



テナントアカウントを作成します

StorageGRID 11.5

NetApp
April 11, 2024

目次

テナントアカウントを作成します	1
StorageGRID がSSOを使用していない場合のテナントアカウントの作成	3
SSOが有効な場合のテナントアカウントの作成	7

テナントアカウントを作成します

StorageGRID システム内のストレージへのアクセスを制御するために、少なくとも1つのテナントアカウントを作成する必要があります。

必要なもの

- Grid 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。

手順

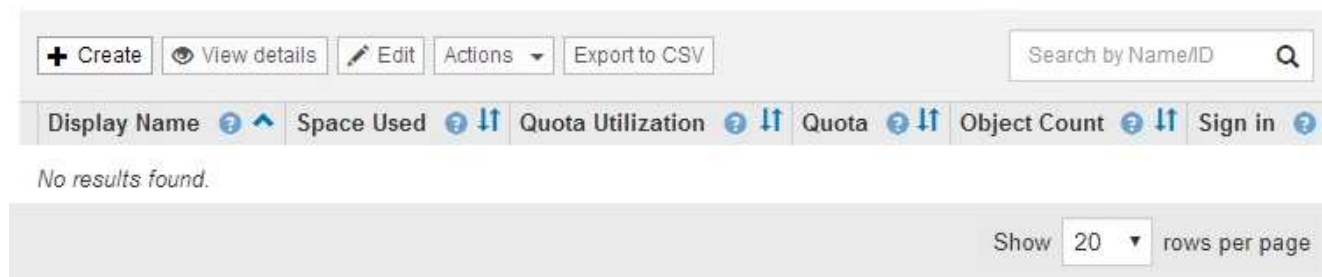
1. 「* tenants *」を選択します

Tenant Accountsページが表示され、既存のテナントアカウントの一覧が表示されます。

Tenant Accounts

View information for each tenant account.

Note: Depending on the timing of ingests, network connectivity, and node status, the usage data shown might be out of date. To view more recent values, select the tenant and select **View Details**.



The screenshot shows the 'Tenant Accounts' interface. At the top, there are several action buttons: '+ Create', 'View details', 'Edit', 'Actions', and 'Export to CSV'. To the right is a search box 'Search by Name/ID'. Below these is a table header with columns: 'Display Name', 'Space Used', 'Quota Utilization', 'Quota', 'Object Count', and 'Sign in'. The table body is empty, with the text 'No results found.' displayed. At the bottom right, there is a pagination control showing 'Show 20 rows per page'.

2. 「* Create *」を選択します。

Create Tenant Accountページが表示されます。このページに表示されるフィールドは、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かどうかによって異なります。

- SSOを使用していない場合、Create Tenant Accountページは次のようになります。

Create Tenant Account

Tenant Details

Display Name

Protocol S3 Swift

Storage Quota (optional)

Authentication [?](#)

Configure how the tenant account will be accessed.

Uses Own Identity Source

Specify a password for the tenant's local root user.

Username root

Password

Confirm Password

Cancel

Save

- SSOが有効な場合、Create Tenant Accountページは次のようになります。

Create Tenant Account

Tenant Details

Display Name

Protocol S3 Swift

Allow Platform Services

Storage Quota (optional)

Authentication

Because single sign-on is enabled, the tenant must use the Grid Manager's identity federation service, and no local users can sign in. You must select an existing federated group to have the initial Root Access permission for the tenant.

Uses Own Identity Source

Single sign-on is enabled. The tenant cannot use its own identity source.

Root Access Group

Cancel

Save

関連情報

["アイデンティティフェデレーションを使用する"](#)

["シングルサインオンを設定しています"](#)

StorageGRID がSSOを使用していない場合のテナントアカウントの作成

テナントアカウントを作成する際は、名前、クライアントプロトコル、およびオプションでストレージクォータを指定します。StorageGRID がシングルサインオン (SSO) を使用していない場合は、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どうかを指定し、テナントのローカルrootユーザの初期パスワードを設定する必要があります。

このタスクについて

Grid Manager用に設定されているアイデンティティソースをテナントアカウントで使用し、テナントアカウントにフェデレーテッドグループへのRoot Access権限を付与する場合は、そのフェデレーテッドグループをGrid Managerにインポートしておく必要があります。この管理グループに Grid Manager の権限を割り当てる必要はありません。の手順を参照してください ["管理者グループの管理"](#)。

手順

1. [表示名]テキストボックスに、このテナントアカウントの表示名を入力します。

表示名は一意である必要はありません。作成したテナントアカウントには、一意の数値アカウントIDが割り当てられます。

2. このテナントアカウントで使用するクライアントプロトコルとして、* S3 または Swift *を選択します。
3. S3テナントアカウントの場合は、このテナントでS3バケットにプラットフォームサービスを使用しないようにする場合を除き、プラットフォームサービスの許可*チェックボックスをオンのままにしておきます。

プラットフォームサービスが有効になっている場合、テナントは外部サービスにアクセスするCloudMirror レプリケーションなどの機能を使用できます。これらの機能の使用を無効にすることで、テナントが消費するネットワーク帯域幅またはその他のリソースの量を制限できます。「プラットフォームサービスの管理」を参照してください。

4. [ストレージクォータ]テキストボックスに、このテナントのオブジェクトで使用可能にする最大ギガバイト数、テラバイト数、またはペタバイト数をオプションで入力します。次に、ドロップダウンリストから単位を選択します。

このテナントのクォータを無制限にする場合は、このフィールドを空白のままにします。



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。ILMのコピーおよびイレイジャーコーディングは、クォータの使用量にはカウントされません。クォータを超過すると、テナントアカウントは新しいオブジェクトを作成できなくなります。



各テナントアカウントのストレージ使用状況を監視するには、「使用状況」を選択します。テナントアカウントは、Tenant Managerのダッシュボードまたはテナント管理APIを使用してストレージ使用状況を監視することもできます。ノードがグリッド内の他のノードから切断されていると、テナントのストレージ使用状況の値が最新ではなくなる場合があります。合計はネットワーク接続が回復すると更新されます。

5. テナントで独自のグループとユーザを管理する場合は、次の手順を実行します。
 - a. [独自のアイデンティティソースを使用する*]チェックボックスをオンにします(デフォルト)。



このチェックボックスをオンにしてテナントグループとユーザにアイデンティティフェデレーションを使用する場合、テナントが独自のアイデンティティソースを設定する必要があります。テナントアカウントを使用する手順を参照してください。

- b. テナントのローカルrootユーザのパスワードを指定します。
6. テナントがGrid Manager用に設定されたグループとユーザを使用する場合は、次の手順を実行します。
 - a. [独自のアイデンティティソースを使用する*]チェックボックスをオフにします。
 - b. 次のいずれか、または両方を実行します。
 - Root Access Groupフィールドで、テナントに対する最初のRoot Access権限を持つ既存のフェデレーテッドグループをGrid Managerから選択します。



適切な権限がある場合は、フィールドをクリックすると、Grid Managerから既存のフェデレーテッドグループが表示されます。それ以外の場合は、グループの一意の名前を入力します。

- テナントのローカルrootユーザのパスワードを指定します。

7. [保存 (Save)] をクリックします。

テナントアカウントが作成されます。

8. 必要に応じて、新しいテナントにアクセスします。それ以外の場合は、の手順に進みます [テナントへのアクセスはあとで行います](#)。

実行する作業	手順
制限されたポートでGrid Managerにアクセスします	<p>このテナントアカウントへのアクセス方法の詳細については、「* Restricted *」をクリックしてください。</p> <p>Tenant Manager の URL の形式は次のとおりです。</p> <pre>https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/</pre> <ul style="list-style-type: none">• <i>FQDN_or_Admin_Node_IP</i> は、管理ノードの完全修飾ドメイン名またはIPアドレスです• <i>port</i> は、テナント専用ポートです• <i>20-digit-account-id</i> は、テナントの一意のアカウントIDです
ポート443でGrid Managerにアクセスしているが、ローカルrootユーザのパスワードを設定していない	[サインイン]をクリックし、ルートアクセスフェデレーテッドグループにユーザのクレデンシャルを入力します。
ポート443でGrid Managerにアクセスし、ローカルrootユーザのパスワードを設定した	次の手順に進みます rootとしてサインインします 。

9. rootとしてテナントにサインインします。

- a. Configure Tenant Account (テナントアカウントの設定) ダイアログボックスで、* Sign in as root (rootとしてサインイン) ボタンをクリックします。

Configure Tenant Account

✔ Account S3 tenant created successfully.

If you are ready to configure this tenant account, sign in as the tenant's root user. Then, click the links below.

Sign in as root

- [Buckets](#) - Create and manage buckets.
- [Groups](#) - Manage user groups, and assign group permissions.
- [Users](#) - Manage local users, and assign users to groups.

Finish

緑のチェックマークがボタン上に表示されます。これは、rootユーザとしてテナントアカウントにサインインしていることを示しています。

Sign in as root ✔

a. リンクをクリックしてテナントアカウントを設定します。

各リンクをクリックすると、Tenant Manager の対応するページが開きます。このページの手順については、テナントアカウントの使用手順を参照してください。

b. [完了]をクリックします。

10. あとでテナントにアクセスするには、次の手順を実行します。

使用するポート	次のいずれかを実行 ...
ポート 443	<ul style="list-style-type: none">• Grid Managerで* tenants を選択し、テナント名の右側にある Sign In *をクリックします。• Web ブラウザにテナントの URL を入力します。 <p><code>https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/</code></p> <ul style="list-style-type: none">◦ <code>FQDN_or_Admin_Node_IP</code> は、管理ノードの完全修飾ドメイン名またはIPアドレスです◦ <code>20-digit-account-id</code> は、テナントの一意のアカウントIDです

使用するポート	次のいずれかを実行 ...
制限されたポート	<ul style="list-style-type: none"> • Grid Managerから* tenants を選択し、Restricted *をクリックします。 • Web ブラウザにテナントの URL を入力します。 <pre>https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id</pre> <ul style="list-style-type: none"> ◦ <i>FQDN_or_Admin_Node_IP</i> は、管理ノードの完全修飾ドメイン名またはIPアドレスです ◦ <i>port</i> は、テナント専用の制限付きポートです ◦ <i>20-digit-account-id</i> は、テナントの一意のアカウントIDです

関連情報

["ファイアウォールによるアクセス制御"](#)

["S3テナントアカウント用のプラットフォームサービスの管理"](#)

["テナントアカウントを使用する"](#)

SSOが有効な場合のテナントアカウントの作成

テナントアカウントを作成する際は、名前、クライアントプロトコル、およびオプションでストレージクォータを指定します。StorageGRID でシングルサインオン (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も指定します。

手順

1. [表示名]テキストボックスに、このテナントアカウントの表示名を入力します。

表示名は一意である必要はありません。作成したテナントアカウントには、一意の数値アカウントIDが割り当てられます。

2. このテナントアカウントで使用するクライアントプロトコルとして、* S3 または Swift *を選択します。
3. S3テナントアカウントの場合は、このテナントでS3バケットにプラットフォームサービスを使用しないようにする場合を除き、プラットフォームサービスの許可*チェックボックスをオンのままにしておきます。

プラットフォームサービスが有効になっている場合、テナントは外部サービスにアクセスする CloudMirror レプリケーションなどの機能を使用できます。これらの機能の使用を無効にすることで、テナントが消費するネットワーク帯域幅またはその他のリソースの量を制限できます。「プラットフォームサービスの管理」を参照してください。

4. [ストレージクォータ]テキストボックスに、このテナントのオブジェクトで使用可能にする最大ギガバイト数、テラバイト数、またはペタバイト数をオプションで入力します。次に、ドロップダウンリストから

単位を選択します。

このテナントのクォータを無制限にする場合は、このフィールドを空白のままにします。



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。ILMのコピーおよびイレイジャーコーディングは、クォータの使用量にはカウントされません。クォータを超過すると、テナントアカウントは新しいオブジェクトを作成できなくなります。



各テナントアカウントのストレージ使用状況を監視するには、「使用状況」を選択します。テナントアカウントは、Tenant Managerのダッシュボードまたはテナント管理APIを使用してストレージ使用状況を監視することもできます。ノードがグリッド内の他のノードから切断されていると、テナントのストレージ使用状況の値が最新ではなくなる場合があります。合計はネットワーク接続が回復すると更新されます。

5. [独自のアイデンティティソースを使用する*]チェックボックスがオフになっており、無効になっていることに注意してください。

SSOが有効であるため、テナントはGrid Manager用に設定されたアイデンティティソースを使用する必要があります。ローカルユーザはサインインできません。

6. [* Root Access Group]フィールドで、テナントに対する最初のRoot Access権限を持つ既存のフェデレーテッドグループをGrid Managerから選択します。



適切な権限がある場合は、フィールドをクリックすると、Grid Managerから既存のフェデレーテッドグループが表示されます。それ以外の場合は、グループの一意の名前を入力します。

7. [保存（ Save ）]をクリックします。

テナントアカウントが作成されます。Tenant Accountsページが表示され、新しいテナントの行が追加されます。

8. Root Accessグループのユーザは、必要に応じて新しいテナントの* Sign In *リンクをクリックしてTenant Managerにすぐにアクセスし、テナントを設定できます。それ以外の場合は、テナントアカウントの管理者に*サインイン*リンクのURLを提供します。（テナントのURLは、いずれかの管理ノードの完全修飾ドメイン名またはIPアドレスのあとにを追加したものです `/?accountId=20-digit-account-id.`）



テナントアカウントのRoot Accessグループに属していない場合は、* Sign In *をクリックするとアクセス拒否のメッセージが表示されます。

関連情報

["シングルサインオンを設定しています"](#)

["S3テナントアカウント用のプラットフォームサービスの管理"](#)

["テナントアカウントを使用する"](#)

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。