CONFIGURATION DES notifications de métadonnées de compartiment"	Renvoie le XML de configuration de notification de métadonnées associé à un compartiment spécifique.
"CONFIGURATION de notification des métadonnées de compartiment"	Configure le service de notification des métadonnées pour un compartiment.
"DÉCOUVREZ l'utilisation du stockage"	Indique la quantité totale de stockage utilisée par un compte et par compartiment associé au compte.
"Obsolète : CreateBucket avec paramètres de conformité"	Obsolète et non pris en charge : vous ne pouvez plus créer de compartiments avec conformité activée.
"Obsolète : CONFORMITÉ DES compartiments"	Obsolète mais pris en charge : renvoie les paramètres de conformité actuellement en vigueur pour un compartiment compatible existant.
"Obsolète : conformité DES compartiments PUT"	Obsolète mais pris en charge : permet de modifier les paramètres de conformité d'un compartiment compatible existant.

## OPTIMISEZ la cohérence des compartiments

La demande de cohérence GET Bucket vous permet de déterminer la cohérence appliquée à un compartiment spécifique.

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

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

## Exemple de demande

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

## Réponse

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

La cohérence	Description
tous	Tous les nœuds reçoivent les données immédiatement, sinon la requête échoue.
forte croissance mondiale	Garantit une cohérence de lecture après écriture pour toutes les demandes client sur tous les sites.
site fort	Garantit la cohérence de lecture après écriture pour toutes les demandes client dans un site.
lecture-après-nouvelle-écriture	(Valeur par défaut) assure la cohérence en lecture après écriture des nouveaux objets et la cohérence des mises à jour des objets. Offre une haute disponibilité et une protection des données garanties. Recommandé dans la plupart des cas.
disponibilité	Assure la cohérence pour les nouveaux objets et les mises à jour d'objets. Pour les compartiments S3, utilisez uniquement si nécessaire (par exemple, pour un compartiment qui contient des valeurs de journal rarement lues ou pour les opérations HEAD ou GET sur des clés qui n'existent pas). Non pris en charge pour les compartiments FabricPool S3.

## Exemple de réponse

```

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

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

```

## Informations associées

["La cohérence"](#)

## PRÉSERVER la cohérence du godet

La demande de cohérence PUT Bucket vous permet d'indiquer la cohérence à appliquer aux opérations effectuées sur un compartiment.

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

### Avant de commencer

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

### Demande

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

La cohérence	Description
tous	Tous les nœuds reçoivent les données immédiatement, sinon la requête échoue.
forte croissance mondiale	Garantit une cohérence de lecture après écriture pour toutes les demandes client sur tous les sites.
site fort	Garantit la cohérence de lecture après écriture pour toutes les demandes client dans un site.
lecture-après-nouvelle-écriture	(Valeur par défaut) assure la cohérence en lecture après écriture des nouveaux objets et la cohérence des mises à jour des objets. Offre une haute disponibilité et une protection des données garanties. Recommandé dans la plupart des cas.

La cohérence	Description
disponibilité	Assure la cohérence pour les nouveaux objets et les mises à jour d'objets. Pour les compartiments S3, utilisez uniquement si nécessaire (par exemple, pour un compartiment qui contient des valeurs de journal rarement lues ou pour les opérations HEAD ou GET sur des clés qui n'existent pas). Non pris en charge pour les compartiments FabricPool S3.

**Note:** en général, vous devez utiliser la cohérence "lecture-après-nouvelle-écriture". Si les demandes ne fonctionnent pas correctement, modifiez le comportement du client d'application si possible. Ou configurez le client de manière à spécifier la cohérence pour chaque requête d'API. Réglez la cohérence au niveau du godet 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 associées

["La cohérence"](#)

## HEURE du dernier accès au compartiment

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

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

### 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 du temps de dernier accès sont activées pour le compartiment.

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

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

## METTRE l'heure du dernier accès au compartiment

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

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

À partir de StorageGRID version 10.3, les mises à jour de l'heure du dernier accès sont désactivées par défaut pour tous les nouveaux compartiments. Si des compartiments ont été créés à l'aide d'une version antérieure de StorageGRID et que vous souhaitez faire correspondre le nouveau comportement par défaut, vous devez désactiver explicitement les mises à jour de la dernière heure d'accès pour chacune de ces rubriques précédentes. Vous pouvez activer ou désactiver les mises à jour de l'heure du dernier accès à l'aide de la demande PUT Bucket Last Access Time ou de la page de détails d'un compartiment dans le Gestionnaire de locataires. Voir "[Activez ou désactivez les mises à jour de l'heure du dernier accès](#)".

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

- 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 ne mettent à jour que les métadonnées mettent également à jour l'heure du dernier accès. L'objet est ajouté aux files d'attente pour l'évaluation ILM.
- Si les mises à jour de l'heure du dernier accès sont désactivées pour le compartiment source, les requêtes CopyObject ne mettent pas à jour l'heure du dernier accès pour le compartiment source. L'objet copié n'est pas ajouté aux files d'attente pour l'évaluation ILM du compartiment source. Cependant, pour la destination, les requêtes 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.
- CompleteMultipartUpload demande la mise à jour de l'heure du dernier accès. L'objet terminé est ajouté aux files d'attente pour l'évaluation ILM.

## Exemples de demandes

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

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

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

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

## SUPPRIMEZ la configuration de notification des métadonnées de compartiment

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

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

### Exemple de demande

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

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

## CONFIGURATION DES notifications de métadonnées de compartiment

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

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

## Exemple de demande

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

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

## Réponse

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

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

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

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

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

Nom	Description	Obligatoire
Urne	<p>URN de la destination où les métadonnées d'objet sont envoyées. Doit être l'URN d'un terminal StorageGRID avec les propriétés suivantes :</p> <ul style="list-style-type: none"> <li>• es doit être le troisième élément.</li> <li>• L'URN doit se terminer par l'index et le type où les métadonnées sont stockées, sous la forme domain-name/myindex/mytype.</li> </ul> <p>Les terminaux sont configurés à l'aide du Gestionnaire de locataires ou de l'API de gestion des locataires. Ils se présentent sous la forme suivante :</p> <ul style="list-style-type: none"> <li>• arn:aws:es:_region:account-ID_:domain/mydomain/myindex/mytype</li> <li>• urn:mysite:es:::mydomain/myindex/mytype</li> </ul> <p>Le noeud final doit être configuré avant la soumission du XML de configuration, ou la configuration échouera avec une erreur 404.</p> <p>L'urne est incluse dans l'élément destination.</p>	Oui

### Exemple de réponse

Le XML inclus entre les

<MetadataNotificationConfiguration></MetadataNotificationConfiguration> balises montre comment l'intégration avec un noeud final d'intégration de recherche est configurée pour le compartiment. Dans cet exemple, les métadonnées d'objet sont envoyées à un index Elasticsearch nommé current et 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 associées

["Utilisez un compte de locataire"](#)

## CONFIGURATION de notification des métadonnées de compartiment

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

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

#### Demande

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

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

Les configurations avec des préfixes qui se chevauchent ne sont pas valides et sont rejetées lorsqu'elles sont soumises. Par exemple, une configuration comprenant une règle pour les objets avec le préfixe et une seconde règle pour les objets avec test le préfixe test2 ne serait pas autorisée.

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

```

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

```

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

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

Nom	Description	Obligatoire
État	<p>L'état peut être « activé » ou « désactivé ». Aucune action n'est prise pour les règles désactivées.</p> <p>Inclus dans l'élément règle.</p>	Oui
Préfixe	<p>Les objets qui correspondent au préfixe sont affectés par la règle et leurs métadonnées sont envoyées à la destination spécifiée.</p> <p>Pour faire correspondre tous les objets, spécifiez un préfixe vide.</p> <p>Inclus dans l'élément règle.</p>	Oui
Destination	<p>Balise de conteneur pour la destination d'une règle.</p> <p>Inclus dans l'élément règle.</p>	Oui
Urne	<p>URN de la destination où les métadonnées d'objet sont envoyées. Doit être l'URN d'un terminal StorageGRID avec les propriétés suivantes :</p> <ul style="list-style-type: none"> <li>• es doit être le troisième élément.</li> <li>• L'URN doit se terminer par l'index et le type où les métadonnées sont stockées, sous la forme domain-name/myindex/mytype.</li> </ul> <p>Les terminaux sont configurés à l'aide du Gestionnaire de locataires ou de l'API de gestion des locataires. Ils se présentent sous la forme suivante :</p> <ul style="list-style-type: none"> <li>• arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype</li> <li>• urn:mysite:es:::mydomain/myindex/mytype</li> </ul> <p>Le noeud final doit être configuré avant la soumission du XML de configuration, ou la configuration échouera avec une erreur 404.</p> <p>L'urne est incluse dans l'élément destination.</p>	Oui

## Exemples de demandes

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

```
PUT /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: 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 des objets qui correspondent au préfixe `/images` sont envoyées à une destination, tandis que les métadonnées d'objet des objets correspondant au préfixe `/videos` sont envoyées à une seconde 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-1:2222222:domain/es-
domain/graphics/videotype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>

```

### JSON généré par le service d'intégration de la recherche

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

Cet exemple montre un exemple de fichier JSON qui pourrait être généré lors de la création d'un objet avec la clé SGWS/Tagging.txt dans un compartiment nommé test. Le test compartiment n'est pas versionné, la balise est donc `versionId` vide.

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

## Métadonnées d'objet incluses dans les notifications de métadonnées

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

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

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

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

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

#### Informations associées

["Utilisez un compte de locataire"](#)

## DEMANDE d'utilisation du stockage

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

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

Par défaut, StorageGRID tente de récupérer les informations d'utilisation à l'aide d'une cohérence globale forte. S'il est impossible d'obtenir une cohérence globale élevée, StorageGRID tente de récupérer les informations relatives à l'utilisation de façon cohérente sur les sites.

Pour effectuer cette opération, vous devez disposer de l'autorisation `s3>ListAllMyseaux` ou être root de compte.

#### 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 contient quatre objets et 12 octets de données dans deux compartiments. Chaque compartiment contient deux objets et six octets de données.

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

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

## Gestion des versions

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

## Informations associées

["La cohérence"](#)

## Demandes de compartiment obsolètes pour la conformité des anciennes

### Demandes de compartiment obsolètes pour la conformité des anciennes

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

### Fonction de conformité obsolète

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

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

- ["Utilisez l'API REST S3 pour configurer le verrouillage objet S3"](#)
- ["Gestion des objets avec ILM"](#)
- ["Base de connaissances NetApp : comment gérer des compartiments conformes aux anciennes générations dans StorageGRID 11.5"](#)

Demandes de conformité obsolètes :

- ["Obsolète - METTRE les modifications de la demande de godet à des fins de conformité"](#)

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

- ["Obsolète : OBTENEZ la conformité des compartiments"](#)

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

- ["Obsolète : conformité DES compartiments PUT"](#)

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

#### **Obsolète : 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 requête XML facultatif des requêtes CreateBucket pour créer un compartiment compatible.

La fonctionnalité de conformité StorageGRID disponible dans les versions précédentes d'StorageGRID est obsolète et a été remplacée par le verrouillage d'objet S3. Pour plus d'informations, consultez les documents suivants :



- ["Utilisez l'API REST S3 pour configurer le verrouillage objet S3"](#)
- ["Base de connaissances NetApp : comment gérer des compartiments conformes aux anciennes générations dans StorageGRID 11.5"](#)

Vous ne pouvez plus créer de compartiments avec la fonctionnalité 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 compartiment compatible :

The Compliance feature is deprecated.

Contact your StorageGRID administrator if you need to create new Compliant buckets.

## Obsolète : RÉCUPÉRER la demande de conformité du compartiment

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

La fonctionnalité de conformité StorageGRID disponible dans les versions précédentes d'StorageGRID est obsolète et a été remplacée par le verrouillage d'objet S3. Pour plus d'informations, consultez les documents suivants :



- ["Utilisez l'API REST S3 pour configurer le verrouillage objet S3"](#)
- ["Base de connaissances NetApp : comment gérer des compartiments conformes aux anciennes générations dans StorageGRID 11.5"](#)

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

### Exemple de demande

Cet exemple de demande vous permet de déterminer les paramètres de conformité du compartiment nommé mybucket.

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

### Exemple de réponse

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

```

HTTP/1.1 200 OK
Date: 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
RetentionPeriodMinutes	Durée de conservation des objets ajoutés à ce compartiment, en minutes. La période de conservation commence lorsque l'objet est ingéré dans la grille.
LegalHold	<ul style="list-style-type: none"> <li>Vrai : ce compartiment est actuellement en attente légale. Les objets de ce compartiment ne peuvent pas être supprimés tant que la conservation légale n'est pas levée, même si leur période de conservation a expiré.</li> <li>Faux : ce godet n'est pas actuellement en attente légale. Les objets de ce compartiment peuvent être supprimés à la fin de leur période de conservation.</li> </ul>
Suppression automatique	<ul style="list-style-type: none"> <li>Vrai : les objets de ce compartiment sont automatiquement supprimés lors de leur expiration, à moins que le compartiment ne soit soumis à une obligation légale.</li> <li>FALSE : les objets de ce compartiment ne sont pas supprimés automatiquement lorsque la période de conservation expiré. Vous devez supprimer ces objets manuellement si vous devez les supprimer.</li> </ul>

#### Réponses d'erreur

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

#### Obsolète : demande de conformité du compartiment PUT

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

La fonctionnalité de conformité StorageGRID disponible dans les versions précédentes d'StorageGRID est obsolète et a été remplacée par le verrouillage d'objet S3. Pour plus d'informations, consultez les documents suivants :

- ["Utilisez l'API REST S3 pour configurer le verrouillage objet S3"](#)
- ["Base de connaissances NetApp : comment gérer des compartiments conformes aux anciennes générations dans StorageGRID 11.5"](#)

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

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

#### Exemple de demande

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

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

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

Nom	Description
RetentionPeriodMinutes	Durée de conservation des objets ajoutés à ce compartiment, en minutes. La période de conservation commence lorsque l'objet est ingéré dans la grille.  <b>Important</b> lorsque vous spécifiez une nouvelle valeur pour RetentionPeriodMinutes, vous devez spécifier une valeur égale ou supérieure à la période de rétention actuelle du compartiment. Une fois la période de rétention du compartiment définie, vous ne pouvez pas la réduire ; vous pouvez uniquement l'augmenter.

Nom	Description
LegalHold	<ul style="list-style-type: none"> <li>Vrai : ce compartiment est actuellement en attente légale. Les objets de ce compartiment ne peuvent pas être supprimés tant que la conservation légale n'est pas levée, même si leur période de conservation a expiré.</li> <li>Faux : ce godet n'est pas actuellement en attente légale. Les objets de ce compartiment peuvent être supprimés à la fin de leur période de conservation.</li> </ul>
Suppression automatique	<ul style="list-style-type: none"> <li>Vrai : les objets de ce compartiment sont automatiquement supprimés lors de leur expiration, à moins que le compartiment ne soit soumis à une obligation légale.</li> <li>FALSE : les objets de ce compartiment ne sont pas supprimés automatiquement lorsque la période de conservation expiré. Vous devez supprimer ces objets manuellement si vous devez les supprimer.</li> </ul>

#### Cohérence pour les paramètres de conformité

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

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

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



Ne forcez jamais la cohérence **Strong-site** pour la conformité PUT bucket à moins que vous n'ayez été dirigé pour le faire par le support technique et à moins que vous ne compreniez 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 en lecture après écriture uniquement pour les demandes des clients au sein d'un site. Il est donc possible que le système StorageGRID dispose de plusieurs paramètres incohérents pour ce compartiment jusqu'à ce que tous les sites et nœuds de stockage soient disponibles. Les paramètres incohérents peuvent entraîner un comportement inattendu et indésirable. Par exemple, si vous placez un compartiment dans une conservation légale et que vous forcez une cohérence inférieure, les paramètres de conformité précédents du compartiment (c'est-à-dire la conservation légale) peuvent continuer à être en vigueur sur certains sites de data Center. Par conséquent, les objets qui, selon vous, sont en attente légale peuvent être supprimés à l'expiration de leur période de conservation, soit par l'utilisateur, soit par AutoDelete, si cette option est activée.

Pour forcer l'utilisation de la cohérence **strong-site**, relancez la demande de conformité PUT Bucket et incluez l'`Consistency-Control` en-tête de requête HTTP, comme suit :

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

#### Réponses d'erreur

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

#### Informations associées

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

## Gérer les politiques d'accès

### Utiliser les politiques d'accès

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

#### Présentation de la stratégie d'accès

StorageGRID prend en charge trois types de politiques d'accès :

- **Stratégies de compartiment**, gérées à l'aide des opérations de l'API GetBucketPolicy, PutBucketPolicy et DeleteBucketPolicy S3 ou du gestionnaire de locataires ou de l'API de gestion des locataires. Les règles de compartiment sont liées aux compartiments. Elles sont donc configurées de façon à contrôler l'accès des utilisateurs du compte du propriétaire du compartiment ou d'autres comptes au compartiment et aux objets. Une politique de compartiment s'applique à un seul compartiment et peut-être à plusieurs groupes.
- **Stratégies de groupe**, qui sont configurées à l'aide du Gestionnaire de locataires ou de l'API de gestion des locataires. Les stratégies de groupe sont associées à un groupe du compte, de sorte qu'elles sont configurées de manière à permettre à ce groupe d'accéder à des ressources spécifiques appartenant à ce compte. Une stratégie de groupe s'applique à un seul groupe et peut-être plusieurs compartiments.
- **Politiques de session**, qui sont incluses dans le cadre d'une demande AssumeRole. Les politiques de session s'appliquent uniquement à la session donnée, définissant plus en détail les autorisations dont dispose l'utilisateur, en plus de celles accordées par la politique de groupe et de compartiment.



Il n'y a aucune différence de priorité entre les stratégies de groupe, de compartiment et de session.

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

- ID de déclaration (ID) (facultatif)

- Effet
- Principal/notPrincipal
- Ressource/NotResource
- Action/NotAction
- Condition (en option)

Les instructions de règles sont créées à l'aide de cette structure pour spécifier les autorisations : accorder <effet> pour autoriser/refuser <principal> d'exécuter <action> sur <ressource> lorsque <condition> s'applique.

Chaque élément de règle est utilisé pour une fonction spécifique :

Elément	Description
SID	L'élément Sid est facultatif. Le SID n'est destiné qu'à la description de l'utilisateur. Il est stocké mais non interprété par le système StorageGRID.
Effet	Utilisez l'élément d'effet pour déterminer si les opérations spécifiées sont autorisées ou refusées. Vous devez identifier les opérations que vous autorisez (ou refusez) les compartiments ou les objets à l'aide des mots clés action Element pris en charge.
Principal/notPrincipal	<p>Vous pouvez autoriser les utilisateurs, groupes et comptes à accéder à des ressources spécifiques et à effectuer des actions spécifiques. Si aucune signature S3 n'est incluse dans la demande, l'accès anonyme est autorisé en spécifiant le caractère générique (*) comme principal. Par défaut, seul le root du compte peut accéder aux ressources qui lui sont propres.</p> <p>Il vous suffit de spécifier l'élément principal dans une stratégie de rubrique. Pour les stratégies de groupe, le groupe auquel la stratégie est associée est l'élément principal implicite.</p>
Ressource/NotResource	L'élément ressource identifie les compartiments et les objets. Vous pouvez autoriser ou refuser des autorisations pour les compartiments et les objets en utilisant le nom de ressource Amazon (ARN) pour identifier la ressource.
Action/NotAction	Les éléments action et effet sont les deux composants des autorisations. Lorsqu'un groupe demande une ressource, l'accès à la ressource est accordé ou refusé. L'accès est refusé sauf si vous attribuez des autorisations spécifiques, mais vous pouvez utiliser le refus explicite pour remplacer une autorisation accordée par une autre stratégie.
Condition	L'élément condition est facultatif. Les conditions vous permettent de créer des expressions pour déterminer quand une stratégie doit être appliquée.

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

s3:GetObject, s3:PutObject et s3:DeleteObject.

```
s3:*Object
```

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

Dans l'élément principal, les caractères génériques ne sont pas pris en charge, sauf pour définir l'accès anonyme, qui accorde l'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 instruction de stratégie de compartiment complète qui utilise l'effet « Autoriser » pour donner aux Principals, au groupe admin federated-group/admin et au groupe financier federated-group/finance , les autorisations d'effectuer l'action s3>ListBucket sur le compartiment nommé mybucket et l'action s3:GetObject sur tous les objets de ce compartiment.

```
{  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Principal": {  
        "AWS": [  
          "arn:aws:iam::27233906934684427525:federated-group/admin",  
          "arn:aws:iam::27233906934684427525:federated-group/finance"  
        ]  
      },  
      "Action": [  
        "s3>ListBucket",  
        "s3GetObject"  
      ],  
      "Resource": [  
        "arn:aws:s3:::mybucket",  
        "arn:aws:s3:::mybucket/*"  
      ]  
    }  
  ]  
}
```

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

5,120 octets.

## Cohérence au niveau des règles

Par défaut, toutes les mises à jour apportées aux stratégies de groupe sont 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 règles. Par défaut, toutes les mises à jour des règles de compartiment sont fortement cohérentes.

Si nécessaire, vous pouvez modifier les garanties de cohérence pour les mises à jour des règles de compartiment. Par exemple, vous pouvez souhaiter qu'une modification de règle de compartiment soit disponible en cas de panne sur le site.

Dans ce cas, vous pouvez définir l' `Consistency-Control` en-tête dans la demande PutBucketPolicy ou utiliser la demande de cohérence PUT Bucket. Lorsqu'une règle de compartiment devient cohérente, les modifications peuvent prendre 8 secondes supplémentaires en raison de la mise en cache des règles.

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

## Quelle est la politique de session ?

Une politique de session est une politique d'accès qui restreint temporairement les autorisations disponibles pendant une session spécifique, par exemple lorsqu'un utilisateur assume un groupe. Une politique de session ne peut autoriser qu'un sous-ensemble d'autorisations et ne peut pas accorder d'autorisations supplémentaires. Le groupe lui-même pourrait avoir des autorisations plus larges.

## Utilisez ARN dans les énoncés de politique

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

- Utilisez cette syntaxe pour spécifier la ressource S3 ARN :

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

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

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

Autres considérations :

- Vous pouvez utiliser l'astérisque (\*) comme caractère générique pour correspondre à zéro ou plus de

caractères dans la clé d'objet.

- Les caractères internationaux, qui peuvent être spécifiés dans la clé d'objet, doivent être codés à l'aide de JSON UTF-8 ou de séquences d'échappement JSON \u. Le codage pourcentage n'est pas pris en charge.

### ["Syntaxe RFC 2141 URN"](#)

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

## Spécifiez les ressources dans une stratégie

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

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

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

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

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

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

## Spécifiez les entités de gestion dans une stratégie

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

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

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

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

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

- Vous pouvez spécifier uniquement la racine du compte :

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

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

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

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

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

- Vous pouvez spécifier un principal anonyme :

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

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

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

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

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

## Spécifiez les autorisations dans une stratégie

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

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

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



Une suppression est effectuée lorsqu'une entrée est utilisée pour remplacer une valeur existante.

#### Autorisations qui s'appliquent aux compartiments

Autorisations	OPÉRATIONS DES API REST S3	Personnalisée pour StorageGRID
s3:CreateBucket	CreateBucket	Oui.  <b>Remarque</b> : utiliser uniquement dans la stratégie de groupe.
s3:DeleteBucket	DeleteBucket	
s3:DeleteBucketMetadatanotification	SUPPRIMEZ la configuration de notification des métadonnées de compartiment	Oui
s3:DeleteBucketPolicy	DeleteBucketPolicy	
s3:DeleteReplicationConfiguration	DeleteBucketReplication	Oui, des autorisations séparées pour PUT et DELETE
s3:GetBucketAcl	GetBucketAcl	
s3:GetBuckeCompliance	GARANTIR la conformité des compartiments (obsolète)	Oui
s3:persistance GetBucketConsistency	OPTIMISEZ la cohérence des compartiments	Oui
s3:GetBucketCORS	GetBucketCors	
s3:GetEncryptionConfiguration	GetBucketEncryption	
s3:GetBucketLastAccessTime	HEURE du dernier accès au compartiment	Oui
s3:GetBucketLocation	GetBucketLocation	
s3:GetBucketMetadatanotification	CONFIGURATION DES notifications de métadonnées de compartiment	Oui
s3:GetBuckenotification	GetBucketNotificationConfiguration	

AUTORISATIONS	OPÉRATIONS DES API REST S3	PERSONNALISÉE POUR STORAGEGRID
s3:GetBuckeObjectLockConfiguration	GetObjectLockConfiguration	
s3:GetBucketPolicy	GetBucketPolicy	
s3:GetBucketTagging	GetBucketTagging	
s3:GetBucketVersioning	GetBucketVersioning	
s3:GetLifecyclConfiguration	GetBucketLifecycleConfiguration	
s3:GetReplicationTM	GetBuckeReplication	
s3>ListAllMyseaux	<ul style="list-style-type: none"> <li>• Listseaux</li> <li>• DÉCOUVREZ l'utilisation du stockage</li> </ul>	Oui, pour OBTENIR l'utilisation du stockage.  <b>Remarque</b> : utiliser uniquement dans la stratégie de groupe.
s3>ListBucket	<ul style="list-style-type: none"> <li>• ListObjects</li> <li>• Godet principal</li> <li>• Objet de restauration</li> </ul>	
s3>ListBuckMultipartUploads	<ul style="list-style-type: none"> <li>• ListMultipartUploads</li> <li>• Objet de restauration</li> </ul>	
s3>ListBuckeVersions	OBTENIR les versions de compartiment	
s3:PutBuckeCompliance	MISE en conformité des compartiments (obsolète)	Oui
s3:persistance de PutBuckeConsistency	PRÉSERVER la cohérence du godet	Oui
s3:PutBuckeCORS	<ul style="list-style-type: none"> <li>• DeleteBuckeCors†</li> <li>• PutBucketCors</li> </ul>	
s3:PutEncryptionConfiguration	<ul style="list-style-type: none"> <li>• DeleteBuckeEncryption</li> <li>• PutBucketEncryption</li> </ul>	
s3:PutBuckeLastAccessTime	METTRE l'heure du dernier accès au compartiment	Oui

Autorisations	OPÉRATIONS DES API REST S3	Personnalisée pour StorageGRID
s3:PutBucketMetadataNotification	CONFIGURATION de notification des métadonnées de compartiment	Oui
s3:PutBucketNotification	PutBucketNotificationConfiguration	
s3:PutBucketObjectLockConfiguration	<ul style="list-style-type: none"> <li>• CreateBucket avec l' `x-amz-bucket-object-lock-enabled: true` en-tête de requête (nécessite également l'autorisation s3:CreateBucket)</li> <li>• PutObjectLockConfiguration</li> </ul>	
s3:PutBucketPolicy	PutBucketPolicy	
s3:PutBucketTagging	<ul style="list-style-type: none"> <li>• DeleteBucketTagging†</li> <li>• Étiquetage PutBucketTagging</li> </ul>	
s3:PutBucketVersioning	PutBucketVersioning	
s3:PutLifecycleConfiguration	<ul style="list-style-type: none"> <li>• DeleteBucketLifecycle†</li> <li>• PutBucketLifecycleConfiguration</li> </ul>	
s3:PutReplicationTM	PutBucketReplication	Oui, des autorisations séparées pour PUT et DELETE

#### Autorisations qui s'appliquent aux objets

Autorisations	OPÉRATIONS DES API REST S3	Personnalisée pour StorageGRID
s3:AbortMultipartUpload	<ul style="list-style-type: none"> <li>• AbortMultipartUpload</li> <li>• Objet de restauration</li> </ul>	
s3:BypassGovernanceRetention	<ul style="list-style-type: none"> <li>• DeleteObject</li> <li>• DeleteObjects</li> <li>• PutObjectRetention</li> </ul>	
s3:DeleteObject	<ul style="list-style-type: none"> <li>• DeleteObject</li> <li>• DeleteObjects</li> <li>• Objet de restauration</li> </ul>	

AUTORISATIONS	OPÉRATIONS DES API REST S3	PERSONNALISÉE POUR STORAGEGRID
s3:DeleteObjectTagging	DeleteObjectTagging	
s3:DeleteObjectVersionTagging	DeleteObjectTagging (une version spécifique de l'objet)	
s3:DeleteObjectVersion	DeleteObject (une version spécifique de l'objet)	
s3:GetObject	<ul style="list-style-type: none"> <li>GetObject</li> <li>Objet principal</li> <li>Objet de restauration</li> <li>SelectObjectContent</li> </ul>	
s3:GetObjectAcl	GetObjectAcl	
s3:GetObjectLegalHold	GetObjectLegalHold	
s3:GetObjectRetention	GetObjectRetention	
s3:GetObjectTagging	GetObjectTagging	
s3:GetObjectVersionTagging	GetObjectTagging (une version spécifique de l'objet)	
s3:GetObjectVersion	GetObject (une version spécifique de l'objet)	
s3>ListMultipartUploadParts	ListParts, RestoreObject	
s3:PutObject	<ul style="list-style-type: none"> <li>PutObject</li> <li>Objet de copie</li> <li>Objet de restauration</li> <li>CreateMultipartUpload</li> <li>CompleteMultipartUpload</li> <li>UploadPart</li> <li>UploadPartCopy</li> </ul>	
s3:PutObjectLegalHold	PutObjectLegalHold	
s3:PutObjectRetention	PutObjectRetention	

Autorisations	OPÉRATIONS DES API REST S3	Personnalisée pour StorageGRID
s3:PutObjectTagging	Marquage PutObject	
s3:PutObjectVersionTagging	PutObjectTagging (une version spécifique de l'objet)	
s3:PutOverwriteObject	<ul style="list-style-type: none"> <li>• PutObject</li> <li>• Objet de copie</li> <li>• Marquage PutObject</li> <li>• DeleteObjectTagging</li> <li>• CompleteMultipartUpload</li> </ul>	Oui
s3:RestoreObject	Objet de restauration	

## Utiliser l'autorisation PutOverwriteObject

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

Les paramètres possibles pour cette autorisation sont les suivants :

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

 Si la stratégie S3 actuelle autorise l'érassement 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.

## Spécifiez les conditions dans une stratégie

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

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

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

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

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

#### Opérateurs de condition pris en charge

Les opérateurs de condition sont classés comme suit :

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

Opérateurs de condition	Description
Equals à jambes de chaîne	Compare une clé à une valeur de chaîne en fonction de la correspondance exacte (sensible à la casse).
Equals stringNotEquals	Compare une clé à une valeur de chaîne basée sur la correspondance niée (sensible à la casse).
StringEqualIgnoreCase	Compare une clé à une valeur de chaîne basée sur la correspondance exacte (ignore case).
StringNotEqualIgnoreCase	Compare une clé à une valeur de chaîne basée sur la correspondance nérée (ignore le cas).
StringLike	Compare une clé à une valeur de chaîne en fonction de la correspondance exacte (sensible à la casse). Peut inclure des caractères génériques * et ?.

Opérateurs de condition	Description
StringNotLike	Compare une clé à une valeur de chaîne basée sur la correspondance niée (sensible à la casse). Peut inclure des caractères génériques * et ?.
Valeurs numériques	Compare une touche à une valeur numérique en fonction de la correspondance exacte.
NumericNotEquals	Compare une touche à une valeur numérique basée sur la correspondance annulée.
NumericGreaterThan	Compare une touche à une valeur numérique basée sur une correspondance « supérieure à ».
NumericGreaterThanOrEqual	Compare une clé à une valeur numérique basée sur une correspondance « supérieure ou égale ».
NumericLessThan	Compare une clé à une valeur numérique basée sur une correspondance « inférieure à ».
NumericLessThanOrEqual	Compare une clé à une valeur numérique basée sur une correspondance « inférieure ou égale ».
BOOL	Compare une clé à une valeur booléenne basée sur une correspondance « vrai ou faux ».
Adresse IP	Compare une clé à une adresse IP ou une plage d'adresses IP.
Adresse de la note	Compare une clé à une adresse IP ou une plage d'adresses IP basée sur la correspondance annulée.
Nul	Vérifie si une clé condition est présente dans le contexte de demande actuel.
SiExiste	Ajouté à n'importe quel opérateur de condition, à l'exception de la condition Null, pour vérifier l'absence de cette clé de condition. Renvoie VRAI si la clé de condition n'est pas présente.

#### Touches de condition prises en charge

Touches condition	Actions	Description
aws:SourceIp	Opérateurs IP	<p>Compare à l'adresse IP à partir de laquelle la demande a été envoyée. Peuvent être utilisées pour les opérations de compartiment ou d'objet.</p> <p><b>Remarque :</b> si la requête S3 a été envoyée via le service Load Balancer sur les nœuds Admin et les passerelles, cela se compare à l'adresse IP en amont du service Load Balancer.</p> <p><b>Remarque :</b> si un équilibrer de charge tiers non transparent est utilisé, il sera comparé à l'adresse IP de cet équilibrer de charge. N'importe quel x-Forwarded-For en-tête sera ignoré car sa validité ne peut pas être établie.</p>
aws:nom d'utilisateur	Ressource/identité	Compare le nom d'utilisateur de l'expéditeur à partir duquel la demande a été envoyée. Peuvent être utilisées pour les opérations de compartiment ou d'objet.
s3:délimiteur	s3>ListBucket et s3:permissions ListBucketVersions	Compare avec le paramètre délimiteur spécifié dans une demande ListObjects ou ListObjectVersions.
s3:ExistingObjectTag/<tag-key>	s3>DeleteObjectTagging s3>DeleteObjectVersionTagging s3:GetObject s3:GetObjectAcl s3:GetObjectTagging s3:GetObjectVersion s3:GetObjectVersionAcl s3:GetObjectVersionTagging s3:PutObjectAcl s3:PutObjectTagging s3:PutObjectVersionAcl s3:PutObjectVersionTagging	Exige que l'objet existant ait la clé et la valeur de balise spécifiques.

Touches condition	Actions	Description
s3:touches max	s3>ListBucket et s3:permissions ListBuckeVersions	Compare avec le paramètre max-keys spécifié dans une requête ListObjects ou ListObjectVersions.
s3 : mode de verrouillage d'objet	s3:PutObject	Comparable à la object-lock-mode développé à partir de l'en-tête de requête dans les requêtes PutObject, CopyObject et CreateMultipartUpload.
s3 : mode de verrouillage d'objet	s3:PutObjectRetention	Comparable à la object-lock-mode développé à partir du corps XML dans la demande PutObjectRetention.
s3 :conservation des jours restants avec un verrouillage objet	s3:PutObject	Compare à la date de conservation jusqu'à spécifiée dans l'en-tête de la demande ou calculée à x-amz-object-lock-retain-until-date partir de la période de conservation par défaut du compartiment pour s'assurer que ces valeurs sont dans la plage autorisée pour les demandes suivantes : <ul data-bbox="845 889 1155 1030" style="list-style-type: none"><li>• PutObject</li><li>• Objet de copie</li><li>• CreateMultipartUpload</li></ul>
s3 :conservation des jours restants avec un verrouillage objet	s3:PutObjectRetention	Compare à la date de conservation jusqu'à spécifiée dans la demande PutObjectRetention pour s'assurer qu'elle se trouve dans la plage autorisée.
s3:préfixe	s3>ListBucket et s3:permissions ListBuckeVersions	Compare avec le paramètre de préfixe spécifié dans une requête ListObjects ou ListObjectVersions.
s3:RequestObjectTag/<tag-key>	s3:PutObject s3:PutObjectTagging s3:PutObjectVersionTagging	Nécessitera une clé de balise et une valeur spécifiques lorsque la demande d'objet inclut le balisage.
s3:x-amz-algorithme-client-de-chiffrement-côté-serveur-	s3:PutObject	Comparable à la sse-customer-algorithm ou à la copy-source-sse-customer-algorithm développé à partir de l'en-tête de requête dans les requêtes PutObject, CopyObject, CreateMultipartUpload, UploadPart, UploadPartCopy et CompleteMultipartUpload.

## Spécifiez les variables d'une règle

Vous pouvez utiliser des variables dans les règles pour remplir les informations relatives aux règles lorsqu'elles sont disponibles. Vous pouvez utiliser des variables de règles dans l' `Resource` élément et dans des comparaisons de chaînes dans l' `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 condition :

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

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

## Créez des règles nécessitant une gestion spéciale

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

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

Description de la politique	Type de règle	Comportement Amazon	Comportement de StorageGRID
Principal est un groupe local	Godet	Principal non valide	Valide
La stratégie accorde à un compte non propriétaire (y compris les comptes anonymes) des autorisations de placer des objets.	Godet	Valide. Les objets sont détenus par le compte de créateur et la stratégie de compartiment ne s'applique pas. Le compte créateur doit accorder des autorisations d'accès à l'objet à l'aide des listes de contrôle d'accès d'objet.	Valide. Les objets sont la propriété du compte du propriétaire du compartiment. La politique de compartiment s'applique.

## Protection WORM (Write-once, Read-many)

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

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

- 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 suivantes et les règles S3 :
  - Ajoutez une opération DE REFUS PutOverwriteObject à la règle S3.
  - Ajoutez une opération DE REFUS DeleteObject à la règle S3.
  - Ajoutez une opération PutObject ALLOW à la règle S3.



La définition de DeleteObject sur REFUSER dans une règle 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 contre)

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

### Situation B: Remplacements séquentiels terminés (protégés contre)

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

## Informations associées

- ["Gestion des objets par les règles StorageGRID ILM"](#)
- ["Exemples de politiques de compartiments"](#)
- ["Exemples de stratégies de groupe"](#)
- ["Exemple de politique de session"](#)
- ["Gestion des objets avec ILM"](#)
- ["Utilisez un compte de locataire"](#)

## Exemple de politique de session

Utilisez l'exemple suivant pour créer une stratégie de session StorageGRID .

### Exemple : configurer une politique de session qui autorise la récupération d'objets

Dans cet exemple, le principal de la session est uniquement autorisé à récupérer des objets à partir du bucket1. Toutes les autres actions sont implicitement refusées, à l'exception des actions spécifiques à StorageGRID, telles que l'utilisation de ["s3:PutOverwriteObject"](#) autorisation. La politique de session peut être fournie sous forme de fichier JSON lors de l'appel de l'API AssumeRole.

```
{  
  "Statement": [  
    {  
      "Action": "s3:GetObject",  
      "Effect": "Allow",  
      "Resource": "arn:aws:s3:::bucket1/*"  
    }  
  ]  
}
```

## Exemples de politiques de compartiments

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

Les politiques de compartiment spécifient les autorisations d'accès pour le compartiment à lequel la politique est attachée. Pour configurer une stratégie de compartiment, utilisez l'API PutBucketPolicy S3 au moyen de l'un des outils suivants :

- ["Gestionnaire de locataires"](#).
- CLI AWS utilisant cette commande (voir ["Opérations sur les compartiments"](#)) :

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

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

Dans cet exemple, tout le monde, y compris anonyme, est autorisé à répertorier les objets dans le compartiment et à effectuer des opérations GetObject sur tous les objets du compartiment. 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, ne peut écrire dans le compartiment.

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

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

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



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

```

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

```

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

Dans cet exemple, tout le monde, y compris anonyme, est autorisé à répertorier le compartiment et à effectuer des opérations GetObject sur tous les objets du compartiment, alors que seuls les utilisateurs appartenant au groupe Marketing du compte spécifié ont un accès complet.

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

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

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

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

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

Dans cet exemple, l'utilisateur fédéré Alex est autorisé à accéder entièrement au examplebucket compartiment et à ses objets. Tous les autres utilisateurs, y compris « root », sont explicitement refusés à toutes les opérations. Notez toutefois que « root » n'est jamais refusé les autorisations de mettre/obtenir/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, l' `Deny` effet de PutOverwriteObject et DeleteObject garantit que personne ne peut écraser ou supprimer les données de l'objet, les métadonnées définies par l'utilisateur et le balisage d'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 stratégies d'accès StorageGRID pour les groupes.

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

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

Lorsque vous 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 les membres de ce groupe auront accès. Voir ["Créez 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 règle de compartiment. Si vous sélectionnez cette option, seul l'utilisateur root peut accéder aux ressources S3 par défaut.
- **Accès en lecture seule** : les utilisateurs de ce groupe ont accès en lecture seule aux ressources S3. Par exemple, les utilisateurs de ce groupe peuvent afficher la liste des objets et lire les données d'objet, les métadonnées et les balises. Lorsque vous sélectionnez cette option, la chaîne JSON pour une stratégie de groupe en lecture seule s'affiche dans la zone de texte. Vous ne pouvez pas modifier cette chaîne.
- **Accès complet** : les utilisateurs de ce groupe ont accès aux ressources S3, y compris aux compartiments. Lorsque vous sélectionnez cette option, la chaîne JSON pour une stratégie de groupe à accès complet s'affiche dans la zone de texte. Vous ne pouvez pas modifier cette chaîne.
- **Atténuation des ransomware** : cet exemple de politique s'applique à tous les compartiments pour ce locataire. Les utilisateurs de ce groupe peuvent effectuer des actions courantes, mais ne peuvent pas supprimer définitivement des objets des compartiments pour lesquels la gestion des versions d'objet est activée.

Les utilisateurs du Gestionnaire de locataires disposant 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), le cas échéant.

- **Custom** : les utilisateurs du groupe disposent des autorisations que vous spécifiez dans la zone de texte.

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

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

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

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

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

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

#### **Exemple : autorisez les membres du groupe à accéder entièrement à leur « dossier » uniquement dans un compartiment**

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

```

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

```

## 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 informations détaillées sur les opérations relatives aux compartiments et aux objets.

### Les opérations des compartiments sont suivies dans les journaux d'audit

- CreateBucket
- DeleteBucket
- DeleteBucketTagging
- DeleteObjects
- GetBucketTagging
- Godet principal
- ListObjects
- ListObjectVersions
- METTEZ le godet en conformité
- Étiquetage PutBucketTagging
- PutBuckeVersioning

## Opérations d'objet suivies dans les journaux d'audit

- CompleteMultipartUpload
- Objet de copie
- DeleteObject
- GetObject
- Objet principal
- PutObject
- Objet de restauration
- SelectObject
- UploadPart (lorsqu'une règle ILM utilise un ingestion équilibrée ou stricte)
- UploadPartCopy (lorsqu'une règle ILM utilise un ingestion équilibrée ou stricte)

### Informations associées

- ["Accéder au fichier journal d'audit"](#)
- ["Écrire des messages d'audit client"](#)
- ["Messages d'audit de lecture du client"](#)

## Informations sur le copyright

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

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

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

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

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

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

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

## Informations sur les marques commerciales

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