S3テナントアカウントの管理

StorageGRID 11.5

NetApp
April 11, 2024

目次

S3テナントアカウントの管理

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

- "S3 アクセスキーの管理"
- "S3バケットの管理"

S3 アクセスキーの管理

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

このタスクについて

S3 アクセスキーは次のように管理できます。

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

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

自分のS3アクセスキーを作成する

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

必要なもの

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

このタスクについて

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

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

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

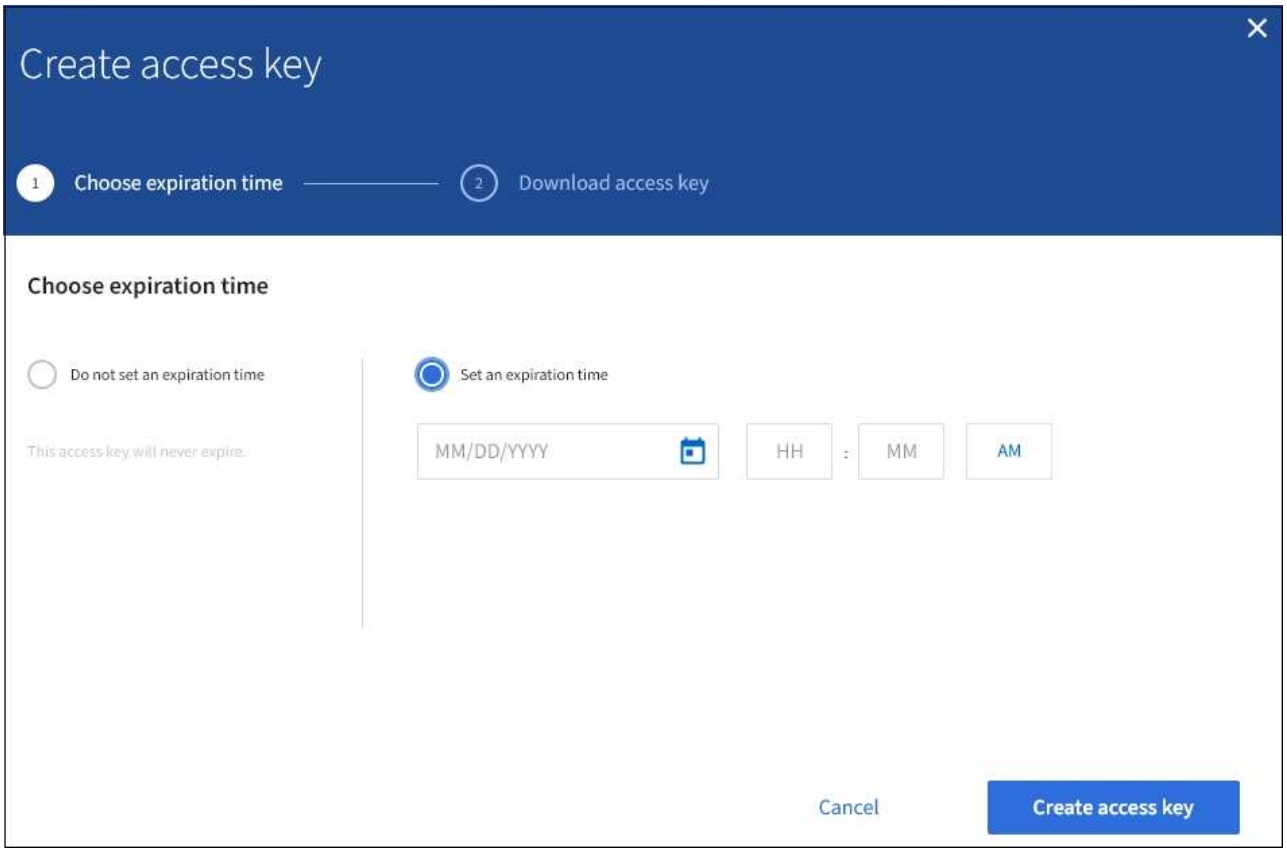
> アカウントに属する S3 バケットとオブジェクトには、 Tenant Manager でアカウントに表示されるアクセスキー ID とシークレットアクセスキーを使用してアクセスできます。このため、アクセスキーはパスワードと同じように保護する必要があります。定期的にアクセスキーをローテーションし、使用されていないキーはアカウントから削除します。また、他のユーザとはアクセスキーを共有しないでください。

手順

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

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

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

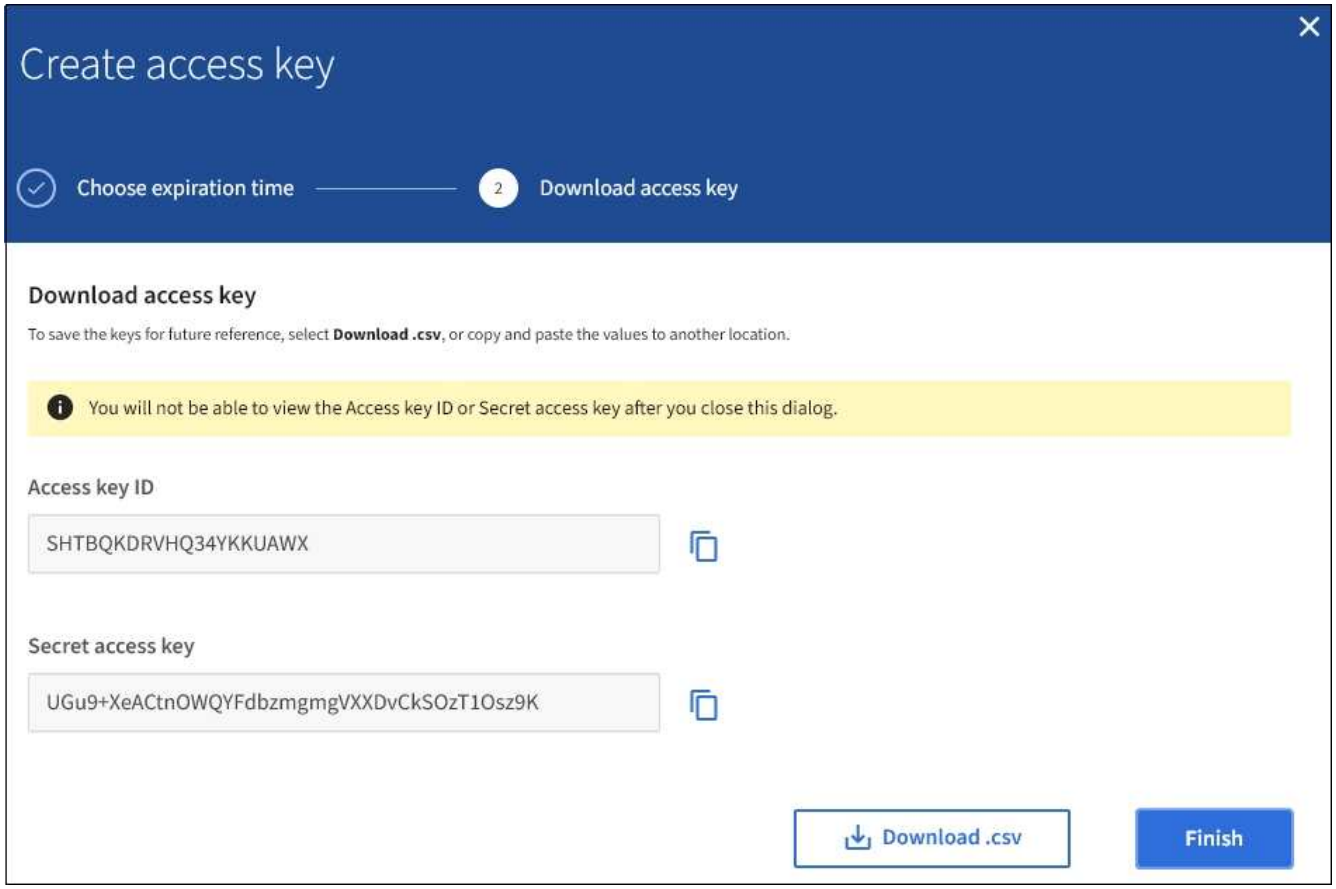


4. [アクセスキーの作成 *] を選択します。

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

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



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。

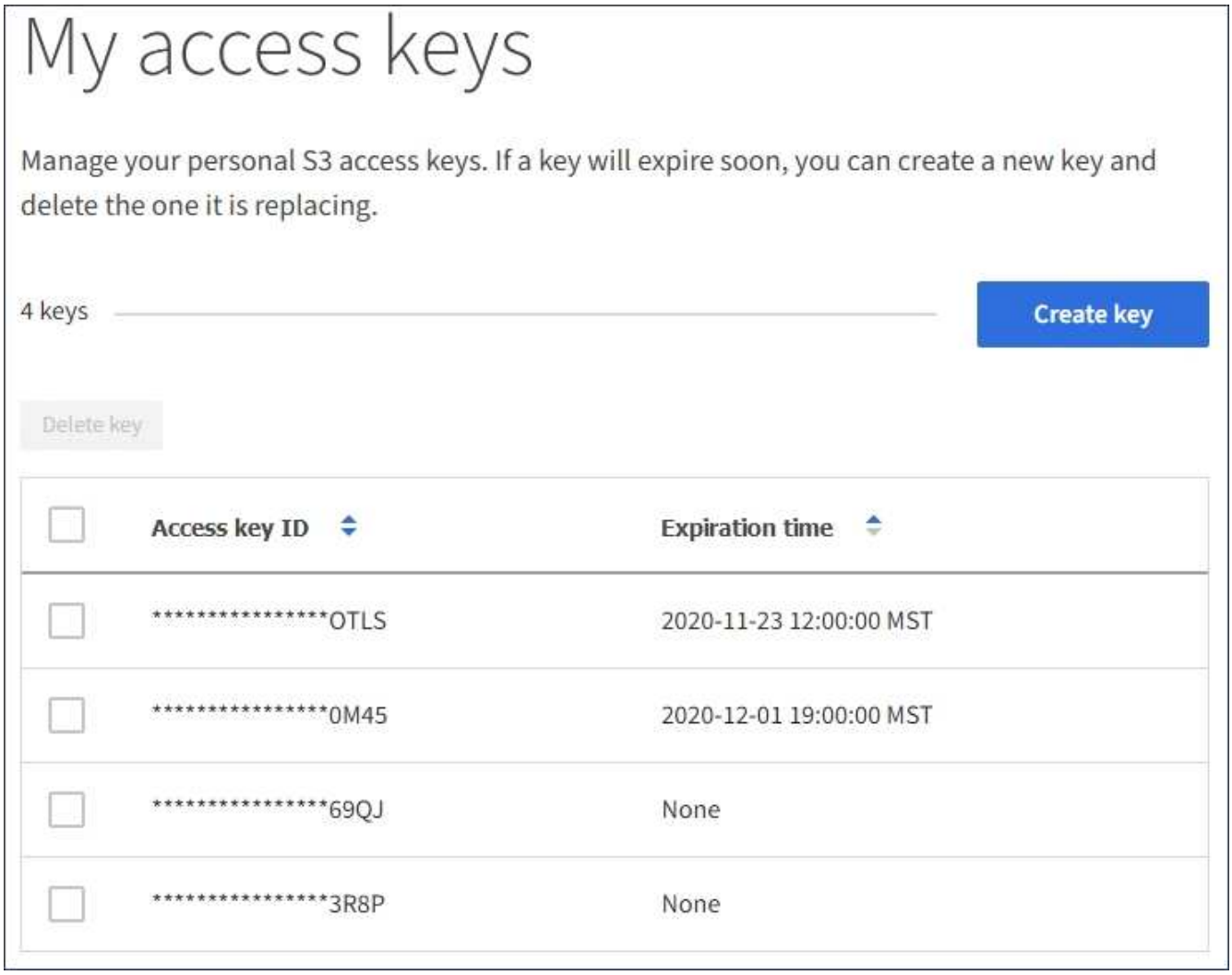
- Manage Your Own S3 Credentials 権限が必要です。

> 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。



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。

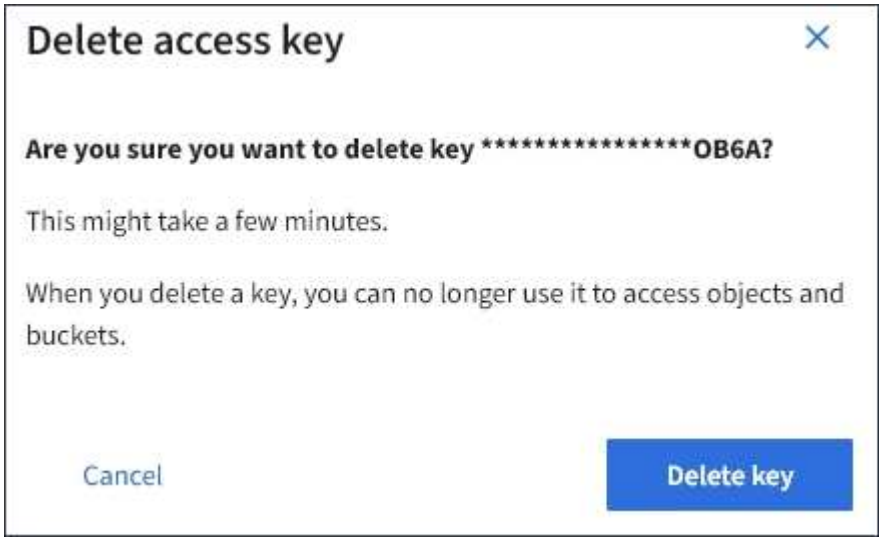
手順

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。

関連情報

"テナント管理権限"

別のユーザの**S3**アクセスキーを作成する

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

必要なもの

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

このタスクについて

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

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

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

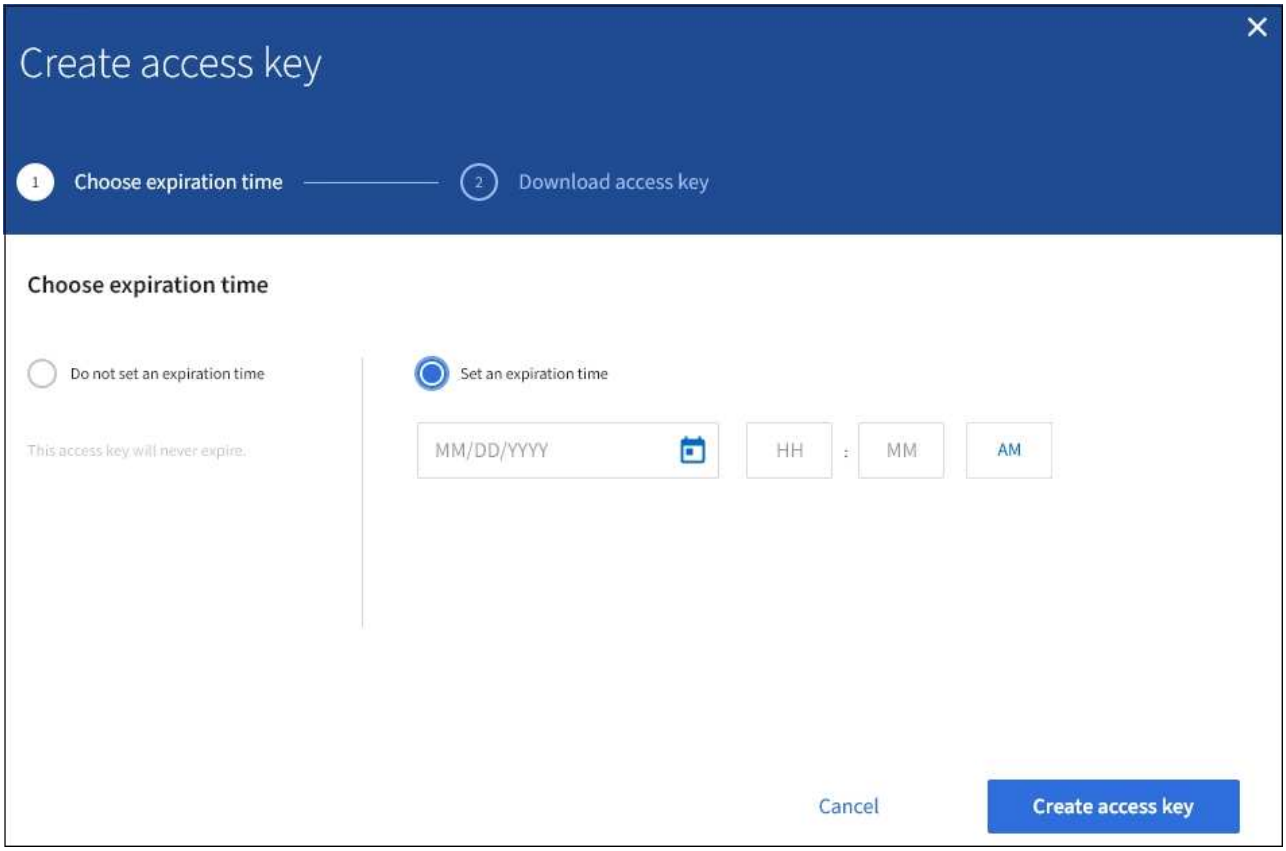
> ユーザに属する S3 バケットとオブジェクトには、 Tenant Manager でそのユーザに対して表示されるアクセスキー ID とシークレットアクセスキーを使用してアクセスできます。このため、アクセスキーはパスワードと同じように保護する必要があります。定期的にアクセスキーをローテーションし、使用されていないキーはアカウントから削除します。また、他のユーザとはアクセスキーを共有しないでください。

手順

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

   ユーザーの詳細ページが表示されます。
3. [* アクセスキー *] を選択し、 [* キーの作成 *] を選択します。
4. 次のいずれかを実行します。
   - 有効期限を設定しない * を選択して、有効期限が切れないキーを作成します。（デフォルト）

◦ [有効期限の設定 *] を選択し、有効期限の日付と時刻を設定します。

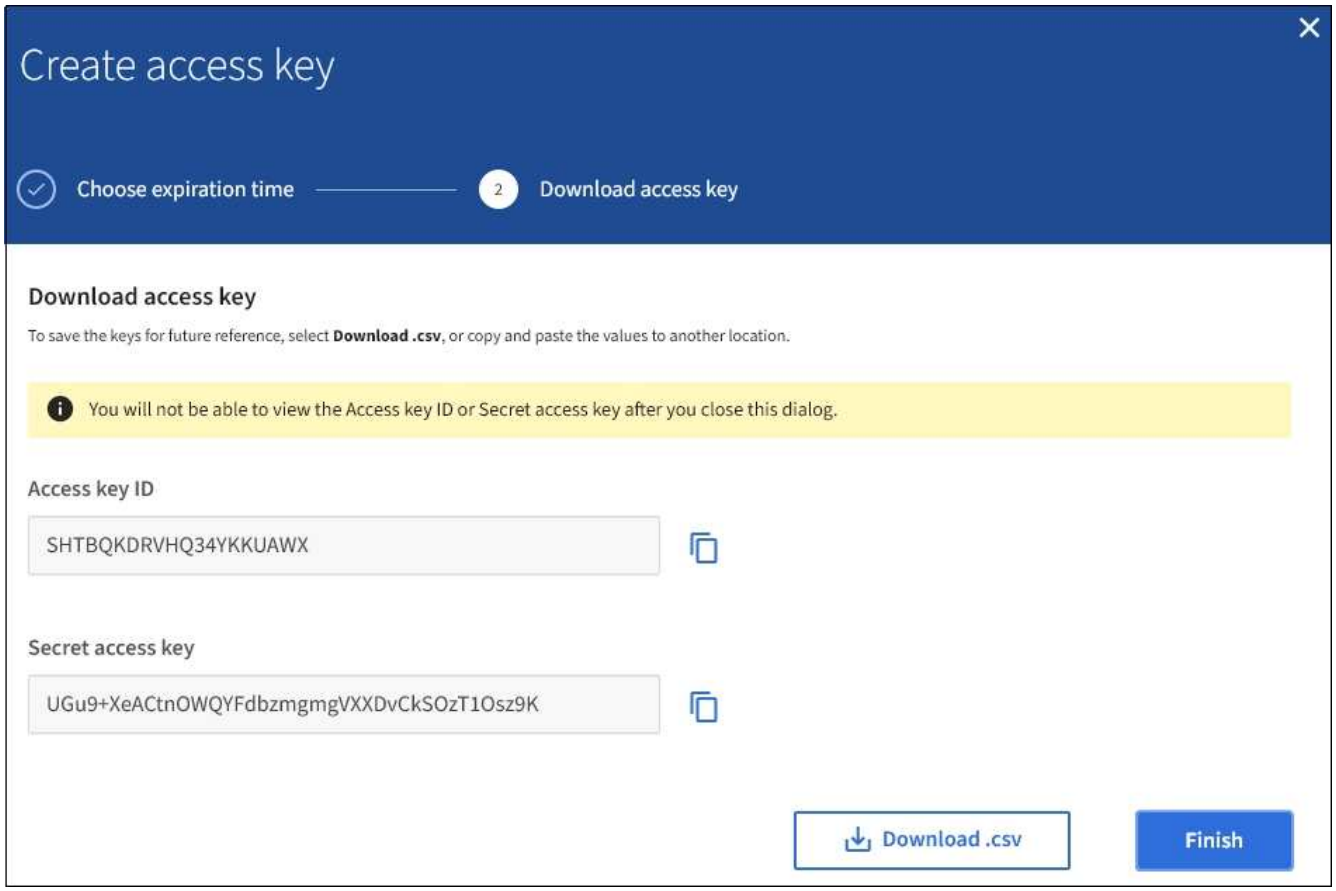


5. [アクセスキーの作成 *] を選択します。

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

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

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



7. [完了] を選択します。

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

関連情報

"テナント管理権限"

別のユーザの**S3**アクセスキーを表示しています

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

必要なもの

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

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

手順

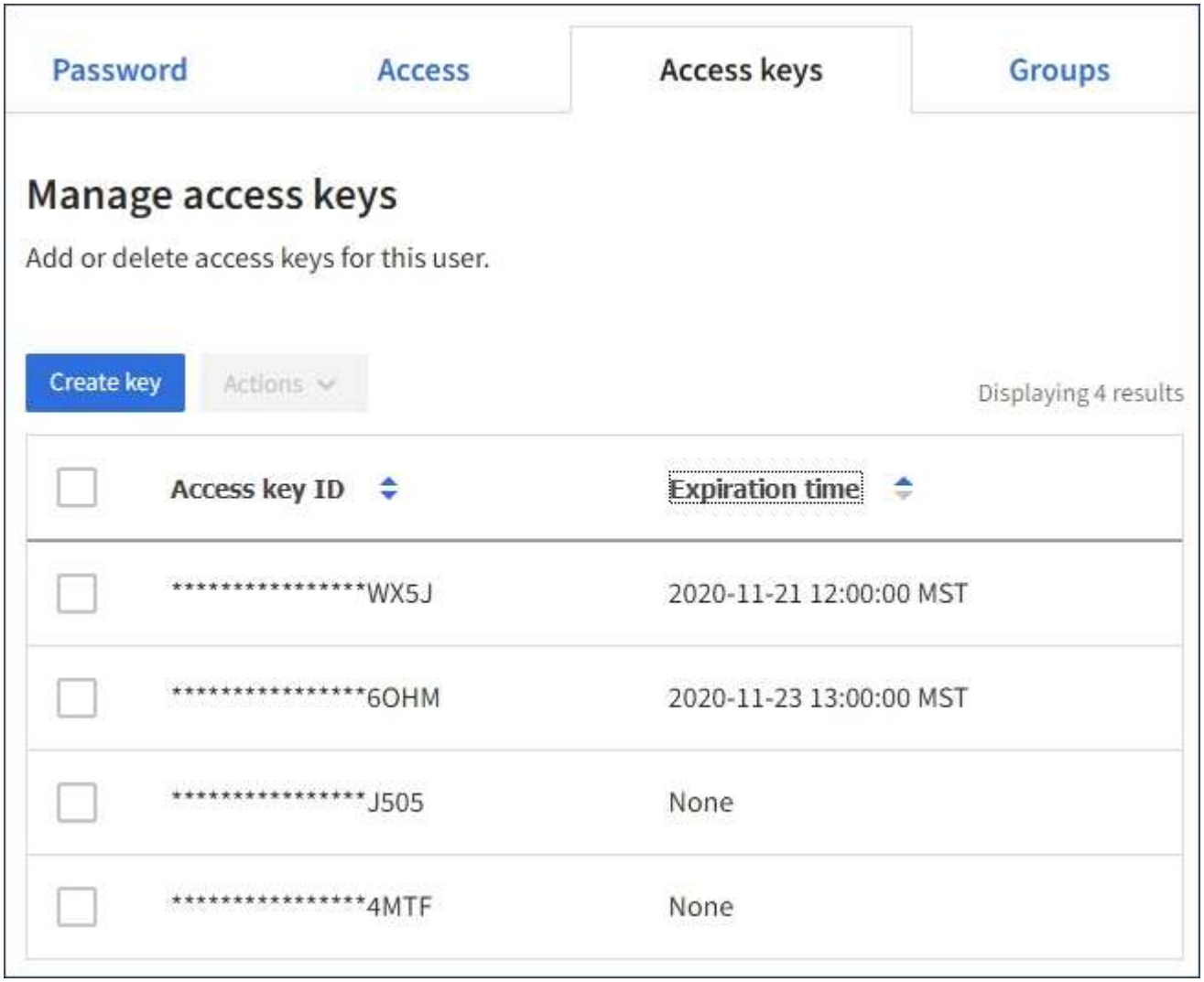
1. アクセス管理 * > * Users * を選択します。

   [ユーザー] ページが表示され、既存のユーザーが一覧表示されます。

2. S3 アクセスキーを表示するユーザを選択します。

   ユーザーの詳細ページが表示されます。

3. 「 * アクセスキー * 」を選択します。



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。

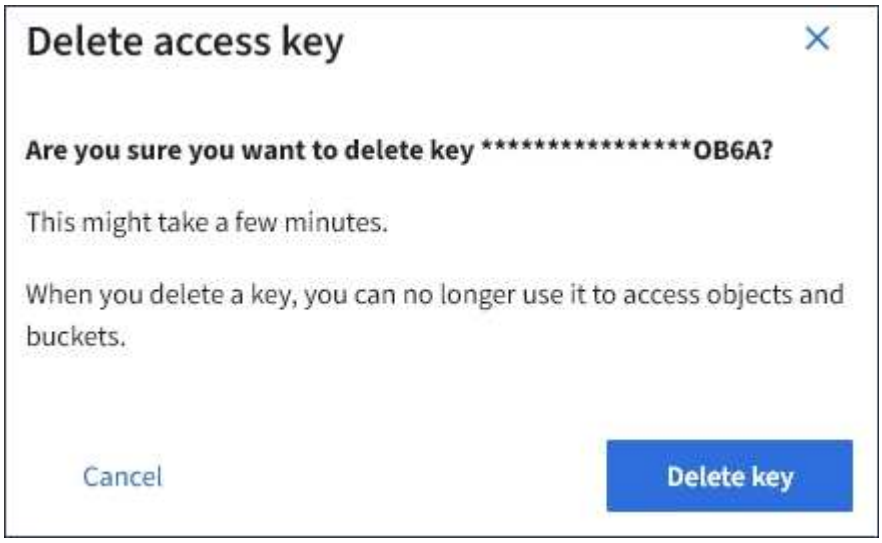
   [ユーザー] ページが表示され、既存のユーザーが一覧表示されます。

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。

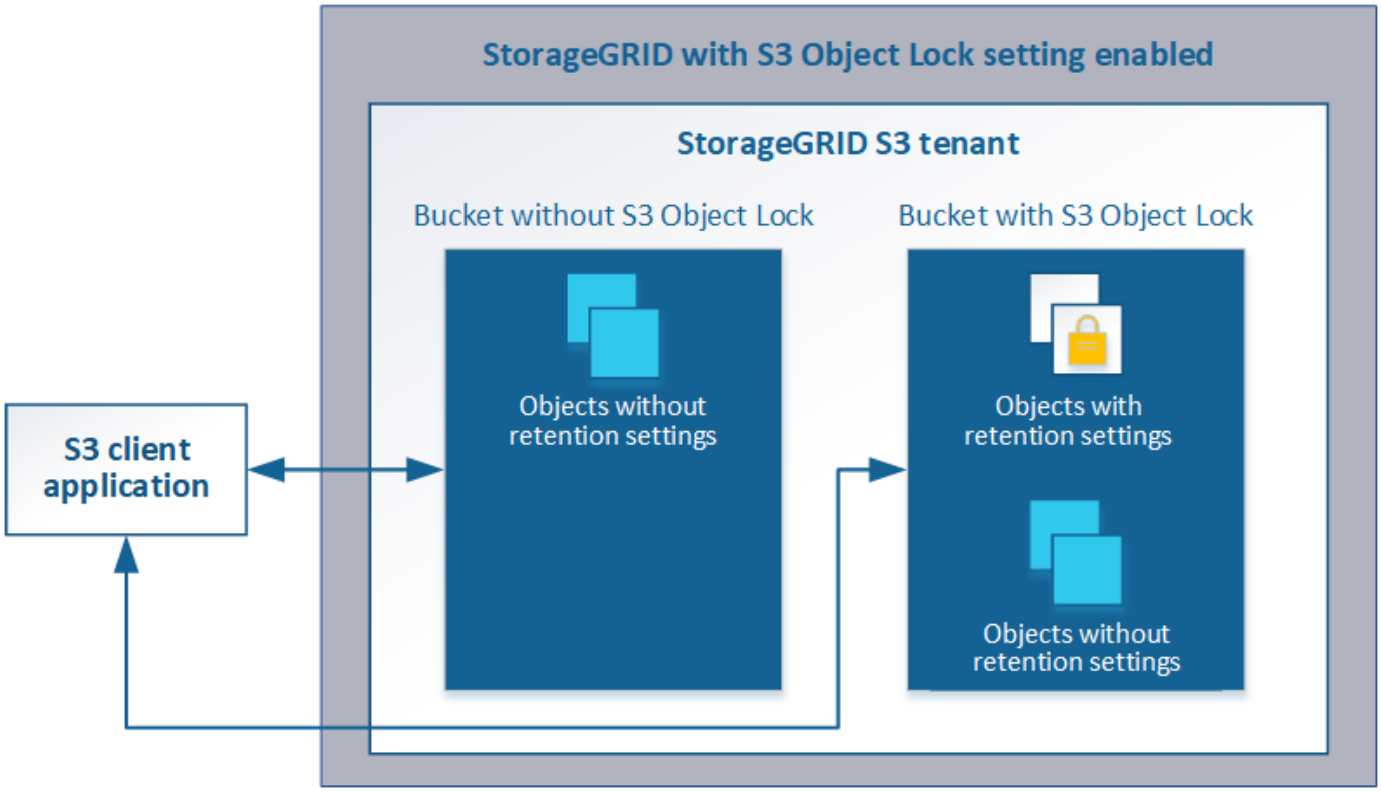
S3 オブジェクトロックを使用する

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。

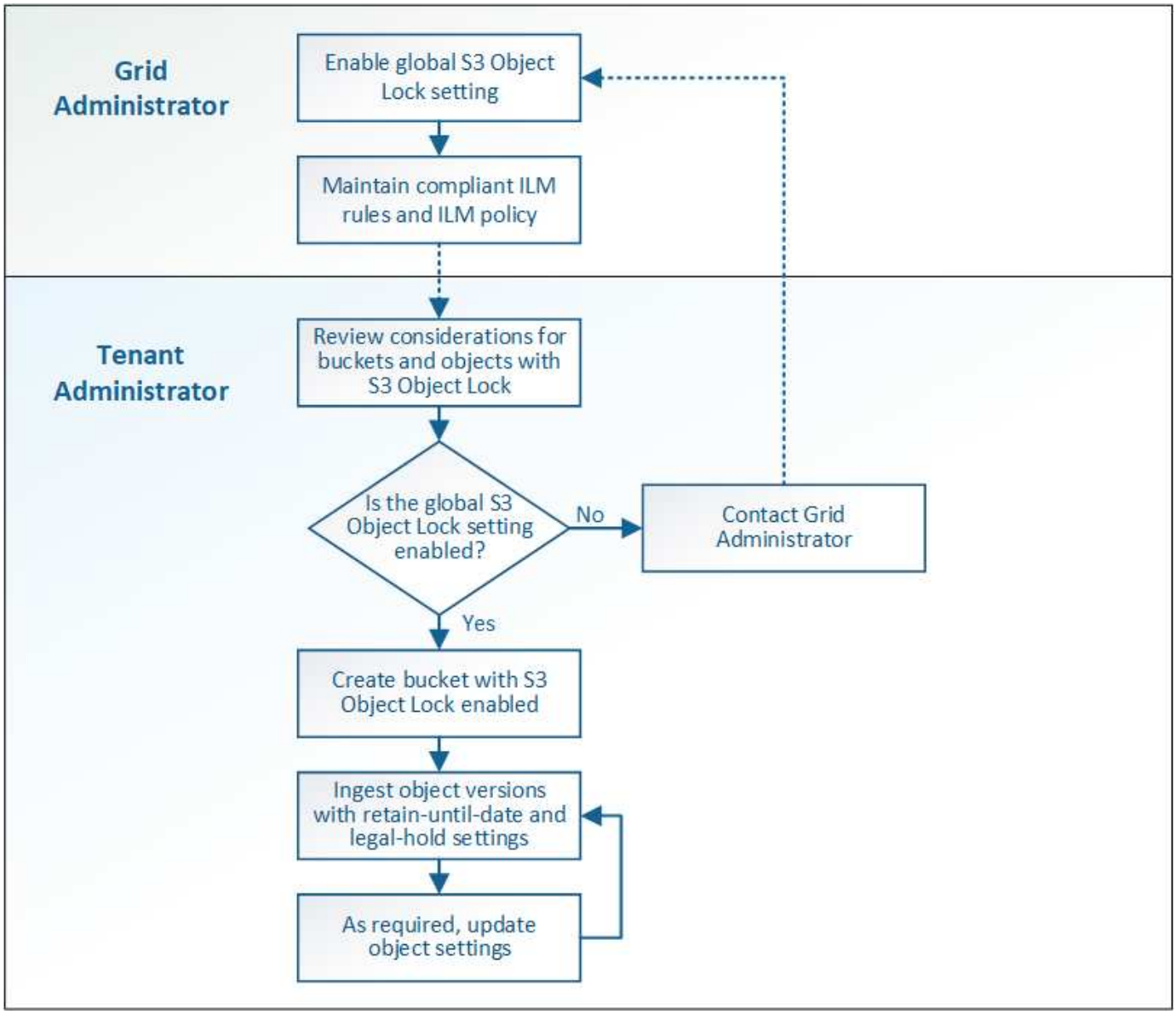
"ネットアップのナレッジベース： StorageGRID 11.5 でレガシー準拠バケットを管理する方法"

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、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"

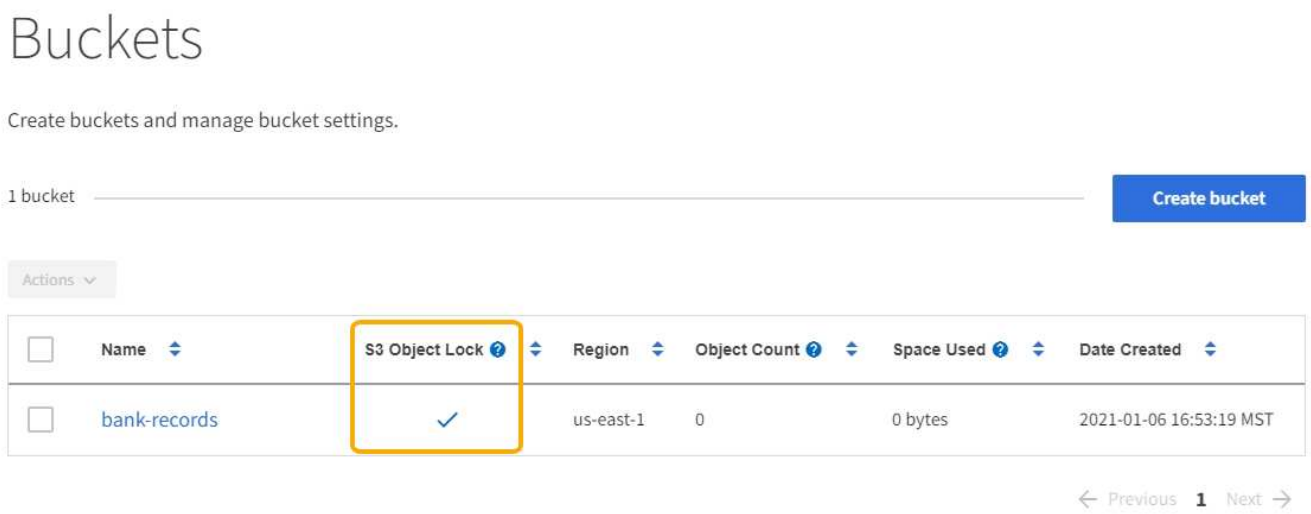
S3 オブジェクトのロックの要件

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。



- 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。

- 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-une-date 設定またはリーガルホールド設定を指定すると、要求で指定されたバージョンのみが保護されます。オブジェクトの以前のバージョンはロックされたまま、オブジェクトの新しいバージョンを作成できます。

S3 オブジェクトのロックが有効なバケット内のオブジェクトのライフサイクル

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

1. * オブジェクトの取り込み *
   - S3 オブジェクトのロックが有効になっているバケットにオブジェクトのバージョンを追加するときに、 S3 クライアントアプリケーションはオプションでオブジェクトの保持設定を指定できます（ retain-until date 、 legal hold 、または both ）。StorageGRID は、そのオブジェクトのメタデータを生成します。これには、一意のオブジェクト ID （ UUID ）と取り込み日時が含まれます。
   - 保持設定のあるオブジェクトのバージョンが取り込まれたあとに、そのデータと S3 ユーザ定義メタデータを変更することはできません。
   - StorageGRID は、オブジェクトメタデータをオブジェクトデータとは別に格納します。各サイトですべてのオブジェクトメタデータのコピーを 3 つ保持します。
2. * オブジェクト保持 *
   - オブジェクトの複数のコピーが StorageGRID によって格納される。コピーの正確な数、タイプ、格納場所は、アクティブな ILM ポリシーの準拠ルールによって決まります。
3. * オブジェクトの削除 *
   - オブジェクトは、 retain-until - date に到達したときに削除できます。
   - リーガルホールドの対象になっているオブジェクトは削除できません。

S3バケットの作成

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

必要なもの

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

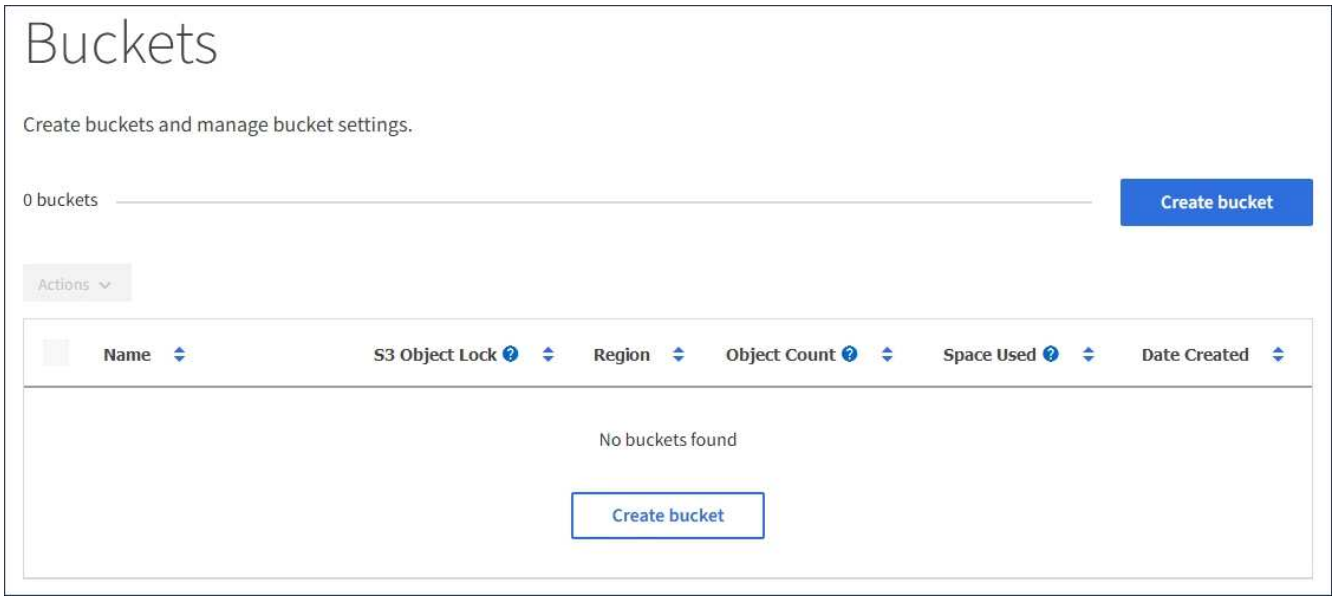
- S3オブジェクトロックを使用してバケットを作成する場合は、StorageGRID システムでグローバルなS3オブジェクトロック設定を有効にしておく必要があります。また、S3オブジェクトロックのバケットとオブジェクトに関する要件を確認しておく必要があります。

  "S3 オブジェクトロックを使用する"

手順

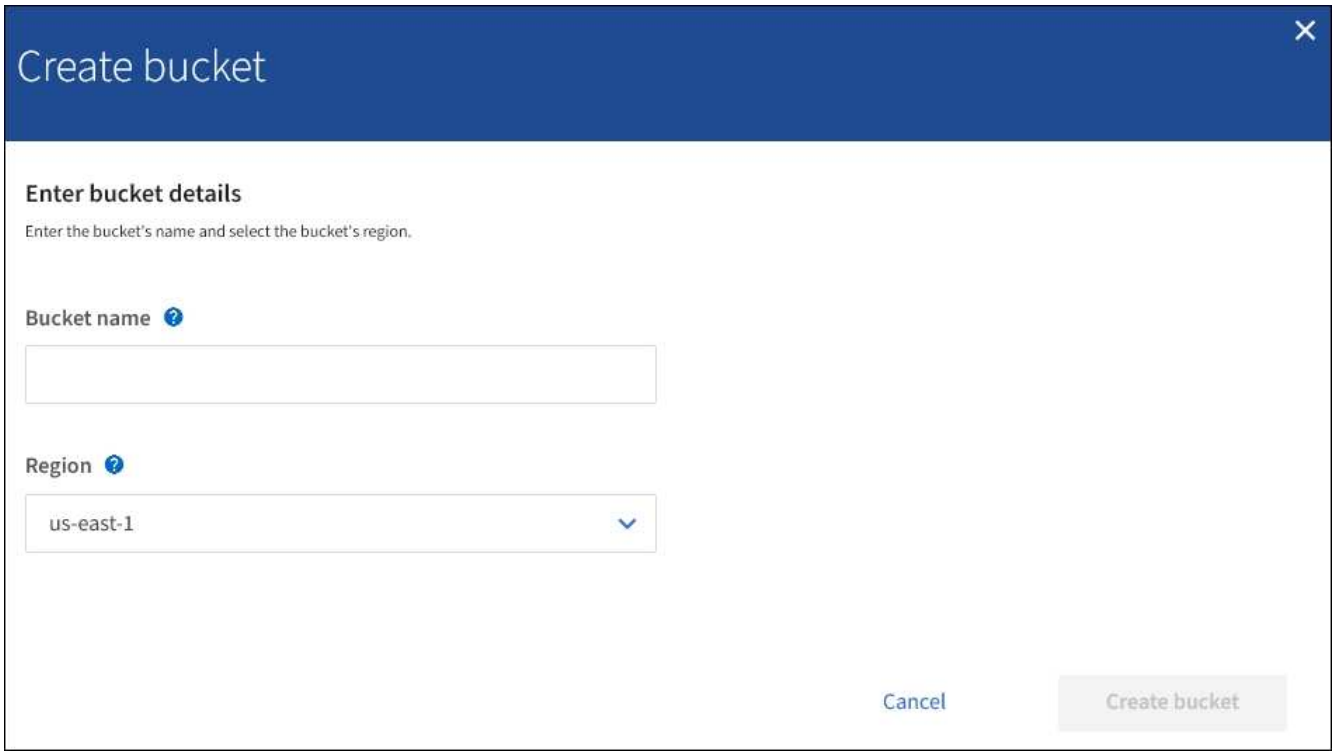
1. ストレージ（ S3 ） * > * バケット * を選択します。

   バケットページが表示され、すでに作成されているバケットが一覧表示されます。



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。



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、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。

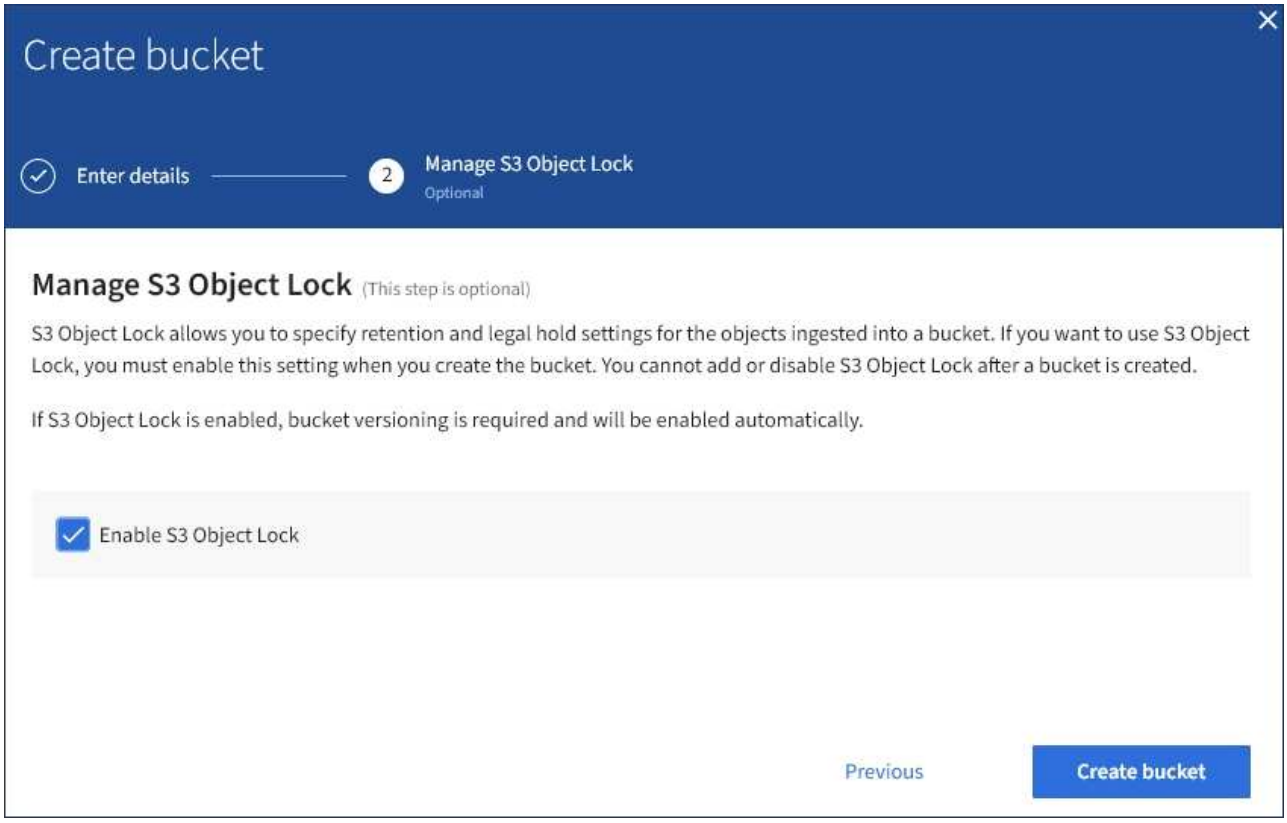
詳細については、Amazon Web Services（AWS）ドキュメントを参照してください。

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に作成されます `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。



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。

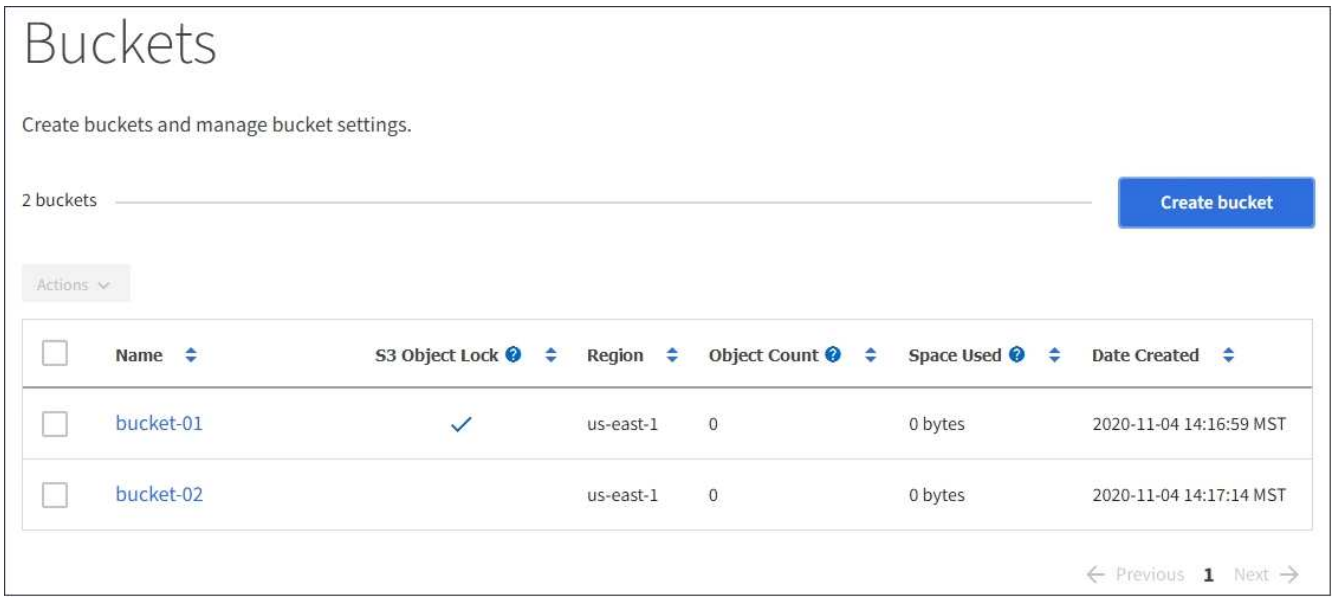
必要なもの

- 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。



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。

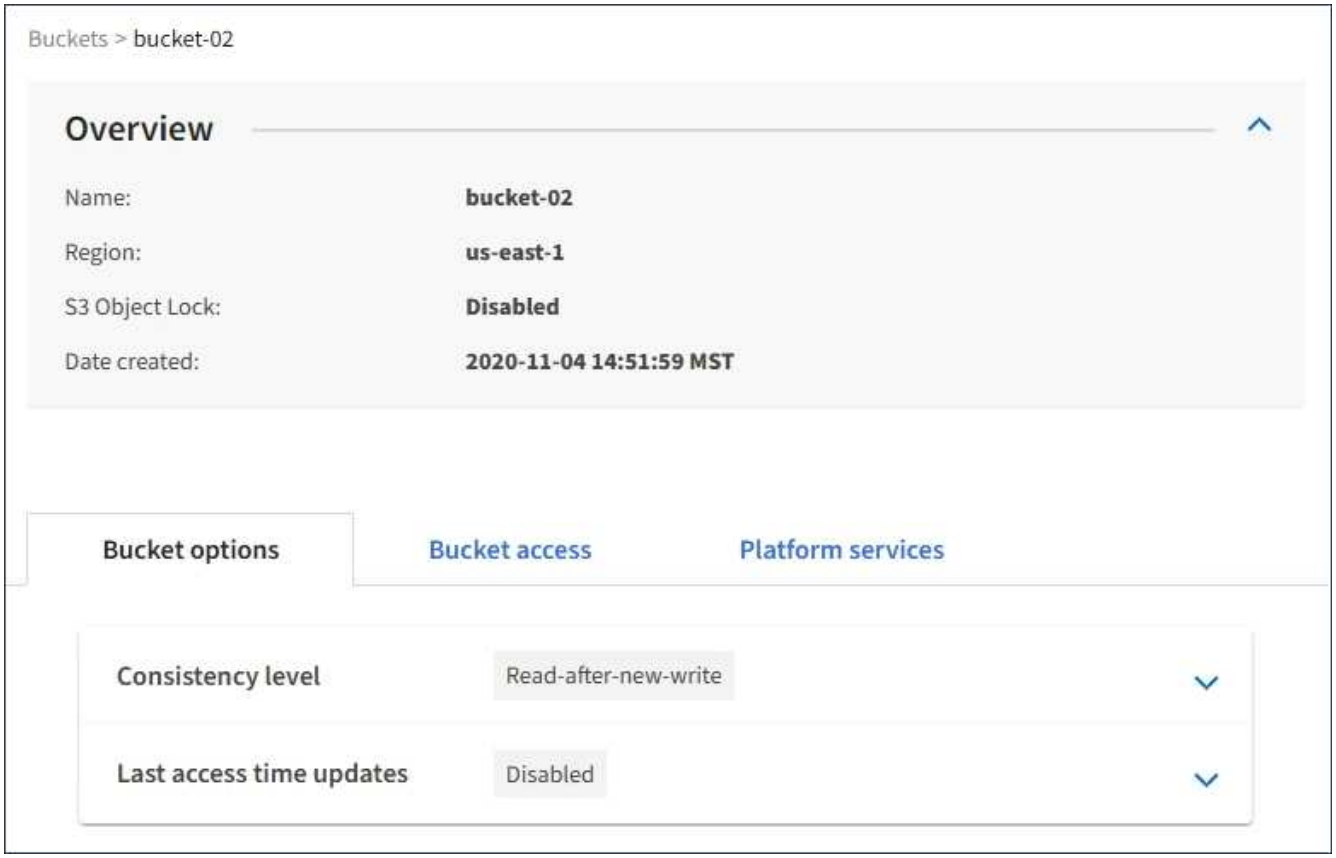
「オブジェクト数」と「使用済みスペース」の値が概算値として表示されます。これらの推定値は、取り込みのタイミング、ネットワーク接続、ノードのステータスによって左右されます。

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。



関連情報

"整合性レベルを変更する"

"最終アクセス日時の更新の有効化または無効化"

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

"CloudMirrorレプリケーションの設定"

"イベント通知を設定する"

"検索統合サービスの設定"

整合性レベルを変更する

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

必要なもの

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

このタスクについて

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

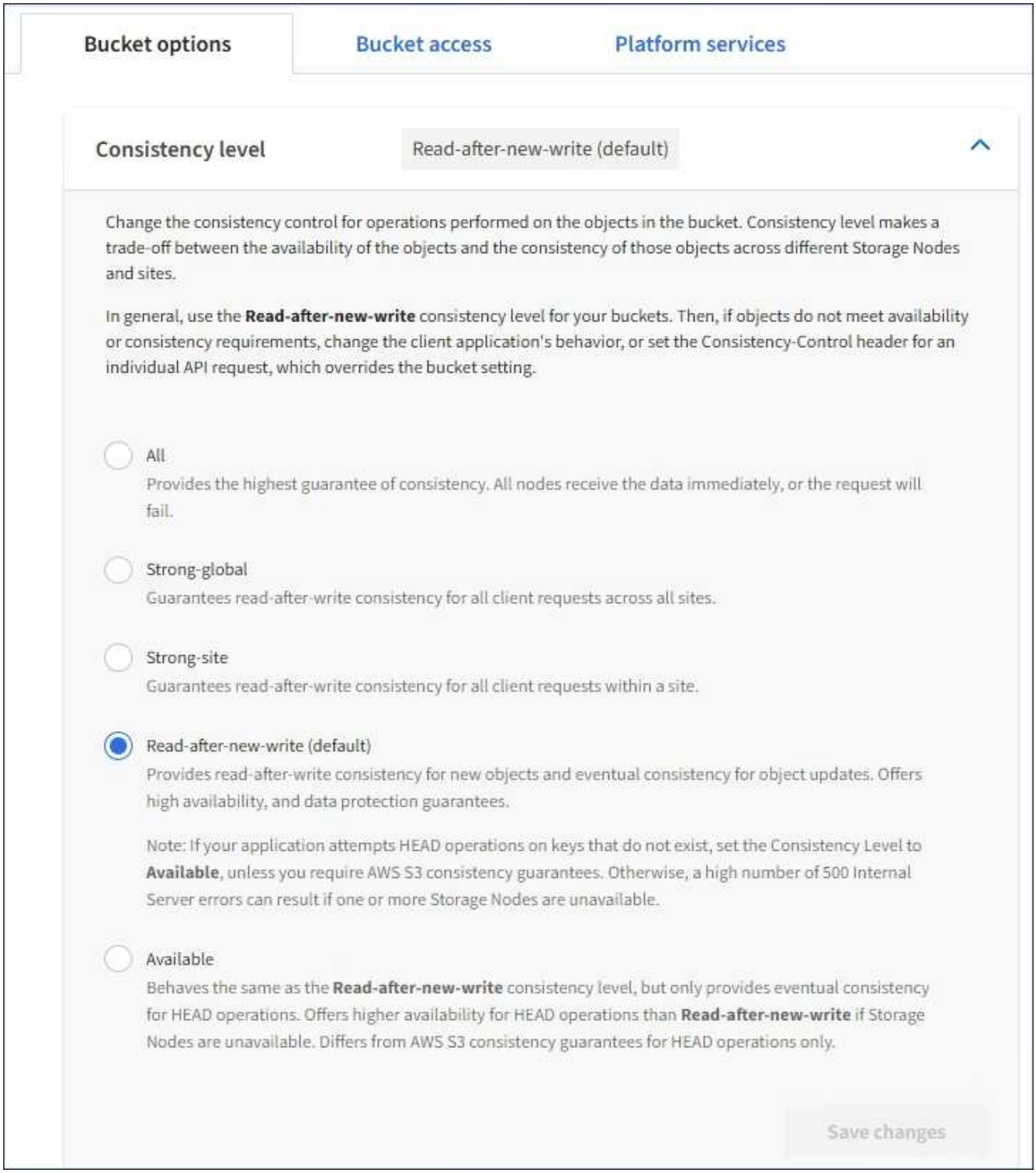
> バケットの整合性レベルを変更した場合、変更後のレベルを満たすことが保証されるのは、変更後に取り込まれたオブジェクトのみです。

手順

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

   バケットの詳細ページが表示されます。

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



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

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

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

5. 「変更を保存」を選択します。

関連情報

"テナント管理権限"

最終アクセス日時の更新の有効化または無効化

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

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

必要なもの

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

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

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

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

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

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

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

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

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

要求のタイプ	最終アクセス時間が無効な場合の動作（デフォルト）		最終アクセス時間が有効な場合の動作	
	最終アクセス時間の更新	ILM 評価キューへのオブジェクトの追加	最終アクセス時間の更新	ILM 評価キューへのオブジェクトの追加
オブジェクト、そのアクセス制御リスト、またはメタデータの読み出し要求	いいえ	いいえ	はい。	はい。
オブジェクトメタデータの更新要求	はい。	はい。	はい。	はい。
バケット間でのオブジェクトのコピー要求	• 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	• 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	• 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	• 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

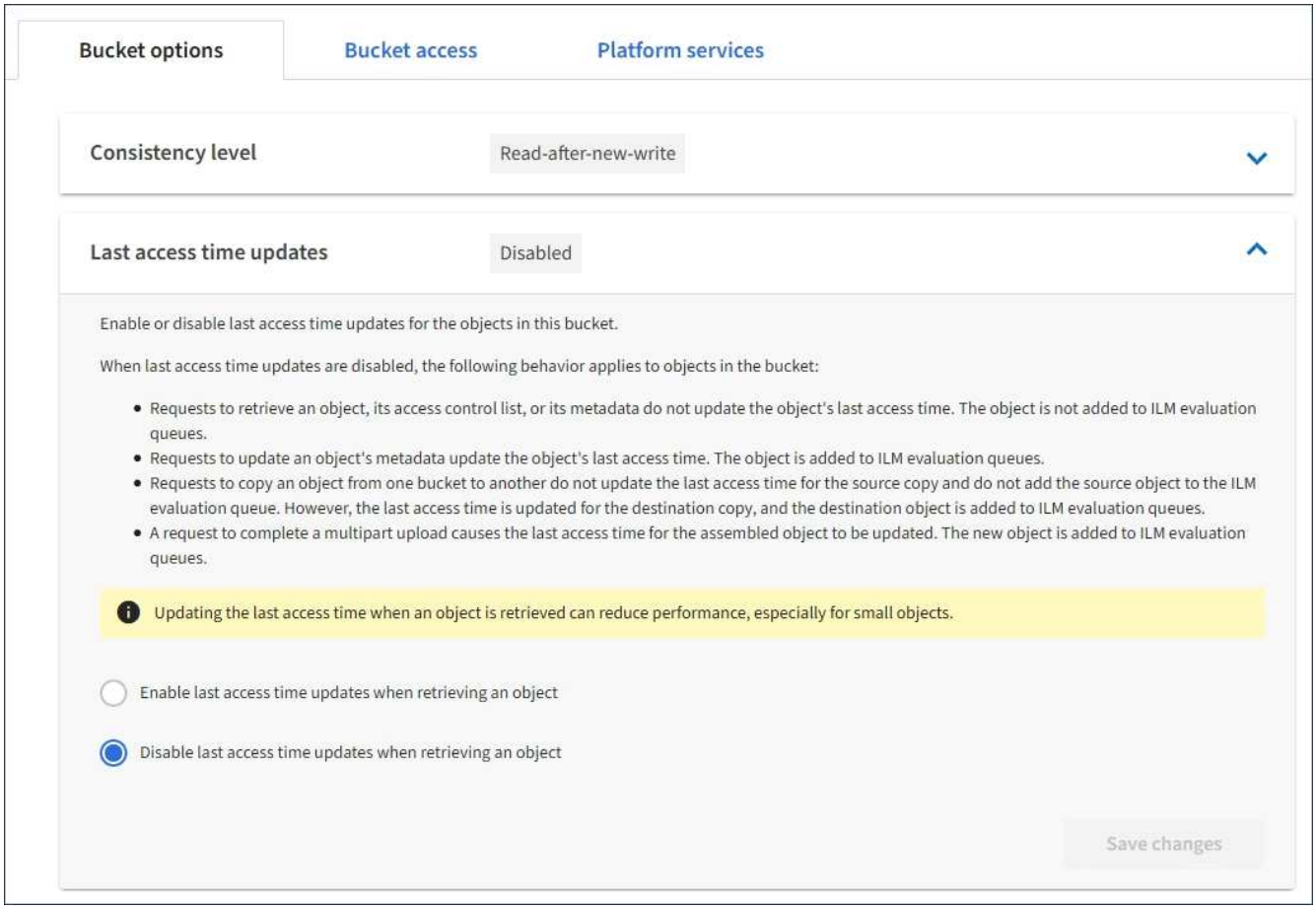
マルチパートアップロードの完了要求	はい、アセンブルされたオブジェクトの場合	はい、アセンブルされたオブジェクトの場合	はい、アセンブルされたオブジェクトの場合	はい、アセンブルされたオブジェクトの場合

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。



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。

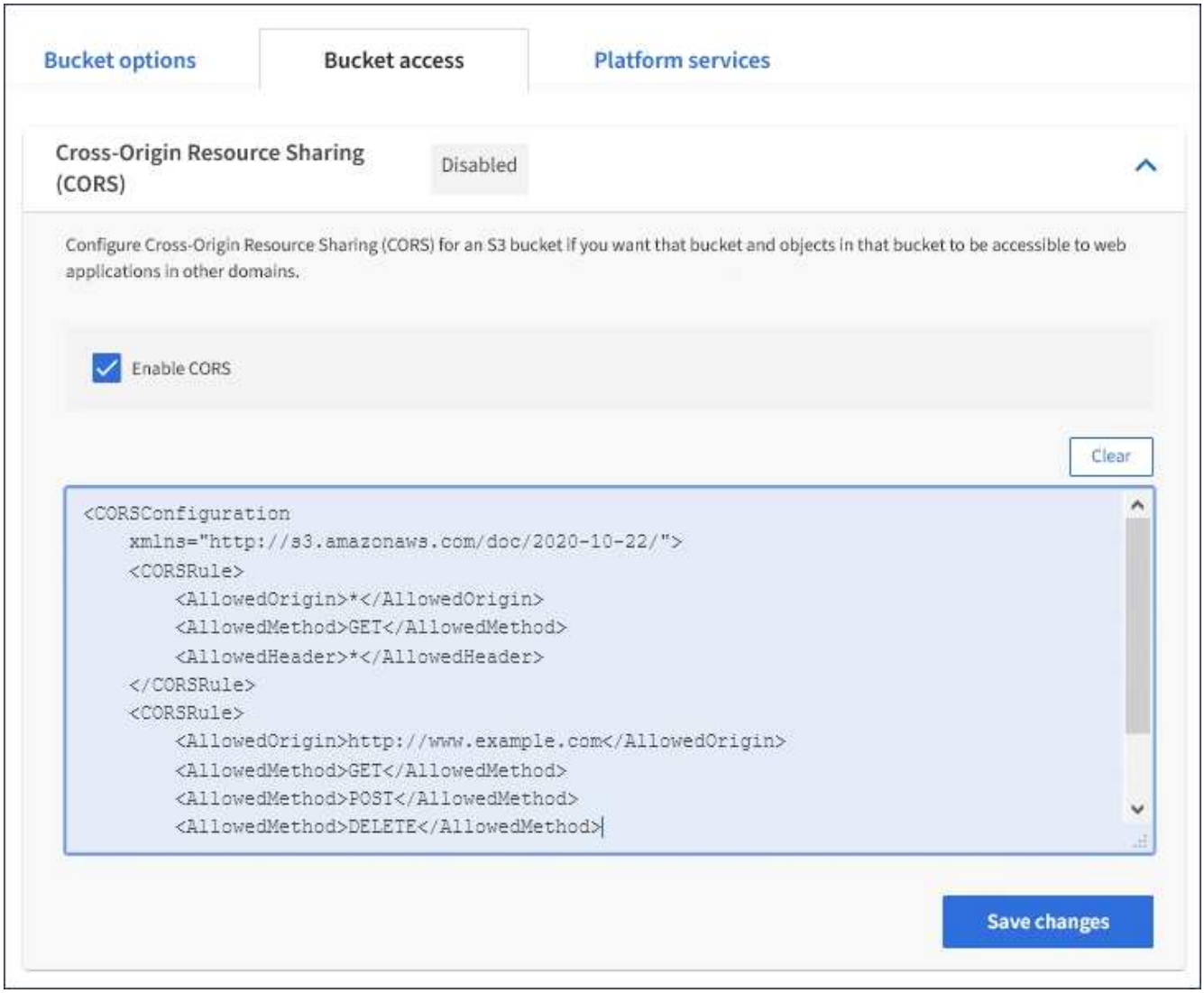
   ```
   <CORSConfiguration
       xmlns="http://s3.amazonaws.com/doc/2020-10-22/">
       <CORSRule>
           <AllowedOrigin>*</AllowedOrigin>
           <AllowedMethod>GET</AllowedMethod>
           <AllowedHeader>*</AllowedHeader>
       </CORSRule>
       <CORSRule>
           <AllowedOrigin>http://www.example.com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



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

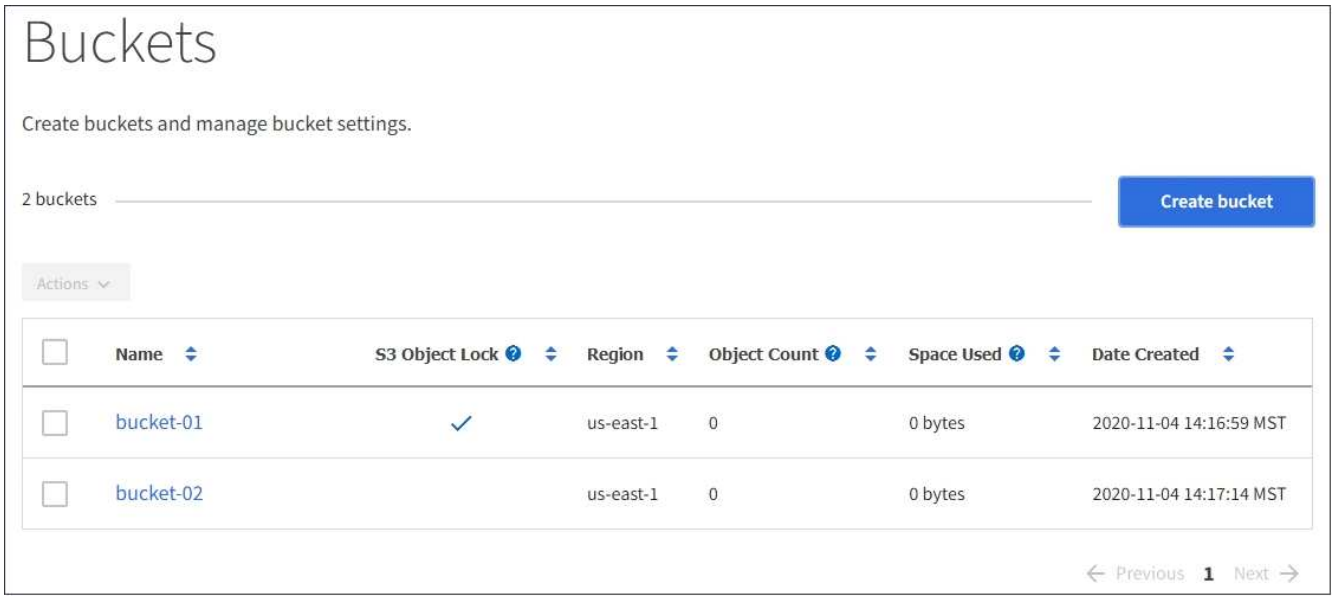
以下の手順では、 Tenant Manager を使用して S3 バケットを削除する方法について説明します。テナント管理APIまたはS3 REST APIを使用してS3バケットを削除することもできます。

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。

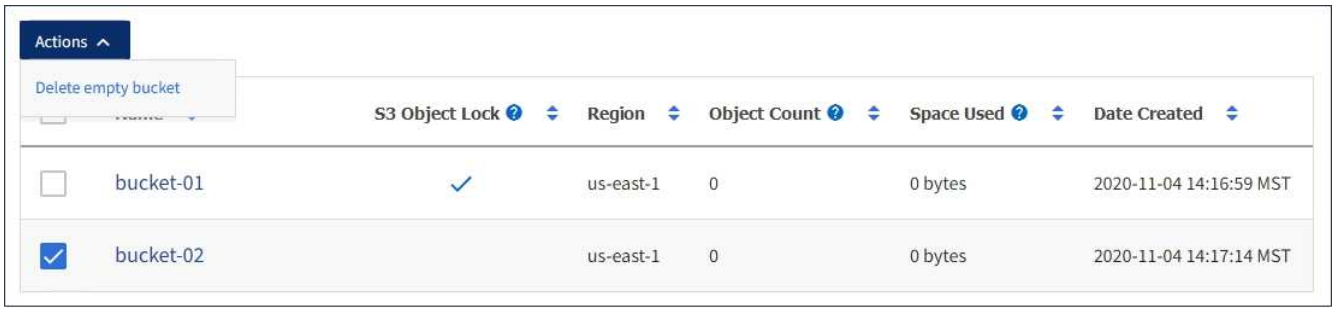
   バケットページが表示され、既存の S3 バケットがすべて表示されます。



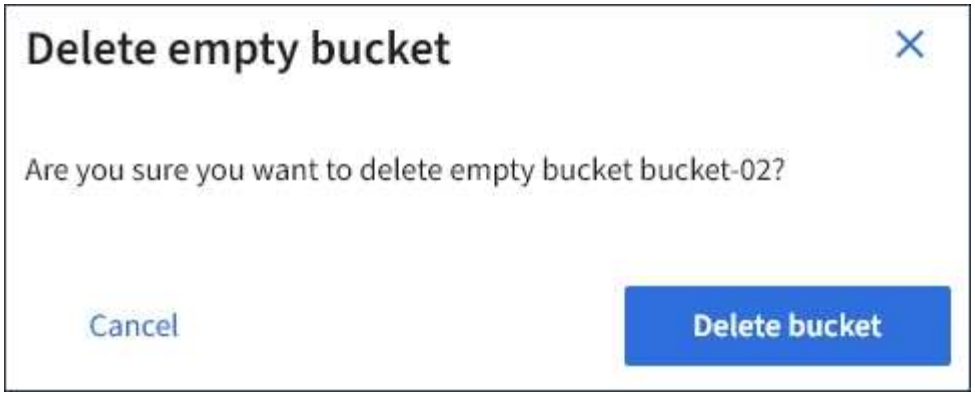
2. 削除する空のバケットのチェックボックスを選択します。

   [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。



   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"

著作権に関する情報

商標に関する情報