



# API de gerenciamento do locatário

## StorageGRID

NetApp  
March 12, 2025

# Índice

API de gerenciamento do locatário .....	1
Entenda a API de gerenciamento do locatário .....	1
Operações da API .....	1
Detalhes da operação .....	2
Emitir solicitações de API .....	3
Controle de versão da API de gerenciamento de locatário .....	4
Determine quais versões de API são suportadas na versão atual .....	5
Especifique uma versão da API para uma solicitação .....	5
Proteger contra falsificação de solicitação entre locais (CSRF) .....	5

# API de gerenciamento do locatário

## Entenda a API de gerenciamento do locatário

Você pode executar tarefas de gerenciamento do sistema usando a API REST do Gerenciamento do locatário em vez da interface de usuário do Gerenciador do locatário. Por exemplo, você pode querer usar a API para automatizar operações ou criar várias entidades, como usuários, mais rapidamente.

A API de gerenciamento do locatário:

- Usa a plataforma de API Swagger de código aberto. O Swagger fornece uma interface de usuário intuitiva que permite que desenvolvedores e não desenvolvedores interajam com a API. A interface do usuário Swagger fornece detalhes completos e documentação para cada operação da API.
- Utiliza ["controle de versão para dar suporte a atualizações sem interrupções"](#).

Para acessar a documentação do Swagger para a API de gerenciamento do locatário:

1. Inicie sessão no Gestor do Locatário.
2. Na parte superior do Gerenciador do Locatário, selecione o ícone de ajuda e selecione **Documentação da API**.

## Operações da API

A API de Gerenciamento do Tenant organiza as operações de API disponíveis nas seguintes seções:

- **\* Conta\***: Operações na conta de locatário atual, incluindo obter informações de uso do armazenamento.
- **Auth**: Operações para realizar autenticação de sessão do usuário.

A API de gerenciamento do locatário suporta o esquema de autenticação de token do portador. Para um login de locatário, você fornece um nome de usuário, senha e AccountID no corpo JSON da solicitação de autenticação (ou seja, `POST /api/v3/authorize`). Se o usuário for autenticado com êxito, um token de segurança será retornado. Esse token deve ser fornecido no cabeçalho de solicitações de API subsequentes ("autorização: Token portador").

Para obter informações sobre como melhorar a segurança de autenticação, ["Proteger contra falsificação de pedidos entre sites"](#) consulte .



Se o logon único (SSO) estiver ativado para o sistema StorageGRID, você deverá executar etapas diferentes para autenticar. Consulte ["Instruções para usar a API Grid Management"](#).

- **Config**: Operações relacionadas à versão do produto e versões da API de Gerenciamento do Tenant. Você pode listar a versão de lançamento do produto e as principais versões da API suportadas por essa versão.
- **Containers**: Operações em baldes S3 ou contentores Swift.
- **Disabled-features**: Operações para visualizar recursos que podem ter sido desativados.
- **Endpoints**: Operações para gerenciar um endpoint. Os endpoints permitem que um bucket do S3 use um serviço externo para replicação, notificações ou integração de pesquisa do StorageGRID CloudMirror.

- \* Grid-federação-conexões\*: Operações em conexões de federação de grade e replicação entre grade.
- **Groups**: Operações para gerenciar grupos de locatários locais e recuperar grupos de locatários federados de uma fonte de identidade externa.
- **Identity-source**: Operações para configurar uma fonte de identidade externa e sincronizar manualmente informações de grupo federado e de usuário.
- **ilm**: Operações nas configurações de gerenciamento do ciclo de vida da informação (ILM).
- **Regions**: Operações para determinar quais regiões foram configuradas para o sistema StorageGRID.
- **S3**: Operações para gerenciar S3 chaves de acesso para usuários arrendatários.
- **S3-object-lock**: Operações em configurações globais de bloqueio de objetos S3D, usadas para suportar a conformidade regulamentar.
- **Usuários**: Operações para visualizar e gerenciar usuários de inquilinos.

## Detalhes da operação

Quando você expande cada operação da API, você pode ver sua ação HTTP, URL do endpoint, uma lista de todos os parâmetros necessários ou opcionais, um exemplo do corpo da solicitação (quando necessário) e as possíveis respostas.

## 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

```
{  
  "responseTime": "2018-02-01T16:22:31.066Z",  
  "status": "success",  
  "apiVersion": "2.1"
```

## Emitir solicitações de API



Todas as operações de API que você executa usando a página da Web do API Docs são operações ativas. Tenha cuidado para não criar, atualizar ou excluir dados de configuração ou outros dados por engano.

### Passos

1. Selecione a ação HTTP para ver os detalhes da solicitação.
2. Determine se a solicitação requer parâmetros adicionais, como um grupo ou ID de usuário. Em seguida, obtenha esses valores. Talvez você precise emitir uma solicitação de API diferente primeiro para obter as informações de que precisa.
3. Determine se você precisa modificar o corpo de solicitação de exemplo. Em caso afirmativo, você pode selecionar **modelo** para aprender os requisitos para cada campo.

4. Selecione **Experimente**.
5. Forneça quaisquer parâmetros necessários ou modifique o corpo do pedido conforme necessário.
6. Selecione **Executar**.
7. Revise o código de resposta para determinar se a solicitação foi bem-sucedida.

## Controle de versão da API de gerenciamento de locatário

A API de gerenciamento do locatário usa o controle de versão para oferecer suporte a atualizações sem interrupções.

Por exemplo, este URL de solicitação especifica a versão 4 da API.

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

A versão principal da API é quebrada quando alterações são feitas que são *não compatíveis* com versões mais antigas. A versão menor da API é quebrada quando alterações são feitas que *são compatíveis* com versões mais antigas. As alterações compatíveis incluem a adição de novos endpoints ou novas propriedades.

O exemplo a seguir ilustra como a versão da API é carregada com base no tipo de alterações feitas.

Tipo de alteração para API	Versão antiga	Nova versão
Compatível com versões mais antigas	2,1	2,2
Não compatível com versões mais antigas	2,1	3,0

Quando você instala o software StorageGRID pela primeira vez, apenas a versão mais recente da API é ativada. No entanto, quando você atualiza para uma nova versão de recurso do StorageGRID, você continua tendo acesso à versão mais antiga da API para pelo menos uma versão de recurso do StorageGRID.



Pode configurar as versões suportadas. Consulte a seção **config** da documentação da API Swagger para "[API de gerenciamento de grade](#)" obter mais informações. Você deve desativar o suporte para a versão mais antiga depois de atualizar todos os clientes de API para usar a versão mais recente.

As solicitações desatualizadas são marcadas como obsoletas das seguintes maneiras:

- O cabeçalho de resposta é "Deprecated: True"
- O corpo de resposta JSON inclui "obsoleto": True
- Um aviso obsoleto é adicionado ao nms.log. Por exemplo:

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

## Determine quais versões de API são suportadas na versão atual

Use a `GET /versions` solicitação de API para retornar uma lista das principais versões da API suportada. Esta solicitação está localizada na seção **config** da documentação da API Swagger.

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

## Especifique uma versão da API para uma solicitação

Você pode especificar a versão da API usando um parâmetro de caminho (`/api/v4`) ou um cabeçalho (`Api-Version: 4`). Se você fornecer ambos os valores, o valor do cabeçalho substitui o valor do caminho.

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

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

## Proteger contra falsificação de solicitação entre locais (CSRF)

Você pode ajudar a proteger contra ataques de falsificação de solicitação entre sites (CSRF) contra StorageGRID usando tokens CSRF para melhorar a autenticação que usa cookies. O Grid Manager e o Tenant Manager habilitam automaticamente esse recurso de segurança; outros clientes de API podem optar por ativá-lo quando fizerem login.

Um invasor que pode acionar uma solicitação para um site diferente (como um POST de formulário HTTP) pode fazer com que certas solicitações sejam feitas usando os cookies do usuário conectado.

O StorageGRID ajuda a proteger contra ataques CSRF usando tokens CSRF. Quando ativado, o conteúdo de um cookie específico deve corresponder ao conteúdo de um cabeçalho específico ou de um parâmetro específico DO corpo DO POST.

Para ativar a funcionalidade, defina o `csrfToken` parâmetro para `true` durante a autenticação. A predefinição é `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"
```

Quando verdadeiro, um `GridCsrfToken` cookie é definido com um valor aleatório para login no Gerenciador de Grade, e o `AccountCsrfToken` cookie é definido com um valor aleatório para login no Gerenciador de Tenant.

Se o cookie estiver presente, todas as solicitações que podem modificar o estado do sistema (POST, PUT, PATCH, DELETE) devem incluir um dos seguintes itens:

- O `X-Csrf-Token` cabeçalho, com o valor do cabeçalho definido para o valor do cookie de token CSRF.
- Para endpoints que aceitam um corpo codificado por formulário: Um `csrfToken` parâmetro corpo de solicitação codificado por formulário.

Para configurar a proteção CSRF, use o ["API de gerenciamento de grade"](#) ou ["API de gerenciamento do locatário"](#).



As solicitações que têm um conjunto de cookies de token CSRF também irão aplicar o cabeçalho `"Content-Type: Application/json"` para qualquer solicitação que espera um corpo de solicitação JSON como uma proteção adicional contra ataques CSRF.



## **Informações sobre direitos autorais**

Copyright © 2025 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

## **Informações sobre marcas comerciais**

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.