



StorageGRIDを使用する

StorageGRID software

NetApp
December 03, 2025

目次

StorageGRIDテナントとクライアントを使用する	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	1
サインインとサインアウトの方法	2
テナントマネージャーダッシュボードを理解する	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
グループとユーザーの管理	29
S3 アクセスキーを管理する	48
S3バケットを管理する	54
S3 プラットフォーム サービスを管理する	78
S3 REST APIを使用する	109
S3 REST API のサポート対象バージョンとアップデート	109
クイックリファレンス: サポートされている S3 API リクエスト	112
S3 REST API 構成のテスト	132
StorageGRIDがS3 REST APIを実装する方法	133
Amazon S3 REST APIのサポート	148
StorageGRIDカスタム操作	198
バケットとグループのアクセスポリシー	219
監査ログで追跡されるS3操作	246
Swift REST API を使用する (サポート終了)	247
Swift REST APIを使用する	247

StorageGRIDテナントとクライアントを使用する

テナントアカウントを使用する

テナントアカウントを使用する

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

テナントアカウントとは何ですか？

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

テナント アカウントを使用すると、保存されたオブジェクトを異なるエンティティごとに分離できます。たとえば、次のいずれかのユースケースでは複数のテナント アカウントを使用できます。

- エンタープライズの使用例: StorageGRIDシステムを企業内で使用している場合、グリッドのオブジェクト ストレージは組織内のさまざまな部門によって分離されている可能性があります。たとえば、マーケティング部門、カスタマー サポート部門、人事部門などのテナント アカウントが存在する場合があります。



S3 クライアント プロトコルを使用する場合は、S3 バケットとバケット ポリシーを使用して、企業内の部門間でオブジェクトを分離することもできます。個別のテナント アカウントを作成する必要はありません。実装手順を参照["S3 バケットとバケットポリシー"](#)詳細についてはこちらをご覧ください。

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

テナントアカウントを作成する方法

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

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

さらに、S3 テナント アカウントが規制要件に準拠する必要がある場合、グリッド管理者はStorageGRIDシステムの S3 オブジェクト ロック設定を有効にすることができます。S3 オブジェクト ロックを有効にすると、すべての S3 テナント アカウントが準拠バケットを作成および管理できるようになります。

S3テナントを構成する

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

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



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

サインインとサインアウトの方法

テナントマネージャーに**Sign in**

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

開始する前に

- ログイン資格情報をお持ちです。
- グリッド管理者から提供された、テナント マネージャーにアクセスするための URL があります。URL は次のいずれかの例のようになります。

```
https://FQDN_or_Admin_Node_IP/
```

```
https://FQDN_or_Admin_Node_IP:port/
```

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

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

URL には、完全修飾ドメイン名 (FQDN)、管理ノードの IP アドレス、または管理ノードの HA グループの仮想 IP アドレスが常に含まれます。ポート番号、20 桁のテナント アカウント ID、またはその両方が含まれる場合もあります。

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

- あなたは以下のユーザーグループに属しています"[特定のアクセス権限](#)".

手順

1. 起動する"[サポートされているウェブブラウザ](#)".
2. ブラウザのアドレスバーに、Tenant Manager にアクセスするための URL を入力します。
3. セキュリティ警告が表示された場合は、ブラウザのインストール ウィザードを使用して証明書をインストールします。
4. テナント マネージャーにSign in。

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

SSOを使用していない

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

- Grid Manager のサインイン ページ。テナント サインイン リンクを選択します。



NetApp StorageGRID®

Grid Manager

Username

Password

Sign in

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

- テナント マネージャーのサインイン ページ。以下に示すように、アカウント フィールドはすでに入力されている可能性があります。

NetApp StorageGRID®

Tenant Manager

Recent

-- Optional --

Account

64600207336181242061

Username

|

Password

Sign in

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

- i. テナントの 20 桁のアカウント ID が表示されない場合は、最近のアカウントの一覧にテナント アカウントの名前が表示されている場合はそれを選択するか、アカウント ID を入力します。
- ii. ユーザー名とパスワードを入力してください。
- iii. *Sign in*を選択します。

テナント マネージャー ダッシュボードが表示されます。

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

SSOの使用

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

- 組織の SSO ページ。例えば：

Sign in with your organizational account

標準の SSO 資格情報を入力し、[Sign in] を選択します。

- テナント マネージャー SSO サインイン ページ。

NetApp StorageGRID[®]
Tenant Manager

Recent

Account

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

- テナントの 20 桁のアカウント ID が表示されない場合は、最近のアカウントの一覧にテナント アカウントの名前が表示されている場合はそれを選択するか、アカウント ID を入力します。
- *Sign in* を選択します。
- 組織の SSO サインイン ページで標準の SSO 資格情報を使用して Sign in。

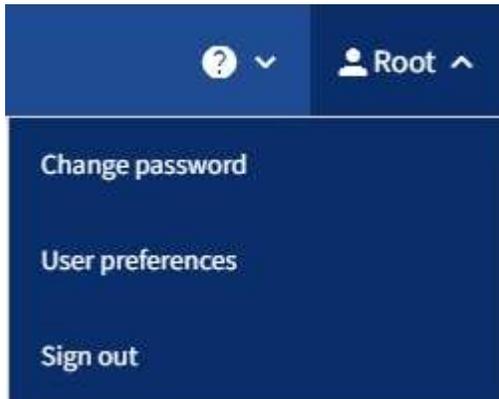
テナント マネージャー ダッシュボードが表示されます。

テナントマネージャーからサインアウトする

テナント マネージャーでの作業が完了したら、権限のないユーザーがStorageGRIDシステムにアクセスできないようにするためにサインアウトする必要があります。ブラウザの Cookie 設定によっては、ブラウザを閉じてシステムからサインアウトされない場合があります。

手順

1. ユーザー インターフェイスの右上隅にあるユーザー名ドロップダウンを見つけます。



2. ユーザー名を選択し、[サインアウト]を選択します。

- SSO が使用されていない場合:

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



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

- SSO が有効な場合:

アクセスしていたすべての管理ノードからサインアウトしました。StorageGRIDSIGN inページが表示されます。アクセスしたテナント アカウントの名前が [最近のアカウント] ドロップダウンにデフォルトで表示され、テナントの アカウント ID が表示されます。



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

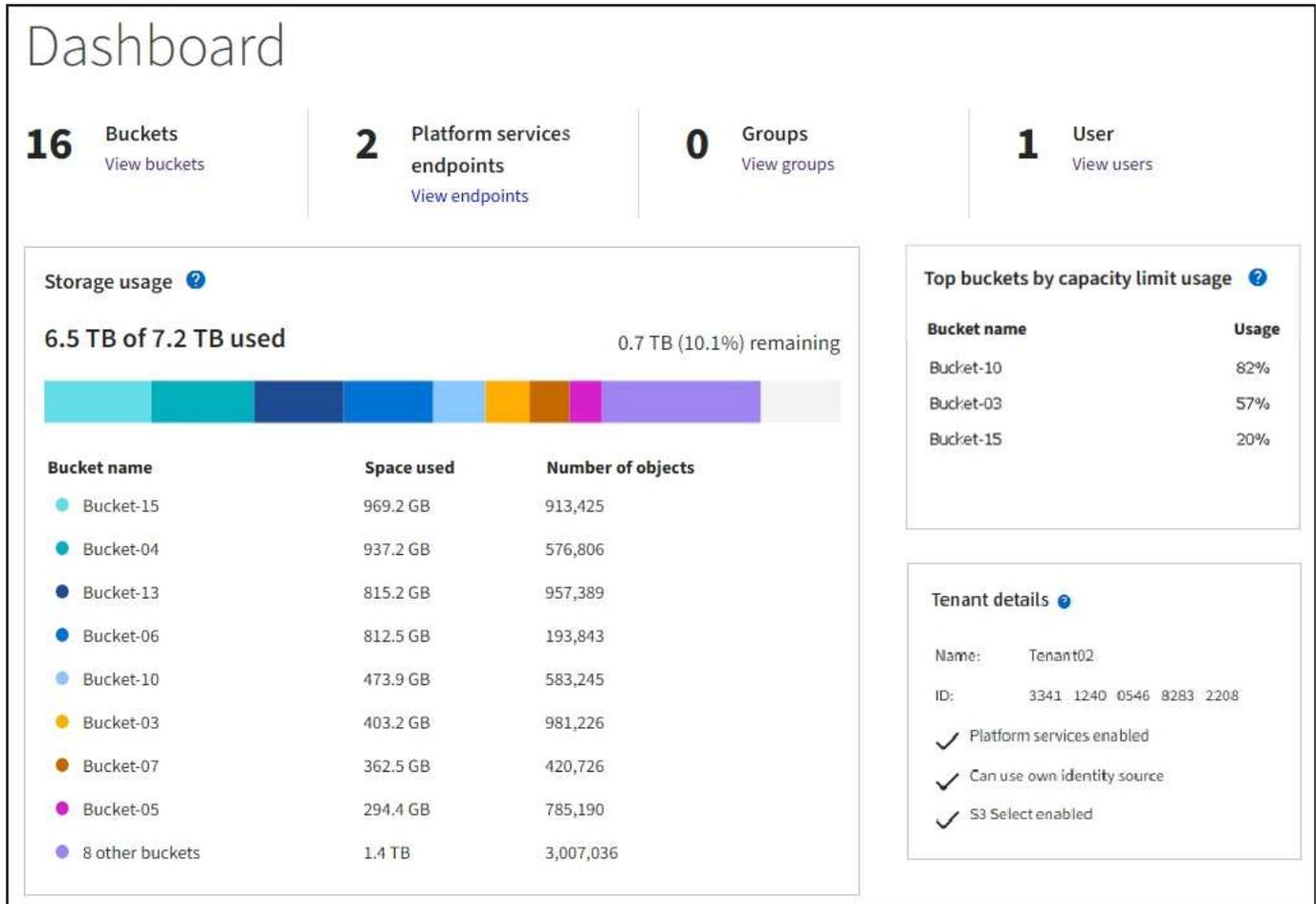
テナントマネージャーダッシュボードを理解する

テナント マネージャー ダッシュボードには、テナント アカウントの構成の概要と、テナントのバケット (S3) またはコンテナ (Swift) 内のオブジェクトによって使用されているスペースの量が表示されます。テナントにクォータがある場合は、ダッシュボードには使用されているクォータの量と残っている量が表示されます。テナント アカウントに関連するエラーがある場合は、ダッシュボードにエラーが表示されます。



使用済みスペースの値は推定値です。これらの見積りは、取り込みのタイミング、ネットワーク接続、およびノードの状態によって影響を受けます。

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



テナントアカウント情報

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

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

ストレージとクォータの使用状況

ストレージ使用量パネルには次の情報が含まれます。

- テナントのオブジェクト データの量。

この値は、アップロードされたオブジェクト データの合計量を示しており、それらのオブジェクトとそのメタデータのコピーを保存するために使用されるスペースを表すものではありません。

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



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

- 最大のバケットまたはコンテナの相対的なサイズを表す棒グラフ。

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



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

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

テナントに 9 個を超えるバケットまたはコンテナがある場合、他のすべてのバケットまたはコンテナはリストの下部にある 1 つのエントリに結合されます。



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

クォータ使用量アラート

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

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

グリッド管理者にクォータの増加を依頼することを検討してください。

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

容量制限の使用状況

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

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

エンドポイントエラー

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

 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.

詳細を見るには"[プラットフォームサービスエンドポイントエラー](#)"で、[エンドポイント] を選択して、エンドポイント ページを表示します。

テナント管理API

テナント管理APIを理解する

テナント マネージャー ユーザー インターフェイスの代わりに、テナント管理 REST API を使用してシステム管理タスクを実行できます。たとえば、API を使用して操作を自動化したり、ユーザーなどの複数のエンティティをより迅速に作成したりすることができます。

テナント管理 API:

- Swagger オープンソース API プラットフォームを使用します。Swagger は、開発者と非開発者が API を操作できる直感的なユーザー インターフェイスを提供します。Swagger ユーザー インターフェイスは、各 API 操作の完全な詳細とドキュメントを提供します。
- 用途"[中断のないアップグレードをサポートするためのバージョン管理](#)"。

テナント管理 API の Swagger ドキュメントにアクセスするには:

1. テナント マネージャーに Sign in。
2. テナント マネージャーの上部から、ヘルプ アイコンを選択し、**API ドキュメント** を選択します。

APIの処理

テナント管理 API は、利用可能な API 操作を次のセクションに分類します。

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

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

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



StorageGRIDシステムでシングル サインオン (SSO) が有効になっている場合は、認証のために別の手順を実行する必要があります。参照["グリッド管理APIの使用手順"](#)。

- **config**: テナント管理 API の製品リリースとバージョンに関連する操作。製品のリリース バージョンと、そのリリースでサポートされている API のメジャー バージョンを一覧表示できます。
- **コンテナ**: S3 バケットまたは Swift コンテナに対する操作。
- **deactivated-features**: 非アクティブ化された可能性のある機能を表示する操作。
- **エンドポイント**: エンドポイントを管理するための操作。エンドポイントにより、S3 バケットはStorageGRID CloudMirror レプリケーション、通知、または検索統合に外部サービスを使用できるようになります。
- **grid-federation-connections**: グリッド フェデレーション接続およびグリッド間レプリケーションに関する操作。
- **グループ**: ローカル テナント グループを管理し、外部 ID ソースからフェデレーション テナント グループを取得するための操作。
- **identity-source**: 外部 ID ソースを構成し、フェデレーション グループとユーザー情報を手動で同期する操作。
- **ilm**: 情報ライフサイクル管理 (ILM) 設定に関する操作。
- **regions**: StorageGRIDシステムに設定されているリージョンを判別する操作。
- **s3**: テナント ユーザーの S3 アクセス キーを管理する操作。
- **s3-object-lock**: 規制コンプライアンスをサポートするために使用される、グローバル S3 オブジェクトロック設定に対する操作。
- **users**: テナント ユーザーを表示および管理する操作。

操作の詳細

各 API 操作を展開すると、HTTP アクション、エンドポイント URL、必須またはオプションのパラメータのリスト、リクエスト本文の例 (必要な場合)、および可能な応答が表示されます。

groups Operations on groups

GET /org/groups Lists Tenant User Groups

Parameters Try it out

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

Responses Response content type: application/json

Code	Description
200	

Example Value | Model

```
{
  "responseTime": "2018-02-01T16:22:31.066Z",
  "status": "success",
  "apiVersion": "2.1"
}
```

API リクエストを発行する



API ドキュメント Web ページを使用して実行するすべての API 操作はライブ操作です。誤って設定データやその他のデータを作成、更新、削除しないように注意してください。

手順

1. リクエストの詳細を表示するには、HTTP アクションを選択します。
2. リクエストにグループ ID やユーザー ID などの追加のパラメータが必要かどうかを判断します。次に、こ

これらの値を取得します。必要な情報を取得するには、最初に別の API リクエストを発行する必要がある場合があります。

3. サンプルのリクエスト本文を変更する必要があるかどうかを判断します。その場合は、「モデル」を選択して、各フィールドの要件を確認することができます。
4. *試してみる*を選択します。
5. 必要なパラメータを指定するか、必要に応じてリクエスト本文を変更します。
6. *実行*を選択します。
7. 応答コードを確認して、リクエストが成功したかどうかを確認します。

テナント管理 API のバージョン管理

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

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

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

古いバージョンと互換性のない変更が行われた場合には、API のメジャー バージョンが引き上げられます。古いバージョンと互換性のある変更が行われた場合に、API のマイナー バージョンが引き上げられます。互換性のある変更には、新しいエンドポイントまたは新しいプロパティの追加が含まれます。

次の例は、行われた変更の種類に基づいて API バージョンがどのように変更されるかを示しています。

APIの変更の種類	旧バージョン	新バージョン
旧バージョンとの互換性あり	2.1	2.2
旧バージョンとは互換性がありません	2.1	3.0

StorageGRIDソフトウェアを初めてインストールすると、最新バージョンの API のみが有効になります。ただし、StorageGRIDの新しい機能リリースにアップグレードすると、少なくとも 1 つのStorageGRID機能リリースについては引き続き古い API バージョンにアクセスできます。



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

古くなったリクエストは、次の方法で非推奨としてマークされます。

- レスポンスヘッダーは「Deprecated: true」です
- JSONレスポンス本文に「deprecated」が含まれています: true
- 非推奨の警告が nms.log に追加されます。例えば：

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

現在のリリースでサポートされている **API** バージョンを確認する

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

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

リクエストの **API** バージョンを指定する

パスパラメータを使用して API バージョンを指定できます (/api/v4) またはヘッダー (Api-Version: 4)。両方の値を指定した場合、ヘッダー値がパス値を上書きします。

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

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

クロスサイトリクエストフォージェリ (**CSRF**) から保護する

CSRF トークンを使用して Cookie を使用する認証を強化することで、StorageGRID に対するクロスサイト リクエスト フォージェリ (CSRF) 攻撃から保護することができます。Grid Manager と Tenant Manager はこのセキュリティ機能を自動的に有効にします。他の API クライアントはサインイン時にこの機能を有効にするかどうかを選択できます。

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

StorageGRID は、CSRF トークンを使用して CSRF 攻撃から保護します。有効にすると、特定の Cookie の内容は、特定のヘッダーまたは特定の POST 本文パラメータのいずれかの内容と一致する必要があります。

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

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

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

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

- その `X-Csrf-Token`ヘッダーの値は CSRF トークン クッキーの値に設定されます。
- フォームエンコードされた本文を受け入れるエンドポイントの場合: `csrfToken`フォームエンコードされたリクエストボディパラメータ。

CSRF保護を設定するには、"[グリッド管理API](#)"または"[テナント管理API](#)"。



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

グリッドフェデレーション接続を使用する

テナントグループとユーザーの複製

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

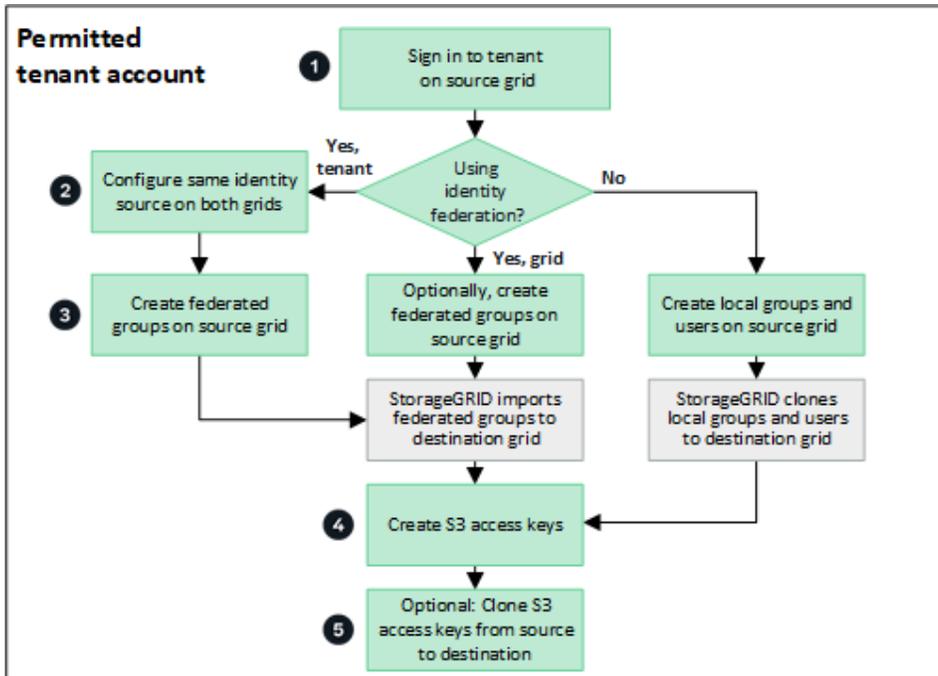
テナントが最初に作成されたStorageGRIDシステムは、テナントのソース グリッドです。テナントが複製されるStorageGRIDシステムは、テナントの宛先グリッドです。両方のテナント アカウントは同じアカウント ID、名前、説明、ストレージ クォータ、割り当てられた権限を持ちますが、宛先テナントには最初はルートユーザー パスワードがありません。詳細については、"[アカウントクローンとは](#)"そして"[許可されたテナントを管理する](#)"。

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

アカウントクローンのテナントワークフロー

テナント アカウントに グリッド フェデレーション接続の使用 権限がある場合は、ワークフロー図を参照して、グループ、ユーザー、および S3 アクセス キーのクローンを作成するために実行する手順を確認してくだ

さい。



ワークフローの主な手順は次のとおりです。

1

テナントに**Sign in**

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

2

オプションで**ID連携**を構成する

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

3

グループとユーザーを作成する

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

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

4

S3アクセスキーを作成する

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

5

オプションでS3アクセスキーを複製する

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

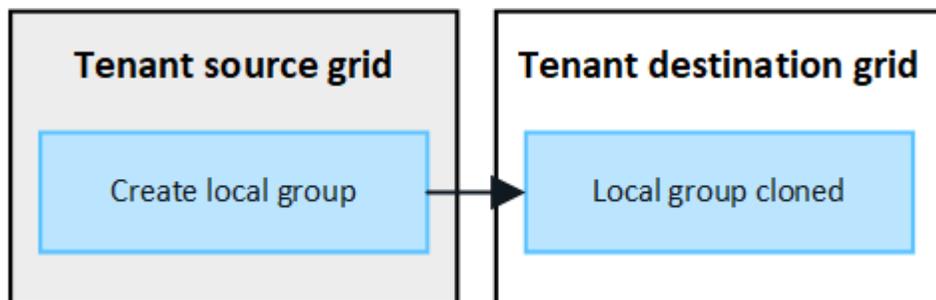
グループ、ユーザー、S3 アクセスキーはどのように複製されますか？

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

ソースグリッド上に作成されたローカルグループは複製されます

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

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

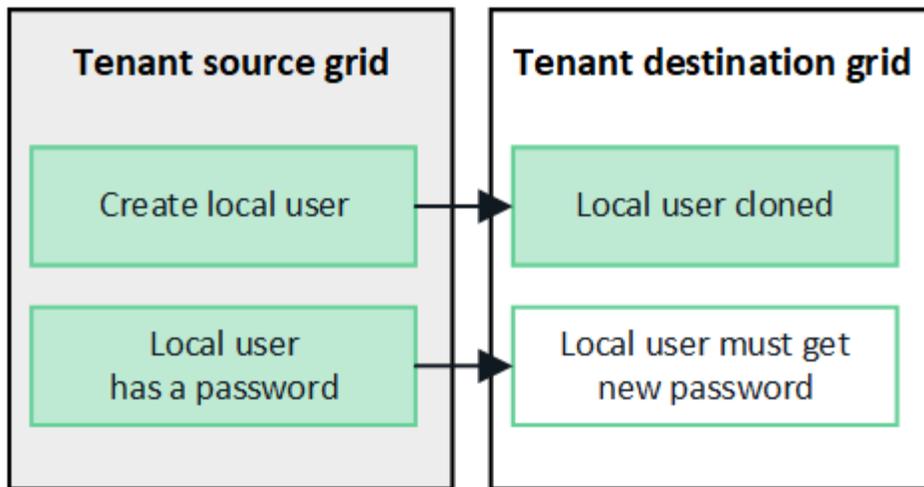


ソースグリッドにローカルグループを作成するときに選択したユーザーは、グループが宛先グリッドに複製されるときには含まれません。このため、グループを作成するときにユーザーを選択しないでください。代わりに、ユーザーを作成するときにグループを選択します。

ソースグリッド上に作成されたローカルユーザーは複製されます

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

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

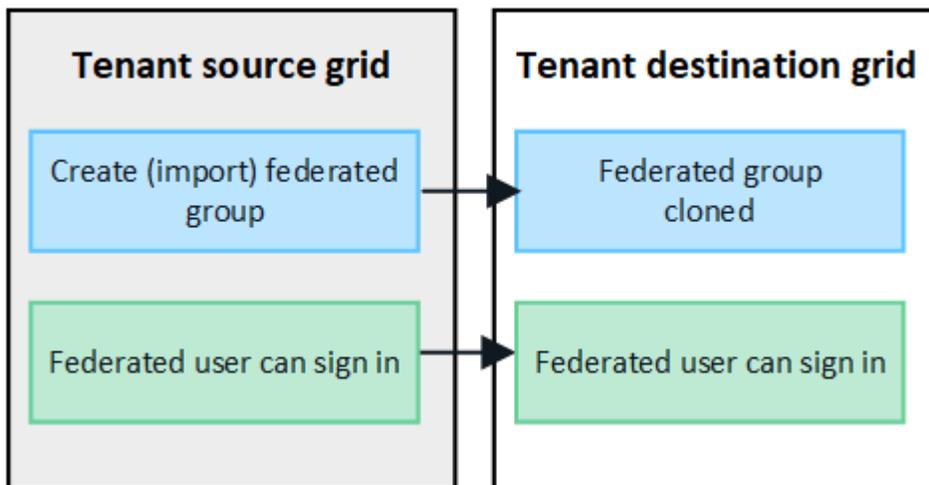


ソースグリッド上に作成されたフェデレーショングループはクローン化されます

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

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

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

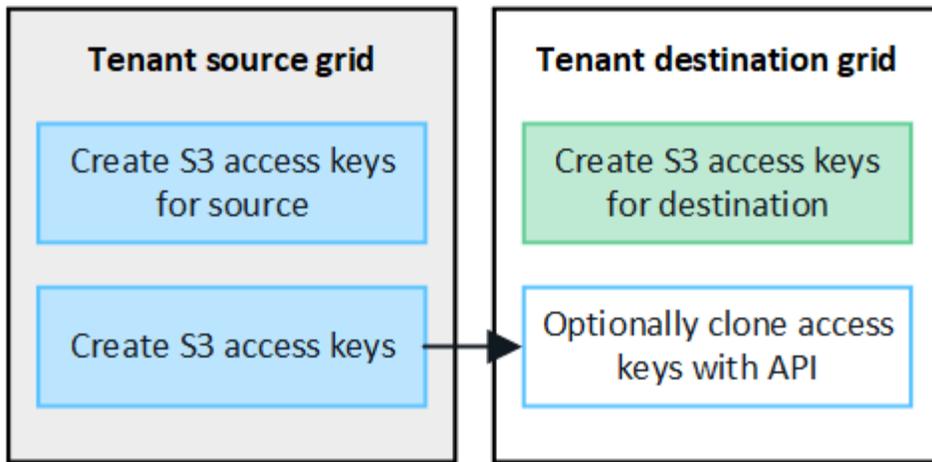


S3アクセスキーは手動で複製できます

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

2つのグリッド上のアクセスキーを管理するには、次のいずれかを実行します。

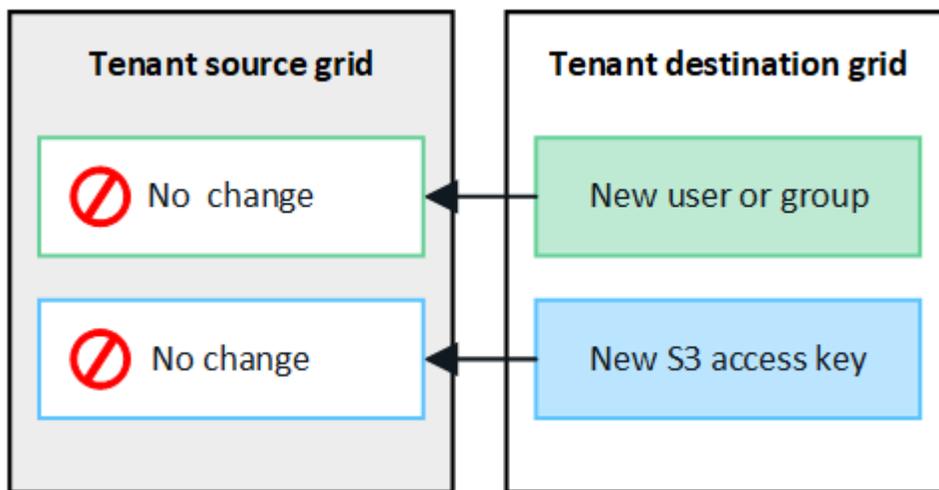
- 各グリッドに同じキーを使用する必要がない場合は、"独自のアクセスキーを作成する"または"別のユーザーのアクセスキーを作成する"各グリッド上。
- 両方のグリッドで同じキーを使用する必要がある場合は、ソースグリッドでキーを作成し、テナントマネージャーAPIを使用して手動で"キーを複製する"目的のグリッドへ。



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

宛先グリッドに追加されたグループとユーザーは複製されません

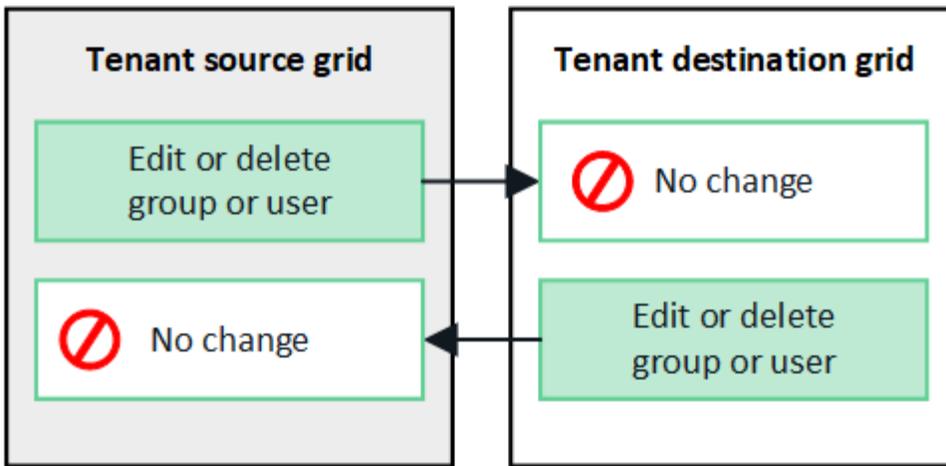
クローン作成は、テナントのソースグリッドからテナントの宛先グリッドにのみ行われます。テナントの宛先グリッドにグループとユーザーを作成またはインポートした場合、StorageGRID はこれらの項目をテナントのソースグリッドに複製しません。



編集または削除されたグループ、ユーザー、アクセスキーは複製されません

クローン作成は、新しいグループとユーザーを作成するときのみ行われます。

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



API を使用して S3 アクセスキーを複製する

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

開始する前に

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



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

独自のアクセスキーを複製する

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

手順

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

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

POST

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



4. ***試してみる***を選択します。

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

各文字列を囲む二重引用符を必ず保持してください。



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

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

他のユーザーのアクセスキーを複製する

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

手順

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

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

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



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

文字列を囲む二重引用符を必ず保持してください。

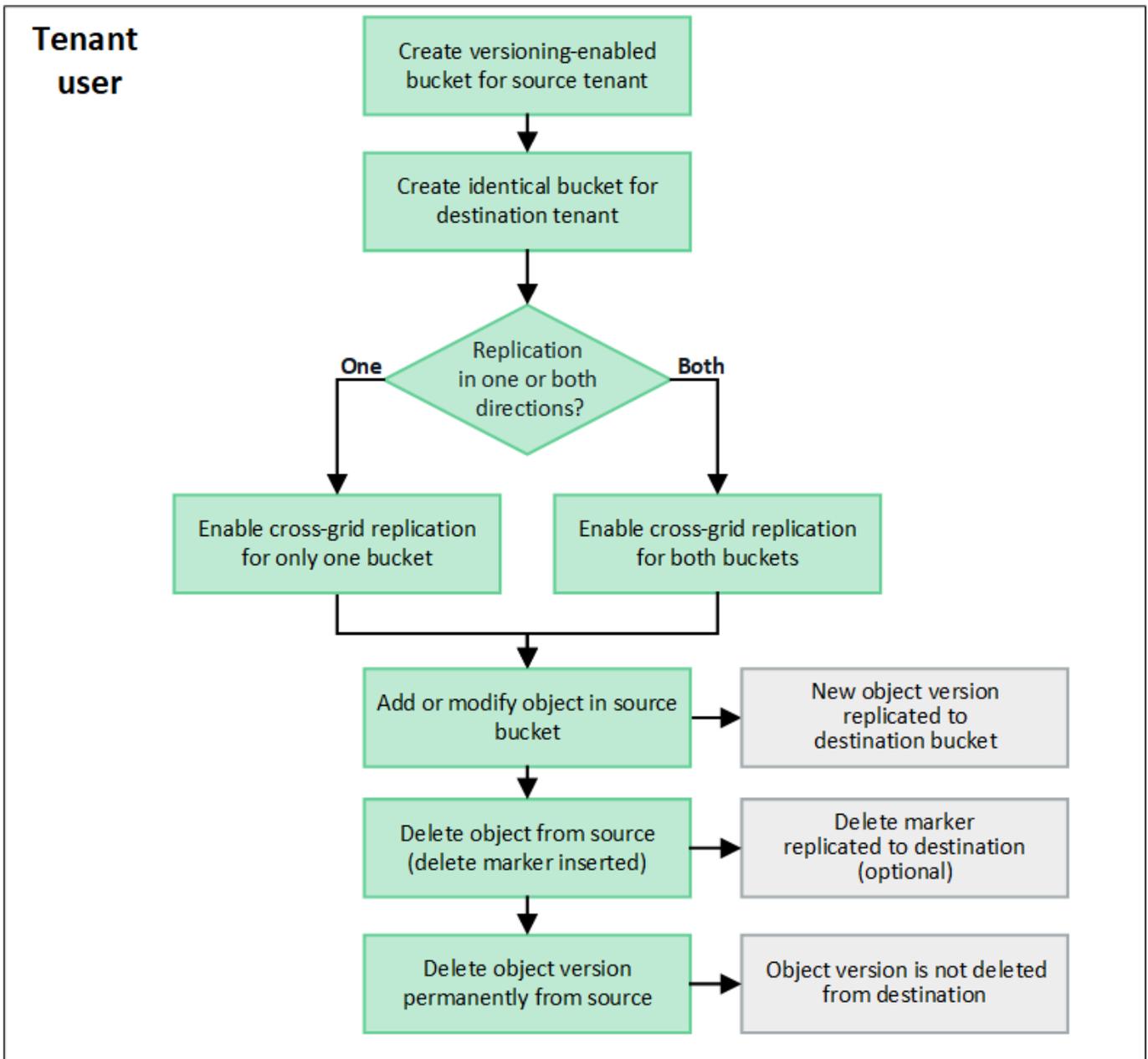
8. キーの有効期限が切れる場合は、**expires***の例のエントリを、**ISO 8601**データ時間形式の文字列として有効期限の日時で置き換えます（例： **2023-02-28T22:46:33-08:00**）。キーに有効期限がない場合は、***expires** エントリの値として **null** を入力します（または **Expires** 行とその前のカンマを削除します）。
9. *実行*を選択します。
10. サーバー応答コードが **204** であることを確認します。これは、キーが宛先グリッドに正常に複製されたことを示します。

クロスグリッドレプリケーションを管理する

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

クロスグリッドレプリケーションのワークフロー

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



クロスグリッドレプリケーションを構成する

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

開始する前に

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

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

同一のバケットを2つ作成する

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

手順

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



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

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



必要に応じて、各バケットは異なるリージョンを使用できます。

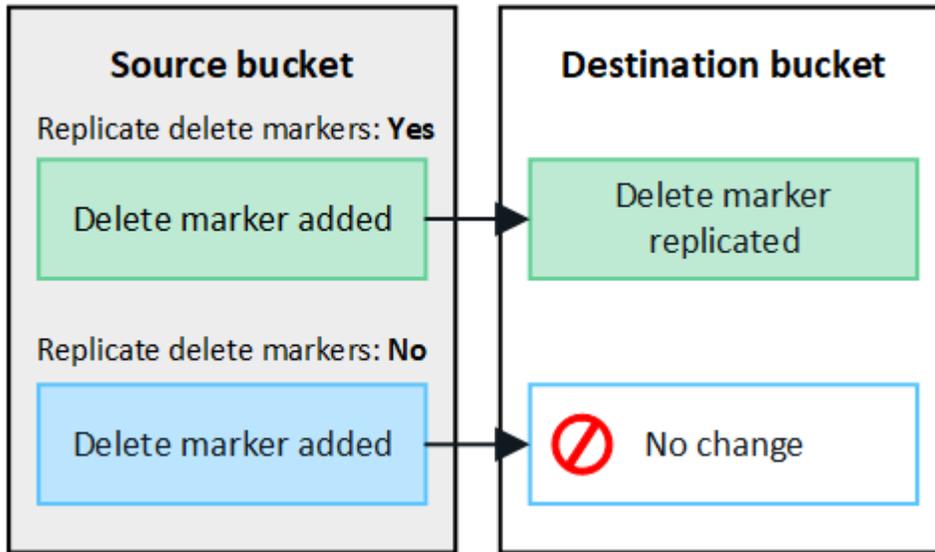
クロスグリッドレプリケーションを有効にする

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

手順

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

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



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

見る"[クロスグリッドレプリケーションとは](#)"詳細については。

- 必要に応じて、クロスグリッド レプリケーション 監査カテゴリの設定を変更して、監査メッセージの量を管理します。
 - エラー (デフォルト): 監査出力には、失敗したクロスグリッド レプリケーション要求のみが含まれます。
 - 通常: すべてのクロスグリッド レプリケーション要求が含まれるため、監査出力の量が大幅に増加します。
- 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。
- *有効化してテスト*を選択します。

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

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

グリッド間のレプリケーションをテストする

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

開始する前に

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

手順

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

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

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

クロスグリッドレプリケーションを無効にする

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

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

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



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

開始する前に

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

手順

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

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

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

グリッドフェデレーション接続を表示する

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

開始する前に

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

手順

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

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

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

2. オプションでバケット名を選択して["バケットの詳細を表示"](#)。

最後のエラーをクリアする

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

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



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

手順

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

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

The screenshot shows a web interface titled "Grid federation connections". At the top, there is a "Clear error" button and a search bar. Below this is a table with columns: "Connection name", "Buckets with cross-grid replication", and "Last error". The table contains one entry for "Grid 1-Grid 2" with bucket "my-cgr-bucket". The "Last error" column shows a timestamp "2022-12-07 16:02:20 MST" and a detailed error message: "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)".

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



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

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

グループとユーザーの管理

アイデンティティフェデレーションを使用する

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

テナントマネージャーの ID フェデレーションを構成する

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

開始する前に

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



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

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

タスク概要

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



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

設定を入力

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

手順

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

LDAP service type

Select the type of LDAP service you want to configure.

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

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

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



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

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

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

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

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

- memberOf`または `isMemberOf
 - アクティブディレクトリ: objectSid、 primaryGroupID、 userAccountControl、そして userPrincipalName
 - アズール: accountEnabled`そして `userPrincipalName
- パスワード: ユーザー名に関連付けられたパスワード。

 将来パスワードを変更する場合は、このページで更新する必要があります。

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

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

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

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

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

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

次のいずれかのパターンを入力します。

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

[USERNAME] を記載どおりに入力してください。

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

- **STARTTLS** を使用する: STARTTLS を使用して、LDAP サーバーとの通信を保護します。これは、Active Directory、OpenLDAP、またはその他の場合に推奨されるオプションですが、このオプションは Azure ではサポートされていません。
- **LDAPS** を使用する: LDAPS (LDAP over SSL) オプションは、TLS を使用して LDAP サーバーへの接続を確立します。Azure の場合はこのオプションを選択する必要があります。
- **TLS** を使用しない: StorageGRIDシステムと LDAP サーバー間のネットワーク トラフィックは保護されません。このオプションは Azure ではサポートされていません。

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

7. STARTTLS または LDAPS を選択した場合は、接続を保護するために使用する証明書を選択します。

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

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

接続をテストし、設定を保存します

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

手順

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

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

Test Connection ✕

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

Test username

The username of a federated user.

Test password

👁

CancelTest Connection

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

アイデンティティソースとの強制同期

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

手順

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

環境によっては同期プロセスに時間がかかる場合があります。



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

ID連携を無効にする

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

タスク概要

ID フェデレーションを無効にする前に、次の点に注意してください。

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

手順

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

OpenLDAPサーバーの設定ガイドライン

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



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

Memberof と refint オーバーレイ

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

インデックス作成

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

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

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

逆グループメンバーシップ維持に関する情報

は、<http://www.openldap.org/doc/admin24/index.html>["OpenLDAP ドキュメント: バージョン 2.4 管理者ガイド"]。

テナントグループの管理

S3テナントのグループを作成する

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

開始する前に

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

グループ作成ウィザードにアクセスする

最初のステップとして、グループの作成ウィザードにアクセスします。

手順

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

Groups

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

0 groups Create group

Actions ▾

i This tenant has **Use grid federation connection** permission for connection Grid 1 to Grid 2. New local tenant groups 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.

3. *グループを作成*を選択します。

グループの種類を選択

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

手順

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

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

- グループの名前を入力します。

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



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

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

- *続行*を選択します。

グループ権限を管理する

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

手順

- アクセス モード では、次のいずれかを選択します。
 - 読み取り/書き込み (デフォルト): ユーザーは Tenant Manager にサインインし、テナント構成を管理できます。
 - 読み取り専用: ユーザーは設定と機能の表示のみが可能です。テナント マネージャーまたはテナント

管理 API で変更を加えたり、操作を実行したりすることはできません。ローカルの読み取り専用ユーザーは自分のパスワードを変更できます。



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

2. このグループに対して 1 つ以上の権限を選択します。

見る ["テナント管理権限"](#)。

3. *続行*を選択します。

S3グループポリシーを設定する

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

手順

1. このグループに使用するポリシーを選択します。

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

グループポリシー	説明
カスタム	グループ内のユーザーには、テキスト ボックスで指定した権限が付与されます。

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

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

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

ユーザーを追加する（ローカルグループのみ）

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



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

手順

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

作成したグループがグループのリストに表示されます。

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

Swiftテナントのグループを作成する

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



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

開始する前に

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

- フェデレーショングループをインポートする予定の場合は、"構成されたID連携"、フェデレーショングループは構成された ID ソースにすでに存在します。

グループ作成ウィザードにアクセスする

手順

最初のステップとして、グループの作成ウィザードにアクセスします。

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

グループの種類を選択

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

手順

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

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

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

グループ権限を管理する

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

手順

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



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

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

3. *続行*を選択します。

Swiftグループポリシーを設定する

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

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

ユーザーを追加する（ローカルグループのみ）

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

手順

1. 必要に応じて、このグループのローカルユーザーを1人以上選択します。

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

2. *グループの作成*と*完了*を選択します。

作成したグループがグループのリストに表示されます。

テナント管理権限

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

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

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

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



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

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

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

許可	説明	詳細
エンドポイントを管理する	ユーザーがテナント マネージャまたはテナント管理 API を使用して、StorageGRIDプラットフォーム サービスの宛先として使用されるプラットフォーム サービス エンドポイントを作成または編集できるようにします。	この権限を持たないユーザーには、プラットフォーム サービス エンドポイント メニュー オプションは表示されません。
S3コンソール タブを使用する	「すべてのバケットの表示」または「すべてのバケットの管理」権限と組み合わせると、ユーザーはバケットの詳細ページの S3 コンソール タブからオブジェクトを表示および管理できるようになります。	

グループの管理

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

開始する前に

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

グループを表示または編集する

各グループの基本情報や詳細を表示、編集できます。

手順

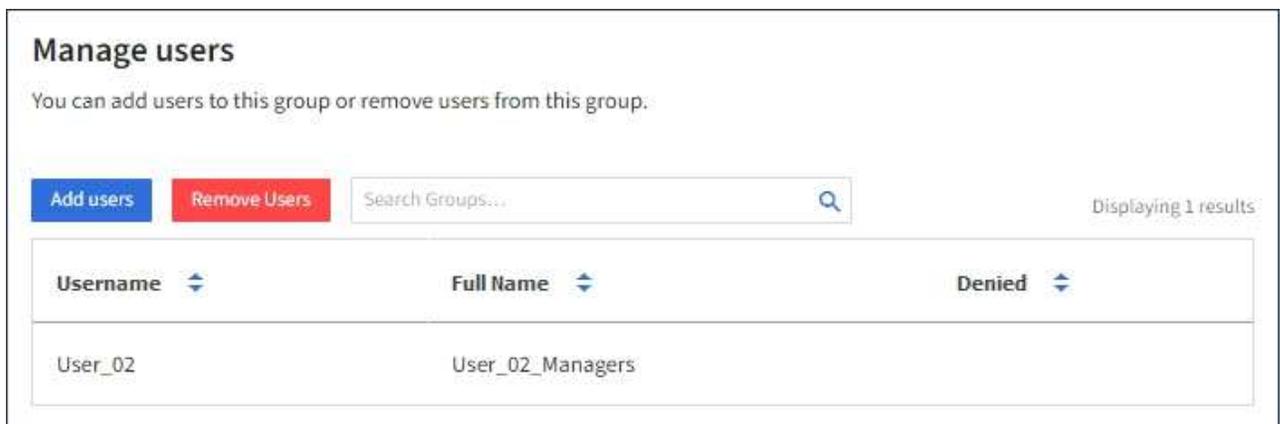
1. アクセス管理 > *グループ*を選択します。
2. [グループ] ページに提供される情報を確認します。このページには、このテナント アカウントのすべてのローカル グループとフェデレーション グループの基本情報が一覧表示されます。

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

- グループを編集または削除した場合、変更内容は他のグリッドに同期されないことを示すバナーメッセージが表示されます。
- 必要に応じて、グループが宛先グリッドのテナントに複製されなかったかどうかを示すバナー メッセージが表示されます。あなたはできる[グループのクローンを再試行する](#)それは失敗しました。

3. グループの名前を変更する場合:
 - a. グループのチェックボックスを選択します。
 - b. アクション > *グループ名の編集*を選択します。
 - c. 新しい名前を入力してください。
 - d. *変更を保存*を選択します。
4. 詳細を表示したり、追加の編集を行ったりする場合は、次のいずれかを実行します。

- グループ名を選択します。
 - グループのチェックボックスを選択し、[アクション] > [グループの詳細を表示] を選択します。
5. 各グループの次の情報が表示される概要セクションを確認します。
- 表示名
 - 一意の名前
 - タイプ
 - アクセス モード
 - 権限
 - S3ポリシー
 - このグループのユーザー数
 - テナント アカウントに グリッド フェデレーション接続の使用 権限があり、テナントのソース グリッド上のグループを表示している場合の追加フィールド:
 - クローン作成ステータス (成功*または*失敗)
 - このグループを編集または削除しても、変更内容は他のグリッドに同期されないことを示す青いバナー。
6. 必要に応じてグループ設定を編集します。見る"[S3テナントのグループを作成する](#)"そして"[Swiftテナントのグループを作成する](#)"入力内容の詳細については、こちらをご覧ください。
- a. 概要セクションで、名前または編集アイコンを選択して表示名を変更します。✎。
 - b. *グループの権限*タブで権限を更新し、*変更を保存*を選択します。
 - c. グループ ポリシー タブで変更を行い、変更の保存 を選択します。
 - S3 グループを編集している場合は、必要に応じて別の S3 グループ ポリシーを選択するか、カスタム ポリシーの JSON 文字列を入力します。
 - Swift グループを編集している場合は、オプションで **Swift** 管理者 チェックボックスをオンまたはオフにします。
7. 1人以上の既存のローカル ユーザーをグループに追加するには:
- a. [ユーザー]タブを選択します。



- b. *ユーザーを追加*を選択します。

- c. 追加する既存のユーザーを選択し、「ユーザーの追加」を選択します。

右上に成功メッセージが表示されます。

8. グループからローカル ユーザーを削除するには:

- a. [ユーザー]タブを選択します。
- b. *ユーザーを削除*を選択します。
- c. 削除するユーザーを選択し、「ユーザーの削除」を選択します。

右上に成功メッセージが表示されます。

9. 変更したセクションごとに*変更を保存*を選択したことを確認します。

重複グループ

既存のグループを複製して、新しいグループをより迅速に作成できます。



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

手順

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

グループのクローンを再試行する

失敗したクローンを再試行するには:

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

詳細については、"[テナントグループとユーザーの複製](#)"を参照してください。

1つ以上のグループを削除する

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



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

手順

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

確認ダイアログボックスが表示されます。

4. *グループの削除*または*グループの削除*を選択します。

ローカルユーザーの管理

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



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

開始する前に

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

ローカルユーザーを作成する

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

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

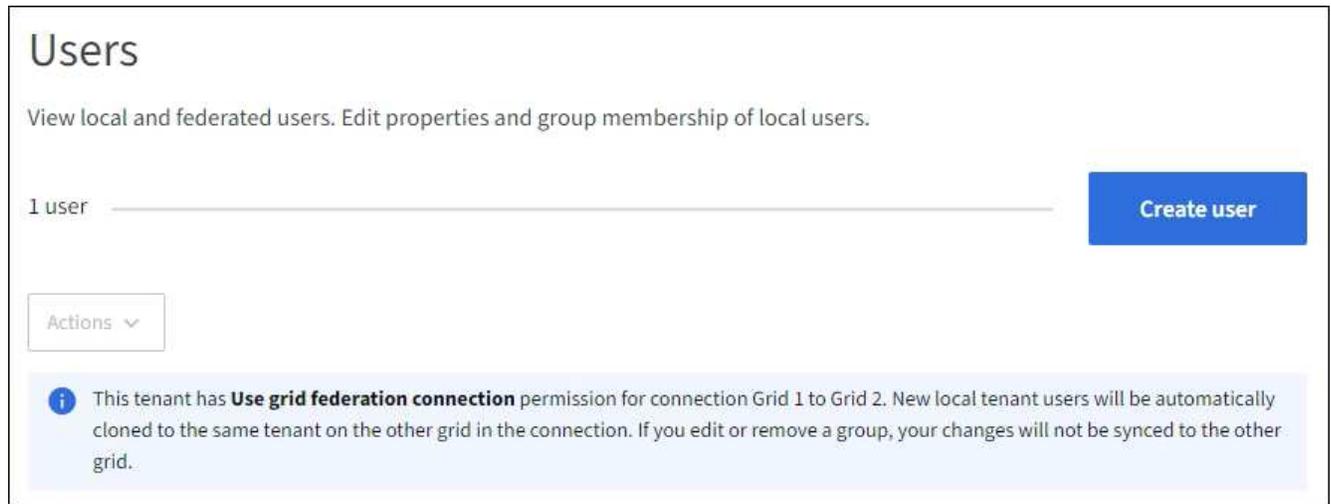
どのグループにも属していない Swift ユーザーには、管理権限も Swift コンテナへのアクセス権もありません。

ユーザー作成ウィザードにアクセスする

手順

1. アクセス管理 > *ユーザー*を選択します。

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



2. *ユーザーの作成*を選択します。

資格情報を入力してください

手順

1. *ユーザー資格情報の入力*手順では、次のフィールドに入力します。

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

2. *続行*を選択します。

グループに割り当てる

手順

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

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

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

2. ***ユーザーの作成***を選択します。

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

3. ***完了***を選択してユーザー ページに戻ります。

ローカルユーザーの表示または編集

手順

1. アクセス管理 > ***ユーザー***を選択します。

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

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

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

3. ユーザーのフルネームを変更する場合:

- a. ユーザーのチェックボックスを選択します。
- b. アクション > ***フルネームの編集***を選択します。
- c. 新しい名前を入力してください。
- d. ***変更を保存***を選択します。

4. 詳細を表示したり、追加の編集を行ったりする場合は、次のいずれかを実行します。

- ユーザー名を選択します。
- ユーザーのチェックボックスを選択し、[アクション] > [ユーザーの詳細を表示] を選択します。

5. 各ユーザーに関する次の情報が表示される概要セクションを確認します。

- フルネーム
- ユーザー名
- ユーザータイプ

- アクセス拒否
 - アクセス モード
 - グループ メンバーシップ
 - テナント アカウントに グリッド フェデレーション接続の使用 権限があり、テナントのソース グリッドでユーザーを表示している場合の追加フィールド:
 - クローン作成ステータス (成功*または*失敗)
 - このユーザーを編集しても、変更内容は他のグリッドに同期されないことを示す青いバナー。
6. 必要に応じてユーザー設定を編集します。見る [ローカルユーザーを作成する](#) 入力内容の詳細については、こちらをご覧ください。
- a. 概要セクションで、名前または編集アイコンを選択してフルネームを変更します。✎。
- ユーザー名を変更することはできません。
- b. *パスワード*タブでユーザーのパスワードを変更し、*変更を保存*を選択します。
 - c. [アクセス] タブで、ユーザーのサインインを許可する場合は [いいえ] を選択し、サインインを禁止する場合は [はい] を選択します。次に、[変更を保存] を選択します。
 - d. *アクセスキー*タブで*キーの作成*を選択し、指示に従ってください。"[別のユーザーのS3アクセスキーを作成する](#)"。
 - e. グループ タブで、グループの編集 を選択して、ユーザーをグループに追加したり、グループからユーザーを削除したりします。次に、「変更を保存」を選択します。
7. 変更したセクションごとに*変更を保存*を選択したことを確認します。

重複したローカルユーザー

ローカル ユーザーを複製して、新しいユーザーをより迅速に作成できます。



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

手順

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

ユーザーのクローンを再試行する

失敗したクローンを再試行するには:

1. ユーザー名の下に「(複製失敗)」と表示されている各ユーザーを選択します。
2. アクション > *ユーザーの複製*を選択します。

3. 複製する各ユーザーの詳細ページから複製操作のステータスを表示します。

詳細については、"[テナントグループとユーザーの複製](#)"を参照してください。

1人以上のローカルユーザーを削除する

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



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



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

手順

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

確認ダイアログボックスが表示されます。

4. *ユーザーの削除*または*ユーザーの削除*を選択します。

S3 アクセスキーを管理する

S3 アクセスキーを管理する

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

S3 アクセスキーは次のように管理できます。

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

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

独自の**S3**アクセスキーを作成する

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

開始する前に

- テナントマネージャーにサインインするには、"[サポートされているウェブブラウザ](#)"。
- あなたは、"[独自のS3認証情報またはルートアクセス権限を管理する](#)"。

タスク概要

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

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

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



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

手順

1. ストレージ **(S3)** > マイアクセスキー を選択します。

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

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



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

4. *アクセスキーの作成*を選択します。

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

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



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

6. *完了*を選択します。

新しいキーは「マイアクセスキー」ページに表示されます。

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

S3 アクセスキーを表示する

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



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

開始する前に

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

手順

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

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

期限切れのキーは自動的に削除されます。

独自のS3アクセスキーを削除する

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

開始する前に

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



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

手順

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

ページの右上に確認メッセージが表示されます。

別のユーザーの**S3**アクセスキーを作成する

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

開始する前に

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

タスク概要

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

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

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



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

手順

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

ユーザーの詳細ページが表示されます。

3. アクセス キー を選択し、キーの作成 を選択します。
4. 次のいずれかを実行します。

- 有効期限のないキーを作成するには、「有効期限を設定しない」を選択します。（デフォルト）
- *有効期限を設定する*を選択し、有効期限の日時を設定します。



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

5. *アクセスキーの作成*を選択します。

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

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



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

7. *完了*を選択します。

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

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

他のユーザーの S3 アクセスキーを表示する

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

開始する前に

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



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

手順

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

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

期限切れのキーは自動的に削除されます。

関連情報

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

他のユーザーのS3アクセスキーを削除する

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

開始する前に

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



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

手順

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

3. [ユーザーの詳細] ページで [アクセス キー] を選択し、削除する各アクセス キーのチェックボックスをオンにします。
4. アクション > *選択したキーを削除*を選択します。
5. 確認ダイアログボックスから*キーの削除*を選択します。

ページの右上に確認メッセージが表示されます。

S3バケットを管理する

S3バケットを作成する

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

開始する前に

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



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

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



各グリッドには最大 100,000 個のバケットを含めることができます。

ウィザードにアクセスする

手順

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

詳細を入力してください

手順

1. バケットの詳細を入力します。

フィールド	説明
バケット名	<p>次のルールに準拠するバケットの名前:</p> <ul style="list-style-type: none"> 各StorageGRIDシステム全体で一意である必要があります (テナント アカウント内で一意だけでなく)。 DNS に準拠している必要があります。 3 文字以上 63 文字以下でなければなりません。 各ラベルは小文字または数字で始まり、終わる必要があります、小文字、数字、ハイフンのみを使用できます。 仮想ホスト形式のリクエストにはピリオドを含めることはできません。ピリオドを使用すると、サーバーのワイルドカード証明書の検証で問題が発生します。 <p>詳細については、"バケット命名ルールに関する Amazon Web Services (AWS) ドキュメント"。</p> <p>注意: バケットを作成した後は、バケット名を変更することはできません。</p>
リージョン	<p>バケットのリージョン。</p> <p>利用可能なリージョンはStorageGRID管理者が管理します。バケットのリージョンは、オブジェクトに適用されるデータ保護ポリシーに影響を与えます可能性があります。デフォルトでは、すべてのバケットは `us-east-1` 地域。</p> <p>注意: バケットを作成した後はリージョンを変更できません。</p>

2. *続行*を選択します。

設定の管理

手順

1. 必要に応じて、バケットのオブジェクトのバージョン管理を有効にします。

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

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

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



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

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

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



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

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

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

デフォルトの保持モード	説明
ガバナンス	<ul style="list-style-type: none"> • ユーザーは `s3:BypassGovernanceRetention` 許可は `x-amz-bypass-governance-retention: true` 保持設定をバイパスするためのリクエスト ヘッダー。 • これらのユーザーは、オブジェクト バージョンを、その保持期限に達する前に削除できます。 • これらのユーザーは、オブジェクトの保持期限を増減または削除できます。
コンプライアンス	<ul style="list-style-type: none"> • オブジェクトは、保持期限に達するまで削除できません。 • オブジェクトの保持期限を増やすことはできますが、減らすことはできません。 • オブジェクトの保持期限は、その日付に達するまで削除できません。 <p>注意: グリッド管理者がコンプライアンス モードの使用を許可する必要があります。</p>

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

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

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

- オプションで、「容量制限を有効にする」を選択します。

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

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

- *バケットを作成*を選択します。

バケットが作成され、「バケット」ページのテーブルに追加されます。

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

バケットの詳細を表示

テナント アカウントでバケットを表示できます。

開始する前に

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

手順

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

バケット ページが表示されます。

- 各バケットの概要表を確認します。

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



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

Name

バケットの一意の名前。変更できません。

有効な機能

バケットに対して有効になっている機能のリスト。

S3 オブジェクトロック

バケットに対して S3 オブジェクト ロックが有効になっているかどうか。

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

リージョン

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

オブジェクト数

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

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

使用スペース

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

この値の更新には最大 10 分かかる場合があります。

使用法

バケットの容量制限の使用率（設定されている場合）。

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

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

容量

設定されている場合、バケットの容量制限。

作成日

バケットが作成された日時。この列はデフォルトでは非表示になっています。

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

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



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

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

d. 必要に応じて、各タブでバケットの設定を表示または変更します。

- **S3 コンソール**: バケットのオブジェクトを表示します。詳細については、"[S3コンソールを使用する](#)"。
- **バケット オプション**: オプション設定を表示または変更します。S3 オブジェクトロックなど一部の設定は、バケットの作成後は変更できません。
 - "[バケットの一貫性を管理する](#)"
 - "[最終アクセス時間の更新](#)"
 - "[容量制限](#)"
 - "[オブジェクトのバージョン管理](#)"
 - "[S3 オブジェクトロック](#)"
 - "[デフォルトのバケット保持](#)"
 - "[クロスグリッドレプリケーションを管理する](#)" (入居者に許可されている場合)
- **プラットフォームサービス**: "[プラットフォームサービスの管理](#)" (入居者に許可されている場合)
- **バケット アクセス**: オプション設定を表示または変更します。特定のアクセス権限が必要です。
 - 設定"[クロスオリジンリソース共有 \(CORS\)](#)" そのため、バケットとバケット内のオブジェクトは他のドメインの Web アプリケーションからアクセスできるようになります。
 - "[ユーザーアクセスを制御する](#)" S3 バケットとそのバケット内のオブジェクト。

バケットに**ILM**ポリシータグを適用する

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

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



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

開始する前に

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

手順

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

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

2. ILM ポリシー タグを割り当てるバケットの名前を選択します。

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



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

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



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

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



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



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



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

バケットポリシーを管理する

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

開始する前に

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

手順

1. *バケット*を選択し、管理するバケットを選択します。

2. バケットの詳細ページで、バケット アクセス > バケット ポリシー を選択します。

3. 次のいずれかを実行します。

- *ポリシーを有効にする*チェックボックスを選択してバケットポリシーを入力します。次に、有効な JSON 形式の文字列を入力します。

各バケット ポリシーのサイズ制限は 20,480 バイトです。

- 文字列を編集して既存のポリシーを変更します。
- *ポリシーを有効にする*の選択を解除してポリシーを無効にします。

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

バケットの一貫性を管理する

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

開始する前に

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

バケットの一貫性ガイドライン

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

バケットの一貫性を変更する

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



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

手順

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

バケットの詳細ページが表示されます。

3. バケット オプション タブから、** アコーディオンを選択します。

4. このバケット内のオブジェクトに対して実行される操作の一貫性を選択します。

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

5. ***変更を保存***を選択します。

バケット設定を変更すると何が起るか

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

次のバケット設定では、デフォルトで強力な一貫性が使用されます。どのサイトでも2つ以上のストレージノードが利用できない場合、またはサイトが利用できない場合は、これらの設定に対する変更が利用できない可能性があります。

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



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

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

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



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

最終アクセス時間の更新を有効または無効にする

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

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

開始する前に

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

タスク概要

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

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

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

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



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

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

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

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

される動作をまとめたものです。

リクエストの種類	最終アクセス時刻が無効になっている場合の動作（デフォルト）		最終アクセス時刻が有効になっている場合の動作	
	最終アクセス時間は更新されましたか？	オブジェクトが ILM 評価キューに追加されましたか？	最終アクセス時間は更新されましたか？	オブジェクトが ILM 評価キューに追加されましたか？
オブジェクト、そのアクセス制御リスト、またはそのメタデータの取得要求	いいえ	いいえ	はい	はい
オブジェクトのメタデータの更新リクエスト	はい	はい	はい	はい
オブジェクトまたはオブジェクトのバージョンの一覧表示のリクエスト	いいえ	いいえ	いいえ	いいえ
あるバケットから別のバケットにオブジェクトをコピーするリクエスト	<ul style="list-style-type: none"> • いいえ、ソースコピーの場合 • はい、宛先コピー用 	<ul style="list-style-type: none"> • いいえ、ソースコピーの場合 • はい、宛先コピー用 	<ul style="list-style-type: none"> • はい、ソースコピーの場合 • はい、宛先コピー用 	<ul style="list-style-type: none"> • はい、ソースコピーの場合 • はい、宛先コピー用
マルチパートアップロードの完了リクエスト	はい、組み立てられたオブジェクトの場合	はい、組み立てられたオブジェクトの場合	はい、組み立てられたオブジェクトの場合	はい、組み立てられたオブジェクトの場合

手順

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

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

バケットのオブジェクトのバージョン管理を変更する

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

開始する前に

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

タスク概要

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

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

詳細については、次を参照してください。

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

手順

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

バケットの詳細ページが表示されます。

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

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

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

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

5. *変更を保存*を選択します。

S3 オブジェクトロックを使用してオブジェクトを保持する

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



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

S3 オブジェクトロックとは何ですか？

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

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

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

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

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

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

保持モード

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

- コンプライアンスモードの場合:

- オブジェクトは、保持期限に達するまで削除できません。
- オブジェクトの保持期限を増やすことはできますが、減らすことはできません。
- オブジェクトの保持期限は、その日付に達するまで削除できません。

- ガバナンス モードの場合:

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

オブジェクトバージョンの保持設定

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

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



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

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

バケットのデフォルトの保持設定

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

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

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

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

S3 オブジェクトロックタスク

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

グリッド管理者

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

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

テナントユーザー

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

S3 オブジェクトロックが有効になっているバケットの要件

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

S3 オブジェクトロックが有効になっているバケット内のオブジェクトの要件

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

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

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

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

1. オブジェクトの取り込み

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

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

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

2. オブジェクトの保持と削除

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

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

従来のコンプライアンス バケットを引き続き管理できますか？

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

S3 オブジェクトロックのデフォルト保持を更新

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

開始する前に

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

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

手順

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

バケットの詳細ページが表示されます。

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

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

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

デフォルトの保持モード	説明
ガバナンス	<ul style="list-style-type: none"> • ユーザーは `s3:BypassGovernanceRetention` 許可は `x-amz-bypass-governance-retention: true` 保持設定をバイパスするためのリクエスト ヘッダー。 • これらのユーザーは、オブジェクト バージョンを、その保持期限に達する前に削除できます。 • これらのユーザーは、オブジェクトの保持期限を増減または削除できます。
コンプライアンス	<ul style="list-style-type: none"> • オブジェクトは、保持期限に達するまで削除できません。 • オブジェクトの保持期限を増やすことはできますが、減らすことはできません。 • オブジェクトの保持期限は、その日付に達するまで削除できません。 <p>注意: グリッド管理者がコンプライアンス モードの使用を許可する必要があります。</p>

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

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

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

7. *変更を保存*を選択します。

クロスオリジンリソース共有 (CORS) を構成する

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

開始する前に

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

タスク概要

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

バケットのCORSを有効にする

手順

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

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

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

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

バケットの詳細ページが表示されます。

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

CORS設定を変更する

手順

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

CORS設定を無効にする

手順

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

バケット内のオブジェクトを削除する

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

考慮事項と要件

これらの手順を実行する前に、次の点に注意してください。

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



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

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

開始する前に

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

手順

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

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

2. アクション メニューまたは特定のバケットの詳細ページを使用します。

[操作]メニュー

- a. オブジェクトを削除する各バケットのチェックボックスを選択します。
- b. アクション > *バケット内のオブジェクトの削除*を選択します。

詳細ページ

- a. バケット名を選択すると、その詳細が表示されます。
- b. *バケット内のオブジェクトを削除*を選択します。

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

4. 削除操作が開始されるまで待ちます。

数分後:

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

Buckets > my-bucket

my-bucket (read-only)

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

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

Delete bucket

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

0% (0 of 3 objects deleted)

Stop deleting objects

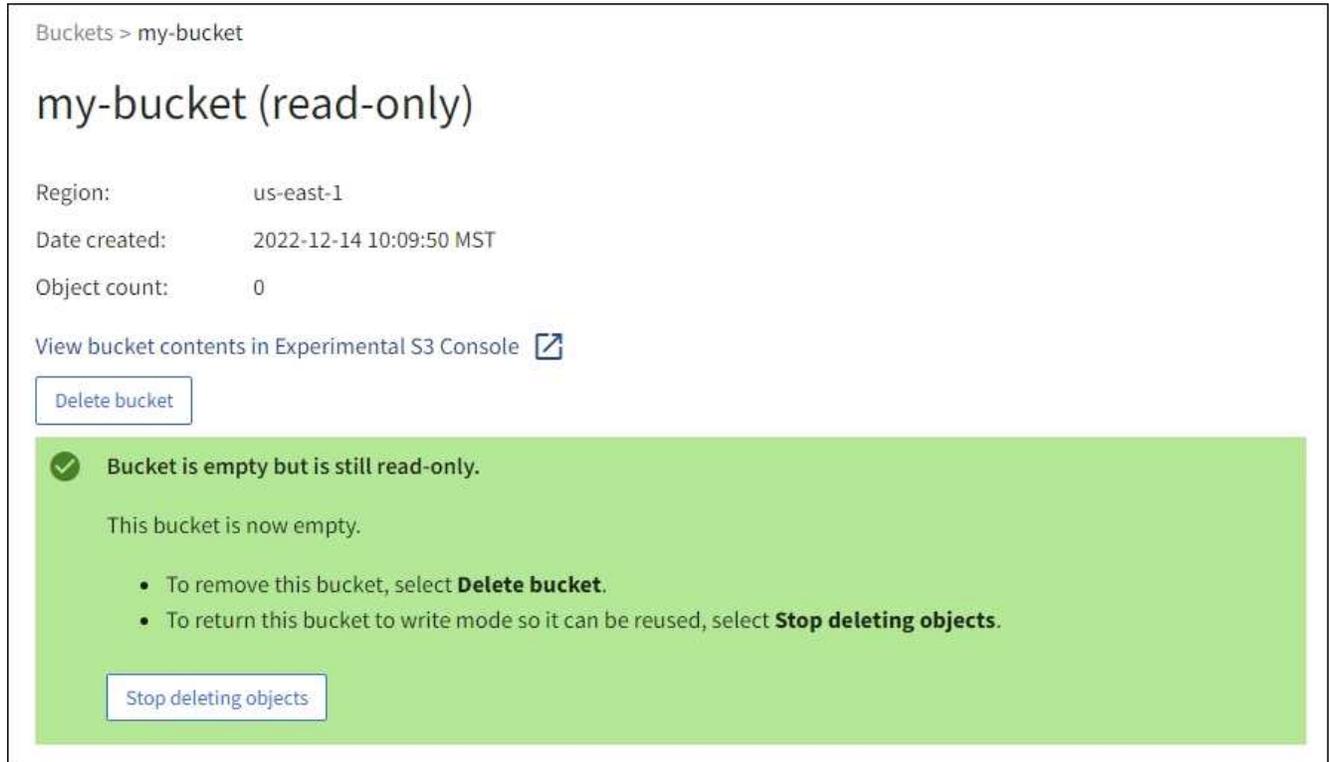
5. 操作の実行中に必要に応じて、[オブジェクトの削除を停止] を選択してプロセスを停止します。次に、オプションで「バケット内のオブジェクトを削除」を選択してプロセスを再開します。

*オブジェクトの削除を停止*を選択すると、バケットは書き込みモードに戻りますが、削除されたオブジ

ェクトにアクセスしたり復元したりすることはできません。

6. 操作が完了するまでお待ちください。

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



7. 次のいずれかを実行します。

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



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

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

S3バケットを削除する

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

開始する前に

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

- 削除するバケットは空です。削除したいバケットが空でない場合は、"[バケットからオブジェクトを削除する](#)"。

タスク概要

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

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

手順

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

「バケット」ページが表示され、既存の S3 バケットがすべて表示されます。

2. アクション メニューまたは特定のバケットの詳細ページを使用します。

[操作]メニュー

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

詳細ページ

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

3. 確認ダイアログボックスが表示されたら、「はい」を選択します。

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

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

S3コンソールを使用する

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

S3 コンソールでは次のことが可能です。

- オブジェクトのアップロード、ダウンロード、名前変更、コピー、移動、削除
- オブジェクトのバージョンを表示、元に戻す、ダウンロード、削除する
- 接頭辞でオブジェクトを検索する
- オブジェクトタグを管理する
- オブジェクトのメタデータを表示する

- フォルダの表示、作成、名前の変更、コピー、移動、削除

S3 コンソールは、最も一般的なケースにおいて、改善されたユーザー エクスペリエンスを提供します。あらゆる状況で CLI または API 操作を置き換えるようには設計されていません。



S3 コンソールを使用すると操作に時間がかかりすぎる場合 (数分または数時間など)、次のことを検討してください。

- 選択したオブジェクトの数を減らす
- 非グラフィカル (API または CLI) メソッドを使用してデータにアクセスする

開始する前に

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

手順

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

追加情報

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

S3 プラットフォーム サービスを管理する

S3 プラットフォームサービス

プラットフォームサービスの概要と考慮事項

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

S3の詳細については、"[S3 REST APIを使用する](#)"。

プラットフォームサービスの概要

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

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

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



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

プラットフォームサービスの構成方法

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

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

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

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

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

プラットフォームサービス	S3 REST API	参照
CloudMirrorレプリケーション	<ul style="list-style-type: none"> • GetBucketReplication • PutBucketレプリケーション 	<ul style="list-style-type: none"> • "CloudMirrorレプリケーション" • "バケットの操作"
通知	<ul style="list-style-type: none"> • GetBucketNotificationConfiguration • PutBucketNotificationConfiguration 	<ul style="list-style-type: none"> • "通知" • "バケットの操作"
検索統合	<ul style="list-style-type: none"> • バケットメタデータ通知設定の取得 • PUT バケットメタデータ通知設定 	<ul style="list-style-type: none"> • "検索統合" • "StorageGRIDカスタム操作"

プラットフォームサービスの利用に関する考慮事項

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

考慮事項	詳細
注文保証	<p>StorageGRID は、サイト内のオブジェクトに対する操作の順序を保証します。オブジェクトに対するすべての操作が同じサイト内で行われる限り、最終的なオブジェクトの状態 (レプリケーションの場合) は常にStorageGRID内の状態と同じになります。</p> <p>StorageGRID は、StorageGRIDサイト間で操作が行われるときに、リクエストを順序付けるために最善を尽くします。たとえば、最初にサイト A にオブジェクトを書き込み、その後サイト B で同じオブジェクトを上書きした場合、CloudMirror によって宛先バケットに複製された最終的なオブジェクトが新しいオブジェクトである保証はありません。</p>
ILMによるオブジェクトの削除	<p>AWS CRR および Amazon Simple Notification Service の削除動作と一致させるため、StorageGRID ILM ルールによりソースバケット内のオブジェクトが削除された場合、CloudMirror およびイベント通知リクエストは送信されません。たとえば、ILM ルールによって 14 日後にオブジェクトが削除された場合、CloudMirror またはイベント通知リクエストは送信されません。</p> <p>対照的に、検索統合リクエストは、ILM によってオブジェクトが削除されたときに送信されます。</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、もしあなたが `ssl.client.auth` に設定 `required` Kafka ブローカー構成では、Kafka エンドポイント構成の問題が発生する可能性があります。</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、ユーザー名とパスワードの認証情報が必要です。</p> <ul style="list-style-type: none"> • SASL/プレーン • SASL/SCRAM-SHA-256 • SASL/SCRAM-SHA-512 <p>注: 構成されたストレージ プロキシ設定は、Kafka プラットフォーム サービス エンドポイントには適用されません。</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
レプリケーションステータス	StorageGRIDはサポートしていません `x-amz-replication-status` ヘッダ。

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

CloudMirrorレプリケーションサービスを理解する

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

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



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

CloudMirror と ILM

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

CloudMirror とクロスグリッドレプリケーション

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

CloudMirror と S3 バケット

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

既存のバケット

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



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

複数の宛先バケット

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

バージョン管理されたバケットまたはバージョン管理されていないバケット

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

削除、レプリケーションループ、イベント

削除動作

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

レプリケーションループからの保護

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



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

宛先バケット内のイベント

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

バケットの通知を理解する

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

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

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

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

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

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

- s3:オブジェクト作成:コピー
 - s3:ObjectCreated:CompleteMultipartUpload
 - s3:オブジェクトが削除されました:
 - s3:オブジェクトが削除されました:削除
 - s3:オブジェクトが削除されました:削除マーカーが作成されました
 - s3:オブジェクトの復元:投稿
- StorageGRIDから送信されるイベント通知では標準の JSON 形式が使用されますが、表に示すように、一部のキーは含まれず、他のキーには特定の値が使用されます。

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

検索統合サービスを理解する

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

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

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

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



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

検索統合とS3バケット

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

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



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

検索通知

メタデータ通知は次の場合に生成され、配信キューに追加されます。

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

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

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

検索統合サービスとElasticsearch

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

プラットフォームサービスのエンドポイントを管理する

プラットフォームサービスのエンドポイントを構成する

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

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

プラットフォーム サービス エンドポイントとは何ですか？

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

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

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

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

CloudMirror レプリケーションのエンドポイント

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

通知のエンドポイント

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

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

検索統合サービスのエンドポイント

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

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

関連情報

["StorageGRIDの管理"](#)

プラットフォーム サービス エンドポイントの **URN** を指定します

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

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

URN要素

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

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

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

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

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

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

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

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

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

AWS および GCP でホストされているサービスの URN

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

- CloudMirror レプリケーション:

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

- 通知:

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

- 検索統合:

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



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

ローカルでホストされるサービスのURN

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

- CloudMirror レプリケーション:

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

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

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

• 通知：

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

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

Kafka エンドポイントを指定します。

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

• 検索統合:

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



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

プラットフォーム サービス エンドポイントを作成する

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

開始する前に

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



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

- ユニークリソース名 (URN)

"プラットフォーム サービス エンドポイントの URN を指定します"

- 認証資格情報（必要な場合）：

検索統合エンドポイント

検索統合エンドポイントでは、次の資格情報を使用できます。

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

CloudMirror レプリケーションエンドポイント

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

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

Amazon SNS エンドポイント

Amazon SNS エンドポイントの場合、次の認証情報を使用できます。

- アクセスキー: アクセスキーIDとシークレットアクセスキー

Kafka エンドポイント

Kafka エンドポイントの場合、次の資格情報を使用できます。

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

- セキュリティ証明書（カスタム CA 証明書を使用している場合）

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

手順

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

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

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

次のいずれかの形式を使用します。

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

ポートを指定しない場合は、次のデフォルトポートが使用されます。

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

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

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

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



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

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

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



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

5. エンドポイントの一意的リソース名 (URN) を入力します。



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

6. *続行*を選択します。

7. *認証タイプ*の値を選択します。

検索統合エンドポイント

検索統合エンドポイントの資格情報を入力またはアップロードします。

指定する資格情報には、宛先リソースに対する書き込み権限が必要です。

認証タイプ	説明	Credentials
匿名	宛先への匿名アクセスを提供します。セキュリティが無効になっているエンドポイントでのみ機能します。	認証なし。
アクセス キー	AWS スタイルの認証情報を使用して、宛先との接続を認証します。	<ul style="list-style-type: none">• アクセス キー ID• シークレット アクセス キー
基本的なHTTP	ユーザー名とパスワードを使用して、宛先への接続を認証します。	<ul style="list-style-type: none">• ユーザー名• パスワード

CloudMirror レプリケーションエンドポイント

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

指定する資格情報には、宛先リソースに対する書き込み権限が必要です。

認証タイプ	説明	Credentials
匿名	宛先への匿名アクセスを提供します。セキュリティが無効になっているエンドポイントでのみ機能します。	認証なし。
アクセス キー	AWS スタイルの認証情報を使用して、宛先との接続を認証します。	<ul style="list-style-type: none">• アクセス キー ID• シークレット アクセス キー
CAP (C2Sアクセスポータル)	証明書とキーを使用して、宛先への接続を認証します。	<ul style="list-style-type: none">• 一時認証情報URL• サーバーCA証明書 (PEMファイルのアップロード)• クライアント証明書 (PEMファイルのアップロード)• クライアント秘密鍵 (PEMファイルのアップロード、OpenSSL暗号化形式、または暗号化されていない秘密鍵形式)• クライアントの秘密鍵のパスフレーズ (オプション)

Amazon SNSエンドポイント

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

指定する資格情報には、宛先リソースに対する書き込み権限が必要です。

認証タイプ	説明	Credentials
匿名	宛先への匿名アクセスを提供します。セキュリティが無効になっているエンドポイントでのみ機能します。	認証なし。
アクセス キー	AWS スタイルの認証情報を使用して、宛先との接続を認証します。	<ul style="list-style-type: none">• アクセス キー ID• シークレット アクセス キー

Kafka エンドポイント

Kafka エンドポイントの資格情報を入力またはアップロードします。

指定する資格情報には、宛先リソースに対する書き込み権限が必要です。

認証タイプ	説明	Credentials
匿名	宛先への匿名アクセスを提供します。セキュリティが無効になっているエンドポイントでのみ機能します。	認証なし。
SASL/プレーン	プレーンテキストのユーザー名とパスワードを使用して、宛先への接続を認証します。	<ul style="list-style-type: none">• ユーザー名• パスワード
SASL/SCRAM-SHA-256	チャレンジ レスポンス プロトコルと SHA-256 ハッシュを使用したユーザー名とパスワードを使用して、宛先への接続を認証します。	<ul style="list-style-type: none">• ユーザー名• パスワード
SASL/SCRAM-SHA-512	チャレンジ レスポンス プロトコルと SHA-512 ハッシュを使用したユーザー名とパスワードを使用して、宛先への接続を認証します。	<ul style="list-style-type: none">• ユーザー名• パスワード

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

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

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

10. *エンドポイントのテストと作成*を選択します。

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



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

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

関連情報

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

プラットフォーム サービス エンドポイントのテスト接続

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

開始する前に

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

タスク概要

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

手順

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

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

2. 接続をテストするエンドポイントを選択します。

エンドポイントの詳細ページが表示されます。

3. *テスト接続*を選択します。

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

プラットフォーム サービス エンドポイントを編集する

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

開始する前に

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

手順

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

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

2. 編集するエンドポイントを選択します。

エンドポイントの詳細ページが表示されます。

3. *構成*を選択します。

4. 必要に応じて、エンドポイントの構成を変更します。



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

- 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 .
- 必要に応じて、URI を変更します。
- 必要に応じて、認証タイプを変更します。
 - アクセス キー認証の場合は、**S3** キーの編集 を選択し、新しいアクセス キー ID とシークレットアクセス キーを貼り付けて、必要に応じてキーを変更します。変更をキャンセルする必要がある場合は、「**S3** キー編集を元に戻す」を選択します。

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



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

d. 必要に応じて、サーバーの検証方法を変更します。

5. *テストして変更を保存*を選択します。

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

プラットフォーム サービス エンドポイントを削除する

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

開始する前に

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

手順

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

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

2. 削除する各エンドポイントのチェックボックスを選択します。



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

3. アクション > *エンドポイントの削除*を選択します。

確認メッセージが表示されます。

4. *エンドポイントの削除*を選択します。

プラットフォーム サービスのエンドポイント エラーのトラブルシューティング

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

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

エラーが発生したかどうかを確認する

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

 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が、プラットフォーム サービス エンドポイント ページの上部にも表示されます。より詳細なエラー メッセージを表示するには:

手順

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

エラーがまだ発生しているか確認する

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

手順

1. エンドポイントを選択します。

エンドポイントの詳細ページが表示されます。
2. 接続 > *接続テスト*を選択します。

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

エンドポイントエラーを解決する

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

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

手順

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

権限が不十分なエンドポイント認証情報

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

関連情報

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

CloudMirrorレプリケーションを構成する

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

開始する前に

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

タスク概要

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

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



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

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

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

手順

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

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

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

バケットの詳細ページが表示されます。

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



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

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

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

- b. オブジェクトが宛先バケットに複製されたことを確認します。

小さなオブジェクトの場合、レプリケーションはすぐに行われます。

関連情報

["プラットフォーム サービス エンドポイントを作成する"](#)

イベント通知の設定

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

開始する前に

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

タスク概要

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

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

バケットのイベント通知を構成するときは、次の要件と特性に注意してください。

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

手順

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

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

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

バケットの詳細ページが表示されます。

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



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

7. イベント通知が正しく構成されていることを確認します。
 - a. 構成 XML で設定された通知をトリガーするための要件を満たすソース バケット内のオブジェクトに対してアクションを実行します。

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

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

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

```

{
  "Records": [
    {
      "eventVersion": "2.0",
      "eventSource": "sgws:s3",
      "eventTime": "2017-08-08T23:52:38Z",
      "eventName": "ObjectCreated:Put",
      "userIdentity": {
        "principalId": "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"
        }
      }
    }
  ]
}

```

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

関連情報

["バケットの通知を理解する"](#)

["S3 REST APIを使用する"](#)

"プラットフォーム サービス エンドポイントを作成する"

検索統合サービスを構成する

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

開始する前に

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

タスク概要

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

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

手順

1. バケットの検索統合を有効にします。

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

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

必要に応じて、[メタデータ構成XMLの例](#)。

```

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

```

メタデータ通知構成 XML の要素:

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

Name	説明	必須
壺	<p>オブジェクト メタデータが送信される宛先の URN。次のプロパティを持つStorageGRIDエンドポイントの URN である必要があります。</p> <ul style="list-style-type: none"> • `es` 3 番目の要素である必要があります。 • URNは、メタデータが格納されているインデックスとタイプで終わる必要があります。形式は次のようになります。 domain-name/myindex/mytype 。 <p>エンドポイントは、テナント マネージャーまたはテナント管理 API を使用して構成されます。それらは次の形式をとりません:</p> <ul style="list-style-type: none"> • arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype • urn:mysite:es:::mydomain/myindex/mytype <p>構成 XML を送信する前にエンドポイントを構成する必要があります。そうしないと、404 エラーが発生して構成が失敗します。</p> <p>URN は Destination 要素に含まれます。</p>	はい

2. テナント マネージャーで、ストレージ **(S3)** > バケット を選択します。

3. ソースバケットの名前を選択します。

バケットの詳細ページが表示されます。

4. プラットフォームサービス > *検索統合*を選択します

5. *検索統合を有効にする*チェックボックスを選択します。

6. メタデータ通知構成をテキスト ボックスに貼り付け、[変更を保存] を選択します。



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

7. 検索統合サービスが正しく構成されていることを確認します。

a. 構成 XML で指定されているメタデータ通知をトリガーするための要件を満たすオブジェクトをソースバケットに追加します。

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

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

終了後の操作

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

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

例: すべてのオブジェクトに適用されるメタデータ通知設定

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

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

例: 2つのルールを使用したメタデータ通知構成

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

```

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Images-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/images</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Videos-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/videos</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-west-1:2222222:domain/es-
domain/graphics/videotype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>

```

メタデータ通知形式

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

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

```

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

```

JSONドキュメントに含まれるフィールド

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

バケットとオブジェクトの情報

bucket: バケットの名前

key: オブジェクトキー名

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

region: バケット領域、例 us-east-1

システムメタデータ

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

md5: オブジェクトハッシュ

ユーザーメタデータ

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

key:value

タグ

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

key:value

Elasticsearchで結果を表示する方法

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

S3 REST APIを使用する

S3 REST API のサポート対象バージョンとアップデート

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

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るようになります。クライアントアプリケーションの現在の S3 REST API 呼び出しの使用に対する最小限の変更が必要です。

サポート対象のバージョン

StorageGRID は、次の特定のバージョンの S3 と HTTP をサポートしています。

項目	version
S3 API仕様	"Amazon Web Services (AWS) ドキュメント: Amazon Simple Storage Service API リファレンス"
HTTP	1.1 HTTP の詳細については、HTTP/1.1 (RFC 7230-35) を参照してください。 "IETF RFC 2616: ハイパーテキスト転送プロトコル (HTTP/1.1)" 注意: StorageGRID はHTTP/1.1 パイプラインをサポートしていません。

S3 REST API サポートの更新

リリース	コメント
11.9	<ul style="list-style-type: none">• 次のリクエストとサポートされているヘッダーに対して、事前計算された SHA-256 チェックサム値のサポートが追加されました。この機能を使用すると、アップロードされたオブジェクトの整合性を検証できます。<ul style="list-style-type: none">◦ 完全なマルチパートアップロード: x-amz-checksum-sha256◦ マルチパートアップロードの作成: x-amz-checksum-algorithm◦ オブジェクトを取得: x-amz-checksum-mode◦ ヘッドオブジェクト: x-amz-checksum-mode◦ ListParts◦ オブジェクトを配置: x-amz-checksum-sha256◦ アップロードパーツ: x-amz-checksum-sha256• グリッド管理者がテナント レベルの保持とコンプライアンス設定を制御できるようになりました。これらの設定は S3 オブジェクト ロックの設定に影響します。<ul style="list-style-type: none">◦ バケットのデフォルトの保持モードとオブジェクト保持モード: グリッド管理者が許可している場合、ガバナンスまたはコンプライアンス。◦ バケットのデフォルトの保持期間とオブジェクトの保持期限: グリッド管理者が設定した最大保持期間で許可されている値以下である必要があります。• サポートの改善 `aws-chunked` コンテンツのエンコーディングとストリーミング `x-amz-content-sha256` 値観。制限事項:<ul style="list-style-type: none">◦ 存在する場合、`chunk-signature` オプションであり検証されません◦ 存在する場合、`x-amz-trailer` コンテンツは無視されます

リリース	コメント
11.8	S3オペレーションの名前を、" Amazon Web Services (AWS) ドキュメント: Amazon Simple Storage Service API リファレンス "。
11.7	<ul style="list-style-type: none"> • 追加した"クイックリファレンス: サポートされている S3 API リクエスト"。 • S3 オブジェクト ロックで GOVERNANCE モードを使用するためのサポートが追加されました。 • StorageGRID固有のサポートを追加 `x-ntap-sg-cgr-replication-status` GET Object および HEAD Object リクエストの応答ヘッダー。このヘッダーは、クロスグリッド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提供します。 • SelectObjectContent リクエストは Parquet オブジェクトをサポートするようになりました。
11.6	<ul style="list-style-type: none"> • 使用するためのサポートを追加しました `partNumber` GET Object リクエストと HEAD Object リクエストのリクエストパラメータ。 • S3 オブジェクト ロックのバケットレベルでのデフォルトの保持モードとデフォルトの保持期間のサポートが追加されました。 • のサポートを追加しました `s3:object-lock-remaining-retention-days` オブジェクトの許容保持期間の範囲を設定するためのポリシー条件キー。 • 単一の PUT Object 操作の最大推奨サイズを 5 GiB (5,368,709,120 バイト) に変更しました。5 GiB を超えるオブジェクトがある場合は、代わりにマルチパートアップロードを使用します。
11.5	<ul style="list-style-type: none"> • バケット暗号化の管理のサポートが追加されました。 • S3 オブジェクト ロックと廃止された従来のコンプライアンス リクエストのサポートが追加されました。 • バージョン管理されたバケットで DELETE Multiple Objects を使用するためのサポートが追加されました。 • その `Content-MD5` リクエストヘッダーが正しくサポートされるようになりました。
11.4	<ul style="list-style-type: none"> • DELETE バケット タグ付け、GET バケット タグ付け、PUT バケット タグ付けのサポートが追加されました。コスト配分タグはサポートされていません。 • StorageGRID 11.4 で作成されたバケットの場合、パフォーマンスのベストプラクティスを満たすためにオブジェクトキー名を制限する必要がなくなりました。 • バケット通知のサポートを追加しました `s3:ObjectRestore:Post` イベントの種類。 • マルチパートパーツに対する AWS サイズ制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は 5 MiB ~ 5 GiB の範囲でなければなりません。最後の部分は 5 MiB より小さくても構いません。 • TLS 1.3のサポートを追加しました

リリース	コメント
11.3	<ul style="list-style-type: none"> 顧客提供のキーを使用したオブジェクト データのサーバー側暗号化 (SSE-C) のサポートが追加されました。 DELETE、GET、PUTバケットライフサイクル操作（有効期限アクションのみ）のサポートが追加されました。`x-amz-expiration`レスポンス ヘッダー。 取り込み時に同期配置を使用する ILM ルールの影響を説明するために、PUT オブジェクト、PUT オブジェクト - コピー、およびマルチパートアップロードを更新しました。 TLS 1.1 暗号はサポートされなくなりました。
11.2	<p>Cloud Storage Pools で使用するための POST Object restore のサポートが追加されました。グループおよび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に AWS 構文を使用するためのサポートが追加されました。StorageGRID構文を使用する既存のグループおよびバケット ポリシーは引き続きサポートされます。</p> <p>注: カスタムStorageGRID機能で使用されるものも含め、他の構成 JSON/XML での ARN/URN の使用は変更されていません。</p>
11.1	クロスオリジン リソース共有 (CORS)、グリッド ノードへの S3 クライアント接続用の HTTP、バケットのコンプライアンス設定のサポートが追加されました。
11.0	バケットのプラットフォーム サービス (CloudMirror レプリケーション、通知、Elasticsearch 検索統合) を構成するためのサポートが追加されました。また、バケットのオブジェクトタグ付け場所制約と、利用可能な一貫性のサポートも追加されました。
10.4	ILM スキャンのバージョン管理の変更、エンドポイント ドメイン名ページの更新、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。
10.2	グループおよびバケット アクセス ポリシー、およびマルチパート コピー (アップロード部分 - コピー) 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、仮想ホストスタイルのリクエスト、v4 認証のサポートが追加されました。
10.0	StorageGRIDシステムによる S3 REST API の初期サポート。現在サポートされている <i>Simple Storage Service API Reference</i> のバージョンは 2006-03-01 です。

クイックリファレンス: サポートされている **S3 API** リクエスト

このページでは、StorageGRID が Amazon Simple Storage Service (S3) API をサポートする方法についてまとめています。

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



各操作の AWS ドキュメントを表示するには、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リクエストヘッダー

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ています。

- versionId (オブジェクト操作に必要な場合)

特に記載がない限り、次の一般的なリクエスト ヘッダーがサポートされています。

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

関連情報

- ["S3 REST API実装の詳細"](#)
- ["Amazon Simple Storage Service API リファレンス: 共通リクエストヘッダー"](#)

"AbortMultipartUpload"

URIクエリパラメータとリクエストヘッダー

StorageGRIDはすべてをサポート [共通パラメータとヘッダー](#) このリクエストには、次の追加の URI クエリ パラメータが含まれます。

- uploadId

リクエスト本文

なし

StorageGRID ドキュメント

["マルチパートアップロードの操作"](#)

"CompleteMultipartUpload"

URIクエリパラメータとリクエストヘッダー

StorageGRIDはすべてをサポート [共通パラメータとヘッダー](#) このリクエストには、次の追加の URI クエリ パラメータが含まれます。

- uploadId
- x-amz-checksum-sha256

リクエストボディのXMLタグ

StorageGRID は、次のリクエスト ボディ XML タグをサポートしています。

- ChecksumSHA256
- CompleteMultipartUpload
- ETag
- Part
- PartNumber

StorageGRIDドキュメント

["CompleteMultipartUpload"](#)

["CopyObject"](#)

URIクエリパラメータとリクエストヘッダー

StorageGRIDはすべてをサポート [共通パラメータとヘッダー](#) このリクエストには、次の追加ヘッダーが含まれます。

- 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>

リクエスト本文

なし

StorageGRIDドキュメント

["CopyObject"](#)

"CreateBucket"

URIクエリパラメータとリクエストヘッダー

StorageGRIDはすべてをサポート [共通パラメータとヘッダー](#) このリクエストには、次の追加ヘッダーが含まれます。

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

リクエスト本文

StorageGRID は、実装時に Amazon S3 REST API によって定義されたすべてのリクエスト ボディ パラメータをサポートします。

StorageGRIDドキュメント

["バケットの操作"](#)

"CreateMultipartUpload"

URIクエリパラメータとリクエストヘッダー

StorageGRIDはすべてをサポート [共通パラメータとヘッダー](#) このリクエストには、次の追加ヘッダーが含まれます。

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- Expires
- x-amz-checksum-algorithm
- 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>

リクエスト本文

なし

StorageGRIDドキュメント

["CreateMultipartUpload"](#)

["DeleteBucket"](#)

URIクエリパラメータとリクエストヘッダー

StorageGRIDはすべてをサポート [共通パラメータとヘッダー](#) このリクエストに対して。

StorageGRIDドキュメント

["バケットの操作"](#)

["バケットCorsの削除"](#)

URIクエリパラメータとリクエストヘッダー

StorageGRIDはすべてをサポート [共通パラメータとヘッダー](#) このリクエストに対して。

リクエスト本文

なし

StorageGRIDドキュメント

["バケットの操作"](#)

["バケット暗号化の削除"](#)

URIクエリパラメータとリクエストヘッダー

StorageGRIDはすべてをサポート [共通パラメータとヘッダー](#) このリクエストに対して。

リクエスト本文

なし

StorageGRIDドキュメント

["バケットの操作"](#)

["DeleteBucketLifecycle"](#)

URIクエリパラメータとリクエストヘッダー

StorageGRIDはすべてをサポート [共通パラメータとヘッダー](#) このリクエストに対して。

リクエスト本文

なし

StorageGRID ドキュメント

- "バケットの操作"
- "S3ライフサイクル設定を作成する"

"DeleteBucketPolicy"

URIクエリパラメータとリクエストヘッダー

StorageGRIDはすべてをサポート [共通パラメータとヘッダー](#) このリクエストに対して。

リクエスト本文

なし

StorageGRID ドキュメント

"バケットの操作"

"バケットレプリケーションの削除"

URIクエリパラメータとリクエストヘッダー

StorageGRIDはすべてをサポート [共通パラメータとヘッダー](#) このリクエストに対して。

リクエスト本文

なし

StorageGRID ドキュメント

"バケットの操作"

"バケットタグの削除"

URIクエリパラメータとリクエストヘッダー

StorageGRIDはすべてをサポート [共通パラメータとヘッダー](#) このリクエストに対して。

リクエスト本文

なし

StorageGRID ドキュメント

"バケットの操作"

"DeleteObject"

URIクエリパラメータとリクエストヘッダー

StorageGRIDはすべてをサポート [共通パラメータとヘッダー](#) このリクエストには、次の追加のリクエストヘッダーが含まれます。

- x-amz-bypass-governance-retention

リクエスト本文

なし

StorageGRIDドキュメント

"オブジェクトに対する操作"

"DeleteObjects"

URIクエリパラメータとリクエストヘッダー

StorageGRIDはすべてをサポート [共通パラメータとヘッダー](#) このリクエストには、次の追加のリクエストヘッダーが含まれます。

- x-amz-bypass-governance-retention

リクエスト本文

StorageGRID は、実装時に Amazon S3 REST API によって定義されたすべてのリクエスト ボディ パラメータをサポートします。

StorageGRIDドキュメント

"オブジェクトに対する操作"

"DeleteObjectTagging"

StorageGRIDはすべてをサポート [共通パラメータとヘッダー](#) このリクエストに対して。

リクエスト本文

なし

StorageGRIDドキュメント

"オブジェクトに対する操作"

"GetBucketAcl"

URIクエリパラメータとリクエストヘッダー

StorageGRIDはすべてをサポート [共通パラメータとヘッダー](#) このリクエストに対して。

リクエスト本文

なし

StorageGRIDドキュメント

"バケットの操作"

"GetBucketCors"

URIクエリパラメータとリクエストヘッダー

StorageGRIDはすべてをサポート [共通パラメータとヘッダー](#) このリクエストに対して。

リクエスト本文

なし

StorageGRIDドキュメント

"バケットの操作"

"バケット暗号化を取得"

URIクエリパラメータとリクエストヘッダー

StorageGRIDはすべてをサポート **共通パラメータとヘッダー**このリクエストに対して。

リクエスト本文

なし

StorageGRIDドキュメント

"バケットの操作"

"GetBucketLifecycleConfiguration"

URIクエリパラメータとリクエストヘッダー

StorageGRIDはすべてをサポート **共通パラメータとヘッダー**このリクエストに対して。

リクエスト本文

なし

StorageGRIDドキュメント

- "バケットの操作"
- "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リクエストヘッダー

StorageGRIDはすべてをサポート **共通パラメータとヘッダー**このリクエストに対して。

リクエスト本文

なし

StorageGRIDドキュメント

"バケットの操作"

"GetBucketNotificationConfiguration"

URIクエリパラメータとリクエストヘッダー

StorageGRIDはすべてをサポート **共通パラメータとヘッダー**このリクエストに対して。

リクエスト本文

なし

StorageGRIDドキュメント

"バケットの操作"

"GetBucketPolicy"

URIクエリパラメータとリクエストヘッダー

StorageGRIDはすべてをサポート [共通パラメータとヘッダー](#) このリクエストに対して。

リクエスト本文

なし

StorageGRIDドキュメント

["バケットの操作"](#)

"GetBucketReplication"

URIクエリパラメータとリクエストヘッダー

StorageGRIDはすべてをサポート [共通パラメータとヘッダー](#) このリクエストに対して。

リクエスト本文

なし

StorageGRIDドキュメント

["バケットの操作"](#)

"GetBucketTagging"

URIクエリパラメータとリクエストヘッダー

StorageGRIDはすべてをサポート [共通パラメータとヘッダー](#) このリクエストに対して。

リクエスト本文

なし

StorageGRIDドキュメント

["バケットの操作"](#)

"GetBucketVersioning"

URIクエリパラメータとリクエストヘッダー

StorageGRIDはすべてをサポート [共通パラメータとヘッダー](#) このリクエストに対して。

リクエスト本文

なし

StorageGRIDドキュメント

["バケットの操作"](#)

"GetObject"

URIクエリパラメータとリクエストヘッダー

StorageGRIDはすべてをサポート [共通パラメータとヘッダー](#) このリクエストには、次の追加の URI クエリ パラメータが含まれます。

- x-amz-checksum-mode
- partNumber
- response-cache-control
- response-content-disposition
- response-content-encoding
- response-content-language
- response-content-type
- response-expires

さらに次の追加のリクエスト ヘッダーがあります。

- 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

リクエスト本文

なし

StorageGRID ドキュメント

["GetObject"](#)

"GetObjectAcl"

URIクエリパラメータとリクエストヘッダー

StorageGRIDはすべてをサポート [共通パラメータとヘッダー](#)このリクエストに対して。

リクエスト本文

なし

StorageGRID ドキュメント

["オブジェクトに対する操作"](#)

"GetObjectLegalHold"

URIクエリパラメータとリクエストヘッダー

StorageGRIDはすべてをサポート [共通パラメータとヘッダー](#)このリクエストに対して。

リクエスト本文

なし

StorageGRID 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する"

"GetObjectLockConfiguration"

URIクエリパラメータとリクエストヘッダー

StorageGRIDはすべてをサポート [共通パラメータとヘッダー](#) このリクエストに対して。

リクエスト本文

なし

StorageGRID 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する"

"GetObjectRetention"

URIクエリパラメータとリクエストヘッダー

StorageGRIDはすべてをサポート [共通パラメータとヘッダー](#) このリクエストに対して。

リクエスト本文

なし

StorageGRID 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する"

"GetObjectTagging"

URIクエリパラメータとリクエストヘッダー

StorageGRIDはすべてをサポート [共通パラメータとヘッダー](#) このリクエストに対して。

リクエスト本文

なし

StorageGRID ドキュメント

"オブジェクトに対する操作"

"HeadBucket"

URIクエリパラメータとリクエストヘッダー

StorageGRIDはすべてをサポート [共通パラメータとヘッダー](#) このリクエストに対して。

リクエスト本文

なし

StorageGRID ドキュメント

"バケットの操作"

"HeadObject"

URIクエリパラメータとリクエストヘッダー

StorageGRIDはすべてをサポート [共通パラメータとヘッダー](#) このリクエストには、次の追加ヘッダーが含まれます。

- x-amz-checksum-mode
- 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

リクエスト本文

なし

StorageGRID ドキュメント

"HeadObject"

"ListBuckets"

URIクエリパラメータとリクエストヘッダー

StorageGRIDはすべてをサポート [共通パラメータとヘッダー](#) このリクエストに対して。

リクエスト本文

なし

StorageGRID ドキュメント

[サービス上の操作](#) > [ListBuckets](#)

"リストマルチパートアップロード"

URIクエリパラメータとリクエストヘッダー

StorageGRIDはすべてをサポート [共通パラメータとヘッダー](#) このリクエストには、次の追加パラメータが含まれます。

- encoding-type
- key-marker
- max-uploads
- prefix
- upload-id-marker

リクエスト本文

なし

StorageGRIDドキュメント

["リストマルチパートアップロード"](#)

"ListObjects"

URIクエリパラメータとリクエストヘッダー

StorageGRIDはすべてをサポート [共通パラメータとヘッダー](#) このリクエストには、次の追加パラメータが含まれます。

- delimiter
- encoding-type
- marker
- max-keys
- prefix

リクエスト本文

なし

StorageGRIDドキュメント

["バケットの操作"](#)

"リストオブジェクトV2"

URIクエリパラメータとリクエストヘッダー

StorageGRIDはすべてをサポート [共通パラメータとヘッダー](#) このリクエストには、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

リクエスト本文

なし

StorageGRIDドキュメント

["バケットの操作"](#)

"ListObjectVersions"

URIクエリパラメータとリクエストヘッダー

StorageGRIDはすべてをサポート [共通パラメータとヘッダー](#) このリクエストには、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

リクエスト本文

なし

StorageGRIDドキュメント

["バケットの操作"](#)

"ListParts"

URIクエリパラメータとリクエストヘッダー

StorageGRIDはすべてをサポート [共通パラメータとヘッダー](#) このリクエストには、次の追加パラメータが含まれます。

- max-parts
- part-number-marker
- uploadId

リクエスト本文

なし

StorageGRIDドキュメント

["リストマルチパートアップロード"](#)

"PutBucketCors"

URIクエリパラメータとリクエストヘッダー

StorageGRIDはすべてをサポート [共通パラメータとヘッダー](#) このリクエストに対して。

リクエスト本文

StorageGRID は、実装時に Amazon S3 REST API によって定義されたすべてのリクエスト ボディ パラメータをサポートします。

StorageGRIDドキュメント

["バケットの操作"](#)

"PutBucketEncryption"

URIクエリパラメータとリクエストヘッダー

StorageGRIDはすべてをサポート [共通パラメータとヘッダー](#) このリクエストに対して。

リクエストボディのXMLタグ

StorageGRID は、次のリクエスト ボディ XML タグをサポートしています。

- ApplyServerSideEncryptionByDefault
- Rule
- ServerSideEncryptionConfiguration
- SSEAlgorithm

StorageGRID ドキュメント

["バケットの操作"](#)

"PutBucketLifecycleConfiguration"

URIクエリパラメータとリクエストヘッダー

StorageGRIDはすべてをサポート [共通パラメータとヘッダー](#) このリクエストに対して。

リクエストボディのXMLタグ

StorageGRID は、次のリクエスト ボディ 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ドキュメント

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

"PutBucketNotificationConfiguration"

URIクエリパラメータとリクエストヘッダー

StorageGRIDはすべてをサポート [共通パラメータとヘッダー](#) このリクエストに対して。

リクエストボディのXMLタグ

StorageGRID は、次のリクエスト ボディ 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ドキュメント

["バケットの操作"](#)

"PutBucketPolicy"

URIクエリパラメータとリクエストヘッダー

StorageGRIDはすべてをサポート [共通パラメータとヘッダー](#) このリクエストに対して。

リクエスト本文

サポートされているJSON本体フィールドの詳細については、以下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する"](#)。

"PutBucketレプリケーション"

URIクエリパラメータとリクエストヘッダー

StorageGRIDはすべてをサポート [共通パラメータとヘッダー](#) このリクエストに対して。

リクエストボディのXMLタグ

- Bucket
- Destination
- Prefix
- ReplicationConfiguration
- Rule
- Status
- StorageClass

StorageGRID ドキュメント

"バケットの操作"

"PutBucketTagging"

URIクエリパラメータとリクエストヘッダー

StorageGRIDはすべてをサポート [共通パラメータとヘッダー](#) このリクエストに対して。

リクエスト本文

StorageGRID は、実装時に Amazon S3 REST API によって定義されたすべてのリクエスト ボディ パラメータをサポートします。

StorageGRID ドキュメント

"バケットの操作"

"PutBucketVersioning"

URIクエリパラメータとリクエストヘッダー

StorageGRIDはすべてをサポート [共通パラメータとヘッダー](#) このリクエストに対して。

リクエストボディパラメータ

StorageGRID は次のリクエスト本体パラメータをサポートしています。

- VersioningConfiguration
- Status

StorageGRID ドキュメント

"バケットの操作"

"PutObject"

URIクエリパラメータとリクエストヘッダー

StorageGRIDはすべてをサポート [共通パラメータとヘッダー](#) このリクエストには、次の追加ヘッダーが含まれます。

- Cache-Control
- Content-Disposition

- Content-Encoding
- Content-Language
- Expires
- x-amz-checksum-sha256
- 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>

リクエスト本文

- オブジェクトのバイナリデータ

StorageGRID ドキュメント

["PutObject"](#)

"PutObjectLegalHold"

URIクエリパラメータとリクエストヘッダー

StorageGRIDはすべてをサポート **共通パラメータとヘッダー**このリクエストに対して。

リクエスト本文

StorageGRID は、実装時に Amazon S3 REST API によって定義されたすべてのリクエスト ボディ パラメータをサポートします。

StorageGRID 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する"](#)

"PutObjectLockConfiguration"

URIクエリパラメータとリクエストヘッダー

StorageGRIDはすべてをサポート **共通パラメータとヘッダー**このリクエストに対して。

リクエスト本文

StorageGRID は、実装時に Amazon S3 REST API によって定義されたすべてのリクエスト ボディ パラメータをサポートします。

StorageGRID 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する"

"PutObjectRetention"

URIクエリパラメータとリクエストヘッダー

StorageGRIDはすべてをサポート [共通パラメータとヘッダー](#) このリクエストには次の追加ヘッダーが含まれません:

- `x-amz-bypass-governance-retention`

リクエスト本文

StorageGRID は、実装時に Amazon S3 REST API によって定義されたすべてのリクエスト ボディ パラメータをサポートします。

StorageGRID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する"

"PutObjectTagging"

URIクエリパラメータとリクエストヘッダー

StorageGRIDはすべてをサポート [共通パラメータとヘッダー](#) このリクエストに対して。

リクエスト本文

StorageGRID は、実装時に Amazon S3 REST API によって定義されたすべてのリクエスト ボディ パラメータをサポートします。

StorageGRIDドキュメント

"オブジェクトに対する操作"

"オブジェクトの復元"

URIクエリパラメータとリクエストヘッダー

StorageGRIDはすべてをサポート [共通パラメータとヘッダー](#) このリクエストに対して。

リクエスト本文

サポートされている本文フィールドの詳細については、"[オブジェクトの復元](#)"。

"オブジェクトコンテンツの選択"

URIクエリパラメータとリクエストヘッダー

StorageGRIDはすべてをサポート [共通パラメータとヘッダー](#) このリクエストに対して。

リクエスト本文

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](#)"
- "[オブジェクトコンテンツの選択](#)"

"UploadPart"

URIクエリパラメータとリクエストヘッダー

StorageGRIDはすべてをサポート [共通パラメータとヘッダー](#) このリクエストには、次の追加の URI クエリ パラメータが含まれます。

- partNumber
- uploadId

さらに次の追加のリクエスト ヘッダーがあります。

- x-amz-checksum-sha256
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5

リクエスト本文

- 部品のバイナリデータ

StorageGRID ドキュメント

"UploadPart"

"UploadPartCopy"

URIクエリパラメータとリクエストヘッダー

StorageGRIDはすべてをサポート [共通パラメータとヘッダー](#) このリクエストには、次の追加の URI クエリ パラメータが含まれます。

- partNumber
- uploadId

さらに次の追加のリクエスト ヘッダーがあります。

- 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-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

リクエスト本文

なし

StorageGRID ドキュメント

["UploadPartCopy"](#)

S3 REST API 構成のテスト

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できることを確認できます。

開始する前に

- AWS CLIをダウンロードしてインストールしました。 ["aws.amazon.com/cli"](https://aws.amazon.com/cli/)。
- オプションとして、["ロードバランサエンドポイントを作成した"](#)。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ます。見る["クライアント接続用のIPアドレスとポート"](#)。
- あなたが持っている["S3テナントアカウントを作成しました"](#)。
- テナントにサインインし、["アクセスキーを作成しました"](#)。

これらの手順の詳細については、["クライアント接続を構成する"](#)。

手順

1. 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 設定を構成します。
 - a. 設定モードに入ります: `aws configure`
 - b. 作成したアカウントのアクセス キー ID を入力します。
 - c. 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。
 - d. 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`。
 - e. 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。
2. バケットを作成

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 バランサー エンドポイントを構成していることを前提としています。

```
aws s3api --endpoint-url https://10.96.101.17:10443
--no-verify-ssl create-bucket --bucket testbucket
```

バケットが正常に作成されると、次の例に示すように、バケットの場所が返されます。

```
"Location": "/testbucket"
```

3. 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
```

オブジェクトが正常にアップロードされると、オブジェクトデータのハッシュである Etag が返されます。

4. バケットの内容を一覧表示して、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がS3 REST APIを実装する方法

競合するクライアント要求

2つのクライアントが同じキーに書き込むなど、競合するクライアント要求は、「最新のもの」を優先して解決されます。

「最新のもの優先」評価のタイミングは、S3クライアントが操作を開始した時点ではなく、StorageGRIDシステムが特定のリクエストを完了した時点に基づきます。

一貫性の値

一貫性は、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一貫性との間のバランスを提供します。アプリケーションの必要に応じて一貫性を変更できます。

デフォルトでは、StorageGRID は新しく作成されたオブジェクトの書き込み後の読み取り一貫性を保証します。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、および削除は、最終的に一貫性が保たれます。上書きが反映されるまでには通常数秒または数分かかりますが、最大 15 日かかる場合があります。

異なる一貫性でオブジェクト操作を実行する場合は、次の操作を実行できます。

- 一貫性を指定する各バケツ。
- 一貫性を指定する各API操作。
- 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一貫性を変更します。
 - グリッド マネージャーで、構成 > システム > ストレージ設定 > デフォルトの一貫性 に移動します。
 - 。



グリッド全体の一貫性の変更は、設定の変更後に作成されたバケツにのみ適用されません。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*`を検索してください)。

一貫性の値

一貫性は、StorageGRID がオブジェクトを追跡するため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、したがってクライアント要求に対するオブジェクトの可用性に影響します。

バケツまたは API 操作の一貫性を次のいずれかの値に設定できます。

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

「新規書き込み後の読み取り」と「利用可能」の一貫性を使用する

HEAD または GET 操作で「Read-after-new-write」一貫性を使用する場合、StorageGRID は次のように複数のステップで検索を実行します。

- まず、低い一貫性を使用してオブジェクトを検索します。
- その検索が失敗した場合、strong-global の動作と同等の一貫性に達するまで、次の一貫性値での検索を繰り返します。

HEAD または GET 操作で「新規書き込み後の読み取り」一貫性が使用され、オブジェクトが存在しない場合

は、オブジェクトの検索は常に strong-global の動作と同等の一貫性に到達します。この一貫性を保つには、各サイトでオブジェクト メタデータの複数のコピーが使用可能である必要があるため、同じサイトにある 2 つ以上のストレージ ノードが使用できない場合、多数の 500 内部サーバー エラーが発生する可能性があります。

Amazon S3 と同様の一貫性の保証が必要ない場合は、一貫性を「利用可能」に設定することで、HEAD および GET 操作でこれらのエラーを防ぐことができます。HEAD または GET 操作で「使用可能」な一貫性が使用される場合、StorageGRID は最終的な一貫性のみを提供します。一貫性が増すにつれて失敗した操作を再試行することはないため、オブジェクト メタデータの複数のコピーが利用可能である必要はありません。

API操作の一貫性を指定する

個々の API 操作の一貫性を設定するには、その操作に対して一貫性の値がサポートされている必要があります。リクエスト ヘッダーで一貫性を指定する必要があります。この例では、GetObject 操作の一貫性を「Strong-site」に設定します。

```
GET /bucket/object HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Consistency-Control: strong-site
```



PutObject 操作と GetObject 操作の両方に同じ一貫性を使用する必要があります。

バケットの一貫性を指定する

バケットの一貫性を設定するには、StorageGRIDを使用します。["PUT バケットの一貫性"](#)リクエスト。あるいは["バケットの一貫性を変更する"](#)テナントマネージャーより。

バケットの一貫性を設定するときは、次の点に注意してください。

- バケットの一貫性を設定すると、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 操作に使用される一貫性が決まります。バケット自体の操作には影響しません。
- 個々の API 操作の一貫性は、バケットの一貫性よりも優先されます。
- 一般に、バケットではデフォルトの一貫性である「新規書き込み後の読み取り」を使用する必要があります。リクエストが正しく機能しない場合は、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、各 API リクエストの一貫性を指定するようにクライアントを構成します。最後の手段としてのみ、バケット レベルで一貫性を設定します。

一貫性とILMルールがどのように相互作用してデータ保護に影響を与えるか

一貫性の選択と ILM ルールの両方が、オブジェクトの保護方法に影響します。これらの設定は相互作用する可能性があります。

たとえば、オブジェクトの保存時に使用される一貫性は、オブジェクト メタデータの初期配置に影響し、ILM ルールに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 はクライアントの要求を満たす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ため、一貫性と取り込み動作に一致する保護レベルを選択すると、初期データ保護が向上し、システム応答がより予測可能になります。

次の"**取り込みオプション**"ILM ルールに使用できるもの:

Dual commit

StorageGRID は直ちにオブジェクトの中間コピーを作成し、クライアントに成功を返します。 ILM ルールで指定されたコピーは、可能な場合に作成されます。

厳しい

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を作成する必要があります。

バランスの取れた

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を作成しようとします。これが不可能な場合は、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。 ILM ルールで指定されたコピーは、可能な場合に作成されます。

一貫性とILMルールがどのように相互作用するか

次の ILM ルールと次の一貫性を持つ 2 つのサイト グリッドがあるとします。

- **ILM** ルール: ローカル サイトとリモート サイトに 1 つずつ、合計 2 つのオブジェクト コピーを作成します。厳密な取り込み動作を使用します。
- 一貫性: 強力なグローバル (オブジェクト メタデータはすべてのサイトに直ちに配布されます)。

クライアントがオブジェクトをグリッドに保存すると、StorageGRID は両方のオブジェクトのコピーを作成し、両方のサイトにメタデータを配布してから、クライアントに成功を返します。

オブジェクトは、取り込み成功メッセージの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でも、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 サイトに残ります。オブジェクトは完全に取得可能です。

代わりに同じ ILM ルールと強力なサイト一貫性を使用した場合、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後、オブジェクト メタデータがそこに配布される前に、クライアントは成功メッセージを受信する可能性があります。この場合、オブジェクト メタデータの保護レベルは、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 サイトが失われた場合、オブジェクト メタデータは失われます。オブジェクトを取得できません。

一貫性と ILM ルール間の相互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るのを防ぎ、オブジェクトの以前のバージョンを取得して復元できるようになります。

StorageGRIDシステムは、ほとんどの機能をサポートするバージョン管理を実装していますが、いくつかの制限があります。StorageGRID は、各オブジェクトの最大 10,000 バージョンをサポートします。

オブジェクトのバージョン管理は、StorageGRID情報ライフサイクル管理 (ILM) または S3 バケット ライフサイクル構成と組み合わせることができます。各バケットに対してバージョン管理を明示的に有効にする必要

があります。バケットのバージョン管理が有効になっている場合、バケットに追加された各オブジェクトには、StorageGRIDシステムによって生成されるバージョン ID が割り当てられます。

MFA (多要素認証) を使用した削除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 スキャン プロセスは、すべてのオブジェクトを継続的にスキャンし、現在の ILM ポリシーに対して再評価します。ILM ポリシーに加えた変更は、以前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、以前に取り込まれたバージョンも含まれます。ILM スキャンは、以前に取り込まれたオブジェクトに新しい ILM 変更を適用します。

バージョン管理が有効なバケット内のS3オブジェクトの場合、バージョン管理のサポートにより、「非現在時刻」を参照時刻として使用するILMルールを作成できます（「このルールを古いオブジェクトバージョンにのみ適用しますか？」という質問に対して*はい*を選択します）。「[ILMルールの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、以前のバージョンは非最新になります。「非現在の時間」フィルターを使用すると、オブジェクトの以前のバージョン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操作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非現在の時間は、マルチパートアップロードが完了したときではなく、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ときに反映されます。場合によっては、元のバージョンの非現在の時刻が現在のバージョンの時刻よりも数時間または数日前になることがあります。

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する

StorageGRIDシステムでグローバル S3 オブジェクト ロック設定が有効になっている場合は、S3 オブジェクト ロックが有効になっているバケットを作成できます。各バケットのデフォルトの保持期間、または各オブジェクト バージョンの保持期間設定を指定できます。

バケットの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 S3 オブジェクト ロック設定が有効になっている場合は、各バケットを作成するときにオプションで S3 オブジェクト ロックを有効にできます。

S3 オブジェクト ロックは、バケットを作成するときのみ有効にできる永続的な設定です。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。

バケットに対して 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。

- テナント マネージャーを使用してバケットを作成します。見る["S3バケットを作成する"](#)。
- CreateBucketリクエストを使用してバケットを作成します。`x-amz-bucket-object-lock-enabled` リクエスト ヘッダー。見る["バケットの操作"](#)。

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。これ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。見る["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

バケットに対して S3 オブジェクトロックが有効になっている場合は、オプションでバケットのデフォルトの保存を有効にし、デフォルトの保存モードとデフォルトの保存期間を指定できます。

デフォルトの保持モード

- コンプライアンスモードの場合:
 - オブジェクトは、保持期限に達するまで削除できません。
 - オブジェクトの保持期限を増やすことはできますが、減らすことはできません。
 - オブジェクトの保持期限は、その日付に達するまで削除できません。
- ガバナンスモードの場合:
 - ユーザーは `s3:BypassGovernanceRetention` 許可は `x-amz-bypass-governance-retention: true` 保持設定をバイパスするためのリクエスト ヘッダー。
 - これらのユーザーは、オブジェクト バージョンを、その保持期限に達する前に削除できます。
 - これらのユーザーは、オブジェクトの保持期限を増減または削除できます。

デフォルト保持期間

各バケットには、年または日数で指定されたデフォルトの保持期間を設定できます。

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。

- テナント マネージャーからバケット設定を管理します。見る["S3バケットを作成する"](#)そして["S3 オブジェクトロックのデフォルト保持を更新"](#)。
- バケットに対して PutObjectLockConfiguration リクエストを発行し、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します。

PutObjectLockConfiguration

PutObjectLockConfiguration リクエストを使用すると、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および変更できます。以前に構成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、次の場合、デフォルトの保持モードが適用されます。`x-amz-object-lock-mode` そして `x-amz-object-lock-retain-until-date` 指定されていません。デフォルトの保存期間は、次の場合に保存期限日を計算するために使用されます。`x-amz-object-lock-retain-until-date` 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 バージョンの保持期間は同じままとなり、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。

あなたは `s3:PutBucketObjectLockConfiguration` この操作を完了するには、権限を持っているか、アカウントの root である必要があります。

その `Content-MD5` PUT リクエストではリクエスト ヘッダーを指定する必要があります。

リクエスト例

この例では、バケットの 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 COMPLIANCE に、デフォルトの保持期間を 6 年に設定します。

```
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決定する方法

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

- テナント マネージャーでバケットを表示します。見る ["S3バケットを表示"](#)。
- `GetObjectLockConfiguration` 要求を発行します。

GetObjectLockConfiguration

`GetObjectLockConfiguration` リクエストを使用すると、バケットに対して S3 オブジェクト ロックが有効になっているかどうかを確認し、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、次の場合、デフォルトの保持モードが適用され

ます。`x-amz-object-lock-mode`指定されていません。デフォルトの保存期間は、次の場合に保存期限日を計算するために使用されます。`x-amz-object-lock-retain-until-date`指定されていません。

あなたは`s3:GetBucketObjectLockConfiguration`この操作を完了するには、権限を持っているか、アカウントのrootである必要があります。

リクエスト例

```
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:
iVmcB7OXXJRkRH1FiVq1151/T24gRfpwpuZrEG11Bb9ImOMAAe98oxSpXlknabA0LTvBYJpSIX
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になっているバケットには、S3 オブジェクトロックの保持設定があるオブジェクトとないオブジェクトの組み合わせを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 を使用して指定されます。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。

各オブジェクトに対して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:** オブジェクト バージョンをStorageGRIDで保持する必要がある期間を指定する日付。
 - COMPLIANCE モードでは、保持期限が将来の日付である場合、オブジェクトを取得することはできませんが、変更または削除することはできません。保持期限を増やすことはできますが、この日付を減らしたり削除したりすることはできません。
 - GOVERNANCE 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、保持期限を延長、短縮、または削除することもできます。
- 法的保留: オブジェクト バージョンに法的保留を適用すると、そのオブジェクトは直ちにロックされます。たとえば、調査や法的紛争に関連するオブジェクトに対して法的保留を設定する必要がある場合があります。法的保留には有効期限はありませんが、明示的に削除されるまで有効のままになります。

オブジェクトの法的保留設定は、保持モードおよび保持期限とは無関係です。オブジェクト バージョンが法的保留中の場合、そのバージョンを削除することは誰にもできません。

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設定を指定するには、**"PutObject"**、**"CopyObject"**、または**"CreateMultipartUpload"**リクエスト。

以下を使用できます。

- ``x-amz-object-lock-mode`` COMPLIANCE または GOVERNANCE (大文字と小文字が区別されます) のいずれかになります。



指定する場合 `x-amz-object-lock-mode`、また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`
 - 保持期限の値は、次の形式でなければなりません。2020-08-10T21:46:00Z。小数秒は許可されませんが、保持されるのは小数点第3位のみです (ミリ秒の精度)。その他の ISO 8601 形式は許可されません。
 - 保持期限は将来の日付にする必要があります。
- `x-amz-object-lock-legal-hold`

法的保留がオンの場合 (大文字と小文字が区別されます)、オブジェクトは法的保留の対象となります。法的保留がオフの場合、法的保留は設定されません。その他の値を指定すると、400 Bad Request (InvalidArgument) エラーが発生します。

これらのリクエスト ヘッダーのいずれかを使用する場合は、次の制限に注意してください。

- その `Content-MD5`` リクエストヘッダーは必須です ``x-amz-object-lock-*`` リクエスト ヘッダーは `PutObject` リクエストに存在します。 ``Content-MD5 CopyObject` または `CreateMultipartUpload` には必要ありません。
- バケットにS3オブジェクトロックが有効になっていない場合、``x-amz-object-lock-*`` リクエスト ヘッダーが存在する場合、400 Bad Request (InvalidRequest) エラーが返されます。

- PutObjectリクエストは、`x-amz-storage-class: REDUCED_REDUNDANCY` AWS の動作と一致させるためです。ただし、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が取り込まれると、StorageGRID は常にデュアルコミット取り込みを実行します。
- 後続のGETまたはHeadObjectバージョンのレスポンスにはヘッダーが含まれます `x-amz-object-lock-mode`、`x-amz-object-lock-retain-until-date`、そして `'x-amz-object-lock-legal-hold'` 設定されていて、リクエスト送信者が正しい `'s3:Get'` 権限。

使用することができます `'s3:object-lock-remaining-retention-days'` オブジェクトの許容される最小および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 バージョンの法的保留または保持設定を更新する必要がある場合は、次のオブジェクトサブリソース操作を実行できます。

- PutObjectLegalHold

新しい法的保留値がONの場合、オブジェクトは法的保留下に置かれます。法的保留値がOFFの場合、法的保留は解除されます。

- PutObjectRetention

- モード値は、COMPLIANCE または GOVERNANCE (大文字と小文字が区別されます) になります。
- 保持期限の値は、次の形式でなければなりません。2020-08-10T21:46:00Z。小数秒は許可されませんが、保持されるのは小数点第3位のみです (ミリ秒の精度)。その他の ISO 8601 形式は許可されません。
- オブジェクト バージョンに既存の保持期限がある場合は、それを増やすことしかできません。新しい値は将来のものである必要があります。

ガバナンスモードの使い方

ユーザーは `'s3:BypassGovernanceRetention'` 権限により、GOVERNANCE 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がバイパスされる可能性があります。DELETEまたはPutObjectRetention操作には、`'x-amz-bypass-governance-retention:true'` リクエスト ヘッダー。これらのユーザー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 または DeleteObjects 操作を実行します。

法的保留中のオブジェクトは削除できません。法的保留は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 GOVERNANCE から COMPLIANCE に変更する PutObjectRetention 操作を実行します。

モードを COMPLIANCE から GOVERNANCE に変更することは許可されません。

- オブジェクト バージョンの保持期間を増加、減少、または削除するには、PutObjectRetention 操作を実行します。

関連情報

- ["S3 オブジェクトロックでオブジェクトを管理する"](#)

- ["S3 オブジェクトロックを使用してオブジェクトを保持する"](#)
- ["Amazon Simple Storage Service ユーザーガイド: オブジェクトのロック"](#)

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システムからいつ削除されるかを制御することができます。

このセクションの簡単な例は、S3 ライフサイクル設定によって、特定の S3 バケットから特定のオブジェクトがいつ削除される (期限切れになる) かを制御する方法を示しています。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、以下を参照してください。"[Amazon Simple Storage Service ユーザーガイド: オブジェクトのライフサイクル管理](#)"。StorageGRID は有効期限アクションのみをサポートし、遷移アクションはサポートしていないことに注意してください。

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。各ルールでは、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 (特定の日付または一定の日数後) を指定します。

StorageGRID は、ライフサイクル構成で最大 1,000 個のライフサイクル ルールをサポートします。各ルールには次の XML 要素を含めることができます。

- 有効期限: 指定した日付に達したとき、またはオブジェクトが取り込まれた時点から指定した日数に達したときに、オブジェクトを削除します。
- NoncurrentVersionExpiration: オブジェクトが非最新になった時点から指定された日数が経過すると、オブジェクトを削除します。
- フィルター (プレフィックス、タグ)
- ステータス
- ID

各オブジェクトは、S3 バケットの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 バケットのライフサイクルが設定されている場合、ライフサイクルの有効期限アクションは、バケットのライフサイクル フィルターに一致するオブジェクトの ILM ポリシーをオーバーライドします。バケットのライフサイクル フィルターに一致しないオブジェクトは、ILM ポリシーの保持設定を使用します。オブジェクトがバケットのライフサイクル フィルタに一致し、有効期限アクション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 バージョンは永久に保持されるものとみなされます。見る"[S3 バケット ライフサイクルと ILM ポリシーの優先順位の例](#)"。

その結果、ILM ルールの配置指示がオブジェクトに適用されているにもかかわらず、オブジェクトがグリッドから削除される可能性があります。または、オブジェクトに対する ILM 配置指示が失効した後も、オブジェクトがグリッド上に保持されることがあります。詳細については、"[ILM がオブジェクトのライフサイクル全体にわたってどのように機能するか](#)"。



バケットのライフサイクル設定は、S3 オブジェクト ロックが有効になっているバケットで使用できますが、従来の準拠バケットではバケットのライフサイクル設定はサポートされていません。

StorageGRID は、ライフサイクル構成を管理するために次のバケット操作の使用をサポートしています。

- DeleteBucketLifecycle
- GetBucketLifecycleConfiguration
- PutBucketLifecycleConfiguration

ライフサイクル構成を作成する

ライフサイクル構成を作成する最初の手順として、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は接頭辞に一致するオブジェクトにのみ適用される `category1`/そして、`key2` の値 `tag2`。その `Expiration` パラメーターは、フィルターに一致するオブジェクトが 2020 年 8 月 22 日の深夜に期限切れになることを指定します。
2. ルール2は接頭辞に一致するオブジェクトにのみ適用される `category2`。その `Expiration` パラメーターは、フィルタに一致するオブジェクトが取り込まれてから 100 日後に期限切れになることを指定します。



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ます。現在の日付が取り込み日に日数を加えた日付を超えている場合、ライフサイクル設定が適用されると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は接頭辞に一致するオブジェクトにのみ適用される `category3`。その `Expiration` パラメーターは、一致するオブジェクトの非現在のバージョンが非現在のバージョンになってから 50 日後に期限切れになることを指定します。

```

{
  "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する

ライフサイクル設定ファイルを作成したら、PutBucketLifecycleConfiguration リクエストを発行してそれをバケットに適用します。

このリクエストは、サンプルファイルのライフサイクル設定を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
```

ライフサイクル構成がバケットに正常に適用されたことを検証するには、GetBucketLifecycleConfiguration リクエストを発行します。例えば：

```
aws s3api --endpoint-url <StorageGRID endpoint> get-bucket-lifecycle-configuration
--bucket testbucket
```

成功した応答には、適用したライフサイクル構成が一覧表示されます。

バケットのライフサイクルの有効期限がオブジェクトに適用されていることを検証する

PutObject、HeadObject、または GetObject リクエストを発行するときに、ライフサイクル構成の有効期限ルールが特定のオブジェクトに適用されるかどうかを判断できます。ルールが適用される場合、応答には `Expiration` オブジェクトの有効期限と、どの有効期限ルールに一致したかを示すパラメーター。



バケットのライフサイクルはILMよりも優先されるため、`expiry-date`表示されるのは、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、["物体の保持がどのように決定されるか"](#)。

例えば、このPutObjectリクエストは2020年6月22日に発行され、オブジェクトを `testbucket` バケツ。

```
aws s3api --endpoint-url <StorageGRID endpoint> put-object
--bucket testbucket --key obj2test2 --body bktjson.json
```

成功応答は、オブジェクトが 100 日後 (2020 年 10 月 1 日) に期限切れになり、ライフサイクル構成のルール 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、この HeadObject リクエストは、testbucket バケット内の同じオブジェクトのメタデータを取得するために使用されました。

```
aws s3api --endpoint-url <StorageGRID endpoint> head-object
--bucket testbucket --key obj2test2
```

成功応答にはオブジェクトのメタデータが含まれており、オブジェクトが 100 日後に期限切れになることと、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": {}
}
```



バージョン対応バケットの場合、`x-amz-expiration` 応答ヘッダーはオブジェクトの現在のバージョンにのみ適用されます。

S3 REST API 実装に関する推奨事項

StorageGRIDで使用するために S3 REST API を実装する場合は、次の推奨事項に従う必要があります。

存在しないオブジェクトへのHEADの推奨事項

アプリケーションが、実際には存在しないと思われるパスにオブジェクトが存在するかどうかを定期的に確認する場合は、「使用可能」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 を実行する前に場所を HEAD する場合は、「Available」一貫性を使用する必要があります。

そうでない場合、HEAD 操作でオブジェクトが見つからないと、同じサイトにある 2 つ以上のストレージ ノードが使用できないか、リモート サイトにアクセスできないときに、多数の 500 内部サーバー エラーが発生する可能性があります。

各バケットの「利用可能」一貫性を設定するには、**"PUT バケットの一貫性"** リクエストごとに一貫性を指定したり、個々の API 操作のリクエスト ヘッダーで一貫性を指定したりすることもできます。

オブジェクトキーに関する推奨事項

バケットが最初に作成された時期に基づいて、オブジェクト キー名に関する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 文字としてランダムな値を使用しないでください。これは、キープレフィックスに関する以前の AWS 推奨事項とは対照的です。代わりに、ランダムではない、ユニークではない接頭辞を使用してください。 image。
- キープレフィックスにランダムで一意的文字を使用するという以前の AWS 推奨事項に従う場合は、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
```

この形式の代わりに:

```
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 プラクティスを満たすためにオブジェクト 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。



例外は、短時間ですべてのオブジェクトを継続的に削除する S3 ワークロードです。このユースケースでのパフォーマンスへの影響を最小限に抑えるには、数千個のオブジェクトごとにキー名の先頭部分を日付などに変更します。たとえば、S3 クライアントが通常 1 秒あたり 2,000 個のオブジェクトを書き込み、ILM またはバケット ライフサイクル ポリシーによって 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/yyyyymmddhhmmss-random_UUID.jpg
```

「レンジリード」の推奨事項

もし"保存された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、S3 クライアントアプリケーションは、返されるバイトの範囲を指定する GetObject 操作の実行を避ける必要があります。これらの「範囲読み取り」操作は、StorageGRID が要求されたバイトにアクセスするためにオブジェクトを効果的に解凍する必要があるため、非効率的です。非常に大きなオブジェクトから小さな範囲のバイトを要求する GetObject 操作は特に非効率的です。たとえば、50 GB の圧縮されたオブジェクトから 10 MB の範囲を読み取るのは非効率的です。

範囲が圧縮されたオブジェクトから読み取られる場合、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 アプリケーションで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ます。

Amazon S3 REST APIのサポート

S3 REST API実装の詳細

StorageGRIDシステムは、ほとんどの操作をサポートする Simple Storage Service API (API バージョン 2006-03-01) を実装していますが、いくつかの制限があります。S3 REST API クライアント アプリケーションを統合する場合は、実装の詳細を理解する必要があります。

StorageGRIDシステムは、仮想ホスト スタイルのリクエストとパス スタイルのリクエストの両方をサポート

します。

日付処理

S3 REST API のStorageGRID実装では、有効な HTTP 日付形式のみがサポートされます。

StorageGRIDシステムは、日付値を受け入れるヘッダーに対して有効な HTTP 日付形式のみをサポートします。日付の時間部分は、グリニッジ標準時 (GMT) 形式、またはタイムゾーン オフセットなしの世界協定時刻 (UTC) 形式で指定できます (+0000 を指定する必要があります)。含めると `x-amz-date` リクエストのヘッダーに Date を指定すると、Date リクエスト ヘッダーに指定された値が上書きされます。AWS署名バージョン4を使用する場合、`x-amz-date`日付ヘッダーはサポートされていないため、署名されたリクエストには日付ヘッダーが存在する必要があります。

一般的なリクエストヘッダー

StorageGRIDシステムは、以下で定義された共通リクエストヘッダーをサポートしています。"[Amazon Simple Storage Service API リファレンス: 共通リクエストヘッダー](#)"ただし、1つの例外があります。

リクエストヘッダー	導入
承認	AWS 署名バージョン 2 の完全サポート AWS 署名バージョン 4 のサポート (ただし、次の例外があります)。 <ul style="list-style-type: none">実際のペイロードチェックサム値を <code>x-amz-content-sha256</code>、値は検証なしで受け入れられ、値が <code>UNSIGNED-PAYLOAD</code> ヘッダーに提供されていました。あなたが <code>x-amz-content-sha256</code> ヘッダー値の意味 <code>aws-chunked</code> ストリーミング (たとえば、<code>STREAMING-AWS4-HMAC-SHA256-PAYLOAD</code>) の場合、チャンク署名はチャンク データに対して検証されません。
x-amz-セキュリティトークン	実装されていません。返品 <code>XNotImplemented</code> 。

一般的なレスポンスヘッダー

StorageGRIDシステムは、1つの例外を除き、「Simple Storage Service API リファレンス」で定義されているすべての共通応答ヘッダーをサポートします。

レスポンスヘッダー	導入
x-amz-id-2	未使用

リクエストを認証する

StorageGRIDシステムは、S3 API を使用したオブジェクトへの認証アクセスと匿名アクセスの両方をサポートします。

S3 API は、S3 API リクエストの認証に署名バージョン 2 と署名バージョン 4 をサポートしています。

認証されたリクエストは、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システムは、HTTPとHTTPSの2つの認証方法をサポートしています。`Authorization`ヘッダーとクエリパラメータを使用します。

HTTP認証ヘッダーを使用する

HTTP `Authorization`ヘッダーは、バケット ポリシーで許可されている匿名リクエストを除くすべての S3 API 操作で使用されます。その `Authorization`ヘッダーには、リクエストを認証するために必要な署名情報がすべて含まれています。

クエリパラメータを使用する

クエリ パラメータを使用して、URL に認証情報を追加できます。これは URL の事前署名と呼ばれ、特定の リソースへの一時的なアクセスを許可するために使用できます。署名済み URL を持つユーザーは、リソースにアクセスするために秘密アクセス キーを知る必要がないため、リソースへのサードパーティの制限付きアクセスを提供できます。

サービス上の操作

StorageGRIDシステムは、サービス上で次の操作をサポートします。

処理	導入
ListBuckets (以前の名称は GET サービス)	すべての Amazon S3 REST API 動作が実装されています。予告なく変更されることがあります。
ストレージ使用量の取得	StorageGRID"ストレージ使用量の取得"リクエストにより、アカウントで使用されているストレージの合計量と、アカウントに関連付けられている各バケットのストレージ量がわかります。これは、/ の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操作です。(?x-ntap-sg-usage) 追加した。
OPTIONS /	クライアントアプリケーションは、OPTIONS / S3 認証資格情報を提供せずに、ストレージ ノードの S3 ポートに要求を送信し、ストレージ ノードが使用可能かどうかを判断します。このリクエストは監視に使用したり、外部ロードバランサーがストレージノードがダウンしたかどうかを識別できるようにするために使用できます。

バケットの操作

StorageGRIDシステムは、S3 テナント アカウントごとに最大 5,000 個のバケットをサポートします。

各グリッドには最大 100,000 個のバケットを含めることができます。

5,000 個のバケットをサポートするには、グリッド内の各ストレージ ノードに少なくとも 64 GB の RAM が必要です。

バケット名の制限は AWS US 標準リージョンの制限に従いますが、S3 仮想ホスト形式のリクエストをサポートするには、DNS 命名規則にさらに制限する必要があります。

詳細については、以下を参照してください。

- ["Amazon Simple Storage Service ユーザーガイド: バケットのクォータ、制限、制約事項"](#)
- ["S3エンドポイントのドメイン名を設定する"](#)

ListObjects (GET Bucket) および ListObjectVersions (GET Bucket object versions) オペレーションはStorageGRIDをサポートします"[一貫性値](#)"。

個々のバケットに対して最終アクセス時刻の更新が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。見る"[GET バケットの最終アクセス時刻](#)"。

次の表は、StorageGRID がS3 REST API バケット操作を実装する方法を示しています。これらの操作を実行するには、アカウントに必要なアクセス資格情報を提供する必要があります。

処理	導入
CreateBucket	<p>新しいバケットを作成します。バケットを作成すると、バケットの所有者になります。</p> <ul style="list-style-type: none"> • バケット名は次の規則に従う必要があります。 <ul style="list-style-type: none"> ◦ 各StorageGRIDシステム全体で一意である必要があります (テナント アカウント内で一意だけでなく)。 ◦ DNS に準拠している必要があります。 ◦ 3 文字以上 63 文字以下でなければなりません。 ◦ 隣接するラベルをピリオドで区切った、1つ以上のラベルの連続にすることができます。各ラベルは小文字または数字で始まり、終わる必要があります。小文字、数字、ハイフンのみを使用できます。 ◦ テキスト形式の IP アドレスのように見えてはいけません。 ◦ 仮想ホスト形式のリクエストでは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、サーバーのワイルドカード証明書の検証で問題が発生します。 • デフォルトでは、バケットは `us-east-1` 地域;ただし、`LocationConstraint` 別のリージョンを指定するには、リクエスト本文にリクエスト要素を追加します。使用する際は `LocationConstraint` 要素を使用する場合は、グリッド マネージャーまたはグリッド管理 API を使用して定義されたリージョンの正確な名前を指定する必要があります。使用すべき地域名がわからない場合は、システム管理者に問い合わせてください。 <p>注意: CreateBucket リクエストで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"> • 以下のものを含めることができます `x-amz-bucket-object-lock-enabled` S3 オブジェクト ロックが有効になっているバケットを作成するためのリクエストヘッダー。見る"S3 REST API を使用して S3 オブジェクトロックを設定する"。 <p>バケットを作成するときに、S3 オブジェクトロックを有効にする必要があります。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。これはバケットを作成すると自動的に有効になります。</p>
DeleteBucket	バケットを削除します。
バケットCorsの削除	バケットの CORS 構成を削除します。
バケット暗号化の削除	バケットからデフォルトの暗号化を削除します。既存の暗号化されたオブジェクトは暗号化されたままですが、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。

処理	導入
DeleteBucketLifecycle	バケットからライフサイクル構成を削除します。見る" S3ライフサイクル設定を作成する "。
DeleteBucketPolicy	バケットに添付されたポリシーを削除します。
バケットレプリケーションの削除	バケットに添付されたレプリケーション設定を削除します。
バケットタグの削除	<p>使用するのは `tagging` バケットからすべてのタグを削除するサブリソース。</p> <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は、`NTAP-SG-ILM-BUCKET-TAG` 値が割り当てられたバケット タグ。DeleteBucketTagging リクエストを発行しないでください。`NTAP-SG-ILM-BUCKET-TAG` バケットタグ。代わりに、PutBucketTagging リクエストを発行し、`NTAP-SG-ILM-BUCKET-TAG` タグとそれに割り当てられた値を入力すると、バケットから他のすべてのタグが削除されます。変更したり削除したりしないでください `NTAP-SG-ILM-BUCKET-TAG` バケットタグ。</p>
GetBucketAcl	肯定応答とバケット所有者の ID、DisplayName、および権限を返し、所有者がバケットへのフルアクセス権を持っていることを示します。
GetBucketCors	返します `cors` バケットの構成。
バケット暗号化を取得	バケットのデフォルトの暗号化設定を返します。
GetBucketLifecycleConfiguration (以前はGET Bucket ライフサイクルと呼ばれていました)	バケットのライフサイクル構成を返します。見る" S3ライフサイクル設定を作成する "。
GetBucketLocation	設定された領域を返します。LocationConstraint CreateBucket リクエスト内の要素。バケットのリージョンが us-east-1、その領域に対して空の文字列が返されます。
GetBucketNotificationConfiguration (以前の名称は GET Bucket 通知)	バケットに添付された通知設定を返します。
GetBucketPolicy	バケットに添付されたポリシーを返します。
GetBucketReplication	バケットに添付されたレプリケーション設定を返します。

処理	導入
GetBucketTagging	<p>使用するのは `tagging` バケットのすべてのタグを返すサブリソース。</p> <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は、`NTAP-SG-ILM-BUCKET-TAG`値が割り当てられたバケット タグ。このタグを変更したり削除したりしないでください。</p>
GetBucketVersioning	<p>この実装では、`versioning`バケットのバージョン管理状態を返すサブリソース。</p> <ul style="list-style-type: none"> • <i>blank</i>: バージョン管理が有効になったことがありません (バケットは「バージョン管理なし」です) • 有効: バージョン管理が有効です • 一時停止: バージョン管理は以前は有効でしたが、一時停止されています
GetObjectLockConfiguration	<p>設定されている場合は、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返します。</p> <p>見る"S3 REST API を使用して S3 オブジェクトロックを設定する"。</p>
HeadBucket	<p>バケットが存在するかどうか、またそれにアクセスする権限があるかどうかを判断します。</p> <p>この操作は次を返します:</p> <ul style="list-style-type: none"> • <code>x-ntap-sg-bucket-id</code>: UUID 形式のバケットの UUID。 • <code>x-ntap-sg-trace-id</code>: 関連付けられたリクエストの一意のトレース ID。
ListObjects と ListObjectsV2 (以前の名称は 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 個) を返します。オブジェクトのストレージクラスは、オブジェクトが `REDUCED_REDUNDANCY` ストレージクラスオプション:</p> <ul style="list-style-type: none"> • `STANDARD` これは、オブジェクトがストレージ ノードで構成されるストレージ プールに保存されていることを示します。 • `GLACIER` これは、オブジェクトが Cloud Storage Pool によって指定された外部バケットに移動されたことを示します。 <p>バケットに同じプレフィックスを持つ削除されたキーが多数含まれている場合、レスポンスには `CommonPrefixes` キーが含まれないもの。</p>
ListObjectVersions (以前の名称は GET Bucket Object バージョン)	<p>バケットへのREADアクセスで、この操作を `versions` サブリソースは、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を一覧表示します。</p>

処理	導入
PutBucketCors	<p>バケットがクロスオリジン リクエストを処理できるように、バケットの CORS 構成を設定します。クロスオリジン リソース共有 (CORS) は、あるドメイン内のクライアント Web アプリケーションが別のドメイン内のリソースにアクセスできるようにするセキュリティ メカニズムです。たとえば、S3バケットの名前が images`グラフィックを保存します。 CORS設定を設定することで `images`バケット内の画像をウェブサイトに表示できるようにすることができます `http://www.example.com。</p>
PutBucketEncryption	<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を有効にすると、バケットに追加された新しいオブジェクトはすべて暗号化されます。StorageGRIDは、StorageGRID管理キーを使用したサーバー側の暗号化をサポートしています。サーバー側暗号化設定ルールを指定するときは、SSEAlgorithm`パラメータに `AES256、そして、`KMSMasterKeyID`パラメータ。</p> <p>オブジェクトのアップロードリクエストで既に暗号化が指定されている場合 (つまり、リクエストに `x-amz-server-side-encryption-*`リクエスト ヘッダー)。</p>
PutBucketLifecycleConfiguration (以前はPUT Bucketライフサイクルと呼ばれていました)	<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を置き換えます。StorageGRID は、ライフサイクル構成で最大 1,000 個のライフサイクル ルールをサポートします。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"> • 有効期限 (日数、日付、ExpiredObjectDeleteMarker) • NoncurrentVersionExpiration (NewerNoncurrentVersions、NoncurrentDays) • フィルター (プレフィックス、タグ) • ステータス • ID <p>StorageGRID は次のアクションをサポートしていません。</p> <ul style="list-style-type: none"> • AbortIncompleteMultipartUpload • 移行 <p>見る"S3ライフサイクル設定を作成する"。バケットライフサイクルの有効期限アクションがILM配置指示とどのように相互作用するかを理解するには、以下を参照してください。"ILMがオブジェクトのライフサイクル全体にわたってどのように機能するか"。</p> <p>注意: バケットのライフサイクル設定は、S3 オブジェクト ロックが有効になっているバケットで使用できますが、従来の準拠バケットではバケットのライフサイクル設定はサポートされていません。</p>

処理	導入
PutBucketNotificationConfiguration (以前の名称はPUT Bucket 通知)	<p>リクエスト本文に含まれる通知構成 XML を使用して、バケットの通知を構成します。次の実装の詳細に注意する必要があります。</p> <ul style="list-style-type: none"> StorageGRID は、送信先として Amazon Simple Notification Service (Amazon SNS) または Kafka トピックをサポートしています。 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。 通知の宛先は、 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、テナント マネージャーまたはテナント管理 API を使用して作成できます。 <p>通知構成を成功させるには、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 `コードとともにエラーが返されます `InvalidArgument。</p> <ul style="list-style-type: none"> 次のイベント タイプに対しては通知を構成できません。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"> s3:ReducedRedundancyLostObject s3:ObjectRestore:Completed StorageGRIDから送信されるイベント通知では、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を使用することを除いて、標準の JSON 形式が使用されます。 <ul style="list-style-type: none"> イベントソース sgws:s3 awsリージョン 含まれません x-amz-id-2 含まれません アーーン urn:sgws:s3:::bucket_name
PutBucketPolicy	バケットに添付されたポリシーを設定します。見る "バケットとグループのアクセスポリシーを使用する" 。

処理	導入
PutBucketレプリケーション	<p>構成"StorageGRID CloudMirror レプリケーション"リクエスト本文で提供されるレプリケーション構成 XML を使用してバケットに対して行います。CloudMirrorレプリケーションの場合、次の実装の詳細に注意する必要があります。</p> <ul style="list-style-type: none"> StorageGRID はレプリケーション構成の V1 のみをサポートします。これは、StorageGRIDが `Filter` ルールの要素であり、オブジェクトバージョンの削除については V1 規則に従います。詳細については、"Amazon Simple Storage Service ユーザーガイド: レプリケーション設定"。 バケットのレプリケーションは、バージョン管理された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ます。 レプリケーション構成 XML の各ルールで異なる宛先バケットを指定できます。ソース バケットは複数の宛先バケットに複製できます。 宛先バケットは、テナント マネージャまたはテナント管理 API で指定されているStorageGRIDエンドポイントの URN として指定する必要があります。見る"CloudMirrorレプリケーションを構成する"。 <p>レプリケーション構成を成功させるには、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、リクエストは失敗し、400 Bad Request エラーメッセージは次のようになります。`Unable to save the replication policy. The specified endpoint URN does not exist: URN.`</p> <ul style="list-style-type: none"> 指定する必要はありません `Role` 構成 XML 内。この値はStorageGRIDでは使用されず、送信されても無視されます。 設定XMLからストレージクラスを省略した場合、StorageGRIDは `STANDARD` デフォルトのストレージ クラス。 ソースバケットからオブジェクトを削除するか、ソースバケット自体を削除した場合、リージョン間のレプリケーションの動作は次のようになります。 <ul style="list-style-type: none"> オブジェクトまたはバケットが複製される前に削除した場合、オブジェクト/バケットは複製されず、通知も行われません。 オブジェクトまたはバケットをレプリケートした後に削除する場合、StorageGRID はクロスリージョンレプリケーションの V1 の標準の Amazon S3 削除動作に従います。

処理	導入
PutBucketTagging	<p>使用するのは `tagging` バケットのタグのセットを追加または更新するためのサブリソース。バケット タグを追加するときは、次の制限に注意してください。</p> <ul style="list-style-type: none"> 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。 バケッ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 キーの長さは最大 128 文字の Unicode 文字です。 タグ値の長さは最大 256 文字の Unicode 文字です。 キーと値は大文字と小文字が区別されます。 <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は、`NTAP-SG-ILM-BUCKET-TAG`値が割り当てられたバケット タグ。必ず `NTAP-SG-ILM-BUCKET-TAG`バケット タグは、すべての PutBucketTagging リクエストで割り当てられた値に含まれます。このタグを変更したり削除したりしないでください。</p> <p>注意: この操作により、バケットにすでに存在するタグが上書きされます。セットから既存のタグが省略されている場合、それらのタグはバケットから削除されます。</p>
PutBucketVersioning	<p>使用するのは `versioning` 既存のバケットのバージョン管理状態を設定するためのサブリソース。バージョン管理の状態は、次のいずれかの値で設定できます。</p> <ul style="list-style-type: none"> 有効: バケット内のオブジェクトのバージョン管理を有効にします。バケットに追加されたすべてのオブジェクトには、一意のバージョン ID が付与されます。 停止: バケット内のオブジェクトのバージョン管理を無効にします。バケットに追加されたすべてのオブジェクトにはバージョンIDが付与されず null。
PutObjectLockConfiguration	<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が変更された場合、既存のオブジェクト バージョンの保持期限は同じままになり、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>見る"S3 REST API を使用して S3 オブジェクトロックを設定する"詳細情報については。</p>

オブジェクトに対する操作

オブジェクトに対する操作

このセクションでは、StorageGRIDシステムがオブジェクトに対して S3 REST API 操作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操作には次の条件が適用されます。

- StorageGRID"**一貫性値**"次の例外を除き、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。
 - GetObjectAcl
 - OPTIONS /
 - PutObjectLegalHold
 - PutObjectRetention
 - オブジェクトコンテンツの選択
- 2つのクライアントが同じキーに書き込むなど、競合するクライアント要求は、「最新のものを優先」して解決されます。「最新のものを優先」評価のタイミングは、S3クライアントが操作を開始した時点ではなく、StorageGRIDシステムが特定のリクエストを完了した時点に基づきます。
- StorageGRIDバケット内のすべてのオブジェクトは、匿名ユーザーまたは別のアカウントによって作成されたオブジェクトを含め、バケット所有者によって所有されます。
- Swift を介してStorageGRIDシステムに取り込まれたデータ オブジェクトには、S3 を介してアクセスできません。

次の表は、StorageGRID がS3 REST API オブジェクト操作を実装する方法を示しています。

処理	導入
DeleteObject	<p>多要素認証 (MFA) とレスポンスヘッダー `x-amz-mfa` サポートされていません。</p> <p>DeleteObject 要求を処理する場合、StorageGRID は保存されているすべての場所からオブジェクトのすべてのコピーを直ちに削除しようとします。成功した場合、StorageGRID はすぐ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 (たとえば、場所が一時的に利用できないなど)、StorageGRID はコピーを削除キューに入れてから、クライアントに成功を通知します。</p> <p>バージョン管理</p> <p>特定のバージョンを削除するには、リクエスト者はバケットの所有者であり、`versionId` 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。もし `versionId` 削除マーカーに対応するレスポンスヘッダー `x-amz-delete-marker` に設定されて返されます `true`。</p> <ul style="list-style-type: none"> オブジェクトが削除された場合、`versionId` バージョン管理が有効になっているバケットのサブリソースを削除すると、削除マーカーが生成されます。その `versionId` 削除マーカーは、`x-amz-version-id` レスポンスヘッダー、および `x-amz-delete-marker` レスポンスヘッダーは次のように設定されて返されます `true`。 オブジェクトが削除された場合、`versionId` バージョン管理が一時停止されているバケットのサブリソースを削除すると、既存の「null」バージョンまたは「null」削除マーカーが永久に削除され、新しい「null」削除マーカーが生成されます。その `x-amz-delete-marker` レスポンスヘッダーは次のように設定されて返されます `true`。 <p>注意: 場合によっては、オブジェクトに対して複数の削除マーカーが存在することがあります。</p> <p>見る"S3 REST API を使用して S3 オブジェクトロックを設定する" GOVERNANCE モードでオブジェクト バージョンを削除する方法を学習します。</p>
DeleteObjects (以前の名称は DELETE Multiple Objects)	<p>多要素認証 (MFA) とレスポンスヘッダー `x-amz-mfa` サポートされていません。</p> <p>同じリクエスト メッセージで複数のオブジェクトを削除できます。</p> <p>見る"S3 REST API を使用して S3 オブジェクトロックを設定する" GOVERNANCE モードでオブジェクト バージョンを削除する方法を学習します。</p>

処理	導入
DeleteObjectTagging	<p>使用するのは `tagging` オブジェクトからすべてのタグを削除するサブリソース。</p> <p>バージョン管理</p> <p>もし `versionId` クエリ パラメータがリクエストに指定されていない場合、この操作では、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である場合、「MethodNotAllowed」ステータスが返されます。 `x-amz-delete-marker` レスポンスヘッダーを `true`。</p>
GetObject	"GetObject"
GetObjectAcl	アカウントに必要なアクセス資格情報が提供されている場合、操作は肯定応答と、オブジェクト所有者の ID、表示名、および権限を返し、所有者がオブジェクトへのフルアクセス権を持っていることを示します。
GetObjectLegalHold	"S3 REST API を使用して S3 オブジェクトロックを設定する"
GetObjectRetention	"S3 REST API を使用して S3 オブジェクトロックを設定する"
GetObjectTagging	<p>使用するのは `tagging` オブジェクトのすべてのタグを返すサブリソース。</p> <p>バージョン管理</p> <p>もし `versionId` クエリ パラメータがリクエストに指定されていない場合、この操作で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である場合、「MethodNotAllowed」ステータスが返されます。 `x-amz-delete-marker` レスポンスヘッダーを `true`。</p>
HeadObject	"HeadObject"
オブジェクトの復元	"オブジェクトの復元"
PutObject	"PutObject"
CopyObject (以前の名前は PUT Object - Copy)	"CopyObject"
PutObjectLegalHold	"S3 REST API を使用して S3 オブジェクトロックを設定する"
PutObjectRetention	"S3 REST API を使用して S3 オブジェクトロックを設定する"

処理	導入
PutObjectTagging	<p>使用するのには `tagging` 既存のオブジェクトにタグのセットを追加するためのサブリソース。</p> <p>オブジェクトタグの制限</p> <p>新しいオブジェクトをアップロードするときにタグを追加したり、既存のオブジェクトにタグを追加したりできます。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。タグキーの長さは最大 128 文字の Unicode 文字、タグ値の長さは最大 256 文字の Unicode 文字です。キーと値は大文字と小文字が区別されます。</p> <p>タグの更新と取り込み動作</p> <p>PutObjectTagging を使用してオブジェクトのタグを更新すると、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 ルールで指定された取り込み動作のオプションが使用されないことを意味します。更新によってトリガーされるオブジェクト配置の変更は、通常のバックグラウンド ILM プロセスによって ILM が再評価されるときに行われます。</p> <p>つまり、ILM ルールが取り込み動作に厳密オプションを使用する場合、必要なオブジェクトを配置できない場合 (たとえば、新しく必要な場所が利用できないなど)、アクションは実行されません。更新されたオブジェクトは、必要な配置が可能になるまで現在の配置を保持します。</p> <p>紛争の解決</p> <p>2 つのクライアントが同じキーに書き込むなど、競合するクライアント要求は、「最新のものを優先」して解決されます。「最新のものの優先」評価のタイミングは、S3 クライアントが操作を開始した時点ではなく、StorageGRIDシステムが特定のリクエストを完了した時点に基づきます。</p> <p>バージョン管理</p> <p>もし `versionId` クエリ パラメータがリクエストに指定されていない場合、この操作では、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が追加されます。オブジェクトの現在のバージョンが削除マーカーである場合、「MethodNotAllowed」ステータスが返されます。`x-amz-delete-marker` レスポンスヘッダーを `true`。</p>
オブジェクトコンテンツの選択	"オブジェクトコンテンツの選択"

S3 Selectを使用する

StorageGRIDは、以下のAmazon S3 Select句、データ型、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ません。

構文については、"[オブジェクトコンテンツの選択](#)"。S3 Selectの詳細については、"[S3 Select の AWS ドキュメント](#)"。

S3 Select が有効になっているテナント アカウントのみが SelectObjectContent クエリを発行できます。参照"[S3 Select の使用に関する考慮事項と要件](#)"。

条項

- SELECTリスト
- FROM句
- WHERE句
- LIMIT句

データ型

- ブール
- integer
- string
- float
- 小数、数値
- タイムスタンプ

有人対応

論理演算子

- および
- ない
- または

比較演算子

- <
- >
- <=
- >=
- =
- =
- <>
- !=
- 間

- で

パターンマッチング演算子

- のように
- _
- %

ユニタリ演算子

- NULLです
- NULLではない

数学演算子

- +
- -
- *
- /
- %

StorageGRID はAmazon S3 Select 演算子の優先順位に従います。

集計関数

- 平均()
- カウント (*)
- 最大()
- 最小値()
- 和 ()

条件関数

- 場合
- 合体
- NULLIF

変換関数

- CAST (サポートされているデータ型の場合)

日付関数

- 日付_追加
- 日付差

- EXTRACT
- TO_STRING
- TO_タイムスタンプ
- UTCNOW

文字列関数

- CHAR_LENGTH、CHARACTER_LENGTH
- より低い
- 部分文字列
- トリム
- アッパー

サーバー側の暗号化を使用する

サーバー側の暗号化により、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ときにデータを暗号化し、オブジェクトにアクセスするときにデータを復号化します。

サーバー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、相互に排他的な 2 つのオプションのいずれかを選択できます。

- **SSE (StorageGRID管理キーによるサーバー側暗号化)**: オブジェクトを保存するための S3 リクエストを発行すると、StorageGRID は一意のキーを使用してオブジェクトを暗号化します。オブジェクトを取得するために S3 リクエストを発行すると、StorageGRID は保存されたキーを使用してオブジェクトを復号化します。
- **SSE-C (顧客提供のキーを使用したサーバー側暗号化)**: オブジェクトを保存するための S3 リクエストを発行するときに、独自の暗号化キーを提供します。オブジェクトを取得するときは、リクエストの一部として同じ暗号化キーを提供します。2 つの暗号化キーが一致する場合、オブジェクトは復号化され、オブジェクト データが返されます。

StorageGRID はすべてのオブジェクトの暗号化および復号化操作を管理しますが、提供する暗号化キーはユーザーが管理する必要があります。



提供された暗号化キーは保存されません。暗号化キーを紛失すると、対応するオブジェクトも失われます。



オブジェクトが SSE または SSE-C で暗号化されている場合、バケット レベルまたはグリッド レベルの暗号化設定はすべて無視されます。

SSE を使用

StorageGRIDによって管理される一意のキーを使用してオブジェクトを暗号化するには、次のリクエスト ヘッダーを使用します。

`x-amz-server-side-encryption`

SSE 要求ヘッダーは、次のオブジェクト操作でサポートされます。

- "PutObject"
- "CopyObject"
- "CreateMultipartUpload"

SSE-Cを使用する

管理する一意のキーを使用してオブジェクトを暗号化するには、次の 3 つのリクエスト ヘッダーを使用します。

リクエストヘッダー	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 AES256。
x-amz-server-side-encryption-customer-key	オブジェクトの暗号化または復号化に使用する暗号化キーを指定します。キーの値は 256 ビット、base64 でエンコードされている必要があります。
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く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 ビットである必要があります。

SSE-C 要求ヘッダーは、次のオブジェクト操作でサポートされます。

- "GetObject"
- "HeadObject"
- "PutObject"
- "CopyObject"
- "CreateMultipartUpload"
- "UploadPart"
- "UploadPartCopy"

顧客提供キーによるサーバー側暗号化 (SSE-C) の使用に関する考慮事項

SSE-C を使用する前に、次の点に注意してください。

- https を使用する必要があります。



StorageGRIDは、SSE-Cを使用する場合、HTTP経由のすべてのリクエストを拒否します。セキュリティ上の考慮事項として、HTTP経由で誤って送信したキーは侵害され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マッピングを管理する必要があります。StorageGRID は暗号化キーを保存しません。各オブジェクトに提供した暗号化キーを追跡するのはユーザーの責任です。
- バケットでバージョン管理が有効になっている場合は、各オブジェクトバージョンに独自の暗号化キーが必要です。各オブジェクトバージョンに使用される暗号化キーを追跡するのはユーザーの責任です。
- 暗号化キーはクライアント側で管理するため、キーのローテーションなどの追加の安全対策もクライアント側で管理する必要があります。



提供された暗号化キーは保存されません。暗号化キーを紛失すると、対応するオブジェクトも失われます。

- 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、SSE-C オブジェクトを取り込むことはできません。取り込み操作は失敗します。

関連情報

["Amazon S3 ユーザーガイド: 顧客提供キーによるサーバー側暗号化 \(SSE-C\) の使用"](#)

CopyObject

S3 CopyObject リクエストを使用して、S3 にすでに保存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 に続いて PutObject を実行するのと同じです。

紛争を解決する

2 つのクライアントが同じキーに書き込むなど、競合するクライアント要求は、「最新のを優先」して解決されます。「最新のもの優先」評価のタイミングは、S3 クライアントが操作を開始した時点ではなく、StorageGRID システムが特定のリクエストを完了した時点に基づきます。

オブジェクトのサイズ

1 回の PutObject 操作の最大推奨 サイズは 5 GiB (5,368,709,120 バイト) です。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"](#)その代わり。

1 回の PutObject 操作でサポートされる最大サイズは 5 TiB (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、5 GiB を超えるオブジェクトをアップロードしようとする、S3 PUT オブジェクトのサイズが大きすぎるという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 の将来のリリースでは 5 GiB 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。

ユーザーメタデータの UTF-8 文字

リクエストに、キー名またはユーザー定義メタデータの値に (エスケープされていない) UTF-8 値が含まれている場合、StorageGRID の動作は未定義になります。

StorageGRID は、ユーザー定義メタデータのキー名または値に含まれるエスケープされた UTF-8 文字を解析または解釈しません。エスケープされた UTF-8 文字は ASCII 文字として扱われます。

- ユーザー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場合、リクエストは成功しません。
- StorageGRIDは `x-amz-missing-meta` キー名または値の解釈された値に印刷できない文字が含まれている場合は、ヘッダーにエラーが発生します。

サポートされているリクエストヘッダー

次のリクエスト 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-、その後にユーザー定義のメタデータを含む名前と値のペアが続く
- x-amz-metadata-directive: デフォルト値は `COPY` これにより、オブジェクトと関連メタデータをコピーできるようになります。

指定できます `REPLACE` オブジェクトをコピーするときに既存のメタデータを上書きするか、オブジェクトのメタデータを更新します。

- x-amz-storage-class
- x-amz-tagging-directive: デフォルト値は `COPY` これにより、オブジェクトとすべてのタグをコピーできるようになります。

指定できます `REPLACE` オブジェクトをコピーするときに既存のタグを上書きしたり、タグを更新したりします。

- S3 オブジェクトロックリクエストヘッダー:

- x-amz-object-lock-mode
- x-amz-object-lock-retain-until-date
- x-amz-object-lock-legal-hold

これらのヘッダーなしでリクエストが行われた場合、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 モードと保持期限が計算されます。見る"[S3 REST API を使用して S3 オブジェクトロックを設定する](#)"。

- SSE リクエスト 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

見る[サーバー側暗号化のリクエストヘッダー]

サポートされていないリクエストヘッダー

次のリクエスト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-checksum-algorithm

オブジェクトをコピーするときに、ソースオブジェクトにチェックサムがある場合、StorageGRIDはそのチェックサム値を新しいオブジェクトにコピーしません。この動作は、使用しようとしたかどうかに関係なく適用されます。`x-amz-checksum-algorithm`オブジェクト要求内。

- x-amz-website-redirect-location

ストレージクラスのオプション

その`x-amz-storage-class`リクエストヘッダーがサポートされており、一致するILMルールがデュアルコミットまたはバランスコミットを使用している場合にStorageGRIDが作成す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ルールがデュアルコミットオプションを使用する場合、またはバランスオプションが中間コピーの作成にフォールバックする場合に、デュアルコミットインジェスト操作を指定します。

- REDUCED_REDUNDANCY

ILMルールがデュアルコミットオプションを使用する場合、またはバランスオプションが中間コピーの作成にフォールバックする場合に、単一コミットの取り込み操作を指定します。



S3オブジェクトロックが有効になっているバケットにオブジェクトを取り込む場合、`REDUCED_REDUNDANCY`オプションは無視されます。レガシーコンプライアンスバケットにオブジェクトを取り込む場合、`REDUCED_REDUNDANCY`オプションはエラーを返します。StorageGRIDは、コンプライアンス要件が満たされていることを確認するために、常にデュアルコミット取り込みを実行します。

CopyObject で x-amz-copy-source を使用する

ソースバケットとキーが `x-amz-copy-source` ヘッダー、値、およびキーが宛先バケットとキーと異なる場合、ソース オブジェクト データのコピーが宛先に書き込まれます。

送信元と送信先が一致し、`x-amz-metadata-directive` ヘッダーは次のように指定されます `REPLACE` オブジェクトのメタデータは、リクエストで提供されたメタデータ値で更新されます。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その場で暗号化したり、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。あなたが `x-amz-server-side-encryption` ヘッダーまたは `x-amz-server-side-encryption-customer-algorithm` ヘッダー、StorageGRID はリクエストを拒否し、`XNotImplemented`。
- 一致する ILM ルールで指定された取り込み動作のオプションは使用されません。更新によってトリガーされるオブジェクト配置の変更は、通常のバックグラウンド ILM プロセスによって ILM が再評価される時に行われます。

つまり、ILM ルールが取り込み動作に厳密オプションを使用する場合、必要なオブジェクトを配置できない場合 (たとえば、新しく必要な場所が利用できないなど)、アクションは実行されません。更新されたオブジェクトは、必要な配置が可能になるまで現在の配置を保持します。

サーバー側暗号化のリクエストヘッダー

もしあなたが"[サーバー側の暗号化を使用する](#)"指定するリクエストヘッダーは、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予定があるかどうかによって異なります。

- ソース オブジェクトが顧客提供のキー (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、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`: 特定 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。
- 提供および管理する一意のキーを使用してターゲット 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`: 特定 AES256。
 - `x-amz-server-side-encryption-customer-key`: 対象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。



提供された暗号化キーは保存されません。暗号化キーを紛失すると、対応するオブジェクトも失われます。顧客提供のキーを使用してオブジェクトデータを保護する前に、以下の考慮事項を確認してください。"[サーバー側暗号化を使用する](#)"。

- StorageGRID (SSE) によって管理される一意のキーを使用してターゲット オブジェクト (コピー) を暗号化する場合は、CopyObject 要求に次のヘッダーを含めます。

◦ `x-amz-server-side-encryption`



その `server-side-encryption` オブジェクトの値を更新できません。代わりに、新しいコピーを作成してください。`server-side-encryption` 値を使用する `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されている場合は、`x-amz-copy-source` オブジェクトの最新バージョンをコピーするためのヘッダー。オブジェクトの特定のバージョンをコピーするには、`versionId` サブリソース。宛先バケットがバージョン管理されている場合、生成されたバージョンは `x-amz-version-id` レスポンス ヘッダー。ターゲットバケットのバージョン管理が停止されている場合は、`x-amz-version-id` 「null」 値を返します。

GetObject

S3 GetObject リクエストを使用して、S3 バケットからオブジェクトを取得できます。

GetObjectとマルチパートオブジェクト

使用することができます `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取得するためのリクエスト パラメータ。その `x-amz-mp-parts-count` レスポンス要素は、オブジェクトに含まれるパーツの数を示します。

設定できます `partNumber` セグメント化/マルチパートオブジェクトと非セグメント化/非マルチパートオブジェクトの両方で1になりますが、`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 オブジェクトに対してのみ返されます。

ユーザーメタデータの UTF-8 文字

StorageGRID は、ユーザー定義のメタデータ内のエスケープされた UTF-8 文字を解析または解釈しません。ユーザー定義のメタデータにエスケープされた UTF-8 文字を含むオブジェクトに対する GET リクエストは、`x-amz-missing-meta` キー名または値に印刷できない文字が含まれている場合は、ヘッダーを作成します。

サポートされているリクエストヘッダー

次のリクエスト ヘッダーがサポートされています。

- `x-amz-checksum-mode` : 特定 ENABLED

その `Range` ヘッダーはサポートされていません `x-amz-checksum-mode` GetObject 用。含める場合 `Range` リクエストに `x-amz-checksum-mode` 有効にすると、StorageGRID は応答でチェックサム値を返しません。

サポートされていないリクエストヘッダー

次のリクエストヘッダーはサポートされていないため、XNotImplemented :

- `x-amz-website-redirect-location`

バージョン管理

もし `versionId` サブリソースが指定されていない場合、この操作で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である場合、「見つかりません」ステータスが返されます。`x-amz-delete-marker`レスポンスヘッダーを`true`。

顧客提供の暗号化キーを使用したサーバー側暗号化のリクエスト ヘッダー (SSE-C)

オブジェクトが指定した一意のキーで暗号化されている場合は、3つのヘッダーすべてを使用します。

- `x-amz-server-side-encryption-customer-algorithm`: 特定 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。



提供された暗号化キーは保存されません。暗号化キーを紛失すると、対応するオブジェクトも失われます。顧客提供のキーを使用してオブジェクトデータを保護する前に、以下の考慮事項を確認してください。["サーバー側の暗号化を使用する"](#)。

Cloud Storage Pool オブジェクトに対する `GetObject` の動作

オブジェクトが["クラウド ストレージ プール"](#) `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。見る["HeadObject"](#) 詳細についてはこちらをご覧ください。



オブジェクトがクラウド ストレージ プールに格納され、そのオブジェクトの1つ以上のコピーがグリッド上にも存在する場合、`GetObject` リクエストは、クラウド ストレージ プールからデータを取得する前に、グリッドからデータを取得しようとします。

オブジェクトの状態	<code>GetObject</code> の動作
StorageGRIDに取り込まれたが ILM によってまだ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 プールに保存されているか消去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取得されます。
Cloud Storage Pool 内のオブジェクトですが、まだ取得不可の状態に移行していません	200 OK オブジェクトのコピーが取得されます。
オブジェクトは取得不可能な状態に移行しました	403 Forbidden、InvalidObjectState 使用 "オブジェクトの復元" オブジェクトを取得可能な状態に復元するよう要求します。
回復不可能な状態から復元中のオブジェクト	403 Forbidden、InvalidObjectState <code>RestoreObject</code> 要求が完了するまで待ちます。

オブジェクトの状態	GetObjectの動作
オブジェクトがクラウド ストレージ プールに完全に復元されました	200 OK オブジェクトのコピーが取得されます。

クラウド ストレージ プール内のマルチパー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、または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して、オブジェクトが Cloud Storage Pool で使用可能かどうかを判断します。場合によっては、GetObjectリクエストが誤って返されることがあります。`200 OK`オブジェクトの一部がすでに回復不可能な状態に移行している場合、またはオブジェクトの一部がまだ復元されていない場合。

このような場合:

- GetObject 要求はデータを返す可能性があります、転送の途中で停止することがあります。
- 後続のGetObjectリクエストは、403 Forbidden。

GetObjectとクロスグリッドレプリケーション

使用している場合"[グリッドフェデレーション](#)"そして"[クロスグリッドレプリケーション](#)"バケットに対して有効になっている場合、S3 クライアントは GetObject リクエスト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 `x-ntap-sg-cgr-replication-status` レスポンス ヘッダーは次のいずれかの値を持ちます。

Grid	レプリケーションステータス
ソース	<ul style="list-style-type: none"> • 完了: レプリケーションは成功しました。 • 保留中: オブジェクトはまだ複製されていません。 • 失敗: レプリケーションは永続的な障害により失敗しました。ユーザーはエラーを解決する必要があります。
デスティネーション	REPLICA: オブジェクトはソース グリッドから複製されました。



StorageGRIDはサポートしていません `x-amz-replication-status` ヘッダー。

HeadObject

S3 HeadObject リクエストを使用すると、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取得できます。オブジェクトが Cloud Storage プールに保存されている場合は、HeadObject を使用してオブジェクトの遷移状態を判別できます。

HeadObjectとマルチパートオブジェクト

使用することができます `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取得するためのリクエスト パラメータ。その `x-amz-mp-parts-count` レスポンス要素は、オブジ

エクトに含まれるパーツの数を示します。

設定できます `partNumber` セグメント化/マルチパートオブジェクトと非セグメント化/非マルチパートオブジェクトの両方で1になりますが、`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 オブジェクトに対してのみ返されます。

ユーザーメタデータの UTF-8 文字

StorageGRID は、ユーザー定義のメタデータ内のエスケープされた UTF-8 文字を解析または解釈しません。ユーザー定義のメタデータにエスケープされた UTF-8 文字を含むオブジェクトに対する HEAD リクエストは、`x-amz-missing-meta` キー名または値に印刷できない文字が含まれている場合は、ヘッダーを作成します。

サポートされているリクエストヘッダー

次のリクエスト ヘッダーがサポートされています。

- `x-amz-checksum-mode`

その `partNumber` パラメータと `Range` ヘッダーはサポートされていません `x-amz-checksum-mode` HeadObject 用。リクエストにそれらを含めると `x-amz-checksum-mode` 有効にすると、StorageGRID は応答でチェックサム値を返しません。

サポートされていないリクエストヘッダー

次のリクエストヘッダーはサポートされていないため、XNotImplemented:

- `x-amz-website-redirect-location`

バージョン管理

もし `versionId` サブリソースが指定されていない場合、この操作で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である場合、「見つかりません」ステータスが返されます。`x-amz-delete-marker` レスポンスヘッダーを `true`。

顧客提供の暗号化キーを使用したサーバー側暗号化のリクエスト ヘッダー (SSE-C)

オブジェクトが指定した一意のキーで暗号化されている場合は、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`: 特定 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。



提供された暗号化キーは保存されません。暗号化キーを紛失すると、対応するオブジェクトも失われます。顧客提供のキーを使用してオブジェクトデータを保護する前に、以下の考慮事項を確認してください。"[サーバー側の暗号化を使用する](#)"。

Cloud Storage Pool オブジェクトの HeadObject 応答

オブジェクトが"クラウド ストレージ プール"、次の応答ヘッダーが返されます。

- x-amz-storage-class: GLACIER
- x-amz-restore

レスポンス ヘッダーには、オブジェクトが Cloud Storage プールに移動され、オプションで取得不可能な状態に移行され、復元される際のオブジェクトの状態に関する情報が提供されます。

オブジェクトの状態	HeadObjectへの応答
StorageGRIDに取り込まれたが ILM によってまだ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 プールに保存されているか消去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。)
Cloud Storage Pool 内のオブジェクトですが、まだ取得不可の状態に移行していません	200 OK x-amz-storage-class: GLACIER x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT" オブジェクトが取得不可能な状態に移行するまで、`expiry-date` 遠い将来のある時点に設定されています。移行の正確な時間はStorageGRIDシステムによって制御されません。
オブジェクトは取得不可能な状態に移行しましたが、少なくとも1つのコピーがグリッド上に存在します	200 OK x-amz-storage-class: GLACIER x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT" の価値 `expiry-date` 遠い将来のある時点に設定されています。 注意: グリッド上のコピーが利用できない場合 (たとえば、ストレージノードがダウンしている場合)、" オブジェクトの復元 "オブジェクトを正常に取得するには、クラウド ストレージ プールからコピーを復元するようにリクエストする必要があります。
オブジェクトは取得不可能な状態に移行し、グリッド上にコピーが存在しません	200 OK x-amz-storage-class: GLACIER

オブジェクトの状態	HeadObjectへの応答
回復不可能な状態から復元中のオブジェクト	<pre>200 OK x-amz-storage-class: GLACIER x-amz-restore: ongoing-request="true"</pre>
オブジェクトがクラウド ストレージ プールに完全に復元されました	<pre>200 OK x-amz-storage-class: GLACIER x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2018 00:00:00 GMT" その `expiry-date`クラウド ストレージ プール内のオブジェクトが取得不可能な状態に戻されるタイミングを示します。</pre>

クラウド ストレージ プール内のマルチパー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、または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して、オブジェクトが Cloud Storage Pool で使用可能かどうかを判断します。場合によっては、HeadObjectリクエストが誤って返されることがあります。`x-amz-restore: ongoing-request="false"`オブジェクトの一部がすでに回復不可能な状態に移行している場合、またはオブジェクトの一部がまだ復元されていない場合。

HeadObjectとクロスグリッドレプリケーション

使用している場合"**グリッドフェデレーション**"そして"**クロスグリッドレプリケーション**"バケットに対して有効になっている場合、S3 クライアントは HeadObject リクエスト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 `x-ntap-sg-cgr-replication-status`レスポンス ヘッダーは次のいずれかの値を持ちます。

Grid	レプリケーションステータス
ソース	<ul style="list-style-type: none"> 完了: レプリケーションは成功しました。 保留中: オブジェクトはまだ複製されていません。 失敗: レプリケーションは永続的な障害により失敗しました。ユーザーはエラーを解決する必要があります。
デスティネーション	REPLICA: オブジェクトはソース グリッドから複製されました。



StorageGRIDはサポートしていません `x-amz-replication-status`ヘッダ。

PutObject

S3 PutObject リクエストを使用して、バケットにオブジェクトを追加できます。

紛争を解決する

2つのクライアントが同じキーに書き込むなど、競合するクライアント要求は、「最新のを優先」して解決されます。「最新のを優先」評価のタイミングは、S3クライアントが操作を開始した時点ではなく、StorageGRIDシステムが特定のリクエストを完了した時点に基づきます。

オブジェクトのサイズ

1回のPutObject操作の最大推奨サイズは5 GiB (5,368,709,120 バイト) です。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」その代わり。

1回のPutObject操作でサポートされる最大サイズは5 TiB (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、5 GiB を超えるオブジェクトをアップロードしようとする、S3 PUT オブジェクトのサイズが大きすぎるという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の将来のリリースでは5 GiB 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。

ユーザーメタデータのサイズ

Amazon S3 では、各 PUT リクエスト ヘッダー内のユーザー定義メタデータのサイズが2 KB に制限されています。StorageGRID はユーザーメタデータを24 KiB に制限します。ユーザー定義メタデータのサイズは、各キーと値のUTF-8 エンコードのバイト数の合計によって測定されます。

ユーザーメタデータの UTF-8 文字

リクエストに、キー名またはユーザー定義メタデータの値に (エスケープされていない) UTF-8 値が含まれている場合、StorageGRID の動作は未定義になります。

StorageGRID は、ユーザー定義メタデータのキー名または値に含まれるエスケープされた UTF-8 文字を解析または解釈しません。エスケープされた UTF-8 文字は ASCII 文字として扱われます。

- ユーザー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場合、PutObject、CopyObject、GetObject、および HeadObject 要求は成功します。
- StorageGRIDは `x-amz-missing-meta` キー名または値の解釈された値に印刷できない文字が含まれている場合は、ヘッダーにエラーが発生します。

オブジェクトタグの制限

新しいオブジェクトをアップロードするときにタグを追加したり、既存のオブジェクトにタグを追加したりできます。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。タグキーの長さは最大128文字のUnicode文字、タグ値の長さは最大256文字のUnicode文字です。キーと値は大文字と小文字が区別されず。

オブジェクトの所有権

StorageGRIDでは、所有者以外のアカウントまたは匿名ユーザーによって作成されたオブジェクトも含め、すべての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ます。

サポートされているリクエストヘッダー

次のリクエストヘッダーがサポートされています。

- Cache-Control
- Content-Disposition
- Content-Encoding

指定する場合 `aws-chunked` のために Content-Encoding StorageGRID は次の項目を検証しません。

- StorageGRIDは、`chunk-signature` チャンクデータに対して。
- StorageGRIDは、指定された値を検証しません。`x-amz-decoded-content-length` オブジェクトに対して。

- Content-Language
- Content-Length
- Content-MD5
- Content-Type
- Expires
- Transfer-Encoding

チャンク転送エンコーディングは、以下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-checksum-sha256
- x-amz-meta-、その後ユーザー定義のメタデータを含む名前と値のペアが続きます。

ユーザー定義のメタデータの名前と値のペアを指定する場合は、次の一般的な形式を使用します。

```
x-amz-meta-name: value
```

ILMルールの参照時間として*ユーザー定義作成時間*オプションを使用する場合は、`creation-time` オブジェクトが作成された日時を記録するメタデータの名前として。例えば：

```
x-amz-meta-creation-time: 1443399726
```

の価値 `creation-time` 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、参照時間の ユーザー定義の作成時間 と、バランスまたは厳密な取り込みオプションの両方を使用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せん。

- `x-amz-tagging`
- S3 オブジェクトロックリクエストヘッダー
 - `x-amz-object-lock-mode`
 - `x-amz-object-lock-retain-until-date`
 - `x-amz-object-lock-legal-hold`

これらのヘッダーなしでリクエストが行われた場合、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モードと保持期限が計算されます。見る["S3 REST API を使用して S3 オブジェクトロックを設定する"](#)。

- SSE リクエストヘッダー:
 - `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`

見る[\[サーバー側暗号化のリクエストヘッダー\]](#)

サポートされていないリクエストヘッダー

次のリクエストヘッダーはサポートされていません。

- `x-amz-acl`
- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`
- `x-amz-website-redirect-location`

その `x-amz-website-redirect-location``ヘッダーリターン ``XNotImplemented`。

ストレージクラスのオプション

その ``x-amz-storage-class``リクエストヘッダーがサポートされています。提出された値は ``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ますが、オブジェクトの永続コピーがStorageGRIDシステムにいくつ保存されるかには影響しません (これは ILM によって決定されます)。

取り込まれたオブジェクトに一致するILMルールが厳密な取り込みオプションを使用している場合、``x-amz-storage-class``ヘッダーは効果がありません。

以下の値は、`x-amz-storage-class`` :

- STANDARD (デフォルト)

- デュアル コミット: ILM ルールで取り込み動作にデュアル コミット 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 番目のコピーが作成され、別のストレージ ノードに配布されます (デュアル コミット)。ILM が評価されると、StorageGRID はこれらの初期の中間コピーがルール内の配置指示を満たしているかどうかを判断します。そうでない場合は、別の場所に新しいオブジェクトのコピーを作成し、初期の中間コピーを削除する必要があるかもしれません。
- バランス: ILM ルールでバランス オプションが指定されていて、StorageGRID がルールで指定されたすべてのコピーをすぐに作成できない場合、StorageGRID は異なるストレージ ノードに 2 つの中間コピーを作成します。

StorageGRIDがILMルールで指定されたすべてのオブジェクトコピーを即時に作成できる場合 (同期配置)、`x-amz-storage-class`ヘッダーは効果がありません。

- REDUCED_REDUNDANCY

- デュアル コミット: ILM ルールで取り込み動作にデュアル コミット 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単一の中間コピーを作成します (単一コミット)。
- バランス: ILM ルールでバランス オプションが指定されている場合、StorageGRID は、システムがルールで指定されたすべてのコピーをすぐに作成できない場合にのみ、単一の中間コピーを作成します。StorageGRID が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。その `REDUCED_REDUNDANCY` このオプションは、オブジェクトに一致する ILM ルールによって単一の複製コピーが作成される場合に最適です。この場合、`REDUCED_REDUNDANCY` すべての取り込み操作で余分なオブジェクト コピーが不必要に作成および削除されるのを防ぎます。

使用して `REDUCED_REDUNDANCY` 他の状況で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 評価が行われる前に障害が発生したストレージ ノードに単一のコピーが最初に保存された場合、データが失われる可能性があります。



任意の期間に複製されたコピーが 1 つしかない場合、データが永久に失われるリスクがあります。オブジェクトの複製されたコピーが 1 つしか存在しない場合、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手順中は、オブジェクトへのアクセス権が一時的に失われます。

指定 `REDUCED_REDUNDANCY` オブジェクトが最初に取り込まれたときに作成されるコピーの数にのみ影響します。これは、オブジェクトがアクティブな ILM ポリシーによって評価されるときに作成されるオブジェクトのコピー数には影響せず、StorageGRIDシステムに低いレベルの冗長性でデータが保存されることにはなりません。



S3オブジェクトロックが有効になっているバケットにオブジェクトを取り込む場合、`REDUCED_REDUNDANCY` オプションは無視されます。レガシーコンプライアンスバケットにオブジェクトを取り込む場合、`REDUCED_REDUNDANCY` オプションはエラーを返します。StorageGRID は、コンプライアンス要件が満たされていることを確認するために、常にデュアルコミット取り込みを実行します。

サーバー側暗号化のリクエストヘッダー

次のリクエスト ヘッダーを使用して、サーバー側暗号化でオブジェクトを暗号化できます。SSE オプションと SSE-C オプションは相互に排他的です。

- **SSE:** StorageGRIDによって管理される一意のキーを使用してオブジェクトを暗号化する場合は、次のヘッダーを使用します。
 - `x-amz-server-side-encryption`

いつ ``x-amz-server-side-encryption`PutObject` リクエストにヘッダーが含まれていない場合、グリッド全体の["保存オブジェクトの暗号化設定"](#)PutObject 応答から省略されます。
- **SSE-C:** 提供および管理する一意のキーを使用してオブジェクトを暗号化する場合は、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`: 特定 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。



提供された暗号化キーは保存されません。暗号化キーを紛失すると、対応するオブジェクトも失われます。顧客提供のキーを使用してオブジェクトデータを保護する前に、以下の考慮事項を確認してください。["サーバー側暗号化を使用する"](#)。



オブジェクトが SSE または SSE-C で暗号化されている場合、バケット レベルまたはグリッドレベルの暗号化設定はすべて無視されます。

バージョン管理

バケットのバージョン管理が有効になっている場合、一意の ``versionId`` 保存されるオブジェクトのバージョンに応じて自動的に生成されます。これ ``versionId`` レスポンスでは、``x-amz-version-id`` レスポンス ヘッダー。

バージョン管理が中断されている場合、オブジェクトのバージョンは null で保存されます。``versionId`` 複数バージョンがすでに存在する場合は上書きされます。

Authorization ヘッダーの署名計算

使用する際は ``Authorization`` ヘッダーを使用してリクエストを認証する点において、StorageGRID は AWS と次の点で異なります。

- StorageGRID は `host`` 含まれるヘッダー ``CanonicalHeaders``。
- StorageGRID は `Content-Type`` 含まれる ``CanonicalHeaders``。
- StorageGRID は `x-amz-*`` 含まれるヘッダー ``CanonicalHeaders``。



一般的なベストプラクティスとして、これらのヘッダーを常に含めてください。``CanonicalHeaders`` 確実に検証するためです。ただし、これらのヘッダーを除外すると、StorageGRID はエラーを返しません。

詳細については、["認証ヘッダーの署名計算: ペイロードを単一チャンクで転送する \(AWS 署名バージョン 4\)"](#)。

関連情報

- ["ILMでオブジェクトを管理する"](#)
- ["Amazon Simple Storage Service API リファレンス: PutObject"](#)

オブジェクトの復元

S3 RestoreObject リクエストを使用して、クラウド ストレージ プールに保存されているオブジェクトを復元できます。

サポートされているリクエストタイプ

StorageGRID は、オブジェクトを復元するための RestoreObject 要求のみをサポートします。サポートされていません SELECT `修復の種類`。選択したリクエストの戻り `XNotImplemented`。

バージョン管理

オプションで指定 `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復元します。指定しない場合 `versionId` オブジェクトの最新バージョンが復元されます

Cloud Storage Pool オブジェクトにおける RestoreObject の動作

オブジェクトが["クラウド ストレージ プール"](#) RestoreObject 要求は、オブジェクトの状態に基づいて次の動作をします。見る["HeadObject"](#)詳細についてはこちらをご覧ください。



オブジェクトがクラウド ストレージ プールに保存され、そのオブジェクトの 1 つ以上のコピーがグリッド上に存在する場合は、RestoreObject リクエストを発行してオブジェクトを復元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	RestoreObjectの動作
オブジェクトはStorageGRIDに取り込まれましたが、ILMによってまだ評価されていません。または、オブジェクトが Cloud Storage Pool にありません。	403 Forbidden、InvalidObjectState
Cloud Storage Pool 内のオブジェクトですが、まだ取得不可の状態に移行していません	`200 OK`変更は行われません。 注意: オブジェクトが取得不可能な状態に移行する前に、そのオブジェクトを変更することはできません。 expiry-date。

オブジェクトの状態	RestoreObjectの動作
オブジェクトは取得不可能な状態に移行しました	<p>`202 Accepted` リクエスト本文で指定された日数の間、オブジェクトの取得可能なコピーを Cloud Storage プールに復元します。この期間が終了すると、オブジェクトは取得不可能な状態に戻されます。</p> <p>オプションとして、Tier`復元ジョブの完了にかかる時間を決定するためのリクエスト要素(`Expedited、Standard、またはBulk)。指定しない場合 Tier、`Standard`ティアが使用されます。</p> <p>重要: オブジェクトがS3 Glacier Deep Archiveに移行されている場合、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、Expedited`層。次のエラーが返されます `403 Forbidden、InvalidTier:Retrieval option is not supported by this storage class。</p>
回復不可能な状態から復元中のオブジェクト	409 Conflict、RestoreAlreadyInProgress
オブジェクトがクラウド ストレージ プールに完全に復元されました	<p>200 OK</p> <p>注: オブジェクトが取得可能な状態に復元された場合、その expiry-date`新しい値でRestoreObjectリクエストを再発行することにより、`Days。復元日付はリクエストの時刻に応じて更新されます。</p>

オブジェクトコンテンツの選択

S3 SelectObjectContent リクエストを使用すると、単純な SQL ステートメントに基づいて S3 オブジェクトの内容をフィルタリングできます。

詳細については、"[Amazon Simple Storage Service API リファレンス: SelectObjectContent](#)"。

開始する前に

- テナント アカウントには S3 Select 権限があります。
- あなたが持っている `s3:GetObject` クエリを実行するオブジェクトに対する権限。
- クエリ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 または BZIP2 アーカイブに圧縮することもできます。
 - 寄木細工。 Parquet オブジェクトの追加要件:
 - S3 Select は、GZIP または Snappy を使用した列指向の圧縮のみをサポートします。 S3 Select は、Parquet オブジェクトのオブジェクト全体の圧縮をサポートしていません。
 - S3 Select は Parquet 出力をサポートしていません。出力形式を CSV または JSON として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 512 MB です。
 - オブジェクトのスキーマで指定された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 256 KB です。
- 入力または結果のレコードの最大長は 1 MiB です。

CSV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>
    <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>
```

Parquet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、米国国勢調査データから州名、2010年の人口、2015年の推定人口、および変化率を取得します。ファイル内の状態ではない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は、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 (Parquet)

```
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 changes.csv の最初の数行は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
```

マルチパートアップロードの操作

マルチパートアップロードの操作

このセクションでは、StorageGRID がマルチパートアップロードの操作をサポートする方法について説明します。

すべてのマルチパートアップロード操作には、次の条件と注意事項が適用されます。

- バケットに対する ListMultipartUploads クエリの結果が不完全な結果を返す可能性があるため、1つのバケットへの同時マルチパートアップロードは 1,000 件を超えないようにしてください。
- StorageGRID は、マルチパートパーツに対して AWS 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ツは、5 MiB (5,242,880 バイト) ~ 5 GiB (5,368,709,120 バイト) の範囲にする必要があります。
 - 最後の部分は 5 MiB (5,242,880 バイト) より小さくても構いません。
 - 一般に、部品サイズは可能な限り大きくする必要があります。たとえば、100 GiB のオブジェクトには 5 GiB のパーツサイズを使用します。各パーツは一意的オブジェクトと見なされるため、大きなパーツ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。
 - 5 GiB 未満のオブジェクトの場合は、代わりに非マルチパートアップロードの使用を検討してください。
- ILM ルールがバランス型または厳密型を使用している場合、ILM は、マルチパートオブジェクトの各部分が取り込まれる際に評価され、マルチパートアップロードが完了するとオブジェクト全体に対して評価されます。["取り込みオプション"](#)。これがオブジェクトとパーツの配置にどのように影響するかは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進行中に ILM が変更されると、マルチパートアップロードが完了したときにオブジェクトの一部が現在の ILM 要件を満たさなくなる可能性があります。正しく配置されていないパーツは ILM 再評価のキューに入れられ、後で正しい場所に移動されます。
- パーツの 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ツのサイズに基づいてフィルタリングします。つまり、オブジェクトの一部は、オブジェクト全体の ILM 要件を満たさない場所に保存される可能性があります。たとえば、10 GB 以上のすべてのオブジェクトを DC1 に保存し、それより小さいすべてのオブジェクトを DC2 に保存するようにルールで指定すると、10 パーツのマルチパートアップロードの各 1 GB の部分は、取り込み時に DC2 に保存されます。ただし、オブジェクト全体に対して ILM が評価されると、オブジェクトのすべての部分が DC1 に移動されます。
- すべてのマルチパートアップロード操作はStorageGRIDをサポートしています"**一貫性値**"。
- 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む場合、"**オブジェクトセグメンテーションしきい値 (1 GiB)**" 適用されません。
- 必要に応じて、"**サーバー側の暗号化**"マルチパートアップロードを使用します。SSE (StorageGRID管理キーによるサーバー側暗号化) を使用するには、 `x-amz-server-side-encryption` CreateMultipartUpload リクエスト内のリクエスト ヘッダーのみ。SSE-C (顧客提供のキーを使用したサーバー側暗号化) を使用するには、CreateMultipartUpload リクエストと後続の各 UploadPart リクエストで同じ 3 つの暗号化キー リクエスト ヘッダーを指定します。

処理	導入
AbortMultipartUpload	すべての Amazon S3 REST API 動作が実装されています。予告なく変更されることがあります。
CompleteMultipartUpload	見る" CompleteMultipartUpload "
CreateMultipartUpload (以前の名称は「マルチパートアップロードの開始」)	見る" CreateMultipartUpload "
リストマルチパートアップロード	見る" リストマルチパートアップロード "
ListParts	すべての Amazon S3 REST API 動作が実装されています。予告なく変更されることがあります。
UploadPart	見る" UploadPart "
UploadPartCopy	見る" UploadPartCopy "

CompleteMultipartUpload

CompleteMultipartUpload 操作は、以前にアップロードされた部分を組み立てることで、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。



StorageGRIDは昇順で連続しない値をサポートします。partNumber CompleteMultipartUpload のリクエスト パラメータ。パラメータは任意の値で始めることができます。

紛争を解決する

2つのクライアントが同じキーに書き込むなど、競合するクライアント要求は、「最新のを優先」して解決されます。「最新のもの優先」評価のタイミングは、S3クライアントが操作を開始した時点ではなく、StorageGRIDシステムが特定のリクエストを完了した時点に基づきます。

サポートされているリクエストヘッダー

次のリクエスト ヘッダーがサポートされています。

- x-amz-checksum-sha256
- x-amz-storage-class

その `x-amz-storage-class` ヘッダーは、一致するILMルールで指定されている場合にStorageGRIDが作成するオブジェクトコピーの数に影響します。**"デュアルコミットまたはバランス取り込みオプション"**。

- STANDARD

(デフォルト) ILM ルールがデュアル コミット オプションを使用する場合、またはバランス オプションが中間コピーの作成にフォールバックする場合に、デュアル コミット インジェスト操作を指定します。

- REDUCED_REDUNDANCY

ILM ルールがデュアル コミット オプションを使用する場合、またはバランス オプションが中間コピーの作成にフォールバックする場合に、単一コミットの取り込み操作を指定します。



S3オブジェクトロックが有効になっているバケットにオブジェクトを取り込む場合、`REDUCED_REDUNDANCY` オプションは無視されます。レガシーコンプライアンスバケットにオブジェクトを取り込む場合、`REDUCED_REDUNDANCY` オプションはエラーを返します。StorageGRID は、コンプライアンス要件が満たされていることを確認するために、常にデュアルコミット取り込みを実行します。



マルチパートアップロードが15日以内に完了しない場合、操作は非アクティブとしてマークされ、関連するすべてのデータがシステムから削除されます。



その `ETag` 返される値はデータのMD5合計ではなく、Amazon S3 API実装に従います。`ETag` マルチパートオブジェクトの値。

サポートされていないリクエストヘッダー

次のリクエスト ヘッダーはサポートされていません。

- x-amz-sdk-checksum-algorithm
- x-amz-trailer

バージョン管理

この操作により、マルチパートアップロードが完了します。バケットのバージョン管理が有効になっている場合、マルチパートアップロードの完了後にオブジェクトバージョンが作成されます。

バケットのバージョン管理が有効になっている場合、一意の `versionId` 保存されるオブジェクトのバージョンに応じて自動的に生成されます。これ `versionId` レスポンスでは、`x-amz-version-id` レスポンス ヘッダー。

バージョン管理が中断されている場合、オブジェクトのバージョンは null で保存されます。`versionId` 複数バージョンがすでに存在する場合は上書きされます。



バケットのバージョン管理が有効になっている場合、同じオブジェクト キーで同時にマルチパートアップロードが完了している場合でも、マルチパートアップロードを完了すると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場合、マルチパートアップロードを開始し、次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を開始して完了させることが可能です。バージョン管理され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が失敗しました

マルチパートアップロードが行われるバケットがプラットフォーム サービス用に構成されている場合、関連付けられたレプリケーションまたは通知アクションが失敗しても、マルチパートアップロードは成功します。

テナントは、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。テナントは、不要な変更を避けるために既存の値を再送信できます。

。 ["プラットフォームサービスのトラブルシューティング"](#)。

CreateMultipartUpload

CreateMultipartUpload (以前の名前は Initiate Multipart Upload) 操作は、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。

その `x-amz-storage-class` リクエスト ヘッダーがサポートされています。提出された値は `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ますが、オブジェクトの永続コピーが StorageGRID システムにいくつ保存されるかには影響しません (これは ILM によって決定されます)。

取り込まれたオブジェクトに一致する ILM ルールが厳密な ["取り込みオプション"](#)、`x-amz-storage-class` ヘッダーは効果がありません。

以下の値は、`x-amz-storage-class` :

- STANDARD (デフォルト)
 - デュアル コミット: ILM ルールでデュアル コミット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 番目のコピーが作成され、別のストレージノードに配布されます (デュアル コミット)。ILM が評価されると、StorageGRID はこれらの初期の中間コピーがルール内の配置指示を満たしているかどうかを判断します。そうでない場合は、別の場所に新しいオブジェクトのコピーを作成し、初期の中間コピーを削除する必要があるかもしれません。
 - バランス: ILM ルールでバランス オプションが指定されていて、StorageGRID がルールで指定された

すべてのコピーをすぐに作成できない場合、StorageGRID は異なるストレージ ノードに 2 つの間コピーを作成します。

StorageGRIDがILMルールで指定されたすべてのオブジェクトコピーを即時に作成できる場合（同期配置）、`x-amz-storage-class`ヘッダーは効果がありません。

- REDUCED_REDUNDANCY

- デュアル コミット: ILM ルールでデュアル コミット オプションが指定されている場合、StorageGRID はオブジェクトが取り込まれると単一の間コピーを作成します (シングル コミット)。
- バランス: ILM ルールでバランス オプションが指定されている場合、StorageGRID は、システムがルールで指定されたすべてのコピーをすぐに作成できない場合にのみ、単一の間コピーを作成します。StorageGRID が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。その `REDUCED_REDUNDANCY` このオプションは、オブジェクトに一致する ILM ルールによって単一の複製コピーが作成される場合に最適です。この場合、`REDUCED_REDUNDANCY` すべての取り込み操作で余分なオブジェクト コピーが不必要に作成および削除されるのを防ぎます。

使用して `REDUCED_REDUNDANCY` 他の状況で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 評価が行われる前に障害が発生したストレージ ノードに単一のコピーが最初に保存された場合、データが失われる可能性があります。



任意の期間に複製されたコピーが 1 つしかない場合、データが永久に失われるリスクがあります。オブジェクトの複製されたコピーが 1 つしか存在しない場合、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手順中は、オブジェクトへのアクセス権が一時的に失われます。

指定 `REDUCED_REDUNDANCY` オブジェクトが最初に取り込まれたときに作成されるコピーの数にのみ影響します。これは、オブジェクトがアクティブな ILM ポリシーによって評価されるときに作成されるオブジェクトのコピー数には影響せず、StorageGRIDシステムに低いレベルの冗長性でデータが保存されることにはなりません。



S3オブジェクトロックが有効になっているバケットにオブジェクトを取り込む場合、`REDUCED_REDUNDANCY` オプションは無視されます。レガシーコンプライアンスバケットにオブジェクトを取り込む場合、`REDUCED_REDUNDANCY` オプションはエラーを返します。StorageGRID は、コンプライアンス要件が満たされていることを確認するために、常にデュアルコミット取り込みを実行します。

サポートされているリクエストヘッダー

次のリクエスト ヘッダーがサポートされています。

- Content-Type
- x-amz-checksum-algorithm

現在、SHA256値のみが `x-amz-checksum-algorithm` サポートされています。

- x-amz-meta-、その後ユーザー定義のメタデータを含む名前と値のペアが続く

ユーザー定義のメタデータの名前と値のペアを指定する場合は、次の一般的な形式を使用します。

```
x-amz-meta-_name_: `value`
```

ILMルールの参照時間として*ユーザー定義作成時間*オプションを使用する場合は、`creation-time`オブジェクトが作成された日時を記録するメタデータの名前として。例えば：

```
x-amz-meta-creation-time: 1443399726
```

の価値 `creation-time` 1970 年 1 月 1 日からの秒数として評価されます。



追加 `creation-time` 従来のコンプライアンス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、ユーザー定義の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リクエストヘッダー:

- x-amz-object-lock-mode
- x-amz-object-lock-retain-until-date
- x-amz-object-lock-legal-hold

これらのヘッダーなしでリクエストが行われた場合、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 バージョンの保持期限が計算されます。

"S3 REST API を使用して S3 オブジェクトロックを設定する"

• SSE リクエスト 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

[サーバー側暗号化のリクエストヘッダー]



StorageGRIDがUTF-8文字を処理する方法については、以下を参照してください。"PutObject"。

サーバー側暗号化のリクエストヘッダー

次のリクエスト ヘッダーを使用して、サーバー側暗号化でマルチパート オブジェクトを暗号化できます。SSE オプションと SSE-C オプションは相互に排他的です。

- **SSE:** StorageGRIDによって管理される一意のキーを使用してオブジェクトを暗号化する場合は、CreateMultipartUpload リクエストで次のヘッダーを使用します。いずれの UploadPart リクエストでもこのヘッダーを指定しないでください。
 - x-amz-server-side-encryption

- **SSE-C**: 提供および管理する一意のキーを使用してオブジェクトを暗号化する場合は、CreateMultipartUpload リクエスト (および後続の各 UploadPart リクエスト) 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: 特定 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。



提供された暗号化キーは保存されません。暗号化キーを紛失すると、対応するオブジェクトも失われます。顧客提供のキーを使用してオブジェクトデータを保護する前に、以下の考慮事項を確認してください。"[サーバー側暗号化を使用する](#)"。

サポートされていないリクエストヘッダー

次のリクエスト ヘッダーはサポートされていません。

- x-amz-website-redirect-location

その x-amz-website-redirect-location `ヘッダーリターン` XNotImplemented。

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、アップロードの一覧表示、パーツのアップロード、アップロードされたパーツの組み立て、アップロードの完了という個別の操作で構成されます。CompleteMultipartUpload 操作が実行されると、オブジェクトが作成され (該当する場合はバージョン管理も行われます)。

リストマルチパートアップロード

ListMultipartUploads オペレーションは、バケットの進行中のマルチパートアップロードを一覧表示します。

次のリクエスト 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、アップロードの一覧表示、パーツのアップロード、アップロードされたパーツの組み立て、アップロードの完了という個別の操作で構成されます。CompleteMultipartUpload 操作が実行されると、オブジェクトが作成され (該当する場合はバージョン管理も行われます)。

UploadPart

UploadPart 操作は、オブジェクトのマルチパートアップロードの一部をアップロードします。

サポートされているリクエストヘッダー

次のリクエスト ヘッダーがサポートされています。

- x-amz-checksum-sha256
- Content-Length
- Content-MD5

サーバー側暗号化のリクエストヘッダー

CreateMultipartUpload リクエストに SSE-C 暗号化を指定した場合は、各 UploadPart リクエストに次のリクエスト ヘッダーも含める必要があります。

- x-amz-server-side-encryption-customer-algorithm: 特定 AES256。
- x-amz-server-side-encryption-customer-key: CreateMultipartUpload リクエストで指定したのと同じ暗号化キーを指定します。
- x-amz-server-side-encryption-customer-key-MD5: CreateMultipartUpload リクエストで指定したのと同じ MD5 ダイジェストを指定します。



提供された暗号化キーは保存されません。暗号化キーを紛失すると、対応するオブジェクトも失われます。顧客提供のキーを使用してオブジェクトデータを保護する前に、以下の考慮事項を確認してください。"サーバー側の暗号化を使用する"。

CreateMultipartUpload リクエスト中に SHA-256 チェックサムを指定した場合は、各 UploadPart リクエストに次のリクエスト ヘッダーも含める必要があります。

- x-amz-checksum-sha256: この部分の SHA-256 チェックサムを指定します。

サポートされていないリクエストヘッダー

次のリクエスト ヘッダーはサポートされていません。

- x-amz-sdk-checksum-algorithm
- x-amz-trailer

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、アップロードの一覧表示、パーツのアップロード、アップロードされたパーツの組み立て、アップロードの完了という個別の操作で構成されます。CompleteMultipartUpload 操作が実行されると、オブジェクトが作成され (該当する場合はバージョン管理も行われます)。

UploadPartCopy

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して、オブジェクトの一部をアップロードします。

UploadPartCopy 操作は、すべての Amazon S3 REST API 動作で実装されます。予告なく変更されることがあります。

このリクエストは、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。

次のリクエスト 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

サーバー側暗号化のリクエストヘッダー

CreateMultipartUpload リクエストに SSE-C 暗号化を指定した場合は、各 UploadPartCopy リクエストに次のリクエスト ヘッダーも含める必要があります。

- x-amz-server-side-encryption-customer-algorithm: 特定 AES256。
- x-amz-server-side-encryption-customer-key: CreateMultipartUpload リクエストで指定したのと同じ暗号化キーを指定します。
- x-amz-server-side-encryption-customer-key-MD5: CreateMultipartUpload リクエストで指定したのと同じ MD5 ダイジェストを指定します。

ソース オブジェクトが顧客提供のキー (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: 特定 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。



提供された暗号化キーは保存されません。暗号化キーを紛失すると、対応するオブジェクトも失われます。顧客提供のキーを使用してオブジェクトデータを保護する前に、以下の考慮事項を確認してください。"[サーバー側の暗号化を使用する](#)"。

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、アップロードの一覧表示、パーツのアップロード、アップロードされたパーツの組み立て、アップロードの完了という個別の操作で構成されます。CompleteMultipartUpload 操作が実行されると、オブジェクトが作成され (該当する場合はバージョン管理も行われます)。

エラー応答

StorageGRIDシステムは、適用されるすべての標準 S3 REST API エラー応答をサポートします。さらに、StorageGRID実装ではいくつかのカスタム応答が追加されます。

サポートされているS3 APIエラーコード

Name	HTTPのステータス
アクセスが拒否されました	403 Forbidden
バッドダイジェスト	400 Bad Request
バケットが既に存在する	409 紛争
バケットが空でない	409 紛争
不完全なボディ	400 Bad Request
内部エラー	500 内部サーバーエラー
無効なアクセスキーID	403 Forbidden
無効な引数	400 Bad Request
無効なバケット名	400 Bad Request
無効なバケット状態	409 紛争
無効なダイジェスト	400 Bad Request
無効な暗号化アルゴリズムエラー	400 Bad Request
無効な部分	400 Bad Request
無効な部品順序	400 Bad Request
無効な範囲	416 要求された範囲は満たされません

Name	HTTPのステータス
無効なリクエスト	400 Bad Request
無効なストレージクラス	400 Bad Request
無効なタグ	400 Bad Request
無効なURI	400 Bad Request
キーが長すぎる	400 Bad Request
不正なXML	400 Bad Request
メタデータが大きすぎる	400 Bad Request
メソッドが許可されていません	405 メソッドは許可されていません
コンテンツの長さが不足しています	411 長さが必要です
リクエストボディエラーが見つかりません	400 Bad Request
セキュリティヘッダーがありません	400 Bad Request
NoSuchBucket	404 Not Found
NoSuchKey	404 Not Found
アップロード不可	404 Not Found
実装されていません	501 実装されていません
NoSuchBucketPolicy	404 Not Found
オブジェクトロック構成が見つかりませんエラー	404 Not Found
前提条件失敗	412 前提条件が失敗しました
リクエスト時間が偏りすぎている	403 Forbidden
サービスは利用できません	503 サービスは利用できません
署名が一致しない	403 Forbidden

Name	HTTPのステータス
バケットが多すぎる	400 Bad Request
ユーザーキーを指定する必要があります	400 Bad Request

StorageGRIDカスタムエラーコード

Name	説明	HTTPのステータス
XBucketライフサイクルが許可されていません	レガシーコンプライアンスバケットではバケットライフサイクル設定は許可されません	400 Bad Request
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 Bad Request
Xコンプライアンス競合	従来のコンプライアンス設定のため、操作は拒否されました。	403 Forbidden
XComplianceReducedRedundancyForbidden	従来の準拠バケットでは冗長性の低下は許可されません	400 Bad Request
XMaxBucketPolicyLength を超えました	ポリシーがバケット ポリシーの最大許容長を超えています。	400 Bad Request
XMissingInternalRequestHeader	内部リクエストのヘッダーがありません。	400 Bad Request
XNoSuchBucketCompliance	指定されたバケットでは、従来のコンプライアンスが有効になっていません。	404 Not Found
X受け入れられない	リクエストには、満たすことができなかった1つ以上の Accept ヘッダーが含まれています。	406 受け入れられません
X未実装	提供されたリクエストには、実装されていない機能が含まれています。	501 実装されていません

StorageGRIDカスタム操作

StorageGRIDカスタム操作

StorageGRIDシステムは、S3 REST API に追加されたカスタム操作をサポートします。

次の表は、StorageGRIDでサポートされているカスタム操作を示しています。

処理	説明
"GETバケットの一貫性"	特定のバケットに適用されている一貫性を返します。
"PUT バケットの一貫性"	特定のバケットに適用される一貫性を設定します。
"GET バケットの最終アクセス時刻"	特定のバケットの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。
"バケットの最終アクセス時刻をPUTする"	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することができます。
"バケットメタデータ通知設定の削除"	特定のバケットに関連付けられたメタデータ通知構成 XML を削除します。
"バケットメタデータ通知設定の取得"	特定のバケットに関連付けられたメタデータ通知構成 XML を返します。
"PUT バケットメタデータ通知設定"	バケットのメタデータ通知サービスを設定します。
"ストレージ使用量の取得"	アカウントと、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合計量を示します。
"非推奨: コンプライアンス設定による CreateBucket"	非推奨およびサポートされていません: コンプライアンスを有効にして新しいバケットを作成することはできなくなりました。
"非推奨: GET バケットコンプライアンス"	非推奨ですがサポートされています: 既存のレガシー コンプライアンスバケットに対して現在有効なコンプライアンス設定を返します。
"非推奨: PUT バケットのコンプライアンス"	非推奨ですがサポートされています: 既存のレガシー コンプライアンスバケットのコンプライアンス設定を変更できます。

GETバケットの一貫性

GET Bucket 整合性リクエストを使用すると、特定のバケットに適用されている整合性を判別できます。

デフォルトの一貫性は、新しく作成されたオブジェクトの書き込み後の読み取りを保証するように設定されています。

この操作を完了するには、s3:GetBucketConsistency 権限を持っているか、アカウント ルートである必要があります。

リクエスト例

```
GET /bucket?x-ntap-sg-consistency HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

応答

レスポンスXMLでは、`<Consistency>`次のいずれかの値を返します。

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

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>
```

PUT バケットの一貫性

PUT Bucket 整合性リクエストを使用すると、バケットに対して実行される操作に適用する整合性を指定できます。

デフォルトの一貫性は、新しく作成されたオブジェクトの書き込み後の読み取りを保証するように設定されています。

開始する前に

この操作を完了するには、s3:PutBucketConsistency 権限を持っているか、アカウント ルートである必要があります。

要求

その `x-ntap-sg-consistency` パラメータには次のいずれかの値が含まれている必要があります。

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

注: 一般的には、「新規書き込み後の読み取り」の一貫性を使用する必要があります。リクエストが正しく機能しない場合は、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、各 API リクエストの一貫性を指定するようにクライアントを構成します。最後の手段としてのみ、バケット レベルで一貫性を設定します。

リクエスト例

```
PUT /bucket?x-ntap-sg-consistency=strong-global HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

関連情報

"一貫性の値"

GET バケットの最終アクセス時刻

GET Bucket 最終アクセス時刻リクエストを使用すると、個々のバケットの最終アクセス時刻の更新が有効になっているか無効になっているかを判断できます。

この操作を完了するには、s3:GetBucketLastAccessTime 権限を持っているか、アカウント ルートである必要があります。

リクエスト例

```
GET /bucket?x-ntap-sg-lastaccesstime HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

応答例

この例では、バケットの最終アクセス時刻の更新が有効になっていることを示しています。

```
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>
```

バケットの最終アクセス時刻をPUTする

PUT Bucket 最終アクセス時刻リクエストを使用すると、個々のバケットの最終アクセス時刻の更新を有効または無効にすることができます。最終アクセス時刻の更新を無効にするとパフォーマンスが向上し、これはバージョン 10.3.0 以降で作成されたすべてのバ

ケットのデフォルト設定になります。

この操作を完了するには、バケットに対する s3:PutBucketLastAccessTime 権限を持っているか、アカウントルートである必要があります。



StorageGRIDバージョン 10.3 以降では、すべての新しいバケットの最終アクセス時間の更新はデフォルトで無効になっています。以前のバージョンのStorageGRIDを使用して作成されたバケットがあり、新しいデフォルトの動作に一致させたい場合は、以前のバケットごとに最終アクセス時刻の更新を明示的に無効にする必要があります。PUT Bucket last access time リクエストを使用するか、テナント マネージャーのバケットの詳細ページから、最終アクセス時間の更新を有効または無効にすることができます。見る"[最終アクセス時間の更新を有効または無効にする](#)"。

バケットの最終アクセス時間の更新が無効になっている場合、バケットに対する操作には次の動作が適用されます。

- GetObject、GetObjectAcl、GetObjectTagging、および HeadObject リクエストでは、最終アクセス時間が更新されません。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 および PutObjectTagging リクエストでは、最終アクセス時刻も更新されます。オブジェクトは ILM 評価のキューに追加されます。
- ソース バケットの最終アクセス時間の更新が無効になっている場合、CopyObject リクエストでは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、宛先の場合、CopyObject 要求によって最終アクセス時刻が常に更新されます。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 は最終アクセス時間の更新を要求します。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。

リクエスト例

この例では、バケットの最終アクセス時間を有効にします。

```
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ます。

```
PUT /bucket?x-ntap-sg-lastaccesstime=disabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

バケットメタデータ通知設定の削除

DELETE Bucket メタデータ通知構成リクエストを使用すると、構成 XML を削除して、

個々のバケットの検索統合サービスを無効にすることができます。

この操作を完了するには、バケットに対する `s3:DeleteBucketMetadataNotification` 権限を持っているか、アカウント ルートである必要があります。

リクエスト例

この例では、バケットの検索統合サービスを無効にする方法を示します。

```
DELETE /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

バケットメタデータ通知設定の取得

GET バケット メタデータ通知構成リクエストを使用すると、個々のバケットの検索統合を構成するために使用される構成 XML を取得できます。

この操作を完了するには、`s3:GetBucketMetadataNotification` 権限を持っているか、アカウント ルートである必要があります。

リクエスト例

このリクエストは、バケットのメタデータ通知設定を取得します。 `bucket`。

```
GET /bucket?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

応答

レスポンス本文には、バケットのメタデータ通知構成が含まれます。メタデータ通知構成では、検索統合用にバケットを構成する方法を決定できます。つまり、どのオブジェクトがインデックスされているか、またそのオブジェクト メタデータがどのエンドポイントに送信されているかを判別できます。

```

<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>

```

各メタデータ通知構成には、1つ以上のルールが含まれます。各ルールは、適用されるオブジェクトと、StorageGRIDがオブジェクトメタデータを送信する宛先を指定します。宛先は、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。

Name	説明	必須
メタデータ通知構成	メタデータ通知のオブジェクトと宛先を指定するために使用されるルールのコンテナ タグ。 1つ以上の Rule 要素が含まれます。	はい
Rule	指定されたインデックスにメタデータを追加するオブジェクトを識別するルールのコンテナ タグ。 プレフィックスが重複するルールは拒否されます。 MetadataNotificationConfiguration 要素に含まれます。	はい
ID	ルールの一意的識別子。 ルール要素に含まれます。	いいえ
ステータス	ステータスは「有効」または「無効」になります。無効にされているルールに対してはアクションは実行されません。 ルール要素に含まれます。	はい

Name	説明	必須
接頭辞	<p>プレフィックスに一致するオブジェクトはルールの影響を受け、そのメタデータは指定された宛先に送信されます。</p> <p>すべてのオブジェクトを一致させるには、空のプレフィックスを指定します。</p> <p>ルール要素に含まれます。</p>	はい
デスティネーション	<p>ルールの宛先のコンテナ タグ。</p> <p>ルール要素に含まれます。</p>	はい
壺	<p>オブジェクト メタデータが送信される宛先の URN。次のプロパティを持つStorageGRIDエンドポイントの URN である必要があります。</p> <ul style="list-style-type: none"> • `es` 3 番目の要素である必要があります。 • URNは、メタデータが格納されているインデックスとタイプで終わる必要があります。形式は次のようになります。 domain-name/myindex/mytype 。 <p>エンドポイントは、テナント マネージャーまたはテナント管理 API を使用して構成されます。それらは次の形式をとります:</p> <ul style="list-style-type: none"> • arn:aws:es:_region:account-ID_:domain/mydomain/myindex/mytype • urn:mysite:es:::mydomain/myindex/mytype <p>構成 XML を送信する前にエンドポイントを構成する必要があります。そうしないと、404 エラーが発生して構成が失敗します。</p> <p>Urn は Destination 要素に含まれます。</p>	はい

応答例

XMLは、`<MetadataNotificationConfiguration></MetadataNotificationConfiguration>` tags は、バケットの検索統合エンドポイントとの統合がどのように構成されているかを示します。この例では、オブジェクトメタデータはElasticsearchインデックスに送信されています。 `current`` と名付けられたタイプ ``2017`` 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 バケットメタデータ通知設定

PUT バケット メタデータ通知構成リクエストを使用すると、個々のバケットの検索統合サービスを有効にすることができます。リクエスト本文に指定するメタデータ通知構成 XML は、メタデータが宛先検索インデックスに送信されるオブジェクトを指定します。

この操作を完了するには、バケットに対する s3:PutBucketMetadataNotification 権限を持っているか、アカウント ルートである必要があります。

要求

リクエストには、リクエスト本文にメタデータ通知構成が含まれている必要があります。各メタデータ通知構成には、1 つ以上のルールが含まれます。各ルールは、適用されるオブジェクトと、StorageGRIDがオブジェクト メタデータを送信する宛先を指定します。

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、プレフィックスを持つオブジェクトのメタデータを送信できます。 /images 1つの宛先に、接頭辞を持つオブジェクト `videos` 別の人に。

プレフィックスが重複する構成は無効であり、送信時に拒否されます。たとえば、接頭辞を持つオブジェクトに対する1つのルールを含む構成では、`test` 接頭辞を持つオブジェクトに対する2番目のルール `test2` 許可されません。

宛先は、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。メタデータ通知設定が送

信されるときにエンドポイントが存在している必要があります。存在しない場合、リクエストは失敗します。400 Bad Request エラーメッセージは次のようになります。`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>
```

この表では、メタデータ通知構成 XML の要素について説明します。

Name	説明	必須
メタデータ通知構成	メタデータ通知のオブジェクトと宛先を指定するために使用されるルールのコンテナ タグ。 1 つ以上の Rule 要素が含まれます。	はい
Rule	指定されたインデックスにメタデータを追加するオブジェクトを識別するルールのコンテナ タグ。 プレフィックスが重複するルールは拒否されます。 MetadataNotificationConfiguration 要素に含まれません。	はい
ID	ルールの一意的識別子。 ルール要素に含まれます。	いいえ
ステータス	ステータスは「有効」または「無効」になります。無効にされているルールに対してはアクションは実行されません。 ルール要素に含まれます。	はい

Name	説明	必須
接頭辞	<p>プレフィックスに一致するオブジェクトはルールの影響を受け、そのメタデータは指定された宛先に送信されます。</p> <p>すべてのオブジェクトを一致させるには、空のプレフィックスを指定します。</p> <p>ルール要素に含まれます。</p>	はい
デスティネーション	<p>ルールの宛先のコンテナ タグ。</p> <p>ルール要素に含まれます。</p>	はい
壺	<p>オブジェクト メタデータが送信される宛先の URN。次のプロパティを持つStorageGRIDエンドポイントの URN である必要があります。</p> <ul style="list-style-type: none"> • `es` 3 番目の要素である必要があります。 • URNは、メタデータが格納されているインデックスとタイプで終わる必要があります。形式は次のようになります。 domain-name/myindex/mytype 。 <p>エンドポイントは、テナント マネージャーまたはテナント管理 API を使用して構成されます。それらは次の形式をとります:</p> <ul style="list-style-type: none"> • arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype • urn:mysite:es:::mydomain/myindex/mytype <p>構成 XML を送信する前にエンドポイントを構成する必要があります。そうしないと、404 エラーが発生して構成が失敗します。</p> <p>Urn は Destination 要素に含まれます。</p>	はい

リクエスト例

この例では、バケットの検索統合を有効にする方法を示します。この例では、すべてのオブジェクトのオブジェクト メタデータが同じ宛先に送信されます。

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

```
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-1:22222222:domain/es-
domain/graphics/videotype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

検索統合サービスによって生成されたJSON

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

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

```

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

```

メタデータ通知に含まれるオブジェクトメタデータ

この表には、検索統合が有効になっているときに宛先エンドポイントに送信される JSON ドキュメントに含まれるすべてのフィールドがリストされています。

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。

タイプ	アイテム名	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	オブジェクトキー名
バケットとオブジェクトの情報	バージョンID	オブジェクトバージョン (バージョン管理されたバケット内のオブジェクトの場合)
バケットとオブジェクトの情報	地域	バケット領域の例 us-east-1
システムメタデータ	サイズ	HTTPクライアントに表示されるオブジェクトサイズ (バイト単位)
システムメタデータ	md5	オブジェクトハッシュ
ユーザーメタデータ	メタデータ <i>key:value</i>	オブジェクトのすべてのユーザーメタデータ (キーと値のペア)

タイプ	アイテム名	説明
タグ	タグ <i>key:value</i>	オブジェクトに定義されたすべてのオブジェクトタグ（キーと値のペア）



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

関連情報

["テナントアカウントを使用する"](#)

GETストレージ使用量リクエスト

GET ストレージ使用量リクエストは、アカウントで使用されているストレージの合計量と、アカウントに関連付けられている各バケットのストレージ量を通知します。

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量は、ListBucketsリクエストを修正することで取得できます。`x-ntap-sg-usage`クエリパラメータ。バケット ストレージの使用量は、システムによって処理される PUT および 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、リクエストの処理に基づいて使用量の値が予想値と一致するまでに多少の遅延が発生する可能性があります。

デフォルトでは、StorageGRID は強力なグローバル一貫性を使用して使用状況情報を取得しようとします。強力なグローバル一貫性を実現できない場合、StorageGRID は強力なサイト一貫性で使用状況情報を取得しようとします。

この操作を完了するには、s3:ListAllMyBuckets 権限を持っているか、アカウント ルートである必要があります。

リクエスト例

```
GET /?x-ntap-sg-usage HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

応答例

この例では、2つのバケットに4つのオブジェクトと12バイトのデータがあるアカウントを示しています。各バケットには2つのオブジェクトと6バイトのデータが含まれます。

```
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

保存されたすべてのオブジェクトバージョンは、`ObjectCount`そして`DataBytes`応答内の値。削除マーカーは追加されません `ObjectCount`合計。

関連情報

"一貫性の値"

従来のコンプライアンスに対するバケット リクエストのサポート終了

従来のコンプライアンスに対するバケット リクエストのサポート終了

従来のコンプライアンス機能を使用して作成されたバケットを管理するには、StorageGRID S3 REST API を使用する必要がある場合があります。

コンプライアンス機能は廃止されました

以前のStorageGRIDバージョンで利用可能だったStorageGRIDコンプライアンス機能は廃止され、S3 オブジェクト ロックに置き換えられました。

以前にグローバルコンプライアンス設定を有効にしていた場合、StorageGRID 11.6 ではグローバル S3 オブジェクトロック設定が有効になっています。コンプライアンス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。ただし、必要に応じて、StorageGRID S3 REST API を使用して、既存のレガシーコンプライアンスバケットを管理することができます。

- ["S3 REST API を使用して S3 オブジェクトロックを設定する"](#)
- ["ILMでオブジェクトを管理する"](#)
- ["NetAppナレッジベース: StorageGRID 11.5 でレガシー準拠バケットを管理する方法"](#)

非推奨のコンプライアンス リクエスト:

- ["非推奨 - コンプライアンスのためのPUT Bucketリクエストの変更"](#)

SGCompliance XML 要素は非推奨です。以前は、PUT Bucket リクエストのオプションの XML リクエスト本文にこのStorageGRIDカスタム要素を含めることで、準拠バケットを作成できました。

- ["非推奨 - GET バケットコンプライアンス"](#)

GET Bucket コンプライアンス リクエストは非推奨です。ただし、このリクエストを引き続き使用して、既存のレガシーコンプライアンスバケットに現在有効なコンプライアンス設定を確認することはできません。

- ["非推奨 - PUT バケットのコンプライアンス"](#)

PUT Bucket コンプライアンス リクエストは非推奨です。ただし、このリクエストを引き続き使用して、既存のレガシーコンプライアンスバケットのコンプライアンス設定を変更することはできます。たとえば、既存のバケットを法的保留状態にしたり、保持期間を延長したりできます。

非推奨: コンプライアンスのための **CreateBucket** リクエストの変更

SGCompliance XML 要素は非推奨です。以前は、このStorageGRIDカスタム要素を CreateBucket リクエストのオプションの XML リクエスト本文に含めることで、準拠バケットを作成できました。



以前のStorageGRIDバージョンで利用可能だったStorageGRIDコンプライアンス機能は廃止され、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、以下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する"](#)
- ["NetAppナレッジベース: StorageGRID 11.5 でレガシー準拠バケットを管理する方法"](#)

コンプライアンス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。コンプライアンスのための CreateBucket リクエストの変更を使用して新しいコンプライアンス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.
```

非推奨: **GET** バケットコンプライアンスリクエスト

GET Bucket コンプライアンス リクエストは非推奨です。ただし、このリクエストを引き続き使用して、既存のレガシー コンプライアンス バケットに現在有効なコンプライアンス設定を確認することはできます。



以前のStorageGRIDバージョンで利用可能だったStorageGRIDコンプライアンス機能は廃止され、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、以下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する"](#)
- ["NetAppナレッジベース: StorageGRID 11.5 でレガシー準拠バケットを管理する方法"](#)

この操作を完了するには、s3:GetBucketCompliance 権限を持っているか、アカウント ルートである必要があります。

リクエスト例

この例のリクエストでは、バケットのコンプライアンス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

レスポンスXMLでは、`<SGCompliance>`バケットに有効なコンプライアンス設定を一覧表示します。このサンプル応答は、オブジェクトがグリッドに取り込まれた時点から 1 年間 (525,600 分) 各オブジェクトが保持されるバケットのコンプライアンス設定を示しています。現在、このバケットには法的保留はありません。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>
```

Name	説明
保持期間 (分)	このバケットに追加されたオブジェクトの保持期間の長さ (分)。保持期間は、オブジェクトがグリッドに取り込まれた時点で開始されます。
法的保留	<ul style="list-style-type: none"> • True: このバケットは現在、法的保留中です。このバケット内のオブジェクトは、保持期間が終了していても、法的保留が解除されるまで削除できません。 • False: このバケットは現在、法的保留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、保持期間が終了すると削除できます。
自動削除	<ul style="list-style-type: none"> • True: バケットが法的保留中でない限り、このバケット内のオブジェクトは、保持期間が終了すると自動的に削除されます。 • False: 保持期間が終了しても、このバケット内のオブジェクトは自動的に削除されません。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。

エラー応答

バケットが準拠して作成されていない場合、レスポンスのHTTPステータスコードは次のようになります。
404 Not Found S3エラーコードは XNoSuchBucketCompliance。

非推奨: **PUT** バケットコンプライアンスリクエスト

PUT Bucket コンプライアンス リクエストは非推奨です。ただし、このリクエストを引き続き使用して、既存のレガシー コンプライアンス バケットのコンプライアンス設定を変更することはできます。たとえば、既存のバケットを法的保留状態にしたり、保持期間を延長したりできます。



以前のStorageGRIDバージョンで利用可能だったStorageGRIDコンプライアンス機能は廃止され、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、以下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する"](#)
- ["NetAppナレッジベース: StorageGRID 11.5 でレガシー準拠バケットを管理する方法"](#)

この操作を完了するには、s3:PutBucketCompliance 権限を持っているか、アカウント ルートである必要があります。

PUT Bucket コンプライアンス リクエストを発行するときは、コンプライアンス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。

リクエスト例

この例のリクエストは、バケットのコンプライアンス設定を変更します。mybucket。この例では、`mybucket` オブジェクトがグリッドに取り込まれた時点から、1年間ではなく2年間(1,051,200分)保持されるようになりました。このバケットには法的拘束力はありません。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>
```

Name	説明
保持期間 (分)	<p>このバケットに追加されたオブジェクトの保持期間の長さ (分)。保持期間は、オブジェクトがグリッドに取り込まれた時点で開始されます。</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が設定されると、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>
法的保留	<ul style="list-style-type: none">• True: このバケットは現在、法的保留中です。このバケット内のオブジェクトは、保持期間が終了していても、法的保留が解除されるまで削除できません。• False: このバケットは現在、法的保留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、保持期間が終了すると削除できます。
自動削除	<ul style="list-style-type: none">• True: バケットが法的保留中でない限り、このバケット内のオブジェクトは、保持期間が終了すると自動的に削除されます。• False: 保持期間が終了しても、このバケット内のオブジェクトは自動的に削除されません。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。

コンプライアンス設定の一貫性

PUT Bucket コンプライアンス リクエストを使用して S3 バケットのコンプライアンス設定を更新すると、StorageGRID はグリッド全体で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は強力なグローバル 整合性を使用して、バケット メタデータを含むすべてのデータ センター サイトとすべてのストレージ ノードで、変更されたコンプライアンス設定に対する書き込み後の読み取り整合性が確保されることを保証します。

データセンターサイトまたはサイト内の複数のストレージノードが利用できないためにStorageGRIDが*強力なグローバル*一貫性を実現できない場合、応答のHTTPステータスコードは次のようになります。 503

Service Unavailable.

この応答を受け取った場合は、グリッド管理者に連絡して、必要なストレージ サービスができるだけ早く利用できるようにする必要があります。グリッド管理者が各サイトで十分なストレージ ノードを用意できない場合、テクニカル サポートは、*強力なサイト*の一貫性を強制して失敗した要求を再試行するように指示することがあります。



テクニカル サポートから指示された場合、またはこのレベルを使用した場合の潜在的な結果を理解していない限り、PUT バケット コンプライアンスに対して **Strong-site** の一貫性を強制しないでください。

一貫性が **Strong-site** に低下すると、StorageGRID は、更新されたコンプライアンス設定がサイト内のクライアント要求に対してのみ書き込み後の読み取り一貫性を持つことを保証します。つまり、すべてのサイトとストレージ ノードが利用可能になるまで、StorageGRIDシステムではこのバケットに対して一時的に複数の矛盾した設定が存在する可能性があります。設定に一貫性がないと、予期しない望ましくない動作が発生す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とし、一貫性を低く強制した場合、一部のデータセンター サイトではバケットの以前のコンプライアンス設定（つまり、リーガルホールドの解除）が引き続き有効になる可能性があります。その結果、法的保留中であると思われるオブジェクトは、保持期間の期限が切れると、ユーザーまたは AutoDelete（有効になっている場合）によって削除される可能性があります。

*Strong-site*一貫性の使用を強制するには、PUT Bucketコンプライアンスリクエストを再発行し、Consistency-Control HTTP リクエスト ヘッダーは次のとおりです。

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Consistency-Control: strong-site
```

エラー応答

- バケットが準備して作成されていない場合、レスポンスのHTTPステータスコードは次のようになります。404 Not Found。
- もし RetentionPeriodMinutes`リクエスト内の値がバケットの現在の保存期間より短い場合、HTTPステータスコードは `400 Bad Request。

関連情報

["非推奨: コンプライアンスのための PUT Bucket リクエストの変更"](#)

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する

StorageGRID は、Amazon Web Services (AWS) ポリシー言語を使用して、S3 テナントが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るようにします。StorageGRIDシステムは、S3 REST API ポリシー言語のサブセットを実装します。S3 API のアクセス ポリシーは JSON で記述されます。

アクセスポリシーの概要

StorageGRIDでサポートされているアクセス ポリシーには2種類あります。

- バケット ポリシー。GetBucketPolicy、PutBucketPolicy、DeleteBucketPolicy S3 API 操作、または Tenant Manager または Tenant Management API 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添付され、バケット所有者アカウントまたはその他のアカウントのユーザー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するように構成されます。バケット ポリシーは1つのバケットにのみ適用され、複数のグループに適用される場合があります。
- グループ ポリシー。これは、Tenant Manager または Tenant Management API を使用して設定されます。グループ ポリシーはアカウント内のグループに添付され、そのグループがそのアカウントが所有する特定のリソースにアクセスできるように構成されます。グループ ポリシーは1つのグループにのみ適用され、複数のバケットに適用される場合もあります。



グループ ポリシーとバケット ポリシーの優先順位に違いはありません。

StorageGRIDバケットおよびグループ ポリシーは、Amazon によって定義された特定の文法に従います。各ポリシー内にはポリシー ステートメントの配列があり、各ステートメントには次の要素が含まれています。

- ステートメントID (Sid) (オプション)
- 効果
- プリンシパル/非プリンシパル
- リソース/非リソース
- アクション/非アクション
- 条件 (オプション)

ポリシー ステートメントは、次の構造を使用して作成され、アクセス許可を指定します: <Condition> が適用される場合に、<Principal> が <Resource> に対して <Action> を実行することを許可/拒否するには、<Effect> を付与します。

各ポリシー要素は特定の機能に使用されます。

要素	説明
シド	Sid 要素はオプションです。Sid はユーザーへの説明としてのみ使用されます。これはStorageGRIDシステムによって保存されますが、解釈されません。
効果	Effect 要素を使用して、指定された操作が許可されるか拒否されるかを決定します。サポートされているアクション要素のキーワードを使用して、バケットまたはオブジェクトに対して許可 (または拒否) する操作を識別する必要があります。

要素	説明
プリンシパル/非プリンシパル	<p>ユーザー、グループ、アカウントが特定のリソースにアクセスし、特定のアクションを実行できるようにすることができます。リクエストに S3 署名が含まれていない場合は、プリンシパルとしてワイルドカード文字 (*) を指定することにより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 ルートのみがアカウントが所有するリソースにアクセスできます。</p> <p>バケット ポリシーでは、Principal 要素のみを指定する必要があります。グループ ポリシーの場合、ポリシーが関連付けられているグループは暗黙的な Principal 要素です。</p>
リソース/非リソース	リソース要素はバケットとオブジェクトを識別します。リソースを識別する Amazon リソースネーム (ARN) を使用して、バケットとオブジェクトへのアクセス許可を許可または拒否できます。
アクション/非アクション	アクション要素と効果要素は、権限の 2 つのコンポーネントです。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ない限りアクセスは拒否されますが、明示的な拒否を使用して、別のポリシーによって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、ポリシーをいつ適用するかを決定する式を作成できます。

Action 要素では、ワイルドカード文字 (*) を使用して、すべての操作または操作のサブセットを指定できます。たとえば、このアクションは、s3:GetObject、s3:PutObject、s3>DeleteObject などの権限と一致します。

```
s3:*Object
```

リソース要素では、ワイルドカード文字 (*) と (?) を使用できます。アスタリスク (*) は 0 個以上の文字に一致しますが、疑問符 (?) は任意の 1 文字に一致します。

Principal 要素では、すべてのユーザーに権限を付与する匿名アクセスを設定する場合を除き、ワイルドカード文字はサポートされていません。たとえば、ワイルドカード (*) をプリンシパル値として設定します。

```
"Principal": "*" }
```

```
"Principal": {"AWS": "*" }
```

次の例では、ステートメントは Effect、Principal、Action、および Resource 要素を使用しています。この例では、効果「許可」を使用してプリンシパル、管理者グループに権限を付与する完全なバケットポリシーステートメントを示しています。federated-group/admin`財務グループ`federated-group/finance、アクションを実行する権限`s3:ListBucket`バケットの名前`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に適用されます。

```

{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::27233906934684427525:federated-group/admin",
          "arn:aws:iam::27233906934684427525:federated-group/finance"
        ]
      },
      "Action": [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::mybucket",
        "arn:aws:s3:::mybucket/*"
      ]
    }
  ]
}

```

バケット ポリシーのサイズ制限は 20,480 バイト、グループ ポリシーのサイズ制限は 5,120 バイトです。

政策の一貫性

デフォルトでは、グループ ポリシーに加えた更新はすべて最終的に一貫性を持ちます。グループ ポリシーが整合すると、ポリシーのキャッシュにより、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 ポリシーに加えた更新はすべて強力な整合性を持ちます。

必要に応じて、バケット ポリシー更新の一貫性保証を変更できます。たとえば、サイトが停止している間もバケット ポリシーの変更を利用できるようにしたい場合があります。

この場合、Consistency-Control PutBucketPolicy リクエストのヘッダーを追加するか、PUT Bucket 一貫性リクエストを使用することもできます。バケット ポリシーが整合すると、ポリシーのキャッシュにより、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一貫性を別の値に設定する場合は、完了したらバケット レベルの設定を元の値に戻してください。それ以外の場合、今後のすべてのバケット リクエストでは変更された設定が使用されます。

ポリシーステートメントで **ARN** を使用する

ポリシーステートメントでは、ARN は Principal 要素と Resource 要素で使用されます。

- S3 リソース ARN を指定するには、次の構文を使用します。

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

- 次の構文を使用して、アイデンティティ リソース ARN (ユーザーとグループ) を指定します。

```
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:

- アスタリスク (*) をワイルドカードとして使用して、オブジェクト キー内の 0 個以上の文字を一致させることができます。
- オブジェクト キーで指定できる国際文字は、JSON UTF-8 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 URN構文"

PutBucketPolicy 操作の HTTP リクエスト本体は、charset=UTF-8 でエンコードする必要があります。

ポリシーでリソースを指定する

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またはオブジェクトを指定できます。

- 各ポリシー ステートメントには、リソース要素が必要です。ポリシーでは、リソースは要素で表されます Resource、または、`NotResource` 除外のため。
- S3 リソース ARN を使用してリソースを指定します。例えば：

```
"Resource": "arn:aws:s3:::mybucket/*"
```

- オブジェクト キー内でポリシー変数を使用することもできます。例えば：

```
"Resource": "arn:aws:s3:::mybucket/home/${aws:username}/*"
```

- リソース値には、グループ ポリシーの作成時にまだ存在しないバケットを指定できます。

ポリシーでプリンシパルを指定する

Principal 要素を使用して、ポリシー ステートメントによってリソースへのアクセスが許可/拒否されるユーザー、グループ、またはテナント アカウントを識別します。

- バケット ポリシー内の各ポリシー 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 ポリシー内のポリシー ステートメントでは、グループがプリンシパルであると認識されるため、Principal 要素は必要ありません。
- ポリシーでは、プリンシパルは要素「Principal」で示され、除外する場合は「NotPrincipal」で示されません。
- アカウントベースの ID は、ID または ARN を使用して指定する必要があります。

```
"Principal": { "AWS": "account_id" }
"Principal": { "AWS": "identity_arn" }
```

- この例では、アカウント ルートとアカウント内のすべてのユーザーを含むテナント アカウント ID 27233906934684427525 を使用します。

```
"Principal": { "AWS": "27233906934684427525" }
```

- アカウント ルートのみを指定することもできます。

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:root" }
```

- 特定のフェデレーション ユーザー (「Alex」) を指定できます。

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
user/Alex" }
```

- 特定のフェデレーション グループ (「マネージャー」) を指定できます。

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
group/Managers" }
```

- 匿名プリンシパルを指定できます。

```
"Principal": "*" 
```

- 曖昧さを避けるために、ユーザー名の代わりにユーザーの UUID を使用できます。

```
arn:aws:iam::27233906934684427525:user-uuid/de305d54-75b4-431b-adb2-
eb6b9e546013
```

例えば、アレックスが組織を離れ、ユーザー名が `Alex` 削除されます。新しいアレックスが組織に参加

し、同じ役割を担う場合 `Alex` ユーザー名を変更すると、新しいユーザーが元のユーザーに付与された権限を意図せず継承してしまう可能性があります。

- プリンシパル値には、バケット ポリシーの作成時にまだ存在しないグループ/ユーザー名を指定できません。

ポリシーで権限を指定する

ポリシーでは、アクション要素はリソースへのアクセス許可を許可/拒否するために使用されます。ポリシーで指定できる一連の権限があり、これらは要素「Action」で示され、除外の場合は「NotAction」で示されません。これらの各要素は、特定の S3 REST API 操作にマッピングされます。

表には、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がリストされています。



Amazon S3 は、PutBucketReplication アクションと DeleteBucketReplication アクションの両方に s3:PutReplicationConfiguration 権限を使用するようになりました。StorageGRID は、元の Amazon S3 仕様に一致する、アクションごとに個別の権限を使用します。



既存の値を上書きするために put が使用されると、削除が実行されます。

バケットに適用される権限

権限	S3 REST API 操作	StorageGRID向けカスタム
s3:バケットの作成	CreateBucket	○ 注: グループ ポリシーでのみ使用しません。
s3:バケットの削除	DeleteBucket	
s3>DeleteBucketMetadata通知	バケットメタデータ通知設定の削除	はい
s3>DeleteBucketポリシー	DeleteBucketPolicy	
s3:レプリケーション構成の削除	バケットレプリケーションの削除	はい、PUT とDELETEに別々の権限が必要です
s3:GetBucketAcl	GetBucketAcl	
s3:GetBucketCompliance	GET バケットコンプライアンス (非推奨)	はい
s3:GetBucketConsistency	GETバケットの一貫性	はい

権限	S3 REST API 操作	StorageGRID向けカスタム
s3:GetBucketCORS	GetBucketCors	
s3:暗号化設定の取得	バケット暗号化を取得	
s3:GetBucketLastAccessTime	GET バケットの最終アクセス時刻	はい
s3:GetBucketLocation	GetBucketLocation	
s3:GetBucketMetadataNotification	バケットメタデータ通知設定の取得	はい
s3:GetBucketNotification	GetBucketNotificationConfiguration	
s3:GetBucketObjectLockConfiguration	GetObjectLockConfiguration	
s3:GetBucketPolicy	GetBucketPolicy	
s3:GetBucketTagging	GetBucketTagging	
s3:GetBucketVersioning	GetBucketVersioning	
s3:GetLifecycleConfiguration	GetBucketLifecycleConfiguration	
s3:GetReplicationConfiguration	GetBucketReplication	
s3:すべてのバケットをリスト	<ul style="list-style-type: none"> ListBuckets ストレージ使用量の取得 	<p>はい、GET ストレージ使用量の場合です。</p> <p>注: グループポリシーでのみ使用しません。</p>
s3:リストバケット	<ul style="list-style-type: none"> ListObjects HeadBucket オブジェクトの復元 	
s3:リストバケットマルチパートアップロード	<ul style="list-style-type: none"> リストマルチパートアップロード オブジェクトの復元 	
s3:バケットバージョンのリスト	GETバケットのバージョン	

権限	S3 REST API 操作	StorageGRID向けカスタム
s3:PutBucketコンプライアンス	PUT バケットコンプライアンス (非推奨)	はい
s3:PutBucketConsistency	PUT バケットの一貫性	はい
s3:PutBucketCORS	<ul style="list-style-type: none"> バケットCorsの削除+ PutBucketCors 	
s3:PutEncryptionConfiguration	<ul style="list-style-type: none"> バケット暗号化の削除 PutBucketEncryption 	
s3:PutBucket最終アクセス時間	バケットの最終アクセス時刻をPUTする	はい
s3:PutBucketMetadataNotification	PUT バケットメタデータ通知設定	はい
s3:PutBucket通知	PutBucketNotificationConfiguration	
s3:PutBucketObjectLockConfiguration	<ul style="list-style-type: none"> CreateBucketで `x-amz-bucket-object-lock-enabled: true` リクエストヘッダー (s3:CreateBucket権限も必要) PutObjectLockConfiguration 	
s3:PutBucketポリシー	PutBucketPolicy	
s3:PutBucketTagging	<ul style="list-style-type: none"> バケットタグの削除+ PutBucketTagging 	
s3:PutBucketバージョン管理	PutBucketVersioning	
s3:PutLifecycleConfiguration	<ul style="list-style-type: none"> バケットライフサイクルの削除+ PutBucketLifecycleConfiguration 	
s3:PutReplicationConfiguration	PutBucketレプリケーション	はい、PUTとDELETEに別々の権限が必要です

オブジェクトに適用される権限

権限	S3 REST API 操作	StorageGRID向けカスタム
s3:マルチパートアップロードの中止	<ul style="list-style-type: none"> AbortMultipartUpload オブジェクトの復元 	
s3:バイパスガバナンス保持	<ul style="list-style-type: none"> DeleteObject DeleteObjects PutObjectRetention 	
s3:オブジェクトの削除	<ul style="list-style-type: none"> DeleteObject DeleteObjects オブジェクトの復元 	
s3:オブジェクトのタグ付けを削除	DeleteObjectTagging	
s3:オブジェクトバージョンタグ付けの削除	DeleteObjectTagging (オブジェクトの特定のバージョン)	
s3:オブジェクトバージョンの削除	DeleteObject (オブジェクトの特定のバージョン)	
s3:GetObject	<ul style="list-style-type: none"> GetObject HeadObject オブジェクトの復元 オブジェクトコンテンツの選択 	
s3:GetObjectAcl	GetObjectAcl	
s3:GetObjectLegalHold	GetObjectLegalHold	
s3:GetObjectRetention	GetObjectRetention	
s3:GetObjectTagging	GetObjectTagging	
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	リストパーツ、復元オブジェクト	

権限	S3 REST API 操作	StorageGRID向けカスタム
s3:PutObject	<ul style="list-style-type: none"> • PutObject • CopyObject • オブジェクトの復元 • CreateMultipartUpload • CompleteMultipartUpload • UploadPart • UploadPartCopy 	
s3:PutObjectLegalHold	PutObjectLegalHold	
s3:PutObjectRetention	PutObjectRetention	
s3:オブジェクトのタグ付け	PutObjectTagging	
s3:PutObjectVersionTagging	PutObjectTagging (オブジェクトの特定のバージョン)	
s3:上書きオブジェクト	<ul style="list-style-type: none"> • PutObject • CopyObject • PutObjectTagging • DeleteObjectTagging • CompleteMultipartUpload 	はい
s3:オブジェクトの復元	オブジェクトの復元	

PutOverwriteObject権限を使用する

s3:PutOverwriteObject 権限は、オブジェクトを作成または更新する操作に適用されるカスタムStorageGRID権限です。この権限の設定により、クライアントがオブジェクトのデータ、ユーザー定義のメタデータ、または S3 オブジェクトのタグ付けを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:

- 許可: 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。
- 拒否: クライアントはオブジェクトを上書きできません。Deny に設定すると、PutOverwriteObject 権限は次のように動作します。
 - 同じパスに既存のオブジェクトが見つかった場合:
 - オブジェクトのデータ、ユーザー定義のメタデータ、または S3 オブジェクトのタグ付けは上書きできません。
 - 進行中の取り込み操作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、Deny 設定により、PutObjectTagging または DeleteObjectTagging 操作によってオブジェクトとその非現在のバージョンの TagSet が変更されることが防止されます。

◦ 既存のオブジェクトが見つからない場合、この権限は効果がありません。

- この権限が存在しない場合は、Allow が設定されている場合と同じ効果になります。



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、クライアントはオブジェクトのデータ、ユーザー定義のメタデータ、またはオブジェクトのタグ付けを上書きできません。さらに、クライアントによる変更を禁止する チェックボックスが選択されている場合 ([構成] > [セキュリティ設定] > [ネットワークとオブジェクト])、その設定は PutOverwriteObject 権限の設定よりも優先されます。

ポリシーで条件を指定する

条件は、ポリシーがいつ有効になるかを定義します。条件は演算子とキーと値のペアで構成されます。

条件では、評価にキーと値のペアを使用します。Condition 要素には複数の条件を含めることができ、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。条件ブロックは次の形式を使用します。

```
Condition: {
  condition_type: {
    condition_key: condition_values
```

次の例では、IpAddress 条件で SourceIp 条件キーが使用されています。

```
"Condition": {
  "IpAddress": {
    "aws:SourceIp": "54.240.143.0/24"
    ...
  },
  ...
```

サポートされている条件演算子

条件演算子は次のように分類されます。

- 弦
- 数字
- ブーリアン
- IPアドレス
- ヌルチェック

条件演算子	説明
文字列に等しい	完全一致 (大文字と小文字を区別) に基づいてキーと文字列値を比較します。
文字列が等しくない	否定一致 (大文字と小文字を区別) に基づいてキーと文字列値を比較します。
文字列が等しい場合、大文字と小文字を区別しない	完全一致 (大文字と小文字は区別されません) に基づいてキーと文字列値を比較します。
文字列が等しくない場合大文字と小文字を区別しない	否定一致 (大文字と小文字を区別しない) に基づいてキーと文字列値を比較します。
文字列のような	完全一致 (大文字と小文字を区別) に基づいてキーと文字列値を比較します。* および? ワイルドカード文字を含めることができます。
文字列が似ていない	否定一致 (大文字と小文字を区別) に基づいてキーと文字列値を比較します。* および? ワイルドカード文字を含めることができます。
数値等しい	完全一致に基づいてキーと数値を比較します。
数値NotEquals	否定一致に基づいてキーと数値を比較します。
数値より大きい	「より大きい」一致に基づいてキーと数値を比較します。
数値より大きい	「以上」の一致に基づいてキーと数値を比較します。
数値の小数点以下	「より小さい」一致に基づいてキーを数値と比較します。
数値の「未満」	「以下」の一致に基づいてキーと数値を比較します。
ブール	「true または false」の一致に基づいてキーをブール値と比較します。
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。
IPアドレスなし	否定一致に基づいて、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。
Null	現在のリクエスト 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

条件キー	アクション	説明
aws:ソースIP	IPオペレーター	<p>リクエストの送信元の 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操作に使用できます。</p> <p>注: S3 リクエストが管理ノードおよびゲートウェイノードのロード バランサ サービスを通じて送信された場合、これはロード バランサ サービスのアップストリームの IP アドレスと比較されます。</p> <p>注: サードパーティの非透過ロードバランサが使用されている場合、これはそのロードバランサの IP アドレスと比較されます。どれでも `X-Forwarded-For` ヘッダーの有効性を確認できないため、無視されます。</p>
aws:ユーザー名	リソース/アイデンティティ	リクエストの送信元のユーザー名と比較します。バケットまたはオブジェクトの操作に使用できます。
s3:区切り文字	s3:ListBucketと s3:ListBucketVersions 権限	ListObjects または ListObjectVersions リクエストで指定された区切り文字パラメータと比較します。

条件キー	アクション	説明
s3:ExistingObjectTag/<タグキー>	s3:オブジェクトのタグ付けを削除 s3:オブジェクトバージョンタグ付けの削除 s3:GetObject s3:GetObjectAcl 3:オブジェクトのタグ付けを取得する s3:GetObjectVersion s3:GetObjectVersionAcl s3:GetObjectVersionTagging s3:PutObjectAcl s3:オブジェクトのタグ付け s3:PutObjectVersionAcl s3:PutObjectVersionTagging	既存のオブジェクトに特定のタグ キーと値があることが必要になります。
s3:最大キー数	s3:ListBucketと s3:ListBucketVersions 権限	ListObjects または ListObjectVersions リクエストで指定された max-keys パラメータと比較します。
s3:オブジェクトロックの残り保持日数	s3:PutObject	指定された保持期限日と比較します `x-amz-object-lock-retain-until-date` リクエスト ヘッダーまたはバケットのデフォルトの保持期間から計算され、これらの値が次のリクエストの許容範囲内であることを確認します。 <ul style="list-style-type: none"> • PutObject • CopyObject • CreateMultipartUpload
s3:オブジェクトロックの残り保持日数	s3:PutObjectRetention	PutObjectRetention リクエストで指定された retain-until-date と比較して、それが許容範囲内であることを確認します。

条件キー	アクション	説明
s3:プレフィックス	s3:ListBucketと s3:ListBucketVersions 権限	ListObjects または ListObjectVersions リクエストで指定されたプレフィックス パラメータと比較します。
s3:RequestObjectTag/<タグキー>	s3:PutObject s3:オブジェクトのタグ付け s3:PutObjectVersionTagging	オブジェクト リクエスト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する

利用可能な場合にポリシー情報を入力するには、ポリシー内の変数を使用できます。ポリシー変数は、`Resource` 要素と文字列の比較では `Condition` 要素。

この例では、変数 `\${aws:username}` リソース要素の一部です:

```
"Resource": "arn:aws:s3:::bucket-name/home/${aws:username}/*"
```

この例では、変数 `\${aws:username}` 条件ブロック内の条件値の一部です。

```
"Condition": {
  "StringLike": {
    "s3:prefix": "${aws:username}/*"
    ...
  },
  ...
}
```

変数	説明
\${aws:SourceIp}	提供された変数として SourceIp キーを使用します。
\${aws:username}	提供された変数としてユーザー名キーを使用します。
\${s3:prefix}	提供された変数としてサービス固有のプレフィックス キーを使用します。
\${s3:max-keys}	提供された変数としてサービス固有の max-keys キーを使用します。
\${*}	特殊文字。文字をリテラル * 文字として使用します。

変数	説明
<code>{?}</code>	特殊文字。文字をリテラル ? 文字として使用します。
<code>{\\$}</code>	特殊文字。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する

場合によっては、ポリシーによって、アカウントのルート ユーザーをロックアウトするなど、セキュリティ上危険な権限や継続的な操作にとって危険な権限が付与されることがあります。StorageGRID S3 REST API 実装は、ポリシー検証時には Amazon よりも制限が少なくなりますが、ポリシー評価時には同様に厳格になります。

ポリシーの説明	ポリシータイプ	アマゾンの行動	StorageGRIDの動作
ルートアカウントへのすべての権限を拒否する	バケット	有効かつ強制されていますが、ルートユーザーアカウントはすべての S3 バケットポリシー操作の権限を保持します。	同じ
ユーザー/グループへのすべての権限を拒否する	グループ	有効かつ強制	同じ
外国のアカウントグループに任意の権限を許可する	バケット	無効なプリンシパル	有効ですが、すべての S3 バケットポリシー操作の権限は、ポリシーで許可されている場合、405 メソッドが許可されていないエラーを返します。
外部アカウントのルートまたはユーザーに任意の権限を許可する	バケット	有効ですが、すべての S3 バケットポリシー操作の権限は、ポリシーで許可されている場合、405 メソッドが許可されていないエラーを返します。	同じ
すべてのアクションに対する権限を全員に許可する	バケット	有効ですが、すべての S3 バケットポリシー操作の権限は、外部アカウントのルートとユーザーに対して 405 Method Not Allowed エラーを返します。	同じ

ポリシーの説明	ポリシータイプ	アマゾンの行動	StorageGRIDの動作
すべてのアクションに対する全員の権限を拒否	バケット	有効かつ強制されていますが、ルートユーザーアカウントはすべての S3 バケットポリシー操作の権限を保持します。	同じ
プリンシパルは存在しないユーザーまたはグループです	バケット	無効なプリンシパル	有効
リソースは存在しないS3バケットです	グループ	有効	同じ
校長は地元のグループです	バケット	無効なプリンシパル	有効
ポリシーは、所有者以外のアカウント (匿名アカウントを含む) にオブジェクトを配置する権限を付与します。	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ACLを使用してオブジェクトへの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ます。バケットポリシーが適用されます。

一度書き込み、何度も読み取り可能な (**WORM**) 保護

データ、ユーザー定義のオブジェクトメタデータ、および S3 オブジェクトのタグ付けを保護するために、Write Once Read Many (WORM) バケットを作成できます。WORM バケットを構成して、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します。ここで説明するいずれかのアプローチを使用します。

上書きが常に拒否されるようにするには、次の操作を実行します。

- グリッド マネージャーから、[構成] > [セキュリティ] > [セキュリティ設定] > [ネットワークとオブジェクト] に移動し、[クライアントの変更を禁止する] チェックボックスをオンにします。
- 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 操作を追加します。
 - S3 ポリシーに DeleteObject DENY 操作を追加します。
 - S3 ポリシーに PutObject ALLOW 操作を追加します。



S3 ポリシーで DeleteObject を DENY に設定しても、「30 日後にコピーがゼロ」などのルールが存在する場合は ILM によるオブジェクトの削除を防ぐことはできません。



これらすべてのルールとポリシーを適用しても、同時書き込みを防ぐことはできません (状況 A を参照)。連続した完了上書きは防止します (状況 B を参照)。

状況A: 同時書き込み（防御されていない）

```
/mybucket/important.doc
PUT#1 ---> OK
PUT#2 -----> OK
```

状況B: 連続した完了上書き（防止対象）

```
/mybucket/important.doc
PUT#1 -----> PUT#2 ---X (denied)
```

関連情報

- ["StorageGRID ILMルールによるオブジェクトの管理方法"](#)
- ["バケットポリシーの例"](#)
- ["グループポリシーの例"](#)
- ["ILMで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 ポリシーを構築します。

バケット ポリシーは、ポリシーが添付されているバケットのアクセス権限を指定します。バケットポリシーは、次のいずれかのツールを通じて S3 PutBucketPolicy API を使用して設定します。

- ["Tenant Manager"](#)。
- このコマンドを使用するAWS CLI（参照["バケットの操作"](#)）:

```
> aws s3api put-bucket-policy --bucket examplebucket --policy
file://policy.json
```

例: すべてのユーザー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、匿名ユーザーを含むすべてのユーザーがバケット内のオブジェクトを一覧表示し、バケット内のすべてのオブジェクトに対して GetObject 操作を実行できます。その他の操作はすべて拒否されます。アカウント ルート以外のユーザーにはバケットへの書き込み権限がないため、このポリシーは特に役に立たない可能性があることに注意してください。

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadOnlyAccess",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:GetObject", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket", "arn:aws:s3:::examplebucket/*"]
    }
  ]
}
```

例: あるアカウントの全員にバケットへのフルアクセスを許可し、別のアカウントの全員に読み取り専用アクセスを許可する

この例では、指定された1つのアカウントの全員にバケットへのフルアクセスが許可されていますが、指定された別のアカウントの全員にはバケットの一覧表示と、バケット内の先頭のオブジェクトに対するGetObject操作の実行のみが許可されています。`shared/`オブジェクト キーのプレフィックス。



StorageGRIDでは、所有者以外のアカウント (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は、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 ポリシーはこれらのオブジェクトに適用されます。

```

{
  "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: バケットへの読み取り専用アクセスを全員に許可し、指定されたグループにはフルアクセスを許可する

この例では、匿名ユーザーを含むすべてのユーザーがバケットの一覧を表示し、バケット内のすべてのオブジェクトに対してGetObject操作を実行できますが、グループに属するユーザーのみが `Marketing` 指定されたアカウントのユーザーにはフルアクセスが許可されます。

```

{
  "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: IP範囲内のクライアントにバケットへの読み取りと書き込みアクセスを許可する

この例では、リクエストが指定された IP 範囲 (54.240.143.0 ~ 54.240.143.255、54.240.143.188 を除く) から送信された場合、匿名ユーザーを含むすべてのユーザーがバケットを一覧表示し、バケット内のすべてのオブジェクトに対して任意のオブジェクト操作を実行できます。その他のすべての操作は拒否され、IP 範囲外のすべての要求は拒否されます。

```
{
  "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: 指定されたフェデレーションユーザーのみがバケットにフルアクセスできるようにする

この例では、フェデレーションユーザーAlexは、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ーは、すべての操作が明示的に拒否されます。ただし、`root`にはPut/Get/DeleteBucketPolicy へのアクセス許可が拒否されることはないことに注意してください。

```

{
  "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、Deny PutOverwriteObject および DeleteObject の効果により、オブジェクトのデータ、ユーザー定義のメタデータ、および S3 オブジェクトのタグ付けを誰も上書きまたは削除できないようになります。

```

{
  "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 ポリシーを構築します。

グループ ポリシーは、ポリシーが関連付けられているグループのアクセス権限を指定します。ありません `Principal` 暗黙的であるため、ポリシーの要素ではありません。グループ ポリシーは、テナント マネージャー または API を使用して構成されます。

例: テナント マネージャーを使用してグループ ポリシーを設定する

テナント マネージャー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 アクセス権を決定できます。見る["S3テナントのグループを作成する"](#)。

- **S3 アクセスなし:** デフォルト オプション。このグループのユーザーは、バケットポリシーでアクセスが許可されない限り、S3 リソースにアクセスできません。このオプションを選択すると、デフォルトではルートユーザーのみが S3 リソースにアクセスできるようになります。
- **読み取り専用アクセス:** このグループのユーザーには、S3 リソースへの読み取り専用アクセス権があります。たとえば、このグループのユーザーはオブジェクトを一覧表示したり、オブジェクトのデータ、メタデータ、タグを読み取ったりできます。このオプションを選択すると、読み取り専用グループ ポリシーの JSON 文字列がテキスト ボックスに表示されます。この文字列は編集できません。
- **フルアクセス:** このグループのユーザーには、バケットを含む S3 リソースへのフルアクセス権があります。このオプションを選択すると、フルアクセス グループ ポリシーの JSON 文字列がテキスト ボックスに表示されます。この文字列は編集できません。
- **ランサムウェア軽減:** 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に適用されます。このグループのユーザーは一般的なアクションを実行できますが、オブジェクトのバージョン管理が有効になっているバケットからオブジェクトを完全に削除することはできません。

すべてのバケットの管理権限を持つテナント マネージャー ユーザーは、このグループ ポリシーを上書きできます。すべてのバケットの管理権限を信頼できるユーザーに制限し、可能な場合は多要素認証 (MFA) を使用します。

- **カスタム:** グループ内のユーザーには、テキスト ボックスで指定した権限が付与されます。

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 ポリシーによって明示的に拒否されない限り、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: すべてのバケットへのグループ読み取り専用アクセスを許可する

この例では、バケット ポリシーによって明示的に拒否されない限り、グループのすべてのメンバーは S3 リソースへの読み取り専用アクセス権を持ちます。たとえば、このグループのユーザーはオブジェクトを一覧表示したり、オブジェクトのデータ、メタデータ、タグを読み取ったりできます。

```
{
  "Statement": [
    {
      "Sid": "AllowGroupReadOnlyAccess",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

例: グループメンバーにバケット内の自分の「フォルダ」のみへのフルアクセスを許可する

この例では、グループのメンバーは、指定されたバケット内の特定のフォルダー (キー プレフィックス) の一覧表示とアクセスのみが許可されます。これらのフォルダーのプライバシーを決定する際には、他のグループポリシーとバケット ポリシーからのアクセス権限を考慮する必要があることに注意してください。

```

{
  "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操作

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 ログ ファイルに保存されます。監査ログで S3 固有の監査メッセージを確認して、バケットおよびオブジェクトの操作に関する詳細を取得できます。

監査ログで追跡されるバケット操作

- CreateBucket
- DeleteBucket
- バケットタグの削除
- DeleteObjects
- GetBucketTagging
- HeadBucket
- ListObjects
- ListObjectVersions
- PUTバケットコンプライアンス
- PutBucketTagging
- PutBucketVersioning

監査ログで追跡されるオブジェクト操作

- CompleteMultipartUpload
- CopyObject
- DeleteObject
- GetObject
- HeadObject
- PutObject
- オブジェクトの復元
- オブジェクトを選択
- UploadPart (ILM ルールが Balanced または Strict の取り込みを使用する場合)
- UploadPartCopy (ILM ルールが Balanced または Strict の取り込みを使用する場合)

関連情報

- ["アクセス監査ログファイル"](#)
- ["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 を使用する（サポート終了）

Swift REST APIを使用する

Swift API のサポートは終了しており、将来のリリースでは削除されます。



このバージョンのドキュメント サイトから Swift の詳細は削除されました。見る ["StorageGRID 11.8: Swift REST API を使用する"](#)。

著作権に関する情報

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

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

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

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

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

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

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

商標に関する情報

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