テナントを管理します
StorageGRID 11.8

NetApp
March 19, 2024

目次

テナントを管理します

テナントの管理：概要

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に使用するテナントアカウントを作成および管理します。

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。

テナントアカウントとは

テナントアカウントでは、 Simple Storage Service （ S3 ） REST API または Swift REST API を使用して、 StorageGRID システムでオブジェクトの格納や読み出しを行うことができます。

各テナントアカウントには、フェデレーテッドグループまたはローカルグループ、ユーザ、S3バケットまたはSwiftコンテナ、およびオブジェクトがあります。

テナントアカウントを使用すると、格納されているオブジェクトをエンティティごとに分離できます。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使用できます。

- * 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。実装の手順を参照してください "S3バケットとバケットポリシー" 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。

詳細については、を参照してください "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するにはどうすればよいですか？

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。

- テナント名、クライアントタイプ（S3またはSwift）、オプションのストレージクォータなどの基本情報。
- テナントアカウントに対する権限（テナントアカウントがS3プラットフォームサービスを使用できるか、独自のアイデンティティソースを設定できるか、S3 Selectを使用できるか、グリッドフェデレーション接続を使用できるかなど）。
- テナントの初期ルートアクセス（StorageGRID システムがローカルグループとユーザ、アイデンティティフェデレーション、シングルサインオン（SSO）のいずれを使用しているかに基づく）。

また、S3テナントアカウントが規制要件に準拠する必要がある場合は、StorageGRID システムでS3オブジェクトロック設定を有効にすることができます。S3 オブジェクトのロックを有効にすると、すべての S3 テナントアカウントで準拠バケットを作成、管理できます。

Tenant Managerの用途

テナントアカウントを作成したら、テナントユーザはTenant Managerにサインインして次の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を設定する（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）
- グループとユーザを管理します
- アカウントのクローン作成とグリッド間レプリケーションにグリッドフェデレーションを使用します
- S3 アクセスキーを管理します
- S3バケットを作成、管理します
- S3プラットフォームサービスを使用する
- S3 Select を使用する
- ストレージの使用状況を監視

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、管理できますが、オブジェクトを取り込み、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。を参照してください "S3 REST APIを使用する" を参照してください。

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。

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。

テナントアカウントの作成手順は、かどうかによって異なります "アイデンティティフェデレーション" および "シングルサインオン" テナントアカウントの作成に使用する Grid Manager アカウントが、 Root アクセス権限を持つ管理者グループに属しているかどうかが設定されます。

作業を開始する前に

- を使用して Grid Manager にサインインします "サポートされている Web ブラウザ"。
- を使用することができます "rootアクセスまたはテナントアカウントの権限"。
- 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 アクセス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。この管理者グループにGrid Manager権限を割り当てる必要はありません。を参照してください "管理者グループを管理する"。

- S3テナントがグリッドフェデレーション接続を使用してアカウントデータをクローニングし、バケットオブジェクトを別のグリッドにレプリケートできるようにする場合は、次の手順を実行します。
  - これで完了です "グリッドフェデレーション接続を設定しました"。
  - 接続のステータスは*接続済み*です。
  - Root Access 権限が割り当てられている。
  - の考慮事項を確認しておきます "グリッドフェデレーションに許可されたテナントの管理"。
  - テナントアカウントが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場合は、両方のグリッドのGrid Managerに同じフェデレーテッドグループをインポートしておく必要があります。

    テナントを作成するときに、このグループを選択して、ソースとデスティネーションの両方のテナントアカウントに対する初期のRootアクセス権限を割り当てます。

> テナントを作成する前にこの管理者グループが両方のグリッドに存在していない場合、テナントはデスティネーションにレプリケートされません。

ウィザードにアクセスします

手順

1. 「 * tenants * 」を選択します
2. 「 * Create * 」を選択します。

詳細を入力します

手順

1. テナントの詳細を入力します。

フィールド	説明
名前	テナントアカウントの名前。テナント名は一意である必要はありません。作成されたテナントアカウントには、20桁の一意のアカウントIDが割り当てられます。
概要 （オプション）	テナントの特定に役立つ概要 。 グリッドフェデレーション接続を使用するテナントを作成する場合は、必要に応じて、このフィールドを使用してソーステナントとデスティネーションテナントを特定します。たとえば、Grid 1に作成されたテナントの概要は、Grid 2にレプリケートされたテナントの「This tenant was created on Grid 1」にも表示されます。
クライアントタイプ	このテナントで使用するクライアントプロトコルのタイプ（* S3 または Swift *）。 注：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。

フィールド	説明
ストレージクォータ（オプション）	このテナントにストレージクォータを設定する場合は、クォータとユニットの数値。

2. 「 * Continue * 」を選択します。

権限を選択

手順

1. 必要に応じて、このテナントに付与する権限を選択します。

これらの権限の一部には追加の要件があります。詳細については、各権限のヘルプアイコンを選択してください。

アクセス権	選択した項目
プラットフォームサービスを許可します	テナントでは、CloudMirrorなどのS3プラットフォームサービスを使用できます。を参照してください "S3 テナントアカウントのプラットフォームサービスを管理します"。
独自のアイデンティティソースを使用する	テナントでは、フェデレーテッドグループおよびフェデレーテッドユーザの独自のアイデンティティソースを設定および管理できます。がある場合、このオプションは無効になります "SSOを設定しました" をStorageGRID クリックします。
S3を許可するを選択します	テナントは、オブジェクトデータのフィルタリングと読み出しを行うためのS3 SelectObjectContent API要求を問題 できます。を参照してください "テナントアカウント用の S3 Select を管理します"。 重要：SelectObjectContent要求を実行すると、すべてのS3クライアントとすべてのテナントのロードバランサのパフォーマンスが低下する可能性があります。この機能は、必要な場合にのみ有効にし、信頼できるテナントに対してのみ有効にします。
グリッドフェデレーション接続を使用する	テナントはグリッドフェデレーション接続を使用できます。 このオプションの選択： • このテナント、およびアカウントに追加されたすべてのテナントグループとユーザが、このグリッド（*source grid*）から、選択した接続（*destination grid*）内の他のグリッドにクローニングされます。 • このテナントで、各グリッド上の対応するバケット間のグリッド間レプリケーションを設定できます。 を参照してください "グリッドフェデレーションに許可されたテナントを管理します"。

2. [Use grid federation connection]*を選択した場合は、使用可能なグリッドフェデレーション接続のいずれかを選択します。

3. 「 * Continue * 」を選択します。

ルートアクセスを定義してテナントを作成

手順

1. StorageGRID システムで使用するアイデンティティフェデレーション、シングルサインオン（SSO）、またはその両方に基づいて、テナントアカウントのルートアクセスを定義します。

オプション	手順
アイデンティティフェデレーションが有効になっていない場合	ローカルrootユーザとしてテナントにサインインするときに使用するパスワードを指定します。
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	a. テナントに対するRoot Access権限を割り当てる既存のフェデレーテッドグループを選択します。 b. 必要に応じて、ローカルrootユーザとしてテナントにサインインする際に使用するパスワードを指定します。
アイデンティティフェデレーションとシングルサインオン（SSO）の両方が有効になっている場合	テナントに対するRoot Access権限を割り当てる既存のフェデレーテッドグループを選択します。ローカルユーザはサインインできません。

2. [テナントの作成] を選択します。

   成功を示すメッセージが表示され、[Tenants]ページに新しいテナントが表示されます。テナントの詳細を表示してテナントアクティビティを監視する方法については、を参照してください "テナントのアクティビティを監視する"。

3. テナントに対して*[Use grid federation connection *]権限を選択した場合は、次の手順を実行します。

   a. 接続内のもう一方のグリッドに同一のテナントがレプリケートされたことを確認します。両方のグリッドのテナントには、同じ20桁のアカウントID、名前、概要 、クォータ、および権限が割り当てられます。

      エラーメッセージ「Tenant created without a clone」が表示される場合は、の手順を参照してください。 "グリッドフェデレーションエラーをトラブルシューティングする"。

   b. rootアクセスを定義するときにローカルrootユーザのパスワードを指定した場合は、 "ローカルrootユーザのパスワードを変更します" （レプリケートされたテナント）。

ローカルrootユーザは、パスワードが変更されるまで、デスティネーショングリッドでTenant Managerにサインインできません。

テナントへのサインイン（オプション）

必要に応じて、新しいテナントにサインインして設定を完了するか、あとでテナントにサインインできます。のサインイン手順は、Grid Managerにサインインする際にデフォルトのポート（443）を使用するか制限されたポートを使用するかによって異なります。を参照してください "外部ファイアウォールでアクセスを制御します"。

今すぐサインインしてください

使用するポート	手順
ポート443にアクセスし、ローカルrootユーザのパスワードを設定します	1. [ルートとしてサインイン]*を選択します。 サインインすると、バケット、アイデンティティフェデレーション、グループ、およびユーザを設定するためのリンクが表示されます。 2. リンクを選択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、を参照してください "テナントアカウントを使用するための手順"。
ポート443およびローカルrootユーザのパスワードを設定していない	[サインイン]*を選択し、ルートアクセスフェデレーテッドグループのユーザのクレデンシャルを入力します。
制限されたポート	1. [完了]*を選択します 2. このテナントアカウントへのアクセスの詳細を確認するには、[Tenant]テーブルで*[Restricted]*を選択します。 Tenant Manager の URL の形式は次のとおりです。 `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/` ◦ *FQDN_or_Admin_Node_IP* 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 ◦ *port* は、テナント専用ポートです ◦ *20-digit-account-id* は、テナントの一意のアカウントIDです

後でサインインします

使用するポート	次のいずれかを実行 ...
ポート443	• Grid Manager で * tenants * を選択し、テナント名の右側にある * Sign In * を選択します。 • Web ブラウザにテナントの URL を入力します。 `https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/` ◦ *FQDN_or_Admin_Node_IP* 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 ◦ *20-digit-account-id* は、テナントの一意のアカウントIDです
制限されたポート	• Grid Manager から * tenants * を選択し、 * Restricted * を選択します。 • Web ブラウザにテナントの URL を入力します。 `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id` ◦ *FQDN_or_Admin_Node_IP* 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 ◦ *port* は、テナント専用の制限付きポートです ◦ *20-digit-account-id* は、テナントの一意のアカウントIDです

テナントを設定します

の手順に従います "テナントアカウントを使用する" テナントグループとユーザ、S3アクセスキー、バケット、プラットフォームサービス、アカウントのクローニングとクロスグリッドレプリケーションを管理するため。

テナントアカウントを編集します

テナントアカウントを編集して、表示名、ストレージクォータ、またはテナント権限を変更できます。

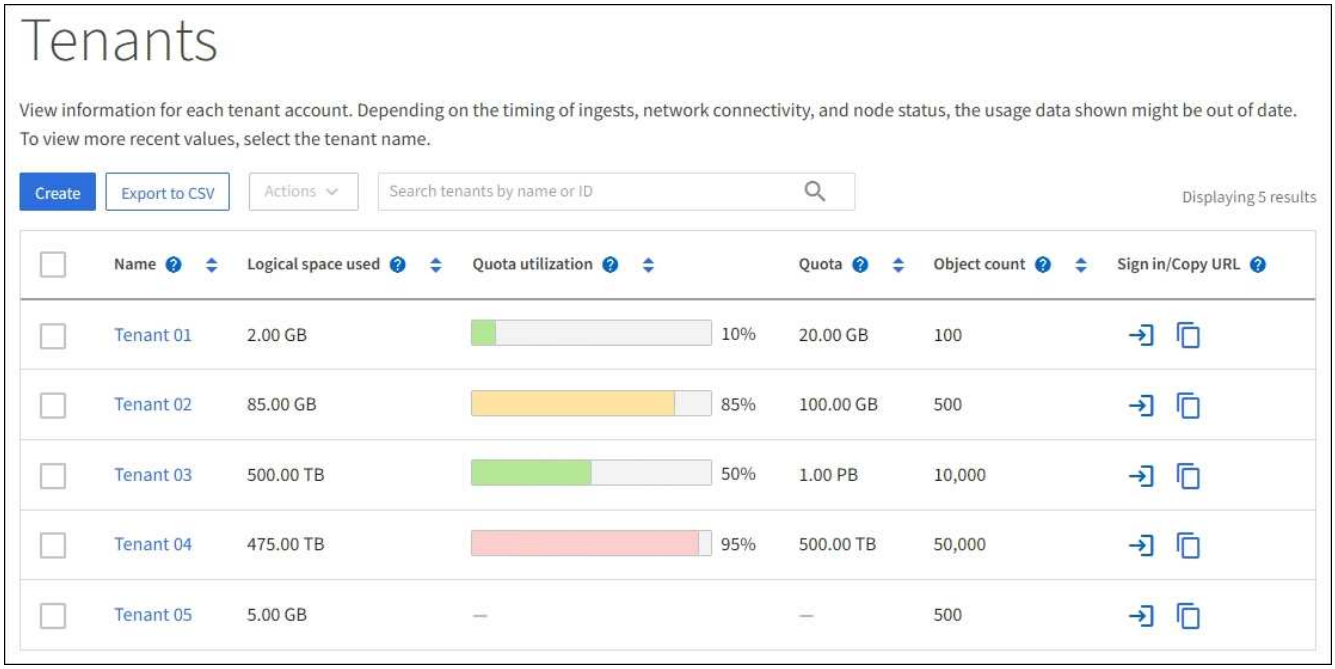
テナントに* Use grid federation connection *権限がある場合は、接続内のいずれかのグリッドからテナントの詳細を編集できます。ただし、接続内の一方のグリッドに加えた変更は、もう一方のグリッドにコピーされません。テナントの詳細をグリッド間で正確に同期させたい場合は、両方のグリッドで同じ編集を行います。を参照してください "グリッドフェデレーション接続に許可されているテナントを管理します"。

作業を開始する前に

- を使用して Grid Manager にサインインします "サポートされている Web ブラウザ"。
- を使用することができます "rootアクセスまたはテナントアカウントの権限"。

手順

1. 「 * tenants * 」を選択します



2. 編集するテナントアカウントを探します。

   検索ボックスを使用して、名前またはテナントIDでテナントを検索します。

3. テナントを選択します。次のいずれかを実行できます。
   - テナントのチェックボックスを選択し、**[操作]**>*[編集]*を選択します。
   - 詳細ページを表示するテナント名を選択し、*[編集]*を選択します。
4. 必要に応じて、次のフィールドの値を変更します。
   - * 名前 *
   - * 概要 *
   - * ストレージクォータ *
5. 「 * Continue * 」を選択します。
6. テナントアカウントの権限を選択または選択解除します。
   - すでに使用しているテナントに対して * Platform services * 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。を参照してください "S3 テナントアカウントのプラットフォームサービスを管理します"。
   - [Uses own identity source]*の設定を変更して、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指定します。

     *が独自のアイデンティティソースを使用する場合*は次のようになります。

     - [Disabled]（選択）を選択した場合、テナントで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。

- [Disabled]で選択されていない場合、StorageGRID システムでSSOが有効になっています。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。

◦ 必要に応じて、[Allow S3 Select]*権限を選択または選択解除します。を参照してください "テナントアカウント用の S3 Select を管理します"。

◦ Use grid federation connection *権限を削除するには、次の手順を実行します。

i. テナントの詳細ページに移動します。

ii. [グリッドフェデレーション]*タブを選択します。

iii. [Remove Permission]*を選択します。

◦ [Use grid federation connection]権限を追加するには、次の手順を実行します。

i. [グリッドフェデレーション接続を使用する]*チェックボックスをオンにします。

ii. 必要に応じて、*[既存のローカルユーザとローカルグループをクローニングする]*を選択してリモートグリッドにクローニングします。必要に応じて、実行中のクローニングを停止したり、前回のクローニング処理の完了後に一部のローカルユーザまたはローカルグループのクローニングに失敗した場合にクローニングを再試行したりできます。

テナントのローカル **root** ユーザのパスワードを変更します

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。

作業を開始する前に

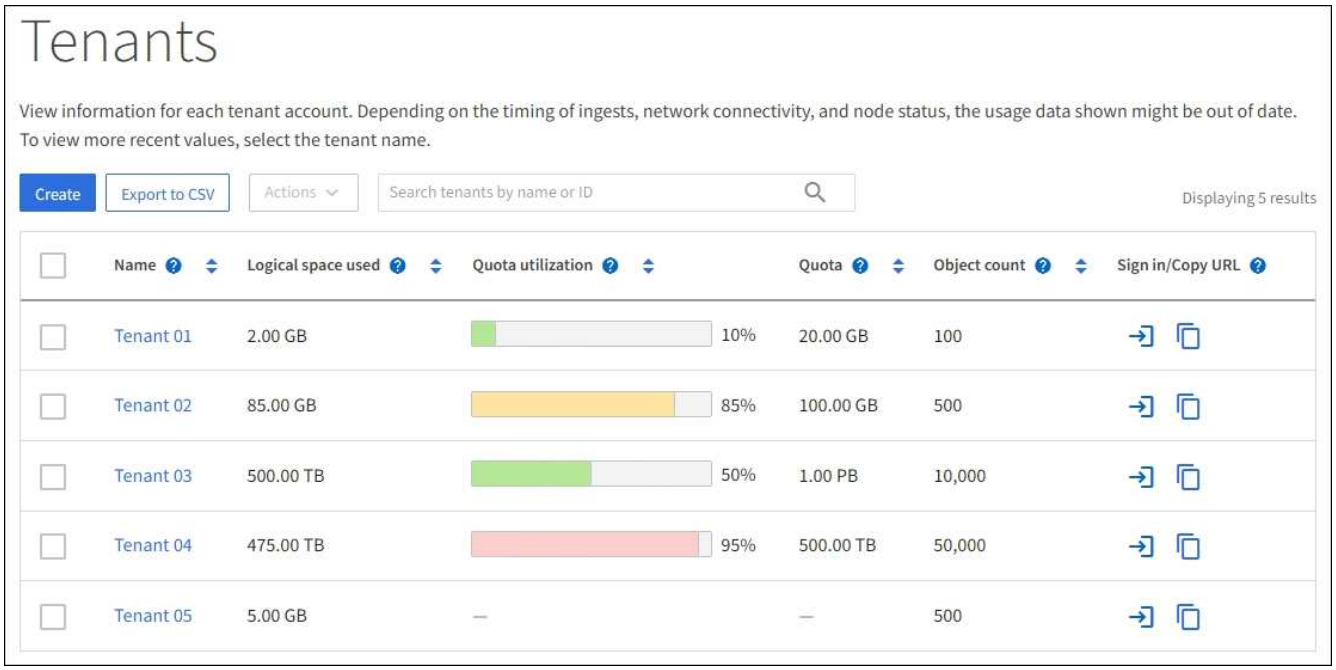
- を使用して Grid Manager にサインインします "サポートされている Web ブラウザ"。
- これで完了です "特定のアクセス権限"。

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



2. テナントアカウントを選択します。次のいずれかを実行できます。
   - テナントのチェックボックスを選択し、**[操作]>*[rootパスワードの変更]***を選択します。
   - テナントの名前を選択して詳細ページを表示し、**[操作]>*[ルートパスワードの変更]***を選択します。
3. テナントアカウントの新しいパスワードを入力します。
4. [保存（ Save ）] を選択します。

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。

作業を開始する前に

- を使用して Grid Manager にサインインします "サポートされている Web ブラウザ"。
- これで完了です "特定のアクセス権限"。
- 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きます。
- テナントにグリッドフェデレーション接続の使用が許可されている場合は、の考慮事項を確認しておきます "Use grid federation connection権限が割り当てられたテナントを削除する"。

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探します。

   検索ボックスを使用して、名前またはテナントIDでテナントを検索します。

3. 複数のテナントを削除するには、チェックボックスをオンにして**>[削除]***を選択します。

4. 単一のテナントを削除するには、次のいずれかを実行します。
   - チェックボックスを選択し、[アクション]>*[削除]*を選択します。
   - テナント名を選択して詳細ページを表示し、[操作]>*[削除]*を選択します。
5. 「 * はい * 」を選択します。

プラットフォームサービスを管理します

テナントのプラットフォームサービスの管理：概要

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。

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。

> CloudMirrorレプリケーションには、クロスグリッドレプリケーション機能と重要な類似点と相違点がいくつかあります。詳細については、を参照してください "グリッド間レプリケーションとCloudMirrorレプリケーションを比較してください"。

> 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KafkaクラスタまたはAmazon Simple Notification Service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。

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されます。

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。

- 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。
- 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。
- 完了できないエンドポイントへの要求は、最大50万件の要求にキューイングされます。この制限はアクティブなテナント間で均等に共有されます。新規テナントは、新規に作成されたテナントに不当なペナルティが課されないように、一時的にこの50万を超えることができます。

関連情報

- "プラットフォームサービスを管理します"
- "ストレージプロキシを設定します"
- "StorageGRID 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
- Amazon Simple Notification Service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
- ローカルでホストされるKafkaクラスタ
- 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**: httpで始まるエンドポイントURIの場合(ほとんどのエンドポイント)
- * 443 *：httpsで始まるエンドポイントURI（ほとんどのエンドポイント）
- *9092 *：httpまたはhttpsで始まるエンドポイントURIの場合（Kafkaエンドポイントのみ）

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、も使用する必要があります "ストレージプロキシを設定します" 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します。

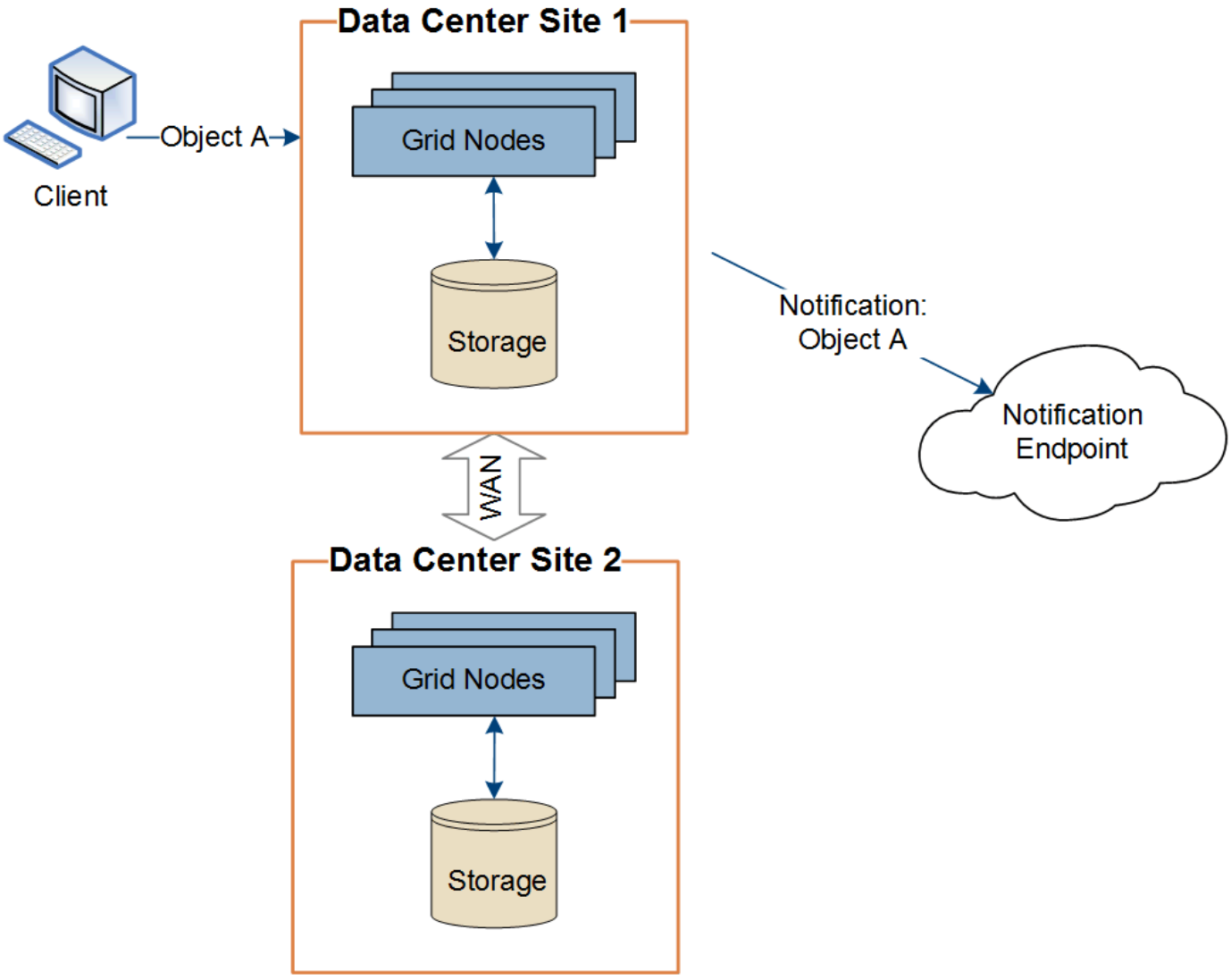
関連情報

- "テナントアカウントを使用する"

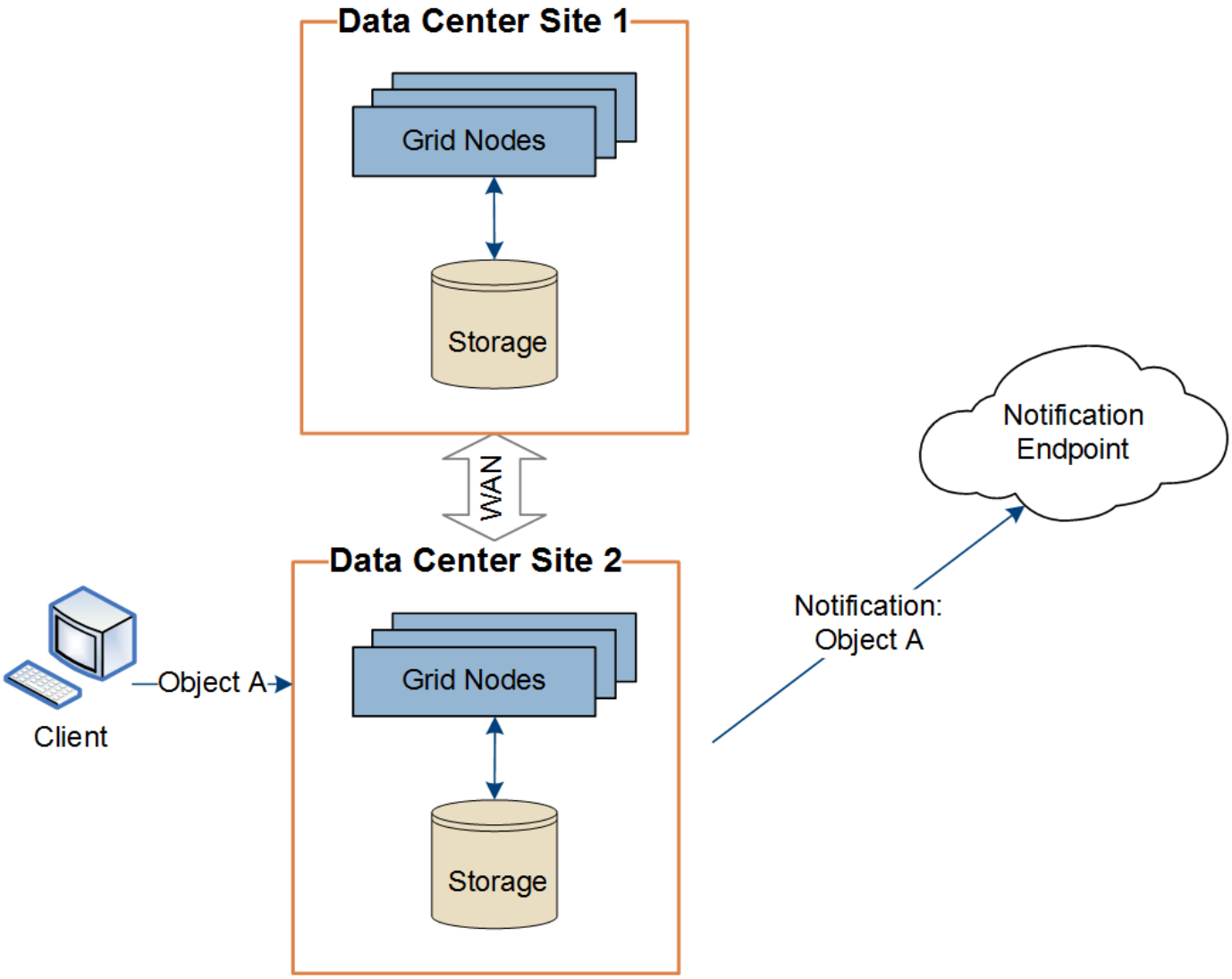
サイト単位のプラットフォームサービスメッセージの配信

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を行う

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、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（StorageGRID S3バケット、Amazon Web Servicesバケット、Amazon Simple Notification Serviceトピック、Kafka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）です。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が検証されます。エンドポイントへの接続

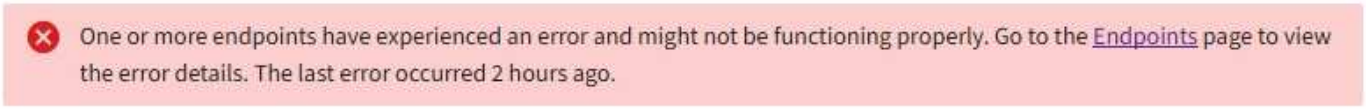
は、各サイトの 1 つのノードから検証されます。

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。

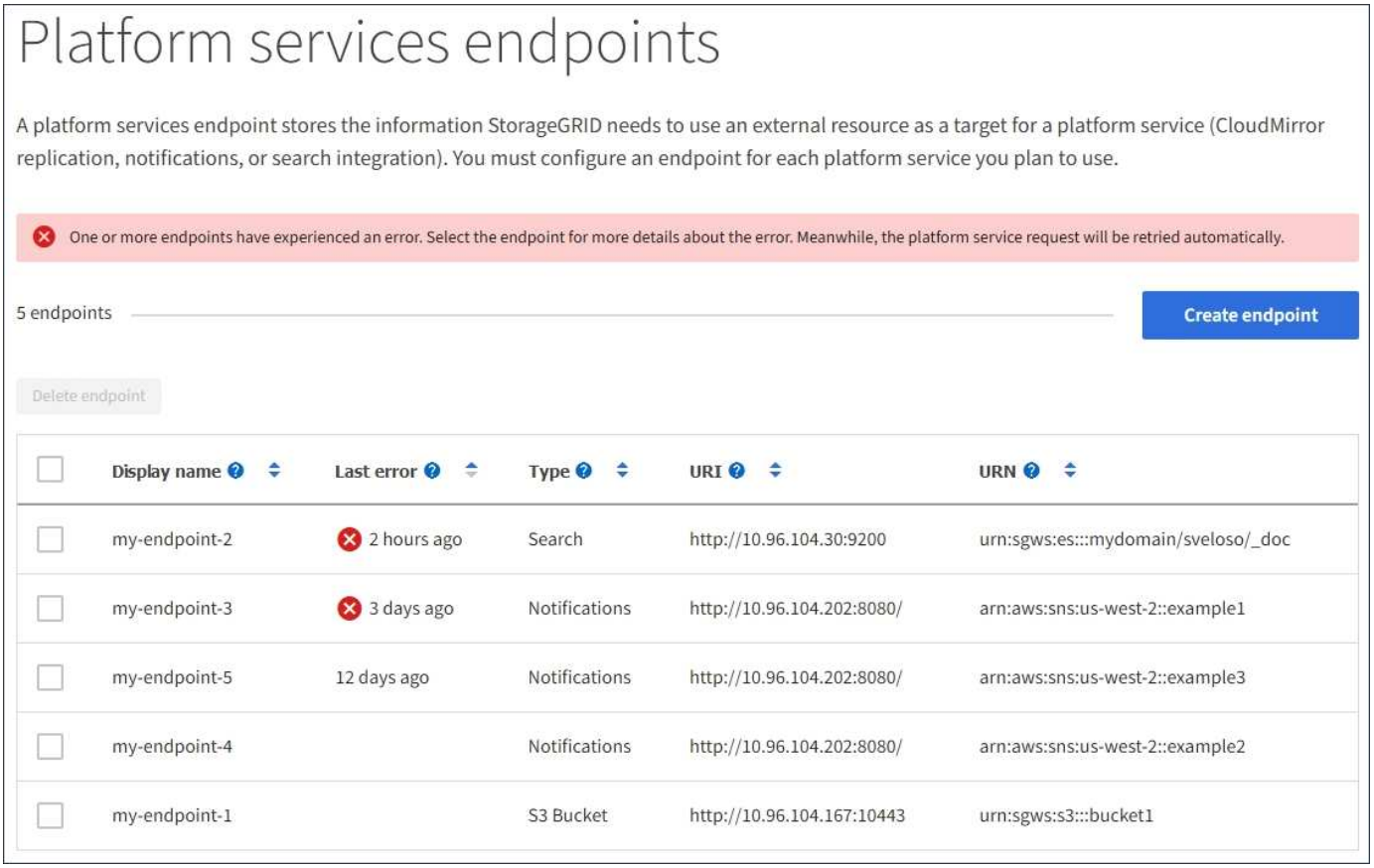
テナントアカウントでプラットフォームサービスが有効になっていないと、エンドポイントの作成が失敗します。

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すると、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。



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。



「 * Last error * 」列の一部のエラーメッセージには、かっこ内にログ 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、 bycast.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

を設定した場合 "ストレージプロキシ" 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で、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場合にエラーが発生することがあります。これらの問題を解決するには、プロキシサーバーの設定をチェックして、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ます

過去7日以内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. サポート * > * ツール * > * グリッドトポロジ * 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 ）のレガシーアラームが生成されます。Total Events レガシーアラームを表示するには、次の手順を実行します

1. サポート * > * ツール * > * グリッドトポロジ * を選択します。
2. _site * > * _node_name > * SSM * > * 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. イベントカウントをリセットするには、 * Configuration * タブを選択します。
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が原因で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、従来のTotal Events（SMTT）アラームがGrid Managerでトリガーされます。

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。

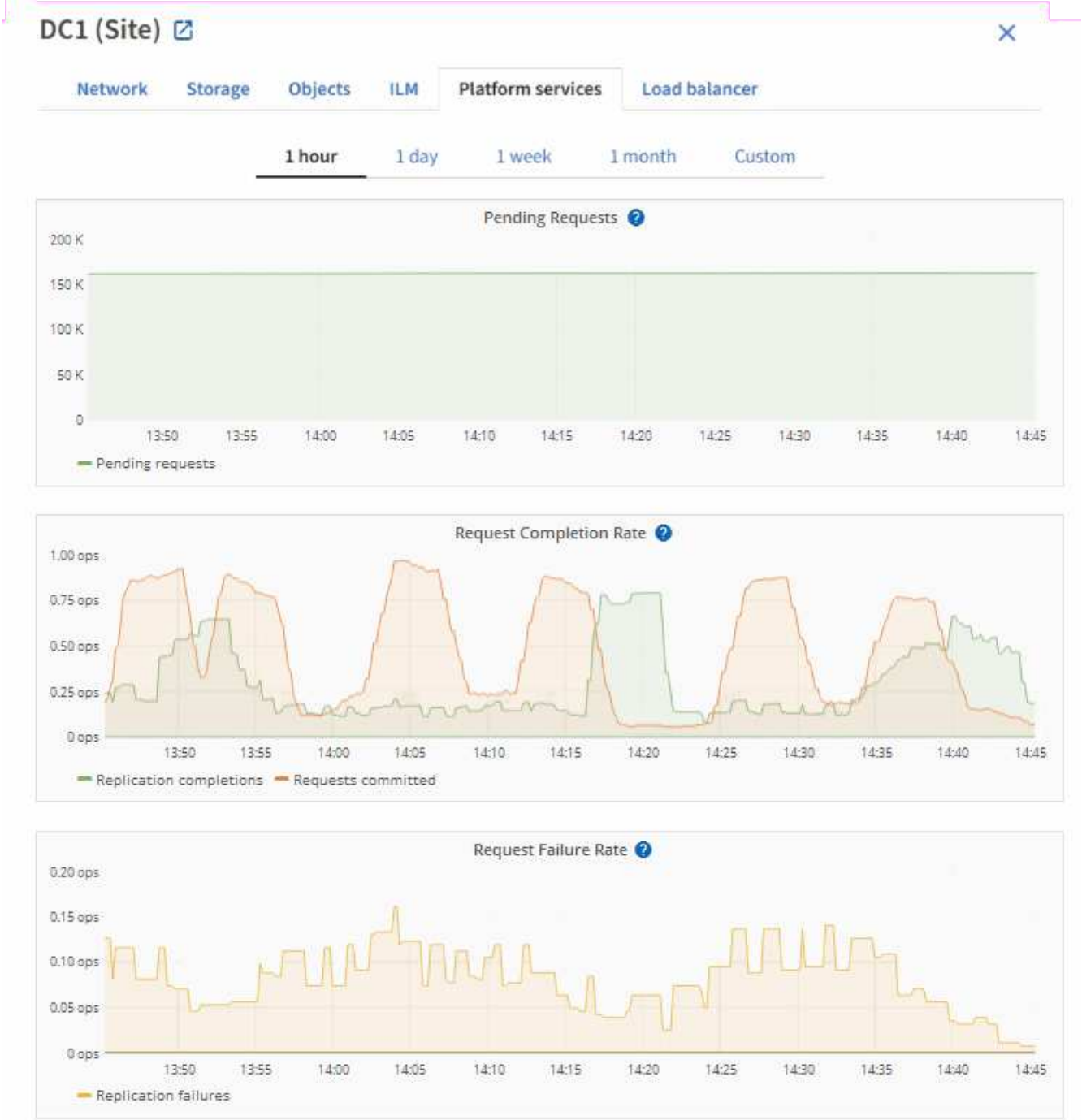
明らかな影響は、受信 S3 要求の実行時間が長くなることだけです。パフォーマンスが大幅に低下していることが検出されるようになった場合は、取り込み速度を下げるか、容量の大きいエンドポイントを使用する必要があります。要求のバックログが増え続けると、クライアント S3 処理（ PUT 要求など）が失敗します。

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. [* nodes （ノード）] を選択します
2. [**_site *>*Platform Services**] を選択します。
3. エラー率のリクエスト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）。 そのあと、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

追加情報 については'を参照してください "テナントアカウントの使用>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"。

関連情報

- "StorageGRID システムのトラブルシューティングを行う"

テナントアカウント用の S3 Select を管理します

特定の S3 テナントが、個々のオブジェクトに対する S3 Select から問題 SelectObjectContent 要求を使用できるようにすることができます。

S3 Select を使用すると、データベースや関連リソースを導入せずに大量のデータを効率的に検索できます。また、データ取得のコストとレイテンシも削減されます。

S3 Select とは何ですか。

S3 Select では、 S3 クライアントが SelectObjectContent 要求を使用して、オブジェクトから必要なデータのみをフィルタリングして読み出すことができます。S3 Select の StorageGRID 実装には、 S3 Select のコマンドと機能の一部が含まれています。

S3 Select を使用する際の考慮事項と要件

グリッド管理の要件

グリッド管理者は、テナントにS3 Select機能を許可する必要があります。Allow S3 Select * When を選択します "テナントを作成します" または "テナントの編集"。

オブジェクト形式の要件

照会するオブジェクトは、次のいずれかの形式である必要があります。

- * CSV *。そのまま使用することも、GZIPやbzip2のアーカイブに圧縮して使用することもできます。
- 寄木細工。寄木細工オブジェクトの追加要件：
  - S3 Selectでは、GZIPまたはSnappyを使用したカラムナ圧縮のみがサポートされます。S3 Selectでは、寄木細工オブジェクトのオブジェクト全体の圧縮はサポートされません。
  - S3 Selectは寄木細工の出力をサポートしていません。出力形式はCSVまたはJSONで指定する必要があります。
  - 圧縮されていない行グループの最大サイズは512MBです。
  - オブジェクトのスキーマで指定されているデータ型を使用する必要があります。
  - interval、json、list、time、またはUUID論理型は使用できません。

エンドポイントの要件

SelectObjectContent 要求は、に送信する必要があります "StorageGRID ロードバランサエンドポイント"。

エンドポイントで使用する管理ノードとゲートウェイノードは、次のいずれかである必要があります。

- SG100またはSG1000アプライアンスノード
- VMwareベースのソフトウェアノード
- cgroup v2が有効なカーネルを実行しているベアメタルノード

一般的な考慮事項

クエリをストレージノードに直接送信することはできません。

> SelectObjectContent 要求を使用すると、すべての S3 クライアントおよびすべてのテナントのロードバランサのパフォーマンスを低下させることができます。この機能は、必要な場合にのみ有効にし、信頼できるテナントに対してのみ有効にします。

を参照してください "S3 Select の使用手順"。

をクリックしてください "Grafana チャート" 一定期間にわたる S3 Select 処理の場合は、 Grid Manager で * support * > * Tools * > * Metrics * を選択します。

著作権に関する情報

商標に関する情報