Entendendo a API de gerenciamento do locatário

StorageGRID

NetApp
March 10, 2025

Índice

Entendendo 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 Tenant usa 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 do usuário Swagger fornece detalhes completos e documentação para cada operação da API.

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

Passos

1. Inicie sessão no Gestor do Locatário.
2. Selecione **Ajuda Documentação da API** no cabeçalho do Gerenciador do Locatário.

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").

  Consulte ""proteção contra falsificação de solicitação entre sites"" para obter informações sobre como melhorar a segurança de autenticação.

  > Se o logon único (SSO) estiver ativado para o sistema StorageGRID, você deverá executar etapas diferentes para autenticar. Consulte ""autenticar na API se o logon único estiver ativado"" nas instruções de administração do StorageGRID.

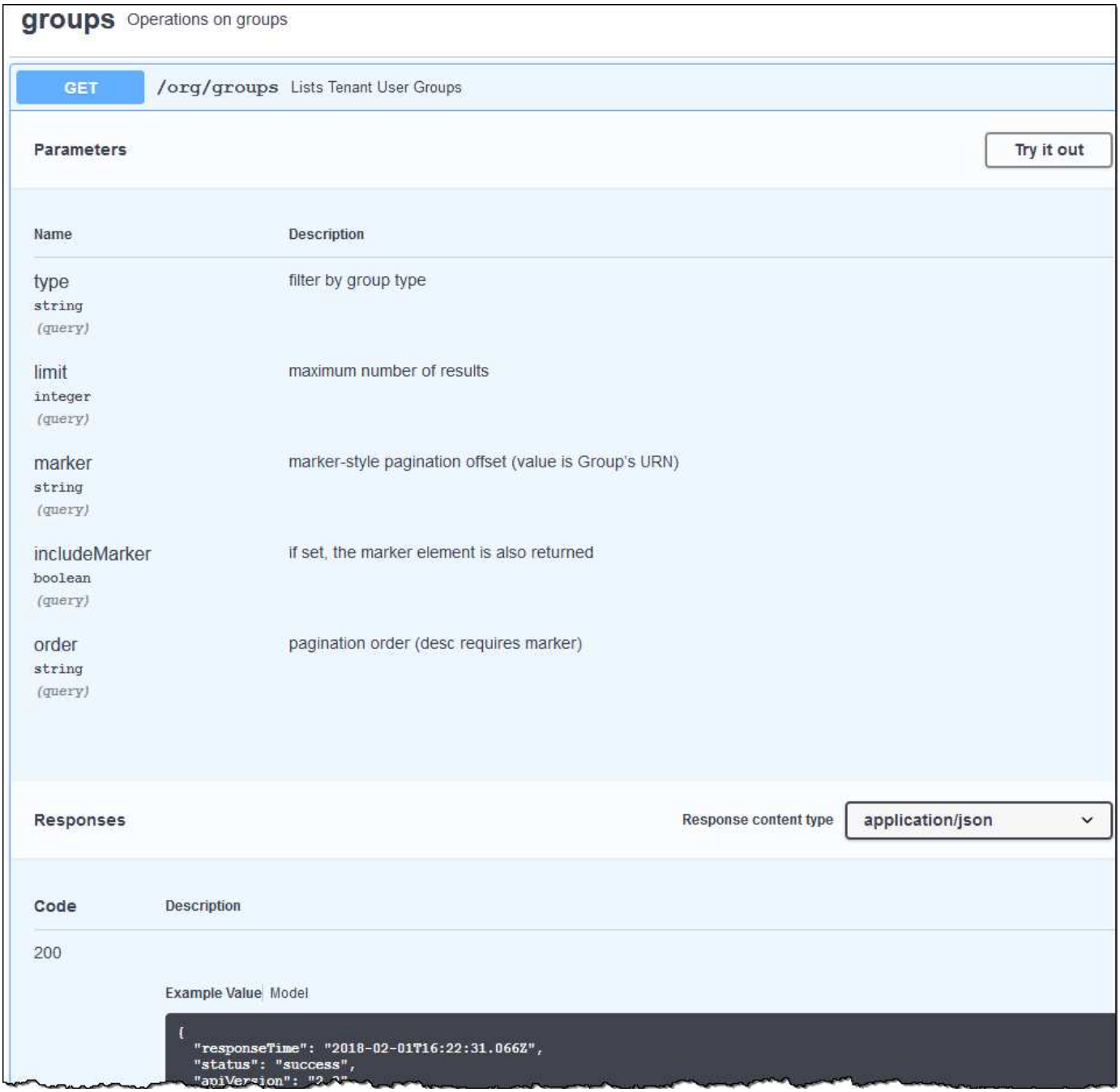
- **Config** — operações relacionadas à versão do produto e versões da API de Gerenciamento do locatário. Você pode listar a versão de lançamento do produto e as principais versões da API suportadas por essa versão.
- **Containers** — operações em baldes S3 ou contentores Swift, como segue:

Protocolo	Permissão permite
S3	• Criação de buckets compatíveis e não compatíveis • Modificação das configurações de conformidade legadas • Definir o controle de consistência para operações executadas em objetos • Criando, atualizando e excluindo a configuração CORS de um bucket • Ativar e desativar as atualizações da última hora de acesso para objetos • Gerenciamento das configurações dos serviços da plataforma, incluindo replicação do CloudMirror, notificações e integração de pesquisa (notificação de metadados) • Eliminar buckets vazios
Rápido	Definir o nível de consistência usado para contentores

- **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.
- **Groups** — operações para gerenciar grupos de locatários locais e recuperar grupos de locatários federados de uma origem de identidade externa.
- **Identity-source** — operações para configurar uma fonte de identidade externa e sincronizar manualmente informações de grupo federado e de usuário.
- **Regions** — operações para determinar quais regiões foram configuradas para o sistema StorageGRID.
- **S3** — operações para gerenciar chaves de acesso S3 para usuários arrendatários.
- **S3-object-lock** — operações para determinar como o bloqueio global de objetos S3 (conformidade) é configurado para o sistema StorageGRID.
- **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.



Emissão de 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. Clique na 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

clicar em **modelo** para aprender os requisitos para cada campo.

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

Informações relacionadas

"Proteção contra falsificação de solicitação entre sites (CSRF)"

"Administrar o StorageGRID"

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 3 da API.

```
https://hostname_or_ip_address/api/v3/authorize
```

A versão principal da API de Gerenciamento do Tenant é desfocada quando são feitas alterações que são ***not compatible*** com versões mais antigas. A versão menor da API de Gerenciamento do Tenant é desfocada quando são feitas alterações que ***are 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 o software StorageGRID é instalado pela primeira vez, apenas a versão mais recente da API de gerenciamento de locatário é ativada. No entanto, quando o StorageGRID é atualizado para uma nova versão de recurso, você continua a ter acesso à versão mais antiga da API para pelo menos uma versão de recurso do StorageGRID.

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

Determinando quais versões de API são suportadas na versão atual

Use a seguinte solicitação de API para retornar uma lista das principais versões da API suportada:

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2019-01-10T20:41:00.845Z",
  "status": "success",
  "apiVersion": "3.0",
  "data": [
    2,
    3
  ]
}
```

Especificando uma versão da API para uma solicitação

Você pode especificar a versão da API usando um parâmetro de caminho (`/api/v3`) ou um cabeçalho (`Api-Version: 3`). Se você fornecer ambos os valores, o valor do cabeçalho substitui o valor do caminho.

```
curl https://[IP-Address]/api/v3/grid/accounts

curl -H "Api-Version: 3" https://[IP-Address]/api/grid/accounts
```

Proteção contra falsificação de solicitação entre sites (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 conetado.

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.

Consulte a documentação da API on-line para obter exemplos e detalhes adicionais.

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

Informações sobre direitos autorais

Informações sobre marcas comerciais