



Utiliser l'API REST de Swift (obsolète)

StorageGRID 11.8

NetApp
March 19, 2024

Sommaire

- Utiliser l'API REST de Swift (obsolète) 1
 - Utilisez l'API REST de Swift : présentation 1
 - Test de la configuration de l'API REST Swift 4
 - Opérations prises en charge par l'API REST Swift 5
 - Opérations de l'API REST StorageGRID Swift 18
 - Les opérations Swift sont suivies dans les journaux d'audit 22

Utiliser l'API REST de Swift (obsolète)

Utilisez l'API REST de Swift : présentation

Les applications client peuvent utiliser l'API OpenStack Swift pour interagir avec le système StorageGRID.



La prise en charge des applications du client Swift a été obsolète et sera supprimée dans une prochaine version.

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

Élément	Version
Spécification SWIFT	OpenStack Swift Object Storage API v1 depuis novembre 2015
HTTP	1.1 Pour plus d'informations sur HTTP, consultez le document HTTP/1.1 (RFC 7230-35). Remarque: StorageGRID ne prend pas en charge HTTP/1.1 pipeline.

Informations associées

["OpenStack : API de stockage objet"](#)

Historique de la prise en charge de l'API Swift dans StorageGRID

Notez que des modifications ont été apportées à la prise en charge du système StorageGRID pour l'API REST Swift.

Relâchez	Commentaires
11.8	
11.7	La prise en charge des applications du client Swift a été obsolète et sera supprimée dans une prochaine version.
11.6	Modifications éditoriales mineures.
11.5	Suppression de la cohérence faible. La cohérence disponible sera utilisée à la place.
11.4	Ajout de la prise en charge de TLS 1.3. Ajout d'une description des relations entre ILM et cohérence.

Relâchez	Commentaires
11.3	Les opérations PUT mises à jour décrivent l'impact des règles ILM qui utilisent le placement synchrone à l'ingestion (options équilibrées et strictes pour le comportement d'ingestion). Ajout d'une description des connexions client qui utilisent des nœuds finaux d'équilibreur de charge ou des groupes de haute disponibilité. Les chiffrements TLS 1.1 ne sont plus pris en charge.
11.2	Modifications rédactionnelles mineures apportées au document
11.1	Ajout de la prise en charge de l'utilisation des connexions client HTTP pour Swift aux nœuds de la grille. Mise à jour des définitions des valeurs de cohérence.
11.0	Ajout de la prise en charge de 1,000 conteneurs pour chaque compte locataire.
10.3	Mises à jour administratives et corrections du document. Suppression des sections pour la configuration des certificats de serveur personnalisés.
10.2	Prise en charge initiale de l'API Swift par le système StorageGRID. La version actuellement prise en charge est l'API de stockage objet OpenStack Swift v1.

Comment StorageGRID implémente l'API REST Swift

Une application client peut utiliser les appels de l'API REST Swift pour se connecter aux nœuds de stockage et aux nœuds de passerelle afin de créer des conteneurs et de stocker et récupérer des objets. Les applications orientées services développées pour OpenStack Swift peuvent ainsi se connecter au stockage objet sur site fourni par le système StorageGRID.

Gestion des objets Swift

Une fois les objets Swift ingérés dans le système StorageGRID, ils sont gérés par les règles de gestion du cycle de vie des informations (ILM) des politiques ILM actives. "[Règles ILM](#)" et "[Règles ILM](#)" Création et distribution de copies des données d'objet par StorageGRID et gestion de ces copies au fil du temps Par exemple, une règle ILM peut s'appliquer aux objets de conteneurs Swift spécifiques et peut spécifier que plusieurs copies d'objets seront enregistrées dans plusieurs data centers pendant un certain nombre d'années.

Contactez votre consultant en services professionnels NetApp ou votre administrateur StorageGRID si vous avez besoin de comprendre en quoi les règles et règles ILM de la grille affecteront les objets de votre compte de locataire Swift.

Requêtes des clients en conflit

Les demandes contradictoires des clients, telles que deux clients qui écrivent sur la même clé, sont résolues sur une base de « derniers-victoires ». Le moment auquel l'évaluation « derniers-victoires » est basé sur la date à laquelle le système StorageGRID remplit une demande donnée et non sur la date à laquelle les clients Swift entament une opération.

Garanties et contrôles de cohérence

Par défaut, StorageGRID fournit une cohérence de lecture après écriture pour les objets nouvellement créés et une cohérence éventuelle pour les mises à jour et les OPÉRATIONS HEAD d'objet. Toutes "OBTENEZ" suite à une exécution réussie "EN" pourra lire les données nouvellement écrites. Les écrasements d'objets existants, les mises à jour de métadonnées et les suppressions sont cohérents. La propagation des écrasements ne prend généralement que quelques secondes ou minutes, mais peut prendre jusqu'à 15 jours.

StorageGRID vous permet également de contrôler la cohérence par conteneur. Les valeurs de cohérence assurent un équilibre entre la disponibilité des objets et la cohérence de ces objets sur différents nœuds et sites de stockage, selon les besoins de votre application.

Recommandations pour l'implémentation de l'API REST Swift

Suivez ces recommandations lors de la mise en œuvre de l'API REST Swift pour une utilisation avec StorageGRID.

Recommandations pour les têtes à des objets inexistantes

Si votre application vérifie régulièrement si un objet existe dans un chemin où vous ne vous attendez pas à ce que l'objet existe réellement, vous devez utiliser la cohérence « disponible ». Par exemple, vous devez utiliser la cohérence « disponible » si votre application effectue une opération de TÊTE À un emplacement avant d'effectuer une opération de MISE À cet emplacement.

Sinon, si l'opération HEAD ne trouve pas l'objet, vous pouvez recevoir un nombre élevé de 500 erreurs de serveur interne si un ou plusieurs nœuds de stockage ne sont pas disponibles.

Vous pouvez définir la cohérence « disponible » pour chaque conteneur à l'aide du "REQUÊTE de cohérence du conteneur". En effet, vous définissez la cohérence « disponible » pour chaque conteneur à l'aide de "DEMANDE DE cohérence du conteneur".

Recommandations pour les noms d'objet

Pour les conteneurs créés dans StorageGRID 11.4 ou version ultérieure, il n'est plus nécessaire de limiter les noms d'objet afin de respecter les bonnes pratiques de performance. Par exemple, vous pouvez maintenant utiliser des valeurs aléatoires pour les quatre premiers caractères des noms d'objets.

Pour les conteneurs créés dans des versions antérieures à StorageGRID 11.4, suivez ces recommandations pour les noms d'objet :

- Vous ne devez pas utiliser de valeurs aléatoires comme les quatre premiers caractères des noms d'objets. Cela contraste avec l'ancienne recommandation AWS pour les préfixes de noms. Au lieu de cela, vous devez utiliser des préfixes non aléatoires et non uniques, tels que `image`.
- Si vous suivez l'ancienne recommandation AWS pour utiliser des caractères aléatoires et uniques dans les préfixes de noms, vous devez préfixer les noms d'objets avec un nom de répertoire. C'est-à-dire, utilisez le format suivant :

```
mycontainer/mydir/f8e3-image3132.jpg
```

Au lieu de ce format :

```
mycontainer/f8e3-image3132.jpg
```

Recommandations pour les « lectures de plage »

Si le "[option globale pour compresser les objets stockés](#)" Est activé, les applications clientes Swift doivent éviter d'effectuer des opérations GET Object qui spécifient une plage d'octets à renvoyer. Ces opérations de « lecture de plage » sont inefficaces car StorageGRID doit décompresser efficacement les objets pour accéder aux octets demandés. LES opérations GET Object qui demandent une petite plage d'octets provenant d'un objet très volumineux sont particulièrement inefficaces. Par exemple, il est très inefficace de lire une plage de 10 Mo à partir d'un objet compressé de 50 Go.

Si les plages sont lues à partir d'objets compressés, les demandes client peuvent être en attente.



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

Test de la configuration de l'API REST Swift

Vous pouvez utiliser l'interface de ligne de commande Swift pour tester votre connexion au système StorageGRID et vérifier que vous pouvez lire et écrire des objets.

Avant de commencer

- Vous avez téléchargé et installé le client de ligne de commande Swift : "[SwiftStack: python-swftclient](#)"
- En option, vous avez "[créé un terminal d'équilibrage de charge](#)". Sinon, vous connaissez l'adresse IP du nœud de stockage auquel vous souhaitez vous connecter et le numéro de port à utiliser. Voir "[Adresses IP et ports pour les connexions client](#)".
- Vous avez "[Compte de locataire Swift créé](#)".
- Vous vous êtes connecté au compte de tenant et avez créé au moins un groupe et un utilisateur. Voir "[Créez des groupes pour un locataire Swift](#)".



Les utilisateurs locataires Swift doivent disposer de l'autorisation Administrateur Group pour s'authentifier auprès de l'API REST Swift.

Description de la tâche

Si vous n'avez pas configuré la sécurité, vous devez ajouter le `--insecure` marqueur pour chacune de ces commandes.

Étapes

1. Interrogez l'URL d'information pour votre déploiement StorageGRID Swift :

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/info
capabilities
```

Cela suffit pour tester le fonctionnement de votre déploiement Swift. Pour tester davantage la configuration des comptes en stockant un objet, passez aux étapes supplémentaires.

2. Placer un objet dans le conteneur :

```
touch test_object
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
upload test_container test_object
--object-name test_object
```

3. Procurez-vous le conteneur pour vérifier l'objet :

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
list test_container
```

4. Supprimez l'objet :

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
delete test_container test_object
```

5. Supprimez le conteneur :

```
swift
-U `<_Tenant_Account_ID:Account_User_Name_>`
-K `<_User_Password_>`
-A `https://<_FQDN_ | _IP_>:<_Port_>/auth/v1.0`
delete test_container
```

Opérations prises en charge par l'API REST Swift

Le système StorageGRID prend en charge la plupart des opérations dans l'API OpenStack Swift. Avant d'intégrer des clients de l'API REST Swift avec StorageGRID, consultez les informations d'implémentation pour les opérations des comptes, des

conteneurs et des objets.

Opérations prises en charge par StorageGRID

Les opérations de l'API Swift suivantes sont prises en charge :

- "Opérations sur le compte"
- "Opérations sur les conteneurs"
- "Opérations sur l'objet"

En-têtes de réponse courants pour toutes les opérations

Le système StorageGRID implémente toutes les en-têtes courants pour les opérations prises en charge, comme défini par l'API de stockage objet OpenStack Swift v1.

Informations associées

["OpenStack : API de stockage objet"](#)

Terminaux API Swift pris en charge

StorageGRID prend en charge les points de terminaison de l'API Swift suivants : l'URL info, l'URL d'authentification et l'URL de stockage.

URL info

Vous pouvez déterminer les capacités et les limites de l'implémentation de StorageGRID Swift en émettant une demande GET à l'URL de base Swift avec le chemin /info.

```
https://FQDN | Node IP:Swift Port/info/
```

Dans la demande :

- *FQDN* est le nom de domaine complet.
- *Node IP* Est l'adresse IP du nœud de stockage ou du nœud de passerelle sur le réseau StorageGRID.
- *Swift Port* Est le numéro de port utilisé pour les connexions API Swift sur le nœud de stockage ou le nœud de passerelle.

Par exemple, l'URL d'information suivante demande des informations à un nœud de stockage avec l'adresse IP 10.99.106.103 et le port 18083.

```
https://10.99.106.103:18083/info/
```

La réponse inclut les fonctionnalités de l'implémentation Swift sous forme de dictionnaire JSON. Un outil client peut analyser la réponse JSON pour déterminer les fonctionnalités de l'implémentation et les utiliser comme contraintes pour les opérations de stockage ultérieures.

La mise en œuvre de StorageGRID de Swift permet un accès non authentifié à l'URL info.

URL d'authentification

Un client peut utiliser l'URL d'authentification Swift pour s'authentifier en tant qu'utilisateur de compte de locataire.

```
https://FQDN | Node IP:Swift Port/auth/v1.0/
```

Vous devez fournir l'ID de compte de tenant, le nom d'utilisateur et le mot de passe comme paramètres dans le X-Auth-User et X-Auth-Key en-têtes de demande, comme suit :

```
X-Auth-User: Tenant_Account_ID:Username
```

```
X-Auth-Key: Password
```

Dans les en-têtes de demande :

- *Tenant_Account_ID* Est l'ID de compte attribué par StorageGRID lors de la création du locataire Swift. Il s'agit du même ID de compte de locataire que celui utilisé sur la page de connexion du Gestionnaire de locataires.
- *Username* Est le nom d'un utilisateur locataire qui a été créé dans le Gestionnaire de tenant. Cet utilisateur doit appartenir à un groupe disposant de l'autorisation Administrateur Swift. L'utilisateur root du locataire ne peut pas être configuré pour utiliser l'API REST Swift.

Si la fédération des identités est activée pour le compte de tenant, indiquez le nom d'utilisateur et le mot de passe de l'utilisateur fédéré à partir du serveur LDAP. Vous pouvez également indiquer le nom de domaine de l'utilisateur LDAP. Par exemple :

```
X-Auth-User: Tenant_Account_ID:Username@Domain_Name
```

- *Password* est le mot de passe de l'utilisateur tenant. Les mots de passe utilisateur sont créés et gérés dans le Gestionnaire de locataires.

La réponse à une demande d'authentification réussie renvoie une URL de stockage et un jeton d'authentification, comme suit :

```
X-Storage-Url: https://FQDN | Node_IP:Swift_Port/v1/Tenant_Account_ID
```

```
X-Auth-Token: token
```

```
X-Storage-Token: token
```

Par défaut, le jeton est valide pendant 24 heures à compter de l'heure de génération.

Des jetons sont générés pour un compte de locataire spécifique. Un jeton valide pour un compte n'autorise pas un utilisateur à accéder à un autre compte.

URL du stockage

Une application client peut émettre des appels de l'API REST Swift pour exécuter des opérations de compte, conteneur et objet prises en charge sur un nœud de passerelle ou un nœud de stockage. Les demandes de stockage sont adressées à l'URL de stockage renvoyée dans la réponse d'authentification. La demande doit également inclure l'en-tête X-Auth-Token et la valeur renvoyée par la demande d'autorisation.

```
https://FQDN | IP:Swift_Port/v1/Tenant_Account_ID
```

`[/container] [/object]`

`X-Auth-Token: token`

Certains en-têtes de réponse de stockage contenant des statistiques d'utilisation peuvent ne pas refléter les chiffres précis des objets récemment modifiés. L'affichage des nombres précis dans ces en-têtes peut prendre quelques minutes.

Les en-têtes de réponse suivants pour les opérations de compte et de conteneur sont des exemples de ceux qui contiennent des statistiques d'utilisation :

- `X-Account-Bytes-Used`
- `X-Account-Object-Count`
- `X-Container-Bytes-Used`
- `X-Container-Object-Count`

Informations associées

["Configurez les comptes et les connexions des locataires"](#)

["Opérations sur le compte"](#)

["Opérations sur les conteneurs"](#)

["Opérations sur l'objet"](#)

Opérations sur le compte

Les opérations de l'API Swift suivantes sont effectuées sur les comptes.

OBTENIR un compte

Cette opération récupère la liste de conteneurs associée aux statistiques d'utilisation du compte et du compte.

Le paramètre de demande suivant est requis :

- `Account`

L'en-tête de demande suivant est requis :

- `X-Auth-Token`

Les paramètres de requête pris en charge suivants sont facultatifs :

- `Delimiter`
- `End_marker`
- `Format`
- `Limit`
- `Marker`
- `Prefix`

Une exécution réussie renvoie les en-têtes suivants avec une réponse « HTTP/1.1 204 pas de contenu » si le compte est trouvé et n'a pas de conteneurs ou si la liste de conteneurs est vide ; ou une réponse « HTTP/1.1 200 OK » si le compte est trouvé et si la liste de conteneurs n'est pas vide :

- Accept-Ranges
- Content-Length
- Content-Type
- Date
- X-Account-Bytes-Used
- X-Account-Container-Count
- X-Account-Object-Count
- X-Timestamp
- X-Trans-Id

Compte PRINCIPAL

Cette opération récupère les informations et les statistiques du compte à partir d'un compte Swift.

Le paramètre de demande suivant est requis :

- Account

L'en-tête de demande suivant est requis :

- X-Auth-Token

Une exécution réussie renvoie les en-têtes suivants avec une réponse "HTTP/1.1 204 No Content" :

- Accept-Ranges
- Content-Length
- Date
- X-Account-Bytes-Used
- X-Account-Container-Count
- X-Account-Object-Count
- X-Timestamp
- X-Trans-Id

Informations associées

["Les opérations Swift sont suivies dans les journaux d'audit"](#)

Opérations sur les conteneurs

StorageGRID prend en charge un maximum de 1,000 conteneurs par compte Swift. Les opérations d'API Swift suivantes sont effectuées sur les conteneurs.

SUPPRIMER le conteneur

Cette opération supprime un conteneur vide d'un compte Swift dans un système StorageGRID.

Les paramètres de demande suivants sont requis :

- Account
- Container

L'en-tête de demande suivant est requis :

- X-Auth-Token

Une exécution réussie renvoie les en-têtes suivants avec une réponse "HTTP/1.1 204 No Content" :

- Content-Length
- Content-Type
- Date
- X-Trans-Id

CONTENEUR

Cette opération récupère la liste d'objets associée au conteneur, ainsi que les statistiques et métadonnées de conteneur dans un système StorageGRID.

Les paramètres de demande suivants sont requis :

- Account
- Container

L'en-tête de demande suivant est requis :

- X-Auth-Token

Les paramètres de requête pris en charge suivants sont facultatifs :

- Delimiter
- End_marker
- Format
- Limit
- Marker
- Path
- Prefix

Une exécution réussie renvoie les en-têtes suivants avec une réponse « HTTP/1.1 200 Success » ou « HTTP/1.1 204 No Content » :

- Accept-Ranges

- Content-Length
- Content-Type
- Date
- X-Container-Bytes-Used
- X-Container-Object-Count
- X-Timestamp
- X-Trans-Id

Conteneur DE TÊTE

Cette opération récupère les statistiques du conteneur et les métadonnées d'un système StorageGRID.

Les paramètres de demande suivants sont requis :

- Account
- Container

L'en-tête de demande suivant est requis :

- X-Auth-Token

Une exécution réussie renvoie les en-têtes suivants avec une réponse "HTTP/1.1 204 No Content" :

- Accept-Ranges
- Content-Length
- Date
- X-Container-Bytes-Used
- X-Container-Object-Count
- X-Timestamp
- X-Trans-Id

PLACER le conteneur

Cette opération crée un conteneur pour un compte dans un système StorageGRID.

Les paramètres de demande suivants sont requis :

- Account
- Container

L'en-tête de demande suivant est requis :

- X-Auth-Token

Une exécution réussie renvoie les en-têtes suivants avec une réponse « HTTP/1.1 201 created » ou «

HTTP/1.1 202 Accepted » (si le conteneur existe déjà sous ce compte) :

- Content-Length
- Date
- X-Timestamp
- X-Trans-Id

Un nom de conteneur doit être unique dans le namespace StorageGRID. Si le conteneur existe sous un autre compte, l'en-tête suivant est renvoyé : « HTTP/1.1 409 Conflict ».

Informations associées

["Surveiller et auditer les opérations"](#)

Opérations sur l'objet

Les opérations suivantes de l'API Swift sont effectuées sur des objets. Ces opérations peuvent être suivies dans ["Journal d'audit StorageGRID"](#).

SUPPRIMER l'objet

Cette opération supprime le contenu et les métadonnées d'un objet du système StorageGRID.

Les paramètres de demande suivants sont requis :

- Account
- Container
- Object

L'en-tête de demande suivant est requis :

- X-Auth-Token

Une exécution réussie renvoie les en-têtes de réponse suivants avec un HTTP/1.1 204 No Content réponse :

- Content-Length
- Content-Type
- Date
- X-Trans-Id

Lors du traitement d'une requête DE SUPPRESSION d'objet, StorageGRID tente de supprimer immédiatement toutes les copies de l'objet des emplacements stockés. En cas de succès, StorageGRID renvoie immédiatement une réponse au client. Si toutes les copies ne peuvent pas être supprimées dans les 30 secondes (par exemple, parce qu'un emplacement est temporairement indisponible), StorageGRID met les copies en file d'attente pour suppression et indique que le client a réussi.

Pour plus d'informations, voir ["Comment supprimer les objets"](#).

OBJET GET

Cette opération récupère le contenu de l'objet et obtient ses métadonnées depuis un système StorageGRID.

Les paramètres de demande suivants sont requis :

- Account
- Container
- Object

L'en-tête de demande suivant est requis :

- X-Auth-Token

Les en-têtes de demande suivants sont facultatifs :

- Accept-Encoding
- If-Match
- If-Modified-Since
- If-None-Match
- If-Unmodified-Since
- Range

Une exécution réussie renvoie les en-têtes suivants avec un HTTP/1.1 200 OK réponse :

- Accept-Ranges
- Content-Disposition, retourné seulement si Content-Disposition les métadonnées ont été définies
- Content-Encoding, retourné seulement si Content-Encoding les métadonnées ont été définies
- Content-Length
- Content-Type
- Date
- ETag
- Last-Modified
- X-Timestamp
- X-Trans-Id

Objet TÊTE

Cette opération récupère les métadonnées et les propriétés d'un objet ingéré à partir d'un système StorageGRID.

Les paramètres de demande suivants sont requis :

- Account
- Container
- Object

L'en-tête de demande suivant est requis :

- X-Auth-Token

Une exécution réussie renvoie les en-têtes suivants avec une réponse "HTTP/1.1 200 OK" :

- Accept-Ranges
- Content-Disposition, retourné seulement si Content-Disposition les métadonnées ont été définies
- Content-Encoding, retourné seulement si Content-Encoding les métadonnées ont été définies
- Content-Length
- Content-Type
- Date
- ETag
- Last-Modified
- X-Timestamp
- X-Trans-Id

PLACER l'objet

Cette opération crée un nouvel objet avec des données et des métadonnées, ou remplace un objet existant par des données et des métadonnées dans un système StorageGRID.

StorageGRID prend en charge les objets jusqu'à 5 Tio (5,497,558,138,880 octets).



Les demandes contradictoires des clients, telles que deux clients qui écrivent sur la même clé, sont résolues sur une base de « derniers-victoires ». Le moment auquel l'évaluation « derniers-victoires » est basé sur la date à laquelle le système StorageGRID remplit une demande donnée et non sur la date à laquelle les clients Swift entament une opération.

Les paramètres de demande suivants sont requis :

- Account
- Container
- Object

L'en-tête de demande suivant est requis :

- X-Auth-Token

Les en-têtes de demande suivants sont facultatifs :

- Content-Disposition

- Content-Encoding

Ne pas utiliser de moucheté Content-Encoding Si la règle ILM appliquée à un objet filtre les objets en fonction de leur taille et utilise le placement synchrone à l'ingestion (options équilibrées ou strictes pour le comportement d'ingestion).

- Transfer-Encoding

N'utilisez pas de compression ou de déboucheté Transfer-Encoding Si la règle ILM appliquée à un objet filtre les objets en fonction de leur taille et utilise le placement synchrone à l'ingestion (options équilibrées ou strictes pour le comportement d'ingestion).

- Content-Length

Si une règle ILM filtre les objets par taille et utilise le placement synchrone lors de l'ingestion, vous devez spécifier Content-Length.



Si vous ne suivez pas ces directives pour Content-Encoding, Transfer-Encoding, et Content-Length, StorageGRID doit enregistrer l'objet avant de déterminer la taille de l'objet et d'appliquer la règle ILM. En d'autres termes, StorageGRID doit créer par défaut des copies intermédiaires d'un objet à l'entrée. C'est-à-dire que StorageGRID doit utiliser l'option de double validation pour le comportement d'ingestion.

Pour plus d'informations sur le placement synchrone et les règles ILM, voir "[Options de protection des données pour l'ingestion](#)".

- Content-Type

- ETag

- X-Object-Meta-<name\> (métadonnées liées aux objets)

Si vous souhaitez utiliser l'option **temps de création défini par l'utilisateur** comme heure de référence pour une règle ILM, vous devez stocker la valeur dans un en-tête défini par l'utilisateur nommé X-Object-Meta-Creation-Time. Par exemple :

```
X-Object-Meta-Creation-Time: 1443399726
```

Ce champ est évalué en secondes depuis le 1er janvier 1970.

- X-Storage-Class: reduced_redundancy

Cet en-tête affecte le nombre de copies d'objet créées par StorageGRID si la règle ILM correspondant à l'objet ingéré spécifie le comportement d'ingestion de la double validation ou de l'équilibrage.

- **Double commit** : si la règle ILM spécifie l'option de double validation pour le comportement d'ingestion, StorageGRID crée une copie intermédiaire unique lors de l'ingestion de l'objet (simple commit).
- **Équilibré** : si la règle ILM spécifie l'option équilibrée, StorageGRID effectue une seule copie intermédiaire uniquement si le système ne peut pas immédiatement effectuer toutes les copies

spécifiées dans la règle. Si StorageGRID peut effectuer un placement synchrone, cet en-tête n'a aucun effet.

Le `reduced_redundancy` L'en-tête est le plus utilisé lorsque la règle ILM correspondant à l'objet crée une copie répliquée unique. Dans ce cas, utilisez `reduced_redundancy` élimine la création et la suppression inutiles d'une copie d'objet supplémentaire pour chaque opération d'ingestion.

À l'aide du `reduced_redundancy` l'en-tête n'est pas recommandé dans d'autres cas, car il augmente le risque de perte de données d'objet lors de l'ingestion. Vous risquez par exemple de perdre des données si une seule copie est initialement stockée sur un nœud de stockage qui échoue avant l'évaluation du ILM.



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

Notez que la spécification `reduced_redundancy` l'impact sur le nombre de copies créées uniquement lors de l'ingestion d'un objet. Cela n'affecte pas le nombre de copies de l'objet effectuées lorsque l'objet est évalué par les règles ILM actives et n'entraîne pas le stockage des données à des niveaux de redondance inférieurs dans le système StorageGRID.

Une exécution réussie renvoie les en-têtes suivants avec une réponse "HTTP/1.1 201 created" :

- Content-Length
- Content-Type
- Date
- ETag
- Last-Modified
- X-Trans-Id

Demande D'OPTIONS

La demande D'OPTIONS vérifie la disponibilité d'un service Swift individuel. La demande D'OPTIONS est traitée par le nœud de stockage ou le nœud passerelle spécifié dans l'URL.

Méthode DES OPTIONS

Par exemple, les applications client peuvent émettre une demande D'OPTIONS vers le port Swift sur un nœud de stockage, sans fournir d'informations d'authentification Swift, pour déterminer si le nœud de stockage est disponible. Vous pouvez utiliser cette requête pour la surveillance ou permettre aux équilibres de charge externes d'identifier lorsqu'un nœud de stockage est arrêté.

Lorsqu'elle est utilisée avec l'URL info ou l'URL de stockage, la méthode OPTIONS renvoie une liste de verbes pris en charge pour l'URL donnée (par exemple, HEAD, GET, OPTIONS et PUT). La méthode D'OPTIONS ne peut pas être utilisée avec l'URL d'authentification.

Le paramètre de demande suivant est requis :

- Account

Les paramètres de demande suivants sont facultatifs :

- Container
- Object

Une exécution réussie renvoie les en-têtes suivants avec une réponse « HTTP/1.1 204 No Content ». La demande D'OPTIONS à l'URL de stockage ne nécessite pas que la cible existe.

- Allow (Une liste de verbes pris en charge pour l'URL donnée, par exemple, HEAD, GET, OPTIONS, Et PUT)
- Content-Length
- Content-Type
- Date
- X-Trans-Id

Informations associées

["Terminaux API Swift pris en charge"](#)

Réponse aux erreurs des opérations de l'API Swift

La compréhension des réponses d'erreur possibles peut vous aider à résoudre les problèmes.

Les codes d'état HTTP suivants peuvent être renvoyés lorsque des erreurs se produisent au cours d'une opération :

Nom de l'erreur Swift	Statut HTTP
AccountNameToolong, ContainerNameToolong, HeaderTooBig, InvalidContainerName, InvalidRequest, InvalidURI, MetadaNameToolong, MetadaValueTooBig, MissingSecurityHeader, ObjectNameToolong, TooManyContainers, TooManyMetadaItems, TotalMetadaTooLarge	400 demande erronée
AccessDenied	403 interdit
ContainerNotEmpty, ContainerAlreadyExists	409 conflit
Erreur interne	500 erreur interne du serveur
InvalidRange	416 Plage demandée non satisfiable
MethodNotAllowed	405 méthode non autorisée

Nom de l'erreur Swift	Statut HTTP
MissingContentLength	411 longueur requise
NOTFOUND	404 introuvable
Note d'implémentation	501 non mis en œuvre
Pré-conditionFailed	412 Echec de la condition préalable
ResourceNotFound	404 introuvable
Non autorisé	401 non autorisé
Entité intraitableEntity	422 entité impossible à traiter

Opérations de l'API REST StorageGRID Swift

Des opérations sont ajoutées à l'API REST Swift qui sont spécifiques au système StorageGRID.

DEMANDE DE cohérence du conteneur

"[Valeurs de cohérence](#)" Équilibre entre disponibilité des objets et cohérence entre ces objets sur différents nœuds et sites de stockage. La demande de cohérence GET Container vous permet de déterminer la cohérence appliquée à un conteneur particulier.

Demande

En-tête HTTP de demande	Description
X-Auth-Token	Spécifie le jeton d'authentification Swift pour le compte à utiliser pour la demande.
x-ntap-sg-cohérence	Spécifie le type de demande, où <code>true</code> = COHÉRENCE GARANTIE entre les conteneurs, et <code>false</code> = CONTENEUR GET.
Hôte	Nom d'hôte auquel la demande est dirigée.

Exemple de demande

```
GET /v1/28544923908243208806/Swift container
X-Auth-Token: SGRD_3a877009a2d24cb1801587bfa9050f29
x-ntap-sg-consistency: true
Host: test.com
```

Réponse

En-tête HTTP de réponse	Description
Date	La date et l'heure de la réponse.
Connexion	Indique si la connexion au serveur est ouverte ou fermée.
X-Trans-ID	Identifiant de transaction unique pour la demande.
Longueur-contenu	Longueur du corps de réponse.
x-ntap-sg-cohérence	<p>Cohérence appliquée au conteneur. Les valeurs suivantes sont prises en charge :</p> <p>All : tous les nœuds reçoivent immédiatement les données ou la demande échoue.</p> <p>Strong-global : garantit la cohérence lecture après écriture pour toutes les demandes client sur tous les sites.</p> <p>Strong-site : garantit la cohérence lecture après écriture pour toutes les demandes client au sein d'un site.</p> <p>Read-After-New-write: (Par défaut) fournit une cohérence lecture-après-écriture pour les nouveaux objets et une cohérence éventuelle pour les mises à jour d'objets. Offre une haute disponibilité et une protection des données garanties. Recommandé dans la plupart des cas.</p> <p>Disponible : assure la cohérence finale pour les nouveaux objets et les mises à jour d'objets. Pour les compartiments S3, utilisez uniquement si nécessaire (par exemple, pour un compartiment qui contient des valeurs de journal rarement lues ou pour les opérations HEAD ou GET sur des clés qui n'existent pas). Non pris en charge pour les compartiments FabricPool S3.</p>

Exemple de réponse

```
HTTP/1.1 204 No Content
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
X-Trans-Id: 1936575373
Content-Length: 0
x-ntap-sg-consistency: strong-site
```

REQUÊTE de cohérence du conteneur

La demande de cohérence PUT Container vous permet d'indiquer la cohérence à appliquer aux opérations

effectuées sur un conteneur. Par défaut, les nouveaux conteneurs sont créés avec la cohérence « Read-after-New-write ».

Demande

En-tête HTTP de demande	Description
X-Auth-Token	Jeton d'authentification Swift pour le compte à utiliser pour la demande.
x-ntap-sg-cohérence	<p>Cohérence à appliquer aux opérations sur le conteneur. Les valeurs suivantes sont prises en charge :</p> <p>All : tous les nœuds reçoivent immédiatement les données ou la demande échoue.</p> <p>Strong-global : garantit la cohérence lecture après écriture pour toutes les demandes client sur tous les sites.</p> <p>Strong-site : garantit la cohérence lecture après écriture pour toutes les demandes client au sein d'un site.</p> <p>Read-After-New-write: (Par défaut) fournit une cohérence lecture-après-écriture pour les nouveaux objets et une cohérence éventuelle pour les mises à jour d'objets. Offre une haute disponibilité et une protection des données garanties. Recommandé dans la plupart des cas.</p> <p>Disponible : assure la cohérence finale pour les nouveaux objets et les mises à jour d'objets. Pour les compartiments S3, utilisez uniquement si nécessaire (par exemple, pour un compartiment qui contient des valeurs de journal rarement lues ou pour les opérations HEAD ou GET sur des clés qui n'existent pas). Non pris en charge pour les compartiments FabricPool S3.</p>
Host	Nom d'hôte auquel la demande est dirigée.

Impact de la cohérence et des règles ILM pour la protection des données

À la fois de votre choix "[valeur de la cohérence](#)" De plus, votre règle ILM affecte la façon dont les objets sont protégés. Ces paramètres peuvent interagir.

Par exemple, la cohérence utilisée lorsqu'un objet est stocké affecte le placement initial des métadonnées de l'objet, tandis que l' "[comportement d'ingestion](#)" Cette case à cocher affecte le placement initial des copies d'objet. Comme StorageGRID requiert l'accès aux métadonnées et aux données d'un objet pour répondre aux demandes des clients, le choix de niveaux de protection correspondants pour la cohérence et le comportement d'ingestion permet une meilleure protection initiale des données et des réponses système plus prévisibles.

Exemple de l'interaction des règles de cohérence et des règles ILM

Supposons que vous disposez d'un grid à deux sites avec la règle ILM suivante et la cohérence suivante :

- **Règle ILM** : créez deux copies d'objet, une sur le site local et une sur un site distant. Le comportement d'entrée strict est sélectionné.

- **: "Fort-global" (les métadonnées de l'objet sont immédiatement distribuées à tous les sites.)

Lorsqu'un client stocke un objet dans la grille, StorageGRID effectue à la fois des copies d'objet et distribue les métadonnées aux deux sites avant de rétablir la réussite du client.

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

Si vous utilisez à la place la même règle ILM et la même cohérence « site fort », le client peut recevoir un message de réussite après la réplication des données d'objet vers le site distant, mais avant la distribution des métadonnées d'objet. Dans ce cas, le niveau de protection des métadonnées d'objet ne correspond pas au niveau de protection des données d'objet. Si le site local est perdu peu de temps après l'ingestion, les métadonnées d'objet sont perdues. Impossible de récupérer l'objet.

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

Exemple de demande

```
PUT /v1/28544923908243208806/_Swift container_
X-Auth-Token: SGRD_3a877009a2d24cb1801587bfa9050f29
x-ntap-sg-consistency: strong-site
Host: test.com
```

Réponse

En-tête HTTP de réponse	Description
Date	La date et l'heure de la réponse.
Connection	Indique si la connexion au serveur est ouverte ou fermée.
X-Trans-Id	Identifiant de transaction unique pour la demande.
Content-Length	Longueur du corps de réponse.

Exemple de réponse

```
HTTP/1.1 204 No Content
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
X-Trans-Id: 1936575373
Content-Length: 0
```

Les opérations Swift sont suivies dans les journaux d'audit

Toutes les opérations réussies DE SUPPRESSION, D'OBTENTION, DE TÊTE, DE POST et DE PUT du stockage sont consignées dans le journal d'audit de StorageGRID. Les échecs et les demandes d'informations, d'authentification ou D'OPTIONS ne sont pas consignés.

Opérations sur le compte

- "OBTENIR un compte"
- "Compte PRINCIPAL"

Opérations sur les conteneurs

- "SUPPRIMER le conteneur"
- "CONTENEUR"
- "Conteneur DE TÊTE"
- "PLACER le conteneur"

Opérations sur l'objet

- "SUPPRIMER l'objet"
- "OBJET GET"
- "Objet TÊTE"
- "PLACER l'objet"

Informations associées

- "Accéder au fichier journal d'audit"
- "Écrire des messages d'audit client"
- "Messages d'audit de lecture du client"

Informations sur le copyright

Copyright © 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.