



StorageGRID を使用します

StorageGRID

NetApp
October 03, 2025

目次

StorageGRID を使用します	1
テナントアカウントを使用する	1
Tenant Managerを使用します	1
テナントユーザのシステムアクセスの管理	16
S3テナントアカウントの管理	38
S3プラットフォームサービスの管理	67
S3 を使用する	109
S3 REST APIのサポート	109
テナントアカウントと接続を設定する	114
StorageGRID でのS3 REST APIの実装	119
S3 REST API のサポートされる処理と制限事項	127
StorageGRID の S3 REST API の処理	178
バケットとグループのアクセスポリシー	200
REST APIのセキュリティの設定	226
処理の監視と監査	229
アクティブ、アイドル、および同時 HTTP 接続のメリット	232
Swift を使用します	235
StorageGRID でのOpenStack Swift APIのサポート	235
テナントアカウントと接続を設定する	239
Swift REST API でサポートされている処理	244
StorageGRID の Swift REST API 処理	256
REST APIのセキュリティの設定	261
処理の監視と監査	264

StorageGRID を使用します

テナントアカウントを使用する

StorageGRID テナントアカウントの使用方法について説明します。

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

Tenant Managerを使用します

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

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

StorageGRID テナントアカウントを使用する

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

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

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

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



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

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

テナントアカウントの作成

テナントアカウントは、StorageGRID のグリッド管理者がグリッドマネージャを使用して作成します。グリ

ッド管理者は、テナントアカウントを作成する際に次の情報を指定します。

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

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

S3テナントを設定する

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

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



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

Swiftテナントを設定します

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

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



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

関連情報

["StorageGRID の管理"](#)

["S3 を使用する"](#)

["Swift を使用します"](#)

Web ブラウザの要件

サポートされている Web ブラウザを使用する必要があります。

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

ブラウザウィンドウの幅を推奨される値に設定してください。

ブラウザの幅	ピクセル
最小 (Minimum)	1024
最適	1280

Tenant Managerにサインインします

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

必要なもの

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

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

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

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

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

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

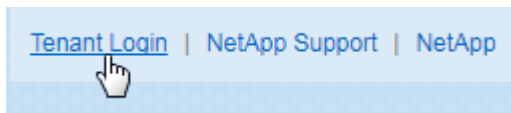
- URL に 20 桁のテナントアカウント ID が含まれていない場合は、このアカウント ID を確認しておく必要があります。
- サポートされている Web ブラウザを使用する必要があります。
- Web ブラウザでクッキーが有効になっている必要があります。
- 特定のアクセス権限が必要です。

手順

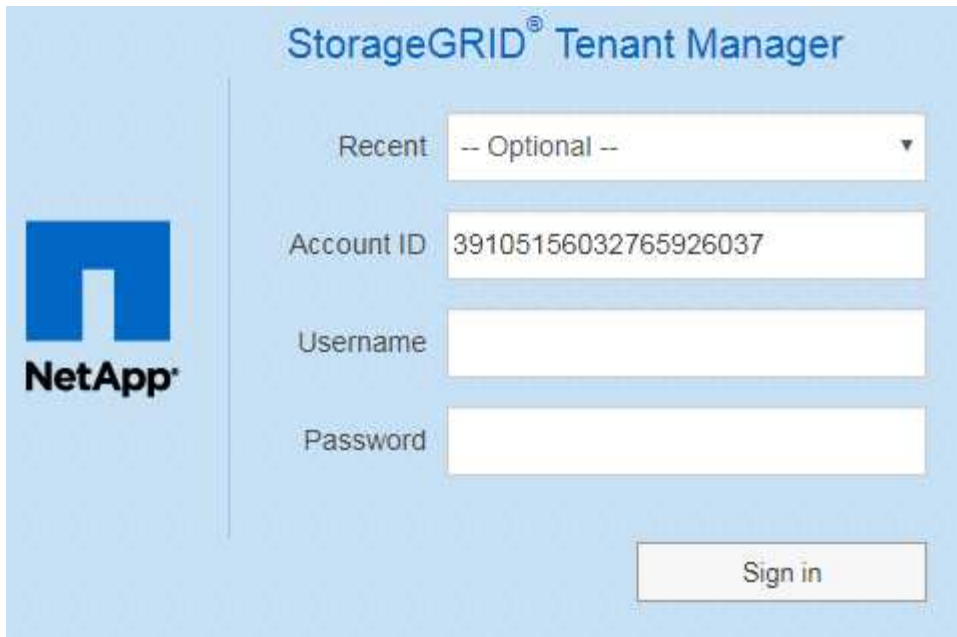
1. サポートされている Web ブラウザを起動します。
2. ブラウザのアドレスバーに、Tenant Manager にアクセスするための URL を入力します。
3. セキュリティアラートが表示された場合は、ブラウザのインストールウィザードを使用して証明書をインストールします。
4. Tenant Manager にサインインします。

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

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



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

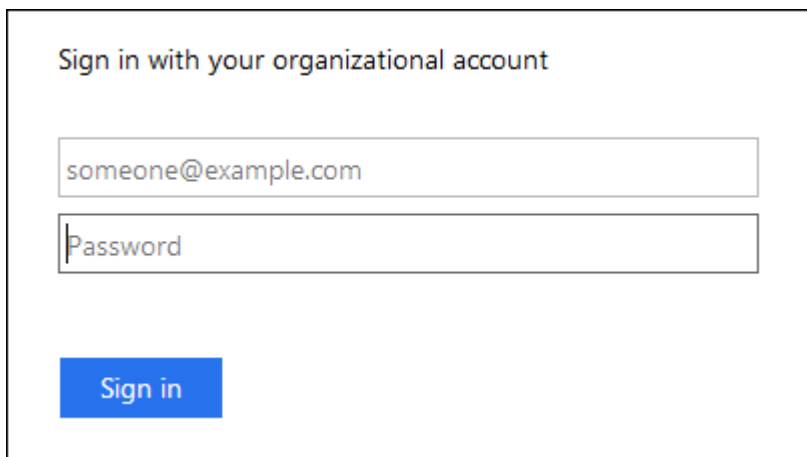


The image shows the StorageGRID Tenant Manager login page. On the left is the NetApp logo. The main area has a light blue background. At the top, it says 'StorageGRID® Tenant Manager'. Below this, there is a 'Recent' dropdown menu with '-- Optional --' selected. Underneath are three input fields: 'Account ID' with the value '39105156032765926037', 'Username', and 'Password'. At the bottom right is a 'Sign in' button.

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

Tenant Manager のダッシュボードが表示されます。

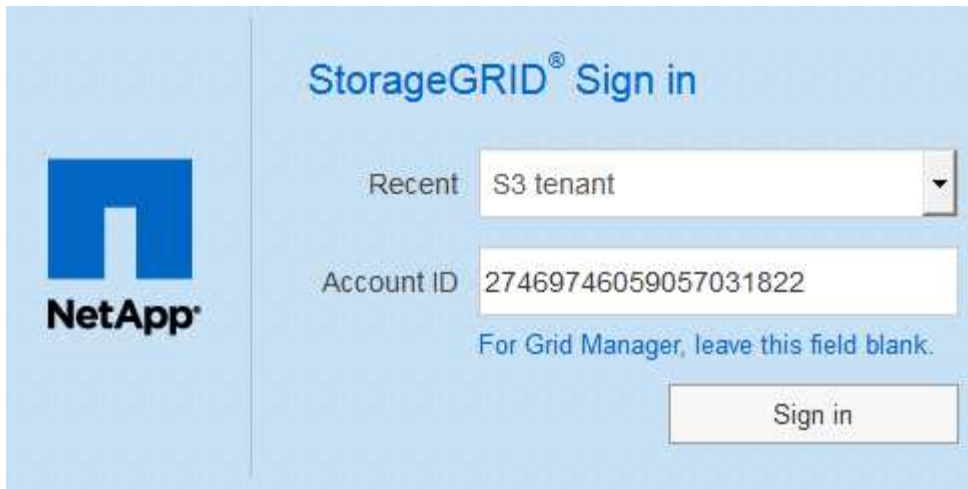
- グリッドで SSO が有効になっている場合は、組織の SSO ページ。例：



The image shows an example of an organizational SSO login form. It has a title 'Sign in with your organizational account'. Below the title are two input fields: the first contains 'someone@example.com' and the second is labeled 'Password'. At the bottom left is a blue 'Sign in' button.

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

- Tenant Manager の SSO サインインページ。

The image shows the StorageGRID Sign in page. On the left is the NetApp logo. The main area has the title "StorageGRID® Sign in". Below it, there is a "Recent" dropdown menu showing "S3 tenant". Below that is an "Account ID" field containing the text "27469746059057031822". A note below the field says "For Grid Manager, leave this field blank." At the bottom right is a "Sign in" button.

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

Tenant Manager のダッシュボードが表示されます。

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



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

関連情報

["StorageGRID の管理"](#)

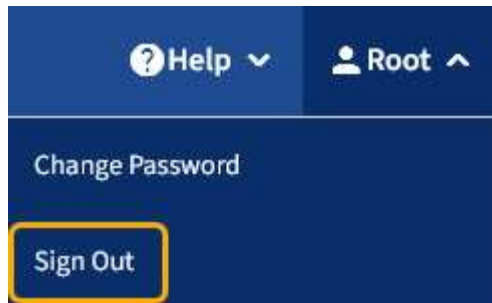
["Web ブラウザの要件"](#)

Tenant Managerからサインアウトします

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

手順

1. ユーザインターフェイスの右上にあるユーザ名ドロップダウンを探します。



2. ユーザー名を選択し、* サインアウト * を選択します。

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

Tenant Managerのダッシュボードについて

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



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

オブジェクトがアップロードされると、ダッシュボードは次のようになります。

Dashboard

16

Buckets

[View buckets](#)

2

Platform services
endpoints

[View endpoints](#)

0

Groups

[View groups](#)

1

User

[View users](#)

Storage usage [?](#)

6.5 TB of 7.2 TB used

0.7 TB (10.1%) remaining



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

Total objects

8,418,886
objects

Tenant details

Name Human Resources
ID 4955 9096 9804 4285 4354

View the instructions for Tenant Manager.

[Go to documentation](#) [↗](#)

テナントアカウントの概要

ダッシュボードの上部には、次の情報が表示されます。

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

リンクを選択すると詳細を確認できます。

ダッシュボードの右側には、次の情報が表示されます。

- テナントのオブジェクトの合計数。

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

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

ストレージとクォータの使用状況

ストレージ使用状況パネルには、次の情報が表示されます。

- テナントのオブジェクトデータの量。



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

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












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

- 最大のバケットまたはコンテナの相対サイズを表す棒グラフ。

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



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

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

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


クォータ使用状況アラート

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

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

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

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


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



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

エンドポイントエラー

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

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

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

関連情報

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

["トラブルシューティングを監視します"](#)

テナント管理APIについて

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

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

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

手順

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

API 処理

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

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

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

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



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

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

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

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

ナントグループを取得するための処理。

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

処理の詳細

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

groups
Operations on groups

GET
/org/groups
Lists Tenant User Groups

Parameters
Try it out

Name	Description
type 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	<div> Example Value Model </div> <pre>{ "responseTime": "2018-02-01T16:22:31.066Z", "status": "success", "apiVersion": "2.1" }</pre>

API要求の実行



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

手順

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

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

関連情報

["クロスサイトリクエストフォージェリ \(CSRF\) の防止"](#)

["StorageGRID の管理"](#)

テナント管理 API のバージョン管理

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

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

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

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

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

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

古い要求は、次の方法で廃止とマークされます。

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

現在のリリースでサポートされているAPIバージョンを確認します

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


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

要求のAPIバージョンの指定

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

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

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

クロスサイトリクエストフォージェリ (CSRF) の防止

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

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

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

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

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

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

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

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

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



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

テナントユーザのシステムアクセスの管理

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

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

アイデンティティフェデレーションを使用する

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

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

フェデレーテッドアイデンティティソースを設定する

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

必要なもの

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

- 特定のアクセス権限が必要です。
- アイデンティティプロバイダとしてActive Directory、OpenLDAP、またはOracle Directory Serverを使用している必要があります。記載されていないLDAP v3サービスを使用する場合は、テクニカルサポートにお問い合わせください。
- LDAP サーバとの通信に Transport Layer Security （ TLS ）を使用する場合は、アイデンティティプロバイダが TLS 1.2 または 1.3 を使用している必要があります。

このタスクについて

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



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

手順

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

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

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

4. [* その他 *] を選択した場合は、[LDAP 属性] セクションのフィールドに入力します。
 - * User Unique Name * : LDAP ユーザの一意的な ID が含まれている属性の名前。この属性はと同じです sAMAccountName Active Directoryおよびの場合 uid OpenLDAPの場合。Oracle Directory Serverを設定する場合は、と入力します uid。
 - * User UUID * : LDAP ユーザの永続的な一意な ID が含まれている属性の名前。この属性はと同じです objectGUID Active Directoryおよびの場合 entryUUID OpenLDAPの場合。Oracle Directory Serverを設定する場合は、と入力します nsuniqueid。指定した属性の各ユーザの値は、16 バイトまたは文字列形式の 32 桁の 16 進数である必要があります。ハイフンは無視されます。
 - * Group Unique name * : LDAPグループの一意的なIDが含まれている属性の名前。この属性はと同じです sAMAccountName Active Directoryおよびの場合 cn OpenLDAPの場合。Oracle Directory Serverを設定する場合は、と入力します cn。
 - * グループ UUID * : LDAP グループの永続的な一意な ID が含まれている属性の名前。この属性はと同じです objectGUID Active Directoryおよびの場合 entryUUID OpenLDAPの場合。Oracle Directory Serverを設定する場合は、と入力します nsuniqueid。指定した属性の各グループの値は、16 バイトまたは文字列形式の 32 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. Configure LDAP server (LDAPサーバの設定) セクションで、必要なLDAPサーバおよびネットワーク接続情報を入力します。
 - * Hostname * : LDAPサーバのホスト名またはIPアドレス。

- *** Port *** : LDAP サーバへの接続に使用するポート。STARTTLS のデフォルトポートは 389、LDAPS のデフォルトポートは 636 です。ただし、ファイアウォールが正しく設定されていれば、任意のポートを使用できます。
- *** Username *** : LDAP サーバに接続するユーザの識別名 (DN) の完全パス。Active Directory の場合は、ダウンレベルログオン名またはユーザープリンシパル名を指定することもできます。

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

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

- *** Password *** : ユーザ名に関連付けられたパスワード。
- *** Group base DN *** : グループを検索するLDAPサブツリーの識別名 (DN) の完全パス。Active Directory では、ベース DN に対して相対的な識別名 (DC=storagegrid、DC=example、DC=com など) のグループをすべてフェデレーテッドグループとして使用できます。

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

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

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

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

- *** STARTTLSを使用 (推奨) *** : STARTTLSを使用してLDAPサーバとの通信を保護します。これが推奨されるオプションです。
- *** LDAPS を使用 *** : LDAPS (LDAP over SSL) オプションでは、TLS を使用して LDAP サーバへの接続を確立します。このオプションは互換性を確保するためにサポートされています。
- *** TLS を使用しないでください *** : StorageGRID システムと LDAP サーバの間のネットワークトラフィックは保護されません。

Active DirectoryサーバでLDAP署名を適用する場合は、このオプションはサポートされていません。STARTTLS または LDAPS を使用する必要があります。

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

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

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

8. 「接続のテスト」を選択して、LDAPサーバーの接続設定を検証します。

接続が有効な場合は、ページの右上に確認メッセージが表示されます。

9. 接続が有効な場合は、*保存*を選択します。

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

LDAP service type

Select the type of LDAP service you want to configure.

Active Directory

OpenLDAP

Other

Configure LDAP server (All fields are required)

Hostname

my-active-directory.example.com

Port

389

Username

MyDomain\Administrator

Password

●●●●●●●●

Group Base DN

DC=storagegrid,DC=example,DC=com

User Base DN

DC=storagegrid,DC=example,DC=com

関連情報

["テナント管理権限"](#)

["OpenLDAP サーバの設定に関するガイドライン"](#)

OpenLDAP サーバの設定に関するガイドライン

アイデンティティフェデレーションに OpenLDAP サーバを使用する場合は、

OpenLDAP サーバで特定の設定が必要です。

memberof オーバーレイと refint オーバーレイ

memberof オーバーレイと refint オーバーレイを有効にする必要があります。詳細については、OpenLDAPの管理者ガイドのリバースグループメンバーシップのメンテナンス手順を参照してください。

インデックス作成

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

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

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

OpenLDAPの管理者ガイドのリバースグループメンバーシップのメンテナンスに関する情報を参照してください。

アイデンティティソースとの強制同期

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

必要なもの

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

手順

1. アクセス管理 * > * アイデンティティフェデレーション * を選択します。

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



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

2. 「サーバーの同期」を選択します。

同期が開始されたことを示す確認メッセージが表示されます。

関連情報

"テナント管理権限"

アイデンティティフェデレーションの無効化

このテナントにアイデンティティフェデレーションサービスを設定した場合は、テナントグループとユーザのアイデンティティフェデレーションを一時的または永続的に無効にすることができます。アイデンティティフェデレーションを無効にすると、StorageGRID システムとアイデンティティソース間のやり取りは発生しません。ただし、設定は保持されるため、簡単に再度有効にすることができます。

必要なもの

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

このタスクについて

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

- フェデレーテッドユーザはサインインできなくなります。
- 現在サインインしているフェデレーテッドユーザは、セッションが有効な間はテナントアカウントにアクセスしたままとなりますが、セッションが期限切れになると以降はサインインできなくなります。
- StorageGRID システムとアイデンティティソース間の同期は行われません。

手順

1. アクセス管理 * > * アイデンティティフェデレーション * を選択します。
2. [アイデンティティフェデレーションを有効にする] チェックボックスをオフにします。
3. [保存 (Save)] を選択します。

関連情報

"テナント管理権限"

グループの管理

テナントユーザが実行できるタスクを制御するには、ユーザグループに権限を割り当てます。Active Directory や OpenLDAP などのアイデンティティソースからフェデレーテッドグループをインポートすることも、ローカルグループを作成することもできます。



StorageGRID システムでシングルサインオン (SSO) が有効になっている場合、ローカルユーザはテナントマネージャにサインインできません。ただし、グループの権限に基づいて S3 リソースと Swift リソースにアクセスすることはできます。

テナント管理権限

テナントグループを作成する前に、そのグループに割り当てる権限を検討してください。テナント管理権限は、Tenant Manager またはテナント管理 API を使用してユーザが実行できるタスクを決定します。ユーザは 1 つ以上のグループに属することができます。権限は、ユーザが複数のグループに属している場合に累積されます。

Tenant Manager にサインインするには、またはテナント管理 API を使用するには、少なくとも 1 つの権限が割り当てられたグループにユーザが属している必要があります。サインインできるすべてのユーザは、次のタスクを実行できます。

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

すべての権限について、グループのアクセスモード設定によって、ユーザが設定を変更して処理を実行できるかどうか、またはユーザが関連する設定と機能のみを表示できるかどうかが決まります。



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

グループには次の権限を割り当てることができます。S3 テナントと Swift テナントではグループの権限が異なるので注意してください。キャッシングに時間がかかるため変更には最大で 15 分を要します。

アクセス権	説明
ルートアクセス（Root Access）	Tenant Manager とテナント管理 API へのフルアクセスを提供します。 • 注： * Swift ユーザがテナントアカウントにサインインするには、Root Access 権限が必要です。
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 • 注： * Swift ユーザが Swift REST API を使用して処理を実行するには、Swift 管理者の権限が必要です。
自分の S3 クレデンシャルを管理します	S3 テナントのみ。ユーザに自分の S3 アクセスキーの作成および削除を許可します。この権限を持たないユーザには、「 * storage （ S3 ） * > * My S3 access keys * 」メニューオプションは表示されません。
すべてのバケットを管理します	 • S3 テナント： S3 のバケットまたはグループポリシーに関係なく、ユーザに Tenant Manager とテナント管理 API を使用して S3 バケットの作成と削除を許可し、テナントアカウント内のすべての S3 バケットの設定を管理することを許可します。 この権限を持たないユーザには、 Bucket メニューオプションは表示されません。 • Swift テナント： Swift ユーザにテナント管理 API を使用して Swift コンテナの整合性レベルを制御することを許可します。 • 注： * テナント管理 API から Swift グループに割り当てることができるのは、Manage All Buckets 権限だけです。この権限は、Tenant Manager を使用して Swift グループに割り当てることはできません。

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

関連情報

["S3 を使用する"](#)

["Swift を使用します"](#)

S3テナント用のグループの作成

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

必要なもの

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

手順

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



2. 「* グループを作成 *」を選択します。

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

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

4. グループの名前を入力します。

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

5. 「* Continue *」を選択します。

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

- * Read-Write * (デフォルト) : ユーザは Tenant Manager にログインしてテナントの設定を管理できます。
- * 読み取り専用 * : ユーザーは設定と機能のみを表示できます。Tenant Manager またはテナント管理 API では、変更や処理を実行することはできません。ローカルの読み取り専用ユーザは自分のパスワードを変更できます。

7. このグループのグループ権限を選択します。

テナント管理権限に関する情報を参照してください。

8. 「* Continue *」を選択します。

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

- * S3 アクセスなし * : デフォルト。バケットポリシーでアクセスが許可されていないかぎり、このグループのユーザは S3 リソースにアクセスできません。このオプションを選択すると、デフォルトでは root ユーザにのみ S3 リソースへのアクセスが許可されます。
- * 読み取り専用アクセス * : このグループのユーザには、S3 リソースへの読み取り専用アクセスが許可されます。たとえば、オブジェクトをリストして、オブジェクトデータ、メタデータ、タグを読み取ることができます。このオプションを選択すると、テキストボックスに読み取り専用グループポリシーの JSON 文字列が表示されます。この文字列は編集できません。
- * フルアクセス * : このグループのユーザには、バケットを含む S3 リソースへのフルアクセスが許可されます。このオプションを選択すると、テキストボックスにフルアクセスグループポリシーの JSON 文字列が表示されます。この文字列は編集できません。
- * カスタム * : グループ内のユーザーには、テキストボックスで指定した権限が付与されます。言語の構文や例など、グループポリシーの詳細については、S3 クライアントアプリケーションを実装する手順を参照してください。

10. 「* Custom *」を選択した場合は、グループポリシーを入力します。各グループポリシーのサイズは 5、120 バイトまでに制限されています。有効な JSON 形式の文字列を入力する必要があります。

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

☐ No S3 Access
 ☐ Read Only Access
 ☐ Full Access
 ☒ Custom
(Must be a valid JSON formatted string.)

```

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

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

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

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

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

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

13. [完了] を選択します。

作成したグループがグループのリストに表示されます。キャッシングに時間がかかるため変更には最大で 15 分を要します。

関連情報

["テナント管理権限"](#)

["S3 を使用する"](#)

Swift テナント用のグループの作成

Swift テナントアカウントに対するアクセス権限を管理するには、フェデレーテッドグル

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

必要なもの

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

手順

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

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

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

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

4. グループの名前を入力します。
 - * ローカルグループ * : 表示名と一意の名前の両方を入力します。表示名はあとで編集できます。
 - * フェデレーショングループ * : 一意の名前を入力します。Active Directoryの場合、に関連付けられている一意の名前です sAMAccountName 属性 (Attribute) : OpenLDAPの場合は、に関連付けられている一意の名前です uid 属性 (Attribute) :
5. 「* Continue *」を選択します。
6. アクセスモードを選択します。ユーザが複数のグループに属していて、いずれかのグループが読み取り専

用に設定されている場合、選択したすべての設定と機能に読み取り専用でアクセスできます。

- * Read-Write *（デフォルト）：ユーザは Tenant Manager にログインしてテナントの設定を管理できます。
- * 読み取り専用 *：ユーザーは設定と機能のみを表示できます。Tenant Manager またはテナント管理 API では、変更や処理を実行することはできません。ローカルの読み取り専用ユーザは自分のパスワードを変更できます。

7. グループ権限を設定します。

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

8. 「* Continue *」を選択します。

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

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

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

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

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

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

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

12. [完了] を選択します。

作成したグループがグループのリストに表示されます。キャッシングに時間がかかるため変更には最大で 15 分を要します。

関連情報

["テナント管理権限"](#)

["Swift を使用します"](#)

グループの詳細を表示および編集する

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

必要なもの

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

手順

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

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

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

Overview

Display name:	Applications 
Unique name:	group/Applications
Type:	Local
Access mode:	Read-write
Permissions:	Root Access
S3 Policy:	None
Number of users in this group:	0

Group permissions

S3 group policy

Users

Manage group permissions

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

Access mode

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

☒ Read-write ☐ Read-only

Group permissions

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

☒ **Root Access**

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

☒ **Manage All Buckets**

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

☒ **Manage Endpoints**

Allows users to configure endpoints for platform services.

☒ **Manage Your Own S3 Credentials**

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

Save changes

3. 必要に応じてグループ設定を変更します。



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

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

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

- b. 必要に応じて、権限を更新します。

- c. グループポリシーの場合は、S3 または Swift テナントに適した変更を行います。

- S3 テナントのグループを編集する場合は、必要に応じて別の S3 グループポリシーを選択します。カスタムの S3 ポリシーを選択した場合は、JSON 文字列を必要に応じて更新します。
- Swift テナントのグループを編集する場合は、必要に応じて、* Swift Administrator * チェックボックスをオンまたはオフにします。

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

- d. 必要に応じて、ユーザを追加または削除します。

4. 変更したセクションごとに「変更を保存」を選択したことを確認します。

キャッシングに時間がかかるため変更には最大で 15 分を要します。

関連情報

["S3テナント用のグループの作成"](#)

["Swiftテナント用のグループの作成"](#)

ローカルグループへのユーザの追加

必要に応じて、ローカルグループにユーザを追加できます。

必要なもの

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

手順

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

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

グループの詳細ページが表示されます。

Overview

Display name:	Applications 
Unique name:	group/Applications
Type:	Local
Access mode:	Read-write
Permissions:	Root Access
S3 Policy:	None
Number of users in this group:	0

Group permissions

S3 group policy

Users

Manage group permissions

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

Access mode

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

☒ Read-write ☐ Read-only

Group permissions

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

☒ **Root Access**

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

☒ **Manage All Buckets**

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

☒ **Manage Endpoints**

Allows users to configure endpoints for platform services.

☒ **Manage Your Own S3 Credentials**

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

Save changes

3. 「ユーザーの管理」を選択し、「ユーザーの追加」を選択します。

Manage users

You can add users to this group or remove users from this group.

Add users **Remove Users** Search Groups... Displaying 1 results

Username	Full Name	Denied
User_02	User_02_Managers	

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

Add users ×

Select local users to add to the group **Applications**.

Search Groups... Displaying 1 results

<input checked="" type="checkbox"/>	Username	Full Name	Denied
<input checked="" type="checkbox"/>	User_01	User_01_Applications	

Cancel **Add users**

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

グループ名を編集する

グループの表示名を編集できます。グループの一意の名前は編集できません。

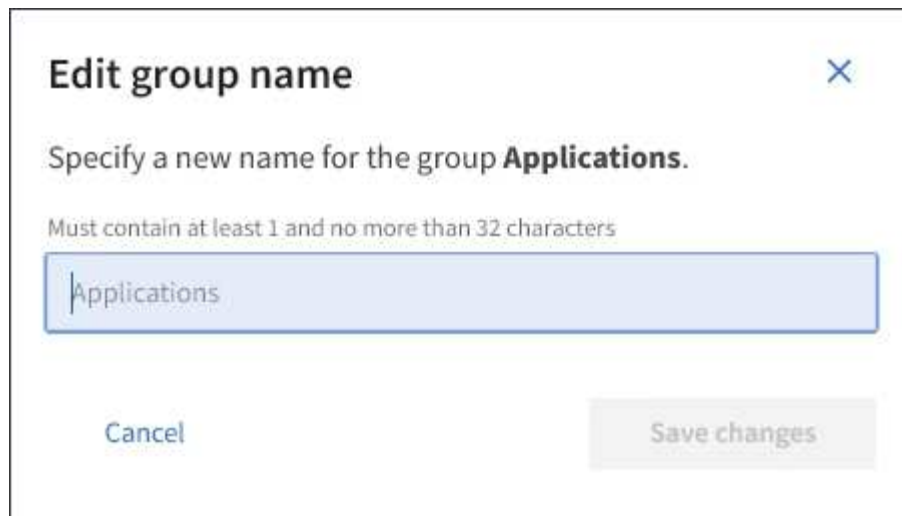
必要なもの

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

手順

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

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



- ローカルグループを編集する場合は、必要に応じて表示名を更新します。

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

- 「変更を保存」を選択します。

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

関連情報

"テナント管理権限"

グループを複製する

既存のグループを複製することで、新しいグループをより迅速に作成できます。

必要なもの

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

手順

- * access management * > * Groups * を選択します。
- 複製するグループのチェックボックスをオンにします。
- 「* グループを複製 *」を選択します。グループの作成の詳細については、S3テナントまたはSwiftテナントのグループを作成する手順を参照してください。
- [ローカルグループ *] タブを選択してローカルグループを作成するか、または [フェデレーショングループ *] タブを選択して、以前に設定したアイデンティティソースからグループをインポートします。

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

- グループの名前を入力します。

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

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

関連情報

["S3テナント用のグループの作成"](#)

["Swiftテナント用のグループの作成"](#)

["テナント管理権限"](#)

グループを削除しています

システムからグループを削除できます。そのグループに属するユーザは、Tenant Manager にサインインしたりテナントアカウントを使用したりすることはできなくなります。

必要なもの

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

手順

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

Groups

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

2 groups Create group

Actions

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

Previous **1** Next

- 削除するグループのチェックボックスを選択します。
- [* アクション * > * グループの削除 *] を選択します。

確認メッセージが表示されます。

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

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

関連情報

["テナント管理権限"](#)

ローカルユーザの管理

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

必要なもの

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



StorageGRID システムでシングルサインオン（SSO）が有効になっている場合、ローカルユーザはテナントマネージャまたはテナント管理 API にサインインできません。ただし、グループの権限に基づいて、S3 または Swift クライアントアプリケーションを使用してテナントのリソースにアクセスすることはできます。

Usersページへのアクセス

アクセス管理 * > * Users * を選択します。

Users

View local and federated users. Edit properties and group membership of local users.

3 users Create user

Actions ▾

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

ローカルユーザを作成しています

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

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

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

手順

1. 「* ユーザーの作成 *」を選択します。
2. 次のフィールドに値を入力します。
 - * フルネーム * : このユーザのフルネーム。たとえば、ユーザの名と姓、またはアプリケーションの名前です。
 - * ユーザ名 * : このユーザがサインインに使用する名前。ユーザ名は一意である必要があり、変更できません。
 - * Password * : ユーザがサインイン時に使用するパスワード。
 - * パスワードの確認 * : [パスワード] フィールドに入力したパスワードと同じパスワードを入力します。

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

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

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

グループに属していないユーザには管理権限は付与されません。アクセス許可は累積的に追加されユーザには、自身が属しているすべてのグループに対するすべての権限が与えられます。

5. 「* ユーザーの作成 *」を選択します。

キャッシングに時間がかかるため変更には最大で 15 分を要します。

ユーザの詳細を編集する


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

手順

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

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

2. 必要に応じてユーザ設定を変更します。

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

ユーザ名は変更できません。

- b. [パスワード *] タブで、必要に応じてユーザーのパスワードを変更します。
- c. [* アクセス *] タブで、ユーザーがサインインすることを許可するか（[* いいえ *] を選択）、ユーザーが必要に応じてサインインしないようにします（[* はい *] を選択）。
- d. [* グループ *] タブで、ユーザーをグループに追加するか、必要に応じてグループから削除します。
- e. 必要に応じて、[変更を保存（ Save Changes ）] を選択します。

キャッシングに時間がかかるため変更には最大で 15 分を要します。

ローカルユーザの複製

ローカルユーザを複製して新しいユーザを迅速に作成することができます。

手順

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

3. 新しいユーザの次のフィールドを変更します。

- *** フルネーム *** : このユーザのフルネーム。たとえば、ユーザの名と姓、またはアプリケーションの名前です。
- *** ユーザ名 *** : このユーザがサインインに使用する名前。ユーザ名は一意である必要があり、変更できません。
- *** Password *** : ユーザがサインイン時に使用するパスワード。
- *** パスワードの確認 *** : [パスワード] フィールドに入力したパスワードと同じパスワードを入力します。
- *** アクセスを拒否 *** : 「* はい」を選択した場合、このユーザはテナントアカウントにサインインできません。これは、ユーザがまだ 1 つ以上のグループに属している可能性がある場合も同様です。

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

4. 「* Continue *」を選択します。

5. 1 つ以上のローカルグループを選択します。

グループに属していないユーザには管理権限は付与されません。アクセス許可は累積的に追加されユーザには、自身が属しているすべてのグループに対するすべての権限が与えられます。

6. 「* ユーザーの作成 *」を選択します。

キャッシングに時間がかかるため変更には最大で 15 分を要します。

ローカルユーザを削除しています

StorageGRID テナントアカウントにアクセスする必要がなくなったローカルユーザは、完全に削除できます。

Tenant Manager を使用して、フェデレーテッドユーザは削除できますが、フェデレーテッドユーザは削除できません。フェデレーテッドユーザを削除するには、フェデレーテッドアイデンティティソースを使用する必要があります。

手順

1. [ユーザ] リストで、削除するローカルユーザのチェックボックスをオンにします。
2. *** アクション * > * ユーザーの削除 *** を選択します。
3. 確認ダイアログボックスで、「* ユーザーの削除 *」を選択して、システムからユーザーを削除することを確認します。

キャッシングに時間がかかるため変更には最大で 15 分を要します。

関連情報

["テナント管理権限"](#)

S3テナントアカウントの管理

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

管理したりできます。

- ["S3 アクセスキーの管理"](#)
- ["S3バケットの管理"](#)

S3 アクセスキーの管理

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

このタスクについて

S3 アクセスキーは次のように管理できます。

- **Manage Your Own S3 Credentials** * 権限が設定されたユーザは、自分の S3 アクセスキーを作成または削除できます。
- **Root Access** * 権限が設定されたユーザは、S3 root アカウントおよびその他すべてのユーザのアクセスキーを管理できます。root アクセスキーは、バケットポリシーで root アクセスキーが明示的に無効になっていないかぎり、テナントのすべてのバケットとオブジェクトへのフルアクセスを提供します。

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

自分の**S3**アクセスキーを作成する

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

必要なもの

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

このタスクについて

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

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

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



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

手順

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

[マイアクセスキー] ページが表示され、既存のアクセスキーが一覧表示されます。

2. 「* キーの作成 *」を選択します。

3. 次のいずれかを実行します。

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

4. [アクセスキーの作成 *] を選択します。

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

5. アクセスキー ID とシークレットアクセスキーを安全な場所にコピーするか、「* Download.csv *」を選択してアクセスキー 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。

Create access key

1 Choose expiration time ————— 2 Download access key

Download access key

To save the keys for future reference, select **Download .csv**, or copy and paste the values to another location.

i You will not be able to view the Access key ID or Secret access key after you close this dialog.

Access key ID

SHTBQKDRVHQ34YKKUAWX

Secret access key

UGu9+XeAActnOWQYFdbzmngmgVXXDvCkSOzT1Osz9K

Download .csv Finish

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。キャッシングに時間がかかるため変更には最大で 15 分を要します。

関連情報

["テナント管理権限"](#)

S3アクセスキーを表示します

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

必要なもの

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



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

手順

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

[マイアクセスキー] ページが表示され、既存のアクセスキーが一覧表示されます。

My access keys

Manage your personal S3 access keys. If a key will expire soon, you can create a new key and delete the one it is replacing.

4 keys Create key

Delete key

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

2. キーを * Expiration time * または * Access key ID * でソートします。
3. 必要に応じて、新しいキーを作成し、使用しなくなったキーを手動で削除します。

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

期限切れのキーは自動的に削除されます。

関連情報

"自分のS3アクセスキーを作成する"

"自分のS3アクセスキーを削除する"

自分の**S3**アクセスキーを削除する

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

必要なもの

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



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

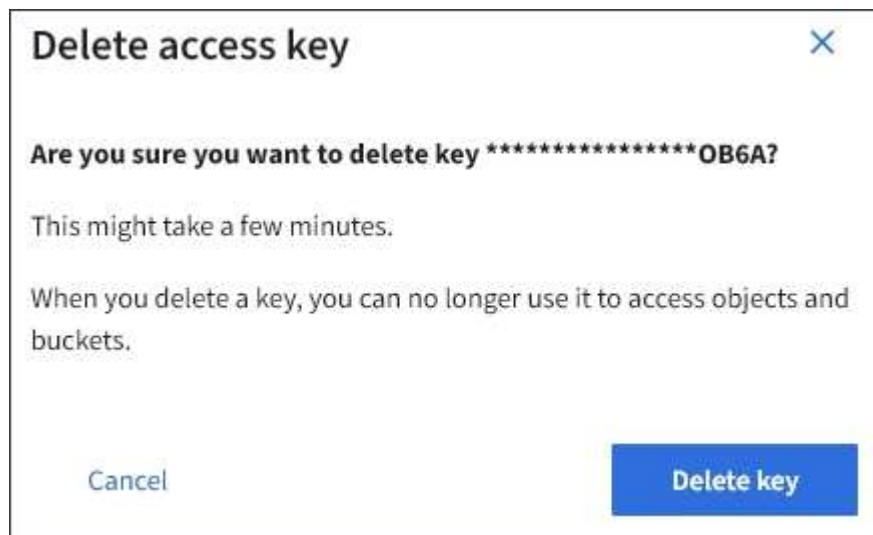
手順

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

[マイアクセスキー] ページが表示され、既存のアクセスキーが一覧表示されます。

2. 削除する各アクセスキーのチェックボックスを選択します。
3. 「* Delete key (キーの削除)」* を選択

確認のダイアログボックスが表示されます。



4. 「* Delete key (キーの削除)」* を選択

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

別のユーザのS3アクセスキーを作成する

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

必要なもの

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

このタスクについて

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

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

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



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

手順

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

ユーザの詳細ページが表示されます。

3. [* アクセスキー *] を選択し、[* キーの作成 *] を選択します。
4. 次のいずれかを実行します。
 - 有効期限を設定しない * を選択して、有効期限が切れないキーを作成します。（デフォルト）
 - [有効期限の設定 *] を選択し、有効期限の日付と時刻を設定します。

Create access key

1 Choose expiration time

2 Download access key

Choose expiration time

☐ Do not set an expiration time

☒ Set an expiration time

This access key will never expire.

MM/DD/YYYY

HH

:

MM

AM

Cancel

Create access key

5. [アクセスキーの作成 *] を選択します。

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

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



この情報をコピーまたはダウンロードするまで、このダイアログボックスを閉じないでください。

Create access key

✓ Choose expiration time

2 Download access key

Download access key

To save the keys for future reference, select **Download .csv**, or copy and paste the values to another location.

You will not be able to view the Access key ID or Secret access key after you close this dialog.

Access key ID

SHTBQKDRVHQ34YKKUAWX

Secret access key

UGu9+XeACtnOWQYFdbzmngmgVXXDvCkSOzT1Osz9K

Download .csv

Finish

7. [完了] を選択します。

新しいキーは、ユーザ詳細ページのアクセスキータブに表示されます。キャッシングに時間がかかるため変更には最大で 15 分を要します。

関連情報

"テナント管理権限"

別のユーザの S3 アクセスキーを表示しています

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

必要なもの

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

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

46

手順

1. アクセス管理 * > * Users * を選択します。

[ユーザー] ページが表示され、既存のユーザーが一覧表示されます。

2. S3 アクセスキーを表示するユーザを選択します。

ユーザーの詳細ページが表示されます。

3. 「 * アクセスキー * 」を選択します。

Manage access keys
Add or delete access keys for this user.

Create key Actions ▾

Displaying 4 results

<input type="checkbox"/>	Access key ID ▴ ▾	Expiration time ▴ ▾
<input type="checkbox"/>	*****WX5J	2020-11-21 12:00:00 MST
<input type="checkbox"/>	*****6OHM	2020-11-23 13:00:00 MST
<input type="checkbox"/>	*****J505	None
<input type="checkbox"/>	*****4MTF	None

4. キーを * Expiration time * または * Access key ID * でソートします。
5. 必要に応じて、新しいキーを作成し、使用しなくなったキーを手動で削除します。

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

期限切れのキーは自動的に削除されます。

関連情報

"別のユーザのS3アクセスキーを作成しています"

"別のユーザのS3アクセスキーを削除しています"

別のユーザのS3アクセスキーを削除しています

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

必要なもの

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



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

手順

1. アクセス管理 * > * Users * を選択します。

[ユーザー] ページが表示され、既存のユーザーが一覧表示されます。

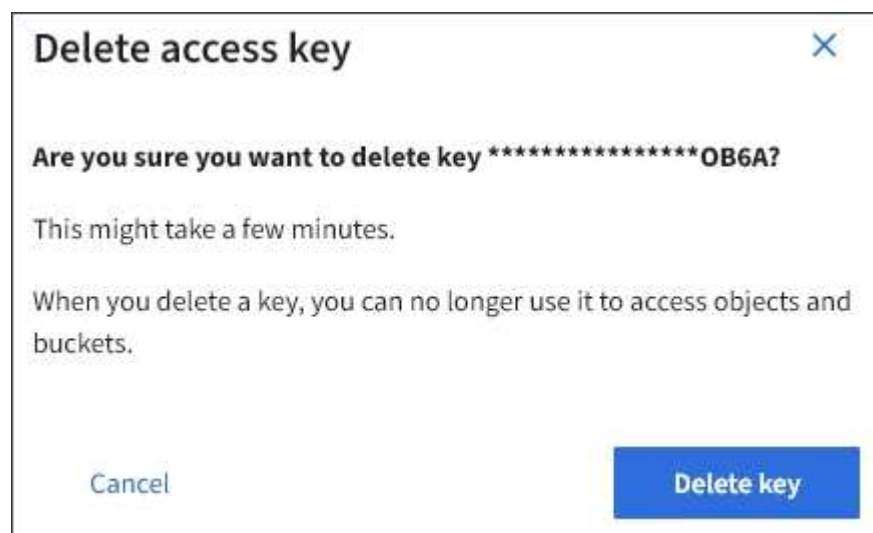
2. S3 アクセスキーを管理するユーザを選択します。

ユーザーの詳細ページが表示されます。

3. アクセスキー * を選択し、削除する各アクセスキーのチェックボックスを選択します。

4. * アクション * > * 選択したキーを削除 * を選択します。

確認のダイアログボックスが表示されます。



5. 「 * Delete key （キーの削除） 」 * を選択

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

関連情報

["テナント管理権限"](#)

S3バケットの管理

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

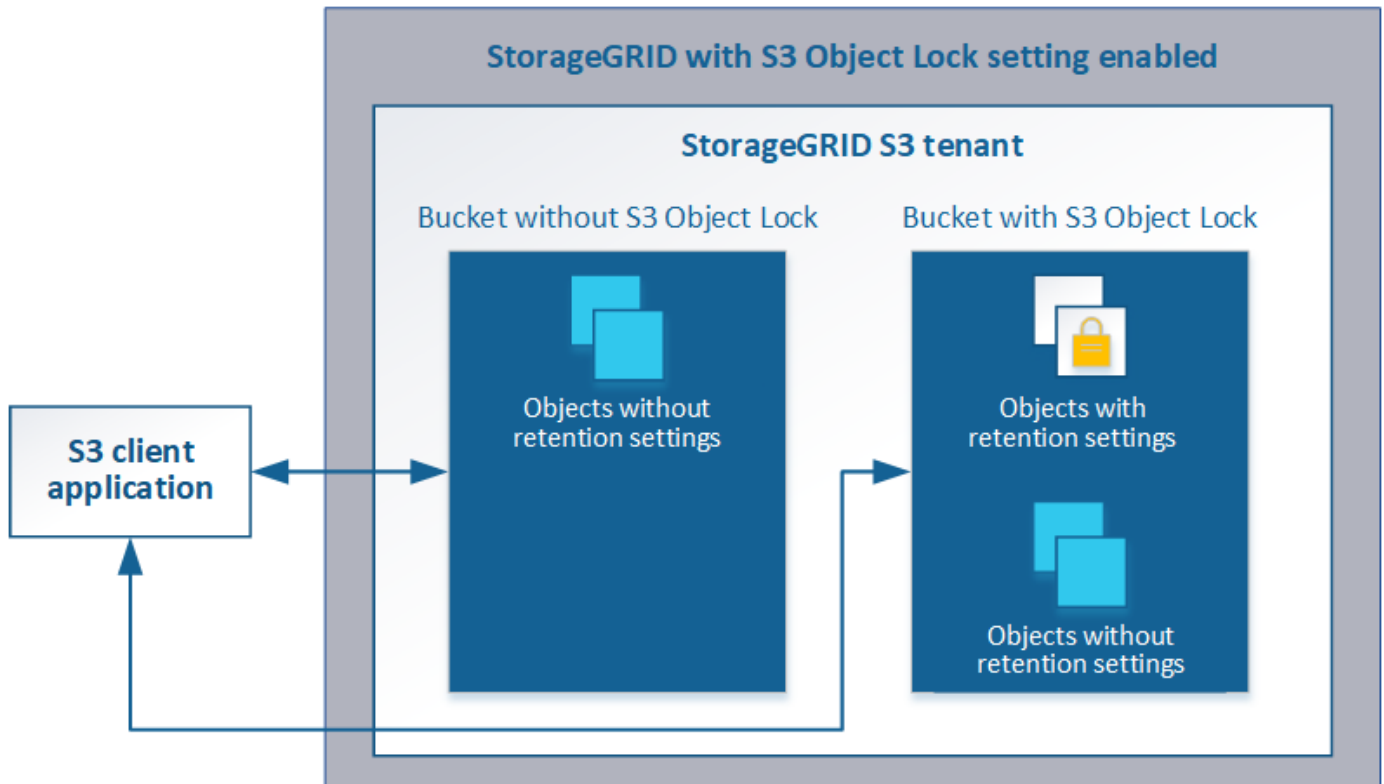
S3 オブジェクトロックを使用する

オブジェクトが保持に関する規制要件に準拠する必要がある場合は、StorageGRID で S3 オブジェクトロック機能を使用できます。

S3 オブジェクトのロックとは何ですか？

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

図に示すように、StorageGRID システムでグローバルな S3 オブジェクトのロック設定が有効になっている場合、S3 テナントアカウントでは、S3 オブジェクトのロックを有効にしているかどうかに関係なくバケットを作成できます。バケットで S3 オブジェクトのロックが有効になっている場合、S3 クライアントアプリケーションは、そのバケット内の任意のオブジェクトバージョンの保持設定を必要に応じて指定できます。オブジェクトのバージョンには、S3 オブジェクトロックで保護するように指定された保持設定が必要です。



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

バケットで S3 オブジェクトロックが有効になっている場合、S3 クライアントアプリケーションは、オブジェクトの作成時または更新時に、次のオブジェクトレベルの保持設定のいずれか、または両方を必要に応じて指定できます。

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

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

従来の準拠バケットの管理

S3 オブジェクトロック機能は、以前のバージョンの StorageGRID で使用されていた準拠機能に代わる機能です。以前のバージョンの StorageGRID を使用して準拠バケットを作成した場合は、引き続きこれらのバケットの設定を管理できますが、新しい準拠バケットは作成できなくなります。手順については、ネットアップの技術情報アーティクルを参照してください。

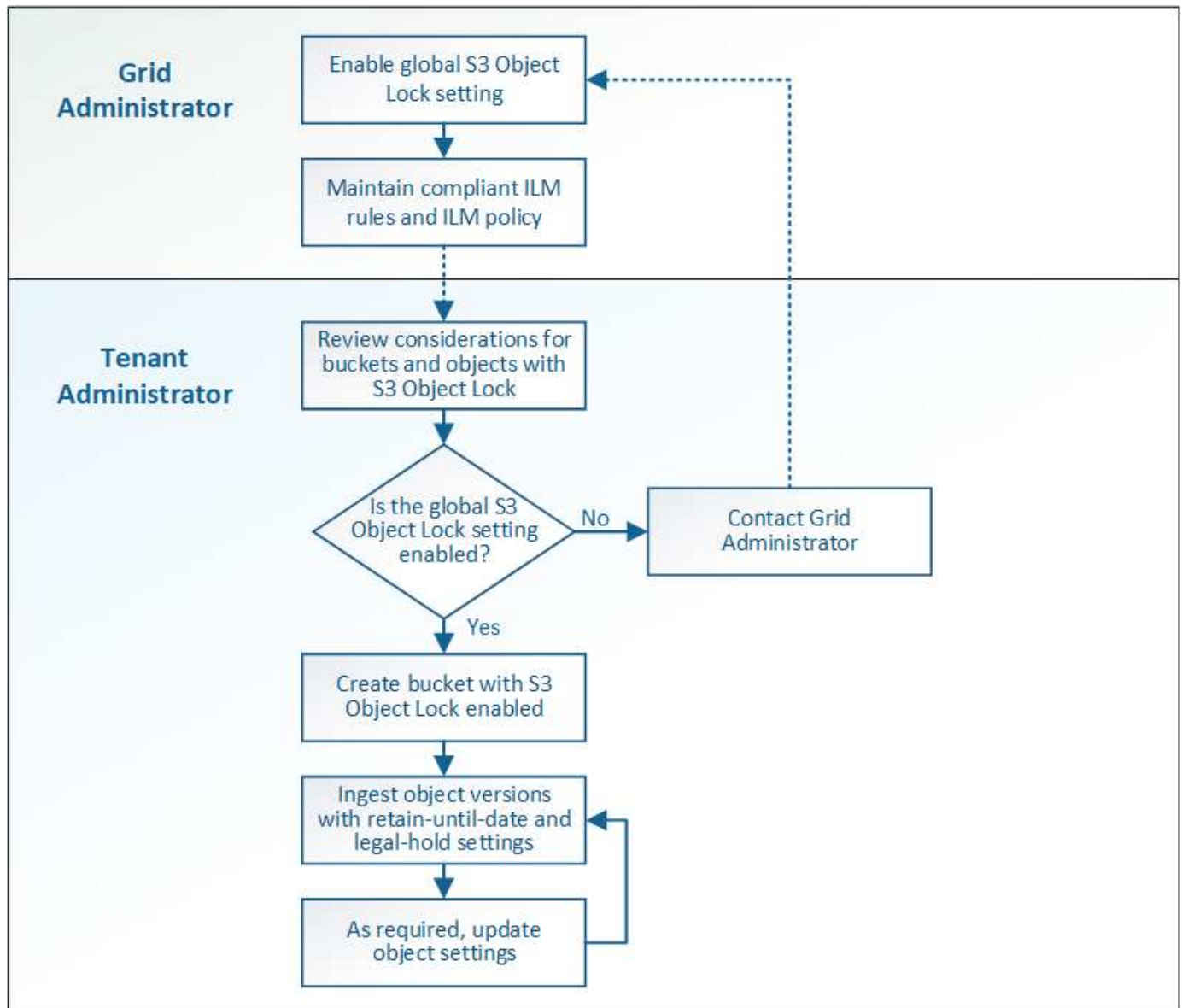
["ネットアップのナレッジベース： StorageGRID 11.5 でレガシー準拠バケットを管理する方法"](#)

S3 オブジェクトロックのワークフロー

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

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

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



関連情報

["ILM を使用してオブジェクトを管理する"](#)

S3 オブジェクトのロックの要件

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

S3 オブジェクトのロックを有効にした場合のバケットの要件

- StorageGRID システムでグローバルな S3 オブジェクトロック設定が有効になっている場合は、テナントマネージャ、テナント管理 API、または S3 REST API を使用して、S3 オブジェクトロックを有効にしたバケットを作成できます。

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

Buckets

Create buckets and manage bucket settings.

1 bucket

Create bucket

Actions ▾

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

← Previous 1 Next →

- S3 オブジェクトのロックを使用する場合は、バケットの作成時に S3 オブジェクトのロックを有効にする必要があります。既存のバケットに対して S3 オブジェクトロックを有効にすることはできません。
- S3 オブジェクトロックでは、バケットのバージョン管理が必要です。バケットで S3 オブジェクトのロックが有効になっている場合は、そのバケットのバージョン管理が StorageGRID で自動的に有効になります。
- S3 オブジェクトのロックを有効にしてバケットを作成したあとに、そのバケットの S3 オブジェクトのロックを無効にしたりバージョン管理を一時停止したりすることはできません。
- S3 オブジェクトのロックが有効になっている StorageGRID バケットでは、デフォルトの保持期間はありません。代わりに、S3 クライアントアプリケーションは、そのバケットに追加されるオブジェクトバージョンごとに保持期限とリーガルホールド設定を指定できます。
- バケットライフサイクル設定は S3 オブジェクトライフサイクルバケットでサポートされます。
- CloudMirror レプリケーションは、S3 オブジェクトロックが有効になっているバケットではサポートされません。

S3 オブジェクトのロックが有効になっているバケット内のオブジェクトの要件

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

ん。

- 係争中の訴訟や規制上の調査に関する通知があった場合、オブジェクトバージョンをリーガルホールドの対象にすることで関連情報を保持できます。オブジェクトバージョンがリーガルホールドの対象になっている場合は、それが retain-until 日に達しても、そのオブジェクトを StorageGRID から削除することはできません。リーガルホールドを解除すると、それまで保持期限に達した場合にオブジェクトバージョンを削除できるようになります。
- S3 オブジェクトロックにはバージョン管理されたバケットを使用する必要があります。保持設定はオブジェクトのバージョンごとに適用されます。オブジェクトバージョンには、retain-until date 設定とリーガルホールド設定の両方を設定できます。ただし、オブジェクトバージョンを保持することはできません。また、どちらも保持することはできません。オブジェクトの retain-until-date 設定またはリーガルホールド設定を指定すると、要求で指定されたバージョンのみが保護されます。オブジェクトの以前のバージョンはロックされたまま、オブジェクトの新しいバージョンを作成できます。

S3 オブジェクトのロックが有効なバケット内のオブジェクトのライフサイクル

S3 オブジェクトのロックが有効になっているバケットに保存された各オブジェクトは、次の 3 つの段階を経て処理されます。

1. * オブジェクトの取り込み *

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

2. * オブジェクト保持 *

- オブジェクトの複数のコピーが StorageGRID によって格納される。コピーの正確な数、タイプ、格納場所は、アクティブな ILM ポリシーの準拠ルールによって決まります。

3. * オブジェクトの削除 *

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

S3バケットの作成

Tenant Manager を使用して、オブジェクトデータ用の S3 バケットを作成できます。バケットを作成するときは、バケットの名前とリージョンを指定する必要があります。StorageGRID システムでグローバルな S3 オブジェクトのロック設定が有効になっている場合は、必要に応じてバケットで S3 オブジェクトのロックを有効にすることができます。

必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Manage All Buckets 権限または Root Access 権限のあるユーザグループに属している必要があります。これらの権限は、グループまたはバケットポリシーの権限の設定よりも優先されます。

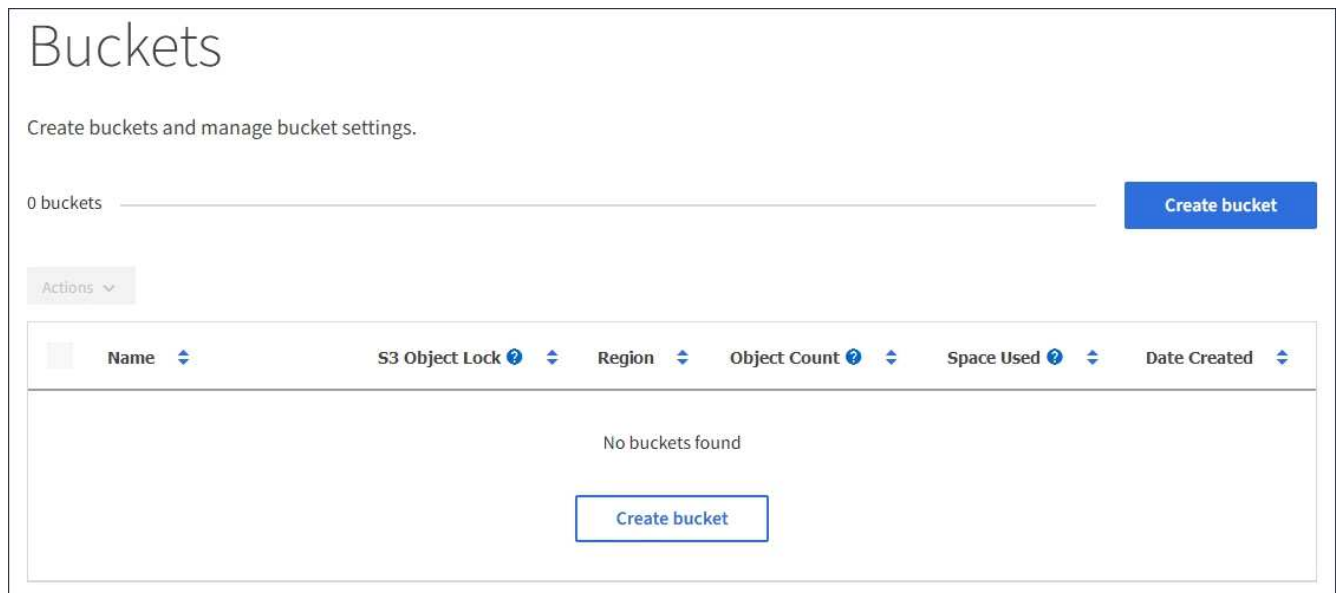
- S3オブジェクトロックを使用してバケットを作成する場合は、StorageGRID システムでグローバルなS3オブジェクトロック設定を有効にしておく必要があります。また、S3オブジェクトロックのバケットとオブジェクトに関する要件を確認しておく必要があります。

"S3 オブジェクトロックを使用する"

手順

1. ストレージ（S3） * > * バケット * を選択します。

バケットページが表示され、すでに作成されているバケットが一覧表示されます。



2. [* バケットの作成 *] を選択します。

Create Bucketウィザードが表示されます。

Create bucket

Enter bucket details

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

Bucket name ?

Region ?

us-east-1

Cancel

Create bucket



グローバルなS3オブジェクトのロック設定が有効になっている場合、バケットの作成には、バケットのS3オブジェクトのロックを管理するための2つ目の手順が含まれます。

3. バケットの一意の名前を入力します。



バケットの作成後にバケット名を変更することはできません。

バケット名は次のルールを満たす必要があります。

- StorageGRID システム全体で（テナントアカウント内だけではなく）一意である必要があります。
- DNS に準拠している必要があります。
- 3 文字以上 63 文字以下にする必要があります。
- 1 つ以上のラベルを連続して指定できます。隣接するラベルはピリオドで区切ります。各ラベルの先頭と末尾の文字は小文字のアルファベットか数字にする必要があります、使用できる文字は小文字のアルファベット、数字、ハイフンのみです。
- テキスト形式の IP アドレスのようにはできません。
- 仮想ホスト形式の要求でピリオドを使用しないでください。ピリオドを使用すると、サーバワイルドカード証明書の検証で原因の問題が発生します。



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

4. このバケットのリージョンを選択します。

StorageGRID 管理者が利用可能なリージョンを管理します。バケットのリージョンは、オブジェクトに適用されるデータ保護ポリシーに影響する可能性があります。デフォルトでは、すべてのバケットが作成されます us-east-1 リージョン：



バケットの作成後にリージョンを変更することはできません。

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

- グローバルなS3オブジェクトのロック設定が有効になっていない場合は、*バケットの作成*を選択します。バケットが作成され、バケットページのテーブルに追加されます。
- グローバルなS3オブジェクトのロック設定が有効になっている場合は、「* Continue *」を選択します。ステップ2：Manage S3 Object Lock（S3オブジェクトのロックの管理）が表示されます。

Create bucket

1 Enter details ————— 2 Manage S3 Object Lock
Optional

Manage S3 Object Lock (This step is optional)

S3 Object Lock allows you to specify retention and legal hold settings for the objects ingested into a bucket. If you want to use S3 Object Lock, you must enable this setting when you create the bucket. You cannot add or disable S3 Object Lock after a bucket is created.

If S3 Object Lock is enabled, bucket versioning is required and will be enabled automatically.

☒ Enable S3 Object Lock

Previous Create bucket

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

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



バケットの作成後に S3 オブジェクトのロックを有効または無効にすることはできません。



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

7. [* バケットの作成 *]を選択します。

バケットが作成され、バケットページのテーブルに追加されます。

関連情報

["ILM を使用してオブジェクトを管理する"](#)

"テナント管理APIについて"

"S3 を使用する"

S3バケットの詳細の表示

テナントアカウントのバケットおよびバケット設定のリストを表示できます。

必要なもの

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

手順

1. ストレージ（S3） * > * バケット * を選択します。

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

Buckets

Create buckets and manage bucket settings.

2 buckets Create bucket

Actions ▾

<input type="checkbox"/>	Name ▾	S3 Object Lock ⓘ ▾	Region ▾	Object Count ⓘ ▾	Space Used ⓘ ▾	Date Created ▾
<input type="checkbox"/>	bucket-01	✓	us-east-1	0	0 bytes	2020-11-04 14:16:59 MST
<input type="checkbox"/>	bucket-02		us-east-1	0	0 bytes	2020-11-04 14:17:14 MST

← Previous 1 Next →

2. 各バケットの情報を確認します。

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

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

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

- Region：バケットのリージョン。変更できません。
- Object Count：このバケット内のオブジェクトの数。
- Space Used：このバケット内のすべてのオブジェクトの論理サイズ。論理サイズには、レプリケートコピーやイレイジャーコーディングコピー、またはオブジェクトメタデータに必要な実際のスペースは含まれていません。
- Date Created：バケットが作成された日時。



「オブジェクト数」と「使用済みスペース」の値が概算値として表示されます。これらの推定値は、取り込みのタイミング、ネットワーク接続、ノードのステータスによって左右されます。

3. バケットの設定を表示および管理するには、バケット名を選択します。

バケットの詳細ページが表示されます。

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

各設定またはプラットフォームサービスの設定手順を参照してください。

Buckets > bucket-02

Overview

Name: **bucket-02**

Region: **us-east-1**

S3 Object Lock: **Disabled**

Date created: **2020-11-04 14:51:59 MST**

Bucket options | Bucket access | Platform services

Consistency level: Read-after-new-write

Last access time updates: Disabled

関連情報

["整合性レベルを変更する"](#)

["最終アクセス日時の更新の有効化または無効化"](#)

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

["CloudMirrorレプリケーションの設定"](#)

["イベント通知を設定する"](#)

["検索統合サービスの設定"](#)

S3 テナントを使用している場合は、テナントマネージャまたはテナント管理 API を使用して、S3 バケット内のオブジェクトに対して実行される処理の整合性制御レベルを変更できます。

必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Manage All Buckets 権限または Root Access 権限のあるユーザグループに属している必要があります。これらの権限は、グループまたはバケットポリシーの権限の設定よりも優先されます。

このタスクについて

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



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

手順

1. ストレージ (S3) * > * バケット * を選択します。
2. リストからバケット名を選択します。

バケットの詳細ページが表示されます。

3. * Bucket options * > * Consistency level * を選択します。

Bucket options

Bucket access

Platform services

Consistency level

Read-after-new-write (default)

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

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

☐

All

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

☐

Strong-global

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

☐

Strong-site

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

☒

Read-after-new-write (default)

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

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

☐

Available

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

Save changes

4. このバケット内のオブジェクトに対して実行される処理の整合性レベルを選択します。

整合性レベル	説明
すべて	すべてのノードが即座にデータを受け取り、受け取れない場合は要求が失敗します。

整合性レベル	説明
strong-global	すべてのサイトのすべてのクライアント要求について、リードアフターライト整合性が保証されます。
strong-site	1つのサイト内のすべてのクライアント要求について、リードアフターライト整合性が保証されます。
read-after-new-write（デフォルト）	新規オブジェクトにはリードアフターライト整合性を、オブジェクトの更新には結果整合性を提供します。高可用性が確保され、データ保護が保証されます。Amazon S3の整合性に相当します。 注：Amazon S3の整合性保証が必要な場合を除き、アプリケーションが存在しないキーに対してHEAD処理を試行する場合は、整合性レベルを「Available *」に設定してください。そうしないと、使用できないストレージノードがある場合に「500 Internal Server Error」が大量に発生する可能性があります。
available（HEAD処理は結果整合性）	read-after-new-write *整合性レベルと動作は同じですが、HEAD処理については結果整合性のみを提供します。ストレージノードを使用できない場合に、HEAD処理に対して「Read-after-new-write」よりも高い可用性が提供される。Amazon S3の整合性と異なるのはHEAD処理のみです。

5. 「変更を保存」を選択します。

関連情報

"テナント管理権限"

最終アクセス日時の更新の有効化または無効化

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


この手順は、配置手順で * Last Access Time * オプションを使用する ILM ルールを 1 つ以上含む StorageGRID システムにのみ適用されます。StorageGRID システムにこのようなルールが含まれていない場合は、この手順を無視してかまいません。

必要なもの


- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Manage All Buckets 権限または Root Access 権限のあるユーザグループに属している必要があります。これらの権限は、グループまたはバケットポリシーの権限の設定よりも優先されます。
- 最終アクセス時間 * は、ILM ルールの * 参照時間 * 配置手順で使用するオプションの 1 つです。ルールの参照時間を最終アクセス日時に設定すると、グリッド管理者は、オブジェクトが最後に読み出された（読み取りまたは表示された）タイミングに基づいて特定のストレージの場所にオブジェクトが配置されるように指定できます。

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

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

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

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

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

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

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

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

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

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

手順

1. ストレージ（S3） * > * バケット * を選択します。
2. リストからバケット名を選択します。

バケットの詳細ページが表示されます。
3. 「 * Bucket options * > * Last access time updates * 」を選択します。
4. 適切なオプションボタンを選択して、最終アクセス日時の更新を有効または無効にします。

The screenshot shows the 'Bucket options' tab in the AWS S3 console. The 'Consistency level' is set to 'Read-after-new-write'. The 'Last access time updates' section is expanded, showing a 'Disabled' status. Below this, there is explanatory text and a list of behaviors when updates are disabled. A yellow warning box states: 'Updating the last access time when an object is retrieved can reduce performance, especially for small objects.' At the bottom, there are two radio buttons: 'Enable last access time updates when retrieving an object' (unselected) and 'Disable last access time updates when retrieving an object' (selected). A 'Save changes' button is located at the bottom right.

5. 「変更を保存」を選択します。

関連情報

["テナント管理権限"](#)

["ILM を使用してオブジェクトを管理する"](#)

Cross-Origin Resource Sharing（CORS）の設定

S3 バケットとバケット内のオブジェクトに他のドメインにある Web アプリケーション

からアクセスできるようにする必要がある場合は、そのバケットに Cross-Origin Resource Sharing （ CORS ） を設定できます。

必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Manage All Buckets 権限または Root Access 権限のあるユーザグループに属している必要があります。これらの権限は、グループまたはバケットポリシーの権限の設定よりも優先されます。

このタスクについて

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

手順

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

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

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

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

2. Tenant Manager で、 * Storage （ S3 ） * > * Buckets * を選択します。
3. リストからバケット名を選択します。

バケットの詳細ページが表示されます。

4. Bucket access * > * Cross-Origin Resource Sharing （ CORS ） * を選択します。

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

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

Cross-Origin Resource Sharing (CORS) Disabled

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

☒ Enable CORS

Clear

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

Save changes

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

S3バケットを削除しています

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

必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Manage All Buckets 権限または Root Access 権限のあるユーザグループに属している必要があります。これらの権限は、グループまたはバケットポリシーの権限の設定よりも優先されます。

このタスクについて

以下の手順では、Tenant Manager を使用して S3 バケットを削除する方法について説明します。テナント管

理APIまたはS3 REST APIを使用してS3バケットを削除することもできます。

オブジェクトまたは最新でないオブジェクトバージョンが含まれている S3 バケットは削除できません。S3バージョン管理オブジェクトの削除方法については、情報ライフサイクル管理を使用してオブジェクトを管理する手順を参照してください。

手順

1. ストレージ（S3） * > * バケット * を選択します。

バケットページが表示され、既存の S3 バケットがすべて表示されます。

Buckets

Create buckets and manage bucket settings.

2 buckets Create bucket

Actions ▾

<input type="checkbox"/>	Name ▾	S3 Object Lock ⓘ ▾	Region ▾	Object Count ⓘ ▾	Space Used ⓘ ▾	Date Created ▾
<input type="checkbox"/>	bucket-01	✓	us-east-1	0	0 bytes	2020-11-04 14:16:59 MST
<input type="checkbox"/>	bucket-02		us-east-1	0	0 bytes	2020-11-04 14:17:14 MST

← Previous 1 Next →

2. 削除する空のバケットのチェックボックスを選択します。

[アクション]メニューが有効になります。

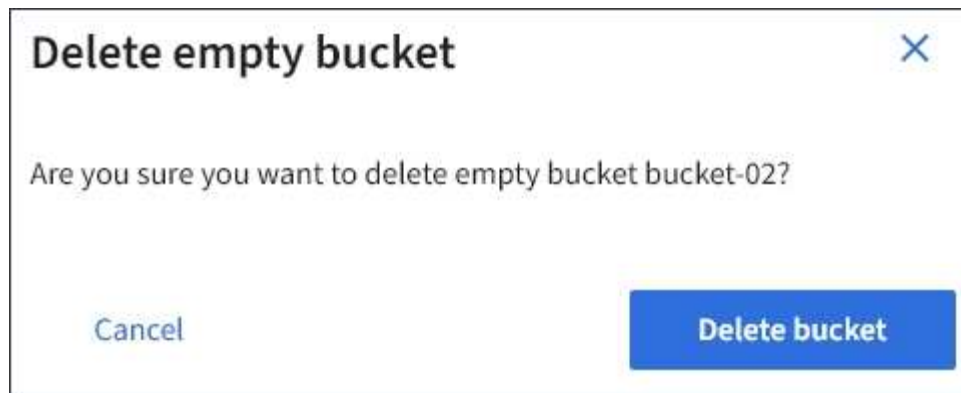
3. アクションメニューから*空のバケットを削除*を選択します。

Actions ▴

Delete empty bucket

<input type="checkbox"/>	Name ▾	S3 Object Lock ⓘ ▾	Region ▾	Object Count ⓘ ▾	Space Used ⓘ ▾	Date Created ▾
<input type="checkbox"/>	bucket-01	✓	us-east-1	0	0 bytes	2020-11-04 14:16:59 MST
<input checked="" type="checkbox"/>	bucket-02		us-east-1	0	0 bytes	2020-11-04 14:17:14 MST

確認メッセージが表示されます。



4. バケットを削除してもよろしいですか？*バケットの削除*を選択します。

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

バケットが空でない場合は、エラーメッセージが表示されます。バケットを削除する前に、すべてのオブジェクトを削除する必要があります。



関連情報

["ILM を使用してオブジェクトを管理する"](#)

S3プラットフォームサービスの管理

S3テナントアカウントにプラットフォームサービスの使用が許可されている場合は、プラットフォームサービスを使用して外部サービスを利用し、S3バケットに対してCloudMirrorレプリケーション、通知、および検索統合を設定できます。

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

プラットフォームサービスとは

StorageGRID プラットフォームサービスは、ハイブリッドクラウドの実装に役立ちます。

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

サービスを設定できます。

- *** CloudMirror レプリケーション *** : StorageGRID CloudMirror レプリケーションサービスは、StorageGRID バケットから指定された外部のデスティネーションに特定のオブジェクトをミラーリングするために使用します。

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



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

- *** 通知 *** : バケット単位のイベント通知は、オブジェクトに対して実行された特定の処理に関する通知を、指定された外部の Amazon Simple Notification Service ™ (SNS) に送信するために使用します。

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



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

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

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



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

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

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



プラットフォームサービスの使用は、StorageGRID 管理者がグリッドマネージャまたはグリッド管理 API を使用してテナントアカウントごとに有効にする必要があります。

プラットフォームサービスの設定方法

プラットフォームサービスは、Tenant Manager またはテナント管理 API を使用して、設定した外部エンドポイントと通信します。各エンドポイントは外部のデスティネーション (StorageGRID S3 バケット、Amazon Web Services バケット、Simple Notification Service (SNS) トピック、ローカル、AWS などにホストさ

れる Elasticsearch クラスタなど) です。

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

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

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

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

プラットフォームサービス	S3 REST API
CloudMirror レプリケーション	<ul style="list-style-type: none">• GET Bucket replication• PUT Bucket replication
通知	<ul style="list-style-type: none">• GET Bucket notification• PUT Bucket notification
検索統合	<ul style="list-style-type: none">• GET Bucket metadata notification configuration• PUT Bucket metadata notification configuration のコマンドです <p>これらは StorageGRID 独自の処理です。</p>

StorageGRID でこれらの API の実装方法の詳細については、S3 クライアントアプリケーションを実装する手順を参照してください。

関連情報

["S3 を使用する"](#)

["CloudMirrorレプリケーションサービスの概要"](#)

["バケットの通知の概要"](#)

["検索統合サービスの概要"](#)

["プラットフォームサービスの使用に関する考慮事項"](#)

CloudMirrorレプリケーションサービスの概要

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

て CloudMirror レプリケーションを有効にすることができます。

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

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



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

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

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

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

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



レプリカのマークに使用されるカスタムヘッダーはです x-ntap-sg-replica。このマーキングは 'カスケード・ミラー' を防止します StorageGRID は、2 つのグリッド間の双方向 CloudMirror をサポートしています。

デスティネーションバケット内ではイベントは一意になるとは限らず、その順序も保証されません。確実に配信することを目的とした処理の結果として、ソースオブジェクトの同一のコピーが複数デスティネーションに配信されることがあります。まれに、複数の異なる StorageGRID サイトから同じオブジェクトが同時に更新された場合、デスティネーションバケットでの処理の順序がソースバケットでのイベントの順序と一致しないことがあります。

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

関連情報

"CloudMirrorレプリケーションの設定"

バケットの通知の概要

S3 バケットに対するイベント通知を有効にすると、指定したイベントに関する通知を StorageGRID からデスティネーションの Amazon Simple Notification Service （SNS）に送信できます。

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

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

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

サポートされている通知およびメッセージです

StorageGRID イベント通知は Amazon S3 API に準拠しますが、次の制限事項があります。

- 次のイベントタイプには通知を設定できません。これらのイベントタイプは * サポートされていません。
 - s3:ReducedRedundancyLostObject
 - s3:ObjectRestore:Completed
- StorageGRID から送信されるイベント通知は標準の JSON 形式を使用しますが、次の表に示すように使用されないキーおよび特定の値が使用されるキーがあります。

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

検索統合サービスの概要

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

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

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

通知は、という名前の JSON ドキュメントの形式で生成されます。バケット名、オブジェクト名、バージョン ID も必要です。各メタデータ通知には、すべてのオブジェクトのタグとユーザメタデータに加えて、オブジェクトのシステムメタデータの標準セットが含まれています。



タグとユーザメタデータの場合、StorageGRID は文字列または S3 イベント通知として Elasticsearch に日付と番号を渡します。これらの文字列を日付または数値として解釈するように Elasticsearch を設定するには、動的フィールドマッピングおよびマッピング日付形式に関する Elasticsearch の手順に従ってください。検索統合サービスを設定する前に、インデックスの動的フィールドマッピングを有効にする必要があります。ドキュメントにインデックスを付けた後は、インデックス内のドキュメントのフィールドタイプを編集できません。

通知は次の場合に常に生成され、配信のキューに登録されます

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

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

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

StorageGRID 検索統合サービスは、デスティネーションとして Elasticsearch クラスターをサポートします。他のプラットフォームサービスと同様、URN がサービスの設定 XML で使用されているエンドポイントにデスティネーションが指定されます。サポートされている Elasticsearch のバージョンを確認するには、Interoperability Matrix Tool を使用してください。

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

"検索統合用の XML を設定します"

"メタデータ通知に含まれているオブジェクトメタデータ"

"検索統合サービスで生成される JSON"

"検索統合サービスの設定"

プラットフォームサービスの使用に関する考慮事項

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

プラットフォームサービスの使用に関する考慮事項

考慮事項	詳細
デスティネーションエンドポイントの監視	各デスティネーションエンドポイントの可用性を監視する必要があります。長時間にわたってデスティネーションエンドポイントへの接続が失われ、要求のバックログが大量に発生している場合、StorageGRID に対する以降のクライアント要求（PUT 要求など）は失敗します。エンドポイントがアクセス可能になったら、失敗した要求を再試行する必要があります。
デスティネーションエンドポイントのスロットル	<p>要求が送信されるペースがデスティネーションエンドポイントで要求を受信できるペースを超えると、StorageGRID ソフトウェアはバケットの受信 S3 要求を調整する場合があります。スロットルは、デスティネーションエンドポイントへの送信を待機している要求のバックログが生じている場合にのみ発生します。</p> <p>明らかな影響は、受信 S3 要求の実行時間が長くなることです。パフォーマンスが大幅に低下していることが検出されるようになった場合は、取り込み速度を下げるか、容量の大きいエンドポイントを使用する必要があります。要求のバックログが増え続けると、クライアント S3 処理（PUT 要求など）が失敗します。</p> <p>通常、CloudMirror 要求には、検索統合やイベント通知の要求よりも多くのデータ転送が含まれるため、デスティネーションエンドポイントのパフォーマンスによる影響を受ける可能性が高くなります。</p>
順序保証	<p>StorageGRID では、1 つのサイト内のオブジェクトに対する処理の順序が保証されます。あるオブジェクトに対するすべての処理が同じサイト内で実行されるかぎり、最終的なオブジェクトの（レプリケーションの）状態は常に StorageGRID の状態と同じになります。</p> <p>StorageGRID は、StorageGRID サイト間で処理が行われる場合、最善の順序で要求を処理しようと試みます。たとえば、最初にサイト A にオブジェクトを書き込んだあと、サイト B で同じオブジェクトを上書きした場合、CloudMirror によって最終的にデスティネーションバケットにレプリケートされるオブジェクトが新しいほうのオブジェクトであるとはかぎりません。</p>

考慮事項	詳細
ILM ベースのオブジェクト削除	<p>AWS CRR サービスと SNS サービスの削除動作を一致させるため、StorageGRID の ILM ルールに基づいてソースバケット内のオブジェクトが削除された場合、CloudMirror 要求とイベント通知要求は送信されません。たとえば、ILM ルールによって 14 日後にオブジェクトが削除された場合、CloudMirror 要求やイベント通知要求は送信されません。</p> <p>一方、ILM に基づいてオブジェクトが削除された場合、検索統合要求は送信されます。</p>

CloudMirrorレプリケーションサービスの使用に関する考慮事項

考慮事項	詳細
レプリケーションのステータス	StorageGRID ではがサポートされません <code>x-amz-replication-status</code> ヘッダー。
オブジェクトのサイズ	CloudMirrorレプリケーションサービスでデスティネーションバケットにレプリケートできるオブジェクトの最大サイズは5TBであり、StorageGRID でサポートされる最大オブジェクトサイズと同じです。
バケットのバージョン管理とバージョン ID	<p>StorageGRID でソース S3 バケットのバージョン管理を有効にした場合、デスティネーションバケットのバージョン管理も有効にする必要があります。</p> <p>バージョン管理を使用している場合、S3 プロトコルの制限事項により、デスティネーションバケットのオブジェクトバージョンの処理はベストエフォートベースで行われ、CloudMirror サービスによる保証はありません。</p> <ul style="list-style-type: none"> 注 * : StorageGRID のソースバケットのバージョン ID は、デスティネーションバケットのバージョン ID とは関連がありません。

オブジェクトバージョンのタグ付け	<p>CloudMirror サービスでは、S3 プロトコルの制限事項により、バージョン ID を提供する PUT Object tagging 要求と DELETE Object tagging 要求がレプリケートされません。ソースとデスティネーションのバージョン ID には関連がないため、特定のバージョン ID へのタグの更新を確実にレプリケートする方法はありません。</p> <p>一方、バージョン ID を指定しない PUT Object tagging 要求と DELETE Object tagging 要求は、CloudMirror サービスによってレプリケートされます。これらの要求は、最新のキー（バケットがバージョン管理されている場合は最新のバージョン）のタグを更新します。（タグの更新ではなく）タグを使用した通常の取り込みもレプリケートされます。</p>
マルチパートアップロードおよび ETag 値	<p>マルチパートアップロードを使用してアップロードされたオブジェクトをミラーリングした場合、CloudMirror サービスではパートが保持されません。その結果、が表示されます ETag ミラーオブジェクトの値は、とは異なります ETag 元のオブジェクトの値。</p>
SSE-C（ユーザ指定のキーによるサーバ側の暗号化）で暗号化されたオブジェクト	<p>CloudMirror サービスでは、SSE-C で暗号化されたオブジェクトがサポートされませんCloudMirror レプリケーションのソースバケットにオブジェクトを取り込む際に、要求に SSE-C 要求ヘッダーが含まれていると、処理が失敗します。</p>
S3 オブジェクトのロックが有効になっているバケット	<p>CloudMirrorレプリケーションのデスティネーションS3バケットでS3オブジェクトロックが有効になっている場合は、レプリケーション処理がAccessDeniedエラーで失敗します。</p>

関連情報

["S3 を使用する"](#)

プラットフォームサービスエンドポイントの設定

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

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

プラットフォームサービスエンドポイントとは

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

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

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

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

CloudMirror レプリケーション用のエンドポイント

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

通知用のエンドポイント

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

検索統合サービスのエンドポイント

StorageGRID は、Elasticsearch クラスタを表す検索統合エンドポイントをサポートします。Elasticsearch クラスタは、ローカルデータセンターにあるか、AWS クラウドなどの別の場所でホストされている可能性があります。

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

関連情報

["StorageGRID の管理"](#)

プラットフォームサービスのエンドポイントのURNの指定

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

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

URN 要素

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

- サービスがAWSでホストされている場合は、を使用します `arn:aws`。
- サービスがローカルでホストされている場合は、を使用します `urn:mysite`

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

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

サービス	を入力します
CloudMirror レプリケーション	S3
通知	SnS
検索統合	ES

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

URN の最後の要素は、デスティネーション URI の特定のターゲットリソースを識別します。

サービス	特定のリソース
CloudMirror レプリケーション	バケット名
通知	sns-topic-name を入力します
検索統合	domain-name/index-name/type-name • 注：Elasticsearch クラスタが * NOT * である場合、インデックスを自動的に作成するように設定されているため、エンドポイントを作成する前にインデックスを手動で作成する必要があります。

AWSでホストされるサービスのURN

AWSのエンティティの場合、完全なURNは有効なAWS ARNです。例：

- CloudMirror レプリケーション：


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

- 通知：

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

- 検索統合：

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



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

ローカルでホストされるサービスの URN

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

- CloudMirror レプリケーション：

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

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

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

- 通知：

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

- 検索統合：

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




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

プラットフォームサービスエンドポイントの作成

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

必要なもの

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



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

- Unique Resource Name （ URN ）

"プラットフォームサービスのエンドポイントのURNの指定"

- 認証クレデンシャル（必要な場合）：
 - Access Key ：アクセスキー ID とシークレットアクセスキー
 - 基本 HTTP 認証：ユーザ名とパスワード
- セキュリティ証明書（カスタム CA 証明書を使用する場合）

手順

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

プラットフォームサービスエンドポイントページが表示されます。

Platform services endpoints

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

0 endpoints

Create endpoint

Delete endpoint

	Display name ?	Last error ?	Type ?	URI ?	URN ?
No endpoints found					
Create endpoint					

2. [* エンドポイントの作成 *] を選択します。

Create endpoint

1 Enter details

2 Select authentication type
Optional

3 Verify server
Optional

Enter endpoint details

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

Display name ?

URI ?

https://example.com

URN ?

arn:aws:s3::bucket_name

Cancel

Continue

3. エンドポイントとその目的を簡単に説明する表示名を入力します。

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

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

次のいずれかの形式を使用します。

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

ポートを指定しない場合、HTTPS URI にはポート 443 が、HTTP URI にはポート 80 が使用されます。

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

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

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



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

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

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



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

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



エンドポイントの作成後に、エンドポイントの URN を変更することはできません。

6. 「* Continue *」を選択します。

7. 「*認証タイプ」の値を選択し、必要なクレデンシャルを入力します。

Create endpoint

1 Enter details 2 Select authentication type 3 Verify server

Optional Optional

Authentication type ?

Select the method used to authenticate connections to the endpoint.

Anonymous

Anonymous

Access Key

Basic HTTP

Previous Continue

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

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

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

×

Create endpoint

✓ Enter details

✓ Select authentication type
Optional

3 Verify server
Optional

Verify server

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

☒ Use custom CA certificate
☐ Use operating system CA certificate
☐ Do not verify certificate

```

-----BEGIN CERTIFICATE-----
abodefghijkl123456780ABCDEFGHIJKL
123456/7890ABCDEFabodefghijklABCD
-----END CERTIFICATE-----

```

Previous

Test and create endpoint

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

10. [* テストとエンドポイントの作成 *] を選択します。

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



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

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

関連情報

["プラットフォームサービスのエンドポイントのURNの指定"](#)

["CloudMirrorレプリケーションの設定"](#)

["イベント通知を設定する"](#)

["検索統合サービスの設定"](#)

プラットフォームサービスエンドポイントの接続をテストしています

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

必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Manage Endpoints 権限のあるユーザグループに属している必要があります。

このタスクについて

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

手順

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

Platform services Endpoints ページが表示され、設定済みのプラットフォームサービスエンドポイントのリストが表示されます。

Platform services endpoints

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

4 endpoints Create endpoint

Delete endpoint

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

2. 接続をテストするエンドポイントを選択します。

エンドポイントの詳細ページが表示されます。

Overview

Display name:

my-endpoint-1

Type:

S3 Bucket

URI:

http://10.96.104.167:10443

URN:

urn:sgws:s3:::bucket1

Connection

Configuration

Verify connection

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

Test connection

3. [接続のテスト *] を選択します。

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

プラットフォームサービスエンドポイントの編集

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

必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Manage Endpoints 権限のあるユーザグループに属している必要があります。

手順

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

Platform services Endpoints ページが表示され、設定済みのプラットフォームサービスエンドポイントのリストが表示されます。







Platform services endpoints

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

4 endpoints

Create endpoint

Delete endpoint

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

2. 編集するエンドポイントを選択します。

エンドポイントの詳細ページが表示されます。

3. 「 * Configuration * 」を選択します。

Overview

Display name: **my-endpoint-3** 

Type: **Notifications**

URI: **http://10.96.104.202:8080/**

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

Connection

Configuration

Edit configuration

Endpoint details

URI 

http://10.96.104.202:8080/

URN 

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

Authentication type

Basic HTTP 

Username 

testme

Password 

••••••••

Edit password

Verify server

- ☐ Use custom CA certificate
- ☒ Use operating system CA certificate
- ☐ Do not verify certificate


```
-----BEGIN CERTIFICATE-----
abcdefghijklmnopqrstuvwxyz
123456/7890ABCDEFabcdefghijklmnopqrstuvwxyz
-----END CERTIFICATE-----
```

Test and save changes

4. 必要に応じて、エンドポイントの設定を変更します。



エンドポイントの作成後に、エンドポイントの URN を変更することはできません。

- a. エンドポイントの表示名を変更するには、編集アイコンを選択します .
- b. 必要に応じて、URI を変更します。
- c. 必要に応じて、認証タイプを変更します。
 - Basic HTTP 認証の場合は、必要に応じてユーザ名を変更します。必要に応じてパスワードを変更するには、「* パスワードを編集」を選択し、新しいパスワードを入力します。変更をキャンセルする必要がある場合は、* パスワードの編集を元に戻す * を選択します。
 - アクセスキー認証の場合は、必要に応じて「* S3 キーの編集」を選択し、新しいアクセスキー ID とシークレットアクセスキーを貼り付けることで、キーを変更します。変更をキャンセルする必要がある場合は、* Revert S3 key edit * を選択します。
- d. 必要に応じて、サーバを検証する方法を変更します。

5. [変更のテストと保存 *] を選択します。

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

関連情報

"プラットフォームサービスエンドポイントの作成"

プラットフォームサービスエンドポイントを削除しています

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

必要なもの

- Tenant Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Manage Endpoints * 権限のあるユーザグループに属している必要があります。

手順

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

Platform services Endpoints ページが表示され、設定済みのプラットフォームサービスエンドポイントのリストが表示されます。

Platform services endpoints

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

4 endpoints

Create endpoint

Delete endpoint

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

- 削除する各エンドポイントのチェックボックスを選択します。



使用中のプラットフォームサービスエンドポイントを削除すると、エンドポイントを使用するすべてのバケットに対して、関連するプラットフォームサービスが無効になります。完了していない要求はすべて破棄されます。新しい要求は、削除された URN を参照しないようにバケット設定を変更するまで、引き続き生成されます。StorageGRID はこれらの要求を回復不能なエラーとして報告します。

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

確認メッセージが表示されます。

Delete endpoint

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

This might take a few minutes.

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

Cancel Delete endpoint


4. [* エンドポイントの削除 *] を選択します。

プラットフォームサービスのエンドポイントエラーのトラブルシューティング

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


エラーが発生したかどうかを確認しています

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

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

ダッシュボードに表示されるのと同じエラーは、プラットフォームサービスのエンドポイントページの上にも表示されます。詳細なエラーメッセージを表示するには、次の手順を実行します

手順

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

Overview

Display name:

my-endpoint-2

Type:

Search

URI:

http://10.96.104.30:9200

URN:

urn:sgws:es:::mydomain/sveloso/_doc

Connection

Configuration

Verify connection

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

Test connection

Last error details

✖

2 hours ago

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

エラーが現在も継続しているかどうかを確認しています

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

手順

1. エンドポイントを選択します。

エンドポイントの詳細ページが表示されます。

2. 接続 > 接続テスト * を選択します。

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

エンドポイントエラーの解決

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

エラーを解決するためにエンドポイントを編集する必要がある場合：* Test and save changes *を選択すると、StorageGRID は更新されたエンドポイントを検証し、現在のクレデンシャルでアクセスできることを確認します。エンドポイントへの接続は、各サイトの 1 つのノードから検証されます。

手順

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

必要な権限がないエンドポイントクレデンシャルです

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

その他のプラットフォームサービスのトラブルシューティング

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

["StorageGRID の管理"](#)

関連情報

["プラットフォームサービスエンドポイントの作成"](#)

["プラットフォームサービスエンドポイントの接続をテストしています"](#)

["プラットフォームサービスエンドポイントの編集"](#)

CloudMirrorレプリケーションの設定

CloudMirror レプリケーションサービスは、3 つの StorageGRID プラットフォームサービスのいずれかです。CloudMirror レプリケーションを使用すると、外部の S3 バケットにオブジェクトを自動的にレプリケートできます。

必要なもの

- テナントアカウントのプラットフォームサービスが StorageGRID 管理者によって有効化されている必要

があります。

- レプリケーションのソースとして機能するバケットを作成しておく必要があります。
- CloudMirror レプリケーションのデスティネーションとして使用するエンドポイントを用意しておく必要があります。また、その URN が必要です。
- テナントアカウント内のすべての S3 バケットの設定を管理できるように、Manage All Buckets 権限または Root Access 権限を持つユーザグループに属している必要があります。これらの権限は、Tenant Manager を使用してバケットを設定する際にグループポリシーまたはバケットポリシーの権限設定よりも優先されます。

このタスクについて

CloudMirror レプリケーションでは、ソースバケットからエンドポイントで指定されたデスティネーションバケットにオブジェクトがコピーされます。バケットの CloudMirror レプリケーションを有効にするには、有効なバケットレプリケーション設定 XML を作成して適用する必要があります。レプリケーション設定 XML では、各デスティネーションとして S3 バケットエンドポイントの URN を使用する必要があります。



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

バケットレプリケーションとその設定方法の一般的な情報については、Amazonのドキュメントのクロスリージョンレプリケーション（CRR）に関する説明を参照してください。StorageGRID がS3バケットのレプリケーション設定APIを実装する方法については、S3クライアントアプリケーションを実装する手順を参照してください。

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

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

手順

1. ソースバケットのレプリケーションを有効にします。

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

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

- REDUCED_REDUNDANCY：重大度が低く、再現可能で、かつ冗長性に劣る状態で保存可能なデータには、このストレージクラスを使用します STANDARD ストレージクラス。

◦ を指定する場合 Role 設定XMLでは無視されます。この値は StorageGRID では使用されません。

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

2. Tenant Manager で、* Storage (S3) * > * Buckets * を選択します。
3. ソースバケットの名前を選択します。

バケットの詳細ページが表示されます。

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

Bucket options

Bucket access

Platform services

Replication

Disabled

^

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

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

☒ Enable replication

Clear

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

Save changes



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

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

前述の例では、プレフィックス「2020」に一致するオブジェクトがレプリケートされます。
 - b. オブジェクトがデスティネーションバケットにレプリケートされたことを確認します。

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

関連情報

["CloudMirrorレプリケーションサービスの概要"](#)

["S3 を使用する"](#)

["プラットフォームサービスエンドポイントの作成"](#)

イベント通知を設定する

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

必要なもの

- テナントアカウントのプラットフォームサービスが StorageGRID 管理者によって有効化されている必要があります。
- 通知のソースとなるバケットを作成しておく必要があります。
- イベント通知のデスティネーションとして使用するエンドポイントが存在し、その URN を把握している必要があります。
- テナントアカウント内のすべての S3 バケットの設定を管理できるように、Manage All Buckets 権限または Root Access 権限を持つユーザグループに属している必要があります。これらの権限は、Tenant Manager を使用してバケットを設定する際にグループポリシーまたはバケットポリシーの権限設定よりも優先されます。

このタスクについて

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

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

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

手順

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

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

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

3. ソースバケットの名前を選択します。

バケットの詳細ページが表示されます。

4. プラットフォームサービス > イベント通知 * を選択します。

5. [イベント通知を有効にする *] チェックボックスをオンにします。

6. 通知設定 XML をテキストボックスに貼り付け、 * 変更を保存 * を選択します。

Bucket options

Bucket access

Platform services

Replication

Disabled

▼

Event notifications

Disabled

▲

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

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

☒ Enable event notifications

Clear

```

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

```

Save changes



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

7. イベント通知が正しく設定されていることを確認します。

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

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

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

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

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

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

されています。

関連情報

["バケットの通知の概要"](#)

["S3 を使用する"](#)

["プラットフォームサービスエンドポイントの作成"](#)

検索統合サービスを使用する

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

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



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

次のカスタムの StorageGRID S3 REST API 処理の詳細については、S3 クライアントアプリケーションを実装する手順を参照してください。

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

関連情報

["検索統合用の XML を設定します"](#)

["メタデータ通知に含まれているオブジェクトメタデータ"](#)

["検索統合サービスで生成される JSON"](#)

["検索統合サービスの設定"](#)

["S3 を使用する"](#)

検索統合用の XML を設定します

検索統合サービスは、内に含まれる一連のルールを使用して設定します

`<MetadataNotificationConfiguration>` および

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

オブジェクトはオブジェクト名のプレフィックスでフィルタリングできます。たとえば、というプレフィックスのオブジェクトのメタデータを送信できます /images を1つのデスティネーションに、プレフィックスがのオブジェクトのメタデータに追加します /videos 別のノードに移動しますプレフィックスが重複している設定は無効で、送信時に拒否されます。たとえば、プレフィックスがのオブジェクトに対するルールを1つ含む設定です test プレフィックスが付いたオブジェクトの2番目のルールです test2 は許可されていません。

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

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

次の表に、メタデータ通知設定 XML の要素を示します。

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

名前	説明	必須
ID	<p>ルールの一意的識別子。</p> <p>Rule 要素に含まれています。</p>	いいえ
ステータス	<p>Status には「Enabled」または「Disabled」を指定できます。無効になっているルールについては操作が実行されません。</p> <p>Rule 要素に含まれています。</p>	はい。
プレフィックス	<p>プレフィックスと一致するオブジェクトにルールが適用され、そのメタデータが指定したデスティネーションに送信されます。</p> <p>すべてのオブジェクトを照合するには、空のプレフィックスを指定します。</p> <p>Rule 要素に含まれています。</p>	はい。
宛先	<p>ルールのデスティネーションのコンテナタグ。</p> <p>Rule 要素に含まれています。</p>	はい。
URN	<p>オブジェクトメタデータが送信されるデスティネーションの URN。次のプロパティを持つ StorageGRID エンドポイントの URN を指定する必要があります。</p> <ul style="list-style-type: none"> • es 3 番目のエレメントである必要があります。 • URNの末尾に、メタデータが格納されるインデックスとタイプを、の形式で指定する必要があります domain-name/myindex/mytype。 <p>エンドポイントは、Tenant Manager またはテナント管理 API を使用して設定します。形式は次のとおりです。</p> <ul style="list-style-type: none"> • arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype • urn:mysite:es:::mydomain/myindex/mytype <p>エンドポイントは設定 XML を送信する前に設定する必要があります。そうしないと、404 エラーで設定が失敗します。</p> <p>Urn は Destination 要素に含まれています。</p>	はい。

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

メタデータ通知設定：環境 のすべてのオブジェクトを対象にした設定です

この例では、すべてのオブジェクトのオブジェクトメタデータが同じデスティネーションに送信されます。

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

2 つのルールを含むメタデータ通知設定

この例では、プレフィックスに一致するオブジェクトのオブジェクトメタデータを指定します /images が1つのデスティネーションに送信され、プレフィックスに一致するオブジェクトのオブジェクトメタデータが送信されます /videos 2番目の送信先に送信されます。

```
<MetadataNotificationConfiguration>
  <Rule>
    <ID>Images-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/images</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-1:33333333:domain/es-
domain/graphics/imagetype</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Videos-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/videos</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

関連情報

"S3 を使用する"

"検索統合サービスで生成される JSON"

"検索統合サービスの設定"

検索統合サービスの設定

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

必要なもの

- テナントアカウントのプラットフォームサービスが StorageGRID 管理者によって有効化されている必要があります。
- コンテンツにインデックスを付ける S3 バケットを作成しておく必要があります。
- 検索統合サービスのデスティネーションとして使用するエンドポイントが存在し、その URN を把握している必要があります。
- テナントアカウント内のすべての S3 バケットの設定を管理できるように、Manage All Buckets 権限または Root Access 権限を持つユーザグループに属している必要があります。これらの権限は、Tenant Manager を使用してバケットを設定する際にグループポリシーまたはバケットポリシーの権限設定よりも優先されます。

このタスクについて

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

手順

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

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

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

3. ソースバケットの名前を選択します。

バケットの詳細ページが表示されます。

4. プラットフォームサービス > 検索統合 * を選択します

5. 検索統合を有効にする * チェックボックスをオンにします。

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

Bucket options

Bucket access

Platform services

Replication

Disabled

▼

Event notifications

Disabled

▼

Search integration

Disabled

▲

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

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

☒ Enable search integration

Clear

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

Save changes



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

7. 検索統合サービスが正しく設定されていることを確認します。

- a. 設定 XML で指定されたメタデータ通知をトリガーする要件を満たすオブジェクトをソースバケットに追加します。

前述の例では、バケットに追加されたすべてのオブジェクトがメタデータ通知をトリガーします。

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

完了後

必要に応じて、次のいずれかの方法でバケットの検索統合を無効にできます。

- Storage (S3) * > * Buckets * を選択し、* Enable search integration * チェックボックスの選択を解除します。
- S3 API を直接使用している場合は、DELETE Bucket メタデータ通知要求を使用します。S3 クライアントアプリケーションを実装する手順を参照してください。

関連情報

["検索統合サービスの概要"](#)

["検索統合用の XML を設定します"](#)

["S3 を使用する"](#)

["プラットフォームサービスエンドポイントの作成"](#)

検索統合サービスで生成される **JSON**

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

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

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

メタデータ通知に含まれているオブジェクトメタデータ

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

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

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

を入力します	項目名と概要
タグ	tags:オブジェクトに定義されているすべてのオブジェクトタグをキーと値のペアとして使用します key:value



タグとユーザメタデータの場合、StorageGRID は文字列または S3 イベント通知として Elasticsearch に日付と番号を渡します。これらの文字列を日付または数値として解釈するように Elasticsearch を設定するには、動的フィールドマッピングおよびマッピング日付形式に関する Elasticsearch の手順に従ってください。検索統合サービスを設定する前に、インデックスの動的フィールドマッピングを有効にする必要があります。ドキュメントにインデックスを付けた後は、インデックス内のドキュメントのフィールドタイプを編集できません。

S3 を使用する

クライアントアプリケーションでS3 APIを使用して、StorageGRID システムを操作する方法を説明します。

- ["S3 REST APIのサポート"](#)
- ["テナントアカウントと接続を設定する"](#)
- ["StorageGRID でのS3 REST APIの実装"](#)
- ["S3 REST API のサポートされる処理と制限事項"](#)
- ["StorageGRID の S3 REST API の処理"](#)
- ["バケットとグループのアクセスポリシー"](#)
- ["REST APIのセキュリティの設定"](#)
- ["処理の監視と監査"](#)
- ["アクティブ、アイドル、および同時 HTTP 接続のメリット"](#)

S3 REST APIのサポート

StorageGRID は、Representational State Transfer（REST）の Web サービスのセットとして実装される Simple Storage Service（S3）をサポートします。S3 REST API のサポートにより、S3 Web サービス用に開発されたサービス指向アプリケーションを、StorageGRID システムを使用するオンプレミスのオブジェクトストレージと接続できます。クライアントアプリケーションで現在使用している S3 REST API 呼び出しの変更は、最小限しか必要ありません。

- ["S3 REST API のサポートに関する変更点"](#)
- ["サポートされるバージョン"](#)
- ["StorageGRID プラットフォームサービスのサポート"](#)

S3 REST API のサポートに関する変更点

StorageGRID システムでの S3 REST API のサポートに関する変更点に注意する必要があります。

リリース。	コメント
11.5	<ul style="list-style-type: none">• バケットの暗号化の管理のサポートが追加されました。• S3 オブジェクトのロックと廃止された従来の準拠要求のサポートを追加しました。• バージョン管理されたバケットでの DELETE Multiple Objects の使用のサポートが追加されました。• 。 Content-MD5 要求ヘッダーが正しくサポートされるようになりました。
11.4	<ul style="list-style-type: none">• DELETE Bucket tagging 、 GET Bucket tagging 、 PUT Bucket tagging のサポートが追加されました。コスト割り当てタグはサポートされていません。• StorageGRID 11.4 で作成されたバケットでは、オブジェクトキー名がパフォーマンスのベストプラクティスに適合するように制限する必要はなくなりました。• でバケット通知のサポートが追加されました <code>s3:ObjectRestore:Post</code> イベントタイプ。• マルチパートの AWS サイズの上限が適用されるようになりました。マルチパートアップロードの各パートのサイズは 5MiB から 5GiB の間にする必要があります。最後の部分は 5MiB より小さくすることができます。• TLS 1.3 のサポートの追加、およびサポートされる TLS 暗号スイートのリストの更新。• CLB サービスは廃止されました。

リリース。	コメント
11.3	<ul style="list-style-type: none"> • ユーザ指定のキーによるオブジェクトデータのサーバー側暗号化（SSE-C）がサポートされるようになりました。 • DELETE Bucket lifecycle、GET Bucket lifecycle、PUT Bucket lifecycleの各処理（Expirationアクションのみ）とがサポートされるようになりました x-amz-expiration 応答ヘッダー。 • PUT Object 、 PUT Object - Copy 、 Multipart Upload が更新されて、取り込み時に同期配置を使用する ILM ルールの影響を受けるようになりました。 • サポートされる TLS 暗号スイートのリストが更新されました。TLS 1.1 暗号はサポートされなくなりました。
11.2	<p>クラウドストレージプールで POST Object restore を使用できるようになりました。グループポリシーとバケットポリシーの ARN 、ポリシー条件キー、およびポリシー変数で AWS 構文を使用できるようになりました。StorageGRID 構文を使用する既存のグループポリシーとバケットポリシーは引き続きサポートされます。</p> <ul style="list-style-type: none"> • 注：カスタム StorageGRID 機能で使用する ARN やその他の構成 JSON / XML での使用に変更はありませんでした。
11.1	Cross-Origin Resource Sharing （ CORS ） 、グリッドノードへの S3 クライアント接続での HTTP の使用、バケットでの準拠設定がサポートされるようになりました。
11.0	バケットでのプラットフォームサービス（CloudMirror レプリケーション、通知、および Elasticsearch 検索統合）の設定がサポートされるようになりました。また、バケットに対するオブジェクトタグ付け機能の場所の制約、および整合性制御設定「available」がサポートされるようになりました。
10.4.	ILM スキャンのバージョン管理、エンドポイントドメインの名前ページの更新、ポリシーの条件と変数、ポリシーの例、および PutOverwriteObject 権限の変更のサポートが追加されました。
10.3	バージョン管理のサポートが追加されました。

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

サポートされるバージョン

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

項目	バージョン
S3 仕様	_Simple Storage Service API Reference_ 2006-03-01
HTTP	1.1 HTTP の詳細については、HTTP/1.1（RFC 7230~7235）を参照してください。 • 注：StorageGRID は、HTTP/1.1 パイプラインをサポートしません。

関連情報

"[IETF RFC 2616](#)：『Hypertext Transfer Protocol（HTTP/1.1）』"

"[Amazon Web Services（AWS）ドキュメント](#)：「[Amazon Simple Storage Service API Reference](#)」"

StorageGRID プラットフォームサービスのサポート

StorageGRID プラットフォームサービスでは、StorageGRID のテナントアカウントでリモート S3 バケット、Simple Notification Service（SNS）エンドポイント、Elasticsearch クラスタなどの外部サービスを利用して、グリッドが提供するサービスを拡張できます。

次の表に、使用可能なプラットフォームサービスとその設定に使用する S3 API を示します。

プラットフォームサービス	目的	サービスの設定に使用する S3 API
CloudMirror レプリケーション	ソースの StorageGRID バケットから、設定したリモートの S3 バケットにオブジェクトをレプリケートします。	PUT Bucket replication
通知	ソースの StorageGRID バケットでのイベントに関する通知を、設定した Simple Notification Service (SNS) エンドポイントに送信します。	PUT Bucket notification
検索統合	StorageGRID バケットに格納されているオブジェクトメタデータを、設定した Elasticsearch インデックスに送信します。	PUT Bucket metadata notification <ul style="list-style-type: none"> 注：* これは StorageGRID のカスタム S3 API です。

グリッド管理者がテナントアカウントでプラットフォームサービスの使用を有効にするには、事前にプラットフォームサービスを使用できるようにする必要があります。その後、テナント管理者が、テナントアカウントのリモートサービスを表すエンドポイントを作成する必要があります。この手順は、サービスを設定する前に実行する必要があります。

プラットフォームサービスの使用に関する推奨事項

プラットフォームサービスを使用する前に、次の推奨事項を確認してください。

- CloudMirror のレプリケーション、通知、検索統合を必要とする S3 要求ではアクティブなテナントが 100 個を超えないようにすることを推奨します。アクティブなテナントが 100 を超えると、S3 クライアントのパフォーマンスが低下する可能性があります。
- StorageGRID システムの S3 バケットで、バージョン管理と CloudMirror レプリケーションの両方が有効になっている場合は、デスティネーションエンドポイントでも S3 バケットのバージョン管理を有効にすることを推奨します。これにより、CloudMirror レプリケーションでエンドポイントに同様のオブジェクトバージョンを生成できます。
- ソースバケットで S3 オブジェクトのロックが有効になっている場合、CloudMirror レプリケーションはサポートされません。
- デスティネーションバケットでレガシー準拠が有効になっていると、CloudMirror レプリケーションは AccessDenied エラーで失敗します。

関連情報

["テナントアカウントを使用する"](#)

["StorageGRID の管理"](#)

["バケットの処理"](#)

["PUT Bucket metadata notification configuration 要求"](#)

テナントアカウントと接続を設定する

クライアントアプリケーションからの接続を受け入れるように StorageGRID を設定するには、テナントアカウントを 1 つ以上作成し、接続を設定する必要があります。

S3 テナントアカウントを作成および設定する

S3 API クライアントが StorageGRID でオブジェクトの格納や読み出しを行うには、S3 テナントアカウントが必要です。各テナントアカウントには、専用のアカウント ID、専用のグループとユーザ、および専用のコンテナとオブジェクトがあります。

S3 テナントアカウントは、StorageGRID のグリッド管理者がグリッドマネージャまたはグリッド管理 API を使用して作成します。グリッド管理者は、S3 テナントアカウントを作成する際に次の情報を指定します。

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

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

- アイデンティティフェデレーションを設定し（グリッドとアイデンティティソースを共有する場合を除く）、ローカルグループとユーザを作成します
- S3 アクセスキーを管理します
- S3 オブジェクトロックが有効になっているバケットを含む S3 バケットを作成して管理します
- プラットフォームサービスを使用する（有効な場合）
- ストレージの使用状況を監視



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

関連情報

["StorageGRID の管理"](#)

["テナントアカウントを使用する"](#)

クライアント接続の設定方法

グリッド管理者は、S3 クライアントがデータの格納と読み出しを行うために StorageGRID に接続する方法に関連する設定を行います。接続するために必要な具体的な情報は、選択した設定によって異なります。

クライアントアプリケーションは、次のいずれかに接続することで、オブジェクトを格納または読み出すことができます。

- 管理ノードまたはゲートウェイノード上のロードバランササービス、または必要に応じて、管理ノードまたはゲートウェイノードのハイアベイラビリティ（HA）グループの仮想 IP アドレス
- ゲートウェイノード上の CLB サービス、または必要に応じて、ゲートウェイノードのハイアベイラビリティグループの仮想 IP アドレス



CLB サービスは廃止されました。StorageGRID 11.3 より前に設定されたクライアントは、ゲートウェイノード上の CLB サービスを引き続き使用できます。ロードバランシングに StorageGRID を使用する他のすべてのクライアントアプリケーションは、ロードバランササービスを使用して接続する必要があります。

- 外部ロードバランサを使用するかどうかに関係なく、ストレージノードに追加されます

StorageGRID を設定する場合、グリッド管理者はグリッドマネージャまたはグリッド管理 API を使用して次の手順を実行できます。これらはすべてオプションです。

1. ロードバランササービスのエンドポイントを設定する。

ロードバランササービスを使用するようにエンドポイントを設定する必要があります。管理ノードまたはゲートウェイノード上のロードバランササービスは、クライアントアプリケーションからの受信ネットワーク接続を複数のストレージノードに分散します。ロードバランサエンドポイントを作成する際、StorageGRID 管理者は、ポート番号、エンドポイントで HTTP / HTTPS 接続を許可するかどうか、エンドポイントを使用するクライアントのタイプ（S3 または Swift）、HTTPS 接続に使用する証明書（該当する場合）を指定します。

2. 信頼されていないクライアントネットワークを設定する

StorageGRID 管理者がノードのクライアントネットワークを信頼されていないクライアントネットワークとして設定した場合、ノードはロードバランサエンドポイントとして明示的に設定されたポートでクライアントネットワークのインバウンド接続だけを受け入れます。

3. ハイアベイラビリティグループを設定する。

管理者が HA グループを作成すると、複数の管理ノードまたはゲートウェイノードのネットワークインターフェイスがアクティブ / バックアップ構成になります。クライアント接続は、HA グループの仮想 IP アドレスを使用して確立されます。

各オプションの詳細については、StorageGRID の管理手順を参照してください。

関連情報

["StorageGRID の管理"](#)

Summary：クライアント接続の IP アドレスとポート

クライアントアプリケーションは、グリッドノードの IP アドレスおよびそのノード上のサービスのポート番号を使用して StorageGRID に接続します。ハイアベイラビリティ（HA）グループが設定されている場合は、HA グループの仮想 IP アドレスを使用してクライアントアプリケーションを接続できます。

クライアント接続に必要な情報

次の表に、クライアントが StorageGRID に接続できるさまざまな方法、および各接続タイプで使用される IP アドレスとポートを示します。詳細については、StorageGRID 管理者にお問い合わせください。または、StorageGRID for a 概要 の管理手順を参照して、グリッドマネージャでこの情報を確認してください。

接続が確立される場所	クライアントが接続するサービス	IP アドレス	ポート
HA グループ	ロードバランサ	HA グループの仮想 IP アドレス	• ロードバランサエンドポイントのポート
HA グループ	CLB の機能です • 注： ** CLB サービスは廃止されました。	HA グループの仮想 IP アドレス	デフォルトの S3 ポート： • HTTPS：8082 • HTTP：8084
管理ノード	ロードバランサ	管理ノードの IP アドレス	• ロードバランサエンドポイントのポート
ゲートウェイノード	ロードバランサ	ゲートウェイノードの IP アドレス	• ロードバランサエンドポイントのポート
ゲートウェイノード	CLB の機能です • 注： ** CLB サービスは廃止されました。	ゲートウェイノードの IP アドレス • 注： ** CLB および LDR の HTTP ポートはデフォルトでは有効になっていません。	デフォルトの S3 ポート： • HTTPS：8082 • HTTP：8084
ストレージノード	LDR	ストレージノードの IP アドレス	デフォルトの S3 ポート： • HTTPS：18082 • HTTP：18084

例

ゲートウェイノードの HA グループのロードバランサエンドポイントに S3 クライアントを接続するには、次のように構造化された URL を使用します。

- `https://VIP-of-HA-group:_LB-endpoint-port_`

たとえば、HA グループの仮想 IP アドレスが 192.0.2.5 で S3 ロードバランサエンドポイントのポート番号が 10443 の場合、S3 クライアントは次の URL を使用して StorageGRID に接続できます。

- `https://192.0.2.5:10443`

クライアントが StorageGRID への接続に使用する IP アドレスに DNS 名を設定できます。ローカルネットワーク管理者にお問い合わせください。

関連情報

["StorageGRID の管理"](#)

HTTPS接続とHTTP接続のどちらを使用するか判断

ロードバランサエンドポイントを使用してクライアント接続を行う場合は、そのエンドポイントに指定されているプロトコル（HTTP または HTTPS）を使用して接続を確立する必要があります。ストレージノードへのクライアント接続またはゲートウェイノード上の CLB サービスへのクライアント接続に HTTP を使用する場合は、HTTP の使用を有効にする必要があります。

デフォルトでは、クライアントアプリケーションがストレージノードまたはゲートウェイノード上の CLB サービスに接続する場合、クライアントアプリケーションはすべての接続に暗号化された HTTPS を使用する必要があります。必要に応じて、Grid Manager で * Enable HTTP Connection * grid オプションを選択して、セキュアでない HTTP 接続を有効にすることができます。たとえば、非本番環境でストレージノードへの接続をテストする際に、クライアントアプリケーションで HTTP を使用できます。



要求が暗号化されずに送信されるため、本番環境のグリッドで HTTP を有効にする場合は注意してください。



CLB サービスは廃止されました。

[Enable HTTP Connection*] オプションが選択されている場合、クライアントは HTTPS とは異なるポートを HTTP に使用する必要があります。StorageGRID の管理手順を参照してください。

関連情報

["StorageGRID の管理"](#)

["アクティブ、アイドル、および同時 HTTP 接続のメリット"](#)

S3 要求のエンドポイントのドメイン名

クライアント要求に S3 ドメイン名を使用できるようにするには、S3 パス形式と S3 仮想ホスト形式の要求で S3 ドメイン名を使用する接続を受け入れるように StorageGRID 管理者がシステムを設定する必要があります。

このタスクについて

S3 仮想ホスト形式の要求を使用できるようにするには、グリッド管理者が次のタスクを実行する必要があります。

- Grid Manager を使用して、S3 エンドポイントのドメイン名を StorageGRID システムに追加します。

- クライアントが StorageGRID への HTTPS 接続に使用する証明書が、クライアントが必要とするすべてのドメイン名に対して署名されていることを確認します。

たとえば、エンドポイントがの場合などです `s3.company.com`、グリッド管理者は、HTTPS接続に使用される証明書にが含まれていることを確認する必要があります `s3.company.com` エンドポイントとエンドポイントのワイルドカードSubject Alternative Name (SAN) : `*.s3.company.com`

- クライアントが使用する DNS サーバを設定して、必要なワイルドカードレコードを含め、エンドポイントのドメイン名と一致する DNS レコードを含めます。

クライアントがロードバランササービスを使用して接続する場合、グリッド管理者は、クライアントが使用するロードバランサエンドポイントの証明書を設定します。



各ロードバランサエンドポイントには独自の証明書があり、異なるエンドポイントドメイン名を認識するように各エンドポイントを設定できます。

クライアントがストレージノードに接続する場合、またはゲートウェイノード上のCLBサービスに接続する場合、グリッド管理者は、グリッドに使用される単一のカスタムサーバ証明書を設定します。



CLB サービスは廃止されました。

詳細については、StorageGRID の管理手順を参照してください。

上記の手順が完了したら、仮想ホスト形式の要求 (`bucket.s3.company.com`)。

関連情報

["StorageGRID の管理"](#)

["REST APIのセキュリティの設定"](#)

S3 REST APIの設定のテスト

Amazon Web Services コマンドラインインターフェイス (AWS CLI) を使用してシステムへの接続をテストし、システムに対するオブジェクトの読み取りと書き込みが可能であることを確認できます。

必要なもの

- AWS CLIをからダウンロードしてインストールしておく必要があります ["aws.amazon.com/cli"](https://aws.amazon.com/cli)。
- StorageGRID システムでS3テナントアカウントを作成しておく必要があります。

手順

1. Amazon Web Services の設定で、StorageGRID システムで作成したアカウントを使用するように設定します。
 - a. コンフィギュレーションモードを開始します。 `aws configure`
 - b. 作成したアカウントの AWS アクセスキー ID を入力します。
 - c. 作成したアカウントの AWS 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 (`us-east-1` など) を入力します。
 - 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. バケットを作成する。

```
aws s3api --endpoint-url https://10.96.101.17:10443
--no-verify-ssl create-bucket --bucket testbucket
```

バケットの作成が完了すると、次の例のようにバケットの場所が返されます。

```
"Location": "/testbucket"
```

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
```

オブジェクトのアップロードが完了すると、オブジェクトデータのハッシュである Etag が返されます。

4. バケットの内容をリストして、オブジェクトがアップロードされたことを確認します。

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
list-objects --bucket testbucket
```

5. オブジェクトを削除します。

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-object --bucket testbucket --key s3.pdf
```

6. バケットを削除します。

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-bucket --bucket testbucket
```

StorageGRID でのS3 REST APIの実装

クライアントアプリケーションは、S3 REST API呼び出しを使用してStorageGRID に接続し、バケットの作成、削除、変更、およびオブジェクトの格納と読み出しを行うことができます。

- "競合するクライアント要求です"
- "整合性制御"
- "StorageGRID の ILM ルールによるオブジェクトの管理"

- ["オブジェクトのバージョン管理"](#)
- ["S3 REST APIを実装する際の推奨事項"](#)

競合するクライアント要求です

同一キーに書き込む2つのクライアントなど'競合するクライアント要求は'最新のWINS形式で解決されます

「latest-wins」評価のタイミングは、S3クライアントが処理を開始するタイミングではなく、StorageGRIDシステムが特定の要求を完了したタイミングに基づいています。

整合性制御

整合性制御では、アプリケーションでの必要に応じて、オブジェクトの可用性と、異なるストレージノード間およびサイト間でのオブジェクトの整合性のどちらかを犠牲にしなければなりません。

StorageGRID では、デフォルトで、新しく作成したオブジェクトのリードアフターライト整合性が保証されます。正常に完了した PUT に続く GET では、新しく書き込まれたデータを読み取ることができます。既存のオブジェクトの上書き、メタデータの更新、および削除の整合性レベルは、結果整合性です。上書きは通常、数秒から数分で反映されますが、最大で 15 日かかることがあります。

別の整合性レベルでオブジェクトの処理を実行する場合は、各バケットまたは各 API 処理に対して整合性制御を指定できます。

整合性制御

整合性制御は、StorageGRID がオブジェクトの追跡に使用するメタデータがノード間に分散される方法、つまりクライアント要求で利用できるオブジェクトの有無に影響します。

バケットまたは API 処理の整合性制御は、次のいずれかの値に設定できます。

整合性制御	説明
すべて	すべてのノードが即座にデータを受け取り、受け取れない場合は要求が失敗します。
strong-global	すべてのサイトのすべてのクライアント要求について、リードアフターライト整合性が保証されます。
strong-site	1つのサイト内のすべてのクライアント要求について、リードアフターライト整合性が保証されます。

整合性制御	説明
read-after-new-write の場合	<p>(デフォルト) 新規オブジェクトにはリードアフターライト整合性を、オブジェクトの更新には結果整合性を提供します。高可用性が確保され、データ保護が保証されます。Amazon S3の整合性に相当します。</p> <ul style="list-style-type: none"> 注：存在しないオブジェクトに対してアプリケーションが HEAD 要求を使用すると、使用できないストレージノードがあると「500 Internal Server Error」が大量に返される可能性があります。これらのエラーを回避するには、Amazon S3 と同様の整合性の保証が必要でない限り、整合性制御を「available」に設定します。
available （HEAD 処理は結果整合性）	<p>「read-after-new-write」整合性レベルと動作は同じですが、HEAD 処理については結果整合性のみを提供します。ストレージ・ノードが使用できない場合、リードアフター・新規ライトよりもヘッド操作の可用性が高くなりますAmazon S3 の整合性と異なるのは HEAD 処理のみです。</p>

「read-after-new-write」および「available」整合性制御を使用する

HEAD操作またはGET操作で「read-after-new-write」整合性制御を使用する場合、またはGET操作で「available」整合性制御を使用する場合、StorageGRID は次のように複数の手順で検索を実行します。

- まず、低い整合性レベルを使用してオブジェクトを検索します。
- このルックアップが失敗すると、最も高い整合性レベル「all」に到達するまで、次の整合性レベルでルックアップが繰り返されます。このとき、オブジェクトメタデータのすべてのコピーが使用可能になります。

HEAD 操作または GET 操作で「read-after-new-write」整合性制御が使用されているが、オブジェクトが存在しない場合、オブジェクトの検索は常に「all」整合性レベルに到達します。この整合性レベルでは、オブジェクトのメタデータのすべてのコピーが利用可能である必要があるため、使用できないストレージノードがあると、500 Internal Server Error が大量に発生する場合があります。

Amazon S3と同様の整合性の保証が必要でない限り、整合性制御を「available」に設定することで、HEAD処理でのこれらのエラーを防ぐことができます。HEAD処理で「available」整合性制御を使用すると、StorageGRID は結果整合性のみを提供します。整合性レベルが「all」に達するまで失敗した処理は再試行されないため、オブジェクトメタデータのすべてのコピーが利用可能である必要はありません。

API処理に対する整合性制御の指定

個々の API 処理に対して整合性制御を設定するには、その処理でサポートされている整合性制御を要求ヘッダーで指定する必要があります。次の例では、GET Object 処理に対して、整合性制御を「strong-site」に設定しています。

```
GET /bucket/object HTTP/1.1
Date: date
Authorization: <em>authorization name</em>
Host: <em>host</em>
Consistency-Control: strong-site
```



PUT Object 処理と GET Object 処理には、同じ整合性制御を使用する必要があります。

バケットの整合性制御の指定

バケットに対して整合性制御を設定するには、StorageGRID の PUT Bucket 整合性要求および GET Bucket 整合性要求を使用できます。または、Tenant Manager またはテナント管理 API を使用できます。

バケットの整合性制御を設定する際は、次の点に注意してください。

- バケットの整合性制御を設定することで、バケット内のオブジェクトまたはバケット設定に対して実行される S3 処理に、どの整合性制御を使用するかを指定できます。バケット自体に対する処理には影響しません。
- 個々の API 処理の整合性制御は、バケットの整合性制御よりも優先されます。
- 通常、バケットはデフォルトの整合性制御「read-after-new-write」を使用する必要があります。要求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、API 要求ごとに整合性制御を指定するようにクライアントを設定します。バケットレベルの整合性制御は最後の手段と考えてください。

整合性制御と ILM ルールの相互作用によるデータ保護への影響

整合性制御と ILM ルールのどちらを選択した場合も、オブジェクトの保護方法に影響します。これらの設定は対話的に操作できます。

たとえば、オブジェクトの格納に使用される整合性制御はオブジェクトメタデータの初期配置に影響し、ILM ルールで選択される取り込み動作はオブジェクトコピーの初期配置に影響します。StorageGRID では、クライアント要求に対応するためにオブジェクトのメタデータとそのデータの両方にアクセスするため、整合性レベルと取り込み動作に一致する保護レベルを選択することで、より適切な初期データ保護と予測可能なシステム応答を実現できます。

ILM ルールでは、次の取り込み動作を使用できます。

- *** Strict *** : ILM ルールに指定されたすべてのコピーを作成しないと、クライアントに成功が返されません。
- *** Balanced *** : StorageGRID は、取り込み時に ILM ルールで指定されたすべてのコピーを作成しようとします。作成できない場合、中間コピーが作成されてクライアントに成功が返されます。可能な場合は、ILM ルールで指定されたコピーが作成されます。
- *** デュアルコミット *** : StorageGRID はオブジェクトの中間コピーをただちに作成し、クライアントに成功を返します。可能な場合は、ILM ルールで指定されたコピーが作成されます。



ILM ルールの取り込み動作を選択する前に、情報ライフサイクル管理を使用してオブジェクトを管理する手順の設定の完全な概要を確認してください。

次の ILM ルールと次の整合性レベル設定の 2 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、2 つのオブジェクトコピーを作成します。Strict 取り込み動作が選択されています。
- * 整合性レベル *: "Strong-GLOBAL" (オブジェクトメタデータはすべてのサイトにただちに分散されます)

クライアントがオブジェクトをグリッドに格納すると、StorageGRID は両方のオブジェクトをコピーし、両方のサイトにメタデータを分散してからクライアントに成功を返します。

オブジェクトは、取り込みが成功したことを示すメッセージが表示された時点で損失から完全に保護されます。たとえば、取り込み直後にローカルサイトが失われた場合、オブジェクトデータとオブジェクトメタデータの両方のコピーがリモートサイトに残っています。オブジェクトを完全に読み出し可能にしている。

代わりに同じ ILM ルールと「strong-site」整合性レベルを使用する場合は、オブジェクトデータがリモートサイトにレプリケートされたあとで、オブジェクトメタデータが分散される前に、クライアントに成功メッセージが送信され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がオブジェクトデータの保護レベルと一致しません。取り込み直後にローカルサイトが失われると、オブジェクトメタデータが失われます。オブジェクトを読み出すことができません。

整合性レベルと ILM ルールの間の関係は複雑になる可能性があります。サポートが必要な場合は、ネットアップにお問い合わせください。

関連情報

["ILM を使用してオブジェクトを管理する"](#)

["GET Bucket consistency 要求を実行します"](#)

["PUT Bucket consistency 要求"](#)

StorageGRID の ILM ルールによるオブジェクトの管理

グリッド管理者が情報ライフサイクル管理 (ILM) ルールを作成して、S3 REST API クライアントアプリケーションから StorageGRID システムに取り込まれたオブジェクトデータを管理します。これらのルールは、以降のオブジェクトデータを格納する方法と場所を指定するために、ILM ポリシーに追加されます。

ILM の設定によって、オブジェクトの次の要素が決まります。

- * 地域 *

StorageGRID システム (ストレージプール) 内またはクラウドストレージプール内のオブジェクトのデータの場所。

- * ストレージグレード *

フラッシュや回転式ディスクなど、オブジェクトデータの格納に使用されるストレージのタイプ。

- * 損失の保護 *

作成されるコピーの数と作成されるコピーのタイプ (レプリケーション、イレイジャーコーディング、ま

たはその両方)。

- * 保持 *

オブジェクトのデータの管理方法、格納場所、損失からの保護方法の経過時間に応じて変更が加えられます。

- * 取り込み中の保護 *

取り込み時にオブジェクトデータを保護する方法。同期配置（取り込み動作に Balanced オプションまたは Strict オプションを使用）または中間コピー作成（Dual commit オプションを使用）のいずれかです。

ILM ルールではオブジェクトをフィルタして選択できます。S3 を使用して取り込まれたオブジェクトは、ILM ルールによって次のメタデータに基づいてフィルタできます。

- テナントアカウント
- バケット名
- 取り込み時間
- キーを押します
- 最終アクセス時間



デフォルトでは、すべての S3 バケットで最終アクセス時間の更新が無効になっています。StorageGRID システムに Last Access Time オプションを使用する ILM ルールが含まれている場合は、そのルールで指定される S3 バケットで最終アクセス時間の更新を有効にする必要があります。最終アクセス時間の更新を有効にするには、Tenant Manager の PUT Bucket last access time 要求、* S3 * > * Buckets * > * Configure Last Access Time * チェックボックス、またはテナント管理 API を使用します。最終アクセス時間の更新を有効にする場合は、特に小さなオブジェクトを含むシステムで StorageGRID のパフォーマンスが低下する可能性があることに注意してください。

- 場所の制約
- オブジェクトサイズ
- ユーザメタデータ
- オブジェクトタグ

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

関連情報

["テナントアカウントを使用する"](#)

["ILM を使用してオブジェクトを管理する"](#)

["PUT Bucket last access time 要求の場合"](#)

オブジェクトのバージョン管理

バージョン管理の機能を使用してオブジェクトの複数のバージョンを保持することで、

オブジェクトが偶発的に削除される事態に対応したり、以前のバージョンのオブジェクトを読み出してリストアしたりできます。

StorageGRID システムでは、バージョン管理のほとんどの機能をサポートしていますが、いくつかの制限事項があります。StorageGRID では、オブジェクトごとに最大 1、000 個のバージョンをサポートしています。

オブジェクトのバージョン管理は、StorageGRID の情報ライフサイクル管理 (ILM) または S3 バケットのライフサイクル設定と組み合わせることができます。バケットでバージョン管理機能を有効にするには、各バケットに対して明示的に有効にする必要があります。バケット内の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) Delete の使用はサポートされていません。



バージョン管理は、StorageGRID バージョン 10.3 以降で作成されたバケットでのみ有効にすることができます。

ILM とバージョン管理

ILM ポリシーはオブジェクトの各バージョンに適用されます。ILM のスキャン処理では、すべてのオブジェクトが継続的にスキャンされ、現在の ILM ポリシーに照らして再評価されます。ILM ポリシーに対する変更は、それまでに取り込まれたすべてのオブジェクトに適用されます。バージョン管理が有効になっている場合は、それまでに取り込まれたバージョンも対象に ILM のスキャン処理により、過去に取り込まれたオブジェクトに変更後の新しい ILM の内容が適用さ

バージョン管理が有効なバケット内の S3 オブジェクトに対しては、参照時間として noncurrent Time を使用する ILM ルールを作成できます。オブジェクトが更新されると、それまでのバージョンは noncurrent になります。noncurrent の時間フィルタを使用することで、旧バージョンのオブジェクトによるストレージへの影響を軽減するポリシーを作成できます。



マルチパートアップロード処理を使用してオブジェクトの新しいバージョンをアップロードすると、オブジェクトの元のバージョンの noncurrent の時間には、マルチパートアップロードの完了時ではなく、新しいバージョンのマルチパートアップロードが作成された時点が反映されます。ただし、オリジナルバージョンの最新でない時間は、現行バージョンの時間よりも数時間 ~ 数日早い場合があります。

S3 バージョン管理オブジェクトの ILM ポリシーの例については、情報ライフサイクル管理を使用してオブジェクトを管理する手順を参照してください。

関連情報

["ILM を使用してオブジェクトを管理する"](#)

S3 REST APIを実装する際の推奨事項

StorageGRID で使用するために S3 REST API を実装する場合は、次の推奨事項を考慮してください。

存在しないオブジェクトに対する HEAD の推奨事項

オブジェクトが実際に存在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アプリケーションが定期的にチェックする場合は、使用可能な整合性制御を使用する必要がありますたとえば、アプリケーションが

その場所に配置する前にその場所に注意する場合は ' 利用可能な整合性制御を使用する必要があります

そうしないと、使用できないストレージノードがある場合に HEAD 処理でオブジェクトが見つからないと、「500 Internal Server Error」が大量に返される可能性があります。

PUT Bucket consistency 要求を使用して各バケットに「available」整合性制御を設定するか、または個々の API 処理の要求ヘッダーで整合性制御を指定できます。

オブジェクトキーの推奨事項

StorageGRID 11.4 以降で作成されたバケットでは、オブジェクトキー名をパフォーマンスのベストプラクティスに準拠するように制限する必要はなくなりました。たとえば、オブジェクトキー名の最初の 4 文字にランダムな値を使用できるようになりました。

StorageGRID 11.4 より前のリリースで作成されたバケットの場合は、オブジェクトキー名に関する次の推奨事項に進みます。

- オブジェクトキーの最初の 4 文字に、ランダムな値を使用しないでください。これは、AWS が以前に推奨していたキープレフィックスの推奨事項とは異なります。代わりに、などの一意ではないランダムなプレフィックスを使用してください image。
- AWS の以前の推奨事項に従ってキープレフィックスにランダムな一意の文字を使用する場合は、オブジェクトキーの前にディレクトリ名を指定してください。つまり、次の形式を使用します。

```
mybucket/mydir/f8e3-image3132.jpg
```

次の形式は使用しないでください。

```
mybucket/f8e3-image3132.jpg
```

「範囲の読み取り」に関する推奨事項

「格納オブジェクトの圧縮」オプション (* Configuration > Grid Options *) を選択した場合、S3 クライアントアプリケーションはバイト範囲を指定した GET Object 処理を実行しないでください。StorageGRID は要求されたバイトにアクセスするためにオブジェクトを圧縮解除する必要があるため、これらの “range read” 操作は非効率的です。非常に大きなオブジェクトから小さい範囲のバイト数を要求する GET Object 処理は特に効率が悪く、たとえば、50GB の圧縮オブジェクトから 10MB の範囲を読み取る処理は非常に非効率的です。

圧縮オブジェクトから範囲を読み取ると、クライアント要求がタイムアウトする可能性があります。



オブジェクトを圧縮する必要があり、クライアントアプリケーションが範囲読み取りを使用する必要がある場合は、アプリケーションの読み取りタイムアウトを増やしてください。

関連情報

["整合性制御"](#)

["PUT Bucket consistency 要求"](#)

["StorageGRID の管理"](#)

S3 REST API のサポートされる処理と制限事項

StorageGRID システムは Simple Storage Service API （ API バージョン 2006-03-01 ）を実装しており、ほとんどの処理をサポートしていますが、いくつかの制限事項があります。S3 REST API クライアントアプリケーションを統合するときは、実装の詳細を理解しておく必要があります。

StorageGRID システムでは、仮想ホスト形式の要求とパス形式の要求の両方がサポートされます。

- "要求の認証"
- "サービスの処理"
- "バケットの処理"
- "バケットのカスタム処理"
- "オブジェクトの処理"
- "マルチパートアップロードの処理"
- "エラー応答"

日付の処理

S3 REST API の StorageGRID 実装では、有効な HTTP の日付形式のみをサポートしています。

StorageGRID システムでは、日付の値を設定できるすべてのヘッダーで、有効な HTTP の日付形式のみがサポートされます。日付の時刻の部分は、Greenwich Mean Time （ GMT ；グリニッジ標準時）の形式で指定するか、タイムゾーンのオフセットなし（ +0000 を指定）の Universal Coordinated Time （ UTC ；協定世界時）の形式で指定できます。を指定する場合は x-amz-date 要求のヘッダー。Date要求ヘッダーで指定された値を上書きします。AWS署名バージョン4を使用している場合は、を参照してください x-amz-date 日付ヘッダーがサポートされていないため、署名済み要求にヘッダーが含まれている必要があります。

代表的な要求ヘッダー

StorageGRID システムでは、以下の例外を除き、_Simple Storage Service API Reference_ で定義されている共通の要求ヘッダーがサポートされます。

要求ヘッダー	実装
承認	<p>AWS 署名バージョン 2 は完全にサポートされます</p> <p>AWS 署名バージョン 4 は次の例外を除いてサポートされます。</p> <ul style="list-style-type: none">• 要求の本文の SHA256 の値は計算されません。ユーザが送信した値は、値の場合と同様に、検証なしで受け入れられます UNSIGNED-PAYLOAD は用に提供されていた x-amz-content-sha256 ヘッダー。

要求ヘッダー	実装
x-amz-security-token を指定します	実装されていませんを返します XNotImplemented。

共通の応答ヘッダー

StorageGRID システムでは、以下の例外を除き、_Simple Storage Service API Reference_で 定義されている共通の応答ヘッダーがすべてサポートされます。

応答ヘッダー	実装
x-amz-id-2	使用されません

関連情報

["Amazon Web Services（AWS）ドキュメント：「Amazon Simple Storage Service API Reference」](#)

要求の認証

StorageGRID システムでは、S3 API を使用したオブジェクトへのアクセスについて、認証アクセスと匿名アクセスの両方をサポートしています。

S3 API では、S3 API 要求の認証で署名バージョン 2 と署名バージョン 4 がサポートされます。

認証された要求は、アクセスキー ID とシークレットアクセスキーを使用して署名する必要があります。

StorageGRID システムでは、HTTPという2つの認証方式がサポートされています Authorization ヘッダーを使用し、クエリパラメータを使用する。

HTTP Authorizationヘッダーを使用する

HTTP Authorization ヘッダーは、バケットポリシーで許可された匿名の要求を除き、すべてのS3 API処理で使用されます。。 Authorization ヘッダーには、要求の認証に必要なすべての署名情報が含まれています。

クエリパラメータを使用する

クエリパラメータを使用すると、URL に認証情報を追加できます。これは署名付き URL と呼ばれ、特定のリソースへの一時的なアクセスを許可する場合に使用できます。署名付き URL を使用すると、シークレットアクセスキーを知らないユーザでもリソースにアクセスできるため、他のユーザに制限付きアクセスを提供することができます。

サービスの処理

StorageGRID システムでは、サービスに対して次の処理をサポートしています。

操作	実装
GET Service の略	Amazon S3 REST API のすべての動作が実装されています。
GET Storage Usage の略	GET Storage Usage 要求を使用すると、アカウントで使用しているストレージの総容量とアカウントに関連付けられているバケットごとの使用容量を確認できます。これは、パス/とカスタムクエリパラメータを使用したサービスに対する処理です (?x-ntap-sg-usage)が追加されました
オプション /	クライアントアプリケーションは問題 を実行できます OPTIONS / S3認証クレデンシャルを入力せずにストレージノード上のS3ポートに要求し、ストレージノードが使用可能かどうかを確認します。この要求は監視に使用できるほか、外部のロードバランサがストレージノードの停止を特定する目的でも使用できます。

関連情報

["GET Storage Usage 要求の略"](#)

バケットの処理

StorageGRID システムでは、 S3 テナントアカウントあたり最大 1、000 個のバケットがサポートされます。

バケット名については、AWS US Standard リージョンの制限が適用されますが、 S3 仮想ホスト形式の要求をサポートするために DNS の命名規則にも従う必要があります。

["Amazon Web Services （AWS）ドキュメント：「Bucket Restrictions and Limitations」"](#)

["S3要求のエンドポイントのドメイン名"](#)

GET Bucket （ List Objects ） 処理と GET Bucket versions 処理では、StorageGRID の整合性制御がサポートされます。

最終アクセス時間の更新が個々のバケットで有効になっているか無効になっているかを確認することができます。

次の表に、StorageGRID での S3 REST API バケット処理の実装方法を示します。これらの処理を実行するには、アカウントに必要なアクセスクレデンシャルが付与されている必要があります。

操作	実装
バケットを削除します	Amazon S3 REST API のすべての動作が実装されています。

操作	実装
バケットの CORS を削除します	この処理は、バケットの CORS 設定を削除します。
バケットの暗号化を削除	この処理は、バケットからデフォルトの暗号化を削除します。既存の暗号化オブジェクトは暗号化されたままですが、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。
バケットライフサイクルを削除	この処理は、バケットからライフサイクル設定を削除します。
バケットポリシーを削除	この処理は、バケットに関連付けられているポリシーを削除します。
バケットレプリケーションを削除します	この処理は、バケットに関連付けられているレプリケーション設定を削除します。
バケットのタグ付けを削除します	この処理にはを使用します tagging サブリソース：バケットからすべてのタグを削除します。
GET Bucket （ List Objects ） 、バージョン 1 およびバージョン 2	<p>この処理は、バケット内のオブジェクトの一部またはすべて（最大 1、000 ）を返します。を使用してオブジェクトを取り込んだ場合でも、オブジェクトのストレージクラスには2つの値が設定されます REDUCED_REDUNDANCY ストレージクラスのオブション：</p> <ul style="list-style-type: none"> • `STANDARD`を指定します。このオブジェクトは、ストレージノードで構成されるストレージプールに格納されます。 • `GLACIER`を指定します。このオブジェクトは、クラウドストレージプールで指定された外部バケットに移動されています。 <p>バケットに同じプレフィックスを持つ削除済みキーが多数含まれている場合、応答に一部のキーが含まれることがあります CommonPrefixes キーが含まれていないもの。</p>
GET Bucket ACL の場合	この処理では、バケットの所有者にバケットに対するフルアクセスがあることを示す応答が返され、所有者の ID 、表示名、および権限が表示されます。
GET Bucket CORS	この処理を実行するとが返されます cors バケットの設定。

操作	実装
GET Bucket encryption	この処理は、バケットのデフォルトの暗号化設定を返します。
GET Bucket lifecycle	この処理は、バケットのライフサイクル設定を返します。
GET Bucket location の各ノードで使用でき	この操作は、を使用して設定されたリージョンを返します LocationConstraint PUT Bucket要求の要素。バケットのリージョンがの場合 `us-east-1` を指定すると、リージョンに対して空の文字列が返されます。
GET Bucket notification	この処理は、バケットに関連付けられている通知設定を返します。
GET Bucket Object versions	バケットに対する読み取りアクセスで、を使用した処理 versions サブリソースには、バケット内のオブジェクトのすべてのバージョンのメタデータが表示されます。
GET Bucket policy の場合	この処理は、バケットに関連付けられているポリシーを返します。
GET Bucket replication	この処理は、バケットに関連付けられているレプリケーション設定を返します。
GET Bucket tagging	この処理にはを使用します tagging サブリソース：バケットのすべてのタグを返す
GET Bucket versioning	この実装ではを使用します versioning サブリソース：バケットのバージョン管理の状態を返します。返されるバージョン管理状態は'バケットがバージョン管理されていないか'バケットがバージョン管理されているか'または一時停止されているかを示します
オブジェクトロック設定の取得	この処理は、バケットでS3オブジェクトのロックが有効になっているかどうかを判断します。" S3 オブジェクトロックを使用する "
HEAD Bucket （ヘッドバケット）	この処理は、バケットが存在し、そのバケットへのアクセス権限があるかどうかを判断します。

操作	実装
PUT Bucket の場合	<p>この処理は、新しいバケットを作成します。バケットを作成すると、そのバケットの所有者になります。</p> <ul style="list-style-type: none"> バケット名は次のルールを満たす必要があります。 <ul style="list-style-type: none"> StorageGRID システム全体で（テナントアカウント内だけではなく）一意である必要があります。 DNS に準拠している必要があります。 3 文字以上 63 文字以下にする必要があります。 1 つ以上のラベルを連続して指定できます。隣接するラベルはピリオドで区切ります。各ラベルの先頭と末尾の文字は小文字のアルファベットか数字にする必要があります、使用できる文字は小文字のアルファベット、数字、ハイフンのみです。 テキスト形式の IP アドレスのようにはできません。 仮想ホスト形式の要求でピリオドを使用しないでください。ピリオドを使用すると、サーバワイルドカード証明書の検証で原因の問題が発生します。 デフォルトでは、バケットには作成されます us-east-1 リージョン。ただし、を使用することはできません LocationConstraint 別のリージョンを指定するように要求本文内の要求要素。を使用する場合 LocationConstraint 要素：Grid Managerまたはグリッド管理APIを使用して定義されているリージョンの正確な名前を指定する必要があります。使用すべきリージョン名がわからない場合は、システム管理者にお問い合わせください。* 注： StorageGRID で定義されていないリージョンを PUT Bucket 要求で使用すると、エラーが発生します。 を含めることができます x-amz-bucket-object-lock-enabled S3オブジェクトのロックを有効にしてバケットを作成する要求ヘッダー。 <p>バケットの作成時に S3 オブジェクトのロックを有効にする必要があります。バケットの作成後に S3 オブジェクトのロックを追加または無効にすることはできません。S3 オブジェクトロックにはバケットのバージョン管理が必要です。バケットの作成時に自動的に有効になります。</p> <p>"S3 オブジェクトロックを使用する"</p>

操作	実装
PUT Bucket CORS	<p>この処理は、バケットの CORS 設定を指定し、クロスオリジン要求を処理できるようにします。Cross-Origin Resource Sharing (CORS) は、あるドメインのクライアント Web アプリケーションが別のドメインのリソースにアクセスできるようにするセキュリティ機能です。たとえば、というS3バケットを使用するとします images グラフィックを保存します。のCORS設定を指定します images バケットを使用すると、そのバケット内の画像をWebサイトに表示できます http://www.example.com。</p>
PUT Bucket encryption	<p>この処理は、既存のバケットのデフォルトの暗号化状態を設定します。バケットレベルの暗号化が有効な場合は、バケットに追加されたすべての新しいオブジェクトが暗号化されます。 StorageGRID では、StorageGRID で管理されるキーによるサーバ側の暗号化がサポートされます。サーバ側の暗号化設定ルールを指定する場合は、を設定します</p> <p>SSEAlgorithm パラメータの値 AES256`を使用せずに、を使用してください `KMSMasterKeyID パラメータ</p> <p>バケットのデフォルトの暗号化設定は、オブジェクトのアップロード要求ですでに暗号化が指定されている場合（要求にが含まれている場合）は無視されます x-amz-server-side-encryption-* 要求ヘッダー）。</p>

操作	実装
PUT Bucket lifecycle の場合	<p>この処理は、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 では、1つのライフサイクル設定で最大 1、000 個のライフサイクルルールがサポートされます。各ルールには、次の XML 要素を含めることができます。</p> <ul style="list-style-type: none"> • 有効期限（日数、日付） • NoncurrentVersionExpiration（NoncurrentDays） • フィルタ（プレフィックス、タグ） • ステータス • ID <p>StorageGRID では、次のアクションはサポートされません。</p> <ul style="list-style-type: none"> • AbortIncompleteMultipartUpload の略 • ExpiredObjectDeleteMarker • 移行 <p>バケット・ライフサイクルの Expiration アクションと ILM 配置手順の相互作用については、情報ライフサイクル管理を使用してオブジェクトを管理する手順のオブジェクトのライフサイクル全体にわたる ILM の動作を参照してください</p> <ul style="list-style-type: none"> • 注：バケットライフサイクル設定は S3 オブジェクトロックが有効なバケットで使用できますが、従来の準拠バケットではバケットライフサイクル設定がサポートされません。

操作	実装
PUT Bucket notification	<p>この処理は、要求の本文に含まれる通知設定 XML を使用してバケットの通知を設定します。実装に関する次の詳細事項に注意してください。</p> <ul style="list-style-type: none"> StorageGRID では、Simple Notification Service （SNS）のトピックがデスティネーションとしてサポートされます。Simple Queue Service （SQS）エンドポイントまたは Amazon Lambda エンドポイントはサポートされていません。 通知のデスティネーションは、StorageGRID エンドポイントの URN として指定する必要があります。エンドポイントは、Tenant Manager またはテナント管理 API を使用して作成できます。 <p>通知設定が機能するためには、エンドポイントが存在している必要があります。エンドポイントが存在しない場合は、400 Bad Request エラーがコードとともに返されます InvalidArgument。</p> <ul style="list-style-type: none"> 次のイベントタイプには通知を設定できません。これらのイベントタイプは * サポートされていません。 <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は標準の JSON 形式を使用しますが、次のように使用されないキーおよび特定の値が使用されるキーがあります。 <ul style="list-style-type: none"> * eventSource* sgws:s3 * awsRegion * 含まれません * x-amz-id-2 * 含まれません * arn * urn:sgws:s3:::bucket_name
PUT Bucket policy の場合	この処理は、バケットに関連付けられているポリシーを設定します。

操作	実装
PUT Bucket replication	<p>この処理では、要求の本文に含まれるレプリケーション設定 XML を使用して、バケットの StorageGRID CloudMirror レプリケーションが設定されます。CloudMirror レプリケーションについては、実装に関する次の詳細事項に注意してください。</p> <ul style="list-style-type: none"> StorageGRID では、V1 のレプリケーション設定のみがサポートされます。つまり、StorageGRID では、の使用はサポートされていません Filter ルールのエレメント。V1の規則に従ってオブジェクトバージョンを削除します。詳細については、レプリケーション設定に関する Amazon のドキュメントを参照してください。 バケットレプリケーションは、バージョン管理されているバケットでもバージョン管理されていないバケットでも設定でき レプリケーション設定 XML の各ルールで異なるデスティネーションバケットを指定できます。1 つのソースバケットを複数のデスティネーションバケットにレプリケートできます。 デスティネーションバケットは、テナントマネージャまたはテナント管理 API で指定された StorageGRID エンドポイントの URN として指定する必要があります。 <p>レプリケーション設定が機能するためには、エンドポイントが存在している必要があります。エンドポイントが存在しない場合は、として要求が失敗します 400 Bad Request。エラーメッセージ: Unable to save the replication policy. The specified endpoint URN does not exist: <i>URN</i>.</p> <ul style="list-style-type: none"> を指定する必要はありません Role 設定XMLを使用します。この値は StorageGRID では使用されず、送信されても無視されます。 設定XMLでストレージクラスを省略した場合、StorageGRID ではを使用します STANDARD デフォルトのストレージクラス。 ソースバケットからオブジェクトを削除する場合、またはソースバケット自体を削除する場合、クロスリージョンレプリケーションは次のように動作します。 <ul style="list-style-type: none"> レプリケートの前にオブジェクトまたはバケットを削除すると、オブジェクトまたはバケットはレプリケートされず、通知は届きません。 レプリケートのあとにオブジェクトまたはバケットを削除すると、StorageGRID は、V1 のクロスリージョンレプリケーションに対する Amazon S3 の通常の削除動作に従います。

操作	実装
PUT Bucket tagging	<p>この処理にはを使用します tagging サブリソース：バケットの一連のタグを追加または更新できます。バケットタグを追加する場合は、次の制限事項に注意してください。</p> <ul style="list-style-type: none"> 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ているタグには、一意のタグキーが必要です。タグキーには Unicode 文字を 128 文字まで使用できます。 タグ値には、Unicode 文字を 256 文字以内で指定します。 キーと値では大文字と小文字が区別されます。
PUT Bucket versioning の場合	<p>この実装ではを使用します versioning サブリソース：既存のバケットのバージョン管理の状態を設定できます。バージョン管理の状態は、次のいずれかの値に設定できます。</p> <ul style="list-style-type: none"> Enabled：バケット内のオブジェクトに対してバージョン管理を有効にします。バケットに追加されるすべてのオブジェクトに、一意のバージョン ID が割り当てられます。 Suspended：バケット内のオブジェクトに対してバージョン管理を無効にします。バケットに追加されるすべてのオブジェクトに、バージョン ID が割り当てられます null。

関連情報

["Amazon Web Services \(AWS\) ドキュメント：「Cross-Region Replication」](#)

["整合性制御"](#)

["GET Bucket last access time 要求"](#)

["バケットとグループのアクセスポリシー"](#)

["S3 オブジェクトロックを使用する"](#)

["監査ログで追跡される S3 処理"](#)

["ILM を使用してオブジェクトを管理する"](#)

["テナントアカウントを使用する"](#)

S3 ライフサイクル設定を作成する

S3 ライフサイクル設定を作成して、特定のオブジェクトが StorageGRID システムから削除されるタイミングを制御できます。

このセクションの簡単な例では、S3 ライフサイクル設定で特定のオブジェクトが特定の S3 バケットから削除（期限切れ）されるタイミングを制御する方法を示します。このセクションの例は、説明のみを目的としています。S3 ライフサイクル設定の作成の詳細については、Amazon Simple Storage Service Developer Guide のオブジェクトライフサイクル管理に関するセクションを参照してください。StorageGRID では、Expiration アクションのみがサポートされ、移行アクションはサポートされません。

["Amazon Simple Storage Service Developer Guide : Object lifecycle management"](#)

ライフサイクル構成とは

ライフサイクル設定は、特定の S3 バケット内のオブジェクトに適用される一連のルールです。各ルールは、影響を受けるオブジェクトと、それらのオブジェクトの有効期限（特定の日付または日数後）を指定します。

StorageGRID では、1 つのライフサイクル設定で最大 1、000 個のライフサイクルルールがサポートされます。各ルールには、次の XML 要素を含めることができます。

- Expiration：指定した日付に達した場合、またはオブジェクトが取り込まれたときから指定した日数に達した場合にオブジェクトを削除します。
- NoncurrentVersionExpiration：指定した日数に達したオブジェクトを削除します。これは、オブジェクトが最新でなくなったときからです。
- フィルタ（プレフィックス、タグ）
- ステータス
- ID

バケットにライフサイクル設定を適用する場合、バケットのライフサイクル設定は常に StorageGRID の ILM 設定よりも優先されます。StorageGRID は、ILM ではなくバケットの Expiration 設定を使用して、特定のオブジェクトを削除するか保持するかを決定します。

そのため、ILM ルールの配置手順がオブジェクトに引き続き適用されていても、オブジェクトがグリッドから削除されることがあります。あるいは、ILM 配置手順がすべて終了したあとも、オブジェクトがグリッドに保持される場合があります。詳細については「情報ライフサイクル管理を使用してオブジェクトを管理する手順」のオブジェクトのライフサイクル全体にわたる ILM の動作を参照してください。



バケットライフサイクル設定は S3 オブジェクトロックが有効になっているバケットで使用できますが、従来の準拠バケットではバケットライフサイクル設定がサポートされません。

StorageGRID では、次のバケット処理を使用してライフサイクル設定を管理できます。

- バケットライフサイクルを削除
- GET Bucket lifecycle
- PUT Bucket lifecycle の場合

ライフサイクル構成を作成します

ライフサイクル設定を作成するための最初の手順として、1つ以上のルールを含む JSON ファイルを作成します。たとえば、この JSON ファイルには次の3つのルールが含まれています。

1. ルール1は、プレフィックスに一致するオブジェクトにのみ適用されます `category1/`とそれにはがあります `key2` の値 `tag2`。Expiration パラメータは、フィルタに一致するオブジェクトの有効期限が2020年8月22日の午前0時に切れるように指定します。
2. ルール2は、プレフィックスに一致するオブジェクトにのみ適用されます `category2/`。Expiration パラメータは、フィルタに一致するオブジェクトの取り込みから100日後に期限切れにするを指定します。



日数を指定するルールは、オブジェクトが取り込まれた時点を基準とした相対的なルールです。現在の日付が取り込み日と日数を超えている場合は、ライフサイクル設定の適用後すぐに一部のオブジェクトがバケットから削除される可能性があります。

3. ルール3は、プレフィックスに一致するオブジェクトにのみ適用されます `category3/`。Expiration パラメータは、最新でないバージョンの一致オブジェクトが最新でなくなったあと50日で期限切れになるように指定します。

```

{
  "Rules": [
    {
      "ID": "rule1",
      "Filter": {
        "And": {
          "Prefix": "category1/",
          "Tags": [
            {
              "Key": "key2",
              "Value": "tag2"
            }
          ]
        }
      },
      "Expiration": {
        "Date": "2020-08-22T00:00:00Z"
      },
      "Status": "Enabled"
    },
    {
      "ID": "rule2",
      "Filter": {
        "Prefix": "category2/"
      },
      "Expiration": {
        "Days": 100
      },
      "Status": "Enabled"
    },
    {
      "ID": "rule3",
      "Filter": {
        "Prefix": "category3/"
      },
      "NoncurrentVersionExpiration": {
        "NoncurrentDays": 50
      },
      "Status": "Enabled"
    }
  ]
}

```

バケットへのライフサイクル設定の適用

ライフサイクル設定ファイルを作成したら、PUT Bucket lifecycle 要求を発行してバケットに適用します。

次の要求は、サンプルファイル内のライフサイクル設定を、という名前のバケット内のオブジェクトに適用します testbucket：バケット

```
aws s3api --endpoint-url <StorageGRID endpoint> put-bucket-lifecycle-configuration
--bucket testbucket --lifecycle-configuration file://bktjson.json
```

ライフサイクル設定がバケットに正常に適用されたことを検証するために、問題 には GET Bucket lifecycle 要求があります。例：

```
aws s3api --endpoint-url <StorageGRID endpoint> get-bucket-lifecycle-configuration
--bucket testbucket
```

成功応答には、適用したライフサイクル設定が表示されます。

バケットライフサイクルの有効期限を検証すると、オブジェクトが環境 に期限切れになります

PUT Object、HEAD Object、または GET Object 要求の発行時に、ライフサイクル設定の有効期限ルールが環境 の特定のオブジェクトかどうかを確認できます。ルールが適用される場合、応答にはが含まれます Expiration オブジェクトの有効期限と一致する有効期限を示すパラメータ。



バケットライフサイクルはILMよりも優先されるため、を参照してください expiry-date 表示されているのは、オブジェクトが削除される実際の日付です。詳細については、StorageGRID 管理の実行手順の「オブジェクト保持の決定方法」を参照してください。

たとえば、このPUT Object要求は2020年6月22日に実行され、にオブジェクトが配置されます testbucket バケット。

```
aws s3api --endpoint-url <StorageGRID endpoint> put-object
--bucket testbucket --key obj2test2 --body bktjson.json
```

成功の応答は、オブジェクトの有効期限が 100 日（2020 年 10 月 1 日）に切れ、ライフサイクル設定のルール 2 に一致したことを示します。

```
{
  *Expiration: "expiry-date=\"Thu, 01 Oct 2020 09:07:49 GMT\"", rule-id="rule2",
  ETag: "\"9762f8a803bc34f5340579d4446076f7\""
}
```

たとえば、この HEAD Object 要求を使用して、testbucket バケット内の同じオブジェクトのメタデータを取得しました。

```
aws s3api --endpoint-url <StorageGRID endpoint> head-object
--bucket testbucket --key obj2test2
```

成功の応答にはオブジェクトのメタデータが含まれ、オブジェクトが 100 日で期限切れになり、ルール 2 に一致したことが示されます。

```
{
  "AcceptRanges": "bytes",
  *Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:48 GMT\", rule-id=\"rule2\"",
  "LastModified": "2020-06-23T09:07:48+00:00",
  "ContentLength": 921,
  "ETag": "\"9762f8a803bc34f5340579d4446076f7\"",
  "ContentType": "binary/octet-stream",
  "Metadata": {}
}
```

関連情報

["バケットの処理"](#)

["ILM を使用してオブジェクトを管理する"](#)

バケットのカスタム処理

StorageGRID システムでは、S3 REST API に追加されたシステム固有のカスタムバケット処理をサポートしています。

次の表に、StorageGRID でサポートされるカスタムバケット処理を示します。

操作	説明	を参照してください。
GET Bucket consistency	特定のバケットに適用されている整合性レベルを返します。	"GET Bucket consistency 要求を実行します"
PUT Bucket consistency	特定のバケットに適用される整合性レベルを設定します。	"PUT Bucket consistency 要求"
GET Bucket last access time の場合	特定のバケットで最終アクセス時間の更新が有効になっているか無効になっているかを返します。	"GET Bucket last access time 要求"

操作	説明	を参照してください。
PUT Bucket last access time のように指定します	特定のバケットの最終アクセス時間の更新を有効または無効にできます。	"PUT Bucket last access time 要求の場合"
バケットのメタデータ通知設定を削除します	特定のバケットに関連付けられているメタデータ通知設定 XML を削除します。	"DELETE Bucket metadata notification configuration 要求"
GET Bucket metadata notification configuration	特定のバケットに関連付けられているメタデータ通知設定 XML を返します。	"GET Bucket metadata notification configuration 要求"
PUT Bucket metadata notification configuration のコマンドです	バケットのメタデータ通知サービスを設定します。	"PUT Bucket metadata notification configuration 要求"
準拠のためのPUT Bucketの変更	廃止およびサポート終了：準拠を有効にした新しいバケットを作成できなくなりました。	"廃止：準拠のための PUT Bucket 要求の変更"
GET Bucket compliance で確認します	廃止されましたがサポートされています：既存の古い準拠バケットに対して現在有効な準拠設定を返します。	"廃止予定： GET Bucket compliance 要求"
PUT Bucket compliance で確認してください	廃止されましたがサポートされています：既存の古い準拠バケットの準拠設定を変更できます。	"廃止予定： PUT Bucket compliance 要求"

関連情報

"[監査ログで追跡される S3 処理](#)"

オブジェクトの処理

このセクションでは、StorageGRID システムでオブジェクトの S3 REST API 処理を実装する方法について説明します。

- "[S3 オブジェクトロックを使用する](#)"
- "[サーバ側の暗号化を使用する](#)"
- "[オブジェクトの取得](#)"
- "[HEAD Object の実行](#)"
- "[POST Object restore の実行](#)"
- "[PUT Object の場合](#)"
- "[PUT Object - Copy の各コマンドを実行します](#)"

すべてのオブジェクトの処理に次の条件が適用されます。

- StorageGRID 整合性制御は、次の点を除いて、オブジェクトに対するすべての処理でサポートされます。
 - GET Object ACL の場合
 - OPTIONS /
 - オブジェクトのリーガルホールドを適用します
 - PUT Object retention のことです
- 同一キーに書き込む2つのクライアントなど'競合するクライアント要求は'最新のWINS形式で解決されます「latest-wins」評価のタイミングは、S3クライアントが処理を開始するタイミングではなく、StorageGRID システムが特定の要求を完了したタイミングに基づいています。
- StorageGRID バケット内のオブジェクトは、匿名ユーザまたは別のアカウントが作成したオブジェクトも含めて、すべてバケット所有者によって所有されます。
- Swift を使用して StorageGRID システムに取り込まれたデータオブジェクトに S3 を使用してアクセスすることはできません。

次の表に、StorageGRID での S3 REST API オブジェクト処理の実装方法を示します。

操作	実装
オブジェクトを削除します	<p>多要素認証（MFA）と応答ヘッダー <code>x-amz-mfa</code> はサポートされていません。</p> <p>StorageGRID は、DELETE Object 要求を処理する際に、オブジェクトのすべてのコピーをすべての格納場所からただちに削除しようとしています。成功すると、StorageGRID はただちにクライアントに応答を返します。30 秒以内にすべてのコピーを削除できなかった場合（格納場所が一時的に使用不能などの理由で）、StorageGRID は削除対象のコピーをキューに登録し、クライアントに処理が成功したことを通知します。</p> <ul style="list-style-type: none"> バージョン管理 * <p>特定のバージョンを削除するには、バケットの所有者を要求元にしてを使用する必要があります <code>versionId</code> サブリソース：このサブリソースを使用すると、バージョンが完全に削除されます。状況に応じて <code>versionId</code> 削除マーカ、応答ヘッダーに対応します <code>x-amz-delete-marker</code> はに設定されています <code>true</code>。</p> <ul style="list-style-type: none"> を使用せずにオブジェクトが削除された場合 <code>versionId</code> バージョンが有効になっているバケットのサブリソースが表示されると、削除マーカが生成されます。。 <code>versionId</code> 削除マーカの場合は、を使用して戻ります <code>x-amz-version-id</code> 応答ヘッダー、および <code>x-amz-delete-marker</code> 応答ヘッダーがに設定されて返されます <code>true</code>。 を使用せずにオブジェクトが削除された場合 <code>versionId</code> バージョンが一時停止中のバケットについて、既存の「null」バージョンまたは「null」削除マーカが完全に削除され、新しい「null」削除マーカが生成されます。。 <code>x-amz-delete-marker</code> 応答ヘッダーがに設定されて返されます <code>true</code>。 注 *：特定の場、1 つのオブジェクトに複数の削除マーカが存在することがあります。
複数のオブジェクトを削除します	<p>多要素認証（MFA）と応答ヘッダー <code>x-amz-mfa</code> はサポートされていません。</p> <p>同じ要求メッセージで複数のオブジェクトを削除できます。</p>

操作	実装
オブジェクトのタグ付けを削除します	<p>を使用します tagging サブリソース：オブジェクトからすべてのタグを削除します。Amazon S3 REST API のすべての動作が実装されています。</p> <ul style="list-style-type: none"> • バージョン管理 * <p>状況に応じて versionId クエリパラメータが要求で指定されていない場合、バージョン管理されたバケット内のオブジェクトの最新バージョンからすべてのタグが削除されます。オブジェクトの現在のバージョンが削除マーカーの場合は、"MethodNotAllowed"ステータスがとともに返されます x-amz-delete-marker 応答ヘッダーをに設定しました true。</p>
オブジェクトの取得	"オブジェクトの取得"
GET Object ACL の場合	アカウントに必要なアクセスクレデンシャルがある場合、オブジェクトの所有者にオブジェクトに対するフルアクセスがあることを示す応答が返され、所有者の ID、表示名、および権限が表示されます。
オブジェクトのリーガルホールドを取得します	"S3 オブジェクトロックを使用する"
GET Object retention のことです	"S3 オブジェクトロックを使用する"
GET Object tagging	<p>を使用します tagging サブリソース：オブジェクトのすべてのタグを返すために使用します。Amazon S3 REST API のすべての動作が実装されています</p> <ul style="list-style-type: none"> • バージョン管理 * <p>状況に応じて versionId クエリパラメータが要求で指定されていない場合、バージョン管理されたバケット内のオブジェクトの最新バージョンからすべてのタグが返されます。オブジェクトの現在のバージョンが削除マーカーの場合は、"MethodNotAllowed"ステータスがとともに返されます x-amz-delete-marker 応答ヘッダーをに設定しました true。</p>
HEAD Object の実行	"HEAD Object の実行"
POST Object restore の実行	"POST Object restore の実行"
PUT Object の場合	"PUT Object の場合"

操作	実装
PUT Object - Copy の各コマンドを実行します	"PUT Object - Copy の各コマンドを実行します"
オブジェクトのリーガルホールドを適用します	"S3 オブジェクトロックを使用する"
PUT Object retention のことです	"S3 オブジェクトロックを使用する"
PUT Object tagging	<p>を使用します tagging サブリソース：既存のオブジェクトに一連のタグを追加します。Amazon S3 REST API のすべての動作が実装されています</p> <ul style="list-style-type: none"> • タグの更新と取り込み動作 * <p>PUT Object tagging を使用してオブジェクトのタグを更新した場合、StorageGRID はオブジェクトを再取り込みしません。これは、一致する ILM ルールで指定されている取り込み動作が使用されないことを意味します。更新によって発生したオブジェクト配置の変更は、通常のバックグラウンド ILM プロセスで ILM が再評価されるときに実施されます。</p> <p>このため、ILM ルールの取り込み動作に Strict オプションが指定されている場合、必要なオブジェクト配置を実行できないと（たとえば、新たに必要となった場所を使用できない場合）、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、必要な配置を実行可能になるまで現在の配置が維持されます。</p> <ul style="list-style-type: none"> • 衝突の解決 * <p>同一キーに書き込む2つのクライアントなど競合するクライアント要求は最新のWINS形式で解決されます「latest-wins」評価のタイミングは、S3クライアントが処理を開始するタイミングではなく、StorageGRID システムが特定の要求を完了したタイミングに基づいています。</p> <ul style="list-style-type: none"> • バージョン管理 * <p>状況に応じて versionId クエリパラメータが要求で指定されていません。処理は、バージョン管理されたバケット内のオブジェクトの最新バージョンにタグを追加します。オブジェクトの現在のバージョンが削除マーカーの場合は、"MethodNotAllowed"ステータスがとともに返されます x-amz-delete-marker 応答ヘッダーをに設定しました true。</p>

関連情報

"整合性制御"

"監査ログで追跡される S3 処理"

S3 オブジェクトロックを使用する

StorageGRID システムでグローバルな S3 オブジェクトのロック設定が有効になっている場合は、S3 オブジェクトのロックを有効にしたバケットを作成し、そのバケットに追加するオブジェクトのバージョンごとに retain-until date および legal hold 設定を指定できます。

S3 オブジェクトロックでは、オブジェクトレベルの設定を指定して、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ないようにすることができます。

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

バケットでS3オブジェクトのロックを有効にする

StorageGRID システムでグローバルな S3 オブジェクトのロック設定が有効になっている場合は、各バケットの作成時に S3 オブジェクトのロックを必要に応じて有効にすることができます。次のいずれかの方法を使用できます。

- Tenant Manager を使用してバケットを作成します。

"テナントアカウントを使用する"

- を指定したPUT Bucket要求を使用してバケットを作成します x-amz-bucket-object-lock_enabled 要求ヘッダー。

"バケットの処理"

バケットの作成後に S3 オブジェクトのロックを追加または無効にすることはできません。S3 オブジェクトロックにはバケットのバージョン管理が必要です。バケットの作成時に自動的に有効になります。

S3 オブジェクトのロックが有効になっているバケットには、S3 オブジェクトのロック設定があるオブジェクトとなっていないオブジェクトを組み合わせる含めることができます。StorageGRID では、S3オブジェクトロックバケット内のオブジェクトのデフォルトの保持はサポートされないため、PUT Object Lock Configurationバケットの処理はサポートされません。

バケットで**S3**オブジェクトのロックが有効になっているかどうかを確認しています

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するには、GET Object Lock Configuration要求を使用します。

"バケットの処理"

S3オブジェクトのロック設定を使用してオブジェクトを作成する

S3 オブジェクトロックが有効に問題 になっているバケットにオブジェクトのバージョンを追加するときに S3 オブジェクトのロック設定を指定するには、PUT Object 、 PUT Object - Copy 、 Initiate Multipart Upload 要

求のいずれかを実行します。次の要求ヘッダーを使用します。



バケットの作成時に S3 オブジェクトのロックを有効にする必要があります。バケットの作成後に S3 オブジェクトのロックを追加または無効にすることはできません。

- ``x-amz-object-lock-mode``は、コンプライアンスに準拠している必要があります（大文字と小文字が区別されます）



を指定する場合 `x-amz-object-lock-mode`、も指定する必要があります `x-amz-object-lock-retain-until-date`。

- `x-amz-object-lock-retain-until-date`
 - `retain-until-date`の値は、の形式で指定する必要があります `2020-08-10T21:46:00Z`。秒数には分数を指定できますが、保持される 10 進数は 3 桁（ミリ秒単位）だけです。それ以外の ISO 8601 形式はサポートされません。
 - `retain-until-date` は将来の日付にする必要があります。
- `x-amz-object-lock-legal-hold`

リーガルホールドがオン（大文字と小文字が区別される）の場合、オブジェクトはリーガルホールドの対象になります。リーガルホールドがオフの場合、リーガルホールドは適用されません。それ以外の値を指定すると、400 Bad Request（InvalidArgument）エラーが発生します。

次のいずれかの要求ヘッダーを使用する場合は、次の制限事項に注意してください。

- `Content-MD5` 要求ヘッダーがある場合は必須です `x-amz-object-lock-*` 要求ヘッダーがPUT Object要求に含まれています。Content-MD5 PUT Object - CopyまたはInitiate Multipart Uploadには必要ありません。
- バケットでS3オブジェクトロックが有効になっていない場合は、とをクリックします `x-amz-object-lock-*` 要求ヘッダーが存在し、400 Bad Request（InvalidRequest）エラーが返されます。
- PUT Object要求では、の使用がサポートされます `x-amz-storage-class: REDUCED_REDUNDANCY` AWSの動作に合わせて調整できます。ただし、S3 オブジェクトのロックが有効になっているバケットにオブジェクトが取り込まれると、StorageGRID は常にデュアルコミットの取り込みを実行します。
- 後続のGETまたはHEAD Objectバージョンの応答では、ヘッダーが含まれます `x-amz-object-lock-mode`、`x-amz-object-lock-retain-until-date``および ``x-amz-object-lock-legal-hold`` が設定されている場合、および要求の送信者が正しいかどうか ``s3:Get*`` 権限：
- それ以降の DELETE Object version 要求または DELETE Objects versions 要求は、`retain-until` 日の前であるか、リーガルホールドがオンの場合には失敗します。

S3オブジェクトのロック設定を更新しています

既存のオブジェクトのバージョンのリーガルホールドや保持の設定を更新する必要がある場合、次のオブジェクトサブリソース処理を実行できます。

- PUT Object legal-hold

新しいリーガルホールドの値が on の場合、オブジェクトはリーガルホールドの対象になります。リーガルホールドの値がオフの場合、リーガルホールドは解除されます。

- PUT Object retention

- モード値は準拠している必要があります（大文字と小文字が区別されます）。
- retain-untilの値は、の形式で指定する必要があります 2020-08-10T21:46:00Z。秒数には分数を指定できますが、保持される 10 進数は 3 桁（ミリ秒単位）だけです。それ以外の ISO 8601 形式はサポートされません。
- オブジェクトバージョンに既存の retain-until がある場合は、オブジェクトバージョンを増やすことはできますが、増やすことはできません。新しい値は将来の必要があります。

関連情報

["ILM を使用してオブジェクトを管理する"](#)

["テナントアカウントを使用する"](#)

["PUT Object の場合"](#)

["PUT Object - Copy の各コマンドを実行します"](#)

["マルチパートアップロードを開始します"](#)

["オブジェクトのバージョン管理"](#)

["Amazon Simple Storage Service User Guide : Using S3 Object Lock"](#)

サーバ側の暗号化を使用

サーバ側の暗号化を使用して、保存中のオブジェクトデータを保護できます。StorageGRID は、オブジェクトを書き込む際にデータを暗号化し、ユーザがオブジェクトにアクセスする際にデータを復号化します。

サーバ側の暗号化を使用する場合は、暗号化キーの管理方法に基づいて、次の 2 つのオプションを同時に選択できます。

- * SSE （ StorageGRID で管理されるキーによるサーバ側の暗号化） * : オブジェクトを格納する S3 要求を問題 で暗号化すると、StorageGRID は一意のキーでオブジェクトを暗号化します。オブジェクトを読み出す S3 要求を問題 で実行すると、StorageGRID は格納されているキーを使用してオブジェクトを復号化します。
- * SSE-C （ユーザ指定のキーによるサーバ側の暗号化） * : オブジェクトを格納する S3 要求を問題 で処理するときに、独自の暗号化キーを指定します。オブジェクトを読み出すときは、同じ暗号化キーを要求に指定します。2 つの暗号化キーが一致すると、オブジェクトが復号化されてオブジェクトデータが返されます。

オブジェクトの暗号化処理と復号化処理はすべて StorageGRID で管理されますが、指定する暗号化キーはユーザが管理する必要があります。



指定した暗号化キーが格納されることはありません。暗号化キーを紛失すると、対応するオブジェクトが失われます。



SSE または SSE-C で暗号化されたオブジェクトは、バケットレベルまたはグリッドレベルの暗号化設定が無視されます。

SSEを使用します

StorageGRID で管理される一意のキーでオブジェクトを暗号化する場合は、次の要求ヘッダーを使用します。

`x-amz-server-side-encryption`

SSE 要求ヘッダーは、次のオブジェクト処理でサポートされます。

- PUT Object の場合
- PUT Object - Copy の各コマンドを実行します
- マルチパートアップロードを開始します

SSE-Cを使用する

ユーザが管理する一意のキーでオブジェクトを暗号化する場合は、次の 3 つの要求ヘッダーを使用します。

要求ヘッダー	説明
<code>x-amz-server-side-encryption-customer-algorithm</code>	暗号化アルゴリズムを指定します。ヘッダー値はある必要があります AES256。
<code>x-amz-server-side-encryption-customer-key</code>	オブジェクトの暗号化と復号化に使用する暗号化キーを指定します。キーの値は、Base64 でエンコードされた 256 ビットである必要があります。
<code>x-amz-server-side-encryption-customer-key-MD5</code>	RFC 1321 に従って暗号化キーの MD5 ダイジェストを指定します。これは、暗号化キーがエラーなしで送信されたことを確認するために使用されます。MD5 ダイジェストの値は、Base64 でエンコードされた 128 ビットである必要があります。

SSE-C 要求ヘッダーは、次のオブジェクト処理でサポートされます。

- オブジェクトの取得
- HEAD Object の実行
- PUT Object の場合
- PUT Object - Copy の各コマンドを実行します
- マルチパートアップロードを開始します
- パーツをアップロードします
- パーツのアップロード - コピー

ユーザ指定のキーによるサーバ側の暗号化（**SSE-C**）を使用する場合の考慮事項

SSE-C を使用する場合は、次の考慮事項に注意してください。

- HTTPS を使用する必要があります。



SSE-C を使用すると、http 経由の要求が StorageGRID ですべて拒否されますセキュリティ上の理由から、誤って http を使用して送信したキーは漏洩する可能性があります。キーを破棄し、必要に応じてローテーションします。

- 応答内の ETag は、オブジェクトデータの MD5 ではありません。
- 暗号化キーとオブジェクトの対応関係を管理する必要があります。StorageGRID では暗号化キーは格納されません。各オブジェクトに対して指定した暗号化キーを管理する責任はユーザにあります。
- バケットのバージョン管理が有効になっている場合は、オブジェクトのバージョンごとに固有の暗号化キーが必要です。各オブジェクトバージョンで使用される暗号化キーを管理する責任はユーザにあります。
- 暗号化キーはクライアント側で管理するため、キーローテーションなどの追加の防護策もクライアント側で管理する必要があります。



指定した暗号化キーが格納されることはありません。暗号化キーを紛失すると、対応するオブジェクトが失われます。

- バケットに CloudMirror レプリケーションが設定されている場合は、SSE-C オブジェクトを取り込むことができません。取り込み処理は失敗します。

関連情報

["オブジェクトの取得"](#)

["HEAD Object の実行"](#)

["PUT Object の場合"](#)

["PUT Object - Copy の各コマンドを実行します"](#)

["マルチパートアップロードを開始します"](#)

["パーツをアップロードします"](#)

["パーツのアップロード - コピー"](#)

["Amazon S3 開発者ガイド：「お客様が用意した暗号化キーによるサーバ側の暗号化（SSE-C）を使用したデータの保護」"](#)

オブジェクトの取得

S3 GET Object 要求を使用して、S3 バケットからオブジェクトを読み出すことができます。

PartNumber要求パラメータはサポートされていません

。partNumber 要求パラメータはGET Object要求ではサポートされません。マルチパートオブジェクトの特定のパートを読み出すGET要求は実行できません。501 Not Implementedエラーが返され、次のメッセージが表示されます。

```
GET Object by partNumber is not implemented
```

ユーザ指定の暗号化キーによるサーバ側の暗号化（**SSE-C**）の要求ヘッダー

指定した一意のキーでオブジェクトが暗号化されている場合は、3つのヘッダーをすべて使用します。

- `x-amz-server-side-encryption-customer-algorithm`: 指定します AES256。
- `x-amz-server-side-encryption-customer-key`: オブジェクトの暗号化キーを指定します
- `x-amz-server-side-encryption-customer-key-MD5`: オブジェクトの暗号化キーのMD5ダイジェストを指定します。



指定した暗号化キーが格納されることはありません。暗号化キーを紛失すると、対応するオブジェクトが失われます。お客様提供の鍵を使用してオブジェクト・データを保護する前に、サーバ側の暗号化の使用に関する考慮事項を確認してください

ユーザメタデータ内の **UTF-8** 文字

StorageGRID は、ユーザ定義メタデータ内のエスケープされた UTF-8 文字を解析も解釈もしません。ユーザ定義メタデータにエスケープされた UTF-8 文字が含まれているオブジェクトに対して GET 要求を実行した場合、からは返されません `x-amz-missing-meta` キーの名前または値に印刷できない文字が含まれている場合は、ヘッダーを指定します。

サポートされない要求ヘッダーです

次の要求ヘッダーはサポートされていません `XNotImplemented` :

- `x-amz-website-redirect-location`

バージョン管理

の場合 `versionId` サブリソースが指定されていません。バージョン管理されたバケット内のオブジェクトの最新バージョンが取得されます。オブジェクトの現在のバージョンが削除マーカーの場合は、「見つからない」ステータスがとともに返されます `x-amz-delete-marker` 応答ヘッダーをに設定しました `true`。

クラウドストレージプールオブジェクトに対する **GET Object** の動作

オブジェクトがクラウドストレージプールに格納されている場合（情報ライフサイクル管理を使用してオブジェクトを管理する手順を参照）、GET Object 要求の動作はオブジェクトの状態によって異なります。詳細については、「head Object」を参照してください。



オブジェクトがクラウドストレージプールに格納され、かつそのオブジェクトのコピーがグリッドに1つ以上存在する場合、GET Object 要求はクラウドストレージプールからデータを読み出す前に、グリッドからデータを読み出そうとします。

オブジェクトの状態	GET Object の動作
StorageGRID に取り込まれているがまだ ILM によって評価されていないオブジェクト、または従来のストレージプールに格納されているオブジェクト、またはイレイジャーコーディングを使用しているオブジェクト	200 OK オブジェクトのコピーが読み出されます。

オブジェクトの状態	GET Object の動作
クラウドストレージプール内にあるが、まだ読み出し不可能な状態に移行していない	200 OK オブジェクトのコピーが読み出されます。
オブジェクトを読み出し不可能な状態に移行した	403 Forbidden、InvalidObjectState POST Object restore 要求を使用して、オブジェクトを読み出し可能な状態にリストアします。
読み出し不可能な状態からリストア中である	403 Forbidden、InvalidObjectState POST Object restore 要求が完了するまで待ちます。
クラウドストレージプールへのリストアが完了している	200 OK オブジェクトのコピーが読み出されます。

クラウドストレージプール内のマルチパートオブジェクトまたはセグメント化されたオブジェクト

マルチパートオブジェクトをアップロードした場合や StorageGRID が大きなオブジェクトをセグメントに分割した場合、StorageGRID はオブジェクトのパーツまたはセグメントのサブセットをサンプリングすることでクラウドストレージプール内のオブジェクトが使用可能かどうかを判断します。GET Object 要求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のパーツがすでに読み出し不可能な状態に移行されている場合や、オブジェクトの一部のパーツがまだリストアされていない場合。

このような場合は、次のよう

- GET Object 要求がデータの一部を返し、転送の途中で停止することがあります。
- 後続の GET Object 要求が返されることがあります 403 Forbidden。

関連情報

["サーバ側の暗号化を使用"](#)

["ILM を使用してオブジェクトを管理する"](#)

["POST Object restore の実行"](#)

["監査ログで追跡される S3 処理"](#)

HEAD Object の実行

S3 HEAD Object 要求を使用すると、オブジェクト自体を返さずにオブジェクトからメタデータを読み出すことができます。オブジェクトがクラウドストレージプールに格納されている場合は、HEAD Object を使用してオブジェクトの移行状態を特定できます。

ユーザ指定の暗号化キーによるサーバ側の暗号化（**SSE-C**）の要求ヘッダー

指定した一意のキーでオブジェクトが暗号化されている場合は、次の 3 つのヘッダーをすべて使用します。

- `x-amz-server-side-encryption-customer-algorithm`: 指定します AES256。
- `x-amz-server-side-encryption-customer-key`: オブジェクトの暗号化キーを指定します
- `x-amz-server-side-encryption-customer-key-MD5`: オブジェクトの暗号化キーのMD5ダイジェストを指定します。



指定した暗号化キーが格納されることはありません。暗号化キーを紛失すると、対応するオブジェクトが失われます。お客様提供の鍵を使用してオブジェクト・データを保護する前に、サーバ側の暗号化の使用に関する考慮事項を確認してください

ユーザメタデータ内の **UTF-8** 文字

StorageGRID は、ユーザ定義メタデータ内のエスケープされた UTF-8 文字を解析も解釈もしません。ユーザ定義メタデータにエスケープされた UTF-8 文字が含まれているオブジェクトに対して HEAD 要求を実行しても、は返されません `x-amz-missing-meta` キーの名前または値に印刷できない文字が含まれている場合は、ヘッダーを指定します。

サポートされない要求ヘッダーです

次の要求ヘッダーはサポートされていません `XNotImplemented` :

- `x-amz-website-redirect-location`

クラウドストレージプールオブジェクトの応答ヘッダー

オブジェクトがクラウドストレージプールに格納されている場合（情報ライフサイクル管理を使用してオブジェクトを管理する手順を参照）、次の応答ヘッダーが返されます。

- `x-amz-storage-class`: GLACIER
- `x-amz-restore`

応答ヘッダーは、オブジェクトがクラウドストレージプールに移動され、必要に応じて読み出し不可能な状態に移行されてリストアされるときの状態に関する情報を提供します。

オブジェクトの状態	HEAD Object への応答
StorageGRID に取り込まれているがまだ ILM によって評価されていないオブジェクト、または従来のストレージプールに格納されているオブジェクト、またはイレイジャーコーディングを使用しているオブジェクト	200 OK（特別な応答ヘッダーは返されません）。

オブジェクトの状態	HEAD Object への応答
クラウドストレージプール内にあるが、まだ読み出し不可能な状態に移行していない	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"</p> <p>オブジェクトが読み出し不可能な状態に移行されるまでの間、の値 expiry-date は、将来の特定の日に時に設定されます。移行の正確な時間は、StorageGRID システムでは制御されません。</p>
オブジェクトが読み出し不可能な状態に移行したが、少なくとも 1 つのコピーがグリッドに存在する	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"</p> <p>の値 expiry-date は、将来の特定の日に時に設定されます。</p> <ul style="list-style-type: none"> 注：グリッド上のコピーを取得できない場合（ストレージノードが停止している場合など）は、オブジェクトを読み出す前に、問題 a POST Object restore 要求を実行してクラウドストレージプールからコピーをリストアする必要があります。
読み出し不可能な状態に移行しており、グリッドにコピーが存在しない	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p>
読み出し不可能な状態からリストア中である	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>x-amz-restore: ongoing-request="true"</p>

オブジェクトの状態	HEAD Object への応答
クラウドストレージプールへのリストアが完了している	200 OK x-amz-storage-class: GLACIER x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2018 00:00:00 GMT" 。 expiry-date クラウドストレージプール内のオブジェクトが読み出し不可能な状態に戻るタイミングを示します。

クラウドストレージプール内のマルチパートオブジェクトまたはセグメント化されたオブジェクト

マルチパートオブジェクトをアップロードした場合や StorageGRID が大きなオブジェクトをセグメントに分割した場合、StorageGRID はオブジェクトのパーツまたはセグメントのサブセットをサンプリングすることでクラウドストレージプール内のオブジェクトが使用可能かどうかを判断します。HEAD Object 要求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のパートがすでに読み出し不可能な状態に移行されている場合や、オブジェクトの一部のパートがまだリストアされていない場合。

バージョン管理

の場合 versionId サブリソースが指定されていません。バージョン管理されたバケット内のオブジェクトの最新バージョンが取得されます。オブジェクトの現在のバージョンが削除マーカーの場合は、「見つからない」ステータスがとともに返されます x-amz-delete-marker 応答ヘッダーをに設定しました true。

関連情報

["サーバ側の暗号化を使用"](#)

["ILM を使用してオブジェクトを管理する"](#)

["POST Object restore の実行"](#)

["監査ログで追跡される S3 処理"](#)

POST Object restore の実行

S3 POST Object restore 要求を使用して、クラウドストレージプールに格納されているオブジェクトをリストアできます。

サポートされている要求タイプ

StorageGRID では、オブジェクトのリストアに POST Object restore 要求のみがサポートされます。ではサポートされません SELECT リストアのタイプ。戻り要求を選択してください XNotImplemented。

バージョン管理

必要に応じて、と指定します `versionId` バージョン管理されたバケット内のオブジェクトの特定のバージョンをリストアする。指定しない場合は ``versionId`` オブジェクトの最新バージョンがリストアされます

クラウドストレージプールオブジェクトでの **POST Object restore** の動作

オブジェクトがクラウドストレージプールに格納されている場合（情報ライフサイクル管理を使用してオブジェクトを管理する手順を参照）、POST Object restore 要求はオブジェクトの状態に基づいて次のように動作します。詳細については、「head Object」を参照してください。



オブジェクトがクラウドストレージプールに格納され、かつそのオブジェクトのコピーがグリッドに 1 つ以上存在する場合は、POST Object restore 要求を実行してオブジェクトをリストアする必要はありません。GET Object 要求を使用してローカルコピーを直接読み出すことができます。

オブジェクトの状態	POST Object restore の動作
StorageGRID に取り込まれているがまだ ILM によって評価されていない、またはオブジェクトがクラウドストレージプールにない	403 Forbidden、InvalidObjectState
クラウドストレージプール内にあるが、まだ読み出し不可能な状態に移行していない	200 OK 変更は行われません。 *注：読み出し不可能な状態に移行する前に、オブジェクトを変更することはできません expiry-date。
オブジェクトを読み出し不可能な状態に移行した	202 Accepted 要求の本文で指定されている日数、オブジェクトの読み出し可能なコピーをクラウドストレージプールにリストアします。この期間が終了すると、オブジェクトは読み出し不可能な状態に戻ります。 必要に応じて、を使用します Tier リストアジョブの完了までにかかる時間を確認するための要求要素 (Expedited、Standard`または `Bulk)。指定しない場合は Tier、Standard 階層を使用しています。 *注意：S3 Glacier Deep Archiveまたはクラウドストレージプールに移行されたオブジェクトや、Azure Blob Storageを使用するクラウドストレージは、を使用してリストアできません Expedited 階層：次のエラーが返されます 403 Forbidden、InvalidTier : Retrieval option is not supported by this storage class。
読み出し不可能な状態からリストア中である	409 Conflict、RestoreAlreadyInProgress

オブジェクトの状態	POST Object restore の動作
クラウドストレージプールへのリストアが完了している	200 OK *注：*オブジェクトが読み出し可能な状態にリストアされている場合は、オブジェクトを変更できます expiry-date 用の新しい値を指定してPOST Object restore要求を再発行する Days。要求が実行された日時に基づいてリストア日が更新されます。

関連情報

["ILM を使用してオブジェクトを管理する"](#)

["HEAD Object の実行"](#)

["監査ログで追跡される S3 処理"](#)

PUT Object の場合

S3 PUT Object 要求を使用すると、オブジェクトをバケットに追加できます。

競合の解決

同一キーに書き込む2つのクライアントなど'競合するクライアント要求は'最新のWINS形式で解決されます「latest-wins」評価のタイミングは、S3クライアントが処理を開始するタイミングではなく、StorageGRID システムが特定の要求を完了したタイミングに基づいています。

オブジェクトのサイズ

StorageGRID は、サイズが最大5TBのオブジェクトをサポートします。

ユーザメタデータのサイズ

Amazon S3 では、各 PUT 要求ヘッダー内のユーザ定義メタデータのサイズが 2KB に制限されます。StorageGRID では、ユーザメタデータが 24KiB に制限されます。ユーザ定義のメタデータのサイズは、各キーと値の UTF-8 エンコードでのバイト数の合計で測定されます。

ユーザメタデータ内の UTF-8 文字

要求のユーザ定義メタデータのキー名または値に（エスケープされていない） UTF-8 文字が含まれている場合、StorageGRID の動作は定義されていません。

ユーザ定義メタデータのキー名または値に含まれているエスケープされた UTF-8 文字は、StorageGRID で解析も解釈もされません。エスケープされた UTF-8 文字は ASCII 文字として扱われます。

- ユーザ定義メタデータにエスケープされた UTF-8 文字が含まれている場合、PUT、PUT Object-Copy、GET、HEAD の各要求は正常に実行されます。
- StorageGRID からが返されない x-amz-missing-meta キーの名前または値の解釈後の値に印刷不能文字が含まれている場合は、ヘッダー。

オブジェクトタグの制限

タグは、新しいオブジェクトをアップロードするときに追加することも、既存のオブジェクトに追加することもできます。StorageGRID と Amazon S3 はどちらも、オブジェクトごとに最大 10 個のタグをサポートします。オブジェクトに関連付けられたタグには、一意のタグキーが必要です。タグキーには Unicode 文字を 128 文字まで、タグ値には Unicode 文字を 256 文字まで使用できます。キーと値では大文字と小文字が区別されます。

オブジェクトの所有権

StorageGRID では、非所有者アカウントまたは匿名ユーザによって作成されたオブジェクトを含むすべてのオブジェクトが、バケット所有者アカウントによって所有されます。

サポートされる要求ヘッダー

次の要求ヘッダーがサポートされています。

- Cache-Control
- Content-Disposition
- Content-Encoding

を指定する場合 aws-chunked の場合 Content-EncodingStorageGRID では、次の項目は検証されません。

- StorageGRID ではが検証されません chunk-signature チャンクデータに対して。
- StorageGRID は、ユーザが指定した値を検証しません x-amz-decoded-content-length をクリックします。

- Content-Language
- Content-Length
- Content-MD5
- Content-Type
- Expires
- Transfer-Encoding

チャンク転送エンコードは、の場合にサポートされます aws-chunked ペイロード署名も使用されます。

- `x-amz-meta-`をクリックし、続けてユーザ定義のメタデータを含む名前と値のペアを作成します。

ユーザ定義メタデータの名前と値のペアを指定する場合、一般的な形式は次のとおりです。

```
x-amz-meta-<name>: <value>
```

ILMルールの参照時間として* User Defined Creation Time *オプションを使用する場合は、を使用する必要があります creation-time を、オブジェクトの作成時に記録されたメタデータの名前として指定します。例：

```
x-amz-meta-creation-time: 1443399726
```

の値 `creation-time` は、1970年1月1日からの秒数として評価されます。



ILM ルールで、参照時間に * User Defined Creation Time * と取り込み動作に `Balanced` オプションまたは `Strict` 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す。

- `x-amz-tagging`
- S3 Object Lock 要求のヘッダー
 - `x-amz-object-lock-mode`
 - `x-amz-object-lock-retain-until-date`
 - `x-amz-object-lock-legal-hold`

"S3 オブジェクトロックを使用する"

- SSE 要求ヘッダー：
 - `x-amz-server-side-encryption`
 - `x-amz-server-side-encryption-customer-key-MD5`
 - `x-amz-server-side-encryption-customer-key`
 - `x-amz-server-side-encryption-customer-algorithm`

"S3 REST API のサポートされる処理と制限事項"

サポートされない要求ヘッダーです

次の要求ヘッダーはサポートされていません。

- ◦ `x-amz-acl` 要求ヘッダーはサポートされていません。
- ◦ `x-amz-website-redirect-location` 要求ヘッダーはサポートされておらず、返されます `XNotImplemented`。

ストレージクラスのオプション

◦ `x-amz-storage-class` 要求ヘッダーがサポートされています。に送信された値 `x-amz-storage-class StorageGRID` が取り込み中にオブジェクトデータを保護する方法に影響し、`StorageGRID` システム (ILMで決定) に格納されるオブジェクトの永続的コピーの数には影響しません。

取り込まれたオブジェクトに一致するILMルールの取り込み動作が`Strict`オプションに指定されている場合、はを使用します `x-amz-storage-class` ヘッダーに影響はありません。

には次の値を使用できます `x-amz-storage-class` :

- `STANDARD` (デフォルト)

- *** Dual commit *** : ILM ルールの取り込み動作が Dual commit オプションに指定されている場合は、オブジェクトの取り込み直後にオブジェクトの 2 つ目のコピーが作成されて別のストレージノードに配置されます (デュアルコミット)。ILM が評価されると、この初期中間コピーがルールの配置手順を満たしているかどうかを StorageGRID が判断します。満たしていない場合は、新しいオブジェクトコピーを別の場所に作成し、初期中間コピーを削除することが必要になる可能性があります。
- *** Balanced *** : ILM ルールで Balanced オプションが指定されていて、ルールで指定されたすべてのコピーを StorageGRID がただちに作成できない場合、StorageGRID は 2 つの中間コピーを別々のストレージノードに作成します。

StorageGRID が ILM ルールに指定されたすべてのオブジェクトコピーをただちに作成できる場合 (同期配置) は、を参照してください `x-amz-storage-class` ヘッダーに影響はありません。

• REDUCED_REDUNDANCY

- *** Dual commit *** : ILM ルールの取り込み動作が Dual commit オプションに指定されている場合は、オブジェクトの取り込み時に StorageGRID が中間コピーを 1 つ作成します (シングルコミット)。
- *** Balanced *** : ILM ルールで Balanced オプションが指定されている場合、StorageGRID は、ルールで指定されたすべてのコピーをただちに作成できない場合にのみ、中間コピーを 1 つ作成します。StorageGRID で同期配置を実行できる場合、このヘッダーは効果がありません。
REDUCED_REDUNDANCY オプションは、オブジェクトに一致する ILM ルールで単一のレプリケートコピーが作成される場合に最適です。この場合は、を使用します REDUCED_REDUNDANCY 取り込み処理のたびに追加のオブジェクトコピーを不要に作成および削除する必要がなくなります。

を使用する REDUCED_REDUNDANCY それ以外の場合は、このオプションは推奨されません。

REDUCED_REDUNDANCY 取り込み中にオブジェクトデータが失われるリスクが高まります。たとえば、ILM 評価の前にコピーが 1 つだけ格納されていたストレージノードに障害が発生すると、データが失われる可能性があります。

- **注意 *** : 一定期間にレプリケートされたコピーを 1 つだけ保持すると、データが永久に失われる危険があります。オブジェクトのレプリケートコピーが 1 つしかない場合、ストレージノードに障害が発生したり、重大なエラーが発生すると、そのオブジェクトは失われます。また、アップグレードなどのメンテナンス作業中は、オブジェクトへのアクセスが一時的に失われます。

を指定します REDUCED_REDUNDANCY オブジェクトの初回取り込み時に作成されるコピー数のみに影響します。オブジェクトがアクティブな ILM ポリシーで評価される際に作成されるオブジェクトのコピー数には影響せず、StorageGRID システムでデータが格納されるときに冗長性レベルが低下することもあります。

***注 :** S3 オブジェクトロックが有効な状態でオブジェクトをバケットに取り込む場合は、を使用します REDUCED_REDUNDANCY オプションは無視されます。古い準拠バケットにオブジェクトを取り込む場合は、を参照してください REDUCED_REDUNDANCY オプションを指定するとエラーが返されます。StorageGRID では、常にデュアルコミットの取り込みが実行され、コンプライアンス要件が満たされます。

サーバ側の暗号化を行うための要求ヘッダー

オブジェクトをサーバ側の暗号化で暗号化するには、次の要求ヘッダーを使用します。SSE オプションと SSE-C オプションを同時に指定することはできません。

- *** SSE *** : StorageGRID で管理される一意のキーでオブジェクトを暗号化するには、次のヘッダーを使用します。
 - `x-amz-server-side-encryption`
- *** SSE-C *** : ユーザが指定および管理する一意のキーでオブジェクトを暗号化する場合は、次の 3 つのヘ

ッダーをすべて使用します。

- `x-amz-server-side-encryption-customer-algorithm`:指定します AES256。
- `x-amz-server-side-encryption-customer-key`:新しいオブジェクトの暗号化キーを指定します。
- `x-amz-server-side-encryption-customer-key-MD5`:新しいオブジェクトの暗号化キーのMD5ダイジェストを指定します。

- ・ 注意： * 指定し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が失われます。お客様提供の鍵を使用してオブジェクト・データを保護する前に'サーバ側の暗号化の使用に関する考慮事項を確認してください

*注：SSEまたはSSE-Cで暗号化されたオブジェクトは、バケットレベルまたはグリッドレベルの暗号化設定が無視されます。

バージョン管理

バケットでバージョン管理が有効になっている場合は、一意です `versionId` は、格納されているオブジェクトのバージョンに対して自動的に生成されます。これ `versionId` は、を使用して応答としても返されます `x-amz-version-id` 応答ヘッダー。

バージョン管理が一時停止中の場合は、オブジェクトバージョンはnullで格納されます `versionId` また、nullバージョンがすでに存在する場合は上書きされます。

関連情報

["ILM を使用してオブジェクトを管理する"](#)

["バケットの処理"](#)

["監査ログで追跡される S3 処理"](#)

["サーバ側の暗号化を使用"](#)

["クライアント接続の設定方法"](#)

PUT Object - Copy の各コマンドを実行します

S3 PUT Object - Copy 要求を使用すると、すでに S3 に格納されているオブジェクトのコピーを作成できます。PUT Object - Copy 処理は、GET を実行してから PUT を実行する処理と同じです。

競合の解決

同一キーに書き込む2つのクライアントなど'競合するクライアント要求は'最新のWINS形式で解決されます「latest-wins」評価のタイミングは、S3クライアントが処理を開始するタイミングではなく、StorageGRIDシステムが特定の要求を完了したタイミングに基づいています。

オブジェクトのサイズ

StorageGRID は、サイズが最大5TBのオブジェクトをサポートします。

ユーザメタデータ内の UTF-8 文字

要求のユーザ定義メタデータのキー名または値に（エスケープされていない） UTF-8 文字が含まれている場合、StorageGRID の動作は定義されていません。

ユーザ定義メタデータのキー名または値に含まれているエスケープされた UTF-8 文字は、StorageGRID で解析も解釈もされません。エスケープされた UTF-8 文字は ASCII 文字として扱われます。

- ユーザ定義メタデータにエスケープされた UTF-8 文字が含まれている場合、要求は正常に実行されます。
- StorageGRID からが返されない x-amz-missing-meta キーの名前または値の解釈後の値に印刷不能文字が含まれている場合は、ヘッダー。

サポートされる要求ヘッダー

次の要求ヘッダーがサポートされています。

- Content-Type
- x-amz-copy-source
- x-amz-copy-source-if-match
- x-amz-copy-source-if-none-match
- x-amz-copy-source-if-unmodified-since
- x-amz-copy-source-if-modified-since
- `x-amz-meta-`をクリックし、続けてユーザ定義のメタデータを含む名前と値のペアを作成します
- x-amz-metadata-directive:デフォルト値はです `COPY`をクリックすると、オブジェクトおよび関連するメタデータをコピーできます。

を指定できます REPLACE オブジェクトのコピー時に既存のメタデータを上書きする場合、またはオブジェクトメタデータを更新する場合。

- x-amz-storage-class
- x-amz-tagging-directive:デフォルト値はです `COPY`をクリックすると、オブジェクトとすべてのタグをコピーできます。

を指定できます REPLACE オブジェクトのコピー時に既存のタグを上書きする場合、またはタグを更新する場合。

- S3 オブジェクトロック要求のヘッダー：
 - x-amz-object-lock-mode
 - x-amz-object-lock-retain-until-date
 - x-amz-object-lock-legal-hold

"S3 オブジェクトロックを使用する"

- SSE 要求ヘッダー：
 - x-amz-copy-source-server-side-encryption-customer-algorithm

- x-amz-copy-source-server-side-encryption-customer-key
- x-amz-copy-source-server-side-encryption-customer-key-MD5
- x-amz-server-side-encryption
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-algorithm

"サーバ側の暗号化を行うための要求ヘッダー"

サポートされない要求ヘッダーです

次の要求ヘッダーはサポートされていません。

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- Expires
- x-amz-website-redirect-location

ストレージクラスのオプション

。 x-amz-storage-class 要求ヘッダーがサポートされ、一致するILMルールで取り込み動作にDual commitまたはBalancedが指定されている場合にStorageGRID で作成されるオブジェクトコピーの数に影響します。

- STANDARD

(デフォルト) ILM ルールで Dual commit オプションが使用されている場合、または Balanced オプションによって中間コピーが作成される場合に、デュアルコミットの取り込み処理を指定します。

- REDUCED_REDUNDANCY

ILM ルールで Dual commit オプションが使用されている場合、または Balanced オプションによって中間コピーが作成される場合に、シングルコミットの取り込み処理を指定します。



S3オブジェクトロックを有効にしてオブジェクトをバケットに取り込む場合は、を使用します REDUCED_REDUNDANCY オプションは無視されます。古い準拠バケットにオブジェクトを取り込む場合は、を参照してください REDUCED_REDUNDANCY オプションを指定するとエラーが返されます。StorageGRID では、常にデュアルコミットの取り込みが実行され、コンプライアンス要件が満たされます。

PUT Object - Copy で x-amz-copy-source を使用しています

ソースのバケットとキーの場合は、で指定します x-amz-copy-source ヘッダーはデスティネーションのバケットおよびキーとは異なり、ソースオブジェクトデータのコピーがデスティネーションに書き込まれます。

送信元と宛先が一致している場合は、および `x-amz-metadata-directive` ヘッダーはのように指定します。`REPLACE`では、要求で指定されたメタデータの値に基づいてオブジェクトのメタデータが更新されます。この場合、StorageGRID はオブジェクトを再取り込みしません。これには2つの重要な結果があります。

- PUT Object - Copy を使用して既存のオブジェクトを暗号化したり、既存のオブジェクトの暗号化を変更したりすることはできません。を用意する場合は `x-amz-server-side-encryption` ヘッダーまたは `x-amz-server-side-encryption-customer-algorithm` ヘッダー。StorageGRID は要求を拒否し、戻ります `XNotImplemented`。
- 一致する ILM ルールで指定されている取り込み動作のオプションが使用されません。更新によって発生したオブジェクト配置の変更は、通常のバックグラウンド ILM プロセスで ILM が再評価されるときに実施されます。

このため、ILM ルールの取り込み動作に Strict オプションが指定されている場合、必要なオブジェクト配置を実行できないと（たとえば、新たに必要となった場所を使用できない場合）、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、必要な配置を実行可能になるまで現在の配置が維持されます。

サーバ側の暗号化を行うための要求ヘッダー

サーバ側の暗号化を使用する場合は、ソースオブジェクトが暗号化されているかどうか、およびターゲットオブジェクトを暗号化するかどうかによって、指定する要求ヘッダーが異なります。

- ソースオブジェクトがユーザ指定のキーを使用して暗号化されている場合（SSE-C）は、オブジェクトを復号化してコピーできるように、PUT Object - Copy 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` を指定します AES256。
 - `x-amz-copy-source-server-side-encryption-customer-key` ソースオブジェクトの作成時に指定した暗号化キーを指定します。
 - `x-amz-copy-source-server-side-encryption-customer-key-MD5`:ソースオブジェクトの作成時に指定したMD5ダイジェストを指定します。
- ユーザが指定および管理する一意のキーでターゲットオブジェクト（コピー）を暗号化する場合は、次の3つのヘッダーを含めます。
 - `x-amz-server-side-encryption-customer-algorithm`:指定します AES256。
 - `x-amz-server-side-encryption-customer-key`:ターゲットオブジェクトの新しい暗号化キーを指定します
 - `x-amz-server-side-encryption-customer-key-MD5`:新しい暗号化キーのMD5ダイジェストを指定します。
- 注意：* 指定し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が失われます。お客様提供の鍵を使用してオブジェクト・データを保護する前に「サーバ側の暗号化の使用に関する考慮事項を確認してください」
- StorageGRID で管理される一意のキーでターゲットオブジェクト（コピー）を暗号化する（SSE）には、PUT Object - Copy 要求に次のヘッダーを含めます。
 - `x-amz-server-side-encryption`

注： `server-side-encryption` オブジェクトの値を更新できません。代わりに、新しいを使用してコピーを作成します `server-side-encryption` を使用した値 `x-amz-metadata-directive`： `REPLACE`。

バージョン管理

ソースバケットがバージョン管理に対応している場合は、を使用できます `x-amz-copy-source` オブジェクトの最新バージョンをコピーするヘッダー。オブジェクトの特定のバージョンをコピーするには、を使用してコピーするバージョンを明示的に指定する必要があります `versionId` サブリソース：デスティネーションバケットがバージョン管理に対応している場合は、で生成されたバージョンが返されます `x-amz-version-id` 応答ヘッダー。ターゲットバケットのバージョン管理が一時停止中の場合は、を実行します `x-amz-version-id` 「null」値を返します。

関連情報

["ILM を使用してオブジェクトを管理する"](#)

["サーバ側の暗号化を使用"](#)

["監査ログで追跡される S3 処理"](#)

["PUT Object の場合"](#)

マルチパートアップロードの処理

このセクションでは、StorageGRID でのマルチパートアップロードの処理のサポートについて説明します。

- ["マルチパートアップロードを表示します"](#)
- ["マルチパートアップロードを開始します"](#)
- ["パーツをアップロードします"](#)
- ["パーツのアップロード - コピー"](#)
- ["Complete Multipart Upload の実行"](#)

マルチパートアップロードのすべての処理に、次の条件と注意事項が適用されます。

- 1 つのバケットに対して同時に実行するマルチパートアップロードが 1、000 件を超えないようにしてください。1、000 件を超えると、そのバケットに対する List Multipart Uploads のクエリで完全な結果が返されないことがあります。
- StorageGRID は、マルチパートに AWS のサイズ制限を適用します。S3 クライアントは次のガイドラインに従う必要があります。
 - マルチパートアップロードの各パートのサイズは 5MiB（5、242、880 バイト）と 5GiB（5、368、709、120 バイト）の間にする必要があります。
 - 最後の部分は 5MiB（5,242,880 バイト）より小さくできます。
 - 一般に、パーツサイズはできるだけ大きくする必要があります。たとえば、100GiB オブジェクトの場合、5GB のパートサイズを使用します。各パートは固有のオブジェクトとみなされるため、大きなパートサイズを使用すると、StorageGRID のメタデータのオーバーヘッドが軽減されます。
 - 5GB 未満のオブジェクトでは、マルチパートではないアップロードの使用を検討してください。
- ILM ルールの取り込み動作が Strict または Balanced に指定されている場合は、マルチパートオブジェクトの各パートが取り込まれるときに ILM が評価され、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全体に対して ILM が評価されます。これがオブジェクトとパートの配置にどのように影響するかに注意する必要があります。

- S3 マルチパートアップロードの進行中に 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時点でオブジェクトの一部のパートが現在の ILM 要件を満たしていないことがあります。正しく配置されていないパートは ILM ルールによる再評価の対象としてキューに登録され、あとで正しい場所に移動されます。
- パートに対して ILM を評価する際、StorageGRID はオブジェクトのサイズではなくパートのサイズでフィルタリングします。つまり、オブジェクト全体としては ILM 要件を満たしていない場所にオブジェクトのパートが格納される可能性があります。たとえば、10GB 以上のオブジェクトをすべて DC1 に格納し、それより小さいオブジェクトをすべて DC2 に格納するルールの場合、10 パートからなるマルチパートアップロードの 1GB の各パートは取り込み時に DC2 に格納されます。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パートが DC1 に移動されます。
- マルチパートアップロードでは、すべての処理で StorageGRID の整合性制御がサポートされます。
- マルチパートアップロードでは、必要に応じてサーバ側の暗号化を使用できます。SSE (StorageGRID で管理されるキーによるサーバ側の暗号化) を使用するには、を指定します `x-amz-server-side-encryption Initiate Multipart Upload` 要求のみの要求ヘッダー。SSE-C (ユーザ指定のキーによるサーバ側の暗号化) を使用する場合は、Initiate Multipart Upload 要求と後続の各 Upload Part 要求に、同じ 3 つの暗号化キー要求ヘッダーを指定します。

操作	実装
マルチパートアップロードをリストします	を参照してください " マルチパートアップロードをリストします "
マルチパートアップロードを開始します	を参照してください " マルチパートアップロードを開始します "
パートをアップロードします	を参照してください " パートをアップロードします "
パートのアップロード - コピー	を参照してください " パートのアップロード - コピー "
Complete Multipart Upload の実行	を参照してください " Complete Multipart Upload の実行 "
マルチパートアップロードを中止します	Amazon S3 REST API のすべての動作が実装されています
パートをリストします	Amazon S3 REST API のすべての動作が実装されています

関連情報

["整合性制御"](#)

["サーバ側の暗号化を使用"](#)

マルチパートアップロードをリストします

List Multipart Uploads 処理では、バケットの進行中のマルチパートアップロードがリストされます。

次の要求パラメータがサポートされています。

- `encoding-type`
- `max-uploads`
- `key-marker`
- `prefix`
- `upload-id-marker`

。 `delimiter` 要求パラメータはサポートされません。

バージョン管理

マルチパートアップロードは、アップロードの開始、アップロードのリストの表示、パートのアップロード、アップロードしたパートのアセンブル、およびアップロードの完了の個別の処理に分けられます。Complete Multipart Upload 処理が実行されると、オブジェクトが作成される時点（およびバージョン管理されている場合）になります。

マルチパートアップロードを開始します

Initiate Multipart Upload 処理は、オブジェクトのマルチパートアップロードを開始し、アップロード ID を返します。

。 `x-amz-storage-class` 要求ヘッダーがサポートされています。に送信された値 `x-amz-storage-class StorageGRID` が取り込み中にオブジェクトデータを保護する方法に影響し、StorageGRID システム（ILMで決定）に格納されるオブジェクトの永続的コピーの数には影響しません。

取り込まれたオブジェクトに一致するILMルールの取り込み動作がStrictオプションに指定されている場合、はを使用します `x-amz-storage-class` ヘッダーに影響はありません。

には次の値を使用できます `x-amz-storage-class` :

- STANDARD（デフォルト）
 - * Dual commit * : ILM ルールの取り込み動作が Dual commit オプションに指定されている場合は、オブジェクトの取り込み直後にオブジェクトの 2 つ目のコピーが作成されて別のストレージノードに配置されます（デュアルコミット）。ILM が評価されると、この初期中間コピーがルールの配置手順を満たしているかどうかを StorageGRID が判断します。満たしていない場合は、新しいオブジェクトコピーを別の場所に作成し、初期中間コピーを削除することが必要になる可能性があります。
 - * Balanced * : ILM ルールで Balanced オプションが指定されていて、ルールで指定されたすべてのコピーを StorageGRID がただちに作成できない場合、StorageGRID は 2 つの中間コピーを別々のストレージノードに作成します。

StorageGRID がILMルールに指定されたすべてのオブジェクトコピーをただちに作成できる場合（同期配置）は、を参照してください `x-amz-storage-class` ヘッダーに影響はありません。

- REDUCED_REDUNDANCY
 - * Dual commit * : ILM ルールの取り込み動作が Dual commit オプションに指定されている場合は、オブジェクトの取り込み時に StorageGRID が中間コピーを 1 つ作成します（シングルコミット）。

- *** Balanced *** : ILM ルールで **Balanced** オプションが指定されている場合、StorageGRID は、ルールで指定されたすべてのコピーをただちに作成できない場合にのみ、中間コピーを 1 つ作成します。StorageGRID で同期配置を実行できる場合、このヘッダーは効果がありません。
REDUCED_REDUNDANCY オプションは、オブジェクトに一致する ILM ルールで単一のレプリケートコピーが作成される場合に最適です。この場合は、を使用します REDUCED_REDUNDANCY 取り込み処理のたびに追加のオブジェクトコピーを不要に作成および削除する必要がなくなります。

を使用する REDUCED_REDUNDANCY それ以外の場合は、このオプションは推奨されません。

REDUCED_REDUNDANCY 取り込み中にオブジェクトデータが失われるリスクが高まります。たとえば、ILM 評価の前にコピーが 1 つだけ格納されていたストレージノードに障害が発生すると、データが失われる可能性があります。

- **注意 *** : 一定期間にレプリケートされたコピーを 1 つだけ保持すると、データが永久に失われる危険があります。オブジェクトのレプリケートコピーが 1 つしかない場合、ストレージノードに障害が発生したり、重大なエラーが発生すると、そのオブジェクトは失われます。また、アップグレードなどのメンテナンス作業中は、オブジェクトへのアクセスが一時的に失われます。

を指定します REDUCED_REDUNDANCY オブジェクトの初回取り込み時に作成されるコピー数のみに影響します。オブジェクトがアクティブな ILM ポリシーで評価される際に作成されるオブジェクトのコピー数には影響せず、StorageGRID システムでデータが格納されるときに冗長性レベルが低下することもあります。

***注 :** S3 オブジェクトロックが有効な状態でオブジェクトをバケットに取り込む場合は、を使用します REDUCED_REDUNDANCY オプションは無視されます。古い準拠バケットにオブジェクトを取り込む場合は、を参照してください REDUCED_REDUNDANCY オプションを指定するとエラーが返されます。StorageGRID では、常にデュアルコミットの取り込みが実行され、コンプライアンス要件が満たされます。

次の要求ヘッダーがサポートされています。

- Content-Type
- `x-amz-meta-` をクリックし、続けてユーザ定義のメタデータを含む名前と値のペアを作成します

ユーザ定義メタデータの名前と値のペアを指定する場合、一般的な形式は次のとおりです。

```
x-amz-meta-_name_: `value`
```

ILM ルールの参照時間として *** User Defined Creation Time *** オプションを使用する場合は、を使用する必要があります creation-time を、オブジェクトの作成時に記録されたメタデータの名前として指定します。例 :

```
x-amz-meta-creation-time: 1443399726
```

の値 creation-time は、1970 年 1 月 1 日からの秒数として評価されます。



追加中です creation-time レガシー準拠が有効になっているバケットにオブジェクトを追加する場合、ユーザ定義メタデータは許可されません。エラーが返されます。

- S3 オブジェクトロック要求のヘッダー :

- x-amz-object-lock-mode

- x-amz-object-lock-retain-until-date
- x-amz-object-lock-legal-hold

"S3 オブジェクトロックを使用する"

- SSE 要求ヘッダー：
 - x-amz-server-side-encryption
 - x-amz-server-side-encryption-customer-key-MD5
 - x-amz-server-side-encryption-customer-key
 - x-amz-server-side-encryption-customer-algorithm

"S3 REST API のサポートされる処理と制限事項"



StorageGRID での UTF-8 文字の処理については、PUT Object に関するドキュメントを参照してください。

サーバ側の暗号化を行うための要求ヘッダー

マルチパートオブジェクトをサーバ側の暗号化で暗号化するには、次の要求ヘッダーを使用します。SSE オプションと SSE-C オプションを同時に指定することはできません。

- * SSE * : StorageGRID で管理される一意のキーでオブジェクトを暗号化する場合は、Initiate Multipart Upload 要求で次のヘッダーを使用します。Upload Part 要求ではこのヘッダーを指定しないでください。
 - x-amz-server-side-encryption
- * SSE-C * : ユーザが指定および管理する一意のキーでオブジェクトを暗号化する場合は、Initiate Multipart Upload 要求（および後続の各 Upload Part 要求）で、次の 3 つのヘッダーをすべて使用します。
 - x-amz-server-side-encryption-customer-algorithm:指定します AES256。
 - x-amz-server-side-encryption-customer-key:新しいオブジェクトの暗号化キーを指定します。
 - x-amz-server-side-encryption-customer-key-MD5:新しいオブジェクトの暗号化キーのMD5 ダイジェストを指定します。
- 注意：* 指定し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が失われます。お客様提供の鍵を使用してオブジェクト・データを保護する前に'サーバ側の暗号化の使用に関する考慮事項を確認してください

サポートされない要求ヘッダーです

次の要求ヘッダーはサポートされていません XNotImplemented

- x-amz-website-redirect-location

バージョン管理

マルチパートアップロードは、アップロードの開始、アップロードのリストの表示、パートのアップロード、アップロードしたパートのアセンブル、およびアップロードの完了の個別の処理に分けられます。Complete

Multipart Upload 処理が実行されると、オブジェクトが作成されます（該当する場合はバージョン管理されます）。

関連情報

["ILM を使用してオブジェクトを管理する"](#)

["サーバ側の暗号化を使用"](#)

["PUT Object の場合"](#)

パーツをアップロードします

Upload Part 処理では、オブジェクトのマルチパートアップロード内のパートがアップロードされます。

サポートされる要求ヘッダー

次の要求ヘッダーがサポートされています。

- Content-Length
- Content-MD5

サーバ側の暗号化を行うための要求ヘッダー

Initiate Multipart Upload 要求に SSE-C 暗号化を指定した場合は、各 Upload Part 要求に次の要求ヘッダーも含める必要があります。

- x-amz-server-side-encryption-customer-algorithm:指定します AES256。
- x-amz-server-side-encryption-customer-key : Initiate Multipart Upload要求で指定した暗号化キーを指定します。
- x-amz-server-side-encryption-customer-key-MD5 : Initiate Multipart Upload要求で指定したMD5ダイジェストを指定します。



指定した暗号化キーが格納されることはありません。暗号化キーを紛失すると、対応するオブジェクトが失われます。お客様提供の鍵を使用してオブジェクト・データを保護する前に'サーバ側の暗号化の使用に関する考慮事項を確認してください

バージョン管理

マルチパートアップロードは、アップロードの開始、アップロードのリストの表示、パートのアップロード、アップロードしたパートのアセンブル、およびアップロードの完了の個別の処理に分けられます。Complete Multipart Upload 処理が実行されると、オブジェクトが作成されます（該当する場合はバージョン管理されます）。

関連情報

["サーバ側の暗号化を使用"](#)

Upload Part - Copy 処理は、データソースとしての既存のオブジェクトからデータをコピーすることで、オブジェクトのパートをアップロードします。

Upload Part - Copy 処理には、すべての Amazon S3 REST API の動作が実装されています。

この要求は、で指定されたオブジェクトデータの読み取りと書き込みを行います x-amz-copy-source-range StorageGRID システム内で実行する。

次の要求ヘッダーがサポートされています。

- x-amz-copy-source-if-match
- x-amz-copy-source-if-none-match
- x-amz-copy-source-if-unmodified-since
- x-amz-copy-source-if-modified-since

サーバ側の暗号化を行うための要求ヘッダー

Initiate Multipart Upload 要求に SSE-C 暗号化を指定した場合は、各 Upload Part - Copy 要求に次の要求ヘッダーも含める必要があります。

- x-amz-server-side-encryption-customer-algorithm:指定します AES256。
- x-amz-server-side-encryption-customer-key: Initiate Multipart Upload要求で指定した暗号化キーを指定します。
- x-amz-server-side-encryption-customer-key-MD5: Initiate Multipart Upload要求で指定したMD5ダイジェストを指定します。

ソースオブジェクトがユーザ指定のキーを使用して暗号化されている場合（SSE-C）は、オブジェクトを復号化してコピーできるように、Upload Part - Copy 要求に次の 3 つのヘッダーを含める必要があります。

- x-amz-copy-source-server-side-encryption-customer-algorithm:指定します AES256。
- x-amz-copy-source-server-side-encryption-customer-key:ソースオブジェクトの作成時に指定した暗号化キーを指定します
- x-amz-copy-source-server-side-encryption-customer-key-MD5:ソースオブジェクトの作成時に指定したMD5ダイジェストを指定します。



指定した暗号化キーが格納されることはありません。暗号化キーを紛失すると、対応するオブジェクトが失われます。お客様提供の鍵を使用してオブジェクト・データを保護する前に「サーバ側の暗号化の使用に関する考慮事項を確認してください

バージョン管理

マルチパートアップロードは、アップロードの開始、アップロードのリストの表示、パートのアップロード、アップロードしたパートのアセンブル、およびアップロードの完了の個別の処理に分けられます。Complete Multipart Upload 処理が実行されると、オブジェクトが作成されます（該当する場合はバージョン管理されます）。

Complete Multipart Upload 処理では、以前にアップロードされたパートをアセンブルすることで、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。

競合の解決

同一キーに書き込む2つのクライアントなど、競合するクライアント要求は、最新のWINS形式で解決されます。「latest-wins」評価のタイミングは、S3クライアントが処理を開始するタイミングではなく、StorageGRID システムが特定の要求を完了したタイミングに基づいています。

オブジェクトのサイズ

StorageGRID は、サイズが最大5TBのオブジェクトをサポートします。

要求ヘッダー

。 `x-amz-storage-class` 要求ヘッダーがサポートされ、一致するILMルールで取り込み動作にDual commitまたはBalancedが指定されている場合にStorageGRID で作成されるオブジェクトコピーの数に影響します。

- STANDARD

(デフォルト) ILM ルールで Dual commit オプションが使用されている場合、または Balanced オプションによって中間コピーが作成される場合に、デュアルコミットの取り込み処理を指定します。

- REDUCED_REDUNDANCY

ILM ルールで Dual commit オプションが使用されている場合、または Balanced オプションによって中間コピーが作成される場合に、シングルコミットの取り込み処理を指定します。



S3オブジェクトロックを有効にしてオブジェクトをバケットに取り込む場合は、を使用します REDUCED_REDUNDANCY オプションは無視されます。古い準拠バケットにオブジェクトを取り込む場合は、を参照してください REDUCED_REDUNDANCY オプションを指定するとエラーが返されます。StorageGRID では、常にデュアルコミットの取り込みが実行され、コンプライアンス要件が満たされます。



マルチパートアップロードが 15 日以内に完了しないと、非アクティブな処理としてマークされ、関連するすべてのデータがシステムから削除されます。



。 ETag 返される値はデータのMD5サムではなく、のAmazon S3 APIの実装に従います ETag マルチパートオブジェクトの値。

バージョン管理

マルチパートアップロードは、この処理で完了します。バケットでバージョン管理が有効になっている場合は、マルチパートアップロードの完了時にオブジェクトのバージョンが作成されます。

バケットでバージョン管理が有効になっている場合は、一意です `versionId` は、格納されているオブジェクトのバージョンに対して自動的に生成されます。これ `versionId` は、を使用して応答としても返されます

x-amz-version-id 応答ヘッダー。

バージョン管理が一時的停止中の場合は、オブジェクトバージョンはnullで格納されます versionId また、nullバージョンがすでに存在する場合は上書きされます。



バケットでバージョン管理が有効になっているときは、同じオブジェクトキーで同時に複数のマルチパートアップロードが実行されている場合でも、マルチパートアップロードが完了するたびに常に新しいバージョンが作成されます。バケットでバージョン管理が有効になっていないときは、マルチパートアップロードの開始後に、同じオブジェクトキーで別のマルチパートアップロードが開始されて先に完了することがあります。バージョン管理が有効になっていないバケットでは、最後に完了したマルチパートアップロードが優先されます。

レプリケーション、通知、またはメタデータ通知に失敗しました

マルチパートアップロードが行われるバケットでプラットフォームサービスが設定されている場合、関連するレプリケーション操作や通知操作が失敗してもマルチパートアップロードは正常に実行されます。

この状況が発生すると、Total Events（SMTT）のアラームがグリッドマネージャで生成されます。Last Event メッセージに、通知が失敗した最後のオブジェクトについて、「Failed to publish notifications for bucket-name object key」と表示されます。（このメッセージを表示するには、*** Nodes > * _ Storage Node > * Events ***を選択します。表の一番上にLast Eventが表示されます）。イベントメッセージは、にも表示されます /var/local/log/bycast-err.log。

テナントでは、オブジェクトのメタデータまたはタグを更新することで、失敗したレプリケーションまたは通知をトリガーできます。テナントでは、既存の値を再送信し、不要な変更を回避できます。

関連情報

["ILM を使用してオブジェクトを管理する"](#)

エラー応答

StorageGRID システムでは、該当する S3 REST API の標準のエラー応答をすべてサポートしています。また、StorageGRID の実装では、カスタム応答もいくつか追加されています。

サポートされている **S3 API** のエラーコード

名前	HTTP ステータス
アクセスが拒否されました	403 禁止
BadDigest の略	400 不正な要求です
BucketAlreadyExists のようになりました	409 競合
BucketNotEmpty のように入力します	409 競合
IncompleteBody	400 不正な要求です

名前	HTTP ステータス
内部エラー	500 Internal Server Error （内部サーバエラー）
InvalidAccessKeyId	403 禁止
アンヴァリッドドキュメント	400 不正な要求です
InvalidBucketName の略	400 不正な要求です
InvalidBucketState の場合	409 競合
InvalidDigest の略	400 不正な要求です
InvalidEncryptionAlgorithmError	400 不正な要求です
InvalidPart	400 不正な要求です
InvalidPartOrder	400 不正な要求です
InvalidRange ：無効な範囲	416 リクエストされた範囲が適合しません
InvalidRequest	400 不正な要求です
InvalidStorageClass	400 不正な要求です
InvalidTag	400 不正な要求です
InvalidURI	400 不正な要求です
KeyTooLong の 2 つのグループがあります	400 不正な要求です
MalformedXML の場合	400 不正な要求です
MetadataTooLarge	400 不正な要求です
MethodNotAllowed のように入力します	405 メソッドは許可されていません
MissingContentLength （ MissingContentLength ）	411 長さが必要です
MissingRequestBodyError	400 不正な要求です
MissingSecurityHeader	400 不正な要求です

名前	HTTP ステータス
NoSuchBucket	404 が見つかりません
NoSuchKey	404 が見つかりません
NoSuchUpload	404 が見つかりません
実装なし	501 は実装されていません
NoSuchBucketPolicy のようになります	404 が見つかりません
ObjectLockConfigurationNotFoundError	404 が見つかりません
PreconditionalFailed	412 事前条件が失敗しました
RequestTimeTooSkewed	403 禁止
サービスを利用できません	503 Service Unavailable （503 サービスが利用でき
SignatureDoesNotMatch のように指定します	403 禁止
TooManyBuckets	400 不正な要求です
UserKeyMustBeSpecified	400 不正な要求です

StorageGRID カスタムのエラーコード

名前	説明	HTTP ステータス
XBucketLifecycleNotAllowed のようになりました	バケットライフサイクル設定は従来の準拠バケットには適用されません	400 不正な要求です
XBucketPolicyParseException	受信したバケットポリシー JSON を解析できませんでした。	400 不正な要求です
XCompliConflict	準拠設定が古いため、処理が拒否されました。	403 禁止
XCompliReducedRedundancyForbidden	レガシー準拠バケットでは冗長性の低下は許可されません	400 不正な要求です

名前	説明	HTTP ステータス
XMaxBucketPolicyLengthExceeded (XMaxBucketLengthExceeded)	ポリシーが許容される最大バケットポリシー長を超えています。	400 不正な要求です
XMissingInternalRequestHeader	内部要求のヘッダーがありません。	400 不正な要求です
XNoSuchBucketCompliance です	指定したバケットで従来の準拠が有効になっていません。	404 が見つかりません
XNotAcceptable	要求に含まれている Accept ヘッダーの 1 つ以上を満たすことができませんでした。	406 は許容されません
XNotImplemented	指定した要求の処理には、実装されていない機能が含まれます。	501 は実装されていません

StorageGRID の S3 REST API の処理

StorageGRID システム固有の処理が S3 REST API に追加されています。

GET Bucket consistency 要求を実行します

GET Bucket consistency 要求を使用すると、特定のバケットに適用されている整合性レベルを確認できます。

新たに作成したオブジェクトに対しては、リードアフターライト整合性を保証するようにデフォルトの整合性制御が設定されます。

この処理を完了するには、s3：GetBucketConsistency権限またはrootアカウントが必要です。

要求例

```
GET /bucket?x-ntap-sg-consistency HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

応答

応答XMLで、<Consistency> は次のいずれかの値を返します。

整合性制御	説明
すべて	すべてのノードが即座にデータを受け取り、受け取れない場合は要求が失敗します。

整合性制御	説明
strong-global	すべてのサイトのすべてのクライアント要求について、リードアフターライト整合性が保証されます。
strong-site	1つのサイト内のすべてのクライアント要求について、リードアフターライト整合性が保証されます。
read-after-new-write の場合	<p>(デフォルト) 新規オブジェクトにはリードアフターライト整合性を、オブジェクトの更新には結果整合性を提供します。高可用性が確保され、データ保護が保証されます。Amazon S3の整合性に相当します。</p> <ul style="list-style-type: none"> 注：存在しないオブジェクトに対してアプリケーションが HEAD 要求を使用すると、使用できないストレージノードがあると「500 Internal Server Error」が大量に返される可能性があります。これらのエラーを回避するには、Amazon S3 と同様の整合性の保証が必要でない限り、整合性制御を「available」に設定します。
available (HEAD 処理は結果整合性)	「read-after-new-write」整合性レベルと動作は同じですが、HEAD 処理については結果整合性のみを提供します。ストレージ・ノードが使用できない場合、リードアフター・新規ライトよりもヘッド操作の可用性が高くなりますAmazon S3 の整合性と異なるのは HEAD 処理のみです。

応答例

```

HTTP/1.1 200 OK
Date: Fri, 18 Sep 2020 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/11.5.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<Consistency xmlns="http://s3.storagegrid.com/doc/2015-02-01/">read-after-
new-write</Consistency>

```

関連情報

["整合性制御"](#)

PUT Bucket consistency 要求

PUT Bucket consistency 要求を使用すると、バケットで実行される処理に適用する整合性レベルを指定できます。

新たに作成したオブジェクトに対しては、リードアフターライト整合性を保証するようにデフォルトの整合性制御が設定されます。

この処理を完了するには、s3:PutBucketConsistency権限またはrootアカウントが必要です。

リクエスト

。 x-ntap-sg-consistency パラメータには次のいずれかの値を指定する必要があります。

整合性制御	説明
すべて	すべてのノードが即座にデータを受け取り、受け取れない場合は要求が失敗します。
strong-global	すべてのサイトのすべてのクライアント要求について、リードアフターライト整合性が保証されます。
strong-site	1つのサイト内のすべてのクライアント要求について、リードアフターライト整合性が保証されます。
read-after-new-write の場合	<p>(デフォルト) 新規オブジェクトにはリードアフターライト整合性を、オブジェクトの更新には結果整合性を提供します。高可用性が確保され、データ保護が保証されます。Amazon S3の整合性に相当します。</p> <p>・ 注：存在しないオブジェクトに対してアプリケーションが HEAD 要求を使用すると、使用できないストレージノードがあると「500 Internal Server Error」が大量に返される可能性があります。これらのエラーを回避するには、Amazon S3と同様の整合性の保証が必要でない限り、整合性制御を「available」に設定します。</p>
available (HEAD 処理は結果整合性)	「read-after-new-write」整合性レベルと動作は同じですが、HEAD 処理については結果整合性ののみを提供します。ストレージ・ノードが使用できない場合、リードアフター・新規ライトよりもヘッド操作の可用性が高くなりますAmazon S3 の整合性と異なるのは HEAD 処理のみです。

- ・ 注：* 一般的には、「read-after-new-write」整合性制御値を使用する必要があります。要求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、API 要求ごとに整合性制御を指定するようにクライアントを設定します。バケットレベルの整合性制御は最後の手段と考えてください。

要求例

```
PUT /bucket?x-ntap-sg-consistency=strong-global HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

関連情報

"整合性制御"

GET Bucket last access time 要求

GET Bucket last access time 要求を使用すると、最終アクセス時間の更新が個々のバケットで有効になっているか無効になっているかを確認できます。

この処理を完了するには、s3 : GetBucketLastAccessTime権限またはrootアカウントが必要です。

要求例

```
GET /bucket?x-ntap-sg-lastaccesstime HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

応答例

次の例では、バケットの最終アクセス時間の更新が有効になっています。

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/10.3.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<LastAccessTime xmlns="http://s3.storagegrid.com/doc/2015-02-01/">enabled
</LastAccessTime>
```

PUT Bucket last access time 要求の場合

PUT Bucket last access time 要求を使用すると、最終アクセス時間の更新を個々のバケットで有効または無効にできます。最終アクセス時間の更新を無効にするとパフォーマンスが向上します。バージョン 10.3.0 以降で作成されたバケットに対しては、いずれもデフォルトで無効になります。

この処理を完了するには、バケットのs3:PutBucketLastAccessTime権限またはrootアカウントが必要です。



StorageGRID バージョン 10.3 以降では、すべての新規バケットで最終アクセス時間の更新がデフォルトで無効になります。以前のバージョンの StorageGRID で作成されたバケットにこの新たなデフォルトの動作を適用する場合は、対象となるバケットごとに最終アクセス時間の更新を無効にする必要があります。Tenant Manager またはテナント管理 API の PUT Bucket last access time 要求、* S3 * > * Buckets * > * Change Last Access Setting * チェックボックスを使用して、最終アクセス時間の更新を有効または無効にできます。

バケットで最終アクセス時間の更新が無効になっている場合、バケットの処理の動作は次のようになります。

- GET Object、GET Object ACL、GET Object Tagging、HEAD Object の各要求では、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 PUT Object - Copy 要求と PUT Object Tagging 要求では、最終アクセス時間も更新されます。オブジェクトは ILM 評価のキューに追加されます。
- ソースバケットで最終アクセス時間の更新が無効になっている場合は、PUT Object - Copy 要求でソースバケットの最終アクセス時間が更新されません。コピーされたオブジェクトは、ソースバケットの ILM 評価のキューに追加されません。ただし、デスティネーションについては、PUT Object - Copy 要求で常に最終アクセス時間が更新されます。オブジェクトのコピーは、ILM 評価のキューに追加されます。
- Complete Multipart Upload 要求では、最終アクセス時間が更新されます。完了したオブジェクトは、ILM 評価のキューに追加されます。

例をリクエストする

この例では、バケットの最終アクセス時間を有効にしています。

```
PUT /bucket?x-ntap-sg-lastaccesstime=enabled HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

この例では、バケットの最終アクセス時間を無効にしています。

```
PUT /bucket?x-ntap-sg-lastaccesstime=disabled HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

関連情報

["テナントアカウントを使用する"](#)

DELETE Bucket metadata notification configuration 要求

DELETE Bucket metadata notification configuration 要求では、設定 XML を削除することで、個々のバケットで検索統合サービスを無効化できます。

この処理を完了するには、バケットのs3:DeleteBucketMetadataNotification権限またはrootアカウントが必要です。

要求例

次の例は、バケットの検索統合サービスを無効にする方法を示しています。

```
DELETE /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

GET Bucket metadata notification configuration 要求

GET Bucket metadata notification configuration 要求では、個々のバケットで検索統合を設定するために使用する設定 XML を読み出すことができます。

この処理を完了するには、s3:GetBucketMetadataNotification権限またはrootアカウントが必要です。

要求例

次の要求は、というバケットのメタデータ通知設定を読み出します bucket。

```
GET /bucket?x-ntap-sg-metadata-notification HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

応答

応答の本文には、バケットのメタデータ通知設定が含まれます。メタデータ通知設定では、バケットでの検索統合の設定を確認できます。つまり、どのオブジェクトにインデックスが付けられ、そのオブジェクトメタデータがどのエンドポイントに送信されるかを確認できます。

```

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>rule-status</Status>
    <Prefix>key-prefix</Prefix>
    <Destination>
      <Urn>arn:aws:es:_region:account-
ID_:domain/_mydomain/myindex/mytype_</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Rule-2</ID>
    ...
  </Rule>
  ...
</MetadataNotificationConfiguration>

```

各メタデータ通知設定には、1 つ以上のルールが含まれています。各ルールは、環境 がオブジェクトを指定し、StorageGRID がオブジェクトメタデータを送信するデスティネーションを指定します。デスティネーションは、StorageGRID エンドポイントの URN を使用して指定する必要があります。

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

名前	説明	必須
ステータス	<p>Status には「 Enabled 」または「 Disabled 」を指定できます。無効になっているルールについては操作が実行されません。</p> <p>Rule 要素に含まれています。</p>	はい。
プレフィックス	<p>プレフィックスと一致するオブジェクトにルールが適用され、そのメタデータが指定したデスティネーションに送信されます。</p> <p>すべてのオブジェクトを照合するには、空のプレフィックスを指定します。</p> <p>Rule 要素に含まれています。</p>	はい。
宛先	<p>ルールのデスティネーションのコンテナタグ。</p> <p>Rule 要素に含まれています。</p>	はい。

名前	説明	必須
URN	<p>オブジェクトメタデータが送信されるデスティネーションの URN。次のプロパティを持つ StorageGRID エンドポイントの URN を指定する必要があります。</p> <ul style="list-style-type: none"> • es 3 番目のエレメントである必要があります。 • URNの末尾に、メタデータが格納されるインデックスとタイプを、の形式で指定する必要があります domain-name/myindex/mytype。 <p>エンドポイントは、Tenant Manager またはテナント管理 API を使用して設定します。形式は次のとおりです。</p> <ul style="list-style-type: none"> • arn:aws:es:_region:account-ID_:domain/mydomain/myindex/mytype • urn:mysite:es:::mydomain/myindex/mytype <p>エンドポイントは設定 XML を送信する前に設定する必要があります。そうしないと、404 エラーで設定が失敗します。</p> <p>Urn は Destination 要素に含まれています。</p>	はい。

応答例

間に含まれるXML

<MetadataNotificationConfiguration></MetadataNotificationConfiguration> タグは、バケットに対して検索統合エンドポイントとの統合がどのように設定されているかを示します。次の例では、という名前のElasticsearchインデックスにオブジェクトメタデータが送信されています current と入力します 2017 という名前のAWSドメインでホストされている records。

```
HTTP/1.1 200 OK
Date: Thu, 20 Jul 2017 18:24:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/11.0.0
x-amz-request-id: 3832973499
Content-Length: 264
Content-Type: application/xml

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>Enabled</Status>
    <Prefix>2017</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-
1:33333333:domain/records/current/2017</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

関連情報

["テナントアカウントを使用する"](#)

PUT Bucket metadata notification configuration 要求

PUT Bucket metadata notification configuration 要求を使用すると、個々のバケットで検索統合サービスを有効化できます。要求の本文に含めるメタデータ通知設定 XML では、デスティネーション検索インデックスにメタデータを送信するオブジェクトを指定します。

この処理を完了するには、バケットのs3:PutBucketMetadataNotification権限またはrootアカウントが必要です。

リクエスト

要求の本文にメタデータ通知設定が含まれている必要があります。各メタデータ通知設定には、1 つ以上のルールが含まれています。各ルールは、環境 がオブジェクトを指定し、StorageGRID がオブジェクトメタデータを送信するデスティネーションを指定します。

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

プレフィックスが重複している設定は無効で、送信時に拒否されます。たとえば、プレフィックスがのオブジェクト用のルールを1つ含む設定などです test プレフィックスが付いたオブジェクトの2番目のルールです test2 許可されません。

デスティネーションは、StorageGRID エンドポイントの URN を使用して指定する必要があります。エンドポイントは、メタデータ通知設定が送信されたときに存在している必要があります。存在していない場合、要

求がとして失敗します 400 Bad Request。エラーメッセージ：Unable to save the metadata notification (search) policy. The specified endpoint URN does not exist: *URN*.

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

次の表に、メタデータ通知設定 XML の要素を示します。

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

名前	説明	必須
ステータス	<p>Status には「 Enabled 」または「 Disabled 」を指定できます。無効になっているルールについては操作が実行されません。</p> <p>Rule 要素に含まれています。</p>	はい。
プレフィックス	<p>プレフィックスと一致するオブジェクトにルールが適用され、そのメタデータが指定したデスティネーションに送信されます。</p> <p>すべてのオブジェクトを照合するには、空のプレフィックスを指定します。</p> <p>Rule 要素に含まれています。</p>	はい。
宛先	<p>ルールのデスティネーションのコンテナタグ。</p> <p>Rule 要素に含まれています。</p>	はい。

名前	説明	必須
URN	<p>オブジェクトメタデータが送信されるデスティネーションの URN。次のプロパティを持つ StorageGRID エンドポイントの URN を指定する必要があります。</p> <ul style="list-style-type: none"> • es 3 番目のエレメントである必要があります。 • URNの末尾に、メタデータが格納されるインデックスとタイプを、の形式で指定する必要があります domain-name/myindex/mytype。 <p>エンドポイントは、Tenant Manager またはテナント管理 API を使用して設定します。形式は次のとおりです。</p> <ul style="list-style-type: none"> • arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype • urn:mysite:es:::mydomain/myindex/mytype <p>エンドポイントは設定 XML を送信する前に設定する必要があります。そうしないと、404 エラーで設定が失敗します。</p> <p>Urn は Destination 要素に含まれています。</p>	はい。

例をリクエストする

次の例は、バケットの検索統合を有効にする方法を示しています。この例では、すべてのオブジェクトのオブジェクトメタデータが同じデスティネーションに送信されます。


```
PUT /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>

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

この例では、プレフィックスに一致するオブジェクトのオブジェクトメタデータを指定します。/images が1つのデスティネーションに送信され、プレフィックスに一致するオブジェクトのオブジェクトメタデータが送信されます。/videos 2番目の送信先に送信されます。

```
PUT /graphics?x-ntap-sg-metadata-notification HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Images-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/images</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-1:33333333:domain/es-
domain/graphics/imagetype</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Videos-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/videos</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

関連情報

"テナントアカウントを使用する"

検索統合サービスで生成される JSON

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

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

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

メタデータ通知に含まれているオブジェクトメタデータ

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

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

を入力します	項目名	説明
バケットとオブジェクトの情報	バケット	バケットの名前
バケットとオブジェクトの情報	キーを押します	オブジェクトキーの名前
バケットとオブジェクトの情報	versionId	バージョン管理されたバケット内のオブジェクトのオブジェクトバージョン
バケットとオブジェクトの情報	リージョン	たとえば、バケットのリージョンのように指定します us-east-1
システムメタデータ	サイズ	HTTP クライアントから認識できるオブジェクトのサイズ（バイト）
システムメタデータ	MD5	オブジェクトのハッシュ
ユーザメタデータ	メタデータ <i>key:value</i>	オブジェクトのすべてのユーザメタデータをキーと値のペアとして格納

を入力します	項目名	説明
タグ	タグ <i>key:value</i>	オブジェクトに対して定義されたすべてのオブジェクトタグをキーと値のペアとして使用します

- 注：StorageGRID は、タグとユーザメタデータに対して、文字列または S3 イベント通知として Elasticsearch に日付と番号を渡します。これらの文字列を日付または数値として解釈するように Elasticsearch を設定するには、動的フィールドマッピングおよびマッピング日付形式に関する Elasticsearch の手順に従ってください。検索統合サービスを設定する前に、インデックスの動的フィールドマッピングを有効にする必要があります。ドキュメントにインデックスを付けた後は、インデックス内のドキュメントのフィールドタイプを編集できません。

GET Storage Usage 要求の略

GET Storage Usage 要求を使用すると、アカウントで使用しているストレージの総容量とアカウントに関連付けられているバケットごとの使用容量を確認できます。

アカウントとそのバケットで使用されているストレージの量は、で GET Service 要求を変更して取得できます `x-ntap-sg-usage` クエリパラメータ。バケットによるストレージの使用量は、システムで処理される PUT 要求や DELETE 要求とは別に追跡されます。特にシステムの負荷が高い場合などは、使用量の値が要求の処理に基づく想定値と同じになるまでに少し時間がかかることがあります。

デフォルトでは、StorageGRID は strong-global 整合性を使用して、使用状況の情報を取得します。strong-global 整合性が保証されていない場合、StorageGRID は、強いサイトで整合性のある使用状況情報を取得しようとします。

この処理を完了するには、`s3:ListAllMyBuckets` 権限または root アカウントが必要です。

要求例

```
GET /?x-ntap-sg-usage HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

応答例

次の例は、2 つのバケットに 4 つのオブジェクトと 12 バイトのデータが格納されたアカウントです。各バケットには、2 つのオブジェクトと 6 バイトのデータが格納されています。

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 00:49:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/10.2.0
x-amz-request-id: 727237123
Content-Length: 427
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<UsageResult xmlns="http://s3.storagegrid.com/doc/2015-02-01">
<CalculationTime>2014-11-19T05:30:11.000000Z</CalculationTime>
<ObjectCount>4</ObjectCount>
<DataBytes>12</DataBytes>
<Buckets>
<Bucket>
<Name>bucket1</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
<Bucket>
<Name>bucket2</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
</Buckets>
</UsageResult>
```

バージョン管理

には、格納されているすべてのオブジェクトバージョンが関連します ObjectCount および DataBytes 応答の値。削除マークはに追加されません ObjectCount 合計。

関連情報

"整合性制御"

従来の準拠のためのバケット要求が廃止されました

従来の準拠機能で作成されたバケットの管理には、StorageGRID S3 REST API の使用が必要になる場合があります。

コンプライアンス機能は廃止されました

以前のバージョンの StorageGRID で提供されていた StorageGRID 準拠機能は廃止され、S3 オブジェクトロックに置き換えられました。

グローバル準拠設定を有効にしている場合は、StorageGRID 11.5にアップグレードすると、グローバルなS3 オブジェクトロック設定が自動的に有効になります。準拠を有効にした新しいバケットは作成できなくなりま

した。ただし、必要に応じて、StorageGRID S3 REST API を使用して、従来の準拠バケットを管理できます。

["S3 オブジェクトロックを使用する"](#)

["ILM を使用してオブジェクトを管理する"](#)

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

廃止：準拠のための **PUT Bucket** 要求の変更

SGCompliance XML 要素は廃止されました。これまでは、この StorageGRID カスタム要素を PUT Bucket 要求のオプションの XML 要求の本文に含めて準拠バケットを作成できました。



以前のバージョンの StorageGRID で提供されていた StorageGRID 準拠機能は廃止され、S3 オブジェクトロックに置き換えられました。

["S3 オブジェクトロックを使用する"](#)

["ILM を使用してオブジェクトを管理する"](#)

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

準拠を有効にした新しいバケットを作成することはできなくなりました。準拠バケットを新しく作成するために PUT Bucket 要求の変更を使用しようとすると、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.
```

関連情報

["ILM を使用してオブジェクトを管理する"](#)

["テナントアカウントを使用する"](#)

廃止予定： **GET Bucket compliance** 要求

GET Bucket compliance 要求は廃止されました。ただし、既存のレガシー準拠バケットに対して現在有効な準拠設定を引き続き確認することができます。



以前のバージョンの StorageGRID で提供されていた StorageGRID 準拠機能は廃止され、S3 オブジェクトロックに置き換えられました。

["S3 オブジェクトロックを使用する"](#)

["ILM を使用してオブジェクトを管理する"](#)

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

この処理を完了するには、s3：GetBucketCompliance権限またはrootアカウントが必要です。

要求例

次の要求例では、という名前のバケットの準拠設定を確認できます mybucket。

```
GET /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

応答例

応答XMLで、<SGCompliance> バケットで有効な準拠設定が表示されます。次の応答例では、バケットの準拠設定が示されており、各オブジェクトはグリッドに取り込まれてから 1 年間（ 525、 600 分）保持されます。このバケットには現在リーガルホールドはありません。各オブジェクトは 1 年後に自動的に削除されます。

```
HTTP/1.1 200 OK
Date: <em>date</em>
Connection: <em>connection</em>
Server: StorageGRID/11.1.0
x-amz-request-id: <em>request ID</em>
Content-Length: <em>length</em>
Content-Type: application/xml

<SGCompliance>
  <RetentionPeriodMinutes>525600</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

名前	説明
RetentionPeriodMinutes です	このバケットに追加されたオブジェクトの保持期間を分で指定します。保持期間は、オブジェクトがグリッドに取り込まれたときからの期間です。
LegalHold のようになります	<ul style="list-style-type: none">• True ：このバケットは、現在リーガルホールドの対象です。このバケット内のオブジェクトは、保持期間が過ぎたあとも、リーガルホールドが解除されるまで削除できません。• False ：このバケットは、現在リーガルホールドの対象ではありません。このバケット内のオブジェクトは、保持期間が過ぎたら削除できます。

名前	説明
自動削除	<ul style="list-style-type: none"> • True : このバケット内のオブジェクトは、バケットがリーガルホールドの対象である場合を除き、保持期間が過ぎると自動的に削除されます。 • false : このバケット内のオブジェクトは、保持期間が過ぎても自動的に削除されません。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

バケットが準拠バケットとして作成されていない場合、応答のHTTPステータスコードはになります 404 Not Found`を返します `XNoSuchBucketCompliance。

関連情報

["ILM を使用してオブジェクトを管理する"](#)

["テナントアカウントを使用する"](#)

廃止予定： **PUT Bucket compliance** 要求

PUT Bucket compliance 要求は廃止されました。ただし、この要求を引き続き使用して、既存のレガシー準拠バケットの準拠設定を変更できます。たとえば、既存のバケットをリーガルホールドの対象にしたり、バケットの保持期間を長くしたりできます。



以前のバージョンの StorageGRID で提供されていた StorageGRID 準拠機能は廃止され、S3 オブジェクトロックに置き換えられました。

["S3 オブジェクトロックを使用する"](#)

["ILM を使用してオブジェクトを管理する"](#)

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

この処理を完了するには、s3:PutBucketCompliance権限またはrootアカウントが必要です。

PUT Bucket compliance 要求を発行する際は、準拠設定のすべてのフィールドに値を指定する必要があります。

要求例

次の要求例では、という名前のバケットの準拠設定を変更します mybucket。この例では、のオブジェクトが表示されています mybucket オブジェクトがグリッドに取り込まれてから1年間ではなく2年間（1、051、200分）保持されます。このバケットにリーガルホールドはありません。各オブジェクトは2年後に自動的に削除されます。


```

PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization name</em>
Host: <em>host</em>
Content-Length: 152

<SGCompliance>
  <RetentionPeriodMinutes>1051200</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>

```

名前	説明
RetentionPeriodMinutes です	<p>このバケットに追加されたオブジェクトの保持期間を分で指定します。保持期間は、オブジェクトがグリッドに取り込まれたときからの期間です。</p> <ul style="list-style-type: none"> • 注意： 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。設定したバケットの保持期間は、増やすことはできますが減らすことはできません。
LegalHold のようになります	<ul style="list-style-type: none"> • True ：このバケットは、現在リーガルホールドの対象です。このバケット内のオブジェクトは、保持期間が過ぎたあとも、リーガルホールドが解除されるまで削除できません。 • False ：このバケットは、現在リーガルホールドの対象ではありません。このバケット内のオブジェクトは、保持期間が過ぎたら削除できます。
自動削除	<ul style="list-style-type: none"> • True ：このバケット内のオブジェクトは、バケットがリーガルホールドの対象である場合を除き、保持期間が過ぎると自動的に削除されます。 • false ：このバケット内のオブジェクトは、保持期間が過ぎても自動的に削除されません。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。

準拠設定の整合性レベル

PUT Bucket compliance 要求によって S3 バケットの準拠設定を更新すると、StorageGRID は、グリッド全体のバケットのメタデータを更新しようとします。デフォルトでは、StorageGRID は * strong-global * 整合性レベルを使用し、バケットのメタデータを含むすべてのデータセンターサイトおよびストレージノードで、変更された準拠設定のリードアフターライト整合性を保証します。

データセンターサイトまたはサイトの複数のストレージノードが利用できないために、StorageGRID が「strong-global」の整合性レベルを保証できない場合は、応答のHTTPステータスコードがになります 503 Service Unavailable.

この応答を受け取った場合は、必要なストレージサービスをできるだけ早く利用可能にするために、グリッド管理者に問い合わせる必要があります。グリッド管理者が各サイトで十分な数のストレージノードを利用可能にできない場合は、テクニカルサポートから、* strong-site * 整合性レベルを強制的に適用することで、失敗した要求を再試行するよう指示される場合があります。



テクニカルサポートから指示があった場合や、このレベルを使用した場合の影響を理解している場合を除き、PUT Bucket compliance で * strong-site * 整合性レベルを強制的に適用することは避けてください。

整合性レベルを * strong-site * に下げると、StorageGRID は、サイト内のクライアント要求に対してのみ、更新された準拠設定のリードアフターライト整合性を保証します。そのため、すべてのサイトおよびストレージノードが利用可能になるまでの間、StorageGRID システムにはこのバケットに対して複数の異なる設定が一時的に存在することになる場合があります。整合性のない設定を使用すると、予期せぬ望ましくない動作が生じる可能性がありますたとえば、あるバケットをリーガルホールドの対象にして、低い整合性レベルを強制的に適用すると、一部のデータセンターサイトでバケットの以前の準拠設定（つまり、リーガルホールドの対象外の状態）が引き続き適用される場合があります。したがって、リーガルホールドの対象と思われるオブジェクトは、保持期間が経過すると、ユーザによって削除される場合と、AutoDelete によって削除される場合があります。

strong-site *整合性レベルを強制的に適用するには、PUT Bucket compliance要求を再発行し、を含めてください Consistency-Control HTTP要求ヘッダー。

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Consistency-Control: strong-site
```

エラー応答

- バケットが準拠バケットとして作成されていない場合、応答のHTTPステータスコードはになります 404 Not Found.
- 状況 RetentionPeriodMinutes 要求がバケットの現在の保持期間よりも短い場合、HTTPステータスコードはになります 400 Bad Request.

関連情報

["廃止：準拠のための PUT Bucket 要求の変更"](#)

["テナントアカウントを使用する"](#)

["ILM を使用してオブジェクトを管理する"](#)

バケットとグループのアクセスポリシー

StorageGRID では、Amazon Web Services（AWS）ポリシー言語を使用して、S3 テナントによるバケットおよびバケット内のオブジェクトへのアクセスを制御できます。StorageGRID システムには、S3 REST API ポリシー言語のサブセットが実装され

ています。S3 API のアクセスポリシーは JSON 形式で記述されます。

アクセスポリシーの概要

StorageGRID では 2 種類のアクセスポリシーがサポートされています。

- * バケットポリシー *。GET Bucket policy、PUT Bucket policy、DELETE Bucket policy の各 S3 API 処理を使用して設定します。バケットポリシーはバケットに関連付けられ、バケットとそのオブジェクトへのバケット所有者アカウントやその他のアカウントのユーザによるアクセスを制御するために使用されます。バケットポリシー環境は 1 つのバケットのみで、場合によっては複数のグループに分かれています。
- * グループポリシー *。Tenant Manager またはテナント管理 API を使用して設定します。グループポリシーはアカウントのグループに関連付けられ、そのアカウントが所有する特定のリソースにそのグループがアクセスできるように設定されます。グループポリシー環境は 1 つのグループに限定され、場合によっては複数のバケットに適用されます。

StorageGRID のバケットとグループのポリシーは、Amazon が定義している特定の文法に従って記述されます。各ポリシーは一連のステートメントからなり、各ステートメントは次の要素で構成されます。

- ステートメント ID (SID) (オプション)
- 効果
- プリンシパル / NotPrincipal
- リソース / メモリソース
- アクション / NotAction
- Condition (オプション)

次の構造を使用して、権限を指定するポリシーステートメントが構築されます。<Effect> を付与して、<Condition> に該当する場合に <Principal> に <Resource> に対する <Action> の実行を許可または拒否します。

各ポリシー要素は、特定の機能に使用されます。

要素 (Element)	説明
SID	Sid 要素はオプションです。SID は、ユーザの概要としてのみ使用されます。StorageGRID システムに格納はされますが、システムで解釈されません。
効果	Effect 要素では、指定した処理を許可するか拒否するかを指定します。Action 要素でサポートされるキーワードを使用して、バケットやオブジェクトで許可（または拒否）する処理を指定する必要があります。

要素（Element）	説明
プリンシパル / NotPrincipal	<p>ユーザ、グループ、およびアカウントに特定のリソースへのアクセスと特定の操作の実行を許可できます。要求に S3 の署名が含まれていない場合は、ワイルドカード文字（*）をプリンシパルとして指定することで匿名アクセスが許可されます。デフォルトでは、アカウントが所有するリソースへのアクセスは root アカウントにのみ許可されます。</p> <p>Principal 要素を指定する必要があるのはバケットポリシーだけです。グループポリシーの場合は、ポリシーが関連付けられたグループが暗黙的にプリンシパルになります。</p>
リソース / メモリソース	Resource 要素では、バケットとオブジェクトを指定します。Amazon リソースネーム（ARN）を使用してリソースを指定し、バケットやオブジェクトに対する権限を許可または拒否することができます。
アクション / NotAction	権限は Action 要素と Effect 要素の 2 つで構成されます。グループがリソースを要求すると、リソースへのアクセスが許可または拒否されます。権限を明示的に割り当てていないかぎりアクセスは拒否されますが、明示的な拒否を使用して別のポリシーで付与された権限を上書きすることもできます。
条件	Condition 要素はオプションです。条件を使用すると、ポリシーを適用する条件を示す式を作成できます。

Action 要素では、ワイルドカード文字（*）を使用してすべての処理または処理のサブセットを指定できます。たとえば、次の Action の値は、s3 : GetObject、s3 : PutObject、s3 : DeleteObject などの権限に一致します。

```
s3:*Object
```

Resource 要素では、ワイルドカード文字（*）および（?）を使用できます。アスタリスク（*）は 0 文字以上の文字に一致し、疑問符（?）は 0 文字以上の文字に一致します。任意の 1 文字に一致します。

Principal 要素では、匿名アクセスを設定してすべてのユーザに権限を付与する場合を除き、ワイルドカード文字はサポートされません。たとえば、Principal の値としてワイルドカード（*）を設定します。

```
"Principal": "*"

```

次の例では、Effect、Principal、Action、および Resource の各要素を使用して記述します。次の例は、「許可」の効果を使用してプリンシパル、admin グループを指定したバケットポリシーのステートメントを示しています federated-group/admin 財務グループなどです federated-group/finance、アクションを

実行する権限 `s3:ListBucket` をバケットにインストールします `mybucket` そしてアクション `s3:GetObject` そのバケット内のすべてのオブジェクト。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::27233906934684427525:federated-group/admin",
          "arn:aws:iam::27233906934684427525:federated-group/finance"
        ]
      },
      "Action": [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:iam:s3::mybucket",
        "arn:aws:iam:s3::mybucket/*"
      ]
    }
  ]
}
```

バケットポリシーのサイズの上限は 20、480 バイトで、グループポリシーのサイズの上限は 5、120 バイトです。

関連情報

["テナントアカウントを使用する"](#)

ポリシーの整合性制御設定

デフォルトでは、グループポリシーに対するすべての更新の整合性レベルは結果整合性です。グループポリシーが整合した状態になっても、ポリシーキャッシュのために、変更が有効になるまでさらに 15 分を要することがあります。デフォルトでは、バケットポリシーに対するすべての更新の整合性レベルも結果整合性です。

バケットポリシーの更新の整合性保証は必要に応じて変更できます。たとえば、セキュリティ上の理由から、できるだけ早くバケットポリシーの変更を有効にしなければならない場合があります。

この場合は、を設定できます `Consistency-Control PUT Bucket policy` 要求のヘッダーを指定するか、`PUT Bucket` 整合性要求を使用できます。この要求で整合性制御を変更する場合は、値「`*all*`」を使用して最高レベルのリードアフターライト整合性を保証する必要があります。それ以外の整合性制御値を `PUT Bucket consistency` 要求のヘッダーで指定すると、要求は拒否されます。`PUT Bucket policy` 要求でそれ以外の値を指定した場合は、値が無視されます。バケットポリシーが整合した状態になっても、ポリシーキャッシュのために、変更が有効になるまでさらに 8 秒を要することがあります。



新しいバケットポリシーを速やかに有効にするために整合性レベルを * all * に設定する場合は、処理が完了したあとに必ずバケットレベルの制御を元の値に戻してください。そうしないと、それ以降のすべてのバケット要求で * all * 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、Principal 要素と Resource 要素で ARN を使用します。

- S3 リソースの ARN の指定には次の構文を使用します。

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

- アイデンティティリソースの ARN（ユーザおよびグループ）の指定には次の構文を使用します。

```
arn:aws:iam::account_id:root
arn:aws:iam::account_id:user/user_name
arn:aws:iam::account_id:group/group_name
arn:aws:iam::account_id:federated-user/user_name
arn:aws:iam::account_id:federated-group/group_name
```

その他の考慮事項：

- オブジェクトキーの一部にワイルドカードとしてアスタリスク（*）を使用すると、0 文字以上の文字に一致します。
- オブジェクトキーで指定できる国際文字は、JSON UTF-8 形式または JSON \u エスケープシーケンスを使用してエンコードする必要があります。パーセントエンコーディングはサポートされていません。

"RFC 2141 の URN 構文"

PUT Bucket policy 処理の HTTP 要求の本文は、charset=UTF-8 でエンコードする必要があります。

ポリシーでのリソースの指定

ポリシーステートメントでは、Resource 要素を使用して、権限を許可または拒否するバケットやオブジェクトを指定できます。

- Resource 要素はポリシーの各ステートメントに必要です。ポリシーでは、リソースは要素で示されます Resource または、`NotResource` 除外のため。
- リソースは S3 リソースの ARN で指定します。例：

```
"Resource": "arn:aws:s3:::mybucket/*"
```

- オブジェクトキーの内部でポリシー変数を使用することもできます。例：

```
"Resource": "arn:aws:s3:::mybucket/home/${aws:username}/*"
```

- グループポリシーの作成時は、まだ存在しないバケットもリソースの値で指定することができます。

関連情報

"ポリシーでの変数の指定"

ポリシーでのプリンシパルの指定

ポリシーステートメントでリソースへのアクセスを許可または拒否するユーザ、グループ、またはテナントアカウントを指定するには、Principal 要素を使用します。

- バケットポリシーの各ポリシーステートメントには、Principal 要素を含める必要があります。グループはプリンシパルとみなされるため、グループポリシーのポリシーステートメントには Principal 要素は不要です。
- ポリシーでは '主体は' 主 (Principal)' または除外のためにもう 1 つの "NotPrincipal" という要素によって示されます
- ID または ARN を使用してアカウントベースのアイデンティティを指定する必要があります。

```
"Principal": { "AWS": "account_id"}  
"Principal": { "AWS": "identity_arn" }
```

- 次の例では、テナントアカウント ID 27233906934684427525 を使用しています。この場合、root アカウントとそのすべてのユーザが含まれます。

```
"Principal": { "AWS": "27233906934684427525" }
```

- root アカウントのみを指定する場合は次のようになります。

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:root" }
```

- 特定のフェデレーテッドユーザ（「Alex」）を指定する場合は次のようになります。

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-  
user/Alex" }
```

- 特定のフェデレーテッドグループ（「Managers」）のみを指定する場合は次のようになります。

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-  
group/Managers" }
```

- 匿名プリンシパルを指定する場合は次のようになります。

```
"Principal": "*"
```

- あいまいさを排除するために、ユーザ名の代わりに UUID を使用できます。

```
arn:aws:iam::27233906934684427525:user-uuid/de305d54-75b4-431b-adb2-eb6b9e546013
```

たとえば、Alexが組織とユーザ名を退職するとします Alex が削除されました。新しいAlexが組織に参加し、同じが割り当てられている場合 Alex ユーザ名。元のユーザに付与された権限が、新しいユーザに意図せず継承されることがあります。

- バケットポリシーの作成時は、まだ存在しないグループ / ユーザの名前もプリンシパルの値で指定することができます。

ポリシーで権限を指定する

ポリシーでは、Action 要素を使用してリソースに対する権限を許可または拒否します。ポリシーには、「Action」要素で示される一連の権限、または除外する「NotAction」要素で指定できる一連の権限があります。それぞれが特定の S3 REST API 処理に対応しています。

次の表に、バケットに適用される権限とオブジェクトに適用される権限を示します。



Amazon S3 では、PUT と DELETE Bucket の両方のレプリケーション処理に s3 : PutReplicationConfiguration 権限が使用されるようになりました。StorageGRID では、元の Amazon S3 仕様に一致する個別の権限が各アクションに使用されます。



DELETE は、PUT を使用して既存の値を上書きするときに実行されます。

バケットに適用される権限

権限	S3 REST API の処理	StorageGRID のカスタム
S3 : CreateBucket を指定します	PUT Bucket の場合	
S3 : DeleteBucket	バケットを削除します	
S3 : DeleteBucketMetadataNotification	バケットのメタデータ通知設定を削除します	はい。
S3 : DeleteBucketPolicy	バケットポリシーを削除	
S3 : DeleteReplicationConfiguration	バケットレプリケーションを削除します	はい。PUT および DELETE の権限は分離されています

権限	S3 REST API の処理	StorageGRID のカスタム
S3 : GetBucketAcl	GET Bucket ACL の場合	
S3 : GetBucketCompliance	GET Bucket compliance (廃止)	はい。
S3 : GetBucketConsistency	GET Bucket consistency	はい。
S3 : GetBucketCORS	GET Bucket CORS	
S3 : GetEncryptionConfiguration	GET Bucket encryption	
S3 : GetBucketLastAccessTime	GET Bucket last access time の場合	はい。
S3 : GetBucketLocation	GET Bucket location の各ノードで使用でき	
S3 : GetBucketMetadataNotification	GET Bucket metadata notification configuration	はい。
S3 : GetBucketNotification	GET Bucket notification	
S3 : GetBucketObjectLockConfiguration	オブジェクトロック設定の取得	
S3 : GetBucketPolicy	GET Bucket policy の場合	
S3 : GetBucketTagging	GET Bucket tagging	
S3 : GetBucketVersioning	GET Bucket versioning	
S3 : GetLifecycleConfiguration	GET Bucket lifecycle	
S3 : GetReplicationConfiguration	GET Bucket replication	
S3 : ListAllMyBuckets	<ul style="list-style-type: none"> • GET Service の略 • GET Storage Usage の略 	GET Storage Usage の場合は、はい
S3 : ListBucket	<ul style="list-style-type: none"> • GET Bucket (List Objects) • HEAD Bucket (ヘッドバケット) • POST Object restore の実行 	

権限	S3 REST API の処理	StorageGRID のカスタム
S3 : ListBucketMultipartUploads	<ul style="list-style-type: none"> マルチパートアップロードをリストします POST Object restore の実行 	
S3 : ListBucketVersions	GET Bucket versions (バケットバージョンの取得)	
S3 : PutBucketCompliance	PUT Bucket compliance (廃止)	はい。
S3 : PutBucketConsistency	PUT Bucket consistency	はい。
S3 : PutBucketCORS	<ul style="list-style-type: none"> バケットの CORS を削除† PUT Bucket CORS 	
S3 : PutEncryptionConfiguration	<ul style="list-style-type: none"> バケットの暗号化を削除 PUT Bucket encryption 	
S3 : PutBucketLastAccessTime	PUT Bucket last access time のように指定します	はい。
S3 : PutBucketMetadataNotification	PUT Bucket metadata notification configuration のコマンドです	はい。
S3 : PutBucketNotification	PUT Bucket notification	
S3 : PutBucketObjectLockConfiguration	PUT Bucket にで接続します x-amz-bucket-object-lock-enabled: true 要求ヘッダー (s3 : CreateBucket 権限も必要)	
S3 : PutBucketPolicy	PUT Bucket policy の場合	
S3 : PutBucketTagging	<ul style="list-style-type: none"> バケットタグを削除† PUT Bucket tagging 	
S3 : PutBucketVersioning	PUT Bucket versioning の場合	
S3 : PutLifecycleConfiguration	<ul style="list-style-type: none"> バケットライフサイクルを削除† PUT Bucket lifecycle の場合 	

権限	S3 REST API の処理	StorageGRID のカスタム
S3 : PutReplicationConfiguration	PUT Bucket replication	はい。PUT および DELETE の権限は分離されています

オブジェクトに適用される権限

権限	S3 REST API の処理	StorageGRID のカスタム
S3 : AbortMultipartUpload	<ul style="list-style-type: none"> マルチパートアップロードを中止します POST Object restore の実行 	
S3 : DeleteObject	<ul style="list-style-type: none"> オブジェクトを削除します 複数のオブジェクトを削除します POST Object restore の実行 	
S3 : DeleteObjectTagging	オブジェクトのタグ付けを削除します	
S3 : DeleteObjectVersionTagging	DELETE Object Tagging (オブジェクトの特定のバージョン)	
S3 : DeleteObjectVersion	DELETE Object (オブジェクトの特定のバージョン)	
S3 : GetObject	<ul style="list-style-type: none"> オブジェクトの取得 HEAD Object の実行 POST Object restore の実行 	
S3 : GetObjectAcl	GET Object ACL の場合	
S3 : GetObjectLegalHold	オブジェクトのリーガルホールドを取得します	
S3 : GetObjectRetention	GET Object retention のことです	
S3 : GetObjectTagging	GET Object Tagging の場合	
S3 : GetObjectVersionTagging	GET Object Tagging (オブジェクトの特定のバージョン)	

権限	S3 REST API の処理	StorageGRID のカスタム
S3 : GetObjectVersion	GET Object (オブジェクトの特定のバージョン)	
S3 : ListMultipartUploadParts	パーツを表示し、POST Object restore を実行します	
S3 : PutObject	<ul style="list-style-type: none"> • PUT Object の場合 • PUT Object - Copy の各コマンドを実行します • POST Object restore の実行 • マルチパートアップロードを開始します • Complete Multipart Upload の実行 • パーツをアップロードします • パーツのアップロード - コピー 	
S3 : PutObjectLegalHold	オブジェクトのリーガルホールドを適用します	
S3 : PutObjectRetention	PUT Object retention のことです	
S3 : PutObjectTagging	PUT Object Tagging の場合	
S3 : PutObjectVersionTagging	PUT Object Tagging (オブジェクトの特定のバージョン)	
S3 : PutOverwriteObject	<ul style="list-style-type: none"> • PUT Object の場合 • PUT Object - Copy の各コマンドを実行します • PUT Object tagging • オブジェクトのタグ付けを削除します • Complete Multipart Upload の実行 	はい。
S3 : RestoreObject	POST Object restore の実行	

PutOverwriteObject権限の使用

s3 : PutOverwriteObject 権限は、オブジェクトの作成または更新を行う環境 処理のカスタムの

StorageGRID 権限です。この権限の設定により、オブジェクトのデータ、ユーザ定義メタデータ、または S3 オブジェクトのタグをクライアントが上書きできるかどうかが決まります。

この権限で可能な設定は次のとおりです。

- *** allow *** : クライアントはオブジェクトを上書きできます。これがデフォルト設定です。
- *** Deny *** : クライアントはオブジェクトを上書きできません。PutOverwriteObject 権限が Deny に設定されている場合の動作は次のとおりです。
 - 同じパスで既存のオブジェクトが見つかった場合は、次の手順を実行します。
 - オブジェクトのデータ、ユーザ定義メタデータ、または S3 オブジェクトのタグを上書きすることはできません。
 - 実行中の取り込み処理はすべてキャンセルされ、エラーが返されます。
 - S3 バージョン管理が有効になっている場合は、Deny に設定すると、PUT Object tagging 処理または DELETE Object tagging 処理によって、オブジェクトとその最新ではないバージョンの TagSet が変更されなくなります。
 - 既存のオブジェクトが見つからない場合は、この権限の設定は影響しません。
- この権限がない場合、Allow が設定されたものと同じ結果になります。



現在の S3 ポリシーで上書きが許可されていても、PutOverwriteObject 権限が Deny に設定されている場合は、オブジェクトのデータ、ユーザ定義メタデータ、またはオブジェクトのタグをクライアントが上書きすることはできません。また、[クライアントの変更を禁止する]チェックボックス（構成>*グリッドオプション*）がオンになっている場合は、この設定がPutOverwriteObject権限の設定よりも優先されます。

関連情報

"S3 グループポリシーの例"

ポリシーで条件を指定する

条件は、ポリシーが有効になるタイミングを定義します。条件は演算子とキーと値のペアで構成されます。

条件はキーと値のペアを使用して評価されます。Condition 要素には複数の条件を指定でき、各条件には複数のキーと値のペアを含めることができます。条件ブロックの形式は次のとおりです。

```
Condition: {  
  <em>condition_type</em>: {  
    <em>condition_key</em>: <em>condition_values</em>
```

次の例では、IpAddress 条件で SourceIp 条件キーを使用しています。

```

"Condition": {
  "IpAddress": {
    "aws:SourceIp": "54.240.143.0/24"
    ...
  },
  ...
}

```

サポートされる条件演算子は次の

条件演算子は次のように分類されます。

- 文字列
- 数値
- ブール値
- IP アドレス
- Null チェック

条件演算子	説明
StringEquals	キーを文字列値と比較し、完全一致であることを確認します（大文字と小文字の区別あり）。
StringNotEquals	キーを文字列値と比較し、不一致であることを確認します（大文字と小文字の区別あり）。
StringEqualsIgnoreCase	キーを文字列値と比較し、完全一致であることを確認します（大文字と小文字の区別なし）。
StringNotEqualsIgnoreCase	キーを文字列値と比較し、不一致であることを確認します（大文字と小文字の区別なし）。
StringLike	キーを文字列値と比較し、完全一致であることを確認します（大文字と小文字の区別あり）。含めることができる * と ? ワイルドカード文字を使用できます。
StringNotLike	キーを文字列値と比較し、不一致であることを確認します（大文字と小文字の区別あり）。含めることができる * と ? ワイルドカード文字を使用できます。
NumericEquals （数値機器）	キーを数値と比較し、完全一致であることを確認します。
NumericNotEquals	キーを数値と比較し、不一致であることを確認します。

条件演算子	説明
NumericGreaterThan	キーを数値と比較し、「大なり」の一致であることを確認します。
NumericGreaterThanEquals	キーを数値と比較し、「大なり」または「等しい」の一致であることを確認します。
NumericLessThan	キーを数値と比較し、「より小さい」の一致であることを確認します。
NumericLessThanEquals	キーを数値と比較し、「より小さい」または「等しい」の一致であることを確認します。
ブール値	キーをブール値と比較し、「true」または「false」の一致であることを確認します。
IP アドレス	キーを IP アドレスまたは IP アドレスの範囲と比較します。
NotIpAddress	キーを IP アドレスまたは IP アドレスの範囲と比較し、不一致であることを確認します。
null	現在の要求コンテキストに条件キーが存在するかどうかを確認します。

サポートされている条件キー

カテゴリ	適用される条件キー	説明
IP 演算子	AWS : sourceIP	<p>要求の送信元の IP アドレスと比較します。バケットまたはオブジェクトの処理に使用できます。</p> <ul style="list-style-type: none"> 注： S3 要求が管理ノードおよびゲートウェイノード上のロードバランササービスを介して送信された場合は、ロードバランササービスのアップストリームの IP アドレスと比較します。 注*：サードパーティ製の非透過型ロードバランサを使用する場合は、そのロードバランサの IP アドレスと比較します。任意 X-Forwarded-For 有効性を確認できないため、ヘッダーは無視されます。

カテゴリ	適用される条件キー	説明
リソース / ID	AWS : ユーザ名	要求の送信者のユーザ名と比較します。バケットまたはオブジェクトの処理に使用できます。
S3 : ListBucketと S3 : ListBucketVersions権限	S3 : デリミタ	GET Bucket 要求または GET Bucket Object versions 要求で指定された delimiter パラメータと比較します。
S3 : ListBucketと S3 : ListBucketVersions権限	S3 : max-keys	GET Bucket 要求または GET Bucket Object versions 要求で指定された max-keys パラメータと比較します。
S3 : ListBucketと S3 : ListBucketVersions権限	S3 : プレフィックス	GET Bucket 要求または GET Bucket Object versions 要求で指定された prefix パラメータと比較します。

ポリシーでの変数の指定

ポリシーで変数を使用すると、該当するポリシーの情報を設定できます。でポリシー変数を使用できます Resource の要素と文字列比較 Condition 要素 (Element) :

この例では、変数を使用しています `${aws:username}` はResource要素の一部です。

```
"Resource": "arn:aws:s3::_bucket-name/home_/${aws:username}/*"
```

この例では、変数を使用しています `${aws:username}` は、条件ブロックの条件値の一部です。

```
"Condition": {
  "StringLike": {
    "s3:prefix": "${aws:username}/*"
    ...
  },
  ...
}
```

変数 (Variable)	説明
<code>\${aws:SourceIp}</code>	SourceIp キーを指定の変数として使用します。
<code>\${aws:username}</code>	username キーを指定の変数として使用します。

変数（ Variable ）	説明
<code>\${s3:prefix}</code>	サービス固有のプレフィックスキーを指定の変数として使用します。
<code>\${s3:max-keys}</code>	サービス固有の max-keys キーを指定の変数として使用します。
<code>\${*}</code>	特殊文字です。文字をリテラル * 文字として使用します。
<code>\${?}</code>	特殊文字です。文字をリテラル文字として使用しますか？を押します。
<code>\${\$}</code>	特殊文字です。文字「\$」をリテラル文字として使用します。

特別な処理を必要とするポリシーの作成

ポリシーで付与される権限によって、アカウントの root ユーザがロックアウトされるなど、セキュリティや継続的な運用に支障が生じることがあります。StorageGRID の S3 REST API の実装では、ポリシーの検証時の制限は Amazon よりも厳しくありませんが、評価時は同等の制限が適用されます。

Policy 概要 の略	ポリシータイプ	Amazon の動作	StorageGRID の動作
自身に対し、root アカウントに対するすべての権限を拒否する	バケット	有効で適用されるが、S3 バケットのすべてのポリシー処理に対する権限は引き続き root ユーザアカウントに付与される	同じ
自身に対しユーザ / グループに対するすべての権限を拒否する	グループ	有効で適用されます	同じ
外部アカウントグループに対し任意の権限を許可します	バケット	無効なプリンシパルです	有効だが、S3 バケットのすべてのポリシー処理に対する権限をポリシーで許可すると 405 Method Not Allowed エラーが返されます
外部アカウントの root またはユーザに任意の権限を許可します	バケット	有効だが、S3 バケットのすべてのポリシー処理に対する権限をポリシーで許可すると 405 Method Not Allowed エラーが返されます	同じ

Policy 概要 の略	ポリシータイプ	Amazon の動作	StorageGRID の動作
すべてのユーザにすべての処理に対する権限を許可します	バケット	有効だが、外部アカウントの root およびユーザについては、S3 バケットのすべてのポリシー処理に対する権限で 405 Method Not Allowed エラーが返されます	同じ
すべてのユーザに対してすべての処理に対する権限を拒否する	バケット	有効で適用されるが、S3 バケットのすべてのポリシー処理に対する権限は引き続き root ユーザアカウントに付与される	同じ
プリンシパルとして新規のユーザまたはグループを指定します	バケット	無効なプリンシパルです	有効
リソースとして新規の S3 バケットを指定する必要があります	グループ	有効	同じ
プリンシパルとしてローカルグループを指定します	バケット	無効なプリンシパルです	有効
ポリシーでは、非所有者アカウント（匿名アカウントを含む）にオブジェクトを PUT する権限が付与されます	バケット	有効。オブジェクトは作成者アカウントによって所有され、バケットポリシーは適用されません。作成者アカウントは、オブジェクトの ACL を使用してオブジェクトにアクセス権限を付与する必要があります。	有効。オブジェクトはバケット所有者アカウントによって所有され、バケットポリシーが適用される。

Write-Once-Read-Many（WORM）による保護

データ、ユーザ定義オブジェクトのメタデータ、S3 オブジェクトのタグを保護するために、Write-Once-Read-Many（WORM）バケットを作成することができます。新しいオブジェクトの作成を許可し、既存のコンテンツの上書きや削除を防止するように WORM バケットを設定します。ここで説明するいずれかの方法を使用します。

上書きを常に拒否するには、次の操作を実行します。

- Grid Managerから* Configuration > Grid Options の順に選択し、Prevent Client Modification *チェックボックスを選択します。
- 次のルールと S3 ポリシーを適用します。

- S3 ポリシーに PutOverwriteObject DENY 処理を追加します。
- S3 ポリシーに DeleteObject DENY 処理を追加します。
- S3 ポリシーに PUT Object ALLOW 処理を追加します。



S3 ポリシーで DeleteObject を DENY に設定しても、「zero copies after 30 days」のようなルールに基づく ILM によるオブジェクトの削除は実行されます。



これらのルールとポリシーがすべて適用されても、同時書き込みからは保護されません（状況 A を参照）。保護の対象になるのはシーケンシャルな上書きです（状況 B を参照）。

- 状況 A * : 同時書き込み（保護対象外）

```
/mybucket/important.doc
PUT#1 ---> OK
PUT#2 -----> OK
```

- 状況 B * : シーケンシャルな上書き（保護対象）

```
/mybucket/important.doc
PUT#1 -----> PUT#2 ---X (denied)
```

関連情報

["ILM を使用してオブジェクトを管理する"](#)

["特別な処理を必要とするポリシーの作成"](#)

["StorageGRID の ILM ルールによるオブジェクトの管理"](#)

["S3 グループポリシーの例"](#)

S3 ポリシーの例

このセクションでは、バケットとグループの StorageGRID アクセスポリシーを作成する例を示します。

S3 バケットポリシーの例

バケットポリシーでは、そのポリシーが関連付けられたバケットに対するアクセス権限を指定します。バケットポリシーは、S3 PutBucketPolicy API を使用して設定します。

バケットポリシーを設定するには、AWS CLI で次のコマンドを使用します。

```
> aws s3api put-bucket-policy --bucket examplebucket --policy
<em>file://policy.json</em>
```

例：すべてのユーザにバケットへの読み取り専用アクセスを許可する

この例では、匿名ユーザを含むすべてのユーザにバケット内のオブジェクトのリストとバケット内のすべてのオブジェクトの GET Object 処理を許可しています。それ以外の処理はすべて拒否されます。バケットへの書き込みが root アカウントにしか許可されないため、このポリシーは限定的な状況でしか使用されない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：あるアカウントのすべてのユーザにフルアクセスを許可し、別のアカウントのすべてのユーザにバケットへの読み取り専用アクセスを許可する

この例では、指定したアカウントのすべてのユーザにバケットへのフルアクセスを許可しています。さらに、アカウントをもう1つ指定し、そのアカウントのすべてのユーザには、で始まるバケットのオブジェクトの List 処理と GetObject 処理のみを許可しています shared/ オブジェクトキープレフィックス。



StorageGRID では、非所有者アカウント（匿名アカウントを含む）によって作成されたオブジェクトが、バケット所有者アカウントによって所有されます。バケットポリシーで、これらのオブジェクトの環境を設定します。

```

{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "95390887230002558202"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::examplebucket/shared/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::examplebucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "shared/*"
        }
      }
    }
  ]
}

```

例：すべてのユーザにバケットへの読み取り専用アクセスを許可し、指定したグループにフルアクセスを許可する

この例では、匿名ユーザを含むすべてのユーザにバケットのList処理とバケット内のすべてのオブジェクトのGET Object処理を許可し、グループに属するユーザのみを許可しています Marketing 指定したアカウントでは、フルアクセスが許可されています。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/Marketing"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": ["s3:ListBucket", "s3:GetObject"],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}
```

例：クライアントの **IP** 範囲を限定して、すべてのユーザにバケットへの読み取り / 書き込みアクセスを許可する

この例では、指定した IP 範囲（54.240.143.0~54.240.143.255 で 54.240.143.188 を除く）からの要求についてのみ、匿名ユーザを含むすべてのユーザにバケットの List 処理とバケット内のすべてのオブジェクトの全処理を許可しています。それ以外の処理はすべて拒否され、IP 範囲外の要求はすべて拒否されます。

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadWriteAccessIfInSourceIpRange",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:*Object", "s3:ListBucket" ],
      "Resource":
[ "arn:aws:s3:::examplebucket", "arn:aws:s3:::examplebucket/*" ],
      "Condition": {
        "IpAddress": { "aws:SourceIp": "54.240.143.0/24" },
        "NotIpAddress": { "aws:SourceIp": "54.240.143.188" }
      }
    }
  ]
}
```

例：指定したフェデレーテッドユーザにのみバケットへのフルアクセスを許可します

この例では、フェデレーテッドユーザのAlexがへのフルアクセスを許可しています examplebucket バケットとそのオブジェクト。'root' を含む他のすべてのユーザは 'すべての操作を明示的に拒否されますただし、「root」による Put/Get/DeleteBucketPolicy は拒否されません。

```

{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Deny",
      "NotPrincipal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}

```

例：PutOverwriteObject 権限

この例では、を使用しています Deny PutOverwriteObjectとDeleteObjectの効果は、オブジェクトのデータ、ユーザ定義メタデータ、S3オブジェクトのタグを上書きまたは削除できないようにします。


```
{
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "s3:PutOverwriteObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion"
      ],
      "Resource": "arn:aws:s3:::wormbucket/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::wormbucket"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"
      },
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::wormbucket/*"
    }
  ]
}
```

関連情報

"バケットの処理"

S3 グループポリシーの例

グループポリシーは、そのポリシーが関連付けられたグループに対するアクセス権限を指定します。はいませ
 ン Principal ポリシーは暗黙的な要素であるため、ポリシー内の要素。グループポリシーは Tenant
 Manager または API を使用して設定します。

例：Tenant Managerを使用してグループポリシーを設定します

Tenant Manager を使用してグループを追加または編集するときは、このグループのメンバーに付与する S3 アクセス権限を定義するグループポリシーの作成方法を次の中から選択できます。

- *** No S3 Access ***：デフォルトオプション。バケットポリシーでアクセスが許可されていないかぎり、このグループのユーザは S3 リソースにアクセスできません。このオプションを選択すると、デフォルトでは root ユーザにのみ S3 リソースへのアクセスが許可されます。
- *** 読み取り専用アクセス ***：このグループのユーザには、S3 リソースへの読み取り専用アクセスが許可されます。たとえば、オブジェクトをリストして、オブジェクトデータ、メタデータ、タグを読み取ることができます。このオプションを選択すると、テキストボックスに読み取り専用グループポリシーの JSON 文字列が表示されます。この文字列は編集できません。
- *** フルアクセス ***：このグループのユーザには、バケットを含む S3 リソースへのフルアクセスが許可されます。このオプションを選択すると、テキストボックスにフルアクセスグループポリシーの JSON 文字列が表示されます。この文字列は編集できません。
- *** 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。

この例では、指定したバケット内の特定のフォルダ（キープレフィックス）のリストおよびアクセスのみがグループのメンバーに許可されます。



☐ No S3 Access

☐ Read Only Access

☐ Full Access

☒ Custom
(Must be a valid JSON formatted string.)

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

例：グループにすべてのバケットへのフルアクセスを許可する

この例では、バケットポリシーで明示的に拒否されている場合を除き、グループのすべてのメンバーにテナントアカウントが所有するすべてのバケットへのフルアクセスが許可されます。

```
{
  "Statement": [
    {
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

例：グループにすべてのバケットへの読み取り専用アクセスを許可する

この例では、バケットポリシーで明示的に拒否されている場合を除き、グループのすべてのメンバーに S3 リソースへの読み取り専用アクセスが許可されます。たとえば、オブジェクトをリストして、オブジェクトデータ、メタデータ、タグを読み取ることができます。

```
{
  "Statement": [
    {
      "Sid": "AllowGroupReadOnlyAccess",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "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各自の「フォルダ」のみへのフルアクセスを許可します

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

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

関連情報

["テナントアカウントを使用する"](#)

["PutOverwriteObject権限の使用"](#)

["Write-Once-Read-Many（WORM）による保護"](#)

REST APIのセキュリティの設定

REST API のセキュリティの実装を確認し、システムの保護方法について理解しておく必要があります。

StorageGRID が**REST API**のセキュリティを提供する仕組み

StorageGRID システムで REST API のセキュリティ、認証、および許可がどのように実装されるかを理解しておく必要があります。

StorageGRID では、次のセキュリティ対策が使用されます。

- ロードバランサエンドポイントで HTTPS が設定されている場合は、ロードバランササービスとのクライアント通信に HTTPS が使用されます。

ロードバランサエンドポイントを設定する際に、オプションで HTTP を有効にすることができます。たとえば、非本番環境でのテストなどに HTTP を使用できます。詳細については、StorageGRID の管理手順を参照してください。

- StorageGRID は、ストレージノードとのクライアント通信およびゲートウェイノード上の CLB サービスとのクライアント通信に、デフォルトで HTTPS を使用します。

これらの接続に対して HTTP を有効にすることもできます。たとえば、非本番環境でのテストなどに HTTP を使用できます。詳細については、StorageGRID の管理手順を参照してください。



CLB サービスは廃止されました。

- StorageGRID とクライアント間の通信は、TLS を使用して暗号化されます。
- ロードバランササービスとグリッド内のストレージノードの間の通信は、ロードバランサエンドポイントが HTTP と HTTPS どちらの接続を受け入れるように設定されているかに関係なく暗号化されます。
- REST API 処理を実行するには、クライアントが StorageGRID に HTTP 認証ヘッダーを提供する必要があります。

セキュリティ証明書とクライアントアプリケーション

クライアントは、ゲートウェイノードまたは管理ノード上のロードバランササービスに接続するか、ストレージノードに直接接続するか、またはゲートウェイノード上の CLB サービスに直接接続することができます。

いずれの場合も、クライアントアプリケーションは、グリッド管理者がアップロードしたカスタムサーバ証明書または StorageGRID システムが生成した証明書を使用して、TLS 接続を確立できます。

- ロードバランササービスに接続する場合、クライアントアプリケーションは、接続に使用するロードバランサエンドポイント用に設定された証明書を使用します。各エンドポイントには独自の証明書があり、グリッド管理者がアップロードしたカスタムサーバ証明書か、グリッド管理者がエンドポイントの設定時に StorageGRID で生成した証明書のいずれかです。
- クライアントアプリケーションをストレージノードまたはゲートウェイノード上の CLB サービスに直接接続する場合、StorageGRID システムのインストール時に生成されたシステム生成のサーバ証明書（システム認証局によって署名された証明書）を使用します。グリッド管理者がグリッド用に指定した単一のカスタムサーバ証明書。

TLS 接続の確立に使用する証明書に署名した認証局を信頼するよう、クライアントを設定する必要があります。

ロードバランサエンドポイントの設定に関する情報や、ストレージノードまたはゲートウェイノード上の CLB サービスへの直接 TLS 接続に使用する単一のカスタムサーバ証明書を追加する方法については、StorageGRID の管理手順を参照してください。

まとめ

次の表に、S3 および Swift の REST API におけるセキュリティの問題に対する実装を示します。

Security 問題 の略	REST API の実装
接続のセキュリティ	TLS
サーバ認証	システム CA によって署名された X.509 サーバ証明書、または管理者から提供されたカスタムサーバ証明書

Security 問題 の略	REST API の実装
クライアント認証	<ul style="list-style-type: none"> • S3 : S3 アカウント (アクセスキー ID とシークレットアクセスキー) • Swift : Swift アカウント (ユーザ名とパスワード)
クライアント許可	<ul style="list-style-type: none"> • S3 : バケットの所有権と適用可能なすべてのアクセス制御ポリシー • Swift : 管理者ロールのアクセス

関連情報

["StorageGRID の管理"](#)

TLS ライブラリのハッシュアルゴリズムと暗号化アルゴリズムがサポートされます

StorageGRID システムでは、クライアントアプリケーションが Transport Layer Security (TLS) セッションを確立する際に使用できる暗号スイートに制限があります。

サポートされる **TLS** のバージョン

StorageGRID では、 TLS 1.2 と TLS 1.3 がサポートされています。



SSLv3 と TLS 1.1 (またはそれ以前のバージョン) はサポートされなくなりました。

サポートされている暗号スイート

TLS バージョン	IANA 暗号スイートの名前
1/2	TLS_ECDHE_RSA_with_AES_256_GCM_SHA384
1/2	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
1/2	TLS_ECDHE_RSA_With_AES_128_GCM_SHA256
1.3	TLS_AES_256_GCM_SHA384
1.3	TLS_CHACHA20_POLY1305_SHA256
1.3	TLS_AES_128_GCM_SHA256

廃止された暗号スイート

次の暗号スイートは廃止されました。これらの暗号のサポートは今後のリリースで廃止される予定です。

IANA 名
TLS_RSA_With_AES_128_GCM_SHA256
TLS_RSA_With_AES_256_GCM_SHA384

関連情報

["クライアント接続の設定方法"](#)

処理の監視と監査

グリッド全体または特定のノードのトランザクションの傾向を確認することで、クライアント処理のワークロードと効率を監視できます。監査メッセージを使用して、クライアント処理とトランザクションを監視できます。

- ["オブジェクトの取り込み速度と読み出し速度を監視する"](#)
- ["監査ログへのアクセスと確認"](#)

オブジェクトの取り込み速度と読み出し速度を監視する

オブジェクトの取り込み速度と読み出し速度、およびオブジェクト数、クエリ、検証関連の指標を監視できます。StorageGRID システムのオブジェクトに対してクライアントアプリケーションが試みた読み取り、書き込み、変更の各処理について、成功した回数と失敗した回数を表示できます。

手順

1. サポートされているブラウザを使用してGrid Managerにサインインします。
2. ダッシュボードで、プロトコル操作セクションを探します。

このセクションには、StorageGRID システムによって実行されたクライアント処理の回数に関する概要が表示されます。プロトコル速度は過去 2 分間の平均値です。

3. [ノード (Nodes)] を選択し
4. ノードのホームページ (導入レベル) で、* ロードバランサ * タブをクリックします。

このグラフには、グリッド内でロードバランサエンドポイントに送信されるすべてのクライアントトラフィックの傾向が表示されます。時間、日、週、月、年単位の間隔を選択できます。または、カスタムの間隔を適用することもできます。

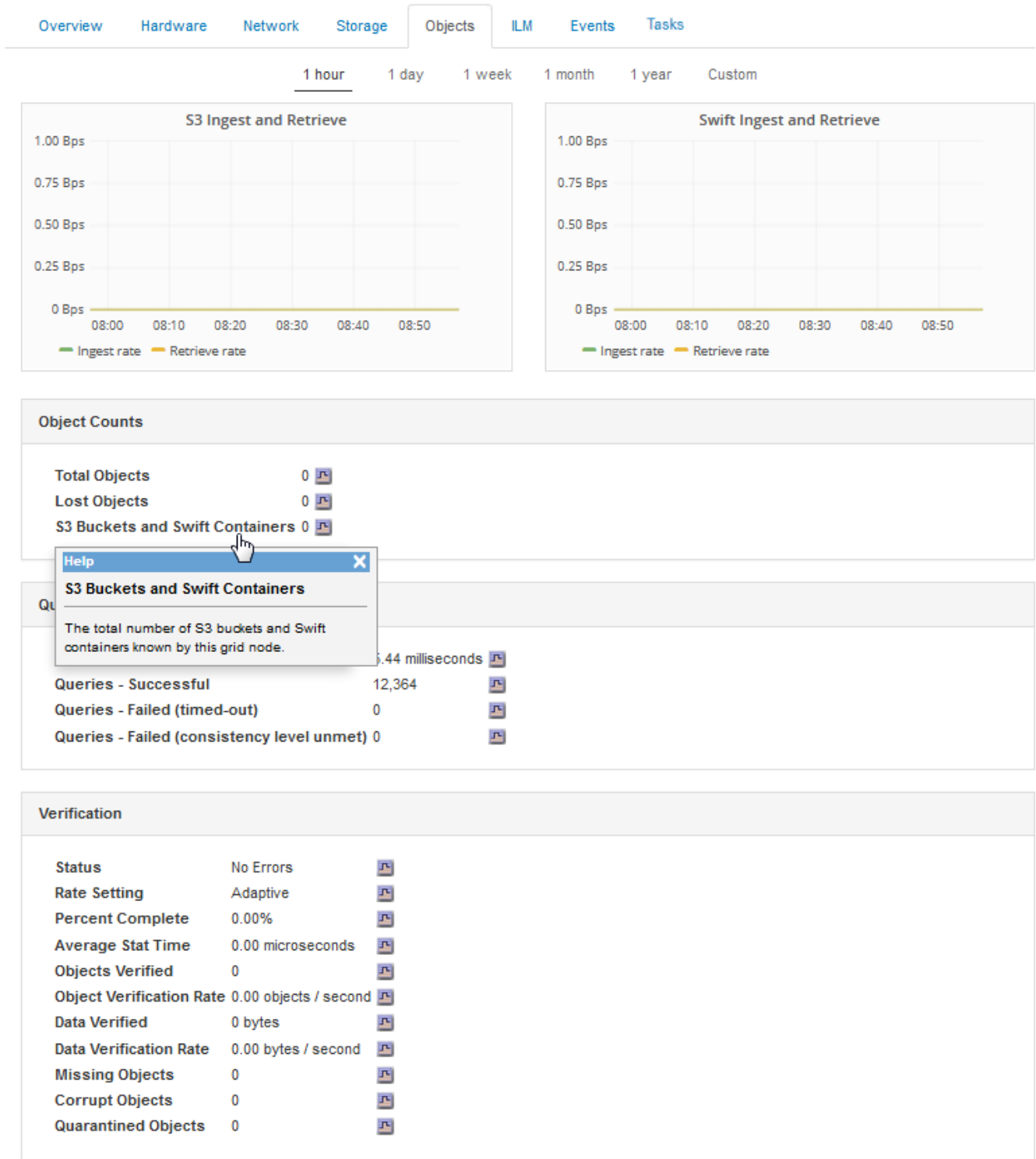
5. ノードのホームページ (導入レベル) で、* Objects * タブをクリックします。

グラフには、StorageGRID システム全体の取り込み速度と読み出し速度が、1 秒あたりのバイト数と合計バイト数で表示されます。時間、日、週、月、年単位の間隔を選択できます。または、カスタムの間隔を適用することもできます。

6. 特定のストレージノードに関する情報を表示するには、左側のリストからノードを選択し、* Objects * タブをクリックします。

グラフには、このストレージノードのオブジェクトの取り込み速度と読み出し速度が表示されます。このタブには、オブジェクト数、クエリ、検証関連の指標も表示されます。ラベルをクリックすると、これらの指標の定義を確認できます。

DC1-S2 (Storage Node)



API Operations セクションには、グリッド全体の概要情報が表示されます。

- c. 「*_ストレージノード_*>*_LDR*>*_クライアントアプリケーション_*>*_概要*>*_Main*」を選択します

Operations セクションには、選択したストレージノードに関する概要情報が表示されます。

監査ログへのアクセスと確認

監査メッセージは StorageGRID サービスによって生成され、テキスト形式のログファイルに保存されます。監査ログの API 固有の監査メッセージにより、セキュリティ、運用、およびパフォーマンスについて、システムの健全性の評価に役立つ重要な監視データが提供されます。

必要なもの

- 特定のアクセス権限が必要です。
- を用意しておく必要があります Passwords.txt ファイル。
- 管理ノードの IP アドレスを確認しておく必要があります。

このタスクについて

アクティブな監査ログファイルの名前はです `audit.log` をクリックし、を管理ノードに格納します。

1日に1回、アクティブなaudit.logファイルが保存され、新しいファイルが作成されます audit.log ファイルが開始されました。保存されたファイルの名前は、保存された日時をの形式で示しています yyyy-mm-dd.txt。

1日後、保存されたファイルは圧縮され、という形式で名前が変更されます `yyyy-mm-dd.txt.gz`元の日付を保持します。

この例は、アクティブを示しています audit.log ファイル。前日のファイルです (2018-04-15.txt) 、および前日の圧縮ファイルです (2018-04-14.txt.gz) 。

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

手順

1. 管理ノードにログインします。
 - a. 次のコマンドを入力します。+ ssh admin@primary_Admin_Node_IP
 - b. に記載されているパスワードを入力します Passwords.txt ファイル。
2. 監査ログファイルが保存されているディレクトリに移動します。

```
cd /var/local/audit/export
```

3. 必要に応じて、現在の監査ログファイルまたは保存された監査ログファイルを表示します。

バケットおよびオブジェクトのいくつかの処理は、StorageGRID の監査ログで追跡されます。

監査ログで追跡されるバケットの処理

- バケットを削除します
- バケットのタグ付けを削除します
- 複数のオブジェクトを削除します
- GET Bucket （ List Objects ）
- GET Bucket Object versions
- GET Bucket tagging
- HEAD Bucket （ヘッドバケット）
- PUT Bucket の場合
- PUT Bucket compliance で確認してください
- PUT Bucket tagging
- PUT Bucket versioning の場合

監査ログで追跡されるオブジェクトの処理

- Complete Multipart Upload の実行
- Upload Part （ ILM ルールの取り込み動作が Strict または Balanced に指定されている場合）
- Upload Part - Copy （ ILM ルールの取り込み動作が Strict または Balanced に指定されている場合）
- オブジェクトを削除します
- オブジェクトの取得
- HEAD Object の実行
- POST Object restore の実行
- PUT Object の場合
- PUT Object - Copy の各コマンドを実行します

関連情報

["バケットの処理"](#)

["オブジェクトの処理"](#)

アクティブ、アイドル、および同時 HTTP 接続のメリット

StorageGRID システムのパフォーマンスに影響するのは、HTTP 接続の設定方法です。設定は、HTTP 接続がアクティブであるかアイドルであるか、同時に複数の接続を使用するかによって異なります。

次の種類の HTTP 接続について、パフォーマンスのメリットを特定することができます。

- アイドル HTTP 接続
- アクティブ HTTP 接続
- 同時 HTTP 接続

関連情報

- ["アイドル HTTP 接続を開いておくメリット"](#)
- ["アクティブ HTTP 接続のメリット"](#)
- ["同時 HTTP 接続のメリット"](#)
- ["読み取り処理用と書き込み処理用に別々の HTTP 接続プールを使用する"](#)

アイドル HTTP 接続を開いておくメリット

クライアントアプリケーションがアイドル状態のときも HTTP 接続を開いておく、クライアントアプリケーションで以降のトランザクションが発生したときに、それらの開いている接続を使用して実行することができます。ネットアップでは、アイドル HTTP 接続を開いておく時間を 10 分までにすることを推奨します。HTTP 接続をアイドル状態のまま 10 分以上開いていると、StorageGRID によって自動的に閉じられることがあります。

アイドル HTTP 接続を開いておく、次のようなメリットがあります。

- HTTP トランザクションの実行が StorageGRID 必要と判断されてから StorageGRID システムでトランザクションが実行されるまでのレイテンシが短縮されます

レイテンシの短縮は、特に TCP / IP 接続と TLS 接続の確立に時間がかかる場合に大きなメリットとなります。

- 実行済みの転送が増えるにしたがって TCP / IP のスロースタートアルゴリズムによってデータ転送速度が向上します
- クライアントアプリケーションと StorageGRID システムの間の接続が中断された、複数の障害状況の瞬時通知

アイドル接続を開いておく適切な時間は、既存の接続のスロースタートから得られるメリットと、内部システムリソースへの理想的な接続の割り当てとのバランスによって決まります。

アクティブ HTTP 接続のメリット

ストレージノードへの直接接続、またはゲートウェイノード上の CLB サービス（廃止）への直接接続を行う場合は、HTTP 接続でトランザクションを継続的に実行する場合でも、アクティブ HTTP 接続の継続時間を 10 分までに制限することを推奨します。

接続を開いておく最大継続時間は、接続を維持することで得られるメリットと内部システムリソースへの理想的な接続の割り当てとのバランスによって決まります。

ストレージノードまたは CLB サービスへのクライアント接続でアクティブ HTTP 接続を制限する利点は次の

とおりです。

- StorageGRID システム全体で負荷を最適に分散できます。

CLB サービスを使用する場合に StorageGRID システム全体で負荷を最適に分散するには、TCP / IP 接続を長時間維持しないようにすることが重要です。それぞれの HTTP 接続の継続時間をクライアントアプリケーションで追跡し、設定した時間が経過したら HTTP 接続を閉じるように設定します。これにより、HTTP 接続を再確立して負荷を再分散できます。

CLB サービスは、クライアントアプリケーションが HTTP 接続を確立したときに、StorageGRID システム全体で負荷を分散します。時間の経過とともに負荷分散の要件が変わったため、HTTP 接続が最適な状態でなくなることがあります。クライアントアプリケーションでトランザクションごとに別の HTTP 接続を確立すれば、システムによる負荷分散は最適になりますが、この場合、接続を維持することで得られるより大きなメリットを失うことになります。



CLB サービスは廃止されました。

- クライアントアプリケーションからの HTTP トランザクションを使用可能な空きスペースがある LDR サービスに転送できる
- メンテナンス手順を開始できます。

メンテナンス手順の中には、実行中のすべての HTTP 接続が完了してからでないと開始されないものがあります。

ロードバランササービスへのクライアント接続では、接続時間を制限することで一部のメンテナンス手順をすぐに開始できます。クライアント接続の継続時間が制限されていない場合は、アクティブな接続が自動的に終了するまでに数分かかることがあります。

同時 HTTP 接続のメリット

StorageGRID システムへの TCP / IP 接続を複数開いて並列処理を可能にしておくと、パフォーマンスが向上します。最適な並列接続数は、さまざまな要因によって異なります。

同時 HTTP 接続には、次のようなメリットがあります。

- レイテンシが短縮されます

他のトランザクションが完了するのを待たずに、トランザクションをすぐに開始できます。

- スループットの向上

StorageGRID システムでは、トランザクションの並列処理が可能なため、全体的なトランザクションのスループットが向上します。

クライアントアプリケーションで複数の HTTP 接続を確立する必要があります。クライアントアプリケーションでトランザクションの実行が必要になったときは、確立された接続の中からトランザクションの処理に現在使用されていない接続を選択してすぐに使用することができます。

同時トランザクションや同時接続の最大スループットは StorageGRID システムのトポロジごとに異なり、それを超えるとパフォーマンスが低下し始めます。最大スループットは、コンピューティングリソース、ネット

ワークリソース、ストレージリソース、WAN リンクなどの要因によって決まります。また、サーバやサービスの数、StorageGRID システムでサポートするアプリケーションの数も影響します。

StorageGRID システムでは、複数のクライアントアプリケーションをサポートすることがよくあります。クライアントアプリケーションで使用する同時接続の最大数を決定する場合は、この点に注意してください。クライアントアプリケーションを構成する複数のソフトウェアエンティティのそれぞれで StorageGRID システムへの接続を確立する場合は、それらのエンティティのすべての接続を合計して考慮する必要があります。次のような場合は、同時接続の最大数の調整が必要になることがあります。

- StorageGRID システムのトポロジによって、システムでサポートできる同時トランザクションや同時接続の最大数が異なります。
- クライアントアプリケーションがネットワークの限られた帯域幅で StorageGRID システムと通信する場合は、個々のトランザクションが妥当な時間で完了するように、必要に応じて同時実行の数を少なくします。
- 多くのクライアントアプリケーションで StorageGRID システムを共有する場合は、システムの制限を超えないように、同時実行の数を少なくする必要があります。

読み取り処理用と書き込み処理用に別々の **HTTP** 接続プールを使用する

読み取り処理と書き込み処理に別々の HTTP 接続プールを使用して、それぞれに使用するプールの容量を制御できます。HTTP 接続のプールを分けることで、トランザクションや負荷分散をより細かく制御できます。

クライアントアプリケーションで生成される負荷には、読み出し中心（読み取り）の負荷と格納中心（書き込み）の負荷があります。読み取りと書き込みで HTTP 接続プールを分けることで、各プールの量を調整してそれぞれのトランザクション専用に使用することができます。

Swift を使用します

クライアントアプリケーションで OpenStack Swift API を使用して、StorageGRID システムを操作する方法について説明します。

- ["StorageGRID での OpenStack Swift API のサポート"](#)
- ["テナントアカウントと接続を設定する"](#)
- ["Swift REST API でサポートされている処理"](#)
- ["StorageGRID の Swift REST API 処理"](#)
- ["REST API のセキュリティの設定"](#)
- ["処理の監視と監査"](#)

StorageGRID での OpenStack Swift API のサポート

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

項目	バージョン
Swift の仕様	2015 年 11 月時点の OpenStack Swift Object Storage API v1
HTTP	<p>1.1 HTTP の詳細については、HTTP/1.1（RFC 7230~7235）を参照してください。</p> <ul style="list-style-type: none"> 注：StorageGRID は、HTTP/1.1 パイプラインをサポートしません。

関連情報

["OpenStack：オブジェクトストレージ API"](#)

StorageGRID での Swift API サポートの履歴

StorageGRID システムでの Swift REST API のサポートに関する変更点に注意する必要があります。

リリース。	コメント
11.5	弱い整合性制御を削除しました。代わりに、available 整合性レベルが使用されます。
11.4	TLS 1.3 のサポートの追加と、サポートされる TLS 暗号スイートのリストの更新CLB は廃止されました。ILM と整合性設定の間の相互関係の概要 が追加されました。
11.3	PUT Object 処理が更新され、取り込み時に同期配置を使用する ILM ルールの影響（取り込み動作の Balanced オプションと Strict オプション）が記述されるようになりました。ロードバランサエンドポイントまたはハイアベイラビリティグループを使用するクライアント接続の概要 が追加されました。サポートされる TLS 暗号スイートのリストが更新されました。TLS 1.1 暗号はサポートされなくなりました。
11.2	ドキュメントに対する編集上の変更がいくつかあります。
11.1	グリッドノードへの Swift クライアント接続での HTTP の使用のサポートが追加されました。整合性制御の定義が更新されました。
11.0	テナントアカウントにつき 1、000 個のコンテナのサポートが追加されました。

リリース。	コメント
10.3	ドキュメントの管理に関する記述の更新と修正カスタムサーバ証明書の設定に関するセクションが削除されました。
10.2	StorageGRID システムで Swift API が初めてサポートされました。現在サポートされているバージョンは、OpenStack Swift Object Storage API v1 です。

StorageGRID でのSwift REST APIの実装

クライアントアプリケーションは、Swift REST API 呼び出しを使用してストレージノードやゲートウェイノードに接続し、コンテナの作成やオブジェクトの格納と読み出しを行うことができます。これを利用して、OpenStack Swift 向けに開発されたサービス指向アプリケーションを、StorageGRID システムで利用できるオンプレミスのオブジェクトストレージに接続することができます。

Swift オブジェクトの管理

StorageGRID システムに取り込まれた Swift オブジェクトは、システムのアクティブな ILM ポリシー内の情報ライフサイクル管理（ILM）ルールによって管理されます。ILM ルールとポリシーは、StorageGRID がオブジェクトデータのコピーを作成および分散し、一定の期間にわたって管理する方法を決定します。たとえば、ILM ルールを特定の Swift コンテナ内のオブジェクトに適用し、複数のオブジェクトコピーを複数のデータセンターに一定期間保存するように指定できます。

グリッドの ILM ルールとポリシーが Swift テナントアカウントのオブジェクトに与える影響については、StorageGRID 管理者にお問い合わせください。

競合するクライアント要求です

同一キーに書き込む2つのクライアントなど'競合するクライアント要求は'最新のWINS形式で解決されます「latest-wins」評価のタイミングは、Swiftクライアントが処理を開始するタイミングではなく、StorageGRID システムが特定の要求を完了したタイミングに基づいています。

整合性の保証と制御

デフォルトでは、StorageGRID は、新規作成されたオブジェクトにはリードアフターライト整合性を、オブジェクトの更新と HEAD 処理には結果整合性を提供します。正常に完了した PUT に続く GET では、新しく書き込まれたデータを読み取ることができます。既存のオブジェクトの上書き、メタデータの更新、および削除の整合性レベルは、結果整合性です。上書きは通常、数秒から数分で反映されますが、最大で 15 日かかることがあります。

StorageGRID では、コンテナごとに整合性を制御することもできます。アプリケーションでの必要に応じて、ストレージノード間およびサイト間でオブジェクトの可用性と整合性のトレードオフを行うために、整合性制御を変更できます。

関連情報

["ILM を使用してオブジェクトを管理する"](#)

"GET コンテナセイコウセイヨウキユウ"

"PUT コンテナセイコウセイヨウキユウ"

Swift REST APIを実装する際の推奨事項

StorageGRID で使用するために Swift REST API を実装する場合は、次の推奨事項を考慮してください。

存在しないオブジェクトに対する HEAD の推奨事項

オブジェクトが実際に存在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アプリケーションが定期的にチェックする場合は '使用可能な整合性制御を使用する必要があります' たとえば 'アプリケーションがそのロケーションに対して PUT 操作を実行する前に ' そのロケーションに対して HEAD 操作を実行する場合は 'Available 整合性制御を使用する必要があります'

そうしないと、使用できないストレージノードがある場合に HEAD 処理でオブジェクトが見つからないと、「500 Internal Server Error」が大量に返される可能性があります。

PUT コンテナ整合性要求を使用して、各コンテナに「available」整合性制御を設定できます。

オブジェクト名の推奨事項

オブジェクト名の最初の 4 文字に、ランダムな値を使用しないでください。代わりに、イメージなど、ランダムで一意的でないプレフィックスを使用してください。

オブジェクト名のプレフィックスにランダムな一意の文字を使用する必要がある場合は、オブジェクト名の前にディレクトリ名を指定してください。つまり、次の形式を使用します。

```
mycontainer/mydir/f8e3-image3132.jpg
```

次の形式は使用しないでください。

```
mycontainer/f8e3-image3132.jpg
```

「範囲の読み取り」に関する推奨事項

「格納オブジェクトの圧縮」オプション（* Configuration > System Settings > Grid Options *）を選択した場合、Swiftクライアントアプリケーションでは、バイト範囲を指定したGET object処理を実行しないでください。StorageGRID は要求されたバイトにアクセスするためにオブジェクトを圧縮解除する必要があるため、これらの“range read”操作は非効率的です非常に大きなオブジェクトから小さい範囲のバイト数を要求するGET Object 処理は特に効率が悪く、たとえば、50GB の圧縮オブジェクトから 10MB の範囲を読み取る処理は非常に非効率的です。

圧縮オブジェクトから範囲を読み取ると、クライアント要求がタイムアウトする可能性があります。



オブジェクトを圧縮する必要がある、クライアントアプリケーションが範囲読み取りを使用する必要がある場合は、アプリケーションの読み取りタイムアウトを増やしてください。

テナントアカウントと接続を設定する

クライアントアプリケーションからの接続を受け入れるように StorageGRID を設定するには、テナントアカウントを 1 つ以上作成し、接続を設定する必要があります。

Swift テナントアカウントを作成および設定します

Swift API クライアントで StorageGRID に対してオブジェクトの格納や読み出しを行うには、Swift テナントアカウントが必要です。各テナントアカウントには、専用のアカウント ID、専用のグループとユーザ、および専用のコンテナとオブジェクトがあります。

Swift テナントアカウントは、StorageGRID のグリッド管理者がグリッドマネージャまたはグリッド管理 API を使用して作成します。

グリッド管理者は、Swift テナントアカウントを作成する際に次の情報を指定します。

- テナントの表示名（テナントのアカウント ID は自動的に割り当てられ、変更できません）
- 必要に応じて、テナントアカウントのストレージクォータ—テナントのオブジェクトで使用可能な最大ギガバイト数、テラバイト数、ペタバイト数。テナントのストレージクォータは、物理容量（ディスクのサイズ）ではなく、論理容量（オブジェクトのサイズ）を表します。
- StorageGRID システムでシングルサインオン（SSO）が使用されていない場合は、テナントアカウントが独自のアイデンティティソースを使用するか、グリッドのアイデンティティソースを共有するか、およびテナントのローカル root ユーザの初期パスワード。
- SSO が有効になっている場合は、テナントアカウントを設定するための Root Access 権限が割り当てられているフェデレーテッドグループ。

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

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



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

"サポートされている Swift API エンドポイント"

クライアント接続の設定方法

グリッド管理者は、Swift クライアントがデータの格納と読み出しを行うために StorageGRID に接続する方法に関連する設定を行います。接続するために必要な具体的な情報は、選択した設定によって異なります。

クライアントアプリケーションは、次のいずれかに接続することで、オブジェクトを格納または読み出すことができます。

- 管理ノードまたはゲートウェイノード上のロードバランササービス、または必要に応じて、管理ノードまたはゲートウェイノードのハイアベイラビリティ（HA）グループの仮想 IP アドレス
- ゲートウェイノード上の CLB サービス、または必要に応じて、ゲートウェイノードのハイアベイラビリティグループの仮想 IP アドレス



CLB サービスは廃止されました。StorageGRID 11.3 より前に設定されたクライアントは、ゲートウェイノード上の CLB サービスを引き続き使用できます。ロードバランシングに StorageGRID を使用する他のすべてのクライアントアプリケーションは、ロードバランササービスを使用して接続する必要があります。

- 外部ロードバランサを使用するかどうかに関係なく、ストレージノードに追加されます

StorageGRID を設定する場合、グリッド管理者はグリッドマネージャまたはグリッド管理 API を使用して次の手順を実行できます。これらはすべてオプションです。

1. ロードバランササービスのエンドポイントを設定する。

ロードバランササービスを使用するようにエンドポイントを設定する必要があります。管理ノードまたはゲートウェイノード上のロードバランササービスは、クライアントアプリケーションからの受信ネットワーク接続を複数のストレージノードに分散します。ロードバランサエンドポイントを作成する際、StorageGRID 管理者は、ポート番号、エンドポイントで HTTP / HTTPS 接続を許可するかどうか、エンドポイントを使用するクライアントのタイプ（S3 または Swift）、HTTPS 接続に使用する証明書（該当する場合）を指定します。

2. 信頼されていないクライアントネットワークを設定する

StorageGRID 管理者がノードのクライアントネットワークを信頼されていないクライアントネットワークとして設定した場合、ノードはロードバランサエンドポイントとして明示的に設定されたポートでクライアントネットワークのインバウンド接続だけを受け入れます。

3. ハイアベイラビリティグループを設定する。

管理者が HA グループを作成すると、複数の管理ノードまたはゲートウェイノードのネットワークインターフェイスがアクティブ / バックアップ構成になります。クライアント接続は、HA グループの仮想 IP アドレスを使用して確立されます。

各オプションの詳細については、StorageGRID の管理手順を参照してください。

Summary：クライアント接続の IP アドレスとポート

クライアントアプリケーションは、グリッドノードの IP アドレスおよびそのノード上のサービスのポート番号を使用して StorageGRID に接続します。ハイアベイラビリティ（HA）グループが設定されている場合

は、HA グループの仮想 IP アドレスを使用してクライアントアプリケーションを接続できます。

クライアント接続に必要な情報

次の表に、クライアントが StorageGRID に接続できるさまざまな方法、および各接続タイプで使用される IP アドレスとポートを示します。詳細については、StorageGRID 管理者にお問い合わせください。または、StorageGRID for a 概要 の管理手順を参照して、グリッドマネージャでこの情報を確認してください。

接続が確立される場所	クライアントが接続するサービス	IP アドレス	ポート
HA グループ	ロードバランサ	HA グループの仮想 IP アドレス	• ロードバランサエンドポイントのポート
HA グループ	CLB の機能です • 注：* CLB サービスは廃止されました。	HA グループの仮想 IP アドレス	デフォルトの Swift ポート： • HTTPS : 8083 • HTTP : 8085
管理ノード	ロードバランサ	管理ノードの IP アドレス	• ロードバランサエンドポイントのポート
ゲートウェイノード	ロードバランサ	ゲートウェイノードの IP アドレス	• ロードバランサエンドポイントのポート
ゲートウェイノード	CLB の機能です • 注：* CLB サービスは廃止されました。	ゲートウェイノードの IP アドレス • 注：デフォルトでは、CLB および LDR の HTTP ポートは有効になっていません。	デフォルトの Swift ポート： • HTTPS : 8083 • HTTP : 8085
ストレージノード	LDR	ストレージノードの IP アドレス	デフォルトの Swift ポート： • HTTPS : 18083 • HTTP : 18085

例

Swift クライアントをゲートウェイノードの HA グループのロードバランサエンドポイントに接続するには、次のように構造化された URL を使用します。

- `https://VIP-of-HA-group:LB-endpoint-port`

たとえば、HA グループの仮想 IP アドレスが 192.0.2.6 で、Swift ロードバランサエンドポイントのポート番

号が 10444 の場合、Swift クライアントは次の URL を使用して StorageGRID に接続できます。

- `https://192.0.2.6:10444`

クライアントが StorageGRID への接続に使用する IP アドレスに DNS 名を設定できます。ローカルネットワーク管理者にお問い合わせください。

HTTPS接続とHTTP接続のどちらを使用するか判断

ロードバランサエンドポイントを使用してクライアント接続を行う場合は、そのエンドポイントに指定されているプロトコル（HTTP または HTTPS）を使用して接続を確立する必要があります。ストレージノードへのクライアント接続またはゲートウェイノード上の CLB サービスへのクライアント接続に HTTP を使用する場合は、HTTP の使用を有効にする必要があります。

デフォルトでは、クライアントアプリケーションがストレージノードまたはゲートウェイノード上の CLB サービスに接続する場合、クライアントアプリケーションはすべての接続に暗号化された HTTPS を使用する必要があります。必要に応じて、Grid Manager で * Enable HTTP Connection * grid オプションを選択して、セキュアでない HTTP 接続を有効にすることができます。たとえば、非本番環境でストレージノードへの接続をテストする際に、クライアントアプリケーションで HTTP を使用できます。



要求が暗号化されずに送信されるため、本番環境のグリッドで HTTP を有効にする場合は注意してください。



CLB サービスは廃止されました。

[Enable HTTP Connection*] オプションが選択されている場合、クライアントは HTTPS とは異なるポートを HTTP に使用する必要があります。StorageGRID の管理手順を参照してください。

関連情報

["StorageGRID の管理"](#)

Swift API設定で接続をテストします

Swift の CLI を使用して、StorageGRID システムへの接続をテストし、システムに対するオブジェクトの読み取りと書き込みが可能であることを確認できます。

必要なもの

- Swift のコマンドラインクライアント `python-swiftclient` をダウンロードしてインストールしておく必要があります。
- StorageGRID システムに Swift テナントアカウントが必要です。

このタスクについて

セキュリティを設定していない場合は、を追加する必要があります `--insecure` これらの各コマンドにフラグを設定します。

手順

1. StorageGRID Swift 環境の情報 URL を照会します。

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/info
capabilities
```

この手順で、Swift 環境が機能することをテストできます。オブジェクトを格納してアカウント設定をさらにテストするには、以降の手順を実行します。

2. オブジェクトをコンテナに配置します。

```
touch test_object
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
upload test_container test_object
--object-name test_object
```

3. コンテナを取得してオブジェクトを確認します。

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
list test_container
```

4. オブジェクトを削除します。

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
delete test_container test_object
```

5. コンテナを削除します。

```
swift
-U `<_Tenant_Account_ID:Account_User_Name_>`
-K `<_User_Password_>`
-A `https://<_FQDN_ | _IP_>:<_Port_>/auth/v1.0'
delete test_container
```

関連情報

["Swiftテナントアカウントを作成および設定します"](#)

["REST APIのセキュリティの設定"](#)

Swift REST API でサポートされている処理

StorageGRID システムは、OpenStack Swift API のほとんどの処理をサポートしています。Swift REST API クライアントを StorageGRID に統合する前に、アカウント、コンテナ、およびオブジェクトの処理の実装に関する詳細を確認します。

StorageGRID でサポートされている操作

次の Swift API 処理がサポートされています。

- ["アカウントの処理"](#)
- ["コンテナの処理"](#)
- ["オブジェクトの処理"](#)

すべての処理に共通の応答ヘッダー

StorageGRID システムでは、OpenStack Swift Object Storage API v1 の定義に従って、サポートされるすべての処理に共通のヘッダーが実装されます。

関連情報

["OpenStack : オブジェクトストレージ API"](#)

サポートされている Swift API エンドポイント

StorageGRID でサポートされている Swift API エンドポイントは、情報 URL、認証 URL、およびストレージ URL です。

情報 URL

StorageGRID Swift 実装の機能と制限事項については、Swift のベース URL に /info パスを付加して GET 要求を発行することで確認できます。

`https://FQDN | Node IP:Swift Port/info/`

要求の内容は次のとおりです。

- *FQDN* は完全修飾ドメイン名です。
- *Node IP* は、StorageGRID ネットワークのストレージノードまたはゲートウェイノードのIPアドレスです。
- *Swift Port* は、ストレージノードまたはゲートウェイノードのSwift API接続に使用するポート番号です。

たとえば、次の情報 URL は、IP アドレスが 10.99.106.103 でポート 18083 を使用しているストレージノードから情報を要求します。

```
https://10.99.106.103:18083/info/
```

応答には、Swift 実装の機能が JSON ディクショナリとして含まれます。クライアントツールは、JSON 応答を解析して実装の機能を特定し、後続のストレージ処理で制約として使用できます。

StorageGRID 実装の Swift では、情報 URL への認証されていないアクセスが許可されます。

認証 URL

クライアントは、Swift 認証 URL を使用してテナントアカウントユーザとして認証できます。

```
https://FQDN | Node IP:Swift Port/auth/v1.0/
```

で、テナントアカウントID、ユーザ名、およびパスワードをパラメータとして指定する必要があります X-Auth-User および X-Auth-Key 次のように要求ヘッダー

```
X-Auth-User: Tenant_Account_ID:Username
```

```
X-Auth-Key: Password
```

要求ヘッダーは次のようになります。

- *Tenant_Account_ID* は、Swiftテナントの作成時にStorageGRID によって割り当てられたアカウントID です。Tenant Manager のサインインページで使用するテナントアカウント ID と同じです。
- *Username* は、Tenant Managerで作成されたテナントユーザの名前です。このユーザは、Swift 管理者権限を持つグループに属している必要があります。テナントの root ユーザを、Swift REST API を使用する ように設定することはできません。

テナントアカウントに対してアイデンティティフェデレーションが有効になっている場合は、LDAP サーバからのフェデレーテッドユーザのユーザ名とパスワードを指定します。または、LDAP ユーザのドメイン名を指定します。例：

```
X-Auth-User: Tenant_Account_ID:Username@Domain_Name
```

- *Password* は、テナントユーザのパスワードです。ユーザパスワードは Tenant Manager で作成および管理します。

認証要求が成功すると、ストレージ URL と認証トークンが次のように返されます。

```
X-Storage-Url: https://FQDN | Node_IP:Swift_Port/v1/Tenant_Account_ID
```

```
X-Auth-Token: token
```

X-Storage-Token: *token*

デフォルトでは、トークンの有効期間は生成時刻から 24 時間です。

トークンは特定のテナントアカウントに対して生成されます。あるアカウントに対して有効なトークンで、別のアカウントにアクセスするユーザを許可することはできません。

ストレージ URL

クライアントアプリケーションは、ゲートウェイノードまたはストレージノードに対して、問題 の Swift REST API 呼び出しを使用して、アカウント、コンテナ、オブジェクトのサポートされる処理を実行できます。ストレージ要求は、認証応答で返されたストレージ URL にアドレスが指定されます。要求には、認証要求から返された X-Auth-Token ヘッダーと値も含める必要があります。

`https://FQDN | IP:Swift_Port/v1/Tenant_Account_ID`

`[/container][/object]`

X-Auth-Token: *token*

使用状況の統計が含まれるストレージ応答ヘッダーに、最近変更されたオブジェクトの正確な数が反映されない場合があります。このヘッダーに正確な数値が表示されるまでに数分かかることがあります。

使用状況の統計が含まれているアカウントおよびコンテナ処理の応答ヘッダーの例を次に示します。

- X-Account-Bytes-Used
- X-Account-Object-Count
- X-Container-Bytes-Used
- X-Container-Object-Count

関連情報

["クライアント接続の設定方法"](#)

["Swiftテナントアカウントを作成および設定します"](#)

["アカウントの処理"](#)

["コンテナの処理"](#)

["オブジェクトの処理"](#)

アカウントの処理

アカウントに対して実行する Swift API 処理を次に示します。

GET アカウント

この処理は、アカウントに関連付けられているコンテナリストおよびアカウントの使用状況を示す統計を取得します。

次の要求パラメータが必要です。

- Account

次の要求ヘッダーが必要です。

- X-Auth-Token

次のサポートされている要求クエリパラメータはオプションです。

- Delimiter
- End_marker
- Format
- Limit
- Marker
- Prefix

実行が成功すると 'アカウントが見つかってコンテナがないかコンテナリストが空である場合' またはアカウントが見つかってコンテナリストが空でない場合には 'HTTP/1.1 204 No Content' の応答とともに '次のヘッダーが返され' コンテナリストが空でない場合は 'HTTP/1.1 200 OK' の応答が返されます

- Accept-Ranges
- Content-Length
- Content-Type
- Date
- X-Account-Bytes-Used
- X-Account-Container-Count
- X-Account-Object-Count
- X-Timestamp
- X-Trans-Id

HEAD アカウント

この処理は、Swift アカウントからアカウント情報と統計情報を取得します。

次の要求パラメータが必要です。

- Account

次の要求ヘッダーが必要です。

- X-Auth-Token

実行が成功すると、「HTTP/1.1 204 No Content」の応答とともに次のヘッダーが返されます。

- Accept-Ranges
- Content-Length
- Date
- X-Account-Bytes-Used
- X-Account-Container-Count
- X-Account-Object-Count
- X-Timestamp
- X-Trans-Id

関連情報

["監査ログで追跡される Swift 処理"](#)

コンテナの処理

StorageGRID では、Swift アカウントあたり最大で 1、000 個のコンテナがサポートされます。コンテナに対して実行する Swift API 処理を次に示します。

コンテナを削除します

この処理は、StorageGRID システムの Swift アカウントから空のコンテナを削除します。

次の要求パラメータが必要です。

- Account
- Container

次の要求ヘッダーが必要です。

- X-Auth-Token

実行が成功すると、「HTTP/1.1 204 No Content」の応答とともに次のヘッダーが返されます。

- Content-Length
- Content-Type
- Date
- X-Trans-Id

GET コンテナ

この処理は、コンテナに関連付けられているオブジェクトリストを、StorageGRID システム内のコンテナの統計情報およびメタデータとともに読み出します。

次の要求パラメータが必要です。

- Account

- Container

次の要求ヘッダーが必要です。

- X-Auth-Token

次のサポートされている要求クエリパラメータはオプションです。

- Delimiter
- End_marker
- Format
- Limit
- Marker
- Path
- Prefix

実行が成功すると、「HTTP/1.1 200 Success」または「HTTP/1.1 204 No Content」の応答とともに次のヘッダーが返されます。

- Accept-Ranges
- Content-Length
- Content-Type
- Date
- X-Container-Bytes-Used
- X-Container-Object-Count
- X-Timestamp
- X-Trans-Id

HEAD コンテナ

この処理は、StorageGRID システムからコンテナの統計情報とメタデータを読み出します。

次の要求パラメータが必要です。

- Account
- Container

次の要求ヘッダーが必要です。

- X-Auth-Token

実行が成功すると、「HTTP/1.1 204 No Content」の応答とともに次のヘッダーが返されます。

- Accept-Ranges

- Content-Length
- Date
- X-Container-Bytes-Used
- X-Container-Object-Count
- X-Timestamp
- X-Trans-Id

PUT コンテナ

この処理は、StorageGRID システムのアカウントにコンテナを作成します。

次の要求パラメータが必要です。

- Account
- Container

次の要求ヘッダーが必要です。

- X-Auth-Token

実行が成功すると、「HTTP/1.1 201 Created」または「HTTP/1.1 202 Accepted」の応答（このアカウントにコンテナがすでに存在する場合）とともに次のヘッダーが返されます。

- Content-Length
- Date
- X-Timestamp
- X-Trans-Id

コンテナ名は StorageGRID ネームスペース内で一意である必要があります。このコンテナが別のアカウントの下に存在する場合は、ヘッダー「HTTP/1.1 409 Conflict」が返されます。

関連情報

["監査ログで追跡される Swift 処理"](#)

オブジェクトの処理

オブジェクトに対して実行する Swift API 処理を次に示します。

オブジェクトを削除します

この処理は、オブジェクトのコンテンツとメタデータを StorageGRID システムから削除します。

次の要求パラメータが必要です。

- Account
- Container

- Object

次の要求ヘッダーが必要です。

- X-Auth-Token

実行が成功すると、が指定された次の応答ヘッダーが返されます HTTP/1.1 204 No Content 対応：

- Content-Length
- Content-Type
- Date
- X-Trans-Id

StorageGRID は、DELETE Object 要求を処理する際に、オブジェクトのすべてのコピーをすべての格納場所からただちに削除しようとします。成功すると、StorageGRID はただちにクライアントに応答を返します。30 秒以内にすべてのコピーを削除できなかった場合（格納場所が一時的に使用不能などの理由で）、StorageGRID は削除対象のコピーをキューに登録し、クライアントに処理が成功したことを通知します。

オブジェクトの削除方法の詳細については、情報ライフサイクル管理を使用してオブジェクトを管理する手順を参照してください。

GET オブジェクト

この処理は、StorageGRID から、オブジェクトのコンテンツを読み出し、オブジェクトメタデータを取得します。

次の要求パラメータが必要です。

- Account
- Container
- Object

次の要求ヘッダーが必要です。

- X-Auth-Token

次の要求ヘッダーはオプションです。

- Accept-Encoding
- If-Match
- If-Modified-Since
- If-None-Match
- If-Unmodified-Since
- Range

実行が成功すると、が指定された次のヘッダーが返されます HTTP/1.1 200 OK 対応：

- Accept-Ranges
- Content-Disposition`の場合にのみ返されます `Content-Disposition メタデータが設定されました
- Content-Encoding`の場合にのみ返されます `Content-Encoding メタデータが設定されました
- Content-Length
- Content-Type
- Date
- ETag
- Last-Modified
- X-Timestamp
- X-Trans-Id

HEAD オブジェクト

この処理は、取り込まれたオブジェクトのメタデータとプロパティを StorageGRID システムから読み出します。

次の要求パラメータが必要です。

- Account
- Container
- Object

次の要求ヘッダーが必要です。

- X-Auth-Token

実行が成功すると、「HTTP/1.1 200 OK」の応答とともに次のヘッダーが返されます。

- Accept-Ranges
- Content-Disposition`の場合にのみ返されます `Content-Disposition メタデータが設定されました
- Content-Encoding`の場合にのみ返されます `Content-Encoding メタデータが設定されました
- Content-Length
- Content-Type
- Date
- ETag
- Last-Modified
- X-Timestamp
- X-Trans-Id

PUT オブジェクト

この処理は、StorageGRID システムで、データとメタデータを含む新しいオブジェクトを作成するか、データとメタデータを含む既存のオブジェクトを置換します。

StorageGRID は、サイズが最大5TBのオブジェクトをサポートします。



同一キーに書き込む2つのクライアントなど競合するクライアント要求は最新のWINS形式で解決されます「latest-wins」評価のタイミングは、Swiftクライアントが処理を開始するタイミングではなく、StorageGRID システムが特定の要求を完了したタイミングに基づいています。

次の要求パラメータが必要です。

- Account
- Container
- Object

次の要求ヘッダーが必要です。

- X-Auth-Token

次の要求ヘッダーはオプションです。

- Content-Disposition
- Content-Encoding

チャンクを使用しないでください Content-Encoding 環境 オブジェクトがサイズに基づいてオブジェクトをフィルタリングし、取り込み時に同期配置を使用するILMルール（取り込み動作にBalancedオプションまたはStrictオプション）の場合。

- Transfer-Encoding

圧縮またはチャンクを使用しないでください Transfer-Encoding 環境 オブジェクトがサイズに基づいてオブジェクトをフィルタリングし、取り込み時に同期配置を使用するILMルール（取り込み動作にBalancedオプションまたはStrictオプション）の場合。

- Content-Length

ILMルールで、オブジェクトがサイズでフィルタリングされ、取り込み時に同期配置が使用される場合は、を指定する必要があります Content-Length。



でこれらのガイドラインに従っていない場合は、を参照してください Content-Encoding、`Transfer-Encoding` および `Content-Length` ではStorageGRID、オブジェクトのサイズを確認してILMルールを適用する前に、オブジェクトを保存しておく必要があります。つまり、StorageGRID で取り込み時にデフォルトでオブジェクトの中間コピーを作成する必要があります。つまり、StorageGRID での取り込み動作には Dual Commit オプションを使用する必要があります。

同期配置と ILM ルールの詳細については、情報ライフサイクル管理を使用してオブジェクトを管理する手順を参照してください。

- Content-Type
- ETag
- X-Object-Meta-<name\> (オブジェクト関連のメタデータ)

ILMルール参照時間として * User Defined Creation Time * オプションを使用する場合は、という名前のユーザ定義のヘッダーに値を格納する必要があります X-Object-Meta-Creation-Time。例：

```
X-Object-Meta-Creation-Time: 1443399726
```

このフィールドの値は、1970年1月1日からの秒数となります。

- X-Storage-Class: reduced_redundancy

このヘッダーは、取り込まれたオブジェクトに一致する ILM ルールで取り込み動作に Dual Commit または Balanced が指定されている場合に StorageGRID で作成されるオブジェクトコピーの数に影響します。

- * Dual commit * : ILM ルールの取り込み動作が Dual commit オプションに指定されている場合は、オブジェクトの取り込み時に StorageGRID が中間コピーを 1 つ作成します (シングルコミット)。
- * Balanced * : ILM ルールで Balanced オプションが指定されている場合、StorageGRID は、ルールで指定されたすべてのコピーをただちに作成できない場合にのみ、中間コピーを 1 つ作成します。StorageGRID で同期配置を実行できる場合、このヘッダーは効果がありません。

◦ reduced_redundancy ヘッダーは、オブジェクトに一致する ILM ルールで単一のレプリケートコピーが作成される場合に最も適しています。この場合は、を使用します reduced_redundancy 取り込み処理のたびに追加のオブジェクトコピーを不要に作成および削除する必要がなくなります。

を使用する reduced_redundancy 取り込み中にオブジェクトデータが失われるリスクが高まるため、他の状況ではヘッダーを使用することは推奨されません。たとえば、ILM 評価の前にコピーが 1 つだけ格納されていたストレージノードに障害が発生すると、データが失われる可能性があります。



レプリケートコピーを一定期間に 1 つだけ作成すると、データが永続的に失われるリスクがあります。オブジェクトのレプリケートコピーが 1 つしかない場合、ストレージノードに障害が発生したり、重大なエラーが発生すると、そのオブジェクトは失われます。また、アップグレードなどのメンテナンス作業中は、オブジェクトへのアクセスが一時的に失われます。

を指定することに注意してください reduced_redundancy オブジェクトの初回取り込み時に作成されるコピー数のみに影響します。オブジェクトがアクティブな ILM ポリシーで評価される際に作成されるオブジェクトのコピー数には影響せず、StorageGRID システムでデータが格納されときの冗長性レベルが低下することはありません。

実行が成功すると、「HTTP/1.1 201 Created」の応答とともに次のヘッダーが返されます。

- Content-Length
- Content-Type
- Date
- ETag

- Last-Modified
- X-Trans-Id

関連情報

["ILM を使用してオブジェクトを管理する"](#)

["監査ログで追跡される Swift 処理"](#)

OPTIONS 要求

OPTIONS 要求は、個々の Swift サービスが使用可能かどうかを確認します。OPTIONS 要求は、URL で指定されたストレージノードまたはゲートウェイノードによって処理されます。

OPTIONS メソッド

たとえば、クライアントアプリケーションでは、Swift 認証クレデンシャルを入力することなく、ストレージノード上の Swift ポートに OPTIONS 要求を問題 で送信して、ストレージノードが使用可能かどうかを判別できます。この要求は、監視に使用できるほか、外部のロードバランサがストレージノードの停止を特定する目的でも使用できます。

情報（info） URL またはストレージ（storage） URL と併用する場合、OPTIONS メソッドは、HEAD、GET、OPTIONS、PUT など、指定された URL でサポートされる動詞のリストを返します。AUTH URL にはオプションを使用できません。

次の要求パラメータが必要です。

- Account

次の要求パラメータはオプションです。

- Container
- Object

実行が成功すると、「HTTP/1.1 204 No Content」の応答とともに次のヘッダーが返されます。ストレージ URL への OPTIONS 要求には、ターゲットが存在する必要はありません。

- Allow（HEAD、GET、OPTIONSなど、指定されたURLでサポートされる動詞のリスト）およびPUT）
- Content-Length
- Content-Type
- Date
- X-Trans-Id

関連情報

["サポートされている Swift API エンドポイント"](#)

Swift API 処理に対するエラー応答

エラー応答について理解しておく、処理をトラブルシューティングする際に役立ちます。

処理中にエラーが発生した場合に返される HTTP ステータスコードを次に示します。

Swift エラーの名前	HTTP ステータス
AccountNameTooLong、ContainerNameTooLong、HeaderTooBig、InvalidContainerName、InvalidRequest、InvalidURI、MetadataNameTooLong、MetadataValueTooBig、MissingSecurityHeader、ObjectNameTooLong、TooManyContainers、TooManyMetadataItems、TotalMetadataTooLarge	400 不正な要求です
アクセスが拒否されました	403 禁止
ContainerNotEmpty、ContainerAlreadyExists です	409 競合
内部エラー	500 Internal Server Error（内部サーバエラー）
InvalidRange：無効な範囲	416 リクエストされた範囲が適合しません
MethodNotAllowed のように入力します	405 メソッドは許可されていません
MissingContentLength（MissingContentLength）	411 長さが必要です
NOTFOUND	404 が見つかりません
実装なし	501 は実装されていません
PreconditionalFailed	412 事前条件が失敗しました
resourceNotFound です	404 が見つかりません
権限がありません	401 認証なし
UnprocessableEntity の場合	422 加工不能エンティティ

StorageGRID の Swift REST API 処理

StorageGRID システム固有の処理が Swift REST API に追加されています。

GET コンテナセイコウセイヨウキユウ

整合性レベルを設定する場合は、オブジェクトの可用性と、異なるストレージノードおよびサイト間におけるオブジェクトの整合性のどちらかを犠牲にしなければなりません。GET コンテナ整合性要求では、特定のコンテナに適用されている整合性レベルを確認できます。

リクエスト

要求の HTTP ヘッダー	説明
X-Auth-Token	要求に使用するアカウントの Swift 認証トークンを指定します。
x-ntap-sg-consistency	要求のタイプを指定します true = GET コンテナ consistency、および false = コンテナを取得します。
Host	要求の転送先のホスト名。

要求例

```
GET /v1/28544923908243208806/Swift container
X-Auth-Token: SGRD_3a877009a2d24cb1801587bfa9050f29
x-ntap-sg-consistency: true
Host: test.com
```

応答

応答の HTTP ヘッダー	説明
Date	応答の日時。
Connection	サーバへの接続が開いているかどうか。
X-Trans-Id	要求の一意のトランザクション ID。
Content-Length	応答の本文の長さ。

応答の HTTP ヘッダー	説明
x-ntap-sg-consistency	<p>コンテナに適用されている整合性制御レベルです。次の値がサポートされています。</p> <ul style="list-style-type: none"> • * all * : すべてのノードが即座にデータを受け取り、受け取れない場合は要求が失敗します。 • * strong-global * : すべてのサイトにおけるすべてのクライアント要求について、リードアフターライト整合性が保証されます。 • * strong-site * : 1 つのサイトにおけるすべてのクライアント要求について、リードアフターライト整合性が保証されます。 • * read-after-new-write * : 新規オブジェクトについてはリードアフターライト整合性が提供され、オブジェクトの更新については結果整合性が提供されます。高可用性が確保され、データ保護が保証されます。 • 注: 存在しないオブジェクトに対してアプリケーションが HEAD 要求を使用すると、使用できないストレージノードがあると「500 Internal Server Error」が大量に返される可能性があります。これらのエラーを防ぐには、「available」レベルを使用します。 • * available * (HEAD オペレーションについては結果整合性) : 「read-after-new-write」整合性レベルと動作は同じですが、HEAD オペレーションについては結果整合性のみを提供します。ストレージ・ノードが使用できない場合、リードアフター・新規ライトよりもヘッド操作の可用性が高くなります。

応答例

```

HTTP/1.1 204 No Content
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
X-Trans-Id: 1936575373
Content-Length: 0
x-ntap-sg-consistency: strong-site

```

関連情報

["テナントアカウントを使用する"](#)

PUT コンテナセイコウセイヨウキユウ

PUT コンテナ整合性要求では、コンテナに対して実行される処理に適用する整合性レベルを指定できます。デフォルトでは '新しいコンテナは' リードアフター・ア・ニュー・ライトの整合性レベルを使用して作成されます

リクエスト

要求の HTTP ヘッダー	説明
X-Auth-Token	要求に使用するアカウントの Swift 認証トークンです。
x-ntap-sg-consistency	<p>コンテナに対する処理に適用される整合性制御レベルです。次の値がサポートされています。</p> <ul style="list-style-type: none">• * all * : すべてのノードが即座にデータを受け取り、受け取れない場合は要求が失敗します。• * strong-global * : すべてのサイトにおけるすべてのクライアント要求について、リードアフターライト整合性が保証されます。• * strong-site * : 1 つのサイトにおけるすべてのクライアント要求について、リードアフターライト整合性が保証されます。• * read-after-new-write * : 新規オブジェクトについてはリードアフターライト整合性が提供され、オブジェクトの更新については結果整合性が提供されます。高可用性が確保され、データ保護が保証されます。• 注: 存在しないオブジェクトに対してアプリケーションが HEAD 要求を使用すると、使用できないストレージノードがあると「500 Internal Server Error」が大量に返される可能性があります。これらのエラーを防ぐには、「available」レベルを使用します。• * available * (HEAD オペレーションについては結果整合性) : 「read-after-new-write」整合性レベルと動作は同じですが、HEAD オペレーションについては結果整合性のみを提供します。ストレージ・ノードが使用できない場合 'リードアフター・新規ライトよりもヘッド操作の可用性が高くなります
Host	要求の転送先のホスト名。

整合性制御と ILM ルールの相互作用によるデータ保護への影響

整合性制御と ILM ルールのどちらを選択した場合も、オブジェクトの保護方法に影響します。これらの設定は対話的に操作できます。

たとえば、オブジェクトの格納に使用される整合性制御はオブジェクトメタデータの初期配置に影響し、ILM ルールで選択される取り込み動作はオブジェクトコピーの初期配置に影響します。StorageGRID では、クライアント要求に対応するためにオブジェクトのメタデータとそのデータの両方にアクセスする必要があるため、整合性レベルと取り込み動作に一致する保護レベルを選択することで、より適切な初期データ保護と予測可能なシステム応答を実現できます。

ILM ルールでは、次の取り込み動作を使用できます。

- *** Strict *** : ILM ルールに指定されたすべてのコピーを作成しないと、クライアントに成功が返されません。
- *** Balanced *** : StorageGRID は、取り込み時に ILM ルールで指定されたすべてのコピーを作成しようとします。作成できない場合、中間コピーが作成されてクライアントに成功が返されます。可能な場合は、ILM ルールで指定されたコピーが作成されます。
- *** デュアルコミット *** : StorageGRID はオブジェクトの中間コピーをただちに作成し、クライアントに成功を返します。可能な場合は、ILM ルールで指定されたコピーが作成されます。



ILM ルールの取り込み動作を選択する前に、情報ライフサイクル管理を使用してオブジェクトを管理する手順の設定の完全な概要を確認してください。

整合性制御と ILM ルールの連動の例

次の ILM ルールと次の整合性レベル設定の 2 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、2 つのオブジェクトコピーを作成します。Strict 取り込み動作が選択されています。
- *** 整合性レベル *** : "Strong-GLOBAL" (オブジェクトメタデータはすべてのサイトにただちに分散されます)

クライアントがオブジェクトをグリッドに格納すると、StorageGRID は両方のオブジェクトをコピーし、両方のサイトにメタデータを分散してからクライアントに成功を返します。

オブジェクトは、取り込みが成功したことを示すメッセージが表示された時点で損失から完全に保護されます。たとえば、取り込み直後にローカルサイトが失われた場合、オブジェクトデータとオブジェクトメタデータの両方のコピーがリモートサイトに残っています。オブジェクトを完全に読み出し可能にしている。

代わりに同じ ILM ルールと「strong-site」整合性レベルを使用する場合は、オブジェクトデータがリモートサイトにレプリケートされたあとで、オブジェクトメタデータがそこに分散される前に、クライアントに成功メッセージが送信され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がオブジェクトデータの保護レベルと一致しません。取り込み直後にローカルサイトが失われると、オブジェクトメタデータが失われます。オブジェクトを読み出すことができません。

整合性レベルと ILM ルールの間の関係は複雑になる可能性があります。サポートが必要な場合は、ネットアップにお問い合わせください。

要求例

```
PUT /v1/28544923908243208806/_Swift_container_  
X-Auth-Token: SGRD_3a877009a2d24cb1801587bfa9050f29  
x-ntap-sg-consistency: strong-site  
Host: test.com
```

応答

応答の HTTP ヘッダー	説明
Date	応答の日時。
Connection	サーバへの接続が開いているかどうか。
X-Trans-Id	要求の一意のトランザクション ID。
Content-Length	応答の本文の長さ。

応答例

```
HTTP/1.1 204 No Content
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
X-Trans-Id: 1936575373
Content-Length: 0
```

関連情報

["テナントアカウントを使用する"](#)

REST APIのセキュリティの設定

REST API のセキュリティの実装を確認し、システムの保護方法について理解しておく必要があります。

StorageGRID がREST APIのセキュリティを提供する仕組み

StorageGRID システムで REST API のセキュリティ、認証、および許可がどのように実装されるかを理解しておく必要があります。

StorageGRID では、次のセキュリティ対策が使用されます。

- ロードバランサエンドポイントで HTTPS が設定されている場合は、ロードバランササービスとのクライアント通信に HTTPS が使用されます。

ロードバランサエンドポイントを設定する際に、オプションで HTTP を有効にすることができます。たとえば、非本番環境でのテストなどに HTTP を使用できます。詳細については、StorageGRID の管理手順を参照してください。

- StorageGRID は、ストレージノードとのクライアント通信およびゲートウェイノード上の CLB サービスとのクライアント通信に、デフォルトで HTTPS を使用します。

これらの接続に対して HTTP を有効にすることもできます。たとえば、非本番環境でのテストなどに HTTP を使用できます。詳細については、StorageGRID の管理手順を参照してください。



CLB サービスは廃止されました。

- StorageGRID とクライアント間の通信は、TLS を使用して暗号化されます。
- ロードバランササービスとグリッド内のストレージノードの間の通信は、ロードバランサエンドポイントが HTTP と HTTPS どちらの接続を受け入れるように設定されているかに関係なく暗号化されます。
- REST API 処理を実行するには、クライアントが StorageGRID に HTTP 認証ヘッダーを提供する必要があります。

セキュリティ証明書とクライアントアプリケーション

クライアントは、ゲートウェイノードまたは管理ノード上のロードバランササービスに接続するか、ストレージノードに直接接続するか、またはゲートウェイノード上の CLB サービスに直接接続することができます。

いずれの場合も、クライアントアプリケーションは、グリッド管理者がアップロードしたカスタムサーバ証明書または StorageGRID システムが生成した証明書を使用して、TLS 接続を確立できます。

- ロードバランササービスに接続する場合、クライアントアプリケーションは、接続に使用するロードバランサエンドポイント用に設定された証明書を使用します。各エンドポイントには独自の証明書があり、グリッド管理者がアップロードしたカスタムサーバ証明書か、グリッド管理者がエンドポイントの設定時に StorageGRID で生成した証明書のいずれかです。
- クライアントアプリケーションをストレージノードまたはゲートウェイノード上の CLB サービスに直接接続する場合、StorageGRID システムのインストール時に生成されたシステム生成のサーバ証明書（システム認証局によって署名された証明書）を使用します。グリッド管理者がグリッド用に指定した単一のカスタムサーバ証明書。

TLS 接続の確立に使用する証明書に署名した認証局を信頼するよう、クライアントを設定する必要があります。

ロードバランサエンドポイントの設定に関する情報や、ストレージノードまたはゲートウェイノード上の CLB サービスへの直接 TLS 接続に使用する単一のカスタムサーバ証明書を追加する方法については、StorageGRID の管理手順を参照してください。

まとめ

次の表に、S3 および Swift の REST API におけるセキュリティの問題に対する実装を示します。

Security 問題 の略	REST API の実装
接続のセキュリティ	TLS
サーバ認証	システム CA によって署名された X.509 サーバ証明書、または管理者から提供されたカスタムサーバ証明書
クライアント認証	<ul style="list-style-type: none">• S3 : S3 アカウント（アクセスキー ID とシークレットアクセスキー）• Swift : Swift アカウント（ユーザ名とパスワード）

Security 問題 の略	REST API の実装
クライアント許可	<ul style="list-style-type: none"> • S3 : バケットの所有権と適用可能なすべてのアクセス制御ポリシー • Swift : 管理者ロールのアクセス

関連情報

["StorageGRID の管理"](#)

TLS ライブラリのハッシュアルゴリズムと暗号化アルゴリズムがサポートされます

StorageGRID システムでは、クライアントアプリケーションが Transport Layer Security (TLS) セッションを確立する際に使用できる暗号スイートに制限があります。

サポートされる **TLS** のバージョン

StorageGRID では、 TLS 1.2 と TLS 1.3 がサポートされています。



SSLv3 と TLS 1.1 (またはそれ以前のバージョン) はサポートされなくなりました。

サポートされている暗号スイート

TLS バージョン	IANA 暗号スイートの名前
1/2	TLS_ECDHE_RSA_with_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	TLS_ECDHE_RSA_With_AES_128_GCM_SHA256
1.3	TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256	TLS_AES_128_GCM_SHA256

廃止された暗号スイート

次の暗号スイートは廃止されました。これらの暗号のサポートは今後のリリースで廃止される予定です。

IANA 名
TLS_RSA_With_AES_128_GCM_SHA256
TLS_RSA_With_AES_256_GCM_SHA384

関連情報

["クライアント接続の設定方法"](#)

処理の監視と監査

グリッド全体または特定のノードのトランザクションの傾向を確認することで、クライアント処理のワークロードと効率を監視できます。監査メッセージを使用して、クライアント処理とトランザクションを監視できます。

オブジェクトの取り込み速度と読み出し速度を監視する

オブジェクトの取り込み速度と読み出し速度、およびオブジェクト数、クエリ、検証関連の指標を監視できます。StorageGRID システムのオブジェクトに対してクライアントアプリケーションが試みた読み取り、書き込み、変更の各処理について、成功した回数と失敗した回数を表示できます。

手順

1. サポートされているブラウザを使用してGrid Managerにサインインします。
2. ダッシュボードで、プロトコル操作セクションを探します。

このセクションには、StorageGRID システムによって実行されたクライアント処理の回数に関する概要が表示されます。プロトコル速度は過去 2 分間の平均値です。

3. [ノード (Nodes)] を選択し
4. ノードのホームページ (導入レベル) で、* ロードバランサ * タブをクリックします。

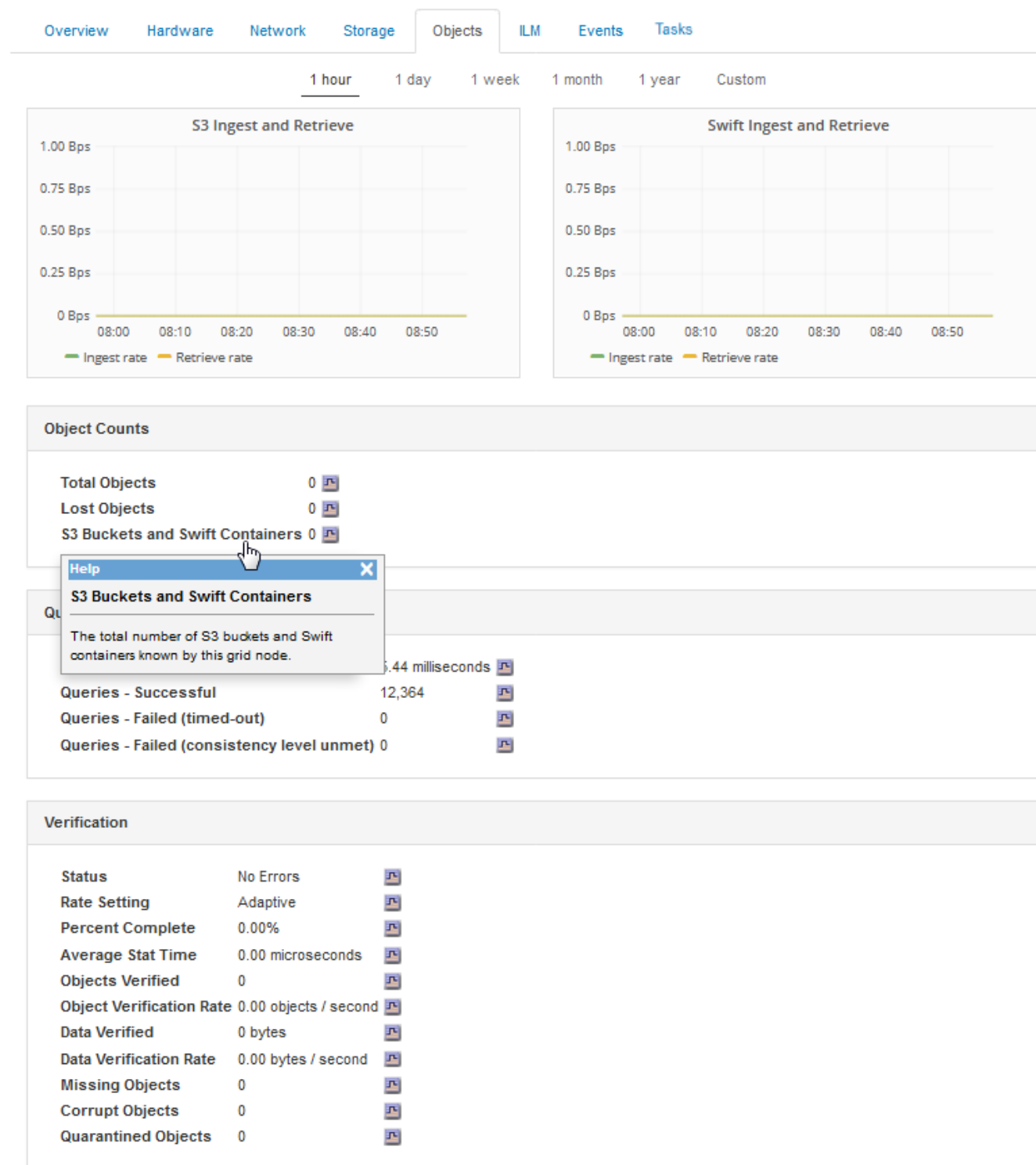
このグラフには、グリッド内でロードバランサエンドポイントに送信されるすべてのクライアントトラフィックの傾向が表示されます。時間、日、週、月、年単位の間隔を選択できます。または、カスタムの間隔を適用することもできます。

5. ノードのホームページ (導入レベル) で、* Objects * タブをクリックします。

グラフには、StorageGRID システム全体の取り込み速度と読み出し速度が、1 秒あたりのバイト数と合計バイト数で表示されます。時間、日、週、月、年単位の間隔を選択できます。または、カスタムの間隔を適用することもできます。

6. 特定のストレージノードに関する情報を表示するには、左側のリストからノードを選択し、* Objects * タブをクリックします。

グラフには、このストレージノードのオブジェクトの取り込み速度と読み出し速度が表示されます。このタブには、オブジェクト数、クエリ、検証関連の指標も表示されます。ラベルをクリックすると、これらの指標の定義を確認できます。



7. さらに詳細な情報が必要な場合は、次の手順に従います

- Support > Tools > Grid Topology *を選択します。
- [_site *>] > [Overview] > [Main*] を選択します。

API Operations セクションには、グリッド全体の概要情報が表示されます。

- c. 「*_ストレージノード_*>*_LDR*>*_クライアントアプリケーション_*>*_概要*>*_Main*」を選択します

Operations セクションには、選択したストレージノードに関する概要情報が表示されます。

監査ログへのアクセスと確認

監査メッセージは StorageGRID サービスによって生成され、テキスト形式のログファイルに保存されます。監査ログの API 固有の監査メッセージにより、セキュリティ、運用、およびパフォーマンスについて、システムの健全性の評価に役立つ重要な監視データが提供されます。

必要なもの

- 特定のアクセス権限が必要です。
- を用意しておく必要があります Passwords.txt ファイル。
- 管理ノードの IP アドレスを確認しておく必要があります。

このタスクについて

アクティブな監査ログファイルの名前はです `audit.log` をクリックし、を管理ノードに格納します。

1 日に 1 回、アクティブな audit.log ファイルが保存され、新しい audit.log ファイルが開始されます。保存されたファイルの名前は、保存された日時をの形式で示しています yyyy-mm-dd.txt。

1 日後、保存されたファイルは圧縮され、という形式で名前が変更されます `yyyy-mm-dd.txt.gz` 元の日付を保持します。

次の例は、アクティブな audit.log ファイル、前日のファイル (2018-04-15.txt)、および前日の圧縮されたファイルを示しています (2018-04-14.txt.gz)。

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

手順

1. 管理ノードにログインします。
 - a. 次のコマンドを入力します。 `ssh admin@primary_Admin_Node_IP`
 - b. に記載されているパスワードを入力します Passwords.txt ファイル。
2. 監査ログファイルが保存されているディレクトリに移動します。 `cd /var/local/audit/export`
3. 必要に応じて、現在の監査ログファイルまたは保存された監査ログファイルを表示します。

関連情報

["監査ログを確認します"](#)

監査ログで追跡される Swift 処理

ストレージに対する成功した DELETE、GET、HEAD、POST、PUT の各処理は、StorageGRID 監査ロ

グで追跡されます。エラーはログに記録されず、情報、認証、オプションの要求も記録されません。

次の Swift 処理で追跡される情報の詳細については、「[監査メッセージの概要](#)」を参照してください。

アカウントの処理

- GET アカウント
- HEAD アカウント

コンテナの処理

- コンテナを削除します
- GET コンテナ
- HEAD コンテナ
- PUT コンテナ

オブジェクトの処理

- オブジェクトを削除します
- GET オブジェクト
- HEAD オブジェクト
- PUT オブジェクト

関連情報

["監査ログを確認します"](#)

["アカウントの処理"](#)

["コンテナの処理"](#)

["オブジェクトの処理"](#)

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。