# API de gestion des locataires

StorageGRID software

NetApp
December 03, 2025

# Sommaire

# API de gestion des locataires

## Comprendre l'API de gestion des locataires

Vous pouvez effectuer des tâches de gestion du système à l'aide de l'API REST de gestion des locataires au lieu de l'interface utilisateur du gestionnaire des locataires. Par exemple, vous souhaiterez peut-être utiliser l'API pour automatiser des opérations ou créer plusieurs entités, telles que des utilisateurs, plus rapidement.

L'API de gestion des locataires :

- Utilise la plateforme 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 de Swagger fournit des détails complets et une documentation pour chaque opération API.
- Utilisations"gestion des versions pour prendre en charge les mises à niveau non perturbatrices" .

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

1. Sign in au gestionnaire de locataires.
2. En haut du gestionnaire de locataires, sélectionnez l'icône d'aide et sélectionnez **Documentation API**.

### Opérations API

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

- **compte** : opérations sur le compte locataire actuel, y compris l'obtention d'informations sur l'utilisation du stockage.
- **auth** : opérations permettant d'effectuer l'authentification de la session utilisateur.

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

  Pour plus d'informations sur l'amélioration de la sécurité de l'authentification, consultez"Protection contre la falsification de requêtes intersites" .

  > Si l'authentification unique (SSO) est activée pour le système StorageGRID , vous devez effectuer différentes étapes pour vous authentifier. Voir le"instructions d'utilisation de l'API de gestion de grille" .

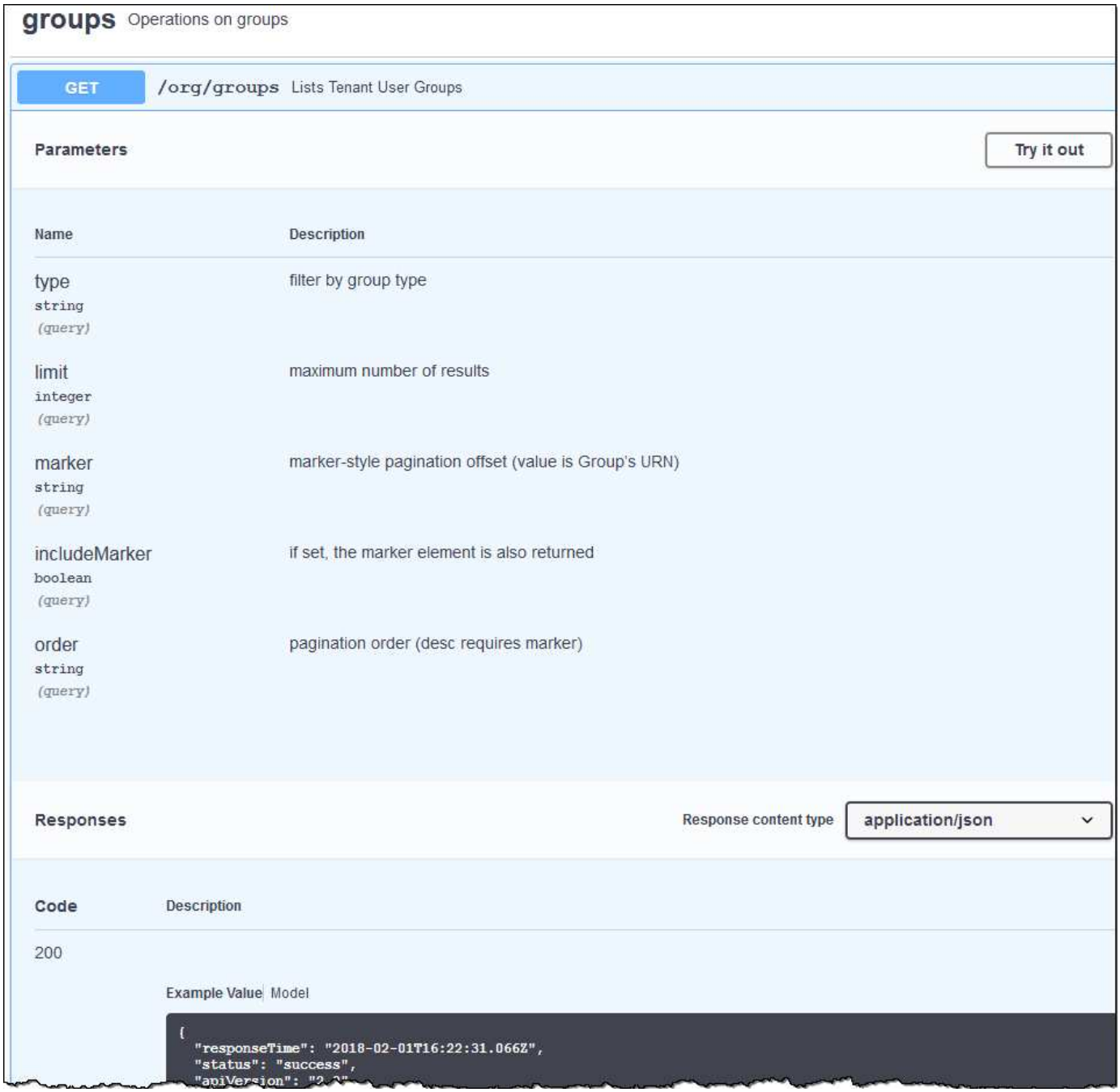
- **config** : opérations liées à la version du produit et aux versions de l'API de gestion des locataires. Vous pouvez répertorier la version du produit et les principales versions de l'API prises en charge par cette version.
- **conteneurs** : opérations sur les buckets S3 ou les conteneurs Swift.
- **fonctionnalités désactivées** : opérations permettant d'afficher les fonctionnalités qui pourraient avoir été désactivées.
- **points de terminaison** : opérations permettant de gérer un point de terminaison. Les points de

terminaison permettent à un bucket S3 d'utiliser un service externe pour la réplication StorageGRID CloudMirror, les notifications ou l'intégration de la recherche.

- **grid-federation-connections** : opérations sur les connexions de fédération de grille et la réplication inter-grille.
- **groupes** : opérations de gestion des groupes de locataires locaux et de récupération des groupes de locataires fédérés à partir d'une source d'identité externe.
- **identity-source** : opérations permettant de configurer une source d'identité externe et de synchroniser manuellement les informations des groupes fédérés et des utilisateurs.
- **ilm** : opérations sur les paramètres de gestion du cycle de vie de l'information (ILM).
- **régions** : opérations permettant de déterminer quelles régions ont été configurées pour le système StorageGRID .
- **s3** : opérations de gestion des clés d'accès S3 pour les utilisateurs locataires.
- **s3-object-lock** : opérations sur les paramètres globaux de verrouillage d'objet S3, utilisées pour prendre en charge la conformité réglementaire.
- **utilisateurs** : opérations permettant d'afficher et de gérer les utilisateurs locataires.

## Détails de l'opération

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




## Émettre des requêtes API

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

**Étapes**

1. Sélectionnez l'action HTTP pour voir les détails de la demande.
2. Déterminez si la demande nécessite des paramètres supplémentaires, tels qu'un ID de groupe ou d'utilisateur. Ensuite, obtenez ces valeurs. Vous devrez peut-être d'abord émettre une demande d'API différente pour obtenir les informations dont vous avez besoin.
3. Déterminez si vous devez modifier le corps de la demande d'exemple. Si tel est le cas, vous pouvez sélectionner **Modèle** pour connaître les exigences de chaque champ.

4. Sélectionnez **Essayer**.
5. Fournissez tous les paramètres requis ou modifiez le corps de la demande selon vos besoins.
6. Sélectionnez **Exécuter**.
7. Consultez le code de réponse pour déterminer si la demande a réussi.

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

## L'API de gestion des locataires utilise le contrôle de version pour prendre en charge les mises à niveau sans interruption.

Par exemple, cette URL de demande spécifie la version 4 de l'API.

`https://hostname_or_ip_address/api/v4/authorize`

La version principale de l'API est mise à jour lorsque des modifications sont apportées qui ne sont pas compatibles avec les versions plus anciennes. La version mineure de l'API est mise à jour lorsque des modifications sont apportées qui sont *compatibles* avec les versions plus anciennes. Les modifications compatibles incluent l'ajout de nouveaux points de terminaison ou de nouvelles propriétés.

L'exemple suivant illustre comment la version de l'API est augmentée en fonction du type de modifications apportées.

| Type de modification de l'API | Ancienne version | Nouvelle version |
|---|---|---|
| Compatible avec les anciennes versions | 2,1 | 2,2 |
| Non compatible avec les anciennes versions | 2,1 | 3,0 |

Lorsque vous installez le logiciel StorageGRID pour la première fois, seule la version la plus récente de l'API est activée. Cependant, lorsque vous effectuez une mise à niveau vers une nouvelle version de fonctionnalité de StorageGRID, vous continuez à avoir accès à l'ancienne version de l'API pour au moins une version de fonctionnalité de StorageGRID .

> Vous pouvez configurer les versions prises en charge. Consultez la section **config** de la documentation de l'API Swagger pour le"API de gestion de grille" pour plus d'informations. Vous devez désactiver la prise en charge de l'ancienne version après avoir mis à jour tous les clients API pour utiliser la version la plus récente.

Les demandes obsolètes sont marquées comme obsolètes des manières suivantes :

- L'en-tête de réponse est « Obsolète : vrai »
- Le corps de la réponse JSON inclut « obsolète » : vrai
- Un avertissement obsolète est ajouté à nms.log. Par exemple:

```
Received call to deprecated v2 API at POST "/api/v2/authorize"
```

### Déterminer quelles versions d'API sont prises en charge dans la version actuelle

Utilisez le `GET /versions` Requête d'API pour renvoyer une liste des versions majeures d'API prises en charge. Cette demande se trouve dans la section **config** de la documentation de l'API Swagger.

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2023-06-27T22:13:50.750Z",
  "status": "success",
  "apiVersion": "4.0",
  "data": [
    2,
    3,
    4
  ]
}
```

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

Vous pouvez spécifier la version de l'API à l'aide d'un paramètre de chemin(`/api/v4` ) ou un en-tête(`Api-Version: 4` ). Si vous fournissez les deux valeurs, la valeur de l'en-tête remplace la valeur du chemin.

```
curl https://[IP-Address]/api/v4/grid/accounts

curl -H "Api-Version: 4" https://[IP-Address]/api/grid/accounts
```

# Protection contre la falsification de requêtes intersites (CSRF)

Vous pouvez contribuer à vous protéger contre les attaques de falsification de requête intersite (CSRF) contre StorageGRID en utilisant des jetons CSRF pour améliorer l'authentification qui utilise des cookies. Le gestionnaire de grille et le gestionnaire de locataires activent automatiquement cette fonctionnalité de sécurité ; les autres clients API peuvent choisir de l'activer ou non lorsqu'ils se connectent.

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

StorageGRID aide à se protéger contre les attaques CSRF en utilisant des jetons CSRF. Lorsqu'elle 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 fonctionnalité, définissez le `csrfToken` paramètre à `true` lors de 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"
```

Lorsque c'est vrai, un `GridCsrfToken` Le cookie est défini avec une valeur aléatoire pour les connexions au Grid Manager, et le `AccountCsrfToken` le cookie est défini avec une valeur aléatoire pour les connexions au Tenant Manager.

Si le cookie est présent, toutes les requêtes pouvant modifier l'état du système (POST, PUT, PATCH, DELETE) doivent inclure l'un des éléments suivants :

- Le `X-Csrf-Token` en-tête, avec la valeur de l'en-tête définie sur la valeur du cookie de jeton CSRF.
- Pour les points de terminaison qui acceptent un corps codé par formulaire : A `csrfToken` paramètre de corps de requête codé par formulaire.

Pour configurer la protection CSRF, utilisez le"API de gestion de grille" ou"API de gestion des locataires" .

> Les requêtes qui ont un cookie de jeton CSRF défini appliqueront également l'en-tête « Content-Type : application/json » pour toute requête qui attend un corps de requête JSON comme protection supplémentaire contre les attaques CSRF.

## Informations sur le copyright



## Informations sur les marques commerciales