



Opérations sur les compartiments

StorageGRID 11.7

NetApp
April 12, 2024

Sommaire

- Opérations sur les compartiments 1
- Opérations personnalisées dans les compartiments 8

Opérations sur les compartiments

Le système StorageGRID prend en charge un maximum de 1,000 compartiments pour chaque compte de locataire S3.

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 :

- ["Documentation Amazon Web Services \(AWS\) : restrictions et limites des compartiments"](#)
- ["Configuration des noms de domaine de terminaux S3"](#)

Les opérations GET Bucket (List Objects) et GET compartiment versions prennent en charge les contrôles de cohérence StorageGRID.

Vous pouvez vérifier si les mises à jour de l'heure du dernier accès sont activées ou désactivées pour les compartiments individuels.

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
SUPPRIMER le compartiment	Cette opération supprime le godet.
SUPPRIMER les godets	Cette opération supprime la configuration CORS pour le compartiment.
SUPPRIMER le chiffrement du compartiment	Cette opération supprime le chiffrement par défaut du compartiment. Les objets chiffrés existants restent chiffrés, mais aucun nouvel objet ajouté au compartiment n'est chiffré.
SUPPRIMER le cycle de vie du compartiment	Cette opération supprime la configuration du cycle de vie du compartiment. Voir "Création de la configuration du cycle de vie S3" .
SUPPRIMER la règle de compartiment	Cette opération supprime la règle attachée au compartiment.
SUPPRIMER la réplication du compartiment	Cette opération supprime la configuration de réplication attachée au compartiment.
SUPPRIMER le balisage du compartiment	Cette opération utilise le <code>tagging</code> sous-ressource pour supprimer toutes les balises d'un compartiment.

Fonctionnement	Mise en place
RUBRIQUE GET (ListObjects) (ListObjectsV2)	<p>Cette opération renvoie une partie ou la totalité (jusqu'à 1,000) des objets dans un godet. La classe de stockage pour les objets peut avoir l'une ou l'autre des deux valeurs, même si l'objet a été ingéré avec le REDUCED_REDUNDANCY option de classe de stockage :</p> <ul style="list-style-type: none"> • STANDARD, Qui indique que l'objet est stocké dans un pool de stockage composé de nœuds de stockage. • GLACIER, Qui indique que l'objet a été déplacé vers le compartiment externe spécifié par le pool de stockage cloud. <p>Si le compartiment contient un grand nombre de clés supprimées qui ont le même préfixe, la réponse peut inclure une partie CommonPrefixes qui ne contiennent pas de clés.</p>
OBTENIR les versions d'objet de compartiment (ListObjectVersions)	<p>Avec accès EN LECTURE sur un godet, cette opération avec le versions sous-ressource répertorie les métadonnées de toutes les versions des objets dans le compartiment.</p>
OBTENIR l'acl du compartiment	<p>Cette opération renvoie une réponse positive et l'ID, le DisplayName et l'autorisation du propriétaire du compartiment, indiquant que le propriétaire a un accès complet au compartiment.</p>
OBTENIR les godets	<p>Cette opération renvoie le cors configuration du compartiment.</p>
CHIFFREMENT des compartiments	<p>Cette opération renvoie la configuration de cryptage par défaut pour le compartiment.</p>
OPTIMISEZ le cycle de vie des compartiments (GetBucketLifecycleConfiguration)	<p>Cette opération retourne la configuration du cycle de vie du godet. Voir "Création de la configuration du cycle de vie S3".</p>
ACCÉDER à l'emplacement du compartiment	<p>Cette opération renvoie la région définie à l'aide de LocationConstraint Élément dans la demande PUT Bucket. Si la région du godet est de us-east-1, une chaîne vide est renvoyée pour la région.</p>
GET Bucket notification (GetBucketNotificationConfiguration)	<p>Cette opération renvoie la configuration de notification attachée au compartiment.</p>
GET Bucket policy	<p>Cette opération renvoie la politique attachée au godet.</p>
RÉPLICATION des compartiments	<p>Cette opération renvoie la configuration de réplique attachée au compartiment.</p>

Fonctionnement	Mise en place
GET Bucket tagging	<p>Cette opération utilise le <code>tagging</code> sous-ressource pour renvoyer toutes les balises d'un compartiment.</p>
GESTION des versions des compartiments	<p>Cette implémentation utilise le <code>versioning</code> sous-ressource pour retourner l'état de gestion des versions d'un compartiment.</p> <ul style="list-style-type: none"> • <i>Blank</i>: La gestion des versions n'a jamais été activée (le compartiment est « non versionné ») • Activé : la gestion des versions est activée • Suspendu : la gestion des versions a déjà été activée et est suspendue
OBTENIR la configuration de verrouillage d'objet	<p>Cette opération renvoie le mode de rétention par défaut du compartiment et la période de conservation par défaut, si configuré.</p> <p>Voir "Utilisez l'API REST S3 pour configurer le verrouillage objet S3".</p>
Godet DE TÊTE	<p>Cette opération détermine si un compartiment existe et que vous êtes autorisé à y accéder.</p> <p>Cette opération renvoie :</p> <ul style="list-style-type: none"> • <code>x-ntap-sg-bucket-id</code>: L'UUID du godet au format UUID. • <code>x-ntap-sg-trace-id</code>: ID de trace unique de la demande associée.

Fonctionnement	Mise en place
PLACER le godet	<p>Cette opération crée un nouveau godet. C'est en créant le compartiment que vous devenez le propriétaire.</p> <ul style="list-style-type: none"> • Les noms de compartiment doivent être conformes aux règles suivantes : <ul style="list-style-type: none"> ◦ Il doit être unique sur chaque système StorageGRID (et pas seulement au sein du compte du locataire). ◦ Doit être conforme DNS. ◦ Doit contenir au moins 3 caractères et pas plus de 63 caractères. ◦ Peut être une série d'une ou plusieurs étiquettes, avec des étiquettes adjacentes séparées par un point. Chaque étiquette doit commencer et se terminer par une lettre ou un chiffre en minuscules et ne peut utiliser que des lettres minuscules, des chiffres et des tirets. ◦ Ne doit pas ressembler à une adresse IP au format texte. ◦ Ne doit pas utiliser de périodes dans des demandes de type hébergement virtuel. Les périodes provoquera des problèmes avec la vérification du certificat générique du serveur. • Par défaut, les compartiments sont créés dans le <code>us-east-1</code> région ; cependant, vous pouvez utiliser le <code>LocationConstraint</code> élément de demande dans le corps de la demande pour spécifier une région différente. Lorsque vous utilisez le <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. <p>Remarque : une erreur se produit si votre demande PUT Bucket utilise une région qui n'a pas été définie dans StorageGRID.</p> <ul style="list-style-type: none"> • Vous pouvez inclure le <code>x-amz-bucket-object-lock-enabled</code> Demander l'en-tête pour créer un compartiment avec le verrouillage objet S3 activé. Voir "Utilisez l'API REST S3 pour configurer le verrouillage objet S3". <p>Vous devez activer le verrouillage d'objet S3 lors de la création du compartiment. Une fois un compartiment créé, vous ne pouvez ni ajouter ni désactiver le verrouillage objet S3. Le verrouillage objet S3 requiert la gestion des versions de compartiment, qui est activée automatiquement lors de la création du compartiment.</p>
PLACEZ les godets	<p>Cette opération définit la configuration du CORS pour un compartiment afin 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 <code>images</code> pour stocker des graphiques. En définissant la configuration CORS pour le <code>images</code> le champ permet d'afficher les images de ce compartiment sur le site web <code>http://www.example.com</code>.</p>

Fonctionnement	Mise en place
PUT Bucket Encryption	<p>Cette opération définit l'état de cryptage 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 de cryptage côté serveur, définissez l' <code>SSEAlgorithm</code> paramètre à <code>AES256</code>, et n'utilisez pas le <code>KMSMasterKeyID</code> paramètre.</p> <p>La configuration de cryptage par défaut du compartiment est ignorée si la demande de téléchargement d'objet spécifie déjà le cryptage (c'est-à-dire, si la demande inclut le <code>x-amz-server-side-encryption-*</code> en-tête de demande).</p>
<p>CYCLE de vie des compartiments</p> <p>(Configuration <code>PutBucketLifecycleConfiguration</code>)</p>	<p>Cette opération crée une nouvelle configuration de cycle de vie pour le compartiment ou remplace une configuration de cycle de vie existante. StorageGRID prend en charge jusqu'à 1,000 règles de cycle de vie dans une configuration cycle de vie. Chaque règle peut inclure les éléments XML suivants :</p> <ul style="list-style-type: none"> • Expiration (jours, date) • <code>NoncurrentVersionExp</code> (Nontactut Days) • Filtre (préfixe, étiquette) • État • ID <p>StorageGRID ne prend pas en charge les actions suivantes :</p> <ul style="list-style-type: none"> • <code>AbortIncompleteMultipartUpload</code> • <code>ExpiredObjectDeleteMarker</code> • Transition <p>Voir "Création de la configuration du cycle de vie S3". Pour comprendre comment l'action d'expiration d'un cycle de vie de compartiment interagit avec les instructions de placement ILM, reportez-vous à la section "Fonctionnement de ILM tout au long de la vie d'un objet".</p> <p>Remarque : la configuration du cycle de vie des compartiments peut être utilisée avec des compartiments avec le verrouillage d'objet S3 activé, mais la configuration du cycle de vie des compartiments n'est pas prise en charge pour les compartiments conformes hérités.</p>

Fonctionnement	Mise en place
PUT Bucket notification (PutBucketNotifationConfirguration)	<p>Cette opération configure les notifications pour le compartiment à l'aide du XML de configuration de notification inclus dans le corps de la demande. Vous devez connaître les détails d'implémentation suivants :</p> <ul style="list-style-type: none"> • StorageGRID prend en charge les rubriques SNS (simple notification Service) comme destinations. Les points finaux SQS (simple Queue Service) ou Lambda d'Amazon ne sont pas pris en charge. • La destination des notifications doit être spécifiée comme URN d'un terminal StorageGRID. Les terminaux peuvent être créés à l'aide du Gestionnaire de locataires ou de l'API de gestion des locataires. <p>Le noeud final doit exister pour que la configuration des notifications réussisse. Si le noeud final n'existe pas, un 400 Bad Request l'erreur est renvoyée avec le code <code>InvalidArgument</code>.</p> <ul style="list-style-type: none"> • Vous ne pouvez pas configurer de notification pour les types d'événements suivants. Ces types d'événements sont non pris en charge. <ul style="list-style-type: none"> ◦ <code>s3:ReducedRedundancyLostObject</code> ◦ <code>s3:ObjectRestore:Completed</code> • Les notifications d'événements envoyées par StorageGRID utilisent le format JSON standard, sauf qu'elles n'incluent pas certaines clés et utilisent des valeurs spécifiques pour d'autres, comme illustré dans la liste suivante : <ul style="list-style-type: none"> ◦ EventSource <li style="padding-left: 20px;"><code>sgws:s3</code> ◦ AwsRegion <li style="padding-left: 20px;">non inclus ◦ x-amz-id-2 <li style="padding-left: 20px;">non inclus ◦ arn <li style="padding-left: 20px;"><code>urn:sgws:s3:::bucket_name</code>
PUT Bucket policy	Cette opération définit la politique associée au compartiment.

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

Fonctionnement	Mise en place
PUT Bucket tagging	<p>Cette opération utilise le <code>tagging</code> sous-ressource pour ajouter ou mettre à jour un ensemble de balises pour un compartiment. Lors de l'ajout de balises de compartiment, tenez compte des limites suivantes :</p> <ul style="list-style-type: none"> • StorageGRID et Amazon S3 prennent en charge jusqu'à 50 balises pour chaque compartiment. • Les étiquettes associées à un compartiment doivent avoir des clés d'étiquette uniques. Une clé de balise peut comporter jusqu'à 128 caractères Unicode. • Les valeurs de balise peuvent comporter jusqu'à 256 caractères Unicode. • Les clés et les valeurs sont sensibles à la casse
GESTION des versions du compartiment	<p>Cette implémentation utilise le <code>versioning</code> sous-ressource pour définir l'état de gestion des versions d'un compartiment existant. Vous pouvez définir l'état de la gestion des versions à l'aide de l'une des valeurs suivantes :</p> <ul style="list-style-type: none"> • Activé : permet la gestion des versions des objets dans le compartiment. Tous les objets ajoutés au compartiment reçoivent un ID de version unique. • Suspendu : désactive la gestion des versions des objets dans le compartiment. Tous les objets ajoutés au compartiment reçoivent l'ID de version <code>null</code>.
CONFIGURATION du verrouillage de l'objet	<p>Cette opération configure ou supprime le mode de conservation par défaut du compartiment et la période de conservation par défaut.</p> <p>Si la période de conservation par défaut est modifiée, la conservation jusqu'à la date des versions d'objet existantes reste la même et n'est pas recalculée en utilisant la nouvelle période de conservation par défaut.</p> <p>Voir "Utilisez l'API REST S3 pour configurer le verrouillage objet S3" pour des informations détaillées.</p>

Informations associées

["Contrôles de cohérence"](#)

["HEURE du dernier accès au compartiment"](#)

["Utilisez les règles d'accès au compartiment et au groupe"](#)

["Opérations S3 suivies dans les journaux d'audit"](#)

Opérations personnalisées dans les compartiments

Le système StorageGRID prend en charge les opérations de compartiment personnalisées, ajoutées à l'API REST S3 et propres au système.

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

Fonctionnement	Description	Pour en savoir plus
OPTIMISEZ la cohérence des compartiments	Renvoie le niveau de cohérence appliqué à un compartiment spécifique.	"OPTIMISEZ la cohérence des compartiments"
PRÉSERVER la cohérence du godet	Définit le niveau de cohérence appliqué à un compartiment spécifique.	"PRÉSERVER la cohérence du godet"
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.	"HEURE du dernier accès au compartiment"
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.	"METTRE l'heure du dernier accès au compartiment"
SUPPRIMEZ la configuration de notification des métadonnées de compartiment	Supprime le XML de configuration de notification de métadonnées associé à un compartiment spécifique.	"SUPPRIMEZ la configuration de notification des métadonnées de compartiment"
CONFIGURATION DES notifications de métadonnées de compartiment	Renvoie le XML de configuration de notification de métadonnées associé à un compartiment spécifique.	"CONFIGURATION DES notifications de métadonnées de compartiment"
CONFIGURATION de notification des métadonnées de compartiment	Configure le service de notification des métadonnées pour un compartiment.	"CONFIGURATION de notification des métadonnées de compartiment"
PUT Bucket with Compliance settings	Obsolète et non pris en charge : vous ne pouvez plus créer de compartiments avec conformité activée.	"Obsolète : METTEZ le compartiment avec les paramètres de conformité"
ASSUREZ la conformité aux compartiments	Obsolète mais pris en charge : renvoie les paramètres de conformité actuellement en vigueur pour un compartiment compatible existant.	"Obsolète : CONFORMITÉ DES compartiments"
METTEZ le godet en conformité	Obsolète mais pris en charge : permet de modifier les paramètres de conformité d'un compartiment compatible existant.	"Obsolète : conformité DES compartiments PUT"

Informations associées

"Opérations S3 suivies dans les journaux d'audit"

Informations sur le copyright

Copyright © 2024 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 DÉLICTEUELLE (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.