



# **Présentation de l'API de gestion des locataires**

StorageGRID 11.5

NetApp  
April 11, 2024

# Sommaire

- Présentation de l'API de gestion des locataires . . . . . 1
  - Opérations d'API . . . . . 1
  - Détails de l'opération . . . . . 2
  - Émission de requêtes API . . . . . 3
  - Gestion des versions de l'API de gestion des locataires . . . . . 4
  - Protection contre la contrefaçon de demandes intersites (CSRF) . . . . . 5

# Présentation de l'API de gestion des locataires

Vous pouvez effectuer des tâches de gestion du système via l'API REST de gestion des locataires plutôt que dans l'interface utilisateur du gestionnaire de locataires. Par exemple, vous pouvez utiliser l'API pour automatiser les opérations ou créer plusieurs entités plus rapidement (par exemple, les utilisateurs).

L'API de gestion des locataires utilise la plateforme d'API open source swagger. Swagger fournit une interface utilisateur intuitive qui permet aux développeurs et aux non-développeurs d'interagir avec l'API. L'interface utilisateur swagger fournit des détails complets et de la documentation pour chaque opération API.

Pour accéder à la documentation de swagger pour l'API de gestion des locataires :

## Étapes

1. Connectez-vous au Gestionnaire de locataires.
2. Sélectionnez **aide** > **Documentation API** dans l'en-tête Gestionnaire de locataires.

## Opérations d'API

L'API de gestion des locataires organise les opérations API disponibles dans les sections suivantes :

- **Compte** — opérations sur le compte de locataire actuel, y compris l'obtention des informations sur l'utilisation du stockage.
- **Auth** — opérations pour effectuer l'authentification de session utilisateur.

L'API de gestion des locataires prend en charge le schéma d'authentification par jeton Bearer. Pour une connexion locataire, vous fournissez un nom d'utilisateur, un mot de passe et un ID de compte dans le corps JSON de la demande d'authentification (c'est-à-dire, `POST /api/v3/authorize`). Si l'utilisateur est authentifié, un jeton de sécurité est renvoyé. Ce token doit être fourni dans l'en-tête des requêtes API suivantes (« autorisation : jeton porteur »).

Voir « protection contre la contrefaçon de demandes intersites » pour des informations sur l'amélioration de la sécurité de l'authentification.



Si l'authentification unique (SSO) est activée pour le système StorageGRID, vous devez effectuer différentes étapes pour l'authentification. Consultez la section « authentification dans l'API si l'authentification unique est activée » dans les instructions d'administration de StorageGRID.

- **Config** — opérations liées à la version du produit et aux versions de l'API tenant Management. Vous pouvez lister la version du produit ainsi que les versions principales de l'API prises en charge par cette version.
- **Conteneurs** — opérations sur des compartiments S3 ou des conteneurs Swift, comme suit :

Protocole	L'autorisation permet
S3	<ul style="list-style-type: none"> <li>• Création de compartiments conformes et non conformes</li> <li>• Modification des paramètres de conformité hérités</li> <li>• Définition du contrôle de cohérence pour les opérations effectuées sur les objets</li> <li>• Création, mise à jour et suppression de la configuration CORS d'un compartiment</li> <li>• Activation et désactivation des mises à jour de l'heure du dernier accès des objets</li> <li>• Gestion des paramètres de configuration des services de plateforme, y compris la réplication CloudMirror, les notifications et l'intégration de la recherche (notification-métadonnées)</li> <li>• Suppression de compartiments vides</li> </ul>
SWIFT	Définition du niveau de cohérence utilisé pour les conteneurs

- **DESACTIVE-fonctions** — opérations pour afficher les fonctions qui pourraient avoir été désactivées.
- **Noeuds finaux** — opérations pour gérer un noeud final. Les terminaux permettent à un compartiment S3 d'utiliser un service externe pour la réplication StorageGRID CloudMirror, les notifications ou l'intégration de la recherche.
- **Groupes** — opérations pour gérer des groupes de locataires locaux et extraire des groupes de locataires fédérés à partir d'un référentiel d'identité externe.
- **Identity-source** — opérations pour configurer un référentiel d'identité externe et synchroniser manuellement les informations de groupe et d'utilisateur fédérés.
- **Régions** — opérations pour déterminer les régions qui ont été configurées pour le système StorageGRID.
- **s3** — opérations pour gérer les clés d'accès S3 pour les utilisateurs locataires.
- **s3-Object-lock** — opérations pour déterminer comment le verrouillage d'objet S3 global (conformité) est configuré pour le système StorageGRID.
- **Utilisateurs** — opérations pour afficher et gérer les utilisateurs locataires.

## Détails de l'opération

Lorsque vous développez chaque opération d'API, vous pouvez voir son action HTTP, son URL de point final, une liste de tous les paramètres obligatoires ou facultatifs, un exemple du corps de la demande (si nécessaire) et les réponses possibles.

**groups**
Operations on groups

GET
/org/groups
Lists Tenant User Groups

Parameters
Try it out

Name	Description
<b>type</b> string (query)	filter by group type
<b>limit</b> integer (query)	maximum number of results
<b>marker</b> string (query)	marker-style pagination offset (value is Group's URN)
<b>includeMarker</b> boolean (query)	if set, the marker element is also returned
<b>order</b> string (query)	pagination order (desc requires marker)

Responses
Response content type
application/json

Code	Description
200	<div> Example Value Model </div> <pre>{   "responseTime": "2018-02-01T16:22:31.066Z",   "status": "success",   "apiVersion": "2.1" }</pre>

## Émission de requêtes API



Toutes les opérations d'API que vous effectuez à l'aide de la page Web API Docs sont des opérations en direct. Veuillez à ne pas créer, mettre à jour ou supprimer des données de configuration ou d'autres données par erreur.

### Étapes

1. Cliquez sur l'action HTTP pour afficher les détails de la demande.
2. Déterminez si la demande nécessite des paramètres supplémentaires, tels qu'un ID de groupe ou d'utilisateur. Ensuite, obtenir ces valeurs. Vous devrez peut-être d'abord lancer une autre demande d'API pour obtenir les informations dont vous avez besoin.
3. Déterminez si vous devez modifier l'exemple de corps de la demande. Si c'est le cas, vous pouvez cliquer

sur **modèle** pour connaître les exigences de chaque champ.

4. Cliquez sur **essayez-le**.
5. Fournir tous les paramètres requis ou modifier le corps de la demande selon les besoins.
6. Cliquez sur **Exécuter**.
7. Vérifiez le code de réponse pour déterminer si la demande a réussi.

#### Informations associées

["Protection contre la contrefaçon de demandes intersites \(CSRF\)"](#)

["Administrer StorageGRID"](#)

## Gestion des versions de l'API de gestion des locataires

L'API de gestion des locataires utilise la gestion des versions pour prendre en charge les mises à niveau sans interruption.

Par exemple, cette URL de demande spécifie la version 3 de l'API.

```
https://hostname_or_ip_address/api/v3/authorize
```

La version majeure de l'API de gestion des locataires est incrémentée lorsque des modifications sont effectuées, qui sont **non compatibles** avec des versions antérieures. La version mineure de l'API de gestion des locataires est incrémentée lorsque des modifications sont effectuées que **sont compatibles** avec des versions antérieures. Les modifications compatibles incluent l'ajout de nouveaux noeuds finaux ou de nouvelles propriétés. L'exemple suivant illustre comment la version de l'API est incrémentée en fonction du type de modifications apportées.

Type de modification de l'API	Ancienne version	Nouvelle version
Compatible avec les versions plus anciennes	2.1	2.2
Non compatible avec les versions plus anciennes	2.1	3.0

Lors de la première installation du logiciel StorageGRID, seule la version la plus récente de l'API de gestion des locataires est activée. Cependant, lorsque StorageGRID est mis à niveau vers une nouvelle version de fonction, vous continuez à accéder à l'ancienne version de l'API pour au moins une version de StorageGRID.

Les requêtes obsolètes sont marquées comme obsolètes de l'une des manières suivantes :

- L'en-tête de réponse est « obsolète : vrai »
- Le corps de la réponse JSON inclut « obsolète » : vrai

## Détermination des versions d'API prises en charge dans la version actuelle

Utilisez la requête d'API suivante pour renvoyer une liste des versions principales de l'API prises en charge :

```
GET https://{IP-Address}/api/versions
{
  "responseTime": "2019-01-10T20:41:00.845Z",
  "status": "success",
  "apiVersion": "3.0",
  "data": [
    2,
    3
  ]
}
```

## Spécification d'une version d'API pour une requête

Vous pouvez spécifier la version de l'API à l'aide d'un paramètre de chemin d'accès (/api/v3) ou un en-tête (Api-Version: 3). Si vous indiquez les deux valeurs, la valeur de l'en-tête remplace la valeur du chemin d'accès.

```
curl https://[IP-Address]/api/v3/grid/accounts

curl -H "Api-Version: 3" https://[IP-Address]/api/grid/accounts
```

## Protection contre la contrefaçon de demandes intersites (CSRF)

Vous pouvez vous protéger contre les attaques de contrefaçon de requêtes intersites (CSRF) contre StorageGRID en utilisant des jetons CSRF pour améliorer l'authentification qui utilise des cookies. Grid Manager et tenant Manager activent automatiquement cette fonction de sécurité ; les autres clients API peuvent choisir de l'activer lorsqu'ils se connectent.

Un attaquant pouvant déclencher une requête vers un autre site (par exemple avec UN POST de formulaire HTTP) peut créer certaines requêtes à l'aide des cookies de l'utilisateur connecté.

StorageGRID contribue à la protection contre les attaques CSRF en utilisant des jetons CSRF. Lorsque cette option est activée, le contenu d'un cookie spécifique doit correspondre au contenu d'un en-tête spécifique ou d'un paramètre DE CORPS POST spécifique.

Pour activer la fonction, définissez l' `csrfToken` paramètre à `true` pendant l'authentification. La valeur par défaut est `false`.

```
curl -X POST --header "Content-Type: application/json" --header "Accept: application/json" -d "{
  \"username\": \"MyUserName\",
  \"password\": \"MyPassword\",
  \"cookie\": true,
  \"csrfToken\": true
}" "https://example.com/api/v3/authorize"
```

Si vrai, un `GridCsrfToken` Le cookie est défini avec une valeur aléatoire pour les connexions dans Grid Manager et dans `AccountCsrfToken` Le cookie est défini avec une valeur aléatoire pour les connexions au Gestionnaire de locataires.

Si le cookie est présent, toutes les demandes pouvant modifier l'état du système (POST, PUT, PATCH, DELETE) doivent inclure l'une des options suivantes :

- Le `X-Csrf-Token` En-tête, avec la valeur de l'en-tête définie sur la valeur du cookie de jeton CSRF.
- Pour les noeuds finaux qui acceptent un corps codé par formulaire : a `csrfToken` paramètre corps de demande codé par formulaire.

Reportez-vous à la documentation en ligne de l'API pour obtenir des exemples et des détails supplémentaires.



Les demandes disposant d'un jeu de cookies de jeton CSRF appliquent également le `"Content-Type: application/json"` En-tête pour toute demande qui attend un corps de requête JSON comme une protection supplémentaire contre les attaques CSRF.



## 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.