



API de gerenciamento de inquilinos

StorageGRID software

NetApp
December 03, 2025

Índice

- API de gerenciamento de inquilinos 1
 - Entenda a API de gerenciamento de locatários 1
 - Operações de API 1
 - Detalhes da operação 2
 - Emitir solicitações de API 3
 - Controle de versão da API de gerenciamento de locatários 4
 - Determinar quais versões de API são suportadas na versão atual 5
 - Especifique uma versão de API para uma solicitação 5
 - Proteja-se contra falsificação de solicitação entre sites (CSRF) 5

API de gerenciamento de inquilinos

Entenda a API de gerenciamento de locatários

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

API de gerenciamento de inquilinos:

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

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

1. Sign in no Gerenciador de Inquilinos.
2. Na parte superior do Gerenciador de Tenants, selecione o ícone de ajuda e selecione **Documentação da API**.

Operações de API

A API de gerenciamento de locatários organiza as operações de API disponíveis nas seguintes seções:

- **conta**: Operações na conta do locatário atual, incluindo obtenção de informações de uso de armazenamento.
- **auth**: Operações para realizar autenticação de sessão do usuário.

A API de gerenciamento de locatários oferece suporte ao esquema de autenticação de token de 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 sucesso, um token de segurança será retornado. Este token deve ser fornecido no cabeçalho de solicitações de API subsequentes ("Autorização: Token do portador").

Para obter informações sobre como melhorar a segurança da autenticação, consulte "[Proteja-se contra falsificação de solicitação entre sites](#)".



Se o logon único (SSO) estiver habilitado para o sistema StorageGRID, você deverá executar etapas diferentes para autenticar. Veja o "[instruções para usar a API de gerenciamento de grade](#)".

- **config**: Operações relacionadas ao lançamento do produto e versões da API de gerenciamento de locatários. Você pode listar a versão de lançamento do produto e as principais versões da API suportadas por essa versão.
- **contêineres**: Operações em buckets S3 ou contêineres Swift.
- **deactivated-features**: Operações para visualizar recursos que podem ter sido desativados.
- **endpoints**: Operações para gerenciar um endpoint. Os endpoints permitem que um bucket S3 use um

serviço externo para replicação, notificações ou integração de pesquisa do StorageGRID CloudMirror.

- **grid-federation-connections:** Operações em conexões de federação de rede e replicação entre redes.
- **grupos:** Operações para gerenciar grupos de inquilinos locais e recuperar grupos de inquilinos federados de uma fonte de identidade externa.
- **identity-source:** Operações para configurar uma fonte de identidade externa e sincronizar manualmente informações de grupos federados e usuários.
- **ilm:** Operações em configurações de gerenciamento do ciclo de vida da informação (ILM).
- **regiões:** Operações para determinar quais regiões foram configuradas para o sistema StorageGRID .
- **s3:** Operações para gerenciar chaves de acesso S3 para usuários locatários.
- **s3-object-lock:** Operações nas configurações globais de bloqueio de objeto S3, usadas para dar suporte à conformidade regulatória.
- **usuários:** Operações para visualizar e gerenciar usuários locatários.

Detalhes da operação

Ao expandir cada operação de API, você pode ver sua ação HTTP, URL do ponto de extremidade, uma lista de quaisquer parâmetros obrigatórios ou opcionais, um exemplo do corpo da solicitação (quando necessário) e as respostas possíveis.

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

Emitir solicitações de API



Todas as operações de API que você realiza usando a página de documentação da API 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 ID de grupo ou usuário. Então, obtenha esses valores. Talvez seja necessário emitir uma solicitação de API diferente primeiro para obter as informações necessárias.
3. Determine se você precisa modificar o corpo da solicitação de exemplo. Se sim, você pode selecionar **Modelo** para saber os requisitos de cada campo.

4. Selecione **Experimentar**.
5. Forneça quaisquer parâmetros necessários ou modifique o corpo da solicitação 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 locatários

A API de gerenciamento de locatários usa controle de versão para oferecer suporte a atualizações sem interrupções.

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

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

A versão principal da API é alterada quando são feitas alterações que *não são compatíveis* com versões mais antigas. A versão secundária da API é alterada quando são feitas alterações que *são compatíveis* com versões mais antigas. Alterações compatíveis incluem a adição de novos pontos de extremidade ou novas propriedades.

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

Tipo de alteração na 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, somente a versão mais recente da API é habilitada. No entanto, ao atualizar 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 .



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

Solicitações desatualizadas são marcadas como obsoletas das seguintes maneiras:

- O cabeçalho de resposta é "Obsoleto: verdadeiro"
- O corpo da resposta JSON inclui "deprecated": true
- Um aviso obsoleto foi adicionado ao nms.log. Por exemplo:

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

Determinar quais versões de API são suportadas na versão atual

Use o `GET /versions` Solicitação de API para retornar uma lista das principais versões de API suportadas. Esta solicitação está localizada na seção **config** da documentação da API do 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 de 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 substituirá o valor do caminho.

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

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

Proteja-se contra falsificação de solicitação entre sites (CSRF)

Você pode ajudar a proteger contra ataques de falsificação de solicitação entre sites (CSRF) contra o StorageGRID usando tokens CSRF para aprimorar a autenticação que usa cookies. O Grid Manager e o Tenant Manager habilitam automaticamente esse recurso de segurança; outros clientes da API podem escolher se desejam habilitá-lo ao efetuar login.

Um invasor que pode disparar uma solicitação para um site diferente (como com um formulário HTTP POST) 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 de corpo POST específico.

Para habilitar o recurso, defina o `csrfToken` parâmetro para `true` durante a autenticação. O padrão 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` O cookie é definido com um valor aleatório para logins no Grid Manager e o `AccountCsrfToken` O cookie é definido com um valor aleatório para logins no Tenant Manager.

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

- O `X-Csrf-Token` cabeçalho, com o valor do cabeçalho definido como o valor do cookie do token CSRF.
- Para terminais que aceitam um corpo codificado em formulário: A `csrfToken` parâmetro do corpo da solicitação codificado em formulário.

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



Solicitações que tenham um cookie de token CSRF definido também aplicarão o cabeçalho `"Content-Type: application/json"` para qualquer solicitação que espere um corpo de solicitação JSON como 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 DOCUMENTOS, 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.