



S3 テナントアカウントを管理します StorageGRID

NetApp
October 03, 2025

目次

S3 テナントアカウントを管理します	1
S3 アクセスキーを管理します	1
独自の S3 アクセスキーを作成します	1
S3 アクセスキーを表示します	3
自分の S3 アクセスキーを削除します	5
別のユーザの S3 アクセスキーを作成します	6
別のユーザの S3 アクセスキーを表示します	8
別のユーザの S3 アクセスキーを削除します	10
S3 バケットを管理する	11
テナントで S3 オブジェクトロックを使用する	11
S3 バケットを作成する	15
S3 バケットの詳細を表示します	17
整合性レベルを変更します	19
最終アクセス日時の更新を有効または無効にします	20
バケットのオブジェクトのバージョン管理を変更する	23
Cross-Origin Resource Sharing (CORS) の設定	24
S3 バケットを削除します	26
Experimental S3 Console を使用します	28

S3 テナントアカウントを管理します

S3 アクセスキーを管理します

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。

独自の S3 アクセスキーを作成します

S3 テナントを使用している場合は、適切な権限があれば、自分の S3 アクセスキーを作成できます。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 にはを使用してサインインする必要があります [サポートされている Web ブラウザ](#)。
- **Manage Your Own S3 Credentials** 権限が必要です。を参照してください [テナント管理権限](#)。

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。

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

Choose expiration time

Do not set an expiration time
This access key will never expire.

Set an expiration time

MM/DD/YYYY [calendar icon] HH : MM AM

Cancel Create access key

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。ダイアログボックスを閉じた後でキーをコピーまたはダウンロードすることはできません。

The screenshot shows a 'Create access key' dialog box with a blue header. The progress bar indicates step 2, 'Download access key', is active. Below the header, the title 'Download access key' is followed by instructions: 'To save the keys for future reference, select **Download .csv**, or copy and paste the values to another location.' A light blue information box states: 'You will not be able to view the Access key ID or Secret access key after you close this dialog.' Two text input fields are shown: 'Access key ID' with the value '003HAHJ2CYU0SLGUL97V' and 'Secret access key' with the value 'djEKBlj3HPj3fYgJtoHUwkg8oEyRGcJaFXgdkCM'. Each field has a copy icon to its right. At the bottom right, there are two buttons: 'Download .csv' and '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。

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 にはを使用してサインインする必要があります [サポートされている Web ブラウザ](#)。
- 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。

<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

[独自の S3 アクセスキーを作成します](#)

[自分の S3 アクセスキーを削除します](#)

自分の S3 アクセスキーを削除します

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

必要なもの

- Tenant Manager にはを使用してサインインする必要があります [サポートされている Web ブラウザ](#)。
- Manage Your Own S3 Credentials 権限が必要です。を参照してください [テナント管理権限](#)。



アカウントに属する S3 バケットとオブジェクトには、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。定期的な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

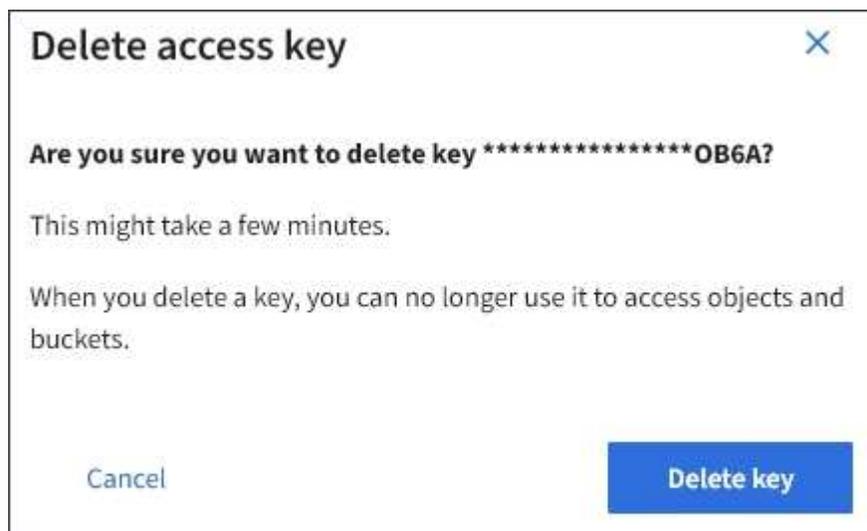
1. 「* storage (S3) * > * My access keys *」を選択します。

[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します

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

必要なもの

- Tenant Manager にはを使用してサインインする必要があります [サポートされている Web ブラウザ](#)。
- 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更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。定期的に変更し、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。

Create access key

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

Choose expiration time

Do not set an expiration time

This access key will never expire.

Set an expiration time

MM/DD/YYYY  HH : MM AM

Cancel **Create access key**

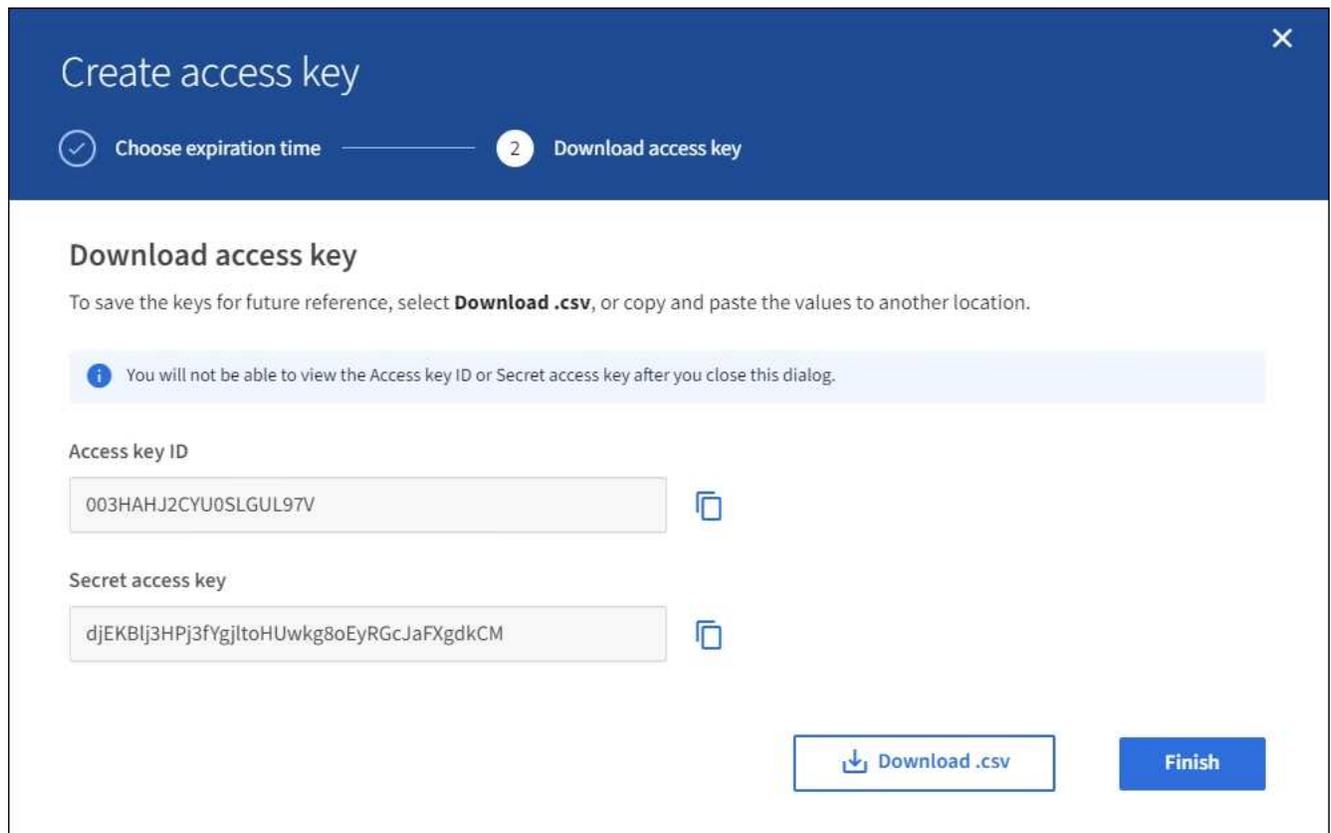
5. [アクセスキーの作成 *] を選択します。

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。ダイアログボックスを閉じた後でキーをコピーまたはダウンロードすることはできません。



7. [完了] を選択します。

新しいキーは、ユーザ詳細ページのアクセスキータブに表示されます。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 にはを使用してサインインする必要があります [サポートされている Web ブラウザ](#)。
- 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。定期的な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

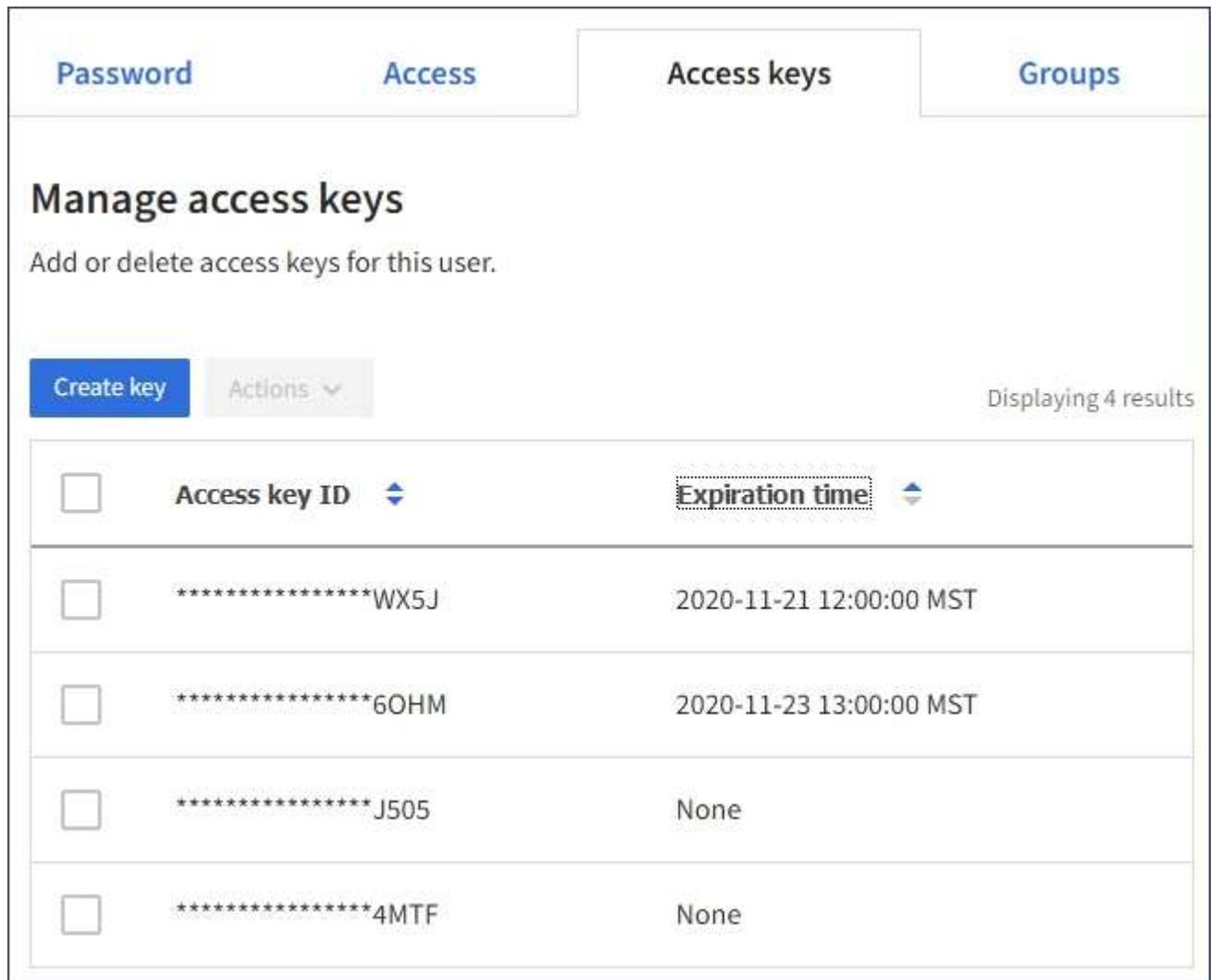
1. アクセス管理 * > * Users * を選択します。

[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。



The screenshot shows the 'Manage access keys' interface in the AWS IAM console. At the top, there are tabs for 'Password', 'Access', 'Access keys', and 'Groups'. Below the tabs, the title 'Manage access keys' is displayed, followed by the instruction 'Add or delete access keys for this user.' There is a 'Create key' button and an 'Actions' dropdown menu. On the right, it says 'Displaying 4 results'. The main content is a table with two columns: 'Access key ID' and 'Expiration time'. The 'Expiration time' column is highlighted with a dashed box. The table contains five rows, each with a checkbox on the left and an arrow on the right. The first row has an empty 'Access key ID' and 'Expiration time' field. The second row has '*****WX5J' and '2020-11-21 12:00:00 MST'. The third row has '*****6OHM' and '2020-11-23 13:00:00 MST'. The fourth row has '*****J505' and 'None'. The fifth row has '*****4MTF' and 'None'.

<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ます

別のユーザの S3 アクセスキーを削除します

別のユーザの **S3** アクセスキーを削除します

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

必要なもの

- Tenant Manager にはを使用してサインインする必要があります [サポートされている Web ブラウザ](#)。
- Root Access 権限が必要です。を参照してください [テナント管理権限](#)。



ユーザに属する S3 バケットとオブジェクトには、Tenant Manager でそのユーザに対して表示されるアクセスキー ID とシークレットアクセスキーを使用してアクセスできます。このため、アクセスキーはパスワードと同じように保護する必要があります。定期的な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。

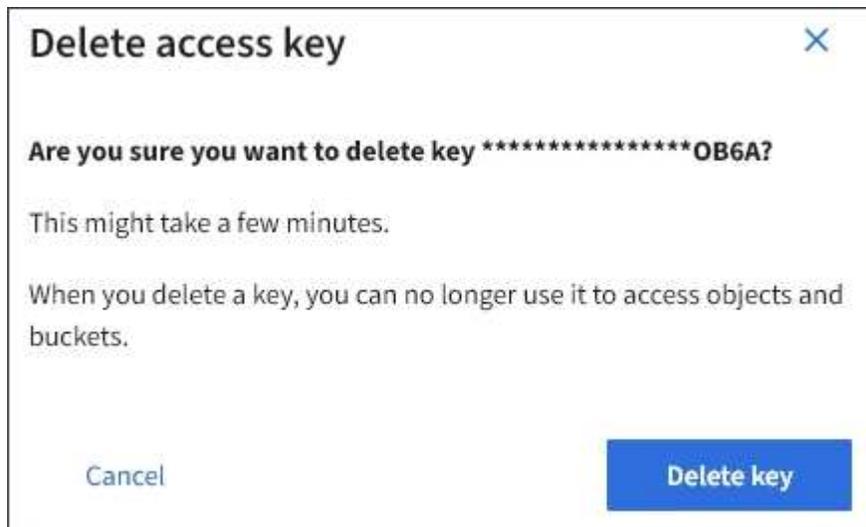
2. S3 アクセスキーを管理するユーザを選択します。

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。

S3 バケットを管理する

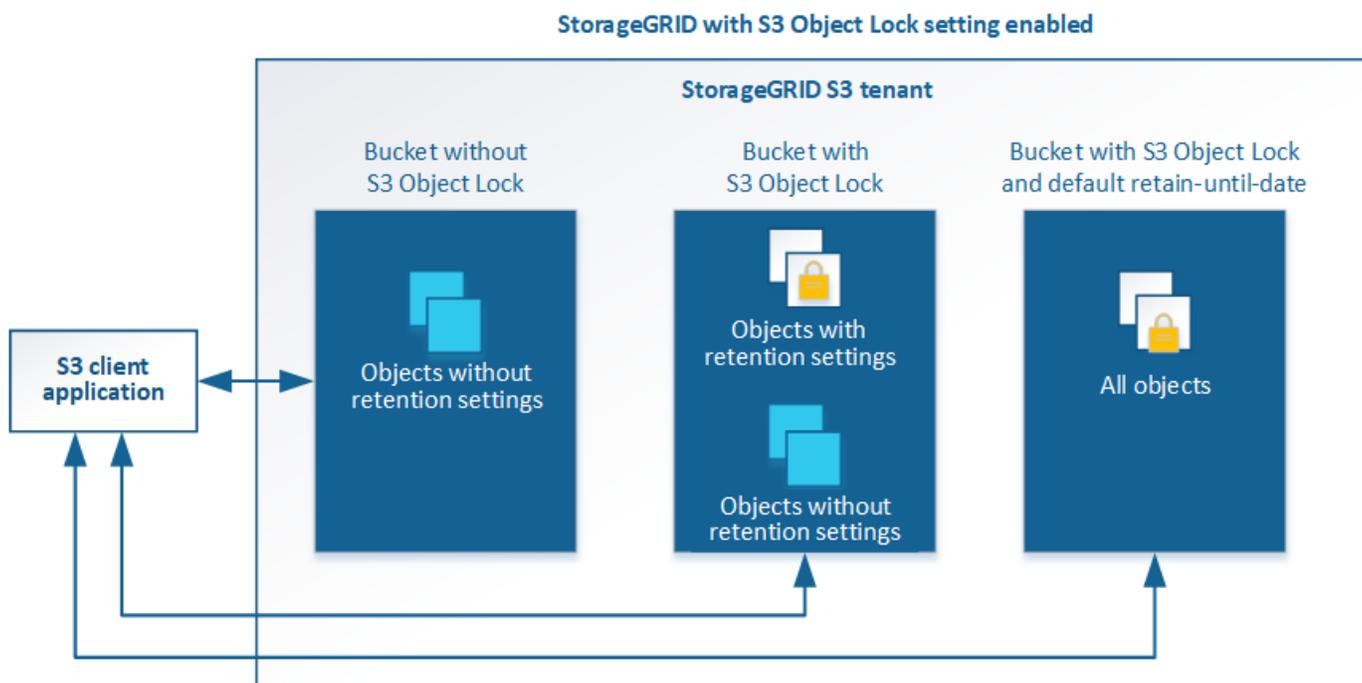
テナントで S3 オブジェクトロックを使用する

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ー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。

また可能です [バケットのデフォルトの保持モードとデフォルトの保持期間を指定](#)。これらのポリシーは、バケットに追加した各オブジェクトに適用され、それぞれの保持設定は指定されません。

これらの設定の詳細については、[を参照してください S3 オブジェクトロックを使用する](#)。

従来の準拠バケットを管理します

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トを参照してください。

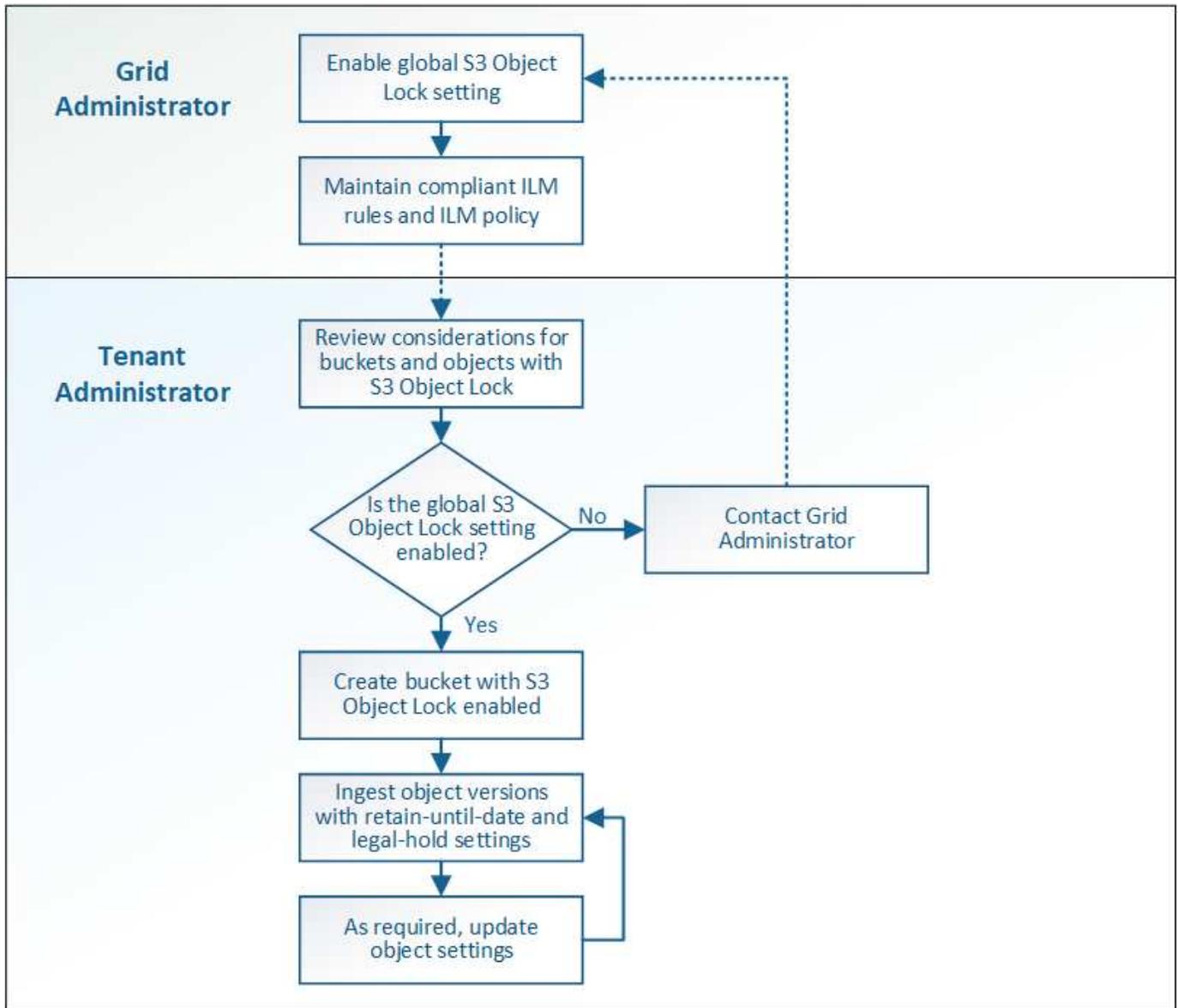
["ネットアップのナレッジベース： StorageGRID 11.5 でレガシー準拠バケットを管理する方法"](#)

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。グリッド管理者は、も確認する必要があります [情報ライフサイクル管理 \(ILM\) ポリシー](#) は「準拠」です。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。



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。
- 必要に応じて、バケットにデフォルトの保持を設定できます。オブジェクトのバージョンがアップロードされると、デフォルトの保持設定がオブジェクトのバージョンに適用されます。バケットのデフォルト設定を上書きするには、オブジェクトバージョンのアップロード要求で保持モードと retain-date を指定します。
- 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

- オブジェクトバージョンを保護するためには、S3 クライアントアプリケーションでバケットのデフォルト保持を設定するか、各アップロード要求で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 バケットを作成する

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 にはを使用してサインインします [サポートされている Web ブラウザ](#)。
- Manage 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、グループまたはバケットポリシーの権限の設定よりも優先されます。



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

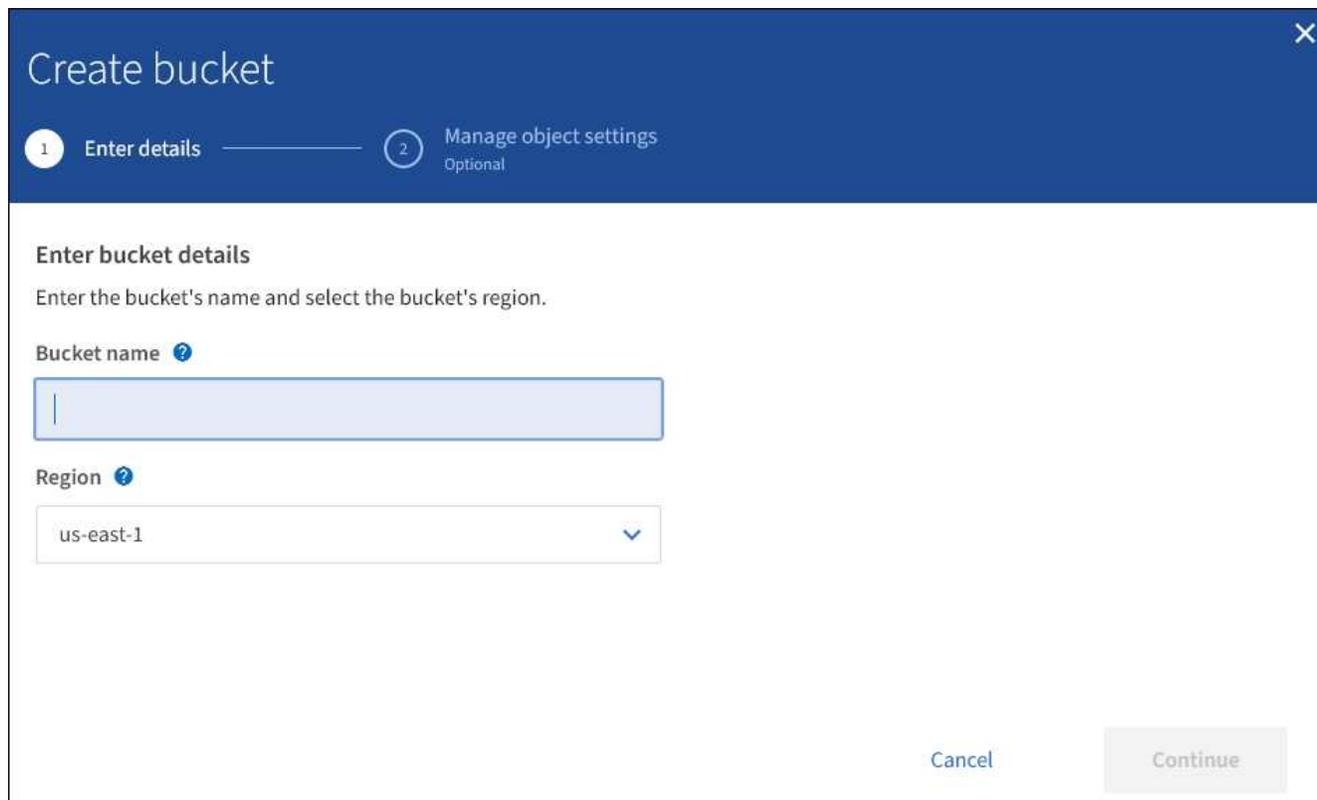
- S3 オブジェクトロックを使用してバケットを作成する場合は、StorageGRID システムで S3 オブジェクトのグローバルロック設定を有効にして、S3 オブジェクトのロックバケットとオブジェクトの要件を確認しておく必要があります。

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。

2. [* バケットの作成 *] を選択します。



3. バケットの一意的名前を入力します。

 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。
- 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。
- 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、を参照してください "[バケットの命名規則に関する Amazon Web Services \(AWS\) のドキュメント](#)".

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、すべてのバケットは「us-east-1」リージョンに作成されます。

 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. 「* Continue *」を選択します。
6. 必要に応じて、バケットのオブジェクトのバージョン管理を有効にします。

このバケット内の各オブジェクトのすべてのバージョンを格納する場合は、オブジェクトのバージョン管理を有効にします。そのあと、必要に応じて以前のバージョンのオブジェクトを読み出すことができます。

7. S3 Object Lock セクションが表示された場合は、必要に応じてバケットの S3 Object Lock を有効にします。



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。

S3 オブジェクトのロックセクションは、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にのみ表示されます。

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。また可能です [バケットのデフォルトの保持モードとデフォルトの保持期間を指定](#) このポリシーは、バケットに取り込まれ、それぞれの保持設定を指定しない各オブジェクトに適用されます。

8. [* 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 について理解する](#)

[S3 を使用する](#)

S3 バケットの詳細を表示します

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 にはを使用してサインインする必要があります [サポートされている Web ブラウザ](#)。

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.

3 buckets Create bucket

Actions Experimental S3 Console [↗](#)

<input type="checkbox"/>	Name	S3 Object Lock	Region	Object Count	Space Used	Date Created
<input type="checkbox"/>	bucket-01a	✓	us-east-1	0	0 bytes	2022-01-06 13:48:08 MST
<input type="checkbox"/>	bucket-02a	✓	us-east-1	0	0 bytes	2022-01-06 13:48:26 MST
<input type="checkbox"/>	bucket-03a		us-east-1	0	0 bytes	2022-01-06 13:48:38 MST

2. 各バケットの情報を確認します。

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

- Name : バケットの一意的な名前。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。バケットでバージョン管理が有効になっている場合は、削除したオブジェクトのバージョンがオブジェクト数に含まれます。

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では、バケットオプション、バケットへのアクセス、およびの設定を表示および編集できます [プラットフォームサービス](#)。

Buckets > bucket-01

Overview

Name: **bucket-01**
Region: **us-east-1**
Date created: **2021-11-30 09:55:55 MST**

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

Bucket options | Bucket access | Platform services

Consistency level	Read-after-new-write (default)	▼
Last access time updates	Disabled	▼
Object versioning	Enabled	▼
S3 Object Lock	Disabled	▼

整合性レベルを変更します

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 にはを使用してサインインする必要があります [サポートされている Web ブラウザ](#)。
- 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。を参照してください [テナント管理権限](#)。

このタスクについて

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

最終アクセス日時の更新を有効または無効にします

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

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 にはを使用してサインインする必要があります [サポートされている Web ブラウザ](#)。
- 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。を参照してください [テナント管理権限](#)。
- 最終アクセス時間 * は、ILM ルールの * 参照時間 * 配置手順で使用できるオプションの 1 つです。ルールの参照時間を最終アクセス日時に設定すると、グリッド管理者は、オブジェクトが最後に読み出された (読み取りまたは表示された) タイミングに基づいて特定のストレージの場所にオブジェクトが配置されるように指定できます。

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

作成できます。

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



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

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



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

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

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

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

要求のタイプ	最終アクセス時間が無効な場合の動作（デフォルト）		最終アクセス時間が有効な場合の動作	
	最終アクセス時間の更新	ILM 評価キューへのオブジェクトの追加	最終アクセス時間の更新	ILM 評価キューへのオブジェクトの追加
オブジェクト、そのアクセス制御リスト、またはメタデータの読み出し要求	いいえ	いいえ	はい。	はい。
オブジェクトメタデータの更新要求	はい。	はい。	はい。	はい。
バケット間でのオブジェクトのコピー要求	<ul style="list-style-type: none"> • 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 (default)'. The 'Last access time updates' section is currently set to 'Disabled'. Below this, there is explanatory text and a list of behaviors when updates are disabled. At the bottom, there are two radio button options: 'Enable last access time updates when retrieving an object' (which is currently unselected) and 'Disable last access time updates when retrieving an object' (which is currently selected). A 'Save changes' button is visible 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

バケットのオブジェクトのバージョン管理を変更する

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

必要なもの

- Tenant Manager にはを使用してサインインします [サポートされている Web ブラウザ](#)。
- Manage 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、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。

テナント管理権限

このタスクについて

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

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

S3 オブジェクトのバージョン管理

S3 バージョン管理オブジェクトの ILM ルールとポリシー（例 4）

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。
3. * バケットオプション * > * オブジェクトバージョン管理 * を選択します。

Bucket options
Bucket access
Platform services

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

Last access time updates Disabled ▼

Object versioning Enabled ▲

Enable object versioning if you want to store every version of each object in this bucket. You can then retrieve a previous object version to recover from an error.

After versioning is enabled, you can optionally suspend versioning for the bucket. New object versions are no longer created, but you can still retrieve any existing object versions.

Enable versioning

Suspend versioning

Save changes

4. このバケット内のオブジェクトのバージョン管理の状態を選択します。



S3 オブジェクトのロックまたはレガシーのコンプライアンスが有効になっている場合、* オブジェクトのバージョン管理 * オプションは無効になります。

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

5. 「変更を保存」を選択します。

Cross-Origin Resource Sharing (CORS) の設定

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

からアクセスできるようにする必要がある場合は、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 にはを使用してサインインする必要があります [サポートされている Web ブラウザ](#)。
- 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、「Images」という名前の S3 バケットを使用してグラフィックスを格納するとします。「Images」バケットの CORS を設定することで、そのバケット内の画像を Web サイト「<http://www.example.com>」に表示できます。

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、すべてのドメインがバケットに GET 要求を送信できますが、POST 要求と DELETE 要求を送信できるのは「[+ http://www.example.com](http://www.example.com)」ドメインだけです。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 にはを使用してサインインする必要があります [サポートされている Web ブラウザ](#)。
- 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。を参照してください [テナント管理権限](#)。
- 削除するバケットが空です。

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。を使用して S3 バケットを削除することもできます [テナント管理 API](#) または [S3 REST API](#)。

オブジェクト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、[を参照してください](#) [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ための手順](#)。

手順

1. ストレージ（S3） * > * バケット * を選択します。

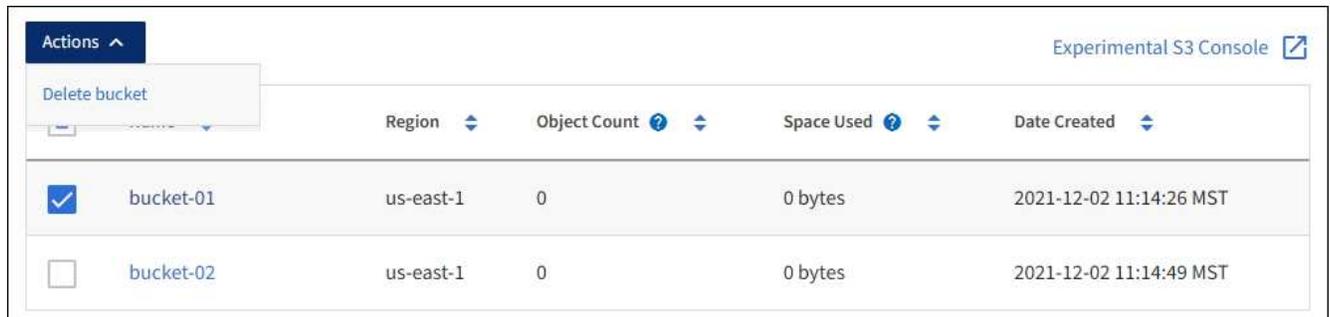
バケットページが表示され、既存の S3 バケットがすべて表示されます。



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。一度に複数のバケットを選択できます。

[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 * バケットの削除 *（複数選択した場合は * バケットの削除 *）を選択します。



4. 確認ダイアログボックスが表示されたら、「* はい *」を選択して、選択したバケットをすべて削除します。

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

バケットが空でない場合は、エラーメッセージが表示されます。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。

Experimental S3 Console を使用します

S3 コンソールを使用して S3 バケット内のオブジェクトを表示できます。

S3 コンソールを使用して、次の操作を実行することもできます。

- オブジェクト、オブジェクトバージョン、およびフォルダの追加と削除
- オブジェクトの名前を変更する
- バケットとフォルダ間でオブジェクトを移動およびコピーする
- オブジェクトタグを管理します
- オブジェクトのメタデータを表示します
- オブジェクトをダウンロードします



S3 コンソールは完全にテストされておらず、「experimental」としてマークされています。オブジェクトの一括管理や本番環境での使用は対象外です。テナントで S3 コンソールを使用するのは、オブジェクトをアップロードして新しい ILM ポリシーをシミュレートするとき、取り込みの問題をトラブルシューティングするとき、コンセプトの実証（POC）グリッドや非本番環境のグリッドを使用するときなど、少数のオブジェクトに対して機能を実行する場合のみにしてください。

必要なもの

- Tenant Manager にはを使用してサインインします [サポートされている Web ブラウザ](#)。
- Manage Your Own S3 Credentials 権限が設定されます。
- バケットを作成しておきます。
- ユーザのアクセスキー ID とシークレットアクセスキーを確認しておきます。オプションで 'この情報を含む'.csv ファイルがありますを参照してください [アクセスキーの作成手順](#)。

手順

1. [* バケット *] を選択します。
2. 選択するオプション **Experimental S3 Console** 。このリンクには、バケットの詳細ページからもアクセスできます。
3. Experimental S3 Console のサインインページで、アクセスキー ID とシークレットアクセスキーをフィールドに貼り付けます。それ以外の場合は、[Upload access keys] を選択し、[.csv] ファイルを選択します。
4. 「サインイン」を選択します。
5. 必要に応じてオブジェクトを管理します。



Buckets > bucket-01

↑ bucket-01

Upload New folder Refresh Actions

<input type="checkbox"/>	Name	Logical space used	Last modified on
<input type="checkbox"/>	03_Grid_Primer_11.5.pdf	2.73 MB	2021-12-03 09:43:26 MST
<input type="checkbox"/>	04_Tenant_Users_Guide_11.5.pdf	1.07 MB	2021-12-03 09:44:24 MST
<input type="checkbox"/>	06_Tenant_Users_Guide_11.5.pdf	1.25 MB	2021-12-03 09:44:27 MST
<input type="checkbox"/>	08_Tenant_Users_Guide_11.5.pdf	1.25 MB	2021-12-03 09:44:27 MST
<input type="checkbox"/>	09_Tenant_Users_Guide_11.5.pdf	1.25 MB	2021-12-03 09:44:26 MST
<input type="checkbox"/>	10_Grid_Primer_11.5.pdf	2.8 MB	2021-12-03 09:43:27 MST

Select an object or folder to view its details.

Displaying 16 objects
Selected 0 objects

|< < Previous 1 Next > >|

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。