



Gérez les services de la plateforme S3

StorageGRID 11.8

NetApp
March 19, 2024

Sommaire

- Gérez les services de la plateforme S3 1
 - Gérer les services de plate-forme : présentation 1
 - Considérations relatives aux services de plateforme 6
 - Configurer les terminaux des services de plateforme 9
 - Configurez la réplication CloudMirror 26
 - Configurer les notifications d'événements 30
 - Utilisez le service d'intégration de la recherche 34

Gérez les services de la plateforme S3

Gérer les services de plate-forme : présentation

Les services de plateforme StorageGRID vous aident à mettre en œuvre une stratégie de cloud hybride en vous permettant d'envoyer des notifications d'événements et des copies d'objets S3 et de métadonnées d'objet à des destinations externes.

Si l'utilisation des services de plateforme est autorisée pour votre compte de locataire, vous pouvez configurer les services suivants pour n'importe quel compartiment S3 :

Réplication CloudMirror

Utiliser "[Service de réplication StorageGRID CloudMirror](#)" Pour mettre en miroir des objets spécifiques d'un compartiment StorageGRID vers une destination externe spécifiée.

Vous pouvez, par exemple, utiliser la réplication CloudMirror pour mettre en miroir des enregistrements client spécifiques dans Amazon S3, puis exploiter les services AWS pour analyser vos données.



La réplication CloudMirror n'est pas prise en charge si le compartiment source est activé pour le verrouillage objet S3.

Notifications

Utiliser "[notifications d'événement par compartiment](#)" Pour envoyer des notifications sur des actions spécifiques effectuées sur des objets à un service Amazon simple notification Service (Amazon SNS) externe spécifié.

Par exemple, vous pouvez configurer l'envoi d'alertes aux administrateurs pour chaque objet ajouté à un compartiment, où les objets représentent les fichiers de journal associés à un événement système critique.



Bien que la notification d'événement puisse être configurée sur un compartiment avec l'option de verrouillage d'objet S3 activée, les métadonnées S3 Object Lock (conservation jusqu'à la date et état de conservation légale) des objets ne seront pas incluses dans les messages de notification.

Service d'intégration de la recherche

Utilisez le "[service d'intégration de la recherche](#)" Permet d'envoyer des métadonnées d'objet S3 à un index Elasticsearch spécifié pour rechercher ou analyser les métadonnées à l'aide du service externe.

Vous pouvez, par exemple, configurer des compartiments pour envoyer les métadonnées d'objet S3 vers un service Elasticsearch distant. Vous pouvez ensuite utiliser Elasticsearch pour effectuer des recherches dans des compartiments et effectuer des analyses sophistiquées des modèles présents dans les métadonnées de l'objet.



Bien que l'intégration avec Elasticsearch puisse être configurée sur un compartiment avec l'option S3 Object Lock activée, les métadonnées S3 Object Lock (conservation jusqu'à la date et état de conservation légale) des objets ne seront pas incluses dans les messages de notification.

L'emplacement cible des services de plateforme étant généralement externe à votre déploiement StorageGRID, les services de plateforme vous offrent la puissance et la flexibilité offertes par l'utilisation de

ressources de stockage externes, de services de notification et de services de recherche ou d'analyse pour vos données.

Toute combinaison de services de plateforme peut être configurée pour un seul compartiment S3. Par exemple, vous pouvez configurer le service CloudMirror et les notifications sur un compartiment StorageGRID S3 afin de pouvoir mettre en miroir des objets spécifiques sur Amazon simple Storage Service, tout en envoyant une notification sur chacun de ces objets à une application de surveillance tierce pour vous aider à suivre vos dépenses AWS.



L'utilisation des services de la plateforme doit être activée pour chaque compte de locataire par un administrateur StorageGRID à l'aide de Grid Manager ou de l'API de gestion du grid.

Configuration des services de plate-forme

Les services de plateforme communiquent avec les terminaux externes que vous configurez à l'aide de "[Gestionnaire de locataires](#)" ou le "[API de gestion des locataires](#)". Chaque terminal représente une destination externe, par exemple un compartiment StorageGRID S3, un compartiment Amazon Web Services, une rubrique Amazon SNS ou un cluster Elasticsearch hébergé localement, sur AWS ou ailleurs.

Après avoir créé un noeud final externe, vous pouvez activer un service de plate-forme pour un compartiment en ajoutant une configuration XML au compartiment. La configuration XML identifie les objets sur lesquels le compartiment doit agir, l'action que le compartiment doit effectuer et le point de terminaison que le compartiment doit utiliser pour le service.

Vous devez ajouter des configurations XML distinctes pour chaque service de plate-forme que vous souhaitez configurer. Par exemple :

- Si vous souhaitez que tous les objets dont les clés commencent par `/images` Pour la réplication vers un compartiment Amazon S3, vous devez ajouter une configuration de réplication dans le compartiment source.
- Si vous souhaitez également envoyer des notifications lorsque ces objets sont stockés dans le compartiment, vous devez ajouter une configuration de notifications.
- Enfin, si vous voulez indexer les métadonnées de ces objets, vous devez ajouter la configuration de notification de métadonnées utilisée pour implémenter l'intégration de la recherche.

Le format du XML de configuration est régi par les API REST S3 utilisées pour mettre en œuvre les services de plateforme StorageGRID :

Service de plateforme	L'API REST S3	Reportez-vous à la section
Réplication CloudMirror	<ul style="list-style-type: none">• GetBuckeReplication• PutBuckeReplication	<ul style="list-style-type: none">• "Réplication CloudMirror"• "Opérations sur les compartiments"
Notifications	<ul style="list-style-type: none">• GetBucketNotifationConfiguration• PutBucketNotifationConfiguration	<ul style="list-style-type: none">• "Notifications"• "Opérations sur les compartiments"

Service de plateforme	L'API REST S3	Reportez-vous à la section
Intégration de la recherche	<ul style="list-style-type: none"> • CONFIGURATION DES notifications de métadonnées de compartiment • CONFIGURATION de notification des métadonnées de compartiment 	<ul style="list-style-type: none"> • "Intégration de la recherche" • "Opérations personnalisées StorageGRID"

Informations associées

["Considérations relatives aux services de plateforme"](#)

Service de réplication CloudMirror

Vous pouvez activer la réplication CloudMirror pour un compartiment S3 si vous souhaitez que StorageGRID réplique des objets spécifiés ajoutés au compartiment dans un ou plusieurs compartiments de destination.

La réplication CloudMirror fonctionne indépendamment des règles ILM actives de la grille. Le service CloudMirror réplique les objets au fur et à mesure qu'ils sont stockés dans le compartiment source et les fournit au compartiment de destination dès que possible. La livraison des objets répliqués est déclenchée lors de la réussite de l'acquisition de l'objet.



La réplication CloudMirror présente des similarités et des différences importantes avec la fonction de réplication multigrille. Pour en savoir plus, voir ["Comparez la réplication entre les grilles et la réplication CloudMirror"](#).

Si vous activez la réplication CloudMirror pour un compartiment existant, seuls les nouveaux objets ajoutés à ce compartiment sont répliqués. Les objets existants dans le compartiment ne sont pas répliqués. Pour forcer la réplication d'objets existants, vous pouvez mettre à jour les métadonnées de l'objet existant en effectuant une copie d'objet.



Si vous utilisez la réplication CloudMirror pour copier des objets vers une destination Amazon S3, sachez qu'Amazon S3 limite la taille des métadonnées définies par l'utilisateur dans chaque en-tête de la requête PUT à 2 Ko. Si un objet possède des métadonnées définies par l'utilisateur supérieures à 2 Ko, cet objet ne sera pas répliqué.

Dans StorageGRID, vous pouvez répliquer les objets dans un compartiment unique vers plusieurs compartiments de destination. Pour ce faire, spécifiez la destination de chaque règle dans le XML de configuration de réplication. Vous ne pouvez pas répliquer un objet dans plusieurs compartiments en même temps.

En outre, vous pouvez configurer la réplication CloudMirror pour les compartiments avec version ou sans version, et spécifier un compartiment avec version ou sans version comme destination. Vous pouvez utiliser n'importe quelle combinaison de compartiments avec version et sans version. Par exemple, vous pouvez spécifier un compartiment avec version comme destination pour un compartiment source sans version, ou vice-versa. Vous pouvez également répliquer les compartiments sans version.

Le comportement de suppression du service de réplication CloudMirror est identique au comportement de suppression du service CRR (Cross Region Replication) fourni par Amazon S3 — la suppression d'un objet dans un compartiment source ne supprime jamais un objet répliqué dans la destination. Si le compartiment

source et le compartiment de destination sont multiversion, le marqueur de suppression est répliqué. Si le compartiment de destination n'est pas multiversion, la suppression d'un objet du compartiment source ne réplique pas le marqueur de suppression vers le compartiment de destination ou supprime l'objet de destination.

Comme les objets sont répliqués dans le compartiment de destination, StorageGRID les marque comme « répliqués ». Un compartiment StorageGRID de destination ne réplique pas à nouveau les objets marqués comme répliqués, ce qui vous protège contre les boucles de réplication accidentelles. Ce marquage de réplication est interne à StorageGRID et ne vous empêche pas d'utiliser AWS CRR lorsque vous utilisez un compartiment Amazon S3 comme destination.



L'en-tête personnalisé utilisé pour marquer une réplique est `x-ntap-sg-replica`. Ce marquage empêche un miroir en cascade. StorageGRID prend en charge un CloudMirror bidirectionnel entre deux grilles.

L'unicité et l'ordre des événements dans le compartiment de destination ne sont pas garantis. Plusieurs copies identiques d'un objet source peuvent être livrées à la destination du fait des opérations effectuées pour garantir le succès de la livraison. Dans de rares cas, lorsque le même objet est mis à jour simultanément depuis deux sites StorageGRID ou plus, il peut ne pas correspondre au ordre d'événements du compartiment source.

La réplication CloudMirror est généralement configurée pour utiliser un compartiment S3 externe comme destination. Vous pouvez cependant également configurer la réplication afin d'utiliser un autre déploiement StorageGRID ou tout service compatible S3.

Description des notifications pour les compartiments

Vous pouvez activer la notification d'événements pour un compartiment S3 si vous souhaitez que StorageGRID envoie des notifications sur des événements spécifiés à un cluster Kafka de destination ou à Amazon simple notification Service.

C'est possible "[configurer les notifications d'événements](#)" En associant XML de configuration de notification à un compartiment source. Le XML de configuration des notifications respecte les conventions S3 pour la configuration des notifications de compartiment. La rubrique Kafka ou Amazon SNS de destination est spécifiée comme URN d'un terminal.

Les notifications d'événements sont créées au niveau du compartiment source, comme indiqué dans la configuration de la notification, et sont envoyées vers le compartiment de destination. Si un événement associé à un objet réussit, une notification concernant cet événement est créée et mise en file d'attente pour la livraison.

L'unicité et l'ordre des notifications ne sont pas garantis. Plusieurs notifications d'événement peuvent être envoyées vers la destination après les opérations effectuées pour garantir la réussite de la livraison. La livraison étant asynchrone, l'ordre dans le temps des notifications au niveau de la destination n'est pas garanti correspondant à l'ordre des événements dans le compartiment source, en particulier pour les opérations provenant de différents sites StorageGRID. Vous pouvez utiliser le `sequencer` Key dans le message d'événement pour déterminer l'ordre des événements pour un objet particulier, tel que décrit dans la documentation Amazon S3.

Notifications et messages pris en charge

Les notifications d'événements StorageGRID suivent l'API Amazon S3 avec quelques limitations :

- Les types d'événements suivants sont pris en charge :

- s3:ObjectCreated:*
 - s3:ObjectCreated:put
 - s3:ObjectCreated:Post
 - s3:ObjectCreated:Copier
 - s3:ObjectCreated:CompleteMultipartUpload
 - s3:ObjectRemoved:*
 - s3:ObjectRemoved:Supprimer
 - s3:ObjectRemoved>DeleteMarkerCreated
 - s3:ObjectRestore:Post
- Les notifications d'événements envoyées par StorageGRID utilisent le format JSON standard, mais n'incluent pas certaines clés et utilisent des valeurs spécifiques pour d'autres, comme illustré dans le tableau :

Nom de la clé	Valeur ajoutée de StorageGRID
Source d'événements	sgws:s3
Région de l'awsRegion	non inclus
x-amz-id-2	non inclus
arn	urn:sgws:s3:::bucket_name

Comprendre le service d'intégration de la recherche

Si vous souhaitez utiliser un service externe de recherche et d'analyse de données pour vos métadonnées d'objet, vous pouvez activer l'intégration de la recherche pour un compartiment S3.

Le service d'intégration de recherche est un service StorageGRID personnalisé qui envoie automatiquement et de manière asynchrone des métadonnées d'objet S3 vers un terminal de destination lors de la mise à jour d'un objet ou de ses métadonnées. Vous pouvez ensuite utiliser des outils sophistiqués de recherche, d'analyse de données, de visualisation ou de machine learning proposés par le service de destination pour rechercher, analyser et obtenir des informations exploitables à partir de vos données d'objet.

Vous pouvez activer le service d'intégration de la recherche pour tout compartiment avec version ou sans version. L'intégration des recherches est configurée en associant le XML de configuration des notifications de métadonnées au compartiment qui spécifie les objets à utiliser et la destination des métadonnées de l'objet.

Les notifications sont générées sous la forme d'un document JSON nommé avec le nom de compartiment, le nom de l'objet et l'ID de version, le cas échéant. Chaque notification de métadonnées contient un ensemble standard de métadonnées système pour l'objet, en plus de toutes les balises de l'objet et de toutes les métadonnées utilisateur.



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.

Les notifications sont générées et mises en file d'attente pour livraison chaque fois que :

- Un objet est créé.
- Un objet est supprimé, notamment lorsque des objets sont supprimés suite au fonctionnement de la règle ILM de la grille.
- Les métadonnées ou les balises d'objet sont ajoutées, mises à jour ou supprimées. L'ensemble complet de métadonnées et de balises est toujours envoyé lors de la mise à jour, et pas seulement les valeurs modifiées.

Après avoir ajouté le XML de configuration de notification des métadonnées à un compartiment, des notifications sont envoyées pour tout nouvel objet que vous créez et pour tout objet que vous modifiez en mettant à jour ses données, métadonnées utilisateur ou balises. Cependant, aucune notification n'est envoyée pour les objets qui se trouvaient déjà dans le compartiment. Pour vous assurer que les métadonnées d'objet de tous les objets du compartiment sont envoyées à la destination, effectuez l'une des opérations suivantes :

- Configurez le service d'intégration de la recherche immédiatement après avoir créé le compartiment et avant d'ajouter des objets.
- Exécutez une action sur tous les objets déjà dans le compartiment pour déclencher un message de notification des métadonnées à envoyer à la destination.

Le service d'intégration de recherche StorageGRID prend en charge un cluster Elasticsearch. Comme pour les autres services de plate-forme, la destination est spécifiée dans le noeud final dont l'URN est utilisé dans le XML de configuration du service. Utilisez le "[Matrice d'interopérabilité NetApp](#)" Afin de déterminer les versions prises en charge par Elasticsearch.

Informations associées

["XML de configuration pour l'intégration de la recherche"](#)

["Métadonnées d'objet incluses dans les notifications de métadonnées"](#)

["JSON généré par le service d'intégration de la recherche"](#)

["Configurez le service d'intégration de la recherche"](#)

Considérations relatives aux services de plateforme

Avant de mettre en œuvre des services de plateforme, examinez les recommandations et les considérations relatives à l'utilisation de ces services.

Pour plus d'informations sur S3, reportez-vous à la section "[UTILISEZ L'API REST S3](#)".

Considérations relatives à l'utilisation des services de plate-forme

Réflexion	Détails
Surveillance des terminaux de destination	<p>Vous devez surveiller la disponibilité de chaque point final de destination. Si la connexion au point final de destination est perdue pendant une période prolongée et qu'il existe un important retard de requêtes, les demandes client supplémentaires (telles QUE LES requêtes ENVOYÉES) à StorageGRID échoueront. Vous devez réessayer ces demandes ayant échoué lorsque le noeud final devient accessible.</p>
Limitation du terminal de destination	<p>Le logiciel StorageGRID peut canaliser les demandes S3 entrantes pour un compartiment si le taux d'envoi des demandes dépasse le taux à partir duquel le terminal de destination peut recevoir les demandes. La restriction ne se produit que lorsqu'il existe un arriéré de demandes en attente d'envoi vers le noeud final de destination.</p> <p>Le seul effet visible est que les requêtes S3 entrantes prennent plus de temps à s'exécuter. Si vous commencez à détecter les performances beaucoup plus lentes, vous devez réduire le taux d'entrée ou utiliser un terminal avec une capacité plus élevée. Si l'arnet de commandes des requêtes continue d'augmenter, les opérations S3 des clients (par EXEMPLE, LES requêtes PUT) finiront par échouer.</p> <p>Les demandes CloudMirror sont plus susceptibles d'être affectées par les performances du terminal de destination, car ces demandes impliquent généralement plus de transfert de données que les demandes d'intégration de recherche ou de notification d'événements.</p>
Garanties de commande	<p>StorageGRID garantit l'ordre des opérations sur un objet d'un site. Tant que toutes les opérations relatives à un objet se trouvent sur le même site, l'état final de l'objet (pour la réplication) sera toujours égal à l'état dans StorageGRID.</p> <p>StorageGRID tente également de commander des demandes lorsque des opérations sont effectuées sur des sites StorageGRID. Par exemple, si vous écrivez un objet initialement sur le site A, puis que vous le remplacez par un autre objet au niveau du site B, le dernier objet répliqué par CloudMirror vers le compartiment de destination n'est pas garanti que ce nouvel objet soit.</p>
Suppressions d'objets basées sur des règles ILM	<p>Pour correspondre au comportement de suppression des CRR AWS et Amazon simple notification Service, les requêtes CloudMirror et de notification d'événement ne sont pas envoyées lorsqu'un objet du compartiment source est supprimé en raison des règles ILM de StorageGRID. Par exemple, aucune demande de notification de CloudMirror ou d'événement n'est envoyée si une règle ILM supprime un objet au bout de 14 jours.</p> <p>Au contraire, les demandes d'intégration de la recherche sont envoyées lorsque les objets sont supprimés du fait de ILM.</p>

Réflexion	Détails
À l'aide des terminaux Kafka	<p>Pour les terminaux Kafka, le protocole TLS mutuel n'est pas pris en charge. Par conséquent, si vous avez <code>ssl.client.auth</code> réglé sur <code>required</code> Dans la configuration de votre courtier Kafka, il peut être à l'origine de problèmes de configuration du terminal Kafka.</p> <p>L'authentification des terminaux Kafka utilise les types d'authentification suivants. Ces types sont différents de ceux utilisés pour l'authentification d'autres terminaux, tels qu'Amazon SNS, et nécessitent des informations d'identification de nom d'utilisateur et de mot de passe.</p> <ul style="list-style-type: none"> • SASL/SIMPLE • SASL/SCRAM-SHA-256 • SASL/SCRAM-SHA-512 <p>Remarque : les paramètres du proxy de stockage configuré ne s'appliquent pas aux noeuds finaux des services de la plateforme Kafka.</p>

Considérations relatives à l'utilisation du service de réplication CloudMirror

Réflexion	Détails
État de la réplication	StorageGRID ne prend pas en charge le <code>x-amz-replication-status</code> en-tête.
Taille de l'objet	<p>La taille maximale des objets qui peuvent être répliqués dans un compartiment de destination par le service de réplication CloudMirror est de 5 Tio, soit la même que la taille maximale de l'objet <i>pris en charge</i>.</p> <p>Remarque : la taille <i>recommandée</i> maximale pour une opération <code>PutObject</code> unique est de 5 Gio (5,368,709,120 octets). Si vos objets sont supérieurs à 5 Gio, utilisez le téléchargement partitionné.</p>
Gestion des versions du compartiment et ID de version	<p>Si le compartiment S3 source de StorageGRID est activé pour la gestion des versions, vous devez également activer la gestion des versions pour le compartiment de destination.</p> <p>Lors de l'utilisation du contrôle de version, notez que l'ordre des versions d'objet dans le compartiment de destination est meilleur effort et n'est pas garanti par le service CloudMirror, en raison des limites du protocole S3.</p> <p>Remarque : les ID de version du compartiment source dans StorageGRID ne sont pas liés aux ID de version du compartiment de destination.</p>

Réflexion	Détails
Balises des versions d'objets	<p>Le service CloudMirror ne réplique pas les requêtes PutObjectTagging ou DeleteObjectTagging qui fournissent un ID de version, en raison des limitations du protocole S3. Étant donné que les ID de version de la source et de la destination ne sont pas liés, il n'est pas possible de s'assurer qu'une mise à jour de balise vers un ID de version spécifique sera répliquée.</p> <p>En revanche, le service CloudMirror réplique les requêtes PutObjectTagging ou DeleteObjectTagging qui ne spécifient pas d'ID de version. Ces demandes mettent à jour les balises pour la clé la plus récente (ou la dernière version si le compartiment est versionné). Les objets normaux avec des étiquettes (et non les mises à jour de marquage) sont également répliqués.</p>
Téléchargements partitionnés et ETag valeurs	Lors de la mise en miroir d'objets qui ont été téléchargés à l'aide d'un téléchargement partitionné, le service CloudMirror ne conserve pas les pièces. En conséquence, le ETag la valeur de l'objet symétrique sera différente de la ETag valeur de l'objet d'origine.
Chiffrement des objets avec SSE-C (chiffrement côté serveur avec clés fournies par le client)	Le service CloudMirror ne prend pas en charge les objets chiffrés avec SSE-C. Si vous tentez d'ingérer un objet dans le compartiment source pour la réplication CloudMirror et que la demande inclut les en-têtes de requête SSE-C, l'opération échoue.
Compartiment avec verrouillage objet S3 activé	Si S3 Object Lock est activé dans le compartiment S3 de destination pour la réplication CloudMirror, la tentative de configuration de la réplication de compartiment (PutBucketReplication) échouera avec une erreur AccessDenied.

Configurer les terminaux des services de plateforme

Avant de pouvoir configurer un service de plateforme pour un compartiment, vous devez configurer au moins un point de terminaison afin qu'il soit la destination du service de plateforme.

L'accès aux services de plateforme est activé par locataire par administrateur StorageGRID. Pour créer ou utiliser un noeud final de services de plate-forme, vous devez être un utilisateur locataire disposant de l'autorisation gérer les noeuds finaux ou accès racine, dans une grille dont la mise en réseau a été configurée pour permettre aux noeuds de stockage d'accéder aux ressources de noeuds finaux externes. Pour un seul locataire, vous pouvez configurer un maximum de 500 terminaux de services de plateforme. Pour plus d'informations, contactez votre administrateur StorageGRID.

Qu'est-ce qu'un terminal de services de plateforme ?

Lorsque vous créez un noeud final de services de plate-forme, vous spécifiez les informations dont StorageGRID a besoin pour accéder à la destination externe.

Par exemple, si vous souhaitez répliquer des objets à partir d'un compartiment StorageGRID vers un compartiment Amazon S3, vous créez un terminal des services de plateforme qui inclut les informations et les identifiants dont StorageGRID a besoin pour accéder au compartiment de destination sur Amazon.

Chaque type de service de plate-forme nécessite son propre terminal, vous devez donc configurer au moins

un point final pour chaque service de plate-forme que vous prévoyez d'utiliser. Après avoir défini un noeud final de services de plate-forme, vous utilisez l'URN du noeud final comme destination dans le XML de configuration utilisé pour activer le service.

Vous pouvez utiliser le même point final que la destination pour plusieurs compartiments source. Par exemple, vous pouvez configurer plusieurs compartiments source pour envoyer les métadonnées d'objet vers le même point de terminaison d'intégration de la recherche, afin d'effectuer des recherches dans plusieurs compartiments. Vous pouvez également configurer un compartiment source pour qu'il utilise plusieurs terminaux comme cible, ce qui vous permet d'envoyer des notifications sur la création d'objets à une rubrique Amazon simple notification Service (Amazon SNS) et des notifications sur la suppression d'objets à une autre rubrique Amazon SNS.

Terminaux pour la réplication CloudMirror

StorageGRID prend en charge les terminaux de réplication qui représentent des compartiments S3. Ces compartiments peuvent être hébergés sur Amazon Web Services, sur le même déploiement StorageGRID, sur un autre service ou sur un autre déploiement à distance.

Terminaux pour les notifications

StorageGRID prend en charge les terminaux Amazon SNS et Kafka. Les terminaux SQS (simple Queue Service) ou Lambda d'AWS ne sont pas pris en charge.

Pour les terminaux Kafka, le protocole TLS mutuel n'est pas pris en charge. Par conséquent, si vous avez `ssl.client.auth` réglé sur `required` Dans la configuration de votre courtier Kafka, il peut être à l'origine de problèmes de configuration du terminal Kafka.

Points d'extrémité du service d'intégration de la recherche

StorageGRID prend en charge des terminaux d'intégration de recherche représentant les clusters Elasticsearch. Ces clusters Elasticsearch peuvent se trouver dans un data Center local ou être hébergés dans un cloud AWS ou ailleurs.

Le point final de l'intégration de la recherche fait référence à un index et à un type Elasticsearch spécifiques. Vous devez créer l'index dans Elasticsearch avant la création du noeud final dans StorageGRID, sinon la création du noeud final échouera. Il n'est pas nécessaire de créer le type avant de créer le noeud final. StorageGRID crée le type si nécessaire lors de l'envoi de métadonnées d'objet au terminal.

Informations associées

["Administrer StorageGRID"](#)

Spécifiez l'URN du terminal des services de plateforme

Lorsque vous créez un noeud final de services de plate-forme, vous devez spécifier un Nom de ressource unique (URN). Vous utiliserez l'URN pour référencer le noeud final lorsque vous créerez un XML de configuration pour le service de plate-forme. L'URN de chaque terminal doit être unique.

StorageGRID valide les terminaux de services de plateforme lors de leur création. Avant de créer un noeud final de services de plate-forme, vérifiez que la ressource spécifiée dans le noeud final existe et qu'elle peut être atteinte.

Éléments DE RETOUR

L'URN d'un terminal de services de plateforme doit commencer par l'un ou l'autre `arn:aws` ou `urn:mystore`, comme suit:

- Si ce service est hébergé sur Amazon Web Services (AWS), utilisez `arn:aws`
- Si ce service est hébergé sur Google Cloud Platform (GCP), utilisez `arn:aws`
- Si le service est hébergé localement, utilisez `urn:mystore`

Par exemple, si vous spécifiez l'URN pour un terminal CloudMirror hébergé sur StorageGRID, il peut commencer par l'URN `urn:sgws`.

L'élément suivant de l'URN spécifie le type de service de plateforme, comme suit :

Service	Type
Réplication CloudMirror	s3
Notifications	sns ou kafka
Intégration de la recherche	es

Par exemple, pour continuer à spécifier l'URN d'un terminal CloudMirror hébergé sur StorageGRID, vous devez ajouter `s3` pour obtenir `urn:sgws:s3`.

L'élément final de l'URN identifie la ressource cible spécifique au niveau de l'URI de destination.

Service	Ressource spécifique
Réplication CloudMirror	bucket-name
Notifications	sns-topic-name ou kafka-topic-name
Intégration de la recherche	domain-name/index-name/type-name Remarque : si le cluster Elasticsearch est NOT configuré pour créer automatiquement des index, vous devez créer l'index manuellement avant de créer le noeud final.

Urns pour les services hébergés sur AWS et GCP

Pour les entités AWS et GCP, l'URN complet est un ARN AWS valide. Par exemple :

- Réplication CloudMirror :

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

- Notifications :

```
arn:aws:sns:region:account-id:topic-name
```

- Intégration de la recherche :

```
arn:aws:es:region:account-id:domain/domain-name/index-name/type-name
```



Pour un terminal d'intégration de recherche AWS, le `domain-name` doit inclure la chaîne littérale `domain/`, comme indiqué ici.

Urnes pour des services hébergés localement

Lors de l'utilisation de services hébergés localement au lieu de services cloud, vous pouvez spécifier l'URN de toute façon qui crée un URN valide et unique, tant que l'URN inclut les éléments requis dans les troisième et dernière positions. Vous pouvez laisser les éléments indiqués en blanc facultatif, ou vous pouvez les spécifier de quelque manière que ce soit pour vous aider à identifier la ressource et à rendre l'URN unique. Par exemple :

- Réplication CloudMirror :

```
urn:mystore:s3:optional:optional:bucket-name
```

Pour un terminal CloudMirror hébergé sur StorageGRID, vous pouvez spécifier un URN valide commençant par `urn:sgws:`

```
urn:sgws:s3:optional:optional:bucket-name
```

- Notifications :

Spécifiez un point de terminaison Amazon simple notification Service :

```
urn:mystore:sns:optional:optional:sns-topic-name
```

Spécifiez un terminal Kafka :

```
urn:mystore:kafka:optional:optional:kafka-topic-name
```

- Intégration de la recherche :

```
urn:mystore:es:optional:optional:domain-name/index-name/type-name
```



Pour les points de terminaison d'intégration de recherche hébergés localement, le `domain-name` L'élément peut être n'importe quelle chaîne tant que l'URN du terminal est unique.

Créer un terminal de services de plate-forme

Vous devez créer au moins un noeud final du type correct avant d'activer un service de plate-forme.

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un ["navigateur web pris en charge"](#).
- Les services de plateforme ont été activés pour votre compte de locataire par un administrateur StorageGRID.
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Gestion des noeuds finaux ou des autorisations d'accès racine"](#).
- La ressource référencée par le noeud final des services de plate-forme a été créée :
 - Réplication CloudMirror : compartiment S3
 - Notification d'événements : Amazon simple notification Service (Amazon SNS) ou rubrique Kafka
 - Notification de recherche : index Elasticsearch, si le cluster de destination n'est pas configuré pour créer automatiquement des index.
- Vous disposez des informations relatives à la ressource de destination :
 - Hôte et port pour l'URI (Uniform Resource identifier)



Si vous prévoyez d'utiliser un compartiment hébergé sur un système StorageGRID comme point de terminaison pour la réplication CloudMirror, contactez l'administrateur de la grille pour déterminer les valeurs à saisir.

- Nom de ressource unique (URN)

["Spécifiez l'URN du terminal des services de plateforme"](#)

- Informations d'authentification (si nécessaire) :

Terminaux d'intégration de la recherche AWS

Pour les terminaux d'intégration de la recherche AWS, vous pouvez utiliser les informations d'identification suivantes :

- Clé d'accès : ID de clé d'accès et clé d'accès secrète
- HTTP de base : nom d'utilisateur et mot de passe
- CAP (C2S Access Portal) : URL d'informations d'identification temporaires, certificats de serveur et de client, clés client et phrase de passe de clé privée de client facultative.

La réplication CloudMirror et les terminaux Amazon SNS

Pour la réplication CloudMirror et les terminaux Amazon SNS, vous pouvez utiliser les informations d'identification suivantes :

- Clé d'accès : ID de clé d'accès et clé d'accès secrète
- CAP (C2S Access Portal) : URL d'informations d'identification temporaires, certificats de serveur et de client, clés client et phrase de passe de clé privée de client facultative.

Les terminaux Kafka

Pour les terminaux Kafka, vous pouvez utiliser les identifiants suivants :

- SASL/PLAIN : nom d'utilisateur et mot de passe
- SASL/SCRAM-SHA-256 : nom d'utilisateur et mot de passe
- SASL/SCRAM-SHA-512 : nom d'utilisateur et mot de passe

◦ Certificat de sécurité (en cas d'utilisation d'un certificat d'autorité de certification personnalisé)

- Si les fonctions de sécurité de Elasticsearch sont activées, vous disposez du privilège Monitor cluster pour les tests de connectivité et du privilège write index ou des privilèges index and delete index pour les mises à jour de documents.

Étapes

1. Sélectionnez **STORAGE (S3) > Platform services Endpoints**. La page noeuds finaux des services de plate-forme s'affiche.
2. Sélectionnez **Créer un noeud final**.
3. Entrez un nom d'affichage pour décrire brièvement le point final et son objectif.

Le type de service de plate-forme pris en charge par le noeud final est affiché à côté du nom du noeud final lorsqu'il est répertorié sur la page noeuds finaux, de sorte que vous n'avez pas besoin d'inclure ces informations dans le nom.

4. Dans le champ **URI**, spécifiez l'identificateur de ressource unique (URI) du noeud final.

Utilisez l'un des formats suivants :

```
https://host:port  
http://host:port
```

Si vous ne spécifiez pas de port, les ports par défaut suivants sont utilisés :

- Port 443 pour les URI HTTPS et port 80 pour les URI HTTP (la plupart des terminaux)
- Port 9092 pour les URI HTTPS et HTTP (terminaux Kafka uniquement)

Par exemple, l'URI d'un compartiment hébergé sur StorageGRID peut être :

```
https://s3.example.com:10443
```

Dans cet exemple, `s3.example.com` Représente l'entrée DNS pour l'adresse IP virtuelle (VIP) du groupe haute disponibilité StorageGRID, et `10443` représente le port défini dans le noeud final de l'équilibreur de charge.



Si possible, vous devez vous connecter à un groupe haute disponibilité de nœuds d'équilibrage de la charge pour éviter un point de défaillance unique.

De la même manière, l'URI d'un compartiment hébergé sur AWS peut être :

```
https://s3-aws-region.amazonaws.com
```



Si le noeud final est utilisé pour le service de réplication CloudMirror, n'incluez pas le nom de compartiment dans l'URI. Vous incluez le nom du compartiment dans le champ **URN**.

5. Entrez le nom de ressource unique (URN) du noeud final.



Vous ne pouvez pas modifier l'URN d'un noeud final après sa création.

6. Sélectionnez **Continuer**.

7. Sélectionnez une valeur pour **Type d'authentification**.

Terminaux d'intégration de la recherche AWS

Entrez ou téléchargez les informations d'identification d'un terminal d'intégration de recherche AWS.

Les informations d'identification que vous fournissez doivent disposer d'autorisations d'écriture pour la ressource de destination.

Type d'authentification	Description	Informations d'identification
Anonyme	Fournit un accès anonyme à la destination. Fonctionne uniquement pour les terminaux dont la sécurité est désactivée.	Pas d'authentification.
Clé d'accès	Utilise des identifiants de style AWS pour authentifier les connexions avec la destination.	<ul style="list-style-type: none">• ID de clé d'accès• Clé d'accès secrète
HTTP de base	Utilise un nom d'utilisateur et un mot de passe pour authentifier les connexions à la destination.	<ul style="list-style-type: none">• Nom d'utilisateur• Mot de passe
CAP (portail d'accès C2S)	Utilise des certificats et des clés pour authentifier les connexions à la destination.	<ul style="list-style-type: none">• URL des informations d'identification temporaires• Certificat autorité de certification du serveur (téléchargement de fichiers PEM)• Certificat client (téléchargement de fichier PEM)• Clé privée client (téléchargement de fichiers PEM, format crypté OpenSSL ou format de clé privée non crypté)• Phrase de passe de clé privée du client (facultatif)

Réplication CloudMirror ou terminaux Amazon SNS

Entrez ou téléchargez les informations d'identification pour une réplication CloudMirror ou un terminal SNS Amazon.

Les informations d'identification que vous fournissez doivent disposer d'autorisations d'écriture pour la ressource de destination.

Type d'authentification	Description	Informations d'identification
Anonyme	Fournit un accès anonyme à la destination. Fonctionne uniquement pour les terminaux dont la sécurité est désactivée.	Pas d'authentification.
Clé d'accès	Utilise des identifiants de style AWS pour authentifier les connexions avec la destination.	<ul style="list-style-type: none"> • ID de clé d'accès • Clé d'accès secrète
CAP (portail d'accès C2S)	Utilise des certificats et des clés pour authentifier les connexions à la destination.	<ul style="list-style-type: none"> • URL des informations d'identification temporaires • Certificat autorité de certification du serveur (téléchargement de fichiers PEM) • Certificat client (téléchargement de fichier PEM) • Clé privée client (téléchargement de fichiers PEM, format crypté OpenSSL ou format de clé privée non crypté) • Phrase de passe de clé privée du client (facultatif)

Les terminaux Kafka

Entrez ou téléchargez les identifiants d'un terminal Kafka.

Les informations d'identification que vous fournissez doivent disposer d'autorisations d'écriture pour la ressource de destination.

Type d'authentification	Description	Informations d'identification
Anonyme	Fournit un accès anonyme à la destination. Fonctionne uniquement pour les terminaux dont la sécurité est désactivée.	Pas d'authentification.
SASL/SIMPLE	Utilise un nom d'utilisateur et un mot de passe avec du texte brut pour authentifier les connexions à la destination.	<ul style="list-style-type: none"> • Nom d'utilisateur • Mot de passe

Type d'authentification	Description	Informations d'identification
SASL/SCRAM-SHA-256	Utilise un nom d'utilisateur et un mot de passe à l'aide d'un protocole de réponse de vérification et d'un hachage SHA-256 pour authentifier les connexions à la destination.	<ul style="list-style-type: none"> Nom d'utilisateur Mot de passe
SASL/SCRAM-SHA-512	Utilise un nom d'utilisateur et un mot de passe à l'aide d'un protocole de réponse de vérification et d'un hachage SHA-512 pour authentifier les connexions à la destination.	<ul style="list-style-type: none"> Nom d'utilisateur Mot de passe

Sélectionnez **utiliser la délégation prise de l'authentification** si le nom d'utilisateur et le mot de passe proviennent d'un jeton de délégation obtenu à partir d'un cluster Kafka.

- Sélectionnez **Continuer**.
- Sélectionnez un bouton radio pour **Verify Server** pour choisir la manière dont la connexion TLS au noeud final est vérifiée.

Create endpoint ✕

✓ Enter details

✓ Select authentication type
Optional

3 Verify server
Optional

Verify server

Use this method to validate the certificate for TLS connections to the endpoint resource. If you select "Use custom CA certificate," copy and paste the custom security certificate in the text box.

Use custom CA certificate

Use operating system CA certificate

Do not verify certificate

```

-----BEGIN CERTIFICATE-----
abodefghijkl123456780ABCDEFGHIUML
123456/7890ABCDEFabodefghijklABCD
-----END CERTIFICATE-----

```

Previous
Test and create endpoint

Type de vérification du certificat	Description
Utiliser un certificat d'autorité de certification personnalisé	Utilisez un certificat de sécurité personnalisé. Si vous sélectionnez ce paramètre, copiez et collez le certificat de sécurité personnalisé dans la zone de texte certificat CA .
Utiliser le certificat CA du système d'exploitation	Utilisez le certificat d'autorité de certification Grid par défaut installé sur le système d'exploitation pour sécuriser les connexions.
Ne vérifiez pas le certificat	Le certificat utilisé pour la connexion TLS n'est pas vérifié. Cette option n'est pas sécurisée.

10. Sélectionnez **Test et Créer un noeud final**.

- Un message de réussite s'affiche si le noeud final peut être atteint à l'aide des informations d'identification spécifiées. La connexion au noeud final est validée à partir d'un noeud sur chaque site.
- Un message d'erreur s'affiche si la validation du noeud final échoue. Si vous devez modifier le noeud final pour corriger l'erreur, sélectionnez **Retour aux détails du noeud final** et mettez à jour les informations. Sélectionnez ensuite **Test et Créer un noeud final**.



La création du terminal échoue si les services de plate-forme ne sont pas activés pour votre compte de locataire. Veuillez contacter votre administrateur StorageGRID.

Après avoir configuré un noeud final, vous pouvez utiliser son URN pour configurer un service de plate-forme.

Informations associées

["Spécifiez l'URN du terminal des services de plateforme"](#)

["Configurez la réplique CloudMirror"](#)

["Configurer les notifications d'événements"](#)

["Configurez le service d'intégration de la recherche"](#)

Tester la connexion pour le point final des services de plate-forme

Si la connexion à un service de plate-forme a changé, vous pouvez tester la connexion du noeud final pour vérifier que la ressource de destination existe et qu'elle peut être atteinte à l'aide des informations d'identification que vous avez spécifiées.

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un ["navigateur web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Gestion des noeuds finaux ou des autorisations d'accès racine"](#).

Description de la tâche

StorageGRID ne vérifie pas que les informations d'identification disposent des autorisations appropriées.

Étapes

1. Sélectionnez **STORAGE (S3) > Platform services Endpoints**.

La page noeuds finaux des services de plate-forme s'affiche et affiche la liste des noeuds finaux des services de plate-forme déjà configurés.

Platform services endpoints

A platform services endpoint stores the information StorageGRID needs to use an external resource as a target for a platform service (CloudMirror replication, notifications, or search integration). You must configure an endpoint for each platform service you plan to use.

4 endpoints [Create endpoint](#)


[Delete endpoint](#)

<input type="checkbox"/>	Display name ? ↕	Last error ? ↕	Type ? ↕	URI ? ↕	URN ? ↕
<input type="checkbox"/>	my-endpoint-1		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket1
<input type="checkbox"/>	my-endpoint-2	✖ 2 hours ago	Search	http://10.96.104.30:9200	urn:sgws:es:::mydomain/sveloso/_doc
<input type="checkbox"/>	my-endpoint-3		Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example1
<input type="checkbox"/>	my-endpoint-4		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket2

2. Sélectionnez le noeud final dont vous souhaitez tester la connexion.

La page des détails du point final s'affiche.

Overview ^

Display name:	my-endpoint-1 
Type:	S3 Bucket
URI:	http://10.96.104.167:10443
URN:	urn:sgws:s3:::bucket1

ConnectionConfiguration

Verify connection

Some errors might continue to appear after they are resolved. To see if an error is current or to force the removal of a resolved error, select **Test connection**.

Test connection

3. Sélectionnez **Tester la connexion**.

- Un message de réussite s'affiche si le noeud final peut être atteint à l'aide des informations d'identification spécifiées. La connexion au noeud final est validée à partir d'un noeud sur chaque site.
- Un message d'erreur s'affiche si la validation du noeud final échoue. Si vous devez modifier le noeud final pour corriger l'erreur, sélectionnez **Configuration** et mettez à jour les informations. Sélectionnez ensuite **Test et enregistrer les modifications**.

Modifier le point final des services de plate-forme

Vous pouvez modifier la configuration d'un point de terminaison de services de plate-forme pour modifier son nom, son URI ou d'autres détails. Par exemple, vous devez peut-être mettre à jour les informations d'identification expirées ou modifier l'URI pour qu'il pointe vers un index Elasticsearch de sauvegarde pour le basculement. Vous ne pouvez pas modifier l'URN d'un terminal de services de plate-forme.

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un ["navigateur web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Gestion des noeuds finaux ou des autorisations d'accès racine"](#).

Étapes

1. Sélectionnez **STORAGE (S3) > Platform services Endpoints**.

La page noeuds finaux des services de plate-forme s'affiche et affiche la liste des noeuds finaux des services de plate-forme déjà configurés.

Platform services endpoints

A platform services endpoint stores the information StorageGRID needs to use an external resource as a target for a platform service (CloudMirror replication, notifications, or search integration). You must configure an endpoint for each platform service you plan to use.

4 endpoints

Create endpoint

Delete endpoint

<input type="checkbox"/>	Display name	Last error	Type	URI	URN
<input type="checkbox"/>	my-endpoint-1		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket1
<input type="checkbox"/>	my-endpoint-2	2 hours ago	Search	http://10.96.104.30:9200	urn:sgws:es:::mydomain/sveloso/_doc
<input type="checkbox"/>	my-endpoint-3		Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example1
<input type="checkbox"/>	my-endpoint-4		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket2

2. Sélectionnez le point final que vous souhaitez modifier.

La page des détails du point final s'affiche.

3. Sélectionnez **Configuration**.

4. Modifiez la configuration du noeud final selon les besoins.



Vous ne pouvez pas modifier l'URN d'un noeud final après sa création.

a. Pour modifier le nom d'affichage du noeud final, sélectionnez l'icône d'édition .

b. Modifiez l'URI si nécessaire.

c. Si nécessaire, modifiez le type d'authentification.

- Pour l'authentification par clé d'accès, modifiez la clé selon vos besoins en sélectionnant **Modifier la clé S3** et en collant une nouvelle ID de clé d'accès et une nouvelle clé d'accès secrète. Si vous devez annuler vos modifications, sélectionnez **Revert S3 key edit**.
- Pour l'authentification CAP (C2S Access Portal), modifiez l'URL des informations d'identification temporaires ou la phrase de passe de la clé privée du client facultative et téléchargez de nouveaux certificats et fichiers de clés selon les besoins.



La clé privée du client doit être au format crypté OpenSSL ou au format de clé privée non crypté.

d. Si nécessaire, modifiez la méthode de vérification du serveur.

5. Sélectionnez **Tester et enregistrer les modifications**.

- Un message de réussite s'affiche si le noeud final peut être atteint à l'aide des informations d'identification spécifiées. La connexion au noeud final est vérifiée à partir d'un noeud sur chaque site.

- Un message d'erreur s'affiche si la validation du noeud final échoue. Modifiez le noeud final pour corriger l'erreur, puis sélectionnez **Test et enregistrer les modifications**.

Supprimer le noeud final des services de plate-forme

Vous pouvez supprimer un noeud final si vous ne souhaitez plus utiliser le service de plate-forme associé.

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Gestion des noeuds finaux ou des autorisations d'accès racine".

Étapes

1. Sélectionnez **STORAGE (S3) > Platform services Endpoints**.

La page noeuds finaux des services de plate-forme s'affiche et affiche la liste des noeuds finaux des services de plate-forme déjà configurés.

Platform services endpoints

A platform services endpoint stores the information StorageGRID needs to use an external resource as a target for a platform service (CloudMirror replication, notifications, or search integration). You must configure an endpoint for each platform service you plan to use.

4 endpoints Create endpoint

Delete endpoint

<input type="checkbox"/>	Display name ?	Last error ?	Type ?	URI ?	URN ?
<input type="checkbox"/>	my-endpoint-1		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket1
<input type="checkbox"/>	my-endpoint-2	✖ 2 hours ago	Search	http://10.96.104.30:9200	urn:sgws:es:::mydomain/sveloso/_doc
<input type="checkbox"/>	my-endpoint-3		Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example1
<input type="checkbox"/>	my-endpoint-4		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket2

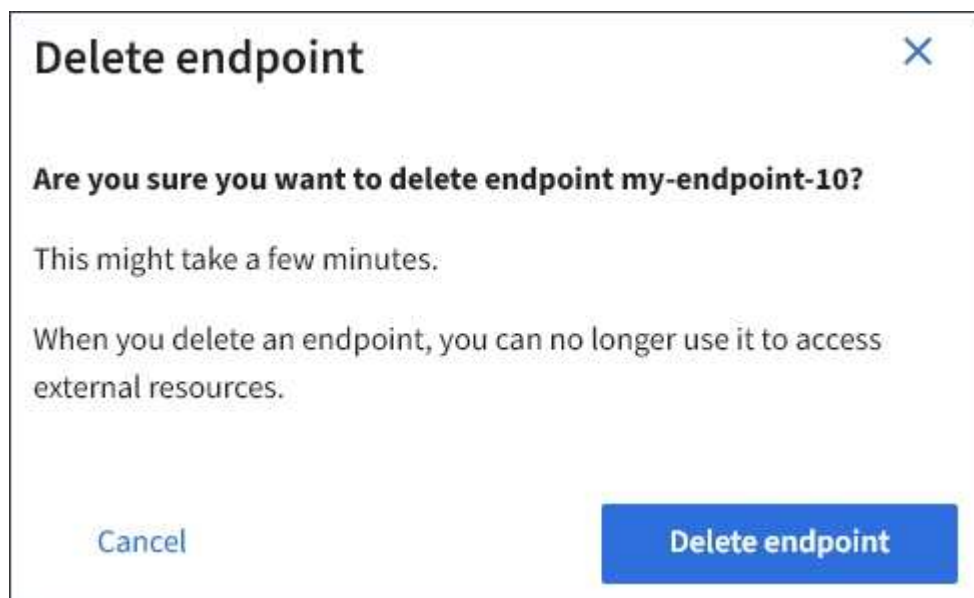
2. Cochez la case correspondant à chaque point final à supprimer.



Si vous supprimez un noeud final de services de plate-forme en cours d'utilisation, le service de plate-forme associé sera désactivé pour tous les compartiments qui utilisent le noeud final. Toutes les demandes qui n'ont pas encore été traitées seront supprimées. Toutes les nouvelles demandes seront toujours générées jusqu'à ce que vous modifiez la configuration de compartiment pour ne plus référencer l'URN supprimé. StorageGRID signale ces demandes comme des erreurs irrécupérables.

3. Sélectionnez **actions** > **Supprimer le point final**.

Un message de confirmation s'affiche.




4. Sélectionnez **Supprimer le point final**.

Dépanner les erreurs de point final des services de plate-forme

Si une erreur se produit lorsque StorageGRID tente de communiquer avec un noeud final de services de plate-forme, un message s'affiche sur le tableau de bord. Sur la page noeuds finaux des services de plate-forme, la colonne dernière erreur indique il y a combien de temps l'erreur s'est produite. Aucune erreur ne s'affiche si les autorisations associées aux informations d'identification d'un noeud final sont incorrectes.


Déterminez si l'erreur s'est produite

Si des erreurs de noeud final de services de plateforme se sont produites au cours des 7 derniers jours, le tableau de bord du gestionnaire de locataires affiche un message d'alerte. Vous pouvez accéder à la page noeuds finaux des services de plate-forme pour obtenir plus de détails sur l'erreur.


 One or more endpoints have experienced an error and might not be functioning properly. Go to the [Endpoints](#) page to view the error details. The last error occurred 2 hours ago.

La même erreur qui s'affiche sur le tableau de bord s'affiche également en haut de la page noeuds finaux Platform Services. Pour afficher un message d'erreur plus détaillé :

Étapes

1. Dans la liste des noeuds finaux, sélectionnez le noeud final qui contient l'erreur.
2. Sur la page des détails du noeud final, sélectionnez **connexion**. Cet onglet affiche uniquement l'erreur la plus récente pour un noeud final et indique il y a combien de temps l'erreur s'est produite. Erreurs incluant l'icône X rouge  s'est produit au cours des 7 derniers jours.

Overview ^

Display name:	my-endpoint-2 
Type:	Search
URI:	http://10.96.104.30:9200
URN:	urn:sgws:es:::mydomain/sveloso/_doc

Connection


Configuration

Verify connection

Some errors might continue to appear after they are resolved. To see if an error is current or to force the removal of a resolved error, select **Test connection**.

Test connection

Last error details

 2 hours ago

Endpoint failure: Endpont has an AWS failure: RequestError: send request failed; caused by: url.Error; caused by: net:OpError; caused by: os.SyscallError (logID: 143H5UDUUKMGDRWJ)

Vérifiez si l'erreur est toujours à jour

Certaines erreurs peuvent continuer à s'afficher dans la colonne **dernière erreur**, même après leur résolution. Pour voir si une erreur est active ou pour forcer la suppression d'une erreur résolue du tableau :

Étapes

1. Sélectionnez l'extrémité.

La page des détails du point final s'affiche.

2. Sélectionnez **connexion** > **Tester la connexion**.

La sélection de **Test Connection** permet à StorageGRID de valider l'existence du noeud final des services de plate-forme et de l'atteindre avec les informations d'identification actuelles. La connexion au noeud final est validée à partir d'un nœud sur chaque site.

Résoudre les erreurs de point final

Vous pouvez utiliser le message **dernière erreur** sur la page des détails du noeud final pour déterminer ce qui est à l'origine de l'erreur. Certaines erreurs peuvent vous obliger à modifier le noeud final pour résoudre le

25

problème. Par exemple, une erreur CloudMirroring peut se produire si StorageGRID ne parvient pas à accéder au compartiment S3 de destination, car il ne dispose pas des autorisations d'accès correctes ou si la clé d'accès a expiré. Le message est "les informations d'identification du noeud final ou l'accès à la destination doivent être mis à jour" et les détails sont "AccessDenied" ou "InvalidAccessKeyId".

Si vous devez modifier le noeud final pour résoudre une erreur, la sélection de **Test et enregistrer les modifications** fait que StorageGRID valide le noeud final mis à jour et confirme qu'il peut être atteint avec les informations d'identification actuelles. La connexion au noeud final est validée à partir d'un noeud sur chaque site.

Étapes

1. Sélectionnez l'extrémité.
2. Sur la page des détails du noeud final, sélectionnez **Configuration**.
3. Modifiez la configuration de point final selon vos besoins.
4. Sélectionnez **connexion > Tester la connexion**.

Identifiants de point de terminaison avec autorisations insuffisantes

Lorsque StorageGRID valide un terminal de services de plateforme, il confirme que les identifiants du terminal peuvent être utilisés pour contacter la ressource de destination et il vérifie les autorisations de base. Cependant, StorageGRID ne valide pas toutes les autorisations requises pour certaines opérations de services de plateforme. Pour cette raison, si vous recevez une erreur lors de la tentative d'utilisation d'un service de plate-forme (tel que « 403 interdit »), vérifiez les autorisations associées aux informations d'identification du noeud final.

Informations associées

- ["Administration de StorageGRID ; dépannage des services de plate-forme"](#)
- ["Créer un terminal de services de plate-forme"](#)
- ["Tester la connexion pour le point final des services de plate-forme"](#)
- ["Modifier le point final des services de plate-forme"](#)

Configurez la réplication CloudMirror

Le "[Service de réplication CloudMirror](#)" Est l'un des trois services de plateforme StorageGRID. Vous pouvez utiliser la réplication CloudMirror pour répliquer automatiquement les objets dans un compartiment S3 externe.

Avant de commencer

- Les services de plateforme ont été activés pour votre compte de locataire par un administrateur StorageGRID.
- Vous avez déjà créé un compartiment qui servira de source de réplication.
- Le noeud final que vous prévoyez d'utiliser comme destination pour la réplication CloudMirror existe déjà, et vous avez son URN.
- Vous appartenez à un groupe d'utilisateurs qui possède le "[Gérez tous les compartiments ou l'autorisation d'accès racine](#)". Ces autorisations remplacent les paramètres d'autorisation des stratégies de groupe ou de compartiment lors de la configuration du compartiment à l'aide du Gestionnaire de locataires.

Description de la tâche

La réplication CloudMirror copie les objets à partir d'un compartiment source vers un compartiment de destination spécifié dans un terminal.



La réplication CloudMirror présente des similarités et des différences importantes avec la fonction de réplication multigrille. Pour en savoir plus, voir "[Comparez la réplication entre les grilles et la réplication CloudMirror](#)".

Pour activer la réplication CloudMirror pour un compartiment, vous devez créer et appliquer un XML de configuration de réplication de compartiment valide. Le XML de configuration de réplication doit utiliser l'URN d'un terminal de compartiment S3 pour chaque destination.



La réplication n'est pas prise en charge pour les compartiments source ou de destination lorsque le verrouillage d'objet S3 est activé.

Pour obtenir des informations générales sur la réplication de compartiment et la configuration de celle-ci, reportez-vous à la section "[Documentation d'Amazon simple Storage Service \(S3\) : réplication d'objets](#)". Pour plus d'informations sur la manière dont StorageGRID implémente GetBuckeReplication, DeleteBuckeReplication et PutBuckeReplication, reportez-vous au "[Opérations sur les compartiments](#)".

Si vous activez la réplication CloudMirror sur un compartiment qui contient des objets, les nouveaux objets ajoutés au compartiment sont répliqués, mais les objets existants du compartiment ne sont pas répliqués. Vous devez mettre à jour des objets existants pour déclencher la réplication.

Si vous spécifiez une classe de stockage dans le fichier XML de configuration de réplication, StorageGRID utilise cette classe lors des opérations sur le terminal S3 de destination. Le noeud final de destination doit également prendre en charge la classe de stockage spécifiée. Veillez à suivre les recommandations fournies par le fournisseur du système de destination.

Étapes

1. Activer la réplication pour le compartiment source :

Utilisez un éditeur de texte pour créer le XML de configuration de réplication requis pour activer la réplication, comme spécifié dans l'API de réplication S3. Lors de la configuration du XML :

- Notez que StorageGRID ne prend en charge que le V1 de la configuration de la réplication. Cela signifie que StorageGRID ne prend pas en charge l'utilisation de `Filter` 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 sur la configuration de la réplication.
- Utiliser l'URN d'un terminal du compartiment S3 comme destination.
- Vous pouvez éventuellement ajouter le `<StorageClass>` et spécifiez l'un des éléments suivants :
 - `STANDARD`: La classe de stockage par défaut. Si vous ne spécifiez pas de classe de stockage lors du téléchargement d'un objet, le `STANDARD` la classe de stockage est utilisée.
 - `STANDARD_IA`: (Standard - accès peu fréquent.) Utilisez cette classe de stockage pour les données auxquelles vous accédez moins fréquemment, mais qui exige toujours un accès rapide lorsque cela est nécessaire.
 - `REDUCED_REDUNDANCY`: Utilisez cette classe de stockage pour les données non stratégiques reproductibles qui peuvent être stockées avec moins de redondance que le `STANDARD` classe de stockage.
- Si vous spécifiez un `Role` Dans le XML de configuration, il sera ignoré. Cette valeur n'est pas utilisée par StorageGRID.

```
<ReplicationConfiguration>
  <Role></Role>
  <Rule>
    <Status>Enabled</Status>
    <Prefix>2020</Prefix>
    <Destination>
      <Bucket>urn:sgws:s3:::2017-records</Bucket>
      <StorageClass>STANDARD</StorageClass>
    </Destination>
  </Rule>
</ReplicationConfiguration>
```

2. Sélectionnez **Afficher les compartiments** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > compartiments**.
3. Sélectionnez le nom du compartiment source.

La page des détails du compartiment s'affiche.
4. Sélectionnez **Platform Services > Replication**.
5. Cochez la case **Activer la réplication**.
6. Collez le XML de configuration de réplication dans la zone de texte et sélectionnez **Enregistrer les modifications**.

Bucket options
Bucket access
Platform services

Replication
Disabled
▲

Enable the CloudMirror replication service to copy objects from a source bucket to a destination bucket that is specified in an endpoint.

- Platform services must be enabled for your tenant account by a StorageGRID administrator.
- You must have already configured an endpoint for each destination bucket.
- You must specify the URN of each endpoint in the replication configuration XML for the source bucket.

Enable replication

Clear

```

<ReplicationConfiguration>
  <Role></Role>
  <Rule>
    <Status>Enabled</Status>
    <Prefix>2020</Prefix>
    <Destination>
      <Bucket>urn:sgws:s3:::2017-records</Bucket>
      <StorageClass>STANDARD</StorageClass>
    </Destination>
  </Rule>
</ReplicationConfiguration>

```

Save changes



Les services de plateforme doivent être activés pour chaque compte de locataire par un administrateur StorageGRID à l'aide de Grid Manager ou de l'API de gestion du grid. Contactez votre administrateur StorageGRID si une erreur se produit lors de l'enregistrement du XML de configuration.

7. Vérifiez que la réplication est configurée correctement :

- a. Ajoutez un objet au compartiment source qui répond aux exigences de réplication telles que spécifiées dans la configuration de la réplication.

Dans l'exemple présenté précédemment, les objets qui correspondent au préfixe « 2020 » sont répliqués.

b. Confirmer que l'objet a été répliqué vers le compartiment de destination.

Pour les objets de petite taille, la réplication s'effectue rapidement.

Informations associées

["Créer un terminal de services de plate-forme"](#)

Configurer les notifications d'événements

Le service de notifications est l'un des trois services de plate-forme StorageGRID. Vous pouvez activer les notifications d'un compartiment pour envoyer des informations sur les événements spécifiés à un cluster ou un service Kafka de destination qui prend en charge AWS simple notification Service (Amazon SNS).

Avant de commencer

- Les services de plateforme ont été activés pour votre compte de locataire par un administrateur StorageGRID.
- Vous avez déjà créé un compartiment qui sert de source de notifications.
- Le noeud final que vous avez l'intention d'utiliser comme destination pour les notifications d'événements existe déjà, et vous avez son URN.
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Gérez tous les compartiments ou l'autorisation d'accès racine"](#). Ces autorisations remplacent les paramètres d'autorisation des stratégies de groupe ou de compartiment lors de la configuration du compartiment à l'aide du Gestionnaire de locataires.

Description de la tâche

Après la configuration des notifications d'événements, chaque fois qu'un événement spécifié se produit pour un objet dans le compartiment source, une notification est générée et envoyée à la rubrique Amazon SNS ou Kafka utilisée comme terminal de destination. Pour activer les notifications pour un compartiment, vous devez créer et appliquer un XML de configuration de notification valide. Le XML de configuration de notification doit utiliser l'URN d'un terminal de notification d'événement pour chaque destination.

Pour obtenir des informations générales sur les notifications d'événements et leur configuration, consultez la documentation Amazon. Pour plus d'informations sur l'implémentation de l'API de configuration des notifications du compartiment S3 par StorageGRID, reportez-vous au ["Instructions d'implémentation des applications client S3"](#).

Si vous activez les notifications d'événements pour un compartiment contenant des objets, les notifications sont envoyées uniquement pour les actions qui sont effectuées après l'enregistrement de la configuration de notification.

Étapes

1. Activer les notifications pour le compartiment source :
 - Utilisez un éditeur de texte pour créer le XML de configuration de notification requis pour activer les notifications d'événement, comme spécifié dans l'API de notification S3.
 - Lors de la configuration du XML, utilisez l'URN d'un terminal de notification d'événements comme sujet de destination.


```
<NotificationConfiguration>
  <TopicConfiguration>
    <Id>Image-created</Id>
    <Filter>
      <S3Key>
        <FilterRule>
          <Name>prefix</Name>
          <Value>images/</Value>
        </FilterRule>
      </S3Key>
    </Filter>
    <Topic>arn:aws:sns:us-east-1:050340950352:sgws-topic</Topic>
    <Event>s3:ObjectCreated:*</Event>
  </TopicConfiguration>
</NotificationConfiguration>
```

2. Dans le Gestionnaire de locataires, sélectionnez **STORAGE (S3) > seaux**.
3. Sélectionnez le nom du compartiment source.

La page des détails du compartiment s'affiche.

4. Sélectionnez **Platform Services > Event Notifications**.
5. Cochez la case **Activer les notifications d'événements**.
6. Collez le XML de configuration de notification dans la zone de texte, puis sélectionnez **Enregistrer les modifications**.

Bucket options
Bucket access
Platform services
S3 Console

Replication
Disabled
▼

Event notifications
Disabled
▲

Enable the event notification service for an S3 bucket if you want StorageGRID to send notifications about specified events to a destination Amazon Simple Notification Service (SNS) or a destination Apache Kafka cluster.

- Platform services must be enabled for your tenant account by a StorageGRID administrator.
- You must have already configured an endpoint for the destination of event notifications.
- You must specify the URN of that endpoint in the notification configuration XML for the source bucket.

Enable event notifications

Clear

```

<NotificationConfiguration>
  <TopicConfiguration>
    <Id>Image-created</Id>
    <Filter>
      <S3Key>
        <FilterRule>
          <Name>prefix</Name>
          <Value>images</Value>
        </FilterRule>
      </S3Key>
    </Filter>

```

Save changes



Les services de plateforme doivent être activés pour chaque compte de locataire par un administrateur StorageGRID à l'aide de Grid Manager ou de l'API de gestion du grid. Contactez votre administrateur StorageGRID si une erreur se produit lors de l'enregistrement du XML de configuration.

7. Vérifiez que les notifications d'événements sont correctement configurées :

- a. Exécutez une action sur un objet du compartiment source qui répond aux exigences de déclenchement d'une notification telles qu'elles sont configurées dans le fichier XML de configuration.

Dans l'exemple, une notification d'événement est envoyée chaque fois qu'un objet est créé avec le `images/` préfixe.

b. Vérifiez qu'une notification a été envoyée à la rubrique Amazon SNS ou Kafka de destination.

Par exemple, si votre sujet de destination est hébergé sur Amazon SNS, vous pouvez configurer le service pour qu'il vous envoie un e-mail lorsque la notification est remise.

```
{
  "Records": [
    {
      "eventVersion": "2.0",
      "eventSource": "sgws:s3",
      "eventTime": "2017-08-08T23:52:38Z",
      "eventName": "ObjectCreated:Put",
      "userIdentity": {
        "principalId": "11111111111111111111"
      },
      "requestParameters": {
        "sourceIPAddress": "193.51.100.20"
      },
      "responseElements": {
        "x-amz-request-id": "122047343"
      },
      "s3": {
        "s3SchemaVersion": "1.0",
        "configurationId": "Image-created",
        "bucket": {
          "name": "test1",
          "ownerIdentity": {
            "principalId": "11111111111111111111"
          },
          "arn": "arn:sgws:s3:::test1"
        },
        "object": {
          "key": "images/cat.jpg",
          "size": 0,
          "eTag": "d41d8cd98f00b204e9800998ecf8427e",
          "sequencer": "14D90402421461C7"
        }
      }
    }
  ]
}
```

+ Si la notification est reçue dans la rubrique de destination, vous avez configuré votre compartiment source pour les notifications StorageGRID.

Informations associées

["Description des notifications pour les compartiments"](#)

["UTILISEZ L'API REST S3"](#)

["Créer un terminal de services de plate-forme"](#)

Utilisez le service d'intégration de la recherche

Le service d'intégration de la recherche est l'un des trois services de plate-forme StorageGRID. Vous pouvez activer ce service pour envoyer des métadonnées d'objet à un index de recherche de destination chaque fois qu'un objet est créé ou supprimé, ou que ses métadonnées ou balises sont mises à jour.

Vous pouvez configurer l'intégration de la recherche à l'aide du Gestionnaire de locataires pour appliquer un code XML de configuration StorageGRID personnalisé à un compartiment.



Comme le service d'intégration de recherche entraîne l'envoi des métadonnées d'objet vers une destination, son XML de configuration est appelé *metadata notification configuration XML*. Ce XML de configuration est différent de la configuration de *notification XML* utilisée pour activer les notifications d'événements.

Voir la ["Instructions d'implémentation des applications client S3"](#) Pour plus d'informations sur les opérations d'API REST personnalisées suivantes de StorageGRID S3 :

- SUPPRIMEZ la configuration de notification des métadonnées de compartiment
- CONFIGURATION DES notifications de métadonnées de compartiment
- CONFIGURATION de notification des métadonnées de compartiment

Informations associées

["XML de configuration pour l'intégration de la recherche"](#)

["Métadonnées d'objet incluses dans les notifications de métadonnées"](#)

["JSON généré par le service d'intégration de la recherche"](#)

["Configurez le service d'intégration de la recherche"](#)

["UTILISEZ L'API REST S3"](#)

XML de configuration pour l'intégration de la recherche

Le service d'intégration de recherche est configuré à l'aide d'un ensemble de règles contenues dans `<MetadataNotificationConfiguration>` et `</MetadataNotificationConfiguration>` balises. Chaque règle spécifie les objets auxquels la règle s'applique, et la destination vers laquelle StorageGRID doit envoyer les métadonnées de ces objets.

Les objets peuvent être filtrés sur le préfixe du nom de l'objet. Par exemple, vous pouvez envoyer les métadonnées pour les objets avec le préfixe `images` à une destination et aux métadonnées pour les objets avec le préfixe `videos` à un autre. Les configurations avec des préfixes qui se chevauchent ne sont pas

valides et sont rejetées lorsqu'elles sont soumises. Par exemple, une configuration qui inclut une règle pour les objets avec le préfixe `test` et une seconde règle pour les objets avec le préfixe `test2` n'est pas autorisé.

Les destinations doivent être spécifiées à l'aide de l'URN d'un terminal StorageGRID créé pour le service d'intégration de la recherche. Ces terminaux font référence à un index et à un type définis dans un cluster Elasticsearch.

```
<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 <code>MetadaNotificationConfiguration</code>	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 préfixes qui se chevauchent sont rejetées. Inclus dans l'élément <code>MetadaNotificationConfiguration</code> .	Oui.
ID	Identifiant unique de la règle. Inclus dans l'élément règle.	Non

Nom	Description	Obligatoire
État	L'état peut être « activé » ou « désactivé ». Aucune action n'est prise pour les règles désactivées. Inclus dans l'élément règle.	Oui.
Préfixe	Les objets qui correspondent au préfixe sont affectés par la règle et leurs métadonnées sont envoyées à la destination spécifiée. Pour faire correspondre tous les objets, spécifiez un préfixe vide. Inclus dans l'élément règle.	Oui.
Destination	Balise de conteneur pour la destination d'une règle. Inclus dans l'élément règle.	Oui.
Urne	URN de la destination où les métadonnées d'objet sont envoyées. Doit être l'URN d'un terminal StorageGRID avec les propriétés suivantes : <ul style="list-style-type: none"> • es doit être le troisième élément. • L'URN doit se terminer par l'index et le type où les métadonnées sont stockées, sous la forme domain-name/myindex/mytype. <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"> • arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype • urn:mysite:es:::mydomain/myindex/mytype <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.

Utilisez l'exemple de XML de configuration de notification de métadonnées pour apprendre à construire votre propre XML.

Configuration de notification des métadonnées qui s'applique à tous les objets

Dans cet exemple, les métadonnées d'objet de tous les objets sont envoyées vers la même destination.

```

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

```

Configuration des notifications de métadonnées avec deux règles

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

```

<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>

```

Informations associées

["UTILISEZ L'API REST S3"](#)

["Métadonnées d'objet incluses dans les notifications de métadonnées"](#)

["JSON généré par le service d'intégration de la recherche"](#)

["Configurez le service d'intégration de la recherche"](#)

Configurer le service d'intégration de la recherche

Le service d'intégration de recherche envoie des métadonnées d'objet à un index de recherche de destination chaque fois qu'un objet est créé ou supprimé, ou que ses métadonnées ou balises sont mises à jour.

Avant de commencer

- Les services de plateforme ont été activés pour votre compte de locataire par un administrateur StorageGRID.
- Vous avez déjà créé un compartiment S3 dont vous souhaitez indexer le contenu.
- Le noeud final que vous avez l'intention d'utiliser comme destination pour le service d'intégration de recherche existe déjà, et vous avez son URN.
- Vous appartenez à un groupe d'utilisateurs qui possède le "[Gérez tous les compartiments ou l'autorisation d'accès racine](#)". Ces autorisations remplacent les paramètres d'autorisation des stratégies de groupe ou de compartiment lors de la configuration du compartiment à l'aide du Gestionnaire de locataires.

Description de la tâche

Une fois que vous avez configuré le service d'intégration de recherche pour un compartiment source, la création d'un objet ou la mise à jour des métadonnées ou des balises d'un objet déclenche l'envoi des métadonnées d'objet vers le terminal de destination. Si vous activez le service d'intégration de recherche pour un compartiment qui contient déjà des objets, les notifications de métadonnées ne sont pas automatiquement envoyées pour les objets existants. Vous devez mettre à jour ces objets existants pour vous assurer que leurs métadonnées sont ajoutées à l'index de recherche de destination.

Étapes

1. Utilisez un éditeur de texte pour créer le XML de notification de métadonnées requis pour activer l'intégration de la recherche.
 - Voir les informations sur le XML de configuration pour l'intégration de la recherche.
 - Lors de la configuration du XML, utilisez l'URN d'un noeud final d'intégration de recherche comme destination.

```
<MetadataNotificationConfiguration>
  <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-
1:1111111111111111:domain/mydomain/myindex/mytype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

2. Dans le Gestionnaire de locataires, sélectionnez **STORAGE (S3) > seaux**.
3. Sélectionnez le nom du compartiment source.

La page des détails du compartiment s'affiche.

- Sélectionnez **Platform Services > Search Integration**
- Cochez la case **Activer l'intégration de la recherche**.
- Collez la configuration de notification de métadonnées dans la zone de texte, puis sélectionnez **Enregistrer les modifications**.

The screenshot shows the 'Platform services' tab in a configuration interface. It features three sections: 'Replication' (Disabled), 'Event notifications' (Disabled), and 'Search integration' (Disabled). The 'Search integration' section is expanded, showing instructions and a list of requirements. A checkbox labeled 'Enable search integration' is checked. Below this is a text area containing XML configuration code for metadata notifications, with a 'Clear' button to its right. A 'Save changes' button is located at the bottom right of the configuration area.

Replication Disabled

Event notifications Disabled

Search integration Disabled

Enable the search integration service to send object metadata to a destination search index whenever an object is created, deleted, or its metadata or tags are updated.

- Platform services must be enabled for your tenant account by a StorageGRID administrator.
- You must have already configured an endpoint for the search integration service.
- You must specify the URN of that endpoint in the search integration configuration XML for the bucket you want to index.

Enable search integration

Clear

```
<MetadataNotificationConfiguration>
  <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-1:111111111111:domain/mydomain/myindex/mytype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

Save changes



Les services de plateforme doivent être activés pour chaque compte de locataire par un administrateur StorageGRID à l'aide de l'API Grid Manager ou de gestion. Contactez votre administrateur StorageGRID si une erreur se produit lors de l'enregistrement du XML de configuration.

- Vérifiez que le service d'intégration de la recherche est configuré correctement :

- a. Ajoutez un objet au compartiment source qui répond aux exigences relatives au déclenchement d'une notification de métadonnées comme spécifié dans le XML de configuration.

Dans l'exemple présenté précédemment, tous les objets ajoutés au compartiment déclenchent une notification de métadonnées.

- b. Vérifiez qu'un document JSON contenant les métadonnées et les balises de l'objet a été ajouté à l'index de recherche spécifié dans le noeud final.

Une fois que vous avez terminé

Si nécessaire, vous pouvez désactiver l'intégration de la recherche pour un compartiment à l'aide de l'une des méthodes suivantes :

- Sélectionnez **STORAGE (S3) > Buckets** et décochez la case **Enable search Integration**.
- Si vous utilisez directement l'API S3, utilisez une demande de notification DE suppression des métadonnées du compartiment. Pour plus d'informations sur l'implémentation des applications client S3, reportez-vous aux instructions.

Informations associées

["Comprendre le service d'intégration de la recherche"](#)

["XML de configuration pour l'intégration de la recherche"](#)

["UTILISEZ L'API REST S3"](#)

["Créer un terminal de services de plate-forme"](#)

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 peut être généré lorsqu'un objet doté de la clé est associé `SGWS/Tagging.txt` est créé dans un compartiment nommé `test`. Le `test` le compartiment n'est pas multiversion `versionId` l'étiquette est vide.

```

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

```

Métadonnées d'objet incluses dans les notifications de métadonnées

Le tableau répertorie tous les champs inclus dans le document JSON 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 et description de l'élément
Informations sur les compartiments et les objets	bucket: Nom du compartiment
key: Nom de la clé d'objet	versionID: Version d'objet, pour les objets dans les compartiments multiversion
region: Région godet, par exemple us-east-1	Métadonnées de système
size: Taille de l'objet (en octets) visible par un client HTTP	md5: Hachage d'objet
Métadonnées d'utilisateur	metadata: Toutes les métadonnées utilisateur de l'objet, en tant que paires clé-valeur key:value
Étiquettes	tags: Toutes les balises d'objet définies pour l'objet, en tant que paires clé-valeur key:value



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 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 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.