StorageGRID の管理

StorageGRID

NetApp
November 05, 2025

目次

StorageGRID の管理 1
StorageGRID の管理：概要 1
これらの手順について 1
作業を開始する前に 1
Grid Managerの使用を開始する 1
Web ブラウザの要件 1
Grid Manager にサインインします 2
Grid Manager からサインアウトします 8
パスワードを変更します 8
StorageGRID ライセンス情報を表示します 9
StorageGRID ライセンス情報を更新します 10
API を使用します 11
StorageGRID へのアクセスを制御します 33
StorageGRID アクセスの制御：概要 33
プロビジョニングパスフレーズを変更します 34
ノードのコンソールパスワードを変更します 35
アイデンティティフェデレーションを使用する 37
管理者グループを管理する 42
管理者グループの権限 45
ユーザを管理します 49
シングルサインオン（ SSO ）を使用 52
グリッドフェデレーションを使用する 81
グリッドフェデレーションとは 81
アカウントクローンとは何ですか？ 83
クロスグリッドレプリケーションとは何ですか。 86
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 92
グリッドフェデレーション接続を作成する 95
グリッドフェデレーション接続を管理します 98
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 104
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 110
失敗したレプリケーション処理を特定して再試行します 116
セキュリティを管理します 119
セキュリティの管理：概要 119
StorageGRID の暗号化方式を確認します 120
証明書を管理します 123
セキュリティを設定します 156
キー管理サーバを設定 161
プロキシ設定を管理します 184
ファイアウォールを制御します 187

テナントを管理します 195
テナントの管理：概要 195
テナントアカウントを作成します 196
テナントアカウントを編集します 201
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 203
テナントアカウントを削除する 204
プラットフォームサービスを管理します 204
テナントアカウント用の S3 Select を管理します 213
クライアント接続を設定します 214
S3およびSwiftクライアント接続を設定します。概要 214
S3セットアップウィザードを使用する 217
HAグループを管理します 228
負荷分散の管理 239
S3エンドポイントのドメイン名を設定 252
Summary ：クライアント接続の IP アドレスとポート 254
ネットワークと接続を管理します 256
ネットワーク設定の構成：概要 256
StorageGRID ネットワークのガイドライン 257
IP アドレスを表示します 258
発信 TLS 接続でサポートされる暗号 260
VLAN インターフェイスを設定します 260
トラフィック分類ポリシーを管理します 264
リンクコストを管理します 271
AutoSupport を使用します 273
AutoSupport を使用：概要 273
AutoSupport を設定します 275
AutoSupport メッセージを手動でトリガーする 280
AutoSupport メッセージのトラブルシューティングを行う 281
E シリーズ AutoSupport メッセージを StorageGRID 経由で送信する 282
ストレージノードを管理します 287
Manage Storage Nodes：概要 287
ストレージノードとは 287
[ストレージ]オプションを使用します 291
オブジェクトメタデータストレージを管理する 296
メタデータ予約領域設定を増やす 303
格納オブジェクトを圧縮します 305
ストレージノード設定 306
ストレージノードがいっぱいになったときの管理 310
管理ノードを管理する 311
管理ノードとは 311
複数の管理ノードを使用する 312

プライマリ管理ノードを特定します . . . 314
通知のステータスとキューを表示します . . . 314
管理ノードによる確認済みアラームの表示（従来のシステム） . . . 315
監査クライアントアクセスを設定します . . . 315
アーカイブノードを管理します . . . 321
アーカイブノードとは . . . 321
S3 API を使用してクラウドにアーカイブします . . . 323
TSM ミドルウェア経由でのテープへのアーカイブ . . . 329
アーカイブノードの読み出し設定を行います . . . 335
アーカイブノードのレプリケーションを設定します . . . 336
アーカイブノード用のカスタムアラームを設定します . . . 337
Tivoli Storage Manager を統合します . . . 337
データを StorageGRID に移行 . . . 344
StorageGRID システムの容量を確認 . . . 344
移行データの ILM ポリシーを決定します . . . 344
移行が運用に与える影響を評価 . . . 345
データ移行のスケジュール設定と監視 . . . 345

StorageGRID の管理

StorageGRID の管理：概要

以下の手順に従って、 StorageGRID システムを設定および管理します。

これらの手順について

以下の手順では、 Grid Manager を使用してグループとユーザを設定し、 S3 および Swift クライアントアプリケーションでオブジェクトの格納と読み出しを許可するテナントアカウントを作成する方法、 StorageGRID ネットワークの設定と管理、 AutoSupport の設定、ノード設定の管理などを行う方法について説明します。

ここで説明する手順は、 StorageGRID システムのインストール後に設定、管理、およびサポートを行う技術担当者を対象としています。

作業を開始する前に

- StorageGRID システムに関する一般的な知識が必要です。
- Linux のコマンドシェル、ネットワーク、サーバハードウェアのセットアップと設定について、詳しい知識が必要です。

Grid Managerの使用を開始する

Web ブラウザの要件

サポートされている Web ブラウザを使用する必要があります。

Web ブラウザ	サポートされる最小バージョン
Google Chrome	107
Microsoft Edge の場合	107
Mozilla Firefox	106.

ブラウザウィンドウの幅を推奨される値に設定してください。

ブラウザの幅	ピクセル
最小（ Minimum ）	1024
最適	1280

Grid Manager にサインインします

Grid Manager のサインインページにアクセスするには、サポートされている Web ブラウザのアドレスバーに管理ノードの完全修飾ドメイン名（ FQDN ）または IP アドレスを入力します。

概要

各 StorageGRID システムには、 1 つのプライマリ管理ノードと、任意の数のプライマリ以外の管理ノードが含まれています。任意の管理ノードでグリッドマネージャにサインインして、 StorageGRID システムを管理できます。ただし、管理ノードはまったく同じではありません。

- ある管理ノードで実行されたアラームの確認応答（従来のシステム）は他の管理ノードにはコピーされません。そのため、各管理ノードでアラームについて異なる情報が表示される可能性があります。
- 一部のメンテナンス手順は、プライマリ管理ノードでしか実行できません。

HAグループに接続します

管理ノードがハイアベイラビリティ（ HA ）グループに含まれている場合は、 HA グループの仮想 IP アドレスまたは仮想 IP アドレスにマッピングされる完全修飾ドメイン名を使用して接続します。プライマリ管理ノードが使用できない場合を除いてプライマリ管理ノード上のグリッド Manager にアクセスするよう、プライマリ管理ノードをグループのプライマリインターフェイスとして選択する必要があります。を参照してください "ハイアベイラビリティグループを管理します"。

SSOを使用します

の場合、サインイン手順は少し異なります "シングルサインオン（SSO）が設定されている"。

最初の管理ノードで**Grid Manager**にサインインします

作業を開始する前に

- ログインクレデンシャルが必要です。
- を使用している "サポートされている Web ブラウザ"。
- Web ブラウザでクッキーが有効になっている必要があります。
- 少なくとも1つの権限が割り当てられたユーザグループに属している必要があります。
- Grid ManagerのURLが必要です。

  `https://FQDN_or_Admin_Node_IP/`

  完全修飾ドメイン名、管理ノードのIPアドレス、または管理ノードのHAグループの仮想IPアドレスを使用できます。

  HTTPSのデフォルトのポート（443）以外のポートでGrid Managerにアクセスするには、URLにポート番号を追加します。

  `https://FQDN_or_Admin_Node_IP:port/`

SSOは制限されたGrid Managerポートでは使用できません。ポート 443 を使用する必要があります。

手順

1. サポートされている Web ブラウザを起動します。
2. ブラウザのアドレスバーに、Grid ManagerのURLを入力します。
3. セキュリティアラートが表示された場合は、ブラウザのインストールウィザードを使用して証明書をインストールします。を参照してください "セキュリティ証明書を管理する"。
4. Grid Manager にサインインします。

   表示されるサインイン画面は、StorageGRID 用にシングルサインオン（SSO）が設定されているかどうかによって異なります。

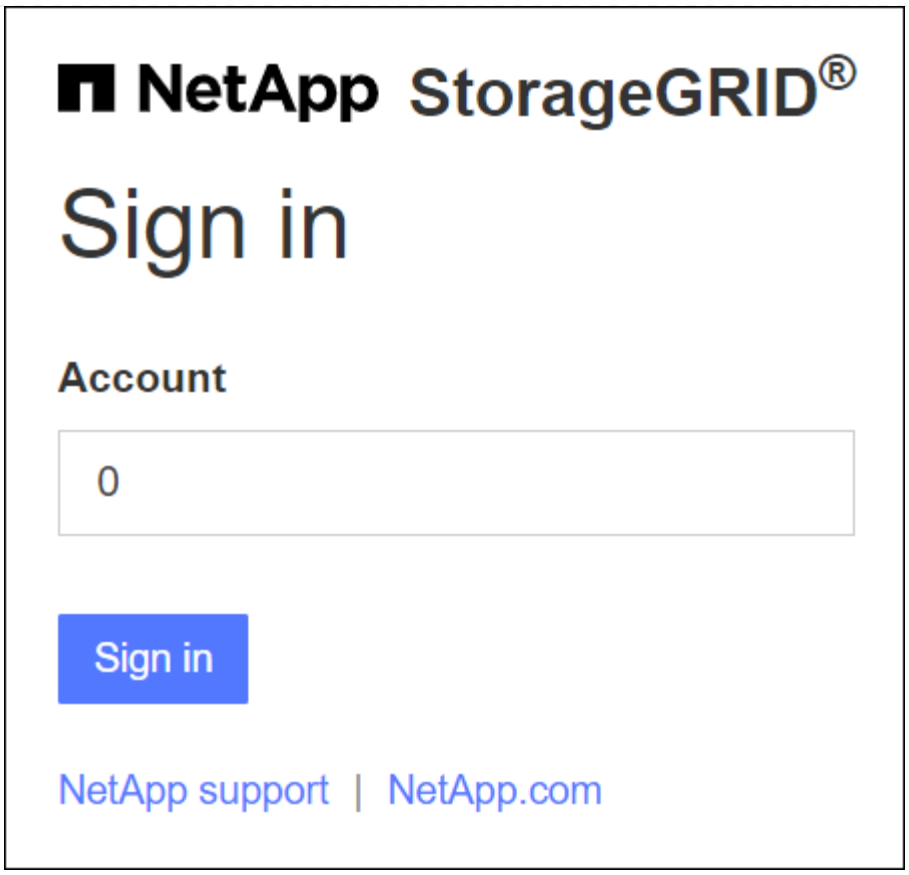
SSOを使用しない

a. Grid Manager のユーザ名とパスワードを入力します。

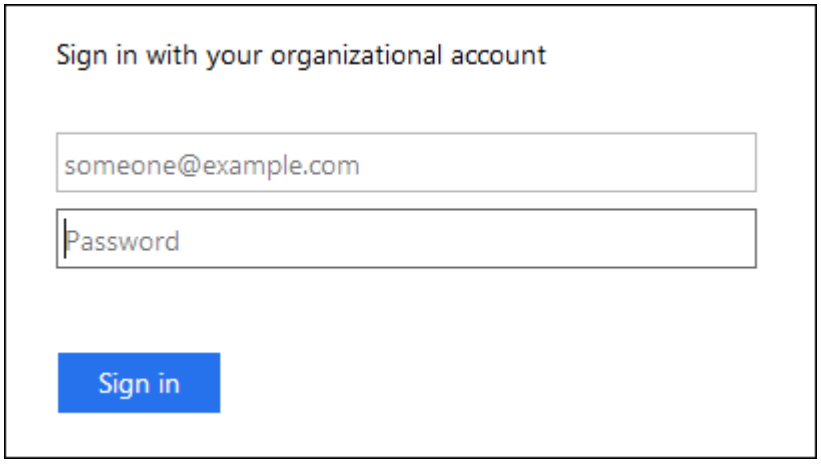
b. 「サインイン」を選択します。

SSOを使用する

- StorageGRID がSSOを使用しており、このブラウザで初めてURLにアクセスした場合は、次の手順を実行します。
  i. 「サインイン」を選択します。[Account]フィールドに0を入力したままにしておくことができます。



ii. 組織の SSO サインインページで標準の SSO クレデンシャルを入力します。例：



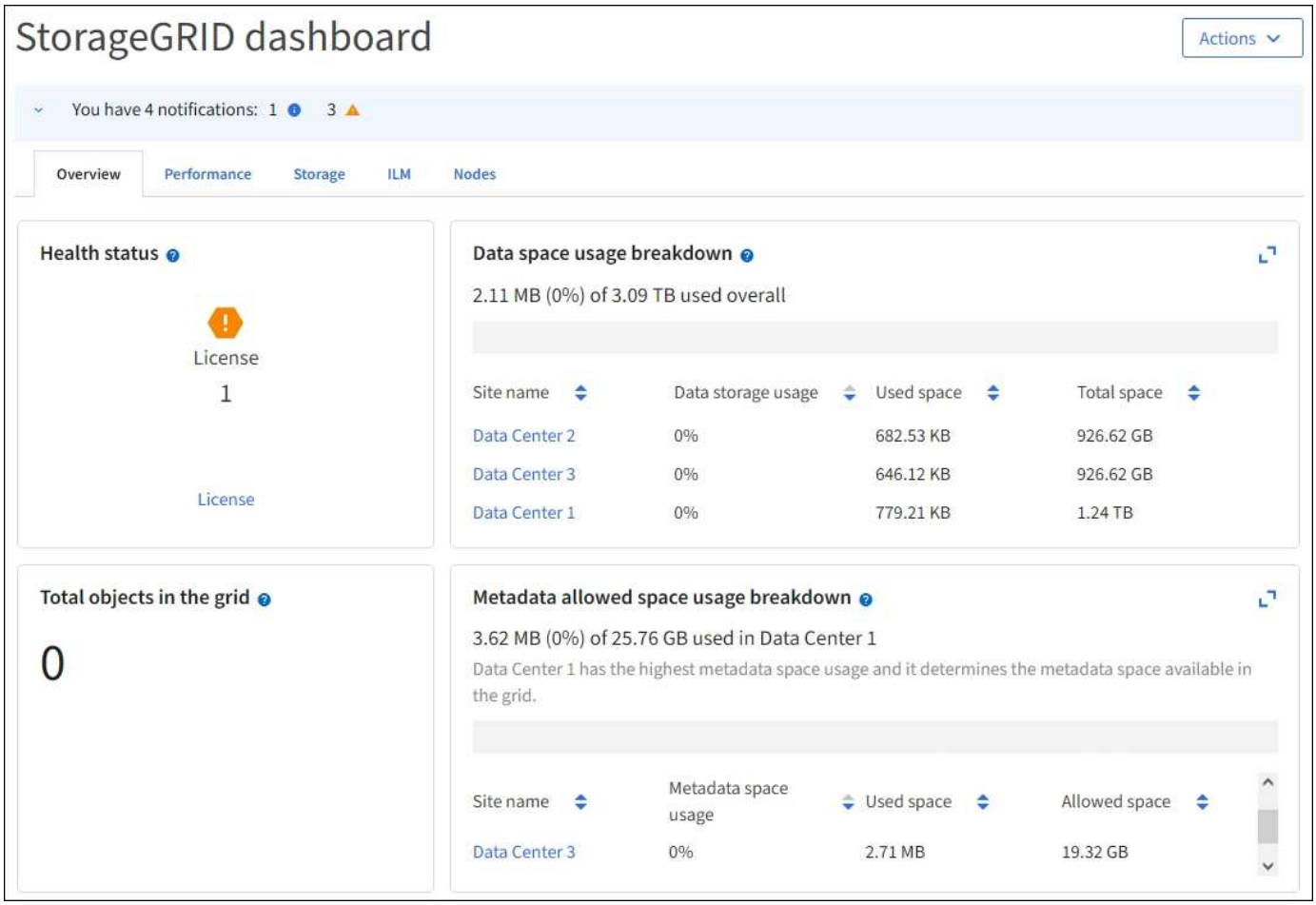
- StorageGRID でSSOを使用しており、Grid Managerまたはテナントアカウントに以前にアクセスしたことがある場合は、次の手順を実行します。

  i. 0 （**Grid Manager**のアカウント**ID**）を入力するか、最近のアカウントのリストに表示されている場合は Grid Manager *を選択します。

ii. 「サインイン」を選択します。

iii. 組織の SSO サインインページで通常使用している SSO クレデンシャルを使用してサインインします。

サインインすると、ダッシュボードを含むGrid Managerのホームページが表示されます。表示される情報については、を参照してください "ダッシュボードを表示および管理します"。



別の管理ノードにサインインします

次の手順に従って、別の管理ノードにサインインします。

SSOを使用しない

手順

1. ブラウザのアドレスバーに、他の管理ノードの完全修飾ドメイン名または IP アドレスを入力します。必要に応じてポート番号を追加します。
2. Grid Manager のユーザ名とパスワードを入力します。
3. 「サインイン」を選択します。

SSOを使用する

SSOを使用しているStorageGRID で1つの管理ノードにサインインしている場合は、再度サインインしなくても他の管理ノードにアクセスできます。

手順

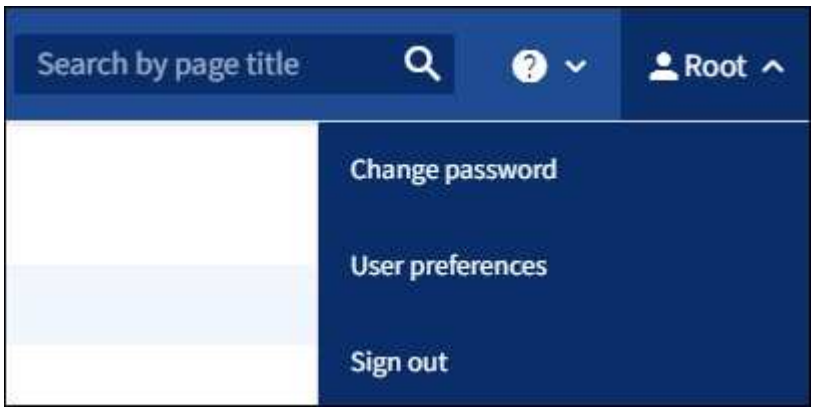
1. ブラウザのアドレスバーに、もう一方の管理ノードの完全修飾ドメイン名またはIPアドレスを入力します。
2. SSOセッションの有効期限が切れている場合は、クレデンシャルを再度入力します。

Grid Manager からサインアウトします

グリッドマネージャの操作が完了したら、サインアウトして、権限のないユーザがStorageGRID システムにアクセスできないようにする必要があります。ブラウザのクッキーの設定によっては、ブラウザを閉じてもシステムからサインアウトされない場合があります。

手順

1. 右上のユーザ名を選択します。



2. [サインアウト]*を選択します。

オプション	説明
SSO は使用されていません	管理ノードからサインアウトされます。 Grid Manager のサインインページが表示されます。 • 注： * 複数の管理ノードにサインインした場合、各ノードからサインアウトする必要があります。
SSO が有効です	アクセスしていたすべての管理ノードからサインアウトされます。StorageGRID のサインインページが表示されます。**Grid Manager** は、 [Recent Accounts] * ドロップダウンにデフォルトとして表示され、 [**Account ID**] フィールドには 0 と表示されます。 注： SSOが有効でTenant Managerにもサインインしている場合は、こちらも必要です "テナントアカウントからサインアウトします" 終了： "SSOからサインアウトします"。

パスワードを変更します

Grid Manager のローカルユーザは自分のパスワードを変更できます。

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"。

このタスクについて

フェデレーテッドユーザとしてStorageGRID にサインインする場合やシングルサインオン（SSO）が有効になっている場合は、Grid Managerでパスワードを変更することはできません。代わりに、 Active Directory や OpenLDAP などの外部 ID ソースでパスワードを変更する必要があります。

手順

1. Grid Manager のヘッダーで、 * _ your name_* > * Change password * を選択します。
2. 現在のパスワードを入力します。
3. 新しいパスワードを入力します。

   パスワードは 8 文字以上 32 文字以下にする必要があります。パスワードでは大文字と小文字が区別されます。

4. 新しいパスワードをもう一度入力します。
5. [保存（ Save ）] を選択します。

StorageGRID ライセンス情報を表示します

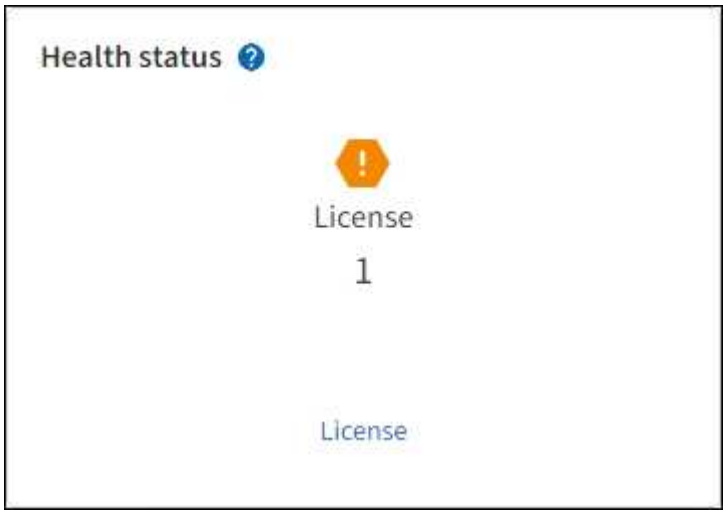
グリッドの最大ストレージ容量など、 StorageGRID システムのライセンス情報を必要に応じていつでも表示できます。

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"。

このタスクについて

このStorageGRID システムのソフトウェアライセンスを持つ問題 がある場合は、ダッシュボードの[Health]ステータスカードにライセンスステータスアイコンと*[License]リンクが表示されます。番号は、ライセンス関連の問題の数を示します。



手順

1. 次のいずれかを実行して[License]ページにアクセスします。
   - ダッシュボードの[Health]ステータスカードで、ライセンスステータスアイコンまたは*[License]*リンクを選択します。このリンクは、ライセンスを持つ問題 が存在する場合にのみ表示されます。

◦ [* maintenance * （メンテナンス * ）] > [* System * （システム * ）] > [* License * （ライセンス *

2. 現在のライセンスの読み取り専用の詳細を表示します。
   - ◦ StorageGRID システム ID 。この StorageGRID インストールの一意の ID 番号です
   - ◦ ライセンスのシリアル番号
   - ◦ ライセンスタイプ（* Perpetual または Subscription *）
   - ◦ グリッドのライセンスが付与されているストレージ容量
   - ◦ サポートされるストレージ容量
   - ◦ ライセンスの終了日。永久ライセンスの場合は「N/A *」と表示されます。
   - ◦ サポートサービス契約の終了日

     この日付は現在のライセンスファイルから読み取られます。ライセンスファイルの取得後にサポートサービス契約を延長または更新した場合は、期限が切れている可能性があります。この値を更新するには、を参照してください"StorageGRID ライセンス情報を更新します"。Active IQデジタルアドバイザ(別名デジタルアドバイザ)を使用して、実際の契約終了日を表示することもできます。

   - ◦ ライセンステキストファイルの内容

> StorageGRID 10.3 より前に発行されたライセンスの場合、ライセンスで許可されているストレージ容量はライセンスファイルに含まれておらず、値の代わりに「 See License Agreement 」というメッセージが表示されます。

StorageGRID ライセンス情報を更新します

ライセンス内容に変更があった場合は、 StorageGRID システムのライセンス情報を更新する必要があります。たとえば、グリッド用のストレージ容量を追加で購入した場合は、ライセンス情報を更新する必要があります。

作業を開始する前に

- StorageGRID システムに適用する新しいライセンスファイルを用意しておきます。
- 特定のアクセス権限が必要です。
- プロビジョニングパスフレーズを用意します。

手順

1. [* maintenance * （メンテナンス * ）] > [* System * （システム * ）] > [* License * （ライセンス *
2. StorageGRID システムのプロビジョニングパスフレーズを*テキストボックスに入力し、[参照]*を選択します。
3. [開く]ダイアログボックスで、新しいライセンスファイルを探して選択します (`.txt`）をクリックし、* Open *を選択します。

   新しいライセンスファイルが検証され、表示されます。

4. [保存（ Save ）] を選択します。

API を使用します

グリッド管理 API を使用します

Grid Manager のユーザインターフェイスの代わりにグリッド管理 REST API を使用して、システム管理タスクを実行できます。たとえば、 API を使用して処理を自動化したり、ユーザなどの複数のエンティティを迅速に作成したりできます。

トップレベルのリソース

グリッド管理 API で使用可能な最上位のリソースは次のとおりです。

- `/grid`：Grid Managerユーザのみがアクセスでき、設定されているグループ権限に基づいてアクセスが制限されます。
- `/org`：テナントアカウントのローカルまたはフェデレーテッドLDAPグループに属するユーザのみがアクセスできます。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"。
- `/private`：Grid Managerユーザのみがアクセスでき、設定されているグループ権限に基づいてアクセスが制限されます。プライベート API は予告なく変更される場合があります。StorageGRID プライベートエンドポイントは、要求の API バージョンも無視します。

問題 API 要求

グリッド管理 API では、 Swagger オープンソース API プラットフォームを使用します。Swagger のわかりやすいユーザインターフェイスを使用して、開発者および一般のユーザは StorageGRID で API を使用してリアルタイムの処理を実行できます。

Swagger のユーザインターフェイスでは、各 API 処理に関する詳細情報とドキュメントを参照できます。

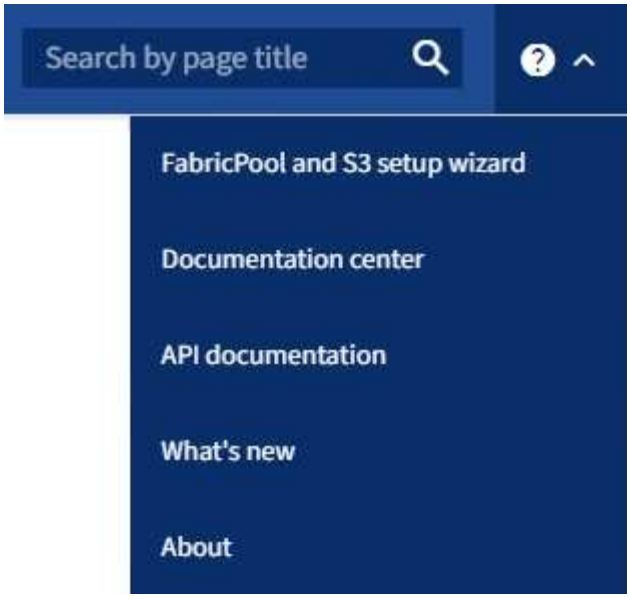
作業を開始する前に

- 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"。
- 特定のアクセス権限が必要です。

> API Docs Web ページを使用して実行する API 処理はすべてその場で実行されます。設定データやその他のデータを誤って作成、更新、または削除しないように注意してください。

手順

1. Grid Managerのヘッダーでヘルプアイコンを選択し、*[API documentation]*を選択します。



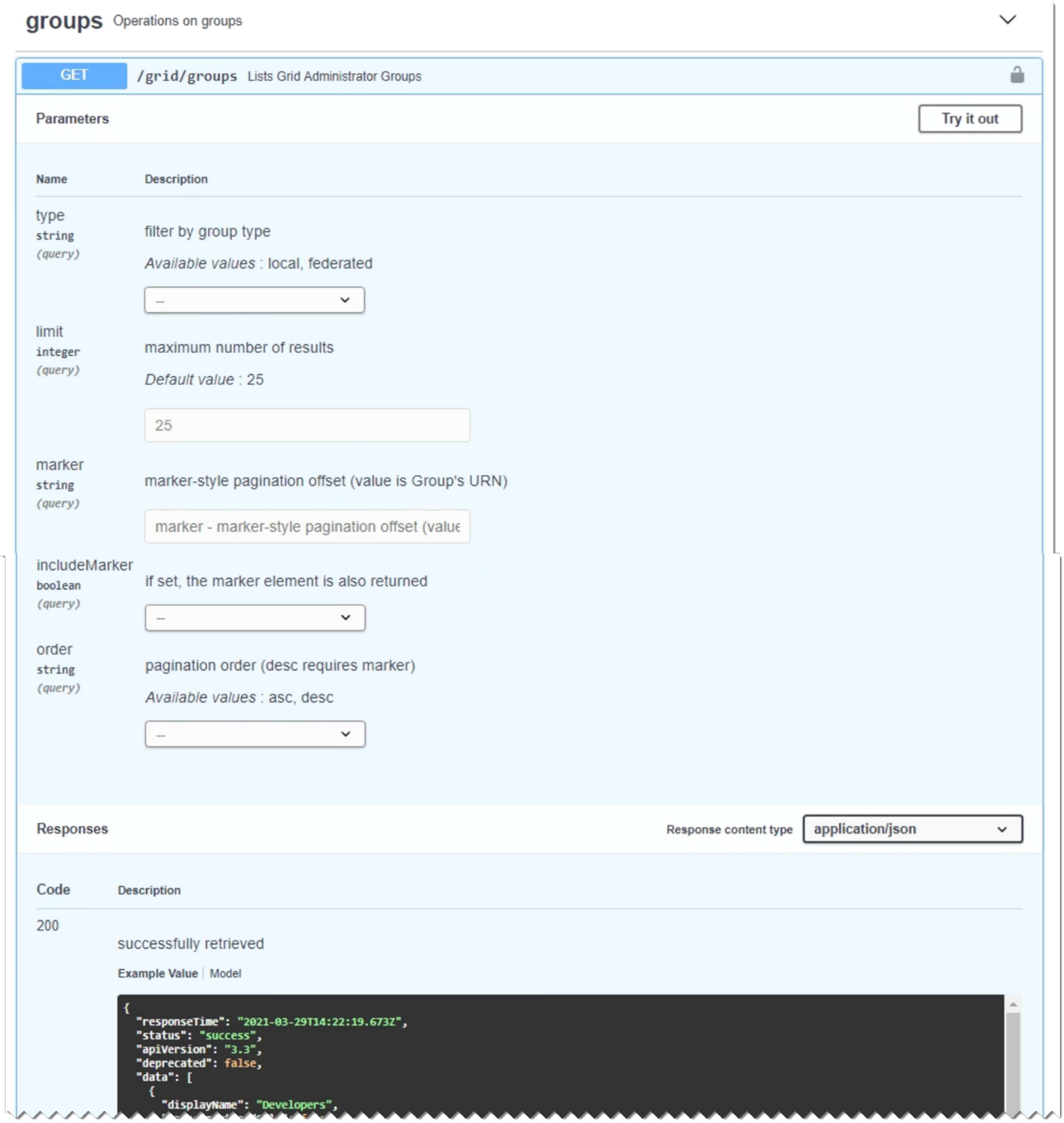
2. プライベート API を使用して操作を実行するには、 StorageGRID 管理 API ページで * プライベート API ドキュメントへ移動 * を選択します。

   プライベート API は予告なく変更される場合があります。StorageGRID プライベートエンドポイントは、要求の API バージョンも無視します。

3. 目的の処理を選択します。

   API 処理を拡張すると、 GET 、 PUT 、 UPDATE 、 DELETE など、使用可能な HTTP アクションを確認できます。

4. HTTP アクションを選択して、要求の詳細を確認します。これには、エンドポイント URL 、必須またはオプションのパラメータのリスト、要求の本文の例（必要な場合）、想定される応答が含まれます。



5. グループやユーザの ID など、要求で追加のパラメータが必要かどうかを確認します。次に、これらの値を取得します。必要な情報を取得するために、先に別の API 要求の問題 が必要になることがあります。
6. 要求の本文の例を変更する必要があるかどうかを判断します。その場合は、 * Model * を選択して各フィールドの要件を確認できます。
7. [* 試してみてください *] を選択します。
8. 必要なパラメータを指定するか、必要に応じて要求の本文を変更します。
9. [* Execute] を選択します。
10. 応答コードを確認し、要求が成功したかどうかを判断します。

グリッド管理 API では、使用可能な処理が次のセクションに分類されます。

このリストには、パブリック API で使用可能な処理のみが含まれます。

- * accounts *：新しいアカウントの作成や特定のアカウントのストレージ使用状況の取得など、ストレージテナントアカウントを管理する処理。
- * alarms *：現在のアラーム（従来のシステム）をリストし、現在のアラートやノードの接続状態の概要など、グリッドの健全性に関する情報を返す処理。
- * alert-history *：解決済みのアラートに対する処理。
- * alert-receivers *：アラート通知受信者（Eメール）に対する処理。
- * alert-rules *：アラートルールに対する処理。
- * alert-silences *：アラートサイレンスに対する処理。
- * alerts *：アラートに対する処理。
- **audit**:監査構成を一覧表示および更新する操作。
- **auth**：ユーザセッション認証を実行する処理。

  グリッド管理 API は、ベアラートークン認証方式をサポートしています。サインインするには、認証要求（つまり、 `POST /api/v3/authorize`）。ユーザが認証されると、セキュリティトークンが返されます。このトークンは、後続の API 要求（「 Authorization ： Bearer_token_ 」）のヘッダーで指定する必要があります。

  StorageGRID システムでシングルサインオンが有効になっている場合は、別の手順による認証が必要です。「シングルサインオンが有効な場合の API へのサインイン」を参照してください。

  認証セキュリティの向上については、「クロスサイトリクエストフォージェリからの保護」を参照してください。

- * client-certificates *：外部の監視ツールを使用してStorageGRID に安全にアクセスできるように、クライアント証明書を設定する処理。
- * config *：製品リリースおよびGrid管理APIのバージョンに関連する処理。製品のリリースバージョンおよびそのリリースでサポートされているグリッド管理 API のメジャーバージョンをリストし、廃止されたバージョンの API を無効にすることができます。
- * deactivated-features *：非アクティブ化された可能性がある機能を表示する操作。
- * dns-servers *：設定されている外部DNSサーバをリストおよび変更する処理。
- * endpoint-domain-names *：S3エンドポイントのドメイン名をリストおよび変更する処理。
- イレイジャーコーディング：イレイジャーコーディングプロファイルに対する処理。
- **expansion**:拡張の操作(プロシージャレベル)。
- * expansion-nodes *：拡張の処理（ノードレベル）。
- * expansion-sites *：拡張の処理（サイトレベル）。

- * grid-networks *：グリッドネットワークリストをリストおよび変更する処理。
- * grid-passwords *：Gridパスワード管理の処理。
- * groups *：ローカルのグリッド管理者グループを管理する処理、およびフェデレーテッドグリッド管理者グループを外部のLDAPサーバから取得する処理。
- *identity-source *：外部のアイデンティティソースを設定する処理、およびフェデレーテッドグループとユーザ情報を手動で同期する処理。
- * ILM *：情報ライフサイクル管理（ILM）の処理。
- * license *：StorageGRID ライセンスを取得および更新する処理。
- * logs *：ログファイルを収集およびダウンロードする処理。
- * metrics *：StorageGRID メトリックに対する処理。特定の時点におけるインスタントメトリッククエリ、および一定期間にわたるメトリッククエリを含みます。グリッド管理 API は、バックエンドのデータソースとして Prometheus システム監視ツールを使用します。Prometheus クエリの構築については、Prometheus の Web サイトを参照してください。

  を含む指標 *`private`* 名前には、内部使用のみを目的としています。これらの指標は、StorageGRID のリリース間で予告なく変更される可能性があります。

- * node-details *：ノードの詳細に対する処理。
- * node-health *：ノードの健常性ステータスに対する処理。
- * node-storage-state *：ノードのストレージステータスに対する処理。
- *ntp-servers *：外部のネットワークタイムプロトコル（NTP）サーバをリストまたは更新する処理。
- * objects *：オブジェクトおよびオブジェクトメタデータに対する処理。
- * recovery*：リカバリ手順 の処理。
- * recovery-package *：リカバリパッケージをダウンロードする処理。
- **regions**:リージョンを表示および作成する操作。
- * s3-object-lock *：グローバルS3オブジェクトロック設定に対する処理。
- * server-certificate *：Grid Managerサーバ証明書を表示および更新する処理。
- **snmp**:現在のSNMP設定に対する操作。
- * traffic-classes *：トラフィック分類ポリシーの処理。
- * untrusted-client-network *：信頼されていないクライアントネットワーク構成に対する処理。
- * users *：Grid Managerユーザを表示および管理する処理。

グリッド管理 **API** のバージョン管理

グリッド管理 API では、バージョン管理を使用して無停止アップグレードがサポートされます。

たとえば、次の要求 URL ではバージョン 3 の API が指定されています。

`https://hostname_or_ip_address/api/v3/authorize`

旧バージョンとの互換性がない *_not compatible _ * の変更が行われると、テナント管理 API のメジャーバージョンが上がります。以前のバージョンと互換性がある _ * の変更を行うと、テナント管理 API のマイナーバージョンが上がります。互換性のある変更には、新しいエンドポイントやプロパティの追加などがあります。次の例は、変更のタイプに基づいて API バージョンがどのように更新されるかを示しています。

API に対する変更のタイプ	古いバージョン	新しいバージョン
旧バージョンと互換性があります	2.1	2.2.
旧バージョンとの互換性がありません	2.1	3.0

StorageGRID ソフトウェアを初めてインストールした時点では、グリッド管理 API の最新のバージョンのみが有効になっています。ただし、 StorageGRID の新機能リリースにアップグレードした場合、少なくとも StorageGRID の機能リリース 1 つ分の間は、古い API バージョンにも引き続きアクセスできます。

グリッド管理 API を使用して、サポートされるバージョンを設定できます。詳細については、 Swagger API のドキュメントの「 config 」セクションを参照してください。すべての Grid 管理 API クライアントを新しいバージョンを使用するように更新したら、古いバージョンのサポートを無効にする必要があります。

古い要求は、次の方法で廃止とマークされます。

- 応答ヘッダーが「 Deprecated ： true 」となる。
- JSON 応答の本文に「 deprecated ： true 」が追加される
- 廃止の警告が nms.log に追加される。例：

```
Received call to deprecated v1 API at POST "/api/v1/authorize"
```

現在のリリースでサポートされている **API** のバージョンを確認します

サポートされている API のメジャーバージョンのリストを返すには、次の API 要求を使用します。

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2019-01-10T20:41:00.845Z",
  "status": "success",
  "apiVersion": "3.0",
  "data": [
    2,
    3
  ]
}
```

要求の **API** バージョンを指定します

パスパラメータを使用してAPIバージョンを指定できます (`/api/v3`）またはヘッダー (`Api-Version: 3`）。両方の値を指定した場合は、ヘッダー値がパス値よりも優先されます。

```
curl https://[IP-Address]/api/v3/grid/accounts

curl -H "Api-Version: 3" https://[IP-Address]/api/grid/accounts
```

クロスサイトリクエストフォージェリ（ **CSRF** ）の防止

CSRF トークンを使用してクッキーによる認証を強化すると、 StorageGRID に対するクロスサイトリクエストフォージェリ（ CSRF ）攻撃を防ぐことができます。Grid Manager と Tenant Manager はこのセキュリティ機能を自動的に有効にします。他の API クライアントは、サインイン時にこの機能を有効にするかどうかを選択できます。

攻撃者が別のサイト（たとえば、 HTTP フォーム POST を使用して）への要求をトリガーできる場合、サインインしているユーザのクッキーを使用して特定の要求を原因 が送信できます。

StorageGRID では、 CSRF トークンを使用して CSRF 攻撃を防ぐことができます。有効にした場合、特定のクッキーの内容が特定のヘッダーまたは特定の POST パラメータの内容と一致する必要があります。

この機能を有効にするには、を設定します `csrfToken` パラメータの値 `true` 認証中です。デフォルトはです `false`。

```
curl -X POST --header "Content-Type: application/json" --header "Accept:
application/json" -d "{
  \"username\": \"MyUserName\",
  \"password\": \"MyPassword\",
  \"cookie\": true,
  \"csrfToken\": true
}" "https://example.com/api/v3/authorize"
```

trueの場合は、Aです `GridCsrfToken` クッキーは、Grid Managerおよびへのサインインにランダムな値を使用して設定されます `AccountCsrfToken` クッキーは、Tenant Managerへのサインインではランダムな値で設定されます。

クッキーが存在する場合は、システムの状態を変更できるすべての要求（ POST 、 PUT 、 PATCH 、 DELETE ）には次のいずれかが含まれている必要があります。

- 。 `X-Csrf-Token` CSRFトークンクッキーの値がヘッダーに設定されています。
- エンドポイントがフォームエンコードされた本文を受け入れる場合：A `csrfToken` フォームエンコードされた要求の本文パラメータ。

その他の例および詳細については、オンラインの API ドキュメントを参照してください。

CSRFトークンクッキーが設定されている要求では、も適用されます "Content-Type: application/json" CSRF攻撃からの保護がさらに強化されるために、JSON要求の本文が必要なすべての要求のヘッダー。

シングルサインオンが有効な場合は、 **API** を使用します

シングルサインオンが有効な場合（ **Active Directory** ）は **API** を使用

ある場合 "シングルサインオン（ SSO ）の設定と有効化" また、 Active Directory を SSO プロバイダとして使用する場合は、一連の API 要求を問題 で実行して、グリッド管理 API またはテナント管理 API で有効な認証トークンを取得する必要があります。

シングルサインオンが有効な場合は、 **API** にサインインします

ここで説明する手順は、 Active Directory を SSO アイデンティティプロバイダとして使用する場合に該当します。

作業を開始する前に

- StorageGRID ユーザグループに属するフェデレーテッドユーザの SSO ユーザ名とパスワードが必要です。
- テナント管理 API にアクセスする場合は、テナントアカウント ID を確認しておきます。

このタスクについて

認証トークンを取得するには、次のいずれかの例を使用します。

- 。 `storagegrid-ssoauth.py` Pythonスクリプト。StorageGRID インストールファイルのディレクトリにあります (`./rpms` Red Hat Enterprise LinuxまたはCentOSの場合： `./debs` UbuntuまたはDebianの場合は、および `./vsphere` VMwareの場合）をクリックします。
- cURL 要求のワークフローの例。

  cURL ワークフローは、実行に時間がかかりすぎるとタイムアウトする場合があります。次のエラーが表示される場合があります。 `A valid SubjectConfirmation was not found on this Response`。

  cURL ワークフローの例では、パスワードが他のユーザに表示されないように保護されていません。

URLエンコード問題 を使用している場合は、次のエラーが表示されることがあります。 `Unsupported SAML version`。

手順

1. 認証トークンを取得するには、次のいずれかの方法を選択します。
   - を使用します `storagegrid-ssoauth.py` Pythonスクリプト。手順 2 に進みます。
   - curl 要求を使用します。手順 3 に進みます。
2. を使用する場合は、を参照してください `storagegrid-ssoauth.py` スクリプトを使用して、Pythonインタープリタにスクリプトを渡し、スクリプトを実行します。

プロンプトが表示されたら、次の引数の値を入力します。

- SSO 方式。ADFS または ADFS と入力します。
- SSO ユーザ名
- StorageGRID がインストールされているドメイン
- StorageGRID のアドレス
- テナント管理 API にアクセスする場合は、テナントアカウント ID 。

```
python3 storagegrid-ssoauth.py
sso_method: adfs
saml_user: my-sso-username
saml_domain: my-domain
sg_address: storagegrid.example.com
tenant_account_id: 12345
Enter the user's SAML password:
********************************************************************************

********************************************************************************
StorageGRID Auth Token: 56eb07bf-21f6-40b7-afob-5c6cacfb25e7
```

StorageGRID 認証トークンが出力に表示されます。SSO を使用していない場合の API の使用方法と同様に、トークンを他の要求に使用できるようになりました。

3. cURL 要求を使用する場合は、次の手順 を使用します。

   a. サインインに必要な変数を宣言します。

```
export SAMLUSER='my-sso-username'
export SAMLPASSWORD='my-password'
export SAMLDOMAIN='my-domain'
export TENANTACCOUNTID='12345'
export STORAGEGRID_ADDRESS='storagegrid.example.com'
export AD_FS_ADDRESS='adfs.example.com'
```

   グリッド管理APIにアクセスするには、として0を使用します `TENANTACCOUNTID`。

   b. 署名付き認証URLを受信するには、へのPOST要求を問題 に送信します `/api/v3/authorize-saml`をクリックし、応答からJSONエンコードを削除します。

   次の例は、の署名付き認証URLに対するPOST要求を示しています `TENANTACCOUNTID`。結果はに渡されます `python -m json.tool` をクリックしてJSONエンコーディングを削除します。

```
curl -X POST "https://$STORAGEGRID_ADDRESS/api/v3/authorize-saml" \
  -H "accept: application/json" -H  "Content-Type: application/json"
\
  --data "{\"accountId\": \"$TENANTACCOUNTID\"}" | python -m
json.tool
```

この例の応答には、 URL エンコードされた署名済み URL が含まれていますが、 JSON エンコードされたレイヤは含まれていません。

```
{
    "apiVersion": "3.0",
    "data":
"https://adfs.example.com/adfs/ls/?SAMLRequest=fZHLbsIwEEV%2FJTuv7...
sSl%2BfQ33cvfwA%3D&RelayState=12345",
    "responseTime": "2018-11-06T16:30:23.355Z",
    "status": "success"
}
```

c. を保存します `SAMLRequest` 後続のコマンドで使用する応答から。

```
export SAMLREQUEST='fZHLbsIwEEV%2FJTuv7...sSl%2BfQ33cvfwA%3D'
```

d. AD FS からクライアント要求 ID を含む完全な URL を取得します。

1 つは、前の応答の URL を使用してログインフォームを要求する方法です。

```
curl "https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=
$SAMLREQUEST&RelayState=$TENANTACCOUNTID" | grep 'form method="post"
id="loginForm"'
```

応答にはクライアント要求 ID が含まれています。

```
<form method="post" id="loginForm" autocomplete="off"
novalidate="novalidate" onKeyPress="if (event && event.keyCode == 13)
Login.submitLoginRequest();" action="/adfs/ls/?
SAMLRequest=fZHRToMwFIZfhb...UJikvo77sXPw%3D%3D&RelayState=12345&clie
nt-request-id=00000000-0000-0000-ee02-0080000000de" >
```

e. 応答からクライアント要求 ID を保存します。

```
export SAMLREQUESTID='00000000-0000-0000-ee02-0080000000de'
```

f. 前の応答のフォームアクションにクレデンシャルを送信します。

```
curl -X POST "https://$AD_FS_ADDRESS
/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=$TENANTACCOUNTID&client
-request-id=$SAMLREQUESTID" \
--data "UserName=$SAMLUSER@$SAMLDOMAIN&Password=
$SAMLPASSWORD&AuthMethod=FormsAuthentication" --include
```

AD FS からヘッダーに追加情報 が含まれた 302 リダイレクトが返されます。

> SSO システムで多要素認証（ MFA ）が有効になっている場合、フォームポストには 2 つ目のパスワードまたはその他のクレデンシャルも含まれます。

```
HTTP/1.1 302 Found
Content-Length: 0
Content-Type: text/html; charset=utf-8
Location:
https://adfs.example.com/adfs/ls/?SAMLRequest=fZHRToMwFIZfhb...UJikvo
77sXPw%3D%3D&RelayState=12345&client-request-id=00000000-0000-0000-
ee02-0080000000de
Set-Cookie: MSISAuth=AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY=; path=/adfs;
HttpOnly; Secure
Date: Tue, 06 Nov 2018 16:55:05 GMT
```

g. を保存します `MSISAuth` 応答からのCookie。

```
export MSISAuth='AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY='
```

h. 認証 POST からクッキーを使用して、指定した場所に GET 要求を送信します。

```
curl "https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=
$SAMLREQUEST&RelayState=$TENANTACCOUNTID&client-request-
id=$SAMLREQUESTID" \
--cookie "MSISAuth=$MSISAuth" --include
```

応答ヘッダーには、あとでログアウトに使用する AD FS セッション情報が含まれます。応答の本文には、非表示のフォームフィールドに SAMLResponse が含まれています。

```
HTTP/1.1 200 OK
Cache-Control: no-cache,no-store
Pragma: no-cache
Content-Length: 5665
Content-Type: text/html; charset=utf-8
Expires: -1
Server: Microsoft-HTTPAPI/2.0
P3P: ADFS doesn't have P3P policy, please contact your site's admin
for more details
Set-Cookie:
SamlSession=a3dpbnRlcnMtUHJpbWFyeS1BZG1pbi0xNzgmRmFsc2Umcng4NnJDZmFKV
XFxVWx3bkl1MnFuUSUzZCUzZCYmJiYmXzE3MjAyZTA5LThmMDgtNDRkZC04Yzg5LTQ3ND
UxYzA3ZjkzYw==; path=/adfs; HttpOnly; Secure
Set-Cookie: MSISAuthenticated=MTEvNy8yMDE4IDQ6MzI6NTkgUE0=;
path=/adfs; HttpOnly; Secure
Set-Cookie: MSISLoopDetectionCookie=MjAxOC0xMS0wNzoxNjozMjo1OVpcMQ==;
path=/adfs; HttpOnly; Secure
Date: Wed, 07 Nov 2018 16:32:59 GMT

<form method="POST" name="hiddenform"
action="https://storagegrid.example.com:443/api/saml-response">
  <input type="hidden" name="SAMLResponse"
value="PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4=" /><input
type="hidden" name="RelayState" value="12345" />
```

i. を保存します `SAMLResponse` 非表示フィールドから：

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. を使用して保存します `SAMLResponse`をクリックして、StorageGRID を作成します`/api/saml-response` StorageGRID 認証トークンの生成要求

の場合 `RelayState`をクリックします。グリッド管理APIにサインインする場合は、テナントアカウントIDを使用します。

```
curl -X POST "https://$STORAGEGRID_ADDRESS:443/api/saml-response" \
  -H "accept: application/json" \
  --data-urlencode "SAMLResponse=$SAMLResponse" \
  --data-urlencode "RelayState=$TENANTACCOUNTID" \
  | python -m json.tool
```

応答には認証トークンが含まれています。

```
{
    "apiVersion": "3.0",
    "data": "56eb07bf-21f6-40b7-af0b-5c6cacfb25e7",
    "responseTime": "2018-11-07T21:32:53.486Z",
    "status": "success"
}
```

a. 認証トークンを応答にという名前で保存します `MYTOKEN`。

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

これで、を使用できます `MYTOKEN` その他の要求の場合は、SSOを使用していない場合のAPIの使用方法と同様です。

シングルサインオンが有効な場合は、 **API** からサインアウトします

シングルサインオン（ SSO ）が有効になっている場合は、グリッド管理 API またはテナント管理 API からサインアウトするための一連の API 要求を問題 で処理する必要があります。ここで説明する手順は、 Active Directory を SSO アイデンティティプロバイダとして使用する場合に該当します

このタスクについて

必要に応じて、組織のシングルログアウトページからログアウトすることで、StorageGRID APIからサインアウトできます。または、 StorageGRID からシングルログアウト（ SLO ）を実行することもできます。この場合、有効な StorageGRID ベアラトークンが必要です。

手順

1. 署名されたログアウト要求を生成するには、合格します `cookie "sso=true"` SLO APIで次の処理を実行します。

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--cookie "sso=true" \
| python -m json.tool
```

ログアウト URL が返されます。

```
{
    "apiVersion": "3.0",
    "data":
"https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3
D",
    "responseTime": "2018-11-20T22:20:30.839Z",
    "status": "success"
}
```

2. ログアウト URL を保存します。

```
export LOGOUT_REQUEST
='https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%
3D'
```

3. 要求をログアウト URL に送信し、 SLO を実行して StorageGRID にリダイレクトします。

```
curl --include "$LOGOUT_REQUEST"
```

302 応答が返されます。リダイレクト先は API のみのログアウトには適用されません。

```
HTTP/1.1 302 Found
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-
logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256
Set-Cookie: MSISSignoutProtocol=U2FtbA==; expires=Tue, 20 Nov 2018
22:35:03 GMT; path=/adfs; HttpOnly; Secure
```

4. StorageGRID Bearer トークンを削除します。

StorageGRID Bearer トークンを削除すると、 SSO を使用しない場合と同じように動作します。状況 `cookie "sso=true"` を指定しないと、SSOの状態に影響を及ぼすことなくユーザがStorageGRID からログアウトされます。

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--include
```

A `204 No Content` 応答として、ユーザがサインアウトしたことが示されます。

```
HTTP/1.1 204 No Content
```

シングルサインオンが有効な場合（ **Azure** ）は **API** を使用

ある場合 "シングルサインオン（ SSO ）の設定と有効化" また、 Azure を SSO プロバイダとして使用している場合は、 2 つのサンプルスクリプトを使用して、グリッド管理 API またはテナント管理 API で有効な認証トークンを取得できます。

Azure シングルサインオンが有効な場合は、 **API** にサインインします

以下の手順は、 Azure を SSO アイデンティティプロバイダとして使用する場合に該当します

作業を開始する前に

- StorageGRID ユーザグループに属するフェデレーテッドユーザの SSO E メールアドレスとパスワードが必要です。
- テナント管理 API にアクセスする場合は、テナントアカウント ID を確認しておきます。

このタスクについて

認証トークンを取得するには、次のサンプルスクリプトを使用します。

- 。 `storagegrid-ssoauth-azure.py` Python スクリプト
- 。 `storagegrid-ssoauth-azure.js` Node.jsスクリプト

どちらのスクリプトも、StorageGRID インストールファイルディレクトリにあります (`./rpms` Red Hat Enterprise LinuxまたはCentOSの場合： `./debs` UbuntuまたはDebianの場合は、および `./vsphere` VMware の場合）をクリックします。

Azureと独自のAPI統合を作成するには、を参照してください `storagegrid-ssoauth-azure.py` スクリプト：Python スクリプトは、 StorageGRID に対して 2 つの要求を直接実行し（まず SAMLRequest を取得し、あとで認証トークンを取得するため）、さらに Node.js スクリプトを呼び出して、 SSO 処理を実行します。

SSO 処理は一連の API 要求を使用して実行できますが、実行するのは簡単ではありません。puppeteer Node.js モジュールは、 Azure SSO インターフェイスを破棄するために使用します。

URLエンコード問題 を使用している場合は、次のエラーが表示されることがあります。 `Unsupported SAML version`。

手順

1. 必要な依存関係を次のようにインストールします。
   a. Node.js をインストールします（を参照） "https://nodejs.org/en/download/"）。
   b. 必要な Node.js モジュール（ puppeteer および jsdom ）を取り付けます。

      ```
      npm install -g <module>
      ```

2. Python スクリプトを Python インタープリタに渡して、スクリプトを実行します。

Python スクリプトは、対応する Node.js スクリプトを呼び出して、 Azure SSO のインタラクションを実行します。

3. プロンプトが表示されたら、次の引数の値を入力します（または、パラメータを使用して渡します）。
   - Azure へのサインインに使用する SSO E メールアドレス
   - StorageGRID のアドレス
   - テナント管理 API にアクセスする場合は、テナントアカウント ID
4. プロンプトが表示されたら、パスワードを入力し、要求された場合に Azure に対する MFA 認証を提供できるように準備します。

```
c:\Users\user\Documents\azure_sso>py storagegrid-azure-ssoauth.py --sso-email-address user@my-domain.com
--sg-address storagegrid.examp.e.com --tenant-account-id 0
Enter the user's SSO password:
********************************************************************************

Watch for and approve a 2FA authorization request
********************************************************************************
StorageGRID Auth Token: {'responseTime': '2021-10-04T21:30:48.807Z', 'status': 'success', 'apiVersion':
'3.4', 'data': '4807d93e-a3df-48f2-9680-906cd255979e'}
```

> このスクリプトでは、 MFA が Microsoft Authenticator を使用して実行されていることを前提として他の形式のMFAをサポートするようにスクリプトを変更する必要がある場合があります（テキストメッセージで受信したコードの入力など）。

StorageGRID 認証トークンが出力に表示されます。SSO を使用していない場合の API の使用方法と同様に、トークンを他の要求に使用できるようになりました。

シングルサインオンが有効な場合は **API** を使用（ **PingFederate** ）

ある場合 "シングルサインオン（ SSO ）の設定と有効化" また、 SSO プロバイダとして PingFederate を使用するには、グリッド管理 API またはテナント管理 API で有効な認証トークンを取得するための一連の API 要求を問題 で処理する必要があります。

シングルサインオンが有効な場合は、 **API** にサインインします

これらの手順は、 SSO アイデンティティプロバイダとして PingFederate を使用している場合に適用されます

作業を開始する前に

- StorageGRID ユーザグループに属するフェデレーテッドユーザの SSO ユーザ名とパスワードが必要です。
- テナント管理 API にアクセスする場合は、テナントアカウント ID を確認しておきます。

このタスクについて

認証トークンを取得するには、次のいずれかの例を使用します。

- 。 `storagegrid-ssoauth.py` Pythonスクリプト。StorageGRID インストールファイルのディレクトリにあります (`./rpms` Red Hat Enterprise LinuxまたはCentOSの場合： `./debs` UbuntuまたはDebianの場合は、および `./vsphere` VMwareの場合）をクリックします。
- cURL 要求のワークフローの例。

cURL ワークフローは、実行に時間がかかりすぎるとタイムアウトする場合があります。次のエラーが表示される場合があります。 `A valid SubjectConfirmation was not found on this Response`。

> cURL ワークフローの例では、パスワードが他のユーザに表示されないように保護されていません。

URLエンコード問題 を使用している場合は、次のエラーが表示されることがあります。 `Unsupported SAML version`。

手順

1. 認証トークンを取得するには、次のいずれかの方法を選択します。
   - を使用します `storagegrid-ssoauth.py` Pythonスクリプト。手順 2 に進みます。
   - curl 要求を使用します。手順 3 に進みます。
2. を使用する場合は、を参照してください `storagegrid-ssoauth.py` スクリプトを使用して、Pythonインタープリタにスクリプトを渡し、スクリプトを実行します。

   プロンプトが表示されたら、次の引数の値を入力します。

   - SSO 方式。「 PingFederate 」（ PingFederate 、 PingFederate など）の任意のバリエーションを入力できます。
   - SSO ユーザ名
   - StorageGRID がインストールされているドメイン。このフィールドは PingFederate には使用されません。空白のままにするか、任意の値を入力できます。
   - StorageGRID のアドレス
   - テナント管理 API にアクセスする場合は、テナントアカウント ID 。

   ```
   python3 storagegrid-ssoauth.py
   sso_method: pingfederate
   saml_user: my-sso-username
   saml_domain:
   sg_address: storagegrid.example.com
   tenant_account_id: 12345
   Enter the user's SAML password:
   ********************************************************************************

   ********************************************************************************
   StorageGRID Auth Token: 56eb07bf-21f6-40b7-afob-5c6cacfb25e7
   ```

   StorageGRID 認証トークンが出力に表示されます。SSO を使用していない場合の API の使用方法と同様に、トークンを他の要求に使用できるようになりました。
3. cURL 要求を使用する場合は、次の手順 を使用します。
   a. サインインに必要な変数を宣言します。

```
export SAMLUSER='my-sso-username'
export SAMLPASSWORD='my-password'
export TENANTACCOUNTID='12345'
export STORAGEGRID_ADDRESS='storagegrid.example.com'
```

グリッド管理APIにアクセスするには、として0を使用します `TENANTACCOUNTID`。

b. 署名付き認証URLを受信するには、へのPOST要求を問題 に送信します `/api/v3/authorize-saml`をクリックし、応答からJSONエンコードを削除します。

次の例は、 TENANTACCOUNTID の署名済み認証 URL を取得するための POST 要求です。結果は python-m json ツールに渡され、 JSON エンコードが削除されます。

```
curl -X POST "https://$STORAGEGRID_ADDRESS/api/v3/authorize-saml" \
  -H "accept: application/json" -H  "Content-Type: application/json"
\
  --data "{\"accountId\": \"$TENANTACCOUNTID\"}" | python -m
json.tool
```

この例の応答には、 URL エンコードされた署名済み URL が含まれていますが、 JSON エンコードされたレイヤは含まれていません。

```
{
    "apiVersion": "3.0",
    "data": "https://my-pf-baseurl/idp/SSO.saml2?...",
    "responseTime": "2018-11-06T16:30:23.355Z",
    "status": "success"
}
```

c. を保存します `SAMLRequest` 後続のコマンドで使用する応答から。

```
export SAMLREQUEST="https://my-pf-baseurl/idp/SSO.saml2?..."
```

d. 応答とクッキーをエクスポートし、応答をエコーします。

```
RESPONSE=$(curl -c - "$SAMLREQUEST")
```

```
echo "$RESPONSE" | grep 'input type="hidden" name="pf.adapterId"
id="pf.adapterId"'
```

e. 'pf.adapterID' 値をエクスポートし、応答をエコーします。

```
export ADAPTER='myAdapter'
```

```
echo "$RESPONSE" | grep 'base'
```

f. 「 href 」値をエクスポートし（末尾のスラッシュ / を削除）、応答をエコーします。

```
export BASEURL='https://my-pf-baseurl'
```

```
echo "$RESPONSE" | grep 'form method="POST"'
```

g. 「 action 」の値をエクスポートします。

```
export SSOPING='/idp/.../resumeSAML20/idp/SSO.ping'
```

h. クレデンシャルとともに Cookie を送信する：

```
curl -b <(echo "$RESPONSE") -X POST "$BASEURL$SSOPING" \
--data "pf.username=$SAMLUSER&pf.pass=
$SAMLPASSWORD&pf.ok=clicked&pf.cancel=&pf.adapterId=$ADAPTER"
--include
```

i. を保存します `SAMLResponse` 非表示フィールドから：

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. を使用して保存します `SAMLResponse`をクリックして、StorageGRID を作成します`/api/saml-response` StorageGRID 認証トークンの生成要求

の場合 `RelayState`をクリックします。グリッド管理APIにサインインする場合は、テナントアカウントIDを使用します。

```
curl -X POST "https://$STORAGEGRID_ADDRESS:443/api/saml-response" \
  -H "accept: application/json" \
  --data-urlencode "SAMLResponse=$SAMLResponse" \
  --data-urlencode "RelayState=$TENANTACCOUNTID" \
  | python -m json.tool
```

応答には認証トークンが含まれています。

```
{
    "apiVersion": "3.0",
    "data": "56eb07bf-21f6-40b7-af0b-5c6cacfb25e7",
    "responseTime": "2018-11-07T21:32:53.486Z",
    "status": "success"
}
```

a. 認証トークンを応答にという名前で保存します `MYTOKEN`。

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

これで、を使用できます `MYTOKEN` その他の要求の場合は、SSOを使用していない場合のAPIの使用方法と同様です。

シングルサインオンが有効な場合は、 **API** からサインアウトします

シングルサインオン（ SSO ）が有効になっている場合は、グリッド管理 API またはテナント管理 API からサインアウトするための一連の API 要求を問題 で処理する必要があります。これらの手順は、 SSO アイデンティティプロバイダとして PingFederate を使用している場合に適用されます

このタスクについて

必要に応じて、組織のシングルログアウトページからログアウトすることで、StorageGRID APIからサインアウトできます。または、 StorageGRID からシングルログアウト（ SLO ）を実行することもできます。この場合、有効な StorageGRID ベアラトークンが必要です。

手順

1. 署名されたログアウト要求を生成するには、合格します `cookie "sso=true"` SLO APIで次の処理を実行します。

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--cookie "sso=true" \
| python -m json.tool
```

ログアウト URL が返されます。

```
{
    "apiVersion": "3.0",
    "data": "https://my-ping-
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D",
    "responseTime": "2021-10-12T22:20:30.839Z",
    "status": "success"
}
```

2. ログアウト URL を保存します。

```
export LOGOUT_REQUEST='https://my-ping-
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D'
```

3. 要求をログアウト URL に送信し、 SLO を実行して StorageGRID にリダイレクトします。

```
curl --include "$LOGOUT_REQUEST"
```

302 応答が返されます。リダイレクト先は API のみのログアウトには適用されません。

```
HTTP/1.1 302 Found
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-
logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256
Set-Cookie: PF=QoKs...SgCC; Path=/; Secure; HttpOnly; SameSite=None
```

4. StorageGRID Bearer トークンを削除します。

StorageGRID Bearer トークンを削除すると、 SSO を使用しない場合と同じように動作します。状況 `cookie "sso=true"` を指定しないと、SSOの状態に影響を及ぼすことなくユーザがStorageGRID からログアウトされます。

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--include
```

A `204 No Content` 応答として、ユーザがサインアウトしたことが示されます。

```
HTTP/1.1 204 No Content
```

API で機能を非アクティブ化します

グリッド管理 API を使用すると、 StorageGRID システムの特定の機能を完全に非アクティブ化できます。機能を非アクティブ化すると、その機能に関連するタスクを実行する権限をユーザに割り当てることができなくなります。

このタスクについて

非活動化されたフィーチャーシステムを使用すると、 StorageGRID システムの特定のフィーチャーへのアクセスを禁止できます。機能の非アクティブ化は、 root ユーザまたは * Root Access * 権限を持つ管理者グループに属するユーザがその機能を使用できないようにする唯一の方法です。

この機能がどのように役立つかを理解するために、次のシナリオを検討してください。

_Company A は、テナントアカウントを作成して StorageGRID システムのストレージ容量をリースするサービスプロバイダです。容量をリースしている顧客のオブジェクトのセキュリティを保護するために、 A 社では、アカウントの導入後に自社の従業員がテナントアカウントにアクセスできないようにしたいと考えています。 _

_ 企業 A は、グリッド管理 API で Deactivate Features システムを使用することで、この目的を達成できます。Grid Manager （ UI と API の両方）で * テナントの root パスワードの変更 * 機能を完全に非アクティブ化することで、 A 社は、 root ユーザおよび * Root Access * 権限を持つグループに属するユーザを含むすべての Admin ユーザが、任意のテナントアカウントの root ユーザのパスワードを変更できるようにすることができます。 _

手順

1. Swagger のグリッド管理 API のドキュメントにアクセスします。を参照してください "グリッド管理 API を使用します"。
2. Deactivate Features エンドポイントを探します。
3. テナントの root パスワードの変更などの機能を非アクティブ化するには、次のような本文を API に送信します。

   ```
   { "grid": {"changeTenantRootPassword": true} }
   ```

   要求が完了すると、テナントの root パスワードの変更機能が無効になります。テナントの root パスワードを変更する * 管理権限がユーザインターフェイスに表示されなくなり、テナントの root パスワードを変更する API 要求はすべて「 403 Forbidden 」エラーで失敗します。

非アクティブ化した機能を再アクティブ

デフォルトでは、グリッド管理 API を使用して、非アクティブ化した機能を再アクティブ化できます。ただし、非アクティブ化された機能が再アクティブ化されないようにするには、 * activateFeatures * 機能自体を非アクティブ化します。

> *activateFeatures*機能を再度有効にすることはできません。この機能を非アクティブ化すると、非アクティブ化した他の機能を永続的に再アクティブ化できなくなることに注意してください。失われた機能をリストアするには、テクニカルサポートにお問い合わせください。

手順

1. Swagger のグリッド管理 API のドキュメントにアクセスします。

2. Deactivate Features エンドポイントを探します。
3. すべての機能を再アクティブ化するには、次のような本文を API に送信します。

```
{ "grid": null }
```

この要求が完了すると、テナントの root パスワード変更機能を含むすべての機能が再アクティブ化されます。ユーザに * Root access * 権限または * Change tenant root password * 管理権限が割り当てられている場合、テナントの root パスワードを変更する API 要求はすべてユーザインターフェイスに表示され、テナントの root パスワードを変更する API 要求は成功します。

> ⓘ 前述の例は、 _all_deactivated 機能を再アクティブ化します。非アクティブ化したままにする必要がある他の機能が非アクティブ化されている場合は、 PUT 要求でそれらを明示的に指定する必要があります。たとえば、テナントのルートパスワード変更機能を再アクティブ化し、アラーム確認応答機能を非アクティブ化し続けるには、次の PUT 要求を送信します。
>
> ```
> { "grid": { "alarmAcknowledgment": true } }
> ```

StorageGRID へのアクセスを制御します

StorageGRID アクセスの制御：概要

StorageGRID にアクセスできるユーザ、およびユーザが実行できるタスクを制御するには、グループとユーザを作成またはインポートし、各グループに権限を割り当てます。必要に応じて、シングルサインオン（ SSO ）を有効にしたり、クライアント証明書を作成したり、グリッドのパスワードを変更したりできます。

Grid Manager へのアクセスを制御

Grid Manager およびグリッド管理 API にアクセスできるユーザを指定するには、アイデンティティフェデレーションサービスからグループとユーザをインポートするか、またはローカルのグループおよびユーザを設定します。

を使用します "アイデンティティフェデレーション" 設定を行います "グループ" および "ユーザ" また、使い慣れたクレデンシャルを使用してStorageGRID にサインインできます。Active Directory 、 OpenLDAP 、または Oracle Directory Server を使用する場合は、アイデンティティフェデレーションを設定できます。

> ⓘ 別の LDAP v3 サービスを使用する場合は、テクニカルサポートにお問い合わせください。

各ユーザが実行できるタスクを指定するには、異なるを割り当てます "権限" 各グループに。たとえば、あるグループのユーザには ILM ルールを管理する権限を、別のグループのユーザにはメンテナンスタスクを実行する権限を与えることができます。システムにアクセスするには、ユーザが少なくとも 1 つのグループに属している必要があります。

必要に応じて、グループを読み取り専用に設定することができます。読み取り専用グループのユーザは、設定と機能のみを表示できます。Grid Managerまたはグリッド管理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。

シングルサインオンを有効にします

StorageGRID システムでは、 Security Assertion Markup Language 2.0 （ SAML 2.0 ）標準を使用したシングルサインオン（ SSO ）がサポートされます。お先にどうぞ "SSOを設定して有効にします"の場合、Grid Manager、Tenant Manager、Grid管理API、またはテナント管理APIにアクセスするには、すべてのユーザが外部のアイデンティティプロバイダによって認証される必要があります。ローカルユーザはStorageGRID にサインインできません。

プロビジョニングパスフレーズを変更します

プロビジョニングパスフレーズは、多くのインストールやメンテナンスの手順、および StorageGRID リカバリパッケージのダウンロードで必要になります。また、 StorageGRID システムのグリッドトポロジ情報と暗号化キーのバックアップをダウンロードする際にもパスフレーズが必要です。可能です "パスフレーズを変更します" 必要に応じて。

ノードのコンソールパスワードを変更します

グリッド内の各ノードには一意のノードコンソールパスワードが設定されます。このパスワードは、SSHを使用してノードに「admin」としてログインするか、VM /物理コンソール接続の場合はrootユーザとしてログインする必要があります。必要に応じて、できます "ノードのコンソールパスワードを変更します" をクリックします。

プロビジョニングパスフレーズを変更します

この手順 を使用して、 StorageGRID プロビジョニングパスフレーズを変更します。パスフレーズは、リカバリ、拡張、およびメンテナンスの手順で必要になります。また、リカバリパッケージのバックアップをダウンロードする際にも、 StorageGRID システムのグリッドトポロジ情報、グリッドノードのコンソールパスワード、暗号化キーが含まれている必要があります。

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"。
- Maintenance または Root アクセス権限が必要です。
- 現在のプロビジョニングパスフレーズを用意します。

このタスクについて

プロビジョニングパスフレーズは、インストールやメンテナンスの手順の多くやで必要になります "リカバリパッケージをダウンロードしています"。プロビジョニングパスフレーズは、に表示されません `Passwords.txt` ファイル。プロビジョニングパスフレーズを記録して、安全な場所に保管してください。

手順

1. * 設定 * > * アクセス制御 * > * Grid パスワード * を選択します。
2. で、[変更]*を選択します
3. 現在のプロビジョニングパスフレーズを入力します。
4. 新しいパスフレーズを入力します。パスフレーズは 8 文字以上 32 文字以下にする必要があります。パスフレーズでは大文字と小文字が区別されます。
5. 新しいプロビジョニングパスフレーズを安全な場所に保存します。インストール、拡張、およびメンテナ

ンスの手順を実行する必要があります。

6. 新しいパスフレーズをもう一度入力し、「 * 保存 * 」を選択します。

   プロビジョニングパスフレーズの変更が完了すると、成功を示す緑のバナーが表示されます。

7. リカバリパッケージ * を選択します。
8. 新しいプロビジョニングパスフレーズを入力して、新しいリカバリパッケージをダウンロードします。

> プロビジョニングパスフレーズを変更したら、すぐに新しいリカバリパッケージをダウンロードする必要があります。リカバリパッケージファイルは、障害が発生した場合にシステムをリストアするために使用します。

ノードのコンソールパスワードを変更します

グリッド内の各ノードには、一意のノードコンソールパスワードが設定されています。このパスワードを使用してノードにログインする必要があります。次の手順に従って、グリッド内のノードごとに一意のノードコンソールパスワードを変更します。

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"。
- Maintenance または Root アクセス権限が必要です。
- 現在のプロビジョニングパスフレーズを用意します。

このタスクについて

ノードのコンソールパスワードを使用して、SSHを使用してノードに「admin」としてログインするか、VM / 物理コンソール接続でrootユーザにログインします。ノードコンソールパスワードの変更プロセスでは、グリッド内の各ノードに対して新しいパスワードが作成され、更新されたに格納されます `Passwords.txt` リカバリパッケージ内のファイル。パスワードは、 Passwords.txt ファイルの Password 列に表示されます。

> ノード間の通信に使用する SSH キー用に、個別の SSH アクセスパスワードがあります。SSH アクセスパスワードは、この手順 では変更されません。

ウィザードにアクセスします

手順

1. * 設定 * > * アクセス制御 * > * Grid パスワード * を選択します。
2. で、[変更する]*を選択します。

プロビジョニングパスフレーズを入力します

手順

1. グリッドのプロビジョニングパスフレーズを入力します。
2. 「 * Continue * 」を選択します。

現在のリカバリパッケージをダウンロードします

ノードコンソールのパスワードを変更する前に、現在のリカバリパッケージをダウンロードします。いずれかのノードでパスワードの変更プロセスが失敗した場合は、このファイルのパスワードを使用できます。

手順

1. [リカバリパッケージのダウンロード] を選択します。
2. リカバリパッケージファイルをコピーします (`.zip`)を2箇所に安全に、安全に、そして別 々 の場所に移動します。

   > リカバリパッケージファイルにはStorageGRID システムからデータを取得するための暗号キーとパスワードが含まれているため、安全に保管する必要があります。

3. 「 * Continue * 」を選択します。
4. 確認ダイアログが表示されたら、ノードコンソールのパスワードの変更を開始する準備ができている場合は*[はい]*を選択します。

   このプロセスは開始後にキャンセルすることはできません。

ノードのコンソールパスワードを変更します

ノードコンソールのパスワードのプロセスが開始されると、新しいパスワードを含む新しいリカバリパッケージが生成されます。その後、各ノードでパスワードが更新されます。

手順

1. 新しいリカバリパッケージが生成されるまで待ちます。これには数分かかることがあります。
2. [新しいリカバリパッケージのダウンロード] を選択します。
3. ダウンロードが完了したら、次の手順を実行

   a. を開きます `.zip` ファイル。

   b. などのコンテンツにアクセスできることを確認します `Passwords.txt` ファイル。ノードコンソールの新しいパスワードを格納します。

   c. 新しいリカバリパッケージファイルをコピーします (`.zip`)を2箇所に安全に、安全に、そして別 々 の場所に移動します。

      > 古いリカバリパッケージを上書きしないでください。

   リカバリパッケージファイルにはStorageGRID システムからデータを取得するための暗号キーとパスワードが含まれているため、安全に保管する必要があります。

4. 新しいリカバリパッケージをダウンロードして内容を確認したことを示すチェックボックスを選択します。
5. [ノードコンソールパスワードの変更]*を選択し、すべてのノードが新しいパスワードで更新されるまで待ちます。この処理には数分かかることがあります。

   すべてのノードでパスワードを変更した場合は、成功を示す緑のバナーが表示されます。次の手順に進みます。

更新プロセスでエラーが発生した場合は、バナーメッセージにパスワードを変更できなかったノードの数が表示されます。パスワードを変更できなかったノードに対して、処理が自動的に再試行されます。プロセスが終了してもパスワードが変更されていないノードがある場合は、「 * Retry * 」ボタンが表示されます。

1 つ以上のノードでパスワードの更新に失敗した場合：

a. 表に表示されたエラーメッセージを確認します。

b. 問題を解決します。

c. [* Retry*] を選択します。

> ⓘ 再試行すると、前回のパスワード変更で失敗したノード上のノードコンソールパスワードのみが変更されます。

6. すべてのノードのノードコンソールパスワードを変更したら、を削除します 最初にダウンロードしたリカバリパッケージ。
7. 必要に応じて、*[リカバリパッケージ]*リンクを使用して、新しいリカバリパッケージの追加コピーをダウンロードします。

アイデンティティフェデレーションを使用する

アイデンティティフェデレーションを使用すると、グループやユーザを迅速に設定できます。また、ユーザは使い慣れたクレデンシャルを使用して StorageGRID にサインインできます。

Grid Manager のアイデンティティフェデレーションを設定する

管理者グループとユーザを Active Directory 、 Azure Active Directory （ Azure AD ）、 OpenLDAP 、 Oracle Directory Server などの別のシステムで管理する場合は、 Grid Manager でアイデンティティフェデレーションを設定できます。

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"。
- 特定のアクセス権限が必要です。
- アイデンティティプロバイダとして Active Directory 、 Azure AD 、 OpenLDAP 、または Oracle Directory Server を使用している。

> ⓘ 記載されていない LDAP v3 サービスを使用する場合は、テクニカルサポートにお問い合わせください。

- OpenLDAP を使用する場合は、 OpenLDAP サーバを設定する必要があります。を参照してください OpenLDAP サーバの設定に関するガイドライン。
- シングルサインオン（ SSO ）を有効にする場合は、を確認しておきます "シングルサインオンの要件と考慮事項"。
- LDAP サーバとの通信に Transport Layer Security （ TLS ）を使用する場合は、アイデンティティプロバイダが TLS 1.2 または 1.3 を使用しています。を参照してください "発信 TLS 接続でサポートされる暗号"。

このタスクについて

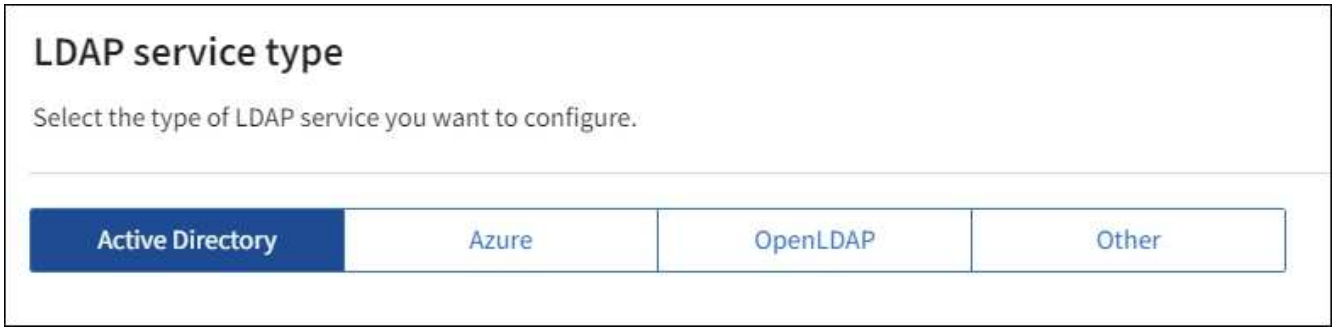
Active Directory 、 Azure AD 、 OpenLDAP 、 Oracle Directory Server などの別のシステムからグループをインポートする場合は、 Grid Manager のアイデンティティソースを設定できます。インポートできるグループのタイプは次のとおりです。

- 管理者グループ。管理者グループ内のユーザは、グループに割り当てられた管理権限に基づいて、 Grid Manager にサインインしてタスクを実行できます。
- 独自のアイデンティティソースを使用しないテナントのテナントユーザグループ。テナントグループ内のユーザは、 Tenant Manager でグループに割り当てられた権限に基づいてタスクを実行し、 Tenant Manager にサインインしてタスクを実行できます。を参照してください "テナントアカウントを作成する" および "テナントアカウントを使用する" を参照してください。

設定を入力します

手順

1. [* 設定 * > * アクセス制御 * > * アイデンティティフェデレーション *] を選択します。
2. [* アイデンティティフェデレーションを有効にする *] を選択
3. LDAP サービスタイプセクションで、設定する LDAP サービスのタイプを選択します。



Oracle Directory Server を使用する LDAP サーバーの値を設定するには、 * その他 * を選択します。

4. [* その他 *] を選択した場合は、 [LDAP 属性] セクションのフィールドに入力します。それ以外の場合は、次の手順に進みます。
   - * User Unique Name * ： LDAP ユーザの一意な ID が含まれている属性の名前。この属性はと同じです `sAMAccountName` Active Directoryおよびの場合 `uid` OpenLDAPの場合。Oracle Directory Server を設定する場合は、と入力します `uid`。
   - * User UUID * ： LDAP ユーザの永続的な一意な ID が含まれている属性の名前。この属性はと同じです `objectGUID` Active Directoryおよびの場合 `entryUUID` OpenLDAPの場合。Oracle Directory Serverを設定する場合は、と入力します `nsuniqueid`。指定した属性の各ユーザの値は、 16 バイトまたは文字列形式の 32 桁の 16 進数である必要があります。ハイフンは無視されます。
   - * Group Unique Name * ： LDAP グループの一意な ID が含まれている属性の名前。この属性はと同じです `sAMAccountName` Active Directoryおよびの場合 `cn` OpenLDAPの場合。Oracle Directory Server を設定する場合は、と入力します `cn`。
   - * グループ UUID * ： LDAP グループの永続的な一意な ID が含まれている属性の名前。この属性はと同じです `objectGUID` Active Directoryおよびの場合 `entryUUID` OpenLDAPの場合。Oracle Directory Serverを設定する場合は、と入力します `nsuniqueid`。指定した属性の各グループの値は、 16 バイトまたは文字列形式の 32 桁の 16 進数である必要があります。ハイフンは無視されます。
5. すべての LDAP サービスタイプについて、 LDAP サーバの設定セクションに必要な LDAP サーバおよび

ネットワーク接続情報を入力します。

- * Hostname * ： LDAP サーバの完全修飾ドメイン名（ FQDN ）または IP アドレス。
- * Port * ： LDAP サーバへの接続に使用するポート。

> STARTTLS のデフォルトポートは 389 、 LDAPS のデフォルトポートは 636 です。ただし、ファイアウォールが正しく設定されていれば、任意のポートを使用できます。

- * Username * ： LDAP サーバに接続するユーザの識別名（ DN ）の完全パス。

  Active Directory の場合は、ダウンレベルログオン名またはユーザープリンシパル名を指定することもできます。

  指定するユーザには、グループおよびユーザを表示する権限、および次の属性にアクセスする権限が必要です。

  - `sAMAccountName` または `uid`
  - `objectGUID`、 `entryUUID`` または `nsuniqueid`
  - `cn`
  - `memberOf` または `isMemberOf`
  - * Active Directory *： `objectSid`、 `primaryGroupID`、 `userAccountControl`` および `userPrincipalName`
  - * Azure *： `accountEnabled` および `userPrincipalName`
- * Password * ：ユーザ名に関連付けられたパスワード。
- * Group Base DN * ：グループを検索する LDAP サブツリーの識別名（ DN ）の完全パス。Active Directory では、ベース DN に対して相対的な識別名（ DC=storagegrid 、 DC=example 、 DC=com など）のグループをすべてフェデレーテッドグループとして使用できます。

> * グループの一意な名前 * 値は、所属する * グループベース DN * 内で一意である必要があります。

- * User Base DN * ：ユーザを検索する LDAP サブツリーの識別名（ DN ）の完全パス。

> * ユーザーの一意な名前 * 値は、それぞれが属する * ユーザーベース DN * 内で一意である必要があります。

- ユーザー名のバインド形式（オプション）：パターンを自動的に決定できない場合にStorageGRID が使用するデフォルトのユーザー名パターン。

  StorageGRID がサービスアカウントにバインドできない場合にユーザがサインインできるようにするため、 * バインドユーザ名形式 * を指定することを推奨します。

  次のいずれかのパターンを入力します。

  - * UserPrincipalNameパターン（Active DirectoryおよびAzure）*： `[USERNAME]@*example*.com`
  - 下位レベルのログオン名パターン（**Active Directory**および**Azure**）： `*example*\[USERNAME]`

- 識別名パターン： `CN=[USERNAME],CN=Users,DC=example,DC=com`

  記載されているとおりに * [username] * を含めます。

6. Transport Layer Security （ TLS ）セクションで、セキュリティ設定を選択します。
   - * STARTTLS を使用 * ： STARTTLS を使用して LDAP サーバとの通信を保護します。Active Directory 、 OpenLDAP 、またはその他のオプションですが、 Azure ではこのオプションはサポートされていません。
   - * LDAPS を使用 * ： LDAPS （ LDAP over SSL ）オプションでは、 TLS を使用して LDAP サーバへの接続を確立します。Azure ではこのオプションを選択する必要があります。
   - * TLS を使用しないでください * ： StorageGRID システムと LDAP サーバの間のネットワークトラフィックは保護されません。このオプションは Azure ではサポートされていません。

   > Active Directory サーバで LDAP 署名が適用される場合、 [TLS を使用しない] オプションの使用はサポートされていません。STARTTLS または LDAPS を使用する必要があります。

7. STARTTLS または LDAPS を選択した場合は、接続の保護に使用する証明書を選択します。
   - * オペレーティングシステムの CA 証明書を使用 * ：オペレーティングシステムにインストールされているデフォルトの Grid CA 証明書を使用して接続を保護します。
   - * カスタム CA 証明書を使用 * ：カスタムセキュリティ証明書を使用します。

     この設定を選択した場合は、カスタムセキュリティ証明書をコピーして CA 証明書テキストボックスに貼り付けます。

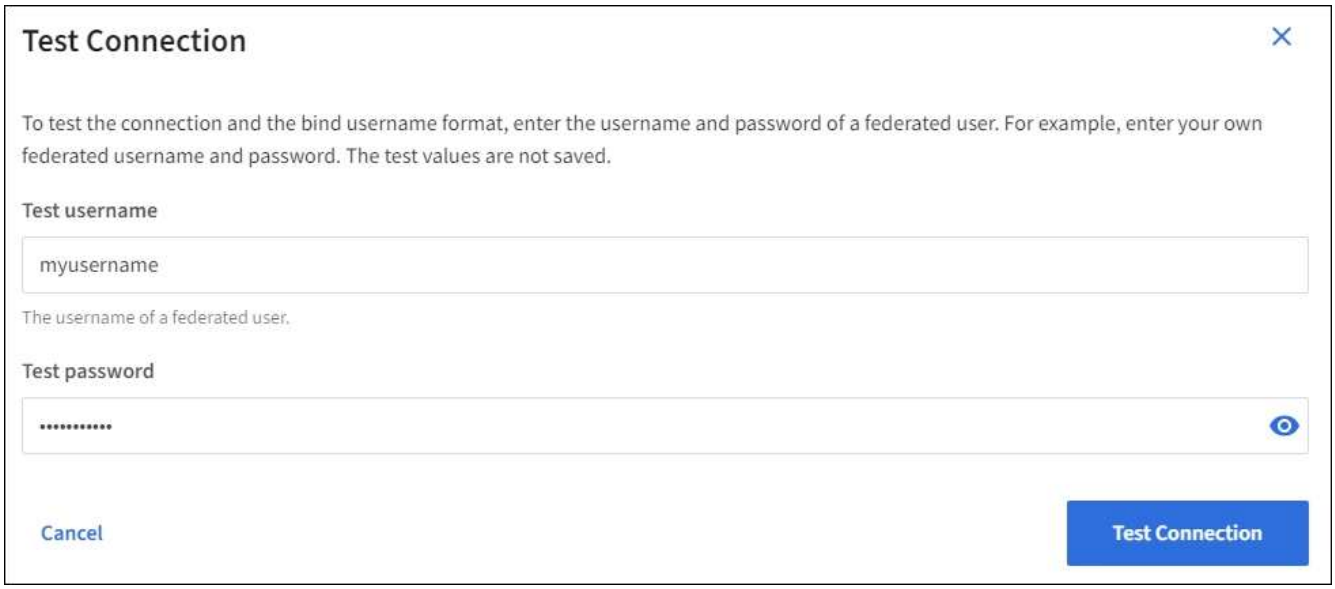
接続をテストして設定を保存します

すべての値を入力したら、設定を保存する前に接続をテストする必要があります。StorageGRID では、 LDAP サーバの接続設定とバインドユーザ名の形式が指定されている場合は検証されます。

手順

1. [接続のテスト *] を選択します。
2. バインドユーザ名の形式を指定しなかった場合は、次の手順を実行します。
   - 接続設定が有効である場合は、「 Test connection successful(接続のテストに成功しました) 」というメッセージが表示されます。[保存（ Save ）] を選択して、構成を保存します。
   - 接続設定が無効な場合は、「 test connection could not be established 」というメッセージが表示されます。[閉じる（ Close ）] を選択します。その後、問題を解決して接続を再度テストします。
3. バインドユーザ名の形式を指定した場合は、有効なフェデレーテッドユーザのユーザ名とパスワードを入力します。

   たとえば、自分のユーザ名とパスワードを入力します。ユーザ名に特殊文字（@、/など）を使用しないでください。



- 接続設定が有効である場合は、「 Test connection successful(接続のテストに成功しました) 」というメッセージが表示されます。[保存（ Save ）] を選択して、構成を保存します。
- 接続設定、バインドユーザ名形式、またはテストユーザ名とパスワードが無効な場合は、エラーメッセージが表示されます。問題を解決してから、もう一度接続をテストしてください。

アイデンティティソースとの強制同期

StorageGRID システムは、アイデンティティソースからフェデレーテッドグループおよびユーザを定期的に同期します。ユーザの権限をすぐに有効にしたり制限したりする必要がある場合は、同期を強制的に開始できます。

手順

1. アイデンティティフェデレーションページに移動します。
2. ページの上部にある「 * サーバーを同期」を選択します。

   環境によっては、同期プロセスにしばらく時間がかかることがあります。

   アイデンティティフェデレーション同期エラー * アラートは、アイデンティティソースからフェデレーテッドグループとユーザを同期する問題 がある場合にトリガーされます。

アイデンティティフェデレーションを無効にする

グループとユーザのアイデンティティフェデレーションを一時的または永続的に無効にすることができます。アイデンティティフェデレーションを無効にすると、 StorageGRID とアイデンティティソース間のやり取りは発生しません。ただし、設定は保持されるため、簡単に再度有効にすることができます。

このタスクについて

アイデンティティフェデレーションを無効にする前に、次の点に注意してください。

- フェデレーテッドユーザはサインインできなくなります。
- 現在サインインしているフェデレーテッドユーザは、セッションが有効な間は StorageGRID システムに引き続きアクセスできますが、セッションが期限切れになると以降はサインインできなくなります。

- StorageGRID システムとアイデンティティソース間の同期は行われず、同期されていないアカウントに対してはアラートやアラームが生成されません。
- シングルサインオン（SSO）が*有効*または*サンドボックスモード*に設定されている場合、*アイデンティティフェデレーションを有効にする*チェックボックスは無効になります。アイデンティティフェデレーションを無効にするには、シングルサインオンページの SSO ステータスが * 無効 * になっている必要があります。を参照してください "シングルサインオンを無効にします"。

手順

1. アイデンティティフェデレーションページに移動します。
2. [アイデンティティフェデレーションを有効にする]*チェックボックスをオフにします。

OpenLDAP サーバの設定に関するガイドライン

アイデンティティフェデレーションに OpenLDAP サーバを使用する場合は、 OpenLDAP サーバで特定の設定が必要です。

> ActiveDirectoryやAzure以外のアイデンティティソースの場合、StorageGRID は外部で無効にしたユーザへのS3アクセスを自動的にブロックしません。S3アクセスをブロックするには、そのユーザのS3キーをすべて削除するか、すべてのグループからユーザを削除します。

memberof オーバーレイと **refint** オーバーレイ

memberof オーバーレイと refint オーバーレイを有効にする必要があります。詳細については、のリバースグループメンバーシップのメンテナンス手順を参照してくださいhttp://www.openldap.org/doc/admin24/index.html["OpenLDAP のドキュメント：バージョン 2.4 管理者ガイド"^]。

インデックス作成

次の OpenLDAP 属性とインデックスキーワードを設定する必要があります。

- `olcDbIndex: objectClass eq`
- `olcDbIndex: uid eq,pres,sub`
- `olcDbIndex: cn eq,pres,sub`
- `olcDbIndex: entryUUID eq`

また、パフォーマンスを最適化するには、 Username のヘルプで説明されているフィールドにインデックスを設定してください。

のリバースグループメンバーシップのメンテナンスに関する情報を参照してくださいhttp://www.openldap.org/doc/admin24/index.html["OpenLDAP のドキュメント：バージョン 2.4 管理者ガイド"^]。

管理者グループを管理する

管理者グループを作成して、 1 人以上の管理者ユーザのセキュリティ権限を管理できます。StorageGRID システムへのアクセスを許可するには、ユーザがグループに属している必要があります。

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"。
- 特定のアクセス権限が必要です。
- フェデレーテッドグループをインポートする場合は、アイデンティティフェデレーションを設定済みで、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ている必要があります。

管理者グループを作成します

管理者グループを使用すると、 Grid Manager およびグリッド管理 API のどのユーザがどの機能や処理にアクセスできるかを決定できます。

ウィザードにアクセスします

手順

1. * configuration * > * Access control * > * Admin 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。

- ローカルユーザに権限を割り当てる場合は、ローカルグループを作成します。
- アイデンティティソースからユーザをインポートするためのフェデレーテッドグループを作成します。

ローカルグループ

手順

1. * ローカルグループ * を選択します。
2. グループの表示名を入力します。必要に応じてあとから更新できます。たとえば、「 Maintenance Users 」または「 ILM Administrators 」のようになります。
3. グループの一意の名前を入力します。この名前は後で更新できません。
4. 「 * Continue * 」を選択します。

フェデレーテッドグループ

手順

1. [フェデレーショングループ] を選択します。
2. インポートするグループの名前を、設定されているアイデンティティソースに表示されているとおりに入力します。
   - Active Directory および Azure の場合は、 sAMAccountName を使用します。
   - OpenLDAP の場合は、 CN （共通名）を使用します。
   - 別の LDAP を使用する場合は、 LDAP サーバに適切な一意の名前を使用します。
3. 「 * Continue * 」を選択します。

グループの権限を管理します

手順

1. * アクセスモード * では、グループ内のユーザが Grid Manager およびグリッド管理 API で設定の変更や処理を実行できるかどうか、あるいは設定と機能のみを表示できるかどうかを選択します。
   - * 読み取り / 書き込み * （デフォルト）：ユーザは設定を変更し、管理権限で許可されている操作を実行できます。
   - * 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。Grid Managerまたはグリッド管理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。

   ユーザー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 * に設定されている場合、ユーザーは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. 1 つ以上を選択します "管理者グループの権限"。

   各グループに 1 つ以上の権限を割り当てる必要があります。そうしないと、グループに属するユーザは StorageGRID にサインインできません。

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）

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、ユーザを追加せずにグループを保存できます。このグループは、ユーザページでユーザに追加できます。を参照してください"ユーザを管理します" を参照してください。

2. [グループの作成 *] と [完了 *] を選択します。

管理者グループを表示および編集します

既存のグループの詳細の表示、グループの変更、またはグループの複製を行うことができます。

- すべてのグループの基本情報を表示するには '[グループ] ページの表を確認します
- 特定のグループのすべての詳細を表示したり、グループを編集したりするには、 * アクション * メニューまたは詳細ページを使用します。

タスク	[アクション] メニュー	詳細ページ
グループの詳細を表示します	a. グループのチェックボックスをオンにします。 b. [* アクション * > * グループの詳細を表示 *] を選択します。	テーブルでグループ名を選択します。

タスク	[アクション] メニュー	詳細ページ
表示名の編集（ローカルグループのみ）	a. グループのチェックボックスをオンにします。 b. [* アクション * > * 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。	a. グループ名を選択して詳細を表示します。 b. 編集アイコンを選択します 。 c. 新しい名前を入力します。 d. 「変更を保存」を選択します。
アクセスモードまたは権限を編集します	a. グループのチェックボックスをオンにします。 b. [* アクション * > * グループの詳細を表示 *] を選択します。 c. 必要に応じて、グループのアクセスモードを変更します。 d. 必要に応じて、を選択または選択解除します "管理者グループの権限"。 e. 「変更を保存」を選択します。	a. グループ名を選択して詳細を表示します。 b. 必要に応じて、グループのアクセスモードを変更します。 c. 必要に応じて、を選択または選択解除します "管理者グループの権限"。 d. 「変更を保存」を選択します。

グループを複製します

手順

1. グループのチェックボックスをオンにします。
2. [* アクション * > * グループの複製 *] を選択します。
3. グループ複製ウィザードを完了します。

グループを削除します

管理者グループを削除すると、システムからそのグループを削除し、グループに関連付けられているすべての権限を削除できます。管理者グループを削除すると、そのグループからすべてのユーザが削除されますが、ユーザは削除されません。

手順

1. [Groups]ページで、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。
2. [* アクション * > * グループの削除 *] を選択します。
3. 「 * グループを削除する * 」を選択します。

管理者グループの権限

管理者ユーザグループを作成する場合は、 Grid Manager の特定の機能へのアクセスを制御する権限を 1 つ以上選択します。その後、作成した 1 つ以上の管理者グループに各ユーザを割り当てて、ユーザが実行できるタスクを決定できます。

各グループに 1 つ以上の権限を割り当てる必要があります。そうしないと、そのグループに属するユーザは Grid Manager またはグリッド管理 API にサインインできません。

デフォルトでは、少なくとも 1 つの権限が割り当てられたグループに属するユーザは次のタスクを実行できます。

- Grid Manager にサインインします
- ダッシュボードを表示します
- ノードページを表示します
- グリッドトポロジを監視する
- 現在のアラートと解決済みのアラートを表示します
- 現在のアラームと履歴アラームの表示（従来のシステム）
- 自分のパスワードを変更する（ローカルユーザのみ）
- [Configuration]ページと[Maintenance]ページに表示される特定の情報を確認します

権限とアクセスモードの相互作用

すべての権限について、グループの * アクセスモード * 設定は、ユーザーが設定を変更して操作を実行できるかどうか、または関連する設定と機能のみを表示できるかどうかを決定します。ユーザー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 * に設定されている場合、ユーザーは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。

以降のセクションでは、管理者グループの作成時または編集時に割り当てることができる権限について説明します。明示的に言及されていない機能には、 * Root Access * 権限が必要です。

ルートアクセス

この権限は、すべてのグリッド管理機能へのアクセスを許可します。

アラームへの確認応答（レガシー）

アラームの確認と応答を許可します（従来型システム）。サインインしたすべてのユーザが現在のアラームと履歴アラームを表示できます。

ユーザにグリッドトポロジの監視とアラームへの確認応答だけを許可するには、この権限を割り当てる必要があります。

テナントの **root** パスワードを変更する

この権限は、テナントページの * root パスワードの変更 * オプションへのアクセスを許可し、テナントのローカル root ユーザのパスワードを変更できるユーザを制御することを可能にします。この権限は、 S3 キーのインポート機能が有効になっている場合に S3 キーの移行にも使用されます。この権限がないユーザには、 * rootパスワードの変更*オプションが表示されません。

> Change root password * オプションが含まれている tenants ページへのアクセスを許可するには、 * Tenant accounts * 権限を割り当てます。

Grid トポロジページの設定

この権限では、サポート * > * ツール * > * グリッドトポロジ * ページの構成タブにアクセスできます。

ILM

この権限は、次の * ILM * メニュー・オプションへのアクセスを提供します。

- ルール
- ポリシー
- イレイジャーコーディング
- リージョン
- ストレージプール

> ストレージグレードを管理するには、ユーザに * Other Grid Configuration * 権限と * Grid Topology Page Configuration * 権限が必要です。

メンテナンス

これらのオプションを使用するには、 Maintenance 権限が必要です。

- * 設定 * > * アクセス制御 * ：
  - Grid のパスワード
- * 設定 * > * ネットワーク * ：
  - S3エンドポイントのドメイン名
- * メンテナンス * > * タスク * ：
  - 運用停止
  - 拡張
  - オブジェクトの存在チェック
  - リカバリ
- * メンテナンス * > * システム * ：
  - リカバリパッケージ
  - ソフトウェアの更新
- * サポート * > * ツール * ：
  - ログ

Maintenance権限がないユーザは、次のページを表示できますが、編集はできません。

- * メンテナンス * > * ネットワーク * ：
  - DNS サーバ
  - Grid ネットワーク

- NTP サーバ

- * メンテナンス * > * システム * ：
  - 使用許諾
- * 設定 * > * ネットワーク * ：
  - S3エンドポイントのドメイン名
- * 設定 * > * セキュリティ * ：
  - 証明書
- * コンフィグレーション * > * モニタリング * ：
  - 監査と syslog サーバ

アラートの管理

この権限では、アラートを管理するためのオプションにアクセスできます。サイレンス、アラート通知、アラートルールを管理するには、この権限が必要です。

指標クエリ

この権限により、次の項目にアクセスできます。

- サポート>*ツール*>*メトリクス*ページ
- グリッド管理API*[Metrics]*セクションを使用したカスタムのPrometheus指標クエリ
- Grid Managerの指標を含むダッシュボードカード

オブジェクトメタデータの検索

この権限は、 * ILM * > * Object metadata lookup * ページへのアクセスを提供します。

その他のグリッド設定

この権限で、追加のグリッド設定オプションにアクセスできます。

これらの追加オプションを表示するには、ユーザに * Grid トポロジページの設定 * 権限が必要です。

- * ILM * ：
  - ストレージグレード
- * コンフィグレーション * > * システム * ：
  - ストレージオプション
- * サポート * > * アラーム（レガシー） * ：
  - カスタムイベント
  - グローバルアラーム
  - 従来の E メール設定

- サポート>*その他*：
  - リンクコスト

ストレージアプライアンス管理者

この権限は、グリッドマネージャを介してストレージアプライアンスの E シリーズ SANtricity システムマネージャにアクセスすることを許可します。

テナントアカウント

この権限により、次のことが可能になります。

- [Tenants]ページにアクセスします。このページで、テナントアカウントを作成、編集、削除できます
- 既存のトラフィック分類ポリシーを表示します
- テナントの詳細を含むGrid Managerのダッシュボードカードを表示します

ユーザを管理します

ローカルユーザとフェデレーテッドユーザを表示できます。また、ローカルユーザを作成してローカル管理者グループに割り当て、そのユーザがアクセスできる Grid Manager 機能を決定することもできます。

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"。
- 特定のアクセス権限が必要です。

ローカルユーザを作成します

1 人以上のローカルユーザを作成し、各ユーザを 1 つ以上のローカルグループに割り当てることができます。このグループの権限は、ユーザがアクセスできる Grid Manager および Grid 管理 API 機能を制御します。

作成できるのはローカルユーザのみです。外部のアイデンティティソースを使用して、フェデレーテッドユーザとフェデレーテッドグループを管理します。

Grid Managerには、「root」という名前の事前定義されたローカルユーザが1人含まれています。 rootユーザは削除できません。

シングルサインオン（SSO）が有効になっている場合、ローカルユーザはStorageGRID にサインインできません。

ウィザードにアクセスします

手順

1. [* 設定 * > * アクセス制御 * > * 管理者ユーザー *] を選択します。
2. 「 * ユーザーの作成 * 」を選択します。

ユーザクレデンシャルを入力します

手順

1. ユーザのフルネーム、一意なユーザ名、およびパスワードを入力します。
2. 必要に応じて、このユーザに Grid Manager または Grid 管理 API へのアクセスを禁止する場合は「 * Yes 」を選択します。
3. 「 * Continue * 」を選択します。

グループに割り当てます

手順

1. 必要に応じて、ユーザを 1 つ以上のグループに割り当てて、そのユーザの権限を決定します。

   まだグループを作成していない場合は、グループを選択せずにユーザを保存できます。このユーザーは、[グループ] ページでグループに追加できます。

   ユーザが複数のグループに属している場合は、権限の累積数が算出されます。を参照してください"管理者グループを管理する" を参照してください。

2. [Create user*] を選択し、 [**Finish**] を選択します。

ローカルユーザを表示および編集します

既存のローカルユーザとフェデレーテッドユーザの詳細を表示できます。ローカルユーザを変更して、ユーザのフルネーム、パスワード、またはグループメンバーシップを変更できます。また、ユーザが Grid Manager およびグリッド管理 API にアクセスすることを一時的に禁止することもできます。

編集できるのはローカルユーザのみです。外部のアイデンティティソースを使用してフェデレーテッドユーザを管理します。

- すべてのローカルユーザとフェデレーテッドユーザの基本情報を表示するには、ユーザページのテーブルを確認してください。
- 特定のユーザの詳細をすべて表示したり、ローカルユーザを編集したり、ローカルユーザのパスワードを変更したりするには、 * Actions * メニューまたは詳細ページを使用します。

  編集内容は、次回ユーザがグリッドマネージャからサインアウトして再度サインインしたときに適用されます。

  ローカルユーザは、Grid Managerのバナーの*[パスワードの変更]*オプションを使用して自分のパスワードを変更できます。

タスク	[アクション] メニュー	詳細ページ
ユーザの詳細を表示します	a. ユーザのチェックボックスを選択します。 b. [* アクション * > * ユーザーの詳細を表示 *] を選択します。	テーブルでユーザの名前を選択します。

タスク	[アクション] メニュー	詳細ページ
フルネームの編集（ローカルユーザのみ）	a. ユーザのチェックボックスを選択します。 b. * アクション * > * フルネームの編集 * 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。	a. 詳細を表示するユーザの名前を選択します。 b. 編集アイコンを選択します 。 c. 新しい名前を入力します。 d. 「変更を保存」を選択します。
StorageGRID アクセスを拒否または許可します	a. ユーザのチェックボックスを選択します。 b. [* アクション * > * ユーザーの詳細を表示 *] を選択します。 c. [アクセス] タブを選択します。 d. ユーザが Grid Manager または Grid 管理 API にサインインできないようにするには「 * Yes 」を選択します。サインインできるようにするには、「 * No * 」を選択します。 e. 「変更を保存」を選択します。	a. 詳細を表示するユーザの名前を選択します。 b. [アクセス] タブを選択します。 c. ユーザが Grid Manager または Grid 管理 API にサインインできないようにするには「 * Yes 」を選択します。サインインできるようにするには、「 * No * 」を選択します。 d. 「変更を保存」を選択します。
パスワードを変更（ローカルユーザのみ）	a. ユーザのチェックボックスを選択します。 b. [* アクション * > * ユーザーの詳細を表示 *] を選択します。 c. [パスワード] タブを選択します。 d. 新しいパスワードを入力します。 e. 「 * パスワードの変更 * 」を選択します。	a. 詳細を表示するユーザの名前を選択します。 b. [パスワード] タブを選択します。 c. 新しいパスワードを入力します。 d. 「 * パスワードの変更 * 」を選択します。
変更グループ（ローカルユーザのみ）	a. ユーザのチェックボックスを選択します。 b. [* アクション * > * ユーザーの詳細を表示 *] を選択します。 c. [グループ] タブを選択します。 d. 必要に応じて、グループ名のあとのリンクを選択し、新しいブラウザタブでグループの詳細を表示します。 e. 「 * グループを編集」を選択して、別のグループを選択します。 f. 「変更を保存」を選択します。	a. 詳細を表示するユーザの名前を選択します。 b. [グループ] タブを選択します。 c. 必要に応じて、グループ名のあとのリンクを選択し、新しいブラウザタブでグループの詳細を表示します。 d. 「 * グループを編集」を選択して、別のグループを選択します。 e. 「変更を保存」を選択します。

ユーザを複製します

既存のユーザを複製して、同じ権限を持つ新しいユーザを作成することができます。

手順

1. ユーザのチェックボックスを選択します。
2. * アクション * > * ユーザーの複製 * を選択します。
3. 複製ユーザーウィザードを完了します。

ユーザを削除します

ローカルユーザを削除して、そのユーザをシステムから完全に削除できます。

rootユーザは削除できません。

手順

1. [Users]ページで、削除する各ユーザのチェックボックスをオンにします。
2. * アクション * > * ユーザーの削除 * を選択します。
3. 「 * ユーザーの削除 * 」を選択します。

シングルサインオン（ **SSO** ）を使用

シングルサインオンを設定します

シングルサインオン（ SSO ）が有効な場合、ユーザは、組織によって実装された SSO サインインプロセスを使用してクレデンシャルが許可されている場合にのみ、 Grid Manager 、テナントマネージャ、 Grid 管理 API 、またはテナント管理 API にアクセスできます。ローカルユーザはStorageGRID にサインインできません。

シングルサインオンの仕組み

StorageGRID システムでは、 Security Assertion Markup Language 2.0 （ SAML 2.0 ）標準を使用したシングルサインオン（ SSO ）がサポートされます。

シングルサインオン（ SSO ）を有効にする前に、 SSO が有効になった場合に StorageGRID のサインインとサインアウトのプロセスにどのような影響があるかを確認してください。

SSO が有効な場合はサインインします

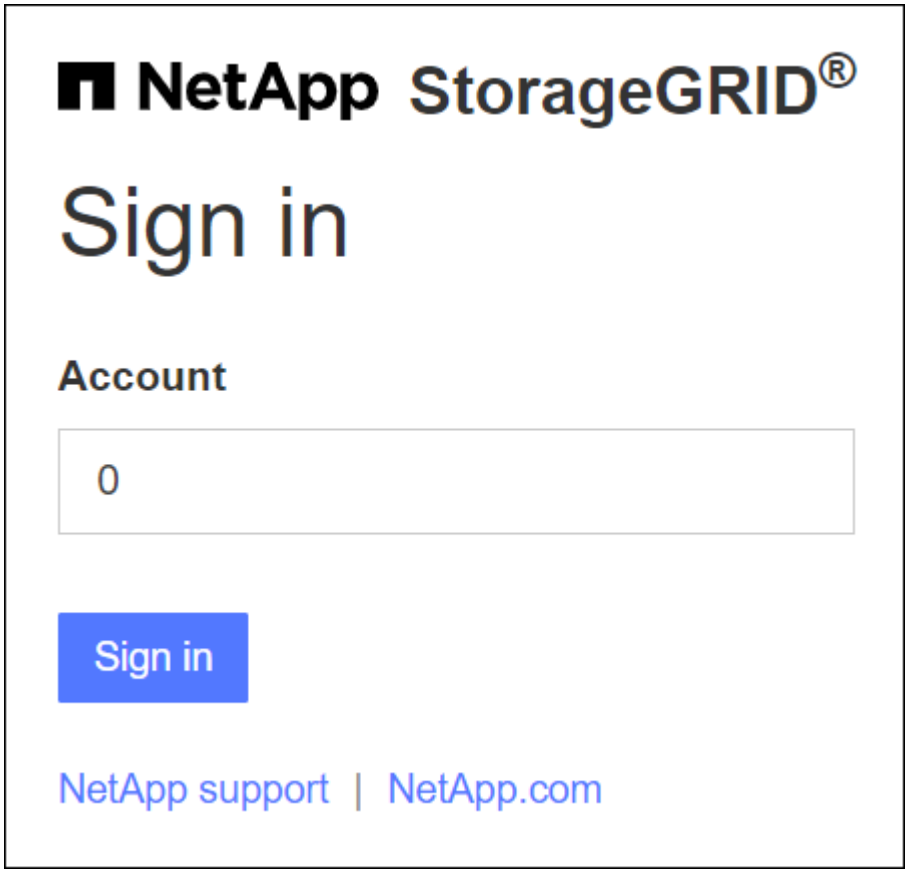
SSO が有効な場合に StorageGRID にサインインすると、組織の SSO ページにリダイレクトされてクレデンシャルが検証されます。

手順

1. Web ブラウザで、 StorageGRID 管理ノードの完全修飾ドメイン名または IP アドレスを入力します。

   StorageGRID のサインインページが表示されます。

- このブラウザで初めて URL にアクセスした場合は、アカウント ID の入力を求められます。

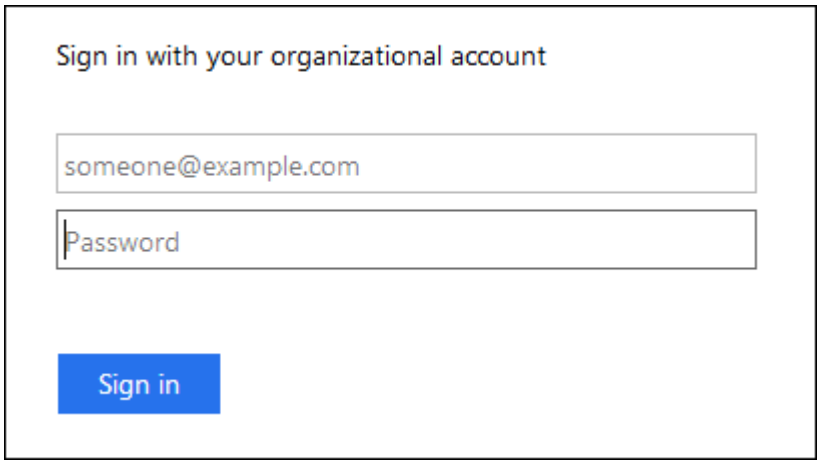


- Grid Manager または Tenant Manager に以前にアクセスしていた場合は、最近のアカウントを選択するか、アカウント ID を入力するように求められます。

テナントアカウントの完全なURL（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）を入力すると、StorageGRID のサインインページは表示されません `/?accountId=20-digit-account-id`）。代わりに、組織の SSO サインインページがすぐに表示されます。このページでは、を実行できます SSO クレデンシャルを使用してサインインします。

2. Grid Manager と Tenant Manager のどちらにアクセスするかを指定します。
   - Grid Manager にアクセスするには、 * Account ID * フィールドを空白のままにします。アカウント ID に「 * 0 」と入力するか、最近のアカウントのリストに * Grid Manager * が表示されている場合はそれを選択します。
   - Tenant Manager にアクセスするには、 20 桁のテナントアカウント ID を入力するか、最近のアカウントのリストにテナントが表示されている場合は名前でテナントを選択します。
3. 「サインイン」を選択します

   StorageGRID は、組織の SSO サインインページにリダイレクトします。例：



4. [[signin_soS] SSO クレデンシャルを使用してサインインします。

   SSO クレデンシャルが正しい場合：

   a. アイデンティティプロバイダ（ IdP ）が StorageGRID に認証応答を返します。
   b. StorageGRID が認証応答を検証します。
   c. 応答が有効で、 StorageGRID アクセス権限のあるフェデレーテッドグループに属している場合は、選択したアカウントに応じて、 Grid Manager またはテナントマネージャにサインインされます。

   サービスアカウントにアクセスできない場合でも、 StorageGRID アクセス権限を持つフェデレーテッドグループに属する既存のユーザであれば、サインインできます。

5. 必要に応じて、他の管理ノードにアクセスします。または、適切な権限がある場合は Grid Manager またはテナントマネージャにアクセスします。

   SSOクレデンシャルを再入力する必要はありません。

SSO が有効な場合はサインアウトします

StorageGRID で SSO が有効になっている場合にサインアウトするとどうなるかは、サインイン先とサインアウト元によって異なります。

手順

1. ユーザインターフェイスの右上隅にある[サインアウト]リンクを探します。
2. [サインアウト]*を選択します。

   StorageGRID のサインインページが表示されます。[Recent Accounts] * ドロップダウンが更新されて、 * Grid Manager * またはテナント名が表示されるようになり、これらのユーザインターフェイスにあとからすばやくアクセスできるようになります。

サインイン先	サインアウト元	サインアウトされる対象
1 つ以上の管理ノードでグリッドマネージャを使用します	任意の管理ノード上の Grid Manager	すべての管理ノード上の Grid Manager • 注： * SSO に Azure を使用している場合、すべての管理ノードからサインアウトするまでに数分かかることがあります。
1 つ以上の管理ノード上の Tenant Manager	任意の管理ノード上の Tenant Manager	すべての管理ノード上の Tenant Manager
Grid Manager と Tenant Manager の両方	Grid Manager の略	Grid Manager のみ。SSO からサインアウトするには、 Tenant Manager からもサインアウトする必要があります。

次の表は、単一のブラウザセッションを使用している場合にサインアウトしたときの動作をまとめたものです。複数のブラウザセッションで StorageGRID にサインインしている場合は、すべてのブラウザセッションから個別にサインアウトする必要があります。

シングルサインオンの要件と考慮事項

StorageGRID システムでシングルサインオン（SSO）を有効にする前に、要件と考慮事項を確認してください。

アイデンティティプロバイダの要件

StorageGRID では、次の SSO アイデンティティプロバイダ（ IdP ）をサポートしています。

- Active Directory フェデレーションサービス（ AD FS ）
- Azure Active Directory （ Azure AD ）
- PingFederate

SSO アイデンティティプロバイダを設定する前に、 StorageGRID システムのアイデンティティフェデレーションを設定する必要があります。アイデンティティフェデレーションに使用する LDAP サービスのタイプによって、実装できる SSO のタイプが制御されます。

LDAP サービスタイプが設定されました	**SSO** アイデンティティプロバイダのオプション
Active Directory	• Active Directory • Azure • PingFederate
Azure	Azure

AD FS の要件

次のいずれかのバージョンの AD FS を使用できます。

- Windows Server 2022 AD FS
- Windows Server 2019 AD FS
- Windows Server 2016 AD FS

> Windows Server 2016 でが使用されている必要があります "KB3201845 の更新プログラム"または それ以上。

- AD FS 3.0 （ Windows Server 2012 R2 Update 以降に付属）。

その他の要件

- Transport Layer Security （ TLS ） 1.2 または 1.3
- Microsoft .NET Framework バージョン 3.5.1 以降

Azureに関する考慮事項

SSOタイプとしてAzureを使用し、ユーザがsAMAccountNameをプレフィックスとして使用しないユーザプリンシパル名を持っている場合、StorageGRID がLDAPサーバとの接続を失うと、ログインの問題が発生する可能性があります。ユーザがサインインできるようにするには、LDAPサーバへの接続を復元する必要があります。

サーバ証明書の要件

デフォルトでは、 StorageGRID は各管理ノード上の管理インターフェイス証明書を使用して、 Grid Manager 、テナントマネージャ、グリッド管理 API 、およびテナント管理 API へのアクセスを保護します。StorageGRID 用の証明書利用者信頼（ AD FS ）、エンタープライズアプリケーション（ Azure ）、またはサービスプロバイダ接続（ PingFederate ）を設定するときは、 StorageGRID 要求の署名証明書としてサーバ証明書を使用します。

まだお持ちでない場合は "管理インターフェイス用のカスタム証明書を設定しました"では、今すぐ実行してください。インストールしたカスタムサーバ証明書はすべての管理ノードで使用され、すべての StorageGRID 証明書利用者信頼、エンタープライズアプリケーション、または SP 接続で使用できます。

管理ノードのデフォルトサーバ証明書を証明書利用者信頼、エンタープライズアプリケーション、または SP 接続で使用することは推奨されません。ノードに障害が発生した場合にそのノードをリカバリすると、新しいデフォルトサーバ証明書が生成されます。リカバリしたノードにサインインするには、証明書利用者信頼、エンタープライズアプリケーション、または SP 接続を新しい証明書で更新する必要があります。

管理ノードのサーバ証明書にアクセスするには、ノードのコマンドシェルにログインしてに移動します `/var/local/mgmt-api` ディレクトリ。カスタムサーバ証明書の名前はです `custom-server.crt`。ノードのデフォルトサーバ証明書の名前はです `server.crt`。

ポート要件

シングルサインオン（ SSO ）は、制限された Grid Manager ポートまたは Tenant Manager ポートでは使用できません。ユーザをシングルサインオンで認証する場合は、デフォルトの HTTPS ポート（ 443 ）を使用する必要があります。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"。

フェデレーテッドユーザがサインインできることを確認する

シングルサインオン（ SSO ）を有効にする前に、少なくとも 1 人のフェデレーテッドユーザが既存のテナントアカウント用に Grid Manager および Tenant Manager にサインインできることを確認する必要があります。

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"。
- 特定のアクセス権限が必要です。
- アイデンティティフェデレーションがすでに設定されている。

手順

1. 既存のテナントアカウントがある場合は、テナントが独自のアイデンティティソースを使用していないことを確認します。

   SSO を有効にすると、 Tenant Manager で設定されたアイデンティティソースが Grid Manager で設定されたアイデンティティソースによって上書きされます。テナントのアイデンティティソースに属するユーザは、 Grid Manager アイデンティティソースのアカウントがないかぎり、サインインできなくなります。

   a. 各テナントアカウントの Tenant Manager にサインインします。
   b. アクセス管理 * > * アイデンティティフェデレーション * を選択します。
   c. [アイデンティティフェデレーションを有効にする]*チェックボックスが選択されていないことを確認します。
   d. 該当する場合は、このテナントアカウントに使用されている可能性のあるフェデレーテッドグループが不要になったことを確認し、チェックボックスをオフにして*[保存]*を選択します。

2. フェデレーテッドユーザが Grid Manager にアクセスできることを確認します。
   a. Grid Manager から * configuration * > * Access control * > * Admin groups * を選択します。
   b. Active Directory アイデンティティソースから少なくとも 1 つのフェデレーテッドグループがインポートされていて、そのグループに Root アクセス権限が割り当てられていることを確認します。

c. サインアウトします。

d. フェデレーテッドグループ内のユーザとして Grid Manager に再度サインインできることを確認します。

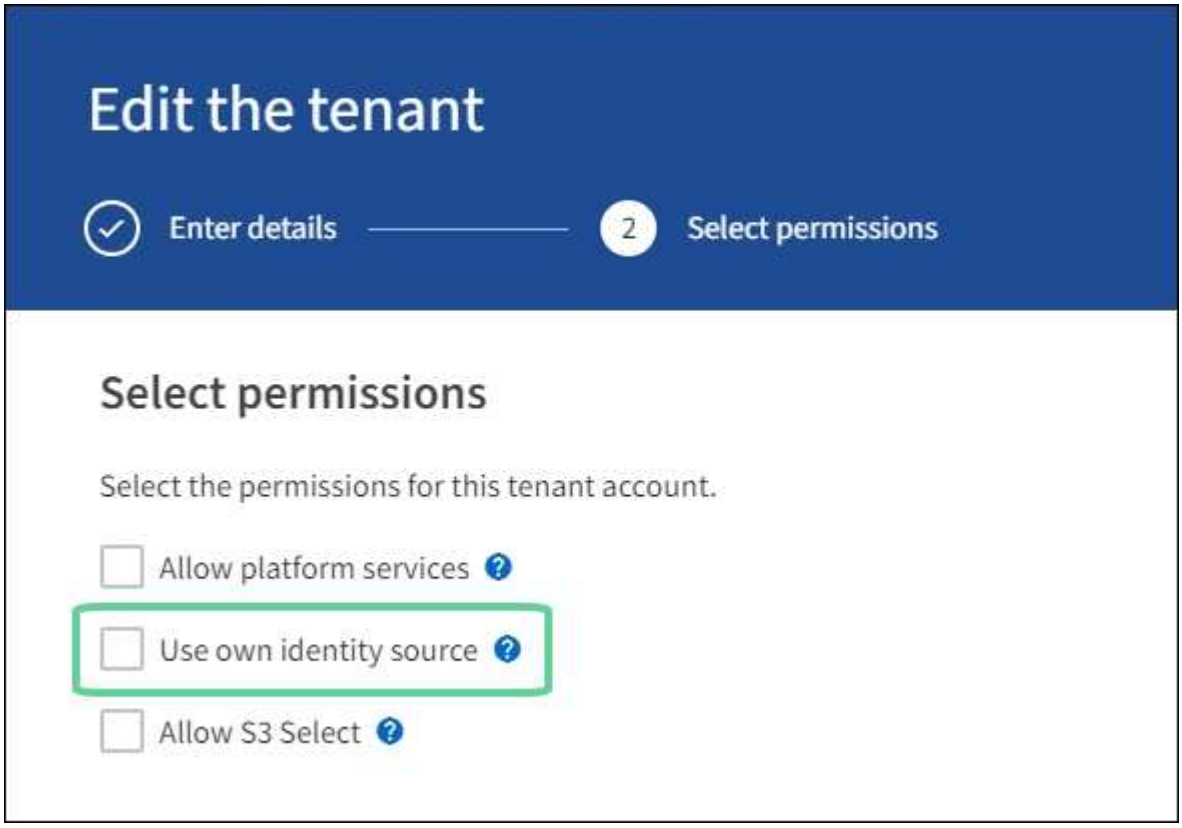
3. 既存のテナントアカウントがある場合は、次の手順を実行して、 Root アクセス権限を持つフェデレーテッドユーザがサインインできることを確認します。

a. Grid Manager から * tenants * を選択します。

b. テナントアカウントを選択し、 * Actions * > * Edit * を選択します。

c. Enter details （詳細の入力）タブで、 * Continue （続行） * を選択します。

d. チェックボックスがオンになっている場合は、チェックボックスをオフにして[Save]*を選択します。



Tenant ページが表示されます。

a. テナントアカウントを選択し、 * サインイン * を選択して、ローカルの root ユーザとしてテナントアカウントにサインインします。

b. Tenant Manager で、 * access management * > * Groups * を選択します。

c. Grid Manager から少なくとも 1 つのフェデレーテッドグループにこのテナントに対する Root アクセス権限が割り当てられていることを確認します。

d. サインアウトします。

e. フェデレーテッドグループ内のユーザとしてテナントに再度サインインできることを確認します。

関連情報

- "シングルサインオンの要件と考慮事項"

- "管理者グループを管理する"
- "テナントアカウントを使用する"

サンドボックスモードを使用する

サンドボックスモードを使用すると、すべての StorageGRID ユーザに対してシングルサインオン（ SSO ）を有効にする前に、シングルサインオン（ SSO ）を設定およびテストできます。SSO を有効にした後は、設定を変更したり再テストしたりする必要がある場合に、サンドボックスモードに戻ることができます。

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"。
- Root アクセス権限が割り当てられている。
- StorageGRID システムにアイデンティティフェデレーションを設定しておきます。
- アイデンティティフェデレーション * LDAP サービスタイプ * では、使用する SSO アイデンティティプロバイダに基づいて、 Active Directory または Azure のいずれかを選択しました。

LDAP サービスタイプが設定されました	**SSO** アイデンティティプロバイダのオプション
Active Directory	• Active Directory • Azure • PingFederate
Azure	Azure

このタスクについて

SSO が有効な場合、ユーザが管理ノードにサインインしようとすると、 StorageGRID から SSO アイデンティティプロバイダに認証要求が送信されます。次に、 SSO アイデンティティプロバイダは、認証要求が成功したかどうかを示す認証応答を StorageGRID に返します。成功した要求の場合：

- Active Directory または PingFederate からの応答には、ユーザの Universally Unique Identifier （ UUID ）が含まれています。
- Azure からの応答には、ユーザプリンシパル名（ UPN ）が含まれます。

StorageGRID （サービスプロバイダ）と SSO アイデンティティプロバイダがユーザ認証要求についてセキュアに通信できるようにするには、 StorageGRID で特定の設定を行う必要があります。次に、 SSO アイデンティティプロバイダのソフトウェアを使用して、管理ノードごとに証明書利用者信頼（ AD FS ）、エンタープライズアプリケーション（ Azure ）、またはサービスプロバイダ（ PingFederate ）を作成する必要があります。最後に、 StorageGRID に戻って SSO を有効にする必要があります。

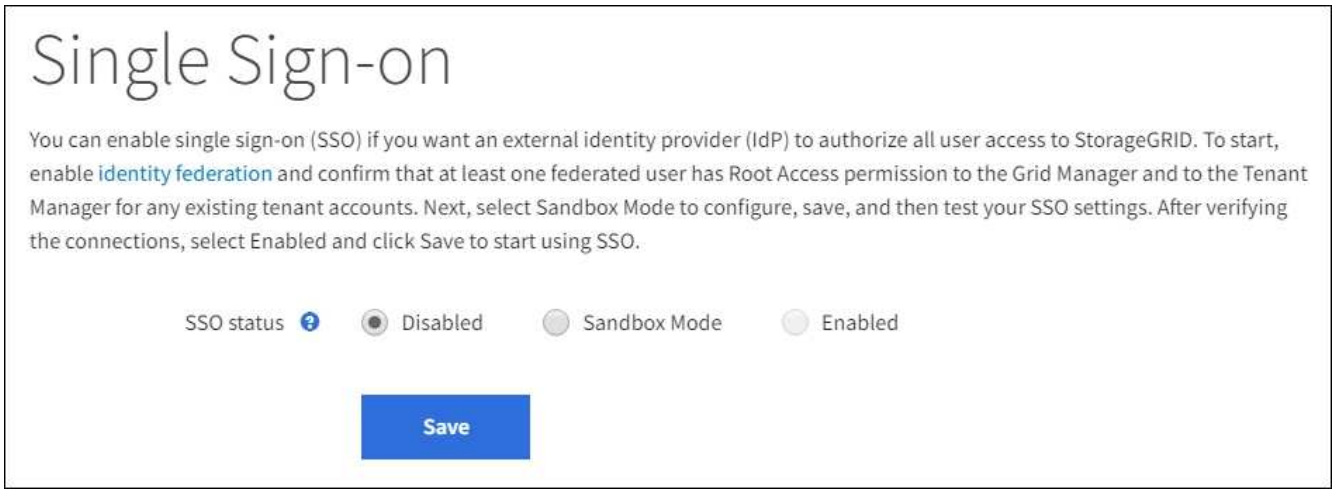
サンドボックスモードでは、 SSO を有効にする前に、この手順を簡単に実行し、すべての設定をテストできます。サンドボックスモードを使用している場合、ユーザはSSOを使用してサインインできません。

サンドボックスモードにアクセスします

手順

1. [* 設定 * > * アクセス制御 * > * シングルサインオン *] を選択します。

   [Single Sign-On] ページが表示され、 [**Disabled**] オプションが選択されます。



   [SSO Status]オプションが表示されない場合は、アイデンティティプロバイダをフェデレーテッドアイデンティティソースとして設定していることを確認します。を参照してください "シングルサインオンの要件と考慮事項"。

2. [* サンドボックスモード *] を選択します。

   [Identity Provider] セクションが表示されます。

アイデンティティプロバイダの詳細を入力します

手順

1. ドロップダウンリストから * SSO タイプ * を選択します。
2. 選択した SSO タイプに基づいて、 [Identity Provider] セクションのフィールドに入力します。

Active Directory

1. アイデンティティプロバイダの * フェデレーションサービス名 * を、 Active Directory フェデレーションサービス（ AD FS ）に表示されているとおりに入力します。

   フェデレーションサービス名を確認するには、 Windows Server Manager に移動します。[ツール *>*AD FS 管理 *] を選択します。[アクション] メニューから、 [* フェデレーションサービスのプロパティの編集 *] を選択します。フェデレーションサービス名が 2 番目のフィールドに表示されます。

2. StorageGRID 要求への応答としてアイデンティティプロバイダが SSO 設定情報を送信するときに、接続の保護に使用する TLS 証明書を指定します。

   - * オペレーティング・システムの CA 証明書を使用 * ：オペレーティング・システムにインストールされているデフォルトの CA 証明書を使用して、接続を保護します。
   - * カスタム CA 証明書を使用 * ：カスタム CA 証明書を使用して接続を保護します。

     この設定を選択した場合は、カスタム証明書のテキストをコピーし、 * CA 証明書 * テキストボックスに貼り付けます。

   - * Do not use TLS* ： TLS 証明書を使用して接続を保護しないでください。

3. 証明書利用者セクションで、 StorageGRID の * 証明書利用者 ID * を指定します。この値は、 AD FS の各証明書利用者信頼に使用する名前を制御します。

   - たとえば、グリッドに管理ノードが1つしかなく、今後管理ノードを追加する予定がない場合は、と入力します `SG` または `StorageGRID`。
   - グリッドに複数の管理ノードがある場合は、という文字列を含めます `[HOSTNAME]` を入力します。例： `SG-[HOSTNAME]`。これにより、ノードのホスト名に基づいて、システム内の管理ノードごとの証明書利用者 ID を示すテーブルが生成されます。

   証明書利用者信頼は StorageGRID システム内の管理ノードごとに作成する必要があります。管理ノードごとに証明書利用者信頼を作成することで、ユーザは管理ノードに対して安全にサインイン / サインアウトすることができます。

4. [保存（ Save ）] を選択します。

   数秒間、 * Save * （保存）ボタンに緑色のチェックマークが表示されます。

Azure

1. StorageGRID 要求への応答としてアイデンティティプロバイダが SSO 設定情報を送信するときに、接続の保護に使用する TLS 証明書を指定します。

   - * オペレーティング・システムの CA 証明書を使用 * ：オペレーティング・システムにインストールされているデフォルトの CA 証明書を使用して、接続を保護します。
   - * カスタム CA 証明書を使用 * ：カスタム CA 証明書を使用して接続を保護します。

この設定を選択した場合は、カスタム証明書のテキストをコピーし、 * CA 証明書 * テキストボックスに貼り付けます。

- * Do not use TLS* ： TLS 証明書を使用して接続を保護しないでください。

2. [エンタープライズアプリケーション] セクションで、 StorageGRID のエンタープライズアプリケーション名 * を指定します。この値は、 Azure AD の各エンタープライズアプリケーションに使用する名前を制御します。

   - たとえば、グリッドに管理ノードが1つしかなく、今後管理ノードを追加する予定がない場合は、と入力します `SG` または `StorageGRID`。
   - グリッドに複数の管理ノードがある場合は、という文字列を含めます `[HOSTNAME]` を入力します。例： `SG-[HOSTNAME]`。これにより、システム内の管理ノードごとに、そのノードのホスト名に基づいてエンタープライズアプリケーション名が表形式で表示されます。

   StorageGRID システムで管理ノードごとにエンタープライズアプリケーションを作成する必要があります。管理ノードごとにエンタープライズアプリケーションを用意することで、ユーザはどの管理ノードに対しても安全にサインイン / サインアウトすることができます。

3. の手順に従います "Azure AD でエンタープライズアプリケーションを作成" 表に記載されている管理ノードごとにエンタープライズアプリケーションを作成するには、次の手順を実行します。
4. Azure AD から、各エンタープライズアプリケーションのフェデレーションメタデータの URL をコピーします。次に、この URL を StorageGRID の対応する * フェデレーションメタデータ URL* フィールドに貼り付けます。
5. すべての管理ノードのフェデレーションメタデータの URL をコピーして貼り付けたら、「 * 保存 * 」を選択します。

   数秒間、 * Save * （保存）ボタンに緑色のチェックマークが表示されます。

PingFederate

1. StorageGRID 要求への応答としてアイデンティティプロバイダが SSO 設定情報を送信するときに、接続の保護に使用する TLS 証明書を指定します。

   - * オペレーティング・システムの CA 証明書を使用 * ：オペレーティング・システムにインストールされているデフォルトの CA 証明書を使用して、接続を保護します。
   - * カスタム CA 証明書を使用 * ：カスタム CA 証明書を使用して接続を保護します。

     この設定を選択した場合は、カスタム証明書のテキストをコピーし、 * CA 証明書 * テキストボックスに貼り付けます。

   - * Do not use TLS* ： TLS 証明書を使用して接続を保護しないでください。

2. Service Provider （ SP ；サービスプロバイダ）セクションで、 StorageGRID の * SP 接続 ID * を指定します。この値は、 PingFederate の各 SP 接続に使用する名前を制御します。

   - たとえば、グリッドに管理ノードが1つしかなく、今後管理ノードを追加する予定がない場合は、と入力します `SG` または `StorageGRID`。

◦ グリッドに複数の管理ノードがある場合は、という文字列を含めます `[HOSTNAME]` を入力します。例： `SG-[HOSTNAME]`。これにより、システム内の管理ノードごとに、そのノードのホスト名に基づいて SP 接続 ID を示す表が生成されます。

> StorageGRID システムで管理ノードごとに SP 接続を作成する必要があります。管理ノードごとに SP 接続を確立することで、ユーザは管理ノードに対して安全にサインイン / サインアウトすることができます。

3. 各管理ノードのフェデレーションメタデータの URL を * Federation metadata url * フィールドで指定します。

   次の形式を使用します。

   ```
   https://<Federation Service
   Name>:<port>/pf/federation_metadata.ping?PartnerSpId=<SP Connection
   ID>
   ```

4. [保存（ Save ）] を選択します。

   数秒間、 * Save * （保存）ボタンに緑色のチェックマークが表示されます。

証明書利用者信頼、エンタープライズアプリケーション、または **SP** 接続を設定する

設定を保存すると、サンドボックスモードの確認メッセージが表示されます。サンドボックスモードが有効になったことを確認し、概要を示します。

StorageGRID は、必要に応じてサンドボックスモードのままにすることができます。ただし、シングルサインオンページで * サンドボックスモード * を選択すると、すべての StorageGRID ユーザーに対して SSO が無効になります。サインインできるのはローカルユーザのみです。

証明書利用者信頼（ Active Directory ）、完全なエンタープライズアプリケーション（ Azure ）、または SP 接続（ PingFederate ）を設定するには、次の手順を実行します。

Active Directory

手順

1. Active Directory フェデレーションサービス（ AD FS ）に移動します。
2. StorageGRID のシングルサインオンページの表に示す各証明書利用者 ID を使用して、 StorageGRID 用の証明書利用者信頼を 1 つ以上作成します。

   次の表に示す管理ノードごとに信頼を 1 つ作成する必要があります。

   手順については、を参照してください "AD FS に証明書利用者信頼を作成します"。

Azure

手順

1. 現在サインインしている管理ノードのシングルサインオンページから、 SAML メタデータをダウンロードして保存するボタンを選択します。
2. グリッド内の他の管理ノードについて、上記の手順を繰り返します。
   a. ノードにサインインします。
   b. [* 設定 * > * アクセス制御 * > * シングルサインオン *] を選択します。
   c. そのノードの SAML メタデータをダウンロードして保存します。
3. Azure ポータルにアクセスします。
4. の手順に従います "Azure AD でエンタープライズアプリケーションを作成" をクリックして、各管理ノードの SAML メタデータファイルを対応する Azure エンタープライズアプリケーションにアップロードします。

PingFederate

手順

1. 現在サインインしている管理ノードのシングルサインオンページから、 SAML メタデータをダウンロードして保存するボタンを選択します。
2. グリッド内の他の管理ノードについて、上記の手順を繰り返します。
   a. ノードにサインインします。
   b. [* 設定 * > * アクセス制御 * > * シングルサインオン *] を選択します。
   c. そのノードの SAML メタデータをダウンロードして保存します。
3. 「 PingFederate 」に移動します。
4. "StorageGRID 用に 1 つ以上の SP 接続を作成します"。各管理ノードの SP 接続 ID （ StorageGRID の Single Sign-On ページの表を参照）と、その管理ノード用にダウンロードした SAML メタデータを使用します。

   次の表に示す管理ノードごとに 1 つの SP 接続を作成する必要があります。

SSO 接続をテストします

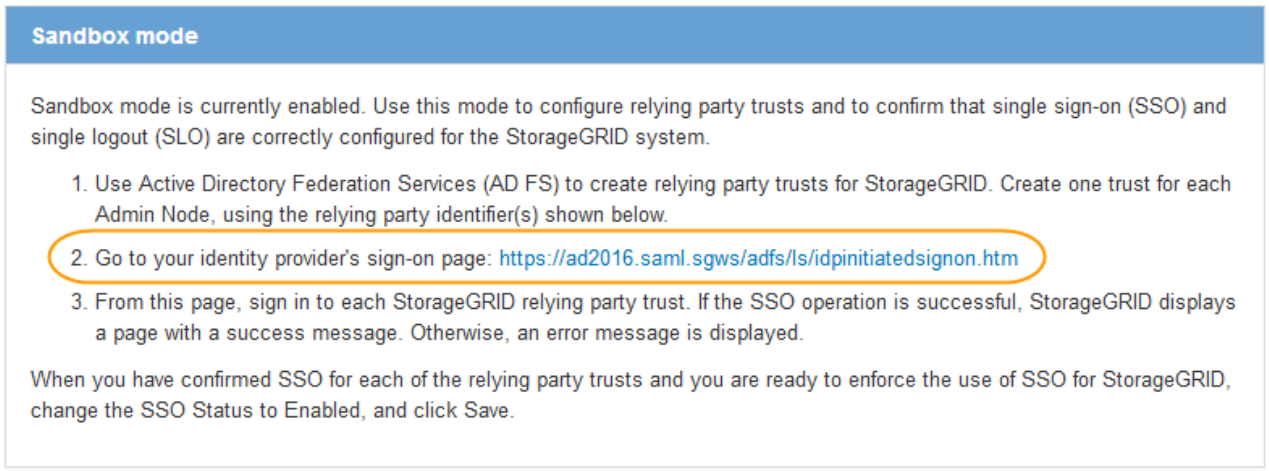
StorageGRID システム全体にシングルサインオンを適用する前に、各管理ノードでシングルサインオンとシングルログアウトが正しく設定されていることを確認する必要があります。

Active Directory

手順

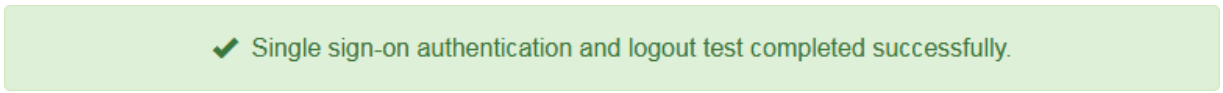
1. StorageGRID のシングルサインオンページで、サンドボックスモードメッセージ内のリンクを探します。

   URL は、 [* フェデレーションサービス名 * （ * Federation service name * ）] フィールドに入力した値から取得されます。



2. リンクを選択するか、 URL をコピーしてブラウザに貼り付け、アイデンティティプロバイダのサインオンページにアクセスします。
3. SSO を使用して StorageGRID にサインインできることを確認するには、 * 次のいずれかのサイトにサインイン * を選択し、プライマリ管理ノードの証明書利用者 ID を選択して * サインイン * を選択します。

4. フェデレーテッドユーザのユーザ名とパスワードを入力します。
   - SSO サインインおよびログアウト処理が成功すると、成功のメッセージが表示されます。



   - SSO 処理が失敗すると、エラーメッセージが表示されます。問題 を修正し、ブラウザのクッキーを消去してやり直してください。

5. 同じ手順を繰り返して、グリッド内の管理ノードごとに SSO 接続を確認します。

Azure

手順

1. Azure ポータルのシングルサインオンページに移動します。
2. [このアプリケーションをテストする *] を選択します。
3. フェデレーテッドユーザのクレデンシャルを入力します。
   - SSO サインインおよびログアウト処理が成功すると、成功のメッセージが表示されます。

     ✔ Single sign-on authentication and logout test completed successfully.

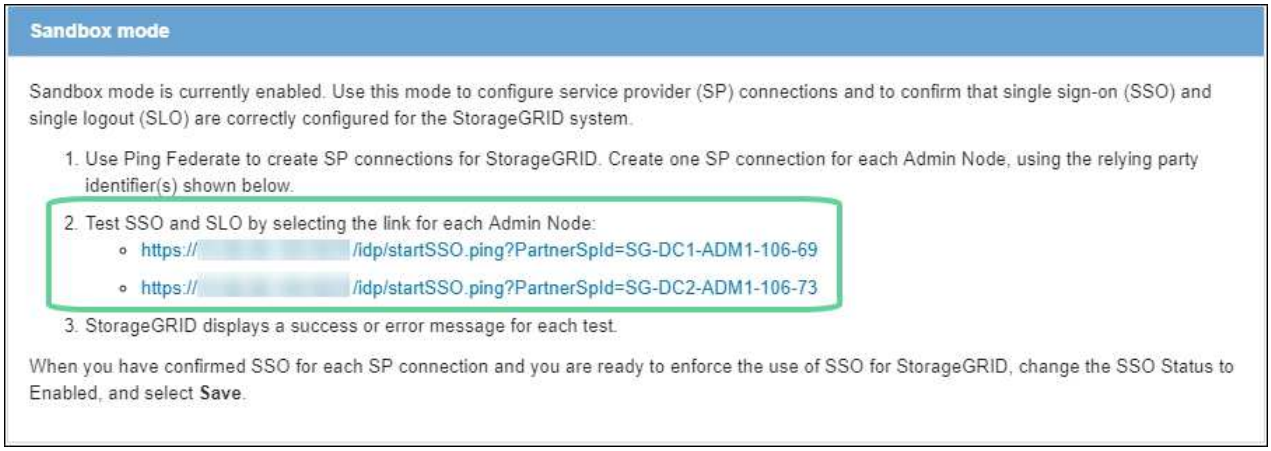
   - SSO 処理が失敗すると、エラーメッセージが表示されます。問題 を修正し、ブラウザのクッキーを消去してやり直してください。
4. 同じ手順を繰り返して、グリッド内の管理ノードごとに SSO 接続を確認します。

PingFederate

手順

1. StorageGRID シングルサインオンページで、サンドボックスモードメッセージの最初のリンクを選択します。

   一度に 1 つのリンクを選択してテストします。

2. フェデレーテッドユーザのクレデンシャルを入力します。
   - SSO サインインおよびログアウト処理が成功すると、成功のメッセージが表示されます。

     ✔ Single sign-on authentication and logout test completed successfully.

   - SSO 処理が失敗すると、エラーメッセージが表示されます。問題 を修正し、ブラウザのクッキーを消去してやり直してください。
3. 次のリンクを選択して、グリッド内の各管理ノードの SSO 接続を確認します。

   「ページの有効期限が切れました」というメッセージが表示された場合は、ブラウザで「 * 戻る * 」

ボタンを選択し、クレデンシャルを再送信してください。

シングルサインオンを有効にします

SSO を使用して各管理ノードにサインインできることを確認したら、 StorageGRID システム全体で SSO を有効にできます。

SSO が有効になっている場合は、すべてのユーザが SSO を使用して Grid Manager 、テナントマネージャ、グリッド管理 API 、およびテナント管理 API にアクセスする必要があります。ローカルユーザは StorageGRID にアクセスできなくなります。

手順

1. [* 設定 * > * アクセス制御 * > * シングルサインオン *] を選択します。
2. SSO ステータスを * Enabled * に変更します。
3. [保存（ Save ）] を選択します。
4. 警告メッセージを確認し、「 * OK 」を選択します。

   シングルサインオンが有効になりました。

Azure ポータルを使用しており、 Azure へのアクセスに使用するコンピュータから StorageGRID にアクセスする場合は、 Azure ポータルユーザが StorageGRID ユーザとしても許可されている（フェデレーテッドグループ内のユーザが StorageGRID にインポートされている）ことを確認してください。 または、 StorageGRID にサインインする前に Azure Portal からログアウトします。

AD FS に証明書利用者信頼を作成します

Active Directory フェデレーションサービス（ AD FS ）を使用して、システム内の管理ノードごとに証明書利用者信頼を作成する必要があります。PowerShell コマンドを使用するか、 StorageGRID から SAML メタデータをインポートするか、またはデータを手動で入力することによって、証明書利用者信頼を作成できます。

作業を開始する前に

- StorageGRID のシングルサインオンを設定し、 SSO タイプとして **AD FS** を選択しました。
- * Grid Manager のシングルサインオンページでサンドボックスモード * が選択されています。を参照してください "サンドボックスモードを使用する"。
- システム内の各管理ノードの完全修飾ドメイン名（または IP アドレス）と証明書利用者 ID を確認しておきます。これらの値は、 StorageGRID のシングルサインオンページの管理ノード詳細テーブルにあります。

  証明書利用者信頼は StorageGRID システム内の管理ノードごとに作成する必要があります。管理ノードごとに証明書利用者信頼を作成することで、ユーザは管理ノードに対して安全にサインイン / サインアウトすることができます。

- AD FS での証明書利用者信頼の作成経験があるか、または Microsoft AD FS のドキュメントを参照できる

必要があります。

- AD FS 管理スナップインを使用していて、 Administrators グループに属している必要があります。
- 証明書利用者信頼を手動で作成する場合は、 StorageGRID 管理インターフェイス用にカスタム証明書をアップロードするか、コマンドシェルから管理ノードにログインする方法を確認しておきます。

このタスクについて

以下の手順は、 Windows Server 2016 AD FS に該当します。別のバージョンの AD FS を使用している場合は、手順 にわずかな違いがあります。不明な点がある場合は、 Microsoft AD FS のドキュメントを参照してください。

Windows PowerShell を使用して証明書利用者信頼を作成します

Windows PowerShell を使用して証明書利用者信頼を簡単に作成できます。

手順

1. Windows のスタートメニューから PowerShell アイコンを右クリックし、 * 管理者として実行 * を選択します。
2. PowerShell コマンドプロンプトで、次のコマンドを入力します。

   ```
   Add-AdfsRelyingPartyTrust -Name "Admin_Node_Identifer" -MetadataURL
   "https://Admin_Node_FQDN/api/saml-metadata"
   ```

   - の場合 `Admin_Node_Identifier`では、管理ノードの証明書利用者IDをSingle Sign-Onページに表示されるとおりに入力します。例： `SG-DC1-ADM1。
   - の場合 `Admin_Node_FQDN`をクリックし、同じ管理ノードの完全修飾ドメイン名を入力します。（必要に応じて、ノードの IP アドレスを代わりに使用できます。ただし、 IP アドレスを入力した場合、その IP アドレスが変わったときには証明書利用者信頼を更新または再作成する必要があります）。
3. Windows Server Manager で、 * Tools * > * AD FS Management * を選択します。

   AD FS 管理ツールが表示されます。
4. 「 * AD FS * > * 証明書利用者信頼」を選択します。

   証明書利用者信頼のリストが表示されます。
5. 新しく作成した証明書利用者信頼にアクセス制御ポリシーを追加します。
   a. 作成した証明書利用者信頼を検索します。
   b. 信頼を右クリックし、 * アクセス制御ポリシーの編集 * を選択します。
   c. アクセス制御ポリシーを選択します。
   d. [* 適用（ Apply ）] を選択し、 [* OK] を選択します
6. 新しく作成した証明書利用者信頼に要求発行ポリシーを追加します。
   a. 作成した証明書利用者信頼を検索します。
   b. 信頼を右クリックし、 ［ * クレーム発行ポリシーの編集 * ］ を選択します。
   c. [* ルールの追加 *] を選択します。

d. ［ルールテンプレートの選択］ページで、リストから ［* LDAP 属性をクレームとして送信 *］ を選択し、 ［* 次へ *］ を選択します。

e. ［ルールの設定］ページで、このルールの表示名を入力します。

たとえば、 **ObjectGUID to Name ID** と入力します。

f. 属性ストアで、 * Active Directory * を選択します。

g. マッピングテーブルの LDAP 属性列に、 * objectGUID * と入力します。

h. マッピングテーブルの発信クレームタイプ列で、ドロップダウンリストから * 名前 ID * を選択します。

i. 「完了」を選択し、「 * OK 」を選択します。

7. メタデータが正常にインポートされたことを確認します。

a. 証明書利用者信頼を右クリックしてプロパティを開きます。

b. [**Endpoints**] 、 [***Identifiers**] 、および [**Signature**] タブのフィールドに値が入力されていることを確認します。

メタデータが見つからない場合は、フェデレーションメタデータのアドレスが正しいことを確認するか、値を手動で入力します。

8. 上記の手順を繰り返して、 StorageGRID システム内のすべての管理ノードに対して証明書利用者信頼を設定します。

9. 完了したら、 StorageGRID に戻ってすべての証明書利用者信頼をテストし、正しく設定されていることを確認します。を参照してください "サンドボックスモードを使用する" 手順については、を参照し

フェデレーションメタデータをインポートして、証明書利用者信頼を作成します

各証明書利用者信頼の値をインポートするには、各管理ノードの SAML メタデータにアクセスします。

手順

1. Windows Server Manager で、 * Tools * を選択し、 * AD FS Management * を選択します。

2. Actions （アクション）で、 * Add （証明書利用者信頼の追加） * を選択します。

3. [ようこそ] ページで、 [* クレーム対応 *] を選択し、 [開始 *] を選択します。

4. [* オンラインまたはローカルネットワーク上で公開されている証明書利用者に関するデータをインポートする *] を選択します。

5. * フェデレーションメタデータアドレス（ホスト名または URL ） * に、この管理ノードの SAML メタデータの場所を入力します。

`https://Admin_Node_FQDN/api/saml-metadata`

の場合 `*Admin_Node_FQDN*` をクリックし、同じ管理ノードの完全修飾ドメイン名を入力します。（必要に応じて、ノードの IP アドレスを代わりに使用できます。ただし、 IP アドレスを入力した場合、その IP アドレスが変わったときには証明書利用者信頼を更新または再作成する必要があります）。

6. 証明書利用者信頼の追加ウィザードを実行し、証明書利用者信頼を保存して、ウィザードを閉じます。

表示名を入力するときは、管理ノードの証明書利用者 ID を使用します。これは、 Grid Manager のシングルサインオンページに表示される情報とまったく同じです。例： `SG-DC1-ADM1`。

7. クレームルールを追加します。
   a. 信頼を右クリックし、 ［ * クレーム発行ポリシーの編集 * ］ を選択します。
   b. [* ルールを追加 * （ Add rule * ）] を
   c. ［ ルールテンプレートの選択 ］ ページで、リストから ［ * LDAP 属性をクレームとして送信 * ］ を選択し、 ［ * 次へ * ］ を選択します。
   d. ［ ルールの設定 ］ ページで、このルールの表示名を入力します。

      たとえば、 **ObjectGUID to Name ID** と入力します。

   e. 属性ストアで、 * Active Directory * を選択します。
   f. マッピングテーブルの LDAP 属性列に、 * objectGUID * と入力します。
   g. マッピングテーブルの発信クレームタイプ列で、ドロップダウンリストから * 名前 ID * を選択します。
   h. 「完了」を選択し、「 * OK 」を選択します。
8. メタデータが正常にインポートされたことを確認します。
   a. 証明書利用者信頼を右クリックしてプロパティを開きます。
   b. [**Endpoints**] 、 [***Identifiers**] 、および [**Signature**] タブのフィールドに値が入力されていることを確認します。

      メタデータが見つからない場合は、フェデレーションメタデータのアドレスが正しいことを確認するか、値を手動で入力します。

9. 上記の手順を繰り返して、 StorageGRID システム内のすべての管理ノードに対して証明書利用者信頼を設定します。
10. 完了したら、 StorageGRID に戻ってすべての証明書利用者信頼をテストし、正しく設定されていることを確認します。を参照してください "サンドボックスモードを使用する" 手順については、を参照し

証明書利用者信頼を手動で作成します

証明書利用者信頼のデータをインポートしないことを選択した場合は、値を手動で入力できます。

手順

1. Windows Server Manager で、 * Tools * を選択し、 * AD FS Management * を選択します。
2. Actions （アクション）で、 * Add （証明書利用者信頼の追加） * を選択します。
3. [ようこそ] ページで、 [* クレーム対応 *] を選択し、 [開始 *] を選択します。
4. [* 証明書利用者に関するデータを手動で入力する *] を選択し、 [* 次へ *] を選択します。
5. 証明書利用者信頼の追加ウィザードを実行します。
   a. この管理ノードの表示名を入力します。

整合性を確保するために、管理ノードの証明書利用者 ID を使用してください。この ID は、 Grid Manager のシングルサインオンページに表示されます。例： `SG-DC1-ADM1`。

b. オプションのトークン暗号化証明書を設定する手順は省略してください。

c. [URLの設定]ページで、* SAML 2.0 WebSSOプロトコルのサポートを有効にする*チェックボックスをオンにします。

d. 管理ノードの SAML サービスエンドポイントの URL を入力します。

`https://Admin_Node_FQDN/api/saml-response`

の場合 `*Admin_Node_FQDN*`で、管理ノードの完全修飾ドメイン名を入力します。（必要に応じて、ノードの IP アドレスを代わりに使用できます。ただし、 IP アドレスを入力した場合、その IP アドレスが変わったときには証明書利用者信頼を更新または再作成する必要があります）。

e. Configure Identifiers ページで、同じ管理ノードの証明書利用者 ID を指定します。

`Admin_Node_Identifier`

の場合 `Admin_Node_Identifier`では、管理ノードの証明書利用者`ID`を`Single Sign-On`ページに表示されるとおりに入力します。例： `SG-DC1-ADM1`。

f. 設定を確認し、証明書利用者信頼を保存して、ウィザードを閉じます。

[クレーム発行ポリシーの編集] ダイアログボックスが表示されます。

ダイアログボックスが表示されない場合は、信頼を右クリックし、 * クレーム発行ポリシーの編集 * を選択します。

6. ［ クレームルール ］ ウィザードを開始するには、 ［ * ルールの追加 * ］ を選択します。

a. ［ ルールテンプレートの選択 ］ ページで、リストから ［ * LDAP 属性をクレームとして送信 * ］ を選択し、 ［ * 次へ * ］ を選択します。

b. ［ ルールの設定 ］ ページで、このルールの表示名を入力します。

たとえば、 **ObjectGUID to Name ID** と入力します。

c. 属性ストアで、 * Active Directory * を選択します。

d. マッピングテーブルの LDAP 属性列に、 * objectGUID * と入力します。

e. マッピングテーブルの発信クレームタイプ列で、ドロップダウンリストから * 名前 ID * を選択します。

f. 「完了」を選択し、「 * OK 」を選択します。

7. 証明書利用者信頼を右クリックしてプロパティを開きます。

8. [* Endpoints] タブで、シングルログアウト（ SLO ）のエンドポイントを設定します。

a. 「 * SAML を追加」を選択します。

b. [* Endpoint Type*>*SAML Logout*] を選択します。

c. 「 * Binding * > * Redirect * 」を選択します。

d. [**Trusted URL**] フィールドに、この管理ノードからのシングルログアウト（ SLO ）に使用する URL を入力します。

```
https://Admin_Node_FQDN/api/saml-logout
```

の場合 `*Admin_Node_FQDN*` をクリックし、管理ノードの完全修飾ドメイン名を入力します。（必要に応じて、ノードの IP アドレスを代わりに使用できます。ただし、 IP アドレスを入力した場合、その IP アドレスが変わったときには証明書利用者信頼を更新または再作成する必要があります）。

a. 「 * OK 」を選択します。

9. [* Signature*] タブで、この証明書利用者信頼の署名証明書を指定します。

a. カスタム証明書を追加します。

- StorageGRID にアップロードしたカスタム管理証明書がある場合は、その証明書を選択します。
- カスタム証明書がない場合は、管理ノードにログインしてに移動します `/var/local/mgmt-api` 管理ノードのディレクトリにを追加します `custom-server.crt` 証明書ファイル。

  *注：*管理ノードのデフォルト証明書を使用 (`server.crt`）は推奨されません。管理ノードで障害が発生した場合、ノードをリカバリする際にデフォルトの証明書が再生成されるため、証明書利用者信頼を更新する必要があります。

b. [* 適用（ Apply ）] を選択し、 [* OK] を選択します。

証明書利用者のプロパティが保存されて閉じられます。

10. 上記の手順を繰り返して、 StorageGRID システム内のすべての管理ノードに対して証明書利用者信頼を設定します。
11. 完了したら、 StorageGRID に戻ってすべての証明書利用者信頼をテストし、正しく設定されていることを確認します。を参照してください "サンドボックスモードを使用する" 手順については、を参照し

Azure AD でエンタープライズアプリケーションを作成

Azure AD を使用して、システム内の管理ノードごとにエンタープライズアプリケーションを作成します。

作業を開始する前に

- StorageGRID 用のシングルサインオンの設定を開始し、 SSO タイプとして「 * Azure* 」を選択しました。
- * Grid Manager のシングルサインオンページでサンドボックスモード * が選択されています。を参照してください "サンドボックスモードを使用する"。
- システム内の管理ノードごとに * Enterprise アプリケーション名 * を用意しておきます。これらの値は、StorageGRID のシングルサインオンページの管理ノードの詳細テーブルからコピーできます。

> StorageGRID システムで管理ノードごとにエンタープライズアプリケーションを作成する必要があります。管理ノードごとにエンタープライズアプリケーションを用意することで、ユーザはどの管理ノードに対しても安全にサインイン / サインアウトすることができます。

- Azure Active Directory でエンタープライズアプリケーションを作成した経験がある。

- アクティブなサブスクリプションを持つ Azure アカウントが必要です。
- Azure アカウントに、グローバル管理者、クラウドアプリケーション管理者、アプリケーション管理者、サービスプリンシパルの所有者のいずれかのロールが割り当てられている。

Azure AD にアクセスします

手順

1. にログインします "Azure ポータル"。
2. に移動します "Azure Active Directory の略"。
3. 選択するオプション "エンタープライズアプリケーション"。

エンタープライズアプリケーションを作成し、 StorageGRID SSO 設定を保存します

AzureのSSO設定をStorageGRID に保存するには、Azureを使用して管理ノードごとにエンタープライズアプリケーションを作成する必要があります。フェデレーションメタデータの URL を Azure からコピーし、StorageGRID のシングルサインオンページの対応する * フェデレーションメタデータの URL * フィールドに貼り付けます。

手順

1. 管理ノードごとに次の手順を繰り返します。
   a. Azure Enterprise アプリケーションペインで、 * 新規アプリケーション * を選択します。
   b. 「 * 独自のアプリケーションを作成する * 」を選択します。
   c. 名前には、 StorageGRID のシングルサインオンページの管理ノード詳細テーブルからコピーした * エンタープライズアプリケーション名 * を入力します。
   d. ギャラリー (ギャラリー以外) で見つからない他のアプリケーションを統合 * ラジオボタンを選択したままにします。
   e. 「 * Create * 」を選択します。
   f. 2 の * Get started * リンクを選択します。シングルサインオン * ボックスを設定するか、左マージンの * シングルサインオン * リンクを選択します。
   g. [* SAML *] ボックスを選択します。
   h. 「 * アプリフェデレーションメタデータ URL * 」をコピーします。この URL は「 * ステップ 3 SAML 署名証明書 * 」にあります。
   i. StorageGRID シングルサインオンページに移動し、使用した * エンタープライズアプリケーション名 * に対応する * フェデレーションメタデータ URL* フィールドに URL を貼り付けます。
2. 各管理ノードのフェデレーションメタデータ URL を貼り付け、 SSO 設定に必要なその他の変更をすべて行ったら、 StorageGRID のシングルサインオンページで「 * 保存」を選択します。

管理ノードごとに SAML メタデータをダウンロードします

SSO 設定を保存したら、 StorageGRID システム内の管理ノードごとに SAML メタデータファイルをダウンロードできます。

手順

1. 管理ノードごとに上記の手順を繰り返します。

a. 管理ノードから StorageGRID にサインインします。

b. [* 設定 * > * アクセス制御 * > * シングルサインオン *] を選択します。

c. ボタンを選択して、その管理ノードの SAML メタデータをダウンロードします。

d. Azure AD にアップロードするファイルを保存します。

SAML メタデータを各エンタープライズアプリケーションにアップロードする

StorageGRID 管理ノードごとに SAML メタデータファイルをダウンロードしたら、 Azure AD で次の手順を実行します。

手順

1. Azure ポータルに戻ります。
2. エンタープライズアプリケーションごとに、次の手順を繰り返します。

> 以前にリストに追加したアプリケーションを表示するには、 [エンタープライズアプリケーション] ページの更新が必要な場合があります。

a. エンタープライズアプリケーションのプロパティページに移動します。

b. [Assignment Required*] を [**No**] に設定します（個別に割り当てを設定する場合を除く）。

c. シングルサインオンページに移動します。

d. SAML の設定を完了します。

e. メタデータファイルのアップロードボタンを選択し、対応する管理ノード用にダウンロードした SAML メタデータファイルを選択します。

f. ファイルがロードされたら、「 * 保存」を選択し、「 * X * 」を選択してパネルを閉じます。SAML を使用してシングルサインオンを設定するページに戻ります。

3. の手順に従います "サンドボックスモードを使用する" 各アプリケーションをテストします。

PingFederate でサービスプロバイダ（ SP ）接続を作成します

PingFederate を使用して、システム内の管理ノードごとにサービスプロバイダ（ SP ）接続を作成します。処理時間を短縮するために、 StorageGRID から SAML メタデータをインポートします。

作業を開始する前に

- StorageGRID にシングルサインオンを設定し、 SSO タイプとして「 Ping federate * 」を選択しました。
- * Grid Manager のシングルサインオンページでサンドボックスモード * が選択されています。を参照してください "サンドボックスモードを使用する"。
- システム内の管理ノードごとに * SP 接続 ID * を用意しておきます。これらの値は、 StorageGRID のシングルサインオンページの管理ノード詳細テーブルにあります。
- システムの管理ノードごとに * SAML メタデータ * をダウンロードしておきます。
- PingFederate サーバーで SP 接続を作成した経験があります。
- を使用することができますhttps://docs.pingidentity.com/bundle/pingfederate-103/page/kfj1564002962494.html["管理者向けリファレンスガイド"^] PingFederate サーバー

用。PingFederate ドキュメントでは、詳細な手順と説明を説明しています。

- PingFederate サーバーの管理者権限があります。

このタスクについて

ここでは、 StorageGRID の SSO プロバイダとして PingFederate Server バージョン 10.3 を設定する方法を簡単に説明します。別のバージョンの PingFederate を使用している場合は、これらの指示を適用する必要があります。ご使用のリリースの詳細な手順については、 PingFederate Server のマニュアルを参照してください。

PingFederate の前提条件を完了します

StorageGRID に使用する SP 接続を作成する前に、 PingFederate で前提条件のタスクを完了する必要があります。SP 接続を設定するときは、これらの前提条件の情報を使用します。

データストアの作成**[[data-store]**

まだ作成していない場合は、 PingFederate を AD FS LDAP サーバーに接続するデータストアを作成します。使用した値は、のときに使用したものです "アイデンティティフェデレーションの設定" StorageGRID の場合。

- * タイプ * ：ディレクトリ（ LDAP ）
- * LDAP タイプ * ： Active Directory
- * バイナリ属性名 *: 「 LDAP バイナリ属性」タブに * objectGUID * を正確に入力します。

パスワードクレデンシャルバリデータの作成

パスワード認証情報バリデータをまだ作成していない場合は、作成します。

- * 「 * 」と入力します。 LDAP ユーザ名パスワード資格情報検証ツール
- * データストア *: 作成したデータストアを選択します。
- * 検索ベース * ： LDAP から情報を入力します（例： DC=SAML 、 DC=sgws ）。
- * 検索フィルタ * ： sAMAccountName = $ ｛ userName ｝
- * スコープ * ：サブツリー

IdPアダプタインスタンス**[**アダプタインスタンス**]**を作成します

IdP アダプタのインスタンスをまだ作成していない場合は作成します。

手順

1. 「 * 認証 * > * 統合 * > * IdP アダプタ * 」に移動します。
2. [新規インスタンスの作成（ Create New Instance ）] を選択します
3. [タイプ] タブで、 [* HTML フォーム IdP アダプタ *] を選択します。
4. [IdP アダプタ] タブで、 [資格情報検証ツール] に新しい行を追加する *] を選択します。
5. を選択します パスワードクレデンシャルバリデータ を作成しました。
6. [アダプタの属性] タブで、 **pseudonym *** の ***username** 属性を選択します。

7. [保存（ Save ）] を選択します。

署名証明書の作成またはインポート**[signing-certificate]**

署名証明書を作成またはインポートしていない場合は、作成します。

手順

1. 「 * Security * > * Signing & Decryption keys & Certificates * 」に移動します。
2. 署名証明書を作成またはインポートします。

PingFederate で **SP** 接続を作成します

PingFederate で SP 接続を作成すると、管理ノード用に StorageGRID からダウンロードした SAML メタデータがインポートされます。メタデータファイルには、必要な値の多くが含まれています。

> ユーザが任意のノードに対して安全にサインインおよびサインアウトできるように、StorageGRID システム内の管理ノードごとに SP 接続を作成する必要があります。次の手順に従って、最初の SP 接続を作成します。次に、に進みます 追加の SP 接続を作成します 追加の接続を作成するには、次の手順を実行します。

SP 接続タイプを選択します

手順

1. [* アプリケーション * > * 統合 * > * SP 接続 *] に移動します。
2. [接続の作成 *] を選択します。
3. 「 * この接続にテンプレートを使用しない * 」を選択します。
4. ブラウザ SSO プロファイル * および * SAML 2.0 * をプロトコルとして選択します。

SP メタデータをインポートします

手順

1. メタデータのインポートタブで、 * ファイル * を選択します。
2. 管理ノードの StorageGRID シングルサインオンページからダウンロードした SAML メタデータファイルを選択します。
3. [Metadata Summary]と[General Info]タブに表示される情報を確認します。

   パートナーのエンティティ ID と接続名は、 StorageGRID SP 接続 ID に設定されています。（例：10.96.105.200-DC1-ADM1-105-200 ）。ベース URL は、 StorageGRID 管理ノードの IP です。

4. 「 * 次へ * 」を選択します。

IdP ブラウザの **SSO** を設定する

手順

1. ブラウザ SSO タブで、 * ブラウザ SSO の設定 * を選択します。
2. SAML プロファイルタブで、 * SP が開始した SSO * 、 * SP - 初期 SLO * 、 * IdP が開始した SSO * 、および * IdP によって開始された SLO * オプションを選択します。

3. 「 * 次へ * 」を選択します。
4. [Assertion Lifetime （アサーションの有効期間）] タブで、変更を行いません。
5. [アサーションの作成] タブで、 [* アサーションの作成の設定 *] を選択します。
   a. [ID マッピング] タブで、 [* 標準 *] を選択します。
   b. [属性契約（ Attribute Contract ）] タブで、属性契約として * sama_subject * を使用し、インポートされた名前形式を指定しません。
6. [Extend the Contract]で、*[Delete]*を選択してを削除します `urn:oid`は使用されません。

アダプタインスタンスをマッピングします

手順

1. [Authentication Source Mapping] タブで、 [* Map New Adapter Instance] を選択します。
2. [アダプタインスタンス] タブで、を選択します アダプタインスタンス を作成しました。
3. [マッピング方法] タブで、 [データストアから追加属性を取得する *] を選択します。
4. [属性ソースとユーザールックアップ] タブで、 [属性ソースの追加] を選択します。
5. [データストア] タブで、概要 を入力し、を選択します データストア を追加しました。
6. LDAP ディレクトリ検索タブで、次の手順を実行します。
   - 「 * ベース DN * 」を入力します。この DN は、 LDAP サーバの StorageGRID で入力した値と完全に一致している必要があります。
   - 検索範囲（ Search Scope ）で、 * サブツリー * （ * Subtree * ）を選択します。
   - ルートオブジェクトクラスの場合は、 * objectGUID * 属性を検索して追加します。
7. [LDAP Binary Attribute Encoding Types] タブで、 *objectGUID * 属性として *Base64 * を選択します。
8. LDAP Filter タブで、 * sAMAccountName = $ ｛ userName ｝ * と入力します。
9. [属性契約履行] タブで、 [ソース] ドロップダウンから [**LDAP(** 属性 **)**] を選択し、 [値] ドロップダウンから [**objectGUID**] を選択します。
10. 属性ソースを確認して保存します。
11. Failsave Attribute Source タブで、 * Abort the SSO Transaction * を選択します。
12. 概要を確認し、「 * Done * 」を選択します。
13. 「 Done （完了）」を選択します。

プロトコルを設定します

手順

1. * SP Connection * > * Browser SSO * > * Protocol Settings * タブで、 * Configure Protocol Settings * を選択します。
2. [アサーションコンシューマサービスURL]タブで、StorageGRID SAMLメタデータからインポートされたデフォルト値を受け入れます（バインドおよびの場合は* POST *） `/api/saml-response` （エンドポイントURLの場合）。
3. [SLOサービスURLs]タブで、StorageGRID SAMLメタデータ（バインドおよび用の* redirect*）からインポートされたデフォルト値を受け入れます `/api/saml-logout` エンドポイントURLの場合。

4. [Allowable SAML Bindings]タブで、[**artifact**]および[**SOAP**]を選択解除します。必要なのは、 * POST * および * redirect * のみです。
5. [Signature Policy]タブで、[* Require Authn Requests to be Signed]チェックボックスと[* Always Sign Assertion]チェックボックスをオンのままにします。
6. ［ 暗号化ポリシー ］ タブで、 ［ * なし * ］ を選択します。
7. 概要を確認し、「 * Done * 」を選択してプロトコル設定を保存します。
8. 概要を確認し、「完了」を選択して、ブラウザ SSO 設定を保存します。

クレデンシャルを設定

手順

1. ［ SP 接続 ］ タブで ' ［ * 資格情報 * ］ を選択します
2. 資格情報タブで、 * 資格情報の設定 * を選択します。
3. を選択します 署名証明書 を作成またはインポートしました。
4. 「 * 次へ * 」を選択して、「 * 署名検証設定の管理 * 」に移動します。
   a. [信頼モデル] タブで、 [*Unanchored] を選択します。
   b. [Signature Verification Certificate] タブで、 StorageGRID SAML メタデータからインポートした署名証明書情報を確認します。
5. 概要画面を確認し、 ［ * 保存 * ］ を選択して SP 接続を保存します。

追加の **SP** 接続を作成します

最初の SP 接続をコピーして、グリッド内の管理ノードごとに必要な SP 接続を作成できます。コピーごとに新しいメタデータをアップロードします。

> 異なる管理ノードの SP 接続では、パートナーのエンティティ ID 、ベース URL 、接続 ID 、接続名、署名の検証を除き、同じ設定を使用します。 と SLO 応答 URL 。

手順

1. * Action * > * Copy * を選択して、追加の管理ノードごとに最初の SP 接続のコピーを作成します。
2. コピーの接続 ID と接続名を入力し、 * 保存 * を選択します。
3. 管理ノードに対応するメタデータファイルを選択します。
   a. 「 * アクション * > * メタデータで更新 * 」を選択します。
   b. 「 * ファイルを選択」を選択し、メタデータをアップロードします。
   c. 「 * 次へ * 」を選択します。
   d. [保存（ Save ）] を選択します。
4. 未使用の属性によるエラーを解決します。
   a. 新しい接続を選択します。
   b. ブラウザ SSO の設定 > アサーションの作成の設定 > 属性契約 * を選択します。
   c. urn ： Oid * のエントリを削除します。

d. [保存（ Save ）] を選択します。

シングルサインオンを無効にします

不要になった場合はシングルサインオン（ SSO ）を無効にすることができます。アイデンティティフェデレーションを無効にする場合は、事前にシングルサインオンを無効にする必要があります。

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"。
- 特定のアクセス権限が必要です。

手順

1. [* 設定 * > * アクセス制御 * > * シングルサインオン *] を選択します。

   [Single Sign-On] ページが表示されます。

2. [* Disabled * （無効 * ）] オプションを選択します。
3. [保存（ Save ）] を選択します。

   ローカルユーザがサインインできるようになったことを示す警告メッセージが表示されます。

4. 「 * OK 」を選択します。

   次回 StorageGRID にサインインすると、 StorageGRID のサインインページが表示され、ローカルユーザまたはフェデレーテッド StorageGRID ユーザのユーザ名とパスワードを入力する必要があります。

1 つの管理ノードのシングルサインオンを一時的に無効にしてから再度有効にする

シングルサインオン（ SSO ）システムが停止すると、 Grid Manager にサインインできない場合があります。この場合は、 1 つの管理ノードに対して SSO を一時的に無効にしてから再度有効にすることができます。SSO を無効にしてから再度有効にするには、ノードのコマンドシェルにアクセスする必要があります。

作業を開始する前に

- 特定のアクセス権限が必要です。
- を使用することができます `Passwords.txt` ファイル。
- ローカルの root ユーザのパスワードを確認しておきます。

このタスクについて

1 つの管理ノードに対して SSO を無効にすると、ローカルの root ユーザとして Grid Manager にサインインできます。StorageGRID システムを保護するために、ノードのコマンドシェルを使用してサインアウト後すぐに管理ノードの SSO を再度有効にする必要があります。

1 つの管理ノードに対して SSO を無効にしても、グリッド内の他の管理ノードの SSO 設定には影響しません。Grid Managerの[Single Sign-on]ページの[Enable SSO]*チェックボックスは選択されたままになり、既存のSSO設定は更新しないかぎり維持されます。

手順

1. 管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@Admin_Node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

      rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

2. 次のコマンドを実行します。`disable-saml`

   環境 this admin Node only コマンドのメッセージが表示されます。

3. SSO を無効にすることを確認します。

   ノードでシングルサインオンが無効になったことを示すメッセージが表示されます。

4. Web ブラウザから、同じ管理ノード上の Grid Manager にアクセスする。

   SSO を無効にしたため、 Grid Manager のサインインページが表示されます。

5. ユーザ名「 root 」とローカルの root ユーザのパスワードを使用してサインインします。
6. SSO 設定の修正が必要なために SSO を一時的に無効にした場合は、次の手順を実行します
   a. [* 設定 * > * アクセス制御 * > * シングルサインオン *] を選択します。
   b. 正しくない SSO 設定または古い SSO 設定を変更します。
   c. [保存（ Save ）] を選択します。

      シングルサインオンページから * Save * を選択すると、グリッド全体で SSO が自動的に再有効化されます。

7. 他の理由で Grid Manager へのアクセスが必要であったために SSO を一時的に無効にした場合は、次の手順を実行します。
   a. 必要なタスクを実行します。
   b. [サインアウト]*を選択し、Grid Managerを閉じます。
   c. 管理ノードで SSO を再度有効にします。次のいずれかの手順を実行します。

      - 次のコマンドを実行します。 `enable-saml`

        環境 this admin Node only コマンドのメッセージが表示されます。

   SSO を有効にすることを確認します。

ノードでシングルサインオンが有効になったことを示すメッセージが表示されます。

- グリッドノードをリブートします。 `reboot`

8. Web ブラウザから、同じ管理ノードから Grid Manager にアクセスする。
9. StorageGRID のサインインページが表示され、グリッドマネージャにアクセスするには SSO クレデンシャルを入力する必要があることを確認します。

グリッドフェデレーションを使用する

グリッドフェデレーションとは

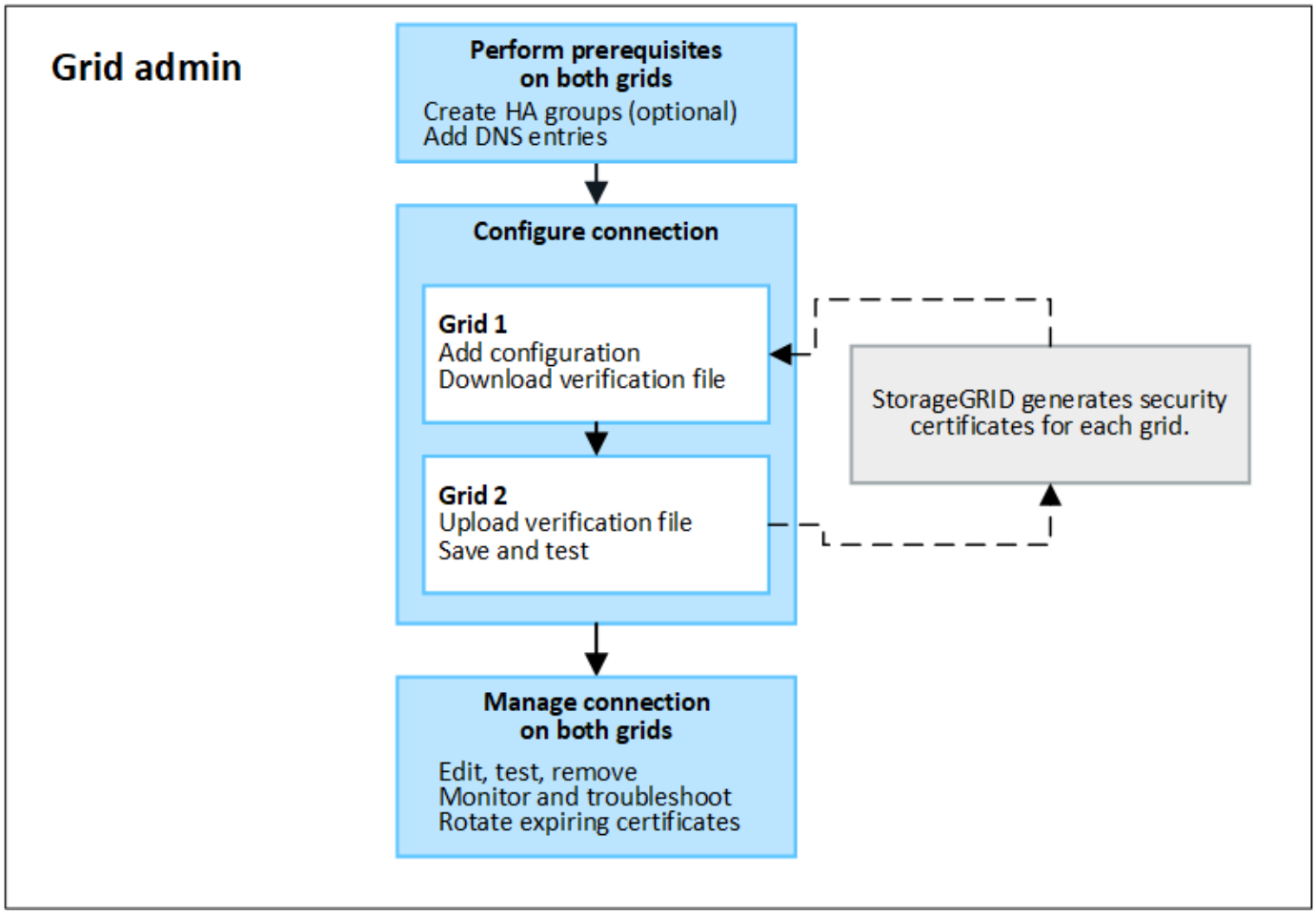
グリッドフェデレーションを使用すると、ディザスタリカバリ用にテナントをクローニングし、2つのStorageGRID システム間でオブジェクトをレプリケートできます。

グリッドフェデレーション接続とは何ですか？

グリッドフェデレーション接続は、2つのStorageGRID システムの管理ノードとゲートウェイノードの間の双方向の信頼されたセキュアな接続です。

グリッドフェデレーションのワークフロー

ワークフロー図は、2つのグリッド間のグリッドフェデレーション接続を設定する手順をまとめたものです。



グリッドフェデレーション接続に関する考慮事項と要件

- グリッドフェデレーションに使用する両方のグリッドでStorageGRID 11.7が実行されている必要があります。
- グリッドは、他のグリッドへの1つ以上のグリッドフェデレーション接続を持つことができます。各グリッドフェデレーション接続は、他の接続とは独立しています。たとえば、Grid 1がGrid 2と1つの接続を持ち、Grid 3と2つ目の接続を持つ場合、Grid 2とGrid 3の間に暗黙的な接続はありません。
- グリッドフェデレーション接続は双方向です。接続が確立されたら、どちらのグリッドからも接続を監視および管理できます。
- を使用するには、グリッドフェデレーション接続が少なくとも1つ存在している必要があります "アカウントのクローン" または "グリッド間レプリケーション"。

ネットワークとIPアドレスの要件

- グリッドフェデレーション接続は、グリッドネットワーク、管理ネットワーク、またはクライアントネットワークで確立できます。
- グリッドフェデレーション接続は、あるグリッドを別のグリッドに接続します。各グリッドの設定では、管理ノード、ゲートウェイノード、またはその両方で構成されるもう一方のグリッド上のグリッドフェデレーションエンドポイントを指定します。
- 接続することを推奨します "ハイアベイラビリティ（HA）グループ" 各グリッド上のゲートウェイノードと管理ノードの数。HAグループを使用すると、ノードを使用できなくなってもグリッドフェデレーション接続をオンラインのまま維持できます。いずれかのHAグループのアクティブインターフェイスで障害が発生した場合は、バックアップインターフェイスを使用して接続を確立できます。
- 単一の管理ノードまたはゲートウェイノードのIPアドレスを使用するグリッドフェデレーション接続を作成することは推奨されません。ノードが使用できなくなると、グリッドフェデレーション接続も使用できなくなります。
- "グリッド間レプリケーション" オブジェクトの数を増やすには、各グリッドのストレージノードが、もう一方のグリッドに設定されている管理ノードとゲートウェイノードにアクセスできる必要があります。グリッドごとに、すべてのストレージノードが、接続に使用する管理ノードまたはゲートウェイノードとしてへの広帯域幅ルートを持っていることを確認します。

FQDNを使用して接続の負荷を分散します

本番環境では、Fully Qualified Domain Name（FQDN；完全修飾ドメイン名）を使用して接続内の各グリッドを識別します。次に、次のように適切なDNSエントリを作成します。

- Grid 1のFQDNを、Grid 1のHAグループの1つ以上の仮想IP（VIP）アドレス、またはGrid 1の1つ以上の管理ノードまたはゲートウェイノードのIPアドレスにマッピングします。
- Grid 2のFQDNを、Grid 2の1つ以上のVIPアドレス、またはGrid 2内の1つ以上の管理ノードまたはゲートウェイノードのIPアドレスにマッピングします。

複数のDNSエントリを使用する場合、接続を使用する要求は次のようにロードバランシングされます。

- 複数のHAグループのVIPアドレスにマッピングされたDNSエントリは、HAグループ内のアクティブノード間で負荷分散されます。
- 複数の管理ノードまたはゲートウェイノードのIPアドレスにマッピングされたDNSエントリは、マッピングしたノード間で負荷分散されます。

ポート要件

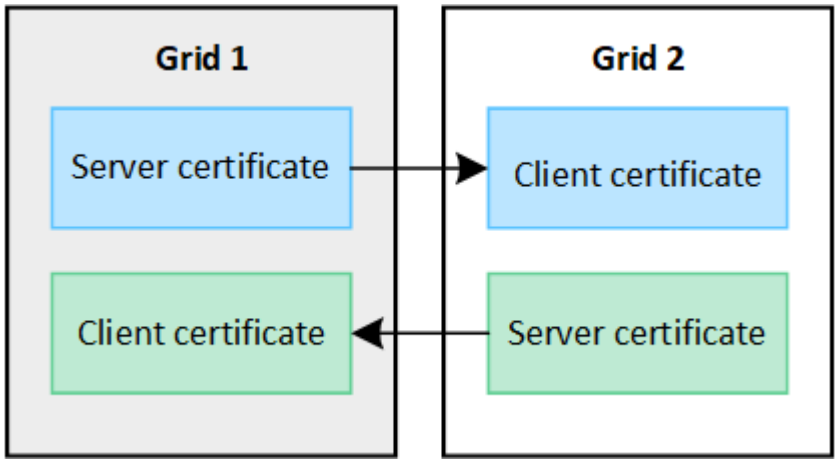
グリッドフェデレーション接続を作成するときは、未使用のポート番号（23000~23999）を指定できます。この接続の両方のグリッドが同じポートを使用します。

どちらのグリッドでも、このポートを他の接続に使用しているノードがないことを確認する必要があります。

証明書の要件

グリッドフェデレーション接続を設定すると、StorageGRID によって次の4つのSSL証明書が自動的に生成されます。

- グリッド1からグリッド2に送信される情報を認証および暗号化するためのサーバ証明書とクライアント証明書
- グリッド2からグリッド1に送信される情報を認証および暗号化するためのサーバ証明書とクライアント証明書



デフォルトでは、証明書の有効期間は730日間（2年間）です。これらの証明書の有効期限が近づくと、* Expiration of grid federation certificate *アラートによって証明書のローテーションを要求されます。これはGrid Managerを使用して実行できます。

> 接続のいずれかの側の証明書が期限切れになると、接続は動作を停止します。証明書が更新されるまで、データレプリケーションは保留されます。

詳細はこちら。

- "グリッドフェデレーション接続を作成する"
- "グリッドフェデレーション接続を管理します"
- "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"

アカウントクローンとは何ですか？

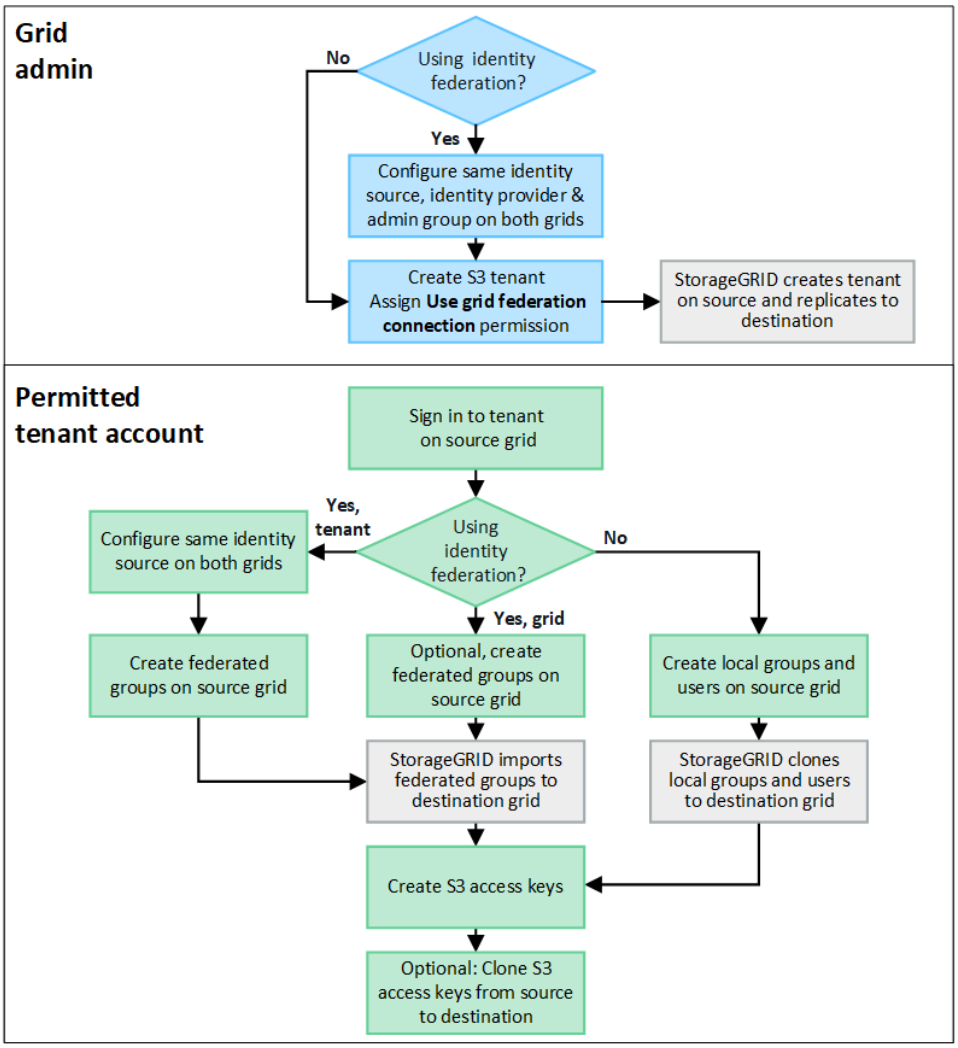
アカウントのクローンは、テナントアカウント、テナントグループ、テナントユーザの自動レプリケーションです。必要に応じて、 内のStorageGRID システム間のS3アクセスキー "グリッドフェデレーション接続"。

ではアカウントのクローンが必要です "グリッド間レプリケーション"。アカウント情報をソースStorageGRID

システムからデスティネーションStorageGRID システムにクローニングすると、テナントユーザとテナントグループがどちらのグリッド上の対応するバケットとオブジェクトにアクセスできるようになります。

アカウントクローンのワークフロー

次のワークフロー図は、グリッド管理者および許可されたテナントがアカウントのクローンを設定するために実行する手順を示しています。これらの手順は、のあとに実行します "グリッドフェデレーション接続が設定されました"。



Grid管理ワークフロー

グリッド管理者が実行する手順は、内のStorageGRID システムかどうかによって異なります "グリッドフェデレーション接続" シングルサインオン（SSO）またはアイデンティティフェデレーションを使用

アカウントクローン用の**SSO**の設定（オプション）

グリッドフェデレーション接続のいずれかのStorageGRID システムでSSOを使用する場合は、両方のグリッドでSSOを使用する必要があります。グリッドフェデレーション用のテナントアカウントを作成する前に、テナントのソースグリッドとデスティネーショングリッドのグリッド管理者が次の手順を実行する必要があります。

手順

1. 両方のグリッドに同じアイデンティティソースを設定します。を参照してください "アイデンティティフェデレーションを使用する"。
2. 両方のグリッドに同じSSO IDプロバイダ（IdP）を設定します。を参照してください "シングルサインオンを設定します"。
3. "同じ管理者グループを作成します" 両方のグリッドで同じフェデレーテッドグループをインポートする。

   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。

アカウントクローン用のグリッドレベルのアイデンティティフェデレーションを設定する（オプション）

どちらかのStorageGRID システムがSSOなしでアイデンティティフェデレーションを使用する場合は、両方のグリッドでアイデンティティフェデレーションを使用する必要があります。グリッドフェデレーション用のテナントアカウントを作成する前に、テナントのソースグリッドとデスティネーショングリッドのグリッド管理者が次の手順を実行する必要があります。

手順

1. 両方のグリッドに同じアイデンティティソースを設定します。を参照してください "アイデンティティフェデレーションを使用する"。
2. 必要に応じて、フェデレーテッドグループに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最初のRootアクセス権限が割り当てられる場合は、 "同じ管理者グループを作成します" 両方のグリッドで同じフェデレーテッドグループをインポートする。

   両方のグリッドに存在しないフェデレーテッドグループにRoot Access権限を割り当てた場合、テナントはデスティネーショングリッドにレプリケートされません。

3. フェデレーテッドグループに両方のアカウントに対する最初のRoot Access権限を付与しない場合は、ローカルrootユーザのパスワードを指定します。

許可された**S3**テナントアカウントを作成します

SSOまたはアイデンティティフェデレーションを必要に応じて設定したら、グリッド管理者が次の手順を実行して、バケットオブジェクトを他のStorageGRID システムにレプリケートできるテナントを特定します。

手順

1. アカウントのクローニング処理でテナントのソースグリッドにするグリッドを決定します。

   テナントが最初に作成されたグリッドは、テナントの_source grid_と呼ばれます。テナントがレプリケートされるグリッドは、テナントの_destination grid_と呼ばれます。

2. そのグリッドに新しいS3テナントアカウントを作成します。
3. Use grid federation connection *権限を割り当てます。
4. テナントアカウントで独自のフェデレーテッドユーザを管理する場合は、* Use own identity source *権限を割り当てます。

この権限が割り当てられている場合は、フェデレーテッドグループを作成する前に、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で同じアイデンティティソースを設定する必要があります。両方のグリッドで同じアイデンティティソースを使用している場合を除き、ソーステナントに追加されたフェデレーテッドグループをデスティネーションテナントにクローニングすることはできません。

5. 特定のグリッドフェデレーション接続を選択します。
6. テナントを保存します。

   [Use grid federation connection]*権限が設定された新しいテナントが保存されると、StorageGRID は次のように、そのテナントのレプリカをもう一方のグリッドに自動的に作成します。

   - 両方のテナントアカウントで、アカウントID、名前、ストレージクォータ、および権限が同じになります。
   - テナントに対するRootアクセス権限を持つフェデレーテッドグループを選択した場合は、そのグループがデスティネーションテナントにクローニングされます。
   - テナントに対するRootアクセス権限を持つローカルユーザを選択した場合、そのユーザはデスティネーションテナントにクローニングされます。ただし、そのユーザのパスワードはクローニングされません。

詳細については、を参照してください"グリッドフェデレーションで許可されるテナントを管理します"。

許可されているテナントアカウントのワークフロー

Use grid federation connection *権限を持つテナントがデスティネーショングリッドにレプリケートされたら、許可されたテナントアカウントで次の手順を実行してテナントグループ、ユーザ、S3アクセスキーをクローニングできます。

手順

1. テナントのソースグリッドでテナントアカウントにサインインします。
2. 許可されている場合は、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でフェデレーションの識別を設定します。
3. ソーステナントでグループとユーザを作成します。

   ソーステナントで新しいグループまたはユーザが作成されると、StorageGRID によって自動的にデスティネーションテナントにクローニングされますが、デスティネーションからソースへのクローニングは行われません。

4. S3アクセスキーを作成
5. 必要に応じて、ソーステナントからデスティネーションテナントにS3アクセスキーをクローニングします。

許可されるテナントアカウントのワークフローの詳細、およびグループ、ユーザ、S3アクセスキーのクローニング方法については、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" および "APIを使用してS3アクセスキーをクローニングします"。

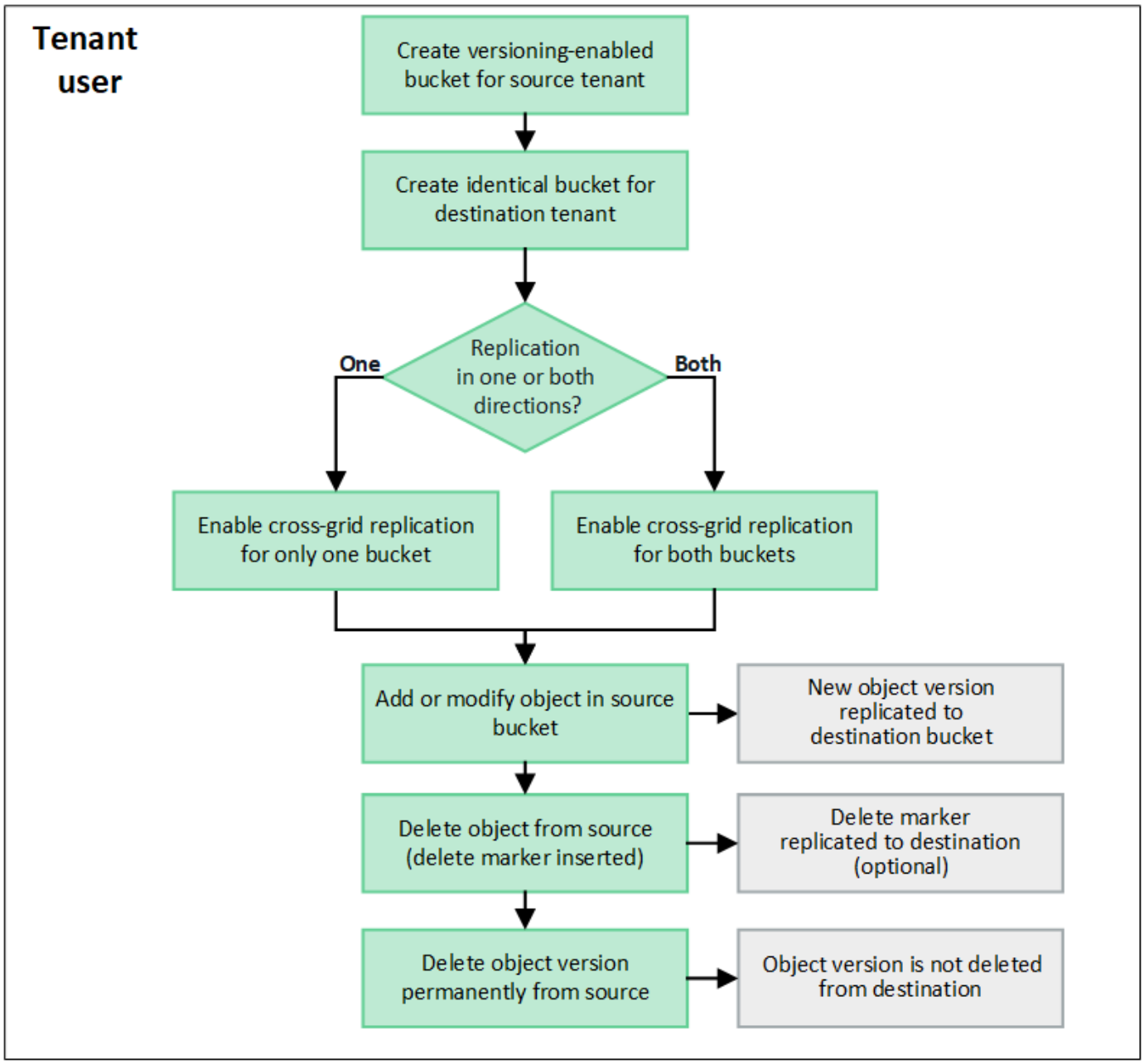
クロスグリッドレプリケーションとは何ですか。

グリッド間レプリケーションは、に接続された2つのStorageGRID システム内の選択したS3バケット間でオブジェクトを自動的にレプリケートするレプリケーションです "グ

リッドフェデレーション接続"。 "アカウントのクローン" は、グリッド間レプリケーションに必要です。

グリッド間レプリケーションのワークフロー

次のワークフロー図は、2つのグリッド上のバケット間でグリッド間レプリケーションを設定する手順をまとめたものです。



グリッド間レプリケーションの要件

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1つ以上を使用します "グリッドフェデレーション接続"では、Root Access権限を持つテナントユーザは、各グリッドの対応するテナントアカウントに同一のバケットを作成できます。次のバケットがあります。

- 名前とリージョンが同じである必要があります

- バージョン管理が有効になっている必要があります
- S3オブジェクトロックを無効にする必要があります
- 空にする必要があります

両方のバケットが作成されたら、一方または両方のバケットに対してクロスグリッドレプリケーションを設定できます。

詳細はこちら。

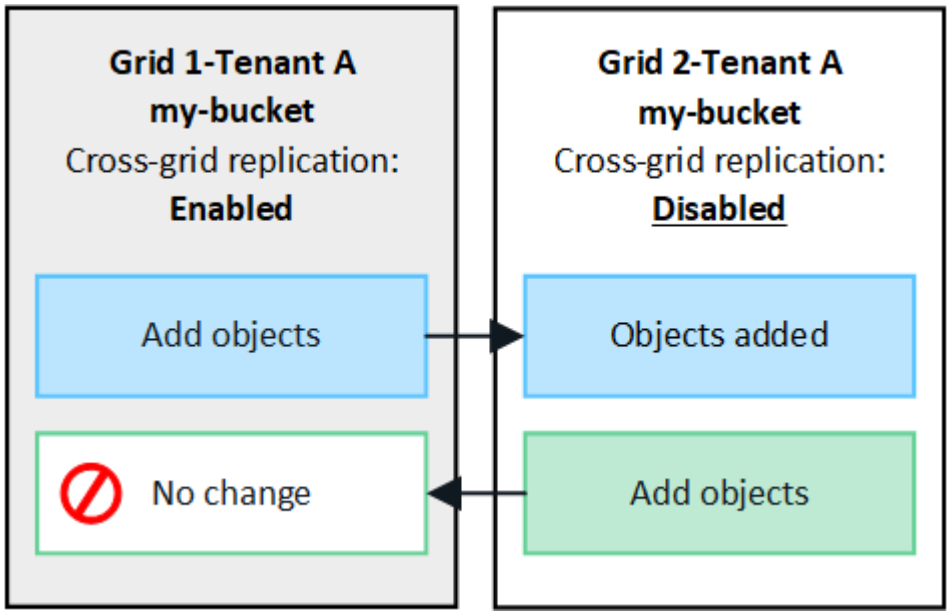
"グリッド間レプリケーションを管理します"

グリッド間レプリケーションの仕組み

グリッド間レプリケーションは、一方向または双方向に実行するように設定できます。

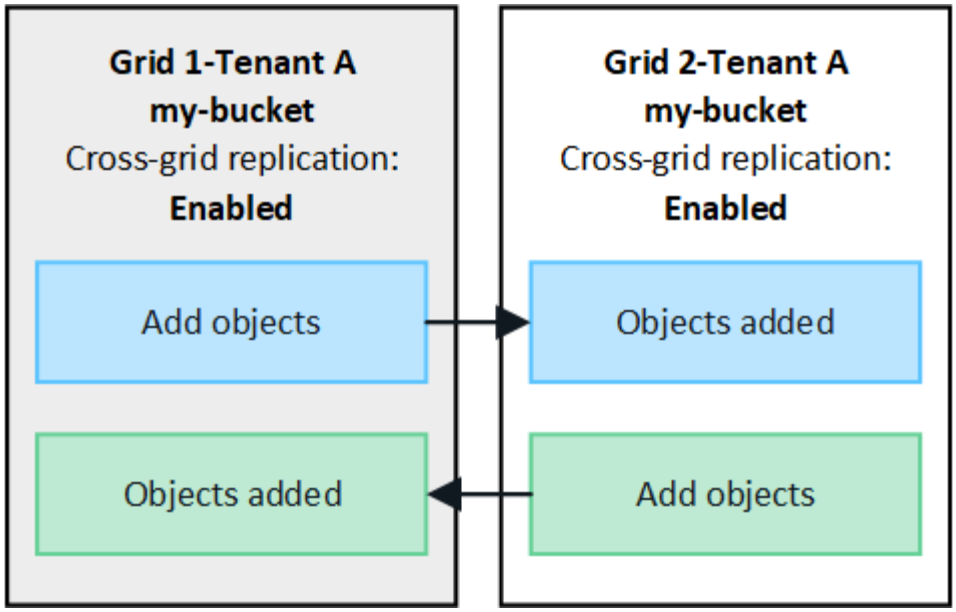
一方向のレプリケーション

あるバケットでグリッド間レプリケーションを有効にしたグリッドが1つだけの場合は、そのバケット（ソースバケット）に追加されたオブジェクトがもう一方のグリッド（デスティネーションバケット）の対応するバケットにレプリケートされます。ただし、デスティネーションバケットに追加されたオブジェクトはソースにレプリケートされません。次の図では、に対してグリッド間レプリケーションが有効になっています `my-bucket` グリッド1からグリッド2までですが、反対方向では有効になっていません。



双方向のレプリケーション

両方のグリッドで同じバケットに対してクロスグリッドレプリケーションを有効にすると、一方のバケットに追加されたオブジェクトがもう一方のグリッドにレプリケートされます。次の図では、に対してグリッド間レプリケーションが有効になっています `my-bucket` 両方向に。



オブジェクトが取り込まれるとどうなりますか？

S3クライアントが、クロスグリッドレプリケーションが有効になっているバケットにオブジェクトを追加すると、次の処理が実行されます。

1. StorageGRID は、ソースバケットからデスティネーションバケットにオブジェクトを自動的にレプリケートします。このバックグラウンドレプリケーション処理の実行時間は、保留中の他のレプリケーション処理の数など、いくつかの要因によって異なります。

   S3クライアントは、GET Object要求またはHEAD Object要求を発行して、オブジェクトのレプリケーションステータスを確認できます。応答にはStorageGRID固有のものが含まれます `x-ntap-sg-cgr-replication-status` 応答ヘッダーには次のいずれかの値が表示されます。S3クライアントは、GET Object要求またはHEAD Object要求を実行してオブジェクトのレプリケーションステータスを確認できます。応答にはStorageGRID固有のものが含まれます `x-ntap-sg-cgr-replication-status` 応答ヘッダー。次のいずれかの値が設定されます。

グリッド（ **Grid** ）	レプリケーションのステータス
ソース	• 成功：すべてのグリッド接続でレプリケーションが成功しました。 • * pending *：オブジェクトは少なくとも1つのグリッド接続にレプリケートされていません。 • 失敗：どのグリッド接続に対してもレプリケーションが保留中ではなく、少なくとも1つが永続的なエラーで失敗しました。ユーザーはエラーを解決する必要があります。
宛先	**replica**:オブジェクトはソースグリッドからレプリケートされました。

   StorageGRID ではがサポートされません `x-amz-replication-status` ヘッダー。

2. StorageGRID は、他のオブジェクトと同様に、各グリッドのアクティブなILMポリシーを使用してオブジ

ェクトを管理します。たとえば、グリッド1のオブジェクトAは2つのレプリケートコピーとして格納されて無期限に保持されるのに対し、グリッド2にレプリケートされたオブジェクトAのコピーは2+1のイレイジャーコーディングを使用して格納され、3年後に削除されるとします。

オブジェクトが削除されるとどうなりますか？

を参照してください "データフローを削除します"StorageGRID は、次のいずれかの理由でオブジェクトを削除できます。

- S3クライアントが削除要求を実行します。
- Tenant Managerユーザがを選択します "バケット内のオブジェクトを削除する" バケットからすべてのオブジェクトを削除するオプション。
- バケットにはライフサイクル設定があり、有効期限が切れます。
- オブジェクトのILMルールの最後の期間が終了し、それ以上の配置が指定されていない。

[Delete objects in bucket]処理、バケットライフサイクルの有効期限、またはILM配置の有効期限が原因でStorageGRID がオブジェクトを削除しても、レプリケートオブジェクトがグリッドフェデレーション接続の他のグリッドから削除されることはありません。ただし、S3クライアントによる削除によってソースバケットに追加された削除マーカーは、必要に応じてデスティネーションバケットにレプリケートできます。

クロスグリッドレプリケーションが有効になっているバケットからS3クライアントがオブジェクトを削除した場合の動作を理解するには、バージョン管理が有効になっているバケットからS3クライアントがオブジェクトを削除する仕組みを次のように確認してください。

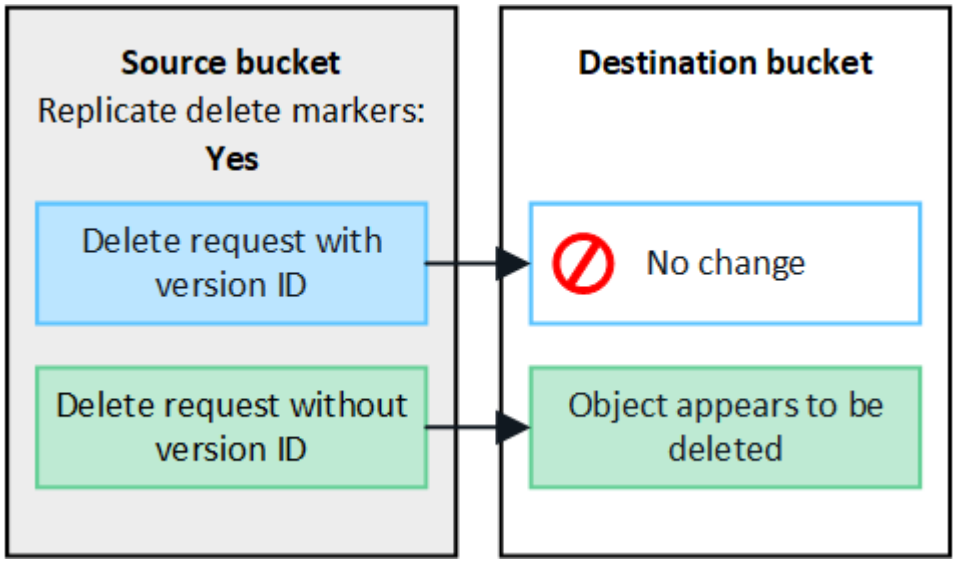
- S3クライアントがバージョンIDを含む削除要求を実行すると、そのバージョンのオブジェクトが完全に削除されます。バケットに削除マーカーは追加されません。
- S3クライアントがバージョンIDを含まない削除要求を実行した場合、StorageGRID はオブジェクトバージョンを削除しません。代わりに、バケットに削除マーカーを追加します。削除マーカーを使用すると、StorageGRID はオブジェクトが削除されたかのように動作します。
  - バージョンIDを指定しないGET要求はで失敗します `404 No Object Found`
  - 有効なバージョンIDを持つGET要求が成功し、要求されたオブジェクトのバージョンが返されます。

S3クライアントがクロスグリッドレプリケーションが有効になっているバケットからオブジェクトを削除すると、StorageGRID は次のように削除要求をデスティネーションにレプリケートするかどうかを判断します。

- 削除要求にバージョンIDが含まれている場合は、そのオブジェクトバージョンがソースグリッドから完全に削除されます。ただし、StorageGRID はバージョンIDを含む削除要求をレプリケートしないため、同じオブジェクトバージョンがデスティネーションから削除されることはありません。
- 削除要求にバージョンIDが含まれていない場合は、バケットのクロスグリッドレプリケーションの設定に基づいて、StorageGRID で削除マーカーをレプリケートすることもできます。
  - 削除マーカーをレプリケートするように選択した場合（デフォルト）は、削除マーカーがソースバケットに追加され、デスティネーションバケットにレプリケートされます。実際には、オブジェクトは両方のグリッドで削除されているように見えます。
  - 削除マーカーをレプリケートしないように選択した場合、削除マーカーはソースバケットに追加されますが、デスティネーションバケットにはレプリケートされません。実際には、ソースグリッドで削除されたオブジェクトはデスティネーショングリッドでは削除されません。

この図では、*レプリケート削除マーカー*が*はい*に設定されています "クロスグリッドレプリケーションが

有効になりました"。バージョンIDを含むソースバケットの削除要求では、デスティネーションバケットからオブジェクトは削除されません。ソースバケットに対するバージョンIDを含まない削除要求は、デスティネーションバケット内のオブジェクトを削除するように表示されます。



オブジェクトの削除をグリッド間で同期したままにする場合は、対応するを作成します "S3ライフサイクル設定" 両方のグリッドのバケット用。

暗号化されたオブジェクトのレプリケート方法

グリッド間レプリケーションを使用してグリッド間でオブジェクトをレプリケートする場合は、個 々 のオブジェクトを暗号化するか、デフォルトのバケット暗号化を使用するか、またはグリッド全体の暗号化を設定できます。バケットに対してグリッド間レプリケーションを有効にする前後に、デフォルトのバケットまたはグリッド全体の暗号化設定を追加、変更、または削除できます。

個 々 のオブジェクトを暗号化するには、SSE（StorageGRIDで管理されるキーによるサーバ側の暗号化）を使用してオブジェクトをソースバケットに追加します。を使用します `x-amz-server-side-encryption` 要求ヘッダーとを指定します `AES256`。を参照してください "サーバ側の暗号化を使用します"。

SSE-C（ユーザ指定のキーによるサーバ側の暗号化）の使用は、グリッド間レプリケーションではサポートされていません。取り込み処理は失敗します。

バケットでデフォルトの暗号化を使用するには、PUT bucket暗号化要求を使用してを設定します `SSEAlgorithm` パラメータの値 `AES256`。バケットレベルの暗号化環境 なしで取り込まれたすべてのオブジェクト `x-amz-server-side-encryption` 要求ヘッダー。を参照してください "バケットの処理"。

グリッドレベルの暗号化を使用するには、* stored object encryption オプションを AES-256 *に設定します。グリッドレベルの暗号化環境 バケットレベルで暗号化されていないオブジェクト、またはなしで取り込まれたオブジェクト `x-amz-server-side-encryption` 要求ヘッダー。を参照してください "ネットワークとオブジェクトのオプションを設定します"。

SSEはAES-128をサポートしていません。aes-128 オプションを使用してソースグリッドで stored object encryption *オプションを有効にした場合、AES-128アルゴリズムの使用はレプリケートオブジェクトに伝播されません。代わりに、デスティネーションのデフォルトのバケットまたはグリッドレベルの暗号化設定（利用可能な場合）がレプリケートオブジェクトで使用されます。

ソースオブジェクトの暗号化方法を決定する際に、StorageGRID は次のルールを適用します。

1. を使用します `x-amz-server-side-encryption` 取り込みヘッダー（存在する場合）。
2. 取り込みヘッダーがない場合は、バケットのデフォルトの暗号化設定（設定されている場合）を使用します。
3. バケット設定が設定されていない場合は、グリッド全体の暗号化設定を使用します（設定されている場合）。
4. グリッド全体の設定がない場合は、ソースオブジェクトを暗号化しないでください。

StorageGRID では、レプリケートオブジェクトの暗号化方法を決定する際に、次の順序でルールが適用されます。

1. ソースオブジェクトがAES-128暗号化を使用している場合を除き、ソースオブジェクトと同じ暗号化を使用します。
2. ソースオブジェクトが暗号化されていない場合やAES-128を使用している場合は、デスティネーションバケットのデフォルトの暗号化設定（設定されている場合）を使用します。
3. デスティネーションバケットに暗号化設定がない場合は、デスティネーションのグリッド全体の暗号化設定を使用します（設定されている場合）。
4. グリッド全体の設定がない場合は、デスティネーションオブジェクトを暗号化しないでください。

PUT Object taggingと**DELETE Object tagging**はサポートされません

クロスグリッドレプリケーションが有効になっているバケット内のオブジェクトでは、PUT Object tagging要求とDELETE Object tagging要求はサポートされません。

S3クライアントがPUT Object tagging要求またはDELETE Object tagging要求を実行すると、 `501 Not Implemented` が返されます。メッセージはです `Put(Delete) ObjectTagging is not available for buckets that have cross-grid replication configured`。

セグメント化されたオブジェクトのレプリケート方法

ソースグリッドの最大セグメントサイズ環境 オブジェクトがデスティネーショングリッドにレプリケートされます。オブジェクトが別のグリッドにレプリケートされる場合、ソースグリッドの*最大セグメントサイズ*設定（構成>*システム*>*ストレージオプション*）が両方のグリッドで使用されます。たとえば、ソースグリッドの最大セグメントサイズが1GBで、デスティネーショングリッドの最大セグメントサイズが50MBであるとします。2GBのオブジェクトをソースグリッドに取り込むと、そのオブジェクトは2GBのセグメントとして保存されます。また、グリッドの最大セグメントサイズが50MBであっても、2つの1GBセグメントとしてデスティネーショングリッドにレプリケートされます。

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

グリッドフェデレーションの使用を開始する際に、両者の類似点と相違点を確認してください "グリッド間レプリケーション" および "StorageGRID CloudMirror レプリケーシ

ョンサービス"。

	グリッド間レプリケーション	**CloudMirror** レプリケーションサービス
主な目的は何ですか？	1つのStorageGRID システムがディザスタリカバリシステムとして機能します。バケット内のオブジェクトは、グリッド間で一方向または両方向にレプリケートできます。	テナントで、StorageGRID （ソース）内のバケットから外部のS3バケット（デスティネーション）にオブジェクトを自動的にレプリケートできます。 CloudMirror レプリケーションでは、独立した S3 インフラにオブジェクトの独立したコピーが作成されます。この独立したコピーはバックアップとしては使用されませんが、多くの場合、クラウドでさらに処理されます。
セットアップ方法は？	1. 2つのグリッド間のグリッドフェデレーション接続を設定します。 2. 新しいテナントアカウントを追加します。このアカウントは自動的にもう一方のグリッドにクローニングされます。 3. 新しいテナントグループとユーザを追加します。これらもクローンとして作成されます。 4. 各グリッドに対応するバケットを作成し、一方向または両方向でグリッド間レプリケーションを実行できるようにします。	1. テナントユーザは、Tenant ManagerまたはS3 APIを使用してCloudMirrorエンドポイント（IPアドレス、クレデンシャルなど）を定義することによってCloudMirrorレプリケーションを設定します。 2. そのテナントアカウントが所有するバケットは、CloudMirrorエンドポイントを指すように設定できます。
設定は誰が担当しますか？	• グリッド管理者が接続とテナントを設定します。 • テナントユーザは、グループ、ユーザ、キー、およびバケットを設定します。	通常はテナントユーザです。
デスティネーションは何ですか？	グリッドフェデレーション接続内のもう一方のStorageGRID システム上の、対応する同一のS3バケット。	• 互換性のある任意のS3インフラ（Amazon S3を含む）。 • Google Cloud Platform （ GCP ）
オブジェクトのバージョン管理は必要ですか。	はい。ソースバケットとデスティネーションバケットの両方でオブジェクトのバージョン管理を有効にする必要があります。	いいえ。CloudMirrorレプリケーションでは、ソースとデスティネーションの両方で、バージョン管理に対応していないバケットとバージョン管理に対応していないバケットを任意に組み合わせて使用できます。

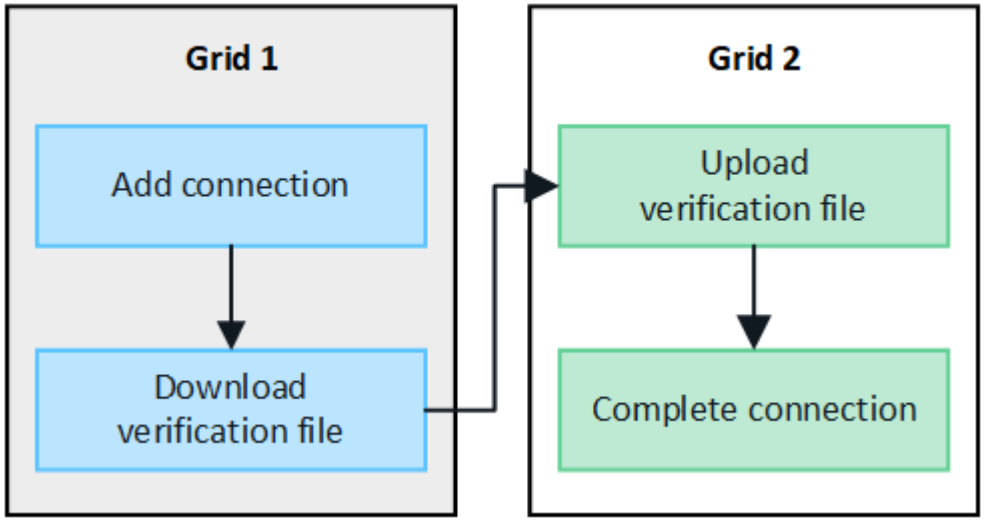
	グリッド間レプリケーション	**CloudMirror** レプリケーションサービス
オブジェクトをデスティネーションに移動する原因は何ですか？	オブジェクトは、グリッド間レプリケーションが有効になっているバケットに追加されると自動的にレプリケートされます。	CloudMirrorエンドポイントが設定されたバケットにオブジェクトが追加されると、オブジェクトが自動的にレプリケートされます。CloudMirrorエンドポイントを設定する前にソースバケットに存在していたオブジェクトは、変更しないかぎりレプリケートされません。
オブジェクトのレプリケート方法	グリッド間レプリケーションでバージョン管理オブジェクトが作成され、バージョンIDがソースバケットからデスティネーションバケットにレプリケートされます。これにより、両方のグリッドでバージョンの順序を維持できます。	CloudMirrorレプリケーションではバージョン管理が有効なバケットは必要ないため、CloudMirrorではサイト内のキーの順序のみを維持できます。別のサイトにあるオブジェクトへの要求の順序が維持される保証はありません。
オブジェクトをレプリケートできない場合はどうなりますか。	オブジェクトは、メタデータストレージの制限に従ってレプリケーションのキューに登録されます。	オブジェクトは、プラットフォームサービスの制限に従ってレプリケーションのキューに登録されます（を参照） "プラットフォームサービスの使用に関する推奨事項"）。
オブジェクトのシステムメタデータはレプリケートされているか？	はい。オブジェクトが他のグリッドにレプリケートされると、そのシステムメタデータもレプリケートされます。メタデータは両方のグリッドで同一になります。	いいえ。オブジェクトが外部バケットにレプリケートされると、そのシステムメタデータが更新されます。メタデータは場所によって異なり、取り込み時間や独立したS3インフラの動作によって異なります。
オブジェクトの読み出し方法	アプリケーションは、いずれかのグリッドのバケットに要求することで、オブジェクトを読み出すことができます。	アプリケーションは、StorageGRID またはS3デスティネーションに要求を行うことで、オブジェクトの読み出しや読み取りを行うことができます。たとえば、 CloudMirror レプリケーションを使用してパートナー組織にオブジェクトをミラーリングするとします。パートナーは、独自のアプリケーションを使用して、 S3 デスティネーションからオブジェクトを直接読み取ったり更新したりできます。StorageGRID を使用する必要はありません。

	グリッド間レプリケーション	**CloudMirror** レプリケーションサービス
オブジェクトが削除された場合の動作	• バージョンIDを含む削除要求は、デスティネーショングリッドにレプリケートされません。 • バージョンIDが含まれていない削除要求では、ソースバケットに削除マーカーが追加され、必要に応じてデスティネーショングリッドにレプリケートできます。 • グリッド間レプリケーションが一方向のみに設定されている場合は、ソースに影響を与えずにデスティネーションバケット内のオブジェクトを削除できます。	結果は、ソースバケットとデスティネーションバケットのバージョン管理状態によって異なります（同じである必要はありません）。 • 両方のバケットがバージョン管理に対応している場合は、削除要求によって両方の場所に削除マーカーが追加されます。 • ソースバケットのみがバージョン管理に対応している場合、削除要求ではソースに削除マーカーが追加されますが、デスティネーションには追加されません。 • どちらのバケットもバージョン管理に対応していない場合、削除要求によってソースからはオブジェクトが削除されますが、デスティネーションからは削除されません。 同様に、デスティネーションバケット内のオブジェクトもソースに影響を与えることなく削除できます。

グリッドフェデレーション接続を作成する

テナントの詳細をクローニングしてオブジェクトデータをレプリケートする場合は、2つのStorageGRID システム間にグリッドフェデレーション接続を作成できます。

図に示すように、グリッド連携接続の作成には、両方のグリッドでの手順が含まれます。一方のグリッドに接続を追加し、もう一方のグリッドで接続を完了します。どちらのグリッドからでも開始できます。



作業を開始する前に

- を確認しておきます "考慮事項と要件" グリッドフェデレーション接続の設定に使用します。
- 各グリッドにIPアドレスまたはVIPアドレスの代わりに完全修飾ドメイン名（FQDN）を使用する場合

は、使用する名前を確認し、各グリッドのDNSサーバに適切なエントリがあることを確認しておきます。

- を使用している "サポートされている Web ブラウザ"。
- 両方のグリッドのRootアクセス権限とプロビジョニングパスフレーズが必要です。

接続を追加します

次の手順は、2つのStorageGRID システムのどちらかで実行します。

手順

1. いずれかのグリッドのプライマリ管理ノードからGrid Managerにサインインします。
2. **>**[システム]**>**[グリッドフェデレーション]*を選択します。
3. [接続の追加]*を選択します。
4. 接続の詳細を入力します。

フィールド	説明
接続名	この接続を識別するための一意の名前。たとえば、「`Grid 1 - Grid 2」のように入力します。
このグリッドのFQDNまたはIP	次のいずれか • 現在サインインしているグリッドのFQDN • このグリッド上のHAグループのVIPアドレスです • このグリッド上の管理ノードまたはゲートウェイノードのIPアドレス。IPは、デスティネーショングリッドが到達可能な任意のネットワーク上に設定できます。
ポート	この接続に使用するポート。23000～23999の任意の未使用ポート番号を入力できます。 この接続の両方のグリッドが同じポートを使用します。どちらのグリッドでも、このポートを他の接続に使用しているノードがないことを確認する必要があります。
このグリッドの証明書有効日数	接続内のこのグリッドのセキュリティ証明書を有効にする日数。デフォルト値は730日（2年）ですが、1～762日の任意の値を入力できます。 接続を保存すると、StorageGRID で各グリッドのクライアント証明書とサーバ証明書が自動的に生成されます。
このグリッドのプロビジョニングパスフレーズ	サインインしているグリッドのプロビジョニングパスフレーズ。

フィールド	説明
もう一方のグリッドのFQDNまたはIP	次のいずれか • 接続先のグリッドのFQDN • もう一方のグリッド上のHAグループのVIPアドレスです • もう一方のグリッド上の管理ノードまたはゲートウェイノードのIPアドレス。IPは、ソースグリッドが到達可能な任意のネットワーク上に設定できます。

5. [保存して続行]*を選択します。
6. [検証ファイルのダウンロード]ステップで、*[検証ファイルのダウンロード]*を選択します。

   もう一方のグリッドで接続が完了すると、どちらのグリッドからも検証ファイルをダウンロードできなくなります。

7. ダウンロードしたファイルを見つけます (*connection-name*.grid-federation）をクリックし、安全な場所に保存します。

   このファイルにはシークレット（としてマスク）が含まれています *)およびその他の機密情報を安全に保存して送信する必要があります。

8. [Close]*を選択して、[Grid Federation]ページに戻ります。
9. 新しい接続が表示され、*接続ステータス*が*接続待ち*になっていることを確認します。
10. を指定します *connection-name*.grid-federation ファイルを他のグリッドのグリッド管理者に送信します。

接続を完了します

接続先のStorageGRID システム（もう一方のグリッド）で次の手順を実行します。

手順

1. プライマリ管理ノードからGrid Managerにサインインします。
2. >[システム]>[グリッドフェデレーション]*を選択します。
3. [Upload verification file]*を選択して、[Upload]ページにアクセスします。
4. [検証ファイルのアップロード]*を選択します。次に、最初のグリッドからダウンロードしたファイルを参照して選択します (*connection-name*.grid-federation）。

   接続の詳細が表示されます。

5. 必要に応じて、このグリッドのセキュリティ証明書に別の有効な日数を入力します。[Certificate Valid Days]*エントリは、最初のグリッドに入力した値にデフォルトで設定されますが、各グリッドでは異なる有効期限を使用できます。

   一般に、接続の両側の証明書には同じ日数を使用します。

接続のいずれかの側の証明書が期限切れになると、接続は動作を停止し、証明書が更新されるまでレプリケーションは保留になります。

6. 現在サインインしているグリッドのプロビジョニングパスフレーズを入力します。
7. [保存してテスト]*を選択します。

   証明書が生成され、接続がテストされます。接続が有効な場合は、成功を示すメッセージが表示され、[Grid Federation]ページに新しい接続がリストされます。は[接続済み]*になります。

   エラーメッセージが表示された場合は、問題に対処します。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"。

8. 最初のグリッドのグリッドフェデレーションページに移動し、ブラウザを更新します。[接続ステータス]*が[接続済み]*になっていることを確認します。
9. 接続が確立されたら、検証ファイルのすべてのコピーを安全に削除します。

   この接続を編集すると、新しい検証ファイルが作成されます。元のファイルは再利用できません。

完了後

- の考慮事項を確認します "許可されたテナントの管理"。
- "新しいテナントアカウントを1つ以上作成します"をクリックし、*[Use grid federation connection]*権限を割り当てて、新しい接続を選択します。
- "接続を管理します" 必要に応じて。接続値の編集、接続のテスト、接続証明書のローテーション、接続の削除を行うことができます。
- "接続を監視します" 通常のStorageGRID 監視アクティビティの一部として使用します。
- "接続のトラブルシューティングを行います"アカウントクローンやグリッド間レプリケーションに関連するアラートやエラーの解決などが含まれます。

グリッドフェデレーション接続を管理します

StorageGRID システム間のグリッドフェデレーション接続の管理には、接続の詳細の編集、証明書のローテーション、テナント権限の削除、未使用の接続の削除が含まれます。

作業を開始する前に

- いずれかのグリッドで、を使用してGrid Managerにサインインしておきます "サポートされている Web ブラウザ"。
- サインインしているグリッドのRootアクセス権限が必要です。

グリッドフェデレーション接続を編集します

グリッドフェデレーション接続を編集するには、接続内のいずれかのグリッドのプライマリ管理ノードにサインインします。最初のグリッドに変更を加えたら、新しい検証ファイルをダウンロードして、もう一方のグリッドにアップロードする必要があります。

接続の編集中も、アカウントのクローンまたはグリッド間のレプリケーション要求では引き続き既存の接続設定が使用されます。最初のグリッドに対して行った編集はすべてローカルに保存されますが、2番目のグリッドにアップロード、保存、およびテストされるまでは使用されません。

接続の編集を開始します

手順

1. いずれかのグリッドのプライマリ管理ノードからGrid Managerにサインインします。
2. [ノード]*を選択し、システムの他のすべての管理ノードがオンラインであることを確認します。

   グリッドフェデレーション接続を編集すると、StorageGRID は最初のグリッドのすべての管理ノードに「候補構成」ファイルを保存しようとします。このファイルをすべての管理ノードに保存できない場合は、*[保存してテスト]*を選択すると警告メッセージが表示されます。

3. >[システム]>[グリッドフェデレーション]*を選択します。
4. [グリッドフェデレーション]ページの*[アクション]*メニューまたは特定の接続の詳細ページを使用して、接続の詳細を編集します。を参照してください "グリッドフェデレーション接続を作成する" 何を入力するかを入力します。

   [アクション] メニュー

   a. 接続のラジオボタンを選択します。
   b. >[編集]*を選択します。
   c. 新しい情報を入力します。

   詳細ページ

   a. 接続名を選択して詳細を表示します。
   b. 「 * 編集 * 」を選択します。
   c. 新しい情報を入力します。

5. サインインしているグリッドのプロビジョニングパスフレーズを入力します。
6. [保存して続行]*を選択します。

   新しい値は保存されますが、別のグリッドに新しい検証ファイルをアップロードするまで接続に適用されません。

7. [検証ファイルのダウンロード]*を選択します。

   後でこのファイルをダウンロードするには、接続の詳細ページに移動します。

8. ダウンロードしたファイルを見つけます (*connection-name*.grid-federation) をクリックし、安全な場所に保存します。

   検証ファイルには秘密が含まれているため、安全に保存および送信する必要があります。

9. [Close]*を選択して、[Grid Federation]ページに戻ります。
10. が[編集保留中]*になっていることを確認します。

> 接続の編集を開始したときに接続ステータスが* Connected 以外の場合、 Pending edit *に変更されません。

11. を指定します *connection-name*.grid-federation ファイルを他のグリッドのグリッド管理者に送信します。

接続の編集を終了します

他のグリッドに検証ファイルをアップロードして、接続の編集を完了します。

手順

1. プライマリ管理ノードからGrid Managerにサインインします。
2. >[システム]>[グリッドフェデレーション]*を選択します。
3. [検証ファイルのアップロード]*を選択して、アップロードページにアクセスします。
4. [検証ファイルのアップロード]*を選択します。次に、最初のグリッドからダウンロードしたファイルを参照して選択します。
5. 現在サインインしているグリッドのプロビジョニングパスフレーズを入力します。
6. [保存してテスト]*を選択します。

   編集した値を使用して接続を確立できる場合は、成功のメッセージが表示されます。それ以外の場合は、エラーメッセージが表示されます。メッセージを確認し、問題があれば対処します。

7. ウィザードを閉じて[Grid Federation]ページに戻ります。
8. [接続ステータス]*が[接続済み]*になっていることを確認します。
9. 最初のグリッドのグリッドフェデレーションページに移動し、ブラウザを更新します。[接続ステータス]*が[接続済み]*になっていることを確認します。
10. 接続が確立されたら、検証ファイルのすべてのコピーを安全に削除します。

グリッドフェデレーション接続をテストします

手順

1. プライマリ管理ノードからGrid Managerにサインインします。
2. >[システム]>[グリッドフェデレーション]*を選択します。
3. [グリッドフェデレーション]ページの*[アクション]*メニューまたは特定の接続の詳細ページを使用して、接続をテストします。

[アクション] メニュー

a. 接続のラジオボタンを選択します。
b. **>**[テスト]*を選択します。

詳細ページ

a. 接続名を選択して詳細を表示します。
b. [接続のテスト *] を選択します。

4. 接続ステータスを確認します。

接続ステータス	説明
接続しました	両方のグリッドが接続され、正常に通信しています。
エラー	接続にエラーが発生しています。たとえば、証明書の有効期限が切れているか、設定値が無効になっている場合などです。
編集を保留中です	このグリッドで接続を編集しましたが、接続は既存の設定を使用しています。編集を完了するには、新しい検証ファイルをもう一方のグリッドにアップロードします。
接続を待機しています	このグリッドで接続が設定されていますが、もう一方のグリッドでは接続が完了していません。このグリッドから検証ファイルをダウンロードし、別のグリッドにアップロードします。
不明です	接続の状態が不明です。ネットワーク問題 またはオフラインノードが原因である可能性があります。

5. 接続ステータスが*エラー*の場合は、問題を解決します。次に、もう一度*[Test connection]*を選択して、問題 が修正されたことを確認します。

[[rotate_grid_fed_certificates]接続証明書のローテーション

各グリッドフェデレーション接続は、自動生成された4つのSSL証明書を使用して接続を保護します。各グリッドの2つの証明書が有効期限に近づくと、* Expiration of grid federation certificate *アラートによって証明書のローテーションを促すメッセージが表示されます。

> 接続のいずれかの側の証明書が期限切れになると、接続は動作を停止し、証明書が更新されるまでレプリケーションは保留になります。

手順

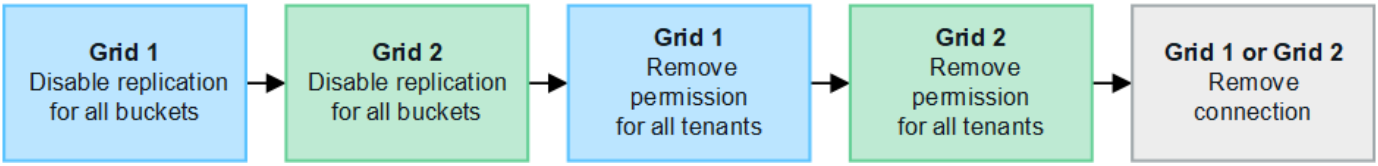
1. いずれかのグリッドのプライマリ管理ノードからGrid Managerにサインインします。
2. **>**[システム]**>**[グリッドフェデレーション]*を選択します。
3. [Grid Federation]ページのいずれかのタブで、接続名を選択して詳細を表示します。

4. ［証明書］タブを選択します。
5. [証明書の回転]*を選択します。
6. 新しい証明書を有効にする日数を指定します。
7. サインインしているグリッドのプロビジョニングパスフレーズを入力します。
8. [証明書の回転]*を選択します。
9. 必要に応じて、接続のもう一方のグリッドで上記の手順を繰り返します。

   一般に、接続の両側の証明書には同じ日数を使用します。

グリッドフェデレーション接続を削除します

接続のいずれかのグリッドからグリッドフェデレーション接続を削除できます。次の図に示すように、両方のグリッドで前提条件となる手順を実行して、どちらのグリッドのテナントでも接続が使用されていないことを確認する必要があります。



接続を削除する前に、次の点に注意してください。

- 接続を削除しても、グリッド間ですでにコピーされている項目は削除されません。たとえば、テナントの権限が削除されても、両方のグリッドに存在するテナントユーザ、グループ、およびオブジェクトはどちらのグリッドからも削除されません。これらのアイテムを削除する場合は、両方のグリッドから手動で削除する必要があります。
- 接続を削除すると、レプリケーションを保留している（取り込まれたがもう一方のグリッドにまだレプリケートされていない）オブジェクトのレプリケーションが永続的に失敗します。

すべてのテナントバケットでレプリケーションを無効にします

手順

1. いずれかのグリッドから、プライマリ管理ノードからGrid Managerにサインインします。
2. >[システム]>[グリッドフェデレーション]*を選択します。
3. 接続名を選択して詳細を表示します。
4. [Permitted Tenants]*タブで、接続がテナントで使用されているかどうかを確認します。
5. テナントが表示されている場合は、すべてのテナントに指示します "グリッド間レプリケーションを無効にします" 接続内の両方のグリッド上のすべてのバケットに対して。

> テナントバケットでグリッド間レプリケーションが有効になっている場合は、* Use grid federation connection *権限を削除することはできません。各テナントアカウントは、両方のグリッドでバケットのグリッド間レプリケーションを無効にする必要があります。

各テナントの権限を削除します

すべてのテナントバケットでグリッド間レプリケーションを無効にしたら、両方のグリッドのすべてのテナントから* Use grid federation permission *を削除します。

手順

1. **>**[システム]**>**[グリッドフェデレーション]*を選択します。
2. 接続名を選択して詳細を表示します。
3. 各テナントについて、**[Permitted Tenants]***タブで、各テナントから[Use Grid Federation connection]*権限を削除します。を参照してください "許可されたテナントを管理する"。
4. もう一方のグリッドで許可されたテナントについて、上記の手順を繰り返します。

接続を削除します

手順

1. どちらのグリッドでも接続を使用しているテナントがない場合は、*[削除]*を選択します。
2. 確認メッセージを確認し、*[削除]*を選択します。
   - 接続を削除できる場合は、成功を示すメッセージが表示されます。これで、グリッドフェデレーション接続が両方のグリッドから削除されます。
   - 接続を削除できない場合（まだ使用中、接続エラーなど）、エラーメッセージが表示されます。次のいずれかを実行できます。
     - エラーを解決します（推奨）。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"。
     - 力で接続を取り外します。次のセクションを参照してください。

グリッドフェデレーション接続を強制的に削除します

必要に応じて、ステータスが*connected*でない接続を強制的に削除できます。

強制的に削除すると、ローカルグリッドからのみ接続が削除されます。接続を完全に削除するには、両方のグリッドで同じ手順を実行します。

手順

1. 確認ダイアログボックスで*[強制削除]*を選択します。

   成功を示すメッセージが表示されます。このグリッドフェデレーション接続は使用できなくなります。ただし、テナントバケットでグリッド間レプリケーションが引き続き有効になっている場合や、接続内のグリッド間で一部のオブジェクトコピーがすでにレプリケートされている場合があります。

2. 接続のもう一方のグリッドで、プライマリ管理ノードからGrid Managerにサインインします。
3. **>**[システム]**>**[グリッドフェデレーション]*を選択します。
4. 接続名を選択して詳細を表示します。
5. **[**削除**]***および[はい]*を選択します。
6. このグリッドから接続を削除するには、*[強制削除]*を選択します。

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

新しいS3テナントアカウントに、2つのStorageGRID システム間のグリッドフェデレーション接続の使用を許可できます。テナントが接続の使用を許可されている場合は、テナントの詳細を編集したり、接続を使用するテナントの権限を完全に削除したりするための特別な手順が必要です。

作業を開始する前に

- いずれかのグリッドで、を使用してGrid Managerにサインインしておきます "サポートされている Web ブラウザ"。
- サインインしているグリッドのRootアクセス権限が必要です。
- これで完了です "グリッドフェデレーション接続を作成しました" 2つのグリッドの間。
- のワークフローを確認しておきます "アカウントのクローン" および "グリッド間レプリケーション"。
- 必要に応じて、接続内の両方のグリッドに対してシングルサインオン（SSO）または識別フェデレーションがすでに設定されている。を参照してください "アカウントクローンとは何ですか"。

許可されたテナントを作成します

テナントアカウントがアカウントのクローニングや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接続を使用できるようにする場合は、の一般的な手順に従ってください "新しいS3テナントを作成します" 次の点に注意してください。

- テナントは、接続のどちらのグリッドからも作成できます。テナントが作成されるグリッドは、_tenantのソースグリッド_です。
- 接続のステータスは* connected *である必要があります。
- [Use grid federation connection]*権限は、新しいS3テナントを作成する場合にのみ選択できます。この権限は、既存のテナントの編集時に有効にすることはできません。
- 新しいテナントが最初のグリッドに保存されると、同じテナントがもう一方のグリッドに自動的にレプリケートされます。テナントがレプリケートされているグリッドは、_テナントのデスティネーショングリッド_です。
- 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。必要に応じて、*概要 *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できます。たとえば、Grid 1に作成されたテナントのこの概要 は、Grid 2にレプリケートされたテナントにも表示されます：「This tenant was created on Grid 1」。
- セキュリティ上の理由から、ローカルrootユーザのパスワードはデスティネーショングリッドにコピーされません。

> ローカルrootユーザがデスティネーショングリッドでレプリケートされたテナントにサインインできるようにするには、そのグリッドのグリッド管理者が事前に必要です "ローカルrootユーザのパスワードを変更します"。

- 両方のグリッドで新しいテナントが利用可能になると、テナントユーザは次の処理を実行できます。
  - テナントのソースグリッドから、グループとローカルユーザを作成します。これらのユーザは、テナントのデスティネーショングリッドに自動的にクローニングされます。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"。

- 新しいS3アクセスキーを作成します。このアクセスキーは、必要に応じて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できます。を参照してください "APIを使用してS3アクセスキーをクローニングします"。
- 接続の両方のグリッドに同一のバケットを作成し、一方向または両方向のグリッド間レプリケーションを有効にします。を参照してください "グリッド間レプリケーションを管理します"。

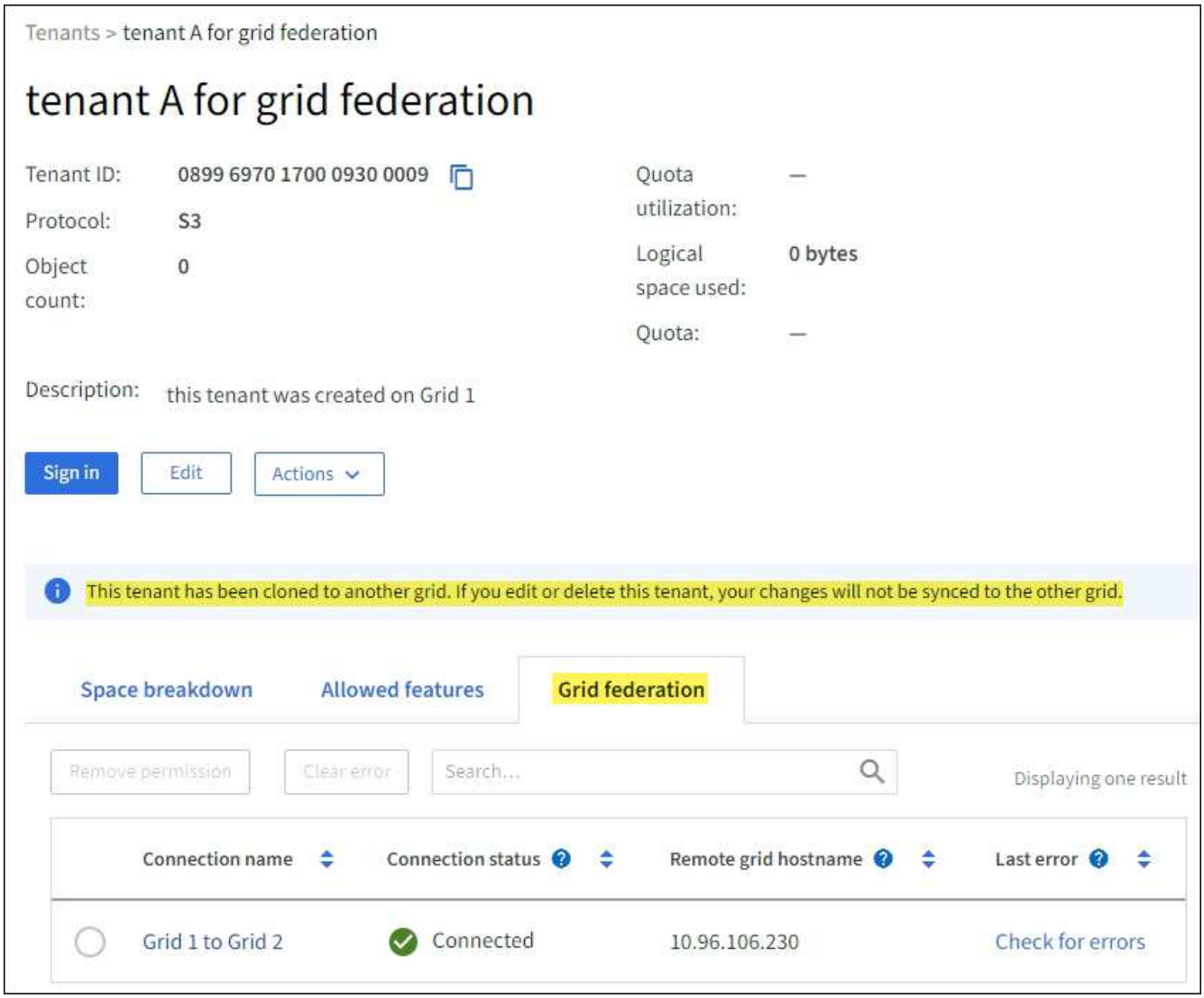
許可されたテナントを表示します

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テナントの詳細を確認できます。

手順

1. 「 * tenants * 」を選択します
2. [Tenants]ページで、テナント名を選択してテナントの詳細ページを表示します。

   テナントのソースグリッド（テナントがこのグリッドで作成された場合）の場合は、テナントが別のグリッドにクローニングされたことを通知するバナーが表示されます。このテナントを編集または削除すると、変更内容は他のグリッドに同期されません。



3. 必要に応じて、* Grid federation *タブをに選択します "グリッドフェデレーション接続を監視します"。

許可されたテナントを編集します

Use grid federation connection *権限が割り当てられているテナントを編集する必要がある場合は、の一般的な手順に従ってください "テナントアカウントを編集しています" 次の点に注意してください。

- 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、変更内容は他のグリッドにはコピーされません。テナントの詳細をグリッド間で同期させる場合は、両方のグリッドで同じ編集を行う必要があります。
- テナントを編集しているときは、*[Use grid federation connection]*権限をクリアできません。
- テナントの編集中に別のグリッドフェデレーション接続を選択することはできません。

許可されたテナントを削除します

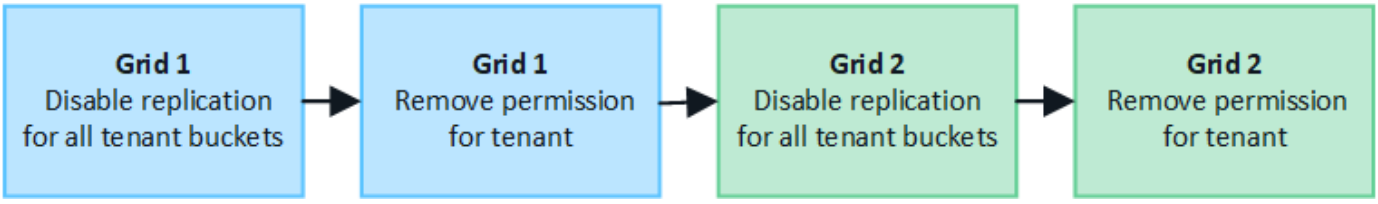
Use grid federation connection *権限が割り当てられているテナントを削除する必要がある場合は、の一般的な手順に従ってください "テナントアカウントを削除しています" 次の点に注意してください。

- ソースグリッドから元のテナントを削除する前に、ソースグリッドからアカウントのすべてのバケットを削除する必要があります。
- デスティネーショングリッドからクローンテナントを削除する前に、デスティネーショングリッドからアカウントのすべてのバケットを削除する必要があります。
- 元のテナントまたはクローニングされたテナントを削除すると、そのアカウントをグリッド間レプリケーションに使用できなくなります。
- ソースグリッドから元のテナントを削除しても、デスティネーショングリッドにクローニングされたテナントグループ、ユーザ、またはキーは影響を受けません。クローニングされたテナントを削除するか、テナントによる独自のグループ、ユーザ、アクセスキー、およびバケットの管理を許可することができます。
- デスティネーショングリッドでクローニングされたテナントを削除すると、元のテナントに新しいグループまたはユーザが追加されるとクローニングエラーが発生します。

  このエラーを回避するには、このグリッドからテナントを削除する前に、グリッドフェデレーション接続を使用するテナントの権限を削除してください。

削除**Use grid federation connection permission**

テナントがグリッドフェデレーション接続を使用できないようにするには、* Use grid federation connection *権限を削除する必要があります。



グリッドフェデレーション接続を使用するテナントの権限を削除する前に、次の点に注意してください。

- テナントから* Use grid federation connection *権限を削除することは永続的な操作です。このテナントの権限を再度有効にすることはできません。
- テナントのバケットでグリッド間レプリケーションが有効になっている場合は、* Use grid federation

connection *権限を削除できません。テナントアカウントでは、まずすべてのバケットでグリッド間レプリケーションを無効にする必要があります。

- [Use grid federation connection]*権限を削除しても、グリッド間ですでにレプリケートされている項目は削除されません。たとえば、テナントの権限が削除されても、両方のグリッドに存在するテナントユーザ、グループ、およびオブジェクトはどちらのグリッドからも削除されません。これらのアイテムを削除する場合は、両方のグリッドから手動で削除する必要があります。

作業を開始する前に

- を使用している "サポートされている Web ブラウザ"。
- 両方のグリッドに対するRoot Access権限が必要です。

テナントバケットのレプリケーションを無効にする

最初に、すべてのテナントバケットでグリッド間レプリケーションを無効にします。

手順

1. いずれかのグリッドから、プライマリ管理ノードからGrid Managerにサインインします。
2. >[システム]>[グリッドフェデレーション]*を選択します。
3. 接続名を選択して詳細を表示します。
4. [Permitted Tenants]*タブで、テナントが接続を使用しているかどうかを確認します。
5. テナントが表示されている場合は、テナントに指示します "グリッド間レプリケーションを無効にします" 接続内の両方のグリッド上のすべてのバケットに対して。

> テナントバケットでグリッド間レプリケーションが有効になっている場合は、* Use grid federation connection *権限を削除することはできません。テナントは、両方のグリッドでバケットのグリッド間レプリケーションを無効にする必要があります。

テナントの権限を削除します

テナントバケットでグリッド間レプリケーションを無効にしたら、グリッドフェデレーション接続を使用するテナントの権限を削除できます。

手順

1. プライマリ管理ノードからGrid Managerにサインインします。
2. [Grid Federation]ページまたは[Tenants]ページから権限を削除します。

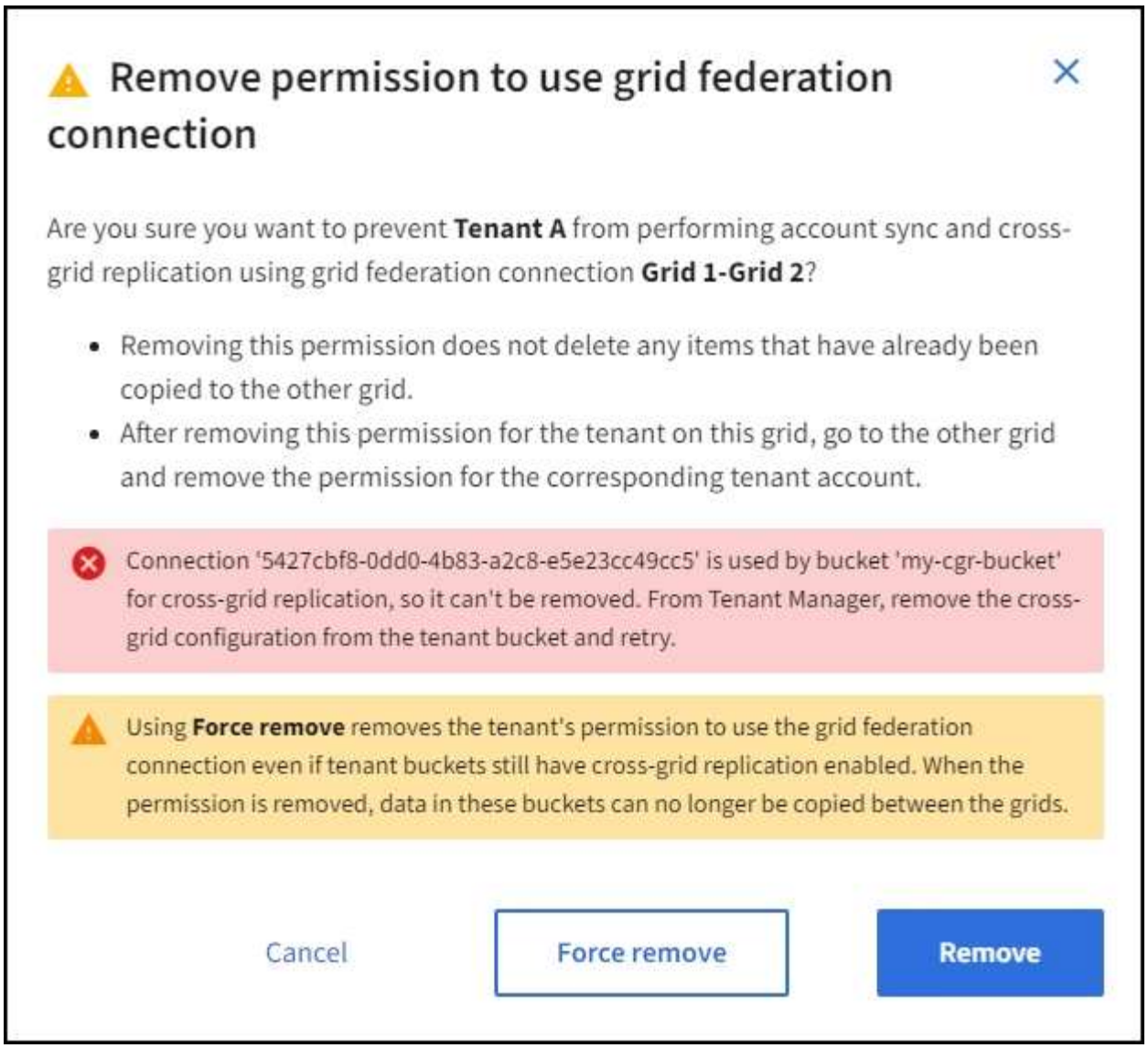
グリッドフェデレーションページ

a. >[システム]>[グリッドフェデレーション]*を選択します。
b. 接続名を選択して詳細ページを表示します。
c. [Permitted Tenants]*タブで、テナントのラジオボタンを選択します。
d. [Remove Permission]*を選択します。

テナントページ

a. 「 * tenants * 」を選択します
b. テナントの名前を選択して詳細ページを表示します。
c. [グリッドフェデレーション]*タブで、接続のラジオボタンを選択します。
d. [Remove Permission]*を選択します。

3. 確認ダイアログボックスで警告を確認し、*[削除]*を選択します。
   - 権限を削除できる場合は、詳細ページに戻り、成功を示すメッセージが表示されます。このテナントはグリッドフェデレーション接続を使用できなくなります。
   - 1つ以上のテナントバケットでグリッド間レプリケーションが有効になっている場合は、エラーが表示されます。



次のいずれかを実行できます。

- （推奨）。 Tenant Managerにサインインし、テナントのバケットごとにレプリケーションを無効にします。を参照してください "グリッド間レプリケーションを管理します"。次に、手順を繰り返して* Use grid connection *権限を削除します。
- 権限を強制的に削除します。次のセクションを参照してください。

4. もう一方のグリッドに移動して上記の手順を繰り返し、もう一方のグリッド上の同じテナントに対する権限を削除します。

権限を強制的に削除します

テナントバケットでグリッド間レプリケーションが有効になっている場合でも、必要に応じて、グリッドフェデレーション接続を使用するテナントの権限を強制的に削除できます。

テナントの権限を強制的に削除する前に、の一般的な考慮事項に注意してください 権限を削除しています その他の考慮事項：

- [Use grid federation connection]*権限を強制的に削除した場合、他のグリッドへのレプリケーションを保留中の（取り込まれたがまだレプリケートされていない）オブジェクトは引き続きレプリケートされま

す。これらのインプロセスオブジェクトがデスティネーションバケットに到達しないようにするには、もう一方のグリッドに対するテナントの権限も削除する必要があります。

- [Use grid federation connection]*権限を削除したあとにソースバケットに取り込まれたオブジェクトは、デスティネーションバケットにレプリケートされません。

手順

1. プライマリ管理ノードからGrid Managerにサインインします。
2. >[システム]>[グリッドフェデレーション]*を選択します。
3. 接続名を選択して詳細ページを表示します。
4. [Permitted Tenants]*タブで、テナントのラジオボタンを選択します。
5. [Remove Permission]*を選択します。
6. 確認ダイアログボックスで警告を確認し、*[強制的に削除]*を選択します。

   成功を示すメッセージが表示されます。このテナントはグリッドフェデレーション接続を使用できなくなります。

7. 必要に応じて、もう一方のグリッドに移動して上記の手順を繰り返し、もう一方のグリッドの同じテナントアカウントに対する権限を強制的に削除します。たとえば、処理中のオブジェクトがデスティネーションバケットに到達しないように、もう一方のグリッドで上記の手順を繰り返します。

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

グリッドフェデレーション接続、アカウントクローン、およびグリッド間レプリケーションに関連するアラートやエラーのトラブルシューティングが必要になる場合があります。

グリッドフェデレーション接続のアラートとエラー

グリッドフェデレーション接続でアラートを受信したり、エラーが発生したりすることがあります。

接続問題 を解決するための変更を行った後、接続をテストして、接続ステータスが*接続済み*に戻ることを確認します。手順については、を参照してください "グリッドフェデレーション接続を管理します"。

Grid Federation Connection Failureアラート

問題

Grid federation connection failure *アラートがトリガーされました。

詳細

グリッド間のグリッド連携接続が機能していない可能性があります。

推奨される対処方法

1. 両方のグリッドの[Grid Federation]ページで設定を確認します。すべての値が正しいことを確認します。を参照してください "グリッドフェデレーション接続を管理します"。
2. 接続に使用した証明書を確認します。有効期限が切れたグリッドフェデレーション証明書に関するアラートがないこと、および各証明書の詳細が有効であることを確認してください。の接続証明書のローテーション手順を参照してください "グリッドフェデレーション接続を管理します"。

3. 両方のグリッドのすべての管理ノードとゲートウェイノードがオンラインで使用可能であることを確認します。これらのノードに影響している可能性があるアラートを解決してから再試行してください。
4. ローカルまたはリモートのグリッドの完全修飾ドメイン名（FQDN）を指定した場合は、DNSサーバがオンラインで使用可能であることを確認します。を参照してください "グリッドフェデレーションとは" ネットワーク、IPアドレス、およびDNSの要件に使用します。

Gridフェデレーション証明書の有効期限に関するアラート

問題

Expiration of grid federation certificate *アラートがトリガーされました。

詳細

このアラートは、1つ以上のグリッドフェデレーション証明書の有効期限が近づいていることを示しています。

推奨される対処方法

の接続証明書のローテーション手順を参照してください "グリッドフェデレーション接続を管理します"。

グリッドフェデレーション接続の編集中にエラーが発生しました

問題

グリッドフェデレーション接続を編集するときに、*[保存してテスト]*を選択すると、「1つ以上のノードで候補構成ファイルを作成できませんでした」という警告メッセージが表示されます。

詳細

グリッドフェデレーション接続を編集すると、StorageGRID は最初のグリッドのすべての管理ノードに「候補構成」ファイルを保存しようとします。管理ノードがオフラインの場合など、このファイルをすべての管理ノードに保存できない場合は、警告メッセージが表示されます。

推奨される対処方法

1. 接続の編集に使用するグリッドで、* nodes *を選択します。
2. そのグリッドのすべての管理ノードがオンラインであることを確認します。
3. オフラインになっているノードがある場合は、それらのノードをオンラインに戻し、接続の編集をやり直します。

アカウントのクローンエラー

クローンされたテナントアカウントにサインインできない

問題

クローンされたテナントアカウントにはサインインできません。Tenant Managerのサインインページに「Your credentials for this account were invalid」というエラーメッセージが表示されます。もう一度実行してください。`"

詳細

セキュリティ上の理由から、テナントアカウントをテナントのソースグリッドから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する場合、テナントのローカルrootユーザに設定したパスワードはクローニングされません。同様に、テナントのソースグリッドでローカルユーザを作成しても、ローカルユーザのパスワードはデスティネーショングリッドにクローニングされません。

推奨される対処方法

rootユーザがテナントのデスティネーショングリッドにサインインするには、まずグリッド管理者が必要です "ローカルrootユーザのパスワードを変更します" をクリックします。

クローニングされたローカルユーザがテナントのデスティネーショングリッドにサインインする前に、クローニングされたテナントのrootユーザがデスティネーショングリッドにユーザのパスワードを追加する必要があります。手順については、を参照してください "ローカルユーザを管理します" Tenant Managerの使用手順を参照してください。

クローンなしでテナントが作成された

問題

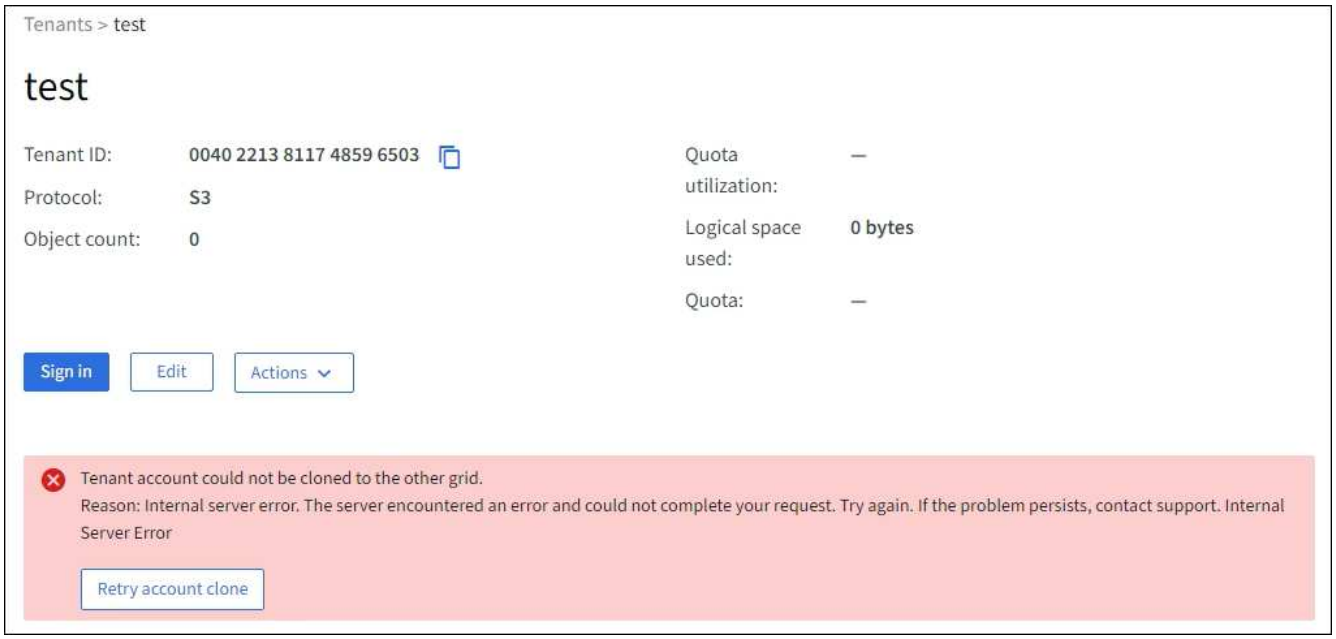
Use grid federation connection *権限で新しいテナントを作成すると、「Tenant created without a clone」というメッセージが表示されます。

詳細

この問題 は、接続ステータスの更新が遅延した場合に発生する可能性があります原因 。これにより、正常でない接続が*接続済み*として表示される可能性があります。

推奨される対処方法

1. エラーメッセージに表示された理由を確認し、接続を妨げる可能性のあるネットワークまたはその他の問題を解決します。を参照してください グリッドフェデレーション接続のアラートとエラー。
2. 手順に従って、でグリッドフェデレーション接続をテストします "グリッドフェデレーション接続を管理します" 問題 が修正されたことを確認します。
3. テナントのソースグリッドで、*[Tenants]*を選択します。
4. クローニングに失敗したテナントアカウントを特定します。
5. テナント名を選択して詳細ページを表示します。
6. [アカウントのクローンを再試行する]*を選択します。

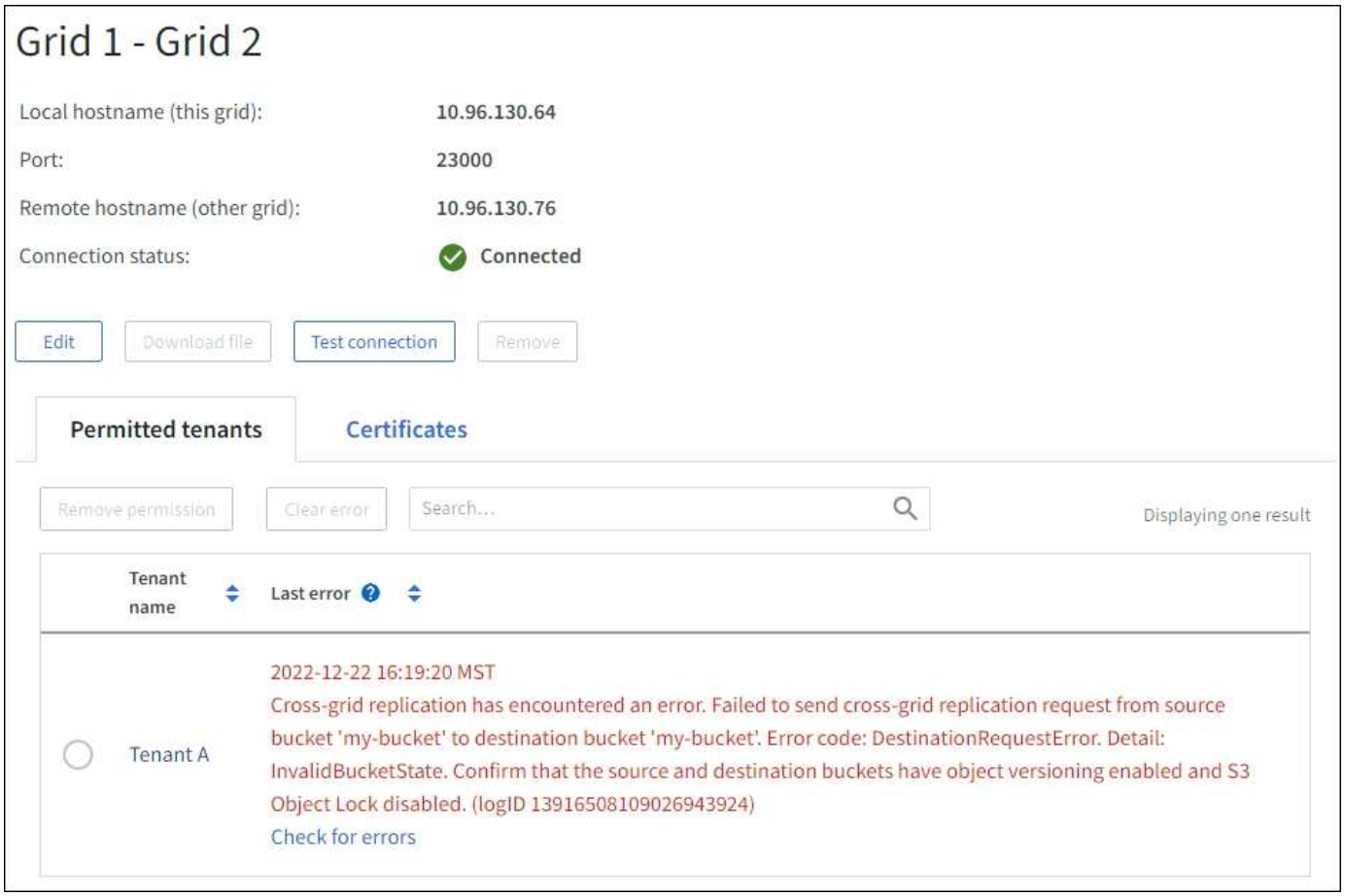


エラーが解決されると、テナントアカウントがもう一方のグリッドにクローニングされます。

接続またはテナントについて表示された最後のエラー

問題

いつ "グリッドフェデレーション接続の表示" （または "許可されたテナントの管理" 接続の場合）、接続の詳細ページの* Last error *列にエラーが表示されます。例：



列に表示されるメッセージを示すスクリーンショット"]

詳細

各グリッドフェデレーション接続の* Last error *列には、テナントのデータが他のグリッドにレプリケートされているときに発生した最新のエラー（存在する場合）が表示されます。この列には、最後に発生したグリッド間レプリケーションエラーのみが表示されます。以前に発生した可能性のあるエラーは表示されません。この列のエラーは、次のいずれかの理由で発生する可能性があります。

- ソースオブジェクトのバージョンが見つかりませんでした。
- ソースバケットが見つかりませんでした。
- デスティネーションバケットが削除されました。
- デスティネーションバケットが別のアカウントで再作成されました。
- デスティネーションバケットのバージョン管理が中断されています。
- デスティネーションバケットが同じアカウントで再作成されましたが、現在バージョン管理されていません。

推奨される対処方法

「* Last error *」列にエラーメッセージが表示された場合は、次の手順を実行します。

1. メッセージテキストを確認します。
2. 推奨される対処方法を実行します。たとえば、グリッド間レプリケーションのためにデスティネーションバケットでバージョン管理が一時停止されていた場合は、そのバケットのバージョン管理を再度有効にします。
3. テーブルから接続またはテナントアカウントを選択します。
4. [Clear error]*を選択します。
5. メッセージをクリアしてシステムのステータスを更新するには、*はい*を選択します。
6. 5~6分待ってから、新しいオブジェクトをバケットに取り込みます。エラーメッセージが再表示されないことを確認します。

   エラーメッセージがクリアされるように、メッセージのタイムスタンプから5分以上経過してから新しいオブジェクトを取り込んでください。

   エラーをクリアしたあとに、同じくエラーが発生している別のバケットにオブジェクトを取り込んだ場合は、新しい* Last error *が表示されることがあります。

7. バケットエラーが原因でレプリケートに失敗したオブジェクトがないかどうかを確認するには、を参照してください "失敗したレプリケーション処理を特定して再試行します"。

Cross-grid replication permanent failureアラート

問題

Cross-grid replication permanent failure *アラートがトリガーされました。

詳細

このアラートは、ユーザによる解決が必要な理由で、2つのグリッド上のバケット間でテナントオブジェクトをレプリケートできない場合に表示されます。このアラートの主な原因は、ソースまたはデスティネーションのバケットが変更されたことです。

推奨される対処方法

1. アラートがトリガーされたグリッドにサインインします。
2. >[システム]>[グリッドフェデレーション]*に移動し、アラートに表示されている接続名を確認します。
3. [Permitted Tenants]タブで、* Last error *列を確認し、エラーが発生しているテナントアカウントを特定します。
4. 障害の詳細については、の手順を参照してください "グリッドフェデレーション接続を監視する" をクリックして、クロスグリッドレプリケーションの指標を確認します。
5. 影響を受ける各テナントアカウント：
   a. の手順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" テナントがグリッド間レプリケーションのデスティネーショングリッドでのクォータを超えていないことを確認する。
   b. 必要に応じて、デスティネーショングリッドでのテナントのクォータを増やして、新しいオブジェクトを保存できるようにします。

6. 影響を受ける各テナントについて、両方のグリッドでTenant Managerにサインインしてバケットのリストを比較できるようにします。
7. クロスグリッドレプリケーションが有効になっている各バケットについて、次の点を確認します。
   - もう一方のグリッドには、同じテナントに対応するバケットがあります（正確な名前を使用する必要があります）。
   - どちらのバケットでもオブジェクトのバージョン管理が有効になっています（どちらのグリッドでもバージョン管理を一時停止することはできません）。
   - 両方のバケットでS3オブジェクトロックが無効になっています。
   - どちらのバケットも「* Deleting objects：read-only *」状態ではありません。
8. 問題 が解決されたことを確認するには、の手順を参照してください "グリッドフェデレーション接続を監視する" クロスグリッドレプリケーションの指標を確認する、または次の手順を実行します。
   a. [Grid Federation]ページに戻ります。
   b. 影響を受けるテナントを選択し、* Last error 列で Clear Error *を選択します。
   c. メッセージをクリアしてシステムのステータスを更新するには、*はい*を選択します。
   d. 5~6分待ってから、新しいオブジェクトをバケットに取り込みます。エラーメッセージが再表示されないことを確認します。

> エラーメッセージがクリアされるように、メッセージのタイムスタンプから5分以上経過してから新しいオブジェクトを取り込んでください。

> 解決後にアラートがクリアされるまでに最大1日かかることがあります。

   a. に進みます "失敗したレプリケーション処理を特定して再試行します" 他のグリッドにレプリケートできなかったオブジェクトを特定するかマーカーを削除し、必要に応じてレプリケーションを再試行します。

Cross-grid replication resource unavailableアラート

問題

Cross-grid replication resource unavailable *アラートがトリガーされました。

詳細

このアラートは、リソースを使用できないためにグリッド間のレプリケーション要求が保留中であることを示しています。たとえば、ネットワークエラーが発生している可能性があります。

推奨される対処方法

1. アラートを監視して、問題 が自動的に解決するかどうかを確認します。
2. 問題 が解消されない場合は、いずれかのグリッドに同じ接続に対する* Grid federation connection failure アラートが表示されているか、またはノードに対して Unable to communicate with node *アラートが表示されているかを確認します。このアラートは、アラートを解決すると解決される場合があります。
3. 障害の詳細については、の手順を参照してください "グリッドフェデレーション接続を監視する" をクリックして、クロスグリッドレプリケーションの指標を確認します。
4. アラートを解決できない場合は、テクニカルサポートにお問い合わせください。

問題 の解決後、グリッド間レプリケーションは通常どおり続行されます。

失敗したレプリケーション処理を特定して再試行します

Cross-grid replication permanent failure *アラートを解決したら、他のグリッドへのレプリケートに失敗したオブジェクトまたは削除マーカーがないかどうかを確認する必要があります。その後、これらのオブジェクトを再取り込みするか、グリッド管理APIを使用してレプリケーションを再試行できます。

Cross-grid replication permanent failure *アラートは、ユーザの介入が必要な理由で2つのグリッド上のバケット間でテナントオブジェクトをレプリケートできないことを示しています。このアラートの主な原因は、ソースまたはデスティネーションのバケットが変更されたことです。詳細については、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"。

レプリケートに失敗したオブジェクトがないかどうかを確認します

オブジェクトまたは削除マーカーが他のグリッドにレプリケートされていないかどうかを確認するには、監査ログでを検索します "CGRR（クロスグリッドレプリケーション要求）" メッセージ。このメッセージは、StorageGRID がオブジェクト、マルチパートオブジェクト、または削除マーカーをデスティネーションバケットにレプリケートできなかった場合にログに追加されます。

を使用できます "audit-explainツール" 結果を読みやすい形式に変換します。

作業を開始する前に

- Root Access 権限が割り当てられている。
- を使用することができます `Passwords.txt` ファイル。
- プライマリ管理ノードのIPアドレスを確認しておきます。

手順

1. プライマリ管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@primary_Admin_Node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

   rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。
2. audit.logでCGRRメッセージを検索し、audit-explainツールを使用して結果をフォーマットします。

   たとえば、このコマンドは過去30分間のすべてのCGRRメッセージをgrepし、audit-explainツールを使用します。

```
# awk -vdate=$(date -d "30 minutes ago" '+%Y-%m-%dT%H:%M:%S') '$1$2 >= date {
print }' audit.log | grep CGRR | audit-explain
```

このコマンドの結果は次の例のようになります。この例には、6つのCGRRメッセージのエントリがあります。この例では、オブジェクトをレプリケートできなかったため、すべてのグリッド間レプリケーション要求

で一般的なエラーが返されています。最初の3つのエラーは「オブジェクトのレプリケート」処理に関するもので、最後の3つのエラーは「マーカーのレプリケート」処理に関するものです。

```
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
object" bucket:bucket123 object:"audit-0"
version:QjRBNDIzODAtNjQ3My0xMUVELTg2QjEtODJBMjAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
object" bucket:bucket123 object:"audit-3"
version:QjRDOTRCOUMtNjQ3My0xMUVELTkzM0YtOTg1MTAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
delete marker" bucket:bucket123 object:"audit-1"
version:NUQ0OEYxMDAtNjQ3NC0xMUVELTg2NjMtOTY5NzAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
delete marker" bucket:bucket123 object:"audit-5"
version:NUQ1ODUwQkUtNjQ3NC0xMUVELTg1NTItRDkwNzAwQkI3NEM4 error:general
error
```

各エントリには、次の情報が含まれています。

フィールド	説明
CGRRクロスグリッドレプリケーション要求	要求の名前
テナント	テナントのアカウントID
接続	グリッドフェデレーション接続のID
操作	試行されたレプリケーション操作のタイプ。 • オブジェクトをレプリケートします • 削除マーカーを複製します • マルチパートオブジェクトをレプリケートします
バケット	バケット名
オブジェクト	オブジェクト名

フィールド	説明
バージョン	オブジェクトのバージョンID
エラー	エラーのタイプ。グリッド間レプリケーションに失敗した場合は、「General error」というエラーが表示されます。

失敗したレプリケーションを再試行します

デスティネーションバケットにレプリケートされなかったオブジェクトのリストを生成して削除マーカーを削除し、根本的な問題を解決したら、次のいずれかの方法でレプリケーションを再試行できます。

- 各オブジェクトをソースバケットに再度取り込みます。
- の説明に従って、グリッド管理プライベートAPIを使用します。

手順

1. Grid Managerの上部でヘルプアイコンを選択し、*[API documentation]*を選択します。
2. [Go to private API documentation]*を選択します。

   「プライベート」とマークされているStorageGRID APIエンドポイントは、予告なく変更される場合があります。StorageGRID プライベートエンドポイントは、要求の API バージョンも無視します。

3. [cross-grid-replication-advanced]*セクションで、次のエンドポイントを選択します。

   ```
   POST /private/cross-grid-replication-retry-failed
   ```

4. [* 試してみてください *] を選択します。
5. body テキストボックスで、 versionId *のサンプルエントリを、失敗したグリッド間レプリケーション要求に対応するaudit.logのバージョンIDに置き換えます。

   文字列は必ず二重引用符で囲んでください。

6. [* Execute] を選択します。
7. サーバ応答コードが「* 204 *」であることを確認します。これは、オブジェクトまたは削除マーカーが他のグリッドへのクロスグリッドレプリケーションのために保留中としてマークされていることを示します。

   Pendingは、クロスグリッドレプリケーション要求が処理のために内部キューに追加されたことを示します。

レプリケーションの再試行を監視します

レプリケーションの再試行処理を監視して、処理が完了していることを確認する必要があります。

オブジェクトまたは削除マーカーが他のグリッドにレプリケートされるまでに数時間以上かかることがあります。

再試行処理は、次の2つの方法で監視できます。

- S3を使用する "HEAD Object の実行" または "オブジェクトの取得" リクエスト。応答にはStorageGRID固有の情報が含まれます `x-ntap-sg-cgr-replication-status` 応答ヘッダー。次のいずれかの値が設定されます。

グリッド（ **Grid** ）	レプリケーションのステータス
ソース	• 成功：レプリケーションは成功しました。 • * pending*：オブジェクトはまだレプリケートされていません。 • **failure**:レプリケーションが永続的なエラーで失敗しました。ユーザーはエラーを解決する必要があります。
宛先	**replica**:オブジェクトはソースグリッドからレプリケートされました。

- の説明に従って、グリッド管理プライベートAPIを使用します。

手順

1. プライベートAPIドキュメントの* cross-grid-replication-advanced *セクションで、次のエンドポイントを選択します。

   ```
   GET /private/cross-grid-replication-object-status/{id}
   ```

2. [* 試してみてください *] を選択します。
3. [Parameter]セクションに、で使用したバージョンIDを入力します `cross-grid-replication-retry-failed` リクエスト。
4. [* Execute] を選択します。
5. サーバ応答コードが*200*であることを確認します。
6. レプリケーションステータスを確認します。次のいずれかになります。
   - * pending*：オブジェクトはまだレプリケートされていません。
   - 完了:レプリケーションは成功しました。
   - **failed**:レプリケーションは永続的なエラーで失敗しました。ユーザーはエラーを解決する必要があります。

セキュリティを管理します

セキュリティの管理：概要

StorageGRID システムのセキュリティを保護するために、 Grid Manager でさまざまなセキュリティ設定を行うことができます。

暗号化を管理します

StorageGRID には、データを暗号化するためのいくつかのオプションがあります。お勧めします "使用可能な暗号化方式を確認します" をクリックして、データ保護の要件を満たすものを特定します。

証明書を管理します

可能です "サーバ証明書を設定および管理します" HTTP接続、またはサーバに対するクライアントIDまたはユーザIDの認証に使用されるクライアント証明書に使用されます。

キー管理サーバを設定

を使用します "キー管理サーバ" アプライアンスがデータセンターから取り外された場合でも、StorageGRID データを保護できます。アプライアンスボリュームが暗号化されると、ノードがKMSと通信できないかぎり、アプライアンスのデータにアクセスすることはできません。

> 暗号化キー管理を使用するには、インストール時にアプライアンスをグリッドに追加する前に、アプライアンスごとに * Node Encryption * の設定を有効にする必要があります。

プロキシ設定を管理します

S3プラットフォームサービスまたはクラウドストレージプールを使用する場合は、を設定できます "ストレージプロキシサーバ" ストレージノードと外部のS3エンドポイントの間。HTTPSまたはHTTPを使用してAutoSupport メッセージを送信する場合は、を設定できます "管理プロキシサーバ" 管理ノードとテクニカルサポートの間。

ファイアウォールを制御します

システムのセキュリティを強化するために、で特定のポートを開いたり閉じたりして、StorageGRID 管理ノードへのアクセスを制御できます "外部ファイアウォール"。各ノードのを設定して、各ノードへのネットワークアクセスを制御することもできます "内部ファイアウォール"。導入に必要なポート以外のすべてのポートでアクセスを禁止できます。

StorageGRID の暗号化方式を確認します

StorageGRID には、データを暗号化するためのいくつかのオプションがあります。使用可能な方法を確認して、データ保護の要件を満たす方法を決定する必要があります。

次の表に、 StorageGRID で使用できる暗号化方式の概要を示します。

暗号化オプション	動作の仕組み	環境
Grid Manager からキー管理サーバ（ KMS ）を取得します	あなた "キー管理サーバを設定" StorageGRID サイトおよびの場合 "アプライアンスのノード暗号化を有効にします"。次に、アプライアンスノードが KMS に接続して、 Key Encryption Key （ KEK ；キー暗号化キー）を要求します。このキーは、各ボリュームのデータ暗号化キー（ DEK ）を暗号化および復号化します。	インストール中にノード暗号化 * が有効になっているアプライアンスノード。アプライアンスのすべてのデータは、物理的な損失やデータセンターからの削除から保護されます。 KMSを使用した暗号化キーの管理は、ストレージノードとサービスアプライアンスでのみサポートされます。
SANtricity System Manager のドライブセキュリティ	SG5700またはSG6000ストレージアプライアンスでドライブセキュリティ機能が有効になっている場合は、を使用できます "SANtricity システムマネージャ" をクリックしてセキュリティキーを作成および管理します。このキーは、セキュリティ保護されたドライブ上のデータにアクセスするために必要です。	Full Disk Encryption（FDE）ドライブまたはFIPSドライブを搭載したストレージアプライアンス。セキュリティ保護されたドライブ上のデータは、すべて物理的な損失やデータセンターからの削除から保護されます。一部のストレージアプライアンスまたはサービスアプライアンスでは使用できません。
格納オブジェクトの暗号化	を有効にします "格納オブジェクトの暗号化" オプションを選択します。有効にすると、バケットレベルまたはオブジェクトレベルで暗号化されていない新しいオブジェクトが取り込み時に暗号化されます。	新たに取り込まれた S3 および Swift オブジェクトデータ。 既存の格納オブジェクトは暗号化されません。オブジェクトメタデータやその他の機密データは暗号化されません。
S3 バケットの暗号化	バケットの暗号化を有効にするには、 PUT Bucket 暗号化要求を問題 に設定します。オブジェクトレベルで暗号化されていない新しいオブジェクトは、取り込み時に暗号化されます。	新たに取り込まれた S3 オブジェクトデータのみ。 バケットに対して暗号化を指定する必要があります。既存のバケットオブジェクトは暗号化されません。オブジェクトメタデータやその他の機密データは暗号化されません。 "バケットの処理"

暗号化オプション	動作の仕組み	環境
S3 オブジェクトのサーバ側の暗号化（ SSE ）	オブジェクトを格納してを含めるS3要求を問題 した `x-amz-server-side-encryption` 要求ヘッダー。	新たに取り込まれた S3 オブジェクトデータのみ。 オブジェクトに対して暗号化を指定する必要があります。オブジェクトメタデータやその他の機密データは暗号化されません。 キーは StorageGRID で管理されます。 "サーバ側の暗号化を使用します"
ユーザ指定のキーによる S3 オブジェクトのサーバ側暗号化（ SSE-C ）	オブジェクトを格納する S3 要求を問題 し、 3 つの要求ヘッダーを含めます。 • `x-amz-server-side-encryption-customer-algorithm` • `x-amz-server-side-encryption-customer-key` • `x-amz-server-side-encryption-customer-key-MD5`	新たに取り込まれた S3 オブジェクトデータのみ。 オブジェクトに対して暗号化を指定する必要があります。オブジェクトメタデータやその他の機密データは暗号化されません。 キーは StorageGRID の外部で管理されます。 "サーバ側の暗号化を使用します"
外部ボリュームまたはデータストアの暗号化	導入プラットフォームで暗号化がサポートされている場合は、StorageGRID の外部の暗号化方式を使用して、ボリュームまたはデータストア全体を暗号化できます。	すべてのボリュームまたはデータストアが暗号化されていることを前提として、すべてのオブジェクトデータ、メタデータ、およびシステム構成データ。 外部暗号化方式を使用すると、暗号化アルゴリズムと暗号キーを厳密に制御できます。は、記載されている他の方法と組み合わせることができます。

暗号化オプション	動作の仕組み	環境
StorageGRID の外部でのオブジェクトの暗号化	StorageGRID に取り込まれる前にオブジェクトデータとメタデータを暗号化するには、 StorageGRID の外部の暗号化メソッドを使用します。	オブジェクトデータとメタデータのみ（システム設定データは暗号化されません）。 外部暗号化方式を使用すると、暗号化アルゴリズムと暗号キーを厳密に制御できます。は、記載されている他の方法と組み合わせることができます。 "Amazon Simple Storage Service - Developer Guide ：クライアント側の暗号化を使用したデータの保護"

複数の暗号化方式を使用します

要件に応じて、一度に複数の暗号化方式を使用できます。例：

- KMS を使用してアプライアンスノードを保護したり、 SANtricity システムマネージャのドライブセキュリティ機能を使用して、同じアプライアンス内の自己暗号化ドライブ上のデータを「二重に暗号化」することもできます。
- KMSを使用してアプライアンスノード上のデータを保護できます。また、[Stored Object Encryption]オプションを使用して、取り込み時にすべてのオブジェクトを暗号化することもできます。

暗号化を必要とするオブジェクトがごく一部しかない場合は、暗号化をバケットレベルまたは個々のオブジェクトレベルで制御することを検討してください。複数レベルの暗号化を有効にすると、パフォーマンスコストが増加します。

証明書を管理します

セキュリティ証明書の管理：概要

セキュリティ証明書は、 StorageGRID コンポーネント間、および StorageGRID コンポーネントと外部システム間のセキュアで信頼された接続の確立に使用される小さいデータファイルです。

StorageGRID では、 2 種類のセキュリティ証明書が使用されます。

- * HTTPS 接続を使用する場合は、サーバー証明書 * が必要です。サーバ証明書は、クライアントとサーバ間のセキュアな接続を確立し、クライアントに対するサーバの ID を認証し、データのセキュアな通信パスを提供するために使用されます。サーバとクライアントには、それぞれ証明書のコピーがあります。
- * クライアント証明書 * は、クライアントまたはユーザー ID をサーバーに対して認証し、パスワードだけではなく、より安全な認証を提供します。クライアント証明書はデータを暗号化しません。

クライアントが HTTPS を使用してサーバに接続すると、サーバはサーバ証明書を返します。このサーバ証明書には公開鍵が含まれています。クライアントは、サーバの署名と証明書のコピーの署名を比較して、この証明書を検証します。署名が一致した場合、クライアントは同じ公開鍵を使用してサーバとのセッションを開始します。

StorageGRID は、一部の接続（ロードバランサエンドポイントなど）のサーバとして、または他の接続（CloudMirror レプリケーションサービスなど）のクライアントとして機能します。

- デフォルトの Grid CA 証明書 *

StorageGRID には、システムのインストール時に内部のグリッド CA 証明書を生成する認証局（ CA ）が組み込まれています。デフォルトでは、グリッド CA 証明書を使用して内部 StorageGRID トラフィックが保護されます。外部の認証局（ CA ）は、組織の情報セキュリティポリシーに完全に準拠した問題 カスタム証明書を作成できます。グリッド CA 証明書は非本番環境で使用できますが、本番環境では外部の認証局が署名したカスタム証明書を使用することを推奨します。証明書のないセキュアでない接続もサポートされますが、推奨されません。

- カスタムCA証明書は内部証明書を削除しません。ただし、カスタム証明書は、サーバ接続の確認用に指定した証明書である必要があります。
- カスタム証明書はすべてがを満たしている必要があります "サーバ証明書に関するシステムセキュリティ強化ガイドライン"。
- StorageGRID では、 CA からの証明書を 1 つのファイル（ CA 証明書バンドル）にバンドルすることがサポートされています。

> StorageGRID には、すべてのグリッドで同じオペレーティングシステムの CA 証明書も含まれています。本番環境では、オペレーティングシステムの CA 証明書の代わりに、外部の認証局によって署名されたカスタム証明書を指定してください。

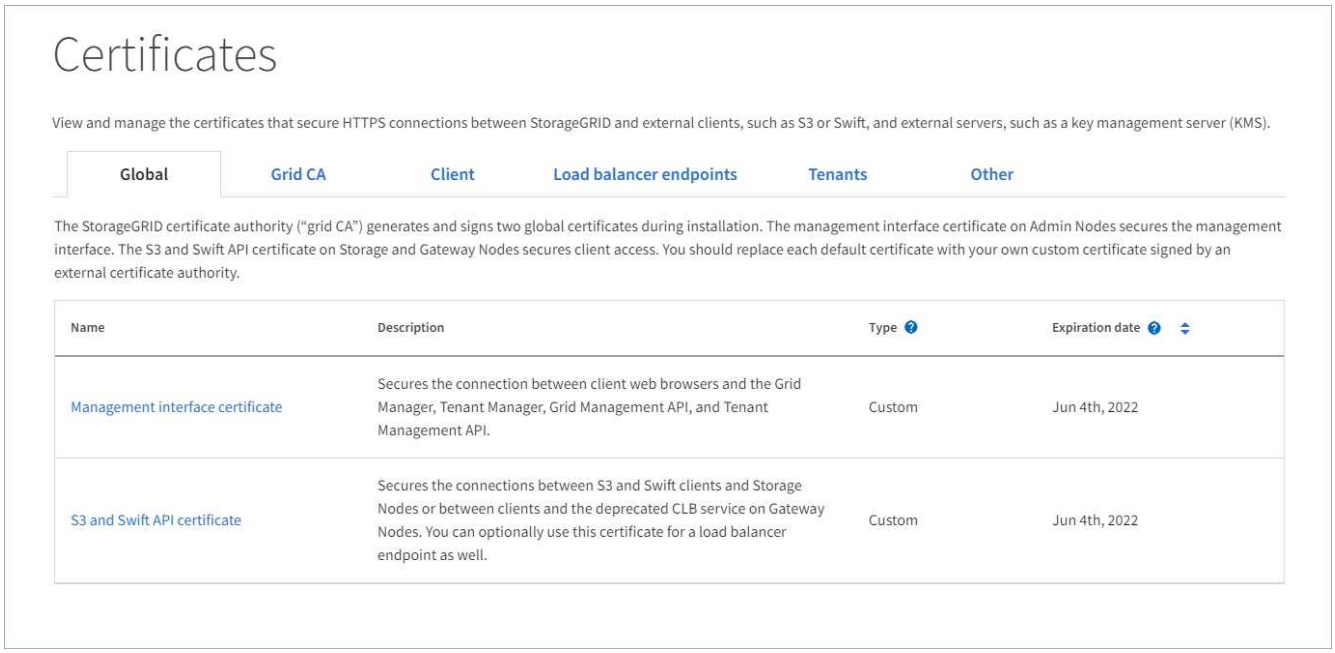
サーバ証明書とクライアント証明書のタイプのバリエーションは、いくつかの方法で実装されます。システムを設定する前に、特定の StorageGRID 構成に必要なすべての証明書を準備しておく必要があります。

アクセスセキュリティ証明書

すべての StorageGRID 証明書に関する情報に一元的にアクセスでき、各証明書の設定ワークフローへのリンクも含まれます。

手順

1. Grid Managerで、* configuration > Security > Certificates *を選択します。



2. [証明書] ページのタブを選択して、各証明書カテゴリの情報を表示し、証明書設定にアクセスします。タブにアクセスできるのは、適切な権限がある場合のみです。

   - * グローバル * ： Web ブラウザおよび外部 API クライアントからの StorageGRID アクセスを保護します。
   - * Grid CA * ：内部 StorageGRID トラフィックを保護します。
   - * クライアント * ：外部クライアントと StorageGRID Prometheus データベースの間の接続を保護します。
   - * ロードバランサエンドポイント * ： S3 および Swift クライアントと StorageGRID ロードバランサ間の接続を保護します。
   - * テナント * ：アイデンティティフェデレーションサーバーまたはプラットフォームサービスエンドポイントから S3 ストレージリソースへの接続を保護します。
   - * その他 * ：特定の証明書を必要とする StorageGRID 接続を保護します。

   各タブについては、証明書の詳細へのリンクを次に示します。

グローバル

グローバル証明書は、 Web ブラウザおよび外部の S3 および Swift API クライアントからの StorageGRID アクセスを保護します。2 つのグローバル証明書は、最初にインストール時に StorageGRID 認証局によって生成されます。本番環境では、外部の認証局によって署名されたカスタム証明書を使用することを推奨します。

- [管理インターフェイスの証明書]: クライアントの Web ブラウザ接続を StorageGRID 管理インターフェイスに保護します。
- S3 および Swift API 証明書：ストレージノード、管理ノード、およびゲートウェイノードへのクライアント API 接続を保護します。これらのノードは、 S3 および Swift クライアントアプリケーションがオブジェクトデータをアップロードおよびダウンロードするために使用します。

インストールされるグローバル証明書には次の情報が含まれます。

- * 名前 * ：証明書の管理リンクを持つ証明書の名前。
- * 概要 *
- * タイプ * ：カスタムまたはデフォルト。+ グリッドセキュリティを向上させるために、常にカスタム証明書を使用する必要があります。
- * 失効日 * ：デフォルトの証明書を使用している場合、有効期限は表示されません。

可能です

- グリッドセキュリティを向上させるには、外部の認証局によって署名されたカスタム証明書でデフォルト証明書を置き換えます。
  - "StorageGRID で生成されたデフォルトの管理インターフェイス証明書を置き換えます" Grid Manager 接続と Tenant Manager 接続に使用されます。
  - "S3 および Swift API 証明書を置き換えます" ストレージノードとロードバランサエンドポイント（オプション）の接続に使用されます。
- "管理インターフェイスのデフォルトの証明書をリストア"
- "S3 および Swift のデフォルトの API 証明書をリストア"
- "スクリプトを使用して、新しい自己署名管理インターフェイス証明書を生成します。"
- をコピーまたはダウンロードします "管理インターフェイスの証明書" または "S3 および Swift API 証明書"。

Grid CA

。 Grid CA 証明書は、 StorageGRID のインストール時に StorageGRID 認証局によって生成され、すべての内部 StorageGRID トラフィックを保護します。

証明書情報には、証明書の有効期限とその内容が含まれます。

可能です "グリッドCA証明書をコピーまたはダウンロードします"しかし、変更することはできません。

クライアント

クライアント証明書は外部の認証局によって生成され、外部の監視ツールと StorageGRID の Prometheus データベースとの間の接続を保護します。

証明書テーブルには、設定されている各クライアント証明書の行があり、証明書の有効期限とともにPrometheus データベースへのアクセスに証明書を使用できるかどうかが示されます。

可能です

- "新しいクライアント証明書をアップロードまたは生成します。"
- 証明書名を選択して証明書の詳細を表示します。表示される情報は次のとおりです。
  - "クライアント証明書の名前を変更します。"
  - "Prometheus のアクセス権限を設定します。"
  - "クライアント証明書をアップロードして置き換えます。"
  - "クライアント証明書をコピーまたはダウンロードします。"
  - "クライアント証明書を削除します。"
- [* アクション * （ Actions * ）] を選択して、すばやく "編集"、 "添付（ Attach ）"または "取り外します" クライアント証明書。最大 10 個のクライアント証明書を選択し、 * Actions * > * Remove * を使用して一度に削除できます。

ロードバランサエンドポイント

ロードバランサエンドポイントの証明書 S3およびSwiftクライアントと、ゲートウェイノードと管理ノード上のStorageGRID ロードバランササービスの間の接続を保護します。

ロードバランサエンドポイントテーブルには、設定されている各ロードバランサエンドポイント用の行があり、グローバルな S3 および Swift API 証明書とカスタムのロードバランサエンドポイント証明書のどちらがエンドポイントに使用されているかを示しています。各証明書の有効期限も表示されます。

> エンドポイント証明書の変更がすべてのノードに適用されるまでに最大 15 分かかることがあります。

可能です

- "ロードバランサエンドポイントを表示します"証明書の詳細を含む。
- "FabricPool のロードバランサエンドポイント証明書を指定します。"
- "グローバルな S3 および Swift API 証明書を使用します" 代わりに、新しいロードバランサエンドポイント証明書を生成します。

テナント

テナントで使用できる アイデンティティフェデレーションサーバの証明書 または プラットフォームサービスエンドポイントの証明書 StorageGRID を使用して接続を保護します。

テナントテーブルには、テナントごとに 1 つの行があり、各テナントに独自のアイデンティティソースまたは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を示します。

可能です

- "Tenant Manager にサインインするテナント名を選択します"
- "テナントのアイデンティティフェデレーションの詳細を表示するテナント名を選択します"
- "テナントプラットフォームサービスの詳細を表示するテナント名を選択します"

- "エンドポイントの作成時にプラットフォームサービスエンドポイント証明書を指定します"

その他

StorageGRID では、特定の目的に他のセキュリティ証明書を使用します。これらの証明書は、機能名で一覧表示されます。その他のセキュリティ証明書には、次のもの

- クラウドストレージプールの証明書
- E メールアラート通知の証明書
- 外部 syslog サーバ証明書
- グリッドフェデレーション接続の証明書
- アイデンティティフェデレーション証明書
- キー管理サーバ（ KMS ）の証明書
- シングルサインオン証明書

情報は、関数が使用する証明書の種類と、そのサーバーおよびクライアント証明書の有効期限を示します。関数名を選択するとブラウザタブが開き、証明書の詳細を表示および編集できます。

他の証明書の情報を表示およびアクセスできるのは、適切な権限がある場合のみです。

可能です

- "S3 、 C2S S3 、または Azure 用のクラウドストレージプール証明書を指定します"
- "アラート E メール通知用の証明書を指定します"
- "外部 syslog サーバの証明書を指定します"
- "グリッドフェデレーション接続の証明書をローテーションします"
- "アイデンティティフェデレーション証明書を表示および編集する"
- "キー管理サーバ（ KMS ）のサーバ証明書とクライアント証明書をアップロードします"
- "証明書利用者信頼のSSO証明書を手動で指定します"

セキュリティ証明書の詳細

各タイプのセキュリティ証明書について、実装手順へのリンクとともに以下に説明します。

管理インターフェイスの証明書

証明書のタイプ	説明	ナビゲーションの場所	詳細
サーバ	クライアントの Web ブラウザと StorageGRID 管理インターフェイスの間の接続を認証することで、ユーザがセキュリティの警告なしで Grid Manager とテナントマネージャにアクセスできるようにします。 この証明書は、 Grid 管理 API 接続とテナント管理 API 接続も認証します。 インストール時に作成されるデフォルトの証明書を使用することも、カスタム証明書をアップロードすることもできます。	• 設定 * > * セキュリティ * > * 証明書 * 、 * グローバル * タブを選択し、 * 管理インターフェイス証明書 * を選択します	"管理インターフェイス証明書を設定"

S3 および **Swift API** 証明書

証明書のタイプ	説明	ナビゲーションの場所	詳細
サーバ	ストレージノードとロードバランサエンドポイントへのS3またはSwiftクライアントのセキュアな接続を認証します（オプション）。	• configuration * > * Security * > * Certificates * を選択し、 * Global * タブを選択して、 * S3 および Swift API certificate * を選択します	"S3 および Swift API 証明書を設定する"

Grid CA 証明書

を参照してください デフォルトの Grid CA 証明書概要。

管理者クライアント証明書

証明書のタイプ	説明	ナビゲーションの場所	詳細
クライアント	StorageGRID が外部クライアントアクセスを認証できるように、各クライアントにインストールします。 • 許可された外部クライアントから StorageGRID Prometheus データベースにアクセスできるようにします。 • 外部ツールを使用して StorageGRID をセキュアに監視できます。	• 設定 * > * セキュリティ * > * 証明書 * を選択し、 * クライアント * タブを選択します	"クライアント証明書を設定"

ロードバランサエンドポイントの証明書

証明書のタイプ	説明	ナビゲーションの場所	詳細
サーバ	S3 または Swift クライアントと、ゲートウェイノードおよび管理ノード上の StorageGRID ロードバランササービス間の接続を認証します。ロードバランサエンドポイントの設定時にロードまたは生成できます。クライアントアプリケーションでは、 StorageGRID に接続する際にロードバランサ証明書を使用してオブジェクトデータを保存および読み出します。 グローバルのカスタムバージョンを使用することもできます S3 および Swift API 証明書 ロードバランササービスへの接続を認証する証明書。グローバル証明書を使用してロードバランサ接続を認証する場合は、ロードバランサエンドポイントごとに個別の証明書をアップロードまたは生成する必要はありません。 • 注： * ロードバランサ認証に使用される証明書は、通常の StorageGRID 処理で最もよく使用される証明書です。	• 設定 * > * ネットワーク * > * ロードバランサエンドポイント *	• "ロードバランサエンドポイントを設定する" • "FabricPool のロードバランサエンドポイントを作成します"

クラウドストレージプールのエンドポイントの証明書

証明書のタイプ	説明	ナビゲーションの場所	詳細
サーバ	StorageGRID クラウドストレージプールから S3 Glacier や Microsoft Azure BLOB ストレージなどの外部ストレージへの接続を認証します。クラウドプロバイダのタイプごとに別の証明書が必要です。	• ilm * > * ストレージ・プール *	"クラウドストレージプールを作成"

E メールアラート通知の証明書

証明書のタイプ	説明	ナビゲーションの場所	詳細
サーバとクライアント	アラート通知に使用される SMTP E メールサーバと StorageGRID 間の接続を認証します。 • SMTP サーバとの通信に Transport Layer Security （ TLS ）が必要な場合は、 E メールサーバの CA 証明書を指定する必要があります。 • SMTP E メールサーバで認証用のクライアント証明書が必要な場合にのみ、クライアント証明書を指定してください。	• アラート > 電子メールセットアップ *	"アラート用の E メール通知を設定します"

外部 **syslog** サーバの証明書

証明書のタイプ	説明	ナビゲーションの場所	詳細
サーバ	StorageGRID にイベントを記録する外部 syslog サーバ間で、 TLS 接続または RELP/TLS 接続を認証します。 • 注：外部 syslog サーバへの TCP 、 RELP/TCP 、および UDP 接続には、外部 syslog サーバ証明書は必要ありません。	• 設定 * > * モニタリング * > * 監査および syslog サーバ * を選択し、 * 外部 syslog サーバの設定 * を選択します	"外部 syslog サーバを設定します"

[[grid-federation-certificate]グリッドフェデレーション接続証明書

証明書のタイプ	説明	ナビゲーションの場所	詳細
サーバとクライアント	グリッドフェデレーション接続で、現在のStorageGRID システムと別のグリッドの間で送信される情報を認証して暗号化します。	設定>*システム*>*グリッドフェデレーション*	• "グリッドフェデレーション接続を作成する" • "接続証明書をローテーションします"

アイデンティティフェデレーション証明書

証明書のタイプ	説明	ナビゲーションの場所	詳細
サーバ	Active Directory 、 OpenLDAP 、 Oracle Directory Server などの外部のアイデンティティプロバイダと StorageGRID の間の接続を認証します。アイデンティティフェデレーションに使用します。管理者グループとユーザを外部システムで管理できます。	• 設定 * > * アクセス制御 * > * アイデンティティフェデレーション *	"アイデンティティフェデレーションを使用する"

キー管理サーバ（ **KMS** ）の証明書

証明書のタイプ	説明	ナビゲーションの場所	詳細
サーバとクライアント	StorageGRID と外部キー管理サーバ（ KMS ）の間の接続を認証します。この接続により、 StorageGRID アプライアンスノードに暗号化キーが提供されます。	• 設定 * > * セキュリティ * > * キー管理サーバ *	"キー管理サーバの追加（ KMS ）"

プラットフォームサービスのエンドポイント証明書

証明書のタイプ	説明	ナビゲーションの場所	詳細
サーバ	StorageGRID プラットフォームサービスから S3 ストレージリソースへの接続を認証します。	• Tenant Manager * > * storage （ S3 ） * > * Platform services endpoints *	"プラットフォームサービスエンドポイントを作成します" "プラットフォームサービスエンドポイントを編集します"

シングルサインオン（ **SSO** ）証明書

証明書のタイプ	説明	ナビゲーションの場所	詳細
サーバ	Active Directory フェデレーションサービス（ AD FS ）やシングルサインオン（ SSO ）要求に使用される StorageGRID などのアイデンティティフェデレーションサービスとの間の接続を認証します。	• 設定 * > * アクセス制御 * > * シングルサインオン *	"シングルサインオンを設定します"

証明書の例

例 **1** ：ロードバランササービス

この例では、 StorageGRID がサーバとして機能します。

1. ロードバランサエンドポイントを設定し、 StorageGRID でサーバ証明書をアップロードまたは生成します。
2. S3 または Swift クライアント接続をロードバランサエンドポイントに設定し、同じ証明書をクライアントにアップロードします。
3. クライアントは、データを保存または取得する際に HTTPS を使用してロードバランサエンドポイントに接続します。
4. StorageGRID は、公開鍵を含むサーバ証明書と、秘密鍵に基づく署名を返します。
5. クライアントは、サーバの署名と証明書のコピーの署名を比較して、この証明書を検証します。署名が一致した場合、クライアントは同じ公開鍵を使用してセッションを開始します。
6. クライアントがオブジェクトデータを StorageGRID に送信

例 **2** ：外部キー管理サーバ（ **KMS** ）

この例では、 StorageGRID がクライアントとして機能します。

1. 外部キー管理サーバソフトウェアを使用する場合は、 StorageGRID を KMS クライアントとして設定し、 CA 署名済みサーバ証明書、パブリッククライアント証明書、およびクライアント証明書の秘密鍵を取得します。
2. Grid Manager を使用して KMS サーバを設定し、サーバ証明書とクライアント証明書およびクライアント秘密鍵をアップロードします。
3. StorageGRID ノードで暗号化キーが必要な場合、証明書からのデータと秘密鍵に基づく署名を含む KMS サーバに要求が送信されます。
4. KMS サーバは証明書の署名を検証し、 StorageGRID を信頼できることを決定します。
5. KMS サーバは、検証済みの接続を使用して応答します。

サーバ証明書を設定

サポートされているサーバ証明書のタイプ

StorageGRID システムでは、 RSA または ECDSA （ Elliptic Curve Digital Signature

Algorithm ）で暗号化されたカスタム証明書がサポートされます。

セキュリティポリシーの暗号タイプは、サーバ証明書タイプと一致している必要があります。たとえば、RSA暗号にはRSA証明書が必要で、ECDSA暗号にはECDSA証明書が必要です。を参照してください "セキュリティ証明書を管理する"。サーバ証明書と互換性のないカスタムセキュリティポリシーを設定する場合は、設定できます "一時的にデフォルトのセキュリティポリシーに戻します"。

StorageGRID でREST APIのクライアント接続を保護する方法の詳細については、を参照してください "S3 REST APIのセキュリティを設定" または "Swift REST APIのセキュリティを設定します"。

管理インターフェイス証明書を設定

デフォルトの管理インターフェイス証明書を単一のカスタム証明書に置き換えると、ユーザがグリッドマネージャとテナントマネージャにアクセスする際にセキュリティの警告が表示されなくなります。デフォルトの管理インターフェイス証明書に戻すか、新しい証明書を生成することもできます。

このタスクについて

デフォルトでは、管理ノードごとに、グリッド CA によって署名された証明書が 1 つずつ発行されます。これらの CA 署名証明書は、単一の共通するカスタム管理インターフェイス証明書および対応する秘密鍵に置き換えることができます。

Grid Manager および Tenant Manager への接続時にクライアントがホスト名を確認する必要がある場合は、単一のカスタム管理インターフェイスの証明書がすべての管理ノードに対して使用されるため、ワイルドカード証明書またはマルチドメイン証明書として指定する必要があります。グリッド内のすべての管理ノードに一致するカスタム証明書を定義してください。

設定はサーバ上で行う必要があります。また、使用しているルート認証局（ CA ）によっては、ユーザが Grid Manager および Tenant Manager へのアクセスに使用する Web ブラウザに Grid CA 証明書をインストールすることも必要になります。

サーバ証明書の問題によって処理が中断されないようにするために、このサーバ証明書の有効期限が近づくと* Expiration of server certificate for Management Interface *アラートがトリガーされます。必要に応じて、 ［グローバル］ タブで ［* 設定 *］ > ［* セキュリティ *］ > ［* 証明書 *］ を選択し、管理インターフェイス証明書の有効期限を確認することで、現在の証明書の有効期限を確認できます。

IP アドレスではなくドメイン名を使用して Grid Manager または Tenant Manager にアクセスする場合は、次のいずれかの場合に証明書のエラーが表示され、バイパスするオプションはありません。

- カスタム管理インターフェイス証明書の有効期限が切れます。
- あなた カスタム管理インターフェイス証明書をデフォルトのサーバ証明書に戻します。

カスタム管理インターフェイス証明書を追加します

カスタムの管理インターフェイス証明書を追加するには、 Grid Manager を使用して独自の証明書を指定するか、証明書を生成します。

手順

1. [* configuration * > * Security * > * Certificates *] を選択します。
2. [* グローバル *] タブで、 [* 管理インターフェイス証明書 *] を選択します。
3. [* カスタム証明書を使用する *] を選択します。
4. 証明書をアップロードまたは生成します。

証明書をアップロードする

必要なサーバ証明書ファイルをアップロードします。

a. [証明書のアップロード] を選択します。

b. 必要なサーバ証明書ファイルをアップロードします。

- * サーバ証明書 * ：カスタムサーバ証明書ファイル（ PEM エンコード）。
- 証明書の秘密鍵：カスタムサーバ証明書の秘密鍵ファイル (`.key`）。

> EC 秘密鍵は 224 ビット以上である必要があります。RSA 秘密鍵は 2048 ビット以上にする必要があります。

- **CA Bundle** ：各中間発行認証局（ CA ）の証明書を含む単一のオプションファイル。このファイルには、 PEM でエンコードされた各 CA 証明書ファイルが、証明書チェーンの順序で連結して含まれている必要があります。

c. [* 証明書の詳細 *] を展開して、アップロードした各証明書のメタデータを表示します。オプションの CA バンドルをアップロードした場合は、各証明書が独自のタブに表示されます。

- 証明書ファイルを保存するには、 * 証明書のダウンロード * を選択します。証明書バンドルを保存するには、 * CA バンドルのダウンロード * を選択します。

  証明書ファイルの名前とダウンロード先を指定します。拡張子を付けてファイルを保存します `.pem`。

  例： `storagegrid_certificate.pem`

- 証明書の内容をコピーして他の場所に貼り付けるには、 * 証明書の PEM のコピー * または * CA バンドル PEM のコピー * を選択してください。

d. [保存（ Save ）] を選択します。+ Grid Manager 、 Tenant Manager 、 Grid Manager API 、または Tenant Manager API への以降のすべての新しい接続にはカスタムの管理インターフェイス証明書が使用されます。

証明書の生成

サーバ証明書ファイルを生成します。

> 本番環境では、外部の認証局によって署名されたカスタム管理インターフェイス証明書を使用することを推奨します。

a. [* 証明書の生成 *] を選択します。

b. 証明書情報を指定します。

フィールド	説明
ドメイン名	証明書に含める1つ以上の完全修飾ドメイン名。複数のドメイン名を表すには、ワイルドカードとして * を使用します。

フィールド	説明
IP	証明書に含める1つ以上のIPアドレス。
件名（オプション）	証明書所有者のX.509サブジェクト名または識別名（DN）。 このフィールドに値を入力しない場合、生成される証明書では、最初のドメイン名またはIPアドレスがサブジェクト共通名（CN）として使用されます。
有効な日数	作成後に証明書の有効期限が切れる日数。
キー使用の拡張機能を追加します	選択されている場合（デフォルトおよび推奨）、キー使用と拡張キー使用拡張が生成された証明書に追加されます。 これらの拡張機能は、証明書に含まれるキーの目的を定義します。 注:証明書にこれらの拡張機能が含まれている場合、古いクライアントで接続の問題が発生する場合を除き、このチェックボックスをオンのままにします。

c. [*Generate （生成）] を選択します

d. 生成された証明書のメタデータを表示するには、 [証明書の詳細] を選択します。

- 証明書ファイルを保存するには、 [証明書のダウンロード] を選択します。

  証明書ファイルの名前とダウンロード先を指定します。拡張子を付けてファイルを保存します `.pem`。

  例： `storagegrid_certificate.pem`

- 証明書の内容をコピーして他の場所に貼り付けるには、 * 証明書の PEM をコピー * を選択します。

e. [保存（ Save ）] を選択します。+ Grid Manager 、 Tenant Manager 、 Grid Manager API 、または Tenant Manager API への以降のすべての新しい接続にはカスタムの管理インターフェイス証明書が使用されます。

5. Web ブラウザが更新されたことを確認するには、ページをリフレッシュしてください。

新しい証明書をアップロードまたは生成したあと、関連する証明書の有効期限アラートがクリアされるまでに最大 1 日かかります。

6. カスタムの管理インターフェイス証明書を追加すると、使用中の証明書の詳細な証明書情報が管理インターフェイスの証明書ページに表示されます。+ 必要に応じて証明書 PEM をダウンロードまたはコピーできます。

管理インターフェイスのデフォルトの証明書をリストア

Grid Manager 接続と Tenant Manager 接続でのデフォルトの管理インターフェイス証明書を使用するように戻すことができます。

手順

1. [* configuration * > * Security * > * Certificates *] を選択します。
2. [* グローバル *] タブで、 [* 管理インターフェイス証明書 *] を選択します。
3. [* デフォルト証明書を使用する *] を選択します。

   管理インターフェイスのデフォルトの証明書をリストアすると、設定したカスタムサーバ証明書ファイルは削除され、システムからはリカバリできなくなります。以降すべての新しいクライアント接続には、デフォルトの管理インターフェイス証明書が使用されます。

4. Web ブラウザが更新されたことを確認するには、ページをリフレッシュしてください。

スクリプトを使用して、新しい自己署名管理インターフェイス証明書を生成します

ホスト名の厳密な検証が必要な場合は、スクリプトを使用して管理インターフェイス証明書を生成できます。

作業を開始する前に

- 特定のアクセス権限が必要です。
- を使用することができます `Passwords.txt` ファイル。

このタスクについて

本番環境では、外部の認証局によって署名された証明書を使用することを推奨します。

手順

1. 各管理ノードの完全修飾ドメイン名（ FQDN ）を取得します。
2. プライマリ管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@primary_Admin_Node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

      rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

3. 新しい自己署名証明書を使用して StorageGRID を設定します。

   ```
   $ sudo make-certificate --domains wildcard-admin-node-fqdn --type management
   ```

   - の場合 `--domains`、ワイルドカードを使用して、すべての管理ノードの完全修飾ドメイン名を表します。例： `*.ui.storagegrid.example.com` ワイルドカード*を使用して表します `admin1.ui.storagegrid.example.com` および `admin2.ui.storagegrid.example.com`。
   - 設定 `--type` 終了： `management` 管理インターフェイスの証明書を設定します。この証明書はGrid ManagerとTenant Managerで使用されます。

◦ デフォルトでは、生成された証明書の有効期間は 1 年間（ 365 日）です。この期間を過ぎる前に証明書を再作成する必要があります。を使用できます `--days` デフォルトの有効期間を上書きする引数。

> 証明書の有効期間は、で始まります `make-certificate` を実行します。管理クライアントが StorageGRID と同じ時間ソースと同期されるようにしてください。同期されていないと、クライアントが証明書を拒否する可能性があります。

```
$ sudo make-certificate --domains *.ui.storagegrid.example.com --type
management --days 720
```

出力には、管理 API クライアントで必要なパブリック証明書が含まれています。

4. 証明書を選択してコピーします。

   BEGIN タグと END タグも含めて選択してください。

5. コマンドシェルからログアウトします。 `$ exit`
6. 証明書が設定されたことを確認します。
   a. Grid Manager にアクセスします。
   b. [* configuration * > * Security * > * Certificates *] を選択します
   c. [* グローバル *] タブで、 [* 管理インターフェイス証明書 *] を選択します。
7. コピーしたパブリック証明書を使用するように管理クライアントを設定します。BEGIN タグと END タグを含めてください。

管理インターフェイス証明書をダウンロードまたはコピーします

管理インターフェイスの証明書の内容を保存またはコピーして、他の場所で使用することができます。

手順

1. [* configuration * > * Security * > * Certificates *] を選択します。
2. [* グローバル *] タブで、 [* 管理インターフェイス証明書 *] を選択します。
3. [**Server**] タブまたは [**CA Bundle**] タブを選択し、証明書をダウンロードまたはコピーします。

証明書ファイルまたは **CA** バンドルをダウンロードします

証明書またはCAバンドルをダウンロードします `.pem` ファイル。オプションの CA バンドルを使用している場合は、バンドル内の各証明書が独自のサブタブに表示されます。

a. [証明書のダウンロード *] または [CA バンドルのダウンロード *] を選択します。

   CA バンドルをダウンロードする場合、 CA バンドルのセカンダリタブにあるすべての証明書が単一のファイルとしてダウンロードされます。

b. 証明書ファイルの名前とダウンロード先を指定します。拡張子を付けてファイルを保存します `.pem`。

   例： `storagegrid_certificate.pem`

証明書または **CA** バンドル **PEM** をコピーしてください

証明書のテキストをコピーして別の場所に貼り付けてください。オプションの CA バンドルを使用している場合は、バンドル内の各証明書が独自のサブタブに表示されます。

a. [Copy certificate PEM* （証明書のコピー）] または [* Copy CA bundle PEM* （ CA バンドル PEM のコピー）

   CA バンドルをコピーする場合、 CA バンドルのセカンダリタブにあるすべての証明書が一緒にコピーされます。

b. コピーした証明書をテキストエディタに貼り付けます。

c. 拡張子を付けてテキストファイルを保存します `.pem`。

   例： `storagegrid_certificate.pem`

S3 および **Swift API** 証明書を設定する

ストレージノードまたはロードバランサエンドポイントへのS3 / Swiftクライアント接続に使用されるサーバ証明書を置き換えたりリストアしたりできます。置き換え用のカスタムサーバ証明書は組織に固有のものです。

このタスクについて

デフォルトでは、すべてのストレージノードに、グリッド CA によって署名された X.509 サーバ証明書が発行されます。これらの CA 署名証明書は、単一の共通するカスタムサーバ証明書および対応する秘密鍵で置き換えることができます。

1 つのカスタムサーバ証明書がすべてのストレージノードに対して使用されるため、ストレージエンドポイントへの接続時にクライアントがホスト名を確認する必要がある場合は、ワイルドカード証明書またはマルチドメイン証明書として指定する必要があります。グリッド内のすべてのストレージノードに一致するカスタム証明書を定義してください。

サーバでの設定が完了したら、使用しているルート認証局（ CA ）によっては、システムへのアクセスに使用する S3 または Swift API クライアントにグリッド CA 証明書をインストールすることも必要になる場合があ

ります。

> サーバ証明書の問題によって処理が中断されないようにするために、ルートサーバ証明書の有効期限が近づくと* Expiration of global server certificate for S3 and Swift API *アラートがトリガーされます。必要に応じて、現在の証明書の有効期限を確認するには、 * configuration * > * Security * > * Certificates * を選択し、 S3 および Swift API 証明書の有効期限を Global タブで確認します。

S3 および Swift のカスタム API 証明書をアップロードまたは生成できます。

S3 および **Swift** のカスタム **API** 証明書を追加します

手順

1. [* configuration * > * Security * > * Certificates *] を選択します。
2. Global * タブで、 * S3 および Swift API 証明書 * を選択します。
3. [* カスタム証明書を使用する *] を選択します。
4. 証明書をアップロードまたは生成します。

証明書をアップロードする

必要なサーバ証明書ファイルをアップロードします。

a. [証明書のアップロード] を選択します。

b. 必要なサーバ証明書ファイルをアップロードします。

- * サーバ証明書 * ：カスタムサーバ証明書ファイル（ PEM エンコード）。
- 証明書の秘密鍵：カスタムサーバ証明書の秘密鍵ファイル (`.key`）。

> EC 秘密鍵は 224 ビット以上である必要があります。RSA 秘密鍵は 2048 ビット以上にする必要があります。

- **CA Bundle** ：各中間発行認証局の証明書を含む単一のオプションファイル。このファイルには、 PEM でエンコードされた各 CA 証明書ファイルが、証明書チェーンの順序で連結して含まれている必要があります。

c. 証明書の詳細を選択して、アップロードしたカスタムの S3 および Swift API 証明書ごとにメタデータと PEM を表示します。オプションの CA バンドルをアップロードした場合は、各証明書が独自のタブに表示されます。

- 証明書ファイルを保存するには、 * 証明書のダウンロード * を選択します。証明書バンドルを保存するには、 * CA バンドルのダウンロード * を選択します。

  証明書ファイルの名前とダウンロード先を指定します。拡張子を付けてファイルを保存します `.pem`。

  例： `storagegrid_certificate.pem`

- 証明書の内容をコピーして他の場所に貼り付けるには、 * 証明書の PEM のコピー * または * CA バンドル PEM のコピー * を選択してください。

d. [保存（ Save ）] を選択します。

以降の新しい S3 および Swift クライアント接続には、カスタムサーバ証明書が使用されます。

証明書の生成

サーバ証明書ファイルを生成します。

a. [* 証明書の生成 *] を選択します。

b. 証明書情報を指定します。

フィールド	説明
ドメイン名	証明書に含める1つ以上の完全修飾ドメイン名。複数のドメイン名を表すには、ワイルドカードとして * を使用します。
IP	証明書に含める1つ以上のIPアドレス。

フィールド	説明
件名（オプション）	証明書所有者のX.509サブジェクト名または識別名（DN）。 このフィールドに値を入力しない場合、生成される証明書では、最初のドメイン名またはIPアドレスがサブジェクト共通名（CN）として使用されます。
有効な日数	作成後に証明書の有効期限が切れる日数。
キー使用の拡張機能を追加します	選択されている場合（デフォルトおよび推奨）、キー使用と拡張キー使用拡張が生成された証明書に追加されます。 これらの拡張機能は、証明書に含まれるキーの目的を定義します。 注:証明書にこれらの拡張機能が含まれている場合、古いクライアントで接続の問題が発生する場合を除き、このチェックボックスをオンのままにします。

c. [*Generate （生成）] を選択します

d. Certificate Details * を選択して、生成されたカスタムの S3 および Swift API 証明書のメタデータと PEM を表示します。

- 証明書ファイルを保存するには、 [証明書のダウンロード] を選択します。

  証明書ファイルの名前とダウンロード先を指定します。拡張子を付けてファイルを保存します `.pem`。

例： `storagegrid_certificate.pem`

- 証明書の内容をコピーして他の場所に貼り付けるには、 * 証明書の PEM をコピー * を選択します。

e. [保存（ Save ）] を選択します。

以降の新しい S3 および Swift クライアント接続には、カスタムサーバ証明書が使用されます。

5. タブを選択して、デフォルトの StorageGRID サーバ証明書、アップロードされた CA 署名証明書、または生成されたカスタム証明書のメタデータを表示します。

> 新しい証明書をアップロードまたは生成したあと、関連する証明書の有効期限アラートがクリアされるまでに最大 1 日かかります。

6. Web ブラウザが更新されたことを確認するには、ページをリフレッシュしてください。

7. カスタムの S3 および Swift API 証明書を追加すると、使用中のカスタムの S3 および Swift API 証明書の詳細な証明書情報が S3 および Swift API の証明書ページに表示されます。+ 必要に応じて証明書 PEM をダウンロードまたはコピーできます。

S3 および Swift のデフォルトの API 証明書をリストア

ストレージノードへのS3およびSwiftクライアント接続でデフォルトのS3およびSwift API証明書を使用するように戻すことができます。ただし、ロードバランサエンドポイントにはデフォルトのS3およびSwift API証明書を使用できません。

手順

1. [* configuration * > * Security * > * Certificates *] を選択します。
2. Global * タブで、 * S3 および Swift API 証明書 * を選択します。
3. [* デフォルト証明書を使用する *] を選択します。

   S3およびSwift APIのグローバル証明書のデフォルトバージョンをリストアすると、設定したカスタムサーバ証明書ファイルは削除され、システムからリカバリすることはできません。ストレージノードへの以降の新しいS3およびSwiftクライアント接続には、デフォルトのS3およびSwift API証明書が使用されます。

4. 警告を確認し、デフォルトの S3 および Swift API 証明書をリストアするには、「 * OK 」を選択します。

   Root Access 権限がある環境で、 S3 および Swift API のカスタム証明書をロードバランサエンドポイントの接続に使用していた場合は、デフォルトの S3 および Swift API 証明書を使用してアクセスできなくなるロードバランサエンドポイントのリストが表示されます。に進みます "ロードバランサエンドポイントを設定する" 影響を受けるエンドポイントを編集または削除します。

5. Web ブラウザが更新されたことを確認するには、ページをリフレッシュしてください。

S3 および Swift API 証明書をダウンロードまたはコピーします

S3 および Swift API 証明書の内容を保存またはコピーして、他の場所で使用することができます。

手順

1. [* configuration * > * Security * > * Certificates *] を選択します。
2. Global * タブで、 * S3 および Swift API 証明書 * を選択します。
3. [**Server**] タブまたは [**CA Bundle**] タブを選択し、証明書をダウンロードまたはコピーします。

証明書ファイルまたは **CA** バンドルをダウンロードします

証明書またはCAバンドルをダウンロードします `.pem` ファイル。オプションの CA バンドルを使用している場合は、バンドル内の各証明書が独自のサブタブに表示されます。

a. [証明書のダウンロード *] または [CA バンドルのダウンロード *] を選択します。

   CA バンドルをダウンロードする場合、 CA バンドルのセカンダリタブにあるすべての証明書が単一のファイルとしてダウンロードされます。

b. 証明書ファイルの名前とダウンロード先を指定します。拡張子を付けてファイルを保存します `.pem`。

   例： `storagegrid_certificate.pem`

証明書または **CA** バンドル **PEM** をコピーしてください

証明書のテキストをコピーして別の場所に貼り付けてください。オプションの CA バンドルを使用している場合は、バンドル内の各証明書が独自のサブタブに表示されます。

a. [Copy certificate PEM* （証明書のコピー）] または [* Copy CA bundle PEM* （ CA バンドル PEM のコピー）

   CA バンドルをコピーする場合、 CA バンドルのセカンダリタブにあるすべての証明書が一緒にコピーされます。

b. コピーした証明書をテキストエディタに貼り付けます。

c. 拡張子を付けてテキストファイルを保存します `.pem`。

   例： `storagegrid_certificate.pem`

関連情報

- "S3 REST APIを使用する"
- "Swift REST APIを使用する"
- "S3エンドポイントのドメイン名を設定"

Grid CA 証明書をコピーする

StorageGRID は、内部の認証局（ CA ）を使用して内部トラフィックを保護します。独自の証明書をアップロードしても、この証明書は変更されません。

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"。
- 特定のアクセス権限が必要です。

このタスクについて

カスタムサーバ証明書が設定されている場合、クライアントアプリケーションはカスタムサーバ証明書を使用

してサーバを検証する必要があります。StorageGRID システムから CA 証明書をコピーしない。

手順

1. [* configuration * > * Security * > * Certificates *] を選択し、 [* Grid CA *] タブを選択します。
2. [Certificate PEM]セクションで、証明書をダウンロードまたはコピーします。

証明書ファイルをダウンロードします

証明書をダウンロードします `.pem` ファイル。

a. [証明書のダウンロード] を選択します。
b. 証明書ファイルの名前とダウンロード先を指定します。拡張子を付けてファイルを保存します `.pem`。

例： `storagegrid_certificate.pem`

証明書 **PEM** をコピーします

証明書のテキストをコピーして別の場所に貼り付けてください。

a. [* 証明書 PEM のコピー *] を選択します。
b. コピーした証明書をテキストエディタに貼り付けます。
c. 拡張子を付けてテキストファイルを保存します `.pem`。

例： `storagegrid_certificate.pem`

FabricPool の **StorageGRID** 証明書を設定します

S3クライアントが厳密なホスト名検証を実行し、厳密なホスト名検証の無効化をサポートしていない場合（FabricPool を使用するONTAP クライアントなど）は、ロードバランサエンドポイントの設定時にサーバ証明書を生成またはアップロードできます。

作業を開始する前に

- 特定のアクセス権限が必要です。
- 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"。

このタスクについて

ロードバランサエンドポイントを作成する際には、自己署名サーバ証明書を生成するか、既知の認証局（ CA ）によって署名された証明書をアップロードできます。本番環境では、既知の CA によって署名された証明書を使用する必要があります。CA によって署名された証明書は、システムを停止することなくローテーションできます。また、中間者攻撃に対する保護としても優れているため、セキュリティも強化されます。

次の手順は、 FabricPool を使用する S3 クライアントを対象とした一般的なガイドラインです。詳細な情報と手順については、を参照してください "StorageGRID for FabricPool を設定します"。

手順

1. 必要に応じて、 FabricPool で使用するハイアベイラビリティ（ HA ）グループを設定します。
2. FabricPool で使用する S3 ロードバランサエンドポイントを作成します。

   HTTPS ロードバランサエンドポイントを作成する際に、サーバ証明書、証明書の秘密鍵、およびオプションの CA バンドルをアップロードするように求められます。

3. ONTAP でクラウド階層として StorageGRID を接続します。

   ロードバランサエンドポイントのポートと、アップロードした CA 証明書で使用する完全修飾ドメイン名を指定します。次に、 CA 証明書を指定します。

> 中間 CA が StorageGRID 証明書を発行した場合は、中間 CA 証明書を指定する必要があります。StorageGRID 証明書がルート CA によって直接発行された場合は、ルート CA 証明書を指定する必要があります。

クライアント証明書を設定

クライアント証明書を使用すると、許可された外部クライアントから StorageGRID の Prometheus データベースにアクセスして、外部ツールで StorageGRID を監視するための安全な方法を提供できます。

外部の監視ツールを使用してStorageGRID にアクセスする必要がある場合は、グリッドマネージャを使用してクライアント証明書をアップロードまたは生成し、証明書の情報を外部ツールにコピーする必要があります。

を参照してください "セキュリティ証明書を管理する" および "カスタムサーバ証明書を設定する"。

> サーバ証明書の問題によって処理が中断されないようにするために、このサーバ証明書の有効期限が近づくと* Expiration of client certificates configured on the Certificates page *アラートがトリガーされます。必要に応じて、 ［クライアント］ タブで ［* 設定 *］ > ［* セキュリティ *］ > ［* 証明書 *］ を選択し、クライアント証明書の有効期限を確認することで、現在の証明書の有効期限を確認できます。

> 特別に設定されたアプライアンスノード上のデータを保護するためにキー管理サーバ（ KMS ）を使用する場合は、についての具体的な情報を参照してください "KMS クライアント証明書をアップロードする"。

作業を開始する前に

- Root Access 権限が割り当てられている。
- 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"。
- クライアント証明書を設定するには：
  - 管理ノードの IP アドレスまたはドメイン名を確認しておきます。
  - StorageGRID 管理インターフェイス証明書を設定している場合は、管理インターフェイス証明書の設定に使用するCA、クライアント証明書、および秘密鍵を用意しておきます。
  - 独自の証明書をアップロードするには、証明書の秘密鍵をローカルコンピュータで使用できます。
  - 秘密鍵は、作成時に保存または記録しておく必要があります。元の秘密鍵がない場合は、新しい秘密

鍵を作成する必要があります。

- クライアント証明書を編集するには：
  - 管理ノードの IP アドレスまたはドメイン名を確認しておきます。
  - 独自の証明書または新しい証明書をアップロードするには、ローカルコンピュータ上で秘密鍵、クライアント証明書、およびCA（使用している場合）を使用できます。

クライアント証明書を追加します

クライアント証明書を追加するには、次のいずれかの手順を実行します。

- [管理インターフェイス証明書はすでに設定されています]
- CAによって発行されたクライアント証明書
- Grid Managerから証明書が生成されました

管理インターフェイス証明書はすでに設定されています

顧客が指定したCA、クライアント証明書、および秘密鍵を使用して管理インターフェイス証明書がすでに設定されている場合は、この手順 を使用してクライアント証明書を追加します。

手順

1. Grid Manager で、 * configuration * > * Security * > * Certificates * を選択し、 * Client * タブを選択します。
2. 「 * 追加」を選択します。
3. 証明書名を入力します。
4. 外部の監視ツールを使用してPrometheus指標にアクセスするには、*[Allow Prometheus]*を選択します。
5. 「 * Continue * 」を選択します。
6. [証明書の接続]*ステップでは、管理インターフェイス証明書をアップロードします。
   a. [証明書のアップロード] を選択します。
   b. [参照]*を選択し、管理インターフェイスの証明書ファイルを選択します (`.pem`）。
      - クライアント証明書の詳細 * を選択して、証明書メタデータと証明書 PEM を表示します。
      - 証明書の内容をコピーして他の場所に貼り付けるには、 * 証明書の PEM をコピー * を選択します。
   c. 証明書を Grid Manager に保存するには、 * Create * を選択します。

      新しい証明書が [クライアント] タブに表示されます。
7. 外部監視ツールを設定します（Grafanaなど）。

CAによって発行されたクライアント証明書

管理インターフェイス証明書が設定されていない場合や、CAによって発行されたクライアント証明書と秘密鍵を使用するPrometheusのクライアント証明書を追加する場合は、この手順 を使用して管理者クライアント証明書を追加します。

手順

1. 手順~を実行します "管理インターフェイス証明書を設定します"。
2. Grid Manager で、 * configuration * > * Security * > * Certificates * を選択し、 * Client * タブを選択します。
3. 「 * 追加」を選択します。
4. 証明書名を入力します。
5. 外部の監視ツールを使用してPrometheus指標にアクセスするには、*[Allow Prometheus]*を選択します。
6. 「 * Continue * 」を選択します。
7. [証明書の添付]手順では、クライアント証明書、秘密鍵、およびCAバンドルファイルをアップロードします。
   a. [証明書のアップロード] を選択します。
   b. [参照]*を選択し、クライアント証明書、秘密鍵、およびCAバンドルファイルを選択します (`.pem`）。
      - クライアント証明書の詳細 * を選択して、証明書メタデータと証明書 PEM を表示します。
      - 証明書の内容をコピーして他の場所に貼り付けるには、 * 証明書の PEM をコピー * を選択します。
   c. 証明書を Grid Manager に保存するには、 * Create * を選択します。

      新しい証明書が[クライアント]タブに表示されます。
8. 外部監視ツールを設定します（Grafanaなど）。

Grid Managerから証明書が生成されました

管理インターフェイス証明書が設定されていない場合やGrid Managerの証明書生成機能を使用するPrometheusのクライアント証明書を追加する場合は、この手順 を使用して管理者クライアント証明書を追加します。

手順

1. Grid Manager で、 * configuration * > * Security * > * Certificates * を選択し、 * Client * タブを選択します。
2. 「 * 追加」を選択します。
3. 証明書名を入力します。
4. 外部の監視ツールを使用してPrometheus指標にアクセスするには、*[Allow Prometheus]*を選択します。
5. 「 * Continue * 」を選択します。
6. ステップで、[証明書の生成]*を選択します。
7. 証明書情報を指定します。
   - * Subject *（オプション）：証明書所有者のX.509サブジェクトまたは識別名（DN）。
   - 有効日：生成された証明書の有効日数（生成時から）。
   - キー使用拡張の追加：選択した場合（デフォルトおよび推奨）、キー使用および拡張キー使用拡張が生成された証明書に追加されます。

     これらの拡張機能は、証明書に含まれるキーの目的を定義します。

証明書にこれらの拡張機能が含まれている場合に古いクライアントで接続の問題が発生する場合を除き、このチェックボックスをオンのままにします

8. [*Generate （生成）] を選択します
9. 証明書メタデータと証明書PEMを表示するには、[クライアント証明書の詳細]を選択します。

ダイアログを閉じると、証明書の秘密鍵を表示できなくなります。キーを安全な場所にコピーまたはダウンロードします。

- 証明書の内容をコピーして他の場所に貼り付けるには、 * 証明書の PEM をコピー * を選択します。
- 証明書ファイルを保存するには、 [証明書のダウンロード] を選択します。

  証明書ファイルの名前とダウンロード先を指定します。拡張子を付けてファイルを保存します `.pem`。

例： `storagegrid_certificate.pem`

- 秘密鍵のコピー * を選択して、証明書の秘密鍵をコピーして別の場所に貼り付けます。
- 秘密鍵をファイルとして保存するには、 * 秘密鍵のダウンロード * を選択します。

  秘密鍵ファイルの名前とダウンロード先を指定します。

10. 証明書を Grid Manager に保存するには、 * Create * を選択します。

    新しい証明書が [クライアント] タブに表示されます。

11. Grid Managerで、* configuration > Security > Certificates を選択し、 Global *タブを選択します。
12. 管理インターフェイス証明書*を選択します。
13. [* カスタム証明書を使用する *] を選択します。
14. 証明書の.pemファイルとprivate_key.pemファイルをからアップロードします クライアント証明書の詳細 ステップ。CAバンドルをアップロードする必要はありません。
    a. [証明書のアップロード] を選択し、 [続行] を選択します。
    b. 各証明書ファイルをアップロードします (`.pem`）。
    c. 証明書を Grid Manager に保存するには、 * Create * を選択します。

       新しい証明書が [クライアント] タブに表示されます。

15. 外部監視ツールを設定します（Grafanaなど）。

外部監視ツールを設定します

手順

1. Grafana などの外部監視ツールで次の設定を行います。
   a. * 名前 * ：接続の名前を入力します。

      StorageGRID ではこの情報は必要ありませんが、接続をテストするための名前を指定する必要があり

ます。

b. * URL * ：管理ノードのドメイン名または IP アドレスを入力します。HTTPS とポート 9091 を指定します。

例： `https://admin-node.example.com:9091`

c. CA 証明書を使用して、 * TLS クライアント認証 * および * を有効にします。

d. TLS/SSL Auth Detailsの下で、+をコピーして貼り付けます

- 管理インターフェイスのCA証明書を**CA Cert**に追加します
- クライアント証明書をクライアント証明書に送信します
- クライアントキー**への秘密鍵

e. * ServerName* ：管理ノードのドメイン名を入力します。

servername は、管理インターフェイス証明書に表示されるドメイン名と一致する必要があります。

2. StorageGRID またはローカルファイルからコピーした証明書と秘密鍵を保存してテストします。

これで、外部の監視ツールを使用して StorageGRID から Prometheus 指標にアクセスできるようになります。

これらの指標の詳細については、を参照してください "StorageGRID の監視手順"。

クライアント証明書を編集します

管理者クライアント証明書を編集して、名前を変更したり、 Prometheus アクセスを有効または無効にしたり、現在の証明書の期限が切れたときに新しい証明書をアップロードしたりできます。

手順

1. [* configuration*>] > [* Security] * > [* Certificates*] を選択し、 [* Client*] タブを選択します。

証明書の有効期限と Prometheus のアクセス権限を次の表に示します。証明書の有効期限が近づいた場合、またはすでに有効期限が切れた場合は、メッセージが表に表示され、アラートがトリガーされます。

2. 編集する証明書を選択します。
3. 「 * Edit * 」を選択し、「 * 名前と権限を編集 * 」を選択します
4. 証明書名を入力します。
5. 外部の監視ツールを使用してPrometheus指標にアクセスするには、*[Allow Prometheus]*を選択します。
6. 証明書を Grid Manager に保存するには、「 * Continue * 」を選択します。

更新された証明書が [クライアント] タブに表示されます。

新しいクライアント証明書を接続します

現在の証明書の期限が切れたときに新しい証明書をアップロードできます。

手順

1. [* configuration*>] > [* Security] * > [* Certificates*] を選択し、 [* Client*] タブを選択します。

   証明書の有効期限と Prometheus のアクセス権限を次の表に示します。証明書の有効期限が近づいた場合、またはすでに有効期限が切れた場合は、メッセージが表に表示され、アラートがトリガーされます。

2. 編集する証明書を選択します。
3. 「 * 編集」を選択し、編集オプションを選択します。

証明書をアップロードする

証明書のテキストをコピーして別の場所に貼り付けてください。

a. [証明書のアップロード] を選択し、 [続行] を選択します。

b. クライアント証明書名をアップロードします (`.pem`）。

   クライアント証明書の詳細 * を選択して、証明書メタデータと証明書 PEM を表示します。

   - 証明書ファイルを保存するには、 [証明書のダウンロード] を選択します。

     証明書ファイルの名前とダウンロード先を指定します。拡張子を付けてファイルを保存します `.pem`。

   例： `storagegrid_certificate.pem`

   - 証明書の内容をコピーして他の場所に貼り付けるには、 * 証明書の PEM をコピー * を選択します。

c. 証明書を Grid Manager に保存するには、 * Create * を選択します。

   更新された証明書が [クライアント] タブに表示されます。

証明書の生成

証明書のテキストを生成して他の場所に貼り付けます。

a. [* 証明書の生成 *] を選択します。

b. 証明書情報を指定します。

   - * Subject *（オプション）：証明書所有者のX.509サブジェクトまたは識別名（DN）。
   - 有効日：生成された証明書の有効日数（生成時から）。
   - キー使用拡張の追加：選択した場合（デフォルトおよび推奨）、キー使用および拡張キー使用拡張が生成された証明書に追加されます。

     これらの拡張機能は、証明書に含まれるキーの目的を定義します。

     証明書にこれらの拡張機能が含まれている場合に古いクライアントで接続の問題が発生する場合を除き、このチェックボックスをオンのままにします

c. [*Generate （生成）] を選択します

d. クライアント証明書の詳細 * を選択して、証明書メタデータと証明書 PEM を表示します。

   ダイアログを閉じると、証明書の秘密鍵を表示できなくなります。キーを安全な場所にコピーまたはダウンロードします。

   - 証明書の内容をコピーして他の場所に貼り付けるには、 * 証明書の PEM をコピー * を選択します。
   - 証明書ファイルを保存するには、 [証明書のダウンロード] を選択します。

証明書ファイルの名前とダウンロード先を指定します。拡張子を付けてファイルを保存します `.pem`。

例： `storagegrid_certificate.pem`

- 秘密鍵のコピー * を選択して、証明書の秘密鍵をコピーして別の場所に貼り付けます。
- 秘密鍵をファイルとして保存するには、 * 秘密鍵のダウンロード * を選択します。

  秘密鍵ファイルの名前とダウンロード先を指定します。

e. 証明書を Grid Manager に保存するには、 * Create * を選択します。

新しい証明書が [クライアント] タブに表示されます。

クライアント証明書をダウンロードまたはコピーします

クライアント証明書をダウンロードまたはコピーして、他の場所で使用することができます。

手順

1. [* configuration*>] > [* Security] * > [* Certificates*] を選択し、 [* Client*] タブを選択します。
2. コピーまたはダウンロードする証明書を選択します。
3. 証明書をダウンロードまたはコピーします。

証明書ファイルをダウンロードします
証明書をダウンロードします `.pem` ファイル。

a. [証明書のダウンロード] を選択します。
b. 証明書ファイルの名前とダウンロード先を指定します。拡張子を付けてファイルを保存します `.pem`。

例： `storagegrid_certificate.pem`

証明書をコピーします
証明書のテキストをコピーして別の場所に貼り付けてください。

a. [* 証明書 PEM のコピー *] を選択します。
b. コピーした証明書をテキストエディタに貼り付けます。
c. 拡張子を付けてテキストファイルを保存します `.pem`。

例： `storagegrid_certificate.pem`

クライアント証明書を削除します

管理者クライアント証明書が不要になった場合は削除できます。

手順

1. [* configuration*>] > [* Security] * > [* Certificates*] を選択し、 [* Client*] タブを選択します。
2. 削除する証明書を選択します。
3. 「 * 削除」を選択して確定します。

> 最大 10 個の証明書を削除するには、 [クライアント] タブで削除する各証明書を選択し、 [* アクション * > * 削除 *] を選択します。

証明書を削除したあと、その証明書を使用していたクライアントは、 StorageGRID Prometheus データベースにアクセスするための新しいクライアント証明書を指定する必要があります。

セキュリティを設定します

TLSおよび**SSH**ポリシーを管理します

TLSおよびSSHポリシーは、クライアントアプリケーションとのセキュアなTLS接続の確立および内部StorageGRID サービスへのセキュアなSSH接続に使用されるプロトコルと暗号を決定します。

セキュリティポリシーは、TLSとSSHによる移動中のデータの暗号化方法を制御します。一般に、お使いのシステムがCCに準拠している必要がある場合、または他の暗号を使用する必要がある場合を除き、最新の互換性（デフォルト）ポリシーを使用してください。

> 一部のStorageGRID サービスは、これらのポリシーで暗号を使用するように更新されていません。

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アクセス権限"。

セキュリティポリシーを選択します

手順

1. * configuration **>** Security **>** Security settings *を選択します。

   TLSおよびSSHポリシー*タブには、使用可能なポリシーが表示されます。ポリシーのタイルには、現在アクティブなポリシーが緑のチェックマークで表示されます。

2. タイルで使用可能なポリシーを確認します。

ポリシー	説明
最新の互換性（デフォルト）	特別な要件がないかぎり、強力な暗号化が必要な場合はデフォルトポリシーを使用します。このポリシーは、ほとんどのTLSおよびSSHクライアントと互換性があります。
レガシー互換性	古いクライアントの互換性オプションを追加する必要がある場合は、このポリシーを使用します。このポリシーにオプションを追加すると、最新の互換性ポリシーよりもセキュリティが低下する可能性があります。
Common Criteriaの略	情報セキュリティ国際評価基準の認定が必要な場合は、このポリシーを使用します。
FIPS strict	このポリシーは、Common Criteria認定が必要で、ロードバランサエンドポイント、Tenant Manager、およびGrid Managerへの外部クライアント接続にNetApp Cryptographic Security Module 3.0.0を使用する必要がある場合に使用します。このポリシーを使用するとパフォーマンスが低下することがあります。
カスタム	独自の暗号を適用する必要がある場合は、カスタムポリシーを作成します。

3. 各ポリシーの暗号、プロトコル、およびアルゴリズムの詳細を表示するには、*[詳細を表示]*を選択します。
4. 現在のポリシーを変更するには、*[ポリシーを使用]*を選択します。

   ポリシータイルの*現在のポリシー*の横に緑のチェックマークが表示されます。

カスタムセキュリティポリシーを作成します

独自の暗号を適用する必要がある場合は、カスタムポリシーを作成できます。

手順

1. 作成するカスタムポリシーに最も近いポリシーのタイルで、*[詳細を表示]*を選択します。
2. を選択し、[キャンセル]*を選択します。

3. [カスタムポリシー]タイルで、*[設定と使用]*を選択します。
4. コピーしたJSONを貼り付けて、必要な変更を行います。
5. [ポリシーを使用]*を選択します。

   [カスタムポリシー]タイルの*[現在のポリシー]*の横に緑のチェックマークが表示されます。

6. 必要に応じて、*[設定の編集]*を選択して、新しいカスタムポリシーをさらに変更します。

一時的にデフォルトのセキュリティポリシーに戻します

カスタムセキュリティポリシーを設定した場合、設定したTLSポリシーがと互換性がないと、Grid Managerにサインインできないことがあります "サーバ証明書を設定しました"。

一時的にデフォルトのセキュリティポリシーに戻すことができます。

手順

1. 管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@Admin_Node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

      rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

2. 次のコマンドを実行します。

   ```
   restore-default-cipher-configurations
   ```

3. Web ブラウザから、同じ管理ノード上の Grid Manager にアクセスする。
4. の手順に従います セキュリティポリシーを選択します をクリックして、ポリシーを再設定します。

ネットワークとオブジェクトのセキュリティを設定して、格納オブジェクトの暗号化、特定のS3およびSwift要求の防止、またはストレージノードへのクライアント接続でHTTPSではなくHTTPを使用できるようにすることができます。

格納オブジェクトの暗号化

格納オブジェクトの暗号化を使用すると、S3経由で取り込まれたすべてのオブジェクトデータを暗号化できます。デフォルトでは、格納オブジェクトは暗号化されませんが、AES‐128またはAES‐256暗号化アルゴリズムを使用してオブジェクトを暗号化することができます。この設定を有効にすると、新たに取り込まれたすべてのオブジェクトが暗号化されますが、既存の格納オブジェクトに対する変更はありません。暗号化を無効にすると、現在暗号化されているオブジェクトは暗号化されたままですが、新しく取り込まれたオブジェクトは暗号化されません

格納オブジェクトの暗号化設定は、バケットレベルまたはオブジェクトレベルの暗号化で暗号化されていないS3オブジェクトにのみ適用されます。

StorageGRID 暗号化方式の詳細については、を参照してください "StorageGRID の暗号化方式を確認します"。

クライアントの変更を防止します

[Prevent client modification]は、システム全体の設定です。[Prevent client modification *]オプションを選択すると、次の要求が拒否されます。

S3 REST API

- バケットの削除要求
- 既存オブジェクトのデータ、ユーザ定義メタデータ、または S3 オブジェクトのタグを変更するすべての要求

Swift REST API

- コンテナの削除要求
- 既存のオブジェクトを変更する要求。たとえば、 Put Overwrite 、 Delete 、 Metadata Update などの処理が拒否されます。

ストレージノード接続用の**HTTP**を有効にします

デフォルトでは、クライアントアプリケーションは、ストレージノードへの直接接続にHTTPSネットワークプロトコルを使用します。非本番環境のグリッドのテストなどの目的で、これらの接続に対して HTTP を有効にすることもできます。

ストレージノード接続にHTTPを使用するのは、S3およびSwiftクライアントからストレージノードへのHTTP接続を直接確立する必要がある場合のみです。HTTPS接続のみを使用するクライアントや、ロードバランササービスに接続するクライアント（を使用できるため）には、このオプションを使用する必要はありません "各ロードバランサエンドポイントを設定します" HTTPまたはHTTPSを使用する場合）。

を参照してください "Summary ：クライアント接続の IP アドレスとポート" を参照してください。HTTPまたはHTTPSを使用してストレージノードに接続する際にS3およびSwiftクライアントが使用するポートを確認できます。

オプションを選択します

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"。
- Root Access 権限が割り当てられている。

手順

1. * configuration > Security > Security settings *を選択します。
2. [ネットワークとオブジェクト]タブを選択します。
3. 格納オブジェクトを暗号化しない場合は*なし*（デフォルト）設定を使用し、格納オブジェクトを暗号化する場合は* AES-128 または AES-256 *を選択します。
4. 必要に応じて、S3およびSwiftクライアントが特定の要求を実行しないようにする場合は、*[Prevent client modification]*を選択します。

   この設定を変更すると、新しい設定が適用されるまで約 1 分かかります。設定した値は、パフォーマンスと拡張用にキャッシュされます。

5. 必要に応じて、クライアントがストレージノードに直接接続し、HTTP接続を使用する場合は、*[ストレージノード接続用のHTTPを有効にする]*を選択します。

   要求が暗号化されずに送信されるため、本番環境のグリッドで HTTP を有効にする場合は注意してください。

6. [保存（ Save ）] を選択します。

ブラウザの非アクティブタイムアウトを変更します

Grid Manager ユーザと Tenant Manager ユーザが一定期間非アクティブになった場合にサインアウトするかどうかを制御できます。

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"。
- Root Access 権限が割り当てられている。

このタスクについて

ブラウザの非アクティブ時のタイムアウトのデフォルトは15分です。ユーザのブラウザがこの時間アクティブでない場合、ユーザはサインアウトされます。

必要に応じて、*非アクティブなユーザーをあとでサインアウト*オプションを設定することで、タイムアウト時間を増減できます。

ブラウザの非アクティブ時のタイムアウトは、次の方法でも制御されます。

- システムセキュリティ用の、個別の設定不可能な StorageGRID タイマー。デフォルトでは、各ユーザの認証トークンはユーザがサインインしてから 16 時間後に期限切れになります。ユーザの認証が期限切れになると、ブラウザの非アクティブタイムアウトが無効になっている場合やブラウザのタイムアウト値に達していない場合でも、そのユーザは自動的にサインアウトされます。トークンを更新するには、再度サインインする必要があります。

- アイデンティティプロバイダのタイムアウト設定（StorageGRID でシングルサインオン（SSO）が有効になっている場合）。

  SSOが有効になっていて、ユーザのブラウザがタイムアウトした場合、StorageGRID に再度アクセスするには、SSOクレデンシャルを再入力する必要があります。を参照してください "シングルサインオンを設定します"。

手順

1. * configuration > Security > Security settings *を選択します。
2. [Browser inactivity timeout]*タブを選択します。
3. [Sign out inactive users after *]フィールドに、ブラウザのタイムアウト時間を60秒から7日の間で指定します。

   ブラウザのタイムアウト時間は、秒、分、時間、または日数で指定できます。

4. [保存（ Save ）] を選択します。ブラウザが一定期間非アクティブになっている場合、ユーザはGrid ManagerまたはTenant Managerからサインアウトされます。

   新しい設定は、現在サインインしているユーザには影響しません。新しいタイムアウト設定を有効にするには、ユーザが再度サインインするか、ブラウザを更新する必要があります。

キー管理サーバを設定

キー管理サーバの設定：概要

1 つ以上の外部キー管理サーバ（ KMS ）を設定して、特別に設定したアプライアンスノード上のデータを保護することができます。

キー管理サーバ（ **KMS** ）とは何ですか？

キー管理サーバ（ KMS ）は、関連する StorageGRID サイトの StorageGRID アプライアンスノードに Key Management Interoperability Protocol （ KMIP ）を使用して暗号化キーを提供する外部のサードパーティシステムです。

インストール時にノード暗号化 * 設定が有効になっている StorageGRID アプライアンスノードのノード暗号化キーを管理するには、 1 つ以上のキー管理サーバを使用します。これらのアプライアンスノードでキー管理サーバを使用すると、アプライアンスをデータセンターから削除した場合でも、データを保護できます。アプライアンスボリュームが暗号化されると、ノードがKMSと通信できないかぎり、アプライアンスのデータにアクセスすることはできません。

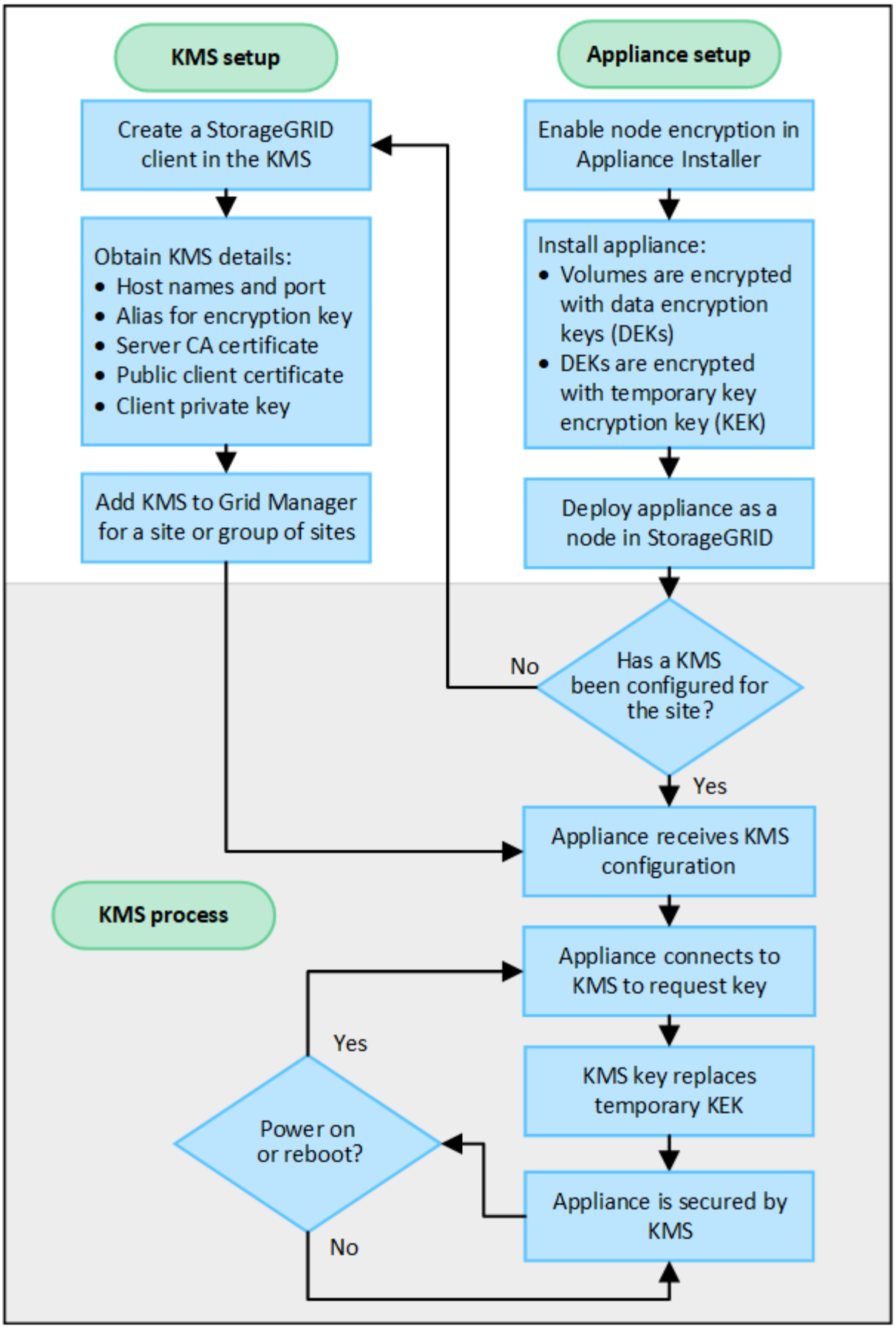
> StorageGRID では、アプライアンスノードの暗号化と復号化に使用する外部キーは作成も管理もされません。外部キー管理サーバを使用して StorageGRID データを保護する場合は、そのサーバの設定方法を理解し、暗号化キーの管理方法を理解しておく必要があります。キー管理タスクの実行については、この手順では説明していません。サポートが必要な場合は、キー管理サーバのドキュメントを参照するか、テクニカルサポートにお問い合わせください。

KMS とアプライアンスの設定の概要

キー管理サーバ（ KMS ）を使用してアプライアンスノード上の StorageGRID データを

保護する前に、 1 つ以上の KMS サーバを設定してアプライアンスノードのノード暗号化を有効にするという 2 つの設定タスクを完了しておく必要があります。これらの 2 つの設定タスクが完了すると、キー管理プロセスが自動的に実行されます。

フローチャートは、 KMS を使用してアプライアンスノード上の StorageGRID データを保護する手順の概要を示しています。



フローチャートには、 KMS のセットアップとアプライアンスのセットアップが並行して行われていることが

示されています。ただし、要件に基づいて、新しいアプライアンスノードのノード暗号化を有効にする前後にキー管理サーバをセットアップできます。

キー管理サーバ（ KMS ）のセットアップ

キー管理サーバのセットアップには、主に次の手順が含まれます。

ステップ	を参照してください
KMS ソフトウェアにアクセスし、各 KMS または KMS クラスタに StorageGRID 用のクライアントを追加します。	"KMS でクライアントとして StorageGRID を設定します"
KMS で StorageGRID クライアントの必要な情報を入手します。	"KMS でクライアントとして StorageGRID を設定します"
Grid Manager に KMS を追加して 1 つのサイトまたはデフォルトのサイトグループに割り当て、必要な証明書をアップロードして、 KMS の設定を保存します。	"キー管理サーバ（ KMS ）を追加する"

アプライアンスをセットアップします

KMS を使用するためにアプライアンスノードをセットアップするには、次の手順に従います。

1. アプライアンスのハードウェア構成フェーズでは、 StorageGRID アプライアンスインストーラを使用してアプライアンスのノード暗号化 * 設定を有効にします。

   > アプライアンスをグリッドに追加したあとに* Node Encryption *設定を有効にすることはできません。また、ノード暗号化が有効になっていないアプライアンスでは外部キー管理を使用できません。

2. StorageGRID アプライアンスインストーラを実行します。インストール時に、次のように各アプライアンスボリュームにランダムデータ暗号化キー（ DEK ）が割り当てられます。
   - DEK は、各ボリュームのデータの暗号化に使用されます。これらのキーは、アプライアンスOSのLinux Unified Key Setup（LUKS）ディスク暗号化を使用して生成され、変更することはできません。
   - 各 DEK は、 KEK （ Master Key Encryption Key ）によって暗号化されます。最初の KEK は、アプライアンスが KMS に接続できるまで DEK を暗号化する一時キーです。
3. StorageGRID にアプライアンスノードを追加します。

を参照してください "ノード暗号化を有効にします" を参照してください。

キー管理の暗号化プロセス（自動的に実行）

キー管理の暗号化には、次の高度な手順が含まれています。これらの手順は自動的に実行されます。

1. ノードの暗号化が有効になっているアプライアンスをグリッドにインストールすると、 StorageGRID は、新しいノードを含むサイトに KMS 設定が存在するかどうかを確認します。

- KMS がすでにサイト用に設定されている場合、アプライアンスは KMS の設定を受信します。
- KMS がサイト用にまだ設定されていない場合は、サイトに KMS を設定し、アプライアンスが KMS の設定を受信するまで、アプライアンス上のデータは一時的な KEK によって暗号化されたままになります。

2. アプライアンスは KMS 設定を使用して KMS に接続し、暗号化キーを要求します。
3. KMS は暗号化キーをアプライアンスに送信します。KMS の新しいキーは一時的な KEK に代わるものであり、アプライアンスボリュームの DEK の暗号化と復号化に使用されるようになりました。

> 暗号化されたアプライアンスノードから設定された KMS に接続する前に存在するデータは、すべて一時キーで暗号化されます。ただし、一時キーを KMS 暗号化キーに置き換えるまでは、アプライアンスボリュームをデータセンターから削除できないようにする必要があります。

4. アプライアンスの電源をオンにするか再接続すると、 KMS に接続してキーを要求します。揮発性メモリに保存されているキーは、電源の喪失や再起動に耐えられません。

キー管理サーバを使用する際の考慮事項と要件

外部キー管理サーバ（ KMS ）を設定する前に、考慮事項と要件を確認しておく必要があります。

KMIP の要件

StorageGRID は KMIP バージョン 1.4 をサポートしています。

"Key Management Interoperability Protocol （キー管理相互運用性プロトコル）仕様バージョン 1.4"

アプライアンスノードと設定された KMS の間の通信には、セキュアな TLS 接続が使用されます。StorageGRID では、 KMIP で次の TLS v1.2 暗号をサポートしています。

- TLS_ECDHE_RSA_with _AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_With _AES_256_GCM_SHA384

ノード暗号化を使用する各アプライアンスノードに、サイト用に設定した KMS または KMS クラスタへのネットワークアクセスがあることを確認してください。

ネットワークのファイアウォールの設定で、各アプライアンスノードが Key Management Interoperability Protocol （ KMIP ）の通信に使用するポートを介して通信できるようにする必要があります。デフォルトの KMIP ポートは 5696 です。

サポートされているアプライアンスはどれですか。

キー管理サーバ（ KMS ）を使用して、「ノード暗号化 * 」が有効になっているグリッド内の StorageGRID アプライアンスの暗号化キーを管理できます。この設定は、 StorageGRID アプライアンスインストーラを使用してアプライアンスをインストールするハードウェア構成の段階でのみ有効にできます。

> アプライアンスをグリッドに追加したあとにノード暗号化を有効にすることはできません。また、ノード暗号化が有効になっていないアプライアンスでは、外部キー管理を使用できません。

StorageGRID アプライアンスおよびアプライアンスノードに対して設定したKMSを使用できます。

次のようなソフトウェアベース（アプライアンス以外）のノードでは、設定されたKMSを使用できません。

- 仮想マシン（ VM ）として導入されたノード
- Linux ホストのコンテナエンジン内に導入されたノード

これらの他のプラットフォームに導入されたノードでは、データストアまたはディスクレベルで StorageGRID 外部の暗号化を使用できます。

キー管理サーバを設定する必要があるのはいつですか？

新規インストールの場合は、テナントを作成する前に Grid Manager で 1 つ以上のキー管理サーバをセットアップするのが一般的です。この順序により、ノード上に格納されるオブジェクトデータよりも先にノードが保護されます。

Grid Manager では、アプライアンスノードのインストール前またはインストール後にキー管理サーバを設定できます。

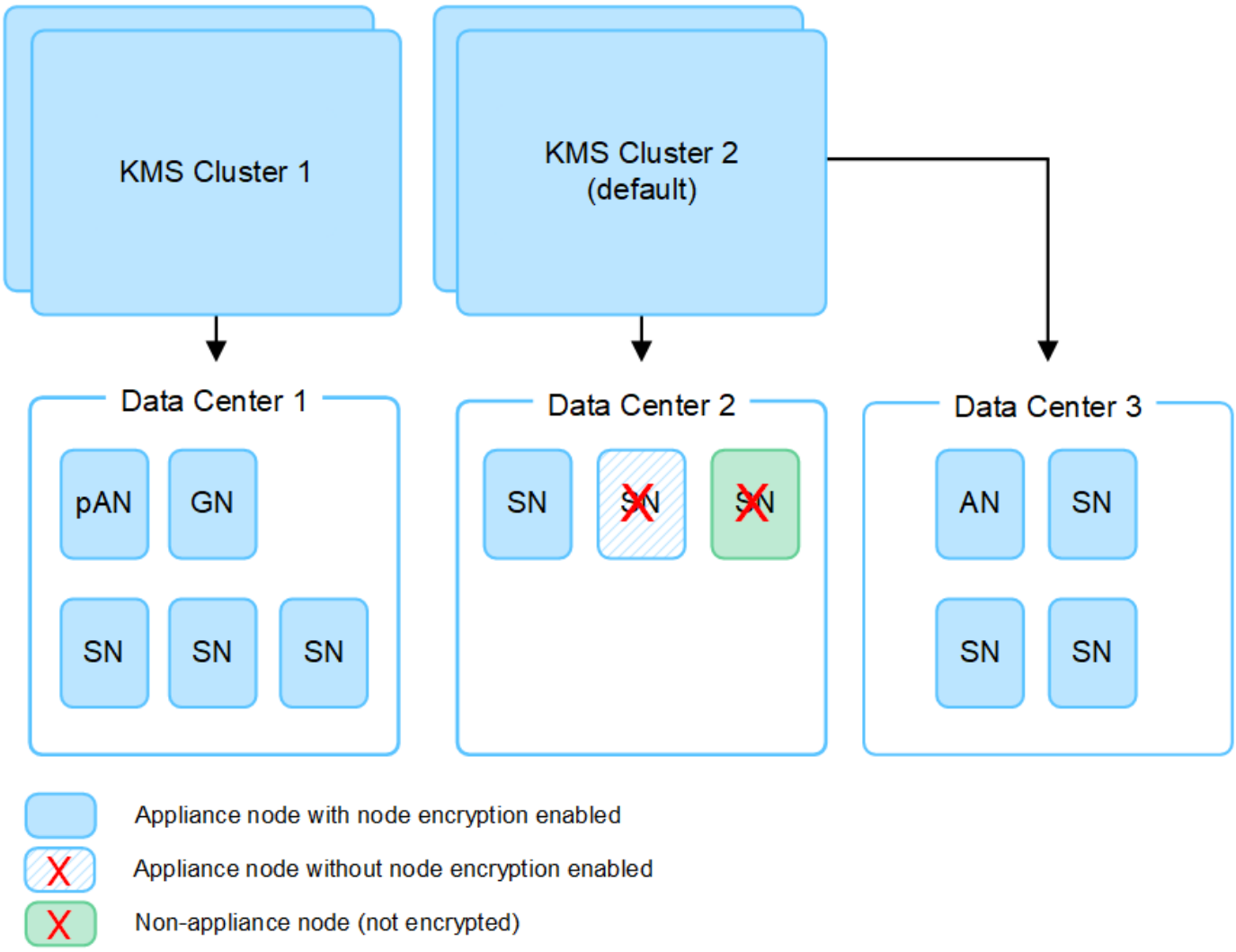
必要なキー管理サーバの数

1 つ以上の外部キー管理サーバを設定して、 StorageGRID システム内のアプライアンスノードに暗号化キーを提供できます。各 KMS は、 1 つのサイトまたはサイトグループにある StorageGRID アプライアンスノードに単一の暗号化キーを提供します。

StorageGRID は KMS クラスタの使用をサポートしています。各 KMS クラスタには、設定と暗号化キーを共有するレプリケートされた複数のキー管理サーバが含まれます。高可用性構成のフェイルオーバー機能が向上するため、 KMS クラスタをキー管理に使用することを推奨します。

たとえば、 StorageGRID システムに 3 つのデータセンターサイトがあるとします。1 つの KMS クラスタを設定して、データセンター 1 のすべてのアプライアンスノードともう 1 つの KMS クラスタのキーを取得し、他のすべてのサイトにあるすべてのアプライアンスノードのキーを取得することができます。2 つ目の KMS クラスタを追加すると、データセンター 2 とデータセンター 3 にデフォルトの KMS を設定できます。

非アプライアンスノード、またはインストール時に* Node Encryption *設定が有効になっていないアプライアンスノードには、KMSを使用できないことに注意してください。



キーをローテーションするとどうなりますか。

セキュリティのベストプラクティスとして、設定された各 KMS で使用される暗号化キーを定期的にローテーションすることを推奨します。

暗号化キーをローテーションするときは、 KMS ソフトウェアを使用して、最後に使用したバージョンのキーを同じキーの新しいバージョンにローテーションします。完全に別のキーに回転しないでください。

> キーのローテーションは、 Grid Manager 内の KMS のキー名（エイリアス）を変更しては実行しないでください。代わりに、 KMS ソフトウェアのキーバージョンを更新してキーをローテーションしてください。以前のキーに使用したものと同じキーエイリアスを新しいキーに使用します。設定されている KMS のキーエイリアスを変更すると、 StorageGRID がデータを復号化できなくなる可能性があります。

新しいキーバージョンが利用可能になった場合：

- このサービスは、 KMS に関連付けられているサイトにある暗号化されたアプライアンスノードに自動的に配信されます。キーが回転した後 1 時間以内に分配が行われる必要があります。
- 新しいキーバージョンが配布されたときに暗号化アプライアンスノードがオフラインになっている場合、ノードはリブート後すぐに新しいキーを受け取ります。

- 何らかの理由で新しいバージョンのキーを使用してアプライアンスボリュームを暗号化できない場合は、アプライアンスノードに対して* kms encryption key rotation failed *アラートがトリガーされます。このアラートの解決方法については、テクニカルサポートへの問い合わせが必要になることがあります。

アプライアンスノードは暗号化したあとに再利用できますか。

暗号化されたアプライアンスを別の StorageGRID システムにインストールする必要がある場合は、先にグリッドノードの運用を停止して、オブジェクトデータを別のノードに移動しておく必要があります。その後、StorageGRID アプライアンスインストーラを使用してを実行できます "KMS構成をクリアします"。KMS の設定をクリアすると、「ノード暗号化 * 」設定が無効になり、アプライアンスノードと StorageGRID サイトの KMS 設定の間の関連付けが解除されます。

KMS 暗号化キーにアクセスできないため、アプライアンスに残っているデータにはアクセスできなくなり、永続的にロックされます。

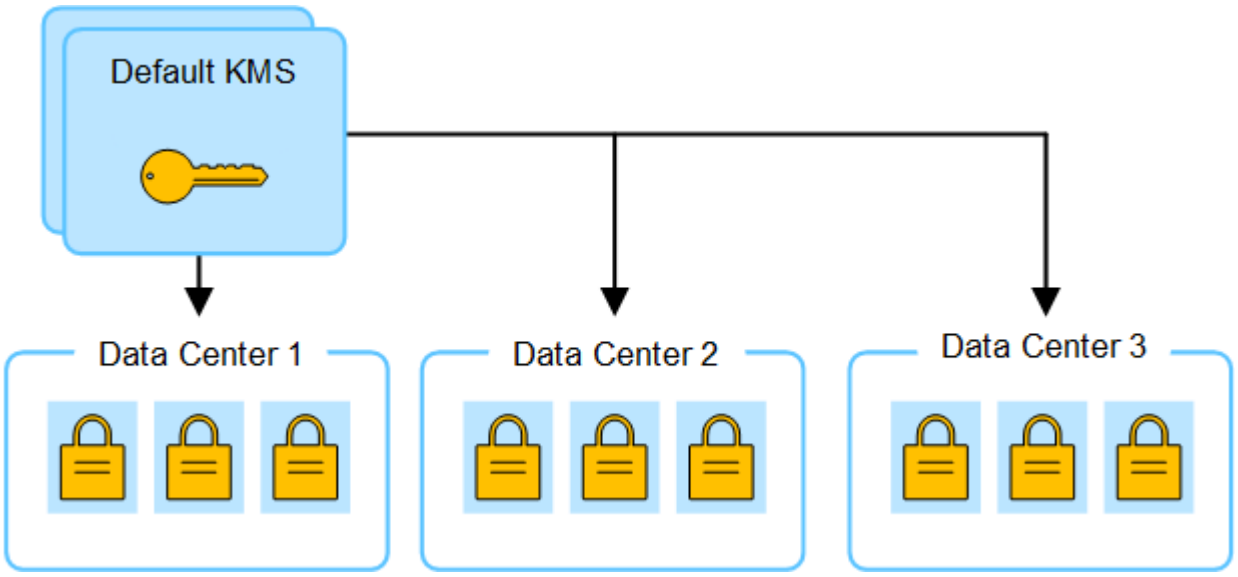
サイトの **KMS** を変更する際の考慮事項

各キー管理サーバ（ KMS ）または KMS クラスタは、 1 つのサイトまたはサイトグループにあるすべてのアプライアンスノードに暗号化キーを提供します。サイトで使用する KMS を変更する必要がある場合は、暗号化キーを KMS から別の KMS にコピーする必要があります。

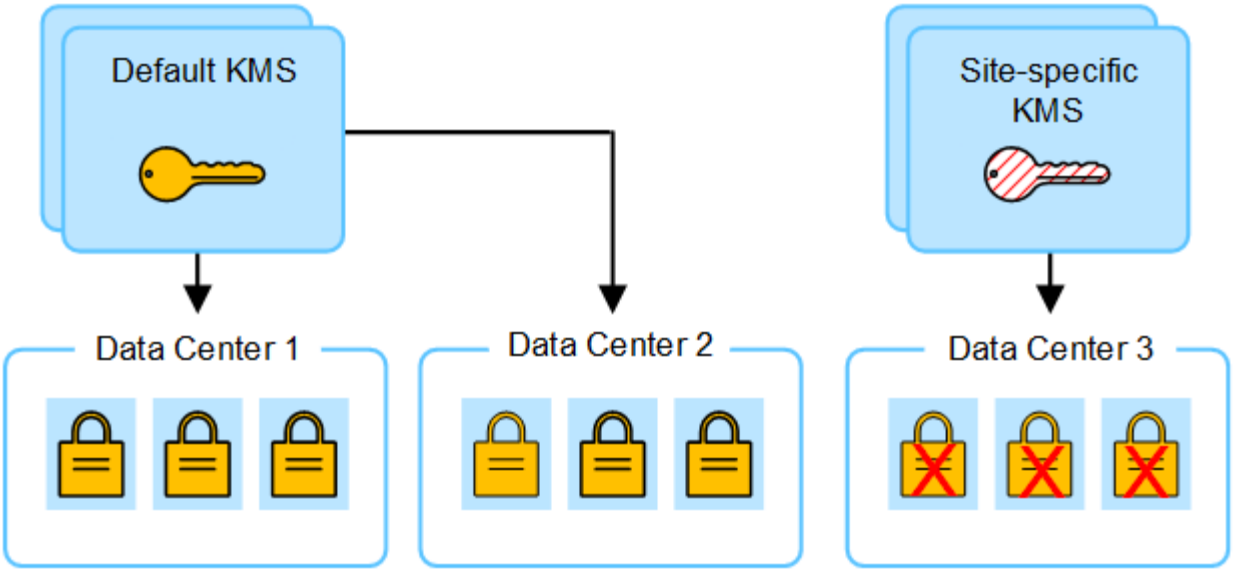
サイトで使用されている KMS を変更する場合は、そのサイトで以前に暗号化したアプライアンスノードを新しい KMS に格納されているキーを使用して復号化できることを確認する必要があります。場合によっては、暗号化キーの現在のバージョンを元の KMS から新しい KMS にコピーする必要があります。サイトで暗号化されたアプライアンスノードを復号化するために、 KMS に正しいキーがあることを確認する必要があります。

例：

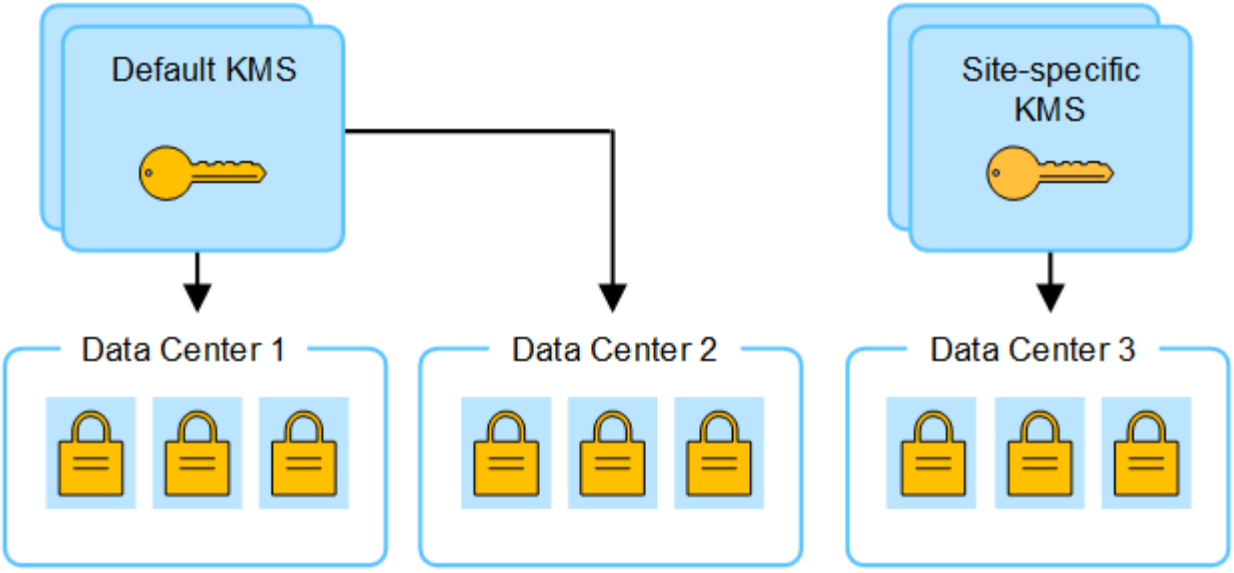
1. 最初に、専用のKMSを持たないすべてのサイトを環境 するデフォルトKMSを構成します。
2. KMS を保存すると、「 Node Encryption * 」設定が有効になっているすべてのアプライアンスノードが KMS に接続して暗号化キーを要求します。このキーは、すべてのサイトのアプライアンスノードの暗号化に使用されます。同じキーを使用して、これらのアプライアンスを復号化する必要もあります。



3. 1 つのサイト（図のデータセンター 3 ）にサイト固有の KMS を追加することにしました。ただし、アプライアンスノードはすでに暗号化されているため、サイト固有の KMS の設定を保存しようとすると検証エラーが発生します。このエラーは、サイト固有の KMS に、そのサイトでノードを復号化するための正しいキーがないことが原因で発生します。



4. 問題 に対応するには、現在のバージョンの暗号化キーをデフォルトの KMS から新しい KMS にコピーします。（技術的には、元のキーを同じエイリアスを持つ新しいキーにコピーします。元のキーが新しいキーの前のバージョンになります）。 サイト固有の KMS に、データセンター 3 でアプライアンスノードを復号化するための正しいキーが付与されるようになり、 StorageGRID に保存できるようになりました。



サイトに使用する **KMS** を変更するユースケース

次の表に、サイトの KMS を変更する一般的なケースに必要な手順をまとめます。

サイトの **KMS** を変更するユースケース	必要な手順
サイト固有の KMS エントリが 1 つ以上あり、それらのエントリの 1 つをデフォルトの KMS として使用する必要があります。	サイト固有の KMS を編集します。[* キー管理対象 *] フィールドで、別の KMS （デフォルト KMS ）で管理されていないサイト * を選択します。サイト固有の KMS がデフォルトの KMS として使用されるようになります。それは専用のKMSを持っていないすべてのサイトに適用されます。 "キー管理サーバ（ KMS ）を編集する"
デフォルトの KMS を使用して、拡張時に新しいサイトを追加する必要があります。新しいサイトにはデフォルトのKMSを使用しないでください。	1. 新しいサイトにあるアプライアンスノードがデフォルトの KMS によって暗号化済みの場合は、 KMS ソフトウェアを使用して、現在のバージョンの暗号化キーをデフォルトの KMS から新しい KMS にコピーします。 2. Grid Manager を使用して新しい KMS を追加し、サイトを選択します。 "キー管理サーバ（ KMS ）を追加する"
サイトの KMS で別のサーバを使用するとします。	1. サイトのアプライアンスノードが既存の KMS によって暗号化済みの場合は、 KMS ソフトウェアを使用して、既存の KMS から新しい KMS に暗号化キーの現在のバージョンをコピーします。 2. Grid Manager を使用して既存の KMS 設定を編集し、新しいホスト名または IP アドレスを入力します。 "キー管理サーバ（ KMS ）を追加する"

KMS でクライアントとして **StorageGRID** を設定します

KMS を StorageGRID に追加する前に、各外部キー管理サーバまたは KMS クラスタのクライアントとして StorageGRID を設定する必要があります。

このタスクについて

これらの手順はタレスCipherTrust Managerに適用されます。サポートされているバージョンの一覧については、を参照してください "ネットアップの Interoperability Matrix Tool （ IMT ）"。

手順

1. KMS ソフトウェアから、使用する KMS または KMS クラスタごとに StorageGRID クライアントを作成します。

   各 KMS は、 1 つのサイトまたはサイトグループにある StorageGRID アプライアンスノードの単一の暗号化キーを管理します。

2. KMS ソフトウェアから、 KMS または KMS クラスタごとに AES 暗号化キーを作成します。

   暗号化キーは2、048ビット以上で、エクスポート可能である必要があります。

3. KMS または KMS クラスタごとに次の情報を記録します。

この情報は、 KMS を StorageGRID に追加するときに必要になります。

- 各サーバのホスト名または IP アドレス。
- KMS で使用される KMIP ポート。
- KMS 内の暗号化キーのキーエイリアス。

> 暗号化キーは KMS にすでに存在している必要があります。StorageGRID は KMS キーを作成または管理しません。

4. KMS または KMS クラスタごとに、認証局（ CA ）が署名したサーバ証明書または PEM でエンコードされた各 CA 証明書ファイルを含む証明書バンドルを、証明書チェーンの順序で連結して取得します。

   サーバ証明書を使用すると、外部 KMS は StorageGRID に対して自身を認証できます。

   - 証明書では、 Privacy Enhanced Mail （ PEM ） Base-64 エンコード X.509 形式を使用する必要があります。
   - 各サーバ証明書の Subject Alternative Name （ SAN ）フィールドには、 StorageGRID が接続する完全修飾ドメイン名（ FQDN ）または IP アドレスを含める必要があります。

     > StorageGRID で KMS を設定する場合は、「 * Hostname * 」フィールドに同じ FQDN または IP アドレスを入力する必要があります。

   - サーバ証明書は、 KMS の KMIP インターフェイスで使用されている証明書と一致する必要があります。通常はポート 5696 が使用されます。

5. 外部 KMS によって StorageGRID に発行されたパブリッククライアント証明書とクライアント証明書の秘密鍵を取得します。

   クライアント証明書は、 StorageGRID が KMS に対して自身を認証することを許可します。

キー管理サーバ（ **KMS** ）を追加する

StorageGRID キー管理サーバウィザードを使用して、各 KMS または KMS クラスタを追加します。

作業を開始する前に

- を確認しておきます "キー管理サーバを使用する際の考慮事項と要件"。
- これで完了です "KMS でクライアントとして StorageGRID を設定"をクリックし、 KMS または KMS クラスタごとに必要な情報を確認しておきます。
- 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"。
- Root アクセス権限が割り当てられている。

このタスクについて

可能環境 であれば、サイト固有のキー管理サーバを設定してから、別の KMS で管理されていないデフォルトの KMS を設定してください。最初にデフォルトの KMS を作成すると、グリッド内のノードで暗号化されたすべてのアプライアンスがデフォルトの KMS で暗号化されます。サイト固有の KMS をあとで作成するには、まず、暗号化キーの現在のバージョンをデフォルトの KMS から新しい KMS にコピーする必要がありま

す。を参照してください "サイトの KMS を変更する際の考慮事項" を参照してください。

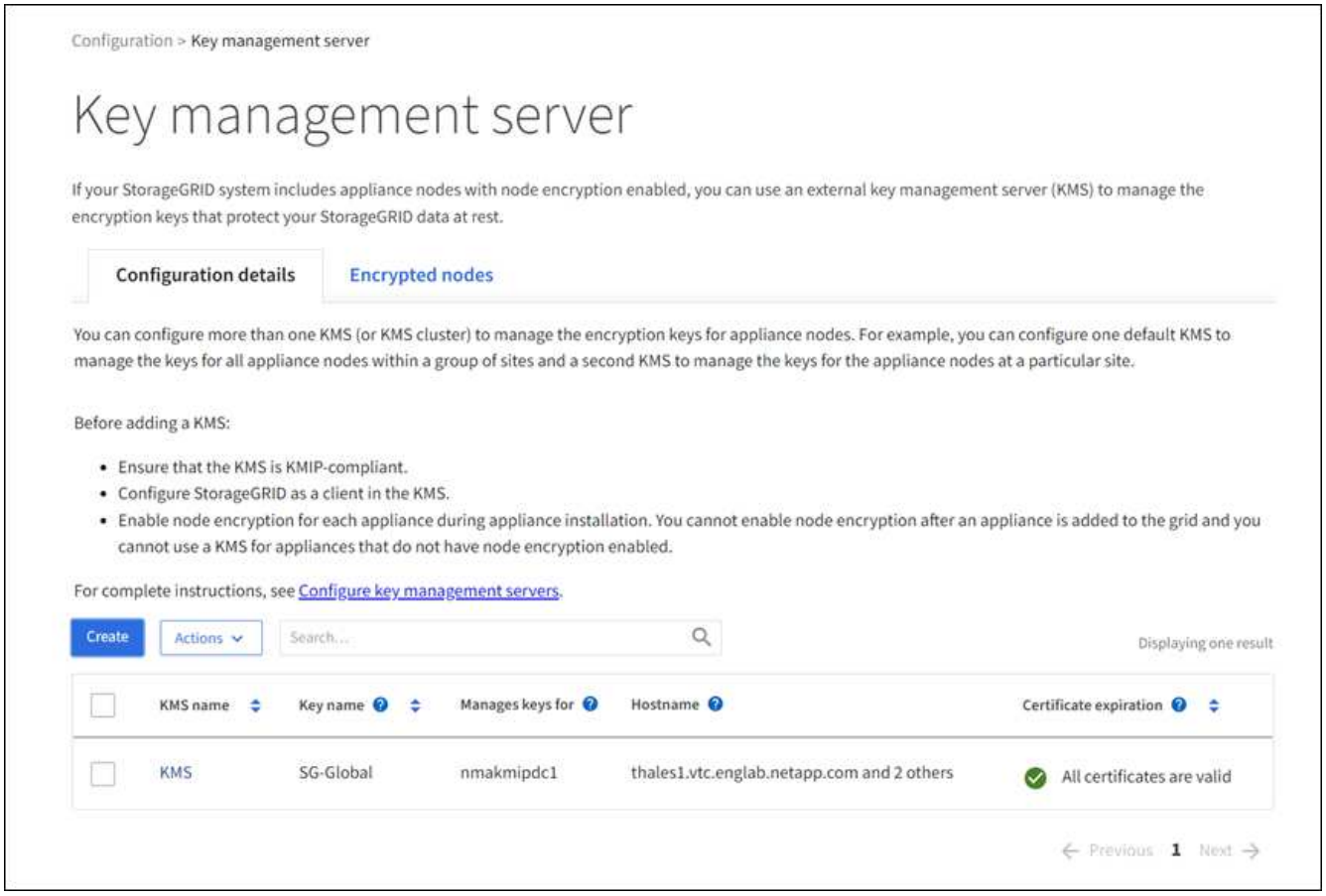
ステップ**1**：**KMS**の詳細

キー管理サーバの追加ウィザードの手順1（KMSの詳細）で、KMSまたはKMSクラスタの詳細を指定します。

手順

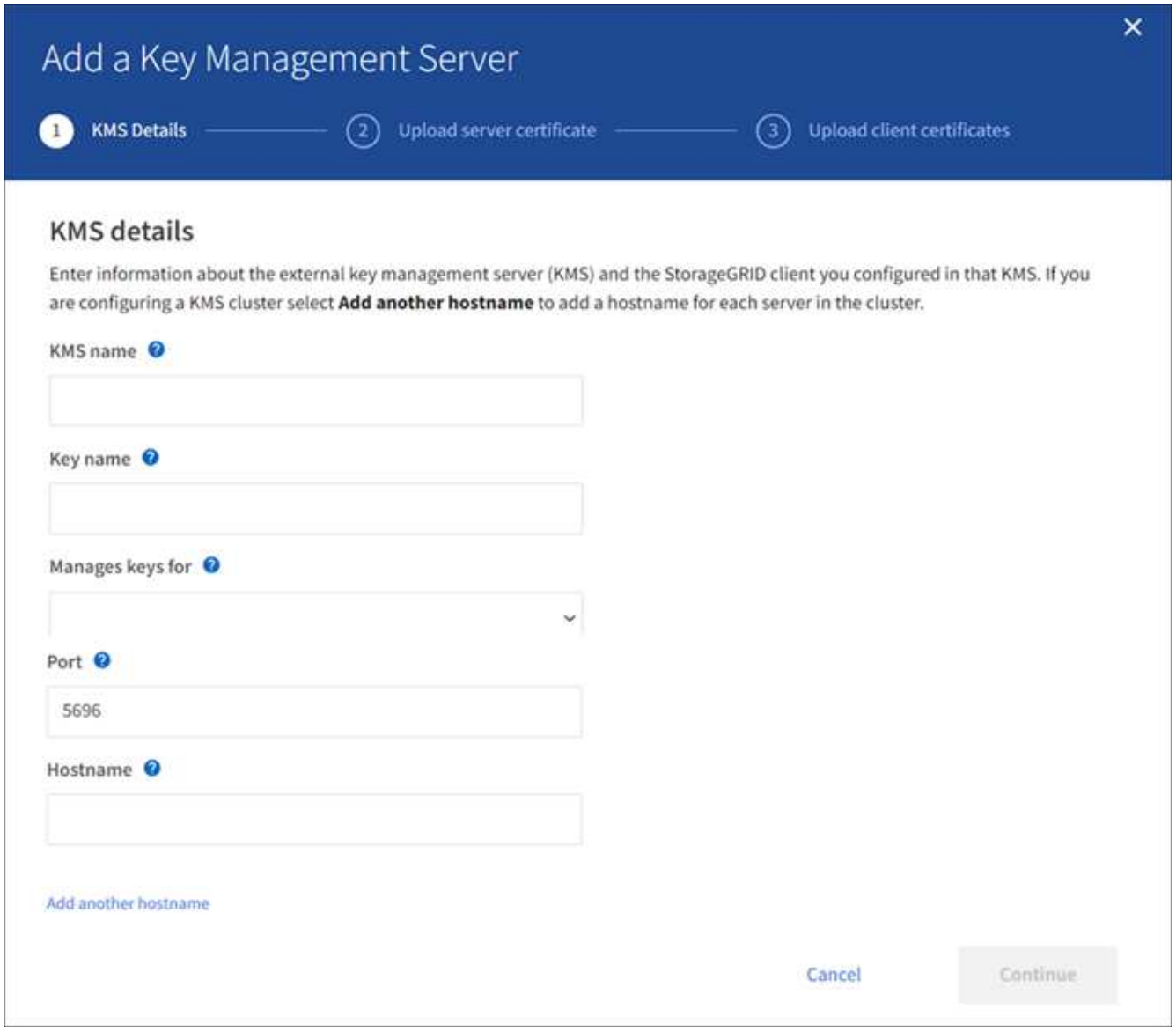
1. 設定 * > * セキュリティ * > * キー管理サーバ * を選択します。

   [設定の詳細]タブが選択された状態で、[キー管理サーバ]ページが表示されます。



2. 「 * Create * 」を選択します。

   キー管理サーバの追加ウィザードの手順1（KMSの詳細）が表示されます。



3. KMS および設定した StorageGRID クライアントの情報を KMS で入力します。

フィールド	説明
KMS名	この KMS を特定するのに役立つわかりやすい名前。1~64 文字で指定します。
キー名	KMS 内の StorageGRID クライアントの正確なキーエイリアス。1~255 文字で指定する必要があります。

フィールド	説明
のキーを管理します	この KMS に関連する StorageGRID サイトを参照してください。可能であれば、サイト固有のキー管理サーバを設定してから、環境 で他の KMS で管理されていないすべてのサイトをデフォルトの KMS で設定する必要があります。 • 特定のサイトのアプライアンスノードの暗号化キーをこの KMS で管理する場合は、サイトを選択します。 • 専用のKMSを持たないサイトや、その後の拡張で追加するサイトに適用されるデフォルトKMSを設定するには、*[別のKMSで管理されていないサイト(デフォルトKMS)]*を選択します。 ◦ 注： * 以前にデフォルト KMS で暗号化されていたサイトを選択しても、新しい KMS に元の暗号化キーの現在のバージョンを提供しなかった場合、 KMS の設定を保存すると、検証エラーが発生します。
ポート	KMS サーバが Key Management Interoperability Protocol （ KMIP ）の通信に使用するポート。デフォルトでは、 KMIP 標準ポートである 5696 が使用されます。
ホスト名	KMS の完全修飾ドメイン名または IP アドレス。 *注：*サーバ証明書のSubject Alternative Name（SAN）フィールドには、ここに入力するFQDNまたはIPアドレスが含まれている必要があります。そうしないと、 StorageGRID は KMS クラスタ内のすべてのサーバに接続できなくなります。

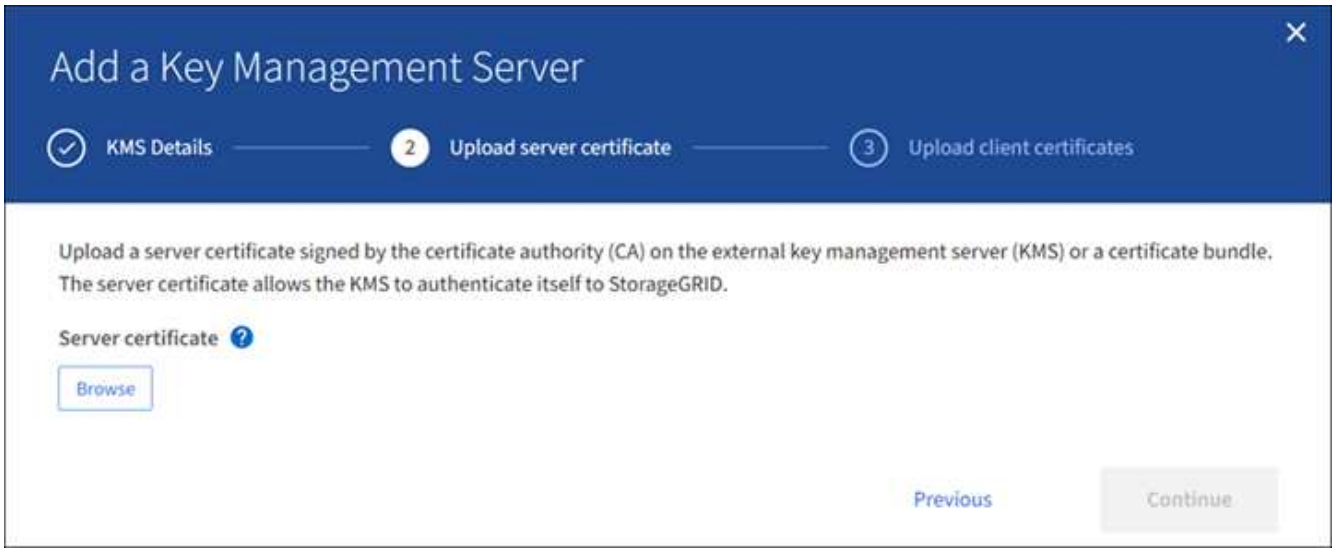
4. KMSクラスタを構成する場合は、*[別のホスト名を追加]*を選択して、クラスタ内の各サーバのホスト名を追加します。
5. 「 * Continue * 」を選択します。

手順**2:**サーバー証明書をアップロードします

キー管理サーバの追加ウィザードの手順2（サーバ証明書をアップロード）で、KMSのサーバ証明書（または証明書バンドル）をアップロードします。サーバ証明書を使用すると、外部 KMS は StorageGRID に対して自身を認証できます。

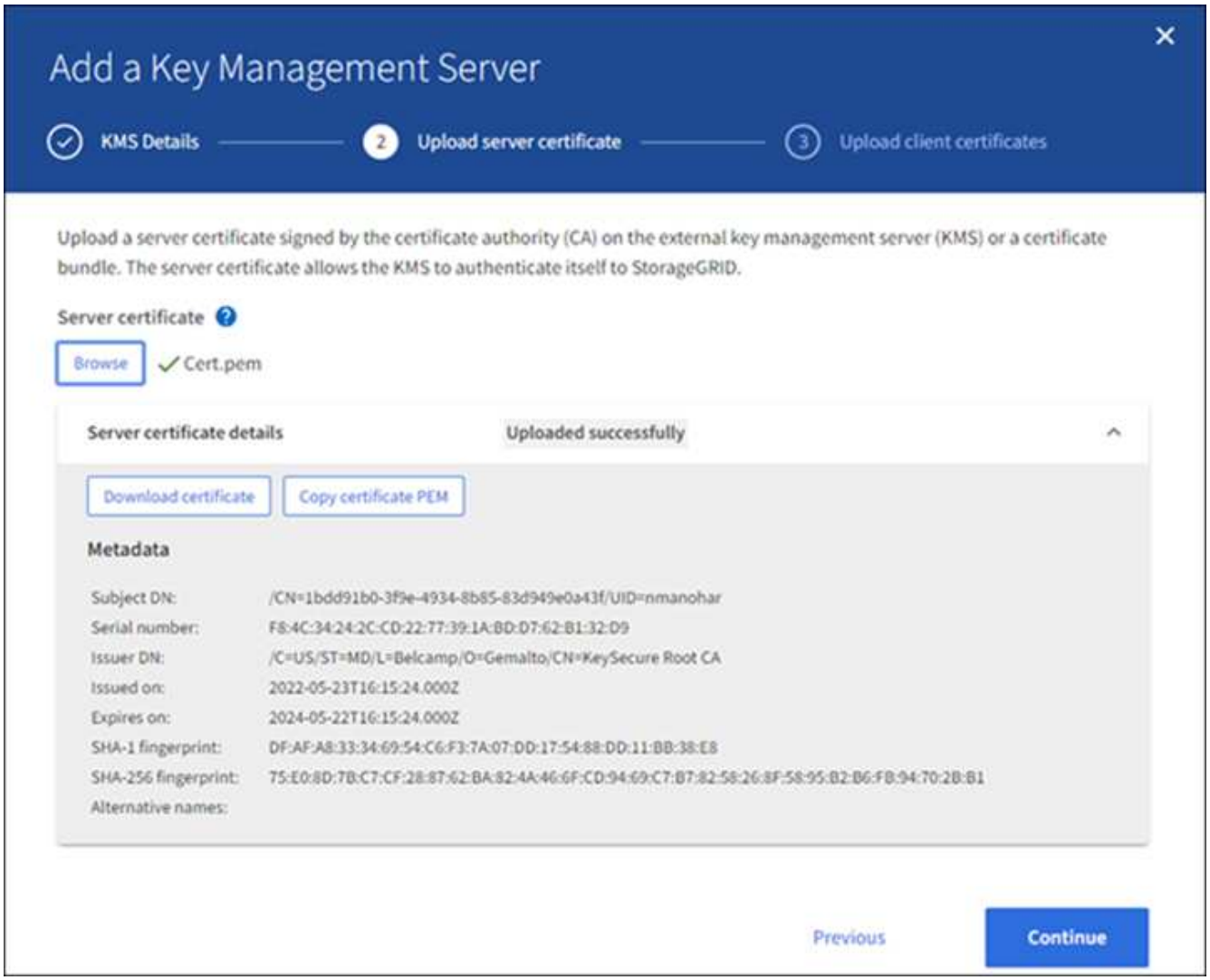
手順

1. [手順2（サーバ証明書のアップロード）]*で、保存されているサーバ証明書または証明書バンドルの場所を参照します。



2. 証明書ファイルをアップロードします。

   サーバ証明書のメタデータが表示されます。



証明書バンドルをアップロードした場合は、各証明書のメタデータが独自のタブに表示されます。

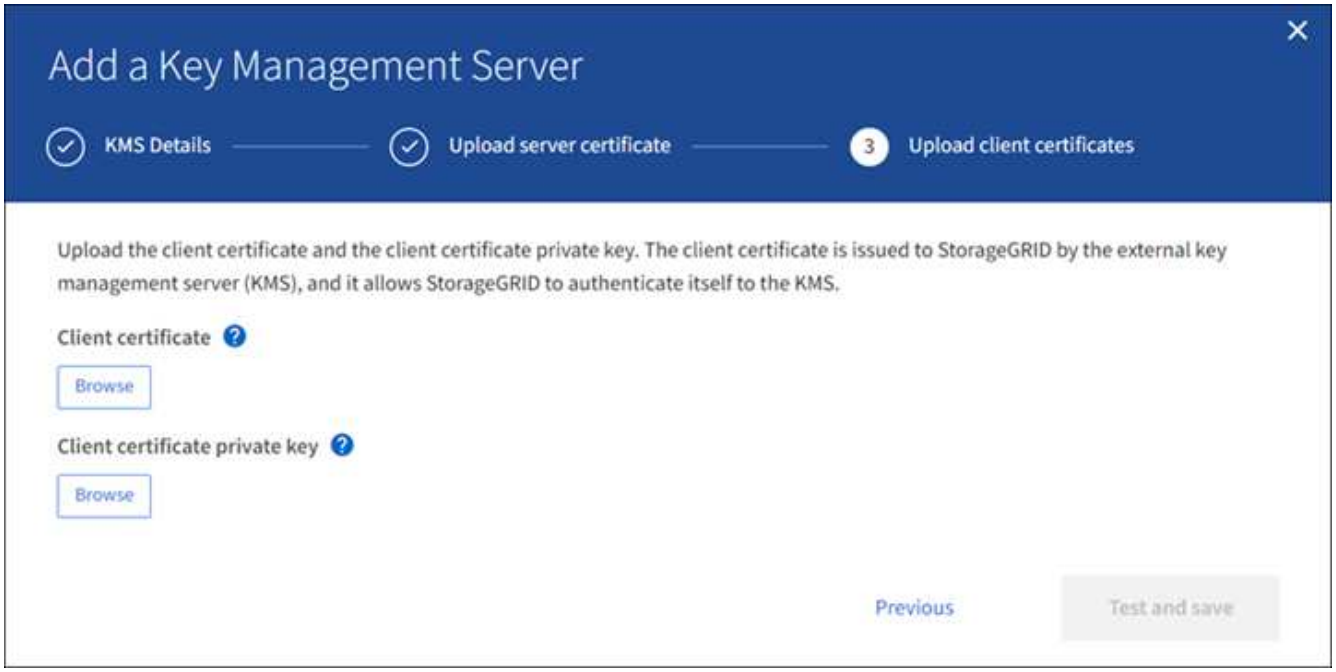
3. 「 * Continue * 」を選択します。

手順**3**：クライアント証明書をアップロードします

キー管理サーバの追加ウィザードの手順3（クライアント証明書のアップロード）で、クライアント証明書とクライアント証明書の秘密鍵をアップロードします。クライアント証明書は、 StorageGRID が KMS に対して自身を認証することを許可します。

手順

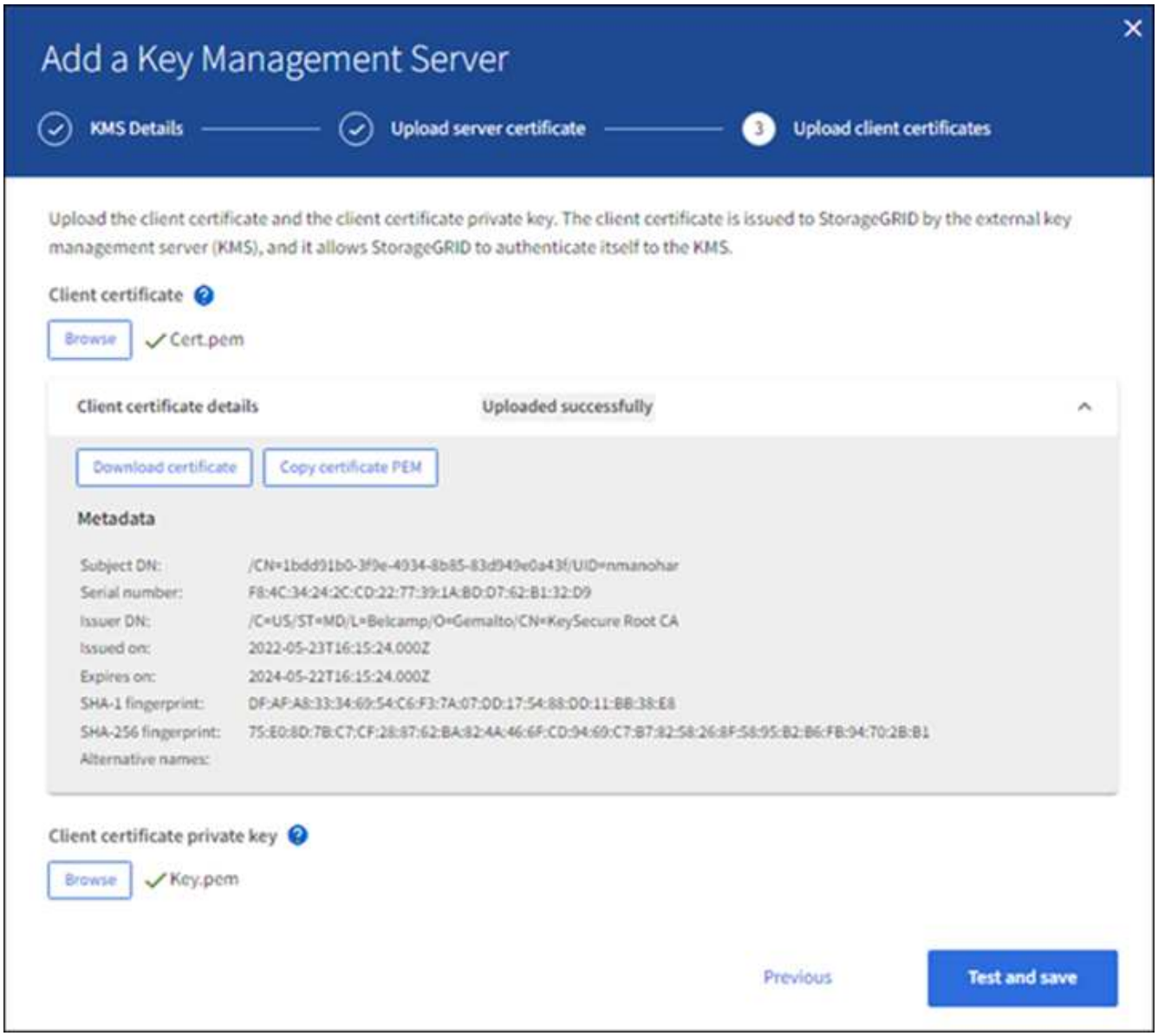
1. ステップ3（クライアント証明書のアップロード）*で、クライアント証明書の場所を参照します。



2. クライアント証明書ファイルをアップロードします。

   クライアント証明書のメタデータが表示されます。

3. クライアント証明書の秘密鍵の場所を参照します。
4. 秘密鍵ファイルをアップロードします。



5. [テストして保存]*を選択します。

   キー管理サーバとアプライアンスノードの間の接続をテストします。すべての接続が有効で、正しいキーが KMS にある場合は、新しいキー管理サーバが Key Management Server ページの表に追加されます。

   > KMS を追加すると、すぐに [Key Management Server] ページの証明書ステータスが [Unknown （不明）] と表示されます。各証明書の実際のステータスの StorageGRID 取得には 30 分程度かかる場合があります。最新のステータスを表示するには、 Web ブラウザの表示を更新する必要があります。

6. を選択したときにエラーメッセージが表示された場合は、メッセージの詳細を確認し、[OK]*を選択します。

   たとえば、接続テストに失敗した場合は、 422 ： Unprocessable Entity エラーが返されることがあります。

7. 外部接続をテストせずに現在の設定を保存する必要がある場合は、*[強制保存]*を選択します。

[Force save]*を選択すると、KMSの構成が保存されますが、各アプライアンスからそのKMSへの外部接続はテストされません。構成を含む問題 がある場合、該当するサイトでノード暗号化が有効になっているアプライアンスノードをリブートできない可能性があります。問題が解決するまでデータにアクセスできなくなる可能性があります。

8. 確認の警告を確認し、設定を強制的に保存する場合は、「 * OK 」を選択します。

   KMS の設定は保存されますが、 KMS への接続はテストされません。

KMS の詳細を確認します

StorageGRID システム内の各キー管理サーバ（ KMS ）に関する情報を確認することができます。これには、サーバ証明書とクライアント証明書の現在のステータスも含まれます。

手順

1. 設定 * > * セキュリティ * > * キー管理サーバ * を選択します。

   [Key management server]ページが表示されます。[設定の詳細]タブには、設定済みのキー管理サーバが表示されます。

2. 各 KMS について、表の情報を確認します。

フィールド	説明
KMS名	KMS の説明的な名前。
キー名	KMS 内の StorageGRID クライアントのキーエイリアス。
のキーを管理します	KMS に関連付けられている StorageGRID サイト。 このフィールドには、特定の StorageGRID サイトの名前、または別の KMS （デフォルト KMS ）で管理されていないサイト * が表示されます
ホスト名	KMS の完全修飾ドメイン名または IP アドレス。 2 台のキー管理サーバからなるクラスタがある場合は、両方のサーバの完全修飾ドメイン名または IP アドレスが表示されます。クラスタに複数のキー管理サーバがある場合は、最初の KMS の完全修飾ドメイン名または IP アドレスと、クラスタ内の追加のキー管理サーバの数が表示されます。 例： `10.10.10.10 and 10.10.10.11` または `10.10.10.10 and 2 others`。 クラスタ内のすべてのホスト名を表示するには、KMSを開き、**[編集]***または[アクション]**>**[編集]*を選択します。

フィールド	説明
証明書の有効期限	サーバ証明書、オプションの CA 証明書、およびクライアント証明書の現在の状態：有効、期限が切れている、期限が近づいている、または不明。 *注：*証明書の有効期限の更新を取得するには、StorageGRID が30分ほどかかる場合があります。現在の値を表示するには、 Web ブラウザの表示を更新する必要があります。

3. 証明書の有効期限が不明な場合は、30分ほど待ってからWebブラウザをリフレッシュしてください。

> KMSを追加した直後に、[Key Management Server]ページに証明書の有効期限が[Unknown]と表示されます。各証明書の実際のステータスの StorageGRID 取得には 30 分程度かかる場合があります。実際のステータスを確認するには、 Web ブラウザの表示を更新する必要があります。

4. [証明書の有効期限]列に証明書の有効期限が切れているか、有効期限が近づいていることが示されている場合は、できるだけ早く問題 に対処してください。

「* kms CA certificate expiration 」、「 kms client certificate expiration 」、「 kms server certificate expiration *」の各アラートがトリガーされたら、各アラートの概要 をメモして推奨される対処方法を実行します。

> データアクセスを維持するために、証明書の問題はできるだけ早く対処する必要があります。

5. このKMSの証明書の詳細を表示するには、表からKMS名を選択します。
6. KMSの概要ページで、サーバ証明書とクライアント証明書の両方のメタデータと証明書のPEMを確認します。必要に応じて、*[証明書の編集]*を選択して証明書を新しい証明書に置き換えます。

暗号化されたノードを表示する

StorageGRID システムでノード暗号化 * 設定が有効になっているアプライアンスノードに関する情報を表示できます。

手順

1. 設定 * > * セキュリティ * > * キー管理サーバ * を選択します。

[Key Management Server] ページが表示されます。Configuration Details タブには、設定済みのすべてのキー管理サーバが表示されます。

2. ページの上部で、*[暗号化されたノード]*タブを選択します。

[Encrypted nodes]タブには、*[Node Encryption]*設定が有効になっているStorageGRID システム内のアプライアンスノードが表示されます。

3. 各アプライアンスノードについて、表の情報を確認します。

列（ **Column** ）	説明
ノード名	アプライアンスノードの名前。
ノードタイプ	ノードのタイプ。 Storage 、 Admin 、または Gateway 。
サイト	ノードがインストールされている StorageGRID サイトの名前。
KMS名	ノードに使用される KMS の説明的な名前。 KMSがリストされていない場合は、[Configuration details]タブを選択してKMSを追加します。 "キー管理サーバ（ KMS ）を追加する"
キー UID	アプライアンスノードでデータの暗号化と復号化に使用する暗号化キーの一意の ID 。キーUID全体を表示するには、セルの上にカーソルを置きます。 ダッシュ（ - - ）は、キー UID が不明であることを示します。アプライアンスノードと KMS 間の接続問題 が原因である可能性があります。
ステータス	KMS とアプライアンスノード間の接続のステータス。ノードが接続されている場合は、タイムスタンプが 30 分ごとに更新されます。KMS の設定変更後に接続ステータスが更新されるまで数分かかることがあります。 • 注： * 新しい値を表示するには、 Web ブラウザを更新する必要があります。

4. ステータス列に KMS 問題 と表示されている場合は、問題 にすぐに対処してください。

   通常の KMS 操作中、ステータスは * KMS * に接続されます。ノードがグリッドから切断されると、ノードの接続状態が（意図的に停止しているか不明である）と表示されます。

   その他のステータスメッセージは、同じ名前の StorageGRID アラートに対応します。

   ◦ KMS の設定をロードできませんでした
   ◦ KMS 接続エラー
   ◦ KMS 暗号化キー名が見つかりません
   ◦ KMS 暗号化キーのローテーションに失敗しました
   ◦ KMS キーでアプライアンスボリュームを復号化できませんでした
   ◦ KMS は設定されていません

   これらのアラートに対して推奨される対処方法を実行します。

問題が発生した場合は、データを完全に保護するために、すぐに対処する必要があります。

キー管理サーバ（ **KMS** ）を編集する

証明書の有効期限が近づいている場合など、キー管理サーバの設定の編集が必要になることがあります。

作業を開始する前に

- を確認しておきます "キー管理サーバを使用する際の考慮事項と要件"。
- KMS 用に選択したサイトを更新する予定がある場合は、を確認してください "サイトの KMS を変更する際の考慮事項"。
- 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"。
- Root アクセス権限が割り当てられている。

手順

1. 設定 * > * セキュリティ * > * キー管理サーバ * を選択します。

   [Key management server]ページが表示され、設定済みのすべてのキー管理サーバが表示されます。

2. 編集するKMSを選択し、**[**アクション**]**>*[編集]*を選択します。

   テーブルでKMS名を選択し、KMS詳細ページで*編集*を選択して、KMSを編集することもできます。

3. 必要に応じて、キー管理サーバの編集ウィザードの*ステップ1（KMSの詳細）*で詳細を更新します。

フィールド	説明
KMS名	この KMS を特定するのに役立つわかりやすい名前。1~64 文字で指定します。

フィールド	説明
キー名	KMS 内の StorageGRID クライアントの正確なキーエイリアス。1~255 文字で指定する必要があります。 キー名の編集が必要になることはほとんどありません。たとえば、エイリアスの名前が KMS で変更された場合や、以前のキーのすべてのバージョンが新しいエイリアスのバージョン履歴にコピーされている場合は、キー名を編集する必要があります。 KMS のキー名 (エイリアス) を変更して、キーの回転を試みないでください。代わりに、 KMS ソフトウェアのキーバージョンを更新してキーをローテーションしてください。StorageGRID では、以前に使用されていたすべてのキーバージョン（および今後使用するすべてのバージョン）に、同じキーエイリアスを使用して KMS からアクセスできることが必要です。設定されている KMS のキーエイリアスを変更すると、 StorageGRID がデータを復号化できなくなる可能性があります。 "キー管理サーバを使用する際の考慮事項と要件"
のキーを管理します	サイト固有のKMSを編集していて、まだデフォルトKMSを持っていない場合は、オプションで*[別のKMSで管理されていないサイト(デフォルトKMS)]*を選択します。このオプションを選択すると、サイト固有のKMSがデフォルトのKMSに変換されます。これは、専用のKMSを持たないすべてのサイトと、拡張で追加されたすべてのサイトに適用されます。 *注:*サイト固有のKMSを編集している場合、別のサイトを選択することはできません。デフォルトのKMSを編集している場合、特定のサイトを選択することはできません。
ポート	KMS サーバが Key Management Interoperability Protocol （ KMIP ）の通信に使用するポート。デフォルトでは、 KMIP 標準ポートである 5696 が使用されます。
ホスト名	KMS の完全修飾ドメイン名または IP アドレス。 *注：*サーバ証明書のSubject Alternative Name（SAN）フィールドには、ここに入力するFQDNまたはIPアドレスが含まれている必要があります。そうしないと、 StorageGRID は KMS クラスタ内のすべてのサーバに接続できなくなります。

4. KMSクラスタを構成する場合は、*[別のホスト名を追加]*を選択して、クラスタ内の各サーバのホスト名を追加します。
5. 「 * Continue * 」を選択します。

   [キー管理サーバの編集]ウィザードの手順2（サーバ証明書のアップロード）が表示されます。
6. サーバー証明書を置き換える必要がある場合は、 * 参照 * を選択して新しいファイルをアップロードしま

す。

7. 「 * Continue * 」を選択します。

   [Edit a Key Management Server]ウィザードの手順3（クライアント証明書のアップロード）が表示されます。

8. クライアント証明書とクライアント証明書の秘密鍵を置き換える必要がある場合は、 * 参照 * を選択して新しいファイルをアップロードします。

9. [テストして保存]*を選択します。

   キー管理サーバと影響を受けるサイトのすべてのノード暗号化アプライアンスノードの間の接続をテストします。すべてのノード接続が有効で、 KMS に正しいキーがある場合は、キー管理サーバが Key Management Server ページの表に追加されます。

10. エラーメッセージが表示された場合は、メッセージの詳細を確認し、「 * OK * 」を選択します。

    たとえば、この KMS 用に選択したサイトが別の KMS によってすでに管理されている場合や、接続テストに失敗した場合は、「 422 ： Unprocessable Entity 」というエラーが表示されます。

11. 接続エラーを解決する前に現在の設定を保存する必要がある場合は、*[強制保存]*を選択します。

    > [Force save]*を選択すると、KMSの構成が保存されますが、各アプライアンスからそのKMSへの外部接続はテストされません。構成を含む問題 がある場合、該当するサイトでノード暗号化が有効になっているアプライアンスノードをリブートできない可能性があります。問題が解決するまでデータにアクセスできなくなる可能性があります。

    KMS の設定が保存されます。

12. 確認の警告を確認し、設定を強制的に保存する場合は、「 * OK 」を選択します。

    KMS の設定は保存されますが、 KMS への接続はテストされません。

キー管理サーバ（ **KMS** ）を削除する

場合によっては、キー管理サーバの削除が必要になることがあります。たとえば、サイトの運用を停止した場合は、サイト固有の KMS を削除できます。

作業を開始する前に

- を確認しておきます "キー管理サーバを使用する際の考慮事項と要件"。
- 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"。
- Root アクセス権限が割り当てられている。

このタスクについて

KMS は以下の場合に削除できます。

- サイトの運用が停止された場合や、ノードの暗号化が有効なアプライアンスノードがサイトに含まれていない場合は、サイト固有の KMS を削除できます。
- ノード暗号化が有効なアプライアンスノードがあるサイトごとにサイト固有の KMS がすでに存在する場

合は、デフォルトの KMS を削除できます。

手順

1. 設定 * > * セキュリティ * > * キー管理サーバ * を選択します。

   [Key management server]ページが表示され、設定済みのすべてのキー管理サーバが表示されます。

2. 削除するKMSを選択し、**[アクション]**>*[削除]*を選択します。

   テーブルでKMS名を選択し、KMS詳細ページで* Remove *を選択して、KMSを削除することもできます。

3. 次の条件に該当することを確認します。

   - アプライアンスノードでノード暗号化が有効になっていないサイトのサイト固有のKMSを削除する場合。
   - デフォルトのKMSを削除しようとしていますが、ノード暗号化を使用して各サイトにサイト固有のKMSがすでに存在しています。

4. 「 * はい * 」を選択します。

   KMS の設定は削除されます。

プロキシ設定を管理します

ストレージプロキシを設定します

プラットフォームサービスまたはクラウドストレージプールを使用している場合は、ストレージノードと外部の S3 エンドポイントの間に非透過型プロキシを設定できます。たとえば、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プラットフォームサービスメッセージを送信する場合などには、非透過型プロキシが必要です。

作業を開始する前に

- 特定のアクセス権限が必要です。
- 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"。

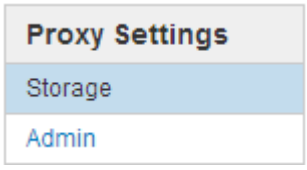
このタスクについて

設定できるストレージプロキシは 1 つです。

手順

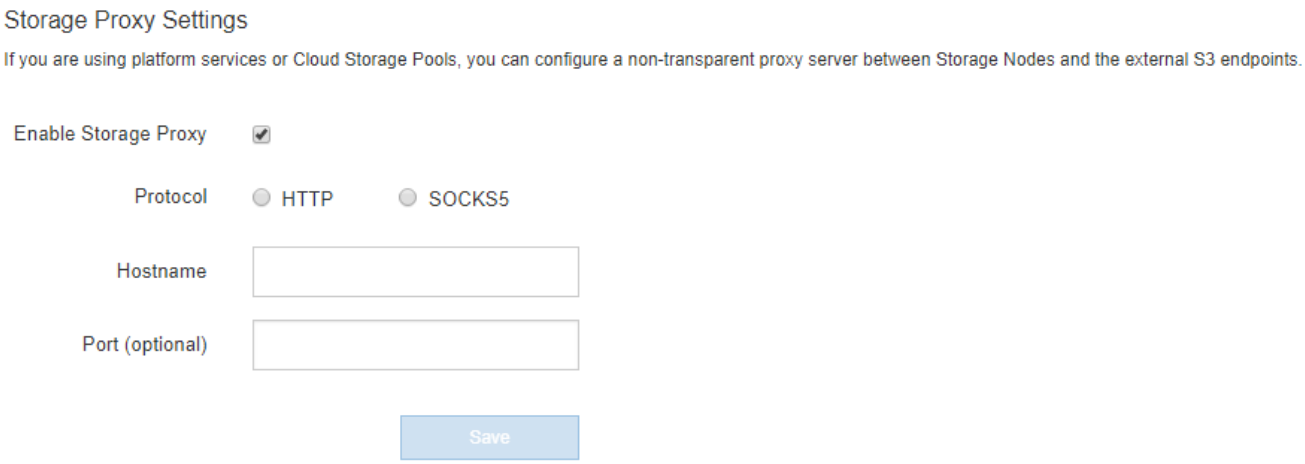
1. [* 設定 * > * セキュリティ * > * プロキシ設定 *] を選択します。

   ストレージプロキシの設定ページが表示されます。デフォルトでは、サイドバーメニューで「 * Storage * 」が選択されています。



2. [ストレージプロキシを有効にする]*チェックボックスを選択します。

   ストレージプロキシを設定するためのフィールドが表示されます。



3. 非透過型ストレージプロキシのプロトコルを選択します。
4. プロキシサーバのホスト名または IP アドレスを入力します。
5. 必要に応じて、プロキシサーバへの接続に使用するポートを入力します。

   プロトコルにデフォルトのポート 80 を使用する場合は、このフィールドを空白のままにできます。HTTP の場合は 80 、 SOCKS5 の場合は 1080 です。

6. [保存（ Save ）] を選択します。

   ストレージプロキシが保存されたら、プラットフォームサービスまたはクラウドストレージプールの新しいエンドポイントを設定してテストできます。

   プロキシの変更が有効になるまでに最大 10 分かかることがあります。

7. プロキシサーバの設定をチェックして、 StorageGRID からのプラットフォームサービス関連メッセージがブロックされないようにします。

完了後

ストレージプロキシを無効にする必要がある場合は、**[ストレージプロキシを有効にする]***チェックボックスをオフにし、[保存]*を選択します。

関連情報

- "プラットフォームサービス用のネットワークとポート"
- "ILM を使用してオブジェクトを管理する"

管理プロキシを設定します

HTTP または HTTPS を使用して AutoSupport メッセージを送信する場合（を参照）"AutoSupport を設定します"）を使用して、管理ノードとテクニカルサポート（ AutoSupport ）の間に非透過型プロキシサーバを設定できます。

作業を開始する前に

- 特定のアクセス権限が必要です。
- 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"。

このタスクについて

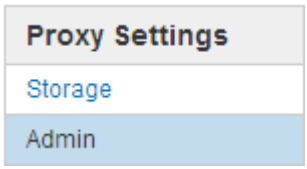
設定できる管理プロキシは 1 つです。

手順

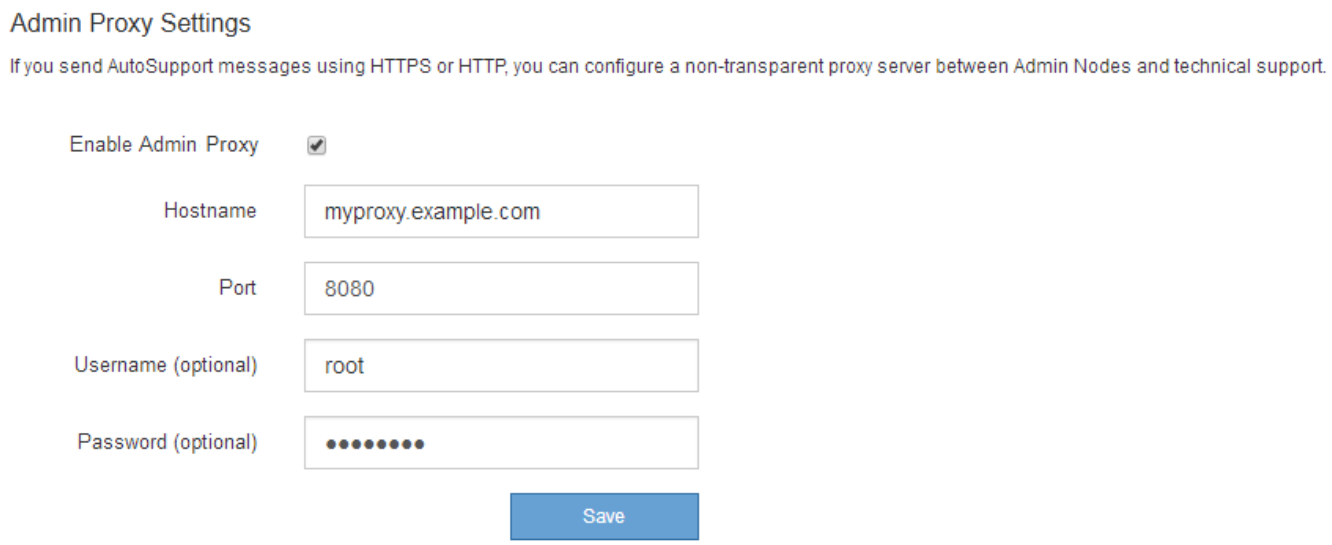
1. [* 設定 * > * セキュリティ * > * プロキシ設定 *] を選択します。

   Admin Proxy Settings ページが表示されます。デフォルトでは、サイドバーメニューで「 * Storage * 」が選択されています。

2. サイドバーのメニューから、 **Admin** を選択します。



3. [Enable Admin Proxy]*チェックボックスをオンにします。



4. プロキシサーバのホスト名または IP アドレスを入力します。
5. プロキシサーバへの接続に使用するポートを入力します。
6. 必要に応じて、プロキシユーザ名を入力します。

   プロキシサーバでユーザ名が不要な場合は、このフィールドを空白のままにします。

7. 必要に応じて、プロキシパスワードを入力します。

   プロキシサーバでパスワードが不要な場合は、このフィールドを空白のままにします。

8. [保存（ Save ）] を選択します。

管理プロキシが保存されると、管理ノードとテクニカルサポートの間にプロキシサーバが設定されます。

プロキシの変更が有効になるまでに最大 10 分かかることがあります。

9. プロキシを無効にする必要がある場合は、**[管理プロキシを有効にする]***チェックボックスをオフにし、[保存]*を選択します。

ファイアウォールを制御します

外部ファイアウォールでアクセスを制御します

外部ファイアウォールで特定のポートを開いたり閉じたりできます。

StorageGRID 管理ノード上のユーザインターフェイスと API へのアクセスは、外部ファイアウォールで特定のポートを開くか、または閉じることで制御できます。たとえば、システムアクセスを制御する他の方法に加えて、ファイアウォールでテナントが Grid Manager に接続できないようにすることができます。

StorageGRID 内部ファイアウォールを設定する場合は、を参照してください "内部ファイアウォールを設定します"。

ポート	説明	ポートが開いている場合
443	管理ノードのデフォルトの HTTPS ポート	Web ブラウザと管理 API クライアントは、 Grid Manager 、 Grid 管理 API 、 Tenant Manager 、およびテナント管理 API にアクセスできます。 • 注： * ポート 443 は一部の内部トラフィックにも使用されます。
8443	管理ノード上の制限された Grid Manager ポート	• Web ブラウザと管理 API クライアントは、 HTTPS を使用して Grid Manager とグリッド管理 API にアクセスできます。 • Webブラウザおよび管理APIクライアントは、Tenant Managerまたはテナント管理APIにアクセスできません。 • 内部コンテンツに対する要求は拒否されます。
ポート 1	管理ノード上の制限された Tenant Manager ポート	• Web ブラウザと管理 API クライアントは HTTPS を使用して Tenant Manager とテナント管理 API にアクセスできます。 • Webブラウザおよび管理APIクライアントは、Grid Managerまたはグリッド管理APIにアクセスできません。 • 内部コンテンツに対する要求は拒否されます。

シングルサインオン（ SSO ）は、制限された Grid Manager ポートまたは Tenant Manager ポートでは使用できません。ユーザをシングルサインオンで認証する場合は、デフォルトの HTTPS ポート（ 443 ）を使用する必要があります。

関連情報

- "Grid Manager にサインインします"
- "テナントアカウントを作成する"
- "外部との通信"

内部ファイアウォールコントロールを管理します

StorageGRID には、各ノードに内部ファイアウォールがあります。このファイアウォールを使用すると、ノードへのネットワークアクセスを制御できるため、グリッドのセキュリティが強化されます。ファイアウォールを使用して、特定のグリッド環境に必要なポートを除くすべてのポートでネットワークアクセスを禁止します。[Firewall]コントロールページで行った設定変更は、各ノードに展開されます。

Firewallコントロールページの3つのタブを使用して、グリッドに必要なアクセスをカスタマイズします。

- 特権アドレスリスト：このタブを使用して、選択したポートへのアクセスを許可します。[Manage external access]タブを使用して閉じたポートにアクセスできるIPアドレスまたはサブネットをCIDR表記で追加できます。
- 外部アクセスの管理：このタブを使用して、デフォルトで開いているポートを閉じるか、以前閉じていたポートを再度開きます。
- 信頼されていないクライアントネットワーク：このタブを使用して、ノードがクライアントネットワークからのインバウンドトラフィックを信頼するかどうかを指定します。

  このタブでは、信頼されていないクライアントネットワークが設定されている場合に開く追加のポートを指定することもできます。これらのポートから、Grid Manager、Tenant Manager、またはその両方へのアクセスを提供できます。

  このタブの設定は、[外部アクセスの管理]タブの設定よりも優先されます。

  - 信頼されていないクライアントネットワークを使用するノードは、そのノードに設定されているロードバランサエンドポイントポート（グローバル、ノードインターフェイス、およびノードタイプにバインドされたエンドポイント）の接続のみを受け入れます。
  - 信頼されていないクライアントネットワークでは、ロードバランサエンドポイントが設定されていない場合でも、[Untrusted Client Network]タブで開いている追加のポートがすべて開いています。
  - 信頼されていないクライアントネットワークでは、[Manage external networks]タブの設定に関係なく、ロードバランサエンドポイントのポートと選択された追加ポート_のみが開いています。
  - 信頼されている場合は、[Manage external access]タブで開いたすべてのポートおよびクライアントネットワークで開いているロードバランサエンドポイントにアクセスできます。

あるタブで行った設定は、別のタブで行ったアクセス変更に影響を与える可能性があります。すべてのタブの設定を確認して、ネットワークが想定どおりに動作することを確認してください。

内部ファイアウォールコントロールを設定するには、を参照してください "ファイアウォールコントロールを設定します"。

外部ファイアウォールとネットワークセキュリティの詳細については、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"。

[Privileged address list]タブと[Manage external access]タブ

特権アドレスリストタブでは、閉じられているグリッドポートへのアクセスを許可する1つ以上のIPアドレスを登録できます。[Manage external access]タブでは、選択した外部ポートまたは開いているすべての外部ポート（デフォルトではグリッド以外のノードからアクセス可能なポート）への外部アクセスを閉じることができます。多くの場合、この2つのタブを一緒に使用して、グリッドに必要な正確なネットワークアクセスをカスタマイズできます。

> 特権IPアドレスには、デフォルトで内部グリッドポートへのアクセスはありません。

例**1:**メンテナンスタスクにジャンプホストを使用します

ネットワーク管理にジャンプホスト（セキュリティ強化ホスト）を使用するとします。次の一般的な手順を使用できます。

1. 特権アドレスリストタブを使用して、ジャンプホストのIPアドレスを追加します。
2. [Manage external access]タブを使用して、すべてのポートをブロックします。

> ポート443と8443をブロックする前に、特権IPアドレスを追加してください。ブロックされたポートに現在接続されているユーザ（ユーザを含む）は、自分のIPアドレスが特権アドレスリストに追加されていないかぎり、Grid Managerにアクセスできません。

設定を保存すると、グリッド内の管理ノードのすべての外部ポートが、ジャンプホストを除くすべてのホストに対してブロックされます。これにより、ジャンプホストを使用して、グリッドでより安全にメンテナンスタスクを実行できるようになります。

例**2**：**Grid Manager**と**Tenant Manager**へのアクセスを制限する

セキュリティ上の理由から、Grid ManagerとTenant Managerへのアクセスを制限するとします。次の一般的な手順を使用できます。

1. [Manage external access]タブのトグルを使用して、ポート443をブロックします。
2. [Manage external access]タブのトグルを使用して、ポート8443へのアクセスを許可します。
3. [Manage external access]タブのトグルを使用して、ポート9443へのアクセスを許可します。

設定を保存すると、ホストはポート443にアクセスできなくなりますが、引き続きGrid Managerにはポート8443経由で、Tenant Managerにはポート9443経由でアクセスできます。

例**3**：敏感なポートをロックダウンします

機密性の高いポートとそのポート上のサービス（たとえば、ポート22のSSH）をロックダウンするとします。次の一般的な手順を使用できます。

1. サービスへのアクセスを必要とするホストにのみアクセスを許可するには、特権アドレスリストタブを使

用します。

2. [Manage external access]タブを使用して、すべてのポートをブロックします。

> ポート443と8443をブロックする前に、特権IPアドレスを追加してください。ブロックされたポートに現在接続されているユーザ（ユーザを含む）は、自分のIPアドレスが特権アドレスリストに追加されていないかぎり、Grid Managerにアクセスできません。

設定を保存すると、特権アドレスリストのホストでポート22とSSHサービスを使用できるようになります。要求の送信元インターフェイスに関係なく、他のすべてのホストはサービスへのアクセスを拒否されます。

例**4**：未使用のサービスへのアクセスを無効にします

ネットワークレベルでは、使用する予定のない一部のサービスを無効にすることができます。たとえば、Swiftアクセスを許可しない場合は、次の一般的な手順を実行します。

1. [Manage external access]タブのトグルを使用して、ポート18083をブロックします。
2. [Manage external access]タブのトグルを使用して、ポート18085をブロックします。

設定を保存すると、ストレージノードでSwift接続は許可されなくなりますが、ブロックされていないポートで他のサービスへのアクセスは引き続き許可されます。

[信頼されていないクライアントネットワーク**]**タブ

クライアントネットワークを使用している場合は、明示的に設定されたエンドポイントまたはこのタブで選択した追加のポートでのみインバウンドクライアントトラフィックを受け入れることで、StorageGRID を悪意のある攻撃から保護できます。

デフォルトでは、各グリッドノードのクライアントネットワークは *trusted_* です。つまり、StorageGRID はデフォルトで、すべてののグリッドノードへのインバウンド接続を信頼します "使用可能な外部ポート"。

各ノードのクライアントネットワークを「 *untrusted_* 」に指定することで、 StorageGRID システムに対する悪意ある攻撃の脅威を軽減できます。ノードのクライアントネットワークが信頼されていない場合、ノードはロードバランサエンドポイントとして明示的に設定されたポートと、[Firewall]制御ページの[Untrusted Client Network]タブを使用して指定した追加のポートでのみインバウンド接続を受け入れます。を参照してください "ロードバランサエンドポイントを設定する" および "ファイアウォールコントロールを設定します"。

例 **1** ：ゲートウェイノードが **HTTPS S3** 要求のみを受け入れる

ゲートウェイノードで、 HTTPS S3 要求を除くクライアントネットワーク上のすべてのインバウンドトラフィックを拒否するとします。この場合、次の一般的な手順を実行します。

1. から "ロードバランサエンドポイント" ページで、HTTPS経由のS3用のロードバランサエンドポイントをポート443に設定します。
2. [Firewall control]ページで、[Untrusted]を選択して、ゲートウェイノードのクライアントネットワークを信頼されていないネットワークとして指定します。

設定を保存すると、ポート 443 での HTTPS S3 要求と ICMP エコー（ ping ）要求を除き、ゲートウェイノードのクライアントネットワーク上のすべてのインバウンドトラフィックが破棄されます。

例 **2** ：ストレージノードが **S3** プラットフォームサービス要求を送信する

あるストレージノードからのアウトバウンドS3プラットフォームサービストラフィックは有効にするが、クライアントネットワークではそのストレージノードへのインバウンド接続は禁止するとします。この場合は、次の手順を実行します。

- [Firewall]制御ページの[Untrusted Client Networks]タブで、ストレージノード上のクライアントネットワークが信頼されていないことを指定します。

設定を保存すると、ストレージノードはクライアントネットワークで受信トラフィックを受け入れなくなりますが、設定されているプラットフォームサービスのデスティネーションへのアウトバウンド要求は引き続き許可します。

例**3**：**Grid Manager**へのアクセスをサブネットに制限する

Grid Managerに特定のサブネットに対するアクセスのみを許可するとします。次の手順を実行します。

1. 管理ノードのクライアントネットワークをサブネットに接続します。
2. [Untrusted Client Network]タブを使用して、クライアントネットワークを信頼されていないものとして設定します。
3. タブの*[信頼されていないクライアントネットワークで開くポートの追加]*セクションで、ポート443または8443を追加します。
4. [Manage external access]タブを使用して、すべての外部ポートをブロックします（サブネット外のホストに対して特権IPアドレスが設定されているかどうかに関係なく）。

設定を保存すると、指定したサブネットのホストだけがGrid Managerにアクセスできるようになります。他のすべてのホストはブロックされます。

内部ファイアウォールを設定します

StorageGRID ノードの特定のポートへのネットワークアクセスを制御するようにStorageGRID ファイアウォールを設定できます。

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"。
- の情報を確認しておきます "ファイアウォールコントロールを管理します" および "ネットワークのガイドライン"。
- 管理ノードまたはゲートウェイノードが明示的に設定されたエンドポイントでのみインバウンドトラフィックを受け入れるように設定する場合は、ロードバランサエンドポイントを定義しておきます。

> クライアントネットワークの設定を変更する際、ロードバランサエンドポイントが設定されていないと、既存のクライアント接続が失敗することがあります。

このタスクについて

StorageGRID には、各ノードに内部ファイアウォールがあります。このファイアウォールを使用して、グリッドのノードの一部のポートを開いたり閉じたりできます。[Firewall]制御タブを使用して、グリッドネットワーク、管理ネットワーク、およびクライアントネットワークでデフォルトで開いているポートを開いたり閉じ

たりできます。閉じているグリッドポートにアクセスできる特権IPアドレスのリストを作成することもできます。クライアントネットワークを使用している場合は、ノードがクライアントネットワークからのインバウンドトラフィックを信頼するかどうかを指定できます。また、クライアントネットワークの特定のポートへのアクセスを設定できます。

グリッドの外部のIPアドレスに対して開くポートの数を絶対に必要なポートだけに制限すると、グリッドのセキュリティが強化されます。3つのファイアウォールコントロールタブのそれぞれの設定を使用して、必要なポートだけが開いていることを確認します。

ファイアウォールコントロールの使用方法（例を含む）の詳細については、を参照してください "ファイアウォールコントロールを管理します"。

外部ファイアウォールとネットワークセキュリティの詳細については、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"。

ファイアウォールコントロールにアクセスします

手順

1. * configuration > Security > Firewall control *を選択します。

   このページの3つのタブについては、を参照してください "ファイアウォールコントロールを管理します"。

2. 任意のタブを選択して、ファイアウォールコントロールを設定します。

   これらのタブは任意の順序で使用できます。1つのタブで設定した設定では、他のタブで実行できる操作は制限されません。ただし、1つのタブで設定を変更すると、他のタブで設定されたポートの動作が変更される可能性があります。

特権アドレスリスト

特権アドレスリストタブを使用して、デフォルトで閉じられているポート、または外部アクセスの管理タブの設定によって閉じられているポートへのアクセスをホストに許可します。

権限付きIPアドレスとサブネットには、デフォルトで内部のグリッドアクセスはありません。また、[Manage external access]タブでブロックされていても、ロードバランサエンドポイントと、[Privileged address list]タブで開いている追加のポートにアクセスできます。

[特権アドレスリスト]タブの設定は、[信頼されていないクライアントネットワーク]タブの設定を上書きすることはできません。

手順

1. 特権アドレスリストタブで、閉じたポートへのアクセスを許可するアドレスまたはIPサブネットを入力します。
2. 必要に応じて、*[Add another IP address or subnet in CIDR notation]*を選択して、権限付きクライアントを追加します。

   特権リストにできるだけ少ないアドレスを追加します。

3. 必要に応じて、*[特権IPアドレスによるStorageGRID 内部ポートへのアクセスを許可する]*を選択します。を参照してください "StorageGRID の内部ポート"。

このオプションを使用すると、内部サービスの保護が一部解除されます。可能であれば無効のままにしておきます。

4. [保存（ Save ）] を選択します。

外部アクセスの管理

[Manage external access]タブでポートを閉じると、特権アドレスリストにIPアドレスを追加しないかぎり、グリッド以外のIPアドレスからポートにアクセスすることはできません。閉じることができるのは、デフォルトで開いているポートだけです。また、閉じたポートのみを開くことができます。

[外部アクセスの管理]タブの設定は、[信頼されていないクライアントネットワーク]タブの設定を上書きすることはできません。たとえば、ノードが信頼されていない場合、クライアントネットワークでポートSSH/22が[外部アクセスの管理]タブで開いていてもブロックされます。[Untrusted Client Network]タブの設定は、クライアントネットワークの閉じているポート（443、8443、9443など）よりも優先されます。

手順

1. [外部アクセスの管理]*を選択します。タブには、グリッド内のノードのすべての外部ポート（デフォルトではグリッド以外のノードからアクセス可能なポート）が表示されます。
2. 次のオプションを使用して、開いたり閉じたりするポートを設定します。
   - 各ポートの横にあるトグルを使用して、選択したポートを開いたり閉じたりします。
   - 表にリストされているすべてのポートを開くには、*表示されているすべてのポートを開く*を選択します。
   - 表に示されているすべてのポートを閉じるには、*[表示されているすべてのポートを閉じる]*を選択します。

Grid Managerポート443または8443を閉じると、ブロックされたポートに現在接続しているユーザ（ユーザを含む）は、ユーザのIPアドレスが特権アドレスのリストに追加されていないかぎり、Grid Managerにアクセスできなくなります。

テーブルの右側にあるスクロールバーを使用して、使用可能なすべてのポートが表示されていることを確認します。検索フィールドを使用して、ポート番号を入力して外部ポートの設定を検索します。ポート番号の一部を入力できます。たとえば、*2*と入力すると、名前に文字列「2」が含まれるすべてのポートが表示されます。

3. [保存（ Save ）] を選択します

Untrusted Client Networkの略

ノードのクライアントネットワークが信頼されていない場合、ノードはロードバランサエンドポイントとして設定されたポート、およびオプションでこのタブで選択した追加のポートでのみインバウンドトラフィックを受け入れます。このタブを使用して、拡張時に追加する新しいノードのデフォルト設定を指定することもできます。

ロードバランサエンドポイントが設定されていないと、既存のクライアント接続が失敗する可能性があります。

タブで設定を変更すると、[外部アクセスの管理]*タブの設定が上書きされます。

手順

1. [信頼されていないクライアントネットワーク]*を選択します。
2. [Set New Node Default]セクションで、拡張手順 で新しいノードをグリッドに追加する際のデフォルト設定を指定します。

   - * Trusted *（デフォルト）：拡張でノードを追加すると、そのクライアントネットワークが信頼されます。
   - * Untrusted * ：拡張でノードが追加されるときに、そのクライアントネットワークは信頼されません。

     必要に応じて、このタブに戻って特定の新しいノードの設定を変更できます。

   この設定は、 StorageGRID システム内の既存のノードには影響しません。

3. 次のオプションを使用して、明示的に設定されたロードバランサエンドポイントまたは選択した追加のポートでのみクライアント接続を許可するノードを選択します。

   - テーブルに表示されたすべてのノードを信頼されていないクライアントネットワークのリストに追加するには、*[表示されたノードで信頼されていないクライアントネットワーク]*を選択します。
   - テーブルに表示されたすべてのノードを信頼されていないクライアントネットワークのリストから削除するには、*[表示されたノードで信頼する]*を選択します。
   - 各ポートの横にある切り替えボタンを使用して、選択したノードのクライアントネットワークを[Trusted]または[Untrusted]に設定します。

     たとえば、*表示されているノードで[Untrust on displayed nodes]*を選択してすべてのノードを[Untrusted Client Network]リストに追加し、個 々 のノードの横にある切り替えを使用してその1つのノードを[Trusted Client Network]リストに追加できます。

   テーブルの右側にあるスクロールバーを使用して、使用可能なすべてのノードが表示されていることを確認します。検索フィールドにノード名を入力して、任意のノードの設定を検索します。名前の一部を入力できます。たとえば、「* gw *」と入力すると、名前に文字列「gw」を含むすべてのノードが表示されます。

4. 必要に応じて、信頼されていないクライアントネットワークで開く追加のポートを選択します。これらのポートから、Grid Manager、Tenant Manager、またはその両方へのアクセスを提供できます。

   たとえば、メンテナンス目的でクライアントネットワークからGrid Managerにアクセスできるようにする場合にこのオプションを使用します。

   これらの追加ポートは、[Manage external access]タブで閉じているかどうかに関係なく、クライアントネットワークで開いています。

5. [保存（ Save ）] を選択します。

   新しいファイアウォール設定がすぐに適用され、適用されます。ロードバランサエンドポイントが設定されていないと、既存のクライアント接続が失敗する可能性があります。

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"。
- Root Access権限またはTenant Accounts権限が必要です。
- 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。
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。

権限を選択します

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"。 注：[Use grid federation connection]*は、新しいS3テナントを作成する場合にのみ選択できます。既存のテナントに対してこの権限を選択することはできません。

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。

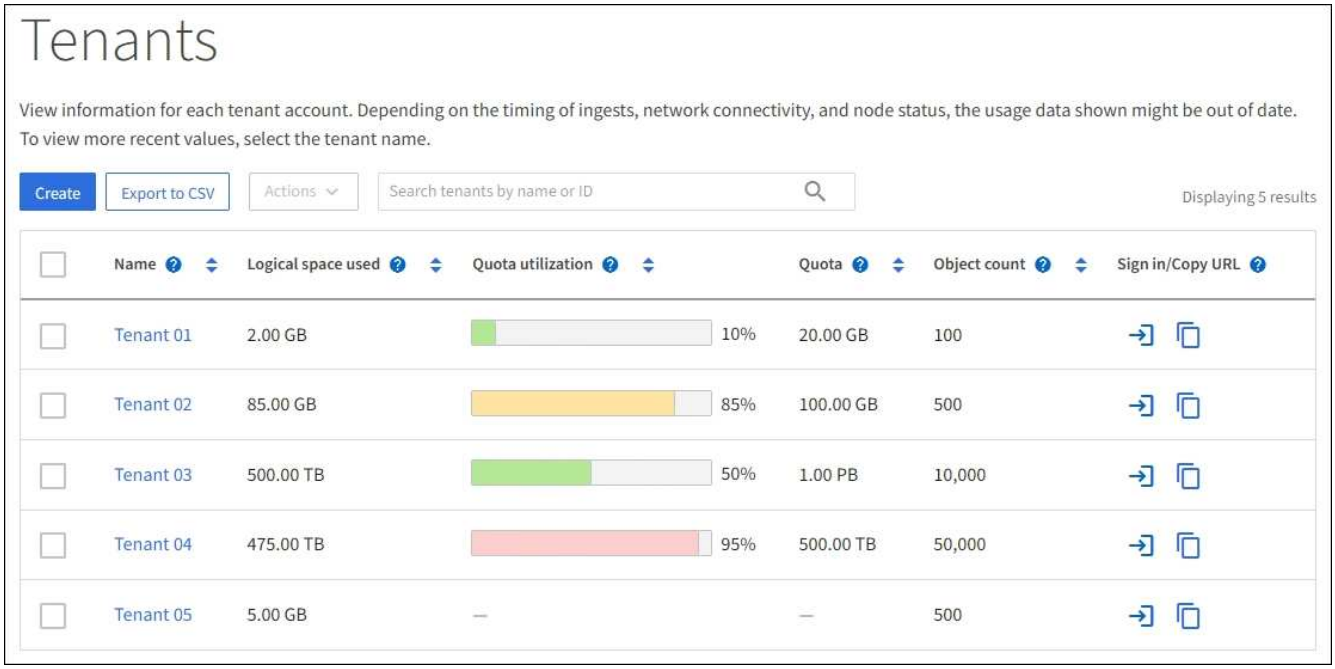
テナントに* Use grid federation connection *権限がある場合は、接続内のいずれかのグリッドからテナントの詳細を編集できます。ただし、接続内の一方のグリッドに加えた変更は、もう一方のグリッドにコピーされません。テナントの詳細をグリッド間で正確に同期させたい場合は、両方のグリッドで同じ編集を行います。を参照してください "グリッドフェデレーション接続に許可されているテナントを管理します"。

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"。
- Root Access権限またはTenant Accounts権限が必要です。

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、の手順に従います "グリッドフェデレーションを使用するテナントの権限を削除しています"。

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"。
- 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

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"。
- 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。

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。

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Amazon Simple Notification Service™（Amazon 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。

- 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

- "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
- Simple Notification Service（Amazon 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、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。

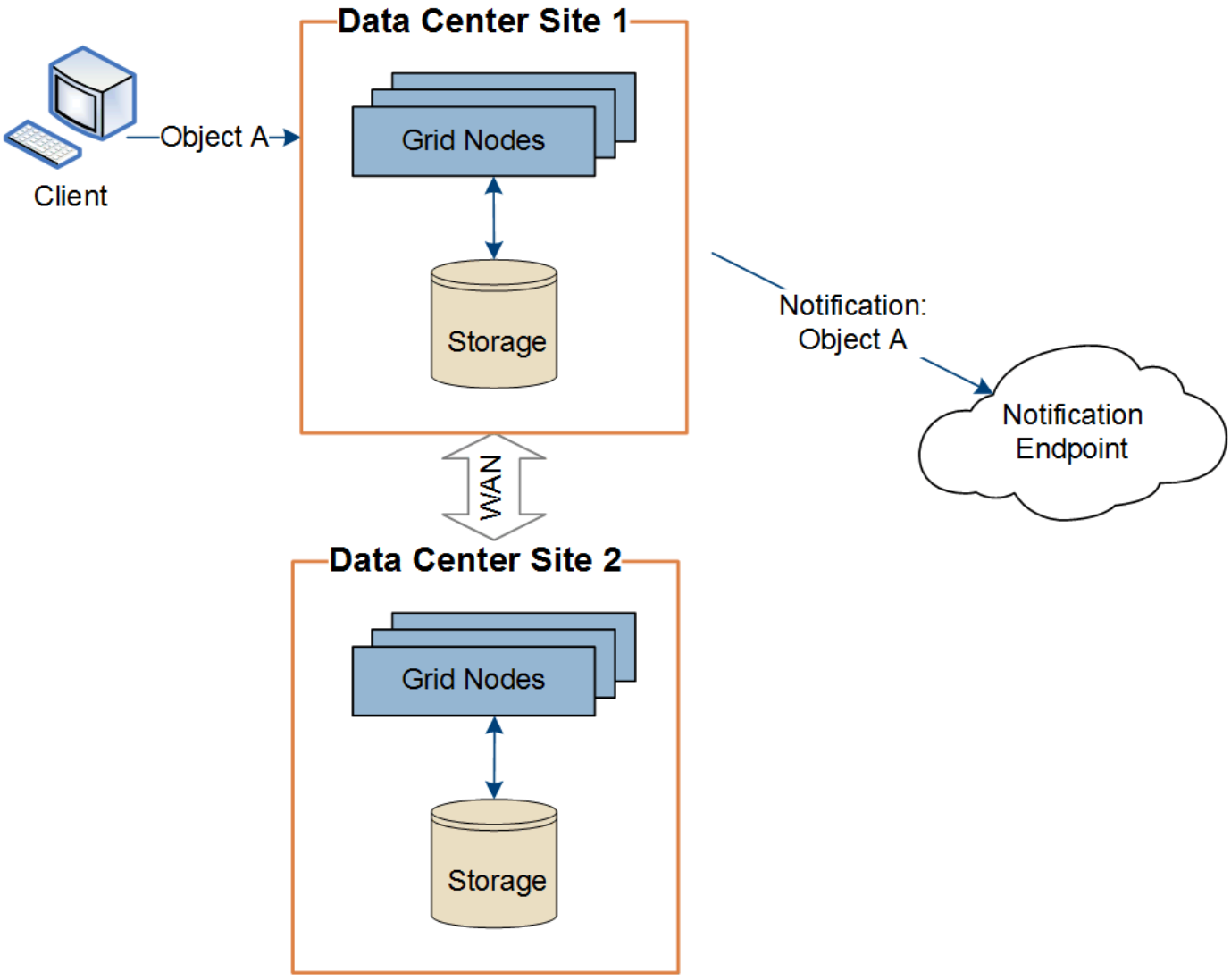
関連情報

- "テナントアカウントを使用する"

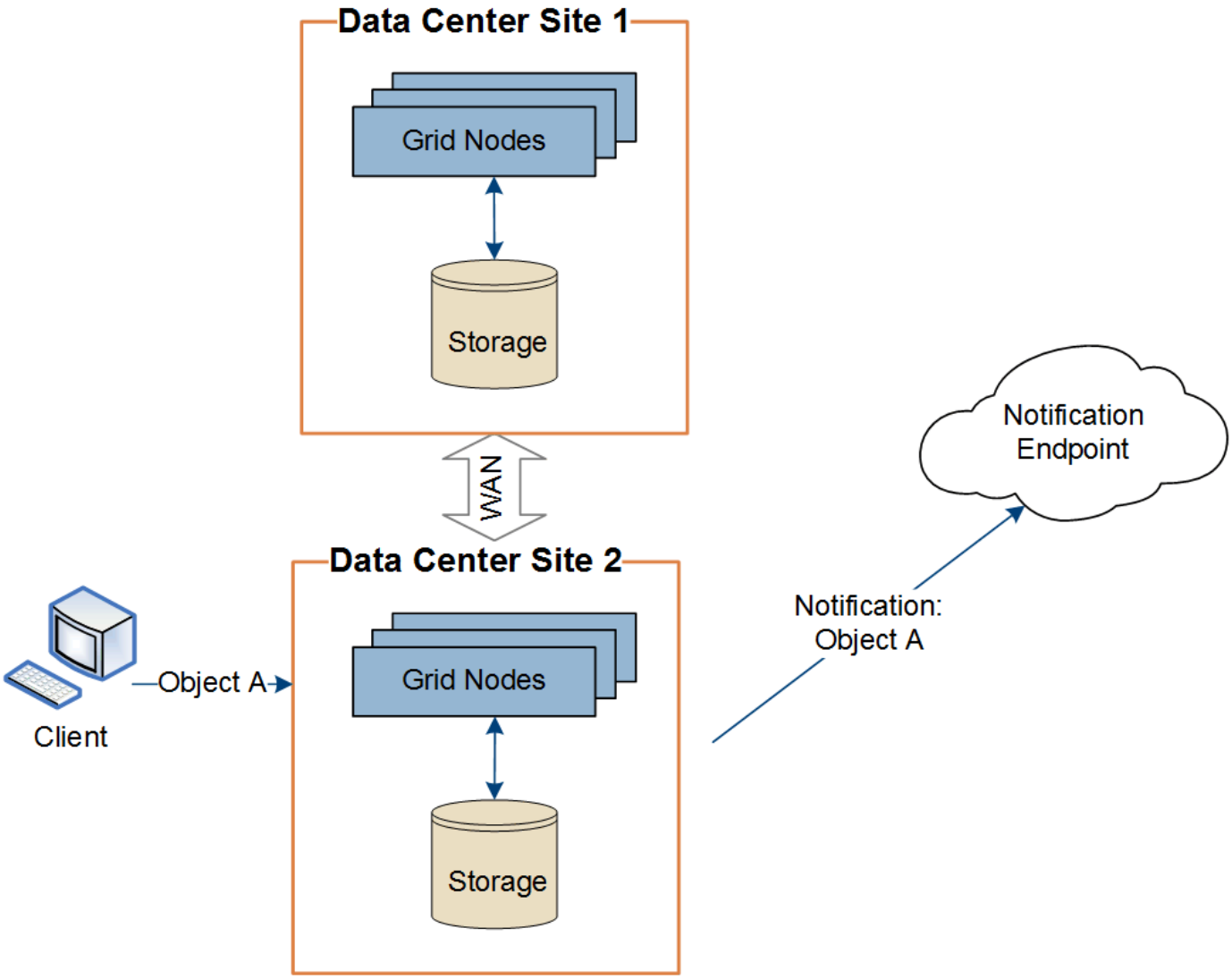
サイト単位のプラットフォームサービスメッセージの配信

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、 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。

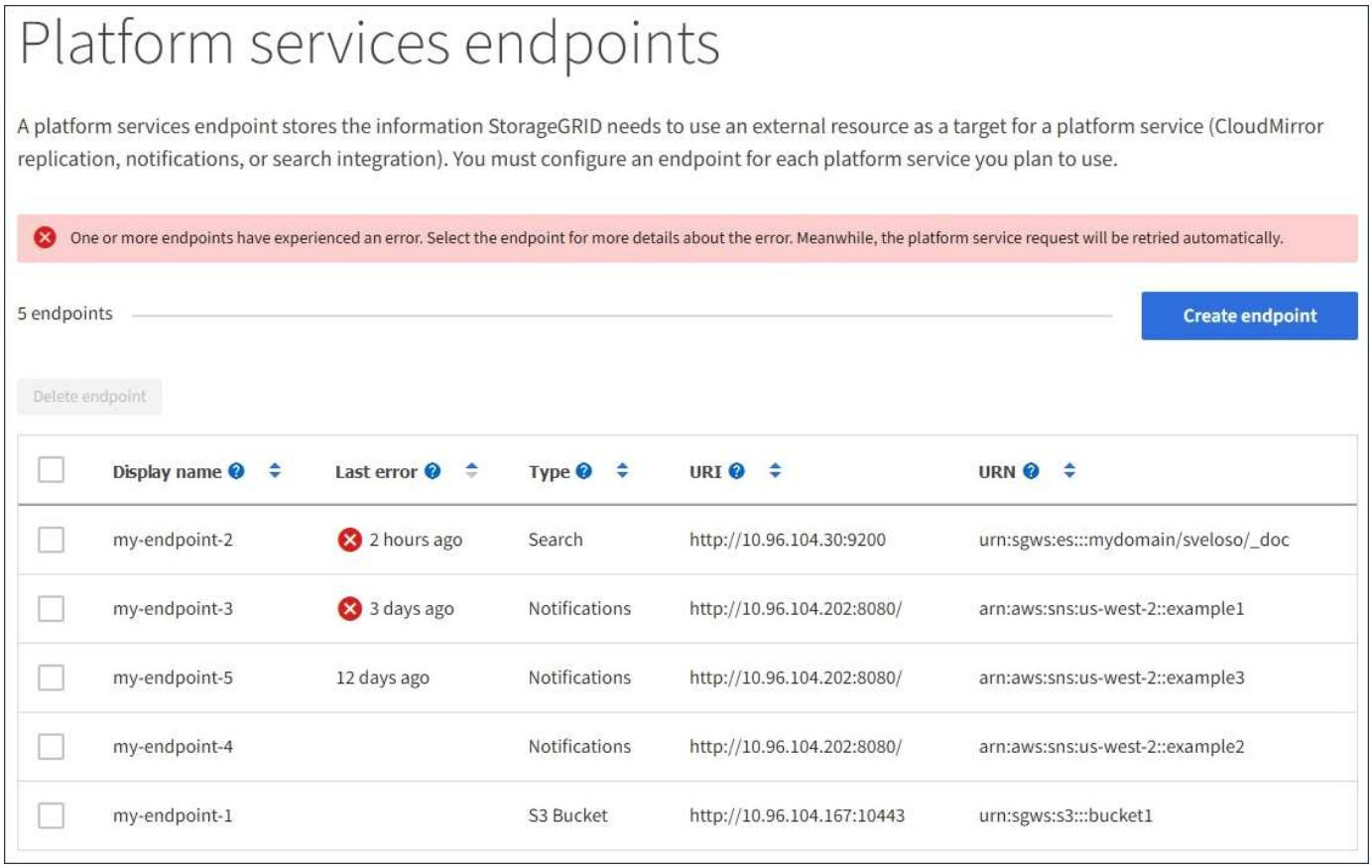
テナントアカウントでプラットフォームサービスが有効になっていないと、エンドポイントの作成が失敗します。

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。

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。



「 * 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。

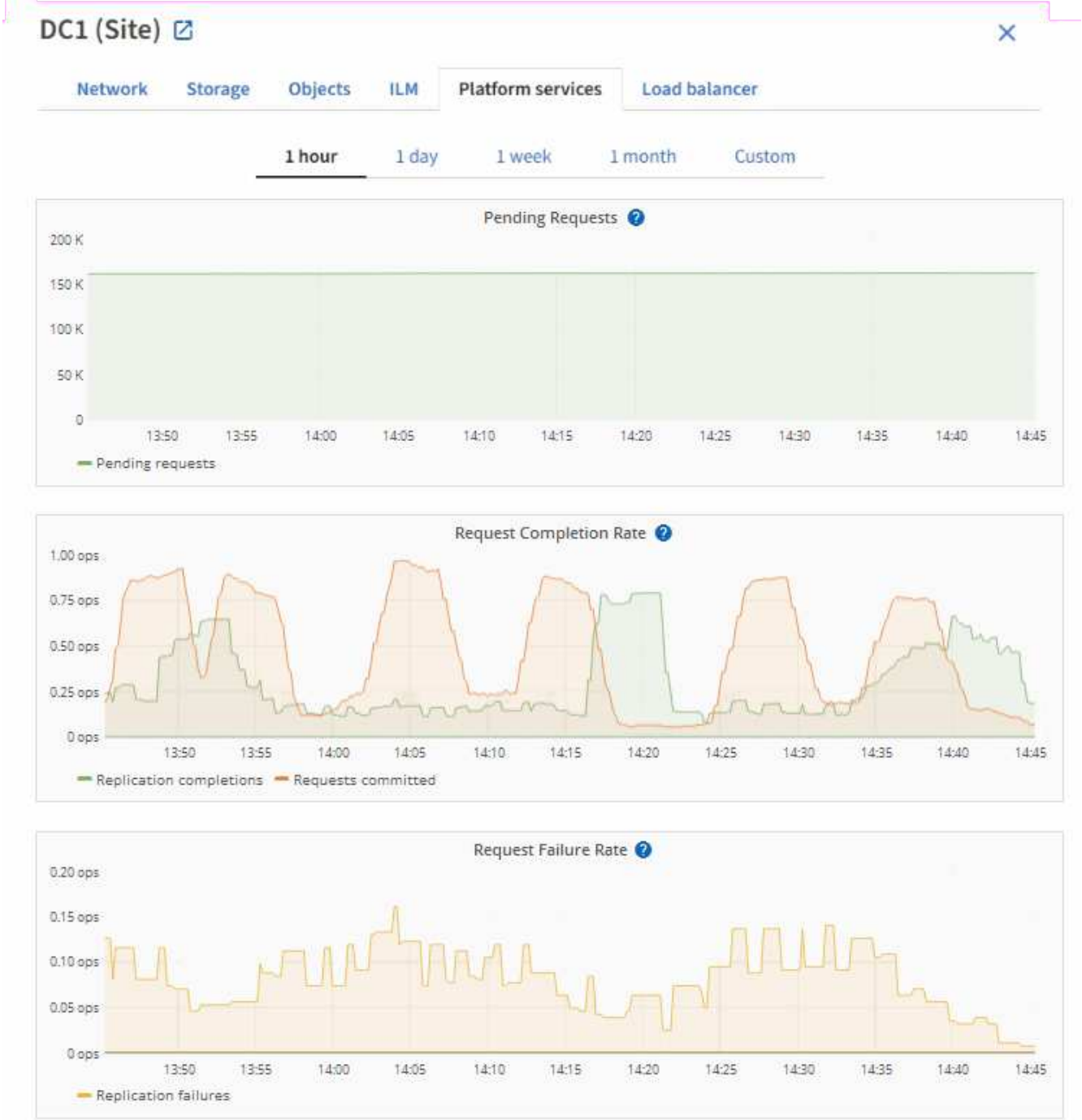
明らかな影響は、受信 S3 要求の実行時間が長くなることだけです。パフォーマンスが大幅に低下していることが検出されるようになった場合は、取り込み速度を下げるか、容量の大きいエンドポイントを使用する必要があります。要求のバックログが増え続けると、クライアント S3 処理（ PUT 要求など）が失敗します。

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を使用して、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を行います"。

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。

クライアント接続を設定します

S3およびSwiftクライアント接続を設定します。概要

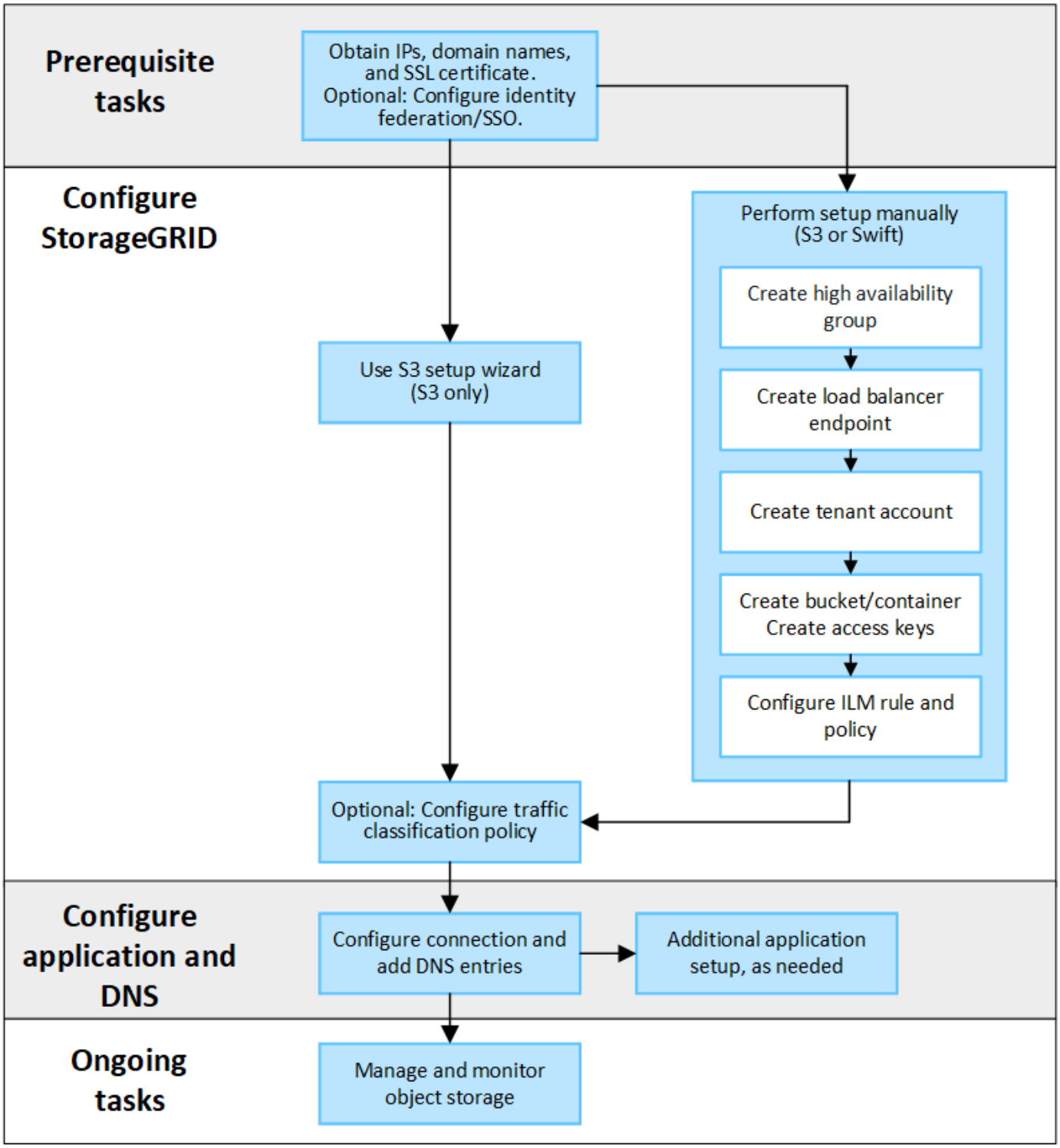
グリッド管理者は設定オプションを管理し、S3およびSwiftクライアントアプリケーションがデータの格納と読み出しを行うためにStorageGRID システムに接続する方法を制御します。

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。

設定ワークフロー

ワークフロー図に示すように、StorageGRID をS3またはSwiftアプリケーションに接続する主な手順は4つあります。

1. クライアントアプリケーションがStorageGRID に接続する方法に基づいて、StorageGRID で前提条件となるタスクを実行します。
2. StorageGRID を使用して、アプリケーションがグリッドに接続するために必要な値を取得します。S3セットアップウィザードを使用するか、各StorageGRID エンティティを手動で設定できます。
3. S3またはSwiftアプリケーションを使用して、StorageGRID への接続を完了します。DNSエントリを作成して、使用するドメイン名にIPアドレスを関連付けます。
4. アプリケーションとStorageGRID で継続的なタスクを実行し、時間の経過に伴うオブジェクトストレージの管理と監視を行います。



クライアントアプリケーションに**StorageGRID** を接続するために必要な情報

S3またはSwiftクライアントアプリケーションにStorageGRID を接続する前に、StorageGRID で設定手順を実行して特定の値を取得する必要があります。

どのような価値が必要か？

次の表に、StorageGRID で設定する必要がある値と、それらの値がS3またはSwiftアプリケーションとDNSサーバで使用される場所を示します。

価値	値が設定されます	値が使用されます
仮想IP（VIP）アドレス	[HA group]をクリックしますStorageGRID	DNSエントリ
ポート	StorageGRID > Load Balancer Endpointの順に選択します	クライアントアプリケーション
SSL 証明書	StorageGRID > Load Balancer Endpointの順に選択します	クライアントアプリケーション
サーバ名（FQDN）	StorageGRID > Load Balancer Endpointの順に選択します	• クライアントアプリケーション • DNSエントリ
S3アクセスキーIDとシークレットアクセスキー	StorageGRID > Tenant and bucketの順に選択します	クライアントアプリケーション
バケット/コンテナ名	StorageGRID > Tenant and bucketの順に選択します	クライアントアプリケーション

これらの値を取得するにはどうすればよいですか。

要件に応じて、次のいずれかの方法で必要な情報を入手できます。

- *を使用します "S3セットアップウィザード"*S3セットアップウィザードを使用すると、StorageGRID に必要な値を簡単に設定でき、S3アプリケーションの設定時に使用できる1つまたは2つのファイルを出力できます。ウィザードの指示に従って必要な手順を実行し、設定がStorageGRID のベストプラクティスに準拠していることを確認できます。

  S3アプリケーションを設定する場合は、特別な要件がある場合や実装に大幅なカスタマイズが必要な場合を除き、S3セットアップウィザードを使用することを推奨します。

- *を使用します "FabricPool セットアップウィザード"*S3セットアップウィザードと同様に、FabricPool セットアップウィザードを使用して必要な値をすばやく設定し、ONTAP でFabricPool クラウド階層を設定するときに使用できるファイルを出力できます。

  StorageGRID をFabricPool クラウド階層のオブジェクトストレージシステムとして使用する場合は、特別な要件がある場合や実装の大幅なカスタマイズが必要になる場合を除き、FabricPool セットアップウィザードを使用することを推奨します。

- 項目を手動で設定する。Swiftアプリケーションに接続する場合（またはS3アプリケーションに接続してS3セットアップウィザードを使用しない場合）は、設定を手動で実行して必要な値を取得できます。次の手順を実行します。

  a. S3またはSwiftアプリケーションに使用するハイアベイラビリティ（HA）グループを設定します。を参照してください "ハイアベイラビリティグループを設定する"。

  b. S3またはSwiftアプリケーションが使用するロードバランサエンドポイントを作成します。を参照してください "ロードバランサエンドポイントを設定する"。

c. S3またはSwiftアプリケーションが使用するテナントアカウントを作成します。を参照してください "テナントアカウントを作成します"。

d. S3テナントの場合は、テナントアカウントにサインインし、アプリケーションにアクセスする各ユーザのアクセスキーIDとシークレットアクセスキーを生成します。を参照してください "独自のアクセスキーを作成します"。

e. テナントアカウント内に1つ以上のS3バケットまたはSwiftコンテナを作成します。S3の場合は、を参照してください "S3 バケットを作成する"。Swiftの場合は、を使用します "PUT（コンテナ）要求"。

f. 新しいテナントまたはバケット/コンテナに属するオブジェクトに対する特定の配置手順を追加するには、新しいILMルールを作成し、そのルールを使用する新しいILMポリシーをアクティブ化します。を参照してください "ILM ルールを作成する" および "ILM ポリシーを作成する"。

S3セットアップウィザードを使用する

S3セットアップウィザードの「考慮事項と要件」を使用します

S3セットアップウィザードを使用して、StorageGRID をS3アプリケーションのオブジェクトストレージシステムとして設定できます。

S3セットアップウィザードを使用するタイミング

S3セットアップウィザードの手順に従って、S3アプリケーションで使用するStorageGRID を設定します。ウィザードを完了すると、ファイルをダウンロードしてS3アプリケーションに値を入力します。ウィザードを使用すると、システムをより迅速に設定し、設定がStorageGRID のベストプラクティスに準拠していることを確認できます。

Root Access権限がある場合は、StorageGRID グリッドマネージャの使用を開始するときにS3セットアップウィザードを完了することも、ウィザードにアクセスして完了することもできます。要件に応じて、必要な項目の一部またはすべてを手動で設定し、ウィザードを使用してS3アプリケーションで必要な値をアセンブルすることもできます。

ウィザードを使用する前に

ウィザードを使用する前に、これらの前提条件を満たしていることを確認してください。

IPアドレスを取得し、VLANインターフェイスを設定します

ハイアベイラビリティ（HA）グループを設定する場合は、S3アプリケーションが接続するノードと使用するStorageGRID ネットワークを確認しておきます。また、サブネットCIDR、ゲートウェイIPアドレス、および仮想IP（VIP）アドレスに入力する値も確認しておきます。

仮想LANを使用してS3アプリケーションからトラフィックを分離する場合は、VLANインターフェイスがすでに設定されています。を参照してください "VLAN インターフェイスを設定します"。

アイデンティティフェデレーションとSSOを設定する

StorageGRID システムでアイデンティティフェデレーションまたはシングルサインオン（SSO）を使用する場合は、これらの機能を有効にしておきます。また、S3アプリケーションが使用するテナントアカウントへのルートアクセスが必要なフェデレーテッドグループも確認しておきます。を参照してください "アイデンティティフェデレーションを使用する" および "シングルサインオンを設定します"。

ドメイン名を取得して設定します

StorageGRID に使用するFully Qualified Domain Name（FQDN；完全修飾ドメイン名）を確認しておきます。ドメインネームサーバ（DNS）のエントリによって、このFQDNが、ウィザードを使用して作成するHAグループの仮想IP（VIP）アドレスにマッピングされます。

S3仮想ホスト形式の要求を使用する場合は、をインストールしておく必要があります "S3エンドポイントのドメイン名が設定されました"。仮想ホスト形式の要求を使用することを推奨します。

ロードバランサとセキュリティ証明書の要件を確認します

StorageGRID ロードバランサを使用する場合は、ロードバランシングに関する一般的な考慮事項を確認しておきます。アップロードする証明書、または証明書の生成に必要な値を用意しておきます。

外部（サードパーティ）のロードバランサエンドポイントを使用する場合は、そのロードバランサの完全修飾ドメイン名（FQDN）、ポート、および証明書が必要です。

グリッドフェデレーション接続を設定します

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、ウィザードを開始する前に次の点を確認してください。

- 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。

S3セットアップウィザードにアクセスして実行します

S3セットアップウィザードを使用して、S3アプリケーションで使用するStorageGRIDを設定できます。セットアップウィザードには、StorageGRID バケットへのアクセスとオブジェクトの保存に必要な値が表示されます。

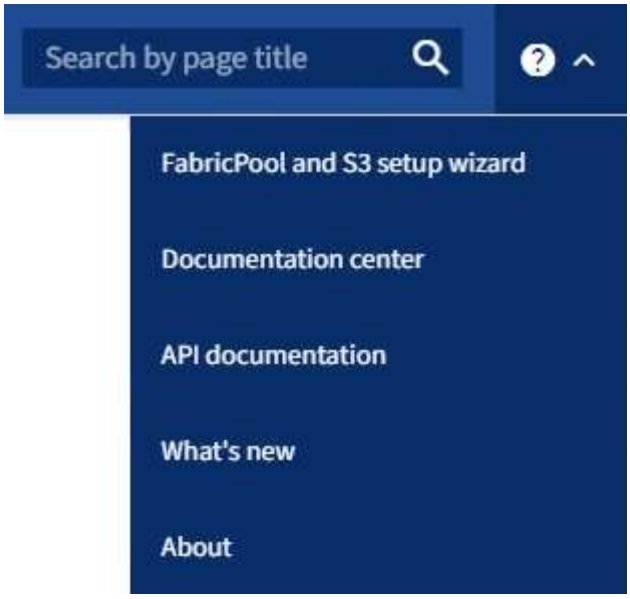
作業を開始する前に

- を使用することができます "rootアクセス権限"。
- を確認しておきます "考慮事項と要件" ウィザードを使用します。

ウィザードにアクセスします

手順

1. 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"。
2. ダッシュボードに「FabricPool and S3 setup wizard」バナーが表示された場合は、バナー内のリンクを選択します。バナーが表示されなくなった場合は、グリッドマネージャのヘッダーバーでヘルプアイコンを選択し、 FabricPool and S3 setup wizard *を選択します。



3. FabricPool とS3のセットアップウィザードのページのS3アプリケーションセクションで、*今すぐ設定*を選択します。

手順**1/6**：**HA**グループを設定する

HAグループは、それぞれにStorageGRID ロードバランササービスが含まれるノードの集まりです。HAグループには、ゲートウェイノード、管理ノード、またはその両方を含めることができます。

HAグループを使用すると、S3データ接続の可用性を維持できます。HAグループのアクティブインターフェイスで障害が発生しても、バックアップインターフェイスでワークロードを管理できるため、S3処理への影響はほとんどありません。

このタスクの詳細については、を参照してください "ハイアベイラビリティグループを管理します"。

手順

1. 外部のロードバランサを使用する場合は、HAグループを作成する必要はありません。[Skip this step]*を選択し、に進みます [手順2/6：ロードバランサエンドポイントを設定します]。
2. StorageGRID ロードバランサを使用するには、新しいHAグループを作成するか、既存のHAグループを使用します。

HA グループを作成します

a. 新しいHAグループを作成するには、*[HAグループの作成]*を選択します。

b. [詳細を入力]*ステップで、次のフィールドに値を入力します。

フィールド	説明
HAグループ名	このHAグループの一意の表示名。
概要 （オプション）	このHAグループの概要 。

c. [インターフェイスの追加]*手順で、このHAグループで使用するノードインターフェイスを選択します。

列ヘッダーを使用して行をソートするか、検索キーワードを入力してインターフェイスをより迅速に検索します。

ノードは1つ以上選択できますが、ノードごとに選択できるインターフェイスは1つだけです。

d. [* prioritize interfaces]ステップでは、このHAグループのプライマリインターフェイスとバックアップインターフェイスを決定します。

行をドラッグして、*優先順位*列の値を変更します。

リストの最初のインターフェイスはプライマリインターフェイスです。プライマリインターフェイスは、障害が発生しないかぎり、アクティブインターフェイスです。

HAグループに複数のインターフェイスが含まれていて、アクティブインターフェイスで障害が発生した場合、仮想IP（VIP）アドレスは優先順位に従って最初のバックアップインターフェイスに移動します。そのインターフェイスに障害が発生すると、 VIP アドレスは次のバックアップインターフェイスに移動します。障害が解決されると、VIPアドレスは使用可能な最もプライオリティの高いインターフェイスに戻ります。

e. [IPアドレスの入力]*ステップで、次のフィールドに値を入力します。

フィールド	説明
サブネットCIDR	VIPサブネットのアドレス（CIDR表記）。IPv4アドレス、スラッシュ、およびサブネットの長さ（0～32）。 ネットワークアドレスにホストビットを設定しないでください。例： `192.16.0.0/22`。
ゲートウェイIPアドレス（オプション）	StorageGRID へのアクセスに使用するS3 IPアドレスがStorageGRID VIPアドレスと同じサブネットにない場合は、StorageGRID VIPローカルゲートウェイのIPアドレスを入力します。ローカルゲートウェイの IP アドレスは VIP サブネット内にある必要があります。

フィールド	説明
仮想IPアドレス	HAグループ内のアクティブインターフェイスのVIPアドレスを1つ以上10個以下で入力します。すべてのVIPアドレスがVIPサブネット内にある必要があります。 IPv4アドレスを少なくとも1つ指定する必要があります。必要に応じて、追加の IPv4 アドレスと IPv6 アドレスを指定できます。

f. を選択し、[終了]*を選択してS3セットアップウィザードに戻ります。

g. [続行]*を選択して、ロードバランサの手順に進みます。

既存の**HA**グループを使用する

a. 既存のHAグループを使用するには、*[HAグループの選択]*からHAグループ名を選択します。

b. [続行]*を選択して、ロードバランサの手順に進みます。

手順**2/6**：ロードバランサエンドポイントを設定します

StorageGRID は、ロードバランサを使用してクライアントアプリケーションからワークロードを管理します。ロードバランシングは、複数のストレージノードにわたって速度と接続容量を最大化します。

すべてのゲートウェイノードと管理ノードに存在するStorageGRID ロードバランササービスを使用することも、外部（サードパーティ）のロードバランサに接続することもできます。StorageGRID ロードバランサを使用することを推奨します。

このタスクの詳細については、を参照してください "ロードバランシングに関する考慮事項"。

StorageGRID ロードバランササービスを使用するには、* StorageGRID load balancer タブを選択し、使用するロードバランサエンドポイントを作成または選択します。外部ロードバランサを使用するには、[外部ロードバランサ]*タブを選択し、設定済みのシステムに関する詳細を入力します。

エンドポイントを作成します

手順

1. ロードバランサエンドポイントを作成するには、*[エンドポイントの作成]*を選択します。
2. Enter endpoint details *ステップで、次のフィールドに値を入力します。

フィールド	説明
名前	エンドポイントのわかりやすい名前。
ポート	ロードバランシングに使用する StorageGRID ポート。最初に作成するエンドポイントのデフォルトは10433ですが、未使用の外部ポートを入力できます。80または443を入力すると、ゲートウェイノードでのみエンドポイントが設定されます。これらのポートは管理ノードで予約されているためです。 *注：*他のグリッドサービスで使用されるポートは許可されません。を参照してください"ネットワークポートのリファレンス"。
クライアントタイプ	は* S3 *にする必要があります。
ネットワークプロトコル	[**HTTPS**] を選択します。 注：TLS暗号化なしでのStorageGRID との通信はサポートされていますが、推奨されません。

3. [結合モードの選択]ステップで、結合モードを指定します。バインドモードは、任意のIPアドレスまたは特定のIPアドレスとネットワークインターフェイスを使用してエンドポイントにアクセスする方法を制御します。

オプション	説明
グローバル（デフォルト）	クライアントは、任意のゲートウェイノードまたは管理ノードのIPアドレス、任意のネットワーク上の任意のHAグループの仮想IP（VIP）アドレス、または対応するFQDNを使用して、エンドポイントにアクセスできます。 このエンドポイントのアクセスを制限する必要がある場合を除き、 * グローバル * 設定（デフォルト）を使用します。
HA グループの仮想 IP	クライアントがこのエンドポイントにアクセスするには、HAグループの仮想IPアドレス（または対応するFQDN）を使用する必要があります。 このバインドモードのエンドポイントでは、エンドポイント用に選択したHAグループが重複しないかぎり、すべて同じポート番号を使用できます。

オプション	説明
ノードインターフェイス	クライアントがこのエンドポイントにアクセスするには、選択したノードインターフェイスのIPアドレス（または対応するFQDN）を使用する必要があります。
ノードタイプ	選択したノードのタイプに基づいて、クライアントがこのエンドポイントにアクセスするには、いずれかの管理ノードのIPアドレス（または対応するFQDN）か、いずれかのゲートウェイノードのIPアドレス（または対応するFQDN）を使用する必要があります。

4. [Tenant access]ステップで、次のいずれかを選択します。

フィールド	説明
Allow all tenants（デフォルト）	すべてのテナントアカウントは、このエンドポイントを使用してバケットにアクセスできます。
選択したテナントを許可します	このエンドポイントを使用してバケットにアクセスできるのは、選択したテナントアカウントのみです。
選択したテナントをブロックします	選択したテナントアカウントは、このエンドポイントを使用してバケットにアクセスできません。他のすべてのテナントでこのエンドポイントを使用できます。

5. [証明書の添付]*ステップで、次のいずれかを選択します。

フィールド	説明
証明書のアップロード（推奨）	このオプションは、CA署名済みサーバ証明書、証明書秘密鍵、およびオプションのCAバンドルをアップロードする場合に使用します。
証明書の生成	このオプションは、自己署名証明書を生成する場合に使用します。を参照してください "ロードバランサエンドポイントを設定する" を参照してください。
StorageGRID S3およびSwift証明書を使用する	このオプションは、StorageGRID グローバル証明書のカスタムバージョンをすでにアップロードまたは生成している場合にのみ使用します。を参照してください "S3 および Swift API 証明書を設定する" を参照してください。

6. [Finish]*を選択してS3セットアップウィザードに戻ります。
7. [続行]*を選択してテナントとバケットの手順に進みます。

エンドポイント証明書の変更がすべてのノードに適用されるまでに最大 15 分かかることがあります。

既存のロードバランサエンドポイントを使用する

手順

1. 既存のエンドポイントを使用する場合は、*[ロードバランサエンドポイントの選択]*からそのエンドポイントの名前を選択します。
2. [続行]*を選択してテナントとバケットの手順に進みます。

外部のロードバランサを使用する

手順

1. 外部のロードバランサを使用するには、次のフィールドに値を入力します。

フィールド	説明
FQDN	外部ロードバランサの完全修飾ドメイン名（FQDN）。
ポート	S3アプリケーションが外部ロードバランサへの接続に使用するポート番号。
証明書	外部ロードバランサのサーバ証明書をコピーして、このフィールドに貼り付けます。

2. [続行]*を選択してテナントとバケットの手順に進みます。

ステップ**3 / 6**：テナントとバケットを作成

テナントは、S3アプリケーションを使用してStorageGRID でオブジェクトの格納と読み出しを行うことができるエンティティです。各テナントには、独自のユーザ、アクセスキー、バケット、オブジェクト、および特定の機能セットがあります。S3アプリケーションがオブジェクトの格納に使用するバケットを作成する前に、テナントを作成する必要があります。

バケットは、テナントのオブジェクトとオブジェクトメタデータを格納するためのコンテナです。一部のテナントには多数のバケットが含まれている場合もありますが、このウィザードを使用すると、テナントとバケットを最も簡単かつ迅速に作成できます。Tenant Managerは、あとで必要なバケットを追加するために使用できます。

このS3アプリケーションで使用する新しいテナントを作成できます。必要に応じて、新しいテナント用のバケットを作成することもできます。最後に、ウィザードでテナントのrootユーザのS3アクセスキーを作成できます。

このタスクの詳細については、を参照してください "テナントアカウントを作成する" および"S3 バケットを作成する"。

手順

1. [テナントの作成] を選択します。
2. [Enter details]ステップで、次の情報を入力します。

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。
概要 （オプション）	テナントの特定に役立つ概要 。
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セットアップウィザードでは、* S3 *が選択され、フィールドは無効になっています。
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、クォータとユニットの数値。

3. 「 * Continue * 」を選択します。
4. 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。

アクセス権	選択した項目
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"。 注：[Use grid federation connection]*は、新しいS3テナントを作成する場合にのみ選択できます。既存のテナントに対してこの権限を選択することはできません。

5. [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。
6. StorageGRID システムでが使用されてい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 "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。

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。

7. ルートユーザのアクセスキーIDとシークレットアクセスキーをウィザードで作成する場合は、* Create root user S3 access key automatically *を選択します。

> テナントのユーザをrootユーザだけにする場合は、このオプションを選択します。他のユーザがこのテナントを使用する場合は、Tenant Managerを使用してキーと権限を設定します。

8. 「 * Continue * 」を選択します。
9. [Create bucket]手順では、必要に応じてテナントのオブジェクト用のバケットを作成します。それ以外の場合は、*[Create tenant without bucket]*を選択してに移動します データステップをダウンロードします。

グリッドでS3オブジェクトロックが有効になっている場合、この手順で作成したバケットではS3オブジェクトロックが有効になりません。このS3アプリケーションにS3オブジェクトロックバケットを使用する必要がある場合は、*[Create tenant without bucket]*を選択します。次に、Tenant Managerを使用してを実行します "バケットを作成します" 代わりに、

a. S3アプリケーションが使用するバケットの名前を入力します。例： `S3-bucket`。

バケットの作成後にバケット名を変更することはできません。

b. このバケットの*[Region]*を選択します。

将来ILMを使用してバケットのリージョンに基づいてオブジェクトをフィルタリングする予定がないかぎり、デフォルトのリージョン（us-east-1）を使用します。

c. このバケットに各オブジェクトの各バージョンを格納する場合は、*[オブジェクトのバージョン管理を有効にする]*を選択します。

d. [Create tenant and bucket]*を選択し、データのダウンロード手順に進みます。

ステップ**4/6**：データをダウンロードします

ダウンロードデータステップでは、1つまたは2つのファイルをダウンロードして、設定した内容の詳細を保存できます。

手順

1. [Create root user S3 access key automatically]*を選択した場合は、次のいずれかまたは両方を実行します。
   - Download access keys（アクセスキーのダウンロード）*を選択してをダウンロードします `.csv` テナントアカウント名、アクセスキーID、シークレットアクセスキーを含むファイル。
   - コピーアイコン（）をクリックして、アクセスキーIDとシークレットアクセスキーをクリップボードにコピーします。
2. [Download configuration values]*を選択してをダウンロードします `.txt` ロードバランサエンドポイント、テナント、バケット、およびrootユーザの設定を含むファイル。
3. この情報を安全な場所に保存してください。

両方のアクセスキーをコピーするまで、このページを閉じないでください。このページを閉じると、キーは使用できなくなります。この情報はStorageGRID システムからデータを取得するために使用できるため、必ず安全な場所に保存してください。

4. プロンプトが表示されたら、チェックボックスをオンにして、キーをダウンロードまたはコピーしたことを確認します。
5. [続行]*を選択してILMルールとポリシーの手順に進みます。

手順**5 / 6**：**S3**の**ILM**ルールと**ILM**ポリシーを確認します

情報ライフサイクル管理（ILM）ルールは、StorageGRID システム内のすべてのオブジェクトの配置、期間、取り込み動作を制御します。StorageGRID に含まれているILMポリシーは、すべてのオブジェクトのレプリケートコピーを2つ作成します。このポリシーは、新しいドラフトポリシーを作成してアクティブ化するまで有効です。

手順

1. ページに表示された情報を確認します。
2. 新しいテナントまたはバケットに属するオブジェクトに対する具体的な手順を追加する場合は、新しいルールと新しいポリシーを作成します。を参照してください "ILM ルールを作成する" および "Create ILM policy ：概要"。
3. [I have review these steps and understand what I need to do]*を選択します。
4. チェックボックスをオンにして、次に何をすべきかを理解していることを示します。
5. を選択して[概要]*に進みます。

ステップ**6 / 6**：概要を確認します

手順

1. 概要を確認します。
2. 次の手順の詳細をメモしておいてください。S3クライアントに接続する前に必要になる可能性がある追加の設定について説明しています。たとえば、*[Sign in as root]*を選択するとTenant Managerに移動し、テナントユーザの追加、バケットの作成、バケットの設定の更新を行うことができます。
3. [完了] を選択します。
4. StorageGRID からダウンロードしたファイルまたは手動で取得した値を使用して、アプリケーションを設定します。

HAグループを管理します

ハイアベイラビリティ（ **HA** ）グループの管理：概要

複数の管理ノードとゲートウェイノードのネットワークインターフェイスをハイアベイラビリティ（ HA ）グループにまとめることができます。HA グループのアクティブインターフェイスで障害が発生した場合、バックアップインターフェイスがワークロードを管理できます。

HA グループとは何ですか？

ハイアベイラビリティ（ HA ）グループを使用して、 S3 / Swift クライアントに可用性の高いデータ接続を提供したり、 Grid Manager および Tenant Manager への可用性の高い接続を提供したりできます。

各 HA グループは、選択したノードの共有サービスへのアクセスを提供します。

- ゲートウェイノード、管理ノード、またはその両方を含む HA グループは、 S3 クライアントと Swift クライアントに可用性の高いデータ接続を提供します。
- 管理ノードだけで構成される HA グループは、 Grid Manager と Tenant Manager への可用性の高い接続を提供します。
- SG100 または SG1000 アプライアンスと VMware ベースのソフトウェアノードだけで構成された HA グループは、の可用性の高い接続を提供できます "S3 Select を使用する S3 テナント"。S3 Select を使用する場合は HA グループを推奨しますが、必須ではありません。

HA グループはどのように作成しますか？

1. 1 つ以上の管理ノードまたはゲートウェイノードのネットワークインターフェイスを選択します。ノードに追加したグリッドネットワーク（ eth0 ）インターフェイス、クライアントネットワーク（ eth2 ）インターフェイス、 VLAN インターフェイス、またはアクセスインターフェイスを使用できます。

   > DHCPによってIPアドレスが割り当てられたHAグループにインターフェイスを追加することはできません。

2. プライマリインターフェイスとして指定するインターフェイスは 1 つです。プライマリインターフェイスは、障害が発生しないかぎり、アクティブインターフェイスです。
3. バックアップインターフェイスの優先順位を決定します。
4. グループに仮想 IP （ VIP ）アドレスを 1 ～ 10 個割り当てます。クライアントアプリケーションは、これらの VIP アドレスのいずれかを使用して StorageGRID に接続できます。

手順については、を参照してください "ハイアベイラビリティグループを設定する"。

アクティブインターフェイスとは何ですか。

通常の運用中は、 HA グループのすべての VIP アドレスが優先順位の最初のインターフェイスであるプライマリインターフェイスに追加されます。プライマリインターフェイスが使用可能な状態であれば、クライアントがグループの任意の VIP アドレスに接続するときに使用されます。つまり、通常の動作中、プライマリ・インターフェイスはグループの「アクティブ」インターフェイスになります。

同様に、通常の動作中は、 HA グループのプライオリティの低いインターフェイスは「 backup 」インターフェイスとして機能します。これらのバックアップインターフェイスは、プライマリ（現在アクティブ）インターフェイスが使用できなくなるまで使用されません。

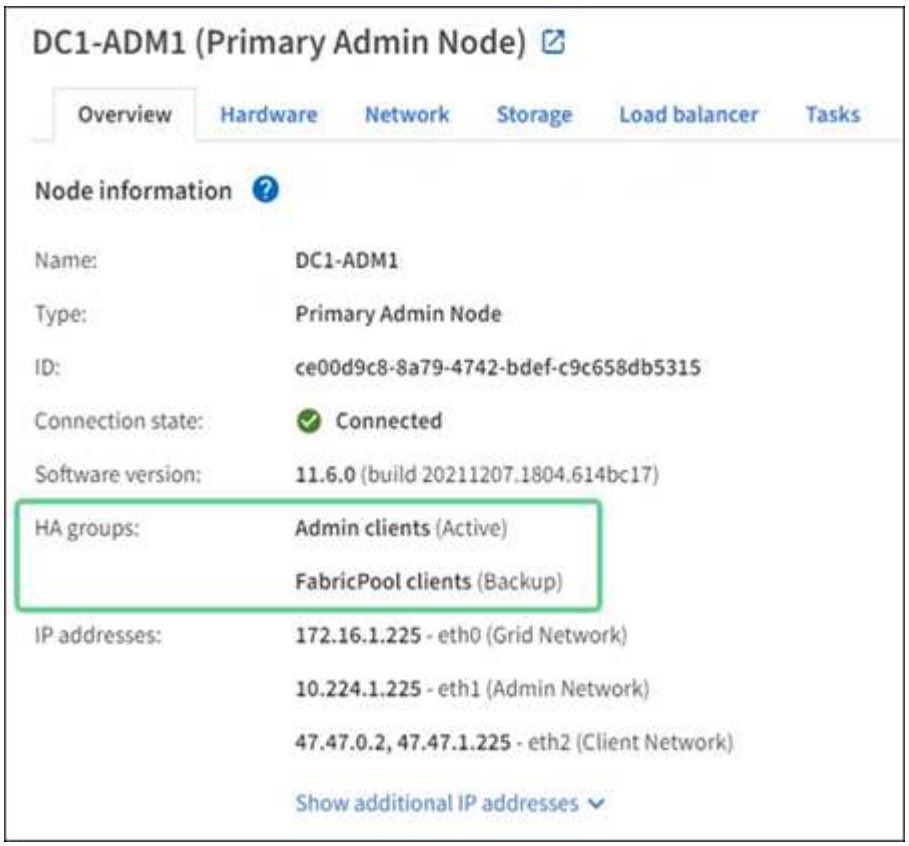
ノードの現在の HA グループのステータスを表示します

ノードが HA グループに割り当てられているかどうかを確認し、現在のステータスを確認するには、 * nodes * > * _node_name を選択します。

概要 * タブに HA グループ * のエントリが含まれている場合、そのノードは表示されている HA グループに割り当てられます。グループ名のあとの値は、 HA グループ内のノードの現在のステータスです。

- * Active * ： HA グループは現在このノードでホストされています。
- * バックアップ * ： HA グループは現在このノードを使用していません。バックアップインターフェイスです。
- 停止：ハイアベイラビリティ（キープアライブ）サービスが手動で停止されているため、このノードでHAグループをホストできません。
- 障害：次の1つ以上の理由により、このノードでHAグループをホストできません：
  - ロードバランサ（ nginx-gw ）サービスがノードで実行されていません。
  - ノードの eth0 または VIP インターフェイスが停止しています。
  - ノードは停止しています。

この例では、プライマリ管理ノードが 2 つの HA グループに追加されています。このノードは、現在、 FabricPool クライアントグループのアクティブインターフェイスであり、クライアントグループのバックアップインターフェイスです。



アクティブインターフェイスに障害が発生するとどうなりますか。

VIP アドレスを現在ホストしているインターフェイスは、アクティブインターフェイスです。HA グループに複数のインターフェイスが含まれている場合にアクティブインターフェイスで障害が発生すると、 VIP アドレスは優先順位に従って、使用可能な最初のバックアップインターフェイスに移動します。そのインターフェイスに障害が発生すると、使用可能な次のバックアップインターフェイスに VIP アドレスが移動します。

フェイルオーバーは、次のいずれかの理由でトリガーされる可能性があります。

- インターフェイスが設定されているノードが停止する。
- インターフェイスが設定されているノードと他のすべてのノードとの接続が少なくとも 2 分間失われます。
- アクティブインターフェイスが停止する。
- ロードバランササービスが停止する。
- ハイアベイラビリティサービスが停止します。

アクティブインターフェイスをホストするノードの外部でネットワーク障害が発生した場合、フェイルオーバーがトリガーされないことがあります。同様に、Grid ManagerまたはTenant Managerのサービスによってフェイルオーバーはトリガーされません。

フェイルオーバープロセスにかかる時間は通常数秒です。クライアントアプリケーションにほとんど影響がなく、通常の再試行で処理を続行できます。

障害が解決され、プライオリティの高いインターフェイスが再び使用可能になると、 VIP アドレスはプライオリティの高いインターフェイスに自動的に移動されます。

HA グループの用途

ハイアベイラビリティ（ HA ）グループを使用すると、オブジェクトデータ用および管理用に StorageGRID への可用性の高い接続を提供できます。

- HA グループは、 Grid Manager または Tenant Manager への可用性の高い管理接続を提供します。
- HA グループは、 S3 / Swift クライアントに可用性の高いデータ接続を提供できます。
- インターフェイスが 1 つしかない HA グループでは、多数の VIP アドレスを指定したり、 IPv6 アドレスを明示的に設定したりできます。

HA グループは、グループに含まれるすべてのノードが同じサービスを提供する場合にのみ高可用性を提供できます。HA グループを作成するときは、必要なサービスを提供するタイプのノードからインターフェイスを追加してください。

- * 管理ノード * ：ロードバランササービスが含まれ、 Grid Manager またはテナントマネージャへのアクセスを有効にします。
- ゲートウェイノード：ロードバランササービスが含まれます。

HA グループの目的	このタイプのノードを **HA** グループに追加します
Grid Manager へのアクセス	• プライマリ管理ノード（ * プライマリ * ） • 非プライマリ管理ノード • 注： * プライマリ管理ノードがプライマリインターフェイスである必要があります。一部のメンテナンス手順は、プライマリ管理ノードでしか実行できません。
Tenant Manager のみにアクセスします	• プライマリ管理ノードまたは非プライマリ管理ノード
S3 または Swift クライアントアクセス - ロードバランササービス	• 管理ノード • ゲートウェイノード
の S3 クライアントアクセス "S3 選択"	• SG100 または SG1000 アプライアンス • VMware ベースのソフトウェアノード • 注： S3 Select を使用する場合は HA グループを推奨しますが、必須ではありません。

Grid Manager または **Tenant Manager** で **HA** グループを使用する場合の制限事項

Grid Manager サービスまたは Tenant Manager サービスに障害が発生した場合は、 HA グループのフェイルオーバーはトリガーされません。

フェイルオーバーの発生時に Grid Manager または Tenant Manager にサインインしている場合はサインアウトされるため、再度サインインしてタスクを再開する必要があります。

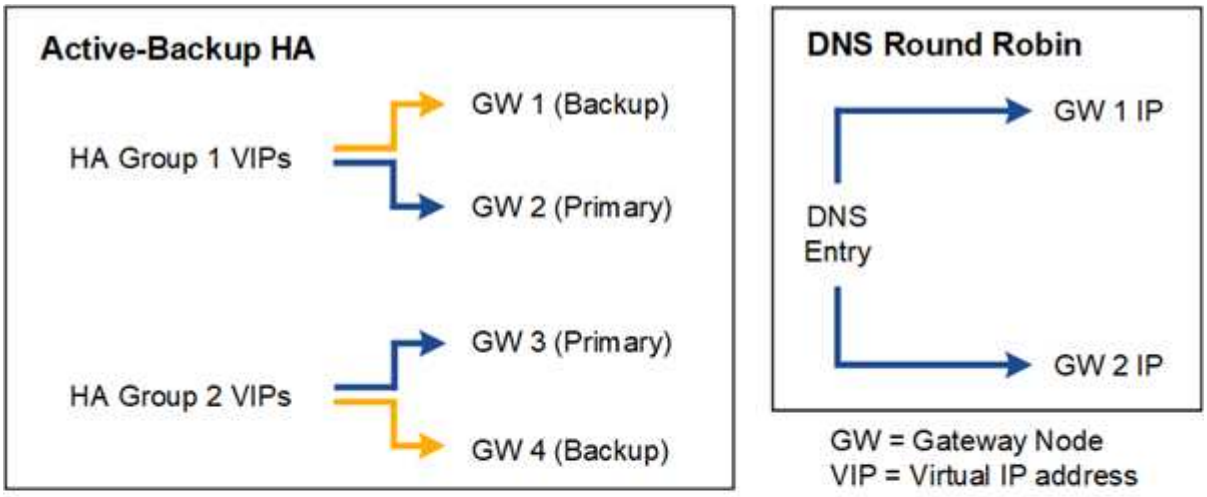
プライマリ管理ノードを使用できないと、一部のメンテナンス手順を実行できません。フェイルオーバー中

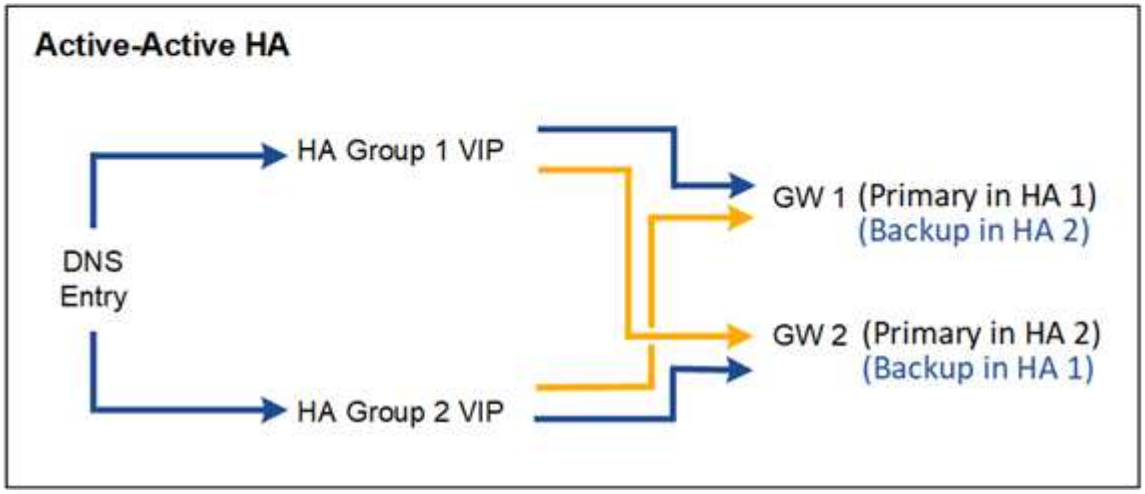
は、 Grid Manager を使用して StorageGRID システムを監視できます。

HA グループの設定オプション

次の図は、 HA グループのさまざまな構成例を示しています。各オプションには長所と短所があります。

次の図では、 HA グループのプライマリインターフェイスが青、 HA グループのバックアップインターフェイスが黄色で示されています。





次の表は、図に示す各 HA 構成のメリットをまとめたものです。

設定	利点	欠点
アクティブ / バックアップ HA	• StorageGRID で管理され、外部のコンポーネントを必要としません。 • 高速フェイルオーバー。	• HA グループ内の 1 つのノードだけがアクティブです。各 HA グループで少なくとも 1 つのノードがアイドル状態になります。

設定	利点	欠点
DNS ラウンドロビン	• 総スループットが向上します。 • アイドル状態のホストはありません。	• クライアントの動作によってはフェイルオーバーが低速になる可能性があります。 • StorageGRID の外部でハードウェアを構成する必要があります。 • ユーザによる健全性チェックが必要です。
アクティブ / アクティブ HA	• トラフィックが複数の HA グループに分散されます。 • HA グループの数が増えるほど総スループットが向上します。 • 高速フェイルオーバー。	• 設定がより複雑になります。 • StorageGRID の外部でハードウェアを構成する必要があります。 • ユーザによる健全性チェックが必要です。

ハイアベイラビリティグループを設定する

ハイアベイラビリティ（ HA ）グループを設定して、管理ノードまたはゲートウェイノード上のサービスへの可用性の高いアクセスを提供できます。

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"。
- Root アクセス権限が割り当てられている。
- HA グループで VLAN インターフェイスを使用する場合は、 VLAN インターフェイスを作成しておきます。を参照してください "VLAN インターフェイスを設定します"。
- HA グループ内のノードに対してアクセスインターフェイスを使用する場合は、インターフェイスを作成しておきます。
  - * Red Hat Enterprise Linux または CentOS （ノードのインストール前） * ： "ノード構成ファイルを作成"
  - * Ubuntu または Debian （ノードをインストールする前） * ： "ノード構成ファイルを作成"
  - * Linux （ノードのインストール後） * ： "Linux ：ノードにトランクインターフェイスまたはアクセスインターフェイスを追加します"
  - * VMware （ノードのインストール後） * ： "VMware ：ノードにトランクインターフェイスまたはアクセスインターフェイスを追加します"

ハイアベイラビリティグループを作成します

ハイアベイラビリティグループを作成する場合は、 1 つ以上のインターフェイスを選択して優先順位順に編成します。次に、グループに 1 つ以上の VIP アドレスを割り当てます。

HA グループに含まれるゲートウェイノードまたは管理ノードのインターフェイスを指定する必要があります。HA グループでは、 1 つのノードに対して使用できるインターフェイスは 1 つだけですが、同じノードの他のインターフェイスは他の HA グループで使用できます。

ウィザードにアクセスします

手順

1. 構成 * > * ネットワーク * > * ハイアベイラビリティグループ * を選択します。
2. 「 * Create * 」を選択します。

HA グループの詳細を入力します

手順

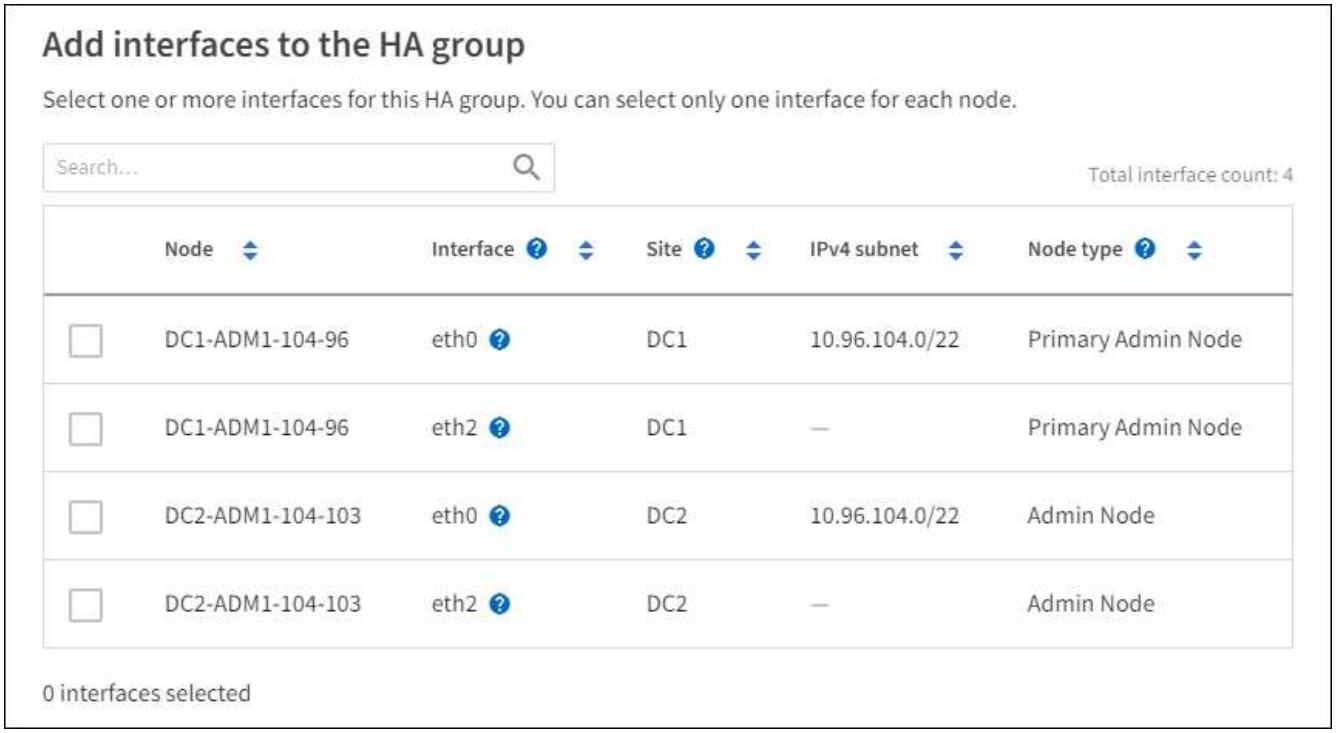
1. HA グループの一意の名前を指定してください。
2. 必要に応じて、 HA グループの概要 を入力します。
3. 「 * Continue * 」を選択します。

HA グループにインターフェイスを追加します

手順

1. この HA グループに追加するインターフェイスを 1 つ以上選択してください。

   列ヘッダーを使用して行をソートするか、検索キーワードを入力してインターフェイスをより迅速に検索します。

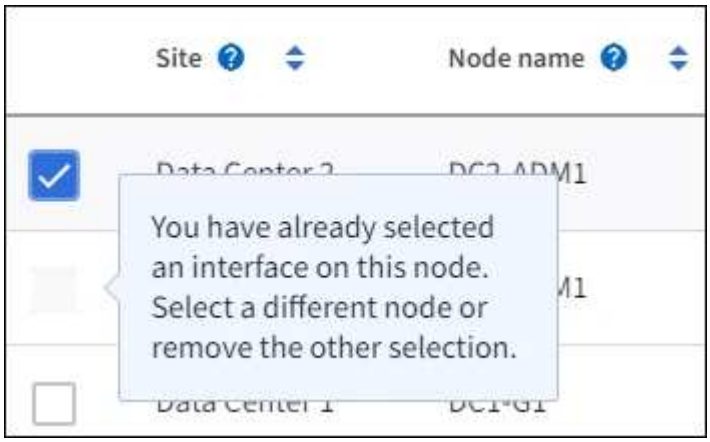


   VLAN インターフェイスを作成したら、新しいインターフェイスがテーブルに表示されるまで最大 5 分間待ちます。

インターフェイスの選択に関するガイドライン

- インターフェイスを少なくとも 1 つ選択してください。
- ノードに対して選択できるインターフェイスは 1 つだけです。

- HA グループがグリッドマネージャとテナントマネージャを含む管理ノードサービスの HA 保護用である場合は、管理ノード上のインターフェイスのみを選択します。
- HA グループが S3 または Swift クライアントトラフィックの HA 保護のためのものである場合は、管理ノード、ゲートウェイノード、またはその両方のインターフェイスを選択します。
- 異なるタイプのノード上のインターフェイスを選択した場合は、情報メモが表示されます。フェイルオーバーが発生すると、以前にアクティブだったノードから提供されたサービスを、新たにアクティブになったノードで使用できなくなる可能性があります。たとえば、バックアップゲートウェイノードは管理ノードサービスのHA保護を提供できません。同様に、バックアップ管理ノードでは、プライマリ管理ノードが提供するすべてのメンテナンス手順を実行できません。
- インターフェイスを選択できない場合、そのチェックボックスは無効になります。詳細については、ツールヒントを参照してください。



- サブネット値またはゲートウェイが選択した別のインターフェイスと競合している場合は、インターフェイスを選択できません。
- 静的IPアドレスが設定されていないインターフェイスは選択できません。

2. 「 * Continue * 」を選択します。

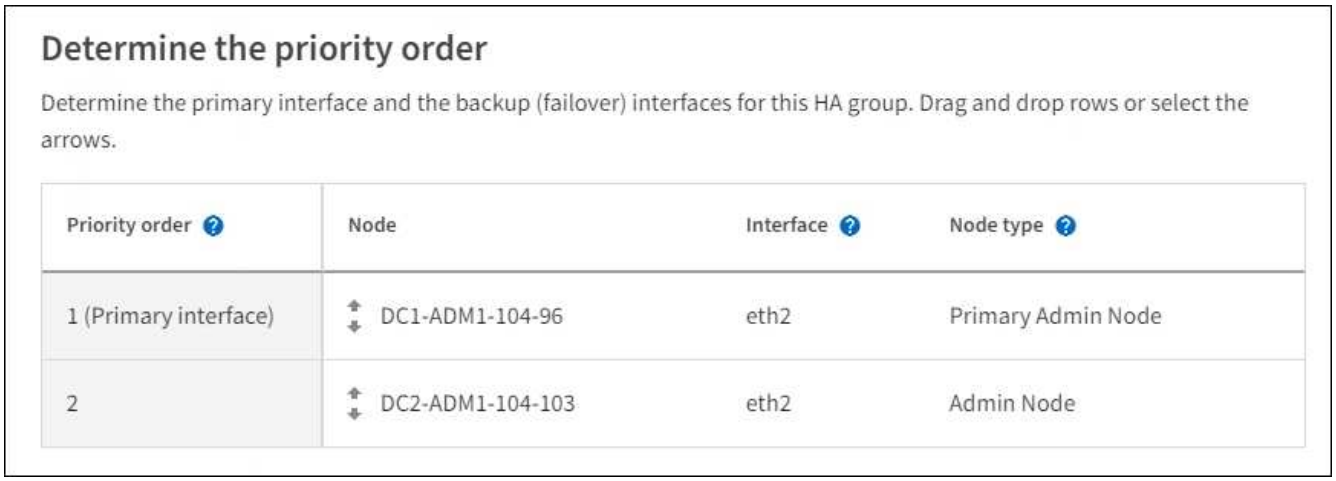
優先順位を決定します

HAグループに複数のインターフェイスが含まれている場合は、プライマリインターフェイスとバックアップ（フェイルオーバー）インターフェイスを判別できます。プライマリインターフェイスに障害が発生すると、VIPアドレスは使用可能な最もプライオリティの高いインターフェイスに移動します。そのインターフェイスに障害が発生すると、 VIP アドレスは次に優先度の高いインターフェイスに移動します。

手順

1. 優先順位*列の行をドラッグして、プライマリインターフェイスとバックアップインターフェイスを決定します。

   リストの最初のインターフェイスはプライマリインターフェイスです。プライマリインターフェイスは、障害が発生しないかぎり、アクティブインターフェイスです。



HA グループが Grid Manager へのアクセスを提供する場合は、プライマリ管理ノード上のインターフェイスを選択してプライマリインターフェイスにする必要があります。一部のメンテナンス手順は、プライマリ管理ノードでしか実行できません。

2. 「 * Continue * 」を選択します。

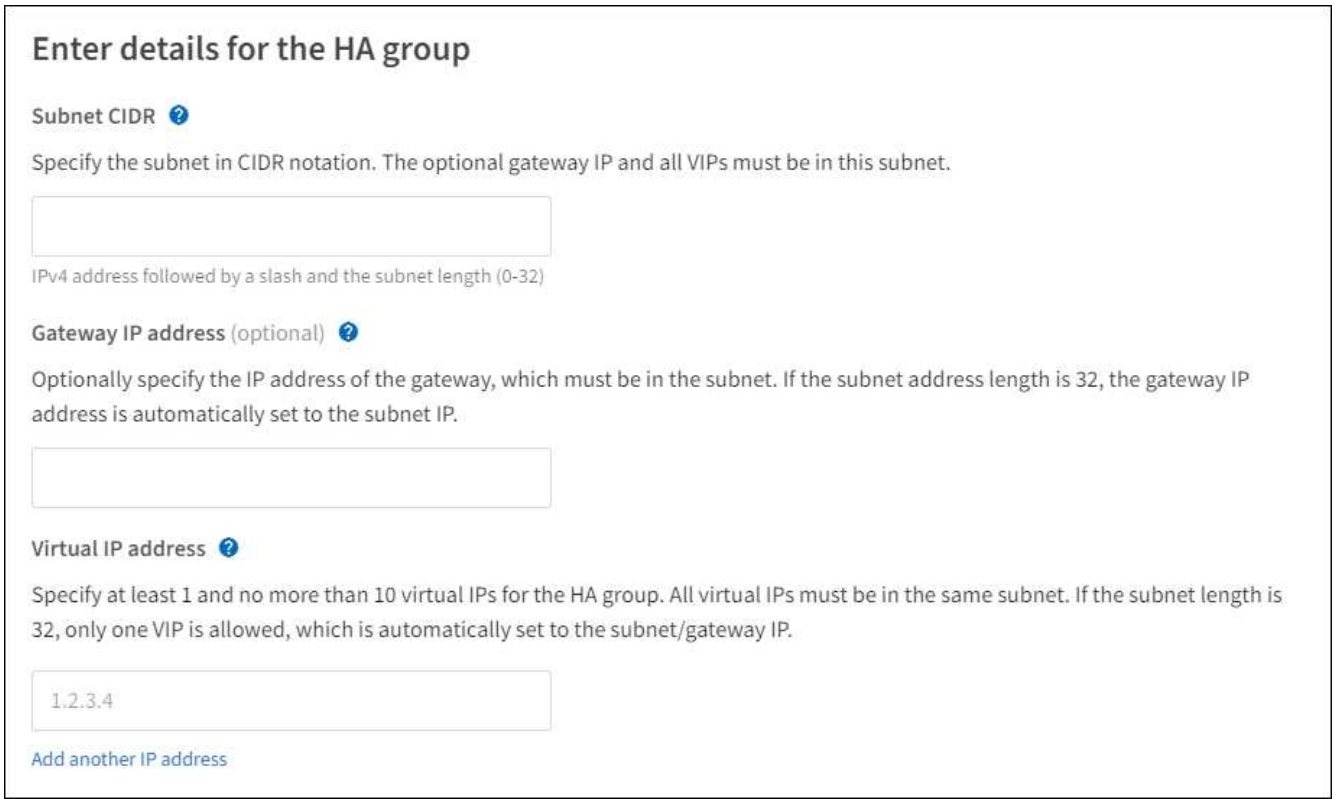
IP アドレスを入力してください

手順

1. [* Subnet CIDR*] フィールドで、 CIDR 表記の VIP サブネット（ IPv4 アドレスの後にスラッシュとサブネットの長さ（ 0 ～ 32 ）を指定します。

   ネットワークアドレスにホストビットを設定しないでください。例： `192.16.0.0/22`。

   32 ビットプレフィックスを使用する場合、 VIP ネットワークアドレスはゲートウェイアドレスおよび VIP アドレスとしても機能します。



2. 必要に応じて、 S3 、 Swift 、管理またはテナントクライアントが別のサブネットからこれらの VIP アドレスにアクセスする場合は、 * ゲートウェイ IP アドレス * を入力します。ゲートウェイアドレスは VIP サブネット内に設定する必要があります。

   クライアントと管理者のユーザは、このゲートウェイを使用して仮想 IP アドレスにアクセスします。

3. HAグループ内のアクティブインターフェイスのVIPアドレスを1つ以上10個以下で入力します。すべてのVIPアドレスはVIPサブネット内に存在する必要があり、すべてがアクティブインターフェイス上で同時にアクティブになります。

   IPv4 アドレスを少なくとも 1 つ指定する必要があります。必要に応じて、追加の IPv4 アドレスと IPv6 アドレスを指定できます。

4. HA グループの作成 * を選択し、 * 完了 * を選択します。

   HA グループが作成され、設定済みの仮想 IP アドレスを使用できるようになります。

HA グループへの変更がすべてのノードに適用されるまで最大 15 分待ちます。

次のステップ

この HA グループをロードバランシングに使用する場合は、ロードバランサエンドポイントを作成してポートとネットワークプロトコルを決定し、必要な証明書を接続します。を参照してください "ロードバランサエンドポイントを設定する"。

ハイアベイラビリティグループを編集します

ハイアベイラビリティ（ HA ）グループを編集して、グループ名と概要 を変更したり、インターフェイスを追加または削除したり、優先順位を変更したり、仮想 IP アドレスを追加または更新したりできます。

たとえば、サイトまたはノードの運用停止手順 で、選択したインターフェイスに関連付けられているノードを削除する場合、 HA グループの編集が必要になることがあります。

手順

1. 構成 * > * ネットワーク * > * ハイアベイラビリティグループ * を選択します。

   ハイアベイラビリティグループページには、既存のすべての HA グループが表示されます。

2. 編集するHAグループのチェックボックスを選択します。
3. 更新する内容に基づいて、次のいずれかを実行します。
   - 仮想 IP アドレスを追加または削除するには、 * Actions * > * Edit virtual IP address * を選択します。
   - *Actions * > * Edit HA group * を選択して、グループ名または概要 を更新したり、インターフェイスを追加または削除したり、優先順位を変更したり、 VIP アドレスを追加または削除したりします。
4. [仮想 IP アドレスの編集 *] を選択した場合：
   a. HA グループの仮想 IP アドレスを更新します。
   b. [保存（ Save ）] を選択します。
   c. [完了] を選択します。
5. HA グループの編集 * を選択した場合：
   a. 必要に応じて、グループの名前または概要 を更新します。
   b. 必要に応じて、チェックボックスをオンまたはオフにしてインターフェイスを追加または削除します。

      HA グループが Grid Manager へのアクセスを提供する場合は、プライマリ管理ノード上のインターフェイスを選択してプライマリインターフェイスにする必要があります。一部のメンテナンス手順は、プライマリ管理ノードでしか実行できません

   c. 必要に応じて、行をドラッグして、このHAグループのプライマリインターフェイスとバックアップインターフェイスの優先順位を変更します。
   d. 必要に応じて、仮想 IP アドレスを更新します。
   e. [保存（ Save ）] を選択し、 [完了（ Finish ）] を選択します。

HA グループへの変更がすべてのノードに適用されるまで最大 15 分待ちます。

ハイアベイラビリティグループを削除する

ハイアベイラビリティ（ HA ）グループは一度に 1 つ以上削除できます。

ロードバランサエンドポイントにバインドされているHAグループは削除できません。HAグループを削除するには、そのグループを使用しているすべてのロードバランサエンドポイントからそのグループを削除する必要があります。

クライアントの停止を回避するには、 HA グループを削除する前に、影響を受ける S3 または Swift クライアントアプリケーションを更新します。各クライアントを更新して、別の IP アドレスを使用して接続します。たとえば、別の HA グループの仮想 IP アドレスや、インストール時にインターフェイスに設定された IP アドレスなどです。

手順

1. 構成 * > * ネットワーク * > * ハイアベイラビリティグループ * を選択します。
2. 削除する各HAグループの*[ロードバランサエンドポイント]*列を確認します。ロードバランサエンドポイントが表示されている場合：
   a. **>**[ネットワーク]**>**[ロードバランサエンドポイント]*の順に選択します。
   b. エンドポイントのチェックボックスを選択します。
   c. [* アクション * （ Actions * ）] > [* エンドポイントバインドモードの編集（ Edit Endpoint binding mode ）]
   d. バインドモードを更新してHAグループを削除します。
   e. 「変更を保存」を選択します。
3. ロードバランサエンドポイントが表示されない場合は、削除する各HAグループのチェックボックスを選択します。
4. **>**[HAグループの削除]*を選択します。
5. メッセージを確認し、「 * HA グループを削除」を選択して選択を確認します。

   選択したすべての HA グループが削除されます。ハイアベイラビリティグループのページに、成功を示す緑色のバナーが表示されます。

負荷分散の管理

ロードバランシングに関する考慮事項

ロードバランシングを使用して、S3およびSwiftクライアントからの取り込みと読み出しのワークロードを処理できます。

ロードバランシングとは何ですか？

クライアントアプリケーションがStorageGRID システムでデータを保存または取得する際、StorageGRID はロードバランサを使用して取り込みと読み出しのワークロードを管理します。ロードバランシングは、複数のストレージノードにワークロードを分散することで、速度と接続容量を最大化します。

StorageGRID ロードバランササービスはすべての管理ノードとすべてのゲートウェイノードにインストールされ、レイヤ 7 のロードバランシングを提供します。クライアント要求の Transport Layer Security （ TLS ）終了を実行し、要求を検査し、ストレージノードへの新しいセキュアな接続を確立します。

各ノード上のロードバランササービスは、クライアントトラフィックをストレージノードに転送する際に独立して動作します。重み付きのプロセスを使用すると、ロードバランササービスは、より多くの要求をより多くの CPU を使用可能なストレージノードにルーティングします。

推奨されるロードバランシングメカニズムは StorageGRID ロードバランササービスですが、代わりにサードパーティのロードバランサを統合することもできます。詳細については、ネットアップの担当者にお問い合わせいただくか、を参照してください "TR-4626 ：『 StorageGRID Third-party and global load balancers 』"。

必要なロードバランシングノードの数

一般的なベストプラクティスとして、 StorageGRID システムの各サイトにロードバランササービスを使用するノードが 2 つ以上必要です。たとえば、サイトに 2 つのゲートウェイノード、または管理ノードとゲートウェイノードの両方が含まれているとします。SG100 または SG100 サービスアプライアンス、ベアメタルノード、仮想マシン（ VM ）ベースのノードのいずれを使用しているかに関係なく、各ロードバランシングノードに適切なネットワーク、ハードウェア、または仮想化インフラがあることを確認します。

ロードバランサエンドポイントとは何ですか？

ロードバランサエンドポイントは、ロードバランササービスを含むノードへのアクセスに送受信クライアントアプリケーション要求が使用するポートとネットワークプロトコル（HTTPSまたはHTTP）を定義します。エンドポイントは、クライアントタイプ（S3またはSwift）、バインドモード、および必要に応じて許可またはブロックされたテナントのリストも定義します。

ロードバランサエンドポイントを作成するには、* configuration > Network > Load balancer endpoints *を選択するか、FabricPool and S3のセットアップウィザードを実行します。手順：

- "ロードバランサエンドポイントを設定する"
- "S3セットアップウィザードを使用します"
- "FabricPool セットアップウィザードを使用します"

ポートに関する考慮事項

ロードバランサエンドポイントのポートは、最初に作成するエンドポイントのデフォルトで10433になりますが、未使用の外部ポートを1~65535の範囲で指定できます。ポート80または443を使用する場合、エンドポイントはゲートウェイノード上のロードバランササービスのみを使用します。これらのポートは管理ノードで予約されています。複数のエンドポイントに同じポートを使用する場合は、エンドポイントごとに異なるバインディングモードを指定する必要があります。

他のグリッドサービスで使用されているポートは許可されません。を参照してください "ネットワークポートのリファレンス"。

ネットワークプロトコルに関する考慮事項

ほとんどの場合、クライアントアプリケーションとStorageGRID の間の接続では、Transport Layer Security（TLS）暗号化を使用する必要があります。TLS暗号化を使用せずにStorageGRID に接続することはサポートされていますが、特に本番環境では推奨されません。StorageGRID ロードバランサエンドポイントのネットワークプロトコルを選択する場合は、*[HTTPS]*を選択する必要があります。

ロードバランサエンドポイント証明書に関する考慮事項

ロードバランサエンドポイントのネットワークプロトコルとして* HTTPS *を選択した場合は、セキュリティ証明書を指定する必要があります。ロードバランサエンドポイントの作成時には、次の3つのオプションのいずれかを使用できます。

- 署名済み証明書をアップロードする（推奨）。この証明書には、公的に信頼された認証局または民間の認証局（CA）が署名できます。一般に信頼されているCAサーバ証明書を使用して接続を保護することを推奨します。生成される証明書とは異なり、CAによって署名された証明書は無停止でローテーションでき、有効期限の問題を回避できます。

  ロードバランサエンドポイントを作成する前に、次のファイルを入手する必要があります。

- カスタムサーバ証明書ファイル。
- カスタムサーバ証明書の秘密鍵ファイル。
- 必要に応じて、各中間発行認証局の証明書のCAバンドル。

- 自己署名証明書の生成。
- グローバル**StorageGRID S3**および**Swift**証明書を使用します。この証明書をロードバランサエンドポイント用に選択するには、事前にこの証明書のカスタムバージョンをアップロードまたは生成する必要があります。を参照してください "S3 および Swift API 証明書を設定する"。

どのような価値が必要か？

証明書を作成するには、S3またはSwiftクライアントアプリケーションがエンドポイントへのアクセスに使用するすべてのドメイン名とIPアドレスを把握しておく必要があります。

証明書の*サブジェクトDN *（識別名）エントリには、クライアントアプリケーションがStorageGRID に使用する完全修飾ドメイン名が含まれている必要があります。例：

```
Subject DN:
/C=Country/ST=State/O=Company,Inc./CN=s3.storagegrid.example.com
```

必要に応じて、ワイルドカードを使用して、ロードバランササービスを実行しているすべての管理ノードおよびゲートウェイノードの完全修飾ドメイン名を表すことができます。例： `*.storagegrid.example.com` ワイルドカード*を使用して表します `adm1.storagegrid.example.com` および `gn1.storagegrid.example.com`。

S3仮想ホスト形式の要求を使用する場合は、証明書ごとに* Alternative Name *エントリも含める必要があります "S3エンドポイントのドメイン名" ワイルドカード名も含めて、を設定しておきます。例：

```
Alternative Name: DNS:*.s3.storagegrid.example.com
```

ドメイン名にワイルドカードを使用する場合は、を参照してください "サーバ証明書のセキュリティ強化ガイドライン"。

また、セキュリティ証明書の名前ごとにDNSエントリを定義する必要があります。

期限切れになる証明書の管理方法を教えてください。

S3アプリケーションとStorageGRID 間の接続の保護に使用した証明書の有効期限が切れると、アプリケーションからStorageGRID に一時的にアクセスできなくなる可能性があります。

証明書の有効期限の問題を回避するには、次のベストプラクティスに従ってください。

- 証明書の有効期限が近づいていることを警告するアラートがあれば、注意深く監視します。たとえば、* Expiration of load balancer endpoint certificate や Expiration of global server certificate for S3 and Swift API *アラートなどです。
- StorageGRID アプリケーションとS3アプリケーションの証明書のバージョンは常に同期しておいてくだ

さい。ロードバランサエンドポイントに使用する証明書を交換または更新する場合は、S3アプリケーションで使用される同等の証明書を交換または更新する必要があります。

- 公開署名されたCA証明書を使用する。CAによって署名された証明書を使用する場合は、有効期限が近い証明書を無停止で交換できます。
- 自己署名StorageGRID 証明書を生成した証明書の有効期限が近づいている場合は、既存の証明書の有効期限が切れる前に、StorageGRID とS3アプリケーションの両方で証明書を手動で置き換える必要があります。

バインディングモードに関する考慮事項

バインディングモードでは、ロードバランサエンドポイントへのアクセスに使用できるIPアドレスを制御できます。エンドポイントがバインディングモードを使用している場合、クライアントアプリケーションは、許可されたIPアドレスまたはそれに対応するFully Qualified Domain Name（FQDN；完全修飾ドメイン名）を使用している場合にのみ、エンドポイントにアクセスできます。他のIPアドレスまたはFQDNを使用するクライアントアプリケーションはエンドポイントにアクセスできません。

次のいずれかのバインディングモードを指定できます。

- グローバル（デフォルト）：クライアントアプリケーションは、任意のゲートウェイノードまたは管理ノードのIPアドレス、任意のネットワーク上の任意のHAグループの仮想IP（VIP）アドレス、または対応するFQDNを使用してエンドポイントにアクセスできます。エンドポイントのアクセスを制限する必要がないかぎり、この設定を使用します。
- * HAグループの仮想IP *。クライアントアプリケーションは、HAグループの仮想IPアドレス（または対応するFQDN）を使用する必要があります。
- ノードインターフェイス。クライアントは、選択したノードインターフェイスのIPアドレス（または対応するFQDN）を使用する必要があります。
- ノードタイプ。選択したノードのタイプに基づいて、クライアントは管理ノードのIPアドレス（または対応するFQDN）またはゲートウェイノードのIPアドレス（または対応するFQDN）のいずれかを使用する必要があります。

テナントアクセスに関する考慮事項

テナントアクセスは、ロードバランサエンドポイントを使用してバケットにアクセスできるStorageGRID テナントアカウントを制御できるオプションのセキュリティ機能です。すべてのテナントにエンドポイントへのアクセスを許可するか（デフォルト）、各エンドポイントで許可またはブロックされたテナントのリストを指定できます。

この機能を使用すると、テナントとそのエンドポイント間のセキュリティをより適切に分離できます。たとえば、この機能を使用して、あるテナントが所有する最高機密または高度に機密性の高いマテリアルに他のテナントから完全にアクセスできないようにすることができます。

> アクセス制御の目的では、クライアント要求で使用されたアクセスキーからテナントが決定されます。要求の一部としてアクセスキーが提供されていない場合（匿名アクセスなど）は、バケット所有者を使用してテナントが決定されます。

テナントアクセスの例

このセキュリティ機能の仕組みを理解するには、次の例を参考にしてください。

1. 次の2つのロードバランサエンドポイントを作成しておきます。

- *パブリック*エンドポイント：ポート10443を使用し、すべてのテナントへのアクセスを許可します。
- * Top secret * endpoint：ポート10444を使用し、* Top secret *テナントにのみアクセスを許可します。他のすべてのテナントはこのエンドポイントへのアクセスをブロックされます。

2. 。 `top-secret.pdf` は、* Top secret *テナントが所有するバケット内にあります。

にアクセスします `top-secret.pdf`、* Top secret *テナントのユーザは、にGET要求を問題 できます `https://w.x.y.z:10444/top-secret.pdf`。このテナントには10444エンドポイントの使用が許可されているため、ユーザはオブジェクトにアクセスできます。ただし、他のテナントに属するユーザが同じURLに対して同じ要求を発行すると、すぐに「Access Denied」というメッセージが表示されます。クレデンシャルと署名が有効であってもアクセスは拒否されます。

CPU の可用性

S3 / Swift トラフィックをストレージノードに転送する際、各管理ノードおよびゲートウェイノード上のロードバランササービスは独立して動作します。重み付きのプロセスを使用すると、ロードバランササービスは、より多くの要求をより多くの CPU を使用可能なストレージノードにルーティングします。ノード CPU 負荷情報は数分ごとに更新されますが、重み付けがより頻繁に更新される場合があります。ノードの使用率が 100% になった場合や、ノードの利用率のレポートに失敗した場合でも、すべてのストレージノードには最小限のベースとなる重みの値が割り当てられます。

CPU の可用性に関する情報が、ロードバランササービスが配置されているサイトに制限されている場合があります。

ロードバランサエンドポイントを設定する

ゲートウェイノードと管理ノードの StorageGRID ロードバランサに接続する際に使用できるポートとネットワークプロトコル S3 / Swift クライアントは、ロードバランサエンドポイントで決まります。

> 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

- 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"。
- Root アクセス権限が割り当てられている。
- を確認しておきます "ロードバランシングに関する考慮事項"。
- ロードバランサエンドポイントに使用するポートを再マッピングした場合は、を使用します "ポートの再マッピングを削除しました"。
- 使用するハイアベイラビリティ（ HA ）グループを作成しておきます。HA グループを推奨しますが、必須ではありません。を参照してください "ハイアベイラビリティグループを管理します"。
- ロードバランサエンドポイントがで使用される場合 "S3 Select 用の S3 テナント"ベアメタルノードの IP アドレスまたは FQDN を使用しないでください。S3 Select に使用するロードバランサエンドポイントには、 SG100 または SG1000 アプライアンスと VMware ベースのソフトウェアノードのみが許可されます。
- 使用する VLAN インターフェイスを設定しておきます。を参照してください "VLAN インターフェイスを設定します"。

- HTTPS エンドポイントを作成する場合（推奨）は、サーバ証明書の情報が必要です。

  エンドポイント証明書の変更がすべてのノードに適用されるまでに最大 15 分かかることがあります。

  - 証明書をアップロードするには、サーバ証明書、証明書の秘密鍵、および必要に応じて CA バンドルが必要です。
  - 証明書を生成するには、 S3 または Swift クライアントがエンドポイントへのアクセスに使用するすべてのドメイン名と IP アドレスが必要です。また、件名（識別名）も知っている必要があります。
  - StorageGRID の S3 および Swift API 証明書（ストレージノードへの直接の接続にも使用できます）を使用する場合は、デフォルトの証明書を外部の認証局によって署名されたカスタム証明書に置き換えておく必要があります。を参照してください"S3 および Swift API 証明書を設定する"。

ロードバランサエンドポイントを作成します

各ロードバランサエンドポイントは、ポート、クライアントタイプ（ S3 または Swift ）、およびネットワークプロトコル（ HTTP または HTTPS ）を指定します。

ウィザードにアクセスします

手順

1. [* configuration * > * Network * > * Load Balancer Endpoints *] を選択します。
2. 「 * Create * 」を選択します。

エンドポイントの詳細を入力します

手順

1. エンドポイントの詳細を入力します。

フィールド	説明
名前	エンドポイントのわかりやすい名前。ロードバランサエンドポイントのページのテーブルに表示されます。
ポート	ロードバランシングに使用する StorageGRID ポート。最初に作成するエンドポイントのデフォルトは10433ですが、1～65535の未使用の外部ポートを入力できます。 「 * 80 * 」または「 * 443 * 」と入力すると、エンドポイントはゲートウェイノードにのみ設定されます。これらのポートは管理ノードで予約されています。
クライアントタイプ	このエンドポイントを使用するクライアントアプリケーションのタイプ。 * S3 * または * Swift * 。

フィールド	説明
ネットワークプロトコル	クライアントがこのエンドポイントに接続するときに使用するネットワークプロトコル。 • セキュアな TLS 暗号化通信を実現するには、「 * HTTPS * 」を選択します（推奨）。エンドポイントを保存するには、セキュリティ証明書を接続する必要があります。 • セキュアで暗号化されていない通信を行うには、「 * HTTP 」を選択します非本番環境のグリッドにのみ HTTP を使用してください。

2. 「 * Continue * 」を選択します。

綴じモードを選択します

手順

1. 任意のIPアドレスまたは特定のIPアドレスとネットワークインターフェイスを使用してエンドポイントへのアクセス方法を制御するには、エンドポイントのバインドモードを選択します。

オプション	説明
グローバル（デフォルト）	クライアントは、任意のゲートウェイノードまたは管理ノードのIPアドレス、任意のネットワーク上の任意のHAグループの仮想IP（VIP）アドレス、または対応するFQDNを使用して、エンドポイントにアクセスできます。 このエンドポイントのアクセスを制限する必要がある場合を除き、 * グローバル * 設定（デフォルト）を使用します。
HA グループの仮想 IP	クライアントがこのエンドポイントにアクセスするには、HAグループの仮想IPアドレス（または対応するFQDN）を使用する必要があります。 このバインドモードのエンドポイントでは、エンドポイント用に選択したHAグループが重複しないかぎり、すべて同じポート番号を使用できます。
ノードインターフェイス	クライアントがこのエンドポイントにアクセスするには、選択したノードインターフェイスのIPアドレス（または対応するFQDN）を使用する必要があります。
ノードタイプ	選択したノードのタイプに基づいて、クライアントがこのエンドポイントにアクセスするには、いずれかの管理ノードのIPアドレス（または対応するFQDN）か、いずれかのゲートウェイノードのIPアドレス（または対応するFQDN）を使用する必要があります。

> 複数のエンドポイントが同じポートを使用する場合、StorageGRID はこの優先順位に従って、使用するエンドポイントを決定します。* HAグループの仮想IP **>***ノードインターフェイス>*ノードタイプ*>*グローバル*。

2. HA グループの仮想 IP * を選択した場合は、 1 つ以上の HA グループを選択します。

3. ノードインターフェイス * を選択した場合は、このエンドポイントに関連付ける管理ノードまたはゲートウェイノードごとに 1 つ以上のノードインターフェイスを選択します。
4. [ノードタイプ]*を選択した場合は、プライマリ管理ノードと非プライマリ管理ノードの両方を含む管理ノードまたはゲートウェイノードのいずれかを選択します。

テナントアクセスを制御

手順

1. [Tenant access]*ステップで、次のいずれかを選択します。

フィールド	説明
Allow all tenants（デフォルト）	すべてのテナントアカウントは、このエンドポイントを使用してバケットにアクセスできます。 テナントアカウントをまだ作成していない場合は、このオプションを選択する必要があります。テナントアカウントを追加したら、ロードバランサエンドポイントを編集して特定のアカウントを許可またはブロックできます。
選択したテナントを許可します	このエンドポイントを使用してバケットにアクセスできるのは、選択したテナントアカウントのみです。
選択したテナントをブロックします	選択したテナントアカウントは、このエンドポイントを使用してバケットにアクセスできません。他のすべてのテナントでこのエンドポイントを使用できます。

2. * HTTP *エンドポイントを作成する場合は、証明書を添付する必要はありません。Create * を選択して、新しいロードバランサエンドポイントを追加します。次に、に進みます 完了後。それ以外の場合は、「 * Continue * 」を選択して証明書を添付します。

証明書を添付します

手順

1. * HTTPS * エンドポイントを作成する場合は、エンドポイントに接続するセキュリティ証明書のタイプを選択します。

   この証明書は、 S3 および Swift クライアントと、管理ノードまたはゲートウェイノード上のロードバランササービスの間の接続を保護します。

   - * 証明書のアップロード * 。アップロードするカスタム証明書がある場合は、このオプションを選択します。
   - * 証明書の生成 * 。カスタム証明書の生成に必要な値がある場合は、このオプションを選択します。
   - * StorageGRID S3 および Swift 証明書を使用 * 。グローバルな S3 および Swift API 証明書を使用する場合は、このオプションを選択します。この証明書は、ストレージノードへの直接接続にも使用できます。

     このオプションは、グリッドCAによって署名されたデフォルトのS3およびSwift API証明書を、外部の認証局によって署名されたカスタム証明書に置き換えている場合を除き、選択できません。を参照し

てください"S3 および Swift API 証明書を設定する"。

2. StorageGRID S3およびSwift証明書を使用しない場合は、証明書をアップロードまたは生成します。

証明書をアップロードする

a. [証明書のアップロード] を選択します。

b. 必要なサーバ証明書ファイルをアップロードします。

- * サーバ証明書 * ： PEM エンコードのカスタムサーバ証明書ファイル。
- 証明書の秘密鍵：カスタムサーバ証明書の秘密鍵ファイル (`.key`）。

> EC 秘密鍵は 224 ビット以上である必要があります。RSA 秘密鍵は 2048 ビット以上にする必要があります。

- **CA Bundle** ：各中間発行認証局（ CA ）の証明書を含む単一のオプションファイル。このファイルには、 PEM でエンコードされた各 CA 証明書ファイルが、証明書チェーンの順序で連結して含まれている必要があります。

c. [* 証明書の詳細 *] を展開して、アップロードした各証明書のメタデータを表示します。オプションの CA バンドルをアップロードした場合は、各証明書が独自のタブに表示されます。

- 証明書ファイルを保存するには、 * 証明書のダウンロード * を選択します。証明書バンドルを保存するには、 * CA バンドルのダウンロード * を選択します。

  証明書ファイルの名前とダウンロード先を指定します。拡張子を付けてファイルを保存します `.pem`。

  例： `storagegrid_certificate.pem`

- 証明書の内容をコピーして他の場所に貼り付けるには、 * 証明書の PEM のコピー * または * CA バンドル PEM のコピー * を選択してください。

d. 「 * Create * 」を選択します。+ ロードバランサエンドポイントが作成された。カスタム証明書は、 S3 / Swift クライアントとエンドポイントの間の以降のすべての新しい接続に使用されます。

証明書の生成

a. [* 証明書の生成 *] を選択します。

b. 証明書情報を指定します。

フィールド	説明
ドメイン名	証明書に含める1つ以上の完全修飾ドメイン名。複数のドメイン名を表すには、ワイルドカードとして * を使用します。
IP	証明書に含める1つ以上のIPアドレス。
件名（オプション）	証明書所有者のX.509サブジェクト名または識別名（DN）。 このフィールドに値を入力しない場合、生成される証明書では、最初のドメイン名またはIPアドレスがサブジェクト共通名（CN）として使用されます。

フィールド	説明
有効な日数	作成後に証明書の有効期限が切れる日数。
キー使用の拡張機能を追加します	選択されている場合（デフォルトおよび推奨）、キー使用と拡張キー使用拡張が生成された証明書に追加されます。 これらの拡張機能は、証明書に含まれるキーの目的を定義します。 注:証明書にこれらの拡張機能が含まれている場合、古いクライアントで接続の問題が発生する場合を除き、このチェックボックスをオンのままにします。

c. [*Generate （生成）] を選択します

d. 生成された証明書のメタデータを表示するには、 [証明書の詳細] を選択します。

   - 証明書ファイルを保存するには、 [証明書のダウンロード] を選択します。

     証明書ファイルの名前とダウンロード先を指定します。拡張子を付けてファイルを保存します `.pem`。

     例： `storagegrid_certificate.pem`

   - 証明書の内容をコピーして他の場所に貼り付けるには、 * 証明書の PEM をコピー * を選択します。

e. 「 * Create * 」を選択します。

   ロードバランサエンドポイントが作成されます。カスタム証明書は、 S3 / Swift クライアントとこのエンドポイントの間の以降のすべての新しい接続に使用されます。

完了後

手順

1. DNSを使用する場合は、クライアントが接続に使用する各IPアドレスにStorageGRID の完全修飾ドメイン名（FQDN）を関連付けるレコードがDNSに含まれていることを確認します。

   DNS レコードに入力する IP アドレスは、負荷分散ノードの HA グループを使用しているかどうかによって異なります。

   - HAグループを設定した場合、クライアントはそのHAグループの仮想IPアドレスに接続します。
   - HAグループを使用しない場合、クライアントはゲートウェイノードまたは管理ノードのIPアドレスを使用してStorageGRID ロードバランササービスに接続します。

     また、 DNS レコードが、ワイルドカード名を含む、必要なすべてのエンドポイントドメイン名を参照していることを確認する必要があります。

2. エンドポイントへの接続に必要な情報を S3 クライアントと Swift クライアントに提供します。

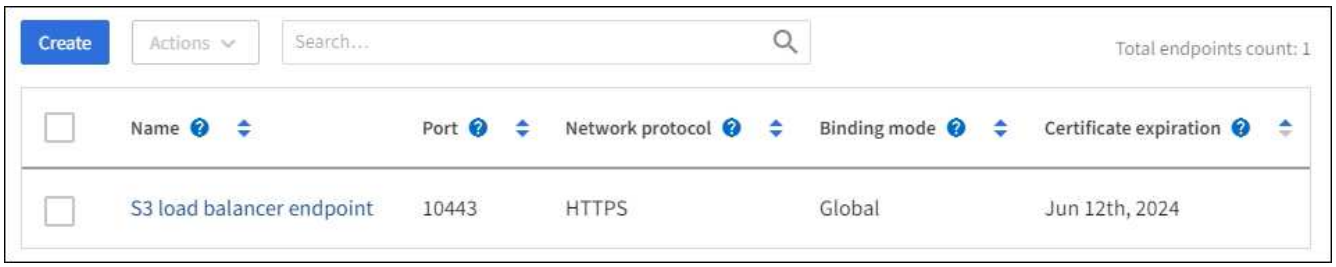
- ポート番号
- 完全修飾ドメイン名または IP アドレス
- 必要な証明書の詳細

ロードバランサエンドポイントを表示および編集します

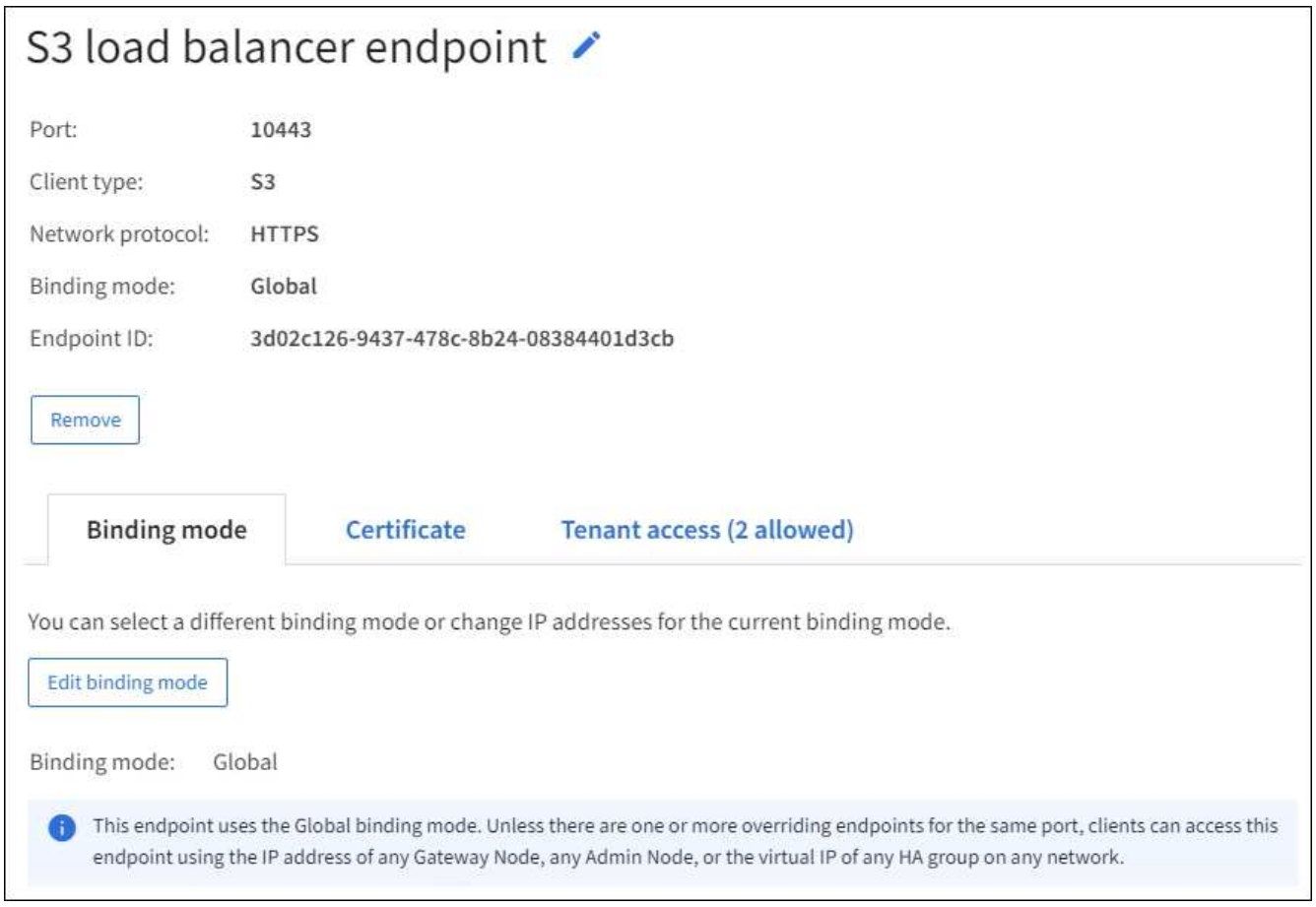
既存のロードバランサエンドポイントの詳細を表示できます。これには、セキュアなエンドポイントの証明書メタデータも含まれます。また、エンドポイントの名前またはバインドモードを変更して、関連付けられている証明書を更新することもできます。

サービスタイプ（S3またはSwift）、ポート、プロトコル（HTTPまたはHTTPS）は変更できません。

- すべてのロードバランサエンドポイントの基本情報を表示するには、 Load Balancer Endpoints ページのテーブルを確認します。



- 証明書メタデータを含む、特定のエンドポイントに関するすべての詳細を表示するには、テーブルでエンドポイントの名前を選択します。



- エンドポイントを編集するには、 [ロードバランサエンドポイント（ Load Balancer Endpoints ）] ページの [* アクション * （ * Actions * ）] メニューを使用するか、特定のエンドポイントの詳細ページを使用します。

エンドポイントの編集後、変更がすべてのノードに適用されるまでに最大 15 分かかる場合があります。

タスク	[アクション] メニュー	詳細ページ
エンドポイント名を編集します	a. エンドポイントのチェックボックスを選択します。 b. [* アクション * > * エンドポイント名の編集 *] を選択します。 c. 新しい名前を入力します。 d. [保存（ Save ）] を選択します。	a. エンドポイント名を選択して詳細を表示します。 b. 編集アイコンを選択します 。 c. 新しい名前を入力します。 d. [保存（ Save ）] を選択します。
エンドポイントバインドモードを編集します	a. エンドポイントのチェックボックスを選択します。 b. [* アクション * （ Actions * ）] > [* エンドポイントバインドモードの編集（ Edit Endpoint binding mode ）] c. 必要に応じて、バインドモードを更新します。 d. 「変更を保存」を選択します。	a. エンドポイント名を選択して詳細を表示します。 b. 「 * バインドモードを編集」を選択します。 c. 必要に応じて、バインドモードを更新します。 d. 「変更を保存」を選択します。
エンドポイント証明書を編集します	a. エンドポイントのチェックボックスを選択します。 b. [* アクション * > * エンドポイント証明書の編集 *] を選択します。 c. 必要に応じて、新しいカスタム証明書をアップロードまたは生成するか、グローバルな S3 および Swift 証明書の使用を開始します。 d. 「変更を保存」を選択します。	a. エンドポイント名を選択して詳細を表示します。 b. [* 証明書 *] タブを選択します。 c. [証明書の編集] を選択します。 d. 必要に応じて、新しいカスタム証明書をアップロードまたは生成するか、グローバルな S3 および Swift 証明書の使用を開始します。 e. 「変更を保存」を選択します。

タスク	[アクション] メニュー	詳細ページ
テナントアクセスを編集します	a. エンドポイントのチェックボックスを選択します。 b. >[テナントアクセスの編集]*を選択します。 c. 別のアクセスオプションを選択するか、リストからテナントを選択または削除するか、またはその両方を実行します。 d. 「変更を保存」を選択します。	a. エンドポイント名を選択して詳細を表示します。 b. [テナントアクセス]*タブを選択します。 c. [テナントアクセスの編集]*を選択します。 d. 別のアクセスオプションを選択するか、リストからテナントを選択または削除するか、またはその両方を実行します。 e. 「変更を保存」を選択します。

ロードバランサエンドポイントを削除する

[* アクション * （ Actions * ）] メニューを使用して 1 つ以上のエンドポイントを削除するか、または詳細ページから 1 つのエンドポイントを削除できます。

クライアントの停止を回避するには、影響を受ける S3 または Swift クライアントアプリケーションを更新してからロードバランサエンドポイントを削除します。各クライアントを更新して、別のロードバランサエンドポイントに割り当てられたポートを使用して接続します。必要な証明書情報も必ず更新してください。

- 1 つ以上のエンドポイントを削除するには、次の手順
  a. [Load balancer]ページで、削除する各エンドポイントのチェックボックスを選択します。
  b. * アクション * > * 削除 * を選択します。
  c. 「 * OK 」を選択します。
- 詳細ページから 1 つのエンドポイントを削除します。
  a. Load Balancer （ロードバランサ）ページから。エンドポイント名を選択します。
  b. 詳細ページで「 * 削除」を選択します。
  c. 「 * OK 」を選択します。

S3エンドポイントのドメイン名を設定

S3仮想ホスト形式の要求をサポートするには、Grid Managerを使用して、S3クライアントの接続先のS3エンドポイントのドメイン名のリストを設定する必要があります。

エンドポイントドメイン名にIPアドレスを使用することはできません。今後のリリースでは、この設定はできません。

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"。
- グリッドのアップグレードが進行中でないことを確認します。

> グリッドのアップグレードの実行中は、ドメイン名の設定を変更しないでください。

このタスクについて

クライアントが S3 エンドポイントのドメイン名を使用できるようにするには、次の作業をすべて実行する必要があります。

- Grid Manager を使用して、 S3 エンドポイントのドメイン名を StorageGRID システムに追加します。
- を確認します "クライアントがStorageGRID へのHTTPS接続に使用する証明書" は、クライアントが必要とするすべてのドメイン名に対して署名されています。

  たとえば、エンドポイントがの場合などです `s3.company.com`、HTTPS接続に使用する証明書にが含まれていることを確認する必要があります `s3.company.com` エンドポイントとエンドポイントのワイルドカードSubject Alternative Name（SAN）： `*.s3.company.com`。

- クライアントが使用する DNS サーバを設定します。クライアントが接続に使用するIPアドレスのDNSレコードを追加し、レコードが必要なすべてのS3エンドポイントのドメイン名（ワイルドカード名を含む）を参照していることを確認します。

> クライアントは、ゲートウェイノード、管理ノード、またはストレージノードの IP アドレスを使用するか、ハイアベイラビリティグループの仮想 IP アドレスに接続することで、StorageGRID に接続できます。DNS レコードに正しい IP アドレスを追加するためには、クライアントアプリケーションがグリッドに接続する方法を理解しておく必要があります。

グリッドへの HTTPS 接続を使用するクライアント（推奨）では、次のいずれかの証明書を使用できます。

- ロードバランサエンドポイントに接続するクライアントは、そのエンドポイント用のカスタム証明書を使用できます。各ロードバランサエンドポイントは、異なるS3エンドポイントのドメイン名を認識するように設定できます。
- ロードバランサエンドポイントに接続するクライアント、またはストレージノードに直接接続するクライアントは、必要なS3エンドポイントのドメイン名をすべて含めるようにS3およびSwift APIのグローバル証明書をカスタマイズできます。

> S3エンドポイントのドメイン名を追加せずにリストが空の場合、S3仮想ホスト形式の要求のサポートは無効になります。

S3エンドポイントのドメイン名を追加します

手順

1. * configuration > Network > S3 endpoint domain names *を選択します。
2. ドメイン名を* Domain name 1 フィールドに入力します。ドメイン名をさらに追加するには、[別のドメイン名を追加する]*を選択します。
3. [保存（ Save ）] を選択します。

4. クライアントが使用するサーバ証明書が、必要なS3エンドポイントのドメイン名と一致していることを確認します。
   - クライアントが独自の証明書を使用するロードバランサエンドポイントに接続する場合は、 "エンドポイントに関連付けられている証明書を更新します"。
   - クライアントがS3およびSwift APIのグローバル証明書を使用するロードバランサエンドポイントに接続するか、またはストレージノードに直接接続する場合は、 "S3およびSwift APIのグローバル証明書を更新します"。
5. エンドポイントのドメイン名要求を解決するために必要な DNS レコードを追加します。

結果

これで、クライアントがエンドポイントを使用するようになります `*bucket.s3.company.com*`を指定すると、DNSサーバが正しいエンドポイントに解決され、証明書がエンドポイントを認証します。

S3エンドポイントのドメイン名を変更します

S3アプリケーションで使用されている名前を変更すると、仮想ホスト形式の要求は失敗します。

手順

1. * configuration > Network > S3 endpoint domain names *を選択します。
2. 編集するドメイン名フィールドを選択し、必要な変更を行います。
3. [保存（ Save ）] を選択します。
4. [はい]*を選択して変更を確定します。

S3エンドポイントのドメイン名を削除します

S3アプリケーションで使用されている名前を削除すると、仮想ホスト形式の要求は失敗します。

手順

1. * configuration > Network > S3 endpoint domain names *を選択します。
2. 削除アイコンを選択します ✕ をクリックします。
3. [はい]*を選択して削除を確定します。

関連情報

- "S3 REST APIを使用する"
- "IP アドレスを表示します"
- "ハイアベイラビリティグループを設定する"

Summary ：クライアント接続の IP アドレスとポート

S3およびSwiftクライアントアプリケーションは、オブジェクトの格納や読み出しを行うために、すべての管理ノードとゲートウェイノードに含まれているロードバランササービスまたはすべてのストレージノードに含まれているLocal Distribution Router（LDR；ローカル分散ルータ）サービスに接続します。

クライアントアプリケーションは、グリッドノードのIPアドレスとそのノード上のサービスのポート番号を使

用してStorageGRID に接続できます。必要に応じて、ロードバランシングノードのハイアベイラビリティ（HA）グループを作成して、仮想IP（VIP）アドレスを使用する可用性の高い接続を確立できます。IPアドレスまたはVIPアドレスの代わりに完全修飾ドメイン名（FQDN）を使用してStorageGRID に接続する場合は、DNSエントリを設定できます。

次の表に、クライアントが StorageGRID に接続できるさまざまな方法、および接続のタイプごとに使用される IP アドレスとポートを示します。ロードバランサエンドポイントとハイアベイラビリティ（HA）グループを作成済みの場合は、を参照してください IPアドレスの検索場所 をクリックして、Grid Managerでこれらの値を確認してください。

接続が確立される場所	クライアントが接続するサービス	**IP** アドレス	ポート
HA グループ	ロードバランサ	HA グループの仮想 IP アドレス	ロードバランサエンドポイントに割り当てられたポート
管理ノード	ロードバランサ	管理ノードの IP アドレス	ロードバランサエンドポイントに割り当てられたポート
ゲートウェイノード	ロードバランサ	ゲートウェイノードの IP アドレス	ロードバランサエンドポイントに割り当てられたポート
ストレージノード	LDR	ストレージノードの IP アドレス	デフォルトの S3 ポート： • HTTPS ： 18082 • HTTP ： 18084 デフォルトの Swift ポート： • HTTPS ： 18083 • HTTP ： 18085

URLの例

クライアントアプリケーションをゲートウェイノードのHAグループのロードバランサエンドポイントに接続するには、次の構造のURLを使用します。

`https://VIP-of-HA-group:LB-endpoint-port`

たとえば、HAグループの仮想IPアドレスが192.0.2.5で、ロードバランサエンドポイントのポート番号が10443の場合、アプリケーションは次のURLを使用してStorageGRID に接続できます。

`https://192.0.2.5:10443`

IPアドレスの検索場所

1. 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"。
2. グリッドノードの IP アドレスを確認するには、次の手順を実行します。
   a. [* nodes （ノード）] を選択します
   b. 接続する管理ノード、ゲートウェイノード、またはストレージノードを選択します。
   c. [* Overview * （概要 * ）] タブを選択します。
   d. Node Information セクションで、ノードの IP アドレスを確認します。
   e. IPv6 アドレスとインターフェイスマッピングを表示するには、 * Show More * を選択します。

      クライアントアプリケーションから、リスト内の任意の IP アドレスへの接続を確立できます。

      - * eth0 ： * グリッドネットワーク
      - * eth1 ： * 管理ネットワーク（オプション）
      - * eth2 ： * クライアントネットワーク（オプション）

      表示されている管理ノードまたはゲートウェイノードがハイアベイラビリティグループのアクティブノードである場合は、 HA グループの仮想 IP アドレスが eth2 に表示されます。

3. ハイアベイラビリティグループの仮想 IP アドレスを検索するには、次の手順を実行します。
   a. 構成 * > * ネットワーク * > * ハイアベイラビリティグループ * を選択します。
   b. HA グループの仮想 IP アドレスを表で確認します。
4. ロードバランサエンドポイントのポート番号を確認するには、次の手順を実行します。
   a. [* configuration * > * Network * > * Load Balancer Endpoints *] を選択します。
   b. 使用するエンドポイントのポート番号をメモします。

      ポート番号が80または443の場合、エンドポイントはゲートウェイノードでのみ設定されます。これらのポートは管理ノードで予約されているためです。それ以外のポートはすべて、ゲートウェイノードと管理ノードの両方に設定されます。

   c. テーブルからエンドポイントの名前を選択します。
   d. [Client type]*（S3またはSwift）が、エンドポイントを使用するクライアントアプリケーションと一致していることを確認します。

ネットワークと接続を管理します

ネットワーク設定の構成：概要

グリッドマネージャからさまざまなネットワーク設定を行い、 StorageGRID システムの動作を微調整できます。

VLAN インターフェイスを設定します

可能です "仮想LAN（VLAN）インターフェイスを作成します" セキュリティ、柔軟性、およびパフォーマンスのためにトラフィックを分離および分割する。各 VLAN インターフェイスは、管理ノードおよびゲートウェイノード上の 1 つ以上の親インターフェイスに関連付けられます。HA グループでは VLAN インターフェイスを使用し、ロードバランサエンドポイントではクライアントトラフィックと管理トラフィックをアプリケーションまたはテナントごとに分離できます。

トラフィック分類ポリシー

を使用できます "トラフィック分類ポリシー" 特定のバケット、テナント、クライアントサブネット、ロードバランサエンドポイントに関連するトラフィックなど、さまざまなタイプのネットワークトラフィックを識別して処理するため。これらのポリシーは、トラフィックの制限と監視に役立ちます。

StorageGRID ネットワークのガイドライン

グリッドマネージャを使用して、 StorageGRID のネットワークと接続を設定および管理できます。

を参照してください "S3 および Swift クライアント接続を設定します" を参照して、 S3 または Swift クライアントを接続する方法を確認してください。

デフォルトの StorageGRID ネットワーク

StorageGRID では、デフォルトでグリッドノードあたり 3 つのネットワークインターフェイスがサポートされ、各グリッドノードのネットワークをセキュリティやアクセスの要件に応じて設定することができます。

ネットワークトポロジの詳細については、を参照してください "ネットワークのガイドライン"。

Grid ネットワーク

必須グリッドネットワークは、すべての内部 StorageGRID トラフィックに使用されます。このネットワークによって、グリッド内のすべてのノードが、すべてのサイトおよびサブネットにわたって相互に接続されます。

管理ネットワーク

任意。通常、管理ネットワークはシステムの管理とメンテナンスに使用されます。クライアントプロトコルアクセスにも使用できます。管理ネットワークは通常はプライベートネットワークであり、サイト間でルーティング可能にする必要はありません。

クライアントネットワーク

任意。クライアントネットワークはオープンネットワークで、主に S3 および Swift クライアントアプリケーションへのアクセスに使用されます。そのため、グリッドネットワークを分離してセキュリティを確保できます。クライアントネットワークは、ローカルゲートウェイ経由でアクセス可能なすべてのサブネットと通信できます。

ガイドライン

- 各 StorageGRID グリッドノードには、割り当て先のネットワークごとに専用のネットワークインターフェイス、 IP アドレス、サブネットマスク、およびゲートウェイが必要です。

- 1つのグリッドノードに複数のインターフェイスを設定することはできません。
- 各ネットワークのグリッドノードごとに、単一のゲートウェイがサポートされます。このゲートウェイはノードと同じサブネット上に配置する必要があります。必要に応じて、より複雑なルーティングをゲートウェイに実装できます。
- 各ノードでは、各ネットワークが特定のネットワークインターフェイスにマッピングされます。

ネットワーク	インターフェイス名
グリッド（ Grid ）	eth0
管理（オプション）	Eth1
クライアント（オプション）	eth2

- ノードが StorageGRID アプライアンスに接続されている場合は、ネットワークごとに特定のポートが使用されます。詳細については、使用しているアプライアンスのインストール手順を参照してください。
- デフォルトルートはノードごとに自動的に生成されます。eth2 が有効な場合、 0.0.0.0/0 は eth2 のクライアントネットワークを使用します。eth2 が無効な場合、 0.0.0.0/0 は eth0 のグリッドネットワークを使用します。
- クライアントネットワークは、グリッドノードがグリッドに参加するまで動作状態になりません
- グリッドが完全にインストールされる前にインストールユーザインターフェイスにアクセスできるように、グリッドノード導入時に管理ネットワークを設定できます。

オプションのインターフェイス

必要に応じて、ノードにインターフェイスを追加できます。たとえば、を使用できるように、管理ノードまたはゲートウェイノードにトランクインターフェイスを追加できます "VLAN インターフェイス" 異なるアプリケーションまたはテナントに属するトラフィックを分離する。または、で使用するアクセスインターフェイスを追加することもできます "ハイアベイラビリティ（ HA ）グループ"。

トランクインターフェイスまたはアクセスインターフェイスを追加するには、次の項を参照してください。

- * VMware （ノードのインストール後） * ： "VMware ：ノードにトランクインターフェイスまたはアクセスインターフェイスを追加します"
  - * RHEL または CentOS （ノードのインストール前） * ： "ノード構成ファイルを作成"
  - * Ubuntu または Debian （ノードをインストールする前） * ： "ノード構成ファイルを作成"
  - * RHEL 、 CentOS 、 Ubuntu 、または Debian （ノードのインストール後） * ： "Linux ：ノードにトランクインターフェイスまたはアクセスインターフェイスを追加します"

IP アドレスを表示します

StorageGRID システムの各グリッドノードの IP アドレスを表示できます。その後、このIPアドレスを使用してコマンドラインでグリッドノードにログインし、さまざまなメンテナンス手順を実行できます。

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"。

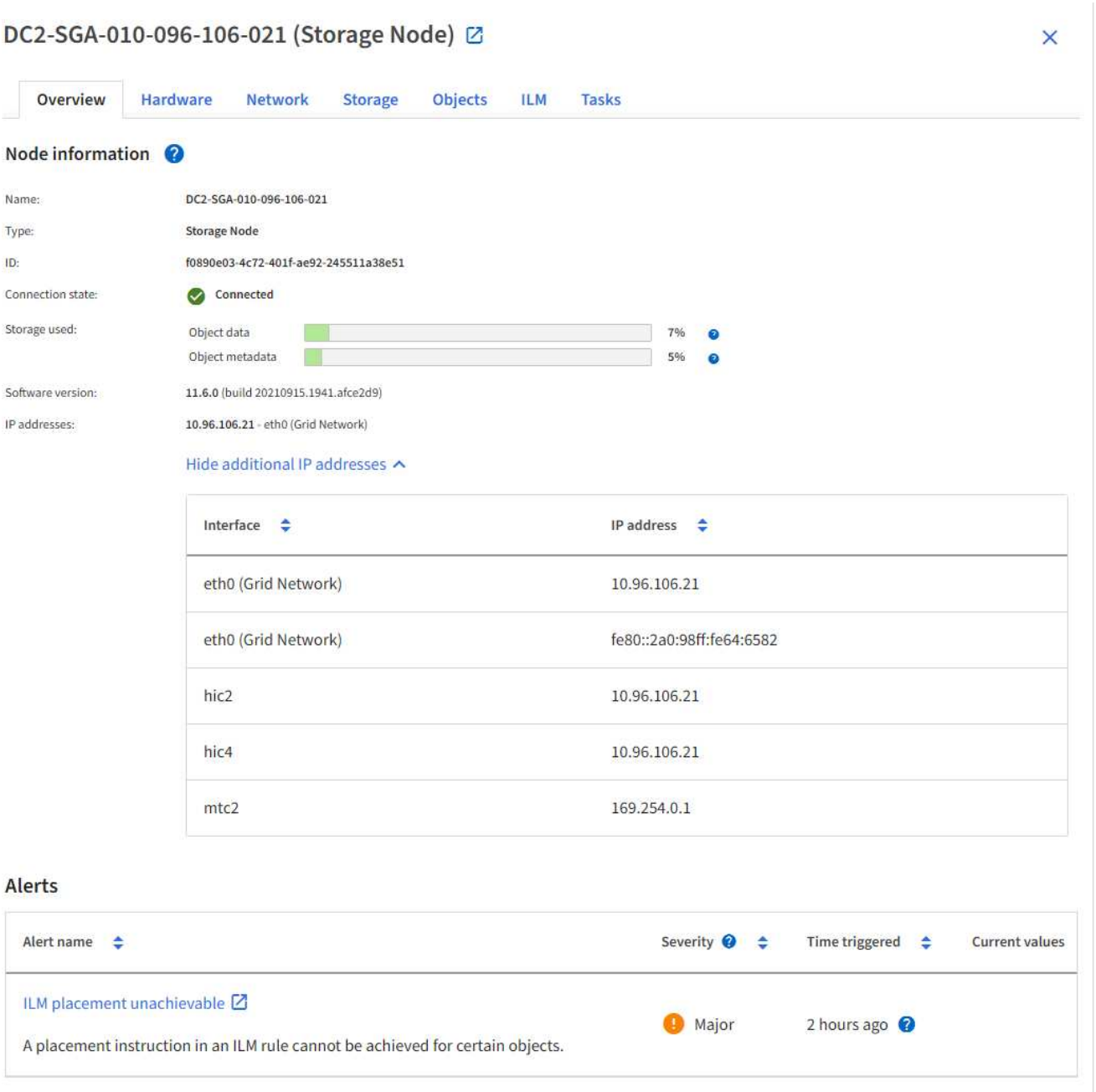
このタスクについて

IPアドレスの変更については、を参照してください "IP アドレスを設定する"。

手順

1. ノード * > * *grid node* > * Overview * を選択します。
2. [IP Addresses] のタイトルの右側にある [**Show More**] を選択します。

   このグリッドノードの IP アドレスがテーブルに表示されます。



発信 **TLS** 接続でサポートされる暗号

StorageGRID システムでは、アイデンティティフェデレーションとクラウドストレージプールに使用される外部システムへの Transport Layer Security （ TLS ）接続でサポートされる暗号スイートに制限があります。

サポートされる **TLS** のバージョン

StorageGRID では、アイデンティティフェデレーションとクラウドストレージプールに使用される外部システムへの接続で TLS 1.2 と TLS 1.3 がサポートされます。

外部システムとの互換性を確保するために、外部システムとの使用がサポートされている TLS 暗号が選択されています。S3 または Swift クライアントアプリケーションで使用できる暗号のリストは、このリストよりも大容量です。暗号を設定するには、**[設定]>*[セキュリティ設定]***に移動し、 TLSおよびSSHポリシー*を選択します。

> プロトコルバージョン、暗号、鍵交換アルゴリズム、MACアルゴリズムなどのTLS設定オプションは、StorageGRID では設定できません。これらの設定について具体的なご要望がある場合は、ネットアップのアカウント担当者にお問い合わせください。

VLAN インターフェイスを設定します

管理ノードとゲートウェイノードに仮想 LAN （ VLAN ）インターフェイスを作成し、それらを HA グループとロードバランサエンドポイントで使用してトラフィックを分離し、セキュリティ、柔軟性、パフォーマンスを向上させることができます。

VLAN インターフェイスに関する考慮事項

- VLAN インターフェイスを作成するには、 VLAN ID を入力し、 1 つ以上のノード上で親インターフェイスを選択します。
- 親インターフェイスは、スイッチでトランクインターフェイスとして設定する必要があります。
- 親インターフェイスは、グリッドネットワーク（ eth0 ）、クライアントネットワーク（ eth2 ）、または VM やベアメタルホスト用の追加のトランクインターフェイス（ ens256 など）です。
- VLAN インターフェイスごとに、特定のノードに対して選択できる親インターフェイスは 1 つだけです。たとえば、同じゲートウェイノードのグリッドネットワークインターフェイスとクライアントネットワークインターフェイスの両方を同じVLANの親インターフェイスとして使用することはできません。
- VLAN インターフェイスが管理ノードトラフィック用で、 Grid Manager および Tenant Manager に関連するトラフィックが含まれている場合は、管理ノード上のインターフェイスのみを選択します。
- VLAN インターフェイスが S3 または Swift クライアントトラフィック用の場合は、管理ノードまたはゲートウェイノード上のインターフェイスを選択します。
- トランクインターフェイスを追加する必要がある場合は、次の詳細を参照してください。
  - * VMware （ノードのインストール後） * ： "VMware ：ノードにトランクインターフェイスまたはアクセスインターフェイスを追加します"
  - * RHEL または CentOS （ノードのインストール前） * ： "ノード構成ファイルを作成"
  - * Ubuntu または Debian （ノードをインストールする前） * ： "ノード構成ファイルを作成"

- * RHEL 、 CentOS 、 Ubuntu 、または Debian （ノードのインストール後） * ： "Linux ：ノードにトランクインターフェイスまたはアクセスインターフェイスを追加します"

VLAN インターフェイスを作成します

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"。
- Root アクセス権限が割り当てられている。
- ネットワークでトランクインターフェイスが設定され、 VM または Linux ノードに接続されている。トランクインターフェイスの名前を確認しておきます。
- 設定する VLAN の ID を確認しておきます。

このタスクについて

ネットワーク管理者が、 1 つ以上のトランクインターフェイスと 1 つ以上の VLAN を設定して、異なるアプリケーションまたはテナントに属するクライアントトラフィックまたは管理トラフィックを分離している場合があります。各 VLAN は、数値 ID またはタグで識別されます。たとえば、ネットワークで FabricPool トラフィックに VLAN 100 を使用し、アーカイブアプリケーションに VLAN 200 を使用しているとします。

グリッドマネージャを使用して、クライアントが特定の VLAN 上の StorageGRID にアクセスできるようにする VLAN インターフェイスを作成できます。VLAN インターフェイスを作成するときは、 VLAN ID を指定し、 1 つ以上のノード上で親（トランク）インターフェイスを選択します。

ウィザードにアクセスします

手順

1. * configuration * > * Network * > * vlan interfaces * を選択します。
2. 「 * Create * 」を選択します。

VLAN インターフェイスの詳細を入力します

手順

1. ネットワーク内の VLAN の ID を指定します。1~4094 の値を入力できます。

   VLAN IDは一意である必要はありません。たとえば、あるサイトの管理トラフィックに VLAN ID 200 を使用し、別のサイトのクライアントトラフィックに同じ VLAN ID を使用できます。各サイトに異なる親インターフェイスのセットを持つ個別の VLAN インターフェイスを作成できます。ただし、IDが同じ2つのVLANインターフェイスでノード上の同じインターフェイスを共有することはできません。すでに使用されている ID を指定すると、メッセージが表示されます。

2. 必要に応じて、 VLAN インターフェイスの短い概要 を入力します。
3. 「 * Continue * 」を選択します。

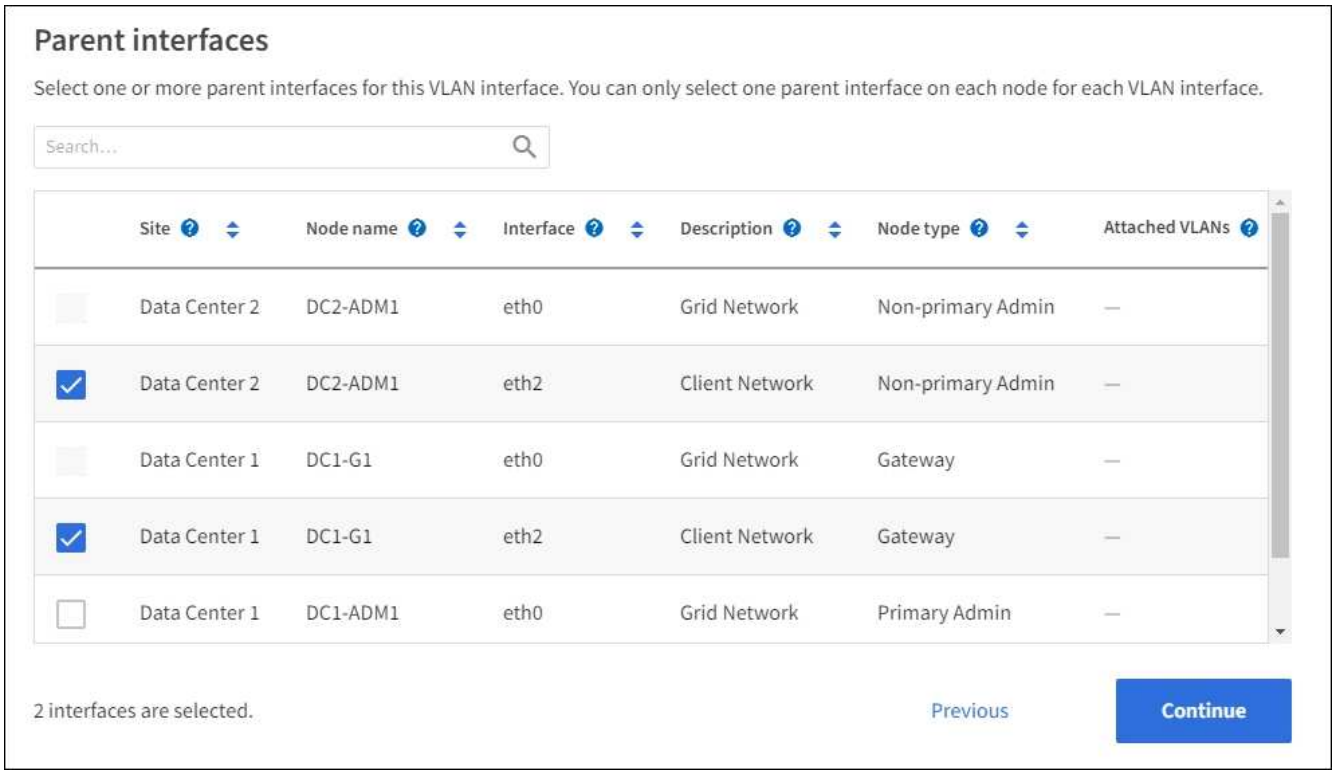
親インターフェイスを選択します

次の表に、グリッドの各サイトのすべての管理ノードとゲートウェイノードで使用可能なインターフェイスを示します。管理ネットワーク（eth1）インターフェイスを親インターフェイスとして使用することはできず、表示されていません。

手順

1. この VLAN を接続する 1 つ以上の親インターフェイスを選択してください。

   たとえば、ゲートウェイノードと管理ノードのクライアントネットワーク（ eth2 ）インターフェイスに VLAN を接続できます。



2. 「 * Continue * 」を選択します。

設定を確認します

手順

1. 構成を確認し、変更を行います。
   - VLAN ID または概要 を変更する必要がある場合は、ページの上部にある *Enter VLAN details * を選択します。
   - 親インターフェイスを変更する必要がある場合は、ページの上部にある「親インターフェイスを選択」を選択するか、「 * 前へ * 」を選択します。
   - 親インターフェイスを削除する必要がある場合は、ごみ箱を選択します 。
2. [保存（ Save ）] を選択します。
3. 新しいインターフェイスが High Availability groups ページで選択されて、ノードの * Network Interfaces * テーブルに表示されるまで、最大 5 分待ちます（ * nodes * > * _parent interface node_name > * Network * ）。

VLAN インターフェイスを編集します

VLAN インターフェイスを編集する場合、次の種類の変更を行うことができます。

- VLAN ID または概要 を変更します。
- 親インターフェイスを追加または削除します。

たとえば、関連付けられているノードの運用を停止する場合、 VLAN インターフェイスから親インターフェイスを削除できます。

次の点に注意してください。

- HA グループで VLAN インターフェイスを使用している場合、 VLAN ID は変更できません。
- HA グループで親インターフェイスが使用されている場合、親インターフェイスを削除することはできません。

  たとえば、 VLAN 200 がノード A および B の親インターフェイスに接続されているとしますHA グループでノード A の VLAN 200 インターフェイスとノード B の eth2 インターフェイスを使用している場合、ノード B の未使用の親インターフェイスを削除できますが、ノード A の使用済みの親インターフェイスを削除することはできません

手順

1. * configuration * > * Network * > * vlan interfaces * を選択します。
2. 編集するVLANインターフェイスのチェックボックスを選択します。次に、 * アクション * > * 編集 * を選択します。
3. 必要に応じて、 VLAN ID または概要 を更新します。次に、 [* Continue （続行）] を選択します。

   HA グループで VLAN が使用されている場合、 VLAN ID は更新できません。

4. 必要に応じて、チェックボックスをオンまたはオフにして、親インターフェイスを追加するか、使用されていないインターフェイスを削除します。次に、 [* Continue （続行）] を選択します。
5. 構成を確認し、変更を行います。
6. [保存（ Save ）] を選択します。

VLAN インターフェイスを削除します

1 つ以上の VLAN インターフェイスを削除できます。

HA グループで現在使用されている VLAN インターフェイスは削除できません。HA グループを削除する前に、 VLAN インターフェイスを HA グループから削除する必要があります。

クライアントトラフィックの中断を回避するには、次のいずれかを実行します。

- この VLAN インターフェイスを削除する前に、 HA グループに新しい VLAN インターフェイスを追加してください。
- この VLAN インターフェイスを使用しない新しい HA グループを作成してください。
- 削除する VLAN インターフェイスが現在アクティブインターフェイスである場合は、 HA グループを編集します。削除する VLAN インターフェイスを優先順位リストの一番下に移動します。新しいプライマリインターフェイスとの通信が確立されるまで待ってから、 HA グループから古いインターフェイスを削除します。最後に、そのノードの VLAN インターフェイスを削除します。

手順

1. * configuration * > * Network * > * vlan interfaces * を選択します。
2. 削除する各VLANインターフェイスのチェックボックスを選択します。次に、 * アクション * > * 削除 * を選択します。

3. 「 * はい * 」を選択して選択を確定します。

   選択したすべての VLAN インターフェイスが削除されます。VLAN Interfaces ページに、グリーンの成功バナーが表示されます。

トラフィック分類ポリシーを管理します

トラフィック分類ポリシーの管理：概要

サービス品質（ QoS ）サービスを強化するために、トラフィック分類ポリシーを作成して、さまざまなタイプのネットワークトラフィックを識別および監視できます。これらのポリシーは、トラフィックの制限と監視に役立ちます。

トラフィック分類ポリシーは、ゲートウェイノードおよび管理ノードの StorageGRID ロードバランササービス上のエンドポイントに適用されます。トラフィック分類ポリシーを作成するには、ロードバランサエンドポイントを作成しておく必要があります。

一致ルール

各トラフィック分類ポリシーには、次のエンティティに関連するネットワークトラフィックを識別する 1 つ以上の一致ルールが含まれています。

- バケット
- サブネット
- テナント
- ロードバランサエンドポイント

StorageGRID は、ルールの目的に応じて、ポリシー内のルールに一致するトラフィックを監視します。ポリシーのルールに一致するトラフィックは、そのポリシーによって処理されます。逆に、指定されたエンティティを除くすべてのトラフィックを照合するルールを設定できます。

トラフィック制限

必要に応じて、次の制限タイプをポリシーに追加できます。

- 総帯域幅
- 要求ごとの帯域幅
- 同時要求
- リクエスト率

制限値はロードバランサごとに適用されます。複数のロードバランサに同時にトラフィックが分散されている場合、合計最大速度は指定した速度制限の倍数になります。

> ポリシーを作成して、アグリゲートの帯域幅を制限したり、要求ごとの帯域幅を制限したりできます。ただし、StorageGRID では、両方のタイプの帯域幅を同時に制限することはできません。アグリゲートの帯域幅の制限により、制限のないトラフィックにパフォーマンスが若干低下する可能性があります。

集約または要求ごとの帯域幅制限の場合、要求は、設定したレートでストリームインまたはアウトされます。StorageGRID では 1 つの速度しか適用できないため、最も特定のポリシーがマッチするのはマッチャーのタイプです。要求によって消費された帯域幅は、集約帯域幅制限ポリシーを含む他のあまり具体的でない一致ポリシーにはカウントされません。それ以外のすべての制限タイプでは、クライアント要求は 250 ミリ秒遅延し、一致するポリシー制限を超える要求に対しては 503 スローダウン応答を受信します。

Grid Manager では、トラフィックチャートを表示して、ポリシーが想定したトラフィック制限を適用していることを確認できます。

SLA でトラフィック分類ポリシーを使用する

トラフィック分類ポリシーを容量制限およびデータ保護とともに使用して、容量、データ保護、およびパフォーマンスに固有のサービスレベル契約（ SLA ）を適用できます。

次の例は、 SLA の 3 つの階層を示しています。トラフィック分類ポリシーを作成して、各 SLA 層のパフォーマンス目標を達成できます。

サービスレベル階層	容量	データ保護	許容される最大パフォーマンス	コスト
ゴールド	1 PB のストレージを使用できます	3 コピーの ILM ルール	25 、 000 要求 / 秒 5 GB/ 秒（ 40 Gbps ）の帯域幅	$$/ 月
シルバー	250 TB のストレージを使用できます	2 コピーの ILM ルール	10 K 要求 / 秒 1.25 GB/ 秒（ 10 Gbps ）の帯域幅	$/ 月
ブロンズ	100TB のストレージを使用できます	2 コピーの ILM ルール	5 、 000 要求 / 秒 1 GB/ 秒（ 8 Gbps ）の帯域幅	月あたりのコスト

トラフィック分類ポリシーを作成します

バケット、バケット正規表現、CIDR、ロードバランサエンドポイント、またはテナントごとにネットワークトラフィックを監視し、必要に応じて制限する場合は、トラフィック分類ポリシーを作成できます。必要に応じて、帯域幅、同時要求数、または要求速度に基づいてポリシーの制限を設定できます。

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"。
- Root アクセス権限が割り当てられている。
- 照合するロードバランサエンドポイントを作成しておきます。
- 該当するテナントを作成しておきます。

手順

1. * configuration * > * Network * > * traffic classification * を選択します。
2. 「 * Create * 」を選択します。
3. ポリシーの名前と概要 （オプション）を入力し、* Continue *を選択します。

   たとえば、このトラフィック分類ポリシー環境 の内容と制限する内容を説明します。

4. ポリシーに一致するルールを1つ以上作成するには、*[ルールの追加]*を選択し、以下の詳細を指定します。作成するポリシーには、一致するルールが少なくとも1つ必要です。「 * Continue * 」を選択します。

フィールド	説明
を入力します	一致するルール環境 のトラフィックのタイプを選択します。トラフィックタイプには、バケット、バケットの正規表現、CIDR、ロードバランサエンドポイント、テナントがあります。
一致値	選択したタイプに一致する値を入力します。 • Bucket：バケット名を1つ以上入力します。 • Bucket regex：バケット名のセットに一致する正規表現を1つ以上入力します。 正規表現は固定されていません。^anchorを使用してバケット名の先頭に一致させ、$anchorを使用して名前の末尾に一致させます。正規表現マッチングでは、PCRE（Perl互換正規表現）構文のサブセットがサポートされます。 • CIDR：CIDR表記で、目的のサブネットに一致するIPv4サブネットを1つ以上入力します。 • Load balancer endpoint：エンドポイント名を選択します。これは、で定義したロードバランサエンドポイントです "ロードバランサエンドポイントを設定する"。 • Tenant：一致するテナントはアクセスキーIDを使用します。要求にアクセスキーID（匿名アクセスなど）が含まれていない場合は、テナントを特定するためにアクセスされるバケットの所有権が使用されます。
逆一致	定義した[Type]および[Match Value]と一致するすべてのネットワークトラフィック_except_trafficを照合する場合は、*[Inverse Match]*チェックボックスをオンにします。それ以外の場合は’チェックボックスをオフのままにします たとえば、このポリシーをいずれかのロードバランサエンドポイントを除くすべてのロードバランサエンドポイントに適用する場合は、除外するロードバランサエンドポイントを指定し、*[逆一致]*を選択します。 少なくとも 1 つが逆マッチャーである複数のマッチャーを含むポリシーの場合、すべてのリクエストに一致するポリシーを作成しないように注意してください。

5. 必要に応じて、*[制限の追加]*を選択し、以下の詳細を選択して1つ以上の制限を追加し、ルールに一致す

るネットワークトラフィックを制御します。

StorageGRID では、制限を追加しなくても指標が収集されるため、トラフィックの傾向を把握できます。

フィールド	説明
を入力します	ルールに一致するネットワークトラフィックに適用する制限のタイプ。たとえば、帯域幅や要求レートを制限できます。 注：ポリシーを作成して、総帯域幅を制限したり、要求ごとの帯域幅を制限したりできます。ただし、StorageGRID では、両方のタイプの帯域幅を同時に制限することはできません。集約帯域幅が使用されている場合、要求ごとの帯域幅は使用できません。逆に、要求ごとの帯域幅が使用されている場合、集約帯域幅は使用できません。アグリゲートの帯域幅の制限により、制限のないトラフィックにパフォーマンスが若干低下する可能性があります。 帯域幅の制限については、設定された制限のタイプに最も一致するポリシーが StorageGRID によって適用されます。たとえば、トラフィックを一方向のみに制限するポリシーがある場合、帯域幅制限が設定されている他のポリシーと一致するトラフィックがあっても、反対方向のトラフィックは無制限になります。StorageGRID では、帯域幅制限に対して次の順序で「最適な」一致が実装されます。 • 正確な IP アドレス（ /32 マスク） • 正確なバケット名 • バケットの正規表現 • テナント • エンドポイント • 正確でない CIDR の一致（ /32 ではない） • 逆一致
環境	これにより、環境 クライアントの読み取り要求（GETまたはHEAD）と書き込み要求（PUT、POST、DELETE）のどちらを制限するか。
価値	選択した単位に基づいて、ネットワークトラフィックが制限される値。たとえば、このルールに一致するネットワークトラフィックが10MiB/sを超えないようにするには、「10」と入力して[MiB/s」を選択します 注：単位の設定に応じて、使用可能な単位は2進数（GiBなど）または10進数（GBなど）のいずれかになります。単位の設定を変更するには、Grid Managerの右上にあるユーザードロップダウンを選択し、*ユーザー設定*を選択します。
単位	入力した値を表す単位。

たとえば、SLAティアに40GB/秒の帯域幅制限を作成する場合は、アグリゲートの帯域幅制限を2つ作成します。GET /headは40GB/秒、PUT /POST/DELETEは40GB/秒です

6. 「 * Continue * 」を選択します。
7. トラフィック分類ポリシーを読んで確認します。前へ*ボタンを使用して前に戻り、必要に応じて変更を行います。ポリシーに問題がなければ、*[保存して続行]*を選択します。

   S3およびSwiftクライアントのトラフィックがトラフィック分類ポリシーに従って処理されるようになりました。

完了後

"ネットワークトラフィックの指標を表示します" ポリシーが想定どおりのトラフィック制限を適用していることを確認します。

トラフィック分類ポリシーを編集します

トラフィック分類ポリシーを編集して、その名前または概要 を変更したり、ポリシーのルールや制限を作成、編集、削除したりできます。

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"。
- Root アクセス権限が割り当てられている。

手順

1. * configuration * > * Network * > * traffic classification * を選択します。

   [Traffic Classification Policies]ページが表示され、既存のポリシーが表に表示されます。

2. [Actions]メニューまたは詳細ページを使用してポリシーを編集します。を参照してください "トラフィック分類ポリシーを作成します" 何を入力するかを入力します。

   [アクション] メニュー

   a. ポリシーのチェックボックスを選択します。
   b. **>**[編集]*を選択します。

   詳細ページ

   a. ポリシー名を選択します。
   b. ポリシー名の横にある*[編集]*ボタンを選択します。

3. [Enter policy name]手順で、必要に応じてポリシー名または概要 を編集し、*[Continue]*を選択します。
4. [一致ルールの追加]ステップで、必要に応じてルールを追加するか、既存のルールの*タイプ*と*一致値*を編集し、*続行*を選択します。
5. [制限の設定]ステップで、必要に応じて制限を追加、編集、または削除し、*[続行]*を選択します。
6. 更新されたポリシーを確認し、*[保存して続行]*を選択します。

   ポリシーに加えた変更が保存され、ネットワークトラフィックはトラフィック分類ポリシーに従って処理されるようになりました。トラフィックチャートを表示して、ポリシーが想定したトラフィック制限を適用していることを確認できます。

トラフィック分類ポリシーを削除します

不要になったトラフィック分類ポリシーは削除できます。削除したポリシーは取得できないため、適切なポリシーを削除してください。

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"。
- Root アクセス権限が割り当てられている。

手順

1. * configuration * > * Network * > * traffic classification * を選択します。

   [Traffic Classification Policies]ページが表示され、既存のポリシーが表に示されます。

2. [アクション]メニューまたは詳細ページを使用してポリシーを削除します。

   [アクション] メニュー

   a. ポリシーのチェックボックスを選択します。

   b. * アクション * > * 削除 * を選択します。

   [ポリシーの詳細]ページ

   a. ポリシー名を選択します。

   b. ポリシー名の横にある*[削除]*ボタンを選択します。

3. [はい]*を選択して、ポリシーの削除を確定します。

   ポリシーが削除されます。

ネットワークトラフィックの指標を表示します

トラフィック分類ポリシーページのグラフを表示して、ネットワークトラフィックを監視できます。

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"。
- Root Access権限またはTenant Accounts権限が必要です。

このタスクについて

既存のトラフィック分類ポリシーについては、ロードバランササービスの指標を表示して、ポリシーがネットワーク全体のトラフィックを正常に制限しているかどうかを確認できます。グラフのデータは、ポリシーの調整が必要かどうかを判断するのに役立ちます。

トラフィック分類ポリシーに制限が設定されていない場合でも、メトリックが収集され、グラフにはトラフィックの傾向を把握するのに役立つ情報が表示されます。

手順

1. * configuration * > * Network * > * traffic classification * を選択します。

   [Traffic Classification Policies]ページが表示され、既存のポリシーがテーブルに表示されます。

2. 指標を表示するトラフィック分類ポリシーの名前を選択します。
3. [Metrics]タブを選択します。

   トラフィック分類ポリシーのグラフが表示されます。このグラフには、選択したポリシーに一致するトラフィックのメトリックだけが表示されます。

   このページには次のグラフが表示されます。

   - [Request rate]：このグラフには、すべてのロードバランサによって処理されたこのポリシーに一致する帯域幅の量が表示されます。受信したデータには、すべての要求の要求ヘッダーと、本文データを含む応答の本文データサイズが含まれます。Sentには、すべての要求の応答ヘッダーと、応答に本文データを含む要求の応答本文のデータサイズが含まれます。

     > 要求が完了すると、このチャートには帯域幅の使用量のみが表示されます。低速なオブジェクト要求や大規模なオブジェクト要求では、実際の帯域幅はこのグラフに表示される値と異なる場合があります。

   - エラー応答率：このグラフは、このポリシーに一致する要求がクライアントにエラー（HTTPステータスコード>=400）を返すおおよその速度を示します。
   - Average request duration（non-error）：このグラフには、このポリシーに一致する成功したリクエストの平均期間が表示されます。
   - Policy Bandwidth usage：このグラフには、すべてのロードバランサによって処理されたこのポリシーに一致する帯域幅の量が表示されます。受信したデータには、すべての要求の要求ヘッダーと、本文データを含む応答の本文データサイズが含まれます。Sentには、すべての要求の応答ヘッダーと、応答に本文データを含む要求の応答本文のデータサイズが含まれます。
4. 折れ線グラフにカーソルを合わせると、グラフの特定の部分の値がポップアップで表示されます。
5. [Metrics]タイトルのすぐ下にある* Grafanaダッシュボード*を選択すると、ポリシーのすべてのグラフが表示されます。[* Metrics]タブの4つのグラフに加えて、さらに2つのグラフを表示できます。
   - Write request rate by object size：このポリシーに一致するPUT / POST / DELETE要求の速度。個 々 のセルに配置すると、1秒あたりのレートが表示されます。ホバービューに表示されるレートは整数に切り捨てられ、バケットに0以外の要求がある場合は0と報告されることがあります。
   - Read request rate by object size：このポリシーに一致するGET / HEAD要求のレート。個 々 のセルに配置すると、1秒あたりのレートが表示されます。ホバービューに表示されるレートは整数に切り捨てられ、バケットに0以外の要求がある場合は0と報告されることがあります。
6. または、 **support** メニューからグラフにアクセスします。
   a. [**support**>] 、 [*Tools] 、 [*Metrics] の順に選択します。
   b. [Grafana]セクションから*[Traffic Classification Policy]*を選択します。
   c. ページ左上のメニューからポリシーを選択します。
   d. グラフにカーソルを合わせると、サンプルの日時、カウントに集計されたオブジェクトサイズ、その期間の1秒あたりの要求数を示すポップアップが表示されます。

      トラフィック分類ポリシーは、その ID によって識別されます。ポリシーIDは、トラフィック分類ポリ

シーページに表示されます。

7. グラフを分析して、ポリシーがトラフィックを制限している頻度と、ポリシーを調整する必要があるかどうかを判断します。

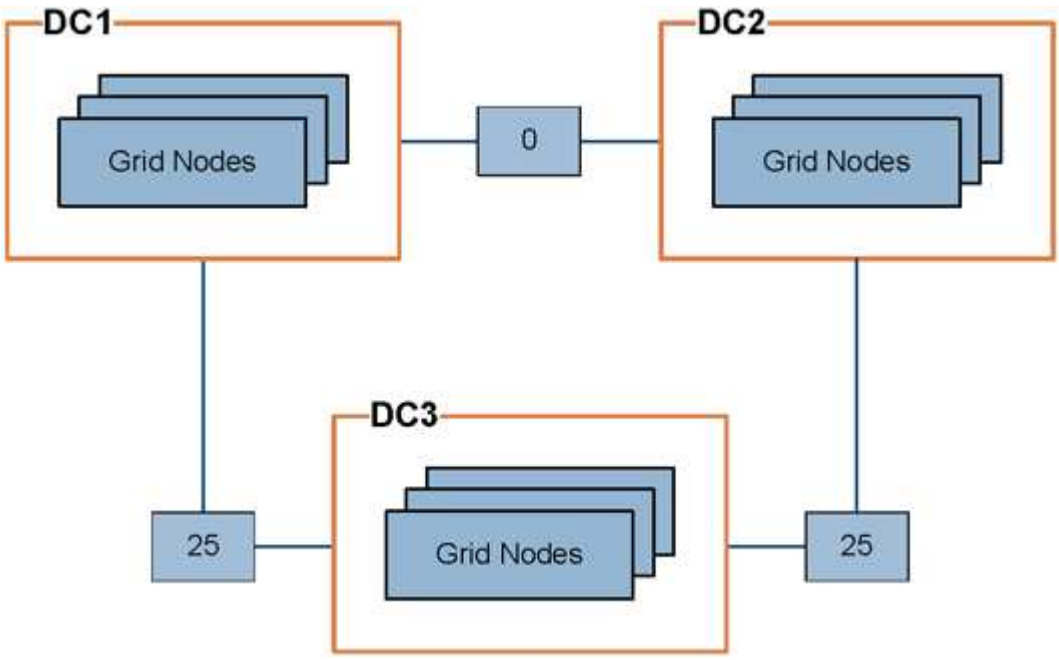
リンクコストを管理します

リンクコストを使用すると、複数のデータセンターサイトが存在する場合に、要求されたサービスを提供するデータセンターサイトの優先順位を決定できます。サイト間のレイテンシに合わせてリンクコストを調整できます。

リンクコストとは

- リンクコストは、オブジェクトの読み出しにどのオブジェクトコピーを使用するかを優先的に処理するために使用されます。
- リンクコストは、グリッド管理 API およびテナント管理 API で、使用する内部 StorageGRID サービスを決定するために使用されます。
- リンクコストは、管理ノードおよびゲートウェイノード上のロードバランササービスでクライアント接続を転送するために使用されます。を参照してください "ロードバランシングに関する考慮事項"。

次の図は、サイト間でリンクコストが設定されている 3 つのサイトグリッドを示しています。



- 管理ノードとゲートウェイノード上のロードバランササービスは、同じデータセンターサイトにあるすべてのストレージノード、およびリンクコストが0のデータセンターサイトにクライアント接続を均等に分散します。

  この例で、データセンターサイト 1 （ DC1 ）にあるゲートウェイノードは、 DC1 にあるストレージノードと DC2 にあるストレージノードにクライアント接続を均等に分散します。DC3 にあるゲートウェイノードは、 DC3 にあるストレージノードにのみクライアント接続を送信します。

- 複数のレプリケートコピーが存在するオブジェクトを読み出す場合、 StorageGRID はリンクコストが最も低いデータセンターにあるコピーを読み出します。

次の例では、DC2にあるクライアントアプリケーションがDC1とDC3の両方に格納されているオブジェクトを読み出す場合、DC1からDC2へのリンクコストは0であり、DC3からDC2へのリンクコスト（25）よりも低いため、オブジェクトはDC1から読み出されます。

リンクコストは、測定単位を伴わない任意の相対的な数値です。たとえば、使用にあたってリンクコスト 50 の優先度はリンクコスト 25 よりも低くなります。次の表に、よく使用されるリンクコストを示します。

リンク	リンクコスト	注：
物理データセンターサイト間	25 （デフォルト）	WAN リンクで接続されたデータセンター。
同じ物理的な場所にある論理データセンターサイト間	0	同じ物理ビルディングまたはキャンパスにある論理データセンターを LAN で接続します。

リンクコストを更新します

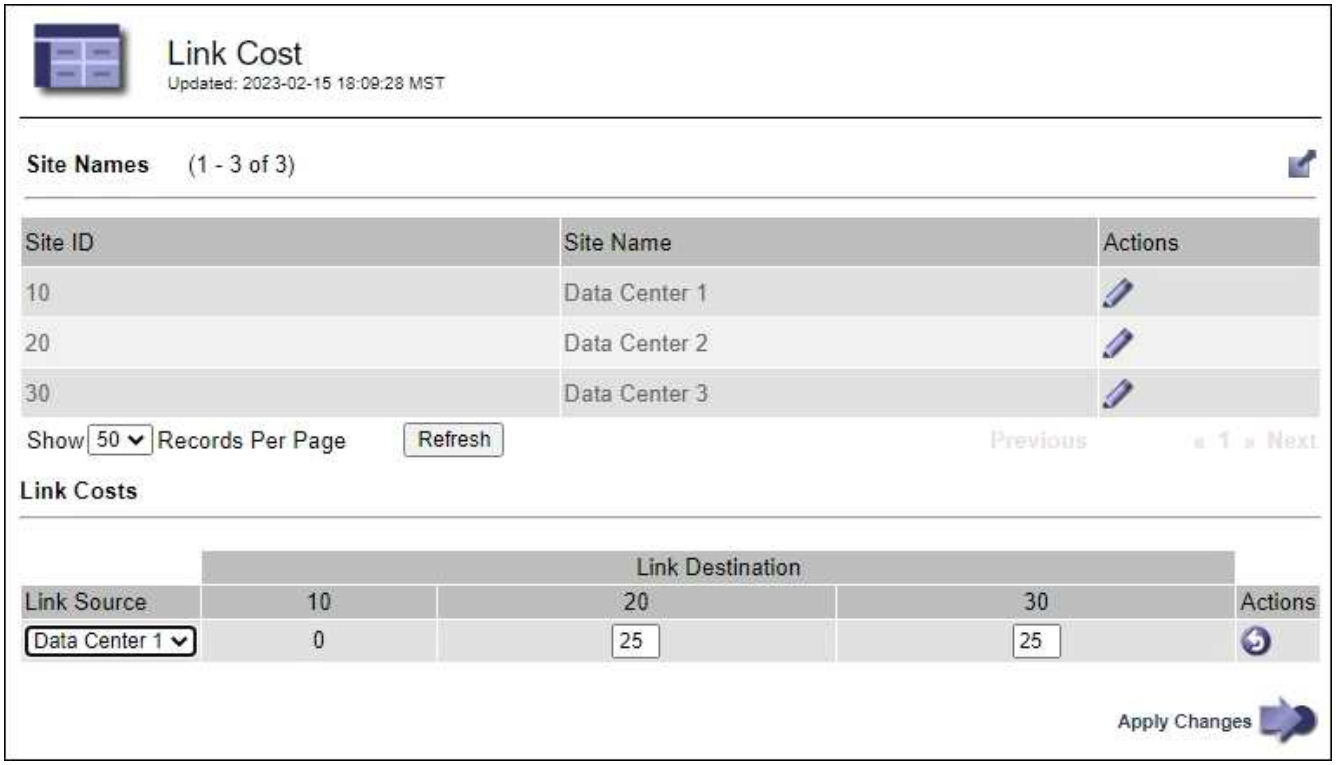
データセンターサイト間のリンクコストを更新して、サイト間のレイテンシを反映させることができます。

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 "Gridトポロジページの設定権限"。

手順

1. * support > other > Link cost *を選択します。



2. [リンク先 *] でサイトを選択し、 [リンク先 *] に 0 ～ 100 のコスト値を入力します。

   送信元が宛先と同じ場合は、リンクコストを変更できません。

   変更をキャンセルするには、を選択します * 復帰 * 。

3. 「 * 変更を適用する * 」を選択します。

AutoSupport を使用します

AutoSupport を使用：概要

AutoSupport 機能を使用すると、 StorageGRID システムのヘルスメッセージおよびステータスメッセージをテクニカルサポートに送信できます。

AutoSupport を使用すると、問題の特定と解決にかかる時間を大幅に短縮できます。また、システムのストレージニーズを監視し、新しいノードやサイトを追加する必要があるかどうかを判断するための支援も行います。必要に応じて、 1 つの別の送信先に AutoSupport メッセージを送信するように設定できます。

StorageGRID AutoSupport はプライマリ管理ノードでのみ設定する必要があります。ただし、を設定する必要があります Hardware AutoSupport の略 各アプライアンス。

AutoSupport メッセージに含まれる情報

AutoSupport メッセージには次のような情報が含まれます。

- StorageGRID ソフトウェアのバージョン
- オペレーティングシステムのバージョン
- システムレベルおよび場所レベルの属性情報
- 最新のアラートとアラーム（従来型システム）
- 履歴データを含む、すべてのグリッドタスクの現在のステータス
- 管理ノードデータベースの使用率
- 失われた、または欠落しているオブジェクトの数
- Grid の設定
- NMS エンティティ
- アクティブな ILM ポリシー
- プロビジョニングされたグリッド仕様ファイル
- 診断メトリック

AutoSupport 機能および個々の AutoSupport オプションは、 StorageGRID の初回インストール時に有効にするか、あとから有効にすることができます。AutoSupport が有効になっていない場合は、グリッド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。このメッセージには、 AutoSupport 設定ページへのリンクが含まれています。

メッセージを閉じても、 AutoSupport が無効なままであっても、ブラウザキャッシュがクリアされるまでは再度表示されません。

Digital Advisorとは

Digital Advisorはクラウドベースで、NetAppのインストールベースから得られた予測分析と集合知を活用します。継続的なリスク評価、予測アラート、規範となるガイダンス、自動化されたアクションによって、問題が発生する前に予防できます。これにより、システムの健全性が向上し、システムの可用性が向上します。

デジタルアドバイザのダッシュボードと機能をNetAppサポートサイトで使用する場合は、AutoSupportを有効にする必要があります。

"Digital Advisorドキュメント"

AutoSupport メッセージを送信するためのプロトコル

AutoSupport メッセージの送信には、次の 3 つのプロトコルのいずれかを選択できます。

- HTTPS
- HTTP
- SMTP

SMTP を AutoSupport メッセージのプロトコルとして使用する場合は、 SMTP メールサーバを設定する必要があります。

AutoSupport オプション

AutoSupport メッセージをテクニカルサポートに送信するには、次のオプションを任意に組み合わせて使用できます。

- * 週単位 * ： AutoSupport メッセージを週に 1 回自動的に送信します。デフォルト設定： Enabled （有効）。
- * イベントトリガー型 * ： 1 時間ごと、または重大なシステムイベントが発生したときに、 AutoSupport メッセージを自動的に送信します。デフォルト設定： Enabled （有効）。
- * On Demand * ： StorageGRID システムが AutoSupport メッセージを自動的に送信するようテクニカルサポートから要求できます。これは、問題 がアクティブに機能している場合に便利です（ HTTPS AutoSupport 転送プロトコルが必要）。デフォルト設定： Disabled （無効）。
- * User-triggered * ： AutoSupport メッセージをいつでも手動で送信します。

[アプライアンスの**AutoSupport**

アプライアンスのAutoSupport ではStorageGRID ハードウェアの問題が報告され、StorageGRID AutoSupport ではStorageGRID ソフトウェアの問題が報告されます（StorageGRID AutoSupport でハードウェアとソフトウェアの両方の問題が報告されるSGF6112を除く）。AutoSupport は、追加の設定を必要としないSGF6112

を除き、各アプライアンスで設定する必要があります。AutoSupport の実装方法は、サービスとストレージアプライアンスで異なります。

各ストレージアプライアンスのSANtricity でAutoSupport を有効にする必要があります。SANtricity AutoSupport は、アプライアンスの初期セットアップ時またはアプライアンスの設置後に設定できます。

- SG6000およびSG5700アプライアンスの場合は、 "SANtricity システムマネージャでAutoSupport を設定します"

でプロキシによるAutoSupport 配信を設定した場合、EシリーズアプライアンスからのAutoSupport メッセージをStorageGRID AutoSupport に含めることができます "SANtricity システムマネージャ"。

StorageGRID AutoSupport では、DIMMやホストインターフェイスカード（HIC）などのハードウェアの問題は報告されません。ただし、一部のコンポーネント障害がトリガーされる可能性があります "ハードウェアアラート"。ベースボード管理コントローラ（BMC）を搭載したStorageGRID アプライアンス（SG100、SG1000、SG6060、SGF6024など）では、ハードウェア障害を報告するためのEメールおよびSNMPトラップを設定できます。

- "アラート用の E メール通知を設定します"
- "SNMPを設定します" SG6000-CNコントローラ、またはSG100およびSG1000サービスアプライアンスの場合

関連情報

"ネットアップサポート"

AutoSupport を設定します

AutoSupport 機能および個々の AutoSupport オプションは、 StorageGRID の初回インストール時に有効にするか、あとから有効にすることができます。

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"。
- Root Access 権限またはその他の Grid 設定権限が必要です。
- AutoSupport メッセージの送信にHTTPSを使用する場合は、プライマリ管理ノードへのアウトバウンドインターネットアクセス（直接または）を設定しておきます "プロキシサーバを使用する" （インバウンド接続は必要ありません）。
- [HTTP] StorageGRID AutoSupport ページで[HTTP]が選択されている場合は、AutoSupport メッセージをHTTPSとして転送するようにプロキシサーバを設定しています。ネットアップのAutoSupport サーバはHTTPを使用して送信されたメッセージを拒否します。

  "管理プロキシの設定について"。

- AutoSupport メッセージのプロトコルとして SMTP を使用する場合は、 SMTP メールサーバを設定しておきます。アラームの E メール通知には同じメールサーバ設定（従来のシステム）が使用されます。

AutoSupport メッセージのプロトコルを指定します

AutoSupport メッセージの送信には、次のいずれかのプロトコルを使用できます。

- * HTTPS * ：これはデフォルトで、新規インストールに推奨される設定です。このプロトコルはポート443を使用します。状況 AutoSupport オンデマンド機能を有効にしますの場合は、HTTPSを使用する必要があります。
- * HTTP *：[HTTP]を選択した場合は、AutoSupport メッセージをHTTPSとして転送するようにプロキシサーバーを設定する必要があります。ネットアップのAutoSupport サーバはHTTPを使用して送信されたメッセージを拒否します。このプロトコルはポート80を使用します。
- * SMTP * ： AutoSupport メッセージを E メールで送信する場合は、このオプションを使用します。SMTP を AutoSupport メッセージのプロトコルとして使用する場合は、レガシー電子メール設定ページ（ * サポート * > * アラーム（レガシー） * > * レガシー電子メール設定 * ）で SMTP メールサーバーを設定する必要があります。

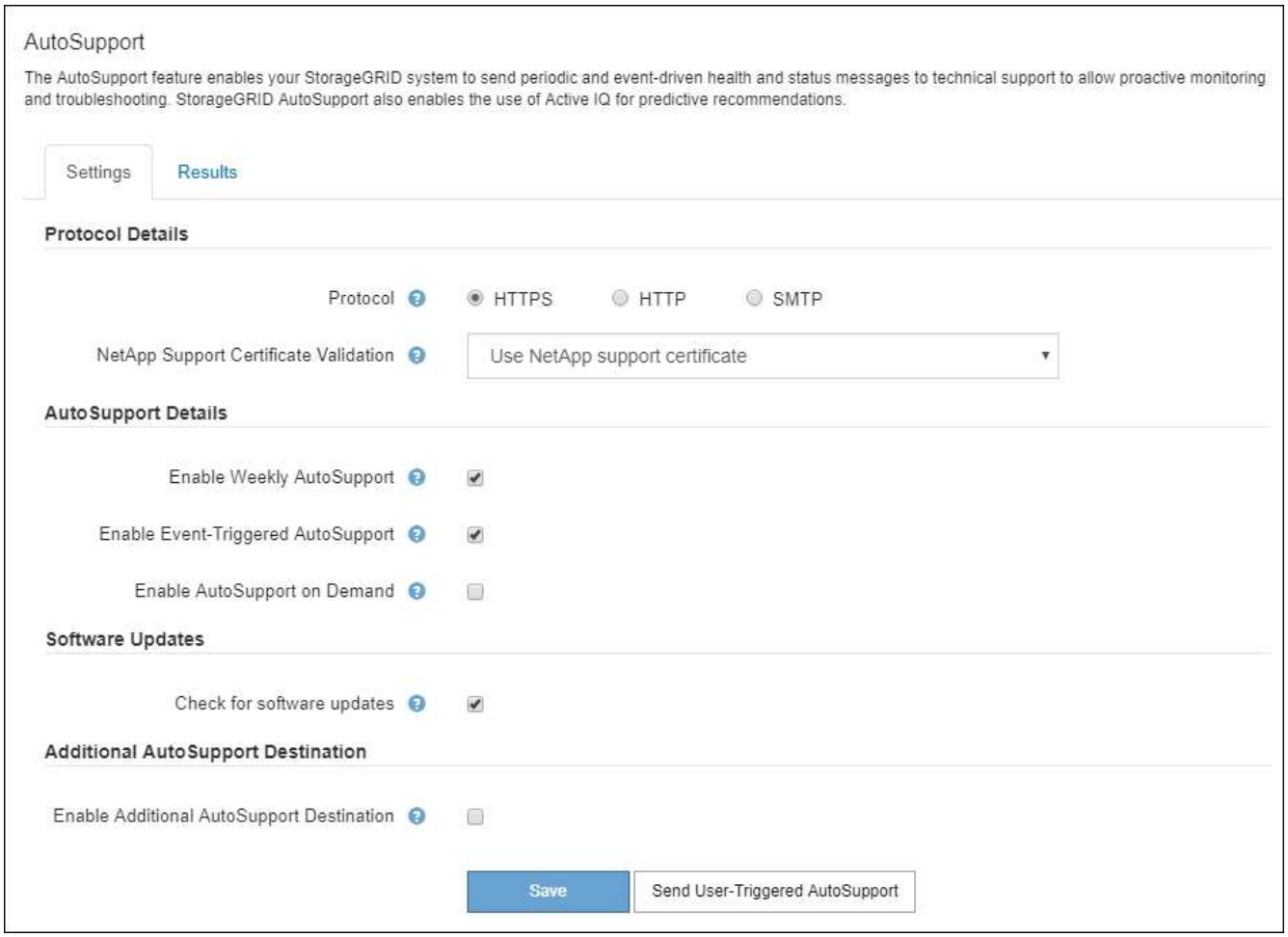
> StorageGRID 11.2 より前のリリースでは、 SMTP が AutoSupport メッセージに使用できる唯一のプロトコルでした。以前のバージョンの StorageGRID をインストールしていた場合は、 SMTP がプロトコルとして選択されている可能性があります。

設定したプロトコルは、すべてのタイプの AutoSupport メッセージの送信に使用されます。

手順

1. [* support * > * Tools * > * AutoSupport *] を選択します。

   AutoSupport ページが表示され、 * 設定 * タブが選択されます。



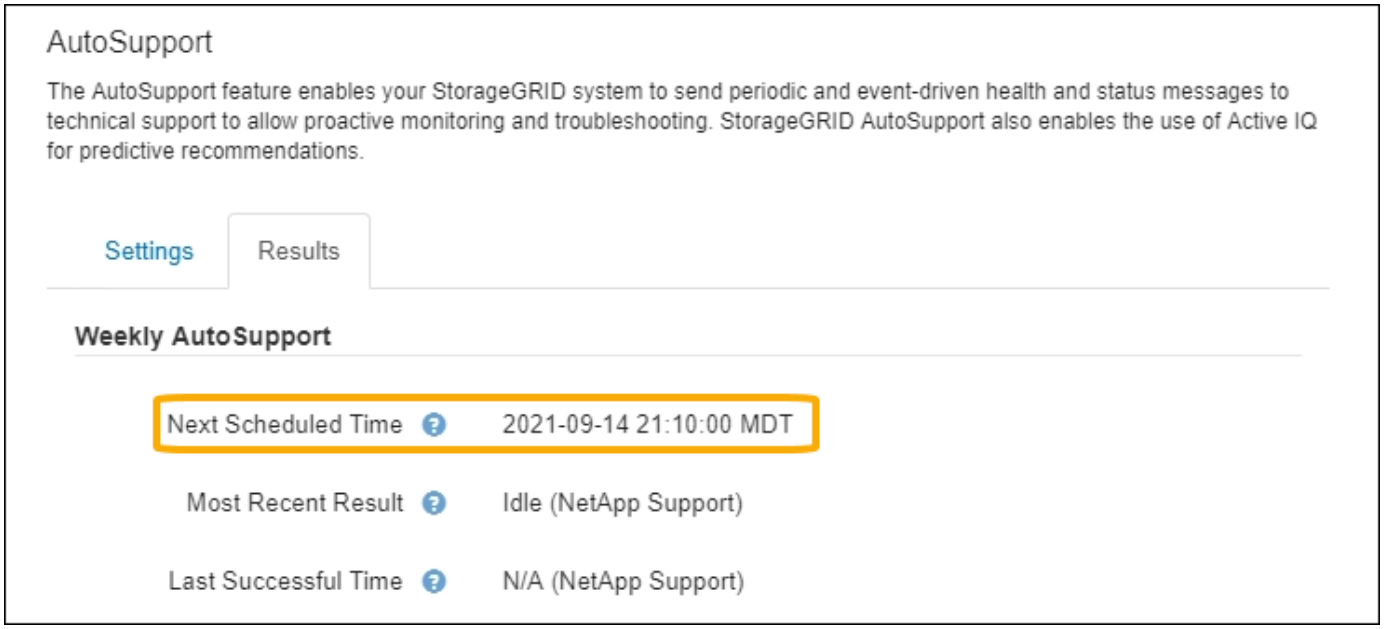
2. AutoSupport メッセージの送信に使用するプロトコルを選択します。
3. 「 * HTTPS * 」を選択した場合、 TLS 証明書を使用してネットアップサポートサーバへの接続を保護するかどうかを選択します。
   - * ネットアップサポート証明書を使用 *（デフォルト）：証明書の検証により、 AutoSupport メッセージの送信を確実に保護します。ネットアップサポート証明書は、 StorageGRID ソフトウェアとともにすでにインストールされています。
   - * 証明書を検証しない * ：このオプションは、証明書に一時的な問題があるなど、証明書の検証を使用しない理由が十分な場合にのみ選択してください。
4. [保存（ Save ）] を選択します。

   毎週、ユーザトリガー型、およびイベントトリガー型のすべてのメッセージが選択したプロトコルを使用して送信されます。

週次 **AutoSupport** メッセージを無効にします

デフォルトでは、 StorageGRID システムは週に 1 回ネットアップサポートに AutoSupport メッセージを送信するように設定されています。

週次 AutoSupport メッセージが送信されるタイミングを確認するには、 * AutoSupport * > * Results * タブに移動します。[* Weekly AutoSupport *] セクションで、 [次のスケジュール時間] の値を確認します。



週単位の AutoSupport メッセージの自動送信はいつでも無効にすることができます。

手順

1. [* support * > * Tools * > * AutoSupport *] を選択します。
2. [毎週のAutoSupport を有効にする]*チェックボックスをオフにします。
3. [保存（ Save ）] を選択します。

イベントトリガー型 **AutoSupport** メッセージを無効にします

デフォルトでは、 StorageGRID システムは、重要なアラートやその他の重大なシステムイベントが発生したときに AutoSupport メッセージをネットアップサポートに送信するように設定されています。

イベントトリガー型 AutoSupport メッセージはいつでも無効にすることができます。

手順

1. [* support * > * Tools * > * AutoSupport *] を選択します。
2. [Enable Event-Triggered AutoSupport *]チェックボックスをオフにします。
3. [保存（ Save ）] を選択します。

AutoSupport On Demand を有効にする

AutoSupport On Demand は、テクニカルサポートが問題解決に積極的に取り組んでいる場合に役立ちます。

デフォルトでは、 AutoSupport On Demand は無効になっています。この機能を有効にすると、テクニカルサポートは、 StorageGRID システムから AutoSupport メッセージを自動的に送信するよう要求できます。テクニカルサポートは、 AutoSupport On Demand クエリのポーリング間隔も設定できます。

テクニカルサポートは、AutoSupport On Demandを有効または無効にできません。

手順

1. [* support * > * Tools * > * AutoSupport *] を選択します。
2. プロトコルの * HTTPS * を選択します。
3. [毎週のAutoSupport を有効にする]*チェックボックスをオンにします。
4. [Enable AutoSupport on Demand]*チェックボックスをオンにします。
5. [保存（ Save ）] を選択します。

   AutoSupport On Demand は有効になっており、テクニカルサポートは AutoSupport On Demand 要求を StorageGRID に送信できます。

ソフトウェアアップデートのチェックを無効にします

デフォルトでは、 StorageGRID はネットアップに連絡して、ご使用のシステムでソフトウェアの更新が利用可能かどうかを判断します。StorageGRID ホットフィックスまたは新しいバージョンが利用可能な場合は、StorageGRID のアップグレードページに新しいバージョンが表示されます。

必要に応じて、ソフトウェアアップデートのチェックを無効にすることもできます。たとえば、 WAN でアクセスできないシステムの場合は、ダウンロードエラーを回避するためにチェックを無効にする必要があります。

手順

1. [* support * > * Tools * > * AutoSupport *] を選択します。
2. [Check for software updates]*チェックボックスをオフにします。
3. [保存（ Save ）] を選択します。

AutoSupport デスティネーションを追加します

AutoSupport を有効にすると、ヘルスメッセージとステータスメッセージがネットアップサポートに送信されます。すべての AutoSupport メッセージに対して、追加の送信先を 1 つ指定できます。

AutoSupport メッセージの送信に使用されるプロトコルを確認または変更するには、の手順を参照してください AutoSupport メッセージのプロトコルを指定します。

SMTPプロトコルを使用してAutoSupport メッセージを追加の送信先に送信することはできません。

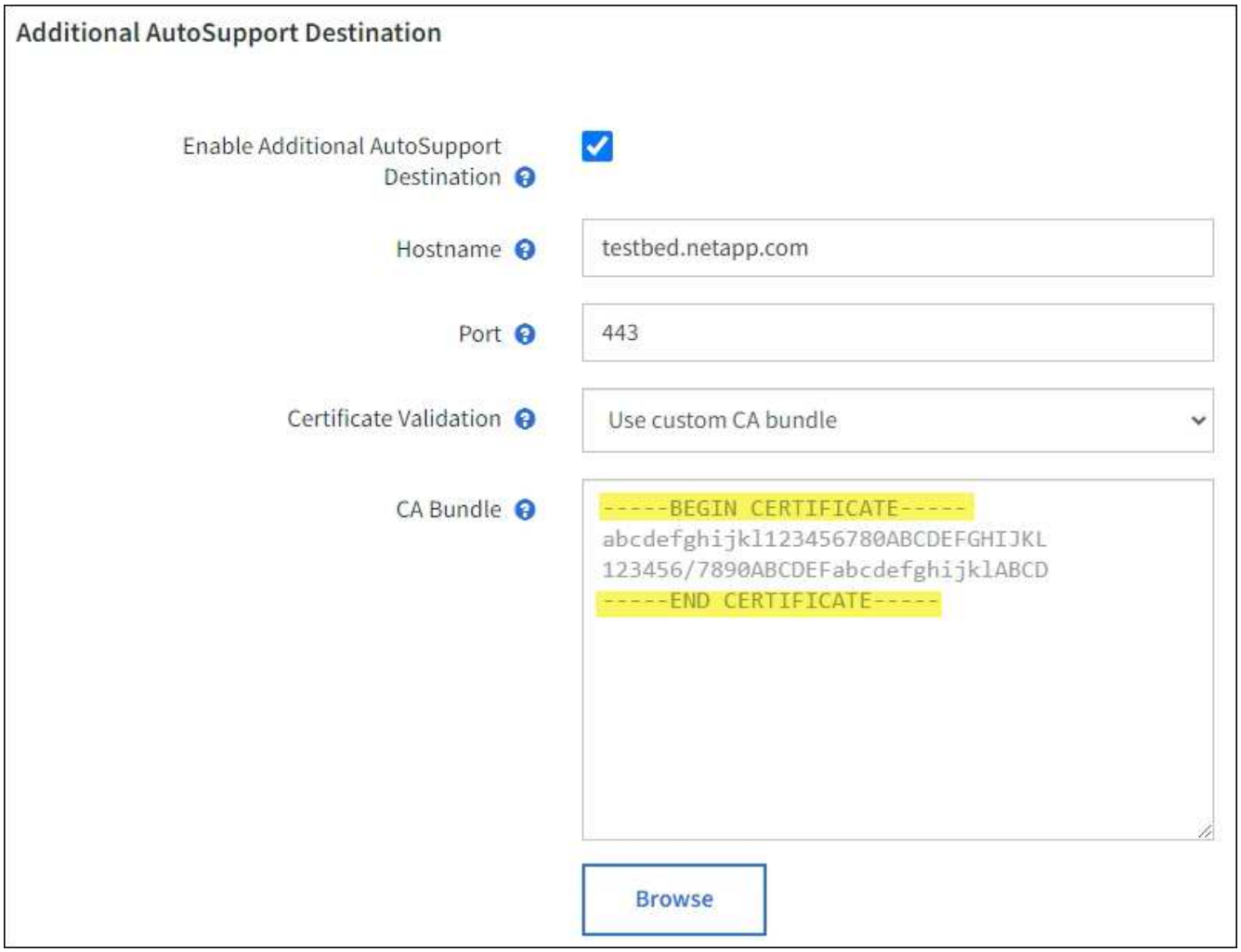
手順

1. [* support * > * Tools * > * AutoSupport *] を選択します。
2. [Enable Additional AutoSupport Destination]*を選択します。
3. 次の情報を指定します。

フィールド	説明
ホスト名	追加のAutoSupport 宛先サーバのサーバホスト名またはIPアドレス。 注：追加の目的地は1つだけ入力できます。
ポート	追加のAutoSupport 宛先サーバへの接続に使用するポート。デフォルトは、HTTPの場合はポート80、HTTPSの場合はポート443です。
証明書の検証	TLS証明書を使用して追加の送信先への接続を保護するかどうか。 • 証明書の検証なしでAutoSupport メッセージを送信するには、[証明書を検証しない]*を選択します。 このオプションは、証明書の検証を使用しない理由がある場合（証明書に一時的な問題がある場合など）にのみ選択してください。 • 証明書の検証を使用する場合は、*[カスタムCAバンドルを使用する]*を選択します。

4. [Use custom CA bundle]*を選択した場合は、次のいずれかを実行します。
   - [* 参照 *] を選択し、証明書が含まれているファイルに移動し、 [* 開く *] を選択してファイルをアップロードします。
   - 編集ツールを使用して、PEMでエンコードされた各CA証明書ファイルのすべての内容を、証明書チェーンの順序で連結された* CA Bundle *フィールドにコピーして貼り付けます。

     を含める必要があります `----BEGIN CERTIFICATE----` および `----END CERTIFICATE----` を選択します。



5. [保存（ Save ）] を選択します。

   それ以降に送信される毎週、イベントトリガー型、およびユーザトリガー型の AutoSupport メッセージは、すべて追加の送信先に送信されます。

AutoSupport メッセージを手動でトリガーする

テクニカルサポートによる StorageGRID システムの問題のトラブルシューティングを支援するために、 AutoSupport メッセージの送信を手動でトリガーできます。

作業を開始する前に

- を使用して Grid Manager にサインインする必要があります "サポートされている Web ブラウザ"。
- Root Access権限またはその他のグリッド設定権限が必要です。

手順

1. [* support * > * Tools * > * AutoSupport *] を選択します。
2. [設定]タブで、*[ユーザートリガーAutoSupport の送信]*を選択します。

   StorageGRID は、テクニカルサポートに AutoSupport メッセージを送信しようとします。試行に成功した場合は、 [結果（ Results ）] タブの [最新結果（ Recent Result ）] * 値と [前回成功した時間（ Last

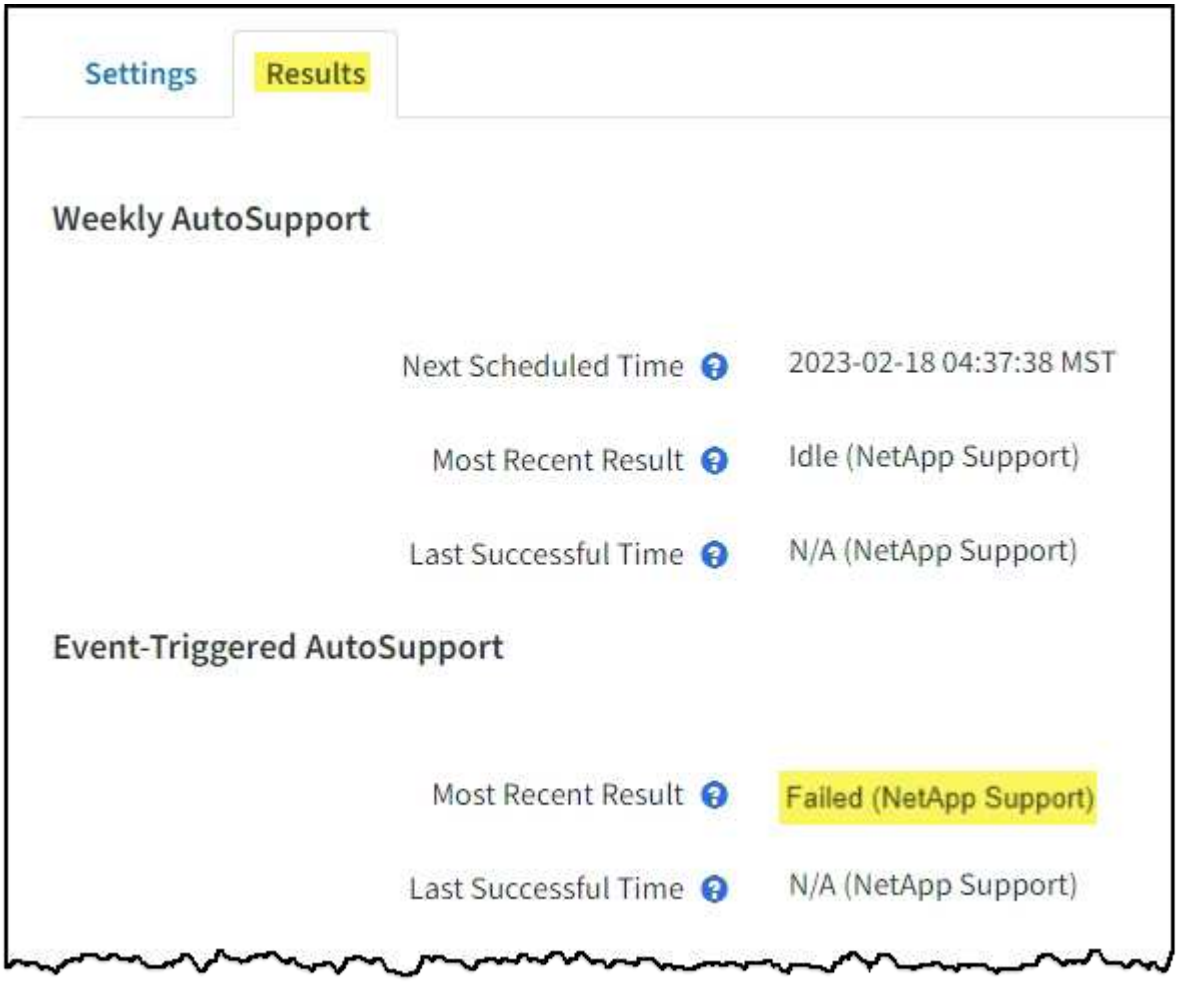
Successful Time ）] * 値が更新されます。問題がある場合、「最新の結果 * 」の値が「失敗」に更新され、 StorageGRID は AutoSupport メッセージの送信を再試行しません。

ユーザトリガー型 AutoSupport メッセージを送信したあと、 1 分後にブラウザの AutoSupport ページを更新して最新の結果にアクセスします。

AutoSupport メッセージのトラブルシューティングを行う

AutoSupport メッセージの送信が失敗すると、 StorageGRID システムは AutoSupport メッセージのタイプに応じて異なる処理を行います。AutoSupport メッセージのステータスを確認するには、 * support * > * Tools * > * AutoSupport * > * Results * を選択します。

AutoSupport メッセージの送信に失敗すると、 AutoSupport ページの * Results * タブに「 Failed 」と表示されます。



AutoSupportメッセージを NetApp に転送するようにプロキシサーバを設定した場合は、 "プロキシサーバの設定が正しいことを確認します。"。

週次 **AutoSupport** メッセージのエラーです

週単位の AutoSupport メッセージの送信に失敗した場合、 StorageGRID システムは次の処理を行います。

1. 最新の結果属性を更新して再試行します。
2. 4 分間隔で 15 回、 1 時間 AutoSupport メッセージの再送信を試みます。
3. 送信エラーが 1 時間発生した後、最新の結果属性を失敗に更新します。
4. AutoSupport メッセージの送信を、次にスケジュールされた時刻に再試行します。
5. NMS サービスが利用できないことが原因でメッセージの送信が失敗した場合、および 7 日以内にメッセージが送信された場合は、 AutoSupport の定期送信スケジュールを維持します。
6. 7 日以上メッセージが送信されていない場合は、 NMS サービスが使用可能な状態に戻った時点で AutoSupport メッセージが送信されます。

ユーザトリガー型またはイベントトリガー型の **AutoSupport** メッセージのエラーです

ユーザトリガー型またはイベントトリガー型の AutoSupport メッセージの送信に失敗した場合、 StorageGRID システムは次の処理を行います。

1. 既知のエラーの場合は、エラーメッセージが表示されます。たとえば、ユーザが正しいEメール設定を指定せずにSMTPプロトコルを選択した場合、次のエラーが表示されます。 `AutoSupport messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`
2. メッセージの再送信は試行されません。
3. にエラーを記録します `nms.log`。

プロトコルとして SMTP が選択されている場合に問題が発生した場合は、 StorageGRID システムの E メールサーバが正しく設定されていることと、 E メールサーバが実行されている（ * support * > * Alarms （レガシー） * > * > Legacy Email Setup * ）ことを確認します。AutoSupport ページに次のエラーメッセージが表示される場合があります。 `AutoSupport messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

方法をご確認ください "Eメールサーバを設定します"。

AutoSupport メッセージのエラーを修正します

プロトコルとして SMTP が選択されている状況で問題が発生した場合は、 StorageGRID システムの E メールサーバが正しく設定されていることと、 E メールサーバが実行されていることを確認します。AutoSupport ページに次のエラーメッセージが表示される場合があります。 `AutoSupport messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

E シリーズ **AutoSupport** メッセージを **StorageGRID** 経由で送信する

E シリーズ SANtricity System Manager AutoSupport メッセージは、ストレージアプライアンスの管理ポートではなく StorageGRID 管理ノードからテクニカルサポートに送信できます。

を参照してください "EシリーズハードウェアAutoSupport" EシリーズアプライアンスでのAutoSupport の使用の詳細については、を参照してください。

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"。
- ストレージアプライアンスの管理者権限またはRoot Access権限が必要です。
- SANtricity AutoSupport が設定されました。
  - SG6000およびSG5700アプライアンスの場合は、 "SANtricity システムマネージャでAutoSupport を設定します"

> Grid Manager を使用して SANtricity System Manager にアクセスするには、 SANtricity ファームウェア 8.70 以降が必要です。

このタスクについて

E シリーズ AutoSupport メッセージには、ストレージハードウェアの詳細が記載されており、 StorageGRID システムから送信される他の AutoSupport メッセージよりも具体的です。

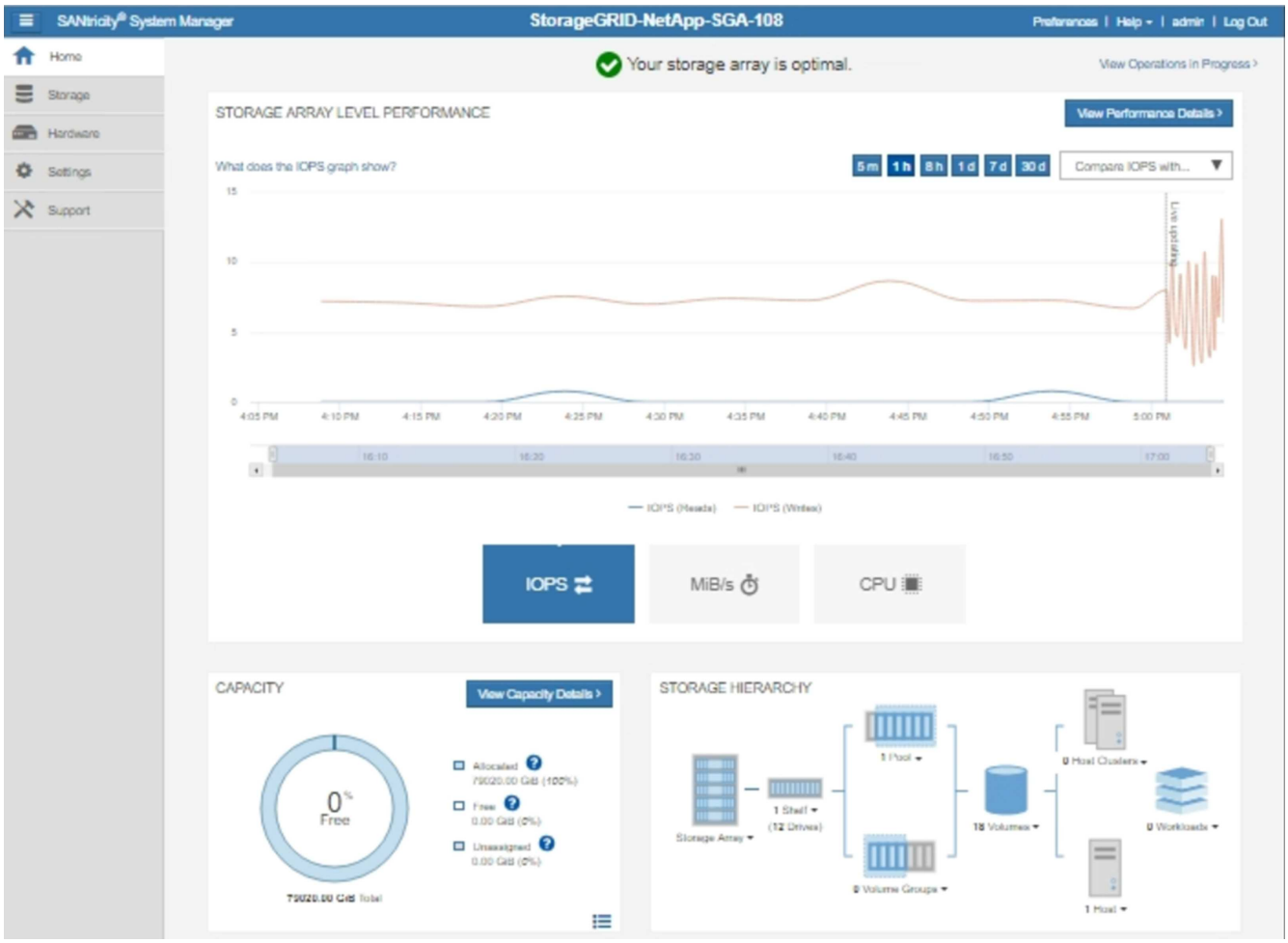
SANtricity System Managerでは、アプライアンスの管理ポートを使用せずにStorageGRID 管理ノード経由でAutoSupport メッセージを送信するように特別なプロキシサーバアドレスを設定できます。この方法で送信されるAutoSupport メッセージは、によって送信されます "優先送信者管理ノード"そして、それらは任意を使用します "管理プロキシの設定" グリッドマネージャで設定されているデータセンターを選択します。

> この手順 は、 E シリーズ AutoSupport メッセージ用に StorageGRID プロキシサーバを設定するためだけに使用します。E シリーズ AutoSupport 構成の詳細については、を参照してください "NetApp E シリーズおよび SANtricity に関するドキュメント"。

手順

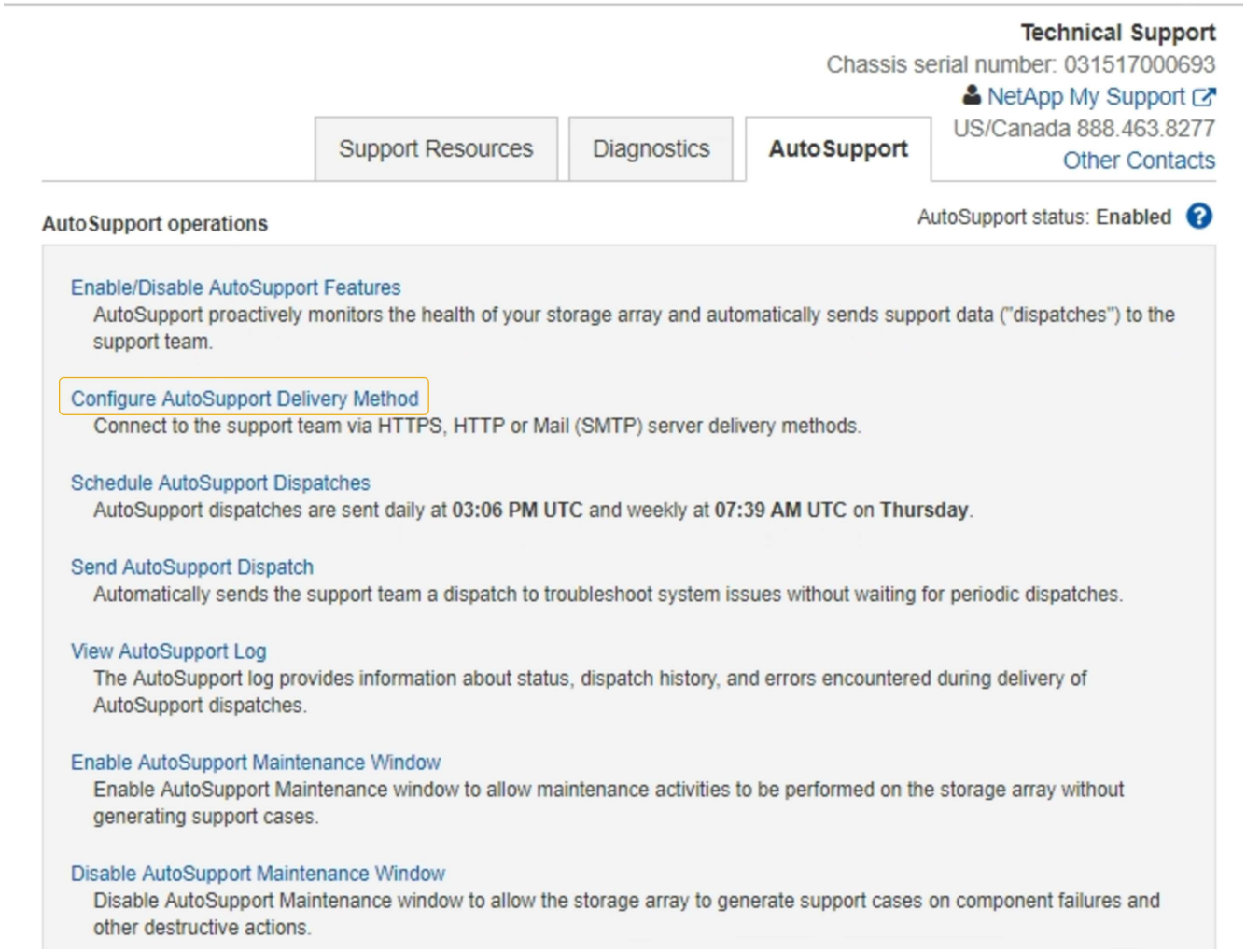
1. Grid Manager で * nodes * を選択します。
2. 左側のノードのリストから、設定するストレージアプライアンスノードを選択します。
3. SANtricity System Manager* を選択します。

   SANtricity の System Manager ホームページが表示されます。



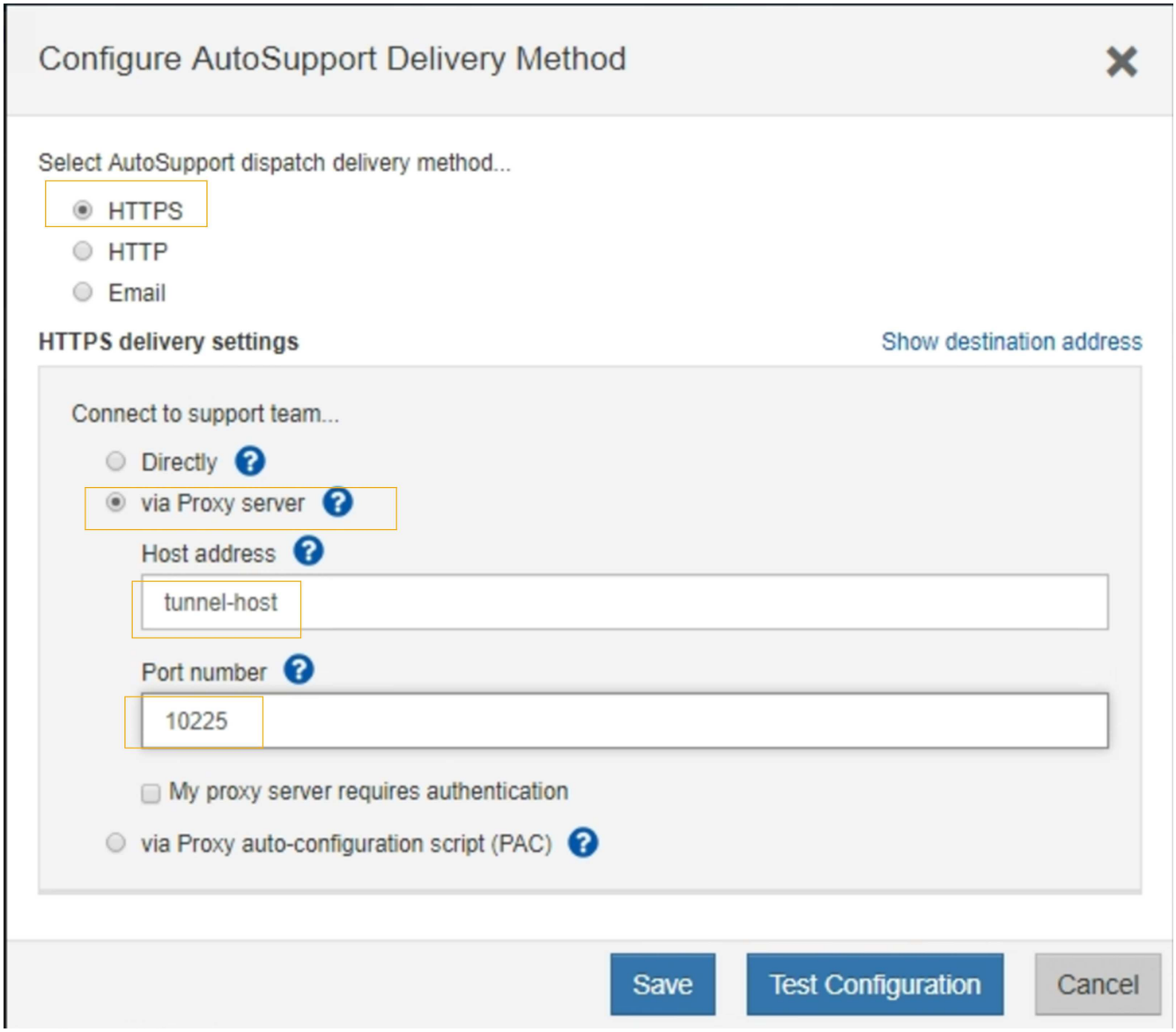
4. サポート * > * サポートセンター * > * AutoSupport * を選択します。

   AutoSupport operations ページが表示されます。



5. AutoSupport 配信方法の設定 * を選択します。

   AutoSupport 配信方法の設定ページが表示されます。



6. 配信方法として「 * HTTPS * 」を選択します。

   HTTPSを有効にする証明書が事前にインストールされています。

7. プロキシサーバー経由 * を選択します。
8. 入力するコマンド `tunnel-host` を入力します。

   `tunnel-host` は、管理ノードを使用してEシリーズAutoSupport メッセージを送信する特別なアドレスです。

9. 入力するコマンド `10225` をクリックします。

   `10225` は、アプライアンスのEシリーズコントローラからAutoSupport メッセージを受信するStorageGRID プロキシサーバのポート番号です。

10. AutoSupport プロキシサーバーのルーティングと設定をテストするには、 * テスト構成 * を選択します。

    正しい場合は、緑色のバナーのメッセージ「 AutoSupport 設定が確認されました。」が表示されます。

テストに失敗した場合は、赤いバナーが表示されます。StorageGRID DNSの設定とネットワークを確認し、を確認します "優先送信者管理ノード" NetApp Support Site に接続して、テストを再試行できます。

11. [保存（ Save ）] を選択します。

構成が保存され ' AutoSupport 配信方法が構成されましたという確認メッセージが表示されます

ストレージノードを管理します

Manage Storage Nodes：概要

ストレージノードは、ディスクストレージの容量とサービスを提供します。ストレージノードの管理には次の作業が必要です。

- ストレージオプションの管理
- ストレージボリュームのウォーターマークと、ストレージノードが読み取り専用になったときにウォーターマークの上書きを使用して制御する方法を理解する
- オブジェクトメタデータに使用されるスペースの監視と管理
- 格納オブジェクトのグローバル設定
- ストレージノード設定を適用しています
- 容量が上限に達したストレージノードの管理

ストレージノードとは

ストレージノードは、オブジェクトデータとメタデータを管理および格納します。各 StorageGRID システムには、少なくとも 3 つのストレージノードが必要です。サイトが複数ある場合は、 StorageGRID システム内の各サイトにも 3 つのストレージノードが必要です。

ストレージノードには、ディスク上のオブジェクトデータとメタデータを格納、移動、検証し、読み出すために必要なサービスとプロセスを提供します。ストレージノードに関する詳細情報は、 * nodes * ページで確認できます。

ADC サービスとは何ですか？

Administrative Domain Controller （ ADC ）サービスは、グリッドノードとその相互接続を認証します。ADC サービスは、サイトにある最初の 3 つのストレージノード上でホストされます。

ADC サービスは、サービスの場所や可用性などのトポロジ情報を管理します。あるグリッドノードが別のグリッドノードからの情報を必要とする場合や、別のグリッドノードによる処理を必要とする場合、そのグリッドノードは ADC サービスにアクセスして要求に最適なグリッドノードを見つけます。また、 ADC サービスは StorageGRID 環境の設定バンドルのコピーを保持するため、すべてのグリッドノードは現在の設定情報を取得できます。ストレージノードの ADC 情報は、グリッドトポロジのページ（ * support * > * Grid topology * ）で表示できます。

分散された処理および孤立した処理に対応するため、各 ADC サービスは、証明書、設定バンドル、およびサービスやトポロジに関する情報を、 StorageGRID システム内の他の ADC サービスと同期します。

一般に、すべてのグリッドノードは少なくとも 1 つの ADC サービスへの接続を維持し、これにより、グリッドノードは常に最新情報にアクセスします。ADC サービスに接続したグリッドノードは他のグリッドノードの証明書をキャッシュするため、ある ADC サービスが利用できない場合でも既知のグリッドノードを使用して引き続き機能できます。新しいグリッドノードが接続を確立するためには、 ADC サービスを使用する必要があります。

ADC サービスは接続された各グリッドノードからトポロジ情報を収集します。このグリッドノード情報には、 CPU 負荷、使用可能なディスクスペース（ストレージがある場合）、サポートされているサービス、およびグリッドノードのサイト ID が含まれます。その他のサービスは、トポロジクエリを介して ADC サービスにトポロジ情報を要求します。ADC サービスは、 StorageGRID システムから受信した最新情報で各クエリに応答します。

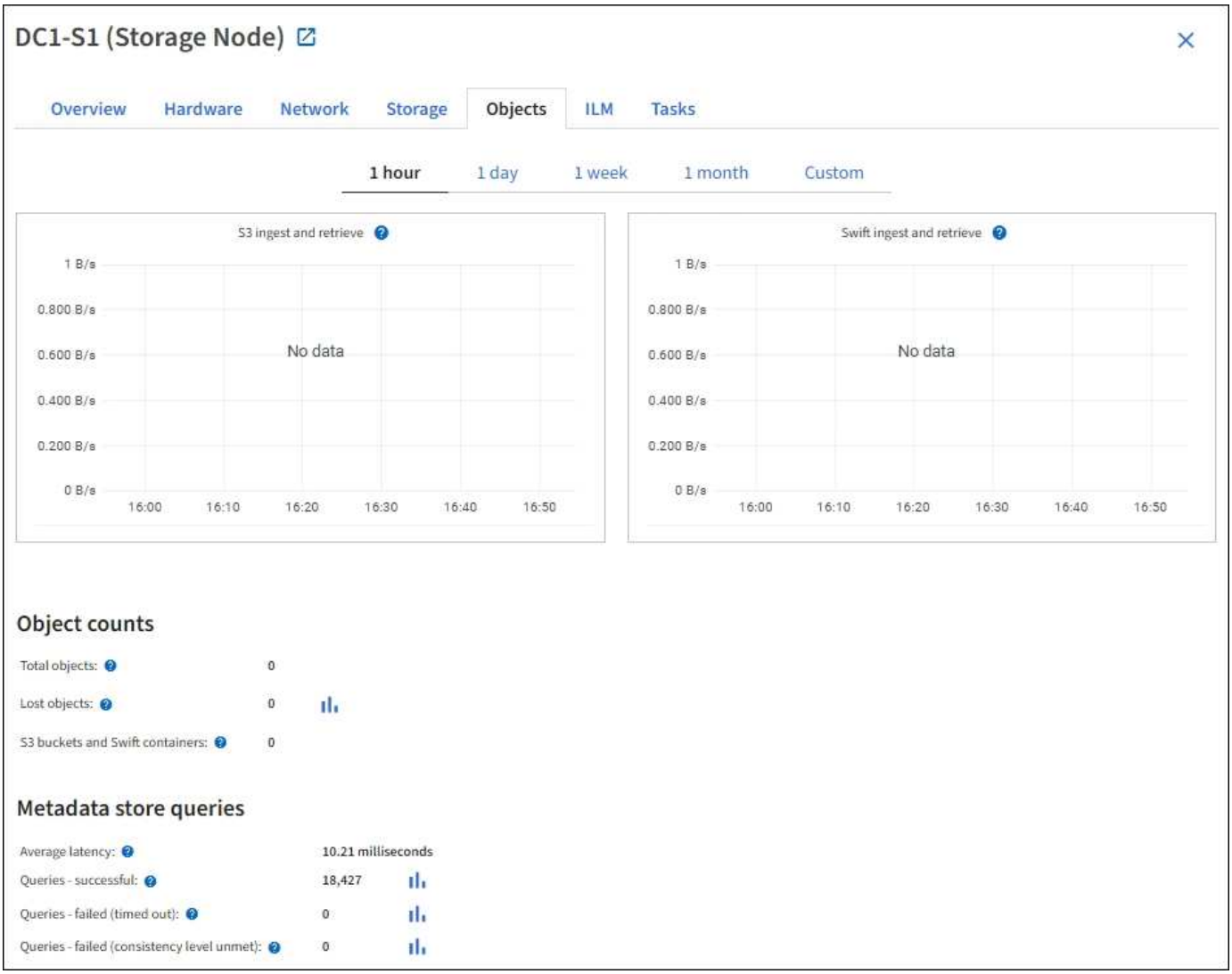
DDS サービスとは何ですか

Distributed Data Store （ DDS ）サービスはストレージノードによってホストされ、 Cassandra データベースとのインターフェイスを提供して、 StorageGRID システムに格納されているオブジェクトメタデータに対してバックグラウンドタスクを実行します。

オブジェクト数

DDS サービスは、 StorageGRID システムに取り込まれたオブジェクトの合計数と、システムでサポートされている各インターフェイス（ S3 または Swift ）を使用して取り込まれたオブジェクトの合計数を追跡します。

すべてのストレージノードについて、ノードページのオブジェクトタブでオブジェクトの総数を確認できます。



クエリ

特定の DDS サービスを使用したメタデータストアに対するクエリの平均実行時間、成功したクエリの合計数、およびタイムアウト問題 が原因で失敗したクエリの合計数を特定できます。

クエリ情報を確認して、メタデータストアである Cassandra の健常性を監視できます。これは、システムの取り込みと読み出しのパフォーマンスに影響します。たとえば、平均的なクエリのレイテンシが遅く、タイムアウトが原因で失敗したクエリの数が多い場合は、メタデータストアの負荷が高いか、または別の処理を実行中である可能性があります。

整合性の問題が原因で失敗したクエリの合計数を確認することもできます。整合性レベルの問題は、特定の DDS サービスを使用してクエリを実行した際に使用可能なメタデータストアの数が不足しているために発生します。

[Diagnostics]ページを使用して、グリッドの現在の状態に関する追加情報 を取得できます。を参照してください "診断を実行します"。

整合性の保証と制御

StorageGRID は、新しく作成されたオブジェクトのリードアフターライト整合性を保証します。正常に完了した PUT 処理に続く GET 処理では、新しく書き込まれたデータを読み取ることができます。既存のオブジェクトの上書き、メタデータの更新、および削除の整合性レベルは、結果整合性です。

LDR サービスとは何ですか。

Local Distribution Router （ LDR ）サービスは各ストレージノードによってホストされ、 StorageGRID システムのコンテンツ転送を処理します。コンテンツ転送には、データストレージ、ルーティング、要求処理など、多数のタスクが含まれます。LDRサービスは、データ転送の負荷とデータトラフィック機能を処理することで、StorageGRID システムのハードワークのほとんどを実行します。

LDR サービスは次のタスクを処理します。

- クエリ
- 情報ライフサイクル管理（ ILM ）のアクティビティ
- オブジェクトの削除
- オブジェクトデータのストレージ
- 別の LDR サービス（ストレージノード）からのオブジェクトデータの転送
- データストレージ管理
- プロトコルインターフェイス（ S3 および Swift ）

また、 LDR サービスは、 StorageGRID システムが取り込まれた各オブジェクトに割り当てる一意な「コンテンツハンドル」（ UUID ）と S3 および Swift オブジェクトのマッピングを管理します。

クエリ

LDR クエリには、読み出しおよびアーカイブ処理におけるオブジェクトの場所のクエリが含まれます。クエリの平均実行時間、成功したクエリの合計数、およびタイムアウト問題 が原因で失敗したクエリの合計数を特定できます。

クエリ情報を確認して、メタデータストアの健常性を監視できます。メタデータストアの健常性は、システムの取り込みと読み出しのパフォーマンスに影響します。たとえば、平均的なクエリのレイテンシが遅く、タイムアウトが原因で失敗したクエリの数が多い場合は、メタデータストアの負荷が高いか、または別の処理を実行中である可能性があります。

整合性の問題が原因で失敗したクエリの合計数を確認することもできます。整合性レベルの問題は、特定の LDR サービスを使用してクエリを実行した際に使用可能なメタデータストアの数が不足しているために発生します。

[Diagnostics]ページを使用して、グリッドの現在の状態に関する追加情報 を取得できます。を参照してください "診断を実行します"。

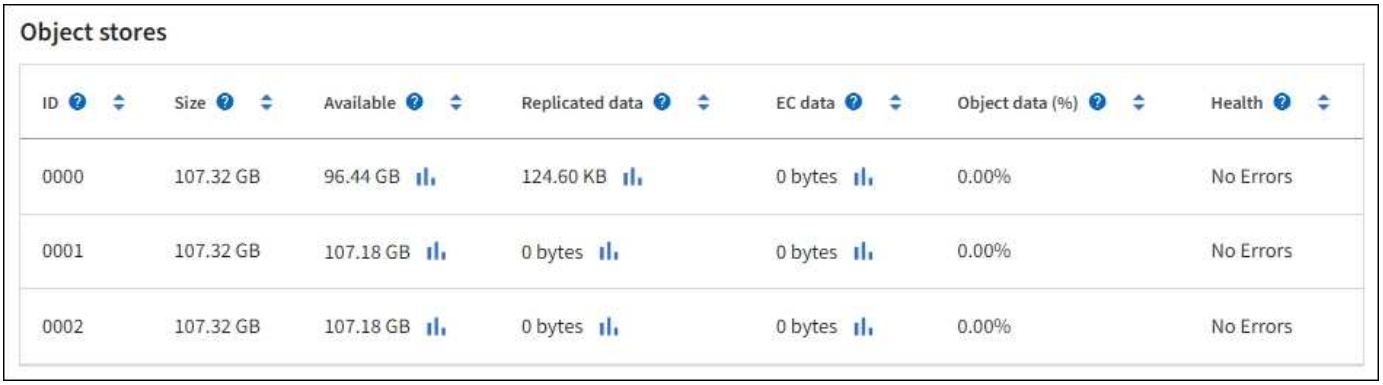
ILM アクティビティ

情報ライフサイクル管理（ ILM ）指標を使用すると、 ILM 実装に対してオブジェクトが評価される速度を監視できます。これらの指標は、ダッシュボードまたは* nodes **>*_ Storage Node_>*** ILM *で確認できます。

オブジェクトストア

LDR サービスの基盤となるデータストレージは、一定数のオブジェクトストア（ストレージボリュームとも呼ばれます）に分割されます。各オブジェクトストアは個別のマウントポイントです。

ストレージノードのオブジェクトストアは、ノードページ > ストレージタブで確認できます。



ストレージノード内のオブジェクトストアは、ボリューム ID と呼ばれる 0000 ~ 002F の 16 進数で識別されます。最初のオブジェクトストア（ボリューム 0 ）では、 Cassandra データベースのオブジェクトメタデータ用にスペースがリザーブされます。このボリュームの残りのスペースはオブジェクトデータに使用されます。他のすべてのオブジェクトストアはオブジェクトデータ専用です。オブジェクトデータにはレプリケートコピーとイレイジャーコーディングフラグメントがあります。

レプリケートコピーのスペース使用量を均等にするために、特定のオブジェクトのオブジェクトデータは、使用可能なストレージスペースに基づいて 1 つのオブジェクトストアに格納されます。1 つ以上のオブジェクトストアの容量を使い果たした場合は、ストレージノード上の容量がなくなるまで、残りのオブジェクトストアが引き続きオブジェクトを格納します。

メタデータの保護

オブジェクトメタデータは、オブジェクトの変更時刻や格納場所など、オブジェクトに関連する情報またはオブジェクトの概要 です。StorageGRID は Cassandra データベースにオブジェクトメタデータを格納します。Cassandra データベースは LDR サービスと連携します。

冗長性を確保してオブジェクトメタデータを損失から保護するために、各サイトでオブジェクトメタデータのコピーが 3 つ保持されます。このレプリケーションは設定できず、自動的に実行されます。

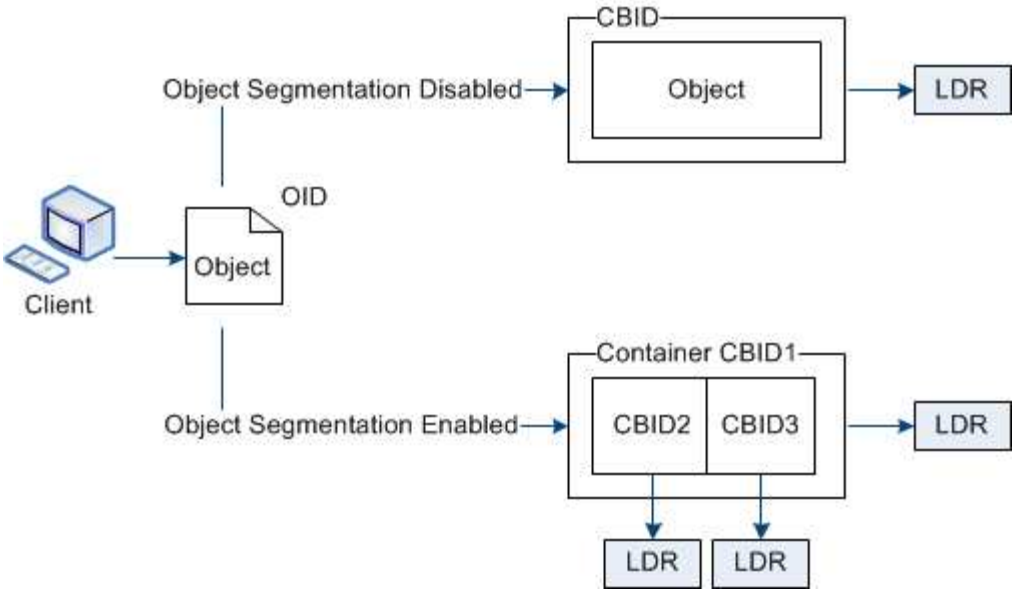
"オブジェクトメタデータストレージを管理する"

[ストレージ]オプションを使用します

オブジェクトのセグメント化とは

オブジェクトのセグメント化は、オブジェクトを小さな固定サイズのオブジェクトの集まりに分割して、大きなオブジェクトのストレージとリソースの使用を最適化するプロセスです。S3 のマルチパートアップロードでもセグメント化されたオブジェクトが作成され、各パートを表すオブジェクトが 1 つ作成されます。

オブジェクトが StorageGRID システムに取り込まれると、 LDR サービスはオブジェクトを複数のセグメントに分割し、すべてのセグメントのヘッダー情報をコンテンツとして表示するセグメントコンテナを作成します。



セグメントコンテナを読み出す際、 LDR サービスは各セグメントから元のオブジェクトを組み立て、クライアントに返します。

コンテナとセグメントは、必ずしも同じストレージノードに格納されるとは限りません。コンテナとセグメントは、 ILM ルールで指定されたストレージプール内の任意のストレージノードに格納できます。

各セグメントは StorageGRID システムによって個別に処理され、 Managed Objects や Stored Objects などの属性の対象としてカウントされます。たとえば、 StorageGRID システムに格納されているオブジェクトが 2 つのセグメントに分割された場合、取り込みが完了すると次のように Managed Objects の値が 3 つ増えます。

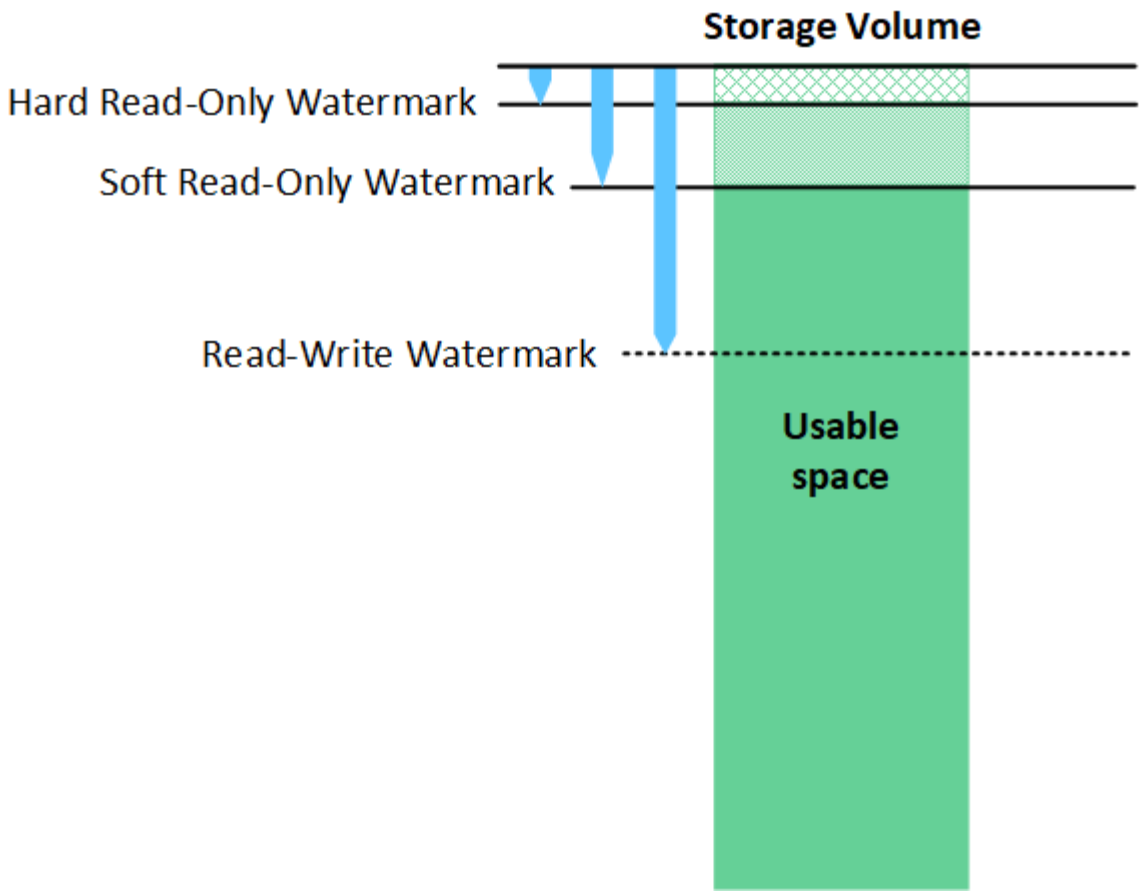
```
segment container + segment 1 + segment 2 = three stored objects
```

大きいオブジェクトを処理する際のパフォーマンスを向上させるには、次の点を確認します。

- 各ゲートウェイおよびストレージノードに、必要なスループットに十分なネットワーク帯域幅があること。たとえば、グリッドネットワークとクライアントネットワークは 10Gbps イーサネットインターフェイス上に別々に設定します。
- 必要なスループットに十分な数のゲートウェイノードとストレージノードが導入されていること。
- 各ストレージノードに、必要なスループットに対して十分なディスクI/Oパフォーマンスがある。

ストレージボリュームのウォーターマークとは何ですか？

StorageGRID では、ストレージボリュームのウォーターマークを 3 つ使用して、スペースの深刻な低下を発生させる前にストレージノードを読み取り専用状態に安全に移行し、読み取り専用状態に移行して再び読み取り / 書き込み可能にすることができます。



ストレージボリュームのウォーターマークは、レプリケートオブジェクトデータとイレイジャーコーディングオブジェクトデータに使用されるスペースにのみ適用されます。ボリューム 0 でオブジェクトメタデータ用にリザーブされているスペースについては、を参照してください"オブジェクトメタデータストレージを管理する"。

Soft Read-Only Watermark とは何ですか？

Storage Volume Soft Read-Only Watermark * は、オブジェクトデータに使用可能なストレージノードのスペースがフルに近づいていることを示す最初のウォーターマークです。

ストレージノード内の各ボリュームの空きスペースがそのボリュームの Soft Read - Only Watermark より少ない場合、ストレージノードは _read-only mode_ に 移行します。読み取り専用モードでは、ストレージノードは StorageGRID システムの他の要素にサービスが読み取り専用であることをアドバタイズしますが、保留中の書き込み要求はすべて実行します。

たとえば、ストレージノード内の各ボリュームにソフト読み取り専用の Watermark が 10GB の場合、各ボリュームの空きスペースが 10GB 未満になると、ストレージノードはソフト読み取り専用モードに移行します。

Hard Read-Only Watermark とは何ですか？

Storage Volume Hard Read-Only Watermark * は、オブジェクトデータに使用可能なノードのスペースがフルに近づいていることを示す 2 つ目のウォーターマークです。

ボリュームの空きスペースがそのボリュームのハード読み取り専用ウォーターマークよりも小さい場合、ボリュームへの書き込みは失敗します。ただし、他のボリュームへの書き込みは、それらのボリュームの空きスペ

ースがハード読み取り専用のウォーターマークよりも少なくなるまで続行できます。

たとえば、ストレージノード内の各ボリュームに Hard Read-Only Watermark が 5GB の状態であるとします。各ボリュームの空きスペースが 5GB 未満になると、ストレージノードは書き込み要求を受け付けなくなります。

Hard Read-Only Watermark は、常に Soft Read-Only Watermark より小さくなります。

Read-Write Watermark とは何ですか

読み取り専用モードに移行した * Storage Volume Read-Write Watermark * 専用環境 ストレージノード。また、ノードが再度読み取り / 書き込み可能になるタイミングを決定します。ストレージノード内のいずれかのストレージボリュームの空きスペースがそのボリュームの Read-Write Watermark より大きい場合、ノードは自動的に読み取り / 書き込み状態に戻ります。

たとえば、ストレージノードが読み取り専用モードに移行したとします。また、各ボリュームの Read-Write Watermark が 30GB であるとします。ボリュームの空きスペースが 30GB に増えると、そのノードは再び読み取り / 書き込み可能になります。

Read-Write Watermark は、 Soft Read-Only Watermark および Hard Read-Only Watermark より常に大きくなります。

ストレージボリュームのウォーターマークを表示する

現在のウォーターマーク設定とシステムに最適化された値を表示できます。最適化された透かしが使用されていない場合は、設定を調整できるかどうかを判断できます。

作業を開始する前に

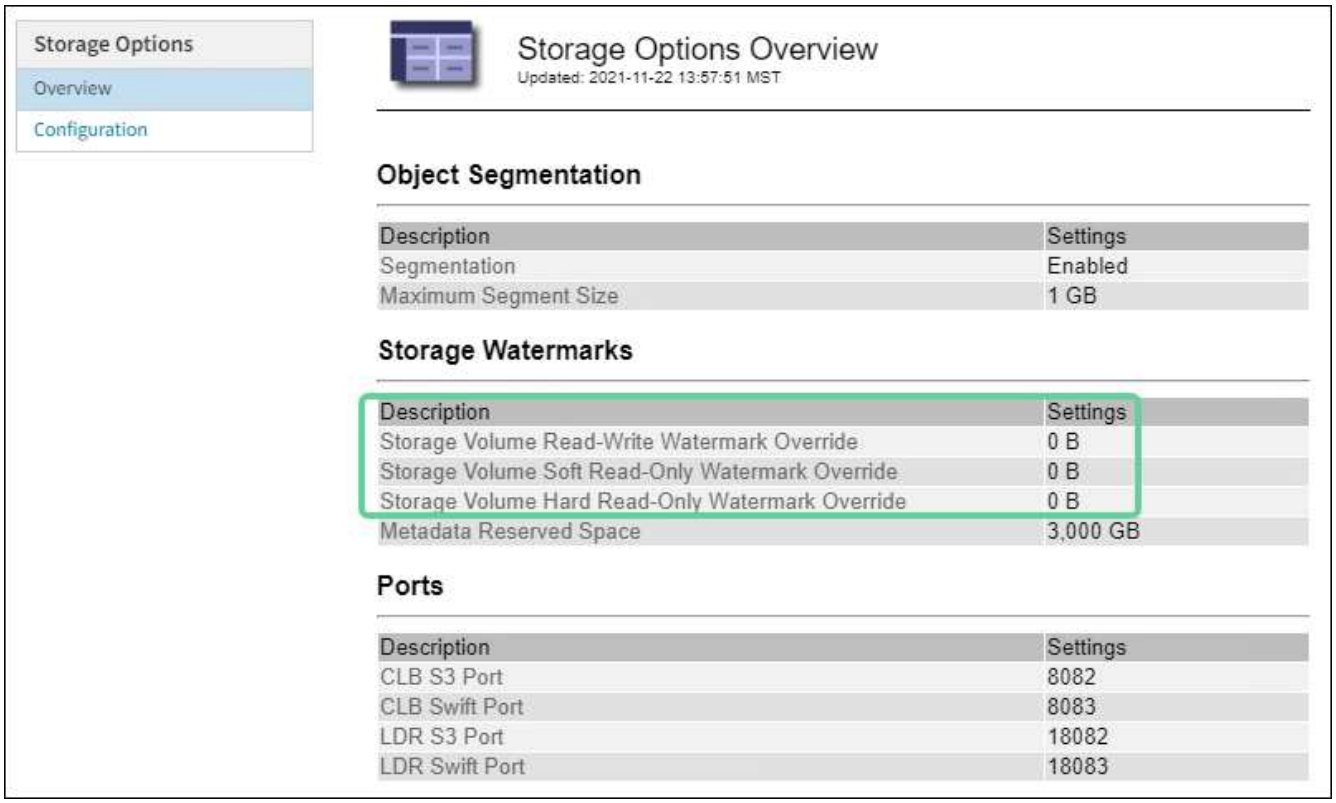
- StorageGRID 11.6以降へのアップグレードが完了している。
- を使用して Grid Manager にサインインします "サポートされている Web ブラウザ"。
- Root アクセス権限が割り当てられている。

現在の透かし設定を表示します

Grid Manager で、現在のストレージのウォーターマーク設定を表示できます。

手順

1. * 設定 * > * システム * > * ストレージ・オプション * を選択します。
2. [ストレージ・ウォーターマーク] セクションで '3 つのストレージ・ボリュームのウォーターマークの上書きに関する設定を確認します



- ウォーターマークの上書きが * 0 * の場合、 3 つのウォーターマークはすべてストレージノードのサイズとボリュームの相対容量に基づいて、各ストレージノード上の各ストレージボリュームに対して最適化されます。

  これがデフォルトで推奨される設定です。これらの値は更新しないでください。必要に応じて、を実行できます [最適化されたストレージウォーターマークを表示する]。

- ウォーターマークの上書きが 0 以外の値の場合は ' カスタム (最適化されていない) ウォーターマークが使用されますカスタム透かし設定の使用はお勧めしません。の手順を使用します "ロー読み取り専用のウォーターマーク上書きアラートのトラブルシューティング" 設定を調整できるかどうかを判断するには、次の手順に従います。

最適化されたストレージウォーターマークを表示する

StorageGRID は、 2 つの Prometheus 指標を使用して、 * Storage Volume Soft Read-Only Watermark * に対して計算された最適値を表示します。グリッド内の各ストレージノードの最適化された最小値と最大値を表示できます。

1. [**support**>] 、 [*Tools] 、 [*Metrics] の順に選択します。
2. Prometheus セクションで、 Prometheus ユーザインターフェイスへのリンクを選択します。
3. 推奨されるソフト読み取り専用の最小ウォーターマークを確認するには、次の Prometheus 指標を入力し、 * Execute * を選択します。

   ```
   storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
   ```

   最後の列には、各ストレージノード上のすべてのストレージボリュームに対して Soft Read-Only Watermark の最小最適値が表示されます。この値が * Storage Volume Soft Read - Only Watermark * のカスタム設定より大きい場合、ストレージノードに対して * Low read-only watermark override * アラートがトリガーされます。

4. 推奨されるソフト読み取り専用の最大ウォーターマークを確認するには、次の Prometheus 指標を入力し、 * Execute * を選択します。

   ```
   storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
   ```

   最後の列には、各ストレージノード上のすべてのストレージボリュームに対して Soft Read-Only Watermark の最大最適値が表示されます。

オブジェクトメタデータストレージを管理する

StorageGRID システムのオブジェクトメタデータ容量は、そのシステムに格納できるオブジェクトの最大数を制御します。StorageGRID システムに新しいオブジェクトを格納するための十分なスペースを確保するには、 StorageGRID がオブジェクトメタデータを格納する場所と方法を理解する必要があります。

オブジェクトメタデータとは

オブジェクトメタデータは、オブジェクトについて記述された任意の情報です。StorageGRID では、オブジェクトメタデータを使用してグリッド全体のすべてのオブジェクトの場所を追跡し、各オブジェクトのライフサイクルを継続的に管理します。

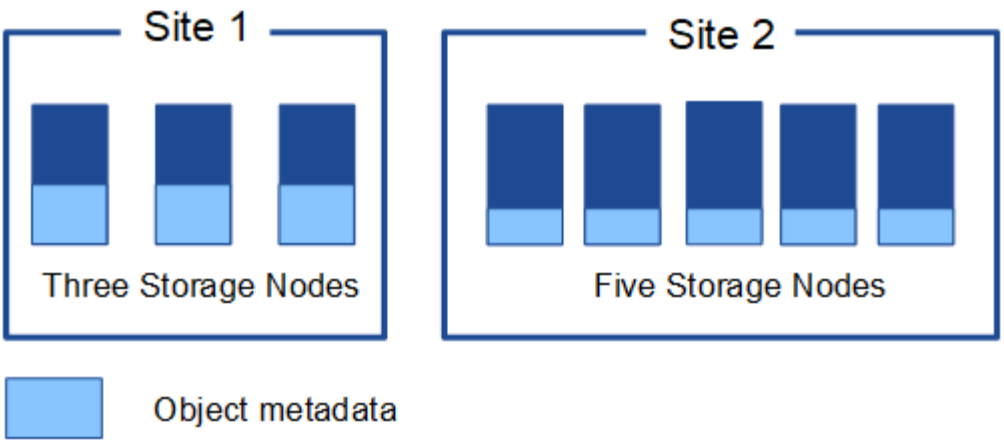
StorageGRID のオブジェクトの場合、オブジェクトメタデータには次の種類の情報が含まれます。

- システムメタデータ（各オブジェクトの一意の ID （ UUID ）、オブジェクト名、 S3 バケットまたは Swift コンテナの名前、テナントアカウントの名前または ID 、オブジェクトの論理サイズ、オブジェクトの作成日時など）、 オブジェクトが最後に変更された日時。
- オブジェクトに関連付けられているカスタムユーザメタデータのキーと値のペア。
- S3 オブジェクトの場合、オブジェクトに関連付けられているオブジェクトタグのキーと値のペア。
- レプリケートオブジェクトコピーの場合、各コピーの現在の格納場所。
- イレイジャーコーディングオブジェクトコピーの場合、各フラグメントの現在の格納場所。
- クラウドストレージプール内のオブジェクトコピーの場合、外部バケットの名前とオブジェクトの一意の識別子を含むオブジェクトの場所。
- セグメント化されたオブジェクトやマルチパートオブジェクトの場合、セグメント ID とデータサイズ。

オブジェクトメタデータの格納方法

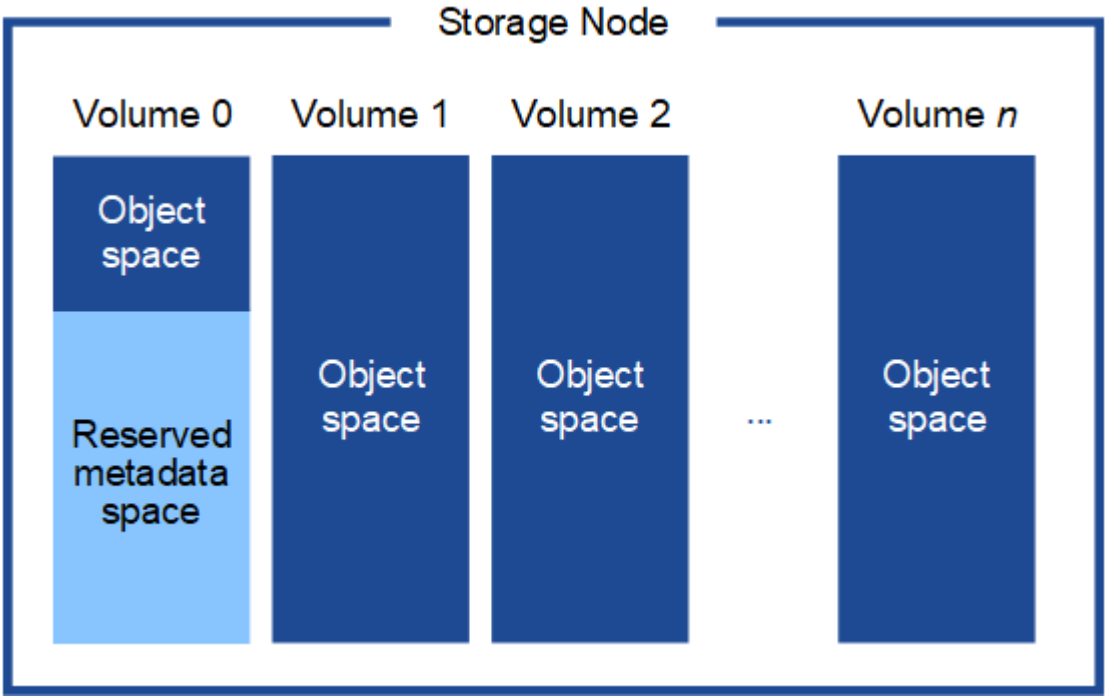
StorageGRID は Cassandra データベースにオブジェクトメタデータを保持し、 Cassandra データベースはオブジェクトデータとは別に格納されます。冗長性を確保し、オブジェクトメタデータを損失から保護するために、 StorageGRID は各サイトのシステム内のすべてのオブジェクトにメタデータのコピーを 3 つずつ格納します。

この図は、 2 つのサイトのストレージノードを表しています。各サイトには同じ量のオブジェクトメタデータが格納され、各サイトのメタデータがそのサイトのすべてのストレージノードに分割されます。



オブジェクトメタデータの格納先

この図は、単一のストレージノードのストレージボリュームを表しています。



図に示すように、 StorageGRID は各ストレージノードのストレージボリューム 0 にオブジェクトメタデータ用のスペースをリザーブします。リザーブスペースを使用してオブジェクトメタデータを格納し、重要なデータベース処理を実行します。ストレージボリューム 0 の残りのスペースとストレージノード内のその他すべてのストレージボリュームは、オブジェクトデータ（レプリケートコピーとイレイジャーコーディングフラグメント）専用に使用されます。

特定のストレージノードでオブジェクトメタデータ用にリザーブされるスペースの量は、いくつかの要因によって異なります。以下にその例を示します。

Metadata Reserved Space の設定

Metadata Reserved Space _ は、各ストレージノードのボリューム 0 でメタデータ用にリザーブされるスペースの量を表すシステム全体の設定です。次の表に示すように、この設定のデフォルト値は次の基準に基づいています。

- StorageGRID の最初のインストール時に使用していたソフトウェアバージョン。
- 各ストレージノード上の RAM の容量。

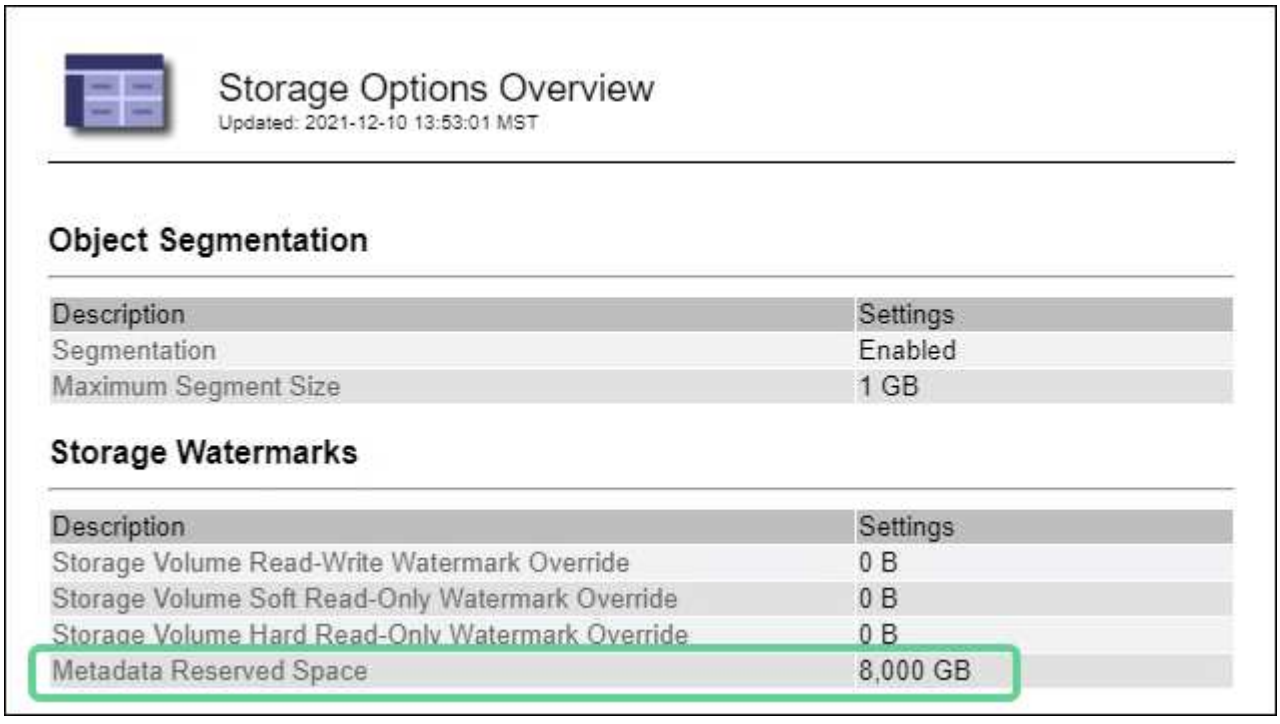
StorageGRID の初期インストールに使用するバージョン	ストレージノード上の **RAM** の容量	**Metadata Reserved Space**のデフォルト設定
11.5から11.7	グリッド内の各ストレージノードで 128GB 以上	8 TB （ 8 、 000 GB ）
	グリッド内の任意のストレージノードで 128GB 未満	3TB （ 3 、 000GB ）
11.1 ～ 11.4	いずれかのサイトの各ストレージノードで 128GB 以上	4TB （ 4 、 000GB ）
	各サイトのストレージノードで 128GB 未満	3TB （ 3 、 000GB ）
11.0 以前	任意の金額	2TB （ 2 、 000 GB ）

Metadata Reserved Space設定を表示します

StorageGRID システムのMetadata Reserved Space設定を表示するには、次の手順を実行します。

手順

1. * 設定 * > * システム * > * ストレージ・オプション * を選択します。
2. Storage Watermarks テーブルで、 * Metadata Reserved Space * を探します。



スクリーンショットでは、「 * Metadata Reserved Space * 」の値が 8 、 000 GB （ 8 TB ）になっています。各ストレージノードに128GB以上のRAMが搭載されているStorageGRID 11.6以降の新規インストールでは、これがデフォルト設定です。

メタデータ用にリザーブされている実際のスペース

システム全体の Metadata Reserved Space 設定とは異なり、オブジェクトメタデータ用の実際のリザーブスペースは、ストレージノードごとに決定されます。ある特定のストレージノードについて、メタデータ用に実際にリザーブされるスペースは、ノードのボリューム 0 のサイズとシステム全体の * Metadata Reserved Space * 設定によって異なります。

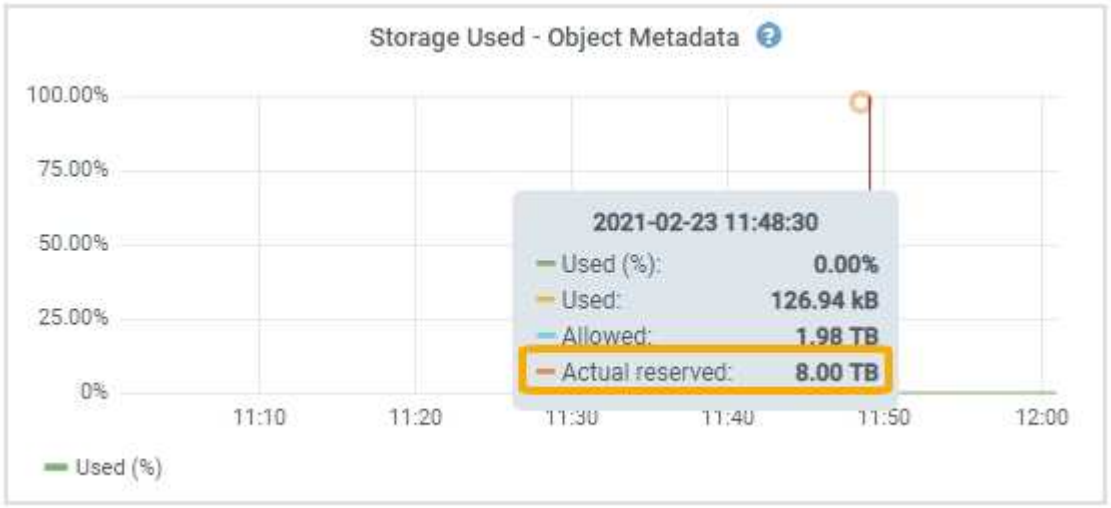
ノードのボリューム **0** のサイズ	メタデータ用にリザーブされている実際のスペース
500GB 未満（非本番環境で使用）	ボリューム 0 の 10%
500GB 以上	次の値のうち小さい方： • ボリューム 0 • Metadata Reserved Space の設定

メタデータ用に実際にリザーブされているスペースを表示する

特定のストレージノードでメタデータ用に実際にリザーブされているスペースを表示する手順は、次のとおりです。

手順

1. Grid Manager から * nodes * > * _ Storage Node_* を選択します。
2. [* ストレージ *] タブを選択します。
3. [Storage Used - Object Metadata]グラフにカーソルを合わせ、* Actual Reserved *の値を確認します。



スクリーンショットでは、実際の予約数 * の値は 8TB です。このスクリーンショットは、 StorageGRID 11.6 を新規にインストールした大規模ストレージノードのものです。システム全体の Metadata Reserved Space 設定がこのストレージノードのボリューム 0 よりも小さいため、このノードの実際のリザーブスペースは

Metadata Reserved Space 設定と同じです。

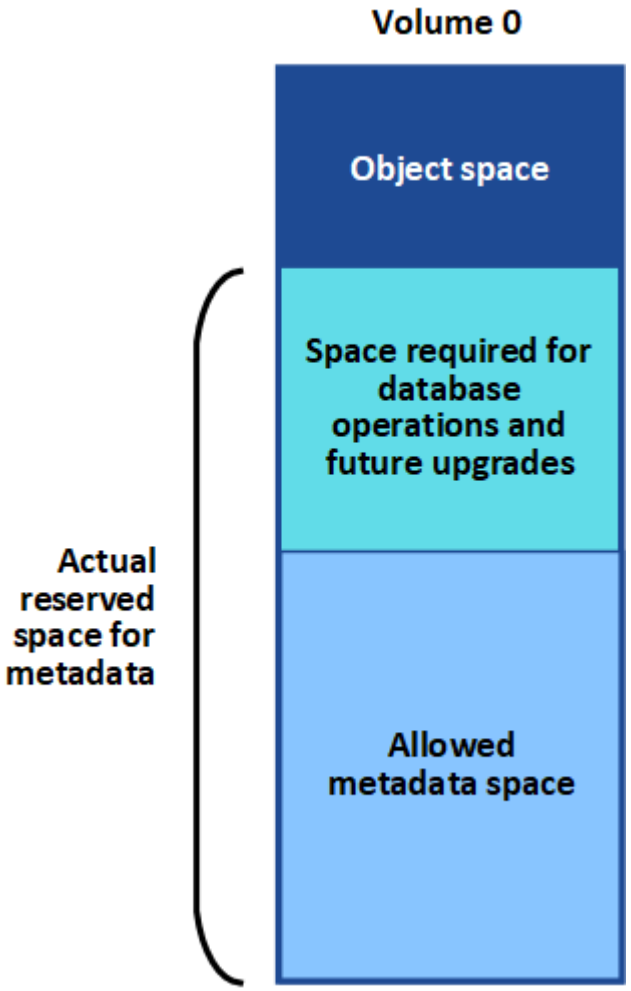
実際にリザーブされているメタデータスペースの例

バージョン11.7を使用して新しいStorageGRID システムをインストールするとします。この例では、各ストレージノードの RAM が 128GB を超え、ストレージノード 1 （ SN1 ）のボリューム 0 が 6TB であるとします。次の値に基づきます。

- システム全体の * Metadata Reserved Space * が 8TB に設定されている（各ストレージノードのRAMが128GBを超える場合、新しいStorageGRID 11.6以降のインストールのデフォルト値です）。
- SN1 のメタデータ用にリザーブされている実際のスペースは 6TB です。（ボリューム 0 が * Metadata Reserved Space * 設定より小さいため、ボリューム全体がリザーブされます）。

許可されているメタデータスペースです

メタデータ用に実際に予約されている各ストレージノードは、オブジェクトメタデータに使用できるスペース（許容されるメタデータスペース _ ）と、重要なデータベース処理（コンパクションや修復など）や将来のハードウェアおよびソフトウェアのアップグレードに必要なスペースに分割されます。許可されるメタデータスペースは、オブジェクトの全体的な容量を決定します。



次の表に、各ストレージノードのメモリ容量とメタデータ用に実際にリザーブされているスペースに基づいてStorageGRID で許容されるメタデータスペース*がどのように計算されるかを示します。

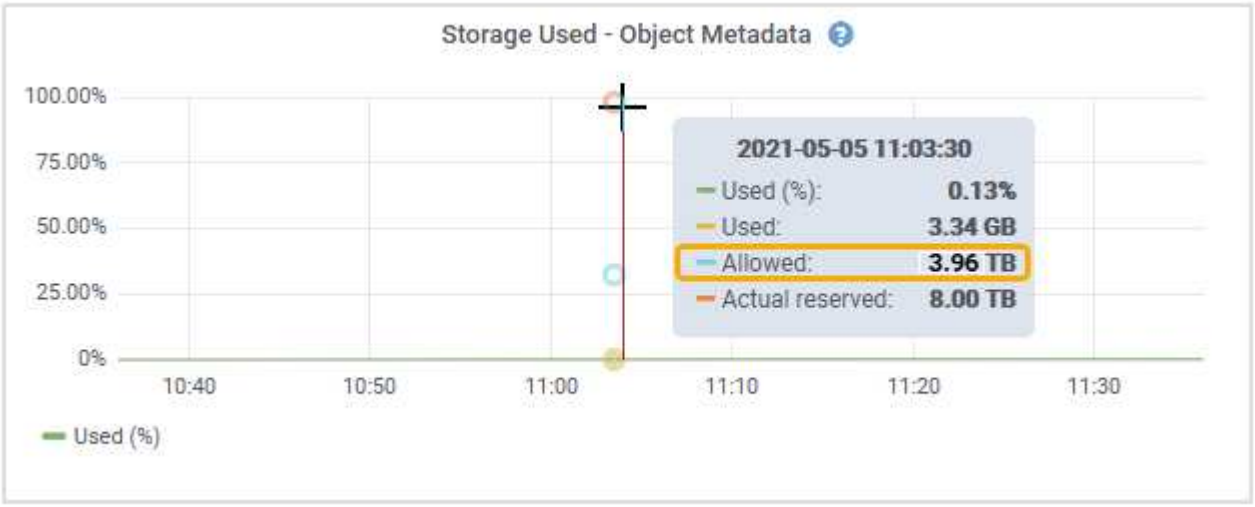
		ストレージノード上のメモリ容量	
	< 128 GB	= 128 GB	メタデータ用に実際にリザーブされているスペース
⇦4 TB	メタデータ用にリザーブされている実際のスペースの 60% 、最大 1.32TB	メタデータ用にリザーブされている実際のスペースの 60% 。最大 1.98 TB	4 TB

許可されているメタデータスペースを表示する

ストレージノードで許可されているメタデータスペースを表示するには、次の手順を実行します。

手順

1. Grid Manager から * nodes * を選択します。
2. ストレージノードを選択します。
3. [* ストレージ *] タブを選択します。
4. [Storage Used - object metadata]グラフにカーソルを合わせ、* allowed *の値を確認します。



スクリーンショットでは、「許可」の値は3.96TBです。これは、メタデータ用に実際にリザーブされているスペースが4TBを超えるストレージノードの最大値です。

「 * Allowed * 」の値は、次の Prometheus 指標に対応します。

```
storagegrid_storage_utilization_metadata_allowed_bytes
```

許可されるメタデータスペースの例

バージョン 11.6 を使用して StorageGRID システムをインストールするとします。この例では、各ストレージノードの RAM が 128GB を超え、ストレージノード 1 （ SN1 ）のボリューム 0 が 6TB であるとします。次

の値に基づきます。

- システム全体の * Metadata Reserved Space * が 8TB に設定されている（各ストレージノードのRAMが128GBを超える場合のStorageGRID 11.6以降のデフォルト値です）。
- SN1 のメタデータ用にリザーブされている実際のスペースは 6TB です。（ボリューム 0 が * Metadata Reserved Space * 設定より小さいため、ボリューム全体がリザーブされます）。
- SN1でのメタデータの許容スペースは、に示す計算に基づいて3TBです メタデータに使用できるスペースの表：（メタデータ用に実際にリザーブされるスペース−1TB）×60%、最大3.96TB。

サイズの異なるストレージノードがオブジェクト容量に与える影響

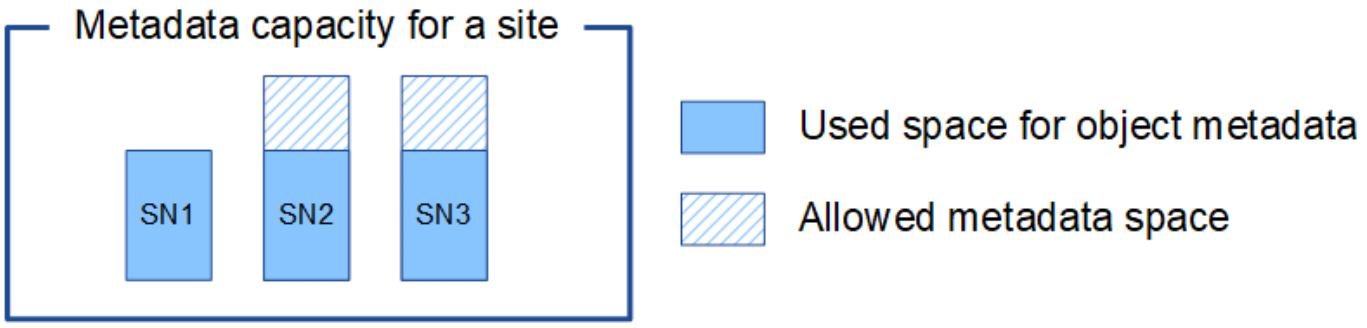
前述したように、 StorageGRID は各サイトのストレージノードにオブジェクトメタデータを均等に分散します。このため、サイトにサイズが異なるストレージノードがある場合、サイトで一番小さいノードがサイトのメタデータ容量を決定します。

次の例を考えてみましょう。

- サイズの異なる 3 つのストレージノードを含む単一サイトのグリッドがある。
- Metadata Reserved Space * の設定は 4TB です。
- ストレージノードには、リザーブされている実際のメタデータスペースと許可されているメタデータスペースについて、次の値があります。

ストレージノード	ボリューム **0** のサイズ	リザーブされている実際のメタデータスペースです	許可されているメタデータスペースです
SN1.	2.2 TB	2.2 TB	1.32TB をサポートします
SN2.	5 TB	4 TB	1.98 TB
SN3	6TB	4 TB	1.98 TB

オブジェクトメタデータはサイトのストレージノード間で均等に分散されるため、この例の各ノードが格納できるメタデータは 1.32TB です。SN2およびSN3で使用できる追加の0.66TBのメタデータスペースは使用できません。



同様に、 StorageGRID は各サイトで StorageGRID システムのすべてのオブジェクトメタデータを管理するため、 StorageGRID システム全体のメタデータ容量は最小サイトのオブジェクトメタデータ容量で決まりま

す。

また、オブジェクトメタデータの容量はオブジェクトの最大数に制御されるため、一方のノードがメタデータの容量を超えると、実質的にグリッドがフルになります。

関連情報

- 各ストレージノードのオブジェクトメタデータ容量を監視する方法については、の手順を参照してください "StorageGRID の監視"。
- システムのオブジェクトメタデータ容量を増やすには、 "グリッドを展開します" 新しいストレージノードを追加する。

メタデータ予約領域設定を増やす

ストレージ ノードが RAM と使用可能なスペースに関する特定の要件を満たしている場合は、メタデータ予約済みスペースのシステム設定を増やすことができる可能性があります。

要件

- 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 Web ブラウザ"。
- あなたは "ルートアクセス権限またはグリッドトポロジページ構成およびその他のグリッド構成権限"。

このタスクについて

システム全体のメタデータ予約領域設定を手動で最大 8 TB まで増やせる可能性があります。

次の両方の条件が満たされている場合にのみ、システム全体のメタデータ予約領域設定の値を増やすことができます。

- システム内のどのサイトにあるストレージ ノードにも、それぞれ 128 GB 以上の RAM が搭載されています。
- システム内のどのサイトにあるストレージ ノードでも、ストレージ ボリューム 0 に十分な空き容量があります。

この設定を増やすと、すべてのストレージ ノードのストレージ ボリューム 0 上のオブジェクト ストレージに使用可能なスペースが同時に減少することに注意してください。このため、予想されるオブジェクト メタデータの要件に基づいて、メタデータ予約領域を 8 TB 未満の値に設定することをお勧めします。

> 一般的に、低い値よりも高い値を使用する方が適切です。メタデータ予約領域の設定が大きすぎる場合は、後で減らすことができます。一方、後で値を増やすと、スペースを解放するためにシステムがオブジェクト データを移動する必要がある場合があります。

メタデータ予約領域設定が特定のストレージノード上のオブジェクトメタデータストレージに許可される領域にどのように影響するかの詳細については、以下を参照してください。 "オブジェクトメタデータストレージを管理する"。

手順

1. 現在のメタデータ予約領域の設定を確認します。
   a. * 設定 * > * システム * > * ストレージ・オプション * を選択します。
   b. ストレージ ウォーターマーク セクションで、メタデータ予約済み領域 の値をメモします。

2. この値を増やすには、各ストレージ ノードのストレージ ボリューム 0 に十分な空き容量があることを確認してください。

   a. [* nodes （ノード）] を選択します

   b. グリッド内の最初のストレージ ノードを選択します。

   c. ストレージタブを選択します。

   d. ボリューム セクションで、**/var/local/rangedb/0** エントリを見つけます。

   e. 使用可能な値が、使用する新しい値と現在のメタデータ予約済みスペースの値の差以上であることを確認します。

      たとえば、メタデータ予約済み領域の設定が現在 4 TB で、これを 6 TB に増やしたい場合、使用可能な値は 2 TB 以上である必要があります。

   f. すべてのストレージ ノードに対してこれらの手順を繰り返します。

      - 1 つ以上のストレージ ノードに十分な空き領域がない場合は、メタデータ予約済み領域の値を増やすことはできません。以降の手順には進まないでください。
      - 各ストレージ ノードのボリューム 0 に十分な使用可能領域がある場合は、次の手順に進みます。

3. 各ストレージ ノードに少なくとも 128 GB の RAM があることを確認してください。

   a. [* nodes （ノード）] を選択します

   b. グリッド内の最初のストレージ ノードを選択します。

   c. [* ハードウェア *] タブを選択します。

   d. メモリ使用量グラフの上にカーソルを置きます。*合計メモリ*が少なくとも 128 GB であることを確認してください。

   e. すべてのストレージ ノードに対してこれらの手順を繰り返します。

      - 1 つ以上のストレージ ノードに使用可能な合計メモリが十分でない場合は、メタデータ予約済みスペースの値を増やすことはできません。以降の手順には進まないでください。
      - 各ストレージ ノードの合計メモリが 128 GB 以上の場合は、次の手順に進みます。

4. メタデータ予約領域の設定を更新します。

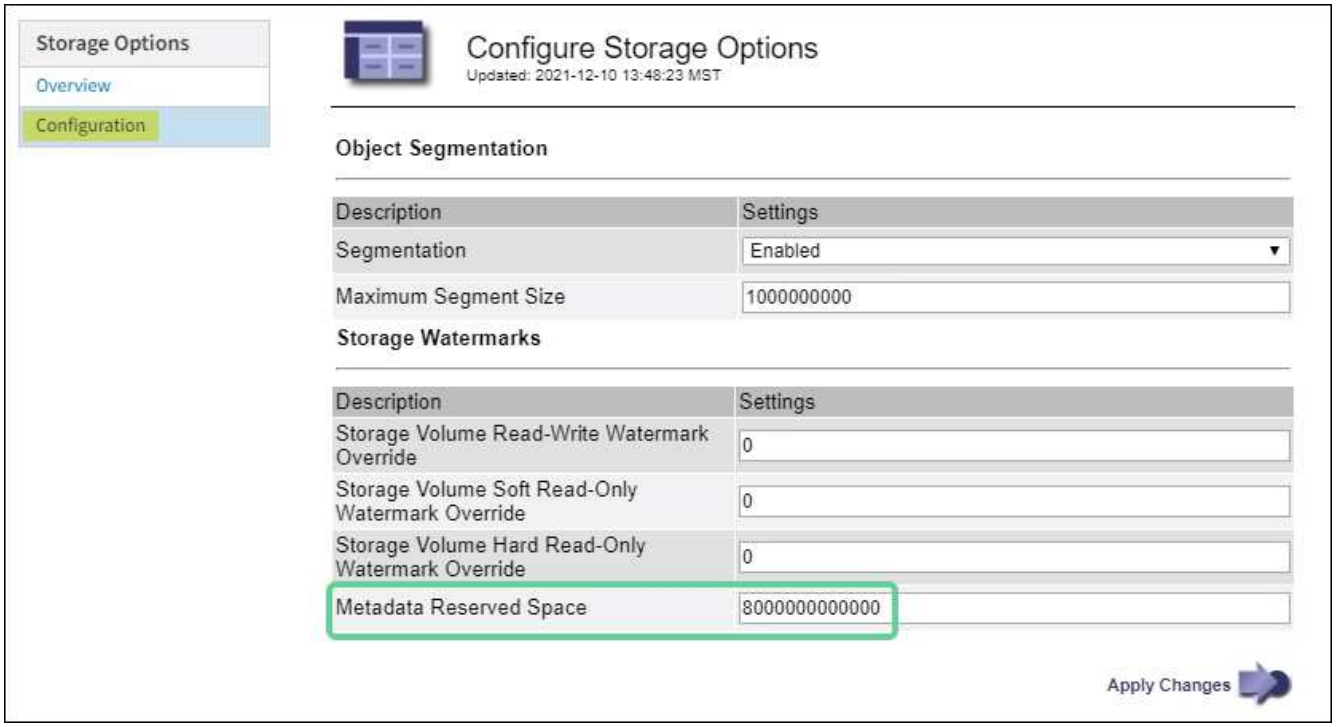
   a. * 設定 * > * システム * > * ストレージ・オプション * を選択します。

   b. [構成]タブを選択します。

   c. ストレージ ウォーターマーク セクションで、メタデータ予約済み領域 を選択します。

   d. 新しい値を入力します。

      たとえば、サポートされている最大値である 8 TB を入力するには、**8000000000000** (8 の後に 12 個のゼロが続く) と入力します。



a. 「 * 変更を適用する * 」を選択します。

格納オブジェクトを圧縮します

オブジェクトの圧縮を有効にすると、StorageGRID に格納されているオブジェクトのサイズを縮小して、オブジェクトによるストレージ消費量を削減できます。

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"。
- 特定のアクセス権限が必要です。

このタスクについて

デフォルトでは、オブジェクトの圧縮は無効になっています。圧縮を有効にすると、StorageGRID はロスレス圧縮を使用して各オブジェクトを保存時に圧縮しようとします。

> この設定を変更すると、新しい設定が適用されるまで約 1 分かかります。設定した値は、パフォーマンスと拡張用にキャッシュされます。

オブジェクトの圧縮を有効にする前に、次の点に注意してください。

- 格納されているデータが圧縮可能であることがわかっている場合を除き、*[Compress stored objects]*を選択しないでください。
- StorageGRID にオブジェクトを保存するアプリケーションは、オブジェクトを圧縮してから保存することがあります。クライアントアプリケーションがすでにオブジェクトを圧縮してからStorageGRID に保存している場合は、このオプションを選択してもオブジェクトのサイズがさらに縮小されることはありません。
- StorageGRID でNetApp FabricPool を使用している場合は、[Compress Stored Objects]*を選択しないでください。

- [Compress stored objects]*を選択した場合は、S3およびSwiftクライアントアプリケーションで、返されるバイト数の範囲を指定するGET Object処理を実行しないようにする必要があります。StorageGRID は要求されたバイトにアクセスするためにオブジェクトを圧縮解除する必要があるため ' これらの “range read” 操作は非効率的です非常に大きなオブジェクトから小さい範囲のバイト数を要求する GET Object 処理は特に効率が悪く、たとえば、 50GB の圧縮オブジェクトから 10MB の範囲を読み取る処理は非効率的です。

  圧縮オブジェクトから範囲を読み取ると、クライアント要求がタイムアウトする可能性があります。

  オブジェクトを圧縮する必要があり、クライアントアプリケーションが範囲読み取りを使用する必要がある場合は、アプリケーションの読み取りタイムアウトを増やしてください。

手順

1. * configuration > System > Object compression *を選択します。
2. [Compress stored objects]*チェックボックスを選択します。
3. [保存（ Save ）] を選択します。

ストレージノード設定

各ストレージノードでは、複数の設定とカウンタを使用します。アラーム（従来のシステム）をクリアするには、現在の設定の表示またはカウンタのリセットが必要になる場合があります。

ドキュメントで特に指示された場合を除き、ストレージノード設定を変更する前にテクニカルサポートにお問い合わせください。必要に応じて、イベントカウンタをリセットしてレガシーアラームをクリアできます。

ストレージノードの設定とカウンタにアクセスするには、次の手順を実行します。

手順

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** 」を選択します。
3. ストレージノードを展開し、サービスまたはコンポーネントを選択します。
4. [* 構成 *] タブを選択します。

次の表に、ストレージノードの構成設定をまとめます。

LDR

属性名（**Attribute Name**）	コード	説明
HTTP State のことです	HSTE	S3、Swift、およびその他の内部StorageGRID トラフィックのHTTPの現在の状態。 • Offline ：処理は許可されず、クライアントアプリケーションが LDR サービスへの HTTP セッションを開こうとするとエラーメッセージが表示されます。アクティブなセッションは正常終了します。 • Online ：処理は正常に続行されます
HTTP を自動起動します	HTAS	• このオプションを選択すると、再起動時のシステムの状態は * LDR * > * Storage * コンポーネントの状態によって異なります。再起動時に * ldr*>* Storage* コンポーネントが読み取り専用の場合、HTTP インターフェイスも読み取り専用です。LDR * > * Storage * コンポーネントが Online の場合、 HTTP も Online になります。それ以外の場合は、 HTTP インターフェイスは Offline 状態のままです。 • 選択しない場合、 HTTP インターフェイスは明示的に有効にするまで Offline のままです。

LDR> データストア

属性名（**Attribute Name**）	コード	説明
Lost Objects 数をリセットします	RCOR	このサービス上にある損失オブジェクト数のカウンタをリセットします。

LDR > Storage の順にクリックします

属性名（**Attribute Name**）	コード	説明
ストレージの状態 — 望ましい	SSD	ストレージコンポーネントに求める状態をユーザが設定できます。LDR サービスはこの値を読み取り、指定されたステータスに一致するように試みます。この値は、再起動後も維持されます。 たとえば、この設定を使用すると、使用可能なストレージスペースが十分にある場合でも、ストレージを強制的に読み取り専用にすることができます。これはトラブルシューティングに役立ちます。 この属性には次のいずれかの値を指定できます。 • Offline ：目的の状態が Offline の場合、 LDR サービスは * LDR * > * Storage * コンポーネントをオフラインにします。 • Read-only ： LDR サービスはストレージを読み取り専用にし、新しいコンテンツの受け入れを停止します。開いているセッションが閉じられるまでの短時間の間、コンテンツが引き続きストレージノードに保存される可能性があります。 • Online ：通常のシステム運用中は、値を Online のままにします。ストレージの状態 — ストレージコンポーネントの現在の状態は ' 使用可能なオブジェクトストレージ容量などの LDR サービスの状態に基づいてサービスによって動的に設定されますスペースが少ない場合、コンポーネントは読み取り専用になります。
ヘルスチェックタイムアウト	SHCT	ストレージボリュームが正常であるとみなされるために、ヘルスチェックテストが完了する必要のある秒数。この値は、サポートから指示があった場合にのみ変更してください。

LDR > Verification の順に選択します

属性名（**Attribute Name**）	コード	説明
欠落オブジェクト数のリセット	VCMI	OMIS （ Missing Objects Detected ）の数をリセットします。オブジェクトの存在チェックが完了した後にのみ使用します。欠落しているレプリケートオブジェクトデータは、 StorageGRID システムによって自動的にリストアされます。
検証レート	VPRI （ VPRI ）	バックグラウンド検証を実行する際のレートを設定します。バックグラウンド検証レートの設定に関する情報を参照してください。

属性名（**Attribute Name**）	コード	説明
破損オブジェクト数のリセット	VCCR	バックグラウンド検証中に見つかった、破損しているレプリケートされたオブジェクトデータのカウンタをリセットします。このオプションを使用すると、 OCOR （ Corrupt Objects Detected ）アラームの状態をクリアできます。
隔離オブジェクトを削除します	OQRT の場合	破損したオブジェクトを隔離ディレクトリから削除し、隔離されたオブジェクトの数をゼロにリセットして、 Quarantined Objects Detected （ OQRT ）アラームをクリアします。このオプションは、破損したオブジェクトが StorageGRID システムによって自動的にリストアされたあとに使用します。 Lost Objects アラームがトリガーされた場合、テクニカルサポートが隔離されたオブジェクトにアクセスを試みる可能性があります。隔離されたオブジェクトが、データのリカバリや、オブジェクトコピーの破損の原因となった根本的な問題のデバッグに役立つ場合があります。

LDR> イレイジャーコーディング

属性名（**Attribute Name**）	コード	説明
書き込みエラー数をリセットします	RSWF	イレイジャーコーディングオブジェクトデータのストレージノードへの書き込みエラーのカウンタをリセットします。
読み取りエラー数をリセットします	RSRF	イレイジャーコーディングオブジェクトデータのストレージノードからの読み取りエラーのカウンタをリセットします。
Reset Deletes Failure Count （エラーカウントをリセット）	自衛隊	イレイジャーコーディングオブジェクトデータのストレージノードからの削除エラーのカウンタをリセットします。
破損コピーのリセット検出数	RSCC	ストレージノード上にあるイレイジャーコーディングオブジェクトデータの破損コピー数のカウンタをリセットします。
破損フラグメントのリセット検出数	RSCD	ストレージノード上にあるイレイジャーコーディングオブジェクトデータの破損フラグメントのカウンタをリセットします。

属性名（**Attribute Name**）	コード	説明
欠落フラグメントの検出数をリセットします	RSMD	ストレージノード上にあるイレイジャーコーディングオブジェクトデータの欠落フラグメントのカウンタをリセットします。オブジェクトの存在チェックが完了した後にのみ使用します。

LDR > Replication の順に選択します

属性名（**Attribute Name**）	コード	説明
インバウンドレプリケーションエラー数をリセットします	RICR	インバウンドレプリケーションエラーのカウンタをリセットします。これを使用すると、 RIRF （ Inbound Replication - - Failed ）アラームをクリアできます。
アウトバウンドレプリケーションのエラー数をリセットします	ROCR	アウトバウンドレプリケーションエラーのカウンタをリセットします。これを使用すると、 RORF （ Outbound Replications - - Failed ）アラームをクリアできます。
インバウンドレプリケーションを無効にします	DSIR	メンテナンスまたは手順 のテストの一環としてインバウンドレプリケーションを無効にする場合に選択します。通常の運用中はオフのままにします。 インバウンドレプリケーションを無効にすると、オブジェクトをストレージノードから読み出してStorageGRID システム内の別の場所にコピーすることはできますが、他の場所からこのストレージノードにオブジェクトをコピーすることはできません。つまり、LDRサービスは読み取り専用です。
アウトバウンドレプリケーションを無効にします	DSOR	メンテナンスまたは手順 のテストの一環としてアウトバウンドレプリケーション（ HTTP 読み出し用のコンテンツ要求を含む）を無効にする場合に選択します。通常の運用中はオフのままにします。 アウトバウンドレプリケーションを無効にすると、このストレージノードにオブジェクトをコピーすることはできますが、ストレージノードからオブジェクトを読み出してStorageGRID システム内の別の場所にコピーすることはできません。LDR サービスは書き込み専用です。

ストレージノードがいっぱいになったときの管理

ストレージノードの容量が上限に達した場合は、新しいストレージを追加して StorageGRID システムを拡張する必要があります。ストレージボリュームの追加、ストレージ拡張シェルフの追加、ストレージノードの追加の 3 つのオプションがあります。

ストレージボリュームを追加します

各ストレージノードは最大数のストレージボリュームをサポートします。定義されている最大値はプラットフォームによって異なります。ストレージノードのストレージボリュームが最大数より少ない場合は、ボリュームを追加して容量を増やすことができます。の手順を参照してください "StorageGRID システムの拡張"。

ストレージ拡張シェルフを追加する

SG6060 などの一部の StorageGRID アプライアンスストレージノードで、追加のストレージシェルフがサポートされます。拡張機能が最大容量まで拡張されていない StorageGRID アプライアンスがある場合は、ストレージシェルフを追加して容量を増やすことができます。の手順を参照してください "StorageGRID システムの拡張"。

ストレージノードを追加します

ストレージノードを追加してストレージ容量を増やすことができます。ストレージを追加する場合は、現在アクティブな ILM ルールと容量の要件について慎重に検討する必要があります。の手順を参照してください "StorageGRID システムの拡張"。

管理ノードを管理する

管理ノードとは

管理ノードは、システムの設定、監視、ロギングなどの管理サービスを提供します。各グリッドにはプライマリ管理ノードが 1 つ必要で、冗長性を確保するために任意の数の非プライマリ管理ノードを設定できます。

Grid Manager または Tenant Manager にサインインすると、管理ノードに接続されます。どの管理ノードにも接続が可能で、各管理ノードに表示される StorageGRID システムのビューもほぼ同じです。ただし、メンテナンス手順はプライマリ管理ノードを使用して実行する必要があります。

管理ノードを使用して、 S3 および Swift クライアントトラフィックの負荷を分散することもできます。

優先送信者とは何ですか

StorageGRID 環境に複数の管理ノードが含まれている場合は、プライマリ管理ノードがアラート通知、AutoSupport メッセージ、SNMPトラップとインフォーム、および従来のアラーム通知の優先送信者となります。

通常のシステム運用では、優先送信者のみが通知を送信します。ただし、他のすべての管理ノードで優先送信者を監視します。問題が検出された場合、他の管理ノードは_standby senders_として動作します。

次の場合、複数の通知が送信されることがあります。

- 管理ノードどうしが「孤立」すると、優先送信者とスタンバイ送信者の両方が通知の送信を試み、通知のコピーが複数受信される可能性があります。
- スタンバイ送信者が優先送信者に関する問題を検出して通知の送信を開始すると、優先送信者は通知を再び送信できるようになることがあります。この場合、重複する通知が送信される可能性があります。優先送信者に関するエラーが検出されなくなると、スタンバイ送信者は通知の送信を停止します。

AutoSupport メッセージのテスト時には、すべての管理ノードからテストEメールが送信されます。アラート通知をテストするときは、すべての管理ノードにサインインして接続を確認する必要があります。

管理ノードのプライマリサービス

次の表に、管理ノードのプライマリサービスを示します。ただし、この表にはすべてのノードサービスが表示されるわけではありません。

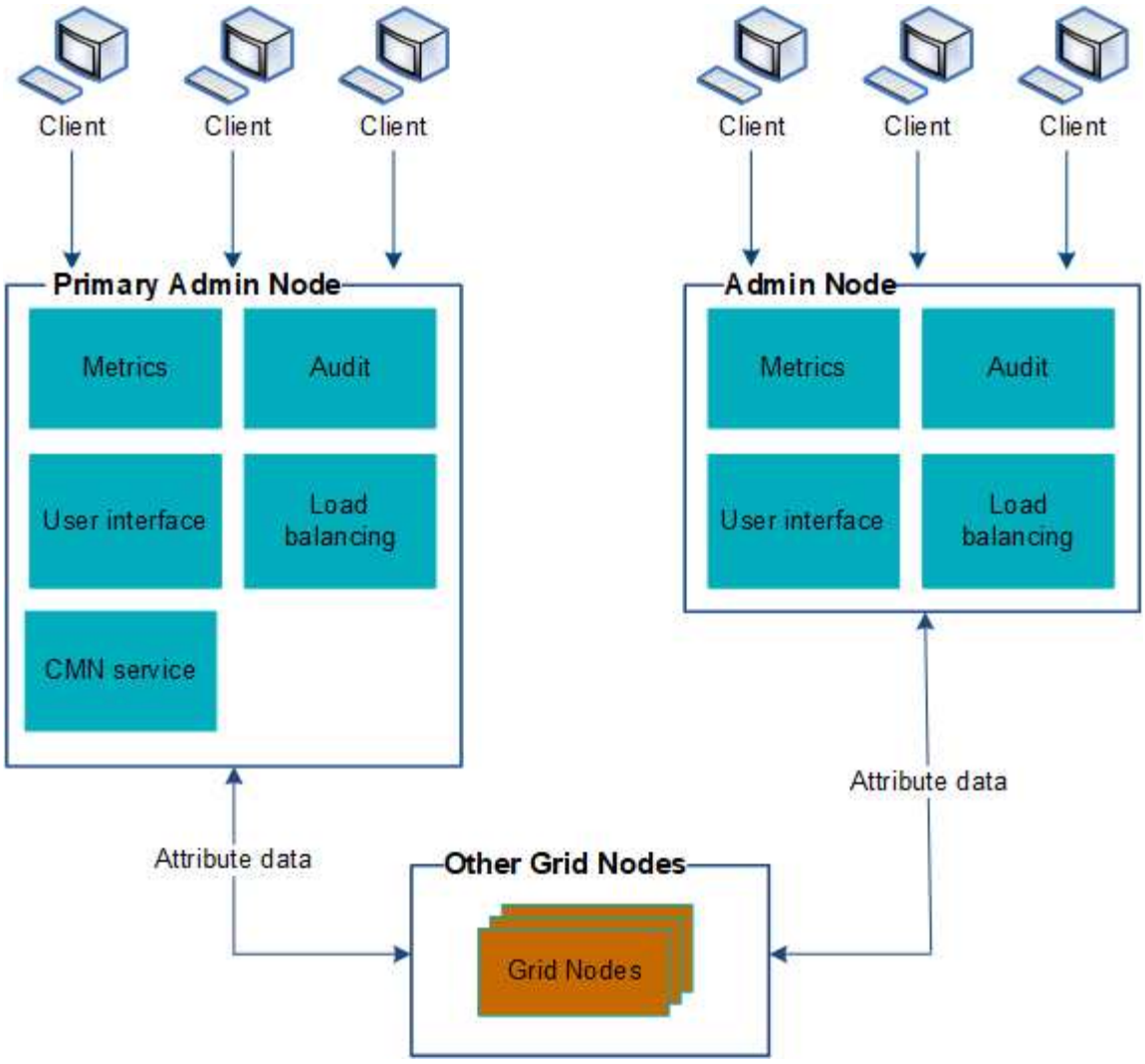
サービス	キー機能
Audit Management System （ AMS ）	システムアクティビティとイベントを追跡します。
Configuration Management Node （ CMN ）	システム全体の設定を管理します。プライマリ管理ノードのみ
管理アプリケーションプログラミングインターフェイス（ mgmt-api ）	グリッド管理 API とテナント管理 API からの要求を処理します。
高可用性	管理ノードとゲートウェイノードのグループのハイアベイラビリティ仮想 IP アドレスを管理します。 • 注： * このサービスはゲートウェイノードにも搭載されています。
ロードバランサ	クライアントからストレージノードへの S3 および Swift トラフィックのロードバランシングを実現します。 • 注： * このサービスはゲートウェイノードにも搭載されています。
ネットワーク管理システム（ NMS ）	Grid Manager の機能を提供します。
Prometheus	すべてのノードのサービスから時系列の指標を収集して格納します。
SSM （サーバステータスモニタ）	オペレーティングシステムと基盤のハードウェアを監視します。

複数の管理ノードを使用する

StorageGRID システムには複数の管理ノードを含めることができます。これにより、 1 つの管理ノードに障害が発生した場合でも、 StorageGRID システムを継続的に監視して設定することができます。

ある管理ノードが使用できなくなっても属性の処理は続行され、アラートとアラーム（従来のシステム）は引き続きトリガーされ、 E メール通知と AutoSupport メッセージは引き続き送信されます。ただし、通知と AutoSupport メッセージ以外のフェイルオーバー保護は提供されません。特に、ある管理ノードからのアラー

ムの確認応答は他の管理ノードにはコピーされません。



管理ノードに障害が発生した場合、次の 2 つの方法で StorageGRID システムを引き続き表示および設定することができます。

- Web クライアントは使用可能な他の管理ノードに再接続できます。
- システム管理者が管理ノードのハイアベイラビリティグループを設定している場合、 Web クライアントは HA グループの仮想 IP アドレスを使用して引き続き Grid Manager または Tenant Manager にアクセスできます。を参照してください "ハイアベイラビリティグループを管理します"。

> HAグループを使用している場合、アクティブな管理ノードで障害が発生するとアクセスが中断されます。ユーザは、 HA グループの仮想 IP アドレスがグループ内の別の管理ノードにフェイルオーバーしたあとで、再度サインインする必要があります。

一部のメンテナンスタスクはプライマリ管理ノードでしか実行できません。プライマリ管理ノードに障害が発生した場合、そのノードをリカバリするまでは、 StorageGRID システムは完全に機能している状態ではありません。

プライマリ管理ノードを特定します

プライマリ管理ノードは CMN サービスをホストします。一部のメンテナンス手順は、プライマリ管理ノードでしか実行できません。

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"。
- 特定のアクセス権限が必要です。

手順

1. サポート * > * ツール * > * グリッドトポロジ * を選択します。
2. 「 * _site * > * Admin Node * 」を選択し、を選択します ➕ をクリックしてトポロジツリーを展開し、この管理ノードでホストされているサービスを表示します。

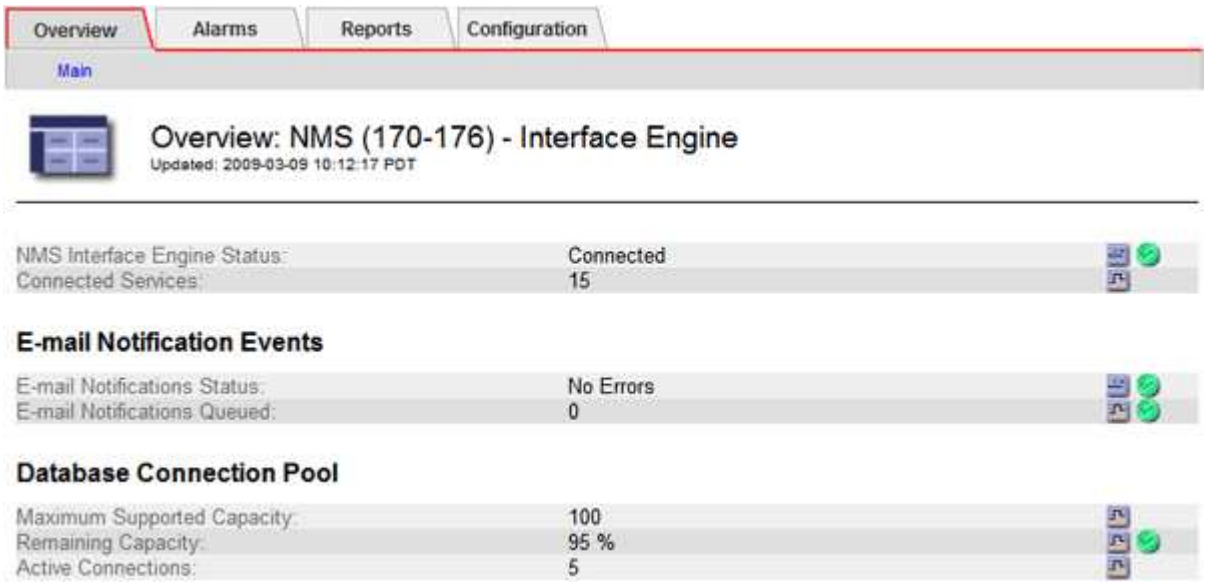
   プライマリ管理ノードは CMN サービスをホストします。

3. この管理ノードが CMN サービスをホストしていない場合、他の管理ノードを確認します。

通知のステータスとキューを表示します

管理ノードの Network Management System （ NMS ）サービスは、メールサーバに通知を送信します。NMS サービスの現在のステータスとその通知キューのサイズは、Interface Engine ページで確認できます。

Interface Engine ページにアクセスするには、 * support * > * Tools * > * Grid topology * を選択します。最後に、 * *site* _ * > * *_Admin Node** > * NMS * > * Interface Engine * を選択します。



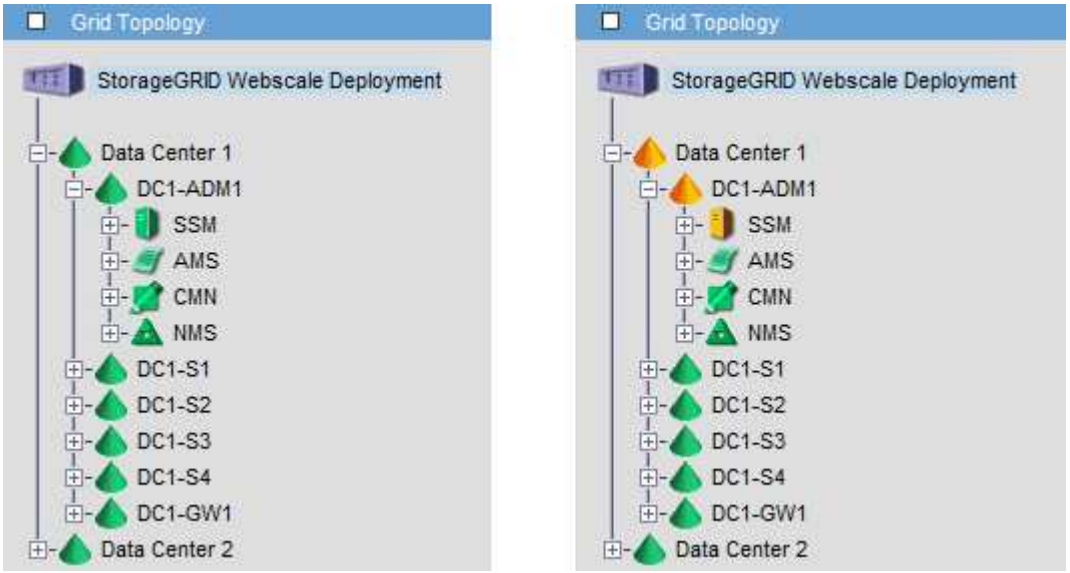
通知は E メール通知キューを通じて処理され、トリガーされた順にメールサーバに送信されます。通知の送信時に問題（ネットワーク接続エラーなど）が発生してメールサーバが使用できなくなった場合は、メールサーバへの再送信が 60 秒間試行されます。60 秒経ってもメールサーバに送信されなかった通知は通知キューから破棄され、キュー内の次の通知の送信が試行されます。

通知が送信されずに通知キューから破棄されることがあるため、通知が送信されずにアラームがトリガーされる可能性があります。通知が送信されずにキューからドロップされると、MINS（E-mail Notification Status ）Minorアラームがトリガーされます。

管理ノードによる確認済みアラームの表示（従来のシステム）

ある管理ノードのアラームを確認しても、確認済みのアラームは他の管理ノードにはコピーされません。確認応答は他の管理ノードにはコピーされないため、[Grid Topology] ツリーの表示が各管理ノードで同じにならないことがあります。

この違いは、 Web クライアントに接続する場合に役立ちます。Web クライアントでは、管理者のニーズに基づいて、 StorageGRID システムをさまざまな方法で表示できます。



通知は、確認応答が発生した管理ノードから送信されます。

監査クライアントアクセスを設定します

NFSの監査クライアントアクセスを設定します

管理ノードは、 Audit Management System （ AMS ）サービスを介して、監査対象のすべてのシステムイベントを、監査共有からアクセス可能なログファイルに記録します。監査共有はインストール時に各管理ノードに追加されます。監査共有は読み取り専用の共有として自動的に有効になります。

監査ログにアクセスするには、NFSの監査共有へのクライアントアクセスを設定します。または、できます "外部syslogサーバを使用します"。

StorageGRID システムは、確認応答を使用して、ログファイルに書き込まれる前に監査メッセージが失われないようにします。AMS サービスまたは中間の監査リレーサービスがメッセージの制御を確認するまで、メッセージはサービスのキューに残ります。詳細については、を参照してください "監査ログを確認します"。

作業を開始する前に

- を使用することができます `Passwords.txt` root / adminパスワードが設定されたファイル。

- を使用することができます `Configuration.txt` ファイル（リカバリパッケージに含まれています）。
- 監査クライアントが NFS バージョン 3 （ NFSv3 ）を使用している。

このタスクについて

この手順 は、監査メッセージの取得先である StorageGRID 環境内の管理ノードごとに実行します。

手順

1. プライマリ管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@primary_Admin_Node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

      rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

2. すべてのサービスの状態が「 Running 」または「 Verified 」であることを確認します。入力するコマンド `storagegrid-status`

   「Running」または「Verified」と表示されないサービスがある場合は、問題を解決してから続行してください。

3. コマンドラインに戻ります。Ctrl キーを押しながら * C キーを押します。
4. NFS 設定ユーティリティを起動します。入力するコマンド `config_nfs.rb`

```
------------------------------------------------------------------
| Shares                | Clients               | Config          |
------------------------------------------------------------------
| add-audit-share       | add-ip-to-share       | validate-config |
| enable-disable-share  | remove-ip-from-share  | refresh-config  |
|                       |                       | help            |
|                       |                       | exit            |
------------------------------------------------------------------
```

5. 監査クライアントを追加します。 `add-audit-share`
   a. プロンプトが表示されたら、監査共有用の監査クライアントのIPアドレスまたはIPアドレス範囲を入力します。 `client_IP_address`
   b. プロンプトが表示されたら、 * Enter * を押します。
6. 複数の監査クライアントに監査共有へのアクセスを許可する場合は、ユーザのIPアドレスを追加します。 `add-ip-to-share`
   a. 監査共有の番号を入力します。 *`audit_share_number`*
   b. プロンプトが表示されたら、監査共有用の監査クライアントのIPアドレスまたはIPアドレス範囲を入力します。 *`client_IP_address`*

c. プロンプトが表示されたら、 * Enter * を押します。

NFS 設定ユーティリティが表示されます。

d. 監査共有に追加する監査クライアントごとに、上記の手順を繰り返します。

7. 必要に応じて、設定を確認します。

a. 次のように入力します。 `validate-config`

サービスがチェックされて表示されます。

b. プロンプトが表示されたら、 * Enter * を押します。

NFS 設定ユーティリティが表示されます。

c. NFS設定ユーティリティを閉じます。 `exit`

8. 他のサイトで監査共有を有効にする必要があるかどうかを確認します。

◦ StorageGRID 環境が単一サイトの場合は、次の手順に進みます。

◦ StorageGRID 環境で他のサイトに管理ノードが含まれている場合は、必要に応じてこれらの監査共有を有効にします。

i. サイトの管理ノードにリモートからログインします。

A. 次のコマンドを入力します。 `ssh admin@grid_node_IP`

B. に記載されているパスワードを入力します `Passwords.txt` ファイル。

C. 次のコマンドを入力してrootに切り替えます。 `su -`

D. に記載されているパスワードを入力します `Passwords.txt` ファイル。

ii. 同じ手順を繰り返して、追加の管理ノードごとに監査共有を設定します。

iii. リモート管理ノードへのリモートの Secure Shell ログインを終了します。入力するコマンド `exit`

9. コマンドシェルからログアウトします。 `exit`

NFS 監査クライアントは、 IP アドレスに基づいて監査共有へのアクセスが許可されます。新しい NFS 監査クライアントに共有に IP アドレスを追加して監査共有へのアクセスを許可するか、または IP アドレスを削除して既存の監査クライアントを削除します。

監査共有に **NFS** 監査クライアントを追加します

NFS 監査クライアントは、 IP アドレスに基づいて監査共有へのアクセスが許可されます。新しい NFS 監査クライアントに監査共有へのアクセスを許可するには、そのクライアントの IP アドレスを監査共有に追加します。

作業を開始する前に

- を使用することができます `Passwords.txt` root / adminアカウントのパスワードが設定されたファイル。
- を使用することができます `Configuration.txt` ファイル（リカバリパッケージに含まれています）。

- 監査クライアントが NFS バージョン 3 （ NFSv3 ）を使用している。

手順

1. プライマリ管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@primary_Admin_Node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

      rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

2. NFS設定ユーティリティを起動します。 `config_nfs.rb`

```
----------------------------------------------------------------------
| Shares                | Clients               | Config           |
----------------------------------------------------------------------
| add-audit-share       | add-ip-to-share       | validate-config  |
| enable-disable-share  | remove-ip-from-share  | refresh-config   |
|                       |                       | help             |
|                       |                       | exit             |
----------------------------------------------------------------------
```

3. 入力するコマンド `add-ip-to-share`

   管理ノードで有効になっている NFS 監査共有のリストが表示されます。監査共有はのように表示されます。 `/var/local/audit/export`

4. 監査共有の番号を入力します。 *`audit_share_number`*
5. プロンプトが表示されたら、監査共有用の監査クライアントのIPアドレスまたはIPアドレス範囲を入力します。 *`client_IP_address`*

   監査クライアントが監査共有に追加されます。

6. プロンプトが表示されたら、 * Enter * を押します。

   NFS 設定ユーティリティが表示されます。

7. 監査共有に追加する監査クライアントごとに、この手順を繰り返します。
8. 必要に応じて、設定を確認します。 `validate-config`

   サービスがチェックされて表示されます。

   a. プロンプトが表示されたら、 * Enter * を押します。

      NFS 設定ユーティリティが表示されます。

9. NFS設定ユーティリティを閉じます。 `exit`
10. StorageGRID 環境が単一サイトの場合は、次の手順に進みます。

    StorageGRID 環境で他のサイトに管理ノードが含まれている場合は、必要に応じてこれらの監査共有を有効にします。

    a. サイトの管理ノードにリモートからログインします。

        i. 次のコマンドを入力します。 `ssh admin@grid_node_IP`

        ii. に記載されているパスワードを入力します `Passwords.txt` ファイル。

        iii. 次のコマンドを入力してrootに切り替えます。 `su -`

        iv. に記載されているパスワードを入力します `Passwords.txt` ファイル。

    b. 同じ手順を繰り返して、管理ノードごとに監査共有を設定します。

    c. リモート管理ノードへのリモートのSecure Shellログインを終了します。 `exit`

11. コマンドシェルからログアウトします。 `exit`

NFS 監査の統合を確認

監査共有を設定して NFS 監査クライアントを追加したら、監査クライアント共有をマウントし、監査共有のファイルにアクセスできることを確認します。

手順

1. AMS サービスをホストしている管理ノードのクライアント側 IP アドレスを使用して、接続（またはクライアントシステムでの操作）を検証します。入力するコマンド `ping IP_address`

    サーバが応答して接続を示していることを確認します。

2. クライアントのオペレーティングシステムに適したコマンドを使用して、読み取り専用の監査共有をマウントします。Linux コマンドの例は次のとおりです（ 1 行で入力します）。

    ```
    mount -t nfs -o hard,intr Admin_Node_IP_address:/var/local/audit/export
    myAudit
    ```

    AMS サービスをホストしている管理ノードの IP アドレスと、監査システムの事前定義された共有名を使用します。マウントポイントには、クライアントが選択した任意の名前を使用できます（例： *myAudit* 前のコマンドを参照）。

3. 監査共有のファイルにアクセスできることを確認します。入力するコマンド `ls myAudit /*`

    ここで、 *myAudit* は、監査共有のマウントポイントです。少なくとも 1 つのログファイルが表示されている必要があります。

監査共有から **NFS** 監査クライアントを削除します

NFS 監査クライアントは、 IP アドレスに基づいて監査共有へのアクセスが許可されます。既存の監査クライアントを削除するには、その IP アドレスを削除します。

作業を開始する前に

- を使用することができます `Passwords.txt` root / adminアカウントのパスワードが設定されたファイル。
- を使用することができます `Configuration.txt` ファイル（リカバリパッケージに含まれています）。

このタスクについて

監査共有へのアクセスを許可した最後のIPアドレスは削除できません。

手順

1. プライマリ管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@primary_Admin_Node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

      rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。

2. NFS設定ユーティリティを起動します。 `config_nfs.rb`

```
----------------------------------------------------------------------
| Shares                | Clients              | Config           |
----------------------------------------------------------------------
| add-audit-share       | add-ip-to-share      | validate-config  |
| enable-disable-share  | remove-ip-from-share | refresh-config   |
|                       |                      | help             |
|                       |                      | exit             |
----------------------------------------------------------------------
```

3. 監査共有からIPアドレスを削除します。 `remove-ip-from-share`

   サーバで設定されている監査共有に番号が振られ、リストに表示されます。監査共有はのように表示されます。 `/var/local/audit/export`

4. 監査共有に対応する番号を入力します。 *`audit_share_number`*

   監査共有へのアクセスを許可している IP アドレスに番号が振られ、リストに表示されます。

5. 削除する IP アドレスに対応する番号を入力します。

   監査共有が更新され、この IP アドレスの監査クライアントからのアクセスは許可されなくなります。

6. プロンプトが表示されたら、 * Enter * を押します。

   NFS 設定ユーティリティが表示されます。

7. NFS設定ユーティリティを閉じます。 `exit`

8. StorageGRID 環境が複数データセンターサイトの環境であり、他のサイトにも管理ノードが含まれている場合は、必要に応じてこれらの監査共有を無効にします。
   a. 各サイトの管理ノードにリモートからログインします。
      i. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
      ii. に記載されているパスワードを入力します `Passwords.txt` ファイル。
      iii. 次のコマンドを入力してrootに切り替えます。 `su -`
      iv. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   b. 同じ手順を繰り返して、追加の管理ノードごとに監査共有を設定します。
   c. リモート管理ノードへのリモートのSecure Shellログインを終了します。 `exit`
9. コマンドシェルからログアウトします。 `exit`

NFS 監査クライアントの **IP** アドレスを変更します

NFS 監査クライアントの IP アドレスを変更する必要がある場合は、次の手順を実行します。

手順

1. 既存の NFS 監査共有に新しい IP アドレスを追加します。
2. 元の IP アドレスを削除します。

関連情報

- "監査共有に NFS 監査クライアントを追加します"
- "監査共有から NFS 監査クライアントを削除します"

アーカイブノードを管理します

アーカイブノードとは

必要に応じて、各 StorageGRID データセンターサイトにアーカイブノードを導入して、Tivoli Storage Manager （ TSM ）などの外部アーカイブストレージシステムに接続できます。

アーカイブノードのサポート（S3 APIを使用してクラウドにアーカイブする場合とTSMミドルウェアを使用してテープにアーカイブする場合の両方）は廃止され、今後のリリースで削除される予定です。アーカイブノードから外部アーカイブストレージシステムへのオブジェクトの移動は、より多くの機能を提供するILMクラウドストレージプールに置き換えられました。

を参照してください

- "オブジェクトをクラウドストレージプールに移行します"
- "クラウドストレージプールを使用"

また、StorageGRID 11.7以前では、アクティブなILMポリシーからアーカイブノードを削除する必要があります。アーカイブノードに格納されているオブジェクトデータを削除すると、将来のアップグレードが簡単になります。を参照してください "ILMルールおよびILMポリシーの操作"。

アーカイブノードは、オブジェクトデータの長期保管用に外部アーカイブストレージシステムをターゲットとするインターフェイスを提供します。また、この接続、および StorageGRID システムとターゲットの外部アーカイブストレージシステム間でのオブジェクトデータ転送も監視します。

外部ターゲットへの接続を設定したあと、 TSM のパフォーマンスを最適化するようにアーカイブノードを設定できます。 TSM サーバの容量が上限に近づいている場合や TSM サーバを使用できない場合は、アーカイブノードをオフラインにできます。また、レプリケーションと読み出しを設定できます。アーカイブノードにカスタムアラームを設定することもできます。

削除はできないが定期的にアクセスされないオブジェクトデータは、ストレージノードの回転式ディスクからクラウドやテープなどの外部アーカイブストレージにいつでも移動できます。オブジェクトデータをこのようにアーカイブするには、データセンターサイトのアーカイブノードを設定し、次にこのアーカイブノードをコンテンツ配置手順の「ターゲット」として選択した ILM ルールを設定します。アーカイブノードは、アーカイブされたオブジェクトデータ自体の管理は行いません。これは外部アーカイブデバイスによって行われます。

オブジェクトメタデータはアーカイブされず、ストレージノードに残ります。

ARC サービスとは

アーカイブノード上の Archive （ ARC ）サービスは、 TSM ミドルウェア経由のテープなど、外部アーカイブストレージへの接続を設定できる管理インターフェイスです。

ARC サービスは、外部のアーカイブストレージシステムと連携することにより、ニアラインストレージ用にオブジェクトデータを送信し、クライアントアプリケーションがアーカイブされたオブジェクトを要求したときに読み出しを実行します。クライアントアプリケーションがアーカイブされたオブジェクトを要求すると、ストレージノードは ARC サービスからオブジェクトデータを要求します。ARC サービスは外部のアーカイブストレージシステムに要求を送信し、アーカイブストレージシステムは要求されたオブジェクトデータを読み出して ARC サービスに送信します。ARC サービスはオブジェクトデータを検証してストレージノードに転送し、ストレージノードは要求元のクライアントアプリケーションにオブジェクトを返します。

TSM ミドルウェア経由でテープにアーカイブされたオブジェクトデータに対する要求は、読み出し効率が向上するように管理されます。要求は、テープに格納されているオブジェクトの順番と同じになるように順序が調整されたうえで、ストレージデバイスへの送信用のキューに登録されます。アーカイブデバイスによっては、異なるボリューム上のオブジェクトに対する複数の要求を同時に処理できます。

S3 API を使用してクラウドにアーカイブします

アーカイブノードは、 Amazon Web Services （ AWS ）に直接接続するように設定することも、 S3 API を使用して StorageGRID システムと連携可能な他のシステムに接続するように設定することもできます。

> アーカイブノードのサポート（S3 APIを使用してクラウドにアーカイブする場合とTSMミドルウェアを使用してテープにアーカイブする場合の両方）は廃止され、今後のリリースで削除される予定です。アーカイブノードから外部アーカイブストレージシステムへのオブジェクトの移動は、より多くの機能を提供するILMクラウドストレージプールに置き換えられました。
>
> を参照してください "クラウドストレージプールを使用"。

S3 API の接続設定を行います

S3 インターフェイスを使用してアーカイブノードに接続する場合は、 S3 API の接続を設定する必要があります。これらの設定が完了するまで ARC サービスは外部アーカイブストレージシステムと通信できないため、 Major アラーム状態のままです。

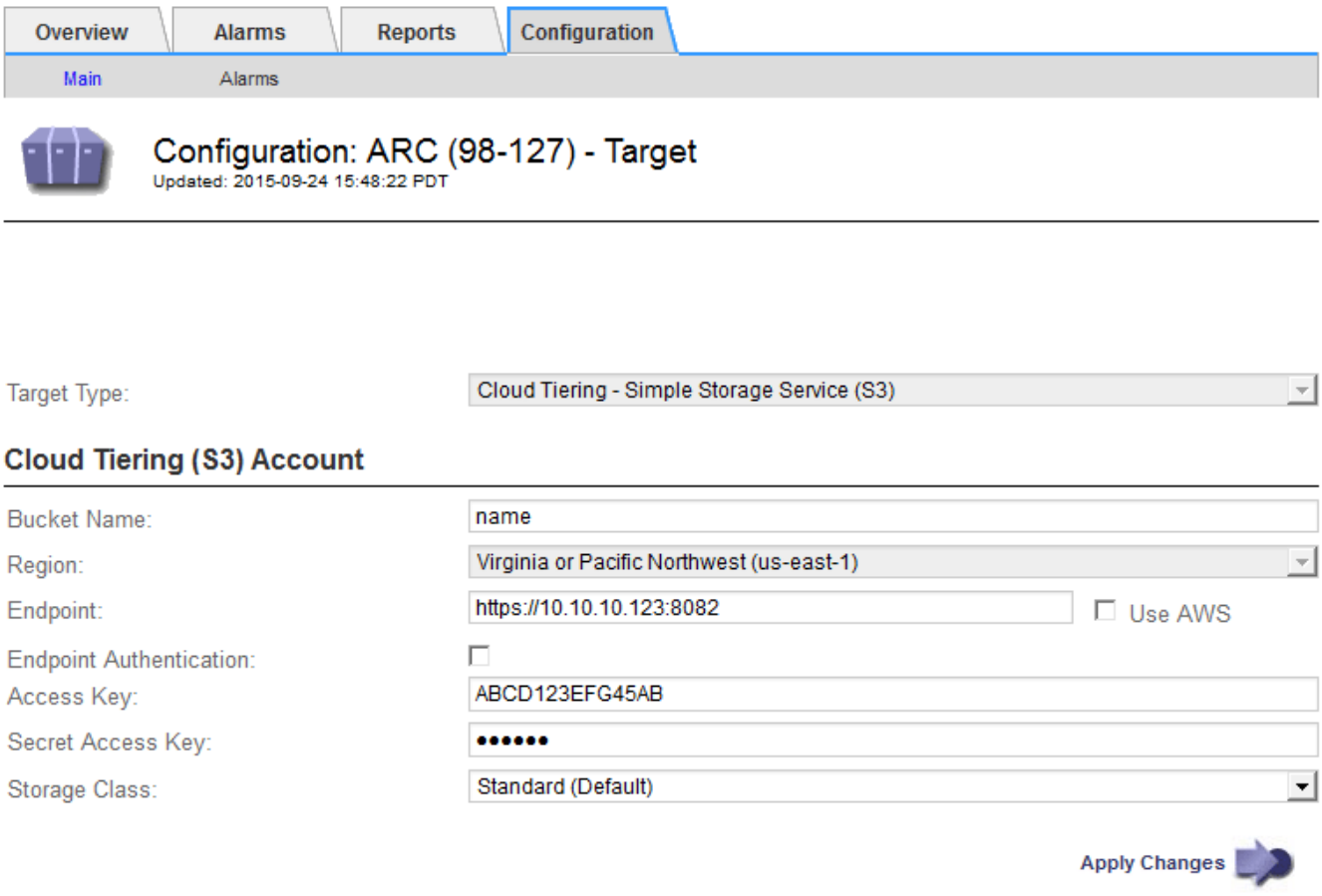
> アーカイブノードのサポート（S3 APIを使用してクラウドにアーカイブする場合とTSMミドルウェアを使用してテープにアーカイブする場合の両方）は廃止され、今後のリリースで削除される予定です。アーカイブノードから外部アーカイブストレージシステムへのオブジェクトの移動は、より多くの機能を提供するILMクラウドストレージプールに置き換えられました。
>
> を参照してください "クラウドストレージプールを使用"。

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"。
- 特定のアクセス権限が必要です。
- ターゲットのアーカイブストレージシステムにバケットを作成しておきます。
  - このバケットは 1 つのアーカイブノード専用です。他のアーカイブノードやアプリケーションでは使用できません。
  - バケットには、ユーザの場所に適したリージョンが選択されています。
  - バケットのバージョン管理は一時停止に設定する必要があります。
- オブジェクトのセグメント化が有効で、最大セグメントサイズは 4.5GiB （ 4 、 831 、 838 、 208 バイト）以下になります。S3 が外部アーカイブストレージシステムとして使用されている場合、この値を超える S3 API 要求は失敗します。

手順

1. サポート * > * ツール * > * グリッドトポロジ * を選択します。
2. アーカイブノード * > * ARC * > * Target * を選択します。
3. * Configuration * > * Main * を選択します。



4. ターゲットタイプドロップダウンリストから * Cloud Tiering - Simple Storage Service （ S3 ） * を選択します。

   ターゲットタイプを選択するまで、構成設定は使用できません。

5. アーカイブノードからターゲットの外部の S3 対応アーカイブストレージシステムへの接続に使用するクラウドの階層化（ S3 ）アカウントを設定します。

   このページのフィールドのほとんどはわかりやすいもので、説明を必要としません。以下は、説明が必要なフィールドです。

   - * Region * ： * Use AWS * が選択されている場合にのみ選択できます。バケットのリージョンと同じリージョンを選択する必要があります。
   - * Endpoint * および * Use AWS * ： Amazon Web Services （ AWS ）の場合は、「 * Use AWS * 」を選択します。* エンドポイント * には、バケット名属性とリージョン属性に基づいてエンドポイント URL が自動的に入力されます。例：

     ```
     https://bucket.region.amazonaws.com
     ```

     AWS 以外のターゲットの場合は、ポート番号を含め、バケットをホストしているシステムの URL を入力します。例：

```
https://system.com:1080
```

   - * エンドポイント認証 *: デフォルトで有効になっています。外部アーカイブストレージシステムへのネットワークが信頼されている場合は、チェックボックスをオフにして、エンドポイントのSSL証明

書と対象の外部アーカイブストレージシステムのホスト名検証を無効にできます。StorageGRID システムの別のインスタンスがターゲットのアーカイブストレージデバイスであり、システムに公開署名された証明書が設定されている場合は、このチェックボックスを選択したままにできます。

- * ストレージクラス * ：通常のストレージには「 * Standard （デフォルト） * 」を選択します。簡単に再作成できるオブジェクトに対してのみ、「冗長性の低下」を選択します。* 冗長性の低下 * 信頼性の低い低コストのストレージを提供します。ターゲットのアーカイブストレージシステムが StorageGRID システムの別のインスタンスの場合、ストレージクラス * はオブジェクトの取り込み時に実行されるオブジェクトの中間コピー数を、デュアルコミットがオブジェクトの取り込み時に使用される場合にターゲットシステムで制御します。

6. 「 * 変更を適用する * 」を選択します。

指定した設定が検証され、 StorageGRID システムに適用されます。設定後、ターゲットを変更することはできません。

S3 API の接続設定を変更します

S3 API を使用して外部のアーカイブストレージシステムに接続するようにアーカイブノードを設定したあとで接続が変更された場合、一部の設定を変更できます。

作業を開始する前に

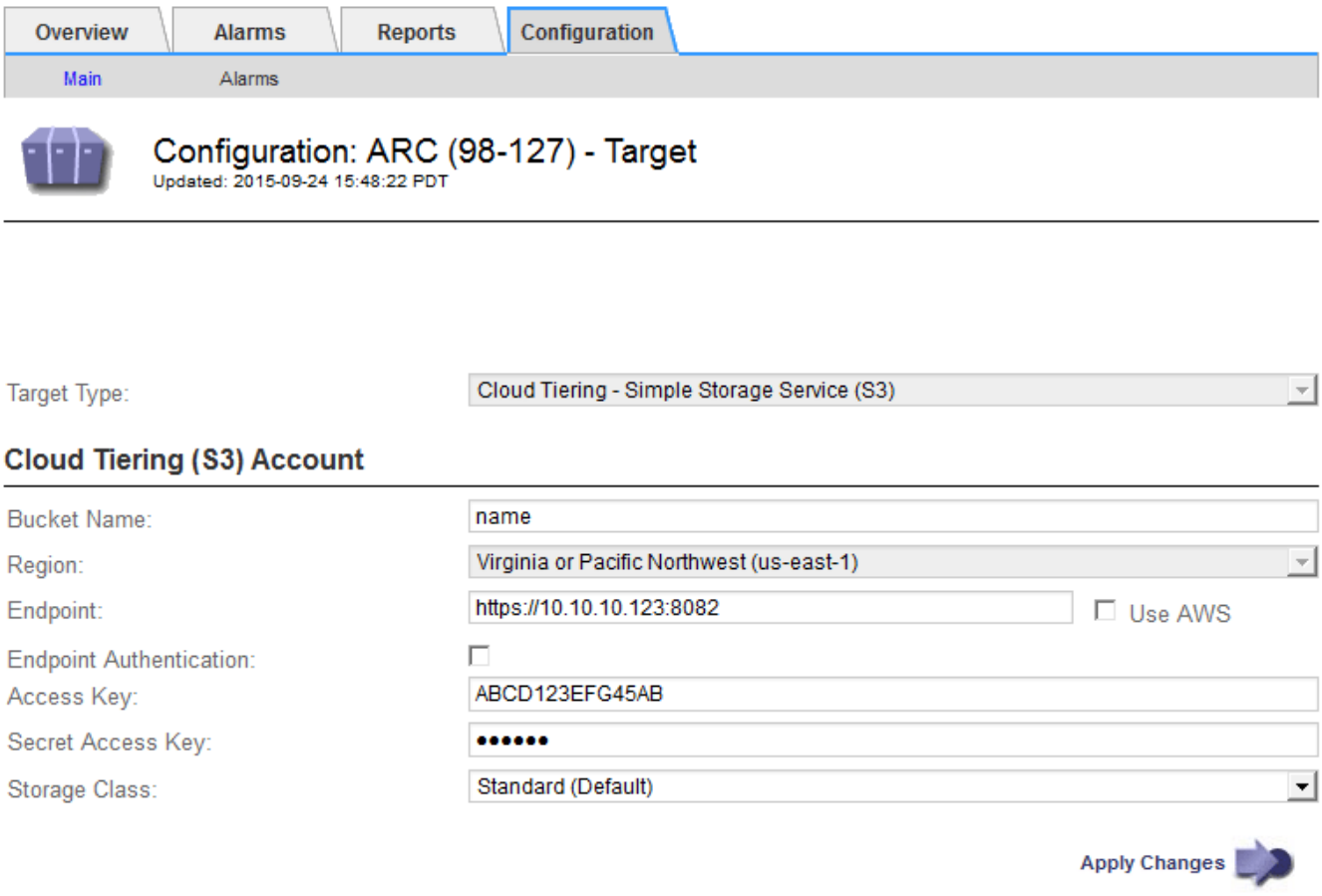
- を使用して Grid Manager にサインインします "サポートされている Web ブラウザ"。
- 特定のアクセス権限が必要です。

このタスクについて

クラウドの階層化（ S3 ）アカウントを変更した場合は、アーカイブノードによって以前にバケットに取り込まれたすべてのオブジェクトを含む、バケットへの読み取り / 書き込みアクセスがユーザアクセスクレデンシャルに割り当てられている必要があります。

手順

1. サポート * > * ツール * > * グリッドトポロジ * を選択します。
2. 「 * _ アーカイブノード _ * > * ARC * > * ターゲット * 」を選択します。
3. * Configuration * > * Main * を選択します。



4. 必要に応じて、アカウント情報を変更します。

   ストレージクラスを変更すると、新しいオブジェクトデータは新しいストレージクラスで格納されます。既存のオブジェクトは、引き続き取り込み時に設定したストレージクラスで格納されます。

   [Bucket Name]、[Region]、および[Endpoint]にはAWSの値が使用され、変更することはできません。

5. 「 * 変更を適用する * 」を選択します。

クラウドの階層化サービスの状態を変更します

クラウドの階層化サービスの状態を変更することで、 S3 API を使用して接続する外部のアーカイブストレージシステムに対してアーカイブノードが読み取り / 書き込みできるかどうかを制御できます。

作業を開始する前に

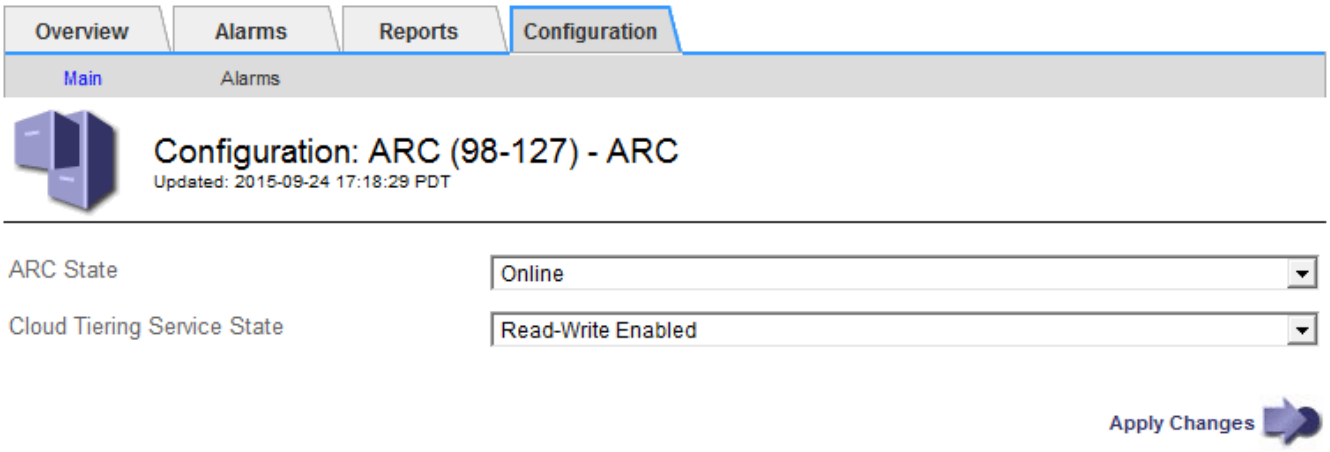
- を使用して Grid Manager にサインインする必要があります "サポートされている Web ブラウザ"。
- 特定のアクセス権限が必要です。
- アーカイブノードが設定されている必要があります。

このタスクについて

クラウドの階層化サービスの状態を「 * Read-Write Disabled 」に変更すると、アーカイブノードを効果的にオフラインにできます。

手順

1. サポート * > * ツール * > * グリッドトポロジ * を選択します。
2. 「 * _ アーカイブノード _ * > * ARC * 」を選択します。
3. * Configuration * > * Main * を選択します。



4. クラウドの階層化サービスの状態 * を選択します。
5. 「 * 変更を適用する * 」を選択します。

S3 API 接続のストア障害数をリセットします

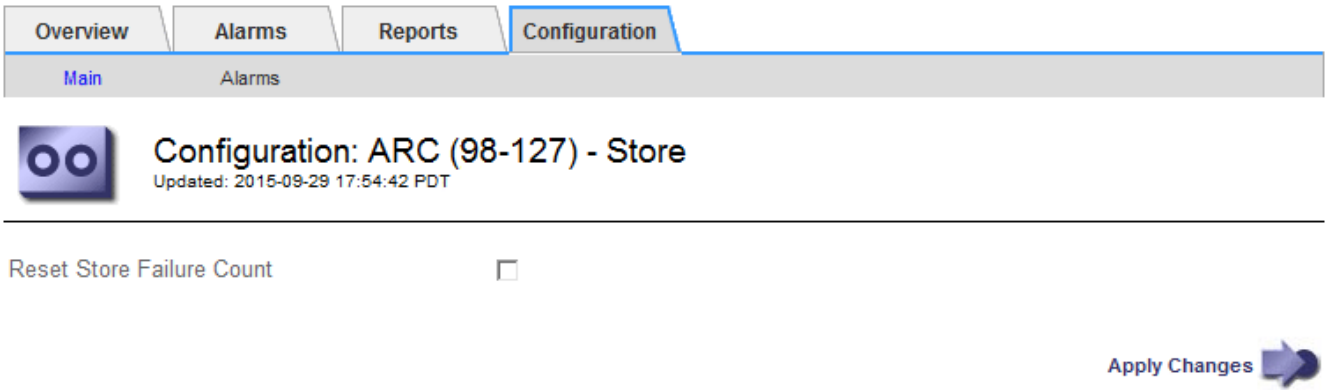
アーカイブノードが S3 API 経由でアーカイブストレージシステムに接続している場合は、ストア障害数をリセットでき、 ARVF （ Store Failures ）アラームをクリアできます。

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"。
- 特定のアクセス権限が必要です。

手順

1. サポート * > * ツール * > * グリッドトポロジ * を選択します。
2. 「 * _ アーカイブノード _ * > * ARC * > * Store * 」を選択します。
3. * Configuration * > * Main * を選択します。



4. 「 Reset Store Failure Count 」を選択します。
5. 「 * 変更を適用する * 」を選択します。

   Store Failures 属性がゼロにリセットされます。

「 **Cloud Tiering - S3** 」からクラウドストレージプールにオブジェクトを移行します

現在* Cloud Tiering - Simple Storage Service（S3）*機能を使用してオブジェクトデータをS3バケットに階層化している場合は、代わりにオブジェクトをクラウドストレージプールに移行する必要があります。クラウドストレージプールは拡張性に優れたアプローチを提供し、 StorageGRID システム内のすべてのストレージノードを活用します。

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"。
- 特定のアクセス権限が必要です。
- クラウド階層化用に設定された S3 バケットにオブジェクトが格納済みである。

> オブジェクトデータを移行する前に、ネットアップのアカウント担当者に問い合わせて関連するコストについて把握してください。

このタスクについて

ILM から見た場合、クラウドストレージプールはストレージプールに似ています。ただし、ストレージプールは StorageGRID システム内のストレージノードまたはアーカイブノードで構成されますが、クラウドストレージプールは外部の S3 バケットで構成されます。

オブジェクトを「 Cloud Tiering - S3 」からクラウドストレージプールに移行する前に、 S3 バケットを作成し、 StorageGRID にクラウドストレージプールを作成する必要があります。次に、新しい ILM ポリシーを作成し、クラウド階層化バケットにオブジェクトを格納するために使用していた ILM ルールをコピーし、同じオブジェクトをクラウドストレージプールに格納するように変更します。

> オブジェクトがクラウドストレージプールに格納されている場合、それらのオブジェクトのコピーをStorageGRID 内にも格納することはできません。現在クラウド階層化に使用している ILM ルールが複数の場所に同時にオブジェクトを格納するように設定されている場合は、その機能が失われるため、このオプションの移行を引き続き実行するかどうかを検討してください。移行を続行する場合は、既存のルールをコピーするのではなく、新しいルールを作成する必要があります。

手順

1. クラウドストレージプールを作成

   クラウドストレージプールに新しい S3 バケットを使用して、クラウドストレージプールで管理されるデータのみが含まれるようにします。

2. クラウド階層化バケットに格納する原因 オブジェクトをアクティブな ILM ポリシーで特定します。
3. 該当するルールをコピーします。
4. コピーしたルールで、配置場所を新しいクラウドストレージプールに変更します。

5. コピーしたルールを保存します。
6. 新しいルールを使用する新しいポリシーを作成します。
7. 新しいポリシーをシミュレートしてアクティブ化します。

   新しいポリシーがアクティブ化されて ILM 評価が実行されると、クラウド階層化用に設定された S3 バケットからクラウドストレージプール用に設定された S3 バケットにオブジェクトが移動します。グリッド上の使用可能なスペースに影響はありません。クラウドストレージプールに移動されたオブジェクトは、クラウド階層化バケットから削除されます。

関連情報

"ILM を使用してオブジェクトを管理する"

TSM ミドルウェア経由でのテープへのアーカイブ

Tivoli Storage Manager （ TSM ）サーバをターゲットとするようにアーカイブノードを構成できます。 TSM サーバは、テープライブラリを含むランダムまたはシーケンシャルアクセスのストレージデバイスとの間でオブジェクトデータを格納および読み出すための論理インターフェイスです。

アーカイブノードの ARC サービスは TSM サーバに対するクライアントとして機能し、 Tivoli Storage Manager をアーカイブストレージシステムと通信するためのミドルウェアとして使用します。

> アーカイブノードのサポート（S3 APIを使用してクラウドにアーカイブする場合とTSMミドルウェアを使用してテープにアーカイブする場合の両方）は廃止され、今後のリリースで削除される予定です。アーカイブノードから外部アーカイブストレージシステムへのオブジェクトの移動は、より多くの機能を提供するILMクラウドストレージプールに置き換えられました。
>
> を参照してください "クラウドストレージプールを使用"。

TSM 管理クラス

TSM ミドルウェアによって定義された管理クラスは、 TSM のバックアップおよびアーカイブ処理がどのように機能するかを示します。この管理クラスを使用して、 TSM サーバによって適用されるコンテンツ用のルールを指定できます。これらのルールは StorageGRID システムの ILM ポリシーとは独立して機能します。オブジェクトは永続的に格納され、アーカイブノードによっていつでも読み出し可能であるという StorageGRID システムの要件と矛盾しないことが必要です。アーカイブノードから TSM サーバにオブジェクトデータが送信されたあと、 TSM サーバが管理するテープにオブジェクトデータが格納される間、 TSM のライフサイクルと保持のルールが適用されます。

TSM 管理クラスは、アーカイブノードから TSM サーバにオブジェクトデータが送信されたあと、データの場所または保持のルールを適用するために TSM サーバで使用されます。たとえば、データベースのバックアップとして識別されたオブジェクト（新しいデータで上書き可能な一時的コンテンツ）を、アプリケーションデータ（無期限に保持する必要のある固定コンテンツ）とは別の方法で処理できます。

TSM ミドルウェアへの接続を設定します

アーカイブノードがTivoli Storage Manager（TSM）ミドルウェアと通信するためには、いくつかの設定を行う必要があります。

作業を開始する前に

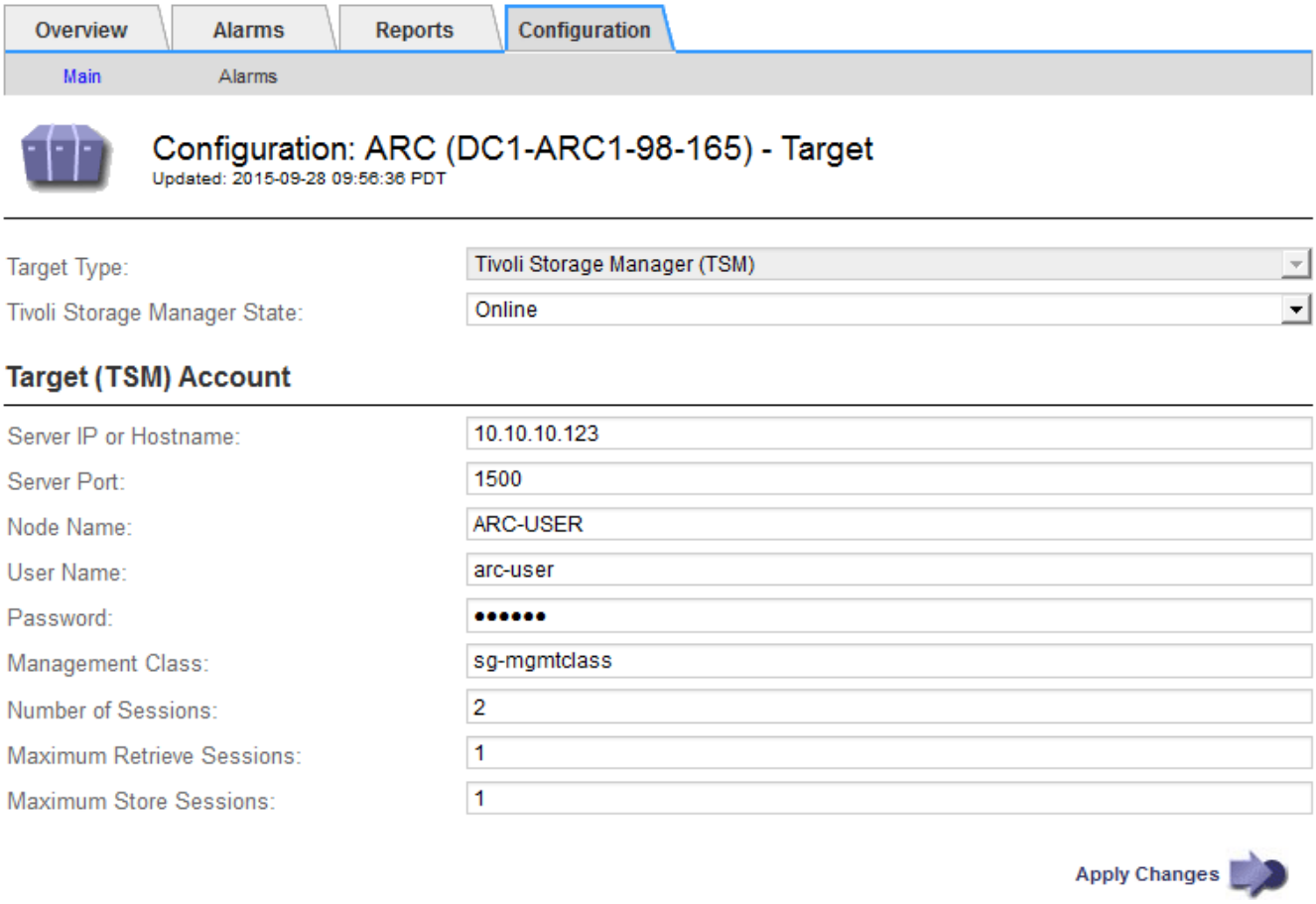
- を使用して Grid Manager にサインインします "サポートされている Web ブラウザ"。
- 特定のアクセス権限が必要です。

このタスクについて

これらの設定が完了するまで ARC サービスは Tivoli Storage Manager と通信できないため、 Major アラーム状態のままです。

手順

1. サポート * > * ツール * > * グリッドトポロジ * を選択します。
2. 「 * _ アーカイブノード _ * > * ARC * > * ターゲット * 」を選択します。
3. * Configuration * > * Main * を選択します。



4. [ターゲット・タイプ] ドロップダウン・リストから **'[** Tivoli Storage Manager(TSM)*] を選択します
5. Tivoli Storage Manager State * では、 TSM ミドルウェアサーバからの読み出しを防ぐために「 * Offline * 」を選択します。

   デフォルトでは、「 Tivoli Storage Manager State 」は「 Online 」に設定されています。つまり、アーカイブノードは TSM ミドルウェアサーバからオブジェクトデータを読み出すことができます。

6. 次の情報を入力します。

   ◦ * Server IP or Hostname * ： ARC サービスが使用する TSM ミドルウェアサーバの IP アドレスまたは

完全修飾ドメイン名を指定します。デフォルトの IP アドレスは 127.0.0.1 です。

- * Server Port * ： ARC サービスの接続先の TSM ミドルウェアサーバ上のポート番号を指定します。デフォルトは 1500 です。
- * Node Name * ：アーカイブノードの名前を指定します。TSM ミドルウェアサーバに登録した名前（ arc - user ）を入力する必要があります。
- * User Name * ： ARC サービスが TSM サーバへのログインに使用するユーザ名を指定します。デフォルトのユーザ名（ arc - user ）またはアーカイブノード用に指定した管理ユーザを入力します。
- * Password * ： ARC サービスが TSM サーバへのログインに使用するパスワードを指定します。
- * 管理クラス * ：オブジェクトが StorageGRID システムに保存されるときに管理クラスが指定されていない場合や、指定した管理クラスが TSM ミドルウェアサーバ上で定義されていない場合に使用するデフォルトの管理クラスを指定します。
- * Number of Sessions * ： TSM ミドルウェアサーバ上にあるアーカイブノード専用のテープドライブの数を指定します。アーカイブノードは、最大でマウントポイントごとに 1 つのセッションと少数（ 5 つ未満）の追加セッションを同時に作成します。

  アーカイブノードを登録または更新したときには、この値を MAXNUMMP （マウントポイントの最大数）と同じ値に変更する必要があります（登録コマンドでは、値が設定されていない場合の MAXNUMMP のデフォルト値は 1 です）。

また、 TSM サーバの MAXSESSIONS の値を、 ARC サービス用に設定されている Sessions の数以上の数値に変更する必要があります。TSM サーバ上の MAXSESSIONS のデフォルト値は 25 です。

- * Maximum Retrieve Sessions * ： ARC サービスが読み出し処理用に TSM ミドルウェアサーバに対して開くことができるセッションの最大数を指定します。ほとんどの場合、適切な値は「セッション数 - ストアセッションの最大数」です。1 つのテープ・ドライブを共有してストレージと取得を行う必要がある場合は ' セッション数に等しい値を指定します
- * Maximum Store Sessions * ： ARC サービスがアーカイブ処理用に TSM ミドルウェアサーバに対して開くことができる同時セッションの最大数を指定します。

  この値は、対象のアーカイブストレージシステムが一杯で、読み出しのみが可能な場合を除き、 1 に設定する必要があります。すべてのセッションを読み出しに使用するには、この値を 0 に設定します。

7. 「 * 変更を適用する * 」を選択します。

TSM ミドルウェアセッション用にアーカイブノードを最適化します

アーカイブノードのセッションを設定することで、 Tivoli Server Manager （ TSM ）に接続するアーカイブノードのパフォーマンスを最適化できます。

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"。
- 特定のアクセス権限が必要です。

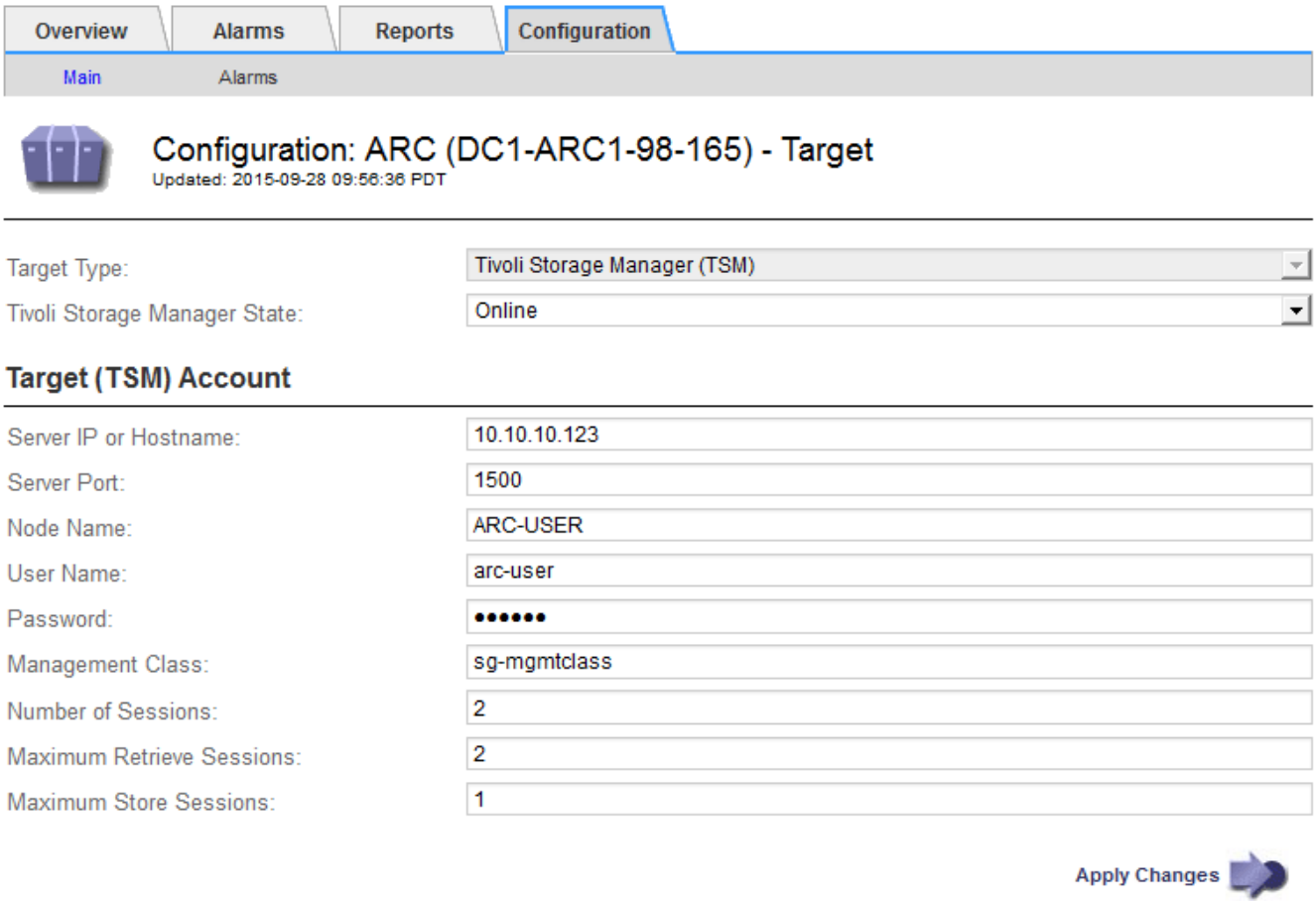
このタスクについて

通常、アーカイブノードが TSM ミドルウェアサーバに対して同時に開くことができるセッションの数は、 TSM サーバが所有するアーカイブノード専用のテープドライブの数に設定されます。1 本のテープドライブがストレージ用に割り当てられ、残りは読み出し用に割り当てられます。ただし、ストレージノードがアーカ

イブノードのコピーからリビルドされている場合や、アーカイブノードが読み取り専用モードで動作している場合は、読み出しセッションの最大数を同時セッション数と同じに設定することで、 TSM サーバのパフォーマンスを最適化できます。したがって、すべてのドライブを同時に読み出しに使用できます。また、必要に応じて、これらのドライブのうち 1 つをストレージに使用することもできます。

手順

1. サポート * > * ツール * > * グリッドトポロジ * を選択します。
2. 「 * _ アーカイブノード _ * > * ARC * > * ターゲット * 」を選択します。
3. * Configuration * > * Main * を選択します。
4. Maximum Retrieve Sessions * を Number of Sessions * と同じに変更します。



5. 「 * 変更を適用する * 」を選択します。

TSM のアーカイブ状態とカウンタを設定します

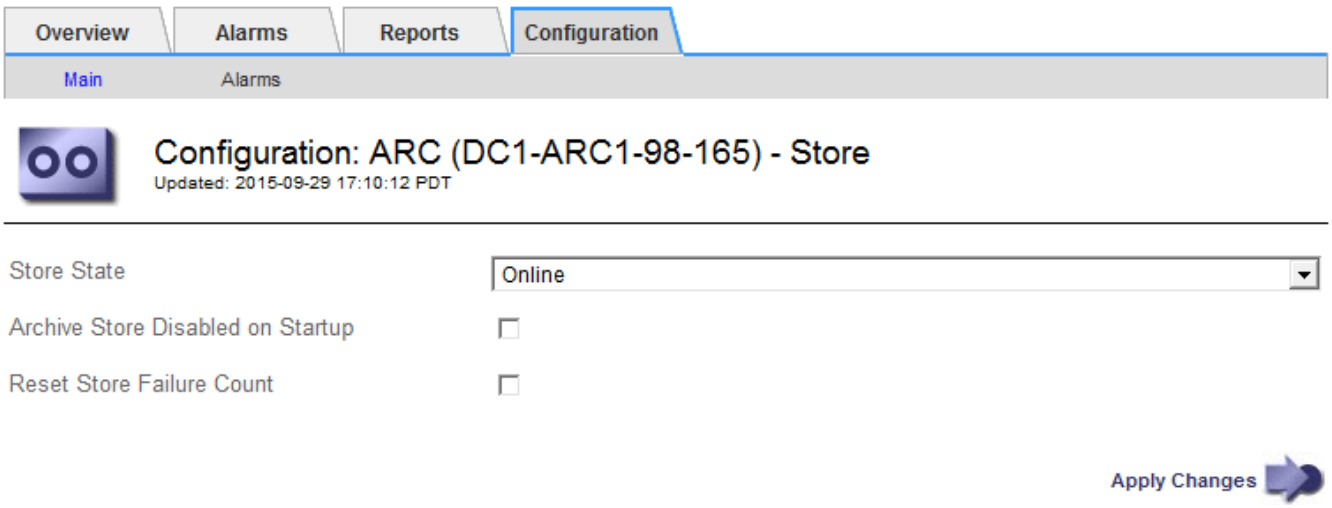
アーカイブノードが TSM ミドルウェアサーバに接続している場合は、アーカイブノードのアーカイブストアの状態をオンラインまたはオフラインに設定できます。また、アーカイブノードの初回起動時にアーカイブストアを無効にしたり、関連するアラーム用に追跡されているエラー数をリセットしたりすることもできます。

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"。
- 特定のアクセス権限が必要です。

手順

1. サポート * > * ツール * > * グリッドトポロジ * を選択します。
2. 「 * _ アーカイブノード _ * > * ARC * > * Store * 」を選択します。
3. * Configuration * > * Main * を選択します。



4. 必要に応じて次の設定を変更します。
   - Store State ：コンポーネントの状態を次のいずれかに設定します。
     - Online ：アーカイブノードはオブジェクトデータを処理してアーカイブストレージシステムに格納できます。
     - Offline ：アーカイブノードはオブジェクトデータを処理してアーカイブストレージシステムに格納できません。
   - Archive Store Disabled on Startup ：オンにすると、アーカイブストアコンポーネントは再起動後も読み取り専用のままになります。ターゲットのアーカイブストレージシステムへの格納を継続的に無効にする場合に使用します。対象のアーカイブストレージシステムでコンテンツを受け入れられない場合に便利です。
   - Reset Store Failure Count ：ストア障害のカウンタをリセットします。この設定を使用して、 ARVF （ Stores Failure ）アラームをクリアできます。
5. 「 * 変更を適用する * 」を選択します。

関連情報

"TSM サーバの容量が上限に達したときのアーカイブノードの管理"

TSM サーバの容量が上限に達したときのアーカイブノードの管理

TSM サーバには、管理対象の TSM データベースまたはアーカイブメディアストレージの容量が上限に近づいている場合にアーカイブノードに通知する手段がありません。この状況を回避するには、 TSM サーバをプロアクティブに監視します。

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"。
- 特定のアクセス権限が必要です。

このタスクについて

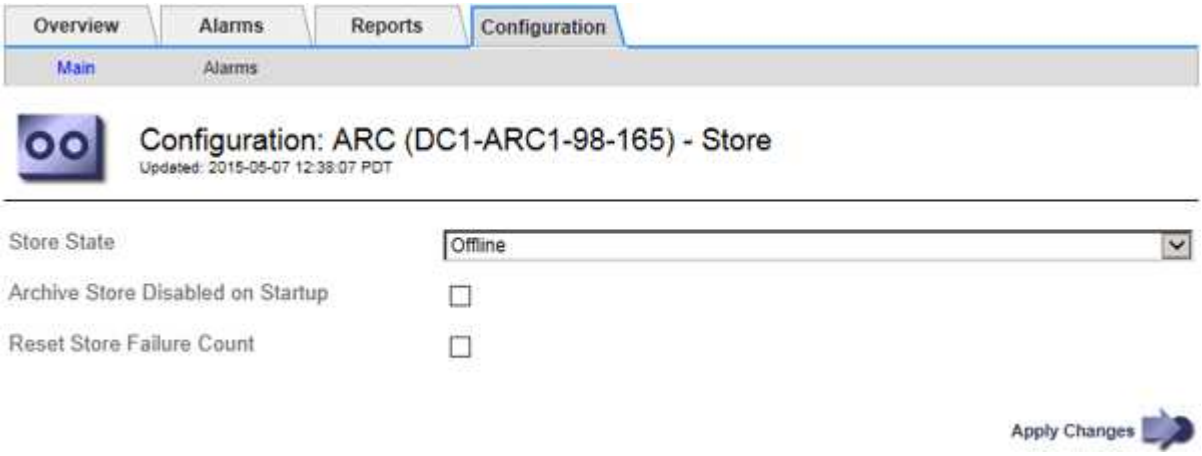
アーカイブノードは、 TSM サーバが新しいコンテンツの受け入れを停止したあとも引き続き TSM サーバに転送するオブジェクトデータを受け入れますが、このコンテンツは'TSMサーバが管理するメディアに書き込むことはできませんアラームがトリガーされます。

ARC サービスから TSM サーバにコンテンツが送信されないようにします

ARC サービスから TSM サーバにさらにコンテンツが送信されないようにするには、アーカイブノードの * ARC * > * Store * コンポーネントをオフラインにします。この手順 は、 TSM サーバがメンテナンスに使用できないときにアラームを生成しない場合にも役立ちます。

手順

1. サポート * > * ツール * > * グリッドトポロジ * を選択します。
2. 「 * _ アーカイブノード _ * > * ARC * > * Store * 」を選択します。
3. * Configuration * > * Main * を選択します。



4. 「Store State」を「」に変更します `Offline`。
5. 「 Archive Store Disabled on Startup * 」を選択します。
6. 「 * 変更を適用する * 」を選択します。

TSM ミドルウェアが容量の限界に達した場合は、アーカイブノードを読み取り専用に設定します

ターゲットの TSM ミドルウェアサーバが容量の限界に達した場合、読み出しのみを実行するようにアーカイブノードを最適化できます。

手順

1. サポート * > * ツール * > * グリッドトポロジ * を選択します。
2. 「 * _ アーカイブノード _ * > * ARC * > * ターゲット * 」を選択します。
3. * Configuration * > * Main * を選択します。
4. Maximum Retrieve Sessions を Number of Sessions に示されている同時セッション数と同じ数に変更します
5. 最大ストアセッション数を 0 に変更します。

アーカイブノードが読み取り専用の場合、最大ストアセッション数を 0 に変更する必要はありません。ストアセッションは作成されません。

6. 「 * 変更を適用する * 」を選択します。

アーカイブノードの読み出し設定を行います

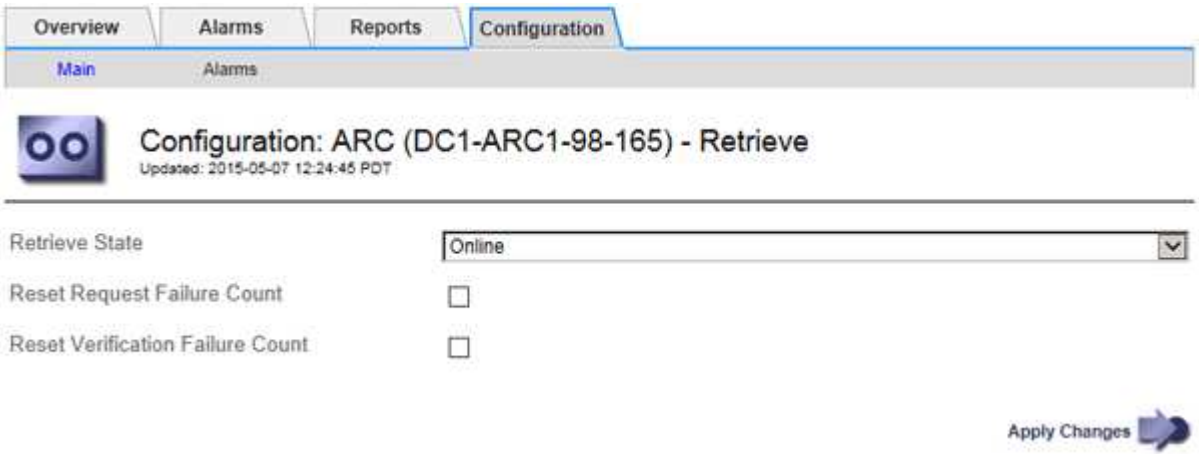
アーカイブノードの読み出し設定を行って、状態をオンラインまたはオフラインに設定したり、関連するアラームで追跡されているエラー数をリセットしたりできます。

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"。
- 特定のアクセス権限が必要です。

手順

1. サポート * > * ツール * > * グリッドトポロジ * を選択します。
2. アーカイブノード * > * ARC * > * Retrieve * を選択します。
3. * Configuration * > * Main * を選択します。



4. 必要に応じて次の設定を変更します。
   - * Retrieve State * ：コンポーネントの状態を次のいずれかに設定します。
     - Online ：グリッドノードがアーカイブメディアデバイスからオブジェクトデータを読み出すことができます。
     - Offline ：グリッドノードはオブジェクトデータを読み出すことができません。
   - Reset Request Failures Count：このチェックボックスを選択すると、要求エラーのカウンタがリセットされます。この設定を使用して、 ARRF （ Request Failures ）アラームをクリアできます。
   - Reset Verification Failure Count：オンにすると、読み出したオブジェクトデータの検証エラーのカウンタがリセットされます。この設定を使用して、 ARRV （ Verification Failures ）アラームをクリアできます。
5. 「 * 変更を適用する * 」を選択します。

アーカイブノードのレプリケーションを設定します

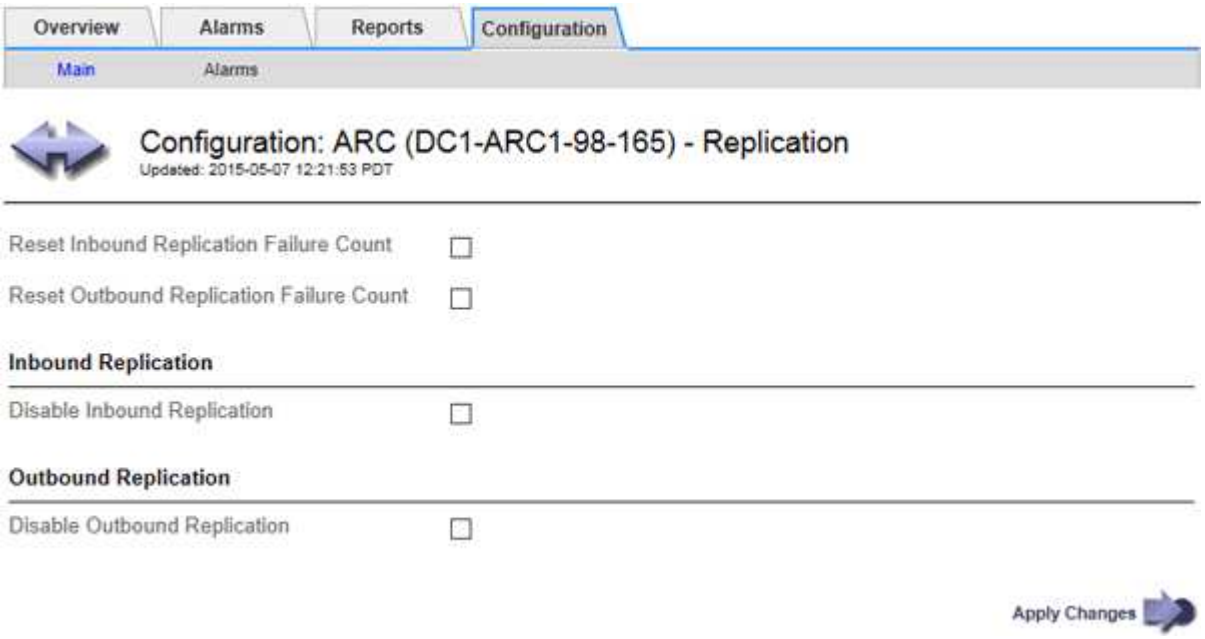
アーカイブノードのレプリケーション設定を行って、インバウンドおよびアウトバウンドのレプリケーションを無効にしたり、関連するアラームで追跡されているエラー数をリセットしたりできます。

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"。
- 特定のアクセス権限が必要です。

手順

1. サポート * > * ツール * > * グリッドトポロジ * を選択します。
2. 「 * _ アーカイブノード _ * > * ARC * > * レプリケーション * 」を選択します。
3. * Configuration * > * Main * を選択します。



4. 必要に応じて次の設定を変更します。
   - * Reset Inbound Replication Failure Count * ：インバウンドレプリケーションエラーのカウンタをリセットする場合に選択します。この設定を使用して、 RIRF （ Inbound Replications - - Failed ）アラームをクリアできます。
   - **Reset Outbound Replication Failure Count** ：アウトバウンドレプリケーションエラーのカウンタをリセットする場合に選択します。これを使用すると、 RORF （ Outbound Replications - - Failed ）アラームをクリアできます。
   - * インバウンド複製を無効にする *: メンテナンスまたは手順 のテストの一環としてインバウンド複製を無効にする場合に選択します。通常の運用中はオフのままにします。

     インバウンドレプリケーションを無効にすると、ARCサービスからオブジェクトデータを読み出してStorageGRID システム内の別の場所にレプリケートすることはできますが、システム内の別の場所からこのARCサービスにオブジェクトをレプリケートすることはできません。ARC サービスは読み取り専用です。

◦ アウトバウンドレプリケーションを無効にする：手順 のメンテナンスまたはテストの一環としてアウトバウンドレプリケーション（HTTP読み出し用のコンテンツ要求を含む）を無効にする場合は、このチェックボックスを選択します。通常の運用中はオフのままにします。

アウトバウンドレプリケーションを無効にすると、このARCサービスにオブジェクトデータをコピーしてILMルールに従うことはできますが、ARCサービスからオブジェクトデータを読み出してStorageGRID システム内の別の場所にコピーすることはできません。ARC サービスは書き込み専用です。

5. 「 * 変更を適用する * 」を選択します。

アーカイブノード用のカスタムアラームを設定します

ARQL 属性と ARRL 属性のカスタムアラームを設定する必要があります。これらの属性は、アーカイブノードがアーカイブストレージシステムからオブジェクトデータを読み出す際の速度と効率を監視します。

- ARQL ：平均キュー長。アーカイブストレージシステムから読み出し用にキューに登録されたオブジェクトデータの平均時間（マイクロ秒）。
- ARRL ：平均リクエストレイテンシ。アーカイブノードがアーカイブストレージシステムからオブジェクトデータを読み出すために必要な平均時間（マイクロ秒）。

これらの属性の許容値は、アーカイブストレージシステムの設定および使用方法によって異なります。（ * ARC * > * Retrieve * > * Overview * > * Main * に移動します）。 要求のタイムアウトに設定された値や、取得要求に使用できるセッション数は特に影響を受けます。

統合が完了したら、アーカイブノードによるオブジェクトデータの読み出しを監視して、通常の読み出し時間およびキューの長さを確認します。次に、異常な動作状態が発生した場合にトリガーされる、 ARQL と ARRL のカスタムアラームを作成します。の手順を参照してください "アラームの管理（従来のシステム）"。

Tivoli Storage Manager を統合します

アーカイブノードの設定と処理

StorageGRID システムは、オブジェクトが無期限に保存され、常にアクセス可能な場所として、アーカイブノードを管理します。

オブジェクトが取り込まれると、 StorageGRID システムに対して定義されている情報ライフサイクル管理（ ILM ）ルールに基づいて、アーカイブノードを含む必要なすべての場所にコピーが作成されます。アーカイブノードは TSM サーバに対するクライアントとして機能し、 StorageGRID ソフトウェアのインストール時に TSM クライアントライブラリがアーカイブノードにインストールされます。ストレージ用にアーカイブノードに転送されたオブジェクトデータは、 TSM サーバに直接保存されます。TSM サーバへの保存前にアーカイブノードがオブジェクトデータをステージングしたり、オブジェクトを集約したりすることはありません。ただし、データ速度が保証されれば、アーカイブノードから TSM サーバに 1 回のトランザクションで複数のコピーを送信できます。

アーカイブノードから TSM サーバに保存されたオブジェクトデータは、ライフサイクル / 保持ポリシーに従って TSM サーバで管理されます。これらの保持ポリシーは、アーカイブノードの処理に対応するように定義する必要があります。つまり、アーカイブノードによって保存されたオブジェクトデータは、アーカイブノードによって削除されないかぎり、無期限に保存されていつでもアーカイブノードからアクセスできる必要があります。

StorageGRID システムの ILM ルールと TSM サーバのライフサイクル / 保持ポリシーの間に接続は確立されていません。それぞれが互いに独立して動作します。ただし、各オブジェクトが StorageGRID システムに取り込まれる際に、そのオブジェクトに TSM 管理クラスを割り当てることができます。この管理クラスは、オブジェクトデータとともに TSM サーバに渡されます。オブジェクトタイプごとに異なる管理クラスを割り当てると、オブジェクトデータを別々のストレージプールに配置したり、必要に応じて異なる移行ポリシーや保持ポリシーを適用したりするように TSM サーバを設定できます。たとえば、データベースのバックアップとして識別されたオブジェクト（新しいデータで上書き可能な一時的コンテンツ）を、アプリケーションデータ（無期限に保持する必要のある固定コンテンツ）とは別の方法で処理できます。

アーカイブノードは新規または既存の TSM サーバと統合でき、専用の TSM サーバは必要ありません。TSM サーバは、サイズが予想される最大負荷に対応していれば、他のクライアントと共有できます。TSM は、アーカイブノードとは別のサーバまたは仮想マシンにインストールする必要があります。

複数のアーカイブノードから同じ TSM サーバに書き込むように設定できますが、この設定が推奨されるのは、アーカイブノードが異なるデータセットを TSM サーバに書き込む場合のみです。各アーカイブノードが同じオブジェクトデータのコピーをアーカイブに書き込む場合は、複数のアーカイブノードを同じ TSM サーバに書き込む設定は推奨されません。後者のシナリオでは、本来ならばオブジェクトデータの独立した、冗長コピーとなるはずが、両方のコピーが単一点障害（ TSM サーバ）となります。

アーカイブノードはTSMのHierarchical Storage Management（HSM；階層型ストレージ管理）コンポーネントを使用しません。

構成のベストプラクティス

TSM サーバをサイジングおよび設定する場合、アーカイブノードとの連携を最適化するベストプラクティスがあります。

TSM サーバをサイジングおよび設定する際には、次の点を考慮する必要があります。

- アーカイブノードは TSM サーバに保存する前にオブジェクトを集約しないため、アーカイブノードに書き込まれるすべてのオブジェクトへの参照を格納できるように TSM データベースをサイジングする必要があります。
- アーカイブノードソフトウェアでは、テープやその他のリムーバブルメディアにオブジェクトを直接書き込む際のレイテンシを許容できません。したがって TSM サーバには、リムーバブルメディアが使用されるたびにアーカイブノードが最初にデータを保存する初期ストレージ用のディスクストレージプールを設定する必要があります。
- イベントベースの保持を使用するには、 TSM の保持ポリシーを設定する必要があります。アーカイブノードでは、作成ベースの TSM 保持ポリシーはサポートされません。保持ポリシーでは、推奨設定である retmin=0 および retver=0 （アーカイブノードが保持イベントをトリガーしたときに保持が開始され、その後 0 日間保持される）を使用してください。ただし、これらの retmin 値および retver 値はオプションです。

ディスクプールは、テーププールにデータを移行するように設定する必要があります（つまり、テーププールをディスクプールの NXTSTGPOOL に設定します）。テーププールは、両方のプールに同時に書き込みを行うディスクプールのコピープールとして設定しないでください（つまり、テーププールをディスクプールのCOPYSTGPOOLにすることはできません）。アーカイブノードデータを含むテープのオフラインコピーを作成するには、 TSM サーバの 2 つ目のテーププールとして、アーカイブノードのデータ用に使用されるテーププールのコピープールを設定します。

インストールプロセスを完了した時点ではアーカイブノードは機能していません。StorageGRID システムが TSM アーカイブノードにオブジェクトを保存できるようにするには、 TSM サーバのインストールと設定を完了し、 TSM サーバと通信するようにアーカイブノードを設定する必要があります。

必要に応じて次の IBM のドキュメントを参照し、 StorageGRID システムでアーカイブノードと TSM サーバを統合する準備をしてください。

- "『 IBM Tape Device Drivers Installation and User's Guide 』（ IBM テープデバイスドライバインストールおよびユーザーズガイド）"
- "IBM Tape Device Drivers Programming Reference"

新しい **TSM** サーバをインストールします

アーカイブノードを新規または既存の TSM サーバと統合できます。新しい TSM サーバをインストールする場合は、 TSM のドキュメントの指示に従ってインストールを完了してください。

アーカイブノードをTSMサーバと同じホストにすることはできません。

TSM サーバを設定します

このセクションでは、 TSM のベストプラクティスに従って TSM サーバを準備する手順を記載します。

次の手順では、のプロセスについて説明します。

- TSM サーバ上でディスクストレージプール、およびテープストレージプール（必要な場合）を定義します
- アーカイブノードから保存されたデータ用に TSM 管理クラスを使用するドメインポリシーを定義し、そのドメインポリシーを使用するようにノードを登録します

これらの手順はあくまでも参考情報です。TSMのドキュメントに代わるものではなく、すべての構成に適した完全で包括的な手順を提供するものでもありません。環境に固有の手順は、詳細な要件を把握し、 TSM サーバのすべてのドキュメントに精通している TSM 管理者に確認する必要があります。

TSM テープストレージプールとディスクストレージプールを定義します

アーカイブノードはディスクストレージプールに書き込みます。コンテンツをテープにアーカイブするには、コンテンツをテープストレージプールに移動するようにディスクストレージプールを設定する必要があります。

このタスクについて

1 台の TSM サーバに対し、 Tivoli Storage Manager でテープストレージプールとディスクストレージプールを定義する必要があります。ディスクプールを定義したら、ディスクボリュームを作成してディスクプールに割り当てます。TSM サーバでディスクのみのストレージを使用する場合、テーププールは必要ありません。

テープストレージプールを作成する前に、TSMサーバでいくつかの手順を実行する必要があります。（テープライブラリを作成し、テープライブラリにドライブを少なくとも 1 本作成します。サーバからライブラリへのパスとサーバからドライブへのパスを定義し、ドライブのデバイスクラスを定義します）。 これらの手順の詳細は、サイトのハードウェア構成とストレージ要件によって異なります。詳細については、 TSM のドキュメントを参照してください。

以下に、このプロセスの手順を示します。サイトの要件は導入の要件によって異なることに注意してください。設定の詳細および手順については、 TSM のドキュメントを参照してください。

次のコマンドを実行するには、管理者権限でサーバにログインし、dsmadmcツールを使用する必要があります。

手順

1. テープライブラリを作成します。

   `define library tapelibrary libtype=scsi`

   ここで *tapelibrary* はテープライブラリの任意の名前で、の値です `libtype` テープライブラリのタイプによって異なる場合があります。

2. サーバからテープライブラリへのパスを定義します。

   `define path servername tapelibrary srctype=server desttype=library device=lib-devicename`

   - *servername* はTSMサーバの名前です
   - *tapelibrary* は、定義したテープライブラリの名前です
   - *lib-devicename* は、テープライブラリのデバイス名です

3. ライブラリのドライブを定義します。

   `define drive tapelibrary drivename`

   - *drivename* は、ドライブに指定する名前です
   - *tapelibrary* は、定義したテープライブラリの名前です

     ハードウェア構成によっては、追加のドライブを設定することが必要になる場合があります。（たとえば、 1 つのテープライブラリからの入力が 2 つあるファイバチャネルスイッチに TSM サーバが接続されている場合は、入力ごとにドライブを定義します）。

4. サーバから定義したドライブへのパスを定義します。

   `define path servername drivename srctype=server desttype=drive library=tapelibrary device=drive-dname`

   - *drive-dname* は、ドライブのデバイス名です
   - *tapelibrary* は、定義したテープライブラリの名前です

     テープライブラリ用に定義したドライブごとに、別のを使用してこの手順を繰り返します *drivename* および *drive-dname* をクリックします。

5. ドライブのデバイスクラスを定義します。

   ```
   define devclass DeviceClassName devtype=lto library=tapelibrary
   format=tapetype
   ```

   - *DeviceClassName* は、デバイスクラスの名前です
   - *lto* は、サーバに接続されているドライブのタイプです
   - *tapelibrary* は、定義したテープライブラリの名前です
   - *tapetype* は、テープのタイプです。たとえば、ultrium3です

6. ライブラリのインベントリにテープボリュームを追加します。

   ```
   checkin libvolume tapelibrary
   ```

   tapelibrary は、定義したテープライブラリの名前です。

7. プライマリテープストレージプールを作成します。

   ```
   define stgpool SGWSTapePool DeviceClassName description=description
   collocate=filespace maxscratch=XX
   ```

   - *SGWSTapePool* はアーカイブノードのテープストレージプールの名前です。テープストレージプールには（ TSM サーバが想定する命名規則に沿ってさえいれば）任意の名前を選択できます。
   - *DeviceClassName* は、テープライブラリのデバイスクラス名です。
   - *description* はストレージプールの概要 で、を使用してTSMサーバに表示できます `query stgpool` コマンドを実行しますたとえば ' アーカイブ・ノード用のテープ・ストレージ・プールなどです
   - *collocate=filespace* は、TSMサーバが同じファイルスペースのオブジェクトを1つのテープに書き込む必要があることを指定します。
   - XX は次のいずれかです。
     - テープライブラリ内の空のテープの数（アーカイブノードだけがライブラリを使用している場合）。
     - StorageGRID システム用に割り当てられているテープの数（テープライブラリが共有されている場合）。

8. TSM サーバで、ディスクストレージプールを作成します。TSM サーバの管理コンソールで、と入力します

   ```
   define stgpool SGWSDiskPool disk description=description
   maxsize=maximum_file_size nextstgpool=SGWSTapePool highmig=percent_high
   lowmig=percent_low
   ```

   - *SGWSDiskPool* はアーカイブノードのディスクプールの名前です。ディスクストレージプールには（ TSM が想定する命名規則に沿ってさえいれば）任意の名前を選択できます。
   - *description* はストレージプールの概要 で、を使用してTSMサーバに表示できます `query stgpool` コマンドを実行しますたとえば ' アーカイブ・ノード用のディスク・ストレージ・プールなどです

- *maximum_file_size* ディスクプールにキャッシュされるのではなく、このサイズよりも大きいオブジェクトをテープに直接書き込みます。を設定することを推奨します *maximum_file_size* を10 GBに設定します。
- *nextstgpool=SGWSTapePool* は、ディスクストレージプールをアーカイブノード用に定義したテープストレージプールと関連付けます。
- *percent_high* ディスクプールの内容のテーププールへの移行を開始する値を設定します。を設定することを推奨します *percent_high* を0に設定すると、データがすぐに移行されます
- *percent_low* テープ・プールへの移行を停止する値を設定します。を設定することを推奨します *percent_low* を0に設定して、ディスクプールをクリアします。

9. TSM サーバで、 1 つ以上のディスクボリュームを作成してディスクプールに割り当てます。

```
define volume SGWSDiskPool volume_name formatsize=size
```

- *SGWSDiskPool* はディスクプール名です。
- *volume_name* はボリュームの完全パスです（例： `/var/local/arc/stage6.dsm`）をテープに転送する準備として、TSMサーバ上でディスクプールの内容を書き込みます。
- *size* は、ディスクボリュームのサイズ（MB単位）です。

  たとえば、テープボリュームの容量が 200GB の場合、ディスクプールのコンテンツで 1 つのテープを使い切るようなディスクボリュームを 1 個作成するには、 size の値を 200000 に設定します。

  ただし、 TSM サーバがディスクプール内の各ボリュームに書き込むことができるため、小さいサイズのディスクボリュームを複数作成する方がよい場合もあります。たとえばテープサイズが 250GB の場合、 10GB （ 10000 ）のディスクボリュームを 25 個作成します。

TSM サーバは、ディスクボリューム用にディレクトリ内のスペースを事前に割り当てます。この処理には、完了までに時間がかかることがあります（ 200GB のディスクボリュームの場合は 3 時間以上）。

ドメインポリシーを定義し、ノードを登録します

アーカイブノードから保存されたデータ用に TSM 管理クラスを使用するドメインポリシーを定義し、そのドメインポリシーを使用するようにノードを登録する必要があります。

> Tivoli Storage Manager （ TSM ）でアーカイブノードのクライアントパスワードの期限が切れると、アーカイブノードのプロセスでメモリリークが発生する可能性があります。アーカイブノードのクライアントユーザ名 / パスワードの期限が切れないように TSM サーバを設定してください。

アーカイブノードとして使用するノードを TSM サーバに登録する（または既存のノードを更新する）場合は、そのノードが書き込み処理に使用できるマウントポイントの数を指定する必要があります。そのためには、 REGISTER NODE コマンドで MAXNUMMP パラメータを指定します。通常、マウントポイントの数は、アーカイブノードに割り当てられているテープドライブのヘッド数と同じです。TSMサーバ上のMAXNUMMPに指定する数は、アーカイブノードの* ARC > Target > Configuration > Main > Maximum Store Sessions *に設定されている値以上である必要があります。 アーカイブノードでは同時格納セッションはサポートされないため、この値は0または1に設定されています。

TSM サーバ用に設定した MAXSESSIONS の値によって、すべてのクライアントアプリケーションが TSM サ

ーバに対して開くことのできる最大セッション数が制御されます。TSM で指定する MAXSESSIONS の値は、アーカイブノードの Grid Manager で * ARC * > * Target * > * Configuration * > * Main * > * Sessions * に指定されている値以上である必要があります。アーカイブノードは、最大でマウントポイントごとに 1 つのセッションと少数（ 5 つ未満）の追加セッションを同時に作成します。

アーカイブノードに割り当てられているTSMノードは、カスタムドメインポリシーを使用します `tsm-domain`。。 `tsm-domain` ドメイン・ポリシーは'標準ドメイン・ポリシーの変更バージョンであり'テープに書き込むように構成され'アーカイブ先がStorageGRID システムのストレージ・プールに設定されています（*`SGWSDiskPool`*）。

ドメインポリシーを作成およびアクティブ化するには、管理者権限を使用して TSM サーバにログインし、 dsmadmc ツールを使用する必要があります。

ドメインポリシーを作成してアクティブ化します

アーカイブノードから送信されたデータを保存するように TSM サーバを設定するには、ドメインポリシーを作成してアクティブ化する必要があります。

手順

1. ドメインポリシーを作成します。

   ```
   copy domain standard tsm-domain
   ```

2. 既存の管理クラスを使用しない場合は、次のいずれかを入力します。

   ```
   define policyset tsm-domain standard

   define mgmtclass tsm-domain standard default
   ```

   `default` は、導入用のデフォルトの管理クラスです。

3. 適切なストレージプールにコピーグループを作成します。（ 1 行に）次のように入力します。

   ```
   define copygroup tsm-domain standard default type=archive
   destination=SGWSDiskPool retinit=event retmin=0 retver=0
   ```

   `default` は、アーカイブノードのデフォルトの管理クラスです。の値 `retinit`、 `retmin`および `retver` アーカイブノードで現在使用されている保持動作を反映するように選択されています

   設定しないでください `retinit` 終了： `retinit=create`。設定 `retinit=create` TSM サーバからコンテンツを削除するために保持イベントが使用されるため、アーカイブノードによるコンテンツの削除をブロックします。

4. 管理クラスをデフォルトに割り当てます。

   ```
   assign defmgmtclass tsm-domain standard default
   ```

5. 新しいポリシーセットをアクティブに設定します。

   ```
   activate policyset tsm-domain standard
   ```

activate コマンドを入力したときに表示される「 no backup copy group 」警告は無視してください。

6. 新しいポリシーセットを使用するノードを TSM サーバに登録します。TSM サーバで、次のように（ 1 行に）入力します。

```
register node arc-user arc-password passexp=0 domain=tsm-domain
MAXNUMMP=number-of-sessions
```

aarc-user と arc-password は、アーカイブノードで定義したクライアントノード名とパスワードです。また、 MAXNUMMP の値は、アーカイブノードの格納セッション用に予約されているテープドライブの数に設定されます。

デフォルトでは、ノードを登録すると、管理ユーザ ID がクライアント所有者の権限で作成され、パスワードが定義されます。

データを StorageGRID に移行

日常業務に StorageGRID システムを使用しながら、同時に StorageGRID システムに大量のデータを移行できます。

このガイドは、StorageGRID システムへの大量のデータの移行を計画する際に使用します。データ移行の一般的なガイドではなく、移行を実行するための詳細な手順も記載されていません。このセクションのガイドラインと手順に従って、日常業務を中断せずに StorageGRID システムにデータを効率的に移行し、移行したデータが StorageGRID システムによって適切に処理されるようにしてください。

StorageGRID システムの容量を確認

StorageGRID システムに大量のデータを移行する前に、予想されるボリュームを処理できるディスク容量が StorageGRID システムにあることを確認します。

StorageGRID システムにアーカイブノードが含まれていて、移行されたオブジェクトのコピーがニアラインストレージ（テープなど）に保存されている場合は、アーカイブノードのストレージに予想される移行データボリュームに対応する十分な容量があることを確認します。

容量評価の一環として、移行を計画しているオブジェクトのデータプロファイルを確認し、必要なディスク容量を計算します。StorageGRID システムのディスク容量の監視の詳細については、を参照してください "ストレージノードを管理します" の説明を参照してください "StorageGRID の監視"。

移行データの ILM ポリシーを決定します

StorageGRID システムの ILM ポリシーは、作成されるコピーの数とその格納先、および保持期間を決定します。ILM ポリシーは、オブジェクトをフィルタリングする方法、および一定の期間にわたってオブジェクトデータを管理する方法を記述した一連の ILM ルールで構成されます。

移行データの使用方法およびその要件によっては、日常業務に使用する ILM ルールとは別の、移行データに固有の ILM ルールを定義することができます。たとえば、日常的なデータ管理と移行対象のデータに異なる規制要件が適用される場合、異なるグレードのストレージに異なる数の移行データのコピーが必要となる可能性があります。

移行データと日常業務で保存されるオブジェクトデータを一意に区別できる場合は、移行データにのみ適用さ

れるルールを設定できます。

いずれかのメタデータ条件を使用してデータのタイプを確実に識別できる場合は、この条件を使用して移行データにのみ適用される ILM ルールを定義できます。

データ移行を開始する前に、 StorageGRID システムの ILM ポリシーとそのポリシーが移行データにどのように適用されるかを確認し、 ILM ポリシーへの変更があればテストしておく必要があります。を参照してください "ILM を使用してオブジェクトを管理する"。

> ILM ポリシーが正しく指定されていないと、原因 によるリカバリ不能なデータ損失が発生する可能性があります。ポリシーを想定どおりに機能させるには、 ILM ポリシーをアクティブ化する前に、 ILM ポリシーに加えたすべての変更をよく確認してください。

移行が運用に与える影響を評価

StorageGRID システムは、オブジェクトを効率的に格納して読み出せるようにすること、およびオブジェクトデータとメタデータの冗長コピーをシームレスに作成することでデータ損失に対する優れた保護を提供することを目的に設計されています。

ただし、データ移行は、日常的なシステム処理に影響を与えないように、または極端な場合にはStorageGRIDシステムに障害が発生した場合にデータが失われる危険性がないように、このガイドの手順に従って慎重に管理する必要があります。

大量のデータを移行すると、システムに新たな負荷がかかります。StorageGRID システムの負荷が高い場合は、オブジェクトの格納および読み出し要求への応答が遅くなります。その結果、日常業務に不可欠な格納および読み出し要求が影響を受ける可能性があります。移行は、原因 のその他の運用上の問題にもなります。たとえば、ストレージノードの容量が上限に近づい原因 ている場合は、一括取り込みによって断続的に大きな負荷がかかると、ストレージノードが読み取り専用と読み書き可能の間で何度も切り替わり、そのたびに通知が生成されます。

負荷の高い状態が続く場合、オブジェクトデータとメタデータの完全な冗長性を確保するために StorageGRID システムが実行する必要のあるさまざまな処理がキューに溜まっていきます。

移行中に StorageGRID システムを安全かつ効率的に運用するためには、本書のガイドラインに従ってデータ移行を慎重に管理する必要があります。データの移行にあたっては、オブジェクトを複数のバッチで取り込むか、または取り込み量を常に調整します。その後、StorageGRID システムを継続的に監視して、さまざまな属性値を超えないようにします。

データ移行のスケジュール設定と監視

所定の期間内に ILM ポリシーに従ってデータが配置されるよう、必要に応じてデータ移行をスケジュールし、監視する必要があります。

データ移行をスケジュール

主要な業務時間中はデータを移行しないでください。データの移行は、夕方や週末など、システムの使用率が低い時間帯にのみ実施してください。

アクティビティの多い時間帯には、データ移行のスケジュールを設定しないでください。ただし、アクティビティレベルが高い期間を完全に回避することが現実的でない場合はそのまま進めてかまいません。その場合は、関連する属性を注意深く監視し、許容値を超えた場合に対処する必要があります。

データ移行を監視

次の表に、データ移行中に監視する必要がある属性とその内容を示します。

取り込み速度を抑制するためにレート制限を指定したトラフィック分類ポリシーを使用する場合は、次の表に示す統計情報とともに、観察されたレートを監視し、必要に応じて制限を減らすことができます。

モニタ	説明
ILM による評価を待機しているオブジェクトの数	1. サポート * > * ツール * > * グリッドトポロジ * を選択します。 2. [***deployment***>*Overview*>*Main*] を選択します。 3. ILM アクティビティセクションで、次の属性について表示されるオブジェクトの数を監視します。 ◦ * Awaiting - All （ XQUZ ） * ： ILM による評価を待機しているオブジェクトの合計数です。 ◦ * Awaiting - Client （ XCQZ ） * ：クライアント処理（取り込みなど）から ILM による評価を待機しているオブジェクトの合計数です。 4. これらの属性のどちらかに対して表示されるオブジェクトの数が 100 、 000 を超えた場合は、オブジェクトの取り込み速度を調整して、 StorageGRID システムへの負荷を軽減してください。
ターゲットアーカイブシステムのストレージ容量	ILM ポリシーによって、移行対象データのコピーがターゲットアーカイブストレージシステム（テープまたはクラウド）に保存される場合は、ターゲットアーカイブストレージシステムの容量を監視して、移行対象データ用の十分な容量が確保されていることを確認してください。
• アーカイブノード * > * ARC * > * Store *	「 Store Failures （ ARVF ） * 」属性のアラームがトリガーされた場合、対象のアーカイブストレージシステムの容量が上限に達している可能性があります。ターゲットアーカイブストレージシステムをチェックして、アラームをトリガーした問題を解決してください。