



テナントグループを管理する

StorageGRID 11.8

NetApp
March 19, 2024

目次

テナントグループを管理する.....	1
S3 テナント用のグループを作成します	1
Swift テナント用のグループを作成します.....	4
テナント管理権限	6
グループを管理します.....	7

テナントグループを管理する

S3 テナント用のグループを作成します

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

作業を開始する前に

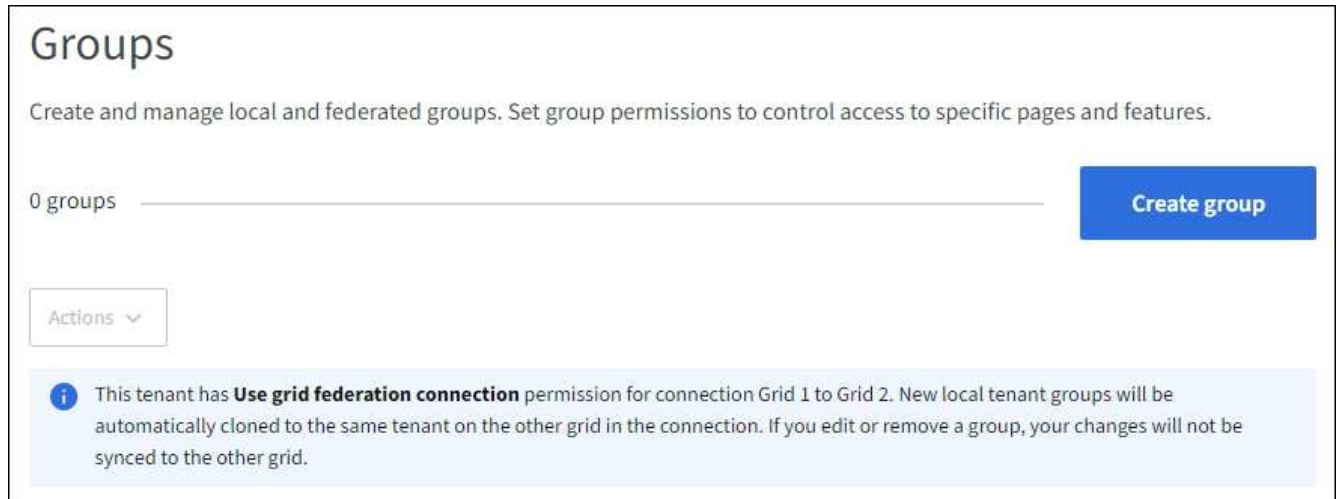
- Tenant Manager にはを使用してサインインします "サポートされている Web ブラウザ"。
- が設定されたユーザグループに属している必要があります "rootアクセス権限"。
- フェデレーテッドグループをインポートする場合は、を用意しておきます "アイデンティティフェデレーションが設定された"およびフェデレーテッドグループが設定済みのアイデンティティソースにすでに存在します。
- テナントアカウントに* Use grid federation connection *権限が割り当てられている場合は、のワークフローと考慮事項を確認しておきます "テナントグループおよびテナン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

グループ作成ウィザードにアクセスします

最初に、グループ作成ウィザードにアクセスします。

手順

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



3. 「* グループを作成 *」を選択します。

グループタイプを選択します

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

手順

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

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

2. グループの名前を入力します。

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



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

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

3. 「* Continue *」を選択します。

グループの権限を管理します

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

手順

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



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

2. このグループの権限を1つ以上選択します。

を参照してください ["テナント管理権限"](#)。

3. 「* Continue *」を選択します。

S3グループポリシーを設定

グループポリシーによって、ユーザに付与するS3アクセス権限が決まります。

手順

1. このグループに使用するポリシーを選択します。

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

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

言語の構文や例など、グループポリシーの詳細については、を参照してください "[グループポリシーの例](#)"。

3. ローカルグループを作成する場合は、「* Continue *」を選択します。フェデレーテッドグループを作成する場合は、* Create group * および * Finish * を選択します。

ユーザの追加（ローカルグループのみ）

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



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

手順

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

作成したグループがグループのリストに表示されます。

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

Swift テナント用のグループを作成します

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



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

作業を開始する前に

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

グループ作成ウィザードにアクセスします

手順

最初に、グループ作成ウィザードにアクセスします。

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

グループタイプを選択します

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

手順

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

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

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

グループの権限を管理します

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

手順

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



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

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

Swiftグループポリシーを設定します

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

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

ユーザの追加 (ローカルグループのみ)

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

手順

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

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

2. [グループの作成 *] と [完了 *] を選択します。

作成したグループがグループのリストに表示されます。

テナント管理権限

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

アクセス権	説明	詳細
ルートアクセス	Tenant Manager とテナント管理 API へのフルアクセスを提供します。	Swiftユーザがテナントアカウントにサインインするには、Root Access権限が必要です。
管理者	Swift テナントのみ。このテナントアカウントの Swift コンテナとオブジェクトへのフルアクセスを提供します	SwiftユーザがSwift REST APIを使用して処理を実行するには、Swift Administrator権限が必要です。
自分のS3クレデンシャルを管理します	ユーザに自分の S3 アクセスキーの作成および削除を許可します。	この権限がないユーザには、* storage (S3) > My S3 access keys *メニューオプションが表示されません。

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

グループを管理します

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

作業を開始する前に

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

- が設定されたユーザグループに属している必要があります ["rootアクセス権限"](#)。

グループを表示または編集します

各グループの基本情報と詳細を表示および編集できます。


手順

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

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

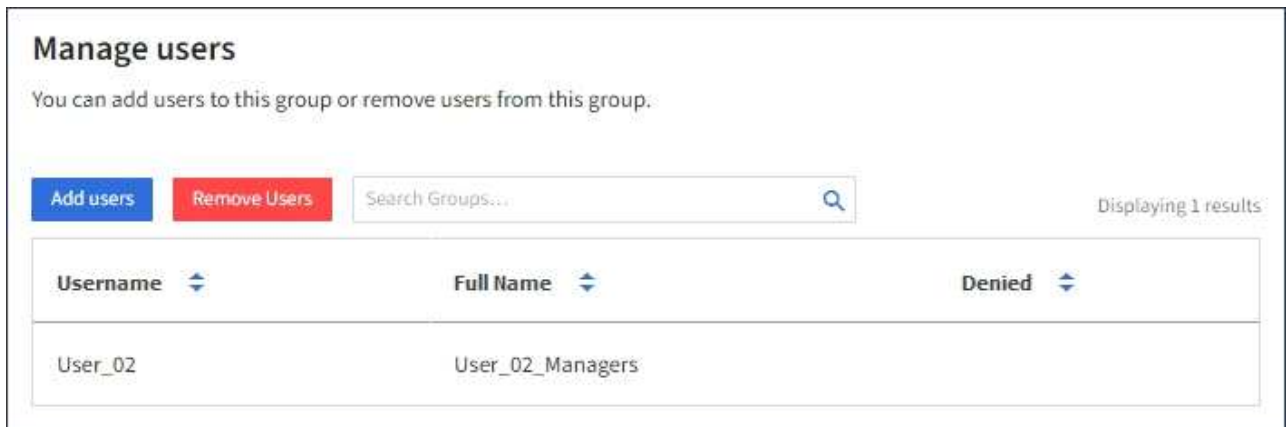
- バナーメッセージは、グループを編集または削除すると、変更内容が他のグリッドに同期されないことを示します。
 - 必要に応じて、デスティネーショングリッドでグループがテナントにクローニングされなかったかどうかを示すバナーメッセージが表示されます。可能です [グループクローンの再試行](#) 失敗した
3. グループの名前を変更する場合は、次の手順を実行します。
 - a. グループのチェックボックスをオンにします。
 - b. `>[グループ名の編集]*` を選択します。
 - c. 新しい名前を入力します。
 - d. `[変更を保存]*` を選択します
 4. 詳細を表示したり、追加の編集を行う場合は、次のいずれかを実行します。
 - グループ名を選択します。
 - グループのチェックボックスを選択し、`[操作]>[グループの詳細を表示]*` を選択します。
 5. [Overview]セクションには、グループごとに次の情報が表示されます。
 - 表示名
 - 一意の名前
 - を入力します
 - アクセスモード
 - 権限
 - S3ポリシー
 - このグループのユーザ数
 - テナントアカウントに `* Use grid federation connection *` 権限があり、テナントのソースグリッドでグループを表示している場合は、次のフィールドが追加されます。
 - クローニングステータス (`* Success` または `Failure *`)
 - このグループを編集または削除すると、変更内容が他のグリッドに同期されないことを示す青のバナーが表示されます。
 6. 必要に応じてグループ設定を編集します。を参照してください ["S3 テナント用のグループを作成します"](#)

および "Swift テナント用のグループを作成します" を参照してください。

- a. [Overview]セクションで、名前または編集アイコンを選択して表示名を変更します .
- b. [グループ権限]タブで権限を更新し、*[変更の保存]*を選択します。
- c. タブで、変更を加えて[変更の保存]*を選択します。
 - S3グループを編集する場合は、必要に応じて別のS3グループポリシーを選択するか、カスタムポリシーのJSON文字列を入力します。
 - Swiftグループを編集する場合は、必要に応じて* Swift Administrator *チェックボックスをオンまたはオフにします。

7. 既存のローカルユーザをグループに追加するには、次の手順を実行します。

- a. [Users]タブを選択します。



Username	Full Name	Denied
User_02	User_02_Managers	

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

右上に成功メッセージが表示されます。

8. グループからローカルユーザを削除するには、次の手順を実行します

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

右上に成功メッセージが表示されます。

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

グループが重複しています

既存のグループを複製して、新しいグループをより迅速に作成できます。



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

手順

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

グループクローンの再試行

失敗したクローンを再試行するには：

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

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

1つ以上のグループを削除します

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



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

手順

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

確認のダイアログボックスが表示されます。

4. または[グループの削除]*を選択します。

著作権に関する情報

Copyright © 2024 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。