テナントの管理
StorageGRID software

NetApp
December 03, 2025

目次

テナントの管理

テナント アカウントとは何ですか?

テナント アカウントを使用すると、Simple Storage Service (S3) REST API を使用して、 StorageGRIDシステム内のオブジェクトを保存および取得できます。

このバージョンのドキュメント サイトから Swift の詳細は削除されました。見る "StorageGRID 11.8: テナントの管理"。

グリッド管理者は、S3 クライアントがオブジェクトの保存と取得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。

各テナント アカウントには、フェデレーション グループまたはローカル グループ、ユーザー、S3 バケット、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、保存されたオブジェクトを異なるエンティティごとに分離できます。たとえば、次のいずれかの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使用例: エンタープライズ アプリケーションでStorageGRIDシステムを管理している場合、組織内のさまざまな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る場合があります。この場合、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、企業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。実装手順を参照"S3 バケットとバケットポリシー"詳細についてはこちらをご覧ください。

- サービス プロバイダーの使用例: StorageGRIDシステムをサービス プロバイダーとして管理している場合は、グリッドのオブジェクト ストレージを、グリッド上でストレージをリースするさまざまなエンティティごとに分離できます。この場合、会社 A、会社 B、会社 C 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、以下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?

グリッド マネージャーを使用してテナント アカウントを作成します。テナント アカウントを作成するときは、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)、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 アカウントの権限 (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どうか、独自の ID ソースを設定できるかどうか、S3 Select を使用できるかどうか、グリッド フェデレーション接続を使用できるかどうかなど)。
- StorageGRIDシステムがローカル グループとユーザー、ID フェデレーション、またはシングル サインオン (SSO) を使用するかどうかに基づく、テナントの初期ルート アクセス。

さらに、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システムの S3 オブ

ジェクト ロック設定を有効にできます。 S3 オブジェクト ロックを有効にすると、すべての S3 テナント アカウントが準拠バケットを作成および管理できるようになります。

Tenant Manager は何に使用されますか?

テナント アカウントを作成すると、テナント ユーザーはテナント マネージャーにサインイン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 フェデレーションを設定する (アイデンティティ ソースがグリッドと共有されていない場合)
- グループとユーザーの管理
- アカウントのクローンとクロスグリッドレプリケーションにグリッドフェデレーションを使用する
- S3 アクセスキーを管理する
- S3バケットの作成と管理
- 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
- ストレージ使用量を監視する

S3 テナント ユーザーは、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、オブジェクトの取り込みと管理には 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。見る"S3 REST APIを使用する"詳細については。

テナントアカウントを作成する

StorageGRIDシステム内のストレージへのアクセスを制御するには、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を作成する手順は、"アイデンティティフェデレーション"そして"シングルサインオン"が構成されているかどうか、およびテナント アカウントの作成に使用する Grid Manager アカウントが、ルート 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を確認します。

開始する前に

- グリッドマネージャにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは"ルートアクセスまたはテナントアカウントの権限"。
- テナント アカウントが Grid Manager 用に構成されたアイデンティティ ソースを使用し、テナント アカウントのルート アクセス権限をフェデレーション グループに付与する場合は、そのフェデレーション グループを Grid Manager にインポートしておきます。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。見る"管理者グループの管理" 。
- 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 データを複製し、バケット オブジェクトを別のグリッドに複製できるようにする場合:
  - あなたが持っている"グリッドフェデレーション接続を構成しました"。
  - 接続のステータスは*接続済み*です。
  - ルートアクセス権限があります。

- 検討事項を確認しました"グリッドフェデレーションの許可されたテナントの管理"。
- テナント アカウントが Grid Manager 用に構成された ID ソースを使用する場合は、両方のグリッドの Grid Manager に同じフェデレーション グループをインポートしたことになります。

  テナントを作成するときに、ソース テナント アカウントと宛先テナント アカウントの両方に対する初期のルート アクセス権限を付与するこのグループを選択します。

> テナントを作成する前にこの管理グループが両方のグリッドに存在しない場合、テナントは宛先に複製されません。

ウィザードにアクセスする

手順

1. *TENANTS*を選択します。
2. *作成*を選択します。

詳細を入力してください

手順

1. テナントの詳細を入力します。

フィールド	説明
Name	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。テナント アカウントが作成されると、一意の 20 桁のアカウント ID が割り当てられます。
説明（オプション）	テナントを識別するのに役立つ説明。 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、オプションでこのフィールドを使用して、ソース テナントと宛先テナントを識別します。たとえば、グリッド 1 で作成されたテナントのこの説明は、グリッド 2 に複製されたテナントにも表示されます:「このテナントはグリッド 1 で作成されました。」
クライアントタイプ	このテナントが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非推奨となっており、将来のリリースでは削除される予定です。
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、クォータの数値と単位を指定します。

2. *続行*を選択します。

権限の選択

手順

1. 必要に応じて、このテナントに付与する基本的な権限を選択します。

   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。

許可	選択した場合...
プラットフォームサービスを許可する	テナントは CloudMirror などの S3 プラットフォーム サービスを使用できます。見る"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する" 。
独自のIDソースを使用する	テナントは、フェデレーション グループおよびユーザーに対して独自の ID ソースを構成および管理できます。このオプションは、"設定されたSSO" StorageGRIDシステム用。
S3 選択を許可する	テナントは、S3 SelectObjectContent API リクエストを発行して、オブジェクト データをフィルタリングおよび取得できます。見る"テナントアカウントのS3 Selectを管理する" 。 重要: SelectObjectContent リクエストにより、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ー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、信頼できるテナントに対してのみ有効にしてください。

2. 必要に応じて、このテナントに付与する高度な権限を選択します。

許可	選択した場合...
グリッドフェデレーション接続	テナントは、次の機能を備えたグリッド フェデレーション接続を使用できます。 • このテナントと、アカウントに追加されたすべてのテナント グループおよびユーザーが、このグリッド (ソース グリッド) から選択した接続内の他のグリッド (宛先グリッド) に複製されます。 • このテナントが各グリッド上の対応するバケット間でクロスグリッド レプリケーションを構成できるようにします。 見る"グリッドフェデレーションの許可されたテナントを管理する" 。
S3 オブジェクトロック	テナントが S3 オブジェクトロックの特定の機能を使用できるようにします。 • 最大保持期間の設定 は、このバケットに追加された新しいオブジェクトが取り込まれた時点から保持される期間を定義します。 • コンプライアンス モードを許可する により、ユーザーは保持期間中に保護されたオブジェクトのバージョンを上書きまたは削除できなくなります。

3. *続行*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する

手順

1. StorageGRIDシステムが ID フェデレーション、シングル サインオン (SSO)、またはその両方を使用するかどうかに基づいて、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	これをする
アイデンティティ連携が有効になっていない場合	ローカル ルート ユーザー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。
アイデンティティ連携が有効になっている場合	a. テナントのルート アクセス権限を付与する既存のフェデレーション グループを選択します。 b. 必要に応じて、ローカル ルート ユーザー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。
ID連携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	テナントのルート アクセス権限を付与する既存のフェデレーション グループを選択します。ローカル ユーザー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。

   成功メッセージが表示され、新しいテナントが [テナント] ページに表示されます。テナントの詳細を表示し、テナントのアクティビティを監視する方法については、以下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" 。

   > グリッド全体にテナント設定を適用するには、ネットワーク接続、ノードのステータス、Cassandra の操作によっては 15 分以上かかる場合があります。

3. テナントに対して*グリッド フェデレーション接続を使用する*権限を選択した場合:

   a. 接続内の他のグリッドに同一のテナントが複製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、説明、クォータ、および権限が与えられます。

      > 「クローンなしでテナントが作成されました」というエラーメッセージが表示された場合は、"グリッドフェデレーションエラーのトラブルシューティング" 。

   b. ルートアクセスを定義する際にローカルルートユーザーのパスワードを指定した場合、"ローカルルートユーザーのパスワードを変更する"複製されたテナント用。

      > パスワードが変更されるまで、ローカル ルート ユーザーは、宛先グリッド上の Tenant Manager にサインインできません。

テナントに**Sign in**（オプション）

必要に応じて、今すぐ新しいテナントにサインインして構成を完了することも、後でテナントにサインインす

ることもできます。サインインの手順は、デフォルト ポート (443) を使用して Grid Manager にサインインしているか、制限されたポートを使用してサインインしているかによって異なります。見る"外部ファイアウォールでアクセスを制御する" 。

今すぐ**Sign in**

...を使用している場合	操作
ポート443でローカルルートユーザーのパスワードを設定する	1. * root としてSign in* を選択します。 サインインすると、バケット、ID フェデレーション、グループ、およびユーザーを構成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 アカウントを構成します。 各リンクをクリックすると、テナント マネージャーの対応するページが開きます。ページを完了するには、"テナントアカウントの使用手順" 。
ポート443で、ローカルルートユーザーのパスワードを設定していない	*Sign in*を選択し、ルートアクセスフェデレーショングループのユーザーの資格情報を入力します。
制限されたポート	1. *完了*を選択 2. 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、テナント テーブルで 制限 を選択してください。 テナント マネージャーの 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`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`テナント専用ポートです ◦ `20-digit-account-id`テナントの一意のアカウントIDです

後で**Sign in**

...を使用している場合	これらのいずれかを行ってください...
ポート443	• グリッド マネージャーから [**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`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`テナントの一意のアカウントIDです
制限されたポート	• グリッド マネージャーから、**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`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`テナント専用の制限ポートです ◦ `20-digit-account-id`テナントの一意のアカウントIDです

テナントを構成する

以下の指示に従ってください"テナントアカウントを使用する"テナント グループとユーザー、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 クローン、クロス グリッド レプリケーションを管理します。

テナントアカウントの編集

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 グリッド フェデレーション接続の使用 権限がある場合は、接続内のどちらのグリッドからでもテナントの詳細を編集できます。ただし、接続内の 1 つのグリッドで行った変更は、他のグリッドにコピーされません。グリッド間でテナントの詳細を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。見る"グリッドフェデレーション接続に許可されたテナントを管理する" 。

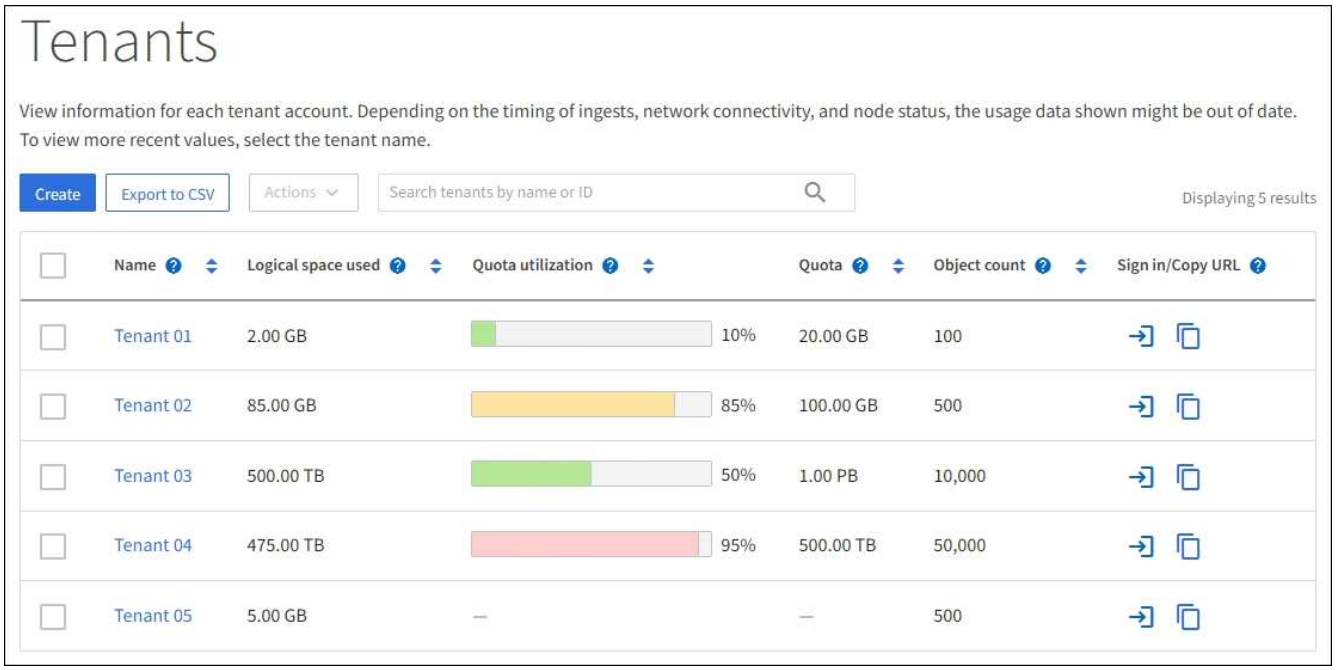
開始する前に

- グリッドマネージャにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは"ルートアクセスまたはテナントアカウントの権限"。

グリッド全体にテナント設定を適用するには、ネットワーク接続、ノードのステータス、Cassandra の操作によっては 15 分以上かかる場合があります。

手順

1. *TENANTS*を選択します。



2. 編集するテナント アカウントを見つけます。

   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、[アクション] > [編集] 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、[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
   - 説明
   - ストレージクォータ
5. *続行*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クリアします。
   - すでにプラットフォーム サービスを使用しているテナントに対して プラットフォーム サービス を無効にすると、S3 バケット用に設定されているサービスは動作しなくなります。テナントにエラー メッセージは送信されません。たとえば、テナントが S3 バケットの CloudMirror レプリケーションを設定している場合、バケット内にオブジェクトを引き続き保存できますが、エンドポイントとして設定した外部 S3 バケットにはそれらのオブジェクトのコピーは作成されなくなります。見る"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する" 。
   - 独自の **ID** ソースを使用する の設定を変更して、テナント アカウントが独自の ID ソースを使用するか、グリッド マネージャー用に構成された ID ソースを使用するかを決定します。

独自の **ID** ソースを使用する の場合:

- 無効になっていて選択されている場合、テナントは独自の ID ソースをすでに有効にしています。テナントは、グリッド マネージャー用に構成された ID ソースを使用する前に、その ID ソースを無効にする必要があります。
- 無効で選択されていない場合、 StorageGRIDシステムに対して SSO が有効になります。テナントは、グリッド マネージャー用に構成された ID ソースを使用する必要があります。

◦ 必要に応じて、「**S3** 選択を許可する」権限を選択またはクリアします。見る"テナントアカウントのS3 Selectを管理する" 。

◦ グリッド フェデレーション接続の使用 権限を削除するには:

i. グリッド フェデレーション タブを選択します。

ii. *権限を削除*を選択します。

◦ グリッド フェデレーション接続の使用 権限を追加するには:

i. グリッド フェデレーション タブを選択します。

ii. 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選択します。

iii. 必要に応じて、「既存のローカル ユーザーとグループの複製」を選択して、リモート グリッドに複製します。必要に応じて、進行中のクローン作成を停止したり、最後のクローン作成操作が完了した後に一部のローカル ユーザーまたはグループのクローン作成に失敗した場合にクローン作成を再試行したりできます。

◦ 最大保持期間を設定するか、コンプライアンス モードを許可するには:

> これらの設定を使用する前に、グリッドで S3 オブジェクト ロックを有効にする必要があります。

i. **S3** オブジェクト ロック タブを選択します。

ii. *最大保存期間の設定*では、値を入力し、プルダウンから期間を選択します。

iii. コンプライアンス モードを許可する のチェックボックスをオンにします。

テナントのローカルルートユーザーのパスワードを変更する

ルート ユーザーがアカウントからロックアウトされている場合は、テナントのローカル ルート ユーザーのパスワードを変更する必要がある場合があります。

開始する前に

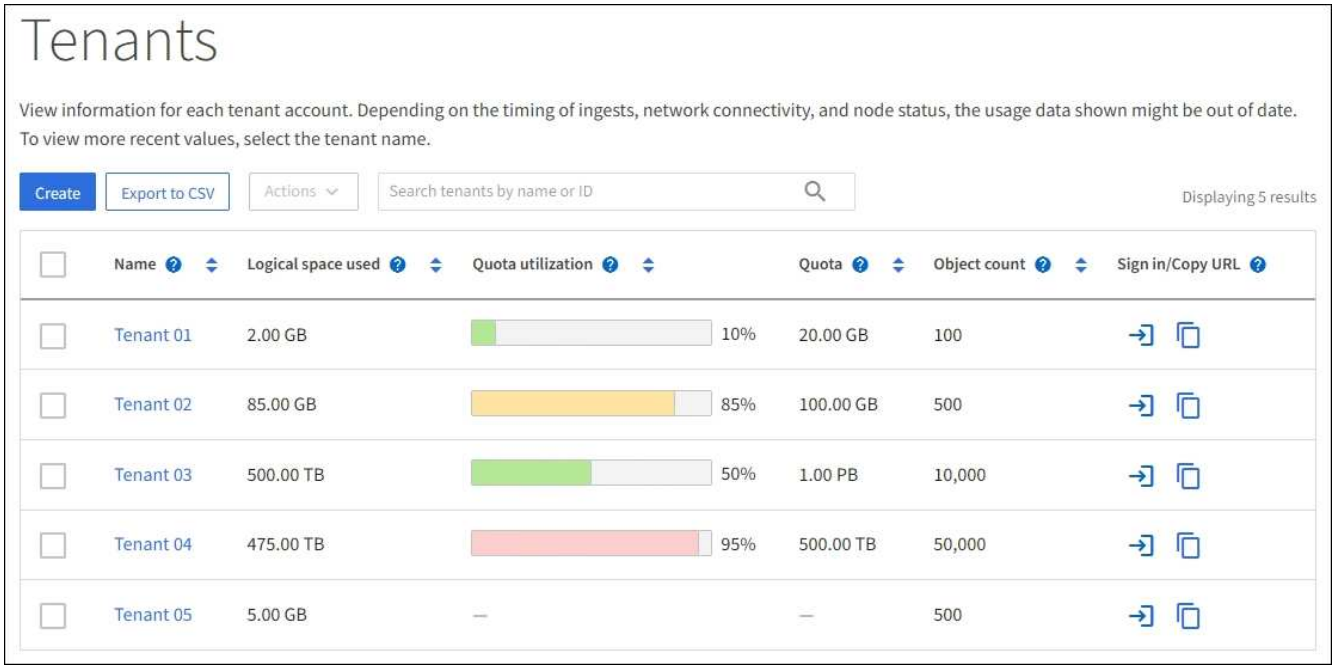
- グリッドマネージャにサインインするには、"サポートされているウェブブラウザ" 。
- あなたが持っている"特定のアクセス権限"。

タスク概要

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 ルート ユーザーはテナント アカウントにサインインできません。ルート ユーザー タスクを実行するには、ユーザーはテナントに対するルート アクセス権限を持つフェデレーション グループに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、アクション > *ルートパスワードの変更*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、アクション > 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*を選択します。

テナントアカウントを削除する

テナントのシステムへのアクセスを完全に削除する場合は、テナント アカウントを削除できます。

開始する前に

- グリッドマネージャにサインインするには、"サポートされているウェブブラウザ" 。
- あなたが持っている"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 S3 バケットとオブジェクトが削除されました。
- テナントがグリッドフェデレーション接続の使用を許可されている場合は、以下の考慮事項を確認しました。"グリッドフェデレーション接続の使用権限を持つ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 アカウントを見つけます。

   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、[アクション] > [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、[アクション] > [削除] を選択します。
5. *はい*を選択してください。

プラットフォームサービスの管理

プラットフォームサービスとは何ですか?

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、検索統合サービスが含まれます。

S3 テナント アカウントに対してプラットフォーム サービスを有効にする場合は、テナントがこれらのサービスを使用するため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構成する必要があります。

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宛先に特定のオブジェクトをミラーリングするために使用されます。

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 サービスを活用してデータの分析を実行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の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、"クロスグリッドレプリケーションとCloudMirrorレプリケーションを比較する" 。

ソースバケットで S3 オブジェクトロックが有効になっている場合、CloudMirror レプリケーションはサポートされません。

通知

バケットごとのイベント通知は、オブジェクトに対して実行された特定のアクションに関する通知を、指定された外部 Kafka クラスターまたは Amazon Simple Notification Service に送信するために使用されます。

たとえば、バケットに追加された各オブジェクト（重要なシステム イベントに関連付けられたログ ファイルを表すオブジェクト）に関するアラートを管理者に送信するように設定できます。

S3 オブジェクト 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 (保持期限や法的保留ステータスを含む) 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、S3 オブジェクト メタデータを指定された Elasticsearch インデックスに送信するために使用され、そこでメタデータは外部サービスを使用して検索または分析できます。

たとえば、S3 オブジェクトのメタデータをリモート Elasticsearch サービスに送信するようにバケットを設定できます。その後、Elasticsearch を使用してバケット全体の検索を実行し、オブジェクト メタデータに存在するパターンの高度な分析を実行できます。

> S3 オブジェクト ロックが有効になっているバケットで 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 (保持期限や法的保留ステータスを含む) は通知メッセージに含まれません。

プラットフォーム サービスにより、テナントは外部ストレージ リソース、通知サービス、およびデータを使用した検索や分析サービスを使用できるようになります。プラットフォーム サービスのターゲットの場所は通常、 StorageGRID展開の外部にあるため、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定する必要があります。その場合は、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。また、テナントが生成するプラットフォーム サービス メッセージが宛先に届くようにネットワークを構成する必要があります。

プラットフォームサービスの利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、次の推奨事項に注意してください。

- StorageGRIDシステム内の 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、宛先エンドポイントの S3 バケットのバージョン管理も有効にする必要があります。これにより、CloudMirror レプリケーションはエンドポイントで同様のオブジェクト バージョンを生成できるようになります。
- CloudMirror レプリケーション、通知、および検索統合を必要とする S3 リクエストでは、100 を超えるアクティブテナントを使用しないでください。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リクエストは、最大 500,000 件のリクエストまでキューに入れられます。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。新しく作成されたテナントが不当に罰せられないように、新しいテナントはこの 500,000 の制限を一時的に超えることが許可されます。

関連情報

- "プラットフォームサービスの管理"
- "ストレージプロキシ設定を構成する"
- "StorageGRIDを監視する"

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 メッセージが宛先に配信されるようにグリッドのネットワークを構成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ときに、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、S3 バケットからの CloudMirror レプリケーション、イベント通知、または検索統合メッセージの送信先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 サービスを実行するストレージ ノードから宛先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宛先エンドポイントを構成する場合があります。

- ローカルにホストされたElasticsearchクラスター
- 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
- ローカルにホストされた Kafka クラスター
- StorageGRIDの同じインスタンスまたは別のインスタンス上のローカルにホストされた 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するには、ADC ストレージ ノードを含むネットワークを構成する必要があります。プラットフォーム サービス メッセージを宛先エンドポイントに送信するには、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（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)

テナントは、エンドポイントを作成または編集するときに別のポートを指定できます。

> StorageGRIDデプロイメントを CloudMirror レプリケーションの宛先として使用すると、レプリケーション メッセージが 80 または 443 以外のポートで受信される可能性があります。宛先StorageGRIDデプロイメントによって 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ます。

非透過プロキシサーバーを使用する場合は、"ストレージプロキシ設定を構成する"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にメッセージを送信できるようにします。

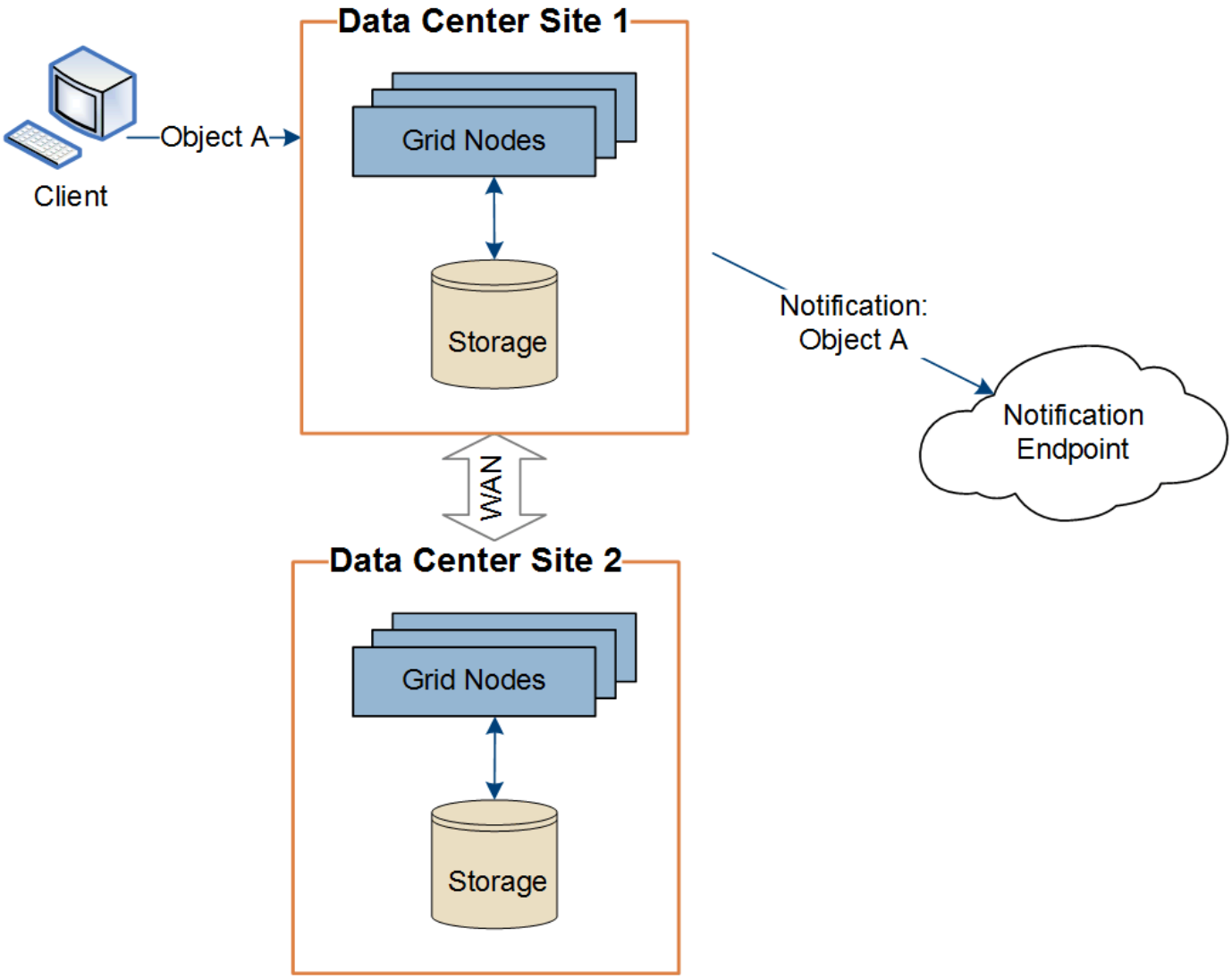
関連情報

"テナントアカウントを使用する"

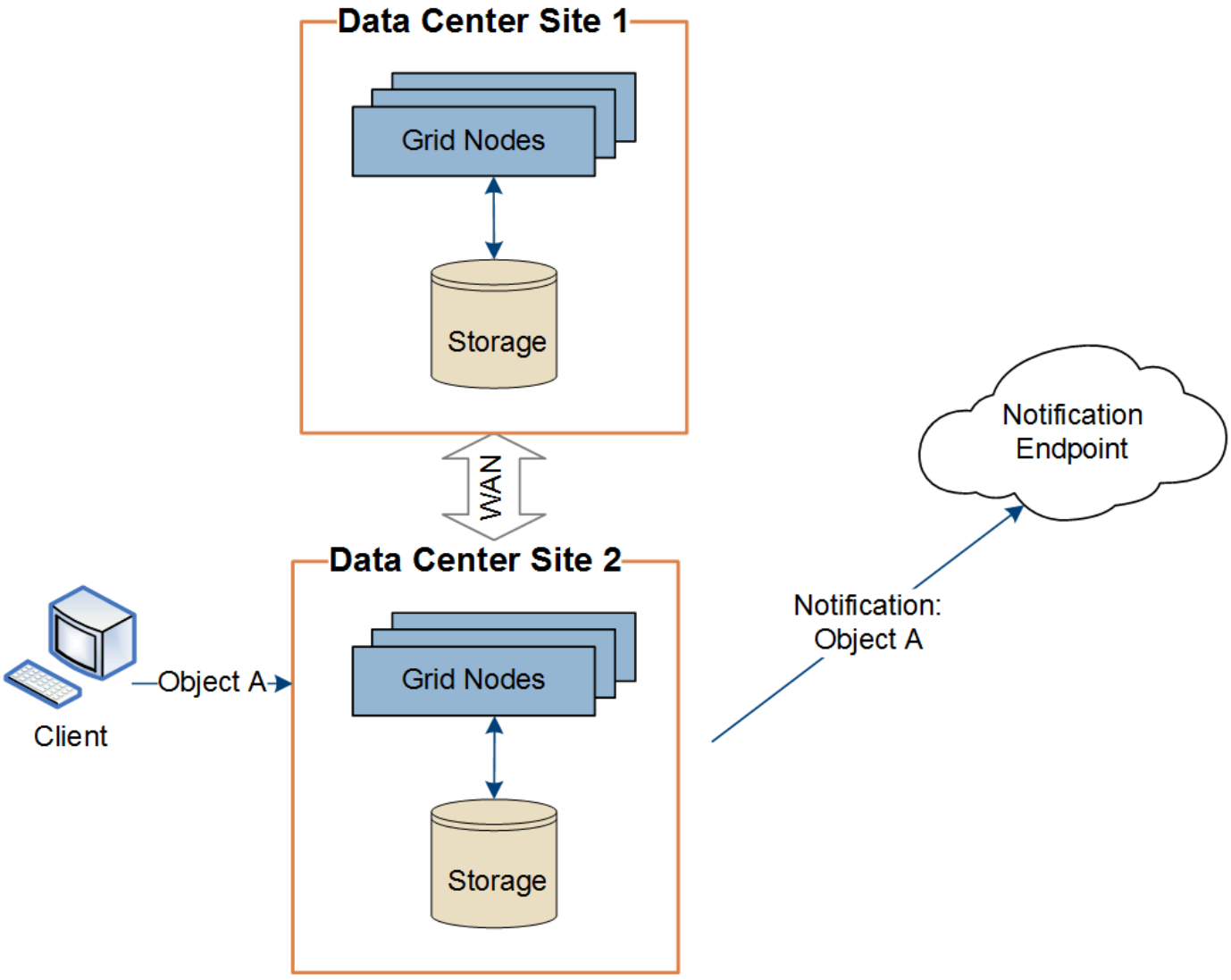
プラットフォームサービスメッセージのサイトごとの配信

すべてのプラットフォーム サービス操作はサイトごとに実行されます。

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 作成操作を実行すると、そのアクションに関する通知がトリガーされ、データセンター サイト 1 から送信されます。



その後、クライアントがデータセンター サイト 2 から同じオブジェクトに対して S3 API 削除操作を実行すると、削除アクションに関する通知がトリガーされ、データセンター サイト 2 から送信されます。



各サイトのネットワークが、プラットフォーム サービス メッセージが宛先に配信されるように構成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 マネージャでテナント ユーザーによって作成および管理されます。ただし、テナントでプラットフォーム サービスの構成または使用に関する問題が発生した場合、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の問題

テナントがプラットフォーム サービスを使用するには、テナント マネージャーを使用して 1 つ以上のエンドポイントを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、Amazon Simple Notification Service トピック、Kafka トピック、ローカルまたは AWS でホストされている Elasticsearch クラスターなど、1 つのプラットフォーム サービスの外部宛先を表します。各エンドポイントには、外部リソースの場所と、そのリソースにアクセスするために必要な資格情報の両方が含まれます。

テナントがエンドポイントを作成すると、 StorageGRIDシステムはエンドポイントが存在し、指定された資

格情報を使用してアクセスできることを検証します。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に失敗した場合、エンドポイントの検証が失敗した理由を説明するエラー メッセージが表示されます。テナント ユーザーは問題を解決してから、エンドポイントの作成を再度試みる必要があります。

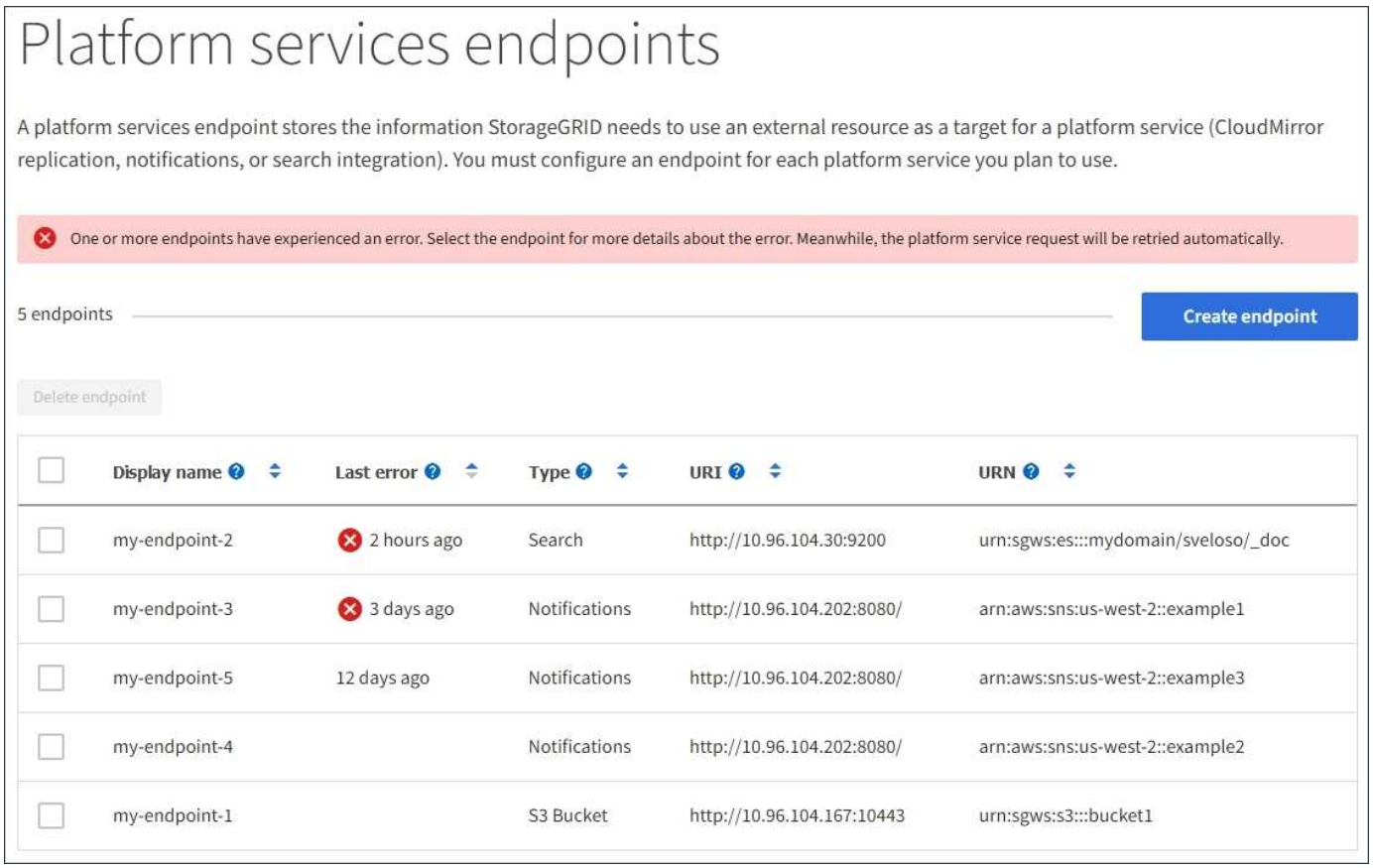
テナント アカウントに対してプラットフォーム サービスが有効になっていない場合、エンドポイントの作成は失敗します。

既存のエンドポイントの問題

StorageGRID が既存のエンドポイントに到達しようとしたときにエラーが発生した場合、テナント マネージャー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 ユーザーは、[エンドポイント] ページにアクセスして、各エンドポイントの最新のエラー メッセージを確認し、エラーが発生した時期を確認できます。 最後のエラー 列には、各エンドポイントの最新のエラー メッセージが表示され、エラーが発生した時刻が示されます。エラーには、アイコンは過去 7 日以内に発生しました。



最後のエラー 列の一部のエラー メッセージには、括弧で囲まれた logID が含まれる場合があります。グリッド管理者またはテクニカル サポートは、この ID を使用して、bycast.log 内のエラーに関する詳細情報を見つけることができます。

プロキシサーバーに関連する問題

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 エンドポイント間で、プロキシ サービスがStorageGRIDからのメッセージを許可しない場合は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 サーバーの設定を確認し、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ます。

エラーが発生したかどうかを確認する

過去 7 日以内にエンドポイント エラーが発生した場合、テナント マネージャーのダッシュボードに警告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」ページにアクセスしてください。

クライアント操作が失敗する

一部のプラットフォーム サービスの問題により、S3 バケットでのクライアント操作が失敗する可能性があります。たとえば、内部の Replicated State Machine (RSM) サービスが停止した場合、または配信キューに入っているプラットフォーム サービス メッセージが多すぎる場合、S3 クライアント操作は失敗します。

サービスのステータスを確認するには:

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。

回復可能なエンドポイント エラーと回復不可能なエンドポイント エラー

エンドポイントが作成された後、さまざまな理由によりプラットフォーム サービス要求エラーが発生する可能性があります。一部のエラーはユーザーの介入によって回復可能です。たとえば、回復可能なエラーは次の理由で発生する可能性があります。

- ユーザーの資格情報は削除されているか、期限が切れています。
- 宛先バケットが存在しません。
- 通知を配信できません。

StorageGRID で回復可能なエラーが発生した場合、プラットフォーム サービス要求は成功するまで再試行されます。

その他のエラーは回復できません。たとえば、エンドポイントが削除されると、回復できないエラーが発生します。

StorageGRID で回復不可能なエンドポイント エラーが発生した場合:

- グリッド マネージャーで、サポート > ツール > メトリック > **Grafana** > プラットフォーム サービスの概要 に移動して、エラーの詳細を表示します。
- テナント マネージャーで、ストレージ **(S3)** > プラットフォーム サービス エンドポイント に移動して、エラーの詳細を表示します。

- チェックしてください `/var/local/log/bycast-err.log`関連するエラーについて。 ADC サービスを持つストレージ ノードには、このログ ファイルが含まれます。

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

宛先でプラットフォーム サービス メッセージを受け入れられない問題が発生した場合、バケットに対するクライアント操作は成功しますが、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、宛先で資格情報が更新され、 StorageGRID が宛先サービスに対して認証できなくなった場合に、このエラーが発生する可能性があります。

関連するアラートを確認します。

プラットフォームサービスリクエストのパフォーマンスが低下

リクエストの送信速度が宛先エンドポイントがリクエストを受信できる速度を超えた場合、 StorageGRIDソフトウェアはバケットの受信 S3 リクエストを調整することがあります。スロットルは、宛先エンドポイントへの送信を待機しているリクエストのバックログがある場合にのみ発生します。

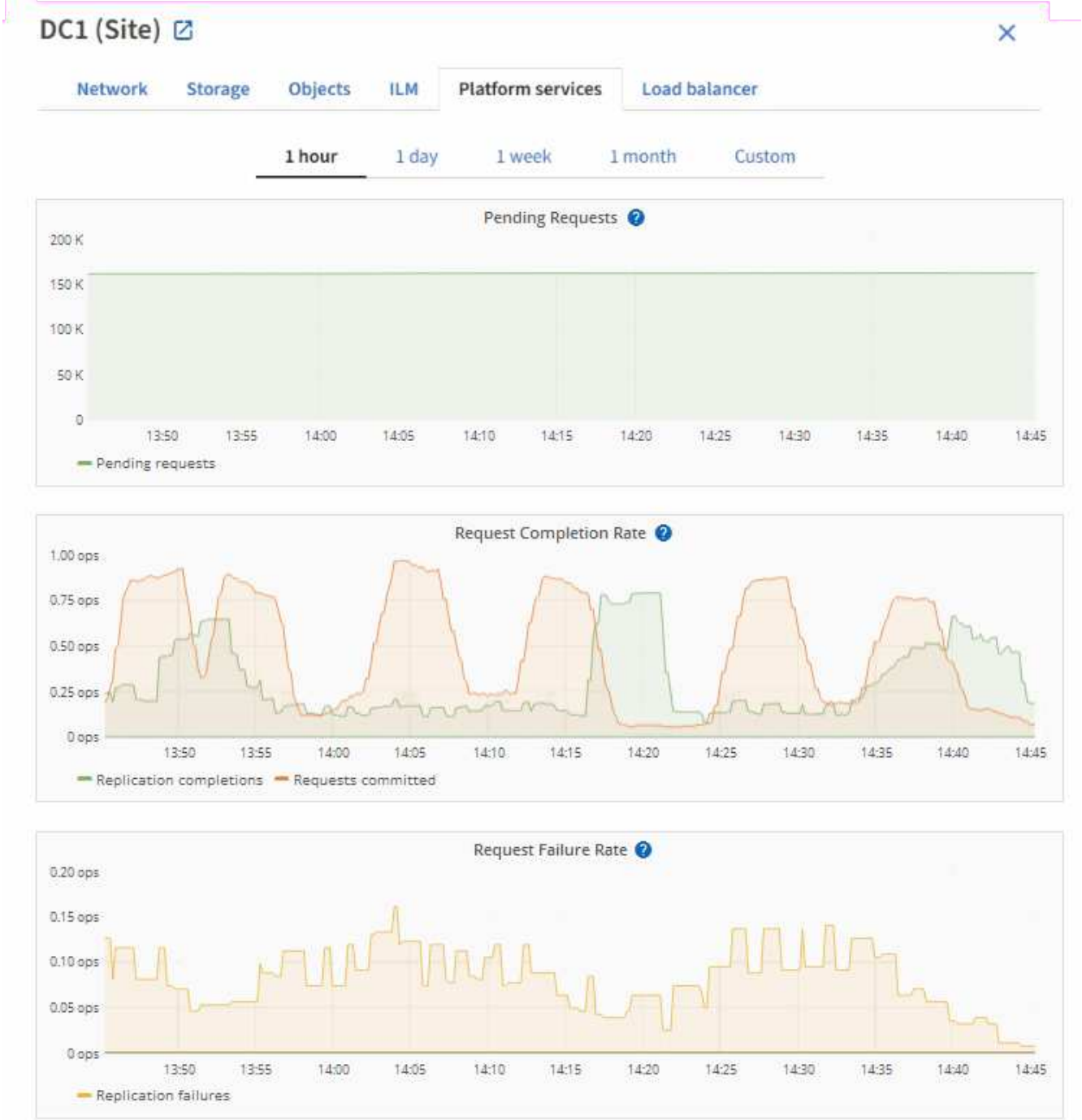
目に見える唯一の影響は、受信する S3 リクエストの実行に時間がかかるようになることです。パフォーマンスが大幅に低下していることが検出された場合は、取り込み速度を下げるか、容量の大きいエンドポイントを使用する必要があります。リクエストのバックログが増え続けると、クライアントの S3 操作 (PUT リクエストなど) は最終的に失敗します。

CloudMirror リクエストは、通常、検索統合リクエストやイベント通知リクエストよりも多くのデータ転送を伴うため、宛先エンドポイントのパフォーマンスの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リクエストが失敗する

プラットフォーム サービスのリクエスト失敗率を表示するには:

1. 「NODES」を選択します。
2. ***site*** > プラットフォーム サービス を選択します。
3. リクエストエラー率グラフを表示します。



プラットフォームサービス利用不可の警告

プラットフォーム サービスが利用できません アラートは、RSM サービスが稼働しているストレージ ノードまたは利用可能なストレージ ノードが少なすぎるため、サイトでプラットフォーム サービス操作を実行できないことを示します。

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確認します。 (RSM サービスは、ADC サービスも含まれるストレージ ノード上に存在します。)次に、それらのストレージ ノードの過半数が実行中であり、利用可能であることを確認します。

サイトで RSM サービスを含む複数のストレージ ノードに障害が発生した場合、そのサイトの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追加のトラブルシューティング ガイダンス

詳細については、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"

テナントアカウントのS3 Selectを管理する

特定の S3 テナントが S3 Select を使用して個々のオブジェクトに対して SelectObjectContent リクエストを発行できるようにすることができます。

S3 Select は、検索を可能にするためにデータベースや関連リソースをデプロイすることなく、大量のデータを効率的に検索する方法を提供します。また、データ取得のコストと待ち時間も削減されます。

S3 Select とは何ですか?

S3 Select を使用すると、S3 クライアントは SelectObjectContent リクエストを使用して、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取得できます。 S3 Select のStorageGRID実装には、S3 Select コマンドと機能のサブセットが含まれています。

S3 Select の使用に関する考慮事項と要件

グリッド管理要件

グリッド管理者はテナントに S3 Select 機能を付与する必要があります。 *S3選択を許可する*を選択する場合"テナントの作成"または"テナントの編集"。

オブジェクト形式の要件

クエリ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 または BZIP2 アーカイブに圧縮することもできます。
- 寄木細工。 Parquet オブジェクトの追加要件:
  - S3 Select は、GZIP または Snappy を使用した列指向の圧縮のみをサポートします。 S3 Select は、Parquet オブジェクトのオブジェクト全体の圧縮をサポートしていません。
  - S3 Select は Parquet 出力をサポートしていません。出力形式を CSV または JSON として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 512 MB です。
  - オブジェクトのスキーマで指定された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。

エンドポイント要件

SelectObjectContentリクエストは、"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され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。

- サービス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 が有効になっている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 リクエストにより、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ー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、信頼できるテナントに対してのみ有効にしてください。

参照"S3 Selectの使用手順"。

表示するには"Grafanaチャート"S3 Select の操作を時間経過と共に表示するには、グリッド マネージャーでサポート > ツール > メトリクス を選択します。

著作権に関する情報

商標に関する情報