



テナントの管理

StorageGRID 11.5

NetApp
April 11, 2024

目次

テナントの管理	1
テナントアカウントとは	1
テナントアカウントを作成および設定する	1
S3テナントを設定する	2
Swiftテナントを設定します	2
テナントアカウントを作成します	3
テナントのローカルrootユーザのパスワードを変更する	10
テナントアカウントを編集する	12
テナントアカウントを削除する	14
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	15

テナントの管理

グリッド管理者は、S3 および Swift クライアントがオブジェクトの格納と読み出し、ストレージ使用状況の監視、および StorageGRID システムを使用してクライアントが実行できる操作の管理に使用するテナントアカウントを作成して管理します。

テナントアカウントとは

テナントアカウントは、Simple Storage Service (S3) REST API または Swift REST API を使用するクライアントアプリケーションが、StorageGRID でオブジェクトの格納や読み出しを行うことを可能にします。

各テナントアカウントで使用できるプロトコルは1つで、アカウントの作成時に指定します。両方のプロトコルを使用して StorageGRID システムにオブジェクトの格納や読み出しを行うには、テナントアカウントを2つ作成する必要があります。1つは S3 バケットとオブジェクト用、もう1つは Swift コンテナとオブジェクト用です。各テナントアカウントには、専用のアカウント ID、許可されたグループとユーザ、バケットまたはコンテナ、およびオブジェクトがあります。

必要に応じて、システムに格納されているオブジェクトをエンティティごとに分ける場合は、追加のテナントアカウントを作成します。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セットアップできます。

- * エンタープライズのユースケース：エンタープライズアプリケーションで StorageGRID システムを管理する場合は、組織内の部門ごとにグリッドのオブジェクトストレージを分離する必要があります。この場合は、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を作成できます。



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できます。テナントアカウントを使用する必要はありません。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。

- * サービスプロバイダのユースケース：サービスプロバイダとして StorageGRID システムを管理する場合は、グリッド上の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離できます。この場合は、A 社、B 社、C 社などのテナントアカウントを作成します。

テナントアカウントを作成および設定する

テナントアカウントを作成する際には次の情報を指定します。

- テナントアカウントの表示名。
- テナントアカウントで使用されるクライアントプロトコル (S3 または Swift)。
- S3 テナントアカウントの場合：テナントアカウントに S3 バケットでプラットフォームサービスを使用する権限があるかどうか。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場合は、プラットフォームサービスを使用できるようグリッドを設定する必要があります。「プラットフォームサービスの管理」を参照してください。
- 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。クォータを超過すると、テナントは新しいオブジェクトを作成できなくなります。



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。

- 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。

テナントアカウントが作成されたら、次のタスクを実行できます。

- * グリッド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でプラットフォームサービスを有効にする場合は、プラットフォームサービスメッセージの配信方法と、StorageGRID 環境でプラットフォームサービスを使用する際のネットワーク要件を理解しておく必要があります。
- * テナントアカウントのストレージ使用状況を監視 * : テナントがアカウントの使用を開始したら、Grid Manager を使用して各テナントが消費するストレージ容量を監視できます。

テナントにクォータを設定している場合は、「テナントクォータ使用率が高い *」アラートを有効にして、テナントがクォータを消費しているかどうかを確認できます。有効にすると、テナントのクォータの 90% が使用されたときにこの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。

- * クライアント処理の設定 * : 一部のタイプのクライアント処理が禁止されているかどうかを設定できません。

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、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
- S3 アクセスキーの管理
- S3 バケットの作成と管理を行う
- ストレージ使用状況を監視しています
- プラットフォームサービスの使用（有効な場合）



S3 テナントユーザは、Tenant Manager を使用して S3 アクセスキーと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みおよび管理するには S3 クライアントアプリケーション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、テナントの root 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

["テナントアカウントを使用する"](#)

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**.

Display Name Space Used Quota Utilization Quota Object Count Sign in

No results found.

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	<input type="text" value="S3 tenant (SSO enabled)"/>
Protocol	<input checked="" type="radio"/> S3 <input type="radio"/> Swift
Allow Platform Services	<input checked="" type="checkbox"/>
Storage Quota (optional)	<input type="text"/> <input type="text" value="GB"/>

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トッドグループを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"](#)

テナントのローカルrootユーザのパスワードを変更する

テナントのローカル root ユーザがアカウントからロックアウトされた場合は、 root ユー

ザのパスワード変更が必要になることがあります。

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。

このタスクについて

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 root ユーザはテナントアカウントにサインインできません。rootユーザのタスクを実行するには、テナントのRoot Access権限を持つフェデレーテッドグループにユーザが属している必要があります。

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がすべてリストされます。

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**.



	Display Name	Space Used	Quota Utilization	Quota	Object Count	Sign in
<input checked="" type="radio"/>	Account01	500.00 KB	0.00%	20.00 GB	100	
<input type="radio"/>	Account02	2.50 MB	0.01%	30.00 GB	500	
<input type="radio"/>	Account03	605.00 MB	4.03%	15.00 GB	31,000	
<input type="radio"/>	Account04	1.00 GB	10.00%	10.00 GB	200,000	
<input type="radio"/>	Account05	0 bytes	—	Unlimited	0	

2. 編集するテナントアカウントを選択します。

システムに20個を超えるアイテムが含まれている場合は、各ページに一度に表示する行数を指定できます。検索ボックスを使用して、表示名またはテナントIDでテナントアカウントを検索します。

[詳細の表示]、[編集]、[アクション]ボタンが有効になります。

3. [アクション (* Actions)]ドロップダウンから、[*ルートパスワードの変更 (Change Root Password)]を選択します。

Change Root User Password - Account03

Username	root
New Password	<input type="password" value="●●●●●●"/>
Confirm New Password	<input type="password"/>

4. テナントアカウントの新しいパスワードを入力します。
5. [保存 (Save)] を選択します。

関連情報

["StorageGRID への管理者アクセスの制御"](#)

テナントアカウントを編集する

テナントアカウントを編集して、表示名の変更、アイデンティティソース設定の変更、プラットフォームサービスの許可または禁止、ストレージクォータの入力を行うことができます。

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がすべてリストされます。

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**.

	Display Name  	Space Used  	Quota Utilization  	Quota  	Object Count  	Sign in 
<input checked="" type="radio"/>	Account01	500.00 KB	0.00%	20.00 GB	100	
<input type="radio"/>	Account02	2.50 MB	0.01%	30.00 GB	500	
<input type="radio"/>	Account03	605.00 MB	4.03%	15.00 GB	31,000	
<input type="radio"/>	Account04	1.00 GB	10.00%	10.00 GB	200,000	
<input type="radio"/>	Account05	0 bytes	—	Unlimited	0	

Show rows per page

2. 編集するテナントアカウントを選択します。

システムに20個を超えるアイテムが含まれている場合は、各ページに一度に表示する行数を指定できます。検索ボックスを使用して、表示名またはテナントIDでテナントアカウントを検索します。

3. 「* 編集 *」を選択します。

Edit Tenant Accountページが表示されます。この例は、シングルサインオン（SSO）を使用しないグリッドを対象としています。このテナントアカウントには、独自のアイデンティティソースが設定されていません。

Edit Tenant Account

Tenant Details

Display Name

Allow Platform Services

Storage Quota (optional)

Uses Own Identity Source

Cancel

Save

4. 必要に応じて、フィールドの値を変更します。
 - a. このテナントアカウントの表示名を変更します。
 - b. テナントアカウントがS3バケットにプラットフォームサービスを使用できるかどうかを確認するには、プラットフォームサービスを許可する*チェックボックスの設定を変更します。



プラットフォームサービスをすでに使用しているテナントに対してこのオプションを無効にすると、テナントがS3バケット用に設定しているサービスが停止します。エラーメッセージはテナントに送信されません。たとえば、テナントで S3 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、引き続きバケットにオブジェクトを格納できますが、エンドポイントとして設定された外部の S3 バケットにはこれらのオブジェクトのコピーが作成されなくなります。

- c. ストレージクォータ*の場合、この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、またはペタバイト数を変更します。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。



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を使用して自分の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。

- d. テナントアカウントで独自のアイデンティティソースを使用するか、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かを決定するには、* Use own Identity Source *チェックボックスの設定を変更します。



[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次の場合：

- 無効にしてオンにした場合、テナントでは独自のアイデンティティソースがすでに有効になっています。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には、テナント側で独自のアイデンティティソースを無効にする必要があります。
- StorageGRID システムで SSO が有効になっている場合は、無効にしてオフにします。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。

5. [保存 (Save)] を選択します。

関連情報

["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"](#)

テナントアカウントを削除する

システムに対するテナントのアクセス権を完全に削除する場合は、テナントアカウントを削除します。

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。

- テナントアカウントに関連付けられているすべてのバケット（S3）、コンテナ（Swift）、およびオブジェクトを削除しておく必要があります。

手順

1. 「* tenants *」を選択します
2. 削除するテナントアカウントを選択します。

システムに20個を超えるアイテムが含まれている場合は、各ページに一度に表示する行数を指定できます。検索ボックスを使用して、表示名またはテナントIDでテナントアカウントを検索します。

3. [アクション (* Actions)]ドロップダウンから、[*削除 (Remove)]を選択します。
4. 「* OK」を選択します。

関連情報

["StorageGRID への管理者アクセスの制御"](#)

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

S3 テナントアカウントでプラットフォームサービスを有効にする場合は、テナントがそのサービスの使用に必要な外部リソースにアクセスできるようにグリッドを設定する必要があります。

- ["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用のネットワークとポート"](#)
- ["サイト単位のプラットフォームサービスメッセージの配信"](#)
- ["プラットフォームサービスのトラブルシューティング"](#)

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には、CloudMirror レプリケーション、イベント通知、および検索統合サービスがあります。

これらのサービスを使用すると、テナントの S3 バケットで次の機能を使用できます。

- *** 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せんが、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。

プラットフォームサービスを使用すると、テナントで、外部ストレージリソース、通知サービス、データの検索または分析サービスを利用できるようになります。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、テナントにこれらのサービスの使用を許可するかどうかを決める必要があります。この方法を使用する場合は、テナントアカウントを作成または編集するときにプラットフォームサービスの使用を有効にする必要があります。テナントで生成されたプラットフォームサービスのメッセージが宛先に届くようにネットワークを設定する必要もあります。

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。

関連情報

["テナントアカウントを使用する"](#)

["ストレージプロキシを設定しています"](#)

["トラブルシューティングを監視します"](#)

プラットフォームサービス用のネットワークとポート

S3 テナントにプラットフォームサービスの使用を許可する場合は、プラットフォームサービスのメッセージがデスティネーションに配信されるようにグリッドのネットワークを設定する必要があります。

テナントアカウントを作成または更新する際に、S3 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できます。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、その S3 バケットからの CloudMirror レプリケーション、イベント通知、または検索統合のメッセージのデスティネーションとして機能するエンドポイントを作成できます。これらのプラットフォームサービスメッセージは、ADC サービスを実行しているストレージノードからデスティネーションエンドポイントに送信されます。

たとえば、テナントは次のタイプのデスティネーションエンドポイントを設定できます。

- ローカルでホストされる Elasticsearch クラスタ
- Simple Notification Service (SNS) メッセージの受信をサポートするローカルアプリケーション
- StorageGRID の同じインスタンス上または別のインスタンス上の、ローカルにホストされる S3 バケット
- Amazon Web Services 上のエンドポイントなどの外部エンドポイント。

プラットフォームサービスメッセージが確実に配信されるように、ADC ストレージノードが含まれるネットワークを設定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へのプラットフォームサービスメッセージの送信に、次のポートを使用できることを確認する必要があります。

デフォルトでは、プラットフォームサービスメッセージは次のポートで送信されます。

- **80** : エンドポイント URI が http で始まる場合
- **442** : https で始まるエンドポイント URI の場合

エンドポイントの作成や編集を行う際に、テナントで別のポートを指定できます。



StorageGRID 環境が CloudMirror レプリケーションのデスティネーションとして使用されている場合は、ポート 80 または 443 以外のポートにレプリケーションメッセージが送信される可能性があります。デスティネーション StorageGRID 環境で S3 に使用されているポートがエンドポイントで指定されていることを確認してください。

非透過型プロキシサーバを使用する場合は、ストレージプロキシの設定で、インターネット上のエンドポイントなどの外部エンドポイントへのメッセージの送信を許可する必要もあります。

関連情報

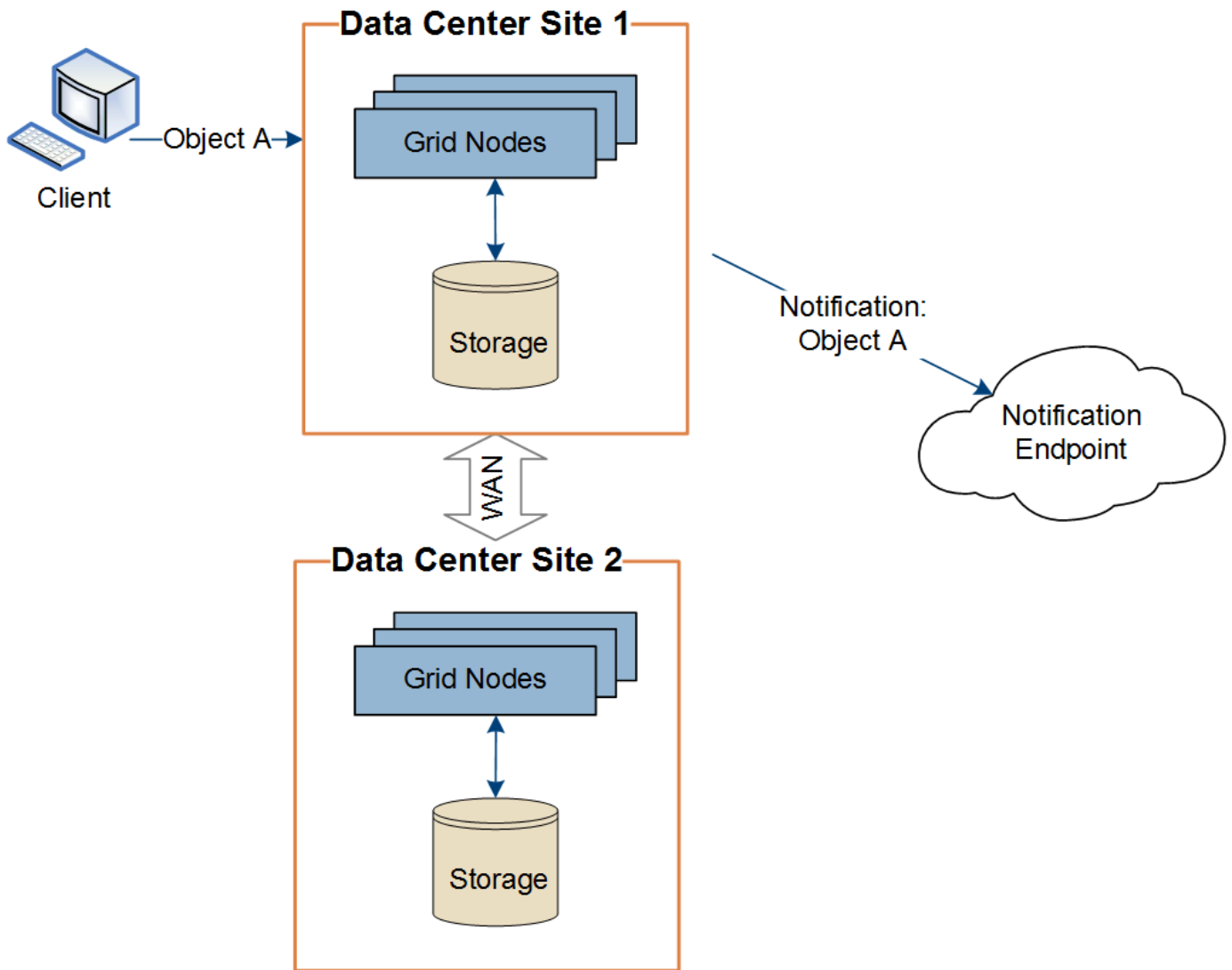
["ストレージプロキシを設定しています"](#)

["テナントアカウントを使用する"](#)

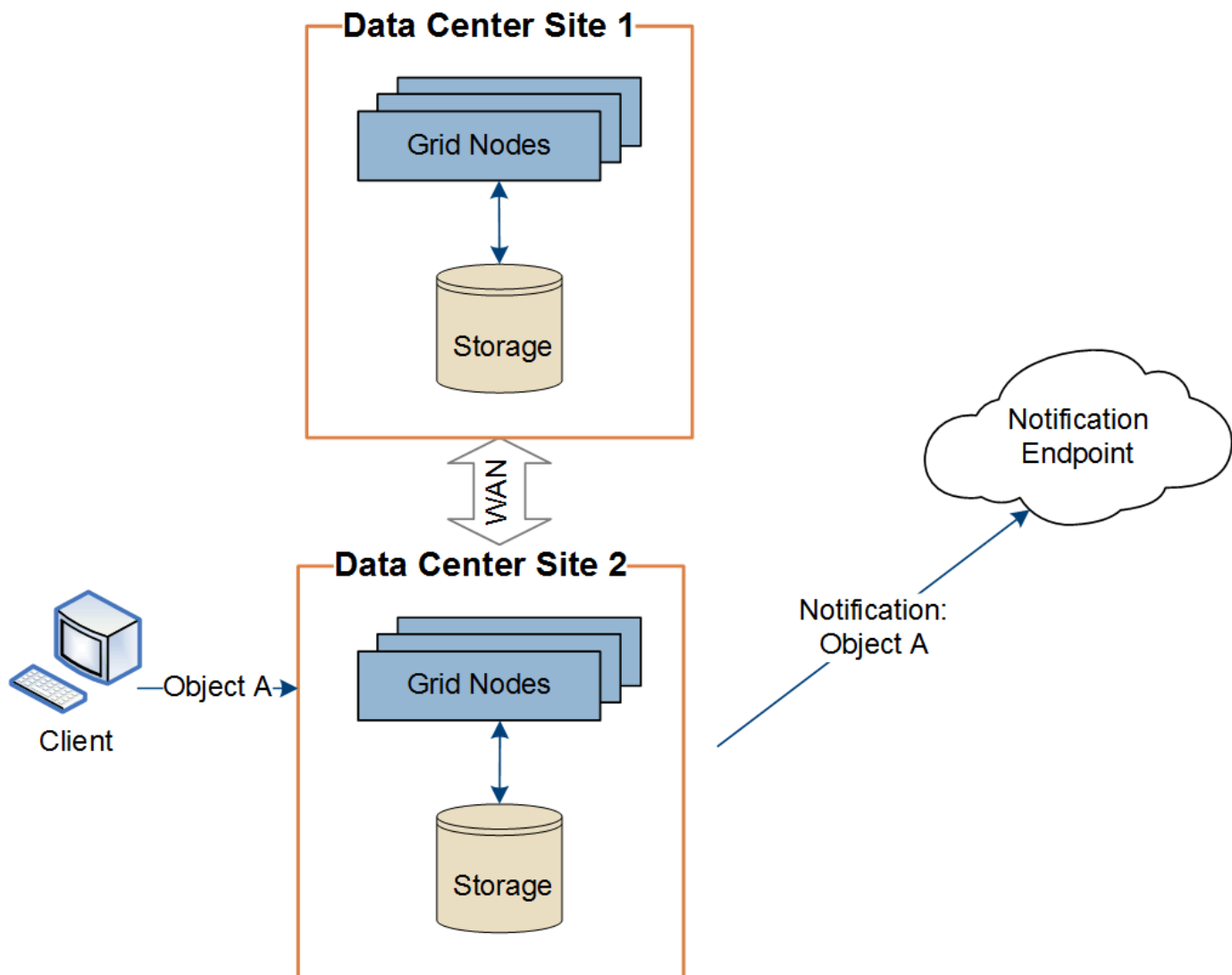
サイト単位のプラットフォームサービスメッセージの配信

プラットフォームサービスの処理はすべてサイト単位で実行されます。

つまり、テナントがクライアントを使用してデータセンターサイト 1 のゲートウェイノードに接続し、オブジェクトに対して S3 API の Create 処理を実行すると、その処理に関する通知はデータセンターサイト 1 からトリガーされて送信されます。



クライアントが続けてデータセンターサイト 2 から同じオブジェクトに対して S3 API の Delete 処理を実行すると、その処理に関する通知はデータセンターサイト 2 からトリガーされて送信されます。



プラットフォームサービスメッセージを宛先に配信できるように、各サイトのネットワークが設定されていることを確認します。

プラットフォームサービスのトラブルシューティング

プラットフォームサービスで使用されるエンドポイントは、テナントユーザが Tenant Manager で作成および管理します。ただし、テナントでプラットフォームサービスの設定または使用に関する問題がテナントで発生した場合は、グリッドマネージャを使用して問題を解決できる可能性があります。

新しいエンドポイントに関する問題

テナントでプラットフォームサービスを使用するには、Tenant Manager を使用してエンドポイントを 1 つ以上作成する必要があります。各エンドポイントは、StorageGRID S3 バケット、Amazon Web Services バケット、Simple Notification Service トピック、ローカルまたは AWS でホストされる Elasticsearch クラスタなど、1 つのプラットフォームサービスの外部のデスティネーションを表します。各エンドポイントには、外部リソースの場所と、そのリソースへのアクセスに必要なクレデンシャルが含まれます。

テナントでエンドポイントを作成すると、StorageGRID システムによって、そのエンドポイントが存在するかどうかと、指定されたクレデンシャルでアクセスできるかどうかを検証されます。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、その理由を記載したエラーメッセージが表示されます。テナントユーザは、問題を解決してから、エンドポイントの作成をもう一度実行する必要があります。



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。

既存のエンドポイントに関する問題

StorageGRID が既存のエンドポイントにアクセスしようとしたときにエラーが発生した場合は、テナントマネージャのダッシュボードにメッセージが表示されます。



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.

テナントユーザは、エンドポイントページに移動して各エンドポイントの最新のエラーメッセージを確認し、エラーが発生してからの時間を特定できます。[* Last error*] 列には、各エンドポイントの最新のエラーメッセージとエラーが発生してからの経過時間が表示されます。が含まれるエラーです アイコンは過去 7 日以内に発生しました。

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.



One or more endpoints have experienced an error. Select the endpoint for more details about the error. Meanwhile, the platform service request will be retried automatically.

5 endpoints

Create endpoint

Delete endpoint

<input type="checkbox"/>	Display name	Last error	Type	URI	URN
<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	3 days ago	Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example1
<input type="checkbox"/>	my-endpoint-5	12 days ago	Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example3
<input type="checkbox"/>	my-endpoint-4		Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example2
<input type="checkbox"/>	my-endpoint-1		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket1



「* Last error *」列の一部のエラーメッセージには、カッコ内にログ ID が含まれている場合があります。グリッド管理者やテクニカルサポートは、この ID を使用して、bypass.log のエラーに関する詳細情報を確認できます。

プロキシサーバに関連する問題

ストレージノードとプラットフォームサービスエンドポイントの間にストレージプロキシを設定している場合、プロキシサービスで StorageGRID からのメッセージが許可されていないとエラーが発生する可能性があります。これらの問題を解決するには、プロキシサーバの設定を調べて、プラットフォームサービス関連のメッセージがブロックされていないことを確認してください。

エラーが発生したかどうかを確認しています

過去 7 日間にエンドポイント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。エラーの詳細を確認するには、エンドポイントのページに移動します。

クライアント処理が失敗する

一部のプラットフォームサービスの問題により、S3 バケットに対する原因 クライアント処理が失敗することがあります。たとえば、内部の Replicated State Machine (RSM) サービスが停止した場合や、配信のためにキューに登録されたプラットフォームサービスメッセージが多すぎる場合は、S3 クライアント処理が失敗します。

サービスのステータスを確認するには、次の手順に従います。

1. Support > Tools > Grid Topology *を選択します。
2. [site >*_Storage Node>*SSM*>*Services] を選択します。

リカバリ可能なエンドポイントエラーとリカバリ不能なエンドポイントエラー

エンドポイントの作成後に、さまざまな理由からプラットフォームサービス要求のエラーが発生することがあります。一部のエラーは、ユーザが対処することでリカバリできます。たとえば、リカバリ可能なエラーは次のような原因で発生する可能性があります。

- ユーザのクレデンシャルが削除されたか、期限切れになっています。
- デスティネーションバケットが存在しません。
- 通知を配信できません。

StorageGRID でリカバリ可能なエラーが発生した場合は、成功するまでプラットフォームサービス要求が再試行されます。

その他のエラーはリカバリできません。たとえば、エンドポイントが削除されるとリカバリ不能なエラーが発生します。

StorageGRID でリカバリ不能なエンドポイントのエラーが発生すると、Grid ManagerでTotal Events (SMTT) アラームが生成されます。Total Eventsアラームを表示するには、次の手順を実行し

1. [ノード (Nodes)]を選択し
2. 「site >*_grid node_name > Events *」 を選択します。
3. 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。

4. SMTT アラームに記載されている指示に従って問題を修正します。

5. [イベントカウントのリセット]をクリックします。
6. プラットフォームサービスメッセージが配信されていないオブジェクトについてテナントに通知します。
7. テナントで、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再度トリガーするよう指定します。

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。

プラットフォームサービスメッセージを配信できません

デスティネーションでプラットフォームサービスメッセージの受信を妨げる問題が検出された場合、バケットに対する処理は成功しますが、プラットフォームサービスメッセージは配信されません。たとえば、デスティネーションでクレデンシャルが更新されたため StorageGRID がデスティネーションサービスを認証できなくなった場合に、このエラーが発生することがあります。

リカバリ不能なエラーによってプラットフォームサービスメッセージを配信できない場合は、Grid Manager で Total Events (SMTT) アラームが生成されます。

プラットフォームサービス要求のパフォーマンスが低下します

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。

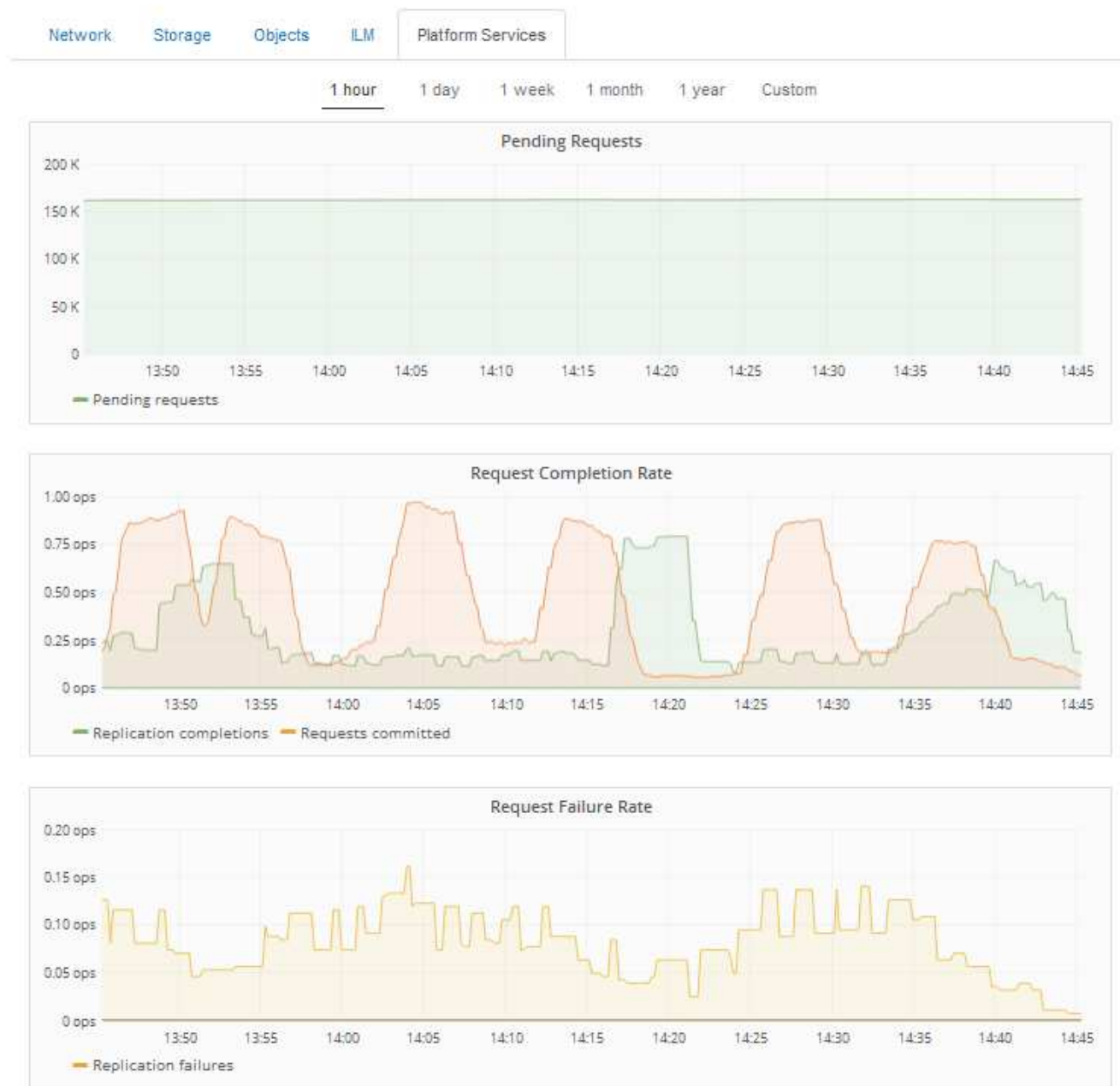
明らかな影響は、受信 S3 要求の実行時間が長くなることだけです。パフォーマンスが大幅に低下していることが検出されるようになった場合は、取り込み速度を下げるか、容量の大きいエンドポイントを使用する必要があります。要求のバックログが増え続けると、クライアント S3 処理 (PUT 要求など) が失敗します。

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。

プラットフォームサービス要求が失敗しました

プラットフォームサービスの要求の失敗率を表示するには、次の手順を実行します。

1. [ノード (Nodes)] を選択し
2. [**_site *->*Platform Services**] を選択します。
3. [障害発生率の要求] チャートを表示します。



Platform services unavailable アラート

「* Platform services unavailable *」アラートは、実行中または使用可能な RSM サービスがあるストレージノードが少なすぎるために、サイトでプラットフォームサービスの処理を実行できないことを示しています。

RSM サービスは、プラットフォームサービス要求がそれぞれのエンドポイントに確実に送信されるようにします。

このアラートを解決するには、サイトのどのストレージノードに RSM サービスが含まれているかを特定します（RSM サービスは、ADC サービスがあるストレージノードにあります）。その後、それらのストレージノードの過半数が稼働していて使用可能であることを確認します。



RSM サービスを含む複数のストレージノードでサイトで障害が発生すると、そのサイトに対する保留中のプラットフォームサービス要求はすべて失われます。

プラットフォームサービスエンドポイントに関するその他のトラブルシューティングガイダンス

プラットフォームサービスエンドポイントのトラブルシューティングに関する追加情報の詳細については、テナントアカウントの使用手順を参照してください。

["テナントアカウントを使用する"](#)

関連情報

["トラブルシューティングを監視します"](#)

["ストレージプロキシを設定しています"](#)

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権については、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。