



テナント管理API

StorageGRID software

NetApp
July 23, 2026

目次

テナント管理API	1
StorageGRIDテナント管理APIについて学ぶ	1
APIの処理	1
操作の詳細	2
API リクエストを発行する	3
StorageGRID テナント管理 API のバージョン管理	4
現在のリリースでサポートされているAPIバージョンを確認する	5
リクエストのAPIバージョンを指定します	5
StorageGRIDでクロスサイトリクエストフォージェリから保護する	5

テナント管理API

StorageGRIDテナント管理APIについて学ぶ

テナントマネージャーのユーザーインターフェースの代わりに、Tenant Management REST API を使用してシステム管理タスクを実行できます。たとえば、API を使用して操作を自動化したり、ユーザーなどの複数のエンティティをより迅速に作成したりすることができます。

テナント管理API：

- Swagger オープンソース API プラットフォームを使用します。Swagger は、開発者だけでなく非開発者も API とやり取りできる直感的なユーザーインターフェースを提供します。Swagger のユーザーインターフェースは、各 API 操作に関する詳細な情報とドキュメントを提供します。
- ["無停止アップグレードをサポートするためのバージョン管理"](#)を使用します。

テナント管理APIのSwaggerドキュメントにアクセスするには：

1. テナントマネージャーにサインインします。
2. テナントマネージャーの上部にあるヘルプアイコンを選択し、*APIドキュメント*を選択します。

APIの処理

テナント管理APIは、利用可能なAPI操作を以下のセクションに分類しています：

- **アカウント**：現在のテナントアカウントに対する操作。ストレージ使用状況情報の取得などが含まれます。
- **auth**：ユーザーセッション認証を実行するための操作。

テナント管理APIは、ベアラートークン認証方式をサポートしています。テナントログインには、ユーザー名、パスワード、および accountId を認証リクエストの JSON ボディ（つまり、POST /api/v3/authorize）に指定します。ユーザー認証が成功すると、セキュリティトークンが返されます。このトークンは、以降のAPIリクエストのヘッダーに必ず含める必要があります（「Authorization: Bearer token」）。

認証セキュリティの改善に関する情報については、["クロスサイトリクエストフォージェリ攻撃から保護する"](#)を参照してください。



StorageGRID システムでシングル サインオン (SSO) が有効になっている場合は、認証のために異なる手順を実行する必要があります。["グリッド管理APIの使用法に関する手順"](#)を参照してください。

- **config**: 製品リリースおよびTenant Management APIのバージョンに関連する操作。製品のリリースバージョンと、そのリリースでサポートされているAPIのメジャーバージョンを一覧表示できます。
- **コンテナ**：S3バケットに対する操作。
- **deactivated-features**：無効化された可能性のある機能を表示するための操作。

- **エンドポイント**：エンドポイントを管理するための操作。エンドポイントを使用すると、S3 バケットが外部サービスを使用して StorageGRID CloudMirror レプリケーション、通知、または検索統合を行うことができます。
- **grid-federation-connections**：グリッドフェデレーション接続およびクロスグリッドレプリケーションに関する操作。
- **グループ**：ローカルテナントグループを管理し、外部IDソースからフェデレーションテナントグループを取得するための操作。
- **identity-source**：外部IDソースを設定し、フェデレーションされたグループとユーザー情報を手動で同期するための操作。
- **ilm**：情報ライフサイクル管理（ILM）設定に対する操作。
- **regions**：StorageGRID システムに設定されているリージョンを確認するための操作。
- **s3**：テナントユーザーのS3アクセスキーを管理する操作。
- **s3-object-lock**：規制遵守をサポートするために使用される、グローバルな S3 Object Lock 設定に対する操作。
- **ユーザー**：テナントユーザーを表示および管理するための操作。

操作の詳細

各API操作を展開すると、そのHTTPアクション、エンドポイントURL、必須またはオプションのパラメータのリスト、リクエストボディの例（必要な場合）、および考えられるレスポンスが表示されます。

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>

API リクエストを発行する



APIドキュメントのウェブページを使用して実行するAPI操作はすべて、ライブ操作となります。設定データやその他のデータを誤って作成、更新、または削除しないように注意してください。

手順

1. リクエストの詳細を表示するには、HTTPアクションを選択してください。
2. リクエストにグループIDやユーザーIDなどの追加パラメータが必要かどうかを判断します。次に、これらの値を取得します。必要な情報を取得するには、まず別のAPIリクエストを発行する必要がある場合があります。
3. サンプルリクエストボディを修正する必要があるかどうかを判断してください。必要な場合は、*モデル*

を選択して各フィールドの要件を確認できます。

4. 「Try it out」を選択します。
5. 必要なパラメータを指定するか、必要に応じてリクエスト本文を変更してください。
6. 「実行」を選択します。
7. リクエストが成功したかどうかを判断するには、レスポンスコードを確認してください。

StorageGRID テナント管理 API のバージョン管理

テナント管理APIは、バージョン管理を利用して、システムへの影響を最小限に抑えたアップグレードをサポートします。

例えば、このリクエスト URL は API のバージョン 4 を指定しています。

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

APIのメジャーバージョンは、古いバージョンと互換性のない変更が行われた場合、更新されます。APIのマイナーバージョンは、古いバージョンと互換性のある変更が行われた場合、更新されます。互換性のある変更には、新しいエンドポイントまたは新しいプロパティの追加が含まれます。

以下の例は、行われた変更の種類に基づいてAPIバージョンがどのように更新されるかを示しています。

APIに対する変更の種類	旧バージョン	新バージョン
旧バージョンとの互換性あり	2.1	2.2
旧バージョンとの互換性はありません	2.1	3.0

StorageGRID ソフトウェアを初めてインストールする場合、最新バージョンの API のみが有効になります。ただし、StorageGRID の新しい機能リリースにアップグレードした場合でも、少なくとも 1 つの StorageGRID 機能リリースの間は、古い API バージョンに引き続きアクセスできます。



対応バージョンを設定できます。詳細については、「[グリッド管理API](#)」の Swagger API ドキュメントの **config** セクションを参照してください。すべての API クライアントを新しいバージョンに更新した後、古いバージョンのサポートを無効にする必要があります。

古いリクエストは、以下の方法で非推奨としてマークされます。

- レスポンスヘッダーは「Deprecated: true」です。
- JSON レスポンスボディには「deprecated」 : true が含まれています
- 非推奨の警告がnms.logに追加されます。例：

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

現在のリリースでサポートされているAPIバージョンを確認する

`GET /versions` API リクエストを使用して、サポートされている API のメジャーバージョンのリストを返します。このリクエストは、Swagger API ドキュメントの `*config*` セクションに記載されています。

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

リクエストのAPIバージョンを指定します

パスパラメータ (`/api/v4`) またはヘッダー (`Api-Version: 4`) を使用して API バージョンを指定できます。両方の値を指定した場合、ヘッダーの値がパスの値を上書きします。

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

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

StorageGRIDでクロスサイトリクエストフォージェリから保護する

CSRF トークンを使用して Cookie を使用する認証を強化することで、StorageGRID に対するクロスサイトリクエストフォージェリ (CSRF) 攻撃からの保護に役立てることができます。Grid Manager と Tenant Manager はこのセキュリティ機能を自動的に有効にします。その他の API クライアントは、サインイン時に有効にするかどうかを選択できます。

別のサイトへのリクエスト (HTTP フォーム POST など) をトリガーできる攻撃者は、ログインしているユーザーの Cookie を使用して特定のリクエストを実行させることができます。

StorageGRID は、CSRF トークンを使用することで、CSRF 攻撃に対する保護に役立ちます。有効にした場合、特定のクッキーの内容は、特定のヘッダーまたは特定の POST ボディパラメータの内容と一致する必要があります。

この機能を有効にするには、認証中に `csrfToken` パラメータを `true` に設定します。デフォルトは `false` です。

```
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"
```

`true` の場合、`GridCsrfToken` クッキーには Grid Manager へのサインイン用のランダムな値が設定され、`AccountCsrfToken` クッキーには Tenant Manager へのサインイン用のランダムな値が設定されます。

Cookieが存在する場合、システムの状態を変更できるすべてのリクエスト（POST、PUT、PATCH、DELETE）には、以下のいずれかを含める必要があります。

- `X-Csrf-Token` ヘッダー。ヘッダーの値は、CSRFトークンクッキーの値に設定されます。
- フォームエンコードされたボディを受け入れるエンドポイントの場合：A `csrfToken` フォームエンコードされたリクエストボディパラメータ。

CSRF保護を設定するには、"[グリッド管理API](#)"または"[テナント管理API](#)"を使用します。



CSRFトークンCookieが設定されているリクエストは、CSRF攻撃に対する追加の保護として、JSONリクエストボディを想定するすべてのリクエストに対して「Content-Type: application/json」ヘッダーを強制的に適用します。

著作権に関する情報

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。