



StorageGRID の管理

StorageGRID software

NetApp
July 23, 2026

目次

StorageGRID の管理	1
StorageGRID の管理	1
これらの説明書について	1
開始する前に	1
Grid Manager の使用を開始する	1
StorageGRIDのWebブラウザ要件	1
StorageGRID Grid Manager にサインインする	2
StorageGRID Grid Manager からログアウトします	4
StorageGRID Grid Managerのパスワードを変更する	5
StorageGRID ライセンス情報の表示	5
StorageGRID ライセンス情報の更新	7
API を使用する	7
StorageGRID へのアクセスを制御する	29
StorageGRID アクセスの制御	29
StorageGRID プロビジョニング パスフレーズを変更する	30
StorageGRIDでノードコンソールのパスワードを変更する	31
StorageGRID 管理ノードの SSH アクセス パスワードを変更する	34
StorageGRIDでIDフェデレーションを使用する	36
StorageGRID で管理者グループを管理する	41
StorageGRID の管理者グループ権限	44
StorageGRID でユーザーを管理する	47
シングル サインオン (SSO) を使用する	51
グリッドフェデレーションを使用する	77
StorageGRID グリッド フェデレーションについて学ぶ	77
StorageGRIDのアカウントクローンについて学ぶ	80
StorageGRID のクロスグリッドレプリケーションについて学ぶ	83
StorageGRIDにおけるグリッド間複製とCloudMirror複製の比較	90
StorageGRID グリッド フェデレーション接続を作成する	93
StorageGRID グリッド フェデレーション接続を管理	96
StorageGRID グリッド フェデレーションで許可されたテナントを管理する	102
StorageGRID でグリッドフェデレーションのエラーをトラブルシューティングします	108
失敗したStorageGRIDレプリケーション処理を特定して再試行する	113
セキュリティを管理する	117
StorageGRID でセキュリティを管理する	117
StorageGRID の暗号化方式の確認	118
証明書の管理	121
セキュリティ設定を構成する	154
キー管理サーバの設定	161
プロキシ設定を管理する	181

ファイアウォールを制御する	183
テナントの管理	190
StorageGRID のテナントアカウント	190
StorageGRID テナント アカウントを作成します	191
StorageGRID テナント アカウントを編集する	197
StorageGRIDテナントのローカルルートユーザーのパスワードを変更する	199
StorageGRID テナント アカウントを削除する	199
プラットフォームサービスを管理する	200
StorageGRID でテナント アカウントの S3 Select を管理する	209
クライアント接続を構成する	210
S3 クライアント接続を StorageGRID に設定	210
StorageGRID の S3 クライアントのセキュリティ	213
S3 セットアップ ウィザードを使用する	214
HAグループを管理する	225
ロード バランシングの管理	236
StorageGRIDでS3エンドポイントドメイン名を設定する	252
StorageGRID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する	256
StorageGRIDネットワーク設定を設定する	256
StorageGRID ネットワークのガイドライン	257
StorageGRIDでIPアドレスを表示する	258
StorageGRIDでVLANインターフェイスを設定する	259
管理インターフェイスの StorageGRID CORS を有効にする	264
トラフィック分類ポリシーを管理する	264
StorageGRIDの送信TLS接続でサポートされている暗号	272
StorageGRID におけるアクティブ、アイドル、および同時 HTTP 接続の利点	272
StorageGRIDでリンクコストを管理する	274
AutoSupport を使用する	277
StorageGRIDのAutoSupportについて学ぶ	277
StorageGRIDでAutoSupportを設定する	281
StorageGRIDでAutoSupportパッケージを手動でトリガーする	285
StorageGRID AutoSupport パッケージのトラブルシューティング	286
StorageGRID を経由して Eシリーズ AutoSupport パッケージを送信する	287
ストレージノードの管理	291
ストレージオブションを使用する	291
StorageGRID でのオブジェクト メタデータ ストレージの管理	294
StorageGRID でメタデータ予約領域の設定を増やす	302
StorageGRID に保存されたオブジェクトを圧縮	303
StorageGRID でストレージノード全体を管理	304
管理ノードの管理	305
StorageGRID で複数の管理ノードを使用する	305

StorageGRID の管理

StorageGRID の管理

これらの手順を使用して、StorageGRID システムを設定および管理します。

これらの説明書について

StorageGRID の設定および管理における主なタスクでは、以下のことが可能です：

- グリッドマネージャーを使用してグループとユーザーを設定します
- S3クライアントアプリケーションがオブジェクトを保存および取得できるように、テナントアカウントを作成します。
- StorageGRID ネットワークの設定と管理
- AutoSupportを設定する
- ノード設定の管理

開始する前に

- StorageGRID システムについて、全般的な理解があります。
- Linux のコマンドシェル、ネットワーク、サーバーハードウェアのセットアップと構成について、十分な知識をお持ちであることを前提としています。

Grid Manager の使用を開始する

StorageGRIDのWebブラウザ要件

対応しているウェブブラウザを使用する必要があります。

Webブラウザ	サポートされている最小バージョン
Google Chrome	138
Microsoft Edge	138
Mozilla Firefox	140

ブラウザウィンドウの幅を推奨値に設定してください。

ブラウザの幅	ピクセル
最小	1024

ブラウザの幅	ピクセル
最適	1280

StorageGRID Grid Manager にサインインする

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アドレスを入力することで、Grid Managerのサインインページにアクセスします。

各 StorageGRID システムは、1つのプライマリ管理ノードと任意の数の非プライマリ管理ノードで構成されます。任意の管理ノードで Grid Manager にサインインして、StorageGRID システムを管理できます。ただし、一部のメンテナンス手順は、プライマリ管理ノードからのみ実行できます。

HAグループに接続する

管理ノードが高可用性（HA）グループに含まれている場合、HAグループの仮想IPアドレス、またはその仮想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。グループのプライマリインターフェースとしてプライマリ管理ノードを選択する必要があります。そうすることで、プライマリ管理ノードが利用できない場合を除き、グリッドマネージャにアクセスする際にはプライマリ管理ノード上でアクセスすることになります。["高可用性グループを管理する"](#)を参照してください。

SSO を使用

サインインの手順は、["シングル サインオン（SSO）が設定されました"](#)場合、若干異なります。

最初の管理ノードで**Grid Manager**にサインインします

開始する前に

- ログイン情報をお持ちです。
- あなたは["対応ウェブブラウザ"](#)を使用しています。
- お使いのウェブブラウザでCookieが有効になっています。
- あなたは、少なくとも1つの権限を持つユーザーグループに属しています。
- グリッドマネージャの URL をお持ちです：

```
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にポート番号を含めてください。

```
https://FQDN_or_Admin_Node_IP:port/
```



制限付きGrid ManagerポートではSSOは利用できません。ポート443を使用する必要があります。

手順

1. 対応ウェブブラウザを起動してください。
2. ブラウザのアドレスバーに、Grid Manager の URL を入力します。
3. セキュリティ警告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てください。["セキュリティ証明書を管理する"](#)を参照してください。
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 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を使用していません

- a. グリッドマネージャーのユーザー名とパスワードを入力してください。
- b. 「サインイン」を選択します。

SSOの使用

- StorageGRID が SSO を使用しており、このブラウザでこの URL に初めてアクセスする場合：
 - i. 「サインイン」を選択します。アカウントフィールドは 0 のままにしておくことができます。
 - ii. 組織のSSOサインインページに、標準のSSO認証情報を入力してください。

例えば、StorageGRID が SSO を使用しており、以前に Grid Manager またはテナントアカウントにアクセスしたことがある場合：

- A. **0** (グリッドマネージャーのアカウントID) を入力するか、最近使用したアカウントの一覧に*グリッドマネージャー*が表示されている場合は、それを選択してください。
- B. 「サインイン」を選択します。
- C. 組織のSSOサインインページで、通常のSSO認証情報を使用してサインインしてください。

ログインすると、ダッシュボードを含むグリッドマネージャーのホーム画面が表示されます。提供される情報については、["ダッシュボードの表示と管理"](#)を参照してください。

別の管理ノードにサインインする

別の管理ノードにサインインするには、以下の手順に従ってください。

SSOを使用していません

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。必要に応じてポート番号を含めてください。
2. グリッドマネージャーのユーザー名とパスワードを入力してください。
3. 「サインイン」を選択します。

SSOの使用

StorageGRID が SSO を使用しており、1つの管理ノードにサインインしている場合、再度サインインすることなく他の管理ノードにアクセスできます。

手順

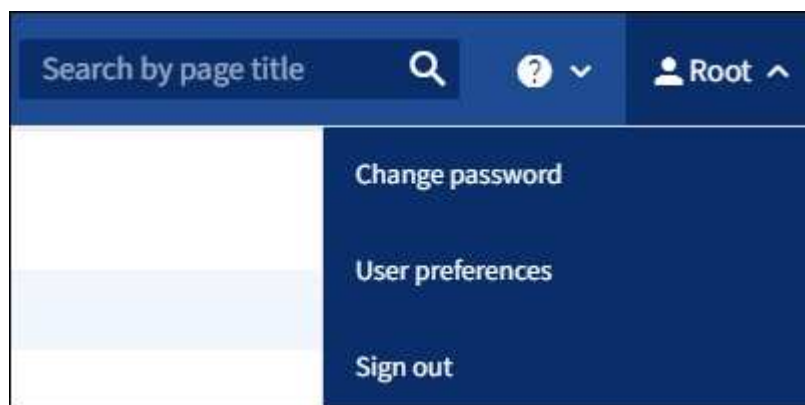
1. ブラウザのアドレスバーに、もう一方の管理ノードの完全修飾ドメイン名またはIPアドレスを入力してください。
2. SSOセッションの有効期限が切れている場合は、再度認証情報を入力してください。

StorageGRID Grid Manager からログアウトします

グリッドマネージャーでの作業が完了したら、不正なユーザーが StorageGRID システムにアクセスできないように、必ずサインアウトしてください。ブラウザの Cookie 設定によっては、ブラウザを閉じて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. 右上隅にあるユーザー名を選択してください。



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	管理者ノードからサインアウトしました。 グリッドマネージャー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は、各ノードからサインアウトする必要があります。
SSOが有効になっている	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した。StorageGRID のサインインページが表示されます。Grid Manager が 最近使用したアカウント ドロップダウンのデフォルトとして表示され、アカウント ID フィールドには 0 が表示されます。 注: SSO が有効になっていて、テナントマネージャーにもサインインしている場合は、"テナントアカウントからサインアウトする" から "SSO からサインアウト" する必要もあります。

StorageGRID Grid Managerのパスワードを変更する

Grid Managerのローカルユーザーであれば、ご自身でパスワードを変更できます。

開始する前に

"[対応ウェブブラウザ](#)" を使用して Grid Manager にサインインしています。

タスク概要

StorageGRID にフェデレーションユーザーとしてサインインしている場合、またはシングル 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. グリッドマネージャーのヘッダーから、**your name** > *パスワードの変更*を選択します。
2. 現在のパスワードを入力してください。
3. 新しいパスワードを入力してください。

パスワードは8文字以上32文字以下でなければなりません。パスワードは大文字と小文字を区別します。

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

StorageGRID ライセンス情報の表示

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

開始する前に

"[対応ウェブブラウザ](#)" を使用して Grid Manager にサインインしています。

タスク概要

この StorageGRID システムのソフトウェアライセンスに問題がある場合、ダッシュボードのヘルスステータスカードにライセンスステータスアイコンと「ライセンス」リンクが表示されます。この数字は、ライセンス関連の問題の数を示しています。



手順

1. 以下のいずれかの方法でライセンスページにアクセスしてください。

- **Maintenance > System > License** を選択します。
- ダッシュボードの「Health status」カードから、「License status」アイコンまたは「License」リンクを選択します。

このリンクは、ライセンスに問題がある場合にのみ表示されます。

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 は、この StorageGRID インストールの固有の識別番号です。
- ライセンスのシリアル番号
- ライセンスの種類（永久ライセンス*または*サブスクリプション）
- グリッドのライセンス済みストレージ容量
- サポートされているストレージ容量
- ライセンスの有効期限。永久ライセンスの場合は **N/A** と表示されます。
- サポート終了日

この日付は現在のライセンスファイルから読み取られたもので、ライセンスファイルを取得後にサポート サービス契約を延長または更新した場合は、最新の情報が反映されていない可能性があります。この値を更新するには、"[StorageGRID ライセンス情報の更新](#)"を参照してください。また、Active IQ を使用して実際の契約終了日を確認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 ライセンス情報の更新

ライセンスの条件が変更された場合は、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、グリッドのストレージ容量を追加購入した場合は、ライセンス情報を更新する必要があります。

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があります。
- ["特定のアクセス権限"](#)があります。
- プロビジョニングパスフレーズをお持ちです。

手順

1. **Maintenance > System > License** を選択します。
2. 「ライセンスの更新」セクションで、***参照***を選択します。
3. 新しいライセンスファイルを探して選択します（.txt）。

新しいライセンスファイルが検証され、表示されます。

4. プロビジョニングパスフレーズを入力してください。
5. ***保存***を選択します。

API を使用する

StorageGRID Grid Management APIを使用する

グリッドマネージャ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 を使用して操作を自動化したり、ユーザなどの複数のエンティティをより迅速に作成したりすることができます。

最上位のリソース

グリッド管理APIは、以下のトップレベルリソースを提供します。

- **/grid** : Grid Managerユーザーへのアクセスに限定されており、設定されたグループ権限に基づいています。
- **/org** : アクセスは、テナントアカウントのローカルまたはフェデレーションLDAPグループに属するユーザーに限定されます。詳細については、["テナントアカウントを使用する"](#)を参照してください。
- **/private** : アクセスはGrid Managerユーザーに限定されており、設定されたグループ権限に基づいています。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、リクエストのAPIバージョンも無視します。

API リクエストを発行する

グリッド管理APIは、オープンソースAPIプラットフォームであるSwaggerを使用しています。Swaggerは、開発者と非開発者がAPIを使用してStorageGRIDでリアルタイム操作を実行できる直感的なユーザーインターフェースを提供します。

Swagger のユーザーインターフェイスは、各 API 操作に関する完全な詳細情報とドキュメントを提供します。

開始する前に

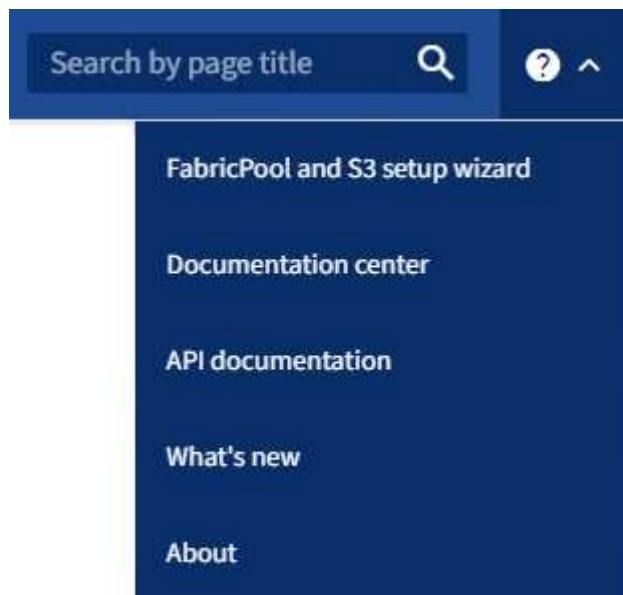
- ["対応ウェブブラウザ"](#) を使用して Grid Manager にサインインしています。
- ["特定のアクセス権限"](#)があります。



APIドキュメントのウェブページを使用して実行するAPI操作はすべて、ライブ操作となります。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. グリッドマネージャーのヘッダーから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 で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、リクエストのAPIバージョンも無視します。

3. 希望する操作を選択してください。

API操作を展開すると、GET、PUT、UPDATE、DELETEなどの利用可能なHTTPアクションが表示されます。

4. HTTPアクションを選択すると、エンドポイントURL、必須またはオプションのパラメーター一覧、リクエストボディの例（必要な場合）、および考えられるレスポンスなど、リクエストの詳細が表示されます。

GET

/grid/groups Lists Grid Administrator Groups

🔒

Parameters

Try it out

Name	Description
type string (query)	filter by group type Available values : local, federated -- ▾
limit integer (query)	maximum number of results Default value : 25 25
marker string (query)	marker-style pagination offset (value is Group's URN) marker - marker-style pagination offset (value
includeMarker boolean (query)	if set, the marker element is also returned -- ▾
order string (query)	pagination order (desc requires marker) Available values : asc, desc -- ▾

Responses

Response content type application/json ▾

Code	Description
200	successfully retrieved Example Value Model <pre>{ "responseTime": "2021-03-29T14:22:19.673Z", "status": "success", "apiVersion": "3.3", "deprecated": false, "data": [{ "displayName": "Developers",</pre>

- リクエストにグループIDやユーザーIDなどの追加パラメータが必要かどうかを判断します。次に、これらの値を取得します。必要な情報を取得するには、まず別のAPIリクエストを発行する必要がある場合があります。
- サンプルリクエストボディを修正する必要があるかどうかを判断してください。必要な場合は、*モデル*を選択して各フィールドの要件を確認できます。
- 「Try it out」を選択します。
- 必要なパラメータを指定するか、必要に応じてリクエスト本文を変更してください。
- 「実行」を選択します。
- リクエストが成功したかどうかを判断するには、レスポンスコードを確認してください。

グリッド管理APIは、利用可能な操作を以下のセクションに分類しています。



このリストには、公開APIで利用可能な操作のみが含まれています。

- **アカウント**：ストレージテナントアカウントを管理するための操作。これには、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が含まれます。
- **alert-history**：解決済みのアラートに対する操作。
- **alert-receivers**：アラート通知受信者（電子メール）に対する操作。
- **alert-rules**：アラートルールに対する操作。
- **alert-silences**：アラートのサイレンスに対する操作。
- **アラート**：アラートに対する操作。
- **監査**：監査設定を一覧表示および更新する操作。
- **auth**：ユーザーセッション認証を実行するための操作。

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、認証リクエストの JSON ボディにユーザー名とパスワードを指定します（つまり、POST /api/v3/authorize）。ユーザー認証が成功すると、セキュリティトークンが返されます。このトークンは、以降のAPIリクエストのヘッダーに含めて指定する必要があります（「Authorization: Bearer *token*」）。トークンは16時間後に期限切れになります。



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、認証のために異なる手順を実行する必要があります。「シングル サインオンが有効な場合のAPIへの認証」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。

- **クライアント証明書**：クライアント証明書を設定して、外部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するための操作。
- **config**：Grid Management API の製品リリースおよびバージョンに関連する操作。製品のリリースバージョンと、そのリリースでサポートされている Grid Management API のメジャーバージョンを一覧表示したり、非推奨バージョンの API を無効にしたりできます。
- **deactivated-features**：無効化された可能性のある機能を表示するための操作。
- **dns-servers**：設定済みの外部 DNS サーバーを一覧表示および変更する操作。
- **drive-details**：特定のストレージアプライアンスモデルのドライブに対する操作。
- **endpoint-domain-names**：S3エンドポイント ドメイン名をリスト表示および変更する操作。
- **erasure-coding**：消去符号化プロファイルに対する操作。
- **展開**：展開に対する操作（プロセスレベル）。
- **expansion-nodes**：展開に関する操作（ノードレベル）。
- **expansion-sites**：拡張に関する作業（サイトレベル）。

- **grid-networks**：グリッドネットワークリストを一覧表示および変更する操作。
- **grid-passwords**：グリッドパスワード管理のための操作。
- **グループ**：ローカルのグリッド管理者グループを管理し、外部LDAPサーバからフェデレーションされたグリッド管理者グループを取得する操作。
- **identity-source**：外部IDソースを設定し、フェデレーションされたグループとユーザー情報を手動で同期するための操作。
- **ilm**：情報ライフサイクル管理（ILM）に対する操作。
- **in-progress-procedures**：現在進行中のメンテナンス手順を取得します。
- **ライセンス**：StorageGRID ライセンスを取得および更新するための操作。
- **logs**：ログファイルの収集とダウンロードの操作。v
- **メトリクス**：StorageGRIDメトリクスに対する操作には、ある時点における即時メトリクスクエリと、一定期間にわたる範囲メトリクスクエリが含まれます。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クエリの構築方法については、PrometheusのWebサイトを参照してください。



名前に`private`が含まれる指標は、内部使用のみを目的としています。これらの指標は、予告なしに StorageGRID リリース間で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操作。
- **node-health**：ノードの健全性状態に関する操作。
- **node-storage-state**：ノードストレージの状態に関する操作。
- **ntp-servers**：外部ネットワークタイムプロトコル（NTP）サーバーを一覧表示または更新する操作。
- **オブジェクト**：オブジェクトおよびオブジェクトメタデータに対する操作。
- **リカバリ**：リカバリ手順のための操作。
- **recovery-package**：リカバリパッケージをダウンロードするための操作。
- **regions**：リージョンを表示および作成するための操作。
- **s3-object-lock**：グローバル S3 オブジェクト ロック設定に対する操作。
- **server-certificate**：Grid Managerサーバー証明書を表示および更新する操作。
- **snmp**：現在のSNMP設定に対する操作。
- **storage-watermarks**：ストレージノードのウォーターマーク。
- **traffic-classes**：トラフィック分類ポリシーの操作。
- **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操作。
- **users**：Grid Managerユーザーを表示および管理するための操作。

StorageGRID におけるグリッド管理 API のバージョン管理

グリッド管理APIは、バージョン管理を利用して、システムへの影響を最小限に抑えたアップグレードをサポートします。

例えば、このリクエスト URL はAPI のバージョン 4 を指定しています。

`https://hostname_or_ip_address/api/v4/authorize`

APIのメジャーバージョンは、古いバージョンと互換性のない変更が行われた場合、更新されます。APIのマイナーバージョンは、古いバージョンと互換性のある変更が行われた場合、更新されます。互換性のある変更には、新しいエンドポイントまたは新しいプロパティの追加が含まれます。

以下の例は、行われた変更の種類に基づいて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に対する変更の種類	旧バージョン	新バージョン
旧バージョンとの互換性あり	2.1	2.2
旧バージョンとの互換性はありません	2.1	3.0

StorageGRID ソフトウェアを初めてインストールする場合、最新バージョンのAPIのみが有効になります。ただし、StorageGRID の新しい機能リリースにアップグレードした場合でも、少なくとも1つのStorageGRID 機能リリースの間は、古いAPIバージョンに引き続きアクセスできます。



対応バージョンを設定できます。詳細については、"[グリッド管理API](#)"のSwagger API 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API クライアントを新しいバージョンに更新した後、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。

古いリクエストは、以下の方法で非推奨としてマークされます。

- レスポンスヘッダーは「Deprecated: true」です。
- JSON レスポンスボディには「deprecated」 : true が含まれています
- 非推奨の警告がnms.logに追加されます。例：

```
Received call to deprecated v2 API at POST "/api/v2/authorize"
```

現在のリリースでサポートされているAPIバージョンを確認する

```
`GET /versions`API リクエストを使用して、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します。このリクエストは、Swagger API ドキュメントの  
*config* セクションに記載されています。
```



```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2023-06-27T22:13:50.750Z",
  "status": "success",
  "apiVersion": "4.0",
  "data": [
    2,
    3,
    4
  ]
}
```

リクエストの**APIバージョン**を指定します

パスパラメータ (`/api/v4`) またはヘッダー (`Api-Version: 4`) を使用して API バージョンを指定できます。両方の値を指定した場合、ヘッダーの値がパスの値を上書きします。

```
curl https://[IP-Address]/api/v4/grid/accounts

curl -H "Api-Version: 4" https://[IP-Address]/api/grid/accounts
```

StorageGRID でクロスサイトリクエストフォージェリ (**CSRF**) から保護する

CSRF トークンを使用して Cookie を使用する認証を強化することで、StorageGRID に対するクロスサイトリクエストフォージェリ (CSRF) 攻撃からの保護に役立てることができます。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。その他の API クライアントは、サインイン時に有効にするかどうかを選択できます。

別のサイトへのリクエスト (HTTP フォーム POST など) をトリガーできる攻撃者は、ログインしているユーザーの Cookie を使用して特定のリクエストを実行させることができます。

StorageGRID は、CSRF トークンを使用することで、CSRF 攻撃に対する保護に役立ちます。有効にした場合、特定のクッキーの内容は、特定のヘッダーまたは特定の POST ボディ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、認証中に ``csrfToken`` パラメータを ``true`` に設定します。デフォルトは ``false`` です。

```
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、GridCsrfToken クッキーには Grid Manager へのサインイン用のランダムな値が設定され、AccountCsrfToken クッキーには Tenant Manager へのサインイン用のランダムな値が設定されます。

Cookieが存在する場合、システムの状態を変更できるすべてのリクエスト（POST、PUT、PATCH、DELETE）には、以下のいずれかを含める必要があります。

- `X-Csrf-Token` ヘッダー。ヘッダーの値は、CSRF トークンクッキーの値に設定されます。
- フォームエンコードされたボディを受け入れるエンドポイントの場合：A `csrfToken` フォームエンコードされたリクエストボディパラメータ。

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



CSRF トークン Cookie が設定されているリクエストは、CSRF 攻撃に対する追加の保護として、JSON リクエストボディを想定するすべてのリクエストに対して「Content-Type: application/json」ヘッダーを強制的に適用します。

シングル サインオンが有効な場合のAPIの使用

StorageGRID API を使用する場合、**Single Sign-On** が有効になっている（**Active Directory**）

"**設定および有効化されたシングル サインオン (SSO)**" を使用しており、Active Directory を SSO プロバイダーとして使用している場合は、Grid Management API または Tenant Management API で有効な認証トークンを取得するために、一連の API リクエストを発行する必要があります。

シングル サインオンが有効になっている場合に**API**にサインインする

これらの手順は、SSOのIDプロバイダーとしてActive Directoryを使用している場合に適用されます。

開始する前に

- StorageGRID ユーザーグループに属するフェデレーションユーザーの SSO ユーザー名とパスワードを把握しています。
- テナント管理APIにアクセスするには、テナントアカウントIDを知っている必要があります。

タスク概要

認証トークンを取得するには、以下のいずれかの例を使用できます。

- `storagegrid-ssoauth.py` Python スクリプトは、StorageGRID インストールファイルディレクトリ（`./rpms` RHEL の場合、`./debs` Ubuntu または Debian の場合、`./vsphere` VMware の場合）にあ

ります。

- curlリクエストのワークフロー例。

curlワークフローは、実行速度が遅すぎるとタイムアウトする可能性があります。次のような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。



この例のcurlワークフローでは、パスワードが他のユーザーに見られるのを防ぐことはできません。

URLエンコードに問題がある場合、次のような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、以下のいずれかの方法を選択してください。
 - `storagegrid-ssoauth.py` Python スクリプトを使用します。ステップ 2 に進みます。
 - curl リクエストを使用します。ステップ 3 に進みます。
2. `storagegrid-ssoauth.py` スクリプトを使用する場合は、Python インタープリタにスクリプトを渡して実行してください。

指示が表示されたら、以下の引数に値を入力してください。

- SSO方式。ADFS または adfs と入力してください。
- 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が必要です。

```
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含まれています。これで、SSO を使用していない場合と同様に、トークンを他のリクエストに使用できます。

3. curlリクエストを使用する場合は、以下の手順に従ってください。
 - a. ログ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、0を`TENANTACCOUNTID`として使用します。

- b. 署名付き認証URLを受け取るには、`/api/v3/authorize-saml`にPOSTリクエストを発行し、レスポンスから余分なJSONエンコーディングを削除します。

この例は、`TENANTACCOUNTID`の署名付き認証 URL に対する POST リクエストを示しています。結果は`python -m json.tool`に渡され、JSON エンコーディングが削除されます。

```
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
```

この例に対する応答には、URLエンコードされた署名付きURLが含まれていますが、追加のJSONエンコード層は含まれていません。

```
{
  "apiVersion": "3.0",
  "data":
  "https://adfs.example.com/adfs/ls/?SAMLRequest=fZHLbsIwEEV%2FJTuv7...
sS1%2BfQ33cvfwA%3D&RelayState=12345",
  "responseTime": "2018-11-06T16:30:23.355Z",
  "status": "success"
}
```

- c. 応答から取得した`SAMLRequest`を、後続のコマンドで使用するために保存します。

```
export SAMLREQUEST='fZHLbsIwEEV%2FJTuv7...sS1%2BfQ33cvfwA%3D'
```

- d. AD FSからクライアントリクエストIDを含む完全なURLを取得します。

一つの方法として、前回のレスポンスのURLを使用してログインフォームをリクエストする方法があります。

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

レスポンスにはクライアントリクエスト ID が含まれます：

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

e. レスポンスからクライアントリクエストIDを保存します。

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

f. 前回のレスポンスで指定したフォームアクションに認証情報を送信してください。

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

AD FSは、ヘッダーに追加情報を含めた302リダイレクトを返します。



SSOシステムで多要素認証（MFA）が有効になっている場合、フォーム送信には2つ目のパスワードまたはその他の認証情報も含まれます。

```
HTTP/1.1 302 Found
Content-Length: 0
Content-Type: text/html; charset=utf-8
Location:
https://adfs.example.com/adfs/ls/?SAMLRequest=fZHRTomwFIZfhh...UJikvo77sXPw%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. レスポンスから `MSISAuth` クッキーを保存します。

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

- h. 認証POSTリクエストから取得したCookieを使用して、指定された場所にGETリクエストを送信します。

```
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、後のログアウト時に使用するための AD FS セッション情報が含まれ、応答本文には非表示のフォームフィールドに SAMLResponse が含まれます。

```
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
XfxVWx3bk1lMnFuUSUzZCUzZCYmJiYmXzE3MjAyZTA5LThtMDgtNDRkZC04Yzg5LTQ3ND
UxYzA3ZjkzYw==; path=/adfs; HttpOnly; Secure
Set-Cookie: MSISAuthenticated=MTEvNy8yMDE4IDQ6MzI6NTkgUE0=;
path=/adfs; HttpOnly; Secure
Set-Cookie: MSISLoopDetectionCookie=MjAxOC0xMS0wNzoxNjozMj0lOVpcMQ==;
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. 非表示フィールドから `SAMLResponse` を保存します：

```
export SAMLResponse='PHNhbWxwOlJlc3Bvb3N...1scDpSZXNwb25zZT4='
```

- j. 保存した `SAMLResponse` を使用して、StorageGRID/api/saml-response リクエストを作成し、StorageGRID 認証トークンを生成します。

`RelayState` には、テナントアカウントIDを使用するか、Grid Management APIにサインインする場合は0を使用してください。

```
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
```

レスポンス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. レスポンス内の認証トークンを `MYTOKEN` として保存します。

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

これで、SSO を使用しない場合と同様に、`MYTOKEN` を他のリクエストに使用できます。

シングル サインオンが有効になっている場合に**API**からサインアウトする

シングル サインオン (SSO) が有効になっている場合は、Grid Management API または Tenant Management API からサインアウトするために、一連の API リクエストを発行する必要があります。これらの手順は、SSO の ID プロバイダーとして Active Directory を使用している場合に適用されます。

タスク概要

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) をトリガーすることもできます。その場合、有効な StorageGRID ベアラートークンが必要です。

手順

1. 署名付きログアウトリクエストを生成するには、cookie "sso=true" を SLO API に渡します。

```
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
```

ログアウト用のURLが返されます：

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

2. ログアウトURLを保存してください。

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

3. ログアウト URL にリクエストを送信して SLO をトリガーし、StorageGRID にリダイレクトします。

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

302レスポンスが返されます。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 ベアラートークンを削除します。

StorageGRID ベアラートークンの削除は、SSO を使用しない場合と同じように機能します。`cookie "sso=true" が指定されていない場合、ユーザーは SSO の状態に影響を与えることなく 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` 応答は、ユーザーがサインアウトしたことを示します。

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

シングルサインオンが有効になっている場合は **StorageGRID API** を使用します (**Entra ID**)

"**設定および有効化されたシングルサインオン (SSO)**"をお持ちで、Entra ID をSSOプロバイダー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、Grid Management APIまたはTenant Management APIで有効な認証トークンを取得できます。

Entra ID のシングルサインオンが有効になっている場合は、**API** にサインインします

これらの手順は、SSOのIDプロバイダーとしてEntra IDを使用している場合に適用されます。

開始する前に

- StorageGRID ユーザーグループに属するフェデレーションユーザーの SSO メールアドレスとパスワードを知っている必要があります。
- テナント管理APIにアクセスするには、テナントアカウントIDを知っている必要があります。

タスク概要

認証トークンを取得するには、以下のサンプルスクリプトを使用できます。

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

両方のスクリプトは、StorageGRID インストールファイルディレクトリ (`./rpms` は RHEL の場合、`./debs` は Ubuntu または Debian の場合、`./vsphere` は VMware の場合) にあります。

Entra ID との独自の API 統合を作成するには、`storagegrid-ssoauth-azure.py` スクリプトを参照してください。Python スクリプトは StorageGRID に対して直接 2 つのリクエストを行い (最初に `SAMLRequest` を取得し、その後認証トークンを取得します)、さらに Node.js スクリプトを呼び出して Entra ID とやり取りし、SSO 操作を実行します。

SSO操作は一連のAPIリクエストを使用して実行できますが、その方法は簡単ではありません。Puppeteer Node.jsモジュールは、Entra ID SSOインターフェースのスクレイピングに使用されます。

URLエンコードに問題がある場合、次のようなエラーが表示されることがあります: `Unsupported SAML version`。

手順

1. 必要な依存関係を以下の手順でインストールします：
 - a. Node.jsをインストールします（"<https://nodejs.org/en/download/>"を参照）。
 - b. 必要なNode.jsモジュール（puppeteerとjsdom）をインストールします：

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

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

次に、Pythonスクリプトが対応するNode.jsスクリプトを呼び出し、Entra ID SSOのやり取りを実行します。

3. プロンプトが表示されたら、以下の引数に値を入力してください（または、パラメータを使用して渡してください）：
 - Entra ID へのサインインに使用される SSO 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. 指示が表示されたらパスワードを入力し、必要に応じて Entra ID への MFA 認証を提供する準備をしてください。

```
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'}
```



このスクリプトは、多要素認証（MFA）がMicrosoft Authenticatorを使用して行われることを前提としています。他の形式の多要素認証（テキストメッセージで受信したコードを入力するなど）をサポートするには、スクリプトを修正する必要がある場合があります。

StorageGRID 認証トークンが出力に含まれています。これで、SSO を使用していない場合と同様に、トークンを他のリクエストに使用できます。

シングル サインオンが有効になっている場合は **StorageGRID API** を使用します（**PingFederate**）

"**設定および有効化されたシングル サインオン（SSO）**"を使用しており、SSOプロバイダーとしてPingFederateを使用している場合は、Grid Management APIまたはTenant Management APIで有効な認証トークンを取得するために、一連のAPIリクエストを発行する必要があります。

シングル サインオンが有効になっている場合に**API**にサインインする

これらの手順は、SSOのIDプロバイダーとしてPingFederateを使用している場合に適用されます

開始する前に

- StorageGRID ユーザーグループに属するフェデレーションユーザーの SSO ユーザー名とパスワードを把握しています。

- テナント管理APIにアクセスするには、テナントアカウントIDを知っている必要があります。

タスク概要

認証トークンを取得するには、以下のいずれかの例を使用できます。

- `storagegrid-ssoauth.py` Python スクリプトは、StorageGRID インストールファイルディレクトリ（`./rpms` RHEL の場合、`./debs` Ubuntu または Debian の場合、`./vsphere` VMware の場合）にあります。
- `curl` リクエストのワークフロー例。

`curl` ワークフローは、実行速度が遅すぎるとタイムアウトする可能性があります。次のような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。



この例の`curl`ワークフローでは、パスワードが他のユーザーに見られるのを防ぐことはできません。

URLエンコードに問題がある場合、次のような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、以下のいずれかの方法を選択してください。
 - `storagegrid-ssoauth.py` Python スクリプトを使用します。ステップ 2 に進みます。
 - `curl` リクエストを使用します。ステップ 3 に進みます。
2. `storagegrid-ssoauth.py` スクリプトを使用する場合は、Python インタープリタにスクリプトを渡して実行してください。

指示が表示されたら、以下の引数に値を入力してください。

- SSO方式。「pingfederate」の任意のバリエーション（PINGFEDERATE、pingfederateなど）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 では使用されません。空欄のままでも、任意の値を入力しても構いません。
- 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が必要です。

```
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含まれています。これで、SSO を使用していない場合と同様に、トークンを他のリクエストに使用できます。

3. curlリクエストを使用する場合は、以下の手順に従ってください。

a. ログ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、0を`TENANTACCOUNTID`として使用します。

b. 署名付き認証URLを受け取るには、`/api/v3/authorize-saml`にPOSTリクエストを発行し、レスポンスから余分なJSONエンコーディングを削除します。

この例は、TENANTACCOUNTID の署名付き認証 URL に対する POST リクエストを示しています。結果は、JSON エンコーディングを削除するために `python -m json.tool` に渡されます。

```
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
```

この例に対する応答には、URLエンコードされた署名付きURLが含まれていますが、追加のJSONエンコード層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. 応答から取得した `SAMLRequest` を、後続のコマンドで使用するために保存します。

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

- d. レスポンスとクッキーをエクスポートし、レスポンスを出力します。

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

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

- e. 'pf.adapterId' の値をエクスポートし、レスポンスをエコーします：

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

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

- f. 「href」 の値をエクスポートし（末尾のスラッシュ / を削除）、レスポンスを出力します：

```
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. 認証情報とともにクッキーを送信する：

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

- i. 非表示フィールドから `SAMLResponse` を保存します：

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

- j. 保存した `SAMLResponse` を使用して、StorageGRID/api/saml-response リクエストを作成し、StorageGRID 認証トークンを生成します。

`RelayState` には、テナントアカウントIDを使用するか、Grid Management APIにサインインする場合は0を使用してください。

```
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
```

レスポンス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. レスポンス内の認証トークンを `MYTOKEN` として保存します。

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

これで、SSO を使用しない場合と同様に、`MYTOKEN` を他のリクエストに使用できます。

シングル サインオンが有効になっている場合にAPIからサインアウトする

シングル サインオン (SSO) が有効になっている場合は、Grid Management APIまたはTenant Management APIからサインアウトするために、一連のAPIリクエストを発行する必要があります。これらの手順は、SSO

のIDプロバイダーとしてPingFederateを使用している場合に適用されます。

タスク概要

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) をトリガーすることもできます。その場合、有効な StorageGRID ベアラートークンが必要です。

手順

1. 署名付きログアウトリクエストを生成するには、cookie "sso=true" を SLO API に渡します。

```
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
```

ログアウト用の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を保存してください。

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

3. ログアウト URL にリクエストを送信して SLO をトリガーし、StorageGRID にリダイレクトします。

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

302レスポンスが返されます。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 ベアラートークンを削除します。

StorageGRID ベアラートークンの削除は、SSO を使用しない場合と同じように機能します。`cookie "sso=true" が指定されていない場合、ユーザーは SSO の状態に影響を与えることなく 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` 応答は、ユーザーがサインアウトしたことを示します。

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

API を使用して StorageGRID 機能を無効化する

Grid Management API を使用すると、StorageGRID システムの特定の機能を完全に無効にできます。機能が無効化されると、その機能に関連するタスクを実行するための権限を誰にも割り当てることができなくなります。

タスク概要

無効化された機能システムを使用すると、StorageGRID システム内の特定の機能へのアクセスを防止できます。機能を無効化することは、ルートユーザー、または **Root access** 権限を持つ管理者グループに属するユーザー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、次のシナリオを考えてみましょう。

A社は、テナントアカウントを作成することで自社の 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ーです。A社は、賃借人のオブジェクトのセキュリティを保護するため、アカウントが展開された後、自社の従業員がテナントアカウントに一切アクセスできないようにしたいと考えています。

A社は、グリッド管理APIの「機能無効化」システムを使用することで、この目標を達成できます。Grid Manager (UIとAPIの両方) で「テナントルートパスワードの変更」機能を完全に無効化することで、A社は、管理者ユーザー（ルートユーザーおよび「ルートアクセス」権限を持つグループに属するユーザーを含む）が、どのテナントアカウントのルートユーザーのパスワードも変更できないようにしています。

手順

1. グリッド管理APIのSwaggerドキュメントにアクセスしてください。["グリッド管理APIを使用する"](#)を参照してください。
2. 機能無効化エンドポイントを探してください。
3. テナントのルートパスワードの変更などの機能を無効にするには、次のような本文を API に送信します。

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

リクエストが完了すると、「テナントのルートパスワードを変更する」機能は無効になります。「テナン

トのルートパスワードの変更」管理権限はユーザーインターフェースに表示されなくなり、テナントのルートパスワードを変更しようとする API リクエストはすべて「403 Forbidden」で失敗します。

無効化された機能を再有効化する

デフォルトでは、グリッド管理APIを使用して、無効化された機能を再度有効化できます。ただし、無効化した機能が二度と有効化されないようにするには、**activateFeatures** 機能そのものを無効化できます。



activateFeatures 機能は再有効化できません。この機能を無効化すると、無効化された他の機能を再有効化する機能が永久に失われることにご注意ください。失われた機能を復元するには、テクニカルサポートにお問い合わせください。

手順

1. グリッド管理APIのSwaggerドキュメントにアクセスします。
2. 機能無効化エンドポイントを探してください。
3. すべての機能を再度有効にするには、次のような本文をAPIに送信してください：

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

このリクエストが完了すると、テナントのルートパスワード変更機能を含むすべての機能が再有効化されます。テナントのルートパスワードの変更 管理権限がユーザーインターフェースに表示されるようになり、ユーザーが ルートアクセス または テナントのルートパスワードの変更 管理権限を持っている場合、テナントのルートパスワードを変更しようとするすべての API リクエストは成功します。



上記の例では、無効化されていたすべての機能が再有効化されます。無効化された機能のうち、無効化されたままにしておくべき機能がある場合は、PUT リクエストでそれらを明示的に指定する必要があります。例えば、テナントルートパスワードの変更機能を再有効化し、storageAdmin 管理権限を引き続き無効化するには、次の PUT リクエストを送信してください：
+ { "grid": { "storageAdmin": true } }

StorageGRID へのアクセスを制御する

StorageGRID アクセスの制御

グループとユーザー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ることで、StorageGRID へのアクセスを許可するユーザーと、ユーザーが実行できるタスクを制御できます。オプションで、シングル サインオン（SSO）の有効化、クライアント証明書の作成、およびグリッドパスワードの変更を行うことができます。

グリッドマネージャーへのアクセスを制御する

Grid ManagerおよびGrid Management APIへのアクセス権限を持つユーザーは、IDフェデレーションサービスからグループとユーザーをインポートするか、ローカルグループとローカルユーザーを設定することで決定します。

"アイデンティティフェデレーション"を使用すると、"groups"および"ユーザ"のセットアップが迅速になり、ユーザーは使い慣れた認証情報を使用して StorageGRID にサインインできるようになります。Active

Directory、OpenLDAP、または Oracle Directory Server を使用している場合は、ID フェデレーションを設定できます。



別のLDAP v3サービスを利用したい場合は、テクニカルサポートにお問い合わせください。

各ユーザーが実行できるタスクは、各グループに異なる**"権限"**を割り当てることで決定します。例えば、あるグループのユーザーには ILM ルールを管理させ、別のグループのユーザーにはメンテナンス作業を実行させたい場合があるでしょう。ユーザーがシステムにアクセスするには、少なくとも 1 つのグループに所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を設定することもできます。読み取り専用グループに属するユーザーは、設定と機能のみを閲覧できます。Grid Manager または Grid Management API では、変更や操作を行うことはできません。

シングル サインオンを有効にする

StorageGRID システムは、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) をサポートしています。**"SSOの設定と有効化"**後、すべてのユーザーは、Grid Manager、Tenant Manager、Grid Management API、または Tenant Management API にアクセスする前に、外部の ID プロバイダーによる認証が必要です。ローカルユーザーは 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の変更

プロビジョニングパスフレーズは、多くのインストールおよびメンテナンス手順と、StorageGRID リカバリパッケージのダウンロードに必要です。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場合にも、パスフレーズが必要です。必要に応じて**"パスフレーズを変更する"**できます。

ノードコンソールのパスワードを変更する

グリッド内の各ノードにはノードコンソールパスワードがあり、SSHを使用して「admin」としてノードにログインするか、VM/物理コンソール接続でrootユーザーとしてログインするには、このパスワードが必要です。必要に応じて、各ノードの**"ノードコンソールのパスワードを変更する"**ことができます。

StorageGRID プロビジョニング パスフレーズを変更する

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に必要です。グリッドトポロジ情報、グリッドノードコンソールパスワード、および StorageGRID システムの暗号化キーを含むリカバリパッケージバックアップをダウンロードするには、パスフレーズも必要です。

開始する前に

- **"対応ウェブブラウザ"** を使用して Grid Manager にサインインしています。
- メンテナンス権限またはルートアクセス権限をお持ちです。
- 現在のプロビジョニングパスフレーズを持っています。

タスク概要

プロビジョニングパスフレーズは、多くのインストールおよびメンテナンス手順と**"リカバリパッケージをダ"**

ダウンロードしています"に必要です。プロビジョニングパスフレーズは `Passwords.txt` ファイルには記載されていません。プロビジョニングパスフレーズは必ず記録し、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 > グリッドパスワード を選択します。
2. *プロビジョニングパスフレーズの変更*で、*変更する*を選択します。
3. 現在使用しているプロビジョニングパスフレーズを入力してください。
4. 新しいパスフレーズを入力してください。パスフレーズは8文字以上32文字以下でなければなりません。パスフレーズは大文字と小文字を区別します。



プロビジョニングパスフレーズは安全な場所に保管してください。これは、インストール、拡張、およびメンテナンスの手順に必要です。

5. 新しいパスフレーズを再入力し、**Save** 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、システムは緑色の成功バナーを表示します。



Provisioning passphrase successfully changed. Go to the [Recovery Package](#) to download a new Recovery Package.

6. 「Recovery Package」を選択します。
7. 新しいプロビジョニングパスフレーズを入力して、新しい復旧パッケージをダウンロードしてください。



プロビジョニングパスフレーズを変更した後は、直ち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を使用すると、障害が発生した場合にシステムを復元できます。

StorageGRIDでノードコンソールのパスワードを変更する

グリッド内の各ノードにはノードコンソールパスワードがあり、それを使ってノードにログインします。デフォルトでは、各ノードには固有のパスワードが設定されています。各パスワードを新しい固有のパスワードに変更することも、すべてのノードのパスワードをグローバルパスワードに変更することもできます。パスワードは復旧パッケージに保存されています。

開始する前に

- "対応ウェブブラウザ" を使用して Grid Manager にサインインしています。
- あなたは"メンテナンス権限またはルートアクセス権限"があります。
- 現在のプロビジョニングパスフレーズを持っています。

タスク概要

SSHを使用してノードに「admin」としてログインする場合、またはVM/物理コンソール接続でrootユーザーとしてログインする場合は、ノードコンソールのパスワードを使用します。ノードコンソールのパスワードは、以下のいずれかの方法で変更できます。

- 各ノードにランダムなパスワードを自動的に適用する

- すべてのノードに1つのグローバルパスワードを指定して適用する
- 1つまたは複数のノードに固有のパスワードを指定して適用する

パスワードは、リカバリパッケージ内の更新された `Passwords.txt` ファイルに保存されます。パスワードはファイルの「パスワード」列に記載されています。



ノード間の通信に使用されるSSHキーの"SSHアクセスパスワード"は、ノードコンソールのパスワードとは別のものです。この手順では、SSHアクセスパスワードは変更されません。

ウィザードにアクセスする

手順

1. 設定 > アクセス制御 > グリッドパスワード を選択します。
2. ノードコンソールのパスワードを変更する の下で、変更する を選択します。

最新のリカバリパッケージをダウンロード

ノードコンソールのパスワードを変更する前に、最新の復旧パッケージをダウンロードしてください。いずれかのノードでパスワード変更プロセスが失敗した場合は、このファイルに記載されているパスワードを使用できます。

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てください。
2. 「リカバリパッケージをダウンロード」を選択します。
3. リカバリパッケージファイル（(.zip)）を、安全で保護された2つの別々の場所にコピーしてください。



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に使用できる暗号化キーとパスワードが含まれているため、保護する必要があります。

4. *続行*を選択します。

新しいパスワードを入力してください

1. 使用したいパスワード変更方法を選択してください。
 - 自動：StorageGRID はすべてのノードに新しいランダムなコンソールパスワードを自動的に割り当てます。
 - カスタム：コンソールパスワードを指定します。

自動

1. *続行*を選択します。

Custom

1. 次のいずれかを選択します。
 - グローバルコンソールパスワード：すべてのノードに同じコンソールパスワードを適用します。
 - 固有のコンソールパスワード：1つまたは複数のノードに異なるパスワードを適用します。
2. **Global console password** を選択した場合は、すべてのノードで使用するパスワードを入力してください。
3. *固有のコンソールパスワード*を選択した場合は、1つ以上のノードに対して固有のパスワードを入力してください。
4. *続行*を選択します。

パスワードの変更を完了してください

1. 確認ダイアログが表示されたら、StorageGRID が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、**Yes** を選択してください。



この処理は開始後にキャンセルすることはできません。

StorageGRID は、新しいパスワードを含む新しいリカバリパッケージを生成します。

2. 新しいリカバリパッケージの準備ができたなら、*新しいリカバリパッケージをダウンロード*を選択して、リカバリパッケージを保存します。
3. *.zip* ファイルを開きます。
4. コンテンツにアクセスできることを確認してください。これには、新しいノードコンソールのパスワードを含む `Passwords.txt` ファイルも含まれます。
5. 新しいリカバリパッケージファイル (`.zip`) を、安全で保護された2つの別々の場所にコピーしてください。



古いリカバリパッケージを上書きしないでください。

リカバリファイルには暗号化キーとパスワードが含まれており、StorageGRID システムからデータを取得するために使用される可能性があるため、安全に保管する必要があります。

6. 新しいリカバリパッケージをダウンロードし、内容を確認したことを示すチェックボックスを選択してください。
7. *続行*を選択します。

StorageGRID は各ノードのパスワードを更新します。

更新処理中にエラーが発生した場合、進行状況バーにはパスワード変更失敗したノードの数が表示されます。パスワード変更失敗したノードについては、システムが自動的に処理を再試行します。処理が完了しても、一部のノードのパスワードが変更されていない場合は、**Retry** ボタンが表示されます。

8. 1つ以上のノードでパスワードの更新が失敗した場合：
 - a. 表に記載されているエラーメッセージを確認してください。
 - b. 問題を解決してください。
 - c. 「再試行」を選択します。



再試行すると、以前のパスワード変更試行で失敗したノードのノードコンソールパスワードのみが変更されます。

9. 進行状況バーに更新が残っていないことが示されたら、*完了*を選択してください。
10. すべてのノードのノードコンソールパスワードが変更されたら、[ダウンロードした最初のリカバリパッケージ](#)を削除します。

StorageGRID 管理ノードの SSH アクセス パスワードを変更する

管理ノードのSSHアクセスパスワードを変更すると、グリッド内の各ノード固有の内部SSHキーセットも更新されます。プライマリ管理ノードは、これらのSSHキーを使用して、安全なパスワードレス認証でノードにアクセスします。

SSH キーを使用して、`admin`としてノードにログインするか、VM または物理コンソール接続で root ユーザーとしてログインします。

開始する前に

- ["対応ウェブブラウザ"](#)を使用して Grid Manager にサインインしています。
- あなたは["メンテナンス権限またはルートアクセス権限"](#)があります。
- 現在のプロビジョニングパスフレーズを持っています。

タスク概要

管理ノードの新しいアクセスパスワードと各ノードの新しい内部キーは、リカバリパッケージの `Passwords.txt` ファイルに保存されています。キーは、そのファイルの「パスワード」列に記載されています。

ノード間の通信に使用されるSSHキーには、それぞれ個別のSSHアクセスパスワードが設定されています。これらのパスワードは、この手順では変更されません。

ウィザードにアクセスする

手順

1. 設定 > アクセス制御 > グリッドパスワード を選択します。
2. 「SSH キーの変更」で、「変更する」を選択します。

最新のリカバリパッケージをダウンロード

SSHアクセスキーを変更する前に、最新のリカバリパッケージをダウンロードしてください。いずれかのノードでキー変更処理が失敗した場合、このファイル内のキーを使用できます。

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てください。
2. 「リカバリパッケージをダウンロード」を選択します。
3. リカバリパッケージファイル（(.zip)）を、安全で保護された2つの別々の場所にコピーしてください。



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に使用できる暗号化キーとパスワードが含まれているため、保護する必要があります。

4. *続行*を選択します。
5. 確認ダイアログが表示されたら、SSH アクセスキーの変更を開始する準備ができている場合は、**Yes** を選択してください。



この処理は開始後にキャンセルすることはできません。

SSHアクセスキーを変更する

SSHアクセスキーの変更処理が開始されると、新しいキーを含む新しいリカバリパッケージが生成されます。次に、各ノードでキーが更新されます。

手順

1. 新しい復旧パッケージが生成されるまでお待ちください。数分かかる場合があります。
2. 「新しいリカバリパッケージをダウンロード」ボタンが有効になったら、*新しいリカバリパッケージをダウンロード*を選択し、新しいリカバリパッケージファイル(.zip) を安全で安心できる、別々の2つの場所に保存してください。
3. ダウンロードが完了すると：
 - a. '.zip' ファイルを開きます。
 - b. 新しい SSH アクセスキーを含む 'Passwords.txt' ファイルを含め、コンテンツにアクセスできることを確認してください。
 - c. 新しいリカバリパッケージファイル（(.zip)）を、安全で保護された2つの別々の場所にコピーしてください。



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に使用できる暗号化キーとパスワードが含まれているため、保護する必要があります。

4. 各ノードでキーが更新されるまでお待ちください。数分かかる場合があります。

すべてのノードのキーが変更されると、緑色の成功バナーが表示されます。

更新処理中にエラーが発生した場合、キーの変更に失敗したノードの数を示すバナーメッセージが表示されます。システムは、キーの変更に失敗したノードに対して、自動的に処理を再試行します。処理が終了した時点で、一部のノードのキーが変更されていない場合は、**Retry** ボタンが表示されます。

1つ以上のノードでキーの更新が失敗した場合：

- a. 表に記載されているエラーメッセージを確認してください。
- b. 問題を解決してください。
- c. 「再試行」を選択します。

再試行すると、以前のキー変更試行で失敗したノード上の SSH アクセスキーのみが変更されます。

5. すべてのノードの SSH アクセスキーが変更されたら、[ダウンロードした最初のリカバリパッケージ](#)を削除します。
6. 必要に応じて、**Maintenance > System > Recovery package** を選択して、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てください。

StorageGRIDでIDフェデレーションを使用する

IDフェデレーションを使用すると、グループとユーザーの設定が速くなり、ユーザーは使い慣れた認証情報を使用してStorageGRIDにサインインできるようになります。

Grid Manager の ID フェデレーションを設定する

Active Directory、Microsoft Entra ID、OpenLDAP、Oracle Directory Serverなどの別のシステムで管理者グループやユーザーを管理したい場合は、Grid ManagerでIDフェデレーションを設定できます。

開始する前に

- Grid Managerに["対応ウェブブラウザ"](#)を使用してサインインしています。
- あなたは["特定のアクセス権限"](#)。
- お客様は、IDプロバイダーとしてActive Directory、Microsoft Entra ID、OpenLDAP、またはOracle Directory Serverを使用しています。



リストに記載されていないLDAP v3サービスを利用したい場合は、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。[OpenLDAPサーバの設定に関するガイドライン](#)を参照してください。
- シングル サインオン（SSO）を有効にする予定がある場合は、["シングル サインオンの要件と考慮事項"](#)を確認済みです。
- LDAPサーバとの通信にTransport Layer Security（TLS）を使用する予定がある場合、アイデンティティプロバイダーはTLS 1.2または1.3を使用しています。["送信TLS接続でサポートされている暗号スイート"](#)を参照してください。

タスク概要

Active Directory、Microsoft Entra ID、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IDソースを設定できます。以下の種類のグループをインポートできます。

- 管理者グループ。管理者グループに属するユーザーは、グループに割り当てられた管理権限に基づいて、グリッドマネージャーにサインインしてタスクを実行できます。
- 独自のIDソースを使用しないテナント向けのテナントユーザーグループ。テナントグループに属するユーザーは、テナントマネージャーにサインインし、テナントマネージャー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できます。詳細については、["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。

設定を入力してください

手順

1. 設定 > アクセス制御 > **IDフェデレーション** を選択します。
2. *ID連携を有効にする*を選択します。
3. LDAPサービスタイプのセクションで、設定するLDAPサービスのタイプを選択します。

LDAP service type

Select the type of LDAP service you want to configure.

Active Directory	Entra ID	OpenLDAP	Other

「その他」を選択して、Oracle Directory Serverを使用するLDAPサーバの値を設定します。

4. 「その他」を選択した場合は、LDAP属性セクションの各項目を入力してください。そうでない場合は、次のステップに進んでください。
 - **ユーザー固有名**：LDAPユーザーの固有識別子を含む属性の名前。この属性は sAMAccountName（Active Directory 用）および uid（OpenLDAP用）と同等です。Oracle Directory Server を設定する場合は、`uid`を入力してください。
 - **ユーザーUUID**：LDAPユーザーの永続的な一意の識別子を含む属性の名前。この属性は、Active Directory の場合は objectGUID、OpenLDAP の場合は `entryUUID` と同等です。Oracle Directory Server を設定する場合は、`nsuniqueid`を入力してください。指定した属性に対する各ユーザーの値は、16バイト形式または文字列形式の32桁の16進数である必要があり、ハイフンは無視されます。
 - **グループ固有名**：LDAPグループの固有識別子を含む属性の名前。この属性は、Active Directory の場合は sAMAccountName、OpenLDAP の場合は `cn` と同等です。Oracle Directory Server を設定する場合は、`cn`を入力してください。
 - **グループUUID**：LDAPグループの永続的な一意の識別子を含む属性の名前。この属性は objectGUID（Active Directory 用）および entryUUID（OpenLDAP用）と同等です。Oracle Directory Server を構成する場合は、`nsuniqueid`を入力してください。各グループの指定属性の値は、16バイト形式または文字列形式の32桁の16進数でなければならず、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サーバとネットワーク接続情報を入力してください。
 - **ホスト名**：LDAPサーバの完全修飾ドメイン名（FQDN）またはIPアドレス。
 - **ポート**：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番、LDAPSのデフォルトポートは636番です。ただし、ファイアウォールが正しく設定されていれば、どのポートでも使用できます。

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

Active Directoryの場合、下位レベルのログオン名またはユーザプリンシパル名を指定することもできます。

指定されたユーザーは、グループとユーザーの一覧表示、および以下の属性へのアクセス権限を持っている必要があります：

- 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
 - **Entra ID**： accountEnabled および userPrincipalName
- パスワード：ユーザー名に関連付けられたパスワード。
-  今後パスワードを変更する場合は、このページで更新する必要があります。
- グループベース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。下記の Active Directory の例では、識別名がベース DN（DC=storagegrid,DC=example,DC=com）に対して相対的なすべてのグループをフェデレーショングループとして使用できます。
-  *グループ固有名*の値は、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。
- ユーザーベースDN：ユーザーを検索するLDAPサブツリーの識別名（DN）の完全パス。
-  *ユーザー固有名*の値は、所属する*ユーザーベース DN*内で一意である必要があります。
- バインドユーザー名フォーマット（オプション）：パターンを自動的に判別できない場合に StorageGRID が使用するデフォルトのユーザー名パターンです。
- *バインドユーザー名形式*を指定することを推奨します。これにより、StorageGRIDがサービスアカウントとバインドできない場合でも、ユーザーがサインインできるようになります。

以下のいずれかのパターンを入力してください：

- **UserPrincipalName**パターン（AD および Entra ID）： [USERNAME]@example.com
- 下位レベルのログオン名パターン（ADおよびEntra ID）： example\[USERNAME]
- 識別名パターン： CN=[USERNAME],CN=Users,DC=example,DC=com

[USERNAME] を記載どおりに正確に含めてください。

6. トランスポート層セキュリティ（TLS）セクションで、セキュリティ設定を選択します。

- **STARTTLS**を使用する：STARTTLSを使用してLDAPサーバとの通信を保護します。これはActive Directory、OpenLDAP、またはその他のシステムでは推奨されるオプションですが、Microsoft Entra

IDではサポートされていません。

- **LDAPS**を使用する：LDAPS（LDAP over SSL）オプションはTLSを使用してLDAPサーバへの接続を確立します。Microsoft Entra IDの場合は、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：StorageGRIDシステムとLDAPサーバ間のネットワークトラフィックはセキュリティで保護されません。このオプションは、Microsoft Entra IDではサポートされていません。



Active Directory サーバーがLDAP署名を強制している場合、「TLSを使用しない」オプション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、接続を保護するために使用する証明書を選択してください。

- オペレーティングシステムの**CA**証明書を使用する：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**証明書を使用する：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証明書のテキストボックスに貼り付けてください。

接続をテストして設定を保存する

すべての値を入力した後、設定を保存する前に接続テストを行う必要があります。StorageGRID は、LDAPサーバの接続設定と、指定した場合はバインドユーザー名の形式を確認します。

手順

1. 「接続テスト」を選択します。
2. バインドユーザー名の形式を指定しなかった場合：
 - 接続設定が有効な場合、「接続テスト成功」というメッセージが表示されます。設定を保存するには、***保存***を選択してください。
 - 接続設定が無効な場合、「テスト接続を確立できませんでした」というメッセージが表示されます。「閉じる」を選択します。その後、問題をすべて解決し、再度接続テストを行ってください。
3. バインドユーザー名の形式を指定した場合は、有効なフェデレーションユーザーのユーザー名とパスワードを入力してください。

例えば、ご自身のユーザー名とパスワードを入力してください。ユーザー名には、@ や / などの特殊文字を含めないでください。

Test Connection

To test the connection and the bind username format, enter the username and password of a federated user. For example, enter your own federated username and password. The test values are not saved.

Test username

The username of a federated user.

Test password

[Cancel](#) [Test Connection](#)

- 接続設定が有効な場合、「接続テスト成功」というメッセージが表示されます。設定を保存するには、*保存*を選択してください。
- 接続設定、バインドユーザー名の形式、またはテストユーザー名とパスワードが無効な場合、エラーメッセージが表示されます。問題を解決し、再度接続テストを行ってください。

IDソースとの強制同期

StorageGRID システムは、IDソースから連携グループとユーザーを定期的に同期します。ユーザー権限をできるだけ早く有効化または制限したい場合は、同期を強制的に開始することができます。

手順

1. ID連携ページに移動します。
2. ページ上部の「Sync server」を選択してください。

同期処理には、お使いの環境によっては時間がかかる場合があります。



「IDフェデレーション同期失敗」アラートは、IDソースからのフェデレーショングループとユーザーの同期に問題が発生した場合にトリガーされます。

IDフェデレーションを無効にする

グループおよびユーザーのID連携を、一時的または永続的に無効にすることができます。ID連携が無効になっている場合、StorageGRIDとIDソース間の通信は行われません。ただし、設定した内容はすべて保持されるため、将来的にID連携を簡単に再度有効にすることができます。

タスク概要

IDフェデレーションを無効にする前に、以下の点に注意してください。

- フェデレーションユーザーはサインインできません。
- 現在サインインしているフェデレーションユーザーは、セッションが期限切れになるまでStorageGRIDシステムへのアクセスを維持できますが、セッションが期限切れになるとサインインできなくなります。

- StorageGRID システムとID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関するアラートも発生しません。
- 「ID フェデレーションを有効にする」チェックボックスは、シングル サインオン (SSO) ステータスが「有効」または「サンドボックスモード」の場合は無効になります。ID フェデレーションを無効にするには、まずシングル サインオンページの SSO ステータスを「無効」に設定する必要があります。参照してください["シングル サインオンを無効にする"](#)。

手順

1. ID連携ページに移動します。
2. ID連携を有効にする チェックボックスのチェックを外します。

OpenLDAPサーバの設定に関するガイドライン

IDフェデレーションにOpenLDAPサーバを使用する場合は、OpenLDAPサーバ上で特定の設定を構成する必要があります。



Active Directory または Microsoft Entra ID 以外の ID ソースの場合、StorageGRID は外部から無効化されたユーザーによる S3 へのアクセスを自動的にブロックしません。S3 へのアクセスをブロックするには、ユーザーの S3 キーをすべて削除するか、ユーザーをすべてのグループから削除してください。

memberof および refint オーバーレイ

memberof および 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、<http://www.openldap.org/doc/admin24/index.html>["OpenLDAP ドキュメント：バージョン 2.4 管理者ガイド"] 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手順を参照してください。

インデックス作成

以下の OpenLDAP 属性を、指定されたインデックスキーワードで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`

さらに、最適なパフォーマンスを得るために、ユーザー名に関するヘルプに記載されているフィールドにインデックスが設定されていることを確認してください。

逆グループメンバーシップの維持に関する情報について

は、<http://www.openldap.org/doc/admin24/index.html>["OpenLDAP ドキュメント：バージョン 2.4 管理者ガイド"]を参照してください。

StorageGRID で管理者グループを管理する

管理者グループを作成することで、1人または複数の管理者ユーザーのセキュリティ権限を管理できます。ユーザーが StorageGRID システムへのアクセス権を付与されるには、グループに所属している必要があります。

開始する前に

- "対応ウェブブラウザ" を使用して Grid Manager にサインインしています。
- "特定のアクセス権限"があります。
- フェデレーショングループをインポートする場合は、IDフェデレーションが構成済みであり、構成済みのIDソースにフェデレーショングループが既に存在している必要があります。

管理者グループを作成する

管理者グループを使用すると、どのユーザーがグリッドマネージャーおよびグリッド管理APIのどの機能や操作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する

手順

1. 設定 > アクセス制御 > 管理者グループ を選択します。
2. 「グループの作成」を選択します。

グループの種類を選択してください

ローカルグループを作成するか、フェデレーショングループをインポートすることができます。

- ローカルユーザーに権限を割り当てる場合は、ローカルグループを作成してください。
- IDソースからユーザーをインポートするためのフェデレーション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てください。必要に応じて後で更新できます。例えば、「Maintenance Users」や「ILM Administrators」など。
3. グループには固有の名前を入力してください。この名前は後から変更できません。
4. *続行*を選択します。

フェデレーテッドグループ

手順

1. 「フェデレーテッドグループ」を選択します。
2. インポートするグループの名前を、設定済みのIDソースに表示されているとおりに正確に入力してください。
 - Active DirectoryおよびMicrosoft Entra IDの場合は、sAMAccountNameを使用してください。
 - OpenLDAPの場合は、CN（Common Name）を使用してください。
 - 別のLDAPの場合は、LDAPサーバに適切な一意の名前を使用します。
3. *続行*を選択します。

手順

1. **Access mode** では、グループ内のユーザーがGrid ManagerおよびGrid Management APIで設定を変更したり操作を実行したりできるかどうか、または設定や機能を表示することのみが可能かどうかを選択します。

- 読み書き（デフォルト）：ユーザーは、管理権限で許可されている設定を変更したり、操作を実行したりできます。
- 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 Grid Management API で変更を加えたり、操作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ーは、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所属していて、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、ユーザーは選択されたすべての設定と機能に対して読み取り専用アクセス権を持ちます。

2. 1つ以上の"**管理者グループの権限**"を選択してください。

各グループに少なくとも1つ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ーはStorageGRIDにサインインできなくなります。

3. ローカルグループを作成する場合は、「**続行**」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、「**グループの作成**」を選択し、「**完了**」を選択します。

ユーザーを追加する（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1人以上のローカルユーザーを選択してください。

ローカルユーザーをまだ作成していない場合は、ユーザーを追加せずにグループを保存できます。このグループは、「**ユーザー**」ページでユーザーに追加できます。詳細については、"**ユーザの管理**"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する

既存のグループの詳細を表示したり、グループを変更したり、グループを複製したりできます。

- すべてのグループの基本情報を確認するには、グループページの表をご覧ください。
- 特定のグループの詳細を表示したり、グループを編集したりするには、**Actions** メニューまたは詳細ページを使用してください。

Task	[操作]メニュー	詳細ページ
グループの詳細を表示	a. 該当するグループのチェックボックスを選択してください。 b. Actions > View group details を選択します。	表の中からグループ名を選択してください。

Task	[操作]メニュー	詳細ページ
表示名を編集する (ローカルグループのみ)	a. 該当するグループのチェックボックスを選択してください。 b. Actions > Edit group name を選択します。 c. 新しい名前を入力してください。 d. 変更を保存 を選択します。	a. 詳細を表示するには、グループ名を選択してください。 b. 編集アイコン  を選択します。 c. 新しい名前を入力してください。 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する	a. 該当するグループのチェックボックスを選択してください。 b. Actions > View group details 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、"管理者グループの権限"を選択またはクリアします。 e. 変更を保存 を選択します。	a. 詳細を表示するには、グループ名を選択してください。 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、"管理者グループの権限"を選択またはクリアします。 d. 変更を保存 を選択します。

グループを複製する

手順

1. 該当するグループのチェックボックスを選択してください。
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てください。

グループを削除する

管理者グループを削除することで、システムからグループを削除し、その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、そのグループからユーザーは削除されますが、ユーザー自体は削除されません。

手順

1. グループページで、削除する各グループのチェックボックスを選択します。
2. **Actions > Delete group** を選択します。
3. 「グループを削除」を選択します。

StorageGRID の管理者グループ権限

管理者ユーザーグループを作成する際、Grid Managerの特定の機能へのアクセスを制御するために、1つ以上の権限を選択します。その後、各ユーザーをこれらの管理者グループの1つ以上に割り当てることで、そのユーザーが実行できるタスクを決定できます。

各グループには少なくとも1つ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ーは Grid Manager またはグリッド管理 API にサインインできなくなります。

デフォルトでは、少なくとも1つの権限を持つグループに属するユーザーは、以下のタスクを実行できます。

- グリッドマネージャーにサインインする
- ダッシュボードを表示する
- ノードページを表示する
- 現在発生しているアラートと解決済みのアラートを表示する
- 自分のパスワードを変更する（ローカルユーザーのみ）
- 構成およびメンテナンスページに記載されている特定の情報を表示する

権限とアクセスモードの相互作用

すべての権限において、グループの*アクセスモード*設定によって、ユーザーが設定を変更したり操作を実行したりできるかどうか、または関連する設定や機能を表示することしかできないかが決まります。ユーザーが複数のグループに所属していて、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、ユーザーは選択されたすべての設定と機能に対して読み取り専用アクセス権を持ちます。

以下のセクションでは、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。明示的に記載されていない機能を使用するには、*ルートアクセス*権限が必要です。

ルート アクセス

この権限により、グリッド管理のすべての機能にアクセスできるようになります。

テナントのルートパスワードを変更する

この権限により、テナントページの「ルートパスワードの変更」オプションにアクセスできるようになります。これにより、テナントのローカルルートユーザーのパスワードを変更できるユーザーを制御できます。この権限は、S3キーインポート機能が有効になっている場合に、S3キーを移行するためにも使用されます。この権限を持たないユーザーは、「ルートパスワードの変更」オプションを表示できません。



「テナント」ページ（*ルートパスワードの変更*オプションが含まれています）へのアクセスを許可するには、*テナントアカウント*権限も割り当ててください。

ILM

この権限により、以下の **ILM** メニューオプションへのアクセスが可能になります：

- ルール
- ポリシー
- ポリシータグ
- ストレージプール
- ストレージグレード
- Regions

- オブジェクトメタデータ検索



ストレージグレードを管理するには、ユーザーは「その他のグリッド構成」権限を持っている必要があります。

メンテナンス

これらのオプションを使用するには、ユーザーはメンテナンス権限を持っている必要があります。

- 設定 > アクセス制御：
 - グリッドパスワード
- 設定 > ネットワーク：
 - S3エンドポイントドメイン名
- 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：
 - 復旧パッケージ
 - ソフトウェアアップデート
- サポート > ツール：
 - Logs

メンテナンス権限を持たないユーザーは、以下のページを閲覧することはできますが、編集することはできません：

- メンテナンス > ネットワーク：
 - DNSサーバ
 - グリッド ネットワーク
 - NTPサーバ
- メンテナンス > システム：
 - ライセンス
- 設定 > ネットワーク：
 - S3エンドポイントドメイン名
- 設定 > セキュリティ：
 - 証明書
- 設定 > 監視：
 - 監査とsyslogサーバ

アラートを管理する

この権限により、アラートを管理するためのオプションにアクセスできるようになります。ユーザーは、サイレンス、アラート通知、およびアラートルールを管理するために、この権限が必要です。

メトリクスクエリ

この権限により、以下のものへのアクセスが可能になります：

- サポート > ツール > メトリクス ページ
- Grid Management API の **Metrics** セクションを使用したカスタム Prometheus メトリクス クエリ
- メトリクスを含むGrid Managerダッシュボードカード

オブジェクトメタデータ検索

この権限により、**ILM** > オブジェクトメタデータ検索 ページへのアクセスが可能になります。

その他のグリッド構成

この権限により、以下の追加のグリッド構成オプションにアクセスできます：

- **ILM**：
 - ストレージグレード
- 設定 > システム：
- 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

この権限により、以下が提供されます：

- グリッドマネージャを使用したストレージアプライアンス上の Eシリーズ SANtricity System Manager へのアクセス。
- これらの操作をサポートするアプライアンスの場合、「ドライブの管理」タブでトラブルシューティングおよびメンテナンス作業を実行できる機能。

テナントアカウント

この権限により、以下のことが可能になります：

- テナントページにアクセスすると、テナントアカウントの作成、編集、削除を行うことができます。
- 既存のトラフィック分類ポリシーを表示する
- テナントの詳細を含む Grid Manager ダッシュボードカードを表示する

StorageGRID でユーザーを管理する

ローカルユーザーとフェデレーションユーザーを表示できます。ローカルユーザーを作

成し、それらをローカル管理者グループに割り当てることで、これらのユーザーがアクセスできる Grid Manager の機能を決定することもできます。

開始する前に

- ["対応ウェブブラウザ"](#) を使用して Grid Manager にサインインしています。
- ["特定のアクセス権限"](#)があります。

ローカルユーザーを作成する

ローカルユーザーを1人または複数作成し、各ユーザーを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。グループの権限によって、ユーザーがアクセスできるGrid ManagerおよびGrid Management APIの機能が決まります。

ローカルユーザーのみ作成可能です。外部のIDソースを使用して、連携ユーザーと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済みのローカルユーザーが 1 人含まれています。root ユーザーは削除できません。



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

ウィザードにアクセスする

手順

1. **Configuration > Access control > Admin users** を選択します。
2. 「ユーザーの作成」を選択します。

ユーザー認証情報を入力してください

手順

1. ユーザーの氏名、固有のユーザー名、およびパスワードを入力してください。
2. 必要に応じて、このユーザーが Grid Manager または Grid Management API にアクセスできないようにする場合は、「はい」を選択します。
3. *続行*を選択します。

グループに割り当てる

手順

1. 必要に応じて、ユーザーを1つまたは複数のグループに割り当てて、ユーザーの権限を決定します。

グループをまだ作成していない場合は、グループを選択せずにユーザーを保存できます。このユーザーをグループに追加するには、「グループ」ページを使用してください。

ユーザーが複数のグループに所属している場合、権限は累積されます。詳細については、["管理者グループの管理"](#)を参照してください。

2. 「ユーザーの作成」を選択し、「完了」を選択します。

ローカルユーザーの表示と編集

既存のローカルユーザーおよびフェデレーションユーザーの詳細を表示できます。ローカルユーザーを変更すると、ユーザーのフルネーム、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、ユーザーがGrid ManagerおよびGrid Management APIにアクセスできないように一時的に制限することもできます。

ローカルユーザーの編集のみ可能です。外部IDソースを使用して、フェデレーションユーザーを管理します。

- ローカルユーザーおよびフェデレーションユーザーすべての基本情報を確認するには、ユーザーページの表を参照してください。
- 特定のユーザーの詳細をすべて表示したり、ローカルユーザーを編集したり、ローカルユーザーのパスワードを変更したりするには、「アクション」メニューまたは詳細ページを使用します。

編集内容は、ユーザーが次回ログアウトしてからグリッド マネージャーに再度ログインした際に適用されます。



ローカルユーザーは、グリッドマネージャーのバナーにある「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。

Task	[操作]メニュー	詳細ページ
ユーザーの詳細を表示	- ユーザーのチェックボックスを選択します。 Actions > View user details を選択します。	表の中からユーザー名を選択してください。
氏名を編集する（ローカルユーザーのみ）	- ユーザーのチェックボックスを選択します。 Actions > Edit full name を選択します。 - 新しい名前を入力してください。 - 変更を保存 を選択します。	- 詳細を表示するには、ユーザー名を選択してください。 - 編集アイコン  を選択します。 - 新しい名前を入力してください。 - 変更を保存 を選択します。
StorageGRID アクセスを拒否または許可する	- ユーザーのチェックボックスを選択します。 Actions > View user details を選択します。 「アクセス」タブを選択します。 - ユーザーがGrid ManagerまたはGrid Management APIにサインインできないようにするには「はい」を選択し、サインインを許可するには「いいえ」を選択してください。 - 変更を保存 を選択します。	- 詳細を表示するには、ユーザー名を選択してください。 「アクセス」タブを選択します。 - ユーザーがGrid ManagerまたはGrid Management APIにサインインできないようにするには「はい」を選択し、サインインを許可するには「いいえ」を選択してください。 - 変更を保存 を選択します。

Task	[操作]メニュー	詳細ページ
パスワードの変更（ローカルユーザーのみ）	a. ユーザーのチェックボックスを選択します。 b. Actions > View user details 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. 詳細を表示するには、ユーザー名を選択してください。 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。
グループの変更（ローカルユーザーのみ）	a. ユーザーのチェックボックスを選択します。 b. Actions > View user details 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、グループ名の後のリンクを選択すると、新しいブラウザタブでグループの詳細を表示できます。 e. 別のグループを選択するには、グループの編集を選択してください。 f. 変更を保存を選択します。	a. 詳細を表示するには、ユーザー名を選択してください。 b. 「グループ」タブを選択します。 c. 必要に応じて、グループ名の後のリンクを選択すると、新しいブラウザタブでグループの詳細を表示できます。 d. 別のグループを選択するには、グループの編集を選択してください。 e. 変更を保存を選択します。

フェデレーションユーザーをインポート

1人または複数人の連携ユーザー（最大100人まで）を、ユーザーページに直接インポートできます。

手順

1. **Configuration > Access control > Admin users** を選択します。
2. 「フェデレーションユーザーのインポート」を選択します。
3. 1人以上のフェデレーションユーザーのUUIDまたはユーザー名を入力してください。

複数のエントリがある場合は、各UUIDまたはユーザー名を新しい行に追加してください。

4. 「インポート」を選択します。

1人以上のユーザーについて「ユーザー」フィールドへのインポートが失敗した場合は、以下の手順を実行してください。

- a. 「インポートされていないユーザー」を展開し、「ユーザーのコピー」を選択します。
- b. 前へ を選択し、コピーしたユーザーを フェデレーションユーザーのインポート ダイアログボックスに貼り付けて、インポートを再試行してください。

「フェデレーションユーザーのインポート」ダイアログボックスを閉じると、正常にインポートされたユ

ーザーのフェデレーションユーザー情報が「ユーザー」ページに表示されます。

ユーザーを複製する

既存のユーザーを複製することで、同じ権限を持つ新しいユーザーを作成できます。

手順

1. ユーザーのチェックボックスを選択します。
2. **Actions** > *ユーザーの複製*を選択します。
3. ユーザー複製ウィザードを完了してください。

ユーザーを削除する

ローカルユーザーを削除すると、そのユーザーがシステムから完全に削除されます。



ルートユーザーは削除できません。

手順

1. ユーザーページから、削除する各ユーザーのチェックボックスを選択します。
2. **Actions** > **Delete user** を選択します。
3. 「ユーザーを削除」を選択します。

シングル サインオン (SSO) を使用する

StorageGRID SSO について学ぶ

シングル サインオン (SSO) が有効になっている場合、ユーザーは、組織が実装したSSOサインインプロセスを使用して認証情報が承認された場合にのみ、Grid Manager、Tenant Manager、Grid Management API、またはTenant Management APIにアクセスできます。ローカルユーザーはStorageGRIDにサインインできません。

StorageGRID システムは、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) をサポートしています。

シングル サインオン (SSO) を有効にする前に、SSO が有効になっている場合に StorageGRID のサインインおよび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が有効な場合のサインイン

SSOが有効になっていてStorageGRIDにサインインすると、認証情報を検証するために組織のSSOページにリダイレクトされます。

手順

1. 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、Web ブラウザに入力してください。

StorageGRID のサインイン ページが表示されます。

- このブラウザでこのURLに初めてアクセスする場合は、アカウントIDの入力を求められます。
- 以前にグリッドマネージャーまたはテナントマネージャーにアクセスしたことがある場合は、最近使用したアカウントを選択するか、アカウントIDを入力するよう求められます。



テナント アカウントの完全な URL（つまり、完全修飾ドメイン名または IP アドレスに続いて `?accountId=20-digit-account-id`）を入力しても、StorageGRID のサインイン ページは表示されません。代わりに、組織の SSO サインイン ページにすぐにリダイレクトされ、そこで[SSO認証情報を使用してサインインしてください](#)。

2. グリッドマネージャーにアクセスするか、テナントマネージャーにアクセスするかを指定してください。
 - 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するか、アカウント ID として **0** を入力するか、最近使用した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てください。
 - テナントマネージャー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、最近使用したアカウントの一覧にテナント名が表示されている場合は、そのテナントを選択してください。
3. 「サインイン」を選択します。

StorageGRID により、組織の SSO サインイン ページにリダイレクトされます。例：

4. SSO認証情報を使用してサインインしてください。

SSO認証情報が正しい場合：

- a. IDプロバイダー（IdP）は、StorageGRID に認証応答を提供します。
- b. StorageGRID は認証応答を検証します。
- c. 応答が有効で、StorageGRID アクセス権限を持つフェデレーショングループに属している場合、選択したアカウントに応じて、Grid Manager またはTenant Manager にサインインします。



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

5. 必要に応じて、適切な権限があれば、他の管理ノードにアクセスしたり、グリッドマネージャーやテナントマネージャーにアクセスしたりできます。

SSO認証情報を再入力する必要はありません。

SSOが有効な場合のサインアウト

StorageGRID で SSO が有効になっている場合、サインアウト時の動作は、サインインしているサービスとサインアウト元の場所によって異なります。

手順

1. ユーザーインターフェースの右上隅にある「サインアウト」リンクを見つけてください。
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。最近使用したアカウント ドロップダウンが更新さ

れ、**Grid Manager** またはテナント名が含まれるようになります。これにより、今後これらのユーザーインターフェイスにすばやくアクセスできます。



この表は、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。

サインインしている場合...	サインアウト元...	サインアウトしました...
1つ以上の管理ノード上のグリッドマネージャー	任意の管理ノード上のグリッドマネージャー	すべての管理ノードの Grid Manager 注: SSO に Entra ID を使用する場合、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場合があります。
1つ以上の管理ノード上のテナントマネージャー	任意の管理ノード上のテナントマネージャー	すべての管理ノードのテナントマネージャー
グリッドマネージャーとテナントマネージャーの両方	Grid Manager	グリッドマネージャーのみ。SSO からサインアウトするには、テナントマネージャーからもサインアウトする必要があります。

StorageGRID SSO の要件と考慮事項

StorageGRID システムのシングル 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は、以下のSSO IDプロバイダー (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)
- Microsoft Entra ID
- PingFederate

StorageGRID システムのIDフェデレーションを設定してから、シングル サインオン IDプロバイダーを設定する必要があります。IDフェデレーションに使用するLDAPサービスの種類によって、実装できるシングル サインオンの種類が決まります。

構成済みのLDAPサービスタイプ	SSO IDプロバイダーのオプション
Active Directory	• Active Directory • Entra ID • PingFederate

構成済みのLDAPサービスタイプ	SSO IDプロバイダーのオプション
Entra ID	Entra ID

AD FSの要件

以下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 は、"[KB3201845 アップデート](#)"以降を使用する必要があります。

その他の要件

- トランスポート層セキュリティ (TLS) 1.2または1.3
- Microsoft .NET Framework、バージョン 3.5.1 以降

Entra IDに関する考慮事項

Entra ID を SSO タイプとして使用し、ユーザーのユーザープリンシパル名がプレフィックスとして sAMAccountName を使用しない場合、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。ユーザー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。

サーバー証明書の要件

デフォルトでは、StorageGRIDは各管理ノードの管理インターフェイス証明書を使用して、グリッドマネージャ、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 (Entra ID)、またはサービスプロバイダー接続 (PingFederate) を設定する場合、StorageGRIDリクエストの署名証明書としてサーバ証明書を使用します。

まだ行っていない場合は"[管理インターフェイスにカスタム証明書を設定しました](#)"、今すぐ実行してください。カスタムサーバー証明書をインストールすると、すべての管理ノードで使用され、すべての StorageGRID 依拠当事者トラスト、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て復旧した場合、新しいデフォルトサーバ証明書が生成されます。復旧したノードにサインインする前に、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、`/var/local/mgmt-api`ディレクトリに移動します。カスタムサーバ証明書の名前は`custom-server.crt`です。ノードのデフォルトサーバ証明書の名前は`server.crt`です。

ポートの要件

制限付きGrid ManagerまたはTenant Managerポートでは、シングル サインオン (SSO) は利用できません。ユーザーがシングル サインオンで認証を行うには、デフォルトのHTTPSポート (443) を使用する必要があります。"[外部ファイアウォールでアクセスを制御する](#)"を参照してください。

フェデレーションユーザーが**StorageGRID**にサインインできることを確認してください

シングル サインオン (SSO) を有効にする前に、既存のテナントアカウントについて、少なくとも1人のフェデレーションユーザーが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。

開始する前に

- "[対応ウェブブラウザ](#)" を使用して Grid Manager にサインインしています。
- "[特定のアクセス権限](#)"があります。
- IDフェデレーションは既に設定済みです。

手順

1. 既存のテナントアカウントがある場合は、いずれのテナントも独自のIDソースを使用していないことを確認してください。



SSO を有効にすると、Tenant Manager で設定された ID ソースは、Grid Manager で設定された ID ソースによって上書きされます。テナントの ID ソースに属するユーザーは、Grid Manager の ID ソースにアカウントを持っていない限り、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テナントマネージャーにサインインします。
 - b. アクセス管理 > IDフェデレーション を選択します。
 - c. ID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てください。
 - d. 該当する場合は、このテナント アカウントで使用されている可能性のあるフェデレーション 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. フェデレーションユーザーがGrid Managerにアクセスできることを確認します。
 - a. グリッドマネージャーから、設定 > アクセス制御 > *管理者グループ*を選択します。
 - b. Active Directory ID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、ルートアクセス権限が割り当てられていることを確認してください。
 - c. サインアウト。
 - d. フェデレーテッドグループのユーザーとして Grid Manager に再度サインインできることを確認してください。
 3. 既存のテナントアカウントがある場合は、ルートアクセス権限を持つフェデレーションユーザーがサインインできることを確認してください。
 - a. グリッドマネージャーから「テナント」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. 「詳細を入力」タブで、*続行*を選択します。
 - d. 独自のIDソースを使用する チェックボックスが選択されている場合は、チェックボックスをオフにし

て 保存 を選択してください。

テナントページが表示されます。

- e. テナントアカウントを選択し、*サインイン*を選択して、ローカルルートユーザーとしてテナントアカウントにサインインします。
- f. テナントマネージャーから、アクセス管理 > *グループ*を選択します。
- g. Grid Manager のフェデレーショングループのうち、少なくとも 1 つにこのテナントのルートアクセス権限が割り当てられていることを確認してください。
- h. サインアウト。
- i. フェデレーショングループのユーザーとしてテナントに再度サインインできることを確認してください。

関連情報

- ["シングル サインオンの要件と考慮事項"](#)
- ["管理者グループの管理"](#)
- ["テナントアカウントを使用する"](#)

StorageGRID で SSO を設定

SSO 構成ウィザードに従ってサンドボックスモードに入り、すべての StorageGRID ユーザーに対して有効にする前に、シングル サインオン (SSO) を構成してテストすることができます。SSO を有効にした後、必要に応じてサンドボックスモードに戻り、設定を変更したり再テストしたりすることができます。

開始する前に

- ["対応ウェブブラウザ"](#) を使用して Grid Manager にサインインしています。
- あなたは["ルートアクセス権限"](#)があります。
- StorageGRID システムの ID フェデレーションを設定しました。
- IDフェデレーションの*LDAPサービスタイプ*については、使用予定の SSO ID プロバイダーに基づいて、Active Directory または Entra ID のいずれかを選択しました。

構成済みのLDAPサービスタイプ	SSO IDプロバイダーのオプション
Active Directory フェデレーション サービス (AD FS)	• Active Directory • Entra ID • PingFederate
Entra ID	Entra ID

タスク概要

SSOが有効になっていて、ユーザーが管理ノードにサインインしようとする、StorageGRIDはSSO IDプロバイダーに認証要求を送信します。続いて、SSO IDプロバイダーはStorageGRIDに認証応答を返信し、認証要求が成功したかどうかを示します。リクエストが成功した場合：

- Active Directory または PingFederate からの応答には、ユーザーの汎用一意識別子（UUID）が含まれます。
- Entra ID からの応答には、ユーザープリンシパル名（UPN）が含まれています。

StorageGRID（サービスプロバイダー）と SSO ID プロバイダーがユーザ認証リクエストについて安全に通信できるようにするには、次のタスクを実行します：

1. StorageGRID で設定を構成します。
2. SSO ID プロバイダーのソフトウェアを使用して、各管理ノード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（Entra ID）、またはサービス プロバイダー（PingFederate）を作成します。
3. StorageGRID に戻り、SSO を有効にします。

サンドボックスモードを使用すると、このような設定のやり取りを簡単に実行でき、SSOを有効にする前に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、ユーザーはSSOを使用してサインインできません。

ウィザードにアクセスする

手順

1. **Configuration > Access control > Single sign-on** を選択します。シングル サインオン ページが表示されます。



「SSO設定の構成」ボタンが無効になっている場合は、IDプロバイダーをフェデレーションIDソースとして構成したことを確認してください。["シングル サインオンの要件と考慮事項"](#)を参照してください。

2. 「SSO設定の構成」を選択します。「IDプロバイダーの詳細を入力」ページが表示されます。

IDプロバイダーの詳細を入力してください

手順

1. ドロップダウンリストから **SSO** タイプ を選択してください。
2. SSO の種類として Active Directory を選択した場合は、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、ID プロバイダーの フェデレーション サービス名 を入力してください。



フェデレーションサービス名を確認するには、Windows Server Manager を開きます。「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を編集」を選択します。フェデレーションサービス名は 2 番目のフィールドに表示されます。

3. ID プロバイダーが StorageGRID リクエストに応答して SSO 構成情報を送信する際に、接続を保護するために使用される TLS 証明書を指定します。
 - オペレーティングシステムの**CA**証明書を使用する：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**証明書を使用する：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て、**CA Certificate** テキストボックスに貼り付けてください。

- **TLS** を使用しない：接続を保護するために TLS 証明書を使用しません。



CA証明書を変更する場合は、すぐに"[管理ノードで mgmt-api サービスを再起動します。](#)"して、Grid ManagerへのSSOが正常に確立されるかどうかをテストしてください。

4. 「続行」を選択してください。「依頼当事者識別子を提供する」ページが表示されます。

依頼当事者識別子を指定してください

1. 選択した SSO タイプに基づいて、「証明書利用者識別子の提供」ページの各項目を入力してください。

Active Directory

- a. StorageGRID の 依拠当事者識別子 を指定します。この値は、AD FS における各証明書利用者信頼に使用する名前を制御します。
 - 例えば、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、`SG`または`StorageGRID`と入力します。
 - グリッドに複数の管理ノードが含まれている場合は、識別子に文字列 [HOSTNAME] `を含めてください。例：`SG-[HOSTNAME]`。この文字列を含めると、グリッド内の各管理ノードのホスト名に基づいて、そのノードの依拠パーティ識別子を示すテーブルが作成されます。



StorageGRID システム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。各管理ノードに証明書利用者信頼を設定することで、ユーザーはどの管理ノードにも安全にサインインおよびサインアウトできるようになります。

- b. 「保存してサンドボックスモードに入る」を選択します。

Entra ID

- a. 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、Entra ID で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。
 - 例えば、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、`SG`または`StorageGRID`と入力します。
 - グリッドに複数の管理ノードが含まれている場合は、識別子に文字列 [HOSTNAME] `を含めてください。例：`SG-[HOSTNAME]`。この文字列を含めると、システム内の各管理ノードのホスト名に基づいて、各ノードのエンタープライズアプリケーション名を表示する表が作成されます。



StorageGRID システム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する必要があります。各管理ノード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、ユーザーはどの管理ノードにも安全にサインインおよびサインアウトできるようになります。

- b. ["Entra IDでエンタープライズアプリケーションを作成する"](#)の手順に従って、表に記載されている各管理ノードのエンタープライズアプリケーションを作成します。
- c. Entra ID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URLをコピーします。次に、このURLをStorageGRIDの対応する **Federation** メタデータ **URL** フィールドに貼り付けます。
- d. すべての管理ノードのフェデレーションメタデータURLをコピーして貼り付けたら、*保存してサンドボックスモードに入る*を選択します。

PingFederate

- a. サービスプロバイダー (SP) セクションでは、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。
 - 例えば、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、`SG`または`StorageGRID`と入力します。
 - グリッドに複数の管理ノードが含まれている場合は、識別子に文字列 [HOSTNAME] `を含め

てください。例：`SG-[HOSTNAME]`。この文字列を含めると、ノードのホスト名に基づいて、システム内の各管理ノードの SP 接続 ID を示す表が表示されます。



StorageGRID システムの管理ノードごとに SP 接続を作成する必要があります。各管理ノードに SP 接続を設定することで、ユーザーはどの管理ノードにも安全にサインインおよびサインアウトできます。

- b. フェデレーションメタデータURL フィールドに、各管理ノードのフェデレーションメタデータURLを指定します。

次の形式を使用してください。

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

- c. 「保存してサンドボックスモードに入る」を選択します。

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** 接続の設定

設定を保存してサンドボックスモードに入ると、選択したSSOタイプの設定を完了してテストできます。

StorageGRID は、必要に応じてサンドボックスモードを維持できます。ただし、サインインできるのはフェデレーションユーザーとローカルユーザーのみです。

Active Directory

手順

1. Active Directory フェデレーション サービス (AD FS) にアクセスしてください。
2. StorageGRID の証明書利用者信頼を1つ以上作成します。その際、「SSO の設定」ページの表に示されている各証明書利用者識別子を使用してください。

表に示されている各管理ノードに対して、1つの信頼関係を作成する必要があります。

手順については、"[AD FSで証明書利用者信頼を作成する](#)"をご覧ください。

Entra ID

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てください。
2. 次に、グリッド内の他の管理ノードについても、以下の手順を繰り返してください。
 - 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てください。
4. "[Entra IDでエンタープライズアプリケーションを作成する](#)"の手順に従って、各管理ノードのSAMLメタデータファイルを対応するEntra IDエンタープライズアプリケーションにアップロードしてください。

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てください。
2. 次に、グリッド内の他の管理ノードについても、以下の手順を繰り返してください。
 - 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 つ以上のサービス プロバイダー \(SP\) 接続を作成します](#)". 各管理ノードの SP 接続 ID (「SSO の設定」ページの表に表示) 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てください。

表に示されている各管理ノードに対して、SP 接続を 1 つ作成する必要があります。

テスト構成

StorageGRID システム全体にシングル サインオンの使用を強制する前に、各管理ノードに対してシングル 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してください。

Active Directory

手順

1. 「SSO の設定」 ページから、ウィザードの「設定のテスト」 手順にあるリンクを確認します。

URLは、*フェデレーションサービス名*フィールドに入力した値から生成されます。

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て、IDプロバイダーのサインオンページにアクセスしてください。
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、「次のサイトのいずれかにサインイン」を選択し、プライマリ管理ノードの証明書利用者識別子を選択して、「サインイン」を選択します。
4. フェデレーションユーザー名とパスワードを入力してください。
 - SSOのサインインとログアウト操作が成功すると、成功メッセージが表示されます。
 - SSO操作が失敗した場合、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Cookieを削除してから、もう一度お試しください。
5. グリッド内の各管理ノードについて、以下の手順を繰り返してSSO接続を確認してください。

Entra ID

手順

1. Azure ポータルのシングル サインオン ページにアクセスしてください。
2. 「このアプリケーションをテストする」を選択してください。
3. フェデレーションユーザーの認証情報を入力してください。
 - SSOのサインインとログアウト操作が成功すると、成功メッセージが表示されます。
 - SSO操作が失敗した場合、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Cookieを削除してから、もう一度お試しください。
4. グリッド内の各管理ノードについて、以下の手順を繰り返してSSO接続を確認してください。

PingFederate

手順

1. 「SSO設定」 ページから、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てください。

2. フェデレーションユーザーの認証情報を入力してください。
 - SSOのサインインとログアウト操作が成功すると、成功メッセージが表示されます。
 - SSO操作が失敗した場合、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Cookieを削除してから、もう一度お試しください。
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 接続を確認してください。

「ページ有効期限切れ」というメッセージが表示された場合は、ブラウザの「戻る」 ボタンを選択し、再度認証情報を送信してください。

シングル サインオンを有効にする

各管理ノードへのサインインにSSOを使用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、すべてのユーザーは、グリッドマネージャ、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にアクセスするためにSSOを使用する必要があります。ローカルユーザーはStorageGRIDにアクセスできなくなります。

手順

1. SSO構成ウィザードの「テスト構成」ステップから、*SSOを有効にする*を選択します。
2. 警告メッセージを確認し、*SSOを有効にする*を選択してください。

シングル サインオンが有効になりました。シングル サインオンページが表示され、先ほど設定した SSO の詳細が表示されます。

3. 設定を編集するには、*編集*を選択してください。
4. シングル サインオンを無効にするには、*「SSOを無効にする」*を選択します。



Azure Portal を使用していて、Entra ID へのアクセスに使用すると同じコンピューターから StorageGRID にアクセスする場合は、Azure Portal のユーザーが承認済みの StorageGRID ユーザー（StorageGRID にインポートされたフェデレーショングループに属するユーザー）であることを確認するか、StorageGRID へのサインインを試みる前に Azure Portal からログアウトしてください。

AD FS で StorageGRID の証明書利用者信頼を作成します

システム内の各管理ノードに対して、Active Directory フェデレーション サービス (AD FS) を使用して証明書利用者信頼を作成する必要があります。証明書利用者信頼を作成するには、PowerShell コマンドを使用する方法、StorageGRID から SAML メタデータをインポートする方法、またはデータを手動で入力する方法があります。

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 に **"サンドボックスモードに入りました"** があります。
- システム内の各管理ノードについて、完全修飾ドメイン名（またはIPアドレス）と証明書利用者識別子を把握する必要があります。これらの値は、StorageGRID の「SSO の設定」ページにある管理ノードの詳細テーブルで確認できます。



StorageGRID システム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。各管理ノードに証明書利用者信頼を設定することで、ユーザーはどの管理ノードにも安全にサインインおよびサインアウトできるようになります。

- AD FS で証明書利用者信頼を作成した経験があるか、または Microsoft AD FS のドキュメントを参照できる環境にあること。
- AD FS Management スナップインを使用しており、Administrators グループに属しています。
- 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アップロードされた

カスタム証明書を持っているか、またはコマンドシェルから管理ノードにログインする方法を知っている必要があります。

タスク概要

これらの手順は、Windows Server 2016 AD FS に適用されます。AD FS の異なるバージョンを使用している場合は、手順に若干の違いがあります。ご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する

Windows PowerShell を使用して、1つまたは複数の証明書利用者信頼をすばやく作成できます。

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"
```

- `Admin_Node_Identifer``には、シングル サインオンページに表示されているとおりに、管理ノードの証明書利用者識別子を入力してください。例： ``SG-DC1-ADM1`。
- ``Admin_Node_FQDN``には、同じ管理ノードの完全修飾ドメイン名を入力してください。（必要に応じて、ノードの IP アドレスを使用することもできます。ただし、ここに IP アドレスを入力した場合、その IP アドレスが変更されたときは、この証明書利用者信頼を更新または再作成する必要があることに注意してください。）

3. Windows Server Manager から、ツール > **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 > Relying Party Trusts** を選択します。

証明書利用者信頼の一覧が表示されます。

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. 先ほど作成した証明書利用者信頼を見つけます。
 - b. 信頼関係を右クリックし、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」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、クレーム発行ポリシーを追加します。
 - a. 先ほど作成した証明書利用者信頼を見つけます。
 - 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. 「ルールを追加」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する」を選択し、「次へ」を選択します。

e. 「ルール設定」 ページで、このルールの表示名を入力します。

例えば、**ObjectGUID to Name ID** または **UPN to Name ID** など。

f. 属性ストアには、**Active Directory** を選択してください。

g. マッピングテーブルの「LDAP属性」列に、**objectGUID** と入力するか、**User-Principal-Name** を選択します。

h. マッピングテーブルの「送信要求タイプ」列で、ドロップダウンリストから「**Name 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てください。

a. 依拠当事者トラストを右クリックして、そのプロパティを開きます。

b. 「エンドポイント」、「識別子」、「署名」タブの各フィールドに入力されていることを確認してください。

メタデータが欠落している場合は、フェデレーションのメタデータアドレスが正しいことを確認するか、値を手動で入力してください。

8. 以下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の証明書利用者信頼を構成します。

9. 完了したら、StorageGRID に戻り、「[すべての証明書利用者信頼をテストする](#)」正しく設定されていることを確認してください。

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する

各管理ノードのSAMLメタデータにアクセスすることで、各証明書利用者信頼の値をインポートできます。

手順

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

2. 「アクション」で「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で公開されている依拠当事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`

`\_Admin\_Node\_FQDN\_`には、同じ管理ノードの完全修飾ドメイン名を入力してください。（必要に応じて、ノードの IP アドレスを使用することもできます。ただし、ここに IP アドレスを入力した場合、その IP アドレスが変更されたときは、この証明書利用者信頼を更新または再作成する必要があることに注意してください。）

6. 証明書利用者信頼ウィザードを完了し、証明書利用者信頼を保存して、ウィザードを閉じます。



表示名を入力する際は、Grid Manager のシングル サインオンページに表示されているとおり、管理ノードの証明書利用者識別子を使用してください。例えば、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」を選択します：
- 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する」を選択し、「次へ」を選択します。
- d. 「ルール設定」ページで、このルールの表示名を入力します。

例えば、**ObjectGUID to Name ID** または **UPN to Name ID** など。

- e. 属性ストアには、**Active Directory** を選択してください。
- f. マッピングテーブルの「LDAP属性」列に、**objectGUID** と入力するか、**User-Principal-Name** を選択します。
- g. マッピングテーブルの「送信要求タイプ」列で、ドロップダウンリストから「**Name 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てください。

- a. 依拠当事者トラストを右クリックして、そのプロパティを開きます。
- b. 「エンドポイント」、「識別子」、「署名」タブの各フィールドに入力されていることを確認してください。

メタデータが欠落している場合は、フェデレーションのメタデータアドレスが正しいことを確認するか、値を手動で入力してください。

9. 以下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の証明書利用者信頼を構成します。
10. 完了したら、StorageGRID に戻り、「[すべての証明書利用者信頼をテストする](#)」正しく設定されていることを確認してください。

証明書利用者信頼を手動で作成する

証明書利用者信頼のデータをインポートしない場合は、値を手動で入力できます。

手順

1. Windows Server Managerで、*ツール*を選択し、次に*AD FS Management*を選択します。
2. 「アクション」で「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. 「依拠当事者に関するデータを手動で入力」を選択し、「次へ」を選択します。
5. 証明書利用者信頼ウィザードを完了します。
 - a. この管理ノードの表示名を入力してください。

一貫性を保つため、管理者ノードの証明書利用者識別子は、グリッドマネージャーのシングル サインオンページに表示されているとおりに使用してください。例えば、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スキップしてください。
- 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選択します。
- d. 管理ノードの SAML サービスエンドポイント URL を入力してください：

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

``\_Admin\_Node\_FQDN``には、管理ノードの完全修飾ドメイン名を入力してください。（必要に応じて、ノードの IP アドレスを使用することもできます。ただし、ここに IP アドレスを入力した場合、その IP アドレスが変更されたときは、この証明書利用者信頼を更新または再作成する必要があることに注意してください。）

- e. 「識別子の設定」ページで、同じ管理ノードの証明書利用者識別子を指定します。

`Admin_Node_Identifier`

``\_Admin\_Node\_Identifier``には、シングルサインオンページに表示されているとおりに、管理ノードの証明書利用者識別子を入力してください。例： ``SG-DC1-ADM1``。

- f. 設定を確認し、依頼当事者の信頼関係を保存して、ウィザードを閉じます。

「請求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、トラストを右クリックして、**Edit claim issuance policy** を選択してください。

- 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する」を選択し、「次へ」を選択します。
 - b. 「ルール設定」ページで、このルールの表示名を入力します。

例えば、**ObjectGUID to Name ID** または **UPN to Name ID** など。
 - c. 属性ストアには、**Active Directory** を選択してください。
 - d. マッピングテーブルの「LDAP属性」列に、**objectGUID** と入力するか、**User-Principal-Name** を選択します。
 - e. マッピングテーブルの「送信要求タイプ」列で、ドロップダウンリストから「**Name ID**」を選択します。
 - f. 「完了」を選択し、「OK」を選択します。

7. 依拠当事者トラストを右クリックして、そのプロパティを開きます。
8. 「エンドポイント」タブで、シングル ログアウト（SLO）用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. エンドポイントタイプ > **SAML ログアウト** 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`

`\_Admin\_Node\_FQDN\_`には、管理ノードの完全修飾ドメイン名を入力してください。（必要に応じて、ノードのIPアドレスを使用することもできます。ただし、ここにIPアドレスを入力した場合、そのIPアドレスが変更された際には、この証明書利用者信頼を更新または再作成する必要があることに注意してください。）

- e. 「OK」を選択します。
9. 「署名」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てください。
 - カスタム証明書をお持ちでない場合は、管理ノードにログインし、管理ノードの `/var/local/mgmt-api` ディレクトリに移動して、`custom-server.crt` 証明書ファイルを追加してください。



管理ノードのデフォルト証明書を使用する（`server.crt`）ことは推奨されません。管理ノードに障害が発生した場合、ノードを復旧するとデフォルトの証明書が再生成されるため、証明書利用者の信頼関係を更新する必要があります。

- b. 「適用」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、閉じられます。

10. 以下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の証明書利用者信頼を構成します。
11. 完了したら、StorageGRID に戻り、**"すべての証明書利用者信頼をテストする"**正しく設定されていることを確認してください。

Entra ID で StorageGRID のエンタープライズ アプリケーションを作成する

Entra IDを使用して、システム内の各管理ノードに対応するエンタープライズアプリケーションを作成します。

開始する前に

- StorageGRID のシングル サインオンの設定を開始し、SSO タイプとして「Entra ID」を選択しました。

- Grid Manager に "[サンドボックスモードに入りました](#)" があります。
- システム内の各管理ノードには、*エンタープライズアプリケーション名*が割り当てられています。これらの値は、「SSO の設定」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する必要があります。各管理ノード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、ユーザーはどの管理ノードにも安全にサインインおよびサインアウトできるようになります。

- Entra ID 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ります。
- 有効なサブスクリプションを持つ Entra ID アカウントをお持ちです。
- Entra ID アカウントで、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、またはサービス プリンシパルの所有者のいずれかのロールを持っています。

Entra ID へのアクセス

手順

1. "[Azure Portal](#)"にログインします。
2. "[Entra ID](#)"に移動します。
3. 選択 "[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** 構成を保存する

StorageGRID で Entra ID の SSO 設定を保存するには、各管理ノードのエンタープライズアプリケーションを Entra ID を使用して作成する必要があります。Entra ID からフェデレーションメタデータ URL をコピーし、「SSO の設定」ページの対応する 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。

手順

1. 以下の手順を各管理ノードに対して繰り返します。
 - a. Entra ID 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、「SSO の設定」ページの「管理ノードの詳細」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 を入力してください。
 - d. 「ギャラリーにないその他のアプリケーションを統合する（ギャラリー以外）」の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 **【はじめに】** リンクを選択します。シングル サインオンを設定する ボックス、または左側の余白にある シングル サインオン リンクを選択します。
 - g. 「SAML」チェックボックスを選択します。
 - h. 「手順3 SAML署名証明書」に記載されている「アプリフェデレーションメタデータURL」をコピーしてください。
 - i. SSO の設定ページに移動し、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構成に必要なその他の変更をすべて行

った後、「SSO の設定」ページで「保存」を選択します。

各管理ノードの**SAML**メタデータをダウンロードする

SSO 設定を保存した後、StorageGRID システムの各管理ノードの SAML メタデータ ファイルをダウンロードできます。

手順

1. 各管理ノードに対して、これら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. その管理ノードの SAML メタデータをダウンロードするには、ボタンを選択してください。
 - d. ファイルを保存します。このファイルをEntra IDにアップロードします。

各エンタープライズアプリケーションに**SAML**メタデータをアップロードする

各 StorageGRID 管理ノードの SAML メタデータファイルをダウンロードしたら、Entra ID で次の手順を実行してください。

手順

1. Azure ポータルに戻ります。
2. 各エンタープライズアプリケーションに対して、以下の手順を繰り返してください。



以前追加したアプリケーションを一覧に表示するには、エンタープライズアプリケーションページを更新する必要がある場合があります。

- 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てください。
 - b. 割り当て必須 を いいえ に設定します（割り当てを個別に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. ファイルが読み込まれたら、*保存*を選択し、次に*X*を選択してウィンドウを閉じます。SAMLによるシングル サインオンの設定ページに戻ります。
3. **"各アプリケーションをテストする"**。

PingFederateで**StorageGRID**用のサービスプロバイダー接続を作成する

PingFederate を使用して、システム内の各管理ノードのサービスプロバイダー（SP）接続を作成します。処理を高速化するために、StorageGRID から SAML メタデータをインポートします。

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「Ping Federate」を選択しました。

- Grid Manager に "[サンドボックスモードに入りました](#)" があります。
- システム内の各管理ノードの **SP connection ID** を確認しておきます。これらの値は、「SSO の設定」ページの管理ノード詳細テーブルで確認できます。
- システム内の各管理ノードのSAMLメタデータをダウンロードしました。
- PingFederate Server で SP 接続を作成した経験があります。
- PingFederate Server
のhttps://docs.pingidentity.com/pingfederate/latest/administrators_reference_guide/pf_administrators_reference_guide.html["管理者向けリファレンスガイド"]があります。PingFederate のドキュメントには、詳細な手順と説明が記載されています。
- PingFederate Server の"[管理者権限](#)"があります。

タスク概要

これらの手順は、StorageGRID のSSOプロバイダーとしてPingFederate サーバーバージョン10.3を設定する方法をまとめたものです。別のバージョンのPingFederateを使用している場合は、これらの手順を適宜調整する必要があります。ご使用のリリースに関する詳細な手順については、PingFederate サーバーのドキュメントを参照してください。

PingFederate の前提条件を完了する

StorageGRID に使用する SP 接続を作成する前に、PingFederate で前提条件となるタスクを完了する必要があります。これらの前提条件からの情報は、SP 接続を設定する際に使用します。

データストア を作成します

まだ作成していない場合は、PingFederate を AD FS LDAPサーバに接続するためのデータストアを作成してください。StorageGRID で"[IDフェデレーションの設定](#)"際に使用した値を使用してください。

- 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、表示されているとおりに*objectGUID*を入力してください。

パスワード認証情報バリデーターを作成します

まだ作成していない場合は、パスワード認証情報検証ツールを作成してください。

- タイプ：LDAP ユーザー名パスワード認証情報検証ツール
- データストア：作成したデータストアを選択してください。
- 検索ベース：LDAPから情報を入力します（例：DC=saml、DC=sgws）。
- 検索フィルター：sAMAccountName=\${username}
- スcope：サブツリー

IdPアダプターインスタンス を作成します

まだ作成していない場合は、IdPアダプターインスタンスを作成してください。

手順

1. **Authentication > Integration > IdP Adapters** に移動します。
2. 「新規インスタンスの作成」を選択します。
3. 「タイプ」タブで、「HTML Form IdP Adapter」を選択します。
4. 「IdP Adapter」タブで、*「Credential Validators」に新しい行を追加する*を選択します。
5. 作成した[パスワード認証情報検証ツール](#)を選択します。
6. アダプター属性タブで、**Pseudonym** の **username** 属性を選択します。
7. * 保存 * を選択します。

署名証明書を作成またはインポートします

まだ作成していない場合は、署名証明書を作成またはインポートしてください。

手順

1. **[セキュリティ] > [署名と復号化の鍵と証明書]** 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** 接続を作成する

PingFederate で SP 接続を作成する際、StorageGRID から管理ノード用にダウンロードした SAML メタデータをインポートします。メタデータファイルには、必要な多くの具体的な値が含まれています。



StorageGRID システムの管理ノードごとに SP 接続を作成する必要があります。これにより、ユーザーはどのノードにも安全にサインインおよびサインアウトできます。これらの手順を使用して、最初の SP 接続を作成します。次に、[追加のSP接続を作成する](#)に移動して、必要な追加の接続を作成します。

SP接続タイプの選択

手順

1. **アプリケーション > 統合 > SP Connections** に移動します。
2. 「接続の作成」を選択します。
3. 「この接続にはテンプレートを使用しない」を選択します。
4. プロトコルとして **Browser SSO Profiles** と **SAML 2.0** を選択します。

SPメタデータのインポート

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「SSO設定」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てください。
3. メタデータ概要と「一般情報」タブに記載されている情報を確認してください。

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. **Next** を選択します。

IdPブラウザSSOの設定

手順

1. ブラウザSSOタブから、*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-initiated SSO**、**SP-initial SLO**、**IdP-initiated SSO**、*IdP-initiated SLO* のオプションを選択します。
3. **Next** を選択します。
4. 「アサーションの有効期間」タブでは、何も変更しないでください。
5. 「アサーション作成」タブで、「アサーション作成の設定」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. 属性契約タブで、属性契約として **SAML_SUBJECT** を使用し、インポートされた未指定の名前形式を使用します。
6. 契約を延長する場合は、*削除*を選択して、使用されていない `urn:oid` を削除します。

マップアダプタインスタンス

手順

1. 「Authentication Source Mapping」タブで、「Map New Adapter Instance」を選択します。
2. アダプターインスタンスタブで、作成した[アダプターインスタンス](#)を選択します。
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. 「Attribute Source & User Lookup」タブで、「Add Attribute Source」を選択します。
5. データ ストア タブで、説明を入力し、追加した [データストア](#) を選択します。
6. LDAP ディレクトリ検索タブで：
 - *ベースDN*を入力してください。この値は、LDAPサーバのStorageGRIDに入力した値と完全に一致する必要があります。
 - 検索範囲として、*サブツリー*を選択します。
 - ルートオブジェクトクラスの場合、次の属性のいずれかを検索して追加します：**objectGUID** または **userPrincipalName**。
7. 「LDAP Binary Attribute Encoding Types」タブで、**objectGUID** 属性に対して **Base64** を選択します。
8. LDAPフィルタータブで、**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** または **userPrincipalName** を選択します。
10. 属性ソースを確認してから保存してください。
11. 「Failsave Attribute Source」タブで、「SSO トランザクションを中止する」を選択します。
12. 概要を確認し、*完了*を選択します。
13. 「完了」を選択します。

プロトコル設定を構成する

手順

1. **SP接続** > ブラウザー **SSO** > プロトコル設定 タブで、プロトコル設定の構成 を選択します。
2. 「アサーション コンシューマー 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（バインディングの場合は **POST**、エンドポイント URL の場合は /api/saml-response）をそのまま使用します。
3. SLO 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（バインディングの場合は **REDIRECT**、エンドポイント URL の場合は /api/saml-logout）をそのまま使用します。
4. 「許可されたSAMLバインディング」タブで、**ARTIFACT** と **SOAP** のチェックを外します。**POST** と **REDIRECT** のみが必須です。
5. 「署名ポリシー」タブで、「認証要求に署名を要求する」と「常にアサーションに署名する」のチェックボックスをオンにしたままにします。
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、*完了*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の 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、**Credentials** を選択します。
2. 「認証情報」タブから「認証情報の構成」を選択します。
3. 作成またはインポートした署名証明書を選択します。
4. 次へ を選択して 署名検証設定の管理 に進みます。
 - a. 「信頼モデル」タブで、「アンカーなし」を選択します。
 - b. 署名検証証明書タブで、StorageGRID SAMLメタデータからインポートされ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接続を作成する

最初の SP 接続をコピーして、グリッド内の各管理ノードに必要な SP 接続を作成できます。各コピー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、署名検証、および SLO 応答 URL を除き、同一の設定が使用されます。

手順

1. 追加の管理ノードごとに最初の SP 接続のコピーを作成するには、アクション > コピー を選択します。
2. コピー先の接続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てください。
 - c. **Next** を選択します。
 - d. *保存*を選択します。
4. 未使用の属性が原因で発生するエラーを解決します。
 - a. 新しい接続を選択します。
 - b. 「Configure Browser SSO」 > 「Configure Assertion Creation」 > 「Attribute Contract」を選択します。
 - c. **urn:oid** のエントリを削除します。
 - d. *保存*を選択します。

StorageGRIDでSSOを無効にする

この機能の使用を中止する場合は、シングル サインオン (SSO) を無効にすることができます。ID フェデレーションを無効にする前に、シングル サインオンを無効にする必要があります。

開始する前に

- "対応ウェブブラウザ" を使用して Grid Manager にサインインしています。
- "特定のアクセス権限"があります。

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。

シングル サインオン ページが表示されます。

2. 「SSO を無効にする」を選択します。
3. 「はい」を選択します。

ローカルユーザー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。

次回 StorageGRID にサインインするときは、StorageGRID のサインイン ページが表示され、ローカルまたはフェデレーション StorageGRID ユーザーのユーザー名とパスワードを入力する必要があります。

StorageGRID 管理ノードの SSO を一時的に無効にして再度有効にします

シングル サインオン (SSO) システムがダウンすると、Grid Manager にサインインできない場合があります。この場合、1つの管理ノードに対してSSOを一時的に無効化してから再度有効化することができます。SSOを無効化してから再度有効化するには、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。

開始する前に

- "特定のアクセス権限"があります。
- あなたは `Passwords.txt` ファイルを持っています。

- ローカルrootユーザーのパスワードを把握する必要があります。

タスク概要

1つの管理ノードでSSOを無効にした後、ローカルのrootユーザーとしてグリッドマネージャーにサインインできます。StorageGRIDシステムのセキュリティを確保するには、サインアウト後すぐに、ノードのコマンドシェルを使用して管理ノードでSSOを再度有効にする必要があります。



1つの管理ノードの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。グリッドマネージャーのシングルサインオンページにある「SSOを有効にする」チェックボックスは選択されたままになり、既存のSSO設定は更新しない限りすべて維持されます。

手順

1. 管理ノードにログインします。

- 次のコマンドを入力します：`ssh admin@Admin_Node_IP`
- `Passwords.txt` ファイルに記載されているパスワードを入力してください。
- 以下のコマンドを入力して `root` に切り替えます：`su -`
- `Passwords.txt` ファイルに記載されているパスワードを入力してください。

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

2. 次のコマンドを実行します。 `disable-saml`

このコマンドはこの管理ノードのみに適用されることを示す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。

シングルサインオンがノード上で無効になっていることを示すメッセージが表示されます。

4. ウェブブラウザから、同じ管理ノード上のグリッドマネージャーにアクセスします。

SSOが無効になっているため、Grid Managerのサインインページが表示されています。

5. ユーザー名 `root` とローカル `root` ユーザーのパスワードを使用してサインインしてください。

6. SSO構成を修正する必要があるため、一時的にSSOを無効にした場合：

- 設定 > アクセス制御 > シングルサインオン を選択します。
- 誤った、または古いSSO設定を変更してください。
- * 保存 * を選択します。

シングルサインオン ページで「保存」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. 何らかの理由でグリッドマネージャーにアクセスする必要があるため、一時的にSSOを無効にした場合：

- 必要な作業を何でも実行してください。
- 「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。以下のいずれかの手順を実行してください。

- 次のコマンドを実行します。 `enable-saml`

このコマンドはこの管理ノードのみに適用されることを示す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。

メッセージは、シングル サインオンがノード上で有効になっていることを示しています。

- グリッドノードを再起動します： `reboot`

8. ウェブブラウザから、同じ管理ノードの Grid Manager にアクセスします。

9. StorageGRID のサインイン ページが表示され、Grid Manager にアクセスするにはシングル サインオンの認証情報を入力する必要があることを確認してください。

グリッドフェデレーションを使用する

StorageGRID グリッド フェデレーションについて学ぶ

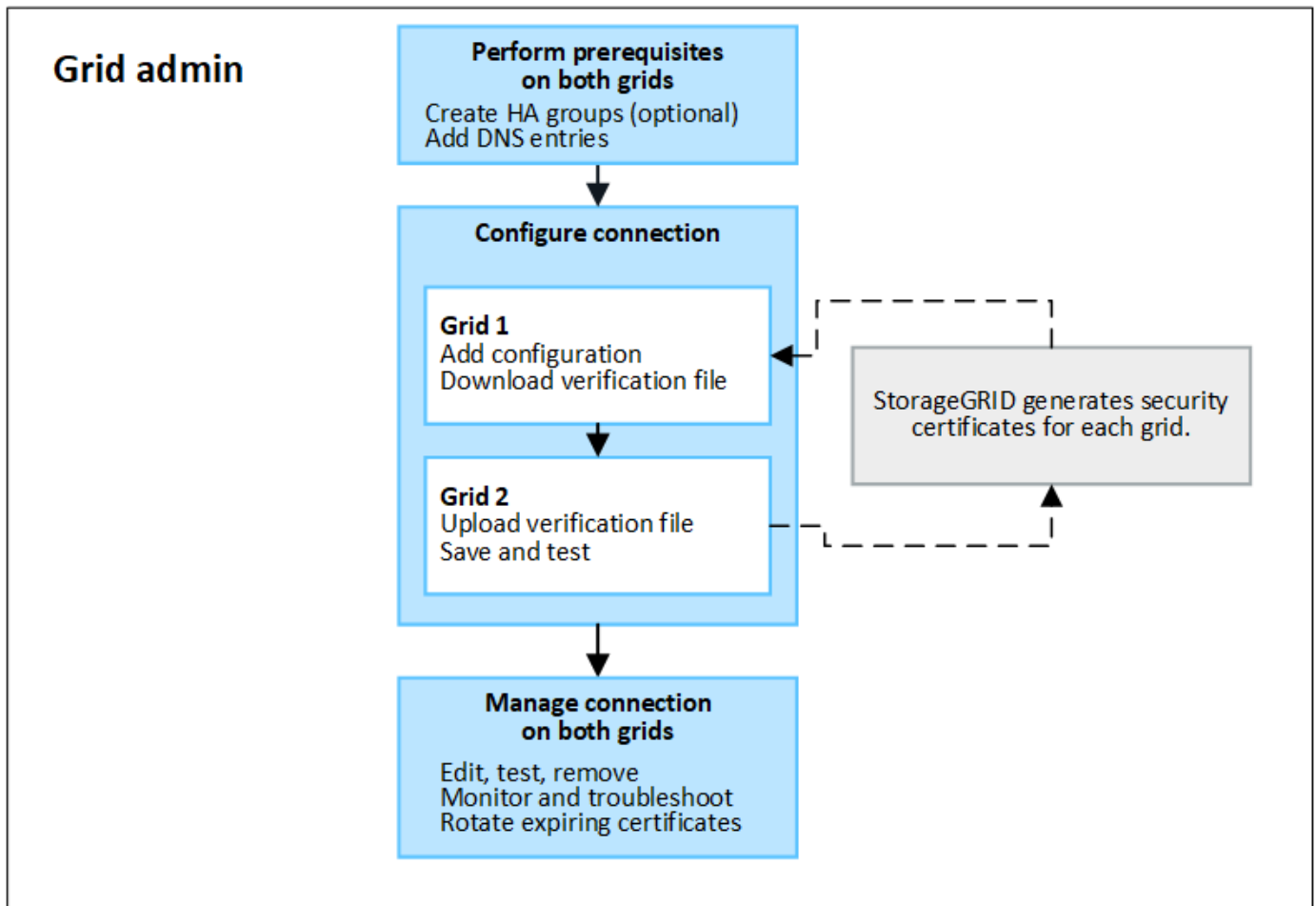
グリッドフェデレーションを使用すると、テナントを複製し、ディザスタリカバリのために2つの StorageGRID システム間でオブジェクトをレプリケートできます。

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間の双方向の信頼できる安全な接続です。

グリッド連携のためのワークフロー

ワークフロー図は、2つのグリッド間でグリッド連携接続を構成する手順をまとめたものです。



グリッド連携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グリッドは、同一バージョン、またはメジャーバージョンの差が1つ以下の StorageGRID バージョンを実行している必要があります。

バージョン要件の詳細については、"[リリース ノート](#)"を参照してください。NetAppアカウントでサインインするか、アカウントを作成してリリースノートにアクセスする必要があります。

- グリッドは、他のグリッドと1つ以上のグリッド連携接続を持つことができます。各グリッド連携接続は、他の接続とは独立しています。例えば、Grid 1がGrid 2と1つの接続を持ち、Grid 3ともう1つの接続を持つ場合、Grid 2とGrid 3の間には暗黙の接続は存在しません。
- グリッド連携接続は双方向です。接続が確立された後は、どちらのグリッドからでも接続を監視および管理できます。
- "[アカウントクローン](#)"または"[グリッド間複製](#)"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つ存在する必要があります。

ネットワークおよび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上で発生する可能性があります。
- グリッド連携接続とは、あるグリッドと別のグリッドを接続するものです。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、他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。

- ベストプラクティスは、各グリッドのゲートウェイノードと管理ノードの**"高可用性 (HA) グループ"**を接続することです。HAグループを使用することで、ノードが利用不能になった場合でも、グリッド連携接続がオンライン状態を維持できます。いずれかのHAグループ内のアクティブなインターフェースに障害が発生した場合、接続はバックアップインターフェースを使用できます。
- 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。ノードが利用不能になると、グリッドフェデレーション接続も利用不能になります。
- **"クロスグリッド複製"**オブジェクトを扱うには、各グリッド上のストレージノードが、他のグリッド上の構成済み管理ノードとゲートウェイノードにアクセスする必要があります。各グリッドについて、すべてのストレージノードが、接続に使用される管理ノードまたはゲートウェイノードへの高帯域幅の経路を持っていることを確認してください。

FQDNを使用して接続の負荷分散を行う

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

- Grid 1 の FQDN は、Grid 1 内の HA グループの 1 つ以上の仮想 IP (VIP) アドレス、または Grid 1 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されます。
- Grid 2 の FQDN は、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もしくはゲートウェイノードの IP アドレスにマッピングされます。

複数のDNSエントリを使用する場合、接続を使用するリクエストは次のように負荷分散されます。

- 複数のHAグループのVIPアドレスにマッピングされるDNSエントリは、HAグループ内のアクティブな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るDNSエントリは、マッピングされたノード間で負荷分散されます。

ポートの要件

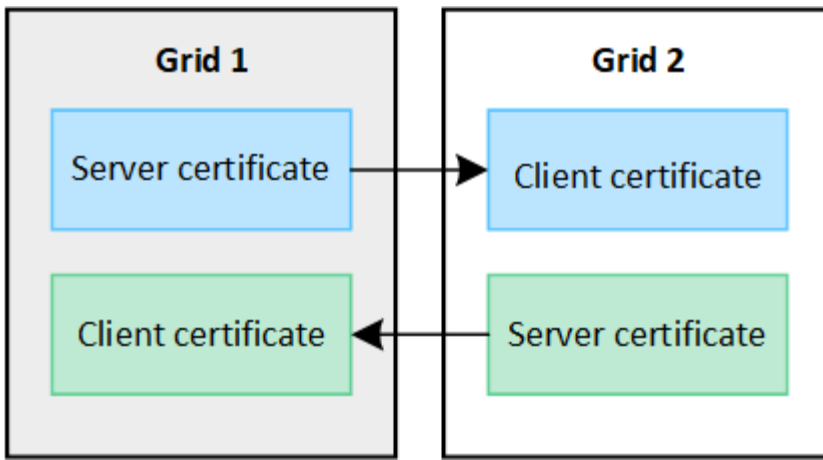
グリッドフェデレーション接続を作成する際、23000から23999までの未使用のポート番号を指定できます。この接続における両方のグリッドは、同じポートを使用します。

どちらのグリッド内のノードも、このポートを他の接続に使用しないようにしてください。

証明書の要件

グリッドフェデレーション接続を構成すると、StorageGRID は SSL 証明書を 4 つ自動的に生成します。

- 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ー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ー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、*グリッドフェデレーション証明書の有効期限切れ*アラートが表示され、証明書のローテーションを促します。証明書のローテーションは、Grid Manager を使用して行うことができます。



接続の両端にある証明書の有効期限が切れると、接続は機能しなくなります。証明書が更新されるまで、データの複製は保留状態となります。

詳細情報

- ["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の管理"](#)
- ["グリッドフェデレーションのエラーをトラブルシューティングする"](#)

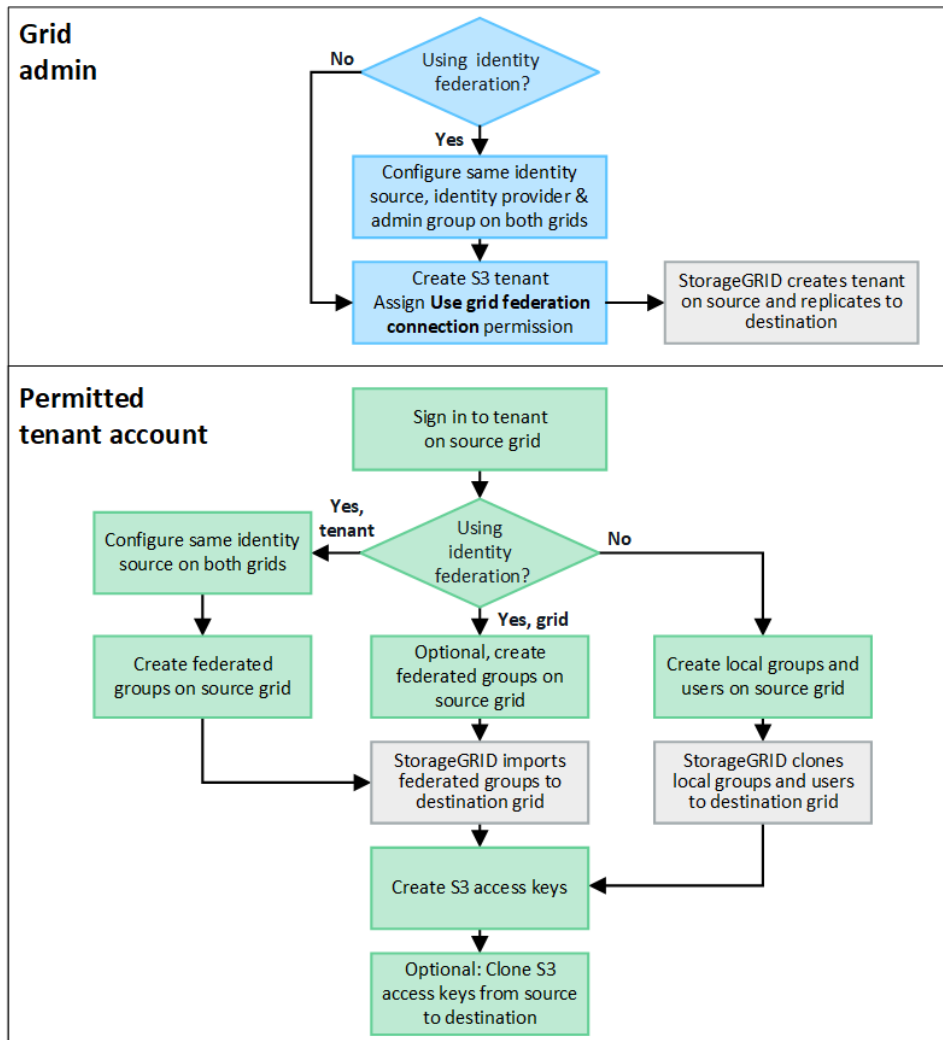
StorageGRIDのアカウントクローンについて学ぶ

アカウントクローンとは、["グリッドフェデレーション接続"](#)内のStorageGRIDシステム間で、テナントアカウント、テナントグループ、テナントユーザー、およびオプションでS3アクセスキーを自動的に複製することです。

["グリッド間複製"](#)にはアカウントのクローン作成が必要です。ソース StorageGRID システムからデスティネーション StorageGRID システムにアカウント情報をクローニングすることで、テナントのユーザーと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も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

ワークフロー図は、グリッド管理者と許可されたテナントがアカウント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、["グリッドフェデレーション接続が設定されています"](#)の後に実行されます。



グリッド管理ワークフロー

"[グリッドフェデレーション接続](#)"内のStorageGRIDシステムがシングル サインオン（SSO）またはIDフェデレーションを使用しているかどうかによって、グリッド管理者が実行する手順は異なります。

アカウントクローン用の**SSO**を設定する（オプション）

グリッド連携接続内のいずれかの StorageGRID システムが SSO を使用する場合、両方のグリッドで SSO を使用する必要があります。グリッド連携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は、以下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IDソースを設定します。["IDフェデレーションを使用する"](#)を参照してください。
2. 両方のグリッドに対して、同じ SSO ID プロバイダー（IdP）を設定してください。["シングル サインオンを設定する"](#)を参照してください。
3. ["同じ管理者グループを作成する"](#)同じフェデレーテッドグループをインポートすることで、両方のグリッドに反映されます。

テナントを作成する際に、このグループを選択して、送信元テナントアカウントと宛先テナントアカウントの両方に対して、初期ルートアクセス権限を付与します。



テナントを作成する前にこの管理グループが両方のグリッドに存在しない場合、テナントは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IDフェデレーションを設定する（オプション）

いずれかの StorageGRID システムが SSO なしの ID フェデレーションを使用する場合、両方のグリッドで ID フェデレーションを使用する必要があります。グリッド連携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は、以下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IDソースを設定します。["IDフェデレーションを使用する"](#)を参照してください。
2. オプションとして、フェデレーテッドグループがソースおよび宛先テナントアカウントの両方に対して初期ルートアクセス権限を持つ場合、同じフェデレーテッドグループをインポートすることで、["同じ管理者グループを作成する"](#)両方のグリッドに反映されます。



両方のグリッドに存在しないフェデレーショングループにルートアクセス権限を割り当てた場合、テナントは宛先グリッドに複製されません。

3. フェデレーショングループに両方のアカウントの初期ルートアクセス権限を持たせたくない場合は、ローカルルートユーザーのパスワードを指定してください。

許可されたS3テナントアカウントを作成する

オプションで SSO または ID フェデレーションを設定した後、グリッド管理者は、どのテナントがバケットオブジェクトを他の StorageGRID システムに複製できるかを判断するために、以下の手順を実行します。

手順

1. テナントのアカウント複製操作におけるソースグリッドとして、どのグリッドを使用するかを決定します。

テナントが最初に作成されたグリッドは、テナントの_ソースグリッド_と呼ばれます。テナントが複製されるグリッドは、テナントの_デスティネーショングリッド_と呼ばれます。

2. そのグリッド上で、新しいS3テナントアカウントを作成するか、既存のアカウントを編集します。
3. 「グリッドフェデレーション接続を使用する」権限を割り当てます。
4. テナントアカウントが独自のフェデレーションユーザーを管理する場合は、「独自のIDソースを使用する」権限を割り当ててください。

この権限が割り当てられている場合、フェデレーショングループを作成する前に、送信元と宛先のテナントアカウントの両方で同じIDソースを設定する必要があります。ソーステナントに追加されたフェデレーショングループは、両方のグリッドが同じIDソースを使用しない限り、宛先テナントに複製できません。

5. 特定のグリッド連携接続を選択してください。
6. 新規または変更されたテナントを保存します。

「グリッドフェデレーション接続を使用する」権限を持つ新しいテナントが保存されると、StorageGRID は次のとおり、そのテナントのレプリカを別のグリッド上に自動的に作成します。

- 両方のテナントアカウントは、同じアカウントID、名前、ストレージクォータ、および割り当てられた権限を持っています。
- テナントに対してルート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、そのグループは宛先テナントに複製されます。
- テナントに対してルートアクセス権限を持つローカルユーザーを選択した場合、そのユーザーは宛先テナントに複製されます。ただし、そのユーザーのパスワードは複製されません。

詳細については、"[グリッドフェデレーションの許可されたテナントを管理する](#)"を参照してください。

許可されたテナントアカウントのワークフロー

*グリッドフェデレーション接続の使用*権限を持つテナントが宛先グリッドにレプリケートされた後、許可されたテナントアカウントは、テナントグループ、ユーザー、およびS3アクセスキーをクローンするために、以下の手順を実行できます。

手順

1. テナントのソースグリッド上で、テナントアカウントにサインインしてください。
2. 許可されている場合は、送信元および宛先テナントアカウントの両方でIDフェデレーションを設定します。
3. ソーステナント上にグループとユーザーを作成します。

ソーステナントで新しいグループまたはユーザーが作成されると、StorageGRID は自動的にそれらを宛先テナントにクローンしますが、宛先からソースへのクローンは行われません。

4. S3アクセスキーを作成します。
5. 必要に応じて、ソーステナントから宛先テナントへ S3 アクセスキーを複製します。

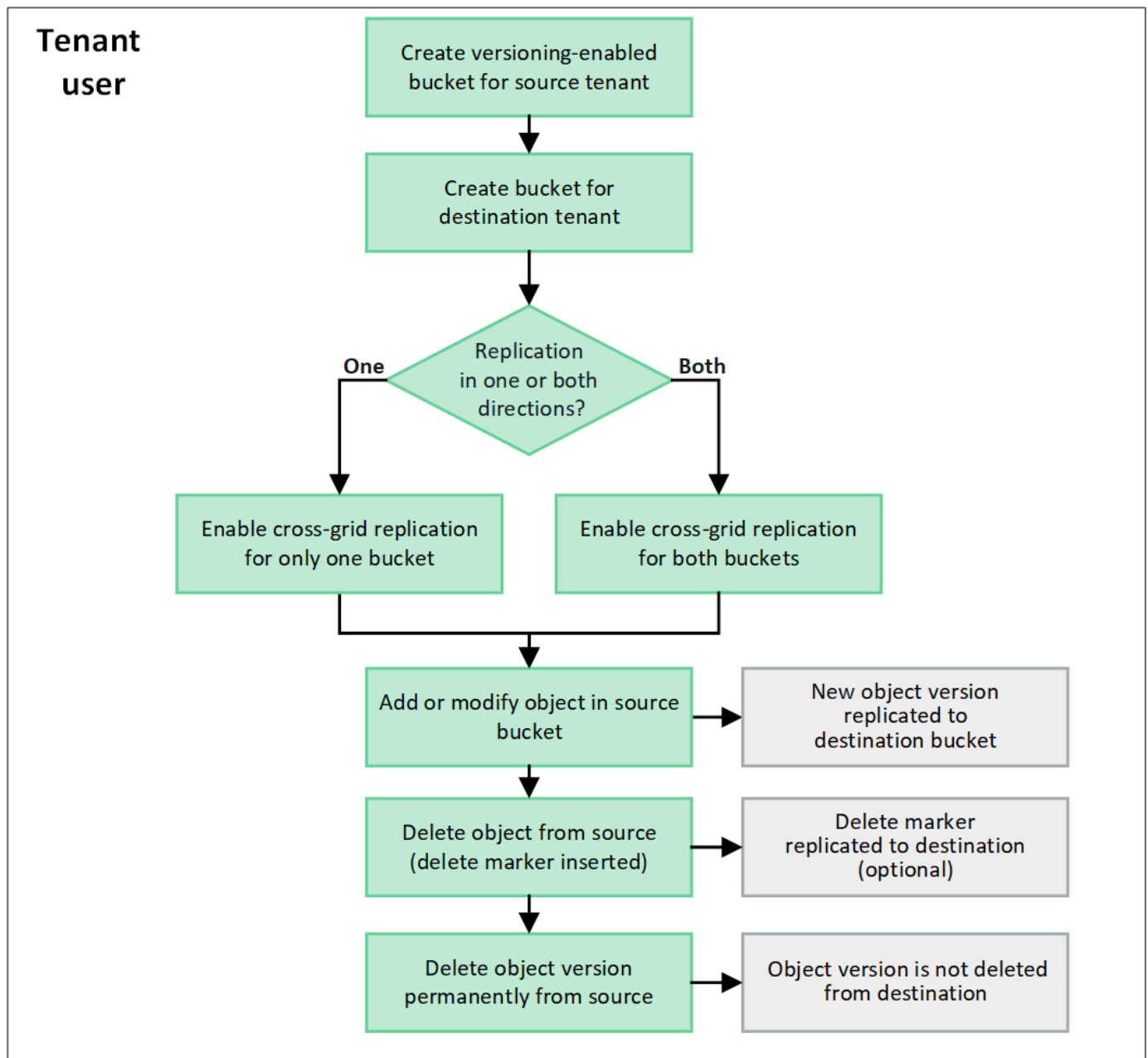
許可されたテナントアカウントのワークフローの詳細、およびグループ、ユーザー、S3 アクセスキーのクローン方法については、"[テナントグループとユーザーを複製する](#)"および"[APIを使用してS3アクセスキーを複製する](#)"を参照してください。

StorageGRID のクロスグリッドレプリケーションについて学ぶ

クロスグリッドレプリケーションとは、"[グリッドフェデレーション接続](#)"で接続された 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機能です。"[アカウントの複製](#)"は、クロスグリッドレプリケーションに必要です。

クロスグリッドレプリケーションのワークフロー

ワークフロー図は、2つのグリッド上のバケット間でクロスグリッドレプリケーションを構成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 グリッドフェデレーション接続を使用する 権限があり、1つ以上の"[グリッドフェデレーション接続](#)"を使用できる場合、ルートアクセス権限を持つテナントユーザーは、各グリッド上の対応するテナントアカウントにバケットを作成できます。これらのバケット：

- それぞれ異なる名前を持つことができます
- 異なるリージョンを持つことができます
- バージョン管理が有効になっている必要があります
- 空欄にする必要があります

両方のバケットが作成された後、どちらか一方、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。

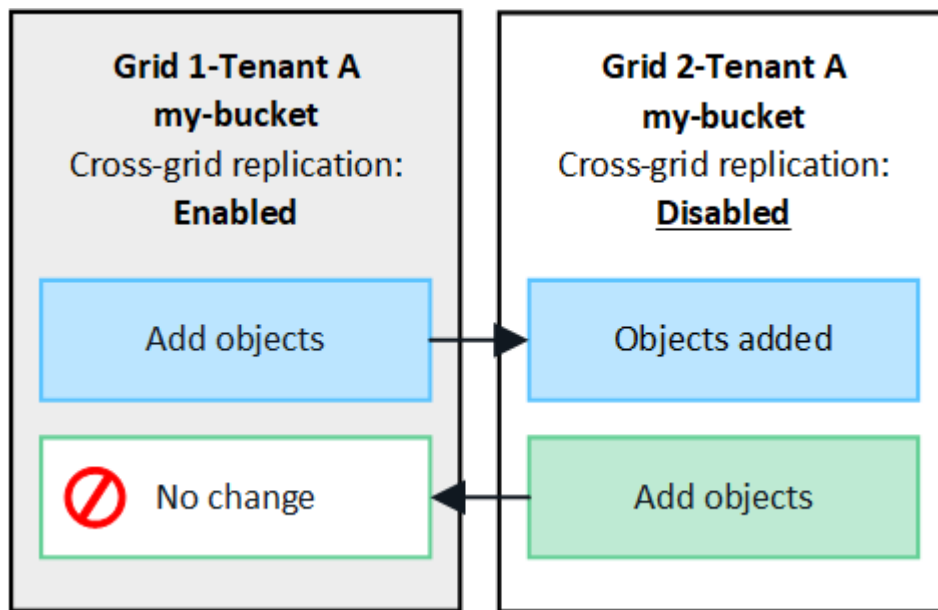
"クロスグリッドレプリケーションを管理する"

クロスグリッドレプリケーションの仕組み

クロスグリッドレプリケーションは、一方向または双方向で実行するように設定できます。

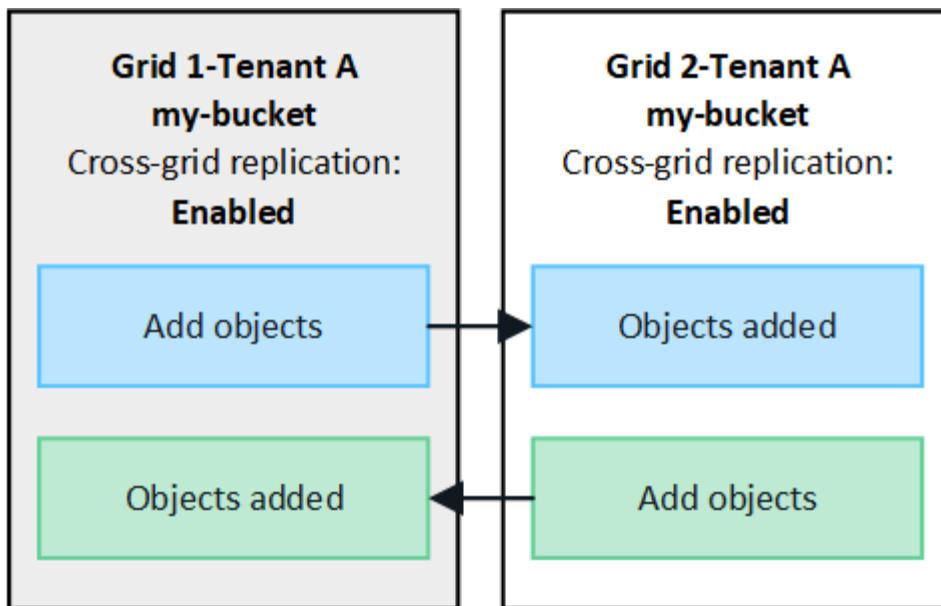
一方向への複製

一方のグリッド上のバケットに対してのみクロスグリッドレプリケーションを有効にした場合、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は、もう一方のグリッド上の対応するバケット（宛先バケット）に複製されます。ただし、宛先バケットに追加されたオブジェクトは、ソースには複製されません。図では、`my-bucket` に対してGrid 1からGrid 2へのクロスグリッドレプリケーションが有効になっていますが、逆方向では有効になっていません。



双方向の複製

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、いずれかのバケットに追加されたオブジェクトは、もう一方のグリッドにも複製されます。図では、`my-bucket` に対してクロスグリッドレプリケーションが両方向で有効になっています。



オブジェクトが取り込まれると何が起きますか？

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、次のことが起きます：

1. StorageGRID は、ソースバケットから宛先バケットへオブジェクトを自動的に複製します。このバックグラウンドレプリケーション操作の実行時間は、保留中の他のレプリケーション操作の数など、いくつかの要因によって異なります。

S3クライアントは、GetObjectまたはHeadObjectリクエストを発行することで、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 `x-ntap-sg-cgr-replication-status` レスポンスヘッダーが含まれており、以下のいずれかの値を持ちます：

Grid	レプリケーションステータス
ソース	• 完了：すべてのグリッド接続でレプリケーションが正常に完了しました。 • PENDING：オブジェクトが少なくとも 1 つのグリッド接続にレプリケートされていません。 • FAILURE：いずれのグリッド接続についてもレプリケーションが保留されておらず、少なくとも1つの接続が永続的な障害で失敗しました。ユーザーはエラーを解決する必要があります。
デスティネーション	レプリカ：オブジェクトはソースグリッドから複製されました。



StorageGRID は `x-amz-replication-status` ヘッダーをサポートしていません。

2. StorageGRID は、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。これは、他のオブジェクトを管理するのと同様です。例えば、グリッド 1 上のオブジェクト A は 2 つの複製コピーとして保存され、永久に保持される一方、グリッド 2 に複製されたオブジェクト A のコピーは 2+1 イレイジャー コーディングを使用して保存され、3 年後に削除される場合があります。

オブジェクトが削除されるとどうなりますか？

"[データフローを削除する](#)"に記載されているとおり、StorageGRID がオブジェクトを削除できる理由は次のとおりです：

- S3クライアントが削除リクエストを発行します。
- テナントマネージャーのユーザーが "[バケット内のオブジェクトを削除する](#)" オプションを選択して、バケットからすべてのオブジェクトを削除します。
- バケットにはライフサイクル設定があり、有効期限が設定されています。
- 当該オブジェクトに対するILMルールの最後の期間が終了し、それ以上の配置は指定されていません。

StorageGRID がバケット内のオブジェクトの削除操作、バケットのライフサイクルの期限切れ、または ILM 配置の期限切れによってオブジェクトを削除した場合、グリッドフェデレーション接続内の他のグリッドから複製されたオブジェクトは削除されません。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クーは、オプションで宛先バケットに複製することができます。

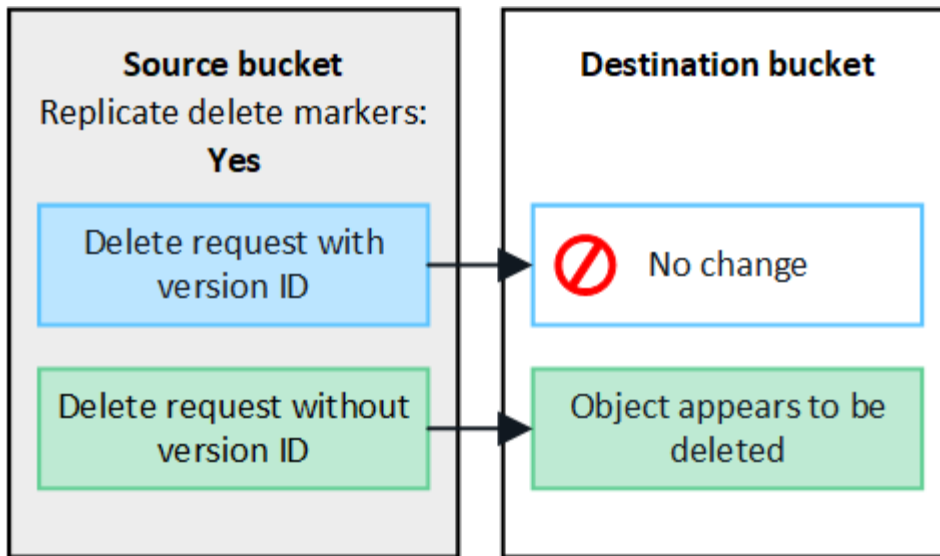
クロスグリッドレプリケーションが有効になっているバケットから S3 クライアントがオブジェクトを削除した場合の動作を理解するには、バージョン管理が有効になっているバケットから S3 クライアントがオブジェクトを削除する方法を以下のとおり確認してください：

- S3クライアントがバージョンIDを含む削除リクエストを発行した場合、そのバージョンのオブジェクトは完全に削除されます。バケットに削除マークーは追加されません。
- S3クライアントがバージョンIDを含まない削除リクエストを発行した場合、StorageGRID はオブジェクトのバージョンを削除しません。その代わりに、バケットに削除マークーを追加します。削除マークーにより、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 GetObject リクエストは失敗します。404 No Object Found
 - 有効なバージョンIDを指定したGetObjectリクエストは成功し、要求されたオブジェクトバージョンを返します。

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 は削除要求を宛先に複製するかどうかを以下のように決定します。

- 削除リクエストにバージョンIDが含まれている場合、そのオブジェクトバージョンは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を含む削除リクエスト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はデスティネーションから削除されません。
- 削除リクエストにバージョン ID が含まれていない場合、StorageGRID はバケットのクロスグリッドレプリケーションの設定方法に応じて、削除マークーを任意で複製できます。
 - 削除マークーを複製することを選択した場合（デフォルト）、削除マークーはソースバケットに追加され、宛先バケットに複製されます。事実上、そのオブジェクトは両方のグリッド上で削除されたように見えます。
 - 削除マークーを複製しないように選択した場合、削除マークーはソースバケットに追加されますが、宛先バケットには複製されません。つまり、ソースグリッドで削除されたオブジェクトは、宛先グリッドでは削除されません。

図では、*削除マークーの複製*は"[グリッド間レプリケーションが有効になりました](#)"のときに*はい*に設定されていました。バージョンIDを含むソースバケットへの削除リクエストは、宛先バケットからオブジェクトを削除しません。バージョンIDを含まないソースバケットへの削除リクエストは、宛先バケット内のオブジェクトを削除するように見えます。



オブジェクトの削除をグリッド間で同期させたい場合は、両方のグリッドのバケットに対応する["S3ライフサイクル構成"](#)を作成してください。

暗号化されたオブジェクトがどのように複製されるか

クロスグリッド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複製する場合、個々のオブジェクトを暗号化したり、デフォルトのバケット暗号化を使用したり、グリッド全体の暗号化を設定したりできます。バケットのクロスグリッドレプリケーションを有効にする前でも後でも、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、オブジェクトをソースバケットに追加する際に、SSE（StorageGRIDが管理するキーを使用したサーバー側暗号化）を使用できます。`x-amz-server-side-encryption`リクエストヘッダーを使用して、`AES256`を指定します。["サーバー側暗号化を使用する"](#)を参照してください。



SSE-C（顧客提供の鍵を使用したサーバー側暗号化）は、クロスグリッド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。

バケットのデフォルト暗号化を使用するには、PutBucketEncryption リクエストを使用して、SSEAlgorithm パラメータを AES256 に設定します。バケットレベルの暗号化は、x-amz-server-side-encryption リクエストヘッダーなしで取り込まれたオブジェクトに適用されます。["バケットに対する操作"](#)を参照してください。

グリッドレベルの暗号化を使用するには、「保存オブジェクトの暗号化」オプションを「AES-256」に設定してください。グリッドレベルの暗号化は、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 `x-amz-server-side-encryption` リクエストヘッダーなしで取り込まれたオブジェクトに適用されます。["ネットワークとオブジェクトのオプションを設定する"](#)を参照してください。



SSEはAES-128をサポートしていません。ソースグリッドで*保存オブジェクトの暗号化*オプションが*AES-128*オプションを使用して有効になっている場合、AES-128アルゴリズムの使用は複製されたオブジェクトには反映されません。代わりに、複製されたオブジェクトは、利用可能であれば、宛先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を使用します。

ソースオブジェクトを暗号化する方法を決定する際、StorageGRID は以下のルールを適用します。

1. `x-amz-server-side-encryption` 取り込みヘッダーが存在する場合は、それを使用します。
2. インジェストヘッダーが存在しない場合は、バケットのデフォルトの暗号化設定が構成されていれば、それを使用します。
3. バケット設定が構成されていない場合は、グリッド全体の暗号化設定が構成されていれば、それを使用します。
4. グリッド全体の設定が存在しない場合は、ソースオブジェクトを暗号化しません。

複製されたオブジェクトを暗号化する方法を決定する際、StorageGRID は以下のルールをこの順序で適用します：

1. ソースオブジェクトがAES-128暗号化を使用していない限り、ソースオブジェクトと同じ暗号化方式を使用してください。
2. ソースオブジェクトが暗号化されていない場合、またはAES-128を使用している場合は、設定されていれば宛先バケットのデフォルトの暗号化設定を使用します。
3. 宛先バケットに暗号化設定がない場合は、宛先のグリッド全体の暗号化設定が構成されていれば、それを使用します。
4. グリッド全体の設定が存在しない場合は、宛先オブジェクトを暗号化しません。

S3オブジェクトロックを使用したクロスグリッドレプリケーション

以下の状況下では、S3 オブジェクトロックが有効になっている StorageGRID バケット間のクロスグリッドレプリケーションを設定できます。

ソースバケットの S3 オブジェクトロックが有効になっている場合...	そして、宛先バケットの S3 オブジェクトロックは...
有効	有効
無効	有効

ソースバケットでS3オブジェクトロックが有効になっている場合：

- オブジェクトは、以下の順序で宛先の保持設定によりロックされます：

- a. ソースオブジェクトの保持ヘッダー値：

`x-amz-object-lock-mode`

`x-amz-object-lock-retain-until-date`

- b. ソースバケットのデフォルトの保持期間（設定されている場合）。
- c. 宛先バケットのデフォルトの保持期間（設定されている場合）。

宛先バケットのデフォルトの保持設定は、ソースオブジェクトから複製された保持設定を上書きしません。

- 宛先オブジェクトの法的保留ステータスは、オブジェクトをアップロードする際に `x-amz-object-lock-legal-hold` を使用して設定できます。

- 宛先テナントまたはバケットが、ソースオブジェクトの S3 オブジェクトロック設定をサポートしていない場合、エラーが発生します。参照先：["グリッド間レプリケーションに関するアラートとエラー。"](#)

ソースバケットのS3オブジェクトロックが無効になっている場合：

- 宛先バケットのデフォルトの保持期間を設定することで、S3 Object Lockの保持設定を宛先オブジェクトに適用できます。
- 宛先オブジェクトは法的保留状態を設定できません。

PutObjectTagging と **DeleteObjectTagging** はサポートされていません

PutObjectTagging および DeleteObjectTagging リクエストは、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に対してはサポートされていません。

S3クライアントがPutObjectTaggingまたはDeleteObjectTaggingリクエストを発行すると、`501 Not Implemented`が返されます。メッセージは `Put(Delete) ObjectTagging isn't available for buckets that have cross-grid replication configured` です。

PutObjectRetention と **PutObjectLegalHold** はサポートされていません

PutObjectRetention および PutObjectLegalHold リクエストは、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に対して完全にはサポートされていません。

S3クライアントがPutObjectRetentionまたはPutObjectLegalHoldリクエストを発行すると、ソースオブジェクトの設定は変更されますが、変更内容は宛先には適用されません。

分割されたオブジェクトがどのように複製されるか

ソースグリッドの最大セグメントサイズは、宛先グリッドに複製されるオブジェクトに適用されます。オブジェクトが別のグリッドに複製される場合、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。例えば、ソースグリッドの最大セグメントサイズが 1 GB で、宛先グリッドの最大セグメントサイズが 50 MB だとします。ソースグリッド上で 2 GB のオブジェクトを取り込んだ場合、そのオブジェクトは 1 GB のセグメント 2 つとして保存されます。また、宛先グリッドの最大セグメントサイズは 50 MB であるにもかかわらず、データは 2 つの 1 GB セグメントとして宛先グリッドに複製されます。

StorageGRIDにおけるグリッド間複製とCloudMirror複製の比較

グリッドフェデレーションの使用を開始するにあたり、["グリッド間複製"](#) と ["StorageGRID CloudMirror レプリケーションサービス"](#) の類似点と相違点を確認してください。



クロスグリッドレプリケーションによって複製されたバケットで CloudMirror を使用することはできません。その逆も同様です。

	クロスグリッド複製	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システムは、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双方向にレプリケートできます。	テナントが StorageGRID のバケット（ソース）から外部の S3 バケット（宛先）にオブジェクトを自動的にレプリケートできるようになります。 CloudMirrorレプリケーションは、独立した S3 インフラストラクチャ内にオブジェクトの独立したコピーを作成します。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、クラウド上でさらに処理されます。
どのように設定されているのですか？	2つのグリッド間でグリッドフェデレーション接続を設定します。 - 新しいテナントアカウントを追加すると、自動的に他のグリッドにも複製されます。 - 新しいテナントグループとユーザーを追加すると、それらも複製されます。 - 各グリッドに対応するバケットを作成し、グリッド間のレプリケーションを片方向または両方向で有効にします。	- テナントユーザーは、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、認証情報など）を定義することで、CloudMirror レプリケーションを設定します。 - 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。
誰が設定を担当するのですか？	- グリッド管理者は、接続とテナントを設定します。 - テナントのユーザーは、グループ、ユーザー、キー、およびバケットを設定します。	通常は、テナントユーザーです。
宛先は何ですか？	グリッドフェデレーション接続における、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S3インフラストラクチャ（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、ソースバケットと宛先バケットの両方でオブジェクトバージョニングが有効になっている必要があります。	いいえ、CloudMirrorレプリケーションは、ソースと宛先の両方において、バージョン管理されていないバケットとバージョン管理されたバケットの任意の組み合わせをサポートします。
オブジェクトが移動先に移動される原因は何ですか？	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、オブジェクトは自動的に複製されます。	オブジェクトは、CloudMirror エンドポイントで設定された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 エンドポイントでバケットが設定される前にソースバケットに存在していたオブジェクトは、変更されない限りレプリケートされません。

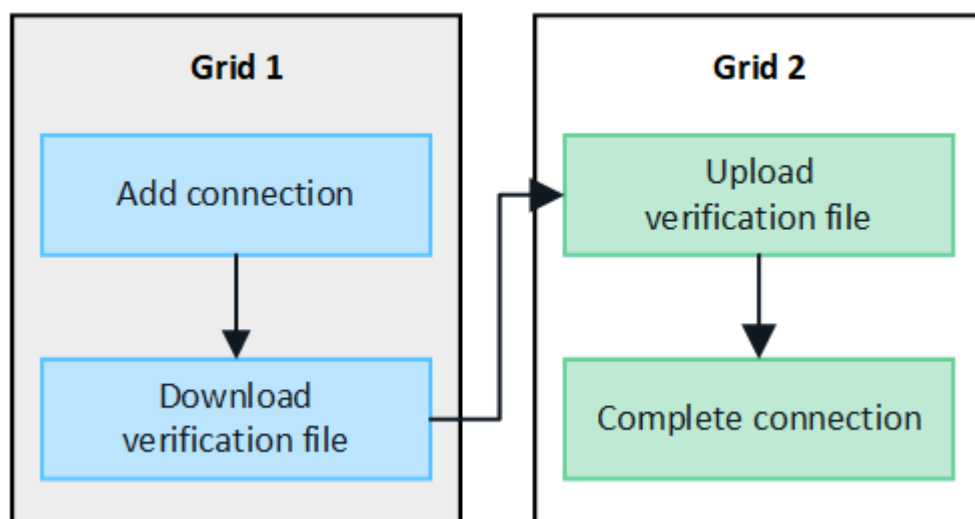
	クロスグリッド複製	CloudMirrorレプリケーションサービス
オブジェクトはどのように複製されるのか？	クロスグリッドレプリケーションはバージョン管理されたオブジェクトを作成し、ソースバケットから宛先バケットにバージョンIDを複製します。これにより、両方のグリッド間でバージョン順序を維持することができます。	CloudMirrorレプリケーションにはバージョン管理が有効になっているバケットは必要ないため、CloudMirrorはサイト内のキーの順序のみを維持できます。異なるサイトにあるオブジェクトへのリクエストに対して、順序が維持される保証はありません。
オブジェクトを複製できない場合はどうすればよいでしょうか？	オブジェクトは、メタデータの保存制限に従って、レプリケーションのためにキューに追加されます。	オブジェクトはレプリケーションのためにキューに入れますが、プラットフォームサービスの制限が適用されます (" プラットフォームサービスの利用に関する推奨事項 "を参照)。
オブジェクトのシステムメタデータは複製されていますか？	はい、オブジェクトが別のグリッドに複製されると、そのシステムメタデータも複製されます。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複製されると、そのシステムメタデータが更新されます。メタデータは、取り込みのタイミングや独立した S3 インフラストラクチャの動作によって、場所ごとに異なります。
オブジェクトはどのように取得されますか？	アプリケーションは、いずれかのグリッド上のバケットにリクエストを送信することで、オブジェクトを取得または読み取ることができます。	アプリケーションは、StorageGRID または S3 宛先にリクエストを送信することで、オブジェクトを取得または読み取ることができます。たとえば、CloudMirror レプリケーションを使用してオブジェクトをパートナー組織に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 宛先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 の使用は必須ではありません。

	クロスグリッド複製	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、どうなりますか？	- バージョンIDを含む削除リクエストは、宛先グリッドには複製されません。 - バージョンIDを含まない削除リクエストは、ソースバケットに削除マーカを追加します。このマーカは、必要に応じて宛先グリッド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一方のみに設定されている場合、宛先バケット内のオブジェクトはソースに影響を与えることなく削除できます。	結果は、ソースバケットと宛先バケットのバージョン管理状態によって異なります（両者が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されている場合、削除リクエストを実行すると、両方の場所に削除マーカが追加されます。 - ソースバケットのみがバージョン管理されている場合、削除リクエストを実行すると、ソースには削除マーカが追加されますが、宛先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されていない場合、削除リクエストはソースからはオブジェクトを削除しますが、宛先からは削除しません。 同様に、宛先バケット内のオブジェクトは、ソースに影響を与えることなく削除できます。

StorageGRID 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 システム間で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、グリッドフェデレーション接続の作成には、両方のグリッド上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成させます。どちらのグリッドからでも開始できます。



開始する前に

- グリッドフェデレーション接続を設定するための["考慮事項と要件"](#)を確認しました。

- 各グリッドにIPアドレスやVIPアドレスの代わりに完全修飾ドメイン名（FQDN）を使用する予定であれば、使用すべき名前を把握しており、各グリッドのDNSサーバーに適切なエントリが登録されていることを確認済みです。
- あなたは"対応ウェブブラウザ"を使用しています。
- 両方のグリッドに対するルートアクセス権限とプロビジョニングパスフレーズを持っています。

接続を追加する

2つの StorageGRID システムのいずれかで、以下の手順を実行してください。

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グリッドマネージャーにサインインしてください。
2. 設定 > システム > グリッド連携 を選択します。
3. 「接続を追加」を選択します。
4. 接続の詳細を入力してください。

フィールド	説明
接続名	この接続を識別しやすくするための固有の名前（例：「Grid 1-Grid 2」）。
このグリッドのFQDNまたはIPアドレス	次のいずれかが必要： • 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 • 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アドレスは、宛先グリッドが到達できる任意のネットワーク上に存在できます。
ポート	この接続に使用するポート番号。23000から23999までの未使用のポート番号を入力できます。 この接続における両方のグリッドは、同じポートを使用します。どちらのグリッド内のノードも、このポートを他の接続に使用しないようにしてください。
このグリッドの証明書の有効日数	この接続におけるこのグリッドのセキュリティ証明書の有効期間（日数）。デフォルト値は730日（2年）ですが、1日から762日までの任意の値を入力できます。 StorageGRID は、接続を保存すると、各グリッドのクライアント証明書とサーバー証明書を自動的に生成します。
このグリッドのプロビジョニングパスフレーズ	現在ログ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
他のグリッドのFQDNまたはIPアドレス	次のいずれかが必要： • 接続先のグリッドのFQDN • 別のグリッド上のHAグループのVIPアドレス • 相手側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アドレスは、送信元グリッドが到達可能なネットワークであれば、どのネットワーク上にあっても構いません。

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」ステップでは、*検証ファイルのダウンロード*を選択してください。

他のグリッドとの接続が完了すると、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 ((*connection-name.grid-federation*)、安全な場所に保存してください。



このファイルには秘密情報（*としてマスクされています）およびその他の機密詳細が含まれており、安全に保管および送信する必要があります。

8. *閉じる*を選択して、グリッド連携ページに戻ります。
9. 新しい接続が表示され、その*接続ステータス*が*接続待ち*になっていることを確認してください。
10. `connection-name.grid-federation` ファイルを他のグリッドのグリッド管理者に提供してください。

接続の完了

以下の手順を、接続先の StorageGRID システム（もう一方のグリッド）で実行します。

手順

1. プライマリ管理ノードからグリッドマネージャーにサインインしてください。
2. 設定 > システム > グリッド連携 を選択します。
3. 「検証ファイルをアップロード」を選択して、アップロードページにアクセスしてください。
4. *検証ファイルをアップロード*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の有効日数を別の日数で入力してください。*証明書の有効日数*の欄には、最初のグリッドに入力した値がデフォルトで設定されますが、各グリッドには異なる有効期限を設定できます。

一般的には、接続の両側で証明書の有効期間を同じ日数に設定してください。



接続の両端にある証明書の有効期限が切れると、接続は停止し、証明書が更新されるまでレプリケーションは保留状態になります。

6. 現在ログ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てください。
7. 「保存してテスト」を選択します。

証明書が生成され、接続テストが行われます。接続が有効な場合、成功メッセージが表示され、新しい接続がグリッド連携ページに表示されます。*接続ステータス*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、問題に対処してください。["グリッドフェデレーションのエラーをトラブルシューティングする"](#)を参照してください。

8. 最初のグリッドのグリッド連携ページに移動し、ブラウザを更新してください。*接続ステータス*が*接続済み*になっていることを確認してください。
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てください。

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。

終了後の操作

- ["許可されたテナントの管理"](#)の考慮事項を確認してください。
- ["1つ以上の新しいテナントアカウントを作成する"](#)、グリッドフェデレーション接続を使用する 権限を割り当て、新しい接続を選択します。
- ["接続を管理する"](#) 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、または接続の削除を行うことができます。
- ["接続状況を監視する"](#) 通常の StorageGRID 監視活動の一環として。
- ["接続のトラブルシューティング"](#) アカウントクローンやクロスグリッドレプリケーションに関連するアラートやエラーの解決も含まれます。

StorageGRID グリッド フェデレーション接続を管理

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、および未使用の接続の削除が含まれます。

開始する前に

- ["対応ウェブブラウザ"](#) を使用して、いずれかのグリッドの Grid Manager にサインインしています。
- 現在サインインしているグリッドの["ルートアクセス権限"](#)があります。

グリッドフェデレーション接続を編集する

グリッド連携接続を編集するには、接続先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てください。最初のグリッドに変更を加えた後は、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。



接続設定の編集中は、アカウントのクローン作成やクロスグリッドレプリケーションのリクエストは、既存の接続設定を引き続き使用します。最初のグリッドに加えた編集内容は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され、保存され、テストされるまでは使用されません。

接続の編集を開始する

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グリッドマネージャーにサインインしてください。
2. *ノード*を選択し、システム内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てください。



グリッドフェデレーション接続を編集する場合、StorageGRID は最初のグリッド上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*を選択したときに警告メッセージが表示されます。

3. 設定 > システム > グリッド連携 を選択します。
4. グリッド連携ページまたは特定の接続の詳細ページにある「アクション」メニューを使用して、接続の詳細を編集します。入力内容については、["グリッドフェデレーション接続を作成する"](#)を参照してください。

[操作]メニュー

- a. 接続のラジオボタンを選択します。
- b. **Actions > Edit** を選択します。
- c. 新しい情報を入力してください。

詳細ページ

- a. 接続名を選択すると、その詳細が表示されます。
- b. *Edit*を選択します。
- c. 新しい情報を入力してください。

5. ログ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てください。
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、新しい検証ファイルを別のグリッドにアップロードするまでは、接続には適用されません。

7. 「検証ファイルをダウンロード」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アクセスしてください。

8. ダウンロードしたファイルを見つけ ((`connection-name.grid-federation`))、安全な場所に保存してください。



検証ファイルには機密情報が含まれているため、安全に保管および送信する必要があります。

9. *閉じる*を選択して、グリッド連携ページに戻ります。
10. *接続ステータス*が*編集保留中*であることを確認してください。



接続の編集を開始した時点で接続状態が「接続済み」以外だった場合、状態は「編集保留中」には変わりません。

11. ``connection-name.grid-federation`` ファイルを他のグリッドのグリッド管理者に提供してください。

接続の編集を完了する

検証ファイルを別のグリッドにアップロードして、接続の編集を完了してください。

手順

1. プライマリ管理ノードからグリッドマネージャーにサインインしてください。
2. 設定 > システム > グリッド連携 を選択します。
3. アップロードページにアクセスするには、*検証ファイルをアップロード*を選択してください。
4. 「検証ファイルをアップロード」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. 現在ログ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てください。
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が確立できた場合、成功メッセージが表示されます。そうでない場合は、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てください。

7. ウィザードを閉じて、グリッド連携ページに戻ります。
8. *接続ステータス*が*接続済み*であることを確認してください。
9. 最初のグリッドのグリッド連携ページに移動し、ブラウザを更新してください。*接続ステータス*が*接続済み*になっていることを確認してください。
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てください。

グリッドフェデレーション接続をテストする

手順

1. プライマリ管理ノードからグリッドマネージャーにサインインしてください。
2. 設定 > システム > グリッド連携 を選択します。
3. グリッド連携ページの*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。

[操作]メニュー

- a. 接続のラジオボタンを選択します。
- b. **Actions > Test** を選択します。

詳細ページ

- a. 接続名を選択すると、その詳細が表示されます。
- b. 「接続テスト」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
接続済み	両方のグリッドは接続されており、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。例えば、証明書の有効期限が切れている、または設定値が無効になっている場合などが挙げられます。
編集保留中	このグリッド上の接続を編集しましたが、接続は依然として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別のグリッドにアップロードしてください。
接続待ち	このグリッド上での接続設定は完了していますが、もう一方のグリッド上での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てください。
不明	接続状態が不明です。ネットワークの問題、またはノードのオフラインが原因である可能性があります。

5. 接続状態が「エラー」の場合は、問題を解決してください。次に、「接続テスト」を再度選択して、問題が解決したことを確認してください。

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、接続を保護するために4つの自動生成されたSSL証明書を使用します。各グリッドの2つの証明書の有効期限が近づくと、*グリッドフェデレーション証明書の有効期限切れ*アラートが表示され、証明書のローテーションを促されます。



接続の両端にある証明書の有効期限が切れると、接続は停止し、証明書が更新されるまでレプリケーションは保留状態になります。

手順

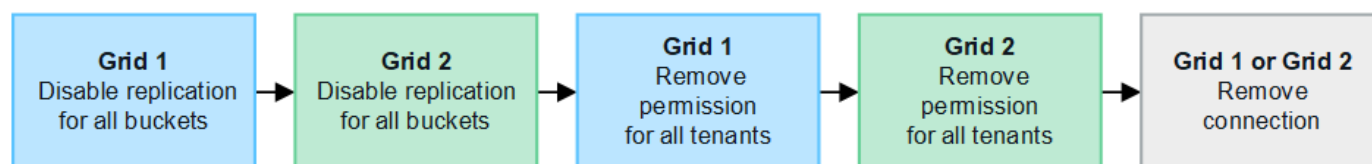
1. いずれかのグリッドのプライマリ管理ノードからグリッドマネージャーにサインインしてください。
2. 設定 > システム > グリッド連携 を選択します。
3. グリッド連携ページのいずれかのタブから、接続名を選択すると、その詳細が表示されます。

4. 「証明書」タブを選択します。
5. 「証明書のローテーション」を選択します。
6. 新しい証明書の有効期間を何日間とするか指定してください。
7. ログ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てください。
8. 「証明書のローテーション」を選択します。
9. 必要に応じて、接続先のもう一方のグリッドでもこれらの手順を繰り返してください。

一般的には、接続の両側で証明書の有効期間を同じ日数に設定してください。

グリッドフェデレーション接続を削除する

接続内のどちらのグリッドからも、グリッドフェデレーション接続を削除できます。図に示すように、どちらのグリッドのテナントによっても接続が使用されていないことを確認するために、両方のグリッドで前提条件となる手順を実行する必要があります。



接続を解除する前に、以下の点にご注意ください。

- 接続を削除しても、グリッド間で既にコピーされたアイテムは削除されません。例えば、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のユーザー、グループ、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。これらの項目を削除するには、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、レプリケーション待ちのオブジェクト（取り込まれたが、まだ他のグリッドに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は永久に失敗します。

すべてのテナントバケットのレプリケーションを無効にする

手順

1. どちらのグリッドからでも、プライマリ管理ノードからGrid Managerにサインインしてください。
2. 設定 > システム > グリッド連携 を選択します。
3. 接続名を選択すると、その詳細が表示されます。
4. *許可されたテナント*タブで、その接続がテナントによって使用されているかどうかを確認します。
5. テナントが一覧表示されている場合は、すべてのテナントに対して、接続先の両方のグリッドにあるすべてのバケットについて**"グリッド間レプリケーションを無効にする"**するよう指示してください。



テナントバケットでクロスグリッドレプリケーションが有効になっている場合、「グリッドフェデレーション接続を使用する」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、両方のグリッド上のバケットについて、クロスグリッド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する

すべてのテナントバケットでクロスグリッドレプリケーションが無効になった後、両方のグリッド上のすべてのテナントから*グリッドフェデレーションを使用する*権限を削除します。

手順

1. 設定 > システム > グリッド連携 を選択します。
2. 接続名を選択すると、その詳細が表示されます。
3. 「許可されたテナント」タブの各テナントについて、各テナントから「グリッドフェデレーション接続を使用する」権限を削除します。["許可されたテナントを管理する"](#)を参照してください。
4. 他のグリッド上の許可されたテナントについても、これらの手順を繰り返してください。

接続を解除する

手順

1. どちらのグリッドでもテナントが接続を使用していない場合は、*削除*を選択してください。
2. 確認メッセージを確認し、*削除*を選択します。
 - 接続を解除できた場合は、成功メッセージが表示されます。グリッド連携接続は、両方のグリッドから削除されました。
 - 接続を解除できない場合（例えば、接続がまだ使用中である場合や、接続エラーが発生した場合）、エラーメッセージが表示されます。以下のいずれかの方法を実行できます。
 - エラーを解決してください（推奨）。["グリッドフェデレーションのエラーをトラブルシューティングする"](#)を参照してください。
 - 強制的に接続を解除してください。次のセクションをご覧ください。

グリッドフェデレーション接続を強制的に削除する

必要に応じて、「接続済み」ステータスではない接続を強制的に削除できます。

強制削除は、ローカルグリッドからの接続を削除するだけです。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てください。

手順

1. 確認ダイアログボックスから「強制削除」を選択します。

成功メッセージが表示されます。このグリッド連携接続は使用できなくなりました。ただし、テナントバケットではクロスグリッドレプリケーションが有効になっている場合があり、接続内のグリッド間で既に一部のオブジェクトコピーが複製されている可能性があります。

2. 接続先の別のグリッドから、プライマリ管理ノードのグリッドマネージャーにサインインします。
3. 設定 > システム > グリッド連携 を選択します。
4. 接続名を選択すると、その詳細が表示されます。
5. 「削除」と「はい」を選択します。
6. **Force remove** を選択して、このグリッドから接続を削除します。

StorageGRID グリッド フェデレーションで許可されたテナントを管理する

S3 テナントアカウントが2つの StorageGRID システム間の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ことができます。テナントが接続を使用することを許可されている場合、テナントの詳細情報を編集したり、テナントの接続使用許可を永久に削除したりするには、特別な手順が必要です。

開始する前に

- ["対応ウェブブラウザ"](#) を使用して、いずれかのグリッドの Grid Manager にサインインしています。
- 現在サインインしているグリッドの["ルートアクセス権限"](#)があります。
- 2つのグリッド間に["グリッドフェデレーション接続を作成しました"](#)があります。
- ["アカウントクローン"](#)と["グリッド間複製"](#)のワークフローを確認しました。
- 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) またはアイデンティティフェデレーションを設定済みであることを確認してください。["アカウントクローンとは何ですか?"](#)を参照してください。

許可されたテナントを作成する

新規または既存のテナントアカウントがアカウントクローンとクロスグリッドレプリケーションにグリッドフェデレーション接続を使用できるようにするには、["新しいS3テナントを作成する"](#)または["テナントアカウントを編集する"](#)の一般的な手順に従い、以下の点に注意してください。

- 接続内のどちらのグリッドからでもテナントを作成できます。テナントが作成されるグリッドは、_テナントのソースグリッド_です。
- 接続状態は **Connected** である必要があります。
- テナントが作成または編集され、「グリッドフェデレーション接続を使用する」権限が有効になり、最初のグリッドに保存されると、同一のテナントが自動的に他のグリッドに複製されます。テナントが複製されるグリッドは、_テナントの宛先グリッド_です。
- 両方のグリッド上のテナントは、同じ20桁のアカウントID、名前、概要、割り当て量、および権限を持ちます。必要に応じて、「概要」フィールドを使用して、ソーステナントと宛先テナントを識別することができます。たとえば、Grid 1 で作成されたテナントのこの概要は、Grid 2 に複製されたテナントにも表示されます：「このテナントは Grid 1 で作成されました。」
- セキュリティ上の理由から、ローカルのルートユーザーのパスワードは宛先グリッドにコピーされません。



ローカルのルートユーザーが宛先グリッド上の複製されたテナントにサインインする前に、そのグリッドのグリッド管理者が["ローカルルートユーザーのパスワードを変更する"](#)必要があります。

- 新規または編集されたテナントが両方のグリッドで利用可能になった後、テナントユーザーは以下の操作を実行できます：
 - 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ーを作成すると、それらは自動的にテナントの宛先グリッドに複製されます。["テナントグループとユーザーを複製する"](#)を参照してください。
 - 新しいS3アクセスキーを作成します。これらのキーは、必要に応じてテナントの宛先グリッドに複製できます。["APIを使用してS3アクセスキーを複製する"](#)を参照してください。

- 。接続内の両方のグリッドに同一のバケットを作成し、一方向または双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 ["クロスグリッドレプリケーションを管理する"](#)。

許可されたテナントを表示する

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. 「テナント」を選択します。
2. テナントページからテナント名を選択すると、テナントの詳細ページが表示されます。

これがテナントのソースグリッドである場合（つまり、テナントがこのグリッド上で作成された場合）、テナントが別のグリッドに複製されたことを知らせ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した場合、変更内容は他のグリッドには同期されません。

Tenants > tenant A for grid federation

tenant A for grid federation

Tenant ID: 0899 6970 1700 0930 0009

Protocol: S3

Object count: 0

Quota utilization: —

Logical space used: 0 bytes

Quota: —

Description: this tenant was created on Grid 1

Sign in

Edit

Actions ▾

This tenant has been cloned to another grid. If you edit or delete this tenant, your changes will not be synced to the other grid.

Space breakdown

Allowed features

Grid federation

Remove permission

Clear error

Search...

Displaying one result

Connection name

Connection status

Remote grid hostname

Last error

Grid 1 to Grid 2

Connected

10.96.106.230

Check for errors

3. 必要に応じて「グリッドフェデレーション」タブを選択して["グリッドフェデレーション接続を監視する"](#)。

許可されたテナントを編集する

*グリッドフェデレーション接続の使用*権限を持つテナントを編集する必要がある場合は、"[テナントアカウントの編集](#)"の一般的な手順に従い、以下の点に注意してください。

- テナントに グリッドフェデレーション接続を使用する 権限が付与されている場合、接続先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、行った変更は他のグリッドには反映されません。テナントの詳細情報のグリッド間の同期を維持するには、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、「グリッドフェデレーション接続を使用する」権限をクリアすることはできません。
- テナントを編集する際に、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する

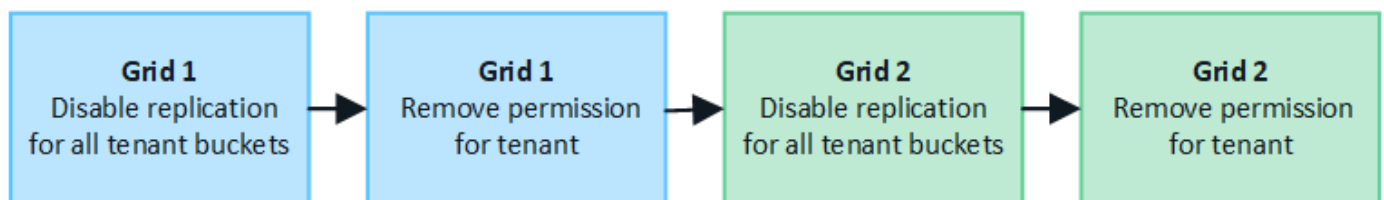
*グリッドフェデレーション接続の使用*権限を持つテナントを削除する必要がある場合は、"[テナントアカウントの削除](#)"の一般的な手順に従い、以下の点に注意してください。

- ソースグリッド上の元のテナントを削除する前に、ソースグリッド上のその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。
- クローンされたテナントを宛先グリッドから削除する前に、宛先グリッド上の当該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ンされたテナントのいずれかを削除すると、そのアカウントはクロスグリッドレプリケーションに使用できなくなります。
- ソースグリッド上の元のテナントを削除する場合、宛先グリッドに複製されたテナントグループ、ユーザー、またはキーは影響を受けません。クローンしたテナントを削除するか、グループ、ユーザー、アクセスキー、バケットを独自に管理させるかを選択できます。
- クローンしたテナントを宛先グリッドから削除する場合、元のテナントに新しいグループまたはユーザーが追加されていると、クローンエラーが発生します。

これらのエラーを回避するには、テナントをこのグリッドから削除する前に、テナントのグリッドフェデレーション接続の使用許可を削除してください。

グリッドフェデレーション接続の使用権限を削除する

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、「グリッドフェデレーション接続を使用する」権限を削除する必要があります。



テナントのグリッドフェデレーション接続の使用許可を取り消す前に、以下の点に注意してください。

- テナントのバケットのいずれかでクロスグリッドレプリケーションが有効になっている場合、「グリッドフェデレーション接続を使用する」権限を削除することはできません。テナントアカウントは、まずすべてのバケットについてクロスグリッドレプリケーションを無効に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」権限を削除しても、既にグリッド間で複製されているアイテムは削除されません。例えば、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のユーザー、グループ、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。これらの項目を削除するには、両方のグリッドから手動で削除する必要があります。
- 同じグリッドフェデレーション接続でこの権限を再度有効にする場合は、まず宛先グリッドでこのテナントを削除してください。そうしないと、この権限を再度有効にするとエラーが発生します。



*グリッドフェデレーション接続を使用する*権限を再度有効にすると、ローカルグリッドがソースグリッドとなり、選択したグリッドフェデレーション接続で指定されたリモートグリッドへのクローン作成が開始されます。テナントアカウントが既にリモートグリッド上に存在する場合、クローンを作成すると競合エラーが発生します。

開始する前に

- あなたは"**対応ウェブブラウザ**"を使用しています。
- 両方のグリッドに対して"**ルートアクセス権限**"があります。

テナントバケットのレプリケーションを無効にする

まず最初に、すべてのテナントバケットのクロスグリッドレプリケーションを無効にします。

手順

1. どちらのグリッドからでも、プライマリ管理ノードからGrid Managerにサインインしてください。
2. 設定 > システム > グリッド連携 を選択します。
3. 接続名を選択すると、その詳細が表示されます。
4. *許可されたテナント*タブで、テナントがその接続を使用しているかどうかを確認します。
5. テナントがリストに表示されている場合は、接続内の両方のグリッドにあるすべてのバケットに対して"**グリッド間レプリケーションを無効にする**"するよう指示してください。



テナントバケットでクロスグリッドレプリケーションが有効になっている場合、「グリッドフェデレーション接続を使用する」権限を削除することはできません。テナントは、両方のグリッド上のバケットについて、クロスグリッド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する

テナントバケットのクロスグリッドレプリケーションを無効にした後、テナントのグリッドフェデレーション接続の使用権限を削除できます。

手順

1. プライマリ管理ノードからグリッドマネージャーにサインインしてください。
2. グリッド連携ページまたはテナントページから権限を削除してください。

グリッドフェデレーションページ

- a. 設定 > システム > グリッド連携 を選択します。
- b. 接続名を選択すると、その詳細ページが表示されます。
- c. 「許可されたテナント」タブで、該当するテナントのラジオボタンを選択します。
- d. 「権限を削除」を選択します。

テナントページ

- a. 「テナント」を選択します。
- b. 詳細ページを表示するには、テナント名を選択してください。
- c. *グリッド連携*タブで、接続用のラジオボタンを選択します。
- d. 「権限を削除」を選択します。

3. 確認ダイアログボックスに表示される警告を確認し、*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、成功メッセージが表示されます。このテナントは、グリッド連携接続を利用できなくなります。
- テナントバケットの1つ以上でクロスグリッドレプリケーションが有効になっている場合、エラーが表示されます。

 **Remove permission to use grid federation connection** 

Are you sure you want to prevent **Tenant A** from performing account sync and cross-grid replication using grid federation connection **Grid 1-Grid 2**?

- Removing this permission does not delete any items that have already been copied to the other grid.
- After removing this permission for the tenant on this grid, go to the other grid and remove the permission for the corresponding tenant account.

 Connection '5427cbf8-0dd0-4b83-a2c8-e5e23cc49cc5' is used by bucket 'my-cgr-bucket' for cross-grid replication, so it can't be removed. From Tenant Manager, remove the cross-grid configuration from the tenant bucket and retry.

 Using **Force remove** removes the tenant's permission to use the grid federation connection even if tenant buckets still have cross-grid replication enabled. When the permission is removed, data in these buckets can no longer be copied between the grids.

Cancel

Force remove

Remove

以下のいずれかの方法を実行できます。

- （推奨。）テナントマネージャーにサインインし、テナントの各バケットのレプリケーションを無効にします。["クロスグリッドレプリケーションを管理する"](#)を参照してください。次に、*グリッド接続を使用する*権限を削除する手順を繰り返します。
- 強制的に権限を削除する。次のセクションを参照してください。

4. 別のグリッドに移動し、同じ手順を繰り返して、もう一方のグリッド上の同じテナントの権限を削除します。

強制的に権限を削除します

必要に応じて、テナントバケットでクロスグリッドレプリケーションが有効になっている場合でも、テナントのグリッドフェデレーション接続の使用許可を強制的に削除できます。

テナントの許可を強制的に取り消す前に、[権限を削除する](#)の一般的な考慮事項と、以下の追加の考慮事項に注意してください：

- 「グリッドフェデレーション接続を使用する」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が保留中のオブジェクト（取り込まれたがまだレプリケーションされていないオブジェクト）

は、引き続きレプリケーションされます。これらの処理中のオブジェクトが宛先バケットに到達するのを防ぐには、他のグリッド上のテナントの権限も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 権限を削除した後にソースバケットに取り込まれたオブジェクトは、宛先バケットに複製されることはありません。

手順

1. プライマリ管理ノードからグリッドマネージャーにサインインしてください。
2. 設定 > システム > グリッド連携 を選択します。
3. 接続名を選択すると、その詳細ページが表示されます。
4. 「許可されたテナント」タブで、該当するテナントのラジオボタンを選択します。
5. 「権限を削除」を選択します。
6. 確認ダイアログボックスに表示される警告を確認し、*強制削除*を選択します。

成功メッセージが表示されます。このテナントは、グリッド連携接続を利用できなくなりました。

7. 必要に応じて、別のグリッドに移動し、これらの手順を繰り返して、別のグリッド上の同じテナントアカウントのアクセス許可を強制的に削除します。例えば、処理中のオブジェクトが宛先バケットに到達しないようにするには、これらの手順を他のグリッドでも繰り返す必要があります。

StorageGRID でグリッドフェデレーションのエラーをトラブルシューティングします

グリッド連携接続、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

グリッド連携接続に関して、アラートが表示されたり、エラーが発生したりする場合があります。

接続の問題を解決するために変更を加えた後は、接続をテストして、接続状態が「接続済み」に戻ることを確認してください。手順については、"[グリッドフェデレーション接続の管理](#)"を参照してください。

グリッドフェデレーション接続障害アラート

問題

*グリッド連携接続失敗*アラートが発動しました。

詳細

このアラートは、グリッド間のグリッド連携接続が機能していないことを示しています。

推奨する対処方法

1. 両方のグリッドについて、グリッド連携ページの設定を確認してください。すべての値が正しいことを確認してください。"[グリッドフェデレーション接続の管理](#)"を参照してください。
2. 接続に使用された証明書を確認してください。グリッドフェデレーション証明書の有効期限切れ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。接続証明書のローテーションに関する手順については、"[グリッドフェデレーション接続の管理](#)"を参照してください。
3. 両方のグリッド内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利用可能であることを確認

してください。これらのノードに影響している可能性のあるアラートをすべて解決してから、もう一度試してください。

4. ローカルまたはリモートのグリッドに完全修飾ドメイン名（FQDN）を指定した場合は、DNSサーバーがオンラインで利用可能であることを確認してください。ネットワーク、IPアドレス、およびDNSの要件については、"[グリッドフェデレーションとは](#)"を参照してください。

グリッドフェデレーション証明書の有効期限切れに関するアラート

問題

「グリッドフェデレーション証明書の有効期限切れ」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間もなく切れることを示しています。

推奨する対処方法

接続証明書のローテーションに関する手順については、"[グリッドフェデレーション接続の管理](#)"を参照してください。

グリッドフェデレーション接続の編集エラー

問題

グリッドフェデレーション接続を編集する際に、*保存してテスト*を選択すると、次の警告メッセージが表示されます：「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。」

詳細

グリッドフェデレーション接続を編集する場合、StorageGRID は最初のグリッド上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になっているなど、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。

推奨する対処方法

1. 接続を編集するために使用しているグリッドから、*ノード*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てください。
3. いずれかのノードがオフラインになっている場合は、それらをオンラインに戻してから、接続の編集を再度試してください。

アカウントクローンエラー

クローンされたテナントアカウントにサインインできません

問題

複製されたテナントアカウントにはサインインできません。テナントマネージャーのサインインページに表示されるエラーメッセージは「このアカウントの認証情報が無効です。もう一度お試しください。」

詳細

セキュリティ上の理由から、テナントアカウントがテナントのソースグリッドからテナントの宛先グリッドにクローンされる場合、テナントのローカルルートユーザーに設定したパスワードはクローンされません。同様に、テナントがソースグリッド上にローカルユーザーを作成した場合、ローカルユーザーのパスワードは宛先グリッドにクローンされません。

推奨する対処方法

ルートユーザーがテナントの宛先グリッドにサインインする前に、グリッド管理者はまず宛先グリッドで"[ローカルルートユーザーのパスワードを変更する](#)"必要があります。

クローンされたローカルユーザーがテナントの宛先グリッドにサインインするには、クローンされたテナントのルートユーザーが、宛先グリッド上でそのユーザー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、テナントマネージャーの使用説明書の"[ユーザの管理](#)"を参照してください。

クローンなしで作成されたテナント

問題

*グリッドフェデレーション接続を使用する*権限で新しいテナントを作成すると、「クローンなしでテナントが作成されました」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、その結果、正常でない接続が **Connected** と表示されることがあります。

推奨する対処方法

1. エラーメッセージに記載されている理由を確認し、接続を妨げている可能性のあるネットワークの問題やその他の問題を解決してください。[グリッドフェデレーション接続アラートとエラー](#)を参照してください。
2. "[グリッドフェデレーション接続の管理](#)"でグリッドフェデレーション接続をテストするには、以下の手順に従って、問題が解決されたことを確認してください。
3. テナントのソースグリッドから*テナント*を選択します。
4. クローン作成に失敗したテナントアカウントを特定してください。
5. 詳細ページを表示するには、テナント名を選択してください。
6. 「アカウントの複製を再試行」を選択します。

Tenants > test

test

Tenant ID: 0040 2213 8117 4859 6503

Protocol: S3

Object count: 0

Quota utilization: —

Logical space used: 0 bytes

Quota: —

Sign in

Edit

Actions

✖

Tenant account could not be cloned to the other grid.
Reason: Internal server error. The server encountered an error and could not complete your request. Try again. If the problem persists, contact support. Internal Server Error

Retry account clone

エラーが解決された場合、テナントアカウントは別のグリッドに複製されます。

クロスグリッドレプリケーションのアラートとエラー

接続またはテナントで最後に表示されたエラー

問題

"[グリッドフェデレーション接続の表示](#)"のとき（または接続の場合に"[許可されたテナントの管理](#)"のとき）、接続詳細ページの*最後のエラー*列にエラーが表示されます。例：

Grid 1 - Grid 2

Local hostname (this grid):10.115.96.170

Port:23000

Remote hostname (other grid):10.115.96.175

Connection status: Connected

EditDownload fileTest connectionRemove

Permitted tenantsCertificates

Remove permissionClear errorSearch...

Displaying one result

Tenant name	Last error ?
 Tenant A	2025-03-13 15:54:59 PDT Cross-grid replication has encountered an error. Failed to send cross-grid replication request from source bucket 'my-bucket' to destination bucket 'my-bucket'. Error code: DestinationRequestError. Detail: InvalidBucketState. Confirm that the source and destination buckets have object versioning enabled. (logID 13371653720226059496) Check for errors

詳細

各グリッド連携接続について、「最終エラー」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際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、最後に発生したクロスグリッドレプリケーションエラーのみが表示されます。それ以前に発生した可能性のあるエラーは表示されません。この列にエラーが表示される原因としては、以下のいずれかが考えられます。

- ・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。
- ・宛先バケットが削除されました。
- ・宛先バケットは別のアカウントによって再作成されました。
- ・宛先バケットではバージョン管理が一時停止されています。
- ・宛先バケットは同じアカウントによって再作成されましたが、現在はバージョン管理されていません。
- ・ソースオブジェクトのS3オブジェクトロック設定が、宛先グリッドのテナントレベルの保持設定に準拠していません。
- ・ソースオブジェクトにはS3オブジェクトロック設定が適用されていますが、宛先バケットではS3オブジェクトロックが無効になっています。

推奨する対処方法

*最後のエラー*列にエラーメッセージが表示された場合は、以下の手順に従ってください。

1. メッセージ本文を確認してください。

2. 推奨された措置をすべて実行してください。例えば、クロスグリッドレプリケーションの宛先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. 表から接続またはテナントアカウントを選択してください。
4. 「エラーをクリア」を選択します。
5. 「はい」を選択すると、メッセージが消去され、システムのステータスが更新されます。
6. 5〜6分待ってから、バケットに新しいオブジェクトを取り込んでください。エラーメッセージが再表示されないことを確認してください。



エラーメッセージが確実に消去されるようにするには、メッセージ内のタイムスタンプから少なくとも5分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。



エラーを解消した後、別のバケットにオブジェクトが取り込まれた際に、そのバケットにもエラーが発生している場合、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オブジェクトの複製に失敗したかどうかを確認するには、"[失敗したレプリケーション操作を特定して再試行する](#)"を参照してください。

クロスグリッドレプリケーションの永続的な障害アラート

問題

「クロスグリッドレプリケーションの永続的な障害」アラートがトリガーされました。

詳細

このアラートは、テナントオブジェクトが2つのグリッド上のバケット間で複製できないことを示しています。解決にはユーザーの介入が必要です。このアラートは通常、送信元バケットまたは送信先バケットのいずれかに変更があった場合に発生します。

推奨する対処方法

1. アラートが発生したグリッドにサインインしてください。
2. 設定 > 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. 「許可されたテナント」タブで、最後のエラー 列を確認すると、エラーが発生しているテナントアカウントがわかります。
4. 障害の詳細については、"[グリッドフェデレーション接続を監視する](#)"の手順を参照して、グリッド間レプリケーションの指標を確認してください。
5. 影響を受けるテナントアカウントごとに：
 - a. "[テナントのアクティビティを監視する](#)"の手順を参照して、テナントがクロスグリッドレプリケーションの宛先グリッドのクォータを超過していないことを確認してください。
 - b. 必要に応じて、新しいオブジェクトを保存できるように、宛先グリッド上のテナントのクォータを増やしてください。
6. 影響を受けるテナントごとに、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してください。
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、以下を確認してください。
 - 同じテナントに対応するバケットが、別のグリッドにも存在します（正確な名前を使用する必要があります）

ります)。

- どちらのバケット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)。
- どちらのバケットも「オブジェクトの削除：読み取り専用」状態ではありません。

8. 問題が解決したことを確認するには、"[グリッドフェデレーション接続を監視する](#)"の手順を参照してグリッド間レプリケーションのメトリクスを確認するか、次の手順を実行してください。
 - a. グリッド連携ページに戻ってください。
 - b. 影響を受けるテナントを選択し、*最後のエラー*列で*エラーをクリア*を選択します。
 - c. 「はい」を選択すると、メッセージが消去され、システムのステータスが更新されます。
 - d. 5〜6分待ってから、バケットに新しいオブジェクトを取り込んでください。エラーメッセージが再表示されないことを確認してください。



エラーメッセージが確実に消去されるようにするには、メッセージ内のタイムスタンプから少なくとも5分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。



問題が解決した後、アラートが解除されるまで最大1日かかる場合があります。

- a. "[失敗したレプリケーション操作を特定して再試行する](#)"に移動して、他のグリッドへのレプリケーションに失敗したオブジェクトまたは削除マーカーを特定し、必要に応じてレプリケーションを再試行してください。

クロスグリッドレプリケーションリソース利用不可アラート

問題

「クロスグリッドレプリケーションリソースが利用できません」というアラートがトリガーされました。

詳細

このアラートは、リソースが利用できないため、クロスグリッドレプリケーション要求が保留状態になっていることを示しています。例えば、ネットワークエラーが発生している可能性があります。

推奨する対処方法

1. アラートを監視して、問題が自然に解決するかどうかを確認してください。
2. 問題が解決しない場合は、いずれかのグリッドで同じ接続に対する **Grid federation connection failure** アラート、またはノードに対する **Unable to communicate with node** アラートが発生しているかどうかを確認してください。これらのアラートを解決すれば、このアラートも解消される可能性があります。
3. 障害の詳細については、"[グリッドフェデレーション接続を監視する](#)"の手順を参照して、グリッド間レプリケーションの指標を確認してください。
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。

問題が解決すれば、グリッド間レプリケーションは通常どおり実行されます。

失敗したStorageGRIDレプリケーション処理を特定して再試行する

「クロスグリッドレプリケーションの永続的な失敗」アラートを解決した後、オブジェ

クトまたは削除マーカが他のグリッドにレプリケートされなかった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むか、Grid Management API を使用してレプリケーションを再試行できます。

「クロスグリッドレプリケーションの永続的な失敗」アラートは、テナントオブジェクトが2つのグリッド上のバケット間でレプリケートできない状態であり、解決にはユーザーの介入が必要であることを示しています。このアラートは通常、送信元バケットまたは送信先バケットのいずれかに変更があった場合に発生します。詳細については、"[グリッドフェデレーションのエラーをトラブルシューティングする](#)"を参照してください。

複製に失敗したオブジェクトがあるかどうかを判断する

オブジェクトまたは削除マーカが他のグリッドに複製されていないかどうかを確認するには、監査ログで"[CGRR（クロスグリッドレプリケーション要求）](#)"メッセージを検索します。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、または削除マーカを宛先バケットに複製できなかった場合にログに追加されます。

"[audit-explain ツール](#)"を使用して、結果をより読みやすい形式に変換できます。

開始する前に

- ルートアクセス権限があります。
- あなたは `Passwords.txt` ファイルを持っています。
- プライマリ管理ノードのIPアドレスを把握している必要があります。

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. `Passwords.txt` ファイルに記載されているパスワードを入力してください。
 - c. 以下のコマンドを入力して root に切り替えます： `su -`
 - d. `Passwords.txt` ファイルに記載されているパスワードを入力してください。

rootとしてログインすると、プロンプトが `\$` から `#` に変わります。
2. audit.log ファイルから 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。

例えば、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で検索し、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
```

コマンドの実行結果は、6つのCGRRメッセージのエントリを含むこの例のようになります。この例では、オブジェクトを複製できなかったため、すべてのクロスグリッドレプリケーション要求で一般的なエラーが返されました。最初の3つのエラーは「replicate object」操作に関するもので、最後の3つのエラーは「replicate delete marker」操作に関するものです。

```

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

```

各エントリには以下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リクエスト	リクエストの名前
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
operation	実行されようとしていたレプリケーション操作の種類： - 複製オブジェクト - 複製削除マーカー - マルチパートオブジェクトを複製する
バケット	バケット名
object（オブジェクト）	オブジェクト名
version	オブジェクトのバージョンID

フィールド	説明
エラー	エラーの種類。グリッド間レプリケーションが失敗した場合、エラーは「General error」となります。

失敗したレプリケーションを再試行する

宛先バケットにレプリケートされなかったオブジェクトと削除マーカのリストを生成し、根本的な問題を解決した後、次の2つの方法のいずれか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取り込みします。
- 説明されているとおり、Grid Management のプライベート API を使用してください。

手順

1. グリッドマネージャーの上部にある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ドキュメントへ移動」を選択します。



StorageGRID の「プライベート」とマークされた 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、リクエストの 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. 「Try it out」を選択します。
5. **body** テキストボックスで、**versionID** の例のエントリを、失敗したクロスグリッドレプリケーション要求に対応する audit.log のバージョン ID に置き換えてください。

文字列を囲む二重引用符は必ず残してください。

6. 「実行」を選択します。
7. サーバー応答コードが **204** であることを確認してください。これは、オブジェクトまたは削除マーカが、他のグリッドへのクロスグリッドレプリケーションの保留状態としてマークされていることを示しています。



「保留中」とは、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意味します。

レプリケーションの再試行を監視する

レプリケーションの再試行操作が確実に完了するように監視する必要があります。



オブジェクトや削除マーカが他のグリッドに複製されるまでには、数時間以上かかる場合があります。

再試行操作を監視するには、次の2つの方法があります。

- S3の"[HeadObject](#)"または"[GetObject](#)"リクエストを使用します。応答にはStorageGRID固有の`x-ntap-sg-cgr-replication-status`レスポンスヘッダーが含まれており、次のいずれかの値を持ちます：

Grid	レプリケーションステータス
ソース	• 完了：複製は成功しました。 • 保留中：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障害で失敗しました。ユーザーはエラーを解決する必要があります。
デスティネーション	レプリカ：オブジェクトはソースグリッドから複製されました。

- 説明されているとおり、Grid Management のプライベート API を使用してください。

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. 「Try it out」を選択します。
3. パラメーターセクションで、`cross-grid-replication-retry-failed` リクエストで使用したバージョンIDを入力します。
4. 「実行」を選択します。
5. サーバー応答コードが **200** であることを確認してください。
6. レプリケーションの状態を確認してください。状態は以下のいずれかになります。
 - 保留中：オブジェクトはまだレプリケートされていません。
 - 完了：複製は成功しました。
 - **FAILED**: 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。

セキュリティを管理する

StorageGRID でセキュリティを管理する

グリッドマネージャーからさまざまなセキュリティ設定を構成して、StorageGRID システムのセキュリティを強化できます。

暗号化を管理する

StorageGRID は、データの暗号化に関していくつかのオプションを提供しています。データ保護要件を満たすオプションを判断するには、"[利用可能な暗号化方式を確認する](#)"を参照してください。

証明書の管理

HTTP接続に使用される"[サーバー証明書の設定と管理](#)"、またはクライアントやユーザーのIDをサーバーに対して認証するために使用されるクライアント証明書を確認できます。

キー管理サーバの設定

"[キー管理サーバ](#)"を使用することで、アプライアンスがデータセンターから撤去された場合でも、StorageGRID データを保護できます。アプライアンスのボリュームが暗号化されると、ノードが KMS と通信できない限り、アプライアンス上のデータにアクセスできなくなります。



暗号化キー管理を使用するには、アプライアンスをグリッドに追加する前に、インストール時に各アプライアンスの「ノード暗号化」設定を有効にする必要があります。

プロキシ設定を管理する

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している場合は、ストレージノードと外部S3エンドポイント間に"[ストレージ プロキシ サーバ](#)"を設定できます。HTTPSまたはHTTPを使用してAutoSupport/パッケージを送信する場合は、管理ノードとテクニカルサポートの間に"[管理者プロキシ サーバ](#)"を設定できます。

ファイアウォールを制御する

システムのセキュリティを強化するために、"[外部ファイアウォール](#)"で特定のポートを開閉することにより、StorageGRID 管理ノードへのアクセスを制御できます。また、"[内部ファイアウォール](#)"を設定することで、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。デプロイメントに必要なポート以外のすべてのポートへのアクセスを制限できます。

StorageGRID の暗号化方式の確認

StorageGRID では、データの暗号化に関していくつかのオプションを提供しています。利用可能な方法を検討し、どの方法が自社のデータ保護要件を満たすかを判断する必要があります。

この表は、StorageGRID で利用可能な暗号化方法の概要を示しています。

暗号化オプション	仕組み	環境
Grid Manager のキー管理サーバ (KMS)	StorageGRIDサイトに対して" キー管理サーバの設定 "し、" アプライアンスのノード暗号化を有効にする "します。次に、アプライアンスノードがKMSに接続して、キー暗号化キー (KEK) 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。	インストール時に Node Encryption が有効になっているアプライアンスノード。アプライアンス上のすべてのデータは、物理的な紛失やデータセンターからの持ち出しから保護されています。 注：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ています。

暗号化オプション	仕組み	環境
StorageGRID アプライアンスインストーラのドライブ暗号化ページ	アプライアンスにハードウェア暗号化をサポートするドライブが搭載されている場合、インストール時にドライブのパスフレーズを設定できます。ドライブにパスフレーズを設定すると、パスフレーズを知らない限り、システムから取り外されたドライブから有効なデータを復元することは誰にも不可能になります。インストールを開始する前に、Configure Hardware > Drive Encryption に移動して、ノード内のすべての StorageGRID 管理対象の自己暗号化ドライブに適用されるドライブパスフレーズを設定してください。	自己暗号化ドライブを搭載した機器。セキュリティ保護されたドライブ上のすべてのデータは、物理的な紛失やデータセンターからの持ち出しから保護されています。 ドライブ暗号化は、SANtricityが管理するドライブには適用されません。自己暗号化ドライブとSANtricityコントローラーを備えたストレージアプライアンスをお持ちの場合は、SANtricityでドライブセキュリティを有効にすることができます。
SANtricity System Manager でのドライブ セキュリティ	StorageGRID 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、"SANtricity System Manager"を使用してセキュリティキーを作成および管理できます。セキュリティで保護されたドライブ上のデータにアクセスするには、キーが必要です。	フルディスク暗号化（FDE）ドライブまたは自己暗号化ドライブを搭載したストレージ機器。セキュリティ保護されたドライブ上のすべてのデータは、物理的な紛失やデータセンターからの持ち出しから保護されています。一部のストレージ機器やサービス機器とは使用できません。
保存オブジェクトの暗号化	Grid Manager で"保存オブジェクトの暗号化"オプションを有効にします。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規オブジェクトは、取り込み時に暗号化されません。	新たに取り込まれたS3オブジェクトデータ。 既に保存されているオブジェクトは暗号化されません。オブジェクトのメタデータやその他の機密データは暗号化されていません。
S3バケットの暗号化	PutBucketEncryption リクエストを発行して、バケットの暗号化を有効にします。オブジェクトレベルで暗号化されていない新規オブジェクトは、取り込み時に暗号化されます。	新規に取り込まれたS3オブジェクトデータのみ。 バケットには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ていません。オブジェクトのメタデータやその他の機密データは暗号化されていません。 "バケットに対する操作"

暗号化オプション	仕組み	環境
S3オブジェクトのサーバー側暗号化（SSE）	オブジェクトを保存するために S3 リクエストを発行し、`x-amz-server-side-encryption` リクエストヘッダーを含めます。	新規に取り込まれたS3オブジェクトデータのみ。 オブジェクトには暗号化を指定する必要があります。オブジェクトのメタデータやその他の機密データは暗号化されていません。 StorageGRIDがキーを管理します。 "サーバー側暗号化を使用する"
S3オブジェクトのサーバー側暗号化（顧客提供キー使用）（SSE-C）	オブジェクトを保存するために S3 リクエストを発行し、3 つのリクエスト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	新規に取り込まれたS3オブジェクトデータのみ。 オブジェクトには暗号化を指定する必要があります。オブジェクトのメタデータやその他の機密データは暗号化されていません。 キーは StorageGRID の外部で管理されます。 "サーバー側暗号化を使用する"
外部ボリュームまたはデータストアの暗号化	デプロイメントプラットフォームがサポートしている場合は、StorageGRID 外部の暗号化方式を使用して、ボリューム全体またはデータストア全体を暗号化できます。	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（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する）。 外部暗号化方式は、暗号化アルゴリズムと鍵をより厳密に制御できます。上記に挙げた他の方法と組み合わせることも可能です。

暗号化オプション	仕組み	環境
StorageGRID 外部でのオブジェクト暗号化	StorageGRID の外部で暗号化方式を使用して、オブジェクトデータとメタデータを StorageGRID に取り込む前に暗号化します。	オブジェクトデータとメタデータのみ（システム構成データは暗号化されません）。 外部暗号化方式は、暗号化アルゴリズムと鍵をより厳密に制御できます。上記に挙げた他の方法と組み合わせることも可能です。 "Amazon Simple Storage Service - ユーザーガイド：クライアント側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する

要件に応じて、複数の暗号化方式を同時に使用することも可能です。例えば：

- KMS を使用してアプライアンス ノードを保護し、SANtricity System Manager のドライブ セキュリティ機能を使用して、同一アプライアンス内の自己暗号化ドライブ上のデータを「二重暗号化」することもできます。
- KMSを使用すると、アプライアンスノード上のデータを保護できるだけでなく、保存済みオブジェクトの暗号化オプションを使用して、オブジェクトを取り込む際にすべてのオブジェクトを暗号化することもできます。

暗号化が必要なオブジェクトがごく一部である場合は、バケットレベルまたは個々のオブジェクトレベルで暗号化を制御することを検討してください。複数の暗号化レベルを有効にすると、パフォーマンスに余分なコストがかかります。

関連情報

["FIPS認証済みの暗号化オプションについて"](#)

証明書の管理

StorageGRIDでセキュリティ証明書を管理する

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安全で信頼できる接続を確立するために使用される小さなデータファイルです。

StorageGRIDは2種類のセキュリティ証明書を使用します。

- HTTPS接続を使用する場合は、***サーバー証明書***が必要です。サーバー証明書は、クライアントとサーバー間の安全な接続を確立するために使用され、クライアントに対してサーバーの身元を認証し、データの安全な通信経路を提供します。サーバーとクライアントはそれぞれ証明書のコピーを保持しています。
- ***クライアント証明書***は、クライアントまたはユーザーの身元をサーバーに対して認証し、パスワードのみの場合よりも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を使用してサーバーに接続すると、サーバーは公開鍵を含むサーバー証明書で応答し

ます。クライアントは、サーバーの署名と、自身が所有する証明書のコピーに記載されている署名を比較します。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ーとのセッションを開始します。

StorageGRID は、一部の接続（ロード バランシング エンドポイントなど）のサーバーとして機能し、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グリッドCA証明書を生成する組み込みの認証局（CA）が備わっています。Grid CA証明書は、デフォルトでStorageGRIDの内部トラフィックを保護するために使用されます。外部認証局（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カスタム証明書を発行できます。

非本番環境では、Grid CA証明書を使用してください。本番環境では、外部認証局によって署名されたカスタム証明書を使用してください。証明書のないセキュリティ保護されていない接続はサポートされていますが、推奨されません。

- カスタムCA証明書は内部証明書を削除するものではありませんが、サーバー接続の検証にはカスタム証明書を指定する必要があります。
- すべてのカスタム証明書は、"[サーバー証明書のシステム強化ガイドライン](#)"を満たす必要があります。
- StorageGRIDは、CAからの証明書を単一のファイルにバンドルする機能（CA証明書バンドルと呼ばれる）をサポートしています。



StorageGRIDには、すべてのグリッドで共通のオペレーティングシステム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。

サーバー証明書とクライアント証明書の種類のバリエーションは、いくつかの方法で実装されています。システムを設定する前に、特定の StorageGRID 構成に必要な証明書をすべて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1か所からアクセスでき、各証明書の設定ワークフローへのリンクも提供されます。

手順

1. Grid Manager から、**Configuration > Security > Certificates** を選択します。

Certificates

View and manage the certificates that secure HTTPS connections between StorageGRID and external clients, such as S3 or Swift, and external servers, such as a key management server (KMS).

Global

Grid CA

Client

Load balancer endpoints

Tenants

Other

The StorageGRID certificate authority ("grid CA") generates and signs two global certificates during installation. The management interface certificate on Admin Nodes secures the management interface. The S3 and Swift API certificate on Storage and Gateway Nodes secures client access. You should replace each default certificate with your own custom certificate signed by an external certificate authority.

Name	Description	Type ⓘ	Expiration date ⓘ ⌵
Management interface certificate	Secures the connection between client web browsers and the Grid Manager, Tenant Manager, Grid Management API, and Tenant Management API.	Custom	Jun 4th, 2022
S3 and Swift API certificate	Secures the connections between S3 and Swift clients and Storage Nodes or between clients and the deprecated CLB service on Gateway Nodes. You can optionally use this certificate for a load balancer endpoint as well.	Custom	Jun 4th, 2022

2. 証明書ページでタブを選択すると、各証明書カテゴリに関する情報が表示され、証明書の設定にアクセスできます。タブにアクセスするには、"[適切な許可](#)"が必要です。

- グローバル：StorageGRID へのウェブブラウザおよび外部 API クライアントからのアクセスを保護します。
- **Grid CA**：内部の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 データベース間の接続を保護します。
- ロード バランシング エンドポイント：S3クライアントとStorageGRID ロード バランシング間の接続を保護します。
- テナント：IDフェデレーションサーバーへの接続、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：特定の証明書が必要なStorageGRID接続を保護します。

各タブの説明と、証明書の詳細情報へのリンクを以下に示します。

グローバル

グローバル証明書は、ウェブブラウザおよび外部S3 APIクライアントからのStorageGRIDへのアクセスを保護します。2つのグローバル証明書は、インストール時にStorageGRID認証局によって最初に生成されます。本番環境のベストプラクティスは、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です。

- [\[管理インターフェイス証明書\]](#)：クライアントのウェブブラウザ接続をStorageGRIDの管理インターフェイスに対してセキュリティで保護します。
- [S3 API証明書](#)：S3クライアントアプリケーションがオブジェクトデータのアップロードとダウンロードに使用する、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。

インストールされているグローバル証明書に関する情報は以下のとおりです。

- 名前：証明書名と、証明書の管理ページへのリンク。
- 概要
- タイプ：カスタムまたはデフォルト。+グリッドのセキュリティを向上させるには、常にカスタム証明書を使用することをお勧めします。
- 有効期限：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。

次の操作を実行できます。

- グリッドセキュリティを向上させるため、デフォルトの証明書を外部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ください：
 - ["デフォルトの StorageGRID が生成した管理インターフェイス証明書を置き換える"](#)グリッドマネージャーおよびテナントマネージャーへの接続に使用されます。
 - ["S3 API証明書を置き換える"](#)ストレージノードおよびロードバランサーエンドポイント（オプション）への接続に使用されます。
- ["デフォルトの管理インターフェイス証明書を復元する"](#)。
- ["デフォルトの S3 API 証明書を復元する"](#)。
- ["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する"](#)。
- ["管理インターフェイス証明書"](#)または["S3 API証明書"](#)をコピーまたはダウンロードします。

グリッドCA

StorageGRIDのインストール時にStorageGRID認証局によって生成された[グリッドCA証明書](#)は、すべてのStorageGRID内部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証明書の内容が含まれます。

["Grid CA証明書をコピーまたはダウンロード"](#)ことはできますが、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](#)外部認証局によって生成されたこれらの証明書は、外部監視ツールとStorageGRID Prometheusデータベース間の接続を保護します。

証明書テーブルには、設定済みのクライアント証明書ごとに1行があり、証明書の有効期限とともに

に、その証明書がPrometheusデータベースへのアクセスに使用できるかどうかを示します。

次の操作を実行できます。

- ["クライアント証明書をアップロードするか、新しい証明書を生成してください。"](#)
- 証明書名を選択すると、証明書の詳細が表示されます。そこでは、以下の操作が可能です。
 - ["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てください。"](#)
 - ["クライアント証明書をコピーまたはダウンロードしてください。"](#)
 - ["クライアント証明書を削除します。"](#)
- アクション*を選択すると、すばやくクライアント証明書を["編集"](#)、["添付"](#)、または["削除"](#)できます。*アクション> *削除*を使用すると、最大10個のクライアント証明書を選択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

[ロードバランサーエンドポイント証明書](#) S3クライアントとStorageGRIDのゲートウェイノードおよび管理ノード上のロードバランサーサービス間の接続を保護します。

ロードバランサーエンドポイントテーブルには、設定済みのロードバランサーエンドポイントごとに1行があり、そのエンドポイントでグローバルS3 API証明書が使用されているか、カスタムロードバランサーエンドポイント証明書が使用されているかを示します。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は、最大15分かかる場合があります。

次の操作を実行できます。

- ["ロードバランサーのエンドポイントを表示する"](#)（証明書の詳細を含む）。
- ["FabricPool のロードバランサーエンドポイント証明書を指定します。"](#)
- ["グローバルS3 API証明書を使用する"](#)新しいロードバランサーエンドポイント証明書を生成する代わりに使用します。

テナント

テナントは[IDフェデレーションサーバー証明書](#)または[プラットフォームサービスエンドポイント証明書](#)を使用して、StorageGRIDとの接続を保護できます。

テナントテーブルにはテナントごとに1行があり、各テナントが自身のID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を持っているかどうかを示します。

次の操作を実行できます。

- ["テナント名を選択してTenant Managerにサインインします。"](#)
- ["テナント名を選択して、テナントIDフェデレーションの詳細を表示します。"](#)
- ["テナント名を選択して、テナントプラットフォームサービスの詳細を表示します。"](#)

- "エンドポイント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 は、特定の目的のため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ています。その他のセキュリティ証明書には以下が含まれます。

- クラウドストレージプール証明書
- メールアラート通知証明書
- 外部のsyslogサーバー証明書
- グリッドフェデレーション接続証明書
- IDフェデレーション証明書
- キー管理サーバー（KMS）証明書
- シングルサインオン証明書

この情報には、関数が使用する証明書の種類、および該当する場合はサーバー証明書とクライアント証明書の有効期限が示されています。関数名を選択すると、ブラウザのタブが開き、そこで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、"適切な許可"がある場合のみです。

次の操作を実行できます。

- "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する"
- "アラートメール通知用の証明書を指定する"
- "外部syslogサーバの証明書を使用する"
- "グリッドフェデレーション接続証明書をローテーションする"
- "IDフェデレーション証明書の表示と編集"
- "キー管理サーバー（KMS）サーバーおよびクライアント証明書をアップロードする"
- "証明書利用者信頼のSSO証明書を手動で指定する"

セキュリティ証明書の詳細

各セキュリティ証明書の種類について、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証明書

証明書の種類	説明	ナビゲーション位置	詳細
サーバ	クライアントのウェブブラウザとStorageGRID 管理インターフェイス間の接続を認証し、ユーザーがセキュリティ警告なしにGrid ManagerとTenant Managerにアクセスできるようにします。 この証明書は、グリッド管理APIおよびテナント管理APIへの接続も認証します。 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。	Configuration > Security > Certificates を選択し、 Global タブを選択してから、 Management interface certificate を選択します。	" 管理インターフェイス証明書の設定 "

S3 API証明書

証明書の種類	説明	ナビゲーション位置	詳細
サーバ	ストレージノードおよびロードバランサーエンドポイントへの安全なS3クライアント接続を認証します（オプション）。	「設定」>「セキュリティ」>「証明書」を選択し、「グローバル」タブを選択してから、「S3 API 証明書」を選択します。	" S3 API証明書の設定 "

グリッドCA証明書

[デフォルトのGrid CA証明書の説明](#)を参照してください。

管理者クライアント証明書

証明書の種類	説明	ナビゲーション位置	詳細
クライアント	各クライアントにインストールされ、StorageGRID が外部クライアントのアクセスを認証できるようにします。 - 承認された外部クライアントが StorageGRID の 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 を安全に監視できます。	「構成」 > 「セキュリティ」 > 「証明書」の順に進み、「クライアント」タブを選択します。	"クライアント証明書の設定"

ロードバランサーエンドポイント証明書

証明書の種類	説明	ナビゲーション位置	詳細
サーバ	S3クライアントとStorageGRIDのゲートウェイノードおよび管理ノード上のロードバランサーサービス間の接続を認証します。ロードバランサーエンドポイントを設定する際に、ロードバランサー証明書をアップ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は、StorageGRIDに接続してオブジェクトデータを保存および取得する際に、ロードバランサー証明書を使用します。 グローバルのS3 API証明書証明書のカスタムバージョンを使用して、ロードバランサーサービスへの接続を認証することもできます。ロードバランサー接続の認証にグローバル証明書を使用する場合、各ロードバランサーエンドポイント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: ロードバランサー認証に使用される証明書は、通常の StorageGRID 運用時に最もよく使用される証明書です。	設定 > ネットワーク > ロードバランサーエンドポイント	• "ロードバランサーのエンドポイントを設定する" • "FabricPool のロードバランサーエンドポイントを作成する"

クラウドストレージプールエンドポイント証明書

証明書の種類	説明	ナビゲーション位置	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場所への接続を認証します。クラウド プロバイダの種類ごとに異なる証明書が必要です。	ILM > ストレージプール	"クラウドストレージプールを作成する"

メールアラート通知証明書

証明書の種類	説明	ナビゲーション位置	詳細
サーバーとクライアント	アラート通知に使用される SMTP メールサーバーと StorageGRID 間の接続を認証します。 • SMTPサーバーとの通信にトランスポート層セキュリティ（TLS）が必要な場合は、メールサーバーのCA証明書を指定する必要があります。 • SMTPメールサーバーが認証にクライアント証明書を必要とする場合にのみ、クライアント証明書を指定してください。	アラート > メール設定	"アラートのメール通知を設定する"

外部のsyslogサーバー証明書

証明書の種類	説明	ナビゲーション位置	詳細
サーバ	StorageGRID でイベントをログに記録する外部 syslog サーバーとの TLS または RELP/TLS 接続を認証します。 注: 外部 syslog サーバーへの TCP、RELP/TCP、および UDP 接続には、外部 syslog サーバー証明書は不要です。	設定 > 監視 > 監査とsyslogサーバ	"外部syslogサーバを使用する"

グリッドフェデレーション接続証明書

証明書の種類	説明	ナビゲーション位置	詳細
サーバーとクライアント	現在の StorageGRID システムとグリッドフェデレーション接続内の別のグリッドとの間で送信される情報を認証および暗号化します。	設定 > システム > グリッド連携	"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する"

IDフェデレーション証明書

証明書の種類	説明	ナビゲーション位置	詳細
サーバ	StorageGRID と、Active Directory、OpenLDAP、Oracle Directory Server などの外部 ID プロバイダー間の接続を認証します。管理者グループとユーザーを外部システムで管理できるようにする ID フェデレーションに使用されます。	設定 > アクセス制御 > ID フェデレーション	"IDフェデレーションを使用する"

キー管理サーバー（KMS）証明書

証明書の種類	説明	ナビゲーション位置	詳細
サーバーとクライアント	StorageGRID とアプライアンスノードに暗号化キーを提供する外部キー管理サーバー（KMS）との間の接続を認証します。	設定 > セキュリティ > キー管理サーバー	"キー管理サーバー（KMS）を追加する"

プラットフォームサービスエンドポイント証明書

証明書の種類	説明	ナビゲーション位置	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。	テナント マネージャー > ストレージ（S3） > プラットフォーム サービス エンドポイント	"プラットフォームサービスエンドポイントを作成する" "プラットフォームサービスエンドポイントを編集"

シングル サインオン (SSO) 証明書

証明書の種類	説明	ナビゲーション位置	詳細
サーバ	Active Directory Federation Services (AD FS) などの ID フェデレーション サービスと、シングル サインオン (SSO) リクエストに使用される StorageGRID 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 サインオンを設定する"

証明書の例

例1：ロードバランサーサービス

この例では、StorageGRID はサーバーとして機能します。

1. StorageGRID でロードバランサーエンドポイントを設定し、サーバー証明書をアップロードまたは生成します。
2. ロードバランサーのエンドポイントへのS3クライアント接続を設定し、同じ証明書をクライアントにアップロードします。
3. クライアントがデータを保存または取得する場合、HTTPS を使用してロード バランサーの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ー証明書と、秘密鍵に基づく署名で応答します。
5. クライアントは、サーバーの署名と、自身が所有する証明書のコピーに記載されている署名を比較します。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. クライアントはオブジェクトデータを StorageGRID に送信します。

例2：外部キー管理サーバー (KMS)

この例では、StorageGRID はクライアントとして機能します。

1. 外部キー管理サーバーソフトウェアを使用して、StorageGRID を KMS クライアントとして設定し、CA 署名付きサーバー証明書、公開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サーバーを設定し、サーバー証明書、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 ノードが暗号化キーを必要とする場合、証明書からのデータと秘密鍵に基づく署名を含むリクエストを KMS サーバーに送信します。
4. KMSサーバーは証明書の署名を検証し、StorageGRID を信頼できると判断します。
5. KMSサーバーは、検証済みの接続を使用して応答します。

StorageGRID でサポートされているサーバー証明書のタイプ

StorageGRID システムは、RSA または ECDSA（楕円曲線デジタル署名アルゴリズム）で暗号化されたカスタム証明書をサポートしています。



セキュリティポリシーの暗号タイプは、サーバー証明書のタイプと一致している必要があります。例えば、RSA暗号にはRSA証明書が必要であり、ECDSA暗号にはECDSA証明書が必要です。["セキュリティ証明書を管理する"](#)を参照してください。サーバー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した場合は、["一時的にデフォルトのセキュリティポリシーに戻す"](#)。

StorageGRID がクライアント接続を保護する方法の詳細については、["S3クライアントのセキュリティ"](#)を参照してください。

StorageGRID で管理インターフェイス証明書を設定する

デフォルトの管理インターフェイス証明書を、ユーザーがセキュリティ警告を表示せずに Grid Manager および Tenant Manager にアクセスできるようにする単一のカスタム証明書に置き換えることができます。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。

タスク概要

デフォルトでは、すべての管理ノードにはグリッドCAによって署名された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。

単一のカスタム管理インターフェイス証明書がすべての管理ノードで使用されるため、クライアントがGrid ManagerおよびTenant Managerに接続する際にホスト名を検証する必要がある場合は、証明書を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ように、カスタム証明書を定義します。

サーバー上で設定を完了する必要があります。また、使用しているルート認証局（CA）によっては、ユーザーがGrid ManagerおよびTenant Managerにアクセスするために使用するWebブラウザにGrid CA証明書をインストールする必要がある場合もあります。



サーバー証明書の障害によって運用が中断されないようにするため、このサーバー証明書の有効期限が近づくと、「管理インターフェイスのサーバー証明書の有効期限」アラートがトリガーされます。必要に応じて、設定 > セキュリティ > 証明書 を選択し、グローバルタブで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にアクセスしている場合、以下のいずれかの事象が発生すると、ブラウザに証明書エラーが表示され、回避するオプションが表示されません。

- お客様の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した。
- あなた [カスタム管理インターフェイス証明書からデフォルトサーバー証明書に戻す](#)。

カスタム管理インターフェイス証明書を追加する

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、独自の証明書を用意するか、Grid Manager を使用して生成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. 「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てください。

証明書をアップロード

必要なサーバー証明書ファイルをアップロードしてください。

- a. 「証明書をアップロード」を選択します。
- b. 必要なサーバー証明書ファイルをアップロードします。
 - サーバー証明書：カスタムサーバー証明書ファイル（PEM エンコード）。
 - 証明書の秘密鍵: カスタムサーバー証明書の秘密鍵ファイル(.key)。



ECの秘密鍵は224ビット以上である必要があります。RSA秘密鍵は2048ビット以上である必要があります。

- **CA バンドル**：各中間発行認証局（CA）からの証明書を含む単一のオプションファイル。ファイルには、PEM 形式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されて含まれている必要があります。
- c. *証明書の詳細*を展開すると、アップロードした各証明書のメタデータが表示されます。オプションの CA バンドルをアップロードした場合、各証明書はそれぞれ別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、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」を選択してください。

証明書ファイル名とダウンロード場所を指定してください。拡張子`.pem`を付けてファイルを保存します。

例：storagegrid_certificate.pem

- 証明書の内容をコピーして別の場所に貼り付けるには、*証明書のPEMをコピー*または*CA バンドルのPEMをコピー*を選択してください。
- d. 「保存」を選択します。+ カスタム管理インターフェイス証明書は、Grid Manager、Tenant Manager、Grid Manager API、またはTenant Manager APIへの以降のすべての新規接続に使用されます。

証明書を生成する

サーバー証明書ファイルを生成します。



本番環境のベストプラクティスは、外部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です。

- 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IPアドレスを1つ以上指定します。

フィールド	説明
件名（任意）	証明書所有者の X.509 サブジェクトまたは識別名（DN）。 このフィールドに値が入力されない場合、生成される証明書は最初のドメイン名またはIPアドレスをサブジェクト共通名（CN）として使用します。
有効日数	証明書が発行されてから有効期限が切れるまでの日数。
キー使用拡張機能を追加する	選択した場合（デフォルトかつ推奨）、鍵使用法と拡張鍵使用法の拡張機能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、証明書に含まれる鍵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は選択したままにしてください。

c. * Generate * 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*を選択してください。

- 証明書ファイルを保存するには、*証明書をダウンロード*を選択してください。

証明書ファイル名とダウンロード場所を指定してください。拡張子`.pem`を付けてファイルを保存します。

例: `storagegrid_certificate.pem`

- 証明書の内容をコピーして別の場所に貼り付けるには、*証明書のPEMをコピー*を選択してください。

e. 「保存」を選択します。+ カスタム管理インターフェイス証明書は、Grid Manager、Tenant Manager、Grid Manager API、またはTenant Manager APIへの以降のすべての新規接続に使用されます。

5. ウェブブラウザが最新の状態であることを確認するために、ページを更新してください。



証明書をアップロードまたは新規生成した後、関連する証明書の有効期限切れアラートが解消されるまで最大1日かかる場合があります。

6. カスタム管理インターフェイス証明書を追加すると、管理インターフェイス証明書ページに使用中の証明書の詳細情報が表示されます。+ 必要に応じて、証明書の PEM をダウンロードまたはコピーできます。

デフォルトの管理インターフェイス証明書を復元する

Grid Manager および Tenant Manager 接続用のデフォルトの管理インターフェイス証明書の使用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. 「デフォルトの証明書を使用する」を選択します。

デフォルトの管理インターフェイス証明書に戻すと、設定したカスタムサーバー証明書ファイルが削除され、システムから復元できなくなります。デフォルトの管理インターフェイス証明書は、以降のすべての新規クライアント接続に使用されます。

4. ウェブブラウザが最新の状態であることを確認するために、ページを更新してください。

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する

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。

開始する前に

- "特定のアクセス権限"があります。
- あなたは `Passwords.txt` ファイルを持っています。

タスク概要

本番環境のベストプラクティスは、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です。

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. `Passwords.txt` ファイルに記載されているパスワードを入力してください。
 - c. 以下のコマンドを入力して root に切り替えます: `su -`
 - d. `Passwords.txt` ファイルに記載されているパスワードを入力してください。

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

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
```

- `--domains` には、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。
例えば、`\*.ui.storagegrid.example.com` は * ワイルドカードを使用して
`admin1.ui.storagegrid.example.com` と `admin2.ui.storagegrid.example.com` を表します。
- `--type` を `management` に設定すると、Grid Manager と Tenant Manager で使用される管理インターフェイス証明書を設定できます。
- デフォルトでは、生成された証明書は1年間（365日間）有効であり、有効期限が切れる前に再作成する必要があります。`--days` 引数を使用して、デフォルトの有効期間を上書きできます。



証明書の有効期間は、`make-certificate` を実行したときに開始されます。管理クライアントが StorageGRID と同じタイムソースに同期されていることを確認してください。同期されていない場合、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
```

出力結果には、管理APIクライアントが必要とする公開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。

選択範囲にはBEGINタグとENDタグを含めてください。

5. コマンドシェルからログアウトしてください。 `$ exit`
6. 証明書が設定されていることを確認します。
 - a. グリッドマネージャーにアクセスします。
 - 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. 管理クライアントを設定して、コピーした公開証明書を使用するようにしてください。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のダウンロードまたはコピー

管理インターフェイス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. 「サーバー」または「CA バンドル」タブを選択し、証明書をダウンロードまたはコピーしてください。

証明書ファイルまたは**CA**バンドルをダウンロードする

証明書またはCAバンドル`.pem`ファイルをダウンロードします。オプションのCAバンドルを使用している場合、バンドル内の各証明書はそれぞれ別のサブタブに表示されます。

- a. 「証明書をダウンロード」または「CAバンドルをダウンロード」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は、単一のファイルとしてダウンロードされます。

- b. 証明書ファイル名とダウンロード場所を指定してください。拡張子`.pem`を付けてファイルを保存します。

例: `storagegrid_certificate.pem`

証明書または**CA**バンドル**PEM**のコピー

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、バンドル内の各証明書はそれぞれ別のサブタブに表示されます。

- a. 「証明書のコピー（PEM形式）」または「CAバンドルのコピー（PEM形式）」を選択します。

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と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. テキストファイルを拡張子`.pem`付きで保存します。

例: `storagegrid_certificate.pem`

StorageGRIDでS3 API証明書を設定

S3クライアントがストレージノードまたはロードバランサーのエンドポイントに接続するために使用されるサーバー証明書を交換または復元できます。交換用のカスタムサーバー証明書は、お客様の組織専用のものです。



このバージョンのドキュメントサイトからは、Swiftに関する詳細情報が削除されました。参照してください ["StorageGRID 11.8 : S3およびSwift API証明書の設定"](#)。

タスク概要

デフォルトでは、すべてのストレージノードには、グリッドCAによって署名されたX.509サーバー証明書が発行されます。これらの認証局署名付き証明書は、単一の共通カスタムサーバー証明書とそれに対応する秘密鍵に置き換えることができます。

すべてのストレージノードで単一のカスタムサーバー証明書が使用されるため、クライアントがストレージエンドポイントに接続する際にホスト名を検証する必要がある場合は、証明書を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ように、カスタム証明書を定義します。

サーバー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 APIクライアントにGrid CA証明書をインストールする必要がある場合があります。



サーバー証明書の不具合によって運用が中断されないようにするため、ルートサーバー証明書の有効期限が近づくと、「S3 API のグローバルサーバー証明書の有効期限切れ」アラートがトリガーされます。必要に応じて、「設定」>「セキュリティ」>「証明書」を選択し、「グローバル」タブで S3 API 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。

カスタムS3 API証明書をアップロードまたは生成できます。

カスタム**S3 API**証明書を追加する

手順

1. **Configuration > Security > Certificates** を選択します。
2. 「グローバル」タブで、「S3 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てください。

証明書をアップロード

必要なサーバー証明書ファイルをアップロードしてください。

- a. 「証明書をアップロード」を選択します。
- b. 必要なサーバー証明書ファイルをアップロードします。
 - サーバー証明書：カスタムサーバー証明書ファイル（PEM エンコード）。
 - 証明書の秘密鍵: カスタムサーバー証明書の秘密鍵ファイル（.key）。



ECの秘密鍵は224ビット以上である必要があります。RSA秘密鍵は2048ビット以上である必要があります。

- **CA bundle**：各中間発行認証局からの証明書を含む、単一のオプションファイル。ファイルには、PEM 形式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されて含まれている必要があります。
- c. 証明書の詳細を選択すると、アップロードされた各カスタム S3 API 証明書のメタデータと PEM が表示されます。オプションの CA バンドルをアップロードした場合、各証明書はそれぞれ別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、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」を選択してください。

証明書ファイル名とダウンロード場所を指定してください。拡張子`.pem`を付けてファイルを保存します。

例：storagegrid_certificate.pem

- 証明書の内容をコピーして別の場所に貼り付けるには、*証明書のPEMをコピー*または*CA バンドルのPEMをコピー*を選択してください。
- d. * 保存 * を選択します。

カスタムサーバー証明書は、以降の新しいS3クライアント接続に使用されます。

証明書を生成する

サーバー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IPアドレスを1つ以上指定します。

フィールド	説明
件名（任意）	証明書所有者の X.509 サブジェクトまたは識別名（DN）。 このフィールドに値が入力されない場合、生成される証明書は最初のドメイン名またはIPアドレスをサブジェクト共通名（CN）として使用します。
有効日数	証明書が発行されてから有効期限が切れるまでの日数。
キー使用拡張機能を追加する	選択した場合（デフォルトかつ推奨）、鍵使用法と拡張鍵使用法の拡張機能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、証明書に含まれる鍵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は選択したままにしてください。

c. * Generate * を選択します。

d. 「証明書の詳細」を選択すると、生成されたカスタム S3 API 証明書のメタデータと PEM が表示されます。

- 証明書ファイルを保存するには、*証明書をダウンロード*を選択してください。

証明書ファイル名とダウンロード場所を指定してください。拡張子`.pem`を付けてファイルを保存します。

例: `storagegrid_certificate.pem`

- 証明書の内容をコピーして別の場所に貼り付けるには、*証明書のPEMをコピー*を選択してください。

e. * 保存 * を選択します。

カスタムサーバー証明書は、以降の新しいS3クライアント接続に使用されます。

5. デフォルトの StorageGRID サーバー証明書、アップロードされた CA 署名付き証明書、または生成されたカスタム証明書のメタデータを表示するには、タブを選択してください。



証明書をアップロードまたは新規生成した後、関連する証明書の有効期限切れアラートが解消されるまで最大1日かかる場合があります。

6. ウェブブラウザが最新の状態であることを確認するために、ページを更新してください。

7. カスタム S3 API 証明書を追加すると、S3 API 証明書ページに、使用中のカスタム S3 API 証明書の詳細な証明書情報が表示されます。+ 必要に応じて、証明書の PEM をダウンロードまたはコピーできます。

デフォルトの **S3 API** 証明書を復元する

S3クライアントからストレージノードへの接続には、デフォルトのS3 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 バランシングのエンドポイントには、デフォルトのS3 API証明書を使用することはできません。

手順

1. **Configuration > Security > Certificates** を選択します。
2. 「グローバル」タブで、「S3 API証明書」を選択します。
3. 「デフォルトの証明書を使用する」を選択します。

グローバル S3 API 証明書のデフォルトバージョンを復元すると、設定したカスタムサーバー証明書ファイルは削除され、システムから復元できなくなります。デフォルトの S3 API 証明書は、以降の Storage Nodes への新しい S3 クライアント接続に使用されます。

4. 警告を確認してデフォルトの S3 API 証明書を復元するには、**OK** を選択します。

ルートアクセス権限があり、ロード バランシングのエンドポイント接続にカスタム S3 API 証明書が使用されていた場合、デフォルトの S3 API 証明書ではアクセスできなくなるロード バランシングのエンドポイントの一覧が表示されます。影響を受けるエンドポイントを編集または削除するには、"[ロードバランサーのエンドポイントを設定する](#)"に移動してください。

5. ウェブブラウザが最新の状態であることを確認するために、ページを更新してください。

S3 API証明書をダウンロードまたはコピー

S3 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. 「グローバル」タブで、「S3 API証明書」を選択します。
3. 「サーバー」または「CA バンドル」タブを選択し、証明書をダウンロードまたはコピーしてください。

証明書ファイルまたは**CA**バンドルをダウンロードする

証明書またはCAバンドル`.pem`ファイルをダウンロードします。オプションのCAバンドルを使用している場合、バンドル内の各証明書はそれぞれ別のサブタブに表示されます。

- a. 「証明書をダウンロード」または「CAバンドルをダウンロード」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は、単一のファイルとしてダウンロードされます。

- b. 証明書ファイル名とダウンロード場所を指定してください。拡張子`.pem`を付けてファイルを保存します。

例: `storagegrid_certificate.pem`

証明書または**CA**バンドル**PEM**のコピー

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、バンドル内の各証明書はそれぞれ別のサブタブに表示されます。

- a. 「証明書のコピー（PEM形式）」または「CAバンドルのコピー（PEM形式）」を選択します。

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と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. テキストファイルを拡張子`.pem`付きで保存します。

例: `storagegrid_certificate.pem`

関連情報

- ["S3 REST APIを使用する"](#)
- ["S3エンドポイントのドメイン名を設定する"](#)

StorageGRID グリッド CA 証明書をコピーします

StorageGRID は、内部トラフィックを保護するために内部認証局（CA）を使用します。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。

開始する前に

- ["対応ウェブブラウザ"](#)を使用して Grid Manager にサインインしています。
- ["特定のアクセス権限"](#)があります。

タスク概要

カスタムサーバー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ー証明書を使用してサーバー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でください。

手順

1. **[構成]** > **[セキュリティ]** > **[証明書]** 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てください。

証明書ファイルをダウンロードする

証明書 `.pem` ファイルをダウンロードします。

- a. 「証明書をダウンロード」を選択します。
- b. 証明書ファイル名とダウンロード場所を指定してください。拡張子 `.pem` を付けてファイルを保存します。

例: `storagegrid_certificate.pem`

証明書 **PEM** のコピー

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. 「証明書のコピー（PEM形式）」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. テキストファイルを拡張子 `.pem` 付きで保存します。

例: `storagegrid_certificate.pem`

StorageGRID 証明書を FabricPool 用に設定する

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 S3 クライアント（FabricPool を使用する ONTAP クライアントなど）の場合、ロードバランサーエンドポイントを設定する際にサーバー証明書を生成またはアップロードできます。

開始する前に

- ["特定のアクセス権限"](#)があります。
- ["対応ウェブブラウザ"](#) を使用して Grid Manager にサインインしています。

タスク概要

ロードバランサーのエンドポイントを作成する際、自己署名サーバー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することができます。本番環境では、既知の認証局（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。認証局（CA）が署名した証明書は、システムへの影響を最小限に抑えながらローテーションできます。また、中間者攻撃に対する保護性能が高いため、セキュリティ面でも優れています。

以下の手順は、FabricPool を使用する S3 クライアントの一般的なガイドラインを示しています。詳細な情報と手順については、["StorageGRID を FabricPool 用に設定する"](#) を参照してください。

手順

1. オプションで、FabricPoolが使用する高可用性（HA）グループを構成します。
2. FabricPool が使用する S3 ロードバランサーエンドポイントを作成します。

HTTPS ロードバランサーエンドポイントを作成する際、サーバー証明書、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. StorageGRID をクラウド階層として ONTAP に接続します。

アップロードした CA 証明書で使われているロードバランサーのエンドポイントポートと完全修飾ドメイン名を指定してください。次に、CA 証明書を提供してください。



中間 CA が StorageGRID 証明書を発行した場合は、中間 CA 証明書を提供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 証明書を提供する必要があります。

StorageGRID で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、承認された外部クライアントが StorageGRID の Prometheus データベースにアクセスできるようになり、外部ツールが StorageGRID を監視するための安全な方法が提供されます。

外部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、Grid Manager 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、証明書情報を外部ツールにコピーする必要があります。

"[セキュリティ証明書を管理する](#)"および"[カスタムサーバー証明書の設定](#)"を参照してください。



サーバー証明書の不具合によって運用が中断されないようにするため、このサーバー証明書の有効期限が近づくと、「証明書」ページで設定されているクライアント証明書の有効期限切れアラートがトリガーされます。必要に応じて、**Configuration > Security > Certificates** を選択し、「クライアント」タブで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。



特別に構成されたアプライアンスノードのデータを保護するためにキー管理サーバー（KMS）を使用している場合は、"[KMSクライアント証明書のアップロード](#)"に関する詳細情報を参照してください。

開始する前に

- ルートアクセス権限があります。
- "[対応ウェブブラウザ](#)"を使用して Grid Manager にサインインしています。
- 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持っています。
 - StorageGRID の管理インターフェイス証明書を設定済みの場合は、管理インターフェイス証明書の設定に使用した CA、クライアント証明書、および秘密鍵が必要です。
 - 独自の証明書をアップロードするには、証明書の秘密鍵がローカルコンピュータに保存されている必要があります。
 - 秘密鍵は、作成時に保存または記録されていなければなりません。元の秘密鍵をお持ちでない場合

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持っています。
 - 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、秘密鍵、クライアント証明書、および CA（使用する場合）がローカルコンピュータで使用可能である必要があります。

クライアント証明書を追加する

クライアント証明書を追加するには、以下のいずれかの手順を使用してください。

- [\[管理インターフェイス証明書は既に設定されています。\]](#)
- [CAが発行したクライアント証明書](#)
- [\[グリッドマネージャーから生成された証明書\]](#)

管理インターフェイス証明書は既に設定されています。

管理インターフェイス証明書が、顧客から提供された CA、クライアント証明書、および秘密鍵を使用してすでに構成されている場合に、クライアント証明書を追加するにはこの手順を使用します。

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. 証明書名を入力してください。
4. 外部監視ツールを使用して Prometheus メトリクスにアクセスするには、***Prometheusを許可する***を選択してください。
5. ***続行***を選択します。
6. 「証明書の添付」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. 「証明書をアップロード」を選択します。
 - b. 「参照」を選択して、管理インターフェイス証明書ファイル(.pem) を選択します。
 - 「クライアント証明書の詳細」を選択すると、証明書のメタデータと証明書 PEM が表示されます。
 - 証明書の内容をコピーして別の場所に貼り付けるには、***証明書のPEMをコピー***を選択してください。
 - c. 証明書をグリッドマネージャーに保存するには、***作成***を選択します。

新しい証明書は「クライアント」タブに表示されます。

7. [外部監視ツールの設定](#)（Grafanaなど）。

CAが発行し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おらず、CAが発行したクライアント証明書と秘密鍵を使用する Prometheus 用のクライアント証明書を追加する予定がある場合は、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. 以下の手順を実行してください["管理インターフェイス証明書を設定する"](#)。
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. 証明書名を入力してください。
5. 外部監視ツールを使用して Prometheus メトリクスにアクセスするには、***Prometheusを許可する***を選択してください。
6. ***続行***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てください。
 - a. 「証明書をアップロード」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」を選択すると、証明書のメタデータと証明書 PEM が表示されます。
 - 証明書の内容をコピーして別の場所に貼り付けるには、***証明書のPEMをコピー***を選択してください。
 - c. 証明書をグリッドマネージャーに保存するには、***作成***を選択します。

新しい証明書は「クライアント」タブに表示されます。

8. [外部監視ツールの設定](#) (Grafanaなど)。

グリッドマネージャーから生成された証明書

管理インターフェイス証明書が設定されておらず、Grid Manager の証明書生成機能を使用して Prometheus 用のクライアント証明書を追加する予定がある場合は、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てください。

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. 証明書名を入力してください。
4. 外部監視ツールを使用して Prometheus メトリクスにアクセスするには、***Prometheusを許可する***を選択してください。
5. ***続行***を選択します。
6. 「証明書を添付する」手順では、「証明書を生成する」を選択します。
7. 証明書情報を指定します：
 - 件名（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）。
 - 有効日数：生成された証明書が、生成された時点から有効となる日数。
 - キー使用拡張機能の追加：選択した場合（デフォルトかつ推奨）、キー使用と拡張キー使用拡張機能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、証明書に含まれる鍵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しない限り、このチェックボックスは選択したままにしてください。

8. *Generate* を選択します。

9. *クライアント証明書の詳細*を選択すると、証明書のメタデータと証明書のPEMが表示されます。



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てください。

- 証明書の内容をコピーして別の場所に貼り付けるには、*証明書のPEMをコピー*を選択してください。
- 証明書ファイルを保存するには、*証明書をダウンロード*を選択してください。

証明書ファイル名とダウンロード場所を指定してください。拡張子`.pem`を付けてファイルを保存します。

例：storagegrid_certificate.pem

- 証明書の秘密鍵をコピーして別の場所に貼り付けるには、「秘密鍵をコピー」を選択してください。
- 秘密鍵をファイルとして保存するには、*秘密鍵をダウンロード*を選択してください。

秘密鍵ファイル名とダウンロード場所を指定してください。

10. 証明書をグリッドマネージャーに保存するには、*作成*を選択します。

新しい証明書は「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. [クライアント証明書の詳細](#) のステップから certificate.pem および private_key.pem ファイルをアップロードします。CA バンドルをアップロードする必要はありません。

- 「証明書をアップロード」を選択し、「続行」を選択します。
- 各証明書ファイルをアップロードします (.pem) 。
- 証明書を Grid Manager に保存するには、*保存*を選択します。

新しい証明書は、管理インターフェイスの証明書ページに表示されます。

15. [外部監視ツールの設定](#) (Grafanaなど) 。

外部監視ツールの設定

手順

1. Grafanaなどの外部監視ツールで、以下の設定を行ってください。

- a. 名前：接続の名前を入力してください。

StorageGRID はこの情報を必要としませんが、接続をテストするには名前を入力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アドレスを入力してください。HTTPSとポート9091を指定してください。

例： `https://admin-node.example.com:9091`

- c. *TLSクライアント認証*と*CA証明書を使用*を有効にします。

- d. TLS/SSL認証の詳細の下に、以下をコピーして貼り付けてください：+

- 管理インターフェイスのCA証明書を**CA Cert**に
- クライアント証明書をクライアント証明書に
- クライアントキーの秘密鍵

- e. **ServerName**：管理ノードのドメイン名を入力してください。

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。

外部監視ツールを使用して、StorageGRID から Prometheus メトリクスにアクセスできるようになりました。

指標に関する情報については、"[StorageGRID の監視に関する手順](#)"を参照してください。

クライアント証明書を編集する

管理者クライアント証明書を編集することで、名前の変更、Prometheus へのアクセスの有効化または無効化、あるいは現在の証明書の有効期限が切れた場合の新しい証明書のアップロードを行うことができます。

手順

1. **Configuration > Security > Certificates** を選択し、**Client** タブを選択します。

証明書の有効期限とPrometheusへのアクセス権限は、表に記載されています。証明書の有効期限が間もなく切れる場合、または既に切れている場合は、テーブルにメッセージが表示され、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てください。
3. 「編集」を選択し、次に「名前と権限の編集」を選択します。
4. 証明書名を入力してください。
5. 外部監視ツールを使用して Prometheus メトリクスにアクセスするには、*Prometheusを許可する*を選択してください。
6. 証明書を Grid Manager に保存するには、**続行** を選択します。

更新された証明書は「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添付する

現在使用している証明書の有効期限が切れた場合は、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へのアクセス権限は、表に記載されています。証明書の有効期限が間もなく切れる場合、または既に切れている場合は、テーブルにメッセージが表示され、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てください。
3. **Edit** を選択し、次に編集オプションを選択します。

証明書をアップロード

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. 「証明書をアップロード」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てください（.pem）。

「クライアント証明書の詳細」を選択すると、証明書のメタデータと証明書 PEM が表示されます。

- 証明書ファイルを保存するには、*証明書をダウンロード*を選択してください。

証明書ファイル名とダウンロード場所を指定してください。拡張子`.pem`を付けてファイルを保存します。

例：storagegrid_certificate.pem

- 証明書の内容をコピーして別の場所に貼り付けるには、*証明書の PEM をコピー*を選択してください。
- c. 証明書をグリッドマネージャーに保存するには、*作成*を選択します。

更新された証明書は「クライアント」タブに表示されます。

証明書を生成する

証明書のテキストを生成し、別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：
 - 件名（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）。
 - 有効日数：生成された証明書が、生成された時点から有効となる日数。
 - キー使用拡張機能の追加：選択した場合（デフォルトかつ推奨）、キー使用と拡張キー使用拡張機能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、証明書に含まれる鍵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しない限り、このチェックボックスは選択したままにしてください。

- c. *Generate* を選択します。
- d. 「クライアント証明書の詳細」を選択すると、証明書のメタデータと証明書 PEM が表示されます。



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てください。

- 証明書の内容をコピーして別の場所に貼り付けるには、*証明書の PEM をコピー*を選択してください。

- 証明書ファイルを保存するには、*証明書をダウンロード*を選択してください。

証明書ファイル名とダウンロード場所を指定してください。拡張子`.pem`を付けてファイルを保存します。

例：storagegrid_certificate.pem

- 証明書の秘密鍵をコピーして別の場所に貼り付けるには、「秘密鍵をコピー」を選択してください。
- 秘密鍵をファイルとして保存するには、*秘密鍵をダウンロード*を選択してください。

秘密鍵ファイル名とダウンロード場所を指定してください。

- e. 証明書をグリッドマネージャーに保存するには、*作成*を選択します。

新しい証明書は「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する

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てください。
3. 証明書をダウンロードまたはコピーしてください。

証明書ファイルをダウンロードする

証明書`.pem`ファイルをダウンロードします。

- a. 「証明書をダウンロード」を選択します。
- b. 証明書ファイル名とダウンロード場所を指定してください。拡張子`.pem`を付けてファイルを保存します。

例：storagegrid_certificate.pem

証明書のコピー

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. 「証明書のコピー（PEM形式）」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. テキストファイルを拡張子`.pem`付きで保存します。

例：storagegrid_certificate.pem

クライアント証明書を削除する

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てください。
3. 「削除」を選択し、確認してください。



最大 10 個の証明書を削除するには、クライアント タブで削除する証明書をそれぞれ選択し、アクション > 削除 を選択します。

証明書が削除されると、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に新しいクライアント証明書を指定する必要があります。

セキュリティ設定を構成する

StorageGRID でTLSおよびSSHポリシーを管理する

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安全なTLS接続および内部StorageGRIDサービスへの安全なSSH接続を確立するため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が転送中のデータをどのように暗号化するかを制御します。一般的には、システムがCommon Criteriaに準拠する必要がある場合や、他の暗号方式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、これらのポリシーの暗号化を使用するように更新されていません。

開始する前に

- "[対応ウェブブラウザ](#)" を使用して Grid Manager にサインインしています。
- あなたは"[ルートアクセス権限](#)"があります。

セキュリティポリシーを選択してください

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、利用可能なポリシーが表示されます。現在有効なポリシーは、ポリシータイトルに緑色のチェックマークで示されます。



2. 各タブを確認して、利用可能なポリシーについて学習してください。

最新互換性（デフォルト）

強力な暗号化が必要で、特別な要件がない場合は、デフォルトポリシーを使用してください。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

古いクライアントとの互換性に関する追加オプションが必要な場合は、レガシー互換性ポリシーを使用してください。このポリシーに含まれる追加オプションは、最新の互換性ポリシーよりもセキュリティを低下させる可能性があります。

共通基準

共通基準認証が必要な場合は、共通基準ポリシーを使用してください。

FIPS strict

Common Criteria認証が必要で、ロードバランサーエンドポイント、テナントマネージャ、およびグリッドマネージャへの外部クライアント接続にNetApp Cryptographic Security Module (NCSM) 3.0.8またはNetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64モジュールを使用する必要がある場合は、FIPSの厳格なポリシーを使用してください。このポリシーを使用すると、パフォーマンスが低下する可能性があります。

NCSM 3.0.8とNetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64モジュールは、以下の操作で使用されます。

◦ NCSM

- 以下のサービス間のTLS接続：ADC、AMS、CMN、DDS、LDR、SSM、NMS、mgmt-api、nginx、nginx-gw、およびcache-svc
- クライアントとnginx-gwサービス（ロードバランサーのエンドポイント）間のTLS接続
- クライアントとLDRサービス間のTLS接続
- SSE-S3、SSE-C、および保存オブジェクト暗号化設定のオブジェクトコンテンツ暗号化
- SSH 接続

詳細については、NIST 暗号化アルゴリズム検証プログラム ["証明書番号4838"](#) を参照してください。

◦ NetApp StorageGRID カーネル暗号化 API モジュール

NetApp StorageGRID カーネル暗号化 API モジュールは、VM および StorageGRID アプライアンス プラットフォームにのみ存在します。

- エントロピーコレクション
- ノード暗号化

詳細については、NIST 暗号化アルゴリズム検証プログラム ["証明書番号A6242～A6257"](#) および ["エントロピー証明書番号E223"](#) を参照してください。

注: このポリシーを選択すると、["ローリングリブートを実行する"](#)すべてのノードで NCSM がアクティブ化されます。メンテナンス > ローリング再起動 を使用して、再起動を開始および監視します。

Custom

独自の暗号方式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てください。

オプションとして、StorageGRID に FIPS 140 の暗号化要件がある場合は、FIPS モード機能を有効にして NCSM 3.0.8 および NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64 モジュールを使用してください：

- a. `fipsMode` パラメータを `true` に設定します。
- b. 指示されたら、"**ローリングリブートを実行する**"すべてのノードの暗号化モジュールをアクティブ化します。**Maintenance > Rolling reboot** を使用して、再起動を開始および監視します。
- c. アクティブな FIPS モジュールバージョンを表示するには、サポート > 診断 を選択してください。

3. 各ポリシーの暗号、プロトコル、アルゴリズムの詳細を確認するには、*詳細を表示*を選択してください。
4. 現在のポリシーを変更するには、*ポリシーを使用する*を選択してください。

ポリシータイトルの **Current policy** の横に緑色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する

独自の暗号方式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. 作成したいカスタムポリシーに最も近いポリシーのタイトルから、*詳細を表示*を選択します。
2. 「クリップボードにコピー」を選択し、次に「キャンセル」を選択します。



3. 「カスタムポリシー」タイトルから「設定して使用する」を選択します。
4. コピーしたJSONを貼り付け、必要に応じて変更を加えてください。
5. 「ポリシーを使用」を選択します。

カスタムポリシーのタイトルにある **Current policy** の横に緑色のチェックマークが表示されます。

- 必要に応じて、設定の編集を選択すると、新しいカスタムポリシーにさらに変更を加えることができます。

一時的にデフォルトのセキュリティポリシーに戻す

カスタムセキュリティポリシーを設定した場合、設定されたTLSポリシーが"[構成済みのサーバー証明書](#)"と互換性がないと、Grid Managerにサインインできない可能性があります。

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

- 管理ノードにログインします。
 - 次のコマンドを入力します：`ssh admin@Admin_Node_IP`
 - 'Passwords.txt' ファイルに記載されているパスワードを入力してください。
 - 以下のコマンドを入力して root に切り替えます：`su -`
 - 'Passwords.txt' ファイルに記載されているパスワードを入力してください。

rootとしてログインすると、プロンプトが`\$`から`#`に変わります。

- 次のコマンドを実行します。

```
restore-default-cipher-configurations
```

- ウェブブラウザから、同じ管理ノード上のグリッドマネージャにアクセスします。
- [セキュリティポリシーを選択してください](#)の手順に従って、ポリシーを再度設定してください。

StorageGRID ネットワークとオブジェクトのセキュリティを設定する

ネットワークおよびオブジェクトのセキュリティを設定することで、保存されているオブジェクトを暗号化したり、特定のS3リクエストを防止したり、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したりできます。

保存オブジェクトの暗号化

保存オブジェクト暗号化機能を使用すると、S3 を介して取り込まれる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、保存された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、新しく取り込まれたすべてのオブジェクトは暗号化されますが、既存の保存済みオブジェクトには変更は加えられません。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になりますが、新しく取り込まれたオブジェクトは暗号化されません。

保存済み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によって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 の暗号化方式の詳細については、"[StorageGRID の暗号化方式の確認](#)"を参照してください。

クライアントの変更を防止する

クライアントによる変更を防止する設定は、システム全体に適用される設定です。*クライアントによる変更

を防止する*オプションが選択されている場合、以下の要求は拒否されます。

S3 REST API

- DeleteBucketリクエスト
- 既存オブジェクトのデータ、ユーザー定義メタデータ、またはS3オブジェクトのタグ付けを変更するリクエスト

ストレージノード接続でHTTPを有効にする

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。必要に応じて、これらの接続でHTTPを有効にすることもできます。たとえば、非本番環境のグリッドをテストする場合などです。

S3クライアントがストレージノードに直接HTTP接続を行う必要がある場合にのみ、ストレージノードへの接続にHTTPを使用してください。HTTPS接続のみを使用するクライアント、またはロードバランサーサービスに接続するクライアントには、このオプションは不要です（HTTPまたはHTTPSのいずれかを使用するように"[各ロードバランサーエンドポイントを設定する](#)"できるため）。

"概要：クライアント接続用の IP アドレスとポート番号"を参照して、S3クライアントがHTTPまたはHTTPSを使用してStorage Nodeに接続する際に使用するポートを確認してください。

オプションを選択

開始する前に

- "[対応ウェブブラウザ](#)"を使用して Grid Manager にサインインしています。
- ルートアクセス権限があります。

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. 保存オブジェクトの暗号化については、保存オブジェクトを暗号化しない場合は **None**（デフォルト）設定を使用し、保存オブジェクトを暗号化する場合は **AES-128** または **AES-256** を選択してください。
4. S3クライアントが特定のリクエストを行うことを禁止する場合は、必要に応じて「クライアントによる変更を禁止する」を選択してください。



この設定を変更した場合、新しい設定が適用されるまで約1分かかります。設定された値は、パフォーマンスとスケーリングのためにキャッシュされます。

5. 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、必要に応じて「ストレージノード接続でHTTPを有効にする」を選択します。



本番環境のグリッドでHTTPを有効にする際は、リクエストが暗号化されずに送信されるため注意が必要です。

6. * 保存 * を選択します。

StorageGRIDインターフェイスのセキュリティ設定を変更する

インターフェイスのセキュリティ設定では、ユーザーが指定された時間以上操作を行わない場合にログアウトするかどうか、および API エラー応答にスタックトレースを含めるかどうかを制御できます。

開始する前に

- ["対応ウェブブラウザ"](#) を使用して Grid Manager にサインインしています。
- ["ルートアクセス権限"](#)があります。

タスク概要

「セキュリティ設定」ページには、「ブラウザの非アクティブタイムアウト」と「管理 API スタックトレース」の設定が含まれています。

ブラウザの非アクティブタイムアウト

ユーザーがサインアウトされるまでに、ブラウザが非アクティブ状態でいられる時間を示します。デフォルトは15分です。

ブラウザの非アクティブタイムアウトは、以下の要素によっても制御されます。

- システムセキュリティのために含まれている、別個の設定不可能な StorageGRID タイマーです。各ユーザーの認証トークンは、ユーザーがサインインしてから 16 時間後に期限切れになります。ユーザー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、そのユーザー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、ユーザーは再度サインインする必要があります。
- IDプロバイダー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を想定）。

SSO が有効になっていて、ユーザーのブラウザがタイムアウトした場合、ユーザーは StorageGRID に再度アクセスするために SSO 認証情報を再入力する必要があります。["SSOの動作"](#)を参照してください。

管理APIスタックトレース

Grid ManagerおよびTenant Manager APIのエラー応答でスタックトレースを返すかどうかを制御します。

このオプションはデフォルトでは無効になっていますが、テスト環境でこの機能を有効にすることをお勧めします。一般的に、API エラーが発生した際に内部ソフトウェアの詳細が漏洩するのを避けるため、本番環境ではスタックトレースを無効にしておくことをお勧めします。

手順

1. **Configuration > Security > Security settings** を選択します。
2. 「インターフェース」タブを選択します。
3. ブラウザの非アクティブタイムアウトの設定を変更するには：
 - a. アコーディオンを展開します。
 - b. タイムアウト期間を変更するには、60秒から7日間の間の値を指定してください。デフォルトのタイムアウト時間は15分です。
 - c. この機能を無効にするには、チェックボックスの選択を解除してください。

- d. * 保存 * を選択します。

この新しい設定は、現在ログインしているユーザーには影響しません。新しいタイムアウト設定を有効にするには、ユーザーは再度ログインするか、ブラウザを更新する必要があります。

4. 管理 API スタック トレースの設定を変更するには：

- a. アコーディオンを展開します。
- b. Grid ManagerおよびTenant Manager APIのエラー応答にスタックトレースを返すには、このチェックボックスを選択してください。



APIエラーが発生した際に内部ソフトウェアの詳細が漏洩するのを防ぐため、本番環境ではスタックトレースを無効のままにしてください。

- c. * 保存 * を選択します。

StorageGRIDで外部SSHアクセスを管理する

外部からのアクセスをブロックまたは許可することで、グリッドへの受信トラフィックに対するSSHアクセスを管理します。SSH外部アクセスを管理しても、グリッド内のノード間のトラフィックには影響しません。

開始する前に

- ["対応ウェブブラウザ"](#) を使用して Grid Manager にサインインしています。
- ["ルートアクセス権限"](#)があります。

タスク概要

システムセキュリティを強化するため、外部からのSSHアクセスはデフォルトでブロックされています。トラブルシューティングなど、受信SSHアクセスを必要とするタスクを実行する必要がある場合は、一時的に外部アクセスを許可してください。作業が完了したら、外部からのアクセスを遮断してください。

手順

1. **Configuration > Security > Security settings** を選択します。
2. 「SSH をブロック」タブを選択します。
3. 外部からの SSH アクセスを管理するには、*受信 SSH アクセスをブロック*オプションを使用します。
 - a. アクセスをブロックするには、チェックボックスを選択します（デフォルト）。
 - b. アクセスを許可するには、チェックボックスの選択を解除してください。



サービス用ラップトップと他のすべてのグリッドノード間で、ポート22へのアクセスが必要です。メンテナンス作業が完了したら、ポート22へのアクセスを削除してください。

4. * 保存 * を選択します。

キー管理サーバの設定

StorageGRIDのキー管理サーバーについて学ぶ

キー管理サーバー（KMS）は、Key Management Interoperability Protocol（KMIP）を使用して、関連付けられた StorageGRID サイトの StorageGRID アプライアンスノードに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。

StorageGRID は特定のキー管理サーバーのみをサポートしています。サポートされている製品とバージョンの一覧については、"[NetApp Interoperability Matrix Tool \(IMT\)](#)"を使用してください。

1 つ以上のキー管理サーバーを使用して、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暗号化キーを管理できます。これらのアプライアンスノードでキー管理サーバーを使用することで、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データを保護できます。アプライアンスのボリュームが暗号化されると、ノードが KMS と通信できない限り、アプライアンス上のデータにアクセスできなくなります。

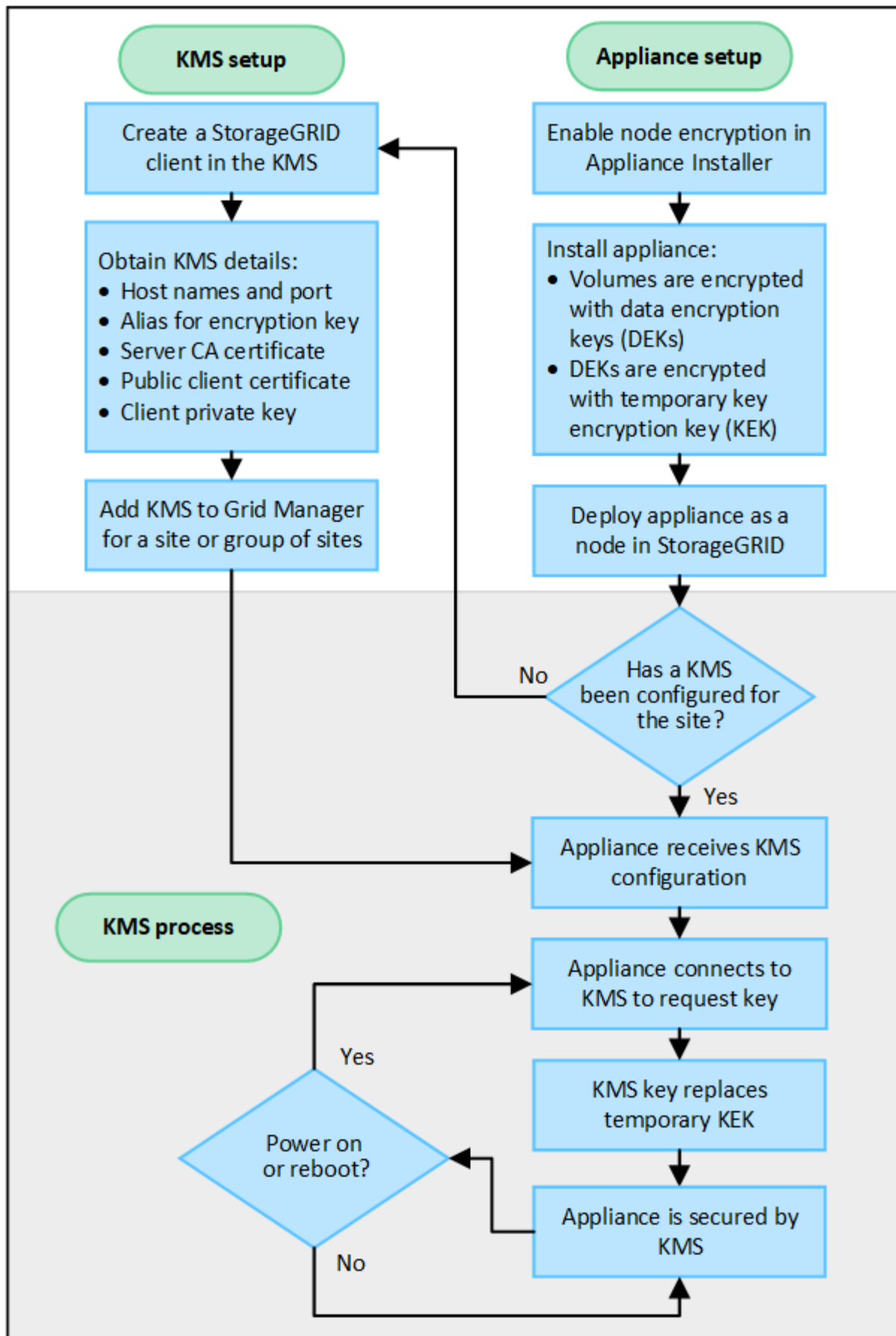


StorageGRID は、アプライアンスノードの暗号化および復号化に使用される外部キーを作成または管理しません。外部キー管理サーバーを使用して StorageGRID データを保護する予定がある場合は、そのサーバーの設定方法と暗号化キーの管理方法を理解する必要があります。キー管理タスクの実行は、本手順書の範囲外です。サポートが必要な場合は、キー管理サーバーのドキュメントを参照するか、テクニカルサポートにお問い合わせください。

StorageGRID キー管理サーバとアプライアンスの設定

キー管理サーバー（KMS）を使用してアプライアンスノード上の StorageGRID データを保護するには、2 つの構成タスクを完了する必要があります。1 つ以上の KMS サーバーをセットアップし、アプライアンスノードのノード暗号化を有効にします。これら 2 つの構成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。

このフローチャートは、KMS を使用してアプライアンスノード上の StorageGRID データを保護するための概要手順を示しています。



フローチャートでは、KMSの設定とアプライアンスの設定が並行して行われるように示されていますが、要

件に応じて、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または後にキー管理サーバーを設定することもできます。

キー管理サーバー（KMS）をセットアップする

キー管理サーバーの設定には、以下の概要手順が含まれます。

手順	参照先
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 のクライアントを追加します。	"StorageGRID をKMS のクライアントとして設定する"
KMS 上の StorageGRID クライアントに必要な情報を取得します。	"StorageGRID をKMS のクライアントとして設定する"
Grid Manager に KMS を追加し、単一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 構成を保存します。	"キー管理サーバー（KMS）を追加する"

機器をセットアップする

KMSで使用するアプライアンスノードの設定には、以下の概要手順が含まれます。

1. アプライアンスのインストールにおけるハードウェア構成段階では、StorageGRID Appliance Installer 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後では、*ノード暗号化*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に対しては、外部キー管理を使用することはできません。

2. StorageGRID アプライアンスインストーラを実行します。インストール中に、ランダムなデータ暗号化キー（DEK）が各アプライアンスボリュームに次のように割り当てられます。
 - DEKは、各ボリューム上のデータを暗号化するために使用されます。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るため、変更することはできません。
 - 各 DEK は、マスターキー暗号化キー（KEK）によって暗号化されます。初期 KEK は、アプライアンスが KMS に接続できるようになるまで DEK を暗号化するための一時的なキーです。
3. アプライアンスノードをStorageGRIDに追加します。

詳細については、["ノード暗号化を有効にする"](#)を参照してください。

鍵管理暗号化プロセス（自動的に実行されます）

キー管理暗号化には、自動的に実行される以下の概要手順が含まれます。

1. ノード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 構成が存在するかどうかを判断します。

- サイトに対して既にKMSが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。
- サイトに対してKMSがまだ構成されていない場合、サイトに対してKMSを構成し、アプライアンスがKMS構成を受信するまで、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続けます。

2. アプライアンスは KMS 構成を使用して 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 から取得した新しいキーは一時的な KEK に取って代わり、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す。



暗号化されたアプライアンスノードが構成済みのKMSに接続する前に存在するデータはすべて、一時的なキーで暗号化されます。ただし、一時キーがKMSの暗号化キーに置き換えられるまでは、アプライアンスボリュームはデータセンターからの持ち出しから保護されているとはみなすべきではありません。

4. 機器の電源がオンになったり再起動されたりすると、KMS に再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、電源喪失や再起動によって失われます。

StorageGRID キー管理サーバの要件と考慮事項

外部キー管理サーバー（KMS）を設定する前に、考慮事項と要件を理解しておく必要があります。

どのバージョンの**KMIP**がサポートされていますか？

StorageGRID は KMIP バージョン 1.4 をサポートしています。

"鍵管理相互運用性プロトコル仕様バージョン1.4"

ネットワークに関する考慮事項は何ですか？

ネットワークファイアウォールの設定では、各アプライアンスノードがキー管理相互運用プロトコル（KMIP）通信に使用され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。KMIPのデフォルトポートは5696です。

ノード暗号化を使用する各アプライアンスノードが、その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 アクセスを持つことを確認する必要があります。

サポートされている**TLS**のバージョンはどれですか？

アプライアンスノードと設定済みのKMS間の通信には、安全なTLS接続が使用されます。StorageGRID は、KMSまたはKMSクラスタへのKMIP接続を行う際に、KMSがサポートする内容と使用している"[TLSおよびSSHポリシー](#)"に基づいて、TLS 1.2またはTLS 1.3プロトコルのいずれかをサポートできます。

StorageGRID は、接続時に KMS とプロトコルおよび暗号（TLS 1.2）または暗号スイート（TLS 1.3）についてネゴシエートします。利用可能なプロトコル バージョンと暗号/暗号スイートを確認するには、グリッドのアクティブな TLS および SSH ポリシーの `tlsOutbound` セクションを参照してください（構成 > セキュリティ セキュリティ設定）。

どの機器がサポートされていますか？

キー管理サーバー（KMS）を使用して、グリッド内の StorageGRID アプライアンスのうち、*ノード暗号化*

設定が有効になっているものの暗号化キーを管理できます。この設定は、StorageGRID Appliance Installer を使用したアプライアンスのインストール時のハードウェア構成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後では、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に対しては、外部キー管理を使用することはできません。

設定済みのKMSは、StorageGRIDアプライアンスおよびアプライアンスノードに使用できます。

構成済みのKMSは、以下のものを含むソフトウェアベース（アプライアンス以外）のノードには使用できません。

- 仮想マシン（VM）としてデプロイされたノード
- Linuxホスト上のコンテナエンジン内にデプロイされたノード

これらの他のプラットフォームに展開されたノードは、データストアまたはディスクレベルで StorageGRID の外部の暗号化を使用できます。

キー管理サーバーはいつ設定すべきですか？

新規インストールの場合、通常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ーを設定する必要があります。この手順により、オブジェクトデータがノードに保存される前に、ノードが保護されることが保証されます。

アプライアンスノードをインストールする前でも後でも、Grid Managerでキー管理サーバーを設定できます。

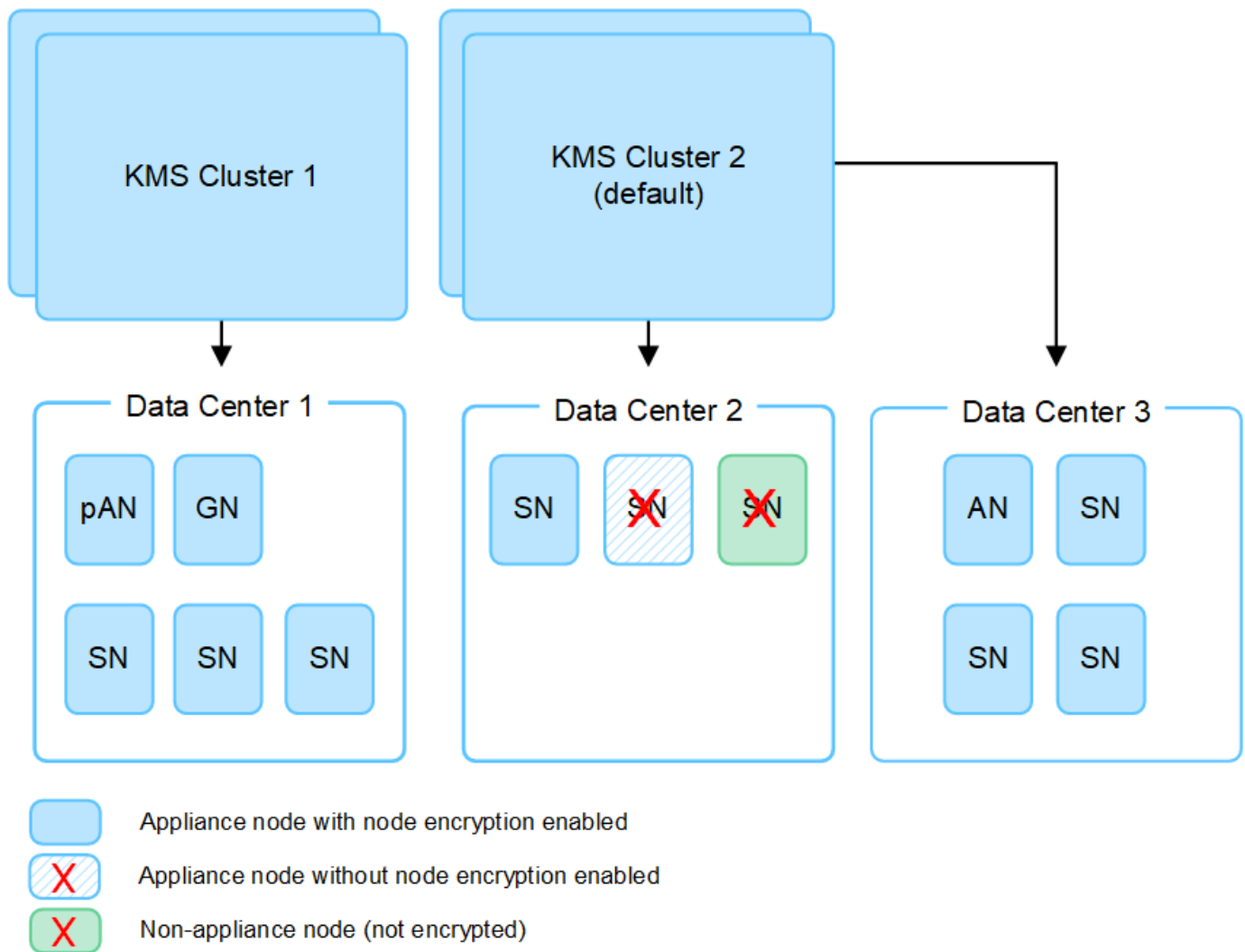
鍵管理サーバーはいくつ必要ですか？

StorageGRID システムのアプライアンスノードに暗号化キーを提供する外部キー管理サーバーを 1 つ以上構成できます。各 KMS は、単一サイトまたは複数サイトのグループにある 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、構成設定と暗号化キーを共有する複数のレプリケートされたキー管理サーバーが含まれています。KMS クラスタをキー管理に使用することを推奨します。これにより、高可用性構成のフェイルオーバー機能が向上します。

例えば、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。データセンター1のすべてのアプライアンスノードにキーを提供するKMSクラスタを1つ構成し、他のすべてのサイトのすべてのアプライアンスノードにキーを提供するKMSクラスタをもう1つ構成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のデフォルトKMSを設定できます。

アプライアンス以外のノード、またはインストール時に「ノード暗号化」設定が有効になっていなかった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、設定済みの各KMSで使用する"**暗号化キーをローテーションする**"を定期的 to 実施する必要があります。

新しいキーバージョンが利用可能になった場合：

- これは、KMSに関連付けられた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布されます。キーのローテーションから1時間以内に配布が行われます。
- 新しいキーバージョンが配布される際に暗号化アプライアンスノードがオフラインの場合、ノードは再起動後すぐに新しいキーを受信します。
- 何らかの理由で新しいキーバージョン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、アプライアンスノードに対して **KMS暗号化キーのローテーション失敗** アラートがトリガーされます。このアラートの解決については、テクニカルサポートにお問い合わせください。

暗号化されたアプライアンスノードを再利用することはできますか？

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、まずグリッドノードを廃止して、オブジェクトデータを別のノードに移動する必要があります。その後、StorageGRID Appliance Installer を使用して "**KMS構成をクリアする**"ことができます。KMS 構成をクリアすると、*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 構成との関連付けが削除されます。



KMSの暗号化キーにアクセスできない場合、アプライアンスに残っているデータはすべてアクセス不能となり、永久にロックされます。

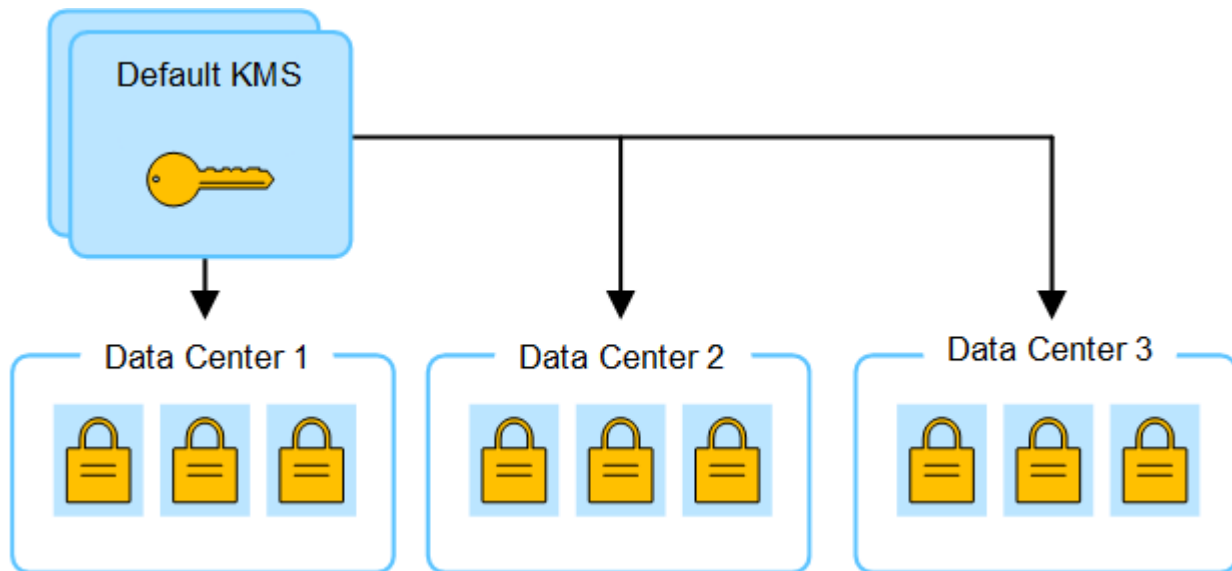
StorageGRID サイトの KMS を変更する際の考慮事項

各キー管理サーバー（KMS）またはKMSクラスタは、単一サイトまたは複数のサイト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、ある KMS から別の KMS に暗号化キーをコピーする必要があります。

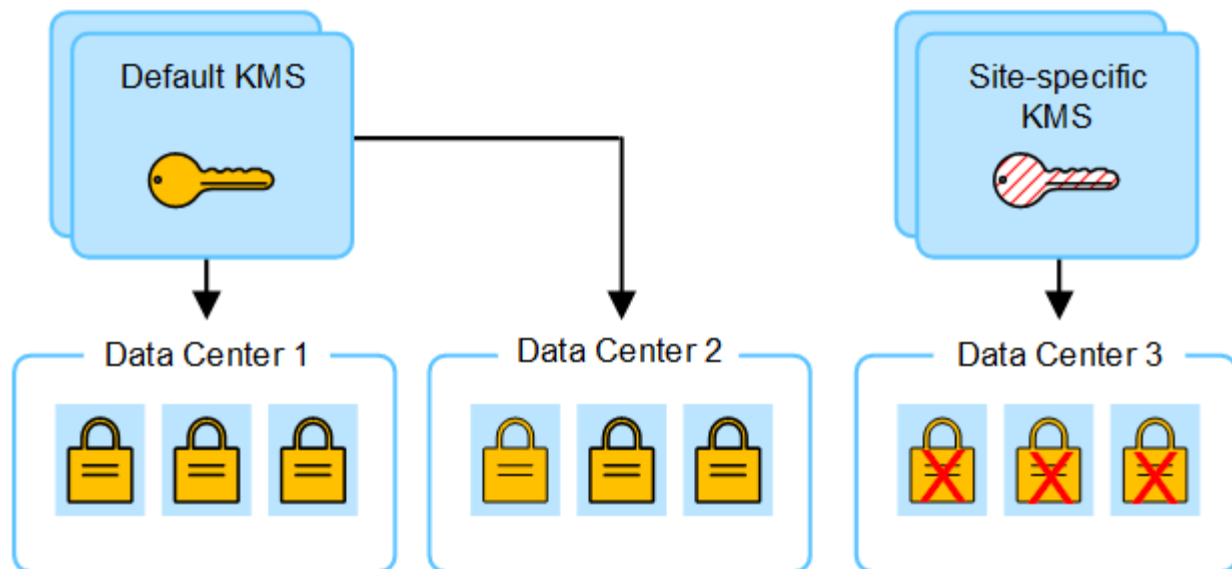
サイトで使用するKMSを変更する場合は、そのサイトの以前に暗号化されていたアプライアンスノードが、新しいKMSに保存されているキーを使用して復号できることを確認する必要があります。場合によっては、現在のバージョンの暗号化キーを元のKMSから新しいKMSにコピーする必要があります。KMSが、サイト内の暗号化されたアプライアンスノードを復号化するための正しいキーを保持していることを確認する必要があります。

次に例を示します。

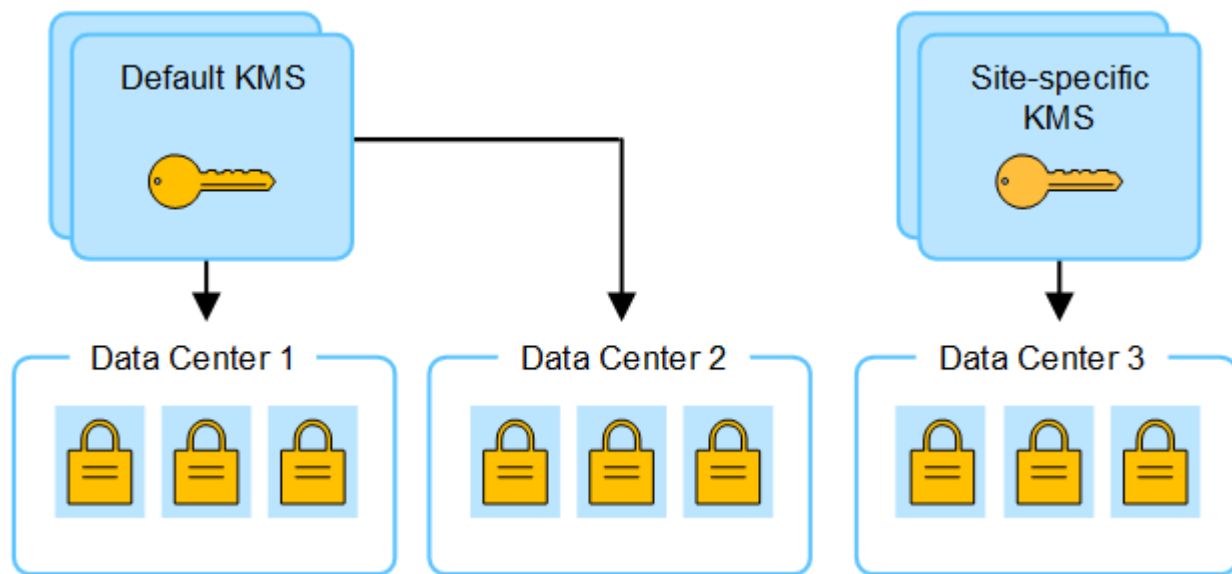
1. 最初に、専用のKMSを持たないすべてのサイトに適用されるデフォルトのKMSを設定します。
2. KMSが保存されると、*ノード暗号化*設定が有効になっているすべてのアプライアンスノードがKMSに接続し、暗号化キーを要求します。このキーは、すべてのサイトにあるアプライアンスノードを暗号化するために使用されます。これらのアプライアンスを復号化するためにも、同じキーを使用する必要があります。



3. 1つのサイト（図中のData Center 3）にサイト固有のKMSを追加することにしました。しかし、アプライアンスノードは既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、そのサイトのノードを復号化するための正しいキーがないために発生します。



4. この問題に対処するには、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。（厳密には、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。元のキーは新しいキーの以前のバージョンになります。）サイト固有の KMS には、データセンター 3 の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含まれているため、StorageGRID に保存できます。



サイトで使用する**KMS**を変更する際のユースケース

この表は、サイトの KMS を変更する最も一般的なケースに必要な手順をまとめたものです。

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、そのうちの 1 つをデフォルトの KMS として使用したい場合。	サイト固有の KMS を編集します。「キーを管理する対象」フィールドで、「他の KMS によって管理されていないサイト（デフォルト KMS）」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。これは、専用の KMS を持たないすべてのサイトに適用されます。 "キー管理サーバー（KMS）を編集する"
デフォルトの KMS があり、拡張で新しいサイトを追加します。新しいサイトにはデフォルトの KMS を使用しない場合。	1. 新しいサイトのアプライアンスノードがすでにデフォルトの KMS によって暗号化されている場合は、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. グリッドマネージャーを使用して、新しい KMS を追加し、サイトを選択します。 "キー管理サーバー（KMS）を追加する"
サイトの KMS に別のサーバーを使用する場合。	1. サイトのアプライアンスノードが既存の KMS によって既に暗号化されている場合は、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既存の KMS から新しい KMS にコピーしてください。 2. グリッドマネージャーを使用して、既存の KMS 構成を編集し、新しいホスト名または IP アドレスを入力します。 "キー管理サーバー（KMS）を追加する"

StorageGRID を KMS のクライアントとして設定する

KMS を StorageGRID に追加する前に、各外部キー管理サーバーまたは KMS クラスターのクライアントとして StorageGRID を設定する必要があります。



これらの手順は、Thales CipherTrust Manager および Hashicorp Vault に適用されます。サポートされている製品とバージョンの一覧については、["NetApp Interoperability Matrix Tool \(IMT\)"](#) を使用してください。

手順

1. KMS ソフトウェアから、使用予定の各 KMS または KMS クラスターに対して StorageGRID クライアントを作成します。

各 KMS は、単一のサイトまたは複数のサイトにある 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. 以下の 2 つの方法のいずれかを使用してキーを作成します：
 - 。お使いの KMS 製品のキー管理ページをご利用ください。各 KMS または KMS クラスターに対して AES 暗号化キーを作成してください。

暗号化キーは2,048ビット以上である必要があります、エクスポート可能である必要があります。

- StorageGRID にキーを作成させます。["クライアント証明書をアップロードしています"](#)の後にテストして保存すると、プロンプトが表示されます。

3. 各KMSまたはKMSクラスタについて、以下の情報を記録してください。

KMS を StorageGRID に追加する際には、この情報が必要です。

- 各サーバーのホスト名またはIPアドレス。
- KMSが使用するKMIPポート。
- KMS の暗号化キーのキーエイリアス。

4. 各KMSまたはKMSクラスタごとに、認証局（CA）によって署名されたサーバー証明書、または証明書チェーンの順序で連結されたPEM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取得します。

サーバー証明書により、外部 KMS が StorageGRID に対して自身を認証できるようになります。

- 証明書は、Privacy Enhanced Mail （PEM） Base-64エンコードのX.509形式を使用する必要があります。
- 各サーバー証明書のサブジェクト代替名（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 を設定する際は、*ホスト名*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。

- サーバー証明書は、KMS の KMIP インターフェースで使用される証明書と一致している必要があります。KMIP インターフェースは通常、ポート 5696 を使用します。
5. 外部 KMS によって StorageGRID に発行された公開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により、StorageGRID が KMS に対して自身を認証できます。

StorageGRIDでキー管理サーバーを追加する

StorageGRID キー管理サーバー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。

開始する前に

- ["キー管理サーバーを使用する際の考慮事項と要件"](#)をレビューしました。
- ["StorageGRID をKMS のクライアントとして設定済み"](#)があり、各KMSまたはKMSクラスタに必要な情報が揃っています。
- ["対応ウェブブラウザ"](#)を使用して Grid Manager にサインインしています。
- あなたは["ルートアクセス権限"](#)があります。

タスク概要

可能であれば、他のKMSで管理されていないすべてのサイトに適用されるデフォルトのKMSを設定する前

に、サイト固有のキー管理サーバー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、グリッド内のすべてのノード暗号化アプライアンスは、デフォルトのKMSによって暗号化されます。後でサイト固有のKMSを作成する場合は、まずデフォルトのKMSから新しいKMSに現在のバージョンの暗号化キーをコピーする必要があります。詳細については、"[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

キー管理サーバーの追加ウィザードのステップ 1（KMS の詳細）では、KMS または KMS クラスタに関する詳細情報を入力します。

手順

1. **Configuration > Security > Key management server** を選択します。

キー管理サーバーページが表示され、「構成の詳細」タブが選択された状態になっています。

2. ***Create***を選択します。

キー管理サーバーの追加ウィザードのステップ 1（KMS の詳細）が表示されます。

3. KMS と、そのKMS で設定した StorageGRID クライアントの情報を入力します。

フィールド	説明
KMS name	このKMSを識別するのに役立つ、わかりやすい名前です。1文字から64文字の間で入力してください。
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文字である必要があります。 注：KMS製品を使用してキーを作成していない場合は、StorageGRID にキーを作成するよう求められます。
キーを管理する対象	このKMSに関連付けられるStorageGRIDサイト。可能であれば、他のKMSで管理されていないすべてのサイトに適用されるデフォルトのKMSを設定する前に、サイト固有のキー管理サーバーを設定してください。 • このKMSが特定のサイトのアプライアンスノードの暗号化キーを管理する場合は、サイトを選択してください。 • 「他の KMS で管理されていないサイト（デフォルト KMS）」を選択すると、専用の KMS がないサイト、および後続の拡張で追加するすべてのサイトに適用されるデフォルト KMS が設定されます。 注: デフォルトの KMS で以前に暗号化されたサイトを選択したが、元の暗号化キーの現在のバージョンを新しい KMS に提供しなかった場合、KMS 構成を保存する際に検証エラーが発生します。

フィールド	説明
ポート	KMSサーバーがKey Management Interoperability Protocol (KMIP) 通信に使用するポート番号。デフォルトは5696番ポートで、これはKMIPの標準ポートです。
Hostname	KMSの完全修飾ドメイン名またはIPアドレス。 注: サーバー証明書のサブジェクト代替名 (SAN) フィールドには、ここで入力する FQDN または IP アドレスを含める必要があります。さもないと、StorageGRID は KMS または KMS クラスタ内のすべてのサーバーに接続できなくなります。

4. KMS クラスタを設定する場合は、別のホスト名を追加 を選択して、クラスタ内の各サーバーのホスト名を追加してください。
5. *続行*を選択します。

ステップ2：サーバー証明書をアップロードする

キー管理サーバーの追加ウィザードのステップ 2（サーバー証明書のアップロード）で、KMS 用のサーバー証明書（または証明書バンドル）をアップロードします。サーバー証明書により、外部 KMS が StorageGRID に対して自身を認証できるようになります。

手順

1. 「手順2（サーバー証明書のアップロード）」から、保存済みのサーバー証明書または証明書バンドルの場所を参照してください。
2. 証明書ファイルをアップロードしてください。

サーバー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、各証明書のメタデータはそれぞれ別のタブに表示されます。

3. *続行*を選択します。

ステップ3：クライアント証明書をアップロードする

キー管理サーバー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により、StorageGRID は KMS に対して自身を認証できます。

手順

1. 「手順 3（クライアント証明書のアップロード）」から、クライアント証明書の場所を参照してください。
2. クライアント証明書ファイルをアップロードしてください。

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保存場所を参照してください。

4. 秘密鍵ファイルをアップロードしてください。

5. 「テストして保存」を選択します。

キーが存在しない場合は、StorageGRID にキーを作成するよう求められます。

キー管理サーバーとアプライアンスノード間の接続がテストされます。すべての接続が有効で、KMS上で正しいキーが見つかった場合、新しいキー管理サーバーがキー管理サーバーページのテーブルに追加されます。



KMSを追加するとすぐに、キー管理サーバーのページで証明書の状態が「不明」と表示されます。StorageGRIDが各証明書の実際のステータスを取得するのに、最大30分かかる場合があります。最新の状況を確認するには、ウェブブラウザを更新してください。

6. 「テストして保存」を選択した際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てから「OK」を選択してください。

例えば、接続テストが失敗した場合、422: Unprocessable Entity エラーが表示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*を選択してください。



Force save を選択すると、KMS の設定は保存されますが、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。構成に問題がある場合、影響を受け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再起動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** を選択してください。

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。

StorageGRID でキー管理サーバーを管理する

キー管理サーバー（KMS）の管理には、詳細情報の表示や編集、証明書の管理、暗号化されたノードの表示、不要になったKMSの削除などが含まれます。

開始する前に

- ["対応ウェブブラウザ"](#) を使用して Grid Manager にサインインしています。
- あなたは["必要なアクセス権限"](#)があります。

KMSの詳細を表示

StorageGRID システムの各キー管理サーバー（KMS）に関する情報（重要な詳細情報、サーバーおよびクライアント証明書の現在のステータスを含む）を表示できます。

手順

1. **Configuration > Security > Key management server** を選択します。

キー管理サーバーページが表示され、以下の情報が表示されます：

- 「構成の詳細」 タブには、構成されているキー管理サーバーが一覧表示されます。

。「暗号化されたノード」タブには、ノード暗号化が有効になっているノードが一覧表示されます。

2. 特定のKMSの詳細を表示したり、そのKMSに対して操作を実行したりするには、KMSの名前を選択してください。KMSの詳細ページには、以下の情報が記載されています。

フィールド	説明
キーを管理する対象	KMSに関連付けられた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「他の KMS で管理されていないサイト（デフォルト KMS ）」が表示されます。
Hostname	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ーがクラスタ化されている場合、両方のサーバー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。クラスタ内に2台以上のキー管理サーバーが存在する場合、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ーの数が表示されます。 例えば（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 を選択し、「編集」または「アクション」>「編集」を選択します。

3. KMS詳細ページでタブを選択すると、以下の情報が表示されます：

Tab	フィールド	説明
主な詳細	キー名	KMS 内の StorageGRID クライアントのキーエイリアス。
キーUID	最新バージョンのキーの一意の識別子。	最終更新日
キーの最新バージョンの日時。	サーバ証明書	メタデータ
証明書のメタデータ（シリアル番号、有効期限日時、証明書 PEM など）。	PEM証明書	証明書のPEM（プライバシー強化メール）ファイルの内容。
クライアント証明書	メタデータ	証明書のメタデータ（シリアル番号、有効期限日時、証明書 PEM など）。

4. 組織のセキュリティ慣行で必要とされる頻度で、*キーのローテーション*を選択するか、KMSソフトウェアを使用して、キーの新しいバージョンを作成します。

キーローテーションが成功すると、キー UID と最終更新日時のフィールドが更新されます。

KMS ソフトウェアを使用して暗号化キーをローテーションする場合は、最後に使用したバージョンのキーから同じキーの新しいバージョンにローテーションしてください。まったく異なるキーにはローテーションしないでください。



KMSのキー名（エイリアス）を変更してキーをローテーションしようとししないでください。StorageGRIDでは、以前使用されたすべてのキーバージョン（および将来のバージョン）が、同じキーエイリアスを使用してKMSからアクセスする必要があります。設定済みの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い可能性があります。

証明書の管理

サーバーまたはクライアントの証明書に関する問題は速やかに解決してください。可能であれば、証明書の有効期限が切れる前に交換してください。



データへのアクセスを維持するためには、証明書に関する問題はできるだけ早く解決する必要があります。

手順

1. **Configuration > Security > Key management server** を選択します。
2. 表で、各KMSの証明書の有効期限の値を確認してください。
3. いずれかのKMSの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ブラウザを更新してください。
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、または有効期限が近づいていることが示されている場合は、KMS を選択して KMS の詳細ページに移動してください。
 - a. 「サーバー証明書」を選択し、「有効期限」フィールドの値を確認してください。
 - b. 証明書を交換するには、*証明書の編集*を選択して新しい証明書をアップロードしてください。
 - c. これらのサブ手順を繰り返し、サーバー証明書の代わりに **Client certificate** を選択してください。
5. **KMS CA**証明書の有効期限切れ、**KMS**クライアント証明書の有効期限切れ、および***KMS**サーバー証明書の有効期限切れ*のアラートがトリガーされた場合は、各アラートの説明を確認し、推奨されるアクションを実行してください。

StorageGRID が証明書の有効期限の更新を取得するまでに、最大 30 分かかる場合があります。最新の値を確認するには、ウェブブラウザを更新してください。



サーバー証明書の状態が不明です というステータスが表示された場合は、KMS がクライアント証明書を必要とせずにサーバー証明書を取得できることを確認してください。

暗号化されたノードを表示する

*ノード暗号化*設定が有効になっているStorageGRIDシステムの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. **Configuration > Security > Key management server** を選択します。

キー管理サーバーのページが表示されます。「構成の詳細」タブには、構成済みのキー管理サーバーが表示されます。

2. ページ上部から「暗号化ノード」タブを選択します。

「暗号化ノード」タブには、StorageGRID システム内で*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が一覧表示されます。

3. 各アプライアンスノードに関する表の情報を確認してください。

列	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	ノードの種類：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 name	ノードに使用される KMS のわかりやすい名前。 KMSが表示されていない場合は、「設定の詳細」タブを選択してKMSを追加してください。 "キー管理サーバー（KMS）を追加する"
キーUID	アプライアンスノード上のデータの暗号化および復号化に使用される暗号化キーの固有IDです。キーUID全体を表示するには、テキストを選択してください。 ダッシュ（--）は、キーのUIDが不明であることを示します。これは、アプライアンスノードとKMS間の接続の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状態。ノードが接続されている場合、タイムスタンプは30分ごとに更新されます。KMSの設定変更後、接続状態が更新されるまでに数分かかる場合があります。 注: 新しい値を確認するには、ウェブブラウザを更新してください。

4. 「ステータス」列に KMS の問題が表示されている場合は、直ちにその問題に対処してください。

通常の KMS 運用中は、ステータスは「KMS に接続済み」となります。ノードがグリッドから切断されている場合、ノードの接続状態（管理上ダウンまたは不明）が表示されます。

その他のステータスメッセージは、同じ名前の StorageGRID アラートに対応しています：

- KMS構成の読み込みに失敗しました
- 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キーがアプライアンスボリュームの復号に失敗しました
- KMSが設定されていない

これらのアラートに対して推奨される対応策を実行してください。



データが完全に保護されるよう、問題があれば直ちに対処する必要があります。

KMSの編集

例えば、証明書の有効期限が近づいている場合など、キー管理サーバーの設定を編集する必要がある場合があります。

開始する前に

- KMS 用を選択したサイトを更新する予定がある場合は、"[サイトのKMSを変更する際の考慮事項](#)"を確認済みです。
- "[対応ウェブブラウザ](#)"を使用して Grid Manager にサインインしています。
- あなたは"[ルートアクセス権限](#)"があります。

手順

1. **Configuration > Security > Key management server** を選択します。

キー管理サーバーページが表示され、設定済みのすべてのキー管理サーバーが表示されます。

2. 編集するKMSを選択し、「アクション」>「編集」を選択します。

KMS を編集するには、表で KMS 名を選択し、KMS 詳細ページで **編集** を選択します。

3. 必要に応じて、「キー管理サーバーの編集」ウィザードの「手順 1（KMS の詳細）」で詳細を更新してください。

フィールド	説明
KMS name	このKMSを識別するのに役立つ、わかりやすい名前です。1文字から64文字の間で入力してください。
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文字である必要があります。 キー名を編集する必要があるのは、ごくまれなケースのみです。例えば、KMSでエイリアスの名前が変更された場合、または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た場合は、キー名を編集する必要があります。

フィールド	説明
キーを管理する対象	サイト固有の KMS を編集していて、デフォルトの KMS がまだ設定されていない場合は、必要に応じて「他の KMS で管理されていないサイト（デフォルトの KMS）」を選択してください。この選択により、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、および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は、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は、特定のサイトを選択することはできません。
ポート	KMSサーバーがKey Management Interoperability Protocol (KMIP) 通信に使用するポート番号。デフォルトは5696番ポートで、これはKMIPの標準ポートです。
Hostname	KMSの完全修飾ドメイン名またはIPアドレス。 注: サーバー証明書のサブジェクト代替名 (SAN) フィールドには、ここで入力する FQDN または IP アドレスを含める必要があります。さもないと、StorageGRID は KMS または KMS クラスタ内のすべてのサーバーに接続できなくなります。

4. KMS クラスタを設定する場合は、別のホスト名を追加 を選択して、クラスタ内の各サーバーのホスト名を追加してください。

5. *続行*を選択します。

キー管理サーバーの編集ウィザードのステップ 2（サーバー証明書のアップロード）が表示されます。

6. サーバー証明書を交換する必要がある場合は、**Browse** を選択して新しいファイルをアップロードしてください。

7. *続行*を選択します。

キー管理サーバーの編集ウィザードのステップ 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交換する必要がある場合は、**Browse** を選択して新しいファイルをアップロードしてください。

9. 「テストして保存」を選択します。

影響を受けるサイトにある、鍵管理サーバーとすべてのノード暗号化アプライアンスノード間の接続がテストされます。すべてのノード接続が有効で、KMS上で正しい暗号化キーが見つかった場合、キー管理サーバーが「キー管理サーバー」ページのテーブルに追加されます。

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** を選択してください。

例えば、この KMS 用に選択したサイトが既に別の KMS によって管理されている場合、または接続テストが失敗した場合、422: Unprocessable Entity エラーが表示されることがあります。

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、**Force save** を選択してください。



Force save を選択すると、KMS の設定は保存されますが、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。構成に問題がある場合、影響を受け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再起動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した。

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** を選択してください。

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。

キー管理サーバー (**KMS**) を削除する

場合によっては、キー管理サーバーを削除することが必要になる場合があります。たとえば、サイトを廃止した場合に、サイト固有の KMS を削除することができます。

開始する前に

- "キー管理サーバーを使用する際の考慮事項と要件"をレビューしました。
- "対応ウェブブラウザ" を使用して Grid Manager にサインインしています。
- あなたは"ルートアクセス権限"があります。

タスク概要

次のような場合は、KMSを削除できます。

- サイトが廃止された場合、またはサイト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が含まれていない場合は、サイト固有のKMSを削除できます。
- アプライアンスノードのノード暗号化が有効になっている各サイトに、サイト固有のKMSが既に存在する場合は、デフォルトのKMSを削除できます。

手順

1. **Configuration > Security > Key management server** を選択します。

キー管理サーバーページが表示され、設定済みのすべてのキー管理サーバーが表示されます。

2. 削除するKMSを選択し、「アクション」>「削除」を選択します。

また、表から KMS 名を選択し、KMS 詳細ページで 削除 を選択することで、KMS を削除することもできます。

3. 以下の内容が正しいことを確認してください：

- 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が存在しないサイトの、サイト固有のKMSを削除しようとしています。
- デフォルトのKMSを削除しようとしています。ノード暗号化が有効なサイト固有のKMSが各サイトに既に存在します。

4. 「はい」を選択します。

KMSの設定が削除されました。

プロキシ設定を管理する

StorageGRID ストレージ プロキシを設定する

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S3エンドポイントの間に非透過型プロキシ サーバを設定できます。例えば、プラットフォームサービスのメッセージをインターネット上のエンドポイントなどの外部エンドポイントに送信できるようにするには、非透過型プロキシ サーバが必要になる場合があります。



構成済みのストレージ プロキシ サーバ設定は、Kafka プラットフォームサービスのエンドポイントには適用されません。

開始する前に

- "特定のアクセス権限"があります。
- "対応ウェブブラウザ" を使用して Grid Manager にサインインしています。

タスク概要

単一のストレージ プロキシ サーバの設定を構成できます。

手順

1. **Configuration > Security > Proxy settings** を選択します。
2. **[Storage]** タブで、**[Enable storage proxy]** チェックボックスを選択します。
3. ストレージ プロキシ サーバのプロトコルを選択してください。
4. プロキシ サーバのホスト名またはIPアドレスを入力してください。
5. オプションで、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。

このフィールドを空白のままにすると、プロトコルのデフォルトポートが使用されます（HTTP の場合は 80、SOCKS5 の場合は 1080）。

6. * 保存 * を選択します。

ストレージ プロキシ サーバを保存した後、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用の新しいエンドポイントを設定およびテストできます。



プロキシの変更が反映されるまで最大10分かかる場合があります。

7. プロキシ サーバの設定を確認し、StorageGRID からの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ないようにしてください。
8. ストレージプロキシを無効にする必要がある場合は、チェックボックスをオフにして*保存*を選択してください。

StorageGRIDで管理プロキシ設定を構成する

HTTPまたはHTTPSを使用してAutoSupportパッケージを送信する場合は、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。

AutoSupport の詳細については、"[AutoSupportを設定する](#)" を参照してください。

開始する前に

- "[特定のアクセス権限](#)"があります。
- "[対応ウェブブラウザ](#)" を使用して Grid Manager にサインインしています。

タスク概要

単一の管理プロキシ サーバの設定を構成できます。

手順

1. **Configuration > Security > Proxy settings** を選択します。

プロキシ設定ページが表示されます。デフォルトでは、タブメニューで「ストレージ」が選択されています。

2. 「Admin」 タブを選択します。
3. 「管理者プロキシを有効にする」 チェックボックスを選択します。
4. プロキシ サーバのホスト名またはIPアドレスを入力してください。
5. プロキシ サーバへの接続に使用するポートを入力してください。
6. 必要に応じて、プロキシ サーバのユーザー名とパスワードを入力してください。

プロキシ サーバにユーザー名やパスワードが不要な場合は、これらのフィールドを空白のままにしてください。

7. 次のいずれかを選択します。

- 管理プロキシへの接続を保護するには、「プロキシ証明書の検証」を選択します。CAバンドルをアップロードして、管理プロキシ サーバが提示するSSL証明書の真正性を検証します。



AutoSupport on Demand、EシリーズのStorageGRID経由のAutoSupport、およびStorageGRIDアップグレードページでの更新パスの決定は、プロキシ証明書が検証されている場合は機能しません。

CAバンドルをアップロードすると、そのメタデータが表示されます。

- 管理プロキシ サーバとの通信時に証明書を検証しない場合は、*「プロキシ証明書を検証しない」*を選択してください。

8. * 保存 * 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間のプロキシ サーバが設定されます。



プロキシの変更が反映されるまで最大10分かかる場合があります。

9. 管理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てから、*保存*を選択します。

ファイアウォールを制御する

外部ファイアウォールで**StorageGRID**アクセスを制御する

外部ファイアウォールで特定のポートを開閉できます。

外部ファイアウォールで特定のポートを開閉することにより、StorageGRID 管理ノードのユーザーインターフェースと API へのアクセスを制御できます。たとえば、システムアクセスを制御するための他の方法に加えて、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したい場合もあるでしょう。

StorageGRID の内部ファイアウォールを設定する場合は、"[内部ファイアウォールの設定](#)"を参照してください。

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	ウェブブラウザおよび管理APIクライアントは、グリッドマネージャ、グリッド管理API、テナントマネージャ、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Grid Managerポートの制限	- ウェブブラウザおよび管理APIクライアントは、HTTPSを使用してグリッドマネージャおよびグリッド管理APIにアクセスできます。 - ウェブブラウザおよび管理APIクライアントは、テナントマネージャまたはテナント管理APIにアクセスできません。 - 内部コンテンツに関するリクエストは拒否されます。
9443	管理ノード上のテナントマネージャ ポートの制限	- ウェブブラウザおよび管理APIクライアントは、HTTPSを使用してテナントマネージャおよびテナント管理APIにアクセスできます。 - ウェブブラウザおよび管理APIクライアントは、グリッドマネージャまたはグリッド管理APIにアクセスできません。 - 内部コンテンツに関するリクエストは拒否されます。



制限付きGrid ManagerまたはTenant Managerポートでは、シングル サインオン（SSO）は利用できません。ユーザーがシングル サインオンで認証を行う場合は、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

- ["グリッドマネージャにサインインする"](#)
- ["テナントアカウントを作成する"](#)

- ["外部通信"](#)

StorageGRIDで内部ファイアウォール制御を管理する

StorageGRID は各ノードに内部ファイアウォールを備えており、ノードへのネットワーク アクセスを制御することでグリッドのセキュリティを強化します。ファイアウォールを使用して、特定のグリッド展開に必要なポートを除くすべてのポートへのネットワーク アクセスを防止します。ファイアウォール制御ページで行った設定変更は、各ノードに展開されます。

ファイアウォール制御ページの3つのタブを使用して、グリッドに必要なアクセス権限をカスタマイズします。

- 特権アドレス一覧：このタブを使用して、閉じられたポートへの特定のアクセスを許可します。「外部アクセス管理」タブを使用して閉じられたポートにアクセスできるIPアドレスまたはCIDR表記のサブネットを追加できます。
- 外部アクセス管理：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たり、以前に閉じたポートを再度開いたりできます。
- 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受信トラフィックを信頼するかどうかを指定します。

このタブの設定は、「外部アクセス管理」タブの設定よりも優先されます。

- 信頼できないクライアントネットワークを持つノードは、そのノードに設定されているロードバランサーエンドポイントポート（グローバル、ノードインターフェース、およびノードタイプにバインドされたエンドポイント）での接続のみを受け入れます。
- ロードバランサーのエンドポイントポートは、外部ネットワークの管理タブの設定に関係なく、信頼されていないクライアントネットワーク上で_唯一開いているポート_です。
- 信頼済みと設定されている場合、「外部アクセス管理」タブで開いているすべてのポート、およびクライアントネットワーク上で開いているロードバランサーの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権限の変更に影響を与える可能性があります。ネットワークが期待どおりに動作することを確認するため、すべてのタブの設定を必ず確認してください。

内部ファイアウォール制御を設定するには、["ファイアウォール制御を設定する"](#)を参照してください。

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、["外部ファイアウォールでアクセスを制御する"](#)を参照してください。

特権アドレス一覧と外部アクセス管理タブ

「特権アドレスリスト」タブでは、閉じられたグリッドポートへのアクセスを許可する1つまたは複数のIPアドレスを登録できます。「外部アクセス管理」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への外部アクセスを閉じることができます（外部ポートとは、デフォルトでグリッド以外のノードからアクセスできるポートのことです）。これらの2つのタブは、多くの場合、組み合わせて使用することで、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アドレスは、デフォルトでは内部グリッドポートへのアクセス権を持ちません。

例1：メンテナンス作業にジャンプホストを使用する

ネットワーク管理のためにジャンプホスト（セキュリティ強化されたホスト）を使用したいとします。以下の一般的な手順をご利用ください。

1. 特権アドレス一覧タブを使用して、ジャンプホストのIPアドレスを追加します。
2. 「外部アクセス管理」タブを使用して、すべてのポートをブロックしてください。



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。現在ブロックされたポートに接続しているユーザー（ご自身を含む）は、IPアドレスが特権アドレスリストに追加されていない限り、Grid Managerへのアクセス権を失います。

設定を保存すると、グリッド内の管理ノード上のすべての外部ポートは、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。その後、ジャンプホストを使用して、グリッド上でより安全にメンテナンス作業を実行できます。

例2：機密性の高いポートをロックダウンする

機密性の高いポートとそのポート上のサービスをロックダウンしたいとします。以下の一般的な手順を使用できます。

1. 特権アドレス一覧タブを使用して、サービスへのアクセスが必要なホストのみにアクセス権を付与してください。
2. 「外部アクセス管理」タブを使用して、すべてのポートをブロックしてください。



Grid ManagerおよびTenant Managerへのアクセスに割り当てられたポート（プリセットポートは443と8443）へのアクセス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。現在ブロックされているポートに接続しているユーザー（お客様自身を含む）は、IPアドレスが特権アドレスリストに追加されていない限り、Grid Managerへのアクセス権を失います。

設定を保存すると、機密性の高いポートとそのポート上のサービスが、特権アドレスリストに登録されているホストから利用可能になります。リクエストの発信元インターフェースに関わらず、その他のホストはすべてサービスへのアクセスを拒否されます。

例3：未使用サービスへのアクセスを無効にする

ネットワークレベルでは、使用しない予定のサービスを無効にすることができます。例えば、HTTP S3クライアントトラフィックをブロックするには、「外部アクセスの管理」タブのトグルを使用してポート18084をブロックします。

信頼でき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でのみ受信クライアントトラフィックを受け入れることで、悪意のある攻撃から StorageGRID を保護し、セキュリティを強化することができます。

デフォルトでは、各グリッドノード上のクライアントネットワークは_信頼済み_です。つまり、デフォルトでは、StorageGRID はすべての**利用可能な外部ポート**で各グリッドノードへの受信接続を信頼します。

各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_と指定することで、StorageGRID システムへの悪意の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

はロードバランサーエンドポイントとして明示的に設定されたポートへの受信接続のみを受け入れます。"[ロードバランサーのエンドポイントを設定する](#)"および"[ファイアウォール制御を設定する](#)"を参照してください。

例1：ゲートウェイノードはHTTPS S3リクエストのみを受け入れます

ゲートウェイノードが、HTTPS S3リクエストを除くクライアントネットワーク上のすべての受信トラフィックを拒否するようにしたいとします。一般的には、以下の手順を実行します。

1. "[ロード バランサ エンドポイント](#)"ページで、ポート443でHTTPS経由のS3用ロードバランサーエンドポイントを設定します。
2. ファイアウォール制御ページから「Untrusted」を選択して、ゲートウェイ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、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受信トラフィックは、ポート 443 の HTTPS S3 リクエストと ICMP エコー (ping) リクエストを除いて破棄されます。

例2：ストレージノードがS3プラットフォームサービスリクエストを送信する

ストレージノードからS3プラットフォームサービスの送信トラフィックを有効にしたいが、クライアントネットワーク上のそのストレージノードへの受信接続はすべて阻止したいとします。一般的な手順は以下のとおりです。

- ・ファイアウォール制御ページの「信頼されていないクライアントネットワーク」タブから、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上の受信トラフィックを受け付けなくなりますが、設定済みのプラットフォームサービス宛先への送信リクエスト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

グリッドマネージャへのアクセスを特定のサブネットのみに制限したいとします。以下の手順を実行してください。

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. 「信頼されていないクライアントネットワーク」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. 管理インターフェイスのロードバランサーエンドポイントを作成する際は、ポートを入力し、そのポートがアクセスする管理インターフェイスを選択してください。
4. 「信頼できないクライアントネットワーク」に対して「はい」を選択します。
5. 「外部アクセス管理」タブを使用して、すべての外部ポートをブロックします（そのサブネット外のホストに特権IPアドレスが設定されているかどうかにかかわらず）。

設定を保存すると、指定したサブネット上のホストのみがグリッドマネージャにアクセスできるようになります。その他のホストはすべてブロックされます。

StorageGRID 内部ファイアウォールを設定する

StorageGRID ファイアウォールを設定して、StorageGRID ノードの特定のポートへのネットワーク アクセスを制御できます。

開始する前に

- ["対応ウェブブラウザ"](#) を使用して Grid Manager にサインインしています。
- ["特定のアクセス権限"](#)があります。
- ["ファイアウォール制御を管理する"](#)および["ネットワーク構築ガイドライン"](#)の情報を確認済みです。
- 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受信トラフィックを受け入れるようにするには、ロードバランサーのエンドポイントを定義します。



クライアントネットワークの設定を変更する際、ロードバランサーのエンドポイントが設定されていない場合、既存のクライアント接続が失敗する可能性があります。

タスク概要

StorageGRID の各ノードには内部ファイアウォールが搭載されており、グリッド内のノード上のポートの一部を開閉することができます。ファイアウォール制御タブを使用すると、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閉できます。また、閉じられた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、ノードがクライアントネットワークからの受信トラフィックを信頼するかどうかを指定したり、クライアントネットワーク上の特定のポートへのアクセスを設定したりできます。

グリッド外のIPアドレスに対して開放するポート数を、必要最低限のものだけに制限することで、グリッドのセキュリティを強化できます。ファイアウォール制御の3つのタブそれぞれの設定を使用して、必要なポートのみが開いていることを確認します。

ファイアウォール制御の使用方法に関する詳細情報（例を含む）については、["ファイアウォール制御を管理する"](#)を参照してください。

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、["外部ファイアウォールでアクセスを制御する"](#)を参照してください。

アクセスファイアウォール制御

手順

1. **Configuration > Security > Firewall control** を選択します。

このページにある 3 つのタブについては、["ファイアウォール制御を管理する"](#)で説明します。

2. ファイアウォールの設定を行うには、いずれかのタブを選択してください。

これらのタブはどの順番で使用しても構いません。1つのタブで設定した内容は、他のタブでの操作を制限するものではありません。ただし、1つのタブで行った設定変更は、他のタブで設定されているポートの動作に影響を与える可能性があります。

特権アドレス一覧

「特権アドレス一覧」タブを使用すると、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権をホストに付与できます。

特権IPアドレスとサブネットは、デフォルトでは内部グリッドへのアクセス権を持ちません。また、ロードバランサーのエンドポイントや、「特権アドレス一覧」タブで開かれた追加ポートは、「外部アクセス管理」タブでブロックされていてもアクセス可能です。



「特権アドレス一覧」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. 「特権アドレス一覧」タブで、閉じられ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、*別のIPアドレスまたはサブネットをCIDR表記で追加する*を選択して、追加の特権クライアントを追加します。



特権リストには、できるだけ少ないアドレスを追加するようにしてください。

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。["StorageGRID内部ポート"](#)を参照してください。



このオプションを選択すると、内部サービスに対する一部の保護機能が解除されます。可能であれば無効にしておいてください。

4. *保存*を選択します。

外部アクセスを管理する

「外部アクセス管理」タブでポートを閉じると、そのIPアドレスを特権アドレスリストに追加しない限り、グリッド以外のIPアドレスからそのポートにアクセスできなくなります。デフォルトで開いているポートのみ閉じることができ、閉じたポートのみ開くことができます。



「外部アクセス管理」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。例えば、ノードが信頼されていない場合、「外部アクセス管理」タブでSSH/22ポートが開いている設定になっていても、クライアントネットワーク上ではSSH/22ポートはブロックされます。「信頼されていないクライアントネットワーク」タブの設定は、クライアントネットワーク上の閉じられたポート（443、8443、9443など）を上書きします。

手順

1. *外部アクセスを管理*を選択します。このタブには、グリッド内のノードの外部ポート（デフォルトでグリッド以外のノードからアクセス可能なポート）をすべて一覧にした表が表示されます。
2. 以下のオプションを使用して、開放または閉鎖するポートを設定します：
 - 各ポートの横にあるトグルスイッチを使用して、選択したポートを開閉します。
 - 表示されているすべてのポートを開く を選択すると、表に表示されているすべてのポートが開きます。
 - 表示されているすべてのポートを閉じる を選択すると、表に表示されているすべてのポートが閉じられます。



Grid Manager のポート 443 または 8443 を閉じると、ご自身を含め、現在ブロックされたポートに接続しているすべてのユーザーは、IP アドレスが特権アドレスリストに追加されていない限り、Grid Manager へのアクセス権を失います。



表の右側にあるスクロールバーを使用して、利用可能なすべてのポートを確認してください。検索フィールドにポート番号を入力することで、任意の外部ポートの設定を検索できます。ポート番号の一部を入力することもできます。たとえば、「2」と入力すると、名前に「2」という文字列が含まれるすべてのポートが表示されます。

3. *保存*を選択します

信頼できないクライアントネットワーク

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ーのエンドポイントとして構成されたポート、およびオプションでこのタブで選択した追加ポートでのみ受信トラフィックを受け入れます。このタブを使用して、拡張で追加され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。



ロードバランサーのエンドポイントが設定されていない場合、既存のクライアント接続が失敗する可能性があります。

「信頼されていないクライアントネットワーク」タブで行った設定変更は、「外部アクセスの管理」タブの設定を上書きします。

手順

1. 「信頼できないクライアントネットワーク」を選択します。
2. 「新規ノードのデフォルト設定」セクションで、拡張手順でグリッドに新しいノードが追加されたときのデフォルト設定を指定します。

- 信頼済み（デフォルト）：拡張でノードが追加されると、そのクライアントネットワークは信頼済みになります。
- 信頼されていない：拡張機能でノードが追加されると、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規ノードの設定を変更できます。



この設定は、StorageGRID システムの既存のノードには影響しません。

3. 以下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ーエンドポイントまたは追加の選択された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てください。

- 「表示されているノードの信頼を解除する」を選択すると、テーブルに表示されているすべてのノードが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されます。
- 「表示されているノードを信頼する」を選択すると、表に表示されているすべてのノードが「信頼されていないクライアントネットワーク」リストから削除されます。
- 各ノードの横にあるトグルスイッチを使用して、選択したノードのクライアントネットワークを「信頼済み」または「信頼されていない」に設定します。

例えば、*表示されているノードを信頼しない*を選択すると、すべてのノードが「信頼されていないクライアントネットワーク」リストに追加され、その後、個々のノードの横にあるトグルを使用して、そのノードを「信頼できるクライアントネットワーク」リストに追加することができます。



表の右側にあるスクロールバーを使用して、利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てください。検索フィールドにノード名を入力することで、任意のノードの設定を検索できます。名前の一部を入力することもできます。例えば、**GW** と入力すると、名前に「GW」という文字列が含まれるすべてのノードが表示されます。

4. * 保存 * を選択します。

新しいファイアウォール設定は即座に適用され、有効になります。ロードバランサーのエンドポイントが設定されていない場合、既存のクライアント接続が失敗する可能性があります。

テナントの管理

StorageGRID のテナントアカウント

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



このバージョンのドキュメントサイトからは、Swiftに関する詳細情報が削除されました。参照してください ["StorageGRID 11.8：テナントの管理"](#)。

グリッド管理者として、S3クライアントがオブジェクトの保存と取得に使用するテナントアカウントを作成および管理します。

各テナントアカウントには、フェデレーショングループまたはローカルグループ、ユーザー、S3 バケット、およびオブジェクトが含まれます。

テナントアカウントを使用すると、保管されているオブジェクトを異なるエンティティごとに分類できます。例えば、複数のテナントアカウントは、以下のいずれかのユースケースに使用できます。

- エンタープライズユースケース：エンタープライズアプリケーションで StorageGRID システムを管理している場合、組織内のさまざまな部門ごとにグリッドのオブジェクトストレージを分離することができます。この場合、マーケティング部門、カスタマーサポート部門、人事部門などのテナントアカウントを作成できます。



S3クライアントプロトコルを使用する場合、S3バケットとバケットポリシーを使用して、企業内の部門間でオブジェクトを分離することができます。テナントアカウントを使用する必要はありません。詳細については、["S3バケットとバケットポリシー"](#)の実装手順を参照してください。

- サービスプロバイダーの使用例：StorageGRID システムをサービスプロバイダーとして管理している場合、グリッド上のストレージをリースするさまざまなエンティティごとに、グリッドのオブジェクトストレージを分離することができます。この場合、Company A、Company B、Company C などのテナントアカウントを作成します。

詳細については、["テナントアカウントを使用する"](#)を参照してください。

テナントアカウントはどのように作成すればよいですか？

Gridマネージャーを使用してテナントアカウントを作成します。テナントアカウントを作成する際には、以下

の情報を指定します。

- テナント名、クライアントタイプ (S3)、オプションのストレージクォータなどの基本情報。
- テナントアカウントの権限。例えば、テナントアカウントが S3 プラットフォームサービスを利用できるかどうか、独自の ID ソースを設定できるかどうか、S3 Select を使用できるかどうか、またはグリッドフェデレーション接続を使用できるかどうかなど。
- テナントの初期ルートアクセスは、StorageGRID システムがローカルグループとユーザー、IDフェデレーション、またはシングル サインオン (SSO) を使用するかどうかによって異なります。

さらに、S3 テナントアカウントが規制要件を遵守する必要がある場合は、StorageGRID システムの S3 オブジェクトロック設定を有効にすることができます。S3 オブジェクトロックが有効になっている場合、すべての S3 テナントアカウントは準拠したバケットを作成および管理できます。

テナントマネージャーは何のために使用されますか？

テナントアカウントを作成すると、テナントユーザーはテナントマネージャーにサインインして、次のようなタスクを実行できます。

- IDフェデレーションを設定します (IDソースがグリッドと共有されている場合を除く)
- グループとユーザーを管理する
- アカウントクローンとクロスグリッドレプリケーションにはグリッドフェデレーションを使用する
- S3アクセスキーの管理
- S3バケットの作成と管理
- S3プラットフォームサービスを使用する
- S3 Selectを使用する
- ストレージ使用量を監視する



S3テナントのユーザーは、テナントマネージャーを使用してS3アクセスキーとバケットを作成および管理できますが、オブジェクトの取り込みと管理にはS3クライアントアプリケーションを使用する必要があります。詳細については、"[S3 REST APIを使用する](#)"を参照してください。

StorageGRID テナント アカウントを作成します

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

テナントアカウントを作成する手順は、"[アイデンティティフェデレーション](#)"および"[シングル サインオン](#)"が設定されているかどうか、また、テナントアカウントを作成するために使用する Grid Manager アカウントがルートアクセス権限を持つ管理者グループに属しているかどうかによって異なります。

開始する前に

- "[対応ウェブブラウザ](#)"を使用して Grid Manager にサインインしています。
- あなたは"[ルートアクセス権限またはテナントアカウントの権限](#)"があります。
- テナントアカウントがGrid Manager用に構成されたIDソースを使用し、かつテナントアカウントのルートアクセス権限をフェデレーショングループに付与する場合は、そのフェデレーショングループをGrid

Managerにインポートする必要があります。この管理者グループには、Grid Managerの権限を割り当てる必要はありません。["管理者グループの管理"](#)を参照してください。

- S3テナントがアカウントデータをクローンし、グリッドフェデレーション接続を使用して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：

- ["グリッドフェデレーション接続を構成しました"](#)があります。
- 接続状態は「接続済み」です。
- ルートアクセス権限があります。
- ["グリッド連携のための許可されたテナントの管理"](#)に関する考慮事項を確認しました。
- テナントアカウントがGrid Manager用に構成されたIDソースを使用する場合、両方のグリッドで同じフェデレーショングループをGrid Managerにインポートしてあります。

テナントを作成する際に、このグループを選択して、送信元テナントアカウントと宛先テナントアカウントの両方に対して、初期ルートアクセス権限を付与します。



テナントを作成する前にこの管理グループが両方のグリッドに存在しない場合、テナントは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する

手順

1. 「テナント」を選択します。
2. *Create*を選択します。

詳細を入力

手順

1. テナントの詳細を入力してください。

フィールド	説明
Name	テナントアカウントの名前。テナント名は一意である必要はありません。テナントアカウントが作成されると、固有の20桁のアカウントIDが付与されます。
概要（任意）	テナントを識別するための概要。 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、必要に応じてこのフィールドを使用して、送信元テナントと宛先テナントを識別することができます。例えば、Grid 1 で作成されたテナントの説明は、Grid 2 に複製されたテナントにも表示されます：「このテナントは Grid 1 で作成されました。」
クライアントタイプ	*S3*である必要があります。

フィールド	説明
ストレージ容量（オプション）	このテナントにストレージクォータを設定する場合は、クォータの数値と単位を指定してください。

2. *続行*を選択します。

権限を選択

手順

1. 必要に応じて、このテナントに付与する基本的な権限を選択してください。



これらの権限の中には、追加の要件があるものもあります。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。

アクセス許可	選択された場合...
プラットフォームサービスを許可する	テナントは、CloudMirror などの S3 プラットフォームサービスを使用できます。" S3テナントアカウントのプラットフォームサービスを管理する "を参照してください。
独自のIDソースを使用する	テナントは、フェデレーショングループおよびユーザー向けに独自のIDソースを設定および管理できます。このオプションは、StorageGRID システムに対して" 設定済みSSO "している場合は無効になります。
S3 Selectを許可する	テナントは、S3 SelectObjectContent API リクエストを発行して、オブジェクトデータをフィルタリングおよび取得できます。参照してください "テナントアカウントのS3 Selectの管理"。 重要：SelectObjectContentリクエストは、すべてのS3クライアントとすべてのテナントのロードバランサーのパフォーマンスを低下させる可能性があります。この機能は、必要な場合にのみ、信頼できるテナントに対してのみ有効にしてください。

2. 必要に応じて、このテナントに付与する高度な権限を選択してください。

アクセス許可	選択された場合...
グリッドフェデレーション接続	テナントは、以下の機能を持つグリッドフェデレーション接続を使用できます。 • このテナントと、アカウントに追加されたすべてのテナントグループおよびユーザーが、このグリッド (<i>source grid</i>) から、選択した接続内の別のグリッド (<i>destination grid</i>) に複製されます。 • このテナントは、各グリッド上の対応するバケット間でクロスグリッドレプリケーションを設定できます。 "グリッドフェデレーションの許可されたテナントを管理する"を参照してください。
S3 Object Lock	テナントがS3オブジェクトロックの特定の機能を使用できるようにする： • *最大保持期間の設定*は、このバケットに追加された新しいオブジェクトが、取り込まれた時点からどのくらいの期間保持されるかを定義します。 • *コンプライアンスモードを許可する*は、保持期間中にユーザーが保護されたオブジェクトのバージョンを上書きまたは削除することを防止します。

3. *続行*を選択します。

ルートアクセスを定義し、テナントを作成する

手順

1. テナントアカウントのルートアクセスを定義します。定義方法は、StorageGRIDシステムがIDフェデレーション、シングルサインオン（SSO）、またはその両方を使用しているかどうかによって異なります。

オプション	これを実行します
IDフェデレーションが有効になっていない場合	ローカルのrootユーザー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てください。
IDフェデレーションが有効になっている場合	a. テナントに対してルートアクセス権限を付与する既存のフェデレーショングループを選択してください。 b. 必要に応じて、ローカルのルートユーザー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	テナントに対してルートアクセス権限を付与する既存のフェデレーショングループを選択してください。ローカルユーザーはログインできません。

2. 「テナントの作成」を選択します。

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

照してください。



テナント設定をグリッド全体に適用するには、ネットワーク接続状況、ノードの状態、およびCassandraの動作状況に応じて、15分以上かかる場合があります。

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

- a. 接続先の他のグリッドにも同一のテナントが複製されていることを確認してください。両方のグリッド上のテナントは、同じ20桁のアカウントID、名前、概要、割り当て量、および権限を持ちます。



「クローンなしでテナントが作成されました」というエラーメッセージが表示された場合は、"[グリッドフェデレーションのエラーをトラブルシューティングする](#)"の手順を参照してください。

- b. ルートアクセスを定義する際にローカルルートユーザーのパスワードを指定した場合、"[ローカルルートユーザーのパスワードを変更する](#)"複製されたテナントに対して適用されます。



ローカルのルートユーザーは、パスワードが変更されるまで、宛先グリッド上のテナントマネージャーにサインインできません。

テナントとしてサインインする（任意）

必要に応じて、今すぐ新しいテナントにサインインして設定を完了することも、後でサインインすることもできます。サインインの手順は、デフォルトポート（443）を使用してGrid Managerにサインインしているか、制限付きポートを使用してサインインしているかによって異なります。"[外部ファイアウォールでアクセスを制御する](#)"を参照してください。

今すぐログイン

対象	操作
ポート443を使用し、ローカルのrootユーザーにパスワードを設定します	「rootとしてサインイン」を選択します。 ログインすると、バケット、ID連携、グループ、ユーザーを設定するためのリンクが表示されます。 - テナントアカウントを設定するには、リンクを選択してください。 各リンクをクリックすると、テナントマネージャー内の対応するページが開きます。ページを完成させるには、"テナントアカウントの使用方法に関する説明"を参照してください。
ポート443を使用していますが、ローカルのrootユーザーにパスワードを設定していません	「サインイン」を選択し、ルートアクセスフェデレーショングループに属するユーザーの認証情報を入力します。

対象	操作
制限されたポート	1. 「完了」を選択します。 2. テナント表で「制限付き」を選択すると、このテナントアカウントへのアクセス方法の詳細を確認できます。 テナントマネージャーの URL の形式は次のとおりです： <pre>https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/</pre> ◦ `FQDN_or_Admin_Node_IP` は、完全修飾ドメイン名または管理ノードのIPアドレスです。 ◦ `port` はテナント専用ポートです ◦ `20-digit-account-id` はテナント固有のアカウントIDです

後でログインする

対象	以下のいずれかを実行してください...
ポート443	• グリッドマネージャーから*テナント*を選択し、テナント名の右側にある*サインイン*を選択します。 • テナントのURLをウェブブラウザに入力します： <pre>https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/</pre> ◦ `FQDN_or_Admin_Node_IP` は、完全修飾ドメイン名または管理ノードのIPアドレスです。 ◦ `20-digit-account-id` はテナント固有のアカウント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。 • テナントのURLをウェブブラウザに入力します： <pre>https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id</pre> ◦ `FQDN_or_Admin_Node_IP` は、完全修飾ドメイン名または管理ノードの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` はテナント固有のアカウントIDです

テナントの設定

"テナントアカウントを使用する"の手順に従って、テナントグループとユーザー、S3アクセスキー、バケット、プラットフォームサービス、アカウントクローン、およびクロスグリッドレプリケーションを管理しま

す。

StorageGRID テナント アカウントを編集する

テナントアカウントを編集することで、表示名、ストレージ容量、またはテナントの権限を変更できます。



テナントに「グリッドフェデレーション接続を使用する」権限が付与されている場合、接続先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、接続されたグリッドのうち一方のグリッドで行った変更は、もう一方のグリッドにはコピーされません。テナントの詳細情報とグリッド間の情報を完全に同期させたい場合は、両方のグリッドで同じ編集を行ってください。["グリッドフェデレーション接続の許可テナントを管理する"](#)を参照してください。

開始する前に

- ["対応ウェブブラウザ"](#) を使用して Grid Manager にサインインしています。
- あなたは["ルートアクセス権限またはテナントアカウントの権限"](#)があります。



テナント設定をグリッド全体に適用するには、ネットワーク接続状況、ノードの状態、およびCassandraの動作状況に応じて、15分以上かかる場合があります。

手順

1. 「テナント」を選択します。

Tenants

View information for each tenant account. Depending on the timing of ingests, network connectivity, and node status, the usage data shown might be out of date. To view more recent values, select the tenant name.

[Create](#) [Export to CSV](#) [Actions](#)

Displaying 5 results

☐	Name	Logical space used	Quota utilization	Quota	Object count	Sign in/Copy URL
☐	Tenant 01	2.00 GB	10%	20.00 GB	100	→ 📄
☐	Tenant 02	85.00 GB	85%	100.00 GB	500	→ 📄
☐	Tenant 03	500.00 TB	50%	1.00 PB	10,000	→ 📄
☐	Tenant 04	475.00 TB	95%	500.00 TB	50,000	→ 📄
☐	Tenant 05	5.00 GB	—	—	500	→ 📄

2. 編集するテナントアカウントを見つけます。

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

3. テナントを選択してください。以下のいずれかの方法を実行できます。
 - テナントのチェックボックスを選択し、**Actions** > **Edit** を選択します。

- 詳細ページを表示するには、テナント名を選択し、*編集*を選択してください。

4. 必要に応じて、以下のフィールドの値を変更してください。

- 名前
- 概要
- ストレージクォータ

5. *続行*を選択します。

6. テナントアカウントのアクセス許可を選択または解除します。

- 既にプラットフォームサービスを利用しているテナントに対してプラットフォームサービスを無効にすると、そのテナントがS3バケット用に設定したサービスは動作しなくなります。テナントにはエラーメッセージは送信されません。例えば、テナントがS3バケットにCloudMirrorレプリケーションを設定している場合、バケット内にオブジェクトを保存することはできますが、エンドポイントとして設定した外部S3バケットには、それらのオブジェクトのコピーは作成されなくなります。["S3テナントアカウントのプラットフォームサービスを管理する"](#)を参照してください。
- *独自のIDソースを使用する*の設定を変更することで、テナントアカウントが独自のIDソースを使用するか、Grid Manager用に構成されたIDソースを使用するかを決定します。

*独自のIDソースを使用する*が次の場合：

- 無効化され、かつ選択されている状態ですが、テナントは既に独自のIDソースを有効にしています。テナントは、Grid Manager用に構成されたIDソースを使用する前に、自身のIDソースを無効にする必要があります。
- 無効で選択されていない場合、SSO は StorageGRID システムに対して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、*S3 Select を許可する*権限を選択または解除してください。["テナントアカウントのS3 Selectの管理"](#)を参照してください。
- 「グリッドフェデレーション接続を使用する」権限を削除するには：
 - i. 「グリッド連携」タブを選択します。
 - ii. 「権限を削除」を選択します。
- 「グリッドフェデレーション接続を使用する」権限を追加するには：
 - i. 「グリッド連携」タブを選択します。
 - ii. 「グリッドフェデレーション接続を使用する」チェックボックスを選択します。
 - iii. 必要に応じて、*既存のローカルユーザーとグループを複製する*を選択すると、それらをリモートグリッドに複製できます。必要に応じて、進行中のクローン作成を停止したり、前回のクローン作成操作完了後に一部のローカルユーザーまたはグループのクローン作成に失敗した場合に、クローン作成を再試行したりできます。
- 最大保持期間を設定するか、コンプライアンスモードを有効にするには：



これらの設定を使用するには、グリッド上でS3オブジェクトロックを有効にする必要があります。

- i. 「S3 Object Lock」タブを選択してください。
- ii. 「最大保持期間を設定」には、値を入力し、プルダウンから期間を選択してください。

- iii. 「コンプライアンスモードを許可する」のチェックボックスを選択してください。

StorageGRIDテナントのローカルルートユーザーのパスワードを変更する

テナントのローカルルートユーザーがアカウントからロックアウトされた場合、ルートユーザーのパスワードを変更する必要があることがあります。

開始する前に

- "対応ウェブブラウザ" を使用して Grid Manager にサインインしています。
- "特定のアクセス権限"があります。

タスク概要

StorageGRID システムでシングル サインオン (SSO) が有効になっている場合、ローカルのルートユーザーはテナントアカウントにサインインできません。ルートユーザーのタスクを実行するには、ユーザーはテナントに対する Root access 権限を持つフェデレーショングループに所属している必要があります。

手順

1. 「テナント」を選択します。

Tenants

View information for each tenant account. Depending on the timing of ingests, network connectivity, and node status, the usage data shown might be out of date. To view more recent values, select the tenant name.

[Create](#) [Export to CSV](#) [Actions](#)

Displaying 5 results

☐	Name	Logical space used	Quota utilization	Quota	Object count	Sign in/Copy URL
☐	Tenant 01	2.00 GB	10%	20.00 GB	100	→ 📄
☐	Tenant 02	85.00 GB	85%	100.00 GB	500	→ 📄
☐	Tenant 03	500.00 TB	50%	1.00 PB	10,000	→ 📄
☐	Tenant 04	475.00 TB	95%	500.00 TB	50,000	→ 📄
☐	Tenant 05	5.00 GB	—	—	500	→ 📄

2. テナントアカウントを選択してください。以下のいずれかの方法を実行できます。
 - テナントのチェックボックスを選択し、**Actions > Change root password** 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、**Actions > Change root password** 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てください。
4. * 保存 * を選択します。

StorageGRID テナント アカウントを削除する

テナントのシステムへのアクセス権を完全に削除したい場合は、テナントアカウントを

削除できます。

開始する前に

- ["対応ウェブブラウザ"](#) を使用して Grid Manager にサインインしています。
- ["特定のアクセス権限"](#)があります。
- テナントアカウントに関連付けられているすべてのS3バケットとオブジェクトを削除しました。
- テナントがグリッドフェデレーション接続の使用を許可されている場合、["グリッドフェデレーション接続の使用権限を持つテナントを削除する"](#)に関する考慮事項を確認済みであることが必要です。

手順

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

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

3. 複数のテナントを削除するには、チェックボックスを選択し、**Actions > Delete** を選択します。
4. 単一のテナントを削除するには、次のいずれかの操作を行います。
 - チェックボックスを選択し、**Actions > Delete** を選択します。
 - テナント名を選択して詳細ページを表示し、アクション > 削除 を選択します。
5. 「はい」を選択します。

プラットフォームサービスを管理する

StorageGRID プラットフォーム サービスについて学ぶ

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含まれます。

S3テナントアカウント向けにプラットフォームサービスを有効にする場合は、テナントがこれらのサービスを利用するために必要な外部リソースにアクセスできるように、グリッドを設定する必要があります。

プラットフォームサービスは["ブランチバケット"](#)ではサポートされていません。

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 バケットの特定のオブジェクトを指定された外部宛先にミラーリングするために使用されます。

例えば、CloudMirror レプリケーションを使用して特定の顧客レコードを Amazon S3 にミラーリングし、AWS サービスを活用してデータの分析を実行することができます。

CloudMirrorレプリケーション機能には、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、["グリッド間レプリケーションとCloudMirrorレプリケーションの比較"](#)を参照してください。



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

通知

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

例えば、バケットに追加された各オブジェクトについて、管理者にアラートを送信するように設定できます。ここでいうオブジェクトとは、重大なシステムイベントに関連付けられたログファイルを表します。



S3オブジェクトロックが有効になっているバケットでイベント通知を設定することは可能ですが、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やLegal Hold statusなど）は通知メッセージには含まれません。

検索統合サービス

検索統合サービスは、S3オブジェクトのメタデータを指定されたElasticsearchインデックスに送信するために使用され、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ます。

例えば、バケットを設定して、S3オブジェクトのメタデータをリモートのElasticsearchサービスに送信するようにすることができます。その後、Elasticsearchを使用してバケット全体にわたる検索を実行したり、オブジェクトのメタデータに存在するパターンの高度な分析を実行したりすることができます。



Elasticsearchとの連携はS3オブジェクトロックが有効になっているバケットで構成できますが、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ステータスなど）は通知メッセージには含まれません。

プラットフォームサービスを利用することで、テナントは外部ストレージリソース、通知サービス、検索サービス、分析サービスなどを自身のデータに対して利用できるようになります。プラットフォームサービスのターゲットロケーションは通常、StorageGRID 環境の外部にあるため、テナントがこれらのサービスを利用することを許可するかどうかを決定する必要があります。その場合は、テナントアカウントを作成または編集する際に、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。テナントが生成するプラットフォームサービスメッセージが宛先に確実に届くように、ネットワークを構成する必要もあります。

プラットフォームサービスの利用に関する推奨事項

プラットフォームサービスを使用する前に、以下の推奨事項に注意してください。

- 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、宛先エンドポイントの S3 バケットのバージョン管理も有効にする必要があります。これにより、CloudMirror レプリケーションがエンドポイント上で類似のオブジェクトバージョンを生成できるようになります。
- S3リクエストで CloudMirror レプリケーション、通知、および検索統合を必要とするアクティブなテナントを100個以上使用しないでください。アクティブなテナントが100を超えると、S3クライアントのパフォーマンスが低下する可能性があります。
- 完了できないエンドポイントへのリクエストは、最大500,000件までキューに格納されます。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。新しいテナントはこの500,000の上限を一時的に超えることが認められており、新規作成されたテナントが不当に不利益を被ることがないようにしています。

関連情報

- ["プラットフォームサービスを管理する"](#)
- ["ストレージプロキシ設定を構成する"](#)
- ["StorageGRID の監視"](#)

StorageGRID プラットフォーム サービス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宛先に確実に配信されるように、グリッドのネットワーク設定を行う必要があります。

S3テナントアカウントの作成時または更新時に、その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することができます。プラットフォームサービスが有効になっている場合、テナントはS3バケットからのCloudMirrorレプリケーション、イベント通知、または検索統合メッセージの宛先として機能するエンドポイントを作成できます。これらのプラットフォームサービスメッセージは、ADCサービスを実行するストレージノードから宛先エンドポイントに送信されます。

例えば、テナントは次のような種類の宛先エンドポイントを設定できます。

- ローカルでホストされているElasticsearchクラスター
- Amazon Simple Notification Service メッセージの受信をサポートするローカルアプリケーション
- ローカルでホストされているKafkaクラスター
- HTTP POST通知リクエストをサポートする、外部またはローカルホストのWebhookエンドポイント。

このエンドポイントは、Fluentdなどのさまざまなウェブサーバー、フレームワーク、またはデータ処理ツールでホストできます。

- 同じまたは別のStorageGRIDインスタンス上にローカルホストされたS3バケット
- Amazon Web Services上のエンドポイントなど、外部エンドポイント。

プラットフォームサービスメッセージが確実に配信されるようにするには、ADCストレージノードを含むネットワークを構成する必要があります。プラットフォームサービスメッセージを宛先エンドポイントに送信するために、以下のポートが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以下のポートで送信されます：

- **80**：httpで始まるエンドポイントURIの場合（ほとんどのエンドポイント）
- **443**：httpsで始まるエンドポイントURIの場合（ほとんどのエンドポイント）
- **9092**：httpまたはhttpsで始まるエンドポイントURIの場合（Kafkaエンドポイントのみ）

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



StorageGRID デプロイメントが CloudMirror レプリケーションの宛先として使用されている場合、レプリケーション メッセージはポート 80 または 443 以外のポートで受信される可能性があります。宛先の StorageGRID デプロイメントが S3 に使用し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。

非透過型のプロキシ サーバを使用する場合は、インターネット上のエンドポイントなどの外部エンドポイントにメッセージを送信できるようにするために、"[ストレージ プロキシ設定を構成する](#)"も必要です。

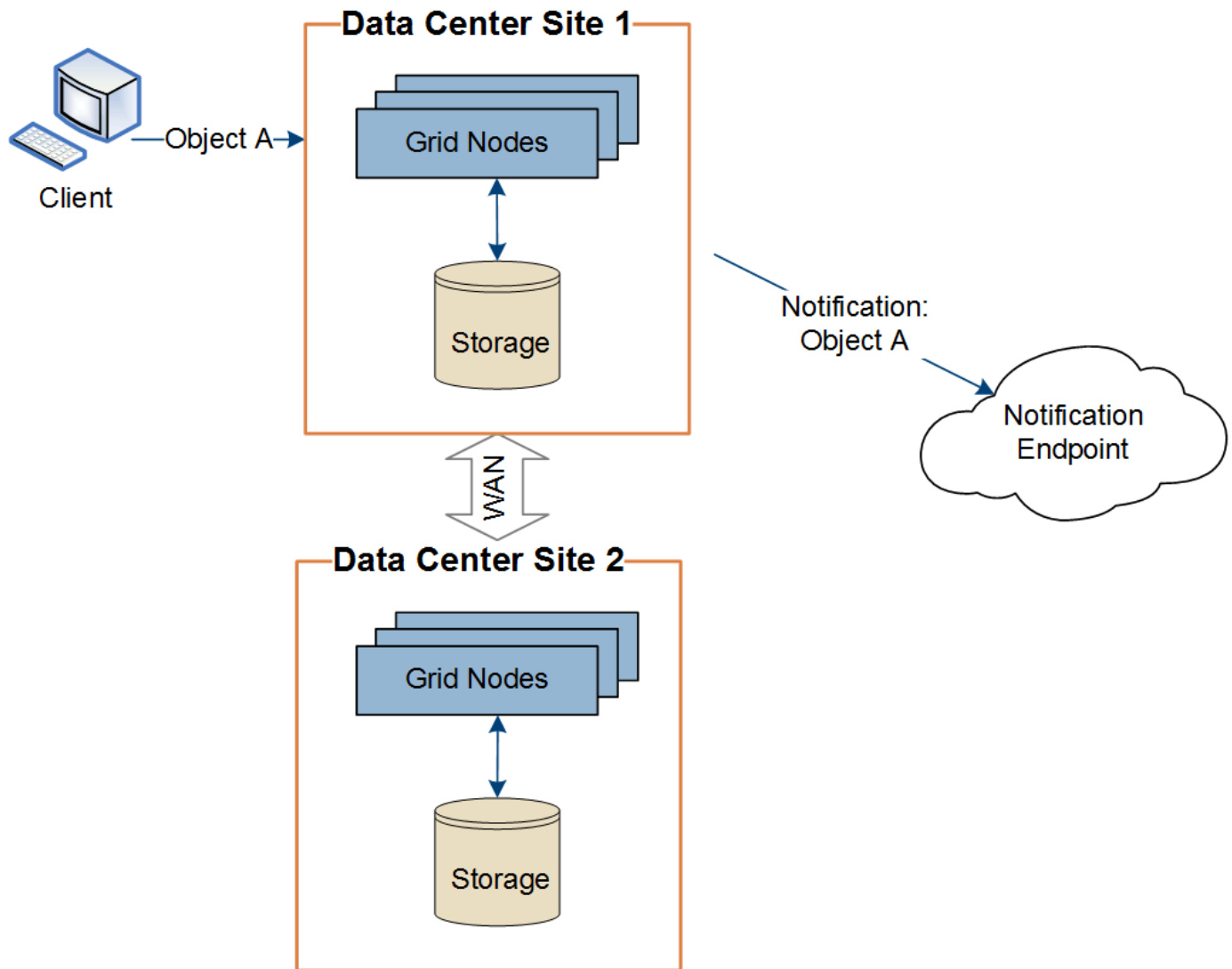
関連情報

["テナントアカウントを使用する"](#)

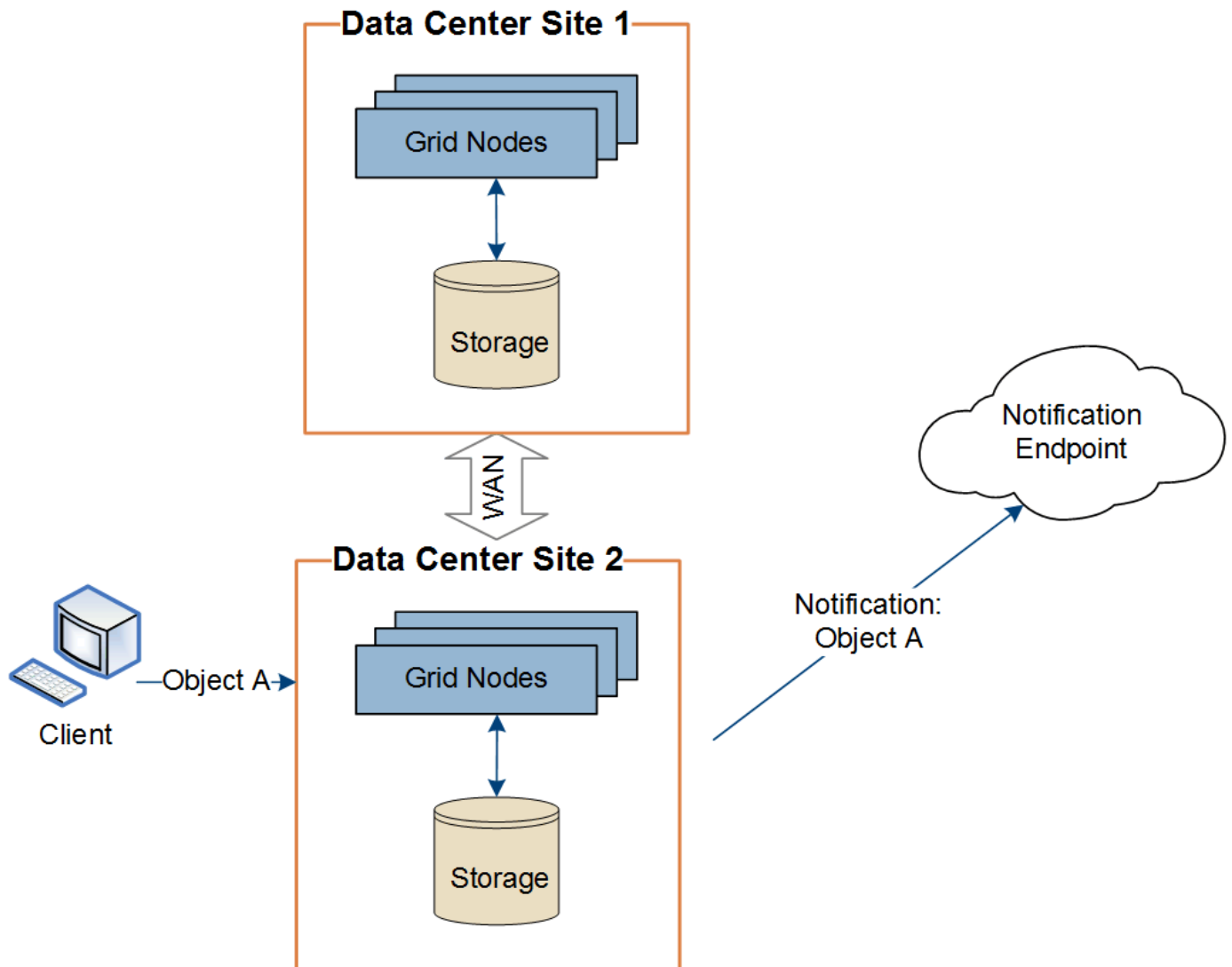
サイトごとの **StorageGRID** プラットフォーム サービス メッセージの配信

プラットフォームサービスのすべての運用は、サイトごとに実行されます。

つまり、テナントがクライアントを使用してデータセンターサイト 1 のゲートウェイノードに接続し、オブジェクトに対して S3 API の作成操作を実行すると、その操作に関する通知がデータセンターサイト 1 からトリガーされ、送信されます。



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



各サイトのネットワークが、プラットフォームサービスのメッセージを宛先に配信できるように構成されていることを確認してください。

StorageGRID プラットフォーム サービスのトラブルシューティング

プラットフォームサービスで使用するエンドポイントは、テナントユーザーがテナントマネージャーで作成および管理します。ただし、テナントがプラットフォームサービスの設定や使用に関して問題を抱えている場合は、グリッドマネージャー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

テナントがプラットフォームサービスを利用するには、まずテナントマネージャーを使用して1つ以上のエンドポイントを作成する必要があります。各エンドポイントは、1つのプラットフォームサービスの外部宛先を表します。たとえば、StorageGRID S3バケット、Amazon Web Servicesバケット、Amazon Simple Notification Serviceトピック、Kafkaトピック、またはローカルもしくはAWSでホストされているElasticsearchクラスターなどです。各エンドポイントには、外部リソースの場所と、そのリソースにアクセスするために必要な認証情報の両方が含まれています。

テナントがエンドポイントを作成すると、StorageGRID システムは、エンドポイントが存在すること、およ

び指定された認証情報を使用してアクセスできることを検証します。エンドポイントへの接続は、各サイトの1つのノードから検証されます。

エンドポイントの検証が失敗した場合、エラーメッセージに失敗した理由が表示されます。テナントユーザーは問題を解決してから、エンドポイントの作成を再度試みてください。



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場合、エンドポイントの作成は失敗します。

既存のエンドポイントに関する問題

StorageGRID が既存のエンドポイントへのアクセスを試みた際にエラーが発生した場合、Tenant Manager のダッシュボードにメッセージが表示されます。



One or more endpoints have experienced an error and might not be functioning properly. Go to the [Endpoints](#) page to view the error details. The last error occurred 2 hours ago.

テナントユーザーは、エンドポイントページにアクセスして、各エンドポイントの最新のエラーメッセージを確認し、エラーが発生した日時を特定できます。「最終エラー」列には、各エンドポイントの最新のエラーメッセージが表示され、エラーが発生した日時が表示されます。 アイコンが表示されているエラーは、過去7日以内に発生したものです。

Platform services endpoints

A platform services endpoint stores the information StorageGRID needs to use an external resource as a target for a platform service (CloudMirror replication, notifications, or search integration). You must configure an endpoint for each platform service you plan to use.



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

5 endpoints

Create endpoint

Delete endpoint

☐	Display name 	Last error 	Type 	URI 	URN 
☐	my-endpoint-2	 2 hours ago	Search	http://10.96.104.30:9200	urn:sgws:es:::mydomain/sveloso/_doc
☐	my-endpoint-3	 3 days ago	Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example1
☐	my-endpoint-5	12 days ago	Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example3
☐	my-endpoint-4		Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example2
☐	my-endpoint-1		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket1



*最終エラー*列に表示されるエラーメッセージの中には、括弧内に logID が含まれている場合があります。グリッド管理者またはテクニカルサポート担当者は、このIDを使用して、bycast.log 内のエラーに関する詳細情報を確認できます。

プロキシ サーバに関する問題

ストレージノードとプラットフォームサービスエンドポイント間に"ストレージプロキシ"を設定している場合、プロキシサービスが StorageGRID からのメッセージを許可しないと、エラーが発生する可能性があります。これらの問題を解決するには、プロキシ サーバの設定を確認して、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、テナントマネージャーのダッシュボードに警告メッセージが表示されます。エラーの詳細については、エンドポイントのページをご覧ください。

クライアント操作が失敗しました

プラットフォームサービスの一部の問題により、S3バケットに対するクライアント操作が失敗する可能性があります。例えば、内部の Replicated State Machine (RSM) サービスが停止した場合、または配信待ちのプラットフォームサービスメッセージが多すぎる場合、S3クライアントの操作は失敗します。

サービスのステータスを確認するには：

1. ノード > サイト > ストレージノード > 概要 を選択します。
2. アラートテーブルでアクティブなアラートを確認してください。
3. 発生しているアラートをすべて解決してください。必要に応じて、テクニカルサポートにお問い合わせください。

回復可能なエンドポイントエラーと回復不可能なエンドポイントエラー

エンドポイントが作成された後、プラットフォームサービスのリクエストエラーは、さまざまな理由で発生する可能性があります。一部のエラーは、ユーザーの介入によって回復可能です。例えば、回復可能なエラーは次のような理由で発生する可能性があります：

- ユーザーの認証情報が削除されたか、有効期限が切れています。
- 宛先バケットが存在しません。
- 通知を送信できません。

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

その他のエラーは回復不可能です。例えば、以下のような理由で回復不可能なエラーが発生する可能性があります。

- エンドポイントは削除されました。
- ウェブフックエンドポイントの宛先が、通知リクエストに対して `400 Bad Request` エラーで応答します。

StorageGRID で回復不可能なエンドポイントエラーが発生した場合：

- Grid Manager で、「サポート」>「ツール」>「メトリクス」>「Grafana」>「プラットフォームサービス概要」に移動して、エラーの詳細を確認します。
- テナントマネージャーで、**STORAGE (S3) > Platform Services Endpoints** に移動して、エラーの詳細を確認してください。
- 関連するエラーについては、`/var/local/log/bycast-err.log`を確認してください。ADC サービスを含むストレージノードには、このログファイルが含まれています。

プラットフォームサービスメッセージを配信できません

宛先側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発生した場合、バケットに対するクライアント操作は成功しますが、プラットフォームサービスメッセージは配信されません。たとえば、宛先で認証情報が更新され、StorageGRID が宛先サービスへの認証を実行できなくなった場合に、このようなエラーが発生することがあります。

関連するアラートを確認してください。

プラットフォームサービスリクエストのパフォーマンスが低下しています

StorageGRID ソフトウェアは、S3 バケットへの受信リクエストの送信速度が、宛先エンドポイントがリクエストを受信できる速度を超えた場合、受信リクエストを制限する可能性があります。スロットリングは、宛先エンドポイントへの送信を待機しているリクエストのバックログが存在する場合にのみ発生します。

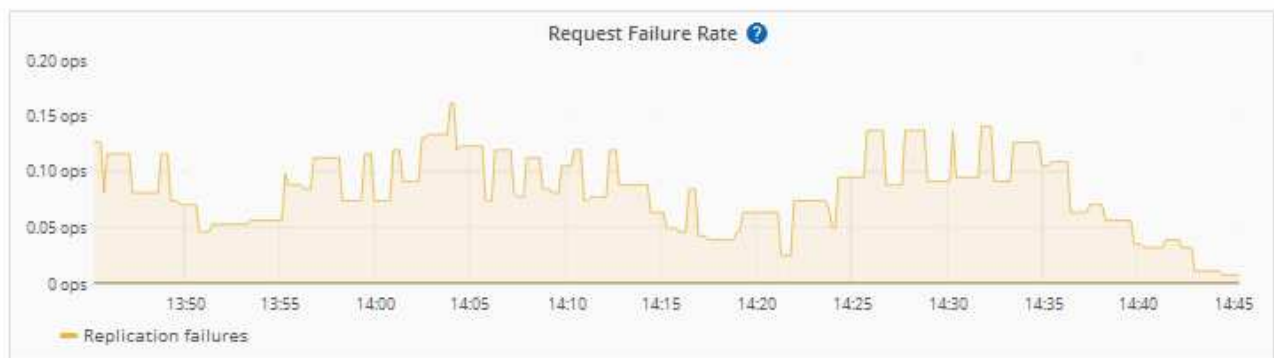
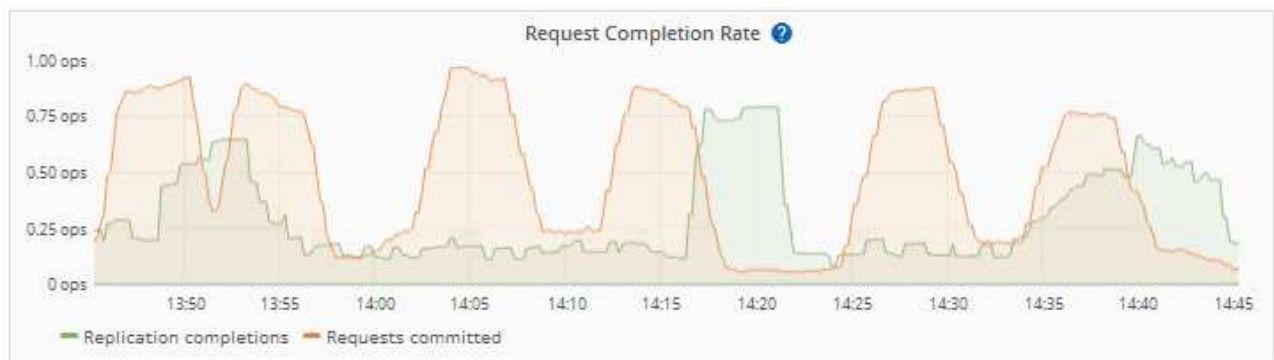
唯一目に見える影響は、受信する S3 リクエストの実行に時間がかかるようになることです。パフォーマンスが著しく低下し始めた場合は、取り込み速度を下げるか、より容量の大きいエンドポイントを使用してください。リクエストのバックログが増大し続けると、クライアントの S3 操作（PUT リクエストなど）は最終的に失敗します。

CloudMirror のリクエストは、検索統合やイベント通知のリクエストよりもデータ転送量が多いため、宛先エンドポイントのパフォーマンスの影響を受けやすい傾向があります。

プラットフォームサービスリクエストが失敗しました

プラットフォームサービスの要求失敗率を確認するには：

1. * Nodes * を選択します。
2. サイト > *プラットフォームサービス*を選択します。
3. リクエストエラー率のグラフを確認します。

[1 hour](#) [1 day](#) [1 week](#) [1 month](#) [Custom](#)

プラットフォームサービスが利用できないというアラート

Platform services unavailable アラートは、RSM サービスが稼働しているか利用可能なストレージノードが少なすぎるため、サイトでプラットフォームサービス操作を実行できないことを示します。

RSMサービスは、プラットフォームサービスのリクエスト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、サイト内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てください。（RSMサービスは、ADCサービスも搭載しているストレージノードに存在します。）次に、それらのストレージノードの過半数が稼働中で利用可能であることを確認してください。



同一サイトにおいて、RSMサービスを含むストレージノードが複数故障した場合、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追加のトラブルシューティングガイダンス

詳細については、[テナントアカウントを使用する](#)、[プラットフォームサービスのエンドポイントのトラブルシューティング](#)を参照してください。

関連情報

["StorageGRID システムのトラブルシューティング"](#)

StorageGRID でテナント アカウントの S3 Select を管理する

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

S3 Selectは、データベースや関連リソースをデプロイすることなく、大量のデータを効率的に検索できる方法を提供します。また、データ取得にかかるコストと遅延も削減します。

S3 Selectとは何ですか？

S3 Select を使用すると、S3 クライアントはSelectObjectContentリクエストを使用して、オブジェクトから必要なデータのみをフィルタリングして取得できます。StorageGRID の S3 Select の実装には、S3 Select のコマンドと機能のサブセットが含まれています。

S3 Selectを使用する際の考慮事項と要件

グリッド管理要件

グリッド管理者は、テナントにS3 Select権限を付与する必要があります。「S3 Selectを許可する」を選択するのは、["テナントの作成"](#)または["テナントの編集"](#)の場合です。

オブジェクトフォーマットの要件

クエリ対象のオブジェクトは、以下のいずれかの形式である必要があります。

- **CSV**。そのまま使用することも、GZIPまたはBZIP2アーカイブに圧縮して使用することもできます。
- **Parquet**。Parquetオブジェクトに関する追加要件：
 - S3 Selectは、GZIPまたはSnappyを使用したカラム型圧縮のみをサポートしています。S3 Selectは、Parquetオブジェクトのオブジェクト全体の圧縮をサポートしていません。
 - S3 SelectはParquet形式の出力に対応していません。出力形式はCSVまたはJSONのいずれかを指定する必要があります。
 - 圧縮されていない行グループの最大サイズは 512 MB です。
 - オブジェクトのスキーマで指定され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の論理型は使用できません。

エンドポイント要件

SelectObjectContent リクエストは、"[StorageGRID ロードバランサーエンドポイント](#)" に送信する必要があります。

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：

- サービスアプライアンスノード
- VMwareベースのソフトウェアノード
- cgroup v2が有効になっているカーネルを実行しているベアメタルノード

一般的な考慮事項

クエリをストレージノードに直接送信することはできません。



SelectObjectContent リクエストは、すべての S3 クライアントとすべてのテナントのロードバランサーのパフォーマンスを低下させる可能性があります。この機能は、必要な場合にのみ、信頼できるテナントに対してのみ有効にしてください。

["S3 Selectの使用方法"](#)を参照してください。

S3 Select 操作の"[Grafanaチャート](#)"を時系列で表示するには、グリッドマネージャで サポート > ツール > メトリクス を選択します。

クライアント接続を構成する

S3 クライアント接続を **StorageGRID** に設定

グリッド管理者として、S3クライアントアプリケーションがデータの保存と取得のためにStorageGRIDシステムに接続する方法を制御する構成オプションを管理します。



このバージョンのドキュメントサイトからは、Swiftに関する詳細情報が削除されました。参照してください ["StorageGRID 11.8: S3およびSwiftクライアント接続の設定"](#)。

設定タスク

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で前提条件タスクを実行します。

必須タスク

以下のものを入手する必要があります：

- IPアドレス
- ドメイン名
- SSL証明書

オプションのタスク

必要に応じて、以下を設定します：

- アイデンティティフェデレーション
- SSO

1. 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することができます。+

S3 セットアップ ウィザードを使用する

S3 セットアップ ウィザードの手順に従ってください。

手動で設定する

1. 高可用性グループを作成する
2. ロードバランサーエンドポイントを作成する
3. テナントアカウントを作成する
4. バケットとアクセスキーを作成する
5. ILMルールとポリシーを設定する

1. S3アプリケーションを使用して、StorageGRIDへの接続を完了します。使用予定のドメイン名にIPアドレスを関連付けるためのDNSエントリを作成してください。

必要に応じて、追加のアプリケーション設定を行ってください。

2. アプリケーションと StorageGRID でオブジェクトストレージを長期にわたって管理および監視するための継続的なタスクを実行します。

StorageGRID をクライアントアプリケーションに接続するために必要な情報

StorageGRID を S3 クライアントアプリケーションに接続する前に、StorageGRID で設定手順を実行し、必要な値を取得する必要があります。

必要な値は何ですか？

次の表に、StorageGRID で設定する必要がある値と、それらの値が S3 アプリケーションおよび DNS サーバーでどのように使用されるかを示します。

Value	値が設定されている場所	価値が活用される場所
仮想IP (VIP) アドレス	StorageGRID > HA グループ	DNSエントリ
ポート	StorageGRID > ロードバランサー エンドポイント	クライアントアプリケーション
SSL証明書	StorageGRID > ロードバランサー エンドポイント	クライアントアプリケーション
サーバー名 (FQDN)	StorageGRID > ロードバランサー エンドポイント	- 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 > テナントとバケッ ト	クライアントアプリケーション
バケット/コンテナ名	StorageGRID > テナントとバケッ ト	クライアントアプリケーション

これらの値はどのように取得できますか？

ご要望に応じて、以下のいずれかの方法で必要な情報を取得できます：

- **"S3セットアップウィザード"**を使用してください。S3 セットアップ ウィザードを使用すると、StorageGRID で必要な値をすばやく設定でき、S3 アプリケーションの設定時に使用できるファイルを 1 つまたは 2 つ出力します。ウィザードは必要な手順を案内し、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します。



S3 アプリケーションを構成する場合、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 ウィザードの使用をお勧めします。

- **"FabricPool セットアップウィザード"**を使用してください。S3 セットアップ ウィザードと同様に、FabricPool セットアップ ウィザードを使用すると、必要な値をすばやく設定でき、ONTAP で FabricPool クラウド階層を設定する際に使用できるファイルが出力されます。



StorageGRID を FabricPool クラウド層のオブジェクトストレージシステムとして使用する予定がある場合は、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、FabricPool セットアップ ウィザードの使用をお勧めします。

- アイテムを手動で設定する。S3 アプリケーションに接続していて、S3 セットアップ ウィザードを使用しない場合は、手動で設定を行うことで必要な値を取得できます。以下の手順に従ってください。
 - a. S3アプリケーションで使用する高可用性 (HA) グループを設定します。**"高可用性グループを構成する"**を参照してください。
 - b. S3アプリケーションが使用するロードバランサーのエンドポイントを作成します。**"ロードバランサーのエンドポイントを設定する"**を参照してください。
 - c. S3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。**"テナントアカウントを作成する"**を参照してください。

- 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ーに対してアクセスキーIDとシークレットアクセスキーを生成します。["独自のアクセスキーを作成する"](#)を参照してください。
- e. テナントアカウント内に1つ以上のS3バケットを作成します。S3については、["S3バケットを作成する"](#)を参照してください。
- 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特定の配置指示を追加するには、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ポリシーを有効化します。["ILMルールを作成する"](#)および["ILMポリシーを作成する"](#)を参照してください。

StorageGRID の S3 クライアントのセキュリティ

StorageGRID テナントアカウントは、S3 クライアントアプリケーションを使用して StorageGRID にオブジェクトデータを保存します。クライアントアプリケーションに実装されているセキュリティ対策を確認してください。

サマリ

以下のリストは、S3 REST APIにおけるセキュリティの実装方法をまとめたものです：

接続セキュリティ

TLS

サーバー認証

システムCAによって署名されたX.509サーバー証明書、または管理者によって提供されたカスタムサーバー証明書

クライアント認証

S3アカウントのアクセスキーIDとシークレットアクセスキー

クライアント許可

バケットの所有権および適用されるすべてのアクセス制御ポリシー

StorageGRID がクライアントアプリケーションにセキュリティを提供する方法

S3クライアントアプリケーションは、ゲートウェイノードまたは管理ノード上のロードバランサーサービス、あるいはストレージノードに直接接続できます。

- ロードバランサーサービスに接続するクライアントは、["ロードバランサーエンドポイントを設定する"](#)の設定方法に応じてHTTPSまたはHTTPを使用できます。

HTTPSはTLS暗号化による安全な通信を提供するため、推奨されます。エンドポイントにセキュリティ証明書を添付する必要があります。

HTTPはセキュリティが低く、暗号化されていない通信を提供するため、非本番環境またはテストグリッドでのみ使用してください。

- ストレージノードに接続するクライアントは、HTTPSまたはHTTPのどちらでも使用できます。

HTTPSがデフォルトであり、推奨されています。

HTTPはセキュリティが低く暗号化されていない通信を提供しますが、非本番環境またはテスト用グリッドに対してオプションで"有効"することができます。

- StorageGRID とクライアント間の通信は、TLS を使用して暗号化されます。
- ロードバランサーサービスとグリッド内のストレージノード間の通信は、ロードバランサーのエンドポイントがHTTP接続を受け入れるように構成されているかHTTPS接続を受け入れるように構成されているかにかかわらず、暗号化されます。
- クライアントは、REST API操作を実行するために"[HTTP認証ヘッダー](#)"をStorageGRIDに提供する必要があります。

セキュリティ証明書とクライアントアプリケーション

いずれの場合も、クライアント アプリケーションは、グリッド管理者がアップロードしたカスタム サーバー証明書、またはStorageGRID システムによって生成された証明書のいずれかを使用して TLS 接続を確立できます：

- クライアントアプリケーションがロードバランサーサービスに接続する際、ロードバランサーエンドポイント用に構成された証明書を使用します。各ロードバランサーエンドポイントには独自の証明書があります—グリッド管理者がアップロードしたカスタムサーバー証明書、またはグリッド管理者がエンドポイントの設定時にStorageGRIDで生成した証明書のいずれかです。

["ロード バランシングに関する考慮事項"](#)を参照してください。

- クライアント アプリケーションがストレージ ノードに直接接続する場合、StorageGRID システムのインストール時にストレージ ノード用に生成されたシステム生成のサーバ証明書（システム認証局によって署名されたもの）、またはグリッド管理者によってグリッド用に提供される単一のカスタム サーバ証明書を使用します。"[カスタムS3 API証明書を追加する](#)"を参照してください。

クライアントは、TLS接続を確立するために使用する証明書に署名した認証局を信頼するように設定する必要があります。

TLSライブラリでサポートされているハッシュおよび暗号化アルゴリズム

StorageGRID システムは、クライアントアプリケーションが TLS セッションを確立する際に使用できる一連の暗号スイートをサポートしています。暗号を設定するには、[設定 > セキュリティ > 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。

サポートされているTLSのバージョン

StorageGRID は TLS 1.2 および TLS 1.3 をサポートしています。



SSLv3およびTLS 1.1（またはそれ以前のバージョン）はサポートされなくなりました。

S3 セットアップ ウィザードを使用する

StorageGRID S3 セットアップ ウィザードの考慮事項と要件

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 ウィザードは、S3アプリケーションで使用するためのStorageGRIDの設定の各ステップをご案内します。ウィザードを完了する過程で、S3アプリケーションに値を入力するために使用できるファイルをダウンロードします。ウィザードを使用してシステムをより迅速に構成し、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してください。

もしあなたが"[ルートアクセス権限](#)"をお持ちの場合、StorageGRID Grid Manager の使用を開始する際に S3 セットアップ ウィザードを完了することも、後からいつでもウィザードにアクセスして完了させることもできます。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、その後ウィザードを使用して S3 アプリケーションに必要な値を組み立てることもできます。

ウィザードを使用する前に

ウィザードを使用する前に、以下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**インターフェースを設定する

高可用性（HA）グループを構成する場合、S3 アプリケーションがどのノードに接続するか、およびどの StorageGRID ネットワークが使用されるかを把握しておく必要があります。サブネット CIDR、ゲートウェイ IP アドレス、仮想 IP（VIP）アドレスに入力する値についても把握しておく必要があります。

S3アプリケーションからのトラフィックを分離するために仮想LANを使用する予定であれば、VLAN インターフェースは既に設定済みです。"[VLANインターフェースを設定する](#)"を参照してください。

IDフェデレーションと**SSO**を設定する

IDフェデレーションを使用する予定がある場合、またはStorageGRIDシステムでシングル サインオン（SSO）を使用する予定がある場合は、これらの機能が有効になっています。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に対して、どのフェデレーショングループにルートアクセス権を付与するかも把握しておく必要があります。"[IDフェデレーションを使用する](#)"および"[シングル サインオンを設定する](#)"を参照してください。

ドメイン名を取得して設定する

StorageGRID に使用する完全修飾ドメイン名（FQDN）を把握しています。ドメインネームサーバー（DNS）のエントリは、このFQDNを、ウィザードを使用して作成したHAグループの仮想IP（VIP）アドレスにマッピングします。

S3仮想ホスト型リクエストを使用する予定がある場合は、"[設定済みのS3エンドポイントドメイン名](#)"が必要です。仮想ホスト型のリクエストを使用することをお勧めします。

ロード バランシングとセキュリティ証明書の要件を確認する

StorageGRID ロード バランシングを使用する予定がある場合は、ロード バランシングに関する一般的な考慮事項を確認済みであることを確認してください。アップロードする証明書、または証明書を生成するために必要な値を用意してください。

外部（サードパーティ）の ロード バランシング エンドポイントを使用する場合は、そのロード バランサー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構成する

S3テナントがアカウントデータをクローンし、グリッドフェデレーション接続を使用してバケットオブジェクトを別のグリッドに複製できるようにする場合は、ウィザードを開始する前に次の点を確認してください。

- ["グリッドフェデレーション接続を構成しました"](#)があります。
- 接続状態は「接続済み」です。
- ルートアクセス権限があります。

StorageGRID で **S3** セットアップ ウィザードにアクセスして完了します

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ための StorageGRID を設定できます。セットアップ ウィザードは、アプリケーションが StorageGRID バケットにアクセスしてオブジェクトを保存するために必要な値を提供します。

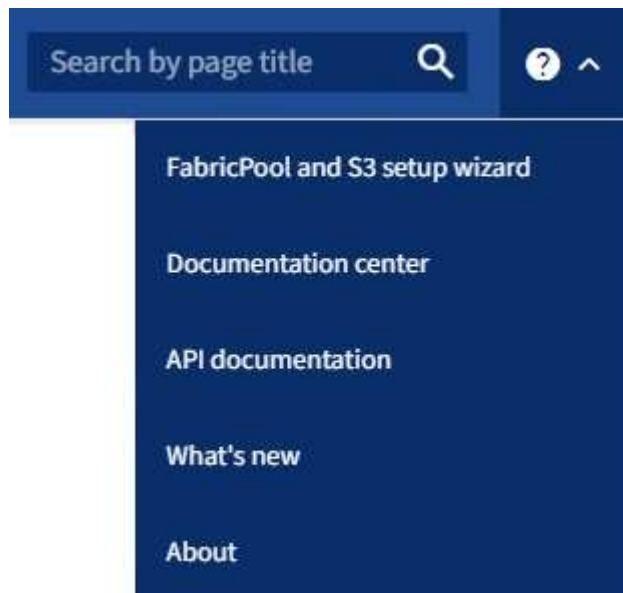
開始する前に

- あなたは["ルートアクセス権限"](#)があります。
- ウィザードを使用するための["考慮事項と要件"](#)を確認しました。

ウィザードにアクセスする

手順

1. グリッドマネージャーにサインインするには、["対応ウェブブラウザ"](#)を使用します。
2. **FabricPool** および **S3** セットアップ ウィザード のバナーがダッシュボードに表示されている場合は、バナー内のリンクを選択してください。バナーが表示されなくなった場合は、Grid Manager のヘッダーバーからヘルプアイコンを選択し、**FabricPool** および **S3** セットアップ ウィザード を選択してください。



3. FabricPool および S3 セットアップ ウィザード 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。

ステップ1/6：HAグループの設定

HA グループは、それぞれが StorageGRID ロード バランシング サービスを含むノードの集合です。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ことで、S3データ接続の可用性を維持するのに役立ちます。HAグループ内のアクティブなインターフェースに障害が発生した場合でも、バックアップインターフェースがワークロードを管理できるため、S3の運用への影響は最小限に抑えられます。

このタスクの詳細については、"[高可用性グループを管理する](#)"を参照してください。

手順

1. 外部ロード バランシングを使用する場合は、HAグループを作成する必要はありません。「この手順をスキップ」を選択して、[ステップ 2/6：ロード バランシング エンドポイントの設定](#)に進みます。
2. StorageGRID のロード バランシングを使用するには、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グループを作成する

- 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」の手順では、以下の項目を入力してください。

フィールド	説明
HAグループ名	このHAグループに固有の表示名。
概要（任意）	このHAグループの説明。

- c. 「インターフェースの追加」ステップでは、このHAグループで使用するノードインターフェースを選択します。

列ヘッダーを使用して行を並べ替えるか、検索語を入力してインターフェースをより迅速に検索してください。

ノードは1つ以上選択できますが、各ノードに対して選択できるインターフェースは1つだけです。

- d. 「インターフェースの優先順位付け」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ースとバックアップインターフェースを決定します。

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ースはプライマリインターフェースです。プライマリインターフェースは、障害が発生しない限りアクティブなインターフェースです。

HAグループに複数のインターフェースが含まれており、アクティブなインターフェースに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ースに移動します。そのインターフェースに障害が発生した場合、VIPアドレスは次のバックアップインターフェースに移動します（以降も同様）。障害が解消されると、VIPアドレスは利用可能な最も優先度の高いインターフェースに戻ります。

- e. 「IPアドレスを入力」の手順では、以下の項目を入力してください。

フィールド	説明
サブネット CIDR	CIDR 表記による VIP サブネットのアドレス — IPv4 アドレスの後にスラッシュとサブネット長（0～32）が続きます。 ネットワークアドレスにはホストビットを設定しないでください。例えば、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上にない場合は、StorageGRID VIP ローカルゲートウェイ IP アドレスを入力してください。ローカルゲートウェイの IP アドレスは、VIP サブネット内に存在する必要があります。

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なインターフェースに対して、少なくとも1つ、最大10個のVIPアドレスを入力してください。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ます。 少なくとも1つのアドレスはIPv4アドレスである必要があります。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. 「HAグループの作成」を選択し、「完了」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 バランシングの手順に進んでください。

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グループを選択*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 バランシングの手順に進んでください。

ステップ 2/6：ロード バランシング エンドポイントの設定

StorageGRID は、ロード バランサーを使用して、クライアントアプリケーションからのワークロードを管理します。ロード バランシングにより、複数のストレージノード間で速度と接続容量を最大化します。

StorageGRID ロード バランシング サービスはすべてのゲートウェイノードと管理ノードに存在しており、このサービスを使用するか、外部（サードパーティ）のロードバランサーに接続することができます。StorageGRID ロード バランシングの使用を推奨します。

このタスクの詳細については、"[ロード バランシングに関する考慮事項](#)"を参照してください。

StorageGRID ロード バランシング サービスを使用するには、**StorageGRID** ロード バランサー タブを選択し、使用するロードバランサー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ーを使用するには、外部ロードバランサー タブを選択し、設定済みのシステムに関する詳細情報を入力します。

エンドポイントを作成する

手順

1. ロード バランシングの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. 「エンドポイントの詳細を入力」の手順では、以下の項目を入力してください。

フィールド	説明
Name	エンドポイントを表す分かりやすい名前。
ポート	ロード バランシングに使用する StorageGRID のポート。このフィールドには、最初に作成するエンドポイントの場合、デフォルトで 10433 が設定されていますが、未使用の外部ポート番号を入力できます。80 または 443 を入力した場合、これらのポートは管理ノードで予約されているため、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。 注: 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ていません。"StorageGRID内部ポート"を参照してください。
クライアントタイプ	*S3*である必要があります。
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 StorageGRID と通信することはサポートされていますが、推奨されません。

3. 「バインディングモードの選択」ステップで、バインディングモードを指定します。バインディングモードは、エンドポイントへのアクセス方法を、任意の IP アドレスを使用するか、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するかによって制御します。

モード	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へのアクセスを制限する必要がない限り、Global 設定（デフォルト）を使用してください。
HAグループの仮想IPアドレス	クライアントはこのエンドポイントにアクセスするために、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。 このバインディングモードを使用するエンドポイントは、エンドポイントに選択した HA グループが重複しない限り、すべて同じポート番号を使用できます。

モード	説明
ノードインターフェース	クライアントは、このエンドポイントにアクセスするために、選択したノードインターフェースの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	選択したノードの種類に応じて、クライアントはこのエンドポイントにアクセスするために、管理ノードのIPアドレス（または対応するFQDN）か、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。

4. テナントアクセス手順では、以下のいずれかを選択してください。

フィールド	説明
すべてのテナントを許可する（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。
選択されたテナントを許可する	選択されたテナントアカウントのみが、このエンドポイントを使用して自身のバケットにアクセスできます。
選択したテナントをブロックする	選択され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はこのエンドポイントを使用できます。

5. 「証明書の添付」手順では、以下のいずれかを選択してください。

フィールド	説明
証明書のアップロード（推奨）	このオプションを使用して、CA署名付きサーバー証明書、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します。
証明書を生成する	このオプションを使用して、自己署名証明書を生成します。入力内容の詳細については、 "ロードバランサーのエンドポイントを設定する" を参照してください。
StorageGRID S3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た場合にのみ使用してください。詳細については、 "S3 API証明書の設定" を参照してください。

6. 「完了」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設定ステップに進みます。



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は、最大15分かかる場合があります。

既存のロード バランシング 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には、「ロード バランシング エンドポイントの選択」からそ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設定ステップに進みます。

外部ロード バランシングを使用する

手順

1. 外部ロード バランシングを使用するには、以下の項目を入力してください。

フィールド	説明
FQDN	外部ロード バランサー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 バランシングに接続するために使用するポート番号。
Certificate	外部ロード バランシングのサーバー証明書をコピーして、このフィールドに貼り付けてください。

2. *続行*を選択して、テナントとバケットの設定ステップに進みます。

ステップ3/6：テナントとバケットを作成する

テナントとは、S3 アプリケーションを使用して StorageGRID にオブジェクトを保存および取得できるエンティティです。各テナントは、独自のユーザー、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を持っています。

バケットとは、テナントのオブジェクトおよびオブジェクトのメタデータを保存するために使用されるコンテナです。テナントは複数のバケットを持つことができますが、ウィザードを使用すると、テナントとバケットを最も迅速かつ簡単に作成できます。後でバケットを追加したり、オプションを設定したりする必要がある場合は、Tenant Manager を使用できます。

このタスクの詳細については、["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"](#)を参照してください。

手順

1. テナントアカウントの名前を入力してください。

テナント名は一意である必要はありません。テナントアカウントが作成されると、固有の数値アカウントIDが付与されます。

2. StorageGRID システムで ["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 \(SSO\)"](#)、またはその両方を使用し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。

オプション	これを実行します
IDフェデレーションが有効になっていない場合	ローカルのrootユーザー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てください。
IDフェデレーションが有効になっている場合	a. 既存のフェデレーテッドグループを選択して、テナントの" ルートアクセス権限 "を付与します。 b. 必要に応じて、ローカルのルートユーザー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	既存のフェデレーテッドグループを選択して、テナントの" ルートアクセス権限 "を設定します。ローカルユーザーはサインインできません。

3. ウィザードにルートユーザーのアクセスキーIDとシークレットアクセスキーを作成させる場合は、**Create root user S3 access key automatically** を選択してください。

テナントの唯一のユーザーがrootユーザーである場合は、このオプションを選択してください。他のユーザーがこのテナントを使用する場合は、"**テナントマネージャーを使用する**"キーと権限を設定してください。

4. このテナント用にバケットを今すぐ作成する場合は、*このテナント用にバケットを作成する*を選択してください。



グリッドに対してS3オブジェクトロックが有効になっている場合、この手順で作成されるバケットではS3オブジェクトロックは有効になりません。このS3アプリケーションで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、今すぐバケットを作成するオプションを選択しないでください。代わりに、Tenant Manager を使用して"**バケットを作成する**"後で行ってください。

- 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てください。例えば、s3-bucket。

バケットを作成した後は、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*リージョン*を選択してください。

デフォルトのリージョン（us-east-1）を使用してください。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ために将来 ILM を使用する予定がない限り。

5. 「作成して続行」を選択します。

ステップ4/6：データのダウンロード

ダウンロードデータ手順では、先ほど設定した内容の詳細を保存するために、1つまたは2つのファイルをダウンロードできます。

手順

1. 「ルートユーザーの S3 アクセスキーを自動的に作成する」を選択した場合は、以下のいずれか、または両方を実行してください。

- 「アクセスキーをダウンロード」を選択して、テナントアカウント名、アクセスキーID、およびシークレットアクセスキーを含む`.csv`ファイルをダウンロードします。
 - コピーアイコン () を選択して、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. *構成値のダウンロード*を選択して、ロード バランシングエンドポイント、テナント、バケット、およびルートユーザーの設定を含む`.txt`ファイルをダウンロードします。
 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、キーは利用できなくなります。この情報は StorageGRID システムのデータの取得に使用される可能性があるため、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、キーをダウンロードまたはコピーしたことを確認するチェックボックスを選択してください。
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。

ステップ 5/6 : S3 の ILM ルールと ILM ポリシーを確認する

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、および取り込み動作を制御します。StorageGRID に付属の 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、少なくとも 1 つの新しいポリシーを有効化するまで有効です。

手順

1. ページに記載されている情報を確認してください。
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して特定の指示を追加する場合は、新しいルールと新しいポリシーを作成してください。["ILMルールを作成する"](#)および["ILMポリシーを使用する"](#)を参照してください。
3. 「これらの手順を確認し、何をすべきか理解しました」を選択してください。
4. 次に何をすべきかを理解している場合は、チェックボックスを選択してください。
5. 続行 を選択して 概要 に進みます。

ステップ 6/6 : 概要の確認

手順

1. 概要を確認してください。
2. 次の手順では、S3クライアントに接続する前に必要となる可能性のある追加の設定について説明していますので、詳細をメモしておいてください。例えば、「rootとしてサインイン」を選択すると、Tenant Manager に移動し、そこでテナントユーザーの追加、バケットの追加作成、バケット設定の更新を行うことができます。
3. **Finish** 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グループを管理する

StorageGRID 高可用性グループについて学ぶ

高可用性（HA）グループは、S3クライアントへの高可用性データ接続、およびGrid ManagerとTenant Managerへの高可用性接続を提供します。

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ースを、高可用性（HA）グループにグループ化することができます。HAグループ内のアクティブなインターフェースに障害が発生した場合、バックアップインターフェースがワークロードを管理できます。

各HAグループは、選択されたノード上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クライアントに対して高可用性のデータ接続を提供します。
- 管理ノードのみを含むHAグループは、グリッドマネージャおよびテナントマネージャへの高可用性接続を提供します。
- サービスアプライアンスとVMwareベースのソフトウェアノードのみを含むHAグループは、["S3 Selectを使用するS3テナント"](#)に対して高可用性接続を提供できます。S3 Selectを使用する際には、HAグループの使用が推奨されますが、必須ではありません。

HAグループはどのように作成するのですか？

- 1つまたは複数の管理ノードまたはゲートウェイノードに対して、ネットワークインターフェースを選択します。グリッドネットワーク（eth0）インターフェース、クライアントネットワーク（eth2）インターフェース、VLANインターフェース、またはノードに追加したアクセスインターフェースを使用できます。



DHCPによって割り当てられたIPアドレスを持つインターフェースは、HAグループに追加できません。

- プライマリインターフェースとして指定するインターフェースを1つ指定します。プライマリインターフェースは、障害が発生しない限りアクティブなインターフェースです。
- バックアップインターフェースの優先順位は、ユーザーが決定します。
- グループには1～10個の仮想IP（VIP）アドレスを割り当てます。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、["高可用性グループを構成する"](#)を参照してください。

アクティブインターフェースとは何ですか？

通常動作時、HAグループのすべてのVIPアドレスは、優先順位で最初のインターフェースであるプライマリインターフェースに追加されます。プライマリインターフェースが利用可能な限り、クライアントがグループのVIPアドレスに接続する際には常にプライマリインターフェースが使用されます。つまり、通常動作時には、プライマリインターフェースがグループの「アクティブな」インターフェースとなります。

同様に、通常動作時において、HAグループの優先度の低いインターフェースは「バックアップ」インターフェー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ースは、プライマリ（現在アクティブな）インターフェースが使用不能になった場合にのみ使用されます。

ノードの現在のHAグループステータスを表示する

ノードがHAグループに割り当てられているかどうか、およびその現在のステータスを確認するには、「ノード」>「node」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、ノードはリストされているHAグループに割り当てられます。グループ名の後の値は、HAグループ内のノードの現在の状態を示します。

- アクティブ：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。これはバックアップインターフェースです。
- 停止：高可用性（keepalived）サービスが手動で停止されたため、このノードでHAグループをホストできません。
- **Fault**: HAグループをこのノードでホストできない理由は、以下のいずれかまたは複数です。
 - ノード上でロード バランシング（nginx-gw）サービスが実行されていません。
 - ノードのeth0またはVIPインターフェースがダウンしています。
 - 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、Admin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、FabricPool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。

DC1-ADM1 (Primary Admin Node)

Overview Hardware Network Storage Load balancer Tasks

Node information

Name: DC1-ADM1

Type: Primary Admin Node

ID: ce00d9c8-8a79-4742-bdef-c9c658db5315

Connection state: ✔ Connected

Software version: 11.6.0 (build 20211207.1804.614bc17)

HA groups:

- Admin clients (Active)
- FabricPool clients (Backup)

IP addresses:

- 172.16.1.225 - eth0 (Grid Network)
- 10.224.1.225 - eth1 (Admin Network)
- 47.47.0.2, 47.47.1.225 - eth2 (Client Network)

[Show additional IP addresses](#)

アクティブなインターフェースが故障した場合、どうなりますか？

現在VIPアドレスをホストしているインターフェースがアクティブなインターフェースです。HAグループに複

数のインターフェースが含まれており、アクティブなインターフェースに障害が発生した場合、VIPアドレスは優先順位に従って、最初に利用可能なバックアップインターフェースに移動します。そのインターフェースに障害が発生した場合、VIPアドレスは次に利用可能なバックアップインターフェースに移動し、以降も同様に続きます。

フェイルオーバーは、以下のいずれかの理由で発生する可能性があります。

- インターフェースが設定されているノードがダウンします。
- インターフェースが設定されているノードは、少なくとも2分間、他のすべてのノードとの接続を失います。
- アクティブなインターフェースがダウンします。
- ロード バランシング サービスが停止します。
- 高可用性サービスが停止します。



フェイルオーバーは、アクティブなインターフェースをホストするノードの外部にあるネットワーク障害によってトリガーされない場合があります。同様に、フェイルオーバーは Grid Manager または Tenant Manager のサービスによってトリガーされません。

フェイルオーバー処理は通常数秒しかかからず、非常に高速であるため、クライアントアプリケーションへの影響はほとんどなく、通常の再試行動作によって動作を継続できます。

障害が解消され、より優先度の高いインターフェースが再び利用可能になると、VIPアドレスは自動的に利用可能な最も優先度の高いインターフェースに移動されます。

StorageGRID HA グループによる高可用性の提供方法

高可用性（HA）グループを使用して、オブジェクトデータおよび管理用途向けに StorageGRID への高可用性接続を提供できます。

- HAグループは、グリッドマネージャーまたはテナントマネージャーへの高可用性の管理接続を提供できます。
- HAグループは、S3クライアントに対して高可用性のデータ接続を提供できます。
- インターフェースが1つだけのHAグループでは、複数の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することができます。

HAグループが高可用性を提供できるのは、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限ります。HAグループを作成する際は、必要なサービスを提供するノードの種類からインターフェースを追加してください。

- 管理ノード：ロードバランサーサービスを含め、グリッドマネージャーまたはテナントマネージャーへのアクセスを有効にします。
- ゲートウェイノード：ロードバランサーサービスを含めます。

HAグループの目的	このタイプのノードをHAグループに追加する
グリッドマネージャーへのアクセス	- 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はプライマリインターフェー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からのみ実行可能です。
テナントマネージャーのみがアクセス可能	プライマリまたは非プライマリの管理ノード
S3クライアントアクセス — ロードバランサーサービス	- 管理ノード - ゲートウェイノード
S3クライアントアクセス ("S3 Select")	- サービス機器 - 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 グループの使用を推奨しますが、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際の制限事項

Grid ManagerまたはTenant Managerサービスに障害が発生した場合、HAグループのフェイルオーバーはトリガーされません。

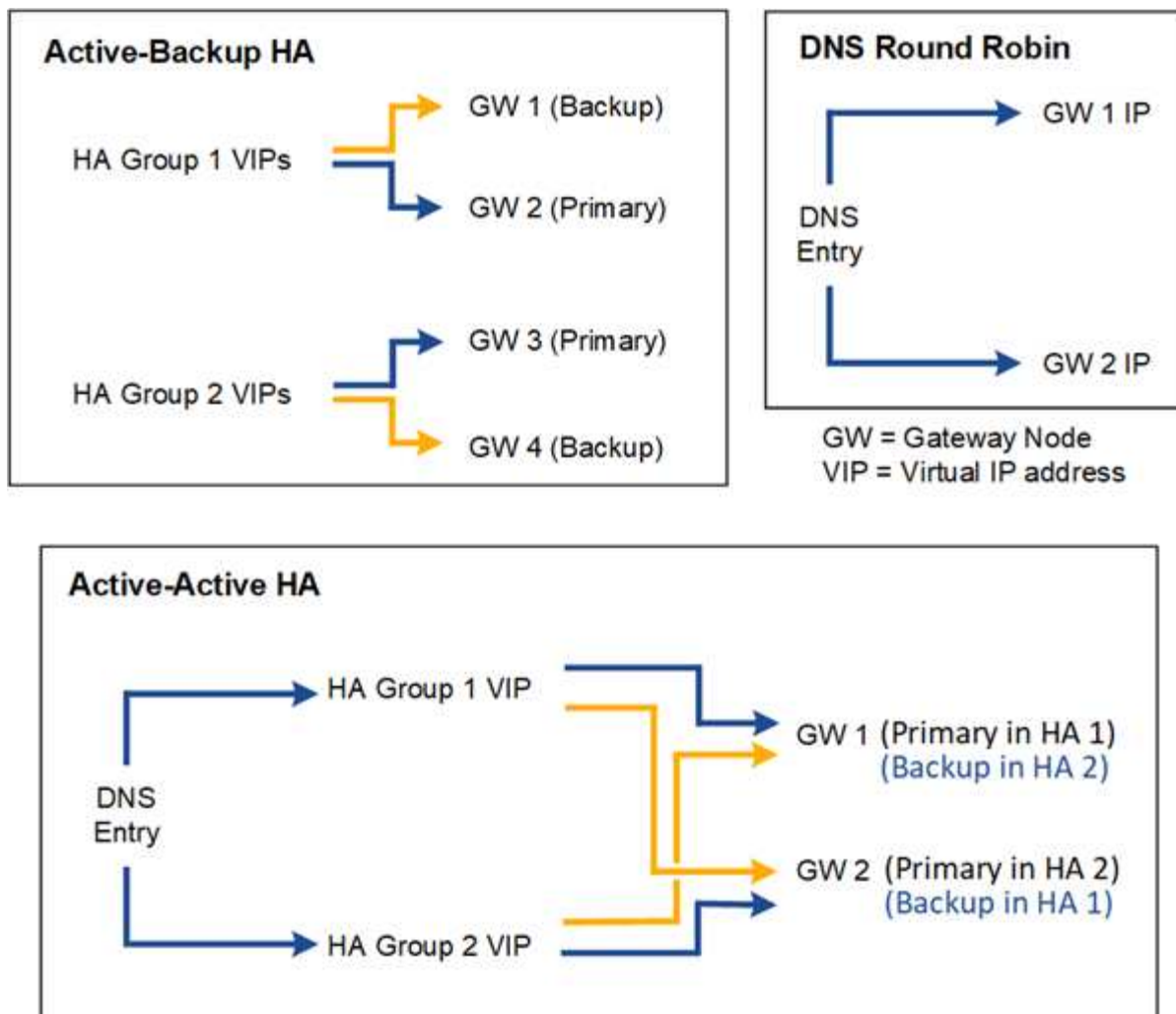
フェイルオーバーが発生した際に、グリッドマネージャーまたはテナントマネージャーにサインインしている場合、サインアウトされるため、作業を再開するには再度サインインする必要があります。

プライマリ管理ノードが利用できない場合、一部のメンテナンス手順は実行できません。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。

StorageGRID 高可用性グループの設定オプション

以下の図は、高可用性（HA）グループを構成するさまざまな方法の例を示しています。それぞれの選択肢には長所と短所があります。

図において、青色はHAグループ内のプライマリインターフェースを、黄色はHAグループ内のバックアップインターフェースを示します。



この表は、図に示されている各HA構成の利点をまとめたものです。

構成	利点	デメリット
アクティブ/バックアップHA	- StorageGRID によって管理され、外部依存関係はありません。 - 高速フェイルオーバー。	HAグループ内でアクティブなノードは1つだけです。HAグループごとに少なくとも1つのノードはアイドル状態になります。
DNSラウンドロビン	- 総処理能力の向上。 - アイドル状態のホストはありません。	- フェイルオーバーが遅い場合があり、クライアントの動作に依存する可能性があります。 - StorageGRID 外部のハードウェア構成が必要です。 - 顧客側で実施するヘルスチェックが必要です。

構成	利点	デメリット
アクティブ-アクティブHA	• トラフィックは複数のHAグループに分散されます。 • HAグループ数に応じて拡張可能な、高い総スループット。 • 高速フェイルオーバー。	• 設定がより複雑です。 • StorageGRID 外部のハードウェア構成が必要です。 • 顧客側で実施するヘルスチェックが必要です。

StorageGRIDで高可用性グループを設定する

高可用性（HA）グループを設定することで、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高可用性アクセスを提供できます。



StorageGRIDシステムには最大255個のHAグループを設定できます。

開始する前に

- ["対応ウェブブラウザ"](#) を使用して Grid Manager にサインインしています。
- あなたは["ルートアクセス権限"](#)があります。
- HAグループでVLANインターフェースを使用する予定がある場合は、VLANインターフェースを作成済みです。参照してください["VLANインターフェースを設定する"](#)。
- HAグループ内のノードにアクセスインターフェイスを使用する予定がある場合は、インターフェイスを作成済みです。
 - **Linux**（ノードをインストールする前）：["ノード設定ファイルを作成する"](#)
 - **Linux**（ノードのインストール後）：["ノードにトランクインターフェースまたはアクセスインターフェースを追加する"](#)
 - **VMware**（ノードのインストール後）：["ノードにトランクインターフェースまたはアクセスインターフェースを追加する"](#)



「Linux」とは、RHEL、Ubuntu、またはDebianのいずれかの環境を指します。サポートされているバージョンの一覧については、["NetApp Interoperability Matrix Tool \(IMT\)"](#)を参照してください。

高可用性グループを作成する

高可用性グループを作成する際には、1つまたは複数のインターフェースを選択し、それらを優先順位に従って整理します。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グループに含めるには、インターフェースはゲートウェイノードまたは管理ノードのものでなければなりません。HAグループは、特定のノードに対して1つのインターフェースしか使用できません。ただし、同じノードの他のインターフェースは、他のHAグループで使用できます。

ウィザードにアクセスする

手順

1. **Configuration > Network > High availability groups** 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てください

手順

1. HAグループに固有の名前を指定してください。
2. 必要に応じて、HAグループの説明を入力してください。
3. *続行*を選択します。

HAグループにインターフェースを追加する

手順

1. このHAグループに追加するインターフェースを1つ以上選択してください。

列ヘッダーを使用して行を並べ替えるか、検索語を入力してインターフェースをより迅速に検索してください。

Add interfaces to the HA group

Select one or more interfaces for this HA group. You can select only one interface for each node.



Total interface count: 4

	Node	Interface	Site	IPv4 subnet	Node type
☐	DC1-ADM1-104-96	eth0	DC1	10.96.104.0/22	Primary Admin Node
☐	DC1-ADM1-104-96	eth2	DC1	—	Primary Admin Node
☐	DC2-ADM1-104-103	eth0	DC2	10.96.104.0/22	Admin Node
☐	DC2-ADM1-104-103	eth2	DC2	—	Admin Node

0 interfaces selected

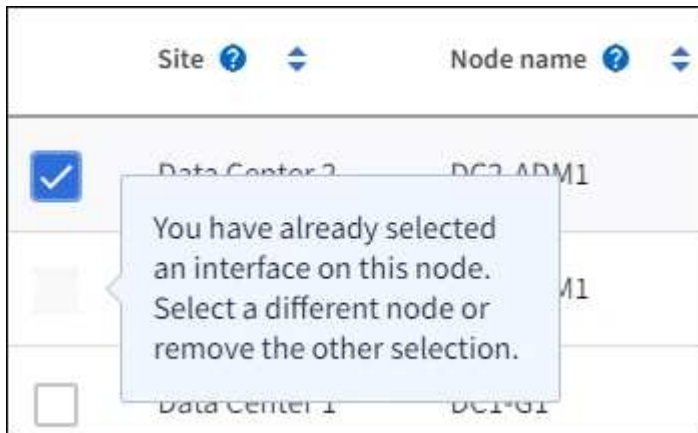


VLANインターフェースを作成した後、新しいインターフェースがテーブルに表示されるまで最大5分お待ちください。

インターフェース選択のためのガイドライン

- 少なくとも1つのインターフェースを選択する必要があります。
- ノードに対して選択できるインターフェースは1つだけです。
- HAグループが、Grid ManagerやTenant Managerを含む管理ノードサービスのHA保護を目的としている場合は、管理ノード上のインターフェースのみを選択してください。
- HAグループがS3クライアントトラフィックのHA保護を目的としている場合は、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ースを選択してください。

- 異なる種類のノード上のインターフェースを選択すると、情報メモが表示されます。フェイルオーバーが発生した場合、以前アクティブだったノードで提供されていたサービスが、新しくアクティブになったノードでは利用できなくなる可能性があることにご注意ください。例えば、バックアップゲートウェイノードでは、管理ノードサービスのHA保護を提供することはできません。同様に、バックアップ管理ノードは、プライマリ管理ノードが提供できるすべてのメンテナンス手順を実行できるわけではありません。
- インターフェー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。ツールチップにはより詳しい情報が表示されます。



- サブネット値またはゲートウェイが、既に選択されている他のインターフェースと競合する場合、そのインターフェースを選択することはできません。
- 静的IPアドレスが設定されていない設定済みインターフェースは選択できません。

2. *続行*を選択します。

優先順位を決定する

HAグループに複数のインターフェースが含まれている場合、プライマリインターフェースとバックアップ（フェイルオーバー）インターフェースを特定できます。プライマリインターフェースに障害が発生した場合、VIPアドレスは利用可能な最も優先度の高いインターフェースに移動します。そのインターフェースに障害が発生した場合、VIPアドレスは次に優先度の高い利用可能なインターフェースに移動し、以降も同様続きます。

手順

- 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ースとバックアップインターフェースを決定します。

リストの最初のインターフェースはプライマリインターフェースです。プライマリインターフェースは、障害が発生しない限りアクティブなインターフェースです。

Determine the priority order

Determine the primary interface and the backup (failover) interfaces for this HA group. Drag and drop rows or select the arrows.

Priority order ?	Node	Interface ?	Node type ?
1 (Primary interface)	⬆ DC1-ADM1-104-96	eth2	Primary Admin Node
2	⬆ DC2-ADM1-104-103	eth2	Admin Node



HAグループがGrid Managerへのアクセスを提供する場合、プライマリ管理ノード上のインターフェースをプライマリインターフェースとして選択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からのみ実行可能です。

2. *続行*を選択します。

IPアドレスを入力

手順

1. **[Subnet CIDR]** フィールドには、VIP サブネットを CIDR 表記で指定します。IPv4 アドレスの後にスラッシュとサブネット長 (0~32) を続けます。

ネットワークアドレスにはホストビットを設定しないでください。例えば、192.16.0.0/22。



32ビットの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とVIPアドレスの両方として機能します。

Enter details for the HA group

Subnet CIDR

Specify the subnet in CIDR notation. The optional gateway IP and all VIPs must be in this subnet.

IPv4 address followed by a slash and the subnet length (0-32)

Gateway IP address (optional)

Optionally specify the IP address of the gateway, which must be in the subnet. If the subnet address length is 32, the gateway IP address is automatically set to the subnet IP.

Virtual IP address

Specify at least 1 and no more than 10 virtual IPs for the HA group. All virtual IPs must be in the same subnet. If the subnet length is 32, only one VIP is allowed, which is automatically set to the subnet/gateway IP.

[Add another IP address](#)

- オプションとして、S3 の管理者クライアント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** を入力してください。ゲートウェイアドレスは VIP サブネット内に存在する必要があります。

クライアントユーザーと管理者ユーザーは、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。

- HAグループ内のアクティブなインターフェースに対して、少なくとも1つ、最大10個のVIPアドレスを入力してください。すべてのVIPアドレスはVIPサブネット内に存在し、アクティブなインターフェース上で同時にすべてアクティブになります。

少なくとも1つのIPv4アドレスを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。

- 「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ました。これで、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。

次の手順

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、ロードバランサー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、必要な証明書を添付してください。["ロードバランサーのエンドポイントを設定する"](#)を参照してください。

高可用性グループを編集する

高可用性（HA）グループを編集して、名前や説明の変更、インターフェースの追加または削除、優先順位の変更、仮想 IP アドレスの追加または更新を行うことができます。

たとえば、サイトまたはノードの廃止手順において、選択したインターフェイスに関連付けられたノードを削除する場合は、HA グループを編集する必要があります。

手順

1. **Configuration > Network > High availability groups** を選択します。

高可用性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. 更新したい内容に応じて、以下のいずれかの操作を行ってください。
 - VIPアドレスを追加または削除するには、アクション > 仮想IPアドレスの編集 を選択します。
 - グループ名や説明の更新、インターフェイスの追加や削除、優先順位の変更、VIP アドレスの追加や削除を行うには、「アクション」 > 「HA グループの編集」を選択します。
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 * を選択します。
 - c. **Finish** 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、グループ名または説明を更新してください。
 - b. 必要に応じて、チェックボックスを選択または解除して、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、プライマリ管理ノード上のインターフェイスを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。一部のメンテナンス手順は、プライマリ管理ノードからのみ実行できます。

- 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」を選択し、次に「完了」を選択します。

高可用性グループを削除する

高可用性 (HA) グループは、一度に1つまたは複数削除できます。



ロード バランサーの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 バランサー エンドポイントから削除する必要があります。

クライアントのサービス中断を防ぐため、HAグループを削除する前に、影響を受けるS3クライアントアプリケーションをすべて更新してください。各クライアントが別のIPアドレスを使用して接続するように更新します。たとえば、別のHAグループの仮想IPアドレス、またはインストール時にインターフェイス用に設定されたIPアドレスなどです。

手順

1. **Configuration > Network > High availability groups** を選択します。
2. 削除する各 HA グループの「ロード バランサー エンドポイント」列を確認してください。ロード バランサー エンドポイントが表示されている場合：
 - a. **Configuration > Network > Load balancer endpoints** に移動します。
 - b. エンドポイントのチェックボックスを選択します。
 - c. **Actions > Edit endpoint binding mode** を選択します。
 - d. HAグループを削除するようにバインディングモードを更新します。
 - e. **変更を保存** を選択します。
3. ロード バランシングのエンドポイントが表示されていない場合は、削除する HA グループごとにチェックボックスを選択してください。
4. **Actions > Remove HA group** を選択します。
5. メッセージを確認し、**Delete HA group** を選択して選択を確定してください。

選択したすべてのHAグループが削除されます。高可用性グループのページに、緑色の成功バナーが表示されます。

ロード バランシングの管理

StorageGRID ロード バランシングについて学ぶ

ロード バランシングを使用して、S3クライアントからの取り込みおよび取得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 システムにデータを保存または取得する場合、StorageGRID はロードバランサーを使用して、データの取り込みと取得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させることで、速度と接続容量を最大化します。

StorageGRID ロード バランシング 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、レイヤー7のロード バランシングを提供します。クライアントからのリクエストに対してトランスポート層セキュリティ (TLS) による終端処理を行い、リクエストを検査し、ストレージノードへの新たな安全な接続を確立します。

各ノード上のロード バランシングサービスは、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、それぞれ独立して動作します。ロード バランシングサービスは、重み付け処理を通じて、CPUの可用性が高いストレージノードに多くのリクエストをルーティングします。



StorageGRID ロード バランシング サービスは推奨されるロード バランシング メカニズムですが、代わりにサードパーティ製のロード バランサを統合することもできます。詳細については、NetApp アカウント担当者にお問い合わせいただくか、["StorageGRIDでサードパーティのロード バランシングを使用する"](#)を参照してください。

ロード バランシング ノードはいくつ必要ですか？

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は、ロード バランシングサービス

を備えたノードが2つ以上含まれている必要があります。例えば、サイトには2つのゲートウェイノードが含まれる場合もあれば、管理ノードとゲートウェイノードの両方が含まれる場合もあります。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場合でも、各ロードバランシングノードに十分なネットワーク、ハードウェア、または仮想化インフラストラクチャが備わっていることを確認してください。

ロードバランサーのエンドポイントとは何ですか？

ロードバランサーエンドポイントは、ロードバランサーサービスを含むノードへのアクセスに使用される、受信および送信クライアントアプリケーション要求の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、クライアントの種類（S3）、バインディングモード、およびオプションで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。

ロードバランサーエンドポイントを作成するには、Grid Manager を使用するか、S3 セットアップおよびFabricPool ウィザードを完了してください：

- ["ロードバランサーのエンドポイントを設定する"](#)
- ["S3 セットアップ ウィザードを使用する"](#)
- ["FabricPool セットアップ ウィザードを使用する"](#)

ロードバランサーのキャッシングに関する考慮事項

ワークロードがデータの一部に対して動作し、オブジェクトに複数回アクセスする場合、キャッシングはパフォーマンスを大幅に向上させます。さらに、キャッシング機能により、完全なグリッド環境を構築することなく、オブジェクトストレージへのリモートアクセスが可能になります。ロードバランサーのキャッシュ機能は、ゲートウェイノードでのみ利用可能です。

ロードバランサーのエンドポイントを作成する際は、以下の点に注意してください。

- キャッシュ可能なワークロードに対してのみキャッシュを有効にしてください。キャッシュされたデータよりもキャッシュされていないデータにアクセスする頻度が高いワークロードは、キャッシュによる処理が行われなかった場合よりもパフォーマンスが低下します。場合によっては、上書きや削除の頻度が高いワークロードでは、保証されているドライブの書き込み耐久性を超える可能性もあります。
- キャッシュに適した個々のワークロードについては、キャッシュ用のエンドポイントまたはノードを追加することを検討してください。
- キャッシュ可能なワークロードとキャッシュ不可能なワークロードには、それぞれ異なるエンドポイントを使用してください。この分離により、キャッシュメカニズムが適切に適用され、キャッシュ不可能なデータ処理に干渉しないことが保証されます。
- 潜在的なキャッシュ可能なワークロードをキャッシュ対応エンドポイントに振り分けることで評価します。キャッシュ ヒット率を監視および検証し、ワークロードがキャッシュに適しているかどうかを判断します。この評価は、パフォーマンスの最適化とキャッシュリソースの効率的な利用を確保するのに役立ちます。
- ["監査ログを確認する"](#)既存のワークロードがキャッシュに適しているかどうかを判断します。指定された期間において、GETリクエストのうち、一意のオブジェクトに対するリクエストが何パーセントを占めるかを確認します。キャッシュに適するためには、この値が50%未満である必要があります。

キャッシュに適したワークロードの例

- データレイク

- 高性能コンピューティング（HPC）
- AI/MLトレーニング
- コンテンツ配信ネットワーク（CDN）
- メディア資産管理
- ビデオ制作



- 複数のオブジェクトバージョンをキャッシュできます。
- 範囲読み取り操作がサポートされています。

キャッシュに適さないワークロードの例

- Fabric Pool
- バックアップアプリケーション
- ストレージ階層化



キャッシュによって提供されるコンテンツが保存時に暗号化を必要とする場合、"[ノードまたはドライブの暗号化を有効にする](#)"キャッシュノード上で行います。

キャッシュされないオブジェクトの種類とリクエスト

- ``response-content-encoding`` クエリパラメータ
- ``partNumber`` クエリパラメータ
- 条件付きヘッダー
 - If-Match
 - If-Modified-Since
 - If-None-Match
 - If-Unmodified-Since
- 保存時に以下のいずれかの方法で暗号化されたリクエスト：
 - SSE（StorageGRID が管理するキーを使用したサーバー側暗号化）
 - SSE-C（顧客提供の鍵を使用したサーバー側暗号化）
 - 保存オブジェクトの暗号化

キャッシュされていないリクエストは、キャッシュが有効になっていない場合と同様に、アップストリームのLDRに転送されます。

関連情報

- "[ロード バランシングのキャッシングのトラブルシューティング](#)"
- ロードバランサーのキャッシングに関する詳細については、テクニカルサポートにお問い合わせください。

ポートに関する考慮事項

ロードバランサーの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場合、デフォルトで10433になりますが、1から65535までの未使用の外部ポートを指定できます。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ー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上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、各エンドポイント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ていません。["StorageGRID内部ポート"](#)を参照してください。

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 間の接続には、トランスポート層セキュリティ (TLS) 暗号化を使用する必要があります。TLS 暗号化なしで 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 ロードバランサー エンドポイントのネットワーク プロトコルを選択する際は、「HTTPS」を選択してください。

ロードバランサーのエンドポイント証明書に関する考慮事項

ロードバランサー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提供する必要があります。ロードバランサーエンドポイントを作成する際には、以下の3つのオプションのいずれかを使用できます。

- *署名済みの証明書をアップロードします (推奨)。*この証明書は、公的に信頼された認証局 (CA) またはプライベート認証局 (CA) のいずれかによって署名できます。接続を保護するために、公的に信頼された CA サーバー証明書を使用することがベストプラクティスです。生成された証明書とは異なり、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るため、有効期限切れの問題を回避するのに役立ちます。

ロードバランサーのエンドポイントを作成する前に、以下のファイル入手する必要があります。

- カスタムサーバー証明書ファイル。
- カスタムサーバー証明書の秘密鍵ファイル。
- オプションとして、各中間発行認証局からの証明書をまとめた CA バンドル。
- 自己署名証明書を生成します。
- グローバル **StorageGRID S3** 証明書を使用する。ロードバランサーのエンドポイントにこの証明書を選択するには、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。参照してください ["S3 API証明書の設定"](#)。

必要な値は何ですか？

証明書を作成するには、S3クライアントアプリケーションがエンドポイントにアクセスするため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を含める必要があります。例：


```
Subject DN:
/C=Country/ST=State/O=Company, Inc./CN=s3.storagegrid.example.com
```

必要に応じて、証明書はワイルドカードを使用して、ロードバランサー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。例えば、

*.storagegrid.example.com は * ワイルドカードを使用して、adm1.storagegrid.example.com および gn1.storagegrid.example.com を表します。

S3仮想ホスト型リクエストを使用する予定の場合は、証明書には、設定済みの各"**S3エンドポイントドメイン名**"の*代替名*エントリも含まれている必要があります（ワイルドカード名を含む）。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、"[サーバー証明書のセキュリティ強化ガイドライン](#)"を確認してください。

セキュリティ証明書に記載されている各名前に対して、DNSエントリを定義する必要もあります。

有効期限切れの証明書はどのように管理すればよいですか？



S3 アプリケーションと StorageGRID 間の接続を保護するために使用される証明書の有効期限が切れると、アプリケーションは一時的に StorageGRID へのアクセスを失う可能性があります。

証明書の有効期限切れの問題を回避するには、以下のベストプラクティスに従ってください：

- 「ロードバランサーエンドポイント証明書の有効期限切れ」や「S3 API のグローバルサーバー証明書の有効期限切れ」などの、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を注意深く監視してください。
- StorageGRID と S3 アプリケーションの証明書のバージョンは、常に同期を保つ必要があります。ロードバランサーのエンドポイントで使用されてい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ている同等の証明書も交換または更新する必要があります。
- 公開署名付きの認証局証明書を使用してください。CA によって署名された証明書を使用すれば、有効期限が近づいている証明書を無停止で交換できます。
- 自己署名の StorageGRID 証明書を生成済みで、その証明書の有効期限が近づいている場合は、既存の証明書が期限切れになる前に、StorageGRID と S3 アプリケーションの両方で証明書を手動で交換する必要があります。

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、ロードバランサーのエンドポイントにアクセスするために使用できる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完全修飾ドメイン名（FQDN）を使用した場合にのみ、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。

以下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。エンドポイントへのアクセスを制限する必要がない限り、この設定を使用してください。
- ・HAグループの仮想IPアドレス。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ース。クライアントは、選択したノードインターフェースの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。選択したノードの種類に応じて、クライアントは、いずれかの管理ノードのIPアドレス（または対応するFQDN）または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。

テナントのアクセスに関する考慮事項

テナントアクセスは、どの StorageGRID テナントアカウントがロードバランサーエンドポイントを使用してバケットにアクセスできるかを制御できるオプションのセキュリティ機能です。すべてのテナントがエンドポイントにアクセスできるように設定することも（デフォルト）、エンドポイントごとにアクセスを許可するテナントまたはアクセスをブロックするテナントのリストを指定することもできます。

この機能を利用することで、テナントとそのエンドポイント間のセキュリティ分離を向上させることができます。例えば、この機能を使用することで、あるテナントが所有する極秘情報や高度に機密性の高い資料が、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、テナントはクライアント要求で使用されたアクセスキーから決定されます。要求の一部としてアクセスキーが提供されない場合（匿名アクセスの場合など）、バケットの所有者がテナントを特定するために使用されます。

テナントアクセス例

このセキュリティ機能の動作を理解するために、次の例を考えてみましょう。

1. 以下のように、2つのロードバランサーエンドポイントを作成しました。
 - ・*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。
 - ・*極秘*エンドポイント：ポート10444を使用し、*極秘*テナントのみに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ています。
2. `top-secret.pdf` は、**Top secret** テナントが所有するバケットに含まれています。

`top-secret.pdf` にアクセスするには、*極秘*テナントのユーザーが
 `https://w.x.y.z:10444/top-secret.pdf` に
 GET リクエストを発行します。このテナントは10444エンドポイントの使用を許可されているため、ユーザー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ーが同じURLに対して同じリクエストを発行した場合、即座にアクセス拒否メッセージが表示されます。認証情報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

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ーサービスは、S3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。ロードバランサーサービスは、重み付け処理を通じて、CPU可用性の高いストレージノードに多くのリクエストを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、重み付けはより頻繁に更新される場合があります。すべてのストレージノードには、たとえノードが100%の利用率を報告した場合でも、あるいは利用率を報告しなかった場合でも、最小限の基本重み値が割り当てられます。

場合によっては、CPUの可用性に関する情報は、ロードバランサーサービスが設置されているサイトに限定されます。

StorageGRIDロード バランサ エンドポイントを設定します

ロード バランシングのエンドポイントは、S3 クライアントがゲートウェイノードと管理ノード上の StorageGRID ロードバランサーに接続する際に使用できるポートとネットワーク プロトコルを決定します。エンドポイントを使用して、グリッドマネージャー、テナントマネージャー、またはその両方にアクセスすることもできます。

開始する前に

- ["対応ウェブブラウザ"](#) を使用して Grid Manager にサインインしています。
- あなたは["ルートアクセス権限"](#)があります。
- ["ロード バランシングに関する考慮事項"](#)をレビューしました。
- 以前にロード バランシング エンドポイントに使用する予定のポートを再マッピングした場合は、["ポート リマップを削除しました"](#)。
- 使用予定の高可用性 (HA) グループをすべて作成しました。HAグループは推奨されますが、必須ではありません。["高可用性グループを管理する"](#)を参照してください。
- ロード バランシングエンドポイントが["S3 Select 用の S3 テナント"](#)によって使用される場合、ベアメタルノードのIPアドレスまたはFQDNを使用してはなりません。S3 Selectに使用されるロード バランシングエンドポイントには、サービスアプライアンスとVMwareベースのソフトウェアノードのみが許可されています。
- 使用予定のVLANインターフェースはすべて設定済みです。["VLANインターフェースを設定する"](#)を参照してください。
- HTTPSエンドポイントを作成する場合（推奨）、サーバー証明書情報はすでに用意されています。



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は、最大15分かかる場合があります。

- 証明書をアップロードするには、サーバー証明書、証明書の秘密鍵、そして必要に応じて CA バンドルが必要です。
- 証明書を生成するには、S3クライアントがエンドポイントにアクセスするため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、サブジェクト（識別名）についても把握しておく必要があります。
- StorageGRID S3 API証明書（ストレージノードへの直接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認証局によって署名されたカスタム証明書に既に置き換えています。["S3 API証明書の設定"](#)を参照してください。

ロード バランシング エンドポイントを作成する

各 S3 クライアント ロード バランシング エンドポイントは、ポート、クライアント タイプ（S3）、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。管理インターフェイスのロード バランシング エンドポイントは、ポート、インターフェイス タイプ、および信頼されていないクライアント ネットワークを指定します。

ウィザードにアクセスする

手順

1. 設定 > ネットワーク > ロード バランシング エンドポイント を選択します。
2. S3クライアントのエンドポイントを作成するには、「S3クライアント」タブを選択します。
3. グリッドマネージャ、テナントマネージャ、またはその両方にアクセスするためのエンドポイントを作成するには、「管理インターフェイス」タブを選択します。
4. *Create*を選択します。

エンドポイントの詳細を入力してください

手順

1. 作成するエンドポイントの種類に応じて、適切な手順を選択して詳細を入力してください。

S3クライアント

フィールド	説明
Name	ロード バランシングエンドポイントページの表に表示される、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。このフィールドには、最初に作成するエンドポイントの場合、デフォルトで 10433 が設定されていますが、1 から 65535 までの未使用の外部ポート番号を入力できます。 80 または 8443 を入力した場合、ポート 8443 を解放していない限り、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。その場合、ポート 8443 を S3 エンドポイントとして使用でき、そのポートはゲートウェイ ノードと管理ノードの両方で設定されます。
クライアントタイプ	*S3*である必要があります。
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際に使用するネットワーク プロトコルです。 • 安全な TLS 暗号化通信には、HTTPS を選択してください（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添付する必要があります。 • セキュリティレベルが低く、暗号化されていない通信の場合は、HTTP を選択してください。HTTP は非本番環境のグリッドでのみ使用してください。
キャッシュを有効にする	このロード バランシング エンドポイントに対して "ゲートウェイノードでのキャッシング" を有効または無効にします。 キャッシュに問題が発生した場合は、"ロード バランシングのキャッシングのトラブルシューティング"を参照してください。

管理インターフェイス

フィールド	説明
Name	ロード バランシングエンドポイントページの表に表示される、エンドポイントのわかりやすい名前。

フィールド	説明
ポート	StorageGRID の Grid Manager、Tenant Manager、またはその両方にアクセスするために使用するポート。 • Grid Manager : 8443 • テナントマネージャー : 9443 • グリッドマネージャーとテナントマネージャーの両方 : 443 注: これらのプリセットポート、またはその他の利用可能なポートを使用できます。
インターフェイス タイプ	このエンドポイントを使用してアクセスする StorageGRID インターフェースのラジオボタンを選択してください。
信頼できないクライアントネットワーク	このエンドポイントを信頼できないクライアントネットワークからアクセス可能にする場合は、「はい」を選択してください。それ以外の場合は、「いいえ」を選択してください。 「はい」を選択すると、信頼されていないすべてのクライアントネットワークでポートが開きます。 注: ポートを信頼できないクライアント ネットワークに対して開くか閉じるかを設定できるのは、ロード バランシング エンドポイントを作成するときのみです。

1. *続行*を選択します。

バインディングモードを選択してください

手順

1. エンドポイントへのアクセス方法を制御するために、エンドポイントのバインディングモードを選択します。任意の IP アドレスを使用するか、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するかを指定できます。

一部のバインディングモードは、クライアントエンドポイントまたは管理インターフェイス エンドポイントのいずれかで使用できます。両方のエンドポイントタイプのすべてのモードがここに一覧表示されています。

モード	説明
グローバル（クライアントエンドポイントのデフォルト）	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へのアクセスを制限する必要がない限り、Global 設定を使用してください。

モード	説明
HAグループの仮想IPアドレス	クライアントはこのエンドポイントにアクセスするために、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。 このバインディングモードを使用するエンドポイントは、エンドポイントに選択した HA グループが重複しない限り、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ース	クライアントは、このエンドポイントにアクセスするために、選択したノードインターフェースの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（クライアントエンドポイントのみ）	選択したノードの種類に応じて、クライアントはこのエンドポイントにアクセスするために、管理ノードのIPアドレス（または対応するFQDN）か、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。
すべての管理ノード（管理インターフェイス エンドポイントのデフォルト）	クライアントは、このエンドポイントにアクセスするために、いずれかの管理ノードの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 は使用するエンドポイントを決定するために次の優先順位を使用します：**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**。

管理インターフェイス エンドポイントを作成する場合、管理ノードのみが許可されます。

2. **HAグループの仮想IP** を選択した場合は、1つ以上のHAグループを選択してください。

管理インターフェイス エンドポイントを作成する場合は、管理ノードのみに関連付けられている VIP 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各管理ノードまたはゲートウェイ ノードに対して、1つ以上のノード インターフェイスを選択してください。
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プライマリ以外の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てください。

テナントのアクセスを制御する



管理インターフェイス エンドポイントは、エンドポイントに **テナントマネージャーの管理インターフェイスタイプ** がある場合にのみ、テナントアクセスを制御できます。

手順

1. 「テナント アクセス」の手順では、以下のいずれかを選択してください。

フィールド	説明
すべてのテナントを許可する（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後、ロードバランシングの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することができます。
選択されたテナントを許可する	選択されたテナントアカウントのみが、このエンドポイントを使用して自身のバケットにアクセスできます。
選択したテナントをブロックする	選択され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は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。作成 を選択して、新しいロード バランシング エンドポイントを追加します。次に、[終了後の操作](#)に移動します。それ以外の場合は、**続行** を選択して証明書を添付します。

証明書を添付する

手順

1. **HTTPS** エンドポイントを作成する場合は、エンドポイントに添付するセキュリティ証明書の種類を選択してください。

この証明書は、S3クライアントと、Admin NodeまたはGateway Node上のLoad Balancerサービスとの間の接続を保護します。

- 証明書をアップロード。カスタム証明書をアップロードする場合は、このオプションを選択してください。
- 証明書を生成します。カスタム証明書を生成するために必要な値が揃っている場合は、このオプションを選択してください。
- **StorageGRID S3** 証明書を使用する。グローバル S3 API 証明書を使用する場合は、このオプションを選択してください。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。

このオプションを選択するには、グリッドCAによって署名されたデフォルトのS3 API証明書を、外部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必要があります。["S3 API証明書の設定"](#)を参照してください。

- 管理インターフェイス証明書を使用する。グローバル管理インターフェイス証明書を使用する場合は、このオプションを選択してください。この証明書は、管理ノードへの直接接続にも使用できます。
2. StorageGRID S3証明書を使用していない場合は、証明書をアップロードするか、生成してください。

証明書をアップロード

- a. 「証明書をアップロード」を選択します。
- b. 必要なサーバー証明書ファイルをアップロードします。
 - サーバー証明書: PEM形式のカスタムサーバー証明書ファイル。
 - 証明書の秘密鍵: カスタムサーバー証明書の秘密鍵ファイル(.key)。



ECの秘密鍵は224ビット以上である必要があります。RSA秘密鍵は2048ビット以上である必要があります。

- **CA バンドル**: 各中間発行認証局 (CA) からの証明書を含む単一のオプションファイル。ファイルには、PEM 形式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されて含まれている必要があります。
- c. *証明書の詳細*を展開すると、アップロードした各証明書のメタデータが表示されます。オプションの CA バンドルをアップロードした場合、各証明書はそれぞれ別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、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」を選択してください。

証明書ファイル名とダウンロード場所を指定してください。拡張子`.pem`を付けてファイルを保存します。

例: `storagegrid_certificate.pem`

- 証明書の内容をコピーして別の場所に貼り付けるには、*証明書のPEMをコピー*または*CA バンドルのPEMをコピー*を選択してください。
- d. 「作成」を選択します。+ ロード バランシング エンドポイントが作成されます。カスタム証明書は、S3 クライアントまたは管理インターフェイスとエンドポイント間のその後のすべての新しい接続に使用されます。

証明書を生成する

- 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IPアドレスを1つ以上指定します。
件名 (任意)	証明書所有者の X.509 サブジェクトまたは識別名 (DN) 。 このフィールドに値が入力されない場合、生成される証明書は最初のドメイン名またはIPアドレスをサブジェクト共通名 (CN) として使用します。

フィールド	説明
有効日数	証明書が発行されてから有効期限が切れるまでの日数。
キー使用拡張機能を追加する	選択した場合（デフォルトかつ推奨）、鍵使用法と拡張鍵使用法の拡張機能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、証明書に含まれる鍵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は選択したままにしてください。

c. *Generate* 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*を選択してください。

- 証明書ファイルを保存するには、*証明書をダウンロード*を選択してください。

証明書ファイル名とダウンロード場所を指定してください。拡張子`.pem`を付けてファイルを保存します。

例: `storagegrid_certificate.pem`

- 証明書の内容をコピーして別の場所に貼り付けるには、*証明書のPEMをコピー*を選択してください。

e. *Create*を選択します。

ロードバランサーのエンドポイントが作成されました。カスタム証明書は、S3 クライアントまたは管理インターフェイスとこのエンドポイント間のその後のすべての新しい接続に使用されます。

終了後の操作

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てください。

DNSレコードに入力するIPアドレスは、ロードバランシングノードの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グループを設定している場合、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グループを使用していない場合、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 ロードバランサーサービスに接続します。

また、DNSレコードには、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が参照されていることを確認する必要があります。

2. S3クライアントがエンドポイントに接続するために必要な情報を提供します。

- 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

ロードバランサーのエンドポイントを表示および編集する

既存のロードバランサーエンドポイントの詳細（セキュリティ保護されたエンドポイントの証明書メタデータを含む）を表示できます。エンドポイントの特定の設定を変更できます。

- すべてのロードバランサーエンドポイントの基本情報を確認するには、ロードバランサーエンドポイントページの表を参照してください。
- 証明書のメタデータを含む、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、表でエンドポイントの名前を選択してください。表示される情報は、エンドポイントの種類と設定方法によって異なります。

S3 load balancer endpoint

Port:	10443
Client type:	S3
Network protocol:	HTTPS
Binding mode:	Global
Endpoint ID:	3d02c126-9437-478c-8b24-08384401d3cb

Remove

Binding mode

Certificate

Tenant access (2 allowed)

You can select a different binding mode or change IP addresses for the current binding mode.

Edit binding mode

Binding mode: Global



This endpoint uses the Global binding mode. Unless there are one or more overriding endpoints for the same port, clients can access this endpoint using the IP address of any Gateway Node, any Admin Node, or the virtual IP of any HA group on any network.

- エンドポイントを編集するには、ロードバランサーのエンドポイントページにある「アクション」メニューを使用します。



管理インターフェイス エンドポイントのポートを編集中に Grid Manager へのアクセスを失った場合は、URL とポートを更新してアクセスを回復してください。



エンドポイントを編集した後、変更内容がすべてのノードに反映されるまで最大 15 分待つ必要がある場合があります。

Task	[操作]メニュー	詳細ページ
エンドポイント名を編集	a. エンドポイントのチェックボックスを選択します。 b. Actions > Edit endpoint name を選択します。 c. 新しい名前を入力してください。 d. * 保存 * を選択します。	a. 詳細を表示するには、エンドポイント名を選択してください。 b. 編集アイコン  を選択します。 c. 新しい名前を入力してください。 d. * 保存 * を選択します。
エンドポイントポートを編集	a. エンドポイントのチェックボックスを選択します。 b. Actions > Edit endpoint port を選択します。 c. 有効なポート番号を入力してください。 d. * 保存 * を選択します。	該当なし
エンドポイントバインディングモードを編集	a. エンドポイントのチェックボックスを選択します。 b. Actions > Edit endpoint binding mode を選択します。 c. 必要に応じてバインディングモードを更新してください。 d. 変更を保存 を選択します。	a. 詳細を表示するには、エンドポイント名を選択してください。 b. 「バインディングモードの編集」を選択します。 c. 必要に応じてバインディングモードを更新してください。 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する	a. エンドポイントのチェックボックスを選択します。 b. Actions > 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 S3 証明書の使用を開始してください。 d. 変更を保存 を選択します。	a. 詳細を表示するには、エンドポイント名を選択してください。 b. 「Certificate」タブを選択してください。 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 S3 証明書の使用を開始してください。 e. 変更を保存 を選択します。

Task	[操作]メニュー	詳細ページ
テナントアクセスを編集する	a. エンドポイントのチェックボックスを選択します。 b. Actions > テナントアクセスを編集を選択します。 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、あるいはその両方を実行してください。 d. 変更を保存 を選択します。	a. 詳細を表示するには、エンドポイント名を選択してください。 b. 「テナントアクセス」タブを選択します。 c. 「テナントアクセスを編集」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、あるいはその両方を実行してください。 e. 変更を保存 を選択します。

ロードバランサーエンドポイントの削除

Actions メニューを使用して1つまたは複数のエンドポイントを削除することも、詳細ページから単一のエンドポイントを削除することもできます。



クライアントのサービス中断を防ぐため、ロードバランサーのエンドポイントを削除する前に、影響を受けるS3クライアントアプリケーションをすべて更新してください。各クライアントが、別のロードバランサー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するように更新してください。必要な証明書情報も必ず更新してください。



管理インターフェイス エンドポイントの削除中に Grid Manager へのアクセスを失った場合は、URL を更新してください。

- 1つ以上のエンドポイントを削除するには：
 - a. ロードバランサーのページから、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. **Actions** > **Remove** を選択します。
 - c. 「OK」を選択します。
- 詳細ページからエンドポイントを1つ削除するには：
 - a. ロードバランサーのページから、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。

StorageGRIDでS3エンドポイントドメイン名を設定する

S3仮想ホスト型リクエストをサポートするには、Grid Managerを使用して、S3クライアントが接続するS3エンドポイント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サポートされていません。今後のリリースでは、この設定は使用できなくなります。

開始する前に

- "対応ウェブブラウザ" を使用して Grid Manager にサインインしています。
- "特定のアクセス権限"があります。
- グリッドのアップグレード作業は実施されていないことを確認済みです。



グリッドのアップグレードが進行中は、ドメイン名の設定を変更しないでください。

タスク概要

クライアントが S3 エンドポイントドメイン名を使用できるようにするには、以下のすべてを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。
- 必ず"**クライアントが StorageGRID への HTTPS 接続に使用する証明書**"が、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ることを確認してください。

例えば、エンドポイントが `s3.company.com` の場合、HTTPS 接続に使用される証明書には、`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` が含まれていることを確認する必要があります。

- 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 レコードを含め、レコードがワイルドカード名を含む必要なすべての S3 エンドポイントドメイン名を参照していることを確認してください。



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、高可用性グループの仮想 IP アドレスに接続することで、StorageGRID に接続できます。クライアントアプリケーションがグリッドに接続する仕組みを理解し、DNS レコードに正しい IP アドレスを含めるようにしてください。

グリッドへの接続に HTTPS 接続（推奨）を使用するクライアントは、以下のいずれかの証明書を使用できます。

- ロードバランサーの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専用のカスタム証明書を使用できます。各ロードバランサーのエンドポイントは、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。
- ロードバランサーのエンドポイ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、グローバル S3 API 証明書をカスタマイズして、必要なすべての S3 エンドポイントドメイン名を含めることができます。



S3 エンドポイントのドメイン名を追加せず、リストが空の場合、S3 仮想ホスト型リクエストのサポートは無効になります。

S3 エンドポイントドメイン名を追加する

手順

1. [設定] > [ネットワーク] > [S3 エンドポイントドメイン名] を選択します。
2. 「ドメイン名 1」フィールドにドメイン名を入力します。「別のドメイン名を追加」を選択して、ドメイン名を追加します。

3. * 保存 * 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てください。
 - 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ーエンドポイントに接続する場合、"[エンドポイントに関連付けられている証明書を更新する](#)"。
 - クライアントがグローバル S3 API 証明書を使用するロード バランサー エンドポイントまたはストレージ ノードに直接接続する場合、"[グローバルS3 API証明書を更新する](#)"。
5. エンドポイントのドメイン名要求が解決できるように、必要な DNS レコードを追加します。

結果

クライアントがエンドポイントを使用する場合 `bucket.s3.company.com`、DNS サーバーは正しいエンドポイントに解決され、証明書は期待どおりに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する

S3アプリケーションで使用される名前を変更すると、仮想ホスト型のリクエストは失敗します。

手順

1. [設定] > [ネットワーク] > [S3エンドポイントドメイン名] を選択します。
2. 編集したいドメイン名フィールドを選択し、必要な変更を行ってください。
3. * 保存 * を選択します。
4. 変更を確定するには「はい」を選択してください。

S3エンドポイントドメイン名の削除

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、仮想ホスト型のリクエストは失敗します。

手順

1. [設定] > [ネットワーク] > [S3エンドポイントドメイン名] を選択します。
2. ドメイン名の横にある削除アイコン  を選択します。
3. 削除を確定するには「はい」を選択してください。

関連情報

- "[S3 REST APIを使用する](#)"
- "[IPアドレスを表示する](#)"
- "[高可用性グループを構成する](#)"

StorageGRIDクライアント接続のIPアドレスとポート

オブジェクトを保存または取得するために、S3クライアントアプリケーションは、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ーサービス、またはすべてのストレージノードに含まれているローカルディストリビューションルーター (LDR) 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。オプションとして、仮想IP（VIP）アドレスを使用する高可用性接続を提供するために、ロードバランシングノードの高可用性（HA）グループを作成できます。IPアドレスや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。

この表は、クライアントが StorageGRID に接続できるさまざまな方法と、各接続タイプで使用する IP アドレスおよびポートをまとめたものです。ロードバランサーエンドポイントと高可用性（HA）グループを既に作成している場合は、[IPアドレスを見つける場所](#)を参照して、Grid Manager でこれらの値を確認してください。

接続が行われる場所	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	ロードバランサー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	ロードバランサー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	ロードバランサー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

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ーエンドポイントに接続するには、以下に示すような構造のURLを使用します。

`https://VIP-of-HA-group:LB-endpoint-port`

例えば、HAグループの仮想IPアドレスが192.0.2.5で、ロードバランサー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アドレスを見つける場所

1. グリッドマネージャーに["対応ウェブブラウザ"](#)を使用してサインインします。
2. グリッドノードのIPアドレスを確認するには：
 - a. * Nodes * を選択します。
 - b. 接続先の管理ノード、ゲートウェイノード、またはストレージノードを選択してください。

- c. * Overview *タブを選択します。
- d. ノード情報セクションで、ノードのIPアドレスをメモしてください。
- e. IPv6アドレスとインターフェースのマッピングを表示するには、*詳細を表示*を選択してください。

クライアントアプリケーションから、リストにある任意のIPアドレスに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)



管理ノードまたはゲートウェイノードを表示していて、それが高可用性グループのアクティブノードである場合、HAグループの仮想IPアドレスがeth2に表示されます。

- 3. 高可用性グループの仮想IPアドレスを確認するには：
 - a. **Configuration > Network > High availability groups** を選択します。
 - b. 表で、HAグループの仮想IPアドレスを確認します。
- 4. ロードバランサーのエンドポイントのポート番号を調べるには：
 - a. **設定 > ネットワーク > ロード バランシング エンドポイント** を選択します。
 - b. 使用したいエンドポイントのポート番号をメモしておいてください。



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構成されます。これは、これらのポートが管理ノードで予約されているためです。その他のポートはすべて、ゲートウェイノードと管理ノードの両方で設定されます。

- c. 表からエンドポイントの名前を選択してください。
- d. クライアントタイプ (S3) 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てください。

ネットワークと接続を管理する

StorageGRIDネットワーク設定を設定する

グリッドマネージャーからさまざまなネットワーク設定を構成して、StorageGRID システムの動作を微調整できます。

VLANインターフェースを設定する

"[仮想LAN \(VLAN\) インターフェースを作成する](#)"を使用して、セキュリティ、柔軟性、パフォーマンス向上のためにトラフィックを分離および分割できます。各 VLAN インターフェースは、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ースに関連付けられています。VLAN インターフェースは、HAグループやロードバランサーエンドポイントで使用することで、クライアントトラフィックや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

"[トラフィック分類ポリシー](#)"を使用して、特定のバケット、テナント、クライアントサブネット、またはロードバランサーエンドポイントに関連するトラフィックを含む、さまざまな種類のネットワークトラフィックを識別して処理できます。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。

StorageGRID ネットワークのガイドライン

Grid Manager 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。

S3クライアントの接続方法については、"[S3クライアント接続の設定](#)"を参照してください。

デフォルトの StorageGRID ネットワーク

デフォルトでは、StorageGRIDはグリッドノードごとに3つのネットワークインターフェースをサポートしているため、セキュリティおよびアクセス要件に合わせて、各グリッドノードのネットワーク設定を個別に構成できます。

ネットワークトポロジの詳細については、"[ネットワーク構築ガイドライン](#)"を参照してください。

グリッド 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。グリッド内のすべてのノード間、すべてのサイトおよびサブネット間の接続を提供します。

管理者ネットワーク

任意。管理ネットワークは通常、システム管理および保守に使用されます。クライアントのプロトコル 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であ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通常、S3クライアントアプリケーションへのアクセスを提供するために使用されるオープンネットワークであるため、グリッドネットワークを分離して保護することができます。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到達可能な任意のサブネットと通信できます。

ガイドライン

- StorageGRIDノードはそれぞれ、割り当てられるネットワークごとに、専用のネットワークインターフェース、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。
- グリッドノードは、ネットワーク上に複数のインターフェースを持つことはできません。
- ネットワークごと、グリッドノードごとに1つのゲートウェイがサポートされ、そのゲートウェイはノードと同じサブネット上に存在する必要があります。必要に応じて、ゲートウェイでより複雑なルーティングを実装できます。
- 各ノードにおいて、各ネットワークは特定のネットワークインターフェースにマッピングされます。

Network	インターフェイス名
Grid	eth0を使用したチャック アップロード署名要求がサポートされるようになりました。
管理者（任意）	eth1を使用したチャック アップロード署名要求がサポートされるようになりました。
クライアント（任意）	eth2を使用したチャック アップロード署名要求がサポートされるようになりました。

- ノードが StorageGRID アプライアンスに接続されている場合、各ネットワークに専用のポートが使用されます。詳細については、お使いのアプライアンスのインストール手順書をご覧ください。
- 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が有効になっている場合、0.0.0.0/0はeth2上のクライアントネットワークを使用します。eth2が有効になっていない場合、0.0.0.0/0はeth0上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しません。
- 管理ネットワークは、グリッドノードの展開時に設定することで、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ーインターフェイスへのアクセスを許可できます。

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。例えば、Admin ノードまたは Gateway ノードにトランク インターフェイスを追加して、["VLANインターフェイス"](#)を使用し、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ことができます。または、["高可用性（HA）グループ"](#)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。

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、以下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する"](#)
 - **Linux**（ノードをインストールする前）：["ノード設定ファイルを作成する"](#)
 - **Linux**（ノードのインストール後）：["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する"](#)



「Linux」とは、RHEL、Ubuntu、またはDebianのいずれかの環境を指します。サポートされているバージョンの一覧については、["NetApp Interoperability Matrix Tool \(IMT\)"](#)を参照してください。

StorageGRIDでIPアドレスを表示する

StorageGRID システムの各グリッドノードの IP アドレスを確認できます。その後、この IP アドレスを使用してコマンドラインから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。

開始する前に

["対応ウェブブラウザ"](#) を使用して Grid Manager にサインインしています。

タスク概要

IPアドレスの変更に関する情報については、"[IPアドレスを設定する](#)"を参照してください。

手順

1. ノード > グリッドノード > 概要 を選択します。
2. 「IP アドレス」 タイトルの右側にある「詳細を表示」を選択します。

そのグリッドノードのIPアドレスは表に記載されています。

DC2-SGA-010-096-106-021 (Storage Node) [🔗](#)



Overview Hardware Network Storage Objects ILM Tasks

Node information [?](#)

Name: DC2-SGA-010-096-106-021
Type: Storage Node
ID: f0890e03-4c72-401f-ae92-245511a38e51
Connection state: Connected
Storage used: Object data 7% [?](#)
Object metadata 5% [?](#)
Software version: 11.6.0 (build 20210915.1941.afce2d9)
IP addresses: 10.96.106.21 - eth0 (Grid Network)

[Hide additional IP addresses](#) [^](#)

Interface ⌵	IP address ⌵
eth0 (Grid Network)	10.96.106.21
eth0 (Grid Network)	fe80::2a0:98ff:fe64:6582
hic2	10.96.106.21
hic4	10.96.106.21
mtc2	169.254.0.1

Alerts

Alert name ⌵	Severity ? ⌵	Time triggered ⌵	Current values
ILM placement unachievable 🔗	Major	2 hours ago ?	
A placement instruction in an ILM rule cannot be achieved for certain objects.			

StorageGRIDでVLANインターフェイスを設定する

管理ノードとゲートウェイノード上に仮想LAN（VLAN）インターフェイスを作成し、そ

れらをHAグループやロードバランサーのエンドポイントで使用することで、セキュリティ、柔軟性、パフォーマンスを向上させるためにトラフィックを分離および分割します。HAグループで選択されたノードは、VLANインターフェースを使用して最大10個の仮想IPアドレスを共有できるため、いずれかのノードがダウンした場合でも、別のノードが仮想IPアドレスとの間のトラフィックを引き継ぐことができます。

VLANインターフェースに関する考慮事項

- VLANインターフェースを作成するには、VLAN IDを入力し、1つまたは複数のノード上の親インターフェースを選択します。
- スイッチ側では、親インターフェースをトランクインターフェースとして設定する必要があります。
- 親インターフェースは、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の追加トランクインターフェース (例: ens256) にすることができます。
- 各VLANインターフェースについて、特定のノードに対して選択できる親インターフェースは1つだけです。例えば、同じゲートウェイノード上で、グリッドネットワークインターフェースとクライアントネットワークインターフェースの両方を、同じVLANの親インターフェースとして使用することはできません。
- VLANインターフェースが、Grid ManagerおよびTenant Managerに関連するトラフィックを含む管理ノードのトラフィック用である場合は、管理ノード上のインターフェースのみを選択してください。
- VLANインターフェースがS3クライアントトラフィック用である場合は、管理ノードまたはゲートウェイノードのいずれかのインターフェースを選択してください。
- トランクインターフェースを追加する必要がある場合は、詳細については以下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する"](#)
 - **Linux** (ノードをインストールする前) : ["ノード設定ファイルを作成する"](#)
 - **Linux** (ノードのインストール後) : ["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する"](#)



「Linux」とは、RHEL、Ubuntu、またはDebianのいずれかの環境を指します。サポートされているバージョンの一覧については、["NetApp Interoperability Matrix Tool \(IMT\)"](#)を参照してください。

VLANインターフェースを作成する

開始する前に

- ["対応ウェブブラウザ"](#) を使用して Grid Manager にサインインしています。
- あなたは["ルートアクセス権限"](#)があります。
- ネットワーク内にトランクインターフェースが設定され、VMまたはLinuxノードに接続されています。トランクインターフェースの名前を確認しておいてください。
- 設定するVLANのIDを確認しておいてください。

タスク概要

ネットワーク管理者は、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するために、1つ以上のトランクインターフェースと1つ以上のVLANを設定している場

合があります。各VLANは、数値IDまたはタグによって識別されます。たとえば、ネットワークでは 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 を使用する場合があります。

Grid Manager を使用すると、クライアントが特定の VLAN 上で 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際には、VLAN ID を指定し、1 つまたは複数のノード上の親（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する

手順

1. **Configuration > Network > VLAN interfaces** を選択します。
2. ***Create***を選択します。

VLANインターフェースの詳細を入力してください

手順

1. ネットワーク内のVLANのIDを指定してください。1から4094までの任意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。例えば、あるサイトでは管理トラフィックにVLAN ID 200を使用し、別のサイトではクライアントトラフィックに同じVLAN IDを使用するといったことが可能です。各サイトで、異なる親インターフェースのセットを持つ個別のVLANインターフェースを作成できます。ただし、同じIDを持つ2つのVLANインターフェースは、ノード上で同じインターフェースを共有することはできません。既に使用されているIDを指定した場合、メッセージが表示されます。

2. 必要に応じて、VLANインターフェースの簡単な説明を入力してください。
3. ***続行***を選択します。

親インターフェースを選択

この表には、グリッド内の各サイトにある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ースが一覧表示されています。管理ネットワーク（eth1）インターフェースは親インターフェースとして使用できず、表示されません。

手順

1. このVLANを接続する親インターフェースを1つ以上選択してください。

例えば、ゲートウェイノードと管理ノード用に、クライアントネットワーク（eth2）インターフェースにVLANを接続したい場合があります。

Parent interfaces

Select one or more parent interfaces for this VLAN interface. You can only select one parent interface on each node for each VLAN interface.

	Site ?	Node name ?	Interface ?	Description ?	Node type ?	Attached VLANs ?
☐	Data Center 2	DC2-ADM1	eth0	Grid Network	Non-primary Admin	—
☒	Data Center 2	DC2-ADM1	eth2	Client Network	Non-primary Admin	—
☐	Data Center 1	DC1-G1	eth0	Grid Network	Gateway	—
☒	Data Center 1	DC1-G1	eth2	Client Network	Gateway	—
☐	Data Center 1	DC1-ADM1	eth0	Grid Network	Primary Admin	—

2 interfaces are selected.

PreviousContinue

2. *続行*を選択します。

設定を確認します

手順

1. 設定を確認し、必要に応じて変更を加えてください。

- VLAN IDまたは説明を変更する必要がある場合は、ページ上部の「VLANの詳細を入力」を選択してください。
- 親インターフェースを変更する必要がある場合は、ページ上部の「親インターフェースを選択」を選択するか、「前へ」を選択してください。
- 親インターフェースを削除する必要がある場合は、ゴミ箱  を選択してください。

2. *保存*を選択します。

3. 新しいインターフェースが高可用性グループページに選択肢として表示され、ノードのネットワークインターフェース テーブル（ノード > 親インターフェースノード > ネットワーク）にリストされるまで、最大5分お待ちください。

VLANインターフェースを編集する

VLANインターフェースを編集する際には、次の種類の変更を行うことができます：

- VLAN IDまたは説明を変更します。
- 親インターフェースを追加または削除します。

たとえば、関連するノードを廃止する予定がある場合は、VLANインターフェイスから親インターフェイスを削除することができます。

次の点に注意してください。

- VLANインターフェイスがHAグループで使用されている場合、VLAN IDを変更することはできません。
- 親インターフェイスがHAグループで使用されている場合、その親インターフェイスを削除することはできません。

例えば、VLAN 200がノードAとノードBの親インターフェイスに接続されているとします。HAグループがノードAにVLAN 200インターフェイスを、ノードBに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は削除できますが、ノードAの使用済みの親インターフェイスは削除できません。

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、**Actions > Edit** を選択します。
3. 必要に応じて、VLAN IDまたは説明を更新します。次に、***続行***を選択します。

VLANがHAグループで使用されている場合、VLAN IDを更新することはできません。

4. 必要に応じて、チェックボックスを選択または解除して、親インターフェイスを追加したり、使用されていないインターフェイスを削除したりできます。次に、「**続行**」を選択します。
5. 設定を確認し、必要に応じて変更を加えてください。
6. *** 保存 *** を選択します。

VLANインターフェイスを削除する

VLANインターフェイスを1つ以上削除できます。

現在HAグループで使用されているVLANインターフェイスは削除できません。VLANインターフェイスを削除するには、まずHAグループからVLANインターフェイスを削除する必要があります。

クライアントのトラフィックに支障が生じないようにするには、以下のいずれかの対策を検討してください。

- 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。
- 削除したいVLANインターフェイスが現在アクティブなインターフェイスである場合は、HAグループを編集してください。削除したい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てください。新しいプライマリインターフェイスで通信が確立されるまで待ってから、古いインターフェイスをHAグループから削除してください。最後に、そのノード上の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. 選択内容を確定するには「**はい**」を選択してください。

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インターフェイスのページに、緑色の成功バナーが表示されます。

管理インターフェイスの **StorageGRID CORS** を有効にする

グリッド管理者は、StorageGRID のデータを管理 API を使用して別のドメインからアクセスできるようにする場合、StorageGRID への管理 API リクエストに対してクロスオリジン リソース共有 (CORS) を有効にすることができます。

開始する前に

- "[対応ウェブブラウザ](#)" を使用して Grid Manager にサインインしています。
- "[ルートアクセス権限](#)" は、すべての CORS 設定リクエストへのアクセスを提供します。

タスク概要

CORS は、あるドメインのクライアント Web アプリケーションが別のドメインのリソースにアクセスできるようにするセキュリティメカニズムです。たとえば、ドメイン `\http://www.example.com` で StorageGRID の監視ダッシュボードを構築するとします。`\http://www.example.com` および「Grid Manager」に対して StorageGRID で CORS を有効にすることで、StorageGRID ドメインは `\http://www.example.com` からの Grid Management API リクエストに応答します。

管理 API (mgmt-api) リクエストに ``application/json`` または ``multipart/formdata`` リクエスト (``Content-Type`` 用) は CORS に対応しています。

手順

1. Grid Manager で、**CONFIGURATION > Network > *管理インターフェイスの CORS 設定*** に移動します。
2. **Grid Manager**、**Tenant Manager**、またはその両方のオプションを選択してください。
 - **Grid Manager** : クロスドメインのグリッド管理 API リクエストに対して CORS を有効にします。
 - **Tenant Manager** : クロスドメインのテナント管理 API リクエストに対して CORS を有効にします。
3. 「ドメイン」フィールドに、もう一方のドメインの URL を入力してください。

複数のドメインに対して StorageGRID で CORS を有効にする場合は、「別のドメインを追加」を選択してください。

4. * 保存 * を選択します。

関連情報

["バケットとオブジェクトの StorageGRID CORS を設定する"](#)

トラフィック分類ポリシーを管理する

StorageGRID のトラフィック分類ポリシー

トラフィック分類ポリシーを使用すると、さまざまな種類のネットワーク 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、サービス品質 (QoS) の向上に貢献します。

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 ロードバランサーサービス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、ロードバランサーのエンドポイントを事前に作成しておく必要があります。

マッチングルール

各トラフィック分類ポリシーには、次のエンティティの1つ以上に関連するネットワークトラフィックを識別するための1つ以上の照合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、ルールの目的に従って、ポリシー内のいずれかのルールに一致するトラフィックを監視します。ポリシーのいずれか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、特定のエンティティを除くすべてのトラフィックに一致するルールを設定することもできます。

トラフィック制限

必要に応じて、ポリシーに以下の制限タイプを追加できます。

- 総帯域幅
- リクエストごとの帯域幅
- 同時リクエスト
- リクエストレート

制限値はロードバランサーごとに適用されます。トラフィックが複数のロードバランサーに同時に分散される場合、合計最大レートは、指定したレート制限の倍数になります。



総帯域幅を制限するポリシー、またはリクエストごとの帯域幅を制限するポリシーを作成できます。ただし、StorageGRID は両方の種類の帯域幅を同時に制限することはできません。総帯域幅制限は、制限のないトラフィックにも軽微なパフォーマンス上の影響を与える可能性があります。

総帯域幅制限またはリクエストごとの帯域幅制限の場合、リクエストは設定した速度で送受信されます。StorageGRID が適用できる速度は1つのみであるため、マッチャータ입による最も具体的なポリシー一致が適用されます。リクエスト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、より一般的なマッチングポリシーにはカウントされません。その他のすべての制限タイプについては、クライアントからのリクエストは250ミリ秒遅延され、該当するポリシー制限を超えるリクエストに対しては503 Slow Down 応答が返されます。

グリッドマネージャーでは、トラフィックチャートを表示し、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できます。

SLAと連携して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やデータ保護と組み合わせて使用することで、容量、データ保護、パフォーマンスに関する具体的な内容を規定するサービスレベル契約（SLA）を適用できます。

以下の例は、SLAの3つの階層を示しています。各SLAティアのパフォーマンス目標を達成するために、トラフィック分類ポリシーを作成できます。

サービスレベルティア	Capacity	データ保護	許容される最大パフォーマンス	コスト
Gold	1 PBのストレージ容量が許可されています	3コピー ILM ルール	25 K requests/sec 5 GB/秒（40 Gbps）の帯域幅	月額\$\$\$
Silver	250 TBのストレージ容量が利用可能	2コピーILMルール	10 K requests/sec 1.25 GB/秒（10 Gbps）の帯域幅	月額\$\$
Bronze	100 TB のストレージ容量が許可されています	2コピーILMルール	5 K requests/sec 1 GB/秒（8 Gbps）の帯域幅	月額\$

StorageGRID トラフィック分類ポリシーを作成する

監視したい場合や、必要に応じてバケット、バケット正規表現、CIDR、ロードバランサーエンドポイント、またはテナントごとにネットワークトラフィックを制限したい場合は、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、同時リクエスト数、またはリクエストレートに基づいて、ポリシーの制限を設定できます。

開始する前に

- ["対応ウェブブラウザ"](#) を使用して Grid Manager にサインインしています。
- あなたは["ルートアクセス権限"](#)があります。
- 一致させたいロードバランサーのエンドポイントをすべて作成しました。
- マッチングさせたいテナントをすべて作成しました。

手順

1. **[設定] > [ネットワーク] > [トラフィック分類]** を選択します。
2. ***Create*** を選択します。
3. ポリシーの名前と説明（任意）を入力し、***続行*** を選択します。

例えば、このトラフィック分類ポリシーが何に適用され、何を制限するかを説明してください。

4. 「**ルールを追加**」を選択し、以下の詳細を指定して、ポリシーに一致するルールを1つ以上作成します。作成するポリシーには、少なくとも1つの一致するルールが必要です。「**続行**」を選択します。

フィールド	説明
Type	マッチングルールを適用するトラフィックの種類を選択してください。トラフィックの種類は、バケット、バケット正規表現、CIDR、ロードバランサーエンドポイント、およびテナントです。

フィールド	説明
値に一致	選択したタイプに一致する値を入力してください。 • バケット：バケット名を1つ以上入力してください。 • バケット正規表現：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。 正規表現はアンカーされていません。バケット名の先頭に一致させるには ^ アンカーを使用し、名前の末尾に一致させるには \$ アンカーを使用します。正規表現マッチングは、PCRE（Perl 互換正規表現）構文のサブセットをサポートしています。 • CIDR：目的のサブネットに一致する IPv4 サブネットを 1 つ以上、CIDR 表記で入力してください。 • ロードバランサーエンドポイント：エンドポイント名を選択してください。これらは、"ロードバランサーのエンドポイントを設定する"で定義したロードバランサーエンドポイントです。 • テナント：テナントのマッチングにはアクセスキーIDが使用されます。リクエストにアクセスキー ID が含まれていない場合（たとえば、匿名アクセス）、アクセスされたバケットの所有権を使用してテナントが決定されます。
逆マッチ	定義したタイプとマッチ値に一致するトラフィックを除くすべてのネットワークトラフィックに一致させる場合は、「逆マッチ」チェックボックスを選択してください。それ以外の場合は、チェックボックスをオフのままにしてください。 例えば、このポリシーをロードバランサーエンドポイントの1つを除くすべてに適用する場合は、除外するロードバランサーエンドポイントを指定し、「逆一致」を選択します。 複数のマッチャーを含むポリシーで、少なくとも1つが逆マッチャーである場合は、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. オプションで「制限を追加」を選択し、次の詳細を選択して、ルールに一致したネットワークトラフィックを制御する 1 つ以上の制限を追加します。



StorageGRID は、制限を追加しなくても指標を収集するため、ネットワークトラフィックの傾向を把握できます。

フィールド	説明
Type	ルールに一致したネットワーク トラフィックに適用する制限の種類。例えば、帯域幅やリクエストレートを制限することができます。 注：総帯域幅を制限するポリシー、またはリクエストごとの帯域幅を制限するポリシーを作成できます。ただし、StorageGRID は両方の種類の帯域幅を同時に制限することはできません。集約帯域幅を使用している場合、リクエストごとの帯域幅は使用できません。逆に、リクエスト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。総帯域幅制限は、制限のないトラフィックにも軽微なパフォーマンス上の影響を与える可能性があります。 帯域幅制限については、StorageGRID は設定された制限の種類に最も適したポリシーを適用します。例えば、トラフィックを一方向のみに制限するポリシーを設定した場合、帯域幅制限のある追加のポリシーに一致するトラフィックが存在する場合でも、逆方向のトラフィックは無制限になります。StorageGRID は、帯域幅制限に対する「最適な」マッチングを以下の順序で実装します。 • 正確なIPアドレス (/32マスク) • 正確なバケット名 • バケット正規表現 • テナント • エンドポイント • 完全一致しないCIDR (/32以外) • 逆マッチ
環境	この制限がクライアントの読み取りリクエスト（GET または HEAD）に適用されるか、書き込みリクエスト（PUT、POST、または DELETE）に適用されるか。
Value	選択したユニットに基づいて、ネットワーク トラフィックが制限される値です。たとえば、10 と入力して MiB/s を選択すると、このルールに一致するネットワークトラフィックが 10 MiB/s を超えないように制限されます。 注：単位設定によっては、使用可能な単位はバイナリ（例：GiB）または10進数（例：GB）のいずれかになります。単位設定を変更するには、グリッドマネージャー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。

例えば、SLAティアに対して4 GB/sの帯域幅制限を設定したい場合は、GET/HEADを4 GB/s、PUT/POST/DELETEを4 GB/sとする2つの集約帯域幅制限を作成します。

6. *続行*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てください。必要に応じて変更を加えるには、「前へ」ボタンを使用してください。ポリシーの内容に問題がなければ、「保存して続行」を選択してください。

S3クライアントのトラフィックは、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。

終了後の操作

"[ネットワーク トラフィック メトリクスの表示](#)"ポリシーが期待どおりのトラフィック制限を適用していることを確認するため。

StorageGRID トラフィック分類ポリシーを編集する

トラフィック分類ポリシーを編集することで、その名前や説明を変更したり、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。

開始する前に

- "[対応ウェブブラウザ](#)"を使用して Grid Manager にサインインしています。
- あなたは"[ルートアクセス権限](#)"があります。

手順

1. **[設定] > [ネットワーク] > [トラフィック分類]** を選択します。

トラフィック分類ポリシーのページが表示され、既存のポリシーが表形式で一覧表示されます。

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編集します。入力内容については、"[トラフィック分類ポリシーを作成する](#)"を参照してください。

[操作]メニュー

- a. 該当するポリシーのチェックボックスを選択してください。
- b. **Actions > Edit** 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. 「ポリシー名の入力」ステップでは、必要に応じてポリシー名または説明を編集し、*続行*を選択してください。
4. 「一致するルールの追加」ステップでは、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. 「制限を設定する」ステップでは、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は保存され、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、ポリシーが想定どおりのトラフィック制限を適用していることを確認できます。

StorageGRID トラフィック分類ポリシーを削除する

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復元できないため、必ず正しいポリシーを削除してください。

開始する前に

- "対応ウェブブラウザ" を使用して Grid Manager にサインインしています。
- あなたは"ルートアクセス権限"があります。

手順

1. [設定] > [ネットワーク] > [トラフィック分類] を選択します。

トラフィック分類ポリシーページが表示され、既存のポリシーが表形式で一覧表示されます。

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。

[操作]メニュー

- a. 該当するポリシーのチェックボックスを選択してください。
- b. **Actions > Remove** を選択します。

ポリシー詳細ページ

- 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. ポリシーを削除することを確認するには、**Yes** を選択してください。

ポリシーが削除されます。

StorageGRIDでネットワーク トラフィック指標を表示

トラフィック分類ポリシーページで利用可能なグラフを表示することで、ネットワークトラフィックを監視できます。

開始する前に

- "対応ウェブブラウザ" を使用して Grid Manager にサインインしています。
- あなたは"ルートアクセス権限またはテナントアカウントの権限"があります。

タスク概要

既存のトラフィック分類ポリシーについては、ロードバランサーサービスのメトリクスを表示することで、ポリシーがネットワーク全体のネットワークトラフィックを適切に制限しているかどうかを判断できます。グラフのデータは、ポリシーを調整する必要がある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、メトリクスは収集され、グラフはネットワークトラフィックの傾向を理解する上で有用な情報を提供します。

手順

1. [設定] > [ネットワーク] > [トラフィック分類] を選択します。

トラフィック分類ポリシーのページが表示され、既存のポリシーが表に一覧表示されます。

2. メトリクスを表示するトラフィック分類ポリシー名を選択してください。

3. 「メトリクス」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。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指標のみが表示されます。

このページには以下のグラフが含まれています。

- ・リクエストレート：このグラフは、このポリシーに一致する帯域幅のうち、すべてのロードバランサーによって処理された量を示します。受信データには、すべてのリクエストのリクエストヘッダーと、ボディデータを含むレスポンスのボディデータサイズが含まれます。送信されたデータには、すべてのリクエストのレスポンスヘッダーと、レスポンスにボディデータが含まれるリクエストのレスポンスボディデータのサイズが含まれます。



リクエストが完了すると、このグラフには帯域幅の使用状況のみが表示されます。処理速度が遅い場合や、オブジェクトのサイズが大きい場合、実際の瞬間帯域幅は、このグラフに示されてい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リクエストがクライアントにエラー（HTTP ステータスコード ≥ 400 ）を返すおおよその割合を示します。
 - ・平均リクエスト処理時間（エラーなし）：このグラフは、このポリシーに一致する正常なリクエストの平均処理時間を示します。
 - ・ポリシー帯域幅の使用状況：このグラフは、このポリシーに一致する帯域幅のうち、すべてのロードバランサーによって処理された帯域幅の量を示します。受信データには、すべてのリクエストのリクエストヘッダーと、ボディデータを含むレスポンスのボディデータサイズが含まれます。送信されたデータには、すべてのリクエストのレスポンスヘッダーと、レスポンスにボディデータが含まれるリクエストのレスポンスボディデータのサイズが含まれます。
4. 折れ線グラフ上にカーソルを合わせると、グラフの特定部分の値がポップアップ表示されます。
5. ポリシーに関するすべてのグラフを表示するには、「メトリクス」タイトルのすぐ下にある「Grafana ダッシュボード」を選択してください。「メトリクス」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。
- ・オブジェクトサイズによる書き込みリクエストレート：このポリシーに一致する PUT/POST/DELETE リクエストのレート。個々のセルに位置を合わせると、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値に切り捨てられるため、バケット内にゼロ以外のリクエストが存在する場合でも、0と表示されることがあります。
 - ・オブジェクトサイズによる読み取りリクエストレート：このポリシーに一致する GET/HEAD リクエストのレート。個々のセルに位置を合わせると、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値に切り捨てられるため、バケット内にゼロ以外のリクエストが存在する場合でも、0と表示されることがあります。
6. または、*サポート*メニューからグラフにアクセスすることもできます。
- a. サポート > ツール > メトリクス を選択します。
 - b. 「Grafana」セクションから「Traffic Classification Policy」を選択してください。
 - c. ページ左上のメニューからポリシーを選択してください。

- d. グラフ上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るオブジェクトのサイズ、およびその期間中の1秒あたりのリクエスト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、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一覧表示されています。

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てください。

StorageGRIDの送信TLS接続でサポートされている暗号

StorageGRID システムは、IDフェデレーションおよび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) 接続に対して、限られた暗号スイートセットをサポートします。

サポートされているTLSのバージョン

StorageGRID は、IDフェデレーションおよび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において、TLS 1.2およびTLS 1.3をサポートします。

外部システムでの使用がサポートされているTLS暗号は、さまざまな外部システムとの互換性を確保するために選択されています。このリストは、S3クライアントアプリケーションで利用できる暗号方式のリストよりも大きくなっています。暗号を設定するには、**Configuration > Security > Security settings** に移動し、**TLS and SSH policies** 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構成オプションは、StorageGRIDでは設定できません。これらの設定に関して具体的なお要望がある場合は、NetAppのアカウント担当者にお問い合わせください。

StorageGRID におけるアクティブ、アイドル、および同時 HTTP 接続の利点

HTTP接続の設定方法は、StorageGRIDシステムのパフォーマンスに影響を与える可能性があります。HTTP接続がアクティブかアイドルか、あるいは複数の接続が同時に存在するかによって、設定は異なります。

以下の種類のHTTP接続におけるパフォーマンス上の利点を確認できます。

- アイドル状態のHTTP接続
- アクティブなHTTP接続
- 同時HTTP接続

アイドル状態のHTTP接続を開いたままにしておくことの利点

クライアントアプリケーションがアイドル状態のときは、後続のトランザクションを可能にするためにHTTP接続を開いたままにしておく。アイドル状態のHTTP接続は、最大10分間開いたままにしてください。StorageGRID は、10分以上開いたままアイドル状態になっているHTTP接続を自動的に閉じる場合があります。

開いているアイドル状態のHTTP接続には、以下の利点があります：

- StorageGRID システムが HTTP トランザクションを実行する必要があると判断してから、実際にトランザクションを実行できるまでの遅延が軽減されます

最大の利点はレイテンシの低減であり、特にTCP/IPおよびTLS接続の確立に必要な時間において顕著です。

- 以前に実行された転送データでTCP/IPスロースタートアルゴリズムを初期化することにより、データ転送速度を向上
- クライアントアプリケーションとStorageGRIDシステム間の接続を中断するいくつかの種類の障害状態の即時通知

スロースタートの利点とリソース配分のバランスを取りながら、アイドル状態の接続をどのくらいの時間開いたままにするかを決定します。

アクティブなHTTP接続の利点

ストレージノードに直接接続する場合、HTTP接続が継続的にトランザクションを実行する場合でも、アクティブなHTTP接続の継続時間を最大10分に制限する必要があります。

接続を維持すべき最大期間を決定することは、接続の持続性による利点と、接続を内部システムリソースに理想的に割り当てることとの間のトレードオフとなります。

ストレージノードへのクライアント接続において、アクティブなHTTP接続を制限することで、以下の利点が得られます。

- StorageGRID システム全体で最適なロード バランシングを実現します。

時間の経過とともに、ロード バランシング要件の変化により、HTTP接続が最適ではなくなる可能性があります。クライアントアプリケーションがトランザクションごとに個別のHTTP接続を確立する場合、システムは最高のロード バランシングを実現しますが、この方法では永続的な接続に伴う貴重な利点が失われてしまいます。

- クライアントアプリケーションが、空き容量のあるLDRサービスにHTTPトランザクションを送信できるようにします。
- メンテナンス手順を開始できるようにします。

一部のメンテナンス手順は、進行中のすべてのHTTP接続が完了した後にのみ開始されます。

ロード バランシングサービスへのクライアント接続において、接続の維持時間を制限することは、一部のメンテナンス手順を迅速に開始するために役立ちます。クライアント接続の継続時間に制限がない場合、アクティブな接続が自動的に終了するまでに数分かかることがあります。

同時HTTP接続の利点

並列処理を可能にしてパフォーマンスを向上させるために、StorageGRID システムへの複数の TCP/IP 接続を開いたままにしておく必要があります。並列接続の最適な数は、さまざまな要因によって決まります。

同時HTTP接続には、以下の利点があります。

- 遅延の低減

他の取引が完了するのを待つことなく、取引をすぐに開始できます。

- スループットの向上

StorageGRID システムは並列トランザクションを実行し、総トランザクションスループットを向上させることができます。

クライアントアプリケーションは、複数のHTTP接続を確立する必要があります。クライアントアプリケーションがトランザクションを実行する必要がある場合、現在トランザクションを処理していない確立済みの接続を選択して、すぐに使用することができます。

各 StorageGRID システムのトポロジは、同時トランザクションと接続に対して異なる最大スループットを持ちます。ピークスループットは、コンピューティング、ネットワーク、ストレージリソース、WAN リンク、および StorageGRID システムがサポートするサーバー、サービス、アプリケーションの数によって異なります。

StorageGRIDシステムは多くの場合、複数のクライアントアプリケーションをサポートしています。同時接続の最大数を決定する際には、この点に留意してください。クライアントアプリケーションが、それぞれStorageGRIDシステムへの接続を確立する複数のソフトウェアエンティティで構成されている場合は、エンティティ間のすべての接続を合計してください。次のような状況では、同時接続の最大数を調整する必要があります場合があります。

- StorageGRID システムのトポロジは、システムがサポートできる同時トランザクション数と接続数の最大数に影響します。
- 帯域幅が限られたネットワーク上で StorageGRID システムと通信するクライアントアプリケーションは、個々のトランザクションが妥当な時間内に完了するよう、同時実行の度合いを下げる必要がある場合があります。
- 多くのクライアントアプリケーションが StorageGRID システムを共有している場合は、システムの制限を超えないように、並行処理の度合いを下げる必要があります。

読み取り操作と書き込み操作のためのHTTP接続プールの分離

読み取り操作と書き込み操作にそれぞれ別のHTTP接続プールを使用し、各操作にプールのどの部分を使用するかを制御できます。HTTP接続を複数のプールに分けることで、トランザクションをより適切に制御し、ロード バランシングを行うことができます。

クライアントアプリケーションは、取得（読み取り）が主体となるロード、または保存（書き込み）が主体となるロードを作成できます。読み取りトランザクションと書き込みトランザクション用にHTTP接続のプールを分けることで、それぞれのプールのうち、読み取りトランザクションまたは書き込みトランザクションに割り当てる割合を調整できます。

StorageGRIDでリンクコストを管理する

リンクコストを使用すると、2つ以上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を優先的に選択できます。サイト間の遅延を反映させるように、リンクコストを調整できます。

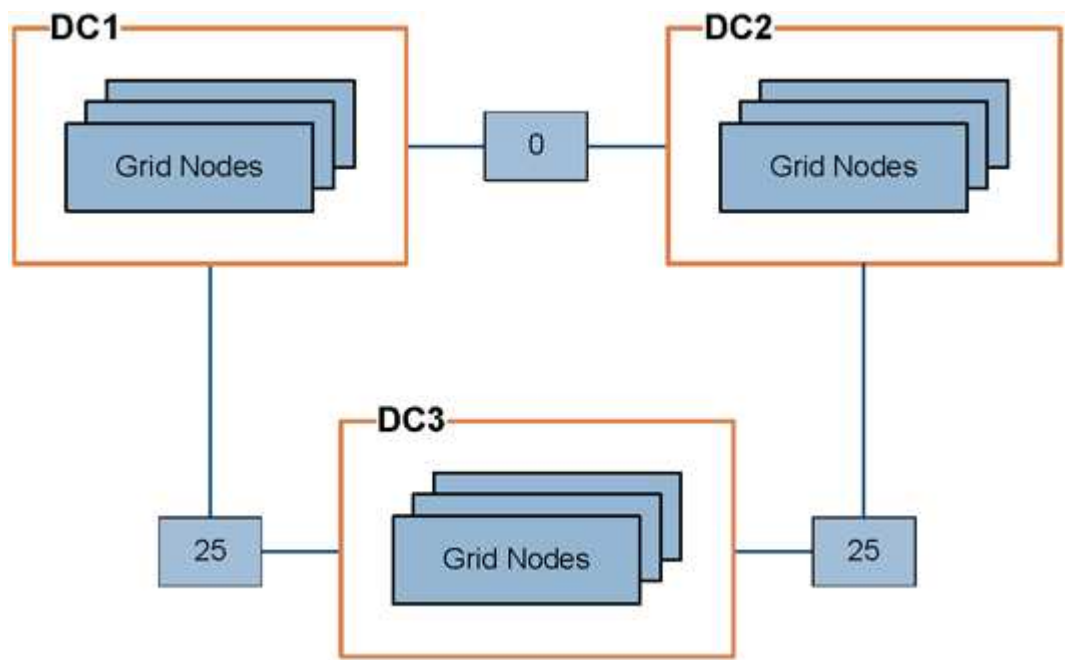
リンクコストとは何ですか？

- リンクコストは、オブジェクト取得を実行するためにどのオブジェクトコピーを使用するかを優先順位付け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とテナント管理APIが、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ーサービスによって、クライアント接続をルーティングするために使用されます。["ロード バランシングに関する考慮事項"](#)を参照してください。

この図は、サイト間のリンクコストが設定された3つのサイトからなる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ーサービスは、クライアント接続を同じデータセンターサイト内のすべてのストレージノード、およびリンクコストが0のすべてのデータセンターサイトに均等に分散します。

この例では、データセンターサイト1（DC1）のゲートウェイノードが、クライアント接続をDC1のストレージノードとDC2のストレージノードに均等に分散します。DC3のゲートウェイノードは、クライアント接続をDC3のストレージノードにのみ送信します。

- 複数の複製コピーとして存在するオブジェクトを取得する場合、StorageGRID はリンクコストが最も低いデータセンターからコピーを取得します。

この例では、DC2 のクライアントアプリケーションが DC1 と DC3 の両方に保存されているオブジェクトを取得する場合、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 から取得されます。

リンクコストは、特定の測定単位を持たない任意の相対数値です。たとえば、リンクコストが50の場合、リンクコストが25の場合よりも優先順位が低くなります。この表は、一般的に使用されるリンクコストを示しています。

リンク	リンクコスト	Notes
物理的な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。

リンク	リンクコスト	Notes
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	同一の建物またはキャンパス内にあり、LANで接続された論理データセンター。

リンク費用の更新

データセンターサイト間のリンクコストを更新することで、サイト間の遅延を反映させることができます。

開始する前に

- "対応ウェブブラウザ" を使用して Grid Manager にサインインしています。
- あなたは"その他のグリッド構成権限"があります。

手順

1. サポート > その他 > リンク費用 を選択します。

Link Cost
Updated: 2023-02-15 18:09:28 MST

Site Names (1 - 3 of 3)

Site ID	Site Name	Actions
10	Data Center 1	
20	Data Center 2	
30	Data Center 3	

Show Records Per Page Previous « 1 » Next

Link Costs

Link Source	Link Destination			Actions
	10	20	30	
Data Center 1	0	25	25	

2. 「リンク元」でサイトを選択し、「リンク先」に0～100のコスト値を入力してください。

送信元と送信先が同じ場合、リンクコストを変更することはできません。

変更をキャンセルするには、 *元に戻す*を選択します。

3. 「変更を適用」を選択します。

AutoSupport を使用する

StorageGRIDのAutoSupportについて学ぶ

AutoSupport 機能を使用すると、StorageGRID は健全性およびステータスパッケージを NetApp テクニカルサポートに送信できます。

AutoSupportを使用すると、問題をより迅速に解決できます。テクニカルサポートは、お客様の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お手伝いをいたします。オプションとして、AutoSupportはパッケージをもう1つの追加の宛先に送信できます。

StorageGRID には 2 種類の AutoSupport があります：

- **StorageGRID AutoSupport** は、StorageGRID ソフトウェアの問題をレポートします。StorageGRID の初回インストール時にデフォルトで有効になります。必要に応じて["デフォルトの AutoSupport 構成を変更する"](#)できます。



StorageGRID AutoSupport が有効になっていない場合、Grid Manager ダッシュボードにメッセージが表示されます。メッセージには、AutoSupport の設定ページへのリンクが含まれています。メッセージを閉じると、AutoSupport が無効のままであっても、ブラウザのキャッシュがクリアされるまで再び表示されません。

- アプライアンスハードウェア **AutoSupport** は、StorageGRID アプライアンスの問題を報告します。次の操作が必要です。["各アプライアンスでハードウェア AutoSupport を設定する"](#)

Active IQ とは何ですか？

Active IQ は、クラウドベースのデジタルアドバイザーであり、NetApp のインストールベースから得られる予測分析とコミュニティの知見を活用します。継続的なリスク評価、予測アラート、処方的ガイダンス、および自動化されたアクションにより、問題が発生する前に防止し、システムの健全性の向上とシステム可用性の向上を実現します。

NetApp Support Site で Active IQ のダッシュボードと機能を使用する場合は、AutoSupport を有効にする必要があります。

["Active IQ Digital Advisor ドキュメント"](#)

AutoSupport パッケージに含まれる情報

AutoSupport パッケージには以下のファイルと詳細情報が含まれています。

ファイル名	フィールド	説明
AUTOSUPPORT-HISTORY.XML	AutoSupport シーケンス番号 + この AutoSupport の宛先 + 配信ステータス + 配信試行回数 + AutoSupport 件名 + 配信 URI + 最終エラー + AutoSupport PUT ファイル名 + 生成時刻 + Autosupport 圧縮サイズ + Autosupport 非圧縮サイズ + 合計収集時間 (ms)	AutoSupport 履歴ファイル。
AUTOSUPPORT.XML	ノード + サポートへの連絡プロトコル + HTTP/HTTPS のサポート URL + サポートアドレス + AutoSupport OnDemand 状態 + AutoSupport OnDemand サーバー URL + AutoSupport OnDemand ポーリング間隔	AutoSupport ステータスファイル。使用されているプロトコルの詳細、テクニカルサポートの URL とアドレス、ポーリング間隔、および OnDemand AutoSupport が有効か無効かを示します。
BUCKETS.XML	バケットID + アカウントID + ビルドバージョン + ロケーション制約構成 + コンプライアンス有効 + コンプライアンス構成 + S3オブジェクトロック有効 + S3オブジェクトロック構成 + 一貫性構成 + CORS有効 + CORS構成 + 最終アクセス時間有効 + ポリシー有効 + ポリシー構成 + 通知有効 + 通知構成 + クラウドミラー有効 + クラウドミラー構成 + 検索有効 + 検索構成 + バケットタグ付け有効 + バケットタグ付け構成 + バージョン管理構成	バケットレベルでの設定詳細と統計情報を提供します。バケット構成の例としては、プラットフォームサービス、コンプライアンス、バケットの一貫性などが挙げられます。
GRID-CONFIGURATIONS.XML	属性ID + 属性名 + 値 + インデックス + テーブルID + テーブル名	グリッド全体の構成情報ファイル。グリッド証明書、メタデータのリザーブスペース、グリッド全体の構成設定（コンプライアンス、S3 オブジェクト ロック、オブジェクト圧縮、アラート、syslog、および ILM 構成）、イレイジャーコーディング プロファイルの詳細、DNS 名、および "NMS name" に関する情報が含まれています。

ファイル名	フィールド	説明
GRID-SPEC.XML	グリッド仕様、生のXML	StorageGRID の設定および展開に使用されます。グリッド仕様、NTP サーバーの IP アドレス、DNS サーバーの IP アドレス、ネットワークポロジー、およびノードのハードウェアプロファイルが含まれています。
GRID-TASKS.XML	ノード + サービスパス + 属性ID + 属性名 + 値 + インデックス + テーブルID + テーブル名	グリッドタスク（保守手順）のステータスファイル。グリッド上で実行中のタスク、終了したタスク、完了したタスク、失敗したタスク、および保留中のタスクの詳細を提供します。
GRID.JSON	グリッド + 改訂版 + ソフトウェアバージョン + 概要 + ライセンス + パスワード + DNS + NTP + サイト + ノード	グリッド情報。
ILM-CONFIGURATION.XML	属性ID + 属性名 + 値 + インデックス + テーブルID + テーブル名	ILM構成の属性一覧。
ILM-STATUS.XML	ノード + サービスパス + 属性ID + 属性名 + 値 + インデックス + テーブルID + テーブル名	ILMメトリクス情報ファイル。各ノードのILM評価率とグリッド全体のメトリクスが含まれています。
ILM.XML	ILMの生のXML	ILMアクティブポリシーファイル。ストレージプールID、取り込み動作、フィルタ、ルール、概要など、アクティブなILMポリシーに関する詳細情報が含まれています。
LOG.TGZ	該当なし	ダウンロード可能なログファイル。各ノードの `bycast-err.log` および `servermanager.log` が含まれます。
MANIFEST.XML	収集順序 + AutoSupport このデータのコンテンツファイル名 + このデータ項目の概要 + 収集されたバイト数 + 収集にかかった時間 + このデータ項目のステータス + エラーの概要 + AutoSupport このデータのコンテンツタイプ	AutoSupport のメタデータとすべての AutoSupport ファイルの簡単な説明が含まれます。

ファイル名	フィールド	説明
NMS-ENTITIES.XML	属性インデックス + エンティティOID + ノードID + デバイスモデルID + デバイスモデルバージョン + エンティティ名	グループおよびサービスエンティティ ("NMSツリー")。グリッドトポロジーの詳細を提供します。ノードは、そのノード上で実行されているサービスに基づいて特定できます。
OBJECTS-STATUS.XML	ノード + サービスパス + 属性ID + 属性名 + 値 + インデックス + テーブルID + テーブル名	オブジェクトの状態（バックグラウンド スキャン ステータス、アクティブ転送、転送速度、総転送量、削除率、破損したフラグメント、失われたオブジェクト、欠落したオブジェクト、修復試行回数、スキャン率、推定スキャン期間、および修復完了ステータスを含む）。
SERVER-STATUS.XML	ノード + サービスパス + 属性ID + 属性名 + 値 + インデックス + テーブルID + テーブル名	サーバー構成。各ノードに関する以下の詳細情報が含まれています：プラットフォームの種類、オペレーティングシステム、インストール済みメモリ、利用可能なメモリ、ストレージ接続、ストレージアプライアンスシャーシのシリアル番号、ストレージコントローラの障害ドライブ数、コンピュートコントローラシャーシの温度、コンピュートハードウェア、コンピュートコントローラのシリアル番号、電源、ドライブサイズ、およびドライブタイプ。
SERVICE-STATUS.XML	ノード + サービスパス + 属性ID + 属性名 + 値 + インデックス + テーブルID + テーブル名	サービスノード情報ファイル。割り当てられたテーブルスペース、空きテーブルスペース、データベースのReaperメトリック、セグメント修復時間、修復ジョブ時間、自動ジョブ再起動、自動ジョブ終了などの詳細情報が含まれます。
STORAGE-GRADES.XML	ストレージグレードID + ストレージグレード名 + ストレージノードID + ストレージノードパス	各ストレージノードに対応するストレージグレード定義ファイル。
SUMMARY-ATTRIBUTES.XML	グループOID + グループパス + サマリー属性ID + サマリー属性名 + 値 + インデックス + テーブルID + テーブル名	StorageGRID の使用状況情報を要約した高レベルのシステムステータスデータです。グリッド名、サイト名、グリッドごとおよびサイトごとのストレージノード数、ライセンスの種類、ライセンス容量と使用状況、ソフトウェアサポート条件、S3 操作の詳細などの情報を提供します。

ファイル名	フィールド	説明
SYSTEM-ALERTS.XML	名前 + 重要度 + ノード名 + アラートステータス + サイト名 + アラート発生時刻 + アラート解決時刻 + ルールID + ノードID + サイトID + ミュート済み + その他の注釈 + その他のラベル	StorageGRID システムの潜在的な問題を示す現在のシステムアラート。
USERAGENTS.XML	ユーザーエージェント + 日数 + HTTP リクエストの合計 + 取り込まれたバイトの合計 + 取得されたバイトの合計 + PUT リクエスト + GET リクエスト + DELETE リクエスト + HEAD リクエスト + POST リクエスト + OPTIONS リクエスト + 平均リクエスト時間 (ms) + 平均 PUT リクエスト時間 (ms) + 平均 GET リクエスト時間 (ms) + 平均 DELETE リクエスト時間 (ms) + 平均 HEAD リクエスト時間 (ms) + 平均 POST リクエスト時間 (ms) + 平均 OPTIONS リクエスト時間 (ms)	アプリケーションのユーザーエージェントに基づいた統計情報。例えば、ユーザーエージェントごとのPUT/GET/DELETE/HEAD操作の回数や、各操作の合計バイトサイズなど。
X-HEADER-DATA	X-Netapp-asup-generated-on + X-Netapp-asup-hostname + X-Netapp-asup-os-version + X-Netapp-asup-serial-num + X-Netapp-asup-subject + X-Netapp-asup-system-id + X-Netapp-asup-model-name	AutoSupport ヘッダーデータ。

StorageGRIDでAutoSupportを設定する

デフォルトでは、StorageGRID AutoSupport 機能は、StorageGRID を最初にインストールしたときに有効になります。ただし、各アプライアンスでハードウェア AutoSupport を設定する必要があります。必要に応じて、AutoSupport の設定を変更できます。

StorageGRID AutoSupport の設定を変更する場合は、プライマリ管理ノードでのみ変更を行ってください。各アプライアンスで [ハードウェア AutoSupport の設定](#) 必要があります。

開始する前に

- "[対応ウェブブラウザ](#)" を使用して Grid Manager にサインインしています。
- あなたは"[ルートアクセス権限](#)"があります。

- HTTPSを使用してAutoSupportパッケージを送信する場合は、直接または["プロキシ サーバを使用する"](#)を介して、プライマリ Admin ノードへのアウトバウンドインターネットアクセスを提供しています（受信接続は不要です）。
- StorageGRID の AutoSupport ページで HTTP を選択した場合、AutoSupport パッケージを HTTPS として転送するには ["プロキシ サーバを設定しました"](#) が必要です。NetApp の AutoSupport サーバは、HTTP を使用して送信されたパッケージを拒否します。
- SMTPをAutoSupportパッケージのプロトコルとして使用する場合は、SMTPメールサーバーを設定済みである必要があります。

タスク概要

以下のオプションを任意に組み合わせて、AutoSupport パッケージをテクニカルサポートに送信できます：

- 毎週：AutoSupport パッケージを週に1回自動的に送信します。デフォルト設定：有効。
- イベントトリガー：1時間ごと、または重大なシステムイベントの発生時に、AutoSupportパッケージを自動的に送信します。デフォルト設定：有効。
- オンデマンド：テクニカルサポートが StorageGRID システムに AutoSupport パッケージを自動的に送信するよう要求できます。これは、問題に積極的に取り組んでいるときに便利です（HTTPS AutoSupport 送信プロトコルが必要です）。デフォルト設定：無効。
- ユーザーによるトリガー：いつでも手動で AutoSupport パッケージを送信できます。
- ログ収集：["ログファイルとシステムデータを手動で収集し、AutoSupport パッケージを送信する"](#)

AutoSupport パッケージのプロトコルを指定します

以下のプロトコルのいずれかを使用して、AutoSupport パッケージを送信できます：

- **HTTPS:** これは新規インストール時のデフォルト設定であり、推奨設定です。このプロトコルはポート443を使用します。[AutoSupport のオンデマンド機能を有効にする](#)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、プロキシ サーバを設定してAutoSupportパッケージをHTTPSで転送する必要があります。NetAppのAutoSupportサーバはHTTPを使用して送信されたパッケージを拒否します。このプロトコルはポート80を使用します。
- **SMTP:** このオプションは、AutoSupport パッケージをメールで送信する場合に使用します。

設定したプロトコルは、あらゆる種類のAutoSupportパッケージの送信に使用されます。

手順

1. サポート > ツール > **AutoSupport** > 設定 を選択します。
2. AutoSupport パッケージの送信に使用するプロトコルを選択してください。
3. *HTTPS*を選択した場合は、テクニカルサポートサーバーへの接続を保護するためにNetAppサポート証明書（TLS証明書）を使用するかどうかを選択します。
 - 証明書の検証（デフォルト）：AutoSupportパッケージの送信が安全であることを確認します。NetApp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：証明書の検証を使用しない正当な理由がある場合（証明書に一時的な問題がある場合など）にのみ、このオプションを選択してください。

4. 「保存」を選択します。毎週送信されるパッケージ、ユーザーによってトリガーされるパッケージ、およびイベントによってトリガーされるパッケージはすべて、選択したプロトコルを使用して送信されます。

毎週のAutoSupportを無効化する

デフォルトでは、StorageGRID システムは週に一度、技術サポートに AutoSupport パッケージを送信するように設定されています。

週次のAutoSupportパッケージが送信されるタイミングを確認するには、**AutoSupport** > *結果*タブに移動してください。*週次AutoSupport*セクションで、*次回の予定時刻*の値を確認してください。

毎週の AutoSupport パッケ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. サポート > ツール > **AutoSupport** > 設定 を選択します。
2. **Enable Weekly AutoSupport** チェックボックスをオフにします。
3. * 保存 * を選択します。

イベントトリガー型 AutoSupport を無効にする

デフォルトでは、StorageGRID システムは、AutoSupport パッケージを1時間ごとにテクニカルサポートに送信するように設定されています。

イベントトリガーのAutoSupportはいつでも無効にすることができます。

手順

1. サポート > ツール > **AutoSupport** > 設定 を選択します。
2. イベントトリガー **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 * を選択します。

オンデマンド AutoSupport を有効にする

AutoSupport on Demand は、テクニカルサポートが現在対応中の問題の解決を支援することができます。

デフォルトでは、AutoSupport オンデマンド機能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がお客様の StorageGRID システムに AutoSupport パッケ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 オンデマンドクエリのポーリング時間間隔を設定することもできます。

テクニカルサポートでは、AutoSupport On Demand を有効または無効にすることはできません。

手順

1. サポート > ツール > **AutoSupport** > 設定 を選択します。
2. プロトコルとして **HTTPS** を選択してください。
3. 毎週 **AutoSupport** を有効にする チェックボックスをオンにします。
4. *AutoSupport On Demand を有効にする*チェックボックスを選択します。
5. * 保存 * を選択します。

AutoSupport on Demand が有効になっており、テクニカルサポートは AutoSupport on Demand リクエストを 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する

デフォルトでは、StorageGRID は NetApp に接続して、お使いのシステムで利用可能なソフトウェアアップデートがあるかどうかを確認します。StorageGRID の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、新しいバージョンは StorageGRID のアップグレードページに表示されます。

必要に応じて、ソフトウェアアップデートの確認を無効にすることもできます。たとえば、システムに WAN アクセスがない場合は、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してください。

手順

1. サポート > ツール > **AutoSupport** > 設定 を選択します。
2. 「ソフトウェアのアップデートを確認する」チェックボックスをオフにします。
3. * 保存 * を選択します。

追加の AutoSupport 送信先を追加する

AutoSupport を有効にすると、ヘルスおよびステータスパッケージがテクニカルサポートに送信されます。すべての AutoSupport パッケージに対して、追加の宛先を1つ指定できます。

AutoSupport パッケ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、[AutoSupport パッケージのプロトコルを指定する](#) の手順を参照してください。



SMTPプロトコルを使用して、AutoSupportパッケージを追加の宛先に送信することはできません。

手順

1. サポート > ツール > **AutoSupport** > 設定 を選択します。
2. 追加の **AutoSupport** 送信先を有効にする を選択します。
3. 以下を指定してください：

Hostname

追加の AutoSupport 宛先サーバーのホスト名または IP アドレス。



追加の宛先は1つだけ入力できます。

ポート

追加のAutoSupport宛先サーバー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

追加の接続先への接続を保護するためにTLS証明書が使用されているかどうか。

- 証明書の検証を行うには、*証明書の検証*を選択してください。
- 証明書の検証なしで AutoSupport パッケージを送信するには、「証明書を検証しない」を選択して

ください。

証明書の検証を使用しない正当な理由がある場合（証明書に一時的な問題がある場合など）にのみ、このオプションを選択してください。

4. *証明書の検証*を選択した場合は、以下の手順を実行してください。

- a. CA証明書の保存場所を参照します。
- b. CA証明書ファイルをアップロードします。

CA証明書のメタデータが表示されます。

5. *保存*を選択します。

今後のすべての週次、イベントトリガー、およびユーザートリガーのAutoSupportパッケージは、追加の宛先に送信されます。

アプライアンスの **AutoSupport** を設定する

AutoSupport（アプライアンス用）はStorageGRIDのハードウェアの問題を報告し、StorageGRID AutoSupportはStorageGRIDのソフトウェアの問題を報告します。ただし、例外が1つあります。SGF6112の場合、StorageGRID AutoSupportはハードウェアとソフトウェアの両方の問題を報告します。SGF6112を除く各アプライアンスでAutoSupportを設定する必要があります。SGF6112は追加の設定を必要としません。AutoSupportは、サービスアプライアンスとストレージアプライアンスとで実装方法が異なります。

SANtricity を使用して、各ストレージアプライアンスの AutoSupport を有効にします。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インストール後に設定できます：

- SG6000およびSG5700アプライアンスの場合、"[SANtricity System Manager で AutoSupport を設定する](#)"

EシリーズアプライアンスのAutoSupportパッケージは、"[SANtricity System Manager](#)"でプロキシによるAutoSupport配信を設定した場合、StorageGRIDのAutoSupportに含めることができます。

StorageGRID AutoSupport は、DIMM やホスト インターフェイス カード（HIC）の障害などのハードウェアの問題を報告しません。ただし、一部のコンポーネントの障害により、"[ハードウェアアラート](#)" がトリガーされる場合があります。ベースボード管理コントローラー（BMC）を搭載した StorageGRID アプライアンスでは、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：

- "[BMC アラートのメール通知を設定する](#)"
- "[BMCのSNMP設定を構成する](#)"

関連情報

["NetAppサポート"](#)

StorageGRIDでAutoSupportパッケージを手動でトリガーする

技術サポートがお客様の StorageGRID システムの問題のトラブルシューティングを支援できるよう、AutoSupport パッケージを手動でトリガーして送信することができます。

開始する前に

- "対応ウェブブラウザ" を使用して Grid Manager にサインインしています。
- ルートアクセス権限、またはその他のグリッド構成権限をお持ちです。

手順

1. サポート > ツール > **AutoSupport** を選択します。
2. *アクション*タブで、*ユーザー起動のAutoSupportの送信*を選択します。

StorageGRID は、AutoSupport パッケージを NetApp Support Site に送信しようとします。試行が成功した場合、「結果」タブの「最新の結果」と「最終成功時刻」の値が更新されます。問題が発生した場合、「最新の結果」の値は「失敗」に更新され、StorageGRID は AutoSupport パッケージの再送信を試みません。

3. 1分後にブラウザでAutoSupportページを更新すると、最新の結果にアクセスできます。



さらに、"より詳細なログファイルとシステムデータを収集する"して、NetApp Support Siteに送信することができます。

StorageGRID AutoSupport パッケージのトラブルシューティング

AutoSupportパッケージの送信に失敗した場合、StorageGRIDシステムはAutoSupportパッケージのタイプに応じて異なるアクションを実行します。AutoSupportパッケージのステータスを確認するには、サポート > ツール > **AutoSupport** > *結果*を選択します。

AutoSupport パッケージの送信に失敗すると、**AutoSupport** ページの「結果」タブに「失敗」と表示されます。



AutoSupportパッケージをNetAppに転送するようにプロキシ サーバを構成した場合は、"プロキシ サーバの設定が正しいことを確認してください"する必要があります。

毎週のAutoSupportパッケージエラー

週次のAutoSupportパッケージの送信に失敗した場合、StorageGRID システムは次のアクションを実行します：

1. 「最新の結果」属性を「再試行中」に更新します。
2. AutoSupport パッケージの再送信を、1時間にわたって4分ごとに15回試みます。
3. 送信失敗が1時間続いた場合、「最新の結果」属性を「失敗」に更新します。
4. 次の予定時刻に AutoSupport パッケージの再送信を試みます。
5. NMS サービスが利用できないためにパッケージの送信が失敗した場合、および 7 日以内にパッケージが送信された場合は、定期的な AutoSupport スケジュールを維持します。
6. NMS サービスが再び利用可能になると、7日以上パッケージが送信されていない場合は、AutoSupport パッケージを直ちに送信します。

ユーザーによるトリガーまたはイベントによるトリガーのAutoSupportパッケージエラー

ユーザーによるトリガーまたはイベントによるトリガーの AutoSupport パッケージの送信に失敗した場合、StorageGRID システムは次のアクションを実行します。

1. 既知のエラーの場合は、エラーメッセージを表示します。例えば、ユーザーが正しいメール設定を入力せずに 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 packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.
2. パッケージの再送信は試みません。
3. エラーを `nms.log` に記録します。

障害が発生し、SMTP が選択されているプロトコルである場合は、StorageGRID システムのメールサーバーが正しく設定されており、メールサーバーが稼働していることを確認してください（サポート > アラーム（レガシー） > レガシーメールの設定）。次のエラーメッセージが AutoSupport ページに表示される場合があります： AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.

["メールサーバーの設定を構成する"](#)方法をご確認ください。

AutoSupport パッケージの障害を修正する

障害が発生し、SMTPが選択されているプロトコルである場合は、StorageGRIDシステムのメールサーバーが正しく設定されており、メールサーバーが稼働していることを確認してください。次のエラーメッセージが AutoSupport ページに表示される場合があります： AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.

StorageGRID を経由して Eシリーズ AutoSupport パッケージを送信する

Eシリーズ SANtricity System ManagerのAutoSupportパッケージは、ストレージアプライアンスの管理ポートではなく、StorageGRIDの管理ノードを経由して技術サポートに送信できます。

AutoSupport を E シリーズアプライアンスで使用方法の詳細については、["EシリーズハードウェアAutoSupport"](#)を参照してください。

開始する前に

- Grid Managerに["対応ウェブブラウザ"](#)を使用してサインインしています。
- あなたは["ストレージアプライアンス管理者またはルートアクセス権限"](#)を持っています。
- SANtricity AutoSupport を設定しました：
 - SG6000およびSG5700アプライアンスの場合、["SANtricity System Manager で AutoSupport を設定する"](#)



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。

タスク概要

EシリーズのAutoSupportパッケージにはストレージ ハードウェアの詳細が含まれており、StorageGRIDシステムから送信される他のAutoSupportパッケージよりも具体的です。

SANtricity System Manager で特別なプロキシ サーバ アドレスを設定することで、アプライアンスの管理ポートを使用せずに StorageGRID 管理ノードを経由して AutoSupport パッケージを送信できます。この方法で送信された AutoSupport パッケージは ["優先送信者 管理ノード"](#) によって送信され、Grid Manager で設定された

すべての "管理者プロキシ設定" が使用されます。

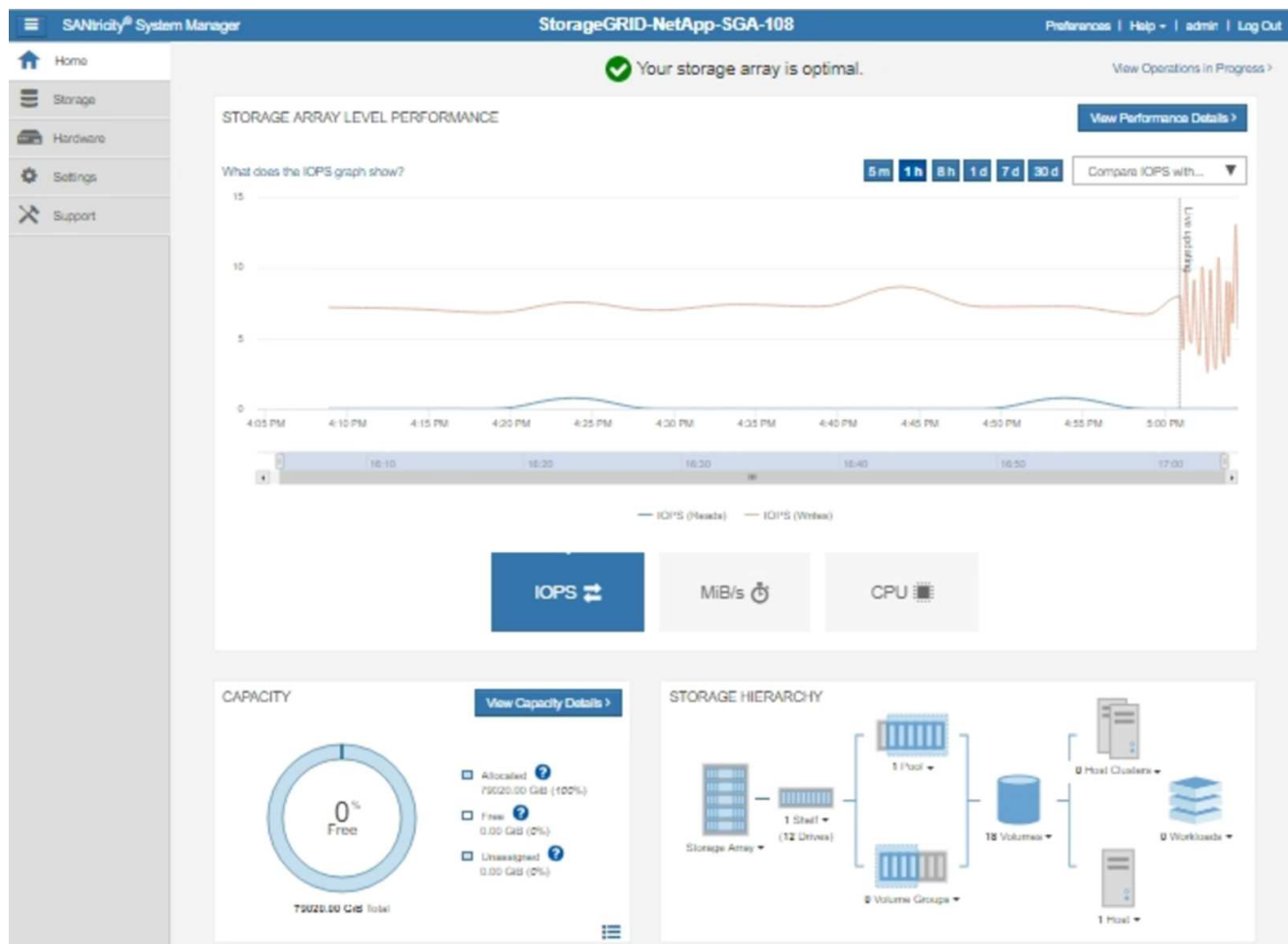


この手順は、EシリーズAutoSupportパッケージ用のStorageGRIDプロキシ サーバを設定する場合にのみ使用します。EシリーズAutoSupport設定の詳細については、"[NetApp EシリーズおよびSANtricityドキュメント](#)"を参照してください。

手順

1. Grid Managerで、*Nodes*を選択します。
2. 左側のノード一覧から、設定するストレージアプライアンスノードを選択してください。
3. **SANtricity System Manager** を選択します。

SANtricity System Manager の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 の操作ページが表示されます。

Technical Support

Chassis serial number: 031517000693

NetApp My Support

US/Canada 888.463.8277

Other Contacts

Support Resources

Diagnostics

AutoSupport

AutoSupport operations

AutoSupport status: Enabled

Enable/Disable AutoSupport Features

AutoSupport proactively monitors the health of your storage array and automatically sends support data ("dispatches") to the support team.

Configure AutoSupport Delivery Method

Connect to the support team via HTTPS, HTTP or Mail (SMTP) server delivery methods.

Schedule AutoSupport Dispatches

AutoSupport dispatches are sent daily at 03:06 PM UTC and weekly at 07:39 AM UTC on Thursday.

Send AutoSupport Dispatch

Automatically sends the support team a dispatch to troubleshoot system issues without waiting for periodic dispatches.

View AutoSupport Log

The AutoSupport log provides information about status, dispatch history, and errors encountered during delivery of AutoSupport dispatches.

Enable AutoSupport Maintenance Window

Enable AutoSupport Maintenance window to allow maintenance activities to be performed on the storage array without generating support cases.

Disable AutoSupport Maintenance Window

Disable AutoSupport Maintenance window to allow the storage array to generate support cases on component failures and other destructive actions.

5. *AutoSupport配信方法の設定*を選択します。

AutoSupport の配信方法の設定ページが表示されます。

Configure AutoSupport Delivery Method

Select AutoSupport dispatch delivery method...

☒ HTTPS

☐ HTTP

☐ Email

HTTPS delivery settings

Show destination address

Connect to support team...

☐ Directly ?

☒ via Proxy server ?

Host address ?

tunnel-host

Port number ?

10225

☐ My proxy server requires authentication

☐ via Proxy auto-configuration script (PAC) ?

Save

Test Configuration

Cancel

6. 配信方法として「HTTPS」を選択してください。



HTTPSを有効にする証明書はプリインストールされています。

7. 「プロキシ サーバ経由」を選択してください。

8. *ホストアドレス*に `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 パッケージを送信するための特別なアドレスです。

9. *ポート番号*に `10225` を入力します。

`10225` は、アプライアンス内の E シリーズコントローラーから AutoSupport パッケージを受信する StorageGRID プロキシ サーバのポート番号です。

10. 「Test Configuration」を選択して、AutoSupport プロキシ サーバのルーティングと設定をテストします。

正しい場合は、緑色のバナーにメッセージが表示されます：「AutoSupportの構成が検証されました。」

テストが失敗すると、赤いバナーにエラーメッセージが表示されます。StorageGRIDのDNS設定とネットワークを確認し、["優先送信者 管理ノード"](#)がNetApp Support Siteに接続できることを確認して、もう一度テストを実行してください。

11. * 保存 * を選択します。

設定が保存され、確認メッセージが表示されます：「AutoSupport の配信方法が設定されました。」

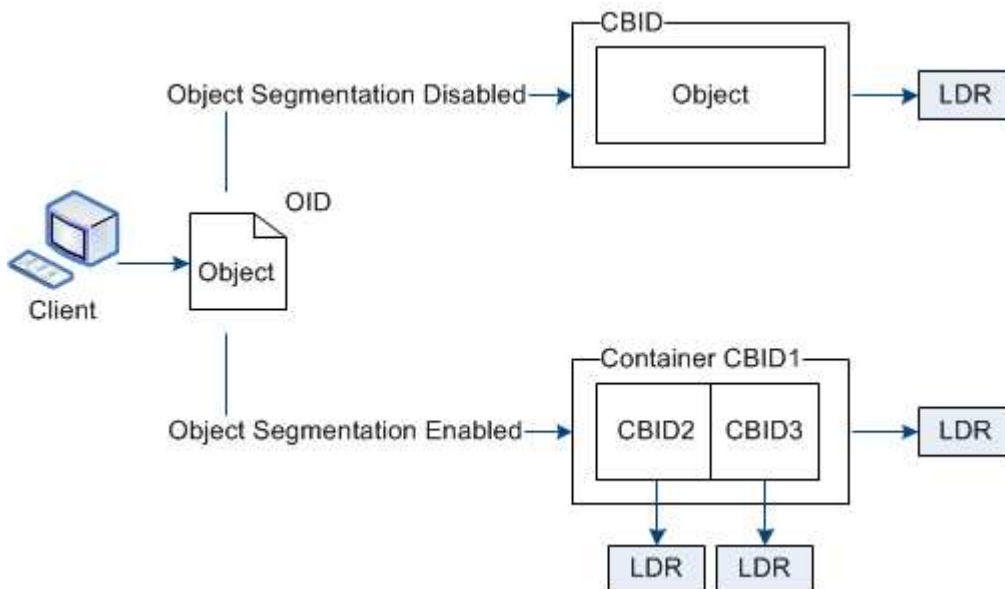
ストレージノードの管理

ストレージオプションを使用する

StorageGRIDのオブジェクトセグメンテーションについて学ぶ

オブジェクト分割とは、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ために、オブジェクトを複数の小さな固定サイズのオブジェクトに分割するプロセスです。S3のマルチパートアップロードでは、各パートを表すオブジェクトが作成される、セグメント化されたオブジェクトも作成されます。

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リスト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取得すると、LDRサービスはそのセグメントから元のオブジェクトを組み立て、クライアントにオブジェクトを返します。

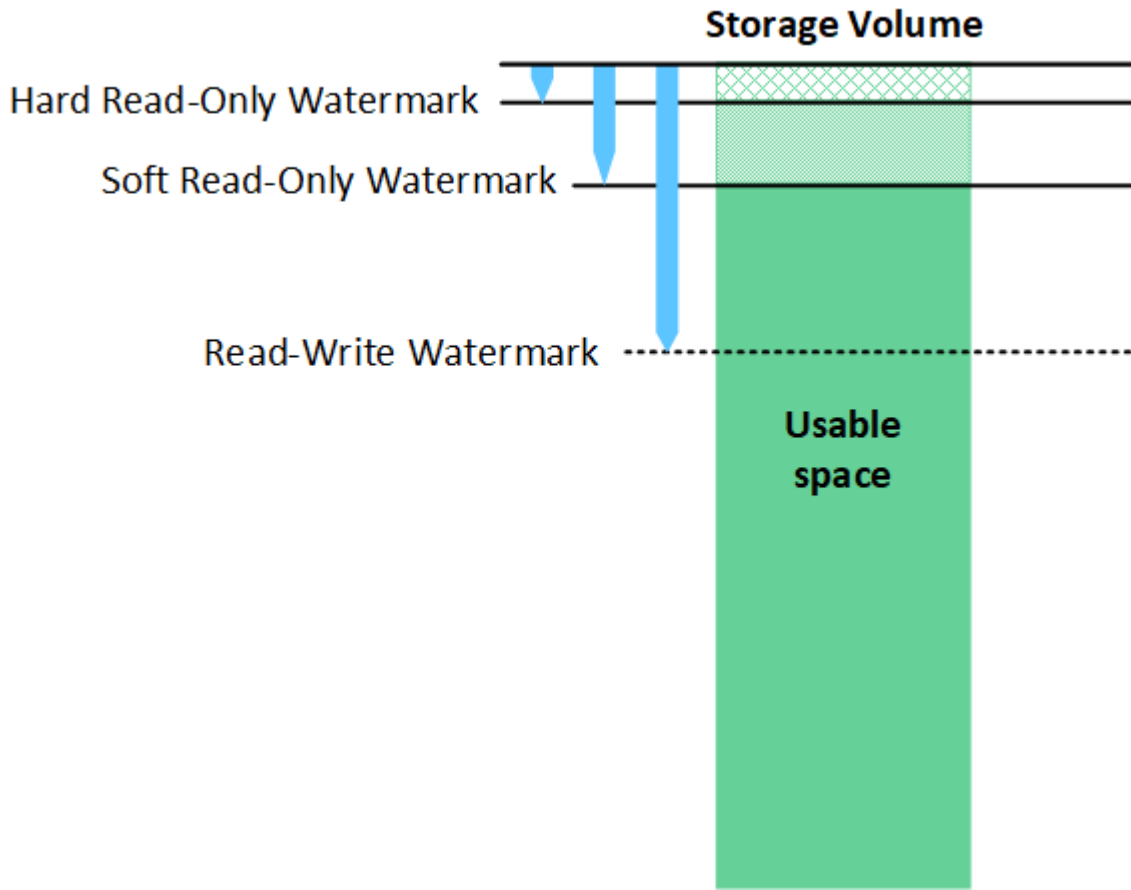
コンテナとセグメントは、必ずしも同じストレージノードに保存されるとは限りません。コンテナとセグメントは、ILMルールで指定されたストレージプール内の任意のストレージノードに保存できます。

各セグメントは StorageGRID システムによって独立して処理され、管理対象オブジェクトや保存済みオブジェクトなどの属性のカウントに反映されます。たとえば、StorageGRID システムに保存されたオブジェクトが2つのセグメントに分割された場合、取り込み完了後に管理対象オブジェクトの値は次のように3つ増加します：

segment container + segment 1 + segment 2 = three stored objects

StorageGRIDのストレージボリュームのウォーターマークについて学ぶ

StorageGRID は 3 つのストレージボリュームウォーターマークを使用して、ストレージノードの空き容量が極端に少なくなる前に安全に読み取り専用状態に移行し、読み取り専用状態に移行したストレージノードが再び読み書き可能になるようにします。



ストレージ容量の透かしは、複製されたオブジェクトデータおよび消去符号化されたオブジェクトデータに使用される領域にのみ適用されます。ボリューム0上のオブジェクトメタデータ用に確保されている領域については、"[オブジェクトメタデータストレージの管理](#)"を参照してください。

ソフト読み取り専用ウォーターマークとは何ですか？

ストレージボリュームのソフト読み取り専用ウォーターマークは、ストレージノードのオブジェクトデータ用の使用可能領域がいっぱいになりつつあ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容量が、そのボリュームのソフト読み取り専用ウォーターマークよりも少ない場合、ストレージノードは読み取り専用モードに移行します。読み取り専用モードとは、ストレージノードが StorageGRID システムの他のノードに読み取り専用サービスをアダプタイズしながら、保留中の書き込み要求をすべて処理することを意味します。

例えば、ストレージノード内の各ボリュームに、10 GBのソフト読み取り専用ウォーターマークが設定されているとします。各ボリュームの空き容量が10 GB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。

ハード読み取り専用ウォーターマークとは何ですか？

*ストレージボリュームのハード読み取り専用ウォーターマーク*は、ノードのオブジェクトデータ用の使用可能な領域がいっぱいになりつつあることを示す次のウォーターマークです。

ボリュームの空き容量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を下回る場合、その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容量がハード読み取り専用ウォーターマークを下回るまで継続できます。

例えば、ストレージノード内の各ボリュームに、5 GB の読み取り専用ハードウォーターマークが設定されているとします。各ボリュームの空き容量が 5 GB 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。

ハード読み取り専用ウォーターマークは、ソフト読み取り専用ウォーターマークよりも常に小さくなります。

読み取り/書き込みウォーターマークとは何ですか？

*ストレージボリュームの読み取り/書き込みウォーターマーク*は、読み取り専用モードに移行したストレージノードにのみ適用されます。これは、ノードが再び読み取り/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容量が、そのボリュームの読み取り/書き込みウォーターマークを超えると、ノードは自動的に読み取り/書き込み状態に戻ります。

例えば、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、各ボリュームの読み書きウォーターマークが 30 GB であると仮定します。いずれかのボリュームの空き容量が 30 GB に増加すると、ノードは再び読み書き可能になります。

読み取り/書き込みウォーターマークは、ソフト読み取り専用ウォーターマークとハード読み取り専用ウォーターマークの両方よりも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

現在の透かし設定とシステム最適化値を確認できます。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、または調整すべきかどうかを判断できます。

開始する前に

- StorageGRID 11.6以降へのアップグレードが完了しました。
- ["対応ウェブブラウザ"](#) を使用して Grid Manager にサインインしています。
- あなたは["ルートアクセス権限"](#)があります。

現在の透かし設定を表示する

グリッドマネージャーで、現在のストレージウォーターマーク設定を確認できます。

手順

1. サポート > その他 > ストレージの透かし を選択します。
2. ストレージのウォーターマークページで、「最適化された値を使用する」チェックボックスを確認してください。
 - チェックボックスが選択されている場合、3つのウォーターマークはすべて、Storage Node のサイズ

とボリュームの相対的な容量に基づいて、各 Storage Node 上の各ストレージボリュームに合わせて最適化されます。

これはデフォルト設定であり、推奨設定です。これらの値を更新しないでください。オプションで、[最適化されたストレージウォーターマークを表示する](#)。

- 。「最適化された値を使用する」チェックボックスが選択されていない場合、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。カスタムウォーターマーク設定の使用は推奨されません。["読み取り専用ウォーターマークの低オーバーライドアラートのトラブルシューティング"](#)の手順に従って、設定を調整できるかどうか、または調整すべきかどうかを判断してください。

カスタム透かし設定を指定する場合は、0より大きい値を入力する必要があります。

最適化されたストレージウォーターマークの表示

StorageGRID は、2 つの Prometheus メトリックを使用して、ストレージボリュームのソフト読み取り専用ウォーターマークに対して計算された最適化された値を表示します。グリッド内の各ストレージノードについて、最適化された最小値と最大値を確認できます。

1. サポート > ツール > メトリクス を選択します。
2. Prometheusセクションで、リンクを選択してPrometheusユーザーインターフェイスにアクセスします。
3. 推奨される最小ソフト読み取り専用ウォーターマークを確認するには、次の Prometheus メトリックを入力し、**Execute** を選択してください。

```
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おける、ソフト読み取り専用ウォーターマークの最小最適化値が表示されます。この値がストレージボリュームのソフト読み取り専用ウォーターマークのカスタム設定値よりも大きい場合、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. 推奨される最大ソフト読み取り専用ウォーターマークを確認するには、次の Prometheus メトリックを入力し、**Execute** を選択してください。

```
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おける、ソフト読み取り専用ウォーターマークの最大最適化値が表示されます。

StorageGRID でのオブジェクト メタデータ ストレージの管理

StorageGRID システムのオブジェクトメタデータ容量は、そのシステムに保存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保存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どこにどのように保存するか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何ですか？

オブジェクトのメタデータとは、オブジェクトを説明するあらゆる情報のことです。StorageGRID は、オブジェクトのメタデータを使用して、グリッド全体にわたるすべてのオブジェクトの位置を追跡し、各オブジェ

クトのライフサイクルを長期にわたって管理します。

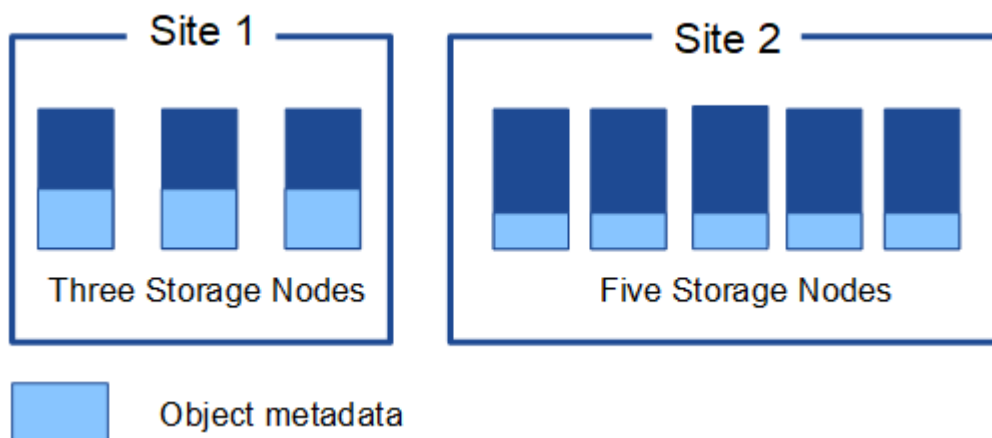
StorageGRID のオブジェクトのメタデータには、次の種類の情報が含まれます：

- ・ システムメタデータには、各オブジェクトの一意のID（UUID）、オブジェクト名、S3バケット名、テナントアカウント名またはID、オブジェクトの論理サイズ、オブジェクトが最初に作成された日時、およびオブジェクトが最後に変更された日時が含まれます。
- ・ オブジェクトに関連付けられた、ユーザー独自の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。
- ・ 複製されたオブジェクトのコピーの場合、各コピーの現在の保存場所。
- ・ 消去符号化された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、外部バケット名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およびマルチパートオブジェクトの場合、セグメント識別子とデータサイズ。

オブジェクトのメタデータはどのように保存されますか？

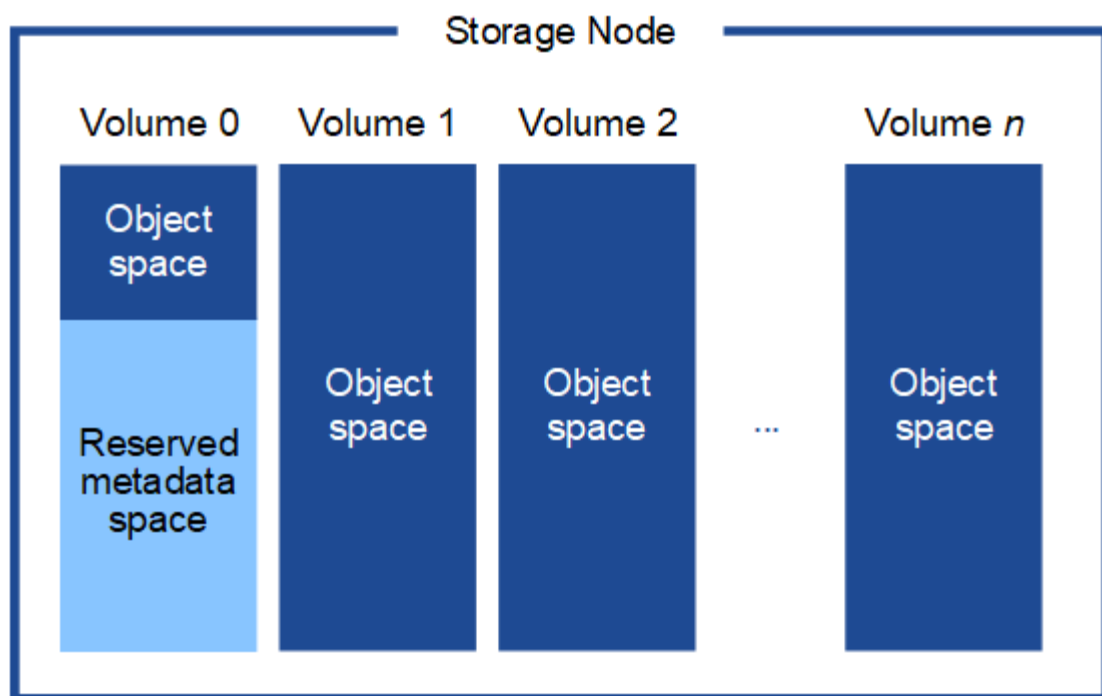
StorageGRID は、オブジェクトのメタデータを Cassandra データベースに保持します。このメタデータは、オブジェクトデータとは独立して保存されます。冗長性を確保し、オブジェクトのメタデータを損失から保護するために、StorageGRID はシステム内のすべてのオブジェクトのメタデータのコピーを各サイトに 3 つ保存します。

この図は、2つのサイトにあるストレージノードを表しています。各サイトは同じ量のオブジェクトメタデータを保持しており、各サイトのメタデータはそのサイト内のすべてのストレージノードに分割されています。



オブジェクトのメタデータはどこに保存されますか？

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リザーブ スペースを確保します。このリザーブ スペースは、オブジェクトメタデータの保存および重要なデータベース操作の実行に使用されます。ストレージボリューム 0 の残りの空き容量およびストレージノード内の他のすべてのストレージボリュームは、オブジェクトデータ（レプリケートされたコピーおよびイレイジャーコーディングされたフラグメント）専用に使

用されます。特定のストレージノード上でオブジェクトメタデータ用に確保される容量は、いくつかの要因によって決まります。それらの要因については、以下で説明します。

メタデータリザーブ スペース設定

Metadata reserved space は、システム全体の設定であり、各ストレージノードのボリューム 0 にメタデータ用に予約される領域の量を表します。表に示すように、この設定のデフォルト値は以下に基づいています：

- 最初に StorageGRID をインストールしたときに使用していたソフトウェアのバージョン。
- 各ストレージノードに搭載されているRAMの容量。

初期 StorageGRID インストールに使用されたバージョン	ストレージノードの RAM 容量	デフォルトのメタデータリザーブ スペース設定
11.5～12.0	グリッド内の各ストレージノード に128 GB以上	8 TB (8,000 GB)
	グリッド内のどのストレージノードでも128GB未満	3 TB (3,000 GB)
11.1～11.4	いずれのサイトにおいても、各ストレージノードに128GB以上の容量が必要	4 TB (4,000 GB)

初期 StorageGRID インストールに使用されたバージョン	ストレージノードの RAM 容量	デフォルトのメタデータリザーブ スペース設定
	各サイトのいずれかのストレージ ノードで128 GB未満	3 TB (3,000 GB)
11.0以前	任意の金額	2 TB (2,000 GB)

メタデータのリザーブ スペース設定の表示

StorageGRID システムのメタデータ リザーブ スペース設定を表示するには、以下の手順に従ってください。

手順

1. **Configuration > System > Storage settings** を選択します。
2. ストレージ設定ページで、メタデータ リザーブ スペース セクションを展開します。

StorageGRID 11.8以降では、メタデータのリザーブ スペース値は100 GB以上1 PB以下である必要があります。

各ストレージノードに 128 GB 以上の RAM が搭載されている新しい StorageGRID 11.6 以降のインストール環境のデフォルト設定は、8,000 GB（8 TB）です。

メタデータの実際のリザーブ スペース

システム全体のメタデータ リザーブ スペース設定とは対照的に、オブジェクトメタデータの_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。任意のストレージノードの場合、メタデータの実際のリザーブ 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メタデータ リザーブ スペース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	メタデータの実際のリザーブ スペース
500 GB未満（非本番環境使用）	ボリューム0の10%
500 GB以上 + または + メタデータ専用ストレージノード	これらの値のうち小さい方： • ボリューム0 • メタデータリザーブ スペース設定 注：メタデータ専用のストレージノードには、rangedb が 1 つだけ必要です。

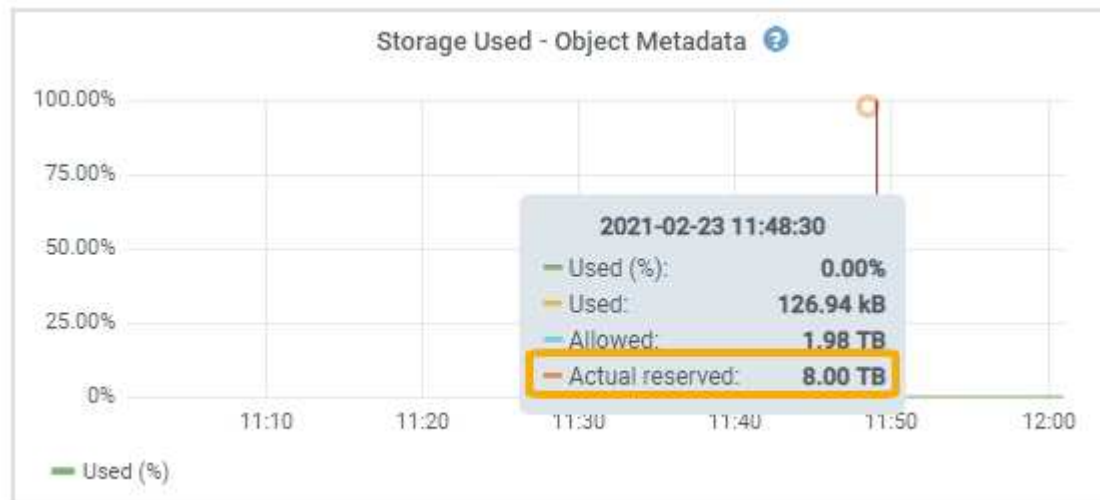
メタデータの実際のリザーブ スペースを表示する

特定のストレージノードのメタデータに対する実際のリザーブ スペースを表示するには、次の手順に従います。

手順

1. グリッドマネージャから、「ノード」>「ストレージノード」を選択します。

2. 「ストレージ」タブを選択します。
3. カーソルを「ストレージ使用量 - オブジェクトメタデータ」チャートの上に移動し、*実際の予約済み*の値を確認します。



スクリーンショットでは、*実際の予約済み*の値は 8 TB です。このスクリーンショットは、新しい StorageGRID 11.6 インストールにおける大規模ストレージノードのもので、システム全体のメタデータリザーブスペース設定がこのストレージノードのボリューム 0 より小さいため、このノードの実際のリザーブスペースはメタデータリザーブスペース設定と等しくなります。

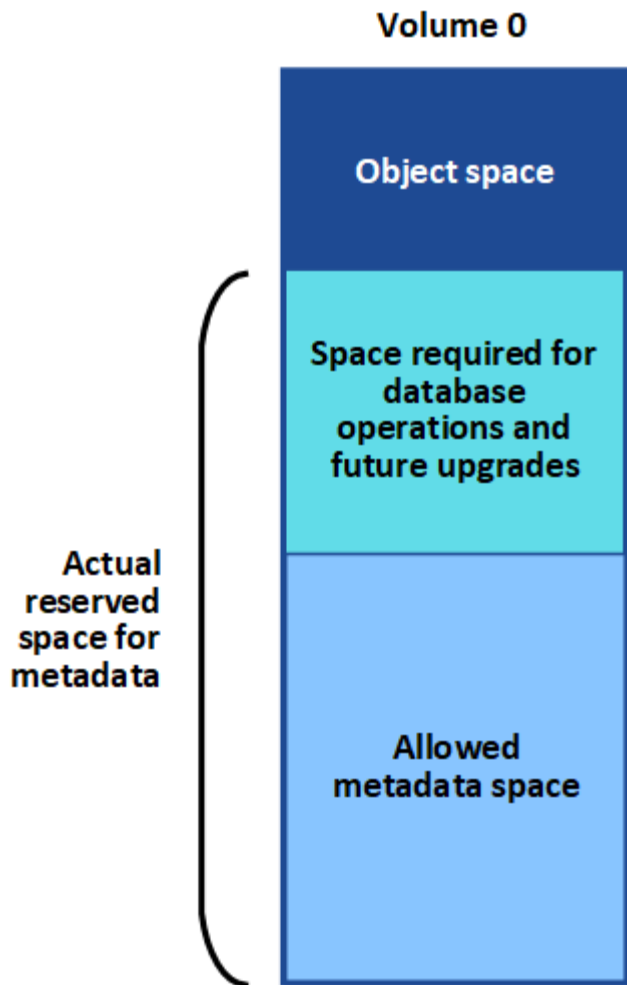
実際のリザーブスペース（メタデータ）の例

バージョン11.7以降を使用して新しい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に128 GBを超えるRAMが搭載されており、ストレージノード1（SN1）のボリューム0が6 TBであると仮定します。これらの値に基づく：

- ・システム全体のメタデータリザーブスペースは 8 TB に設定されています。（これは、各ストレージノードの RAM が 128 GB を超える場合に、新規 StorageGRID 11.6 以降のインストールに適用されるデフォルト値です。）
- ・SN1 のメタデータの実際のリザーブスペースは 6 TB です。（ボリューム 0 が「メタデータのリザーブスペース」設定よりも小さいため、ボリューム全体がリザーブされています。）

許可されたメタデータ領域

各ストレージノードのメタデータ用の実際のリザーブスペースは、オブジェクトメタデータに使用可能な領域（許可されたメタデータ領域）と、データベースの基本的な操作（圧縮や修復など）および将来のハードウェアとソフトウェアのアップグレードに必要な領域に細分化されます。許可されるメタデータ領域によって、オブジェクト全体の容量が決まります。



次の表は、ノードのメモリ量とメタデータの実際のリザーブ スペースに基づいて、StorageGRID がさまざまなストレージノードの*許可されたメタデータスペース*をどのように計算するかを示しています。

	ストレージノード上のメモリ容量		
	< 128 GB	>= 128 GB	メタデータ用の実際のリザーブ スペース
≤ 4 TB	メタデータ用の 実際のリザーブ スペースの60% (最大1.32 TB)	メタデータ用の実際のリザーブ ス ペースの60% (最大1.98 TB)	4 TB

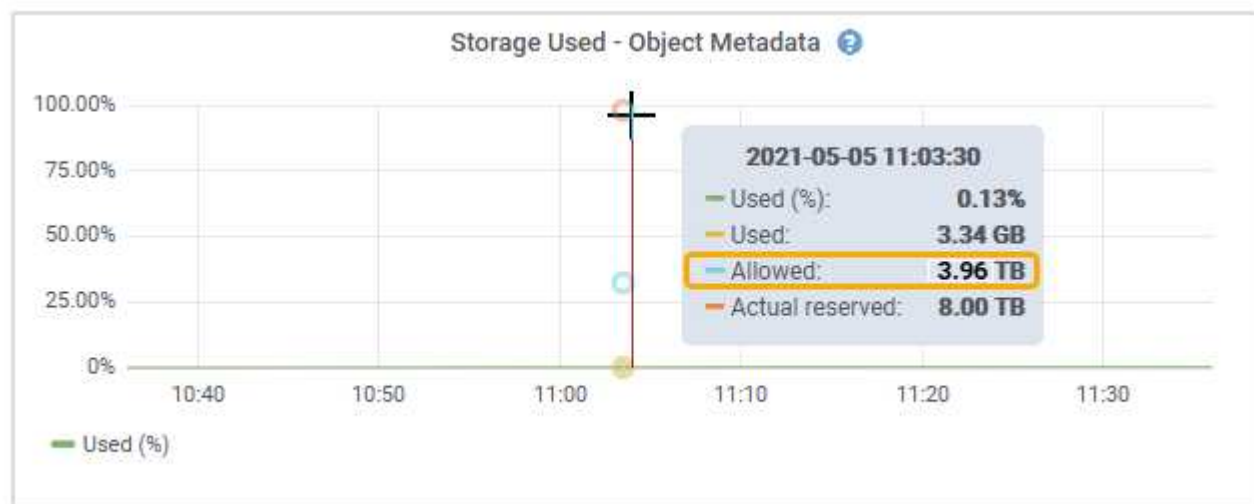
許可されているメタデータスペースを表示する

ストレージノードに許可されているメタデータ領域を確認するには、以下の手順に従ってください。

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. カーソルを「ストレージ使用量 - オブジェクトメタデータ」チャートの上に移動し、*許可*の値を確認します。



スクリーンショットでは、*許可*の値は 3.96 TB です。これは、メタデータの実際のリザーブ スペースが 4 TB を超えるストレージノードの最大値です。

「許可」の値は、この Prometheus メトリックに対応します：

`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に 128 GB を超える RAM が搭載されており、ストレージノード 1 (SN1) のボリューム 0 が 6 TB であると仮定します。これらの値に基づくと：

- ・システム全体のメタデータリザーブスペースは 8 TB に設定されています。（これは、各ストレージノードの RAM が 128 GB を超える場合の StorageGRID 11.6 以降のデフォルト値です。）
- ・SN1 のメタデータの実際のリザーブスペースは 6 TB です。（ボリューム 0 が「メタデータのリザーブスペース」設定よりも小さいため、ボリューム全体がリザーブされています。）
- ・SN1 のメタデータに許可される容量は 3 TB です。これは [メタデータに許可されるスペースの表](#) に示す計算式に基づいています：（メタデータの実際のリザーブスペース - 1 TB）× 60%、最大 3.96 TB まで。

ストレージノードのサイズの違いがオブジェクト容量に与える影響

上記のように、StorageGRID は各サイトのストレージノード全体にオブジェクトのメタデータを均等に分散します。このため、サイト内にサイズの異なるストレージノードが存在する場合、サイト内の最小サイズのノードがサイトのメタデータ容量を決定します。

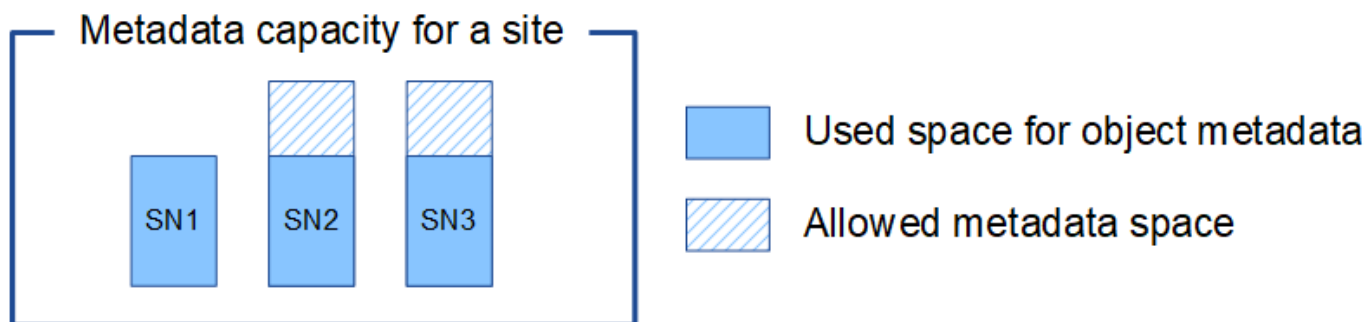
次の例を考えてみましょう。

- ・異なるサイズのストレージノードが3つ含まれる、単一サイトのグリッド環境があります。

- *メタデータ リザーブ スペース*の設定は 4 TB です。
- ストレージノードには、実際のリザーブ スペースのメタデータと許可されたメタデータ領域について、以下の値が設定されます。

ストレージ ノード	ボリュームサイズ 0	実際のリザーブ スペース（メタデータ）	許可されたメタデータ領域
SN1を使用したチャンク アップロード署名要求が サポートされるようになりました。	2.2 TB	2.2 TB	1.32 TB
SN2を使用したチャンク アップロード署名要求が サポートされるようになりました。	5 TB	4 TB	1.98 TB
SN3を使用したチャンク アップロード署名要求が サポートされるようになりました。	6 TB	4 TB	1.98 TB

オブジェクトのメタデータはサイト内のストレージノード全体に均等に分散されるため、この例では各ノードが保持できるメタデータは1.32 TBまでとなります。SN2およびSN3に許可されている追加の0.66 TBのメタデータ領域は使用できません。



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保持するため、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によって決まります。

オブジェクトのメタデータ容量がオブジェクトの最大数を制御するため、いずれかのノードのメタデータ容量が不足すると、グリッドは事実上満杯になります。

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、"[StorageGRID の監視](#)"の手順を参照してください。
- システムのオブジェクトメタデータ容量を増やすには、新しいストレージノードを追加することで"[グリッドを拡張する](#)"。

StorageGRID でメタデータ予約領域の設定を増やす

ストレージノードが特定の RAM および空き容量要件を満たしている場合、メタデータ予約領域のシステム設定を増やすことができます。

要件

- ["対応ウェブブラウザ"](#) を使用して Grid Manager にサインインしています。
- あなたは["ルートアクセス権限、またはその他のグリッド構成権限"](#)があります。

タスク概要

システム全体のメタデータ予約領域の設定を、手動で最大 8 TB まで増やすことができます。

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るのは、以下の2つの条件が両方とも満たされている場合のみです。

- お客様のシステム内のどのサイトにあるストレージノードも、それぞれ128 GB以上のRAMを搭載しています。
- 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。

この設定値を上げると、同時にすべてのストレージノードのストレージボリューム 0 におけるオブジェクトストレージに使用できる容量が減少することに注意してください。そのため、想定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 より小さい値に設定することをお勧めします。



一般的には、低い値よりも高い値を使用の方が適切です。メタデータ予約領域の設定値が大きすぎる場合は、後で小さくすることができます。一方、後で値を増やすと、システムは空き容量を確保するために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の設定が、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についての詳細な説明については、["オブジェクトメタデータストレージの管理"](#)を参照してください。

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. **Configuration > System > Storage settings** を選択します。
 - b. *メタデータ予約領域*の値を確認してください。
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* 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てください。
 - 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** というエントリを探します。
 - e. 利用可能な値が、使用したい新しい値と現在のメタデータ予約領域の値との差以上であることを確認してください。

例えば、メタデータ予約領域の設定が現在 4 TB で、それを 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てください。

- 1つ以上のストレージノードに十分な空き容量がない場合、メタデータ予約容量の値を増やすことはできません。この手順を続行しないでください。
- 各ストレージノードのボリューム0に十分な空き容量がある場合は、次のステップに進みます。

3. 各ストレージノードには、少なくとも128 GB のRAMが搭載されていることを確認してください。

- * Nodes * を選択します。
- グリッド内の最初のストレージノードを選択してください。
- 「ハードウェア」タブを選択します。
- メモリ使用量グラフにカーソルを合わせてください。*合計メモリ*が 128 GB 以上であることを確認してください。
- 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てください。
 - 1つ以上のストレージノードに十分な合計メモリ容量がない場合、メタデータ予約領域の値を増やすことはできません。この手順を続行しないでください。
 - 各ストレージノードの合計メモリ容量が128 GB以上であれば、次のステップに進みます。

4. メタデータ予約領域の設定を更新します。

- Configuration > System > Storage settings** を選択します。
- 「Metadata Reserved Space」を選択してください。
- 新しい値を入力してください。

例えば、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の後にゼロが12個続く）と入力します。

- * 保存 * を選択します。

StorageGRID に保存されたオブジェクトを圧縮

オブジェクト圧縮を有効にすると、StorageGRID に保存されるオブジェクトのサイズを縮小し、オブジェクトが消費するストレージ容量を削減できます。

開始する前に

- ["対応ウェブブラウザ"](#) を使用して Grid Manager にサインインしています。
- ["特定のアクセス権限"](#) があります。

タスク概要

デフォルトでは、オブジェクト圧縮は無効になっています。圧縮を有効にすると、StorageGRID は保存時に各オブジェクトを圧縮しようと試み、その際にロスレス圧縮を使用します。



この設定を変更した場合、新しい設定が適用されるまで約1分かかります。設定された値は、パフォーマンスとスケーリングのためにキャッシュされます。

オブジェクト圧縮を有効にする前に、以下の点にご注意ください。

- 保存す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、*保存されたオブジェクトを圧縮する*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、保存前にオブジェクトを圧縮する場合があります。クライアントアプリケーションが StorageGRID にオブジェクトを保存する前に既に圧縮している場合、このオプションを選択しても、オブジェクトのサイズはそれ以上縮小されません。
- NetApp FabricPool と StorageGRID を使用している場合は、「保存されたオブジェクトを圧縮する」を選択しないでください。
- 「保存されたオブジェクトを圧縮する」が選択されている場合、S3クライアントアプリケーションは、返されるバイト範囲を指定するGetObject操作の実行を避ける必要があります。これらの「範囲読み取り」操作は非効率的です。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実質的に解凍する必要があるためです。非常に大きなオブジェクトから少数のバイト範囲を要求するGetObject操作は特に非効率的です。たとえば、50 GB の圧縮オブジェクトから 10 MB の範囲を読み取ることは非効率的です。

圧縮されたオブジェクトから範囲を読み取る場合、クライアントからのリクエスト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長くしてください。

手順

1. **Configuration > System > Storage settings > Object compression** を選択します。
2. 「保存されたオブジェクトを圧縮する」チェックボックスを選択します。
3. * 保存 * を選択します。

StorageGRID でストレージノード全体を管理

ストレージノードが容量に達したら、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。使用可能なオプションは3つあります：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、およびストレージノードの追加です。

ストレージボリュームを追加する

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。定義された最大値はプラットフォームによって異なります。ストレージノードに含まれるストレージボリュームの数が最大数に満たない場合、ボリュームを追加することで容量を増やすことができます。["StorageGRID システムの拡張"](#)の手順を参照してください。

ストレージ拡張シェルフの追加

SG6060やSG6160などの一部のStorageGRIDアプライアンスストレージノードは、追加のストレージシェルフをサポートできます。拡張機能を備えたStorageGRIDアプライアンスをお持ちで、まだ最大容量まで拡張されていない場合は、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。["StorageGRID システムの拡張"](#)の手順を参照してください。

ストレージノードを追加する

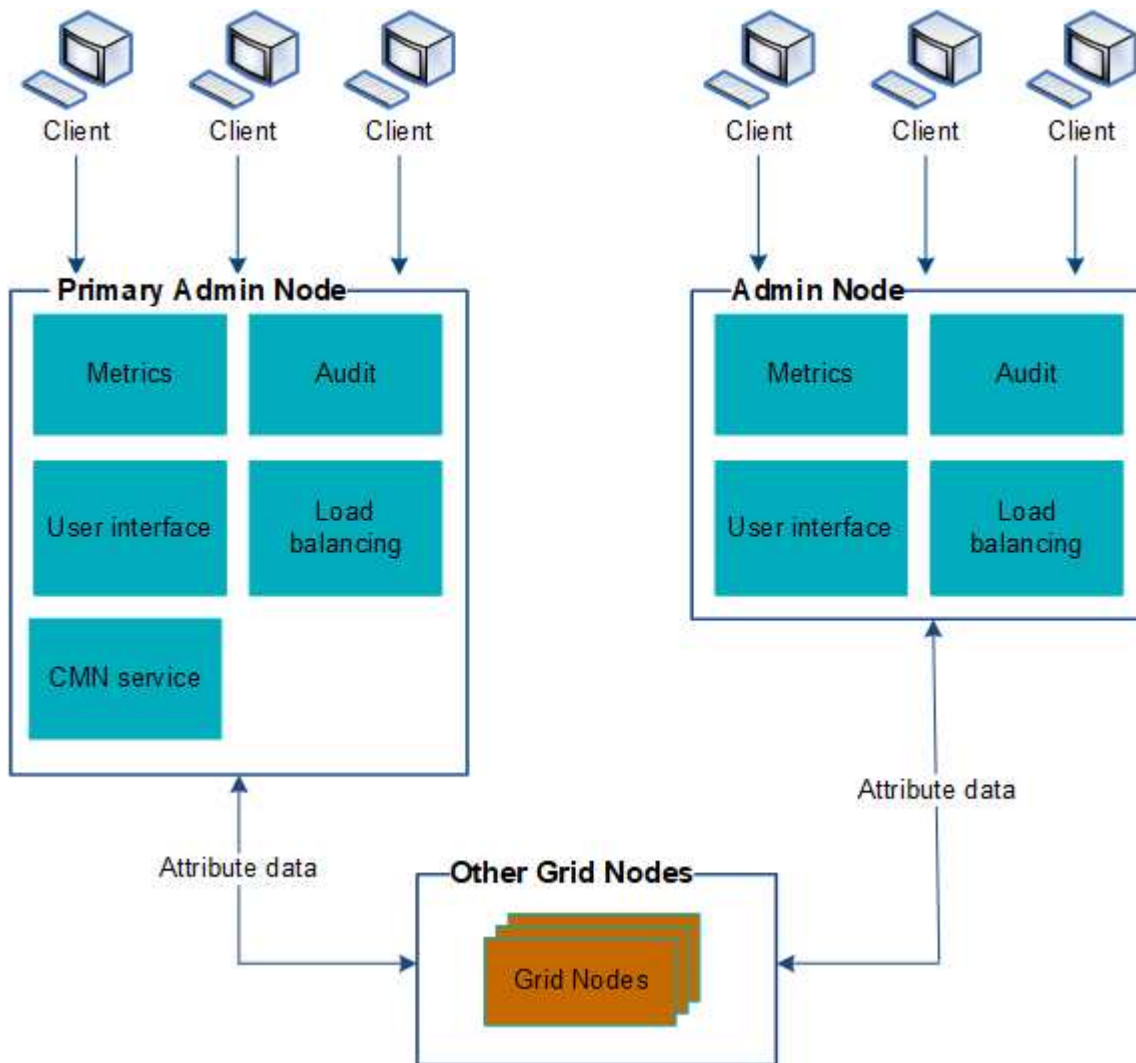
ストレージノードを追加することで、ストレージ容量を増やすことができます。ストレージを追加する際には、現在有効なILMルールおよび容量要件を慎重に検討する必要があります。["StorageGRID システムの拡張"](#)の手順を参照してください。

管理ノードの管理

StorageGRID で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、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および設定することができます。

管理ノードが利用できなくなった場合でも、属性処理は継続され、アラートは引き続きトリガーされ、電子メール通知とAutoSupportパッケージは引き続き送信されます。ただし、複数の管理ノードがあっても、通知とAutoSupportパッケージを除き、フェイルオーバー保護は提供されません。



管理ノードに障害が発生した場合に StorageGRID システムの表示と設定を続行するには、次の 2 つのオプションがあります：

- Webクライアントは、利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高可用性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Grid ManagerまたはTenant Managerに引き続きアクセスできます。["高可用性グループを管理する"](#)を参照してください。



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に障害が発生すると、アクセスが中断されます。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後、ユーザーは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作業は、プライマリ管理ノードを使用してのみ実行できます。プライマリ管理ノードに障害が発生した場合は、StorageGRID システムが完全に機能する状態に戻る前に、プライマリ管理ノードをリカバリする必要があります。

StorageGRID で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、非プライマリ管理ノードよりも多くの機能を提供します。例えば、一部の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。

管理ノードの詳細については、["管理ノードとは何ですか？"](#)を参照してください。

開始する前に

- ["対応ウェブブラウザ"](#) を使用して Grid Manager にサインインしています。
- ["特定のアクセス権限"](#)があります。

手順

1. * Nodes * を選択します。
2. 検索ボックスに「**primary**」と入力してください。

検索結果から、「タイプ」列に「Primary Admin Node」と表示されているノードを特定してください。プライマリ管理ノードが1つ表示されます。

著作権に関する情報

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。