



API de gestion des locataires

StorageGRID software

NetApp
July 23, 2026

Sommaire

- API de gestion des locataires 1
 - Découvrez l'API de gestion des locataires StorageGRID 1
 - `${post_edited_translations.segment}` 1
 - `${post_edited_translations.segment}` 2
 - Émettre des requêtes API 3
 - Versionnage de l'API de gestion des locataires StorageGRID 4
 - Déterminez quelles versions d'API sont prises en charge dans la version actuelle 5
 - Spécifiez une version d'API pour une requête 5
 - Protégez-vous contre la falsification de requêtes intersites (CSRF) dans StorageGRID 5

API de gestion des locataires

Découvrez l'API de gestion des locataires StorageGRID

Vous pouvez effectuer des tâches de gestion système à l'aide de l'API REST Tenant Management plutôt qu'en utilisant l'interface utilisateur du Tenant Manager. Par exemple, vous pourriez vouloir utiliser l'API pour automatiser des opérations ou pour créer plusieurs entités, telles que des utilisateurs, plus rapidement.

`${post_edited_translations.segment}`

- Utilisez 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 de Swagger fournit des détails complets et de la documentation pour chaque opération d'API.
- Utilisez `"${post_edited_translations.segment}"`.

`${post_edited_translations.segment}`

1. Connectez-vous au Tenant Manager.
2. En haut du Tenant Manager, sélectionnez l'icône d'aide et sélectionnez **API documentation**.

`${post_edited_translations.segment}`

`${post_edited_translations.segment}`

- `${post_edited_translations.segment}`
- **auth** : Opérations permettant d'authentifier la session utilisateur.

L'API de gestion des locataires prend en charge le schéma d'authentification par jeton Bearer. Pour la connexion d'un 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 demandes d'API ultérieures ("Authorization: Bearer token").

Pour obtenir des informations sur l'amélioration de la sécurité de l'authentification, consultez ["Protégez-vous contre la falsification de requêtes intersites"](#).



Si l'authentification unique (SSO) est activée pour le système StorageGRID, vous devez effectuer des étapes différentes pour vous authentifier. Voir le `"${post_edited_translations.segment}"`.

- **config** : opérations relatives à la version du produit et aux versions de l'API de gestion des locataires. Vous pouvez lister la version du produit et les versions majeures de l'API prises en charge par cette version.
- `${post_edited_translations.segment}`
- **Fonctionnalités désactivées** : Opérations permettant d'afficher les fonctionnalités qui pourraient avoir été désactivées.
- **endpoints** : opérations de gestion d'un point de terminaison. Les points de terminaison permettent à un compartiment S3 d'utiliser un service externe pour la réplication CloudMirror de StorageGRID, les

notifications ou l'intégration de la recherche.

- `${post_edited_translations.segment}`
- **Groupes** : Opérations permettant de gérer les groupes de locataires locaux et de récupérer les groupes de locataires fédérés à partir d'une source d'identité externe.
- **identity-source** : Opérations permettant de configurer une source d'identité externe et de synchroniser manuellement les informations de groupe et d'utilisateur fédérés.
- **ilm** : Opérations sur les paramètres de gestion du cycle de vie de l'information (ILM).
- `${post_edited_translations.segment}`
- `${post_edited_translations.segment}`
- `${post_edited_translations.segment}`
- **utilisateurs** : Opérations permettant de consulter et de gérer les utilisateurs locataires.

`${post_edited_translations.segment}`

`${post_edited_translations.segment}`

groups
Operations on groups

GET
/org/groups
Lists Tenant User Groups

Parameters
Try it out

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

Responses
Response content type
application/json

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

Émettre des requêtes API



Toute opération API effectuée via la page de documentation API est une opération en direct. Veuillez à ne pas créer, modifier ou supprimer par erreur des données de configuration ou autres.

Étapes

1. Sélectionnez l'action HTTP pour afficher les détails de la requête.
2. Déterminez si la requête nécessite des paramètres supplémentaires, tels qu'un identifiant de groupe ou d'utilisateur. Ensuite, obtenez ces valeurs. Vous devrez peut-être d'abord effectuer une autre requête API pour obtenir les informations dont vous avez besoin.
3. Déterminez si vous devez modifier le corps de la requête d'exemple. Le cas échéant, vous pouvez sélectionner **Modèle** pour connaître les exigences relatives à chaque champ.

4. Sélectionnez **Try it out**.
5. Fournissez les paramètres requis ou modifiez le corps de la requête selon les besoins.
6. Sélectionnez **Exécuter**.
7. Examinez le code de réponse pour déterminer si la requête a réussi.

Versionnage de l'API de gestion des locataires StorageGRID

L'API de gestion des locataires utilise le versionnage pour permettre des mises à niveau sans interruption de service.

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

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

La version majeure de l'API est mise à jour lorsque des modifications qui ne sont pas compatibles avec les versions précédentes sont apportées. La version mineure de l'API est mise à jour lorsque des modifications qui sont compatibles avec les versions précédentes sont apportées. 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 incrémentée en fonction du type de modifications apportées.

Type de modification de l'API	Ancienne version	Nouvelle version
Compatible avec les versions antérieures	2,1	2,2
Non compatible avec les versions antérieures	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 StorageGRID, vous continuez à avoir accès à l'ancienne version de l'API pendant au moins une version de StorageGRID.



Vous pouvez configurer les versions prises en charge. Consultez la section **config** de la documentation de l'API Swagger pour "[API de gestion de grille](#)" plus d'informations. Vous devez désactiver la prise en charge de l'ancienne version après avoir mis à jour tous les clients API vers la nouvelle version.

Les requêtes obsolètes sont marquées comme dépréciées de la manière suivante :

- L'en-tête de réponse est « Deprecated: true »
- Le corps de la réponse JSON inclut "deprecated": true
- Un avertissement de dépréciation est ajouté au fichier nms.log. Par exemple :

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

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

Utilisez la `GET /versions` requête API pour obtenir une liste des versions majeures de l'API prises en charge. Cette requête 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
  ]
}
```

Spécifiez 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 d'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
```

Protégez-vous contre la falsification de requêtes intersites (CSRF) dans StorageGRID

Vous pouvez contribuer à protéger StorageGRID contre les attaques de type Cross-Site Request Forgery (CSRF) en utilisant des jetons CSRF pour renforcer l'authentification qui utilise des cookies. Le Grid Manager et le Tenant Manager activent automatiquement cette fonctionnalité de sécurité ; les autres clients API peuvent choisir de l'activer ou non lors de leur connexion.

Un attaquant capable de déclencher une requête vers un autre site (par exemple avec un formulaire HTTP POST) peut faire en sorte que certaines requêtes soient effectuées en utilisant les cookies de l'utilisateur connecté.

StorageGRID contribue à la protection contre les attaques CSRF grâce à l'utilisation de jetons CSRF. Lorsqu'elle est activée, le contenu d'un cookie spécifique doit correspondre à celui d'un en-tête spécifique ou d'un paramètre spécifique du corps de la requête POST.

Pour activer cette fonctionnalité, définissez le paramètre `csrfToken` sur `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 cette option est activée, un `GridCsrfToken` cookie est défini avec une valeur aléatoire pour les connexions au Grid Manager, et le `AccountCsrfToken` cookie est défini avec une valeur aléatoire pour les connexions au Tenant Manager.

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

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

Pour configurer la protection CSRF, utilisez le ["API de gestion de grille"](#) ou le ["API de gestion des locataires"](#).



Les requêtes comportant un cookie de jeton CSRF défini appliqueront également l'en-tête `"Content-Type: application/json"` à toute requête attendant un corps de requête JSON, comme protection supplémentaire contre les attaques CSRF.

Informations sur le copyright

Copyright © 2026 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.