Tenant Managerを使用します

StorageGRID

NetApp
October 03, 2025

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

目次

Tenant Managerを使用します . . . 1
StorageGRID テナントアカウントを使用する . . . 1
テナントアカウントの作成 . . . 1
S3テナントを設定する . . . 2
Swiftテナントを設定します . . . 2
Web ブラウザの要件 . . . 2
Tenant Managerにサインインします . . . 3
Tenant Managerからサインアウトします . . . 6
Tenant Managerのダッシュボードについて . . . 6
テナントアカウントの概要 . . . 7
ストレージとクォータの使用状況 . . . 8
クォータ使用状況アラート . . . 9
エンドポイントエラー . . . 9
テナント管理APIについて . . . 10
API 処理 . . . 10
処理の詳細 . . . 11
API要求の実行 . . . 12
テナント管理 API のバージョン管理 . . . 13
クロスサイトリクエストフォージェリ（CSRF）の防止 . . . 14

Tenant Managerを使用します

Tenant Manager では、 StorageGRID テナントアカウントのすべての要素を管理できます。

Tenant Manager を使用して、テナントアカウントのストレージ使用率を監視したり、アイデンティティフェデレーションを使用するかローカルのグループとユーザを作成してユーザを管理したりできます。S3 テナントアカウントの場合は、 S3 キーの管理、 S3 バケットの管理、プラットフォームサービスの設定も行うことができます。

StorageGRID テナントアカウントを使用する

テナントアカウントでは、 Simple Storage Service （ S3 ） REST API または Swift REST API を使用して、StorageGRID システムでオブジェクトの格納や読み出しを行うことができます。

各テナントアカウントには、フェデレーテッド / ローカルグループ、ユーザ、 S3 バケットまたは Swift コンテナ、オブジェクトがあります。

必要に応じて、テナントアカウントを使用して、格納されているオブジェクトをエンティティごとに分離できます。たとえば、次のようなユースケースでは複数のテナントアカウントを使用できます。

- * エンタープライズのユースケース： StorageGRID システムがエンタープライズ内で使用されている場合は、組織の部門ごとにグリッドのオブジェクトストレージを分けることができます。たとえば、マーケティング部門、カスタマーサポート部門、人事部門などのテナントアカウントが存在する場合があります。

> S3 クライアントプロトコルを使用する場合は、 S3 バケットとバケットポリシーを使用してエンタープライズ内の部門間でオブジェクトを分離することもできます。個別のテナントアカウントを作成する必要はありません。S3 クライアントアプリケーションを実装するための手順を参照してください。

- * サービスプロバイダのユースケース： * StorageGRID システムがサービスプロバイダによって使用されている場合は、ストレージをリースするエンティティごとにグリッドのオブジェクトストレージを分けることができます。たとえば、会社 A 、会社 B 、会社 C などのテナントアカウントを作成できます。

テナントアカウントの作成

テナントアカウントは、 StorageGRID のグリッド管理者がグリッドマネージャを使用して作成します。グリッド管理者は、テナントアカウントを作成する際に次の情報を指定します。

- テナントの表示名（テナントのアカウント ID は自動的に割り当てられ、変更できません）。
- テナントアカウントが S3 と Swift のどちらを使用するか。
- S3 テナントアカウントの場合：テナントアカウントにプラットフォームサービスの使用を許可するかどうか。プラットフォームサービスの使用が許可されている場合は、グリッドがその使用をサポートするように設定されている必要があります。
- 必要に応じて、テナントアカウントのストレージクォータ — テナントのオブジェクトで使用可能な最大ギガバイト数、テラバイト数、ペタバイト数。テナントのストレージクォータは、物理容量（ディスクのサイズ）ではなく、論理容量（オブジェクトのサイズ）を表します。
- StorageGRID システムでアイデンティティフェデレーションが有効になっている場合は、テナントアカウ

ントを設定するための Root Access 権限が割り当てられているフェデレーテッドグループ。

- StorageGRID システムでシングルサインオン（ SSO ）が使用されていない場合は、テナントアカウントが独自のアイデンティティソースを使用するか、グリッドのアイデンティティソースを共有するか、およびテナントのローカル root ユーザの初期パスワード。

また、 S3 テナントアカウントが規制要件に準拠する必要がある場合は、グリッド管理者が StorageGRID システムに対して S3 オブジェクトロック設定を有効にすることができます。S3 オブジェクトのロックを有効にすると、すべての S3 テナントアカウントで準拠バケットを作成、管理できます。

S3テナントを設定する

S3 テナントアカウントが作成されたら、 Tenant Manager にアクセスして次のタスクを実行できます。

- アイデンティティフェデレーションの設定（グリッドとアイデンティティソースを共有する場合を除く）、またはローカルグループおよびユーザの作成
- S3 アクセスキーの管理
- 準拠バケットを含む S3 バケットを作成、管理します
- プラットフォームサービスの使用（有効な場合）
- ストレージ使用状況を監視しています

> Tenant Manager を使用して S3 バケットを作成および管理できますが、オブジェクトを取り込んで管理するには、 S3 アクセスキーを取得し、 S3 REST API を使用する必要があります。

Swiftテナントを設定します

Swift テナントアカウントが作成されたら、 Root Access 権限を持つユーザは Tenant Manager にアクセスして、次のようなタスクを実行できます。

- アイデンティティフェデレーションの設定（グリッドとアイデンティティソースを共有する場合を除く）、およびローカルグループとユーザの作成
- ストレージ使用状況を監視しています

> Swift ユーザが Tenant Manager にアクセスするには、 Root Access 権限が必要です。ただし Root Access 権限では、 Swift REST API に認証してコンテナを作成したりオブジェクトを取り込んだりすることはできません。Swift REST API に認証するには、 Swift 管理者の権限が必要です。

関連情報

"StorageGRID の管理"

"S3 を使用する"

"Swift を使用します"

Web ブラウザの要件

サポートされている Web ブラウザを使用する必要があります。

Web ブラウザ	サポートされる最小バージョン
Google Chrome	87
Microsoft Edge の場合	87
Mozilla Firefox	84

ブラウザウィンドウの幅を推奨される値に設定してください。

ブラウザの幅	ピクセル
最小（ Minimum ）	1024
最適	1280

Tenant Managerにサインインします

Tenant Manager にアクセスするには、サポート対象の Web ブラウザのアドレスバーにテナントの URL を入力します。

必要なもの

- ログインクレデンシャルが必要です。
- Grid 管理者から提供された Tenant Manager にアクセスするための URL を用意しておく必要があります。URL は次のいずれかの例のようになります。

```
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
```

  URL には、管理ノードへのアクセスに使用される完全修飾ドメイン名（ FQDN ）または IP アドレスが必ず含まれ、オプションでポート番号、 20 桁のテナントアカウント ID 、またはその両方が追加されます。

- URL に 20 桁のテナントアカウント ID が含まれていない場合は、このアカウント ID を確認しておく必要があります。
- サポートされているWebブラウザを使用する必要があります。

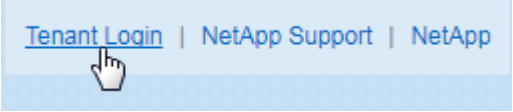
- Web ブラウザでクッキーが有効になっている必要があります。
- 特定のアクセス権限が必要です。

手順

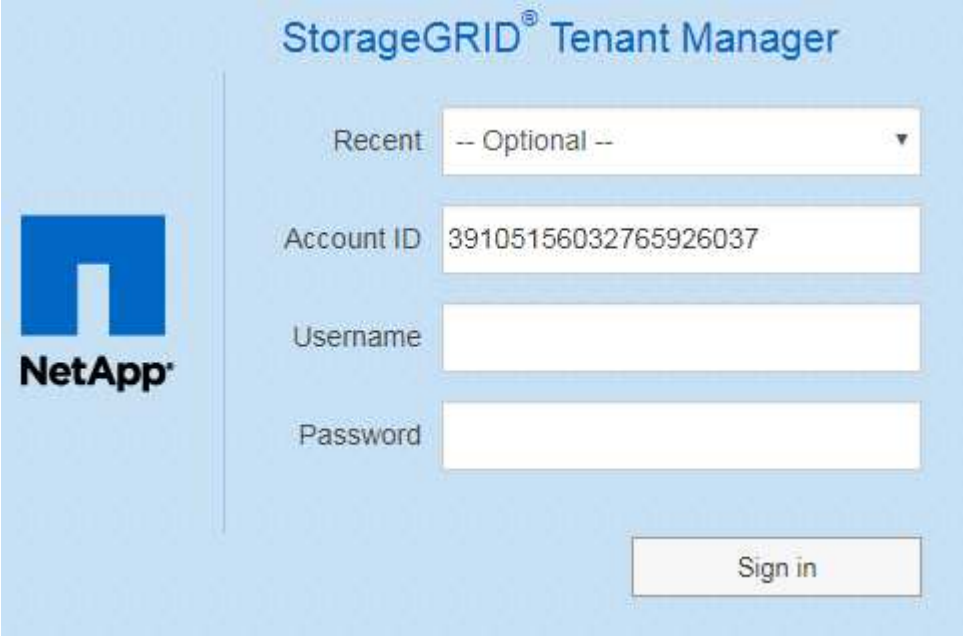
1. サポートされている Web ブラウザを起動します。
2. ブラウザのアドレスバーに、 Tenant Manager にアクセスするための URL を入力します。
3. セキュリティアラートが表示された場合は、ブラウザのインストールウィザードを使用して証明書をインストールします。
4. Tenant Manager にサインインします。

   表示されるサインイン画面は、入力した URL と、組織がシングルサインオン（ SSO ）を使用しているかどうかによって異なります。次のいずれかの画面が表示されます。

   - Grid Manager のサインインページが表示されます。右上の * Tenant Login * リンクをクリックします。

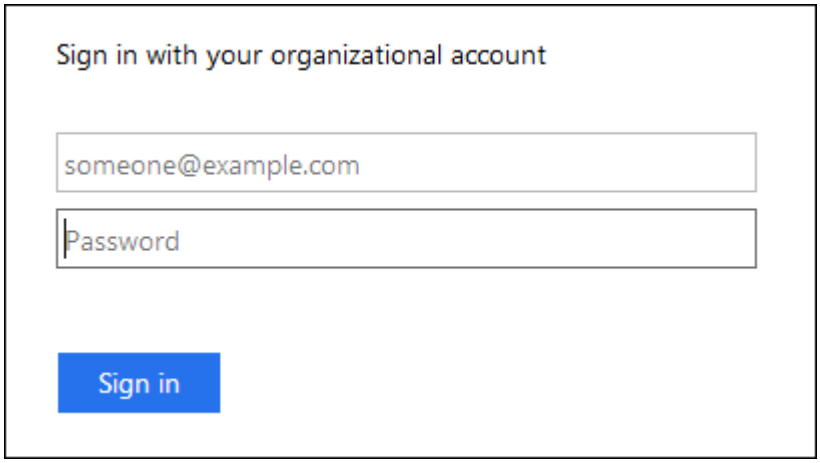
   - Tenant Manager のサインインページが表示されます。以下に示すように、「 * アカウント ID * 」フィールドはすでに入力されている可能性があります。

     i. テナントの 20 桁のアカウント ID が表示されない場合は、最近のアカウントのリストにテナントアカウントが表示されている場合はその名前を選択するか、アカウント ID を入力します。
     ii. ユーザ名とパスワードを入力します。
     iii. [* サインイン *] をクリックします。

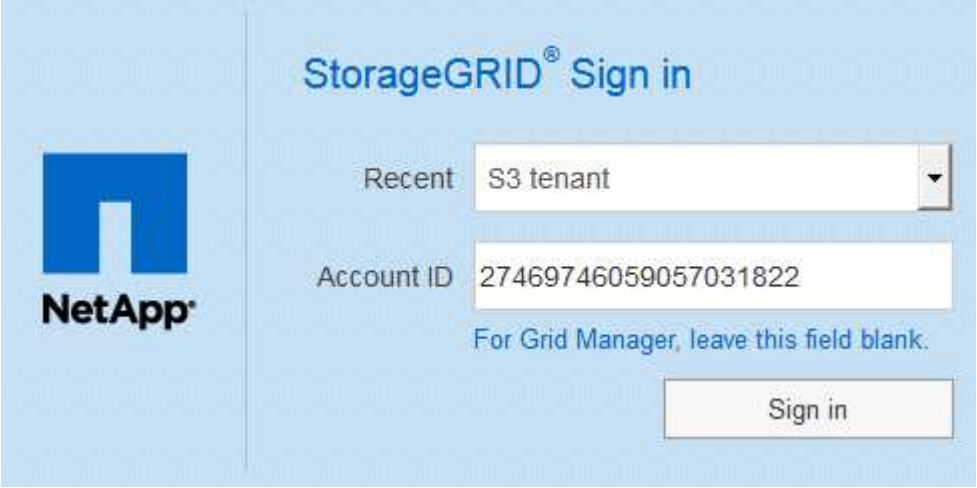
     Tenant Manager のダッシュボードが表示されます。

- グリッドで SSO が有効になっている場合は、組織の SSO ページ。例：



標準の SSO クレデンシャルを入力し、 * サインイン * をクリックします。

- Tenant Manager の SSO サインインページ。



  i. テナントの 20 桁のアカウント ID が表示されない場合は、最近のアカウントのリストにテナントアカウントが表示されている場合はその名前を選択するか、アカウント ID を入力します。
  ii. [* サインイン *] をクリックします。
  iii. 組織の SSO サインインページで通常使用している SSO クレデンシャルを使用してサインインします。

  Tenant Manager のダッシュボードが表示されます。

5. 他のユーザーから初期パスワードを受け取った場合は、アカウントを保護するためにパスワードを変更してください。[***username***>*Change Password*] を選択します。

> StorageGRID システムで SSO が有効になっている場合は、テナントマネージャからパスワードを変更できません。

関連情報

"StorageGRID の管理"

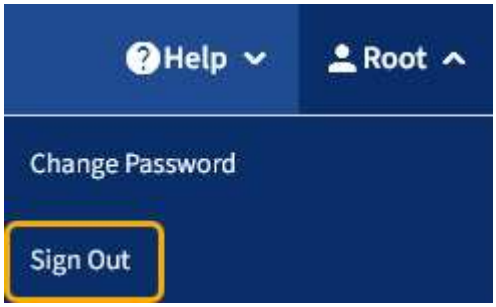
"Web ブラウザの要件"

Tenant Managerからサインアウトします

Tenant Manager の使用が完了したら、サインアウトして、権限のないユーザが StorageGRID システムにアクセスできないようにする必要があります。ブラウザのクッキーの設定によっては、ブラウザを閉じてもシステムからサインアウトされない場合があります。

手順

1. ユーザインターフェイスの右上にあるユーザ名ドロップダウンを探します。



2. ユーザー名を選択し、 * サインアウト * を選択します。

オプション	説明
SSO は使用されていません	管理ノードからサインアウトされます。Tenant Manager のサインインページが表示されます。 • 注： * 複数の管理ノードにサインインした場合、各ノードからサインアウトする必要があります。
SSO が有効です	アクセスしていたすべての管理ノードからサインアウトされます。StorageGRID のサインインページが表示されます。アクセスしたテナントアカウントの名前がデフォルトで「 Recent Accounts * 」ドロップダウンに表示され、テナントの * アカウント ID * が表示されます。 *注：SSOが有効でGrid Managerにもサインインしている場合は、SSOからサインアウトするためにGrid Managerからもサインアウトする必要があります。

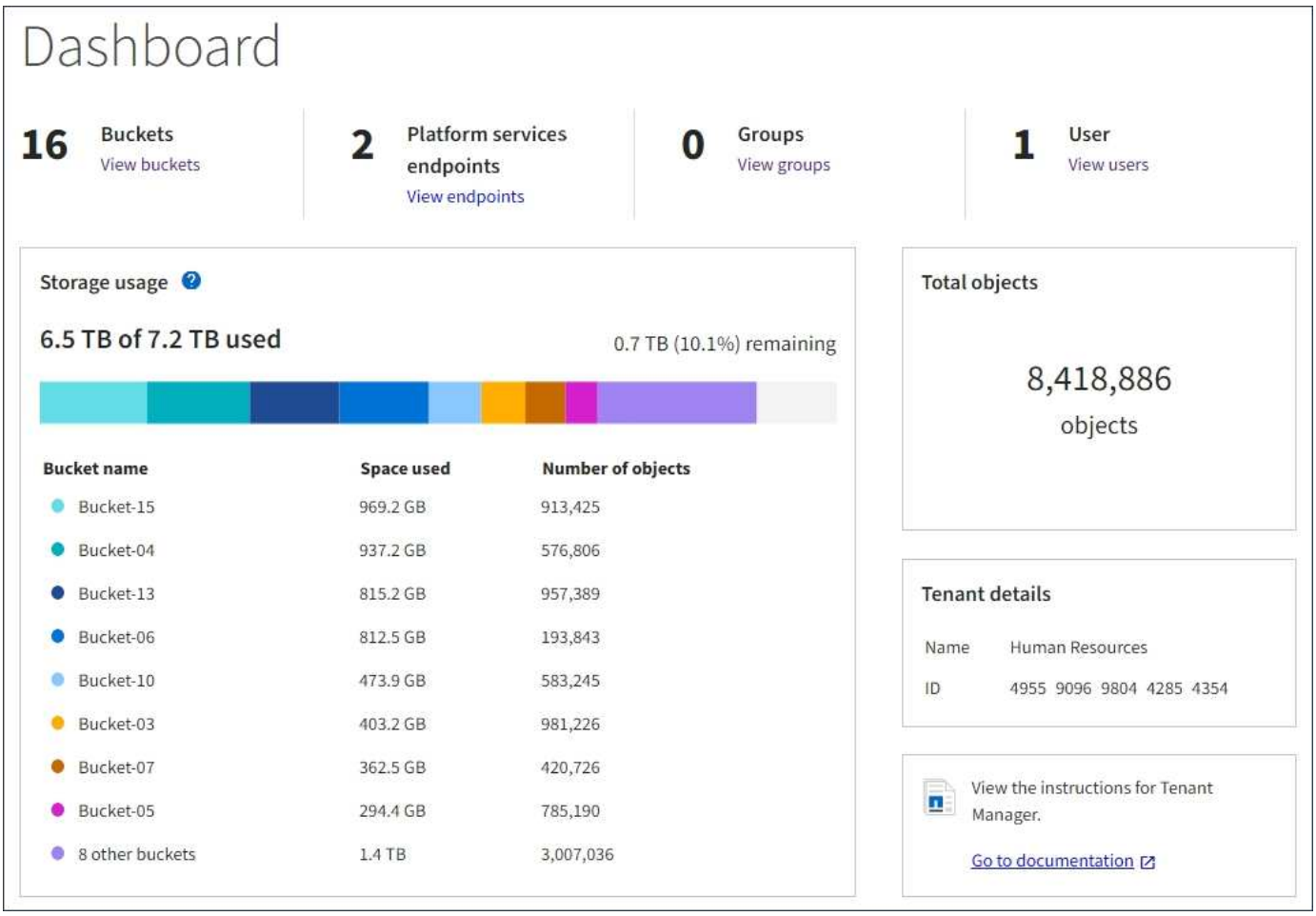
Tenant Managerのダッシュボードについて

Tenant Manager Dashboard には、テナントアカウントの設定の概要とテナントのバケット（ S3 ）またはコンテナ（ Swift ）でオブジェクトに使用されているスペースの量が表示されます。テナントにクォータがある場合は、クォータの使用量と残りの容量がダッシュボードに表示されます。テナントアカウントに関連するエラーがある場合は、ダ

ッシュボードにそのエラーが表示されます。

> 使用済みスペースの値は推定値です。これらの推定値は、取り込みのタイミング、ネットワーク接続、ノードのステータスによって左右されます。

オブジェクトがアップロードされると、ダッシュボードは次のようになります。



テナントアカウントの概要

ダッシュボードの上部には、次の情報が表示されます。

- 設定されているバケットまたはコンテナ、グループ、およびユーザの数
- プラットフォームサービスエンドポイントの数（設定されている場合）

リンクを選択すると詳細を確認できます。

ダッシュボードの右側には、次の情報が表示されます。

- テナントのオブジェクトの合計数。

  S3 アカウントでは、オブジェクトが取り込まれておらず、 Root Access 権限がある場合は、オブジェクトの総数ではなく、「 Getting started 」というガイドラインが表示されます。

- テナントアカウントの名前とID。
- StorageGRID のドキュメントへのリンク。

ストレージとクォータの使用状況

ストレージ使用状況パネルには、次の情報が表示されます。

- テナントのオブジェクトデータの量。

> アップロードされたオブジェクトデータの合計量を示します。オブジェクトとそのメタデータのコピーを格納するために使用されるスペースは表示されません。

- クォータが設定されている場合は、オブジェクトデータに使用できるスペースの合計容量、および残りのスペースの量と割合。クォータは、取り込むことができるオブジェクトデータの量を制限します。

> クォータ使用率は内部の推定値に基づいており、場合によっては超過することがあります。たとえば、テナントがクォータを超えた場合、 StorageGRID はテナントがオブジェクトのアップロードを開始したときにクォータをチェックし、新しい取り込みを拒否します。ただし、 StorageGRID では、クォータを超過したかどうかを判断する際に、現在のアップロードのサイズは考慮されません。オブジェクトが削除された場合、クォータ使用率が再計算されるまでテナントが一時的に新しいオブジェクトをアップロードできなくなることがあります。クォータ使用率の計算には 10 分以上かかることがあります。

- 最大のバケットまたはコンテナの相対サイズを表す棒グラフ。

  任意のグラフセグメントにカーソルを合わせると、そのバケットまたはコンテナで消費されている合計スペースが表示されます。

- 棒グラフに対応するために、オブジェクトデータの合計量と各バケットまたはコンテナのオブジェクト数を含む最大のバケットまたはコンテナのリスト。

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

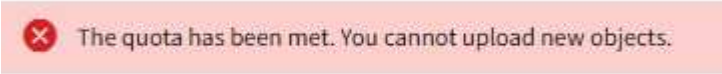
テナントに 9 つ以上のバケットまたはコンテナがある場合は、他のすべてのバケットまたはコンテナがリストの一番下にある 1 つのエントリに結合されます。

クォータ使用状況アラート

Grid Manager でクォータ使用アラートが有効になっている場合、クォータの下限または超過時に次のように Tenant Manager に表示されます。

テナントのクォータの 90% 以上が使用されると、「テナントクォータ使用率が高い * 」アラートがトリガーされます。詳細については、 StorageGRID の監視とトラブルシューティングの手順にあるアラートリファレンスを参照してください。

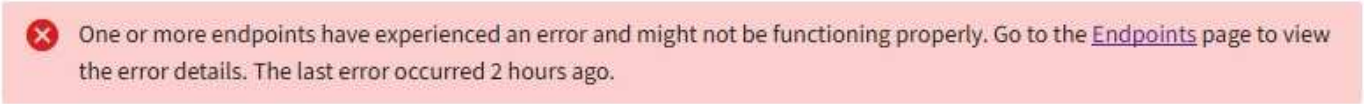
クォータを超えた場合、新しいオブジェクトをアップロードすることはできません。



詳細を表示してアラートのルールと通知を管理するには、 StorageGRID の監視とトラブルシューティングの手順を参照してください。

エンドポイントエラー

Grid Manager を使用して 1 つ以上のエンドポイントをプラットフォームサービスで使用するように設定している場合は、 Tenant Manager のダッシュボードに過去 7 日以内にエンドポイントエラーが発生した場合にアラートが表示されます。



エンドポイントエラーの詳細を表示するには、エンドポイントを選択してエンドポイントページを表示します。

関連情報

"プラットフォームサービスのエンドポイントエラーのトラブルシューティング"

"トラブルシューティングを監視します"

テナント管理APIについて

Tenant Manager のユーザインターフェイスの代わりにテナント管理 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 を使用して処理を自動化したり、ユーザなどの複数のエンティティを迅速に作成したりできます。

テナント管理APIでは、SwaggerオープンソースAPIプラットフォームを使用します。Swagger では、開発者でもそうでないユーザでも、わかりやすいユーザインターフェイスを利用して API を操作できます。Swagger のユーザインターフェイスでは、各 API 処理に関する詳細情報とドキュメントを参照できます。

Swagger のテナント管理 API のドキュメントにアクセスするには、次の手順を実行します。

手順

1. Tenant Manager にサインインします。
2. Tenant Managerのヘッダーで* Help **>** API Documentation *を選択します。

API 処理

テナント管理 API では、使用可能な API 処理が次のセクションに分類されます。

- **account** — 現在のテナントアカウントに対する処理。ストレージの使用状況情報の取得も含まれます。
- **auth** — ユーザセッション認証を実行するための操作。

  テナント管理 API では、 Bearer トークン認証方式がサポートされています。テナントにログインするには、認証要求（つまり、 `POST /api/v3/authorize`）。ユーザが認証されると、セキュリティトークンが返されます。このトークンは、後続の API 要求（「 Authorization ： Bearer トークン」）のヘッダーで指定する必要があります。

  認証セキュリティの向上については、「クロスサイトリクエストフォージェリに対する保護」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、別の手順による認証が必要です。StorageGRID の管理手順の「シングルサインオンが有効な場合のAPIへのサインイン」を参照してください。

- *config * — 製品リリースとテナント管理 API のバージョンに関連する操作。製品リリースバージョンおよ

びそのリリースでサポートされる API のメジャーバージョンを一覧表示できます。

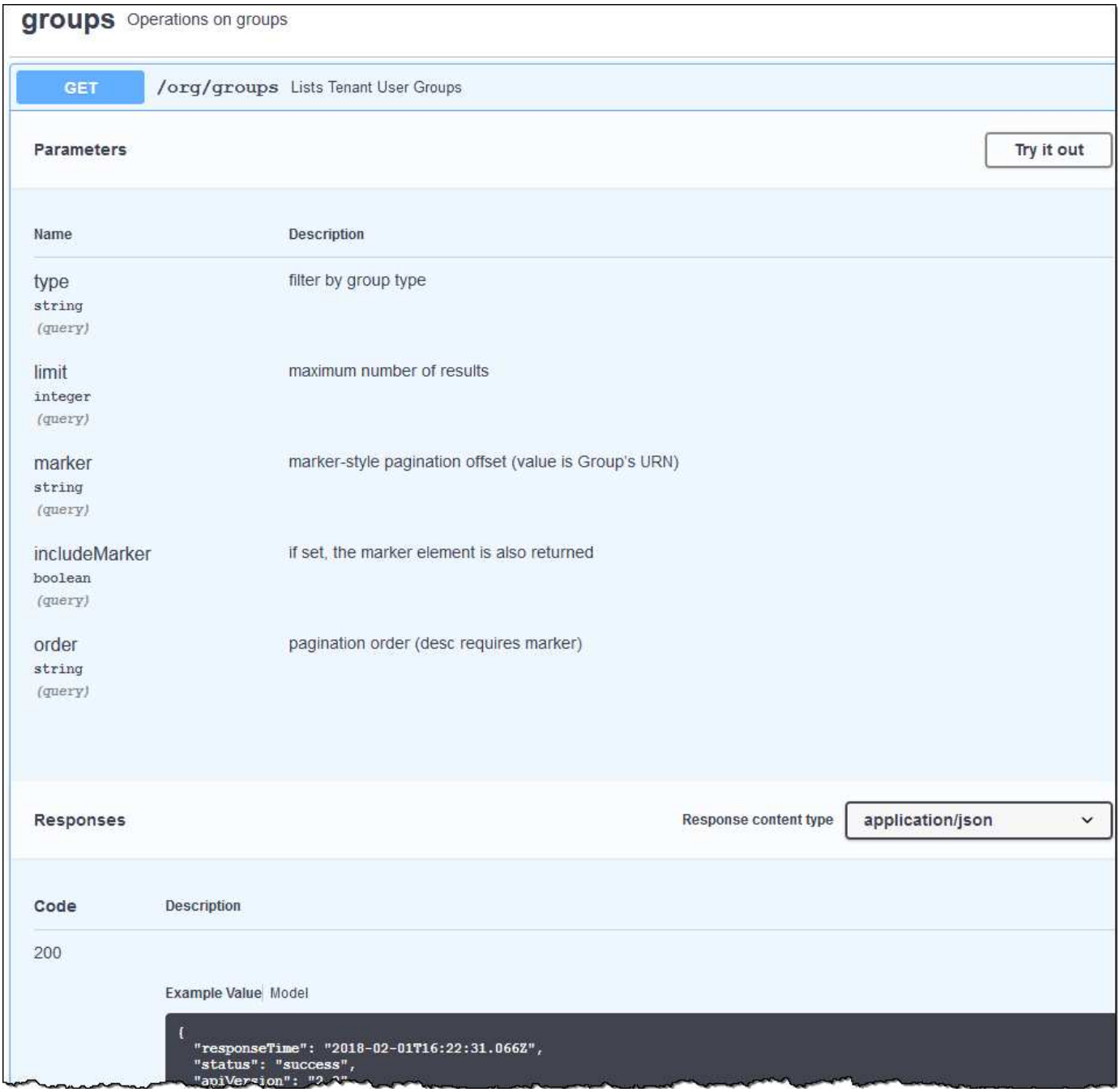
- *containers * — S3 バケットまたは Swift コンテナに対する次の処理。

プロトコル	許可するアクセス許可
S3	• 準拠バケットと非準拠バケットを作成する • 古い準拠設定の変更 • オブジェクトに対して実行される処理の整合性制御を設定します • バケットのCORS設定を作成、更新、および削除する • オブジェクトの最終アクセス日時の更新の有効化と無効化 • CloudMirrorレプリケーション、通知、検索統合（メタデータ通知）などのプラットフォームサービスの構成設定の管理 • 空のバケットを削除中
Swift	コンテナに使用する整合性レベルを設定します

- * deactivated-features * — 非アクティブ化された可能性のある機能を表示する操作。
- * endpoints * — エンドポイントを管理するための処理。エンドポイントを使用することで、 S3 バケットは外部のサービスを StorageGRID CloudMirror レプリケーション、通知、または検索統合に使用できます。
- *groups * — ローカルテナントグループを管理し、外部アイデンティティソースからフェデレーテッドテナントグループを取得するための処理。
- * identity-source * — 外部のアイデンティティソースを設定する処理、およびフェデレーテッドグループとユーザ情報を手動で同期する処理。
- **regions** — StorageGRID システムに設定されているリージョンを判別するための処理。
- * s3 * - テナントユーザの S3 アクセスキーを管理する処理。
- *s3-object-lock *-- StorageGRID システムのグローバルなS3オブジェクトロック（準拠）の構成を確認する処理。
- * users * — テナントユーザーを表示および管理するための操作。

処理の詳細

各 API 処理を展開表示すると、 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、要求の本文の例（必要な場合）、想定される応答を確認できます。



API要求の実行

API Docs Web ページを使用して実行する API 処理はすべてその場で実行されます。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. HTTPアクションをクリックして、要求の詳細を表示します。
2. グループやユーザの ID など、要求で追加のパラメータが必要かどうかを確認します。次に、これらの値を取得します。必要な情報を取得するために、先に別の API 要求の問題 が必要になることがあります。
3. 要求の本文の例を変更する必要があるかどうかを判断します。その場合は、[*Model]をクリックして各フィールドの要件を確認できます。

4. [* 試してみてください *] をクリックします。
5. 必要なパラメータを指定するか、必要に応じて要求の本文を変更します。
6. [* Execute] をクリックします。
7. 応答コードを確認し、要求が成功したかどうかを判断します。

関連情報

"クロスサイトリクエストフォージェリ（CSRF）の防止"

"StorageGRID の管理"

テナント管理 **API** のバージョン管理

テナント管理 API では、バージョン管理機能を使用して無停止アップグレードがサポートされます。

たとえば、次の要求 URL ではバージョン 3 の API が指定されています。

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

旧バージョンとの互換性がない *_not compatible _ * の変更が行われると、テナント管理 API のメジャーバージョンが上がります。以前のバージョンと互換性がある _ * の変更を行うと、テナント管理 API のマイナーバージョンが上がります。互換性のある変更には、新しいエンドポイントやプロパティの追加などがあります。次の例は、変更のタイプに基づいて 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 に対する変更のタイプ	古いバージョン	新しいバージョン
旧バージョンと互換性があります	2.1	2.2.
旧バージョンとの互換性がありません	2.1	3.0

StorageGRID ソフトウェアを初めてインストールした場合は、最新バージョンのテナント管理 API のみが有効になります。ただし、 StorageGRID を新しい機能リリースにアップグレードした場合、少なくとも StorageGRID の機能リリース 1 つ分の間は、古い API バージョンにも引き続きアクセスできます。

古い要求は、次の方法で廃止とマークされます。

- 応答ヘッダーが「 Deprecated ： true 」となる。
- JSON 応答の本文に「 deprecated ： true 」が追加される

現在のリリースでサポートされている**API**バージョンを確認します

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すには、次の API 要求を使用します。

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

要求の**API**バージョンの指定

パスパラメータを使用してAPIバージョンを指定できます (`/api/v3`）またはヘッダー (`Api-Version: 3`）。両方の値を指定した場合は、ヘッダー値がパス値よりも優先されます。

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

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

クロスサイトリクエストフォージェリ（**CSRF**）の防止

CSRF トークンを使用してクッキーによる認証を強化すると、 StorageGRID に対するクロスサイトリクエストフォージェリ（ CSRF ）攻撃を防ぐことができます。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。他の API クライアントは、サインイン時にこの機能を有効にするかどうかを選択できます。

攻撃者が別のサイト（たとえば、 HTTP フォーム POST を使用して）への要求をトリガーできる場合、サインインしているユーザのクッキーを使用して特定の要求を原因 が送信できます。

StorageGRID では、 CSRF トークンを使用して CSRF 攻撃を防ぐことができます。有効にした場合、特定のクッキーの内容が特定のヘッダーまたは特定の POST 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、を設定します `csrfToken` パラメータの値 `true` 認証中です。デフォルトはです `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"
```

trueの場合は、Aです `GridCsrfToken` クッキーは、Grid Managerおよびへのサインインにランダムな値を使用して設定されます `AccountCsrfToken` クッキーは、Tenant Managerへのサインインではランダムな値で設定されます。

クッキーが存在する場合は、システムの状態を変更できるすべての要求（ POST 、 PUT 、 PATCH 、 DELETE ）には次のいずれかが含まれている必要があります。

- 。 `X-Csrf-Token` CSRFトークンクッキーの値がヘッダーに設定されています。
- エンドポイントがフォームエンコードされた本文を受け入れる場合：A `csrfToken` フォームエンコードされた要求の本文パラメータ。

その他の例および詳細については、オンラインの API ドキュメントを参照してください。

> CSRFトークンクッキーが設定されている要求では、も適用されます `"Content-Type: application/json"` CSRF攻撃からの保護がさらに強化されるために、JSON要求の本文が必要なすべての要求のヘッダー。

著作権に関する情報

Copyright © 2025 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権を有し、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権については、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。