À l'aide du Gestionnaire de locataires

StorageGRID

NetApp
October 03, 2025

This PDF was generated from https://docs.netapp.com/fr-fr/storagegrid-115/tenant/web-browser-requirements.html on October 03, 2025. Always check docs.netapp.com for the latest.

Sommaire

À l'aide du Gestionnaire de locataires . . . 1
- Utilisation d'un compte de locataire StorageGRID . . . 1
  - Création de comptes de tenant . . . 1
  - Configuration des locataires S3 . . . 2
  - Configuration des locataires Swift . . . 2
- Navigateurs Web pris en charge . . . 3
- Connexion au Gestionnaire de locataires . . . 3
- Déconnexion du Gestionnaire de locataires . . . 6
- Présentation du tableau de bord de tenant Manager . . . 6
  - Récapitulatif du compte de locataire . . . 7
  - Utilisation du stockage et des quotas . . . 8
  - Alertes d'utilisation des quotas . . . 9
  - Erreurs de point final . . . 9
- Présentation de l'API de gestion des locataires . . . 9
  - Opérations d'API . . . 10
  - Détails de l'opération . . . 11
  - Émission de requêtes API . . . 12
  - Gestion des versions de l'API de gestion des locataires . . . 13
  - Protection contre la contrefaçon de demandes intersites (CSRF) . . . 14

À l'aide du Gestionnaire de locataires

Le gestionnaire de locataires permet de gérer tous les aspects d'un compte de locataire StorageGRID.

Vous pouvez utiliser le gestionnaire des locataires pour surveiller l'utilisation du stockage d'un compte de locataire et gérer les utilisateurs avec une fédération des identités ou en créant des groupes et des utilisateurs locaux. Pour les comptes locataires S3, vous pouvez également gérer des clés S3, gérer des compartiments S3 et configurer les services de plateforme.

Utilisation d'un compte de locataire StorageGRID

Un compte de locataire vous permet d'utiliser l'API REST S3 (simple Storage Service) ou l'API REST Swift pour stocker et récupérer des objets dans un système StorageGRID.

Chaque compte de locataire possède ses propres groupes, utilisateurs, compartiments S3, conteneurs Swift et objets fédérés.

Il est possible d'utiliser des comptes de tenant pour isoler les objets stockés par différentes entités. Par exemple, vous pouvez utiliser plusieurs comptes locataires pour l'une de ces utilisations :

- **Utilisation en entreprise :** si le système StorageGRID est utilisé au sein d'une entreprise, le stockage objet de la grille peut être séparé par les différents services de l'organisation. Par exemple, il peut y avoir des comptes de tenant pour le service Marketing, le service Customer support, le service des ressources humaines, etc.

  > Si vous utilisez le protocole client S3, vous pouvez également utiliser des compartiments S3 et des règles de compartiment pour isoler les objets entre les différents départements d'une entreprise. Il n'est pas nécessaire de créer des comptes de tenant distincts. Voir les instructions d'implémentation des applications client S3.

- **Cas d'utilisation du fournisseur de services :** si le système StorageGRID est utilisé par un fournisseur de services, le stockage objet de la grille peut être séparé par les différentes entités qui louent le stockage. Il peut s'agir, par exemple, de comptes de locataires pour la société A, la société B, la société C, etc.

Création de comptes de tenant

Les comptes de locataires sont créés par un administrateur grid StorageGRID à l'aide de Grid Manager. Lors de la création d'un compte de locataire, 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).
- Si le compte de locataire utilise S3 ou Swift.
- Pour les comptes de locataire S3 : si le compte de locataire est autorisé à utiliser des services de plateforme. Si l'utilisation des services de plateforme est autorisée, la grille doit être configurée pour prendre en charge leur utilisation.
- 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 la fédération des identités est activée pour le système StorageGRID, quel groupe fédéré a l'autorisation

d'accès racine pour configurer le compte de tenant.

- 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.

En outre, les administrateurs du grid peuvent activer le paramètre de verrouillage objet S3 pour le système StorageGRID si les comptes de locataires S3 doivent être conformes aux exigences réglementaires. Lorsque le verrouillage des objets S3 est activé, tous les comptes de locataires S3 peuvent créer et gérer des compartiments conformes.

Configuration des locataires S3

Une fois le compte de locataire S3 créé, vous pouvez accéder au Gestionnaire des locataires pour effectuer les tâches suivantes :

- Configuration de la fédération des identités (sauf si le référentiel d'identité est partagé avec la grille) ou création de groupes et d'utilisateurs locaux
- Gestion des clés d'accès S3
- Création et gestion des compartiments S3, notamment des compartiments conformes
- Utilisation des services de plate-forme (si activé)
- Contrôle de l'utilisation du stockage

> Vous pouvez créer et gérer des compartiments S3 avec le Gestionnaire des locataires. Toutefois, vous devez disposer de clés d'accès S3 et utiliser l'API REST S3 pour ingérer et gérer les objets.

Configuration des locataires Swift

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"

"Utilisation de S3"

"Utiliser Swift"

Navigateurs Web pris en charge

Vous devez utiliser un navigateur Web pris en charge.

Navigateur Web	Version minimale prise en charge
Google Chrome	87
Microsoft Edge	87
Mozilla Firefox	84

Vous devez régler la fenêtre du navigateur sur une largeur recommandée.

Largeur du navigateur	Pixels
Minimum	1024
Optimale	1280

Connexion au Gestionnaire de locataires

Pour accéder au Gestionnaire de locataires, entrez l'URL du locataire dans la barre d'adresse d'un navigateur Web pris en charge.

Ce dont vous avez besoin

- Vous devez disposer de vos identifiants de connexion.
- Vous devez disposer d'une URL pour accéder au Gestionnaire de locataires, telle que fournie par votre administrateur de grid. L'URL se présente comme l'un de ces exemples :

```
https://FQDN_or_Admin_Node_IP/
```

```
https://FQDN_or_Admin_Node_IP:port/
```

```
https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id
```

```
https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id
```

L'URL contient toujours le nom de domaine complet (FQDN) ou l'adresse IP utilisée pour accéder à un nœud d'administration, et peut également inclure un numéro de port, l'ID de compte de locataire à 20 chiffres, ou les deux.

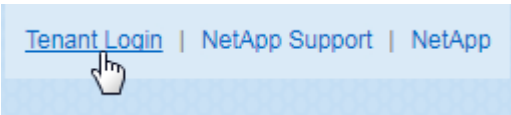
- Si l'URL n'inclut pas l'ID de compte à 20 chiffres du locataire, vous devez avoir cet ID de compte.
- Vous devez utiliser un navigateur Web pris en charge.
- Les cookies doivent être activés dans votre navigateur Web.
- Vous devez disposer d'autorisations d'accès spécifiques.

Étapes

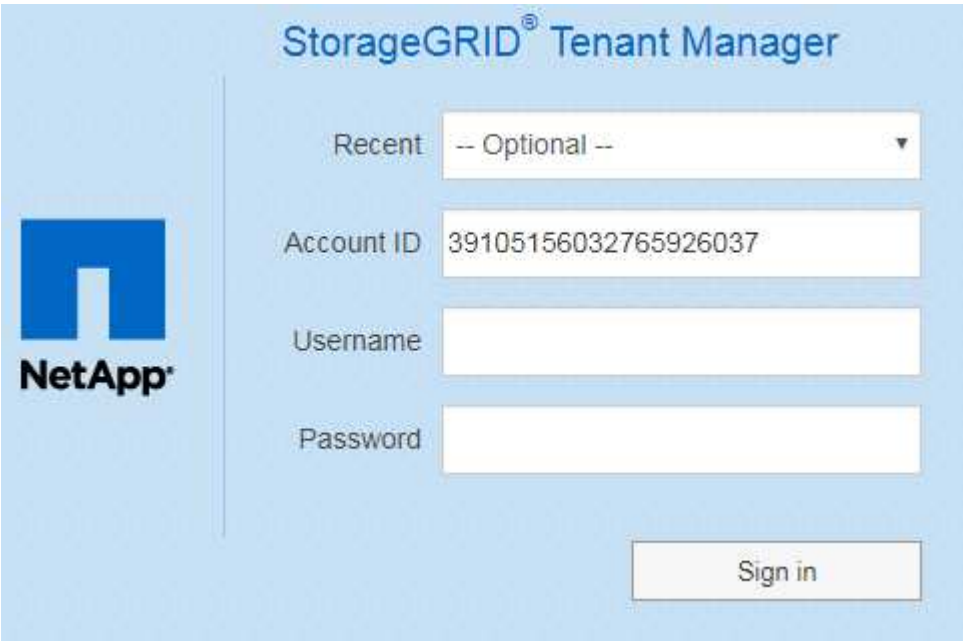
1. Lancez un navigateur Web pris en charge.
2. Dans la barre d'adresse du navigateur, entrez l'URL d'accès au Gestionnaire de locataires.
3. Si vous êtes invité à recevoir une alerte de sécurité, installez le certificat à l'aide de l'assistant d'installation du navigateur.
4. Connectez-vous au Gestionnaire de locataires.

   L'écran de connexion que vous voyez dépend de l'URL que vous avez saisie et de l'utilisation de SSO (Single Sign-on) par votre organisation. Vous verrez l'un des écrans suivants :

   - Page de connexion de Grid Manager. Cliquez sur le lien **tenant Login** dans le coin supérieur droit.

   - Page de connexion du Gestionnaire de locataires. Le champ **ID de compte** peut déjà être complété, comme indiqué ci-dessous.

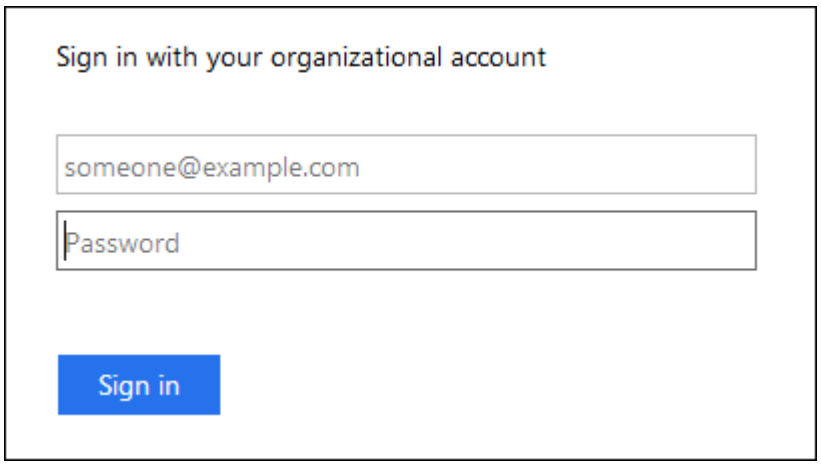
     i. Si l'ID de compte à 20 chiffres du locataire ne s'affiche pas, sélectionnez le nom du compte du locataire s'il apparaît dans la liste des comptes récents ou saisissez l'ID du compte.

     ii. Saisissez votre nom d'utilisateur et votre mot de passe.

     iii. Cliquez sur **connexion**.

     Le tableau de bord de tenant Manager s'affiche.

◦ La page SSO de votre entreprise, si SSO est activé sur le grid. Par exemple :



Entrez vos informations d'identification SSO standard, puis cliquez sur **connexion**.

◦ Page de connexion SSO du Gestionnaire de locataires.

i. Si l'ID de compte à 20 chiffres du locataire ne s'affiche pas, sélectionnez le nom du compte du locataire s'il apparaît dans la liste des comptes récents ou saisissez l'ID du compte.

ii. Cliquez sur **connexion**.

iii. Connectez-vous à l'aide de vos identifiants SSO standard sur la page de connexion SSO de votre entreprise.

Le tableau de bord de tenant Manager s'affiche.

5. Si vous avez reçu un mot de passe initial de quelqu'un d'autre, modifiez votre mot de passe pour sécuriser votre compte. Sélectionnez ***username*** > **Modifier le mot de passe**.

> Si l'authentification SSO est activée pour le système StorageGRID, vous ne pouvez pas modifier votre mot de passe à partir du Gestionnaire de locataires.

Informations associées

"Administrer StorageGRID"

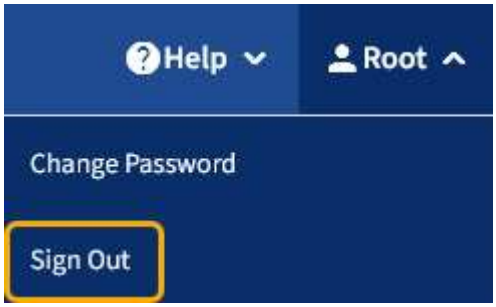
"Navigateurs Web pris en charge"

Déconnexion du Gestionnaire de locataires

Lorsque vous avez terminé de travailler avec le Gestionnaire de locataires, vous devez vous déconnecter pour vous assurer que les utilisateurs non autorisés ne peuvent pas accéder au système StorageGRID. La fermeture de votre navigateur risque de ne pas vous déconnecter du système, en fonction des paramètres des cookies du navigateur.

Étapes

1. Localisez la liste déroulante Nom d'utilisateur dans le coin supérieur droit de l'interface utilisateur.



2. Sélectionnez le nom d'utilisateur, puis **Déconnexion**.

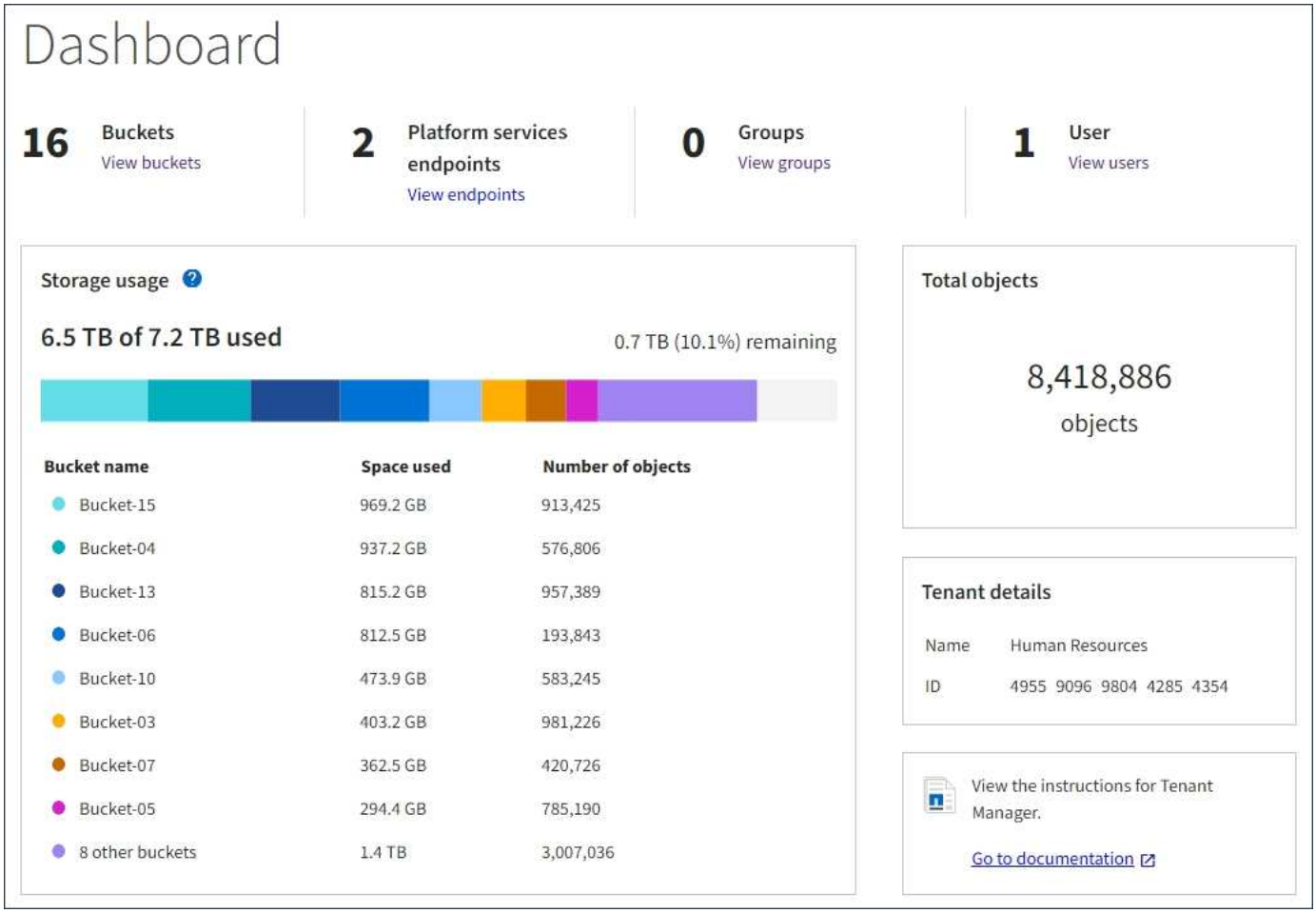
Option	Description
SSO non utilisé	Vous êtes déconnecté du nœud d'administration. La page de connexion au Gestionnaire de locataires s'affiche. **Remarque :** si vous vous êtes connecté à plusieurs nœuds d'administration, vous devez vous déconnecter de chaque nœud.
SSO activé	Vous êtes déconnecté de tous les nœuds d'administration auxquels vous accédiez. La page de connexion StorageGRID s'affiche. Le nom du compte de locataire que vous venez d'accéder est indiqué par défaut dans la liste déroulante **comptes récents** et le **ID de compte** du locataire s'affiche. **Remarque :** si SSO est activé et que vous êtes également connecté à Grid Manager, vous devez également vous déconnecter de Grid Manager pour vous déconnecter de SSO.

Présentation du tableau de bord de tenant Manager

Le tableau de bord de tenant Manager présente la configuration des comptes d'un locataire ainsi que la quantité d'espace utilisé par les objets dans les compartiments (S3) ou les conteneurs (Swift) du locataire. Si le locataire dispose d'un quota, le tableau de bord affiche la part du quota utilisée et la quantité restante. En cas d'erreurs liées au compte du locataire, les erreurs sont affichées sur le tableau de bord.

Les valeurs espace utilisé sont des estimations. Ces estimations sont affectées par le moment de l'ingestion, la connectivité réseau et l'état des nœuds.

Lorsque des objets ont été téléchargés, le Tableau de bord ressemble à l'exemple suivant :



Récapitulatif du compte de locataire

La partie supérieure du tableau de bord contient les informations suivantes :

- Le nombre de compartiments ou de conteneurs configurés, de groupes et d'utilisateurs
- Le nombre de terminaux de services de plate-forme, le cas échéant, ont été configurés

Vous pouvez sélectionner les liens pour afficher les détails.

La partie droite du tableau de bord contient les informations suivantes :

- Nombre total d'objets pour le locataire.

  Pour un compte S3, si aucun objet n'a été ingéré et que vous disposez de l'autorisation d'accès racine, les instructions relatives à la mise en route s'affichent au lieu du nombre total d'objets.

- Nom et ID du compte de locataire.
- Un lien vers la documentation StorageGRID.

Utilisation du stockage et des quotas

Le panneau utilisation du stockage contient les informations suivantes :

- Volume des données d'objet pour le locataire.

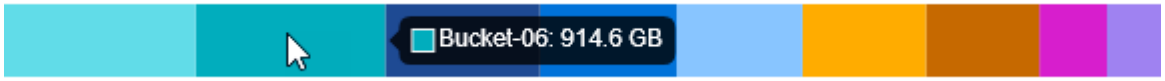
  Cette valeur indique la quantité totale de données d'objet chargées et ne représente pas l'espace utilisé pour stocker les copies de ces objets et leurs métadonnées.

- Si un quota est défini, la quantité totale d'espace disponible pour les données d'objet ainsi que la quantité et le pourcentage d'espace restant. Le quota limite la quantité de données d'objet pouvant être ingérées.

  L'utilisation des quotas est basée sur des estimations internes et peut être dépassée dans certains cas. Par exemple, StorageGRID vérifie le quota lorsqu'un locataire commence à charger des objets et rejette les nouvelles ingère si le locataire a dépassé le quota. Cependant, StorageGRID ne prend pas en compte la taille du téléchargement actuel lors de la détermination du dépassement du quota. Si des objets sont supprimés, un locataire peut être temporairement empêché de charger de nouveaux objets jusqu'à ce que l'utilisation des quotas soit recalculée. Le calcul de l'utilisation des quotas peut prendre au moins 10 minutes.

- Un graphique à barres qui représente les tailles relatives des grands godets ou conteneurs.

  Vous pouvez placer le curseur sur n'importe quel segment de graphique pour afficher l'espace total utilisé par ce compartiment ou ce conteneur.



- Pour correspondre au graphique à barres, une liste des plus grands seaux ou conteneurs, y compris la quantité totale de données d'objet et le nombre d'objets pour chaque godet ou conteneur.

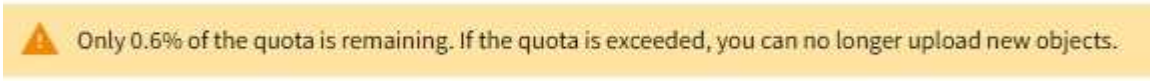
Bucket name	Space used	Number of objects
Bucket-02	944.7 GB	7,575
Bucket-09	899.6 GB	589,677
Bucket-15	889.6 GB	623,542
Bucket-06	846.4 GB	648,619
Bucket-07	730.8 GB	808,655
Bucket-04	700.8 GB	420,493
Bucket-11	663.5 GB	993,729
Bucket-03	656.9 GB	379,329
9 other buckets	2.3 TB	5,171,588

Si le locataire possède plus de neuf compartiments ou conteneurs, tous les autres compartiments ou conteneurs sont regroupés en une seule entrée au bas de la liste.

Alertes d'utilisation des quotas

Si les alertes d'utilisation des quotas ont été activées dans Grid Manager, elles s'affichent dans le Gestionnaire de locataires lorsque le quota est faible ou dépassé, comme suit :

Si 90 % ou plus du quota d'un locataire a été utilisé, l'alerte **usage du quota de locataire élevé** est déclenchée. Pour plus d'informations, consultez la référence des alertes dans les instructions de surveillance et de dépannage de StorageGRID.

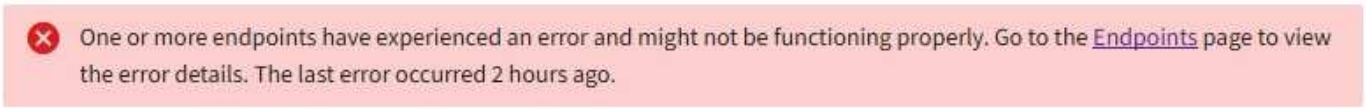


Si vous dépassez votre quota, vous ne pouvez pas télécharger de nouveaux objets.

Pour afficher des informations supplémentaires et gérer les règles et notifications relatives aux alertes, reportez-vous aux instructions de surveillance et de dépannage de StorageGRID.

Erreurs de point final

Si vous avez utilisé Grid Manager pour configurer un ou plusieurs terminaux pour les services de plateforme, le tableau de bord du Gestionnaire de locataires affiche une alerte si des erreurs de point final se sont produites au cours des sept derniers jours.



Pour afficher des détails sur une erreur de point final, sélectionnez noeuds finaux pour afficher la page noeuds finaux.

Informations associées

"Dépannage des erreurs de point final des services de plate-forme"

"Moniteur et amp ; dépannage"

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 :

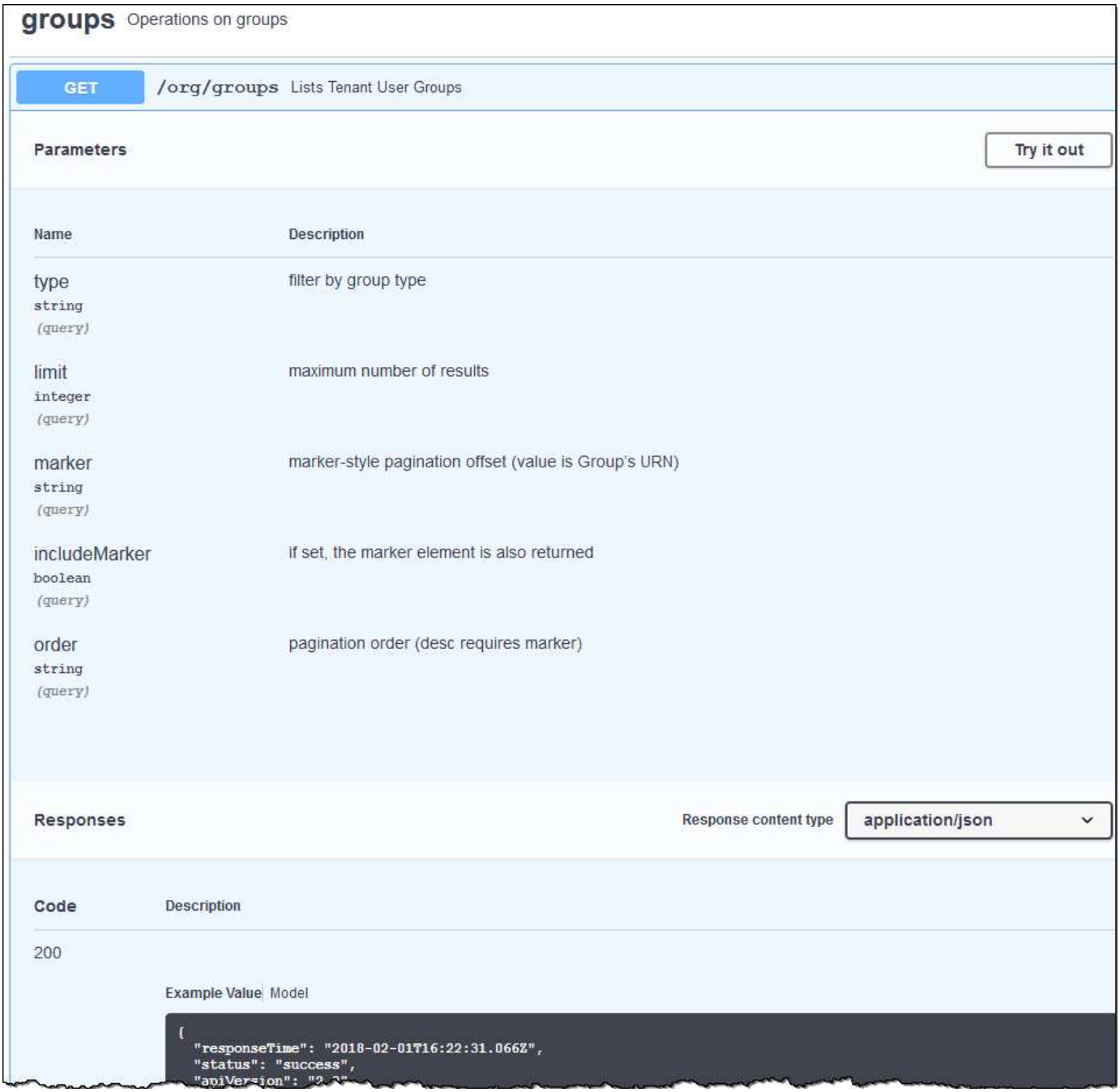
Protocole	L'autorisation permet
S3	• Création de compartiments conformes et non conformes • Modification des paramètres de conformité hérités • Définition du contrôle de cohérence pour les opérations effectuées sur les objets • Création, mise à jour et suppression de la configuration CORS d'un compartiment • Activation et désactivation des mises à jour de l'heure du dernier accès des objets • Gestion des paramètres de configuration des services de plateforme, y compris la réplication CloudMirror, les notifications et l'intégration de la recherche (notification-métadonnées) • Suppression de compartiments vides

Protocole	L'autorisation permet
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.



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. Veillez 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 © 2025 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 DÉLICTUELLE (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.