



Opérations personnalisées StorageGRID

StorageGRID software

NetApp
July 23, 2026

This PDF was generated from <https://docs.netapp.com/fr-fr/storagegrid-120/s3/custom-operations-on-buckets.html> on July 23, 2026. Always check docs.netapp.com for the latest.

Sommaire

Opérations personnalisées StorageGRID	1
Opérations personnalisées de compartiment prises en charge dans StorageGRID	1
Récupérez le niveau de cohérence du compartiment dans StorageGRID avec la requête GET Bucket consistency	2
Exemple de requête	2
Réponse	2
Exemple de réponse	3
Spécifiez les niveaux de cohérence dans StorageGRID avec la requête PUT Bucket consistency	3
Demande	3
Exemple de requête	4
Récupérez l'état de la dernière date d'accès au bucket dans StorageGRID avec la requête GET Bucket last access time	4
Exemple de requête	4
Exemple de réponse	4
Activer et désactiver les mises à jour du temps d'accès dans StorageGRID avec la requête PUT Bucket last access time	5
Exemples de requêtes	6
Désactivez le service d'intégration de recherche avec la requête DELETE Bucket metadata notification configuration dans StorageGRID	6
Exemple de requête	6
Configurez l'intégration de la recherche dans StorageGRID avec la requête de configuration de notification des métadonnées du compartiment GET	6
Exemple de requête	7
Réponse	7
Exemple de réponse	9
Activez le service d'intégration de recherche dans StorageGRID avec la requête de configuration de notification des métadonnées du compartiment PUT	10
Demande	10
Exemples de requêtes	13
JSON généré par le service d'intégration de recherche	14
Métadonnées d'objet incluses dans les notifications de métadonnées	15
Récupérez l'utilisation du stockage du compte et du bucket dans StorageGRID avec la requête GET Storage Usage	16
Exemple de requête	16
Exemple de réponse	17
Versionnage	17
\${post_edited_translations.segment}	17
Requêtes de compartiment obsolètes pour la conformité StorageGRID héritée	17
Élément SGCompliance obsolète dans StorageGRID	18
Requête GET Bucket compliance obsolète dans StorageGRID	19
Requête PUT Bucket compliance obsolète dans StorageGRID	20

Opérations personnalisées StorageGRID

Opérations personnalisées de compartiment prises en charge dans StorageGRID

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

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

Opération	Description
"Cohérence du bucket GET"	Renvoie la cohérence appliquée à un compartiment particulier.
"Cohérence PUT Bucket"	Définit la cohérence appliquée à un compartiment particulier.
"Obtenir le temps d'accès du compartiment"	Indique si les mises à jour du temps d'accès sont activées ou désactivées pour un compartiment donné.
"PUT temps d'accès du dernier accès au compartiment"	Permet d'activer ou de désactiver les mises à jour du temps d'accès pour un compartiment particulier.
"SUPPRIMER la configuration de notification des métadonnées du compartiment"	Supprime le fichier XML de configuration des notifications de métadonnées associé à un compartiment particulier.
"Obtenir la configuration de notification des métadonnées du bucket"	Renvoie le fichier XML de configuration des notifications de métadonnées associé à un compartiment particulier.
"Configuration de notification des métadonnées du compartiment PUT"	Configure le service de notification des métadonnées pour un compartiment.
"Obtenir l'utilisation du stockage"	Indique la capacité totale de stockage utilisée par un compte et pour chaque compartiment associé au compte.
"Déprécié : CreateBucket avec paramètres de conformité"	Obsolète et non pris en charge : vous ne pouvez plus créer de nouveaux compartiments avec la conformité activée.
"Obsolète : GET Bucket compliance"	Déprécié mais toujours pris en charge : renvoie les paramètres de conformité actuellement en vigueur pour un compartiment Compliant hérité existant.
"Obsolète : PUT Bucket compliance"	Obsolète mais pris en charge : permet de modifier les paramètres de conformité d'un compartiment Compliant hérité existant.

Récupérez le niveau de cohérence du compartiment dans StorageGRID avec la requête GET Bucket consistency

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

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

Vous devez disposer de l'autorisation `s3:GetBucketConsistency`, ou être administrateur du compte, pour effectuer cette opération.

Exemple de requête

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

Réponse

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

Cohérence	Description
tous	Tous les nœuds reçoivent les données immédiatement, ou la requête échouera.
fort-mondial	Garantit la cohérence en lecture après écriture pour toutes les requêtes client sur tous les sites.
site fort	Garantit la cohérence des données en lecture après écriture pour toutes les requêtes client au sein d'un site.
lecture après une nouvelle écriture	(Par défaut) Assure la cohérence en lecture après écriture pour les nouveaux objets et la cohérence éventuelle pour les mises à jour d'objets. Offre une haute disponibilité et des garanties de protection des données. Recommandé dans la plupart des cas.
disponible	Garantit la cohérence éventuelle des nouveaux objets et des mises à jour d'objets. Pour les compartiments S3, utilisez cette fonctionnalité uniquement lorsque cela est nécessaire (par exemple, pour un compartiment contenant 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 S3 FabricPool.

Exemple de réponse

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

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

Informations connexes

["Cohérence"](#)

Spécifiez les niveaux de cohérence dans StorageGRID avec la requête PUT Bucket consistency

`${post_edited_translations.segment}`

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

Avant de commencer

Vous devez disposer de l'autorisation `s3:PutBucketConsistency`, ou être le compte racine, pour effectuer cette opération.

Demande

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

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

Cohérence	Description
disponible	Garantit la cohérence éventuelle des nouveaux objets et des mises à jour d'objets. Pour les compartiments S3, utilisez cette fonctionnalité uniquement lorsque cela est nécessaire (par exemple, pour un compartiment contenant 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 S3 FabricPool.

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

Exemple de requête

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

Informations connexes

["Cohérence"](#)

Récupérez l'état de la dernière date d'accès au bucket dans StorageGRID avec la requête GET Bucket last access time

La requête GET Bucket last access time vous permet de déterminer si les mises à jour du temps d'accès sont activées ou désactivées pour chaque compartiment.

Vous devez disposer de l'autorisation `s3:GetBucketLastAccessTime`, ou être administrateur du compte, pour effectuer cette opération.

Exemple de requête

```
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 dernier temps d'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>
```

Activer et désactiver les mises à jour du temps d'accès dans StorageGRID avec la requête PUT Bucket last access time

La requête PUT Bucket last access time vous permet d'activer ou de désactiver les mises à jour du temps d'accès pour les compartiments individuels. La désactivation des mises à jour du temps d'accès améliore les performances et constitue le paramètre par défaut pour tous les compartiments créés avec la version 10.3.0 ou ultérieure.

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



À partir de la version 10.3 de StorageGRID, les mises à jour du temps d'accès sont désactivées par défaut pour tous les nouveaux compartiments. Si vous avez des compartiments créés avec une version antérieure de StorageGRID et que vous souhaitez adopter le nouveau comportement par défaut, vous devez explicitement désactiver les mises à jour du temps d'accès pour chacun de ces compartiments. Vous pouvez activer ou désactiver les mises à jour du temps d'accès à l'aide de la requête PUT Bucket last access time ou depuis la page de détails d'un compartiment dans le Tenant Manager. Voir ["Activer ou désactiver la mise à jour du temps d'accès"](#).

`${post_edited_translations.segment}`

- `GetObject`, `GetObjectAcl`, `GetObjectTagging`, et `HeadObject` ne mettent pas à jour le temps d'accès. L'objet n'est pas ajouté aux files d'attente pour l'évaluation de la gestion du cycle de vie de l'information (ILM).
- Les requêtes `CopyObject` et `PutObjectTagging` qui mettent à jour uniquement les métadonnées mettent également à jour le temps d'accès. L'objet est ajouté aux files d'attente pour l'évaluation ILM.
- Si les mises à jour du temps d'accès sont désactivées pour le compartiment source, les requêtes `CopyObject` ne mettent pas à jour le temps d'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 le temps d'accès. La copie de l'objet est ajoutée aux files d'attente pour l'évaluation ILM.
- `CompleteMultipartUpload` les requêtes mettent à jour le temps d'accès. L'objet finalisé est ajouté aux files d'attente pour l'évaluation ILM.

Exemples de requêtes

Cet exemple active le dernier temps d'accès pour un compartiment.

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

Cet exemple désactive le temps d'accès pour un compartiment.

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

Désactivez le service d'intégration de recherche avec la requête DELETE Bucket metadata notification configuration dans StorageGRID

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

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

Exemple de requête

Cet exemple montre comment désactiver le 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
```

Configurez l'intégration de la recherche dans StorageGRID avec la requête de configuration de notification des métadonnées du compartiment GET

La requête de configuration de notification des métadonnées GET Bucket vous permet de récupérer le fichier XML de configuration utilisé pour configurer l'intégration de la

recherche pour des compartiments individuels.

Vous devez disposer de l'autorisation `s3:GetBucketMetadataNotification`, ou être administrateur du compte, pour effectuer cette opération.

Exemple de requête

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

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

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

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

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

Nom	Description	Obligatoire
Urn	URN de la destination où les métadonnées de l'objet sont envoyées. Doit être l'URN d'un point de terminaison StorageGRID possédant les propriétés suivantes : • es doit être le troisième élément. • L'URN doit se terminer par l'index et le type où les métadonnées sont stockées, sous la forme <code>domain-name/myindex/mytype</code>. Les points de terminaison sont configurés à l'aide du Gestionnaire de locataires ou de l'API de gestion des locataires. Ils se présentent sous la forme suivante : • <code>arn:aws:es:_region:account-ID_:domain/mydomain/myindex/mytype</code> • <code>urn:mysite:es:::mydomain/myindex/mytype</code> Le point de terminaison doit être configuré avant la soumission du fichier XML de configuration, sinon la configuration échouera avec une erreur 404. Urn est inclus dans l'élément Destination.	Oui

Exemple de réponse

Le code XML inclus entre les

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

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

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

Informations connexes

["Utilisez un compte locataire"](#)

Activez le service d'intégration de recherche dans StorageGRID avec la requête de configuration de notification des métadonnées du compartiment PUT

La requête PUT de configuration de notification des métadonnées de compartiment permet d'activer le service d'intégration de recherche pour des compartiments individuels. Le fichier XML de configuration de notification des métadonnées fourni dans le corps de la requête spécifie les objets dont les métadonnées sont envoyées à l'index de recherche de destination.

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

Demande

La requête doit inclure la configuration de notification des métadonnées dans son corps. Chaque configuration de notification des métadonnées comprend une ou plusieurs règles. Chaque règle spécifie les objets auxquels elle s'applique et la destination où StorageGRID doit envoyer les métadonnées des objets.

Il est possible de filtrer les objets en fonction du préfixe de leur nom. Par exemple, vous pouvez envoyer les métadonnées des objets avec le préfixe `/images` vers une destination, et les objets avec le préfixe `/videos` vers une autre.

Les configurations comportant des préfixes qui se chevauchent ne sont pas valides et sont rejetées lors de leur soumission. Par exemple, une configuration incluant une règle pour les objets ayant le préfixe `test` et une autre règle pour les objets ayant le préfixe `test2` ne serait pas autorisée.

Les destinations doivent être spécifiées à l'aide de l'URN d'un point de terminaison StorageGRID. Le point de terminaison doit exister lors de la soumission de la configuration de notification des métadonnées, sinon la requête 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 fichier XML de configuration des notifications de métadonnées.

Nom	Description	Obligatoire
MetadataNotificationConfi guration	Balise 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 conteneur pour une règle qui identifie les objets dont les métadonnées doivent être ajoutées à un index spécifié. Les règles comportant des préfixes qui se chevauchent sont rejetées. Inclus dans l'élément MetadataNotificationConfiguration.	Oui

Nom	Description	Obligatoire
ID	Identifiant unique de la règle. Inclus dans l'élément Rule.	Non
Statut	Le statut peut être « Activé » ou « Désactivé ». Aucune action n'est entreprise pour les règles désactivées. Inclus dans l'élément Rule.	Oui
Préfixe	Les objets correspondant au préfixe sont concernés par la règle et leurs métadonnées sont envoyées à la destination spécifiée. Pour faire correspondre tous les objets, spécifiez un préfixe vide. Inclus dans l'élément Rule.	Oui
Destination	Étiquette conteneur pour la destination d'une règle. Inclus dans l'élément Rule.	Oui
Urn	URN de la destination où les métadonnées de l'objet sont envoyées. Doit être l'URN d'un point de terminaison StorageGRID possédant les propriétés suivantes : • es doit être le troisième élément. • L'URN doit se terminer par l'index et le type où les métadonnées sont stockées, sous la forme <code>domain-name/myindex/mytype</code>. Les points de terminaison sont configurés à l'aide du Gestionnaire de locataires ou de l'API de gestion des locataires. Ils se présentent sous la forme suivante : • <code>arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype</code> • <code>urn:mysite:es:::mydomain/myindex/mytype</code> Le point de terminaison doit être configuré avant la soumission du fichier XML de configuration, sinon la configuration échouera avec une erreur 404. Urn est inclus dans l'élément Destination.	Oui

Exemples de requêtes

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

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

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

Dans cet exemple, les métadonnées d'objet pour les objets qui correspondent au préfixe `/images` sont envoyées à une destination, tandis que les métadonnées d'objet pour les objets qui correspondent 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-1:33333333:domain/es-
domain/graphics/imagetype</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Videos-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/videos</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

JSON généré par le service d'intégration de recherche

`${post_edited_translations.segment}`

Cet exemple montre un exemple du JSON qui pourrait être généré lorsqu'un objet avec la clé `SGWS/Tagging.txt` est créé dans un compartiment nommé `test`. Le compartiment `test` n'est pas versionné, la balise `versionId` est donc 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 point de terminaison de destination lorsque l'intégration de la recherche est activée.

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

Type	Nom de l'article	Description
Informations sur le bucket et l'objet	bucket	Nom du compartiment
Informations sur le bucket et l'objet	<code>\${post_edited_translations.segment}</code>	Nom de la clé de l'objet
Informations sur le bucket et l'objet	versionID	Version de l'objet, pour les objets dans des compartiments versionnés
Informations sur le bucket et l'objet	région	Région de compartiment, par exemple <code>us-east-1</code>
Métadonnées système	taille	<code>\${post_edited_translations.segment}</code>
Métadonnées système	md5	<code>\${post_edited_translations.segment}</code>

Type	Nom de l'article	Description
Métadonnées utilisateur	métadonnées <i>key:value</i>	Toutes les métadonnées utilisateur de l'objet, sous forme de paires clé-valeur
Étiquettes	balises <i>key:value</i>	Toutes les étiquettes d'objet définies pour l'objet, sous forme de paires clé-valeur



Pour les balises et les métadonnées utilisateur, StorageGRID transmet les dates et les nombres à Elasticsearch sous forme de chaînes de caractères ou de notifications d'événements S3. Pour configurer Elasticsearch afin qu'il interprète ces chaînes comme des dates ou des nombres, suivez les instructions Elasticsearch pour le mappage dynamique des champs et le mappage des formats de date. Vous devez activer le mappage dynamique des champs sur l'index avant de configurer le service d'intégration de recherche. Après l'indexation d'un document, vous ne pouvez plus modifier les types de champs du document dans l'index.

Informations connexes

["Utilisez un compte locataire"](#)

Récupérez l'utilisation du stockage du compte et du bucket dans StorageGRID avec la requête GET Storage Usage

La requête GET Storage Usage vous indique la quantité totale de stockage utilisée par un compte, ainsi que pour chaque compartiment associé à ce compte.

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

Par défaut, StorageGRID tente de récupérer les informations d'utilisation en utilisant une cohérence globale forte. Si une cohérence globale forte ne peut pas être atteinte, StorageGRID tente de récupérer les informations d'utilisation avec une cohérence site forte.

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

Exemple de requête

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

Exemple de réponse

Cet exemple illustre un compte contenant quatre objets et 12 octets de données répartis 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>
```

Versionnage

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

Informations connexes

["Cohérence"](#)

`${post_edited_translations.segment}`

Requêtes de compartiment obsolètes pour la conformité StorageGRID héritée

Vous pourriez avoir besoin d'utiliser l'API REST S3 de StorageGRID pour gérer les compartiments créés à l'aide de l'ancienne fonctionnalité de conformité.

Fonctionnalité de conformité obsolète

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

Si vous aviez précédemment activé le paramètre de conformité global, le paramètre de verrouillage global des objets S3 est activé dans StorageGRID 11.6. Vous ne pouvez plus créer de nouveaux compartiments avec la conformité activée ; cependant, si nécessaire, vous pouvez utiliser l'API REST S3 de StorageGRID pour gérer tout compartiment conforme existant.

- ["Utilisez l'API REST S3 pour configurer S3 Object Lock"](#)
- ["Gérez les objets avec ILM"](#)
- ["Base de connaissances NetApp : Comment gérer les compartiments conformes hérités dans StorageGRID 11.5"](#)

Demandes de conformité obsolètes :

- ["Déprécié - Modifications des requêtes PUT Bucket pour la conformité"](#)

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

- ["Obsolète - GET Bucket compliance"](#)

La requête GET Bucket compliance est obsolète. Cependant, vous pouvez continuer à utiliser cette requête pour déterminer les paramètres de conformité actuellement en vigueur pour un bucket Compliant existant.

- ["Obsolète - PUT Bucket compliance"](#)

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

Élément SGCompliance obsolète dans StorageGRID

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



La fonctionnalité de conformité StorageGRID, disponible dans les versions précédentes de StorageGRID, est obsolète et a été remplacée par S3 Object Lock. Pour plus de détails, consultez ce qui suit :

- ["Utilisez l'API REST S3 pour configurer S3 Object Lock"](#)
- ["Base de connaissances NetApp : Comment gérer les compartiments conformes hérités dans StorageGRID 11.5"](#)

Vous ne pouvez plus créer de nouveaux compartiments avec la conformité activée. Le message d'erreur suivant est renvoyé si vous tentez d'utiliser les modifications de la requête CreateBucket pour la conformité

afin de créer un nouveau compartiment conforme :

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

Requête GET Bucket compliance obsolète dans StorageGRID

La requête GET Bucket compliance est obsolète. Cependant, vous pouvez continuer à utiliser cette requête pour déterminer les paramètres de conformité actuellement en vigueur pour un bucket Compliant existant.



La fonctionnalité de conformité StorageGRID, disponible dans les versions précédentes de StorageGRID, est obsolète et a été remplacée par S3 Object Lock. Pour plus de détails, consultez ce qui suit :

- ["Utilisez l'API REST S3 pour configurer S3 Object Lock"](#)
- ["Base de connaissances NetApp : Comment gérer les compartiments conformes hérités dans StorageGRID 11.5"](#)

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

Exemple de requête

Cette requête d'exemple 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 la réponse XML, `<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 son ingestion dans la grille. Il n'y a actuellement aucune restriction légale sur ce compartiment. 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	La durée de la période de conservation des objets ajoutés à ce compartiment, en minutes. La période de conservation commence lorsque l'objet est ingérée dans la grille.
LegalHold	• Vrai : Ce compartiment fait actuellement l'objet d'une rétention légale. Les objets dans ce compartiment ne peuvent pas être supprimés tant que la rétention légale n'est pas levée, même si leur période de conservation est expirée. • Faux : ce compartiment n'est actuellement soumis à aucune restriction légale. Les objets de ce compartiment peuvent être supprimés à l'expiration de leur période de conservation.
AutoDelete	• Vrai : les objets dans ce compartiment seront automatiquement supprimés à l'expiration de leur période de conservation, sauf si le compartiment fait l'objet d'une rétention légale. • Faux : les objets de ce compartiment ne seront pas supprimés automatiquement à l'expiration de la période de rétention. Vous devez supprimer ces objets manuellement si vous devez les supprimer.

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.

Requête PUT Bucket compliance obsolète dans StorageGRID

La requête PUT Bucket compliance est obsolète. Cependant, vous pouvez continuer à utiliser cette requête pour modifier les paramètres de conformité d'un compartiment Compliant existant. Par exemple, vous pouvez placer un compartiment existant en

rétenction légale ou augmenter sa période de conservation.



La fonctionnalité de conformité StorageGRID, disponible dans les versions précédentes de StorageGRID, est obsolète et a été remplacée par S3 Object Lock. Pour plus de détails, consultez ce qui suit :

- ["Utilisez l'API REST S3 pour configurer S3 Object Lock"](#)
- ["Base de connaissances NetApp : Comment gérer les compartiments conformes hérités dans StorageGRID 11.5"](#)

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

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

Exemple de requête

Cette requête d'exemple modifie les paramètres de conformité du compartiment nommé `mybucket`. Dans cet exemple, les objets dans `mybucket` seront désormais conservés pendant deux ans (1 051 200 minutes) au lieu d'un an, à compter de leur ingestion dans la grille. Ce compartiment n'est soumis à aucune restriction légale. 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	La durée de la période de conservation des objets ajoutés à ce compartiment, en minutes. La période de conservation commence lorsque l'objet est ingérée dans la grille. Important Lorsque vous définissez une nouvelle valeur pour <code>RetentionPeriodMinutes</code>, vous devez indiquer une valeur supérieure ou égale à la période de rétention actuelle du compartiment. Une fois la période de rétention du compartiment définie, vous ne pouvez plus diminuer cette valeur ; vous pouvez seulement l'augmenter.

Nom	Description
LegalHold	• Vrai : Ce compartiment fait actuellement l'objet d'une rétention légale. Les objets dans ce compartiment ne peuvent pas être supprimés tant que la rétention légale n'est pas levée, même si leur période de conservation est expirée. • Faux : ce compartiment n'est actuellement soumis à aucune restriction légale. Les objets de ce compartiment peuvent être supprimés à l'expiration de leur période de conservation.
AutoDelete	• Vrai : les objets dans ce compartiment seront automatiquement supprimés à l'expiration de leur période de conservation, sauf si le compartiment fait l'objet d'une rétention légale. • Faux : les objets de ce compartiment ne seront pas supprimés automatiquement à l'expiration de la période de rétention. Vous devez supprimer ces objets manuellement si vous devez les supprimer.

Cohérence des paramètres de conformité

Lorsque vous mettez à jour les paramètres de conformité d'un compartiment S3 à l'aide d'une requête PUT Bucket compliance, StorageGRID tente de mettre à jour les métadonnées du compartiment sur l'ensemble de la grille. Par défaut, StorageGRID utilise la cohérence **Strong-global** pour garantir que tous les sites de centres de données et tous les nœuds de stockage contenant des métadonnées de compartiment bénéficient d'une cohérence en lecture après écriture pour les paramètres de conformité modifiés.

Si StorageGRID ne peut pas atteindre la cohérence **Strong-global** parce qu'un site de centre de données ou plusieurs Storage Nodes d'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 disponibles suffisamment de Storage Nodes sur chaque site, le support technique pourrait vous demander de relancer la requête ayant échoué en forçant la cohérence **Strong-site**.



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

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

Pour forcer l'utilisation de la cohérence **Strong-site**, réenvoyez la requête 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 inférieur à la période de rétention actuelle du compartiment, le code d'état HTTP est 400 Bad Request.

Informations connexes

["Déprécié : Modifications des requêtes PUT Bucket pour conformité"](#)

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 JOUISSANCE, 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 DÉLICTELLE (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.