テナントアカウントを使用する
StorageGRID software

NetApp
December 03, 2025

This PDF was generated from https://docs.netapp.com/ja-jp/storagegrid-119/tenant/index.html on December 03, 2025. Always check docs.netapp.com for the latest.

目次

テナントアカウントを使用する

テナントアカウントを使用する

テナント アカウントを使用すると、Simple Storage Service (S3) REST API または Swift REST API を使用して、 StorageGRIDシステムにオブジェクトを保存および取得できます。

テナントアカウントとは何ですか?

各テナント アカウントには、独自のフェデレーション グループまたはローカル グループ、ユーザー、S3 バケットまたは Swift コンテナ、およびオブジェクトがあります。

テナント アカウントを使用すると、保存されたオブジェクトを異なるエンティティごとに分離できます。たとえば、次のいずれかの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使用例: StorageGRIDシステムを企業内で使用している場合、グリッドのオブジェクト ストレージは組織内のさまざまな部門によって分離されている可能性があります。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、企業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。実装手順を参照"S3 バケットとバケットポリシー"詳細についてはこちらをご覧ください。

- サービス プロバイダーの使用例: StorageGRIDシステムがサービス プロバイダーによって使用されている場合、グリッドのオブジェクト ストレージは、ストレージをリースするさまざまなエンティティによって分離される可能性があります。たとえば、会社 A、会社 B、会社 C などのテナント アカウントが存在する場合があります。

テナントアカウントを作成する方法

テナントアカウントは、"グリッド マネージャを使用するStorageGRIDグリッド管理者" 。テナント アカウントを作成するときに、グリッド管理者は次のことを指定します。

- テナント名、クライアント タイプ (S3)、オプションのストレージ クォータなどの基本情報。
- テナント アカウントの権限 (テナント アカウントが S3 プラットフォーム サービスを使用できるかどうか、独自の ID ソースを設定できるかどうか、S3 Select を使用できるかどうか、グリッド フェデレーション接続を使用できるかどうかなど)。
- StorageGRIDシステムがローカル グループとユーザー、ID フェデレーション、またはシングル サインオン (SSO) を使用するかどうかに基づく、テナントの初期ルート アクセス。

さらに、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、グリッド管理者はStorageGRIDシステムの 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 ロックを有効にすると、すべての S3 テナント アカウントが準拠バケットを作成および管理できるようになります。

S3テナントを構成する

その後"S3テナントアカウントが作成される"、テナント マネージャーにアクセスして、次のようなタスクを実行できます。

- アイデンティティ フェデレーションを設定する (アイデンティティ ソースがグリッドと共有されていない場合)
- グループとユーザーの管理
- アカウントのクローンとクロスグリッドレプリケーションにグリッドフェデレーションを使用する
- S3 アクセスキーを管理する
- S3バケットの作成と管理
- S3プラットフォームサービスを使用する
- S3 Selectを使用する
- ストレージ使用量を監視する

テナントマネージャでS3バケットを作成および管理できますが、"S3クライアント"または"S3コンソール"オブジェクトを取り込んで管理します。

サインインとサインアウトの方法

テナントマネージャーに**Sign in**

テナントマネージャにアクセスするには、テナントのURLをブラウザのアドレスバーに入力します。"サポートされているウェブブラウザ" 。

開始する前に

- ログイン資格情報をお持ちです。
- グリッド管理者から提供された、テナント マネージャーにアクセスするための URL 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、完全修飾ドメイン名 (FQDN)、管理ノードの IP アドレス、または管理ノードの HA グループの仮想 IP アドレスが常に含まれます。ポート番号、20 桁のテナント アカウント ID、またはその両方が含まれる場合もあります。

- URL にテナントの 20 桁のアカウント ID が含まれていない場合は、このアカウント ID が存在します。
- 使用しています"サポートされているウェブブラウザ"。
- Web ブラウザで Cookie が有効になっています。

- あなたは以下のユーザーグループに属しています"特定のアクセス権限"。

手順

1. 起動する"サポートされているウェブブラウザ"。
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. セキュリティ警告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. テナント マネージャーにSign in。

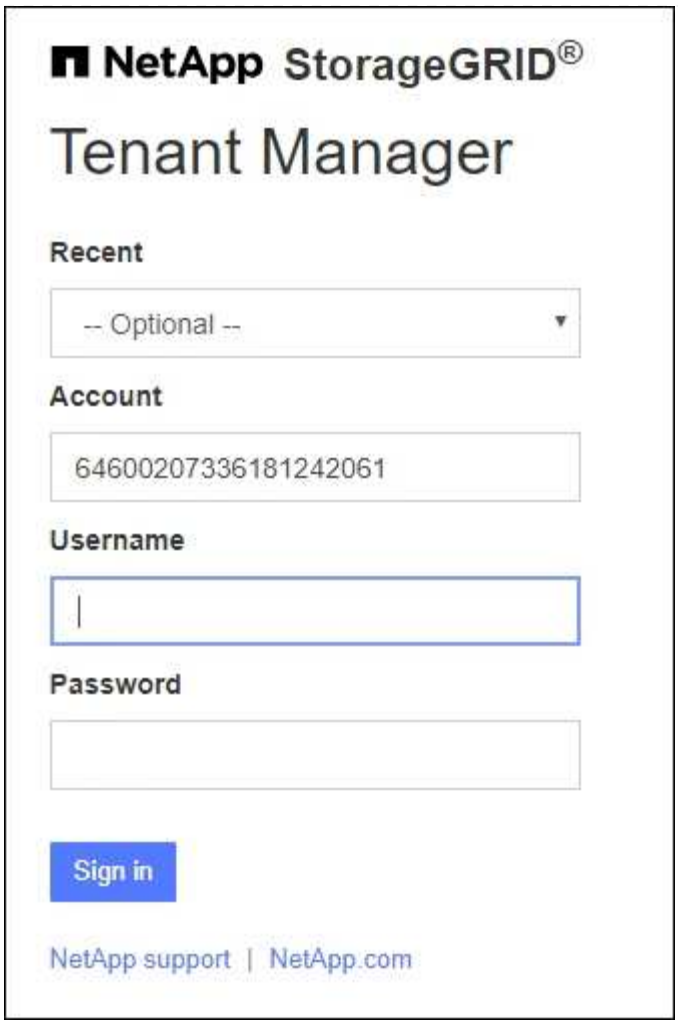
   表示されるサインイン画面は、入力した URL と、 StorageGRIDに対してシングル サインオン (SSO) が設定されているかどうかによって異なります。

SSOを使用していない

StorageGRIDが SSO を使用していない場合は、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。 テナント サインイン リンクを選択します。

- テナント マネージャーのサインイン ページ。以下に示すように、アカウント 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一覧にテナント アカウントの名前が表示されている場合はそれを選択するか、アカウント ID を入力します。

ii. ユーザー名とパスワードを入力してください。

iii. *Sign in*を選択します。

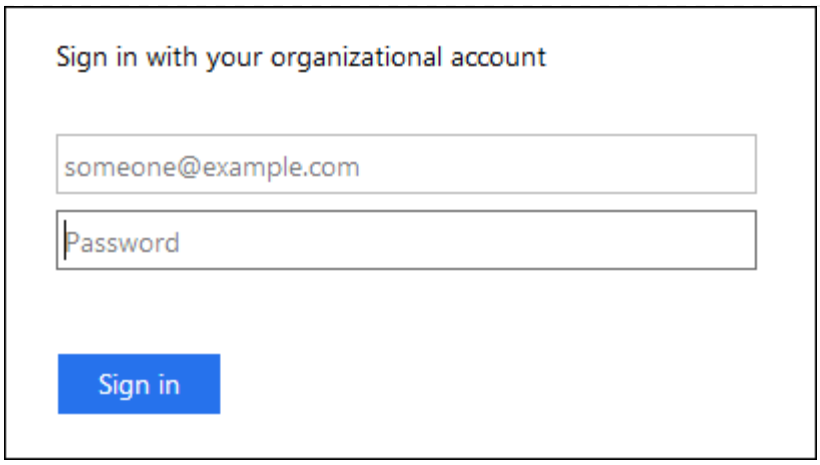
テナント マネージャー ダッシュボードが表示されます。

iv. 他の人から初期パスワードを受け取った場合は、***username*** > パスワードの変更 を選択してアカウントを保護します。

SSOの使用

StorageGRIDが SSO を使用している場合は、次のいずれかの画面が表示されます。

◦ 組織の SSO ページ。例えば：



標準の SSO 資格情報を入力し、[**Sign in**] を選択します。

- テナント マネージャー 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一覧にテナント アカウントの名前が表示されている場合はそれを選択するか、アカウント ID を入力します。

ii. *Sign in*を選択します。

iii. 組織の SSO サインイン ページで標準の SSO 資格情報を使用してSign in。

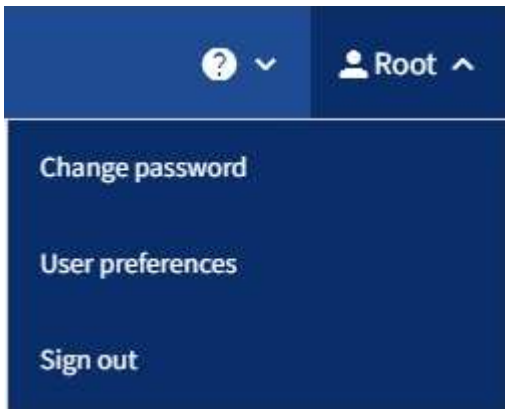
テナント マネージャー ダッシュボードが表示されます。

テナントマネージャーからサインアウトする

テナント マネージャーでの作業が完了したら、権限のないユーザーがStorageGRIDシステムにアクセスできないようにするためにサインアウトする必要があります。ブラウザの Cookie 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. ユーザー インターフェイスの右上隅にあるユーザー名ドロップダウンを見つけます。



2. ユーザー名を選択し、[サインアウト] を選択します。

   - SSO が使用されていない場合:

     管理ノードからサインアウトしました。テナント マネージャーのサインイン ページが表示されます。

     > 複数の管理ノードにサインインしている場合は、各ノードからサインアウトする必要があります。

   - SSO が有効な場合:

     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しました。 StorageGRIDSign in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 [最近のアカウント] ドロップダウンにデフォルトで表示され、テナントの アカウント **ID** が表示されます。

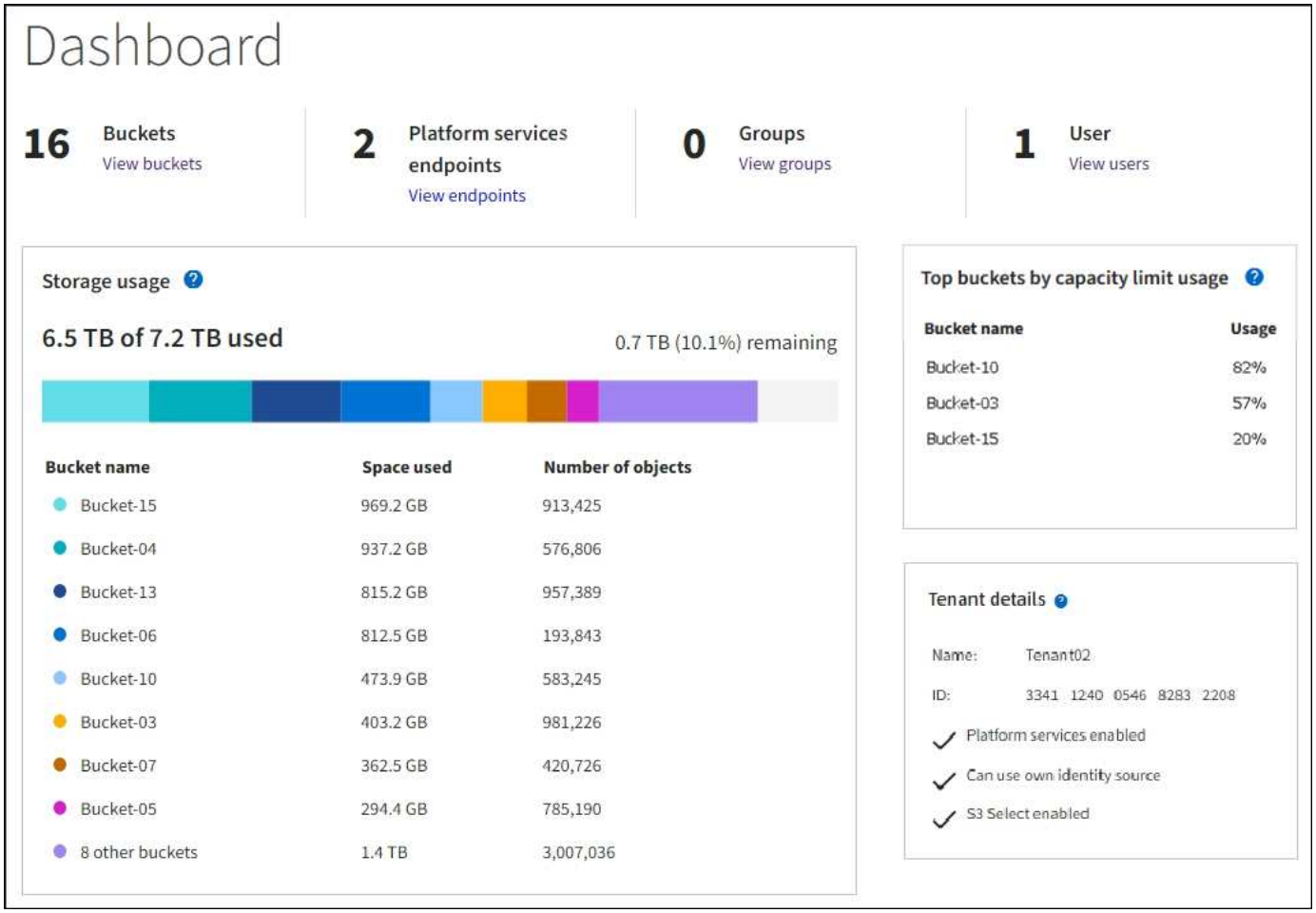
     > SSO が有効になっていて、Grid Manager にもサインインしている場合は、SSO からサインアウトするには Grid Manager からもサインアウトする必要があります。

テナントマネージャーダッシュボードを理解する

テナント マネージャー ダッシュボードには、テナント アカウントの構成の概要と、テナントのバケット (S3) またはコンテナ (Swift) 内のオブジェクトによって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、ダッシュボードには使用されているクォータの量と残っている量が表示されます。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。これらの見積りは、取り込みのタイミング、ネットワーク接続、およびノードの状態によって影響を受けます。

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例のようになります。



テナントアカウント情報

ダッシュボードの上部には、構成されたバケットまたはコンテナ、グループ、およびユーザーの数が表示されます。また、プラットフォーム サービス エンドポイントが構成されている場合は、その数も表示されます。詳細を表示するにはリンクを選択してください。

に応じて"テナント管理権限"ダッシュボードの残りの部分には、所有しているリソースと構成したオプションに応じて、ガイドライン、ストレージ使用量、オブジェクト情報、テナントの詳細のさまざまな組み合わせが表示されます。

ストレージとクォータの使用状況

ストレージ使用量パネルには次の情報が含まれます。

- テナントのオブジェクト データの量。

  この値は、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ており、それらのオブジェクトとそのメタデータのコピーを保存するために使用されるスペースを表すものではありません。

- クォータが設定されている場合、オブジェクト データに使用可能なスペースの合計量と、残りのスペースの量と割合。クォータにより、取り込めるオブジェクト データの量が制限されます。

> クォータ使用量は内部推定に基づいており、場合によっては超過する可能性があります。たとえば、 StorageGRID は、テナントがオブジェクトのアップロードを開始するとクォータをチェックし、テナントがクォータを超過している場合は新しい取り込みを拒否します。ただし、 StorageGRID 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を考慮しません。オブジェクトが削除されると、クォータ使用量が再計算されるまで、テナントは一時的に新しいオブジェクトのアップロードができなくなる可能性があります。クォータ使用量の計算には 10 分以上かかる場合があります。

- 最大のバケットまたはコンテナの相対的なサイズを表す棒グラフ。

  いずれかのチャートのセグメントにカーソルを置くと、そのバケットまたはコンテナによって消費される合計スペースが表示されます。

- 棒グラフに対応して、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 個を超えるバケットまたはコンテナがある場合、他のすべてのバケットまたはコンテナはリストの下部にある 1 つのエントリに結合されます。

> テナント マネージャーに表示されるストレージ値の単位を変更するには、テナント マネージャーの右上にあるユーザー ドロップダウンを選択し、ユーザー設定 を選択します。

クォータ使用量アラート

グリッド マネージャーでクォータ使用量アラートが有効になっている場合、クォータが少ないか超過すると、次のようにテナント マネージャーにアラートが表示されます。

- テナントのクォータの 90% 以上が使用されている場合、テナントのクォータ使用量が高い アラートがトリガーされます。

  グリッド管理者にクォータの増加を依頼することを検討してください。

- 割り当て量を超えると、新しいオブジェクトをアップロードできないことを通知するメッセージが表示されます。

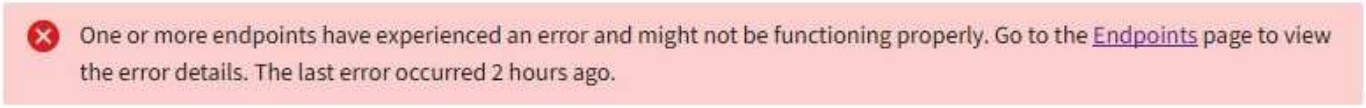
容量制限の使用状況

バケットに容量制限を設定している場合は、Tenant Manager ダッシュボードに、容量制限の使用状況による上位のバケットのリストが表示されます。

バケットに制限が設定されていない場合、その容量は無制限になります。ただし、テナント アカウントに合計ストレージ クォータがあり、そのクォータに達した場合は、バケットの残りの容量制限に関係なく、それ以上のオブジェクトを取り込むことはできません。

エンドポイントエラー

グリッド マネージャーを使用して、プラットフォーム サービスで使用する 1 つ以上のエンドポイントを構成した場合、過去 7 日以内にエンドポイント エラーが発生すると、テナント マネージャー ダッシュボードにアラートが表示されます。



詳細を見るには"プラットフォームサービスエンドポイントエラー"で、[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。

テナント管理API

テナント管理APIを理解する

テナント マネージャー ユーザー 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、開発者と非開発者が API を操作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 ユーザー インターフェースは、各 API 操作の完全な詳細とドキュメントを提供します。

- 用途"中断のないアップグレードをサポートするためのバージョン管理"。

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Sign in。
2. テナント マネージャーの上部から、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 操作を次のセクションに分類します。

- **account**: ストレージ使用状況情報の取得など、現在のテナント アカウントに対する操作。
- **auth**: ユーザーセッション認証を実行する操作。

  テナント管理 API は、ベアラー トークン認証スキームをサポートしています。テナントログインの場合、認証リクエストのJSON本文にユーザー名、パスワード、アカウントIDを指定します（つまり、 `POST /api/v3/authorize` ）。ユーザーが正常に認証されると、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 リクエストのヘッダー (「Authorization: Bearer token」) で提供する必要があります。

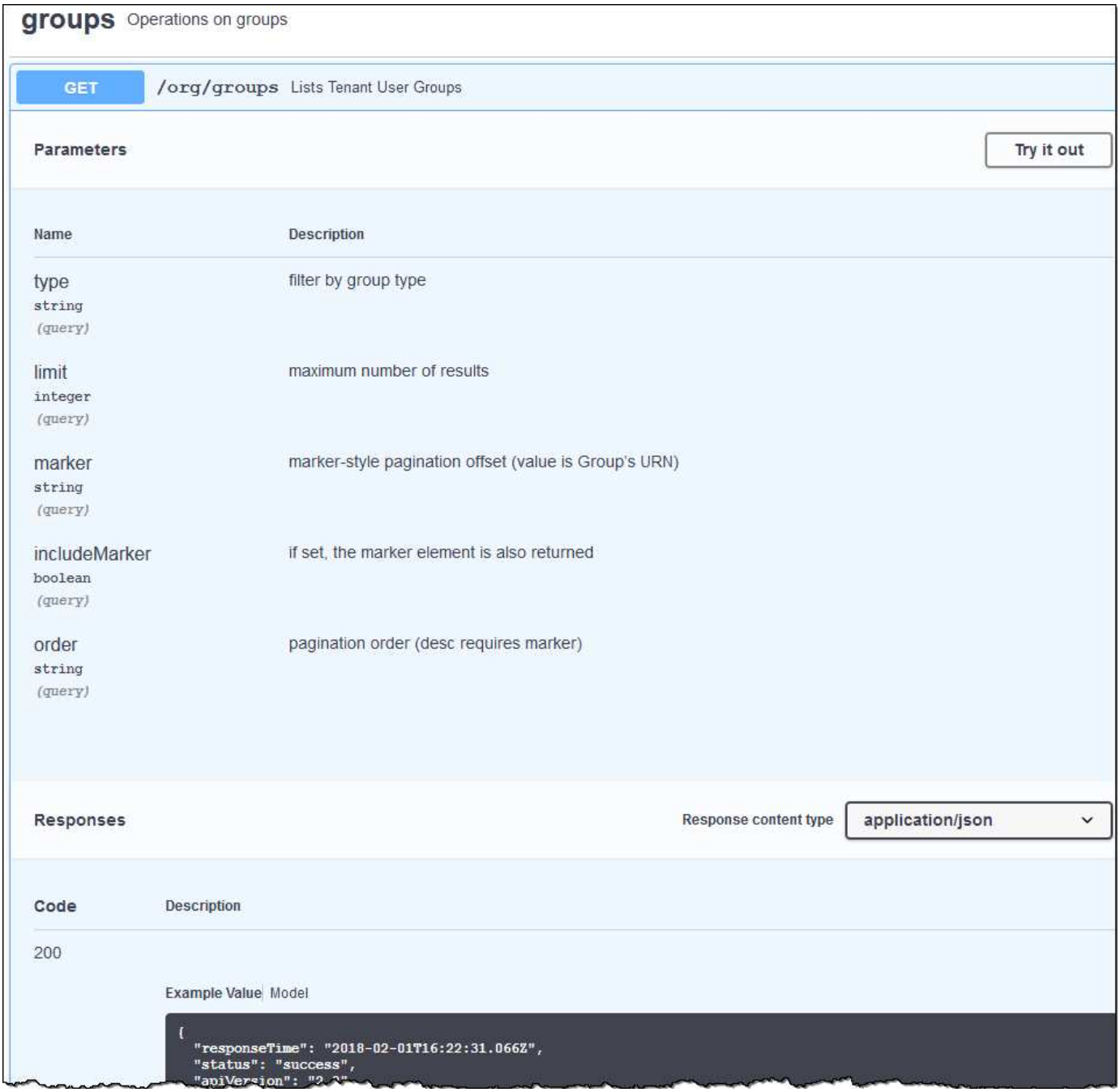
  認証セキュリティの向上については、以下を参照してください。"クロスサイトリクエストフォージェリから保護する" 。

  > 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、認証のために別の手順を実行する必要があります。参照"グリッド管理APIの使用手順"。

- **config**: テナント管理 API の製品リリースと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 バケットまたは Swift コンテナに対する操作。
- **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。
- エンドポイント: エンドポイントを管理するための操作。エンドポイントにより、S3 バケットはStorageGRID CloudMirror レプリケーション、通知、または検索統合に外部サービスを使用できるようになります。
- **grid-federation-connections**: グリッド フェデレーション接続およびグリッド間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 ソースを構成し、フェデレーション グループとユーザー情報を手動で同期する操作。
- **ilm**: 情報ライフサイクル管理 (ILM) 設定に関する操作。
- **regions**: StorageGRIDシステムに設定されているリージョンを判別する操作。
- **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**: 規制コンプライアンスをサポートするために使用される、グローバル S3 オブジェクトロック設定に対する操作。
- **users**: テナント ユーザーを表示および管理する操作。

操作の詳細

各 API 操作を展開すると、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、リクエスト本文の例 (必要な場合)、および可能な応答が表示されます。



APIリクエストを発行する

API ドキュメント Web ページを使用して実行するすべての API 操作はライブ操作です。誤って設定データやその他のデータを作成、更新、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ます。
2. リクエストにグループ ID やユーザー ID などの追加の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、最初に別の API リクエストを発行する必要がある場合があります。

3. サンプルのリクエスト本文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、「モデル」を選択して、各フィールドの要件を確認することができます。
4. *試してみる*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ます。
6. *実行*を選択します。
7. 応答コードを確認して、リクエストが成功したかどうかを確認します。

テナント管理 **API** のバージョン管理

テナント管理 API は、バージョン管理を使用して、中断のないアップグレードをサポートします。

たとえば、このリクエスト URL は API バージョン 4 を指定します。

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

古いバージョンと互換性のない変更が行われた場合には、API のメジャー バージョンが引き上げられます。古いバージョンと互換性のある変更が行われた場合に、API のマイナー バージョンが引き上げられます。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。

次の例は、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変更されるかを示しています。

APIの変更の種類	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
旧バージョンとは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すると、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すると、少なくとも 1 つのStorageGRID機能リリースについては引き続き古い API バージョンにアクセスできます。

> サポートされるバージョンを設定できます。 Swagger APIドキュメントの*config*セクションを参照してください。"グリッド管理API"詳細についてはこちらをご覧ください。すべての API クライアントを更新して新しいバージョンを使用するようにした後、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。

古くなったリクエストは、次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レスポンス本文に「deprecated」が含まれています: true
- 非推奨の警告が nms.log に追加されます。例えば：

```
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

使用 `GET /versions`サポートされている API メジャー バージョンのリストを返す API リクエスト。このリクエストは、Swagger API ドキュメントの **config** セクションにあります。

```
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**バージョンを指定する

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/v4`）またはヘッダー(`Api-Version: 4`）。両方の値を指定した場合、ヘッダー値がパス値を上書きします。

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

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

クロスサイトリクエストフォージェリ（**CSRF**）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) 攻撃から保護することができます。 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。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。

別のサイトへのリクエストをトリガーできる攻撃者 (HTTP フォーム POST など) は、サインインしたユーザーの Cookie を使用して特定のリクエストを実行させる可能性があります。

StorageGRID は、CSRF トークンを使用して CSRF 攻撃から保護します。有効にすると、特定の Cookie の内容は、特定のヘッダーまたは特定の POST 本文パラメータのいずれか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、 `csrfToken`パラメータに `true`認証中。デフォルトは `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"
```

真の場合、 `GridCsrfToken`グリッドマネージャへのサインイン時にランダムな値でクッキーが設定され、 `AccountCsrfToken`テナント マネージャーへのサインイン用に、Cookie にランダムな値が設定されます。

クッキーが存在する場合、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、次のいずれかが含まれている必要があります。

- その `X-Csrf-Token`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本文を受け入れるエンドポイントの場合: `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"。

> CSRF トークン クッキーが設定されているリクエストでは、CSRF 攻撃に対する追加の保護として、JSON リクエスト本文を期待するすべてのリクエストに「Content-Type: application/json」ヘッダーも適用されます。

グリッドフェデレーション接続を使用する

テナントグループとユーザーの複製

グリッド フェデレーション接続を使用するようにテナントが作成または編集された場合、そのテナントは 1 つのStorageGRIDシステム (ソース テナント) から別のStorageGRIDシステム (レプリカ テナント) に複製されます。テナントが複製された後、ソース テナントに追加されたグループとユーザーはレプリカ テナントに複製されます。

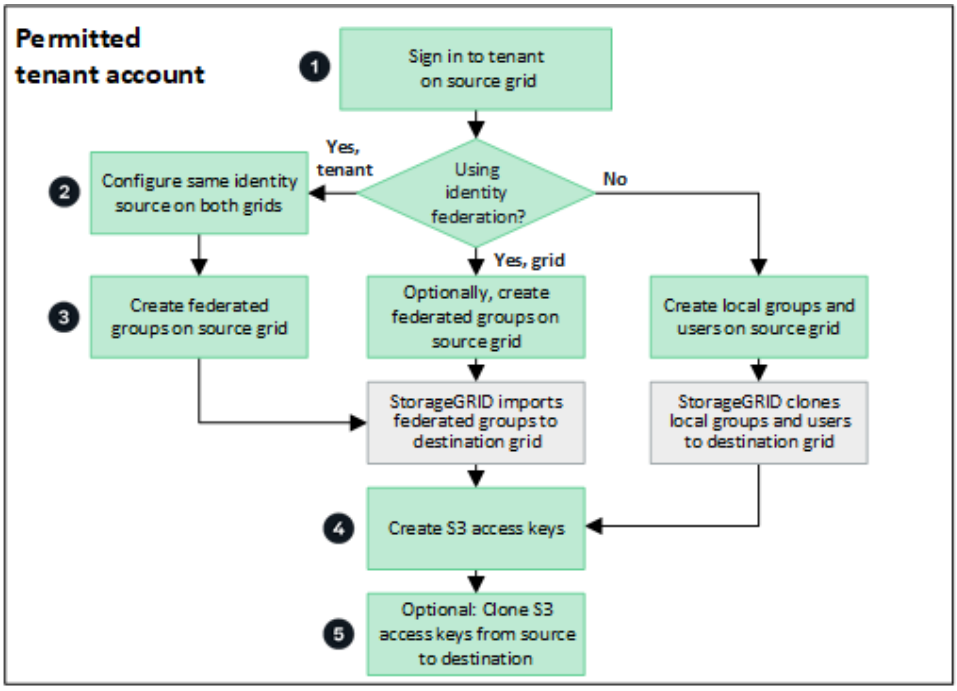
テナントが最初に作成されたStorageGRIDシステムは、テナントの ソース グリッド です。テナントが複製されるStorageGRIDシステムは、テナントの 宛先グリッド です。両方のテナント アカウントは同じアカウント ID、名前、説明、ストレージ クォータ、割り当てられた権限を持ちますが、宛先テナントには最初はルート ユーザー パスワードがありません。詳細については、"アカウントクローンとは"そして"許可されたテナントを管理する"。

テナントアカウント情報の複製は、"クロスグリッドレプリケーション"バケット オブジェクトの。両方のグリッドに同じテナント グループとユーザーが存在すると、どちらのグリッドでも対応するバケットとオブジェクトにアクセスできるようになります。

アカウントクローンのテナントワークフロー

テナント アカウントに グリッド フェデレーション接続の使用 権限がある場合は、ワークフロー図を参照し

て、グループ、ユーザー、および S3 アクセス キーのクローンを作成するために実行する手順を確認してください。



ワークフローの主な手順は次のとおりです。

1 テナントに**Sign in**

ソース グリッド (テナントが最初に作成されたグリッド) のテナント アカウントにSign in。

2 オプションで**ID**連携を構成する

テナント アカウントに、フェデレーション グループとユーザーを使用するための 独自の **ID** ソースを使用する 権限がある場合は、ソース テナント アカウントと宛先テナント アカウントの両方に同じ ID ソース (同じ設定) を構成します。両方のグリッドが同じ ID ソースを使用していない限り、フェデレーション グループとユーザーは複製できません。手順については、"アイデンティティフェデレーションを使用する" 。

3 グループとユーザーを作成する

グループとユーザーを作成するときは、常にテナントのソース グリッドから開始します。新しいグループを追加すると、 StorageGRIDによってそのグループが宛先グリッドに自動的に複製されます。

- StorageGRIDシステム全体またはテナントアカウントに対してIDフェデレーションが設定されている場合、"新しいテナントグループを作成する"アイデンティティ ソースからフェデレーション グループをインポートします。
- ID連携を使用していない場合は、"新しいローカルグループを作成する"その後"ローカルユーザーを作成する"。

4 **S3**アクセスキーを作成する

あなたはできる"独自のアクセスキーを作成する"または"別のユーザーのアクセスキーを作成する"ソース グリッドまたは宛先グリッドのいずれかで、そのグリッド上のバケットにアクセスします。

5 オプションで**S3**アクセスキーを複製する

両方のグリッドで同じアクセス キーを使用してバケットにアクセスする必要がある場合は、ソース グリッドでアクセス キーを作成し、Tenant Manager API を使用してそれらのアクセス キーを手動で宛先グリッドに複製します。手順については、"API を使用して S3 アクセスキーを複製する" 。

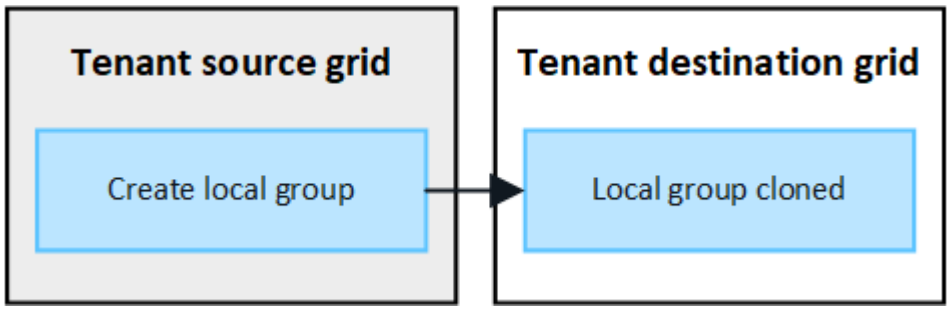
グループ、ユーザー、**S3** アクセスキーはどのように複製されますか**?**

このセクションを確認して、テナント ソース グリッドとテナント デスティネーション グリッド間でグループ、ユーザー、および S3 アクセス キーがどのように複製されるかを理解してください。

ソースグリッド上に作成されたローカルグループは複製されます

テナント アカウントが作成され、宛先グリッドに複製された後、 StorageGRID はテナントのソース グリッドに追加したローカル グループをテナントの宛先グリッドに自動的に複製します。

元のグループとそのクローンには、同じアクセス モード、グループ権限、および S3 グループ ポリシーがあります。手順については、"S3テナントのグループを作成する" 。

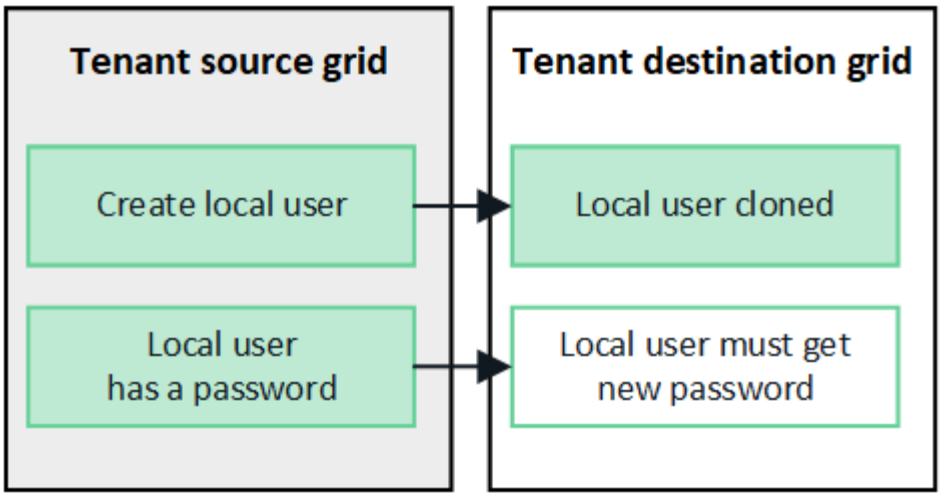


ソース グリッドにローカル グループを作成するときに選択したユーザーは、グループが宛先グリッドに複製されるときには含まれません。このため、グループを作成するときにユーザーを選択しないでください。代わりに、ユーザーを作成するときにグループを選択します。

ソースグリッド上に作成されたローカルユーザーは複製されます

ソース グリッドに新しいローカル ユーザーを作成すると、 StorageGRIDによってそのユーザーが宛先グリッドに自動的に複製されます。元のユーザーとそのクローンの両方に、同じフルネーム、ユーザー名、およびアクセス拒否 設定があります。両方のユーザーは同じグループに属しています。手順については、"ローカルユーザーの管理" 。

セキュリティ上の理由から、ローカル ユーザーのパスワードは宛先グリッドに複製されません。ローカル ユーザーが宛先グリッド上の Tenant Manager にアクセスする必要がある場合、テナント アカウントのルート ユーザーは、宛先グリッド上のそのユーザーのパスワードを追加する必要があります。手順については、"ローカルユーザーの管理" 。

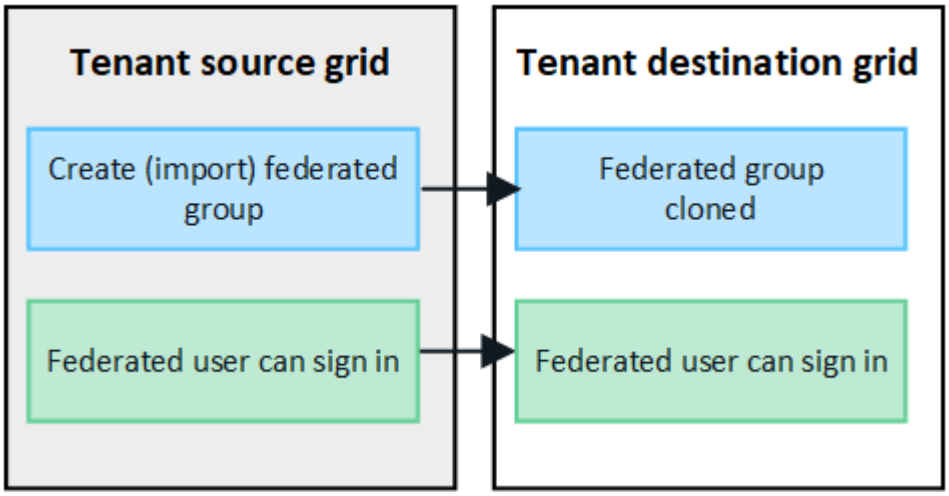


ソースグリッド上に作成されたフェデレーショングループはクローン化されます

アカウントクローンを使用するための要件を想定すると、"シングルサインオン"そして"アイデンティティフェデレーション"条件が満たされると、ソース グリッドのテナント用に作成 (インポート) したフェデレーション グループは、宛先グリッドのテナントに自動的に複製されます。

両方のグループには、同じアクセス モード、グループ権限、および S3 グループ ポリシーがあります。

ソース テナントに対してフェデレーション グループが作成され、宛先テナントに複製されると、フェデレーション ユーザーはどちらのグリッド上のテナントにもサインインできるようになります。

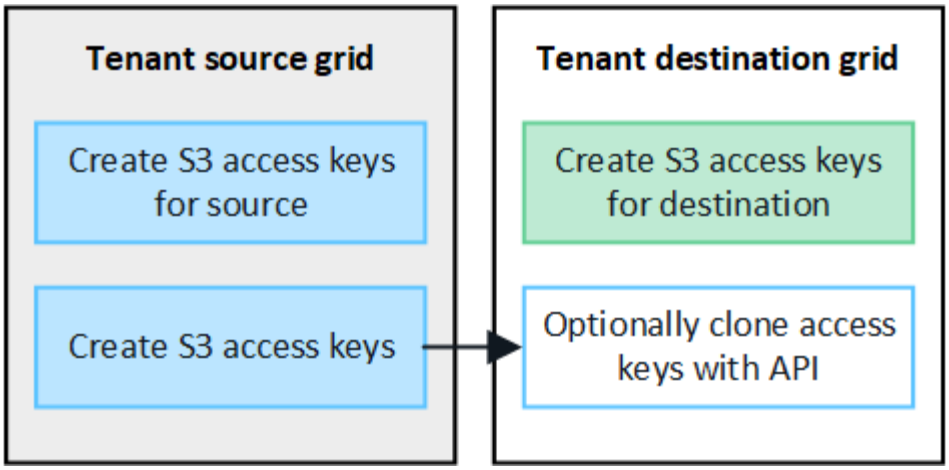


S3アクセスキーは手動で複製できます

StorageGRID は、グリッドごとに異なるキーを持つことでセキュリティが向上するため、S3 アクセス キーを自動的に複製しません。

2 つのグリッド上のアクセス キーを管理するには、次のいずれかを実行します。

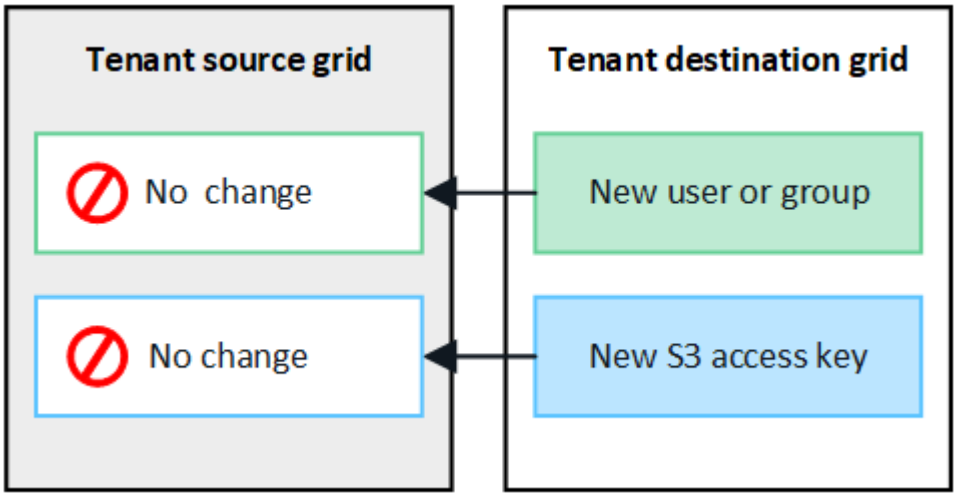
- 各グリッドに同じキーを使用する必要がない場合は、"独自のアクセスキーを作成する"または"別のユーザーのアクセスキーを作成する"各グリッド上。
- 両方のグリッドで同じキーを使用する必要がある場合は、ソースグリッドでキーを作成し、テナントマネージャーAPIを使用して手動で"キーを複製する"目的のグリッドへ。



フェデレーション ユーザーの S3 アクセス キーを複製すると、ユーザーと S3 アクセス キーの両方が宛先テナントに複製されます。

宛先グリッドに追加されたグループとユーザーは複製されません

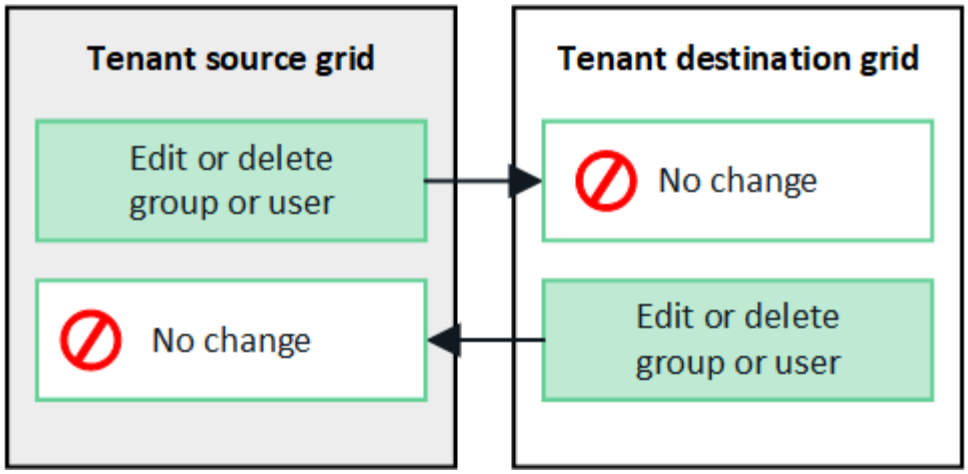
クローン作成は、テナントのソース グリッドからテナントの宛先グリッドにのみ行われます。テナントの宛先グリッドにグループとユーザーを作成またはインポートした場合、 StorageGRID はこれらの項目をテナントのソース グリッドに複製しません。



編集または削除されたグループ、ユーザー、アクセスキーは複製されません

クローン作成は、新しいグループとユーザーを作成するときにのみ行われます。

どちらかのグリッドでグループ、ユーザー、またはアクセス キーを編集または削除しても、変更内容は他のグリッドに複製されません。



API を使用して S3 アクセスキーを複製する

テナント アカウントに グリッド フェデレーション接続の使用 権限がある場合は、テナント管理 API を使用して、ソース グリッドのテナントから宛先グリッドのテナントに S3 アクセス キーを手動で複製できます。

開始する前に

- テナント アカウントには、グリッド フェデレーション接続の使用 権限があります。
- グリッド フェデレーション接続の 接続ステータス は 接続済み です。
- テナントのソースグリッドのテナントマネージャにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは、"独自のS3認証情報またはルートアクセス権限を管理する" 。
- ローカル ユーザーのアクセス キーを複製する場合、そのユーザーは両方のグリッドに既に存在します。

> フェデレーション ユーザーの S3 アクセス キーを複製すると、ユーザーと S3 アクセス キーの両方が宛先テナントに追加されます。

独自のアクセスキーを複製する

両方のグリッドで同じバケットにアクセスする必要がある場合は、独自のアクセス キーを複製できます。

手順

1. ソースグリッド上のテナントマネージャを使用して、"独自のアクセスキーを作成する"ダウンロードして `.csv`ファイル。
2. テナント マネージャーの上部から、ヘルプ アイコンを選択し、**API** ドキュメント を選択します。
3. **s3** セクションで、次のエンドポイントを選択します。

   ```
   POST /org/users/current-user/replicate-s3-access-key
   ```

4. *試してみる*を選択します。

5. **body** テキスト ボックスで、**accessKey** と **secretAccessKey** の例のエントリを、ダウンロードした **.csv** ファイルの値に置き換えます。

   各文字列を囲む二重引用符を必ず保持してください。

6. キーの有効期限が切れる場合は、**expires***の例のエントリを、**ISO 8601**データ時間形式の文字列として有効期限の日時で置き換えます（例： `2024-02-28T22:46:33-08:00` ）。キーに有効期限がない場合は、***expires** エントリの値として **null** を入力します (または **Expires** 行とその前のカンマを削除します)。
7. *実行*を選択します。
8. サーバー応答コードが **204** であることを確認します。これは、キーが宛先グリッドに正常に複製されたことを示します。

他のユーザーのアクセスキーを複製する

両方のグリッドで同じバケットにアクセスする必要がある場合は、別のユーザーのアクセス キーを複製できます。

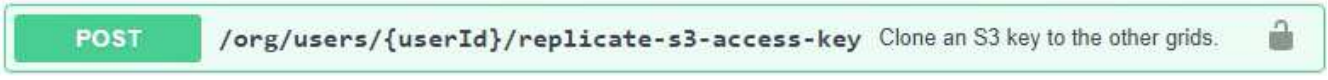
手順

1. ソースグリッド上のテナントマネージャを使用して、"他のユーザーのS3アクセスキーを作成する"ダウンロードして `.csv`ファイル。
2. テナント マネージャーの上部から、ヘルプ アイコンを選択し、**API** ドキュメント を選択します。
3. ユーザーIDを取得します。他のユーザーのアクセス キーを複製するには、この値が必要になります。
   a. **users** セクションから、次のエンドポイントを選択します。

      `GET /org/users`

   b. *試してみる*を選択します。
   c. ユーザーを検索するときに使用するパラメータを指定します。
   d. *実行*を選択します。
   e. キーを複製するユーザーを見つけて、**id** フィールドの番号をコピーします。
4. **s3** セクションで、次のエンドポイントを選択します。

   `POST /org/users/{userId}/replicate-s3-access-key`



5. *試してみる*を選択します。
6. **userId** テキスト ボックスに、コピーしたユーザー ID を貼り付けます。
7. 本文 テキスト ボックスで、サンプル アクセス キー と シークレット アクセス キー の例のエントリを、そのユーザーの **.csv** ファイルの値に置き換えます。

   文字列を囲む二重引用符を必ず保持してください。

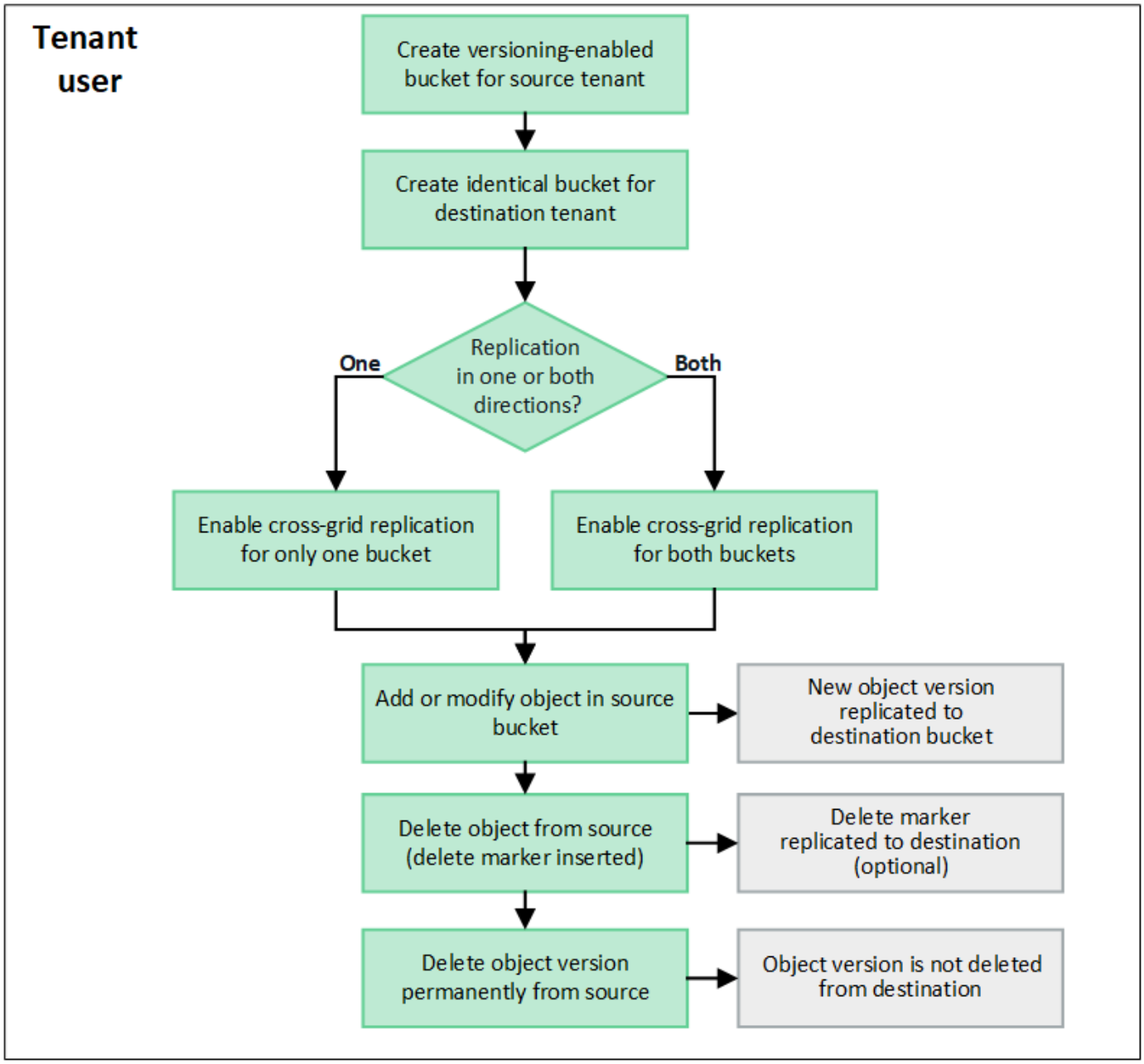
8. キーの有効期限が切れる場合は、**expires***の例のエントリを、**ISO 8601**データ時間形式の文字列として有効期限の日時で置き換えます（例： `2023-02-28T22:46:33-08:00` ）。キーに有効期限がない場合は、***expires** エントリの値として **null** を入力します (または **Expires** 行とその前のカンマを削除します)。
9. *実行*を選択します。
10. サーバー応答コードが **204** であることを確認します。これは、キーが宛先グリッドに正常に複製されたことを示します。

クロスグリッドレプリケーションを管理する

テナント アカウントの作成時に グリッド フェデレーション接続の使用 権限が割り当てられている場合は、クロス グリッド レプリケーションを使用して、テナントのソース グリッド上のバケットとテナントの宛先グリッド上のバケット間でオブジェクトを自動的に複製できます。グリッド間のレプリケーションは、一方向または双方向で発生する可能性があります。

クロスグリッドレプリケーションのワークフロー

ワークフロー図は、2 つのグリッド上のバケット間のグリッド間レプリケーションを構成するために実行する手順をまとめたものです。これらの手順については以下で詳しく説明します。



クロスグリッドレプリケーションを構成する

クロスグリッドレプリケーションを使用する前に、各グリッドの対応するテナント アカウントにサインインし、同一のバケットを作成する必要があります。次に、いずれかまたは両方のバケットでクロスグリッド レプリケーションを有効にできます。

開始する前に

- クロスグリッド レプリケーションの要件を確認しました。見る"クロスグリッドレプリケーションとは" 。
- 使用しています"サポートされているウェブブラウザ"。
- テナント アカウントには グリッド フェデレーション接続を使用する 権限があり、両方のグリッドに同一のテナント アカウントが存在します。見る"グリッドフェデレーション接続に許可されたテナントを管理する" 。
- サインインするテナントユーザーは両方のグリッドに既に存在し、"ルートアクセス権限" 。

- テナントの宛先グリッドにローカル ユーザーとしてサインインする場合、テナント アカウントのルート ユーザーがそのグリッド上のユーザー アカウントのパスワードを設定しています。

同一のバケットを2つ作成する

最初のステップとして、各グリッドの対応するテナント アカウントにサインインし、同一のバケットを作成します。

手順

1. グリッド フェデレーション接続のいずれかのグリッドから開始して、新しいバケットを作成します。
   a. 両方のグリッドに存在するテナント ユーザーの資格情報を使用して、テナント アカウントにSign in。

      ローカル ユーザーとしてテナントの宛先グリッドにサインインできない場合は、テナント アカウントのルート ユーザーがユーザー アカウントのパスワードを設定していることを確認します。

   b. 指示に従って"S3バケットを作成する"。
   c. *オブジェクト設定の管理*タブで、*オブジェクトのバージョン管理を有効にする*を選択します。
   d. StorageGRIDシステムで S3 オブジェクト ロックが有効になっている場合は、バケットで S3 オブジェクト ロックを有効にしないでください。
   e. *バケットを作成*を選択します。
   f. *完了*を選択します。
2. これらの手順を繰り返して、グリッド フェデレーション接続内の他のグリッド上の同じテナント アカウントに対して同一のバケットを作成します。

   必要に応じて、各バケットは異なるリージョンを使用できます。

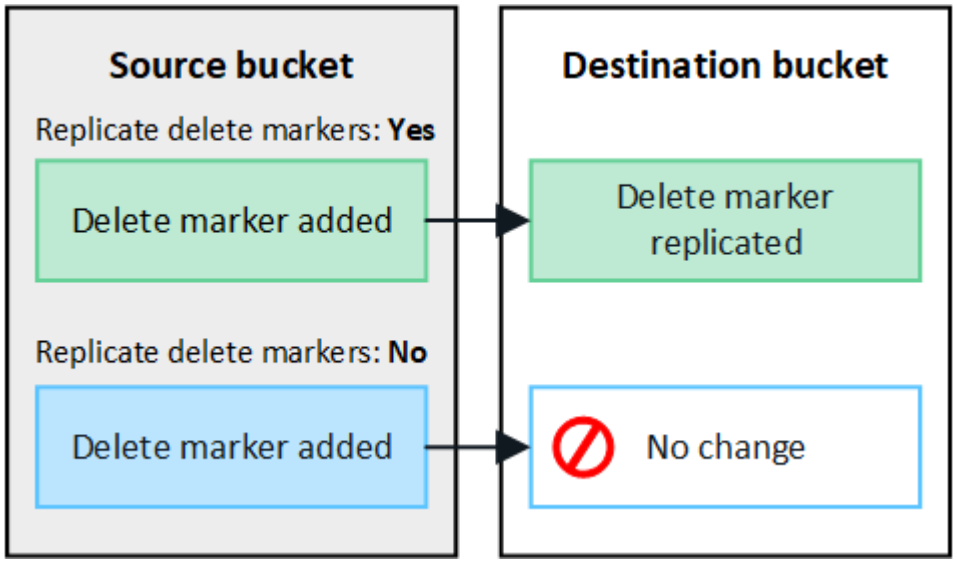
クロスグリッドレプリケーションを有効にする

いずれかのバケットにオブジェクトを追加する前に、これらの手順を実行する必要があります。

手順

1. 複製したいオブジェクトがあるグリッドから開始し、"一方向のクロスグリッドレプリケーション" :
   a. バケットのテナント アカウントにSign in。
   b. ダッシュボードから*バケットの表示*を選択するか、ストレージ **(S3)** > *バケット*を選択します。
   c. バケットの詳細ページにアクセスするには、テーブルからバケット名を選択します。
   d. *クロスグリッドレプリケーション*タブを選択します。
   e. *有効*を選択し、要件のリストを確認します。
   f. すべての要件が満たされている場合は、使用するグリッド フェデレーション接続を選択します。
   g. オプションで、削除マーカーを複製する の設定を変更して、S3 クライアントがバージョン ID を含まないソース グリッドへの削除リクエストを発行した場合に、宛先グリッドで何が起こるかを決定します。

- はい (デフォルト): 削除マーカーがソース バケットに追加され、宛先バケットに複製されます。
- いいえ: 削除マーカーはソースバケットに追加されますが、宛先バケットには複製されません。



削除リクエストにバージョン ID が含まれている場合、そのオブジェクト バージョンはソース バケットから完全に削除されます。StorageGRID はバージョン ID を含む削除要求を複製しないため、同じオブジェクト バージョンが宛先から削除されません。

見る"クロスグリッドレプリケーションとは"詳細については。

a. 必要に応じて、クロスグリッド レプリケーション 監査カテゴリの設定を変更して、監査メッセージの量を管理します。
   - エラー (デフォルト): 監査出力には、失敗したクロスグリッド レプリケーション要求のみが含まれます。
   - 通常: すべてのクロスグリッド レプリケーション要求が含まれるため、監査出力の量が大幅に増加します。
b. 選択内容を確認します。両方のバケットが空でない限り、これらの設定を変更することはできません。
c. *有効化してテスト*を選択します。

   しばらくすると、成功メッセージが表示されます。このバケットに追加されたオブジェクトは、他のグリッドに自動的に複製されるようになります。クロスグリッド レプリケーション は、バケットの詳細ページで有効な機能として表示されます。

2. オプションとして、他のグリッドの対応するバケットに移動し、"双方向のグリッド間レプリケーションを有効にする" 。

グリッド間のレプリケーションをテストする

バケットに対してクロスグリッド レプリケーションが有効になっている場合は、接続とクロスグリッド レプリケーションが正しく機能していること、およびソース バケットと宛先バケットがすべての要件を満たしていること (たとえば、バージョン管理がまだ有効になっていること) を確認する必要がある場合があります。

開始する前に

- 使用しています"サポートされているウェブブラウザ"。
- あなたは、"ルートアクセス権限" 。

手順

1. バケットのテナント アカウントにSign in。
2. ダッシュボードから*バケットの表示*を選択するか、ストレージ **(S3)** > *バケット*を選択します。
3. バケットの詳細ページにアクセスするには、テーブルからバケット名を選択します。
4. *クロスグリッドレプリケーション*タブを選択します。
5. *テスト接続*を選択します。

   接続が正常な場合は、成功バナーが表示されます。それ以外の場合はエラー メッセージが表示され、グリッド管理者はそのメッセージを使用して問題を解決できます。詳細については、 "グリッドフェデレーションエラーのトラブルシューティング" 。

6. クロスグリッド レプリケーションが双方向で実行されるように構成されている場合は、他のグリッドの対応するバケットに移動し、[テスト接続] を選択して、クロスグリッド レプリケーションが反対方向で動作していることを確認します。

クロスグリッドレプリケーションを無効にする

オブジェクトを他のグリッドにコピーする必要がなくなった場合は、グリッド間のレプリケーションを完全に停止できます。

クロスグリッド レプリケーションを無効にする前に、次の点に注意してください。

- グリッド間のレプリケーションを無効にしても、グリッド間ですでにコピーされているオブジェクトは削除されません。例えば、 `my-bucket`グリッド1にコピーされた `my-bucket`グリッド 2 のバケットのクロスグリッド レプリケーションを無効にしても、そのバケットのクロスグリッド レプリケーションは削除されません。これらのオブジェクトを削除する場合は、手動で削除する必要があります。
- 各バケットに対してクロスグリッド レプリケーションが有効になっている場合 (つまり、双方向でレプリケーションが行われる場合)、いずれかまたは両方のバケットに対してクロスグリッド レプリケーションを無効にすることができます。たとえば、オブジェクトの複製を無効にしたい場合、 `my-bucket`グリッド1から `my-bucket`グリッド2では、 `my-bucket`グリッド2から `my-bucket`グリッド1上。
- グリッド フェデレーション接続を使用するためのテナントの権限を削除する前に、クロス グリッド レプリケーションを無効にする必要があります。見る"許可されたテナントを管理する" 。
- オブジェクトを含むバケットのクロスグリッド レプリケーションを無効にすると、ソース バケットと宛先バケットの両方からすべてのオブジェクトを削除しない限り、クロスグリッド レプリケーションを再度有効にすることはできません。

> 両方のバケットが空でない限り、レプリケーションを再度有効にすることはできません。

開始する前に

- 使用しています"サポートされているウェブブラウザ"。
- あなたは、"ルートアクセス権限" 。

手順

1. 複製する必要がなくなったオブジェクトを含むグリッドから開始して、バケットのグリッド間レプリケーションを停止します。
   a. バケットのテナント アカウントにSign in。
   b. ダッシュボードから*バケットの表示*を選択するか、ストレージ **(S3)** > *バケット*を選択します。
   c. バケットの詳細ページにアクセスするには、テーブルからバケット名を選択します。
   d. *クロスグリッドレプリケーション*タブを選択します。
   e. *レプリケーションを無効にする*を選択します。
   f. このバケットのクロスグリッド レプリケーションを無効にする場合は、テキスト ボックスに「はい」と入力し、「無効」を選択します。

      しばらくすると、成功メッセージが表示されます。このバケットに追加された新しいオブジェクトは、他のグリッドに自動的に複製できなくなります。 クロスグリッド レプリケーション は、バケット ページで有効な機能として表示されなくなりました。

2. クロスグリッド レプリケーションが双方向で実行されるように構成されている場合は、他のグリッド上の対応するバケットに移動し、反対方向のクロスグリッド レプリケーションを停止します。

グリッドフェデレーション接続を表示する

テナント アカウントに グリッド フェデレーション接続の使用 権限がある場合は、許可された接続を表示できます。

開始する前に

- テナント アカウントには、グリッド フェデレーション接続の使用 権限があります。
- テナントマネージャーにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは、"ルートアクセス権限" 。

手順

1. ストレージ **(S3)** > グリッド フェデレーション接続 を選択します。

   グリッド フェデレーション接続ページが表示され、次の情報をまとめた表が含まれます。

列	説明
接続名	このテナントが使用権限を持つグリッド フェデレーション接続。
クロスグリッドレプリケーションを備えたバケット	グリッド フェデレーション接続ごとに、クロス グリッド レプリケーションが有効になっているテナント バケット。これらのバケットに追加されたオブジェクトは、接続内の他のグリッドに複製されます。
最後のエラー	各グリッド フェデレーション接続について、データが他のグリッドに複製されているときに発生した最新のエラー (ある場合)。見る最後のエラーをクリアする 。

2. オプションでバケット名を選択して"バケットの詳細を表示"。

最後のエラーをクリアする

次のいずれかの理由により、「最後のエラー」列にエラーが表示される場合があります。

- ソース オブジェクト バージョンが見つかりませんでした。
- ソースバケットが見つかりませんでした。
- 宛先バケットが削除されました。
- 宛先バケットが別のアカウントによって再作成されました。
- 宛先バケットのバージョン管理が停止されています。
- 宛先バケットは同じアカウントによって再作成されましたが、現在はバージョン管理されていません。

> この列には、最後に発生したグリッド間レプリケーション エラーのみが表示されます。以前に発生した可能性のあるエラーは表示されません。

手順

1. *最後のエラー*列にメッセージが表示された場合は、メッセージ テキストを表示します。

   たとえば、このエラーは、クロスグリッド レプリケーションの宛先バケットが無効な状態であったことを示します。これは、バージョン管理が中断されていたか、S3 オブジェクト ロックが有効になっていたことが原因である可能性があります。

2. 推奨されるアクションを実行します。たとえば、クロスグリッド レプリケーションの宛先バケットでバージョン管理が中断されていた場合は、そのバケットのバージョン管理を再度有効にします。
3. 表から接続を選択します。
4. *エラーをクリア*を選択します。
5. メッセージをクリアしてシステムのステータスを更新するには、[はい] を選択します。
6. 5 ～ 6 分待ってから、新しいオブジェクトをバケットに取り込みます。エラーメッセージが再度表示されないことを確認します。

   > エラー メッセージを確実にクリアするには、新しいオブジェクトを取り込む前に、メッセージ内のタイムスタンプから少なくとも 5 分間待機します。

7. バケットエラーにより複製に失敗したオブジェクトがあるかどうかを確認するには、"失敗したレプリケーション操作を識別して再試行する" 。

グループとユーザーの管理

アイデンティティフェデレーションを使用する

アイデンティティ フェデレーションを使用すると、テナント グループとユーザーの設定が高速化され、テナント ユーザーは使い慣れた資格情報を使用してテナント アカウントにサインインできるようになります。

テナント マネージャーの **ID** フェデレーションを構成する

テナント グループとユーザーを Active Directory、Azure Active Directory (Azure AD)、OpenLDAP、Oracle Directory Server などの別のシステムで管理する場合は、テナント マネージャーの ID フェデレーションを構成できます。

開始する前に

- テナントマネージャーにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは、"ルートアクセス権限" 。
- ID プロバイダーとして、Active Directory、Azure AD、OpenLDAP、または Oracle Directory Server を使用しています。

> リストされていない LDAP v3 サービスを使用する場合は、テクニカル サポートにお問い合わせください。

- OpenLDAP を使用する予定の場合は、OpenLDAP サーバーを構成する必要があります。見るOpenLDAP サーバーの設定ガイドライン 。
- LDAP サーバーとの通信にトランスポート層セキュリティ (TLS) を使用する予定の場合、ID プロバイダーは TLS 1.2 または 1.3 を使用する必要があります。見る"送信 TLS 接続でサポートされている暗号" 。

タスク概要

テナントに対して ID フェデレーション サービスを構成できるかどうかは、テナント アカウントの設定方法によって異なります。テナントは、Grid Manager 用に構成された ID フェデレーション サービスを共有する場合があります。 「アイデンティティ フェデレーション」ページにアクセスしたときにこのメッセージが表示される場合、このテナントに対して個別のフェデレーション ID ソースを構成することはできません。

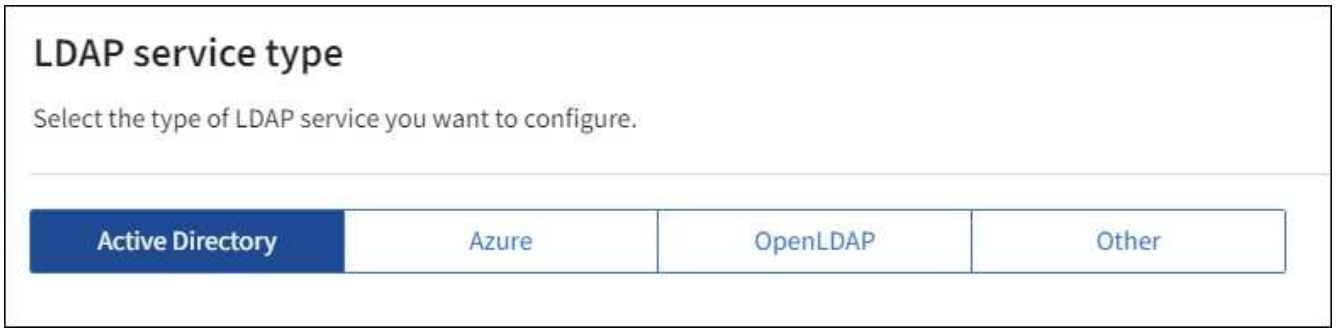
> This tenant account uses the LDAP server that is configured for the Grid Manager. Contact the grid administrator for information or to change this setting.

設定を入力

ID フェデレーションを構成するときは、 StorageGRID がLDAP サービスに接続するために必要な値を指定します。

手順

1. アクセス管理 > *アイデンティティ連携*を選択します。
2. **ID** フェデレーションを有効にする を選択します。
3. LDAP サービス タイプ セクションで、構成する LDAP サービスのタイプを選択します。



Oracle Directory Server を使用する LDAP サーバーの値を構成するには、「その他」を選択します。

4. *その他*を選択した場合は、LDAP 属性セクションのフィールドに入力します。次の手順に進みます。
   - ユーザーの一意の名前: LDAP ユーザーの一意の識別子を含む属性の名前。この属性は、`sAMAccountName` Active Directoryおよび `uid`OpenLDAP 用。`Oracle Directory Server`を構成する場合は、次のように入力します。 `uid`。
   - ユーザー **UUID**: LDAP ユーザーの永続的な一意の識別子を含む属性の名前。この属性は、`objectGUID` Active Directoryおよび `entryUUID`OpenLDAP 用。`Oracle Directory Server`を構成する場合は、次のように入力します。 `nsuniqueid`。指定された属性の各ユーザーの値は、16 バイト形式または文字列形式の 32 桁の 16 進数である必要があります。ハイフンは無視されます。
   - グループの一意の名前: LDAP グループの一意の識別子を含む属性の名前。この属性は、`sAMAccountName` Active Directoryおよび `cn`OpenLDAP 用。`Oracle Directory Server`を構成する場合は、次のように入力します。 `cn`。
   - グループ **UUID**: LDAP グループの永続的な一意の識別子を含む属性の名前。この属性は、`objectGUID` Active Directoryおよび `entryUUID`OpenLDAP 用。`Oracle Directory Server`を構成する場合は、次のように入力します。 `nsuniqueid`。指定された属性の各グループの値は、16 バイト形式または文字列形式の 32 桁の 16 進数である必要があります。ハイフンは無視されます。
5. すべての LDAP サービス タイプについて、[LDAP サーバーの構成] セクションで必要な LDAP サーバーおよびネットワーク接続情報を入力します。
   - ホスト名: LDAP サーバーの完全修飾ドメイン名 (FQDN) または IP アドレス。
   - ポート: LDAP サーバーに接続するために使用されるポート。

     STARTTLS のデフォルト ポートは 389 で、LDAPS のデフォルト ポートは 636 です。ただし、ファイアウォールが正しく設定されている限り、どのポートでも使用できます。

   - ユーザー名: LDAP サーバーに接続するユーザーの識別名 (DN) の完全パス。

     Active Directory の場合は、ダウンレベル ログオン名またはユーザー プリンシパル名を指定することもできます。

     指定されたユーザーには、グループとユーザーを一覧表示し、次の属性にアクセスする権限が必要です。

     - `sAMAccountName`または `uid`
     - `objectGUID`、 `entryUUID` 、 または `nsuniqueid`
     - `cn`

- `memberOf`または `isMemberOf`
- アクティブディレクトリ: `objectSid`、 `primaryGroupID`、 `userAccountControl`、 そして `userPrincipalName`
- アズール: `accountEnabled`そして `userPrincipalName`

◦ パスワード: ユーザー名に関連付けられたパスワード。

> 将来パスワードを変更する場合は、このページで更新する必要があります。

◦ グループ ベース **DN**: グループを検索する LDAP サブツリーの識別名 (DN) の完全パス。 Active Directory の例 (下記) では、識別名がベース DN (DC=storagegrid、DC=example、DC=com) を基準とするすべてのグループをフェデレーション グループとして使用できます。

> グループの一意の名前*の値は、それが属する *グループ ベース **DN** 内で一意である必要があります。

◦ ユーザー ベース **DN**: ユーザーを検索する LDAP サブツリーの識別名 (DN) の完全パス。

> ユーザー固有名 の値は、それが属する ユーザー ベース **DN** 内で一意である必要があります。

◦ バインド ユーザー名の形式 (オプション): パターンを自動的に決定できない場合にStorageGRIDが使用するデフォルトのユーザー名パターン。

StorageGRID がサービス アカウントにバインドできない場合にユーザーがサインインできるように、バインド ユーザー名形式 を指定することをお勧めします。

次のいずれかのパターンを入力します。

- **UserPrincipalName** パターン **(Active Directory** および **Azure)**: `[USERNAME]@*example*.com`
- ダウンレベル ログオン名パターン **(Active Directory** および **Azure)**: `*example*\[USERNAME]`
- 識別名パターン: `CN=[USERNAME],CN=Users,DC=*example*,DC=com`

[USERNAME] を記載どおりに入力してください。

6. [トランスポート層セキュリティ (TLS)] セクションで、セキュリティ設定を選択します。

◦ **STARTTLS** を使用する: STARTTLS を使用して、LDAP サーバーとの通信を保護します。これは、Active Directory、OpenLDAP、またはその他の場合に推奨されるオプションですが、このオプションは Azure ではサポートされていません。

◦ **LDAPS** を使用する: LDAPS (LDAP over SSL) オプションは、TLS を使用して LDAP サーバーへの接続を確立します。Azure の場合はこのオプションを選択する必要があります。

◦ **TLS** を使用しない: StorageGRIDシステムと LDAP サーバー間のネットワーク トラフィックは保護されません。このオプションは Azure ではサポートされていません。

> Active Directory サーバーが LDAP 署名を強制している場合、「TLS を使用しない」オプションの使用はサポートされません。STARTTLS または LDAPS を使用する必要があります。

7. STARTTLS または LDAPS を選択した場合は、接続を保護するために使用する証明書を選択します。
   - オペレーティング システムの **CA** 証明書を使用する: オペレーティング システムにインストールされているデフォルトの Grid CA 証明書を使用して、接続を保護します。
   - カスタム **CA** 証明書を使用する: カスタム セキュリティ証明書を使用します。

     この設定を選択した場合は、カスタム セキュリティ証明書をコピーして CA 証明書テキスト ボックスに貼り付けます。

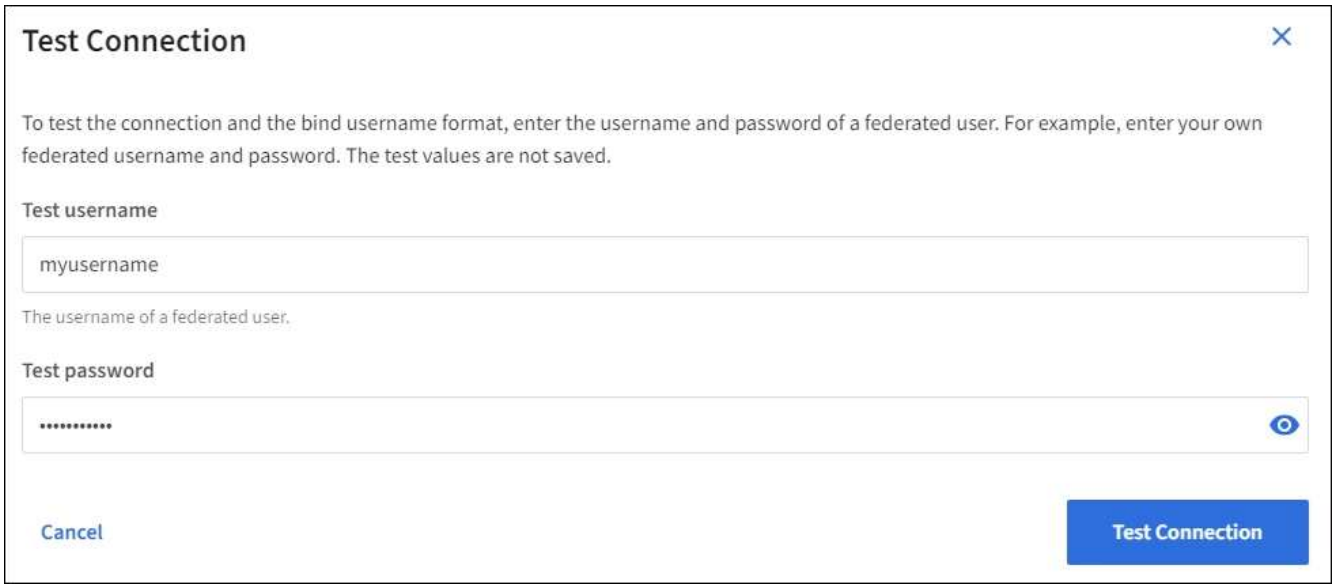
接続をテストし、設定を保存します

すべての値を入力した後、構成を保存する前に接続をテストする必要があります。 StorageGRID は、LDAP サーバーの接続設定と、指定された場合はバインド ユーザー名の形式を検証します。

手順

1. *テスト接続*を選択します。
2. バインドユーザー名の形式を指定しなかった場合:
   - 接続設定が有効な場合は、「テスト接続が成功しました」というメッセージが表示されます。設定を保存するには、[保存] を選択します。
   - 接続設定が無効な場合、「テスト接続を確立できませんでした」というメッセージが表示されます。 *閉じる*を選択します。次に、問題を解決して、再度接続をテストします。
3. バインド ユーザー名形式を指定した場合は、有効なフェデレーション ユーザーのユーザー名とパスワードを入力します。

   たとえば、独自のユーザー名とパスワードを入力します。ユーザー名には @ や / などの特殊文字を含めないでください。



   - 接続設定が有効な場合は、「テスト接続が成功しました」というメッセージが表示されます。設定を保存するには、[保存] を選択します。
   - 接続設定、バインド ユーザー名の形式、またはテスト ユーザー名とパスワードが無効な場合は、エラー メッセージが表示されます。問題を解決して、再度接続をテストしてください。

アイデンティティソースとの強制同期

StorageGRIDシステムは、フェデレーション グループとユーザーを ID ソースから定期的に同期します。できるだけ早くユーザー権限を有効化または制限したい場合は、同期を強制的に開始できます。

手順

1. アイデンティティ フェデレーション ページに移動します。
2. ページの上部にある*同期サーバー*を選択します。

   環境によっては同期プロセスに時間がかかる場合があります。

> アイデンティティ ソースからのフェデレーション グループとユーザーの同期に問題がある場合、アイデンティティ フェデレーション同期の失敗 アラートがトリガーされます。

ID連携を無効にする

グループおよびユーザーの ID フェデレーションを一時的または永続的に無効にすることができます。アイデンティティ フェデレーションが無効になっている場合、 StorageGRIDとアイデンティティ ソース間の通信は行われません。ただし、構成した設定はすべて保持されるため、将来、簡単に ID フェデレーションを再度有効にすることができます。

タスク概要

ID フェデレーションを無効にする前に、次の点に注意してください。

- フェデレーション ユーザーはサインインできなくなります。
- 現在サインインしているフェデレーション ユーザーは、セッションの有効期限が切れるまでStorageGRIDシステムへのアクセスを保持しますが、セッションの有効期限が切れた後はサインインできなくなります。
- StorageGRIDシステムとアイデンティティ ソース間の同期は行われず、同期されていないアカウントに対してアラートは発生しません。
- シングル サインオン (SSO) が 有効 または サンドボックス モード に設定されている場合、**ID** フェデレーションを有効にする チェックボックスは無効になります。ID フェデレーションを無効にする前に、シングル サインオン ページの SSO ステータスを 無効 にする必要があります。見る"シングルサインオンを無効にする" 。

手順

1. アイデンティティ フェデレーション ページに移動します。
2. **ID** フェデレーションを有効にする チェックボックスをオフにします。

OpenLDAPサーバーの設定ガイドライン

ID フェデレーションに OpenLDAP サーバーを使用する場合は、OpenLDAP サーバーで特定の設定を構成する必要があります。

> ActiveDirectory または Azure 以外の ID ソースの場合、 StorageGRID は外部的に無効になっているユーザーへの S3 アクセスを自動的にブロックしません。S3 アクセスをブロックするには、ユーザーの S3 キーを削除するか、すべてのグループからユーザーを削除します。

Memberof と refint オーバーレイ

memberof および refint オーバーレイを有効にする必要があります。詳細については、http://www.openldap.org/doc/admin24/index.html["OpenLDAP ドキュメント: バージョン 2.4 管理者ガイド"^] 。

インデックス作成

指定されたインデックス キーワードを使用して、次の OpenLDAP 属性を設定する必要があります。

- `olcDbIndex: objectClass eq`
- `olcDbIndex: uid eq,pres,sub`
- `olcDbIndex: cn eq,pres,sub`
- `olcDbIndex: entryUUID eq`

さらに、最適なパフォーマンスを得るために、ユーザー名のヘルプに記載されているフィールドがインデックス化されていることを確認してください。

逆グループメンバーシップ維持に関する情報は、http://www.openldap.org/doc/admin24/index.html["OpenLDAP ドキュメント: バージョン 2.4 管理者ガイド"^] 。

テナントグループの管理

S3テナントのグループを作成する

フェデレーテッド グループをインポートするか、ローカル グループを作成することによって、S3 ユーザー グループの権限を管理できます。

開始する前に

- テナントマネージャーにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは、"ルートアクセス権限" 。
- フェデレーショングループをインポートする予定の場合は、"構成されたID連携" 、フェデレーション グループは構成された ID ソースにすでに存在します。
- テナントアカウントに*グリッドフェデレーション接続を使用する*権限がある場合は、ワークフローと考慮事項を確認しました。"テナントグループとユーザーの複製" 、テナントのソース グリッドにサインインしています。

グループ作成ウィザードにアクセスする

最初のステップとして、グループの作成ウィザードにアクセスします。

手順

1. アクセス管理 > *グループ*を選択します。
2. テナント アカウントに グリッド フェデレーション接続の使用 権限がある場合は、このグリッドで作成された新しいグループが接続内の他のグリッド上の同じテナントに複製されることを示す青いバナーが表示されることを確認します。このバナーが表示されない場合は、テナントの宛先グリッドにサインインしている可能性があります。

3. *グループを作成*を選択します。

グループの種類を選択

ローカル グループを作成したり、フェデレーション グループをインポートしたりできます。

手順

1. ローカル グループを作成するには ローカル グループ タブを選択し、以前に構成した ID ソースからグループをインポートするには フェデレーション グループ タブを選択します。

   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、ローカル グループに属するユーザーは、グループの権限に基づいてクライアント アプリケーションを使用してテナントのリソースを管理することはできますが、テナント マネージャにサインインすることはできません。

2. グループの名前を入力します。
   - ローカル グループ: 表示名と一意の名前の両方を入力します。表示名は後で編集できます。

     テナント アカウントに グリッド フェデレーション接続の使用 権限がある場合、宛先グリッドのテナントに同じ 一意の名前 がすでに存在すると、複製エラーが発生します。

   - フェデレーション グループ: 一意の名前を入力します。 Active Directoryの場合、一意の名前は `sAMAccountName`属性。 OpenLDAPの場合、一意の名前は `uid`属性。
3. *続行*を選択します。

グループ権限を管理する

グループ権限は、ユーザーがテナント マネージャーおよびテナント管理 API で実行できるタスクを制御します。

手順

1. アクセス モード では、次のいずれかを選択します。
   - 読み取り/書き込み (デフォルト): ユーザーは Tenant Manager にサインインし、テナント構成を管理できます。
   - 読み取り専用: ユーザーは設定と機能の表示のみが可能です。テナント マネージャーまたはテナント管理 API で変更を加えたり、操作を実行したりすることはできません。ローカルの読み取り専用ユー

ザーは自分のパスワードを変更できます。

> ユーザーが複数のグループに属しており、いずれかのグループが読み取り専用に設定されている場合、ユーザーは選択したすべての設定と機能に対して読み取り専用アクセス権を持ちます。

2. このグループに対して 1 つ以上の権限を選択します。

   見る"テナント管理権限" 。

3. *続行*を選択します。

S3グループポリシーを設定する

グループ ポリシーによって、ユーザーに付与される S3 アクセス権限が決まります。

手順

1. このグループに使用するポリシーを選択します。

グループポリシー	説明
S3 アクセスなし	デフォルト。このグループのユーザーは、バケットポリシーでアクセスが許可されない限り、S3 リソースにアクセスできません。このオプションを選択すると、デフォルトではルートユーザーのみが S3 リソースにアクセスできるようになります。
読み取り専用アクセス	このグループのユーザーには、S3 リソースへの読み取り専用アクセス権があります。たとえば、このグループのユーザーはオブジェクトを一覧表示したり、オブジェクトのデータ、メタデータ、タグを読み取ったりできます。このオプションを選択すると、読み取り専用グループ ポリシーの JSON 文字列がテキスト ボックスに表示されます。この文字列は編集できません。
フル アクセス	このグループのユーザーには、バケットを含む S3 リソースへのフルアクセス権が付与されます。このオプションを選択すると、フルアクセス グループ ポリシーの JSON 文字列がテキスト ボックスに表示されます。この文字列は編集できません。
ランサムウェア対策	このサンプルポリシーは、このテナントのすべてのバケットに適用されます。このグループのユーザーは一般的なアクションを実行できますが、オブジェクトのバージョン管理が有効になっているバケットからオブジェクトを完全に削除することはできません。 *すべてのバケットの管理*権限を持つテナント マネージャー ユーザーは、このグループ ポリシーを上書きできます。すべてのバケットの管理権限を信頼できるユーザーに制限し、可能な場合は多要素認証 (MFA) を使用します。
カスタム	グループ内のユーザーには、テキスト ボックスで指定した権限が付与されます。

2. *カスタム*を選択した場合は、グループ ポリシーを入力します。各グループ ポリシーのサイズ制限は 5,120 バイトです。有効な JSON 形式の文字列を入力する必要があります。

   言語構文や例を含むグループポリシーの詳細については、以下を参照してください。"グループポリシーの例" 。

3. ローカル グループを作成する場合は、[続行] を選択します。フェデレーション グループを作成する場合は、[グループの作成] と [完了] を選択します。

ユーザーを追加する（ローカルグループのみ）

ユーザーを追加せずにグループを保存することも、オプションで既存のローカル ユーザーを追加することもできます。

> テナント アカウントに グリッド フェデレーション接続の使用 権限がある場合、ソース グリッドにローカル グループを作成するときに選択したユーザーは、グループが宛先グリッドに複製されるときには含まれません。このため、グループを作成するときにユーザーを選択しないでください。代わりに、ユーザーを作成するときにグループを選択します。

手順

1. 必要に応じて、このグループのローカル ユーザーを 1 人以上選択します。
2. *グループの作成*と*完了*を選択します。

   作成したグループがグループのリストに表示されます。

   テナント アカウントに グリッド フェデレーション接続の使用 権限があり、テナントのソース グリッドにいる場合、新しいグループはテナントの宛先グリッドに複製されます。グループの詳細ページの概要セクションに、*複製ステータス*として*成功*が表示されます。

Swiftテナントのグループを作成する

フェデレーション グループをインポートするか、ローカル グループを作成することによって、Swift テナント アカウントのアクセス権限を管理できます。少なくとも 1 つのグループに Swift 管理者権限が必要です。この権限は、Swift テナント アカウントのコンテナーとオブジェクトを管理するために必要なものです。

> Swift クライアント アプリケーションのサポートは非推奨となり、将来のリリースでは削除される予定です。

開始する前に

- テナントマネージャーにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは、"ルートアクセス権限" 。
- フェデレーショングループをインポートする予定の場合は、"構成されたID連携" 、フェデレーション グループは構成された ID ソースにすでに存在します。

グループ作成ウィザードにアクセスする

手順

最初のステップとして、グループの作成ウィザードにアクセスします。

1. アクセス管理 > *グループ*を選択します。
2. *グループを作成*を選択します。

グループの種類を選択

ローカル グループを作成したり、フェデレーション グループをインポートしたりできます。

手順

1. ローカル グループを作成するには ローカル グループ タブを選択し、以前に構成した ID ソースからグループをインポートするには フェデレーション グループ タブを選択します。

   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、ローカル グループに属するユーザーは、グループの権限に基づいてクライアント アプリケーションを使用してテナントのリソースを管理することはできますが、テナント マネージャにサインインすることはできません。

2. グループの名前を入力します。
   - ローカル グループ: 表示名と一意の名前の両方を入力します。表示名は後で編集できます。
   - フェデレーション グループ: 一意の名前を入力します。 Active Directoryの場合、一意の名前は `sAMAccountName`属性。 OpenLDAPの場合、一意の名前は `uid`属性。
3. *続行*を選択します。

グループ権限を管理する

グループ権限は、ユーザーがテナント マネージャーおよびテナント管理 API で実行できるタスクを制御します。

手順

1. アクセス モード では、次のいずれかを選択します。
   - 読み取り/書き込み (デフォルト): ユーザーは Tenant Manager にサインインし、テナント構成を管理できます。
   - 読み取り専用: ユーザーは設定と機能の表示のみが可能です。テナント マネージャーまたはテナント管理 API で変更を加えたり、操作を実行したりすることはできません。ローカルの読み取り専用ユーザーは自分のパスワードを変更できます。

   > ユーザーが複数のグループに属しており、いずれかのグループが読み取り専用に設定されている場合、ユーザーは選択したすべての設定と機能に対して読み取り専用アクセス権を持ちます。

2. グループ ユーザーが Tenant Manager または Tenant Management API にサインインする必要がある場合は、ルート アクセス チェックボックスをオンにします。
3. *続行*を選択します。

Swiftグループポリシーを設定する

Swift ユーザーは、コンテナを作成してオブジェクトを取り込むために、Swift REST API に認証するための管理者権限が必要です。

1. グループ ユーザーが Swift REST API を使用してコンテナーとオブジェクトを管理する必要がある場合は、**Swift** 管理者 チェックボックスをオンにします。
2. ローカル グループを作成する場合は、[続行] を選択します。フェデレーション グループを作成する場合は、[グループの作成] と [完了] を選択します。

ユーザーを追加する（ローカルグループのみ）

ユーザーを追加せずにグループを保存することも、オプションで既存のローカル ユーザーを追加することもできます。

手順

1. 必要に応じて、このグループのローカル ユーザーを 1 人以上選択します。

   ローカル ユーザーをまだ作成していない場合は、[ユーザー] ページでこのグループをユーザーに追加できます。見る"ローカルユーザーの管理" 。

2. *グループの作成*と*完了*を選択します。

   作成したグループがグループのリストに表示されます。

テナント管理権限

テナント グループを作成する前に、そのグループに割り当てる権限を検討してください。テナント管理権限によって、ユーザーがテナント マネージャーまたはテナント管理 API を使用して実行できるタスクが決まります。ユーザーは 1 つ以上のグループに所属できます。ユーザーが複数のグループに属している場合、権限は累積されます。

テナント マネージャーにサインインしたり、テナント管理 API を使用したりするには、ユーザーは少なくとも 1 つの権限を持つグループに属している必要があります。サインインできるすべてのユーザーは、次のタスクを実行できます。

- ダッシュボードを見る
- 自分のパスワードを変更する（ローカルユーザーの場合）

すべての権限について、グループのアクセス モード設定によって、ユーザーが設定を変更して操作を実行できるかどうか、または関連する設定と機能の表示のみが可能かどうかが決まります。

> ユーザーが複数のグループに属しており、いずれかのグループが読み取り専用に設定されている場合、ユーザーは選択したすべての設定と機能に対して読み取り専用アクセス権を持ちます。

グループには次の権限を割り当てることができます。S3 テナントと Swift テナントには異なるグループ権限があることに注意してください。

許可	説明	詳細
ルート アクセス	テナント マネージャーとテナント管理 API へのフル アクセスを提供します。	Swift ユーザーは、テナント アカウントにサインインするためにルート アクセス権限を持っている必要があります。

許可	説明	詳細
管理者	Swift テナントのみ。このテナント アカウントの Swift コンテナとオブジェクトへのフルアクセスを提供します	Swift ユーザーは、Swift REST API を使用して操作を実行するために、Swift 管理者権限を持っている必要があります。
独自のS3認証情報を管理する	ユーザーが独自の S3 アクセスキーを作成および削除できるようにします。	この権限を持たないユーザーには、ストレージ **(S3)** > マイ **S3** アクセス キー メニュー オプションは表示されません。
すべてのバケットを表示	**S3** テナント: ユーザーがすべてのバケットとバケット構成を表示できるようにします。 **Swift** テナント: Swift ユーザーがテナント管理 API を使用してすべてのコンテナとコンテナ構成を表示できるようにします。	すべてのバケットの表示権限またはすべてのバケットの管理権限を持たないユーザーには、バケット メニュー オプションは表示されません。 この権限は、すべてのバケットの管理権限に置き換えられます。これは、S3 クライアントまたは S3 コンソールで使用される S3 バケットまたはグループ ポリシーには影響しません。 この権限は、テナント管理 API から Swift グループにのみ割り当てることができます。テナント マネージャーを使用して、Swift グループにこの権限を割り当てることはできません。
すべてのバケットを管理する	**S3** テナント: ユーザーがテナント マネージャーとテナント管理 API を使用して S3 バケットを作成および削除したり、S3 バケットまたはグループ ポリシーに関係なく、テナントアカウント内のすべての S3 バケットの設定を管理したりできるようにします。 **Swift** テナント: Swift ユーザーがテナント管理 API を使用して Swift コンテナの一貫性を制御できるようにします。	すべてのバケットの表示権限またはすべてのバケットの管理権限を持たないユーザーには、バケット メニュー オプションは表示されません。 この権限は、「すべてのバケットを表示」権限よりも優先されます。これは、S3 クライアントまたは S3 コンソールで使用される S3 バケットまたはグループ ポリシーには影響しません。 この権限は、テナント管理 API から Swift グループにのみ割り当てることができます。テナント マネージャーを使用して、Swift グループにこの権限を割り当てることはできません。
エンドポイントを管理する	ユーザーがテナント マネージャまたはテナント管理 API を使用して、 StorageGRIDプラットフォーム サービスの宛先として使用されるプラットフォーム サービス エンドポイントを作成または編集できるようにします。	この権限を持たないユーザーには、プラットフォーム サービス エンドポイント メニュー オプションは表示されません。

許可	説明	詳細
S3コンソールタブを使用する	「すべてのバケットの表示」または「すべてのバケットの管理」権限と組み合わせると、ユーザーはバケットの詳細ページの S3 コンソール タブからオブジェクトを表示および管理できるようになります。	

グループの管理

必要に応じてテナント グループを管理し、グループの表示、編集、複製などを行います。

開始する前に

- テナントマネージャーにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは、"ルートアクセス権限" 。

グループを表示または編集する

各グループの基本情報や詳細を表示、編集できます。

手順

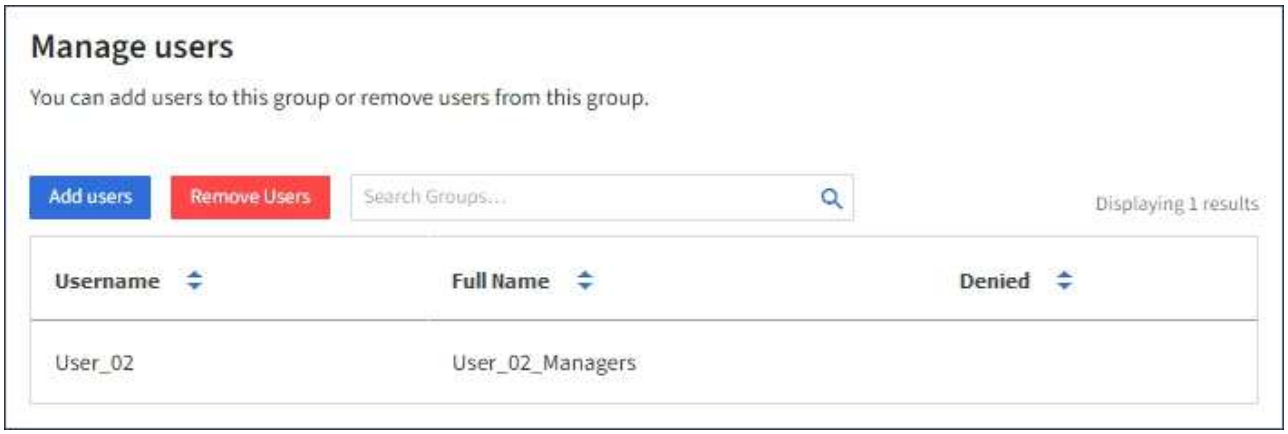
1. アクセス管理 > *グループ*を選択します。
2. [グループ] ページに提供される情報を確認します。このページには、このテナント アカウントのすべてのローカル グループとフェデレーション グループの基本情報が一覧表示されます。

   テナント アカウントに グリッド フェデレーション接続の使用 権限があり、テナントのソース グリッド上のグループを表示している場合:

   - グループを編集または削除した場合、変更内容は他のグリッドに同期されないことを示すバナーメッセージが表示されます。
   - 必要に応じて、グループが宛先グリッドのテナントに複製されなかったかどうかを示すバナー メッセージが表示されます。あなたはできるグループのクローンを再試行するそれは失敗しました。
3. グループの名前を変更する場合:
   a. グループのチェックボックスを選択します。
   b. アクション > *グループ名の編集*を選択します。
   c. 新しい名前を入力してください。
   d. *変更を保存*を選択します。
4. 詳細を表示したり、追加の編集を行ったりする場合は、次のいずれかを実行します。
   - グループ名を選択します。
   - グループのチェックボックスを選択し、[アクション] > [グループの詳細を表示] を選択します。
5. 各グループの次の情報が表示される概要セクションを確認します。
   - 表示名

- 一意の名前
- タイプ
- アクセス モード
- 権限
- S3ポリシー
- このグループのユーザー数
- テナント アカウントに グリッド フェデレーション接続の使用 権限があり、テナントのソース グリッド上のグループを表示している場合の追加フィールド:
  - クローン作成ステータス（成功*または*失敗）
  - このグループを編集または削除しても、変更内容は他のグリッドに同期されないことを示す青いバナー。

6. 必要に応じてグループ設定を編集します。見る"S3テナントのグループを作成する"そして"Swiftテナントのグループを作成する"入力内容の詳細については、こちらをご覧ください。
   a. 概要セクションで、名前または編集アイコンを選択して表示名を変更します。 。
   b. *グループの権限*タブで権限を更新し、*変更を保存*を選択します。
   c. グループ ポリシー タブで変更を行い、変更の保存 を選択します。
      - S3 グループを編集している場合は、必要に応じて別の S3 グループ ポリシーを選択するか、カスタム ポリシーの JSON 文字列を入力します。
      - Swift グループを編集している場合は、オプションで **Swift** 管理者 チェックボックスをオンまたはオフにします。
7. 1 人以上の既存のローカル ユーザーをグループに追加するには:
   a. [ユーザー]タブを選択します。



   b. *ユーザーを追加*を選択します。
   c. 追加する既存のユーザーを選択し、「ユーザーの追加」を選択します。

      右上に成功メッセージが表示されます。

8. グループからローカル ユーザーを削除するには:
   a. [ユーザー]タブを選択します。

b. *ユーザーを削除*を選択します。

c. 削除するユーザーを選択し、「ユーザーの削除」を選択します。

右上に成功メッセージが表示されます。

9. 変更したセクションごとに*変更を保存*を選択したことを確認します。

重複グループ

既存のグループを複製して、新しいグループをより迅速に作成できます。

> テナント アカウントに グリッド フェデレーション接続の使用 権限があり、テナントのソース グリッドからグループを複製する場合、複製されたグループはテナントの宛先グリッドに複製されます。

手順

1. アクセス管理 > *グループ*を選択します。
2. 複製するグループのチェックボックスを選択します。
3. アクション > *グループの複製*を選択します。
4. 見る"S3テナントのグループを作成する"または"Swiftテナントのグループを作成する"入力内容の詳細については、こちらをご覧ください。
5. *グループを作成*を選択します。

グループのクローンを再試行する

失敗したクローンを再試行するには:

1. グループ名の下に「(複製失敗)」と表示されている各グループを選択します。
2. アクション > *グループの複製*を選択します。
3. 複製する各グループの詳細ページから複製操作のステータスを表示します。

詳細については、"テナントグループとユーザーの複製"を参照してください。

1つ以上のグループを削除する

1 つ以上のグループを削除できます。削除されたグループにのみ属しているユーザーは、テナント マネージャーにサインインしたり、テナント アカウントを使用したりできなくなります。

> テナント アカウントに グリッド フェデレーション接続の使用 権限があり、グループを削除した場合、 StorageGRID は他のグリッド上の対応するグループを削除しません。この情報を同期させておく必要がある場合は、両方のグリッドから同じグループを削除する必要があります。

手順

1. アクセス管理 > *グループ*を選択します。
2. 削除する各グループのチェックボックスを選択します。
3. アクション > グループの削除 または アクション > グループの削除 を選択します。

確認ダイアログボックスが表示されます。

4. *グループの削除*または*グループの削除*を選択します。

ローカルユーザーの管理

ローカル ユーザーを作成してローカル グループに割り当て、これらのユーザーがアクセスできる機能を決定できます。テナント マネージャーには、「root」という名前の定義済みローカル ユーザーが 1 人含まれています。ローカル ユーザーを追加および削除することはできますが、ルート ユーザーを削除することはできません。

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、ローカル ユーザーは、グループ権限に基づいてクライアント アプリケーションを使用してテナントのリソースにアクセスすることはできますが、テナント マネージャまたはテナント管理 API にサインインすることはできません。

開始する前に

- テナントマネージャーにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは、"ルートアクセス権限" 。
- テナントアカウントに*グリッドフェデレーション接続を使用する*権限がある場合は、ワークフローと考慮事項を確認しました。"テナントグループとユーザーの複製" 、テナントのソース グリッドにサインインしています。

ローカルユーザーを作成する

ローカル ユーザーを作成し、そのユーザーを 1 つ以上のローカル グループに割り当てて、アクセス権限を制御できます。

どのグループにも属していない S3 ユーザーには、管理権限も S3 グループ ポリシーも適用されません。これらのユーザーには、バケットポリシーを通じて S3 バケットへのアクセスが許可されている可能性があります。

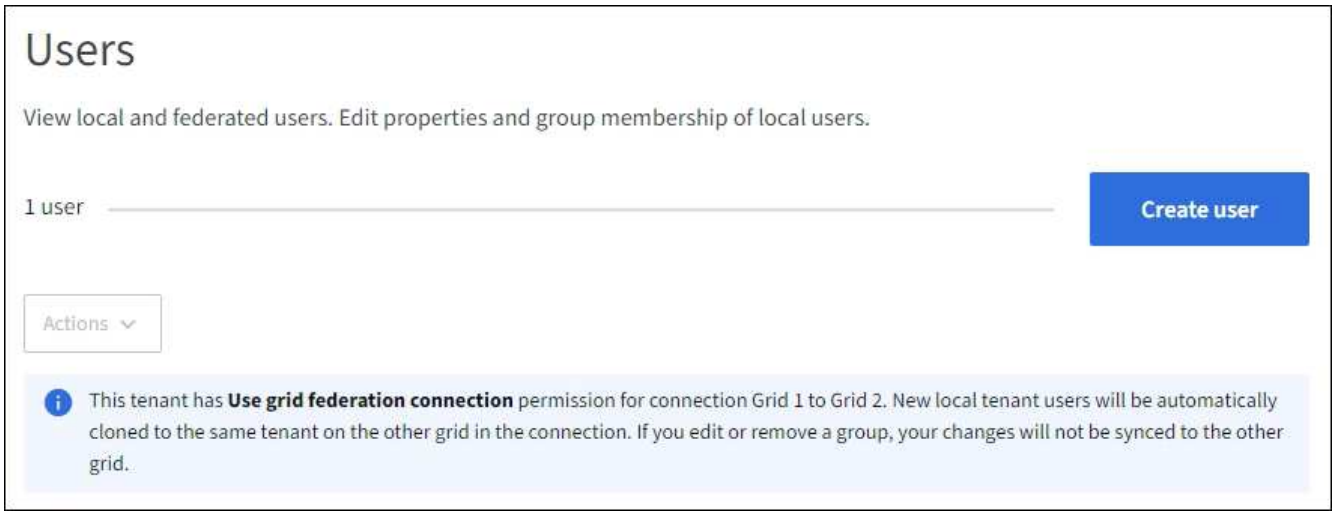
どのグループにも属していない Swift ユーザーには、管理権限も Swift コンテナへのアクセス権もありません。

ユーザー作成ウィザードにアクセスする

手順

1. アクセス管理 > *ユーザー*を選択します。

   テナント アカウントに グリッド フェデレーション接続の使用 権限がある場合、青いバナーはこれがテナントのソース グリッドであることを示します。このグリッド上に作成したローカル ユーザーは、接続内の他のグリッドに複製されます。



2. *ユーザーの作成*を選択します。

資格情報を入力してください

手順

1. *ユーザー資格情報の入力*手順では、次のフィールドに入力します。

フィールド	説明
フルネーム	このユーザーのフルネーム。たとえば、人の名と姓、またはアプリケーションの名前などです。
ユーザー名	このユーザーがサインインに使用する名前。ユーザー名は一意である必要があり、変更できません。 注意: テナント アカウントに グリッド フェデレーション接続の使用 権限がある場合、宛先グリッドのテナントに同じ ユーザー名 が既に存在すると、複製エラーが発生します。
パスワードとパスワードの確認	ユーザーがサインイン時に最初に使用するパスワード。
アクセスを拒否	このユーザーが 1 つ以上のグループに属している場合でも、テナント アカウントにサインインできないようにするには、[はい] を選択します。 たとえば、ユーザーのサインイン機能を一時的に停止するには、「はい」を選択します。

2. *続行*を選択します。

グループに割り当てる

手順

1. ユーザーを 1 つ以上のローカル グループに割り当てて、ユーザーが実行できるタスクを決定します。

ユーザーをグループに割り当てることはオプションです。必要に応じて、グループを作成または編集するときにユーザーを選択することもできます。

どのグループにも属していないユーザーには管理権限がありません。権限は累積されます。ユーザーは、所属するすべてのグループに対するすべての権限を持ちます。見る"テナント管理権限" 。

2. *ユーザーの作成*を選択します。

テナント アカウントに グリッド フェデレーション接続の使用 権限があり、テナントのソース グリッド上にいる場合、新しいローカル ユーザーはテナントの宛先グリッドに複製されます。ユーザーの詳細ページの概要セクションの 複製ステータス に 成功 が表示されます。

3. *完了*を選択してユーザー ページに戻ります。

ローカルユーザーの表示または編集

手順

1. アクセス管理 > *ユーザー*を選択します。
2. [ユーザー] ページに提供される情報を確認します。このページには、このテナント アカウントのすべてのローカル ユーザーとフェデレーション ユーザーの基本情報が一覧表示されます。

テナント アカウントに グリッド フェデレーション接続の使用 権限があり、テナントのソース グリッドでユーザーを表示している場合:

- バナー メッセージには、ユーザーを編集または削除した場合、その変更は他のグリッドに同期されないことが示されます。
- 必要に応じて、ユーザーが宛先グリッドのテナントに複製されなかったかどうかを示すバナー メッセージが表示されます。あなたは 失敗したユーザークローンを再試行する。

3. ユーザーのフルネームを変更する場合:
   a. ユーザーのチェックボックスを選択します。
   b. アクション > *フルネームの編集*を選択します。
   c. 新しい名前を入力してください。
   d. *変更を保存*を選択します。
4. 詳細を表示したり、追加の編集を行ったりする場合は、次のいずれかを実行します。
   - ユーザー名を選択します。
   - ユーザーのチェックボックスを選択し、[アクション] > [ユーザーの詳細を表示] を選択します。
5. 各ユーザーに関する次の情報が表示される概要セクションを確認します。
   - フルネーム
   - ユーザー名
   - ユーザータイプ
   - アクセス拒否
   - アクセス モード
   - グループ メンバーシップ

- テナント アカウントに グリッド フェデレーション接続の使用 権限があり、テナントのソース グリッドでユーザーを表示している場合の追加フィールド:
  - クローン作成ステータス（成功*または*失敗）
  - このユーザーを編集しても、変更内容は他のグリッドに同期されないことを示す青いバナー。

6. 必要に応じてユーザー設定を編集します。見るローカルユーザーを作成する入力内容の詳細については、こちらをご覧ください。
   a. 概要セクションで、名前または編集アイコンを選択してフルネームを変更します。 。

      ユーザー名を変更することはできません。

   b. *パスワード*タブでユーザーのパスワードを変更し、*変更を保存*を選択します。
   c. [アクセス] タブで、ユーザーのサインインを許可する場合は [いいえ] を選択し、サインインを禁止する場合は [はい] を選択します。次に、[変更を保存] を選択します。
   d. *アクセスキー*タブで*キーの作成*を選択し、指示に従ってください。"別のユーザーのS3アクセスキーを作成する" 。
   e. グループ タブで、グループの編集 を選択して、ユーザーをグループに追加したり、グループからユーザーを削除したりします。次に、「変更を保存」を選択します。
7. 変更したセクションごとに*変更を保存*を選択したことを確認します。

重複したローカルユーザー

ローカル ユーザーを複製して、新しいユーザーをより迅速に作成できます。

> テナント アカウントに グリッド フェデレーション接続の使用 権限があり、テナントのソース グリッドからユーザーを複製する場合、複製されたユーザーはテナントの宛先グリッドに複製されます。

手順

1. アクセス管理 > *ユーザー*を選択します。
2. 複製するユーザーのチェックボックスを選択します。
3. アクション > *重複ユーザー*を選択します。
4. 見るローカルユーザーを作成する入力内容の詳細については、こちらをご覧ください。
5. *ユーザーの作成*を選択します。

ユーザーのクローンを再試行する

失敗したクローンを再試行するには:

1. ユーザー名の下に「(複製失敗)」と表示されている各ユーザーを選択します。
2. アクション > *ユーザーの複製*を選択します。
3. 複製する各ユーザーの詳細ページから複製操作のステータスを表示します。

詳細については、"テナントグループとユーザーの複製"を参照してください。

1人以上のローカルユーザーを削除する

StorageGRIDテナント アカウントにアクセスする必要がなくなった 1 人以上のローカル ユーザーを完全に削除できます。

> テナント アカウントに グリッド フェデレーション接続の使用 権限があり、ローカル ユーザーを削除した場合、 StorageGRID は他のグリッド上の対応するユーザーを削除しません。この情報を同期させておく必要がある場合は、両方のグリッドから同じユーザーを削除する必要があります。

> フェデレーション ユーザーを削除するには、フェデレーション ID ソースを使用する必要があります。

手順

1. アクセス管理 > *ユーザー*を選択します。
2. 削除する各ユーザーのチェックボックスを選択します。
3. アクション > ユーザーの削除 または アクション > ユーザーの削除 を選択します。

   確認ダイアログボックスが表示されます。
4. *ユーザーの削除*または*ユーザーの削除*を選択します。

S3 アクセスキーを管理する

S3 アクセスキーを管理する

S3 テナント アカウントの各ユーザーは、 StorageGRIDシステムにオブジェクトを保存および取得するためのアクセス キーを持っている必要があります。アクセス キーは、アクセス キー ID とシークレット アクセス キーで構成されます。

S3 アクセスキーは次のように管理できます。

- 独自の **S3** 認証情報の管理 権限を持つユーザーは、独自の S3 アクセス キーを作成または削除できます。
- *ルートアクセス*権限を持つユーザーは、S3 ルートアカウントと他のすべてのユーザーのアクセスキーを管理できます。ルート アクセス キーは、バケット ポリシーによって明示的に無効にされていない限り、テナントのすべてのバケットとオブジェクトへのフル アクセスを提供します。

StorageGRID は、署名バージョン 2 および署名バージョン 4 の認証をサポートしています。バケット ポリシーによって明示的に有効にされていない限り、アカウント間のアクセスは許可されません。

独自の**S3**アクセスキーを作成する

S3 テナントを使用しており、適切な権限がある場合は、独自の S3 アクセス キーを作成できます。バケットとオブジェクトにアクセスするには、アクセス キーが必要です。

開始する前に

- テナントマネージャーにサインインするには、"サポートされているウェブブラウザ" 。

- あなたは、"独自のS3認証情報またはルートアクセス権限を管理する" 。

タスク概要

テナント アカウントのバケットを作成および管理できるようにする 1 つ以上の S3 アクセス キーを作成できます。新しいアクセス キーを作成したら、新しいアクセス キー ID とシークレット アクセス キーを使用してアプリケーションを更新します。セキュリティのため、必要以上のキーを作成しないでください。また、使用していないキーは削除してください。キーが 1 つしかなく、そのキーの有効期限が近づいている場合は、古いキーの有効期限が切れる前に新しいキーを作成し、古いキーを削除します。

各キーには、特定の有効期限を設定することも、有効期限を設定しないこともできます。有効期限については次のガイドラインに従ってください。

- キーの有効期限を設定して、アクセスを特定の期間に制限します。有効期限を短く設定すると、アクセス キー ID とシークレット アクセス キーが誤って公開された場合のリスクを軽減できます。期限切れのキーは自動的に削除されます。
- 環境内のセキュリティ リスクが低く、定期的に新しいキーを作成する必要がない場合は、キーの有効期限を設定する必要はありません。後で新しいキーを作成する場合は、古いキーを手動で削除します。

> アカウントに属する S3 バケットとオブジェクトには、テナント マネージャーでアカウントに対して表示されるアクセス キー ID とシークレット アクセス キーを使用してアクセスできます。このため、アクセス キーはパスワードと同じように保護してください。アクセス キーを定期的にローテーションし、使用していないキーはアカウントから削除し、他のユーザーと共有しないでください。

手順

1. ストレージ **(S3)** > マイアクセスキー を選択します。

   「マイ アクセス キー」ページが表示され、既存のアクセス キーが一覧表示されます。

2. *キーの作成*を選択します。
3. 次のいずれかを実行します。
   - 有効期限のないキーを作成するには、「有効期限を設定しない」を選択します。（デフォルト）
   - *有効期限を設定する*を選択し、有効期限の日時を設定します。

     > 有効期限は現在の日付から最大 5 年までとなります。有効期限は、現在の時刻から最低 1 分後に設定できます。

4. *アクセスキーの作成*を選択します。

   「アクセス キーのダウンロード」ダイアログ ボックスが表示され、アクセス キー ID とシークレット アクセス キーが一覧表示されます。

5. アクセス キー ID とシークレット アクセス キーを安全な場所にコピーするか、**.csv** をダウンロード を選択して、アクセス キー ID とシークレット アクセス キーを含むスプレッドシート ファイルを保存します。

   > この情報をコピーまたはダウンロードするまで、このダイアログ ボックスを閉じないでください。ダイアログ ボックスを閉じた後は、キーをコピーまたはダウンロードすることはできません。

6. *完了*を選択します。

   新しいキーは「マイアクセスキー」ページに表示されます。

7. テナント アカウントに グリッド フェデレーション接続の使用 権限がある場合は、オプションでテナント管理 API を使用して、ソース グリッドのテナントから宛先グリッドのテナントに S3 アクセス キーを手動で複製します。見る"API を使用して S3 アクセスキーを複製する" 。

S3 アクセスキーを表示する

S3テナントを使用しており、"適切な許可" 、S3 アクセスキーのリストを表示できます。リストを有効期限で並べ替えることができるため、どのキーがもうすぐ期限切れになるかを判断できます。必要に応じて、"新しいキーを作成する"または"削除キー"もう使用していないもの。

> アカウントに属する S3 バケットとオブジェクトには、テナント マネージャーでアカウントに対して表示されるアクセス キー ID とシークレット アクセス キーを使用してアクセスできます。このため、アクセス キーはパスワードと同じように保護してください。アクセス キーを定期的にローテーションし、使用していないキーはアカウントから削除し、他のユーザーと共有しないでください。

開始する前に

- テナントマネージャーにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは、独自のS3認証情報を管理する権限を持つユーザーグループに属しています"アクセス権"。

手順

1. ストレージ **(S3)** > マイアクセスキー を選択します。
2. 「マイ アクセス キー」ページで、既存のアクセス キーを 有効期限 または アクセス キー **ID** で並べ替えます。
3. 必要に応じて、新しいキーを作成するか、使用しなくなったキーを削除します。

   既存のキーの有効期限が切れる前に新しいキーを作成すると、アカウント内のオブジェクトへのアクセスを一時的に失うことなく、新しいキーの使用を開始できます。

   期限切れのキーは自動的に削除されます。

独自のS3アクセスキーを削除する

S3 テナントを使用しており、適切な権限がある場合は、独自の S3 アクセスキーを削除できます。アクセス キーを削除すると、そのアクセス キーを使用してテナント アカウント内のオブジェクトやバケットにアクセスできなくなります。

開始する前に

- テナントマネージャーにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは"独自のS3認証情報を管理する権限"。

アカウントに属する S3 バケットとオブジェクトには、テナント マネージャーでアカウントに対して表示されるアクセス キー ID とシークレット アクセス キーを使用してアクセスできます。このため、アクセス キーはパスワードと同じように保護してください。アクセス キーを定期的にローテーションし、使用していないキーはアカウントから削除し、他のユーザーと共有しないでください。

手順

1. ストレージ **(S3)** > マイアクセスキー を選択します。
2. 「マイ アクセス キー」ページで、削除する各アクセス キーのチェックボックスをオンにします。
3. *Deleteキー*を選択します。
4. 確認ダイアログボックスから*キーの削除*を選択します。

   ページの右上に確認メッセージが表示されます。

別のユーザーの**S3**アクセスキーを作成する

S3 テナントを使用しており、適切な権限がある場合は、バケットやオブジェクトへのアクセスが必要なアプリケーションなど、他のユーザーの S3 アクセスキーを作成できます。

開始する前に

- テナントマネージャーにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは、"ルートアクセス権限" 。

タスク概要

他のユーザーが自分のテナント アカウントのバケットを作成および管理できるように、1 つ以上の S3 アクセス キーを作成できます。新しいアクセス キーを作成したら、新しいアクセス キー ID とシークレット アクセス キーを使用してアプリケーションを更新します。セキュリティのため、ユーザーが必要とする以上のキーを作成しないでください。また、使用されていないキーは削除してください。キーが 1 つしかなく、そのキーの有効期限が近づいている場合は、古いキーの有効期限が切れる前に新しいキーを作成し、古いキーを削除します。

各キーには、特定の有効期限を設定することも、有効期限を設定しないこともできます。有効期限については次のガイドラインに従ってください。

- キーの有効期限を設定して、ユーザーのアクセスを特定の期間に制限します。有効期限を短く設定すると、アクセス キー ID とシークレット アクセス キーが誤って公開された場合のリスクを軽減できます。期限切れのキーは自動的に削除されます。
- 環境内のセキュリティ リスクが低く、定期的に新しいキーを作成する必要がない場合は、キーの有効期限を設定する必要はありません。後で新しいキーを作成する場合は、古いキーを手動で削除します。

ユーザーに属する S3 バケットとオブジェクトには、テナント マネージャーでそのユーザーに対して表示されるアクセス キー ID とシークレット アクセス キーを使用してアクセスできます。このため、アクセス キーはパスワードと同じように保護してください。アクセス キーを定期的にローテーションし、使用されていないキーはアカウントから削除し、他のユーザーと共有しないでください。

手順

1. アクセス管理 > *ユーザー*を選択します。
2. S3 アクセスキーを管理するユーザーを選択します。

   ユーザーの詳細ページが表示されます。

3. アクセス キー を選択し、キーの作成 を選択します。
4. 次のいずれかを実行します。
   - 有効期限のないキーを作成するには、「有効期限を設定しない」を選択します。（デフォルト）
   - *有効期限を設定する*を選択し、有効期限の日時を設定します。

   > 有効期限は現在の日付から最大 5 年までとなります。有効期限は、現在の時刻から最低 1 分後に設定できます。

5. *アクセスキーの作成*を選択します。

   「アクセス キーのダウンロード」ダイアログ ボックスが表示され、アクセス キー ID とシークレット アクセス キーが一覧表示されます。

6. アクセス キー ID とシークレット アクセス キーを安全な場所にコピーするか、**.csv** をダウンロード を選択して、アクセス キー ID とシークレット アクセス キーを含むスプレッドシート ファイルを保存します。

   > この情報をコピーまたはダウンロードするまで、このダイアログ ボックスを閉じないでください。ダイアログ ボックスを閉じた後は、キーをコピーまたはダウンロードすることはできません。

7. *完了*を選択します。

   新しいキーは、ユーザー詳細ページの [アクセス キー] タブに表示されます。

8. テナント アカウントに グリッド フェデレーション接続の使用 権限がある場合は、オプションでテナント管理 API を使用して、ソース グリッドのテナントから宛先グリッドのテナントに S3 アクセス キーを手動で複製します。見る"API を使用して S3 アクセスキーを複製する" 。

他のユーザーの **S3** アクセスキーを表示する

S3 テナントを使用しており、適切な権限を持っている場合は、他のユーザーの S3 アクセス キーを表示できます。リストを有効期限で並べ替えることができるので、どのキーがもうすぐ期限切れになるかを判断できます。必要に応じて、新しいキーを作成したり、使用されなくなったキーを削除したりできます。

開始する前に

- テナントマネージャーにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは"ルートアクセス権限"。

ユーザーに属する S3 バケットとオブジェクトには、テナント マネージャーでそのユーザーに対して表示されるアクセス キー ID とシークレット アクセス キーを使用してアクセスできます。このため、アクセス キーはパスワードと同じように保護してください。アクセス キーを定期的にローテーションし、使用されていないキーはアカウントから削除し、他のユーザーと共有しないでください。

手順

1. アクセス管理 > *ユーザー*を選択します。
2. 「ユーザー」ページで、S3 アクセスキーを表示するユーザーを選択します。
3. ユーザー詳細ページで、*アクセス キー*を選択します。
4. キーを*有効期限*または*アクセス キー ID*で並べ替えます。
5. 必要に応じて、新しいキーを作成し、使用されなくなったキーを手動で削除します。

   既存のキーの有効期限が切れる前に新しいキーを作成すると、ユーザーはアカウント内のオブジェクトへのアクセスを一時的に失うことなく、新しいキーの使用を開始できます。

   期限切れのキーは自動的に削除されます。

関連情報

- "別のユーザーのS3アクセスキーを作成する"
- "他のユーザーのS3アクセスキーを削除する"

他のユーザーの**S3**アクセスキーを削除する

S3 テナントを使用しており、適切な権限がある場合は、別のユーザーの S3 アクセスキーを削除できます。アクセス キーを削除すると、そのアクセス キーを使用してテナント アカウント内のオブジェクトやバケットにアクセスできなくなります。

開始する前に

- テナントマネージャーにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは"ルートアクセス権限"。

ユーザーに属する S3 バケットとオブジェクトには、テナント マネージャーでそのユーザーに対して表示されるアクセス キー ID とシークレット アクセス キーを使用してアクセスできます。このため、アクセス キーはパスワードと同じように保護してください。アクセス キーを定期的にローテーションし、使用されていないキーはアカウントから削除し、他のユーザーと共有しないでください。

手順

1. アクセス管理 > *ユーザー*を選択します。
2. 「ユーザー」ページで、S3 アクセスキーを管理するユーザーを選択します。
3. [ユーザーの詳細] ページで [アクセス キー] を選択し、削除する各アクセス キーのチェックボックスをオンにします。
4. アクション > *選択したキーを削除*を選択します。

5. 確認ダイアログボックスから*キーの削除*を選択します。

   ページの右上に確認メッセージが表示されます。

S3バケットを管理する

S3バケットを作成する

テナント マネージャーを使用して、オブジェクト データ用の S3 バケットを作成できます。

開始する前に

- テナントマネージャーにサインインするには、"サポートされているウェブブラウザ" 。
- ルートアクセスまたはすべてのバケットの管理権限を持つユーザーグループに属している"アクセス権"。これらの権限は、グループまたはバケット ポリシーの権限設定をオーバーライドします。

  バケットまたはオブジェクトのS3オブジェクトロックプロパティを設定または変更する権限は、"バケットポリシーまたはグループポリシー" 。

- バケットに対して S3 オブジェクト ロックを有効にする予定の場合は、グリッド管理者がStorageGRIDシステムのグローバル S3 オブジェクト ロック設定を有効にし、S3 オブジェクト ロック バケットとオブジェクトの要件を確認しておきます。
- 各テナントに 5,000 個のバケットがある場合、グリッド内の各ストレージ ノードには最低 64 GB の RAM があります。

  各グリッドには最大 100,000 個のバケットを含めることができます。

ウィザードにアクセスする

手順

1. ダッシュボードから*バケットの表示*を選択するか、ストレージ **(S3)** > *バケット*を選択します。
2. *バケットを作成*を選択します。

詳細を入力してください

手順

1. バケットの詳細を入力します。

フィールド	説明
バケット名	次のルールに準拠するバケットの名前: • 各StorageGRIDシステム全体で一意である必要があります (テナント アカウント内で一意なだけでなく)。 • DNS に準拠している必要があります。 • 3 文字以上 63 文字以下でなければなりません。 • 各ラベルは小文字または数字で始まり、終わる必要があり、小文字、数字、ハイフンのみを使用できます。 • 仮想ホスト形式のリクエストにはピリオドを含めることはできません。ピリオドを使用すると、サーバーのワイルドカード証明書の検証で問題が発生します。 詳細については、 "バケット命名ルールに関する Amazon Web Services (AWS) ドキュメント" 。 注意: バケットを作成した後は、バケット名を変更することはできません。
リージョン	バケットのリージョン。 利用可能なリージョンはStorageGRID管理者が管理します。バケットのリージョンは、オブジェクトに適用されるデータ保護ポリシーに影響を与える可能性があります。デフォルトでは、すべてのバケットは `us-east-1`地域。 注意: バケットを作成した後はリージョンを変更できません。

2. *続行*を選択します。

設定の管理

手順

1. 必要に応じて、バケットのオブジェクトのバージョン管理を有効にします。

   このバケット内の各オブジェクトのすべてのバージョンを保存する場合は、オブジェクトのバージョン管理を有効にします。必要に応じて、オブジェクトの以前のバージョンを取得できます。バケットをクロスグリッド レプリケーションに使用する場合は、オブジェクトのバージョン管理を有効にする必要があります。

2. グローバル S3 オブジェクトロック設定が有効になっている場合は、オプションでバケットの S3 オブジェクトロックを有効にして、Write Once Read Many (WORM) モデルを使用してオブジェクトを保存します。

   特定の規制要件を満たすためなど、オブジェクトを一定期間保持する必要がある場合にのみ、バケットに対して S3 オブジェクトロックを有効にします。S3 オブジェクト ロックは、一定期間または無期限にオブジェクトが削除または上書きされるのを防ぐのに役立つ永続的な設定です。

バケットに対して S3 オブジェクトロック設定を有効にすると、無効にすることはできません。適切な権限を持つユーザーは誰でも、変更できないオブジェクトをこのバケットに追加できます。これらのオブジェクトまたはバケット自体を削除できない可能性があります。

バケットに対して S3 オブジェクトロックを有効にすると、バケットのバージョン管理が自動的に有効になります。

3. *S3 オブジェクトロックを有効にする*を選択した場合は、オプションでこのバケットの*デフォルトの保持期間*を有効にします。

グリッド管理者は、次の権限を与える必要があります。"S3 オブジェクトロックの特定の機能を使用する" 。

デフォルトの保持期間 が有効になっている場合、バケットに追加された新しいオブジェクトは、削除または上書きされないように自動的に保護されます。*デフォルトの保持期間*設定は、独自の保持期間を持つオブジェクトには適用されません。

a. *デフォルトの保持*が有効になっている場合は、バケットの*デフォルトの保持モード*を指定します。

デフォルトの保持モード	説明
ガバナンス	• ユーザーは `s3:BypassGovernanceRetention`許可は `x-amz-bypass-governance-retention: true`保持設定をバイパスするためのリクエスト ヘッダー。 • これらのユーザーは、オブジェクト バージョンを、その保持期限に達する前に削除できます。 • これらのユーザーは、オブジェクトの保持期限を増減または削除できます。
コンプライアンス	• オブジェクトは、保持期限に達するまで削除できません。 • オブジェクトの保持期限を増やすことはできますが、減らすことはできません。 • オブジェクトの保持期限は、その日付に達するまで削除できません。 注意: グリッド管理者がコンプライアンス モードの使用を許可する必要があります。

b. *デフォルトの保持*が有効になっている場合は、バケットの*デフォルトの保持期間*を指定します。

デフォルトの保持期間 は、このバケットに追加された新しいオブジェクトが取り込まれた時点から保持される期間を示します。グリッド管理者によって設定されたテナントの最大保持期間以下の値を指定します。

グリッド管理者がテナントを作成するときに、1 日から 100 年までの値に設定できる最大保持期間が設定されます。 _デフォルト_の保持期間を設定する場合、最大保持期間に設定された値を超えることはできません。必要に応じて、グリッド管理者に最大保存期間の増減を依頼してください。

4. オプションで、「容量制限を有効にする」を選択します。

   容量制限は、このバケットのオブジェクトに使用できる最大容量です。この値は物理的な量 (ディスク上のサイズ) ではなく、論理的な量 (オブジェクトのサイズ) を表します。

   制限が設定されていない場合、このバケットの容量は無制限になります。参照"容量制限の使用"詳細についてはこちらをご覧ください。

5. *バケットを作成*を選択します。

   バケットが作成され、「バケット」ページのテーブルに追加されます。

6. オプションで*バケットの詳細ページに移動*を選択して"バケットの詳細を表示"追加の構成を実行します。

バケットの詳細を表示

テナント アカウントでバケットを表示できます。

開始する前に

- テナントマネージャーにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは、"ルートアクセス、すべてのバケットの管理、またはすべてのバケットの表示権限" 。これらの権限は、グループまたはバケット ポリシーの権限設定をオーバーライドします。

手順

1. ダッシュボードから*バケットの表示*を選択するか、ストレージ **(S3)** > *バケット*を選択します。

   バケット ページが表示されます。

2. 各バケットの概要表を確認します。

   必要に応じて、任意の列で情報を並べ替えたり、リスト内を前後に移動したりできます。

   > ⓘ 表示されるオブジェクト数、使用領域、使用量の値は推定値です。これらの見積りは、取り込みのタイミング、ネットワーク接続、およびノードの状態によって影響を受けます。バケットでバージョン管理が有効になっている場合、削除されたオブジェクトのバージョンもオブジェクト数に含まれます。

   Name
   バケットの一意の名前。変更できません。

   有効な機能
   バケットに対して有効になっている機能のリスト。

   S3 オブジェクトロック
   バケットに対して S3 オブジェクト ロックが有効になっているかどうか。

   この列は、グリッドで S3 オブジェクト ロックが有効になっている場合にのみ表示されます。この列には、従来の準拠バケットの情報も表示されます。

リージョン

バケットのリージョン。変更できません。この列はデフォルトでは非表示になっています。

オブジェクト数

このバケット内のオブジェクトの数。バケットでバージョン管理が有効になっている場合、この値には現在のオブジェクト以外のバージョンが含まれます。

オブジェクトが追加または削除されても、この値はすぐに更新されない場合があります。

使用スペース

バケット内のすべてのオブジェクトの論理サイズ。論理サイズには、複製されたコピーや消去コード化されたコピー、あるいはオブジェクト メタデータに必要な実際のスペースは含まれません。

この値の更新には最大 10 分かかる場合があります。

使用法

バケットの容量制限の使用率（設定されている場合）。

使用量の値は内部推定に基づいており、場合によっては超過する可能性があります。たとえば、StorageGRID は、テナントがオブジェクトのアップロードを開始すると容量制限 (設定されている場合) をチェックし、テナントが容量制限を超えている場合はこのバケットへの新しい取り込みを拒否します。ただし、 StorageGRID は、容量制限を超え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を考慮しません。オブジェクトが削除されると、容量制限の使用量が再計算されるまで、テナントはこのバケットに新しいオブジェクトをアップロードできなくなる場合があります。計算には10分以上かかる場合があります。

この値は、オブジェクトとそのメタデータを格納するために必要な物理サイズではなく、論理サイズを示します。

容量

設定されている場合、バケットの容量制限。

作成日

バケットが作成された日時。この列はデフォルトでは非表示になっています。

3. 特定のバケットの詳細を表示するには、テーブルからバケット名を選択します。
   a. Web ページの上部にある概要情報を表示して、リージョンやオブジェクト数などのバケットの詳細を確認します。
   b. 容量制限の使用状況バーを表示します。使用率が 100% または 100% に近い場合は、制限を増やすか、一部のオブジェクトを削除することを検討してください。
   c. 必要に応じて、「バケット内のオブジェクトの削除」と「バケットの削除」を選択します。

これらの各オプションを選択したときに表示される注意事項に十分注意してください。詳細については、以下を参照してください。

- "バケット内のすべてのオブジェクトを削除する"
- "バケットを削除する"(バケットは空である必要があります)

d. 必要に応じて、各タブでバケットの設定を表示または変更します。

- **S3** コンソール: バケットのオブジェクトを表示します。詳細については、 "S3コンソールを使用する" 。
- バケット オプション: オプション設定を表示または変更します。 S3 オブジェクトロックなどの一部の設定は、バケットの作成後は変更できません。
  - "バケットの一貫性を管理する"
  - "最終アクセス時間の更新"
  - "容量制限"
  - "オブジェクトのバージョン管理"
  - "S3 オブジェクトロック"
  - "デフォルトのバケット保持"
  - "クロスグリッドレプリケーションを管理する"（入居者に許可されている場合）
- プラットフォームサービス:"プラットフォームサービスの管理" （入居者に許可されている場合）
- バケット アクセス: オプション設定を表示または変更します。特定のアクセス権限が必要です。
  - 設定"クロスオリジンリソース共有（CORS）"そのため、バケットとバケット内のオブジェクトは他のドメインの Web アプリケーションからアクセスできるようになります。
  - "ユーザーアクセスを制御する"S3 バケットとそのバケット内のオブジェクト。

バケットにILMポリシータグを適用する

オブジェクト ストレージの要件に基づいて、バケットに適用する ILM ポリシー タグを選択します。

ILM ポリシーは、オブジェクト データが保存される場所と、一定期間後に削除されるかどうかを制御します。グリッド管理者は ILM ポリシーを作成し、複数のアクティブ ポリシーを使用する場合は ILM ポリシー タグに割り当てます。

> バケットのポリシータグを頻繁に再割り当てすることは避けてください。そうしないと、パフォーマンスの問題が発生する可能性があります。

開始する前に

- テナントマネージャーにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは、"ルートアクセス、すべてのバケットの管理、またはすべてのバケットの表示権限" 。これらの権限は、グループまたはバケット ポリシーの権限設定をオーバーライドします。

手順

1. ダッシュボードから*バケットの表示*を選択するか、ストレージ **(S3)** > *バケット*を選択します。

   バケット ページが表示されます。必要に応じて、任意の列で情報を並べ替えたり、リスト内を前後に移動したりできます。

2. ILM ポリシー タグを割り当てるバケットの名前を選択します。

すでにタグが割り当てられているバケットの ILM ポリシー タグの割り当てを変更することもできます。

> 表示されるオブジェクト数と使用済みスペースの値は推定値です。これらの見積りは、取り込みのタイミング、ネットワーク接続、およびノードの状態によって影響を受けます。バケットでバージョン管理が有効になっている場合、削除されたオブジェクトのバージョンもオブジェクト数に含まれます。

3. バケット オプション タブで、ILM ポリシー タグ アコーディオンを展開します。このアコーディオンは、グリッド管理者がカスタム ポリシー タグの使用を有効にしている場合にのみ表示されます。
4. 各ポリシータグの説明を読んで、バケットに適用するタグを決定します。

> バケットの ILM ポリシー タグを変更すると、バケット内のすべてのオブジェクトの ILM 再評価がトリガーされます。新しいポリシーでオブジェクトを一定期間保持する場合、古いオブジェクトは削除されます。

5. バケットに割り当てるタグのラジオボタンを選択します。
6. *変更を保存*を選択します。キーを持つバケットに新しいS3バケットタグが設定されます `NTAP-SG-ILM-BUCKET-TAG`ILM ポリシー タグ名の値。

> S3 アプリケーションが誤って新しいバケット タグを上書きまたは削除しないようにします。新しいタグセットをバケットに適用するときにこのタグを省略すると、バケット内のオブジェクトはデフォルトの ILM ポリシーに基づいて評価される状態に戻ります。

> ILM ポリシー タグが検証される Tenant Manager または Tenant Manager API のみを使用して、ILM ポリシー タグを設定および変更します。変更しないでください `NTAP-SG-ILM-BUCKET-TAG`S3 PutBucketTagging API または S3 DeleteBucketTagging API を使用した ILM ポリシータグ。

> バケットに割り当てられたポリシー タグを変更すると、新しい ILM ポリシーを使用してオブジェクトが再評価されている間、一時的にパフォーマンスに影響が出ます。

バケットポリシーを管理する

S3 バケットとそのバケット内のオブジェクトに対するユーザー アクセスを制御できます。

開始する前に

- テナントマネージャーにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは、"ルートアクセス権限" 。 「すべてのバケットを表示」および「すべてのバケットを管理」権限では、表示のみが許可されます。
- 必要な数のストレージ ノードとサイトが利用可能であることを確認しました。どのサイトでも 2 つ以上のストレージ ノードが利用できない場合、またはサイトが利用できない場合は、これらの設定を変更できない可能性があります。

手順

1. *バケット*を選択し、管理するバケットを選択します。

2. バケットの詳細ページで、バケット アクセス > バケット ポリシー を選択します。
3. 次のいずれかを実行します。
   - *ポリシーを有効にする*チェックボックスを選択してバケットポリシーを入力します。次に、有効な JSON 形式の文字列を入力します。

     各バケット ポリシーのサイズ制限は 20,480 バイトです。
   - 文字列を編集して既存のポリシーを変更します。
   - *ポリシーを有効にする*の選択を解除してポリシーを無効にします。

言語構文や例を含むバケットポリシーの詳細については、以下を参照してください。"バケットポリシーの例"
。

バケットの一貫性を管理する

一貫性値を使用すると、バケット設定の変更の可用性を指定できるほか、バケット内のオブジェクトの可用性と、異なるストレージ ノードおよびサイト間でのオブジェクトの一貫性のバランスをとることもできます。クライアント アプリケーションが運用上のニーズを満たすことができるように、一貫性の値を既定値とは異なる値に変更できます。

開始する前に

- テナントマネージャーにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは、"すべてのバケットまたはルートアクセス権限を管理する" 。これらの権限は、グループまたはバケット ポリシーの権限設定をオーバーライドします。

バケットの一貫性ガイドライン

バケットの一貫性は、その S3 バケット内のオブジェクトに影響を与えるクライアント アプリケーションの一貫性を決定するために使用されます。一般に、バケットには 新規書き込み後の読み取り の一貫性を使用する必要があります。

バケットの一貫性を変更する

Read-after-new-write の整合性がクライアントアプリケーションの要件を満たしていない場合は、バケットの整合性を設定するか、 `Consistency-Control`ヘッダ。その `Consistency-Control`ヘッダーはバケットの一貫性を上書きします。

> バケットの一貫性を変更すると、変更後に取り込まれたオブジェクトのみが、修正された設定を満たすことが保証されます。

手順

1. ダッシュボードから*バケットの表示*を選択するか、ストレージ **(S3)** > *バケット*を選択します。
2. テーブルからバケット名を選択します。

   バケットの詳細ページが表示されます。
3. バケット オプション タブから、** アコーディオンを選択します。

4. このバケット内のオブジェクトに対して実行される操作の一貫性を選択します。
    - すべて: 最高レベルの一貫性を提供します。すべてのノードがデータを直ちに受信します。そうでない場合、要求は失敗します。
    - 強力なグローバル: すべてのサイトにわたるすべてのクライアント要求の書き込み後の読み取り一貫性を保証します。
    - 強力なサイト: サイト内のすべてのクライアント要求に対して、書き込み後の読み取りの一貫性を保証します。
    - 新規書き込み後の読み取り (デフォルト): 新しいオブジェクトに対して書き込み後の読み取りの一貫性を提供し、オブジェクトの更新に対して最終的な一貫性を提供します。高可用性とデータ保護の保証を提供します。ほとんどの場合に推奨されます。
    - 利用可能: 新しいオブジェクトとオブジェクトの更新の両方に対して最終的な一貫性を提供します。S3 バケットの場合は、必要な場合にのみ使用してください (たとえば、めったに読み取られないログ値を含むバケットの場合や、存在しないキーに対する HEAD または GET 操作の場合など)。 S3 FabricPoolバケットではサポートされていません。
5. *変更を保存*を選択します。

バケット設定を変更すると何が起こるか

バケットには、バケットとバケット内のオブジェクトの動作に影響する複数の設定があります。

次のバケット設定では、デフォルトで 強力な 一貫性が使用されます。どのサイトでも 2 つ以上のストレージノードが利用できない場合、またはサイトが利用できない場合は、これらの設定に対する変更が利用できない可能性があります。

- "バックグラウンドで空のバケットを削除"
- "最終アクセス時間"
- "バケットのライフサイクル"
- "バケットポリシー"
- "バケットのタグ付け"
- "バケットのバージョン管理"
- "S3 オブジェクトロック"
- "バケット暗号化"

> バケットのバージョン管理、S3 オブジェクト ロック、およびバケットの暗号化の一貫性値は、強力に一貫性のない値に設定することはできません。

次のバケット設定では強力な一貫性が使用されず、変更の可用性が高くなります。これらの設定の変更が反映されるまでには、しばらく時間がかかる場合があります。

- "プラットフォーム サービスの構成: 通知、レプリケーション、または検索の統合"
- "CORS設定"
- バケットの一貫性を変更する

バケット設定を変更する際に使用されるデフォルトの一貫性がクライアントアプリケーションの要件を満たしていない場合は、 `Consistency-Control`ヘッダー"S3 REST API"または、 `reducedConsistency`または `force`オプション"テナント管理API"。

最終アクセス時間の更新を有効または無効にする

グリッド管理者は、 StorageGRIDシステムの情報ライフサイクル管理 (ILM) ルールを作成するときに、オブジェクトの最終アクセス時刻を使用して、そのオブジェクトを別のストレージの場所に移動するかどうかを判断するようにオプションで指定できます。 S3 テナントを使用している場合は、S3 バケット内のオブジェクトの最終アクセス時刻の更新を有効にすることで、このようなルールを利用できます。

これらの手順は、最終アクセス時刻 オプションを詳細フィルターまたは参照時刻として使用する ILM ルールが少なくとも 1 つ含まれるStorageGRIDシステムにのみ適用されます。 StorageGRIDシステムにそのようなルールが含まれていない場合は、これらの手順を無視できます。見る"ILMルールで最終アクセス時刻を使用する"詳細については。

開始する前に

- テナントマネージャーにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは、"すべてのバケットまたはルートアクセス権限を管理する" 。これらの権限は、グループまたはバケット ポリシーの権限設定をオーバーライドします。

タスク概要

最終アクセス時間 は、ILM ルールの 参照時間 配置指示に使用できるオプションの 1 つです。ルールの参照時間を最終アクセス時間に設定すると、グリッド管理者は、オブジェクトが最後に取得 (読み取りまたは表示) された時間に基づいて、オブジェクトが特定のストレージの場所に配置されるように指定できます。

たとえば、最近表示したオブジェクトがより高速なストレージに残るようにするために、グリッド管理者は以下を指定する ILM ルールを作成できます。

- 過去 1 か月間に取得されたオブジェクトは、ローカル ストレージ ノードに残ります。
- 過去 1 か月間に回収されていないオブジェクトは、オフサイトの場所に移動する必要があります。

デフォルトでは、最終アクセス時刻の更新は無効になっています。 StorageGRIDシステムに 最終アクセス時刻 オプションを使用する ILM ルールが含まれており、このオプションをこのバケット内のオブジェクトに適用する場合は、そのルールで指定された S3 バケットの最終アクセス時刻の更新を有効にする必要があります。

オブジェクトが取得されたときに最終アクセス時間を更新すると、特に小さなオブジェクトの場合、 StorageGRID のパフォーマンスが低下する可能性があります。

StorageGRID はオブジェクトが取得されるたびに次の追加手順を実行する必要があるため、最終アクセス時刻の更新によってパフォーマンスに影響が生じます。

- 新しいタイムスタンプでオブジェクトを更新する
- オブジェクトをILMキューに追加して、現在のILMルールとポリシーに照らして再評価できるようにします。

この表は、最終アクセス時間が無効または有効になっている場合にバケット内のすべてのオブジェクトに適用

される動作をまとめたものです。

リクエストの種類	最終アクセス時刻が無効になっている場合の動作（デフォルト）		最終アクセス時刻が有効になっている場合の動作	
	最終アクセス時間は更新されましたか?	オブジェクトが ILM 評価キューに追加されましたか?	最終アクセス時間は更新されましたか?	オブジェクトが ILM 評価キューに追加されましたか?
オブジェクト、そのアクセス制御リスト、またはそのメタデータの取得要求	いいえ	いいえ	はい	はい
オブジェクトのメタデータの更新リクエスト	はい	はい	はい	はい
オブジェクトまたはオブジェクトのバージョンの一覧表示のリクエスト	いいえ	いいえ	いいえ	いいえ
あるバケットから別のバケットにオブジェクトをコピーするリクエスト	• いいえ、ソースコピーの場合 • はい、宛先コピー用	• いいえ、ソースコピーの場合 • はい、宛先コピー用	• はい、ソースコピーの場合 • はい、宛先コピー用	• はい、ソースコピーの場合 • はい、宛先コピー用
マルチパートアップロードの完了リクエスト	はい、組み立てられたオブジェクトの場合	はい、組み立てられたオブジェクトの場合	はい、組み立てられたオブジェクトの場合	はい、組み立てられたオブジェクトの場合

手順

1. ダッシュボードから*バケットの表示*を選択するか、ストレージ **(S3)** > *バケット*を選択します。
2. テーブルからバケット名を選択します。

   バケットの詳細ページが表示されます。

3. バケット オプション タブから、最終アクセス時間の更新 アコーディオンを選択します。
4. 最終アクセス時間の更新を有効または無効にします。
5. *変更を保存*を選択します。

バケットのオブジェクトのバージョン管理を変更する

S3 テナントを使用している場合は、S3 バケットのバージョン管理状態を変更できます。

開始する前に

- テナントマネージャーにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは、"すべてのバケットまたはルートアクセス権限を管理する" 。これらの権限は、グループまたはバケット ポリシーの権限設定をオーバーライドします。
- 必要な数のストレージ ノードとサイトが利用可能であることを確認しました。どのサイトでも 2 つ以上のストレージ ノードが利用できない場合、またはサイトが利用できない場合は、これらの設定を変更できない可能性があります。

タスク概要

バケットのオブジェクトのバージョン管理を有効化または一時停止できます。バケットのバージョン管理を有効にすると、バージョン管理されていない状態に戻すことはできません。ただし、バケットのバージョン管理を一時停止することはできます。

- 無効: バージョン管理が有効になったことはありません
- 有効: バージョン管理が有効です
- 一時停止: バージョン管理は以前は有効でしたが、一時停止されています

詳細については、次を参照してください。

- "オブジェクトのバージョン管理"
- "S3 バージョン管理オブジェクトの ILM ルールとポリシー (例 4)"
- "オブジェクトの削除方法"

手順

1. ダッシュボードから*バケットの表示*を選択するか、ストレージ **(S3)** > *バケット*を選択します。
2. テーブルからバケット名を選択します。

   バケットの詳細ページが表示されます。
3. バケット オプション タブから、オブジェクトのバージョン管理 アコーディオンを選択します。
4. このバケット内のオブジェクトのバージョン管理状態を選択します。

   クロスグリッド レプリケーションに使用されるバケットでは、オブジェクトのバージョン管理を有効にしておく必要があります。 S3 オブジェクト ロックまたはレガシー コンプライアンスが有効になっている場合、オブジェクトのバージョン管理 オプションは無効になります。

オプション	説明
バージョン管理を有効にする	このバケット内の各オブジェクトのすべてのバージョンを保存する場合は、オブジェクトのバージョン管理を有効にします。必要に応じて、オブジェクトの以前のバージョンを取得できます。 バケット内にすでに存在するオブジェクトは、ユーザーによって変更されるとバージョン管理されます。

オプション	説明
バージョン管理を一時停止	新しいオブジェクト バージョンを作成する必要がなくなった場合は、オブジェクトのバージョン管理を一時停止します。既存のオブジェクト バージョンを引き続き取得できます。

5. *変更を保存*を選択します。

S3 オブジェクトロックを使用してオブジェクトを保持する

バケットとオブジェクトが保持に関する規制要件に準拠する必要がある場合は、S3 オブジェクトロックを使用できます。

グリッド管理者は、S3 オブジェクト ロックの特定の機能を使用するための権限を付与する必要があります。

S3 オブジェクトロックとは何ですか?

StorageGRID S3 オブジェクト ロック機能は、Amazon Simple Storage Service (Amazon S3) の S3 オブジェクト ロックと同等のオブジェクト保護ソリューションです。

StorageGRIDシステムでグローバル S3 オブジェクト ロック設定が有効になっている場合、S3 テナント アカウントは、S3 オブジェクト ロックが有効になっているかどうかに関係なくバケットを作成できます。バケットで S3 オブジェクトロックが有効になっている場合は、バケットのバージョン管理が必要となり、自動的に有効になります。

S3 オブジェクト ロックのないバケット には、保持設定が指定されていないオブジェクトのみを含めることができます。取り込まれたオブジェクトには保持設定はありません。

S3 オブジェクト ロックが有効なバケット には、S3 クライアント アプリケーションによって指定された保持設定のあるオブジェクトと、保持設定のないオブジェクトを含めることができます。取り込まれたオブジェクトの中には保持設定を持つものがあります。

S3 オブジェクト ロックとデフォルトの保持期間が設定されたバケット には、保持期間設定が指定されたアップロード済みオブジェクトと、保持期間設定のない新しいオブジェクトを含めることができます。保持設定がオブジェクト レベルで構成されていないため、新しいオブジェクトではデフォルト設定が使用されます。

実際には、デフォルトの保持期間が設定されている場合、新しく取り込まれたすべてのオブジェクトに保持設定が行われます。オブジェクト保持設定のない既存のオブジェクトは影響を受けません。

保持モード

StorageGRID S3 オブジェクト ロック機能は、オブジェクトに異なるレベルの保護を適用するための 2 つの保持モードをサポートしています。これらのモードは、Amazon S3 保持モードと同等です。

- コンプライアンスモードの場合:
  - オブジェクトは、保持期限に達するまで削除できません。
  - オブジェクトの保持期限を増やすことはできますが、減らすことはできません。
  - オブジェクトの保持期限は、その日付に達するまで削除できません。

- ガバナンス モードの場合:
  - 特別な権限を持つユーザーは、リクエストでバイパス ヘッダーを使用して、特定の保持設定を変更できます。
  - これらのユーザーは、オブジェクト バージョンを、その保持期限に達する前に削除できます。
  - これらのユーザーは、オブジェクトの保持期限を増減または削除できます。

オブジェクトバージョンの保持設定

S3 オブジェクト ロックを有効にしてバケットを作成した場合、ユーザーは S3 クライアント アプリケーションを使用して、バケットに追加されるオブジェクトごとに次の保持設定をオプションで指定できます。

- 保持モード: コンプライアンスまたはガバナンスのいずれか。
- 保持期限: オブジェクト バージョンの保持期限が将来の日付である場合、オブジェクトを取得することはできますが、削除することはできません。
- 法的保留: オブジェクト バージョンに法的保留を適用すると、そのオブジェクトは直ちにロックされます。たとえば、調査や法的紛争に関連するオブジェクトに対して法的保留を設定する必要がある場合があります。法的保留には有効期限はありませんが、明示的に削除されるまで有効のままになります。法的保留は、保持期限とは無関係です。

> ⓘ オブジェクトが法的保留中の場合、保持モードに関係なく、誰もそのオブジェクトを削除することはできません。

オブジェクト設定の詳細については、"S3 REST API を使用して S3 オブジェクトロックを設定する" 。

バケットのデフォルトの保持設定

S3 オブジェクトロックを有効にしてバケットを作成すると、ユーザーはオプションでバケットの次のデフォルト設定を指定できます。

- デフォルトの保持モード: コンプライアンスまたはガバナンスのいずれか。
- デフォルトの保持期間: このバケットに追加された新しいオブジェクト バージョンを、追加された日から保持する期間。

デフォルトのバケット設定は、独自の保持設定を持たない新しいオブジェクトにのみ適用されます。これらのデフォルト設定を追加または変更しても、既存のバケット オブジェクトは影響を受けません。

見る"S3バケットを作成する"そして"S3 オブジェクトロックのデフォルト保持を更新"。

S3 オブジェクトロックタスク

グリッド管理者とテナント ユーザー向けの次のリストには、S3 オブジェクト ロック機能を使用するための高レベルのタスクが含まれています。

グリッド管理者

- StorageGRIDシステム全体に対してグローバル S3 オブジェクト ロック設定を有効にします。
- 情報ライフサイクル管理（ILM）ポリシーが準拠していることを確認する。つまり、"S3 オブジェクトロックが有効になっているバケットの要件" 。

- 必要に応じて、テナントがコンプライアンスを保持モードとして使用できるようにします。それ以外の場合は、ガバナンス モードのみが許可されます。
- 必要に応じて、テナントの最大保持期間を設定します。

テナントユーザー

- S3 オブジェクトロックを使用したバケットとオブジェクトに関する考慮事項を確認します。
- 必要に応じて、グリッド管理者に連絡して、グローバル S3 オブジェクト ロック設定を有効にし、権限を設定します。
- S3 オブジェクトロックを有効にしてバケットを作成します。
- 必要に応じて、バケットのデフォルトの保持設定を構成します。
  - デフォルトの保持モード: グリッド管理者が許可している場合、ガバナンスまたはコンプライアンス。
  - デフォルトの保持期間: グリッド管理者によって設定された最大保持期間以下である必要があります。
- S3 クライアント アプリケーションを使用してオブジェクトを追加し、オプションでオブジェクト固有の保持期間を設定します。
  - 保持モード。グリッド管理者によって許可されている場合、ガバナンスまたはコンプライアンス。
  - 保持期限: グリッド管理者が設定した最大保持期間で許可されている値以下である必要があります。

S3 オブジェクトロックが有効になっているバケットの要件

- StorageGRIDシステムでグローバル S3 オブジェクト ロック設定が有効になっている場合は、テナント マネージャ、テナント管理 API、または S3 REST API を使用して、S3 オブジェクト ロックが有効になっているバケットを作成できます。
- S3 オブジェクトロックを使用する予定の場合は、バケットを作成するときに S3 オブジェクトロックを有効にする必要があります。既存のバケットに対して S3 オブジェクトロックを有効にすることはできません。
- バケットに対して S3 オブジェクト ロックが有効になっている場合、 StorageGRID はそのバケットのバージョン管理を自動的に有効にします。 S3 オブジェクトロックを無効にしたり、バケットのバージョン管理を一時停止したりすることはできません。
- オプションで、テナント マネージャー、テナント管理 API、または S3 REST API を使用して、各バケットのデフォルトの保持モードと保持期間を指定できます。バケットのデフォルトの保持設定は、バケットに追加された、独自の保持設定を持たない新しいオブジェクトにのみ適用されます。アップロード時に各オブジェクト バージョンの保持モードと保持期限を指定することにより、これらのデフォルト設定を上書きできます。
- バケットのライフサイクル設定は、S3 オブジェクト ロックが有効になっているバケットでサポートされます。
- S3 オブジェクト ロックが有効になっているバケットでは、CloudMirror レプリケーションはサポートされません。

S3 オブジェクトロックが有効になっているバケット内のオブジェクトの要件

- オブジェクト バージョンを保護するには、バケットのデフォルトの保持設定を指定するか、オブジェクト バージョンごとに保持設定を指定できます。オブジェクト レベルの保持設定は、S3 クライアント アプリケーションまたは S3 REST API を使用して指定できます。

- 保持設定は個々のオブジェクト バージョンに適用されます。オブジェクト バージョンには、保持期限設定と法的保留設定の両方が含まれる場合もあれば、どちらか一方だけが含まれる場合もあり、どちらも含まれない場合もあります。オブジェクトに対して保持期限または法的保留設定を指定すると、リクエストで指定されたバージョンのみが保護されます。オブジェクトの以前のバージョンはロックされたまま、オブジェクトの新しいバージョンを作成できます。

S3 オブジェクトロックが有効になっているバケット内のオブジェクトのライフサイクル

S3 オブジェクトロックが有効になっているバケットに保存された各オブジェクトは、以下の段階を経ます。

1. オブジェクトの取り込み

   S3 オブジェクトロックが有効になっているバケットにオブジェクトバージョンが追加されると、保持設定が次のように適用されます。

   - オブジェクトに保持設定が指定されている場合は、オブジェクト レベルの設定が適用されます。デフォルトのバケット設定はすべて無視されます。
   - オブジェクトに保持設定が指定されていない場合は、デフォルトのバケット設定（存在する場合）が適用されます。
   - オブジェクトまたはバケットに保持設定が指定されていない場合、オブジェクトは S3 オブジェクトロックによって保護されません。

   保持設定が適用されると、オブジェクトと S3 ユーザー定義メタデータの両方が保護されます。

2. オブジェクトの保持と削除

   保護された各オブジェクトの複数のコピーは、指定された保持期間にわたってStorageGRIDによって保存されます。オブジェクト コピーの正確な数とタイプ、および保存場所は、アクティブな ILM ポリシーの準拠ルールによって決まります。保護されたオブジェクトを、その保持期限に達する前に削除できるかどうかは、その保持モードによって異なります。

   - オブジェクトが法的保留中の場合、保持モードに関係なく、誰もそのオブジェクトを削除することはできません。

従来のコンプライアンス バケットを引き続き管理できますか**?**

S3 オブジェクト ロック機能は、以前のStorageGRIDバージョンで利用可能だったコンプライアンス機能に代わるものです。以前のバージョンのStorageGRIDを使用して準拠バケットを作成した場合、これらのバケットの設定を引き続き管理できますが、新しい準拠バケットを作成することはできなくなります。手順については、https://kb.netapp.com/Advice_and_Troubleshooting/Hybrid_Cloud_Infrastructure/StorageGRID/How_to_manage_legacy_Compliant_buckets_in_StorageGRID_11.5["NetAppナレッジベース: StorageGRID 11.5 でレガシー準拠バケットを管理する方法"^] 。

S3 オブジェクトロックのデフォルト保持を更新

バケットの作成時に S3 オブジェクトロックを有効にした場合は、バケットを編集してデフォルトの保持設定を変更できます。デフォルトの保持を有効 (または無効) にしたり、デフォルトの保持モードと保持期間を設定したりできます。

開始する前に

- テナントマネージャーにサインインするには、"サポートされているウェブブラウザ" 。

- あなたは、"すべてのバケットまたはルートアクセス権限を管理する" 。これらの権限は、グループまたはバケット ポリシーの権限設定をオーバーライドします。
- S3 オブジェクト ロックはStorageGRIDシステムに対してグローバルに有効になっており、バケットの作成時に S3 オブジェクト ロックが有効になっています。見る"S3 オブジェクトロックを使用してオブジェクトを保持する" 。

手順

1. ダッシュボードから*バケットの表示*を選択するか、ストレージ **(S3)** > *バケット*を選択します。
2. テーブルからバケット名を選択します。

   バケットの詳細ページが表示されます。

3. バケット オプション タブから、**S3** オブジェクト ロック アコーディオンを選択します。
4. 必要に応じて、このバケットの*デフォルトの保持期間*を有効または無効にします。

   この設定の変更は、バケット内にすでに存在するオブジェクトや、独自の保持期間を持つ可能性のあるオブジェクトには適用されません。

5. *デフォルトの保持*が有効になっている場合は、バケットの*デフォルトの保持モード*を指定します。

デフォルトの保持モード	説明
ガバナンス	• ユーザーは `s3:BypassGovernanceRetention`許可は `x-amz-bypass-governance-retention: true`保持設定をバイパスするためのリクエスト ヘッダー。 • これらのユーザーは、オブジェクト バージョンを、その保持期限に達する前に削除できます。 • これらのユーザーは、オブジェクトの保持期限を増減または削除できます。
コンプライアンス	• オブジェクトは、保持期限に達するまで削除できません。 • オブジェクトの保持期限を増やすことはできますが、減らすことはできません。 • オブジェクトの保持期限は、その日付に達するまで削除できません。 注意: グリッド管理者がコンプライアンス モードの使用を許可する必要があります。

6. *デフォルトの保持*が有効になっている場合は、バケットの*デフォルトの保持期間*を指定します。

   デフォルトの保持期間 は、このバケットに追加された新しいオブジェクトが取り込まれた時点から保持される期間を示します。グリッド管理者によって設定されたテナントの最大保持期間以下の値を指定します。

   グリッド管理者がテナントを作成するときに、1 日から 100 年までの値に設定できる最大保持期間が設定されます。 _デフォルト_の保持期間を設定する場合、最大保持期間に設定された値を超えることはできません。必要に応じて、グリッド管理者に最大保存期間の増減を依頼してください。

7. *変更を保存*を選択します。

クロスオリジンリソース共有（CORS）を構成する

S3 バケットとそのバケット内のオブジェクトを他のドメインの Web アプリケーションからアクセスできるようにする場合は、S3 バケットに対してクロスオリジン リソース共有 (CORS) を設定できます。

開始する前に

- テナントマネージャーにサインインするには、"サポートされているウェブブラウザ" 。
- GET CORS設定リクエストの場合、あなたは以下の権限を持つユーザーグループに属しています。"すべてのバケットの管理またはすべてのバケットの表示権限" 。これらの権限は、グループまたはバケット ポリシーの権限設定をオーバーライドします。
- PUT CORS設定リクエストの場合、あなたは以下の権限を持つユーザーグループに属しています。"すべてのバケットの権限を管理する" 。この権限は、グループまたはバケット ポリシーの権限設定をオーバーライドします。
- その"ルートアクセス権限"すべての CORS 構成リクエストへのアクセスを提供します。

タスク概要

クロスオリジン リソース共有 (CORS) は、あるドメイン内のクライアント Web アプリケーションが別のドメイン内のリソースにアクセスできるようにするセキュリティ メカニズムです。たとえば、S3バケットの名前が `Images`グラフィックを保存します。 `CORS`を設定することで、 `Images`バケット内の画像をウェブサイトに表示できるようにすることができます `http://www.example.com`。

バケットの**CORS**を有効にする

手順

1. テキスト エディターを使用して必要な XML を作成します。この例では、S3 バケットの CORS を有効にするために使用される XML を示しています。具体的な制限事項は次のとおりです。
   - 任意のドメインがバケットにGETリクエストを送信できるようにします
   - のみ許可します `http://www.example.com`GET、POST、DELETEリクエストを送信するドメイン
   - すべてのリクエストヘッダーが許可されます

```
<CORSConfiguration
    xmlns="http://s3.amazonaws.com/doc/2020-10-22/">
    <CORSRule>
        <AllowedOrigin>*</AllowedOrigin>
        <AllowedMethod>GET</AllowedMethod>
        <AllowedHeader>*</AllowedHeader>
    </CORSRule>
    <CORSRule>
        <AllowedOrigin>http://www.example.com</AllowedOrigin>
        <AllowedMethod>GET</AllowedMethod>
        <AllowedMethod>POST</AllowedMethod>
        <AllowedMethod>DELETE</AllowedMethod>
        <AllowedHeader>*</AllowedHeader>
    </CORSRule>
</CORSConfiguration>
```

CORS構成XMLの詳細については、以下を参照してください。 "Amazon Web Services (AWS) ドキュメント: Amazon Simple Storage Service ユーザーガイド" 。

2. ダッシュボードから*バケットの表示*を選択するか、ストレージ **(S3)** > *バケット*を選択します。
3. テーブルからバケット名を選択します。

   バケットの詳細ページが表示されます。

4. バケット アクセス タブから、クロスオリジン リソース共有 **(CORS)** アコーディオンを選択します。
5. **CORS** を有効にする チェックボックスを選択します。
6. CORS 構成 XML をテキスト ボックスに貼り付けます。
7. *変更を保存*を選択します。

CORS設定を変更する

手順

1. テキスト ボックス内の CORS 構成 XML を更新するか、[クリア] を選択して最初からやり直します。
2. *変更を保存*を選択します。

CORS設定を無効にする

手順

1. **CORS** を有効にする チェックボックスをオフにします。
2. *変更を保存*を選択します。

バケット内のオブジェクトを削除する

テナント マネージャを使用して、1 つ以上のバケット内のオブジェクトを削除できま

す。

考慮事項と要件

これらの手順を実行する前に、次の点に注意してください。

- バケット内のオブジェクトを削除すると、 StorageGRID は、選択した各バケット内のすべてのオブジェクトとすべてのオブジェクト バージョンを、 StorageGRIDシステム内のすべてのノードとサイトから完全に削除します。 StorageGRID は関連するオブジェクト メタデータも削除します。この情報を回復することはできません。
- バケット内のすべてのオブジェクトを削除するには、オブジェクトの数、オブジェクトのコピー数、同時操作数に応じて、数分、数日、または数週間かかる場合があります。
- バケツに"S3 オブジェクトロックが有効"、 オブジェクトの削除: 読み取り専用 状態が 年間 続く可能性があります。

> S3 オブジェクト ロックを使用するバケットは、すべてのオブジェクトの保持期限に達し、法的保留が解除されるまで、オブジェクトの削除: 読み取り専用 状態のままになります。

- オブジェクトの削除中、バケットの状態は オブジェクトの削除: 読み取り専用 になります。この状態では、バケットに新しいオブジェクトを追加することはできません。
- すべてのオブジェクトが削除されると、バケットは読み取り専用状態のままになります。次のいずれかを実行できます。
  - バケットを書き込みモードに戻し、新しいオブジェクトに再利用します。
  - バケットを削除する
  - バケットを読み取り専用モードにして、将来の使用に備えて名前を予約します。
- バケットでオブジェクトのバージョン管理が有効になっている場合、 StorageGRID 11.8 以降で作成された削除マーカーは、バケット内のオブジェクトの削除操作を使用して削除できます。
- バケットでオブジェクトのバージョン管理が有効になっている場合、オブジェクトの削除操作では、StorageGRID 11.7 以前で作成された削除マーカーは削除されません。バケット内のオブジェクトの削除に関する情報は、"S3 バージョン管理オブジェクトの削除方法" 。
- 使用する場合"クロスグリッドレプリケーション"次の点に注意してください。
  - このオプションを使用すると、他のグリッドのバケットからオブジェクトは削除されません。
  - ソース バケットに対してこのオプションを選択した場合、他のグリッドの宛先バケットにオブジェクトを追加すると、クロス グリッド レプリケーションの失敗 アラートがトリガーされます。他のグリッドのバケットに誰もオブジェクトを追加しないことを保証できない場合は、"クロスグリッドレプリケーションを無効にする"すべてのバケット オブジェクトを削除する前に、そのバケットに対して実行します。

開始する前に

- テナントマネージャーにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは、"ルートアクセス権限" 。この権限は、グループまたはバケット ポリシーの権限設定をオーバーライドします。

手順

1. ダッシュボードから*バケットの表示*を選択するか、ストレージ **(S3)** > *バケット*を選択します。

「バケット」ページが表示され、既存の S3 バケットがすべて表示されます。

2. アクション メニューまたは特定のバケットの詳細ページを使用します。

   [操作]メニュー

   a. オブジェクトを削除する各バケットのチェックボックスを選択します。

   b. アクション > *バケット内のオブジェクトの削除*を選択します。

   詳細ページ

   a. バケット名を選択すると、その詳細が表示されます。

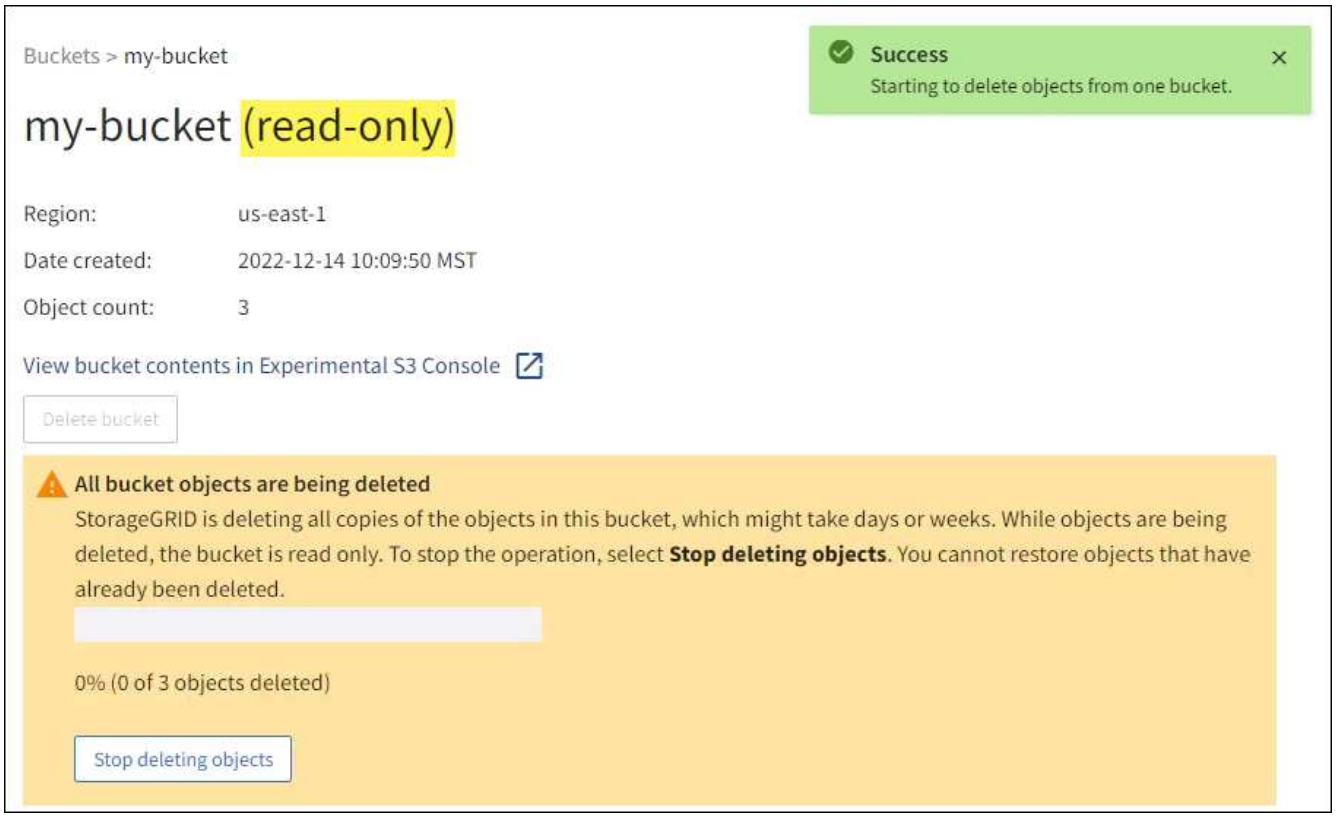
   b. *バケット内のオブジェクトを削除*を選択します。

3. 確認ダイアログボックスが表示されたら、詳細を確認し、「はい」と入力して、「OK」を選択します。

4. 削除操作が開始されるまで待ちます。

   数分後:

   - バケットの詳細ページに黄色のステータス バナーが表示されます。進行状況バーは、削除されたオブジェクトの割合を示します。
   - **(読み取り専用)** は、バケットの詳細ページでバケットの名前の後に表示されます。
   - **(オブジェクトの削除: 読み取り専用)** が [バケット] ページのバケット名の横に表示されます。

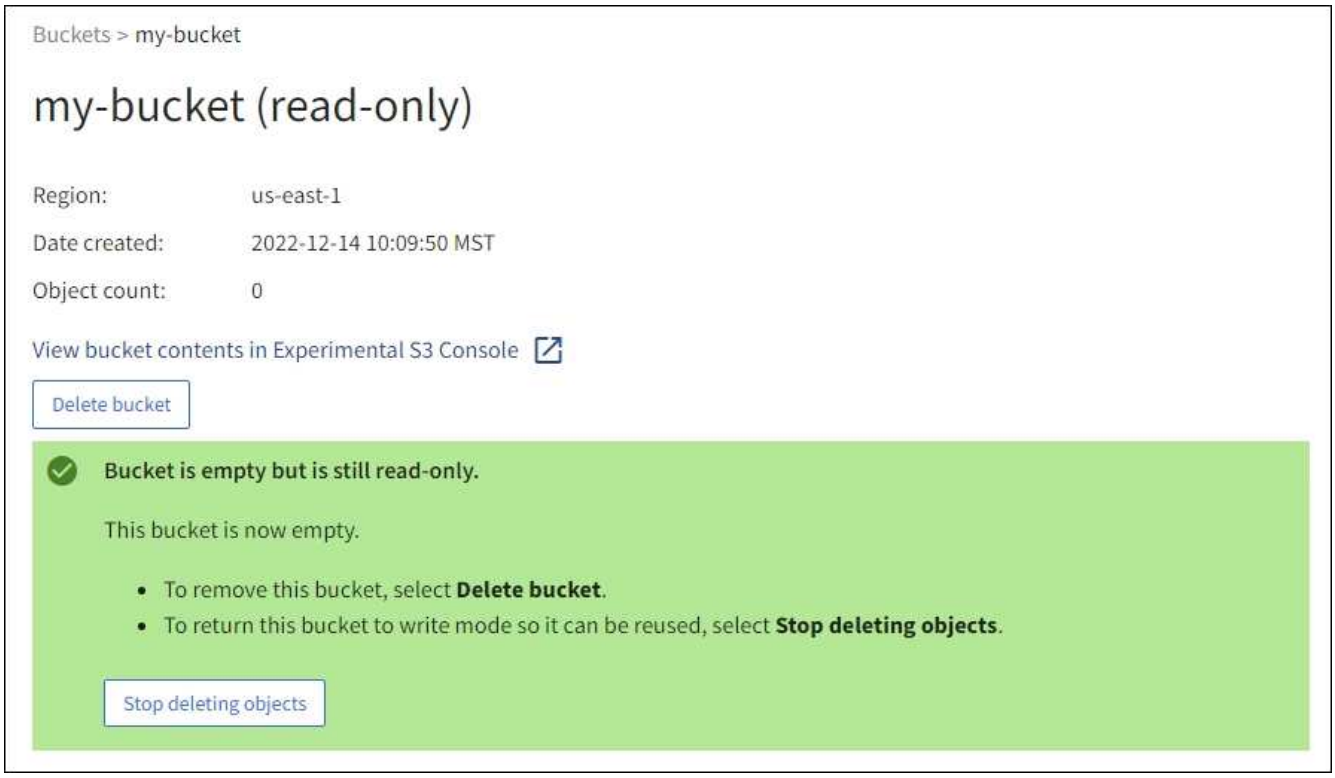


5. 操作の実行中に必要に応じて、[オブジェクトの削除を停止] を選択してプロセスを停止します。次に、オプションで「バケット内のオブジェクトを削除」を選択してプロセスを再開します。

*オブジェクトの削除を停止*を選択すると、バケットは書き込みモードに戻りますが、削除されたオブジェクトにアクセスしたり復元したりすることはできません。

6. 操作が完了するまでお待ちください。

   バケットが空の場合、ステータス バナーは更新されますが、バケットは読み取り専用のままになります。



7. 次のいずれかを実行します。

   - バケットを読み取り専用モードのままにするには、ページを終了します。たとえば、将来の使用に備えてバケット名を予約するために、空のバケットを読み取り専用モードで保持することができます。
   - バケットを削除します。 1 つのバケットを削除するには、「バケットの削除」を選択するか、「バケット」ページに戻って「アクション > バケットの削除」を選択して複数のバケットを削除します。

     すべてのオブジェクトを削除した後でもバージョン管理されたバケットを削除できない場合は、削除マーカーが残る可能性があります。バケットを削除するには、残っている削除マーカーをすべて削除する必要があります。

   - バケットを書き込みモードに戻し、オプションで新しいオブジェクトに再利用します。 1 つのバケットに対して オブジェクトの削除を停止 を選択するか、バケット ページに戻って、複数のバケットに対して アクション > オブジェクトの削除を停止 を選択できます。

S3バケットを削除する

テナント マネージャーを使用して、空の 1 つ以上の S3 バケットを削除できます。

開始する前に

- テナントマネージャーにサインインするには、"サポートされているウェブブラウザ" 。

- あなたは、"すべてのバケットまたはルートアクセス権限を管理する" 。これらの権限は、グループまたはバケット ポリシーの権限設定をオーバーライドします。
- 削除するバケットは空です。削除したいバケットが空でない場合は、"バケットからオブジェクトを削除する" 。

タスク概要

これらの手順では、テナント マネージャーを使用して S3 バケットを削除する方法について説明します。 S3 バケットを削除するには、"テナント管理API"または"S3 REST API"。

S3 バケットにオブジェクト、非現在のオブジェクトバージョン、または削除マーカーが含まれている場合は、そのバケットを削除できません。 S3バージョン管理オブジェクトの削除方法については、以下を参照してください。"オブジェクトの削除方法" 。

手順

1. ダッシュボードから*バケットの表示*を選択するか、ストレージ **(S3)** > *バケット*を選択します。

   「バケット」ページが表示され、既存の S3 バケットがすべて表示されます。

2. アクション メニューまたは特定のバケットの詳細ページを使用します。

   [操作]メニュー

   a. 削除する各バケットのチェックボックスを選択します。
   b. アクション > *バケットの削除*を選択します。

   詳細ページ

   a. バケット名を選択すると、その詳細が表示されます。
   b. *バケットの削除*を選択します。

3. 確認ダイアログボックスが表示されたら、「はい」を選択します。

   StorageGRID は各バケットが空であることを確認し、各バケットを削除します。この処理には数分程度かかります。

   バケットが空でない場合は、エラー メッセージが表示されます。絶対です"バケット内のすべてのオブジェクトと削除マーカーを削除します"バケットを削除する前に。

S3コンソールを使用する

S3 コンソールを使用して、S3 バケット内のオブジェクトを表示および管理できます。

S3 コンソールでは次のことが可能です。

- オブジェクトのアップロード、ダウンロード、名前変更、コピー、移動、削除
- オブジェクトのバージョンを表示、元に戻す、ダウンロード、削除する
- 接頭辞でオブジェクトを検索する

- オブジェクトタグを管理する
- オブジェクトのメタデータを表示する
- フォルダの表示、作成、名前の変更、コピー、移動、削除

> S3 コンソールは、最も一般的なケースにおいて、改善されたユーザー エクスペリエンスを提供します。あらゆる状況で CLI または API 操作を置き換えるようには設計されていません。
>
> S3 コンソールを使用すると操作に時間がかかりすぎる場合 (数分または数時間など)、次のことを検討してください。
>
> - 選択したオブジェクトの数を減らす
> - 非グラフィカル（API または CLI）メソッドを使用してデータにアクセスする

開始する前に

- テナントマネージャーにサインインするには、"サポートされているウェブブラウザ" 。
- オブジェクトを管理する場合は、ルート アクセス権限を持つユーザー グループに属している必要があります。または、「S3 コンソール タブの使用」権限と、「すべてのバケットの表示」権限または「すべてのバケットの管理」権限のいずれかを持つユーザー グループに属しています。見る"テナント管理権限" 。
- ユーザーに対して S3 グループまたはバケット ポリシーが設定されています。見る"バケットとグループのアクセスポリシーを使用する" 。
- ユーザーのアクセス キー ID とシークレット アクセス キーがわかっています。オプションとして、 `.csv` この情報を含むファイル。参照"アクセスキーの作成手順"。

手順

1. ストレージ > バケット > バケット名 を選択します。
2. S3 コンソールタブを選択します。
3. アクセス キー ID とシークレット アクセス キーをフィールドに貼り付けます。それ以外の場合は、「アクセスキーをアップロード」を選択し、 `.csv`ファイル。
4. *Sign in*を選択します。
5. バケット オブジェクトのテーブルが表示されます。必要に応じてオブジェクトを管理できます。

追加情報

- プレフィックスによる検索: プレフィックス検索機能は、現在のフォルダーを基準として特定の単語で始まるオブジェクトのみを検索します。検索には、他の場所にその単語が含まれるオブジェクトは含まれません。このルールはフォルダー内のオブジェクトにも適用されます。例えば、 `folder1/folder2/somefile-`範囲内のオブジェクトを返します `folder1/folder2/`フォルダと単語で始まる `somefile-`。
- ドラッグ アンド ドロップ: コンピュータのファイル マネージャーから S3 コンソールにファイルをドラッグ アンド ドロップできます。ただし、フォルダをアップロードすることはできません。
- フォルダーの操作: フォルダーを移動、コピー、または名前変更すると、フォルダー内のすべてのオブジェクトが一度に 1 つずつ更新されるため、時間がかかる場合があります。
- バケットのバージョン管理が無効になっている場合の永続的な削除: バージョン管理が無効になっているバケット内のオブジェクトを上書きまたは削除すると、その操作は永続的になります。見る"バケットのオブジェクトのバージョン管理を変更する" 。

S3 プラットフォーム サービスを管理する

S3 プラットフォームサービス

プラットフォームサービスの概要と考慮事項

プラットフォーム サービスを実装する前に、これらのサービスの使用に関する概要と考慮事項を確認してください。

S3の詳細については、"S3 REST APIを使用する" 。

プラットフォームサービスの概要

StorageGRIDプラットフォーム サービスは、イベント通知や S3 オブジェクトおよびオブジェクト メタデータのコピーを外部の宛先に送信できるようにすることで、ハイブリッド クラウド戦略の実装を支援します。

プラットフォーム サービスのターゲットの場所は通常、 StorageGRID展開の外部にあるため、プラットフォーム サービスにより、データの外部ストレージ リソース、通知サービス、検索サービスや分析サービスを使用することで得られるパワーと柔軟性が得られます。

単一の S3 バケットに対して、プラットフォーム サービスの任意の組み合わせを構成できます。たとえば、"CloudMirrorサービス"そして"通知"StorageGRID S3 バケットに作成することで、特定のオブジェクトを Amazon Simple Storage Service (S3) にミラーリングできると同時に、各オブジェクトに関する通知をサードパーティの監視アプリケーションに送信して、AWS 経費を追跡できるようになります。

プラットフォーム サービスの使用は、Grid Manager または Grid Management API を使用して、 StorageGRID管理者がテナント アカウントごとに有効にする必要があります。

プラットフォームサービスの構成方法

プラットフォームサービスは、"Tenant Manager"または"テナント管理API"。各エンドポイントは、StorageGRID S3 バケット、Amazon Web Services バケット、Amazon SNS トピック、ローカル、AWS、またはその他の場所でホストされている Elasticsearch クラスターなどの外部の宛先を表します。

外部エンドポイントを作成した後、バケットに XML 構成を追加して、バケットのプラットフォーム サービスを有効にできます。 XML 構成では、バケットが操作するオブジェクト、バケットが実行するアクション、およびバケットがサービスに使用するエンドポイントが識別されます。

構成するプラットフォーム サービスごとに個別の XML 構成を追加する必要があります。例えば：

- キーが次の文字で始まるすべてのオブジェクトを取得したい場合 `/images`Amazon S3 バケットにレプリケートするには、ソースバケットにレプリケーション設定を追加する必要があります。
- これらのオブジェクトがバケットに保存されたときにも通知を送信する場合は、通知設定を追加する必要があります。
- これらのオブジェクトのメタデータをインデックスする場合は、検索統合を実装するために使用されるメタデータ通知構成を追加する必要があります。

構成 XML の形式は、 StorageGRIDプラットフォーム サービスを実装するために使用される S3 REST API によって管理されます。

プラットフォームサービス	**S3 REST API**	参照
CloudMirrorレプリケーション	• GetBucketReplication • PutBucketレプリケーション	• "CloudMirrorレプリケーション" • "バケットの操作"
通知	• GetBucketNotificationConfiguration • PutBucketNotificationConfiguration	• "通知" • "バケットの操作"
検索統合	• バケットメタデータ通知設定の取得 • PUT バケットメタデータ通知設定	• "検索統合" • "StorageGRIDカスタム操作"

プラットフォームサービスの利用に関する考慮事項

考慮事項	詳細
宛先エンドポイントの監視	各宛先エンドポイントの可用性を監視する必要があります。宛先エンドポイントへの接続が長時間失われ、大量の要求のバックログが存在する場合、StorageGRIDへの追加のクライアント要求 (PUT 要求など) は失敗します。エンドポイントに到達可能になったら、これらの失敗したリクエストを再試行する必要があります。
宛先エンドポイントのスロットリング	リクエストの送信速度が宛先エンドポイントがリクエストを受信できる速度を超えた場合、 StorageGRIDソフトウェアはバケットの受信 S3 リクエストを調整することがあります。スロットルは、宛先エンドポイントへの送信を待機しているリクエストのバックログがある場合にのみ発生します。 目に見える唯一の影響は、受信する S3 リクエストの実行に時間がかかるようになることです。パフォーマンスが大幅に低下していることが検出された場合は、取り込み速度を下げるか、容量の大きいエンドポイントを使用する必要があります。リクエストのバックログが増え続けると、クライアントの S3 操作 (PUT リクエストなど) は最終的に失敗します。 CloudMirror リクエストは、通常、検索統合リクエストやイベント通知リクエストよりも多くのデータ転送を伴うため、宛先エンドポイントのパフォーマンスの影響を受ける可能性が高くなります。

考慮事項	詳細
注文保証	StorageGRID は、サイト内のオブジェクトに対する操作の順序を保証します。オブジェクトに対するすべての操作が同じサイト内で行われる限り、最終的なオブジェクトの状態 (レプリケーションの場合) は常にStorageGRID内の状態と同じになります。 StorageGRID は、 StorageGRIDサイト間で操作が行われるときに、リクエストを順序付けるために最善を尽くします。たとえば、最初にサイト A にオブジェクトを書き込み、その後サイト B で同じオブジェクトを上書きした場合、CloudMirror によって宛先バケットに複製された最終的なオブジェクトが新しいオブジェクトである保証はありません。
ILMによるオブジェクトの削除	AWS CRR および Amazon Simple Notification Service の削除動作と一致させるため、 StorageGRID ILM ルールによりソースバケット内のオブジェクトが削除された場合、CloudMirror およびイベント通知リクエストは送信されません。たとえば、ILM ルールによって 14 日後にオブジェクトが削除された場合、CloudMirror またはイベント通知リクエストは送信されません。 対照的に、検索統合リクエストは、ILM によってオブジェクトが削除されたときに送信されます。
Kafkaエンドポイントの使用	Kafka エンドポイントでは、相互 TLS はサポートされていません。その結果、もしあなたが `ssl.client.auth`に設定 `required`Kafka ブローカー構成では、Kafka エンドポイント構成の問題が発生する可能性があります。 Kafka エンドポイントの認証では、次の認証タイプが使用されます。これらのタイプは、Amazon SNS などの他のエンドポイントの認証に使用されるタイプとは異なり、ユーザー名とパスワードの認証情報が必要です。 • SASL/プレーン • SASL/SCRAM-SHA-256 • SASL/SCRAM-SHA-512 注: 構成されたストレージ プロキシ設定は、Kafka プラットフォーム サービス エンドポイントには適用されません。

CloudMirrorレプリケーションサービスの使用に関する考慮事項

考慮事項	詳細
レプリケーションステータス	StorageGRIDはサポートしていません `x-amz-replication-status`ヘッダ。

考慮事項	詳細
オブジェクトのサイズ	CloudMirror レプリケーション サービスによって宛先バケットにレプリケートできるオブジェクトの最大サイズは 5 TiB で、これはサポートされているオブジェクトの最大サイズと同じです。 注: 1 回の PutObject 操作の最大 推奨 サイズは 5 GiB (5,368,709,120 バイト) です。 5 GiB を超えるオブジェクトがある場合は、代わりにマルチパートアップロードを使用します。
バケットのバージョン管理とバージョンID	StorageGRIDのソース S3 バケットでバージョン管理が有効になっている場合は、宛先バケットでもバージョン管理を有効にする必要があります。 バージョン管理を使用する場合、S3 プロトコルの制限により、宛先バケット内のオブジェクト バージョンの順序付けはベスト エフォートであり、CloudMirror サービスによって保証されないことに注意してください。 注意: StorageGRIDのソース バケットのバージョン ID は、宛先バケットのバージョン ID とは関連がありません。
オブジェクトバージョンのタグ付け	CloudMirror サービスは、S3 プロトコルの制限により、バージョン ID を提供する PutObjectTagging または DeleteObjectTagging リクエストを複製しません。ソースと宛先のバージョン ID は関連していないため、特定のバージョン ID へのタグ更新が確実に複製されるかどうかはわかりません。 対照的に、CloudMirror サービスは、バージョン ID を指定しない PutObjectTagging リクエストまたは DeleteObjectTagging リクエストを複製します。これらのリクエストは、最新のキー (バケットがバージョン管理されている場合は最新バージョン) のタグを更新します。タグ付きの通常の取り込み (タグ付けの更新ではない) も複製されます。
マルチパートアップロードと `ETag`価値観	マルチパートアップロードを使用してアップロードされたオブジェクトをミラーリングする場合、CloudMirror サービスはパートを保持しません。その結果、`ETag`ミラーリングされたオブジェクトの値は、 `ETag`元のオブジェクトの値。
SSE-C（顧客提供のキーによるサーバー側暗号化）で暗号化されたオブジェクト	CloudMirror サービスは、SSE-C で暗号化されたオブジェクトをサポートしていません。CloudMirror レプリケーションのソースバケットにオブジェクトを取り込もうとする際に、リクエストに SSE-C リクエストヘッダーが含まれていると、操作は失敗します。
S3 オブジェクトロックが有効になっているバケット	S3 オブジェクトロックが有効になっているソースバケットまたは宛先バケットでは、レプリケーションはサポートされません。

CloudMirrorレプリケーションサービスを理解する

StorageGRID がバケットに追加された特定のオブジェクトを 1 つ以上の外部宛先バケットに複製するようにする場合は、S3 バケットに対して CloudMirror レプリケーションを有効にすることができます。

たとえば、CloudMirror レプリケーションを使用して特定の顧客レコードを Amazon S3 にミラーリングし、AWS サービスを活用してデータの分析を実行することができます。

ソースバケットで S3 オブジェクトロックが有効になっている場合、CloudMirror レプリケーションはサポートされません。

CloudMirrorとILM

CloudMirror レプリケーションは、グリッドのアクティブな ILM ポリシーとは独立して動作します。CloudMirror サービスは、オブジェクトがソース バケットに保存されるとすぐにそれを複製し、できるだけ早く宛先バケットに配信します。オブジェクトの取り込みが成功すると、複製されたオブジェクトの配信がトリガーされます。

CloudMirrorとクロスグリッドレプリケーション

CloudMirror レプリケーションには、クロスグリッド レプリケーション機能との重要な類似点と相違点があります。。 "クロスグリッドレプリケーションとCloudMirrorレプリケーションを比較する" 。

CloudMirrorとS3バケット

CloudMirror レプリケーションは通常、外部の S3 バケットを宛先として使用するように構成されます。ただし、別のStorageGRIDデプロイメントまたは任意の S3 互換サービスを使用するようにレプリケーションを構成することもできます。

既存のバケット

既存のバケットに対して CloudMirror レプリケーションを有効にすると、そのバケットに追加された新しいオブジェクトのみがレプリケートされます。バケット内の既存のオブジェクトは複製されません。既存のオブジェクトのレプリケーションを強制するには、オブジェクトのコピーを実行して既存のオブジェクトのメタデータを更新できます。

CloudMirror レプリケーションを使用してオブジェクトを Amazon S3 の宛先にコピーする場合、Amazon S3 では各 PUT リクエスト ヘッダー内のユーザー定義メタデータのサイズが 2 KB に制限されていることに注意してください。オブジェクトに 2 KB を超えるユーザー定義のメタデータがある場合、そのオブジェクトは複製されません。

複数の宛先バケット

単一のバケット内のオブジェクトを複数の宛先バケットに複製するには、レプリケーション設定 XML で各ルールの宛先を指定します。オブジェクトを同時に複数のバケットに複製することはできません。

バージョン管理されたバケットまたはバージョン管理されていないバケット

バージョン管理されたバケットまたはバージョン管理されていないバケットで CloudMirror レプリケーションを設定できます。宛先バケットはバージョン管理付きでもバージョン管理なしでも構いません。バージョン管理されたバケットとバージョン管理されていないバケットを任意に組み合わせて使用できます。たとえば、バージョン管理されたバケットをバージョン管理されていないソース バケットの宛先として指定したり、その逆を行ったりすることができます。バージョン管理されていないバケット間でレプリケートすることもできます。

削除、レプリケーションループ、イベント

削除動作

Amazon S3 サービス、クロスリージョンレプリケーション (CRR) の削除動作と同じです。ソースバケット内のオブジェクトを削除しても、宛先内の複製されたオブジェクトは削除されません。ソースバケットと宛先バケットの両方がバージョン管理されている場合、削除マーカーが複製されます。宛先バケットがバージョン管理されていない場合、ソースバケット内のオブジェクトを削除しても、削除マーカーが宛先バケットに複製されず、宛先オブジェクトも削除されません。

レプリケーションループからの保護

オブジェクトが宛先バケットに複製されると、 StorageGRID はそれらを「レプリカ」としてマークします。宛先StorageGRIDバケットは、レプリカとしてマークされたオブジェクトを再度レプリケートしないため、偶発的なレプリケーション ループから保護されます。このレプリカ マーキングはStorageGRID内部のものであり、Amazon S3 バケットを宛先として使用するときに AWS CRR を活用できないことはありません。

> ⓘ レプリカをマークするために使用されるカスタムヘッダーは `x-ntap-sg-replica`。このマーキングはカスケードミラーを防止します。 StorageGRID は、2 つのグリッド間の双方向 CloudMirror をサポートしています。

宛先バケット内のイベント

宛先バケット内のイベントの一意性と順序は保証されません。配信の成功を保証するために実行された操作の結果として、ソース オブジェクトの複数の同一コピーが宛先に配信される場合があります。まれに、同じオブジェクトが 2 つ以上の異なるStorageGRIDサイトから同時に更新されると、宛先バケットでの操作の順序がソース バケットでのイベントの順序と一致しない場合があります。

バケットの通知を理解する

StorageGRID が指定されたイベントに関する通知を宛先の Kafka クラスターまたは Amazon Simple Notification Service に送信するようにする場合は、S3 バケットのイベント通知を有効にすることができます。

たとえば、バケットに追加された各オブジェクト（重要なシステム イベントに関連付けられたログ ファイルを表すオブジェクト）に関するアラートを管理者に送信するように設定できます。

イベント通知は、通知設定で指定されたとおりにソース バケットで作成され、宛先に配信されます。オブジェクトに関連付けられたイベントが成功すると、そのイベントに関する通知が作成され、配信のためにキューに入れられます。

通知の一意性と順序は保証されません。配信の成功を保証するために実行された操作の結果として、イベントの通知が複数宛先に配信される場合があります。また、配信は非同期であるため、特に異なるStorageGRIDサイトから発信された操作の場合、宛先での通知の時間順序がソース バケット上のイベントの順序と一致することは保証されません。使用することができます `sequencer`Amazon S3 ドキュメントで説明されているように、イベント メッセージ内のキーを使用して、特定のオブジェクトのイベントの順序を決定します。

StorageGRIDイベント通知は、いくつかの制限付きで Amazon S3 API に準拠します。

- 次のイベント タイプがサポートされています。
  - s3:オブジェクトが作成されました:
  - s3:オブジェクト作成:配置
  - s3:オブジェクト作成:投稿

- s3:オブジェクト作成:コピー
- s3:ObjectCreated:CompleteMultipartUpload
- s3:オブジェクトが削除されました:
- s3:オブジェクトが削除されました:削除
- s3:オブジェクトが削除されました:削除マーカーが作成されました
- s3:オブジェクトの復元:投稿

- StorageGRIDから送信されるイベント通知では標準の JSON 形式が使用されますが、表に示すように、一部のキーは含まれず、他のキーには特定の値が使用されます。

キー名	**StorageGRID**の価値
イベントソース	`sgws:s3`
awsリージョン	含まれていません
x-amz-id-2	含まれていません
アーン	`urn:sgws:s3:::bucket_name`

検索統合サービスを理解する

オブジェクト メタデータに外部の検索およびデータ分析サービスを使用する場合は、S3 バケットの検索統合を有効にすることができます。

検索統合サービスは、オブジェクトが作成または削除されるか、そのメタデータまたはタグが更新されるたびに、S3 オブジェクトのメタデータを宛先エンドポイントに自動的かつ非同期的に送信するカスタムStorageGRIDサービスです。その後、宛先サービスによって提供される高度な検索、データ分析、視覚化、または機械学習ツールを使用して、オブジェクト データを検索、分析し、洞察を得ることができます。

たとえば、S3 オブジェクトのメタデータをリモート Elasticsearch サービスに送信するようにバケットを設定できます。その後、Elasticsearch を使用してバケット全体の検索を実行し、オブジェクト メタデータに存在するパターンの高度な分析を実行できます。

S3 オブジェクト ロックが有効になっているバケットで Elasticsearch 統合を設定できますが、オブジェクトの S3 オブジェクト ロック メタデータ (保持期限や法的保留ステータスを含む) は、Elasticsearch に送信されるメタデータに含まれません。

検索統合サービスによりオブジェクト メタデータが宛先に送信されるため、その構成 XML は「メタデータ 通知構成 XML」と呼ばれます。この構成 XML は、イベント 通知を有効にするために使用される「通知構成 XML」とは異なります。

検索統合と**S3**バケット

バージョン管理されているバケットまたはバージョン管理されていないバケットに対して検索統合サービスを有効にできます。検索統合は、メタデータ通知構成 XML を、操作対象のオブジェクトとオブジェクト メタデータの宛先を指定するバケットに関連付けることによって構成されます。

メタデータ通知は、バケット名、オブジェクト名、およびバージョン ID (存在する場合) で名前が付けられた JSON ドキュメントの形式で生成されます。各メタデータ通知には、オブジェクトのすべてのタグとユーザー メタデータに加えて、オブジェクトのシステム メタデータの標準セットが含まれています。

> タグとユーザー メタデータの場合、 StorageGRID は日付と数値を文字列または S3 イベント通知として Elasticsearch に渡します。これらの文字列を日付または数値として解釈するように Elasticsearch を構成するには、動的フィールド マッピングと日付形式のマッピングに関する Elasticsearch の指示に従います。検索統合サービスを構成する前に、インデックスで動的フィールド マッピングを有効にする必要があります。ドキュメントのインデックスが作成された後は、インデックス内のドキュメントのフィールド タイプを編集することはできません。

検索通知

メタデータ通知は次の場合に生成され、配信キューに追加されます。

- オブジェクトが作成されます。
- グリッドの ILM ポリシーの操作の結果としてオブジェクトが削除される場合を含め、オブジェクトが削除されます。
- オブジェクトのメタデータまたはタグが追加、更新、または削除されます。更新時には、変更された値だけでなく、メタデータとタグの完全なセットが常に送信されます。

メタデータ通知構成 XML をバケットに追加すると、作成した新しいオブジェクトと、データ、ユーザー メタデータ、またはタグを更新して変更したオブジェクトについて通知が送信されます。ただし、バケット内にすでに存在するオブジェクトについては通知は送信されません。バケット内のすべてのオブジェクトのオブジェクト メタデータが宛先に送信されることを確認するには、次のいずれかを実行する必要があります。

- バケットを作成した直後、オブジェクトを追加する前に、検索統合サービスを構成します。
- バケット内にすでに存在するすべてのオブジェクトに対してアクションを実行し、メタデータ通知メッセージを宛先に送信するようにトリガーします。

検索統合サービスと**Elasticsearch**

StorageGRID検索統合サービスは、Elasticsearch クラスターを宛先としてサポートします。他のプラットフォーム サービスと同様に、宛先は、サービスの構成 XML で URN が使用されるエンドポイントで指定されます。使用 "NetApp Interoperability Matrix Tool"サポートされている Elasticsearch のバージョンを確認します。

プラットフォーム サービスのエンドポイントを管理する

プラットフォーム サービスのエンドポイントを構成する

バケットのプラットフォーム サービスを構成する前に、プラットフォーム サービスの宛先となるエンドポイントを少なくとも 1 つ構成する必要があります。

プラットフォーム サービスへのアクセスは、 StorageGRID管理者によってテナントごとに有効化されます。プラットフォーム サービス エンドポイントを作成または使用するには、ストレージ ノードが外部エンドポイント リソースにアクセスできるようにネットワークが構成されているグリッド内で、エンドポイントの管理権限またはルート アクセス権限を持つテナント ユーザーである必要があります。 1 つのテナントに対して、最大 500 個のプラットフォーム サービス エンドポイントを構成できます。詳細については、 StorageGRID管理者にお問い合わせください。

プラットフォーム サービス エンドポイントとは何ですか?

プラットフォーム サービス エンドポイントは、 StorageGRID が外部の宛先にアクセスするために必要な情報を指定します。

たとえば、 StorageGRIDバケットから Amazon S3 バケットにオブジェクトを複製する場合は、 StorageGRID がAmazon の宛先バケットにアクセスするために必要な情報と認証情報を含むプラットフォーム サービス エンドポイントを作成します。

各タイプのプラットフォーム サービスには独自のエンドポイントが必要であるため、使用する予定のプラットフォーム サービスごとに少なくとも 1 つのエンドポイントを構成する必要があります。プラットフォーム サービス エンドポイントを定義した後、サービスを有効にするために使用される構成 XML で、エンドポイントの URN を宛先として使用します。

複数のソース バケットの宛先として同じエンドポイントを使用できます。たとえば、複数のソース バケットを構成して、オブジェクト メタデータを同じ検索統合エンドポイントに送信するようにすることで、複数のバケットにわたって検索を実行できるようになります。また、ソースバケットを複数のエンドポイントをターゲットとして使用するように設定することもできます。これにより、オブジェクトの作成に関する通知を 1 つの Amazon Simple Notification Service (Amazon SNS) トピックに送信し、オブジェクトの削除に関する通知を 2 番目の Amazon SNS トピックに送信するといったことが可能になります。

CloudMirror レプリケーションのエンドポイント

StorageGRID は、S3 バケットを表すレプリケーション エンドポイントをサポートしています。これらのバケットは、Amazon Web Services、同じまたはリモートのStorageGRIDデプロイメント、あるいは別のサービスでホストされている場合があります。

通知のエンドポイント

StorageGRID は、Amazon SNS および Kafka エンドポイントをサポートしています。Simple Queue Service (SQS) または AWS Lambda エンドポイントはサポートされていません。

Kafka エンドポイントでは、相互 TLS はサポートされていません。その結果、もしあなたが `ssl.client.auth` に設定 `required`Kafka ブローカー構成では、Kafka エンドポイント構成の問題が発生する可能性があります。

検索統合サービスのエンドポイント

StorageGRID は、Elasticsearch クラスターを表す検索統合エンドポイントをサポートしています。これらの Elasticsearch クラスターは、ローカルデータセンターに配置することも、AWS クラウドやその他の場所でホストすることもできます。

検索統合エンドポイントは、特定の Elasticsearch インデックスとタイプを参照します。 StorageGRIDでエンドポイントを作成する前に、Elasticsearch でインデックスを作成する必要があります。そうしないと、エンドポイントの作成は失敗します。エンドポイントを作成する前にタイプを作成する必要はありません。 StorageGRID は、オブジェクト メタデータをエンドポイントに送信するときに、必要に応じてタイプを作成します。

関連情報

"StorageGRIDの管理"

プラットフォーム サービス エンドポイントを作成するときは、一意のリソース名 (URN) を指定する必要があります。プラットフォーム サービスの構成 XML を作成するときに、URN を使用してエンドポイントを参照します。各エンドポイントの URN は一意である必要があります。

StorageGRID は、プラットフォーム サービス エンドポイントを作成するときにそれを検証します。プラットフォーム サービス エンドポイントを作成する前に、エンドポイントで指定されたリソースが存在し、アクセスできることを確認してください。

URN要素

プラットフォームサービスエンドポイントのURNは、次のいずれかで始まる必要があります。 `arn:aws`または `urn:mysite`、 次のように：

- サービスがAmazon Web Services（AWS）でホストされている場合は、 `arn:aws`
- サービスがGoogle Cloud Platform（GCP）でホストされている場合は、 `arn:aws`
- サービスがローカルでホストされている場合は、 `urn:mysite`

たとえば、 StorageGRIDでホストされているCloudMirrorエンドポイントのURNを指定する場合、URNは次のようになります。 `urn:sgws` 。

URN の次の要素は、次のようにプラットフォーム サービスの種類を指定します。

サービス	タイプ
CloudMirrorレプリケーション	`s3`
通知	`sns`または `kafka`
検索統合	`es`

たとえば、 StorageGRIDでホストされているCloudMirrorエンドポイントのURNを引き続き指定するには、以下を追加します。 `s3`取得するため `urn:sgws:s3`。

URN の最後の要素は、宛先 URI の特定のターゲット リソースを識別します。

サービス	特定のリソース
CloudMirrorレプリケーション	`bucket-name`
通知	`sns-topic-name`または `kafka-topic-name`

サービス	特定のリソース
検索統合	`domain-name/index-name/type-name` 注: Elasticsearch クラスターがインデックスを自動的に作成するように設定されていない場合は、エンドポイントを作成する前に手動でインデックスを作成する必要があります。

AWS および **GCP** でホストされているサービスの **URN**

AWS および GCP エンティティの場合、完全な URN は有効な AWS ARN です。例えば：

- CloudMirror レプリケーション:

```
arn:aws:s3:::bucket-name
```

- 通知：

```
arn:aws:sns:region:account-id:topic-name
```

- 検索統合:

```
arn:aws:es:region:account-id:domain/domain-name/index-name/type-name
```

> AWS検索統合エンドポイントの場合、 `domain-name`リテラル文字列を含める必要があります `domain/`、ここに示すように。

ローカルでホストされるサービスの**URN**

クラウド サービスではなくローカルでホストされるサービスを使用する場合、URN の 3 番目と最後の位置に必要な要素が含まれていれば、有効で一意の URN を作成する任意の方法で URN を指定できます。オプションで指定された要素は空白のままにしておくことも、リソースを識別して URN を一意にする方法で指定することもできます。例えば：

- CloudMirror レプリケーション:

```
urn:mysite:s3:optional:optional:bucket-name
```

StorageGRIDでホストされているCloudMirrorエンドポイントの場合、次の文字で始まる有効なURNを指定できます。 `urn:sgws`：

```
urn:sgws:s3:optional:optional:bucket-name
```

- 通知：

  Amazon Simple Notification Service エンドポイントを指定します。

  ```
  urn:mysite:sns:optional:optional:sns-topic-name
  ```

  Kafka エンドポイントを指定します。

  ```
  urn:mysite:kafka:optional:optional:kafka-topic-name
  ```

- 検索統合:

  ```
  urn:mysite:es:optional:optional:domain-name/index-name/type-name
  ```

  ローカルにホストされた検索統合エンドポイントの場合、 `domain-name`エンドポイントの URN が一意である限り、要素には任意の文字列を指定できます。

プラットフォーム サービス エンドポイントを作成する

プラットフォーム サービスを有効にする前に、正しいタイプのエンドポイントを少なくとも 1 つ作成する必要があります。

開始する前に

- テナントマネージャーにサインインするには、"サポートされているウェブブラウザ" 。
- StorageGRID管理者によって、テナント アカウントに対してプラットフォーム サービスが有効化されました。
- あなたは、"エンドポイントまたはルートアクセス権限を管理する" 。
- プラットフォーム サービス エンドポイントによって参照されるリソースが作成されました。
  - CloudMirrorレプリケーション: S3バケット
  - イベント通知: Amazon Simple Notification Service (Amazon SNS) または Kafka トピック
  - 検索通知: 宛先クラスターがインデックスを自動的に作成するように構成されていない場合の Elasticsearch インデックス。
- 宛先リソースに関する情報は次の通りです。
  - URI (Uniform Resource Identifier) のホストとポート

    StorageGRIDシステムでホストされているバケットを CloudMirror レプリケーションのエンドポイントとして使用する予定の場合は、グリッド管理者に問い合わせて、入力する必要がある値を確認してください。

  - ユニークリソース名 (URN)

"プラットフォーム サービス エンドポイントの URN を指定します"

- 認証資格情報（必要な場合）：

  検索統合エンドポイント

  検索統合エンドポイントでは、次の資格情報を使用できます。

  - アクセスキー: アクセスキーIDとシークレットアクセスキー
  - 基本的なHTTP: ユーザー名とパスワード

  CloudMirror レプリケーションエンドポイント

  CloudMirror レプリケーション エンドポイントの場合、次の認証情報を使用できます。

  - アクセスキー: アクセスキーIDとシークレットアクセスキー
  - CAP (C2S アクセス ポータル): 一時資格情報 URL、サーバーおよびクライアント証明書、クライアント キー、およびオプションのクライアント秘密キー パスフレーズ。

  Amazon SNSエンドポイント

  Amazon SNS エンドポイントの場合、次の認証情報を使用できます。

  - アクセスキー: アクセスキーIDとシークレットアクセスキー

  Kafkaエンドポイント

  Kafka エンドポイントの場合、次の資格情報を使用できます。

  - SASL/PLAIN: ユーザー名とパスワード
  - SASL/SCRAM-SHA-256: ユーザー名とパスワード
  - SASL/SCRAM-SHA-512: ユーザー名とパスワード

- セキュリティ証明書（カスタム CA 証明書を使用している場合）

- Elasticsearch セキュリティ機能が有効になっている場合は、接続テストのためのクラスター監視権限と、ドキュメント更新のためのインデックス書き込み権限またはインデックスとインデックス削除の両方の権限が付与されます。

手順

1. ストレージ **(S3)** > プラットフォーム サービス エンドポイント を選択します。プラットフォーム サービス エンドポイント ページが表示されます。
2. *エンドポイントの作成*を選択します。
3. エンドポイントとその目的を簡単に説明する表示名を入力します。

   エンドポイントがサポートするプラットフォーム サービスのタイプは、エンドポイント ページにリストされるときにエンドポイント名の横に表示されるため、名前にその情報を含める必要はありません。

4. **URI** フィールドに、エンドポイントの一意のリソース識別子 (URI) を指定します。

   次のいずれかの形式を使用します。

```
https://host:port
http://host:port
```

ポートを指定しない場合は、次のデフォルト ポートが使用されます。

- HTTPS URIの場合はポート443、HTTP URIの場合はポート80（ほとんどのエンドポイント）
- HTTPS および HTTP URI のポート 9092 (Kafka エンドポイントのみ)

たとえば、 StorageGRIDでホストされているバケットの URI は次のようになります。

```
https://s3.example.com:10443
```

この例では、 `s3.example.com` StorageGRID高可用性（HA）グループの仮想IP（VIP）のDNSエントリを表し、 `10443`ロード バランサーのエンドポイントで定義されたポートを表します。

> 可能な限り、単一障害点を回避するために、負荷分散ノードの HA グループに接続する必要があります。

同様に、AWS でホストされているバケットの URI は次のようになります。

```
https://s3-aws-region.amazonaws.com
```

> エンドポイントが CloudMirror レプリケーション サービスに使用される場合は、URI にバケット名を含めないでください。 **URN** フィールドにバケット名を含めます。

5. エンドポイントの一意のリソース名 (URN) を入力します。

> エンドポイントを作成した後は、エンドポイントの URN を変更することはできません。

6. *続行*を選択します。
7. *認証タイプ*の値を選択します。

検索統合エンドポイント

検索統合エンドポイントの資格情報を入力またはアップロードします。

指定する資格情報には、宛先リソースに対する書き込み権限が必要です。

認証タイプ	説明	**Credentials**
匿名	宛先への匿名アクセスを提供します。セキュリティが無効になっているエンドポイントでのみ機能します。	認証なし。
アクセス キー	AWS スタイルの認証情報を使用して、宛先との接続を認証します。	• アクセス キー ID • シークレット アクセス キー
基本的なHTTP	ユーザー名とパスワードを使用して、宛先への接続を認証します。	• ユーザー名 • パスワード

CloudMirror レプリケーションエンドポイント

CloudMirror レプリケーション エンドポイントの資格情報を入力またはアップロードします。

指定する資格情報には、宛先リソースに対する書き込み権限が必要です。

認証タイプ	説明	**Credentials**
匿名	宛先への匿名アクセスを提供します。セキュリティが無効になっているエンドポイントでのみ機能します。	認証なし。
アクセス キー	AWS スタイルの認証情報を使用して、宛先との接続を認証します。	• アクセス キー ID • シークレット アクセス キー
CAP（C2Sアクセスポータル）	証明書とキーを使用して、宛先への接続を認証します。	• 一時認証情報URL • サーバーCA証明書（PEMファイルのアップロード） • クライアント証明書（PEMファイルのアップロード） • クライアント秘密鍵（PEMファイルのアップロード、OpenSSL暗号化形式、または暗号化されていない秘密鍵形式） • クライアントの秘密鍵のパスフレーズ（オプション）

Amazon SNSエンドポイント

Amazon SNS エンドポイントの認証情報を入力またはアップロードします。

指定する資格情報には、宛先リソースに対する書き込み権限が必要です。

認証タイプ	説明	**Credentials**
匿名	宛先への匿名アクセスを提供します。セキュリティが無効になっているエンドポイントでのみ機能します。	認証なし。
アクセス キー	AWS スタイルの認証情報を使用して、宛先との接続を認証します。	• アクセス キー ID • シークレット アクセス キー

Kafkaエンドポイント

Kafka エンドポイントの資格情報を入力またはアップロードします。

指定する資格情報には、宛先リソースに対する書き込み権限が必要です。

認証タイプ	説明	**Credentials**
匿名	宛先への匿名アクセスを提供します。セキュリティが無効になっているエンドポイントでのみ機能します。	認証なし。
SASL/プレーン	プレーンテキストのユーザー名とパスワードを使用して、宛先への接続を認証します。	• ユーザー名 • パスワード
SASL/SCRAM-SHA-256	チャレンジ レスポンス プロトコルと SHA-256 ハッシュを使用したユーザー名とパスワードを使用して、宛先への接続を認証します。	• ユーザー名 • パスワード
SASL/SCRAM-SHA-512	チャレンジ レスポンス プロトコルと SHA-512 ハッシュを使用したユーザー名とパスワードを使用して、宛先への接続を認証します。	• ユーザー名 • パスワード

ユーザー名とパスワードが Kafka クラスターから取得された委任トークンから派生している場合は、委任された認証を使用する を選択します。

8. *続行*を選択します。
9. *サーバーの検証*のラジオ ボタンを選択して、エンドポイントへの TLS 接続を検証する方法を選択します。

証明書検証の種類	説明
カスタムCA証明書を使用する	カスタム セキュリティ証明書を使用します。この設定を選択した場合は、カスタム セキュリティ証明書をコピーして、[CA 証明書] テキスト ボックスに貼り付けます。
オペレーティング システムの CA 証明書を使用する	接続を保護するには、オペレーティング システムにインストールされているデフォルトの Grid CA 証明書を使用します。
証明書を検証しない	TLS 接続に使用される証明書が検証されていません。このオプションは安全ではありません。

10. *エンドポイントのテストと作成*を選択します。
    - 指定された資格情報を使用してエンドポイントに到達できる場合は、成功メッセージが表示されます。エンドポイントへの接続は、各サイトの 1 つのノードから検証されます。
    - エンドポイントの検証に失敗した場合、エラー メッセージが表示されます。エラーを修正するためにエンドポイントを変更する必要がある場合は、[エンドポイントの詳細に戻る] を選択して情報を更新します。次に、*エンドポイントのテストと作成*を選択します。

> テナント アカウントでプラットフォーム サービスが有効になっていない場合、エンドポイントの作成は失敗します。 StorageGRID管理者に問い合わせてください。

エンドポイントを構成したら、その URN を使用してプラットフォーム サービスを構成できます。

関連情報

- "プラットフォーム サービス エンドポイントの URN を指定します"
- "CloudMirrorレプリケーションを構成する"
- "イベント通知の設定"
- "検索統合サービスを構成する"

プラットフォーム サービス エンドポイントのテスト接続

プラットフォーム サービスへの接続が変更された場合は、エンドポイントの接続をテストして、宛先リソースが存在し、指定した資格情報を使用してアクセスできることを検証できます。

開始する前に

- テナントマネージャーにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは、"エンドポイントまたはルートアクセス権限を管理する" 。

タスク概要

StorageGRID は、資格情報に正しい権限があるかどうかを検証しません。

手順

1. ストレージ **(S3)** > プラットフォーム サービス エンドポイント を選択します。

プラットフォーム サービス エンドポイント ページが表示され、すでに構成されているプラットフォーム サービス エンドポイントのリストが表示されます。

2. 接続をテストするエンドポイントを選択します。

   エンドポイントの詳細ページが表示されます。

3. *テスト接続*を選択します。
   - 指定された資格情報を使用してエンドポイントに到達できる場合は、成功メッセージが表示されます。エンドポイントへの接続は、各サイトの 1 つのノードから検証されます。
   - エンドポイントの検証に失敗した場合、エラー メッセージが表示されます。エラーを修正するためにエンドポイントを変更する必要がある場合は、[構成] を選択して情報を更新します。次に、[テストして変更を保存]を選択します。

プラットフォーム サービス エンドポイントを編集する

プラットフォーム サービス エンドポイントの構成を編集して、名前、URI、その他の詳細を変更できます。たとえば、期限切れの資格情報を更新したり、フェイルオーバーのためにバックアップ Elasticsearch インデックスを指すように URI を変更したりする必要がある場合があります。プラットフォーム サービス エンドポイントの URN を変更することはできません。

開始する前に

- テナントマネージャーにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは、"エンドポイントまたはルートアクセス権限を管理する" 。

手順

1. ストレージ **(S3)** > プラットフォーム サービス エンドポイント を選択します。

   プラットフォーム サービス エンドポイント ページが表示され、すでに構成されているプラットフォーム サービス エンドポイントのリストが表示されます。

2. 編集するエンドポイントを選択します。

   エンドポイントの詳細ページが表示されます。

3. *構成*を選択します。
4. 必要に応じて、エンドポイントの構成を変更します。

   エンドポイントを作成した後は、エンドポイントの URN を変更することはできません。

   a. エンドポイントの表示名を変更するには、編集アイコンを選択します。
   b. 必要に応じて、URI を変更します。
   c. 必要に応じて、認証タイプを変更します。
      - アクセス キー認証の場合は、**S3** キーの編集 を選択し、新しいアクセス キー ID とシークレット アクセス キーを貼り付けて、必要に応じてキーを変更します。変更をキャンセルする必要がある場合は、「**S3** キー編集を元に戻す」を選択します。

- CAP (C2S アクセス ポータル) 認証の場合、一時的な資格情報の URL またはオプションのクライアント秘密キーのパスフレーズを変更し、必要に応じて新しい証明書とキー ファイルをアップロードします。

> クライアントの秘密キーは、OpenSSL 暗号化形式または暗号化されていない秘密キー形式である必要があります。

d. 必要に応じて、サーバーの検証方法を変更します。

5. *テストして変更を保存*を選択します。
   - 指定された資格情報を使用してエンドポイントに到達できる場合は、成功メッセージが表示されます。エンドポイントへの接続は、各サイトの 1 つのノードから検証されます。
   - エンドポイントの検証に失敗した場合、エラー メッセージが表示されます。エンドポイントを変更してエラーを修正し、[テストして変更を保存] を選択します。

プラットフォーム サービス エンドポイントを削除する

関連付けられているプラットフォーム サービスを使用したくなくなった場合は、エンドポイントを削除できます。

開始する前に

- テナントマネージャーにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは、"エンドポイントまたはルートアクセス権限を管理する" 。

手順

1. ストレージ **(S3)** > プラットフォーム サービス エンドポイント を選択します。

   プラットフォーム サービス エンドポイント ページが表示され、すでに構成されているプラットフォーム サービス エンドポイントのリストが表示されます。

2. 削除する各エンドポイントのチェックボックスを選択します。

> 使用中のプラットフォーム サービス エンドポイントを削除すると、そのエンドポイントを使用するすべてのバケットに対して関連付けられたプラットフォーム サービスが無効になります。まだ完了していないリクエストはすべて削除されます。削除された URN を参照しないようにバケット構成を変更するまで、新しいリクエストは引き続き生成されます。StorageGRID はこれらの要求を回復不能なエラーとして報告します。

3. アクション > *エンドポイントの削除*を選択します。

   確認メッセージが表示されます。

4. *エンドポイントの削除*を選択します。

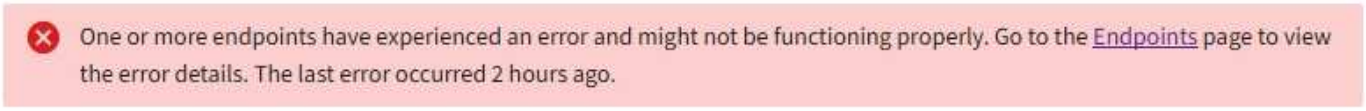
プラットフォーム サービスのエンドポイント エラーのトラブルシューティング

StorageGRID がプラットフォーム サービス エンドポイントとの通信を試行するときにエラーが発生すると、ダッシュボードにメッセージが表示されます。プラットフォーム サービス エンドポイント ページの [最後のエラー] 列には、エラーが発生した時間が表

示されます。エンドポイントの資格情報に関連付けられた権限が正しくない場合、エラーは表示されません。

エラーが発生したかどうかを確認する

過去 7 日以内にプラットフォーム サービス エンドポイント エラーが発生した場合、Tenant Manager ダッシュボードに警告メッセージが表示されます。エラーの詳細を確認するには、プラットフォーム サービス エンドポイント ページにアクセスしてください。



ダッシュボードに表示されるのと同じエラーが、プラットフォーム サービス エンドポイント ページの上部にも表示されます。より詳細なエラー メッセージを表示するには:

手順

1. エンドポイントのリストから、エラーが発生しているエンドポイントを選択します。
2. エンドポイントの詳細ページで、*接続*を選択します。このタブには、エンドポイントの最新のエラーのみが表示され、エラーが発生した時間を示します。赤いXアイコンを含むエラー過去 7 日以内に発生しました。

エラーがまだ発生しているか確認する

一部のエラーは、解決された後も 最後のエラー 列に引き続き表示される場合があります。エラーが最新であるかどうかを確認するか、解決済みのエラーをテーブルから強制的に削除するには、次の手順を実行します。

手順

1. エンドポイントを選択します。

   エンドポイントの詳細ページが表示されます。

2. 接続 > *接続テスト*を選択します。

*テスト接続*を選択すると、 StorageGRID はプラットフォーム サービス エンドポイントが存在し、現在の資格情報でアクセスできることを検証します。エンドポイントへの接続は、各サイトの 1 つのノードから検証されます。

エンドポイントエラーを解決する

エンドポイントの詳細ページの 最後のエラー メッセージを使用すると、エラーの原因を特定するのに役立ちます。エラーによっては、問題を解決するためにエンドポイントを編集する必要がある場合があります。たとえば、適切なアクセス権限がないかアクセス キーの有効期限が切れているためにStorageGRID が宛先 S3 バケットにアクセスできない場合、CloudMirroring エラーが発生する可能性があります。メッセージは「エンドポイント資格情報または宛先アクセスのいずれかを更新する必要があります」で、詳細は「AccessDenied」または「InvalidAccessKeyId」です。

エラーを解決するためにエンドポイントを編集する必要がある場合は、[テストして変更を保存] を選択すると、 StorageGRIDによって更新されたエンドポイントが検証され、現在の資格情報でアクセスできることが確認されます。エンドポイントへの接続は、各サイトの 1 つのノードから検証されます。

手順

1. エンドポイントを選択します。
2. エンドポイントの詳細ページで、*構成*を選択します。
3. 必要に応じてエンドポイント構成を編集します。
4. 接続 > *接続テスト*を選択します。

権限が不十分なエンドポイント認証情報

StorageGRID は、プラットフォーム サービス エンドポイントを検証する際に、エンドポイントの資格情報を使用して宛先リソースに接続できることを確認し、基本的な権限チェックを実行します。ただし、StorageGRID は、特定のプラットフォーム サービス操作に必要なすべての権限を検証するわけではありません。このため、プラットフォーム サービスを使用しようとしたときにエラー (「403 Forbidden」など) が発生した場合は、エンドポイントの資格情報に関連付けられている権限を確認してください。

関連情報

- **StorageGRIDの管理** › プラットフォームサービスのトラブルシューティング
- "プラットフォーム サービス エンドポイントを作成する"
- "プラットフォーム サービス エンドポイントのテスト接続"
- "プラットフォーム サービス エンドポイントを編集する"

CloudMirrorレプリケーションを構成する

バケットの CloudMirror レプリケーションを有効にするには、有効なバケット レプリケーション構成 XML を作成して適用します。

開始する前に

- StorageGRID管理者によって、テナント アカウントに対してプラットフォーム サービスが有効化されました。
- レプリケーション ソースとして機能するバケットはすでに作成されています。
- CloudMirror レプリケーションの宛先として使用するエンドポイントがすでに存在し、その URN があること。
- あなたは、"すべてのバケットまたはルートアクセス権限を管理する" 。これらの権限は、テナント マネージャを使用してバケットを構成するときに、グループまたはバケット ポリシーの権限設定をオーバーライドします。

タスク概要

CloudMirror レプリケーションは、ソース バケットからエンドポイントで指定された宛先バケットにオブジェクトをコピーします。

バケットレプリケーションとその設定方法に関する一般的な情報については、以下を参照してください。"Amazon Simple Storage Service (S3) ドキュメント: オブジェクトのレプリケーション" 。 StorageGRIDがGetBucketReplication、DeleteBucketReplication、およびPutBucketReplicationを実装する方法については、"バケットの操作" 。

CloudMirror レプリケーションには、クロスグリッド レプリケーション機能との重要な類似点と相違点があります。詳細については、"クロスグリッドレプリケーションとCloudMirrorレプリケーションを比較する" 。

CloudMirror レプリケーションを構成するときは、次の要件と特性に注意してください。

- 有効なバケットレプリケーション設定 XML を作成して適用する場合、各宛先の S3 バケットエンドポイントの URN を使用する必要があります。
- S3 オブジェクトロックが有効になっているソースバケットまたは宛先バケットでは、レプリケーションはサポートされません。
- オブジェクトを含むバケットで CloudMirror レプリケーションを有効にすると、バケットに追加された新しいオブジェクトはレプリケートされますが、バケット内の既存のオブジェクトはレプリケートされません。レプリケーションをトリガーするには、既存のオブジェクトを更新する必要があります。
- レプリケーション設定 XML でストレージ クラスを指定すると、 StorageGRID は宛先 S3 エンドポイントに対して操作を実行するときにそのクラスを使用します。宛先エンドポイントも指定されたストレージ クラスをサポートする必要があります。宛先システムベンダーから提供される推奨事項に必ず従ってください。

手順

1. ソースバケットのレプリケーションを有効にします。
    - テキスト エディターを使用して、S3 レプリケーション API で指定されているように、レプリケーションを有効にするために必要なレプリケーション構成 XML を作成します。
    - XML を構成する場合:
        - StorageGRID はレプリケーション構成の V1 のみをサポートすることに注意してください。これは、 StorageGRIDが `Filter`ルールの要素であり、オブジェクト バージョンの削除については V1 規則に従います。詳細については、レプリケーション構成に関する Amazon のドキュメントを参照してください。
        - 宛先として S3 バケットエンドポイントの URN を使用します。
        - オプションで `<StorageClass>`要素を選択し、次のいずれかを指定します。
            - `STANDARD`: デフォルトのストレージ クラス。オブジェクトをアップロードするときにストレージクラスを指定しない場合は、 `STANDARD`ストレージクラスが使用されます。
            - `STANDARD_IA`: (標準 - アクセス頻度が低い)このストレージ クラスは、アクセス頻度は低いが、必要なときに迅速なアクセスが必要なデータに使用します。
            - `REDUCED_REDUNDANCY`: このストレージクラスは、冗長性が低くても保存できる、重要でない再現可能なデータに使用します。 `STANDARD`ストレージクラス。
        - 指定する場合 `Role`構成 XML では無視されます。この値はStorageGRIDでは使用されません。

```
<ReplicationConfiguration>
    <Role></Role>
    <Rule>
        <Status>Enabled</Status>
        <Prefix>2020</Prefix>
        <Destination>
           <Bucket>urn:sgws:s3:::2017-records</Bucket>
           <StorageClass>STANDARD</StorageClass>
         </Destination>
     </Rule>
</ReplicationConfiguration>
```

2. ダッシュボードから*バケットの表示*を選択するか、ストレージ **(S3)** > *バケット*を選択します。
3. ソースバケットの名前を選択します。

   バケットの詳細ページが表示されます。

4. プラットフォーム サービス > レプリケーション を選択します。
5. *レプリケーションを有効にする*チェックボックスを選択します。
6. レプリケーション構成 XML をテキスト ボックスに貼り付け、[変更を保存] を選択します。

   プラットフォーム サービスは、Grid Manager または Grid Management API を使用して、StorageGRID管理者によって各テナント アカウントに対して有効にする必要があります。構成 XML を保存するときにエラーが発生した場合は、 StorageGRID管理者に問い合わせてください。

7. レプリケーションが正しく構成されていることを確認します。
   a. レプリケーション設定で指定されたレプリケーションの要件を満たすオブジェクトをソース バケットに追加します。

      前述の例では、プレフィックス「2020」に一致するオブジェクトが複製されます。

   b. オブジェクトが宛先バケットに複製されたことを確認します。

      小さなオブジェクトの場合、レプリケーションはすぐに行われます。

関連情報

"プラットフォーム サービス エンドポイントを作成する"

イベント通知の設定

バケットの通知を有効にするには、通知設定 XML を作成し、テナント マネージャを使用してその XML をバケットに適用します。

開始する前に

- StorageGRID管理者によって、テナント アカウントに対してプラットフォーム サービスが有効化されました。
- 通知のソースとして機能するバケットはすでに作成されています。
- イベント通知の宛先として使用するエンドポイントがすでに存在し、その URN を所有していること。
- あなたは、"すべてのバケットまたはルートアクセス権限を管理する" 。これらの権限は、テナント マネージャを使用してバケットを構成するときに、グループまたはバケット ポリシーの権限設定をオーバーライドします。

タスク概要

通知設定 XML をソース バケットに関連付けることで、イベント通知を設定します。通知設定 XML は、バケット通知を設定するための S3 規則に従い、宛先の Kafka または Amazon SNS トピックをエンドポイントの URN として指定します。

イベント通知とその設定方法に関する一般的な情報については、 "Amazonのドキュメント" 。 StorageGRIDがS3バケット通知設定APIを実装する方法については、"S3 クライアントアプリケーションの実装手順" 。

バケットのイベント通知を構成するときは、次の要件と特性に注意してください。

- 有効な通知構成 XML を作成して適用する場合は、各宛先のイベント通知エンドポイントの URN を使用する必要があります。
- S3 オブジェクトロックが有効になっているバケットでイベント通知を設定できますが、オブジェクトの S3 オブジェクトロックメタデータ (保持期限や法的保留ステータスを含む) は通知メッセージに含まれません。
- イベント通知を設定すると、ソースバケット内のオブジェクトに対して指定されたイベントが発生するたびに通知が生成され、宛先エンドポイントとして使用される Amazon SNS または Kafka トピックに送信されます。
- オブジェクトを含むバケットに対してイベント通知を有効にすると、通知設定が保存された後に実行されたアクションに対してのみ通知が送信されます。

手順

1. ソースバケットの通知を有効にします。
    - テキスト エディタを使用して、S3 通知 API で指定されているように、イベント通知を有効にするために必要な通知設定 XML を作成します。
    - XML を構成するときは、イベント通知エンドポイントの URN を宛先トピックとして使用します。

```
<NotificationConfiguration>
  <TopicConfiguration>
     <Id>Image-created</Id>
     <Filter>
        <S3Key>
          <FilterRule>
            <Name>prefix</Name>
            <Value>images/</Value>
          </FilterRule>
        </S3Key>
    </Filter>
    <Topic>arn:aws:sns:us-east-1:050340950352:sgws-topic</Topic>
    <Event>s3:ObjectCreated:*</Event>
   </TopicConfiguration>
 </NotificationConfiguration>
```

2. テナント マネージャーで、ストレージ **(S3)** > バケット を選択します。
3. ソースバケットの名前を選択します。

   バケットの詳細ページが表示されます。

4. プラットフォーム サービス > イベント通知 を選択します。
5. *イベント通知を有効にする*チェックボックスを選択します。
6. 通知構成 XML をテキスト ボックスに貼り付け、[変更を保存] を選択します。

   > プラットフォーム サービスは、Grid Manager または Grid Management API を使用して、StorageGRID管理者によって各テナント アカウントに対して有効にする必要があります。構成 XML を保存するときにエラーが発生した場合は、 StorageGRID管理者に問い合わせてください。

7. イベント通知が正しく構成されていることを確認します。

   a. 構成 XML で設定された通知をトリガーするための要件を満たすソース バケット内のオブジェクトに対してアクションを実行します。

      この例では、オブジェクトが作成されるたびにイベント通知が送信されます。 `images/`接頭辞。

   b. 通知が宛先の Amazon SNS または Kafka トピックに配信されたことを確認します。

      たとえば、宛先トピックが Amazon SNS でホストされている場合は、通知が配信されたときに電子メールを送信するようにサービスを設定できます。

```
{
   "Records":[
      {
         "eventVersion":"2.0",
         "eventSource":"sgws:s3",
         "eventTime":"2017-08-08T23:52:38Z",
         "eventName":"ObjectCreated:Put",
         "userIdentity":{
            "principalId":"11111111111111111"
         },
         "requestParameters":{
            "sourceIPAddress":"193.51.100.20"
         },
         "responseElements":{
            "x-amz-request-id":"122047343"
         },
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"Image-created",
            "bucket":{
               "name":"test1",
               "ownerIdentity":{
                  "principalId":"11111111111111111"
               },
               "arn":"arn:sgws:s3:::test1"
            },
            "object":{
               "key":"images/cat.jpg",
               "size":0,
               "eTag":"d41d8cd98f00b204e9800998ecf8427e",
               "sequencer":"14D90402421461C7"
            }
         }
      }
   ]
}
```

+ 通知が宛先トピックで受信された場合、ソース バケットがStorageGRID通知用に正常に構成されています。

関連情報

"バケットの通知を理解する"

"S3 REST APIを使用する"

"プラットフォーム サービス エンドポイントを作成する"

検索統合サービスを構成する

バケットの検索統合を有効にするには、検索統合 XML を作成し、テナント マネージャを使用してその XML をバケットに適用します。

開始する前に

- StorageGRID管理者によって、テナント アカウントに対してプラットフォーム サービスが有効化されました。
- インデックスを作成する内容を含む S3 バケットはすでに作成されています。
- 検索統合サービスの宛先として使用するエンドポイントが既に存在し、その URN を所有していること。
- あなたは、"すべてのバケットまたはルートアクセス権限を管理する" 。これらの権限は、テナント マネージャを使用してバケットを構成するときに、グループまたはバケット ポリシーの権限設定をオーバーライドします。

タスク概要

ソース バケットの検索統合サービスを構成すると、オブジェクトを作成するか、オブジェクトのメタデータまたはタグを更新すると、オブジェクトのメタデータが宛先エンドポイントに送信されます。

すでにオブジェクトが含まれているバケットに対して検索統合サービスを有効にすると、既存のオブジェクトのメタデータ通知は自動的に送信されません。これらの既存のオブジェクトを更新して、そのメタデータが宛先検索インデックスに追加されるようにします。

手順

1. バケットの検索統合を有効にします。
    - テキスト エディターを使用して、検索統合を有効にするために必要なメタデータ通知 XML を作成します。
    - XML を構成するときは、検索統合エンドポイントの URN を宛先として使用します。

      オブジェクトは、オブジェクト名のプレフィックスでフィルタリングできます。たとえば、プレフィックスを持つオブジェクトのメタデータを送信できます。 `images` 1つの宛先に、そしてプレフィックスを持つオブジェクトのメタデータ `videos`別の人に。プレフィックスが重複する構成は無効であり、送信時に拒否されます。たとえば、プレフィックスを持つオブジェクトに対して1つのルールを含む構成では、 `test`接頭辞を持つオブジェクトに対する2番目のルール `test2`は許可されません。

      必要に応じて、メタデータ構成XMLの例 。

```
<MetadataNotificationConfiguration>
 <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
       <Urn>/Urn>
       </Destination>
 </Rule>
</MetadataNotificationConfiguration>
```

メタデータ通知構成 XML の要素:

Name	説明	必須
メタデータ通知構成	メタデータ通知のオブジェクトと宛先を指定するために使用されるルールのコンテナ タグ。 1 つ以上の Rule 要素が含まれます。	はい
Rule	指定されたインデックスにメタデータを追加するオブジェクトを識別するルールのコンテナ タグ。 プレフィックスが重複するルールは拒否されます。 MetadataNotificationConfiguration 要素に含まれます。	はい
ID	ルールの一意の識別子。 ルール要素に含まれます。	いいえ
ステータス	ステータスは「有効」または「無効」になります。無効にされているルールに対してはアクションは実行されません。 ルール要素に含まれます。	はい
接頭辞	プレフィックスに一致するオブジェクトはルールの影響を受け、そのメタデータは指定された宛先に送信されます。 すべてのオブジェクトを一致させるには、空のプレフィックスを指定します。 ルール要素に含まれます。	はい
デスティネーション	ルールの宛先のコンテナ タグ。 ルール要素に含まれます。	はい

Name	説明	必須
壷	オブジェクト メタデータが送信される宛先の URN。次のプロパティを持つStorageGRIDエンドポイントの URN である必要があります。 • `es`3 番目の要素である必要があります。 • URNは、メタデータが格納されているインデックスとタイプで終わる必要があります。形式は次のようになります。 `domain-name/myindex/mytype` 。 エンドポイントは、テナント マネージャーまたはテナント管理 API を使用して構成されます。それらは次の形式をとります: • `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` 構成 XML を送信する前にエンドポイントを構成する必要があります。そうしないと、404 エラーが発生して構成が失敗します。 URN は Destination 要素に含まれます。	はい

2. テナント マネージャーで、ストレージ **(S3)** > バケット を選択します。
3. ソースバケットの名前を選択します。

   バケットの詳細ページが表示されます。

4. プラットフォームサービス > *検索統合*を選択します
5. *検索統合を有効にする*チェックボックスを選択します。
6. メタデータ通知構成をテキスト ボックスに貼り付け、[変更を保存] を選択します。

   プラットフォーム サービスは、Grid Manager または Management API を使用して、StorageGRID管理者がテナント アカウントごとに有効にする必要があります。構成 XML を保存するときにエラーが発生した場合は、 StorageGRID管理者に問い合わせてください。

7. 検索統合サービスが正しく構成されていることを確認します。
   a. 構成 XML で指定されているメタデータ通知をトリガーするための要件を満たすオブジェクトをソースバケットに追加します。

      前述の例では、バケットに追加されたすべてのオブジェクトによってメタデータ通知がトリガーされます。

   b. オブジェクトのメタデータとタグを含む JSON ドキュメントがエンドポイントで指定された検索インデックスに追加されたことを確認します。

終了後の操作

必要に応じて、次のいずれかの方法を使用してバケットの検索統合を無効にすることができます。

- ストレージ **(S3)** > バケット を選択し、検索統合を有効にする チェックボックスをオフにします。
- S3 API を直接使用している場合は、DELETE Bucket メタデータ通知リクエストを使用します。 S3 クライアント アプリケーションの実装手順を参照してください。

例: すべてのオブジェクトに適用されるメタデータ通知設定

この例では、すべてのオブジェクトのオブジェクト メタデータが同じ宛先に送信されます。

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
           <Urn>urn:myes:es:::sgws-notifications/test1/all</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

例: **2**つのルールを使用したメタデータ通知構成

この例では、プレフィックスに一致するオブジェクトのオブジェクトメタデータ `/images`一つの宛先に送信される一方、プレフィックスに一致するオブジェクトのオブジェクトメタデータは `/videos`2 番目の宛先に送信されます。

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Images-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/images</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Videos-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/videos</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

メタデータ通知形式

バケットの検索統合サービスを有効にすると、オブジェクトのメタデータまたはタグが追加、更新、または削除されるたびに、JSON ドキュメントが生成され、宛先エンドポイントに送信されます。

この例では、キーを持つオブジェクトが生成された場合に生成されるJSONの例を示します。 `SGWS/Tagging.txt`バケットに作成されます `test`。その `test`バケットはバージョン管理されていないため、 `versionId`タグが空です。

```
{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region":"us-east-1",
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}
```

JSONドキュメントに含まれるフィールド

ドキュメント名には、バケット名、オブジェクト名、バージョン ID (存在する場合) が含まれます。

バケットとオブジェクトの情報

`bucket`: バケットの名前

`key`: オブジェクトキー名

`versionID`: オブジェクト バージョン（バージョン管理されたバケット内のオブジェクトの場合）

`region`: バケット領域、例 `us-east-1`

システムメタデータ

`size`: HTTPクライアントに表示されるオブジェクトサイズ（バイト単位）

`md5`: オブジェクトハッシュ

ユーザーメタデータ

`metadata`: オブジェクトのすべてのユーザーメタデータ（キーと値のペア）

`key:value`

タグ

`tags`: オブジェクトに定義されているすべてのオブジェクトタグ（キーと値のペア）

`key:value`

Elasticsearchで結果を表示する方法

タグとユーザー メタデータの場合、 StorageGRID は日付と数値を文字列または S3 イベント通知として

Elasticsearch に渡します。これらの文字列を日付または数値として解釈するように Elasticsearch を構成するには、動的フィールド マッピングと日付形式のマッピングに関する Elasticsearch の指示に従います。検索統合サービスを構成する前に、インデックスで動的フィールド マッピングを有効にします。ドキュメントのインデックスが作成された後は、インデックス内のドキュメントのフィールド タイプを編集することはできません。

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。