



# テナントアカウントを使用する StorageGRID 11.8

NetApp  
March 19, 2024

# 目次

テナントアカウントを使用する	1
テナントアカウントを使用する：概要	1
サインインとサインアウトの方法	2
Tenant Managerのダッシュボードについて理解する	7
テナント管理 API	10
グリッドフェデレーション接続を使用する	15
グループとユーザを管理します	29
S3 アクセスキーを管理します	48
S3 バケットを管理する	54
S3 プラットフォームサービスを管理します	76

# 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：概要

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

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

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

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



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

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

## テナントアカウントを作成する方法

テナントアカウントは、によって作成されます ["グリッドマネージャを使用した StorageGRID のグリッド管理者"](#)。グリッド管理者は、テナントアカウントを作成する際に次の項目を指定します。

- テナント名、クライアントタイプ（S3またはSwift）、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に対する権限（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、独自のアイデンティティソースを設定できるか、S3 Selectを使用できるか、グリッドフェデレーション接続を使用できるかなど）。
- テナントの初期ルートアクセス（StorageGRID システムがローカルグループとユーザ、アイデンティティフェデレーション、シングルサインオン（SSO）のいずれを使用しているかに基づく）。

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

## S3 テナントを設定する

その後 "[S3 テナントアカウントが作成されます](#)"では、Tenant Manager にアクセスして次のようなタスクを実行できます。

- アイデンティティフェデレーションを設定する（グリッドとアイデンティティソースを共有する場合を除く）
- グループとユーザを管理します
- アカウントのクローン作成とグリッド間レプリケーションにグリッドフェデレーションを使用します
- S3 アクセスキーを管理します
- S3バケットを作成、管理します
- 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
- ストレージの使用状況を監視



S3バケットはTenant Managerを使用して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](#)"オブジェクトの取り込みと管理を行います。

## Swift テナントを設定します

その後 "[Swift テナントアカウントが作成される](#)"では、Tenant Manager にアクセスして次のようなタスクを実行できます。

- アイデンティティフェデレーションを設定する（グリッドとアイデンティティソースを共有する場合を除く）
- グループとユーザを管理します
- ストレージの使用状況を監視



Swift ユーザが Tenant Manager にアクセスするには、Root Access 権限が必要です。ただし、Root Access権限では、ユーザへの認証を実行できません "[Swift REST API](#)" コンテナを作成してオブジェクトを取り込むため。Swift REST API に認証するには、Swift 管理者の権限が必要です。

# サインインとサインアウトの方法

## Tenant Manager にサインインします

Tenant Manager にアクセスするには、のアドレスバーにテナントの URL を入力します "[サポートされている Web ブラウザ](#)"。

作業を開始する前に

- ログインクレデンシャルが必要です。
- Tenant ManagerにアクセスするためのURLを、グリッド管理者から入手しておきます。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、必ず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、またはその両方を指定することもできます。

- URLに20桁のテナントアカウントIDが含まれていない場合は、このアカウントIDが必要です。
- を使用している ["サポートされている Web ブラウザ"](#)。
- Web ブラウザでクッキーが有効になっている必要があります。
- ユーザは、のユーザグループに属しています ["特定のアクセス権限"](#)。

#### 手順

1. を起動します ["サポートされている Web 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. セキュリティアラートが表示された場合は、ブラウザのインストールウィザードを使用して証明書をインストールします。
4. Tenant Manager にサインインします。

表示されるサインイン画面は、入力したURLと、StorageGRID 用に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が表示されます。[Tenant sign-in]\*リンクを選択します。



**NetApp StorageGRID®**

# Grid Manager

Username

Password

[Sign in](#)

[Tenant sign in](#) | [NetApp support](#) | [NetApp.com](#)

- Tenant Manager のサインインページが表示されます。[Account]\*フィールドは、次のようにすでに入力されている場合があります。

**NetApp StorageGRID®**

# Tenant Manager

**Recent**

-- Optional --

**Account**

64600207336181242061

**Username**

|

**Password**

Sign in

[NetApp support](#) | [NetApp.com](#)

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

Tenant Managerダッシュボードが表示されます。

- iv. 他のユーザーから初期パスワードを受け取った場合は、**\_username\_>\* Change password \***を選択してアカウントを保護します。

### SSOを使用する

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：

Sign in with your organizational account

標準のSSOクレデンシャルを入力し、\*[サインイン]\*を選択します。

- Tenant Manager の SSO サインインページ。

**NetApp StorageGRID®**  
**Tenant Manager**

**Recent**

  
**Account**  
  
[NetApp support](#) | [NetApp.com](#)

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

Tenant Managerダッシュボードが表示されます。

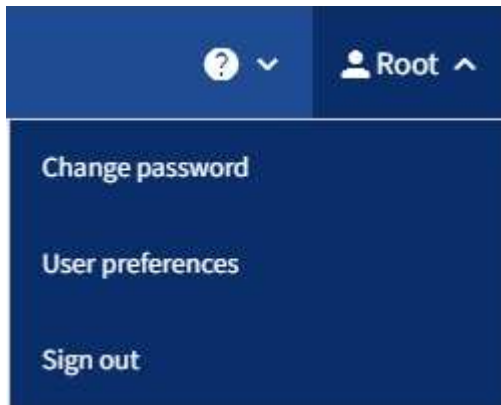


## Tenant Manager からサインアウトします

Tenant Managerの操作が完了したら、サインアウトして、権限のないユーザがStorageGRID システムにアクセスできないようにする必要があります。ブラウザのクッキーの設定によっては、ブラウザを閉じて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にあるユーザ名ドロップダウンを探します。



2. ユーザ名を選択し、\*[サインアウト]\*を選択します。

- SSO を使用していない場合：

管理ノードからサインアウトされます。Tenant Manager のサインインページが表示されます。



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

- SSO が有効になっている場合は、次

アクセスしていたすべての管理ノードからサインアウトされます。StorageGRID のサインインページが表示されます。アクセスしたテナントアカウントの名前がデフォルトで「Recent Accounts \*」ドロップダウンに表示され、テナントの \* アカウント ID \* が表示されます。



SSO が有効で Grid Manager にもサインインしている場合は、Grid Manager からもサインアウトして SSO からサインアウトする必要があります。

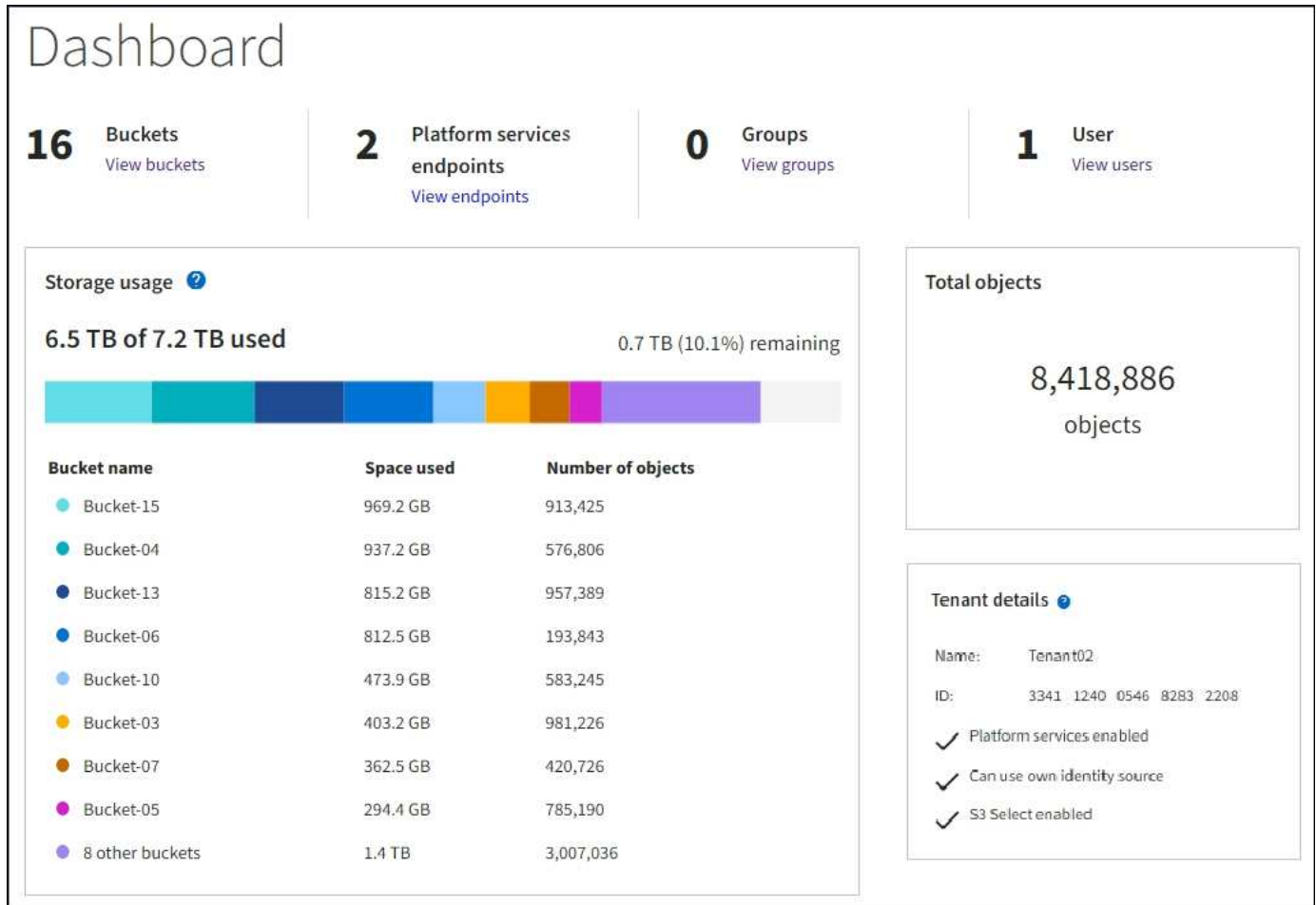
## Tenant Managerのダッシュボードについて理解する

Tenant Managerダッシュボードには、テナントアカウントの設定の概要と、テナントのバケット (S3) またはコンテナ (Swift) でオブジェクトに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、クォータのうち使用されている容量と残りの容量がダッシュボードに表示されます。テナントアカウントに関連するエラーがある場合は、ダッシュボードにそのエラーが表示されます。



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

オブジェクトがアップロードされると、ダッシュボードは次の例のようになります。



## テナントアカウントの概要

ダッシュボードの上部には、次の情報が表示されます。

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

リンクを選択すると詳細を確認できます。

ダッシュボードの右側には、次の情報が表示されます。

- テナントのオブジェクトの合計数。

S3アカウントでオブジェクトが取り込まれておらず、**"rootアクセス権限"**では、オブジェクトの総数ではなく、使用開始のガイドラインが表示されます。

- テナントアカウントの名前と ID、テナントで使用できるかどうかなど、テナントの詳細 **"プラットフォームサービス"**、**"独自のアイデンティティソース"**、**"グリッドフェデレーション"**または **"S3 選択"**（有効な権限だけが表示されます）。

## ストレージとクォータの使用状況

ストレージ使用状況パネルには、次の情報が表示されます。

- テナントのオブジェクトデータの量。



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

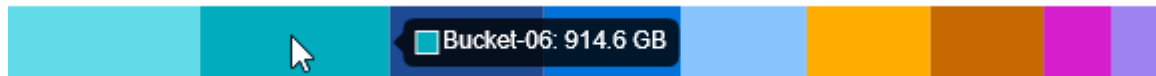
- クォータが設定されている場合は、オブジェクトデータに使用できるスペースの合計容量、および残りのスペースの量と割合。クォータは、取り込むことができるオブジェクトデータの量を制限します。



クォータ使用量は内部の見積もりに基づいており、場合によっては超過する可能性があります。たとえば、テナントがクォータを超えた場合、StorageGRID はテナントがオブジェクトのアップロードを開始したときにクォータをチェックし、新しい取り込みを拒否します。ただし、StorageGRID では、クォータを超過したかどうかを判断する際に、現在のアップロードのサイズは考慮されません。オブジェクトが削除されると、クォータ使用量が再計算されるまでテナントが新しいオブジェクトを一時的にアップロードできなくなる場合があります。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サイズを表す棒グラフ。

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



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

Bucket name	Space used	Number of objects
Bucket-02	944.7 GB	7,575
Bucket-09	899.6 GB	589,677
Bucket-15	889.6 GB	623,542
Bucket-06	846.4 GB	648,619
Bucket-07	730.8 GB	808,655
Bucket-04	700.8 GB	420,493
Bucket-11	663.5 GB	993,729
Bucket-03	656.9 GB	379,329
9 other buckets	2.3 TB	5,171,588

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



Tenant Manager に表示されるストレージ値の単位を変更するには、Tenant Manager の右上にあるユーザドロップダウンを選択し、\*[User preferences]\*を選択します。

## クォータ使用状況アラート

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

テナントのクォータの 90% 以上が使用されると、「テナントクォータ使用率が高い\*」アラートがトリガーされます。アラートの推奨される対処方法を実行します。

Only 0.6% of the quota is remaining. If the quota is exceeded, you can no longer upload new objects.

クォータを超えた場合は、新しいオブジェクトをアップロードできません。

The quota has been met. You cannot upload new objects.

## エンドポイントエラー

Grid Manager 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設定した場合、過去 7 日以内にエンドポイントエラーが発生すると、Tenant Manager ダッシュボードにアラートが表示されます。

One or more endpoints have experienced an error and might not be functioning properly. Go to the [Endpoints](#) page to view the error details. The last error occurred 2 hours ago.

をクリックして詳細を表示します "プラットフォームサービスエンドポイントエラー" を選択し、\*[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 について理解する

Tenant Manager のユーザインターフェイスの代わりにテナント管理 REST API を使用してシステム管理タスクを実行できます。たとえば、API を使用して処理を自動化したり、ユーザなどの複数のエンティティを迅速に作成したりできます。

テナント管理 API :

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

- 使用 ["無停止アップグレードをサポートするためのバージョン管理"](#)。

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

1. Tenant Manager にサインインします。
2. Tenant Managerの上部で、ヘルプアイコンを選択し、\*[API documentation]\*を選択します。

## API 処理

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

- **\* account \***：現在のテナントアカウントに対する処理（ストレージの使用状況情報の取得など）。
- **\* auth \***：ユーザセッション認証を実行する処理。

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

認証セキュリティの向上については、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"](#)。



StorageGRID システムでシングルサインオン（SSO）が有効になっている場合は、別の手順による認証が必要です。を参照してください ["Grid 管理 API の使用手順"](#)。

- **\* config \***：製品リリースおよびテナント管理APIのバージョンに関連する処理。製品リリースバージョンおよびそのリリースでサポートされる API のメジャーバージョンを一覧表示できます。
- **\* containers \***：S3バケットまたはSwiftコンテナに対する処理。
- **\* deactivated-features \***：非アクティブ化された可能性がある機能を表示する操作。
- **\* endpoints \***：エンドポイントを管理する処理。エンドポイントを使用することで、S3 バケットは外部のサービスを StorageGRID CloudMirror レプリケーション、通知、または検索統合に使用できます。
- **\* 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対する処理。
- **\* groups \***：ローカルテナントグループを管理する処理、およびフェデレーテッドテナントグループを外部のアイデンティティソースから取得する処理。
- **\* identity-source \***：外部のアイデンティティソースを設定する処理、およびフェデレーテッドグループとユーザ情報を手動で同期する処理。
- **\* ILM \***：情報ライフサイクル管理（ILM）設定に対する処理。
- **\* regions \***：StorageGRID システムに設定されているリージョンを特定する処理。
- **\* s3 \***：テナントユーザのS3アクセスキーを管理する処理。
- **\* s3-object-lock \***：グローバルS3オブジェクトロック設定に対する処理。法規制への準拠をサポートするために使用されます。
- **\* users \***：テナントユーザを表示および管理する処理。

## 処理の詳細

各 API 処理を展開表示すると、HTTP アクション、エンドポイント URL、必須またはオプションのパラメータのリスト、要求の本文の例（必要な場合）、想定される応答を確認できます。

### groups Operations on groups

**GET** /org/groups Lists Tenant User Groups

**Parameters** Try it out

Name	Description
type string (query)	filter by group type
limit integer (query)	maximum number of results
marker string (query)	marker-style pagination offset (value is Group's URN)
includeMarker boolean (query)	if set, the marker element is also returned
order string (query)	pagination order (desc requires marker)

**Responses** Response content type: application/json

Code	Description
200	

Example Value | Model

```
{
  "responseTime": "2018-02-01T16:22:31.066Z",
  "status": "success",
  "apiVersion": "2.0"
}
```

## 問題 API 要求



API Docs Web ページを使用して実行する API 処理はすべてその場で実行されます。設定データやその他のデータを誤って作成、更新、または削除しないように注意してください。

## 手順

1. HTTP アクションを選択して、要求の詳細を表示します。
2. グループやユーザの ID など、要求で追加のパラメータが必要かどうかを確認します。次に、これらの値

を取得します。必要な情報を取得するために、先に別の API 要求の問題 が必要になることがあります。

3. 要求の本文の例を変更する必要があるかどうかを判断します。その場合は、\* Model \* を選択して各フィールドの要件を確認できます。
4. [\* 試してみてください\*] を選択します。
5. 必要なパラメータを指定するか、必要に応じて要求の本文を変更します。
6. [\* Execute] を選択します。
7. 応答コードを確認し、要求が成功したかどうかを判断します。

## テナント管理 API のバージョン管理

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

たとえば、このリクエストURLはAPIのバージョン4を指定します。

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

APIのメジャーバージョンは、古いバージョンと互換性がない\_変更を行うと更新されます。APIのマイナーバージョンは、\_が古いバージョンと互換性がある\_に変更されると更新されます。互換性のある変更には、新しいエンドポイントやプロパティの追加などがあります。

次の例は、変更のタイプに基づいて API バージョンがどのように更新されるかを示しています。

API に対する変更のタイプ	古いバージョン	新しいバージョン
旧バージョンと互換性があります	2.1	2.2
旧バージョンとの互換性はありません	2.1	3.0

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



サポートされるバージョンを設定できます。詳細については、Swagger APIドキュメントの\* config \*セクションを参照してください。"Grid 管理 API" を参照してください。すべてのAPIクライアントを新しいバージョンを使用するように更新したら、古いバージョンのサポートを無効にする必要があります。

古い要求は、次の方法で廃止とマークされます。

- 応答ヘッダーが「Deprecated : true」となる。
- JSON 応答の本文に「deprecated : true」が追加される
- 廃止の警告が nms.log に追加される。例：

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

現在のリリースでサポートされている **API** のバージョンを確認します

を使用します 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要求。この要求は、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
  ]
}
```

要求の **API** バージョンを指定します

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は、ヘッダー値がパス値よりも優先されます。

```
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**）の防止

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

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

StorageGRID では、CSRF トークンを使用して CSRF 攻撃を防ぐことができます。有効にした場合、特定のクッキーの内容が特定のヘッダーまたは特定の POST パラメータの内容と一致する必要があります。

この機能を有効にするには、を設定します csrfToken パラメータの値 true 認証中です。デフォルトはです false。



```
curl -X POST --header "Content-Type: application/json" --header "Accept: application/json" -d "{
  \"username\": \"MyUserName\",
  \"password\": \"MyPassword\",
  \"cookie\": true,
  \"csrfToken\": true
}" "https://example.com/api/v3/authorize"
```

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

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

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

CSRF 保護を設定するには、を使用してください ["Grid 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要求では、CSRF攻撃に対する追加の保護としてJSON要求本文が必要な要求に対して「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テナントユーザのクローンを作成します

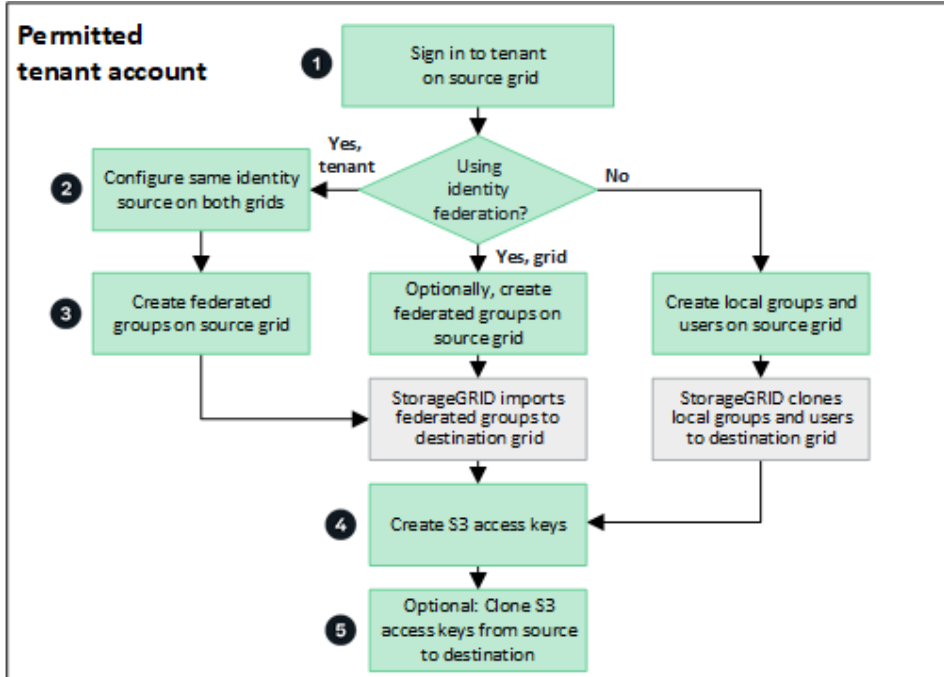
グリッドフェデレーション接続を使用するようにテナントを作成または編集した場合、そのテナントは1つのStorageGRIDシステム（ソーステナント）から別のStorageGRIDシステム（レプリカテナント）にレプリケートされます。テナントがレプリケートされると、ソーステナントに追加されたすべてのグループおよびユーザがレプリカテナントにクローニングされます。

テナントが最初に作成されたStorageGRID システムは、テナントの\_source grid\_です。テナントがレプリケートされているStorageGRID システムは、テナントの\_destination grid\_です。両方のテナントアカウントに、アカウントID、名前、概要、ストレージクォータ、および割り当てられた権限が同じである。ただし、デスティネーションテナントには最初はrootユーザのパスワードが設定されていません。詳細については、を参照してください ["アカウントクローンとは何ですか"](#) および ["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クローニングは、が必要です ["グリッド間レプリケーション"](#) バケットオブジェクト。両方のグリッドに同じテナントグループとユーザが配置されているため、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\* Use grid federation connection \*権限がある場合は、ワークフロー図を確認して、グループ、ユーザ、S3アクセスキーをクローニング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

テナントにサインインします

ソースグリッド（テナントが最初に作成されたグリッド）でテナントアカウントにサインインします。

2

必要に応じて、アイデンティティフェデレーションを設定します

フェデレーテッドグループとユーザを使用するための\* Use own identity source \*権限がテナントアカウントにある場合は、ソースとデスティネーションの両方のテナントアカウントに同じアイデンティティソース（同じ設定）を設定します。フェデレーテッドグループとフェデレーテッドユーザは、両方のグリッドで同じアイデンティティソースを使用していないかぎりクローニングできません。手順については、[を参照してください "アイデンティティフェデレーションを使用する"](#)。

3

グループとユーザを作成します

グループとユーザを作成する場合は、必ずテナントのソースグリッドから開始してください。新しいグループを追加すると、StorageGRID によってデスティネーショングリッドに自動的にクローンが作成されます。

- StorageGRID システム全体またはテナントアカウントに対してアイデンティティフェデレーションが設定されている場合は、["新しいテナントグループを作成します"](#) アイデンティティソースからフェデレーテッドグループをインポートする。
- アイデンティティフェデレーション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します"](#) 次に ["ローカルユーザを作成します"](#)。

## 4

**S3アクセスキーを作成**

可能です **"独自のアクセスキーを作成します"** またはをクリックします **"別のユーザのアクセスキーを作成します"** ソースグリッドまたはデスティネーション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

**必要に応じて、S3アクセスキーをクローニングします**

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を使用してデスティネーショングリッドに手動でクローニングします。手順については、を参照してください **"APIを使用してS3アクセスキーをクローニングします"**。

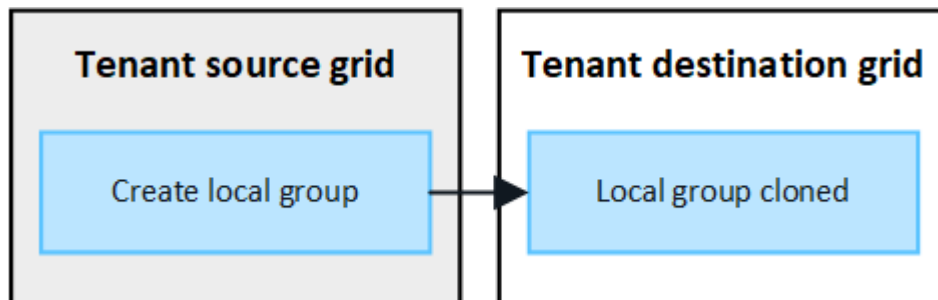
**グループ、ユーザ、S3アクセスキーのクローニング方法**

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の間で、グループ、ユーザ、S3アクセスキーがどのようにクローニングされるかを理解するには、このセクションを確認します。

ソースグリッドに作成されたローカルグループがクローニングされます

テナントアカウントが作成されてデスティネーショングリッドにレプリケートされると、StorageGRID はテナントのソースグリッドに追加したすべてのローカルグループをテナントのデスティネーショングリッドに自動的にクローニングします。

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、S3グループポリシーが設定されています。手順については、を参照してください **"S3 テナント用のグループを作成します"**。



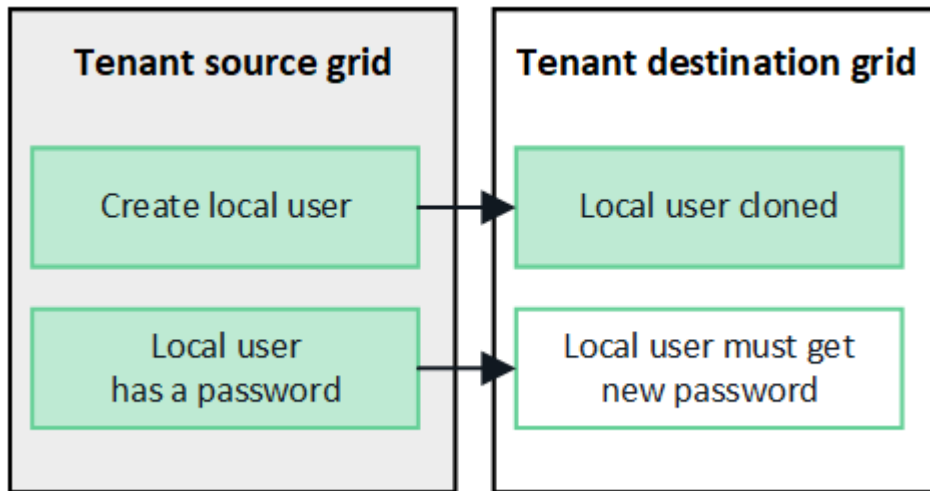
ソースグリッドでローカルグループを作成するときに選択したユーザは、そのグループがデスティネーショングリッドにクローニングされる時に含まれません。このため、グループを作成するときにユーザを選択しないでください。代わりに、ユーザの作成時にグループを選択します。

ソースグリッドに作成されたローカルユーザがクローニングされます

ソースグリッドに新しいローカルユーザを作成すると、StorageGRID によってそのユーザがデスティネーショングリッドに自動的にクローニングされます。元のユーザとそのクローンのフルネーム、ユーザ名、および\* Deny access \*設定が同じです。両方のユーザも同じグループに属しています。手順については、を参照してください **"ローカルユーザを管理します"**。

セキュリティ上の理由から、ローカルユーザのパスワードはデスティネーショングリッドにクローニングされません。デスティネーショングリッドでローカルユーザがTenant Managerにアクセスする必要がある場合は、テナントアカウントのrootユーザがデスティネーショングリッドでそのユーザのパスワードを追加する必

必要があります。手順については、を参照してください "[ローカルユーザを管理します](#)".

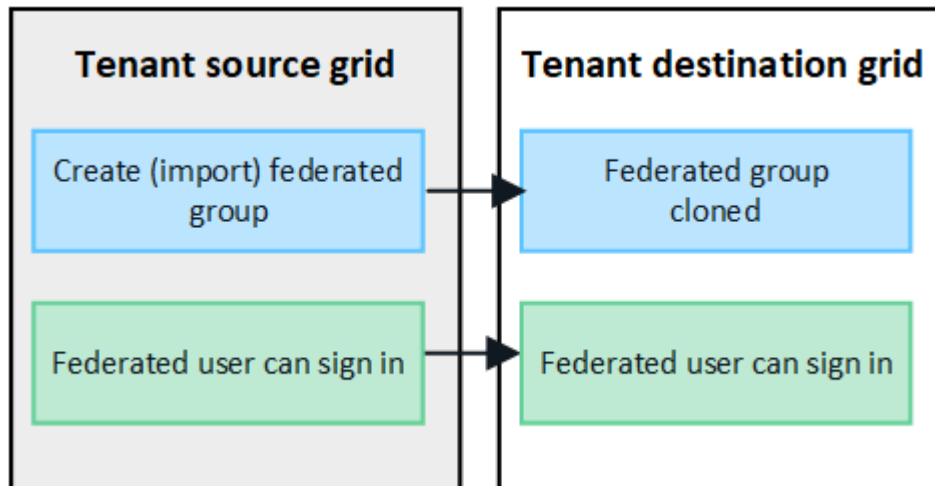


ソースグリッドに作成されたフェデレーテッドグループがクローニングされます

でアカウントクローンを使用するための要件を想定しています "[シングルサインオン](#)" および "[アイデンティティフェデレーション](#)"。これで、ソースグリッドでテナント用に作成（インポート）したフェデレーテッドグループがデスティネーショングリッドのテナントに自動的にクローニングされます。

両方のグループに同じアクセスモード、グループ権限、S3グループポリシーが設定されています。

ソーステナント用にフェデレーテッドグループを作成し、デスティネーションテナントにクローニングすると、フェデレーテッドユーザはどちらのグリッドからテナントにサインインできるようになります。



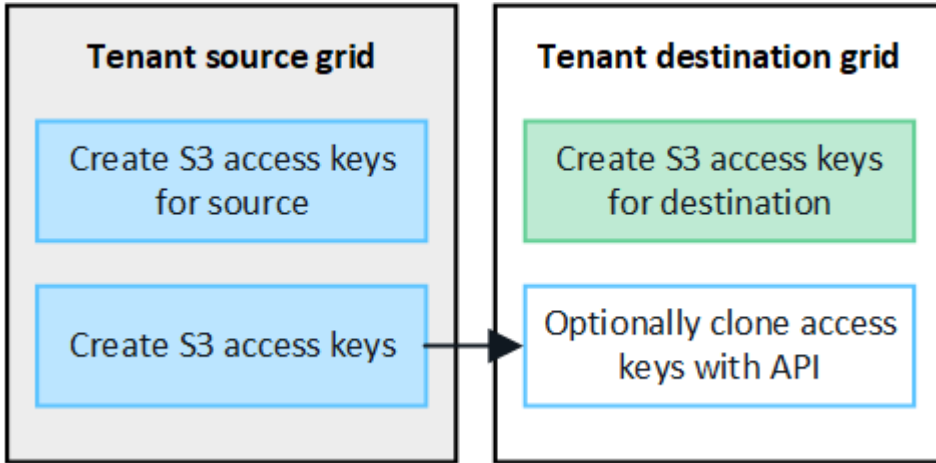
**S3**アクセスキーは手動でクローニングできます

StorageGRID では、S3アクセスキーが自動的にクローニングされることはありません。これは、グリッドごとにキーが異なるためです。

2つのグリッドで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。

- グリッドごとに同じキーを使用する必要がない場合は、できます "[独自のアクセスキーを作成します](#)" または "[別のユーザのアクセスキーを作成します](#)" をクリックします。
- 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、Tenant

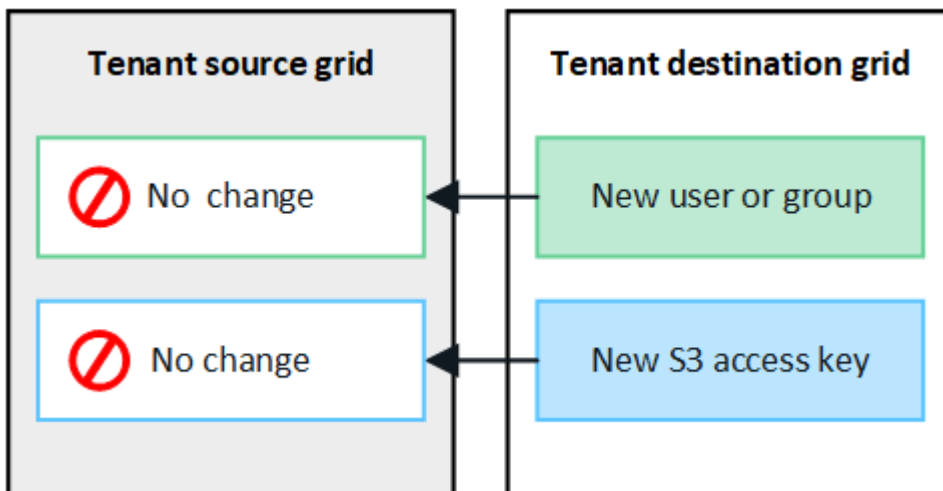
Manager APIを使用して手動でキーを作成できます "キーのクローンを作成します" ターゲットグリッドに移動します。



フェデレーテッドユーザのS3アクセスキーをクローニングすると、ユーザとS3アクセスキーの両方がデスティネーションテナントにクローニングされます。

デスティネーショングリッドに追加されたグループおよびユーザはクローンされません

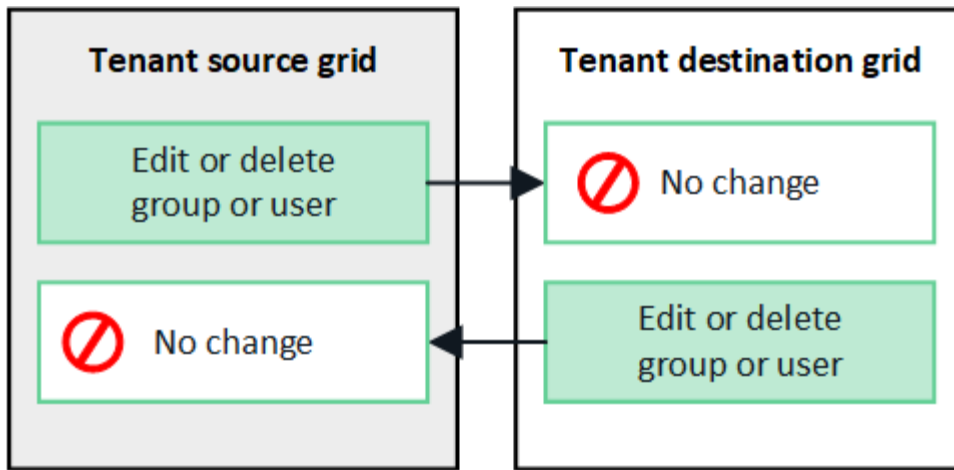
クローニングは、テナントのソースグリッドからテナントのデスティネーショングリッドにのみ実行されます。テナントのデスティネーショングリッドでグループとユーザを作成またはインポートした場合、StorageGRID はこれらの項目をテナントのソースグリッドにクローニングしません。



編集または削除されたグループ、ユーザ、およびアクセスキーのクローンは作成されません

クローニングは、新しいグループおよびユーザを作成した場合にのみ実行されます。

いずれかのグリッドでグループ、ユーザ、またはアクセスキーを編集または削除した場合、変更内容はもう一方のグリッドにクローニングされません。



## APIを使用してS3アクセスキーをクローニングします

テナントアカウントに\* Use grid federation connection \*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デスティネーショングリッドのテナントにS3アクセスキーを手動でクローニングできます。

作業を開始する前に

- テナントアカウントには、\* Use grid federation connection \*権限が割り当てられています。
- グリッドフェデレーション接続は\*[接続済み]\*になっています。
- を使用してテナントのソースグリッドでTenant Managerにサインインしておきます ["サポートされている Web ブラウザ"](#)。
- が設定されたユーザグループに属している必要があります ["自分のS3クレデンシャルまたはRoot Access 権限を管理します"](#)。
- ローカルユーザのアクセスキーをクローニングする場合、そのユーザは両方のグリッドにすでに存在しています。



フェデレーテッドユーザのS3アクセスキーをクローニングすると、ユーザとS3アクセスキーの両方がデスティネーションテナントに追加されます。

自分のアクセスキーのクローンを作成します

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クローニングできます。

手順

1. ソースグリッドでTenant Managerを使用し、 ["独自のアクセスキーを作成します"](#) をダウンロードします .csv ファイル。
2. Tenant Managerの上部で、ヘルプアイコンを選択し、\*[API documentation]\*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. [\* 試してみてください \*] を選択します。
5. body テキストボックスで、AccessKey および secretAccessKey のエントリ例を、ダウンロードした csv \*ファイルの値に置き換えます。

各文字列は必ず二重引用符で囲んでください。



```
body * required
(body)
Edit Value | Model
{
  "accessKey": "AKIAIOSFODNN7EXAMPLE",
  "secretAccessKey": "wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY",
  "expires": "2028-09-04T00:00:00.000Z"
}
```

6. キーが期限切れになる場合は、\* expires の例のエントリを、ISO 8601データタイム形式の文字列として有効期限の日時に置き換えます（例：2024-02-28T22:46:33-08:00）。キーが期限切れにならない場合は、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. [\* Execute] を選択します。
8. サーバ応答コードが「\* 204 \*」であることを確認します。これは、キーがデスティネーショングリッドに正常にクローニングされたことを示します。

別のユーザのアクセスキーのクローンを作成します

別のユーザが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、そのユーザのアクセスキーをクローニングできます。

手順

1. ソースグリッドでTenant Managerを使用し、"[他のユーザのS3アクセスキーを作成します](#)" をダウンロードします .csv ファイル。
2. Tenant Managerの上部で、ヘルプアイコンを選択し、\*[API documentation]\*を選択します。
3. ユーザIDを取得します。この値は、他のユーザのアクセスキーのクローンを作成するときに必要になります。
  - a. [Users]セクションで、次のエンドポイントを選択します。

```
GET /org/users
```
  - b. [\* 試してみてください \*] を選択します。
  - c. ユーザを検索するときに使用するパラメータを指定します。
  - d. [\* Execute] を選択します。
  - e. 複製するキーを持つユーザーを検索し、\* 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

**POST** /org/users/{userId}/replicate-s3-access-key Clone an S3 key to the other grids. 

5. [\* 試してみてください \*] 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IDを貼り付けます。
7. \* body テキストボックスで、 example access key および secret access key のサンプルエントリを、そのユーザの。 csv \*ファイルの値に置き換えます。

文字列は必ず二重引用符で囲んでください。

8. キーが期限切れになる場合は、\* expires の例のエントリを、**ISO 8601**データタイム形式の文字列として有効期限の日時に置き換えます（例：**2023-02-28T22:46:33-08:00**）。キーが期限切れにならない場合は、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. [\* Execute] を選択します。
10. サーバ応答コードが「\* 204 \*」であることを確認します。これは、キーがデスティネーショングリッドに正常にクローニングされたことを示します。

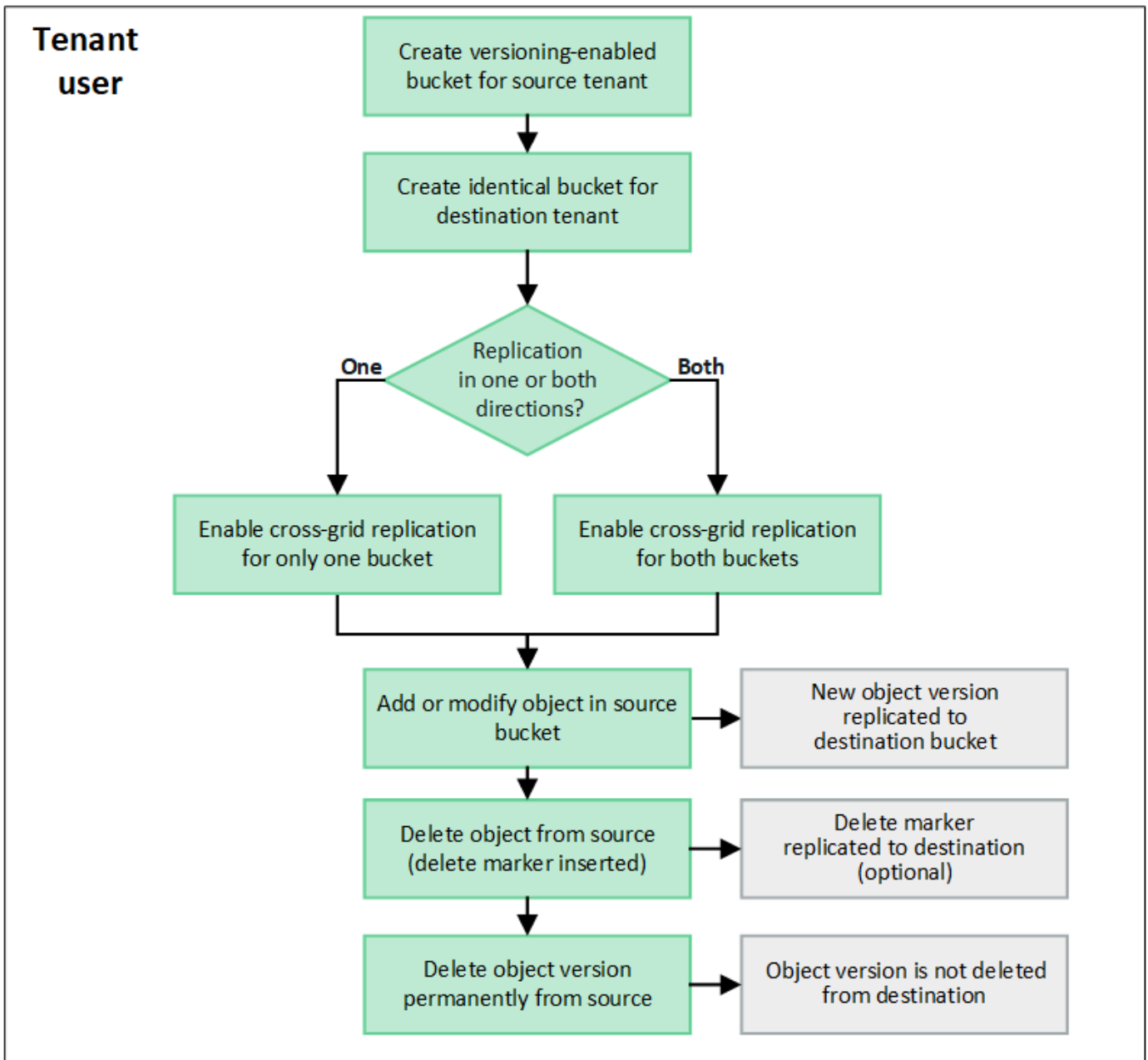
## グリッド間レプリケーションを管理します

テナントアカウントの作成時に「Use grid federation connection \*」権限が割り当てられていた場合は、グリッド間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デスティネーショングリッド上のバケット間でオブジェクトを自動的にレプリケートできます。グリッド間レプリケーションは、一方または両方の方向で実行できます。

### グリッド間レプリケーションのワークフロー

次のワークフロー図は、2つのグリッド上のバケット間でグリッド間レプリケーションを設定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。





### グリッド間レプリケーションを設定する

グリッド間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。その後、一方または両方のバケットでグリッド間レプリケーションを有効にできます。

#### 作業を開始する前に

- グリッド間レプリケーションの要件を確認しておく必要があります。を参照してください ["クロスグリッドレプリケーションとは"](#)。
- を使用している ["サポートされている Web ブラウザ"](#)。
- テナントアカウントには `* Use grid federation connection *`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。を参照してください ["グリッドフェデレーション接続に許可されているテナントを管理します"](#)。
- サインインするテナントユーザが両方のグリッドにすでに存在し、を含むユーザグループに属している

## "rootアクセス権限".

- テナントのデスティネーショングリッドにローカルユーザとしてサインインする場合は、テナントアカウントのrootユーザがそのグリッドでユーザアカウントのパスワードを設定している必要があります。

同一のバケットを2つ作成します

最初の手順として、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、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のクレデンシャルを使用してテナントアカウントにサインインします。



テナントのデスティネーショングリッドにローカルユーザとしてサインインできない場合は、テナントアカウントのrootユーザがユーザ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. の指示に従ってください "**S3バケットを作成**".
  - c. 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. [\*バケットの作成\*]を選択します。
  - f. [完了]を選択します。
2. 同じテナントアカウントに対して同じバケットをグリッドフェデレーション接続のもう一方のグリッドに作成するには、上記の手順を繰り返します。



必要に応じて、各バケットで異なるリージョンを使用できます。

グリッド間レプリケーションを有効にする

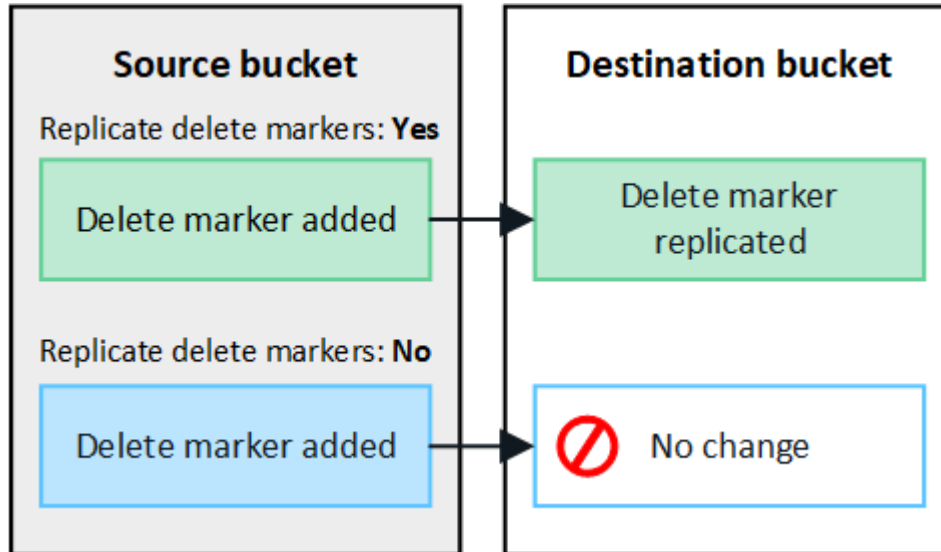
これらの手順は、いずれかのバケットにオブジェクトを追加する前に実行する必要があります。

手順

1. オブジェクトを複製するグリッドから開始して、を有効にします "**一方向のグリッド間レプリケーション**"
  - 
    - a. バケットのテナントアカウントにサインインします。
    - b. ダッシュボードで\* View Buckets を選択するか、 storage (S3) > Buckets \*を選択します。
    - c. 表からバケット名を選択して、バケットの詳細ページにアクセスします。
    - 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. [有効化]\*を選択し、要件のリストを確認します。
    - f. すべての要件を満たしている場合は、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. 必要に応じて、[Replicate delete markers]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

ない削除要求をソースグリッドに対して実行した場合のデスティネーショングリッドでの動作を確認します。

- \* Yes \* (デフォルト) : 削除マーカがソースバケットに追加され、デスティネーションバケットにレプリケートされます。
- \* No \* : 削除マーカはソースバケットに追加されますが、デスティネーションバケットにはレプリケートされません。



削除要求にバージョンIDが含まれている場合は、そのオブジェクトのバージョンが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を含む削除要求をレプリケートしないため、同じオブジェクトバージョンがデスティネーションから削除されることはありません。

を参照してください "[クロスグリッドレプリケーションとは](#)" を参照してください。

- 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) : 失敗したグリッド間レプリケーション要求のみが監査出力に含まれます。
  - \* Normal \* : グリッドをまたぐレプリケーション要求がすべて含まれるため、監査出力の量が大幅に増加します。
- 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。
- [有効にしてテスト]\*を選択します。

しばらくすると、成功の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、もう一方のグリッドに自動的にレプリケートされます。\*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になっている機能として表示されます。

- 必要に応じて、もう一方のグリッドの対応するバケットに移動します "[双方向のグリッド間レプリケーションを有効にします](#)"。

## グリッド間のレプリケーションをテスト

バケットで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、接続とグリッド間レプリケーションが正しく機能していること、ソースとデスティネーションのバケットがすべての要件を満たしていること（バージョン管理が有効になっている場合など）を確認する必要があります。

作業を開始する前に

- を使用している ["サポートされている Web ブラウザ"](#)。
- が設定されたユーザグループに属している必要があります ["rootアクセス権限"](#)。

手順

1. バケットのテナントアカウントにサインインします。
2. ダッシュボードで\* View Buckets を選択するか、storage (S3) > Buckets \*を選択します。
3. 表からバケット名を選択して、バケットの詳細ページにアクセスします。
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. [接続のテスト \*] 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。そうしないとエラーメッセージが表示され、ユーザとグリッド管理者はこ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、[を参照してください](#) ["グリッドフェデレーションエラーをトラブルシューティングする"](#)。

6. グリッド間レプリケーションが両方向で実行されるように設定されている場合は、もう一方のグリッドの対応するバケットに移動して\*[Test connection]\*を選択し、グリッド間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。

## グリッド間レプリケーションを無効にします

オブジェクトをもう一方のグリッドにコピーする必要がなくなった場合は、グリッド間レプリケーションを永続的に停止できます。

グリッド間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。たとえば、のオブジェクトなどです my-bucket にコピーされたグリッド1上 my-bucket グリッド2では、そのバケットのグリッド間レプリケーションを無効にしても削除されません。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。
- 各バケットでグリッド間レプリケーションが有効になっている場合（双方向でレプリケーションが発生した場合）は、一方または両方のバケットでグリッド間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、からのオブジェクトのレプリケーションを無効にすることができます my-bucket グリッド1から my-bucket グリッド2上で、からオブジェクトをレプリケートし続けます my-bucket グリッド2から my-bucket グリッド1上 (On Grid 1) :
- グリッドフェデレーション接続を使用するテナントの権限を削除するには、グリッド間レプリケーションを無効にする必要があります。[を参照してください](#) ["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でクロスグリッドレプリケーションを無効にすると、ソースとデスティネーションの両方のバケットからすべてのオブジェクトを削除しないかぎり、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。

作業を開始する前に

- を使用している ["サポートされている Web ブラウザ"](#)。
- が設定されたユーザグループに属している必要があります ["rootアクセス権限"](#)。

手順

1. レプリケートするオブジェクトが含まれていないグリッドから、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サインインします。
  - b. ダッシュボードで [\\* View Buckets](#) を選択するか、 [storage \(S3\) > Buckets](#) \*を選択します。
  - c. 表からバケット名を選択して、バケットの詳細ページにアクセスします。
  - 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. このバケットでグリッド間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 [「\\* Yes](#) 」と入力し、 [Disable](#) \*を選択します。

しばらくすると、成功の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を他のグリッドに自動的にレプリケートすることはできなくなります。[\\*クロスグリッドレプリケーション\\*](#)は、[\[Buckets\]](#)ページに有効な機能として表示されなくなりました。

2. グリッド間レプリケーションが双方向で実行されるように設定されている場合は、もう一方のグリッドの対応するバケットに移動し、別の方向へのグリッド間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します

テナントアカウントに [\\* Use grid federation connection](#) \*権限がある場合は、許可されている接続を表示できます。

作業を開始する前に

- テナントアカウントには、 [\\* Use grid federation connection](#) \*権限が割り当てられています。
- Tenant Manager にはを使用してサインインします ["サポートされている Web ブラウザ"](#)。
- が設定されたユーザグループに属している必要があります ["rootアクセス権限"](#)。

手順

1. [\\* storage \(S3\) > Grid federation connections](#) \*を選択します。

[\[Grid Federation Connection\]](#)ページが表示され、次の情報を要約した表が含まれます。

列 ( Column )	説明
接続名	このテナントには、使用する権限があるグリッドフェデレーション接続。

列 (Column)	説明
バケットにクロスグリッドレプリケーションが設定されている	グリッドフェデレーション接続ごとに、グリッド間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、接続内のもう一方のグリッドにレプリケートされます。
前回のエラー	グリッドフェデレーション接続ごとに、データがもう一方のグリッドにレプリケートされていたときに発生する最新のエラー（存在する場合）。を参照してください <a href="#">最後のエラーをクリアします</a> 。

2. 必要に応じて、にバケット名を選択します "[バケットの詳細を表示します](#)".

最後のエラーをクリアします

次のいずれかの理由で、\* Last error \*列にエラーが表示されることがあります。

- ソースオブジェクトの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。
- デスティネーションバケットが削除されました。
- デスティネーションバケットが別のアカウントで再作成されました。
- デスティネーションバケットのバージョン管理が中断されています。
- デスティネーションバケットが同じアカウントで再作成されましたが、現在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. 「\* Last error \*」列にメッセージが表示された場合は、メッセージのテキストを確認します。

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デスティネーションバケットが無効な状態であることを示しています。バージョン管理が中断されたか、S3オブジェクトロックが有効になっている可能性があります。

## Grid federation connections

Clear error

🔍
Displaying one result

Connection name	Buckets with cross-grid replication	Last error
○ Grid 1-Grid 2	my-cgr-bucket	<p style="color: red; margin: 0;">2022-12-07 16:02:20 MST</p> <p style="font-size: small; margin: 0;">Cross-grid replication has encountered an error. Failed to send cross-grid replication request from source bucket 'my-cgr-bucket' to destination bucket 'my-cgr-bucket'. Error code: DestinationRequestError. Detail: InvalidBucketState. Confirm that the source and destination buckets have object versioning enabled and S3 Object Lock disabled. (logID 4791585492825418592)</p>

2. 推奨される対処方法を実行します。たとえば、グリッド間レプリケーションのためにデスティネーションバケットでバージョン管理が一時停止されていた場合は、そのバケットのバージョン管理を再度有効にします。
3. テーブルから接続を選択します。
4. [Clear error]\*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表示されないことを確認します。



エラーメッセージがクリアされるように、メッセージのタイムスタンプから5分以上経過してから新しいオブジェクトを取り込んでください。

7. バケットエラーが原因でレプリケートに失敗したオブジェクトがないかどうかを確認するには、を参照してください ["失敗したレプリケーション処理を特定して再試行します"](#)。

## グループとユーザを管理します

### 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テナントユーザを迅速に設定できます。またテナントユーザは、使い慣れたクレデンシャルを使用してテナントアカウントにサインインできます。

### Tenant Manager 用のアイデンティティフェデレーションを設定する

テナントグループとユーザを 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、Tenant Manager 用のアイデンティティフェデレーションを設定できます。

作業を開始する前に

- Tenant Manager にはを使用してサインインします ["サポートされている Web ブラウザ"](#)。
- が設定されたユーザグループに属している必要があります ["rootアクセス権限"](#)。
- アイデンティティプロバイダとして Active Directory、Azure AD、OpenLDAP、または Oracle Directory Server を使用している。



記載されていない 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 を使用する場合は、OpenLDAP サーバを設定する必要があります。を参照してください [OpenLDAP サーバの設定に関するガイドライン](#)。
- LDAP サーバとの通信に Transport Layer Security（TLS）を使用する場合は、アイデンティティプロバイダが TLS 1.2 または 1.3 を使用している必要があります。を参照してください ["発信 TLS 接続でサポートされる暗号"](#)。

このタスクについて

テナントにアイデンティティフェデレーションサービスを設定できるかどうかは、テナントアカウントの設定方法によって異なります。テナントが Grid Manager 用に設定されたアイデンティティフェデレーションサービスを共有する場合があります。[Identity Federation]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は、このテナントに別のフェデレーテッドアイデンティティソースを設定することはできません。

**i** 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.

構成を入力します

フェデレーションの識別を設定するときは、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 \* > \* アイデンティティフェデレーション \* を選択します。
2. [ \* アイデンティティフェデレーションを有効にする \* ] を選択
3. LDAP サービスタイプセクションで、設定する LDAP サービスのタイプを選択します。

### LDAP service type

Select the type of LDAP service you want to configure.

Active Directory	Azure	OpenLDAP	Other
------------------	-------	----------	-------

Oracle Directory Server を使用する LDAP サーバーの値を設定するには、\* 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。それ以外の場合は、次の手順に進みます。
  - \* User Unique Name \* : LDAP ユーザの一意的な ID が含まれている属性の名前。この属性は同じです sAMAccountName Active Directory およびの場合 uid OpenLDAP の場合。Oracle Directory Server を設定する場合は、と入力します uid。
  - \* User UUID \* : LDAP ユーザの永続的な一意な ID が含まれている属性の名前。この属性は同じです objectGUID Active Directory およびの場合 entryUUID OpenLDAP の場合。Oracle Directory Server を設定する場合は、と入力します nsuniqueid。指定した属性の各ユーザの値は、16 バイト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。
  - \* Group Unique Name \* : LDAP グループの一意的な ID が含まれている属性の名前。この属性は同じです sAMAccountName Active Directory およびの場合 cn OpenLDAP の場合。Oracle Directory Server を設定する場合は、と入力します cn。
  - \* グループ UUID \* : LDAP グループの永続的な一意な ID が含まれている属性の名前。この属性は同じです objectGUID Active Directory およびの場合 entryUUID OpenLDAP の場合。Oracle Directory Server を設定する場合は、と入力します nsuniqueid。指定した属性の各グループの値は、16 バイト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 サーバの設定セクションに必要な LDAP サーバおよびネットワーク接続情報を入力します。



- \* Hostname \* : LDAP サーバの完全修飾ドメイン名 ( FQDN ) または IP アドレス。
- \* Port \* : LDAP サーバへの接続に使用するポート。



STARTTLS のデフォルトポートは 389、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れば、任意のポートを使用できます。

- \* Username \* : LDAP サーバに接続するユーザの識別名 ( 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。

指定するユーザには、グループおよびユーザを表示する権限、および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
- \* Active Directory \* : objectSid、primaryGroupID、userAccountControl、および `userPrincipalName`
- \* Azure \* : accountEnabled および userPrincipalName

- \* Password \* : ユーザ名に関連付けられたパスワード。



今後パスワードを変更する場合は、このページでパスワードを更新する必要があります。

- \* Group Base 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 では、ベース DN に対して相対的な識別名 ( DC=storagegrid、DC=example、DC=com など ) のグループをすべてフェデレーテッドグループとして使用できます。



\* グループの一意な名前 \* 値は、所属する \* グループベース DN \* 内で一意である必要があります。

- \* User Base DN \* : ユーザを検索する LDAP サブツリーの識別名 ( DN ) の完全パス。



\* ユーザーの一意な名前 \* 値は、それぞれが属する \* ユーザーベース DN \* 内で一意である必要があります。

- ユーザー名のバインド形式 ( 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がサインインできるようにするため、\* バインドユーザ名形式 \* を指定することを推奨します。

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
- 下位レベルの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

記載されているとおりに \* [username] \* を含めます。

## 6. Transport Layer Security (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 \* : STARTTLS を使用して LDAP サーバとの通信を保護します。Active Directory、OpenLDAP、またはその他のオプションですが、Azure ではこのオプションはサポートされていません。
- \* LDAPS を使用 \* : LDAPS (LDAP over SSL) オプションでは、TLS を使用して LDAP サーバへの接続を確立します。Azure ではこのオプションを選択する必要があります。
- \* TLS を使用しないでください \* : StorageGRID システムと LDAP サーバの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 サーバで LDAP 署名が適用される場合、[TLS を使用しない] オプションの使用はサポートされていません。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、接続の保護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 \* : 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 \* : 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。

接続をテストして設定を保存します

すべての値を入力したら、設定を保存する前に接続をテストする必要があります。StorageGRID では、LDAP サーバの接続設定とバインドユーザ名の形式が指定されている場合は検証されます。

手順

1. [接続のテスト \*] を選択します。
2. バインドユーザ名の形式を指定しなかった場合は、次の手順を実行します。
  - 接続設定が有効な場合は、「Test connection successful」というメッセージが表示されます。[保存 (Save)] を選択して、構成を保存します。
  - 接続設定が無効な場合は、「test connection could not be established」というメッセージが表示されます。[閉じる (Close)] を選択します。その後、問題を解決して接続を再度テストします。
3. バインドユーザ名の形式を指定した場合は、有効なフェデレーテッドユーザのユーザ名とパスワードを入力します。

たとえば、自分のユーザ名とパスワードを入力します。ユーザ名に特殊文字 (@、/ など) を使用しないでください。

### Test Connection ✕

To test the connection and the bind username format, enter the username and password of a federated user. For example, enter your own federated username and password. The test values are not saved.

**Test username**

The username of a federated user.

**Test password**

 👁

CancelTest Connection

- 接続設定が有効な場合は、「Test connection successful」というメッセージが表示されます。[保存 (Save)] を選択して、構成を保存します。
- 接続設定、バインドユーザ名形式、またはテストユーザ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。問題を解決してから、もう一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、アイデンティティソースからフェデレーテッドグループおよびユーザを定期的に同期します。ユーザの権限をすぐに有効にしたり制限したりする必要がある場合は、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「\*サーバーを同期」を選択します。

環境によっては、同期プロセスにしばらく時間がかかることがあります。



アイデンティティフェデレーション同期エラー \* アラートは、アイデンティティソースからフェデレーテッドグループとユーザを同期する問題がある場合にトリガーされます。

#### アイデンティティフェデレーションを無効にする

グループとユーザのアイデンティティ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を無効にすると、StorageGRID とアイデンティティソース間のやり取りは発生しません。ただし、設定は保持されるため、簡単に再度有効にすることができます。

#### このタスクについて

アイデンティティ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。

- フェデレーテッドユーザ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テッドユーザは、セッションが有効な間は StorageGRID システムに引き続きアクセスできますが、セッションが期限切れになると以降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はアラートやアラームが生成されません。
- 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、\*アイデンティティ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。アイデンティティフェデレーションを無効にするには、シングルサインオンページの SSO ステータスが \*無効\* になっている必要があります。を参照してください ["シングルサインオンを無効にします"](#)。

#### 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. [アイデンティティ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 サーバの設定に関するガイドライン

アイデンティティフェデレーションに OpenLDAP サーバを使用する場合は、OpenLDAP サーバで特定の設定が必要です。



ActiveDirectoryやAzure以外のアイデンティティソースの場合、StorageGRID は外部で無効にしたユーザへの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、そのユーザのS3キーをすべて削除するか、すべてのグループからユーザを削除します。

#### memberof オーバーレイと refint オーバーレイ

memberof オーバーレイと 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、[のリバースグループメンバーシップのメンテナンス手順を参照してください](#) ["OpenLDAP のドキュメント：バージョン 2.4 管理者ガイド"](#)。

#### インデックス作成

次の OpenLDAP 属性とインデックスキーワード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`

また、パフォーマンスを最適化するには、Username のヘルプで説明されているフィールドにインデックスを設定してください。

[のリバースグループメンバーシップのメンテナンスに関する情報を参照してください](#) ["OpenLDAP のドキュメント：バージョン 2.4 管理者ガイド"](#)。

### テナントグループを管理する

#### S3 テナント用のグループを作成します

S3 ユーザグループの権限を管理するには、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します。

作業を開始する前に

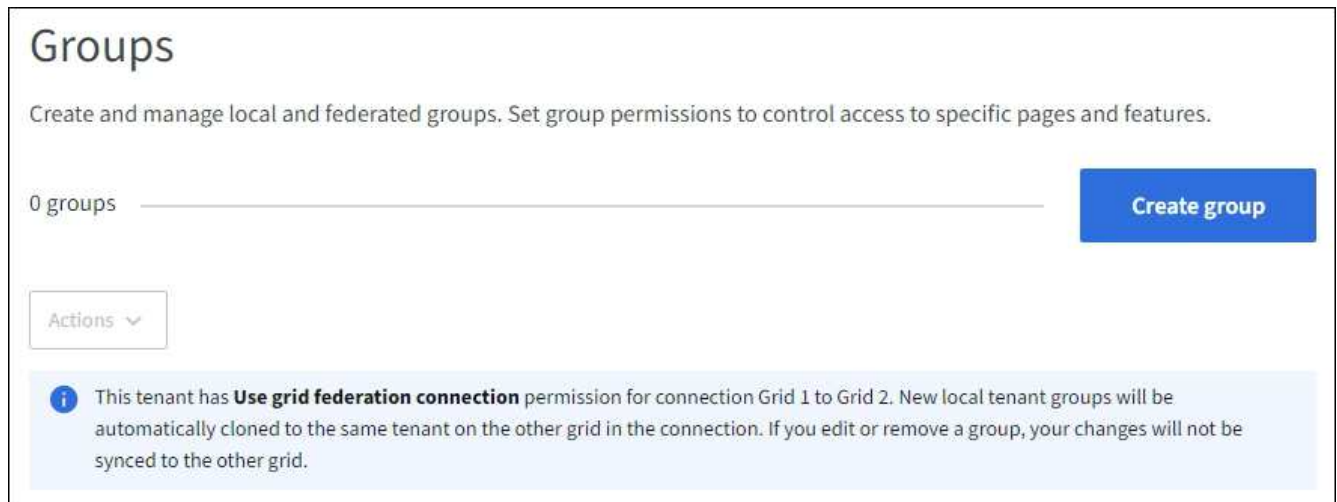
- Tenant Manager にはを使用してサインインします "サポートされている Web ブラウザ"。
- が設定されたユーザグループに属している必要があります "rootアクセス権限"。
- フェデレーテッドグループをインポートする場合は、を用意しておきます "アイデンティティフェデレーションが設定された"およびフェデレーテッドグループが設定済みのアイデンティティソースにすでに存在します。
- テナントアカウントに\* Use grid federation connection \*権限が割り当てられている場合は、のワークフローと考慮事項を確認しておきます "テナントグループおよびテナントユーザのクローニング"をクリックし、テナントのソースグリッドにサインインします。

グループ作成ウィザードにアクセスします

最初に、グループ作成ウィザードにアクセスします。

手順

1. \* access management \* > \* Groups \* を選択します。
2. テナントアカウントに「Use grid federation connection \*」権限がある場合は、このグリッドに作成された新しいグループが接続内の他のグリッドの同じテナントにクローニング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、テナントのデスティネーション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。

グループタイプを選択します

ローカルグループを作成するか、フェデレーテッドグループをインポートできます。

手順

1. [ローカルグループ\*] タブを選択してローカルグループを作成するか、または [フェデレーショングループ\*] タブを選択して、以前に設定したアイデンティティソースからグループをインポートします。

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は Tenant Manager にサインインできません。ただし、クライアントアプリケーションを使用して、グループの権限に基づいてテナントのリソースを管理することはできます。

## 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。表示名はあとで編集できます。



テナントアカウントで\* Use grid federation connection 権限が設定されている場合、デスティネーショングリッドにテナントに同じ unique name \*がすでに存在すると、クロージング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、に関連付けられている一意の名前です sAMAccountName 属性 (Attribute) : OpenLDAPの場合は、に関連付けられている一意の名前です uid 属性 (Attribute) :

## 3. 「\* Continue \*」を選択します。

### グループの権限を管理します

グループ権限は、ユーザがTenant Manager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、次のいずれかを選択します。

- \* Read-write \* (デフォルト) : ユーザはTenant Managerにサインインしてテナント設定を管理できません。
- \* 読み取り専用 \* : ユーザーは設定と機能のみを表示できます。Tenant Managerまたはテナント管理APIでは、変更を加えたり処理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は自分のパスワードを変更できます。



ユーザが複数のグループに属していて、いずれかのグループが読み取り専用設定されている場合、選択したすべての設定と機能に読み取り専用でアクセスできます。

#### 2. このグループの権限を1つ以上選択します。

を参照してください ["テナント管理権限"](#)。

#### 3. 「\* Continue \*」を選択します。

### S3グループポリシーを設定

グループポリシーによって、ユーザに付与する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アクセスがありません	デフォルト。バケットポリシーでアクセスが許可されていないかぎり、このグループのユーザは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 root ユーザにのみ S3 リソースへのアクセスが許可されます。

グループポリシー	説明
読み取り専用アクセス	このグループのユーザには、S3リソースへの読み取り専用アクセスが許可されます。たとえば、オブジェクトをリストして、オブジェクトデータ、メタデータ、タグを読み取ることができます。このオプションを選択すると、テキストボックスに読み取り専用グループポリシーの JSON 文字列が表示されます。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には、バケットを含むS3リソースへのフルアクセスが許可されます。このオプションを選択すると、テキストボックスにフルアクセスグループポリシーの JSON 文字列が表示されます。この文字列は編集できません。
ランサムウェアの軽減	この例では、このテナントのすべてのバケットを環境するポリシーを示します。このグループのユーザは共通の操作を実行できますが、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。  このグループポリシーは、* Manage all buckets *権限を持つTenant Managerユーザが上書きできます。[すべてのバケットを管理]権限を信頼できるユーザに制限し、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には、テキストボックスで指定した権限が付与されます。

- 「\* Custom \*」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は 5、120 バイトまでに制限されています。有効な JSON 形式の文字列を入力する必要があります。

言語の構文や例など、グループポリシーの詳細については、を参照してください "[グループポリシーの例](#)"。

- ローカルグループを作成する場合は、「\* Continue \*」を選択します。フェデレーテッドグループを作成する場合は、\* Create group \* および \* Finish \* を選択します。

#### ユーザの追加 (ローカルグループのみ)

ユーザを追加せずにグループを保存することも、必要に応じて既存のローカルユーザを追加することもできます。



テナントアカウントに\* Use grid federation connection \*権限がある場合、ソースグリッドでローカルグループを作成するときに選択したユーザは、グループをデスティネーショングリッドにクローニングするときに含まれません。このため、グループを作成するときにユーザを選択しないでください。代わりに、ユーザの作成時にグループを選択します。

#### 手順

- 必要に応じて、このグループに対して 1 人以上のローカルユーザを選択します。
- [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\* Use grid federation connection 権限があり、テナントのソースグリッドにアクセスしている場合、新しいグループはテナントのデスティネーショングリッドにクローニングされます。Success は、グループの詳細ページの**Overview**セクションに Cloning status \*として表示されます。

## Swift テナント用のグループを作成します

Swift テナントアカウントに対するアクセス権限を管理するには、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します。Swift テナントアカウントのコンテナとオブジェクトを管理するには、少なくとも 1 つのグループが Swift 管理者権限を持っている必要があります。



Swiftクライアントアプリケーションのサポートは廃止され、今後のリリースで削除される予定です。

作業を開始する前に

- Tenant Manager にはを使用してサインインします ["サポートされている Web ブラウザ"](#)。
- が設定されたユーザグループに属している必要があります ["rootアクセス権限"](#)。
- フェデレーテッドグループをインポートする場合は、を用意しておきます ["アイデンティティフェデレーションが設定された"](#)およびフェデレーテッドグループが設定済みのアイデンティティ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します

手順

最初に、グループ作成ウィザードにアクセスします。

1. \* access management \* > \* Groups \* を選択します。
2. 「\* グループを作成 \*」を選択します。

グループタイプを選択します

ローカルグループを作成するか、フェデレーテッドグループをインポートできます。

手順

1. [ローカルグループ\*] タブを選択してローカルグループを作成するか、または [フェデレーショングループ\*] タブを選択して、以前に設定したアイデンティティソースからグループをインポートします。

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は Tenant Manager にサインインできません。ただし、クライアントアプリケーションを使用して、グループの権限に基づいてテナントのリソースを管理することはできます。

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。表示名はあとで編集できます。
  - \* 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、に関連付けられている一意の名前です sAMAccountName 属性 (Attribute) : OpenLDAPの場合は、に関連付けられている一意の名前です uid 属性 (Attribute) :



3. 「\* Continue \*」を選択します。

グループの権限を管理します

グループ権限は、ユーザがTenant Manager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、次のいずれかを選択します。

- \* Read-write \* (デフォルト) : ユーザはTenant Managerにサインインしてテナント設定を管理できます。
- \* 読み取り専用 \* : ユーザーは設定と機能のみを表示できます。Tenant Managerまたはテナント管理APIでは、変更を加えたり処理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は自分のパスワードを変更できます。



ユーザが複数のグループに属していて、いずれかのグループが読み取り専用で設定されている場合、選択したすべての設定と機能に読み取り専用でアクセスできます。

2. グループユーザがTenant Managerまたはテナント管理APIにサインインする必要がある場合は、\* Root access \*チェックボックスを選択します。
3. 「\* Continue \*」を選択します。

**Swift**グループポリシーを設定します

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

1. グループユーザがSwift REST APIを使用してコンテナとオブジェクトを管理する必要がある場合は、\* Swift administrator \*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、「\* Continue \*」を選択します。フェデレーテッドグループを作成する場合は、\* Create group \* および \* Finish \* を選択します。

ユーザの追加 (ローカルグループのみ)

ユーザを追加せずにグループを保存することも、必要に応じて既存のローカルユーザを追加することもできます。

手順

1. 必要に応じて、このグループに対して1人以上のローカルユーザを選択します。

ローカルユーザをまだ作成していない場合は、[ユーザ]ページでこのグループをユーザに追加できます。  
を参照してください ["ローカルユーザを管理します"](#)。

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

い。テナント管理権限は、Tenant Manager またはテナント管理 API を使用してユーザが実行できるタスクを決定します。ユーザは 1 つ以上のグループに属することができます。権限は、ユーザが複数のグループに属している場合に累積されます。

Tenant Manager にサインインするには、またはテナント管理 API を使用するには、少なくとも 1 つの権限が割り当てられたグループにユーザが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は、次のタスクを実行できます。

- ダッシュボードを表示します
- 自分のパスワードを変更する（ローカルユーザの場合）

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、ユーザが設定を変更して処理を実行できるかどうか、またはユーザが関連する設定と機能のみを表示できるかどうかが決まります。



ユーザが複数のグループに属していて、いずれかのグループが読み取り専用設定されている場合、選択したすべての設定と機能に読み取り専用でアクセスできます。

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 テナントではグループの権限が異なるので注意してください。

アクセス権	説明	詳細
ルートアクセス	Tenant Manager とテナント管理 API へのフルアクセスを提供します。	Swift ユーザがテナントアカウントにサインインするには、Root Access 権限が必要です。
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 ユーザが Swift REST API を使用して処理を実行するには、Swift Administrator 権限が必要です。
自分の S3 クレデンシャルを管理します	ユーザに自分の S3 アクセスキーの作成および削除を許可します。	この権限がないユーザには、* storage (S3) > My S3 access keys * メニューオプションが表示されません。
すべてのバケットを表示	<ul style="list-style-type: none"> <li>• S3 テナント*：すべてのバケットとバケットの設定を表示できます。</li> <li>• Swift テナント*：Swift ユーザに、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設定を表示することを許可します。</li> </ul>	<p>View All Buckets 権限または Manage All Buckets 権限がないユーザには、* Buckets * メニューオプションは表示されません。</p> <p>この権限は、Manage All Buckets 権限よりも優先されます。S3 クライアントまたは S3 コンソールで使用される S3 バケットポリシーやグループポリシーには影響しません。</p> <p>この権限を Swift グループに割り当てるには、テナント管理 API を使用する必要があります。Tenant Manager 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。</p>

アクセス権	説明	詳細
すべてのバケットを管理	<ul style="list-style-type: none"> <li>• S3テナント*：S3のバケットまたはグループポリシーに関係なく、テナントマネージャとテナント管理APIを使用してS3バケットを作成および削除し、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することをユーザに許可します。</li> <li>• Swiftテナント*：Swiftユーザにテナント管理APIを使用してSwiftコンテナの整合性を制御することを許可します。</li> </ul>	<p>View All Buckets権限またはManage All Buckets権限がないユーザには、* Buckets *メニューオプションは表示されません。</p> <p>この権限は、View All Buckets権限よりも優先されます。S3クライアントまたはS3コンソールで使用されるS3バケットポリシーやグループポリシーには影響しません。</p> <p>この権限をSwiftグループに割り当てるには、テナント管理APIを使用する必要があります。Tenant Manager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。</p>
エンドポイントを管理します	ユーザに、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デスティネーションとして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または編集することを許可します。	この権限がないユーザーには、*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。
S3コンソールタブを使用	View All Buckets権限またはManage All Buckets権限と組み合わせると、ユーザはバケットの詳細ページにあるS3 Consoleタブでオブジェクトの表示と管理を行うことができます。	

## グループを管理します

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。

作業を開始する前に

- Tenant Manager にはを使用してサインインします "サポートされている Web ブラウザ"。
- が設定されたユーザグループに属している必要があります "rootアクセス権限"。


グループを表示または編集します

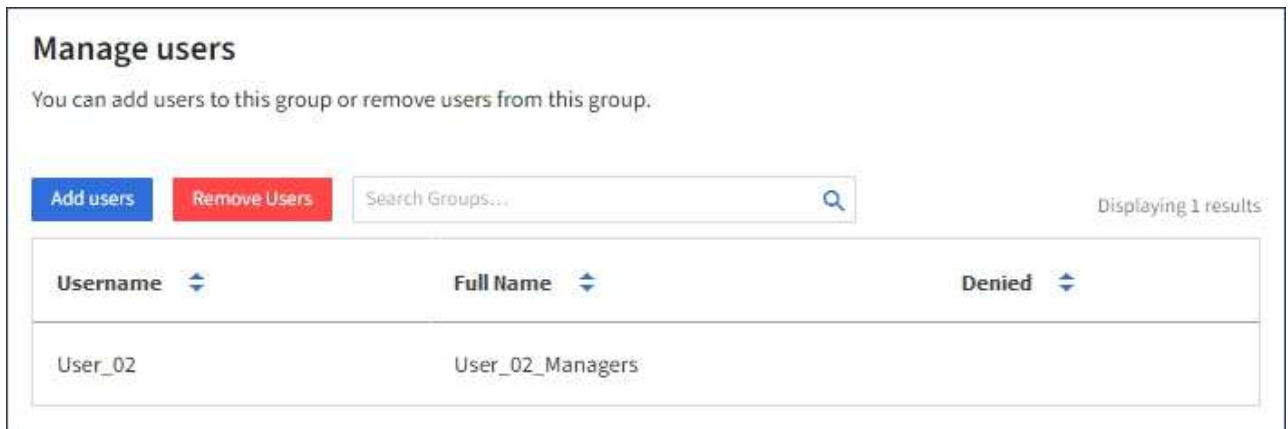
各グループの基本情報と詳細を表示および編集できます。

手順

1. \* access management \* > \* Groups \* を選択します。
2. [Groups]ページに表示される情報を確認します。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テッドグループの基本情報が表示されます。

テナントアカウントに\* Use grid federation connection \*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：

- バナーメッセージは、グループを編集または削除すると、変更内容が他のグリッドに同期されないことを示します。
  - 必要に応じて、デスティネーショングリッドでグループがテナントにクローニング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。可能です [グループクローンの再試行](#) 失敗した
3. グループの名前を変更する場合は、次の手順を実行します。
    - a. グループのチェックボックスをオンにします。
    - b. >[グループ名の編集]\*を選択します。
    - c. 新しい名前を入力します。
    - d. [変更を保存]\*を選択します
  4. 詳細を表示したり、追加の編集を行う場合は、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、[操作]>[グループの詳細を表示]\*を選択します。
  5. [Overview]セクションには、グループごとに次の情報が表示されます。
    - 表示名
    - 一意の名前
    - を入力します
    - アクセスモード
    - 権限
    - S3ポリシー
    - このグループのユーザ数
    - テナントアカウントに\* Use grid federation connection \*権限があり、テナントのソースグリッドでグループを表示している場合は、次のフィールドが追加されます。
      - クローニングステータス (\* Success または Failure \*)
      - このグループを編集または削除すると、変更内容が他のグリッドに同期されないことを示す青のバナーが表示されます。
  6. 必要に応じてグループ設定を編集します。を参照してください "[S3 テナント用のグループを作成します](#)" および "[Swift テナント用のグループを作成します](#)" を参照してください。
    - a. [Overview]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. [グループ権限]タブで権限を更新し、\*[変更の保存]\*を選択します。
    - c. タブで、変更を加えて[変更の保存]\*を選択します。
      - S3グループを編集する場合は、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グループを編集する場合は、必要に応じて\* Swift Administrator \*チェックボックスをオンまたはオフにします。
  7. 既存のローカルユーザをグループに追加するには、次の手順を実行します。
    - a. [Users]タブを選択します。



- b. [ユーザの追加]\*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を削除するには、次の手順を実行します
  - a. [Users]タブを選択します。
  - b. [ユーザの削除]\*を選択します。
  - c. 削除するユーザを選択し、\*[ユーザの削除]\*を選択します。

右上に成功メッセージが表示されます。

- 9. 変更した各セクションで[変更を保存]\*が選択されていることを確認します。

グループが重複しています

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\* Use grid federation connection \*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と、複製されたグループがテナントのデスティネーショングリッドにクローニングされます。

手順

1. \* access management \* > \* Groups \* 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オンにします。
3. [\* アクション \* > \* グループの複製 \* ] を選択します。
4. を参照してください ["S3 テナント用のグループを作成します"](#) または ["Swift テナント用のグループを作成します"](#) を参照してください。
5. 「\* グループを作成 \*」を選択します。

グループクローンの再試行

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\_ (Cloning failed) \_と表示されている各グループを選択します。

2. >[クローングループ]\*を選択します。
3. クローニングする各グループの詳細ページで、クローニング処理のステータスを確認します。

追加情報の場合は、を参照してください ["テナントグループとテナントユーザのクローンを作成します"](#)。

1つ以上のグループを削除します

1つ以上のグループを削除できます。削除したグループにのみ属しているユーザは、Tenant Manager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\* Use grid federation connection \*権限が割り当てられている場合にグループを削除すると、StorageGRID はもう一方のグリッド上の対応するグループを削除しません。この情報を同期する必要がある場合は、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. \* access management \* > \* Groups \* 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オンにします。
3. >[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。

確認のダイアログボックスが表示されます。

4. または[グループの削除]\*を選択します。

ローカルユーザを管理します

ローカルユーザを作成してローカルグループに割り当て、ユーザがアクセスできる機能を決定することができます。Tenant Managerには、「root」という名前の事前定義されたローカルユーザが1人含まれています。ローカルユーザは追加および削除できますが、rootユーザは削除できません。



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、ローカルユーザはクライアントアプリケーションを使用してグループ権限に基づいてテナントのリソースにアクセスできますが、Tenant Manager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。

作業を開始する前に

- Tenant Manager にはを使用してサインインします ["サポートされている Web ブラウザ"](#)。
- が設定されたユーザグループに属している必要があります ["rootアクセス権限"](#)。
- テナントアカウントに\* Use grid federation connection \*権限が割り当てられている場合は、のワークフローと考慮事項を確認しておきます ["テナントグループおよびテナントユーザのクローニング"](#)をクリックし、テナントのソースグリッドにサインインします。

ローカルユーザを作成します

ローカルユーザを作成して1つ以上のローカルグループに割り当て、ユーザのアクセス権限を制御することができます。

どのグループにも属していないS3ユーザには、管理権限やS3グループポリシーが適用されていません。これらのユーザは、バケットポリシーを通じて S3 バケットアクセスを許可されている場合があります。

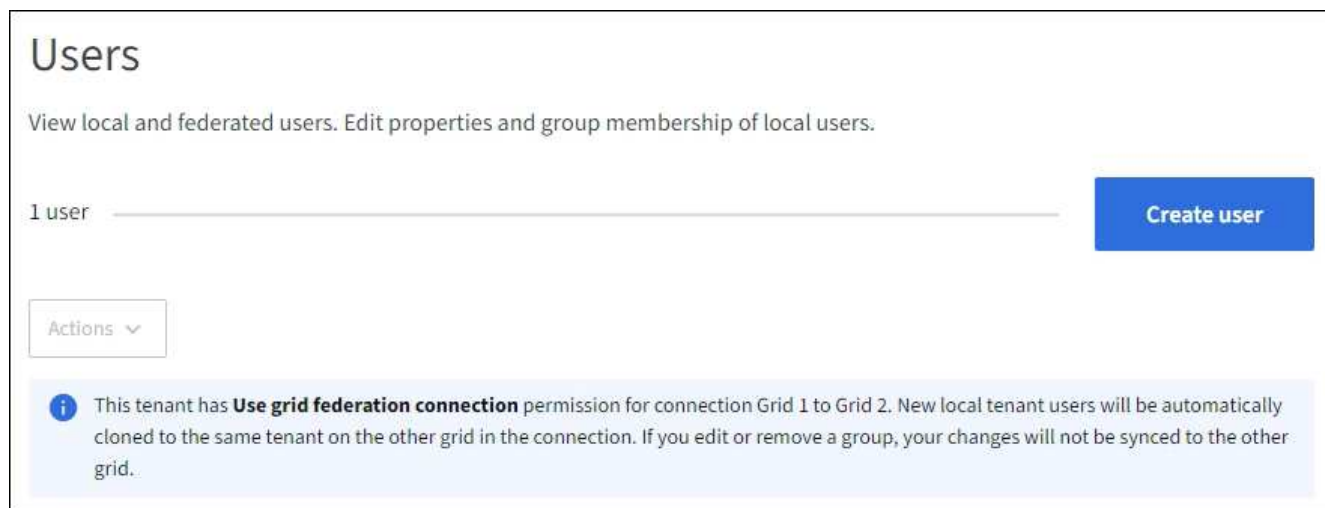
いずれのグループにも属していないSwiftユーザには、管理権限やSwiftコンテナへのアクセス権がありません。

Create userウィザードにアクセスします

手順

1. アクセス管理 \* > \* Users \* を選択します。

テナントアカウントで\* Use grid federation connection \*権限が割り当てられている場合は、青のバナーがテナントのソースグリッドであることを示します。このグリッドに作成したローカルユーザは、接続内の他のグリッドにクローニングされます。



2. 「\* ユーザーの作成 \*」を選択します。

資格情報を入力します

手順

1. [ユーザクレデンシャルの入力]\*ステップで、次のフィールドに値を入力します。

フィールド	説明
フルネーム	このユーザーのフルネーム（ユーザーの名と姓、アプリケーションの名前など）。
ユーザ名	このユーザがサインインに使用する名前。ユーザ名は一意である必要があり、変更できません。  注：テナントアカウントに* Use grid federation connection 権限が設定されている場合、デスティネーショングリッドにテナントに同じ Username *がすでに存在すると、クローニングエラーが発生します。
	ユーザがサインイン時に最初に使用するパスワード。

フィールド	説明
アクセスを拒否します	このユーザが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、*[はい]*を選択すると、ユーザーのサインイン機能が一時的に中断されます。

2. 「\* Continue \*」を選択します。

グループに割り当てます

手順

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

グループへのユーザの割り当ては任意です。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できます。

どのグループにも属していないユーザには、管理権限はありません。アクセス許可は累積的に追加されユーザには、自身が属しているすべてのグループに対するすべての権限が与えられます。を参照してください ["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\* Use grid federation connection 権限があり、テナントのソースグリッドにアクセスしている場合は、新しいローカルユーザがテナントのデスティネーショングリッドにクローニングされます。Success は、ユーザーの詳細ページの**Overview**セクションに Cloning status \*として表示されません。

3. [完了]\*を選択して[ユーザー]ページに戻ります。

ローカルユーザを表示または編集します

手順


1. アクセス管理 \* > \* Users \* を選択します。
2. [Users]ページに表示される情報を確認します。このテナントアカウントのすべてのローカルユーザとフェデレーテッドユーザの基本情報が表示されます。

テナントアカウントに\* Use grid federation connection \*権限があり、テナントのソースグリッドでユーザを表示している場合は、次の手順を実行します。

- バナーメッセージは、ユーザを編集または削除すると、変更内容が他のグリッドに同期されないことを示します。
- 必要に応じて、ユーザがデスティネーショングリッドのテナントにクローニングされていないかどうかを示すバナーメッセージが表示されます。可能です [失敗したユーザクローンを再試行します。](#)

3. ユーザのフルネームを変更する場合は、次の手順を実行します。
  - a. ユーザのチェックボックスを選択します。
  - b. >[フルネームの編集]\*を選択します。



- c. 新しい名前を入力します。
  - d. [変更を保存]\*を選択します
4. 詳細を表示したり、追加の編集を行う場合は、次のいずれかを実行します。
- ユーザ名を選択します。
  - ユーザのチェックボックスを選択し、[操作]>\*[ユーザの詳細を表示]\*を選択します。
5. [Overview]セクションには、ユーザごとに次の情報が表示されます。
- フルネーム
  - ユーザ名
  - ユーザタイプ
  - アクセスを拒否しました
  - 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\* Use grid federation connection \*権限があり、テナントのソースグリッドでユーザを表示している場合は、次のフィールドが追加されます。
    - クローニングステータス (\* Success または Failure \*)
    - このユーザを編集すると、変更内容が他のグリッドに同期されないことを示す青いバナーが表示されます。
6. 必要に応じてユーザー設定を編集します。を参照してください [ローカルユーザを作成します](#) を参照してください。
- a. [Overview]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 。  
  
ユーザー名は変更できません。
  - b. タブで、ユーザ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、[いいえ]を選択してユーザーがサインインできるようにするか、[はい]を選択してユーザーがサインインできないようにします。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、の手順に従います "[別のユーザのS3アクセスキーを作成しています](#)".
  - e. 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するか、ユーザーをグループから削除します。次に、\*変更を保存\*を選択します。
7. 変更した各セクションで[変更を保存]\*が選択されていることを確認します。

ローカルユーザが重複しています

ローカルユーザを複製して新しいユーザを迅速に作成することができます。



テナントアカウントに\* Use grid federation connection \*権限があり、テナントのソースグリッドからユーザを複製すると、複製されたユーザはテナントのデスティネーショングリッドにクローニングされます。

手順

1. アクセス管理 \* > \* Users \* を選択します。
2. 複製するユーザのチェックボックスをオンにします。
3. >[ユーザの複製]\*を選択します。
4. を参照してください [ローカルユーザを作成します](#) を参照してください。
5. 「 \* ユーザの作成 \* 」を選択します。

#### ユーザクローンの再試行

失敗したクローンを再試行するには：

1. ユーザ名の下に\_ (Cloning failed) \_と表示されている各ユーザを選択します。
2. >[ユーザのクローン]\*を選択します。
3. クローニングする各ユーザの詳細ページで、クローニング処理のステータスを確認します。

追加情報の場合は、を参照してください ["テナントグループとテナントユーザのクローンを作成します"](#)。

#### 1人以上のローカルユーザを削除します

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を完全に削除できます。



テナントアカウントに \* Use grid federation connection \* 権限が割り当てられている場合にローカルユーザを削除すると、StorageGRID はもう一方のグリッド上の対応するユーザを削除しません。この情報を同期する必要がある場合は、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。



フェデレーテッドユーザを削除するには、フェデレーテッドアイデンティティソースを使用する必要があります。

#### 手順

1. アクセス管理 \* > \* Users \* を選択します。
2. 削除する各ユーザのチェックボックスをオンにします。
3. >[ユーザの削除]または[操作]>[ユーザの削除]\*を選択します。

確認のダイアログボックスが表示されます。

4. または[ユーザの削除]\*を選択します。

## S3 アクセスキーを管理します

### S3アクセスキーの管理：概要

S3 テナントアカウントの各ユーザには、StorageGRID システムでオブジェクトの格納と読み出しを行うためのアクセスキーが必要です。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。

- Manage your own S3 credentials \*権限を持つユーザは、自分のS3アクセスキーを作成または削除できません。
- Root access \*権限を持つユーザは、S3 rootアカウントとその他すべてのユーザのアクセスキーを管理できます。root アクセスキーは、バケットポリシーで root アクセスキーが明示的に無効になっていないかぎり、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 では、署名バージョン 2 と署名バージョン 4 の認証がサポートされています。クロスアカウントアクセスは、バケットポリシーで明示的に有効になっていないかぎり、許可されません。

## 独自の S3 アクセスキーを作成します

S3 テナントを使用している場合は、適切な権限があれば、自分の 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。

作業を開始する前に

- Tenant Manager にはを使用してサインインします "サポートされている Web ブラウザ"。
- が設定されたユーザグループに属している必要があります "自分のS3クレデンシャルまたはRoot Access 権限を管理します"。

このタスクについて

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 S3 アクセスキーを 1 つ以上作成できます。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で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、使用していないキーを削除してください。キーが 1 つしかなく、有効期限が近づいている場合は、古いキーが期限切れになる前に新しいキーを作成してから、古いキーを削除します。

各キーには、特定の有効期限または有効期限を設定できません。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。短い有効期限を設定すると、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るリスクを低減できます。期限切れのキーは自動的に削除されます。
- 環境のセキュリティリスクが低く、新しいキーを定期的に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。あと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、Tenant Manager でアカウントに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する必要があります。定期的にアクセスキーをローテーションし、使用されていないキーはアカウントから削除します。また、他のユーザとはアクセスキーを共有しないでください。

手順

1. 「\* storage (S3) \* > \* My access keys \*」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。

- 有効期限を設定しない \* を選択して、有効期限が切れないキーを作成します。（デフォルト）
- [有効期限の設定 \*] を選択し、有効期限の日付と時刻を設定します。



有効期限は、現在の日付から最大5年間です。有効期限は、現在の時刻から少なくとも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。

Download access key（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、「\* Download.csv \*」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 \* Use grid federation connection \* 権限がある場合は、必要に応じてテナント管理APIを使用して、ソースグリッドのテナントからデスティネーショングリッドのテナントにS3アクセスキーを手動でクローニングします。を参照してください ["APIを使用してS3アクセスキーをクローニングします"](#)。

## S3 アクセスキーを表示します

S3テナントを使用していて、["適切な権限"](#)をクリックすると、S3アクセスキーのリストが表示されます。有効期限でリストをソートすると、まもなく期限切れになるキーを確認できます。必要に応じて、できます ["新しいキーを作成します"](#) または ["キーを削除します"](#) を使用していません。



アカウントに属する S3 バケットとオブジェクトには、Tenant Manager でアカウントに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する必要があります。定期的にアクセスキーをローテーションし、使用されていないキーはアカウントから削除します。また、他のユーザとはアクセスキーを共有しないでください。

作業を開始する前に

- Tenant Manager にはを使用してサインインします ["サポートされている Web ブラウザ"](#)。
- [Manage Your Own S3 credential]が設定されたユーザグループに属する必要があります ["アクセス権"](#)。

手順

1. 「\* storage (S3) \* > \* My access keys \*」を選択します。

2. [アクセスキー]ページで、既存のアクセスキーを\*または[アクセスキーID]\*でソートします。
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した場合は、アカウントのオブジェクトに一時的にアクセスできなくなることなく、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。

## 自分の **S3** アクセスキーを削除します

S3 テナントを使用している場合は、適切な権限があれば、自分の 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、テナントアカウント内のオブジェクトとバケットにそのアクセスキーでアクセスできなくなります。

作業を開始する前に

- Tenant Manager にはを使用してサインインします ["サポートされている Web ブラウザ"](#)。
- を使用することができます ["Manage Your Own S3 credentials"](#)。



アカウントに属する S3 バケットとオブジェクトには、Tenant Manager でアカウントに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する必要があります。定期的にアクセスキーをローテーションし、使用されていないキーはアカウントから削除します。また、他のユーザとはアクセスキーを共有しないでください。

手順

1. 「\* storage (S3) \* > \* My access keys \*」を選択します。
2. [My access keys]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 key (キーの削除) \*」を選択
4. 確認ダイアログボックスで、\* Delete key \*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。

## 別のユーザの **S3** アクセスキーを作成します

S3 テナントを使用している場合は、適切な権限があれば、バケットやオブジェクトにアクセスする必要があるアプリケーションなど、他のユーザの S3 アクセスキーを作成できます。

作業を開始する前に

- Tenant Manager にはを使用してサインインします ["サポートされている Web ブラウザ"](#)。
- が設定されたユーザグループに属している必要があります ["rootアクセス権限"](#)。

このタスクについて

他のユーザが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でア

アプリケーションを更新します。セキュリティを確保するため、ユーザが必要とする数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、有効期限が近づいている場合は、古いキーが期限切れになる前に新しいキーを作成してから、古いキーを削除します。

各キーには、特定の有効期限または有効期限を設定できません。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、ユーザのアクセスを一定期間に制限します。短い有効期限を設定すると、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るリスクを低減できます。期限切れのキーは自動的に削除されます。
- 環境のセキュリティリスクが低く、新しいキーを定期的に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。あと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。



ユーザに属する S3 バケットとオブジェクトには、Tenant Manager でそのユーザ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する必要があります。定期的にアクセスキーをローテーションし、使用されていないキーはアカウントから削除します。また、他のユーザとはアクセスキーを共有しないでください。

#### 手順

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

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）
  - [有効期限の設定 \*] を選択し、有効期限の日付と時刻を設定します。



有効期限は、現在の日付から最大5年間です。有効期限は、現在の時刻から少なくとも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。

Download access key（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、「\* Download.csv \*」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\* Use grid federation connection \*権限がある場合は、必要に応じてテナント管理APIを使用して、ソースグリッドのテナントからデスティネーショングリッドのテナントにS3アクセスキーを手動でクローニングします。を参照してください ["APIを使用してS3アクセスキーをクローニングします"](#)。

## 別のユーザの S3 アクセスキーを表示します

S3 テナントを使用している場合は、適切な権限があれば、別のユーザの S3 アクセスキーを表示できます。有効期限でリストをソートすると、まもなく期限切れになるキーを確認できます。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。

作業を開始する前に

- Tenant Manager にはを使用してサインインします ["サポートされている Web ブラウザ"](#)。
- を使用することができます ["rootアクセス権限"](#)。



ユーザに属する S3 バケットとオブジェクトには、Tenant Manager でそのユーザ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する必要があります。定期的なアクセスキーをローテーションし、使用されていないキーはアカウントから削除します。また、他のユーザとはアクセスキーを共有しないでください。

手順

1. アクセス管理 \* > \* Users \* を選択します。
2. [Users]ページで、表示するS3アクセスキーを所有するユーザを選択します。
3. [ユーザの詳細]ページで、\*[アクセスキー]\*を選択します。
4. キーを \* Expiration time \* または \* Access key ID \* でソートします。
5. 必要に応じて、新しいキーを作成し、使用し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した場合、ユーザはアカウントのオブジェクトに一時的にアクセスできなくなることなく、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

["別のユーザの S3 アクセスキーを作成します"](#)

["別のユーザの S3 アクセスキーを削除します"](#)

## 別のユーザの S3 アクセスキーを削除します

S3 テナントを使用している場合は、適切な権限があれば、別のユーザの 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、テナントアカウント内のオブジェクトとバケットにそのアクセスキーでアクセスできなくなります。

作業を開始する前に

- Tenant Manager にはを使用してサインインします ["サポートされている Web ブラウザ"](#)。
- を使用することができます ["rootアクセス権限"](#)。



ユーザに属する S3 バケットとオブジェクトには、Tenant Manager でそのユーザ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する必要があります。定期的にアクセスキーをローテーションし、使用されていないキーはアカウントから削除します。また、他のユーザとはアクセスキーを共有しないでください。

#### 手順

1. アクセス管理 \* > \* Users \* を選択します。
2. [Users]ページで、管理するS3アクセスキーを所有するユーザを選択します。
3. [User details]ページで、\*[Access Keys]\*を選択し、各アクセスキーのチェックボックスを選択します。を削除します。
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で、\* Delete key \*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 バケットを作成します。

Tenant Manager 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。

#### 作業を開始する前に

- Tenant Manager にはを使用してサインインします ["サポートされている Web ブラウザ"](#)。
- [Root access]または[Manage all buckets]が設定されたユーザグループに属している必要があります ["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の設定よりも優先されます。



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、で付与できます ["バケットポリシーまたはグループポリシー"](#)。

- バケットでS3オブジェクトロックを有効にする場合は、グリッド管理者がStorageGRID システムに対してグローバルな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のバケットとオブジェクトの要件を確認しておく必要があります。を参照してください ["S3オブジェクトロックを使用してオブジェクトを保持します"](#)。

#### ウィザードにアクセスします

#### 手順

1. ダッシュボードで\* View Buckets を選択するか、 storage (S3) > Buckets \*を選択します。
2. [\* バケットの作成 \*]を選択します。



## 詳細を入力します

### 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	<p>次のルールを満たすバケットの名前。</p> <ul style="list-style-type: none"><li>• StorageGRID システム全体で（テナントアカウント内だけでなく）一意である必要があります。</li><li>• DNS に準拠している必要があります。</li><li>• 3 文字以上 63 文字以下にする必要があります。</li><li>• 各ラベルの先頭と末尾の文字は小文字のアルファベットか数字にする必要があります、使用できる文字は小文字のアルファベット、数字、ハイフンのみです。</li><li>• 仮想ホスト形式の要求でピリオドを使用しないでください。ピリオドを使用すると、サーバワイルドカード証明書の検証で原因の問題が発生しません。</li></ul> <p>詳細については、を参照してください "<a href="#">バケットの命名規則に関する Amazon Web Services（AWS）のドキュメント</a>"。</p> <p>注：バケットの作成後にバケット名を変更することはできません。</p>
地域	<p>バケットのリージョン。</p> <p>StorageGRID 管理者が利用可能なリージョンを管理します。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する可能性があります。デフォルトでは、すべてのバケットがに作成されます us-east-1 リージョン：</p> <p>注：バケットの作成後にリージョンを変更することはできません。</p>

2. 「\* Continue \*」を選択します。

## オブジェクトの設定を管理します

### 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格納する場合は、オブジェクトのバージョン管理を有効にします。そのあと、必要に応じて以前のバージョンのオブジェクトを読み出すことができます。バケットをグリッド間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. S3オブジェクトロックのグローバル設定が有効になっている場合は、必要に応じて、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格納します。

バケットのS3オブジェクトロックは、一定の規制要件を満たすために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有効にしてください。S3オブジェクトロックは永続的な設定で、オブジェクトの削除や上書きを一定期間または無期限に防ぐことができます。



バケットでS3オブジェクトロックの設定を有効にしたあとに無効にすることはできません。このバケットには、適切な権限を持つユーザがオブジェクトを追加して変更できないようにすることができます。これらのオブジェクトやバケット自体を削除できない場合があります。

バケットで S3 オブジェクトの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、必要に応じてこのバケットに対して\*デフォルトの保持\*を有効にします。

default retention \*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が自動的に削除または上書きされなくなります。デフォルトの保持\*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. default retention が有効になっている場合は、バケットの default retention mode \*を指定します。

デフォルトの保持モード	説明
コンプライアンス	<ul style="list-style-type: none"><li>• retain-until-dateに達するまで、オブジェクトを削除できません。</li><li>• オブジェクトのretain-until-dateは増やすことはできますが、減らすことはできません。</li><li>• オブジェクトのretain-until-dateは、その日付に達するまで削除できません。</li></ul>
ガバナンス	<ul style="list-style-type: none"><li>• を使用するユーザ <code>s3:BypassGovernanceRetention</code> 権限はを使用できます <code>x-amz-bypass-governance-retention: true</code> 保持設定をバイパスする要求ヘッダー。</li><li>• これらのユーザは、retain-until-dateに達する前にオブジェクトバージョンを削除できます。</li><li>• これらのユーザは、オブジェクトのretain-until-dateを増減、または削除できます。</li></ul>

- b. default retention が有効になっている場合は、バケットの default retention period \*を指定します。

Default retention period \*は、このバケットに追加された新しいオブジェクトを取り込んだ時点から保持する期間です。1~36,500日、または1~100年の値を指定します。

4. [\* バケットの作成 \*]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。

5. 必要に応じて、\*[Go to bucket details page]\*を選択します "バケットの詳細を表示します" 追加の設定を実行します。

## バケットの詳細を表示します

テナントアカウント内のバケットを表示できます。

作業を開始する前に

- Tenant Manager にはを使用してサインインします "サポートされている Web ブラウザ"。
- が設定されたユーザグループに属している必要があります "rootアクセス、Manage All Buckets、View All Buckets権限"。これらの権限は、グループポリシーまたはバケットポリシーの権限設定よりも優先されません。

手順

1. ダッシュボードで\* View Buckets を選択するか、 storage (S3) > Buckets \*を選択します。

[Buckets]ページが表示されます。

2. 各バケットの概要情報を確認します。

必要に応じて、任意の列で情報をソートしたり、リストを前後にページ移動したりできます。



「オブジェクト数」と「使用済みスペース」の値が概算値として表示されます。これらの推定値は、取り込みのタイミング、ネットワーク接続、ノードのステータスによって左右されます。バケットでバージョン管理が有効になっている場合は、削除したオブジェクトのバージョンがオブジェクト数に含まれます。

列 ( Column )	説明
名前	バケットの一意の名前。変更することはできません。
有効な機能	バケットで有効になっている機能のリスト。
S3 オブジェクトのロック	バケットで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、古い準拠バケットの情報も表示されます。
地域	バケットのリージョン。変更できません。
オブジェクト数	このバケット内のオブジェクトの数。オブジェクトが追加または削除されたときに、この値がすぐに更新されないことがあります。バケットでバージョン管理が有効になっている場合は、最新でないオブジェクトバージョンがこの値に含まれます。
使用済みスペース	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、レプリケートコピーやイレイジャーコーディングコピー、また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ていません。
作成日	バケットが作成された日時。

3. 特定のバケットの詳細を表示するには、テーブルで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。必要な権限があれば、このページで次のタスクを実行できます。

- バケットオプションを設定および管理します。
  - ["ILMポリシータグ"](#)
  - ["バケットの整合性の管理"](#)
  - ["最終アクセス時間の更新"](#)
  - ["オブジェクトのバージョン管理"](#)
  - ["S3 オブジェクトのロック"](#)
  - ["デフォルトのバケット保持"](#)
- バケットアクセスを設定します（など） ["Cross-Origin Resource Sharing \(CORS\) "](#)
- ["プラットフォームサービスを管理します"](#)（テナントで許可されている場合）CloudMirrorレプリケーション、イベント通知、検索統合など
- とを有効にします ["グリッド間レプリケーションを管理します"](#)（テナントで許可されている場合）このバケットに取り込まれたオブジェクトを別のStorageGRID システムにレプリケートする
- にアクセスします ["S3コンソール"](#) をクリックしてバケット内のオブジェクトを管理します
- ["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"](#) それはすでに空です

## ILMポリシータグをバケットに適用する

オブジェクトストレージ要件に基づいて、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の格納場所と一定期間後に削除するかどうかを制御します。グリッド管理者は、複数のアクティブポリシーを使用している場合に、ILMポリシーを作成して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は頻繁に再割り当てしないでください。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

作業を開始する前に

- Tenant Manager にはを使用してサインインします ["サポートされている Web ブラウザ"](#)。
- が設定されたユーザグループに属している必要があります ["rootアクセス、Manage All Buckets、View All Buckets権限"](#)。これらの権限は、グループポリシーまたはバケットポリシーの権限設定よりも優先されません。

手順

1. ダッシュボードで\* View Buckets を選択するか、storage (S3) > Buckets \*を選択します。

[Buckets]ページが表示されます。必要に応じて、任意の列で情報をソートしたり、リストを前後にページ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に対するILMポリシータグの割り当てを変更することもできます。



「オブジェクト数」と「使用済みスペース」の値が概算値として表示されます。これらの推定値は、取り込みのタイミング、ネットワーク接続、ノードのステータスによって左右されます。バケットでバージョン管理が有効になっている場合は、削除したオブジェクトのバージョンがオブジェクト数に含まれます。

3. [Bucket options]タブで、ILMポリシータグの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. 各ポリシータグの概要を読んで、バケットに適用するタグを特定します。



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による再評価がトリガーされます。新しいポリシーで一定期間オブジェクトが保持されると、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。バケットにキーを使用して新しいS3バケットタグが設定される `NTAP-SG-ILM-BUCKET-TAG` および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てください。バケットに新しいTagSetを適用するときは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ポリシーに照らして評価されます。



ILMポリシータグの設定と変更には、ILMポリシータグが検証されるTenant Manager APIまたはTenant Manager APIのみを使用します。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ている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る間、一時的にパフォーマンスに影響します。

## バケットの整合性の管理

整合性の値を使用して、バケット設定を変更できるかどうかを指定したり、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やサイト間でのオブジェクトの整合性のバランスを調整したりできます。クライアントアプリケーションの運用上のニーズを満たすために、整合性の値をデフォルト値とは異なる値に変更することができます。

作業を開始する前に

- Tenant Manager にはを使用してサインインします ["サポートされている Web ブラウザ"](#)。
- が設定されたユーザグループに属している必要があります ["すべてのバケットまたはRoot Access権限を管理します"](#)。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の設定よりも優先されます。

## バケットの整合性に関するガイドライン

バケットの整合性は、そのS3バケット内のオブジェクトに影響しているクライアントアプリケーションの整合性を判断するために使用されます。一般に、バケットには\* Read-after-new-write \*整合性を使用する必要があります。

### バケット整合性の変更

Read-after-new-write \*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 ヘッダー。。Consistency-Control ヘッダーはバケットの整合性よりも優先されます。



バケットの整合性を変更した場合、変更後に取り込まれたオブジェクトのみが変更後の設定を満たすことが保証されます。

### 手順

1. ダッシュボードで\* View Buckets を選択するか、storage (S3) > Buckets \*を選択します。
2. 表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. [Bucket options]タブで、[\*\*]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処理の整合性を選択します。
  - **all**:最高レベルの一貫性を提供します。すべてのノードが即座にデータを受け取り、受け取れない場合は要求が失敗します。
  - \* strong-global \* :すべてのサイトのすべてのクライアント要求について、リードアフターライト整合性が保証されます。
  - \*strong-site \* : サイト内のすべてのクライアント要求に対してリードアフターライト整合性が保証されます。
  - \* Read-after-new-write \* (デフォルト) :新規オブジェクトにはリードアフターライト整合性を提供し、オブジェクトの更新には結果整合性を提供します。高可用性が確保され、データ保護が保証されます。ほとんどの場合に推奨されます。
  - \* available \* :新しいオブジェクトとオブジェクトの更新の両方について、結果整合性を提供します。S3バケットの場合は、必要な場合にのみ使用します（読み取り頻度の低いログ値を含むバケットや、存在しないキーに対するHEAD処理やGET処理など）。S3 FabricPool バケットではサポートされません。
5. 「変更を保存」を選択します。

### バケット設定を変更した場合の動作

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\* Strong \* consistencyが使用されます。どのサイトでも複数のストレージノードを使用できない場合やサイトを使用できない場合は、それらの設定を変更できない可能性があります。

- ["バックグラウンドでの空のバケット削除"](#)

- "最終アクセス時間"
- "バケットライフサイクル"
- "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 オブジェクトのロック"
- "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、およびバケット暗号化の整合性の値を強くし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整合性が強くなく、変更の可用性も高くなります。これらの設定の変更が反映されるまでに時間がかかることがあります。

- "プラットフォームサービスの設定：通知、レプリケーション、検索の統合"
- "CORS設定"
- [バケットの整合性を変更](#)



バケット設定の変更時に使用したデフォルト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、Consistency-Controlのヘッダー **"S3 REST API"** または、`reducedConsistency` または `force` のオプションを指定します **"テナント管理 API"**。

## 最終アクセス日時の更新を有効または無効にします

グリッド管理者が StorageGRID システムの情報ライフサイクル管理 (ILM) ルールを作成する際に、オブジェクトを別の格納場所に移動するかどうかを決定する際にオブジェクトの最終アクセス日時を使用するように指定できます。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に対して最終アクセス日時の更新を有効にすることで、このようなルールを活用できます。

以下の手順は、[最終アクセス時間]\*オプションを高度なフィルタまたは参照時間として使用するILMルールを少なくとも1つ含むStorageGRID システムにのみ該当します。StorageGRID システムにこのようなルールが含まれていない場合は、この手順を無視してかまいません。を参照してください ["ILMルールで最終アクセス時間を使用"](#) を参照してください。

作業を開始する前に

- Tenant Manager にはを使用してサインインします ["サポートされている Web ブラウザ"](#)。
- が設定されたユーザグループに属している必要があります ["すべてのバケットまたはRoot Access権限を管理します"](#)。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の設定よりも優先されます。

このタスクについて

最終アクセス時間\*は、ILMルールの Reference time \*配置手順で使用できるオプションの1つです。ルールの[Reference time]を[Last access time]に設定すると、オブジェクトが最後に読み出された（読み取りまたは表示された）日時に基づいてオブジェクトを特定の格納場所に配置するようにグリッド管理者が指定できます。

たとえば、最近表示したオブジェクトを高速ストレージに保持するには、次のように指定した ILM ルールを作成できます。

- 過去 1 カ月間に読み出されたオブジェクトは、ローカルストレージノードに保持する。
- 過去 1 カ月間に読み出されなかったオブジェクトは、オフサイトの場所に移動する。

デフォルトでは、最終アクセス時間の更新は無効です。StorageGRID システムに\*最終アクセス時間\*オプションを使用する ILM ルールが含まれている場合に、このバケット内のオブジェクトにこのオプションを適用するには、そのルールで指定された S3 バケットに対して最終アクセス時間の更新を有効にする必要があります。



オブジェクトが読み出されるときに最終アクセス日時を更新すると、特に小さなオブジェクトについては StorageGRID のパフォーマンスが低下する可能性があります。

最終アクセス時間の更新では、オブジェクトが読み出されるたびに StorageGRID で以下の追加手順が実行されるため、パフォーマンスが低下します。

- 新しいタイムスタンプでオブジェクトを更新します
- 現在の ILM ルールとポリシーに照らしてオブジェクトが再評価されるように、ILM キューにオブジェクトを追加します

次の表に、最終アクセス時間が有効または無効な場合の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ます。

要求のタイプ	最終アクセス時間が無効な場合の動作（デフォルト）		最終アクセス時間が有効な場合の動作	
	最終アクセス時間の更新	ILM 評価キューへのオブジェクトの追加	最終アクセス時間の更新	ILM 評価キューへのオブジェクトの追加
オブジェクト、そのアクセス制御リスト、またはメタデータの読み出し要求	いいえ	いいえ	はい。	はい。
オブジェクトメタデータの更新要求	はい。	はい。	はい。	はい。
バケット間でのオブジェクトのコピー要求	<ul style="list-style-type: none"> <li>• ソースコピーに対しては、「いいえ」と指定します</li> <li>• デスティネーションコピーについては、はい</li> </ul>	<ul style="list-style-type: none"> <li>• ソースコピーに対しては、「いいえ」と指定します</li> <li>• デスティネーションコピーについては、はい</li> </ul>	<ul style="list-style-type: none"> <li>• ソースコピーについては、はい</li> <li>• デスティネーションコピーについては、はい</li> </ul>	<ul style="list-style-type: none"> <li>• ソースコピーについては、はい</li> <li>• デスティネーションコピーについては、はい</li> </ul>



マルチパートアップロードの完了要求	はい、アセンブルされたオブジェクトの場合	はい、アセンブルされたオブジェクトの場合	はい、アセンブルされたオブジェクトの場合	はい、アセンブルされたオブジェクトの場合
-------------------	----------------------	----------------------	----------------------	----------------------

#### 手順

1. ダッシュボードで\* View Buckets を選択するか、 storage (S3) > Buckets \*を選択します。
2. 表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. [Bucket options]タブで、[Last access time updates]\*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。

作業を開始する前に

- Tenant Manager にはを使用してサインインします "[サポートされている Web ブラウザ](#)".
- が設定されたユーザグループに属している必要があります "[すべてのバケットまたはRoot Access権限を管理します](#)". 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の設定よりも優先されます。
- すべてのストレージノードが使用可能です。

このタスクについて

バケットでオブジェクトのバージョン管理を有効または一時停止することができます。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ることはできません。ただし、バケットのバージョン管理は一時停止できます。

- 無効：バージョン管理は一度も有効になっていません
- 有効：バージョン管理が有効になっています
- 中断：バージョン管理は以前有効になっていて、中断されています

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. ダッシュボードで\* View Buckets を選択するか、 storage (S3) > Buckets \*を選択します。
2. 表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. タブで、[Object versioning]\*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の状態を選択します。

グリッド間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 オブジェクトのロックまたはレガシーの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格納する場合は、オブジェクトのバージョン管理を有効にします。そのあと、必要に応じて以前のバージョンのオブジェクトを読み出すことができます。  バケットにすでに含まれていたオブジェクトは、ユーザによる変更時にバージョン管理されます。
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しない場合は、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は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します

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。

#### S3 オブジェクトのロックとは何ですか？

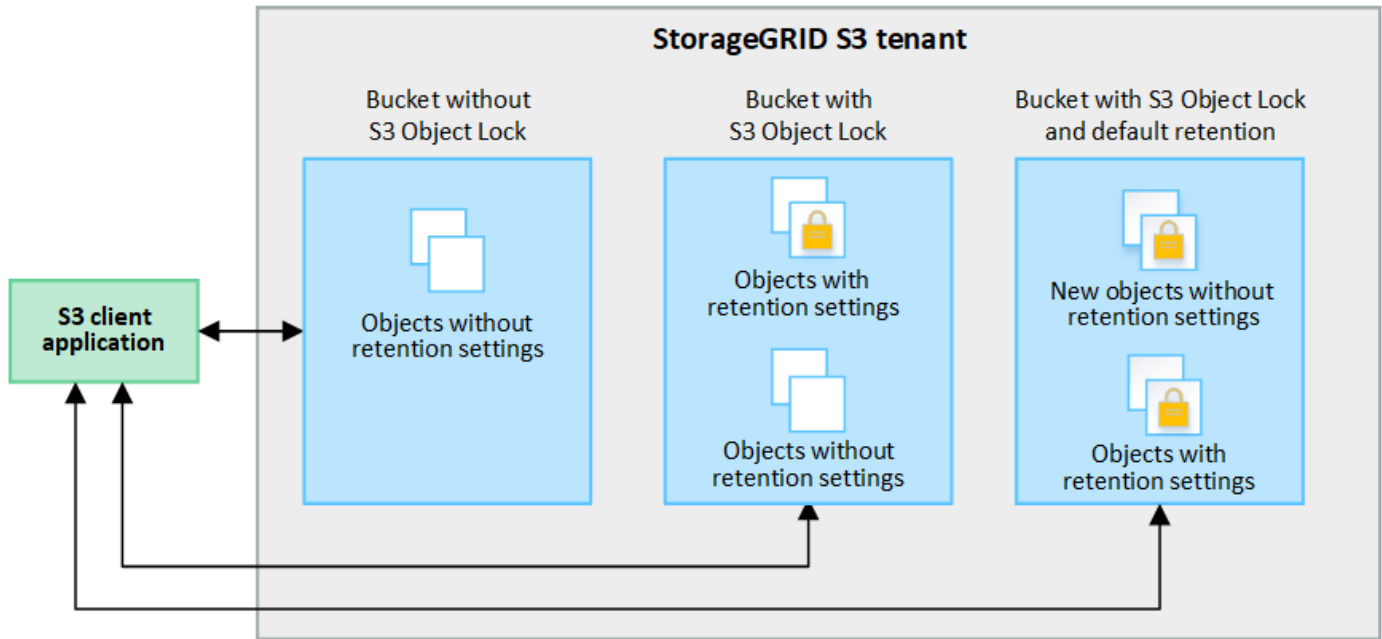
StorageGRID S3 オブジェクトロック機能は、Amazon Simple Storage Service（Amazon S3）での S3 オブジェクトロックに相当するオブジェクト保護解決策です。

図に示すように、StorageGRID システムでグローバルな S3 オブジェクトの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では、S3 オブジェクトのロックを有効にし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であり、自動的に有効になります。

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、S3クライアントアプリケーションは、そのバケットに保存されているすべてのオブジェクトバージョンの保持設定をオプションで指定できます。

また、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、オプションでデフォルトの保持モードと保持期間を設定できます。デフォルトの設定は、独自の保持設定がない状態でバケットに追加されたオブジェクトにのみ適用されます。

## StorageGRID with S3 Object Lock setting enabled



### 保持モード

StorageGRID S3オブジェクトロック機能は、2つの保持モードをサポートしており、さまざまなレベルの保護をオブジェクトに適用できます。これらのモードは、Amazon S3の保持モードに相当します。

- コンプライアンスモードの場合：
  - retain-until-dateに達するまで、オブジェクトを削除できません。
  - オブジェクトのretain-until-dateは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retain-until-date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は、要求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。
  - これらのユーザは、retain-until-dateに達する前にオブジェクトバージョンを削除できます。
  - これらのユーザは、オブジェクトのretain-until-date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各オブジェクトに次の保持設定を必要に応じて指定できます。

- 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。
- \* Retain-until-date \*：オブジェクトバージョンのretain-until-dateが将来の日付の場合、オブジェクトは読み出すことはできますが、削除することはできません。
- \* リーガルホールド \*：オブジェクトバージョンにリーガルホールドを適用すると、そのオブジェクトがただちにロックされます。たとえば、調査または法的紛争に関連するオブジェクトにリーガルホールドを設定する必要がある場合があります。リーガルホールドには有効期限はありませんが、明示的に削除されるまで保持されます。リーガルホールドは、それまでの保持期間とは関係ありません。



オブジェクトがリーガルホールドの対象である場合、保持モードに関係なく、誰もオブジェクトを削除できません。

オブジェクト設定の詳細については、[を参照してください "S3 REST APIを使用してS3オブジェクトロックを設定します"](#)。

#### 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した場合は、必要に応じて次のバケット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、独自の保持設定が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には影響しません。

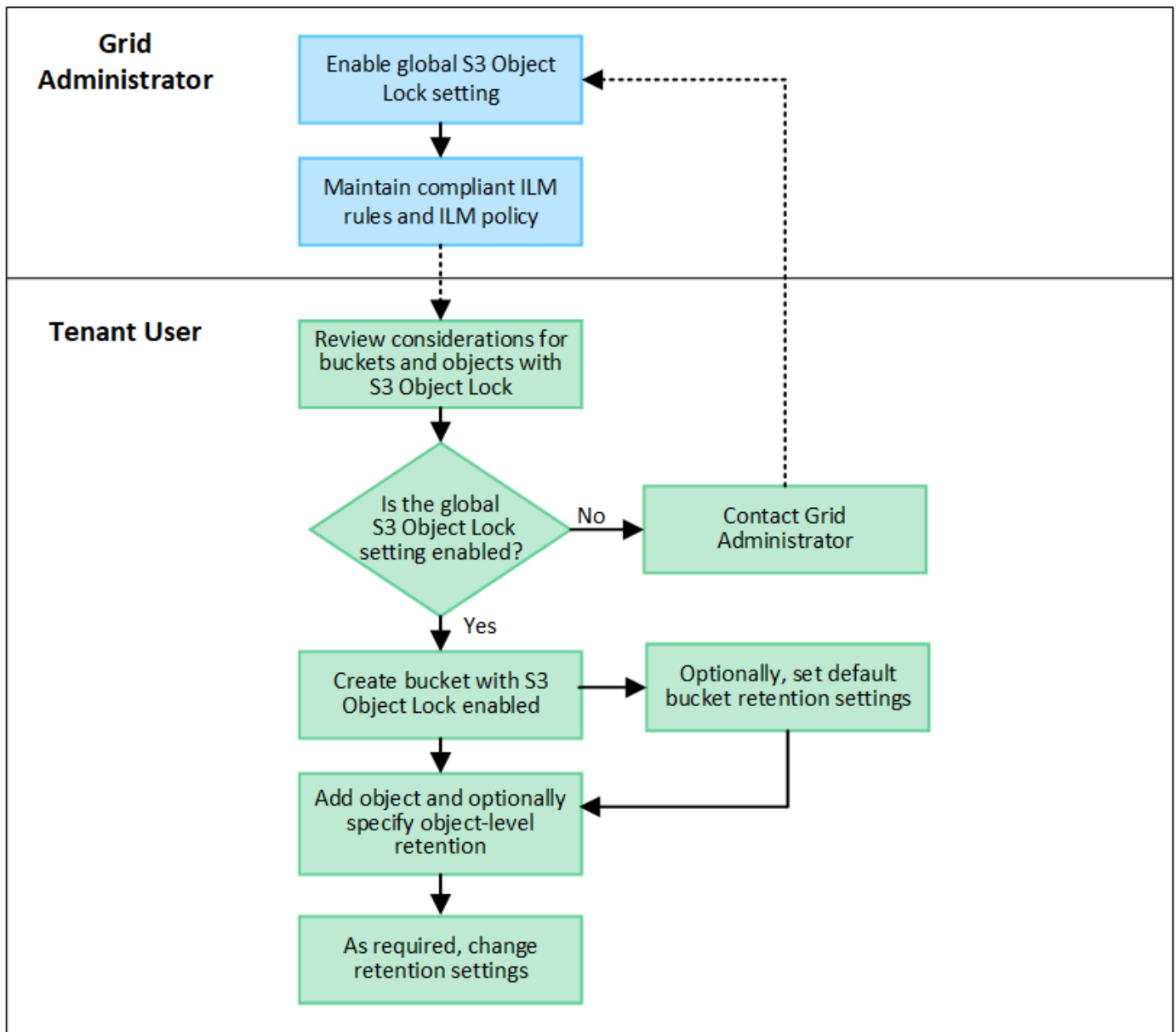
[を参照してください "S3 バケットを作成します。"](#) および ["S3オブジェクトロックのデフォルトの保持期間を更新します"](#)。

#### S3 オブジェクトロックのワークフロー

次のワークフロー図は、StorageGRID で S3 オブジェクトロック機能を使用する場合の大まかな手順を示しています。

S3 オブジェクトのロックを有効にしてバケットを作成する前に、グリッド管理者が StorageGRID システム全体に対してグローバルな S3 オブジェクトのロック設定を有効にする必要があります。グリッド管理者は、情報ライフサイクル管理 (ILM) ポリシーが「準拠」であることを確認し、S3オブジェクトロックが有効なバケットの要件を満たしている必要もあります。詳細については、グリッド管理者に問い合わせるか、[の手順を参照してください "S3オブジェクトロックを使用してオブジェクトを管理します"](#)。

S3オブジェクトロックのグローバル設定を有効にしたら、S3オブジェクトロックを有効にしてバケットを作成し、必要に応じて各バケットにデフォルトの保持設定を指定できます。また、S3クライアントアプリケーションを使用して、必要に応じて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。



### S3 オブジェクトのロックを有効にした場合のバケットの要件

- StorageGRID システムでグローバルな 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を有効にしたバケットを作成できます。
- S3 オブジェクトのロックを使用する場合は、バケットの作成時に S3 オブジェクトのロックを有効にする必要があります。既存のバケットで S3 オブジェクトロックを有効にすることはできません。
- バケットで S3 オブジェクトのロックが有効になっている場合は、そのバケットのバージョン管理が StorageGRID で自動的に有効になります。バケットの S3 オブジェクトロックを無効にしたり、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。
- 必要に応じて、Tenant Manager、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新しいオブジェクトのうち、独自の保持設定がな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は、アップロード時にオブジェクトバージョンごとに保持モードと retain-until-date を指定することで上書きできます。

- バケットライフサイクル設定は、S3オブジェクトロックが有効なバケットでサポートされます。
- CloudMirror レプリケーションは、S3 オブジェクトロックが有効になっているバケットではサポートされません。

### S3 オブジェクトの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します。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。
- 保持設定はオブジェクトのバージョンごとに適用されます。オブジェクトバージョンには、retain-until-date 設定とリーガルホールド設定の両方を設定できます。ただし、オブジェクトバージョンを保持することはできません。また、どちらも保持することはできません。オブジェクトの retain-until-date 設定またはリーガルホールド設定を指定すると、要求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 オブジェクトのロックが有効な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なバケットに保存された各オブジェクトは、次の段階を経ます。

#### 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を追加すると、保持設定は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が適用されます（存在する場合）。
- 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ている場合は、オブジェクトとS3ユーザ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

指定した保持期間中、各保護オブジェクトの複数のコピーがStorageGRID によって格納されます。オブジェクトコピーの正確な数、タイプ、格納場所は、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。retain-until-dateに達する前に保護オブジェクトを削除できるかどうかは、保持モードによって異なります。

- オブジェクトがリーガルホールドの対象である場合、保持モードに関係なく、誰もオブジェクトを削除できません。

従来の準拠バケットは引き続き管理できますか。

S3 オブジェクトロック機能は、以前のバージョンの StorageGRID で使用されていた準拠機能に代わる機能です。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は、引き続きこれらのバケットの設定を管理できますが、新しい準拠バケットは作成できなくなります。手順については、を参照してください ["ネットアップのナレッジベース： 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の保持期間を更新します

バケットの作成時にS3 Object Lock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せん。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。

作業を開始する前に

- Tenant Manager にはを使用してサインインします ["サポートされている Web ブラウザ"](#)。
- が設定されたユーザグループに属している必要があります ["すべてのバケットまたはRoot Access権限を管理します"](#)。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の設定よりも優先されます。
- 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り、バケットの作成時に有効にしました。を参照してください ["S3オブジェクトロックを使用してオブジェクトを保持します"](#)。

手順

1. ダッシュボードで\* View Buckets を選択するか、 storage (S3) > Buckets \*を選択します。
2. 表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. [Bucket options]タブで、[S3 Object Lock]\*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\*を有効または無効にします。

この設定の変更は、バケットにすでに含まれているオブジェクトや、保持期間が独自に設定されている可能性のあるオブジェクトには適用されません。

5. default retention が有効になっている場合は、バケットの default retention mode \*を指定します。

デフォルトの保持モード	説明
コンプライアンス	<ul style="list-style-type: none"><li>• retain-until-dateに達するまで、オブジェクトを削除できません。</li><li>• オブジェクトのretain-until-dateは増やすことはできますが、減らすことはできません。</li><li>• オブジェクトのretain-until-dateは、その日付に達するまで削除できません。</li></ul>
ガバナンス	<ul style="list-style-type: none"><li>• を使用するユーザ <code>s3:BypassGovernanceRetention</code> 権限は使用できます <code>x-amz-bypass-governance-retention: true</code> 保持設定をバイパスする要求ヘッダー。</li><li>• これらのユーザは、retain-until-dateに達する前にオブジェクトバージョンを削除できます。</li><li>• これらのユーザは、オブジェクトのretain-until-dateを増減、または削除できます。</li></ul>

6. default retention が有効になっている場合は、バケットの default retention period \*を指定します。

Default retention period \*は、このバケットに追加された新しいオブジェクトを取り込んだ時点から保持す

る期間です。1~36,500日、または1~100年の値を指定します。

7. 「変更を保存」を選択します。

## Cross-Origin Resource Sharing ( CORS ) の設定

S3バケットとバケット内のオブジェクトに他のドメインにあるWebアプリケーションからアクセスできるようにするには、そのバケットにCross-Origin Resource Sharing (CORS) を設定します。

作業を開始する前に

- Tenant Manager にはを使用してサインインします "サポートされている Web ブラウザ"。
- が設定されたユーザグループに属している必要があります "すべてのバケットまたはRoot Access権限を管理します"。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の設定よりも優先されます。

このタスクについて

Cross-Origin Resource Sharing ( CORS ) は、あるドメインのクライアント Web アプリケーションが別のドメインのリソースにアクセスできるようにするセキュリティ機能です。たとえば、というS3バケットを使用するとします Images グラフィックを保存します。のCORSを設定する Images バケットを使用すると、そのバケット内の画像をWebサイトに表示できます <http://www.example.com>。

バケットの**CORS**を有効にします

手順

1. テキストエディタを使用して、必要なXMLを作成します。

次の例は、 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。このXMLでは、すべてのドメインにバケットへのGET要求の送信が許可されていますが、にしか許可されていません <http://www.example.com> POST要求と削除要求を送信するドメイン。要求ヘッダーはすべて許可されます。

```
<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 設定 XML の詳細については、を参照してください "[Amazon Web Services \(AWS\) ドキュメント](#) : 「[Amazon Simple Storage Service Developer Guide](#)」。

2. ダッシュボードで\* View Buckets を選択するか、 storage (S3) > Buckets \*を選択します。
3. 表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. [Bucket access]タブで、[Cross-Origin Resource Sharing (CORS) ]\*アコーディオンを選択します。
5. [Enable CORS]チェックボックスをオンにします。
6. CORS設定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設定を変更します

#### 手順

1. テキストボックスのCORS設定XMLを更新するか、\* Clear \*を選択してやり直します。
2. 「変更を保存」を選択します。

### CORS設定を無効にします

#### 手順

1. [Enable CORS]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

Tenant Manager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StorageGRID システム内のすべてのノードとサイトから、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。
- オブジェクト、オブジェクトコピー、および同時処理の数によっては、バケット内のすべてのオブジェクトの削除に数分、数日、場合によっては数週間かかることがあります。
- バケットにがある場合 "[S3オブジェクトロックが有効になりました](#)"の場合は、\_年\_の間、\* Deleting objects : read-only \*状態のままになることがあります。



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てリーガルホールドが解除されるまで、\* Deleting objects : read-only \*状態のままです。

- オブジェクトの削除中、バケットの状態は\* Deleting objects : read-only \*です。この状態の場合、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
  - バケットを削除します
  - バケット名はあとで使用できるように、読み取り専用モードのままにしておきます
- 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は、StorageGRID 11.8以降で作成された削除マーカを削除するには、[Delete objects in bucket]処理を使用します。
- 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 11.7以前で作成された削除マーカは削除されません。バケット内のオブジェクトの削除に関する情報を参照：["S3 バージョン管理オブジェクトの削除方法"](#)。
- を使用する場合 ["グリッド間レプリケーション"](#) 次の点に注意してください。
  - このオプションを使用しても、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すると、もう一方のグリッドのデスティネーションバケットにオブジェクトを追加すると \* Cross-grid replication failure \* 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オブジェクトが追加されないことを保証できない場合は、["グリッド間レプリケーションを無効にします"](#) をクリックしてから、すべてのバケットオブジェクトを削除してください。

#### 作業を開始する前に

- Tenant Manager にはを使用してサインインします ["サポートされている Web ブラウザ"](#)。
- が設定されたユーザグループに属している必要があります ["rootアクセス権限"](#)。この権限は、グループポリシーまたはバケットポリシーの権限設定よりも優先されます。

#### 手順

1. ダッシュボードで \* View Buckets を選択するか、storage (S3) > Buckets \* 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. 特定のバケットの\*[Actions]\*メニューまたは詳細ページを使用します。

##### [アクション]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. >[Delete objects in bucket]\*を選択します。

##### 詳細ページ

- a. 詳細を表示するバケット名を選択します。
- b. [Delete objects in bucket]\*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、\* Yes と入力して OK \*を選択します。
4. 削除処理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表します。
- 「(読み取り専用)」は、バケットの詳細ページでバケット名のあとに表示されます。
- [Buckets]ページでバケット名の横に「(Deleting objects : read-only)」と表示されます。

Buckets > my-bucket

**my-bucket (read-only)**

Region: us-east-1  
Date created: 2022-12-14 10:09:50 MST  
Object count: 3

View bucket contents in Experimental S3 Console [↗](#)

Delete bucket

**⚠ All bucket objects are being deleted**  
StorageGRID is deleting all copies of the objects in this bucket, which might take days or weeks. While objects are being deleted, the bucket is read only. To stop the operation, select **Stop deleting objects**. You cannot restore objects that have already been deleted.

0% (0 of 3 objects deleted)

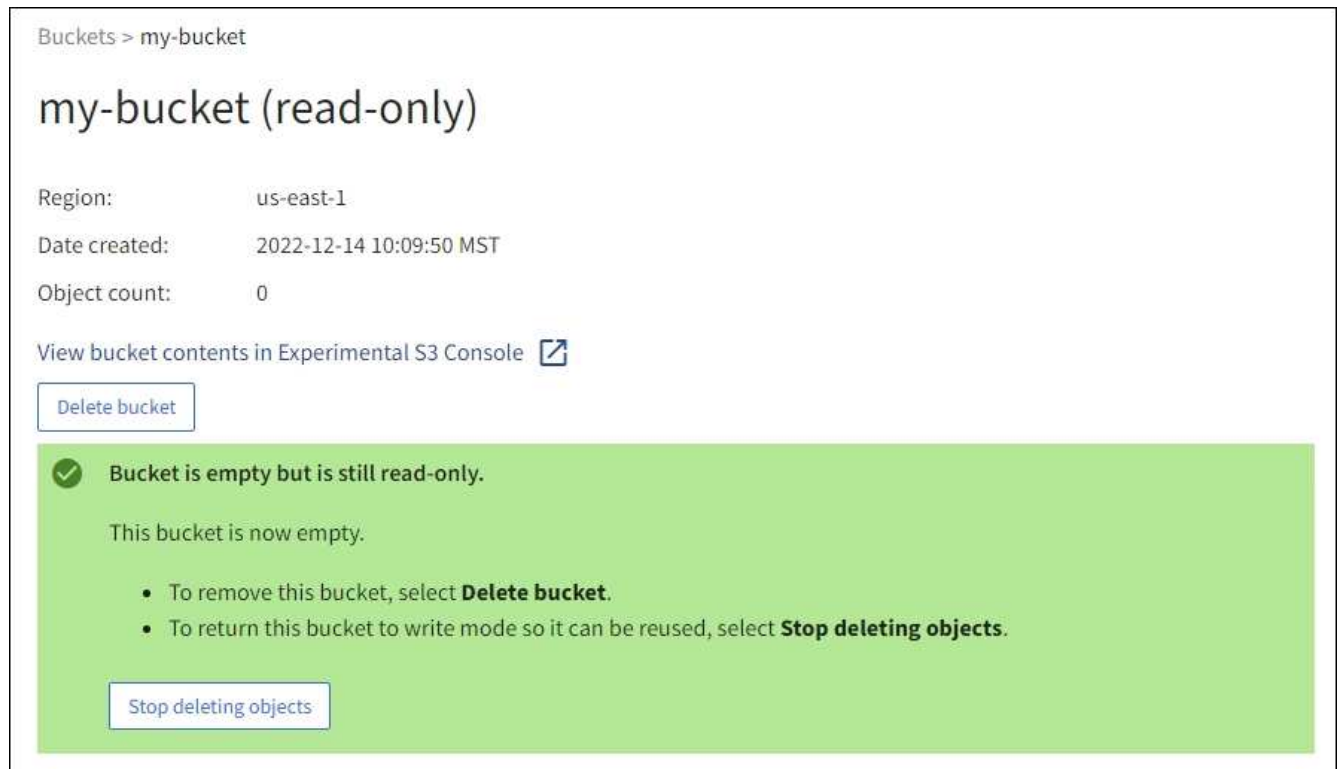
Stop deleting objects

5. 処理の実行中に必要に応じて、[オブジェクトの削除の停止]\*を選択してプロセスを停止します。次に、必要に応じて[Delete objects in bucket]\*を選択してプロセスを再開します。

[Stop deleting objects]\*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リストアしたりすることはできません。

6. 処理が完了するまで待ちます。

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です。



7. 次のいずれかを実行します。

- ページを終了して、バケットを読み取り専用モードのままにします。たとえば、空のバケットを読み取り専用モードのままにしておくと、あとで使用できるようにバケット名を予約できます。
- バケットを削除します。1つのバケットを削除する場合は、**[Delete bucket]\***を選択します。複数のバケットを削除する場合は、**[Buckets]**ページに戻って**[Actions]>[Delete \* Buckets]**を選択します。



すべてのオブジェクトの削除後にバージョン管理されたバケットを削除できない場合は、削除マーカが残っていることがあります。バケットを削除するには、残りのすべての削除マーカを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、必要に応じて新しいオブジェクト用に再利用します。1つのバケットに対して**[Stop deleting objects]**を選択するか、**[Buckets]**ページに戻って、複数のバケットに対して**[Action]>[Stop deleting objects]\***を選択します。

## S3 バケットを削除します

Tenant Manager を使用して、空の S3 バケットを削除できます。

作業を開始する前に

- Tenant Manager にはを使用してサインインします **"サポートされている Web ブラウザ"**。
- が設定されたユーザグループに属している必要があります **"すべてのバケットまたはRoot Access権限を管理します"**。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の設定よりも優先されます。
- 削除するバケットが空です。削除するバケットが `_not_empty` の場合は、**"バケットからオブジェクトを削除する"**。

このタスクについて

以下の手順では、Tenant Manager 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。を使用して S3 バケットを削除することもできます ["テナント管理 API"](#) または ["S3 REST API"](#)。

オブジェクト、最新でないオブジェクトバージョン、またはマーカーが含まれているS3バケットは削除できません。S3バージョン管理オブジェクトの削除方法については、を参照してください ["オブジェクトの削除方法"](#)。

#### 手順

1. ダッシュボードで\* View Buckets を選択するか、 storage (S3) > Buckets \*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. 特定のバケットの\*[Actions]\*メニューまたは詳細ページを使用します。

#### [アクション]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. >[Delete Buckets]\*を選択します。

#### 詳細ページ

- a. 詳細を表示するバケット名を選択します。
- b. [Delete bucket]\*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てから、各バケットを削除します。この処理には数分かかることがあります。

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。実行する必要があります ["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する"](#) バケットを削除する前に。

## S3コンソールを使用

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、次の操作を実行できます。

- アップロード、ダウンロード、名前変更、コピー、移動、オブジェクトの削除
- オブジェクトバージョンの表示、リポート、ダウンロード、削除
- プレフィックスでオブジェクトを検索
- オブジェクトタグを管理します
- オブジェクトのメタデータを表示します
- 表示、作成、名前変更、コピー、移動、フォルダの削除

S3コンソールでは、最も一般的なケースのユーザエクスペリエンスが向上しています。すべての状況において、CLIやAPIの処理に代わるものではありません。



S3コンソールを使用すると処理に時間がかかりすぎる場合（分や時間など）は、次の点を考慮してください。

- 選択したオブジェクトの数を減らす
- グラフィカルでない方法（APIまたはCLI）を使用したデータへのアクセス

作業を開始する前に

- Tenant Manager にはを使用してサインインします ["サポートされている Web ブラウザ"](#)。
- オブジェクトを管理する場合は、Root Access権限のあるユーザグループに属している必要があります。または、Use S3 Console Tab権限とView All Buckets権限またはManage All Buckets権限のいずれかのユーザグループに属している必要があります。を参照してください ["テナント管理権限"](#)。
- S3グループまたはバケットポリシーがユーザに設定されている。を参照してください ["バケットとグループのアクセスポリシーを使用"](#)。
- ユーザのアクセスキー ID とシークレットアクセスキーを確認しておきます。必要に応じて、があります .csv この情報を含むファイル。を参照してください ["アクセスキーの作成手順"](#)。

手順

1. storage > Buckets *\*>\*bucket name\**を選択します。
2. [S3][Console]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、*\*アクセスキーのアップロード\**を選択し、*\*アップロード\**を選択します .csv ファイル。
4. 「サインイン」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

- 接頭辞で検索：接頭辞検索機能は、現在のフォルダに対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、他の場所でその単語を含むオブジェクトは含まれません。このルールは、フォルダ内のオブジェクトも環境します。たとえば、folder1/folder2/somefile- 内部にあるオブジェクトを返します。folder1/folder2/ フォルダを作成し、次の単語で開始します。somefile-。
- ドラッグアンドドロップ:コンピューターのファイルマネージャから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。
- フォルダの操作:フォルダを移動、コピー、または名前変更すると、フォルダ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な場合の完全削除：バージョン管理が無効なバケット内のオブジェクトを上書きまたは削除すると、処理は永続的に実行されます。を参照してください ["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します

## プラットフォームサービスの管理：概要

StorageGRID プラットフォームサービスでは、イベント通知やS3オブジェクトとオブジェクトメタデータのコピーを外部のデスティネーションに送信できるため、ハイブリッドクラウド戦略の実装に役立ちます。

テナントアカウントにプラットフォームサービスの使用が許可されている場合は、S3 バケットに対して次のサービスを設定できます。

### CloudMirror レプリケーション

使用 ["StorageGRID CloudMirror レプリケーションサービス"](#) StorageGRID バケットから指定した外部のデスティネーションに特定のオブジェクトをミラーリングする。

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 サービスを利用してデータを分析することができます。



ソースバケットで S3 オブジェクトの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。

### 通知

使用 ["バケット単位のイベント通知"](#) オブジェクトに対して実行された特定の処理に関する通知を、指定した外部のAmazon Simple Notification Service (Amazon SNS) に送信すること。

たとえば、バケットに追加された各オブジェクトについてアラートが管理者に送信されるように設定できます。この場合、オブジェクトは重大なシステムイベントに関連付けられているログファイルです。



S3 オブジェクトの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することはできますが、オブジェクトの S3 オブジェクトロックメタデータ (Retain Until Date および Legal Hold のステータスを含む) は通知メッセージに含まれません。

### 検索統合サービス

を使用します ["検索統合サービス"](#) 外部サービスを使用してメタデータを検索または分析できるように、指定されたElasticsearchインデックスにS3オブジェクトメタデータを送信する場合。

たとえば、リモートの Elasticsearch サービスに S3 オブジェクトメタデータを送信するようにバケットを設定できます。次に、Elasticsearch を使用してバケット間で検索を実行し、オブジェクトメタデータのパターンに対して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なバケットでは 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 (Retain Until Date および Legal Hold のステータスを含む) は通知メッセージに含まれません。

通常、プラットフォームサービスのターゲットは StorageGRID 環境の外部にあるため、プラットフォームサービスを使用することで外部ストレージリソース、通知サービス、検索または分析サービスの機能と柔軟性をデータに対して利用できます。

単一の S3 バケットに対して複数のプラットフォームサービスを組み合わせることで設定できます。たとえば、StorageGRID S3 バケットに対して CloudMirror サービスと通知の両方を設定して、特定のオブジェクトを Amazon Simple Storage Service にミラーリングし、同時に各オブジェクトに関する通知を他社製の監視アプリケーションに送信して AWS の費用を追跡できます。



プラットフォームサービスの使用は、StorageGRID 管理者がグリッドマネージャまたはグリッド管理 API を使用して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設定方法

プラットフォームサービスは、を使用して設定した外部エンドポイントと通信します ["Tenant Manager の略"](#) または ["テナント管理 API"](#)。各エンドポイントは外部のデスティネーション（StorageGRID S3バケット、Amazon Web Servicesバケット、Amazon SNSトピック、ローカルやAWSなどでホストされるElasticsearchクラスタなど）です。

外部エンドポイントを作成したら、バケットにXML設定を追加してプラットフォームサービスを有効にできます。XML 設定は、バケットが処理を実行するオブジェクト、実行する処理、およびサービスに使用するエンドポイントを特定します。

設定するプラットフォームサービスごとに XML 設定を追加する必要があります。例：

- キーがで始まるすべてのオブジェクトを指定する場合 /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格納されたときに通知も送信するには、通知設定を追加する必要があります。
- 最後に、これらのオブジェクトのメタデータのインデックスを作成する場合は、検索統合を実装するためのメタデータ通知設定を追加する必要があります。

設定 XML の形式は、StorageGRID プラットフォームサービスの実装に使用する S3 REST API に従います。

プラットフォームサービス	S3 REST API	を参照してください
CloudMirror レプリケーション	<ul style="list-style-type: none"> <li>• GetBucketReplicationの略</li> <li>• PutBucketReplicationの略</li> </ul>	<ul style="list-style-type: none"> <li>• <a href="#">"CloudMirror レプリケーション"</a></li> <li>• <a href="#">"バケットの処理"</a></li> </ul>
通知	<ul style="list-style-type: none"> <li>• GetBucketNotificationConfigurationを参照してください</li> <li>• PutBucketNotificationConfigurationの略</li> </ul>	<ul style="list-style-type: none"> <li>• <a href="#">"通知"</a></li> <li>• <a href="#">"バケットの処理"</a></li> </ul>
検索統合	<ul style="list-style-type: none"> <li>• GET Bucket metadata notification configuration</li> <li>• PUT Bucket metadata notification configuration のコマンドです</li> </ul>	<ul style="list-style-type: none"> <li>• <a href="#">"検索統合"</a></li> <li>• <a href="#">"StorageGRIDのカスタム処理"</a></li> </ul>

## 関連情報

["プラットフォームサービスに関する考慮事項"](#)

## CloudMirror レプリケーションサービス

StorageGRID で、ある S3 バケットに追加されたオブジェクトを指定して 1 つ以上のデスティネーションバケットにレプリケートする必要がある場合は、そのバケットに対し



て CloudMirror レプリケーションを有効にすることができます。

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、ソースバケットに格納された時点でオブジェクトをレプリケートし、できるだけ早くデスティネーションバケットに配信します。レプリケートオブジェクトの配信は、オブジェクトの取り込みが成功したときにトリガーされます。



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重要な類似点と相違点があります。詳細については、[を参照してください "グリッド間レプリケーションとCloudMirrorレプリケーションを比較してください"](#)。

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レプリケートされません。既存のオブジェクトのレプリケーションを強制的に実行するには、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します。



CloudMirrorレプリケーションを使用してオブジェクトをAmazon S3デスティネーションにコピーする場合は、Amazon S3で各PUT要求ヘッダー内のユーザ定義メタデータのサイズが2KBに制限されることに注意してください。オブジェクトのユーザ定義メタデータが 2KB を超える場合、そのオブジェクトはレプリケートされません。

StorageGRID では、1つのバケット内のオブジェクトを複数のデスティネーションバケットにレプリケートできます。そのためには、レプリケーション設定 XML で各ルールのデスティネーションを指定します。オブジェクトを複数のバケットに同時にレプリケートすることはできません。

また、バージョン管理に対応している / していないバケットで CloudMirror レプリケーションを設定することもでき、バージョン管理に対応している / していないバケットをデスティネーションとして指定できます。バージョン管理に対応しているバケットとしていないバケットを組み合わせる使用することができます。たとえば、バージョン管理に対応しているバケットをバージョン管理に対応していないソースバケットのデスティネーションとして指定することも、その逆を指定することもできます。また、バージョン管理に対応していないバケット間でもレプリケートできます。

CloudMirror レプリケーションサービスの削除は、Amazon S3 が提供する Cross Region Replication (CRR ; クロスリージョンレプリケーション) サービスの削除と同様に機能します。つまり、ソースバケット内のオブジェクトを削除してもデスティネーションのレプリケートオブジェクトは削除されません。ソースとデスティネーションの両方のバケットがバージョン管理に対応している場合は、削除マーカーがレプリケートされます。デスティネーションバケットがバージョン管理に対応していない場合は、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はデスティネーションバケットにレプリケートされず、デスティネーションオブジェクトも削除されません。

StorageGRIDは、デスティネーションバケットにレプリケートされたオブジェクトを「レプリカ」としてマークします。デスティネーション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びレプリケートしないため、誤ってレプリケーションがループすることはありません。このレプリカマーキングはStorageGRIDの内部処理で、Amazon S3バケットをデスティネーションとして使用する際にAWS CRRを使用することには支障はありません。



レプリカのマークに使用されるカスタムヘッダーはです `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では、2つのグリッド間の双向CloudMirrorがサポートされます。

デスティネーションバケット内のイベントは一意であることや順序が保証されるわけではありません。確実に配信することを目的とした処理の結果として、ソースオブジェクトの同一のコピーが複数デスティネーション

に配信されることがあります。まれに、複数の異なる StorageGRID サイトから同じオブジェクトが同時に更新された場合、デスティネーションバケットでの処理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ことがあります。

通常、CloudMirror レプリケーションは外部の S3 バケットをデスティネーションとして使用するよう設定します。ただし、他の StorageGRID 環境や任意の S3 互換サービスを使用するようにレプリケーションを設定することもできます。

バケットの通知について理解します

S3バケットのイベント通知を有効にすると、指定したイベントに関する通知をStorageGRIDからデスティネーションKafkaクラスタまたはAmazon Simple Notification Serviceに送信できます。

可能です ["イベント通知を設定する"](#) 通知設定 XML をソースバケットに関連付けます。通知設定XMLにはS3の規則に従ってバケット通知を設定し、デスティネーションの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。

イベント通知は通知設定に従ってソースバケットで作成され、デスティネーションに配信されます。オブジェクトに関連付けられている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て配信のためにキューに登録されます。

通知の一貫性と順序は保証されません。確実に配信することを目的とした処理の結果として、1つのイベントに関する通知が複数デスティネーションに配信されることがあります。また配信は非同期で実行されるため、特に異なる StorageGRID サイトで開始された処理の場合、デスティネーションでの通知の時間的順序がソースバケットでのイベントの順序と一致する保証はありません。を使用できます sequencer Amazon S3 のドキュメントに従って、イベントメッセージを入力して特定のオブジェクトに対するイベントの順序を決定します。

サポートされている通知およびメッセージです

StorageGRID のイベント通知はAmazon S3 APIに従いますが、いくつかの制限事項があります。

- 次のイベントタイプがサポートされています。
  - S3 : ObjectCreated : \*
  - S3 : ObjectCreated : PUT
  - S3 : ObjectCreated : Post
  - S3 : ObjectCreated : コピー
  - S3 : ObjectCreated : CompleteMultipartUpload
  - S3 : ObjectRemoved : \*
  - S3 : ObjectRemoved : 削除
  - S3 : ObjectRemoved : DeleteMarkerCreated
  - S3 : ObjectRestore : POSTコマンド
- StorageGRID から送信されるイベント通知は標準のJSON形式を使用しますが、次の表に示すように、一部のキーを含めずに特定の値を使用するキーもあります。

キー名	StorageGRID 値
eventSource	sgws:s3
awsRegion のようになります	含まれません
x-amz-id-2	含まれません
ARN	urn:sgws:s3:::bucket_name

## 検索統合サービスについて理解する

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必要がある場合は、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カスタムの StorageGRID サービスです。S3 オブジェクトまたはそのメタデータが更新されるたびに、オブジェクトメタデータを非同期的に自動でデスティネーションエンドポイントに送信します。その後、デスティネーションサービスが提供する高度な検索、データ分析、視覚化、機械学習のツールを使用して、オブジェクトデータを検索、分析し、情報を把握できます。

検索統合サービスはバージョン管理に対応している / していないに関わらずすべてのバケットに対して有効にすることができます。検索統合を設定するには、対象のオブジェクトおよびオブジェクトメタデータのデスティネーションを指定したメタデータ通知設定 XML をバケットに関連付けます。

通知は、という名前の JSON ドキュメントの形式で生成されます。バケット名、オブジェクト名、バージョン ID も必要です。各メタデータ通知には、すべてのオブジェクトのタグとユーザ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。



タグとユーザメタデータの場合、StorageGRID は文字列または S3 イベント通知として Elasticsearch に日付と番号を渡します。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 を設定するには、動的フィールドマッピングおよびマッピング日付形式に関する Elasticsearch の手順に従ってください。検索統合サービスを設定する前に、インデックスの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作成後は、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。

通知は次の場合に常に生成され、配信のキューに登録されます

- オブジェクトが作成されます。
- オブジェクトが削除されたとき。グリッドの ILM ポリシーの処理が実行された結果、オブジェクトが削除される場合も含まれます。
- オブジェクトのメタデータまたはタグが追加、更新、または削除されたとき。変更された値だけでなく、すべてのメタデータとタグが常に更新時に送信されます。

バケットにメタデータ通知設定 XML を追加すると、新しく作成したオブジェクトや、データ、ユーザメタデータ、またはタグの更新によって変更したオブジェクトに関する通知が送信されます。ただし、バケットにすでに含まれていたオブジェクトについては通知は送信されません。バケットに含まれるすべてのオブジェクトのオブジェクトメタデータを確実にデスティネーションに送信するには、次のいずれかを行う必要があります。

- バケットの作成後、オブジェクトを追加する前に、検索統合サービスを設定する。
- すでにバケットに含まれているすべてのオブジェクトに対して、メタデータ通知メッセージをデスティネーションに送信するトリガーとなる処理を実行する。

StorageGRID 検索統合サービスは、デスティネーションとして Elasticsearch クラスタをサポートします。他のプラットフォームサービスと同様、URN がサービスの設定 XML で使用されているエンドポイントにデスティネーションが指定されます。を使用します ["NetApp Interoperability Matrix Tool で確認できます"](#) サポートされている Elasticsearch のバージョンを確認できます。

#### 関連情報

["検索統合用の XML を設定します"](#)

["メタデータ通知に含まれているオブジェクトメタデータ"](#)

["検索統合サービスで生成される JSON"](#)

["検索統合サービスを設定する"](#)

#### プラットフォームサービスに関する考慮事項

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推奨事項と考慮事項を確認してください。

S3 の詳細については、[を参照してください "S3 REST APIを使用する"](#)。

#### プラットフォームサービスの使用に関する考慮事項

考慮事項	詳細
デスティネーションエンドポイントの監視	各デスティネーションエンドポイントの可用性を監視する必要があります。長時間にわたってデスティネーションエンドポイントへの接続が失われ、要求のバックログが大量に発生している場合、StorageGRID に対する以降のクライアント要求（PUT 要求など）は失敗します。エンドポイントがアクセス可能になったら、失敗した要求を再試行する必要があります。
デスティネーションエンドポイントのスロットル	<p>要求が送信されるペースがデスティネーションエンドポイントで要求を受信できるペースを超えると、StorageGRID ソフトウェアはバケットの受信 S3 要求を調整する場合があります。スロットルは、デスティネーションエンドポイントへの送信を待機している要求のバックログが生じている場合にのみ発生します。</p> <p>明らかな影響は、受信 S3 要求の実行時間が長くなることだけです。パフォーマンスが大幅に低下していることが検出されるようになった場合は、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。要求のバックログが増え続けると、クライアント S3 処理（PUT 要求など）が失敗します。</p> <p>通常、CloudMirror 要求には、検索統合やイベント通知の要求よりも多くのデータ転送が含まれるため、デスティネーションエンドポイントのパフォーマンスによる影響を受ける可能性が高くなります。</p>

考慮事項	詳細
順序保証	<p>StorageGRID では、1つのサイト内のオブジェクトに対する処理の順序が保証されます。あるオブジェクトに対するすべての処理が同じサイト内で実行されるかぎり、最終的なオブジェクトの（レプリケーションの）状態は常に StorageGRID の状態と同じになります。</p> <p>StorageGRID は、StorageGRID サイト間で処理が行われる場合、最善の順序で要求を処理しようと試みます。たとえば、最初にサイト A にオブジェクトを書き込んだあと、サイト B で同じオブジェクトを上書きした場合、CloudMirror によって最終的にデスティネーションバケットにレプリケートされるオブジェクトが新しいほうのオブジェクトであるとはかぎりません。</p>
ILM ベースのオブジェクト削除	<p>AWS CRRとAmazon Simple Notification Serviceの削除動作と一致するように、StorageGRID ILMルールに基づいてソースバケット内のオブジェクトが削除された場合、CloudMirror要求とイベント通知要求は送信されません。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 要求やイベント通知要求は送信されません。</p> <p>一方、ILM に基づいてオブジェクトが削除された場合、検索統合要求は送信されません。</p>
Kafkaエンドポイントの使用	<p>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、<code>ssl.client.auth</code> をに設定し <code>required</code> Kafkaブローカーの設定では、原因Kafkaエンドポイントの設定に問題がある可能性があります。</p> <p>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、ユーザ名とパスワードのクレデンシャルが必要です。</p> <ul style="list-style-type: none"> <li>• SASL/プレーン</li> <li>• SASL/SCRAM-SHA-256</li> <li>• SASL/SCRAM-SHA-512</li> </ul> <p>*注：*構成済みの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。</p>

### 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
レプリケーションのステータス	StorageGRID ではがサポートされません <code>x-amz-replication-status</code> ヘッダー。

考慮事項	詳細
オブジェクトのサイズ	<p>CloudMirror レプリケーションサービスでデスティネーション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 5TiB で、maximum_supported_object サイズと同じです。</p> <p>注：1回のPutObject処理の最大推奨サイズは5GiB（5、368、709、120バイト）です。5GB より大きいオブジェクトがある場合は、マルチパートアップロードを使用してください。</p>
バケットのバージョン管理とバージョン ID	<p>StorageGRID でソース S3 バケットのバージョン管理を有効にした場合、デスティネーションバケットのバージョン管理も有効にする必要があります。</p> <p>バージョン管理を使用している場合、S3 プロトコルの制限事項により、デスティネーションバケットのオブジェクトバージョンの処理はベストエフォートベースで行われ、CloudMirror サービスによる保証はありません。</p> <p>注：StorageGRID のソースバケットのバージョンIDは、デスティネーションバケットのバージョンIDとは関係ありません。</p>
オブジェクトバージョンのタグ付け	<p>S3プロトコルの制限により、バージョンIDを提供するPutObjectTagging要求やDeleteObjectTagging要求はCloudMirrorサービスではレプリケートされません。ソースとデスティネーションのバージョンIDは関連付けられていないため、特定のバージョンIDへのタグの更新を確実にレプリケートする方法はありません。</p> <p>一方、CloudMirrorサービスでは、バージョンIDを指定しないPutObjectTagging要求またはDeleteObjectTagging要求はレプリケートされません。これらの要求は、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のバージョン）のタグを更新します。（タグの更新ではなく）タグを使用した通常の取り込みもレプリケートされます。</p>
マルチパートアップロードおよび ETag 値	<p>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した場合、CloudMirror サービスではパートが保持されません。その結果、が表示されます ETag ミラーオブジェクトの値は、とは異なります ETag 元のオブジェクトの値。</p>
SSE-C（ユーザ指定のキーによるサーバ側の暗号化）で暗号化されたオブジェクト	<p>CloudMirror サービスでは、SSE-C で暗号化されたオブジェクトがサポートされません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む際に、要求に SSE-C 要求ヘッダーが含まれていると、処理が失敗します。</p>
S3 オブジェクトのロックが有効になっているバケット	<p>CloudMirrorレプリケーションのデスティネーションS3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、バケットのレプリケーションを設定しようとするとAccessDeniedエラーで失敗します。</p>

## プラットフォームサービスエンドポイントを設定する

バケットのプラットフォームサービスを設定する前に、少なくとも1つのエンドポイントをプラットフォームサービスのデスティネーションとして設定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 管理者がテナント単位で有効にします。プラットフォームサービスエンドポイントを作成または使用するには、ストレージノードが外部のエンドポイントリソースにアクセスできるようネットワークが設定されているグリッドで、Manage EndpointsまたはRoot Access 権限を持つテナントユーザである必要があります。1つのテナントに対して設定できるプラットフォームサービスエンドポイントは最大500個です。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を作成するときは、StorageGRID が外部のデスティネーション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レプリケートする場合は、StorageGRID がAmazonのデスティネーションバケットにアクセスするために必要な情報とクレデンシャル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。

プラットフォームサービスのタイプごとに独自のエンドポイントが必要なため、使用する各プラットフォームサービスについて少なくとも1つのエンドポイントを設定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の定義が完了したら、サービスを有効にするための設定XMLでエンドポイントのURNをデスティネーションとして指定します。

同じエンドポイントを複数のソースバケットのデスティネーションとして使用できます。たとえば、複数のバケット間で検索を実行できるように、複数のソースバケットが同じ検索統合エンドポイントにオブジェクトメタデータを送信するように設定できます。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ソースバケットを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あるAmazon Simple Notification Service (Amazon SNS) トピックに送信したり、オブジェクトの削除に関する通知を別のAmazon SNSトピックに送信したりできます。

### CloudMirror レプリケーション用のエンドポイント

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ます。このバケットは、Amazon Web Services、同一またはリモートのStorageGRID 環境、あるいは別のサービスでホストされている可能性があります。

### 通知用のエンドポイント

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、`ssl.client.auth` をに設定します `required` Kafkaブローカーの設定では、原因Kafkaエンドポイントの設定に問題があ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 クラスタを表す検索統合エンドポイントをサポートします。Elasticsearch クラスタは、ローカルデータセンターに配置することも、AWSクラウドなどの別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、Elasticsearch の特定の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しておく必要があります。作成していない場合、エンドポイントの作成に失敗します。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。

"StorageGRID の管理"

プラットフォームサービスのエンドポイントの **URN** を指定してください

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、Unique Resource Name (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設定XMLを作成するときは、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。

プラットフォームサービスエンドポイントは、作成時に StorageGRID で検証されます。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、アクセス可能であ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のエンドポイントのURNは、いずれかで開始する必要があります `arn:aws` または `urn:mysite`、次のようにします。

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

たとえば、StorageGRID でホストされるCloudMirrorエンドポイントのURNを指定する場合、URNはで始まる可能性があります `urn:sgws`。

URN の次の要素では、次のようにプラットフォームサービスのタイプを指定します。

サービス	を入力します
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 でホストされるCloudMirrorエンドポイントのURNを指定する場合は、と指定します `s3` をダウンロードしてください `urn:sgws:s3`。

URN の最後の要素は、デスティネーション 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 クラスタが *NOT* である場合、インデックスを自動的に作成するように設定されているため、エンドポイントを作成する前にインデックスを手動で作成する必要があります。

#### AWS と GCP でホストされるサービスの URN

AWS と GCP のエンティティの場合、完全な URN は有効な AWS ARN です。例：

- 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は、を参照してください domain-name リテラル文字列を含める必要があります `domain/` を参照してください。

#### 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は、URN の 3 番目と最後の必須要素が含まれていて、有効かつ一意な URN が作成されるのであれば、どのような方法で URN を指定してもかまいません。となっている要素はオプションで空白にすることも、リソースを識別して一意な URN の作成に役立つ任意の情報を指定することもできます。例：

- CloudMirror レプリケーション：

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

StorageGRID でホストされるCloudMirrorエンドポイントの場合は、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
```



ローカルでホストされる検索統合エンドポイントの場合は、を参照してください domain-name エンドポイントのURNが一意であるかぎり、Elementには任意の文字列を指定できません。

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

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 つ作成しておく必要があります。

作業を開始する前に

- Tenant Manager にはを使用してサインインします ["サポートされている Web ブラウザ"](#)。
- テナントアカウントのプラットフォームサービスがStorageGRID 管理者によって有効にされている。
- が設定されたユーザグループに属している必要があります ["エンドポイントまたはRoot Access権限を管理します"](#)。
- 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を作成しておきます。
  - 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： インデックスを自動的に作成するようにデスティネーションクラスタが設定されていない場合、 Elasticsearch インデックス。
- デスティネーションリソースに関する情報を確認しておきます。
  - Uniform Resource Identifier (URI) 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場合は、グリッド管理者に問い合わせて入力が必要な値を決定してください。

- Unique Resource Name (URN)

## "プラットフォームサービスのエンドポイントの URN を指定してください"

- 認証クレデンシャル（必要な場合）：

### **AWS**ケンサクトウコウエントポイント

AWS検索統合エンドポイントの場合は、次のクレデンシャルを使用できます。

- Access Key：アクセスキー ID とシークレットアクセスキー
- 基本 HTTP 認証：ユーザ名とパスワード
- CAP（C2S Access Portal）：一時的なクレデンシャル URL、サーバ証明書と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鍵パスフレーズ。

### **CloudMirror**レプリケーションと**Amazon SNS**エンドポイント

CloudMirrorレプリケーションエンドポイントとAmazon SNSエンドポイントの場合は、次のクレデンシャルを使用できます。

- Access Key：アクセスキー ID とシークレットアクセスキー
- CAP（C2S Access Portal）：一時的なクレデンシャル URL、サーバ証明書と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鍵パスフレーズ。

### **Kafka**エンドポイント

Kafkaエンドポイントの場合は、次のクレデンシャルを使用できます。

- SASL/plain：ユーザ名とパスワード
- SASL/SCRAM-SHA-256：ユーザ名とパスワード
- SASL/SCRAM-SHA-512：ユーザ名とパスワード

- セキュリティ証明書（カスタム CA 証明書を使用する場合）

- Elasticsearchセキュリティ機能が有効になっている場合は、接続テスト用のmonitor cluster権限と、ドキュメント更新用のwrite index権限、またはindex権限とdelete index権限の両方があります。

## 手順

1. ストレージ（S3） \* > \* プラットフォームサービスのエンドポイント \* 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、[Endpoints]ページのエンドポイント名の横に表示されるため、この情報を名前に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 Unique Resource Identifier（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にはポート443、HTTP URIにはポート80（ほとんどのエンドポイント）
- HTTPSおよびHTTP URI用のポート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 ハイアベイラビリティ（HA）グループの仮想IP（VIP）のDNSエントリ、およびを表します 10443 ロードバランサエンドポイントで定義されたポートを表します。



単一点障害（Single Point of Failure）を回避するために、可能な限りロードバランシングノードの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。バケット名は「\* URN \*」フィールドに含める必要があります。

5. エンドポイントの Unique Resource Name（URN）を入力します。



エンドポイントの作成後にエンドポイントのURNを変更することはできません。

6. 「\* Continue \*」を選択します。

7. [認証タイプ]\*の値を選択します。

### AWSケンサクトウコウエントポイント

AWS検索統合エンドポイントのクレデンシャルを入力またはアップロードします。

指定するクレデンシャルには、デスティネーション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	クレデンシャル
匿名	デスティネーションへの匿名アクセスを許可します。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形式のクレデンシャルを使用してデスティネーションとの接続を認証します。	<ul style="list-style-type: none"><li>• アクセスキー ID</li><li>• シークレットアクセスキー</li></ul>
基本 HTTP	ユーザ名とパスワードを使用して、デスティネーションへの接続を認証します。	<ul style="list-style-type: none"><li>• ユーザ名</li><li>• パスワード</li></ul>
CAP (C2S Access Portal)	証明書とキーを使用してデスティネーションへの接続を認証します。	<ul style="list-style-type: none"><li>• 一時的な資格情報 URL</li><li>• サーバ CA 証明書 (PEM ファイルのアップロード)</li><li>• クライアント証明書 (PEM ファイルのアップロード)</li><li>• 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)</li><li>• クライアント秘密鍵のパスフレーズ (オプション)</li></ul>

### CloudMirrorレプリケーションまたはAmazon SNSエンドポイント

CloudMirrorレプリケーションまたはAmazon SNSエンドポイントのクレデンシャルを入力またはアップロードします。

指定するクレデンシャルには、デスティネーション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	クレデンシャル
匿名	デスティネーションへの匿名アクセスを許可します。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。

認証タイプ	説明	クレデンシャル
アクセスキー	AWS 形式のクレデンシャルを使用してデスティネーションとの接続を認証します。	<ul style="list-style-type: none"> <li>• アクセスキー ID</li> <li>• シークレットアクセスキー</li> </ul>
CAP ( C2S Access Portal )	証明書とキーを使用してデスティネーションへの接続を認証します。	<ul style="list-style-type: none"> <li>• 一時的な資格情報 URL</li> <li>• サーバ CA 証明書 ( PEM ファイルのアップロード)</li> <li>• クライアント証明書 ( PEM ファイルのアップロード)</li> <li>• 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)</li> <li>• クライアント秘密鍵のパスフレーズ (オプション)</li> </ul>

#### Kafkaエンドポイント

Kafkaエンドポイントのクレデンシャルを入力またはアップロードします。

指定するクレデンシャルには、デスティネーション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	クレデンシャル
匿名	デスティネーションへの匿名アクセスを許可します。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名とパスワードを使用して、宛先への接続を認証します。	<ul style="list-style-type: none"> <li>• ユーザ名</li> <li>• パスワード</li> </ul>
SASL/SCRAM-SHA-256	チャレンジ応答プロトコルとSHA-256 ハッシュを使用してユーザ名とパスワードを使用し、宛先への接続を認証します。	<ul style="list-style-type: none"> <li>• ユーザ名</li> <li>• パスワード</li> </ul>
SASL/SCRAM-SHA-512	チャレンジ応答プロトコルとSHA-512 ハッシュを使用してユーザ名とパスワードを使用し、宛先への接続を認証します。	<ul style="list-style-type: none"> <li>• ユーザ名</li> <li>• パスワード</li> </ul>

ユーザ名とパスワードがKafkaクラスタから取得した委任トークンから取得されたものである場合は、\* Use delegation taken authentication \*を選択します。

8. 「 \* Continue \* 」を選択します。
9. Verify server \* のラジオボタンを選択して、エンドポイントへの TLS 接続の検証方法を選択します。

×

## Create endpoint

✓ Enter details
 ✓ Select authentication type Optional
3 Verify server Optional

### Verify server

Use this method to validate the certificate for TLS connections to the endpoint resource. If you select "Use custom CA certificate," copy and paste the custom security certificate in the text box.

Use custom CA certificate

Use operating system CA certificate

Do not verify certificate

```

          -----BEGIN CERTIFICATE-----
          abcdefghijkl123456780ABCDEFGHIJKL
          123456/7890ABCDEFabcdefghijklABCD
          -----END CERTIFICATE-----
        
```

Previous
Test and create endpoint

証明書検証のタイプ	説明
カスタム CA 証明書を使用する	カスタムの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 * CA 証明書 * テキストボックスにコピーして貼り付けます。
オペレーティングシステムの CA 証明書を使用します	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。
証明書を検証しないでください	TLS 接続に使用される証明書は検証されません。このオプションはセキュアではありません。

10. [ \* テストとエンドポイントの作成 \* ] を選択します。
  - 指定したクレデンシャルを使用してエンドポイントにアクセスできた場合は、成功を伝える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が失敗した場合は、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、「 \* Test 」を選択し、エンドポイントを作成します。 \*



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と、エンドポイントの作成が失敗します。StorageGRID 管理者にお問い合わせください。

エンドポイントの設定が完了したら、その URN を使用してプラットフォームサービスを設定できます。

#### 関連情報

["プラットフォームサービスのエンドポイントの URN を指定してください"](#)

["CloudMirror レプリケーションを設定します"](#)

["イベント通知を設定する"](#)

["検索統合サービスを設定する"](#)

プラットフォームサービスエンドポイントの接続をテストします

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、エンドポイントへの接続をテストして、デスティネーションリソースが存在すること、および指定したクレデンシャルでアクセスできることを確認できます。

作業を開始する前に

- Tenant Manager にはを使用してサインインします ["サポートされている Web ブラウザ"](#)。
- が設定されたユーザグループに属している必要があります ["エンドポイントまたはRoot Access権限を管理します"](#)。

このタスクについて

StorageGRID は、クレデンシャル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のエンドポイント](#) \* を選択します。

Platform services Endpoints ページが表示され、設定済みの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。



# Platform services endpoints

A platform services endpoint stores the information StorageGRID needs to use an external resource as a target for a platform service (CloudMirror replication, notifications, or search integration). You must configure an endpoint for each platform service you plan to use.

4 endpoints

Create endpoint

Delete endpoint

<input type="checkbox"/>	Display name <a href="#">?</a> <a href="#">↕</a>	Last error <a href="#">?</a> <a href="#">↕</a>	Type <a href="#">?</a> <a href="#">↕</a>	URI <a href="#">?</a> <a href="#">↕</a>	URN <a href="#">?</a> <a href="#">↕</a>
<input type="checkbox"/>	my-endpoint-1		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket1
<input type="checkbox"/>	my-endpoint-2	<span>✖</span> 2 hours ago	Search	http://10.96.104.30:9200	urn:sgws:es:::mydomain/sveloso/_doc
<input type="checkbox"/>	my-endpoint-3		Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example1
<input type="checkbox"/>	my-endpoint-4		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket2

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。

## Overview [^](#)

Display name: **my-endpoint-1** [✎](#)

Type: **S3 Bucket**

URI: **http://10.96.104.167:10443**

URN: **urn:sgws:s3:::bucket1**

---

**Connection** **Configuration**

### Verify connection [?](#)

Some errors might continue to appear after they are resolved. To see if an error is current or to force the removal of a resolved error, select **Test connection**.

**Test connection**

### 3. [接続のテスト \*] を選択します。

- 指定したクレデンシャルを使用してエンドポイントにアクセスできた場合は、成功を伝える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が失敗した場合は、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、「\* Configuration \*」を選択して情報を更新します。次に、[テスト] を選択し、変更を保存します。\*

プラットフォームサービスエンドポイントを編集します

プラットフォームサービスエンドポイントの設定を編集して、名前、URI、またはその他の詳細を変更できます。たとえば、期限切れのクレデンシャルを更新したり、フェールオーバー用のバックアップ Elasticsearch インデックスを指すように URI を変更したりすることが必要な場合があります。プラットフォームサービスエンドポイントのURN は変更できません。

作業を開始する前に

- Tenant Manager にはを使用してサインインします "サポートされている Web ブラウザ"。
- が設定されたユーザグループに属している必要があります "エンドポイントまたはRoot Access権限を管理します"。

手順

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

Platform services Endpoints ページが表示され、設定済みの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。

## Platform services endpoints

A platform services endpoint stores the information StorageGRID needs to use an external resource as a target for a platform service (CloudMirror replication, notifications, or search integration). You must configure an endpoint for each platform service you plan to use.

4 endpoints [Create endpoint](#)

[Delete endpoint](#)

<input type="checkbox"/>	Display name <a href="#">?</a> <a href="#">↕</a>	Last error <a href="#">?</a> <a href="#">↕</a>	Type <a href="#">?</a> <a href="#">↕</a>	URI <a href="#">?</a> <a href="#">↕</a>	URN <a href="#">?</a> <a href="#">↕</a>
<input type="checkbox"/>	my-endpoint-1		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3::bucket1
<input type="checkbox"/>	my-endpoint-2	<span style="color: red;">✖</span> 2 hours ago	Search	http://10.96.104.30:9200	urn:sgws:es::mydomain/sveloso/_doc
<input type="checkbox"/>	my-endpoint-3		Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example1
<input type="checkbox"/>	my-endpoint-4		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3::bucket2

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. 「\* Configuration \*」を選択します。

4. 必要に応じて、エンドポイントの設定を変更します。



エンドポイントの作成後にエンドポイントの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、必要に応じて「\* 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ることで、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、\* Revert S3 key edit \* を選択します。
- CAP（C2S Access Portal）認証の場合は、一時的なクレデンシャル URL またはオプションのクライアント秘密鍵パスフレーズを変更し、必要に応じて新しい証明書と鍵ファイルをアップロードします。



クライアント秘密鍵は、OpenSSL 暗号化形式または暗号化されていない秘密鍵形式である必要があります。

d. 必要に応じて、サーバを検証する方法を変更します。

5. [変更のテストと保存\*]を選択します。

- 指定したクレデンシャルを使用してエンドポイントにアクセスできた場合は、成功を伝える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が失敗した場合は、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、[変更のテストと保存]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します

関連するプラットフォームサービスが不要になった場合は、エンドポイントを削除できません。

作業を開始する前に

- Tenant Manager にはを使用してサインインします ["サポートされている Web ブラウザ"](#)。
- が設定されたユーザグループに属している必要があります ["エンドポイントまたはRoot Access権限を管理します"](#)。

手順

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

Platform services Endpoints ページが表示され、設定済みの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。

# Platform services endpoints

A platform services endpoint stores the information StorageGRID needs to use an external resource as a target for a platform service (CloudMirror replication, notifications, or search integration). You must configure an endpoint for each platform service you plan to use.

4 endpoints

Create endpoint

Delete endpoint

<input type="checkbox"/>	Display name <a href="#">?</a> <a href="#">↕</a>	Last error <a href="#">?</a> <a href="#">↕</a>	Type <a href="#">?</a> <a href="#">↕</a>	URI <a href="#">?</a> <a href="#">↕</a>	URN <a href="#">?</a> <a href="#">↕</a>
<input type="checkbox"/>	my-endpoint-1		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket1
<input type="checkbox"/>	my-endpoint-2	<span style="color: red;">✖</span> 2 hours ago	Search	http://10.96.104.30:9200	urn:sgws:es:::mydomain/sveloso/_doc
<input type="checkbox"/>	my-endpoint-3		Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example1
<input type="checkbox"/>	my-endpoint-4		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket2

- 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、エンドポイントを使用するすべてのバケットに対して、関連するプラットフォームサービスが無効になります。完了していない要求はすべて破棄されます。新しい要求は、削除された URN を参照しないようにバケット設定を変更するまで、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。

- [ \* 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。

## Delete endpoint ✕

**Are you sure you want to delete endpoint my-endpoint-10?**

This might take a few minutes.

When you delete an endpoint, you can no longer use it to access external resources.

Cancel Delete endpoint


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を行います

StorageGRID がプラットフォームサービスエンドポイントと通信しようとした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。Platform services Endpoints ページの Last error 列は、エラーが発生してからの時間を示します。エンドポイントのクレデンシャルに関連付けられている権限が正しくない場合は、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します

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は、Tenant Managerダッシュボードにアラートメッセージが表示されます。プラットフォームサービスのエンドポイントページに移動して、エラーの詳細を確認できます。


 One or more endpoints have experienced an error and might not be functioning properly. Go to the [Endpoints](#) page to view the error details. The last error occurred 2 hours ago.

ダッシュボードに表示されるのと同じエラーは、[Platform services Endpoints]ページの上部にも表示されます。詳細なエラーメッセージを表示するには、次の手順を実行します

手順

1. エンドポイントのリストで、エラーが発生した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と、エラーが発生してからの経過時間が表示されます。赤の X アイコンを含むエラー  過去 7 日以内に発生しました。

## Overview ^

Display name:	<b>my-endpoint-2</b> 
Type:	<b>Search</b>
URI:	<b>http://10.96.104.30:9200</b>
URN:	<b>urn:sgws:es:::mydomain/sveloso/_doc</b>

Connection


Configuration

### Verify connection

Some errors might continue to appear after they are resolved. To see if an error is current or to force the removal of a resolved error, select **Test connection**.

Test connection

#### Last error details

 2 hours ago

Endpoint failure: Endpont has an AWS failure: RequestError: send request failed; caused by: url.Error; caused by: net:OpError; caused by: os.SyscallError (logID: 143H5UDUUKMGDRWJ)

エラーがまだ最新であるかどうかを確認します

一部のエラーは、解決後も「\* Last error \*」列に引き続き表示される場合があります。エラーが現在発生しているかどうかを確認したり、解決済みのエラーをテーブルから強制的に削除したりするには、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。

[接続のテスト \*] 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すること、および現在のクレデンシャル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。

100

## エンドポイントエラーの解決

エンドポイントの詳細ページの「\* Last error \*」メッセージを使用して、エラーの原因を特定できます。一部のエラーでは、問題を解決するためにエンドポイントの編集が必要になります。たとえば、StorageGRID に正しいアクセス権限がないか、アクセスキーが期限切れになっているためにデスティネーションの S3 バケットにアクセスできない場合、CloudMirror のエラーが発生することがあります。メッセージは「Either the endpoint credentials or the destination access needs to be updated」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、「\* 変更のテストと保存 \*」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、現在のクレデンシャルで到達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の設定を編集します。
4. 接続 > 接続テスト \* を選択します。

### 必要な権限がないエンドポイントクレデンシャルです

StorageGRID によるプラットフォームサービスエンドポイントの検証では、エンドポイントのクレデンシャルを使用してデスティネーションリソースに接続できること、および基本的な権限チェックを実行できることが確認されます。ただし、StorageGRID では、特定のプラットフォームサービス処理に必要なすべての権限が検証されるわけではありません。そのため、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）が表示された場合は、エンドポイントのクレデンシャル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します"](#)
- ["プラットフォームサービスエンドポイントの接続をテストします"](#)
- ["プラットフォームサービスエンドポイントを編集します"](#)

## CloudMirror レプリケーションを設定します

。 ["CloudMirror レプリケーションサービス"](#) は、3 つの StorageGRID プラットフォームサービスのうちの 1 つです。CloudMirror レプリケーションを使用すると、外部の S3 バケットにオブジェクトを自動的にレプリケートできます。

### 作業を開始する前に

- テナントアカウントのプラットフォームサービスがStorageGRID 管理者によって有効にされている。
- レプリケーションソースとして機能するバケットがすでに作成されている。
- CloudMirrorレプリケーションのデスティネーションとして使用するエンドポイントがすでに存在し、そのURNが必要です。
- が設定されたユーザグループに属している必要があります ["すべてのバケットまたはRoot Access権限を管理します"](#)。これらの権限は、Tenant Manager を使用してバケットを設定する際にグループポリシーまた

はバケットポリシーの権限設定よりも優先されます。

このタスクについて

CloudMirror レプリケーションでは、ソースバケットからエンドポイントで指定されたデスティネーションバケットにオブジェクトがコピーされます。



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重要な類似点と相違点があります。詳細については、を参照してください "[グリッド間レプリケーションとCloudMirrorレプリケーションを比較してください](#)"。

バケットで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設定XMLを作成して適用する必要があります。レプリケーション設定 XML では、各デスティネーションとして 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なソースバケットまたはデスティネーションバケットでは、レプリケーションはサポートされません。

バケットレプリケーションとその設定方法の一般的な情報については、を参照してください "[Amazon Simple Storage Service \(S3\) のドキュメント：「オブジェクトのレプリケート](#)". StorageGRID で `GetBucketReplication`、`DeleteBucketReplication`、および `PutBucketReplication` の実装方法については、を参照してください "[バケットの処理](#)".

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が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した場合は、デスティネーション S3 エンドポイントに対して処理を実行する際に StorageGRID でそのクラスが使用されます。指定したストレージクラスは、デスティネーションエンドポイントでもサポートされている必要があります。デスティネーションシステムのベンダーからの推奨事項がある場合は、それに準拠してください。

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。

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設定 XML をテキストエディタで作成します。XML を設定する場合は、次の点に

- StorageGRID では、V1 のレプリケーション設定のみがサポートされます。つまり、StorageGRID では、の使用はサポートされていません `Filter` ルールのエレメント。V1の規則に従ってオブジェクトバージョンを削除します。詳細については、レプリケーション設定に関する Amazon のドキュメントを参照してください。
- デスティネーションとして S3 バケットエンドポイントの URN を使用してください。
- 必要に応じてを追加します `<StorageClass>` エレメントを選択し、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、が表示されます `STANDARD` ストレージクラスが使用されている。
  - `STANDARD_IA`：（標準-アクセス頻度の低いアクセス）このストレージクラスは、アクセス頻度は低いが、必要に応じて高速アクセスが必要なデータに使用します。
  - `REDUCED_REDUNDANCY`：重大度が低く、再現可能で、かつ冗長性に劣る状態で保存可能なデータには、このストレージクラスを使用します `STANDARD` ストレージクラス。



- を指定する場合 Role 設定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. ダッシュボードで\* View Buckets を選択するか、 storage (S3) > Buckets \*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. レプリケーション設定 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。

Bucket options      Bucket access      Platform services

---

**Replication**      Disabled      ^

Enable the CloudMirror replication service to copy objects from a source bucket to a destination bucket that is specified in an endpoint.

- Platform services must be enabled for your tenant account by a StorageGRID administrator.
- You must have already configured an endpoint for each destination bucket.
- You must specify the URN of each endpoint in the replication configuration XML for the source bucket.

Enable replication

Clear

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

Save changes



StorageGRID 管理者がグリッドマネージャまたはグリッド管理 API を使用して各テナントアカウントのプラットフォームサービスを有効にしておく必要があります。設定 XML の保存時にエラーが発生した場合は、StorageGRID 管理者にお問い合わせください。

7. レプリケーションが正しく設定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レプリケートされます。
  - b. オブジェクトがデスティネーションバケットにレプリケートされたことを確認します。

サイズの小さいオブジェクトについては、レプリケーションの所要時間が短くなります。

## 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します"](#)

## イベント通知を設定する

通知サービスは、3つの StorageGRID プラットフォームサービスのうちの1つです。バケットの通知を有効にすると、指定したイベントに関する情報をAWS Simple Notification Service (Amazon SNS) をサポートするデスティネーションKafkaクラスタまたはサービスに送信できます。

### 作業を開始する前に

- テナントアカウントのプラットフォームサービスがStorageGRID 管理者によって有効にされている。
- 通知のソースとして機能するバケットを作成しておきます。
- イベント通知のデスティネーションとして使用するエンドポイントがすでに存在し、URNが設定されている必要があります。
- が設定されたユーザグループに属している必要があります ["すべてのバケットまたはRoot Access権限を管理します"](#)。これらの権限は、Tenant Manager を使用してバケットを設定する際にグループポリシーまたはバケットポリシーの権限設定よりも優先されます。

### このタスクについて

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で指定したイベントが発生するたびに通知が生成され、デスティネーションエンドポイントとして使用されているAmazon SNSまたはKafkaトピックに送信されます。バケットの通知を有効にするには、有効な通知設定 XML を作成して適用する必要があります。通知設定 XML では、各デスティネーションとして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。

イベント通知とその設定方法の一般的な情報については、Amazonのドキュメントを参照してください。StorageGRIDでS3バケットの通知設定APIを実装する方法については、[を参照してください。"S3 クライアントアプリケーションを実装するための手順"](#)。

オブジェクトを含むあるバケットのイベント通知を有効にした場合、通知は通知設定の保存後に実行された処理に対してのみ送信されます。

### 手順

1. ソースバケットの通知を有効にします。
  - イベント通知を有効にするために必要な通知設定 XML を、S3 通知 API で指定されている内容に従ってテキストエディタで作成します。
  - XML を設定するにあたっては、デスティネーショントピックとしてイベント通知エンドポイントの URN を使用します。

```
<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. Tenant Manager で、 \* Storage ( S3 ) \* > \* Buckets \* 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オンにします。

6. 通知設定 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。

Bucket options    Bucket access    Platform services    S3 Console

Replication    Disabled

Event notifications    Disabled

Enable the event notification service for an S3 bucket if you want StorageGRID to send notifications about specified events to a destination Amazon Simple Notification Service (SNS) or a destination Apache Kafka cluster.

- Platform services must be enabled for your tenant account by a StorageGRID administrator.
- You must have already configured an endpoint for the destination of event notifications.
- You must specify the URN of that endpoint in the notification configuration XML for the source bucket.

Enable event notifications

Clear

```
<NotificationConfiguration>
  <TopicConfiguration>
    <Id>Image-created</Id>
    <Filter>
      <S3Key>
        <FilterRule>
          <Name>prefix</Name>
          <Value>images</Value>
        </FilterRule>
      </S3Key>
    </Filter>
  </TopicConfiguration>
</NotificationConfiguration>
```

Save changes



StorageGRID 管理者がグリッドマネージャまたはグリッド管理 API を使用して各テナントアカウントのプラットフォームサービスを有効にしておく必要があります。設定 XML の保存時にエラーが発生した場合は、StorageGRID 管理者にお問い合わせください。

7. イベント通知が正しく設定されていることを確認します。

- 設定 XML で設定した通知をトリガーする要件を満たす操作をソースバケット内のオブジェクトに対して実行します。

この例では、を使用して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/ プレフィックス。

b. デスティネーションのAmazon SNSまたはKafkaトピックに通知が配信されたことを確認します。

たとえば、デスティネーショントピックが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E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": "11111111111111111111"
      },
      "requestParameters": {
        "sourceIPAddress": "193.51.100.20"
      },
      "responseElements": {
        "x-amz-request-id": "122047343"
      },
      "s3": {
        "s3SchemaVersion": "1.0",
        "configurationId": "Image-created",
        "bucket": {
          "name": "test1",
          "ownerIdentity": {
            "principalId": "11111111111111111111"
          },
          "arn": "arn:sgws:s3:::test1"
        },
        "object": {
          "key": "images/cat.jpg",
          "size": 0,
          "eTag": "d41d8cd98f00b204e9800998ecf8427e",
          "sequencer": "14D90402421461C7"
        }
      }
    }
  ]
}
```

+ デスティネーショントピックに通知が届いた場合は、StorageGRID 通知のソースバケットが正しく設定されています。

["バケットの通知について理解します"](#)

["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します"](#)

## 検索統合サービスを使用する

検索統合サービスは、3つの StorageGRID プラットフォームサービスのうちの1つです。このサービスを有効にすると、オブジェクトが作成、削除されたとき、またはそのメタデータやタグが更新されたときに、デスティネーションの検索インデックスにオブジェクトメタデータを送信できます。

テナントマネージャを使用して検索統合を設定し、カスタム StorageGRID 設定 XML をバケットに適用できます。



検索統合サービスではオブジェクトメタデータがデスティネーションに送信されるため、その設定 XML は `_メタデータ通知設定.xml` と呼ばれます。この設定 XML は、イベント通知を有効にするための `_通知設定.xml` とは異なります。

を参照してください ["S3 クライアントアプリケーションを実装するための手順"](#) 次のカスタムの StorageGRID S3 REST API 処理の詳細については、以下を参照してください。

- バケットのメタデータ通知設定を削除します
- GET Bucket metadata notification configuration
- PUT Bucket metadata notification configuration のコマンドです

### 関連情報

["検索統合用の XML を設定します"](#)

["メタデータ通知に含まれているオブジェクトメタデータ"](#)

["検索統合サービスで生成される JSON"](#)

["検索統合サービスを設定する"](#)

["S3 REST APIを使用する"](#)

### 検索統合用の XML を設定します

検索統合サービスは、内に含まれる一連のルールを使用して設定します

```
<MetadataNotificationConfiguration> および  
</MetadataNotificationConfiguration> タグ。各ルールは、ルール環境で指定されたオブジェクト、および StorageGRID からそのオブジェクトのメタデータを送信するデスティネーションを指定します。
```

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、`images` というプレフィックスのオブジェクトのメタデータを送信できます `images` を1つのデスティネーションに、プレフィックスがの

オブジェクトのメタデータに追加します videos 別のノードに移動しますプレフィックスが重複している設定は有効ではなく、送信時に拒否されます。たとえば、プレフィックスがオブジェクトに対するルールを1つ含む設定です test プレフィックスが付いたオブジェクトの2番目のルールです test2 は許可されていません。

デスティネーションは、検索統合サービス用に作成された StorageGRID エンドポイントの URN を使用して指定する必要があります。これらのエンドポイントは、Elasticsearch クラスタ上に定義されているインデックスとタイプを参照します。

```
<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>rule-status</Status>
    <Prefix>key-prefix</Prefix>
    <Destination>
      <Urn>arn:aws:es:region:account-
ID:domain/mydomain/myindex/mytype</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Rule-2</ID>
    ...
  </Rule>
  ...
</MetadataNotificationConfiguration>
```

次の表に、メタデータ通知設定 XML の要素を示します。

名前	説明	必須
MetadataNotificationConfiguration のページです	メタデータ通知でオブジェクトとデスティネーションの指定に使用されるルール用のテナントタグ。  1 つ以上の Rule 要素を含みます。	はい。
ルール	指定したインデックスにメタデータを追加する必要があるオブジェクトを特定するルール用のテナントタグ。  プレフィックスが重複しているルールは拒否されます。  MetadataNotificationConfiguration 要素に含まれています。	はい。
ID	ルールの一意的識別子。  Rule 要素に含まれています。	いいえ



名前	説明	必須
ステータス	<p>Status には「Enabled」または「Disabled」を指定できません。無効になっているルールについては操作が実行されません。</p> <p>Rule 要素に含まれています。</p>	はい。
プレフィックス	<p>プレフィックスと一致するオブジェクトにルールが適用され、そのメタデータが指定したデスティネーションに送信されます。</p> <p>すべてのオブジェクトを照合するには、空のプレフィックスを指定します。</p> <p>Rule 要素に含まれています。</p>	はい。
宛先	<p>ルールのデスティネーションのコンテナタグ。</p> <p>Rule 要素に含まれています。</p>	はい。
URN	<p>オブジェクトメタデータが送信されるデスティネーションの URN。次のプロパティを持つ StorageGRID エンドポイントの URN を指定する必要があります。</p> <ul style="list-style-type: none"> <li>• es 3番目のエレメントである必要があります。</li> <li>• URNの末尾に、メタデータが格納されるインデックスとタイプを、の形式で指定する必要があります domain-name/myindex/mytype。</li> </ul> <p>エンドポイントは、Tenant Manager またはテナント管理 API を使用して設定します。形式は次のとおりです。</p> <ul style="list-style-type: none"> <li>• arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype</li> <li>• urn:mysite:es:::mydomain/myindex/mytype</li> </ul> <p>エンドポイントは設定 XML を送信する前に設定する必要があります。そうしないと、404 エラーで設定が失敗します。</p> <p>Urn は Destination 要素に含まれています。</p>	はい。

サンプルのメタデータ通知設定 XML を使用して、独自の XML を作成する方法を確認できます。

メタデータ通知設定：環境 のすべてのオブジェクトを対象にした設定です

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デスティネーションに送信されます。

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

## 2つのルールを含むメタデータ通知設定

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を指定します /images が1つのデスティネーションに送信され、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が送信されます /videos 2番目の送信先に送信されます。

```
<MetadataNotificationConfiguration>
  <Rule>
    <ID>Images-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/images</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-1:33333333: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>
```

## 関連情報

["S3 REST APIを使用する"](#)

"メタデータ通知に含まれているオブジェクトメタデータ"

"検索統合サービスで生成される JSON"

"検索統合サービスを設定する"

検索統合サービスを設定します

検索統合サービスでは、オブジェクトが作成、削除、またはそのメタデータ / タグが更新されるたびに、デスティネーションの検索インデックスにオブジェクトメタデータが送信されます。

作業を開始する前に

- テナントアカウントのプラットフォームサービスがStorageGRID 管理者によって有効にされている。
- コンテンツにインデックスを付けるS3バケットを作成しておきます。
- 検索統合サービスのデスティネーションとして使用するエンドポイントがすでに存在し、URNが設定されている必要があります。
- が設定されたユーザグループに属している必要があります ["すべてのバケットまたはRoot Access権限を管理します"](#)。これらの権限は、Tenant Manager を使用してバケットを設定する際にグループポリシーまたはバケットポリシーの権限設定よりも優先されます。

このタスクについて

ソースバケットに対して検索統合サービスを設定した場合、オブジェクトを作成またはオブジェクトのメタデータ / タグを更新すると、オブジェクトメタデータがデスティネーション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で検索統合サービスを有効にすると、既存のオブジェクトに関するメタデータ通知は自動的に送信されません。既存のオブジェクトのメタデータがデスティネーションの検索インデックスに追加されるようにするには、オブジェクトを更新する必要があります。

手順

1. 検索統合を有効にするために必要なメタデータ通知 XML をテキストエディタで作成します。
  - 検索統合用の設定 XML に関する情報を参照してください。
  - XML を設定するにあたっては、デスティネーションとして検索統合エンドポイントの URN を使用します。

```
<MetadataNotificationConfiguration>
  <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-
1:1111111111111111:domain/mydomain/myindex/mytype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

2. Tenant Manager で、 \* Storage ( S3 ) \* > \* Buckets \* 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オンにします。

6. テキストボックスにメタデータ通知設定を貼り付け、 \* 変更を保存 \* を選択します。

The screenshot shows the 'Platform services' tab with three sections: 'Replication' (Disabled), 'Event notifications' (Disabled), and 'Search integration' (Disabled). The 'Search integration' section is expanded, showing instructions and a checked checkbox for 'Enable search integration'. Below the checkbox is a text area containing the following XML configuration:

```
<MetadataNotificationConfiguration>
  <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-1:111111111111:domain/mydomain/myindex/mytype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

A 'Clear' button is located to the right of the text area, and a 'Save changes' button is at the bottom right of the 'Search integration' section.



StorageGRID 管理者がグリッドマネージャまたは管理 API を使用して各テナントアカウントのプラットフォームサービスを有効にしておく必要があります。設定 XML の保存時にエラーが発生した場合は、StorageGRID 管理者にお問い合わせください。

7. 検索統合サービスが正しく設定されていることを確認します。
  - a. 設定 XML で指定されたメタデータ通知をトリガーする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がメタデータ通知をトリガーします。
  - 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。

完了後

必要に応じて、次のいずれかの方法でバケットの検索統合を無効にできます。

- Storage (S3) > Buckets を選択し、Enable search integration \*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 メタデータ通知要求を使用します。S3 クライアントアプリケーションを実装する手順を参照してください。

関連情報

["検索統合サービスについて理解する"](#)

["検索統合用の XML を設定します"](#)

["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します"](#)

検索統合サービスで生成される **JSON**

バケットで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の追加、更新、削除が行われるたびに、JSON ドキュメントが生成されてデスティネーションエンドポイントに送信されます。

次の例は、キーを含むオブジェクトの場合に生成されるJSONを示しています。SGWS/Tagging.txt は、という名前のバケットに作成されます test。 test バケットはバージョン管理されていないため、を使用します 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"
  }
}

```

メタデータ通知に含まれているオブジェクトメタデータ

次の表に、検索統合が有効になっている場合にデスティネーションエンドポイントに送信される JSON ドキュメント内のすべてのフィールドを示します。

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。

を入力します	項目名と概要
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: バージョン管理されたバケット内のオブジェクトのオブジェクトバージョン
region: バケットリージョンなど 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のサイズ(バイト単位)	md5: オブジェクトハッシュ
ユーザメタデータ	metadata: オブジェクトのすべてのユーザメタデータをキーと値のペアとして格納  key: value

を入力します	項目名と概要
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をキーと値のペアとして使用します  key:value



タグとユーザメタデータの場合、StorageGRID は文字列または S3 イベント通知として Elasticsearch に日付と番号を渡します。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 を設定するには、動的フィールドマッピングおよびマッピング日付形式に関する Elasticsearch の手順に従ってください。検索統合サービスを設定する前に、インデックスの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作成後は、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 © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

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

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

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

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

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

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

## 商標に関する情報

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