



## テナントアカウントを使用する StorageGRID

NetApp  
October 03, 2025

# 目次

テナントアカウントを使用する	1
Tenant Managerを使用します	1
StorageGRID テナントアカウントを使用する	1
Web ブラウザの要件	3
Tenant Managerにサインインします	3
Tenant Managerからサインアウトします	6
Tenant Managerのダッシュボードについて	7
テナント管理APIについて	10
テナントユーザのシステムアクセスの管理	16
アイデンティティフェデレーションを使用する	16
グループの管理	21
ローカルユーザの管理	35
S3テナントアカウントの管理	39
S3 アクセスキーの管理	39
S3バケットの管理	49
S3プラットフォームサービスの管理	67
プラットフォームサービスとは	67
プラットフォームサービスの使用に関する考慮事項	73
プラットフォームサービスエンドポイントの設定	75
CloudMirrorレプリケーションの設定	93
イベント通知を設定する	97
検索統合サービスを使用する	101

# テナントアカウントを使用する

StorageGRID テナントアカウントの使用方法について説明します。

- ・ "Tenant Managerを使用します"
- ・ "テナントユーザのシステムアクセスの管理"
- ・ "S3テナントアカウントの管理"
- ・ "S3プラットフォームサービスの管理"

## Tenant Managerを使用します

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

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

## StorageGRID テナントアカウントを使用する

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

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

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

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



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

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

## テナントアカウントの作成

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

- ・テナントの表示名（テナントのアカウント ID は自動的に割り当てられ、変更できません）。
- ・テナントアカウントが S3 と Swift のどちらを使用するか。
- ・S3 テナントアカウントの場合：テナントアカウントにプラットフォームサービスの使用を許可するかどうか。プラットフォームサービスの使用が許可されている場合は、グリッドがその使用をサポートするように設定されている必要があります。
- ・必要に応じて、テナントアカウントのストレージクォータ—テナントのオブジェクトで使用可能な最大ギガバイト数、テラバイト数、ペタバイト数。テナントのストレージクォータは、物理容量（ディスクのサイズ）ではなく、論理容量（オブジェクトのサイズ）を表します。
- ・StorageGRID システムでアイデンティティフェデレーションが有効になっている場合は、テナントアカウントを設定するための Root Access 権限が割り当てられているフェデレーテッドグループ。
- ・StorageGRID システムでシングルサインオン（SSO）が使用されていない場合は、テナントアカウントが独自のアイデンティティソースを使用するか、グリッドのアイデンティティソースを共有するか、およびテナントのローカル root ユーザの初期パスワード。

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

## S3テナントを設定する

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

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



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

## Swiftテナントを設定します

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

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



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

## 関連情報

["StorageGRID の管理"](#)

["S3 を使用する"](#)

["Swift を使用します"](#)

## Web ブラウザの要件

サポートされている Web ブラウザを使用する必要があります。

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

ブラウザウィンドウの幅を推奨される値に設定してください。

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

## Tenant Managerにサインインします

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

### 必要なもの

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

`https://FQDN_or_Admin_Node_IP/`

`https://FQDN_or_Admin_Node_IP:port/`

`https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id`

`https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id`

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

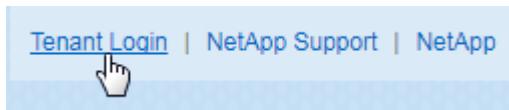
- URL に 20 術のテナントアカウント ID が含まれていない場合は、このアカウント ID を確認しておく必要があります。
- サポートされている Web ブラウザを使用する必要があります。
- Web ブラウザでクッキーが有効になっている必要があります。
- 特定のアクセス権限が必要です。

#### 手順

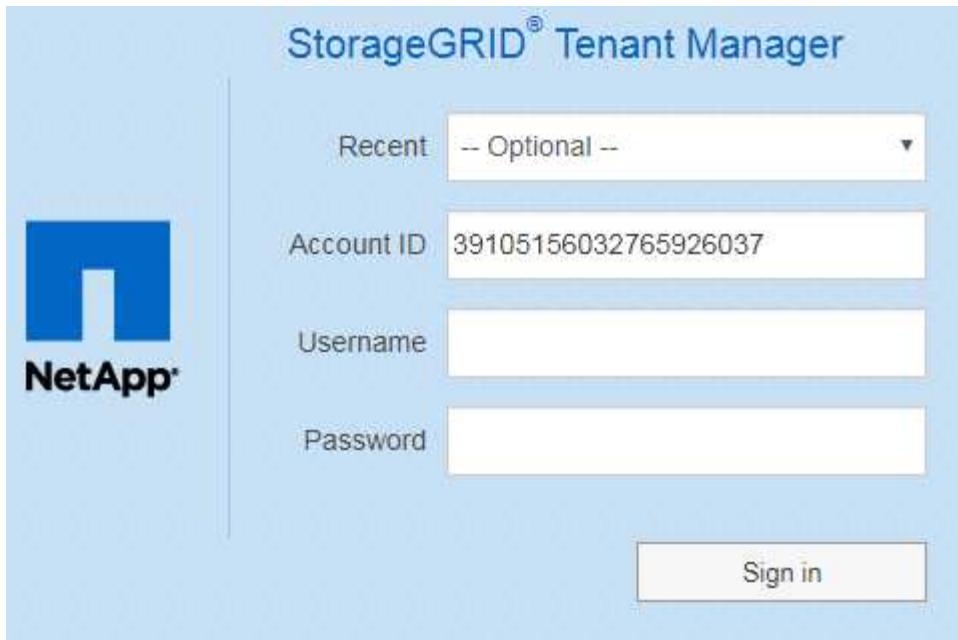
1. サポートされている Web ブラウザを起動します。
2. ブラウザのアドレスバーに、 Tenant Manager にアクセスするための URL を入力します。
3. セキュリティアラートが表示された場合は、ブラウザのインストールウィザードを使用して証明書をインストールします。
4. Tenant Manager にサインインします。

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

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



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



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

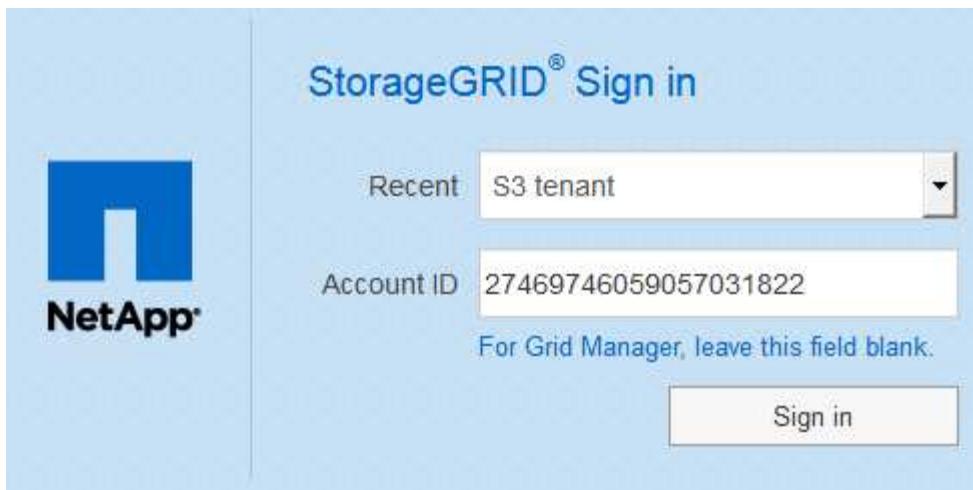
Tenant Manager のダッシュボードが表示されます。

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

The image shows a sign-in form for an organizational account. It has a white background with a thin black border. At the top, it says "Sign in with your organizational account". Below that is an input field with the placeholder "someone@example.com". Underneath is another input field with the placeholder "Password". At the bottom is a blue "Sign in" button.

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

- Tenant Manager の SSO サインインページ。



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

Tenant Manager のダッシュボードが表示されます。

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



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

#### 関連情報

["StorageGRID の管理"](#)

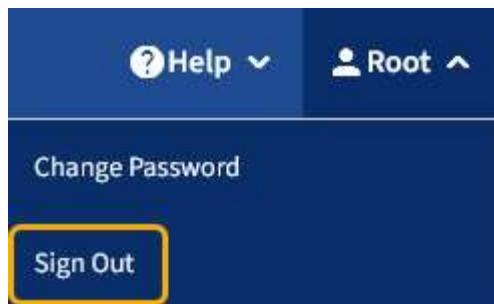
["Web ブラウザの要件"](#)

#### Tenant Manager からサインアウトします

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

#### 手順

1. ユーザインターフェイスの右上にあるユーザ名ドロップダウンを探します。



2. ユーザー名を選択し、\* サインアウト \* を選択します。

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

## Tenant Managerのダッシュボードについて

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



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

オブジェクトがアップロードされると、ダッシュボードは次のようにになります。

# Dashboard

**16** Buckets  
[View buckets](#)

**2** Platform services endpoints  
[View endpoints](#)

**0** Groups  
[View groups](#)

**1** User  
[View users](#)

## Storage usage [?](#)

6.5 TB of 7.2 TB used

0.7 TB (10.1%) remaining



Bucket name	Space used	Number of objects
Bucket-15	969.2 GB	913,425
Bucket-04	937.2 GB	576,806
Bucket-13	815.2 GB	957,389
Bucket-06	812.5 GB	193,843
Bucket-10	473.9 GB	583,245
Bucket-03	403.2 GB	981,226
Bucket-07	362.5 GB	420,726
Bucket-05	294.4 GB	785,190
8 other buckets	1.4 TB	3,007,036

## Total objects

8,418,886  
objects

## Tenant details

Name	Human Resources
ID	4955 9096 9804 4285 4354

 View the instructions for Tenant Manager.

[Go to documentation](#) 

## テナントアカウントの概要

ダッシュボードの上部には、次の情報が表示されます。

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

リンクを選択すると詳細を確認できます。

ダッシュボードの右側には、次の情報が表示されます。

- テナントのオブジェクトの合計数。

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

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

## ストレージとクォータの使用状況

ストレージ使用状況パネルには、次の情報が表示されます。

- テナントのオブジェクトデータの量。



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

- クオ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。クオータは、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。



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

- 最大のバケットまたはコンテナの相対サイズを表す棒グラフ。

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



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

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

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

## クオータ使用状況アラート

Grid Manager でクオータ使用アラートが有効になっている場合、クオ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。

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

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

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

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



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

## エンドポイントエラー

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



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.

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

### 関連情報

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

["トラブルシューティングを監視します"](#)

## テナント管理APIについて

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

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

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

## 手順

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

## API 処理

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

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

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

認証セキュリティの向上については、「クロスサイトリクエストフォージェリに対する保護」を参照してください。



StorageGRID システムでシングルサインオン（SSO）が有効になっている場合は、別の手順による認証が必要です。StorageGRID の管理手順の「シングルサインオンが有効な場合のAPIへのサインイン」を参照してください。

- \*config\*—製品リリースとテナント管理 API のバージョンに関する操作。製品リリースバージョンおよびそのリリースでサポートされる API のメジャー・バージョンを一覧表示できます。
- \*containers\*—S3 バケットまたは Swift コンテナに対する次の処理。

プロトコル	許可するアクセス許可
S3	<ul style="list-style-type: none"><li>• 準拠バケットと非準拠バケットを作成する</li><li>• 古い準拠設定の変更</li><li>• オブジェクトに対して実行される処理の整合性制御を設定します</li><li>• バケットのCORS設定を作成、更新、および削除する</li><li>• オブジェクトの最終アクセス日時の更新の有効化と無効化</li><li>• CloudMirror レプリケーション、通知、検索統合（メタデータ通知）などのプラットフォームサービスの構成設定の管理</li><li>• 空のバケットを削除中</li></ul>
Swift	コンテナに使用する整合性レベルを設定します

- \* deactivated-features\*—非アクティブ化された可能性のある機能を表示する操作。
- \* endpoints\*—エンドポイントを管理するための処理。エンドポイントを使用することで、S3 バケットは外部のサービスを StorageGRID CloudMirror レプリケーション、通知、または検索統合に使用できます。
- \* groups\*—ローカルテナントグループを管理し、外部アイデンティティソースからフェデレーテッドテ

ナントグループを取得するための処理。

- **\* identity-source \***— 外部のアイデンティティソースを設定する処理、およびフェデレーテッドグループとユーザ情報を手動で同期する処理。
- **regions**— StorageGRID システムに設定されているリージョンを判別するための処理。
- **\* s3 \*** - テナントユーザの S3 アクセスキーを管理する処理。
- **\*s3-object-lock \***-- StorageGRID システムのグローバルなS3オブジェクトロック（準拠）の構成を確認する処理。
- **\* users \*** — テナントユーザーを表示および管理するための操作。

#### 処理の詳細

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

## groups Operations on groups

GET /org/groups Lists Tenant User Groups

### Parameters

Try it out

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

### Responses

Response content type

application/json

Code	Description
200	

Example Value Model

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

## API要求の実行



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

### 手順

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

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

#### 関連情報

["クロスサイトリクエストフォージェリ \(CSRF\) の防止"](#)

["StorageGRID の管理"](#)

#### テナント管理 API のバージョン管理

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

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

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

旧バージョンとの互換性がない `*_not compatible_*` の変更が行われると、テナント管理 API のメジャーバージョンが上がります。以前のバージョンと互換性がある `*` の変更を行うと、テナント管理 API のマイナーバージョンが上がります。互換性のある変更には、新しいエンドポイントやプロパティの追加などがあります。次の例は、変更のタイプに基づいて API バージョンがどのように更新されるかを示しています。

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

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

古い要求は、次の方法で廃止とマークされます。

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

現在のリリースでサポートされている API バージョンを確認します

サポートされている API のメジャーバージョンのリストを返すには、次の API 要求を使用します。

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

#### 要求のAPIバージョンの指定

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

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

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

#### クロスサイトリクエストフォージェリ (CSRF) の防止

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

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

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

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

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

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

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

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

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



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

## テナントユーザのシステムアクセスの管理

テナントアカウントへのアクセス権をユーザに付与するには、フェデレーテッドアイデンティティソースからグループをインポートして、管理権限を割り当てます。StorageGRID システム全体でシングルサインオン（SSO）が有効になっていない限り、ローカルテナントグループおよびユーザを作成することもできます。

- "アイデンティティフェデレーションを使用する"
- "グループの管理"
- "ローカルユーザの管理"

### アイデンティティフェデレーションを使用する

アイデンティティフェデレーションを使用すると、テナントグループと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。

- "フェデレーテッドアイデンティティソースを設定する"
- "アイデンティティソースとの強制同期"
- "アイデンティティフェデレーションの無効化"

### フェデレーテッドアイデンティティソースを設定する

テナントグループとユーザをActive Directory、OpenLDAP、Oracle Directory Serverなどの別のシステムで管理する場合は、アイデンティティフェデレーションを設定できます。

### 必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。

- ・特定のアクセス権限が必要です。
- ・アイデンティティプロバイダとしてActive Directory、OpenLDAP、またはOracle Directory Serverを使用している必要があります。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。
- ・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。

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。アイデンティティフェデレーションページにアクセスしたときにこのメッセージが表示される場合は、このテナント用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.

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サービスのタイプセクションで、\* Active Directory 、 OpenLDAP 、または Other \*を選択します。

OpenLDAP \*を選択した場合は、OpenLDAPサーバを設定します。OpenLDAPサーバの設定に関するガイドラインを参照してください。

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。
  - \* User Unique Name \* : LDAP ユーザの一意な ID が含まれている属性の名前。この属性はと同じです 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。この属性はと同じです 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 衡の 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 グループの一意な ID が含まれている属性の名前。この属性はと同じです 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。この属性はと同じです 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 衡の 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. Configure LDAP server (LDAPサーバの設定) セクションで、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サーバのホスト名または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
- \* Password \* : ユーザ名に関連付けられたパスワード。
  - \* 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\*グループのベース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。

#### 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（推奨）\* : STARTTLSを使用してLDAPサーバとの通信を保護します。これが推奨されるオプションです。
- \* 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。このオプションは互換性を確保するためにサポートされています。
- \* 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。

Active DirectoryサーバでLDAP署名を適用する場合は、このオプション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。

#### 8. 「接続のテスト」を選択して、LDAPサーバーの接続設定を検証します。

接続が有効な場合は、ページの右上に確認メッセージが表示されます。

9. 接続が有効な場合は、\*保存\*を選択します。

次のスクリーンショットは、Active Directoryを使用するLDAPサーバの設定例を示しています。

**LDAP service type**

Select the type of LDAP service you want to configure.

**Active Directory**   **OpenLDAP**   **Other**

**Configure LDAP server** (All fields are required)

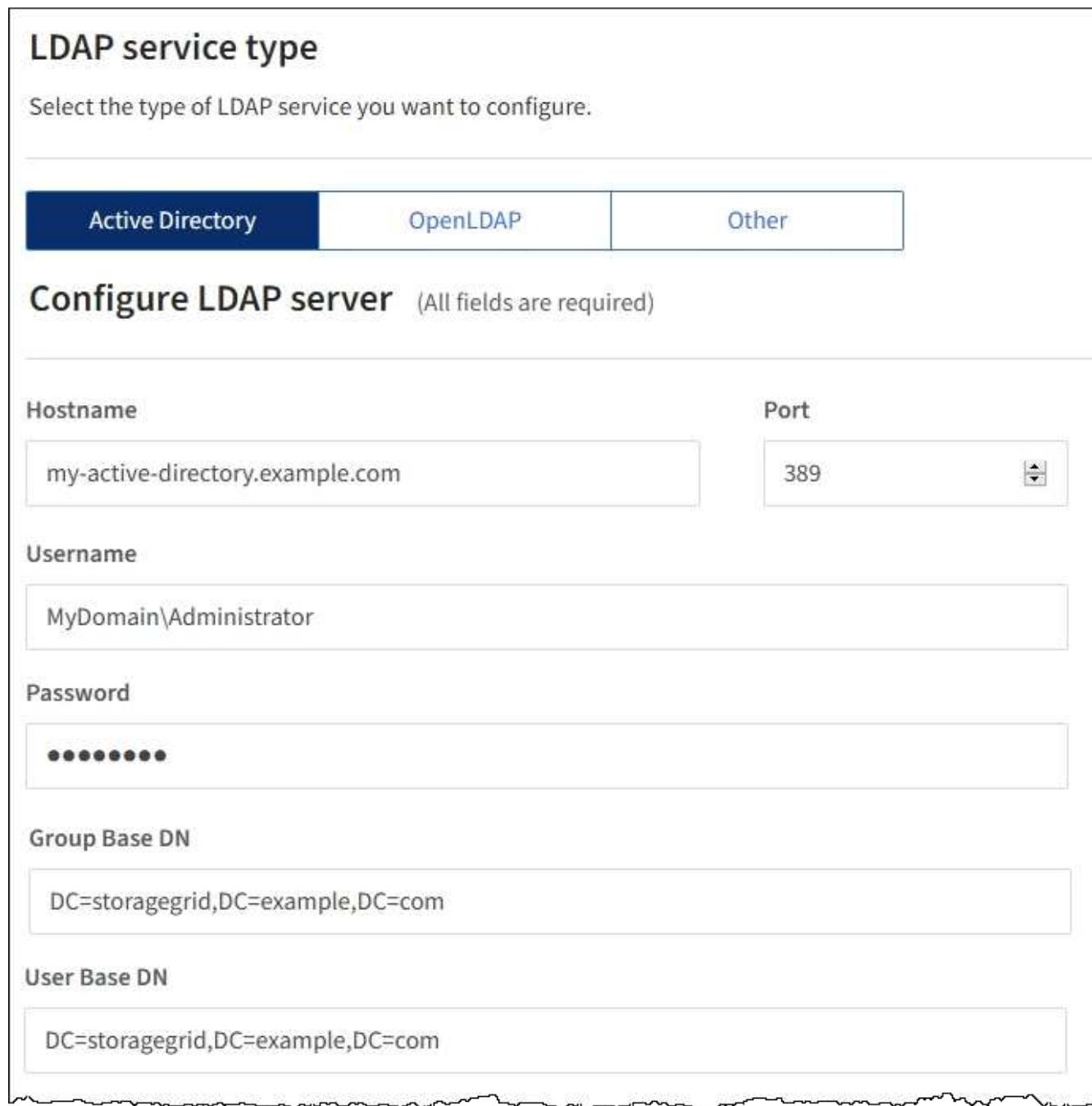
**Hostname**   **Port**  
my-active-directory.example.com   389

**Username**  
MyDomain\Administrator

**Password**  
\*\*\*\*\*

**Group Base DN**  
DC=storagegrid,DC=example,DC=com

**User Base DN**  
DC=storagegrid,DC=example,DC=com



#### 関連情報

["テナント管理権限"](#)

["OpenLDAP サーバの設定に関するガイドライン"](#)

[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。

## 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、OpenLDAPの管理者ガイド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。

### 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。

OpenLDAPの管理者ガイド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。

### 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。

#### 必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。
- 保存されたアイデンティティソースが有効になっている必要があります。

#### 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。

アイデンティティフェデレーションページが表示されます。「サーバーの同期」ボタンは、ページの右上にあります。



保存されているアイデンティティソースが有効になっていない場合、\*サーバーの同期\*ボタンはアクティブになりません。

2. 「サーバーの同期」を選択します。

同期が開始されたことを示す確認メッセージが表示されます。

#### 関連情報

["テナント管理権限"](#)

## アイデンティティフェデレーションの無効化

この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した場合は、テナント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なると、StorageGRID システム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。

### 必要なもの

- Tenant Manager にはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

### 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テナントアカウントにアクセスしたままとなります。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ません。

### 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] チェックボックスをオフにします。
3. [保存 (Save)] を選択します。

### 関連情報

["テナント管理権限"](#)

## グループの管理

テナントユーザが実行できるタスクを制御するには、ユーザグループに権限を割り当てます。Active Directory や OpenLDAP などの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ことも、ローカルグループを作成することもできます。



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、ローカルユーザはテナントマネージャにサインインできません。ただし、グループの権限に基づいて S3 リソースと Swift リソースにアクセスすることはできます。

### テナント管理権限

テナントグループを作成する前に、そのグループに割り当てる権限を検討してください。テナント管理権限は、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に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。キャッシングに時間がかかるため変更には最大で 15 分を要します。

アクセス権	説明
ルートアクセス（Root Access）	Tenant Manager とテナント管理 API へのフルアクセスを提供します。 <ul style="list-style-type: none"><li>・注：* 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。</li></ul>
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 <ul style="list-style-type: none"><li>・注：* Swift ユーザが Swift REST API を使用して処理を実行するには、Swift 管理者の権限が必要です。</li></ul>
自分の S3 クレデンシャルを管理します	S3 テナントのみ。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。この権限を持たないユーザには、「* storage ( S3 ) * > * My S3 access keys *」メニューオプションは表示されません。
すべてのバケットを管理します	<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、ユーザに Tenant Manager とテナント管理 API を使用して S3 バケットの作成と削除を許可し、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許可します。 この権限を持たないユーザには、Bucket メニューオプションは表示されません。</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 コンテナの整合性レベルを制御することを許可します。</li><li>・注：* テナント管理 API から Swift グループに割り当てるには、Manage All Buckets 権限だけです。この権限は、Tenant Manager を使用して Swift グループに割り当てるにはできません。</li></ul>

アクセス権	説明
エンドポイントを管理します	<p>S3 テナントのみ。ユーザが Tenant Manager 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エンドポイントを作成または編集できるようにします。</p> <p>この権限を持たないユーザーには、* プラットフォームサービスエンドポイント * メニューオプションは表示されません。</p>

## 関連情報

["S3 を使用する"](#)

["Swift を使用します"](#)

## S3テナント用のグループの作成

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。

### 必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限を持つユーザグループに属している必要があります。
- フェデレーテッドグループをインポートする場合は、アイデンティティフェデレーションを設定済みで、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ている必要があります。

### 手順

- \* access management \* > \* Groups \* を選択します。



Groups

Create and manage local and federated groups. Set group permissions to control access to specific pages and features.

2 groups

Create group

Actions	Name	ID	Type	Access mode
<input type="checkbox"/>	Applications	22cc2e27-88ee-4461-a8c6-30b550beeeec0	Local	Read-write
<input type="checkbox"/>	Managers	8b15b131-1d21-4539-93ad-f2298347c4d8	Local	Read-write

← Previous 1 Next →

- 「\* グループを作成 \*」を選択します。

3. [ 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。

4. 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の場合には、に関連付けられている一意の名前です uid 属性 (Attribute) :

5. 「 \* Continue \* 」を選択します。

6. アクセスモードを選択します。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に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。

- \* Read-Write \* (デフォルト) : ユーザは Tenant Manager にログインしてテナントの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、変更や処理を実行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。

7. このグループのグループ権限を選択します。

テナント管理権限に関する情報を参照してください。

8. 「 \* Continue \* 」を選択します。

9. グループポリシーを選択して、このグループのメンバーに付与する S3 アクセス権限を決定します。

- \* S3 アクセスなし \* : 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。
- \* 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。
- \* 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。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、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。

10. 「 \* 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。

この例では、指定したバケット内のユーザ名（キープレフィックス）に一致するフォルダの表示とアクセスのみがグループのメンバーに許可されます。これらのフォルダのプライバシー設定を決めるときは、他のグループポリシーやバケットポリシーのアクセス権限を考慮する必要があります。

No S3 Access

Read Only Access

Full Access

Custom  
(Must be a valid JSON formatted string.)

```
{
  "Statement": [
    {
      "Sid": "AllowListBucketOfASpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3>ListBucket",
      "Resource": "arn:aws:s3:::department-bucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "${aws:username}/*"
        }
      }
    },
    {
      "Sid": "AllowUserSpecificActionsOnlyInTheSpecificFolder",
      "Effect": "Allow",
      "Action": "s3:*Object",
      "Resource": "arn:aws:s3:::department-bucket/${aws:username}/*"
    }
  ]
}
```

11. フェデレーテッドグループとローカルグループのどちらを作成するかに応じて、表示されるボタンを選択します。

- フェデレーテッドグループ： \* グループを作成 \*
- ローカルグループ： \* 続行 \*

ローカルグループを作成している場合は、「\* Continue \*」を選択すると、ステップ 4（ユーザーの追加）が表示されます。この手順は、フェデレーテッドグループに対しては表示されません。

12. グループに追加する各ユーザーのチェックボックスをオンにし、 \* グループの作成 \* を選択します。

必要に応じて、ユーザを追加せずにグループを保存することもできます。後でグループにユーザを追加することも、新しいユーザを追加するときにグループを選択することもできます。

13. [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。キャッシングに時間がかかるため変更には最大で 15 分を要します。

#### 関連情報

["テナント管理権限"](#)

["S3 を使用する"](#)

#### Swift テナント用のグループの作成

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。

#### 必要なもの

- Tenant Manager にはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限を持つユーザグループに属している必要があります。
- フェデレーテッドグループをインポートする場合は、アイデンティティフェデレーションを設定済みで、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ている必要があります。

#### 手順

1. \* access management \* > \* Groups \* を選択します。



Name	ID	Type	Access mode
Applications	22cc2e27-88ee-4461-a8c6-30b550beeeec0	Local	Read-write
Managers	8b15b131-1d21-4539-93ad-f2298347c4d8	Local	Read-write

2. 「\* グループを作成 \*」を選択します。
  3. [ 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。
4. 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) :
  5. 「\* Continue \*」を選択します。
  6. アクセスマードを選択します。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

用に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。

- \* Read-Write \* (デフォルト) : ユーザは Tenant Manager にログインしてテナントの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、変更や処理を実行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。

7. グループ権限を設定します。

- 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オンにします。 (デフォルト)
- ユーザが Tenant Manager またはテナント管理 API にアクセスする必要がない場合は、 \* Root Access \* チェックボックスをオフにします。たとえば、テナントにアクセスする必要がないアプリケーションのチェックボックスをオフにします。次に、 \* Swift Administrator \* 権限を割り当てて、これらのユーザにコンテナとオブジェクトの管理を許可します。

8. 「 \* Continue \* 」を選択します。

9. Swift REST API を使用する必要がある場合は、 \* Swift 管理者 \* チェックボックスを選択します。

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

10. フェデレーテッドグループとローカルグループのどちらを作成するかに応じて、表示されるボタンを選択します。

- フェデレーテッドグループ： \* グループを作成 \*
- ローカルグループ： \* 続行 \*

ローカルグループを作成している場合は、「 \* Continue \* 」を選択すると、ステップ 4 (ユーザーの追加) が表示されます。この手順は、フェデレーテッドグループに対しては表示されません。

11. グループに追加する各ユーザーのチェックボックスをオンにし、 \* グループの作成 \* を選択します。

必要に応じて、ユーザを追加せずにグループを保存することもできます。このグループにあとでユーザを追加することも、新しいユーザを作成するときにグループを選択することもできます。

12. [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。キャッシングに時間がかかるため変更には最大で 15 分を要します。

#### 関連情報

["テナント管理権限"](#)

["Swift を使用します"](#)

グループの詳細を表示および編集する

グループの詳細を表示する際に、グループの表示名、権限、ポリシー、およびグループに属するユーザを変更することができます。

## 必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限を持つユーザグループに属している必要があります。

## 手順

1. \* access management \* > \* Groups \* を選択します。
  2. 詳細を表示または編集するグループの名前を選択します。
- または、 \* Actions \* > \* View group details \* を選択します。

グループの詳細ページが表示されます。次の例は、 S3 グループの詳細ページを表示します。

## Overview

Display name:	<a href="#">Applications</a>
Unique name:	group/Applications
Type:	Local
Access mode:	Read-write
Permissions:	Root Access
S3 Policy:	None
Number of users in this group:	0

### Group permissions

### S3 group policy

### Users

## Manage group permissions

Select an access mode for this group and select one or more permissions.

### Access mode ?

Select whether users can change settings and perform operations or whether they can only view settings and features.

Read-write  Read-only

### Group permissions ?

Select the tenant account permissions you want to assign to this group.

#### Root Access

Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.

#### Manage All Buckets

Allows users to change settings of all S3 buckets (or Swift containers) in this account.

#### Manage Endpoints

Allows users to configure endpoints for platform services.

#### Manage Your Own S3 Credentials

Allows users to create and delete their own S3 access keys.

[Save changes](#)

### 3. 必要に応じてグループ設定を変更します。



変更内容を確実に保存するには、各セクションで変更を行った後に「変更を保存」を選択します。変更を保存すると、ページの右上に確認メッセージが表示されます。

- 必要に応じて、表示名または編集アイコンを選択します 表示名を更新します。

グループの一意の名前は変更できません。フェデレーテッドグループの表示名は編集できません。

- 必要に応じて、権限を更新します。
- グループポリシーの場合は、S3 または Swift テナントに適した変更を行います。

- S3 テナントの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します。カスタムの S3 ポリシーを選択した場合は、JSON 文字列を必要に応じて更新します。
- Swift テナントの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。

Swift Administrator 権限の詳細については、Swift テナント用のグループを作成する手順を参照してください。

- 必要に応じて、ユーザを追加または削除します。

### 4. 変更したセクションごとに「変更を保存」を選択したことを確認します。

キャッシングに時間がかかるため変更には最大で 15 分を要します。

#### 関連情報

["S3テナント用のグループの作成"](#)

["Swiftテナント用のグループの作成"](#)

#### ローカルグループへのユーザの追加

必要に応じて、ローカルグループにユーザを追加できます。

#### 必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限を持つユーザグループに属している必要があります。

#### 手順

- \* access management \* > \* Groups \* を選択します。
- ユーザを追加するローカルグループの名前を選択します。

または、\* Actions \* > \* View group details \* を選択します。

グループの詳細ページが表示されます。

## Overview

Display name:	<a href="#">Applications</a>
Unique name:	group/Applications
Type:	Local
Access mode:	Read-write
Permissions:	Root Access
S3 Policy:	None
Number of users in this group:	0

### Group permissions

### S3 group policy

### Users

## Manage group permissions

Select an access mode for this group and select one or more permissions.

### Access mode ?

Select whether users can change settings and perform operations or whether they can only view settings and features.

Read-write  Read-only

### Group permissions ?

Select the tenant account permissions you want to assign to this group.

#### Root Access

Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.

#### Manage All Buckets

Allows users to change settings of all S3 buckets (or Swift containers) in this account.

#### Manage Endpoints

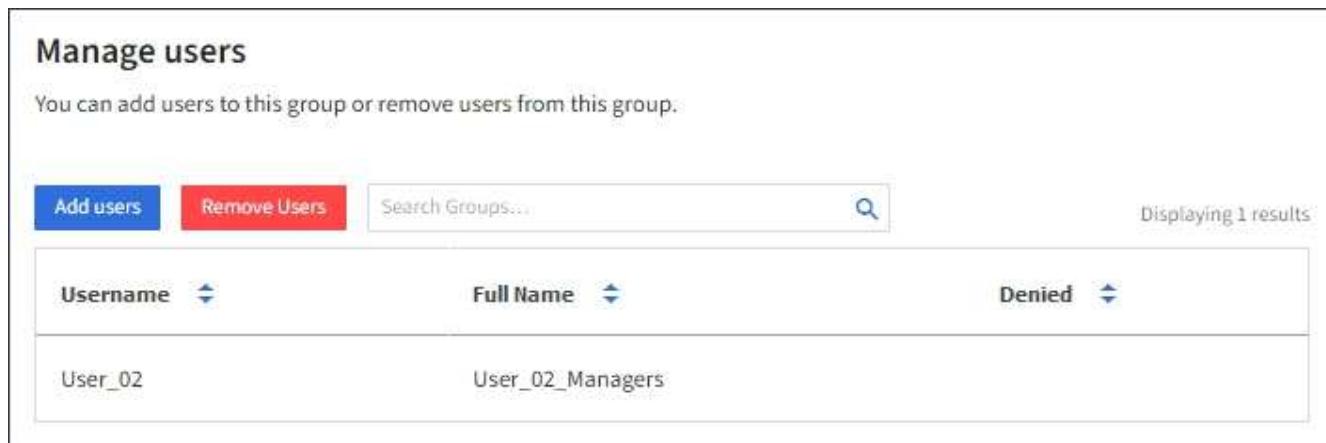
Allows users to configure endpoints for platform services.

#### Manage Your Own S3 Credentials

Allows users to create and delete their own S3 access keys.

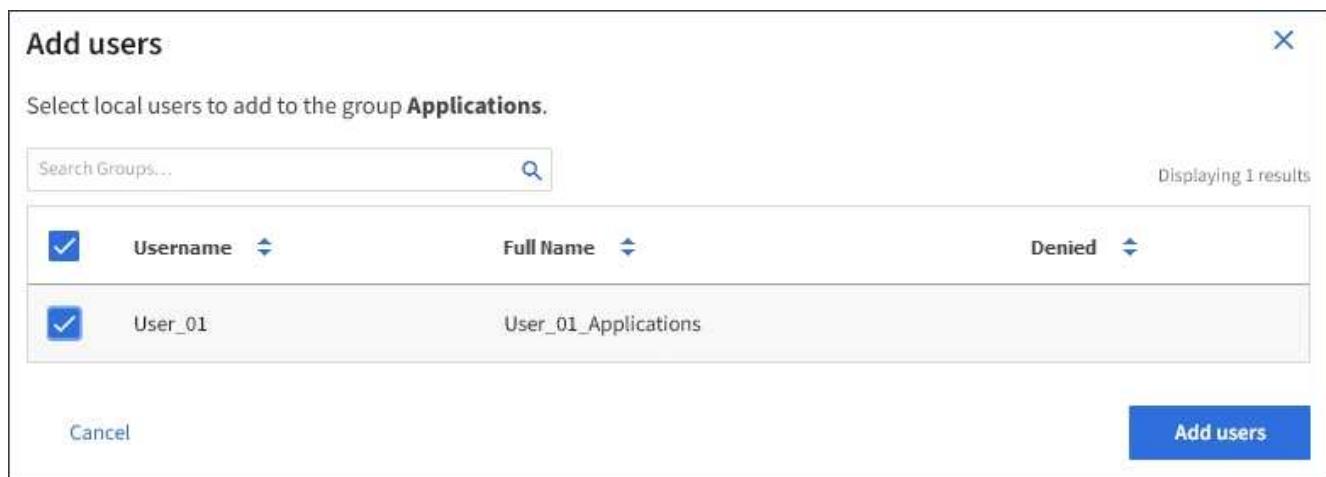
[Save changes](#)

3. 「ユーザーの管理」を選択し、「ユーザーの追加」を選択します。



The screenshot shows the 'Manage users' interface. At the top, there are buttons for 'Add users' (blue) and 'Remove Users' (red). Below them is a search bar with the placeholder 'Search Groups...' and a magnifying glass icon. To the right, it says 'Displaying 1 results'. The main area is a table with three columns: 'Username', 'Full Name', and 'Denied'. The data row shows 'User\_02' in the 'Username' column and 'User\_02\_Managers' in the 'Full Name' column. The 'Denied' column shows a downward arrow. The table has a light gray background with white rows and a thin gray border.

4. グループに追加するユーザーを選択し、\* ユーザーの追加 \* を選択します。



The screenshot shows the 'Add users' dialog box. At the top, it says 'Select local users to add to the group **Applications**'. Below is a search bar with 'Search Groups...' and a magnifying glass icon. To the right, it says 'Displaying 1 results'. The main area is a table with three columns: 'Username', 'Full Name', and 'Denied'. The data row shows a checked checkbox in the 'Username' column, 'User\_01' in the 'Full Name' column, and a downward arrow in the 'Denied' column. The table has a light gray background with white rows and a thin gray border. At the bottom left is a 'Cancel' button, and at the bottom right is a blue 'Add users' button.

ページの右上に確認メッセージが表示されます。キャッシングに時間がかかるため変更には最大で 15 分を要します。

グループ名を編集する

グループの表示名を編集できます。グループの一意の名前は編集できません。

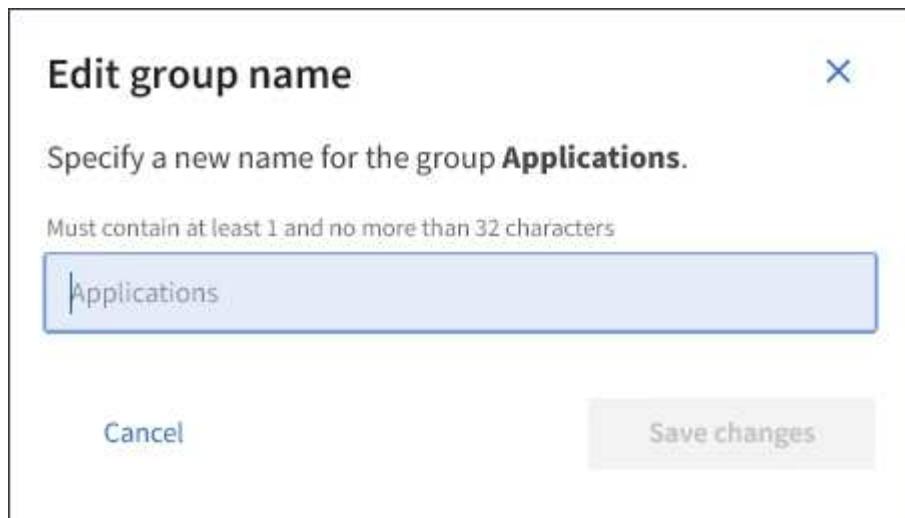
必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限を持つユーザグループに属している必要があります。

手順

1. \* access management \* > \* Groups \* を選択します。
2. 表示名を編集するグループのチェックボックスを選択します。
3. [ \* アクション \* > \* グループ名の編集 \* ] を選択します。

Edit group name (グループ名の編集) ダイアログボックスが表示されます。



4. ローカルグループを編集する場合は、必要に応じて表示名を更新します。

グループの一意の名前は変更できません。フェデレーテッドグループの表示名は編集できません。

5. 「変更を保存」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。キャッシングに時間がかかるため変更には最大で 15 分を要します。

#### 関連情報

["テナント管理権限"](#)

#### グループを複製する

既存のグループを複製することで、新しいグループをより迅速に作成できます。

#### 必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限を持つユーザグループに属している必要があります。

#### 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. 「\* グループを複製 \*」を選択します。グループの作成の詳細については、S3テナントまたはSwiftテナントのグループを作成する手順を参照してください。
4. [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。

5. 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) :

6. 「\* Continue \*」を選択します。
7. 必要に応じて、このグループの権限を変更します。
8. 「\* Continue \*」を選択します。
9. 必要に応じて、S3 テナントのグループを複製する場合は、\* S3 ポリシーの追加 \* オプションボタンとは別のポリシーを選択します。カスタムポリシーを選択した場合は、JSON 文字列を必要に応じて更新します。
10. 「\* グループを作成 \*」を選択します。

#### 関連情報

["S3テナント用のグループの作成"](#)

["Swiftテナント用のグループの作成"](#)

["テナント管理権限"](#)

#### グループを削除しています

システムからグループを削除できます。そのグループに属するユーザは、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することはできなくなります。

#### 必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限を持つユーザグループに属している必要があります。

#### 手順

1. \* access management \* > \* Groups \* を選択します。

# Groups

Create and manage local and federated groups. Set group permissions to control access to specific pages and features.

2 groups

Create group

Actions

<input type="checkbox"/>	Name	ID	Type	Access mode
<input type="checkbox"/>	Applications	22cc2e27-88ee-4461-a8c6-30b550beec0	Local	Read-write
<input type="checkbox"/>	Managers	8b15b131-1d21-4539-93ad-f2298347c4d8	Local	Read-write

← Previous 1 Next →

2. 削除するグループのチェックボックスを選択します。

3. [\* アクション \* > \* グループの削除 \*] を選択します。

確認メッセージが表示されます。

4. [\* グループの削除 \*] を選択して、確認メッセージに示されたグループを削除することを確認します。

ページの右上に確認メッセージが表示されます。キャッシングに時間がかかるため変更には最大で 15 分を要します。

## 関連情報

["テナント管理権限"](#)

## ローカルユーザの管理

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 つ含まれています。ローカルユーザは追加および削除できますが、root ユーザを削除することはできません。

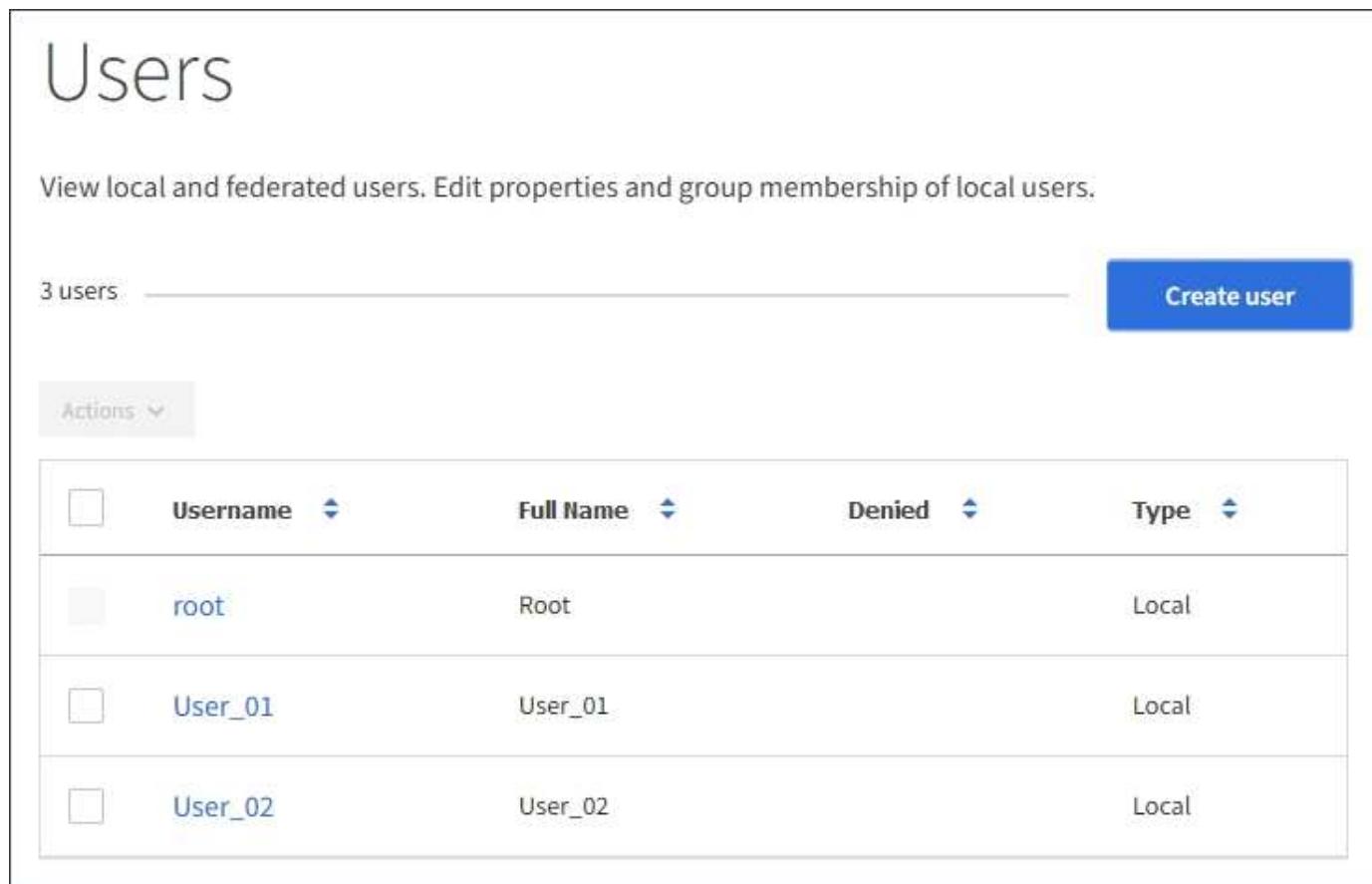
## 必要なもの

- Tenant Manager にはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限が設定された読み取り / 書き込みユーザグループに属している必要があります。

 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、ローカルユーザはテナントマネージャまたはテナント管理 API にサインインできません。ただし、グループの権限に基づいて、S3 または Swift クライアントアプリケーションを使用してテナントのリソースにアクセスすることはできます。

## Usersページへのアクセス

アクセス管理 \* > \* Users \* を選択します。



The screenshot shows the AWS IAM 'Users' page. At the top, it says 'View local and federated users. Edit properties and group membership of local users.' Below this, it shows '3 users' and a 'Create user' button. A 'Actions' dropdown menu is open. The main table lists three users:

	Username	Full Name	Denied	Type
<input type="checkbox"/>	root	Root		Local
<input type="checkbox"/>	User_01	User_01		Local
<input type="checkbox"/>	User_02	User_02		Local

ローカルユーザを作成しています

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。

いずれのグループにも属していない S3 ユーザには、管理権限または S3 グループポリシーが適用されません。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。

グループに属していない Swift ユーザには、管理権限または Swift コンテナへのアクセスは付与されません。

手順

1. 「\* ユーザーの作成 \*」を選択します。

2. 次のフィールドに値を入力します。

- \* フルネーム \* : このユーザのフルネーム。たとえば、ユーザの名と姓、またはアプリケーションの名前です。

- \* 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。

- \* Password \* : ユーザがサインイン時に使用するパスワード。

- \* パスワードの確認 \* : [ パスワード ] フィールドに入力したパスワードと同じパスワードを入力します。

◦ \* アクセスを拒否 \* : 「\* はい」を選択した場合、このユーザはテナントアカウントにサインインできません。これは、ユーザがまだ 1 つ以上のグループに属している可能性がある場合も同様です。

たとえば、この機能を使用すると、ユーザが一時的にサインインできないようにすることができます。

3. 「\* Continue \*」を選択します。
4. 1 つ以上のローカルグループにユーザを割り当てます。

グループに属していないユーザには管理権限は付与されません。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。

5. 「\* ユーザーの作成 \*」を選択します。

キャッシングに時間がかかるため変更には最大で 15 分を要します。

## ユーザの詳細を編集する

ユーザの詳細を編集する際に、ユーザのフルネームとパスワードを変更したり、ユーザを別のグループに追加したり、ユーザがテナントにアクセスできないようにしたりできます。

### 手順

1. [ ユーザー ] リストで、詳細を表示または編集するユーザの名前を選択します。

または、ユーザーのチェックボックスをオンにして、\* アクション \* > \* ユーザーの詳細を表示 \* を選択することもできます。

2. 必要に応じてユーザ設定を変更します。

a. フルネームまたは編集アイコンを選択して、必要に応じてユーザのフルネームを変更します  をクリックします。

ユーザ名は変更できません。

b. [ パスワード \*] タブで、必要に応じてユーザーのパスワードを変更します。

c. [ \* アクセス \* ] タブで、ユーザーがサインインすることを許可するか ([ \* いいえ \* ] を選択) 、ユーザーが必要に応じてサインインしないようにします ([ \* はい \* ] を選択) 。

d. [ \* グループ \*] タブで、ユーザーをグループに追加するか、必要に応じてグループから削除します。

e. 必要に応じて、[ 変更を保存 ( Save Changes ) ] を選択します。

キャッシングに時間がかかるため変更には最大で 15 分を要します。

## ローカルユーザの複製

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。

### 手順

1. [ ユーザー ] リストで、複製するユーザを選択します。
2. 「\* ユーザーを複製 \*」を選択します。

### 3. 新しいユーザの次のフィールドを変更します。

- \* フルネーム \* : このユーザのフルネーム。たとえば、ユーザの名と姓、またはアプリケーションの名前です。
- \* 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。
- \* Password \* : ユーザがサインイン時に使用するパスワード。
- \* パスワードの確認 \* : [ パスワード ] フィールドに入力したパスワードと同じパスワードを入力します。
- \* アクセスを拒否 \* : 「\* はい」を選択した場合、このユーザはテナントアカウントにサインインできません。これは、ユーザがまだ 1 つ以上のグループに属している可能性がある場合も同様です。

たとえば、この機能を使用すると、ユーザが一時的にサインインできないようにすることができます。

### 4. 「\* Continue \*」を選択します。

### 5. 1 つ以上のローカルグループを選択します。

グループに属していないユーザには管理権限は付与されません。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。

### 6. 「\* ユーザーの作成 \*」を選択します。

キャッシングに時間がかかるため変更には最大で 15 分を要します。

## ローカルユーザを削除しています

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ローカルユーザは、完全に削除できます。

Tenant Manager を使用して、フェデレーテッドユーザは削除できますが、フェデレーテッドユーザは削除できません。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. [ ユーザ ] リストで、削除するローカルユーザのチェックボックスをオンにします。
2. \* アクション \* > \* ユーザーの削除 \* を選択します。
3. 確認ダイアログボックスで、「\* ユーザーの削除 \*」を選択して、システムからユーザーを削除することを確認します。

キャッシングに時間がかかるため変更には最大で 15 分を要します。

## 関連情報

["テナント管理権限"](#)

## S3テナントアカウントの管理

Tenant Managerを使用して、S3アクセスキーを管理したり、S3バケットを作成および管理したりできます。

- ・ "S3 アクセスキーの管理"
- ・ "S3バケットの管理"

### S3 アクセスキーの管理

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。

このタスクについて

S3 アクセスキーは次のように管理できます。

- ・ Manage Your Own S3 Credentials \* 権限が設定されたユーザは、自分の S3 アクセスキーを作成または削除できます。
- ・ Root Access \* 権限が設定されたユーザは、S3 root アカウントおよび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。

自分のS3アクセスキーを作成する

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。S3 テナントアカウントの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。

必要なもの

- ・ Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- ・ Manage Your Own S3 Credentials 権限が必要です。

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。セキュリティ上の理由から、必要以上の数のキーを作成しないでください。また、使用していないキーは削除してください。キーが 1 つしかなく、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

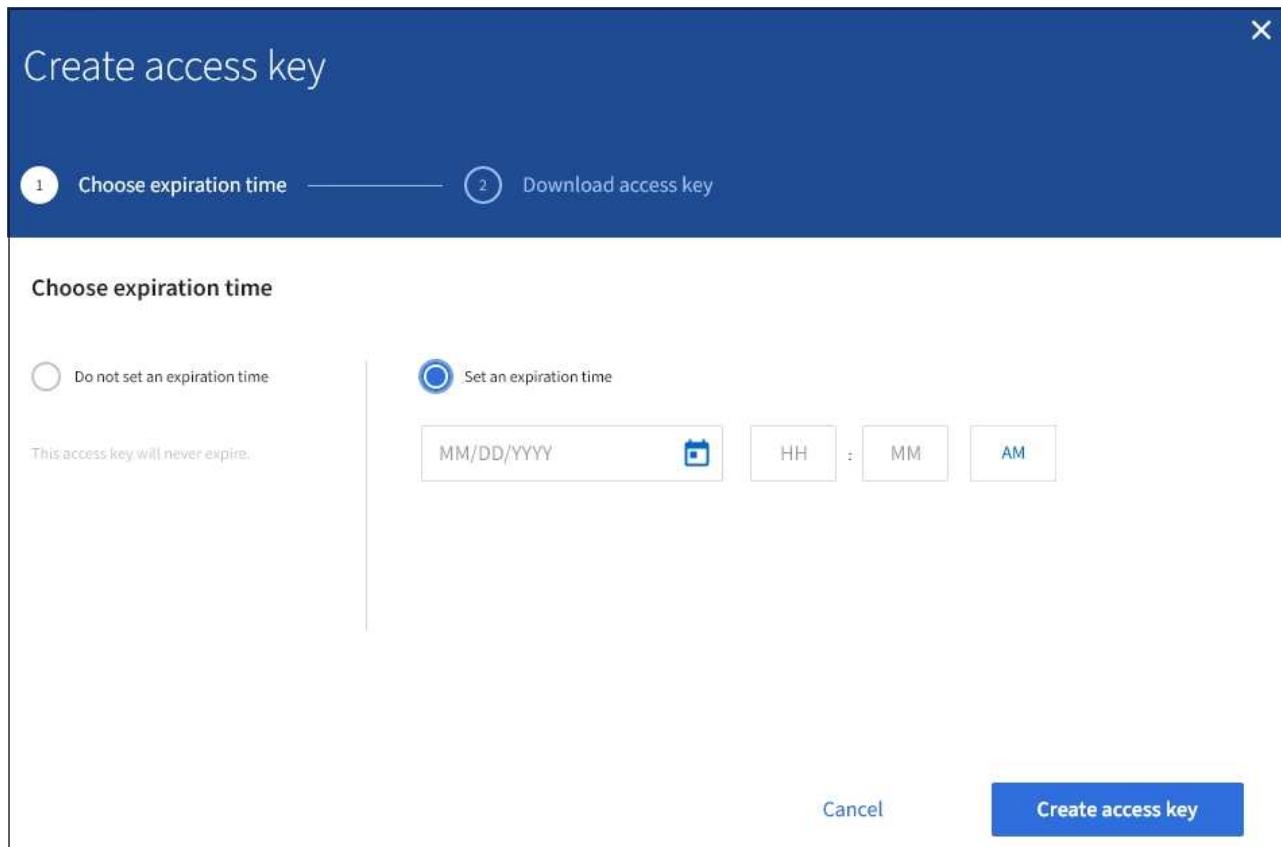
1. 「\* storage (S3) \* > \* My access keys \*」を選択します。

[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。



4. [ アクセスキーの作成 \*] を選択します。

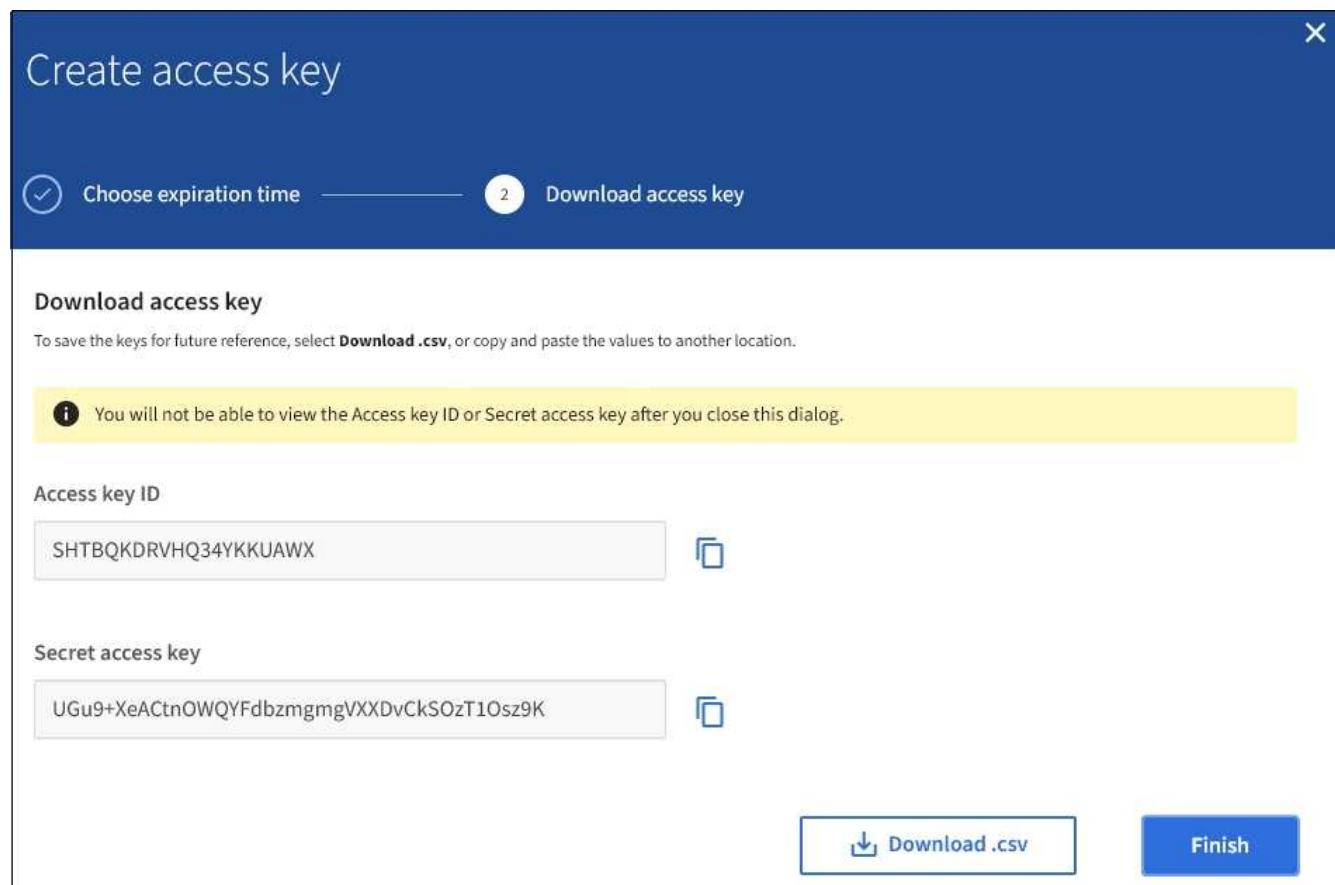
Download access key (アクセスキーのダウンロード) ダイアログボックスが表示され、アクセスキー ID とシークレットアクセスキーが一覧表示されます。

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

択してアクセキー ID とシークレットアクセ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。



6. [完了] を選択します。

新しいキーは [マイアクセキー] ページに表示されます。キャッシュングに時間がかかるため変更には最大で 15 分を要します。

関連情報

["テナント管理権限"](#)

**S3** アクセキーを表示します

S3 テナントを使用している場合は、適切な権限があれば、S3 アクセキーのリストを表示できます。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、使用しなくなったキーを削除したりできます。

必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Manage Your Own S3 Credentials 権限が必要です。



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

- 「\* 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。

<input type="checkbox"/>	Access key ID	Expiration time
<input type="checkbox"/>	*****OTLS	2020-11-23 12:00:00 MST
<input type="checkbox"/>	*****0M45	2020-12-01 19:00:00 MST
<input type="checkbox"/>	*****69QJ	None
<input type="checkbox"/>	*****3R8P	None

- キーを \* Expiration time \* または \* Access key ID \* でソートします。
- 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

"自分のS3アクセキーを作成する"

"自分のS3アクセキーを削除する"

自分のS3アクセキーを削除する

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 アクセキーを削除できます。アクセキーを削除すると、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キーでアクセスできなくなります。

必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Manage Your Own S3 Credentials 権限が必要です。

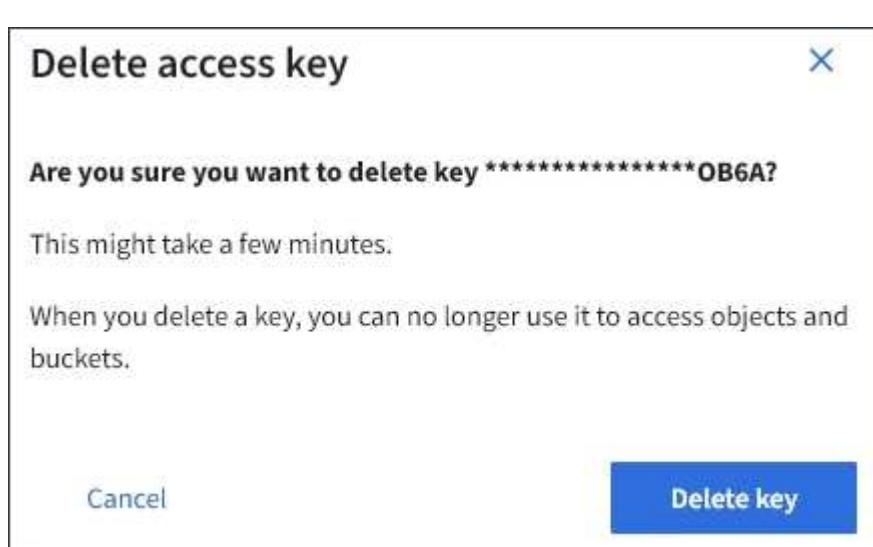


アカウントに属する S3 バケットとオブジェクトには、Tenant Manager でアカウントに表示されるアクセキー ID とシークレットアクセキーを使用してアクセスできます。このため、アクセキーはパスワードと同じように保護する必要があります。定期的にアクセキーをローテーションし、使用されていないキーはアカウントから削除します。また、他のユーザとはアクセキーを共有しないでください。

手順

1. 「\* storage ( S3 ) \* > \* My access keys \*」を選択します。  
[マイアクセキー] ページが表示され、既存のアクセキーが一覧表示されます。
2. 削除する各アクセキーのチェックボックスを選択します。
3. 「\* Delete key (キーの削除) \*」を選択

確認のダイアログボックスが表示されます。



4. 「\* Delete key (キーの削除) \*」を選択

ページの右上に確認メッセージが表示されます。キャッシングに時間がかかるため変更には最大で 15 分を要します。

## 関連情報

### "テナント管理権限"

別のユーザのS3アクセスキーを作成する

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。

必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限が必要です。

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プリケーションを更新します。セキュリティ上の理由から、ユーザが必要とする以上のキーは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。



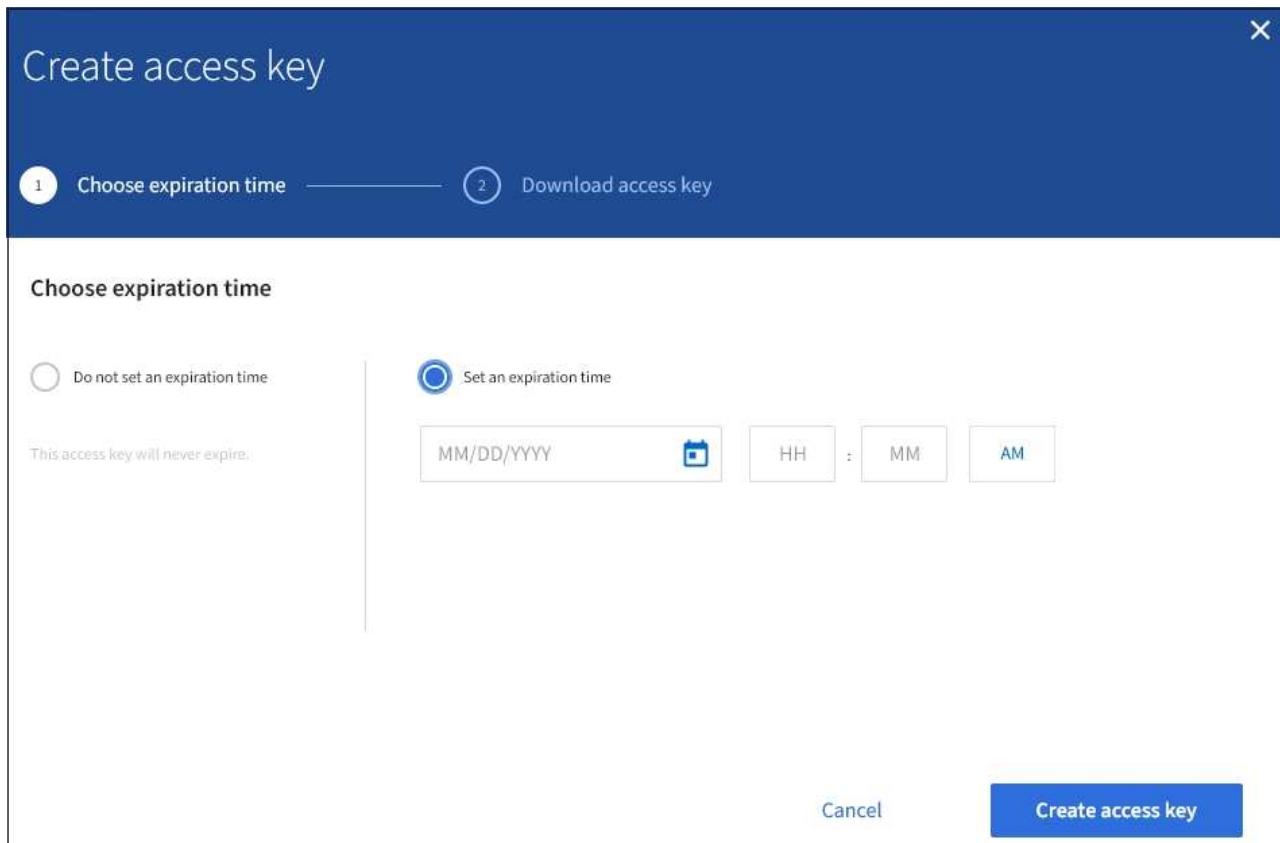
ユーザに属する S3 バケットとオブジェクトには、Tenant Manager でそのユーザに対して表示されるアクセスキー ID とシークレットアクセスキーを使用してアクセスできます。このため、アクセスキーはパスワードと同じように保護する必要があります。定期的にアクセスキーをローテーションし、使用されていないキーはアカウントから削除します。また、他のユーザとはアクセスキーを共有しないでください。

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。



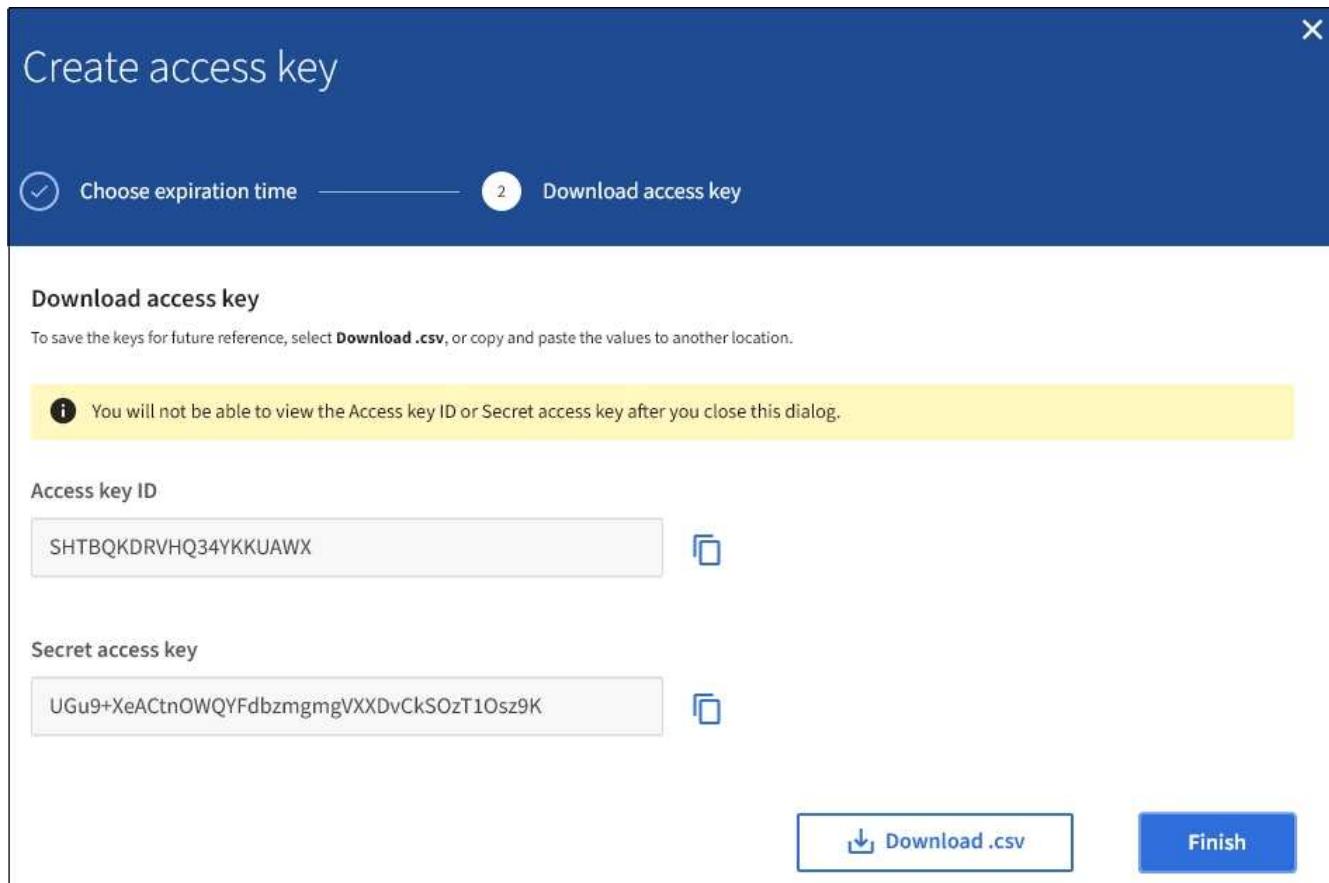
5. [ アクセスキーの作成 \*] を選択します。

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。



#### 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。キャッシングに時間がかかるため変更には最大で 15 分を要します。

#### 関連情報

["テナント管理権限"](#)

別のユーザのS3アクセスキーを表示しています

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。

#### 必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限が必要です。

 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

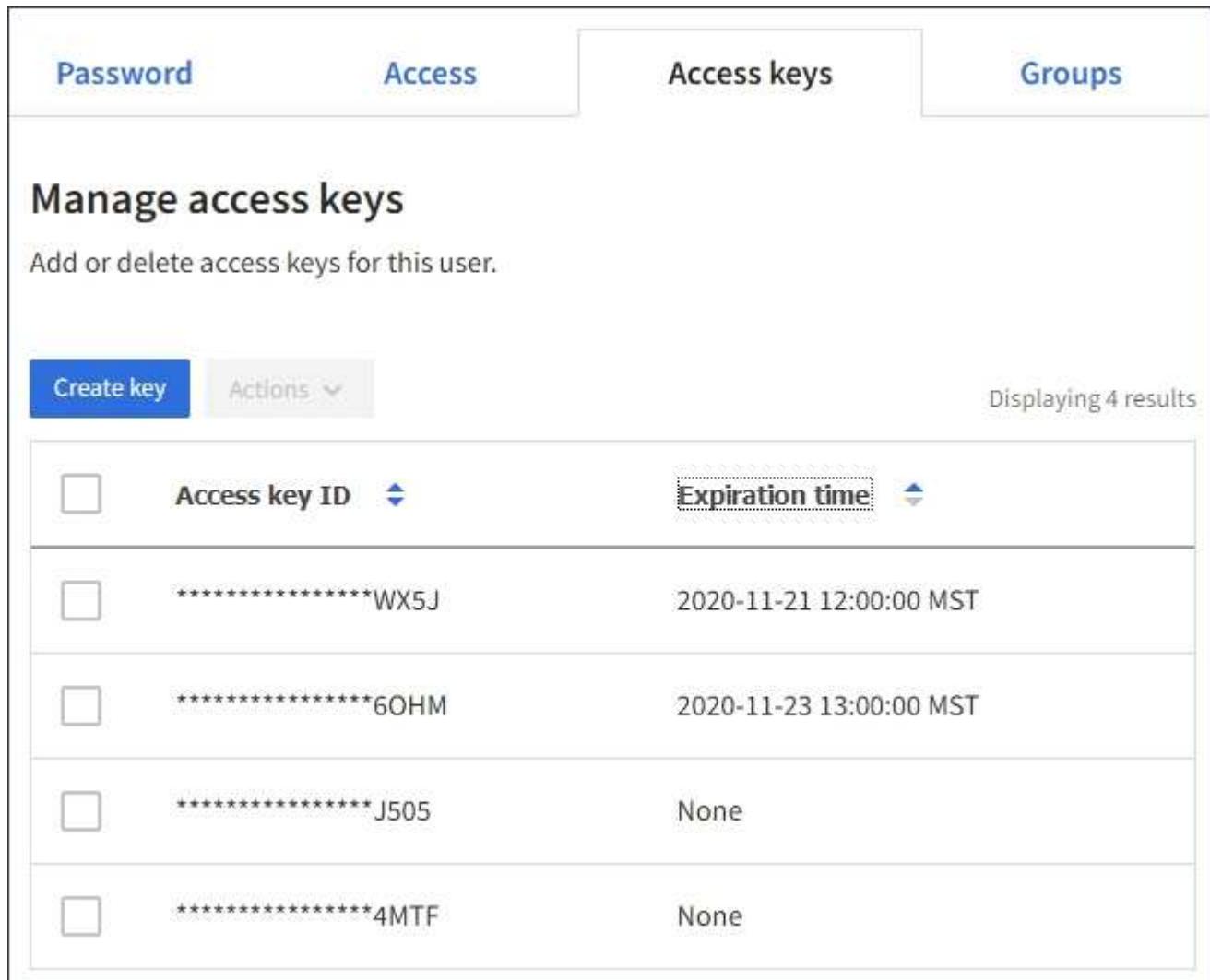
1. アクセス管理 \* > \* Users \* を選択します。

[ ユーザー ] ページが表示され、既存のユーザーが一覧表示されます。

2. S3 アクセスキーを表示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 \*」を選択します。



Access key ID	Expiration time
*****WX5J	2020-11-21 12:00:00 MST
*****60HM	2020-11-23 13:00:00 MST
*****J505	None
*****4MTF	None

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ています"

"別のユーザのS3アクセスキーを削除しています"

別のユーザのS3アクセスキーを削除しています

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。

必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限が必要です。



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。

[ ユーザー ] ページが表示され、既存のユーザーが一覧表示されます。

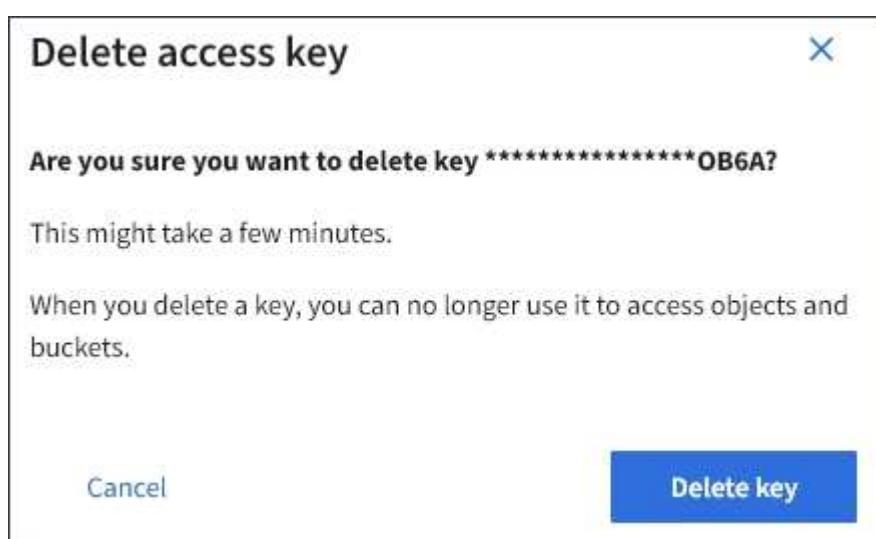
2. S3 アクセスキーを管理するユーザを選択します。

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、削除する各アクセスキーのチェックボックスを選択します。

4. \* アクション \* > \* 選択したキーを削除 \* 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。



## 5. 「\* Delete key (キーの削除) 」 \* を選択

ページの右上に確認メッセージが表示されます。キャッシングに時間がかかるため変更には最大で 15 分を要します。

### 関連情報

["テナント管理権限"](#)

## S3バケットの管理

S3テナントを適切な権限で使用している場合は、S3バケットの作成、表示、削除、整合性レベルの設定の更新、Cross-Origin Resource Sharing (CORS) の設定、最終アクセス日時の更新の有効化と無効化、S3プラットフォームサービスの管理を実行できます。

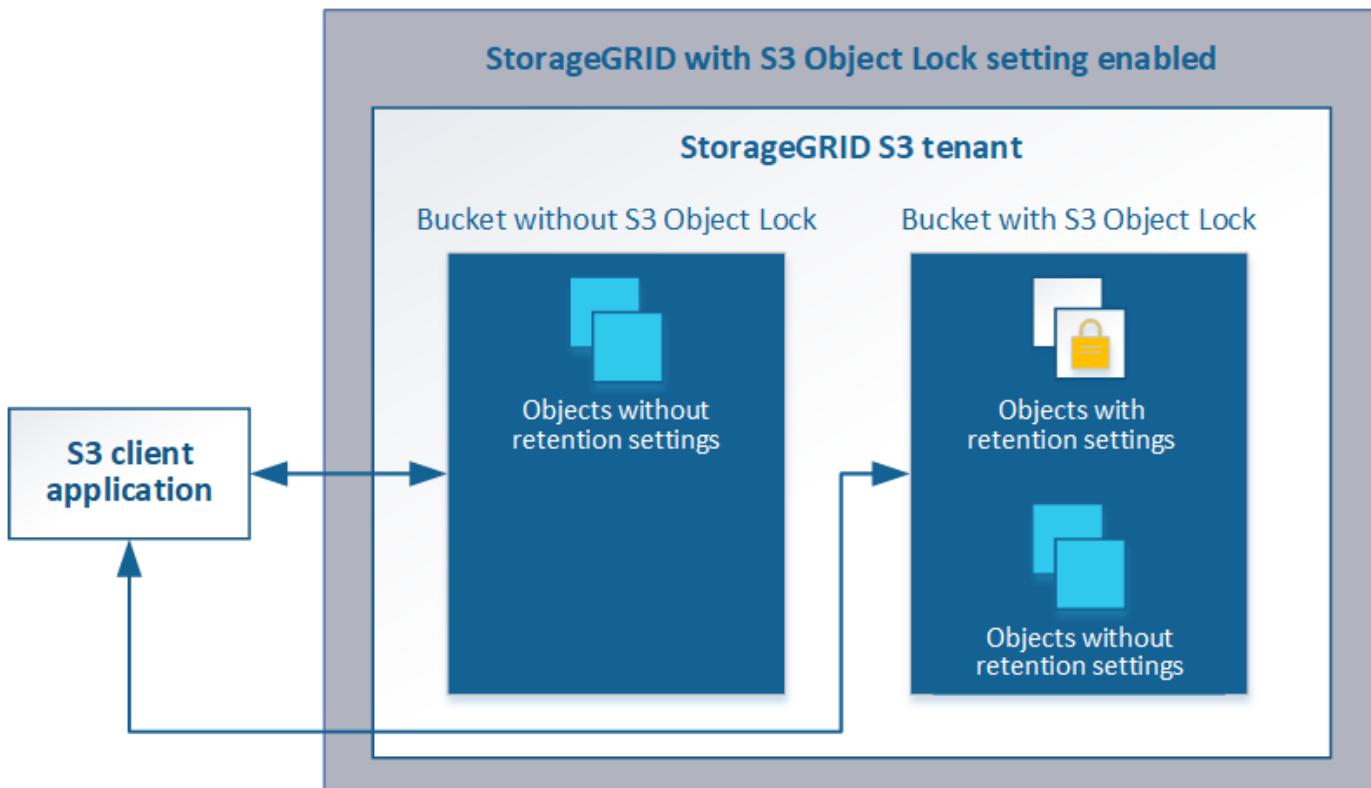
### S3 オブジェクトロックを使用する

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、StorageGRID で S3 オブジェクトロック機能を使用できます。

#### 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 オブジェクトの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、そのバケット内の任意のオブジェクトバージョンの保持設定を必要に応じて指定できます。オブジェクトのバージョンには、S3 オブジェクトロックで保護するように指定された保持設定が必要です。



StorageGRID S3 オブジェクトロック機能は、Amazon S3 準拠モードと同等の単一の保持モードを提供します。デフォルトでは、保護されたオブジェクトバージョンは、どのユーザーでも上書きまたは削除できません。StorageGRID S3 オブジェクトのロック機能では、ガバナンスモードはサポートされず、特別な権限を持つユーザは保持設定を省略したり保護されたオブジェクトを削除したりすることはできません。

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、オブジェクトの作成時または更新時に、次のオブジェクトレベルの保持設定のいずれか、または両方を必要に応じて指定できます。

- **Retain Until - date** : オブジェクトバージョンの `retain-until - date` が将来の日付である場合、オブジェクトは読み出し可能ですが、変更または削除することはできません。必要に応じて、オブジェクトの `retain-date` を増やすことはできますが、この日付を減らすことはできません。
- \* 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。

これらの設定の詳細については、の「Using S3 object lock」を参照してください ["S3 REST API のサポートされる処理と制限事項"](#)。

#### 従来の準拠バケットの管理

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、ネットアップの技術情報アーティクルを参照してください。

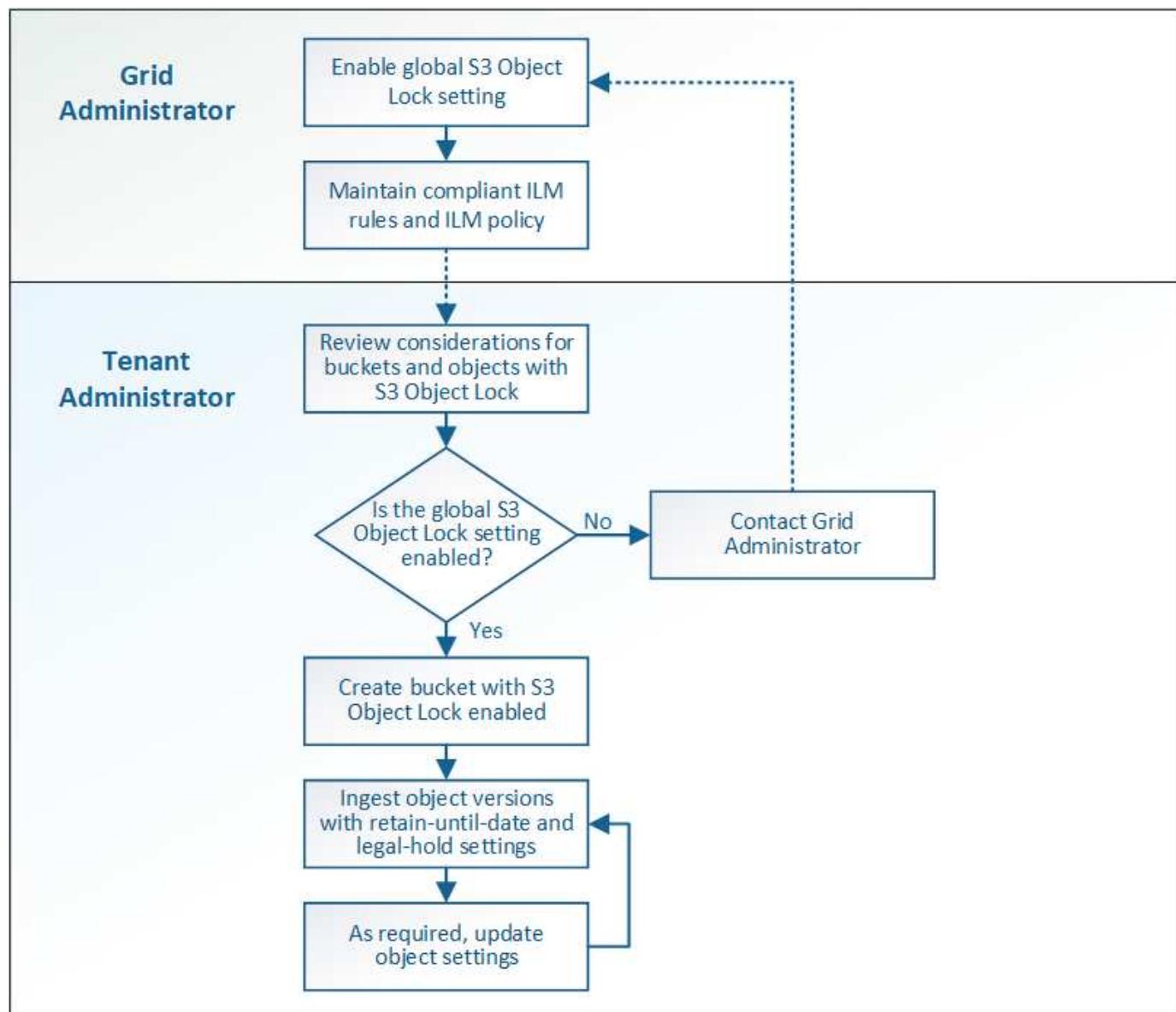
["ネットアップのナレッジベース： StorageGRID 11.5 でレガシー準拠バケットを管理する方法"](#)

### 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。また、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」であることを確認する必要があります。S3 オブジェクトロックが有効になっているバケットの要件を満たしている必要があります。詳細については、グリッド管理者に問い合わせるか、情報ライフサイクル管理を使用してオブジェクトを管理する手順を参照してください。

グローバルな S3 オブジェクトのロック設定を有効にしたあと、S3 オブジェクトのロックを有効にしてバケットを作成できます。その後、S3 クライアントアプリケーションを使用して、オブジェクトのバージョンごとに保持設定を必要に応じて指定できます。



#### 関連情報

["ILM を使用してオブジェクトを管理する"](#)

### S3 オブジェクトのロックの要件

バケットで S3 オブジェクトのロックを有効にする前に、S3 オブジェクトのロックが有効になっているバケットおよびオブジェクトの要件と、バケット内のオブジェクトのライフサイクルを確認します。

### 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。

次の Tenant Manager の例では、S3 オブジェクトのロックが有効になっているバケットを示しています。

## Buckets

Create buckets and manage bucket settings.

1 bucket							<a href="#">Create bucket</a>
Actions		Name	S3 Object Lock	Region	Object Count	Space Used	Date Created
<input type="checkbox"/>	<a href="#">bank-records</a>		✓	us-east-1	0	0 bytes	2021-01-06 16:53:19 MST

← Previous 1 Next →

- 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。既存のバケットに対して S3 オブジェクトロックを有効にすることはできません。
- S3 オブジェクトロックでは、バケットのバージョン管理が必要です。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。
- S3 オブジェクトのロックを有効にしてバケットを作成したあとに、そのバケットの S3 オブジェクトの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。
- S3 オブジェクトのロックが有効になっている StorageGRID バケットでは、デフォルトの保持期間はありません。代わりに、S3 クライアントアプリケーションは、そのバケットに追加されるオブジェクトバージョンごとに保持期限とリーガルホールド設定を指定できます。
- バケットライフサイクル設定は S3 オブジェクトライフサイクル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

- S3 クライアントアプリケーションは、S3 オブジェクトのロックで保護する必要があるオブジェクトごとに保持設定を指定する必要があります。
- オブジェクトバージョンの retain-until date は増やすことができますが、この値を減らすことはできません。

ん。

- ・係争中の訴訟や規制上の調査に関する通知があった場合、オブジェクトバージョンをリーガルホールドの対象にすることで関連情報を保持できます。オブジェクトバージョンがリーガルホールドの対象になっている場合は、それが `retain-until` 日に達しても、そのオブジェクトを StorageGRID から削除することはできません。リーガルホールドを解除すると、それまで保持期限に達した場合にオブジェクトバージョンを削除できるようになります。
- ・S3 オブジェクトロックにはバージョン管理されたバケットを使用する必要があります。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 オブジェクトのロックが有効になっているバケットに保存された各オブジェクトは、次の 3 つの段階を経て処理されます。

#### 1. \* オブジェクトの取り込み \*

- S3 オブジェクトのロックが有効になっているバケットにオブジェクトのバージョンを追加するときに、S3 クライアントアプリケーションはオプションでオブジェクトの保持設定を指定できます（`retain-until date`、`legal hold`、または `both`）。StorageGRID は、そのオブジェクトのメタデータを生成します。これには、一意のオブジェクト ID（UUID）と取り込み日時が含まれます。
- 保持設定のあるオブジェクトのバージョンが取り込まれたあとに、そのデータと S3 ユーザ定義メタデータを変更することはできません。
- StorageGRID は、オブジェクトメタデータをオブジェクトデータとは別に格納します。各サイトですべてのオブジェクトメタデータのコピーを 3 つ保持します。

#### 2. \* オブジェクト保持 \*

- オブジェクトの複数のコピーが StorageGRID によって格納される。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。

#### 3. \* オブジェクトの削除 \*

- オブジェクトは、`retain-until - date` に到達したときに削除できます。
- リーガルホールドの対象になっているオブジェクトは削除できません。

### **S3 バケットの作成**

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。バケットを作成するときは、バケットの名前とリージョンを指定する必要があります。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は、必要に応じてバケットで S3 オブジェクトのロックを有効にすることができます。

#### 必要なもの

- ・Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- ・Manage All Buckets 権限または 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。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。

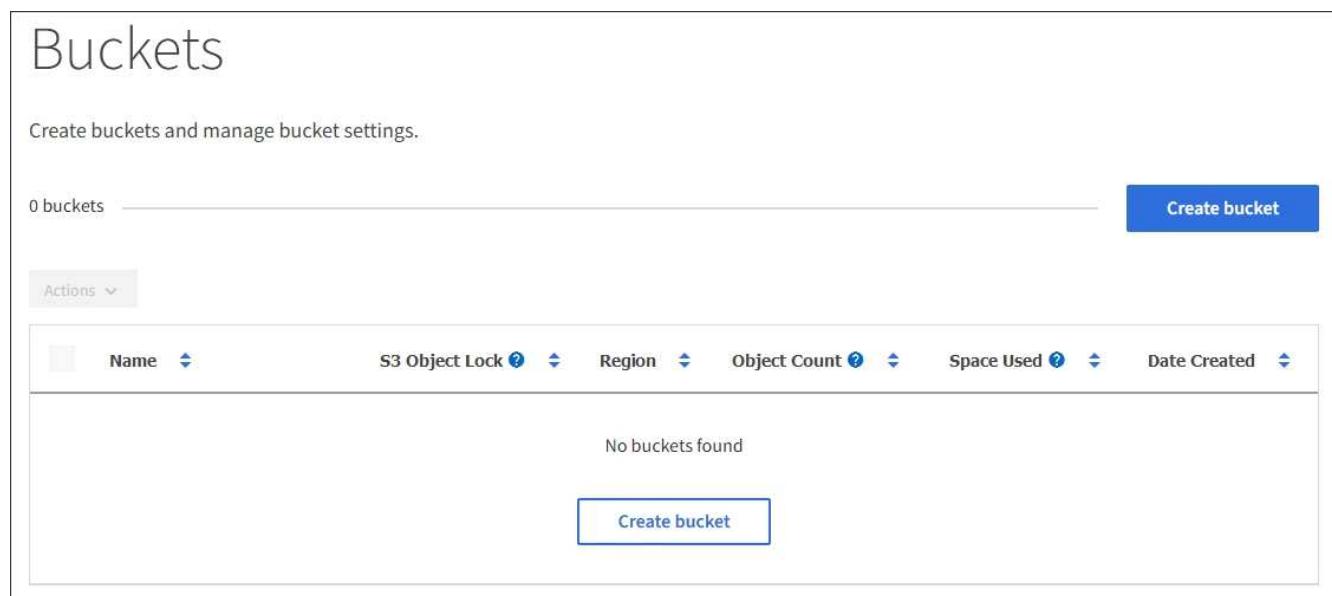
- S3オブジェクトロックを使用してバケットを作成する場合は、StorageGRIDシステムでグローバルなS3オブジェクトロック設定を有効にしておく必要があります。また、S3オブジェクトロックのバケットとオブジェクトに関する要件を確認しておく必要があります。

### "S3 オブジェクトロックを使用する"

#### 手順

1. ストレージ（S3） \* > \* バケット \* を選択します。

バケットページが表示され、すでに作成されているバケットが一覧表示されます。



The screenshot shows the AWS S3 Buckets page. The title is 'Buckets' and the sub-instruction is 'Create buckets and manage bucket settings.' Below the title, it says '0 buckets'. On the right, there is a blue 'Create bucket' button. Under the table header, there is an 'Actions' dropdown menu. The table header includes columns: 'Name', 'S3 Object Lock', 'Region', 'Object Count', 'Space Used', and 'Date Created'. The main content area below the table header displays the message 'No buckets found'. At the bottom of the page, there is another 'Create bucket' button.

2. [\* バケットの作成 \*] を選択します。

Create Bucket ウィザードが表示されます。

# Create bucket

Enter bucket details

Enter the bucket's name and select the bucket's region.

Bucket name [?](#)

Region [?](#)

 [▼](#)[Cancel](#)[Create bucket](#)

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、バケットの作成には、バケットのS3オブジェクトのロックを管理するための2つ目の手順が含まれます。

3. バケットの一意の名前を入力します。



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。

バケット名は次のルールを満たす必要があります。

- StorageGRID システム全体で（テナントアカウント内だけではなく）一意である必要があります。
- DNS に準拠している必要があります。
- 3 文字以上 63 文字以下にする必要があります。
- 1 つ以上のラベルを連続して指定できます。隣接するラベルはピリオドで区切ります。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。
- テキスト形式の IP アドレスのようにはできません。
- 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す。



詳細については、Amazon Web Services (AWS) ドキュメントを参照してください。

4. このバケットのリージョンを選択します。

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us-east-1リージョンで作成されます。

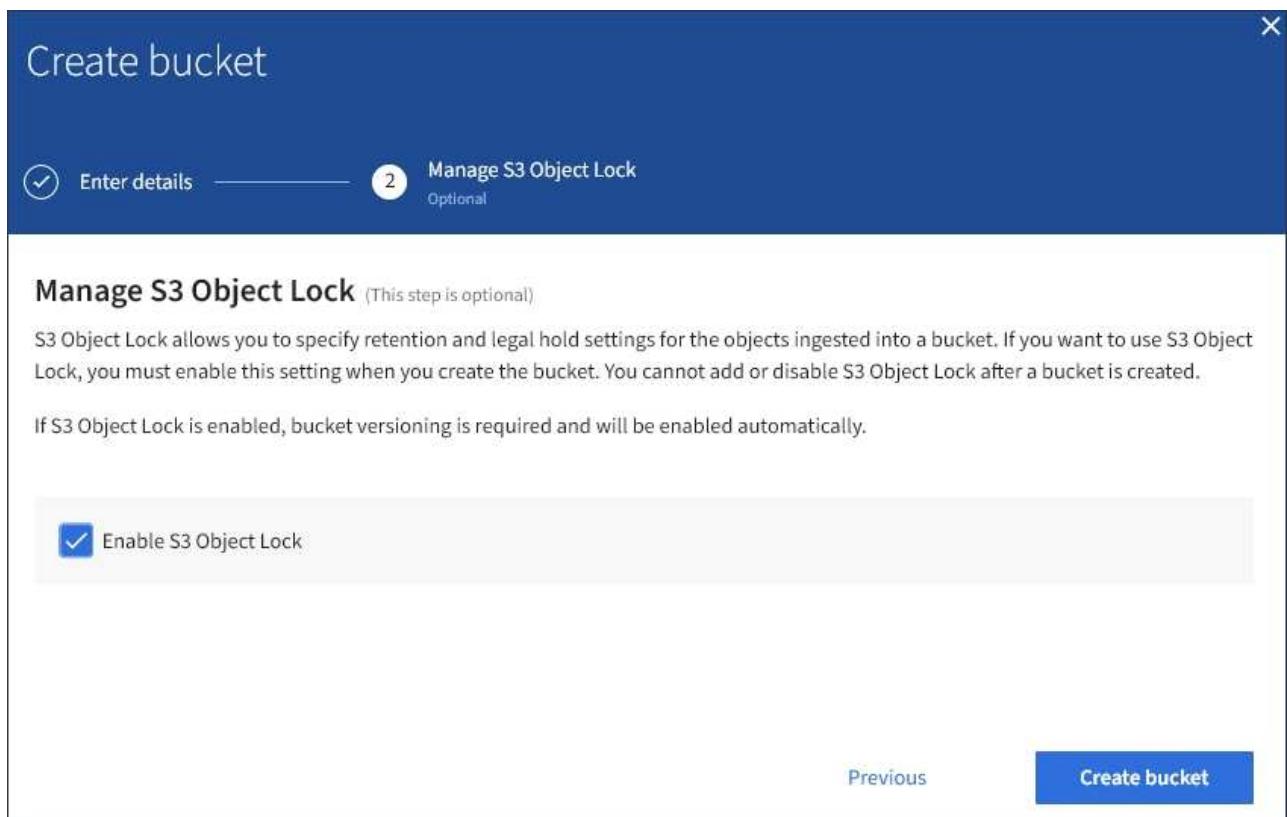
[X](#)



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。

##### 5. Create bucket または Continue \*を選択します。

- 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ない場合は、\*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。
- 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は、「\* Continue \*」を選択します。ステップ2：Manage S3 Object Lock (S3オブジェクトのロックの管理) が表示されます。



##### 6. 必要に応じて、このバケットでS3オブジェクトロックを有効にする場合は、チェックボックスを選択します。

S3 クライアントアプリケーションがバケットに追加されたオブジェクトの最新の保持設定とリーガルホールド設定を指定するには、バケットに対して S3 オブジェクトロックを有効にする必要があります。



バケットの作成後に S3 オブジェクトのロックを有効または無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。

##### 7. [\* 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。

#### 関連情報

["ILM を使用してオブジェクトを管理する"](#)

"テナント管理APIについて"

"S3 を使用する"

S3バケットの詳細の表示

テナントアカウントのバケットおよびバケット設定のリストを表示できます。

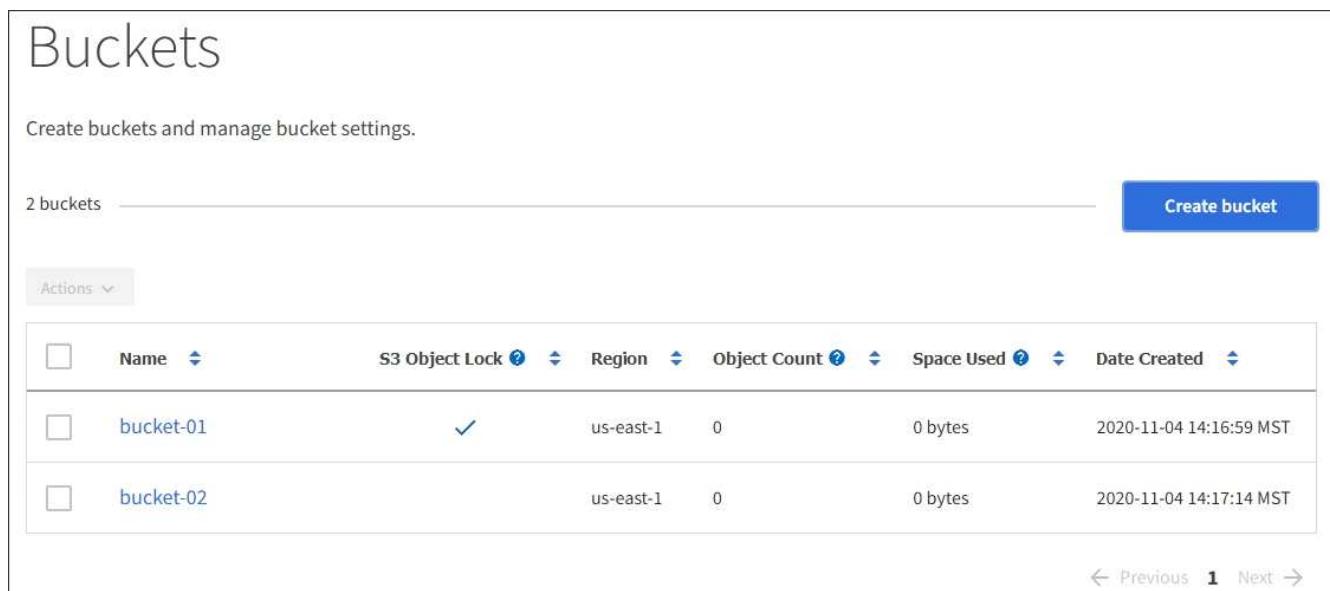
必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。

手順

1. ストレージ（S3）\* > \* バケット\* を選択します。

バケットページが表示され、テナントアカウントのすべてのバケットがリストされます。



Name	S3 Object Lock	Region	Object Count	Space Used	Date Created
bucket-01	✓	us-east-1	0	0 bytes	2020-11-04 14:16:59 MST
bucket-02		us-east-1	0	0 bytes	2020-11-04 14:17:14 MST

2. 各バケットの情報を確認します。

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。

- Name : バケットの一意の名前。変更できません。
- S3 Object Lock : このバケットで S3 オブジェクトのロックが有効になっているかどうか。

グローバルな S3 オブジェクトのロック設定が無効になっている場合は、この列は表示されません。この列には、古い準拠バケットの情報も表示されます。

- Region : バケットのリージョン。変更できません。
- Object Count : このバケット内のオブジェクトの数。
- Space Used : この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。
- Date Created : バケットが作成された日時。



「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。

3. バケットの設定を表示および管理するには、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。

このページでは、バケットオプション、バケットアクセス、およびプラットフォームサービスの設定を表示および編集できます。

各設定またはプラットフォームサービスの設定手順を参照してください。

Buckets > **bucket-02**

**Overview** ^

Name:	<b>bucket-02</b>
Region:	<b>us-east-1</b>
S3 Object Lock:	<b>Disabled</b>
Date created:	<b>2020-11-04 14:51:59 MST</b>

**Bucket options** **Bucket access** **Platform services**

Consistency level	Read-after-new-write	▼
Last access time updates	Disabled	▼

#### 関連情報

["整合性レベルを変更する"](#)

["最終アクセス日時の更新の有効化または無効化"](#)

["Cross-Origin Resource Sharing \(CORS\) の設定"](#)

["CloudMirrorレプリケーションの設定"](#)

["イベント通知を設定する"](#)

["検索統合サービスの設定"](#)

## 整合性レベルを変更する

S3 テナントを使用している場合は、テナントマネージャまたはテナント管理 API を使用して、S3 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制御レベルを変更できます。

### 必要なもの

- Tenant Manager にはサポートされているブラウザを使用してサインインする必要があります。
- Manage All Buckets 権限または 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。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

整合性レベルを設定する場合は、オブジェクトの可用性と、異なるストレージノードおよびサイト間におけるオブジェクトの整合性のどちらかを犠牲にしなければなりません。通常は、バケットに \* Read-after-new-write \* 整合性レベルを使用してください。Read-after-new-write \* 整合性レベルがクライアントアプリケーションの要件を満たさない場合は、バケットの整合性レベルを設定するか、を使用して整合性レベルを変更できます Consistency-Control ヘッダー。。 Consistency-Control ヘッダーはバケットの整合性レベルよりも優先されます。



バケットの整合性レベルを変更した場合、変更後のレベルを満たすことが保証されるのは、変更後に取り込まれたオブジェクトのみです。

### 手順

1. ストレージ (S3) \* > \* バケット \* を選択します。
  2. リスト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 \* > \* Consistency level \* を選択します。

Bucket options      Bucket access      Platform services

Consistency level      Read-after-new-write (default) ^

Change the consistency control for operations performed on the objects in the bucket. Consistency level makes a trade-off between the availability of the objects and the consistency of those objects across different Storage Nodes and sites.

In general, use the **Read-after-new-write** consistency level for your buckets. Then, if objects do not meet availability or consistency requirements, change the client application's behavior, or set the *Consistency-Control* header for an individual API request, which overrides the bucket setting.

All  
 Provides the highest guarantee of consistency. All nodes receive the data immediately, or the request will fail.

Strong-global  
 Guarantees read-after-write consistency for all client requests across all sites.

Strong-site  
 Guarantees read-after-write consistency for all client requests within a site.

Read-after-new-write (default)  
 Provides read-after-write consistency for new objects and eventual consistency for object updates. Offers high availability, and data protection guarantees.

Note: If your application attempts HEAD operations on keys that do not exist, set the Consistency Level to **Available**, unless you require AWS S3 consistency guarantees. Otherwise, a high number of 500 Internal Server errors can result if one or more Storage Nodes are unavailable.

Available  
 Behaves the same as the **Read-after-new-write** consistency level, but only provides eventual consistency for HEAD operations. Offers higher availability for HEAD operations than **Read-after-new-write** if Storage Nodes are unavailable. Differs from AWS S3 consistency guarantees for HEAD operations only.

Save changes

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レベルを選択します。

整合性レベル	説明
すべて	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。

整合性レベル	説明
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	1つのサイト内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。
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、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。Amazon S3の整合性に相当します。  注: Amazon S3の整合性保証が必要な場合を除き、アプリケーションが存在しないキーに対してHEAD処理を試行する場合は、整合性レベルを「Available *」に設定してください。そうしないと、使用できないストレージノードがある場合に「500 Internal Server Error」が大量に発生する可能性があります。
available (HEAD処理は結果整合性)	read-after-new-write *整合性レベルと動作は同じですが、HEAD処理については結果整合性のみを提供します。ストレージノードを使用できない場合に、HEAD処理に対して「Read-after-new-write」よりも高い可用性が提供される。Amazon S3の整合性と異なるのはHEAD処理のみです。

## 5. 「変更を保存」を選択します。

### 関連情報

#### ["テナント管理権限"](#)

### 最終アクセス日時の更新の有効化または無効化

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。

この手順は、配置手順で \* Last Access Time \* オプションを使用する ILM ルールを 1 つ以上含む StorageGRID システムにのみ適用されます。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。

### 必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Manage All Buckets 権限または 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。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。
- 最終アクセス時間 \* は、ILM ルールの \* 参照時間 \* 配置手順で使用できるオプションの 1 つです。ルールの参照時間を最終アクセス日時に設定すると、グリッド管理者は、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）タイミングに基づいて特定のストレージの場所にオブジェクトが配置されるように指定できます。

たとえば、最近表示したオブジェクト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。



情報ライフサイクル管理を使用してオブジェクトを管理する手順を参照してください。

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、\* Last Access Time \* オプションを使用する ILM ルールが含まれている場合に、このオプションをこのバケット内のオブジェクトに適用するには、そのルールで指定される S3 バケットで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 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 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

- ストレージ (S3) \* > \* バケット \* を選択します。
- リスト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。
- 「\* Bucket options \* > \* Last access time updates \*」を選択します。
- 適切なオプションボタンを選択して、最終アクセス日時の更新を有効または無効にします。

The screenshot shows the 'Bucket options' tab selected in the AWS S3 console. The 'Last access time updates' section is expanded, showing the current setting is 'Disabled'. A note below explains that when disabled, certain behaviors apply to objects in the bucket. A yellow callout box highlights a note about updating last access time when retrieving objects, stating it can reduce performance. Two radio button options are shown: 'Enable last access time updates when retrieving an object' (unchecked) and 'Disable last access time updates when retrieving an object' (checked). A 'Save changes' button is at the bottom right.

- 「変更を保存」を選択します。

## 関連情報

["テナント管理権限"](#)

["ILM を使用してオブジェクトを管理する"](#)

**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必要がある場合は、そのバケットに Cross-Origin Resource Sharing (CORS) を設定できます。

#### 必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Manage All Buckets 権限または 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。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>。

#### 手順

1. CORS を有効にするために必要な XML をテキストエディタで作成します。

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. Tenant Manager で、 \* Storage (S3) \* > \* Buckets \* を選択します。

3. リスト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 \* > \* Cross-Origin Resource Sharing (CORS) \* を選択します。

- [ \* CORS を有効にする \* ] チェックボックスをオンにします。
- CORS 設定 XML をテキストボックスに貼り付け、\* 変更内容を保存 \* を選択します。

Cross-Origin Resource Sharing (CORS) Disabled

Configure Cross-Origin Resource Sharing (CORS) for an S3 bucket if you want that bucket and objects in that bucket to be accessible to web applications in other domains.

Enable CORS

Clear

```
<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>
  </corsRule>

```

Save changes

- バケットの CORS 設定を変更するには、テキストボックスで CORS 設定 XML を更新するか、\* Clear \* を選択してやり直してください。次に、「変更を保存」を選択します。
- バケットの CORS を無効にするには、\* CORS を有効にする \* チェックボックスの選択を解除し、\* 変更内容を保存 \* を選択します。

### S3/バケットを削除しています

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

#### 必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Manage All Buckets 権限または 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。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

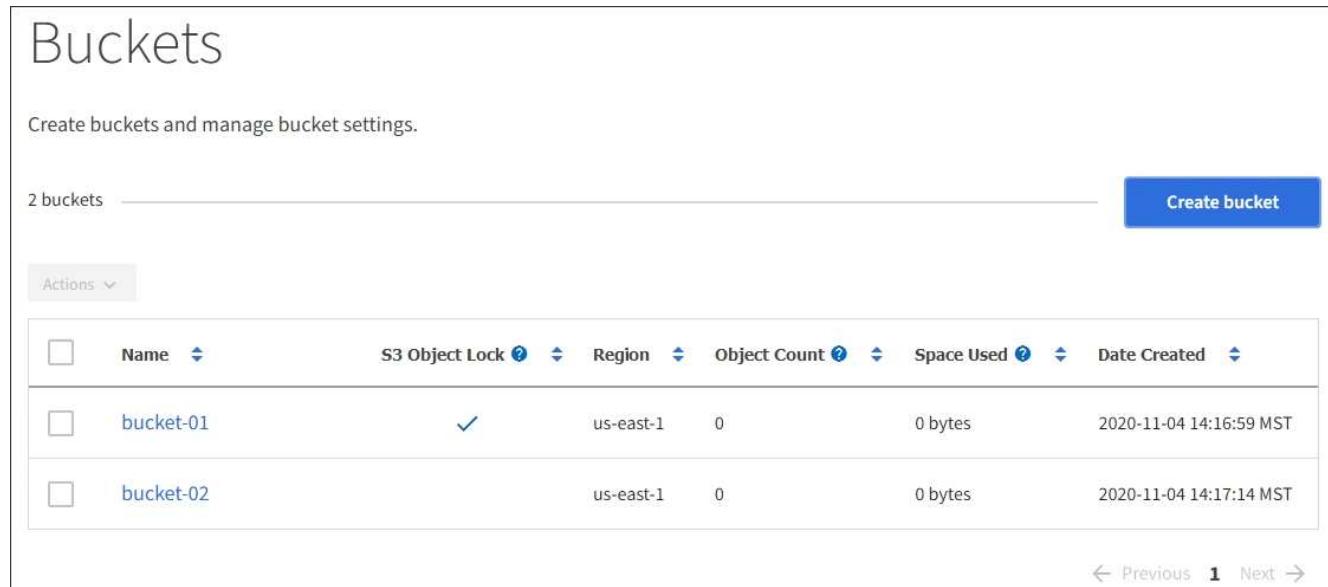
以下の手順では、Tenant Manager を使用して S3 バケットを削除する方法について説明します。テナント管理APIまたはS3 REST APIを使用してS3バケットを削除することもできます。

オブジェクトまたは最新でないオブジェクトバージョンが含まれている 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、情報ライフサイクル管理を使用してオブジェクトを管理する手順を参照してください。

## 手順

- ストレージ ( S3 ) \* > \* バケット \* を選択します。

バケットページが表示され、既存の S3 バケットがすべて表示されます。



Buckets

Create buckets and manage bucket settings.

2 buckets

Actions

Name	S3 Object Lock	Region	Object Count	Space Used	Date Created
bucket-01	✓	us-east-1	0	0 bytes	2020-11-04 14:16:59 MST
bucket-02		us-east-1	0	0 bytes	2020-11-04 14:17:14 MST

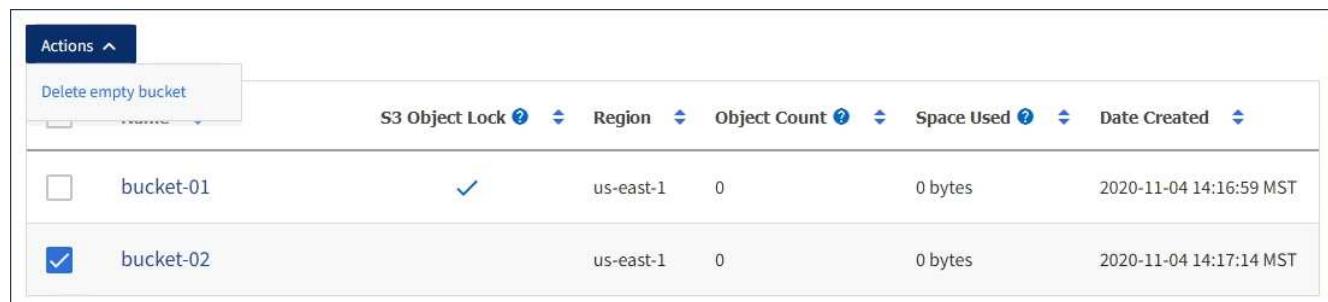
Create bucket

← Previous 1 Next →

- 削除する空のバケットのチェックボックスを選択します。

[ アクション ] メニューが有効になります。

- アクションメニューから\*空のバケットを削除\*を選択します。

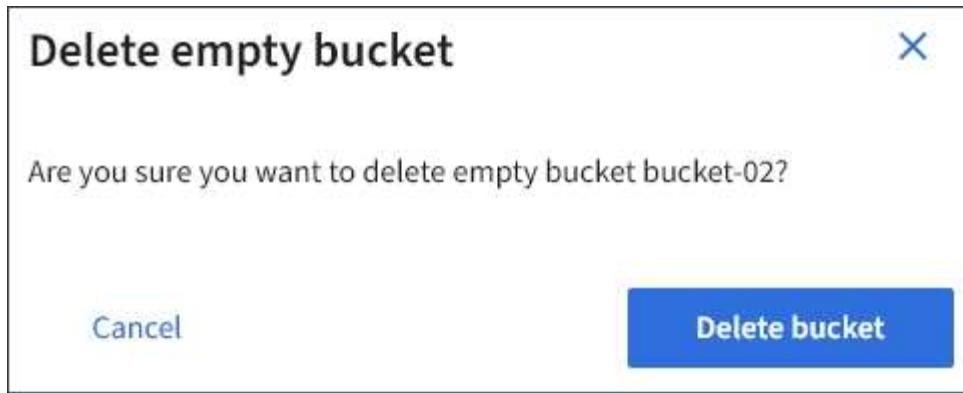


Actions

Delete empty bucket

Name	S3 Object Lock	Region	Object Count	Space Used	Date Created
bucket-01	✓	us-east-1	0	0 bytes	2020-11-04 14:16:59 MST
bucket-02	✓	us-east-1	0	0 bytes	2020-11-04 14:17:14 MST

確認メッセージが表示されます。



4. バケットを削除してもよろしいですか？\*バケットの削除\*を選択します。

StorageGRID は、バケットが空であることを確認してから、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。バケットを削除する前に、すべてのオブジェクトを削除する必要があります。

 Unable to delete the bucket because it is not empty. You must delete all objects before you can delete this bucket.

#### 関連情報

["ILM を使用してオブジェクトを管理する"](#)

## S3プラットフォームサービスの管理

S3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、プラットフォームサービスを使用して外部サービスを利用し、S3バケットに対してCloudMirrorレプリケーション、通知、および検索統合を設定できます。

- ["プラットフォームサービスとは"](#)
- ["プラットフォームサービスの使用に関する考慮事項"](#)
- ["プラットフォームサービスエンドポイントの設定"](#)
- ["CloudMirrorレプリケーションの設定"](#)
- ["イベント通知を設定する"](#)
- ["検索統合サービスを使用する"](#)

### プラットフォームサービスとは

StorageGRID プラットフォームサービスは、ハイブリッドクラウド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 \* : StorageGRID CloudMirror レプリケーションサービスは、StorageGRID バケットから指定され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め使用します。

たとえば、CloudMirror レプリケーションを使用して特定の顧客レコードを Amazon S3 にミラーリングし、AWS サービスを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 \* : バケット単位のイベント通知は、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、指定された外部の Amazon Simple Notification Service™ (SNS) に送信するために使用します。

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 \* : 検索統合サービスは、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ために使用します。

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て設定できます。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、Tenant Manager またはテナント管理 API を使用して、設定した外部エンドポイントと通信します。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、Simple Notification Service (SNS) トピック、ローカル、AWS など) にホストさ

れる Elasticsearch クラスタなど) です。

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することができます。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
CloudMirror レプリケーション	<ul style="list-style-type: none"><li>GET Bucket replication</li><li>PUT Bucket replication</li></ul>
通知	<ul style="list-style-type: none"><li>GET Bucket notification</li><li>PUT Bucket notification</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> <p>これらは StorageGRID 独自の処理です。</p>

StorageGRID でのこれらの API の実装方法の詳細については、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

["S3 を使用する"](#)

["CloudMirror レプリケーションサービスの概要"](#)

["バケットの通知の概要"](#)

["検索統合サービスの概要"](#)

["プラットフォームサービスの使用に関する考慮事項"](#)

**CloudMirror レプリケーションサービスの概要**

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 ポリシーとは別に動作します。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。

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 AWS S3 デスティネーションにオブジェクトをコピーする場合は、Amazon S3 では各 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。1 つの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て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。

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は、StorageGRID によって「replicas.」とマークされます。デスティネーションの 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、意図しないレプリケーションのループが発生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 は、2 つのグリッド間の双方向 CloudMirror をサポートしています。

デスティネーションバケット内ではイベントは一意になるとは限らず、その順序も保証されません。確実に配信することを目的とした処理の結果として、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に設定します。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。

#### 関連情報

["CloudMirrorレプリケーションの設定"](#)

#### バケットの通知の概要

S3 バケットに対する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の Amazon Simple Notification Service ( SNS ) に送信できます。

イベント通知を設定するには、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の通知を設定し、デスティネーションの 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。

一意になるとは限らず、その順序も保証されません。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 イベント通知は Amazon S3 API に準拠しますが、次の制限事項があります。

- 次のイベントタイプには通知を設定できません。これらのイベントタイプは \* サポートされていません。
  - ° `s3:ReducedRedundancyLostObject`
  - ° `s3:ObjectRestore:Completed`
- 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使用されないキーおよび特定の値が使用されるキーがあります。

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

## 関連情報

### ["イベント通知を設定する"](#)

## 検索統合サービスの概要

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る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。ドキュメントにインデックスを付けた後は、インデックス内のドキュメントのフィールドタイプを編集できません。

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、バケット内の既存のオブジェクトに関する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。サポートされている Elasticsearch のバージョンを確認するには、Interoperability Matrix Tool を使用してください。

## 関連情報

"NetApp Interoperability Matrix Tool で確認できます"

"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"

"検索統合サービスの設定"

## プラットフォームサービスの使用に関する考慮事項

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。

### 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	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。  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。  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。
順序保証	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。  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。

考慮事項	詳細
ILM ベースのオブジェクト削除	<p>AWS CRR サービスと SNS サービスの削除動作を一致させるため、StorageGRID の 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す。</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 ではサポートされません <code>x-amz-replication-status</code> ヘッダー。
オブジェクトのサイズ	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5TBであり、StorageGRID でサポートされる最大オブジェクトサイズと同じです。
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> <ul style="list-style-type: none"> <li>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 とは関連がありません。</li> </ul>

オブジェクトバージョンのタグ付け	<p>CloudMirror サービスでは、S3 プロトコルの制限事項により、バージョン ID を提供する PUT Object tagging 要求と DELETE Object tagging 要求が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 には関連がないため、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、バージョン ID を指定しない PUT Object tagging 要求と DELETE Object tagging 要求は、CloudMirror サービスによってレプリケートされます。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は、レプリケーション処理がAccessDeniedエラーで失敗します。</p>

#### 関連情報

["S3 を使用する"](#)

### プラットフォームサービスエンドポイントの設定

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トリ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 権限のあるテナントユーザである必要があります。詳細については、StorageGRID 管理者にお問い合わせください。

## プラットフォームサービスエンドポイントとは

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 S3 バケットにオブジェクトをレプリケートする場合は、AWS のデスティネーションバケットにアクセスするために StorageGRID で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。また、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。この方法は、オブジェクトの作成に関する通知がある SNS トピックに送信し、オブジェクトの削除に関する通知を別の SNS トピックに送信する場合などに使用します。

### 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、Simple Notification Service (SNS) エンドポイントをサポートします。Simple Queue Service (SQS) エンドポイントまたは AWS Lambda エンドポイントはサポートされていません。

### 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あるか、AWS クラウドなどの別の場所でホストされている可能性があります。

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。タイプはエンドポイントの作成前に作成しておく必要があります。StorageGRID は、オブジェクトメタデータをエンドポイントに送信するときに必要に応じてタイプを作成します。

### 関連情報

#### ["StorageGRID の管理"](#)

### プラットフォームサービスのエンドポイントのURNの指定

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 を作成する際、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
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	バケット名
通知	<code>sns-topic-name</code> を入力します
検索統合	<code>domain-name/index-name/type-name</code>  • 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でホストされるサービスのURN

AWS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：

```
urn:mysite:sns:optional:optional:sns-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す。

## プラットフォームサービスエンドポイントの作成

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。

### 必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 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化されている必要があります。
- Manage Endpoints 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。
- 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く必要があります。
  - CloudMirror レプリケーション： S3 バケット
  - イベント通知： SNS 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く必要があります。
  - 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の指定"](#)

- 認証クレデンシャル (必要な場合)：
  - 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
- セキュリティ証明書 (カスタム CA 証明書を使用する場合)

### 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。

# 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.

0 endpoints

[Create endpoint](#)

[Delete endpoint](#)

Display name [?](#) [▲](#)

Last error [?](#) [▲](#)

Type [?](#) [▲](#)

URI [?](#) [▲](#)

URN [?](#) [▲](#)

No endpoints found

[Create endpoint](#)

2. [\* エンドポイントの作成 \*] を選択します。

# Create endpoint

1 Enter details 2 Select authentication type 3 Verify server

Optional

Optional

## Enter endpoint details

Enter the endpoint's display name, URI, and URN.

Display name ?

URI ?

URN ?

Cancel

Continue

3. エンドポイントとその目的を簡単に説明する表示名を入力します。

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

4. [\* URI\*] フィールドに、エンドポイントの 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、 HTTPS URI にはポート 443 が、 HTTP URI にはポート 80 が使用されます。

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。



単一点障害を回避するには、できるだけ負荷分散ノードの HA グループに接続する必要があります。

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

```
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で使用される場合は、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、必要なクレデンシャルを入力します。

Create endpoint

1 Enter details      2 Select authentication type      3 Verify server

**Authentication type** ?

Select the method used to authenticate connections to the endpoint.

Anonymous

Anonymous

Access Key

Basic HTTP

Previous Continue

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>

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

1 Enter details      2 Select authentication type      3 Verify server

**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-----
abcdefghijklmnopqrstuvwxyz0ABCDEFGHIJKLM
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でない場合は、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の指定"](#)

["CloudMirrorレプリケーションの設定"](#)

["イベント通知を設定する"](#)

["検索統合サービスの設定"](#)

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ています

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。

#### 必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Manage Endpoints 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。

#### 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	Last error	Type	URI	URN
<input type="checkbox"/>	my-endpoint-1		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket1
<input type="checkbox"/>	my-endpoint-2	✖ 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。

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

Type: [S3 Bucket](#)

URI: <http://10.96.104.167:10443>

URN: [urn:sgws:s3:::bucket1](#)

**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は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の編集

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のエンドポイントの URN を変更することはできません。

#### 必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Manage Endpoints 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。

#### 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	Last error	Type	URI	URN
<input type="checkbox"/>	my-endpoint-1		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket1
<input type="checkbox"/>	my-endpoint-2	✖ 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。

## Overview

Display name:	my-endpoint-3 
Type:	Notifications
URI:	http://10.96.104.202:8080/
URN:	arn:aws:sns:us-west-2::example1

[Connection](#)

[Configuration](#)

## Edit configuration

### Endpoint details

URI 

http://10.96.104.202:8080/

URN 

arn:aws:sns:us-west-2::example1

### Authentication type

Basic HTTP

Username 

testme

Password 

\*\*\*\*\*

[Edit password](#)

### Verify server

Use custom CA certificate

Use operating system CA certificate

Do not verify certificate

```
-----BEGIN CERTIFICATE-----  
abcdefghijklmnopqrstuvwxyz0ABCDEFGHIJKLMNOPQRSTUVWXYZ  
-----END CERTIFICATE-----
```

[Test and save changes](#)

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。
    - Basic HTTP 認証の場合は、必要に応じてユーザ名を変更します。必要に応じてパスワードを変更するには、「\* パスワードを編集」を選択し、新しいパスワードを入力します。変更をキャンセルする必要がある場合は、\* パスワードの編集を元に戻す\*を選択します。
    - 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。
  - 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。

#### 関連情報

["プラットフォームサービスエンドポイントの作成"](#)

プラットフォームサービスエンドポイントを削除しています

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す。

#### 必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Manage Endpoints \* 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。

#### 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	Last error	Type	URI	URN
<input type="checkbox"/>	my-endpoint-1		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket1
<input type="checkbox"/>	my-endpoint-2	✖ 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

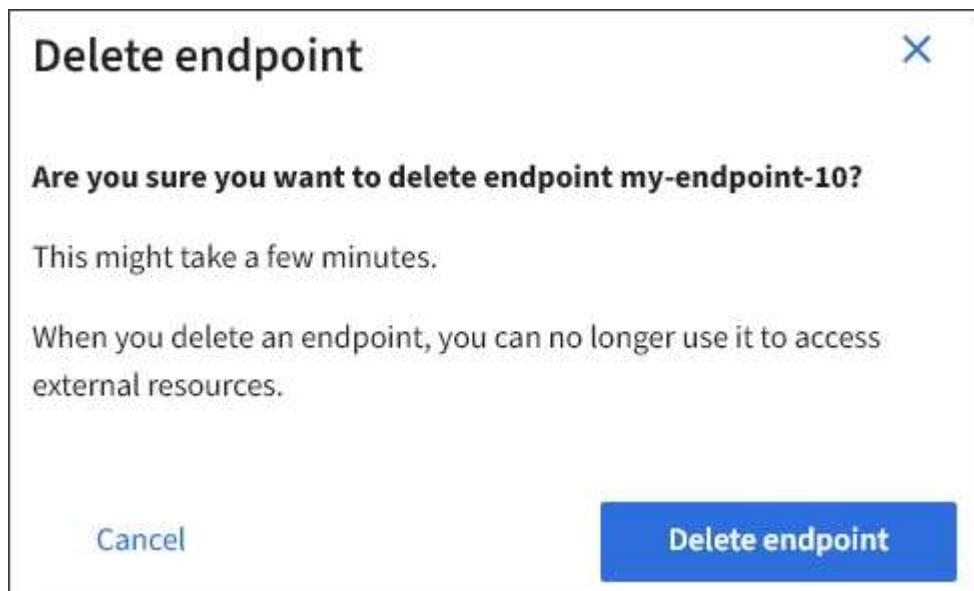
2. 削除する各エンドポイントのチェックボックスを選択します。



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。

3. [\* アクション \* > \* エンドポイントの削除 \*] を選択します。

確認メッセージが表示されます。



4. [\* エンドポイントの削除 \*] を選択します。

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

StorageGRID がプラットフォームサービスのエンドポイントとの通信を試みたときにエラーが発生した場合は、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ています

過去 7 日間にプラットフォームサービスエンドポイントでエラーが発生した場合は、 Tenant Manager の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、プラットフォームサービスのエンドポイント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:	<a href="#">my-endpoint-2</a> 
Type:	Search
URI:	<a href="http://10.96.104.30:9200">http://10.96.104.30:9200</a>
URN:	<a href="#">urn:sgws:es:::mydomain/sveloso/_doc</a>

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

エラーが現在も継続しているかどうかを確認しています

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。

## 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'エンドポイントの資格情報または宛先アクセスを更新する必要があります詳細は'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：\* Test and save changes \*を選択すると、StorageGRIDは更新されたエンドポイントを検証し、現在のクレデンシャルでアクセスできることを確認します。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。

### 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。このため、プラットフォームサービスの使用時にエラーが発生した場合（「403 Forbidden」など）、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。

他のプラットフォームサービスのトラブルシューティング

追加情報 プラットフォームサービスのトラブルシューティングについては、StorageGRIDの管理手順を参照してください。

### ["StorageGRIDの管理"](#)

#### 関連情報

##### ["プラットフォームサービスエンドポイントの作成"](#)

##### ["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ています"](#)

##### ["プラットフォームサービスエンドポイントの編集"](#)

## CloudMirrorレプリケーションの設定

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いずれかです。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。

#### 必要なもの

- ・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化されている必要

があります。

- ・レプリケーションのソースとして機能するバケットを作成しておく必要があります。
- ・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を用意しておく必要があります。また、その URN が必要です。
- ・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できるように、Manage All Buckets 権限または Root Access 権限を持つユーザグループに属している必要があります。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。バケットの CloudMirror レプリケーションを有効にするには、有効なバケットレプリケーション設定 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、Amazon のドキュメントのクロスリージョンレプリケーション (CRR) に関する説明を参照してください。StorageGRID が S3 バケットのレプリケーション設定 API を実装する方法については、S3 クライアント アプリケーションを実装する手順を参照してください。

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、を参照してください STANDARD ストレージクラスが使用されています。
  - 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. 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 \* > \* 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オンにします。

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。

- 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。

- 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

["CloudMirrorレプリケーションサービスの概要"](#)

["S3 を使用する"](#)

["プラットフォームサービスエンドポイントの作成"](#)

## 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™ (SNS) をサポートするデスティネーションサービスに送信できます。

### 必要なもの

- ・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化されている必要があります。
- ・通知のソースとなるバケットを作成しておく必要があります。
- ・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存在し、そのURNを把握している必要があります。
- ・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できるように、Manage All Buckets 権限またはRoot Access 権限を持つユーザグループに属している必要があります。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るSimple Notification Service (SNS) の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 がS3 バケットの通知設定 API を実装する方法については、S3 クライアントアプリケーションを実装する手順を参照してください。

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つ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

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).

- 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>
    <Topic>arn:aws:sns:us-east-1:050340950352:sgws-topic</Topic>
  </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。

a. 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 SNS 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 AWS Simple Notification Service ( SNS ) でホストされている場合は、通知が配信されたらユーザに 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。

#### 関連情報

["バケットの通知の概要"](#)

["S3 を使用する"](#)

["プラットフォームサービスエンドポイントの作成"](#)

### 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。

次のカスタムのStorageGRID S3 REST API処理の詳細については、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。

- `DELETE Bucket metadata notification configuration` 要求
- `GET Bucket metadata notification configuration` 要求
- `PUT Bucket metadata notification configuration` 要求

#### 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"](#)

["検索統合サービスの設定"](#)

["S3 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、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無効で、送信時に拒否されます。たとえば、プレフィックスがの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コンテナタグ。  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コンテナタグ。  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。

名前	説明	必須
ID	<p>ルールの一意の識別子。</p> <p>Rule 要素に含まれています。</p>	いいえ
ステータス	<p>Status には「 Enabled 」または「 Disabled 」を指定できます。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-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Videos-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/videos</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-west-1:2222222:domain/es-
domain/graphics/videotype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

関連情報

"S3 を使用する"

"検索統合サービスで生成される JSON"

"検索統合サービスの設定"

検索統合サービスの設定

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。

必要なもの

- 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化されている必要があります。
- 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く必要があります。
- 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存在し、その URN を把握している必要があります。
- 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できるように、 Manage All Buckets 権限または Root Access 権限を持つユーザグループに属している必要があります。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。オブジェクトをすでに含む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は送信されません。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-1:111111111111: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 of the AWS StorageGRID Tenant Manager. The 'Search integration' section is expanded, showing the following configuration:

Enable the search integration service to send object metadata to a destination search index whenever an object is created, deleted, or its metadata or tags are updated.

- Platform services must be enabled for your tenant account by a StorageGRID administrator.
- You must have already configured an endpoint for the search integration service.
- You must specify the URN of that endpoint in the search integration configuration XML for the bucket you want to index.

Enable search integration

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

**Save changes**



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 \* チェックボックスの選択を解除します。
- 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

["検索統合サービスの概要"](#)

["検索統合用の XML を設定します"](#)

["S3 を使用する"](#)

["プラットフォームサービスエンドポイントの作成"](#)

**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 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	<p>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</p> <p>key: value</p>

を入力します	項目名と概要
タグ	<p>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</p> <p>key:value</p>

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 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。ドキュメントにインデックスを付けた後は、インデックス内のドキュメントのフィールドタイプを編集できません。



## 著作権に関する情報

Copyright © 2025 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

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

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

ネットアップは、ここに記載されているすべての製品に対する変更を隨時、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 5225.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

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

## 商標に関する情報

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