



# **Utilisez l'API REST de Swift**

## **StorageGRID 11.5**

NetApp  
April 11, 2024

This PDF was generated from <https://docs.netapp.com/fr-fr/storagegrid-115/swift/history-of-swift-api-support-in-storagegrid.html> on April 11, 2024. Always check docs.netapp.com for the latest.

# Sommaire

- Utiliser Swift ..... 1
  - Prise en charge de l'API OpenStack Swift dans StorageGRID ..... 1
  - Configuration des comptes et des connexions des locataires ..... 4
  - Opérations prises en charge par l'API REST Swift ..... 9
  - Opérations de l'API REST StorageGRID Swift ..... 22
  - Configuration de la sécurité pour l'API REST ..... 27
  - Surveillance et audit des opérations ..... 30

# Utiliser Swift

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

- ["Prise en charge de l'API OpenStack Swift dans StorageGRID"](#)
- ["Configuration des comptes et des connexions des locataires"](#)
- ["Opérations prises en charge par l'API REST Swift"](#)
- ["Opérations de l'API REST StorageGRID Swift"](#)
- ["Configuration de la sécurité pour l'API REST"](#)
- ["Surveillance et audit des opérations"](#)

## Prise en charge de l'API OpenStack Swift dans StorageGRID

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).  <b>Remarque:</b> 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
11.5	Suppression du contrôle de cohérence faible Le niveau de cohérence disponible sera utilisé à la place.
11.4	Ajout de la prise en charge de TLS 1.3 et mise à jour de la liste des suites de chiffrement TLS prises en charge. CLB est obsolète. Ajout d'une description de l'interrelation entre ILM et paramètre de 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 noeuds finaux d'équilibreur de charge ou des groupes de haute disponibilité. Liste mise à jour des suites de chiffrement TLS prises en charge. 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 contrôles 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

À l'entrée des objets Swift dans le système StorageGRID, ils sont gérés par les règles de gestion du cycle de vie des informations de la politique ILM active du système. Les règles et règles ILM déterminent la façon dont StorageGRID crée et distribue des copies de données d'objet ainsi que la façon dont elles gèrent 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 administrateur StorageGRID si vous avez besoin de savoir comment les règles et règles ILM

du grid affectent 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 la base des « derniers-victoires ». Le calendrier de l'évaluation « derniers-victoires » est basé sur le moment où le système StorageGRID remplit une demande donnée et non sur le moment où les clients Swift démarrent 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. Tout GET suivant un PUT réussi sera en mesure de 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. Vous pouvez modifier le contrôle de cohérence pour assurer une reprise entre la disponibilité des objets et la cohérence de ces objets sur plusieurs nœuds et sites de stockage, selon les besoins de votre application.

#### **Informations associées**

["Gestion des objets avec ILM"](#)

["DEMANDE DE cohérence du conteneur"](#)

["REQUÊTE de cohérence du conteneur"](#)

### **Recommandations pour la mise en œuvre 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 sur un chemin où vous ne vous attendez pas à ce que l'objet existe réellement, vous devez utiliser le contrôle de cohérence « disponible ». Par exemple, vous devez utiliser le contrôle de 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 le contrôle de cohérence « disponible » pour chaque conteneur à l'aide de la demande DE cohérence DU conteneur PUT.

#### **Recommandations pour les noms d'objet**

Vous ne devez pas utiliser de valeurs aléatoires comme les quatre premiers caractères des noms d'objets. Au lieu de cela, vous devez utiliser des préfixes non aléatoires et non uniques, tels que l'image.

Si vous avez besoin d'utiliser des caractères aléatoires et uniques dans les préfixes de nom d'objet, vous devez préfixer les noms d'objet 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 « plages de lectures »

Si l'option **Compress emmagasé Objects** est sélectionnée (**Configuration > Paramètres système > Grid Options**), les applications client Swift doivent éviter d'effectuer des opérations GET object spécifiant une plage d'octets à renvoyer. Ces opérations de « lecture à 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.

#### Informations associées

["DEMANDE DE cohérence du conteneur"](#)

["REQUÊTE de cohérence du conteneur"](#)

["Administrer StorageGRID"](#)

## Configuration des comptes et des connexions des locataires

Pour configurer StorageGRID pour accepter les connexions à partir des applications client, vous devez créer un ou plusieurs comptes de tenant et configurer les connexions.

### Création et configuration de comptes de tenant Swift

Un compte de locataire Swift est requis pour que les clients de l'API Swift puissent stocker et récupérer des objets sur StorageGRID. Chaque compte de locataire possède son propre ID de compte, groupes et utilisateurs, ainsi que des conteneurs et des objets.

Les comptes de locataires Swift sont créés par un administrateur StorageGRID GRID à l'aide de Grid Manager ou de l'API de gestion du grid.

Lors de la création d'un compte de locataire Swift, l'administrateur du grid spécifie les informations suivantes :

- Nom d'affichage du locataire (l'ID de compte du locataire est attribué automatiquement et ne peut pas être modifié)
- Éventuellement, un quota de stockage pour le compte du locataire, soit le nombre maximal de gigaoctets, téraoctets ou pétaoctets disponibles pour les objets du locataire. Le quota de stockage d'un locataire

représente une quantité logique (taille d'objet), et non une quantité physique (taille sur disque).

- Si l'authentification unique (SSO) n'est pas utilisée pour le système StorageGRID, que le compte de tenant utilise son propre référentiel d'identité ou partage le référentiel d'identité de la grille et le mot de passe initial de l'utilisateur racine local du locataire.
- Si SSO est activé, quel groupe fédéré dispose d'une autorisation d'accès racine pour configurer le compte locataire.

Après la création d'un compte de locataire Swift, les utilisateurs disposant de l'autorisation accès racine peuvent accéder au Gestionnaire de locataires pour effectuer les tâches suivantes :

- Configuration de la fédération des identités (sauf si le référentiel d'identité est partagé avec la grille) et création de groupes et d'utilisateurs locaux
- Contrôle de l'utilisation du stockage



Les utilisateurs Swift doivent disposer de l'autorisation d'accès racine pour accéder au gestionnaire de locataires. Toutefois, l'autorisation accès racine ne permet pas aux utilisateurs de s'authentifier auprès de l'API REST Swift pour créer des conteneurs et ingérer des objets. Les utilisateurs doivent disposer de l'autorisation Administrateur Swift pour s'authentifier dans l'API REST de Swift.

#### Informations associées

["Administrer StorageGRID"](#)

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

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

## Configuration des connexions client

Un administrateur du grid fait des choix de configuration qui affectent la manière dont les clients Swift se connectent à StorageGRID pour stocker et récupérer les données. Les informations spécifiques dont vous avez besoin pour établir une connexion dépendent de la configuration choisie.

Les applications client peuvent stocker ou récupérer des objets en se connectant à l'un des éléments suivants :

- Le service Load Balancer sur les nœuds d'administration ou de passerelle, ou, le cas échéant, l'adresse IP virtuelle d'un groupe de nœuds d'administration ou de nœuds de passerelle haute disponibilité
- Le service CLB sur les nœuds de passerelle ou, éventuellement, l'adresse IP virtuelle d'un groupe de nœuds de passerelle haute disponibilité



Le service CLB est obsolète. Les clients configurés avant la version de StorageGRID 11.3 peuvent continuer à utiliser le service CLB sur les nœuds de passerelle. Toutes les autres applications client qui dépendent de StorageGRID pour fournir un équilibrage de la charge doivent se connecter à l'aide du service Load Balancer.

- Des nœuds de stockage, avec ou sans équilibreur de charge externe

Lors de la configuration de StorageGRID, un administrateur de la grille peut utiliser le gestionnaire de grille ou l'API de gestion de grille pour effectuer les étapes suivantes, qui sont toutes facultatives :

1. Configurez les nœuds finaux pour le service Load Balancer.

Vous devez configurer les noeuds finaux pour utiliser le service Load Balancer. Le service Load Balancer sur les nœuds d'administration ou de passerelle distribue les connexions réseau entrantes des applications client aux nœuds de stockage. Lors de la création d'un terminal d'équilibrage de charge, l'administrateur StorageGRID spécifie un numéro de port, si le terminal accepte les connexions HTTP ou HTTPS, le type de client (S3 ou Swift) qui utilisera le terminal ainsi que le certificat à utiliser pour les connexions HTTPS (le cas échéant).

## 2. Configurer des réseaux clients non fiables.

Si un administrateur StorageGRID configure le réseau client d'un nœud pour qu'il ne soit pas fiable, le nœud accepte uniquement les connexions entrantes sur le réseau client sur les ports explicitement configurés en tant que noeuds finaux d'équilibreur de charge.

## 3. Configurez les groupes haute disponibilité.

Si l'administrateur crée un groupe haute disponibilité, les interfaces réseau de plusieurs nœuds d'administration ou nœuds de passerelle sont placées dans une configuration de sauvegarde active/active. Les connexions client sont établies à l'aide de l'adresse IP virtuelle du groupe haute disponibilité.

Pour plus d'informations sur chaque option, reportez-vous aux instructions d'administration de StorageGRID.

### Résumé : adresses IP et ports pour les connexions client

Les applications client se connectent à StorageGRID en utilisant l'adresse IP d'un nœud de grid et le numéro de port d'un service sur ce nœud. Si des groupes de haute disponibilité sont configurés, les applications client peuvent se connecter en utilisant l'adresse IP virtuelle du groupe de haute disponibilité.

#### Informations requises pour établir des connexions client

Le tableau récapitule les différentes façons dont les clients peuvent se connecter à StorageGRID ainsi que les adresses IP et les ports utilisés pour chaque type de connexion. Contactez votre administrateur StorageGRID pour en savoir plus ou consultez les instructions d'administration de StorageGRID pour obtenir une description de la recherche de ces informations dans le Gestionnaire de grille.

Là où la connexion est établie	Service auquel le client se connecte	Adresse IP	Port
Groupe HAUTE DISPONIBILITÉ	Équilibreur de charge	Adresse IP virtuelle d'un groupe haute disponibilité	<ul style="list-style-type: none"> <li>Port du terminal de l'équilibreur de charge</li> </ul>
Groupe HAUTE DISPONIBILITÉ	CLB <b>Note:</b> le service CLB est obsolète.	Adresse IP virtuelle d'un groupe haute disponibilité	Ports Swift par défaut : <ul style="list-style-type: none"> <li>HTTPS: 8083</li> <li>HTTP : 8085</li> </ul>
Nœud d'administration	Équilibreur de charge	Adresse IP du nœud d'administration	<ul style="list-style-type: none"> <li>Port du terminal de l'équilibreur de charge</li> </ul>
Nœud de passerelle	Équilibreur de charge	Adresse IP du nœud de passerelle	<ul style="list-style-type: none"> <li>Port du terminal de l'équilibreur de charge</li> </ul>



Là où la connexion est établie	Service auquel le client se connecte	Adresse IP	Port
Nœud de passerelle	CLB  <b>Note:</b> le service CLB est obsolète.	Adresse IP du nœud de passerelle  <b>Remarque :</b> par défaut, les ports HTTP pour CLB et LDR ne sont pas activés.	Ports Swift par défaut :  • HTTPS: 8083 • HTTP : 8085
Nœud de stockage	LDR	Adresse IP du nœud de stockage	Ports Swift par défaut :  • HTTPS: 18083 • HTTP : 18085

### Exemple

Pour connecter un client Swift au point de terminaison Load Balancer d'un groupe HA de nœuds de passerelle, utilisez une URL structurée comme indiqué ci-dessous :

- `https://VIP-of-HA-group:LB-endpoint-port`

Par exemple, si l'adresse IP virtuelle du groupe HA est 192.0.2.6 et que le numéro de port d'un nœud final Swift Load Balancer est 10444, un client Swift peut utiliser l'URL suivante pour se connecter à StorageGRID :

- `https://192.0.2.6:10444`

Il est possible de configurer un nom DNS pour l'adresse IP que les clients utilisent pour se connecter à StorageGRID. Contactez votre administrateur réseau local.

### Choix d'utiliser des connexions HTTPS ou HTTP

Lorsque les connexions client sont effectuées à l'aide d'un nœud final Load Balancer, les connexions doivent être effectuées à l'aide du protocole (HTTP ou HTTPS) spécifié pour ce nœud final. Pour utiliser HTTP pour les connexions client aux nœuds de stockage ou au service CLB sur les nœuds de passerelle, vous devez activer son utilisation.

Par défaut, lorsque les applications client se connectent aux nœuds de stockage ou au service CLB sur les nœuds de passerelle, elles doivent utiliser le protocole HTTPS chiffré pour toutes les connexions. Vous pouvez également activer des connexions HTTP moins sécurisées en sélectionnant l'option de grille **Activer connexion HTTP** dans le Gestionnaire de grille. Par exemple, une application client peut utiliser HTTP lors du test de la connexion à un nœud de stockage dans un environnement non-production.



Soyez prudent lorsque vous activez HTTP pour une grille de production car les demandes seront envoyées de manière non chiffrée.



Le service CLB est obsolète.

Si l'option **Activer connexion HTTP** est sélectionnée, les clients doivent utiliser des ports HTTP différents de ceux qu'ils utilisent pour HTTPS. Voir les instructions d'administration de StorageGRID.

## Informations associées

"Administrer StorageGRID"

## Test de votre connexion dans la configuration de l'API Swift

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

### Ce dont vous avez besoin

- Vous devez avoir téléchargé et installé python-swiftclient, le client de ligne de commande Swift.
- Vous devez disposer d'un compte de locataire Swift dans le système StorageGRID.

### 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
```

#### Informations associées

["Création et configuration de comptes de tenant Swift"](#)

["Configuration de la sécurité pour l'API REST"](#)

## 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

["Configuration des connexions client"](#)

["Création et configuration de comptes de tenant Swift"](#)

"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 aucun contenu » si le compte est trouvé et qu'aucun conteneur n'est vide, ou une réponse « HTTP/1.1 200 OK » si le compte est trouvé et que 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**

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

## Opérations sur l'objet

Les opérations suivantes de l'API Swift sont effectuées sur des objets.

### 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, si un emplacement est temporairement indisponible), StorageGRID met les copies en file d'attente pour suppression, puis indique que le client a réussi à les supprimer.

Pour plus d'informations sur la suppression des objets, reportez-vous aux instructions relatives à la gestion des objets avec la gestion du cycle de vie des informations.

### 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 pouvant atteindre 5 To.



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

N'utilisez pas de hachés 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 ni de hachée 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, reportez-vous aux instructions relatives à la gestion des objets avec des informations relatives à la gestion du cycle de vie.

- 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 temps 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 ne fait une copie provisoire que si le système ne peut pas immédiatement faire 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. Elle n'affecte pas le nombre de copies de l'objet lorsque celui-ci est évalué par la règle ILM active et n'entraîne pas le stockage des données avec 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

#### Informations associées

["Gestion des objets avec ILM"](#)

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

## 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
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

Nom de l'erreur Swift	Statut HTTP
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

Le niveau de cohérence assure une reprise entre la disponibilité des objets et la cohérence de ces objets sur différents sites et nœuds de stockage. La demande DE cohérence DU conteneur GET vous permet de déterminer le niveau de cohérence appliqué 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-consistency	Spécifie le type de demande, où <code>true</code> = COHÉRENCE GARANTIE entre les conteneurs, et <code>false</code> = CONTENEUR GET.
Host	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.
Connection	Indique si la connexion au serveur est ouverte ou fermée.



En-tête HTTP de réponse	Description
X-Trans-Id	Identifiant de transaction unique pour la demande.
Content-Length	Longueur du corps de réponse.
x-ntap-sg-consistency	<p>Niveau de contrôle de cohérence appliqué au conteneur. Les valeurs suivantes sont prises en charge :</p> <ul style="list-style-type: none"> <li>• <b>Tous</b> : tous les nœuds reçoivent les données immédiatement ou la demande échouera.</li> <li>• <b>Forte-global</b>: Garantit la cohérence lecture-après-écriture pour toutes les demandes client sur tous les sites.</li> <li>• <b>Site fort</b> : garantit la cohérence de lecture après écriture pour toutes les demandes de clients au sein d'un site.</li> <li>• <b>Lecture-après-nouvelle-écriture</b> : offre 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.</li> </ul> <p><b>Remarque</b> : si votre application utilise des demandes HEAD sur des objets qui n'existent pas, vous pouvez recevoir un nombre élevé de 500 erreurs de serveur interne si un ou plusieurs nœuds de stockage ne sont pas disponibles. Pour éviter ces erreurs, utilisez le niveau « disponible ».</p> <ul style="list-style-type: none"> <li>• <b>Disponible</b> (cohérence éventuelle pour les opérations DE TÊTE) : se comporte de la même façon que le niveau de cohérence "entre les nouvelles écritures", mais ne fournit qu'une cohérence éventuelle pour les opérations DE TÊTE. Niveaux de disponibilité supérieurs à ceux de la « nouvelle écriture » en cas d'indisponibilité des nœuds de stockage</li> </ul>

### 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
```

#### Informations associées

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

## REQUÊTE de cohérence du conteneur

La demande DE cohérence PUT dans le conteneur vous permet de spécifier le niveau de cohérence à appliquer aux opérations effectuées dans un conteneur. Par défaut, les nouveaux conteneurs sont créés à l'aide du niveau de 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.

En-tête HTTP de demande	Description
x-ntap-sg-consistency	<p>Niveau de contrôle de cohérence à appliquer aux opérations sur le conteneur. Les valeurs suivantes sont prises en charge :</p> <ul style="list-style-type: none"> <li>• <b>Tous</b> : tous les nœuds reçoivent les données immédiatement ou la demande échouera.</li> <li>• <b>Forte-global</b>: Garantit la cohérence lecture-après-écriture pour toutes les demandes client sur tous les sites.</li> <li>• <b>Site fort</b> : garantit la cohérence de lecture après écriture pour toutes les demandes de clients au sein d'un site.</li> <li>• <b>Lecture-après-nouvelle-écriture</b> : offre 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.</li> </ul> <p><b>Remarque</b> : si votre application utilise des demandes HEAD sur des objets qui n'existent pas, vous pouvez recevoir un nombre élevé de 500 erreurs de serveur interne si un ou plusieurs nœuds de stockage ne sont pas disponibles. Pour éviter ces erreurs, utilisez le niveau « disponible ».</p> <ul style="list-style-type: none"> <li>• <b>Disponible</b> (cohérence éventuelle pour les opérations DE TÊTE) : se comporte de la même façon que le niveau de cohérence "entre les nouvelles écritures", mais ne fournit qu'une cohérence éventuelle pour les opérations DE TÊTE. Niveaux de disponibilité supérieurs à ceux de la « nouvelle écriture » en cas d'indisponibilité des nœuds de stockage</li> </ul>
Host	Nom d'hôte auquel la demande est dirigée.

## Interaction des contrôles de cohérence et des règles ILM pour la protection des données

Le contrôle de cohérence et la règle ILM de votre choix affectent la protection des objets. Ces paramètres peuvent interagir.

Par exemple, le contrôle de cohérence utilisé lorsqu'un objet est stocké affecte le placement initial des métadonnées d'objet, tandis que le comportement d'ingestion sélectionné pour la règle ILM affecte le placement initial des copies d'objet. Étant donné que StorageGRID nécessite l'accès aux métadonnées d'un objet et à ses données pour répondre aux demandes client, la sélection de niveaux de protection correspondant au niveau de cohérence et au comportement d'ingestion permet d'améliorer la protection des données initiale et de mieux prévoir les réponses du système.

Les comportements d'ingestion suivants sont disponibles pour les règles ILM :

- **Strict** : toutes les copies spécifiées dans la règle ILM doivent être effectuées avant que le succès ne soit renvoyé au client.
- **Équilibré** : StorageGRID tente de faire toutes les copies spécifiées dans la règle ILM à l'entrée; si ce n'est pas possible, des copies intermédiaires sont faites et le succès est renvoyé au client. Les copies spécifiées dans la règle ILM sont effectuées lorsque cela est possible.
- **Double commit** : StorageGRID effectue immédiatement des copies intermédiaires de l'objet et retourne le succès au client. Les copies spécifiées dans la règle ILM sont effectuées lorsque cela est possible.



Avant de sélectionner le comportement d'entrée d'une règle ILM, lisez la description complète de ces paramètres dans les instructions de gestion des objets avec la gestion du cycle de vie des informations.

### Exemple d'interaction du contrôle de cohérence et de la règle ILM

Supposons que vous disposez d'une grille à deux sites avec la règle ILM suivante et le paramètre de niveau de cohérence suivant :

- **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.
- **Niveau de cohérence** : "Sept-global" (les métadonnées d'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 le niveau de cohérence "sept-site", le client peut recevoir un message de réussite après la répllication des données d'objet vers le site distant, mais avant que les métadonnées d'objet ne soient distribuées sur ce site. 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. L'objet ne peut pas être récupéré.

L'interdépendance entre les niveaux de 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
```

### Informations associées

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

## Configuration de la sécurité pour l'API REST

Il est recommandé de passer en revue les mesures de sécurité mises en œuvre pour l'API REST et de comprendre comment sécuriser votre système.

### Comment StorageGRID assure la sécurité pour l'API REST

Vous devez comprendre comment le système StorageGRID implémente la sécurité, l'authentification et l'autorisation pour l'API REST.

StorageGRID utilise les mesures de sécurité suivantes.

- Les communications client avec le service Load Balancer utilisent HTTPS si HTTPS est configuré pour le noeud final Load Balancer.

Lorsque vous configurez un point final d'équilibreur de charge, HTTP peut éventuellement être activé. Par exemple, vous pouvez utiliser HTTP à des fins de test ou autres que la production. Pour plus d'informations, reportez-vous aux instructions d'administration de StorageGRID.

- Par défaut, StorageGRID utilise HTTPS pour les communications client avec les nœuds de stockage et le service CLB sur les nœuds de passerelle.

HTTP peut éventuellement être activé pour ces connexions. Par exemple, vous pouvez utiliser HTTP à des fins de test ou autres que la production. Pour plus d'informations, reportez-vous aux instructions d'administration de StorageGRID.



Le service CLB est obsolète.

- Les communications entre StorageGRID et le client sont chiffrées à l'aide de TLS.
- Les communications entre le service Load Balancer et les nœuds de stockage dans la grille sont cryptées que le terminal de l'équilibreur de charge soit configuré pour accepter les connexions HTTP ou HTTPS.
- Les clients doivent fournir des en-têtes d'authentification HTTP à StorageGRID pour effectuer des opérations d'API REST.

## Certificats de sécurité et applications client

Les clients peuvent se connecter au service Load Balancer sur les nœuds de passerelle ou les nœuds d'administration, directement aux nœuds de stockage ou au service CLB sur les nœuds de passerelle.

Dans tous les cas, les applications client peuvent établir des connexions TLS à l'aide d'un certificat de serveur personnalisé chargé par l'administrateur de la grille ou d'un certificat généré par le système StorageGRID :

- Lorsque les applications client se connectent au service Load Balancer, elles le font à l'aide du certificat configuré pour le nœud final de l'équilibreur de charge spécifique utilisé pour établir la connexion. Chaque nœud final possède son propre certificat, qui est soit un certificat de serveur personnalisé chargé par l'administrateur de la grille, soit un certificat que l'administrateur de la grille a généré dans StorageGRID lors de la configuration du nœud final.
- Lorsque les applications client se connectent directement à un nœud de stockage ou au service CLB des nœuds de passerelle, elles utilisent soit les certificats de serveur générés par le système pour les nœuds de stockage lorsque le système StorageGRID a été installé (qui sont signés par l'autorité de certification du système), ou un seul certificat de serveur personnalisé fourni par un administrateur de grille pour la grille.

Les clients doivent être configurés pour approuver l'autorité de certification qui a signé le certificat qu'ils utilisent pour établir des connexions TLS.

Pour plus d'informations sur la configuration des nœuds finaux de l'équilibreur de charge et pour obtenir des instructions sur l'ajout d'un certificat de serveur personnalisé pour les connexions TLS directement aux nœuds de stockage ou au service CLB sur les nœuds de passerelle, reportez-vous aux instructions de la section Administration de StorageGRID.

## Récapitulatif

Le tableau suivant montre comment les problèmes de sécurité sont implémentés dans les API REST S3 et Swift :

Problème de sécurité	Implémentation pour l'API REST
Sécurité de la connexion	TLS
Authentification du serveur	Certificat de serveur X.509 signé par l'autorité de certification du système ou certificat de serveur personnalisé fourni par l'administrateur

Problème de sécurité	Implémentation pour l'API REST
Authentification client	<ul style="list-style-type: none"> <li>• S3 : compte S3 (ID de clé d'accès et clé d'accès secrète)</li> <li>• SWIFT : compte Swift (nom d'utilisateur et mot de passe)</li> </ul>
Autorisation du client	<ul style="list-style-type: none"> <li>• S3 : propriété des compartiments et toutes les règles de contrôle d'accès applicables</li> <li>• SWIFT : accès aux rôles d'administrateur</li> </ul>

#### Informations associées

["Administrer StorageGRID"](#)

## Algorithmes de hachage et de cryptage pris en charge pour les bibliothèques TLS

Le système StorageGRID prend en charge un ensemble limité de suites de chiffrement que les applications clientes peuvent utiliser lors de l'établissement d'une session TLS (transport Layer Security).

#### Versions supportées de TLS

StorageGRID supporte TLS 1.2 et TLS 1.3.



SSLv3 et TLS 1.1 (ou versions antérieures) ne sont plus pris en charge.

#### Suites de chiffrement prises en charge

Version TLS	Nom IANA de la suite de chiffrement
1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_CHA20_POLY1305_SHA256	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
1.3	TLS_AES_256_GCM_SHA384
TLS_CHA20_POLY1305_SHA256	TLS_AES_128_GCM_SHA256

#### Suites de chiffrement obsolètes

Les suites de chiffrement suivantes sont obsolètes. La prise en charge de ces chiffrements sera supprimée dans une prochaine version.

Nom IANA
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384

## Surveillance et audit des opérations

Vous pouvez surveiller les charges de travail et l'efficacité des opérations client en visualisant les tendances de transaction pour l'ensemble du grid ou pour des nœuds spécifiques. Vous pouvez utiliser des messages d'audit pour surveiller les opérations et les transactions des clients.

### Contrôle des taux d'entrée et de récupération des objets

Vous pouvez surveiller les taux d'entrée et de récupération des objets, ainsi que les mesures relatives au nombre d'objets, aux requêtes et à la vérification. Vous pouvez afficher le nombre de tentatives de lecture, d'écriture et de modification d'objets du système StorageGRID ayant échoué et réussies par les applications client.

#### Étapes

1. Connectez-vous au Grid Manager à l'aide d'un navigateur pris en charge.
2. Dans le tableau de bord, recherchez la section opérations de protocole.

Cette section récapitule le nombre d'opérations client effectuées par votre système StorageGRID. La moyenne des débits de protocole est calculée au cours des deux dernières minutes.

3. Sélectionnez **noeuds**.
4. Dans la page d'accueil noeuds (niveau de déploiement), cliquez sur l'onglet **Load Balancer**.

Les graphiques présentent les tendances de tout le trafic client dirigé vers les terminaux d'équilibreur de charge dans la grille. Vous pouvez sélectionner un intervalle de temps en heures, jours, semaines, mois ou années, vous pouvez également appliquer un intervalle personnalisé.

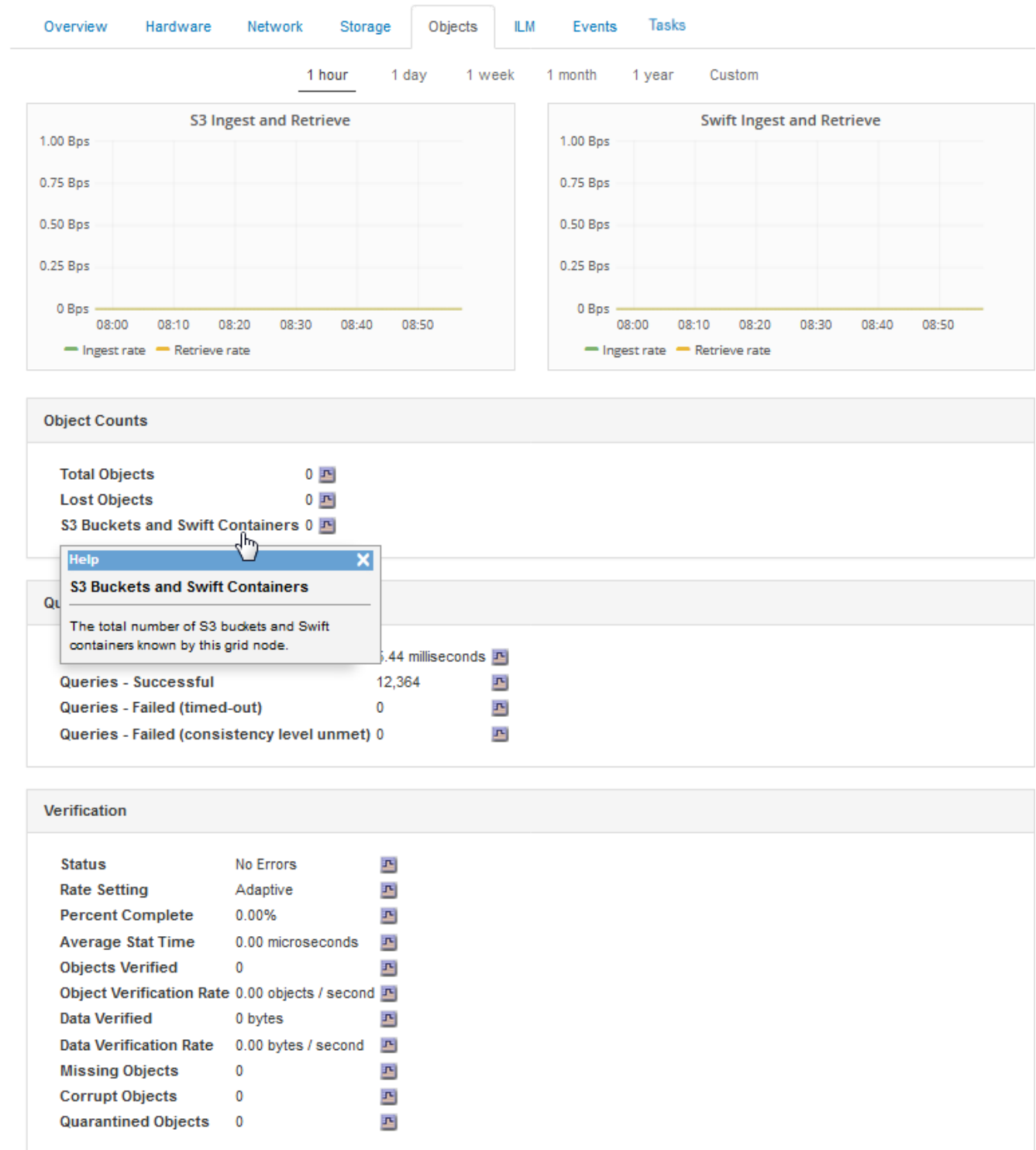
5. Dans la page d'accueil noeuds (niveau de déploiement), cliquez sur l'onglet **objets**.

Le graphique montre les taux d'entrée et de récupération de l'intégralité de votre système StorageGRID en octets par seconde et en octets totaux. Vous pouvez sélectionner un intervalle de temps en heures, jours, semaines, mois ou années, vous pouvez également appliquer un intervalle personnalisé.

6. Pour afficher les informations relatives à un nœud de stockage particulier, sélectionnez-le dans la liste de gauche, puis cliquez sur l'onglet **objets**.

Le tableau affiche les taux d'entrée et de récupération de l'objet pour ce nœud de stockage. L'onglet inclut également des mesures pour le nombre d'objets, les requêtes et la vérification. Vous pouvez cliquer sur les étiquettes pour afficher les définitions de ces mesures.





7. Si vous voulez encore plus de détails :
- Sélectionnez **support > Outils > topologie de grille**.
  - Sélectionnez **site > Présentation > main**.

La section opérations d'API affiche un récapitulatif des informations sur l'ensemble de la grille.

- Sélectionnez **Storage Node > LDR > client application > Présentation > main**

La section opérations affiche un récapitulatif des informations sur le nœud de stockage sélectionné.

## Accès aux journaux d'audit et vérification

Les messages d'audit sont générés par les services StorageGRID et stockés dans des fichiers journaux texte. Des messages d'audit spécifiques aux API dans les journaux d'audit fournissent des données stratégiques de sécurité, d'exploitation et de surveillance des performances qui vous aideront à évaluer l'état de votre système.

### Ce dont vous avez besoin

- Vous devez disposer d'autorisations d'accès spécifiques.
- Vous devez avoir le `Passwords.txt` fichier.
- Vous devez connaître l'adresse IP d'un nœud d'administration.

### Description de la tâche

Le fichier journal d'audit actif est nommé `audit.log`, Et il est stocké sur des nœuds d'administration.

Une fois par jour, le fichier `audit.log` actif est enregistré et un nouveau fichier `audit.log` est lancé. Le nom du fichier enregistré indique quand il a été enregistré, au format `yyyy-mm-dd.txt`.

Après un jour, le fichier enregistré est compressé et renommé, au format `yyyy-mm-dd.txt.gz`, qui conserve la date originale.

Cet exemple montre le fichier `audit.log` actif, le fichier de la veille (`2018-04-15.txt`) et le fichier compressé de la veille (`2018-04-14.txt.gz`).

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

### Étapes

1. Connectez-vous à un nœud d'administration :
  - a. Saisissez la commande suivante : `ssh admin@primary_Admin_Node_IP`
  - b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
2. Accédez au répertoire contenant les fichiers journaux d'audit : `cd /var/local/audit/export`
3. Afficher le fichier journal d'audit actuel ou enregistré, selon les besoins.

### Informations associées

["Examiner les journaux d'audit"](#)

### 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 ne sont pas consignés, ni les demandes d'info, d'auth ou D'OPTIONS.

Voir *compréhension des messages d'audit* pour plus de détails sur les informations suivies pour les opérations Swift suivantes.

### **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**

["Examiner les journaux d'audit"](#)

["Opérations sur le compte"](#)

["Opérations sur les conteneurs"](#)

["Opérations sur l'objet"](#)

## 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.