



# **StorageGRID を使用します**

## StorageGRID

NetApp  
November 04, 2025

# 目次

StorageGRIDのテナントとクライアントの使用	1
テナントアカウントを使用する	1
テナントアカウントを使用する：概要	1
サインインとサインアウトの方法	2
Tenant Managerのダッシュボードについて理解する	7
テナント管理 API	10
グリッドフェデレーション接続を使用する	15
グループとユーザを管理します	29
S3 アクセスキーを管理します	49
S3 バケットを管理する	54
S3 プラットフォームサービスを管理します	76
S3 REST APIを使用する	117
S3 REST APIでサポートされるバージョンと更新	117
クイックリファレンス：サポートされるS3 API要求	120
S3 REST API設定のテスト	139
StorageGRID での S3 REST API の実装	141
Amazon S3 REST APIのサポート	156
StorageGRIDのカスタム処理	206
バケットとグループのアクセスポリシー	227
監査ログで追跡される S3 処理	254
Swift REST APIの使用（廃止）	255
Swift REST APIの使用：概要	255
Swift REST API設定のテスト	258
Swift REST API でサポートされている処理	260
StorageGRID の Swift REST API 処理	272
監査ログで追跡される Swift 処理	276

# StorageGRIDのテナントとクライアントの使用

## テナントアカウントを使用する

### テナントアカウントを使用する：概要

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

テナントアカウントとは何ですか？

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

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

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



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

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

### テナントアカウントを作成する方法

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

- ・ テナント名、 クライアントタイプ (S3 または Swift) 、 オプションのストレージクォータなどの基本情報。
- ・ テナントアカウントに対する権限 ( テナントアカウントが S3 プラットフォームサービスを使用できるか、 独自のアイデンティティソースを設定できるか、 S3 Select を使用できるか、 グリッドフェデレーション接続を使用できるかなど ) 。
- ・ テナントの初期ルートアクセス ( StorageGRID システムがローカルグループとユーザ、 アイデンティティフェデレーション、 シングルサインオン (SSO) のいずれを使用しているかに基づく ) 。

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

### S3 テナントを設定する

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

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



S3バケットはTenant Managerを使用して作成および管理できますが、 "S3 クライアント" または "S3コンソール" オブジェクトの取り込みと管理を行います。

### Swift テナントを設定します

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

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



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

## サインインとサインアウトの方法

### Tenant Manager にサインインします

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

作業を開始する前に

- ・ログインクレデンシャルが必要です。
- ・Tenant ManagerにアクセスするためのURLを、グリッド管理者から入手しておきます。URL は次のいずれかの例のようになります。

`https://FQDN_or_Admin_Node_IP/`

`https://FQDN_or_Admin_Node_IP:port/`

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

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

URLには、必ず完全修飾ドメイン名（FQDN）、管理ノードのIPアドレス、または管理ノードのHAグループの仮想IPアドレスが含まれます。ポート番号、20桁のテナントアカウントID、またはその両方を指定することもできます。

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

#### 手順

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

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

## SSOを使用しない

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

- Grid Manager のサインインページが表示されます。[Tenant sign-in]\*リンクを選択します。

The screenshot shows the login interface for the NetApp StorageGRID Grid Manager. At the top, the title 'NetApp StorageGRID® Grid Manager' is displayed. Below it are two input fields: 'Username' and 'Password'. A blue 'Sign in' button is positioned below the password field. At the bottom of the page, there are three links: 'Tenant sign in' (which is highlighted with a green rectangular border), 'NetApp support', and 'NetApp.com'.

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



# Tenant Manager

## Recent

## Account

## Username

## Password

**Sign in**

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

- 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. ユーザ名とパスワードを入力します。
- iii. 「サインイン」を選択します。

Tenant Managerダッシュボードが表示されます。

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

## SSOを使用する

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

- 組織のSSOページ。例：

Sign in with your organizational account

Sign in

標準のSSOクレデンシャルを入力し、\*[サインイン]\*を選択します。

- Tenant Manager の SSO サインインページ。

NetApp StorageGRID®

## Tenant Manager

### Recent

### Account

Sign in

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

- 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」を選択します。
- 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。

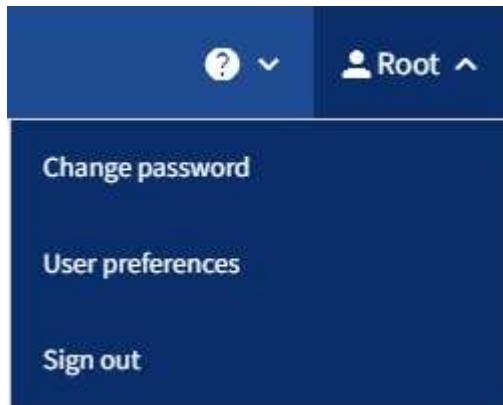
Tenant Managerダッシュボードが表示されます。

## Tenant Manager からサインアウトします

Tenant Managerの操作が完了したら、サインアウトして、権限のないユーザがStorageGRID システムにアクセスできないようにする必要があります。ブラウザのクッキーの設定によっては、ブラウザを閉じて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. ユーザ名を選択し、\*[サインアウト]\*を選択します。

- SSO を使用していない場合：

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



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

- SSO が有効になっている場合は、次

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



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

## Tenant Managerのダッシュボードについて理解する

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



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

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

# 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: Tenant02  
ID: 3341 1240 0546 8283 2208

Platform services enabled  
 Can use own identity source  
 S3 Select enabled

## テナントアカウントの概要

ダッシュボードの上部には、次の情報が表示されます。

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

リンクを選択すると詳細を確認できます。

ダッシュボードの右側には、次の情報が表示されます。

- テナントのオブジェクトの合計数。

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

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

## ストレージとクォータの使用状況

ストレージ使用状況パネルには、次の情報が表示されます。

- テナントのオブジェクトデータの量。



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

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



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



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

## ク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\*」アラートがトリガれます。アラートの推奨される対処方法を実行します。



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

クオータを超えた場合は、新しいオブジェクトをアップロードできません。



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

## エンドポイントエラー

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



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

をクリックして詳細を表示します "プラットフォームサービスエンドポイントエラー"を選択し、\*[エンドポイント]\*を選択して[エンドポイント]ページを表示します

## テナント管理 API

### テナント管理 APIについて理解する

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

### テナント管理 API :

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

- ・使用 "無停止アップグレードをサポートするためのバージョン管理"。

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

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

## API 处理

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

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

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

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



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

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

## 処理の詳細

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

**groups** Operations on groups

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

**Parameters**

**Name** **Description**

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

**Responses**

Response content type **application/json**

**Code** **Description**

200	Example Value: Model
-----	----------------------

```
{  
  "responseTime": "2018-02-01T16:22:31.066Z",  
  "status": "success",  
  "apiVersion": "2.2"  
}
```

## 問題 API 要求



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

## 手順

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

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

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

#### テナント管理 API のバージョン管理

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

たとえば、このリクエストURLはAPIのバージョン4を指定します。

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

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

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

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

StorageGRIDソフトウェアを初めてインストールすると、最新バージョンのAPIのみが有効になります。ただし、StorageGRID の新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。



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

古い要求は、次の方法で廃止とマークされます。

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

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

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

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

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

要求の **API** バージョンを指定します

パスパラメータを使用して API バージョンを指定できます (`/api/v4`) またはヘッダー (`Api-Version: 4`)。両方の値を指定した場合は、ヘッダー値がパス値よりも優先されます。

```
curl https://[IP-Address]/api/v4/grid/accounts
curl -H "Api-Version: 4" https://[IP-Address]/api/grid/accounts
```

## クロスサイトリクエストフォージェリ (CSRF) の防止

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

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

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

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

```

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

```

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。

CSRF 保護を設定するには、を使用してください "[Grid 管理 API](#)" または "[テナント管理 API](#)"。



CSRFトークンクッキーが設定されている要求では、CSRF攻撃に対する追加の保護としてJSON要求本文が必要な要求に対して「Content-Type:application/json」ヘッダーも適用されます。

## グリッドフェデレーション接続を使用する

テナントグループとテナントユーザのクローンを作成します

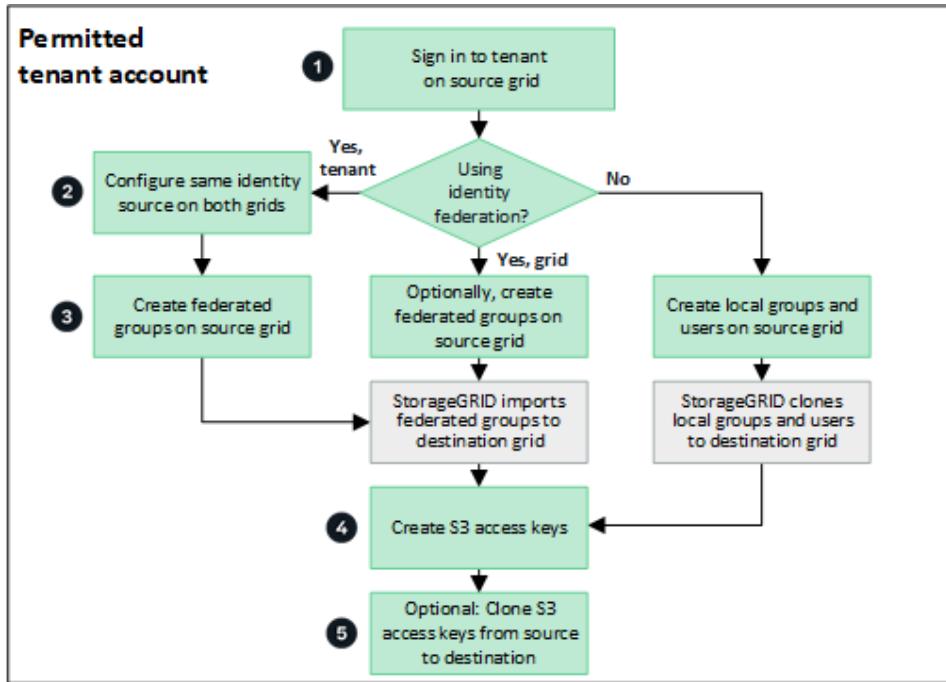
グリッドフェデレーション接続を使用するようにテナントを作成または編集した場合、そのテナントは1つのStorageGRIDシステム（ソーステナント）から別のStorageGRIDシステム（レプリカテナント）にレプリケートされます。テナントがレプリケートされると、ソーステナントに追加されたすべてのグループおよびユーザがレプリカテナントにクローニングされます。

テナントが最初に作成されたStorageGRIDシステムは、テナントの\_source grid\_です。テナントがレプリケートされているStorageGRIDシステムは、テナントの\_destination grid\_です。両方のテナントアカウントに、アカウントID、名前、概要、ストレージクオータ、および割り当てられた権限が同じである。ただし、デスティネーションテナントには最初はrootユーザのパスワードが設定されていません。詳細については、を参照してください "[アカウントクローンとは何ですか](#)" および "[許可されたテナントを管理する](#)"。

テナントアカウント情報のクローニングは、で必要です "[グリッド間レプリケーション](#)" バケットオブジェクト。両方のグリッドに同じテナントグループとユーザが配置されているため、どちらのグリッドでも対応するバケットとオブジェクトにアクセスできます。

## アカウントクローンのテナントワークフロー

テナントアカウントに\* Use grid federation connection \*権限がある場合は、ワークフロー図を確認して、グループ、ユーザ、S3アクセスキーをクローニングする手順を確認してください。



ワークフローの主な手順は次のとおりです。

1

テナントにサインインします

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

2

必要に応じて、アイデンティティフェデレーションを設定します

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

3

グループとユーザを作成します

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

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

4

#### S3アクセスキーを作成

可能です "独自のアクセスキーを作成します" またはをクリックします "別のユーザのアクセスキーを作成します" ソースグリッドまたはデスティネーショングリッドのいずれかで、そのグリッド上のバケットにアクセスします。

5

#### 必要に応じて、S3アクセスキーをクローニングします

両方のグリッドで同じアクセスキーを使用してバケットにアクセスする必要がある場合は、ソースグリッドでアクセスキーを作成し、Tenant Manager APIを使用してデスティネーショングリッドに手動でクローニングします。手順については、を参照してください "[APIを使用してS3アクセスキーをクローニングします](#)"。

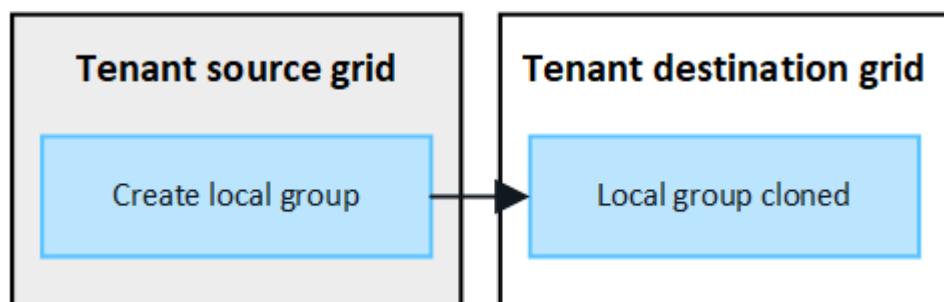
グループ、ユーザ、S3アクセスキーのクローニング方法

テナントソースグリッドとテナントデスティネーショングリッドの間で、グループ、ユーザ、S3アクセスキーがどのようにクローニングされるかを理解するには、このセクションを確認します。

ソースグリッドに作成されたローカルグループがクローニングされます

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

元のグループとそのクローンには、同じアクセスモード、グループ権限、S3グループポリシーが設定されています。手順については、を参照してください "[S3 テナント用のグループを作成します](#)"。



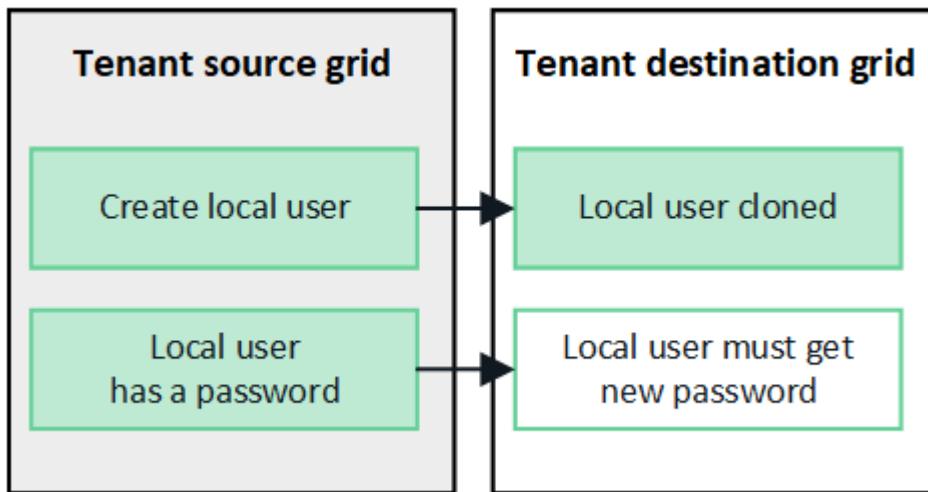
ソースグリッドでローカルグループを作成するときに選択したユーザは、そのグループがデスティネーショングリッドにクローニングされるときに含まれません。このため、グループを作成するときにユーザーを選択しないでください。代わりに、ユーザの作成時にグループを選択します。

ソースグリッドに作成されたローカルユーザがクローニングされます

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

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

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

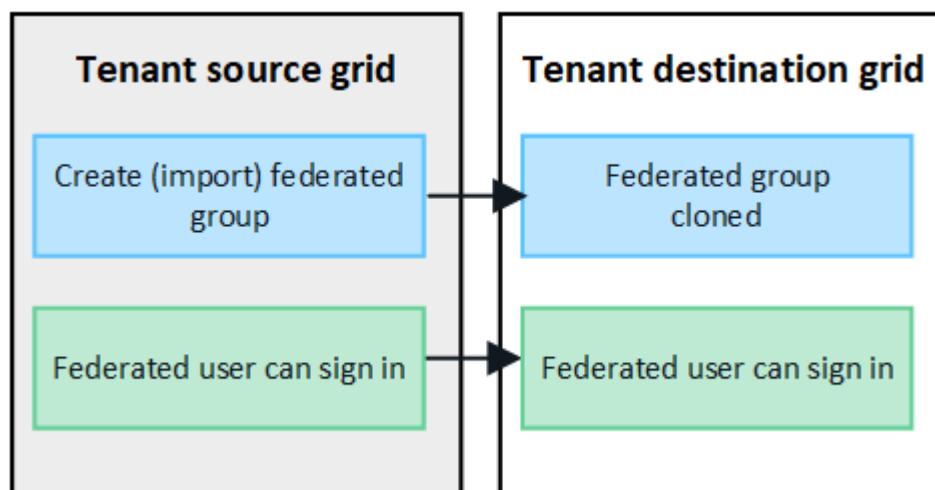


ソースグリッドに作成されたフェデレーテッドグループがクローニングされます

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

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

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



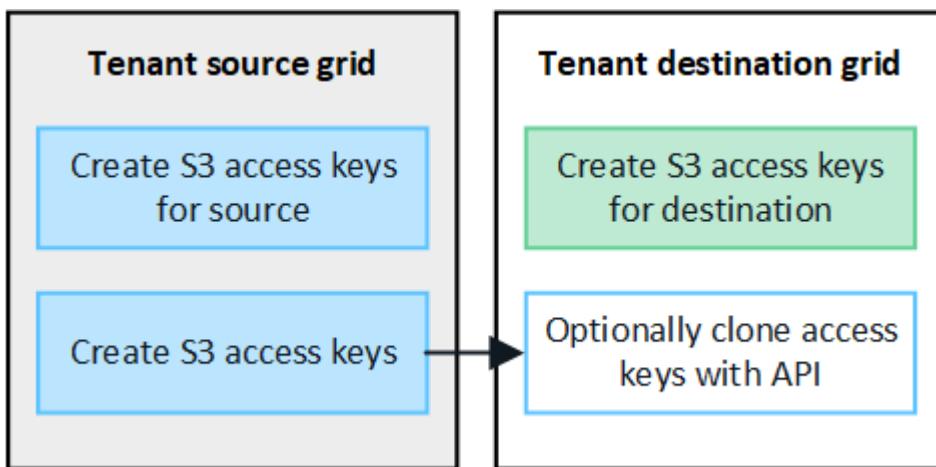
S3アクセキーは手動でクローニングできます

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

2つのグリッドでアクセキーを管理するには、次のいずれかを実行します。

- グリッドごとに同じキーを使用する必要がない場合は、できます "独自のアクセキーを作成します" または "別のユーザのアクセキーを作成します" をクリックします。
- 両方のグリッドで同じキーを使用する必要がある場合は、ソースグリッドでキーを作成し、Tenant

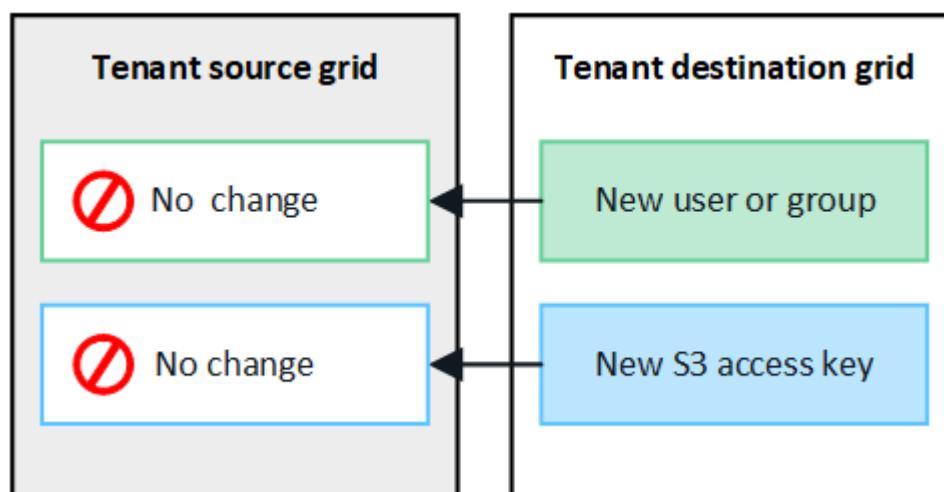
Manager APIを使用して手動でキーを作成できます "キーのクローンを作成します" ターゲットグリッドに移動します。



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

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

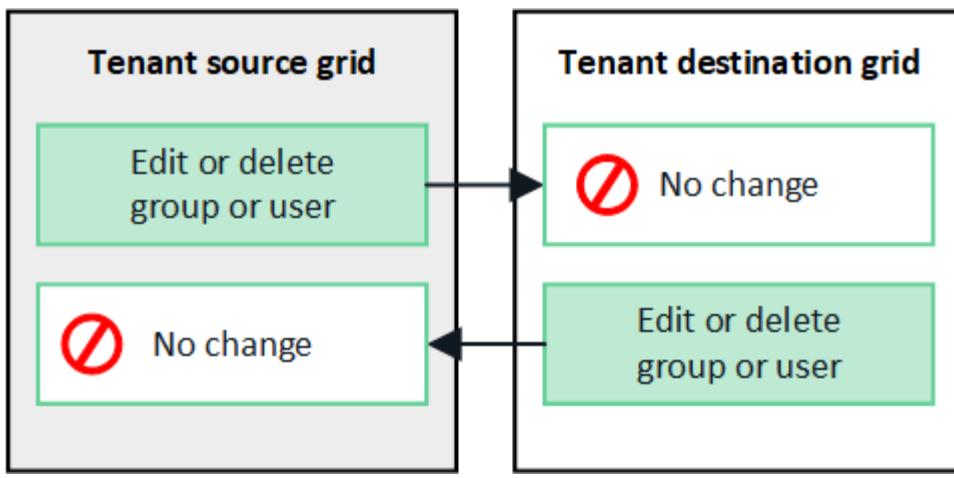
クローンングは、テナントのソースグリッドからテナントのデスティネーショングリッドにのみ実行されます。テナントのデスティネーショングリッドでグループとユーザを作成またはインポートした場合、StorageGRIDはこれらの項目をテナントのソースグリッドにクローンングしません。



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

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

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



APIを使用してS3アクセスキーをクローニングします

テナントアカウントに\* Use grid federation connection \*権限がある場合は、テナント管理APIを使用して、ソースグリッドのテナントからデスティネーショングリッドのテナントにS3アクセスキーを手動でクローニングできます。

作業を開始する前に

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



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

自分のアクセスキーのクローンを作成します

両方のグリッドで同じバケットにアクセスする必要がある場合は、独自のアクセスキーをクローニングできます。

手順

1. ソースグリッドでTenant Managerを使用し、"独自のアクセスキーを作成します" をダウンロードします .csv ファイル。
2. Tenant Managerの上部で、ヘルプアイコンを選択し、\*[API documentation]\*を選択します。
3. [\* s3 \*]セクションで、次のエンドポイントを選択します。

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

POST

/org/users/current-user/replicate-s3-access-key Clone the current user's S3 key to the other grids.



4. [\* 試してみてください \*] を選択します。
5. body テキストボックスで、AccessKey および secretAccessKey のエントリ例を、ダウンロードした csv \*ファイルの値に置き換えます。

各文字列は必ず二重引用符で囲んでください。

The screenshot shows a UI element for setting a 'body' parameter. It has a red asterisk and the word 'required' next to the label 'body'. Below it is a '(body)' placeholder. To the right is a 'Model' button. The main area contains a JSON object:

```
{  
    "accessKey": "AKIAIOSFODNN7EXAMPLE",  
    "secretAccessKey": "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY",  
    "expires": "2028-09-04T00:00:00Z"  
}
```

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

別のユーザのアクセキーのクローンを作成します

別のユーザが両方のグリッドで同じバケットにアクセスする必要がある場合は、そのユーザのアクセキーをクローニングできます。

手順

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

GET /org/users

- b. [\* 試してみてください \*] を選択します。
  - c. ユーザを検索するときに使用するパラメータを指定します。
  - d. [\* Execute] を選択します。
  - e. 複製するキーを持つユーザーを検索し、\* id \*フィールドの番号をコピーします。
4. [\* s3 \*]セクションで、次のエンドポイントを選択します。

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

POST

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



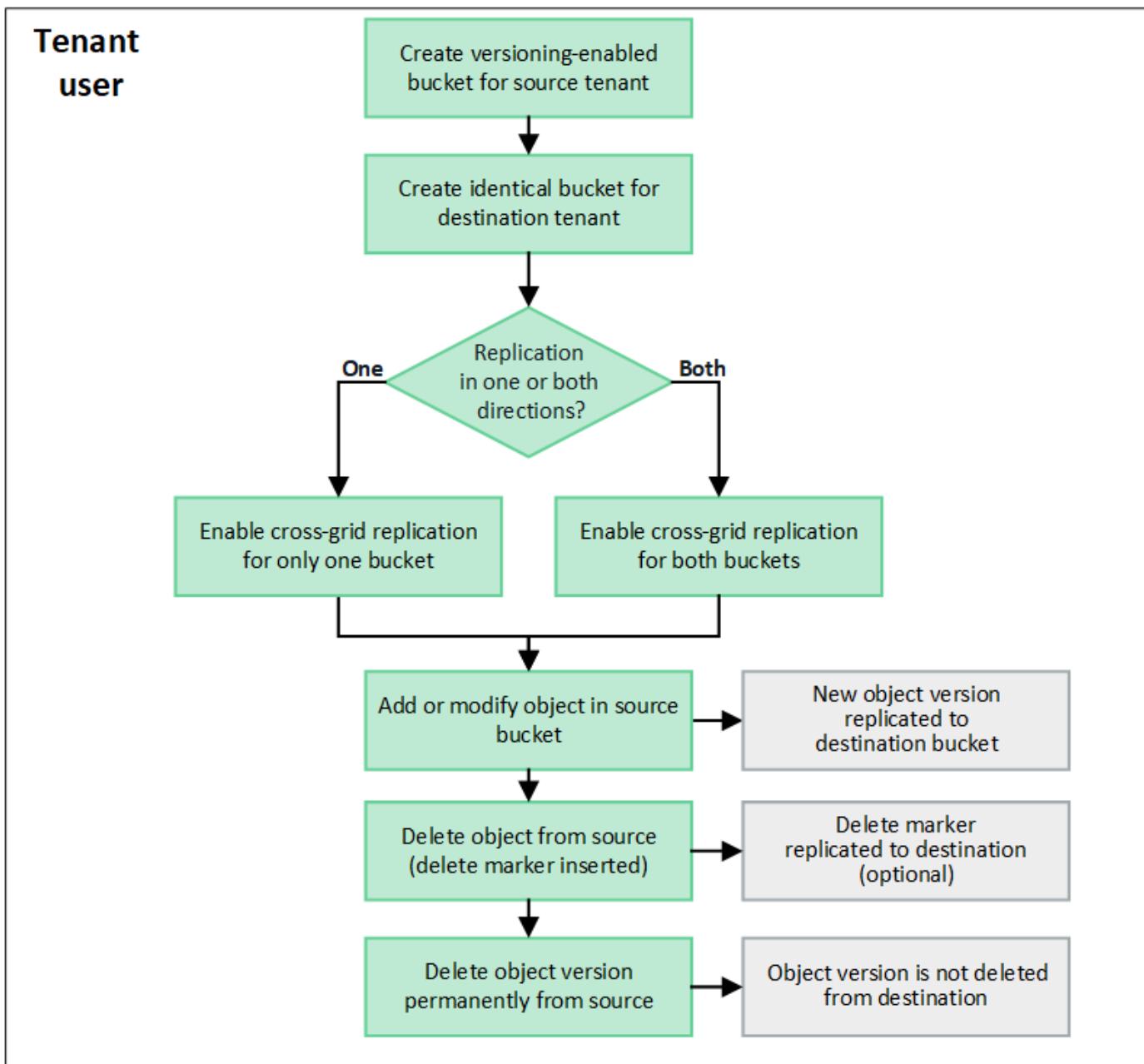
5. [\* 試してみてください \*] を選択します。
6. [userid] テキストボックスに、コピーしたユーザIDを貼り付けます。
7. \* body テキストボックスで、example access key および secret access key のサンプルエントリを、そのユーザの csv ファイルの値に置き換えます。  
文字列は必ず二重引用符で囲んでください。
8. キーが期限切れになる場合は、\* expires の例のエントリを、ISO 8601データタイム形式の文字列として有効期限の日時に置き換えます（例：2023-02-28T22:46:33-08:00）。キーが期限切れにならない場合は、expires エントリの値として null を入力します（または expires \*行とその前のカンマを削除します）。
9. [\* Execute] を選択します。
10. サーバ応答コードが「\* 204 \*」であることを確認します。これは、キーがデスティネーショングリッドに正常にクローニングされたことを示します。

#### グリッド間レプリケーションを管理します

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

#### グリッド間レプリケーションのワークフロー

次のワークフロー図は、2つのグリッド上のバケット間でグリッド間レプリケーションを設定する手順をまとめたものです。これらの手順については、以下で詳しく説明します。



#### グリッド間レプリケーションを設定する

グリッド間レプリケーションを使用する前に、各グリッドの対応するテナントアカウントにサインインし、同一のバケットを作成する必要があります。その後、一方または両方のバケットでグリッド間レプリケーションを有効にできます。

#### 作業を開始する前に

- グリッド間レプリケーションの要件を確認しておく必要があります。を参照してください "[クロスグリッドレプリケーションとは](#)"。
- を使用している "[サポートされている Web ブラウザ](#)"。
- テナントアカウントには\* Use grid federation connection \*権限があり、両方のグリッドに同一のテナントアカウントが存在します。を参照してください "[グリッドフェデレーション接続に許可されているテナントを管理します](#)"。
- サインインするテナントユーザが両方のグリッドにすでに存在し、を含むユーザグループに属している

"rootアクセス権限"。

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

同一のバケットを2つ作成します

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

手順

- グリッドフェデレーション接続のいずれかのグリッドから、新しいバケットを作成します。
  - 両方のグリッドに存在するテナントユーザのクレデンシャルを使用してテナントアカウントにサインインします。

 テナントのデスティネーショングリッドにローカルユーザとしてサインインできない場合は、テナントアカウントのrootユーザがユーザアカウントのパスワードを設定していることを確認します。
  - の指示に従ってください "[S3バケットを作成](#)"。
  - タブで、[オブジェクトのバージョン管理を有効にする]\*を選択します。
  - StorageGRID システムでS3オブジェクトロックが有効になっている場合は、バケットでS3オブジェクトロックを有効にしないでください。
  - [ \* バケットの作成 \* ]を選択します。
  - [完了]を選択します。
- 同じテナントアカウントに対して同じバケットをグリッドフェデレーション接続のもう一方のグリッドに作成するには、上記の手順を繰り返します。



必要に応じて、各バケットで異なるリージョンを使用できます。

グリッド間レプリケーションを有効にする

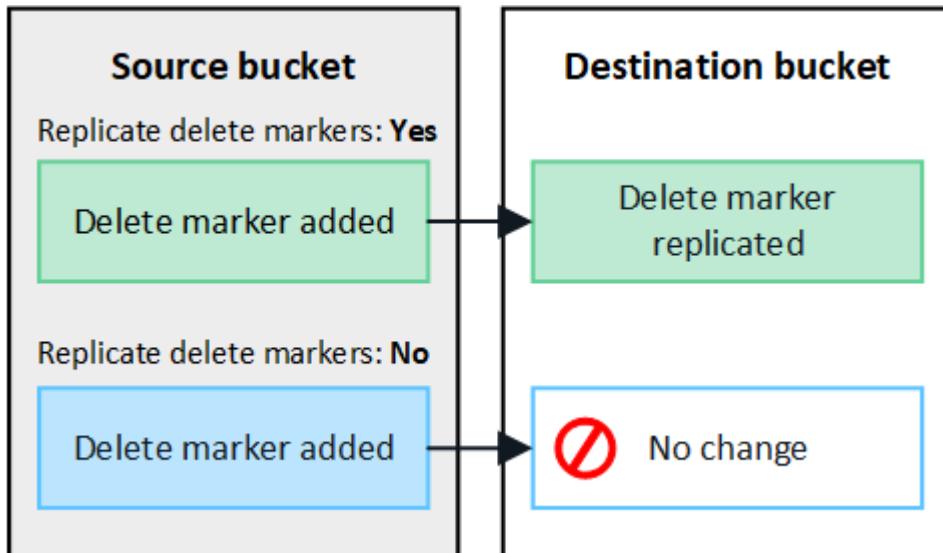
これらの手順は、いずれかのバケットにオブジェクトを追加する前に実行する必要があります。

手順

- オブジェクトを複製するグリッドから開始して、を有効にします "[一方向のグリッド間レプリケーション](#)"：
  - バケットのテナントアカウントにサインインします。
  - ダッシュボードで\* View Buckets を選択するか、storage (S3) > Buckets \*を選択します。
  - 表からバケット名を選択して、バケットの詳細ページにアクセスします。
  - [クロスグリッドレプリケーション]\*タブを選択します。
  - [有効化]\*を選択し、要件のリストを確認します。
  - すべての要件を満たしている場合は、使用するグリッドフェデレーション接続を選択します。
  - 必要に応じて、[Replicate delete markers]の設定を変更して、S3クライアントがバージョンIDを含ま

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

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



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

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

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

しばらくすると、成功のメッセージが表示されます。このバケットに追加されたオブジェクトは、もう一方のグリッドに自動的にレプリケートされます。\*クロスグリッドレプリケーション\*は、バケットの詳細ページで有効になっている機能として表示されます。

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

## グリッド間のレプリケーションをテスト

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

### 作業を開始する前に

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

### 手順

1. バケットのテナントアカウントにサインインします。
2. ダッシュボードで\* View Buckets を選択するか、 storage (S3) > Buckets \*を選択します。
3. 表からバケット名を選択して、バケットの詳細ページにアクセスします。
4. [クロスグリッドレプリケーション]\*タブを選択します。
5. [接続のテスト \*] を選択します。

接続が正常な場合は、成功バーが表示されます。そうしないとエラーメッセージが表示され、ユーザとグリッド管理者はこのメッセージを使用して問題を解決できます。詳細については、を参照してください "グリッドフェデレーションエラーをトラブルシューティングする"。

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

### グリッド間レプリケーションを無効にします

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

グリッド間レプリケーションを無効にする前に、次の点に注意してください。

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



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

## 作業を開始する前に

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

## 手順

1. レプリケートするオブジェクトが含まれていないグリッドから、バケットのグリッド間レプリケーションを停止します。
  - a. バケットのテナントアカウントにサインインします。
  - b. ダッシュボードで\* View Buckets を選択するか、storage (S3) > Buckets \*を選択します。
  - c. 表からバケット名を選択して、バケットの詳細ページにアクセスします。
  - d. [クロスグリッドレプリケーション]\*タブを選択します。
  - e. [レプリケーションを無効にする]\*を選択します。
  - f. このバケットでグリッド間レプリケーションを無効にする場合は、テキストボックスに「\* Yes 」と入力し、Disable \*を選択します。

しばらくすると、成功のメッセージが表示されます。このバケットに追加された新しいオブジェクトを他のグリッドに自動的にレプリケートすることはできなくなります。\*クロスグリッドレプリケーション\*は、[Buckets]ページに有効な機能として表示されなくなりました。

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

## グリッドフェデレーション接続を表示します

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

## 作業を開始する前に

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

## 手順

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

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

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

列 (Column)	説明
バケットにクロスグリッドレプリケーションが設定されている	グリッドフェデレーション接続ごとに、グリッド間レプリケーションが有効になっているテナントバケット。これらのバケットに追加されたオブジェクトは、接続内のもう一方のグリッドにレプリケートされます。
前回のエラー	グリッドフェデレーション接続ごとに、データがもう一方のグリッドにレプリケートされていたときに発生する最新のエラー（存在する場合）。を参照してください <a href="#">最後のエラーをクリアします</a> 。

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

最後のエラーをクリアします

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

- ソースオブジェクトのバージョンが見つかりませんでした。
- ソースバケットが見つかりませんでした。
- デスティネーションバケットが削除されました。
- デスティネーションバケットが別のアカウントで再作成されました。
- デスティネーションバケットのバージョン管理が中断されています。
- デスティネーションバケットが同じアカウントで再作成されましたが、現在バージョン管理されていません。



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

手順

### 1. 「\* Last error \*」列にメッセージが表示された場合は、メッセージのテキストを確認します。

たとえば、このエラーは、クロスグリッドレプリケーションのデスティネーションバケットが無効な状態であることを示しています。バージョン管理が中断されたか、S3オブジェクトロックが有効になっている可能性があります。

Grid federation connections

Clear error
Search...

Displaying one result

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

2. 推奨される対処方法を実行します。たとえば、グリッド間レプリケーションのためにデスティネーションバケットでバージョン管理が一時停止されていた場合は、そのバケットのバージョン管理を再度有効にします。
3. テーブルから接続を選択します。
4. [Clear error]\*を選択します。
5. メッセージをクリアしてシステムのステータスを更新するには、\*はい\*を選択します。
6. 5~6分待ってから、新しいオブジェクトをバケットに取り込みます。エラーメッセージが再表示されないことを確認します。



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

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

## グループとユーザを管理します

アイデンティティフェデレーションを使用する

アイデンティティフェデレーションを使用すると、テナントグループとテナントユーザを迅速に設定できます。またテナントユーザは、使い慣れたクレデンシャルを使用してテナントアカウントにサインインできます。

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

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

作業を開始する前に

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



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

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

このタスクについて

テナントにアイデンティティフェデレーションサービスを設定できるかどうかは、テナントアカウントの設定

方法によって異なります。テナントが Grid Manager 用に設定されたアイデンティティフェデレーションサービスを共有する場合があります。[Identity Federation]ページにアクセスしたときにこのメッセージが表示される場合は、このテナントに別のフェデレーテッドアイデンティティソースを設定することはできません。

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

## 構成を入力します

フェデレーションの識別を設定するときは、StorageGRID がLDAPサービスに接続するために必要な値を指定します。

### 手順

1. アクセス管理 \* > \* アイデンティティフェデレーション \* を選択します。
2. [\* アイデンティティフェデレーションを有効にする \*] を選択
3. LDAP サービスタイプセクションで、設定する LDAP サービスのタイプを選択します。

**LDAP service type**

Select the type of LDAP service you want to configure.

<b>Active Directory</b>	Azure	OpenLDAP	Other
-------------------------	-------	----------	-------

Oracle Directory Server を使用する LDAP サーバーの値を設定するには、\* その他 \* を選択します。

4. [\* その他 \*] を選択した場合は、[LDAP 属性] セクションのフィールドに入力します。それ以外の場合は、次の手順に進みます。
  - \* User Unique Name \* : LDAP ユーザの一意な 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 衔の 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 衔の 16 進数である必要があります。ハイフンは無視されます。
5. すべての LDAP サービスタイプについて、LDAP サーバの設定セクションに必要な LDAP サーバおよびネットワーク接続情報を入力します。

◦ \* Hostname \* : LDAP サーバの完全修飾ドメイン名（ FQDN ）または IP アドレス。

◦ \* Port \* : LDAP サーバへの接続に使用するポート。



STARTTLS のデフォルトポートは 389 、 LDAPS のデフォルトポートは 636 です。ただし、ファイアウォールが正しく設定されていれば、任意のポートを使用できます。

◦ \* Username \* : LDAP サーバに接続するユーザの識別名（ DN ）の完全パス。

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

指定するユーザには、グループおよびユーザを表示する権限、および次の属性にアクセスする権限が必要です。

- sAMAccountName または uid
- objectGUID 、 entryUUID 、または `nsuniqueid`
- cn
- memberOf または isMemberOf
- \* Active Directory \* : objectSid 、 primaryGroupID 、 userAccountControl および `userPrincipalName`
- \* Azure \* : accountEnabled および userPrincipalName

◦ \* Password \* : ユーザ名に関連付けられたパスワード。



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

◦ \* Group Base DN \* : グループを検索する LDAP サブツリーの識別名（ DN ）の完全パス。Active Directory では、ベース DN に対して相対的な識別名（ DC=storagegrid 、 DC=example 、 DC=com など）のグループをすべてフェデレーテッドグループとして使用できます。



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

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



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

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

StorageGRID がサービスアカウントにバインドできない場合にユーザがサインインできるようにするため、 \* バインドユーザ名形式 \* を指定することを推奨します。

次のいずれかのパターンを入力します。

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

記載されているとおりに \* [username] \* を含めます。

## 6. Transport Layer Security (TLS) セクションで、セキュリティ設定を選択します。

- \* STARTTLS を使用 \* : STARTTLS を使用して LDAP サーバとの通信を保護します。Active Directory 、 OpenLDAP 、またはその他のオプションですが、 Azure ではこのオプションはサポートされていません。
- \* LDAPS を使用 \* : LDAPS (LDAP over SSL) オプションでは、 TLS を使用して LDAP サーバへの接続を確立します。Azure ではこのオプションを選択する必要があります。
- \* TLS を使用しないでください \* : StorageGRID システムと LDAP サーバの間のネットワークトラフィックは保護されません。このオプションは Azure ではサポートされていません。



Active Directory サーバで LDAP 署名が適用される場合、 [TLS を使用しない] オプションの使用はサポートされていません。STARTTLS または LDAPS を使用する必要があります。

## 7. STARTTLS または LDAPS を選択した場合は、接続の保護に使用する証明書を選択します。

- \* オペレーティングシステムの CA 証明書を使用 \* : オペレーティングシステムにインストールされているデフォルトの Grid CA 証明書を使用して接続を保護します。
- \* カスタム CA 証明書を使用 \* : カスタムセキュリティ証明書を使用します。

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

接続をテストして設定を保存します

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

手順

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

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

**Test Connection**

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

Test username  
myusername  
The username of a federated user.

Test password  
.....  
Cancel Test Connection

- 接続設定が有効な場合は、「Test connection successful」というメッセージが表示されます。[ 保存 ( Save ) ] を選択して、構成を保存します。
- 接続設定、バインドユーザ名形式、またはテストユーザ名とパスワードが無効な場合は、エラーメッセージが表示されます。問題を解決してから、もう一度接続をテストしてください。

#### アイデンティティソースとの強制同期

StorageGRID システムは、アイデンティティソースからフェデレーテッドグループおよびユーザを定期的に同期します。ユーザの権限をすぐに有効にしたり制限したりする必要がある場合は、同期を強制的に開始できます。

#### 手順

- アイデンティティフェデレーションページに移動します。
- ページの上部にある「\* サーバーを同期」を選択します。

環境によっては、同期プロセスにしばらく時間がかかることがあります。



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

#### アイデンティティフェデレーションを無効にする

グループとユーザのアイデンティティフェデレーションを一時的または永続的に無効にすることができます。アイデンティティフェデレーションを無効にすると、StorageGRID とアイデンティティソース間のやり取りは発生しません。ただし、設定は保持されるため、簡単に再度有効にすることができます。

#### このタスクについて

アイデンティティフェデレーションを無効にする前に、次の点に注意してください。

- フェデレーテッドユーザはサインインできなくなります。
- 現在サインインしているフェデレーテッドユーザは、セッションが有効な間は StorageGRID システムに引き続きアクセスできますが、セッションが期限切れになると以降はサインインできなくなります。

- StorageGRID システムとアイデンティティソース間の同期は行われず、同期されていないアカウントに対してはアラートやアラームが生成されません。
- シングルサインオン (SSO) が\*有効\*または\*サンドボックスモード\*に設定されている場合、\*アイデンティフェデレーションを有効にする\*チェックボックスは無効になります。アイデンティティフェデレーションを無効にするには、シングルサインオンページの SSO ステータスが \* 無効 \* になっている必要があります。を参照してください "[シングルサインオンを無効にします](#)"。

## 手順

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

## OpenLDAP サーバの設定に関するガイドライン

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



ActiveDirectoryやAzure以外のアイデンティティソースの場合、StorageGRID は外部で無効にしたユーザへのS3アクセスを自動的にブロックしません。S3アクセスをブロックするには、そのユーザのS3キーをすべて削除するか、すべてのグループからユーザを削除します。

## memberof オーバーレイと refint オーバーレイ

memberof オーバーレイと refint オーバーレイを有効にする必要があります。詳細については、のリバースグループメンバーシップのメンテナンス手順を参照してください "[OpenLDAP のドキュメント：バージョン 2.4 管理者ガイド](#)"。

## インデックス作成

次の OpenLDAP 属性とインデックスキーワードを設定する必要があります。

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

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

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

## テナントグループを管理する

### S3 テナント用のグループを作成します

S3 ユーザグループの権限を管理するには、フェデレーテッドグループをインポートするか、ローカルグループを作成します。

## 作業を開始する前に

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

## グループ作成ウィザードにアクセスします

最初に、グループ作成ウィザードにアクセスします。

### 手順

1. \* access management \* > \* Groups \* を選択します。
2. テナントアカウントに「Use grid federation connection \*」権限がある場合は、このグリッドに作成された新しいグループが接続内の他のグリッドの同じテナントにクローニングされることを示す青いバナーが表示されることを確認します。このバナーが表示されない場合は、テナントのデスティネーショングリッドにサインインしている可能性があります。

3. 「\* グループを作成 \*」を選択します。

## グループタイプを選択します

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

### 手順

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

StorageGRID システムでシングルサインオン（SSO）が有効になっている場合、ローカルグループに属するユーザは Tenant Manager にサインインできません。ただし、クライアントアプリケーションを使用して、グループの権限に基づいてテナントのリソースを管理することはできます。

## 2. グループの名前を入力します。

- \* ローカルグループ\* : 表示名と一意の名前の両方を入力します。表示名はあとで編集できます。



テナントアカウントで\* Use grid federation connection 権限が設定されている場合、デステイネーショングリッドにテナントと同じ unique name \*がすでに存在すると、クローニングエラーが発生します。

- \* フェデレーショングループ\* : 一意の名前を入力します。Active Directoryの場合、に関連付けられている一意の名前です sAMAccountName 属性 (Attribute) : OpenLDAPの場合は、に関連付けられている一意の名前です uid 属性 (Attribute) :

## 3. 「\* Continue \*」を選択します。

グループの権限を管理します

グループ権限は、ユーザがTenant Managerおよびテナント管理APIで実行できるタスクを制御します。

手順

### 1. [アクセスモード]\*で、次のいずれかを選択します。

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



ユーザが複数のグループに属していて、いずれかのグループが読み取り専用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。

### 2. このグループの権限を1つ以上選択します。

を参照してください "[テナント管理権限](#)"。

### 3. 「\* Continue \*」を選択します。

S3グループポリシーを設定

グループポリシーによって、ユーザに付与するS3アクセス権限が決まります。

手順

### 1. このグループに使用するポリシーを選択します。

グループポリシー	説明
S3アクセスがありません	デフォルト。バケットポリシーでアクセスが許可されていない限り、このグループのユーザはS3リソースにアクセスできません。このオプションを選択すると、デフォルトでは root ユーザにのみ S3 リソースへのアクセスが許可されます。

グループポリシー	説明
読み取り専用アクセス	このグループのユーザには、S3リソースへの読み取り専用アクセスが許可されます。たとえば、オブジェクトをリストして、オブジェクトデータ、メタデータ、タグを読み取ることができます。このオプションを選択すると、テキストボックスに読み取り専用グループポリシーの JSON 文字列が表示されます。この文字列は編集できません。
フルアクセス	このグループのユーザには、バケットを含むS3リソースへのフルアクセスが許可されます。このオプションを選択すると、テキストボックスにフルアクセスグループポリシーの JSON 文字列が表示されます。この文字列は編集できません。
ランサムウェアの軽減	<p>この例では、このテナントのすべてのバケットを環境するポリシーを示します。このグループのユーザは共通の操作を実行できますが、オブジェクトのバージョン管理が有効になっているバケットからオブジェクトを完全に削除することはできません。</p> <p>このグループポリシーは、 * Manage all buckets *権限を持つTenant Managerユーザが上書きできます。[すべてのバケットを管理]権限を信頼できるユーザに制限し、可能な場合は多要素認証（MFA）を使用します。</p>
カスタム	グループ内のユーザには、テキストボックスで指定した権限が付与されます。

- 「\* Custom \*」を選択した場合は、グループポリシーを入力します。各グループポリシーのサイズは 5 、 120 バイトまでに制限されています。有効な JSON 形式の文字列を入力する必要があります。
- 言語の構文や例など、グループポリシーの詳細については、を参照してください "グループポリシーの例"。
- ローカルグループを作成する場合は、「\* Continue \*」を選択します。フェデレーテッドグループを作成する場合は、 \* Create group \* および \* Finish \* を選択します。

#### ユーザの追加（ローカルグループのみ）

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



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

#### 手順

- 必要に応じて、このグループに対して 1 人以上のローカルユーザを選択します。
- [ グループの作成 \*] と [ 完了 \*] を選択します。

作成したグループがグループのリストに表示されます。

テナントアカウントに \* Use grid federation connection 権限があり、テナントのソースグリッドにアクセスしている場合、新しいグループはテナントのデスティネーショングリッドにクローニングされます。Success は、グループの詳細ページのOverviewセクションに Cloning status \*として表示されます。

#### Swift テナント用のグループを作成します

Swift テナントアカウントに対するアクセス権限を管理するには、フェデレーテッドグループをインポートするか、ローカルグループを作成します。Swift テナントアカウントのコンテナとオブジェクトを管理するには、少なくとも 1 つのグループが Swift 管理者権限を持っている必要があります。



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

#### 作業を開始する前に

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

#### グループ作成ウィザードにアクセスします

##### 手順

最初に、グループ作成ウィザードにアクセスします。

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

#### グループタイプを選択します

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

##### 手順

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

StorageGRID システムでシングルサインオン（SSO）が有効になっている場合、ローカルグループに属するユーザは Tenant Manager にサインインできません。ただし、クライアントアプリケーションを使用して、グループの権限に基づいてテナントのリソースを管理することはできます。

2. グループの名前を入力します。

- \* ローカルグループ \* : 表示名と一意の名前の両方を入力します。表示名はあとで編集できます。
- \* フェデレーショングループ \* : 一意の名前を入力します。Active Directory の場合、に関連付けられている一意の名前です sAMAccountName 属性 (Attribute) : OpenLDAP の場合は、に関連付けられている一意の名前です uid 属性 (Attribute) :

3. 「\* Continue \*」を選択します。

#### グループの権限を管理します

グループ権限は、ユーザがTenant Managerおよびテナント管理APIで実行できるタスクを制御します。

#### 手順

1. [アクセスモード]\*で、次のいずれかを選択します。

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



ユーザが複数のグループに属していて、いずれかのグループが読み取り専用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。

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

3. 「\* Continue \*」を選択します。

#### Swiftグループポリシーを設定します

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

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

#### ユーザの追加（ローカルグループのみ）

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

#### 手順

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

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

2. [グループの作成 \*] と [完了 \*] を選択します。

作成したグループがグループのリストに表示されます。

#### テナント管理権限

テナントグループを作成する前に、そのグループに割り当てる権限を検討してください

い。テナント管理権限は、Tenant Manager またはテナント管理 API を使用してユーザー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ることができます。S3 テナントと Swift テナントではグループの権限が異なるので注意してください。

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

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

グループを管理します

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

作業を開始する前に

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

グループを表示または編集します

各グループの基本情報と詳細を表示および編集できます。

手順

- \* access management \* > \* Groups \* を選択します。
- [Groups]ページに表示される情報を確認します。このテナントアカウントのすべてのローカルグループとフェデレーテッドグループの基本情報が表示されます。

テナントアカウントに\* Use grid federation connection \*権限があり、テナントのソースグリッド上のグループを表示している場合：

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

The screenshot shows a user management interface titled 'Manage users'. It includes buttons for 'Add users' (blue) and 'Remove Users' (red). A search bar with placeholder text 'Search Groups...' and a magnifying glass icon is present. The results table has columns: 'Username' (sorted by 'User\_02'), 'Full Name' (sorted by 'User\_02\_Managers'), and 'Denied' (sorted by 'Denied'). A message at the top states 'You can add users to this group or remove users from this group.' Below the table, it says 'Displaying 1 results'.

- b. [ユーザの追加]\*を選択します。
- c. 追加する既存のユーザーを選択し、\*ユーザーの追加\*を選択します。

右上に成功メッセージが表示されます。

#### 8. グループからローカルユーザを削除するには、次の手順を実行します

- a. [Users]タブを選択します。
- b. [ユーザの削除]\*を選択します。
- c. 削除するユーザを選択し、\*[ユーザの削除]\*を選択します。

右上に成功メッセージが表示されます。

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

グループが重複しています

既存のグループを複製して、新しいグループをより迅速に作成できます。



テナントアカウントに\* Use grid federation connection \*権限があり、テナントのソースグリッドからグループを複製すると、複製されたグループがテナントのデスティネーショングリッドにクローニングされます。

手順

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

グループクローンの再試行

失敗したクローンを再試行するには：

1. グループ名の下に\_ (Cloning failed) \_と表示されている各グループを選択します。
2. >[クローニンググループ]\*を選択します。
3. クローニングする各グループの詳細ページで、クローニング処理のステータスを確認します。

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

#### 1つ以上のグループを削除します

1つ以上のグループを削除できます。削除したグループにのみ属しているユーザは、Tenant Managerにサインインしたりテナントアカウントを使用したりできなくなります。



テナントアカウントに\* Use grid federation connection \*権限が割り当てられている場合にグループを削除すると、StorageGRID はもう一方のグリッド上の対応するグループを削除しません。この情報を同期する必要がある場合は、両方のグリッドから同じグループを削除する必要があります。

#### 手順

1. \* access management \* > \* Groups \* を選択します。
2. 削除する各グループのチェックボックスをオンにします。
3. >[グループの削除]または[アクション]>[グループの削除]\*を選択します。

確認のダイアログボックスが表示されます。

4. または[グループの削除]\*を選択します。

#### ローカルユーザを管理します

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



StorageGRID システムでシングルサインオン (SSO) が有効になっている場合、ローカルユーザはクライアントアプリケーションを使用してグループ権限に基づいてテナントのリソースにアクセスできますが、Tenant Managerまたはテナント管理APIにサインインすることはできません。

#### 作業を開始する前に

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

## ローカルユーザを作成します

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

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

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

### Create user ウィザードにアクセスします

手順

1. アクセス管理 \* > \* Users \* を選択します。

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

The screenshot shows the 'Users' page in the AWS Management Console. At the top, it says 'View local and federated users. Edit properties and group membership of local users.' Below this, it shows '1 user'. On the right, there is a blue 'Create user' button. Underneath the user count, there is a 'Actions' dropdown menu. A tooltip message provides information about the 'Use grid federation connection' permission: 'This tenant has Use grid federation connection permission for connection Grid 1 to Grid 2. New local tenant users will be automatically cloned to the same tenant on the other grid in the connection. If you edit or remove a group, your changes will not be synced to the other grid.'

2. 「\* ユーザーの作成 \*」を選択します。

### 資格情報を入力します

手順

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

フィールド	説明
フルネーム	このユーザーのフルネーム（ユーザーの名と姓、アプリケーションの名前など）。

フィールド	説明
ユーザ名	<p>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。</p> <p>注：テナントアカウントに* Use grid federation connection 権限が設定されている場合、デスティネーショングリッドにテナントに同じ Username *がすでに存在すると、クローニングエラーが発生します。</p>
	ユーザがサインイン時に最初に使用するパスワード。
アクセスを拒否します	<p>このユーザが1つ以上のグループに属している場合でもテナントアカウントにサインインできないようにするには、*[はい]*を選択します。</p> <p>たとえば、*[はい]*を選択すると、ユーザーのサインイン機能が一時的に中断されます。</p>

## 2. 「\* Continue \*」を選択します。

グループに割り当てます

手順

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

グループへのユーザの割り当ては任意です。必要に応じて、グループを作成または編集するときにユーザーを選択できます。

どのグループにも属していないユーザには、管理権限はありません。アクセス許可は累積的に追加されユーザには、自身が属しているすべてのグループに対するすべての権限が与えられます。を参照してください "[テナント管理権限](#)"。

### 2. 「\* ユーザーの作成 \*」を選択します。

テナントアカウントに\* Use grid federation connection 権限があり、テナントのソースグリッドにアクセスしている場合は、新しいローカルユーザがテナントのデスティネーショングリッドにクローニングされます。Success は、ユーザーの詳細ページのOverviewセクションに Cloning status \*として表示されます。

### 3. [完了]\*を選択して[ユーザー]ページに戻ります。

ローカルユーザを表示または編集します

手順

### 1. アクセス管理 \* > \* Users \* を選択します。

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

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

- バナーメッセージは、ユーザを編集または削除すると、変更内容が他のグリッドに同期されないことを示します。
  - 必要に応じて、ユーザがデスティネーショングリッドのテナントにクローニングされていないかどうかを示すバナーメッセージが表示されます。可能です [失敗したユーザクローンを再試行します。](#)
3. ユーザのフルネームを変更する場合は、次の手順を実行します。
    - a. ユーザのチェックボックスを選択します。
    - b. >[フルネームの編集]\*を選択します。
    - c. 新しい名前を入力します。
    - d. [変更を保存]\*を選択します
  4. 詳細を表示したり、追加の編集を行う場合は、次のいずれかを実行します。
    - ユーザ名を選択します。
    - ユーザのチェックボックスを選択し、[\[操作\]>\\*\[ユーザの詳細を表示\]\\*](#)を選択します。
  5. [Overview]セクションには、ユーザごとに次の情報が表示されます。
    - フルネーム
    - ユーザ名
    - ユーザタイプ
    - アクセスを拒否しました
    - アクセスマード
    - グループメンバーシップ
    - テナントアカウントに\* Use grid federation connection \*権限があり、テナントのソースグリッドでユーザを表示している場合は、次のフィールドが追加されます。
      - クローニングステータス (\* Success または Failure \*)
      - このユーザを編集すると、変更内容が他のグリッドに同期されないことを示す青いバナーが表示されます。
  6. 必要に応じてユーザー設定を編集します。を参照してください [ローカルユーザを作成します](#) を参照してください。
    - a. [Overview]セクションで、名前または編集アイコンを選択してフルネームを変更します 。

ユーザー名は変更できません。
    - b. タブで、ユーザのパスワードを変更し、[変更を保存]\*を選択します。
    - c. [アクセス]タブで、[いいえ]を選択してユーザーがサインインできるようにするか、[はい]を選択してユーザーがサインインできないようにします。次に、\*変更を保存\*を選択します。
    - d. [アクセスキー]タブで、\*[キーの作成]\*を選択し、の手順に従います ["別のユーザのS3アクセスキーを作成しています"](#)。
    - e. タブで[グループの編集]\*を選択して、ユーザーをグループに追加するか、ユーザーをグループから削除します。次に、\*変更を保存\*を選択します。
  7. 変更した各セクションで[変更を保存]\*が選択されていることを確認します。

ローカルユーザが重複しています

ローカルユーザを複製して新しいユーザを迅速に作成することができます。



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

## 手順

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

ユーザクローンの再試行

失敗したクローンを再試行するには：

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

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

1人以上のローカルユーザを削除します

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



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



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

## 手順

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

確認のダイアログボックスが表示されます。

4. または[ユーザの削除]\*を選択します。

## S3 アクセスキーを管理します

### S3アクセスキーの管理：概要

S3 テナントアカウントの各ユーザには、StorageGRID システムでオブジェクトの格納と読み出しを行うためのアクセスキーが必要です。アクセスキーは、アクセスキー ID とシークレットアクセスキーで構成されます。

S3 アクセスキーは次のように管理できます。

- Manage your own S3 credentials \*権限を持つユーザは、自分のS3アクセスキーを作成または削除できます。
- Root access \*権限を持つユーザは、S3 rootアカウントとその他すべてのユーザのアクセスキーを管理できます。root アクセスキーは、バケットポリシーで root アクセスキーが明示的に無効になっていないかぎり、テナントのすべてのバケットとオブジェクトへのフルアクセスを提供します。

StorageGRID では、署名バージョン 2 と署名バージョン 4 の認証がサポートされています。クロスアカウントアクセスは、バケットポリシーで明示的に有効になっていないかぎり、許可されません。

### 独自の S3 アクセスキーを作成します

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

作業を開始する前に

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

このタスクについて

テナントアカウントのバケットを作成および管理できる S3 アクセスキーを 1 つ以上作成できます。新しいアクセスキーを作成したら、新しいアクセスキー ID とシークレットアクセスキーでアプリケーションを更新します。セキュリティのため、必要以上のキーを作成しないで、使用していないキーを削除してください。キーが 1 つしかなく、有効期限が近づいている場合は、古いキーが期限切れになる前に新しいキーを作成してから、古いキーを削除します。

各キーには、特定の有効期限または有効期限を設定できません。有効期限については、次のガイドラインに従ってください。

- キーの有効期限を設定して、アクセスを特定の期間に制限します。短い有効期限を設定すると、アクセスキー ID とシークレットアクセスキーが誤って公開されるリスクを低減できます。期限切れのキーは自動的に削除されます。
- 環境のセキュリティリスクが低く、新しいキーを定期的に作成する必要がない場合は、キーの有効期限を設定する必要はありません。あとで新しいキーを作成する場合は、古いキーを手動で削除します。



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

## 手順

- 「\* 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。

- 「\* キーの作成 \*」を選択します。

- 次のいずれかを実行します。

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



有効期限は、現在の日付から最大5年間です。有効期限は、現在の時刻から少なくとも1分後に設定できます。

- [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。

- アクセスキー ID とシークレットアクセスキーを安全な場所にコピーするか、「\* Download.csv \*」を選択してアクセスキー ID とシークレットアクセスキーを含むスプレッドシートファイルを保存します。



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

- [完了] を選択します。

新しいキーは [マイアクセスキー] ページに表示されます。

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

## S3 アクセスキーを表示します

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



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

作業を開始する前に

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

手順

1. 「\* storage (S3) \* > \* My access keys \*」を選択します。
2. [アクセスキー]ページで、既存のアクセスキーを\*または[アクセスキーID]\*でソートします。
3. 必要に応じて、新しいキーを作成するか、使用しなくなったキーを削除します。

既存のキーの有効期限が切れる前に新しいキーを作成した場合は、アカウントのオブジェクトに一時的にアクセスできなくなることなく、新しいキーの使用を開始できます。

期限切れのキーは自動的に削除されます。

自分の S3 アクセスキーを削除します

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

作業を開始する前に

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



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

手順

1. 「\* storage (S3) \* > \* My access keys \*」を選択します。
2. [My access keys]ページで、削除する各アクセスキーのチェックボックスをオンにします。
3. 「\* Delete key (キーの削除)」\*を選択
4. 確認ダイアログボックスで、\* Delete key \*を選択します。

ページの右上に確認メッセージが表示されます。

## 別のユーザの S3 アクセスキーを作成します

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

作業を開始する前に

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

このタスクについて

他のユーザがテナントアカウントのバケットを作成および管理できるように、1つ以上の S3 アクセスキーを作成できます。新しいアクセスキーを作成したら、新しいアクセスキー ID とシークレットアクセスキーでアプリケーションを更新します。セキュリティを確保するため、ユーザが必要とする数以上のキーを作成しないでください。また、使用されていないキーは削除してください。キーが1つしかなく、有効期限が近づいている場合は、古いキーが期限切れになる前に新しいキーを作成してから、古いキーを削除します。

各キーには、特定の有効期限または有効期限を設定できません。有効期限については、次のガイドラインに従ってください。

- キーの有効期限を設定して、ユーザのアクセスを一定期間に制限します。短い有効期限を設定すると、アクセスキー ID とシークレットアクセスキーが誤って公開されるリスクを低減できます。期限切れのキーは自動的に削除されます。
- 環境のセキュリティリスクが低く、新しいキーを定期的に作成する必要がない場合は、キーの有効期限を設定する必要はありません。あとで新しいキーを作成する場合は、古いキーを手動で削除します。

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

手順

1. アクセス管理 \* > \* Users \* を選択します。
  2. S3 アクセスキーを管理するユーザを選択します。
- ユーザーの詳細ページが表示されます。
3. [\* アクセスキー \*] を選択し、[\* キーの作成 \*] を選択します。
  4. 次のいずれかを実行します。
    - 有効期限のないキーを作成するには、[有効期限を設定しない]\*を選択します。 (デフォルト)
    - [有効期限の設定 \*] を選択し、有効期限の日付と時刻を設定します。



有効期限は、現在の日付から最大5年間です。有効期限は、現在の時刻から少なくとも1分後に設定できます。

5. [アクセスキーの作成 \*] を選択します。

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

6. アクセスキー ID とシークレットアクセスキーを安全な場所にコピーするか、「\* Download.csv \*」を選択してアクセスキー ID とシークレットアクセスキーを含むスプレッドシートファイルを保存します。



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

7. [完了] を選択します。

新しいキーは、ユーザ詳細ページのアクセスキータブに表示されます。

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

別のユーザの S3 アクセスキーを表示します

S3 テナントを使用している場合は、適切な権限があれば、別のユーザの S3 アクセスキーを表示できます。有効期限でリストをソートすると、まもなく期限切れになるキーを確認できます。必要に応じて、新しいキーを作成したり、使用されなくなったキーを削除したりできます。

作業を開始する前に

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



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

手順

1. アクセス管理 \* > \* Users \* を選択します。
2. [Users] ページで、表示するS3アクセスキーを所有するユーザを選択します。
3. [ユーザの詳細] ページで、\*[アクセスキー]\*を選択します。
4. キーを \* Expiration time \* または \* Access key ID \* でソートします。
5. 必要に応じて、新しいキーを作成し、使用しなくなったキーを手動で削除します。

既存のキーの有効期限が切れる前に新しいキーを作成した場合、ユーザはアカウントのオブジェクトに一時的にアクセスできなくなることなく、新しいキーの使用を開始できます。

期限切れのキーは自動的に削除されます。

## 関連情報

"別のユーザの S3 アクセスキーを作成します"

"別のユーザの S3 アクセスキーを削除します"

別のユーザの **S3** アクセスキーを削除します

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

作業を開始する前に

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

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

手順

1. アクセス管理 \* > \* Users \* を選択します。
2. [Users]ページで、管理するS3アクセスキーを所有するユーザを選択します。
3. [User details]ページで、\*[Access Keys]\*を選択し、各アクセスキーのチェックボックスを選択します。を削除します。
4. \* アクション \* > \* 選択したキーを削除 \* を選択します。
5. 確認ダイアログボックスで、\* Delete key \*を選択します。

ページの右上に確認メッセージが表示されます。

## S3 バケットを管理する

S3 バケットを作成します。

Tenant Manager を使用して、オブジェクトデータ用の S3 バケットを作成できます。

作業を開始する前に

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



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

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

ウィザードにアクセスします

手順

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

詳細を入力します

手順

- バケットの詳細を入力します。

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

- 「 \* Continue \* 」を選択します。

## オブジェクトの設定を管理します

### 手順

- 必要に応じて、バケットのオブジェクトのバージョン管理を有効にします。

このバケット内の各オブジェクトのすべてのバージョンを格納する場合は、オブジェクトのバージョン管理を有効にします。そのあと、必要に応じて以前のバージョンのオブジェクトを読み出すことができます。バケットをグリッド間レプリケーションに使用する場合は、オブジェクトのバージョン管理を有効にする必要があります。

- S3オブジェクトロックのグローバル設定が有効になっている場合は、必要に応じて、バケットのS3オブジェクトロックを有効にして、Write-Once-Read-Many (WORM) モデルを使用してオブジェクトを格納します。

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



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

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

- [S3オブジェクトロックを有効にする]\*を選択した場合は、必要に応じてこのバケットに対して\*デフォルトの保持\*を有効にします。

default retention \*を有効にすると、バケットに追加された新しいオブジェクトが自動的に削除または上書きされなくなります。デフォルトの保持\*設定は、独自の保持期間を持つオブジェクトには適用されません。

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

デフォルトの保持モード	説明
コンプライアンス	<ul style="list-style-type: none"><li>retain-until-dateに達するまで、オブジェクトを削除できません。</li><li>オブジェクトのretain-until-dateは増やすことはできますが、減らすことはできません。</li><li>オブジェクトのretain-until-dateは、その日付に達するまで削除できません。</li></ul>

デフォルトの保持モード	説明
ガバナンス	<ul style="list-style-type: none"> <li>• 使用するユーザ s3:BypassGovernanceRetention 権限はを使用できます x-amz-bypass-governance-retention: true 保持設定をバイパスする要求ヘッダー。</li> <li>• これらのユーザは、retain-until-dateに達する前にオブジェクトバージョンを削除できます。</li> <li>• これらのユーザは、オブジェクトのretain-until-dateを増減、または削除できます。</li> </ul>

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

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

4. [\* バケットの作成 \*] を選択します。

バケットが作成され、バケットページのテーブルに追加されます。

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

バケットの詳細を表示します

テナントアカウント内のバケットを表示できます。

作業を開始する前に

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

手順

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

[Buckets]ページが表示されます。

2. 各バケットの概要情報を確認します。

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



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

列 (Column)	説明
名前	バケットの一意の名前。変更することはできません。
有効な機能	バケットで有効になっている機能のリスト。
S3 オブジェクトのロック	バケットでS3オブジェクトロックが有効になっているかどうか。 この列は、グリッドでS3オブジェクトロックが有効になっている場合にのみ表示されます。この列には、古い準拠バケットの情報も表示されます。
地域	バケットのリージョン。変更できません。
オブジェクト数	このバケット内のオブジェクトの数。オブジェクトが追加または削除されたとき、この値がすぐに更新されないことがあります。バケットでバージョン管理が有効になっている場合は、最新でないオブジェクトバージョンがこの値に含まれます。
使用済みスペース	バケット内のすべてのオブジェクトの論理サイズ。論理サイズには、レプリケートコピーやイレイジヤーコーディングコピー、またはオブジェクトメタデータに必要な実際のスペースは含まれていません。
作成日	バケットが作成された日時。

3. 特定のバケットの詳細を表示するには、テーブルでバケット名を選択します。

バケットの詳細ページが表示されます。必要な権限があれば、このページで次のタスクを実行できます。

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

## ILMポリシータグをバケットに適用する

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

ILMポリシーは、オブジェクトデータの格納場所と一定期間後に削除するかどうかを制御します。グリッド管理者は、複数のアクティブポリシーを使用している場合に、ILMポリシーを作成してILMポリシータグに割り当てます。



バケットのポリシータグは頻繁に再割り当てしないでください。そうしないと、パフォーマンスの問題が発生する可能性があります

作業を開始する前に

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

手順

- ダッシュボードで\* View Buckets を選択するか、storage (S3) > Buckets \*を選択します。  
[Buckets]ページが表示されます。必要に応じて、任意の列で情報をソートしたり、リストを前後にページ移動したりできます。
- ILMポリシータグを割り当てるバケットの名前を選択します。

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



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

- [Bucket options]タブで、ILMポリシータグのアコーディオンを展開します。このアコーディオンは、グリッド管理者がカスタムポリシータグの使用を有効にしている場合にのみ表示されます。
- 各ポリシータグの概要を読んで、バケットに適用するタグを特定します。



バケットのILMポリシータグを変更すると、バケット内のすべてのオブジェクトのILMによる再評価がトリガーされます。新しいポリシーで一定期間オブジェクトが保持されると、古いオブジェクトは削除されます。

- バケットに割り当てるタグのラジオボタンを選択します。
- 「変更を保存」を選択します。バケットにキーを使用して新しいS3バケットタグが設定される NTAP-SG-ILM-BUCKET-TAG およびILMポリシータグ名の値。



S3アプリケーションが誤って新しいバケットタグを上書きまたは削除しないようにしてください。バケットに新しいTagSetを適用するときにこのタグを省略すると、バケット内のオブジェクトはデフォルトのILMポリシーに照らして評価されます。



ILMポリシータグの設定と変更には、ILMポリシータグが検証されるTenant Manager APIまたはTenant Manager APIのみを使用します。変更しないでください NTAP-SG-ILM-BUCKET-TAG S3 PutBucketTagging APIまたはS3 DeleteBucketTagging APIを使用したILMポリシータグ。



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

## バケットの整合性の管理

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

### 作業を開始する前に

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

### バケットの整合性に関するガイドライン

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

### バケット整合性の変更

Read-after-new-write \*整合性がクライアントアプリケーションの要件を満たしていない場合は、バケットの整合性を設定するか、Consistency-Control ヘッダー。。 Consistency-Control ヘッダーはバケットの整合性よりも優先されます。



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

### 手順

1. ダッシュボードで\* View Buckets を選択するか、storage (S3) > Buckets \*を選択します。
2. 表からバケット名を選択します。

バケットの詳細ページが表示されます。

3. [Bucket options]タブで、[\*\*]アクションを選択します。
4. このバケット内のオブジェクトに対して実行される処理の整合性を選択します。

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

## 5. 「変更を保存」を選択します。

バケット設定を変更した場合の動作

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

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

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



バケットのバージョン管理、S3オブジェクトロック、およびバケット暗号化の整合性の値を強くない値に設定することはできません。

次のバケット設定では整合性が強くなり、変更の可用性も高くなります。これらの設定の変更が反映されるまでに時間がかかることがあります。

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



バケット設定の変更時に使用したデフォルトの整合性がクライアントアプリケーションの要件を満たしていない場合は、Consistency-Control のヘッダー "S3 REST API" または、reducedConsistency または force のオプションを指定します "テナント管理 API"。

最終アクセス日時の更新を有効または無効にします

グリッド管理者が StorageGRID システムの情報ライフサイクル管理 ( ILM ) ルールを作成する際に、オブジェクトを別の格納場所に移動するかどうかを決定する際にオブジェクトの最終アクセス日時を使用するように指定できます。S3 テナントを使用している場合は、S3 バケット内のオブジェクトに対して最終アクセス日時の更新を有効にすることで、このようなルールを活用できます。

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

作業を開始する前に

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

このタスクについて

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

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

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

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



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

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

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

次の表に、最終アクセス時間が有効または無効な場合のバケット内のすべてのオブジェクトに適用される動作をまとめます。

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

## 手順

1. ダッシュボードで\* View Buckets を選択するか、storage (S3) > Buckets \*を選択します。
  2. 表からバケット名を選択します。
- バケットの詳細ページが表示されます。
3. [Bucket options]タブで、[Last access time updates]\*アコーディオンを選択します。
  4. 最終アクセス時間の更新を有効または無効にします。
  5. 「変更を保存」を選択します。

バケットのオブジェクトのバージョン管理を変更する

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

作業を開始する前に

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

理します”。これらの権限は、グループまたはバケットポリシーの権限の設定よりも優先されます。

- すべてのストレージノードが使用可能です。

#### このタスクについて

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

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

詳細については、次を参照してください。

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

#### 手順

- ダッシュボードで\* View Buckets を選択するか、storage (S3) > Buckets \*を選択します。
  - 表からバケット名を選択します。
- バケットの詳細ページが表示されます。
- タブで、[Object versioning]\*アコーディオンを選択します。
  - このバケット内のオブジェクトのバージョン管理の状態を選択します。

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

オプション	説明
バージョン管理を有効にする	<p>このバケット内の各オブジェクトのすべてのバージョンを格納する場合は、オブジェクトのバージョン管理を有効にします。そのあと、必要に応じて以前のバージョンのオブジェクトを読み出すことができます。</p> <p>バケットにすでに含まれていたオブジェクトは、ユーザによる変更時にバージョン管理されます。</p>
バージョン管理を一時停止	新しいオブジェクトバージョンを作成しない場合は、オブジェクトのバージョン管理を一時停止します。既存のオブジェクトバージョンは引き続き取得できます。

- 「変更を保存」を選択します。

**S3オブジェクトロック**を使用してオブジェクトを保持します

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

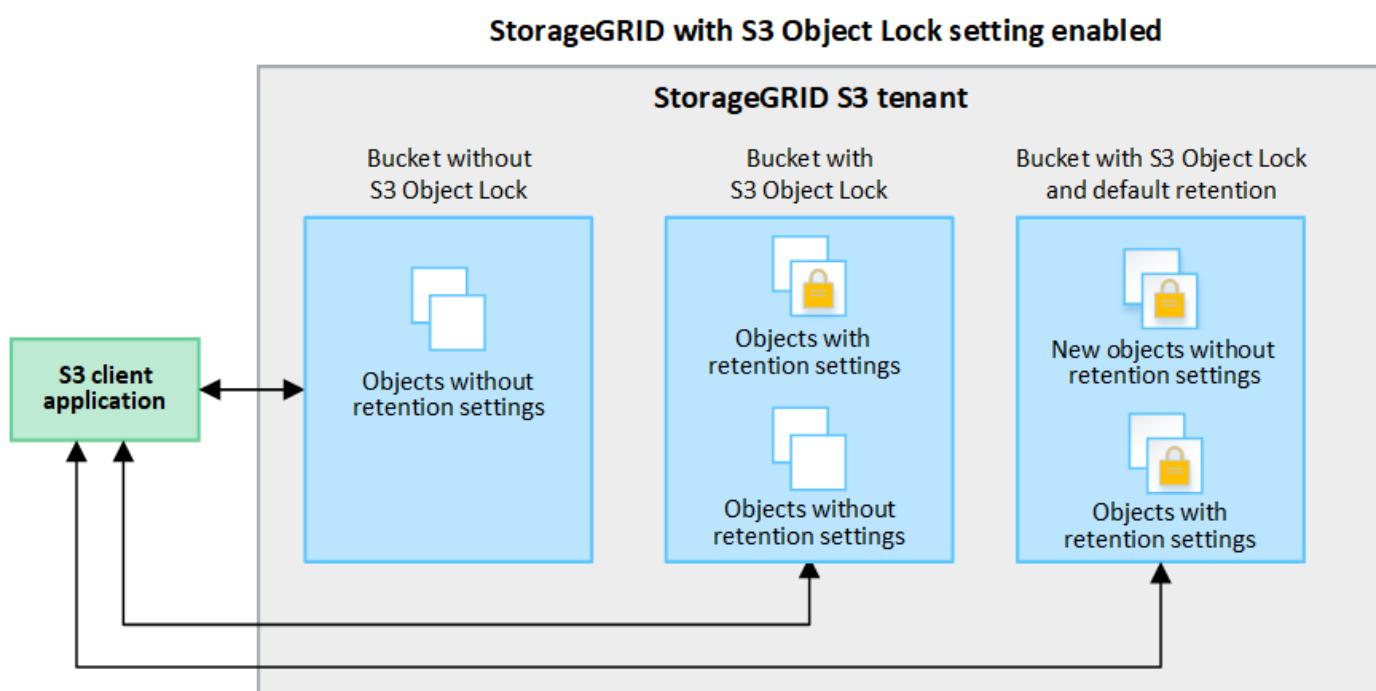
**S3 オブジェクトのロック**とは何ですか？

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

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

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

また、S3 オブジェクトロックが有効になっているバケットでは、オプションでデフォルトの保持モードと保持期間を設定できます。デフォルトの設定は、独自の保持設定がない状態でバケットに追加されたオブジェクトにのみ適用されます。



保持モード

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

- コンプライアンスモードの場合：

- retain-until-date に達するまで、オブジェクトを削除できません。
- オブジェクトの retain-until-date は増やすことはできますが、減らすことはできません。

- オブジェクトのretain-until-dateは、その日付に達するまで削除できません。
- ガバナンスモードの場合：
  - 特別な権限を持つユーザは、要求でバイパスヘッダーを使用して、特定の保持設定を変更できます。
  - これらのユーザは、retain-until-dateに達する前にオブジェクトバージョンを削除できます。
  - これらのユーザは、オブジェクトのretain-until-dateを増減、または削除できます。

## オブジェクトバージョンの保持設定

S3オブジェクトロックを有効にしてバケットを作成した場合、ユーザはS3クライアントアプリケーションを使用して、バケットに追加される各オブジェクトに次の保持設定を必要に応じて指定できます。

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



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

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

## バケットのデフォルトの保持設定

S3オブジェクトロックを有効にしてバケットを作成した場合は、必要に応じて次のバケットのデフォルト設定を指定できます。

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

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

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

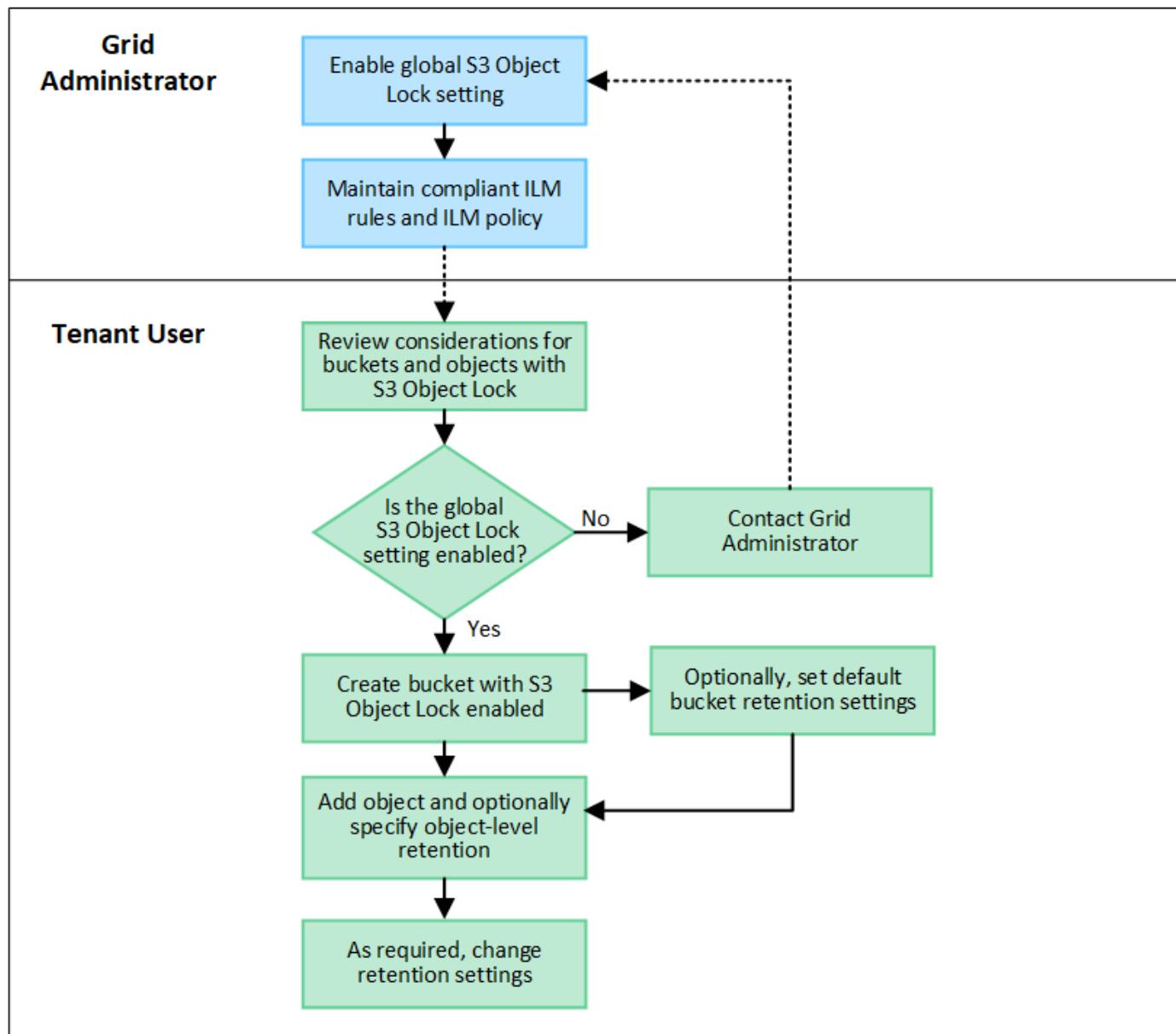
## S3 オブジェクトロックのワークフロー

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

S3 オブジェクトのロックを有効にしてバケットを作成する前に、グリッド管理者が StorageGRID システム全体に対してグローバルな S3 オブジェクトのロック設定を有効にする必要があります。グリッド管理者は、情報ライフサイクル管理 (ILM) ポリシーが「準拠」であることを確認し、S3オブジェクトロックが有効なバケ

ットの要件を満たしている必要があります。詳細については、グリッド管理者に問い合わせるか、の手順を参照してください "S3オブジェクトロックを使用してオブジェクトを管理します"。

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



#### S3 オブジェクトのロックを有効にした場合のバケットの要件

- StorageGRID システムでグローバルな S3 オブジェクトロック設定が有効になっている場合は、テナントマネージャ、テナント管理 API、または S3 REST API を使用して、S3 オブジェクトロックを有効にしたバケットを作成できます。
- S3 オブジェクトのロックを使用する場合は、バケットの作成時に S3 オブジェクトのロックを有効にする必要があります。既存のバケットで S3 オブジェクトロックを有効にすることはできません。
- バケットで S3 オブジェクトのロックが有効になっている場合は、そのバケットのバージョン管理が StorageGRID で自動的に有効になります。バケットの S3 オブジェクトロックを無効にしたり、バージョン管理を一時停止したりすることはできません。

- 必要に応じて、Tenant Manager、テナント管理API、またはS3 REST APIを使用して、各バケットのデフォルトの保持モードと保持期間を指定できます。バケットのデフォルトの保持設定は、バケットに追加された新しいオブジェクトのうち、独自の保持設定がないオブジェクトにのみ適用されます。これらのデフォルト設定は、アップロード時にオブジェクトバージョンごとに保持モードとretain-until-dateを指定することで上書きできます。
- バケットライフサイクル設定は、S3オブジェクトロックが有効なバケットでサポートされます。
- CloudMirror レプリケーションは、S3 オブジェクトロックが有効になっているバケットではサポートされません。

### S3 オブジェクトのロックが有効になっているバケット内のオブジェクトの要件

- オブジェクトバージョンを保護するには、バケットのデフォルトの保持設定を指定するか、オブジェクトバージョンごとに保持設定を指定します。オブジェクトレベルの保持設定は、S3クライアントアプリケーションまたはS3 REST APIを使用して指定できます。
- 保持設定はオブジェクトのバージョンごとに適用されます。オブジェクトバージョンには、retain-until-date 設定とリーガルホールド設定の両方を設定できます。ただし、オブジェクトバージョンを保持することはできません。また、どちらも保持することはできません。オブジェクトの retain-until-date 設定またはリーガルホールド設定を指定すると、要求で指定されたバージョンのみが保護されます。オブジェクトの以前のバージョンはロックされたまま、オブジェクトの新しいバージョンを作成できます。

### S3 オブジェクトのロックが有効なバケット内のオブジェクトのライフサイクル

S3オブジェクトロックが有効なバケットに保存された各オブジェクトは、次の段階を経ます。

#### 1. \* オブジェクトの取り込み \*

S3オブジェクトロックが有効になっているバケットにオブジェクトバージョンを追加すると、保持設定は次のように適用されます。

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

保持設定が適用されている場合は、オブジェクトとS3ユーザ定義メタデータの両方が保護されます。

#### 2. オブジェクトの保持と削除

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

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

従来の準拠バケットは引き続き管理できますか。

S3 オブジェクトロック機能は、以前のバージョンの StorageGRID で使用されていた準拠機能に代わる機能で

す。以前のバージョンの StorageGRID を使用して準拠バケットを作成した場合は、引き続きこれらのバケットの設定を管理できますが、新しい準拠バケットは作成できなくなります。手順については、[を参照してください](#)

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

## S3オブジェクトロックのデフォルトの保持期間を更新します

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

作業を開始する前に

- Tenant Manager にはを使用してサインインします "[サポートされている Web ブラウザ](#)"。
- が設定されたユーザグループに属している必要があります "[すべてのバケットまたはRoot Access権限を管理します](#)"。これらの権限は、グループまたはバケットポリシーの権限の設定よりも優先されます。
- S3オブジェクトロックはStorageGRID システムに対してグローバルに有効になり、バケットの作成時に有効にしました。を参照してください "[S3オブジェクトロックを使用してオブジェクトを保持します](#)"。

手順

1. ダッシュボードで\* View Buckets を選択するか、 storage (S3) > Buckets \*を選択します。
2. 表からバケット名を選択します。

バケットの詳細ページが表示されます。

3. [Bucket options]タブで、[S3 Object Lock]\*アコーディオンを選択します。
4. 必要に応じて、このバケットの\*デフォルトの保持\*を有効または無効にします。

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

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

デフォルトの保持モード	説明
コンプライアンス	<ul style="list-style-type: none"><li>• retain-until-dateに達するまで、オブジェクトを削除できません。</li><li>• オブジェクトのretain-until-dateは増やすことはできますが、減らすことはできません。</li><li>• オブジェクトのretain-until-dateは、その日付に達するまで削除できません。</li></ul>

デフォルトの保持モード	説明
ガバナンス	<ul style="list-style-type: none"> <li>• 使用するユーザ s3:BypassGovernanceRetention 権限は使用できます x-amz-bypass-governance-retention: true 保持設定をバイパスする要求ヘッダー。</li> <li>• これらのユーザは、retain-until-dateに達する前にオブジェクトバージョンを削除できます。</li> <li>• これらのユーザは、オブジェクトのretain-until-dateを増減、または削除できます。</li> </ul>

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

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

7. 「変更を保存」を選択します。

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

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

作業を開始する前に

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

このタスクについて

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

バケットのCORSを有効にします

手順

1. テキストエディタを使用して、必要なXMLを作成します。

次の例は、S3 バケットの CORS を有効にするために使用される XML を示しています。このXMLでは、すべてのドメインにバケットへのGET要求の送信が許可されていますが、にしか許可されません <http://www.example.com> POST要求と削除要求を送信するドメイン。要求ヘッダーはすべて許可されます。

```

<corsConfiguration
    xmlns="http://s3.amazonaws.com/doc/2020-10-22/">
    <corsRule>
        <allowedOrigin>*</allowedOrigin>
        <allowedMethod>GET</allowedMethod>
        <allowedHeader>*</allowedHeader>
    </corsRule>
    <corsRule>
        <allowedOrigin>http://www.example.com</allowedOrigin>
        <allowedMethod>GET</allowedMethod>
        <allowedMethod>POST</allowedMethod>
        <allowedMethod>DELETE</allowedMethod>
        <allowedHeader>*</allowedHeader>
    </corsRule>
</corsConfiguration>

```

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

2. ダッシュボードで \* View Buckets を選択するか、 storage (S3) > Buckets \*を選択します。
3. 表からバケット名を選択します。

バケットの詳細ページが表示されます。

4. [Bucket access]タブで、[Cross-Origin Resource Sharing (CORS) ]\*アコーディオンを選択します。
5. [Enable CORS]チェックボックスをオンにします。
6. CORS設定XMLをテキストボックスに貼り付けます。
7. 「変更を保存」を選択します。

**CORS**設定を変更します

手順

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

**CORS**設定を無効にします

手順

1. [Enable CORS]チェックボックスをオフにします。
2. 「変更を保存」を選択します。

バケット内のオブジェクトを削除する

Tenant Managerを使用して、1つ以上のバケット内のオブジェクトを削除できます。

## 考慮事項と要件

これらの手順を実行する前に、次の点に注意してください。

- バケット内のオブジェクトを削除すると、StorageGRID はStorageGRID システム内のすべてのノードとサイトから、選択した各バケット内のすべてのオブジェクトとすべてのオブジェクトバージョンを完全に削除します。StorageGRID は、関連するオブジェクトメタデータも削除します。この情報を回復することはできません。
- オブジェクト、オブジェクトコピー、および同時処理の数によっては、バケット内のすべてのオブジェクトの削除に数分、数日、場合によっては数週間かかることがあります。
- バケットにがある場合 "S3オブジェクトロックが有効になりました" の場合は、\_年\_の間、\* Deleting objects : read-only \*状態のままになることがあります。



S3オブジェクトロックを使用するバケットは、すべてのオブジェクトの保持期限に達してリーガルホールドが解除されるまで、\* Deleting objects : read-only \*状態のままでです。

- オブジェクトの削除中、バケットの状態は\* Deleting objects : read-only \*です。この状態の場合、バケットに新しいオブジェクトを追加することはできません。
- すべてのオブジェクトが削除されると、バケットは読み取り専用状態のままになります。次のいずれかを実行できます。
  - バケットを書き込みモードに戻し、新しいオブジェクトに再利用します
  - バケットを削除します
  - バケット名はあとで使用できるように、読み取り専用モードのままにしておきます
- バケットでオブジェクトのバージョン管理が有効になっている場合は、StorageGRID 11.8以降で作成された削除マーカーを削除するには、[Delete objects in bucket]処理を使用します。
- バケットでオブジェクトのバージョン管理が有効になっている場合、StorageGRID 11.7以前で作成された削除マーカーは削除されません。バケット内のオブジェクトの削除に関する情報を参照："S3 バージョン管理オブジェクトの削除方法"。
- を使用する場合 "グリッド間レプリケーション"次の点に注意してください。
  - このオプションを使用しても、他のグリッドのバケットからオブジェクトは削除されません。
  - ソースバケットに対してこのオプションを選択すると、もう一方のグリッドのデスティネーションバケットにオブジェクトを追加すると\* Cross-grid replication failure \*アラートがトリガーされます。他のグリッドのバケットにオブジェクトが追加されないことを保証できない場合は、"グリッド間レプリケーションを無効にします" をクリックしてから、すべてのバケットオブジェクトを削除してください。

作業を開始する前に

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

手順

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

バケットページが表示され、既存の S3 バケットがすべて表示されます。

2. 特定のバケットの\*[Actions]\*メニューまたは詳細ページを使用します。

【アクション】メニュー

- オブジェクトを削除する各バケットのチェックボックスを選択します。
- >[Delete objects in bucket]\*を選択します。

詳細ページ

- 詳細を表示するバケット名を選択します。
- [Delete objects in bucket]\*を選択します。

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

4. 削除処理が開始されるまで待ちます。

数分後：

- バケットの詳細ページに黄色のステータスバーが表示されます。進行状況バーは、削除されたオブジェクトの割合を表します。
- 「（読み取り専用）」は、バケットの詳細ページでバケット名のあとに表示されます。
- [Buckets]ページでバケット名の横に「（Deleting objects : read-only）」と表示されます。

The screenshot shows the AWS S3 Buckets page with a single bucket named "my-bucket". The bucket details are as follows:

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

A green success message at the top right says "Starting to delete objects from one bucket." Below the bucket name, there is a yellow warning box stating: "All bucket objects are being deleted. StorageGRID is deleting all copies of the objects in this bucket, which might take days or weeks. While objects are being deleted, the bucket is read only. To stop the operation, select Stop deleting objects. You cannot restore objects that have already been deleted." A progress bar at the bottom of this box shows "0% (0 of 3 objects deleted)". At the bottom left of the yellow box is a button labeled "Stop deleting objects".

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

[Stop deleting objects]\*を選択すると、バケットは書き込みモードに戻りますが、削除されたオブジェクト

にアクセスしたりリストアしたりすることはできません。

## 6. 処理が完了するまで待ちます。

バケットが空の場合、ステータスバーは更新されますが、バケットは読み取り専用のままです。

Buckets > my-bucket

## my-bucket (read-only)

Region: us-east-1

Date created: 2022-12-14 10:09:50 MST

Object count: 0

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

Delete bucket

**Bucket is empty but is still read-only.**

This bucket is now empty.

- To remove this bucket, select **Delete bucket**.
- To return this bucket to write mode so it can be reused, select **Stop deleting objects**.

Stop deleting objects

## 7. 次のいずれかを実行します。

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



すべてのオブジェクトの削除後にバージョン管理されたバケットを削除できない場合  
は、削除マーカーが残っていることがあります。バケットを削除するには、残りのすべての削除マーカーを削除する必要があります。

- バケットを書き込みモードに戻し、必要に応じて新しいオブジェクト用に再利用します。1つのバケットに対して**[Stop deleting objects]**を選択するか、**[Buckets]**ページに戻って、複数のバケットに対して**[Action]>\*[Stop deleting objects]\***を選択します。

## S3 バケットを削除します

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

作業を開始する前に

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

- 削除するバケットが空です。削除するバケットが`_not_empty`の場合は、"バケットからオブジェクトを削除する"。

このタスクについて

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

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

手順

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

バケットページが表示され、既存の S3 バケットがすべて表示されます。

- 特定のバケットの\*[Actions]\*メニューまたは詳細ページを使用します。

【アクション】メニュー

- 削除する各バケットのチェックボックスを選択します。
- >[Delete Buckets]\*を選択します。

詳細ページ

- 詳細を表示するバケット名を選択します。
- [Delete bucket]\*を選択します。

- 確認ダイアログボックスが表示されたら、\*[はい]\*を選択します。

StorageGRID は、各バケットが空であることを確認してから、各バケットを削除します。この処理には数分かかることがあります。

バケットが空でない場合は、エラーメッセージが表示されます。実行する必要があります "[バケット内のすべてのオブジェクトと削除マークを削除する](#)" バケットを削除する前に。

## S3コンソールを使用

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

S3コンソールでは、次の操作を実行できます。

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

- 表示、作成、名前変更、コピー、移動、フォルダの削除

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



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

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

作業を開始する前に

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

手順

- storage > Buckets \* > \*bucket name\* を選択します。
- [S3][Console]タブを選択します。
- アクセスキーIDとシークレットアクセスキーをフィールドに貼り付けます。それ以外の場合は、\*アクセスキーのアップロード\*を選択し、を選択します .csv ファイル。
- 「サインイン」を選択します。
- バケットオブジェクトのテーブルが表示されます。必要に応じてオブジェクトを管理できます。

追加情報

- 接頭辞で検索：接頭辞検索機能は、現在のフォルダに対して特定の単語で始まるオブジェクトのみを検索します。検索には、他の場所でその単語を含むオブジェクトは含まれません。このルールは、フォルダ内のオブジェクトも環境します。たとえば、folder1/folder2/somefile- 内部にあるオブジェクトを返します。folder1/folder2/ フォルダを作成し、次の単語で開始します。somefile-。
- ドラッグアンドドロップ:コンピューターのファイルマネージャからS3コンソールにファイルをドラッグアンドドロップできます。ただし、フォルダをアップロードすることはできません。
- フォルダの操作:フォルダを移動、コピー、または名前変更すると、フォルダ内のすべてのオブジェクトが一度に1つずつ更新されるため、時間がかかる場合があります。
- バケットのバージョン管理が無効な場合の完全削除：バージョン管理が無効なバケット内のオブジェクトを上書きまたは削除すると、処理は永続的に実行されます。を参照してください ["バケットのオブジェクトのバージョン管理を変更する"](#)。

## S3 プラットフォームサービスを管理します

## プラットフォームサービスの管理：概要

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

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

### CloudMirror レプリケーション

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

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



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

### 通知

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

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



S3 オブジェクトのロックが有効になっているバケットでイベント通知を設定することはできますが、オブジェクトの S3 オブジェクトロックメタデータ (Retain Until Date および Legal Hold のステータスを含む) は通知メッセージに含まれません。

### 検索統合サービス

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

たとえば、リモートの Elasticsearch サービスに S3 オブジェクトメタデータを送信するようにバケットを設定できます。次に、Elasticsearch を使用してバケット間で検索を実行し、オブジェクトメタデータのパターンに対して高度な分析を実行できます。



S3 オブジェクトロックが有効なバケットでは Elasticsearch 統合を設定できますが、オブジェクトの S3 オブジェクトロックメタデータ (Retain Until Date および Legal Hold のステータスを含む) は通知メッセージに含まれません。

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

単一の S3 バケットに対して複数のプラットフォームサービスを組み合わせて設定できます。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、を使用して設定した外部エンドポイントと通信します "[Tenant Manager の略](#)" または "[テナント管理 API](#)"。各エンドポイントは外部のデステイネーション（StorageGRID S3バケット、Amazon Web Servicesバケット、Amazon SNSトピック、ローカルやAWSなどでホストされるElasticsearchクラスタなど）です。

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

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

- キーがで始まるすべてのオブジェクトを指定する場合 /images Amazon S3バケットにレプリケートするには、ソースバケットにレプリケーション設定を追加する必要があります。
- これらのオブジェクトがバケットに格納されたときに通知も送信するには、通知設定を追加する必要があります。
- 最後に、これらのオブジェクトのメタデータのインデックスを作成する場合は、検索統合を実装するためのメタデータ通知設定を追加する必要があります。

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

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

#### 関連情報

["プラットフォームサービスに関する考慮事項"](#)

#### CloudMirror レプリケーションサービス

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

て CloudMirror レプリケーションを有効にすることができます。

CloudMirror レプリケーションは、グリッドのアクティブな ILM ポリシーとは独立して動作します。CloudMirror サービスは、ソースバケットに格納された時点でオブジェクトをレプリケートし、できるだけ早くデスティネーションバケットに配信します。レプリケートオブジェクトの配信は、オブジェクトの取り込みが成功したときにトリガーされます。

 CloudMirror レプリケーションには、クロスグリッドレプリケーション機能と重要な類似点と相違点があります。詳細については、["グリッド間レプリケーションと CloudMirror レプリケーションを比較してください"](#)。

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

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

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

また、バージョン管理に対応している / していないバケットで CloudMirror レプリケーションを設定することもでき、バージョン管理に対応している / していないバケットをデスティネーションとして指定できます。バージョン管理に対応しているバケットとしていないバケットを組み合わせ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。

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

 レプリカのマークに使用されるカスタムヘッダーは `x-ntap-sg-replica`。このマーキングは「カスケード・ミラーを防止します」StorageGRID では、2つのグリッド間の双方向 CloudMirror がサポートされます。

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

に配信されることがあります。まれに、複数の異なる StorageGRID サイトから同じオブジェクトが同時に更新された場合、デスティネーションバケットでの処理の順序がソースバケットでのイベントの順序と一致しないことがあります。

通常、CloudMirror レプリケーションは外部の S3 バケットをデスティネーションとして使用するように設定します。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。

バケットの通知について理解します

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

可能です "イベント通知を設定する" 通知設定 XML をソースバケットに関連付けます。通知設定 XML には S3 の規則に従ってバケット通知を設定し、デスティネーションの Kafka または Amazon SNS トピックをエンドポイントの URN として指定します。

イベント通知は通知設定に従ってソースバケットで作成され、デスティネーションに配信されます。オブジェクトに関連付けられているイベントが成功すると、そのイベントに関する通知が作成されて配信のためにユーザーに登録されます。

通知の一意性と順序は保証されません。確実に配信することを目的とした処理の結果として、1 つのイベントに関する通知が複数デスティネーションに配信されることがあります。また配信は非同期で実行されるため、特に異なる StorageGRID サイトで開始された処理の場合、デスティネーションでの通知の時間的順序がソースバケットでのイベントの順序と一致する保証はありません。を使用できます sequencer Amazon S3 のドキュメントに従って、イベントメッセージを入力して特定のオブジェクトに対するイベントの順序を決定します。

サポートされている通知およびメッセージです

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

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

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

検索統合サービスについて理解する

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

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

検索統合サービスはバージョン管理に対応している / していないに関わらずすべてのバケットに対して有効にすることができ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。ドキュメントのインデックス作成後は、インデックス内のドキュメントのフィールドタイプを編集することはできません。

通知は次の場合に常に生成され、配信のキューに登録されます

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

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

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

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

#### 関連情報

["検索統合用の XML を設定します"](#)

["メタデータ通知に含まれているオブジェクトメタデータ"](#)

["検索統合サービスで生成される JSON"](#)

["検索統合サービスを設定する"](#)

#### プラットフォームサービスに関する考慮事項

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

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

#### プラットフォームサービスの使用に関する考慮事項

考慮事項	詳細
デスティネーションエンドポイントの監視	各デスティネーションエンドポイントの可用性を監視する必要があります。長時間にわたってデスティネーションエンドポイントへの接続が失われ、要求のバックログが大量に発生している場合、StorageGRID に対する以降のクライアント要求（PUT 要求など）は失敗します。エンドポイントがアクセス可能になったら、失敗した要求を再試行する必要があります。
デスティネーションエンドポイントのスロットル	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。

考慮事項	詳細
順序保証	<p>StorageGRID では、1つのサイト内のオブジェクトに対する処理の順序が保証されます。あるオブジェクトに対するすべての処理が同じサイト内で実行されるかぎり、最終的なオブジェクトの（レプリケーションの）状態は常に StorageGRID の状態と同じになります。</p> <p>StorageGRID は、StorageGRID サイト間で処理が行われる場合、最善の順序で要求を処理しようと試みます。たとえば、最初にサイト A にオブジェクトを書き込んだあと、サイト B で同じオブジェクトを上書きした場合、CloudMirror によって最終的にデスティネーションバケットにレプリケートされるオブジェクトが新しいほうのオブジェクトであるとはかぎりません。</p>
ILM ベースのオブジェクト削除	<p>AWS CRR と Amazon Simple Notification Service の削除動作と一致するように、StorageGRID ILM ルールに基づいてソースバケット内のオブジェクトが削除された場合、CloudMirror 要求とイベント通知要求は送信されません。たとえば、ILM ルールによって 14 日後にオブジェクトが削除された場合、CloudMirror 要求やイベント通知要求は送信されません。</p> <p>一方、ILM に基づいてオブジェクトが削除された場合、検索統合要求は送信されます。</p>
Kafkaエンドポイントの使用	<p>Kafkaエンドポイントでは、相互TLSはサポートされていません。その結果、<code>ssl.client.auth</code> をに設定します <code>required</code> Kafkaプローカーの設定では、原因Kafkaエンドポイントの設定に問題がある可能性があります。</p> <p>Kafkaエンドポイントの認証では、次の認証タイプが使用されます。これらのタイプは、Amazon SNSなどの他のエンドポイントの認証に使用されるタイプとは異なり、ユーザ名とパスワードのクレデンシャルが必要です。</p> <ul style="list-style-type: none"> <li>• SASL/プレーン</li> <li>• SASL/SCRAM-SHA-256</li> <li>• SASL/SCRAM-SHA-512</li> </ul> <p>*注：*構成済みのストレージプロキシ設定は、Kafkaプラットフォームサービスエンドポイントには適用されません。</p>

#### CloudMirror レプリケーションサービスの使用に関する考慮事項

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

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

プラットフォームサービスエンドポイントを設定する

バケットのプラットフォームサービスを設定する前に、少なくとも 1 つのエンドポイントをプラットフォームサービスのデスティネーションとして設定する必要があります。

プラットフォームサービスへのアクセスは、StorageGRID 管理者がテナント単位で有効にします。プラットフォームサービスエンドポイントを作成または使用するには、ストレージノードが外部のエンドポイントリソースにアクセスできるようネットワークが設定されているグリッドで、Manage Endpoints または Root Access 権限を持つテナントユーザである必要があります。1つのテナントに対して設定できるプラットフォームサービスエンドポイントは最大500個です。詳細については、StorageGRID 管理者にお問い合わせください。

プラットフォームサービスエンドポイントとは何ですか。

プラットフォームサービスエンドポイントを作成するときは、StorageGRID が外部のデスティネーションにアクセスするために必要な情報を指定します。

たとえば、StorageGRID バケットからAmazon S3バケットにオブジェクトをレプリケートする場合は、StorageGRID がAmazonのデスティネーションバケットにアクセスするために必要な情報とクレデンシャルを含むプラットフォームサービスエンドポイントを作成します。

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

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

#### CloudMirror レプリケーション用のエンドポイント

StorageGRID は、S3 バケットを表すレプリケーションエンドポイントをサポートします。このバケットは、Amazon Web Services、同一またはリモートの StorageGRID 環境、あるいは別のサービスでホストされている可能性があります。

#### 通知用のエンドポイント

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

Kafka エンドポイントでは、相互 TLS はサポートされていません。その結果、`ssl.client.auth` をに設定します `required` Kafka ブローカーの設定では、原因 Kafka エンドポイントの設定に問題がある可能性があります。

#### 検索統合サービスのエンドポイント

StorageGRID は、Elasticsearch クラスタを表す検索統合エンドポイントをサポートします。Elasticsearch クラスタは、ローカルデータセンターに配置することも、AWS クラウドなどの別の場所でホストすることもできます。

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

## 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** を指定してください

プラットフォームサービスエンドポイントを作成するときは、 Unique Resource Name ( URN ) を指定する必要があります。プラットフォームサービスの設定XMLを作成するときは、 URNを使用してエンドポイントを参照します。各エンドポイントの URN は一意である必要があります。

プラットフォームサービスエンドポイントは、作成時に StorageGRID で検証されます。プラットフォームサービスエンドポイントを作成する前に、エンドポイントで指定されたリソースが存在し、アクセス可能であることを確認してください。

#### URN 要素

プラットフォームサービスのエンドポイントのURNは、 いずれかで開始する必要があります `arn:aws` または `urn:mysite`、次のようにします。

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

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

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

サービス	を入力します
CloudMirror レプリケーション	<code>s3</code>
通知	<code>sns</code> または <code>kafka</code>
検索統合	<code>es</code>

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	<code>bucket-name</code>
通知	<code>sns-topic-name</code> または <code>kafka-topic-name</code>

サービス	特定のリソース
検索統合	<p>domain-name/index-name/type-name</p> <ul style="list-style-type: none"> <li>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。</li> </ul>

## AWS と GCP でホストされるサービスの URN

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

- CloudMirror レプリケーション：

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

- 通知：

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

- 検索統合：

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



AWS検索統合エンドポイントの場合は、を参照してください domain-name リテラル文字列を含める必要があります `domain/` を参照してください。

## ローカルでホストされるサービスの URN

クラウド サービス ではなくローカルでホストされるサービスを使用する場合は、URN の 3 番目と最後の必須要素が含まれていて、有効かつ一意な URN が作成されるのであれば、どのような方法で URN を指定してもかまいません。となっている要素はオプションで空白にすることも、リソースを識別して一意な URN の作成に役立つ任意の情報を指定することもできます。例：

- CloudMirror レプリケーション：

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

StorageGRID でホストされるCloudMirrorエンドポイントの場合は、で始まる有効なURNを指定できます  
urn:sgws:

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

- ・通知：

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

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

Kafkaエンドポイントを指定します。

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

- ・検索統合：

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



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

プラットフォームサービスエンドポイントを作成します

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

作業を開始する前に

- ・Tenant Manager にはを使用してサインインします "サポートされている Web ブラウザ"。
- ・テナントアカウントのプラットフォームサービスがStorageGRID 管理者によって有効にされている。
- ・が設定されたユーザグループに属している必要があります "エンドポイントまたはRoot Access権限を管理します"。
- ・プラットフォームサービスエンドポイントによって参照されるリソースを作成しておきます。
  - CloudMirror レプリケーション：S3 バケット
  - イベント通知：Amazon Simple Notification Service (Amazon SNS) またはKafka トピック
  - 検索通知：インデックスを自動的に作成するようにデスティネーションクラスタが設定されていない場合、Elasticsearch インデックス。
- ・デスティネーションリソースに関する情報を確認しておきます。
  - Uniform Resource Identifier (URI) のホストとポート



StorageGRID システムでホストされているバケットを CloudMirror レプリケーションのエンドポイントとして使用する場合は、グリッド管理者に問い合わせて入力が必要な値を決定してください。

◦ Unique Resource Name (URN)

"プラットフォームサービスのエンドポイントの URN を指定してください"

- 認証クレデンシャル（必要な場合）：

#### 検索統合エンドポイント

検索統合エンドポイントには、次のクレデンシャルを使用できます。

- Access Key : アクセスキー ID とシークレットアクセスキー
- 基本 HTTP 認証 : ユーザ名とパスワード

#### CloudMirrorレプリケーションエンドポイント

CloudMirrorレプリケーションでは、次のクレデンシャルを使用できます。

- Access Key : アクセスキー ID とシークレットアクセスキー
- CAP ( C2S Access Portal ) : 一時的なクレデンシャル URL、サーバ証明書とクライアント証明書、クライアントキー、およびオプションのクライアント秘密鍵パスフレーズ。

#### Amazon SNSエンドポイント

Amazon SNSエンドポイントの場合は、次のクレデンシャルを使用できます。

- Access Key : アクセスキー ID とシークレットアクセスキー

#### Kafkaエンドポイント

Kafkaエンドポイントの場合は、次のクレデンシャルを使用できます。

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

- セキュリティ証明書（カスタム CA 証明書を使用する場合）

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

#### 手順

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

エンドポイントがサポートするプラットフォームサービスのタイプは、[Endpoints]ページのエンドポイント名の横に表示されるため、この情報を名前に含める必要はありません。

4. [\* URI\*] フィールドに、エンドポイントの Unique Resource Identifier ( URI ) を指定します。

次のいずれかの形式を使用します。

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

ポートを指定しない場合は、次のデフォルトポートが使用されます。

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

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

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

この例では、s3.example.com StorageGRIDハイアベイラビリティ(HA)グループの仮想IP(VIP)のDNSエントリ、およびを表します10443ロードバランサエンドポイントで定義されたポートを表します。



単一点障害 (Single Point of Failure) を回避するために、可能なかぎりロードバランシングノードのHAグループに接続する必要があります。

同様に、AWSでホストされているバケットのURIは次のようにになります。

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



エンドポイントがCloudMirrorレプリケーションサービスに使用される場合は、URIにバケット名を含めないでください。バケット名は「\* URN \*」フィールドに含める必要があります。

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



エンドポイントの作成後にエンドポイントのURNを変更することはできません。

6. 「\* Continue \*」を選択します。

7. [認証タイプ]\*の値を選択します。

### 検索統合エンドポイント

検索統合エンドポイントのクレデンシャルを入力またはアップロードします。

指定するクレデンシャルには、デスティネーションリソースに対する書き込み権限が必要です。

認証タイプ	説明	クレデンシャル
匿名	デスティネーションへの匿名アクセスを許可します。セキュリティが無効になっているエンドポイントでのみ機能します。	認証なし。
アクセスキー	AWS 形式のクレデンシャルを使用してデスティネーションとの接続を認証します。	<ul style="list-style-type: none"><li>・アクセスキー ID</li><li>・シークレットアクセスキー</li></ul>
基本 HTTP	ユーザ名とパスワードを使用して、デスティネーションへの接続を認証します。	<ul style="list-style-type: none"><li>・ユーザ名</li><li>・パスワード</li></ul>

### CloudMirrorレプリケーションエンドポイント

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

指定するクレデンシャルには、デスティネーションリソースに対する書き込み権限が必要です。

認証タイプ	説明	クレデンシャル
匿名	デスティネーションへの匿名アクセスを許可します。セキュリティが無効になっているエンドポイントでのみ機能します。	認証なし。
アクセスキー	AWS 形式のクレデンシャルを使用してデスティネーションとの接続を認証します。	<ul style="list-style-type: none"><li>・アクセスキー ID</li><li>・シークレットアクセスキー</li></ul>

認証タイプ	説明	クレデンシャル
CAP ( C2S Access Portal )	証明書とキーを使用してデスティネーションへの接続を認証します。	<ul style="list-style-type: none"> <li>一時的な資格情報 URL</li> <li>サーバ CA 証明書 ( PEM ファイルのアップロード)</li> <li>クライアント証明書 ( PEM ファイルのアップロード)</li> <li>クライアント秘密鍵 ( PEM ファイルのアップロード、 OpenSSL 暗号化形式、または暗号化されていない秘密鍵形式)</li> <li>クライアント秘密鍵のパスフレーズ ( オプション )</li> </ul>

#### Amazon SNSエンドポイント

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

指定するクレデンシャルには、デスティネーションリソースに対する書き込み権限が必要です。

認証タイプ	説明	クレデンシャル
匿名	デスティネーションへの匿名アクセスを許可します。セキュリティが無効になっているエンドポイントでのみ機能します。	認証なし。
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>

#### Kafkaエンドポイント

Kafkaエンドポイントのクレデンシャルを入力またはアップロードします。

指定するクレデンシャルには、デスティネーションリソースに対する書き込み権限が必要です。

認証タイプ	説明	クレデンシャル
匿名	デスティネーションへの匿名アクセスを許可します。セキュリティが無効になっているエンドポイントでのみ機能します。	認証なし。
SASL/プレーン	プレーンテキストのユーザ名とパスワードを使用して、宛先への接続を認証します。	<ul style="list-style-type: none"> <li>ユーザ名</li> <li>パスワード</li> </ul>

認証タイプ	説明	クレデンシャル
SASL/SCRAM-SHA-256	チャレンジ応答プロトコルとSHA-256ハッシュを使用してユーザ名とパスワードを使用し、宛先への接続を認証します。	<ul style="list-style-type: none"> <li>・ユーザ名</li> <li>・パスワード</li> </ul>
SASL/SCRAM-SHA-512	チャレンジ応答プロトコルとSHA-512ハッシュを使用してユーザ名とパスワードを使用し、宛先への接続を認証します。	<ul style="list-style-type: none"> <li>・ユーザ名</li> <li>・パスワード</li> </ul>

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

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

Enter details
Select authentication type
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-----
abcdefgijkl1234567890ABCDEFGHIJKLM
123456/7890ABCDEFabcdefgijkl1234567890ABCDEFGHIJKLM
-----END CERTIFICATE-----
```

[Previous](#)
Test and create endpoint

証明書検証のタイプ	説明
カスタム CA 証明書を使用する	カスタムのセキュリティ証明書を使用します。この設定を選択した場合は、カスタムセキュリティ証明書を * CA 証明書 * テキストボックスにコピーして貼り付けます。
オペレーティングシステムの CA 証明書を使用します	オペレーティングシステムにインストールされているデフォルトの Grid CA 証明書を使用して接続を保護します。
証明書を検証しないでください	TLS 接続に使用される証明書は検証されません。このオプションはセキュアではありません。

10. [\* テストとエンドポイントの作成 \*] を選択します。

- 指定したクレデンシャルを使用してエンドポイントにアクセスできた場合は、成功を伝えるメッセージが表示されます。エンドポイントへの接続は、各サイトの 1 つのノードから検証されます。
- エンドポイントの検証が失敗した場合は、エラーメッセージが表示されます。エラーを修正するためエンドポイントを変更する必要がある場合は、\* エンドポイントの詳細に戻る \* を選択して情報を更新します。次に、「\* Test」を選択し、エンドポイントを作成します。\*



テナントアカウントでプラットフォームサービスが有効になっていないと、エンドポイントの作成が失敗します。StorageGRID 管理者にお問い合わせください。

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

#### 関連情報

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

["CloudMirror レプリケーションを設定します"](#)

["イベント通知を設定する"](#)

["検索統合サービスを設定する"](#)

プラットフォームサービスエンドポイントの接続をテストします

プラットフォームサービスへの接続が変更された場合は、エンドポイントへの接続をテストして、デスティネーションリソースが存在すること、および指定したクレデンシャルでアクセスできることを確認できます。

#### 作業を開始する前に

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

#### このタスクについて

StorageGRID は、クレデンシャルに正しい権限があるかどうかを検証しません。

## 手順

- 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					<a href="#">Create endpoint</a>
<a href="#">Delete endpoint</a>	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

- 接続をテストするエンドポイントを選択します。

エンドポイントの詳細ページが表示されます。

**Overview**

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

Type: **S3 Bucket**

URI: <http://10.96.104.167:10443>

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

**Connection**    **Configuration**

**Verify connection** [?](#)

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

**Test connection**

3. [接続のテスト \*] を選択します。

- 指定したクレデンシャルを使用してエンドポイントにアクセスできた場合は、成功を伝えるメッセージが表示されます。エンドポイントへの接続は、各サイトの1つのノードから検証されます。
- エンドポイントの検証が失敗した場合は、エラーメッセージが表示されます。エラーを修正するために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を編集します

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

作業を開始する前に

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

手順

- 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

Display name	Last error	Type	URI	URN
my-endpoint-1		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket1
my-endpoint-2	2 hours ago	Search	http://10.96.104.30:9200	urn:sgws:es:::mydomain/sveloso/_doc
my-endpoint-3		Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example1
my-endpoint-4		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket2

2. 編集するエンドポイントを選択します。

エンドポイントの詳細ページが表示されます。

3. 「\* Configuration \*」を選択します。
4. 必要に応じて、エンドポイントの設定を変更します。



エンドポイントの作成後にエンドポイントのURNを変更することはできません。

- a. エンドポイントの表示名を変更するには、編集アイコンを選択します
- b. 必要に応じて、URIを変更します。
- c. 必要に応じて、認証タイプを変更します。
  - アクセスキー認証の場合は、必要に応じて「\* S3 キーの編集」を選択し、新しいアクセスキー ID とシークレットアクセスキーを貼り付けることで、キーを変更します。変更をキャンセルする必要がある場合は、\* Revert S3 key edit \* を選択します。
  - CAP (C2S Access Portal) 認証の場合は、一時的なクレデンシャル URL またはオプションのクライアント秘密鍵パスフレーズを変更し、必要に応じて新しい証明書と鍵ファイルをアップロードします。



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

- d. 必要に応じて、サーバを検証する方法を変更します。
5. [変更のテストと保存 \*] を選択します。

- 指定したクレデンシャルを使用してエンドポイントにアクセスできた場合は、成功を伝えるメッセージが表示されます。エンドポイントへの接続は、各サイトの1つのノードから検証されます。
- エンドポイントの検証が失敗した場合は、エラーメッセージが表示されます。エンドポイントを変更してエラーを修正し、[変更のテストと保存]を選択します。

プラットフォームサービスエンドポイントを削除します

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

作業を開始する前に

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

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.

The screenshot shows a table with the following data:

<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

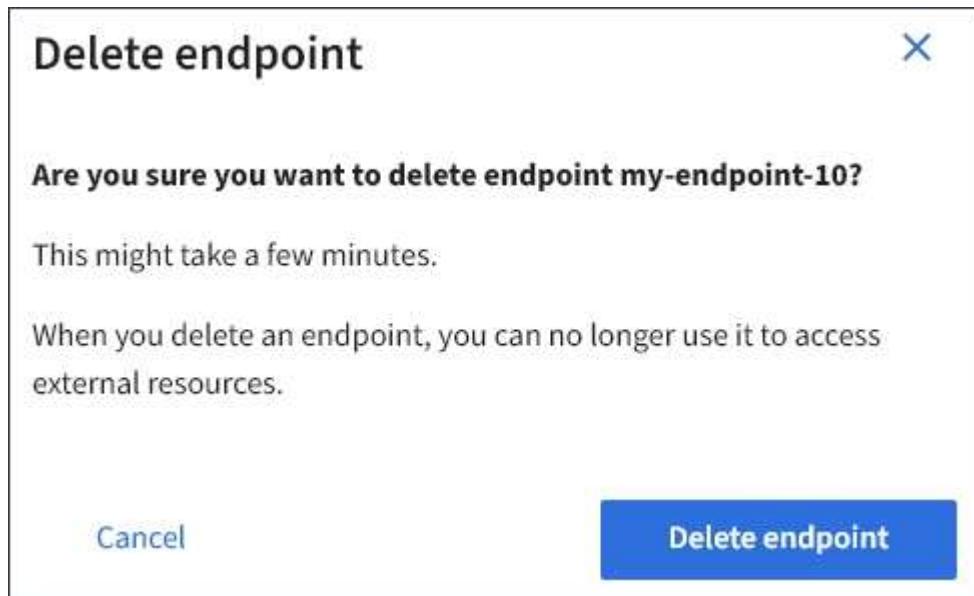
2. 削除する各エンドポイントのチェックボックスを選択します。



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を行います

StorageGRID がプラットフォームサービスエンドポイントと通信しようとしたときにエラーが発生すると、ダッシュボードにメッセージが表示されます。Platform services Endpoints ページの Last error 列は、エラーが発生してからの時間を示します。エンドポイントのクレデンシャルに関連付けられている権限が正しくない場合は、エラーは表示されません。

エラーが発生したかどうかを確認します

過去7日以内にプラットフォームサービスエンドポイントエラーが発生した場合は、Tenant Managerダッシュボードにアラートメッセージが表示されます。プラットフォームサービスのエンドポイントページに移動して、エラーの詳細を確認できます。

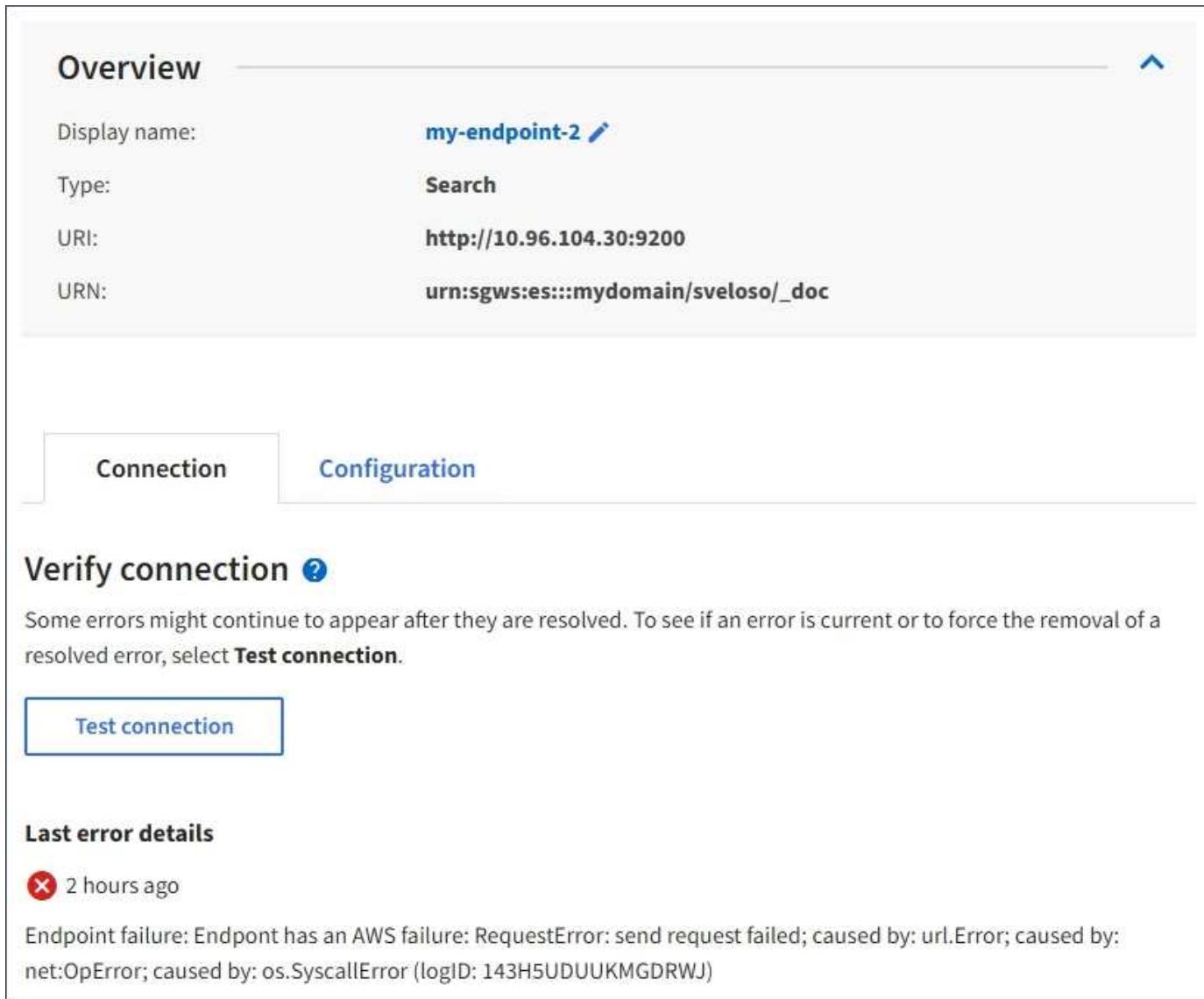


One or more endpoints have experienced an error and might not be functioning properly. Go to the [Endpoints](#) page to view the error details. The last error occurred 2 hours ago.

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

## 手順

1. エンドポイントのリストで、エラーが発生したエンドポイントを選択します。
2. エンドポイントの詳細ページで、 \* 接続 \* を選択します。このタブには、エンドポイントの最新のエラーと、エラーが発生してからの経過時間が表示されます。赤の X アイコンを含むエラー  過去 7 日以内に発生しました。



The screenshot shows the AWS Lambda Overview page for an endpoint named "my-endpoint-2". The endpoint details are as follows:

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

The "Configuration" tab is selected. Below it, the "Verify connection" section contains a "Test connection" button. The "Last error details" section shows a recent error from 2 hours ago:

 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)

エラーがまだ最新であるかどうかを確認します

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

## 手順

1. エンドポイントを選択します。

エンドポイントの詳細ページが表示されます。

2. 接続 > 接続テスト \* を選択します。

[接続のテスト \*] を選択すると、StorageGRID はプラットフォームサービスエンドポイントが存在すること、および現在のクレデンシャルでアクセスできることを検証します。エンドポイントへの接続は、各サイトの 1 つのノードから検証されます。

## エンドポイントエラーの解決

エンドポイントの詳細ページの「\* Last error \*」メッセージを使用して、エラーの原因を特定できます。一部のエラーでは、問題を解決するためにエンドポイントの編集が必要になります。たとえば、StorageGRID に正しいアクセス権限がないか、アクセスキーが期限切れになっているためにデスティネーションの S3 バケットにアクセスできない場合、CloudMirror のエラーが発生することがあります。メッセージは「Either the endpoint credentials or the destination access needs to be updated」で、詳細は「AccessDenied」または「InvalidAccessKeyId」です。

エラーを解決するためにエンドポイントを編集する必要がある場合は、「\* 変更のテストと保存 \*」を選択すると、StorageGRID によって更新されたエンドポイントが検証され、現在のクレデンシャルで到達できることが確認されます。エンドポイントへの接続は、各サイトの 1 つのノードから検証されます。

## 手順

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

## 必要な権限がないエンドポイントクレデンシャルです

StorageGRID によるプラットフォームサービスエンドポイントの検証では、エンドポイントのクレデンシャルを使用してデスティネーションリソースに接続できること、および基本的な権限チェックを実行できることが確認されます。ただし、StorageGRID では、特定のプラットフォームサービス処理に必要なすべての権限が検証されるわけではありません。そのため、プラットフォームサービスを使用しようとしたときにエラー（「403 Forbidden」など）が表示された場合は、エンドポイントのクレデンシャルに関連付けられている権限を確認してください。

## 関連情報

- "[StorageGRID の管理 > プラットフォームサービスのトラブルシューティング](#)"
- "[プラットフォームサービスエンドポイントを作成します](#)"
- "[プラットフォームサービスエンドポイントの接続をテストします](#)"
- "[プラットフォームサービスエンドポイントを編集します](#)"

## CloudMirror レプリケーションを設定します

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

## 作業を開始する前に

- テナントアカウントのプラットフォームサービスが StorageGRID 管理者によって有効にされている。
- レプリケーションソースとして機能するバケットがすでに作成されている。

- CloudMirrorレプリケーションのデスティネーションとして使用するエンドポイントがすでに存在し、そのURNが必要です。
- が設定されたユーザグループに属している必要があります "すべてのバケットまたはRoot Access権限を管理します"。これらの権限は、Tenant Manager を使用してバケットを設定する際にグループポリシーまたはバケットポリシーの権限設定よりも優先されます。

このタスクについて

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



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

バケットでCloudMirrorレプリケーションを有効にするには、有効なバケットレプリケーション設定XMLを作成して適用する必要があります。レプリケーション設定 XML では、各デスティネーションとして S3 バケットエンドポイントの URN を使用する必要があります。



S3 オブジェクトロックが有効なソースバケットまたはデスティネーションバケットでは、レプリケーションはサポートされません。

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

オブジェクトを含むバケットでCloudMirrorレプリケーションを有効にすると、バケットに追加された新しいオブジェクトがレプリケートされますが、バケット内の既存のオブジェクトはレプリケートされません。レプリケーションをトリガーするには、既存のオブジェクトを更新する必要があります。

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

手順

- ソースバケットのレプリケーションを有効にします。

S3 レプリケーション API で指定されているように、レプリケーションを有効にするために必要なレプリケーション設定 XML をテキストエディタで作成します。XML を設定する場合は、次の点に

- StorageGRID では、V1 のレプリケーション設定のみがサポートされます。つまり、StorageGRID では、の使用はサポートされていません Filter ルールのエレメント。V1の規則に従ってオブジェクトバージョンを削除します。詳細については、レプリケーション設定に関する Amazon のドキュメントを参照してください。
- デスティネーションとして S3 バケットエンドポイントの URN を使用してください。
- 必要に応じてを追加します <StorageClass> エレメントを選択し、次のいずれかを指定します。
  - STANDARD：デフォルトのストレージクラス。オブジェクトをアップロードするときにストレージクラスを指定しない場合は、が表示されます STANDARD ストレージクラスが使用されている。

- STANDARD\_IA : (標準-アクセス頻度の低いアクセス) このストレージクラスは、アクセス頻度は低いが、必要に応じて高速アクセスが必要なデータに使用します。
  - REDUCED\_REDUNDANCY : 重大度が低く、再現可能で、かつ冗長性に劣る状態で保存可能なデータには、このストレージクラスを使用します STANDARD ストレージクラス。
- を指定する場合 Role 設定 XML では無視されます。この値は StorageGRID では使用されません。

```

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

```

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

3. ソースバケットの名前を選択します。

バケットの詳細ページが表示されます。

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

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

**Replication**    **Disabled**    **^**

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

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

Enable replication

**Clear**

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

**Save changes**



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

## 7. レプリケーションが正しく設定されていることを確認します。

- 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

["プラットフォームサービスエンドポイントを作成します"](#)

## イベント通知を設定する

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

### 作業を開始する前に

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

### このタスクについて

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

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

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

## 手順

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

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

2. Tenant Manager で、 \* Storage ( S3 ) \* > \* Buckets \* を選択します。
3. ソースバケットの名前を選択します。  
バケットの詳細ページが表示されます。
4. プラットフォームサービス > イベント通知 \* を選択します。
5. [イベント通知を有効にする]\*チェックボックスをオンにします。
6. 通知設定 XML をテキストボックスに貼り付け、 \* 変更を保存 \* を選択します。

Bucket options   Bucket access   Platform services   S3 Console

**Replication**   Disabled

**Event notifications**   Disabled

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

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

Enable event notifications

**Clear**

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

```

**Save changes**



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

## 7. イベント通知が正しく設定されていることを確認します。

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

この例では、を使用してオブジェクトが作成されるたびにイベント通知が送信されます `images/` プレフィックス。

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

たとえば、デスティネーショントピックがAmazon SNSでホストされている場合は、通知が配信されたときにEメールを送信するようにサービスを設定できます。

```
{  
    "Records": [  
        {  
            "eventVersion": "2.0",  
            "eventSource": "sgws:s3",  
            "eventTime": "2017-08-08T23:52:38Z",  
            "eventName": "ObjectCreated:Put",  
            "userIdentity": {  
                "principalId": "11111111111111111111"  
            },  
            "requestParameters": {  
                "sourceIPAddress": "193.51.100.20"  
            },  
            "responseElements": {  
                "x-amz-request-id": "122047343"  
            },  
            "s3": {  
                "s3SchemaVersion": "1.0",  
                "configurationId": "Image-created",  
                "bucket": {  
                    "name": "test1",  
                    "ownerIdentity": {  
                        "principalId": "11111111111111111111"  
                    },  
                    "arn": "arn:sgws:s3:::test1"  
                },  
                "object": {  
                    "key": "images/cat.jpg",  
                    "size": 0,  
                    "eTag": "d41d8cd98f00b204e9800998ecf8427e",  
                    "sequencer": "14D90402421461C7"  
                }  
            }  
        }  
    ]  
}
```

+

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

## 関連情報

"[バケットの通知について理解します](#)"

"[S3 REST APIを使用する](#)"

"[プラットフォームサービスエンドポイントを作成します](#)"

検索統合サービスを使用する

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

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



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

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

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

## 関連情報

"[検索統合用の XML を設定します](#)"

"[メタデータ通知に含まれているオブジェクトメタデータ](#)"

"[検索統合サービスで生成される JSON](#)"

"[検索統合サービスを設定する](#)"

"[S3 REST APIを使用する](#)"

検索統合用の **XML** を設定します

検索統合サービスは、内に含まれる一連のルールを使用して設定します

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

オブジェクトはオブジェクト名のプレフィックスでフィルタリングできます。たとえば、というプレフィックスのオブジェクトのメタデータを送信できます images を1つのデスティネーションに、プレフィックスがの

オブジェクトのメタデータに追加します `videos` 別のノードに移動しますプレフィックスが重複している設定は有効ではなく、送信時に拒否されます。たとえば、プレフィックスが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。
ID	ルールの一意の識別子。  Rule 要素に含まれています。	いいえ

名前	説明	必須
ステータス	<p>Status には「 Enabled 」または「 Disabled 」を指定できます。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 REST APIを使用する"](#)

"メタデータ通知に含まれているオブジェクトメタデータ"

"検索統合サービスで生成される JSON"

"検索統合サービスを設定する"

検索統合サービスを設定します

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

作業を開始する前に

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

このタスクについて

ソースバケットに対して検索統合サービスを設定した場合、オブジェクトを作成またはオブジェクトのメタデータ / タグを更新すると、オブジェクトメタデータがデスティネーションエンドポイントに送信されます。すでにオブジェクトが含まれているバケットで検索統合サービスを有効にすると、既存のオブジェクトに関するメタデータ通知は自動的には送信されません。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。

Bucket options Bucket access Platform services

Replication Disabled ▾

Event notifications Disabled ▾

Search integration Disabled ▾

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

Clear

```
<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 \*チェックボックスをオフにします。
- S3 API を直接使用している場合は、DELETE Bucket メタデータ通知要求を使用します。S3 クライアントアプリケーションを実装する手順を参照してください。

関連情報

["検索統合サービスについて理解する"](#)

["検索統合用の XML を設定します"](#)

["S3 REST APIを使用する"](#)

["プラットフォームサービスエンドポイントを作成します"](#)

検索統合サービスで生成される JSON

バケットで検索統合サービスを有効にすると、オブジェクトのメタデータまたはタグの追加、更新、削除が行われるたびに、JSON ドキュメントが生成されてデスティネーションエンドポイントに送信されます。

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

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

メタデータ通知に含まれているオブジェクトメタデータ

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

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

を入力します	項目名と概要
バケットとオブジェクトの情報	bucket: バケットの名前
key: オブジェクトキー名	versionID: バージョン管理されたバケット内のオブジェクトバージョン
region: バケットリージョンなど us-east-1	システムメタデータ
size: HTTP クライアントに表示されるオブジェクトのサイズ(バイト単位)	md5: オブジェクトハッシュ
ユーザメタデータ	metadata: オブジェクトのすべてのユーザメタデータをキーと値のペアとして格納  key:value

を入力します	項目名と概要
タグ	<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。ドキュメントのインデックス作成後は、インデックス内のドキュメントのフィールドタイプを編集することはできません。

## S3 REST APIを使用する

### S3 REST APIでサポートされるバージョンと更新

StorageGRID は、Representational State Transfer (REST) の Web サービスのセットとして実装される Simple Storage Service (S3) をサポートします。

S3 REST APIのサポートにより、S3 Webサービス用に開発されたサービス指向アプリケーションを、StorageGRID システムを使用するオンプレミスのオブジェクトストレージに接続できます。クライアントアプリケーションで現在S3 REST API呼び出しを使用している場合は、変更を最小限に抑える必要があります。

### サポートされるバージョン

StorageGRID でサポートしている S3 および HTTP のバージョンは次のとおりです。

項目	バージョン
S3 API仕様	"Amazon Web Services (AWS) ドキュメント：「Amazon Simple Storage Service API Reference」"
HTTP	<p>1.1</p> <p>HTTP の詳細については、HTTP/1.1 (RFC 7230~7235) を参照してください。</p> <p>"IETF RFC 2616 : 『Hypertext Transfer Protocol (HTTP/1.1)』"</p> <ul style="list-style-type: none"> <li>注：StorageGRID は、HTTP/1.1 パイプラインをサポートしません。</li> </ul>

## S3 REST APIのサポートが更新されました

リリース。	コメント
11.8	S3処理の名前がで使用されている名前に更新されました。 "Amazon Web Services ( AWS ) ドキュメント：「Amazon Simple Storage Service API Reference」。
11.7	<ul style="list-style-type: none"> <li>を追加しました "クイックリファレンス：サポートされるS3 API要求"。</li> <li>S3オブジェクトロックでのガバナンスマードの使用のサポートが追加されました。</li> <li>StorageGRID固有のサポートが追加されました x-ntap-sg-cgr-replication-status GET Object要求とHEAD Object要求の応答ヘッダー。このヘッダーは、グリッド間レプリケーションのオブジェクトのレプリケーションステータスを示します。</li> <li>SelectObjectContent要求でParquetオブジェクトがサポートされるようになりました。</li> </ul>
11.6	<ul style="list-style-type: none"> <li>の使用のサポートが追加されました partNumber GET Object要求とHEAD Object要求のRequestパラメータ。</li> <li>S3 オブジェクトロックのデフォルト保持モードとデフォルトの保持期間がバケットレベルでサポートされるようになりました。</li> <li>のサポートが追加されました s3:object-lock-remaining-retention-days オブジェクトに許可される保持期間の範囲を設定するためのPolicy Conditionキー。</li> <li>単一のPUT Object処理のmaximum_recommended_sizeを5GiB (5、368、709、120バイト) に変更しました。5GB より大きいオブジェクトがある場合は、マルチパートアップロードを使用してください。</li> </ul>
11.5.	<ul style="list-style-type: none"> <li>バケットの暗号化の管理のサポートが追加されました。</li> <li>S3 オブジェクトのロックと廃止された従来の準拠要求のサポートを追加しました。</li> <li>バージョン管理されたバケットでの DELETE Multiple Objects の使用のサポートが追加されました。</li> <li>。 Content-MD5 要求ヘッダーが正しくサポートされるようになりました。</li> </ul>

リリース。	コメント
11.4	<ul style="list-style-type: none"> <li>DELETE Bucket tagging、GET Bucket tagging、PUT Bucket tagging のサポートが追加されました。コスト割り当てタグはサポートされていません。</li> <li>StorageGRID 11.4 で作成されたバケットでは、オブジェクトキー名がパフォーマンスのベストプラクティスに適合するように制限する必要はなくなりました。</li> <li>バケット通知のサポートが追加されました s3:ObjectRestore:Post イベントタイプ。</li> <li>マルチパートの AWS サイズの上限が適用されるようになりました。マルチパートアップロードの各パートのサイズは 5MiB から 5GiB の間にします必要があります。最後の部分は 5MiB より小さくすることができます。</li> <li>TLS 1.3 のサポートが追加されました</li> </ul>
11.3	<ul style="list-style-type: none"> <li>ユーザ指定のキーによるオブジェクトデータのサーバ側暗号化（SSE-C）がサポートされるようになりました。</li> <li>DELETE Bucket lifecycle、GET Bucket lifecycle、PUT Bucket lifecycle の各処理（Expiration アクションのみ）がサポートされるようになりました x-amz-expiration 応答ヘッダー。</li> <li>PUT Object、PUT Object - Copy、Multipart Upload が更新されて、取り込み時に同期配置を使用する ILM ルールの影響を受けるようになりました。</li> <li>TLS 1.1 暗号はサポートされなくなりました。</li> </ul>
11.2.	<p>クラウドストレージプールで POST Object restore を使用できるようになりました。グループポリシーとバケットポリシーの ARN、ポリシー条件キー、およびポリシー変数で AWS 構文を使用できるようになりました。StorageGRID 構文を使用する既存のグループポリシーとバケットポリシーは引き続きサポートされます。</p> <ul style="list-style-type: none"> <li>注：カスタム StorageGRID 機能で使用される ARN やその他の構成 JSON / XML での使用に変更はありませんでした。</li> </ul>
11.1.	Cross-Origin Resource Sharing (CORS)、グリッドノードへの S3 クライアント接続での HTTP、バケットでの準拠設定のサポートが追加されました。
11.0	バケットでのプラットフォームサービス（CloudMirror レプリケーション、通知、および Elasticsearch 検索統合）の設定がサポートされるようになりました。また、バケットに対するオブジェクトタギングの場所の制約と「available」の整合性がサポートされるようになりました。
10.4	ILM スキャンのバージョン管理、エンドポイントドメインの名前ページの更新、ポリシーの条件と変数、ポリシーの例、および PutOverwriteObject 権限の変更のサポートが追加されました。
10.3	バージョン管理のサポートが追加されました。

リリース。	コメント
10.2	グループとバケットのアクセスポリシー、およびマルチパートコピー（Upload Part-Copy）のサポートが追加されました。
10.1	マルチパートアップロード、仮想ホスト形式の要求、および v4 認証のサポートが追加されました。
10.0	StorageGRID システムで S3 REST API のサポートが初めて導入されました。現在サポートされているバージョンの _Simple Storage Service API Reference_is 2006-03-01。

## クイックリファレンス：サポートされる**S3 API**要求

このページでは、StorageGRID がAmazon Simple Storage Service (S3) APIをどのようにサポートしているかをまとめます。

このページには、StorageGRID でサポートされるS3処理のみが含まれています。



各処理のAWSドキュメントを参照するには、見出しのリンクを選択します。

### 一般的なURIクエリパラメータと要求ヘッダー

特に記載がない限り、次の一般的なURIクエリパラメータがサポートされます。

- versionId (オブジェクトの処理に必要な場合)

特に記載がない限り、次の一般的な要求ヘッダーがサポートされます。

- Authorization
- Connection
- Content-Length
- Content-MD5
- Content-Type
- Date
- Expect
- Host
- x-amz-date

### 関連情報

- "[S3 REST APIの実装の詳細](#)"
- "[Amazon Simple Storage Service API Reference : Common Request Headers](#)"

## "AbortMultipartUpload の略"

### URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求に加えて、次の追加のURIクエリパラメータを指定します。

- uploadId

本文を要求します

なし

### StorageGRID のドキュメント

#### "マルチパートアップロードの処理"

## "CompleteMultipartUpload"

### URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求に加えて、次の追加のURIクエリパラメータを指定します。

- uploadId

本文XMLタグを要求します

StorageGRID は、次の要求本文XMLタグをサポートしています。

- CompleteMultipartUpload
- ETag
- Part
- PartNumber

### StorageGRID のドキュメント

#### "CompleteMultipartUpload"

## "CopyObject"

### URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求に加え、次のヘッダーが追加されています。

- x-amz-copy-source
- x-amz-copy-source-if-match
- x-amz-copy-source-if-modified-since
- x-amz-copy-source-if-none-match
- x-amz-copy-source-if-unmodified-since
- x-amz-copy-source-server-side-encryption-customer-algorithm

- x-amz-copy-source-server-side-encryption-customer-key
- x-amz-copy-source-server-side-encryption-customer-key-MD5
- x-amz-metadata-directive
- x-amz-object-lock-legal-hold
- x-amz-object-lock-mode
- x-amz-object-lock-retain-until-date
- x-amz-server-side-encryption
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-storage-class
- x-amz-tagging
- x-amz-tagging-directive
- x-amz-meta-<metadata-name>

本文を要求します

なし

#### **StorageGRID のドキュメント**

"[CopyObject](#)"

#### **"CreateBucketを選択します"**

##### **URIクエリパラメータと要求ヘッダー**

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求に加え、次のヘッダーが追加されています。

- x-amz-bucket-object-lock-enabled

本文を要求します

StorageGRID は、実装時にAmazon S3 REST APIで定義されたすべての要求本文パラメータをサポートします。

#### **StorageGRID のドキュメント**

"[バケットの処理](#)"

#### **"CreateMultipartUpload を実行します"**

##### **URIクエリパラメータと要求ヘッダー**

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求に加え、次のヘッダーが追加されています。

- Cache-Control

- Content-Disposition
- Content-Encoding
- Content-Language
- Expires
- x-amz-server-side-encryption
- x-amz-storage-class
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-tagging
- x-amz-object-lock-mode
- x-amz-object-lock-retain-until-date
- x-amz-object-lock-legal-hold
- x-amz-meta-<metadata-name>

本文を要求します

なし

#### **StorageGRID のドキュメント**

["CreateMultipartUpload を実行します"](#)

#### ["DeleteBucketの場合"](#)

##### **URI** クエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

#### **StorageGRID のドキュメント**

["バケットの処理"](#)

#### ["DeleteBucketCors"](#)

##### **URI** クエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

なし

#### **StorageGRID のドキュメント**

["バケットの処理"](#)

## "DeleteBucketEncryption"

**URI** クエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

なし

**StorageGRID** のドキュメント

["バケットの処理"](#)

## "DeleteBucketLifecycle"

**URI** クエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

なし

**StorageGRID** のドキュメント

- ["バケットの処理"](#)
- ["S3 ライフサイクル設定を作成する"](#)

## "DeleteBucketPolicy のようになります"

**URI** クエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

なし

**StorageGRID** のドキュメント

["バケットの処理"](#)

## "DeleteBucketReplication"

**URI** クエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

なし

**StorageGRID** のドキュメント

["バケットの処理"](#)

## "DeleteBucketTagging"

**URI** クエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

なし

**StorageGRID のドキュメント**

["バケットの処理"](#)

## "deleteObject"

**URI** クエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求と追加の要求ヘッダー：

- x-amz-bypass-governance-retention

本文を要求します

なし

**StorageGRID のドキュメント**

["オブジェクトの処理"](#)

## "オブジェクトを削除します"

**URI** クエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求と追加の要求ヘッダー：

- x-amz-bypass-governance-retention

本文を要求します

StorageGRID は、実装時にAmazon S3 REST APIで定義されたすべての要求本文パラメータをサポートします。

**StorageGRID のドキュメント**

["オブジェクトの処理"](#)

## "DeleteObjectTagging の場合"

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

なし

**StorageGRID のドキュメント**

["オブジェクトの処理"](#)

## "GetBucketAcl"

**URI** クエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

なし

**StorageGRID** のドキュメント

["バケットの処理"](#)

## "GetBucketCors"

**URI** クエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

なし

**StorageGRID** のドキュメント

["バケットの処理"](#)

## "GetBucketEncryptionの略"

**URI** クエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

なし

**StorageGRID** のドキュメント

["バケットの処理"](#)

## "GetBucketLifecycleConfiguration"

**URI** クエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

なし

**StorageGRID** のドキュメント

- ["バケットの処理"](#)
- ["S3 ライフサイクル設定を作成する"](#)

## "GetBucketLocation"

**URI** クエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

なし

**StorageGRID** のドキュメント

["バケットの処理"](#)

## "GetBucketNotificationConfiguration を参照してください"

**URI** クエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

なし

**StorageGRID** のドキュメント

["バケットの処理"](#)

## "GetBucketPolicy のようになります"

**URI** クエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

なし

**StorageGRID** のドキュメント

["バケットの処理"](#)

## "GetBucketReplication の略"

**URI** クエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

なし

**StorageGRID** のドキュメント

["バケットの処理"](#)

## "GetBucketTagging"

**URI** クエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

なし

### StorageGRID のドキュメント

#### "バケットの処理"

##### "GetBucketVersioningの各ノードの設定"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

なし

### StorageGRID のドキュメント

#### "バケットの処理"

##### "GetObject"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求に加えて、次の追加のURIクエリパラメータを使用します。

- partNumber
- response-cache-control
- response-content-disposition
- response-content-encoding
- response-content-language
- response-content-type
- response-expires

追加の要求ヘッダーは次のとおりです。

- Range
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- If-Match
- If-Modified-Since
- If-None-Match
- If-Unmodified-Since

本文を要求します

なし

#### StorageGRID のドキュメント

"GetObject"

##### "GetObjectAcl"

###### URI クエリ パラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

なし

#### StorageGRID のドキュメント

"オブジェクトの処理"

##### "GetObjectLegalHold"

###### URI クエリ パラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

なし

#### StorageGRID のドキュメント

"S3 REST API を使用して S3 オブジェクトロックを設定します"

##### "GetObjectLockConfiguration の略"

###### URI クエリ パラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

なし

#### StorageGRID のドキュメント

"S3 REST API を使用して S3 オブジェクトロックを設定します"

##### "GetObjectRetention の略"

###### URI クエリ パラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

なし

#### StorageGRID のドキュメント

"S3 REST API を使用して S3 オブジェクトロックを設定します"

## "GetObjectTagging の 2 つの機能を"

**URI** クエリ パラメータと要求 ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

なし

**StorageGRID** のドキュメント

["オブジェクトの処理"](#)

**"ヘッド バケット"**

**URI** クエリ パラメータと要求 ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

なし

**StorageGRID** のドキュメント

["バケットの処理"](#)

**"HeadObject (ヘッド オブジェクト)"**

**URI** クエリ パラメータと要求 ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求に加え、次のヘッダーが追加されています。

- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `If-Match`
- `If-Modified-Since`
- `If-None-Match`
- `If-Unmodified-Since`
- `Range`

本文を要求します

なし

**StorageGRID** のドキュメント

["HeadObject \(ヘッド オブジェクト\)"](#)

## "ListBuckets"

**URI** クエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

なし

**StorageGRID** のドキュメント

["サービス> ListBucketsの操作"](#)

## "ListMultipartUploads"

**URI** クエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求に加え、次の追加パラメータが含まれます。

- delimiter
- encoding-type
- key-marker
- max-uploads
- prefix
- upload-id-marker

本文を要求します

なし

**StorageGRID** のドキュメント

["ListMultipartUploads"](#)

## "ListObjects"

**URI** クエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求に加え、次の追加パラメータが含まれます。

- delimiter
- encoding-type
- marker
- max-keys
- prefix

本文を要求します

なし

## **StorageGRID のドキュメント**

### "バケットの処理"

#### **"ListObjectsV2"**

##### **URIクエリパラメータと要求ヘッダー**

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求に加え、次の追加パラメータが含まれます。

- continuation-token
- delimiter
- encoding-type
- fetch-owner
- max-keys
- prefix
- start-after

本文を要求します

なし

## **StorageGRID のドキュメント**

### "バケットの処理"

#### **"ListObjectVersions"**

##### **URIクエリパラメータと要求ヘッダー**

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求に加え、次の追加パラメータが含まれます。

- delimiter
- encoding-type
- key-marker
- max-keys
- prefix
- version-id-marker

本文を要求します

なし

## **StorageGRID のドキュメント**

### "バケットの処理"

## ["ListParts"](#)

**URI** クエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求に加え、次の追加パラメータが含まれます。

- max-parts
- part-number-marker
- uploadId

本文を要求します

なし

**StorageGRID** のドキュメント

## ["ListMultipartUploads"](#)

### ["PutBucketCorsの略"](#)

**URI** クエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

StorageGRID は、実装時にAmazon S3 REST APIで定義されたすべての要求本文パラメータをサポートします。

**StorageGRID** のドキュメント

## ["バケットの処理"](#)

### ["PutBucketEncryptionの略"](#)

**URI** クエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文**XML**タグを要求します

StorageGRID は、次の要求本文**XML**タグをサポートしています。

- ApplyServerSideEncryptionByDefault
- Rule
- ServerSideEncryptionConfiguration
- SSEAlgorithm

**StorageGRID** のドキュメント

## ["バケットの処理"](#)

## "PutBucketLifecycleConfigurationの略"

### URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

### 本文XMLタグを要求します

StorageGRID は、次の要求本文XMLタグをサポートしています。

- And
- Days
- Expiration
- ExpiredObjectDeleteMarker
- Filter
- ID
- Key
- LifecycleConfiguration
- NewerNoncurrentVersions
- NoncurrentDays
- NoncurrentVersionExpiration
- Prefix
- Rule
- Status
- Tag
- Value

### StorageGRID のドキュメント

- "バケットの処理"
- "S3 ライフサイクル設定を作成する"

## "PutBucketNotificationConfigurationの略"

### URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

### 本文XMLタグを要求します

StorageGRID は、次の要求本文XMLタグをサポートしています。

- Event
- Filter
- FilterRule

- Id
- Name
- NotificationConfiguration
- Prefix
- S3Key
- Suffix
- Topic
- TopicConfiguration
- Value

## StorageGRID のドキュメント

### "バケットの処理"

#### "PutBucketPolicyのように指定します"

##### URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

サポートされているJSON本文フィールドの詳細については、を参照してください  
"バケットとグループのアクセスポリシーを使用"。

#### "PutBucketReplicationの略"

##### URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文XMLタグを要求します

- Bucket
- Destination
- Prefix
- ReplicationConfiguration
- Rule
- Status
- StorageClass

## StorageGRID のドキュメント

### "バケットの処理"

## "PutBucketTaggingの略"

**URI** クエリ パラメータと要求 ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

StorageGRID は、実装時に Amazon S3 REST API で定義されたすべての要求本文 パラメータをサポートします。

**StorageGRID のドキュメント**

["バケットの処理"](#)

## "PutBucketVersioningの各ノードの設定"

**URI** クエリ パラメータと要求 ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文 パラメータを要求します

StorageGRID は、次の要求本文 パラメータをサポートしています。

- VersioningConfiguration
- Status

**StorageGRID のドキュメント**

["バケットの処理"](#)

## "PutObject"

**URI** クエリ パラメータと要求 ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求に加え、次のヘッダーが追加されています。

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- x-amz-server-side-encryption
- x-amz-storage-class
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-tagging
- x-amz-object-lock-mode
- x-amz-object-lock-retain-until-date

- `x-amz-object-lock-legal-hold`
- `x-amz-meta-<metadata-name>`

本文を要求します

- オブジェクトのバイナリデータ

**StorageGRID のドキュメント**

["PutObject"](#)

["PutObjectLegalHold"](#)

**URI** クエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

StorageGRID は、実装時にAmazon S3 REST APIで定義されたすべての要求本文パラメータをサポートします。

**StorageGRID のドキュメント**

["S3 REST APIを使用してS3オブジェクトロックを設定します"](#)

["PutObjectLockConfigurationの略"](#)

**URI** クエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

StorageGRID は、実装時にAmazon S3 REST APIで定義されたすべての要求本文パラメータをサポートします。

**StorageGRID のドキュメント**

["S3 REST APIを使用してS3オブジェクトロックを設定します"](#)

["PutObjectRetentionの略"](#)

**URI** クエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求とこの追加ヘッダー：

- `x-amz-bypass-governance-retention`

本文を要求します

StorageGRID は、実装時にAmazon S3 REST APIで定義されたすべての要求本文パラメータをサポートします。

**StorageGRID のドキュメント**

["S3 REST APIを使用してS3オブジェクトロックを設定します"](#)

## "PutObjectTagging の 2 つのグループが"

**URI** クエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

StorageGRID は、実装時に Amazon S3 REST API で定義されたすべての要求本文パラメータをサポートします。

**StorageGRID のドキュメント**

["オブジェクトの処理"](#)

## "RestoreObject"

**URI** クエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

サポートされている本文フィールドの詳細については、を参照してください。 ["RestoreObject"](#)。

## "SelectObjectContent の順に選択します"

**URI** クエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

サポートされている本文フィールドの詳細については、以下を参照してください。

- ["S3 Select を使用する"](#)
- ["SelectObjectContent の順に選択します"](#)

## "UploadPart のアップロード"

**URI** クエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求に加えて、次の追加の **URI** クエリパラメータを使用します。

- partNumber
- uploadId

追加の要求ヘッダーは次のとおりです。

- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5

本文を要求します

- 部品のバイナリデータ

## StorageGRID のドキュメント

"UploadPart のアップロード"

"[UploadPartCopyをクリックします](#)"

URI エリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求に加えて、次の追加の URI エリパラメータを使用します。

- partNumber
- uploadId

追加の要求ヘッダーは次のとおりです。

- x-amz-copy-source
- x-amz-copy-source-if-match
- x-amz-copy-source-if-modified-since
- x-amz-copy-source-if-none-match
- x-amz-copy-source-if-unmodified-since
- x-amz-copy-source-range
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-copy-source-server-side-encryption-customer-algorithm
- x-amz-copy-source-server-side-encryption-customer-key
- x-amz-copy-source-server-side-encryption-customer-key-MD5

本文を要求します

なし

## StorageGRID のドキュメント

"[UploadPartCopyをクリックします](#)"

## S3 REST API 設定のテスト

Amazon Web Services コマンドラインインターフェイス (AWS CLI) を使用して、システムへの接続をテストし、オブジェクトの読み取りと書き込みが可能であることを確認できます。

作業を開始する前に

- AWS CLI をからダウンロードしてインストールしておきます ["aws.amazon.com/cli"](https://aws.amazon.com/cli)。

- 必要に応じて、"ロードバランサエンドポイントを作成しました"。それ以外の場合は、接続するストレージノードのIPアドレスと使用するポート番号がわかっている必要があります。を参照してください "クライアント接続用のIPアドレスとポート"。
- これで完了です "S3テナントアカウントが作成されました"。
- テナントにサインインし、"アクセスキーの作成"。

これらの手順の詳細については、を参照してください "クライアント接続を設定します"。

## 手順

- StorageGRID システムで作成したアカウントを使用するようにAWS CLIを設定します。
  - コンフィギュレーションモードを開始します。 aws configure
  - 作成したアカウントのアクセスキーIDを入力します。
  - 作成したアカウントのシークレットアクセスキーを入力します。
  - 使用するデフォルトのリージョンを入力します。例：us-east-1。
  - 使用するデフォルトの出力形式を入力するか、\* Enter \* キーを押して JSON を選択します。
- バケットを作成する。

この例では、IPアドレス10.96.101.17とポート10443を使用するようにロードバランサエンドポイントが設定されていると想定しています。

```
aws s3api --endpoint-url https://10.96.101.17:10443
--no-verify-ssl create-bucket --bucket testbucket
```

バケットの作成が完了すると、次の例のようにバケットの場所が返されます。

```
"Location": "/testbucket"
```

- オブジェクトをアップロードします。

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
put-object --bucket testbucket --key s3.pdf --body C:\s3-
test\upload\s3.pdf
```

オブジェクトのアップロードが完了すると、オブジェクトデータのハッシュである Etag が返されます。

- バケットの内容をリストして、オブジェクトがアップロードされたことを確認します。

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
list-objects --bucket testbucket
```

## 5. オブジェクトを削除します。

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl  
delete-object --bucket testbucket --key s3.pdf
```

## 6. バケットを削除します。

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl  
delete-bucket --bucket testbucket
```

## StorageGRID での S3 REST API の実装

競合するクライアント要求です

同じキーに書き込む 2 つのクライアントなど、競合するクライアント要求は、「latest-wins」ベースで解決されます。

「latest-wins」評価は、S3 クライアントが処理を開始するタイミングではなく、StorageGRID システムが特定の要求を完了したタイミングで行われます。

整合性の値

整合性では、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でのオブジェクトの整合性のバランスが維持されます。アプリケーションの必要に応じて整合性を変更できます。

StorageGRID では、デフォルトで、新しく作成したオブジェクトのリードアフターライト整合性が保証されます。正常に完了した PUT に続く GET では、新しく書き込まれたデータを読み取ることができます。既存のオブジェクトの上書き、メタデータの更新、および削除の整合性レベルは、結果整合性です。上書きは通常、数秒から数分で反映されますが、最大で 15 日かかることがあります。

別の整合性でオブジェクトの処理を実行する場合は、次の操作を実行できます。

- 整合性の指定 [各バケット](#)。
- 整合性の指定 [各API処理](#)。
- 次のいずれかのタスクを実行して、グリッド全体のデフォルトの整合性を変更します。
  - Grid Manager で、[設定] >\* > [ストレージ設定] > [デフォルトの整合性]\* の順に選択します。
  - 。



グリッド全体の整合性に対する変更は、設定の変更後に作成されたバケットにのみ適用されます。変更の詳細を確認するには、次の場所にある監査ログを参照してください。  
`/var/local/log (* consistencyLevel *を検索)`。

## 整合性の値

整合性は、StorageGRIDがオブジェクトの追跡に使用するメタデータがノード間でどのように分散されるかに影響し、その結果、クライアント要求に対するオブジェクトの可用性にも影響します。

バケットまたはAPI処理の整合性は、次のいずれかの値に設定できます。

- \* all \* : すべてのノードがすぐにデータを受信しないと、要求は失敗します。
- \* strong-global \* : すべてのサイトのすべてのクライアント要求について、リードアフターライト整合性が保証されます。
- \*strong-site \* : サイト内のすべてのクライアント要求に対してリードアフターライト整合性が保証されます。
- \* Read-after-new-write \* : (デフォルト) 新規オブジェクトにはリードアフターライト整合性を提供し、オブジェクトの更新には結果整合性を提供します。高可用性が確保され、データ保護が保証されます。ほとんどの場合に推奨されます。
- \* available \* : 新しいオブジェクトとオブジェクトの更新の両方について、結果整合性を提供します。S3 バケットの場合は、必要な場合にのみ使用します（読み取り頻度の低いログ値を含むバケットや、存在しないキーに対するHEAD処理やGET処理など）。S3 FabricPool バケットではサポートされません。

### 「Read-after-new-write」整合性と「available」整合性を使用

HEAD処理またはGET処理で「Read-after-new-write」整合性が使用されている場合、StorageGRIDは次のように複数の手順で検索を実行します。

- まず、低い整合性レベルを使用してオブジェクトを検索します。
- そのルックアップが失敗すると、次の整合性値でルックアップが繰り返され、strong-globalの動作と同等の整合性が得られるようになります。

HEAD処理またはGET処理で「Read-after-new-write」整合性が使用されているが、オブジェクトが存在しない場合、オブジェクト検索の整合性は常にstrong-globalの動作と同じになります。この整合性のためには、オブジェクトメタデータのコピーが各サイトで複数ある必要があるため、同じサイトで使用できないストレージノードが複数ある場合に「500 Internal Server Error」が大量に発生する可能性があります。

Amazon S3と同様の整合性の保証が必要ないかぎり、整合性を「available」に設定することで、HEAD処理とGET処理でのこれらのエラーを回避できます。HEAD処理またはGET処理で「available」整合性が使用されている場合、StorageGRIDでは結果整合性のみが提供されます。整合性が向上しても失敗した処理が再試行されることはないため、オブジェクトメタデータのコピーが複数ある必要はありません。

### [api-operation-consistency-control]] API処理の整合性を指定します。

個々のAPI処理に対して整合性を設定するには、処理でサポートされている整合性の値を要求ヘッダーで指定する必要があります。この例では、GetObject処理の整合性を「strong-site」に設定しています。

```
GET /bucket/object HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Consistency-Control: strong-site
```



PutObject処理とGetObject処理では、同じ整合性を使用する必要があります。

#### バケットの整合性を指定する

バケットの整合性を設定するには、StorageGRID "PUT Bucket consistency" リクエスト。または "バケットの整合性を変更する" Tenant Managerから削除します。

バケットに整合性を設定する場合は、次の点に注意してください。

- ・バケットに整合性を設定することで、バケット内のオブジェクトまたはバケット設定に対して実行されるS3処理に使用する整合性が決まります。バケット自体に対する処理には影響しません。
- ・個々のAPI処理の整合性がバケットの整合性よりも優先されます。
- ・通常、バケットではデフォルト整合性の「Read-after-new-write」を使用する必要があります。要求が正しく動作しない場合は、可能であればアプリケーションクライアントの動作を変更します。または、API要求ごとに整合性を指定するようにクライアントを設定します。バケットレベルの整合性は最後の手段として設定してください。

#### 整合性とILMルールの相互作用によるデータ保護への影響

選択した整合性とILMルールは、どちらもオブジェクトの保護方法に影響します。これらの設定は対話的に操作できます。

たとえば、オブジェクトの格納時に使用される整合性はオブジェクトメタデータの初期配置に影響し、ILMルールで選択された取り込み動作はオブジェクトコピーの初期配置に影響します。StorageGRIDでは、クライアント要求に対応するためにオブジェクトのメタデータとそのデータの両方にアクセスする必要があるため、整合性と取り込み動作で同じ保護レベルを選択すると、初期データ保護が向上し、システム応答の予測性が向上します。

次のようにになります "取り込みオプション" ILMルールで使用できます。

#### デュアルコミット

StorageGRIDはオブジェクトの中間コピーをただちに作成し、クライアントに成功を返します。可能な場合は、ILMルールで指定されたコピーが作成されます。

#### strict

クライアントに成功が返される前に、ILMルールで指定されたすべてのコピーが作成されている必要があります。

#### 中間（Balanced）

StorageGRIDは、取り込み時にILMルールで指定されたすべてのコピーの作成を試みます。作成できない場合は中間コピーが作成され、クライアントに成功が返されます。可能な場合は、ILMルールで指定されたコピーが作成されます。

#### 整合性とILMルールの相互作用の例

2サイトのグリッドで次のILMルールと整合性が設定されているとします。

- ・ \* ILM ルール \* : ローカルサイトとリモートサイトに 1 つずつ、2 つのオブジェクトコピーを作成します。取り込み動作は Strict を使用します。
- ・ \* consistency \* : strong-global (オブジェクトメタデータがすべてのサイトに即座に分散されます)。

クライアントがオブジェクトをグリッドに格納すると、StorageGRIDは両方のオブジェクトをコピーし、両方のサイトにメタデータを分散してからクライアントに成功を返します。

オブジェクトは、取り込みが成功したことを示すメッセージが表示された時点で損失から完全に保護されます。たとえば、取り込み直後にローカルサイトが失われた場合、オブジェクトデータとオブジェクトメタデータの両方のコピーがリモートサイトに残っています。オブジェクトを完全に読み出し可能にしている。

同じILMルールでstrong-site整合性を使用した場合、オブジェクトデータがリモートサイトにレプリケートされたあと、オブジェクトメタデータが分散される前にクライアントに成功メッセージが返されることがあります。この場合、オブジェクトメタデータの保護レベルがオブジェクトデータの保護レベルと一致しません。取り込み直後にローカルサイトが失われると、オブジェクトメタデータが失われます。オブジェクトを取得できません。

整合性ルールとILMルールの関係は複雑になる可能性があります。サポートが必要な場合は、NetAppにお問い合わせください。

### オブジェクトのバージョン管理

各オブジェクトの複数のバージョンを保持する場合は、バケットのバージョン管理状態を設定できます。バケットのバージョン管理を有効にすると、オブジェクトが誤って削除されないように保護したり、以前のバージョンのオブジェクトを読み出してリストアしたりできます。

StorageGRIDシステムでは、バージョン管理のほとんどの機能をサポートしていますが、いくつかの制限事項があります。StorageGRIDでは、オブジェクトごとに最大1,000個のバージョンをサポートしています。

オブジェクトのバージョン管理は、StorageGRIDの情報ライフサイクル管理(ILM)またはS3バケットのライフサイクル設定と組み合わせることができます。バージョン管理はバケットごとに明示的に有効にする必要があります。バケットでバージョン管理を有効にすると、バケットに追加される各オブジェクトにバージョンIDが割り当てられ、このIDがStorageGRIDシステムによって生成されます。

MFA（多要素認証）Deleteの使用はサポートされていません。



バージョン管理は、StorageGRIDバージョン10.3以降で作成されたバケットでのみ有効にすることができます。

### ILMとバージョン管理

ILMポリシーはオブジェクトの各バージョンに適用されます。ILMのスキャン処理では、すべてのオブジェクトが継続的にスキャンされ、現在のILMポリシーに照らして再評価されます。ILMポリシーに対する変更は、それまでに取り込まれたすべてのオブジェクトに適用されます。バージョン管理が有効になっている場合は、それまでに取り込まれたバージョンも対象にILMのスキャン処理により、過去に取り込まれたオブジェクトに変更後の新しいILMの内容が適用さ

バージョン管理が有効なバケット内のS3オブジェクトについては、バージョン管理のサポートにより、参照時間に「noncurrent time」を使用するILMルールを作成できます（質問、「Apply this rule to older object versions only？」に対して\* Yes \*を選択します）。イン["ILMルール作成ウィザードのステップ1"](#)。オブジェクトが更新されると、それまでのバージョンはnoncurrentになります。「noncurrent time」フィルタを使用すると、以前のバージョンのオブジェクトによるストレージへの影響を軽減するポリシーを作成できます。



マルチパートアップロード処理を使用してオブジェクトの新しいバージョンをアップロードすると、オブジェクトの元のバージョンの noncurrent の時間には、マルチパートアップロードの完了時ではなく、新しいバージョンのマルチパートアップロードが作成された時点が反映されます。ただし、オリジナルバージョンの最新でない時間は、現行バージョンの時間よりも数時間～数日早い場合があります。

#### 関連情報

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

#### S3 REST APIを使用してS3オブジェクトロックを設定します

StorageGRID システムでS3オブジェクトロックのグローバル設定が有効になっている場合は、S3オブジェクトロックを有効にしてバケットを作成できます。デフォルトの保持設定はバケットごとに指定することも、オブジェクトバージョンごとに指定することもできます。

##### バケットでS3オブジェクトロックを有効にする方法

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、各バケットの作成時に S3 オブジェクトのロックを必要に応じて有効にすることができます。

S3オブジェクトロックは永続的な設定で、バケットの作成時にのみ有効にできます。バケットの作成後にS3 オブジェクトロックを追加または無効にすることはできません。

バケットでS3オブジェクトロックを有効にするには、次のいずれかの方法を使用します。

- ・ Tenant Manager を使用してバケットを作成します。を参照してください ["S3 バケットを作成する"](#)。
- ・ CreateBucket要求を使用してバケットを作成します。 x-amz-bucket-object-lock-enabled 要求ヘッダー。を参照してください ["バケットの処理"](#)。

S3オブジェクトロックにはバケットのバージョン管理が必要です。バージョン管理はバケットの作成時に自動的に有効になります。バケットのバージョン管理を一時停止することはできません。を参照してください ["オブジェクトのバージョン管理"](#)。

##### バケットのデフォルトの保持設定

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、必要に応じてバケットのデフォルトの保持を有効にし、デフォルトの保持モードとデフォルトの保持期間を指定できます。

##### デフォルトの保持モード

- ・ コンプライアンスマードの場合：
  - retain-until-dateに達するまで、オブジェクトを削除できません。
  - オブジェクトのretain-until-dateは増やすことはできますが、減らすことはできません。
  - オブジェクトのretain-until-dateは、その日付に達するまで削除できません。
- ・ ガバナンスマードの場合：

- 使用するユーザ s3:BypassGovernanceRetention 権限はを使用できます x-amz-bypass-governance-retention: true 保持設定をバイパスする要求ヘッダー。
- これらのユーザは、retain-until-dateに達する前にオブジェクトバージョンを削除できます。
- これらのユーザは、オブジェクトのretain-until-dateを増減、または削除できます。

## デフォルトの保持期間

各バケットのデフォルトの保持期間は、年または日数で指定できます。

### バケットのデフォルトの保持期間を設定する方法

バケットのデフォルトの保持期間を設定するには、次のいずれかの方法を使用します。

- Tenant Managerからバケット設定を管理します。を参照してください "[S3 バケットを作成します。](#)" および "[S3オブジェクトロックのデフォルトの保持期間の更新](#)"。
- 問題デフォルトのモードとデフォルトの日数または年数を指定するための、バケットに対する PutObjectLockConfiguration 要求。

## PutObjectLockConfigurationの略

PutObjectLockConfiguration 要求を使用すると、S3オブジェクトロックが有効になっているバケットに対して、デフォルトの保持モードとデフォルトの保持期間を設定および変更できます。以前に設定したデフォルトの保持設定を削除することもできます。

新しいオブジェクトバージョンがバケットに取り込まれると、にデフォルトの保持モードが適用されます x-amz-object-lock-mode および x-amz-object-lock-retain-until-date は指定されていません。デフォルトの保持期間は、の retain-until-date の計算に使用されます x-amz-object-lock-retain-until-date が指定されていません。

オブジェクトバージョンの取り込み後にデフォルトの保持期間が変更された場合、オブジェクトバージョンの retain-until はそのまま残り、新しいデフォルトの保持期間を使用して再計算されることはありません。

を用意しておく必要があります s3:PutBucketObjectLockConfiguration この処理を完了するための権限 (rootアカウント)。

- Content-MD5 PUT 要求に要求ヘッダーを指定する必要があります。

## 要求例

この例では、バケットで S3オブジェクトロックを有効にし、デフォルトの保持モードを準拠に設定し、デフォルトの保持期間を 6 年に設定しています。

```

PUT /bucket?object-lock HTTP/1.1
Accept-Encoding: identity
Content-Length: 308
Host: host
Content-MD5: request header
User-Agent: s3sign/1.0.0 requests/2.24.0 python/3.8.2
X-Amz-Date: date
X-Amz-Content-SHA256: authorization-string
Authorization: authorization-string

<ObjectLockConfiguration>
  <ObjectLockEnabled>Enabled</ObjectLockEnabled>
  <Rule>
    <DefaultRetention>
      <Mode>COMPLIANCE</Mode>
      <Years>6</Years>
    </DefaultRetention>
  </Rule>
</ObjectLockConfiguration>

```

#### バケットのデフォルトの保持期間を確認する方法

バケットでS3オブジェクトロックが有効になっているかどうかを確認し、デフォルトの保持モードと保持期間を確認するには、次のいずれかの方法を使用します。

- Tenant Managerでバケットを表示します。を参照してください "[S3バケットを表示します](#)"。
- 問題GetObjectLockConfiguration要求。

#### GetObjectLockConfigurationの略

GetObjectLockConfiguration要求を使用すると、S3 Object Lockがバケットで有効になっているかどうかを確認できます。有効になっている場合は、バケットにデフォルトの保持モードと保持期間が設定されているかどうかを確認できます。

新しいオブジェクトバージョンがバケットに取り込まれると、にデフォルトの保持モードが適用されます *x-amz-object-lock-mode* が指定されていません。デフォルトの保持期間は、の*retain-until-date*の計算に使用されます *x-amz-object-lock-retain-until-date* が指定されていません。

を用意しておく必要があります *s3:GetBucketObjectLockConfiguration* この処理を完了するための権限 (rootアカウント) 。

#### 要求例

```
GET /bucket?object-lock HTTP/1.1
Host: host
Accept-Encoding: identity
User-Agent: aws-cli/1.18.106 Python/3.8.2 Linux/4.4.0-18362-Microsoft
botocore/1.17.29
x-amz-date: date
x-amz-content-sha256: authorization-string
Authorization: authorization-string
```

## 応答例

```
HTTP/1.1 200 OK
x-amz-id-2:
iVmcB70XXJRkRH1Fivq1151/T24gRfpwpuZrEG11Bb9ImOMAAe98oxSpX1knabA0LTvBYJpSIX
k=
x-amz-request-id: B34E94CACB2CEF6D
Date: Fri, 04 Sep 2020 22:47:09 GMT
Transfer-Encoding: chunked
Server: AmazonS3

<?xml version="1.0" encoding="UTF-8"?>
<ObjectLockConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
    <ObjectLockEnabled>Enabled</ObjectLockEnabled>
    <Rule>
        <DefaultRetention>
            <Mode>COMPLIANCE</Mode>
            <Years>6</Years>
        </DefaultRetention>
    </Rule>
</ObjectLockConfiguration>
```

## オブジェクトの保持設定を指定する方法

S3オブジェクトロックが有効なバケットには、S3オブジェクトロックの保持設定の有無に関係なく、オブジェクトを組み合わせて含めることができます。

オブジェクトレベルの保持設定は、S3 REST APIを使用して指定します。オブジェクトの保持設定は、バケットのデフォルトの保持設定よりも優先されます。

オブジェクトごとに次の設定を指定できます。

- 保持モード：コンプライアンスまたはガバナンスのいずれか。
- \* retain-until-date \* : StorageGRID がオブジェクトバージョンを保持する期間を指定する日付。
  - コンプライアンスマードでは、retain-until-dateが将来の日付の場合、オブジェクトを読み出すことはできますが、変更や削除はできません。retain-until-dateは増やすことができますが、この日付を減ら

すことも削除することもできません。

- ガバナンスモードでは、特別な権限を持つユーザーは、retain-until-date設定をバイパスできます。保持期間が経過する前にオブジェクトバージョンを削除できます。また、retain-until-dateを増減したり、削除したりすることもできます。
- \* 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。

オブジェクトのリーガルホールド設定は、保持モードやretain-until-dateとは関係ありません。オブジェクトの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、そのバージョンは誰も削除できません。

バケットにオブジェクトバージョンを追加するときにS3オブジェクトロックの設定を指定するには、問題Aを実行します "PutObject"、 "CopyObject" または "CreateMultipartUpload を実行します" リクエスト。

次のものを使用できます。

- `x-amz-object-lock-mode` コンプライアンスまたはガバナンス（大文字と小文字が区別されます）。



を指定する場合 x-amz-object-lock-mode、も指定する必要があります x-amz-object-lock-retain-until-date。

- x-amz-object-lock-retain-until-date

◦ retain-until-dateの値は、の形式で指定する必要があります 2020-08-10T21:46:00Z。秒数には分数を指定できますが、保持される 10 進数は 3 衔（ミリ秒単位）だけです。その他のISO 8601形式は使用できません。

◦ retain-until-date は将来の日付にする必要があります。

- x-amz-object-lock-legal-hold

リーガルホールドがオン（大文字と小文字が区別される）の場合、オブジェクトはリーガルホールドの対象になります。リーガルホールドがオフの場合、リーガルホールドは適用されません。それ以外の値を指定すると、400 Bad Request（InvalidArgument）エラーが発生します。

次のいずれかの要求ヘッダーを使用する場合は、次の制限事項に注意してください。

- Content-MD5 要求ヘッダーがある場合は必須です x-amz-object-lock-\* 要求ヘッダーがPutObject要求に存在します。Content-MD5 CopyObjectまたはCreateMultipartUploadには必要ありません。
- バケットでS3オブジェクトロックが有効になっていない場合は、とをクリックします x-amz-object-lock-\* 要求ヘッダーが存在し、400 Bad Request（InvalidRequest）エラーが返されます。
- PutObject要求は、次の使用をサポートします。x-amz-storage-class: REDUCED\_REDUNDANCY AWSの動作に合わせて調整できます。ただし、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が取り込まれると、StorageGRID は常にデュアルコミットの取り込みを実行します。
- 後続のGETまたはHeadObjectバージョンの応答には、ヘッダーが含まれます。x-amz-object-lock-mode、x-amz-object-lock-retain-until-date`および `x-amz-object-lock-legal-hold` が設定されている場合、および要求の送信者が正しいかどうか `s3:Get` 権限：

を使用できます `s3:object-lock-remaining-retention-days` オブジェクトの最小保持期間と最大保持期間を制限するポリシー条件キー。

#### オブジェクトの保持設定を更新する方法

既存のオブジェクトのバージョンのリーガルホールドや保持の設定を更新する必要がある場合、次のオブジェクトサブリソース処理を実行できます。

- `PutObjectLegalHold`

新しいリーガルホールドの値が `on` の場合、オブジェクトはリーガルホールドの対象になります。リーガルホールドの値がオフの場合、リーガルホールドは解除されます。

- `PutObjectRetention`

- `mode` 値は `compliance` または `governance` です（大文字と小文字が区別されます）。
- `retain-until-date` の値は、の形式で指定する必要があります `2020-08-10T21:46:00Z`。秒数には分数を指定できますが、保持される 10 進数は 3 衔（ミリ秒単位）だけです。その他の ISO 8601 形式は使用できません。
- オブジェクトバージョンに既存の `retain-until` がある場合は、オブジェクトバージョンを増やすことはできますが、増やすことはできません。新しい値は将来の必要があります。

#### ガバナンスモードの使用方法

を持つユーザ `s3:BypassGovernanceRetention` 権限は、ガバナンスモードを使用するオブジェクトのアクティブな保持設定をバイパスできます。DELETE 处理または `PutObjectRetention` 处理には、`x-amz-bypass-governance-retention:true` 要求ヘッダー。これらのユーザは、次の追加操作を実行できます。

- 保持期間が経過する前にオブジェクトバージョンを削除するには、`DeleteObject` 处理または `DeleteObjects` 处理を実行します。

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。リーガルホールドをオフにする必要があります。

- オブジェクトの保持期間が経過する前にオブジェクトバージョンのモードをガバナンスからコンプライアンスに変更する `PutObjectRetention` 处理を実行します。

コンプライアンスモードからガバナンスモードに変更することはできません。

- `PutObjectRetention` 处理を実行して、オブジェクトバージョンの保持期間を増減、または削除します。

#### 関連情報

- "[S3 オブジェクトロックでオブジェクトを管理します](#)"
- "[S3 オブジェクトロックを使用してオブジェクトを保持します](#)"
- "[Amazon Simple Storage Service User Guide : Using S3 Object Lock](#)"

#### S3 ライフサイクル設定を作成する

S3 ライフサイクル設定を作成して、特定のオブジェクトが StorageGRID システムから削除されるタイミングを制御できます。

このセクションの簡単な例では、S3 ライフサイクル設定で特定のオブジェクトが特定の S3 バケットから削除（期限切れ）されるタイミングを制御する方法を示します。このセクションの例は、説明のみを目的としています。S3 ライフサイクル設定の作成の詳細については、を参照してください ["Amazon Simple Storage Serviceユーザガイド：オブジェクトのライフサイクル管理"](#)。StorageGRID では、Expiration アクションのみがサポートされ、移行アクションはサポートされません。

ライフサイクル構成とは

ライフサイクル設定は、特定の S3 バケット内のオブジェクトに適用される一連のルールです。各ルールは、影響を受けるオブジェクトと、それらのオブジェクトの有効期限（特定の日付または日数後）を指定します。

StorageGRID では、1 つのライフサイクル設定で最大 1,000 個のライフサイクルルールがサポートされます。各ルールには、次の XML 要素を含めることができます。

- **Expiration** : 指定した日付に達した場合、またはオブジェクトが取り込まれたときから指定した日数に達した場合にオブジェクトを削除します。
- **NoncurrentVersionExpiration** : 指定した日数に達したオブジェクトを削除します。これは、オブジェクトが最新でなくなったときからです。
- フィルタ（プレフィックス、タグ）
- ステータス
- ID

各オブジェクトは、S3 バケットライフサイクルまたは ILM ポリシーの保持設定に従います。S3 バケットライフサイクルが設定されている場合は、バケットライフサイクルフィルタに一致するオブジェクトの ILM ポリシーがライフサイクル有効期限のアクションで上書きされます。バケットライフサイクルフィルタに一致しないオブジェクトには、ILM ポリシーの保持設定が使用されます。オブジェクトがバケットライフサイクルフィルタに一致し、有効期限の操作が明示的に指定されていない場合、ILM ポリシーの保持設定は使用されず、オブジェクトのバージョンが無期限に保持されることが暗黙的に示されます。を参照してください ["S3 バケットライフサイクルと ILM ポリシーの優先度の例"](#)。

そのため、ILM ルールの配置手順がオブジェクトに引き続き適用されても、オブジェクトがグリッドから削除されることがあります。あるいは、ILM 配置手順がすべて終了したあとも、オブジェクトがグリッドに保持される場合があります。詳細については、を参照してください ["オブジェクトのライフサイクル全体にわたる ILM の動作"](#)。



バケットライフサイクル設定は S3 オブジェクトロックが有効になっているバケットで使用できますが、従来の準拠バケットではバケットライフサイクル設定がサポートされません。

StorageGRID では、次のバケット処理を使用してライフサイクル設定を管理できます。

- DeleteBucketLifecycle
- GetBucketLifecycleConfiguration
- PutBucketLifecycleConfiguration の略

ライフサイクル構成を作成します

ライフサイクル設定を作成するための最初の手順として、1 つ以上のルールを含む JSON ファイルを作成します。たとえば、この JSON ファイルには次の 3 つのルールが含まれています。

1. ルール1は、プレフィックスに一致するオブジェクトにのみ適用されます category1/とそれにはがあり

ます `key2` の値 `tag2`。 `Expiration` パラメータは、フィルタに一致するオブジェクトの有効期限が2020年8月22日の午前0時に切れるように指定します。

2. ルール2は、プレフィックスに一致するオブジェクトにのみ適用されます。`category2%`。  
`Expiration` パラメータは、フィルタに一致するオブジェクトの取り込みから100日後に期限切れにするを指定します。



日数を指定するルールは、オブジェクトが取り込まれた時点を基準とした相対的なルールです。現在の日付が取り込み日と日数を超えている場合は、ライフサイクル設定の適用後すぐに一部のオブジェクトがバケットから削除される可能性があります。

3. ルール3は、プレフィックスに一致するオブジェクトにのみ適用されます。`category3%`。  
`Expiration` パラメータは、最新でないバージョンの一致オブジェクトが最新でなくなったあと50日で期限切れになるように指定します。

```
{  
    "Rules": [  
        {  
            "ID": "rule1",  
            "Filter": {  
                "And": {  
                    "Prefix": "category1/",  
                    "Tags": [  
                        {  
                            "Key": "key2",  
                            "Value": "tag2"  
                        }  
                    ]  
                }  
            },  
            "Expiration": {  
                "Date": "2020-08-22T00:00:00Z"  
            },  
            "Status": "Enabled"  
        },  
        {  
            "ID": "rule2",  
            "Filter": {  
                "Prefix": "category2/"  
            },  
            "Expiration": {  
                "Days": 100  
            },  
            "Status": "Enabled"  
        },  
        {  
            "ID": "rule3",  
            "Filter": {  
                "Prefix": "category3/"  
            },  
            "NoncurrentVersionExpiration": {  
                "NoncurrentDays": 50  
            },  
            "Status": "Enabled"  
        }  
    ]  
}
```

バケットにライフサイクル設定を適用

ライフサイクル設定ファイルを作成したら、PutBucketLifecycleConfiguration要求を発行してバケットに適用します。

次の要求は、サンプルファイル内のライフサイクル設定を、という名前のバケット内のオブジェクトに適用します testbucket。

```
aws s3api --endpoint-url <StorageGRID endpoint> put-bucket-lifecycle-configuration  
--bucket testbucket --lifecycle-configuration file://bktjson.json
```

ライフサイクル設定がバケットに正常に適用されたことを確認するには、GetBucketLifecycleConfiguration要求を問題します。例：

```
aws s3api --endpoint-url <StorageGRID endpoint> get-bucket-lifecycle-configuration  
--bucket testbucket
```

成功応答には、適用したライフサイクル設定が表示されます。

バケットライフサイクルの有効期限が環境 オブジェクトであることを検証します

PutObject、HeadObject、またはGetObjectのいずれか環境の要求を発行するときに、ライフサイクル設定の有効期限ルールが特定のオブジェクトであるかどうかを確認できます。ルールが適用される場合、応答にはが含まれます `Expiration` オブジェクトの有効期限と一致する有効期限を示すパラメータ。



バケットライフサイクルはILMよりも優先されるため、を参照してください `expiry-date` 表示されているのは、オブジェクトが削除される実際の日付です。詳細については、を参照してください "[オブジェクト保持期間の決定方法](#)"。

たとえば、このPutObject要求は2020年6月22日に発行され、オブジェクトを testbucket バケット。

```
aws s3api --endpoint-url <StorageGRID endpoint> put-object  
--bucket testbucket --key obj2test2 --body bktjson.json
```

成功の応答は、オブジェクトの有効期限が 100 日（2020 年 10 月 1 日）に切れ、ライフサイクル設定のルール 2 に一致したことを示します。

```
{  
    *"Expiration": "expiry-date=\\"Thu, 01 Oct 2020 09:07:49 GMT\\\"", rule-id=\\"rule2\\\"",  
    "ETag": "\\"9762f8a803bc34f5340579d4446076f7\\""  
}
```

たとえば、次のHeadObject要求を使用して、testbucketバケット内の同じオブジェクトのメタデータを取得しました。

```
aws s3api --endpoint-url <StorageGRID endpoint> head-object  
--bucket testbucket --key obj2test2
```

成功の応答にはオブジェクトのメタデータが含まれ、オブジェクトが 100 日で期限切れになり、ルール 2 に一致したことが示されます。

```
{  
    "AcceptRanges": "bytes",  
    * "Expiration": "expiry-date=\\"Thu, 01 Oct 2020 09:07:48 GMT\\\"", rule-  
      id=\\"rule2\\\"",  
    "LastModified": "2020-06-23T09:07:48+00:00",  
    "ContentLength": 921,  
    "ETag": "\\"9762f8a803bc34f5340579d4446076f7\\\""  
    "ContentType": "binary/octet-stream",  
    "Metadata": {}  
}
```



バージョン管理が有効なバケットの場合は、`x-amz-expiration` 応答ヘッダーは、現在のバージョンのオブジェクトにのみ適用されます。

## S3 REST API を実装する際の推奨事項

StorageGRID で使用するために S3 REST API を実装する場合は、次の推奨事項を考慮してください。

### 存在しないオブジェクトに対する HEAD の推奨事項

オブジェクトが実際に存在するとは思わないパスにオブジェクトが存在するかどうかをアプリケーションが定期的にチェックする場合は、「available」を使用する必要があります。 [「一貫性」](#)。たとえば、アプリケーションがPUTを実行する前に特定の場所に移動する場合は、「available」整合性を使用する必要があります。

そうしないと、同じサイトに複数のストレージノードが使用できない場合やリモートサイトに到達できない場合に、HEAD処理でオブジェクトが見つからないと「500 Internal Server Error」が大量に返されることがあります。

バケットごとに「available」整合性を設定するには、["PUT Bucket consistency"](#) または、個々のAPI処理の要求ヘッダーで整合性を指定できます。

### オブジェクトキーの推奨事項

オブジェクトキーについて、バケットが最初に作成された日時に基づいて次の推奨事項に従ってください。

### StorageGRID 11.4以前で作成されたバケット

- ・オブジェクトキーの最初の4文字にランダムな値を使用しないでください。これは、AWSが以前に推奨していたキープレフィックスの推奨事項とは異なります。代わりに、など、ランダムではなく一意ではないプレフィックスを使用します `image`。
- ・以前のAWSの推奨事項に従ってキープレフィックスにランダムな一意の文字を使用する場合は、オブジェクトキーの前にディレクトリ名を付けます。つまり、次の形式を使用します。

`mybucket/mydir/f8e3-image3132.jpg`

次の形式は使用しないでください。

`mybucket/f8e3-image3132.jpg`

### StorageGRID 11.4以降で作成されたバケット

パフォーマンスのベストプラクティスに合わせてオブジェクトキー名を制限する必要はありません。ほとんどの場合、オブジェクトキー名の最初の4文字にはランダムな値を使用できます。

ただし、短期間ですべてのオブジェクトを継続的に削除するS3ワークロードは例外です。このユースケースのパフォーマンスへの影響を最小限に抑えるには、キー名の先頭部分を数千個のオブジェクトごとに、日付などの値を変更します。たとえば、S3クライアントが1秒あたり2,000個のオブジェクトを書き込むのが一般的で、ILMまたはバケットライフサイクルポリシーで3日後にすべてのオブジェクトが削除されるとします。パフォーマンスへの影響を最小限に抑えるには、次のようなパターンを使用してキーに名前を付けます。

`/mybucket/mydir/yyyymmddhhmmss-random_UUID.jpg`

#### 「範囲読み取り」に関する推奨事項

状況に応じて "格納オブジェクトを圧縮するグローバルオプション" が有効になっている場合は、S3クライアントアプリケーションで返されるバイト数の範囲を指定するGetObject処理を実行しないでください。これらの「範囲読み取り」処理は効率的ではありません。StorageGRIDでは、要求されたバイトにアクセスするためにオブジェクトの圧縮を実質的に解除する必要があるためです。非常に大きなオブジェクトから小さい範囲のバイト数を要求するGetObject処理は特に非効率的です。たとえば、50GBの圧縮オブジェクトから10MBの範囲を読み取る処理は非効率的です。

圧縮オブジェクトから範囲を読み取ると、クライアント要求がタイムアウトする可能性があります。

○ オブジェクトを圧縮する必要があり、クライアントアプリケーションが範囲読み取りを使用する必要がある場合は、アプリケーションの読み取りタイムアウトを増やしてください。

## Amazon S3 REST APIのサポート

### S3 REST APIの実装の詳細

StorageGRIDシステムはSimple Storage Service API（APIバージョン2006-03-01）を実装しており、ほとんどの処理をサポートしていますが、いくつかの制限事項があります。S3 REST APIクライアントアプリケーションを統合するときは、実装の詳細を理解しておく必要があります。

StorageGRIDシステムでは、仮想ホスト形式の要求とパス形式の要求の両方がサポートされます。

## 日付の処理

S3 REST API の StorageGRID 実装では、有効な HTTP の日付形式のみをサポートしています。

StorageGRID システムでは、日付の値を設定できるすべてのヘッダーで、有効な HTTP の日付形式のみがサポートされます。日付の時刻の部分は、Greenwich Mean Time (GMT ; グリニッジ標準時) の形式で指定するか、タイムゾーンのオフセットなし (+0000 を指定) の Universal Coordinated Time (UTC ; 協定世界時) の形式で指定できます。を指定する場合は `x-amz-date` 要求のヘッダー。Date要求ヘッダーで指定された値を上書きします。AWS署名バージョン4を使用している場合は、を参照してください `x-amz-date` 日付ヘッダーがサポートされていないため、署名済み要求にヘッダーが含まれている必要があります。

## 代表的な要求ヘッダー

StorageGRID システムは、で定義されている共通の要求ヘッダーをサポートします ["Amazon Simple Storage Service API Reference : Common Request Headers"](#)<sup>1</sup> つの例外を除いて。

要求ヘッダー	実装
承認	AWS 署名バージョン 2 は完全にサポートされます  AWS 署名バージョン 4 は次の例外を除いてサポートされます。 <ul style="list-style-type: none"><li>要求の本文の SHA256 の値は計算されません。ユーザが送信した値は、値の場合と同様に、検証なしで受け入れられます <code>UNSIGNED-PAYLOAD</code> は用に提供されていた <code>x-amz-content-sha256</code> ヘッダー。</li></ul>
<code>x-amz-security-token</code> を指定します	実装されていませんを返します <code>xNotImplemented</code> 。

## 共通の応答ヘッダー

StorageGRID システムでは、以下の例外を除き、[\\_Simple Storage Service API Reference\\_](#) で定義されている共通の応答ヘッダーがすべてサポートされます。

応答ヘッダー	実装
<code>x-amz-id-2</code>	使用されません

## 要求を認証します

StorageGRID システムでは、S3 API を使用したオブジェクトへのアクセスについて、認証アクセスと匿名アクセスの両方をサポートしています。

S3 API では、S3 API 要求の認証で署名バージョン 2 と署名バージョン 4 がサポートされます。

認証された要求は、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署名する必要があります。

StorageGRID システムでは、HTTP という2つの認証方式がサポートされています `Authorization` ヘッダーを使用し、クエリパラメータを使用する。

## HTTP Authorization ヘッダーを使用します

HTTP Authorization ヘッダーは、バケットポリシーで許可された匿名の要求を除き、すべてのS3 API処理で使用されます。Authorization ヘッダーには、要求の認証に必要なすべての署名情報が含まれています。

## クエリパラメータを使用します

クエリパラメータを使用すると、URLに認証情報を追加できます。これは署名付き URL と呼ばれ、特定のリソースへの一時的なアクセスを許可する場合に使用できます。指定されたURLを持つユーザは、リソースにアクセスする際にシークレットアクセスキーを知っている必要はありません。これにより、リソースへのサービスパーティの制限付きアクセスを提供できます。

## サービスの処理

StorageGRID システムでは、サービスに対して次の処理をサポートしています。

操作	実装
ListBuckets (以前の名前はGET Service)	Amazon S3 REST API のすべての動作が実装されています。予告なく変更される場合があります。
GET Storage Usage の略	StorageGRID "GET Storage Usage の略" [Request]には、アカウントで使用されているストレージの合計容量と、アカウントに関連付けられている各バケットについての情報が表示されます。これは、パス/とカスタムクエリパラメータを使用したサービスに対する処理です (?x-ntap-sg-usage)が追加されました
オプション /	クライアントアプリケーションは問題を実行できます OPTIONS / S3 認証クレデンシャルを入力せずにストレージノード上のS3ポートに要求し、ストレージノードが使用可能かどうかを確認します。この要求は監視に使用できるほか、外部のロードバランサがストレージノードの停止を特定する目的でも使用できます。

## バケットの処理

StorageGRID システムでは、S3 テナントアカウントあたり最大 1,000 個のバケットがサポートされます。

バケット名にはAWS US Standardリージョンの制限事項が適用されますが、S3仮想ホスト形式の要求をサポートするためにDNSの命名規則にも制限する必要があります。

詳細については、次を参照してください。

- ・ "Amazon Simple Storage Serviceユーザガイド：『Bucket Restrictions and Limitations』"
- ・ "S3エンドポイントのドメイン名を設定"

ListObjects (GET Bucket) 処理とListObjectVersions (GET Bucketオブジェクトバージョン) 処理でStorageGRIDがサポートされるようになりました。"整合性の値"。

最終アクセス時間の更新が個々のバケットで有効になっているか無効になっているかを確認することができます。を参照してください

"[GET Bucket last access time の場合](#)"。

次の表に、StorageGRID での S3 REST API バケット処理の実装方法を示します。これらの処理を実行するには、アカウントに必要なアクセスキーが付与されている必要があります。

操作	実装
CreateBucketを選択します	<p>新しいバケットを作成します。バケットを作成すると、そのバケットの所有者になります。</p> <ul style="list-style-type: none"><li>バケット名は次のルールを満たす必要があります。<ul style="list-style-type: none"><li>StorageGRID システム全体で（テナントアカウント内だけではなく）一意である必要があります。</li><li>DNS に準拠している必要があります。</li><li>3 文字以上 63 文字以下にする必要があります。</li><li>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。</li><li>テキスト形式の IP アドレスのようにはできません。</li><li>仮想ホスト形式の要求でピリオドを使用しないでください。ピリオドを使用すると、サーバワイルドカード証明書の検証で原因の問題が発生します。</li></ul></li><li>デフォルトでは、バケットはに作成されます us-east-1 リージョン。ただし、を使用することはできます LocationConstraint 別のリージョンを指定するように要求本文内の要求要素。を使用する場合 LocationConstraint 要素：Grid Managerまたはグリッド管理APIを使用して定義されているリージョンの正確な名前を指定する必要があります。使用するリージョン名がわからない場合は、システム管理者にお問い合わせください。</li></ul> <p>注：CreateBucket要求がStorageGRIDで定義されていないリージョンを使用すると、エラーが発生します。</p> <ul style="list-style-type: none"><li>を含めることができます x-amz-bucket-object-lock-enabled 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要求ヘッダー。を参照してください "<a href="#">S3 REST APIを使用してS3オブジェクトロックを設定します</a>"。</li></ul> <p>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。バケットの作成後にS3オブジェクトロックを追加または無効にすることはできません。S3 オブジェクトロックにはバケットのバージョン管理が必要です。バケットの作成時に自動的に有効になります。</p>
DeleteBucketの場合	バケットを削除します。

操作	実装
DeleteBucketCors	バケットのCORS設定を削除します。
DeleteBucketEncryption	バケットからデフォルトの暗号化を削除します。既存の暗号化オブジェクトは暗号化されたままでですが、バケットに追加された新しいオブジェクトは暗号化されません。
DeleteBucketLifecycle	バケットからライフサイクル設定を削除します。を参照してください " <a href="#">S3 ライフサイクル設定を作成する</a> "。
DeleteBucketPolicy のようになります	バケットに関連付けられているポリシーを削除します。
DeleteBucketReplication	バケットに関連付けられているレプリケーション設定を削除します。
DeleteBucketTagging	を使用します <code>tagging</code> サブリソース：バケットからすべてのタグを削除します。  注意：このバケットにデフォルト以外のILMポリシータグが設定されている場合、 <code>NTAP-SG-ILM-BUCKET-TAG</code> 値が割り当てられたバケットタグ。DeleteBucketTagging要求がある場合は問題を実行しない <code>NTAP-SG-ILM-BUCKET-TAG</code> バケットタグ。代わりに、問題でPutBucketTagging要求を実行し、 <code>NTAP-SG-ILM-BUCKET-TAG</code> 他のすべてのタグをバケットから削除するには、タグとその割り当て値を使用します。を変更または削除しないでください。 <code>NTAP-SG-ILM-BUCKET-TAG</code> バケットタグ。
GetBucketAcl	バケットの所有者にバケットへのフルアクセスがあることを示す応答が返され、所有者のID、表示名、および権限が表示されます。
GetBucketCors	を返します。 <code>cors</code> バケットの設定。
GetBucketEncryption の略	バケットのデフォルトの暗号化設定を返します。
GetBucketLifecycleConfiguration (以前のGET Bucket lifecycle)	バケットのライフサイクル設定を返します。を参照してください " <a href="#">S3 ライフサイクル設定を作成する</a> "。
GetBucketLocation	を使用して設定されたリージョンを返します。 <code>LocationConstraint</code> CreateBucket要求の要素。バケットのリージョンがの場合 <code>'us-east-1'</code> を指定すると、リージョンに対して空の文字列が返されます。

操作	実装
GetBucketNotificationConfigurationを参照してください  (以前の名前のGET Bucket notification)	バケットに関連付けられている通知設定を返します。
GetBucketPolicyのようになります	バケットに関連付けられているポリシーを返します。
GetBucketReplicationの略	バケットに関連付けられているレプリケーション設定を返します。
GetBucketTagging	を使用します <code>tagging</code> サブリソース：バケットのすべてのタグを返す  注意：このバケットにデフォルト以外のILMポリシータグが設定されている場合、NTAP-SG-ILM-BUCKET-TAG 値が割り当てられたバケットタグ。このタグを変更または削除しないでください。
GetBucketVersioningの各ノードの設定	この実装ではを使用します <code>versioning</code> サブリソース：バケットのバージョン管理の状態を返します。 <ul style="list-style-type: none"> <li>• <code>blank</code>：バージョン管理が一度も有効になっていない（バケットは「バージョン管理されていない」）</li> <li>• <code>有效</code>：バージョン管理が有効になっています</li> <li>• <code>中断</code>：バージョン管理は以前有効になっていて、中断されています</li> </ul>
GetObjectLockConfigurationの略	バケットのデフォルトの保持モードとデフォルトの保持期間（設定されている場合）を返します。  を参照してください " <a href="#">S3 REST APIを使用してS3オブジェクトロックを設定します</a> "。
ヘッドバケット	バケットが存在し、そのバケットにアクセスする権限があるかどうかを確認します。  この処理から返される情報は次の <ul style="list-style-type: none"> <li>• <code>x-ntap-sg-bucket-id</code>：バケットのUUID（UUID形式）。</li> <li>• <code>x-ntap-sg-trace-id</code>：関連付けられた要求の一意のトレースID。</li> </ul>

操作	実装
listObjectsおよびListObjectsV2  (以前の名前はGET Bucket)	<p>バケット内のオブジェクトの一部またはすべて（最大1,000）を返します。を使用してオブジェクトを取り込んだ場合でも、オブジェクトのストレージクラスには2つの値が設定されます <code>REDUCED_REDUNDANCY</code> ストレージクラスのオプション：</p> <ul style="list-style-type: none"> <li>`STANDARD`を指定します。このオブジェクトは、ストレージノードで構成されるストレージプールに格納されます。</li> <li>`GLACIER`を指定します。このオブジェクトは、クラウドストレージプールで指定された外部バケットに移動されています。</li> </ul> <p>バケットに同じプレフィックスを持つ削除済みキーが多数含まれている場合、応答に一部のキーが含まれることがあります <code>CommonPrefixes</code> 鍵が入っていないものです</p>
ListObjectVersions  (以前のGET Bucket Object versions)	バケットに対する読み取りアクセスが許可されている場合、 <code>versions</code> サブリソースには、バケット内のオブジェクトのすべてのバージョンのメタデータが表示されます。
PutBucketCorsの略	クロスオリジン要求を処理できるように、バケットのCORS設定を設定します。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 <code>images</code> グラフィックを保存します。のCORS設定を指定します <code>images</code> 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 <code>http://www.example.com</code> 。
PutBucketEncryptionの略	<p>既存のバケットのデフォルトの暗号化状態を設定します。バケットレベルの暗号化が有効な場合は、バケットに追加されたすべての新しいオブジェクトが暗号化されます。StorageGRIDでは、StorageGRIDで管理されるキーによるサーバ側の暗号化がサポートされます。サーバ側の暗号化設定ルールを指定する場合は、を設定します <code>SSEAlgorithm</code> パラメータの値 <code>AES256</code>、を使用しないでください <code>KMSMasterKeyID</code> パラメータ</p> <p>バケットのデフォルトの暗号化設定は、オブジェクトのアップロード要求すでに暗号化が指定されている場合（要求にが含まれている場合）は無視されます <code>x-amz-server-side-encryption-*</code> 要求ヘッダー）。</p>

操作	実装
<p>PutBucketLifecycleConfiguration の略 (以前のPUT Bucket lifecycle)</p>	<p>バケットの新しいライフサイクル設定を作成するか、既存のライフサイクル設定と置き換えます。StorageGRID では、1つのライフサイクル設定で最大1,000個のライフサイクルルールがサポートされます。各ルールには、次の XML 要素を含めることができます。</p> <ul style="list-style-type: none"> <li>• 有効期限（日数、日付、ExpiredObjectDeleteMarker）</li> <li>• NoncurrentVersionExpiration（NewerNoncurrentVersions、NoncurrentDays）</li> <li>• フィルタ（プレフィックス、タグ）</li> <li>• ステータス</li> <li>• ID</li> </ul> <p>StorageGRID では、次のアクションはサポートされません。</p> <ul style="list-style-type: none"> <li>• AbortIncompleteMultipartUpload の略</li> <li>• 移行</li> </ul> <p>を参照してください <a href="#">"S3 ライフサイクル設定を作成する"</a>。バケットライフサイクルのExpirationアクションとILMの配置手順の相互作用については、を参照してください <a href="#">"オブジェクトのライフサイクル全体にわたる ILM の動作"</a>。</p> <ul style="list-style-type: none"> <li>• 注：バケットライフサイクル設定は S3 オブジェクトロックが有効なバケットで使用できますが、従来の準拠バケットではバケットライフサイクル設定がサポートされません。</li> </ul>

操作	実装
PutBucketNotificationConfigurationの略 (以前の名前のPUT Bucket通知)	<p>要求の本文に含まれる通知設定XMLを使用してバケットの通知を設定します。実装に関する次の詳細事項に注意してください。</p> <ul style="list-style-type: none"> <li>StorageGRIDでは、Amazon Simple Notification Service (Amazon SNS) またはKafkaトピックがデスティネーションとしてサポートされます。Simple Queue Service (SQS) またはAmazon Lambdaエンドポイントはサポートされていません。</li> <li>通知のデスティネーションは、StorageGRID エンドポイントの URN として指定する必要があります。エンドポイントは、Tenant Manager またはテナント管理 API を使用して作成できます。</li> </ul> <p>通知設定が機能するためには、エンドポイントが存在している必要があります。エンドポイントが存在しない場合は、400 Bad Request エラーがコードとともに返されます InvalidArgument。</p> <ul style="list-style-type: none"> <li>次のイベントタイプに対して通知を設定することはできません。これらのイベントタイプは * サポートされていません。 <ul style="list-style-type: none"> <li>s3:ReducedRedundancyLostObject</li> <li>s3:ObjectRestore:Completed</li> </ul> </li> <li>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、次のリストに示すように、一部のキーが含まれず、他のキーには特定の値が使用されます。 <ul style="list-style-type: none"> <li>* eventSource*</li> <li>sgws:s3</li> <li>* awsRegion *</li> <li>含まれません</li> <li>* x-amz-id-2 *</li> <li>含まれません</li> <li>* arn *</li> <li>urn:sgws:s3:::bucket_name</li> </ul> </li> </ul>
PutBucketPolicyのように指定します	バケットに関連付けられたポリシーを設定します。を参照してください "バケットとグループのアクセスポリシーを使用"。

操作	実装
PutBucketReplicationの略	<p>構成 "StorageGRID CloudMirrorレプリケーション"（バケット用）。要求の本文に含まれるレプリケーション設定XMLを使用します。CloudMirror レプリケーションについては、実装に関する次の詳細事項に注意してください。</p> <ul style="list-style-type: none"> <li>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、を参照してください "<a href="#">Amazon Simple Storage Serviceユーザガイド：レプリケーションの設定</a>"。</li> <li>バケットレプリケーションは、バージョン管理されているバケットでもバージョン管理されていないバケットでも設定でき</li> <li>レプリケーション設定 XML の各ルールで異なるデスティネーションバケットを指定できます。1つのソースバケッ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。</li> <li>デスティネーションバケットは、テナントマネージャまたはテナント管理 API で指定された StorageGRID エンドポイントの URN として指定する必要があります。を参照してください "<a href="#">CloudMirror レプリケーションを設定します</a>"。</li> </ul> <p>レプリケーション設定が機能するためには、エンドポイントが存在している必要があります。エンドポイントが存在しない場合は、として要求が失敗します 400 Bad Request。エラーメッセージ：Unable to save the replication policy. The specified endpoint URN does not exist: URN.</p> <ul style="list-style-type: none"> <li>を指定する必要はありません Role 設定XMLを使用します。この値は StorageGRID では使用されず、送信されても無視されます。</li> <li>設定XMLでストレージクラスを省略した場合、StorageGRID ではを使用します STANDARD デフォルトのストレージクラス。</li> <li>ソースバケットからオブジェクトを削除する場合、またはソースバケット自身を削除する場合、クロスリージョンレプリケーションは次のように動作します。 <ul style="list-style-type: none"> <li>レプリケートの前にオブジェクトまたはバケットを削除した場合、オブジェクトまたはバケットはレプリケートされず、通知も送信されません。</li> <li>レプリケートのあとにオブジェクトまたはバケットを削除すると、StorageGRID は、V1 のクロスリージョンレプリケーションに対する Amazon S3 の通常の削除動作に従います。</li> </ul> </li> </ul>

操作	実装
PutBucketTaggingの略	<p>を使用します <code>tagging</code> サブリソース：バケットの一連のタグを追加または更新できます。バケットタグを追加する場合は、次の制限事項に注意してください。</p> <ul style="list-style-type: none"> <li>StorageGRID と Amazon S3 はどちらもバケットごとに最大 50 個のタグをサポートします。</li> <li>バケットに関連付けられているタグには、一意のタグキーが必要です。タグキーには Unicode 文字を 128 文字まで使用できます。</li> <li>タグ値には、Unicode 文字を 256 文字以内で指定します。</li> <li>キーと値では大文字と小文字が区別されます。</li> </ul> <p>注意：このバケットにデフォルト以外のILMポリシータグが設定されている場合、NTAP-SG-ILM-BUCKET-TAG 値が割り当てられたバケットタグ。次のことを確認します。NTAP-SG-ILM-BUCKET-TAG バケットタグは、すべてのPutBucketTagging要求で割り当てられた値に含まれます。このタグを変更または削除しないでください。</p> <p>注：この処理を実行すると、バケットにすでに設定されている現在のタグが上書きされます。セットから既存のタグを省略すると、それらのタグはバケットから削除されます。</p>
PutBucketVersioningの各ノードの設定	<p>を使用します <code>versioning</code> サブリソース：既存のバケットのバージョン管理の状態を設定できます。バージョン管理の状態は、次のいずれかの値に設定できます。</p> <ul style="list-style-type: none"> <li>Enabled : バケット内のオブジェクトに対してバージョン管理を有効にします。バケットに追加されるすべてのオブジェクトに、一意のバージョン ID が割り当てられます。</li> <li>Suspended : バケット内のオブジェクトに対してバージョン管理を無効にします。バケットに追加されるすべてのオブジェクトに、バージョンIDが割り当てられます null。</li> </ul>
PutObjectLockConfigurationの略	<p>バケットのデフォルトの保持モードとデフォルトの保持期間を設定または削除します。</p> <p>デフォルトの保持期間を変更した場合、既存のオブジェクトバージョンの <code>retain-until</code> はそのまま残り、新しいデフォルトの保持期間を使用して再計算されることはありません。</p> <p>を参照してください <a href="#">"S3 REST APIを使用してS3オブジェクトロックを設定します"</a> を参照してください。</p>

## オブジェクトの処理

### オブジェクトの処理

このセクションでは、StorageGRID システムでオブジェクトの S3 REST API 処理を実装する方法について説明します。

すべてのオブジェクトの処理に次の条件が適用されます。

- StorageGRID "整合性の値" オブジェクトに対するすべての操作でサポートされます。ただし、次の操作はサポートされません。
  - GetObjectAcl
  - OPTIONS /
  - PutObjectLegalHold
  - PutObjectRetentionの略
  - SelectObjectContent の順に選択します
- 同じキーに書き込む 2 つのクライアントなど、競合するクライアント要求は、「latest-wins」ベースで解決されます。「latest-wins」評価は、S3 クライアントが処理を開始するタイミングではなく、StorageGRID システムが特定の要求を完了したタイミングで行われます。
- StorageGRID バケット内のオブジェクトは、匿名ユーザまたは別のアカウントが作成したオブジェクトも含めて、すべてバケット所有者によって所有されます。
- Swiftを使用してStorageGRID システムに取り込まれたデータオブジェクトにS3を使用してアクセスすることはできません。

次の表に、StorageGRID での S3 REST API オブジェクト処理の実装方法を示します。

操作	実装
deleteObject	<p>多要素認証（MFA）と応答ヘッダー <code>x-amz-mfa</code> はサポートされていません。</p> <p>DeleteObject要求を処理すると、StorageGRIDはすべての格納場所からオブジェクトのすべてのコピーをただちに削除しようとします。成功すると、StorageGRIDはただちにクライアントに応答を返します。30秒以内にすべてのコピーを削除できない場合（場所が一時的に使用できない場合など）、StorageGRIDは削除対象のコピーをキューに登録し、クライアントに成功を通知します。</p> <p><b>バージョン管理</b></p> <p>特定のバージョンを削除するには、バケットの所有者を要求元にしてを使用する必要があります <code>versionId</code> サブリソース：このサブリソースを使用すると、バージョンが完全に削除されます。状況に応じて <code>versionId</code> 削除マーカー、応答ヘッダーに対応します <code>x-amz-delete-marker</code> はに設定されています <code>true</code>。</p> <ul style="list-style-type: none"> <li>• を使用せずにオブジェクトが削除された場合 <code>versionId</code> バージョンが有効になっているバケットのサブリソースが表示されると、削除マーカーが生成されます。。 <code>versionId</code> 削除マーカーの場合は、を使用して戻ります <code>x-amz-version-id</code> 応答ヘッダー、および <code>x-amz-delete-marker</code> 応答ヘッダーがに設定されて返されます <code>true</code>。</li> <li>• を使用せずにオブジェクトが削除された場合 <code>versionId</code> バージョンが一時停止中のバケットについて、既存の「null」バージョンまたは「null」削除マーカーが完全に削除され、新しい「null」削除マーカーが生成されます。。 <code>x-amz-delete-marker</code> 応答ヘッダーがに設定されて返されます <code>true</code>。</li> <li>• 注 * : 特定の場合、1つのオブジェクトに複数の削除マーカーが存在することがあります。</li> </ul> <p>を参照してください "<a href="#">S3 REST APIを使用してS3オブジェクトロックを設定します</a>" ガバナンスマードでオブジェクトバージョンを削除する方法については、を参照してください。</p>
オブジェクトを削除します (以前の名前はDELETE Multiple Objects)	<p>多要素認証（MFA）と応答ヘッダー <code>x-amz-mfa</code> はサポートされていません。</p> <p>同じ要求メッセージで複数のオブジェクトを削除できます。</p> <p>を参照してください "<a href="#">S3 REST APIを使用してS3オブジェクトロックを設定します</a>" ガバナンスマードでオブジェクトバージョンを削除する方法については、を参照してください。</p>

操作	実装
DeleteObjectTagging の場合	<p>を使用します tagging サブリソース：オブジェクトからすべてのタグを削除します。</p> <p>バージョン管理</p> <p>状況に応じて <code>versionId</code> クエリパラメータが要求で指定されていない場合、バージョン管理されたバケット内のオブジェクトの最新バージョンからすべてのタグが削除されます。オブジェクトの現在のバージョンが削除マーカーの場合は、「MethodNotAllowed」ステータスが返され、<code>x-amz-delete-marker</code> 応答ヘッダーをに設定しました <code>true</code>。</p>
GetObject	" <a href="#">GetObject</a> "
GetObjectAcl	アカウントに必要なアクセスクレデンシャルがある場合、オブジェクトの所有者にオブジェクトに対するフルアクセスがあることを示す応答が返され、所有者の ID、表示名、および権限が表示されます。
GetObjectLegalHold	" <a href="#">S3 REST APIを使用してS3オブジェクトロックを設定します</a> "
GetObjectRetentionの略	" <a href="#">S3 REST APIを使用してS3オブジェクトロックを設定します</a> "
GetObjectTagging の 2 つの機能を	<p>を使用します tagging サブリソース：オブジェクトのすべてのタグを返すために使用します。</p> <p>バージョン管理</p> <p>状況に応じて <code>versionId</code> クエリパラメータが要求で指定されていない場合、バージョン管理されたバケット内のオブジェクトの最新バージョンからすべてのタグが返されます。オブジェクトの現在のバージョンが削除マーカーの場合は、「MethodNotAllowed」ステータスが返され、<code>x-amz-delete-marker</code> 応答ヘッダーをに設定しました <code>true</code>。</p>
HeadObject (ヘッドオブジェクト )	" <a href="#">HeadObject (ヘッドオブジェクト)</a> "
RestoreObject	" <a href="#">RestoreObject</a> "
PutObject	" <a href="#">PutObject</a> "
CopyObject (以前の名前はPUT Object - Copy )	" <a href="#">CopyObject</a> "
PutObjectLegalHold	" <a href="#">S3 REST APIを使用してS3オブジェクトロックを設定します</a> "

操作	実装
PutObjectRetentionの略	<a href="#">"S3 REST APIを使用してS3オブジェクトロックを設定します"</a>
PutObjectTagging の 2 つのグループが	<p>を使用します <code>tagging</code> サブリソース：既存のオブジェクトに一連のタグを追加します。</p> <p><b>オブジェクトタグの制限</b></p> <p>タグは、新しいオブジェクトをアップロードするときに追加することも、既存のオブジェクトに追加することもできます。StorageGRID と Amazon S3 はどちらも、オブジェクトごとに最大 10 個のタグをサポートします。オブジェクトに関連付けられたタグには、一意のタグキーが必要です。タグキーには Unicode 文字を 128 文字まで、タグ値には Unicode 文字を 256 文字まで使用できます。キーと値では大文字と小文字が区別されます。</p> <p><b>タグの更新と取り込み動作</b></p> <p>PutObjectTaggingを使用してオブジェクトのタグを更新した場合、StorageGRIDはオブジェクトを再取り込みしません。これは、一致する ILM ルールで指定されている取り込み動作が使用されないことを意味します。更新によって発生したオブジェクト配置の変更是、通常のバックグラウンド ILM プロセスで ILM が再評価されるときに実施されます。</p> <p>つまり、ILMルールの取り込み動作にStrictオプションが使用されている場合、必要なオブジェクト配置を実行できない場合（新たに必要な場所が使用できない場合など）は処理されません。更新されたオブジェクトは、必要な配置を実行可能になるまで現在の配置が維持されます。</p> <p><b>競合の解決</b></p> <p>同じキーに書き込む 2 つのクライアントなど、競合するクライアント要求は、「latest-wins」ベースで解決されます。「latest-wins」評価は、S3 クライアントが処理を開始するタイミングではなく、StorageGRID システムが特定の要求を完了したタイミングで行われます。</p> <p><b>バージョン管理</b></p> <p>状況に応じて <code>versionId</code> クエリパラメータが要求で指定されていません。処理は、バージョン管理されたバケット内のオブジェクトの最新バージョンにタグを追加します。オブジェクトの現在のバージョンが削除マーカーの場合は、「MethodNotAllowed」ステータスが返され、<code>x-amz-delete-marker</code> 応答ヘッダーをに設定しました <code>true</code>。</p>
SelectObjectContent の順に選択します	<a href="#">"SelectObjectContent の順に選択します"</a>

## S3 Select を使用する

StorageGRID は、次の Amazon S3 Select 句、データ型、および演算子をサポートしています "SelectObjectContent コマンド"。



リストされていない項目はサポートされていません。

構文については、を参照してください "SelectObjectContent の順に選択します"。S3 Select の詳細については、を参照してください "S3 Select に関する AWS のドキュメント"。

問題 SelectObjectContent クエリを実行できるのは、S3 Select が有効になっているテナントアカウントのみです。を参照してください "S3 Select を使用する際の考慮事項と要件"。

### 句

- リストを選択します
- FROM 句
- WHERE 句
- Limit 句

### データ型

- ブール値
- 整数
- 文字列
- 浮動小数点
- 10 進数、数値
- タイムスタンプ

### 演算子

#### 論理演算子

- および
- ありません
- または

#### 比較演算子

- <
- >
- ⇐
- >=
- =

- =
- <>
- !=
- 間 ( Between )
- インチ

### パターンマッチング演算子

- いいね
- \_
- %

### 単一の演算子

- は NULL です
- は NULL ではありません

### 数学演算子

- [+]
- -
- \*
- /
- %

StorageGRID はAmazon S3 Selectオペレータの優先順位に従います。

### 集合関数

- 平均 ()
- カウント (\*)
- 最大 ()
- 最小 ()
- 合計 ()

### 条件付き関数

- ケース
- 集合体
- NULLIF

### 変換関数

- CAST (サポートされているデータタイプ用)

## 日付関数

- date\_add
- DATE\_DIFF
- 抽出 ( Extract )
- 文字列まで ( \_STRING )
- 終了タイムスタンプ
- UTCNOW

## 文字列関数

- char\_length、character\_length
- 低い
- サブストリング
- トリム ( Trim )
- 上限

サーバ側の暗号化を使用します

サーバ側の暗号化を使用して、保存中のオブジェクトデータを保護できます。StorageGRID は、オブジェクトを書き込む際にデータを暗号化し、ユーザがオブジェクトにアクセスする際にデータを復号化します。

サーバ側の暗号化を使用する場合は、暗号化キーの管理方法に基づいて、次の 2 つのオプションを同時に選択できます。

- \* SSE ( StorageGRID で管理されるキーによるサーバ側の暗号化) \* : オブジェクトを格納する S3 要求を問題で暗号化すると、StorageGRID は一意のキーでオブジェクトを暗号化します。オブジェクトを読み出す S3 要求を問題で実行すると、StorageGRID は格納されているキーを使用してオブジェクトを復号化します。
- \* SSE-C ( ユーザ指定のキーによるサーバ側の暗号化) \* : オブジェクトを格納する S3 要求を問題で処理するときに、独自の暗号化キーを指定します。オブジェクトを読み出すときは、同じ暗号化キーを要求に指定します。2 つの暗号化キーが一致すると、オブジェクトが復号化されてオブジェクトデータが返されます。

オブジェクトの暗号化処理と復号化処理はすべて StorageGRID で管理されますが、指定する暗号化キーはユーザが管理する必要があります。



指定した暗号化キーが格納されることはありません。暗号化キーを紛失すると、対応するオブジェクトが失われます。



SSE または SSE-C で暗号化されたオブジェクトは、バケットレベルまたはグリッドレベルの暗号化設定が無視されます。

## SSE を使用します

StorageGRID で管理される一意のキーでオブジェクトを暗号化する場合は、次の要求ヘッダーを使用します。

x-amz-server-side-encryption

SSE 要求ヘッダーは、次のオブジェクト処理でサポートされます。

- "[PutObject](#)"
- "[CopyObject](#)"
- "[CreateMultipartUpload を実行します](#)"

## SSE-C を使用します

ユーザが管理する一意のキーでオブジェクトを暗号化する場合は、次の 3 つの要求ヘッダーを使用します。

要求ヘッダー	説明
x-amz-server-side-encryption-customer-algorithm	暗号化アルゴリズムを指定します。ヘッダー値はである必要があります AES256。
x-amz-server-side-encryption-customer-key	オブジェクトの暗号化と復号化に使用する暗号化キーを指定します。キーの値は、Base64 でエンコードされた 256 ビットであることが必要です。
x-amz-server-side-encryption-customer-key-MD5	RFC 1321 に従って暗号化キーの MD5 ダイジェストを指定します。これは、暗号化キーがエラーなしで送信されたことを確認するために使用されます。MD5 ダイジェストの値は、Base64 でエンコードされた 128 ビットであることが必要です。

SSE-C 要求ヘッダーは、次のオブジェクト処理でサポートされます。

- "[GetObject](#)"
- "[HeadObject \(ヘッドオブジェクト\)](#)"
- "[PutObject](#)"
- "[CopyObject](#)"
- "[CreateMultipartUpload を実行します](#)"
- "[UploadPart のアップロード](#)"
- "[UploadPartCopyをクリックします](#)"

ユーザ指定のキーによるサーバ側の暗号化（SSE-C）を使用する場合の考慮事項

SSE-C を使用する場合は、次の考慮事項に注意してください。

- HTTPS を使用する必要があります。



SSE-C を使用すると、http 経由の要求が StorageGRID すべて拒否されますセキュリティ上の理由から、誤って http を使用して送信したキーは漏洩する可能性があります。キーを破棄し、必要に応じてローテーションします。

- 応答内の ETag は、オブジェクトデータの MD5 ではありません。
- 暗号化キーとオブジェクトの対応関係を管理する必要があります。StorageGRID では暗号化キーは格納されません。各オブジェクトに対して指定した暗号化キーを管理する責任はユーザにあります。
- バケットのバージョン管理が有効になっている場合は、オブジェクトのバージョンごとに固有の暗号化キーが必要です。各オブジェクトバージョンで使用される暗号化キーを管理する責任はユーザにあります。
- 暗号化キーはクライアント側で管理するため、キーローテーションなどの追加の防護策もクライアント側で管理する必要があります。



指定した暗号化キーが格納されることはありません。暗号化キーを紛失すると、対応するオブジェクトが失われます。

- バケットにクロスグリッドレプリケーションまたはCloudMirrorレプリケーションが設定されている場合は、SSE-Cオブジェクトを取り込むことはできません。取り込み処理は失敗します。

#### 関連情報

["Amazon S3ユーザガイド：ユーザ指定のキーによるサーバ側の暗号化（SSE-C）の使用"](#)

#### CopyObject

S3 CopyObject要求を使用して、すでにS3に格納されているオブジェクトのコピーを作成できます。CopyObject操作は、GetObjectを実行してからPutObjectを実行する操作と同じです。

#### 競合を解決します

同じキーに書き込む 2 つのクライアントなど、競合するクライアント要求は、「latest-wins」ベースで解決されます。「latest-wins」評価は、S3 クライアントが処理を開始するタイミングではなく、StorageGRID システムが特定の要求を完了したタイミングで行われます。

#### オブジェクトのサイズ

1回のPutObject処理の最大推奨サイズは5GiB（5、368、709、120バイト）です。5GiBを超えるオブジェクトがある場合は、["マルチパートアップロード"](#)代わりに、

1回のPutObject処理のmaximum\_supported\_sizeは5TiB（5、497、558、138、880バイト）です。



StorageGRID 11.6以前からアップグレードした場合、5GiBを超えるオブジェクトをアップロードしようとすると、S3 PUT Object size too largeアラートがトリガーされます。StorageGRID 11.7または11.8を新規にインストールした場合、この場合アラートはトリガーされません。ただし、AWS S3標準に準拠するため、StorageGRIDの今後のリリースでは5GiBを超えるオブジェクトのアップロードはサポートされません。

## ユーザメタデータ内の UTF-8 文字

要求のユーザ定義メタデータのキー名または値に（エスケープされていない）UTF-8 文字が含まれている場合、StorageGRID の動作は定義されていません。

ユーザ定義メタデータのキー名または値に含まれているエスケープされた UTF-8 文字は、StorageGRID で解析も解釈もされません。エスケープされた UTF-8 文字は ASCII 文字として扱われます。

- ユーザ定義メタデータにエスケープされた UTF-8 文字が含まれている場合、要求は正常に実行されます。
- StorageGRID からが返されない `x-amz-missing-meta` キーの名前または値の解釈後の値に印刷不能文字が含まれている場合は、ヘッダー。

## サポートされる要求ヘッダー

次の要求ヘッダーがサポートされています。

- `Content-Type`
- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-if-modified-since`
- `x-amz-meta-`をクリックし、続けてユーザ定義のメタデータを含む名前と値のペアを作成します
- `x-amz-metadata-directive`: デフォルト値はです `COPY` をクリックすると、オブジェクトおよび関連するメタデータをコピーできます。

を指定できます `REPLACE` オブジェクトのコピー時に既存のメタデータを上書きする場合、またはオブジェクトメタデータを更新する場合。

- `x-amz-storage-class`
- `x-amz-tagging-directive`: デフォルト値はです `COPY` をクリックすると、オブジェクトとすべてのタグをコピーできます。

を指定できます `REPLACE` オブジェクトのコピー時に既存のタグを上書きする場合、またはタグを更新する場合。

- S3 オブジェクトロック要求のヘッダー：
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

これらのヘッダーを指定せずに要求を行うと、バケットのデフォルトの保持設定を使用してオブジェクトバージョンモードと `retain-until-date` が計算されます。を参照してください ["S3 REST APIを使用してS3オブジェクトロックを設定します"](#)。

- SSE 要求ヘッダー :

- x-amz-copy-source-server-side-encryption-customer-algorithm
- x-amz-copy-source-server-side-encryption-customer-key
- x-amz-copy-source-server-side-encryption-customer-key-MD5
- x-amz-server-side-encryption
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-algorithm

を参照してください [サーバ側の暗号化を行うための要求ヘッダー]

サポートされない要求ヘッダーです

次の要求ヘッダーはサポートされていません。

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- Expires
- x-amz-website-redirect-location

ストレージクラスのオプション

◦ x-amz-storage-class 要求ヘッダーがサポートされ、一致するILMルールでDual commitまたはBalancedが使用されている場合にStorageGRIDで作成されるオブジェクトコピーの数に影響します。 "取り込みオプション"。

- STANDARD

(デフォルト) ILM ルールで Dual commit オプションが使用されている場合、または Balanced オプションによって中間コピーが作成される場合に、デュアルコミットの取り込み処理を指定します。

- REDUCED\_REDUNDANCY

ILM ルールで Dual commit オプションが使用されている場合、または Balanced オプションによって中間コピーが作成される場合に、シングルコミットの取り込み処理を指定します。



S3オブジェクトロックを有効にしてオブジェクトをバケットに取り込む場合は、を使用します REDUCED\_REDUNDANCY オプションは無視されます。古い準拠バケットにオブジェクトを取り込む場合は、を参照してください REDUCED\_REDUNDANCY オプションを指定するとエラーが返されます。StorageGRID では、常にデュアルコミットの取り込みが実行され、コンプライアンス要件が満たされます。

## CopyObjectでのx-amz-copy-sourceの使用

ソースのバケットとキーの場合は、で指定します `x-amz-copy-source` ヘッダーはデスティネーションのバケットおよびキーとは異なり、ソースオブジェクトデータのコピーがデスティネーションに書き込まれます。

送信元と宛先が一致している場合は、および `x-amz-metadata-directive` ヘッダーはのように指定します。`REPLACE`では、要求で指定されたメタデータの値に基づいてオブジェクトのメタデータが更新されます。この場合、StorageGRIDはオブジェクトを再取り込みしません。これには2つの重要な結果があります。

- CopyObjectを使用して既存のオブジェクトを暗号化したり、既存のオブジェクトの暗号化を変更したりすることはできません。を用意する場合は `x-amz-server-side-encryption` ヘッダーまたは `x-amz-server-side-encryption-customer-algorithm` ヘッダー。StorageGRIDは要求を拒否し、戻ります `XNotImplemented`。
- 一致する ILM ルールで指定されている取り込み動作のオプションが使用されません。更新によって発生したオブジェクト配置の変更は、通常のバックグラウンド ILM プロセスで ILM が再評価されるときに実施されます。

つまり、ILMルールの取り込み動作にStrictオプションが使用されている場合、必要なオブジェクト配置を実行できない場合（新たに必要な場所が使用できない場合など）は処理されません。更新されたオブジェクトは、必要な配置を実行可能になるまで現在の配置が維持されます。

### サーバ側の暗号化を行うための要求ヘッダー

あなたの場合 "サーバ側の暗号化を使用する" 指定する要求ヘッダーは、ソースオブジェクトが暗号化されているかどうか、およびターゲットオブジェクトを暗号化するかどうかによって異なります。

- ソースオブジェクトがユーザ指定のキーを使用して暗号化されている場合 (SSE-C) は、オブジェクトを復号化してコピーできるように、CopyObject要求に次の3つのヘッダーを含める必要があります。
  - `x-amz-copy-source-server-side-encryption-customer-algorithm`: 指定します AES256。
  - `x-amz-copy-source-server-side-encryption-customer-key`: ソースオブジェクトの作成時に指定した暗号化キーを指定します
  - `x-amz-copy-source-server-side-encryption-customer-key-MD5`: ソースオブジェクトの作成時に指定したMD5ダイジェストを指定します。
- ユーザが指定および管理する一意のキーでターゲットオブジェクト (コピー) を暗号化する場合は、次の3つのヘッダーを含めます。
  - `x-amz-server-side-encryption-customer-algorithm`: 指定します AES256。
  - `x-amz-server-side-encryption-customer-key`: ターゲットオブジェクトの新しい暗号化キーを指定します
  - `x-amz-server-side-encryption-customer-key-MD5`: 新しい暗号化キーのMD5ダイジェストを指定します。



指定した暗号化キーが格納されることはありません。暗号化キーを紛失すると、対応するオブジェクトが失われます。ユーザ指定のキーを使用してオブジェクトデータを保護する前に、の考慮事項を確認してください "サーバ側の暗号化を使用する"。

- ターゲットオブジェクト (コピー) をStorageGRID (SSE) で管理される一意のキーで暗号化する場合は、CopyObject要求に次のヘッダーを含めます。

- x-amz-server-side-encryption



◦ server-side-encryption オブジェクトの値を更新できません。代わりに、新しいを使用してコピーを作成します server-side-encryption を使用した値 x-amz-metadata-directive : REPLACE。

## バージョン管理

ソースバケットがバージョン管理に対応している場合は、を使用できます x-amz-copy-source オブジェクトの最新バージョンをコピーするヘッダー。オブジェクトの特定のバージョンをコピーするには、を使用してコピーするバージョンを明示的に指定する必要があります versionId サブリソース：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る場合は、で生成されたバージョンが返されます x-amz-version-id 応答ヘッダー。ターゲットバケットのバージョン管理が一時停止中の場合は、を実行します x-amz-version-id "null" 値を返します。

### GetObject

S3 GetObject要求を使用すると、S3バケットからオブジェクトを読み出すことができます。

### GetObjectオブジェクトとマルチパートオブジェクト

を使用できます partNumber マルチパートまたはセグメント化されたオブジェクトの特定の部分を読み出す要求パラメータ。。 x-amz-mp-parts-count response要素は、オブジェクトに含まれるパートの数を示します。

設定できます partNumber セグメント化されたオブジェクト/マルチパートオブジェクトとセグメント化されていないオブジェクト/マルチパート以外のオブジェクトの場合は1になります。ただし、 x-amz-mp-parts-count 応答要素は、セグメント化されたオブジェクトまたはマルチパートオブジェクトの場合にのみ返されます。

### ユーザメタデータ内の UTF-8 文字

StorageGRID は、ユーザ定義メタデータ内のエスケープされた UTF-8 文字を解析も解釈もしません。ユーザ定義のメタデータにエスケープされたUTF-8文字が含まれているオブジェクトに対するGET要求で、 x-amz-missing-meta キーの名前または値に印刷できない文字が含まれている場合は、ヘッダーを指定します。

サポートされない要求ヘッダーです

次の要求ヘッダーはサポートされていません xNotImplemented :

- x-amz-website-redirect-location

## バージョン管理

の場合 versionId サブリソースが指定されていません。バージョン管理されたバケット内のオブジェクトの最新バージョンが取得されます。オブジェクトの現在のバージョンが削除マーカーの場合は、「Not Found」ステータスが x-amz-delete-marker 応答ヘッダーをに設定しました true。

## ユーザ指定の暗号化キーによるサーバ側の暗号化（**SSE-C**）の要求ヘッダー

指定した一意のキーでオブジェクトが暗号化されている場合は、3つのヘッダーをすべて使用します。

- **x-amz-server-side-encryption-customer-algorithm**: 指定します AES256。
- **x-amz-server-side-encryption-customer-key**: オブジェクトの暗号化キーを指定します
- **x-amz-server-side-encryption-customer-key-MD5**: オブジェクトの暗号化キーのMD5ダイジェストを指定します。



指定した暗号化キーが格納されることはありません。暗号化キーを紛失すると、対応するオブジェクトが失われます。ユーザ指定のキーを使用してオブジェクトデータを保護する前に、の考慮事項を確認してください "サーバ側の暗号化を使用します"。

## クラウドストレージプールオブジェクトに対する**GetObject**の動作

オブジェクトがに格納されている場合 "クラウドストレージプール"の場合、GetObject要求の動作はオブジェクトの状態によって異なります。を参照してください "[HeadObject（ヘッドオブジェクト）](#)" 詳細：



オブジェクトがクラウドストレージプールに格納されていて、そのオブジェクトのコピーがグリッドに1つ以上存在する場合、GetObject要求はクラウドストレージプールからデータを読み出す前にグリッドからデータを読み出そうとします。

オブジェクトの状態	<b>GetObject</b> の動作
StorageGRID に取り込まれているがまだ ILM によって評価されていないオブジェクト、または従来のストレージプールに格納されているオブジェクト、またはイレイジャーコーディングを使用しているオブジェクト	200 OK オブジェクトのコピーが読み出されます。
クラウドストレージプール内にあるが、まだ読み出し不可能な状態に移行していない	200 OK オブジェクトのコピーが読み出されます。
オブジェクトを読み出し不可能な状態に移行した	403 Forbidden、 InvalidObjectState を使用します " <a href="#">RestoreObject</a> " 読み出し可能な状態へのオブジェクトのリストア要求。
読み出し不可能な状態からリストア中である	403 Forbidden、 InvalidObjectState RestoreObject要求が完了するまで待ちます。
クラウドストレージプールへのリストアが完了している	200 OK オブジェクトのコピーが読み出されます。

クラウドストレージプール内のマルチパートオブジェクトまたはセグメント化されたオブジェクト

マルチパートオブジェクトをアップロードした場合や StorageGRID が大きなオブジェクトをセグメントに分割した場合、StorageGRID はオブジェクトのパートまたはセグメントのサブセットをサンプリングすることでクラウドストレージプール内のオブジェクトが使用可能かどうかを判断します。GetObject要求が誤って返されることがある 200 OK オブジェクトの一部のパートがすでに読み出し不可能な状態に移行されている場合や、オブジェクトの一部のパートがまだリストアされていない場合。

このような場合は、次のように

- GetObject要求から一部のデータが返される場合がありますが、転送の途中で停止することがあります。
- 後続のGetObject要求で次のように返されることがある 403 Forbidden。

### GetObjectとグリッド間レプリケーション

使用するポート "グリッドフェデレーション" および "グリッド間レプリケーション" バケットで有効になっている場合、S3クライアントはGetObject要求を発行してオブジェクトのレプリケーションステータスを確認できます。応答にはStorageGRID固有の情報が含まれます x-ntap-sg-cgr-replication-status 応答ヘッダー。次のいずれかの値が設定されます。

グリッド ( Grid )	レプリケーションのステータス
ソース	<ul style="list-style-type: none"><li>成功：レプリケーションは成功しました。</li><li>* pending*：オブジェクトはまだレプリケートされていません。</li><li>failure：レプリケーションが永続的なエラーで失敗しました。ユーザーはエラーを解決する必要があります。</li></ul>
宛先	replica:オブジェクトはソースグリッドからレプリケートされました。



StorageGRID ではサポートされません x-amz-replication-status ヘッダー。

### HeadObject ( ヘッドオブジェクト )

S3 HeadObject要求を使用すると、オブジェクト自体を返さずにオブジェクトからメタデータを読み出すことができます。オブジェクトがクラウドストレージプールに格納されている場合は、HeadObjectを使用してオブジェクトの移行状態を確認できます。

### HeadObjectオブジェクトとマルチパートオブジェクト

を使用できます partNumber マルチパートまたはセグメント化されたオブジェクトの特定の部分のメタデータを読み出す要求パラメータ。。。 x-amz-mp-parts-count response要素は、オブジェクトに含まれるパートの数を示します。

設定できます partNumber セグメント化されたオブジェクト/マルチパートオブジェクトとセグメント化されていないオブジェクト/マルチパート以外のオブジェクトの場合は1になります。ただし、x-amz-mp-parts-count 応答要素は、セグメント化されたオブジェクトまたはマルチパートオブジェクトの場合にのみ返されます。

## ユーザメタデータ内の UTF-8 文字

StorageGRID は、ユーザ定義メタデータ内のエスケープされた UTF-8 文字を解析も解釈もしません。ユーザ定義メタデータにエスケープされたUTF-8文字が含まれているオブジェクトに対するHEAD要求では、が返されません `x-amz-missing-meta` キーの名前または値に印刷できない文字が含まれている場合は、ヘッダーを指定します。

サポートされない要求ヘッダーです

次の要求ヘッダーはサポートされていません `XNotImplemented` :

- `x-amz-website-redirect-location`

## バージョン管理

の場合 `versionId` サブリソースが指定されていません。バージョン管理されたバケット内のオブジェクトの最新バージョンが取得されます。オブジェクトの現在のバージョンが削除マーカーの場合は、「Not Found」ステータスが `x-amz-delete-marker` 応答ヘッダーをに設定しました `true`。

## ユーザ指定の暗号化キーによるサーバ側の暗号化（SSE-C）の要求ヘッダー

指定した一意のキーでオブジェクトが暗号化されている場合は、次の 3 つのヘッダーをすべて使用します。

- `x-amz-server-side-encryption-customer-algorithm`: 指定します AES256。
- `x-amz-server-side-encryption-customer-key`: オブジェクトの暗号化キーを指定します
- `x-amz-server-side-encryption-customer-key-MD5`: オブジェクトの暗号化キーのMD5ダイジェストを指定します。

 指定した暗号化キーが格納されることはありません。暗号化キーを紛失すると、対応するオブジェクトが失われます。ユーザ指定のキーを使用してオブジェクトデータを保護する前に、の考慮事項を確認してください "["サーバ側の暗号化を使用します"](#)。

## クラウドストレージプールオブジェクトに対するHeadObject応答

オブジェクトがに格納されている場合 "[クラウドストレージプール](#)"を指定すると、次の応答ヘッダーが返されます。

- `x-amz-storage-class: GLACIER`
- `x-amz-restore`

応答ヘッダーは、オブジェクトがクラウドストレージプールに移動され、必要に応じて読み出し不可能な状態に移行されてリストアされるときの状態に関する情報を提供します。

オブジェクトの状態	HeadObjectへの応答
StorageGRID に取り込まれているがまだ ILM によって評価されていないオブジェクト、または従来のストレージプールに格納されているオブジェクト、またはイレイジャーコーディングを使用しているオブジェクト	200 OK (特別な応答ヘッダーは返されません)。
クラウドストレージプール内にあるが、まだ読み出し不可能な状態に移行していない	<p>200 OK  x-amz-storage-class: GLACIER  'x-amz-restore : ongoing-request="false"、 expiry-date="2030年7月23日（土）00:00:00 GMT'</p> <p>オブジェクトが読み出し不可能な状態に移行されるまでの間、の値 expiry-date は、将来の特定の日時に設定されます。移行の正確な時間は、StorageGRID システムでは制御されません。</p>
オブジェクトが読み出し不可能な状態に移行したが、少なくとも 1 つのコピーがグリッドに存在する	<p>200 OK  x-amz-storage-class: GLACIER  'x-amz-restore : ongoing-request="false"、 expiry-date="2030年7月23日（土）00:00:00 GMT'</p> <p>の値 expiry-date は、将来の特定の日時に設定されます。</p> <p>注：グリッド上のコピーを使用できない場合（ストレージノードが停止している場合など）は、問題を実行する必要があります "RestoreObject" オブジェクトを読み出す前にクラウドストレージプールからコピーをリストアする要求。</p>
読み出し不可能な状態に移行しており、グリッドにコピーが存在しない	<p>200 OK  x-amz-storage-class: GLACIER</p>
読み出し不可能な状態からリストア中である	<p>200 OK  x-amz-storage-class: GLACIER  'x-amz-restore : ongoing-request="true"</p>

オブジェクトの状態	HeadObjectへの応答
クラウドストレージプールへのリストアが完了している	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>'x-amz-restore : ongoing-request="false"、 expiry-date="2018年7月23日（土）00:00:00 (GMT)"</p> <ul style="list-style-type: none"> <li>。expiry-date クラウドストレージプール内のオブジェクトが読み出し不可能な状態に戻るタイミングを示します。</li> </ul>

クラウドストレージプール内のマルチパートオブジェクトまたはセグメント化されたオブジェクト

マルチパートオブジェクトをアップロードした場合や StorageGRID が大きなオブジェクトをセグメントに分割した場合、StorageGRID はオブジェクトのパートまたはセグメントのサブセットをサンプリングすることでクラウドストレージプール内のオブジェクトが使用可能かどうかを判断します。オブジェクトの一部の部分がすでに読み出し不可能な状態に移行されている場合や、オブジェクトの一部がまだリストアされていない場合、HeadObject要求が誤って「x-amz-restore : ongoing-request="false"」を返すことがあります。

#### HeadObjectとクロスグリッドレプリケーション

使用するポート "グリッドフェデレーション" および "グリッド間レプリケーション" バケットで有効になっている場合、S3クライアントはHeadObject要求を発行してオブジェクトのレプリケーションステータスを確認できます。応答にはStorageGRID固有の情報が含まれます x-ntap-sg-cgr-replication-status 応答ヘッダー。次のいずれかの値が設定されます。

グリッド ( Grid )	レプリケーションのステータス
ソース	<ul style="list-style-type: none"> <li>• 成功：レプリケーションは成功しました。</li> <li>• * pending*：オブジェクトはまだレプリケートされていません。</li> <li>• failure: レプリケーションが永続的なエラーで失敗しました。ユーザーはエラーを解決する必要があります。</li> </ul>
宛先	replica: オブジェクトはソースグリッドからレプリケートされました。



StorageGRID ではがサポートされません x-amz-replication-status ヘッダー。

#### PutObject

S3 PutObject要求を使用して、バケットにオブジェクトを追加できます。

競合を解決します

同じキーに書き込む 2 つのクライアントなど、競合するクライアント要求は、「latest-wins」ベースで解決されます。「latest-wins」評価は、S3 クライアントが処理を開始するタイミングではなく、StorageGRID システムが特定の要求を完了したタイミングで行われます。

## オブジェクトのサイズ

1回のPutObject処理の最大推奨サイズは5GiB（5、368、709、120バイト）です。5GiBを超えるオブジェクトがある場合は、"マルチパートアップロード"代わりに、

1回のPutObject処理のmaximum\_supported\_sizeは5TiB（5、497、558、138、880バイト）です。

 StorageGRID 11.6以前からアップグレードした場合、5GiBを超えるオブジェクトをアップロードしようとすると、S3 PUT Object size too largeアラートがトリガーされます。StorageGRID 11.7または11.8を新規にインストールした場合、この場合アラートはトリガーされません。ただし、AWS S3標準に準拠するため、StorageGRIDの今後のリリースでは5GiBを超えるオブジェクトのアップロードはサポートされません。

## ユーザメタデータのサイズ

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 に制限されます。StorageGRID では、ユーザメタデータが 24KiB に制限されます。ユーザ定義のメタデータのサイズは、各キーと値の UTF-8 エンコードでのバイト数の合計で測定されます。

### ユーザメタデータ内の UTF-8 文字

要求のユーザ定義メタデータのキー名または値に（エスケープされていない）UTF-8 文字が含まれている場合、StorageGRID の動作は定義されていません。

ユーザ定義メタデータのキー名または値に含まれているエスケープされた UTF-8 文字は、StorageGRID で解析も解釈もされません。エスケープされた UTF-8 文字は ASCII 文字として扱われます。

- ユーザ定義メタデータにエスケープされたUTF-8文字が含まれている場合、PutObject、CopyObject、GetObject、およびHeadObjectの各要求は成功します。
- StorageGRID からが返されない x-amz-missing-meta キーの名前または値の解釈後の値に印刷不能文字が含まれている場合は、ヘッダー。

## オブジェクトタグの制限

タグは、新しいオブジェクトをアップロードするときに追加することも、既存のオブジェクトに追加することもできます。StorageGRID と Amazon S3 はどちらも、オブジェクトごとに最大 10 個のタグをサポートします。オブジェクトに関連付けられたタグには、一意のタグキーが必要です。タグキーには Unicode 文字を 128 文字まで、タグ値には Unicode 文字を 256 文字まで使用できます。キーと値では大文字と小文字が区別されます。

## オブジェクトの所有権

StorageGRID では、非所有者アカウントまたは匿名ユーザによって作成されたオブジェクトを含むすべてのオブジェクトが、バケット所有者アカウントによって所有されます。

## サポートされる要求ヘッダー

次の要求ヘッダーがサポートされています。

- Cache-Control
- Content-Disposition

- Content-Encoding

を指定する場合 aws-chunked の場合 Content-EncodingStorageGRID では、次の項目は検証されません。

- StorageGRID ではが検証されません chunk-signature チャンクデータに対して。
- StorageGRID は、ユーザが指定した値を検証しません x-amz-decoded-content-length をクリックします。

- Content-Language

- Content-Length

- Content-MD5

- Content-Type

- Expires

- Transfer-Encoding

チャンク転送エンコードは、の場合にサポートされます aws-chunked ペイロード署名も使用されます。

- `x-amz-meta-`をクリックし、続けてユーザ定義のメタデータを含む名前と値のペアを作成します。

ユーザ定義メタデータの名前と値のペアを指定する場合、一般的な形式は次のとおりです。

```
x-amz-meta-name: value
```

ILMルールの参照時間に\*[ユーザ定義の作成時間]\*オプションを使用する場合は、を使用する必要があります creation-time を、オブジェクトの作成時に記録されたメタデータの名前として指定します。例：

```
x-amz-meta-creation-time: 1443399726
```

の値 creation-time は、1970年1月1日からの秒数として評価されます。



ILMルールでは、参照時間に\*ユーザ定義の作成時間\*を使用し、取り込みオプションをBalancedまたはStrictの両方にすることはできません。ILM ルールの作成時にエラーが返されます。

- x-amz-tagging

- S3 Object Lock 要求のヘッダー
  - x-amz-object-lock-mode
  - x-amz-object-lock-retain-until-date
  - x-amz-object-lock-legal-hold

これらのヘッダーを指定せずに要求を行うと、バケットのデフォルトの保持設定を使用してオブジェクトバージョンモードとretain-until-dateが計算されます。を参照してください ["S3 REST APIを使用し](#)

てS3オブジェクトロックを設定します"。

- SSE 要求ヘッダー：

- x-amz-server-side-encryption
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-algorithm

を参照してください [サーバ側の暗号化を行うための要求ヘッダー]

サポートされない要求ヘッダーです

次の要求ヘッダーはサポートされていません。

- x-amz-acl 要求ヘッダーはサポートされていません。
- x-amz-website-redirect-location 要求ヘッダーはサポートされておらず、返されます XNotImplemented。

ストレージクラスのオプション

◦ x-amz-storage-class 要求ヘッダーがサポートされています。に送信された値 x-amz-storage-class StorageGRID が取り込み中にオブジェクトデータを保護する方法に影響し、StorageGRID システム (ILMで決定) に格納されるオブジェクトの永続的コピーの数には影響しません。

取り込まれたオブジェクトに一致するILMルールでStrict取り込みオプションが使用されている場合は、 x-amz-storage-class ヘッダーに影響はありません。

には次の値を使用できます x-amz-storage-class :

- STANDARD (デフォルト)

- \* Dual commit \* : ILM ルールの取り込み動作が Dual commit オプションに指定されている場合は、オブジェクトの取り込み直後にオブジェクトの 2 つ目のコピーが作成されて別のストレージノードに配置されます (デュアルコミット)。ILMが評価されると、StorageGRID はこれらの初期中間コピーがルールの配置手順を満たしているかどうかを判断します。作成されていない場合は、新しいオブジェクトコピーを別の場所に作成し、最初の中間コピーを削除しなければならないことがあります。
- \* Balanced \* : ILMルールでBalancedオプションが指定されていて、ルールで指定されたすべてのコピーをStorageGRID がすぐに作成できない場合、StorageGRID は2つの中間コピーを別々のストレージノードに作成します。

StorageGRID がILMルールに指定されたすべてのオブジェクトコピーをただちに作成できる場合 (同期配置) は、を参照してください x-amz-storage-class ヘッダーに影響はありません。

- REDUCED\_REDUNDANCY

- \* Dual commit \* : ILM ルールの取り込み動作が Dual commit オプションに指定されている場合は、オブジェクトの取り込み時に StorageGRID が中間コピーを 1 つ作成します (シングルコミット)。
- \* Balanced \* : ILMルールでBalancedオプションが指定されている場合、StorageGRID は、ルールで指

定されたすべてのコピーをただちに作成できない場合にのみ中間コピーを1つ作成します。StorageGRID IDで同期配置を実行できる場合、このヘッダーは効果がありません。

。 REDUCED\_REDUNDANCY オプションは、オブジェクトに一致するILMルールで単一のレプリケートコピーが作成される場合に最適です。この場合は、を使用します REDUCED\_REDUNDANCY 取り込み処理のたびに追加のオブジェクトコピーを不要に作成および削除する必要がなくなります。

を使用する REDUCED\_REDUNDANCY それ以外の場合は、このオプションは推奨されません。

REDUCED\_REDUNDANCY 取り込み中にオブジェクトデータが失われるリスクが高まります。たとえば、ILM評価の前にコピーが1つだけ格納されていたストレージノードに障害が発生すると、データが失われる可能性があります。

 レプリケートコピーを一定期間に1つだけ作成すると、データが永続的に失われるリスクがあります。オブジェクトのレプリケートコピーが1つしかない場合、ストレージノードに障害が発生したり、重大なエラーが発生すると、そのオブジェクトは失われます。また、アップグレードなどのメンテナンス作業中は、オブジェクトへのアクセスが一時的に失われます。

を指定します REDUCED\_REDUNDANCY オブジェクトの初回取り込み時に作成されるコピー数のみに影響します。オブジェクトがアクティブなILMポリシーで評価される際に作成されるオブジェクトのコピー数には影響せず、StorageGRIDシステムでデータが格納される際の冗長性レベルが低下することもありません。

 S3オブジェクトロックを有効にしてオブジェクトをバケットに取り込む場合は、を使用します REDUCED\_REDUNDANCY オプションは無視されます。古い準拠バケットにオブジェクトを取り込む場合は、を参照してください REDUCED\_REDUNDANCY オプションを指定するとエラーが返されます。StorageGRIDでは、常にデュアルコミットの取り込みが実行され、コンプライアンス要件が満たされます。

#### サーバ側の暗号化を行うための要求ヘッダー

オブジェクトをサーバ側の暗号化で暗号化するには、次の要求ヘッダーを使用します。SSEオプションと SSE-C オプションを同時に指定することはできません。

- \* SSE \* : StorageGRIDで管理される一意のキーでオブジェクトを暗号化するには、次のヘッダーを使用します。

◦ x-amz-server-side-encryption

- \* SSE-C \* : ユーザが指定および管理する一意のキーでオブジェクトを暗号化する場合は、次の3つのヘッダーをすべて使用します。

◦ x-amz-server-side-encryption-customer-algorithm:指定します AES256。

◦ x-amz-server-side-encryption-customer-key:新しいオブジェクトの暗号化キーを指定します。

◦ x-amz-server-side-encryption-customer-key-MD5:新しいオブジェクトの暗号化キーのMD5ダイジェストを指定します。

 指定した暗号化キーが格納されることはありません。暗号化キーを紛失すると、対応するオブジェクトが失われます。ユーザ指定のキーを使用してオブジェクトデータを保護する前に、の考慮事項を確認してください "["サーバ側の暗号化を使用する"](#)"。

 SSEまたはSSE-Cで暗号化されたオブジェクトは、バケットレベルまたはグリッドレベルの暗号化設定が無視されます。

## バージョン管理

バケットでバージョン管理が有効になっている場合は、一意です `versionId` は、格納されているオブジェクトのバージョンに対して自動的に生成されます。これ `versionId` は、を使用して応答としても返されます `x-amz-version-id` 応答ヘッダー。

バージョン管理が一時停止中の場合は、オブジェクトバージョンはnullで格納されます `versionId` また、null バージョンがすでに存在する場合は上書きされます。

### Authorizationヘッダーのシグニチャ計算

を使用する場合 `Authorization` 要求を認証するためのヘッダー。StorageGRID は AWS と次の点で異なります。

- StorageGRID は必要ありません `host` に含めるヘッダー `CanonicalHeaders`。
- StorageGRID は必要ありません `Content-Type` に含まれています `CanonicalHeaders`。
- StorageGRID は必要ありません `x-amz-*` に含めるヘッダー `CanonicalHeaders`。



一般的なベストプラクティスとして、には常にこれらのヘッダーを含めてください `CanonicalHeaders` これらのヘッダーが検証されるようにするためにですが、これらのヘッダーを除外しても、StorageGRID はエラーを返しません。

詳細については、を参照してください "[Authorizationヘッダーのシグニチャ計算：単一チャンクでのペイロードの転送（AWS Signature Version 4）](#)"。

## 関連情報

["ILM を使用してオブジェクトを管理する"](#)

## RestoreObject

S3 `RestoreObject` 要求を使用して、クラウドストレージプールに格納されているオブジェクトをリストアできます。

### サポートされている要求タイプ

StorageGRIDでは、オブジェクトのリストアで `RestoreObject` 要求のみがサポートされます。ではサポートされません `SELECT` リストアのタイプ。戻り要求を選択してください `XNotImplemented`。

## バージョン管理

必要に応じて、と指定します `versionId` バージョン管理されたバケット内のオブジェクトの特定のバージョンをリストアする。指定しない場合 `versionId` オブジェクトの最新バージョンがリストアされます

### クラウドストレージプールオブジェクトでの `RestoreObject` の動作

オブジェクトがに格納されている場合 "クラウドストレージプール" の `RestoreObject` 要求の動作は、オブジェクトの状態に基づいて次のようにになります。を参照してください "[HeadObject（ヘッドオブジェクト）](#)" 詳細：



オブジェクトがクラウドストレージプールに格納されていて、そのオブジェクトのコピーがグリッドに1つ以上存在する場合は、`RestoreObject`要求を実行してオブジェクトをリストアする必要はありません。代わりに、`GetObject`要求を使用してローカルコピーを直接取得できます。

オブジェクトの状態	<code>RestoreObject</code> の動作
StorageGRID に取り込まれているがまだ ILM によって評価されていない、またはオブジェクトがクラウドストレージプールにない	403 Forbidden、 InvalidObjectState
クラウドストレージプール内にあるが、まだ読み出し不可能な状態に移行していない	200 OK 変更は行われません。 注：オブジェクトが読み出し不可能な状態に移行されるまでは変更できません <code>expiry-date</code> 。
オブジェクトを読み出し不可能な状態に移行した	202 Accepted 要求の本文で指定されている日数、オブジェクトの読み出し可能なコピーをクラウドストレージプールにリストアします。この期間が終了すると、オブジェクトは読み出し不可能な状態に戻ります。 必要に応じて、を使用します <code>Tier</code> リストアジョブの完了までにかかる時間を確認するための要求要素 ( <code>Expedited</code> 、 <code>Standard</code> 、または <code>Bulk</code> )。指定しない場合 <code>Tier</code> 、 <code>Standard</code> 階層を使用しています。  重要：オブジェクトがS3 Glacier Deep Archiveに移行された場合、またはクラウドストレージプールがAzure BLOBストレージを使用している場合は、を使用してリストアできません <code>Expedited</code> 階層：次のエラーが返されます 403 Forbidden、 InvalidTier: Retrieval option is not supported by this storage class.
読み出し不可能な状態からリストア中である	409 Conflict、 <code>RestoreAlreadyInProgress</code>
クラウドストレージプールへのリストアが完了している	200 OK  *注：*オブジェクトが読み出し可能な状態にリストアされている場合は、オブジェクトを変更できます <code>expiry-date</code> 新しい値を指定して <code>RestoreObject</code> 要求を再発行する Days。要求が実行された日時に基づいてリストア日が更新されます。

`SelectObjectContent` の順に選択します

S3 `SelectObjectContent` 要求を使用すると、シンプルな SQL ステートメントに基づいて S3 オブジェクトのコンテンツをフィルタリングできます。

詳細については、を参照してください ["Amazon Simple Storage Service API リファレンス : SelectObjectContent"](#)。

## 作業を開始する前に

- ・ テナントアカウントには S3 Select 権限が割り当てられます。
- ・ これで完了です s3:GetObject 照会するオブジェクトの権限。
- ・ 照会するオブジェクトは、次のいずれかの形式である必要があります。
  - \* CSV \*。そのまま使用することも、GZIPやbzip2のアーカイブに圧縮して使用することもできます。
  - 寄木細工。寄木細工オブジェクトの追加要件：
    - S3 Selectでは、GZIPまたはSnappyを使用したカラムナ圧縮のみがサポートされます。S3 Select では、寄木細工オブジェクトのオブジェクト全体の圧縮はサポートされません。
    - S3 Selectは寄木細工の出力をサポートしていません。出力形式はCSVまたはJSONで指定する必要があります。
    - 圧縮されていない行グループの最大サイズは512MBです。
    - オブジェクトのスキーマで指定されているデータ型を使用する必要があります。
    - interval、json、list、time、またはUUID論理型は使用できません。
- ・ SQL 式の最大長は 256KB です。
- ・ 入力または結果のすべてのレコードの最大長は 1MiB です。

## CSV要求の構文例

```
POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
    <Expression>string</Expression>
    <ExpressionType>string</ExpressionType>
    <RequestProgress>
        <Enabled>boolean</Enabled>
    </RequestProgress>
    <InputSerialization>
        <CompressionType>GZIP</CompressionType>
        <CSV>
            <AllowQuotedRecordDelimiter>boolean</AllowQuotedRecordDelimiter>
            <Comments>#</Comments>
            <FieldDelimiter>\t</FieldDelimiter>
            <FileHeaderInfo>USE</FileHeaderInfo>
            <QuoteCharacter>'</QuoteCharacter>
            <QuoteEscapeCharacter>\\</QuoteEscapeCharacter>
            <RecordDelimiter>\n</RecordDelimiter>
        </CSV>
    </InputSerialization>
    <OutputSerialization>
        <CSV>
            <FieldDelimiter>string</FieldDelimiter>
            <QuoteCharacter>string</QuoteCharacter>
            <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
            <QuoteFields>string</QuoteFields>
            <RecordDelimiter>string</RecordDelimiter>
        </CSV>
    </OutputSerialization>
    <ScanRange>
        <End>long</End>
        <Start>long</Start>
    </ScanRange>
</SelectObjectContentRequest>
```

## 寄木リクエスト構文の例

```

POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
    <Expression>string</Expression>
    <ExpressionType>string</ExpressionType>
    <RequestProgress>
        <Enabled>boolean</Enabled>
    </RequestProgress>
    <InputSerialization>
        <CompressionType>GZIP</CompressionType>
        <PARQUET>
        </PARQUET>
    </InputSerialization>
    <OutputSerialization>
        <CSV>
            <FieldDelimiter>string</FieldDelimiter>
            <QuoteCharacter>string</QuoteCharacter>
            <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
            <QuoteFields>string</QuoteFields>
            <RecordDelimiter>string</RecordDelimiter>
        </CSV>
    </OutputSerialization>
    <ScanRange>
        <End>long</End>
        <Start>long</Start>
    </ScanRange>
</SelectObjectContentRequest>

```

## SQL クエリの例

このクエリは、州名、2010年人口、2015年推定人口、米国的人口調査データからの変化率を取得します。状態でないファイル内のレコードは無視されます。

```

SELECT STNAME, CENSUS2010POP, POPESTIMATE2015, CAST((POPESTIMATE2015 -
CENSUS2010POP) AS DECIMAL) / CENSUS2010POP * 100.0 FROM S3Object WHERE
NAME = STNAME

```

照会するファイルの最初の数行 `SUB-EST2020\_ALL.csv` 次のようになります。

```

SUMLEV,STATE,COUNTY,PLACE,COUSUB,CONCIT,PRIMGEO_FLAG,FUNCSTAT,NAME,STNAME,
CENSUS2010POP,
ESTIMATESBASE2010,POPESTIMATE2010,POPESTIMATE2011,POPESTIMATE2012,POPESTIM
ATE2013,POPESTIMATE2014,
POPESTIMATE2015,POPESTIMATE2016,POPESTIMATE2017,POPESTIMATE2018,POPESTIMAT
E2019,POPESTIMATE042020,
POPESTIMATE2020
040,01,000,00000,00000,00000,0,A,Alabama,Alabama,4779736,4780118,4785514,4
799642,4816632,4831586,
4843737,4854803,4866824,4877989,4891628,4907965,4920706,4921532
162,01,000,00124,00000,00000,0,A,Abbeville
city,Alabama,2688,2705,2699,2694,2645,2629,2610,2602,
2587,2578,2565,2555,2555,2553
162,01,000,00460,00000,00000,0,A,Adamsville
city,Alabama,4522,4487,4481,4474,4453,4430,4399,4371,
4335,4304,4285,4254,4224,4211
162,01,000,00484,00000,00000,0,A,Addison
town,Alabama,758,754,751,750,745,744,742,734,734,728,
725,723,719,717

```

## AWS-CLIの使用例（CSV）

```

aws s3api select-object-content --endpoint-url https://10.224.7.44:10443
--no-verify-ssl --bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.csv --expression-type SQL --input-serialization '{"CSV":'
{"FileHeaderInfo": "USE", "Comments": "#", "QuoteEscapeCharacter": "\"",
"RecordDelimiter": "\n", "FieldDelimiter": ",", "QuoteCharacter": "\"",
"AllowQuotedRecordDelimiter": false}, "CompressionType": "NONE"}' --output
-serialization '{"CSV": {"QuoteFields": "ASNEEDED",
"QuoteEscapeCharacter": "#", "RecordDelimiter": "\n", "FieldDelimiter": ",",
"QuoteCharacter": "\""} }' --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" changes.csv

```

出力ファイルの最初の数行 `changes.csv` 次のようになります。

```

Alabama,4779736,4854803,1.5705260708959658022953568983726297854
Alaska,710231,738430,3.9703983633493891424057806544631253775
Arizona,6392017,6832810,6.8959922978928247531256565807005832431
Arkansas,2915918,2979732,2.1884703204959810255295244928012378949
California,37253956,38904296,4.4299724839960620557988526104449148971
Colorado,5029196,5454328,8.4532796097030221132761578590295546246

```

## AWS-CLIの使用例（寄木細工）

```
aws s3api select-object-content --endpoint-url https://10.224.7.44:10443  
--bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-  
EST2020_ALL.parquet --expression "SELECT STNAME, CENSUS2010POP,  
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /  
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" --expression-type  
'SQL' --input-serialization '{"Parquet":{}}' --output-serialization  
'{"CSV": {}}' changes.csv
```

出力ファイルの最初のいくつかの行は、.csvを変更します。次のようにになります。

```
Alabama,4779736,4854803,1.5705260708959658022953568983726297854  
Alaska,710231,738430,3.9703983633493891424057806544631253775  
Arizona,6392017,6832810,6.8959922978928247531256565807005832431  
Arkansas,2915918,2979732,2.1884703204959810255295244928012378949  
California,37253956,38904296,4.4299724839960620557988526104449148971  
Colorado,5029196,5454328,8.4532796097030221132761578590295546246
```

## マルチパートアップロードの処理

### マルチパートアップロードの処理：概要

このセクションでは、StorageGRIDでのマルチパートアップロードの処理のサポートについて説明します。

マルチパートアップロードのすべての処理に、次の条件と注意事項が適用されます。

- 1つのバケットに対して同時に実行するマルチパートアップロードの数が1,000を超えないようにしてください。そのバケットに対するListMultipartUploadsのクエリで不完全な結果が返されることがあります。
- StorageGRIDは、マルチパートにAWSのサイズ制限を適用します。S3クライアントは次のガイドラインに従う必要があります。
  - マルチパートアップロードの各パートのサイズは5MiB（5、242、880バイト）と5GiB（5、368、709、120バイト）の間にする必要があります。
  - 最後の部分は5MiB（5,242,880バイト）より小さくできます。
  - 一般に、パートサイズはできるだけ大きくする必要があります。たとえば、100GiBオブジェクトの場合、5GBのパートサイズを使用します。各パートは固有のオブジェクトとみなされるため、大きなパートサイズを使用するとStorageGRIDメタデータのオーバーヘッドが削減されます。
  - 5GB未満のオブジェクトでは、マルチパートではないアップロードの使用を検討してください。
- ILMルールでBalancedまたはStrictが使用されている場合は、マルチパートオブジェクトの各パートの取り込み時にILMが評価され、マルチパートアップロードの完了時にオブジェクト全体に対してILMが評価されます。["取り込みオプション"](#)。これがオブジェクトとパートの配置にどのように影響するかに注意する必要があります。
  - S3マルチパートアップロードの実行中にILMが変更されると、マルチパートアップロードの完了時に

オブジェクトの一部の部分が現在のILM要件を満たしていない可能性があります。正しく配置されていないパートはILMルールによる再評価の対象としてキューに登録され、あとで正しい場所に移動されます。

- ° パートに対して ILM を評価する際、StorageGRID はオブジェクトのサイズではなくパートのサイズでフィルタリングします。つまり、オブジェクト全体のILM要件を満たしていない場所にオブジェクトの一部を格納できます。たとえば、10GB以上のオブジェクトをすべてDC1に格納し、それより小さいオブジェクトをすべてDC2に格納するルールの場合、10パートのマルチパートアップロードの1GBの各パートは取り込み時にDC2に格納されます。ただし、オブジェクト全体に対してILMが評価される上、オブジェクトのすべての部分がDC1に移動されます。
- マルチパートアップロードのすべての処理でStorageGRIDがサポートされます。 "整合性の値"。
- マルチパートアップロードを使用してオブジェクトを取り込んだ場合、 "オブジェクトのセグメント化しきい値 (1GiB)" は適用されません。
- 必要に応じて、 "サーバ側の暗号化" マルチパートアップロードの場合：SSE (StorageGRIDで管理されるキーによるサーバ側の暗号化) を使用するには、を指定します `x-amz-server-side-encryption` CreateMultipartUpload要求の要求ヘッダーのみ。 SSE-C (ユーザ指定のキーによるサーバ側の暗号化) を使用するには、CreateMultipartUpload要求と後続の各UploadPart要求に同じ3つの暗号化キー要求ヘッダーを指定します。

操作	実装
AbortMultipartUpload の略	Amazon S3 REST API のすべての動作が実装されています。予告なく変更される場合があります。
CompleteMultipartUpload	を参照してください " <a href="#">CompleteMultipartUpload</a> "
CreateMultipartUpload を実行します (以前の名前はInitiate Multipart Upload )	を参照してください " <a href="#">CreateMultipartUpload を実行します</a> "
ListMultipartUploads	を参照してください " <a href="#">ListMultipartUploads</a> "
ListParts	Amazon S3 REST API のすべての動作が実装されています。予告なく変更される場合があります。
UploadPart のアップロード	を参照してください " <a href="#">UploadPart のアップロード</a> "
UploadPartCopyをクリックします	を参照してください " <a href="#">UploadPartCopyをクリックします</a> "

#### CompleteMultipartUpload

CompleteMultipartUpload処理は、以前にアップロードされたパートをアセンブルして、オブジェクトのマルチパートアップロードを完了します。

競合を解決します

同じキーに書き込む 2 つのクライアントなど、競合するクライアント要求は、「latest-wins」ベースで解決

されます。「latest-wins」評価は、S3 クライアントが処理を開始するタイミングではなく、StorageGRID システムが特定の要求を完了したタイミングで行われます。

## 要求ヘッダー

。 `x-amz-storage-class` 要求ヘッダーがサポートされ、一致するILMルールでDual commitまたはBalancedに指定されている場合にStorageGRIDで作成されるオブジェクトコピーの数に影響します。 "取り込みオプション"。

- STANDARD

(デフォルト) ILM ルールで Dual commit オプションが使用されている場合、または Balanced オプションによって中間コピーが作成される場合に、デュアルコミットの取り込み処理を指定します。

- REDUCED\_REDUNDANCY

ILM ルールで Dual commit オプションが使用されている場合、または Balanced オプションによって中間コピーが作成される場合に、シングルコミットの取り込み処理を指定します。



S3オブジェクトロックを有効にしてオブジェクトをバケットに取り込む場合は、を使用します `REDUCED_REDUNDANCY` オプションは無視されます。古い準拠バケットにオブジェクトを取り込む場合は、を参照してください `REDUCED_REDUNDANCY` オプションを指定するとエラーが返されます。StorageGRID では、常にデュアルコミットの取り込みが実行され、コンプライアンス要件が満たされます。



マルチパートアップロードが 15 日以内に完了しないと、非アクティブな処理としてマークされ、関連するすべてのデータがシステムから削除されます。



。 ETag 返される値はデータのMD5サムではなく、のAmazon S3 APIの実装に従います ETag マルチパートオブジェクトの値。

## バージョン管理

マルチパートアップロードは、この処理で完了します。バケットでバージョン管理が有効になっている場合は、マルチパートアップロードの完了後にオブジェクトのバージョンが作成されます。

バケットでバージョン管理が有効になっている場合は、一意です `versionId` は、格納されているオブジェクトのバージョンに対して自動的に生成されます。これ `versionId` は、を使用して応答としても返されます `x-amz-version-id` 応答ヘッダー。

バージョン管理が一時停止中の場合は、オブジェクトバージョンはnullで格納されます `versionId` また、null バージョンがすでに存在する場合は上書きされます。



バケットでバージョン管理が有効になっているときは、同じオブジェクトキーで同時に複数のマルチパートアップロードが実行されている場合でも、マルチパートアップロードが完了するたびに常に新しいバージョンが作成されます。バケットでバージョン管理が有効になっていないときは、マルチパートアップロードの開始後に、同じオブジェクトキーで別のマルチパートアップロードが開始されて先に完了することがあります。バージョン管理が有効になっていないバケットでは、最後に完了したマルチパートアップロードが優先されます。

レプリケーション、通知、またはメタデータ通知に失敗しました

マルチパートアップロードが行われるバケットでプラットフォームサービスが設定されている場合、関連するレプリケーション操作や通知操作が失敗してもマルチパートアップロードは正常に実行されます。

この状況が発生すると、Total Events (SMTT) のアラームがグリッドマネージャで生成されます。通知に失敗した最後のオブジェクトについて、[Last Event]メッセージに「Failed to publish notifications for bucket-nameobject key」と表示されます。（このメッセージを表示するには、\* nodes \* > \* \_ Storage Node\_\* > \* Events \* を選択します。表の一番上にLast Eventが表示されます）。イベントメッセージは、にも表示されます /var/local/log/bycast-err.log。

テナントでは、オブジェクトのメタデータまたはタグを更新することで、失敗したレプリケーションまたは通知をトリガーできます。テナントでは、既存の値を再送信し、不要な変更を回避できます。

**CreateMultipartUpload** を実行します

**CreateMultipartUpload** (以前のInitiate Multipart Upload) 処理は、オブジェクトのマルチパートアップロードを開始し、アップロードIDを返します。

。 `x-amz-storage-class` 要求ヘッダーがサポートされています。に送信された値 `x-amz-storage-class` StorageGRID が取り込み中にオブジェクトデータを保護する方法に影響し、StorageGRID システム (ILMで決定) に格納されるオブジェクトの永続的コピーの数には影響しません。

取り込まれたオブジェクトに一致するILMルールでStrictが使用されている場合 "取り込みオプション"、`x-amz-storage-class` ヘッダーに影響はありません。

には次の値を使用できます `x-amz-storage-class` :

- STANDARD (デフォルト)

- \* Dual commit \* : ILMルールでDual commit取り込みオプションが指定されている場合は、オブジェクトが取り込まれるとすぐにそのオブジェクトの2つ目のコピーが作成されて別のストレージノードに分散されます（デュアルコミット）。ILMが評価されると、StorageGRID はこれらの初期中間コピーがルールの配置手順を満たしているかどうかを判断します。作成されていない場合は、新しいオブジェクトコピーを別の場所に作成し、最初の中間コピーを削除しなければならぬことがあります。
- \* Balanced \* : ILMルールでBalancedオプションが指定されていて、ルールで指定されたすべてのコピーをStorageGRID がすぐに作成できない場合、StorageGRID は2つの中間コピーを別々のストレージノードに作成します。

StorageGRID がILMルールに指定されたすべてのオブジェクトコピーをただちに作成できる場合（同期配置）は、を参照してください `x-amz-storage-class` ヘッダーに影響はありません。

- REDUCED\_REDUNDANCY

- \* Dual commit \* : ILMルールでDual commitオプションが指定されている場合、StorageGRIDはオブジェクトの取り込み時に中間コピーを1つ作成します（シングルコミット）。
- \* Balanced \* : ILMルールでBalancedオプションが指定されている場合、StorageGRID は、ルールで指定されたすべてのコピーをただちに作成できない場合にのみ中間コピーを1つ作成します。StorageGRID で同期配置を実行できる場合、このヘッダーは効果がありません。
- REDUCED\_REDUNDANCY オプションは、オブジェクトに一致するILMルールで単一のレプリケートコピーが作成される場合に最適です。この場合は、を使用します REDUCED\_REDUNDANCY 取り込み処理のたびに追加のオブジェクトコピーを不要に作成および削除する必要がなくなります。

を使用する REDUCED\_REDUNDANCY それ以外の場合は、このオプションは推奨されません。REDUCED\_REDUNDANCY 取り込み中にオブジェクトデータが失われるリスクが高まります。たとえば、ILM 評価の前にコピーが 1 つだけ格納されていたストレージノードに障害が発生すると、データが失われる可能性があります。

 レプリケートコピーを一定期間に 1 つだけ作成すると、データが永続的に失われるリスクがあります。オブジェクトのレプリケートコピーが 1 つしかない場合、ストレージノードに障害が発生したり、重大なエラーが発生すると、そのオブジェクトは失われます。また、アップグレードなどのメンテナンス作業中は、オブジェクトへのアクセスが一時的に失われます。

を指定します REDUCED\_REDUNDANCY オブジェクトの初回取り込み時に作成されるコピー数のみに影響します。オブジェクトがアクティブな ILM ポリシーで評価される際に作成されるオブジェクトのコピー数には影響せず、StorageGRID システムでデータが格納される際の冗長性レベルが低下することもありません。

 S3 オブジェクトロックを有効にしてオブジェクトをバケットに取り込む場合は、を使用します REDUCED\_REDUNDANCY オプションは無視されます。古い準拠バケットにオブジェクトを取り込む場合は、を参照してください REDUCED\_REDUNDANCY オプションを指定するとエラーが返されます。StorageGRID では、常にデュアルコミットの取り込みが実行され、コンプライアンス要件が満たされます。

次の要求ヘッダーがサポートされています。

- Content-Type
- `x-amz-meta-` をクリックし、続けてユーザ定義のメタデータを含む名前と値のペアを作成します

ユーザ定義メタデータの名前と値のペアを指定する場合、一般的な形式は次のとおりです。

```
x-amz-meta-_name_: `value`
```

ILM ルールの参照時間に \*[ユーザ定義の作成時間]\* オプションを使用する場合は、を使用する必要があります creation-time を、オブジェクトの作成時に記録されたメタデータの名前として指定します。例：

```
x-amz-meta-creation-time: 1443399726
```

の値 creation-time は、1970年1月1日からの秒数として評価されます。



追加中です creation-time レガシー準拠が有効になっているバケットにオブジェクトを追加する場合、ユーザ定義メタデータは許可されません。エラーが返されます。

- S3 オブジェクトロック要求のヘッダー：

- x-amz-object-lock-mode
- x-amz-object-lock-retain-until-date
- x-amz-object-lock-legal-hold

これらのヘッダーがない状態で要求を送信した場合、バケットのデフォルトの保持設定を使用して、オブジェクトバージョンの retain-date が計算されます。

### "S3 REST APIを使用してS3オブジェクトロックを設定します"

- SSE 要求ヘッダー：

- x-amz-server-side-encryption
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-algorithm

#### [サーバ側の暗号化を行うための要求ヘッダー]



StorageGRIDでのUTF-8文字の処理方法については、を参照してください。 "[PutObject](#)"。

#### サーバ側の暗号化を行うための要求ヘッダー

マルチパートオブジェクトをサーバ側の暗号化で暗号化するには、次の要求ヘッダーを使用します。 SSE オプションと SSE-C オプションを同時に指定することはできません。

- **SSE**: StorageGRIDによって管理される一意のキーでオブジェクトを暗号化する場合  
は、CreateMultipartUpload要求で次のヘッダーを使用します。 UploadPart要求でこのヘッダーを指定しないでください。
  - x-amz-server-side-encryption
- \* SSE-C \* : 指定および管理する一意のキーでオブジェクトを暗号化する場合は、CreateMultipartUpload  
要求（および後続の各UploadPart要求）でこれら3つのヘッダーをすべて使用します。
  - x-amz-server-side-encryption-customer-algorithm:指定します AES256。
  - x-amz-server-side-encryption-customer-key:新しいオブジェクトの暗号化キーを指定しま  
す。
  - x-amz-server-side-encryption-customer-key-MD5:新しいオブジェクトの暗号化キーのMD5  
ダイジェストを指定します。



指定した暗号化キーが格納されることはありません。暗号化キーを紛失すると、対応するオブ  
ジェクトが失われます。ユーザ指定のキーを使用してオブジェクトデータを保護する前に、の  
考慮事項を確認してください "["サーバ側の暗号化を使用する"](#)"。

#### サポートされない要求ヘッダーです

次の要求ヘッダーはサポートされていません xNotImplemented

- x-amz-website-redirect-location

#### バージョン管理

マルチパートアップロードは、アップロードの開始、アップロードのリストの表示、パートのアップロード、  
アップロードしたパートのアセンブル、およびアップロードの完了の個別の処理に分けられま

す。CompleteMultipartUpload処理が実行されると、オブジェクトが作成されます（該当する場合はバージョン管理されます）。

### ListMultipartUploads

ListMultipartUploads処理を実行すると、バケットで実行中のマルチパートアップロードがリストされます。

次の要求パラメータがサポートされています。

- encoding-type
- key-marker
- max-uploads
- prefix
- upload-id-marker
- Host
- Date
- Authorization

### バージョン管理

マルチパートアップロードは、アップロードの開始、アップロードのリストの表示、パートのアップロード、アップロードしたパートのアセンブル、およびアップロードの完了の個別の処理に分けられます。CompleteMultipartUpload処理が実行されると、オブジェクトが作成されます（該当する場合はバージョン管理されます）。

### UploadPart のアップロード

UploadPart処理は、オブジェクトのマルチパートアップロード内のパートをアップロードします。

#### サポートされる要求ヘッダー

次の要求ヘッダーがサポートされています。

- Content-Length
- Content-MD5

#### サーバ側の暗号化を行うための要求ヘッダー

CreateMultipartUpload要求にSSE-C暗号化を指定した場合は、各UploadPart要求に次の要求ヘッダーも含める必要があります。

- x-amz-server-side-encryption-customer-algorithm: 指定します AES256。
- x-amz-server-side-encryption-customer-key : CreateMultipartUpload要求で指定したものと同じ暗号化キーを指定します。

- `x-amz-server-side-encryption-customer-key-MD5` : CreateMultipartUpload要求で指定したMD5ダイジェストと同じMD5ダイジェストを指定します。



指定した暗号化キーが格納されることはありません。暗号化キーを紛失すると、対応するオブジェクトが失われます。ユーザ指定のキーを使用してオブジェクトデータを保護する前に、の考慮事項を確認してください "サーバ側の暗号化を使用します"。

## バージョン管理

マルチパートアップロードは、アップロードの開始、アップロードのリストの表示、パートのアップロード、アップロードしたパートのアセンブル、およびアップロードの完了の個別の処理に分けられます。CompleteMultipartUpload処理が実行されると、オブジェクトが作成されます（該当する場合はバージョン管理されます）。

**UploadPartCopy**をクリックします

UploadPartCopy操作は、データソースとして既存のオブジェクトからデータをコピーすることによって、オブジェクトの一部をアップロードします。

UploadPartCopy処理は、Amazon S3 REST APIのすべての動作で実装されます。予告なく変更される場合があります。

この要求は、で指定されたオブジェクトデータの読み取りと書き込みを行います `x-amz-copy-source-range` StorageGRID システム内で実行する。

次の要求ヘッダーがサポートされています。

- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-if-modified-since`

## サーバ側の暗号化を行うための要求ヘッダー

CreateMultipartUpload要求にSSE-C暗号化を指定した場合は、各UploadPartCopy要求に次の要求ヘッダーも含める必要があります。

- `x-amz-server-side-encryption-customer-algorithm`: 指定します AES256。
- `x-amz-server-side-encryption-customer-key` : CreateMultipartUpload要求で指定したものと同じ暗号化キーを指定します。
- `x-amz-server-side-encryption-customer-key-MD5` : CreateMultipartUpload要求で指定したMD5ダイジェストと同じMD5ダイジェストを指定します。

ソースオブジェクトがユーザ指定のキー (SSE-C) を使用して暗号化されている場合は、オブジェクトを復号化してコピーできるように、UploadPartCopy要求に次の3つのヘッダーを含める必要があります。

- `x-amz-copy-source-server-side-encryption-customer-algorithm`: 指定します AES256。
- `x-amz-copy-source-server-side-encryption-customer-key`: ソースオブジェクトの作成時に指

## 定した暗号化キーを指定します

- `x-amz-copy-source-server-side-encryption-customer-key-MD5`: ソースオブジェクトの作成時に指定したMD5ダイジェストを指定します。



指定した暗号化キーが格納されることはありません。暗号化キーを紛失すると、対応するオブジェクトが失われます。ユーザ指定のキーを使用してオブジェクトデータを保護する前に、の考慮事項を確認してください "サーバ側の暗号化を使用します"。

## バージョン管理

マルチパートアップロードは、アップロードの開始、アップロードのリストの表示、パートのアップロード、アップロードしたパートのアセンブル、およびアップロードの完了の個別の処理に分けられます。CompleteMultipartUpload処理が実行されると、オブジェクトが作成されます（該当する場合はバージョン管理されます）。

## エラー応答

StorageGRID システムでは、該当する S3 REST API の標準のエラー応答をすべてサポートしています。また、StorageGRID の実装では、カスタム応答もいくつか追加されています。

### サポートされている S3 API のエラーコード

名前	HTTPステータス
アクセスが拒否されました	403 禁止
BadDigest の略	400 不正な要求です
BucketAlreadyExists のようになりました	409 競合
BucketNotEmpty のように入力します	409 競合
IncompleteBody	400 不正な要求です
内部エラー	500 Internal Server Error (内部サーバエラー)
InvalidAccessKeyId	403 禁止
アンヴァリッドドキュメント	400 不正な要求です
InvalidBucketName の略	400 不正な要求です
InvalidBucketState の場合	409 競合
InvalidDigest の略	400 不正な要求です

名前	HTTPステータス
InvalidEncryptionAlgorithmError	400 不正な要求です
InvalidPart	400 不正な要求です
InvalidPartOrder	400 不正な要求です
InvalidRange : 無効な範囲	416 リクエストされた範囲が適合しません
InvalidRequest	400 不正な要求です
InvalidStorageClass	400 不正な要求です
InvalidTag	400 不正な要求です
InvalidURI	400 不正な要求です
KeyTooLong の 2 つのグループがあります	400 不正な要求です
MalformedXML の場合	400 不正な要求です
MetadataTooLarge	400 不正な要求です
MethodNotAllowed のように入力します	405 メソッドは許可されていません
MissingContentLength ( MissingContentLength )	411 長さが必要です
MissingRequestBodyError	400 不正な要求です
MissingSecurityHeader	400 不正な要求です
NoSuchBucket	404 が見つかりません
NoSuchKey	404 が見つかりません
NoSuchUpload	404 が見つかりません
実装なし	501 は実装されていません
NoSuchBucketPolicy のようになります	404 が見つかりません
ObjectLockConfigurationNotFoundError	404 が見つかりません

名前	HTTPステータス
PreconditionalFailed	412 事前条件が失敗しました
RequestTimeTooSkewed	403 禁止
サービスを利用できません	503 Service Unavailable ( 503 サービスが利用でき
SignatureDoesNotMatch のように指定します	403 禁止
TooManyBuckets	400 不正な要求です
UserKeyMustBeSpecified	400 不正な要求です

#### StorageGRID カスタムのエラーコード

名前	説明	HTTPステータス
XBucketLifecycleNotAllowed のようになりました	バケットライフサイクル設定は従来の準拠バケットには適用されません	400 不正な要求です
XBucketPolicyParseException	受信したバケットポリシー JSON を解析できませんでした。	400 不正な要求です
XCompliConflict	準拠設定が古いため、処理が拒否されました。	403 禁止
XCompliReducedRedundancyForbidden	レガシー準拠バケットでは冗長性の低下は許可されません	400 不正な要求です
XMaxBucketPolicyLengthExceeded ( XMaxBucketLengthExceeded )	ポリシーが許容される最大バケットポリシー長を超えています。	400 不正な要求です
XMissingInternalRequestHeader	内部要求のヘッダーがありません。	400 不正な要求です
XNoSuchBucketCompliance です	指定したバケットで従来の準拠が有効になっていません。	404 が見つかりません
XNotAcceptable	要求に含まれている Accept ヘッダーの 1 つ以上を満たすことができませんでした。	406 は許容されません
XNotImplemented	指定した要求の処理には、実装されていない機能が含まれます。	501 は実装されていません

## StorageGRIDのカスタム処理

### StorageGRIDのカスタム処理：概要

StorageGRIDシステムでは、S3 REST APIに追加されるカスタム処理をサポートしています。

次の表に、StorageGRIDでサポートされるカスタム処理を示します。

操作	説明
"GET Bucket consistency"	特定のバケットに適用されている整合性を返します。
"PUT Bucket consistency"	特定のバケットに適用する整合性を設定します。
"GET Bucket last access time の場合"	特定のバケットで最終アクセス時間の更新が有効になっているか無効になっているかを返します。
"PUT Bucket last access time のように指定します"	特定のバケットの最終アクセス時間の更新を有効または無効にできます。
"バケットのメタデータ通知設定を削除します"	特定のバケットに関連付けられているメタデータ通知設定 XML を削除します。
"GET Bucket metadata notification configuration"	特定のバケットに関連付けられているメタデータ通知設定 XML を返します。
"PUT Bucket metadata notification configuration のコマンドです"	バケットのメタデータ通知サービスを設定します。
"GET Storage Usage の略"	アカウントおよびアカウントに関連付けられている各バケットで使用されているストレージの総容量が表示されます。
"廃止予定：準拠設定を使用してCreateBucket"	廃止およびサポート終了：準拠を有効にした新しいバケットを作成できなくなりました。
"廃止予定：バケット準拠を取得します"	廃止されましたかサポートされています：既存の古い準拠バケットに対して現在有効な準拠設定を返します。
"廃止予定：PUT Bucket compliance"	廃止されましたかサポートされています：既存の古い準拠バケットの準拠設定を変更できます。

### GET Bucket consistency

GET Bucket consistency要求を使用すると、特定のバケットに適用されている整合性を確認できます。

デフォルトの整合性は、新規作成されたオブジェクトのリードアフターライトを保証するように設定されます。

この処理を完了するには、s3 : GetBucketConsistency権限またはrootアカウントが必要です。

#### 要求例

```
GET /bucket?x-ntap-sg-consistency HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

#### 応答

応答XMLで、<Consistency> は次のいずれかの値を返します。

整合性	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。
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 の場合	(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。ほとんどの場合に推奨されます。
利用可能	新規オブジェクトとオブジェクトの更新の両方について結果整合性を提供します。S3バケットの場合は、必要な場合にのみ使用します（読み取り頻度の低いログ値を含むバケットや、存在しないキーに対するHEAD処理やGET処理など）。S3 FabricPool バケットではサポートされません。

#### 応答例

```

HTTP/1.1 200 OK
Date: Fri, 18 Sep 2020 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/11.5.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<Consistency xmlns="http://s3.storagegrid.com/doc/2015-02-01/">read-after-new-write</Consistency>

```

## 関連情報

["整合性の値"](#)

### PUT Bucket consistency

PUT Bucket consistency要求では、バケットで実行される処理に適用する整合性を指定できます。

デフォルトの整合性は、新規作成されたオブジェクトのリードアフターライトを保証するように設定されます。

作業を開始する前に

この処理を完了するには、s3 : PutBucketConsistency権限またはrootアカウントが必要です。

## リクエスト

- x-ntap-sg-consistency パラメータには次のいずれかの値を指定する必要があります。

整合性	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。
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 の場合	(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。ほとんどの場合に推奨されます。

整合性	説明
利用可能	新規オブジェクトとオブジェクトの更新の両方について結果整合性を提供します。S3バケットの場合は、必要な場合にのみ使用します（読み取り頻度の低いログ値を含むバケットや、存在しないキーに対するHEAD処理やGET処理など）。S3 FabricPool バケットではサポートされません。

\*注：\*一般に、「Read-after-new-write」整合性を使用する必要があります。要求が正しく動作しない場合は、可能であればアプリケーションクライアントの動作を変更します。または、API要求ごとに整合性を指定するようにクライアントを設定します。バケットレベルの整合性は最後の手段として設定してください。

#### 要求例

```
PUT /bucket?x-ntap-sg-consistency=strong-global HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

#### 関連情報

["整合性の値"](#)

#### GET Bucket last access time の場合

GET Bucket last access time 要求を使用すると、最終アクセス時間の更新が個々のバケットで有効になっているか無効になっているかを確認できます。

この処理を完了するには、s3 : GetBucketLastAccessTime権限またはrootアカウントが必要です。

#### 要求例

```
GET /bucket?x-ntap-sg-lastaccesstime HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

#### 応答例

次の例では、バケットの最終アクセス時間の更新が有効になっています。

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/10.3.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<LastAccessTime xmlns="http://s3.storagegrid.com/doc/2015-02-01/">enabled
</LastAccessTime>
```

### PUT Bucket last access time のように指定します

PUT Bucket last access time 要求を使用すると、最終アクセス時間の更新を個々のバケットで有効または無効にできます。最終アクセス時間の更新を無効にするとパフォーマンスが向上します。バージョン 10.3.0 以降で作成されたバケットに対しては、いずれもデフォルトで無効になります。

この処理を完了するには、バケットのs3 : PutBucketLastAccessTime権限またはrootアカウントが必要です。

 StorageGRID バージョン 10.3 以降では、すべての新規バケットで最終アクセス時間の更新がデフォルトで無効になります。以前のバージョンの StorageGRID で作成されたバケットにこの新たなデフォルトの動作を適用する場合は、対象となるバケットごとに最終アクセス時間の更新を無効にする必要があります。最終アクセス時間の更新を有効または無効にするには、PUT Bucket last access time要求を使用するか、Tenant Managerのバケットの詳細ページを使用します。を参照してください ["最終アクセス日時の更新を有効または無効にします"](#)。

バケットで最終アクセス時間の更新が無効になっている場合、バケットの処理の動作は次のようにになります。

- GetObject、GetObjectAcl、GetObjectTagging、HeadObjectの各要求では、最終アクセス時間は更新されません。オブジェクトは、情報ライフサイクル管理（ILM）評価のキューに追加されません。
- メタデータのみを更新するCopyObject要求とPutObjectTagging要求では、最終アクセス時間も更新されます。オブジェクトは ILM 評価のキューに追加されます。
- ソースバケットで最終アクセス時間の更新が無効になっている場合、CopyObject要求でソースバケットの最終アクセス時間が更新されません。コピーされたオブジェクトは、ソースバケットの ILM 評価のキューに追加されません。ただし、デスティネーションについては、CopyObject要求で常に最終アクセス時間が更新されます。オブジェクトのコピーは、ILM 評価のキューに追加されます。
- CompleteMultipartUpload要求で最終アクセス時間が更新されます。完了したオブジェクトは、ILM 評価のキューに追加されます。

例をリクエストする

この例では、バケットの最終アクセス時間を有効にしています。

```
PUT /bucket?x-ntap-sg-lastaccesstime=enabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

この例では、バケットの最終アクセス時間を無効にしています。

```
PUT /bucket?x-ntap-sg-lastaccesstime=disabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

バケットのメタデータ通知設定を削除します

**DELETE Bucket metadata notification configuration** 要求では、設定 XML を削除することで、個々のバケットで検索統合サービスを無効化できます。

この処理を完了するには、バケットのs3 : DeleteBucketMetadataNotification権限またはrootアカウントが必要です。

要求例

次の例は、バケットの検索統合サービスを無効にする方法を示しています。

```
DELETE /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

### **GET Bucket metadata notification configuration**

**GET Bucket metadata notification configuration** 要求では、個々のバケットで検索統合を設定するために使用する設定 XML を読み出すことができます。

この処理を完了するには、s3 : GetBucketMetadataNotification権限またはrootアカウントが必要です。

要求例

次の要求は、というバケットのメタデータ通知設定を読み出します bucket。

```
GET /bucket?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

## 応答

応答の本文には、バケットのメタデータ通知設定が含まれます。メタデータ通知設定では、バケットでの検索統合の設定を確認できます。つまり、どのオブジェクトにインデックスが付けられ、そのオブジェクトメタデータがどのエンドポイントに送信されるかを確認できます。

```
<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>
```

各メタデータ通知設定には、1つ以上のルールが含まれています。各ルールは、環境がオブジェクトを指定し、StorageGRIDがオブジェクト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。デスティネーションは、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。

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。

名前	説明	必須
ルール	<p>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。</p> <p>プレフィックスが重複しているルールは拒否されます。</p> <p>MetadataNotificationConfiguration 要素に含まれています。</p>	はい。
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。

名前	説明	必須
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。

## 応答例

### 間に含まれるXML

<MetadataNotificationConfiguration></MetadataNotificationConfiguration> タグは、バケットに対して検索統合エンドポイントとの統合がどのように設定されているかを示します。次の例では、という名前のElasticsearchインデックスにオブジェクトメタデータが送信されています current と入力します 2017 という名前のAWSドメインでホストされている records。

```
HTTP/1.1 200 OK
Date: Thu, 20 Jul 2017 18:24:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/11.0.0
x-amz-request-id: 3832973499
Content-Length: 264
Content-Type: application/xml

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>Enabled</Status>
    <Prefix>2017</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-
1:3333333:domain/records/current/2017</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

## 関連情報

["テナントアカウントを使用する"](#)

## PUT Bucket metadata notification configuration のコマンドです

PUT Bucket metadata notification configuration 要求を使用すると、個々のバケットで検索統合サービスを有効化できます。要求の本文に含めるメタデータ通知設定 XML では、デスティネーション検索インデックスにメタデータを送信するオブジェクトを指定します。

この処理を完了するには、バケットのs3 : PutBucketMetadataNotification権限またはrootアカウントが必要です。

## リクエスト

要求の本文にメタデータ通知設定が含まれている必要があります。各メタデータ通知設定には、1つ以上のルールが含まれています。各ルールは、環境がオブジェクトを指定し、StorageGRIDがオブジェクト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に追加します /videos 別のノードに移動します

プレフィックスが重複している設定は有効ではなく、送信時に拒否されます。たとえば、プレフィックスがのオブジェクト用のルールを1つ含む設定などです 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 許可されません。

デスティネーションは、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。エンドポイントは、メタデータ通知設定が送信されたときに存在している必要があります。存在していない場合、要求がとして失敗します 400 Bad Request。エラーメッセージ：Unable to save the metadata notification (search) policy. The specified endpoint URN does not exist: URN.

```
<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。
ID	ルールの一意の識別子。  Rule 要素に含まれています。	いいえ

名前	説明	必須
ステータス	<p>Status には「 Enabled 」または「 Disabled 」を指定できます。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。

例をリクエストする

次の例は、バケットの検索統合を有効にする方法を示しています。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。

```
PUT /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

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

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。

```

PUT /graphics?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

<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>

```

#### 検索統合サービスで生成される JSON

バケットで検索統合サービスを有効にすると、オブジェクトのメタデータまたはタグの追加、更新、削除が行われるたびに、JSON ドキュメントが生成されてデスティネーションエンドポイントに送信されます。

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

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

メタデータ通知に含まれているオブジェクトメタデータ

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

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

を入力します	項目名	説明
バケットとオブジェクトの情報	バケット	バケットの名前
バケットとオブジェクトの情報	キーを押します	オブジェクトキーの名前
バケットとオブジェクトの情報	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
バケットとオブジェクトの情報	リージョン	たとえば、バケットのリージョンのように指定します us-east-1
システムメタデータ	サイズ	HTTP クライアントから認識できるオブジェクトのサイズ（バイト）
システムメタデータ	MD5	オブジェクトのハッシュ
ユーザメタデータ	メタデータ <i>key:value</i>	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

を入力します	項目名	説明
タグ	タグ <i>key:value</i>	オブジェクトに対して定義された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

(i) 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。ドキュメントのインデックス作成後は、インデックス内のドキュメントのフィールドタイプを編集することはできません。

#### 関連情報

["テナントアカウントを使用する"](#)

#### GET Storage Usage 要求の略

GET Storage Usage 要求を使用すると、アカウントで使用しているストレージの総容量とアカウントに関連付けられているバケットごとの使用容量を確認できます。

アカウントとそのバケットで使用されているストレージの容量は、 `x-ntap-sg-usage` クエリパラメータ。バケットによるストレージの使用量は、システムで処理される PUT 要求や DELETE 要求とは別に追跡されます。特にシステムの負荷が高い場合などは、使用量の値が要求の処理に基づく想定値と同じになるまでに少し時間がかかることがあります。

デフォルトでは、 StorageGRID は strong-global 整合性を使用して、使用状況の情報を取得します。strong-global整合性を達成できない場合、 StorageGRID はstrong-site整合性で使用状況情報を取得しようとします。

この処理を完了するには、 s3 : ListAllMyBuckets 権限またはrootアカウントが必要です。

#### 要求例

```
GET /?x-ntap-sg-usage HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

#### 応答例

次の例は、 2 つのバケットに 4 つのオブジェクトと 12 バイトのデータが格納されたアカウントです。各バケットには、 2 つのオブジェクトと 6 バイトのデータが格納されています。

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 00:49:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/10.2.0
x-amz-request-id: 727237123
Content-Length: 427
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<UsageResult xmlns="http://s3.storagegrid.com/doc/2015-02-01">
<CalculationTime>2014-11-19T05:30:11.000000Z</CalculationTime>
<ObjectCount>4</ObjectCount>
<DataBytes>12</DataBytes>
<Buckets>
<Bucket>
<Name>bucket1</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
<Bucket>
<Name>bucket2</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
</Buckets>
</UsageResult>
```

## バージョン管理

には、格納されているすべてのオブジェクトバージョンが関連します ObjectCount および DataBytes 応答の値。削除マーカーはに追加されません ObjectCount 合計。

## 関連情報

### ["整合性の値"](#)

従来の準拠のためのバケット要求が廃止されました

従来の準拠のためのバケット要求が廃止されました

従来の準拠機能で作成されたバケットの管理には、 StorageGRID S3 REST API の使用が必要になる場合があります。

コンプライアンス機能は廃止されました

以前のバージョンの StorageGRID で提供されていた StorageGRID 準拠機能は廃止され、 S3 オブジェクトロックに置き換えられました。

グローバル準拠設定を有効にしている場合は、StorageGRID 11.6 でグローバル S3 オブジェクトロック設定が有効になっています。準拠を有効にした新しいバケットは作成できなくなりました。ただし、必要に応じて、StorageGRID S3 REST API を使用して、従来の準拠バケットを管理できます。

- "S3 REST APIを使用してS3オブジェクトロックを設定します"
- "ILM を使用してオブジェクトを管理する"
- "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"

廃止された準拠要求：

- "DEPRECATED - PUT Bucket request modifications for compliance"

SGCompliance XML 要素は廃止されました。これまで、この StorageGRID カスタム要素を PUT Bucket 要求のオプションの XML 要求の本文に含めて準拠バケットを作成できました。

- "廃止予定- GET Bucket compliance"

GET Bucket compliance 要求は廃止されました。ただし、既存のレガシー準拠バケットに対して現在有効な準拠設定を引き続き確認することができます。

- "廃止されました。PUT Bucket compliance"

PUT Bucket compliance 要求は廃止されました。ただし、この要求を引き続き使用して、既存のレガシー準拠バケットの準拠設定を変更できます。たとえば、既存のバケットをリーガルホールドの対象にしたり、バケットの保持期間を長くしたりできます。

廃止予定：準拠のためのCreateBucket要求の変更

SGCompliance XML 要素は廃止されました。以前は、このStorageGRIDカスタム要素をCreateBucket要求のオプションのXML要求本文に含めて、準拠バケットを作成できました。

以前のバージョンの StorageGRID で提供されていた StorageGRID 準拠機能は廃止され、S3 オブジェクトロックに置き換えられました。詳細については、次を参照してください。

- ①
- "S3 REST APIを使用してS3オブジェクトロックを設定します"
  - "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"

準拠を有効にした新しいバケットを作成することはできなくなりました。準拠のためにCreateBucket要求の変更を使用して新しい準拠バケットを作成しようとすると、次のエラーメッセージが返されます。

The Compliance feature is deprecated.

Contact your StorageGRID administrator if you need to create new Compliant buckets.

## 廃止予定：GET Bucket compliance要求

GET Bucket compliance要求は廃止されました。ただし、既存のレガシー準拠バケットに対して現在有効な準拠設定を引き続き確認することができます。

以前のバージョンの StorageGRID で提供されていた StorageGRID 準拠機能は廃止され、S3 オブジェクトロックに置き換えられました。詳細については、次を参照してください。



- "S3 REST APIを使用してS3オブジェクトロックを設定します"
- "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"

この処理を完了するには、s3 : GetBucketCompliance権限またはrootアカウントが必要です。

## 要求例

次の要求例では、という名前のバケットの準拠設定を確認できます mybucket。

```
GET /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

## 応答例

応答XMLで、<SGCompliance> バケットで有効な準拠設定が表示されます。次の応答例では、バケットの準拠設定が示されており、各オブジェクトはグリッドに取り込まれてから 1 年間（525、600 分）保持されます。このバケットには現在リーガルホールドはありません。各オブジェクトは 1 年後に自動的に削除されます。

```
HTTP/1.1 200 OK
Date: date
Connection: connection
Server: StorageGRID/11.1.0
x-amz-request-id: request ID
Content-Length: length
Content-Type: application/xml

<SGCompliance>
  <RetentionPeriodMinutes>525600</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

名前	説明
RetentionPeriodMinutes です	このバケットに追加されたオブジェクトの保持期間を分で指定します。保持期間は、オブジェクトがグリッドに取り込まれたときからの期間です。
LegalHold のようになります	<ul style="list-style-type: none"> <li>True : このバケットは、現在リーガルホールドの対象です。このバケット内のオブジェクトは、保持期間が過ぎても、リーガルホールドが解除されるまで削除できません。</li> <li>False : このバケットは、現在リーガルホールドの対象ではありません。このバケット内のオブジェクトは、保持期間が過ぎたら削除できます。</li> </ul>
自動削除	<ul style="list-style-type: none"> <li>True : このバケット内のオブジェクトは、バケットがリーガルホールドの対象である場合を除き、保持期間が過ぎると自動的に削除されます。</li> <li>false : このバケット内のオブジェクトは、保持期間が過ぎても自動的には削除されません。これらのオブジェクトを削除する必要がある場合は、手動で削除する必要があります。</li> </ul>

## エラー応答

バケットが準拠バケットとして作成されていない場合、応答のHTTPステータスコードはになります 404 Not Found`を返します `XNoSuchBucketCompliance。

## 廃止予定：PUT Bucket compliance 要求

PUT Bucket compliance 要求は廃止されました。ただし、この要求を引き続き使用して、既存のレガシー準拠バケットの準拠設定を変更できます。たとえば、既存のバケットをリーガルホールドの対象にしたり、バケットの保持期間を長くしたりできます。

以前のバージョンの StorageGRID で提供されていた StorageGRID 準拠機能は廃止され、S3 オブジェクトロックに置き換えられました。詳細については、次を参照してください。



- "S3 REST APIを使用してS3オブジェクトロックを設定します"
- "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"

この処理を完了するには、s3 : PutBucketCompliance権限またはrootアカウントが必要です。

PUT Bucket compliance 要求を発行する際は、準拠設定のすべてのフィールドに値を指定する必要があります。

## 要求例

次の要求例では、という名前のバケットの準拠設定を変更します mybucket。この例では、のオブジェクトが表示されています mybucket オブジェクトがグリッドに取り込まれてから1年間ではなく2年間（1、051、200分）保持されます。このバケットにリーガルホールドはありません。各オブジェクトは2年後に自動的

に削除されます。

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Content-Length: 152

<SGCompliance>
  <RetentionPeriodMinutes>1051200</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

名前	説明
RetentionPeriodMinutes です	<p>このバケットに追加されたオブジェクトの保持期間を分で指定します。保持期間は、オブジェクトがグリッドに取り込まれたときからの期間です。</p> <p>重要 RetentionPeriodMinutesに新しい値を指定する場合は、バケットの現在の保持期間以上の値を指定する必要があります。バケットの保持期間の設定後は、その値を減らすことはできず、増やすことしかできません。</p>
LegalHold のようになります	<ul style="list-style-type: none"><li>True : このバケットは、現在リーガルホールドの対象です。このバケット内のオブジェクトは、保持期間が過ぎても、リーガルホールドが解除されるまで削除できません。</li><li>False : このバケットは、現在リーガルホールドの対象ではありません。このバケット内のオブジェクトは、保持期間が過ぎたら削除できます。</li></ul>
自動削除	<ul style="list-style-type: none"><li>True : このバケット内のオブジェクトは、バケットがリーガルホールドの対象である場合を除き、保持期間が過ぎると自動的に削除されます。</li><li>false : このバケット内のオブジェクトは、保持期間が過ぎても自動的には削除されません。これらのオブジェクトを削除する必要がある場合は、手動で削除する必要があります。</li></ul>

### 準拠設定の整合性

PUT Bucket compliance 要求によって S3 バケットの準拠設定を更新すると、StorageGRID は、グリッド全体のバケットのメタデータを更新しようとします。デフォルトでは、StorageGRIDは\* strong-global \*整合性を使用して、バケットのメタデータを含むすべてのデータセンターサイトとストレージノードで、変更された準拠設定のリードアフターライト整合性を保証します。

データセンターサイトまたはサイトの複数のストレージノードが利用できないために、StorageGRIDが\* strong-global \*整合性を達成できない場合、応答のHTTPステータスコードは次のようにになります。 503

この応答を受け取った場合は、必要なストレージサービスをできるだけ早く利用可能にするために、グリッド管理者に問い合わせる必要があります。グリッド管理者が各サイトで十分な数のストレージノードを利用可能にできない場合、テクニカルサポートから\* strong-site \*整合性を強制的に適用して、失敗した要求を再試行するよう指示されることがあります。



テクニカルサポートから指示され、このレベルを使用した場合の潜在的な影響を理解している場合を除き、PUT bucket complianceで\* strong-site \*整合性を強制的に実行しないでください。

整合性を\* strong-site \*に減らすと、StorageGRIDは、サイト内のクライアント要求についてのみ、更新された準拠設定のリードアフターライト整合性を保証します。そのため、すべてのサイトおよびストレージノードが利用可能になるまでの間、StorageGRID システムにはこのバケットに対して複数の異なる設定が一時的に存在することになる場合があります。整合性のない設定を使用すると、予期せぬ望ましくない動作が生じる可能性がありますたとえば、バケットをリーガルホールドの対象にする場合に、より低い整合性を強制的に適用すると、一部のデータセンターサイトでバケットの以前の準拠設定（リーガルホールドのオフ）が引き続き有効になることがあります。したがって、リーガルホールドの対象と思われるオブジェクトは、保持期間が経過すると、ユーザによって削除される場合と、AutoDelete によって削除される場合があります。

strong-site \*整合性を強制的に使用するには、PUT Bucket compliance要求を再実行し、Consistency-Control HTTP要求ヘッダー。

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Consistency-Control: strong-site
```

## エラー応答

- バケットが準拠バケットとして作成されていない場合、応答のHTTPステータスコードはになります 404 Not Found。
- 状況 RetentionPeriodMinutes 要求がバケットの現在の保持期間よりも短い場合、HTTPステータスコードはになります 400 Bad Request。

## 関連情報

["廃止：準拠のための PUT Bucket 要求の変更"](#)

## バケットとグループのアクセスポリシー

### バケットとグループのアクセスポリシーを使用

StorageGRID では、Amazon Web Services ( AWS ) ポリシー言語を使用して、S3 テナントによるバケットおよびバケット内のオブジェクトへのアクセスを制御できます。StorageGRID システムには、S3 REST API ポリシー言語のサブセットが実装されています。S3 API のアクセスポリシーは JSON 形式で記述されます。

### アクセスポリシーの概要

StorageGRID では 2 種類のアクセスポリシーがサポートされています。

- バケットポリシー。S3 APIのGetBucketPolicy、PutBucketPolicy、およびDeleteBucketPolicyの各処理を使用して管理されます。バケットポリシーはバケットに関連付けられ、バケットとそのオブジェクトへのバケット所有者アカウントやその他のアカウントのユーザによるアクセスを制御するために使用されます。バケットポリシー環境は1つのバケットのみで、場合によっては複数のグループに分かれています。
- \* グループポリシー \*。Tenant Manager またはテナント管理 API を使用して設定します。グループポリシーはアカウントのグループに関連付けられ、そのアカウントが所有する特定のリソースにそのグループがアクセスできるように設定されます。グループポリシー環境は1つのグループに限定され、場合によっては複数のバケットに適用されます。



グループポリシーとバケットポリシーの優先度に違いはありません。

StorageGRID のバケットとグループのポリシーは、Amazon が定義している特定の文法に従って記述されます。各ポリシーは一連のステートメントからなり、各ステートメントは次の要素で構成されます。

- ステートメント ID (SID) (オプション)
- 効果
- プリンシパル / NotPrincipal
- リソース / メモリソース
- アクション / NotAction
- Condition (オプション)

次の構造を使用して、権限を指定するポリシーステートメントが構築されます。<Effect> を付与して、<Condition> に該当する場合に <Principal> に <Resource> に対する <Action> の実行を許可または拒否します。

各ポリシー要素は、特定の機能に使用されます。

要素 (Element)	説明
SID	Sid 要素はオプションです。SID は、ユーザの概要としてのみ使用されます。StorageGRID システムに格納はされますが、システムで解釈されません。
効果	Effect 要素では、指定した処理を許可するか拒否するかを指定します。Action 要素でサポートされるキーワードを使用して、バケットやオブジェクトで許可（または拒否）する処理を指定する必要があります。
プリンシパル / NotPrincipal	ユーザ、グループ、およびアカウントに特定のリソースへのアクセスと特定の操作の実行を許可できます。要求に S3 の署名が含まれていない場合は、ワイルドカード文字 (*) をプリンシパルとして指定することで匿名アクセスが許可されます。デフォルトでは、アカウントが所有するリソースへのアクセスは root アカウントにのみ許可されます。  Principal 要素を指定する必要があるのはバケットポリシーだけです。グループポリシーの場合は、ポリシーが関連付けられたグループが暗黙的にプリンシパルになります。

要素 ( Element )	説明
リソース / メモリソース	Resource 要素では、バケットとオブジェクトを指定します。Amazon リソースネーム (ARN) を使用してリソースを指定し、バケットやオブジェクトに対する権限を許可または拒否することができます。
アクション / NotAction	権限は Action 要素と Effect 要素の 2 つで構成されます。グループがリソースを要求すると、リソースへのアクセスが許可または拒否されます。権限を明示的に割り当てていないかぎりアクセスは拒否されますが、明示的な拒否を使用して別のポリシーで付与された権限を上書きすることができます。
条件	Condition 要素はオプションです。条件を使用すると、ポリシーを適用する条件を示す式を作成できます。

Action 要素では、ワイルドカード文字 (\*) を使用してすべての処理または処理のサブセットを指定できます。たとえば、次の Action の値は、s3 : GetObject、s3 : PutObject、s3 : DeleteObject などの権限に一致します。

```
s3:*Object
```

Resource 要素では、ワイルドカード文字 (\\*) および (?) を使用できます。アスタリスク (\*) は 0 文字以上の文字に一致し、疑問符 (?) は 0 文字以上の文字に一致します。任意の 1 文字に一致します。

Principal要素では、匿名アクセスを設定してすべてのユーザに権限を付与する場合を除き、ワイルドカード文字はサポートされません。たとえば、Principal の値としてワイルドカード (\*) を設定します。

```
"Principal": "*"
```

```
"Principal": {"AWS": "*"} 
```

次の例では、Effect、Principal、Action、および Resource の各要素を使用して記述します。次の例は、「許可」の効果を使用してプリンシパル、adminグループを指定したバケットポリシーのステートメントを示しています federated-group/admin 財務グループなどです federated-group/finance、アクションを実行する権限 s3>ListBucket をバケットにインストールします mybucket そしてアクション s3:GetObject そのバケット内のすべてのオブジェクト。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::27233906934684427525:federated-group/admin",
          "arn:aws:iam::27233906934684427525:federated-group/finance"
        ]
      },
      "Action": [
        "s3>ListBucket",
        "s3GetObject"
      ],
      "Resource": [
        "arn:aws:iam:s3:::mybucket",
        "arn:aws:iam:s3:::mybucket/*"
      ]
    }
  ]
}
```

バケットポリシーのサイズの上限は 20、480 バイトで、グループポリシーのサイズの上限は 5、120 バイトです。

#### ポリシーノセイコウセイ

デフォルトでは、グループポリシーに対するすべての更新の整合性レベルは結果整合性です。グループポリシーの整合性が取れた場合、ポリシーキャッシュのために変更が有効になるまでにさらに15分かかることがあります。デフォルトでは、バケットポリシーに対する更新の整合性は非常に高くなります。

バケットポリシーの更新の整合性保証は必要に応じて変更できます。たとえば、サイトが停止しているときにバケットポリシーを変更できるようにすることができます。

この場合は、を設定できます `Consistency-Control` `PutBucketPolicy` 要求のヘッダー、または `PUT Bucket consistency` 要求を使用できます。バケットポリシーの整合性が確保されると、ポリシーキャッシュのために変更が有効になるまでにさらに8秒かかることがあります。



一時的な状況を回避するために整合性の値を別の値に設定する場合は、完了後にバケットレベルの設定を元の値に戻してください。そうしないと、以降のすべてのバケット要求で変更後の設定が使用されます。

ポリシーステートメントでは **ARN** を使用します

ポリシーステートメントでは、`Principal` 要素と `Resource` 要素で ARN を使用します。

- S3 リソースの ARN の指定には次の構文を使用します。

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

- アイデンティティリソースのARN（ユーザおよびグループ）の指定には次の構文を使用します。

```
arn:aws:iam::account_id:root  
arn:aws:iam::account_id:user/user_name  
arn:aws:iam::account_id:group/group_name  
arn:aws:iam::account_id:federated-user/user_name  
arn:aws:iam::account_id:federated-group/group_name
```

その他の考慮事項：

- オブジェクトキーの一部にワイルドカードとしてアスタリスク (\*) を使用すると、0文字以上の文字に一致します。
- オブジェクトキーで指定できる国際文字は、JSON UTF-8 形式または JSON \u エスケープシーケンスを使用してエンコードする必要があります。パーセントエンコーディングはサポートされていません。

#### "RFC 2141 の URN 構文"

PutBucketPolicy処理のHTTP要求の本文は、charset=UTF-8でエンコードする必要があります。

ポリシー内のリソースを指定します

ポリシーステートメントでは、Resource要素を使用して、権限を許可または拒否するバケットやオブジェクトを指定できます。

- Resource要素はポリシーの各ステートメントに必要です。ポリシーでは、リソースは要素で示されます`Resource`または、`NotResource`除外のため。
- リソースはS3リソースのARNで指定します。例：

```
"Resource": "arn:aws:s3:::mybucket/*"
```

- オブジェクトキーの内部でポリシー変数を使用することもできます。例：

```
"Resource": "arn:aws:s3:::mybucket/home/${aws:username}/*"
```

- グループポリシーの作成時は、まだ存在しないバケットもリソースの値で指定することができます。

ポリシーでプリンシパルを指定します

ポリシーステートメントでリソースへのアクセスを許可または拒否するユーザ、グループ、またはテナントアカウントを指定するには、Principal要素を使用します。

- バケットポリシーの各ポリシーステートメントには、Principal 要素を含める必要があります。グループはプリンシパルとみなされるため、グループポリシーのポリシーステートメントではPrincipal要素は必要ありません。
- ポリシーでは、「Principal」要素または「NotPrincipal」要素（除外の場合）でプリンシパルを指定します。
- ID または ARN を使用してアカウントベースのアイデンティティを指定する必要があります。

```
"Principal": { "AWS": "account_id"}  
"Principal": { "AWS": "identity_arn" }
```

- 次の例では、テナントアカウント ID 27233906934684427525 を使用しています。この場合、root アカウントとそのすべてのユーザが含まれます。

```
"Principal": { "AWS": "27233906934684427525" }
```

- root アカウントのみを指定する場合は次のようにになります。

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:root" }
```

- 特定のフェデレーテッドユーザ（「Alex」）を指定する場合は次のようにになります。

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-user/Alex" }
```

- 特定のフェデレーテッドグループ（「Managers」）のみを指定する場合は次のようにになります。

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-group/Managers" }
```

- 匿名プリンシパルを指定する場合は次のようにになります。

```
"Principal": "*"
```

- あいまいさを排除するために、ユーザ名の代わりに UUID を使用できます。

```
arn:aws:iam::27233906934684427525:user-uuid/de305d54-75b4-431b-adb2-eb6b9e546013
```

たとえば、Alexが組織とユーザ名を退職するとします Alex が削除されました。新しいAlexが組織に参加

し、同じが割り当てられている場合 Alex ユーザ名。元のユーザに付与された権限が、新しいユーザに意図せず継承されることがあります。

- バケットポリシーの作成時は、まだ存在しないグループ / ユーザの名前もプリンシパルの値で指定することができます。

#### ポリシーで権限を指定します

ポリシーでは、Action 要素を使用してリソースに対する権限を許可または拒否します。ポリシーには、「Action」要素で示される一連の権限、または除外する「NotAction」要素で指定できる一連の権限があります。それぞれが特定の S3 REST API 処理に対応しています。

次の表に、バケットに適用される権限とオブジェクトに適用される権限を示します。

- Amazon S3では、PutBucketReplicationとDeleteBucketReplicationの両方のアクションにs3 : PutReplicationConfiguration権限が使用されるようになりました。StorageGRIDでは、元のAmazon S3仕様に一致する個別の権限が各アクションに使用されます。
- DELETEは、PUTを使用して既存の値を上書きした場合に実行されます。

#### バケットに適用される権限

権限	S3 REST API の処理	StorageGRID のカスタム
S3 : CreateBucket を指定します	CreateBucketを選択します	はい。 注：グループポリシーでのみ使用します。
S3 : DeleteBucket	DeleteBucketの場合	
S3 : DeleteBucketMetadataNotification	バケットのメタデータ通知設定を削除します	はい。
S3 : DeleteBucketPolicy	DeleteBucketPolicyのようになります	
S3 : DeleteReplicationConfiguration	DeleteBucketReplication	○ (PUTとDELETEに別々の権限を設定)
S3 : GetBucketAcl	GetBucketAcl	
S3 : GetBucketCompliance	GET Bucket compliance (廃止)	はい。
S3 : GetBucketConsistency	GET Bucket consistency	はい。

権限	S3 REST API の処理	StorageGRID のカスタム
S3 : GetBucketCORS	GetBucketCors	
S3 : GetEncryptionConfiguration	GetBucketEncryptionの略	
S3 : GetBucketLastAccessTime	GET Bucket last access time の場合	はい。
S3 : GetBucketLocation	GetBucketLocation	
S3 : GetBucketMetadataNotification	GET Bucket metadata notification configuration	はい。
S3 : GetBucketNotification	GetBucketNotificationConfigurationを参照してください	
S3 : GetBucketObjectLockConfiguration	GetObjectLockConfigurationの略	
S3 : GetBucketPolicy	GetBucketPolicyのようになります	
S3 : GetBucketTagging	GetBucketTagging	
S3 : GetBucketVersioning	GetBucketVersioningの各ノードの設定	
S3 : GetLifecycleConfiguration	GetBucketLifecycleConfiguration	
S3 : GetReplicationConfiguration	GetBucketReplicationの略	
S3 : ListAllMyBuckets	<ul style="list-style-type: none"> <li>• ListBuckets</li> <li>• GET Storage Usage の略</li> </ul>	<ul style="list-style-type: none"> <li>◦ (GET Storage Usage)。</li> </ul> <p>注：グループポリシーでのみ使用します。</p>
S3 : ListBucket	<ul style="list-style-type: none"> <li>• ListObjects</li> <li>• ヘッドバケット</li> <li>• RestoreObject</li> </ul>	
S3 : ListBucketMultipartUploads	<ul style="list-style-type: none"> <li>• ListMultipartUploads</li> <li>• RestoreObject</li> </ul>	
S3 : ListBucketVersions	GET Bucket versions (バケットバージョンの取得	

権限	S3 REST API の処理	StorageGRID のカスタム
S3 : PutBucketCompliance	PUT Bucket compliance (廃止)	はい。
S3 : PutBucketConsistency	PUT Bucket consistency	はい。
S3 : PutBucketCORS	<ul style="list-style-type: none"> <li>• DeleteBucketCors†</li> <li>• PutBucketCorsの略</li> </ul>	
S3 : PutEncryptionConfiguration	<ul style="list-style-type: none"> <li>• DeleteBucketEncryption</li> <li>• PutBucketEncryptionの略</li> </ul>	
S3 : PutBucketLastAccessTime	PUT Bucket last access time のように指定します	はい。
S3 : PutBucketMetadataNotification	PUT Bucket metadata notification configuration のコマンドです	はい。
S3 : PutBucketNotification	PutBucketNotificationConfigurationの略	
S3 : PutBucketObjectLockConfiguration	<ul style="list-style-type: none"> <li>• を使用してCreateBucketを作成します。 <code>x-amz-bucket-object-lock-enabled: true</code> 要求ヘッダー (s3 : CreateBucket権限も必要)</li> <li>• PutObjectLockConfigurationの略</li> </ul>	
S3 : PutBucketPolicy	PutBucketPolicyのように指定します	
S3 : PutBucketTagging	<ul style="list-style-type: none"> <li>• DeleteBucketTagging†</li> <li>• PutBucketTaggingの略</li> </ul>	
S3 : PutBucketVersioning	PutBucketVersioningの各ノードの設定	
S3 : PutLifecycleConfiguration	<ul style="list-style-type: none"> <li>• DeleteBucketLifecycle†</li> <li>• PutBucketLifecycleConfigurationの略</li> </ul>	
S3 : PutReplicationConfiguration	PutBucketReplicationの略	<ul style="list-style-type: none"> <li>○ (PUTとDELETEに別々の権限を設定)</li> </ul>

オブジェクトに適用される権限

権限	S3 REST API の処理	StorageGRID のカスタム
S3 : AbortMultipartUpload	<ul style="list-style-type: none"> <li>AbortMultipartUpload の略</li> <li>RestoreObject</li> </ul>	
S3 : Bypassガバナー 保持	<ul style="list-style-type: none"> <li>deleteObject</li> <li>オブジェクトを削除します</li> <li>PutObjectRetentionの略</li> </ul>	
S3 : DeleteObject	<ul style="list-style-type: none"> <li>deleteObject</li> <li>オブジェクトを削除します</li> <li>RestoreObject</li> </ul>	
S3 : DeleteObjectTagging	DeleteObjectTagging の場合	
S3 : DeleteObjectVersionTagging	DeleteObjectTagging (オブジェクトの特定のバージョン)	
S3 : DeleteObjectVersion	deleteObject (オブジェクトの特定のバージョン)	
S3 : GetObject	<ul style="list-style-type: none"> <li>GetObject</li> <li>HeadObject (ヘッドオブジェクト)</li> <li>RestoreObject</li> <li>SelectObjectContent の順に選択します</li> </ul>	
S3 : GetObjectAcl	GetObjectAcl	
S3 : GetObjectLegalHold	GetObjectLegalHold	
S3 : GetObjectRetention	GetObjectRetentionの略	
S3 : GetObjectTagging	GetObjectTagging の 2 つの機能を	
S3 : GetObjectVersionTagging	GetObjectTagging (オブジェクトの特定のバージョン)	
S3 : GetObjectVersion	GetObject (オブジェクトの特定のバージョン)	
S3 : ListMultipartUploadParts	ListParts、RestoreObject	

権限	S3 REST API の処理	StorageGRID のカスタム
S3 : PutObject	<ul style="list-style-type: none"> <li>PutObject</li> <li>CopyObject</li> <li>RestoreObject</li> <li>CreateMultipartUpload を実行します</li> <li>CompleteMultipartUpload</li> <li>UploadPart のアップロード</li> <li>UploadPartCopyをクリックします</li> </ul>	
S3 : PutObjectLegalHold	PutObjectLegalHold	
S3 : PutObjectRetention	PutObjectRetentionの略	
S3 : PutObjectTagging	PutObjectTagging の 2 つのグループが	
S3 : PutObjectVersionTagging	PutObjectTagging (オブジェクトの特定のバージョン)	
S3 : PutOverwriteObject	<ul style="list-style-type: none"> <li>PutObject</li> <li>CopyObject</li> <li>PutObjectTagging の 2 つのグループが</li> <li>DeleteObjectTagging の場合</li> <li>CompleteMultipartUpload</li> </ul>	はい。
S3 : RestoreObject	RestoreObject	

#### PutOverwriteObject 権限を使用します

s3 : PutOverwriteObject 権限は、オブジェクトの作成または更新を行う環境 处理のカスタムの StorageGRID 権限です。この権限の設定により、オブジェクトのデータ、ユーザ定義メタデータ、または S3 オブジェクトのタグをクライアントが上書きできるかどうかが決まります。

この権限で可能な設定は次のとおりです。

- \* allow \* : クライアントはオブジェクトを上書きできます。これがデフォルト設定です。
- Deny:** クライアントはオブジェクトを上書きできません。PutOverwriteObject 権限が Deny に設定されている場合の動作は次のとおりです。
  - 同じパスで既存のオブジェクトが見つかった場合は、次の手順を実行します。
    - オブジェクトのデータ、ユーザ定義メタデータ、またはS3オブジェクトのタグを上書きすることはできません。
    - 実行中の取り込み処理はすべてキャンセルされ、エラーが返されます。

- S3のバージョン管理が有効になっている場合は、Denyに設定すると、PutObjectTagging処理またはDeleteObjectTagging処理によってオブジェクトとその最新でないバージョンのTagSetが変更されなくなります。
  - 既存のオブジェクトが見つからない場合は、この権限の設定は影響しません。
- この権限がない場合、Allowが設定されたものと同じ結果になります。



現在のS3ポリシーで上書きが許可されていて、PutOverwriteObject権限がDenyに設定されている場合、オブジェクトのデータ、ユーザ定義メタデータ、またはオブジェクトのタグをクライアントが上書きすることはできません。また、[Prevent client modification]\*チェックボックスが選択されている場合（configuration > Security settings > Network and objects \*）、この設定はPutOverwriteObject権限の設定よりも優先されます。

ポリシーの条件を指定します

条件は、ポリシーが有効になるタイミングを定義します。条件は演算子とキーと値のペアで構成されます。

条件はキーと値のペアを使用して評価されます。Condition要素には複数の条件を指定でき、各条件には複数のキーと値のペアを含めることができます。条件ブロックの形式は次のとおりです。

```
Condition: {
  condition_type: {
    condition_key: condition_values
  }
}
```

次の例では、IpAddress条件で SourceIp条件キーを使用しています。

```
"Condition": {
  "IpAddress": {
    "aws:SourceIp": "54.240.143.0/24"
    ...
  },
  ...
}
```

サポートされる条件演算子は次の

条件演算子は次のように分類されます。

- 文字列
- 数値
- ブール値
- IP アドレス
- Null チェック

条件演算子	説明
StringEquals	キーを文字列値と比較し、完全一致であるかを確認します（大文字と小文字の区別あり）。
StringNotEquals	キーを文字列値と比較し、不一致であるかを確認します（大文字と小文字の区別あり）。
StringEqualsIgnoreCase	キーを文字列値と比較し、完全一致であるかを確認します（大文字と小文字の区別なし）。
StringNotEqualsIgnoreCase	キーを文字列値と比較し、不一致であるかを確認します（大文字と小文字の区別なし）。
StringLike	キーを文字列値と比較し、完全一致であるかを確認します（大文字と小文字の区別あり）。含めることができる * と ? ワイルドカード文字を使用できます。
StringNotLike	キーを文字列値と比較し、不一致であるかを確認します（大文字と小文字の区別あり）。含めることができる * と ? ワイルドカード文字を使用できます。
NumericEquals (数値機器)	キーを数値と比較し、完全一致であるかを確認します。
NumericNotEquals	キーを数値と比較し、不一致であるかを確認します。
NumericGreaterThan	キーを数値と比較し、「より大きい」の一致であるかどうかを確認します。
NumericGreaterThanOrEqual	キーを数値と比較し、「以上」の一致であるかどうかを確認します。
NumericLessThan	キーを数値と比較し、「より小さい」一致であるかを確認します。
NumericLessThanOrEqual	キーを数値と比較し、「小なり」の一致であるかを確認します。
ブール値	キーをブール値と比較し、「trueまたはfalse」の一致であるかを確認します。
IP アドレス	キーを IP アドレスまたは IP アドレスの範囲と比較します。
NotIpAddress	キーを IP アドレスまたは IP アドレスの範囲と比較し、不一致であるかを確認します。
null	現在の要求コンテキストに条件キーが存在するかどうかを確認します。

## サポートされている条件キー

Conditionキー	アクション	説明
AWS : sourceIP	IP 演算子	<p>要求の送信元の IP アドレスと比較します。バケットまたはオブジェクトの処理に使用できます。</p> <ul style="list-style-type: none"> <li>注：S3 要求が管理ノードおよびゲートウェイノード上のロードバランササービスを介して送信された場合は、ロードバランササービスのアップストリームの IP アドレスと比較します。</li> <li>注 *：サードパーティ製の非透過型ロードバランサを使用する場合は、そのロードバランサの IP アドレスと比較します。任意 X-Forwarded-For ヘッダーの有効性を確認できないため、ヘッダーは無視されます。</li> </ul>
AWS : ユーザ名	リソース / ID	要求の送信者のユーザ名と比較します。バケットまたはオブジェクトの処理に使用できます。
S3 : デリミタ	S3 : ListBucket と S3 : ListBucketVersions 権限	ListObjects 要求または ListObjectVersions 要求で指定された delimiter パラメータと比較します。

Conditionキー	アクション	説明
S3 : ExistingObjectTag /<tag-key>	S3 : DeleteObjectTagging S3 : DeleteObjectVersionTagging S3 : GetObject S3 : GetObjectAcl S3 : GetObjectTagging S3 : GetObjectVersion S3 : GetObjectVersionAcl S3 : GetObjectVersionTagging S3 : PutObjectAcl S3 : PutObjectTagging S3 : PutObjectVersionAcl S3 : PutObjectVersionTagging	既存のオブジェクトに特定のタグキーと値が必要になります。
S3 : max-keys	S3 : ListBucket と S3 : ListBucketVersions 権限	ListObjects要求またはListObjectVersions要求で指定されたmax-keysパラメータと比較します。
S3 : object-lock-remaining-retention-days	S3 : PutObject	<p>で指定されたretain-until-dateと比較します x-amz-object-lock-retain-until-date 次の要求について、これらの値が許容範囲内であることを確認するために、要求ヘッダーまたはバケットのデフォルト保持期間から計算されます。</p> <ul style="list-style-type: none"> <li>• PutObject</li> <li>• CopyObject</li> <li>• CreateMultipartUpload を実行します</li> </ul>
S3 : object-lock-remaining-retention-days	S3 : PutObjectRetention	は、PutObjectRetention要求で指定されたretain-until-dateと比較して、許容範囲内であることを確認します。

Conditionキー	アクション	説明
S3 : プレフィックス	S3 : ListBucket と S3 : ListBucketVersions 権限	ListObjects要求またはListObjectVersions要求で指定されたprefixパラメータと比較します。
S3 : RequestObjectTag /<tag-key>	S3 : PutObject S3 : PutObjectTagging S3 : PutObjectVersionTagging	オブジェクト要求にタグ付けが含まれている場合は、特定のタグキーと値が必要になります。

ポリシーで変数を指定します

ポリシーで変数を使用すると、該当するポリシーの情報を設定できます。でポリシー変数を使用できます Resource の要素と文字列比較 Condition 要素 (Element) :

この例では、変数を使用しています \${aws:username} はResource要素の一部です。

```
"Resource": "arn:aws:s3:::bucket-name/home/${aws:username}/*"
```

この例では、変数を使用しています \${aws:username} は、条件ブロックの条件値の一部です。

```
"Condition": {  
    "StringLike": {  
        "s3:prefix": "${aws:username}/*"  
        ...  
    },  
    ...  
}
```

変数 ( Variable )	説明
\${aws:SourceIp}	SourceIp キーを指定の変数として使用します。
\${aws:username}	username キーを指定の変数として使用します。
`\${s3:prefix}`	サービス固有のプレフィックスキーを指定の変数として使用します。
`\${s3:max-keys}`	サービス固有の max-keys キーを指定の変数として使用します。
`\${*}`	特殊文字です。文字をリテラル * 文字として使用します。

変数 ( Variable )	説明
<code>\${?}</code>	特殊文字です。文字をリテラル文字として使用しますか？を押します。
<code>\${\$}</code>	特殊文字です。文字「\$」をリテラル文字として使用します。

特別な処理を必要とするポリシーを作成します

ポリシーで付与される権限によって、アカウントの root ユーザがロックアウトされるなど、セキュリティや継続的な運用に支障が生じことがあります。StorageGRID の S3 REST API の実装では、ポリシーの検証時の制限は Amazon よりも厳しくありませんが、評価時は同等の制限が適用されます。

Policy 概要 の 略	ポリシータイプ	Amazon の動作	StorageGRID の動作
自身に対し、root アカウントに対するすべての権限を拒否する	バケット	有効で適用されるが、S3 バケットのすべてのポリシー処理に対する権限は引き続き root ユーザアカウントに付与される	同じ
自身に対しユーザ / グループに対するすべての権限を拒否する	グループ	有効で適用されます	同じ
外部アカウントグループに対し任意の権限を許可します	バケット	無効なプリンシパルです	有効だが、S3 バケットのすべてのポリシー処理に対する権限をポリシーで許可すると 405 Method Not Allowed エラーが返されます
外部アカウントの root またはユーザに任意の権限を許可します	バケット	有効だが、S3 バケットのすべてのポリシー処理に対する権限をポリシーで許可すると 405 Method Not Allowed エラーが返されます	同じ
すべてのユーザにすべての処理に対する権限を許可します	バケット	有効だが、外部アカウントの root およびユーザについては、S3 バケットのすべてのポリシー処理に対する権限で 405 Method Not Allowed エラーが返されます	同じ
すべてのユーザに対してすべての処理に対する権限を拒否する	バケット	有効で適用されるが、S3 バケットのすべてのポリシー処理に対する権限は引き続き root ユーザアカウントに付与される	同じ

Policy 概要 の 略	ポリシータイプ	Amazon の動作	StorageGRID の動作
プリンシパルとして新規のユーザまたはグループを指定します	バケット	無効なプリンシパルです	有効
リソースとして新規の S3 バケットを指定する必要があります	グループ	有効	同じ
プリンシパルとしてローカルグループを指定します	バケット	無効なプリンシパルです	有効
ポリシーは、オブジェクトをPUTするための非所有者アカウント（匿名アカウントを含む）権限を付与します。	バケット	有効。オブジェクトは作成者アカウントによって所有され、バケットポリシーは適用されません。作成者アカウントは、オブジェクトの ACL を使用してオブジェクトにアクセス権限を付与する必要があります。	有効。オブジェクトはバケット所有者アカウントによって所有され、バケットポリシーが適用される。

#### Write-Once-Read-Many (WORM) による保護

データ、ユーザ定義オブジェクトのメタデータ、S3 オブジェクトのタグを保護するために、Write-Once-Read-Many (WORM) バケットを作成することができます。新しいオブジェクトの作成を許可し、既存のコンテンツの上書きや削除を防止するように WORM バケットを設定します。ここで説明するいずれかの方法を使用します。

上書きを常に拒否するには、次の操作を実行します。

- Grid Managerで、\* configuration > Security > Security settings > Network and objects の順に選択し、Prevent client modification \*チェックボックスを選択します。
- 次のルールと S3 ポリシーを適用します。
  - S3 ポリシーに PutOverwriteObject DENY 処理を追加します。
  - S3 ポリシーに DeleteObject DENY 処理を追加します。
  - S3 ポリシーに PutObject Allow 処理を追加します。



S3ポリシーでDeleteObjectをDENYに設定しても、「zero copies after 30 days」などのルールが存在する場合はILMによってオブジェクトが削除されます。



これらのルールとポリシーがすべて適用されても、同時書き込みからは保護されません（状況Aを参照）。保護の対象になるのはシーケンシャルな上書きです（状況Bを参照）。

- 状況 A \* : 同時書き込み（保護対象外）

```
/mybucket/important.doc  
PUT#1 ---> OK  
PUT#2 -----> OK
```

- ・状況 B \* : シーケンシャルな上書き（保護対象）

```
/mybucket/important.doc  
PUT#1 -----> PUT#2 ---X (denied)
```

#### 関連情報

- ・ "StorageGRID の ILM ルールによるオブジェクトの管理"
- ・ "バケットポリシーの例"
- ・ "グループポリシーの例"
- ・ "ILM を使用してオブジェクトを管理する"
- ・ "テナントアカウントを使用する"

#### バケットポリシーの例

このセクションの例を使用して、バケットのStorageGRID アクセスポリシーを作成します。

バケットポリシーでは、そのポリシーが関連付けられたバケットに対するアクセス権限を指定します。バケットポリシーは、S3 PutBucketPolicy API を使用して設定します。を参照してください "[バケットの処理](#)"。

バケットポリシーを設定するには、AWS CLI で次のコマンドを使用します。

```
> aws s3api put-bucket-policy --bucket examplebucket --policy  
file://policy.json
```

例：すべてのユーザにバケットへの読み取り専用アクセスを許可する

この例では、匿名ユーザを含むすべてのユーザにバケット内のオブジェクトのリストとバケット内のすべてのオブジェクトのGetObject処理を許可しています。それ以外の処理はすべて拒否されます。バケットへの書き込み権限がrootアカウント以外に付与されていないため、このポリシーは特に有用ではない場合があります。

```
{  
  "Statement": [  
    {  
      "Sid": "AllowEveryoneReadOnlyAccess",  
      "Effect": "Allow",  
      "Principal": "*",  
      "Action": [ "s3:GetObject", "s3>ListBucket" ],  
      "Resource":  
        ["arn:aws:s3:::examplebucket", "arn:aws:s3:::examplebucket/*"]  
    }  
  ]  
}
```

例：あるアカウントのすべてのユーザにフルアクセスを許可し、別のアカウントのすべてのユーザにバケットへの読み取り専用アクセスを許可する

この例では、指定したアカウントのすべてのユーザにバケットへのフルアクセスを許可しています。さらに、アカウントをもう1つ指定し、そのアカウントのすべてのユーザには、で始まるバケットのオブジェクトのList処理とGetObject処理のみを許可しています shared/ オブジェクトキープレフィックス。



StorageGRID では、非所有者アカウント（匿名アカウントを含む）によって作成されたオブジェクトが、バケット所有者アカウントによって所有されます。バケットポリシーで、これらのオブジェクトの環境を設定します。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "95390887230002558202"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::examplebucket/shared/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3>ListBucket",
      "Resource": "arn:aws:s3:::examplebucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "shared/*"
        }
      }
    }
  ]
}
```

例：すべてのユーザにバケットへの読み取り専用アクセスを許可し、指定したグループにフルアクセスを許可する

この例では、グループに属するユーザのみがバケットのList処理とバケット内のすべてのオブジェクトのGetObject処理を実行できるように匿名ユーザを含むすべてのユーザに許可しています。Marketing 指定したアカウントでは、フルアクセスが許可されています。

```

{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/Marketing"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": ["s3>ListBucket", "s3:GetObject"],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}

```

例：クライアントの IP 範囲を限定して、すべてのユーザにバケットへの読み取り / 書き込みアクセスを許可する

この例では、指定した IP 範囲（54.240.143.0~54.240.143.255 で 54.240.143.188 を除く）からの要求についてのみ、匿名ユーザを含むすべてのユーザにバケットの List 処理とバケット内のすべてのオブジェクトの全処理を許可しています。それ以外の処理はすべて拒否され、IP 範囲外の要求はすべて拒否されます。

```
{  
  "Statement": [  
    {  
      "Sid": "AllowEveryoneReadWriteAccessIfInSourceIpRange",  
      "Effect": "Allow",  
      "Principal": "*",  
      "Action": [ "s3:*Object", "s3>ListBucket" ],  
      "Resource":  
        ["arn:aws:s3:::examplebucket", "arn:aws:s3:::examplebucket/*"],  
      "Condition": {  
        "IpAddress": {"aws:SourceIp": "54.240.143.0/24"},  
        "NotIpAddress": {"aws:SourceIp": "54.240.143.188"}  
      }  
    }  
  ]  
}
```

例：指定したフェデレーテッドユーザにのみバケットへのフルアクセスを許可します

この例では、フェデレーテッドユーザのAlexがへのフルアクセスを許可しています examplebucket バケットとそのオブジェクト。'root' を含む他のすべてのユーザは 'すべての操作を明示的に拒否されますただし、「root」による Put/Get/DeleteBucketPolicy は拒否されません。

```
{  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Principal": {  
                "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"  
            },  
            "Action": [  
                "s3:*"  
            ],  
            "Resource": [  
                "arn:aws:s3:::examplebucket",  
                "arn:aws:s3:::examplebucket/*"  
            ]  
        },  
        {  
            "Effect": "Deny",  
            "NotPrincipal": {  
                "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"  
            },  
            "Action": [  
                "s3:*"  
            ],  
            "Resource": [  
                "arn:aws:s3:::examplebucket",  
                "arn:aws:s3:::examplebucket/*"  
            ]  
        }  
    ]  
}
```

#### 例：PutOverwriteObject 権限

この例では、を使用しています Deny PutOverwriteObjectとDeleteObjectの効果は、オブジェクトのデータ、ユーザ定義メタデータ、S3オブジェクトのタグを上書きまたは削除できないようにします。

```
{
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "s3:PutOverwriteObject",
        "s3>DeleteObject",
        "s3>DeleteObjectVersion"
      ],
      "Resource": "arn:aws:s3:::wormbucket/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"
      },
      "Action": "s3>ListBucket",
      "Resource": "arn:aws:s3:::wormbucket"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"
      },
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::wormbucket/*"
    }
  ]
}
```

## グループポリシーの例

このセクションの例を使用して、グループのStorageGRID アクセスポリシーを作成します。

グループポリシーは、そのポリシーが関連付けられたグループに対するアクセス権限を指定します。はいません Principal 要素は暗黙的であるため、ポリシーに含まれます。グループポリシーは Tenant Manager または API を使用して設定します。

例：Tenant Manager を使用してグループポリシーを設定します

Tenant Managerでグループを追加または編集するときに、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できます。を参照してください "S3 テナント用のグループを作成します"。

- \* No S3 Access \* : デフォルトオプション。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。
- ランサムウェアの軽減：このサンプルポリシーは、このテナントのすべてのバケットを環境します。このグループのユーザは共通の操作を実行できますが、オブジェクトのバージョン管理が有効になっているバケットからオブジェクトを完全に削除することはできません。

Manage All Buckets権限を持つTenant Managerユーザは、このグループポリシーよりも優先できます。[すべてのバケットを管理]権限を信頼できるユーザに制限し、可能な場合は多要素認証（MFA）を使用します。

- \* カスタム \* : グループ内のユーザーには、テキストボックスで指定した権限が付与されます。

例：グループにすべてのバケットへのフルアクセスを許可する

この例では、バケットポリシーで明示的に拒否されている場合を除き、グループのすべてのメンバーにテナントアカウントが所有するすべてのバケットへのフルアクセスが許可されます。

```
{  
  "Statement": [  
    {  
      "Action": "s3:*",  
      "Effect": "Allow",  
      "Resource": "arn:aws:s3:::*"  
    }  
  ]  
}
```

例：グループにすべてのバケットへの読み取り専用アクセスを許可する

この例では、バケットポリシーで明示的に拒否されている場合を除き、グループのすべてのメンバーに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。

```
{  
  "Statement": [  
    {  
      "Sid": "AllowGroupReadOnlyAccess",  
      "Effect": "Allow",  
      "Action": [  
        "s3>ListAllMyBuckets",  
        "s3>ListBucket",  
        "s3>ListBucketVersions",  
        "s3GetObject",  
        "s3GetObjectTagging",  
        "s3GetObjectVersion",  
        "s3GetObjectVersionTagging"  
      ],  
      "Resource": "arn:aws:s3:::*"  
    }  
  ]  
}
```

例：グループメンバーにバケット内の「フォルダ」へのフルアクセスのみを許可する

この例では、指定したバケット内の特定のフォルダ（キープレフィックス）のリストおよび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。

```

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

```

## 監査ログで追跡される S3 処理

監査メッセージは StorageGRID サービスによって生成され、テキスト形式のログファイルに保存されます。監査ログのS3固有の監査メッセージを確認して、バケットとオブジェクトの処理に関する詳細を確認できます。

### 監査ログで追跡されるバケットの処理

- CreateBucketを選択します
- DeleteBucketの場合
- DeleteBucketTagging
- オブジェクトを削除します
- GetBucketTagging
- ヘッドバケット
- ListObjects
- ListObjectVersions
- PUT Bucket compliance で確認してください
- PutBucketTaggingの略
- PutBucketVersioningの各ノードの設定

## 監査ログで追跡されるオブジェクトの処理

- CompleteMultipartUpload
- CopyObject
- deleteObject
- GetObject
- HeadObject (ヘッドオブジェクト)
- PutObject
- RestoreObject
- SelectObject
- UploadPart (ILMルールの取り込みがBalancedまたはStrictの場合)
- UploadPartCopy (ILMルールの取り込みがBalancedまたはStrictの場合)

### 関連情報

- ["監査ログファイルにアクセスします"](#)
- ["クライアント書き込み監査メッセージ"](#)
- ["クライアント読み取り監査メッセージ"](#)

## Swift REST APIの使用（廃止）

### Swift REST APIの使用：概要

クライアントアプリケーションでは、OpenStack Swift API を使用して、StorageGRID システムを操作できます。



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

StorageGRID でサポートしている Swift および HTTP のバージョンは次のとおりです。

項目	バージョン
Swift の仕様	2015 年 11 月時点の OpenStack Swift Object Storage API v1
HTTP	1.1 HTTP の詳細については、HTTP/1.1（RFC 7230~7235）を参照してください。 • 注：StorageGRID は、HTTP/1.1 パイプラインをサポートしません。

### 関連情報

- ["OpenStack : オブジェクトストレージ API"](#)

## StorageGRID での Swift API サポートの履歴

StorageGRID システムでの Swift REST API のサポートに関する変更点に注意する必要があります。

リリース。	コメント
11.8	
11.7	Swiftクライアントアプリケーションのサポートは廃止され、今後のリリースで削除される予定です。
11.6	編集上のいくつかの変更点。
11.5.	弱い整合性を削除しました。代わりに、available整合性が使用されます。
11.4	TLS 1.3のサポートが追加されました。ILMと整合性の相互関係の概要が追加されました。
11.3	PUT Object 处理が更新され、取り込み時に同期配置を使用する ILM ルールの影響（取り込み動作の Balanced オプションと Strict オプション）が記述されるようになりました。ロードバランサエンドポイントまたはハイアベイラビリティグループを使用するクライアント接続の概要が追加されました。TLS 1.1 暗号はサポートされなくなりました。
11.2.	ドキュメントに対する編集上の変更がいくつかあります。
11.1.	グリッドノードへの Swift クライアント接続での HTTP の使用のサポートが追加されました。整合性の値の定義が更新されました。
11.0	テナントアカウントにつき 1、000 個のコンテナのサポートが追加されました。
10.3	ドキュメントの管理に関する記述の更新と修正カスタムサーバ証明書の設定に関するセクションが削除されました。
10.2	StorageGRID システムで Swift API が初めてサポートされました。現在サポートされているバージョンは、OpenStack Swift Object Storage API v1 です。

## StorageGRID での Swift REST API の実装

クライアントアプリケーションは、Swift REST API呼び出しを使用してストレージノードやゲートウェイノードに接続し、コンテナの作成やオブジェクトの格納と読み出しを行うことができます。これを利用して、OpenStack Swift 向けに開発されたサービス指向アプリケーションを、StorageGRID システムで利用できるオンプレミスのオブジェクトストレージに接続することができます。

## Swift オブジェクトの管理

StorageGRIDシステムに取り込まれたSwiftオブジェクトは、アクティブなILMポリシー内の情報ライフサイクル管理（ILM）ルールによって管理されます。 "[ILM ルール](#)" および "[ILMポリシー](#)" StorageGRID でオブジェクトデータのコピーを作成および分散し、一定の期間にわたって管理する方法を決定します。たとえば、 ILM ルールを特定の Swift コンテナ内のオブジェクトに適用し、複数のオブジェクトコピーを複数のデータセンターに一定期間保存するように指定できます。

グリッドのILMルールとポリシーがSwiftテナントアカウントのオブジェクトに与える影響については、ネットアッププロフェッショナルサービスのコンサルタントまたはStorageGRID 管理者にお問い合わせください。

競合するクライアント要求です

同じキーに書き込む 2 つのクライアントなど、競合するクライアント要求は、「latest-wins」ベースで解決されます。「latest-wins」評価は、Swift クライアントが処理を開始するタイミングではなく、StorageGRID システムが特定の要求を完了したタイミングで行われます。

整合性の保証と制御

デフォルトでは、StorageGRID は、新規作成された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と HEAD 処理には結果整合性を提供します。任意 "[取得](#)" 正常に完了しました "[PUT](#)" 新しく書き込まれたデータを読み取ることができます。既存のオブジェクトの上書き、メタデータの更新、および削除の整合性レベルは、結果整合性です。上書きは通常、数秒から数分で反映されますが、最大で 15 日かかることがあります。

StorageGRID では、コンテナごとに整合性を制御することもできます。整合性の値は、アプリケーションの必要に応じて、オブジェクトの可用性と異なるストレージノードおよびサイト間でのオブジェクトの整合性のバランスを提供します。

## Swift REST API を実装する際の推奨事項

StorageGRID で使用するために Swift REST API を実装する場合は、次の推奨事項を考慮してください。

### 存在しないオブジェクトに対する HEAD の推奨事項

オブジェクトが実際に存在するとは思わないパスにオブジェクトが存在するかどうかをアプリケーションが定期的にチェックする場合は、「available」整合性を使用する必要があります。たとえば、アプリケーションがある場所へのPUT処理の前にある場所へのHEAD処理を実行する場合は、「available」整合性を使用する必要があります。

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 HEAD 処理でオブジェクトが見つからないと、「500 Internal Server Error」が大量に返される可能性があります。

コンテナごとに「available」整合性を設定するには、 "[PUT コンテナセイコウセイヨウキユウ](#)"。コンテナごとに「available」整合性を設定するには、 "[GET \(コンテナ整合性\) 要求](#)"。

### オブジェクト名の推奨事項

StorageGRID 11.4 以降で作成されたコンテナの場合、オブジェクト名がパフォーマンスのベストプラクティスに適合するように制限する必要はなくなりました。たとえば、オブジェクト名の最初の 4 文字にランダムな値を使用できるようになりました。

StorageGRID 11.4 よりも前のリリースで作成されたコンテナの場合は、オブジェクト名に関する次の推奨事項に進みます。

- ・オブジェクト名の最初の 4 文字に、ランダムな値を使用しないでください。これは、AWS が以前に推奨していた名前プレフィックスの推奨とは異なります。代わりに、などの一意ではないランダムなプレフィックスを使用してください `image`。
- ・名前のプレフィックスにランダムな一意の文字を使用するように AWS の以前の推奨事項に従っている場合は、オブジェクト名の前にディレクトリ名を指定する必要があります。つまり、次の形式を使用します。

```
mycontainer/mydir/f8e3-image3132.jpg
```

次の形式は使用しないでください。

```
mycontainer/f8e3-image3132.jpg
```

#### 「範囲読み取り」に関する推奨事項

状況に応じて "格納オブジェクトを圧縮するグローバルオプション" が有効になっている場合は、Swiftクライアントアプリケーションで、返されるバイト数の範囲を指定するGET Object処理を実行しないでください。これらの「範囲読み取り」処理は効率的ではありません。StorageGRIDでは、要求されたバイトにアクセスするためにオブジェクトの圧縮を実質的に解除する必要があるためです。非常に大きなオブジェクトから小さい範囲のバイト数を要求する GET Object 処理は特に効率が悪く、たとえば、50GB の圧縮オブジェクトから 10MB の範囲を読み取る処理は非常に非効率的です。

圧縮オブジェクトから範囲を読み取ると、クライアント要求がタイムアウトする可能性があります。



オブジェクトを圧縮する必要があり、クライアントアプリケーションが範囲読み取りを使用する必要がある場合は、アプリケーションの読み取りタイムアウトを増やしてください。

## Swift REST API設定のテスト

Swift CLIを使用して、StorageGRIDシステムへの接続をテストし、オブジェクトの読み取りと書き込みが可能であることを確認できます。

作業を開始する前に

- ・Swiftコマンドラインクライアントをダウンロードしてインストールしておきます。 "[swiftnStack : python-swiftclient](#)"
- ・必要に応じて、 "[ロードバランサエンドポイントを作成しました](#)"。それ以外の場合は、接続するストレージノードのIPアドレスと使用するポート番号がわかっている必要があります。を参照してください "[クライアント接続用のIPアドレスとポート](#)"。
- ・これで完了です "[Swiftテナントアカウントを作成しました](#)"。
- ・テナントアカウントにサインインし、グループとユーザを少なくとも1つ作成しておきます。を参照してください "[Swift テナント用のグループを作成します](#)"。



SwiftテナントユーザがSwift REST APIに認証するには、Administratorグループ権限が必要です。

#### このタスクについて

セキュリティを設定していない場合は、を追加する必要があります `--insecure` これらの各コマンドにフラグを設定します。

#### 手順

1. StorageGRID Swift 環境の情報 URL を照会します。

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/info
capabilities
```

この手順で、Swift 環境が機能することをテストできます。オブジェクトを格納してアカウント設定をさらにテストするには、以降の手順を実行します。

2. オブジェクトをコンテナに配置します。

```
touch test_object
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
upload test_container test_object
--object-name test_object
```

3. コンテナを取得してオブジェクトを確認します。

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
list test_container
```

4. オブジェクトを削除します。

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
delete test_container test_object
```

## 5. コンテナを削除します。

```
swift
-U `<_Tenant_Account_ID:Account_User_Name_>`
-K `<_User_Password_>`
-A `\\https://<_FQDN_|_IP_>:<_Port_>/auth/v1.0`
delete test_container
```

## Swift REST API でサポートされている処理

StorageGRID システムは、OpenStack Swift API のほとんどの処理をサポートしています。Swift REST API クライアントを StorageGRID に統合する前に、アカウント、コンテナ、およびオブジェクトの処理の実装に関する詳細を確認します。

### StorageGRID でサポートされている操作

次の Swift API 処理がサポートされています。

- ・ "アカウントの処理"
- ・ "コンテナの処理"
- ・ "オブジェクトの処理"

### すべての処理に共通の応答ヘッダー

StorageGRID システムでは、OpenStack Swift Object Storage API v1 の定義に従って、サポートされるすべての処理に共通のヘッダーが実装されます。

### 関連情報

["OpenStack : オブジェクトストレージ API"](#)

### サポートされている Swift API エンドポイント

StorageGRID でサポートされている Swift API エンドポイントは、情報 URL、認証 URL、およびストレージ URL です。

### 情報 URL

StorageGRID Swift 実装の機能と制限事項については、Swift のベース URL に /info パスを付加して GET 要求

を発行することで確認できます。

`https://FQDN | Node IP:Swift Port/info/`

要求の内容は次のとおりです。

- *FQDN* は完全修飾ドメイン名です。
- *Node IP* は、StorageGRID ネットワークのストレージノードまたはゲートウェイノードのIPアドレスです。
- *Swift Port* は、ストレージノードまたはゲートウェイノードのSwift API接続に使用するポート番号です。

たとえば、次の情報 URL は、IP アドレスが 10.99.106.103 でポート 18083 を使用しているストレージノードから情報を要求します。

`https://10.99.106.103:18083/info/`

応答には、Swift 実装の機能が JSON ディクショナリとして含まれます。クライアントツールは、JSON 応答を解析して実装の機能を特定し、後続のストレージ処理で制約として使用できます。

StorageGRID 実装の Swift では、情報 URL への認証されていないアクセスが許可されます。

#### 認証 URL

クライアントは、Swift 認証 URL を使用してテナントアカウントユーザとして認証できます。

`https://FQDN | Node IP:Swift Port/auth/v1.0/`

で、テナントアカウントID、ユーザ名、およびパスワードをパラメータとして指定する必要があります `X-Auth-User` および `X-Auth-Key` 次のように要求ヘッダー

`X-Auth-User: Tenant_Account_ID:Username`

`X-Auth-Key: Password`

要求ヘッダーは次のようになります。

- *Tenant\_Account\_ID* は、Swiftテナントの作成時にStorageGRID によって割り当てられたアカウントID です。Tenant Manager のサインインページで使用するテナントアカウント ID と同じです。
- *Username* は、Tenant Managerで作成されたテナントユーザの名前です。このユーザは、Swift 管理者権限を持つグループに属している必要があります。テナントのrootユーザをSwift REST APIを使用するように設定することはできません。

テナントアカウントに対してアイデンティティフェデレーションが有効になっている場合は、LDAP サーバからのフェデレーテッドユーザのユーザ名とパスワードを指定します。または、LDAP ユーザのドメイン名を指定します。例：

`X-Auth-User: Tenant_Account_ID:Username@Domain_Name`

- *Password* は、テナントユーザのパスワードです。ユーザパスワードは Tenant Manager で作成および管理します。

認証要求が成功すると、ストレージ URL と認証トークンが次のように返されます。

X-Storage-Url: https://FQDN | Node\_IP:Swift\_Port/v1/Tenant\_Account\_ID

X-Auth-Token: token

X-Storage-Token: token

デフォルトでは、トークンの有効期間は生成時刻から 24 時間です。

トークンは特定のテナントアカウントに対して生成されます。あるアカウントに対して有効なトークンで、別のアカウントにアクセスするユーザを許可することはできません。

#### ストレージ URL

クライアントアプリケーションは、ゲートウェイノードまたはストレージノードに対して、問題の Swift REST API 呼び出しを使用して、アカウント、コンテナ、オブジェクトのサポートされる処理を実行できます。ストレージ要求は、認証応答で返されたストレージ URL にアドレスが指定されます。要求には、認証要求から返された X-Auth-Token ヘッダーと値も含める必要があります。

https://FQDN | IP:Swift\_Port/v1/Tenant\_Account\_ID

[/container] [/object]

X-Auth-Token: token

使用状況の統計が含まれるストレージ応答ヘッダーに、最近変更されたオブジェクトの正確な数が反映されない場合があります。このヘッダーに正確な数値が表示されるまでに数分かかることがあります。

使用状況の統計が含まれているアカウントおよびコンテナ処理の応答ヘッダーの例を次に示します。

- X-Account-Bytes-Used
- X-Account-Object-Count
- X-Container-Bytes-Used
- X-Container-Object-Count

#### 関連情報

["テナントアカウントと接続を設定する"](#)

["アカウントの処理"](#)

["コンテナの処理"](#)

["オブジェクトの処理"](#)

#### アカウントの処理

アカウントに対して実行する Swift API 処理を次に示します。

## **GET**アカウント

この処理は、アカウントに関連付けられているコンテナリストおよびアカウントの使用状況を示す統計を取得します。

次の要求パラメータが必要です。

- Account

次の要求ヘッダーが必要です。

- X-Auth-Token

次のサポートされている要求クエリパラメータはオプションです。

- Delimiter
- End\_marker
- Format
- Limit
- Marker
- Prefix

実行が成功すると、アカウントが見つかってコンテナがないかコンテナリストが空の場合は「HTTP/1.1 204 No Content」の応答とともに次のヘッダーが返されます。アカウントが見つかってコンテナリストが空でない場合は「HTTP/1.1 200 OK」の応答も返されます。

- Accept-Ranges
- Content-Length
- Content-Type
- Date
- X-Account-Bytes-Used
- X-Account-Container-Count
- X-Account-Object-Count
- X-Timestamp
- X-Trans-Id

## **HEAD**アカウント

この処理は、Swift アカウントからアカウント情報と統計情報を取得します。

次の要求パラメータが必要です。

- Account

次の要求ヘッダーが必要です。

- X-Auth-Token

実行が成功すると、「HTTP/1.1 204 No Content」の応答とともに次のヘッダーが返されます。

- Accept-Ranges
- Content-Length
- Date
- X-Account-Bytes-Used
- X-Account-Container-Count
- X-Account-Object-Count
- X-Timestamp
- X-Trans-Id

#### 関連情報

["監査ログで追跡される Swift 処理"](#)

#### コンテナの処理

StorageGRID では、Swift アカウントあたり最大で 1,000 個のコンテナがサポートされます。コンテナに対して実行する Swift API 処理を次に示します。

コンテナを削除します

この処理は、StorageGRID システムの Swift アカウントから空のコンテナを削除します。

次の要求パラメータが必要です。

- Account
- Container

次の要求ヘッダーが必要です。

- X-Auth-Token

実行が成功すると、「HTTP/1.1 204 No Content」の応答とともに次のヘッダーが返されます。

- Content-Length
- Content-Type
- Date
- X-Trans-Id

#### GET コンテナ

この処理は、コンテナに関連付けられているオブジェクトリストを、StorageGRID システム内のコンテナの統計情報およびメタデータとともに読み出します。

次の要求パラメータが必要です。

- Account
- Container

次の要求ヘッダーが必要です。

- X-Auth-Token

次のサポートされている要求クエリパラメータはオプションです。

- Delimiter
- End\_marker
- Format
- Limit
- Marker
- Path
- Prefix

実行が成功すると、「HTTP/1.1 200 Success」または「HTTP/1.1 204 No Content」の応答とともに次のヘッダーが返されます。

- Accept-Ranges
- Content-Length
- Content-Type
- Date
- X-Container-Bytes-Used
- X-Container-Object-Count
- X-Timestamp
- X-Trans-Id

#### **HEAD (コンテナ)**

この処理は、StorageGRID システムからコンテナの統計情報とメタデータを読み出します。

次の要求パラメータが必要です。

- Account
- Container

次の要求ヘッダーが必要です。

- X-Auth-Token

実行が成功すると、「HTTP/1.1 204 No Content」の応答とともに次のヘッダーが返されます。

- Accept-Ranges
- Content-Length
- Date
- X-Container-Bytes-Used
- X-Container-Object-Count
- X-Timestamp
- X-Trans-Id

#### PUT (コンテナ)

この処理は、StorageGRID システムのアカウントにコンテナを作成します。

次の要求パラメータが必要です。

- Account
- Container

次の要求ヘッダーが必要です。

- X-Auth-Token

実行が成功すると、「HTTP/1.1 201 Created」または「HTTP/1.1 202 Accepted」の応答（このアカウントにコンテナがすでに存在する場合）とともに次のヘッダーが返されます。

- Content-Length
- Date
- X-Timestamp
- X-Trans-Id

コンテナ名は StorageGRID ネームスペース内で一意である必要があります。このコンテナが別のアカウントの下に存在する場合は、ヘッダー「HTTP/1.1 409 Conflict」が返されます。

#### 関連情報

["監視と監査の処理"](#)

#### オブジェクトの処理

オブジェクトに対して実行する Swift API 処理を次に示します。これらの処理はで追跡できます ["StorageGRID 監査ログ"](#)。

オブジェクトを削除します

この処理は、オブジェクトのコンテンツとメタデータを StorageGRID システムから削除します。

次の要求パラメータが必要です。

- Account
- Container
- Object

次の要求ヘッダーが必要です。

- X-Auth-Token

実行が成功すると、が指定された次の応答ヘッダーが返されます HTTP/1.1 204 No Content 対応：

- Content-Length
- Content-Type
- Date
- X-Trans-Id

StorageGRID は、DELETE Object 要求を処理する際に、オブジェクトのすべてのコピーをすべての格納場所からただちに削除しようとします。成功すると、StorageGRID はただちにクライアントに応答を返します。30秒以内にすべてのコピーを削除できない場合（場所が一時的に使用できない場合など）、StorageGRID は削除対象のコピーをキューに登録し、クライアントに成功を通知します。

詳細については、を参照してください ["オブジェクトの削除方法"](#)。

#### GET (オブジェクト)

この処理は、StorageGRID から、オブジェクトのコンテンツを読み出し、オブジェクトメタデータを取得します。

次の要求パラメータが必要です。

- Account
- Container
- Object

次の要求ヘッダーが必要です。

- X-Auth-Token

次の要求ヘッダーはオプションです。

- Accept-Encoding
- If-Match
- If-Modified-Since
- If-None-Match
- If-Unmodified-Since

- Range

実行が成功すると、が指定された次のヘッダーが返されます HTTP/1.1 200 OK 対応：

- Accept-Ranges
- Content-Disposition の場合にのみ返されます `Content-Disposition メタデータが設定されました
- Content-Encoding の場合にのみ返されます `Content-Encoding メタデータが設定されました
- Content-Length
- Content-Type
- Date
- ETag
- Last-Modified
- X-Timestamp
- X-Trans-Id

#### HEADオブジェクト

この処理は、取り込まれたオブジェクトのメタデータとプロパティを StorageGRID システムから読み出します。

次の要求パラメータが必要です。

- Account
- Container
- Object

次の要求ヘッダーが必要です。

- X-Auth-Token

実行が成功すると、「HTTP/1.1 200 OK」の応答とともに次のヘッダーが返されます。

- Accept-Ranges
- Content-Disposition の場合にのみ返されます `Content-Disposition メタデータが設定されました
- Content-Encoding の場合にのみ返されます `Content-Encoding メタデータが設定されました
- Content-Length
- Content-Type
- Date
- ETag
- Last-Modified

- X-Timestamp
- X-Trans-Id

#### PUT (オブジェクト)

この処理は、StorageGRID システムで、データとメタデータを含む新しいオブジェクトを作成するか、データとメタデータを含む既存のオブジェクトを置換します。

StorageGRID では、サイズが 5TiB (5、497、558、138、880 バイト) までのオブジェクトがサポートされます。



同じキーに書き込む 2 つのクライアントなど、競合するクライアント要求は、「latest-wins」ベースで解決されます。「latest-wins」評価は、Swift クライアントが処理を開始するタイミングではなく、StorageGRID システムが特定の要求を完了したタイミングで行われます。

次の要求パラメータが必要です。

- Account
- Container
- Object

次の要求ヘッダーが必要です。

- X-Auth-Token

次の要求ヘッダーはオプションです。

- Content-Disposition
- Content-Encoding

chunked は使用しないでください Content-Encoding 環境 オブジェクトがサイズに基づいてオブジェクトをフィルタリングし、取り込み時に同期配置を使用する ILM ルール（取り込み動作に Balanced オプションまたは Strict オプション）の場合。

- Transfer-Encoding

圧縮やチャunkは使用しないでください Transfer-Encoding 環境 オブジェクトがサイズに基づいてオブジェクトをフィルタリングし、取り込み時に同期配置を使用する ILM ルール（取り込み動作に Balanced オプションまたは Strict オプション）の場合。

- Content-Length

ILM ルールで、オブジェクトがサイズでフィルタリングされ、取り込み時に同期配置が使用される場合は、を指定する必要があります Content-Length。



のこれらのガイドラインに従わない場合 Content-Encoding、'Transfer-Encoding`および`Content-Length`ではStorageGRID、オブジェクトのサイズを確認してILMルールを適用する前に、オブジェクトを保存しておく必要があります。つまり、StorageGRIDで取り込み時にデフォルトでオブジェクトの中間コピーを作成する必要があります。つまり、StorageGRIDでの取り込み動作には Dual Commit オプションを使用する必要があります。

同期配置とILMルールの詳細については、を参照してください ["取り込みのデータ保護オプション"](#)。

- Content-Type
- ETag
- X-Object-Meta-<name\> (オブジェクト関連のメタデータ)

ILMルールの参照時間として\* User defined creation time \*オプションを使用する場合は、というユーザ定義のヘッダーに値を格納する必要があります X-Object-Meta-Creation-Time。例：

```
X-Object-Meta-Creation-Time: 1443399726
```

このフィールドの値は、1970年1月1日からの秒数となります。

- X-Storage-Class: reduced\_redundancy

このヘッダーは、取り込まれたオブジェクトに一致する ILM ルールで取り込み動作に Dual Commit または Balanced が指定されている場合に StorageGRID で作成されるオブジェクトコピーの数に影響します。

- \* Dual commit \* : ILM ルールの取り込み動作が Dual commit オプションに指定されている場合は、オブジェクトの取り込み時に StorageGRID が中間コピーを 1 つ作成します（シングルコミット）。
- \* Balanced \* : ILM ルールで Balanced オプションが指定されている場合、StorageGRID は、ルールで指定されたすべてのコピーをただちに作成できない場合にのみ中間コピーを 1 つ作成します。StorageGRID で同期配置を実行できる場合、このヘッダーは効果がありません。
- reduced\_redundancy ヘッダーは、オブジェクトに一致する ILM ルールで单一のレプリケートコピーが作成される場合に最も適しています。この場合は、を使用します reduced\_redundancy 取り込み処理のたびに追加のオブジェクトコピーを不要に作成および削除する必要がなくなります。

を使用する reduced\_redundancy 取り込み中にオブジェクトデータが失われるリスクが高まるため、他の状況ではヘッダーを使用することは推奨されません。たとえば、ILM 評価の前にコピーが 1 つだけ格納されていたストレージノードに障害が発生すると、データが失われる可能性があります。



レプリケートコピーを一定期間に 1 つだけ作成すると、データが永続的に失われるリスクがあります。オブジェクトのレプリケートコピーが 1 つしかない場合、ストレージノードに障害が発生したり、重大なエラーが発生すると、そのオブジェクトは失われます。また、アップグレードなどのメンテナンス作業中は、オブジェクトへのアクセスが一時的に失われます。

を指定することに注意してください reduced\_redundancy オブジェクトの初回取り込み時に作成されるコピー数のみに影響します。オブジェクトがアクティブな ILM ポリシーで評価される際に作成されるオブジェクトのコピー数には影響せず、StorageGRID システムでデータが格納される際の冗長性レベルが低下することもありません。

実行が成功すると、「HTTP/1.1 201 Created」の応答とともに次のヘッダーが返されます。

- Content-Length
- Content-Type
- Date
- ETag
- Last-Modified
- X-Trans-Id

## OPTIONS 要求

OPTIONS 要求は、個々の Swift サービスが使用可能かどうかを確認します。OPTIONS 要求は、URL で指定されたストレージノードまたはゲートウェイノードによって処理されます。

### OPTIONS メソッド

たとえば、クライアントアプリケーションでは、Swift 認証クレデンシャルを入力することなく、ストレージノード上の Swift ポートに OPTIONS 要求を問題で送信して、ストレージノードが使用可能かどうかを判別できます。この要求は、監視に使用できるほか、外部のロードバランサがストレージノードの停止を特定する目的でも使用できます。

情報（info） URL またはストレージ（storage） URL と併用する場合、OPTIONS メソッドは、HEAD、GET、OPTIONS、PUT など、指定された URL でサポートされる動詞のリストを返します。OPTIONS メソッドは認証 URL では使用できません。

次の要求パラメータが必要です。

- Account

次の要求パラメータはオプションです。

- Container
- Object

実行が成功すると、「HTTP/1.1 204 No Content」の応答とともに次のヘッダーが返されます。ストレージ URL への OPTIONS 要求には、ターゲットが存在する必要はありません。

- Allow (HEAD、GET、OPTIONSなど、指定された URL でサポートされる動詞のリスト) および PUT
- Content-Length
- Content-Type
- Date
- X-Trans-Id

## 関連情報

["サポートされている Swift API エンドポイント"](#)

## Swift API 処理に対するエラー応答

エラー応答について理解しておくと、処理をトラブルシューティングする際に役立ちます。

処理中にエラーが発生した場合に返される HTTP ステータスコードを次に示します。

Swift エラーの名前	HTTPステータス
AccountNameTooLong、 ContainerNameTooLong、 HeaderTooBig、 InvalidContainerName、 InvalidRequest、 InvalidURI、 MetadataNameTooLong、 MetadataValueTooBig、 MissingSecurityHeader、 ObjectNameTooLong、 TooManyContainers、 TooManyMetadataItems、 TotalMetadataTooLarge	400 不正な要求です
アクセスが拒否されました	403 禁止
ContainerNotEmpty、 ContainerAlreadyExists です	409 競合
内部エラー	500 Internal Server Error (内部サーバエラー)
InvalidRange :無効な範囲	416 リクエストされた範囲が適合しません
MethodNotAllowed のように入力します	405 メソッドは許可されていません
MissingContentLength ( MissingContentLength )	411 長さが必要です
NOTFOUND	404 が見つかりません
実装なし	501 は実装されていません
PreconditionalFailed	412 事前条件が失敗しました
resourceNotFound です	404 が見つかりません
権限がありません	401 認証なし
UnprocessableEntity の場合	422 加工不能エンティティ

## StorageGRID の Swift REST API 処理

StorageGRID システム固有の処理が Swift REST API に追加されています。

## GET（コンテナ整合性）要求

"整合性の値" オブジェクトの可用性と、異なるストレージノードおよびサイト間でのオブジェクトの整合性のバランスを確保します。GET（コンテナ整合性）要求を使用すると、特定のコンテナに適用されている整合性を確認できます。

リクエスト

要求の HTTP ヘッダー	説明
X-Auth-Tokenの略	要求に使用するアカウントの Swift 認証トークンを指定します。
x-ntap-sg-consistencyの略	要求のタイプを指定します true = GETコンテナconsistency、および false = コンテナを取得します。
ホスト	要求の転送先のホスト名。

要求例

```
GET /v1/28544923908243208806/Swift container
X-Auth-Token: SGRD_3a877009a2d24cb1801587bfa9050f29
x-ntap-sg-consistency: true
Host: test.com
```

応答

応答の HTTP ヘッダー	説明
日付	応答の日時。
接続	サーバへの接続が開いているかどうか。
X-Trans-ID	要求の一意のトランザクション ID。
Content-Lengthの略	応答の本文の長さ。

応答の HTTP ヘッダー	説明
x-ntap-sg-consistencyの略	<p>コンテナに適用されている整合性。次の値がサポートされています。</p> <ul style="list-style-type: none"> <li>• all * : すべてのノードがすぐにデータを受信しないと、要求が失敗します。</li> <li>• 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。</li> </ul> <p>*strong-site * : サイト内のすべてのクライアント要求に対してリードアフターライト整合性が保証されます。</p> <ul style="list-style-type: none"> <li>• Read-after-new-write * : (デフォルト) 新規オブジェクトにはリードアフターライト整合性を提供し、オブジェクトの更新には結果整合性を提供します。高可用性が確保され、データ保護が保証されます。ほとんどの場合に推奨されます。</li> <li>• available * : 新しいオブジェクトとオブジェクトの更新の両方について、結果整合性を提供します。S3バケットの場合は、必要な場合にのみ使用します（読み取り頻度の低いログ値を含むバケットや、存在しないキーに対するHEAD処理やGET処理など）。S3 FabricPool バケットではサポートされません。</li> </ul>

#### 応答例

```

HTTP/1.1 204 No Content
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
X-Trans-Id: 1936575373
Content-Length: 0
x-ntap-sg-consistency: strong-site

```

#### PUT コンテナセイコウセイヨウキユウ

PUT (コンテナ整合性) 要求では、コンテナで実行される処理に適用する整合性を指定できます。デフォルトでは、新しいコンテナは「Read-after-new-write」整合性を使用して作成されます。

#### リクエスト

要求の HTTP ヘッダー	説明
X-Auth-Tokenの略	要求に使用するアカウントの Swift 認証トークンです。

要求の HTTP ヘッダー	説明
x-ntap-sg-consistencyの略	<p>コンテナに対する処理に適用される整合性。次の値がサポートされています。</p> <ul style="list-style-type: none"> <li>• all * : すべてのノードがすぐにデータを受信しないと、要求が失敗します。</li> <li>• 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。</li> </ul> <p>*strong-site * : サイト内のすべてのクライアント要求に対してリードアフターライト整合性が保証されます。</p> <ul style="list-style-type: none"> <li>• Read-after-new-write * : (デフォルト) 新規オブジェクトにはリードアフターライト整合性を提供し、オブジェクトの更新には結果整合性を提供します。高可用性が確保され、データ保護が保証されます。ほとんどの場合に推奨されます。</li> <li>• available * : 新しいオブジェクトとオブジェクトの更新の両方について、結果整合性を提供します。S3バケットの場合は、必要な場合にのみ使用します（読み取り頻度の低いログ値を含むバケットや、存在しないキーに対するHEAD処理やGET処理など）。S3 FabricPool バケットではサポートされません。</li> </ul>
Host	要求の転送先のホスト名。

#### 整合性とILMルールの相互作用によるデータ保護への影響

あなたの選択の両方 "整合性の値" オブジェクトの保護方法にはILMルールが影響します。これらの設定は対話的に操作できます。

たとえば、オブジェクトの格納時に使用される整合性はオブジェクトメタデータの初期配置に影響し、一方で "取り込み動作" ILMルールに対して選択すると、オブジェクトコピーの初期配置に影響します。StorageGRIDでは、クライアント要求に対応するためにオブジェクトのメタデータとそのデータの両方にアクセスする必要があるため、整合性と取り込み動作で同じ保護レベルを選択すると、初期データ保護が向上し、システム応答の予測性が向上します。

#### 整合性ルールとILMルールの相互作用の例

2サイトのグリッドで次のILMルールと整合性が設定されているとします。

- \* ILM ルール \* : ローカルサイトとリモートサイトに 1 つずつ、2 つのオブジェクトコピーを作成します。Strict 取り込み動作が選択されています。
- \*\* : 「strong-global」（オブジェクトメタデータがすべてのサイトに即座に分散される）

クライアントがオブジェクトをグリッドに格納すると、StorageGRID は両方のオブジェクトをコピーし、両方のサイトにメタデータを分散してからクライアントに成功を返します。

オブジェクトは、取り込みが成功したことを示すメッセージが表示された時点で損失から完全に保護されます。たとえば、取り込み直後にローカルサイトが失われた場合、オブジェクトデータとオブジェクトメタデータの両方のコピーがリモートサイトに残っています。オブジェクトを完全に読み出し可能にしている。

同じILMルールと「strong-site」整合性を使用した場合、オブジェクトデータがリモートサイトにレプリケートされたあと、オブジェクトメタデータが分散される前にクライアントに成功メッセージが返されることがあります。この場合、オブジェクトメタデータの保護レベルがオブジェクトデータの保護レベルと一致しません。取り込み直後にローカルサイトが失われると、オブジェクトメタデータが失われます。オブジェクトを取得できません。

整合性ルールとILMルールの関係は複雑になる可能性があります。サポートが必要な場合は、ネットアップにお問い合わせください。

#### 要求例

```
PUT /v1/28544923908243208806/_Swift_container_
X-Auth-Token: SGRD_3a877009a2d24cb1801587bfa9050f29
x-ntap-sg-consistency: strong-site
Host: test.com
```

#### 応答

応答の HTTP ヘッダー	説明
Date	応答の日時。
Connection	サーバへの接続が開いているかどうか。
X-Trans-Id	要求の一意のトランザクション ID。
Content-Length	応答の本文の長さ。

#### 応答例

```
HTTP/1.1 204 No Content
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
X-Trans-Id: 1936575373
Content-Length: 0
```

#### 監査ログで追跡される Swift 処理

ストレージに対する成功した DELETE、GET、HEAD、POST、PUT の各処理は、StorageGRID 監査ログで追跡されます。失敗およびinfo、auth、OPTIONS の各要求はログに記録されません。

#### アカウントの処理

- "GETアカウント"

- "HEADアカウント"

#### コンテナの処理

- "コンテナを削除します"
- "GET コンテナ"
- "HEAD (コンテナ) "
- "PUT (コンテナ) "

#### オブジェクトの処理

- "オブジェクトを削除します"
- "GET (オブジェクト) "
- "HEADオブジェクト"
- "PUT (オブジェクト) "

#### 関連情報

- "監査ログファイルにアクセスします"
- "クライアント書き込み監査メッセージ"
- "クライアント読み取り監査メッセージ"

## 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。