



StorageGRIDの管理

StorageGRID software

NetApp
December 03, 2025

目次

StorageGRIDの管理	1
StorageGRIDの管理	1
これらの指示について	1
開始する前に	1
グリッドマネージャーを使い始める	1
Webブラウザの要件	1
グリッドマネージャーにSign in	2
グリッドマネージャーからサインアウトする	8
パスワードを変更する	8
StorageGRIDライセンス情報を表示する	9
StorageGRIDライセンス情報を更新する	10
APIを使用する	10
StorageGRIDへのアクセスを制御する	33
StorageGRIDアクセスを制御する	33
プロビジョニングパスフレーズを変更する	34
ノードコンソールのパスワードを変更する	35
管理ノードのSSHアクセスパスワードを変更する	37
アイデンティティフェデレーションを使用する	39
管理者グループの管理	44
管理者グループの権限	47
ユーザの管理	51
シングルサインオン（SSO）を使用する	54
グリッドフェデレーションを使用する	84
グリッドフェデレーションとは何ですか？	84
アカウントクローンとは何ですか？	86
クロスグリッドレプリケーションとは何ですか？	89
クロスグリッドレプリケーションとCloudMirrorレプリケーションを比較する	95
グリッドフェデレーション接続を作成する	98
グリッドフェデレーション接続を管理する	101
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	106
グリッドフェデレーションエラーのトラブルシューティング	112
失敗したレプリケーション操作を識別して再試行する	118
セキュリティを管理する	121
セキュリティを管理する	121
StorageGRIDの暗号化方式を確認する	122
証明書の管理	125
セキュリティ設定を構成する	158
キー管理サーバーを構成する	163
プロキシ設定を管理する	183

ファイアウォールを制御する	185
テナントの管理	192
テナント アカウントとは何ですか?	192
テナントアカウントを作成する	193
テナントアカウントの編集	199
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	201
テナントアカウントを削除する	202
プラットフォームサービスの管理	202
テナントアカウントのS3 Selectを管理する	211
クライアント接続を構成する	212
S3クライアント接続を構成する	212
S3 クライアントのセキュリティ	215
S3セットアップウィザードを使用する	216
HAグループの管理	226
負荷分散を管理する	237
S3エンドポイントのドメイン名を設定する	251
概要: クライアント接続の IP アドレスとポート	253
ネットワークと接続を管理する	255
ネットワークの設定	255
StorageGRIDネットワークのガイドライン	256
IPアドレスを表示	257
VLANインターフェースを構成する	258
トラフィック分類ポリシーを管理する	263
送信 TLS 接続でサポートされている暗号	270
アクティブ、アイドル、同時HTTP接続の利点	270
リンクコストを管理する	272
AutoSupportを使用する	274
AutoSupportとは何ですか?	274
AutoSupportを構成する	279
AutoSupportパッケージを手動でトリガーする	283
AutoSupportパッケージのトラブルシューティング	284
EシリーズAutoSupportパッケージをStorageGRID経由で送信する	285
ストレージノードの管理	289
ストレージノードの管理	289
ストレージオプションを使用する	289
オブジェクトメタデータストレージの管理	293
メタデータ予約領域設定を増やす	300
保存されたオブジェクトを圧縮する	303
完全なストレージノードを管理する	303
管理ノードの管理	304
複数の管理ノードを使用する	304

プライマリ管理ノードを特定する	305
通知ステータスとキューを表示する	306

StorageGRIDの管理

StorageGRIDの管理

StorageGRIDシステムを構成および管理するには、次の手順に従います。

これらの指示について

StorageGRID を構成および管理するための主なタスクでは、次のことが可能になります。

- グリッドマネージャ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ネットワークの構成と管理
- AutoSupportを構成する
- ノード設定を管理する

開始する前に

- StorageGRIDシステムに関する一般的な知識があること。
- Linux 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関するかなり詳細な知識があります。

グリッドマネージャーを使い始める

Webブラウザの要件

サポートされている Web ブラウザを使用する必要があります。

Webブラウザ	サポートされる最小バージョン
Google Chrome	119
Microsoft Edge	119
Mozilla Firefox	119

ブラウザウィンドウを推奨幅に設定する必要があります。

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

グリッドマネージャーにSign in

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

各StorageGRIDシステムには、1つのプライマリ管理ノードと任意の数の非プライマリ管理ノードが含まれます。任意の管理ノードの 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は、HA グループの仮想 IP アドレスまたは仮想 IP アドレスにマップされる完全修飾ドメイン名を使用して接続します。プライマリ管理ノードをグループのプライマリ インターフェイスとして選択する必要があります。これにより、プライマリ管理ノードが使用できない場合を除き、グリッド マネージャーにアクセスするときにプライマリ管理ノードからアクセスできるようになります。見る["高可用性グループの管理"](#)。

SSO を使用

サインインの手順は、以下の場合、若干異なります。["シングルサインオン \(SSO\) が設定されています"](#)。

最初の管理ノードでグリッド マネージャーにSign in

開始する前に

- ログイン資格情報をお持ちです。
- 使用しています["サポートされているウェブブラウザ"](#)。
- Web ブラウザで Cookie が有効になっています。
- 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 マネージャーの URL は次のとおりです。

```
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ます。

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



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

手順

1. サポートされている Web ブラウザを起動します。
2. ブラウザのアドレスバーに、グリッド マネージャーの 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ます。見る["セキュリティ証明書を管理する"](#)。
4. グリッド マネージャーにSign in。

表示されるサインイン画面は、StorageGRIDに対してシングル 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を使用していない

- 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ます。
- b. *サインイン*を選択します。



The image shows the login interface for NetApp StorageGRID Grid Manager. At the top, the logo "NetApp StorageGRID®" is displayed, followed by the title "Grid Manager". Below this, there are two input fields: "Username" and "Password". The "Username" field has a blue border and a vertical cursor. Below the "Password" field is a blue "Sign in" button. At the bottom, there are three links: "Tenant sign in", "NetApp support", and "NetApp.com".

SSOの使用

- StorageGRIDが SSO を使用しており、このブラウザで URL にアクセスするのは初めての場合:
 - i. *Sign in*を選択します。アカウント フィールドには 0 を残しておけます。



Sign in

Account

Sign in

[NetApp support](#) | [NetApp.com](#)

- ii. 組織の SSO サインイン ページで標準の SSO 資格情報を入力します。例えば：

Sign in with your organizational account

Sign in

- ° 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：

- i. 0 (グリッド マネージャーのアカウント ID) を入力するか、最近のアカウントのリストに 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ます。

The image shows a web interface for NetApp StorageGRID. At the top, there is a logo consisting of a square icon followed by the text "NetApp StorageGRID®". Below the logo is the heading "Sign in". Underneath the heading, there is a section labeled "Recent" with a dropdown menu showing "Grid Manager". Below that is a section labeled "Account" with a text input field containing the number "0". At the bottom of the form is a blue button with the text "Sign in". Below the button, there is a link that says "NetApp support | NetApp.com".

NetApp StorageGRID®

Sign in

Recent

Grid Manager ▼

Account

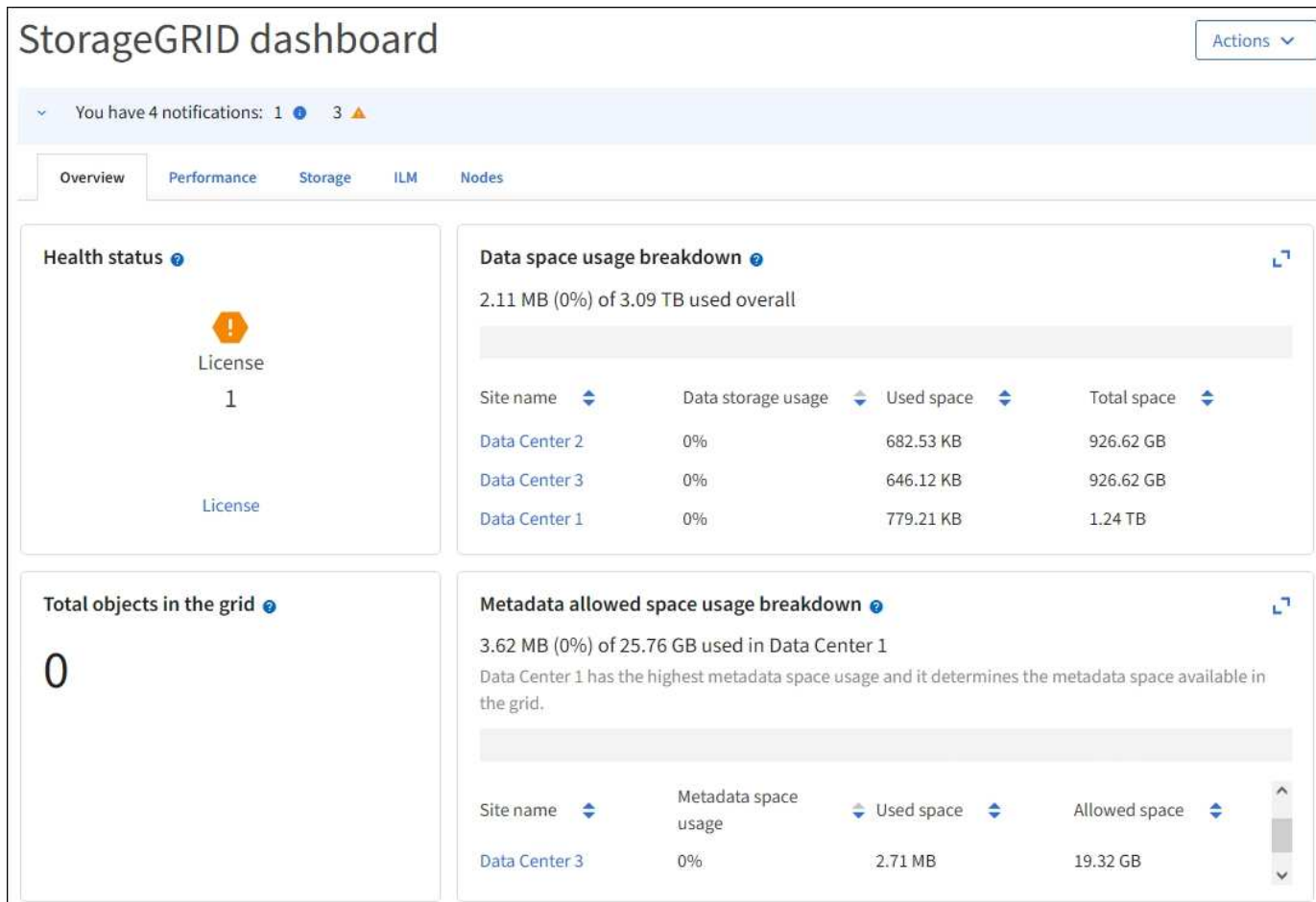
0

Sign in

[NetApp support](#) | [NetApp.com](#)

- ii. *Sign in*を選択します。
- iii. 組織の SSO サインイン ページで標準の SSO 資格情報を使用してSign in。

サインインすると、ダッシュボードを含むグリッド マネージャーのホームページが表示されます。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](#)"。



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、次の手順に従います。

SSOを使用していない

手順

1. ブラウザのアドレス バーに、他の管理ノードの完全修飾ドメイン名または IP アドレスを入力します。必要に応じてポート番号を含めます。
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ます。
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は、再度サインインしなくても他の管理ノードにアクセスできます。

手順

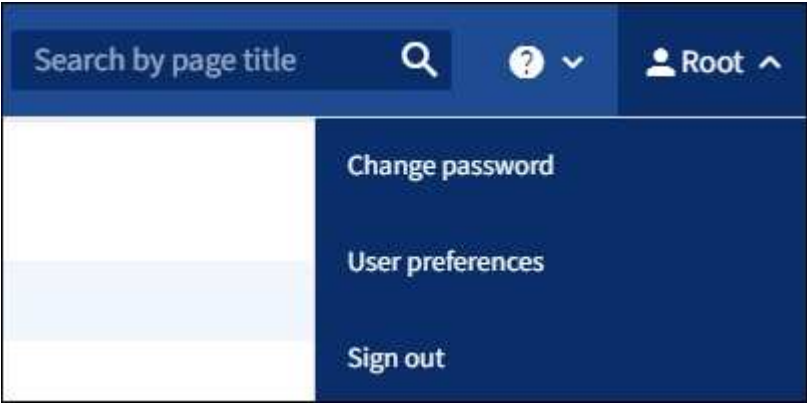
1. ブラウザのアドレス バーに、他の管理ノードの完全修飾ドメイン名または IP アドレスを入力します。
2. SSO セッションの有効期限が切れている場合は、資格情報を再度入力してください。

グリッドマネージャーからサインアウトする

Grid Manager での作業が完了したら、権限のないユーザーがStorageGRIDシステムにアクセスできないようにするためにサインアウトする必要があります。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ます。



2. *サインアウト*を選択します。

オプション	説明
SSOは使用されていません	管理ノードからサインアウトしました。 Grid Manager のサインイン ページが表示されます。 注意: 複数の管理ノードにサインインしている場合は、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	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しました。StorageGRIDサインイン ページが表示されます。 Grid Manager は最近のアカウント ドロップダウンにデフォルトとしてリストされ、アカウント ID フィールドには 0 が表示されます。 注意: SSOが有効になっていて、テナントマネージャ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" に"SSOからサインアウト"。

パスワードを変更する

Grid Manager のローカル ユーザーの場合は、自分のパスワードを変更できます。

開始する前に

グリッドマネージャにサインインするには、"[サポートされているウェブブラウザ](#)"。

タスク概要

フェデレーション ユーザーとしてStorageGRIDに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 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。パスワードでは大文字と小文字が区別されます。

4. 新しいパスワードをもう一度入力します。
5. *保存*を選択します。

StorageGRIDライセンス情報を表示する

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

開始する前に

グリッドマネージャにサインインするには、["サポートされているウェブブラウザ"](#)。

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は、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。数字はライセンス関連の問題の数を示します。



手順

1. 次のいずれかの方法でライセンス ページにアクセスします。
 - メンテナンス > システム > *ライセンス*を選択します。
 - ダッシュボードのヘルス ステータス カードから、ライセンス ステータス アイコンまたは ライセンス

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。これは、このStorageGRIDインストールの一意的識別番号です。
- ライセンスシリアル番号
- ライセンスの種類（永久*または*サブスクリプション）
- グリッドのライセンスされたストレージ容量
- サポートされているストレージ容量
- ライセンスの終了日。永久ライセンスの場合は*N/A*が表示されます。
- 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ますが、ライセンス ファイルの取得後にサポート サービス契約を延長または更新した場合は、日付が古くなっている可能性があります。この値を更新するには、"[StorageGRIDライセンス情報を更新する](#)"。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ライセンス情報を更新する

ライセンスの条件が変更されるたびに、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、グリッドに追加のストレージ容量を購入する場合は、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。
- あなたが持っている"[特定のアクセス権限](#)"。
- プロビジョニング パスフレーズを持っています。

手順

1. メンテナンス > システム > *ライセンス*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見つけて選択します(.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ます。
5. *保存*を選択します。

APIを使用する

グリッド管理APIを使用する

Grid Manager ユーザー インターフェイスの代わりに Grid Management 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、ユーザー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。

トップレベルのリソース

グリッド管理 API は、次の最上位リソースを提供します。

- /grid: アクセスは Grid Manager ユーザーに制限され、構成されたグループ権限に基づいて行われます。
- /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制限されます。詳細については、["テナントアカウントを使用する"](#)。
- /private: アクセスは Grid Manager ユーザーに制限され、構成されたグループ権限に基づいて行われます。プライベート API は予告なく変更される場合があります。StorageGRID プライベート エンドポイントは、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、Swagger オープン ソース API プラットフォームを使用します。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 インターフェイスを提供します。

Swagger ユーザー インターフェイスは、各 API 操作の完全な詳細とドキュメントを提供します。

開始する前に

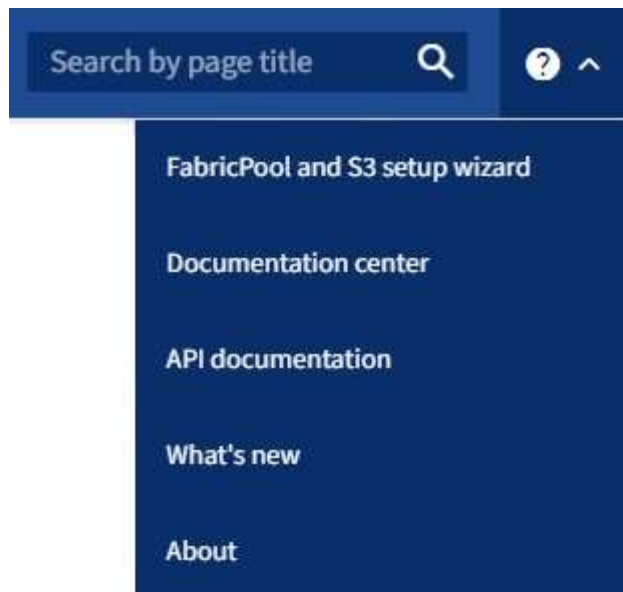
- グリッドマネージャにサインインするには、["サポートされているウェブブラウザ"](#)。
- あなたが持っている["特定のアクセス権限"](#)。



API ドキュメント Web ページを使用して実行するすべての API 操作はライブ操作です。誤って設定データやその他のデータを作成、更新、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 ヘッダーからヘルプ アイコンを選択し、**API ドキュメント** を選択します。



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

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のリスト、リクエスト本文の例 (必要な場合)、および可能な応答などの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 などの追加の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、最初に別の API リクエストを発行する必要がある場合があります。
- サンプルのリクエスト本文を変更する必要があるかどうかを判断します。その場合は、「モデル」を選択して、各フィールドの要件を確認することができます。
- *試してみる*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ます。
- *実行*を選択します。
- 応答コードを確認して、リクエストが成功したかどうかを確認します。

グリッド管理 API は、利用可能な操作を次のセクションに分類します。



このリストには、パブリック API で利用可能な操作のみが含まれます。

- **アカウント**: 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量の取得など、ストレージ テナント アカウントを管理するための操作。
- **alert-history**: 解決された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**: アラートサイレンスに関する操作。
- **アラート**: アラートに関する操作。
- **audit**: 監査構成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操作。

グリッド管理 API は、ベアラー トークン認証スキーム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本文にユーザー名とパスワードを入力します (つまり、`POST /api/v3/authorize`)。ユーザーが正常に認証されると、セキュリティ トークンが返されます。このトークンは、後続の API リクエストのヘッダー (「*Authorization: Bearer token*」) で提供する必要があります。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、認証のために別の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 フォージェリの防止」を参照してください。

- **client-certificates**: 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クライアント 証明書を構成する操作。
- **config**: Grid Management API の製品リリースとバージョンに関連する操作。製品リリース 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、API の非推奨バージョンを無効にしたりできます。
- **deactivated-features**: 非アクティブ化された可能性のある機能を表示する操作。
- **dns-servers**: 構成された外部 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 エンドポイントのドメイン名を一覧表示および変更する操作。
- **消去コーディング**: 消去コーディング プロファイルに対する操作。
- **展開**: 展開に関する操作 (プロシージャ レベル)。
- **expansion-nodes**: 拡張 (ノード レベル) に関する操作。
- **拡張サイト**: 拡張に関する操作 (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 パスワード管理の操作。
- **groups**: ローカル グリッド管理者グループを管理し、外部 LDAP サーバーからフェデレーション グリッド管理者グループを取得するための操作。
- **identity-source**: 外部 ID ソースを構成し、フェデレーション グループとユーザー情報を手動で同期する操作。
- **ilm**: 情報ライフサイクル管理 (ILM) に関する操作。
- **in-progress-procedures**: 現在進行中のメンテナンス手順を取得します。
- **license**: StorageGRIDライセンスを取得および更新する操作。
- **logs**: ログファイルを収集およびダウンロードするための操作。v
- **metrics**: 単一時点でのインスタント メトリック クエリや、一定範囲の時間にわたる範囲メトリック クエリなどのStorageGRIDメトリックに対する操作。グリッド管理 API は、バックエンド データ ソースとして Prometheus システム監視ツールを使用します。Prometheus クエリの構築については、Prometheus Web サイトを参照してください。



含まれる指標`private`名前に含まれる文字は内部使用のみを目的としています。これらのメトリックは、StorageGRIDリリース間で予告なく変更されることがあります。

- **node-details**: ノードの詳細に関する操作。
- **node-health**: ノードのヘルスステータスに関する操作。
- **node-storage-state**: ノードストレージステータスに関する操作。
- **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。
- **recovery**: 回復手順のための操作。
- **recovery-package**: リカバリ パッケージをダウンロードする操作。
- **regions**: リージョンを表示および作成する操作。
- **s3-object-lock**: グローバル S3 オブジェクトロック設定に対する操作。
- **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 構成に対する操作。
- **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**: 信頼できないクライアント ネットワーク構成での操作。
- **users**: Grid Manager ユーザーを表示および管理する操作。

グリッド管理 API のバージョン管理

グリッド管理 API は、バージョン管理を使用して、中断のないアップグレードをサポートします。

たとえば、このリクエスト URL はAPI バージョン 4 を指定します。

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

古いバージョンと互換性のない変更が行われた場合には、API のメジャー バージョンが引き上げられます。古いバージョンと互換性のある変更が行われた場合に、API のマイナー バージョンが引き上げられます。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。

次の例は、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変更されるかを示しています。

APIの変更の種類	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
旧バージョンとは互換性がありません	2.1	3.0

StorageGRIDソフトウェアを初めてインストールすると、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すると、少なくとも 1 つのStorageGRID機能リリースについては引き続き古い API バージョンにアクセスできます。



サポートされるバージョンを設定できます。Swagger APIドキュメントの*config*セクションを参照してください。["グリッド管理API"](#)詳細についてはこちらをご覧ください。すべてのAPIクライアントを更新して新しいバージョンを使用するようにした後、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。

古くなったリクエストは、次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レスポンス本文に「deprecated」が含まれています: true
- 非推奨の警告が nms.log に追加されます。例えば：

```
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

使用 `GET /versions` サポートされている API メジャー バージョンのリストを返す API リクエスト。このリクエストは、Swagger API ドキュメントの **config** セクションにあります。

```
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**を指定する

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

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

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

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) 攻撃から保護することができます。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。他の API クライアントはサインイン時にこの機能を有効にするかどうかを選択できます。

別のサイトへのリクエストをトリガーできる攻撃者 (HTTP フォーム POST など) は、サインインしたユーザーの Cookie を使用して特定のリクエストを実行させる可能性があります。

StorageGRID は、CSRF トークンを使用して CSRF 攻撃から保護します。有効にすると、特定の Cookie の内容は、特定のヘッダーまたは特定の POST 本文パラメータのいずれか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、csrfToken`パラメータに `true` 認証中。デフォルトは `false`。

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

真の場合、`GridCsrfToken`グリッドマネージャへのサインイン時にランダムな値でクッキーが設定され、`AccountCsrfToken`テナント マネージャーへのサインイン用に、Cookie にランダムな値が設定されます。

クッキーが存在する場合、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、次のいずれかが含まれている必要があります。

- その `X-Csrf-Token`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本文を受け入れるエンドポイントの場合: `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。

追加の例と詳細については、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 クッキーが設定されているリクエストでは、CSRF 攻撃に対する追加の保護として、JSON リクエスト本文を期待するすべてのリクエストに「Content-Type: application/json」ヘッダーも適用されます。

シングルサインオンが有効になっている場合は**API**を使用する

シングル サインオンが有効になっている場合は **API** を使用する (**Active Directory**)

もしあなたが"**シングル サインオン (SSO) を設定して有効にする**"Active Directory を SSO プロバイダーとして使用する場合は、一連の API 要求を発行して、グリッド管理 API またはテナント管理 API に有効な認証トークンを取得する必要があります。

シングル サインオンが有効になっている場合は、**API** に**Sign in**。

これらの手順は、Active Directory を SSO ID プロバイダーとして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がわかっています。
- テナント管理 API にアクセスする場合は、テナント アカウント ID がわか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、次のいずれかの例を使用できます。

- その `storagegrid-ssoauth.py` `StorageGRIDインストール ファイル ディレクトリにある Python スクリプト (./rpms`Red Hat Enterprise Linuxの場合、 ./debs UbuntuまたはDebianの場合、 ./vsphere VMware の場合)。
- curl リクエストのワークフローの例。

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。



サンプルの curl ワークフローでは、パスワードが他のユーザーから見られないように保護されません。

URL エンコードの問題がある場合は、次のエラーが表示されることがあります。Unsupported SAML

version。

手順

1. 認証トークンを取得するには、次のいずれかの方法を選択します。
 - 使用 `storagegrid-ssoauth.py` Python スクリプト。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. 使用したい場合は `storagegrid-ssoauth.py` スクリプトの場合は、スクリプトを Python インタープリターに渡してスクリプトを実行します。

プロンプトが表示されたら、次の引数の値を入力します。

- SSO 方式。ADFS または adfs を入力します。
- SSO ユーザー名
- 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のテナント アカウント ID。

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

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

StorageGRID 認証トークンが出力に提供されます。SSO が使用されていない場合に API を使用すると同様に、他のリクエストにもトークンを使用できるようになりました。

3. curl リクエストを使用する場合は、次の手順に従います。

- a. サインインに必要な変数を宣言します。

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



グリッド管理APIにアクセスするには、0を次のように使用します。
TENANTACCOUNTID。

- b. 署名された認証URLを受け取るには、POSTリクエストを発行します。 /api/v3/authorize-saml、レスポンスから追加の JSON エンコーディングを削除します。

この例では、署名付き認証URLのPOSTリクエストを示しています。 TENANTACCOUNTID。結果は`python -m json.tool`JSON エンコーディングを削除します。

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

この例の応答には、URL エンコードされた署名付き URL が含まれますが、追加の JSON エンコードレイヤーは含まれません。

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

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

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

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

1 つのオプションは、前の応答からの URL を使用してログイン フォームを要求することです。

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

応答にはクライアント要求 ID が含まれます。


```
<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. 応答からクライアント要求 ID を保存します。

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

- f. 前の応答からのフォーム アクションに資格情報を送信します。

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

AD FS は、ヘッダーに追加情報を含む 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は、フォーム投稿に 2 番目のパスワードまたはその他の資格情報も含まれます。

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

- g. 保存する `MSISAuth` 応答から Cookie を取得します。

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

- h. 認証 POST からの Cookie を含む GET リクエストを指定された場所へ送信します。

```
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、後でログアウトする際に使用する AD FS セッション情報が含まれ、応答本体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
XFxVWx3bkl1MnFuUSUzZCUzZCYmJiYmXzE3MjAyZTA5LThtMDgtNDRkZC04Yzg5LTQ3ND
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="PHNhbWxwOlJlc3Bvb3N1scDpsZXNwb25zZT4=" /><input
type="hidden" name="RelayState" value="12345" />
```

- i. 保存する `SAMLResponse` 隠しフィールドから:

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

- j. 保存した SAMLResponse、StorageGRIDを作成する /api/saml-responseStorageGRID認証トークンを生成するためのリクエスト。

のために RelayState、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 を使用します。

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

応答には認証トークンが含まれます。

```
{
  "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次のように保存します。MYTOKEN。

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

使用できるようになりました `MYTOKEN` その他のリクエストについては、SSO が使用されていない場合に API を使用する方法と同様です。

シングル サインオンが有効になっている場合は、**API** からサインアウトします。

シングル サインオン (SSO) が有効になっている場合は、グリッド管理 API またはテナント管理 API からサインアウトするための一連の API 要求を発行する必要があります。これらの手順は、Active Directory を SSO ID プロバイダーとして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、有効なStorageGRIDベアラー トークンを必要とする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。

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 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 を保存します。

```
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 応答が返されます。リダイレクト場所は、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: MSISignoutProtocol=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 がない場合と同じように機能します。`cookie "sso=true"` が提供されない場合、ユーザーは SSO 状態に影響を与えずに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
```

あ `204 No Content` この応答は、ユーザーが現在サインアウトしていることを示します。

```
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 **API** を使用する (**Azure**)

もしあなたが**"シングルサインオン (SSO) を設定して有効にする"**Azure を SSO プロバイダーとして使用する場合、2 つのサンプル スクリプトを使用して、グリッド管理 API またはテナント管理 API に有効な認証トークンを取得できます。

Azure シングルサインオンが有効になっている場合は、**API** に**Sign in**。

これらの手順は、Azure を SSO ID プロバイダーとして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 電子メール アドレスとパスワードがわかっています。
- テナント管理 API にアクセスする場合は、テナント アカウント ID がわか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、次のサンプル スクリプトを使用できます。

- その `storagegrid-ssoauth-azure.py` Python スクリプト
- その `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にあります。(./rpms Red Hat Enterprise Linuxの場合、./debs UbuntuまたはDebianの場合、./vsphere VMware の場合)。

Azureとの独自のAPI統合を作成するには、`storagegrid-ssoauth-azure.py` スクリプト。Python スクリプトは、StorageGRIDに2つのリクエストを直接送信します(最初にSAMLRequestを取得し、後で認証トークンを取得します)。また、Node.js スクリプトを呼び出して Azure と対話し、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、実行するのは簡単ではありません。Puppeteer Node.js モジュールは、Azure SSO インターフェイスをスクレイピングするために使用されます。

URL エンコードの問題がある場合は、次のエラーが表示されることがあります。Unsupported SAML version。

手順

1. 次のように、必要な依存関係をインストールします。
 - a. Node.jsをインストールする ("<https://nodejs.org/en/download/>") 。
 - 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 インタープリターに渡してスクリプトを実行します。

次に、Python スクリプトは対応する Node.js スクリプトを呼び出して、Azure SSO のやり取りを実行します。

3. プロンプトが表示されたら、次の引数の値を入力します (またはパラメータを使用して渡します)。
 - Azure へのサインインに使用する SSO 電子メール 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のテナント アカウント ID
4. プロンプトが表示されたら、パスワードを入力し、要求された場合に Azure に MFA 認証を提供できるように準備します。

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

Watch for and approve a 2FA authorization request
*****

StorageGRID Auth Token: {'responseTime': '2021-10-04T21:30:48.807Z', 'status': 'success', 'apiVersion':
'3.4', 'data': '4807d93e-a3df-48f2-9680-906cd255979e'}
```



このスクリプトでは、MFA が Microsoft Authenticator を使用して実行されることを前提としています。他の形式の MFA (テキスト メッセージで受信したコードの入力など) をサポートするには、スクリプトを変更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提供されます。SSO が使用されていない場合に API を使用するのと同様に、他のリクエストにもトークンを使用できるようになりました。

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

もしあなたが**シングル サインオン (SSO) を設定して有効にする** PingFederate を SSO プロバイダーとして使用する場合は、一連の API 要求を発行して、Grid Management API または Tenant Management API に有効な認証トークンを取得する必要があります。

シングル サインオンが有効になっている場合は、**API** に**Sign in**。

これらの手順は、PingFederateをSSO IDプロバイダーとして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がわかっています。
- テナント管理 API にアクセスする場合は、テナント アカウント ID がわか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、次のいずれかの例を使用できます。

- その storagegrid-ssoauth.py`StorageGRIDインストール ファイル ディレクトリにある Python スクリプト (./rpms`Red Hat Enterprise Linuxの場合、 ./debs UbuntuまたはDebianの場合、 ./vsphere VMware の場合)。
- curl リクエストのワークフローの例。

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。



サンプルの curl ワークフローでは、パスワードが他のユーザーから見られないように保護されません。

URL エンコードの問題がある場合は、次のエラーが表示されることがあります。 Unsupported SAML version。

手順

1. 認証トークンを取得するには、次のいずれかの方法を選択します。
 - 使用 `storagegrid-ssoauth.py` Python スクリプト。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. 使用したい場合は `storagegrid-ssoauth.py` スクリプトの場合は、スクリプトを Python インタープリターに渡してスクリプトを実行します。

プロンプトが表示されたら、次の引数の値を入力します。

- SSO 方式。「pingfederate」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。空白のままにすることも、任意の値を入力することもできます。
- StorageGRID のアドレス
- テナント管理 API にアクセスする場合のテナント アカウント ID。

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

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

StorageGRID 認証トークンが出力に提供されます。SSO が使用されていない場合に API を使用するのと同様に、他のリクエストにもトークンを使用できるようになりました。

3. curl リクエストを使用する場合は、次の手順に従います。
 - a. サインインに必要な変数を宣言します。

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



グリッド管理APIにアクセスするには、0を次のように使用します。
TENANTACCOUNTID。

- b. 署名された認証URLを受け取るには、POSTリクエストを発行します。 /api/v3/authorize-saml、レスポンスから追加の 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
```

この例の応答には、URL エンコードされた署名付き URL が含まれますが、追加の JSON エンコードレイヤーは含まれません。

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

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

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

- d. 応答と Cookie をエクスポートし、応答をエコーします。

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

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

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

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



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

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

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

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

- g. 「アクション」 値をエクスポートします。

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

- h. 資格情報とともに Cookie を送信します。

```
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. 保存する `SAMLResponse` 隠しフィールドから:

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

- j. 保存した SAMLResponse、StorageGRIDを作成する/api/saml-responseStorageGRID認証トークンを生成するためのリクエスト。

のために RelayState、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 を使用します。

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

応答には認証トークンが含まれます。

```
{
  "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次のように保存します。MYTOKEN。

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

使用できるようになりました `MYTOKEN` その他のリクエストについては、SSO が使用されていない場合に API を使用する方法と同様です。

シングル サインオンが有効になっている場合は、**API** からサインアウトします。

シングル サインオン (SSO) が有効になっている場合は、グリッド管理 API またはテナント管理 API からサインアウトするための一連の API 要求を発行する必要があります。これらの手順は、PingFederateをSSO IDプロバイダーとして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、有効なStorageGRIDベアラー トークンを必要とする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。

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 URL が返されます:

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

2. ログアウト URL を保存します。

```
export LOGOUT_REQUEST='https://my-ping-
url/ldap/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 応答が返されます。リダイレクト場所は、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 がない場合と同じように機能します。`cookie "sso=true"` が提供されない場合、ユーザーは SSO 状態に影響を与えずに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
```

あ `204 No Content` この応答は、ユーザーが現在サインアウトしていることを示します。

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

APIを使用して機能を無効にする

Grid Management API を使用すると、StorageGRIDシステムの特定の機能を完全に非アクティブ化できます。機能が非アクティブ化されると、その機能に関連するタスクを実行する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

非アクティブ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禁止できます。機能を非アクティブ化することは、ルート ユーザーまたは ルート アクセス 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には、次のシナリオを検討してください。

_A 社は、テナント アカウントを作成してStorageGRIDシステムのストレージ容量をリースするサービス プロバイダーです。賃借人の物件のセキュリティを保護するために、A 社は、アカウントが展開された後は自社の従業員がテナント アカウントにアクセスできないようにしたいと考えています。

_A 社は、グリッド管理 API の非アクティブ化機能システムを使用してこの目標を達成できます。A 社は、グリッド マネージャー (UI と API の両方) の テナント ルート パスワードの変更 機能を完全に無効にすることで、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、テナント アカウントのルート ユーザーのパスワードを変更できないようにします。

手順

1. グリッド管理 API の Swagger ドキュメントにアクセスします。見る["グリッド管理APIを使用する"](#)。
2. 機能の非アクティブ化エンドポイントを見つけます。
3. テナント 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 ルート パスワードの変更機能は無効になります。テナント 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すべての API 要求は「403 禁止」で失敗します。

無効化された機能を再有効化

デフォルトでは、Grid Management API を使用して、非アクティブ化された機能を再アクティブ化できます。ただし、非アクティブ化された機能が再度アクティブ化されないようにしたい場合は、**activateFeatures** 機能自体を非アクティブ化することができます。



activateFeatures 機能は再アクティブ化できません。この機能を非アクティブ化することにした場合、非アクティブ化された他の機能を再アクティブ化することができなくなることに注意してください。失われた機能を復元するには、テクニカル サポートに連絡する必要があります。

手順

1. グリッド管理 API の Swagger ドキュメントにアクセスします。
2. 機能の非アクティブ化エンドポイントを見つけます。
3. すべての機能を再アクティブ化するには、次のように本文を API に送信します。

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

この要求が完了すると、テナント ルート パスワードの変更機能を含むすべての機能が再アクティブ化されます。テナント ルート パスワードの変更 管理権限がユーザー インターフェイ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 ルート パスワードの変更 管理権限を持っていると仮定すると、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 要求が成功します。



前の例では、非アクティブ化されたすべての機能が再アクティブ化されます。非アクティブ化されていて非アクティブのままにしておく必要がある他の機能が非アクティブ化されている場合は、PUT 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。たとえば、テナント ルート パスワードの変更機能を再度アクティブ化し、storageAdmin 管理権限を引き続き非アクティブ化するには、次の PUT リクエストを送信します。+ { "grid": { "storageAdmin": true} }

StorageGRIDへのアクセスを制御する

StorageGRIDアクセスを制御する

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 にアクセスでき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) を有効にしたり、クライアント証明書を作成したり、グリッド パスワードを変更したりすることもできます。

グリッドマネージャーへのアクセスを制御する

アイデンティティ フェデレーション サービスからグループとユーザ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、Grid Manager と Grid Management API にアクセスできるユーザーを決定します。

使用["アイデンティティフェデレーション"](#)セットアップが容易["グループ"](#)そして["ユーザ"](#)より高速になり、ユーザーは使い慣れた資格情報を使用して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 を使用する場合は、ID フェデレーションを構成できます。



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

各ユーザーが実行できるタスクを決定するには、異なる["権限"](#)各グループに。たとえば、あるグループのユーザーに ILM ルールを管理させ、別のグループのユーザーにメンテナンス タスクを実行させたい場合があります。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できます。読み取り専用グループのユーザーは、設定と機能の表示のみが可能です。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。

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。お先にどうぞ["SSOを設定して有効にする"](#)すべてのユーザーは、グリッド マネージャー、テナント マネージャー、グリッド管理 API、またはテナント管理 API にアクセスする前

に、外部 ID プロバイダーによって認証される必要があります。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を変更する

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、およびStorageGRIDリカバリ パッケージのダウンロードに必要です。パスフレーズは、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必要です。あなたはできる["パスフレーズを変更する"](#)必要に応じて。

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一意のノード 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必要があります。必要に応じて、["ノードコンソールのパスワードを変更する"](#)各ノードに対して。

プロビジョニングパスフレーズを変更する

StorageGRIDプロビジョニング パスフレーズを変更するには、この手順を使用します。パスフレーズは、回復、拡張、およびメンテナンスの手順に必要です。パスフレーズは、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場合にも必要です。

開始する前に

- グリッドマネージャにサインインするには、["サポートされているウェブブラウザ"](#)。
- メンテナンス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

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で必要であり、["リカバリパッケージのダウンロード"](#)。プロビジョニングパスフレーズは、`Passwords.txt` ファイル。プロビジョニングパスフレーズを必ず文書化し、安全な場所に保管してください。

手順

1. 構成 > 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*の下で*変更する*を選択します
3. 現在のプロビジョニング パスフレーズを入力します。
4. 新しいパスフレーズを入力します。パスフレーズには 8 文字以上 32 文字以下を含める必要があります。パスフレーズでは大文字と小文字が区別されます。
5. 新しいプロビジョニング パスフレーズを安全な場所に保存します。インストール、拡張、およびメンテナンスの手順に必要です。
6. 新しいパスフレーズを再度入力し、「保存」を選択します。

プロビジョニング パスフレーズの変更が完了すると、緑色の成功バナーが表示されます。



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

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



プロビジョニング パスフレーズを変更した後は、すぐに新しいリカバリ パッケージをダウンロードする必要があります。リカバリ パッケージ ファイルを使用すると、障害が発生した場合にシステムを復元できます。

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一意のノード コンソール パスワードがあり、ノードにログインするにはこのパスワードが必要です。グリッド内の各ノードの固有のノード コンソール パスワードを変更するには、次の手順に従います。

開始する前に

- グリッドマネージャにサインインするには、"[サポートされているウェブブラウザ](#)"。
- あなたは"[メンテナンスまたはルートアクセス権限](#)"。
- 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

ノード コンソールのパスワードを使用して、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します。ノードコンソールのパスワード変更プロセスは、グリッド内の各ノードに新しいパスワードを作成し、更新されたパスワードを保存します。
`Passwords.txt` リカバリ パッケージ内のファイル。パスワードは、Passwords.txt ファイルの「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、個別の SSH アクセス パスワードがあります。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. 構成 > 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の変更 の下で、変更を行う を選択します。

プロビジョニングパスフレーズを入力してください

手順

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

現在のリカバリパッケージをダウンロードする

ノード コンソールのパスワードを変更する前に、現在のリカバリ パッケージをダウンロードしてください。

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、このファイル内のパスワードを使用できます。

手順

1. *リカバリ パッケージのダウンロード*を選択します。
2. リカバリパッケージファイルをコピーする(.zip)を2つの安全でセキュリティ保護された別の場所に保管します。



リカバリ パッケージ ファイルには、StorageGRIDシステムからデータを取得するため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、セキュリティ保護する必要があります。

3. *続行*を選択します。
4. 確認ダイアログが表示されたら、ノード コンソールのパスワードの変更を開始する準備ができたなら [はい] を選択します。

このプロセスは開始後にキャンセルすることはできません。

ノードコンソールのパスワードを変更する

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

手順

1. 新しい回復パッケージが生成されるまで待ちます。これには数分かかる場合があります。
2. *新しいリカバリ パッケージのダウンロード*を選択します。
3. ダウンロードが完了すると次のようになります。
 - a. 開く `.zip` ファイル。
 - b. 以下のコンテンツにアクセスできることを確認してください。`Passwords.txt` ファイルには新しいノード コンソールのパスワードが含まれています。
 - c. 新しいリカバリパッケージファイルをコピーします(.zip)を2つの安全でセキュリティ保護された別の場所に保管します。



古いリカバリ パッケージを上書きしないでください。

リカバリ パッケージ ファイルには、StorageGRIDシステムからデータを取得するため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、セキュリティ保護する必要があります。

4. 新しいリカバリ パッケージをダウンロードし、その内容を確認したことを示すには、チェックボックスを選択します。
5. ノード コンソールのパスワードの変更 を選択し、すべてのノードが新しいパスワードで更新されるまで待ちます。これには数分かかる場合があります。

すべてのノードのパスワードが変更されると、緑色の成功バナーが表示されます。次の手順へ進みます。

更新プロセス中にエラーが発生した場合、バナー メッセージにパスワードの変更に失敗したノードの数が

表示されます。システムは、パスワードの変更に失敗したノードに対してプロセスを自動的に再試行します。一部のノードでパスワードが変更されていない状態でプロセスが終了した場合は、[再試行] ボタンが表示されます。

1 つ以上のノードでパスワードの更新に失敗した場合:

- a. 表にリストされているエラー メッセージを確認します。
- 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の試行中に失敗したノード上のノード コンソールパスワードのみが変更されます。

6. すべてのノードのノードコンソールのパスワードが変更されたら、[最初にダウンロードしたリカバリパッケージ](#)。
7. 必要に応じて、リカバリ パッケージ リンクを使用して、新しいリカバリ パッケージの追加コピーをダウンロードします。

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の一意の内部 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キーを使用してノードにログインします `admin` または、VM または物理コンソール接続上の root ユーザーにアクセスします。

開始する前に

- グリッドマネージャにサインインするには、["サポートされているウェブブラウザ"](#)。
- あなたは["メンテナンスまたはルートアクセス権限"](#)。
- 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、`Passwords.txt` リカバリ パッケージ内のファイル。キーはそのファイルの「パスワード」列にリストされています。

ノード間の通信に使用される SSH キーには、個別の SSH アクセス パスワードがあります。これら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. 構成 > 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 の下で、変更を加える を選択します。

現在のリカバリパッケージをダウンロードする

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プロセスが失敗した場合は、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ます。
2. *リカバリ パッケージのダウンロード*を選択します。
3. リカバリパッケージファイルをコピーする(.zip) を 2 つの安全でセキュリティ保護された別の場所に保管します。



リカバリ パッケージ ファイルには、StorageGRIDシステムからデータを取得するため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、セキュリティ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た [はい] を選択します。



このプロセスは開始後にキャンセルすることはできません。

SSHアクセスキーを変更する

SSH アクセス キーの変更プロセスが開始されると、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。その後、各ノードでキーが更新されます。

手順

1. 新しい回復パッケージが生成されるまで待ちます。これには数分かかる場合があります。
2. 新しいリカバリパッケージのダウンロードボタンが有効になったら、*新しいリカバリパッケージのダウンロード*を選択し、新しいリカバリパッケージファイルを保存します。(.zip) を 2 つの安全でセキュリティ保護された別の場所に保管します。
3. ダウンロードが完了すると次のようになります。
 - a. 開く `zip` ファイル。
 - b. 以下のコンテンツにアクセスできることを確認してください。`Passwords.txt`新しい SSH アクセス キーが含まれるファイル。
 - c. 新しいリカバリパッケージファイルをコピーします(.zip) を 2 つの安全でセキュリティ保護された別の場所に保管します。



古いリカバリ パッケージを上書きしないでください。

リカバリ パッケージ ファイルには、StorageGRIDシステムからデータを取得するため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、セキュリティ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待ちます。これには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。

更新プロセス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がバナー メッセージにリストされます。システムは、キーの変更に失敗したノード上でプロセスを自動的に再試行します。一部のノードにまだ変更されたキーがない状態でプロセスが終了した場合は、[再試行] ボタンが表示されます。

1 つ以上のノードでキーの更新に失敗した場合:

- a. 表にリストされているエラー メッセージを確認します。
- 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、以前のキー変更の試行中に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、[最初にダウンロードしたリカバリパッケージ](#)。
6. オプションで、メンテナンス > システム > リカバリ パッケージ 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ます。

アイデンティティフェデレーションを使用する

アイデンティティ フェデレーションを使用すると、グループとユーザーの設定が高速化され、ユーザーは使い慣れた資格情報を使用して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構成する

管理者グループとユーザーを Active Directory、Azure Active Directory (Azure AD)、OpenLDAP、Oracle Directory Server などの別のシステムで管理する場合は、Grid Manager で ID フェデレーションを構成できます。

開始する前に

- グリッドマネージャにサインインするには、["サポートされているウェブブラウザ"](#)。
- あなたが持っている["特定のアクセス権限"](#)。
- ID プロバイダーとして、Active Directory、Azure AD、OpenLDAP、または Oracle Directory Server を使用しています。



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

- OpenLDAP を使用する予定の場合は、OpenLDAP サーバーを構成する必要があります。見る[OpenLDAP サーバーの設定ガイドライン](#)。
- シングルサインオン (SSO) を有効にする予定の場合は、["シングルサインオンの要件と考慮事項"](#)。
- LDAP サーバーとの通信にトランスポート層セキュリティ (TLS) を使用する予定の場合、ID プロバイダーは TLS 1.2 または 1.3 を使用しています。見る["送信 TLS 接続でサポートされている暗号"](#)。

タスク概要

Active Directory、Azure AD、OpenLDAP、Oracle Directory Server などの別のシステムからグループをインポートする場合は、Grid Manager の ID ソースを構成できます。次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。管理グループ内のユーザーは、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のテナント ユーザー グループ。テナント グループ内のユーザーは、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。見る["テナントアカウントを作成する"](#)そして["テナントアカウントを使用する"](#)詳細については。

設定を入力する

手順

1. 構成 > アクセス制御 > **ID フェデレーション** を選択します。
2. **ID フェデレーションを有効にする** を選択します。
3. LDAP サービス タイプ セクションで、構成する 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	Azure	OpenLDAP	Other

Oracle Directory Server を使用する LDAP サーバーの値を構成するには、「その他」を選択します。

4. *その他*を選択した場合は、LDAP 属性セクションのフィールドに入力します。次の手順に進みます。
 - ユーザーの一意の名前: LDAP ユーザーの一意の識別子を含む属性の名前。この属性は、`sAMAccountName` Active Directoryおよび `uid` OpenLDAP 用。Oracle Directory Serverを構成する場合は、次のように入力します。 ``uid``。
 - 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、`objectGUID` Active Directoryおよび `entryUUID` OpenLDAP 用。Oracle Directory Serverを構成する場合は、次のように入力します。 ``nsuniqueid``。指定された属性の各ユーザーの値は、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ます。ハイフンは無視されます。
 - グループの一意の名前: LDAP グループの一意の識別子を含む属性の名前。この属性は、`sAMAccountName` Active Directoryおよび `cn` OpenLDAP 用。Oracle Directory Serverを構成する場合は、次のように入力します。 ``cn``。
 - 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および `entryUUID` OpenLDAP 用。Oracle Directory Serverを構成する場合は、次のように入力します。 ``nsuniqueid``。指定された属性の各グループの値は、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ます。ハイフンは無視されます。
5. すべての LDAP サービス タイプについて、[LDAP サーバーの構成] セクションで必要な LDAP サーバーおよびネットワーク接続情報を入力します。
 - ホスト名: LDAP サーバーの完全修飾ドメイン名 (FQDN) または IP アドレス。
 - ポート: LDAP サーバーに接続するために使用されるポート。



STARTTLS のデフォルト ポートは 389 で、LDAPS のデフォルト ポートは 636 です。ただし、ファイアウォールが正しく設定されている限り、どのポートでも使用できます。

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

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

指定されたユーザーには、グループとユーザーを一覧表示し、次の属性にアクセスする権限が必要です。

- sAMAccountName または uid
- objectGUID、entryUUID、または nsuniqueid
- cn
- memberOf または isMemberOf
- アクティブディレクトリ: objectSid、primaryGroupID、userAccountControl、そして userPrincipalName
- アズール: accountEnabled、そして userPrincipalName

- パスワード: ユーザー名に関連付けられたパスワード。



将来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。Active Directory の例 (下記) では、識別名がベース DN (DC=storagegrid、DC=example、DC=com) を基準とする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。



グループの一意の名前*の値は、それが属する *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、それが属する ユーザー ベース **DN** 内で一意である必要があります。

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

StorageGRID がサービス アカウントにバインドできない場合にユーザーがサインインできるように、バインド ユーザー名形式 を指定することをお勧めします。

次のいずれかのパターンを入力します。

- **UserPrincipalName** パターン (**Active Directory** および **Azure**): [USERNAME]@example.com
- ダウンレベル ログオン名パターン (**Active Directory** および **Azure**): example\[USERNAME]
- 識別名パターン: CN=[USERNAME],CN=Users,DC=example,DC=com

[USERNAME] を記載どおりに入力してください。

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 サーバーとの通信を保護します。これは、Active Directory、OpenLDAP、またはその他の場合に推奨されるオプションですが、このオプションは Azure 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 サーバーへの接続を確立します。Azure 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 サーバー間のネットワーク トラフィックは保護されません。このオプションは Azure ではサポートされていません。



Active Directory サーバーが LDAP 署名を強制している場合、「TLS を使用しない」オプションの使用はサポートされません。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 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 사용합니다。

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

接続をテストし、設定を保存します

すべての値を入力した後、構成を保存する前に接続をテストする必要があります。StorageGRID は、LDAP サーバーの接続設定と、指定された場合はバインド ユーザー名の形式を検証します。

手順

1. *テスト接続*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は、「テスト接続が成功しました」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] を選択します。
 - 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。次に、問題を解決して、再度接続をテストします。
3. バインド ユーザー名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ます。

たとえば、独自のユーザー名とパスワードを入力します。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は、「テスト接続が成功しました」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] を選択します。
- ・ 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は、エラー メッセージが表示されます。問題を解決して、再度接続をテストしてください。

アイデンティティソースとの強制同期

StorageGRIDシステムは、フェデレーション グループとユーザーを ID ソースから定期的に同期します。できるだけ早くユーザー権限を有効化または制限したい場合は、同期を強制的に開始できます。

手順

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

環境によっては同期プロセスに時間がかかる場合があります。



アイデンティティ 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ある場合、アイデンティティ フェデレーション同期の失敗 アラートがトリガーされます。

ID連携を無効にする

グループおよびユーザーの ID フェデレーションを一時的または永続的に無効にすることができます。アイデンティティ フェデレーションが無効になっている場合、StorageGRIDとアイデンティティ ソース間の通信は行われません。ただし、構成した設定はすべて保持されるため、将来、簡単に ID フェデレーションを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、次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なくなります。
- ・ 現在サインインしているフェデレーション ユーザーは、セッションの有効期限が切れるまでStorageGRIDシステムへのアクセスを保持しますが、セッションの有効期限が切れた後はサインインできなくなります。

す。

- StorageGRIDシステムとアイデンティティ ソース間の同期は行われず、同期されていないアカウントに対してアラートは発生しません。
- シングル サインオン (SSO) が有効 または サンドボックス モード に設定されている場合、ID フェデレーションを有効にする チェックボックスは無効になります。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 ページの SSO ステータスを 無効 にする必要があります。見る"[シングルサインオンを無効にする](#)"。

手順

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

OpenLDAP サーバーの設定ガイドライン

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



ActiveDirectory または Azure 以外の ID ソースの場合、StorageGRID は外部的に無効になっているユーザーへの S3 アクセスを自動的にブロックしません。S3 アクセスをブロックするには、ユーザーの S3 キーを削除するか、すべてのグループからユーザーを削除します。

Memberof と 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"]。

インデックス作成

指定されたインデックス キーワードを使用して、次の OpenLDAP 属性を設定する必要があります。

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

さらに、最適なパフォーマンスを得るために、ユーザー名のヘルプに記載されているフィールドがインデックス化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維持に関する情報

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"]。

管理者グループの管理

管理者グループを作成して、1 人以上の管理者ユーザーのセキュリティ権限を管理できます。StorageGRIDシステムへのアクセス権を付与するには、ユーザーはグループに属している必要があります。

開始する前に

- グリッドマネージャにサインインするには、"サポートされているウェブブラウザ"。
- あなたが持っている"特定のアクセス権限"。
- フェデレーション グループをインポートする予定の場合は、ID フェデレーションが構成されており、構成された ID ソースにフェデレーション グループがすでに存在します。

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、グリッド マネージャーおよびグリッド管理 API のどの機能と操作にどのユーザーが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. 構成 > アクセス制御 > *管理者グループ*を選択します。
2. *グループを作成*を選択します。

グループの種類を選択

ローカル グループを作成したり、フェデレーション グループをインポートしたりできます。

- ローカル ユーザーに権限を割り当てる場合は、ローカル グループを作成します。
- アイデンティティ 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ます。これは必要に応じて後で更新できます。たとえば、「メンテナンス ユーザー」や「ILM 管理者」などです。
3. グループの一意の名前を入力します。この名前は後で更新できません。
4. *続行*を選択します。

連合グループ

手順

1. *フェデレーション グループ*を選択します。
2. 構成された ID ソースに表示されるとおりに、インポートするグループの名前を入力します。
 - Active Directory および Azure の場合は、sAMAccountName を使用します。
 - OpenLDAP の場合は、CN (共通名) を使用します。
 - 別の LDAP の場合は、LDAP サーバーの適切な一意の名前を使用します。
3. *続行*を選択します。

グループ権限を管理する

手順

1. アクセス モード 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、それとも設定と機能の表示のみが可能かを選択します。
 - 読み取り/書き込み (デフォルト): ユーザーは設定を変更したり、管理権限で許可された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表示のみが可能です。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属しており、いずれかのグループが 読み取り専用 に設定されている場合、ユーザーは選択したすべての設定と機能に対して読み取り専用アクセス権を持ちます。

2. 1つ以上選択してください"**管理者グループの権限**".

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。フェデレーション グループを作成する場合は、[グループの作成] と [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、このグループのローカル ユーザーを 1 人以上選択します。

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。このグループをユーザー ページに追加できます。見る"**ユーザの管理**"詳細については。

2. *グループの作成*と*完了*を選択します。

管理者グループの表示と編集

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

Task	[操作]メニュー	詳細ページ
グループの詳細を表示	a. グループのチェックボックスを選択します。 b. アクション > *グループの詳細を表示*を選択します。	表内のグループ名を選択します。

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. グループのチェックボックスを選択します。 b. アクション > *グループ名の編集*を選択します。 c. 新しい名前を入力してください。 d. *変更を保存*を選択します。	a. グループ名を選択すると詳細が表示されます。 b. 編集アイコンを選択  。 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. グループのチェックボックスを選択します。 b. アクション > *グループの詳細を表示*を選択します。 c. 必要に応じて、グループのアクセスモードを変更します。 d. 必要に応じて選択またはクリアします"管理者グループの権限"。 e. *変更を保存*を選択します。	a. グループ名を選択すると詳細が表示されます。 b. 必要に応じて、グループのアクセスモードを変更します。 c. 必要に応じて選択またはクリアします"管理者グループの権限"。 d. *変更を保存*を選択します。

グループを複製する

手順

1. グループのチェックボックスを選択します。
2. アクション > *グループの複製*を選択します。
3. 複製グループウィザードを完了します。

グループを削除する

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

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. アクション > *グループの削除*を選択します。
3. *グループの削除*を選択します。

管理者グループの権限

管理者ユーザー グループを作成するときは、グリッド マネージャーの特定の機能へのアクセスを制御するための 1 つ以上の権限を選択します。その後、各ユーザーを 1 つ以上の管理者グループに割り当てて、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 Grid Management 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すべてのユーザーは、次のタスクを実行できます。

- グリッドマネージャーにSign in
- ダッシュボードを見る
- ノードページを表示する
- 現在の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）
- 構成ページとメンテナンスページで提供される特定の情報を表示します

権限とアクセスモードの相互作用

すべての権限について、グループの アクセス モード 設定によって、ユーザーが設定を変更して操作を実行できるかどうか、または関連する設定と機能の表示のみが可能かどうかが決まります。ユーザーが複数のグループに属しており、いずれかのグループが 読み取り専用 に設定されている場合、ユーザーは選択したすべての設定と機能に対して読み取り専用アクセス権を持ちます。

次のセクションでは、管理者グループを作成または編集するとき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、すべてのグリッド管理機能にアクセスできます。

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、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 キーの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には、ルート パスワードの変更 オプションは表示されません。



ルート パスワードの変更 オプションを含むテナント ページへのアクセスを許可するには、テナント アカウント 権限も割り当てます。

グリッドトポロジページの構成

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



グリッド トポロジ ページは非推奨となり、将来のリリースで削除される予定です。

ILM

この権限により、次の **ILM** メニュー オプションにアクセスできます。

- ルール

- ポリシー
- ポリシータグ
- ストレージプール
- 保管グレード
- 地域
- 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 および グリッド トポロジ ページ構成 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。

- 構成 > アクセス制御:
 - グリッドパスワード
- 設定 > ネットワーク:
 - S3エンドポイントのドメイン名
- メンテナンス > タスク:
 - 運用停止
 - 拡張
 - オブジェクトの存在チェック
 - リカバリ
- メンテナンス > システム:
 - 回復パッケージ
 - 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、次のページを表示できますが、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エンドポイントのドメイン名
- 構成 > セキュリティ:
 - 証明書
- 構成 > 監視:
 - 監査および Syslog サーバー

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ます。サイレンス、アラート通知、アラート ルールを管理するには、ユーザー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、次のものへのアクセスが提供されます:

- サポート > ツール > メトリクス ページ
- グリッド管理 API の **Metrics** セクションを使用したカスタム Prometheus メトリック クエリ
- メトリックを含むグリッド マネージャー 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提供されます。

その他のグリッド構成

この権限により、追加のグリッド構成オプションにアクセスできます。



これらの追加オプションを表示するには、ユーザーは **グリッド トポロジ ページの構成** 権限も持っている必要があります。

- **ILM:**
 - 保管グレード
- 構成 > 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、次のことが提供されます。

- グリッド マネージャーを介してストレージ アプライアンス上の E シリーズ SANtricity システム マネージャーにアクセスします。
- これらの操作をサポートするアプライアンスの「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 タスクを実行する機能。

テナントアカウント

この権限により、次のことが可能になります:

- テナントページにアクセスして、テナントアカウントを作成、編集、削除できます。
- 既存のトラフィック分類ポリシーを表示する
- テナントの詳細を含むグリッド マネージャー ダッシュボード カードを表示する

ユーザの管理

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

開始する前に

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

ローカルユーザーを作成する

1 人以上のローカル ユーザーを作成し、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。グループの権限は、ユーザーがアクセスできる Grid Manager および Grid Management API 機能を制御します。

ローカル ユーザーのみを作成できます。外部 ID ソースを使用して、フェデレーション ユーザーとグループを管理します。

グリッド マネージャーには、「root」という名前の定義済みローカル ユーザーが 1 人含まれています。ルートユーザーを削除することはできません。



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. 構成 > アクセス制御 > *管理者ユーザー*を選択します。
2. *ユーザーの作成*を選択します。

ユーザー資格情報を入力してください

手順

1. ユーザーのフルネーム、一意のユーザー名、およびパスワードを入力します。
2. オプションで、このユーザーに Grid Manager または Grid Management API へのアクセスを許可しない場合は、「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 つ以上のグループに割り当てて、ユーザーの権限を決定します。

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

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

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 ユーザーとフェデレーション ユーザーの詳細を表示できます。ローカル ユーザーを変更して、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設定することもできます。

編集できるのはローカル ユーザーのみです。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。

- すべてのローカル ユーザーとフェデレーション ユーザーの基本情報を表示するには、[ユーザー] ページの表を確認します。
- 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、ユーザーが次回グリッド マネージャーからサインアウトし、再度サインインしたときに適用されます。



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

Task	[操作]メニュー	詳細ページ
ユーザーの詳細を表示	a. ユーザーのチェックボックスを選択します。 b. アクション > *ユーザーの詳細を表示*を選択します。	表からユーザーの名前を選択します。
フルネームを編集する（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. アクション > *フルネームの編集*を選択します。 c. 新しい名前を入力してください。 d. *変更を保存*を選択します。	a. 詳細を表示するには、ユーザーの名前を選択します。 b. 編集アイコンを選択 . 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。

Task	[操作]メニュー	詳細ページ
StorageGRIDアクセスを拒否または許可する	a. ユーザーのチェックボックスを選択します。 b. アクション > *ユーザーの詳細を表示*を選択します。 c. [アクセス]タブを選択します。 d. ユーザーが 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、ユーザーがサインインできるようにするには [いいえ] を選択します。 e. *変更を保存*を選択します。	a. 詳細を表示するには、ユーザーの名前を選択します。 b. [アクセス]タブを選択します。 c. ユーザーが 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、ユーザーがサインインできるようにするには [いいえ] を選択します。 d. *変更を保存*を選択します。
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. アクション > *ユーザーの詳細を表示*を選択します。 c. パスワードタブを選択します。 d. 新しいパスワードを入力します。 e. *パスワードの変更*を選択します。	a. 詳細を表示するには、ユーザーの名前を選択します。 b. パスワードタブを選択します。 c. 新しいパスワードを入力します。 d. *パスワードの変更*を選択します。
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. アクション > *ユーザーの詳細を表示*を選択します。 c. [グループ]タブを選択します。 d. 必要に応じて、グループ名の後のリンクを選択して、新しいブラウザ タブでグループの詳細を表示します。 e. 別のグループを選択するには、「グループの編集」を選択します。 f. *変更を保存*を選択します。	a. 詳細を表示するには、ユーザーの名前を選択します。 b. [グループ]タブを選択します。 c. 必要に応じて、グループ名の後のリンクを選択して、新しいブラウザ タブでグループの詳細を表示します。 d. 別のグループを選択するには、「グループの編集」を選択します。 e. *変更を保存*を選択します。

ユーザーを複製する

既存のユーザーを複製して、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. アクション > *重複ユーザー*を選択します。

3. 複製ユーザーウィザードを完了します。

ユーザーを削除する

ローカル ユーザーを削除すると、そのユーザーをシステムから完全に削除できます。



ルートユーザーを削除することはできません。

手順

1. 「ユーザー」 ページで、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. アクション > *ユーザーの削除*を選択します。
3. *ユーザーの削除*を選択します。

シングルサインオン (SSO) を使用する

シングルサインオンを構成する

シングル サインオン (SSO) が有効になっている場合、組織によって実装された SSO サインイン プロセスを使用して資格情報が承認されている場合にのみ、ユーザーは 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。

シングルサインオンの仕組み

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 プロセスがどのように影響を受けるかを確認してください。

SSO が有効になっているときにSign in

SSO が有効になっているときにStorageGRIDにサインインすると、資格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. Web ブラウザに、任意のStorageGRID管理ノードの完全修飾ドメイン名または IP アドレスを入力します。

StorageGRIDSIGN inページが表示されます。

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



Sign in

Account

Sign in

[NetApp support](#) | [NetApp.com](#)

- 以前に Grid Manager または Tenant Manager にアクセスしたことがある場合は、最近のアカウントを選択するか、アカウント ID を入力するように求められます。



Tenant Manager

Recent

Account

Sign in

[NetApp support](#) | [NetApp.com](#)



テナントアカウントの完全なURL（完全修飾ドメイン名またはIPアドレスの後に続く）を入力した場合、StorageGRIDSIGN inページは表示されません。/?accountId=20-digit-account-id）。代わりに、組織のSSOサインインページにすぐにリダイレクトされ、[SSO認証情報でサインイン](#)。

2. グリッド マネージャにアクセスするか、テナント マネージャにアクセスするかを指定します。

- グリッド マネージャにアクセスするには、アカウント 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、最近のアカウントのリストに グリッド マネージャ が表示されている場合はそれを選択します。
- テナント マネージャにアクセスするには、20 桁のテナント アカウント ID を入力するか、最近のアカウントのリストにテナントが表示されている場合は名前でテナントを選択します。

3. *Sign in*を選択

StorageGRID は組織の SSO サインイン ページにリダイレクトします。例えば：

Sign in with your organizational account

someone@example.com

Password

Sign in

4. SSO 資格情報を使用してSign in。

SSO 資格情報が正しい場合:

- a. アイデンティティ 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. 応答が有効であり、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は、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、適切な権限がある場合は、他の管理ノードにアクセスしたり、グリッド マネージャまたはテナント マネージャにアクセスしたりします。

SSO 資格情報を再入力する必要はありません。

SSO が有効になっているときにサインアウトする

StorageGRIDで SSO が有効になっている場合、サインアウト時に何が起こるかは、何にサインインしているか、どこからサインアウトしているか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 リンクを見つけます。
2. *サインアウト*を選択します。

StorageGRIDSigin ページが表示されます。最近のアカウント ドロップダウンが更新され、グリッド マネージャー またはテナントの名前が含まれるようになったため、今後はこれらのユーザー インターフェイスにすばやくアクセスできるようになります。

...にサインインしている場合	そしてサインアウトします...	ログアウトしています...
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上のグリッド マネージャー 注: SSO に Azure 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ことがあります。
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上のテナント マネージャー
グリッドマネージャとテナントマネージャの両方	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。



次の表は、単一のブラウザ セッションを使用している場合にサインアウトすると何が起こるかをまとめたものです。複数のブラウザ セッションにわたってStorageGRIDにサインインしている場合は、すべてのブラウザ セッションから個別にサインアウトする必要があります。

シングルサインオンの要件と考慮事項

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

アイデンティティ プロバイダの要件

StorageGRID は、次の SSO ID プロバイダー (IdP) をサポートしています。

- アクティブ ディレクトリ フェデレーション サービス (AD FS)
- Azure アクティブ ディレクトリ (Azure AD)
- PingFederate

SSO ID プロバイダーを構成する前に、StorageGRIDシステムの ID フェデレーションを構成する必要があります。ID フェデレーションに使用する LDAP サービスのタイプによって、実装できる SSO のタイプが制御されます。

構成された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 • Azure • PingFederate
Azure	Azure

AD FSの要件

AD FS の次のいずれかのバージョンを使用できます。

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



Windows Server 2016では、"[KB3201845 アップデート](#)"、またはそれ以上。

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 以上

Azureに関する考慮事項

SSO タイプとして Azure を使用し、ユーザーのユーザー プリンシパル名にプレフィックスとして sAMAccountName が使用されていない場合、StorageGRID がLDAP サーバー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 サーバー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 は各管理ノードで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に対して証明書利用者信頼 (AD FS)、エンタープライズ アプリケーション (Azure)、またはサービス プロバイダー接続 (PingFederate) を構成する場合は、サーバー証明書をStorageGRID要求の署名証明書として使用します。

まだお持ちでない場合は"[管理インターフェイス用のカスタム証明書を構成しました](#)"、今すぐそうすべきです。カスタム サーバ証明書をインストールすると、その証明書はすべての管理ノードに使用され、すべてのStorageGRID証明書利用者信頼、エンタープライズ アプリケーション、またはSP接続で使用できるようになります。



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接続で管理ノードのデフォルトのサーバー証明書を使用することはお勧めしません。ノードに障害が発生し、それを回復すると、新しいデフォルトのサーバー証明書が生成されます。回復され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ー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`。カスタムサーバー証明書の名前は ``custom-server.crt`。ノードのデフォルトのサーバー証明書の名前は `server.crt`。

ポート要件

シングル サインオン (SSO) は、制限された Grid Manager ポートまたは Tenant Manager ポートでは使用できません。ユーザーをシングル サインオンで認証する場合は、デフォルトの HTTPS ポート (443) を使用する必要があります。見る["外部ファイアウォールでアクセスを制御する"](#)。

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する

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ountの少なくとも 1 人のフェデレーション ユーザーが Grid Manager と 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

- グリッドマネージャにサインインするには、["サポートされているウェブブラウザ"](#)。
- あなたが持っている["特定のアクセス権限"](#)。
- すでに ID フェデレーションを構成しています。

手順

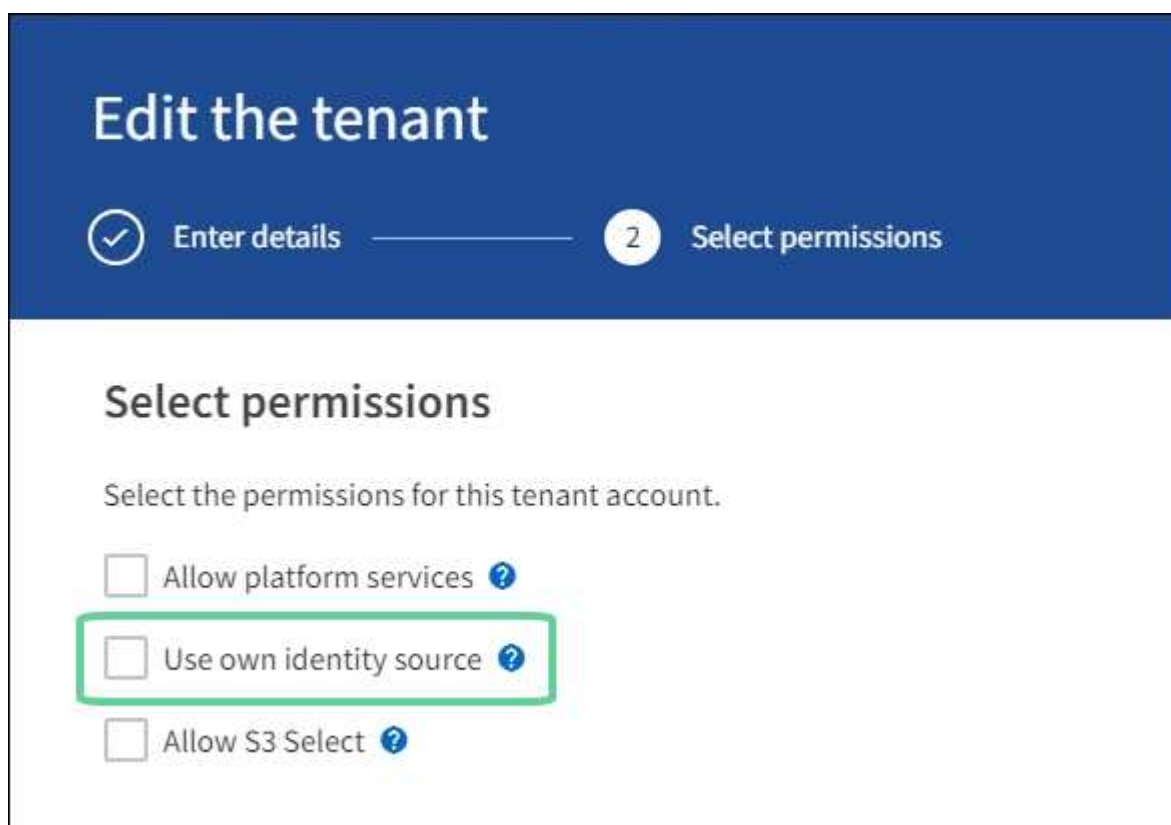
1. 既存のテナント アカountがある場合は、いずれのテナントも独自の ID ソースを使用していないことを確認します。



SSO を有効にすると、テナント マネージャで構成された ID ソースは、グリッド マネージャで構成された ID ソースによって上書きされます。テナントのアイデンティティ ソースに属するユーザーは、Grid Manager アイデンティティ ソースの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ountのテナント マネージャにSign in。
 - b. アクセス管理 > *アイデンティティ連携*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ます。
 - d. そうである場合は、このテナント アカountに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ていることを確認し、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 マネージャから、構成 > アクセス制御 > 管理者グループ を選択します。
 - b. 少なくとも 1 つのフェデレーション グループが Active Directory ID ソースからインポートされ、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ます。

- c. サインアウト。
 - d. フェデレーション グループ内のユーザーとして Grid Manager に再度サインインできることを確認します。
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ます。
- a. グリッド マネージャーから、**TENANTS** を選択します。
 - b. テナント アカウントを選択し、[アクション]>[編集] を選択します。
 - c. 詳細入力タブで、[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 を選択します。



テナント ページが表示されます。

- a. テナント アカウントを選択し、[Sign in] 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。
- b. 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。
- c. グリッド マネージャーからの少なくとも 1 つのフェデレーション グループに、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ます。
- d. サインアウト。
- e. フェデレーション グループ内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ます。

関連情報

- ["シングルサインオンの要件と考慮事項"](#)

- "管理者グループの管理"
- "テナントアカウントを使用する"

サンドボックスモードを使用する

すべてのStorageGRIDユーザーに対してシングル サインオン (SSO) を有効にする前に、サンドボックス モードを使用してシングル サインオン (SSO) を構成してテストすることができます。SSO を有効にした後は、構成を変更または再テストする必要があるときはいつでもサンドボックス モードに戻ることができます。

開始する前に

- グリッドマネージャにサインインするには、"サポートされているウェブブラウザ"。
- あなたは"ルートアクセス権限"。
- StorageGRIDシステムの ID フェデレーションを構成しました。
- ID フェデレーションの **LDAP** サービス タイプ では、使用する予定の SSO ID プロバイダーに基づいて、Active Directory または Azure のいずれかを選択しました。

構成された 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 • Azure • PingFederate
Azure	Azure

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。次に、SSO ID プロバイダーは、認証要求が成功したかどうかを示す認証応答をStorageGRIDに返します。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、ユーザーのユニバーサル一意識別子 (UUID) が含まれます。
- Azure からの応答には、ユーザー プリンシパル名 (UPN) が含まれます。

StorageGRID (サービス プロバイダー) と SSO ID プロバイダーがユーザー認証要求について安全に通信できるようにするには、StorageGRIDで特定の設定を構成する必要があります。次に、SSO ID プロバイダーのソフトウェアを使用して、各管理ノードに対して証明書利用者信頼 (AD FS)、エンタープライズ アプリケーション (Azure)、またはサービス プロバイダー (PingFederate) を作成する必要があります。最後に、StorageGRIDに戻って SSO を有効にする必要があります。

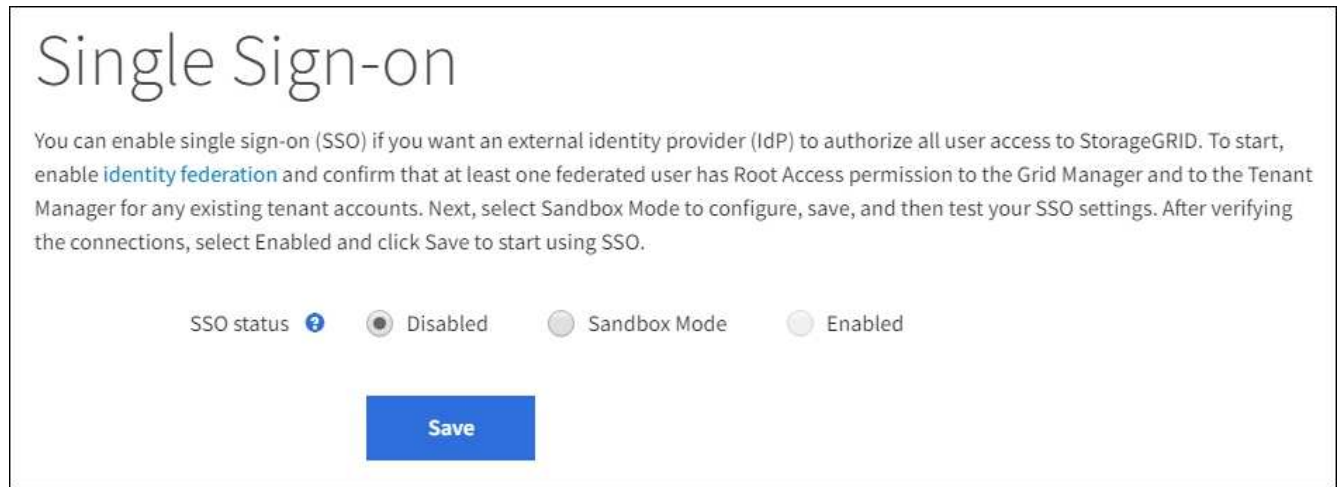
サンドボックス モードを使用すると、この双方向の構成を簡単に実行でき、SSO を有効にする前にすべての設定をテストできます。サンドボックス モードを使用している場合、ユーザーは SSO を使用してサインインできません。

サンドボックスモードにアクセスする

手順

1. 構成 > アクセス制御 > シングル サインオン を選択します。

*無効*オプションが選択された状態で、シングル サインオン ページが表示されます。



SSO ステータス オプションが表示されない場合は、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ていることを確認してください。見る["シングルサインオンの要件と考慮事項"](#)。

2. *サンドボックスモード*を選択します。

アイデンティティプロバイダーセクションが表示されます。

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*を選択します。
2. 選択した SSO タイプに基づいて、アイデンティティ プロバイダー セクションのフィールドに入力します。

Active Directory

- a. Active Directory フェデレーション サービス (AD FS) に表示されるとおりに、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ます。



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

- b. アイデンティティ プロバイダーが StorageGRID 要求に応答して SSO 構成情報を送信するときに、接続を保護するために使用する TLS 証明書を指定します。

- ・オペレーティング システムの **CA** 証明書を使用する: 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、「**CA 証明書**」テキストボックスに貼り付けます。

- ・**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、直ちに「[管理ノードで mgmt-api サービスを再起動します](#)」。

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

- ・たとえば、グリッドに管理ノードが1つしかなく、将来的に管理ノードを追加する予定がない場合は、次のように入力します。SG`または `StorageGRID。
- ・グリッドに複数の管理ノードが含まれている場合は、文字列 [HOSTNAME] `識別子内。例: `SG-[HOSTNAME]`。これにより、ノードのホスト名に基づいて、システム内の各管理ノードの依存パーティ識別子を示すテーブルが生成されます。



StorageGRID システム内の各管理ノードに対して、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対して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。

- d. *保存*を選択します。

*保存*ボタンに緑色のチェックマークが数秒間表示されます。



Azure

- a. アイデンティティ プロバイダーが StorageGRID 要求に応答して SSO 構成情報を送信するとき

に、接続を保護するために使用する TLS 証明書を指定します。

- オペレーティング システムの **CA** 証明書を使用する: 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、「**CA 証明書**」テキストボックスに貼り付けます。

- **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、直ちに**管理ノードで mgmt-api サービスを再起動します。**"グリッド マネージャーへの SSO が成功するかどうかをテストします。

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

- たとえば、グリッドに管理ノードが1つしかなく、将来的に管理ノードを追加する予定がない場合は、次のように入力します。SG`または `StorageGRID。
- グリッドに複数の管理ノードが含まれている場合は、文字列 [HOSTNAME]`識別子内。例: `SG-[HOSTNAME]`。これにより、ノードのホスト名に基づいて、システム内の各管理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テーブルが生成されます。



StorageGRIDシステム内の各管理ノードに対してエンタープライズ 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。

- c. 以下の手順に従ってください**Azure AD でエンタープライズ アプリケーションを作成する**表にリストされている各管理ノードに対してエンタープライズ アプリケーションを作成します。
- d. Azure AD から、各エンタープライズ アプリケーションのフェデレーション メタデータ URL をコピーします。次に、この URL をStorageGRIDの対応する **Federation metadata URL** フィールドに貼り付けます。
- e. 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] を選択します。

*保存*ボタンに緑色のチェックマークが数秒間表示されます。



PingFederate

- a. アイデンティティ プロバイダーがStorageGRID要求に応答して SSO 構成情報を送信するときに、接続を保護するために使用する TLS 証明書を指定します。
- オペレーティング システムの **CA** 証明書を使用する: 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、「**CA 証明書**」テキストボックスに貼り付けます。

- **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、直ちに**"管理ノードで mgmt-api サービスを再起動します。"**グリッド マネージャーへの SSO が成功するかどうかをテストします。

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

- たとえば、グリッドに管理ノードが1つしかなく、将来的に管理ノードを追加する予定がない場合は、次のように入力します。 SG`または `StorageGRID。
- グリッドに複数の管理ノードが含まれている場合は、文字列 [HOSTNAME] `識別子内。例: `SG-[HOSTNAME]`。これにより、ノードのホスト名に基づいて、システム内の各管理ノードのSP接続 ID を示すテーブルが生成されます。



StorageGRIDシステム内の各管理ノードに対してSP接続を作成する必要があります。各管理ノードにSP接続があると、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。

- c. 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>
```

- d. *保存*を選択します。

*保存*ボタンに緑色のチェックマークが数秒間表示されます。

Save 

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**接続を構成する

設定が保存されると、サンドボックス モードの確認通知が表示されます。この通知は、サンドボックス モードが有効になったことを確認し、概要の手順を示します。

StorageGRID は、必要な限りサンドボックス モードのままにすることができます。ただし、シングル サインオン ページで サンドボックス モード が選択されている場合、すべてのStorageGRIDユーザーに対して SSO

が無効になります。ローカルユーザーのみがサインインできます。

証明書利用者信頼 (Active Directory) を構成する、エンタープライズ アプリケーション (Azure) を完了する、またはSP接続 (PingFederate) を構成するには、次の手順に従います。

Active Directory

手順

1. Active Directory フェデレーション サービス (AD FS) に移動します。
2. StorageGRIDシングル サインオン ページの表に示されている各証明書利用者 ID を使用して、StorageGRIDに対して 1 つ以上の証明書利用者信頼を作成します。

表に示されている管理ノードごとに 1 つの信頼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](#)"。

Azure

手順

1. 現在サインインしている管理ノードのシングル サインオン ページで、SAML メタデータをダウンロードして保存するためのボタンを選択します。
2. 次に、グリッド内の他の管理ノードに対して、次の手順を繰り返します。
 - a. ノードにSign in。
 - b. 構成 > 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 ポータルに移動します。
4. 以下の手順に従ってください"[Azure AD でエンタープライズ アプリケーションを作成する](#)"各管理ノードの SAML メタデータ ファイルを対応する Azure エンタープライズ アプリケーションにアップロードします。

PingFederate

手順

1. 現在サインインしている管理ノードのシングル サインオン ページで、SAML メタデータをダウンロードして保存するためのボタンを選択します。
2. 次に、グリッド内の他の管理ノードに対して、次の手順を繰り返します。
 - a. ノードにSign in。
 - b. 構成 > 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 にアクセスします。
4. "[StorageGRIDの 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 (StorageGRIDシングル サインオン 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ます。

表に示されている管理ノードごとに 1 つのSP接続を作成する必要があります。

SSO接続をテストする

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する必要があります。

Active Directory

手順

1. StorageGRIDシングル サインオン ページで、サンドボックス モード メッセージ内のリンクを見つけます。

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派生します。

Sandbox mode

Sandbox mode is currently enabled. Use this mode to configure relying party trusts and to confirm that single sign-on (SSO) and single logout (SLO) are correctly configured for the StorageGRID system.

1. Use Active Directory Federation Services (AD FS) to create relying party trusts for StorageGRID. Create one trust for each Admin Node, using the relying party identifier(s) shown below.
2. Go to your identity provider's sign-on page: <https://ad2016.saml.sgws/adfs/ls/idpinitiatedsignon.htm>
3. From this page, sign in to each StorageGRID relying party trust. If the SSO operation is successful, StorageGRID displays a page with a success message. Otherwise, an error message is displayed.

When you have confirmed SSO for each of the relying party trusts and you are ready to enforce the use of SSO for StorageGRID, change the SSO Status to Enabled, and click Save.

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、ID プロバイダーのサインオン ページにアクセスします。
3. SSO を使用してStorageGRIDにサインインできることを確認するには、* 次のいずれかのサイトに Sign in* を選択し、プライマリ管理ノードの証明書利用者 ID を選択して、**Sign in** を選択します。

You are not signed in.

☐ Sign in to this site.

☒ Sign in to one of the following sites:

SG-DC1-ADM1

Sign in

4. フェデレーションユーザー名とパスワードを入力します。
 - SSO サインインおよびログアウト操作が成功すると、成功メッセージが表示されます。

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

- 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 をクリアして、もう一度お試しください。

5. これらの手順を繰り返して、グリッド内の各管理ノードの SSO 接続を確認します。

Azure

手順

1. Azure ポータルのシングル サインオン ページに移動します。
2. *このアプリケーションをテスト*を選択します。
3. フェデレーション ユーザーの資格情報を入力します。
 - SSO サインインおよび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。

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

- 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 をクリアして、もう一度お試しください。
4. これらの手順を繰り返して、グリッド内の各管理ノードの SSO 接続を確認します。

PingFederate

手順

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

一度に 1 つのリンクを選択してテストします。

Sandbox mode

Sandbox mode is currently enabled. Use this mode to configure service provider (SP) connections and to confirm that single sign-on (SSO) and single logout (SLO) are correctly configured for the StorageGRID system.

1. Use Ping Federate to create SP connections for StorageGRID. Create one SP connection for each Admin Node, using the relying party identifier(s) shown below.
2. Test SSO and SLO by selecting the link for each Admin Node:
 - [https://\[redacted\]/idp/startSSO.ping?PartnerSpId=SG-DC1-ADM1-106-69](https://[redacted]/idp/startSSO.ping?PartnerSpId=SG-DC1-ADM1-106-69)
 - [https://\[redacted\]/idp/startSSO.ping?PartnerSpId=SG-DC2-ADM1-106-73](https://[redacted]/idp/startSSO.ping?PartnerSpId=SG-DC2-ADM1-106-73)
3. StorageGRID displays a success or error message for each test.

When you have confirmed SSO for each SP connection and you are ready to enforce the use of SSO for StorageGRID, change the SSO Status to Enabled, and select **Save**.

2. フェデレーション ユーザーの資格情報を入力します。
 - SSO サインインおよび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。

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

- 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 をクリアして、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 接続を確認します。

「ページの有効期限が切れました」というメッセージが表示された場合は、ブラウザの「戻る」ボタンを選択し、資格情報を再送信してください。

シングルサインオンを有効にする

SSO を使用して各管理ノードにサインインできることを確認したら、StorageGRIDシステム全体に対して 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 Grid Manager、Tenant Manager、Grid Management API、および Tenant Management 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. 構成 > アクセス制御 > シングル サインオン を選択します。
2. SSO ステータスを 有効 に変更します。
3. *保存*を選択します。
4. 警告メッセージを確認し、[OK] を選択します。

シングル サインオンが有効になりました。



Azure ポータルを使用しており、Azure にアクセスするために使用するのと同じコンピューターからStorageGRIDにアクセスする場合は、Azure ポータル ユーザーが承認された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内のユーザー) であることを確認するか、StorageGRIDにサインインする前に Azure ポータルからログアウトしてください。

AD FS で証明書利用者信頼を作成する

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

開始する前に

- StorageGRIDのシングル サインオンを構成し、SSO タイプとして **AD FS** を選択しました。
- グリッド マネージャーのシングル サインオン ページで サンドボックス モード が選択されています。見る["サンドボックスモードを使用する"](#)。
- システム内の各管理ノードの完全修飾ドメイン名 (または IP アドレス) と証明書利用者識別子がわかっています。これらの値は、StorageGRIDシングル サインオン ページの管理ノードの詳細テーブルで確認できます。



StorageGRIDシステム内の各管理ノードに対して、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対して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、Microsoft AD FS ドキュメントにアクセスする必要があります。
- AD FS 管理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

カスタム証明書があるか、コマンド シェルから管理ノードにログインする方法を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。異なるバージョンの AD FS を使用している場合は、手順が若干異なります。ご質問がある場合は、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 を使用すると、1 つ以上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"
```

- のために *Admin_Node_Identifer*、シングル サインオン ページに表示されるとおりに、管理ノードの証明書利用者識別子を入力します。例： SG-DC1-ADM1。
- のために *Admin_Node_FQDN*、同じ管理ノードの完全修飾ドメイン名を入力します。(必要に応じて、代わりにノードの IP アドレスを使用することもできます。ただし、ここに IP アドレスを入力する場合、その IP アドレスが変更されたとき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ります。)に注意してください。

3. Windows Server Manager から、[ツール] > [AD FS 管理] を選択します。

AD FS 管理ツールが表示されます。

4. **AD FS** > 証明書利用者信頼 を選択します。

証明書利用者信頼のリストが表示されます。

5. 新しく作成され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. 新しく作成され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] を選択し、[次へ] を選択します。

e. 「ルール構成」ページで、このルールの表示名を入力します。

たとえば、**ObjectGUID** から **Name ID** または **UPN** から **Name ID** です。

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

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

h. マッピング テーブルの [送信クレーム タイプ] 列で、ドロップダウン リストから [名前 ID] を選択します。

i. *完了*を選択し、*OK*を選択します。

7. メタデータが正常にインポートされたことを確認します。

a. 証明書利用者信頼を右クリックして、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*タブのフィールドに値が入力されていることを確認します。

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

8. これらの手順を繰り返して、StorageGRIDシステム内のすべての管理ノードに対して証明書利用者信頼を構成します。

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して、正しく構成されていることを確認します。見る["サンドボックスモードを使用する"](#)手順についてはこちらをご覧ください。

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、[AD FS 管理] を選択します。

2. [アクション] の下で、[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証明書利用者に関するデータをインポートするを選択します。

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

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

のために `Admin_Node_FQDN`、同じ管理ノードの完全修飾ドメイン名を入力します。(必要に応じて、代わりにノードの IP アドレスを使用することもできます。ただし、ここに IP アドレスを入力する場合、その IP アドレスが変更されたとき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。

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。



表示名を入力するときは、グリッド マネージャーのシングル サインオン ページに表示されるとおりに、管理ノードの依存パーティ識別子を使用します。例: SG-DC1-ADM1。

7. クレームルールを追加します。
 - a. 信頼を右クリックし、[クレーム発行ポリシーの編集] を選択します。
 - b. *ルールを追加*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] を選択し、[次へ] を選択します。
 - d. 「ルールの構成」 ページで、このルールの表示名を入力します。

たとえば、**ObjectGUID** から **Name ID** または **UPN** から **Name ID** です。
 - e. 属性ストアには、**Active Directory** を選択します。
 - f. マッピング テーブルの LDAP 属性列に **objectGUID** と入力するか、**User-Principal-Name** を選択します。
 - g. マッピング テーブルの [送信クレーム タイプ] 列で、ドロップダウン リストから [名前 ID] を選択します。
 - h. *完了*を選択し、*OK*を選択します。
8. メタデータが正常にインポートされたことを確認します。
 - a. 証明書利用者信頼を右クリックして、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*タブのフィールドに値が入力されていることを確認します。

メタデータが見つからない場合、フェデレーション メタデータ アドレスが正しいことを確認するか、値を手動で入力します。
9. これらの手順を繰り返して、StorageGRIDシステム内のすべての管理ノードに対して証明書利用者信頼を構成します。
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して、正しく構成されていることを確認します。見る["サンドボックスモードを使用する"手順](#)についてはこちらをご覧ください。

証明書利用者信頼を手動で作成する

依存部分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、[AD FS 管理] を選択します。
2. [アクション] の下で、[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. *証明書利用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ます。

一貫性を保つために、グリッド マネージャーのシングル サインオン ページに表示されるとおりに、管理ノードの依存パーティ ID を使用します。例：SG-DC1-ADM1。
 - b. オプションのトークン暗号化証明書を構成する手順をスキップします。

- c. [URL の構成] ページで、[**SAML 2.0 WebSSO** プロトコルのサポートを有効にする] チェックボックスをオンにします。
- d. 管理ノードの SAML サービス エンドポイント URL を入力します。

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

のために `Admin_Node_FQDN`、管理ノードの完全修飾ドメイン名を入力します。(必要に応じて、代わりにノードの IP アドレスを使用することもできます。ただし、ここに IP アドレスを入力する場合、その IP アドレスが変更されたとき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. 「識別子の構成」 ページで、同じ管理ノードの依存パーティ識別子を指定します。

`Admin_Node_Identifier`

のために `Admin_Node_Identifier`、シングル サインオン ページに表示されるとおりに、管理ノードの証明書利用者識別子を入力します。例：SG-DC1-ADM1。

- f. 設定を確認し、証明書利用者信頼を保存して、ウィザードを閉じます。

[クレーム発行ポリシーの編集] ダイアログ ボックスが表示されます。



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

- 6. クレーム ルール ウィザードを開始するには、[ルールを追加] を選択します。
 - a. [ルール テンプレートの選択] ページで、リストから [LDAP 属性をクレームとして送信] を選択し、[次へ] を選択します。
 - b. 「ルール構成」 ページで、このルールの表示名を入力します。

たとえば、**ObjectGUID** から **Name ID** または **UPN** から **Name ID** です。
 - c. 属性ストアには、**Active Directory** を選択します。
 - d. マッピング テーブルの LDAP 属性列に **objectGUID** と入力するか、**User-Principal-Name** を選択します。
 - e. マッピング テーブルの [送信クレーム タイプ] 列で、ドロップダウン リストから [名前 ID] を選択します。
 - f. *完了*を選択し、*OK*を選択します。
- 7. 証明書利用者信頼を右クリックして、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) のエンドポイントを構成します。
 - a. *SAML の追加*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. バインド > *リダイレクト*を選択します。
 - d. 信頼できる **URL** フィールドに、この管理ノードからのシングル ログアウト (SLO) に使用する URL を入力します。

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

のために `Admin_Node_FQDN`、管理ノードの完全修飾ドメイン名を入力します。(必要に応じて、代わりにノードの IP アドレスを使用することもできます。ただし、ここに IP アドレスを入力する場合、その IP アドレスが変更されたとき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。

a. 「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ます。
- 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、`/var/local/mgmt-api`管理ノードのディレクトリに`custom-server.crt`証明書ファイル。`



管理ノードのデフォルト証明書を使用する(`server.crt`) は推奨されません。管理ノードに障害が発生した場合、ノードを回復するとデフォルトの証明書が再生成されるため、証明書利用者信頼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。

依存パーティのプロパティが保存され、閉じられます。

10. これらの手順を繰り返して、StorageGRIDシステム内のすべての管理ノードに対して証明書利用者信頼を構成します。
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して、正しく構成されていることを確認します。見る["サンドボックスモードを使用する"](#)手順についてはこちらをご覧ください。

Azure AD でエンタープライズ アプリケーションを作成する

Azure AD を使用して、システム内の各管理ノードに対してエンタープライズ 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 サインオンの構成を開始し、SSO タイプとして **Azure** を選択しました。
- グリッド マネージャーのシングル サインオン ページで サンドボックス モード が選択されています。見る["サンドボックスモードを使用する"](#)。
- システム内の各管理ノードには エンタープライズ アプリケーション名 があります。これらの値は、StorageGRIDシングル サインオン ページの管理ノードの詳細テーブルからコピーできます。



StorageGRIDシステム内の各管理ノードに対してエンタープライズ 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。

- Azure Active Directory でエンタープライズ アプリケーションを作成した経験があること。
- アクティブなサブスクリプションを持つ Azure アカウントがあります。

- Azure 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ること。

Azure AD にアクセスする

手順

1. ログイン "[Azureポータル](#)".
2. 移動先 "[Azure アクティブ ディレクトリ](#)".
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に Azure の SSO 構成を保存するには、Azure を使用して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する必要があります。Azure からフェデレーション メタデータ URL をコピーし、StorageGRIDシングル サインオン ページの対応する フェデレーション メタデータ **URL** フィールドに貼り付けます。

手順

1. 各管理ノードに対して次の手順を繰り返します。
 - a. Azure エンタープライズ アプリケーション ペインで、新しいアプリケーション を選択します。
 - b. *独自のアプリケーションを作成する*を選択します。
 - c. 名前には、StorageGRIDシングル サインオン ページの管理ノードの詳細テーブルからコピーした エンタープライズ アプリケーション名 を入力します。
 - d. ギャラリーに見つから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) ラジオ ボタンを選択したままにします。
 - e. *作成*を選択します。
 - f. **2** の *開始 リンクを選択します。 シングル サインオンの設定 ボックスをクリックするか、左余白の シングル サインオン リンクを選択します。
 - g. **SAML** ボックスを選択します。
 - h. ステップ **3 SAML** 署名証明書 の下にある アプリ フェデレーション メタデータ **URL** をコピーします。
 - i. StorageGRIDシングル サインオン ページに移動し、使用した エンタープライズ アプリケーション名 に対応する フェデレーション メタデータ **URL** フィールドに URL を貼り付けます。
2. 各管理ノードのフェデレーション メタデータ URL を貼り付け、SSO 構成に必要なその他の変更をすべて行った後、StorageGRIDシングル サインオン ページで [保存] を選択します。

すべての管理ノードの**SAML**メタデータをダウンロードする

SSO 構成を保存した後、StorageGRIDシステム内の各管理ノードの 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Sign in。

- b. 構成 > アクセス制御 > シングル サインオン を選択します。
- c. ボタンを選択して、その管理ノードの SAML メタデータをダウンロードします。
- d. ファイルを保存します。このファイルは Azure AD にアップロードされます。

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後、Azure AD で次の手順を実行します。

手順

1. Azure ポータルに戻ります。
2. 各エンタープライズ アプリケーションに対して次の手順を繰り返します。



以前にリストに追加したアプリケーションを表示するには、エンタープライズ アプリケーション ページ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 ページに移動します。
 - b. *割り当てが必要*を*いいえ*に設定します（割り当てを個別に構成する場合を除く）。
 - c. シングル サインオン ページに移動します。
 - d. SAML 構成を完了します。
 - 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、[X] を選択してペインを閉じます。SAML を使用したシングル サインオンの設定ページに戻ります。
3. 以下の手順に従ってください"**サンドボックスモードを使用する**"各アプリケーションをテストします。

PingFederateでサービスプロバイダー（**SP**）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。プロセスを高速化するには、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 サインオンを構成し、SSO タイプとして **Ping Federate** を選択しました。
- グリッド マネージャーのシングル サインオン ページで サンドボックス モード が選択されています。見る"**サンドボックスモードを使用する**"。
- システム内の各管理ノードには * SP接続 ID* があります。これらの値は、StorageGRIDシングル サインオン ページの管理ノードの詳細テーブルで確認できます。
- 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ること。
- あなたはhttps://docs.pingidentity.com/pingfederate/latest/administrators_reference_guide/pf_administrators_reference_guide.html["管理者リファレンスガイド"]PingFederate サーバー用。PingFederate のドキュメント

には、詳細な手順と説明がステップバイステップで記載されています。

- あなたは["管理者権限"](#)PingFederate サーバー用。

タスク概要

これらの手順は、PingFederate Server バージョン 10.3 をStorageGRIDの SSO プロバイダーとして構成する方法をまとめたものです。PingFederate の別のバージョンを使用している場合は、これらの手順を調整する必要がある可能性があります。ご使用のリリースの詳細な手順については、PingFederate Server の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。SP接続を構成するときは、これらの前提条件の情報を使用します。

データストアを作成する

まだ作成していない場合は、PingFederate を AD FS LDAP サーバーに接続するためのデータ ストアを作成します。使用した値を使用してください["アイデンティティ連携の設定"](#)StorageGRIDで。

- タイプ: ディレクトリ (LDAP)
- **LDAP** タイプ: アクティブ ディレクトリ
- 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** を入力します。

パスワード認証情報検証ツールを作成する

まだ作成していない場合は、パスワード資格情報検証を作成してください。

- タイプ: LDAP ユーザー名 パスワード 資格情報検証
- データ ストア: 作成したデータ ストアを選択します。
- 検索ベース: LDAP からの情報を入力します (例: DC=saml、DC=sgws)。
- 検索フィルター: sAMAccountName=\${username}
- スcope: サブツリー

IdPアダプタインスタンスを作成する

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ます。

手順

1. 認証 > 統合 > **IdP** アダプタ に移動します。
2. *新しいインスタンスの作成*を選択します。
3. [タイプ] タブで、[HTML フォーム IdP アダプタ] を選択します。
4. IdP アダプタ タブで、「資格情報検証」に新しい行を追加する を選択します。
5. 選択してください[パスワード認証検証ツール](#)あなたが作成したもの。
6. [アダプタ属性] 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する

署名証明書をまだ作成またはインポートしていない場合は、作成またはインポートします。

手順

1. セキュリティ > 署名と復号化キーと証明書 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接続を作成するときは、管理ノードのStorageGRIDからダウンロードした 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、必要な特定の値が多数含まれています。



ユーザーが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るように、StorageGRID システム内の各管理ノードに対してSP接続を作成する必要があります。最初のSP接続を作成するには、次の手順に従います。次に、[追加のSP接続を作成する](#)必要な追加の接続を作成します。

SP接続タイプを選択

手順

1. アプリケーション > 統合 > * SP接続* に移動します。
2. *接続の作成*を選択します。
3. *この接続に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*ブラウザSSOプロファイル*と*SAML 2.0*を選択します。

SPメタデータをインポートする

手順

1. [メタデータのインポート] タブで、[ファイル] を選択します。
2. 管理ノードのStorageGRIDシングル サインオン ページからダウンロードした SAML メタデータ ファイルを選択します。
3. メタデータの概要と、[一般情報] タブに表示される情報を確認します。

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

4. *次へ*を選択します。

IdPブラウザSSOを構成する

手順

1. [ブラウザ SSO] タブから、[ブラウザ SSO の構成] を選択します。
2. SAML プロファイル タブで、* SP開始 SSO*、* SP開始 SLO*、* IdP 開始 SSO*、および * IdP 開始 SLO* オプションを選択します。
3. *次へ*を選択します。

4. 「アサーションの有効期間」タブでは、変更を加えません。
5. [アサーション作成] タブで、[アサーション作成の構成] 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. [属性コントラクト] タブで、属性コントラクトとして **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. 契約の延長の場合は、「削除」を選択して削除します。`urn:oid`は使用されません。

マップアダプタインスタンス

手順

1. 認証ソース マッピング タブで、新しいアダプタ インスタンスのマップ を選択します。
2. アダプタインスタンスタブで、[アダプタインスタンス](#)あなたが作成したもの。
3. マッピング方法タブで、*データ ストアから追加の属性を取得する*を選択します。
4. [属性ソースとユーザー検索] タブで、[属性ソースの追加] を選択します。
5. データストアタブで説明を入力し、[データストア](#)と追加しました。
6. LDAP ディレクトリ検索タブ:
 - **Base DN** を入力します。これは、LDAP サーバーのStorageGRIDで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 クラスの場合は、**objectGUID** または **userPrincipalName** のいずれかの属性を検索して追加します。
7. LDAP バイナリ属性エンコード タイプ タブで、**objectGUID** 属性に **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. [属性コントラクトの履行] 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** のいずれかを選択します。
10. 属性ソースを確認して保存します。
11. フェールセーブ属性ソースタブで、*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 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（バインディングおよび `/api/saml-response` エンドポイント URL 用）。
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（バインディングおよび `/api/saml-logout` エンドポイント URL 用）。
4. [許可される SAML バインディング] タブで、**ARTIFACT** と **SOAP** をクリアします。 **POST** と **REDIRECT** のみが必要です。

5. [署名ポリシー] タブで、[認証リクエストに署名を要求する] および [アサーションに常に署名する] チェックボックスをオンのままにします。
6. [暗号化ポリシー] タブで、[なし] を選択します。
7. 概要を確認し、[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 SSO 設定を保存します。

クレデンシャルを設定

手順

1. SP接続タブから、*資格情報*を選択します。
2. [資格情報] タブから、[資格情報の構成] を選択します。
3. 選択してください [署名証明書](#) 作成またはインポートした。
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。コピーごとに新しいメタデータをアップロードします。



異なる管理ノードのSP接続では、パートナーのエンティティ ID、ベース URL、接続 ID、接続名、署名検証、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初期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. コピーの接続 ID と接続名を入力し、[保存] を選択します。
3. 管理ノードに対応するメタデータ ファイルを選択します。
 - a. アクション > *メタデータで更新*を選択します。
 - b. *ファイルを選択*を選択し、メタデータをアップロードします。
 - c. *次へ*を選択します。
 - d. *保存*を選択します。
4. 未使用の属性によるエラーを解決します。
 - a. 新しい接続を選択します。
 - b. ブラウザ **SSO** の構成 > アサーション作成の構成 > 属性コントラクト 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。

シングルサインオンを無効にする

この機能を使用しなくなくなった場合は、シングル サインオン (SSO) を無効にすることができます。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

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

手順

1. 構成 > 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. *無効*オプションを選択します。
3. *保存*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。

4. 「OK」を選択します。

次回StorageGRIDにサインインするときに、StorageGRIDSig inページが表示されるので、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。

1つの管理ノードのシングルサインオンを一時的に無効にし、再度有効にする

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

開始する前に

- あなたが持っている"[特定のアクセス権限](#)"。
- あなたは `Passwords.txt` ファイル。
- ローカル ルート ユーザーのパスワードを知っています。

タスク概要

1 つの管理ノードの SSO を無効にした後、ローカル ルート ユーザーとして Grid Manager にサインインできます。StorageGRIDシステムを保護するには、サインアウトしたら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 マネージャのシングル サインオン ページの **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、更新しない限り既存の SSO 設定は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`
- 記載されているパスワードを入力してください `Passwords.txt` ファイル。
- ルートに切り替えるには、次のコマンドを入力します。 `su -`
- 記載されているパスワードを入力してください `Passwords.txt` ファイル。

ルートとしてログインすると、プロンプトは `$` に `#`。

2. 次のコマンドを実行します。 `disable-saml`

メッセージは、コマンドがこの管理ノードにのみ適用されることを示します。

3. SSO を無効にすることを確認します。

ノード上でシングル サインオンが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. Web 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で Sign in。

6. SSO 構成を修正する必要があるために SSO を一時的に無効にした場合:

- 構成 > アクセス制御 > シングル サインオン を選択します。
- 不正確または古い SSO 設定を変更します。
- *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、グリッド全体の SSO が自動的に再度有効になります。

7. 他の理由でグリッド マネージャーにアクセスする必要があるため、SSO を一時的に無効にした場合:

- 実行する必要があるタスクをすべて実行します。
- *サインアウト*を選択し、グリッド マネージャーを閉じます。
- 管理ノードで SSO を再度有効にします。次のいずれかの手順を実行できます。

- 次のコマンドを実行します。 `enable-saml`

メッセージは、コマンドがこの管理ノードにのみ適用されることを示します。

SSO を有効にすることを確認します。

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

- グリッド ノードを再起動します。 `reboot`

8. Web ブラウザから、同じ管理ノードからグリッド マネージャーにアクセスします。

9. StorageGRIDSIGN in ページが表示され、Grid Manager にアクセスするには SSO 資格情報を入力する必要があります。

グリッドフェデレーションを使用する

グリッドフェデレーションとは何ですか？

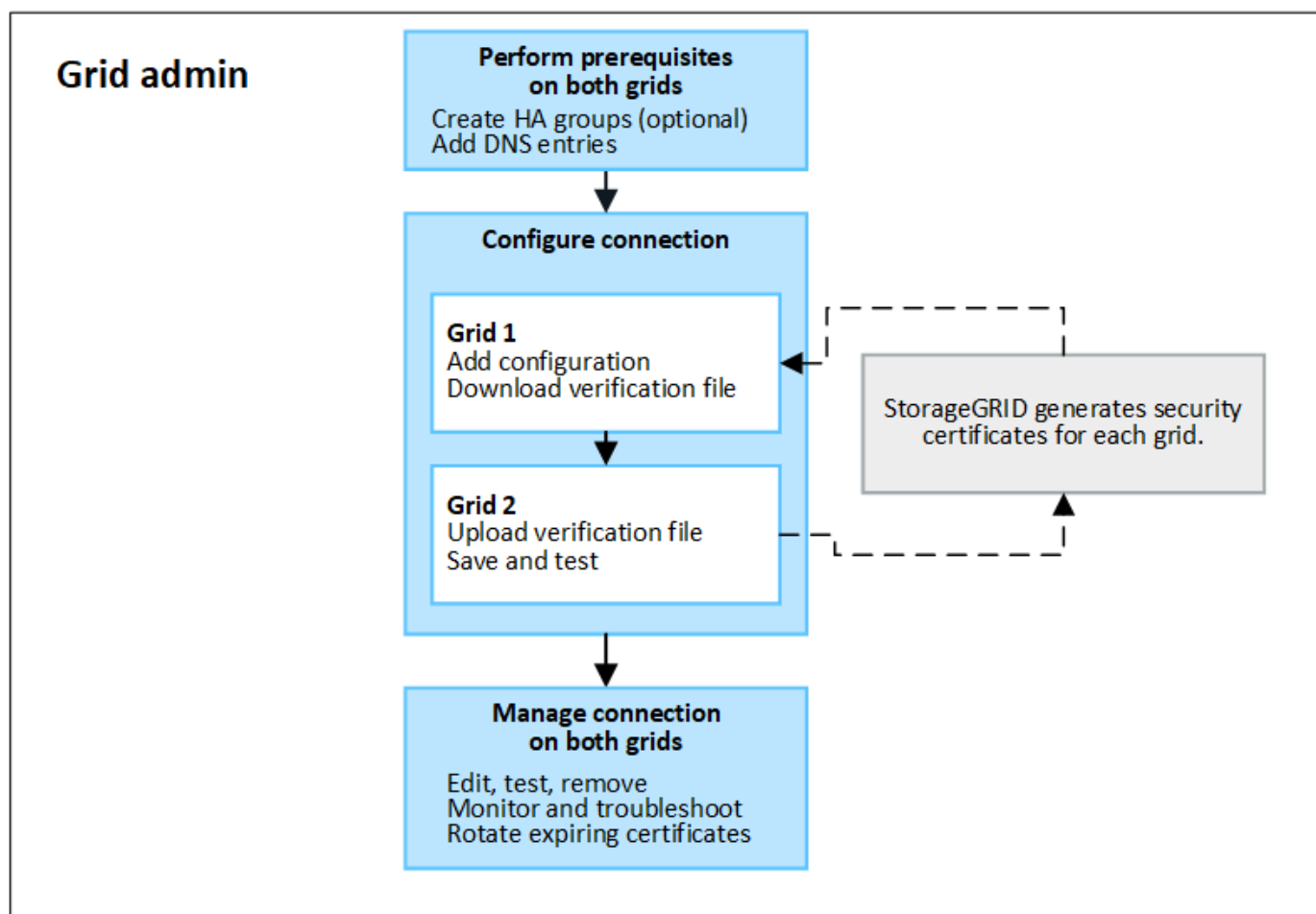
グリッド フェデレーションを使用すると、テナントのクローンを作成し、そのオブジェクトを 2 つのStorageGRIDシステム間で複製して災害復旧を行うことができます。

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システム内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。

グリッドフェデレーションのワークフロー

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



グリッドフェデレーション接続に関する考慮事項と要件

- グリッド フェデレーションに使用するグリッドでは、同一のStorageGRIDバージョンが実行されている

か、メジャー バージョンの違いが 1 つ以下である必要があります。

バージョン要件の詳細については、"[リリース ノート](#)"。

- グリッドには、他のグリッドへの 1 つ以上のグリッド フェデレーション接続を設定できます。各グリッド フェデレーション接続は、他の接続からは独立しています。たとえば、グリッド 1 にグリッド 2 との接続が 1 つあり、グリッド 3 との接続が 2 つある場合、グリッド 2 とグリッド 3 の間には暗黙的な接続はありません。
- グリッド フェデレーション接続は双方向です。接続が確立されると、どちらのグリッドからも接続を監視および管理できます。
- 使用する前に、少なくとも1つのグリッドフェデレーション接続が存在している必要があります。"[アカウントクローン](#)"または"[クロスグリッドレプリケーション](#)"。

ネットワークとIPアドレスの要件

- グリッド フェデレーション接続は、グリッド ネットワーク、管理ネットワーク、またはクライアント ネットワークで発生します。
- グリッド フェデレーション接続は、1 つのグリッドを別のグリッドに接続します。各グリッドの構成では、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接続することです"[高可用性 \(HA\) グループ](#)"各グリッド上のゲートウェイノードと管理ノード。 HA グループを使用すると、ノードが使用できなくなった場合でも、グリッド フェデレーション接続がオンラインのままになることが保証されます。いずれかの HA グループのアクティブ インターフェイスに障害が発生した場合、接続ではバックアップ インターフェイスを使用できます。
- 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お勧めしません。ノードが使用できなくなった場合、グリッド フェデレーション接続も使用できなくなります。
- "[クロスグリッドレプリケーション](#)"オブジェクトを管理するには、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された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ルートを持っていることを確認します。

FQDNを使用して接続の負荷を分散する

運用環境では、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、次のように適切な DNS エントリを作成します。

- グリッド 1 の FQDN は、グリッド 1 内の HA グループの 1 つ以上の仮想 IP (VIP) アドレス、またはグリッド 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 アドレスにマップされます。
- グリッド 2 の FQDN は、グリッド 2 の 1 つ以上の VIP アドレス、またはグリッド 2 内の 1 つ以上の管理ノードまたはゲートウェイ ノードの IP アドレスにマップされます。

複数の DNS エントリを使用する場合、接続を使用する要求は次のように負荷分散されます。

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

ポート要件

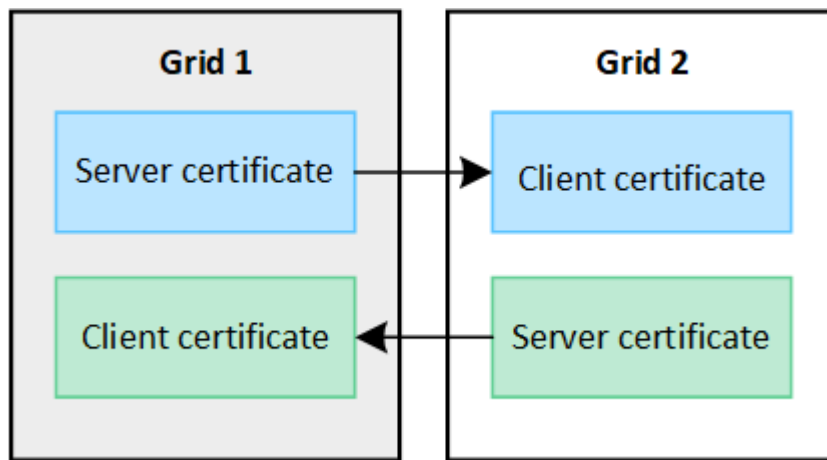
グリッド フェデレーション接続を作成するときに、23000 から 23999 までの未使用のポート番号を指定できます。この接続の両方のグリッドは同じポートを使用します。

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ていないことを確認する必要があります。

証明書の要件

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

- グリッド 1 からグリッド 2 に送信される情報を認証および暗号化するためのサーバ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」アラートが表示され、証明書のローテーションを促すメッセージが表示されます。これは、グリッド マネージャーを使用して実行できます。



接続のいずれかの端の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になります。

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を管理する"](#)
- ["グリッドフェデレーションエラーのトラブルシューティング"](#)

アカウントクローンとは何ですか？

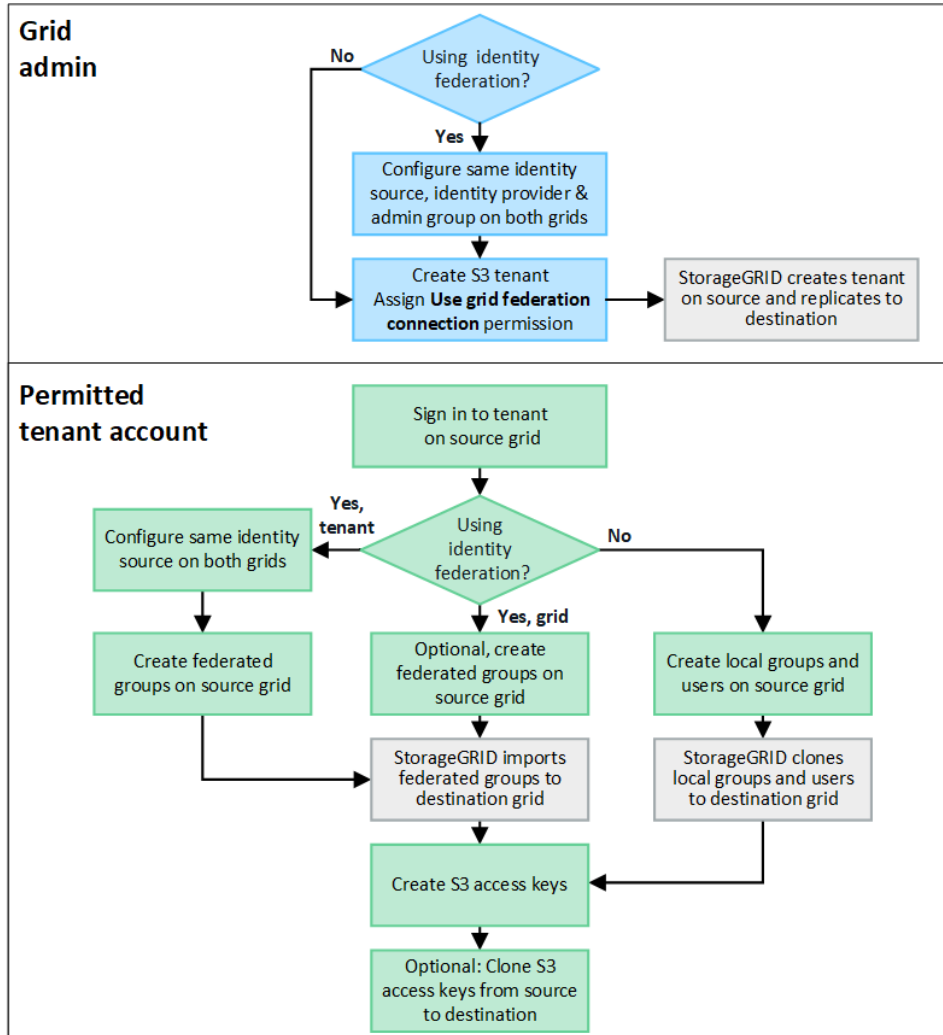
アカウントクローンとは、テナントアカウント、テナントグループ、テナントユーザー、およびオプションでS3アクセスキーをStorageGRIDシステム間で自動的に複製することです。"[グリッドフェデレーション接続](#)"。

アカウントのクローンが必要です"[クロスグリッドレプリケーション](#)"。ソースStorageGRIDシステムから宛

先StorageGRIDシステムにアカウント情報を複製すると、テナント ユーザーとグループは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構成されている](#)"。



グリッド管理ワークフロー

グリッド管理者が実行する手順は、グリッド内のStorageGRIDシステムが"[グリッドフェデレーション接続](#)"シングル サインオン (SSO) または ID フェデレーションを使用します。

アカウントクローンのSSOを設定する (オプション)

グリッド フェデレーション接続内のいずれかのStorageGRIDシステムが SSO を使用する場合は、両方のグリッドで SSO を使用する必要があります。グリッド フェデレーション用のテナント アカウントを作成する前に、テナントのソース グリッドと宛先グリッドのグリッド管理者は次の手順を実行する必要があります。

手順

1. 両方のグリッドに同じ ID ソースを構成します。見る"[アイデンティティフェデレーションを使用する](#)"。

2. 両方のグリッドに同じ SSO ID プロバイダー (IdP) を構成します。見る["シングルサインオンを構成する"](#)。
3. ["同じ管理者グループを作成する"](#)同じフェデレーション グループをインポートすることで、両方のグリッドで実行できます。

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



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

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

いずれかのStorageGRIDシステムが SSO なしで 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 フェデレーション用のテナント アカウントを作成する前に、テナントのソース グリッドと宛先グリッドのグリッド管理者は次の手順を実行する必要があります。

手順

1. 両方のグリッドに同じ ID ソースを構成します。見る["アイデンティティフェデレーションを使用する"](#)。
2. オプションとして、フェデレーショングループがソーステナントアカウントと宛先テナントアカウントの両方に対して初期ルートアクセス権限を持つ場合、["同じ管理者グループを作成する"](#)同じフェデレーショングループをインポートすることで、両方のグリッドで実行できます。



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ると、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に対する初期のルート アクセス権限を付与したくない場合は、ローカル ルート ユーザーのパスワードを指定します。

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構成した後、グリッド管理者は次の手順を実行して、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決定します。

手順

1. アカウント クローン操作のテナントのソース グリッドとするグリッドを決定します。

テナントが最初に作成されたグリッドは、テナントの 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 宛先グリッド と呼ばれます。

2. そのグリッドで、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ます。

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、ソース テナント アカウントと宛先テナント アカウントの両方で同じ ID ソースを構成する必要があります。両方のグリッドが同じ ID ソースを使用しない限り、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、宛先テナ

ントに複製できません。

5. 特定のグリッド フェデレーション接続を選択します。
6. 新しいテナント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の使用 権限を持つ新しいテナントが保存されると、StorageGRID は次のように他のグリッドにそのテナントのレプリカを自動的に作成します。

- 両方のテナント アカウントには、同じアカウント ID、名前、ストレージ クォータ、割り当てられた権限があります。
- テナントのルート アクセス権限を持つフェデレーション 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。
- テナントのルート 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"](#)。

許可されたテナントアカウントワークフロー

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複製された後、許可されたテナント アカウントはこれらの手順を実行して、テナント グループ、ユーザー、および S3 アクセス キーを複製できます。

手順

1. テナントのソース グリッド上のテナント アカウントにSign in。
2. 許可されている場合は、ソース テナント アカウントと宛先テナント アカウントの両方で ID フェデレーションを構成します。
3. ソーステナントにグループとユーザーを作成します。

ソース テナントに新しいグループまたはユーザーが作成されると、StorageGRID はそれらを宛先テナントに自動的に複製しますが、宛先からソースへの複製は行われません。

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に S3 アクセスキーを複製します。

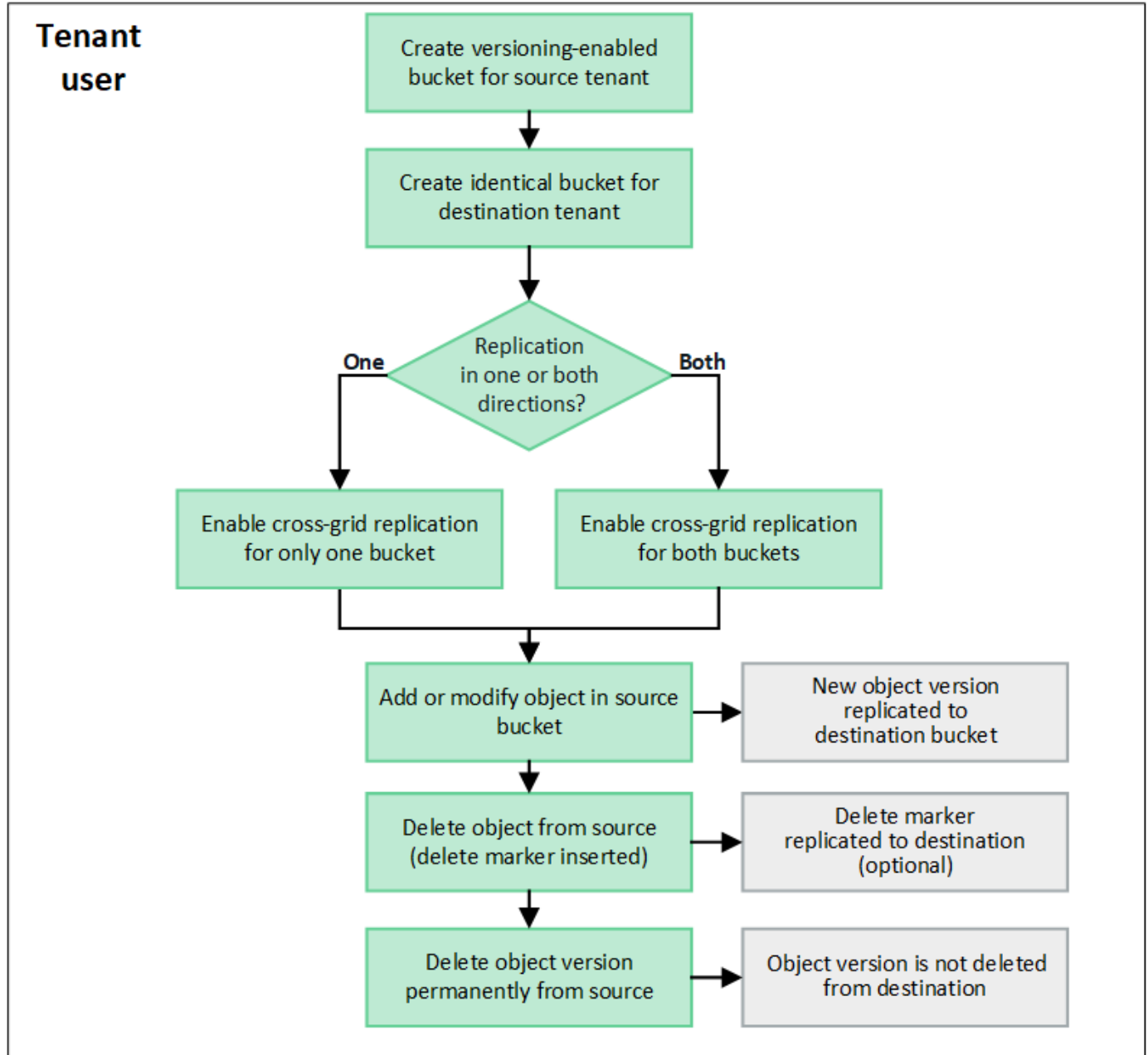
許可されたテナントアカウントのワークフローの詳細と、グループ、ユーザー、S3アクセスキーのクローン作成方法については、以下を参照してください。["テナントグループとユーザーの複製"](#)そして["API を使用して S3 アクセスキーを複製する"](#)。

クロスグリッドレプリケーションとは何ですか？

クロスグリッドレプリケーションとは、2つのStorageGRIDシステム間で接続された選択されたS3バケット間でのオブジェクトの自動レプリケーションです。["グリッドフェデレーション接続"](#)。["アカウントのクローン"](#)クロスグリッドレプリケーションには必要です。

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の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。



クロスグリッド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](#)"ルートアクセス権限を持つテナント ユーザーは、各グリッドの対応するテナント アカウントに同一のバケットを作成できます。これらのバケット:

- 名前は同じである必要がありますが、地域は異なっていても構いません
- バージョン管理が有効になっている必要があります
- S3 オブジェクトロックを無効にする必要があります

- 空である必要があります

両方のバケットが作成された後、いずれか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構成できます。

詳細情報

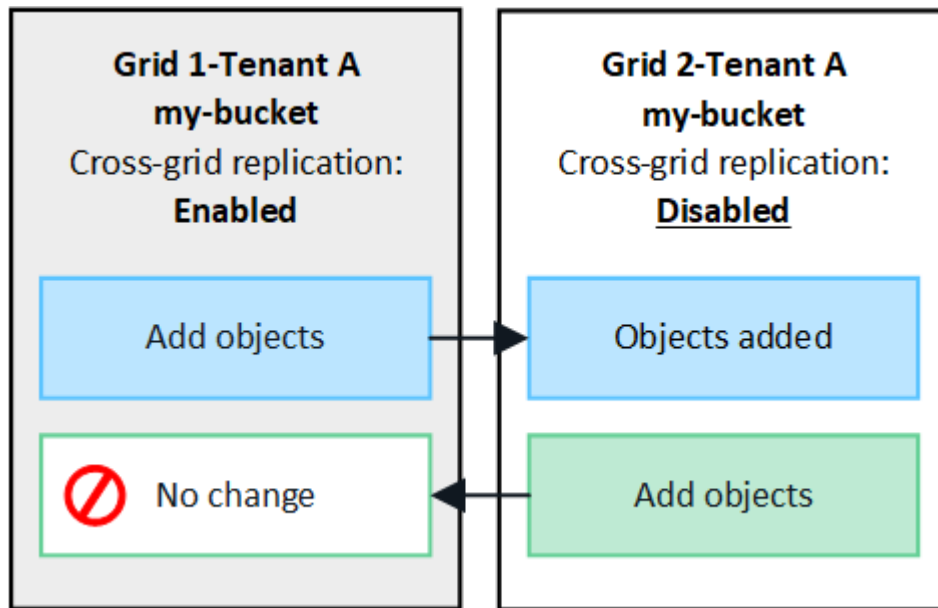
"クロスグリッドレプリケーションを管理する"

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されるように構成できます。

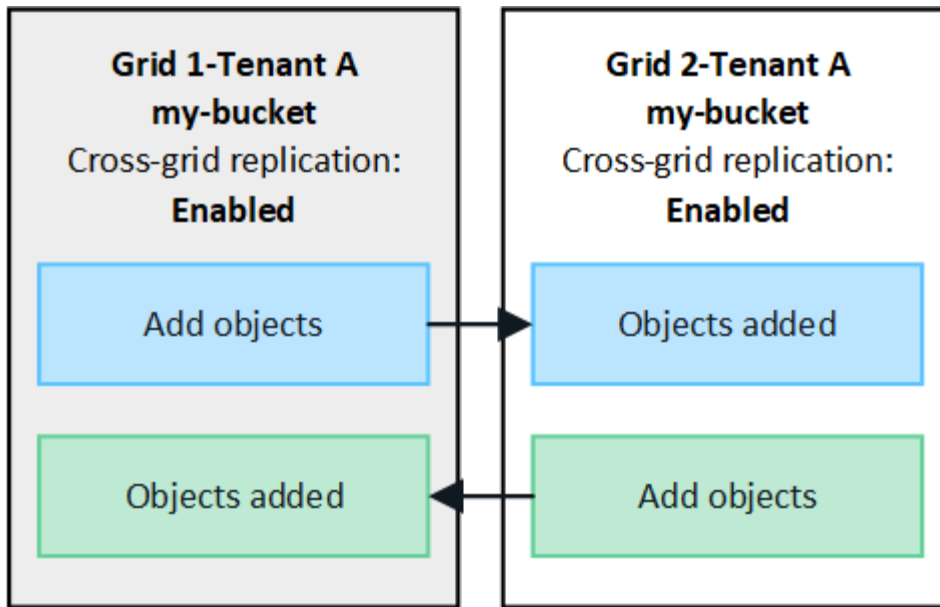
一方向の複製

1 つのグリッドのみのバケットに対してグリッド間レプリケーションを有効にすると、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、他のグリッド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複製されません。図では、クロスグリッドレプリケーションが有効になっています。`my-bucket` グリッド 1 からグリッド 2 への方向は有効になっていますが、逆方向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のクロスグリッド 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が他のグリッドに複製されます。図では、クロスグリッドレプリケーションが有効になっています。`my-bucket` 両方向に。



オブジェクトが撮取されると何が起こりますか？

S3 クライアントが、クロスグリッド レプリケーションが有効になっているバケットにオブジェクトを追加すると、次のことが起こります。

1. StorageGRID は、ソース バケットから宛先バケットに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を実行する時間は、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 リクエストを発行してオブジェクトのレプリケーション ステータスを確認できます。レスポンスにはStorageGRID固有の `x-ntap-sg-cgr-replication-status` 応答ヘッダーには、次のいずれかの値が含まれます。S3 クライアントは、GetObject または HeadObject リクエストを発行して、オブジェクトのレプリケーション ステータスを確認できます。レスポンスにはStorageGRID固有の `x-ntap-sg-cgr-replication-status` レスポンス ヘッダーは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: すべてのグリッド接続のレプリケーションが成功しました。 - 保留中: オブジェクトは少なくとも 1 つのグリッド接続に複製されていません。 - 失敗: どのグリッド接続でもレプリケーションは保留中ではなく、少なくとも 1 つ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	REPLICA: オブジェクトはソース グリッドから複製されました。



StorageGRIDはサポートしていません `x-amz-replication-status` ヘッダ。

2. StorageGRID は、他のオブジェクトと同様に、各グリッドのアクティブな ILM ポリシーを使用してオブジェクトを管理します。たとえば、グリッド 1 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 消失訂正符号を使用して保存され、3 年後に削除される可能性があります。

オブジェクトが削除されると何が起きますか？

記載の通り"[データフローを削除](#)"StorageGRID は、次のいずれかの理由でオブジェクトを削除することがあります。

- 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ユーザーが"[バケット内のオブジェクトを削除する](#)"バケットからすべてのオブジェクトを削除するオプション。
- バケットには有効期限のあるライフサイクル構成があります。
- オブジェクトの ILM ルールの最後の期間が終了し、それ以上の配置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有効期限、または ILM 配置の有効期限のためにオブジェクトを削除した場合、複製されたオブジェクトはグリッド フェデレーション接続内の他のグリッドから削除されることはありません。ただし、S3 クライアントの削除によってソースバケットに追加された削除マーカは、オプションで宛先バケットに複製できます。

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した場合に何が起るかを理解するには、次のように、S3 クライアントがバージョン管理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方法を確認します。

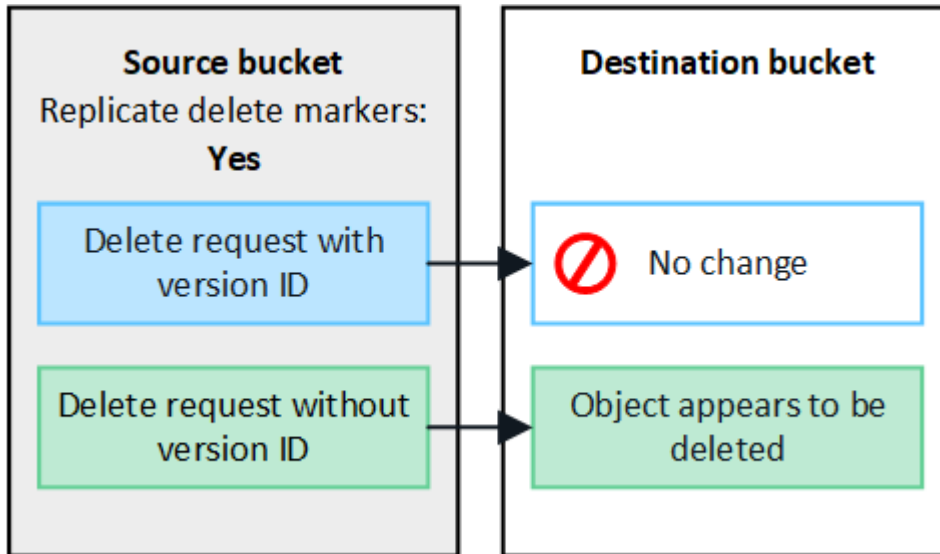
- S3 クライアントがバージョン ID を含む削除リクエストを発行すると、オブジェクトのそのバージョンは完全に削除されます。バケットに削除マーカは追加されません。
- S3 クライアントがバージョン ID を含まない削除リクエストを発行した場合、StorageGRID はオブジェクト バージョンを削除しません。代わりに、バケットに削除マーカを追加します。削除マーカにより、StorageGRID はオブジェクトが削除されたかのように動作します。
 - バージョンIDのないGetObjectリクエストは失敗します。404 No Object Found
 - 有効なバージョン ID を持つ GetObject 要求は成功し、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 は次のように削除要求を宛先に複製するかどうかを決定します。

- 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 を含む削除要求を複製しないため、同じオブジェクト バージョンは宛先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に基づいて、オプションで削除マーカを複製できます。
 - 削除マーカを複製することを選択した場合 (デフォルト)、削除マーカがソース バケットに追加され、宛先バケットに複製されます。実際には、オブジェクトは両方のグリッドで削除されたように見えます。
 - 削除マーカを複製しないことを選択した場合、削除マーカ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。実際には、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、[*削除マーカの複製*](#)が*はい*に設定されています。["クロスグリッドレプリケーションが有効になりました"](#)。バージョン ID を含むソース バケットの削除リクエストでは、宛先バケットからオブジェクトは削

除されません。バージョン ID を含まないソース バケット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表示されます。



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

暗号化されたオブジェクトが複製される仕組み

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レプリケートする場合、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構成したりすることができます。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ときに SSE (StorageGRID管理キーを使用したサーバー側暗号化) を使用できます。使用 `x-amz-server-side-encryption` リクエストヘッダーを指定して `AES256`。見る"[サーバー側の暗号化を使用する](#)"。



SSE-C (顧客提供のキーを使用したサーバー側暗号化) の使用は、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。取り込み操作は失敗します。

バケットにデフォルトの暗号化を使用するには、`PutBucketEncryption` リクエストを使用し、`SSEAlgorithm` パラメータに `AES256`。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。見る"[バケットの操作](#)"。

グリッド レベルの暗号化を使用するには、保存されたオブジェクトの暗号化 オプションを **AES-256** に設定します。グリッドレベルの暗号化は、バケットレベルで暗号化されていないオブジェクト、またはバケットレベルで暗号化されずに取り込まれたオブジェクトに適用されます。`x-amz-server-side-encryption` リクエストヘッダー。見る"[ネットワークとオブジェクトのオプションを構成する](#)"。



SSEはAES-128をサポートしません。**AES-128** オプションを使用してソース グリッドに対して保存されたオブジェクトの暗号化 オプションが有効になっている場合、AES-128 アルゴリズムの使用はレプリケートされたオブジェクトに伝播されません。代わりに、複製されたオブジェクトは、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 (使用可能な場合) 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に、StorageGRID は次のルールを適用します。

1. 使用 `x-amz-server-side-encryption` 存在する場合、インジェスト ヘッダー。
2. 取り込み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（構成されている場合）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（構成されている場合）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ないでください。

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に、StorageGRID は次の順序でルールを適用します。

1. 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を使用します。
2. ソース オブジェクトが暗号化されていないか、AES-128 を使用している場合は、宛先バケットのデフォルトの暗号化設定（構成されている場合）を使用します。
3. 宛先バケットに暗号化設定がない場合、宛先のグリッド全体の暗号化設定（構成されている場合）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ないでください。

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ではサポートされません。

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 is not available for buckets that have cross-grid replication configured。

セグメント化されたオブジェクト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と、ソース グリッドの 最大セグメント サイズ 設定 ([構成] > *システム > ストレージ オプション) が両方のグリッドで使用されます。たとえば、ソース グリッドの最大セグメント サイズが 1 GB で、宛先グリッドの最大セグメント サイズが 50 MB であるとします。ソース グリッドに 2 GB のオブジェクトを取り込むと、そのオブジェクトは 2 つの 1 GB セグメントとして保存されます。また、グリッドの最大セグメント サイズが 50 MB であるにもかかわらず、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。

クロスグリッドレプリケーションと**CloudMirror**レプリケーションを比較する

グリッドフェデレーションの使用を開始する際には、以下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](#)"そして"[StorageGRID CloudMirror レプリケーション サービス](#)"。

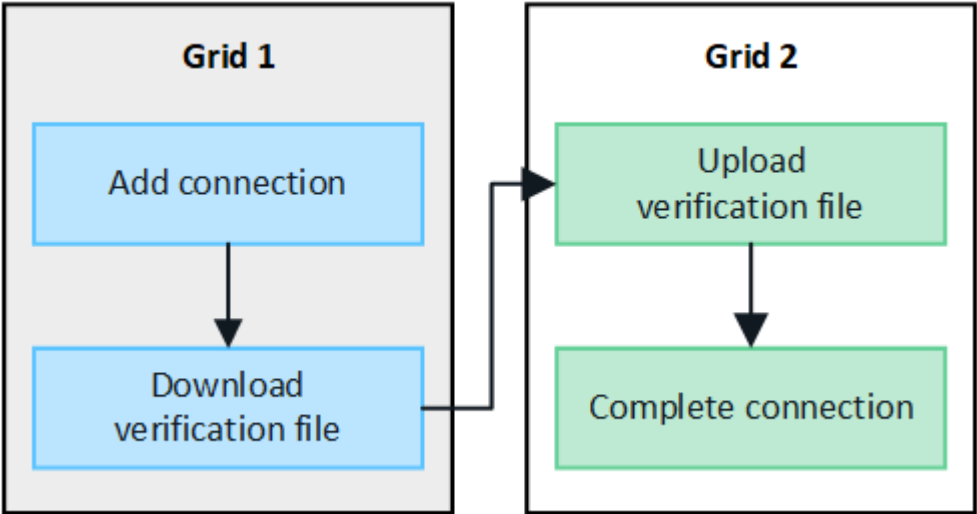
	クロスグリッドレプリケーション	CloudMirrorレプリケーションサービス
主な目的は何ですか？	1 つのStorageGRIDシステムが災害復旧システムとして機能します。バケット内のオブジェクトは、グリッド間で一方向または双方向に複製できます。	テナントがStorageGRID内のバケット (ソース) から外部の S3 バケット (宛先) にオブジェクトを自動的に複製できるようにします。 CloudMirror レプリケーションは、独立した S3 インフラストラクチャ内にオブジェクトの独立したコピーを作成します。この独立したコピーはバックアップとしては使用されませんが、多くの場合、クラウドでさらに処理されます。
どのように設定されていますか？	2 つのグリッド間のグリッド フェデレーション接続を構成します。 - 新しいテナント アカウントを追加します。これは他のグリッドに自動的に複製されます。 - 新しいテナント グループとユーザーを追加します。こ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、一方向または双方向でグリッド間のレプリケーションを有効にします。	- テナント ユーザーは、テナント マネージャーまたは S3 API を使用して CloudMirror エンドポイント (IP アドレス、資格情報など) を定義することにより、CloudMirror レプリケーションを構成します。 - 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構成できます。
設定の責任者は誰ですか？	- グリッド管理者は接続とテナントを構成します。 - テナント ユーザーは、グループ、ユーザー、キー、バケットを構成します。	通常は、テナント ユーザーです。
目的地はどこですか？	グリッド フェデレーション接続内の他のStorageGRIDシステム上の対応する同一の S3 バケット。	- 互換性のある任意の S3 インフラストラクチャ (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須ですか？	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のバージョン管理が有効になっている必要があります。	いいえ、CloudMirror レプリケーションでは、ソースと宛先の両方で、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がサポートされます。
オブジェクトが目的地に移動される原因は何ですか？	オブジェクトは、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に追加されると、自動的にレプリケートされます。	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、自動的に複製されます。バケットが CloudMirror エンドポイントで構成される前にソース バケットに存在していたオブジェクトは、変更されない限り複製されません。

	クロスグリッドレプリケーション	CloudMirrorレプリケーションサービス
オブジェクトはどのように複製されますか？	クロスグリッドレプリケーションではバージョン管理されたオブジェクトが作成され、バージョン ID がソース バケットから宛先バケットに複製されます。これにより、両方のグリッド間でバージョンの順序を維持できます。	CloudMirror レプリケーションではバージョン管理が有効なバケットは必要ないため、CloudMirror はサイト内のキーの順序のみを維持できます。別のサイトにあるオブジェクトへのリクエストの順序が維持されるという保証はありません。
オブジェクトを複製できない場合はどうなりますか？	オブジェクトは、メタデータ ストレージの制限に従って、レプリケーションのキューに入れます。	オブジェクトは、プラットフォームサービスの制限に従って、レプリケーションのキューに入れます ("プラットフォームサービスの利用に関する推奨事項")。
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、オブジェクトが他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、取り込み時間と独立した S3 インフラストラクチャの動作に応じて、場所によって異なります。
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、どちらかのグリッド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 の送信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。
オブジェクトが削除されるとどうなりますか？	- バージョン ID を含む削除要求は、宛先グリッドに複製されることはありません。 - バージョン ID が含まれてい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。これは、オプションで宛先グリッドに複製できます。 - クロスグリッドレプリケーションが一方方向のみに設定されている場合、ソースに影響を与えずに宛先バケット内のオブジェクトを削除できます。	結果は、ソースバケットと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 (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、削除リクエストによって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、削除リクエストによってソースに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、削除リクエストによってソースからはオブジェクトが削除されますが、宛先からは削除されません。 同様に、ソースに影響を与えずに宛先バケット内のオブジェクトを削除できます。

グリッドフェデレーション接続を作成する

テナントの詳細を複製し、オブジェクト データを複製する場合は、2 つのStorageGRID システム間にグリッド フェデレーション接続を作成できます。

図に示すように、グリッド フェデレーション接続を作成するには、両方のグリッドでの手順が含まれます。1 つのグリッドに接続を追加し、他のグリッドで接続を完了します。どちらのグリッドからでも開始できます。



開始する前に

- あなたは、["考慮事項と要件"](#)グリッド フェデレーション接続を構成します。
- 各グリッドに IP アドレスまたは VIP アドレスではなく完全修飾ドメイン名 (FQDN) を使用する予定の場合は、使用する名前がわかっており、各グリッドの DNS サーバーに適切なエントリがあることを確認しています。
- 使用しています["サポートされているウェブブラウザ"](#)。
- 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

2 つのStorageGRIDシステムのいずれかでこれらの手順を実行します。

手順

1. どちら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Sign in。
2. 構成 > システム > グリッド フェデレーション を選択します。
3. ***接続を追加***を選択します。
4. 接続の詳細を入力します。

フィールド	説明
接続名	この接続を認識するのに役立つ一意の名前 (例: 「Grid 1-Grid 2」)。

フィールド	説明
このグリッドのFQDNまたはIP	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 は、宛先グリッドが到達可能な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。23000 から 23999 までの未使用のポート番号を入力できます。 この接続の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ていないことを確認する必要があります。
このグリッドの証明書の有効日数	接続内のこのグリッドのセキュリティ証明書を有効にする日数。デフォルト値は 730 日 (2 年) ですが、1 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、グリッドごとに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	サインインしているグリッドのプロビジョニング パスフレーズ。
他のグリッドのFQDNまたはIP	次のいずれかが必要： • 接続するグリッドのFQDN • 他のグリッド上のHAグループのVIPアドレス • 他のグリッド上の管理ノードまたはゲートウェイ ノードの IP アドレス。IP は、ソース グリッドが到達可能な任意のネットワーク上に存在できます。

5. *保存して続行*を選択します。

6. 検証ファイルのダウンロード手順では、*検証ファイルのダウンロード*を選択します。

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

7. ダウンロードしたファイルを見つける(`connection-name.grid-federation`) を作成し、安全な場所に保存します。



このファイルには秘密情報 (*) やその他の機密詳細が含まれるため、安全に保存して送信する必要があります。

8. 閉じる を選択して、グリッド フェデレーション 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*接続待機中*であることを確認します。
10. 提供する `connection-name.grid-federation`他のグリッドのグリッド管理者にファイルを送信します。

完全な接続

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

手順

1. プライマリ管理ノードからグリッド マネージャーにSign in。
2. 構成 > システム > グリッド フェデレーション 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、[検証ファイルのアップロード] を選択します。
4. *確認ファイルのアップロード*を選択します。次に、最初のグリッドからダウンロードしたファイルを参照して選択します。(`connection-name.grid-federation`)。

接続の詳細が表示されます。

5. 必要に応じて、このグリッドのセキュリティ証明書の有効日数を入力します。証明書の有効日数 エントリは、最初のグリッドで入力した値がデフォルトで設定されますが、グリッドごとに異なる有効期限を使用できます。

一般に、接続の両側の証明書には同じ日数を使用します。



接続のいずれかの端の証明書の有効期限が切れると、接続は機能しなくなり、証明書が更新されるまでレプリケーションは保留になります。

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

証明書が生成され、接続がテストされます。接続が有効な場合は、成功メッセージが表示され、新しい接続がグリッド フェデレーション 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。見る["グリッドフェデレーションエラーのトラブルシューティング"](#)。

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

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

終了後の操作

- 検討事項を確認する["許可されたテナントの管理"](#)。
- ["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、接続値を編集したり、接続をテストしたり、接続証明書をローテーション

ンしたり、接続を削除したりできます。

- ["接続を監視する"](#)通常のStorageGRID監視アクティビティの一環として。
- ["接続のトラブルシューティング"](#)アカウントのクローンとグリッド間のレプリケーションに関連するアラートとエラーの解決も含まれます。

グリッドフェデレーション接続を管理する

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

開始する前に

- いずれかのグリッドのグリッドマネージャにサインインするには、["サポートされているウェブブラウザ"](#)。
- あなたは["ルートアクセス権限"](#)サインインしているグリッドの。

グリッドフェデレーション接続を編集する

接続内のいずれかのグリッドのプライマリ管理ノードにサインインすることで、グリッド フェデレーション接続を編集できます。最初のグリッドに変更を加えた後、新しい検証ファイルをダウンロードして、他のグリッドにアップロードする必要があります。



接続の編集時、アカウントのクローンまたはグリッド間レプリケーション要求では、既存の接続設定が引き続き使用されます。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、テストされるまで使用されません。

接続の編集を開始する

手順

1. どちら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Sign in。
2. **NODES** 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ます。



グリッド フェデレーション接続を編集すると、StorageGRID は最初のグリッド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] を選択すると警告メッセージが表示されます。

3. 構成 > システム > グリッド フェデレーション を選択します。
4. グリッド フェデレーション ページまたは特定の接続の詳細ページの 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。見る["グリッドフェデレーション接続を作成する"](#)何を入力するか。

[操作]メニュー

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

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

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

7. *確認ファイルのダウンロード*を選択します。

このファイルを後でダウンロードするには、接続の詳細ページに移動します。

8. ダウンロードしたファイルを見つける(`connection-name.grid-federation`) を作成し、安全な場所に保存します。



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

9. 閉じる を選択して、グリッド フェデレーション 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ます。



接続の編集を開始したときに接続ステータスが 接続済み 以外だった場合、編集保留中 には変更されません。

11. 提供する ``connection-name.grid-federation``他のグリッドのグリッド管理者にファイルを送信します。

接続の編集を完了する

他のグリッドに検証ファイルをアップロードして、接続の編集を完了します。

手順

1. プライマリ管理ノードからグリッド マネージャーにSign in。
2. 構成 > システム > グリッド フェデレーション 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、[検証ファイルのアップロード] を選択します。
4. *確認ファイルのアップロード*を選択します。次に、最初のグリッドからダウンロードしたファイルを参照して選択します。

5. 現在サインインしているグリッドのプロビジョニング パスフレーズを入力します。

6. *保存してテスト*を選択します。

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

7. ウィザードを閉じて、グリッド フェデレーション 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ます。

9. 最初のグリッドのグリッド フェデレーション ページに移動し、ブラウザーを更新します。 *接続ステータス*が*接続済み*になっていることを確認します。

10. 接続が確立されたら、検証ファイルのすべてのコピーを安全に削除します。

グリッドフェデレーション接続をテストする

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Sign in。

2. 構成 > システム > グリッド フェデレーション を選択します。

3. グリッド フェデレーション ページまたは特定の接続の詳細ページの アクション メニュー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. アクション > *テスト*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. *テスト接続*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	接続がエラー状態です。たとえば、証明書の有効期限が切れているか、構成値が有効でなくなっている場合などです。
編集保留中	このグリッド上の接続を編集しましたが、接続では既存の構成がまだ使用されています。編集を完了するには、新しい検証ファイルを他のグリッドにアップロードします。

接続ステータス	説明
接続を待っています	このグリッドでは接続を構成しましたが、他のグリッドでは接続が完了していません。このグリッドから検証ファイルをダウンロードし、他のグリッドにアップロードします。
不明	接続は不明な状態です。ネットワークの問題またはオフライン ノードが原因である可能性があります。

5. 接続ステータスが「エラー」の場合は、問題を解決してください。次に、*接続テスト*をもう一度選択して、問題が修正されたことを確認します。

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では、接続を保護するために、自動的に生成された 4 つの SSL 証明書が使用されます。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」アラートが表示され、証明書をローテーションするように通知されます。



接続のいずれかの端の証明書の有効期限が切れると、接続は機能しなくなり、証明書が更新されるまでレプリケーションは保留になります。

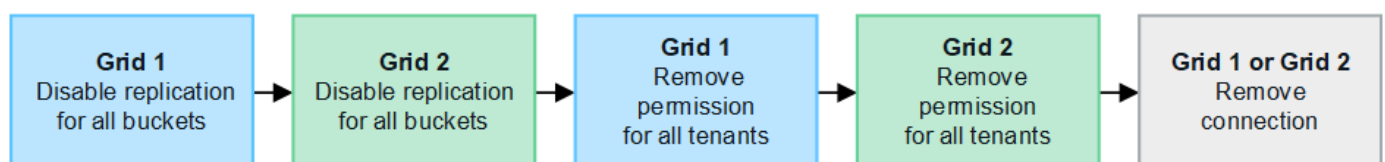
手順

1. どちら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Sign in。
2. 構成 > システム > グリッド フェデレーション を選択します。
3. グリッド フェデレーション ページのいずれかのタブから、接続名を選択して詳細を表示します。
4. *証明書*タブを選択します。
5. *証明書のローテーション*を選択します。
6. 新しい証明書の有効期間を日数指定します。
7. サインインしているグリッドのプロビジョニング パスフレーズを入力します。
8. *証明書のローテーション*を選択します。
9. 必要に応じて、接続内の他のグリッドでこれらの手順を繰り返します。

一般に、接続の両側の証明書には同じ日数を使用します。

グリッドフェデレーション接続を削除する

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



接続を削除する前に、次の点に注意してください。

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

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開始しても、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ます。
2. 構成 > システム > グリッド フェデレーション を選択します。
3. 接続名を選択すると、その詳細が表示されます。
4. *許可されたテナント*タブで、接続がいずれかの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. テナントがリストされている場合は、すべてのテナントに指示してください。"[クロスグリッドレプリケーションを無効にする](#)"接続内の両方のグリッド上のすべてのバケットに対して。



いずれかのテナント バケットでクロス グリッド レプリケーションが有効になっている場合は、グリッド フェデレーション接続の使用 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のグリッド間レプリケーションを無効にする必要があります。

各テナントの権限を削除する

すべてのテナント バケットに対してグリッド間レプリケーションが無効になった後、両方のグリッドのすべてのテナントから グリッド フェデレーションの使用権限 を削除します。

手順

1. 構成 > システム > グリッド フェデレーション を選択します。
2. 接続名を選択すると、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の使用*権限を削除します。見る"[許可されたテナントを管理する](#)"。
4. 他のグリッド上の許可されたテナントに対しても、これらの手順を繰り返します。

接続を削除

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] を選択します。
2. 確認メッセージを確認し、[削除] を選択します。
 - 接続を削除できる場合は、成功メッセージが表示されます。グリッド フェデレーション接続は両方のグリッドから削除されました。

。接続を削除できない場合 (たとえば、まだ使用中であるか、接続エラーが発生している) は、エラーメッセージが表示されます。次のいずれかを実行できます。

- ・ エラーを解決します (推奨)。見る["グリッドフェデレーションエラーのトラブルシューティング"](#)。
- ・ 強制的に接続を解除します。次のセクションを参照してください。

グリッドフェデレーション接続を強制的に削除する

必要に応じて、「接続済み」ステータスになっていない接続を強制的に削除できます。

強制削除では、ローカル グリッドからの接続のみが削除されます。接続を完全に削除するには、両方のグリッドで同じ手順を実行します。

手順

1. 確認ダイアログボックスから*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 フェデレーション接続は使用できなくなりました。ただし、テナント バケットではグリッド間レプリケーションがまだ有効になっている可能性があり、一部のオブジェクト コピーが接続内のグリッド間ですでにレプリケートされている可能性があります。

2. 接続内の他のグリッドで、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ます。
3. 構成 > システム > グリッド フェデレーション を選択します。
4. 接続名を選択すると、その詳細が表示されます。
5. *削除*と*はい*を選択します。
6. このグリッドから接続を削除するには、「強制削除」を選択します。

グリッドフェデレーションの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。テナントに接続の使用が許可されている場合、テナントの詳細を編集したり、テナントの接続使用権限を完全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

- ・ いずれかのグリッドのグリッドマネージャにサインインするには、["サポートされているウェブブラウザ"](#)。
- ・ あなたは["ルートアクセス権限"](#)サインインしているグリッドの。
- ・ あなたが持っている["グリッドフェデレーション接続を作成しました"](#)2つのグリッドの間。
- ・ ワークフローを確認しました["アカウントクローン"](#)そして["クロスグリッドレプリケーション"](#)。
- ・ 必要に応じて、接続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 ID フェデレーションがすでに構成されています。見る["アカウントクローンとは"](#)。

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のためにグリッドフェデレーション接続を使用できるようにする場合は、一般的な手順に従ってください。["新しいS3テナ"](#)

ントを作成する"または"テナントアカウントを編集する"次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。
- 接続のステータスは「接続済み」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の使用」権限が有効になって最初のグリッドに保存されると、同一のテナントが他のグリッドに自動的に複製されます。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。
- 両方のグリッドのテナントには、同じ 20 桁のアカウント ID、名前、説明、クォータ、および権限が与えられます。オプションで、説明 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、グリッド 1 で作成されたテナントのこの説明は、グリッド 2 に複製されたテナントにも表示されます:「このテナントはグリッド 1 で作成されました。」
- セキュリティ上の理由から、ローカル 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は["ローカルルートユーザーのパスワードを変更する"](#)。

- 新しいテナントまたは編集されたテナントが両方のグリッドで使用可能になると、テナント ユーザーは次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 ユーザーを作成します。これらはテナントの宛先グリッドに自動的に複製されます。見る["テナントグループとユーザーの複製"](#)。
 - オプションでテナントの宛先グリッドに複製できる新しい S3 アクセス キーを作成します。見る["API を使用して S3 アクセスキーを複製する"](#)。
 - 接続の両方のグリッドに同一のバケットを作成し、一方向または双方向のグリッド間レプリケーションを有効にします。見る["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表示できます。

手順

1. *TENANTS*を選択します。
2. 「テナント」 ページでテナント名を選択し、テナントの詳細ページを表示します。

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に作成された場合)、テナントが別のグリッドに複製されたことを通知するバナーが表示されます。このテナントを編集または削除すると、変更内容は他のグリッドに同期されません。

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](#)  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. オプションで*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を使用する*権限を持つテナントを編集する必要がある場合は、以下の一般的な手順に従ってください。"[テナントアカウントの編集](#)"次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の使用 権限がある場合は、接続内のどちらのグリッドからでもテナントの詳細を編集できます。ただし、変更内容は他のグリッドにコピーされません。グリッド間でテナントの詳細を同期させたい場合は、両方のグリッドで同じ編集を行う必要があります。
- テナントを編集しているときに、グリッド フェデレーション接続の使用 権限をクリアすることはできません。
- テナントを編集しているときに、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

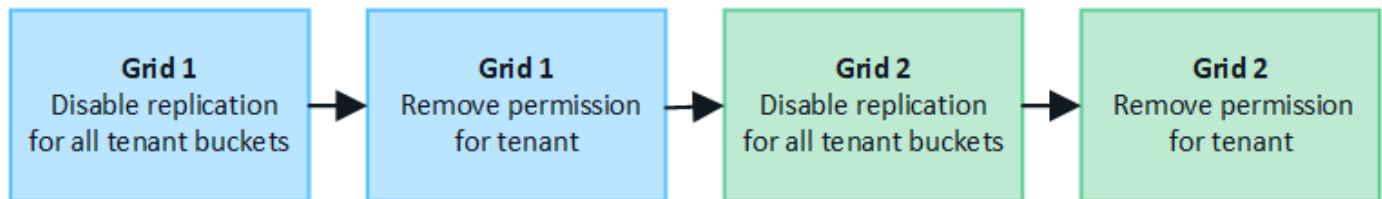
*グリッドフェデレーション接続を使用する*権限を持つテナントを削除する必要がある場合は、以下の一般的な手順に従ってください。"[テナントアカウントの削除](#)"次の点に注意してください。

- 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。
- 宛先グリッド上のクローンされたテナントを削除する前に、宛先グリッド上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。
- 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、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。クローンされたテナントを削除するか、独自のグループ、ユーザー、アクセス キー、バケットを管理できるようにすることができます。
- 宛先グリッド上の複製されたテナントを削除する場合、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ると、複製エラーが発生します。

これらのエラーを回避するには、このグリッドからテナントを削除する前に、テナントのグリッド フェデレーション接続を使用する権限を削除します。

グリッドフェデレーション接続の使用権限を削除します

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の使用 権限を削除する必要があります。



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

- テナント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のクロス 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の使用 権限を削除しても、グリッド間で既に複製されているアイテムは削除されません。たとえば、テナントの権限が削除されても、両方のグリッドに存在するテナント ユーザー、グループ、およびオブジェクトはどちらのグリッドからも削除されません。これらの項目を削除する場合は、両方のグリッドから手動で削除する必要があります。
- 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ます。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の使用 権限を再度有効にすると、ローカル グリッドがソース グリッドになり、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トリガーされます。リモート グリッドにテナント アカウントがすでに存在する場合、複製を行うと競合エラーが発生します。

開始する前に

- 使用しています["サポートされているウェブブラウザ"](#)。
- あなたは["ルートアクセス権限"](#)両方のグリッドに対して。

テナントバケットのレプリケーションを無効にする

最初のステップとして、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開始しても、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ます。
2. 構成 > システム > グリッド フェデレーション を選択します。
3. 接続名を選択すると、その詳細が表示されます。
4. *許可されたテナント*タブで、テナントが接続を使用しているかどうかを確認します。
5. 入居者がリストに載っている場合は、"[クロスグリッドレプリケーションを無効にする](#)"接続内の両方のグリッド上のすべてのバケットに対して。



いずれかのテナント バケットでクロス グリッド レプリケーションが有効になっている場合は、グリッド フェデレーション接続の使用 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のグリッド間レプリケーションを無効にする必要があります。

テナントの権限を削除する

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、グリッド フェデレーション接続を使用するテナントの権限を削除できます。

手順

1. プライマリ管理ノードからグリッド マネージャーにSign in。
2. グリッド フェデレーション ページまたはテナント ページから権限を削除します。

グリッドフェデレーションページ

- a. 構成 > システム > グリッド フェデレーション を選択します。
- b. 接続名を選択すると、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、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。

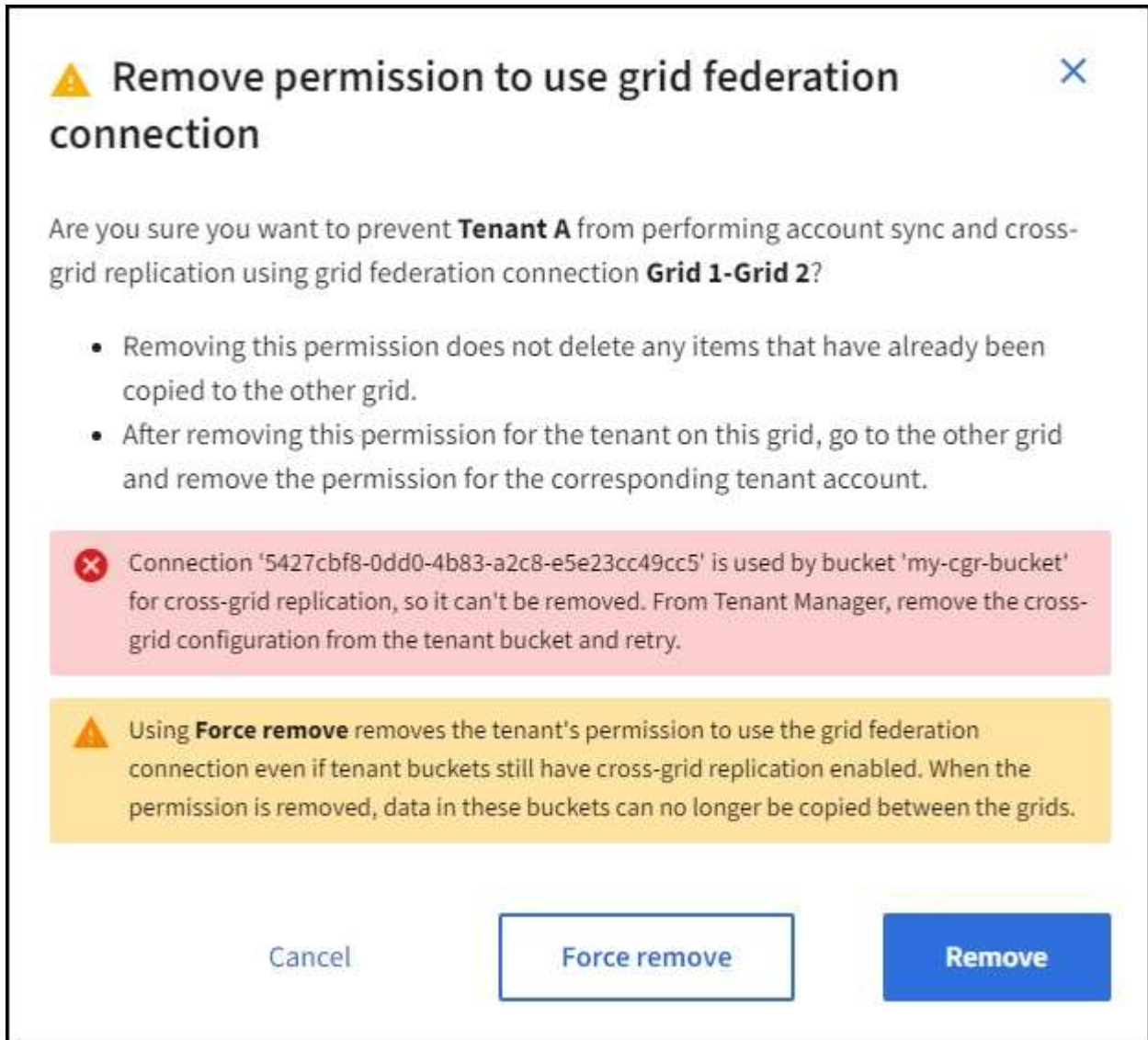
テナントページ

- a. *TENANTS*を選択します。
- b. テナントの名前を選択すると、詳細ページが表示されます。
- c. グリッド フェデレーション タブで、接続のラジオ ボタンを選択します。
- d. *権限を削除*を選択します。

3. 確認ダイアログボックスの警告を確認し、[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 フェデレーション接続を使用できなくなりました。

- 1 つ以上のテナント バケットでグリッド間レプリケーションがまだ有効になっている場合は、エラーが表示されます。



次のいずれかを実行できます。

- (推奨。)テナント マネージャーにSign in、各テナントのバケットのレプリケーションを無効にします。見る["クロスグリッドレプリケーションを管理する"](#)。次に、手順を繰り返して、「グリッド接続を使用する」権限を削除します。
 - 権限を強制的に削除します。次のセクションを参照してください。
4. 他のグリッドに移動し、これらの手順を繰り返して、他のグリッド上の同じテナントの権限を削除します。

権限を強制的に削除する

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、グリッド フェデレーション接続を使用するテナントの権限を強制的に削除できます。

強制的に入居者の許可を取り消す前に、以下の一般的な考慮事項に注意してください。 [権限を削除する](#) さらに、次の点も考慮する必要があります。

- グリッド フェデレーション接続の使用 権限を強制的に削除すると、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しないようにするには、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の使用 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Sign in。
2. 構成 > システム > グリッド フェデレーション を選択します。
3. 接続名を選択すると、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、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の警告を確認し、「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 フェデレーション接続を使用できなくなりました。

7. 必要に応じて、他のグリッドに移動してこれらの手順を繰り返し、他のグリッド上の同じテナント アカウ
ントの権限を強制的に削除します。たとえば、処理中のオブジェクトが宛先バケットに到達しないように
するには、他のグリッドでこれらの手順を繰り返す必要があります。

グリッドフェデレーションエラーのトラブルシューティング

グリッド フェデレーション接続、アカウント クローン、およびクロス グリッド レプリ
ケーションに関連するアラートとエラーのトラブルシューティングが必要になる場合が
あります。

グリッドフェデレーション接続のアラートとエラー

グリッド フェデレーション接続でアラートが表示されたり、エラーが発生したりする可能性があります。

接続の問題を解決するために変更を加えた後、接続をテストして、接続ステータスが「接続済み」に戻ることを
確認します。手順については、「[グリッドフェデレーション接続を管理する](#)」。

グリッドフェデレーション接続失敗アラート

問題

グリッド フェデレーション接続失敗 アラートがトリガーされました。

詳細

このアラートは、グリッド間のグリッド フェデレーション接続が機能していないことを示します。

推奨する対処方法

1. 両方のグリッドの「グリッド フェデレーション」ページの設定を確認します。すべての値が正しいことを
確認します。見る「[グリッドフェデレーション接続を管理する](#)」。
2. 接続に使用された証明書を確認します。期限切れのグリッド フェデレーション証明書に関するアラートが

ないこと、および各証明書の詳細が有効であることを確認します。接続証明書のローテーション手順については、"[グリッドフェデレーション接続を管理する](#)"。

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使用可能であることを確認します。これらのノードに影響を与えている可能性のあるアラートを解決して、再試行してください。
4. ローカル グリッドまたはリモート 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使用可能であることを確認します。見る"[グリッドフェデレーションとは何ですか?](#)"ネットワーク、IP アドレス、および DNS の要件。

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

問題

グリッド フェデレーション証明書の有効期限 アラートがトリガーされました。

詳細

このアラートは、1 つ以上のグリッド フェデレーション証明書の有効期限が近づいていることを示します。

推奨する対処方法

接続証明書のローテーション手順については、"[グリッドフェデレーション接続を管理する](#)"。

グリッド フェデレーション接続の編集中にエラーが発生しました

問題

グリッド フェデレーション接続を編集するときに、[保存してテスト] を選択すると、次の警告メッセージが表示されます: 「1 つ以上のノードに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と、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。たとえば、管理ノードがオフラインであるなどの理由で、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、**NODES** を選択します。
2. そのグリッドのすべての管理ノードがオンラインであることを確認します。
3. オフラインになっているノードがある場合は、オンラインに戻して接続を再度編集してみてください。

アカウント複製エラー

複製されたテナント アカウントにサインインできない

問題

複製されたテナント アカウントにサインインすることはできません。テナント マネージャーのサインイン ページのエラー メッセージは、「このアカウントの資格情報が無効です。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複製されるときに、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複製されません。同様に、テナントがソース グリッドにローカル ユーザーを作成すると、ローカル ユーザーのパスワードは宛先グリッドに複製されません。

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["ローカルルートユーザーのパスワードを変更する"](#)宛先グリッド上。

クローン作成されたローカル ユーザーがテナントの宛先グリッドにサインインする前に、クローン作成されたテナントのルート ユーザーが宛先グリッド上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、["ローカルユーザーの管理"](#)テナント マネージャーの使用手順について説明します。

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の使用 権限を使用して新しいテナントを作成した後、「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れると発生する可能性があり、その結果、正常でない接続が 接続済み としてリストされる可能性があります。

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ます。見る[グリッドフェデレーション接続のアラートとエラー](#)。
2. 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ください。["グリッドフェデレーション接続を管理する"](#)問題が修正されたことを確認します。
3. テナントのソース グリッドから、**TENANTS** を選択します。
4. 複製に失敗したテナント アカウントを見つけます。
5. テナント名を選択すると詳細ページが表示されます。
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 アカウントは他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に表示された最後のエラー

問題

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

Grid 1 - Grid 2

Local hostname (this grid): 10.96.130.64
Port: 23000
Remote hostname (other grid): 10.96.130.76
Connection status: Connected

[Edit](#) [Download file](#) [Test connection](#) [Remove](#)

Permitted tenants

Certificates

[Remove permission](#) [Clear error](#)

Displaying one result

Tenant name	Last error
Tenant A	2022-12-22 16:19:20 MST 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 and S3 Object Lock disabled. (logID 13916508109026943924) Check for errors

詳細

各グリッド フェデレーション接続の 最後のエラー 列には、テナントのデータが他のグリッドに複製されているときに発生した最新のエラー (ある場合) が表示されます。この列には、最後に発生したグリッド間レプリケーション エラーのみが表示されます。以前に発生した可能性のあるエラーは表示されません。この列のエラーは、次のいずれかの理由で発生する可能性があります。

- ・ ソース オブジェクト 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。
- ・ 宛先バケットが別のアカウントによって再作成されました。
- ・ 宛先バケットのバージョン管理が停止されています。
- ・ 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。

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る場合は、次の手順に従ってください。

1. メッセージテキストを確認します。
2. 推奨されるアクションを実行します。たとえば、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中断されていた場合は、そのバケットのバージョン管理を再度有効にします。
3. テーブルから接続またはテナント アカウントを選択します。
4. *エラーをクリア*を選択します。
5. メッセージをクリアしてシステムのステータスを更新するには、[はい] を選択します。
6. 5 ～ 6 分待ってから、新しいオブジェクトをバケットに取り込みます。エラーメッセージが再度表示されないことを確認します。



エラー メッセージを確実にクリアするには、新しいオブジェクトを取り込む前に、メッセージ内のタイムスタンプから少なくとも 5 分間待機します。



エラーをクリアした後、同じくエラーが発生している別のバケットにオブジェクトが取り込まれると、新しい 最後のエラー が表示されることがあります。

7. バケットエラーにより複製に失敗したオブジェクトがある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識別して再試行する"](#)。

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、解決にユーザーの介入が必要な理由により、2 つのグリッド上のバケット間でテナント オブジェクトを複製できないことを示します。このアラートは通常、ソース バケットまたは宛先バケットのいずれかの変更によって発生します。

推奨する対処方法

1. アラートがトリガーされたグリッドに Sign in。
2. **CONFIGURATION > System > Grid federation** に移動し、アラートにリストされている接続名を見つけます。
3. [許可されたテナント] タブで、[最後のエラー] 列を確認し、エラーのあるテナント アカウントを特定します。
4. 障害の詳細については、["グリッドフェデレーション接続を監視する"](#)クロスグリッドレプリケーションメトリックを確認します。
5. 影響を受けるテナント アカウントごとに:
 - a. の指示を参照してください["テナントのアクティビティを監視する"](#)テナントが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ます。
 - 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ます。
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ます。
7. クロスグリッド レプリケーションが有効になっているバケットごとに、次の点を確認します。

- 他のグリッドに同じテナントに対応するバケットがあります (正確な名前を使用する必要があります)。
 - 両方のバケットでオブジェクトのバージョン管理が有効になっています (どちらのグリッドでもバージョン管理を一時停止することはできません)。
 - 両方のバケットで S3 オブジェクト ロックが無効になっています。
 - どちらのバケットも「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](#)"クロスグリッドレプリケーションメトリックを確認するには、次の手順を実行します。
- a. グリッド フェデレーション ページに戻ります。
 - 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. メッセージをクリアしてシステムのステータスを更新するには、[はい] を選択します。
 - d. 5 ～ 6 分待ってから、新しいオブジェクトをバケットに取り込みます。エラーメッセージが再度表示されないことを確認します。



エラー メッセージを確実にクリアするには、新しいオブジェクトを取り込む前に、メッセージ内のタイムスタンプから少なくとも 5 分間待機します。



アラートが解決されてから消えるまでに最大 1 日かかる場合があります。

- a. へ移動"[失敗したレプリケーション操作を識別して再試行する](#)"他のグリッドに複製できなかったオブジェクトを識別したりマーカーを削除したりして、必要に応じて複製を再試行します。

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、グリッド間レプリケーション要求が保留中であることを示します。たとえば、ネットワーク エラーが発生している可能性があります。

推奨する対処方法

1. アラートを監視して、問題が自動的に解決されるかどうかを確認します。
2. 問題が解決しない場合は、どちらかのグリッドに同じ接続に対する グリッド フェデレーション接続エラー アラートがあるかどうか、またはノードに対する ノードと通信できません アラートがあるかどうかを確認します。これらのアラートを解決すると、このアラートも解決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](#)"クロスグリッドレプリケーションメトリックを確認します。
4. アラートを解決できない場合は、テクニカル サポートにお問い合わせください。

問題が解決されると、クロスグリッド レプリケーションは通常どおり続行されます。

失敗したレプリケーション操作を識別して再試行する

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、他のグリッドにレプリケートできなかったオブジェクトまたは削除マーカがあるかどうかを確認する必要があります。その後、これらのオブジェクトを再取り込みするか、グリッド管理 API を使用してレプリケーションを再試行できます。

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、解決にユーザーの介入が必要な理由により、2つのグリッド上のバケット間でテナント オブジェクトをレプリケートできないことを示します。このアラートは通常、ソース バケットまたは宛先バケットのいずれかの変更によって発生します。詳細については、"[グリッドフェデレーションエラーのトラブルシューティング](#)"。

複製に失敗したオブジェクトがあるかどうかを確認する

他のグリッドに複製されていないオブジェクトや削除マーカがあるかどうかを確認するには、監査ログで次の項目を検索します。["CGRR \(クロスグリッドレプリケーション要求\)"](#)メッセージ。このメッセージは、StorageGRID がオブジェクト、マルチパート オブジェクト、または削除マーカ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。

使用することができます["監査説明ツール"](#)結果をより読みやすい形式に変換します。

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。
- プライマリ管理ノードの IP アドレスがわかっています。

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. 記載されているパスワードを入力してください `Passwords.txt` ファイル。
 - c. ルートに切り替えるには、次のコマンドを入力します。 `su -`
 - d. 記載されているパスワードを入力してください `Passwords.txt` ファイル。

ルートとしてログインすると、プロンプトは `$` に `#`。

2. `audit.log` で CGRR メッセージを検索し、`audit-explain` ツールを使用して結果をフォーマットします。

たとえば、このコマンドは過去 30 分間のすべての CGRR メッセージを `grep` し、`audit-explain` ツールを使用します。

```
# awk -vdate=$(date -d "30 minutes ago" '+%Y-%m-%dT%H:%M:%S') '$1$2 >= date { print }' audit.log | grep CGRR | audit-explain
```

コマンドの結果は次の例のようになり、6つの CGRR メッセージのエントリが含まれます。この例では、オブジェクトをレプリケートできなかったため、すべてのクロスグリッド レプリケーション要求で一般エラーが返されました。最初の3つのエラーは「オブジェクトの複製」操作に関するもので、最後の3つのエラーは「削除マーカの複製」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

```

各エントリには次の情報が含まれます。

フィールド	説明
CGRR クロスグリッドレプリケーション要求	リクエストの名前
テナント	テナントのアカウントID
繋がり	グリッドフェデレーション接続のID
operation	試行されたレプリケーション操作の種類: • オブジェクトを複製する • 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。クロスグリッド レプリケーションが失敗した場合、エラーは「一般エラー」になります。

失敗したレプリケーションを再試行する

宛先バケットに複製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。
- 説明に従って、Grid Management プライベート API を使用します。

手順

1. グリッド マネージャーの上部から、ヘルプ アイコンを選択し、**API ドキュメント** を選択します。
2. *プライベート API ドキュメントに移動*を選択します。



「プライベート」とマークされているStorageGRID API エンドポイントは、予告なく変更されることがあります。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. *試してみる*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 に置き換えます。

文字列を囲む二重引用符を必ず保持してください。

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ます。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中としてマークされていることを示します。



保留中は、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を監視して、完了したことを確認する必要があります。



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

再試行操作は、次の 2 つの方法のいずれかで監視できます。

- S3を使用する"**HeadObject**"または"**GetObject**"リクエスト。応答にはStorageGRID固有の`x-ntap-sg-cgr-replication-status`レスポンス ヘッダーは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: レプリケーションは成功しました。 • 保留中: オブジェクトはまだ複製されていません。 • 失敗: レプリケーションは永続的な障害により失敗しました。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	REPLICA : オブジェクトはソース グリッドから複製されました。

- 説明に従って、Grid Management プライベート API を使用します。

手順

1. プライベート API ドキュメントの **cross-grid-replication-advanced** セクションで、次のエンドポイントを選択します。

```
GET /private/cross-grid-replication-object-status/{id}
```

2. *試してみる*を選択します。
3. パラメータセクションで、`cross-grid-replication-retry-failed`リクエスト。
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ます。
6. レプリケーション ステータスを確認します。次のいずれかになります。
 - 保留中: オブジェクトはまだ複製されていません。
 - 完了: レプリケーションは成功しました。
 - 失敗: レプリケーションは永続的な障害により失敗しました。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

セキュリティを管理する

Grid Manager 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、データを暗号化するためのいくつかのオプションを提供します。あなたがすべき"[利用可能な暗号化方式を確認する](#)"どれがデータ保護要件を満たしているかを判断します。

証明書の管理

あなたはできる"[サーバー証明書の設定と管理](#)"HTTP 接続に使用され、またはサーバーに対してクライアントまたはユーザーの ID を認証するために使用されるクライアント証明書です。

キー管理サーバーを構成する

使用して"[鍵管理サーバー](#)"アプライアンスがデータセンターから削除された場合でも、StorageGRIDデータを保護できます。アプライアンス ボリュームが暗号化された後は、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、インストール中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、"[ストレージプロキシサーバー](#)"ストレージノードと外部 S3 エンドポイント間。HTTPSまたはHTTPを使用してAutoSupportパッケージを送信する場合は、"[管理プロキシサーバー](#)"管理ノードとテクニカル サポート間。

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、特定のポートを開いたり閉じたりすることで、StorageGRID管理ノードへのアクセスを制御できます。"[外部ファイアウォール](#)"。各ノードのネットワークアクセスを制御するには、"[内部ファイアウォール](#)"。展開に必要なポートを除くすべてのポートへのアクセスを禁止できます。

StorageGRIDの暗号化方式を確認する

StorageGRID は、データを暗号化するためのいくつかのオプションを提供します。利用可能な方法を確認して、どの方法が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で使える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	適用対象
グリッド マネージャーのキー管理サーバー (KMS)	あなた" キー管理サーバーを構成する "StorageGRIDサイトと " アプライアンスのノード暗号化を有効にする "。次に、アプライアンス ノードは 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、各ボリューム上のデータ暗号化キー (DEK) を暗号化および復号化します。	インストール中に ノード暗号化 が有効になっているアプライアンス ノード。アプライアンス上のすべてのデータは、物理的な損失やデータセンターからの削除から保護されます。 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ます。

暗号化オプション	仕組み	適用対象
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含まれている場合は、インストール中にドライブのパスフレーズを設定できます。ドライブ 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、システムから削除されたドライブから有効なデータを回復することは不可能になります。インストールを開始する前に、ハードウェアの構成 > ドライブ暗号化 に移動して、ノード内のすべてのStorageGRID管理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ます。	自己暗号化ドライブを搭載したアプライアンス。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削除から保護されます。 ドライブ暗号化は、SANtricity管理ドライブには適用されません。自己暗号化ドライブとSANtricityコントローラを備えたストレージ アプライアンスがある場合は、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 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"セキュリティ キーを作成および管理します。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備えたストレージアプライアンス。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削除から保護されます。一部のストレージ アプライアンスまたはサービス アプライアンスでは使用できません。
保存されたオブジェクトの暗号化	有効にすると、"保存されたオブジェクトの暗号化"グリッド マネージャーのオプション。有効にすると、バケット レベルまたはオブジェクト レベルで暗号化されていない新しいオブジェクトは、取り込み時に暗号化されます。	新しく取り込まれた S3 オブジェクト データ。 既存の保存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ません。
S3バケットの暗号化	バケットの暗号化を有効にするには、PutBucketEncryption リクエストを発行します。オブジェクト レベルで暗号化されていない新しいオブジェクトは、取り込み中に暗号化されます。	新しく取り込まれた S3 オブジェクト データのみ。 バケットに暗号化を指定する必要があります。既存のバケット オブジェクトは暗号化されません。オブジェクトのメタデータやその他の機密データは暗号化されません。 "バケットの操作"

暗号化オプション	仕組み	適用対象
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。	新しく取り込まれた 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ません。 StorageGRID がキーを管理します。 "サーバー側の暗号化を使用する"
顧客提供キーを使用した S3 オブジェクトのサーバー側暗号化 (SSE-C)	オブジェクトを保存するための 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	新しく取り込まれた 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ません。 キーはStorageGRIDの外部で管理されます。 "サーバー側の暗号化を使用する"
外部ボリュームまたはデータストアの暗号化	導入プラットフォームでサポートされている場合は、StorageGRID 外部の暗号化方法を使用してボリューム全体またはデータストアを暗号化します。	すべてのボリュームまたはデータストアが暗号化されていると仮定した場合、すべてのオブジェクト データ、メタデータ、およびシステム構成データ。 外部暗号化方式により、暗号化アルゴリズムとキーをより厳密に制御できます。記載されている他の方法と組み合わせることができます。

暗号化オプション	仕組み	適用対象
StorageGRID外部のオブジェクト暗号化	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するには、StorageGRID外部の暗号化方式を使用します。	オブジェクト データとメタデータのみ (システム構成データは暗号化されません)。 外部暗号化方式により、暗号化アルゴリズムとキーをより厳密に制御できます。記載されている他の方法と組み合わせることができます。 "Amazon Simple Storage Service - 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、一度に複数の暗号化方法を使用できます。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、同じアプライアンス内の自己暗号化ドライブ上のデータを「二重に暗号化」することもできます。
- KMS を使用してアプライアンス ノード上のデータを保護し、保存されたオブジェクトの暗号化オプションを使用して、取り込まれたすべてのオブジェクトを暗号化することもできます。

オブジェクトのごく一部にのみ暗号化が必要な場合は、代わりにバケット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。複数レベルの暗号化を有効にすると、パフォーマンスコストが追加されます。

証明書の管理

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作成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し、クライアントに対してサーバーの ID を認証し、データの安全な通信パスを提供するために使用されます。サーバーとクライアントはそれぞれ証明書のコピーを持ちます。
- クライアント証明書 は、クライアントまたはユーザーの ID をサーバーに対して認証し、パスワードのみを使用する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、サーバーは公開キーを含むサーバー証明書で応答します。クライアントは、サーバーの署名を証明書のコピーの署名と比較することによって、この証明書を検証します。署名が一致する場合、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 バランサ 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。

デフォルトのグリッドCA証明書

StorageGRID には、システムのインストール中に内部グリッド CA 証明書を生成する組み込みの証明機関 (CA) が含まれています。デフォルトでは、グリッド CA 証明書が、内部StorageGRIDトラフィックのセキュリティ保護に使用されます。外部証明機関 (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。グリッド CA 証明書は非実稼働環境でも使用できますが、実稼働環境では、外部証明機関によって署名されたカスタム証明書を使用するのがベスト プラクティスです。証明書のない安全でない接続もサポートされていますが、推奨されません。

- カスタム CA 証明書では内部証明書は削除されませんが、カスタム証明書はサーバー接続の検証用に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](#)"。
- StorageGRID は、CA からの証明書を 1 つのファイルにバンドルすること (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同じオペレーティング システム CA 証明書も含まれています。運用環境では、オペレーティング システムの CA 証明書の代わりに、外部証明機関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ます。システムを構成する前に、特定のStorageGRID構成に必要なすべての証明書を準備しておく必要があります。

セキュリティ証明書にアクセスする

すべてのStorageGRID証明書に関する情報と、各証明書の構成ワークフローへのリンクに 1 か所でアクセスできます。

手順

1. Grid Manager から、構成 > セキュリティ > 証明書 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. 各証明書カテゴリに関する情報や証明書設定にアクセスするには、「証明書」ページのタブを選択します。タブにアクセスするには、["適切な許可"](#)。
- グローバル: Web ブラウザおよび外部 API クライアントからのStorageGRIDアクセスを保護します。
 - グリッド **CA**: 内部StorageGRIDトラフィックを保護します。
 - クライアント: 外部クライアントとStorageGRID Prometheus データベース間の接続を保護します。
 - ロード バランサ エンドポイント: S3 クライアントとStorageGRIDロード バランサ間の接続を保護します。
 - テナント: 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: 特定の証明書を必要とするStorageGRID接続を保護します。

各タブについては、追加の証明書の詳細へのリンクとともに以下で説明します。

グローバル

グローバル証明書は、Web ブラウザおよび外部 S3 API クライアントからのStorageGRIDアクセスを保護します。インストール中に、StorageGRID証明機関によって最初に 2 つのグローバル証明書が生成されます。実稼働環境でのベストプラクティスは、外部証明機関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。

- [\[管理インターフェース証明書\]](#): StorageGRID管理インターフェイスへのクライアント Web ブラウザ接続を保護します。
- [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、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次のとおりです。

- 名前: 証明書を管理するためのリンクを含む証明書の名前。
- 説明
- 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強化するには、常にカスタム証明書を使用する必要があります。
- 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。

- グリッドのセキュリティを強化するために、デフォルトの証明書を外部証明機関によって署名されたカスタム証明書に置き換えます。
 - ["デフォルトのStorageGRID生成管理インターフェース証明書を置き換えます"](#)Grid Manager および Tenant Manager 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 ノードとロード バランサ エンドポイント (オプション) の接続に使用されます。
- ["デフォルトの管理インターフェー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ース証明書を生成する"](#)。
- コピーまたはダウンロード["管理インターフェース証明書"](#)または["S3 API証明書"](#)。

グリッドCA

その[グリッド CA 証明書](#)は、StorageGRID のインストール中にStorageGRID証明機関によって生成され、すべての内部StorageGRIDトラフィックを保護します。

証明書情報には、証明書の有効期限と証明書の内容が含まれます。

あなたはできる["グリッドCA証明書をコピーまたはダウンロードする"](#)ただし、変更することはできません。

クライアント

[クライアント証明書](#)外部証明機関によって生成された証明書は、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、構成されたクライアント証明書ごとに行があり、証明書の有効期限とともに、証明書が Prometheus データベース アクセスに使用できるかが示されます。

次の操作を実行できます。

- ["新しいクライアント証明書をアップロードまたは生成します。"](#)
- 証明書名を選択すると、証明書の詳細が表示され、次の操作を実行できます。
 - ["クライアント証明書の名前を変更します。"](#)
 - ["Prometheus のアクセス権限を設定します。"](#)
 - ["クライアント証明書をアップロードして置き換えます。"](#)
 - ["クライアント証明書をコピーまたはダウンロードします。"](#)
 - ["クライアント証明書を削除します。"](#)
- アクション*を選択してすぐに["編集"](#)、["添付する"](#)、または["削除"](#)クライアント証明書。*アクション > 削除 を使用して、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

[ロードバランサのエンドポイント証明書](#)ゲートウェイ ノードおよび管理ノード上の S3 クライアントと StorageGRID ロード バランサ 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、構成されたロード バランサー エンドポイントごとに 1 行あり、エンドポイントにグローバル 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 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のエンドポイント証明書を生成する代わりに。

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](#)StorageGRIDとの接続を保護します。

テナント テーブルにはテナントごとに 1 行あり、各テナントに独自の 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があ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テナント マネージャーにサインインします"](#)
- ["テナントIDフェデレーションの詳細を表示するには、テナント名を選択してください"](#)
- ["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。"](#)

- ["エンドポイントの作成時にプラットフォーム サービス エンドポイント証明書を指定します"](#)

その他

StorageGRID 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別にリストされています。その他のセキュリティ証明書には次のものがあります:

- [クラウド ストレージ プールの証明書](#)
- [電子メールアラート通知証明書](#)
- [外部 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](#)
- [アイデンティティフェデレーション証明書](#)
- [キー管理サーバー \(KMS\) 証明書](#)
- [シングルサインオン証明書](#)

情報は、関数が使用する証明書の種類と、該当する場合はサーバーおよびクライアント証明書の有効期限を示します。関数名を選択するとブラウザタブが開き、証明書の詳細を表示および編集できます。



他の証明書の情報を閲覧したりアクセスしたりするには、["適切な許可"](#)。

次の操作を実行できます。

- ["S3、C2S S3、またはAzureのクラウドストレージプール証明書を指定します"](#)
- ["アラートメール通知用の証明書を指定する"](#)
- ["外部Syslogサーバー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のローテーション"](#)
- ["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 \(KMS\) のサーバー証明書と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

各タイプのセキュリティ証明書については、実装手順へのリンクとともに以下で説明します。

管理インターフェース証明書

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 Web 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でGrid Manager および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 接続も認証します。 インストール中に作成された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。	構成 > セキュリティ > *証明書*で、*グローバル*タブを選択し、*管理インターフェイス証明書*を選択します。	" 管理インターフェイス証明書を構成する "

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 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)。	構成 > セキュリティ > 証明書、*グローバル*タブを選択し、*S3 API証明書*を選択します。	" S3 API証明書を設定する "

グリッド CA 証明書

参照[デフォルトのグリッドCA証明書の説明](#)。

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 アクセスを認証できるようになります。 - 承認された外部クライアントがStorageGRID Prometheus データベースにアクセスできるようにします。 - 外部ツールを使用してStorageGRIDを安全に監視できます。	構成 > セキュリティ > 証明書 を選択し、クライアント タブを選択します。	"クライアント証明書を構成する"

ロードバランサの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	ゲートウェイ ノードおよび管理ノード上の S3 クライアントとStorageGRIDロード バランサ サービス間の接続を認証します。ロード バランサー エンドポイントを構成するときに、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ときに、ロード バランサ証明書を使用します。 グローバルのカスタムバージョンを使用することもできますS3 API証明書ロード バランサ サービスへの接続を認証するための証明書。グローバル証明書を使用してロード バランサー接続を認証する場合は、ロード バランサーのエンドポイントごとに個別の証明書をアップロードまたは生成する必要はありません。 注: ロード バランサの認証に使用される証明書は、通常のStorageGRID操作中に最もよく使用される証明書です。	構成 > ネットワーク > ロードバランサエンドポイント	• "ロードバランサのエンドポイントを構成する" • "FabricPoolのロードバランサエンドポイントを作成する"

クラウド ストレージ プールの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の場所への接続を認証します。クラウド プロバイダー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"

電子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 電子メール 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、電子メール サーバーの CA 証明書を指定する必要があります。 • SMTP 電子メール 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ます。	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 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にイベントを記録する外部 syslog サーバー間の TLS または RELP/TLS 接続を認証します。 注: 外部 syslog サーバへの TCP、RELP/TCP、および UDP 接続には、外部 syslog サーバ証明書は必要ありません。	構成 > 監視 > 監査および Syslog サーバー	"外部のSyslogサーバーを使用する"

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間で送信される情報を認証および暗号化します。	構成 > システム > グリッドフェデレーション	"グリッドフェデレーション接続を作成する" "接続証明書をローテーションする"

アイデンティティ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。	構成 > アクセス制御 > アイデンティティ連携	"アイデンティティフェデレーションを使用する"

キー管理サーバー (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、StorageGRID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) 間の接続を認証します。	構成 > 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する"

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 フェデレーション サービス (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) 要求に使用されるStorageGRID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構成する"

証明書の例

例1: ロードバランササービス

この例では、StorageGRID がサーバーとして機能します。

1. ロード バランサのエンドポイントを構成し、StorageGRIDでサーバー証明書をアップロードまたは生成します。
2. ロードバランサーエンドポイントへの S3 クライアント接続を構成し、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 エンドポイントに接続します。
4. StorageGRID は、公開キーを含むサーバー証明書と、秘密キーに基づく署名で応答します。
5. クライアントは、サーバーの署名を証明書のコピーの署名と比較することによって、この証明書を検証します。署名が一致する場合、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 がクライアントとして機能します。

1. 外部のキー管理サーバ ソフトウェアを使用して、StorageGRID をKMS クライアントとして構成し、CA 署名付きサーバ証明書、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キーを取得します。

2. Grid Manager を使用して、KMS サーバーを構成し、サーバー証明書とクライアント証明書およびクライアント秘密キーをアップロードします。
3. StorageGRID ノードは暗号化キーを必要とする場合、証明書のデータと秘密キーに基づく署名を含む要求を 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 サーバーは検証された接続を使用して応答します。

サポートされているサーバー証明書の種類

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、サーバー証明書タイプと一致する必要があります。たとえば、RSA 暗号には RSA 証明書が必要であり、ECDSA 暗号には ECDSA 証明書が必要です。見る["セキュリティ証明書を管理する"](#)。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構成する場合は、["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、以下を参照してください。["S3 クライアントのセキュリティ"](#)。

管理インターフェイス証明書を構成する

デフォルトの管理インターフェイス証明書を単一のカスタム証明書に置き換えて、ユーザーがセキュリティ警告に遭遇することなく Grid Manager および Tenant Manager にアクセスできるようにすることができます。デフォルトの管理インターフェイス証明書に戻したり、新しい証明書を生成したり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 署名付き証明書は、単一の共通カスタム管理インターフェイス証明書と対応する秘密キーに置き換えることができます。

すべての管理ノードに単一のカスタム管理インターフェイス証明書が使用されるため、クライアントが Grid Manager および Tenant Manager に接続するとき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と一致するようにカスタム証明書を定義します。

サーバー上で構成を完了する必要があります。また、使用しているルート証明機関 (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 ブラウザーに Grid CA 証明書をインストールする必要もあります。



失敗したサーバー証明書によって操作が中断されないように、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、**[*CONFIGURATION] > [Security] > [Certificates]** を選択し、**[Global]** 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、次のいずれかが発生すると、ブラウザにバイパス オプションのない証明書エラーが表示されます。

- カスタム管理インターフェース証明書の有効期限が切れます。
- あなた [カスタム管理インターフェース証明書からデフォルトのサーバー証明書に戻す](#)。

カスタム管理インターフェース証明書を追加する

カスタム管理インターフェース証明書を追加するには、独自の証明書を提供するか、グリッド マネージャーを使用して証明書を生成します。

手順

1. 構成 > セキュリティ > *証明書*を選択します。
2. *グローバル*タブで、*管理インターフェース証明書*を選択します。
3. *カスタム証明書を使用する*を選択します。
4. 証明書をアップロードまたは生成します。

証明書をアップロード

必要なサーバー証明書ファイルをアップロードします。

- a. *証明書のアップロード*を選択します。
- b. 必要なサーバ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 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**: 各中間発行証明機関 (CA) からの証明書を含む単一のオプション ファイル。このファイルには、PEM でエンコードされた各 CA 証明書ファイルが、証明書チェーンの順序で連結されて含まれている必要があります。
- c. *証明書の詳細*を展開して、アップロードした各証明書のメタデータを表示します。オプションの CA バンドルをアップロードした場合、各証明書は独自のタブに表示されます。
 - 証明書ファイルを保存するには 証明書のダウンロード を選択するか、証明書バンドルを保存するには **CA** バンドルのダウンロード を選択します。

証明書ファイル名とダウンロード場所を指定します。拡張子を付けてファイルを保存する .pem。

例: storagegrid_certificate.pem

- 証明書の内容をコピーして他の場所に貼り付けるには、「証明書 **PEM** のコピー」または「**CA** バンドル **PEM** のコピー」を選択します。
- 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しい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。



実稼働環境でのベスト プラクティスは、外部証明機関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。

フィールド	説明
IP	証明書に含める 1 つ以上の IP アドレス。
件名（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、生成された証明書では、最初のドメイン名または IP アドレスがサブジェクト共通名 (CN) として使用されます。
有効日数	証明書の有効期限が切れるまでの作成後日数。
キー使用拡張機能を追加する	選択した場合 (デフォルト、推奨)、生成された証明書にキー使用法と拡張キー使用法の拡張機能が追加されます。 これらの拡張機能は、証明書に含まれるキーの目的を定義します。 注意: 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との接続の問題が発生しない限り、このチェックボックスをオンのままにしておきます。

c. *生成*を選択します。

d. 生成された証明書のメタデータを表示するには、「証明書の詳細」を選択します。

- 証明書ファイルを保存するには、[証明書のダウンロード] を選択します。

証明書ファイル名とダウンロード場所を指定します。拡張子を付けてファイルを保存する .pem。

例: storagegrid_certificate.pem

- 証明書の内容をコピーして他の場所に貼り付けるには、「証明書 **PEM** のコピー」を選択します。

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しい接続に使用されます。

5. ページを更新して、Web ブラウザが更新されていることを確認します。



新しい証明書をアップロードまたは生成した後、関連する証明書の有効期限アラートがクリアされるまで最大 1 日かかります。

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な証明書情報が表示されます。+ 必要に応じて証明書 PEM をダウンロードまたはコピーできます。

デフォルトの管理インターフェース証明書を復元する

Grid Manager および Tenant Manager 接続にデフォルトの管理インターフェース証明書を使用するように戻すことができます。

手順

1. 構成 > セキュリティ > *証明書*を選択します。
2. *グローバル*タブで、*管理インターフェース証明書*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ース証明書を復元すると、構成したカスタム サーバー証明書ファイルが削除され、システムから回復できなくなります。以降のすべての新しいクライアント接続には、デフォルトの管理インターフェース証明書が使用されます。

4. ページを更新して、Web ブラウザが更新されていることを確認します。

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ース証明書を生成する

厳密なホスト名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ース証明書を生成できます。

開始する前に

- あなたが持っている"[特定のアクセス権限](#)"。
- あなたは `Passwords.txt` ファイル。

タスク概要

実稼働環境でのベストプラクティスは、外部の証明機関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. 記載されているパスワードを入力してください `Passwords.txt` ファイル。
 - c. ルートに切り替えるには、次のコマンドを入力します。 `su -`
 - d. 記載されているパスワードを入力してください `Passwords.txt` ファイル。

ルートとしてログインすると、プロンプトは `$` に `#`。

3. 新しい自己署名証明書を使用してStorageGRIDを構成します。

```
$ sudo make-certificate --domains wildcard-admin-node-fqdn --type management
```

- のために `--domains`、ワイルドカードを使用して、すべての管理ノードの完全修飾ドメイン名を表します。例えば、`*.ui.storagegrid.example.com` *ワイルドカードを使用して `admin1.ui.storagegrid.example.com` `そして` `admin2.ui.storagegrid.example.com`。
- セット `--type` に `management` Grid Manager および Tenant Manager で使用される管理インターフェース証明書を構成します。

- 。デフォルトでは、生成された証明書の有効期間は 1 年間 (365 日間) で、有効期限が切れる前に再作成する必要があります。使用することができます `--days` デフォルトの有効期間を上書きする引数。



証明書の有効期間は、`make-certificate` 実行されます。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する必要があります。そうでない場合、クライアントは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
```

結果の出力には、管理 API クライアントに必要な公開証明書が含まれます。

4. 証明書を選択してコピーします。

選択範囲に BEGIN タグと END タグを含めます。

5. コマンド シェルからログアウトします。\$ exit
6. 証明書が構成されたことを確認します。
 - a. グリッド マネージャーにアクセスします。
 - b. 構成 > セキュリティ > *証明書* を選択します。
 - c. *グローバル* タブで、*管理インターフェース証明書* を選択します。
7. コピーした公開証明書を使用するように管理クライアントを構成します。BEGIN タグと END タグを含めます。

管理インターフェース証明書をダウンロードまたはコピーします

管理インターフェースの証明書の内容を保存またはコピーして、他の場所で使用することができます。

手順

1. 構成 > セキュリティ > *証明書* を選択します。
2. *グローバル* タブで、*管理インターフェース証明書* 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ます。

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バンドルをダウンロードする`.pem`ファイル。オプションの CA バンドルを使用している場合、バンドル内の各証明書はそれぞれのサブタブに表示されます。

- a. *証明書のダウンロード*または*CAバンドルのダウンロード*を選択します。

CA バンドルをダウンロードする場合、CA バンドルのセカンダリ タブ内のすべての証明書が 1 つ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ます。拡張子を付けてファイルを保存する`.pem`。

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他の場所に貼り付けます。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のサブタブに表示されます。

- a. 証明書 **PEM** のコピー または **CA** バンドル **PEM** のコピー 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 タブ内の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 エディターに貼り付けます。
- c. 拡張子をつけてテキストファイルを保存する`.pem`。

例: `storagegrid_certificate.pem`

S3 API証明書を設定する

ストレージ ノードまたはロード バランサー エンドポイントへの S3 クライアント接続に使用されるサーバー証明書を置き換えたり復元したりできます。交換用のカスタム サーバー証明書は、組織に固有のものです。



このバージョンのドキュメント サイトから Swift の詳細は削除されました。見る ["StorageGRID 11.8: 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 CA 署名付き証明書は、単一の共通カスタム サーバー証明書と対応する秘密キーに置き換えることができます。

すべてのストレージ ノードに単一のカスタム 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とき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。

サーバーでの設定が完了したら、使用しているルート証明機関 (CA) に応じて、システムにアクセスするために使用する 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もあります。



失敗したサーバー証明書によって操作が中断されないように、ルート サーバー証明書の有効期限が切れそうになると、**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. 構成 > セキュリティ > *証明書*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ます。

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ます。

- a. *証明書のアップロード*を選択します。
- b. 必要なサーバ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 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**: 各中間発行証明機関からの証明書を含む単一のオプション ファイル。このファイルには、PEM でエンコードされた各 CA 証明書ファイルが、証明書チェーンの順序で連結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、各証明書は独自のタブに表示されます。
 - 証明書ファイルを保存するには 証明書のダウンロード を選択するか、証明書バンドルを保存するには **CA バンドル**のダウンロード を選択します。

証明書ファイル名とダウンロード場所を指定します。拡張子を付けてファイルを保存する .pem。

例: storagegrid_certificate.pem

- 証明書の内容をコピーして他の場所に貼り付けるには、「証明書 **PEM** のコピー」または「**CA バンドル PEM** のコピー」を選択します。
- d. *保存*を選択します。

カスタム サーバー証明書は、後続の新しい 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 1 つ以上の IP アドレス。

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、生成された証明書では、最初のドメイン名または IP アドレスがサブジェクト共通名 (CN) として使用されます。
有効日数	証明書の有効期限が切れるまでの作成後日数。
キー使用拡張機能を追加する	選択した場合 (デフォルト、推奨)、生成された証明書にキー使用法と拡張キー使用法の拡張機能が追加されます。 これらの拡張機能は、証明書に含まれるキーの目的を定義します。 注意: 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との接続の問題が発生しない限り、このチェックボックスをオンのままにしておきます。

c. ***生成***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、[証明書のダウンロード] を選択します。

証明書ファイル名とダウンロード場所を指定します。拡張子を付けてファイルを保存する .pem。

例: storagegrid_certificate.pem

- 証明書の内容をコピーして他の場所に貼り付けるには、「証明書 **PEM** のコピー」を選択します。

e. ***保存***を選択します。

カスタム サーバー証明書は、後続の新しい S3 クライアント接続に使用されます。

5. タブを選択すると、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が表示されます。



新しい証明書をアップロードまたは生成した後、関連する証明書の有効期限アラートがクリアされるまで最大 1 日かかります。

6. ページを更新して、Web ブラウザが更新されていることを確認します。

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 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

ストレージノードへの S3 クライアント接続にデフォルトの 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、ロードバランサーエンドポイントにはデフォルトの S3 API 証明書は使用できません。

手順

1. 構成 > セキュリティ > *証明書*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 S3 API 証明書は、ストレージ ノードへの後続の新しい S3 クライアント接続に使用されます。

4. **OK** を選択して警告を確認し、デフォルトの S3 API 証明書を復元します。

ルートアクセス権限があり、カスタム S3 API 証明書がロードバランサーのエンドポイント接続に使用されていた場合、デフォルトの S3 API 証明書を使用してアクセスできなくなるロードバランサーのエンドポイントのリストが表示されます。へ移動["ロードバランサのエンドポイントを構成する"](#)影響を受けるエンドポイントを編集または削除します。

5. ページを更新して、Web ブラウザが更新されていることを確認します。

S3 API証明書をダウンロードまたはコピーします

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. 構成 > セキュリティ > *証明書*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ます。

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バンドルをダウンロードする`.pem`ファイル。オプションの CA バンドルを使用している場合、バンドル内の各証明書はそれぞれのサブタブに表示されます。

- a. *証明書のダウンロード*または*CAバンドルのダウンロード*を選択します。

CA バンドルをダウンロードする場合、CA バンドルのセカンダリ タブ内のすべての証明書が 1 つ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ます。拡張子を付けてファイルを保存する .pem。

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他の場所に貼り付けます。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のサブタブに表示されます。

- a. 証明書 **PEM** のコピー または **CA** バンドル **PEM** のコピー 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 タブ内の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 エディターに貼り付けます。
- c. 拡張子をつけてテキストファイルを保存する .pem。

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"](#)

グリッド**CA**証明書をコピーする

StorageGRID は、内部証明機関 (CA) を使用して内部トラフィックを保護します。独自の証明書をアップロードした場合、この証明書は変更されません。

開始する前に

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

タスク概要

カスタム サーバー証明書が構成されている場合、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、グリッド **CA** タブを選択します。
2. 証明書 **PEM** セクションで、証明書をダウンロードまたはコピーします。

証明書ファイルをダウンロード

証明書をダウンロードする `.pem` ファイル。

- a. *証明書のダウンロード*を選択します。
- b. 証明書ファイル名とダウンロード場所を指定します。拡張子を付けてファイルを保存する `.pem`。

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他の場所に貼り付けます。

- a. *証明書**PEM**のコピー*を選択します。
- b. コピーした証明書をテキスト エディターに貼り付けます。
- c. 拡張子をつけてテキストファイルを保存する `.pem`。

例: `storagegrid_certificate.pem`

FabricPoolのStorageGRID証明書を構成する

FabricPoolを使用するONTAPクライアントなど、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 クライアントの場合は、ロードバランサのエンドポイントを設定するときにサーバ証明書を生成またはアップロードできません。

開始する前に

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

タスク概要

ロード バランサー エンドポイントを作成するときに、自己署名サーバ証明書を生成するか、既知の証明機関 (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。運用環境では、既知の CA によって署名された証明書を使用する必要があります。CA によって署名された証明書は、中断することなくローテーションできます。また、中間者攻撃に対する保護が強化されるため、安全性も高まります。

次の手順は、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。詳しい情報と手順については、["FabricPool用にStorageGRIDを構成する"](#)。

手順

1. 必要に応じて、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 エンドポイントを作成します。

HTTPS ロード バランサ エンドポイントを作成すると、サーバー証明書、証明書の秘密キー、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ONTAPのクラウド層として接続します。

アップロードした CA 証明書で使用するロード 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ます。次に、CA 証明書を提供します。



中間 CA がStorageGRID証明書を発行した場合は、中間 CA 証明書を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。

クライアント証明書を構成する

クライアント証明書により、承認された外部クライアントがStorageGRID 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 を安全に監視できるようになります。

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。

見る["セキュリティ証明書を管理する"](#)そして["カスタムサーバー証明書を構成する"](#)。



失敗したサーバー証明書によって操作が中断されないように、このサーバー証明書の有効期限が近づくと、*証明書ページで構成されたクライアント証明書の有効期限*アラートがトリガーされます。必要に応じて、[構成] > [セキュリティ] > [証明書] 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上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"](#)。

開始する前に

- ルートアクセス権限があります。
- グリッドマネージャにサインインするには、["サポートされているウェブブラウザ"](#)。
- クライアント証明書を構成するには:
 - 管理ノードの IP アドレスまたはドメイン名があります。
 - StorageGRID管理インターフェイス証明書を設定している場合は、管理インターフェイス証明書を設定するために使用した CA、クライアント証明書、および秘密キーがあります。
 - 独自の証明書をアップロードするには、証明書の秘密キーがローカル コンピューター上で利用可能である必要があります。
 - 秘密鍵は作成時に保存または記録されている必要があります。元の秘密鍵がない場合は、新しい秘密鍵を作成する必要があります。
- クライアント証明書を編集するには:

- 管理ノードの IP アドレスまたはドメイン名があります。
- 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、秘密キー、クライアント証明書、および CA (使用されている場合) がローカル コンピューター上で使用可能です。

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、次のいずれかの手順を使用します。

- [\[管理インターフェース証明書はすでに構成されています\]](#)
- [CA発行のクライアント証明書](#)
- [\[グリッドマネージャーから生成された証明書\]](#)

管理インターフェース証明書はすでに構成されています

顧客提供の CA、クライアント証明書、および秘密キーを使用して管理インターフェース証明書がすでに構成されている場合は、この手順を使用してクライアント証明書を追加します。

手順

1. グリッド マネージャーで、[構成] > [セキュリティ] > [証明書] を選択し、[クライアント] タブを選択します。
2. *追加*を選択します。
3. 証明書名を入力します。
4. 外部監視ツールを使用して Prometheus メトリックにアクセスするには、**Prometheus** を許可 を選択します。
5. *続行*を選択します。
6. *証明書の添付*手順では、管理インターフェース証明書をアップロードします。
 - a. *証明書のアップロード*を選択します。
 - b. *参照*を選択し、管理インターフェース証明書ファイルを選択します。(.pem)。
 - 証明書のメタデータと証明書 PEM を表示するには、[クライアント証明書の詳細] を選択します。
 - 証明書の内容をコピーして他の場所に貼り付けるには、「証明書 **PEM** のコピー」を選択します。
 - c. 作成 を選択して、証明書をグリッド マネージャーに保存します。

新しい証明書が [クライアント] タブに表示されます。

7. [外部監視ツールを構成する](#) Grafana など。

CA発行のクライアント証明書

管理インターフェース証明書が設定されておらず、CA 発行のクライアント証明書と秘密キーを使用する Prometheus のクライアント証明書を追加する予定の場合は、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ます["管理インターフェース証明書を構成する"](#)。

2. グリッド マネージャーで、[構成] > [セキュリティ] > [証明書] を選択し、[クライアント] タブを選択します。
3. *追加*を選択します。
4. 証明書名を入力します。
5. 外部監視ツールを使用して Prometheus メトリックにアクセスするには、**Prometheus** を許可 を選択します。
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、秘密キー、および CA バンドル ファイルをアップロードします。
 - a. *証明書のアップロード*を選択します。
 - b. *参照*を選択し、クライアント証明書、秘密鍵、CAバンドルファイルを選択します。(.pem)。
 - 証明書のメタデータと証明書 PEM を表示するには、[クライアント証明書の詳細] を選択します。
 - 証明書の内容をコピーして他の場所に貼り付けるには、「証明書 **PEM** のコピー」を選択します。
 - c. 作成 を選択して、証明書をグリッド マネージャーに保存します。

新しい証明書が [クライアント] タブに表示されます。

8. [外部監視ツールを構成する](#) Grafana など。

グリッドマネージャーから生成された証明書

管理インターフェース証明書が構成されておらず、Grid Manager の証明書生成機能を使用する Prometheus のクライアント証明書を追加する予定の場合は、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. グリッド マネージャーで、[構成] > [セキュリティ] > [証明書] を選択し、[クライアント] タブを選択します。
2. *追加*を選択します。
3. 証明書名を入力します。
4. 外部監視ツールを使用して Prometheus メトリックにアクセスするには、**Prometheus** を許可 を選択します。
5. *続行*を選択します。
6. *証明書の添付*手順では、*証明書の生成*を選択します。
7. 証明書情報を指定します。
 - **Subject** (オプション): 証明書所有者の X.509 サブジェクトまたは識別名 (DN)。
 - 有効日数: 生成された証明書が有効な日数 (生成された時点から計算)。
 - キー使用拡張機能の追加: 選択した場合 (デフォルト、推奨)、生成された証明書にキー使用拡張機能と拡張キー使用拡張機能が追加されます。

これらの拡張機能は、証明書に含まれるキーの目的を定義します。



証明書にこれらの拡張機能が含まれている場合に古いクライアントとの接続の問題が発生しない限り、このチェックボックスをオンのままにしておきます。

8. *生成*を選択します。

9. 証明書のメタデータと証明書 PEM を表示するには、[クライアント証明書の詳細] を選択します。



ダイアログを閉じると、証明書の秘密キーを表示できなくなります。キーを安全な場所にコピーまたはダウンロードします。

- 証明書の内容をコピーして他の場所に貼り付けるには、「証明書 **PEM** のコピー」を選択します。
- 証明書ファイルを保存するには、[証明書のダウンロード] を選択します。

証明書ファイル名とダウンロード場所を指定します。拡張子を付けてファイルを保存する .pem。

例：storagegrid_certificate.pem

- 証明書の秘密キーをコピーして他の場所に貼り付けるには、「秘密キーのコピー」を選択します。
- 秘密鍵をファイルとして保存するには、「秘密鍵のダウンロード」を選択します。

秘密鍵ファイル名とダウンロード場所を指定します。

10. 作成 を選択して、証明書をグリッド マネージャーに保存します。

新しい証明書が [クライアント] タブに表示されます。

11. グリッド マネージャーで、[構成] > [セキュリティ] > [証明書] を選択し、[グローバル] 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. certificate.pemとprivate_key.pemファイルをアップロードします。クライアント証明書の詳細ステップ。
CA バンドルをアップロードする必要はありません。

- a. *証明書のアップロード*を選択し、*続行*を選択します。
- b. 各証明書ファイルをアップロードする(.pem)。
- c. 保存 を選択して、証明書をグリッド マネージャーに保存します。

新しい証明書が管理インターフェイスの証明書ページに表示されます。

15. 外部監視ツールを構成するGrafana など。

外部監視ツールを設定する

手順

1. Grafana などの外部監視ツールで次の設定を構成します。

- a. 名前: 接続の名前を入力します。

StorageGRIDこの情報は必要ありませんが、接続をテストするには名前を指定する必要があります。

- b. **URL**: 管理ノードのドメイン名または IP アドレスを入力します。HTTPS とポート 9091 を指定します。

例: `https://admin-node.example.com:9091`

- c. **TLS** クライアント認証 と **CA** 証明書 を有効にします。
- d. TLS/SSL認証の詳細の下に、以下の内容をコピーして貼り付けます:
- 管理インターフェース CA 証明書を **CA Cert** へ
 - **Client Cert** へのクライアント証明書
 - 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ます。

ServerName は、管理インターフェイス証明書に表示されるドメイン名と一致する必要があります。

2. StorageGRIDまたはローカル ファイルからコピーした証明書と秘密キー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 メトリックにアクセスできるようになりました。

指標の詳細については、"[StorageGRIDの監視手順](#)"。

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して名前を変更したり、Prometheus アクセスを有効または無効にしたり、現在の証明書の有効期限が切れたときに新しい証明書をアップロードしたりできます。

手順

1. 構成 > セキュリティ > 証明書 を選択し、クライアント タブを選択します。

証明書の有効期限と Prometheus のアクセス権限が表にリストされています。証明書の有効期限が間もなく切れるか、すで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ます。
3. *編集*を選択し、*名前と権限の編集*を選択します。
4. 証明書名を入力します。
5. 外部監視ツールを使用して Prometheus メトリックにアクセスするには、**Prometheus** を許可 を選択します。
6. *続行*を選択して、グリッド マネージャーに証明書を保存します。

更新された証明書が [クライアント] タブに表示されます。

新しいクライアント証明書を添付する

現在の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. 構成 > セキュリティ > 証明書 を選択し、クライアント タブを選択します。

証明書の有効期限と Prometheus のアクセス権限が表にリストされています。証明書の有効期限が間もなく切れるか、すで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ます。
3. *編集*を選択し、編集オプションを選択します。

証明書をアップロード

証明書のテキストをコピーして他の場所に貼り付けます。

- a. *証明書のアップロード*を選択し、*続行*を選択します。
- b. クライアント証明書名をアップロードする(.pem)。

証明書のメタデータと証明書 PEM を表示するには、[クライアント証明書の詳細] を選択します。

- 証明書ファイルを保存するには、[証明書のダウンロード] を選択します。

証明書ファイル名とダウンロード場所を指定します。拡張子を付けてファイルを保存する .pem。

例: storagegrid_certificate.pem

- 証明書の内容をコピーして他の場所に貼り付けるには、「証明書 **PEM** のコピー」を選択します。
- c. 作成 を選択して、証明書をグリッド マネージャーに保存します。

更新された証明書が [クライアント] タブに表示されます。

証明書を生成する

他の場所に貼り付けるための証明書テキストを生成します。

- 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。

- **Subject** (オプション): 証明書所有者の X.509 サブジェクトまたは識別名 (DN)。
- 有効日数: 生成された証明書が有効な日数 (生成された時点から計算)。
- キー使用拡張機能の追加: 選択した場合 (デフォルト、推奨)、生成された証明書にキー使用拡張機能と拡張キー使用拡張機能が追加されます。

これらの拡張機能は、証明書に含まれるキーの目的を定義します。



証明書にこれらの拡張機能が含まれている場合に古いクライアントとの接続の問題が発生しない限り、このチェックボックスをオンのままにしておきます。

- c. *生成*を選択します。
- d. 証明書のメタデータと証明書 PEM を表示するには、[クライアント証明書の詳細] を選択します。



ダイアログを閉じると、証明書の秘密キーを表示できなくなります。キーを安全な場所にコピーまたはダウンロードします。

- 証明書の内容をコピーして他の場所に貼り付けるには、「証明書 **PEM** のコピー」を選択します。

- 証明書ファイルを保存するには、[証明書のダウンロード] を選択します。

証明書ファイル名とダウンロード場所を指定します。拡張子を付けてファイルを保存する .pem。

例： storagegrid_certificate.pem

- 証明書の秘密キーをコピーして他の場所に貼り付けるには、「秘密キーのコピー」を選択します。
- 秘密鍵をファイルとして保存するには、「秘密鍵のダウンロード」を選択します。

秘密鍵ファイル名とダウンロード場所を指定します。

- e. 作成 を選択して、証明書をグリッド マネージャーに保存します。

新しい証明書が [クライアント] タブに表示されます。

クライアント証明書をダウンロードまたはコピーする

他の場所で使用するためにクライアント証明書をダウンロードまたはコピーすることができます。

手順

1. 構成 > セキュリティ > 証明書 を選択し、クライアント タブを選択します。
2. コピーまたはダウンロードする証明書を選択します。
3. 証明書をダウンロードまたはコピーします。

証明書ファイルをダウンロード

証明書をダウンロードする `pem` ファイル。

- a. *証明書のダウンロード*を選択します。
- b. 証明書ファイル名とダウンロード場所を指定します。拡張子を付けてファイルを保存する .pem。

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他の場所に貼り付けます。

- a. *証明書PEMのコピー*を選択します。
- b. コピーした証明書をテキスト エディターに貼り付けます。
- c. 拡張子をつけてテキストファイルを保存する .pem。

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. 構成 > セキュリティ > 証明書 を選択し、クライアント タブを選択します。
2. 削除する証明書を選択します。
3. *削除*を選択して確認します。



最大 10 個の証明書を削除するには、[クライアント] タブで削除する各証明書を選択し、[アクション] > [削除] を選択します。

証明書が削除された後、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

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 接続と内部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 が移動中のデータを暗号化する方法を制御します。一般に、システムが Common Criteria に準拠している必要がある場合、または他の暗号を使用する必要がない限り、最新の互換性 (デフォルト) ポリシーを使用します。



一部のStorageGRIDサービスは、これらのポリシーの暗号を使用するように更新されていません。

開始する前に

- グリッドマネージャにサインインするには、["サポートされているウェブブラウザ"](#)。
- あなたは["ルートアクセス権限"](#)。

セキュリティポリシーを選択する

手順

1. 構成 > セキュリティ > *セキュリティ設定*を選択します。

TLS および **SSH** ポリシー タブには、使用可能なポリシーが表示されます。現在アクティブなポリシーは、ポリシー タイルに緑色のチェック マークで表示されます。



2. タイルを確認して、利用可能なポリシーについて学習します。

ポリシー	説明
最新の互換性（デフォルト）	強力な暗号化が必要な場合や特別な要件がない限り、デフォルトのポリシーを使用します。このポリシーは、ほとんどの TLS および SSH クライアントと互換性があります。
レガシー互換性	古いクライアントに追加の互換性オプションが必要な場合は、このポリシーを使用します。このポリシーの追加オプションにより、モダン互換性ポリシーよりも安全性が低くなる可能性があります。
コモンクライテリア	Common Criteria 認証が必要な場合は、このポリシーを使用します。
FIPS厳格	Common Criteria 認定が必要であり、ロード バランサ エンドポイント、Tenant Manager、および Grid Manager への外部クライアント接続にNetApp暗号化セキュリティ モジュール 3.0.8 を使用する必要がある場合は、このポリシーを使用します。このポリシー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。 注意: このポリシーを選択した後は、すべてのノードが" ローリング方式で再起動 "NetApp暗号化セキュリティ モジュールをアクティブ化します。再起動を開始および監視するには、[メンテナンス]>[ローリング再起動]を使用します。
カスタム	独自の暗号を適用する必要がある場合は、カスタム ポリシーを作成します。

3. 各ポリシーの暗号、プロトコル、アルゴリズムの詳細を表示するには、[詳細を表示] を選択します。
4. 現在のポリシーを変更するには、[ポリシーの使用] を選択します。

ポリシー タイルの 現在のポリシー の横に緑色のチェック 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

独自の暗号を適用する必要がある場合は、カスタム ポリシーを作成できます。

手順

1. 作成するカスタム ポリシーに最も類似したポリシーのタイルから、[詳細の表示] を選択します。

2. *クリップボードにコピー*を選択し、*キャンセル*を選択します。



3. カスタム ポリシー タイルから、構成して使用 を選択します。
4. コピーした JSON を貼り付けて、必要な変更を加えます。
5. *ポリシーを使用する*を選択します。

カスタム ポリシー タイルの 現在のポリシー の横に緑色のチェック マークが表示されます。

6. 必要に応じて、[構成の編集] を選択して、新しいカスタム ポリシーにさらに変更を加えます。

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"構成されたサーバー証明書"。

一時的にデフォルトのセキュリティ ポリシーに戻すことができます。

手順

1. 管理ノードにログインします。
 - a. 次のコマンドを入力します。 `ssh admin@Admin_Node_IP`
 - b. 記載されているパスワードを入力してください `Passwords.txt` ファイル。
 - c. ルートに切り替えるには、次のコマンドを入力します。 `su -`
 - d. 記載されているパスワードを入力してください `Passwords.txt` ファイル。

ルートとしてログインすると、プロンプトは `$`` に ``#`。

2. 次のコマンドを実行します。

```
restore-default-cipher-configurations
```

3. Web ブラウザから、同じ管理ノード上のグリッド マネージャーにアクセスします。
4. 以下の手順に従ってください[セキュリティポリシーを選択する](#)ポリシーを再度構成します。

ネットワークとオブジェクトのセキュリティを構成する

ネットワークとオブジェクトのセキュリティを設定して、保存された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。

保存されたオブジェクトの暗号化

保存されたオブジェクトの暗号化により、S3 を介して取り込まれるすべてのオブジェクト データの暗号化が可能になります。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を選択できます。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が暗号化されますが、既存の保存されたオブジェクトは変更されません。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。

保存された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暗号化方式の詳細については、以下を参照してください。["StorageGRIDの暗号化方式を確認する"](#)。

クライアントの変更を防止する

クライアントの変更を禁止するのはシステム全体の設定です。クライアントの変更を禁止する オプションを選択すると、次の要求は拒否されます。

S3 REST API

- DeleteBucketリクエスト
- 既存のオブジェクトのデータ、ユーザー定義のメタデータ、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に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。オプションで、非本番グリッドをテストする場合など、これらの接続に対して HTTP を有効にすることもできます。

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 ノード接続に HTTP を使用します。HTTPS接続のみを使用するクライアントや、ロードバランササービスに接続するクライアントの場合は、このオプションを使用する必要はありません (["各ロードバランサのエンドポイントを構成する"](#) HTTP または HTTPS のいずれかを使用します)。

見る["概要: クライアント接続の IP アドレスとポート"](#)HTTP または HTTPS を使用してストレージ ノードに接続するときに S3 クライアントが使用するポートを確認します。

オプションを選択

開始する前に

- グリッドマネージャにサインインするには、["サポートされているウェブブラウザ"](#)。
- ルートアクセス権限があります。

手順

1. 構成 > セキュリティ > *セキュリティ設定*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. 保存されたオブジェクトの暗号化については、保存されたオブジェクトを暗号化しない場合は なし (デフォルト) 設定を使用し、保存されたオブジェクトを暗号化するには **AES-128** または **AES-256** を選択します。
4. S3 クライアントが特定のリクエストを行わないようにする場合は、オプションで クライアントの変更を 禁止する を選択します。



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。構成された値は、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、オプションで [ストレージ ノード接続に **HTTP** を有効にする] を選択します。



実稼働グリッドで HTTP を有効にする場合は、リクエストが暗号化されずに送信されるため注意してください。

6. *保存*を選択します。

インターフェースのセキュリティ設定を変更する

インターフェース セキュリティ設定では、指定された時間を超えてユーザーが非アクティブだった場合にユーザーを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

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

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するまでに、ユーザーのブラウザが非アクティブになって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、次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組み込まれた、個別の構成不可能なStorageGRIDタイマー。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。ユーザーの認証の有効期限が切れると、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。
- StorageGRIDでシングル サインオン (SSO) が有効になっていることを前提とした、ID プロバイダーのタイムアウト設定。

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 SSO 資格情報を再入力して StorageGRID に再度アクセスする必要があります。見る["シングルサインオンを構成する"](#)。

管理APIスタックトレース

Grid Manager および Tenant Manager API エラー応答でスタックトレースが返されるかどうかを制御します。

このオプションはデフォルトで無効になっていますが、テスト環境ではこの機能を有効にする必要がある場合があります。一般に、API エラーが発生したときに内部ソフトウェアの詳細が公開されないように、運用環境ではスタックトレースを無効のままにしておく必要があります。

手順

1. 構成 > セキュリティ > *セキュリティ設定*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 日間の値を指定します。デフォルトのタイムアウトは 15 分です。
 - c. この機能を無効にするには、チェックボックスをオフにします。
 - d. *保存*を選択します。

新しい設定は、現在サイン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、ユーザーは再度サインインするか、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. チェックボックスを選択すると、Grid Manager および Tenant Manager API エラー応答でスタックトレースが返されます。



API エラーが発生したときに内部ソフトウェアの詳細が公開されないように、運用環境ではスタックトレースを無効のままにしておきます。

- c. *保存*を選択します。

キー管理サーバーを構成する

キー管理サーバー (KMS) とは何ですか？

キー管理サーバー (KMS) は、キー管理相互運用性プロトコル (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ます。サポートされている製品とバージョンのリストについては、["NetApp Interoperability Matrix Tool \(IMT\)"](#)。

インストール中に ノード暗号化 設定が有効になっているStorageGRIDアプライアンス ノードのノード暗号化キーを管理するには、1 つ以上のキー管理サーバーを使用できます。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と、アプライアンスがデータ センターから削除された場合でもデータを保護できます。アプライアンス ボリュームが暗号化された後は、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。

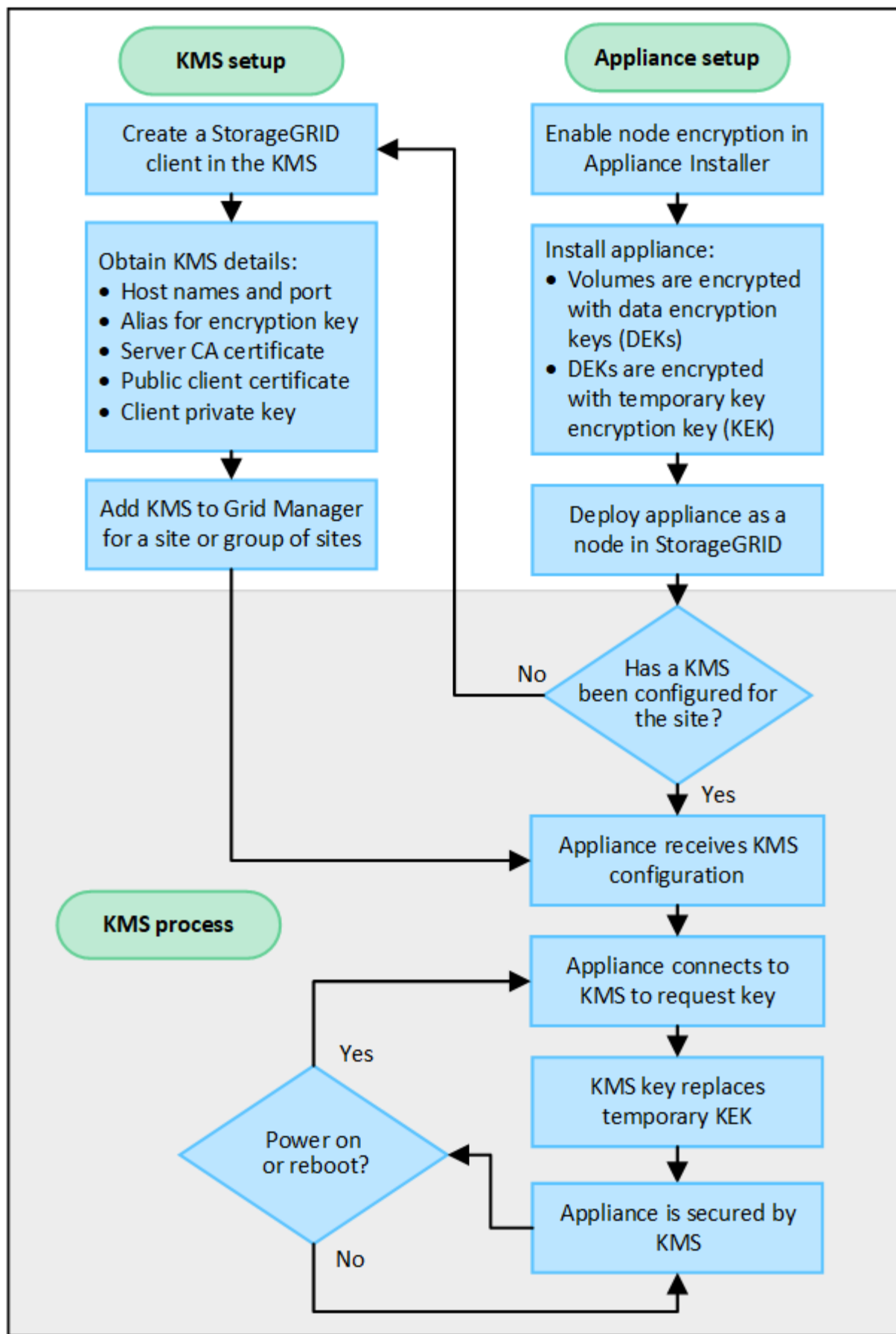


StorageGRID は、アプライアンス ノードの暗号化と復号化に使用される外部キーを作成または管理しません。StorageGRIDデータを保護するために外部のキー管理サーバを使用する予定の場合は、そのサーバの設定方法と暗号化キーの管理方法を理解する必要があります。キー管理タスクの実行は、これらの手順の範囲外です。ヘルプが必要な場合は、キー管理サーバーのドキュメントを参照するか、テクニカル サポートにお問い合わせください。

KMSとアプライアンスの構成

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データを保護する前に、1 つ以上の KMS サーバーを設定し、アプライアンス ノードのノード暗号化を有効にするという 2 つの構成タスクを完了する必要があります。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大まかな手順を示しています。



フローチャートでは、KMS セットアップとアプライアンス セットアップが並行して行われていることを示し

ています。ただし、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セットアップできます。

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、次の大まかな手順が含まれます。

手順	参照
KMS ソフトウェアにアクセスし、各 KMS または KMS クラスターに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"
KMS を Grid Manager に追加し、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"

アプライアンスのセットアップ

KMS を使用するためにアプライアンス ノードを設定するには、次の大まかな手順が含まれます。

1. アプライアンスのインストールのハードウェア構成段階で、StorageGRIDアプライアンス インストーラを使用して、アプライアンスの ノード暗号化 設定を有効にします。



アプライアンスをグリッドに追加された後は、*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で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、次のようにランダム データ暗号化キー (DEK) が各アプライアンス ボリューム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、変更できません。
 - 個々の 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。

見る ["ノード暗号化を有効にする"](#)詳細については。

キー管理暗号化プロセス（自動的に実行）

キー管理暗号化には、自動的に実行される次の高レベルの手順が含まれます。

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 KMS がすでに構成されている場合、アプライアンスは KMS 構成を受け取ります。

。サイトに KMS がまだ構成されていない場合は、サイトに KMS が構成され、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 はアプライアンスに暗号化キーを送信します。KMS からの新しいキーは一時的な KEK に置き換えられ、アプライアンス ボリュームの DEK の暗号化と復号化に使用されるようになりました。



暗号化されたアプライアンス ノードが構成された KMS に接続する前に存在するすべてのデータは、一時キーで暗号化されます。ただし、一時キーが KMS 暗号化キーに置き換えられるまで、アプライアンス ボリュームはデータ センターからの削除から保護されているとは見なされません。

4. アプライアンスの電源がオンになったり再起動したりすると、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るキーは、電源喪失や再起動により失われます。

鍵管理サーバーの使用に関する考慮事項と要件

外部キー管理サーバー (KMS) を構成する前に、考慮事項と要件を理解しておく必要があります。

サポートされている **KMIP** のバージョンは何ですか？

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 ファイアウォール設定では、各アプライアンス ノードがキー管理相互運用性プロトコル (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。デフォルトの KMIP 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、サイト用に構成した KMS または KMS クラスターへのネットワーク アクセス権を持っていることを確認する必要があります。

どのバージョンの **TLS** がサポートされていますか？

アプライアンス ノードと構成された 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がサポートするものと、"[TLSおよびSSHポリシー](#)"使用しているもの。

StorageGRID は、接続時に KMS とプロトコルと暗号 (TLS 1.2) または暗号スイート (TLS 1.3) を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、`tlsOutbound` グリッドのアクティブな TLS および SSH ポリシーのセクション (*[構成] > [セキュリティ][セキュリティ設定])。

どのアプライアンス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 ノード暗号化 設定が有効になっている任意のStorageGRIDアプライアンスの暗号化キーを管理できます。この設定は、StorageGRIDアプライアンス インストーラを使用したアプライアンスのインストール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された後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では外部キー管理を使用することはできません。

構成された 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。

構成された KMS は、次のようなソフトウェア ベース (アプライアンス以外) のノードには使用できません。

- 仮想マシン (VM) として展開されたノード
- 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構成すればよいですか？

新規インストールの場合、通常、テナントを作成する前に、グリッド マネージャーで 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。この順序により、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または後に、グリッド マネージャーでキー管理サーバーを構成できます。

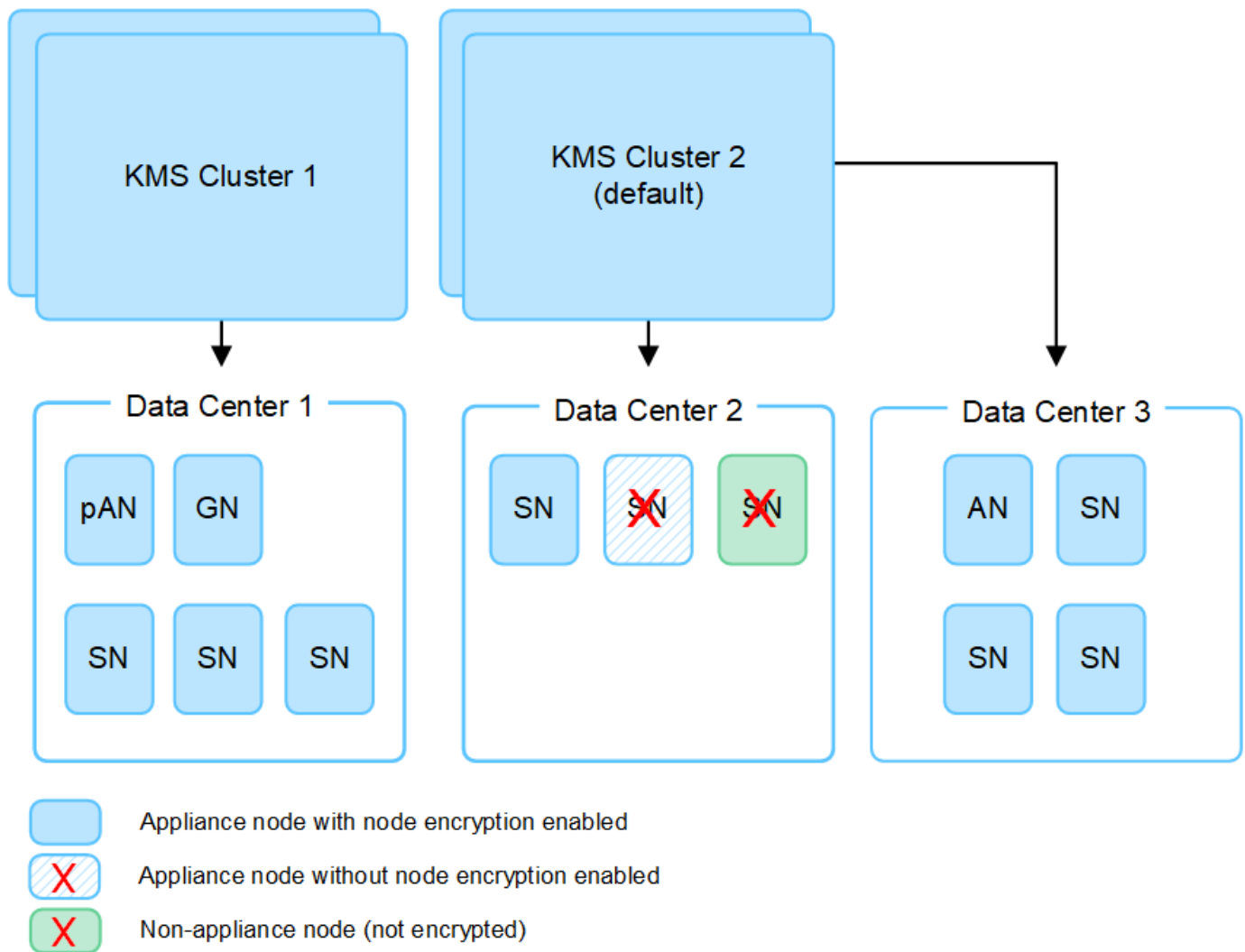
キー管理サーバーは何台必要ですか？

StorageGRID システム内のアプライアンス ノードに暗号化キーを提供するように、1 つ以上の外部キー管理サーバーを設定できます。各 KMS は、単一のサイトまたはサイト グループの 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 クラスターの使用をサポートしています。各 KMS クラスターには、構成設定と暗号化キーを共有する複数の複製されたキー管理サーバーが含まれています。高可用性構成のフェイルオーバー機能が向上するため、キー管理に KMS クラスターを使用することをお勧めします。

たとえば、StorageGRID システムに 3 つのデータ センター サイトがあるとします。1 つの KMS クラスターを構成してデータ センター 1 のすべてのアプライアンス ノードにキーを提供し、2 つ目の KMS クラスターを構成して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といったことが可能です。2 番目の KMS クラスターを追加すると、データセンター 2 とデータセンター 3 のデフォルトの KMS を構成できます。

アプライアンス以外のノードや、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 ノードでは、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何が起こりますか？

セキュリティのベストプラクティスとして、定期的に"**暗号化キーをローテーションする**"構成された各 KMS によって使用されます。

新しいキー バージョンが利用可能になると、次のようになります。

- これは、KMS に関連付けられたサイトまたはサイト内の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。配布は、キーがローテーションされてから 1 時間以内に行われる必要があります。
- 新しいキー バージョンが配布されたときに暗号化されたアプライアンス ノードがオフラインの場合、ノードは再起動するとすぐに新しいキーを受け取ります。
- 何らかの理由で新しいキー 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は、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に失敗しました というアラートがトリガーされます。このアラートを解決するには、テクニカル サポートに問い合わせる必要があります。

アプライアンス ノードを暗号化した後に再利用できますか？

暗号化されたアプライアンスを別のStorageGRIDシステムにインストールする必要がある場合は、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

アプライアンスインストーラを使用して **"KMS構成をクリアする"**。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 構成間の関連付けが削除されます。



KMS 暗号化キーにアクセスできないと、アプライアンスに残っているデータにはアクセスできなくなり、永久にロックされます。

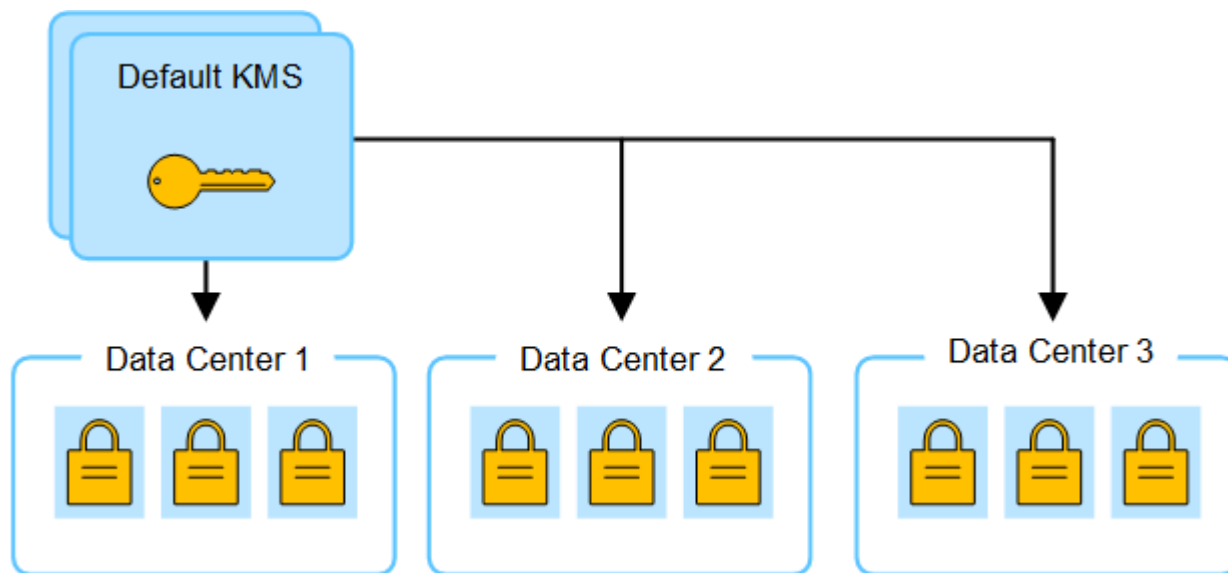
サイトのKMSを変更する際の考慮事項

各キー管理サーバー (KMS) または KMS クラスターは、単一のサイトまたはサイト グループにあるすべてのアプライアンス ノードに暗号化キーを提供します。サイトを使用する KMS を変更する必要がある場合は、暗号化キーをある KMS から別の KMS にコピーする必要がある場合があります。

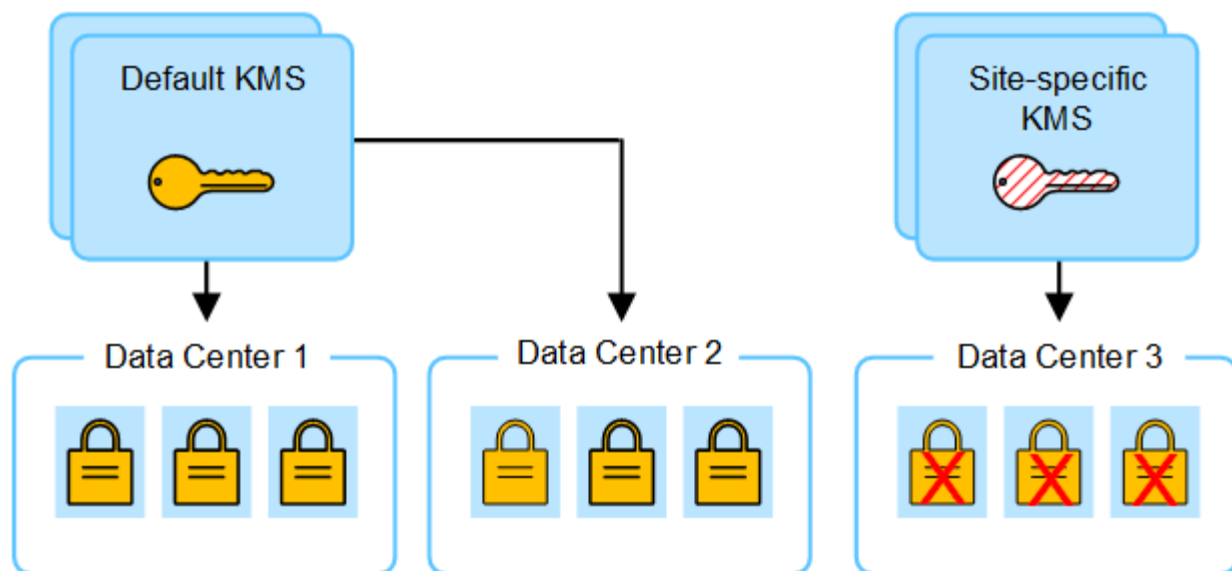
サイトに使用されている KMS を変更する場合は、そのサイトにある以前に暗号化されたアプライアンス ノードを、新しい KMS に保存されているキーを使用して復号化できることを確認する必要があります。場合によっては、現在のバージョンの暗号化キーを元の KMS から新しい KMS にコピーする必要があります。サイトの暗号化されたアプライアンス ノードを復号化するには、KMS に正しいキーがあることを確認する必要があります。

例えば：

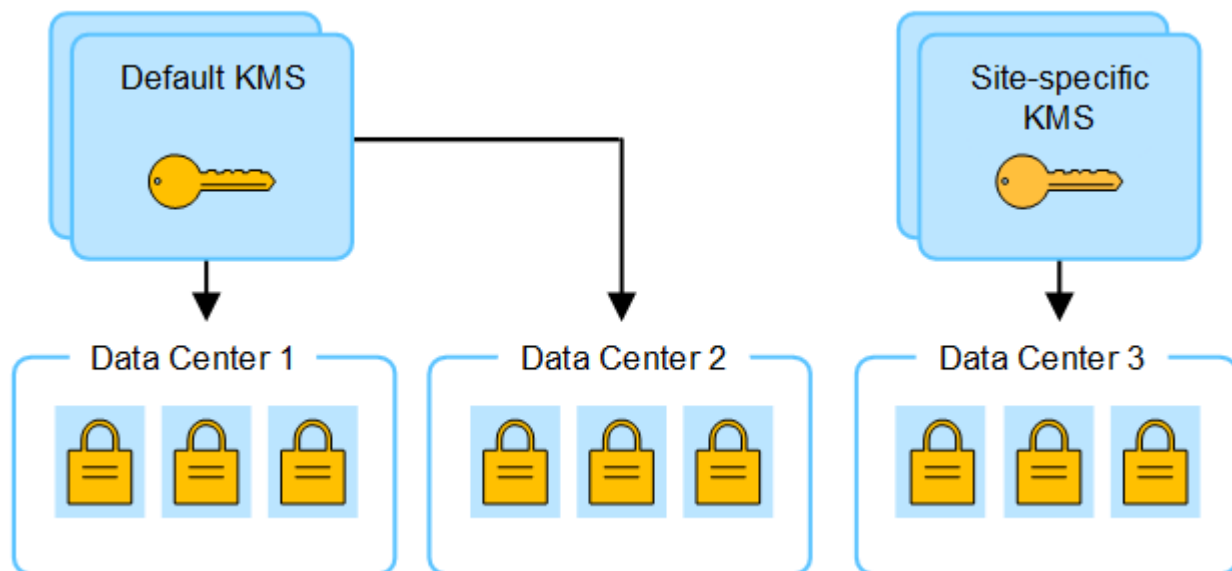
1. 最初に、専用の KMS がいないすべてのサイトに適用されるデフォルトの KMS を構成します。
2. KMS が保存されると、*ノード暗号化*設定が有効になっているすべてのアプライアンス ノードが KMS に接続し、暗号化キーを要求します。このキーは、すべてのサイトのアプライアンス ノードを暗号化するために使用されます。これらのアプライアンスを復号化する場合にも、同じキーを使用する必要があります。



3. 1つのサイト (図のデータ センター 3) にサイト固有の KMS を追加することにしました。ただし、アプライアンス ノードはすでに暗号化されているため、サイト固有の KMS の構成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発生します。



4. この問題を解決するには、暗号化キーの現在のバージョンをデフォルトの KMS から新しい KMS にコピーします。(技術的には、元のキーを同じエイリアスを持つ新しいキーにコピーします。元のキー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るようになったため、StorageGRID に保存できるようになりました。



サイトで使用する **KMS** を変更するユースケース

次の表は、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
1 つ以上のサイト固有の KMS エントリがあり、そのうちの 1 つをデフォルトの KMS として使用します。	サイト固有の KMS を編集します。キーの管理対象 フィールドで、別の KMS によって管理されていないサイト (デフォルトの 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。新しいサイトではデフォルトの KMS を使用しません。	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、暗号化キーの現在のバージョンをデフォルトの KMS から新しい KMS にコピーします。 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 で別のサーバーを使用する必要がある。	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、暗号化キーの現在のバージョンを既存の 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、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に追加するには、まず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 を構成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リストについては、["NetApp Interoperability Matrix Tool \(IMT\) "](#)。

手順

1. KMS ソフトウェアから、使用する予定の KMS または KMS クラスターごとに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サイト グループにあるStorageGRIDアプライアンス ノードの単一の暗号化キーを管理します。

2. 次の 2 つの方法のいずれかを使用してキーを作成します。
 - KMS 製品のキー管理ページを使用します。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ます。

暗号化キーは 2,048 ビット以上で、エクスポート可能である必要があります。

- StorageGRIDにキーを作成させます。テストして保存するとプロンプトが表示されます"[クライアント証明書のアップロード](#)"。

3. 各 KMS または KMS クラスターについて次の情報を記録します。

KMS をStorageGRIDに追加するときに、次の情報が必要になります。

- 各サーバーのホスト名または IP アドレス。
- KMS で使用される KMIP ポート。
- KMS 内の暗号化キーのキーエイリアス。

4. 各 KMS または KMS クラスターごとに、証明機関 (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各 PEM エンコードされた 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 はStorageGRIDに対して自身を認証できるようになります。

- 証明書には、Privacy Enhanced Mail (PEM) Base-64 エンコード X.509 形式を使用する必要があります。
- 各サーバー証明書のサブジェクト別名 (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 アドレスが含まれている必要があります。



StorageGRIDで KMS を構成する場合は、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、通常ポート 5696 を使用する KMS の KMIP インターフェイスで使用される証明書と一致する必要があります。
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キーを取得します。

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るようになります。

キー管理サーバー (KMS) を追加する

各 KMS または KMS クラスターを追加するには、StorageGRIDキー管理サーバ ウィザードを使用します。

開始する前に

- あなたは、"[キー管理サーバーの使用に関する考慮事項と要件](#)"。
- あなたが持っている"[StorageGRIDをKMSのクライアントとして構成しました](#)"各 KMS または KMS クラスターの必要な情報が得られます。
- グリッドマネージャにサインインするには、"[サポートされているウェブブラウザ](#)"。
- あなたは"[ルートアクセス権限](#)"。

タスク概要

可能であれば、別の KMS によって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 を構成

する前に、サイト固有のキー管理サーバーを構成します。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がデフォルトの 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、まず、暗号化キーの現在のバージョンをデフォルトの KMS から新しい KMS にコピーする必要があります。見る["サイトのKMSを変更する際の考慮事項"](#)詳細については。

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手順 1 (KMS の詳細) では、KMS または KMS クラスターの詳細を指定します。

手順

1. 構成 > セキュリティ > *キー管理サーバー*を選択します。

構成の詳細タブが選択された状態で、キー管理サーバー ページが表示されます。

2. *作成*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 で構成したStorageGRIDクライアントについて、次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説明的な名前。 1 ～ 64 文字にする必要があります。
キー名	KMS 内のStorageGRIDクライアントの正確なキーエイリアス。 1 ～255 文字にする必要があります。 注: KMS 製品を使用してキーを作成していない場合は、StorageGRIDでキーを作成するように求められます。
キーを管理します	この KMS に関連付けられるStorageGRIDサイト。可能であれば、別の KMS によって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 を構成する前に、サイト固有のキー管理サーバーを構成する必要があります。 • 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、サイトを選択します。 • 専用の KMS を持たないサイトと、その後の拡張で追加するサイトに適用されるデフォルトの KMS を構成するには、[別の KMS によって管理されていないサイト (デフォルトの KMS)] を選択します。 注意: 以前にデフォルトの KMS によって暗号化されたサイトを選択し、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 構成を保存するときに検証エラーが発生します。

フィールド	説明
ポート	KMS サーバーがキー管理相互運用性プロトコル (KMIP) 通信に使用するポート。デフォルトは KMIP 標準ポートである 5696 です。
ホスト名	KMS の完全修飾ドメイン名または IP アドレス。 注: サーバー証明書のサブジェクト別名 (SAN) フィールドには、ここで入力する FQDN または IP アドレスが含まれている必要があります。そうしないと、StorageGRID は KMS または KMS クラスター内のすべてのサーバーに接続できなくなります。

4. KMS クラスターを構成する場合は、「別のホスト名を追加」を選択して、クラスター内の各サーバーのホスト名を追加します。
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手順 2 (サーバー証明書のアップロード) では、KMS 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 は StorageGRID に対して自身を認証できるようになります。

手順

1. ステップ 2 (サーバー証明書のアップロード) から、保存されたサーバー証明書または証明書バンドルの場所を参照します。
2. 証明書ファイルをアップロードします。

サーバ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がそれぞれ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) では、クライアント証明書とクライアント証明書の秘密キー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るようになります。

手順

1. ステップ 3 (クライアント証明書のアップロード) から、クライアント証明書の場所を参照します。
2. クライアント証明書ファイルをアップロードします。

クライアント証明書のメタデータが表示されます。

3. クライアント証明書の秘密キーの場所を参照します。
4. 秘密鍵ファイルをアップロードします。

5. *テストして保存*を選択します。

キーが存在しない場合は、StorageGRIDにキーを作成するように要求されます。

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、正しいキーが KMS に見つかった場合、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] ページの証明書のステータスが [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には、最大 30 分かかる場合があります。現在のステータスを確認するには、Web ブラウザを更新する必要があります。

6. テストして保存 を選択したときにエラー メッセージが表示される場合は、メッセージの詳細を確認して **OK** を選択します。

たとえば、接続テストが失敗した場合、「422: 処理できないエンティティ」という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構成を保存する必要がある場合は、「強制保存」を選択します。



*強制保存*を選択すると、KMS 構成は保存されますが、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は、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。問題が解決されるまで、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、構成を強制的に保存する場合は **[OK]** を選択します。

KMS 構成は保存されますが、KMS への接続はテストされません。

KMSを管理する

キー管理サーバー (KMS) の管理には、詳細の表示または編集、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 の削除が含まれます。

開始する前に

- グリッドマネージャにサインインするには、"[サポートされているウェブブラウザ](#)"。
- あなたは"[必要なアクセス許可](#)"。

KMSの詳細を表示

StorageGRIDシステム内の各キー管理サーバー (KMS) に関する情報 (キーの詳細、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など) を表示できます。

手順

1. 構成 > セキュリティ > *キー管理サーバー*を選択します。

キー管理サーバー ページが表示され、次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の一覧が表示されます。
- 「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。

- 特定の KMS の詳細を表示し、その KMS に対して操作を実行するには、KMS の名前を選択します。KMS の詳細ページには、次の情報が表示されます。

フィールド	説明
キーを管理します	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、または別の KMS によって管理されていないサイト (デフォルトの KMS) が表示されます。
ホスト名	KMS の完全修飾ドメイン名または IP アドレス。 2 つのキー管理サーバーのクラスターがある場合は、両方のサーバーの完全修飾ドメイン名または IP アドレスがリストされます。クラスター内に 3 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 アドレスが、クラスター内の追加のキー管理サーバーの数とともに一覧表示されます。 例えば： 10.10.10.10 and 10.10.10.11`または `10.10.10.10 and 2 others。 クラスター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。

- KMS 詳細ページでタブを選択すると、次の情報が表示されます。

タブ	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	キーの最新バージョンの一意の識別子。	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、時刻、証明書 PEM など)。	証明書PEM	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、時刻、証明書 PEM など)。

4. 組織のセキュリティ慣行で必要な頻度で、「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新しいバージョンのキーを作成します。

キーのローテーションが成功すると、キー UID と最終変更日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、最後に使用したキーのバージョンから同じキーの新しいバージョンにローテーションします。まったく異なるキーに回転しないでください。



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ないでください。StorageGRID、以前に使用したすべてのキー 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。構成された KMS のキー エイリアスを変更すると、StorageGRID はデータを復号化できなくなる可能性があります。

証明書の管理

サーバーまたはクライアント証明書に関する問題があれば速やかに対処してください。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 アクセスを維持するには、証明書の問題をできるだけ早く解決する必要があります。

手順

1. 構成 > セキュリティ > *キー管理サーバー*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ます。
3. いずれかの KMS の証明書の有効期限が不明な場合は、最大 30 分待ってから 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か、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ます。
 - 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ます。
 - b. 証明書を置き換えるには、[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ます。
 - c. これらのサブステップを繰り返し、サーバー証明書の代わりに*クライアント証明書*を選択します。
5. **KMS CA** 証明書の有効期限、**KMS** クライアント証明書の有効期限、および **KMS** サーバー証明書の有効期限 アラートがトリガーされた場合は、各アラートの説明をメモし、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には、最大 30 分かかる場合があります。現在の値を表示するには、Web ブラウザを更新してください。



サーバー証明書のステータスが不明 というステータスが表示される場合は、KMS で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 システム内のアプライアンス ノードに関する情報を表示できます。

手順

1. 構成 > セキュリティ > *キー管理サーバー*を選択します。

キー管理サーバー ページが表示されます。[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表示されます。

2. ページの上部から、[暗号化されたノード] タブを選択します。

[暗号化されたノード] タブには、StorageGRIDシステム内の 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 ノードの表の情報を確認します。

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	ノードのタイプ: ストレージ、管理、またはゲートウェイ。
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 の説明的な名前。 KMS がリストされていない場合は、[構成の詳細] タブを選択して KMS を追加します。 "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と復号化に使用される暗号化キーの一意の ID。キー UID 全体を表示するには、テキストを選択します。 ダッシュ (--) は、アプライアンス ノードと KMS 間の接続の問題が原因で、キー UID が不明であることを示します。
ステータス	KMS とアプライアンス ノード間の接続の状態。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 構成の変更後、接続ステータスが更新されるまでに数分かかる場合があります。 注: 新しい値を表示するには、Web ブラウザを更新してください。

4. ステータス列に KMS の問題が示されている場合は、すぐに問題に対処してください。

通常の KMS 操作中は、ステータスは **KMS** に接続済み になります。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 ボリュームの暗号化に失敗しました
- KMSが設定されていません

これらのアラートに対して推奨されるアクションを実行します。



データが完全に保護されるようにするには、問題があればすぐに対処する必要があります。

KMSの編集

たとえば、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構成を編集する必要がある場合があります。

開始する前に

- KMS用に選択したサイトを更新する予定の場合は、"[サイトのKMSを変更する際の考慮事項](#)"。
- グリッドマネージャにサインインするには、"[サポートされているウェブブラウザ](#)"。
- あなたは"[ルートアクセス権限](#)"。

手順

1. 構成 > セキュリティ > *キー管理サーバー*を選択します。

キー管理サーバー ページが表示され、構成されている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。

表内の KMS 名を選択し、KMS 詳細ページで 編集 を選択して、KMS を編集することもできます。

3. 必要に応じて、キー管理サーバーの編集ウィザードの*ステップ 1 (KMS の詳細)* で詳細を更新します。

フィールド	説明
KMS name	この KMS を識別するのに役立つ説明的な名前。 1 ～ 64 文字にする必要があります。
キー名	KMS 内のStorageGRIDクライアントの正確なキーエイリアス。 1～255 文字にする必要があります。 キー名を編集する必要があるのは、まれなケースのみです。たとえば、KMS でエイリアスの名前が変更された場合や、以前のキーのすべてのバージョンが新しいエイリアスのバージョン履歴にコピーされた場合は、キー名を編集する必要があります。

フィールド	説明
キーを管理します	サイト固有の KMS を編集していて、デフォルトの KMS がまだない場合は、オプションで 別の KMS によって管理されていないサイト (デフォルトの KMS) を選択します。これを選択すると、サイト固有の KMS がデフォルトの KMS に変換され、専用の KMS を持たないすべてのサイトと、拡張で追加されたすべてのサイトに適用されます。 注意: 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 サーバーがキー管理相互運用性プロトコル (KMIP) 通信に使用するポート。デフォルトは KMIP 標準ポートである 5696 です。
ホスト名	KMS の完全修飾ドメイン名または IP アドレス。 注: サーバー証明書のサブジェクト別名 (SAN) フィールドには、ここで入力する FQDN または IP アドレスが含まれている必要があります。そうしないと、StorageGRID は KMS または KMS クラスター内のすべてのサーバーに接続できなくなります。

4. KMS クラスターを構成する場合は、「別のホスト名を追加」を選択して、クラスター内の各サーバーのホスト名を追加します。

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. サーバー証明書を置き換える必要がある場合は、[参照] を選択して新しいファイルをアップロードします。

7. *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キーを置き換える必要がある場合は、[参照] を選択して新しいファイルをアップロードします。

9. *テストして保存*を選択します。

影響を受けるサイトにあるキー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、正しいキーが KMS 上に見つかった場合、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」を選択します。

たとえば、この KMS 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は、「422: 処理できないエンティティ」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構成を保存する必要がある場合は、[強制保存] を選択します。



*強制保存*を選択すると、KMS 構成は保存されますが、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は、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。問題が解決されるまで、データにアクセスできなくなる可能性があります。

KMS 構成が保存されます。

12. 確認の警告を確認し、構成を強制的に保存する場合は **[OK]** を選択します。

KMS 構成は保存されますが、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必要がある場合があります。たとえば、サイトを廃止した場合は、サイト固有の KMS を削除する必要がある場合があります。

開始する前に

- あなたは、"[キー管理サーバーの使用に関する考慮事項と要件](#)"。
- グリッドマネージャにサインインするには、"[サポートされているウェブブラウザ](#)"。
- あなたは"[ルートアクセス権限](#)"。

タスク概要

次の場合には 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。
- ノード暗号化が有効になっているアプライアンス ノードがある各サイトにサイト固有の KMS がすでに存在する場合は、デフォルトの KMS を削除できます。

手順

1. 構成 > セキュリティ > *キー管理サーバー*を選択します。

キー管理サーバー ページが表示され、構成されている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。

テーブル内の KMS 名を選択し、KMS 詳細ページで 削除 を選択して、KMS を削除することもできます。

3. 次の点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 ノードがないサイトのサイト固有の KMS を削除しています。
- デフォルトの KMS を削除していますが、ノード暗号化が行われたサイトごとにサイト固有の KMS が既に存在しています。

4. *はい*を選択してください。

KMS 構成が削除されます。

プロキシ設定を管理する

ストレージプロキシを構成する

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 エンドポイント間に非透過プロキシを構成できます。たとえば、プラットフォーム サービス 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、非透過プロキシが必要になる場合があります。



構成されたストレージ プロキシ設定は、Kafka プラットフォーム サービス エンドポイントには適用されません。

開始する前に

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

タスク概要

単一のストレージ プロキシの設定を構成できます。

手順

1. 構成 > セキュリティ > *プロキシ設定*を選択します。
2. *ストレージ*タブで、*ストレージ プロキシを有効にする*チェックボックスをオンにします。
3. ストレージ プロキシのプロトコルを選択します。
4. プロキシ サーバーのホスト名または IP アドレスを入力します。
5. 必要に応じて、プロキシ サーバーに接続するために使用するポートを入力します。

プロトコルのデフォルト ポート (HTTP の場合は 80、SOCKS5 の場合は 1080) を使用するには、このフィールドを空白のままにします。

6. *保存*を選択します。

ストレージ プロキシを保存した後、プラットフォーム サービスまたはクラウド ストレージ プールの新しいエンドポイントを構成してテストできます。



プロキシの変更が有効になるまでに最大 10 分かかる場合があります。

7. プロキシ サーバーの設定を確認し、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ます。
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] を選択します。

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) の間に非透過プロキシ サーバーを設定できます。

AutoSupportの詳細については、以下を参照してください。"[AutoSupportを構成する](#)"。

開始する前に

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

タスク概要

単一の管理プロキシの設定を構成できます。

手順

1. 構成 > セキュリティ > *プロキシ設定*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. *管理者*タブを選択します。
3. *管理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 サーバーのホスト名または IP アドレスを入力します。
5. プロキシ サーバーに接続するために使用するポートを入力します。
6. 必要に応じて、プロキシ サーバーのユーザー名とパスワードを入力します。

プロキシ サーバーでユーザー名または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おきます。

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場合は、「プロキシ証明書の検証」を選択します。管理プロキシ サーバーによって提示された SSL 証明書の信頼性を検証するために、CA バンドルをアップロードします。



プロキシ証明書が検証されている場合、AutoSupport on Demand、StorageGRID経由の E シリーズ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 サーバーと通信するとき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] を選択します。

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 サーバーが構成されます。



プロキシの変更が有効になるまでに最大 10 分かかる場合があります。

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、[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いたり閉じたりすることができます。

外部ファイアウォールで特定のポートを開いたり閉じたりすることで、StorageGRID管理ノード上のユーザー インターフェイスと API へのアクセスを制御できます。たとえば、他の方法を使用してシステム アクセスを制御するだけでなく、ファイアウォールでテナントが Grid Manager に接続できないようにすることもできます。

StorageGRID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を構成する"](#)。

ポート	説明	ポートが開いている場合...
443	管理ノードのデフォルトの HTTPS ポート	Web ブラウザおよび管理 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	管理ノード上の制限されたグリッド マネージャー ポート	• Web ブラウザおよび管理 API クライアントは、HTTPS を使用して Grid Manager および Grid Management API にアクセスできます。 • Web ブラウザおよび管理 API クライアントは、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。 • 内部コンテンツのリクエストは拒否されます。
9443	管理ノード上の制限されたテナント マネージャー ポート	• Web ブラウザと管理 API クライアントは、HTTPS を使用してテナント マネージャとテナント管理 API にアクセスできます。 • Web ブラウザおよび管理 API クライアントは、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。 • 内部コンテンツのリクエストは拒否されます。



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

関連情報

- ["グリッド マネージャに Sign in"](#)
- ["テナント アカウントを作成する"](#)
- ["外部 コミュニケーション"](#)

StorageGRID には各ノードに内部ファイアウォールが含まれており、ノードへのネットワーク アクセスを制御できるため、グリッドのセキュリティが強化されます。ファイアウォールを使用して、特定のグリッド展開に必要なポートを除くすべてのポートでのネットワーク 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構成の変更は、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をカスタマイズします。

- 特権アドレス リスト: このタブを使用して、閉じたポートへの選択したアクセスを許可します。「外部アクセスの管理」タブを使用して、閉じられたポートにアクセスできる IP アドレスまたはサブネットを CIDR 表記で追加できます。
- 外部アクセスの管理: このタブを使用して、デフォルトで開いているポートを閉じたり、以前に閉じたポートを再度開いたりします。
- 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、「外部アクセスの管理」タブの設定を上書きします。

- 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 エンドポイント ポート (グローバル、ノード インターフェイス、およびノード タイプにバインドされたエンドポイント) 上の接続のみを受け入れます。
- ロード バランサのエンドポイント 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。
- 信頼されている場合、[外部アクセスの管理] タブで開かれているすべてのポートと、クライアント ネットワークで開かれているすべてのロード バランサー エンドポイントにアクセスできるようになります。



あるタブで行った設定は、別のタブで行うアクセスの変更に影響を与える可能性があります。すべてのタブの設定を必ず確認し、ネットワークが期待どおりに動作することを確認してください。

内部ファイアウォール制御を構成するには、["ファイアウォール制御を構成する"](#)。

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、以下を参照してください。["外部ファイアウォールでアクセスを制御する"](#)。

特権アドレスリストと外部アクセスの管理タブ

特権アドレス リスト タブでは、閉じられているグリッド ポートへのアクセスが許可される 1 つ以上の IP アドレスを登録できます。[外部アクセスの管理] 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 (外部ポートは、デフォルトで非グリッド ノードからアクセスできるポートです)。多くの場合、これら 2 つのタブを一緒に使用して、グリッドに許可する必要があるネットワーク アクセスを正確にカスタマイズできます。



特権 IP アドレスには、デフォルトでは内部グリッド ポートへのアクセス権がありません。

例1: メンテナンスタスクにジャンプホストを使用する

ネットワーク管理にジャンプ ホスト (セキュリティが強化されたホスト) を使用するとします。次の一般的な手順を使用できます。

1. 特権アドレス リスト タブを使用して、ジャンプ ホストの IP アドレスを追加します。
2. すべてのポートをブロックするには、「外部アクセスの管理」タブを使用します。



ポート 443 および 8443 をブロックする前に、特権 IP アドレスを追加します。ブロックされたポートに現在接続しているユーザー (あなたを含む) は、その IP アドレスが特権アドレス リストに追加されていない限り、Grid Manager にアクセスできなくなります。

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が、ジャンプ ホストを除くすべてのホストに対してブロックされます。その後、ジャンプ ホストを使用して、グリッド上でメンテナンス タスクをより安全に実行できるようになります。

例2: 機密ポートをロックダウンする

機密ポートとそのポート上のサービス (たとえば、ポート 22 上の SSH) をロックダウンするとします。次の一般的な手順を使用できます。

1. 特権アドレス リスト タブを使用して、サービスへのアクセスが必要なホストにのみアクセスを許可します。
2. すべてのポートをブロックするには、「外部アクセスの管理」タブを使用します。



Grid Manager および Tenant Manager にアクセスするために割り当てられたポートへのアクセスをブロックする前に、特権 IP アドレスを追加します (プリセット ポートは 443 と 8443)。ブロックされたポートに現在接続しているユーザー (あなたを含む) は、その IP アドレスが特権アドレス リストに追加されていない限り、Grid Manager にアクセスできなくなります。

設定を保存すると、特権アドレス リスト上のホストでポート 22 と SSH サービスが利用できるようになります。他のすべてのホストは、リクエストがどのインターフェースから送信されたかに関係なく、サービスへのアクセスを拒否されます。

例3: 使用されていない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、使用しない予定の一部のサービスを無効にすることができます。たとえば、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、明示的に構成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、StorageGRID を敵対的な攻撃から保護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はすべてのグリッドノードへの受信接続を信頼します。["利用可能な外部ポート"](#)。

各ノードのクライアント ネットワークを信頼できないものとして指定することで、StorageGRIDシステムに対する敵対的な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 バランサのエンドポイントとして明示的に構成されたポート上の受信接続のみを受け入れま

す。見る"[ロードバランサのエンドポイントを構成する](#)"そして"[ファイアウォール制御を構成する](#)"。

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る

ゲートウェイ ノードで、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とします。次のような一般的な手順を実行します。

1. から"[ロード バランサ エンドポイント](#)"ページで、ポート 443 で HTTPS 経由の S3 のロード バランサー エンドポイントを構成します。
2. ファイアウォール制御ページで、「信頼できない」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できないことを指定します。

設定を保存すると、ポート 443 の HTTPS S3 要求と ICMP エコー (ping) 要求を除き、ゲートウェイ ノードのクライアント ネットワーク上のすべての受信トラフィックがドロップされます。

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 ノードからの送信 S3 プラットフォーム サービス 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を禁止したいとします。次のような一般的な手順を実行します。

- ・ファイアウォール制御ページの「信頼できないクライアント ネットワーク」タブで、ストレージ ノード上のクライアント ネットワークが信頼できないことを示します。

構成を保存すると、ストレージ ノードはクライアント ネットワーク上の着信トラフィックを受け入れなくなりますが、構成されたプラットフォーム サービスの宛先への送信要求は引き続き許可されます。

例3: グリッドマネージャへのアクセスをサブネットに制限する

特定のサブネット上でのみ Grid Manager アクセスを許可するとします。次の手順を実行します。

1. 管理ノードのクライアント ネットワークをサブネットに接続します。
2. 「信頼できないクライアント 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できないものとして構成します。
3. 管理インターフェイス ロード バランサ エンドポイントを作成するときは、ポートを入力し、ポートがアクセスする管理インターフェイスを選択します。
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. [外部アクセスの管理] タブを使用して、すべての外部ポート (そのサブネットの外部のホストに特権 IP アドレスが設定されているかどうかに関係なく) をブロックします。

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。

内部ファイアウォールを構成する

StorageGRIDファイアウォールを設定して、StorageGRIDノード上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

- グリッドマネージャにサインインするには、["サポートされているウェブブラウザ"](#)。
- あなたが持っている["特定のアクセス権限"](#)。
- 下記の情報を確認しました["ファイアウォール制御を管理する"](#)そして["ネットワークガイドライン"](#)。
- 管理ノードまたはゲートウェイ ノードが明示的に構成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場合は、ロード バランサのエンドポイントを定義しておきます。



クライアント ネットワークの設定を変更する場合、ロード バランサのエンドポイントが構成されていないと、既存のクライアント接続が失敗する可能性があります。

タスク概要

StorageGRID には各ノードに内部ファイアウォールが含まれており、グリッドのノード上の一部のポートを開いたり閉じたりすることができます。ファイアウォール コントロール タブを使用して、グリッド ネットワーク、管理ネットワーク、およびクライアント ネットワークでデフォルトで開いているポートを開いたり閉じたりすることができます。閉じられているグリッド ポートにアクセスできる特権 IP アドレスのリストを作成することもできます。クライアント ネットワークを使用している場合は、ノードがクライアント ネットワークからの受信トラフィックを信頼するかどうかを指定し、クライアント ネットワーク上の特定のポートのアクセスを構成できます。

グリッド外部の IP アドレスに開くポートの数を絶対に必要なものだけに制限すると、グリッドのセキュリティが強化されます。3 つのファイアウォール制御タブのそれぞれの設定を使用して、必要なポートのみが開かれていることを確認します。

ファイアウォール制御の使用に関する詳細（例を含む）については、以下を参照してください。["ファイアウォール制御を管理する"](#)。

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、以下を参照してください。["外部ファイアウォールでアクセスを制御する"](#)。

ファイアウォール制御へのアクセス

手順

1. 構成 > セキュリティ > *ファイアウォール制御*を選択します。

このページの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"](#)。

2. ファイアウォール コントロールを構成するには、任意のタブを選択します。

これらのタブは任意の順序で使用できます。1 つのタブで設定した内容によって他のタブで実行できる内容が制限されることはありませんが、1 つのタブで行った設定変更によって、他のタブで設定されたポートの動作が変わる場合があります。

特権アドレスリスト

[特権アドレス リスト] タブを使用して、デフォルトで閉じられているポート、または [外部アクセスの管理] タブの設定によって閉じられているポートへのホスト アクセスを許可します。

特権 IP アドレスとサブネットには、デフォルトでは内部グリッド アクセスがありません。また、[特権アドレス一覧] タブで開かれたロード バランサーのエンドポイントと追加のポートには、[外部アクセスの管理] タブでブロックされていてもアクセスできます。



[特権アドレス リスト] タブの設定は、[信頼されていないクライアント ネットワーク] タブの設定を上書きできません。

手順

1. [特権アドレス リスト] タブで、閉じたポートへのアクセスを許可するアドレスまたは IP サブネットを入力します。
2. 必要に応じて、別の IP アドレスまたはサブネットを **CIDR** 表記で追加 を選択して、特権クライアントを追加します。



特権リストに追加するアドレスはできる限り少なくします。

3. 必要に応じて、「特権 IP アドレスにStorageGRID内部ポートへのアクセスを許可する」を選択します。見る "[StorageGRID内部ポート](#)"。



このオプションは、内部サービスに対する一部の保護を削除します。可能であれば無効のままにしておきます。

4. *保存*を選択します。

外部アクセスを管理する

[外部アクセスの管理] タブでポートが閉じられている場合、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 アドレスからポートにアクセスすることはできません。閉じることができるのはデフォルトで開いているポートのみであり、開くことができるのは閉じたポートのみです。



[外部アクセスの管理] タブの設定は、[信頼されていないクライアント ネットワーク] タブの設定を上書きできません。たとえば、ノードが信頼されていない場合、ポート SSH/22 は [外部アクセスの管理] タブで開いている場合でも、クライアント ネットワーク上でブロックされます。[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. *外部アクセスの管理*を選択します。タブには、グリッド内のノードのすべての外部ポート (デフォルトでは非グリッド ノードからアクセス可能なポート) を含むテーブルが表示されます。
2. 次のオプションを使用して、開くポートと閉じるポートを構成します。
 - 各ポートの横にあるトグルを使用して、選択したポートを開いたり閉じたりします。
 - 表にリストされているすべてのポートを開くには、「表示されているすべてのポートを開く」を選択します。
 - 表にリストされているすべてのポートを閉じるには、「表示されているすべてのポートを閉じる」を選択します。



Grid Manager ポート 443 または 8443 を閉じると、ブロックされたポートに現在接続しているすべてのユーザー (自分を含む) は、その IP アドレスが特権アドレス リストに追加されていない限り、Grid Manager にアクセスできなくなります。



利用可能なすべてのポートが表示されていることを確認するには、表の右側にあるスクロールバーを使用します。検索フィールドにポート番号を入力して、任意の外部ポートの設定を検索します。ポート番号の一部を入力できます。たとえば、「2」と入力すると、名前の一部に文字列「2」が含まれるすべてのポートが表示されます。

3. *保存*を選択

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 バランサのエンドポイントとして構成されたポートと、オプションでこのタブで選択した追加のポート上の受信トラフィックのみを受け入れます。このタブを使用して、拡張で追加された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 バランサのエンドポイントが構成されていない場合、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 タブで行った構成の変更は、外部アクセスの管理 タブの設定を上書きします。

手順

1. *信頼されていないクライアントネットワーク*を選択します。
2. [新しいノードのデフォルトの設定] セクションでは、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されます。
- 信頼されていない: 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されなくなります。

必要に応じて、このタブに戻って特定の新しいノードの設定を変更できます。



この設定は、StorageGRIDシステム内の既存のノードには影響しません。

3. 明示的に構成されたロード バランサ 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するには、次のオプションを使用します。

- *表示されているノードを信頼しない*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できないクライアント ネットワーク 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、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 リストから削除されます。
- 各ノードの横にあるトグルを使用して、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なしに設定します。

たとえば、「表示されているノードを信頼しない」を選択して、すべてのノードを信頼できないクライアント ネットワーク リストに追加し、個々のノードの横にあるトグルを使用して、その単一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。



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するには、テーブルの右側にあるスクロールバーを使用します。検索フィールドにノード名を入力して、任意のノードの設定を検索します。名前の一部を入力できます。たとえば、**GW** と入力すると、名前の一部に文字列「GW」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すぐに適用され、強制されます。ロード バランサのエンドポイントが構成されていない場合、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

テナント アカウントとは何ですか？

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



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

グリッド管理者は、S3 クライアントがオブジェクトの保存と取得に使用するテナント アカウントを作成および管理します。

各テナント アカウントには、フェデレーション グループまたはローカル グループ、ユーザー、S3 バケット、オブジェクトがあります。

テナント アカウントを使用すると、保存されたオブジェクトを異なるエンティティごとに分離できます。たとえば、次のいずれかのユースケースでは複数のテナント アカウントを使用できます。

- エンタープライズの使用例: エンタープライズ アプリケーションでStorageGRIDシステムを管理している場合、組織内のさまざまな部門ごとにグリッドのオブジェクト ストレージを分離する必要がある場合があります。この場合、マーケティング部門、カスタマー サポート部門、人事部門などのテナント アカウントを作成できます。



S3 クライアント プロトコルを使用する場合は、S3 バケットとバケット ポリシーを使用して、企業内の部門間でオブジェクトを分離できます。テナント アカウントを使用する必要はありません。実装手順を参照["S3 バケットとバケットポリシー"](#)詳細についてはこちらをご覧ください。

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

詳細については、以下を参照してください。 ["テナントアカウントを使用する"](#)。

テナント アカウントを作成するにはどうすればよいですか？

グリッド マネージャーを使用してテナント アカウントを作成します。テナント アカウントを作成するときは、次の情報を指定します。

- テナント名、クライアント タイプ (S3)、オプションのストレージ クォータなどの基本情報。
- テナント アカウントの権限 (テナント アカウントが S3 プラットフォーム サービスを使用できるかどうか、独自の ID ソースを設定できるかどうか、S3 Select を使用できるかどうか、グリッド フェデレーション接続を使用できるかどうかなど)。
- StorageGRIDシステムがローカル グループとユーザー、ID フェデレーション、またはシングル サインオン (SSO) を使用するかどうかに基づく、テナントの初期ルート アクセス。

さらに、S3 テナント アカウントが規制要件に準拠する必要がある場合は、StorageGRIDシステムの S3 オブジェクト ロック設定を有効にできます。S3 オブジェクト ロックを有効にすると、すべての S3 テナント アカウントが準拠バケットを作成および管理できるようになります。

Tenant Manager は何に使用されますか？

テナント アカウントを作成すると、テナント ユーザーはテナント マネージャーにサインインして次のようなタスクを実行できます。

- アイデンティティ フェデレーションを設定する (アイデンティティ ソースがグリッドと共有されていない場合)
- グループとユーザーの管理
- アカウントのクローンとクロスグリッドレプリケーションにグリッドフェデレーションを使用する
- S3 アクセスキーを管理する
- S3バケットの作成と管理
- S3プラットフォームサービスを使用する
- S3 Selectを使用する
- ストレージ使用量を監視する



S3 テナント ユーザーは、Tenant Manager を使用して S3 アクセス キーとバケットを作成および管理できますが、オブジェクトの取り込みと管理には S3 クライアント アプリケーションを使用する必要があります。見る["S3 REST APIを使用する"](#)詳細については。

テナントアカウントを作成する

StorageGRIDシステム内のストレージへのアクセスを制御するには、少なくとも 1 つのテナント アカウントを作成する必要があります。

テナントアカウントを作成する手順は、["アイデンティティフェデレーション"](#)そして["シングルサインオン"](#)が構成されているかどうか、およびテナント アカウントの作成に使用する Grid Manager アカウントが、ルートアクセス権限を持つ管理者グループに属しているかどうかを確認します。

開始する前に

- グリッドマネージャにサインインするには、["サポートされているウェブブラウザ"](#)。
- あなたは["ルートアクセスまたはテナントアカウントの権限"](#)。
- テナント アカウントが Grid Manager 用に構成されたアイデンティティ ソースを使用し、テナント アカウントのルート アクセス権限をフェデレーション グループに付与する場合は、そのフェデレーション グループを Grid Manager にインポートしておきます。この管理者グループに Grid Manager 権限を割り当て

る必要はありません。見る["管理者グループの管理"](#)。

- S3 テナントがグリッド フェデレーション接続を使用してアカウント データを複製し、バケット オブジェクトを別のグリッドに複製できるようにする場合:
 - あなたが持っている["グリッドフェデレーション接続を構成しました"](#)。
 - 接続のステータスは*接続済み*です。
 - ルートアクセス権限があります。
 - 検討事項を確認しました["グリッドフェデレーションの許可されたテナントの管理"](#)。
 - テナント アカウントが Grid Manager 用に構成された ID ソースを使用する場合は、両方のグリッドの Grid Manager に同じフェデレーション グループをインポートしたことになります。

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



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

ウィザードにアクセスする

手順

1. *TENANTS*を選択します。
2. *作成*を選択します。

詳細を入力してください

手順

1. テナントの詳細を入力します。

フィールド	説明
Name	テナント アカウントの名前。テナント名は一意である必要はありません。テナント アカウントが作成されると、一意の 20 桁のアカウント ID が割り当てられます。
説明（オプション）	テナントを識別するのに役立つ説明。 グリッド フェデレーション接続を使用するテナントを作成する場合は、オプションでこのフィールドを使用して、ソース テナントと宛先テナントを識別します。たとえば、グリッド 1 で作成されたテナントのこの説明は、グリッド 2 に複製されたテナントにも表示されます: 「このテナントはグリッド 1 で作成されました。」

フィールド	説明
クライアントタイプ	このテナントが使用するクライアント プロトコルのタイプ (S3 または Swift)。 注: Swift クライアント アプリケーションのサポートは非推奨となっており、将来のリリースでは削除される予定です。
ストレージクォータ (オプション)	このテナントにストレージ クォータを設定する場合は、クォータの数値と単位を指定します。

2. *続行*を選択します。

権限の選択

手順

1. 必要に応じて、このテナントに付与する基本的な権限を選択します。



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

許可	選択した場合...
プラットフォームサービスを許可する	テナントは CloudMirror などの S3 プラットフォーム サービスを使用できます。見る "S3テナントアカウントのプラットフォームサービスを管理する" 。
独自のIDソースを使用する	テナントは、フェデレーション グループおよびユーザーに対して独自の ID ソースを構成および管理できます。このオプションは、 "設定されたSSO" StorageGRIDシステム用。
S3 選択を許可する	テナントは、S3 SelectObjectContent API リクエストを発行して、オブジェクト データをフィルタリングおよび取得できます。見る "テナントアカウントのS3 Selectを管理する" 。 重要: SelectObjectContent リクエストにより、すべての S3 クライアントとすべてのテナントのロードバランサーのパフォーマンスが低下する可能性があります。この機能は、必要な場合にのみ、信頼できるテナントに対してのみ有効にしてください。

2. 必要に応じて、このテナントに付与する高度な権限を選択します。

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

3. *続行*を選択します。

ルートアクセスを定義してテナントを作成する

手順

1. StorageGRIDシステムが ID フェデレーション、シングル サインオン (SSO)、またはその両方を使用するかどうかに基づいて、テナント アカウントのルート アクセスを定義します。

オプション	これをする
アイデンティティ連携が有効になっていない場合	ローカル ルート ユーザーとしてテナントにサインインするときに使用するパスワードを指定します。
アイデンティティ連携が有効になっている場合	a. テナントのルート アクセス権限を付与する既存のフェデレーション グループを選択します。 b. 必要に応じて、ローカル ルート ユーザーとしてテナントにサインインするときに使用するパスワードを指定します。
ID連携とシングルサインオン (SSO) の両方が有効になっている場合	テナントのルート アクセス権限を付与する既存のフェデレーション グループを選択します。ローカル ユーザーはサインインできません。

2. *テナントの作成*を選択します。

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



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

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

- a. 接続内の他のグリッドに同一のテナントが複製されたことを確認します。両方のグリッドのテナントには、同じ 20 桁のアカウント ID、名前、説明、クォータ、および権限が与えられます。



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

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



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

テナントに**Sign in**（オプション）

必要に応じて、今すぐ新しいテナントにサインインして構成を完了することも、後でテナントにサインインすることもできます。サインインの手順は、デフォルト ポート (443) を使用して Grid Manager にサインインしているか、制限されたポートを使用してサインインしているかによって異なります。見る"[外部ファイアウォールでアクセスを制御する](#)"。

今すぐ**Sign in**

...を使用している場合	操作
ポート443でローカルルートユーザーのパスワードを設定する	1. * root としてSign in* を選択します。 サインインすると、バケット、ID フェデレーション、グループ、およびユーザーを構成するためのリンクが表示されます。 2. リンクを選択してテナント アカウントを構成します。 各リンクをクリックすると、テナント マネージャーの対応するページが開きます。ページを完了するには、"テナントアカウントの使用手順"。
ポート443で、ローカルルートユーザーのパスワードを設定していない	*Sign in*を選択し、ルートアクセスフェデレーショングループのユーザーの資格情報を入力します。

...を使用している場合	操作
制限されたポート	1. *完了*を選択 2. このテナント アカウントへのアクセス方法の詳細については、テナント テーブルで 制限 を選択してください。 テナント マネージャーの URL の形式は次のとおりです。 <pre>https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/</pre> ◦ `FQDN_or_Admin_Node_IP` 管理ノードの完全修飾ドメイン名またはIPアドレスです ◦ `port` テナント専用ポートです ◦ `20-digit-account-id` テナントの一意のアカウントIDです

後でSign in

...を使用している場合	これらのいずれかを行ってください...
ポート443	• グリッド マネージャーから [TENANTS] を選択し、テナント名の右側にある [Sign in] を選択します。 • Web ブラウザにテナントの URL を入力します。 <pre>https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/</pre> ◦ `FQDN_or_Admin_Node_IP` 管理ノードの完全修飾ドメイン名またはIPアドレスです ◦ `20-digit-account-id` テナントの一意のアカウントIDです
制限されたポート	• グリッド マネージャーから、TENANTS を選択し、Restricted を選択します。 • Web ブラウザにテナントの URL を入力します。 <pre>https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id</pre> ◦ `FQDN_or_Admin_Node_IP` 管理ノードの完全修飾ドメイン名またはIPアドレスです ◦ `port` テナント専用の制限ポートです ◦ `20-digit-account-id` テナントの一意のアカウントIDです

テナントを構成する

以下の指示に従ってください["テナントアカウントを使用する"](#)テナント グループとユーザー、S3 アクセス キ

一、バケット、プラットフォーム サービス、アカウント クローン、クロス グリッド レプリケーションを管理します。

テナントアカウントの編集

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



テナントに グリッド フェデレーション接続の使用 権限がある場合は、接続内のどちらのグリッドからでもテナントの詳細を編集できます。ただし、接続内の 1 つのグリッドで行った変更は、他のグリッドにコピーされません。グリッド間でテナントの詳細を正確に同期させたい場合は、両方のグリッドで同じ編集を行います。見る["グリッドフェデレーション接続に許可されたテナントを管理する"](#)。

開始する前に

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



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

手順

1. *TENANTS*を選択します。

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 でテナントを検索します。

3. テナントを選択します。次のいずれかを実行できます。

- テナントのチェックボックスを選択し、[アクション] > [編集] を選択します。

- テナント名を選択して詳細ページを表示し、[編集] を選択します。

4. 必要に応じて、次のフィールドの値を変更します。

- 名前
- 説明
- ストレージクォータ

5. *続行*を選択します。

6. テナント アカウントの権限を選択またはクリアします。

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

独自の ID ソースを使用する の場合:

- 無効になっていて選択されている場合、テナントは独自の ID ソースをすでに有効にしています。テナントは、グリッド マネージャー用に構成された ID ソースを使用する前に、その ID ソースを無効にする必要があります。
- 無効で選択されていない場合、StorageGRIDシステムに対して SSO が有効になります。テナントは、グリッド マネージャー用に構成された ID ソースを使用する必要があります。
- 必要に応じて、「**S3** 選択を許可する」権限を選択またはクリアします。見る["テナントアカウントのS3 Selectを管理する"](#)。
- グリッド フェデレーション接続の使用 権限を削除するには:
 - i. グリッド フェデレーション タブを選択します。
 - ii. *権限を削除*を選択します。
- グリッド フェデレーション接続の使用 権限を追加するには:
 - i. グリッド フェデレーション タブを選択します。
 - ii. グリッド フェデレーション接続を使用する チェックボックスを選択します。
 - iii. 必要に応じて、「既存のローカル ユーザーとグループの複製」を選択して、リモート グリッドに複製します。必要に応じて、進行中のクローン作成を停止したり、最後のクローン作成操作が完了した後に一部のローカル ユーザーまたはグループのクローン作成に失敗した場合にクローン作成を再試行したりできます。
- 最大保持期間を設定するか、コンプライアンス モードを許可するには:



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

- i. **S3** オブジェクト ロック タブを選択します。
- ii. *最大保存期間の設定*では、値を入力し、プルダウンから期間を選択します。

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

テナントのローカルルートユーザーのパスワードを変更する

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

開始する前に

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

タスク概要

StorageGRIDシステムでシングル サインオン (SSO) が有効になっている場合、ローカル ルート ユーザーはテナント アカウントにサインインできません。ルート ユーザー タスクを実行するには、ユーザーはテナントに対するルート アクセス権限を持つフェデレーション グループに属している必要があります。

手順

1. *TENANTS*を選択します。

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 ▾	Search tenants by name or ID		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ます。次のいずれかを実行できます。
 - テナントのチェックボックスを選択し、アクション > *ルートパスワードの変更*を選択します。
 - テナントの名前を選択して詳細ページを表示し、アクション > ルート パスワードの変更 を選択します。
3. テナント アカウントの新しいパスワードを入力します。
4. *保存*を選択します。

テナントアカウントを削除する

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

開始する前に

- グリッドマネージャにサインインするには、"[サポートされているウェブブラウザ](#)"。
- あなたが持っている"[特定のアクセス権限](#)"。
- テナント アカウントに関連付けられているすべての S3 バケットとオブジェクトが削除されました。
- テナントがグリッドフェデレーション接続の使用を許可されている場合は、以下の考慮事項を確認しました。"[グリッドフェデレーション接続の使用権限を持つテナントを削除する](#)"。

手順

1. *TENANTS*を選択します。
2. 削除するテナント アカウントを見つけます。

検索ボックスを使用して、名前またはテナント ID でテナントを検索します。

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

プラットフォームサービスの管理

プラットフォームサービスとは何ですか？

プラットフォーム サービスには、CloudMirror レプリケーション、イベント通知、検索統合サービスが含まれます。

S3 テナント アカウントに対してプラットフォーム サービスを有効にする場合は、テナントがこれらのサービスを使用するために必要な外部リソースにアクセスできるようにグリッドを構成する必要があります。

CloudMirrorレプリケーション

StorageGRID CloudMirror レプリケーション サービスは、StorageGRIDバケットから指定された外部宛先に特定のオブジェクトをミラーリングするために使用されます。

たとえば、CloudMirror レプリケーションを使用して特定の顧客レコードを Amazon S3 にミラーリングし、AWS サービスを活用してデータの分析を実行することができます。



CloudMirror レプリケーションには、クロスグリッド レプリケーション機能との重要な類似点と相違点がいくつかあります。詳細については、"[クロスグリッドレプリケーションとCloudMirrorレプリケーションを比較する](#)"。



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

通知

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

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



S3 オブジェクト ロックが有効になっているバケットでイベント通知を設定できますが、オブジェクトの S3 オブジェクト ロック メタデータ (保持期限や法的保留ステータスを含む) は通知メッセージに含まれません。

検索統合サービス

検索統合サービスは、S3 オブジェクト メタデータを指定された Elasticsearch インデックスに送信するために使用され、そこでメタデータは外部サービスを使用して検索または分析できます。

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



S3 オブジェクト ロックが有効になっているバケットで Elasticsearch 統合を設定できますが、オブジェクトの S3 オブジェクト ロック メタデータ (保持期限や法的保留ステータスを含む) は通知メッセージに含まれません。

プラットフォーム サービスにより、テナントは外部ストレージ リソース、通知サービス、およびデータを使用した検索や分析サービスを使用できるようになります。プラットフォーム サービスのターゲットの場所は通常、StorageGRID展開の外部にあるため、テナントにこれらのサービスの使用を許可するかどうかを決定する必要があります。その場合は、テナント アカウントを作成または編集するときに、プラットフォーム サービスの使用を有効にする必要があります。また、テナントが生成するプラットフォーム サービス メッセージが宛先に届くようにネットワークを構成する必要があります。

プラットフォームサービスの利用に関する推奨事項

プラットフォーム サービスを使用する前に、次の推奨事項に注意してください。

- StorageGRIDシステム内の S3 バケットでバージョン管理と CloudMirror レプリケーションの両方が有効になっている場合は、宛先エンドポイントの S3 バケットのバージョン管理も有効にする必要があります。これにより、CloudMirror レプリケーションはエンドポイントで同様のオブジェクト バージョンを生成できるようになります。
- CloudMirror レプリケーション、通知、および検索統合を必要とする S3 リクエストでは、100 を超えるアクティブテナントを使用しないでください。アクティブなテナントが 100 を超えると、S3 クライアントのパフォーマンスが低下する可能性があります。
- 完了できないエンドポイントへのリクエストは、最大 500,000 件のリクエストまでキューに入れられます。この制限はアクティブなテナント間で均等に共有されます。新しく作成されたテナントが不当に罰せられないように、新しいテナントはこの 500,000 の制限を一時的に超えることが許可されます。

関連情報

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

プラットフォームサービス用のネットワークとポート

S3 テナントにプラットフォーム サービスの使用を許可する場合は、プラットフォーム サービス メッセージが宛先に配信されるようにグリッドのネットワークを構成する必要があります。

テナント アカウントを作成または更新するときに、S3 テナント アカウントのプラットフォーム サービスを有効にできます。プラットフォーム サービスが有効になっている場合、テナントは、S3 バケットからの CloudMirror レプリケーション、イベント通知、または検索統合メッセージの送信先として機能するエンドポイントを作成できます。これらのプラットフォーム サービス メッセージは、ADC サービスを実行するストレージ ノードから宛先エンドポイントに送信されます。

たとえば、テナントは次のタイプの宛先エンドポイントを構成する場合があります。

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

プラットフォーム サービス メッセージが確実に配信されるようにするには、ADC ストレージ ノードを含むネットワークを構成する必要があります。プラットフォーム サービス メッセージを宛先エンドポイントに送信するには、次のポートを使用できることを確認する必要があります。

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

- **80:** httpで始まるエンドポイントURI（ほとんどのエンドポイント）
- **443:** httpsで始まるエンドポイントURI（ほとんどのエンドポイント）
- **9092:** http または https で始まるエンドポイント URI の場合 (Kafka エンドポイントのみ)

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



StorageGRIDデプロイメントを CloudMirror レプリケーションの宛先として使用すると、レプリケーション メッセージが 80 または 443 以外のポートで受信される可能性があります。宛先StorageGRIDデプロイメントによって S3 に使用されているポートがエンドポイントで指定されていることを確認します。

非透過プロキシサーバーを使用する場合は、["ストレージプロキシ設定を構成する"](#)インターネット上のエンドポイントなどの外部エンドポイントにメッセージを送信できるようにします。

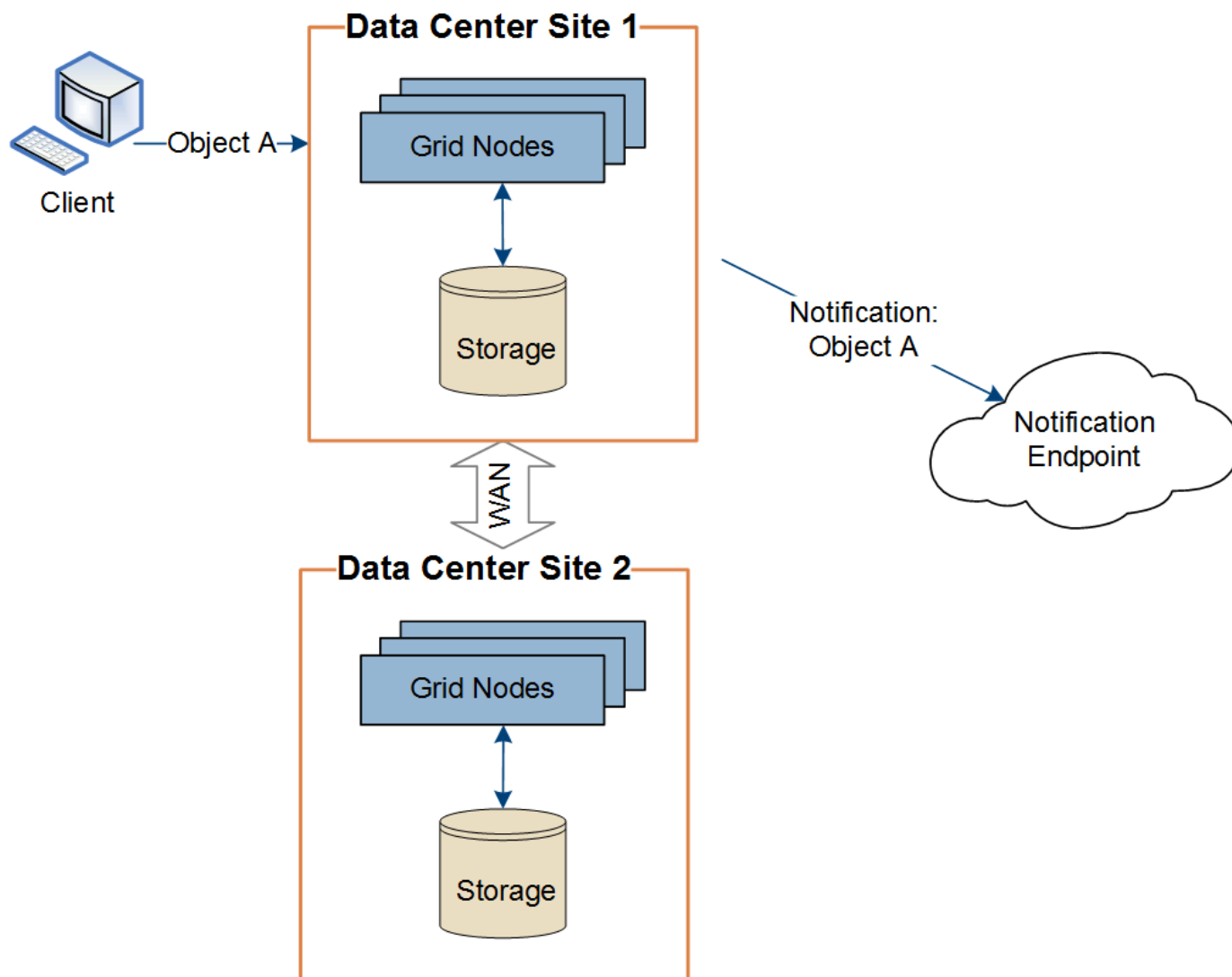
関連情報

["テナントアカウントを使用する"](#)

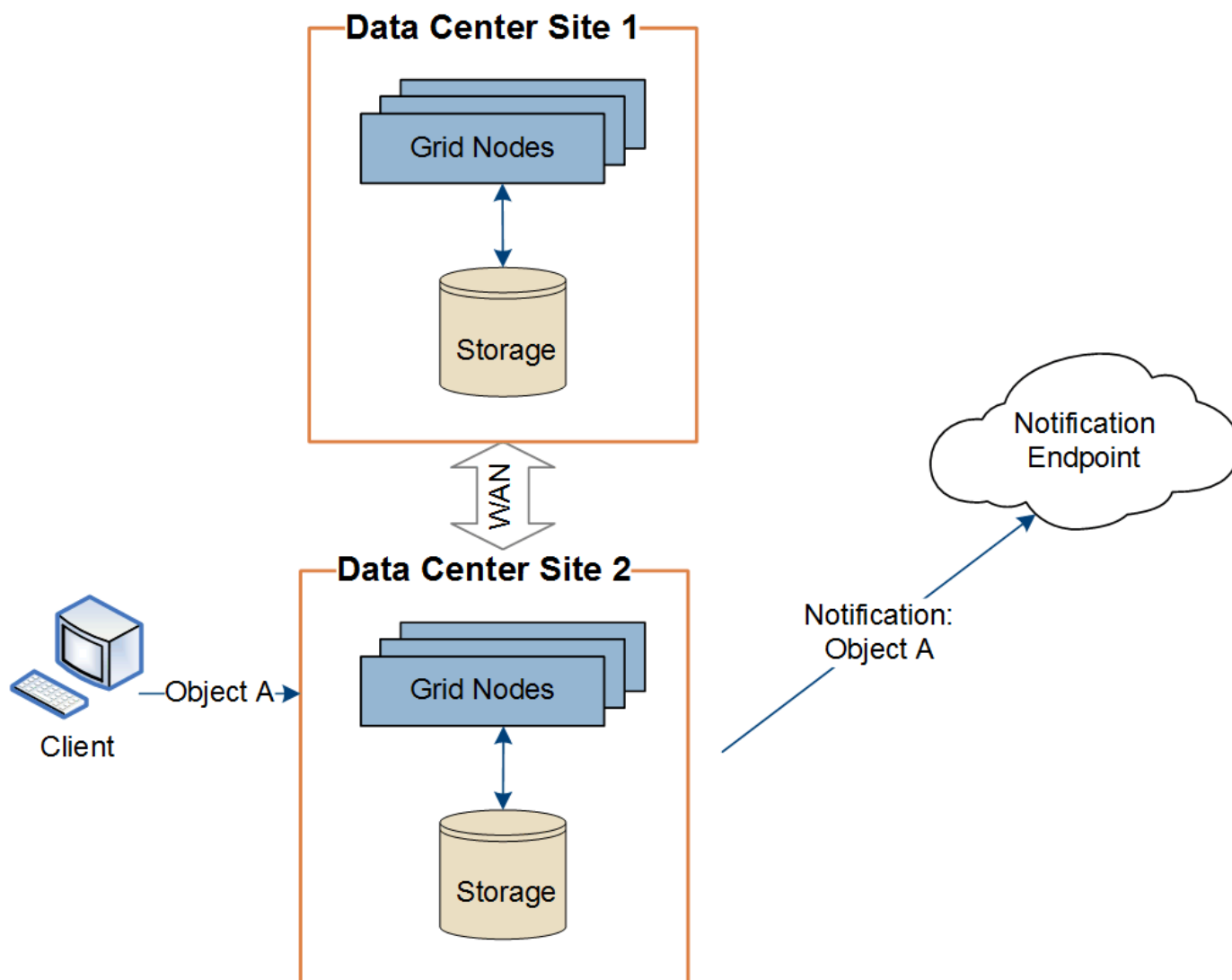
プラットフォームサービスメッセージのサイトごとの配信

すべてのプラットフォーム サービス操作はサイトごとに実行されます。

つまり、テナントがクライアントを使用してデータセンター サイト 1 のゲートウェイ ノードに接続し、オブジェクトに対して S3 API 作成操作を実行すると、そのアクションに関する通知がトリガーされ、データセンター サイト 1 から送信されます。



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



各サイトのネットワークが、プラットフォーム サービス メッセージが宛先に配信されるように構成されていることを確認します。

プラットフォームサービスのトラブルシューティング

プラットフォーム サービスで使用するエンドポイントは、テナント マネージャでテナント ユーザーによって作成および管理されます。ただし、テナントでプラットフォーム サービスの構成または使用に関する問題が発生した場合、グリッド マネージャを使用して問題を解決できる可能性があります。

新しいエンドポイントの問題

テナントがプラットフォーム サービスを使用するには、テナント マネージャを使用して 1 つ以上のエンドポイントを作成する必要があります。各エンドポイントは、StorageGRID S3 バケット、Amazon Web Services バケット、Amazon Simple Notification Service トピック、Kafka トピック、ローカルまたは AWS でホストされている Elasticsearch クラスタなど、1 つのプラットフォーム サービスの外部宛先を表します。各エンドポイントには、外部リソースの場所と、そのリソースにアクセスするために必要な資格情報の両方が含まれます。

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

格情報を使用してアクセスできることを検証します。エンドポイントへの接続は、各サイトの 1 つのノードから検証されます。

エンドポイントの検証に失敗した場合、エンドポイントの検証が失敗した理由を説明するエラーメッセージが表示されます。テナント ユーザーは問題を解決してから、エンドポイントの作成を再度試みる必要があります。



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

既存のエンドポイントの問題

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



One or more endpoints have experienced an error and might not be functioning properly. Go to the [Endpoints](#) page to view the error details. The last error occurred 2 hours ago.

テナント ユーザーは、[エンドポイント] ページにアクセスして、各エンドポイントの最新のエラーメッセージを確認し、エラーが発生した時期を確認できます。最後のエラー 列には、各エンドポイントの最新のエラーメッセージが表示され、エラーが発生した時刻が示されます。エラーには、 アイコンは過去 7 日以内に発生しました。

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



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

プロキシサーバーに関連する問題

設定した場合"**ストレージプロキシ**"ストレージノードとプラットフォーム サービス エンドポイント間で、プロキシ サービスがStorageGRIDからのメッセージを許可しない場合はエラーが発生する可能性があります。これらの問題を解決するには、プロキシ サーバーの設定を確認し、プラットフォーム サービス関連のメッセージがブロックされていないことを確認します。

エラーが発生したかどうかを確認する

過去 7 日以内にエンドポイント エラーが発生した場合、テナント マネージャーのダッシュボードに警告メッセージが表示されます。エラーの詳細を確認するには、「エンドポイント」ページにアクセスしてください。

クライアント操作が失敗する

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

サービスのステータスを確認するには:

1. サポート > ツール > グリッド トポロジ を選択します。
2. **site > Storage Node > SSM > Services** を選択します。

回復可能なエンドポイント エラーと回復不可能なエンドポイント エラー

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

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

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

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

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

- グリッド マネージャーで、サポート > ツール > メトリック > **Grafana** > プラットフォーム サービスの概要 に移動して、エラーの詳細を表示します。
- テナント マネージャーで、ストレージ (**S3**) > プラットフォーム サービス エンドポイント に移動して、エラーの詳細を表示します。
- チェックしてください `/var/local/log/bicast-err.log` 関連するエラーについて。ADC サービスを持つスト

レージ ノードには、このログ ファイルが含まれます。

プラットフォームサービスメッセージを配信できません

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

関連するアラートを確認します。

プラットフォームサービスリクエストのパフォーマンスが低下

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

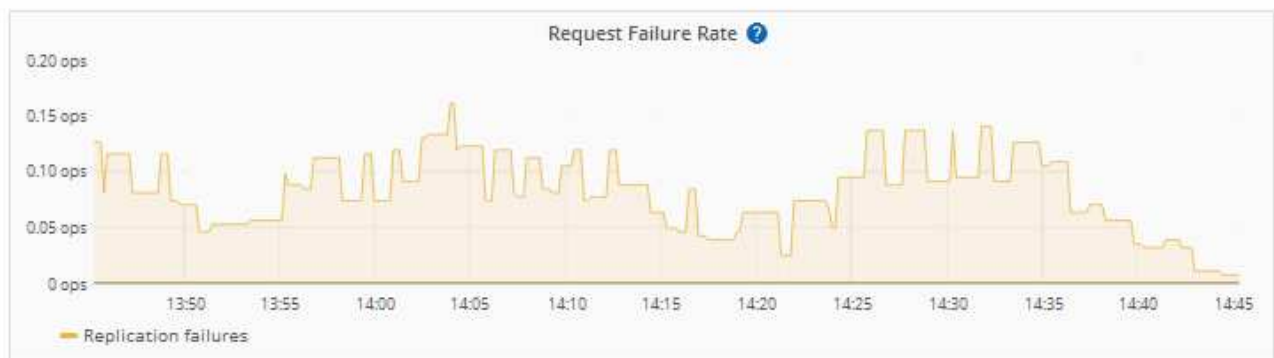
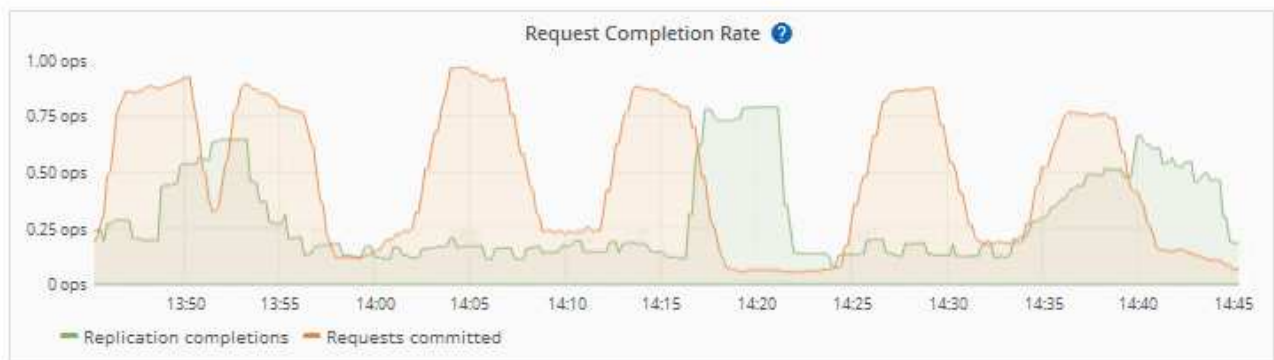
目に見える唯一の影響は、受信する S3 リクエストの実行に時間がかかるようになることです。パフォーマンスが大幅に低下していることが検出された場合は、取り込み速度を下げるか、容量の大きいエンドポイントを使用する必要があります。リクエストのバックログが増え続けると、クライアントの S3 操作 (PUT リクエストなど) は最終的に失敗します。

CloudMirror リクエストは、通常、検索統合リクエストやイベント通知リクエストよりも多くのデータ転送を伴うため、宛先エンドポイントのパフォーマンスの影響を受ける可能性が高くなります。

プラットフォームサービスリクエストが失敗する

プラットフォーム サービスのリクエスト失敗率を表示するには:

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

[1 hour](#) [1 day](#) [1 week](#) [1 month](#) [Custom](#)

プラットフォームサービス利用不可の警告

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

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

このアラートを解決するには、サイトのどのストレージ ノードに RSM サービスが含まれているかを確認します。(RSM サービスは、ADC サービスも含まれるストレージ ノード上に存在します。)次に、それらのストレージ ノードの過半数が実行中であり、利用可能であることを確認します。



サイトで RSM サービスを含む複数のストレージ ノードに障害が発生した場合、そのサイトの保留中のプラットフォーム サービス要求はすべて失われます。

プラットフォーム サービス エンドポイントに関する追加のトラブルシューティング ガイダンス

詳細については、[テナント アカウントの使用](#)、[プラットフォーム サービス エンドポイントのトラブルシューティング](#)。

関連情報

["StorageGRIDシステムのトラブルシューティング"](#)

テナントアカウントのS3 Selectを管理する

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

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

S3 Select とは何ですか？

S3 Select を使用すると、S3 クライアントは SelectObjectContent リクエストを使用して、オブジェクトから必要なデータのみをフィルタリングして取得できます。S3 Select のStorageGRID実装には、S3 Select コマンドと機能のサブセットが含まれています。

S3 Select の使用に関する考慮事項と要件

グリッド管理要件

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

オブジェクト形式の要件

クエリするオブジェクトは、次のいずれかの形式である必要があります。

- **CSV**。そのまま使用することも、GZIP または BZIP2 アーカイブに圧縮することもできます。
- 寄木細工。Parquet オブジェクトの追加要件:
 - S3 Select は、GZIP または Snappy を使用した列指向の圧縮のみをサポートします。S3 Select は、Parquet オブジェクトのオブジェクト全体の圧縮をサポートしていません。
 - S3 Select は Parquet 出力をサポートしていません。出力形式を CSV または JSON として指定する必要があります。
 - 圧縮されていない行グループの最大サイズは 512 MB です。
 - オブジェクトのスキーマで指定されたデータ型を使用する必要があります。
 - INTERVAL、JSON、LIST、TIME、または UUID 論理型は使用できません。

エンドポイント要件

SelectObjectContent リクエストは、"[StorageGRID ロードバランサ エンドポイント](#)"。

エンドポイントで使用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 リクエストにより、すべての S3 クライアントとすべてのテナントのロードバランサーのパフォーマンスが低下する可能性があります。この機能は、必要な場合にのみ、信頼できるテナントに対してのみ有効にしてください。

参照 "[S3 Select の使用手順](#)"。

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

クライアント接続を構成する

S3 クライアント接続を構成する

グリッド管理者は、S3 クライアント アプリケーションが StorageGRID システムに接続してデータを保存および取得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 Swift の詳細は削除されました。見る "[StorageGRID 11.8: S3 および Swift クライアント接続の設定](#)"。

構成タスク

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 で前提条件となるタスクを実行します。

必要なタスク

以下のものを取得する必要があります:

- IPアドレス
- ドメイン名
- SSL証明書

オプションタスク

オプションで、以下を設定します。

- アイデンティティ連携
- 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構成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います。

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構成する

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。DNS エントリを作成し、使用する予定のドメイン名に IP アドレスを関連付けます。

必要に応じて、追加のアプリケーションセットアップを実行します。

2. アプリケーションとStorageGRIDで継続的なタスクを実行し、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、特定の値を取得する必要があります。

どのような値が必要ですか？

次の表は、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 サーバーによって使用される場所を示しています。

Value	値が設定される場所	価値が使われる場所
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

これらの値を取得するにはどうすればいいでしょうか？

要件に応じて、次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"**。S3 セットアップ ウィザードを使用すると、StorageGRIDで必要な値を簡単に構成でき、S3 アプリケーションを構成するときに使用できる 1 つまたは 2 つのファイルを出力できます。ウィザードは必要な手順をガイドし、設定がStorageGRID のベスト プラクティスに準拠していることを確認できるようにします。



S3 アプリケーションを構成する場合は、特別な要件があることがわかっている場合や実装に大幅なカスタマイズが必要になる場合を除き、S3 セットアップ ウィザードを使用することをお勧めします。

- **"FabricPoolセットアップ ウィザード"**。S3 セットアップ ウィザードと同様に、FabricPoolセットアップ ウィザードを使用すると、必要な値をすばやく設定し、ONTAPでFabricPoolクラウド層を設定するときに使用できるファイルを出力できます。



StorageGRID をFabricPoolクラウド層のオブジェクト ストレージ システムとして使用することを計画している場合は、特別な要件があることがわかっている場合や実装に大幅なカスタマイズが必要であることがない限り、FabricPoolセットアップ ウィザードを使用することをお勧めします。

- 項目を手動で設定します。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、手動で構成を実行して必要な値を取得できます。次の手順を実行します。
 - a. S3 アプリケーションに使用する高可用性 (HA) グループを構成します。見る["高可用性グループを構成する"](#)。
 - b. S3 アプリケーションが使用するロードバランサーエンドポイントを作成します。見る["ロードバランサのエンドポイントを構成する"](#)。

- 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。見る["テナントアカウントを作成する"](#)。
- 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のアクセス キー ID とシークレット アクセス キーを生成します。見る["独自のアクセスキーを作成する"](#)。
- 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"](#)。
- 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 ポリシーをアクティブ化します。見る["ILMルールを作成する"](#)そして["ILMポリシーを作成する"](#)。

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オブジェクト データをStorageGRIDに保存します。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する必要があります。

まとめ

次のリストは、S3 REST API の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

バケットの所有権と適用可能な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仕組み

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 サービスに接続するか、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、接続方法に応じてHTTPSまたはHTTPを使用できます。["ロードバランサのエンドポイントを構成する"](#)。

HTTPS は安全な TLS 暗号化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 は安全性が低く、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 グリッドにのみ使用する必要があります。

- 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 も使用できます。

HTTPS がデフォルトであり、推奨されます。

HTTPは安全性が低く、暗号化されていない通信を提供しますが、オプションで"[有効](#)"非本番環境またはテスト グリッド用。

- 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 エンドポイントが HTTP 接続または HTTPS 接続を受け入れるように構成されているかどうかに関係なく、グリッド内のロード バランサ サービスとストレージ ノード間の通信は暗号化されます。
- クライアントは以下を提供する必要があります"[HTTP認証ヘッダー](#)"REST API 操作を実行するためにStorageGRIDを使用します。

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を使用して TLS 接続を行うことができます。

- クライアント アプリケーションが Load Balancer サービスに接続すると、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が使用されます。各ロード バランサ エンドポイントには独自の証明書（グリッド管理者がアップロードしたカスタム サーバ証明書、またはエンドポイントの構成時にグリッド管理者がStorageGRIDで生成した証明書）があります。

見る"[負荷分散に関する考慮事項](#)"。

- 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サーバ証明書 (システム証明機関によって署名されている)、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 サーバ証明書のいずれかを使用します。見る"[カスタムS3 API証明書を追加する](#)"。

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証明機関を信頼するように構成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ときに使用できる暗号スイートのセットをサポートしています。暗号を構成するには、構成 > 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 と 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

S3 セットアップウィザードの使用: 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場合

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にStorageGRIDを構成する各手順をガイドします。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。ウィザードを使用すると、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できます。

もしあなたが["ルートアクセス権限"](#)StorageGRID Grid Manager の使用を開始するときに S3 セットアップ ウィザードを完了することも、後でいつでもウィザードにアクセスして完了することもできます。要件に応じて、必要な項目の一部またはすべてを手動で設定し、ウィザードを使用して S3 アプリケーション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、これらの前提条件が満たされ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は、S3 アプリケーションが接続するノードと、使用されるStorageGRIDネットワークがわかります。また、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もわかっています。

仮想 LAN を使用して S3 アプリケーションからのトラフィックを分離する予定の場合は、VLAN インターフェイスはすでに構成されています。見る["VLANインターフェースを構成する"](#)。

ID連携とSSOを構成する

StorageGRIDシステムで ID フェデレーションまたはシングル サインオン (SSO) を使用する予定の場合は、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 アカウントのルート アクセス権を持つフェデレーショングループも把握しています。見る["アイデンティティフェデレーションを使用する"](#)そして["シングルサインオンを構成する"](#)。

ドメイン名の取得と設定

StorageGRIDに使用する完全修飾ドメイン名 (FQDN) がわかっていること。ドメイン ネーム サーバー (DNS) エントリは、この FQDN を、ウィザードを使用して作成する HA グループの仮想 IP (VIP) アドレスにマッピングします。

S3仮想ホスト形式のリクエストを使用する予定の場合は、["設定されたS3エンドポイントドメイン名"](#)。仮想ホスト形式のリクエストを使用することをお勧めします。

ロードバランサとセキュリティ証明書の要件を確認する

StorageGRIDロード バランサを使用する予定の場合は、ロード バランシングに関する一般的な考慮事項を確認しておきます。アップロードする証明書、または証明書を生成するために必要な値があります。

外部 (サードパーティ) ロード バランサー エンドポイントを使用する予定の場合は、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 テナントがグリッド フェデレーション接続を使用してアカウント データを複製し、バケット オブジェクトを別のグリッドに複製できるようにする場合は、ウィザードを開始する前に次の点を確認してください。

- あなたが持っている["グリッドフェデレーション接続を構成しました"](#)。
- 接続のステータスは*接続済み*です。

- ルートアクセス権限があります。

S3 セットアップウィザードにアクセスして完了する

S3 セットアップ ウィザードを使用して、StorageGRID をS3 アプリケーションで使用するように構成できます。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。

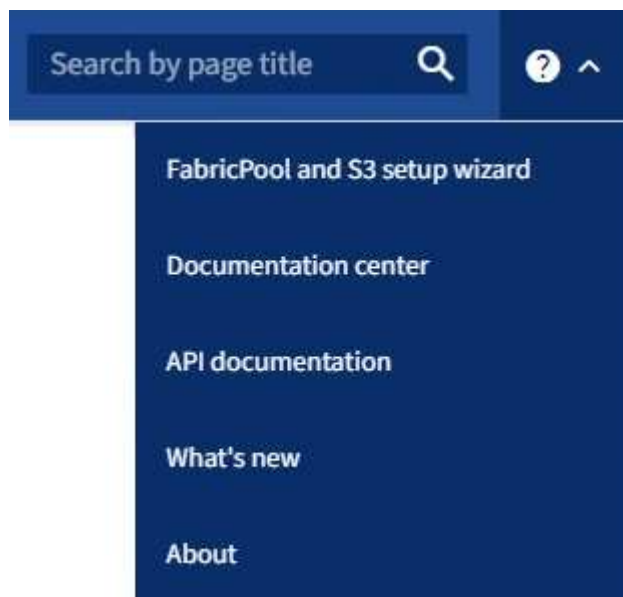
開始する前に

- あなたは["ルートアクセス権限"](#)。
- あなたは、["考慮事項と要件"](#)ウィザードを使用するためのものです。

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Sign inには、["サポートされているウェブブラウザ"](#)。
2. ダッシュボードに * FabricPoolおよび S3 セットアップ ウィザード* バナーが表示された場合は、バナー内のリンクを選択します。バナーが表示されなくなった場合は、グリッド マネージャーのヘッダー 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* を選択します。



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、[今すぐ構成] を選択します。

ステップ 1/6: HA グループを構成する

HA グループは、それぞれにStorageGRID Load Balancer サービスが含まれるノードの集合です。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と、S3 データ接続を利用可能な状態に保つことができます。HA グループ内のアクティブ インターフェイスに障害が発生した場合、バックアップ インターフェイスが S3 操作にほとんど影響を与えずにワークロードを管理できます。

このタスクの詳細については、"[高可用性グループの管理](#)"。

手順

1. 外部ロードバランサーを使用する予定の場合は、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: ロードバランサーのエンドポイントを構成する](#)。
2. StorageGRIDロード バランサを使用するには、新しい HA グループを作成するか、既存の HA グループを使用することができます。

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*手順では、次のフィールドに入力します。

フィールド	説明
HAグループ名	この HA グループの一意の表示名。
説明（オプション）	この HA グループの説明。

- c. *インターフェースの追加*手順では、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速く見つけます。

1 つ以上のノードを選択できますが、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*手順では、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。障害が発生しない限り、プライマリ インターフェースはアクティブ インターフェースになります。

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 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の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、これが繰り返されます。障害が解決されると、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、次のフィールドに入力します。

フィールド	説明
サブネットCIDR	CIDR 表記の 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の長さ (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：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される 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 アドレスを入力します。ローカル ゲートウェイ IP アドレスは VIP サブネット内にある必要があります。

フィールド	説明
仮想IPアドレス	HA グループ内のアクティブ インターフェイスに、少なくとも 1 個、最大 10 個の VIP アドレスを入力します。すべての VIP アドレスは VIP サブネット内にある必要があります。 少なくとも 1 つのアドレスは IPv4 である必要があります。必要に応じて、追加の IPv4 および 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、ロードバランサーのステップに進みます。

既存の**HA**グループを使用する

a. 既存の HA グループを使用するには、「**HA** グループの選択」から HA グループ名を選択します。

b. *続行*を選択して、ロードバランサーのステップに進みます。

ステップ **2/6**: ロードバランサーのエンドポイントを構成する

StorageGRID はロード バランサを使用してクライアント アプリケーションからのワークロードを管理します。負荷分散により、複数のストレージ ノード間の速度と接続容量が最大化されます。

すべてのゲートウェイおよび管理ノードに存在するStorageGRIDロード バランサ サービスを使用することも、外部 (サードパーティ) ロード バランサに接続することもできます。StorageGRIDロード バランサの使用をお勧めします。

このタスクの詳細については、"[負荷分散に関する考慮事項](#)"。

StorageGRIDロード バランサ サービスを使用するには、* StorageGRIDロード バランサ* タブを選択し、使用するロード バランサ エンドポイントを作成または選択します。外部ロード バランサを使用するには、[外部ロード バランサ] タブを選択し、すでに構成したシステムの詳細を入力します。

エンドポイントを作成する

手順

1. ロード バランサー 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 ステップで、次のフィールドに入力します。

フィールド	説明
Name	エンドポイントの説明的な名前。
ポート	負荷分散に使用するStorageGRIDポート。このフィールドは、最初に作成するエンドポイントに対してデフォルトで 10433 に設定されますが、未使用の外部ポートを入力できます。80 または 443 を入力すると、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 ノードでのみ構成されます。 注意: 他のグリッド サービスで使用するポートは許可されません。参照 "ネットワークポートリファレンス" 。
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 暗号化なしでのStorageGRIDとの通信はサポートされていますが、推奨されません。

3. 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、任意の IP アドレスまたは特定の IP アドレスとネットワーク インターフェイスを使用してエンドポイントにアクセスする方法を制御します。

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のアクセシビリティを制限する必要がない限り、*グローバル*設定 (デフォルト) を使用します。
HAグループの仮想IP	クライアント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 モードのエンドポイントは、エンドポイントに選択した HA グループが重複していない限り、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イス	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 インターフェイスの IP アドレス (または対応する FQDN) を使用する必要があります。
ノード タイプ	選択したノードのタイプに基づいて、クライアントは、このエンドポイントにアクセスするために、任意の管理ノードの IP アドレス (または対応する FQDN) または任意のゲートウェイ ノードの IP アドレス (または対応する FQDN) を使用する必要があります。

4. テナント アクセス ステップでは、次のいずれかを選択します。

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。
選択し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	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*ステップでは、次のいずれかを選択します。

フィールド	説明
証明書をアップロードする (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、証明書の秘密キー、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。見る" ロードバランサのエンドポイントを構成する "入力内容の詳細については、こちらをご覧ください。
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ている場合にのみ使用してください。見る" S3 API証明書を設定する "詳細については、

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最大 15 分かかる場合があります。

既存のロードバランサエンドポイントを使用する

手順

1. 既存のエンドポイントを使用するには、「ロードバランサー 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ステップに進みます。

外部ロードバランサを使用する

手順

1. 外部ロードバランサーを使用するには、次のフィールドに入力します。

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サーに接続するために使用するポート番号。
Certificate	外部ロードバランサー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ます。

2. *続行*を選択して、テナントとバケットの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。各テナントには、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があります。

バケットは、テナントのオブジェクトとオブジェクト メタデータを保存するために使用されるコンテナです。テナントには多くのバケットが存在する可能性があります。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、テナント マネージャーを使用できます。

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"](#)そして["S3バケットを作成する"](#)。

手順

1. テナント アカウントの名前を入力します。

テナント名は一意である必要はありません。テナント アカウントが作成されると、一意の数値アカウント ID が割り当てられます。

2. StorageGRIDシステムが使用するかどうかに基づいて、テナントアカウントのルートアクセスを定義します。["アイデンティティフェデレーション"](#)、["シングルサインオン \(SSO\)"](#)、またはその両方。

オプション	これをする
アイデンティティ連携が有効になっていない場合	ローカル ルート ユーザーとしてテナントにサインインするときに使用するパスワードを指定します。

オプション	これをする
アイデンティティ連携が有効になっている場合	a. 既存のフェデレーショングループを選択して" ルートアクセス権限 "テナントのために。 b. 必要に応じて、ローカル ルート ユーザーとしてテナントにサインインするときに使用するパスワードを指定します。
ID連携とシングルサインオン (SSO) の両方が有効になっている場合	既存のフェデレーショングループを選択して" ルートアクセス権限 "テナントのために。ローカル ユーザーはサインインできません。

- ウィザードでルート ユーザーのアクセス キー ID とシークレット アクセス キーを作成する場合は、[ルート ユーザーの S3 アクセス キーを自動的に作成する] を選択します。

テナントの唯一のユーザーがルート ユーザーである場合は、このオプションを選択します。他のユーザーがこのテナントを使用する場合、"**テナントマネージャーを使用する**"キーと権限を設定します。

- 今すぐこのテナントのバケットを作成する場合は、「このテナントのバケットを作成」を選択します。



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たバケットでは S3 オブジェクト ロックは有効になりません。この S3 アプリケーションに S3 オブジェクトロック バケットを使用する必要がある場合は、今すぐバケットの作成を選択しないでください。代わりに、テナントマネージャーを使用して"**バケットを作成する**"後で。

- S3 アプリケーションが使用するバケットの名前を入力します。例： s3-bucket。

バケットを作成した後は、バケット名を変更することはできません。

- このバケットの*リージョン*を選択します。

デフォルトの地域を使用する(us-east-1) 将来的に ILM を使用してバケットのリージョンに基づいてオブジェクトをフィルタリングする予定がない限り、このポリシーは適用されません。

- *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

データのダウンロード手順では、1 つまたは 2 つのファイルをダウンロードして、構成した内容の詳細を保存できます。

手順

- 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、次のいずれかまたは両方を実行します。
 - *アクセスキーをダウンロード*を選択してダウンロードします `csv` テナント アカウント名、アクセス キー ID、シークレット アクセス キーを含むファイル。
 - コピーアイコン () をクリックして、アクセス キー ID とシークレット アクセス キーをクリップボードにコピーします。
- *設定値をダウンロード*を選択してダウンロードします `txt` ロードバランサのエンドポイント、テナン

ト、バケット、およびルートユーザーの設定を含むファイル。

3. この情報を安全な場所に保存してください。



両方のアクセス キーをコピーするまでこのページを閉じないでください。このページを閉じると、キーは使用できなくなります。この情報はStorageGRIDシステムからデータを取得するために使用される可能性があるため、必ず安全な場所に保存してください。

4. プロンプトが表示されたら、チェックボックスを選択して、キーをダウンロードまたはコピーしたことを確認します。
5. *続行*を選択して、ILM ルールとポリシーのステップに進みます。

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に含まれる ILM ポリシーは、すべてのオブジェクトの複製コピーを 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アクティブ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ます。
2. 新しいテナントまたはバケットに属するオブジェクトに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ます。見る["ILMルールを作成する"](#)そして["ILMポリシーを使用する"](#)。
3. *これらの手順を確認し、実行する必要があることを理解しました*を選択します。
4. 次に何をすべきかを理解していることを示すために、チェックボックスを選択します。
5. *続行*を選択して*概要*に進みます。

ステップ6/6: レビューの概要

手順

1. 概要を確認します。
2. 次の手順では、S3 クライアントに接続する前に必要になる可能性のある追加の構成について説明しているので、詳細をメモしておいてください。たとえば、「* root としてSign in*」を選択すると、テナント マネージャに移動し、テナント ユーザーを追加したり、追加のバケットを作成したり、バケット設定を更新したりできます。
3. *完了*を選択します。
4. StorageGRIDからダウンロードしたファイルまたは手動で取得した値を使用してアプリケーションを構成します。

HAグループの管理

高可用性 (HA) グループとは何ですか？

高可用性 (HA) グループは、S3 クライアントに高可用性のデータ接続を提供し、グリッド マネージャーおよびテナント マネージャーに高可用性の接続を提供します。

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 インターフェイスを高可用性 (HA) グループにグル

ープ化できます。HA グループ内のアクティブ インターフェイスに障害が発生した場合、バックアップ インターフェイスがワークロードを管理できます。

各 HA グループは、選択し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 マネージャとテナント 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、高可用性接続を提供できます。["S3 Select を使用する S3 テナント"](#)。S3 Select を使用する場合は HA グループが推奨されますが、必須ではありません。

HA グループはどのように作成しますか？

1. 1 つ以上の管理ノードまたはゲートウェイ ノードのネットワーク インターフェイスを選択します。グリッド ネットワーク (eth0) インターフェイス、クライアント ネットワーク (eth2) インターフェイス、VLAN インターフェイス、またはノードに追加したアクセス インターフェイスを使用できます。



DHCP によって割り当てられた IP アドレスがある場合、HA グループにインターフェイスを追加することはできません。

2. 1 つ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指定します。障害が発生しない限り、プライマリ インターフェイスはアクティブ インターフェイスになります。
3. バックアップ インターフェイスの優先順位を決定します。
4. グループに 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"](#)。

アクティブインターフェイスとは何ですか？

通常の動作中、HA グループのすべての VIP アドレスは、優先順位の最初のインターフェイスであるプライマリ インターフェイスに追加されます。プライマリ インターフェイスが使用可能である限り、クライアントがグループの任意の VIP アドレスに接続するときにそのインターフェイスが使用されます。つまり、通常の操作中は、プライマリ インターフェイスがグループの「アクティブ」インターフェイスになります。

同様に、通常の操作中は、HA グループの優先度の低いインターフェイスは「バックアップ」インターフェイスとして機能します。これらのバックアップ インターフェイスは、プライマリ (現在アクティブ) インターフェイスが使用できなくなった場合を除き、使用されません。

ノードの現在のHAグループのステータスを表示する

ノードが HA グループに割り当てられているかどうかを確認し、現在のステータスを確認するには、**NODES > 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ステータスです。

- 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 インターフェイスです。
- 停止: 高可用性 (keepalived) サービスが手動で停止されているため、このノードで HA グループをホストできません。
- 障害: 次の 1 つ以上の理由により、このノードで HA グループをホストできません。
 - ロード バランサ (nginx-gw) サービスがノード上で実行されていません。
 - ノードの eth0 または VIP インターフェイスがダウンしています。
 - 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、管理クライアント 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 インターフェイスに障害が発生するとどうなりますか？

現在 VIP アドレスをホストしているインターフェイスがアクティブ インターフェイスです。HA グループに複数のインターフェイスが含まれており、アクティブ インターフェイ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使用可能なバックアップ インターフェイスに移動します。そのインターフェイスに障害が発生した場合、VIP アドレスは次の利用可能なバックアップ インターフェイスに移動し、これが繰り返されます。

フェイルオーバーは、次のいずれかの理由でトリガーされる可能性があります。

- インターフェイスが設定されているノードがダウンします。
- インターフェイ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 インターフェイスがダウンします。
- ロード バランサー サービスが停止します。
- 高可用性サービスが停止します。



アクティブ インターフェイスをホストするノード外部のネットワーク障害によってフェイルオーバーが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 プロセスは通常、数秒しかかからず、クライアント アプリケーションへの影響がほとんどなく、通常の再試行動作によって操作を続行できるほど高速です。

障害が解決され、より優先度の高いインターフェイスが再び使用可能になると、VIP アドレスは使用可能な最も優先度の高いインターフェイスに自動的に移動されます。

HA グループはどのように使用されますか？

高可用性 (HA) グループを使用すると、オブジェクト データおよび管理用途のために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 マネージャまたはテナント マネージャ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 クライアントに高可用性のデータ接続を提供できます。
- インターフェイスが 1 つだけ含まれる HA グループでは、多数の VIP アドレスを提供したり、IPv6 アドレスを明示的に設定したりできます。

HA グループは、グループに含まれるすべてのノードが同じサービスを提供する場合にのみ、高可用性を提供できます。HA グループを作成するときは、必要なサービスを提供するノードの種類からインターフェイスを追加します。

- 管理ノード: ロード バランサ サービスを含め、グリッド マネージャまたはテナント マネージャへのアクセスを有効にします。
- ゲートウェイ ノード: ロード バランサ サービスを含めます。

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 インターフェイスである必要があります。一部のメンテナンス手順は、プライマリ管理ノードからのみ実行できます。
テナントマネージャのみへのアクセス	• プライマリまたは非プライマリ管理ノード

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
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セレクト"	• サービスアプライアンス • VMwareベースのソフトウェアノード 注意: S3 Select を使用する場合は HA グループが推奨されますが、必須ではありません。

グリッド マネージャーまたはテナント マネージャーで **HA** グループを使用する際の制限

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。

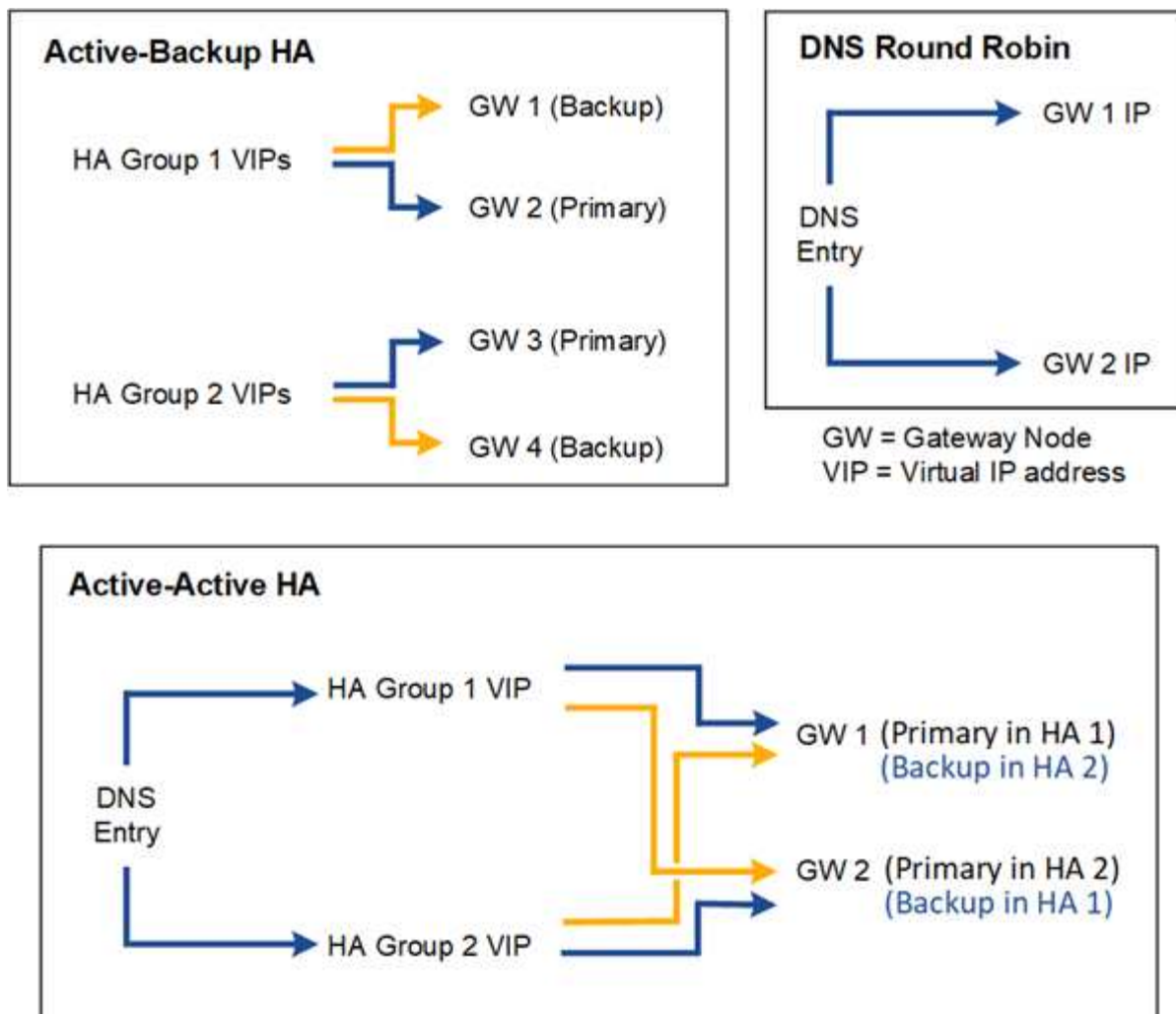
フェイルオーバーが発生したときに Grid Manager または Tenant Manager にサインインしている場合は、サインアウトされるため、タスクを再開するには再度サインインする必要があります。

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。

HAグループの構成オプション

次の図は、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。

図では、青は HA グループ内のプライマリ インターフェイスを示し、黄色は HA グループ内のバックアップ インターフェイスを示します。



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	- 外部依存なしでStorageGRIDによって管理されます。 - 高速フェイルオーバー。	HA グループ内の 1 つのノードのみがアクティブになります。 HA グループごとに少なくとも 1 つのノードがアイドル状態になります。
DNSラウンドロビン	- 総スループットの向上。 - 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く、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の構成が必要です。 - 顧客が実装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 グループの数に応じて拡張される高い集約スループット。 • 高速フェイルオーバー。	• 設定がより複雑になります。 • StorageGRID外部のハードウェアの構成が必要です。 • 顧客が実装するヘルスチェックが必要です。

高可用性グループを構成する

高可用性 (HA) グループを構成して、管理ノードまたはゲートウェイ ノード上のサービスへの高可用性アクセスを提供できます。

開始する前に

- グリッドマネージャにサインインするには、["サポートされているウェブブラウザ"](#)。
- あなたは["ルートアクセス権限"](#)。
- HA グループで VLAN インターフェイスを使用する予定の場合は、VLAN インターフェイスを作成しておきます。見る["VLANインターフェイスを構成する"](#)。
- 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の場合は、インターフェイスを作成しておく必要があります。
 - **Red Hat Enterprise Linux** (ノードをインストールする前):["ノード構成ファイルを作成する"](#)
 - **Ubuntu** または **Debian** (ノードをインストールする前):["ノード構成ファイルを作成する"](#)
 - **Linux** (ノードのインストール後):["Linux: ノードにトランクまたはアクセスインターフェイスを追加する"](#)
 - **VMware** (ノードのインストール後):["VMware: ノードにトランクまたはアクセス インターフェイスを追加する"](#)

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ときは、1 つ以上のインターフェイスを選択し、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、ゲートウェイ ノードまたは管理ノード用のインターフェイスが必要です。HA グループは、特定のノードに対して 1 つのインターフェイスのみを使用できます。ただし、同じノードの他のインターフェイスは、他の HA グループで使用できます。

ウィザードにアクセスする

手順

1. 構成 > ネットワーク > *高可用性グループ*を選択します。
2. *作成*を選択します。

HAグループの詳細を入力します

手順

1. HA グループに一意の名前を付けます。
2. 必要に応じて、HA グループの説明を入力します。
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 1 つ以上の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速く見つけます。

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

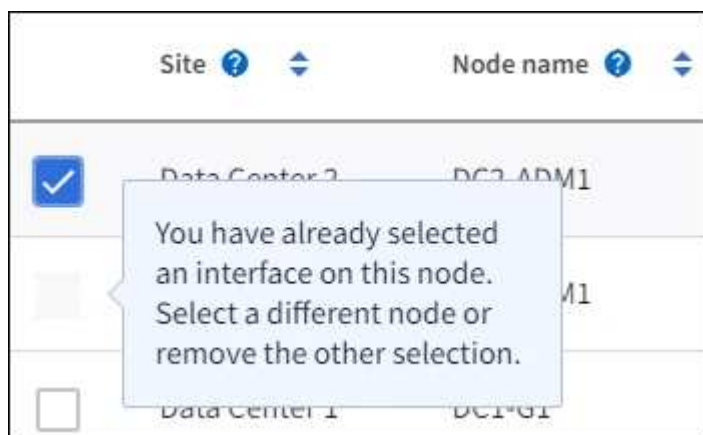


VLAN インターフェースを作成した後、新しいインターフェースがテーブルに表示されるまで最大 5 分間待ちます。

インターフェース選択のガイドライン

- 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 グループがグリッド マネージャとテナント マネージャを含む管理ノード サービスの HA 保護用である場合は、管理ノード上のインターフェースのみを選択します。
- HA グループが S3 クライアント トラフィックの HA 保護用である場合は、管理ノード、ゲートウェイノード、またはその両方のインターフェースを選択します。
- 異なるタイプのノード上のインターフェースを選択すると、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によって提供されていたサービスは、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注意してください。たとえば、バックアップ ゲートウェイ ノードは、管理ノード サービスの HA 保護を提供できません。同様に、バックアップ管理ノードは、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することはできません。

- 。インターフェースを選択できない場合は、そのチェックボックスは無効になります。ツールヒントにはさらに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選択した別のインターフェースと競合する場合は、そのインターフェースを選択できません。
- 。静的 IP アドレスがない場合、構成されたインターフェースを選択することはできません。

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は、どのインターフェースがプライマリ インターフェースで、どのインターフェースがバックアップ (フェイルオーバー) インターフェースであるかを決定できます。プライマリ インターフェースに障害が発生した場合、VIP アドレスは使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 アドレスは利用可能な次の最も優先度の高いインターフェースに移動し、これを繰り返します。

手順

1. *優先順位*列の行をドラッグして、プライマリ インターフェ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。障害が発生しない限り、プライマリ インターフェースはアクティブ インターフェースになります。

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 グループがグリッド マネージャへのアクセスを提供する場合は、プライマリ管理ノード上のインターフェイスをプライマリ 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。

2. *続行*を選択します。

IPアドレスを入力してください

手順

1. サブネット **CIDR** フィールドで、CIDR 表記 (IPv4 アドレスの後にスラッシュとサブネットの長さ (0 ~ 32)) で VIP サブネットを指定します。

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： 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 アドレスおよび VIP アドレスとしても機能します。

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](#)

2. オプションとして、S3 管理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 を入力します。ゲートウェイ アドレスは VIP サブネット内にある必要があります。

クライアントおよび管理者ユーザーは、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。

3. HA グループ内のアクティブ インターフェイスに、少なくとも 1 個、最大 10 個の VIP アドレスを入力します。すべての VIP アドレスは VIP サブネット内にある必要があり、アクティブ インターフェイス上ですべてが同時に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 および IPv6 アドレスを指定できます。

4. HA グループの作成 を選択し、完了 を選択します。

HA グループが作成され、構成された仮想 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 グループを負荷分散に使用する場合は、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ます。見る["ロードバランサのエンドポイントを構成する"](#)。

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、名前や説明を変更したり、インターフェイスを追加または削除したり、優先順位を変更したり、仮想 IP アドレスを追加または更新したりできます。

たとえば、サイトまたはノードの廃止手順で選択したインターフェイスに関連付けられているノードを削除する場合は、HA グループを編集する必要がある場合があります。

手順

1. 構成 > ネットワーク > *高可用性グループ*を選択します。

高可用性グループ ページには、既存の HA グループがすべて表示されます。

2. 編集する HA グループのチェックボックスを選択します。

3. 更新する内容に応じて、次のいずれかを実行します。

- 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。
- グループの名前または説明を更新したり、インターフェイスを追加または削除したり、優先順位を変更したり、VIP アドレスを追加または削除したりするには、[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:

- HA グループの仮想 IP アドレスを更新します。
- *保存*を選択します。
- *完了*を選択します。

5. HA グループの編集 を選択した場合:

- 必要に応じて、グループの名前または説明を更新します。
- 必要に応じて、チェックボックスを選択または選択解除して、インターフェイスを追加または削除します。



HA グループがグリッド マネージャへのアクセスを提供する場合は、プライマリ管理ノード上のインターフェイスをプライマリ 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

- 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、*完了*を選択します。

高可用性グループを削除する

一度に 1 つ以上の高可用性 (HA) グループを削除できます。



HA グループがロードバランサーエンドポイントにバインドされている場合、その HA グループを削除することはできません。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そのグループを削除する必要があります。

クライアントの中断を防ぐには、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更新してください。別の IP アドレス (別の HA グループの仮想 IP アドレスや、インストール時にインターフェイスに構成された IP アドレスなど) を使用して接続するように各クライアントを更新します。

手順

1. 構成 > ネットワーク > *高可用性グループ*を選択します。
2. 削除する各 HA グループの ロード バランサ エンドポイント 列を確認します。ロード バランサのエンドポイントがリストされている場合:
 - a. 構成 > ネットワーク > ロードバランサーエンドポイント 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. アクション > エンドポイント バインディング モードの編集 を選択します。
 - d. バインディング モードを更新して HA グループを削除します。
 - e. *変更を保存*を選択します。
3. ロード バランサ エンドポイントがリストされていない場合は、削除する各 HA グループのチェックボックスをオンにします。
4. アクション > **HA** グループの削除 を選択します。
5. メッセージを確認し、「**HA** グループの削除」を選択して選択を確定します。

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 ページに緑色の成功バナーが表示されます。

負荷分散を管理する

負荷分散に関する考慮事項

負荷分散を使用して、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。

負荷分散とは何ですか？

クライアント アプリケーションがStorageGRIDシステムからデータを保存または取得する場合、StorageGRID はロード バランサを使用して取り込みおよび取得のワークロードを管理します。負荷分散は、複数のストレージ ノードにワークロードを分散することで、速度と接続容量を最大化します。

StorageGRIDロード バランサ サービスは、すべての管理ノードとすべてのゲートウェイ ノードにインストールされ、レイヤー 7 のロード バランシングを提供します。クライアント要求のトランスポート層セキュリティ (TLS) 終了を実行し、要求を検査し、ストレージ ノードへの新しい安全な接続を確立します。

各ノードのロード バランサ サービスは、クライアント トラフィックをストレージ ノードに転送するときに独立して動作します。重み付けプロセスを通じて、ロード バランサ サービスは、CPU 可用性が高いストレージ ノードに、より多くの要求をルーティングします。



推奨される負荷分散メカニズムとしてはStorageGRID Load Balancer サービスがありますが、代わりにサードパーティのロード バランサを統合することもできます。詳細については、[NetAppのアカウント担当者にお問い合わせいただくか、"TR-4626: StorageGRIDサードパーティおよびグローバルロードバランサー"](#)。

負荷分散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 バランサ サービスを備えた 2 つ以上のノードを含める必要があります。たとえば、サイトには 2 つのゲートウェイ ノード、または管理ノードとゲートウェイ ノードの両方が含まれる場合があります。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かに関係なく、各負荷分散ノードに適切なネットワーク、ハードウェア、または仮想化インフラストラクチャがあることを確認します。

ロードバランサーエンドポイントとは何ですか？

ロード バランサ エンドポイントは、受信および送信クライアント アプリケーション要求がロード バランサ サービスを含むノードにアクセスするために使用するポートとネットワーク プロトコル (HTTPS または HTTP) を定義します。エンドポイントは、クライアント タイプ (S3)、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 エンドポイントを作成するには、[構成] > [ネットワーク] > [ロード バランサ エンドポイント] を選択するか、FabricPoolおよび S3 セットアップ ウィザードを完了します。手順については、以下をご覧ください。

- ["ロードバランサのエンドポイントを構成する"](#)
- ["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"](#)

港湾に関する考慮事項

ロード バランサー 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ではデフォルトで 10433 に設定されますが、1 ~ 65535 の間の未使用の外部ポートを任意に指定できます。ポート 80 または 443 を使用する場合は、エンドポイントはゲートウェイ ノード上のロード バランサ サービスのみを使用します。これらのポートは管理ノードで予約されています。複数のエンドポイントに同じポートを使用する場合は、エンドポイントごとに異なるバインディング モードを指定する必要があります。

他のグリッド サービスによって使用されるポートは許可されません。参照["ネットワークポートリファレンス"](#)。

ネットワークプロトコルに関する考慮事項

ほとんどの場合、クライアント アプリケーションとStorageGRID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 暗号化なしでのStorageGRIDへの接続はサポートされて

いますが、特に実稼働環境では推奨されません。StorageGRIDロード バランサ エンドポイントのネットワーク プロトコルを選択するときは、**HTTPS** を選択する必要があります。

ロードバランサ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 エンドポイントを作成するときは、次の3つのオプションのいずれかを使用できます。

- 署名された証明書をアップロードします (推奨)。この証明書は、公的に信頼された証明機関 (CA) またはプライベート証明機関 (CA) 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のがベスト プラクティスです。生成された証明書とは対照的に、CA によって署名された証明書は中断することなくローテーションできるため、有効期限の問題を回避するのに役立ちます。

ロード バランサ エンドポイントを作成する前に、次のファイルを取得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キー ファイル。
- オプションで、各中間発行証明機関からの証明書の 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** 証明書を使用します。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。見る"[S3 API証明書を設定する](#)"。

どのような値が必要ですか？

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 アドレスを知っておく必要があります。

証明書の **Subject 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。例えば：

```
Subject DN:
/C=Country/ST=State/O=Company, Inc./CN=s3.storagegrid.example.com
```

必要に応じて、証明書ではワイルドカードを使用して、ロード バランサ サービスを実行しているすべての管理ノードとゲートウェイ 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 *ワイルドカードを使用して adm1.storagegrid.example.com`そして`gn1.storagegrid.example.com。

S3仮想ホスト形式のリクエストを使用する場合は、証明書には各リクエストの*別名*エントリも含める必要があります。"[S3エンドポイントドメイン名](#)"ワイルドカード名を含め、構成したすべての名前。例えば：

```
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、"[サーバー証明書の強化ガイドライン](#)"。

セキュリティ証明書内の名前ごとに DNS エントリを定義する必要もあります。

期限切れの証明書を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。

証明書の有効期限の問題を回避するには、次のベスト プラクティスに従ってください。

- ロードバランサエンドポイント証明書の有効期限 や **S3 API** のグローバルサーバー証明書の有効期限 アラートなど、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ます。
- StorageGRIDと S3 アプリケーションの証明書のバージョンを常に同期させます。ロードバランサーのエンドポイントに使用される証明書を置き換えたり更新したりする場合は、S3 アプリケーションで使用する同等の証明書も置き換えたり更新したりする必要があります。
- 公的に署名された CA 証明書を使用します。CA によって署名された証明書を使用する場合は、期限が近づいている証明書を中断せずに置き換えることができます。
- 自己署名のStorageGRID証明書を生成していて、その証明書の有効期限が近づいている場合は、既存の証明書の有効期限が切れる前に、StorageGRIDと S3 アプリケーションの両方で証明書を手動で置き換える必要があります。

バインディングモードに関する考慮事項

バインディング モードを使用すると、ロード バランサー エンドポイントへのアクセスに使用できる IP アドレスを制御できます。エンドポイントがバインディング モードを使用する場合、クライアント アプリケーションは、許可された IP アドレスまたは対応する完全修飾ドメイン名 (FQDN) を使用する場合にのみエンドポイントにアクセスできます。他の IP アドレスまたは FQDN を使用するクライアント アプリケーションはエンドポイントにアクセスできません。

次のいずれかのバインディング モードを指定できます。

- **グローバル (デフォルト)**: クライアント アプリケーションは、任意のゲートウェイ ノードまたは管理ノードの IP アドレス、任意のネットワーク上の任意の HA グループの仮想 IP (VIP) アドレス、または対応する FQDN を使用してエンドポイントにアクセスできます。エンドポイントのアクセシビリティを制限する必要がない限り、この設定を使用します。
- **HA グループの仮想 IP**。クライアント アプリケーションは、HA グループの仮想 IP アドレス (または対応する FQDN) を使用する必要があります。
- **ノード インターフェイス**。クライアントは、選択したノード インターフェイスの IP アドレス (または対応する FQDN) を使用する必要があります。
- **ノード タイプ**。選択したノードのタイプに基づいて、クライアントは任意の管理ノードの IP アドレス (または対応する FQDN) または任意のゲートウェイ ノードの IP アドレス (または対応する FQDN) のいずれかを使用する必要があります。

テナントアクセスに関する考慮事項

テナント アクセスは、どのStorageGRIDテナント アカウントがロード バランサ エンドポイントを使用してバケットにアクセスできるかを制御できるオプションのセキュリティ機能です。すべてのテナントにエンドポイントへのアクセスを許可するか (デフォルト)、エンドポイントごとに許可または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。

この機能を使用すると、テナントとそのエンドポイント間のセキュリティ分離を強化できます。たとえば、この機能を使用すると、あるテナントが所有する極秘または機密性の高い資料に他のテナントがまったく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するアクセス キーから決定されます。要求の一部としてアクセス キーが提供されていない場合 (匿名アクセスの場合など)、バケット所有者を使用してテナントが決定されます。

テナントアクセスの例

このセキュリティ機能がどのように機能するかを理解するには、次の例を検討してください。

1. 次のように 2 つのロード バランサ 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。
 - トップシークレット エンドポイント: ポート 10444 を使用し、トップシークレット テナントへのアクセスのみを許可します。他のすべてのテナントはこのエンドポイントへのアクセスをブロックされます。
2. その `top-secret.pdf`***極秘***テナントが所有するバケット内にあります。

アクセスするには `top-secret.pdf`*Top secret*テナントのユーザーはGETリクエストを発行して `https://w.x.y.z:10444/top-secret.pdf`。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すると、直ちにアクセス拒否メッセージが表示されます。資格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

各管理ノードとゲートウェイ ノード上のロード バランサ サービスは、S3 トラフィックをストレージ ノードに転送するときに独立して動作します。重み付けプロセスを通じて、ロード バランサ サービスは、CPU 可用性が高いストレージ ノードに、より多くの要求をルーティングします。ノードの 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。ノードが 100% の使用率を報告したり、使用率を報告できなかったりする場合でも、すべてのストレージ ノードには最小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 サービスが配置されているサイトに限定されます。

ロードバランサのエンドポイントを構成する

ロード バランサー エンドポイントは、ゲートウェイおよび管理ノード上のStorageGRID ロード バランサーに接続するときに S3 クライアントが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。



このバージョンのドキュメント サイトから Swift の詳細は削除されました。見る ["S3とSwiftクライアント接続を構成する"](#)。

開始する前に

- グリッドマネージャにサインインするには、["サポートされているウェブブラウザ"](#)。

- あなたは["ルートアクセス権限"](#)。
- あなたは、["負荷分散に関する考慮事項"](#)。
- ロードバランサーのエンドポイントに使用するポートを以前に再マップした場合は、["ポートの再マップを削除しました"](#)。
- 使用を計画している高可用性 (HA) グループを作成しました。HA グループは推奨されますが、必須ではありません。見る["高可用性グループの管理"](#)。
- ロードバランサーのエンドポイントが["S3 Select の S3 テナント"](#)ただし、ベアメタル ノードの IP アドレスまたは FQDN は使用できません。S3 Select に使用されるロードバランサー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ます。
- 使用する予定の VLAN インターフェイスを構成しました。見る["VLANインターフェイスを構成する"](#)。
- HTTPS エンドポイント (推奨) を作成する場合は、サーバー証明書があります。



エンドポイント証明書の変更がすべてのノードに適用されるまでに最大 15 分かかる場合があります。

- 証明書をアップロードするには、サーバー証明書、証明書の秘密キー、およびオプションで 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。件名（識別名）も知っ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可能) を使用する場合は、デフォルトの証明書を外部証明機関によって署名されたカスタム証明書にすでに置き換えています。見る["S3 API証明書を設定する"](#)。

ロードバランサエンドポイントを作成する

各 S3 クライアント ロード バランサ エンドポイントは、ポート、クライアント タイプ (S3)、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 ロード バランサ エンドポイントは、ポート、インターフェイス タイプ、および信頼できないクライアント 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. 構成 > ネットワーク > ロード バランサー エンドポイント を選択します。
2. S3 または Swift クライアントのエンドポイントを作成するには、**S3** または **Swift** クライアント タブを選択します。
3. Grid Manager、Tenant Manager、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. ***作成***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. 適切な手順を選択して、作成するエンドポイントの種類の詳細を入力します。

S3 または Swift クライアント

フィールド	説明
Name	エンドポイントの説明的な名前。ロード バランサー エンドポイント ページの表に表示されます。
ポート	負荷分散に使用するStorageGRIDポート。このフィールドは、最初で作成するエンドポイントに対してデフォルトで 10433 に設定されますが、1 ～ 65535 の未使用の外部ポートを入力できます。 80 または 8443 を入力すると、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 ノードでのみ構成されます。次に、ポート 8443 を S3 エンドポイントとして使用できるようになり、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	このエンドポイントを使用するクライアント アプリケーションのタイプ (S3 または Swift)。
ネットワークプロトコル	クライアントがこのエンドポイントに接続するときに使用するネットワークプロトコル。 • 安全な TLS 暗号化通信には HTTPS を選択します (推奨)。エンドポイントを保存する前に、セキュリティ証明書を添付する必要があります。 • 安全性の低い暗号化されていない通信の場合は HTTP を選択します。非本番グリッドには HTTP のみを使用します。

管理インターフェイス

フィールド	説明
Name	エンドポイントの説明的な名前。ロード バランサー エンドポイント ページの表に表示されます。
ポート	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StorageGRIDポート。 • グリッドマネージャー: 8443 • テナントマネージャー: 9443 • グリッドマネージャとテナントマネージャの両方: 443 注: これらのプリセット ポートまたはその他の使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インターフェイスのラジオ ボタンを選択します。

フィールド	説明
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されていないクライアント ネットワークからアクセスできるようにする場合は、[はい] を選択します。それ以外の場合は、[いいえ]を選択します。 「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: ロード バランサ エンドポイントを作成するときのみ、信頼されていないクライアント ネットワークに対してポートを開くか閉じるかを構成できます。

1. *続行*を選択します。

バインディングモードを選択する

手順

1. エンドポイントのバインディング モードを選択して、任意の IP アドレスまたは特定の IP アドレスとネットワーク インターフェイスを使用してエンドポイントにアクセスする方法を制御します。

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リストされます。

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のアクセシビリティを制限する必要がない限り、*グローバル*設定を使用します。
HAグループの仮想IP	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 モードのエンドポイントは、エンドポイントに選択した HA グループが重複していない限り、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イス	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 インターフェイスの IP アドレス (または対応する FQDN) を使用する必要があります。
ノードタイプ (クライアントエンドポイントのみ)	選択したノードのタイプに基づいて、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、任意の管理ノードの IP アドレス (または対応する FQDN) または任意のゲートウェイ 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。

モード	説明
すべての管理ノード（管理インターフェー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、任意の管理ノードの 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 は次の優先順位を使用して、使用するエンドポイントを決めます: **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。

管理インターフェース エンドポイントを作成する場合は、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** グループを選択します。

管理インターフェース エンドポイントを作成する場合は、管理ノードにのみ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管理ノードまたはゲートウェイ ノードごとに 1 つ以上のノード インターフェイスを選択します。
4. ノード タイプ を選択した場合は、プライマリ管理ノードと非プライマリ管理ノードの両方を含む管理ノード、またはゲートウェイ ノードのいずれかを選択します。

テナントアクセスを制御する



管理インターフェースエンドポイントは、エンドポイントが**テナントマネージャーのインターフェースタイプ**。

手順

1. テナント アクセス ステップでは、次のいずれかを選択します。

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 バランサー エンドポイントを編集して、特定のアカウントを許可またはブロックできます。
選択したテナントを許可する	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	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。新しいロードバランサー

エンドポイントを追加するには、[作成] を選択します。次に、[終了後の操作](#)。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ます。

証明書は、S3 クライアントと管理ノードまたはゲートウェイ ノード上のロード バランサ サービス間の接続を保護します。

- 証明書をアップロード。アップロードするカスタム証明書がある場合は、このオプションを選択します。
- *証明書を生成*します。カスタム証明書を生成するために必要な値がある場合は、このオプションを選択します。
- * StorageGRID S3 証明書を使用します*。ストレージノードへの直接接続にも使用できるグローバル S3 API 証明書を使用する場合は、このオプションを選択します。

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、外部証明機関によって署名されたカスタム証明書に置き換えていない限り、このオプションを選択することはできません。見る"[S3 API 証明書を設定する](#)"。

- 管理インターフェース証明書を使用します。管理ノードへの直接接続にも使用できるグローバル管理インターフェース証明書を使用する場合は、このオプションを選択します。
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または生成します。

証明書をアップロード

- a. *証明書のアップロード*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 エンコードされたカスタム 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 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**: 各中間発行証明機関 (CA) からの証明書を含む単一のオプション ファイル。このファイルには、PEM でエンコードされた各 CA 証明書ファイルが、証明書チェーンの順序で連結されて含まれている必要があります。
- c. *証明書の詳細*を展開して、アップロードした各証明書のメタデータを表示します。オプションの CA バンドルをアップロードした場合、各証明書は独自のタブに表示されます。
 - 証明書ファイルを保存するには 証明書のダウンロード を選択するか、証明書バンドルを保存するには **CA バンドル**のダウンロード を選択します。

証明書ファイル名とダウンロード場所を指定します。拡張子を付けてファイルを保存する .pem。

例: storagegrid_certificate.pem

- 証明書の内容をコピーして他の場所に貼り付けるには、「証明書 **PEM** のコピー」または「**CA バンドル PEM** のコピー」を選択します。
- d. *作成*を選択します。+ ロードバランサー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ースとエンドポイント間の後続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 1 つ以上の IP アドレス。
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、生成された証明書では、最初のドメイン名または IP アドレスがサブジェクト共通名 (CN) として使用されます。

フィールド	説明
有効日数	証明書の有効期限が切れるまでの作成後日数。
キー使用拡張機能を追加する	選択した場合 (デフォルト、推奨)、生成された証明書にキー使用法と拡張キー使用法の拡張機能が追加されます。 これらの拡張機能は、証明書に含まれるキーの目的を定義します。 注意: 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との接続の問題が発生しない限り、このチェックボックスをオンのままにしておきます。

c. ***生成***を選択します。

d. 生成された証明書のメタデータを表示するには、「証明書の詳細」を選択します。

- 証明書ファイルを保存するには、[証明書のダウンロード]を選択します。

証明書ファイル名とダウンロード場所を指定します。拡張子を付けてファイルを保存する .pem。

例: storagegrid_certificate.pem

- 証明書の内容をコピーして他の場所に貼り付けるには、「証明書 **PEM** のコピー」を選択します。

e. ***作成***を選択します。

ロード バランサー 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ースとこのエンドポイント間の以降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、StorageGRIDの完全修飾ドメイン名 (FQDN) をクライアントが接続に使用する各 IP アドレスに関連付けるレコードが DNS に含まれていることを確認します。

DNS レコードに入力する IP アドレスは、負荷分散ノードの HA グループを使用しているかどうかによって異なります。

- HA グループを構成している場合、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 サービスに接続します。

また、DNS レコードがワイルドカード名を含むすべての必要なエンドポイント ドメイン名を参照していることも確認する必要があります。

2. エンドポイントに接続するために必要な情報を S3 クライアントに提供します。

- ポート番号
- 完全修飾ドメイン名またはIPアドレス
- 必要な証明書の詳細

ロードバランサのエンドポイントの表示と編集

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など、既存のロード バランサ エンドポイントの詳細を表示できます。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表示するには、「ロード バランサー エンドポイント」ページの表を確認します。
- 証明書メタデータを含む特定のエンドポイントに関するすべての詳細を表示するには、テーブルでエンドポイントの名前を選択します。表示される情報は、エンドポイントの種類と構成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 エンドポイント ページの アクション メニューを使用します。



管理インターフェースのエンドポイントのポート編集時に 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再度アクセスできるようにします。



エンドポイントを編集した後、変更がすべてのノードに適用されるまで最大 15 分ほどかかる場合があります。

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. アクション > *エンドポイント名の編集*を選択します。 c. 新しい名前を入力してください。 d. *保存*を選択します。	a. エンドポイント名を選択して詳細を表示します。 b. 編集アイコンを選択. 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. アクション > *エンドポイントポートの編集*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. アクション > エンドポイント 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 モードを更新します。 d. *変更を保存*を選択します。	a. エンドポイント名を選択して詳細を表示します。 b. *バイン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 モードを更新します。 d. *変更を保存*を選択します。
エンドポイント証明書編集する	a. エンドポイントのチェックボックスを選択します。 b. アクション > *エンドポイント証明書の編集*を選択します。 c. 必要に応じて、新しいカスタム証明書をアップロードまたは生成するか、グローバル S3 証明書の使用を開始します。 d. *変更を保存*を選択します。	a. エンドポイント名を選択して詳細を表示します。 b. *証明書*タブを選択します。 c. *証明書の編集*を選択します。 d. 必要に応じて、新しいカスタム証明書をアップロードまたは生成するか、グローバル S3 証明書の使用を開始します。 e. *変更を保存*を選択します。

Task	[操作]メニュー	詳細ページ
テナントアクセスの編集	a. エンドポイントのチェックボックスを選択します。 b. アクション > テナント アクセスの編集 を選択します。 c. 別のアクセス オプションを選択するか、リストからテナントを選択または削除するか、あるいはその両方を実行します。 d. *変更を保存*を選択します。	a. エンドポイント名を選択して詳細を表示します。 b. テナント アクセス タブを選択します。 c. テナント アクセスの編集 を選択します。 d. 別のアクセス オプションを選択するか、リストからテナントを選択または削除するか、あるいはその両方を実行します。 e. *変更を保存*を選択します。

ロードバランサのエンドポイントを削除する

アクション メニューを使用して 1 つ以上のエンドポイントを削除することも、詳細ページから 1 つのエンドポイントを削除することもできます。



クライアントの中断を防ぐには、ロードバランサー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更新してください。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各クライアントを更新します。必要な証明書情報も必ず更新してください。



管理インターフェースのエンドポイントを削除中に Grid Manager にアクセスできなくなった場合は、URL を更新します。

- 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 ページで、削除する各エンドポイントのチェックボックスをオンにします。
 - b. アクション > *削除*を選択します。
 - c. 「OK」を選択します。
- 詳細ページからエンドポイントを 1 つ削除するには:
 - a. ロード バランサー ページからエンドポイント名を選択します。
 - b. 詳細ページで*削除*を選択します。
 - c. 「OK」を選択します。

S3 エンドポイントのドメイン名を設定する

S3 仮想ホスト スタイルのリクエストをサポートするには、グリッド マネージャーを使用して、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。将来のリリースではこの構成は禁止されます。

開始する前に

- グリッドマネージャにサインインするには、"[サポートされているウェブブラウザ](#)"。
- あなたが持っている"[特定のアクセス権限](#)"。
- グリッドのアップグレードが進行中ではないことを確認しました。



グリッドのアップグレードが進行中の場合は、ドメイン名の構成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、次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 ドメイン名をStorageGRIDシステムに追加します。
- 確実に"[クライアントがStorageGRIDへのHTTPS接続に使用する証明書](#)"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ます。

たとえば、エンドポイントが `s3.company.com`、HTTPS接続に使用する証明書に次の内容が含まれていることを確認する必要があります。 `s3.company.com`` エンドポイントとエンドポイントのワイルドカード サブジェクト別名 (SAN) : ``*.s3.company.com`。

- クライアントが使用する DNS サーバーを構成します。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すべての必要な 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ます。



クライアントは、ゲートウェイ ノード、管理ノード、またはストレージ ノードの IP アドレスを使用するか、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方法を理解して、DNS レコードに正しい IP アドレスを含める必要があります。

グリッドへの HTTPS 接続 (推奨) を使用するクライアントは、次のいずれかの証明書を使用できます。

- ロード バランサー 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のカスタム証明書を使用できます。各ロードバランサーエンドポイントは、異なる S3 エンドポイントドメイン名を認識するように設定できます。
- ロードバランサーエンドポイントに接続するクライアント、またはストレージノードに直接接続するクライアントは、必要なすべての S3 エンドポイントドメイン名を含めるようにグローバル S3 API 証明書をカスタマイズできます。



S3 エンドポイント ドメイン名を追加せず、リストが空の場合、S3 仮想ホスト スタイルの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. 構成 > 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。さらにドメイン名を追加するには、「別のドメイン名を追加」を選択します。
3. *保存*を選択します。
4. クライアントが使用するサーバー証明書が、必要な S3 エンドポイント ドメイン名と一致していることを確認します。
 - クライアントが独自の証明書を使用するロードバランサエンドポイントに接続する場合、"[エンドポイントに関連付けられた証明書を更新する](#)"。
 - 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に接続するか、直接ストレージノードに接続する場合、"[グローバルS3 API証明書を更新する](#)"。
5. エンドポイント ドメイン名要求を解決できるようにするために必要な DNS レコードを追加します。

結果

さて、クライアントがエンドポイントを使用すると `bucket.s3.company.com` DNS サーバーは正しいエンドポイントに解決し、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、仮想ホスト形式のリクエストは失敗します。

手順

1. 構成 > 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. 編集するドメイン名フィールドを選択し、必要な変更を加えます。
3. *保存*を選択します。
4. 変更を確認するには、[はい] を選択します。

S3エンドポイントドメイン名を削除する

S3 アプリケーションで使用される名前を削除すると、仮想ホスト形式のリクエストは失敗します。

手順

1. 構成 > 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. 削除アイコンを選択します  ドメイン名の横にあります。
3. 削除を確認するには、[はい] を選択します。

関連情報

- "[S3 REST APIを使用する](#)"
- "[IPアドレスを表示](#)"
- "[高可用性グループを構成する](#)"

概要: 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

すべての管理ノードとゲートウェイ ノードに含まれるロード バランサ サービス、またはすべてのストレージ ノードに含まれるローカル ディストリビューション ルータ (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。オプションで、負荷分散ノードの高可用性 (HA) グループを作成して、仮想 IP (VIP) アドレスを使用する高可用性接続を提供することもできます。IP アドレスまたは VIP アドレスではなく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される IP アドレスとポートをまとめたものです。ロードバランサエンドポイントと高可用性 (HA) グループをすでに作成している場合は、[IPアドレスを見つける場所](#)グリッド マネージャーでこれらの値を見つけます。

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	ロードバランサの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	ロードバランサの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	ロードバランサの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 エンドポイントに接続するには、次に示すような構造の URL を使用します。

```
https://VIP-of-HA-group:LB-endpoint-port
```

たとえば、HA グループの仮想 IP アドレスが 192.0.2.5 で、ロード バランサ エンドポイントのポート番号が 10443 の場合、アプリケーションは次の URL を使用してStorageGRIDに接続できます。

```
https://192.0.2.5:10443
```

IPアドレスを見つける場所

1. グリッドマネージャーにSign inには、["サポートされているウェブブラウザ"](#)。

2. グリッド ノードの IP アドレスを見つけるには:

- a. 「NODES」を選択します。
- b. 接続する管理ノード、ゲートウェイ ノード、またはストレージ ノードを選択します。
- c. *概要*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 アドレスをメモします。
- e. IPv6 アドレスとインターフェース マッピングを表示するには、[詳細を表示] を選択します。

クライアント アプリケーションからリスト内の任意の IP アドレスへの接続を確立できます。

- **eth0:** グリッドネットワーク
- **eth1:** 管理ネットワーク (オプション)
- **eth2:** クライアントネットワーク (オプション)



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内のアクティブ 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 アドレスを見つけるには:

- a. 構成 > ネットワーク > *高可用性グループ*を選択します。
- b. 表で、HA グループの仮想 IP アドレスを書き留めます。

4. ロード バランサ エンドポイントのポート番号を見つけるには:

- a. 構成 > ネットワーク > ロード バランサー エンドポイント を選択します。
- b. 使用するエンドポイントのポート番号をメモします。



ポート番号が 80 または 443 の場合、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 ノードでのみ構成されます。他のすべてのポートは、ゲートウェイ ノードと管理ノードの両方で構成されます。

- c. テーブルからエンドポイントの名前を選択します。
- d. 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ます。

ネットワークと接続を管理する

ネットワークの設定

Grid Manager 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構成する

あなたはできる"**仮想LAN (VLAN) インターフェースを作成する**"セキュリティ、柔軟性、パフォーマンスを確保するためにトラフィックを分離および分割します。各 VLAN インターフェイスは、管理ノードおよびゲ

ートウェイ ノード上の 1 つ以上の親インターフェイスに関連付けられます。HA グループおよびロード バランサ エンドポイントで VLAN インターフェイスを使用して、クライアントまたは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

使用できます"[トラフィック分類ポリシー](#)"特定のバケット、テナント、クライアント サブネット、ロード バランサ エンドポイントに関連するトラフィックなど、さまざまな種類のネットワーク トラフィックを識別して処理します。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 ネットワークと接続を構成および管理できます。

見る"[S3 クライアント接続を構成する](#)"S3 クライアントを接続する方法を学習します。

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 インターフェイスをサポートしているため、セキュリティとアクセスの要件に合わせて各グリッド ノードのネットワークを構成できます。

ネットワークトポロジの詳細については、以下を参照してください。"[ネットワークガイドライン](#)"。

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

オプション。管理ネットワークは通常、システムの管理とメンテナンスに使用されます。クライアント プロトコル アクセスにも使用できます。管理ネットワークは通常はプライベート ネットワークであり、サイト間でルーティング可能である必要はありません。

クライアント ネットワーク

オプション。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

- 各StorageGRIDノードには、割り当てられているネットワークごとに専用のネットワーク インターフェイス、IP アドレス、サブネット マスク、ゲートウェイが必要です。
- グリッド ノードは、ネットワーク上で複数のインターフェイ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ており、ノードと同じサブネット上にある必要があります。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。
- 各ノードでは、各ネットワークが特定のネットワーク インターフェイスにマップされます。

ネットワーク	インターフェイス名
Grid	eth0
管理者（オプション）	eth1
クライアント（オプション）	eth2

- ノードがStorageGRIDアプライアンスに接続されている場合、各ネットワークに特定のポートが使用されます。詳細については、アプライアンスのインストール手順を参照してください。
- デフォルト ルートはノードごとに自動的に生成されます。eth2 が有効な場合、0.0.0.0/0 は eth2 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。
- グリッド ノードの展開中に管理ネットワークを構成して、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 インターフェイスにアクセスできるようにすることができます。

オプションインターフェース

オプションで、ノードに追加のインターフェースを追加できます。たとえば、管理ノードまたはゲートウェイノードにトランクインターフェースを追加して、["VLANインターフェイス"](#)異なるアプリケーションまたはテナントに属するトラフィックを分離します。または、アクセスインターフェースを追加して、["高可用性（HA）グループ"](#)。

トランクまたはアクセス インターフェースを追加するには、次を参照してください。

- **VMware** (ノードのインストール後):["VMware: ノードにトランクまたはアクセス インターフェースを追加する"](#)
 - **Red Hat Enterprise Linux** (ノードをインストールする前):["ノード構成ファイルを作成する"](#)
 - **Ubuntu** または **Debian** (ノードをインストールする前):["ノード構成ファイルを作成する"](#)
 - **RHEL、Ubuntu、または Debian** (ノードをインストールした後):["Linux: ノードにトランクまたはアクセスインターフェースを追加する"](#)

IPアドレスを表示

StorageGRIDシステム内の各グリッド ノードの IP アドレスを表示できます。この IP アドレスを使用して、コマンド ラインでグリッド ノードにログインし、さまざまなメンテナンス手順を実行できます。

開始する前に

グリッドマネージャにサインインするには、["サポートされているウェブブラウザ"](#)。

タスク概要

IPアドレスの変更については、以下を参照してください。["IPアドレスを設定する"](#)。

手順

1. **NODES > grid node > *概要***を選択します。
2. IP アドレスのタイトルの右側にある [詳細表示] を選択します。

そのグリッド ノードの IP アドレスがテーブルにリストされます。

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.			

VLAN インターフェースを構成する

管理ノードとゲートウェイ ノードに仮想 LAN (VLAN) インターフェースを作成し、HA グループとロード バランサ エンドポイントで使用してトラフィックを分離および分割し、セキュリティ、柔軟性、パフォーマンスを向上させることができます。HA グループ内の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、1 つのノードがダウンしても、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ぎます。

VLAN インターフェイスに関する考慮事項

- VLAN ID を入力し、1 つ以上のノード上の親インターフェイスを選択して、VLAN インターフェイスを作成します。
- 親インターフェイスは、スイッチでトランク インターフェイスとして設定する必要があります。
- 親インターフェイスは、グリッド ネットワーク (eth0)、クライアント ネットワーク (eth2)、または VM またはベアメタル ホストの追加のトランク インターフェイス (ens256 など) にすることができます。
- 各 VLAN インターフェイスでは、特定のノードに対して親インターフェイスを 1 つだけ選択できます。たとえば、同じゲートウェイ ノード上のグリッド ネットワーク インターフェイスとクライアント ネットワーク インターフェイスの両方を、同じ VLAN の親インターフェイスとして使用することはできません。
- VLAN インターフェイスが、グリッド マネージャおよびテナント マネージャに関連するトラフィックを含む管理ノード 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イスのみを選択します。
- VLAN インターフェイスが 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 ノードのいずれかでインターフェイスを選択します。
- トランク インターフェイスを追加する必要がある場合は、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: ノードにトランクまたはアクセス インターフェイスを追加する](#)"
 - **RHEL** (ノードをインストールする前): "[ノード構成ファイルを作成する](#)"
 - **Ubuntu** または **Debian** (ノードをインストールする前): "[ノード構成ファイルを作成する](#)"
 - **RHEL**、**Ubuntu**、または **Debian** (ノードをインストールした後): "[Linux: ノードにトランクまたはアクセスインターフェイスを追加する](#)"

VLAN インターフェイスを作成する

開始する前に

- グリッドマネージャにサインインするには、"[サポートされているウェブブラウザ](#)"。
- あなたは"[ルートアクセス権限](#)"。
- トランク インターフェイスがネットワークに設定され、VM または Linux ノードに接続されています。トランク インターフェイスの名前がわかっています。
- 設定する VLAN の ID がわかっています。

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 インターフェイスと 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 上のStorageGRIDにアクセスできるようにする VLAN インターフェイスを作成できます。VLAN インターフェイスを作成するときは、VLAN ID を指定し、1 つ以上のノード上の親 (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. 構成 > ネットワーク > **VLAN** インターフェース を選択します。
2. *作成*を選択します。

VLANインターフェースの詳細を入力します

手順

1. ネットワーク内の VLAN の ID を指定します。1 ～ 4094 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。たとえば、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 を使用する場合があります。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できません。すでに使用されている 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ます。
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イスがリストされています。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 つ以上選択します。

たとえば、ゲートウェイ ノードと管理ノードのクライアント ネットワーク (eth2) インターフェイスに VLAN を接続する場合があります。

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.

2. *続行*を選択します。

設定を確認する

手順

1. 構成を確認し、変更を加えます。

- VLAN ID または説明を変更する必要がある場合は、ページの上部にある **VLAN** の詳細を入力 を選択します。
- 親インターフェースを変更する必要がある場合は、ページの上部にある*親インターフェースの選択*を選択するか、*前へ*を選択します。
- 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イスが [高可用性グループ] ページの選択肢として表示され、ノードの [ネットワーク インターフェイス] テーブルにリストされるまで、最大 5 分間待機します ([ノード] > [親インターフェイス ノード] > [ネットワーク])。

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場合、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、関連付けられたノードを廃止する予定の場合は、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必要がある場合があります。

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、親インターフェイスを削除することはできません。

たとえば、VLAN 200 がノード A と 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使用し、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を削除できますが、ノード A の使用済みの親インターフェイスを削除することはできません。

手順

1. 構成 > ネットワーク > **VLAN** インターフェイス を選択します。
2. 編集する VLAN インターフェイスのチェックボックスを選択します。次に、[アクション] > [編集] を選択します。
3. 必要に応じて、VLAN ID または説明を更新します。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オンまたはオフにして、親インターフェイスを追加したり、未使用のインターフェイスを削除したりします。次に、[続行] を選択します。
5. 構成を確認し、変更を加えます。
6. *保存*を選択します。

VLAN インターフェイスを削除する

1 つ以上の VLAN インターフェイスを削除できます。

現在 HA グループで使用されている VLAN インターフェイスを削除することはできません。VLAN インターフェイスを削除する前に、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 トラフィックの中断を回避するには、次のいずれかを実行すること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、新しい VLAN インターフェイスを HA グループに追加します。
- この VLAN インターフェイスを使用しない新しい HA グループを作成します。
- 削除する VLAN インターフェイスが現在アクティブ インターフェイスである場合は、HA グループを編集します。削除する VLAN インターフェイスを優先リストの一番下に移動します。新しいプライマリ インターフェイス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ます。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. 構成 > ネットワーク > **VLAN** インターフェイス 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. 選択を確認するには、[はい] を選択します。

選択したすべての VLAN インターフェイスが削除されます。VLAN インターフェイス ページに緑色の成功バナーが表示されます。

トラフィック分類ポリシーを管理する

トラフィック分類ポリシーとは何ですか？

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) の向上に役立ちます。

トラフィック分類ポリシーは、ゲートウェイ ノードと管理ノードのStorageGRIDロード バランサ 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 エンドポイントをあらかじめ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 1 つ以上のエンティティに関連するネットワーク トラフィックを識別するための 1 つ以上の一致ルールが含まれています。

- バケット
- サブネット
- テナント
- ロード バランサ エンドポイント

StorageGRID は、ルールの目的に従って、ポリシー内の任意のルールに一致するトラフィックを監視します。ポリシーのルールに一致するトラフィックはすべて、そのポリシーによって処理されます。逆に、指定した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。

交通制限

必要に応じて、次の制限タイプをポリシーに追加できます。

- 総帯域幅
- 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。



総帯域幅を制限したり、リクエストごとの帯域幅を制限したりするポリシーを作成できます。ただし、StorageGRID両方のタイプの帯域幅を同時に制限することはできません。総帯域幅を制限すると、制限のないトラフィックのパフォーマンスも多少低下する可能性があります。

総計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レートでストリーミングされます。StorageGRID は1つの速度のみを適用できるため、マッチャー タイプによる最も具体的なポリシー マッチが適用されます。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、より具体的でない他の一致ポリシーに対してカウントされません。その他のすべての制限タイプでは、クライアント要求は 250 ミリ秒遅延され、一致するポリシー制限を超える要求に対して 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できます。

SLA を使用したトラフィック分類ポリシーの使用

トラフィック分類ポリシーを容量制限およびデータ保護と組み合わせて使用することで、容量、データ保護、およびパフォーマンスの詳細を提供するサービス レベル アグリーメント (SLA) を適用できます。

次の例は、SLA の 3 つの層を示しています。各 SLA 層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。

サービスレベル層	容量	データ保護	許容される最大パフォーマンス	料金
Gold	1 PBのストレージが許可されます	3コピーILMルール	25Kリクエスト/秒 5 GB/秒 (40 Gbps) の帯域幅	月額\$\$\$
Silver	250 TBのストレージが許可されます	2コピーILMルール	10Kリクエスト/秒 1.25 GB/秒 (10 Gbps) の帯域幅	月額\$\$
Bronze	100 TBのストレージが許可されます	2コピーILMルール	5K リクエスト/秒 1 GB/秒 (8 Gbps) の帯域幅	月額\$

トラフィック分類ポリシーを作成する

監視する場合、トラフィック分類ポリシーを作成し、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 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できます。オプションで、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

- グリッドマネージャにサインインするには、"[サポートされているウェブブラウザ](#)"。
- あなたは"[ルートアクセス権限](#)"。
- 一致させるロード バランサー エンドポイントを作成しました。
- 一致させるテナントを作成しました。

手順

1. 構成 > ネットワーク > *トラフィック分類*を選択します。
2. *作成*を選択します。
3. ポリシーの名前と説明（オプション）を入力し、「続行」を選択します。

たとえば、このトラフィック分類ポリシーが何に適用され、何が制限されるかを説明します。

4. *ルールを追加*を選択し、次の詳細を指定して、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
タイプ	一致ルールが適用されるトラフィックの種類を選択します。トラフィック タイプは、バケット、バケット正規表現、CIDR、ロード バランサ エンドポイント、テナントです。
一致値	選択したタイプに一致する値を入力します。 • バケット: 1 つ以上のバケット名を入力します。 • バケット正規表現: バケット名のセットを一致させるために使用される 1 つ以上の正規表現を入力します。 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ます。 • CIDR: 目的のサブネットに一致する 1 つ以上の IPv4 サブネットを CIDR 表記で入力します。 • 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ます。これらは、"ロードバランサのエンドポイントを構成する"。 • 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 (匿名アクセスなど)、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	定義したタイプと一致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を一致させる場合は、[逆一致] チェックボックスをオンにします。それ以外の場合は、チェックボックスをオフのままにします。 たとえば、このポリシーを 1 つを除くすべてのロード バランサー エンドポイントに適用する場合は、除外するロード バランサー 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み、そのうち少なくとも 1 つが逆マッチャーであるポリシーの場合は、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. 必要に応じて、「制限を追加」を選択し、次の詳細を選択して、ルールに一致するネットワークトラフィックを制御するための 1 つ以上の制限を追加します。



StorageGRID は、制限を追加しない場合でもメトリックを収集するため、トラフィックの傾向を把握できます。

フィールド	説明
タイプ	ルールに一致するネットワーク トラフィックに適用する制限の種類。たとえば、帯域幅や要求レートを制限できます。 注: 総帯域幅を制限したり、リクエストごとの帯域幅を制限したりするポリシーを作成できます。ただし、StorageGRID両方のタイプの帯域幅を同時に制限することはできません。集約帯域幅が使用されている場合、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、集約帯域幅は利用できません。総帯域幅を制限すると、制限のないトラフィックのパフォーマンスも多少低下する可能性があります。 帯域幅制限の場合、StorageGRID は設定された制限の種類に最も一致するポリシーを適用します。たとえば、一方向のトラフィックのみを制限するポリシーがある場合、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あっても、反対方向のトラフィックは無制限になります。StorageGRID は、次の順序で帯域幅制限の「最適な」一致を実装します。 • 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 • CIDR の完全一致ではない (/32 ではない) • 逆マッチ
適用対象	この制限がクライアントの読み取り要求 (GET または HEAD) に適用されるか、書き込み要求 (PUT、POST、または DELETE) に適用されるかを示します。
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。たとえば、このルールに一致するネットワーク トラフィックが 10 MiB/s を超えないようにするには、10 と入力して MiB/s を選択します。 注: 単位の設定に応じて、使用可能な単位はバイナリ (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。

たとえば、SLA 層に 40 GB/秒の帯域幅制限を作成する場合は、40 GB/秒の GET/HEAD と 40 GB/秒の PUT/POST/DELETE の 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ます。 前へ*ボタンを使用して戻って、必要に応じて変更を加えます。ポリシーに満足したら、[*保存して続行] を選択します。

S3 クライアント 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のメトリックを表示する](#)"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します。

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して、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

- グリッドマネージャにサインインするには、"[サポートされているウェブブラウザ](#)"。
- あなたは"[ルートアクセス権限](#)"。

手順

1. 構成 > 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、既存のポリシーがテーブルにリストされます。

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。見る"[トラフィック分類ポリシーを作成する](#)"何を入力するか。

[操作]メニュー

- a. ポリシーのチェックボックスを選択します。
- b. アクション > *編集*を選択します。

詳細ページ

- a. ポリシー名を選択します。
- b. ポリシー名の横にある*編集*ボタンを選択します。

3. ポリシー名の入力手順では、必要に応じてポリシー名または説明を編集し、[続行] を選択します。
4. 「一致ルールの追加」ステップでは、オプションでルールを追加するか、既存のルールの*タイプ*と*一致値*を編集して、*続行*を選択します。
5. 「制限の設定」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が保存され、ネットワーク トラフィックはトラフィック分類ポリシーに従って処理されるようになりました。トラフィック チャートを表示し、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できます。

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。ポリシーは削除すると取得で

きないため、正しいポリシーを削除するようにしてください。

開始する前に

- グリッドマネージャにサインインするには、"[サポートされているウェブブラウザ](#)"。
- あなたは"[ルートアクセス権限](#)"。

手順

1. 構成 > 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、既存のポリシーがテーブルにリストされます。

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. ポリシーのチェックボックスを選択します。
- b. アクション > *削除*を選択します。

ポリシーの詳細ページ

- a. ポリシー名を選択します。
- b. ポリシー名の横にある*削除*ボタンを選択します。

3. ポリシーを削除することを確認するには、[はい] を選択します。

ポリシーが削除されます。

ネットワークトラフィックのメトリックを表示する

トラフィック分類ポリシー ページから利用できる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

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

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 サービスのメトリックを表示して、ポリシーがネットワーク全体のトラフィックを正常に制限しているかどうかを確認できます。グラフのデータは、ポリシー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、メトリックが収集され、グラフによってトラフィックの傾向を理解するのに役立つ情報が提供されます。

手順

1. 構成 > 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にリストされます。

2. メトリックを表示するトラフィック分類ポリシー名を選択します。

3. *メトリック*タブを選択します。

トラフィック分類ポリシー 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メトリックのみが表示されます。

このページには次のグラフが含まれています。

- 要求レート: このグラフには、すべてのロード バランサーによって処理される、このポリシーに一致する帯域幅の量が表示されます。受信データには、すべてのリクエストのリクエスト ヘッダーと、本文データを持つ応答の本文データ サイズが含まれます。送信には、すべてのリクエストの応答ヘッダーと、応答に本文データが含まれるリクエストの応答本文データ 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。低速または大きなオブジェクト要求の場合、実際の瞬間帯域幅はこのグラフで報告される値と異なる場合があります。

- エラー応答率: このグラフは、このポリシーに一致する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。
 - 平均リクエスト期間 (エラーなし): このグラフには、このポリシーに一致する成功したリクエストの平均期間が表示されます。
 - ポリシー帯域幅の使用状況: このグラフには、すべてのロード バランサーによって処理される、このポリシーに一致する帯域幅の量が表示されます。受信データには、すべてのリクエストのリクエスト ヘッダーと、本文データを持つ応答の本文データ サイズが含まれます。送信には、すべてのリクエストの応答ヘッダーと、応答に本文データが含まれるリクエストの応答本文データ サイズが含まれます。
4. 折れ線グラフの上にカーソルを置くと、グラフの特定の部分の値のポップアップが表示されます。
5. ポリシーのすべてのグラフを表示するには、メトリック タイトルのすぐ下にある **Grafana** ダッシュボードを選択します。メトリック 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 サイズ別の書き込み要求レート: このポリシーに一致する PUT/POST/DELETE 要求のレート。個々のセルに配置すると、1 秒あたりのレートが表示されます。ホバー ビューに表示されるレートは整数カウントに切り捨てられ、バケット内にゼロ以外のリクエストがある場合は 0 と報告されることがあります。
 - オブジェクト サイズ別の読み取り要求レート: このポリシーに一致する GET/HEAD 要求のレート。個々のセルに配置すると、1 秒あたりのレートが表示されます。ホバー ビューに表示されるレートは整数カウントに切り捨てられ、バケット内にゼロ以外のリクエストがある場合は 0 と報告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します。
- a. サポート > ツール > *メトリック*を選択します。
 - b. **Grafana** セクションから トラフィック分類ポリシー を選択します。
 - c. ページの左上にあるメニューからポリシーを選択します。
 - d. グラフの上にカーソルを置くと、サンプルの日時、カウントに集計されるオブジェクト サイズ、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 ページにリストされます。

7. グラフを分析して、ポリシーがトラフィックを制限している頻度と、ポリシーを調整する必要があるかどうかを判断します。

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トランスポート層セキュリティ (TLS) 接続用の限定された暗号スイートのセットをサポートしています。

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 TLS 1.2 および TLS 1.3 をサポートしています。

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よう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の使用がサポートされている暗号のリストよりも大きくなります。暗号を構成するには、構成 > 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。



プロトコル バージョン、暗号、キー交換アルゴリズム、MAC アルゴリズムなどの TLS 構成オプションは、StorageGRIDでは構成できません。これらの設定について具体的なリクエストがある場合は、NetAppアカウント担当者にお問い合わせください。

アクティブ、アイドル、同時HTTP接続の利点

HTTP 接続の構成方法は、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。構成は、HTTP 接続がアクティブかアイドルか、または複数の同時接続があるかによって異なります。

次の種類の HTTP 接続の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でも HTTP 接続を開いたままにして、クライアント アプリケーションが開いている接続を介して後続のトランザクションを実行できるようにする必要があります。NetAppでは、アイドルHTTP接続を開いておく時間を10分までにすることを推奨します。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。

オープンおよびアイドル状態の HTTP 接続には、次のような利点があります。

- 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た時点から、StorageGRIDシステムがトランザクションを実行できる時点までのレイテンシが短縮されます。

待ち時間の短縮は、特に TCP/IP および TLS 接続を確立するために必要な時間に関して、主な利点です。

- 以前に実行された転送でTCP/IPスロースタートアルゴリズムを準備することにより、データ転送速度が向上します。
- 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クラスの障害状態を即時に通知します。

アイドル接続を開いたままにする時間を決定することは、既存の接続に関連付けられたスロースタートの利点と、内部システム リソースへの接続の理想的な割り当てとの間のトレードオフです。

アクティブHTTP接続の利点

ストレージ ノードに直接接続する場合、HTTP 接続でトランザクションが継続的に実行される場合でも、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。

接続を開いたままにしておくべき最大期間を決定することは、接続の永続性の利点と、内部システム リソースへの接続の理想的な割り当てとの間のトレードオフです。

ストレージ ノードへのクライアント接続の場合、アクティブな HTTP 接続を制限すると、次の利点が得られます。

- StorageGRIDシステム全体で最適な負荷分散を実現します。

時間の経過とともに、負荷分散の要件が変化するため、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 接続を確立すると、システムは最適な負荷分散を実行しますが、これにより、永続的な接続に関連するより貴重な利点が打ち消されます。

- クライアント アプリケーションが、使用可能なスペースを持つ 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ます。

一部のメンテナンス手順は、進行中の HTTP 接続がすべて完了した後にのみ開始されます。

ロード バランサ サービスへのクライアント接続の場合、開いている接続の期間を制限すると、一部のメンテナンス手順をすぐに開始できるようになります。クライアント接続の期間が制限されていない場合は、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には、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異なります。

同時 HTTP 接続には次のような利点があります。

- 遅延の低減

他のトランザクションが完了するのを待たずに、トランザクション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された接続を選択してすぐに使用できます。

各StorageGRIDシステムのトポロジでは、パフォーマンスが低下し始めるまでの同時トランザクションおよび接続のピーク スループットが異なります。ピーク スループットは、コンピューティング リソース、ネットワーク リソース、ストレージ リソース、WAN リンクなどの要因によって異なります。サーバーとサービスの数、およびStorageGRIDシステムがサポートするアプリケーションの数も要因となります。

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ます。クライアント アプリケーションで使用される同時接続の最大数を決定するときは、この点に留意する必要があります。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する必要があります。次の状況では、同時接続の最大数を調整する必要がある場合があります。

- 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と接続の最大数に影響します。
- 帯域幅が制限されたネットワーク経由でStorageGRIDシステムと対話するクライアント アプリケーションでは、個々のトランザクションが適切な時間内に完了するように同時実行の度合いを下げる必要がある場合があります。
- 多数のクライアント アプリケーションがStorageGRIDシステムを共有する場合、システムの制限を超えないように同時実行の度合いを下げる必要がある場合があります。

読み取り操作と書き込み操作の HTTP 接続プールの分離

読み取り操作と書き込み操作に別々の HTTP 接続プールを使用し、それぞれに使用するプールの量を制御できます。HTTP 接続の個別のプールにより、トランザクションをより適切に制御し、負荷を分散できるようになります。

クライアント アプリケーションは、取得主体 (読み取り) または保存主体 (書き込み) の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に別々の HTTP 接続プールを使用することで、各プールのどれだけを読み取りまたは書き込みトランザクション専用にするかを調整できます。

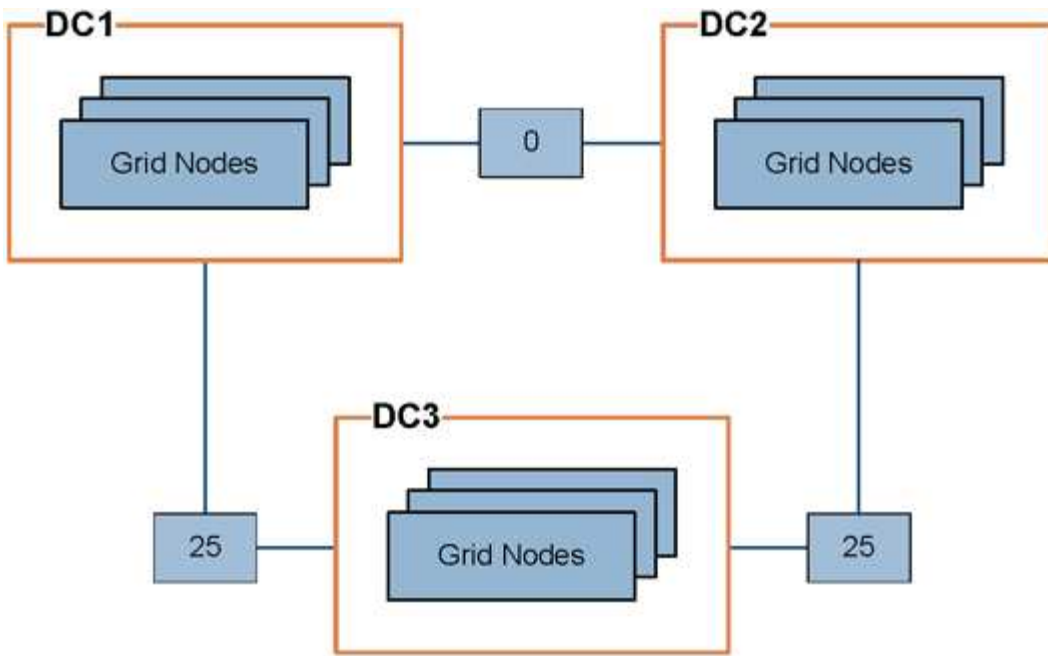
リンクコストを管理する

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 サイトを優先順位付けできます。サイト間の遅延を反映するためにリンク 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、オブジェクトの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 によって、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、管理ノードとゲートウェイ ノード上のロード バランサ サービスによってクライアント 接続を誘導するために使用されます。見る["負荷分散に関する考慮事項"](#)。

この図は、サイト間のリンク コストが構成された 3 つのサイト グリッドを示しています。



- 管理ノードとゲートウェイノード上のロードバランササービスは、同じデータセンターサイトにあり、すべてのストレージノードと、リンクコストが0であるすべてのデータセンターサイトにクライアント接続を均等に分散します。

この例では、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にある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 の両方に格納されているオブジェクトを取得する場合、DC1 から DC2 へのリンクコストが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 50 は、リンクコスト 25 よりも優先的に使用されます。この表には、一般的に使用されるリンクコストが表示されます。

リンク	リンクコスト	注記
物理データセンターサイト間	25 (デフォルト)	WAN リンクで接続されたデータセンター。
同じ物理的な場所にある論理データセンターサイト間	0	LAN で接続された同じ物理的な建物またはキャンパス内の論理データセンター。

リンクコストの更新

データセンターサイト間のリンクコストを更新して、サイト間のレイテンシを反映できます。

開始する前に

- グリッドマネージャにサインインするには、"サポートされているウェブブラウザ"。
- あなたは"グリッドトポロジページの構成権限"。

手順

1. サポート > その他 > リンク コスト 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 ソース の下でサイトを選択し、リンク先 の下に 0 から 100 までのコスト値を入力します。

送信元と宛先が同じ場合は、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。

3. *変更を適用*を選択します。

AutoSupportを使用する

AutoSupportとは何ですか？

AutoSupport機能により、StorageGRID はヘルスおよびステータス パッケージをNetAppテクニカル サポートに送信できるようになります。

AutoSupportを使用すると、問題の特定と解決が大幅に高速化されます。テクニカル サポートでは、システムのストレージのニーズを監視し、新しいノードまたは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もいたします。オプションで、AutoSupportパッケージを 1 つの追加の送信先に送信するように設定できます。

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報告します。StorageGRIDを初めてインストールすると、デフォルトで有効になります。あなたはできる["デフォルトのAutoSupport設定を変更する"](#)必要であれば。



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構成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メッセージは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。絶対です["各アプライアンスでハードウェアAutoSupportを構成する"](#)。

Active IQとは何ですか？

Active IQは、NetApp のインストールベースからの予測分析とコミュニティの知恵を活用するクラウドベースのデジタル アドバイザーです。継続的なリスク評価、予測アラート、規範的なガイダンス、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することができ、システムの健全性が向上し、システムの可用性が高まります。

NetAppサポート サイトでActive IQ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 IQDigital Advisorのドキュメント"](#)

AutoSupportパッケージに含まれる情報

AutoSupportパッケージには、次のファイルと詳細が含まれています。

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解凍サイズ + 合計収集時間（ミリ秒）	AutoSupport履歴ファイル。
AUTOSUPPORT.XML	ノード + サポートへの問い合わせプロトコル + HTTP/HTTPS のサポート URL + サポート アドレス + AutoSupport OnDemand の状態 + AutoSupport OnDemand サーバ URL + AutoSupport OnDemand のポーリング間隔	AutoSupportステータス ファイル。使用されているプロトコル、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 (有効または無効) の詳細を提供します。

ファイル名	フィールド	説明
バケット.XML	バケット ID + アカウント ID + ビルド バージョン + 場所制約設定 + コンプライアンス有効化 + コンプライアンス設定 + S3 オブジェクト ロック有効化 + S3 オブジェクト ロック設定 + 一貫性設定 + CORS 有効化 + CORS 設定 + 最終アクセス時刻有効化 + ポリシー有効化 + ポリシー設定 + 通知有効化 + 通知設定 + クラウド ミラー有効化 + クラウド ミラー設定 + 検索有効化 + 検索設定 + バケットタグ付け有効化 + バケットタグ付け設定 + バージョン設定	バケット レベルで構成の詳細と統計を提供します。バケット構成の例には、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あります。
グリッド構成.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、メタデータ予約領域、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、ILM構成）、消失訂正コーディングプロファイルの詳細、DNS名、および"NMS name"。
GRID-SPEC.XML	グリッド仕様、生のXML	StorageGRID の構成と展開に使用されます。グリッド仕様、NTP サーバー IP、DNS サーバー IP、ネットワーク ポロジ、およびノードのハードウェア プロファイルが含まれます。
グリッドタスク.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) ステータス ファイル。グリッドのアクティブ、終了、完了、失敗、および保留中のタスクの詳細を提供します。
グリッド.JSON	グリッド + リビジョン + ソフトウェアバージョン + 説明 + 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 構成の属性のリスト。

ファイル名	フィールド	説明
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 メトリック情報ファイル。各ノードの ILM 評価レートとグリッド全体のメトリックが含まれます。
ILM.XML	ILM 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、フィルター、ルール、説明など、アクティブな ILM ポリシーに関する詳細が含まれます。
ログ.TGZ	該当なし	ダウンロード可能なログ ファイル。含む `bycast-err.log` そして `servermanager.log` 各ノードから。
マニフェスト.XML	収集順序 + このデータの AutoSupport コンテンツ ファイル名 + このデータ項目の説明 + 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 + エラーの説明 + このデータの AutoSupport コンテンツタイプ	AutoSupport 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ています。
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 トポロジの詳細を提供します。ノードは、ノード上で実行されているサービスに基づいて決定できます。
オブジェクトステータス.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	オブジェクトのステータス。バックグラウンド スキャンのステータス、アクティブな転送、転送速度、合計転送数、削除率、破損したフラグメント、失われたオブジェクト、不足しているオブジェクト、試行された修復、スキャン速度、推定スキャン期間、および修復完了ステータスが含まれます。

ファイル名	フィールド	説明
サーバーステータス.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。各ノードについて、プラットフォームの種類、オペレーティング システム、インストールされているメモリ、使用可能なメモリ、ストレージの接続性、ストレージ アプライアンスの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が発生したドライブの数、コンピューティング コントローラのシャーシの温度、コンピューティング ハードウェア、コンピューティング コントローラのシリアル番号、電源、ドライブ サイズ、およびドライブの種類の詳細が含まれます。
サービスステータス.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。割り当てられた表スペース、空き表スペース、データベースの Reaper メトリック、セグメント修復期間、修復ジョブ期間、自動ジョブ再起動、自動ジョブ終了などの詳細が含まれます。
ストレージグレード.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 ノードのストレージ グレード定義ファイル。
サマリー属性.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。グリッド名、サイト名、グリッドおよびサイトあたりのストレージ ノードの数、ライセンスの種類、ライセンスの容量と使用状況、ソフトウェア サポート条件、S3 操作の詳細などの詳細を提供します。
システムアラート.XML	名前 + 重大度 + 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 + サイレンス + 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。

ファイル名	フィールド	説明
ユーザーエージェント.XML	ユーザーエージェント + 日数 + 合計 HTTP リクエスト + 取り込まれた合計バイト数 + 取得された合計バイト数 + 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 (ミリ秒) + 平均 PUT リクエスト時間 (ミリ秒) + 平均 GET リクエスト時間 (ミリ秒) + 平均 DELETE リクエスト時間 (ミリ秒) + 平均 HEAD リクエスト時間 (ミリ秒) + 平均 POST リクエスト時間 (ミリ秒) + 平均 OPTIONS リクエスト時間 (ミリ秒)	アプリケーション ユーザー エージェントに基づく統計。たとえば、ユーザーエージェントごとの PUT/GET/DELETE/HEAD 操作の数と各操作の合計バイト サイズなどです。
X-ヘッダーデータ	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。

AutoSupportを構成する

デフォルトでは、StorageGRID を初めてインストールすると、StorageGRID AutoSupport機能が有効になります。ただし、各アプライアンスでハードウェアAutoSupportを構成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。絶対です **ハードウェアAutoSupportを構成する** 各アプライアンスで。

開始する前に

- グリッドマネージャにサインインするには、**"サポートされているウェブブラウザ"**。
- あなたは**"ルートアクセス権限"**。
- AutoSupport/パッケージの送信にHTTPSを使用する場合は、プライマリ管理ノードへのアウトバウンドインターネットアクセスを直接または**"プロキシサーバーを使用する"**(着信接続は必要ありません)。
- StorageGRID AutoSupportページでHTTPを選択した場合は、**"プロキシサーバーを設定しました"** AutoSupport/パッケージを HTTPS として転送します。NetApp のAutoSupportサーバーは、HTTP を使用して送信されたパッケージを拒否します。
- AutoSupport/パッケージのプロトコルとして SMTP を使用する場合は、SMTP メール サーバーを設定します。

タスク概要

AutoSupport/パッケージをテクニカル サポートに送信するには、次のオプションを任意に組み合わせて使用できます。

- 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 時間ごとに、または重要なシステム イベントが発生したときに、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リクエストできるようにします。これは、問題に積極的に取り組んでいる場合に役立ちます (HTTPS AutoSupport転送プロトコルが必要です)。デフォルト設定: 無効。
- ユーザートリガー: いつでもAutoSupport/パッケージを手動で送信します。

AutoSupport/パッケージのプロトコルを指定します

AutoSupport/パッケージを送信するには、次のいずれかのプロトコルを使用できます。

- **HTTPS:** これは、新規インストールのデフォルトおよび推奨設定です。このプロトコルはポート 443 を使用します。あなたがしたい場合は[AutoSupport on Demand機能を有効にする](#)、HTTPS を使用する必要があります。
- **HTTP:** HTTP を選択した場合は、AutoSupport/パッケージを HTTPS として転送するようにプロキシ サーバーを構成する必要があります。NetApp のAutoSupportサーバーは、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:** AutoSupport/パッケージを電子メールで送信する場合は、このオプションを使用します。

設定したプロトコルは、すべての種類の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ます。
3. **HTTPS** を選択した場合は、テクニカル サポート サーバ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: 証明書に一時的な問題がある場合など、証明書の検証を使用しない正当な理由がある場合にのみ、このオプションを選択します。
4. *保存*を選択します。すべての毎週、ユーザーによってトリガーされる、およびイベントによってトリガーされるパッケージは、選択したプロトコルを使用して送信されます。

毎週のAutoSupportを無効にする

デフォルトでは、StorageGRIDシステムは、AutoSupport/パッケージを週に 1 回テクニカル サポートに送信するように設定されています。

毎週のAutoSupport/パッケージがいつ送信されるかを決定するには、[* AutoSupport*] > [結果] タブに移動します。*Weekly AutoSupport*セクションで、*Next Scheduled Time*の値を確認します。

毎週のAutoSupport/パッケージの自動送信はいつでも無効にできます。

手順

1. サポート > ツール > * AutoSupport* > 設定 を選択します。
2. *週次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。

イベントトリガーの**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。

オンデマンドで**AutoSupport**を有効にする

AutoSupport on Demand は、テクニカル サポートが積極的に取り組んでいる問題の解決に役立ちます。

デフォルトでは、AutoSupport on Demand は無効になっています。この機能を有効にすると、テクニカル サポートはStorageGRIDシステムにAutoSupportパッケージを自動的に送信するよう要求できるようになります。テクニカル サポートでは、AutoSupport on Demand 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*を選択します。
3. *週次AutoSupportを有効にする*チェックボックスを選択します。
4. オンデマンドの**AutoSupport**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に問い合わせ、システムでソフトウェア アップデートが利用可能かどうかを判断します。StorageGRID の修正プログラムまたは新しいバージョンが利用可能な場合は、StorageGRIDのアップグレード ページに新しいバージョンが表示されます。

必要に応じて、ソフトウェア更新のチェック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する必要があります。

手順

1. サポート > ツール > * AutoSupport* > 設定 を選択します。
2. *ソフトウェアの更新を確認する*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宛先を追加する

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 1 つの追加の宛先を指定できます。

AutoSupportパッケージの送信に使用す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](#)。



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**宛先を有効にする を選択します。
3. 以下を指定します。

ホスト名

追加のAutoSupport宛先サーバーのサーバー ホスト名または IP アドレス。



追加の目的地は 1 つだけ入力できます。

ポート

追加のAutoSupport宛先サーバーに接続するために使用されるポート。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

追加の宛先への接続を保護するために TLS 証明書が使用されるかどうか。

- 証明書検証を使用するには、[証明書の検証] を選択します。
- 証明書を検証せずにAutoSupportパッケージを送信するには、「証明書を検証しない」を選択します。

証明書に一時的な問題がある場合など、証明書の検証を使用しない正当な理由がある場合にのみ、この選択肢を選択してください。

4. *証明書の検証*を選択した場合は、次の操作を行います。
 - a. CA 証明書の場所を参照します。
 - 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、毎週、イベントによってトリガーされ、ユーザーによってトリガーされるすべての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を構成する

アプライアンスのAutoSupportはStorageGRIDハードウェアの問題を報告し、StorageGRID AutoSupportはStorageGRIDソフトウェアの問題を報告しますが、1つの例外として、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。追加の構成を必要としないSGF6112を除く各アプライアンスでAutoSupportを構成する必要があります。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で異なる方法で実装されます。

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。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、SANtricity AutoSupportを設定できます。

- SG6000およびSG5700アプライアンスの場合、["SANtricity System ManagerでAutoSupportを構成する"](#)

EシリーズアプライアンスからのAutoSupportパッケージは、プロキシによるAutoSupport配信を設定すると、StorageGRID AutoSupportに含めることができます。["SANtricity System Manager"](#)。

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故障により、["ハードウェアアラート"](#)。ベースボード管理コントローラ(BMC)を備えたStorageGRIDアプライアンスの場合、ハードウェア障害を報告するために電子メールと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"](#)

AutoSupportパッケージを手動でトリガーする

StorageGRIDシステムの問題のトラブルシューティングでテクニカルサポートを支援するために、AutoSupportパッケージの送信を手動でトリガーできます。

開始する前に

- グリッドマネージャにサインインするには、["サポートされているウェブブラウザ"](#)。
- ルートアクセスまたはその他のグリッド構成権限が必要です。

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、*ユーザーがトリガーしたAutoSupportの送信*を選択します。

StorageGRIDは、AutoSupportパッケージをNetAppサポートサイトに送信しようとしています。試行が成功すると、[結果] タブの [最新の結果] と [前回の成功時刻] の値が更新されます。問題がある場合は、「最新の結果」の値が「失敗」に更新され、StorageGRIDはAutoSupportパッケージの再送信を試行しません。



ユーザーがトリガーしたAutoSupportパッケージを送信した後、1 分後にブラウザでAutoSupportページを更新して、最新の結果にアクセスします。

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パッケージの種類に応じて異なるアクションを実行します。**SUPPORT > Tools > * AutoSupport * > Results** を選択すると、AutoSupportパッケージのステータスを確認できます。

AutoSupportパッケージの送信に失敗した場合、* 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ーを設定した場合は、"[プロキシサーバーの構成設定が正しいことを確認する](#)"。

毎週のAutoSupportパッケージの失敗

毎週の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」に更新します。
2. 1 時間にわたって 4 分ごとに 15 回、AutoSupportパッケージの再送信を試行します。
3. 送信失敗が 1 時間続くと、最新の結果属性が失敗に更新されます。
4. 次回のスケジュールされた時間にAutoSupportパッケージを再度送信しようとします。
5. NMS サービスが利用できないためにパッケージが失敗した場合、および 7 日が経過する前にパッケージが送信された場合は、通常の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ったときに、パッケージが 7 日以上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。

ユーザーまたはイベントによってトリガーされたAutoSupportパッケージの障害

ユーザーがトリガーした、またはイベントがトリガーした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. エラーが既知の場合はエラー メッセージが表示されます。たとえば、ユーザーが正しい電子メール構成設定を指定せずに SMTP プロトコルを選択した場合、次のエラーが表示されます。AutoSupport 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を試行しません。
3. エラーを記録する `nms.log`。

障害が発生し、選択されたプロトコルとして SMTP が使用されている場合は、StorageGRIDシステムの電子メールサーバーが正しく設定されており、電子メールサーバーが実行中であることを確認します (**SUPPORT > アラーム (レガシー) > レガシー電子メール セットアップ**)。AutoSupportページに次のエラー メッセージが表示される場合があります。AutoSupport 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"。

AutoSupportパッケージの障害を修正する

障害が発生し、選択されたプロトコルが SMTP である場合は、StorageGRIDシステムの電子メール サーバーが正しく構成され、電子メール サーバーが実行中であることを確認してください。AutoSupportページに次のエラー メッセージが表示される場合があります。AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.

EシリーズAutoSupportパッケージをStorageGRID経由で送信する

E シリーズSANtricity System Manager AutoSupportパッケージは、ストレージ アプライアンス管理ポートではなく、StorageGRID管理ノードを介してテクニカル サポートに送信できます。

見る ["EシリーズハードウェアAutoSupport"](#)E シリーズ アプライアンスでAutoSupportを使用する方法の詳細については、こちらをご覧ください。

開始する前に

- グリッドマネージャにサインインするには、["サポートされているウェブブラウザ"](#)。
- あなたは["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"](#)。
- 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を構成する"](#)



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 以上が必要です。

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AAutoSupport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と、アプライアンスの管理ポートを使用せずに、StorageGRID管理ノードを介してAutoSupportパッケージを転送できます。この方法で送信されるAutoSupport/パッケージは、["優先送信者管理ノード"](#)、そして彼らはどんな["管理者プロキシ設定"](#)グリッドマネージャーで構成されているもの。

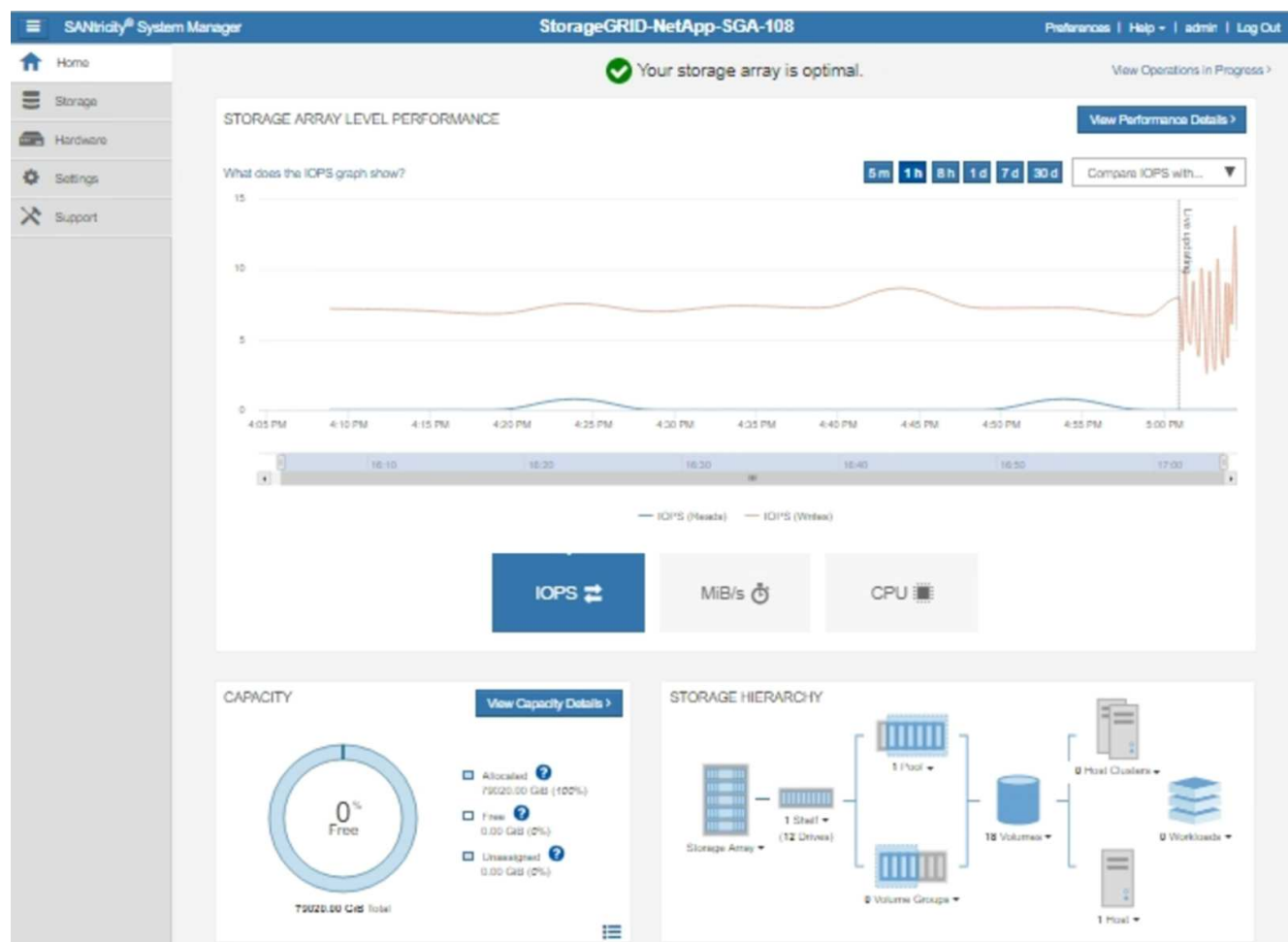


この手順は、E シリーズAutoSupportパッケージ用のStorageGRIDプロキシ サーバを構成するためだけのものです。EシリーズのAutoSupport設定の詳細については、["NetApp EシリーズおよびSANtricityのドキュメント"](#)。

手順

1. グリッド マネージャーで、**NODES** を選択します。
2. 左側のノード リストから、構成するストレージ アプライアンス ノードを選択します。
3. * SANtricity System Manager* を選択します。

SANtricity 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*を選択します。



HTTPS を有効にする証明書が事前にインストールされています。

7. *プロキシサーバー経由*を選択します。

8. 入力 tunnel-hostホストアドレス です。

`tunnel-host`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. 入力 10225ポート番号 です。

`10225`アプライアンス内の E シリーズ コントローラからAutoSupportパッケージを受信するStorageGRIDプロキシ サーバ上のポート番号です。

10. AutoSupportプロキシ サーバーのルーティングと構成をテストするには、「構成のテスト」を選択します。

正しい場合は、緑色のバナーに「AutoSupport構成が検証されました。」というメッセージが表示されます。

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"](#) NetAppサポート サイトに接続して、再度テストを実行できます。

11. *保存*を選択します。

設定が保存され、「AutoSupport配信方法が設定されました」という確認メッセージが表示されます。

ストレージノードの管理

ストレージノードの管理

ストレージ ノードは、ディスク ストレージ容量とサービスを提供します。ストレージ ノードの管理には次の作業が必要です。

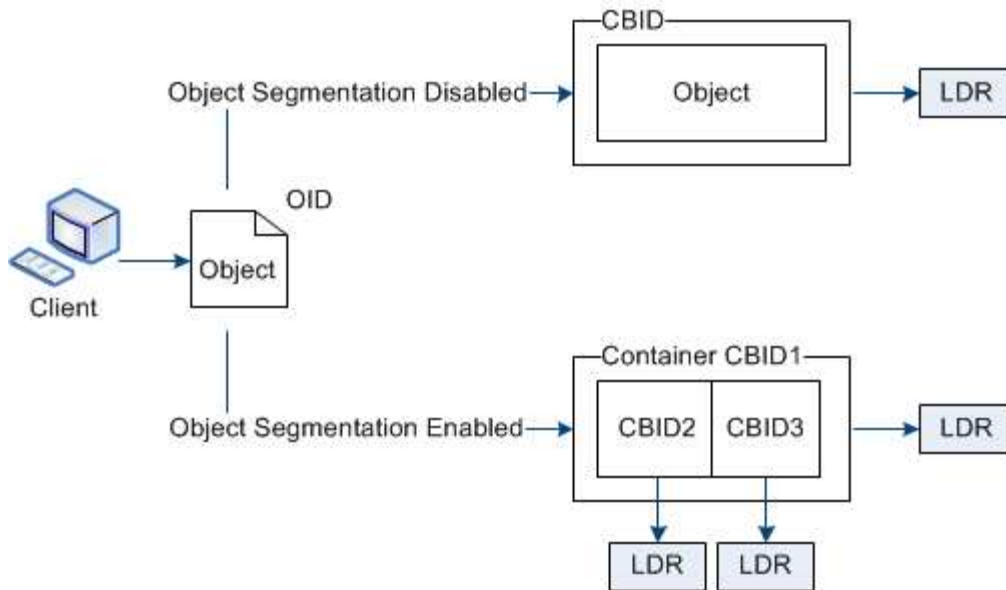
- ストレージオプションの管理
- ストレージボリュームのウォーターマークとは何か、またウォーターマークのオーバーライドを使用してストレージノードが読み取り専用になるタイミングを制御する方法を理解する
- オブジェクトメタデータに使用されるスペースの監視と管理
- 保存されたオブジェクトのグローバル設定を構成する
- ストレージノード構成設定の適用
- フルストレージノードの管理

ストレージオプションを使用する

オブジェクトセグメンテーションとは何ですか？

オブジェクト セグメンテーションは、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、オブジェクトを小さな固定サイズのオブジェクトのコレクションに分割するプロセスです。S3 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を持つ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 サービスはセグメントから元のオブジェクトを組み立て、そのオブジェクトをクライアントに返します。

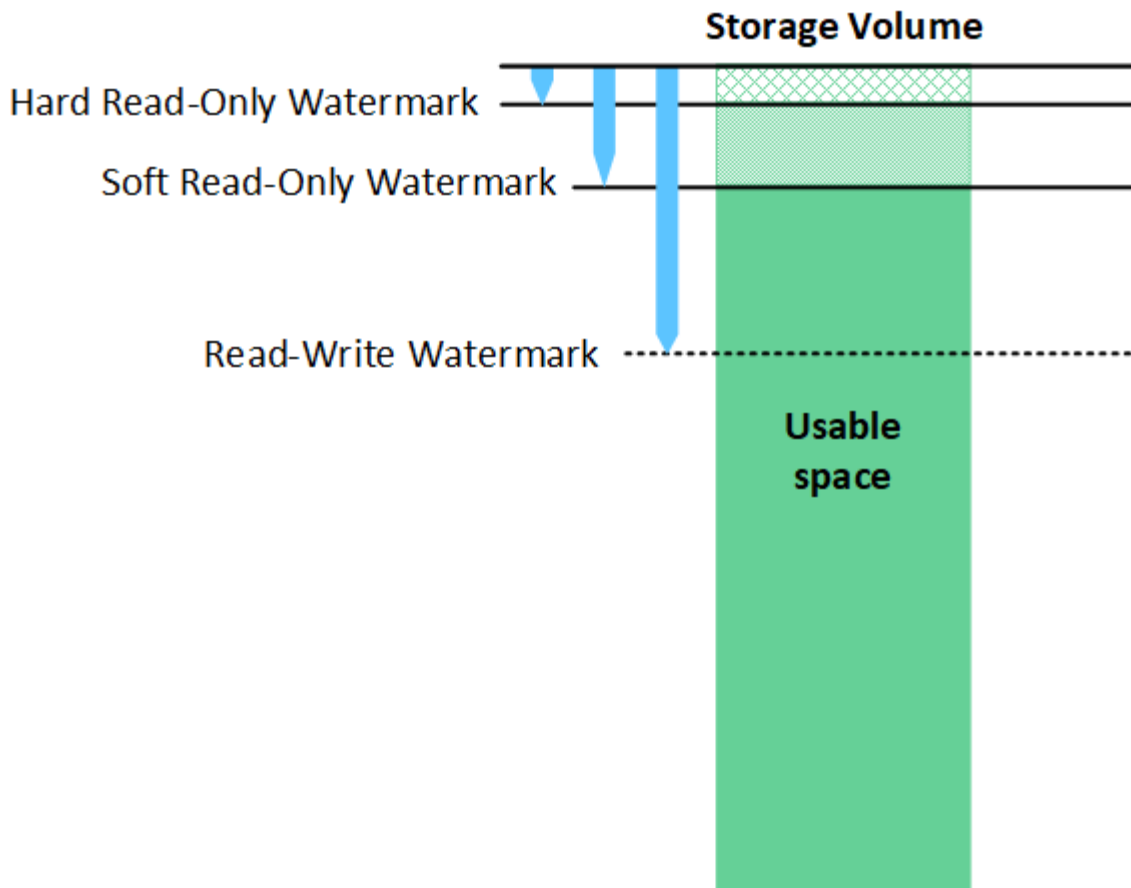
コンテナとセグメントは必ずしも同じストレージ ノードに保存されるわけではありません。コンテナとセグメントは、ILM ルールで指定されたストレージ プール内の任意のストレージ ノードに保存できます。

各セグメントはStorageGRIDシステムによって個別に処理され、管理対象オブジェクトや保存オブジェクトなどの属性の数に寄与します。たとえば、StorageGRIDシステムに保存されているオブジェクトが2つのセグメントに分割されている場合、取り込みが完了すると、管理対象オブジェクトの値は次のように3増加します。

segment container + segment 1 + segment 2 = three stored objects

ストレージ ボリューム ウォーターマークとは何ですか？

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 ノードの容量が極端に少なくなる前に、ストレージ ノードが安全に読み取り専用状態に移行されるようにし、読み取り専用状態に移行したストレージ ノードが再び読み取り/書き込み可能になるようにします。



ストレージ ボリューム ウォーターマークは、複製および消去コード化されたオブジェクト データに使用されるスペースにのみ適用されます。ボリューム0のオブジェクトメタデータ用に予約されているスペースの詳細については、"[オブジェクトメタデータストレージの管理](#)"。

ソフト読み取り専用透かしとは何ですか？

ストレージ ボリューム ソフト読み取り専用ウォーターマーク は、オブジェクト データ用のストレージ ノードの使用可能なスペース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 ノードが読み取り専用サービスをStorageGRIDシステムの残りの部分に通知しますが、保留中の書き込み要求はすべて満たすことを意味します。

たとえば、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あるとします。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透かしとは何ですか？

ストレージ ボリューム ハード読み取り専用ウォーターマーク は、オブジェクト データ用のノードの使用可能なスペース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。

ボリュームの空き領域がそのボリュームのハード読み取り専用ウォーターマークよりも少ない場合、ボリュームへの書き込みは失敗します。ただし、他のボリュームへの書き込みは、それらのボリュームの空き領域がハード読み取り専用ウォーターマークよりも少なくなるまで続行できます。

たとえば、ストレージ ノード内の各ボリュームに 5 GB のハード読み取り専用ウォーターマークがあるとして、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入れなくなります。

ハード読み取り専用ウォーターマークは常にソフト読み取り専用ウォーターマークよりも小さくなります。

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。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 ボリュームの空き領域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よりも大きい場合、ノードは自動的に読み取り/書き込み状態に戻ります。

たとえば、ストレージ ノードが読み取り専用モードに移行したとします。また、各ボリュームの読み取り/書き込みウォーターマークが 30 GB であるとして、いずれかのボリュームの空き容量が 30 GB に増加すると、ノードは再び読み取り/書き込み可能になります。

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された値を表示できます。最適化された透かしが使用されていない場合は、設定を調整できるかどうか、または調整する必要がある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。
- グリッドマネージャにサインインするには、["サポートされているウェブブラウザ"](#)。
- あなたは["ルートアクセス権限"](#)。

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表示できます。

手順

1. サポート > その他 > *ストレージのウォーターマーク*を選択します。
2. [ストレージ 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ます。
 - チェックボックスをオンにすると、ストレージ ノードのサイズとボリュームの相対容量に基づいて、すべてのストレージ ノード上のすべてのストレージ ボリュームに対して 3 つのウォーターマークすべてが最適化されます。

これはデフォルトであり、推奨される設定です。これらの値を更新しないでください。オプションとして、[最適化されたストレージの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は、カスタム (最適化されていない) 透かしが使用されます。カスタム透かし設定の使用はお勧めしません。指示に従って["トラブルシューティング 読み取り専用ウォーターマークの上書き警告"](#)設定を調整できるかどうか、または調整する必要があるかどうかを判断します。

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を表示する

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 ノードの最適化された最小値と最大値を表示できます。

1. サポート > ツール > *メトリック*を選択します。
2. Prometheus セクションで、Prometheus ユーザー インターフェースにアクセスするためのリンクを選択します。
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、[実行] を選択します。

```
storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
```

最後の列には、各ストレージ ノード上のすべてのストレージ ボリュームの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より大きい場合、ストレージ ノードに対して **Low read-only watermark override** アラートがトリガーされます。

4. 推奨される最大の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、[実行] を選択します。

```
storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
```

最後の列には、各ストレージ ノード上のすべてのストレージ ボリュームのソフト読み取り専用ウォーターマークの最適化された最大値が表示されます。

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があることを確認するには、StorageGRID がオブジェクトの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 メタデータは、オブジェクトを説明する情報です。StorageGRID はオブジェクト メタデータを使用して、グリッド全体のすべてのオブジェクトの場所を追跡し、各オブジェクトのライフサイクルを長期的にわたって管理します。

StorageGRID内のオブジェクトの場合、オブジェクト メタデータには次の種類の情報が含まれます。

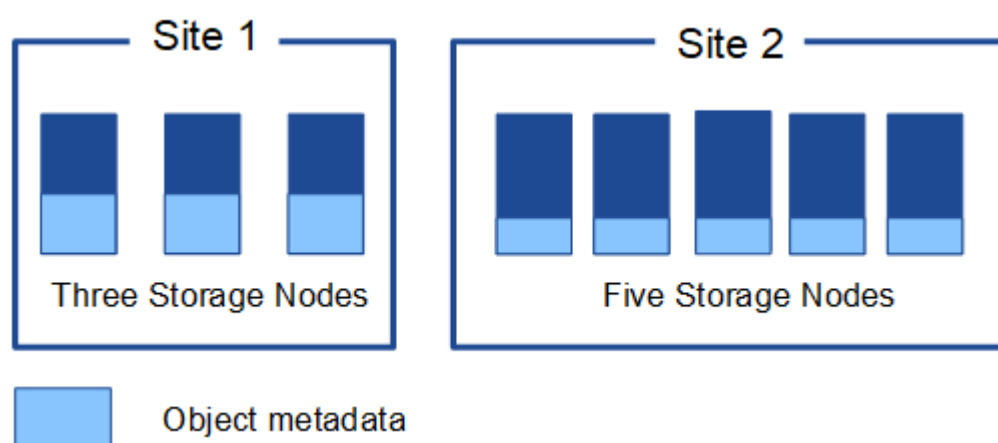
- システム メタデータには、各オブジェクトの一意の ID (UUID)、オブジェクト名、S3 バケットの名前、テナント アカウント名または ID、オブジェクトの論理サイズ、オブジェクトが最初に作成された日時、オブジェクトが最後に変更された日時が含まれます。
- オブジェクトに関連付けられたカスタム ユーザー メタデータのキーと値のペア。
- S3 オブジェクトの場合、オブジェクトに関連付けられたオブジェクト タグのキーと値のペア。
- 複製されたオブジェクトのコピーの場合、各コピーの現在の保存場所。

- 消失訂正符号化オブジェクトのコピーの場合、各フラグメントの現在の保存場所。
- Cloud Storage プール内のオブジェクト コピーの場合、外部バケットの名前とオブジェクトの一意的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とマルチパート 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 メタデータはどのように保存されますか？

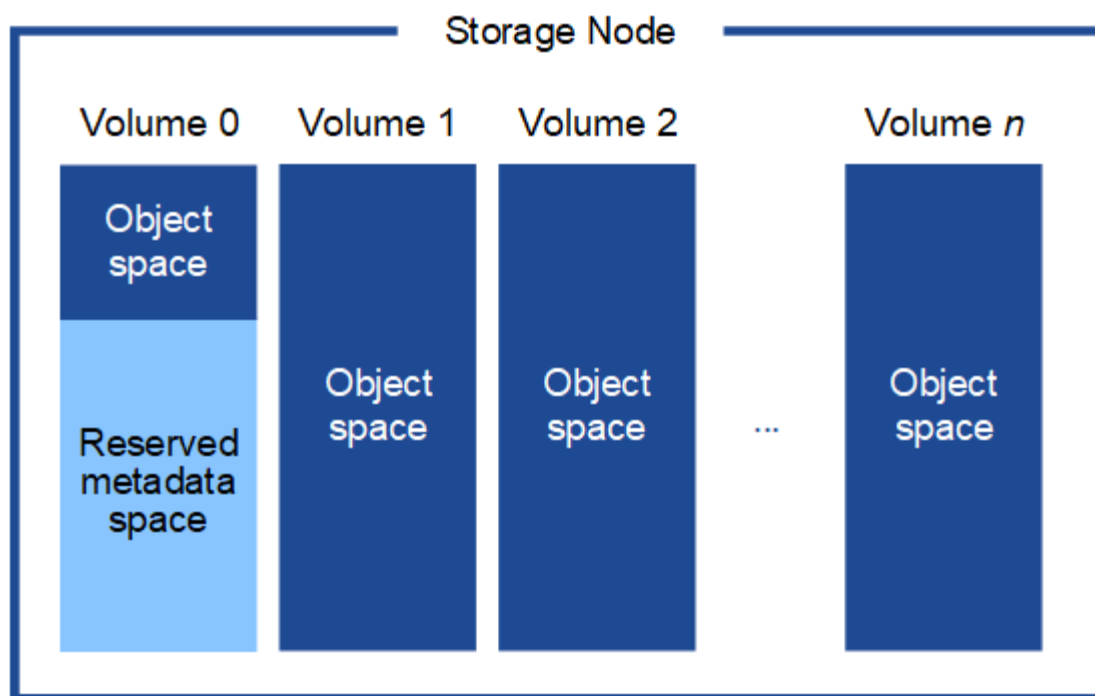
StorageGRID は、オブジェクト データとは独立して保存される Cassandra データベースにオブジェクト メタデータを維持します。冗長性を提供し、オブジェクト メタデータの損失を防ぐために、StorageGRID はシステム内のすべてのオブジェクトのメタデータのコピーを各サイトに 3 つ保存します。

この図は、2 つのサイトのストレージ ノードを表しています。各サイトには同じ量のオブジェクト メタデータがあり、各サイトのメタデータはそのサイトのすべてのストレージ ノード間で分割されます。



オブジェクト 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 メタデータ用のスペースを予約します。予約されたスペースを使用して、オブジェクトのメタデータを保存し、重要なデータベース操作を実行します。ストレージ ボリューム 0 およびストレージ ノード内の他のすべてのストレージ ボリュームの残りのスペースは、オブジェクト データ (複製されたコピーおよび消去コード化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 ノード上のオブジェクト メタデータ用に予約されるスペースの量は、以下で説明するいくつかの要因によって異なります。

メタデータ予約領域の設定

メタデータ予約済みスペース は、各ストレージ ノードのボリューム 0 上のメタデータ用に予約されるスペースの量を表すシステム全体の設定です。表に示すように、この設定のデフォルト値は次のものに基づいています。

- StorageGRIDを最初にインストールしたときに使用していたソフトウェア バージョン。
- 各ストレージ ノード上の RAM の量。

StorageGRIDの初期インストールに使用されるバージョン	ストレージノード上の RAM の量	デフォルトのメタデータ予約領域設定
11.5～11.9	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 128 GB 未満	3 TB (3,000 GB)
11.1～11.4	1 つのサイトの各ストレージ ノードに 128 GB 以上	4 TB (4,000 GB)

StorageGRIDの初期インストールに使用されるバージョン	ストレージノード上の RAM の量	デフォルトのメタデータ予約領域設定
	各サイトのストレージノード上の容量が 128 GB 未満	3 TB (3,000 GB)
11.0以前	任意の金額	2 TB (2,000 GB)

メタデータ予約領域設定の表示

StorageGRIDシステムのメタデータ予約領域設定を表示するには、次の手順に従います。

手順

1. 構成 > システム > *ストレージ設定*を選択します。
2. ストレージ設定ページで、*メタデータ予約済み領域*セクションを展開します。

StorageGRID 11.8 以降の場合、メタデータ予約領域の値は 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StorageGRID 11.6 以降の新規インストールのデフォルト設定は 8,000 GB (8 TB) です。

メタデータ用に実際に予約されたスペース

システム全体のメタデータ予約済みスペース設定とは対照的に、オブジェクト メタデータの 実際の予約済みスペース はストレージ ノードごとに決定されます。特定のストレージ ノードの場合、メタデータ用に実際に予約される領域は、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予約領域の設定によって異なります。

ノードのボリューム0のサイズ	メタデータ用に実際に予約されたスペース
500 GB未満（非本番環境用）	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: • 第0巻 • メタデータ予約領域の設定 注: メタデータのためのストレージ ノードに必要な rangedb は 1 つだけです。

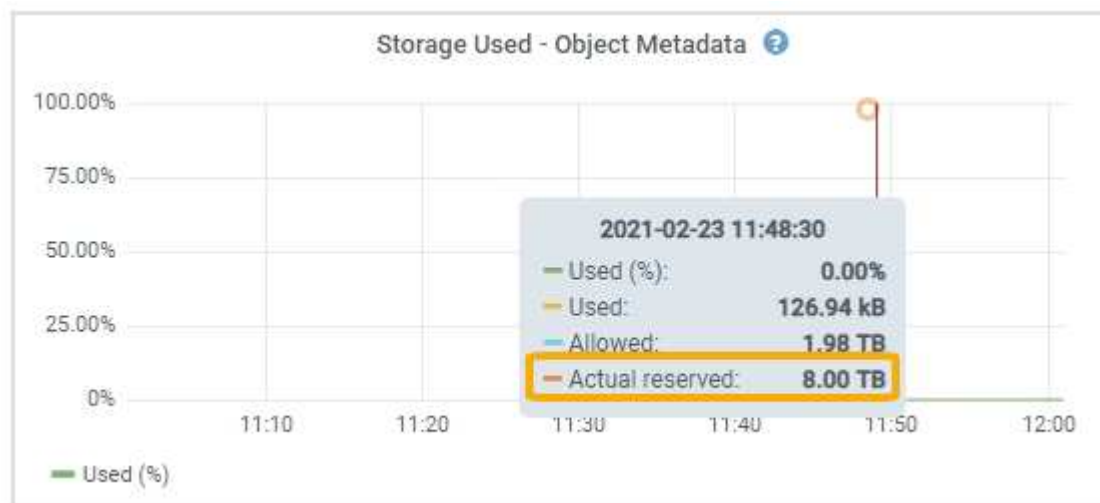
メタデータ用に実際に予約されているスペースを表示する

特定のストレージ ノード上のメタデータ用に実際に予約されている領域を表示するには、次の手順に従います。

手順

1. グリッド マネージャーから、**NODES > Storage Node** を選択します。
2. *ストレージ*タブを選択します。

3. 使用済みストレージ - オブジェクト メタデータ チャートの上にカーソルを置き、実際の予約済み の値を見つけます。



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 インストール内の大規模なストレージ ノードのものです。システム全体のメタデータ予約済み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予約済みスペースはメタデータ予約済みスペース設定と等しくなります。

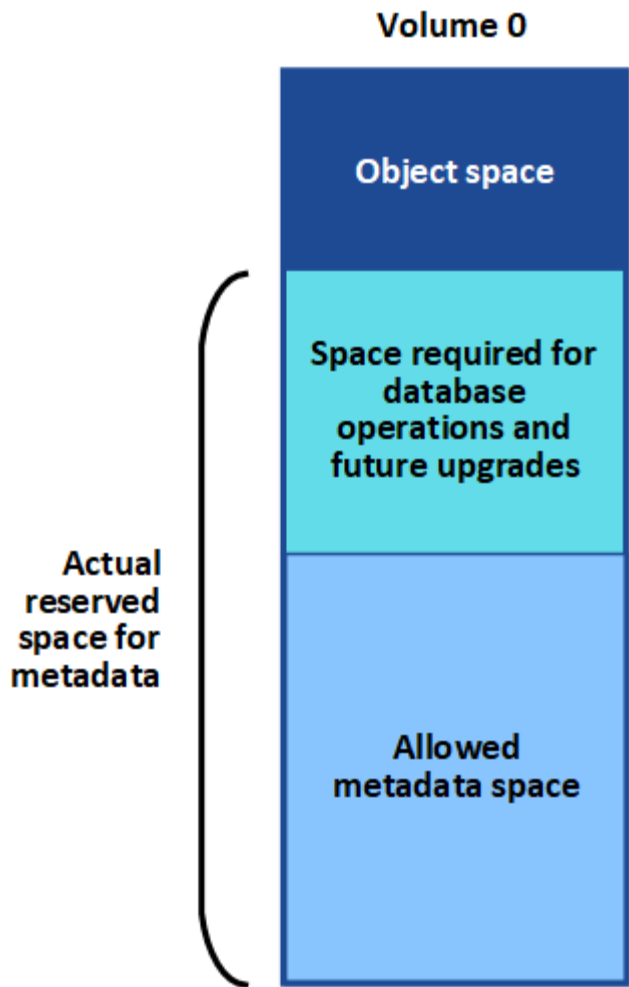
実際に予約されたメタデータ空間の例

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 があり、ストレージ ノード 1 (SN1) のボリューム 0 が 6 TB であると想定します。これらの値に基づきます:

- システム全体の*メタデータ予約領域*は 8 TB に設定されています。(各ストレージ ノードに 128 GB を超える RAM がある場合、これはStorageGRID 11.6 以降の新規インストールのデフォルト値です。)
- SN1 のメタデータ用に実際に予約されているスペースは 6 TB です。(ボリューム 0 は メタデータ予約領域 の設定よりも小さいため、ボリューム全体が予約されます。)

許可されたメタデータスペース

各ストレージ ノードのメタデータ用に実際に予約されているスペースは、オブジェクト メタデータに使用可能なスペース (許可されたメタデータ スペース) と、基本的なデータベース操作 (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スペースに分割されます。許可された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用に実際に予約された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 を計算する方法を示しています。

		ストレージノードのメモリ量	
	128 GB未満	128 GB以上	メタデータ用に実際に予約されたスペース
4 TB 以上	メタデータ用に実際に予約されているスペースの60%、最大1.32 TB	メタデータ用に実際に予約されているスペースの60%、最大1.98 TB	4TB以上

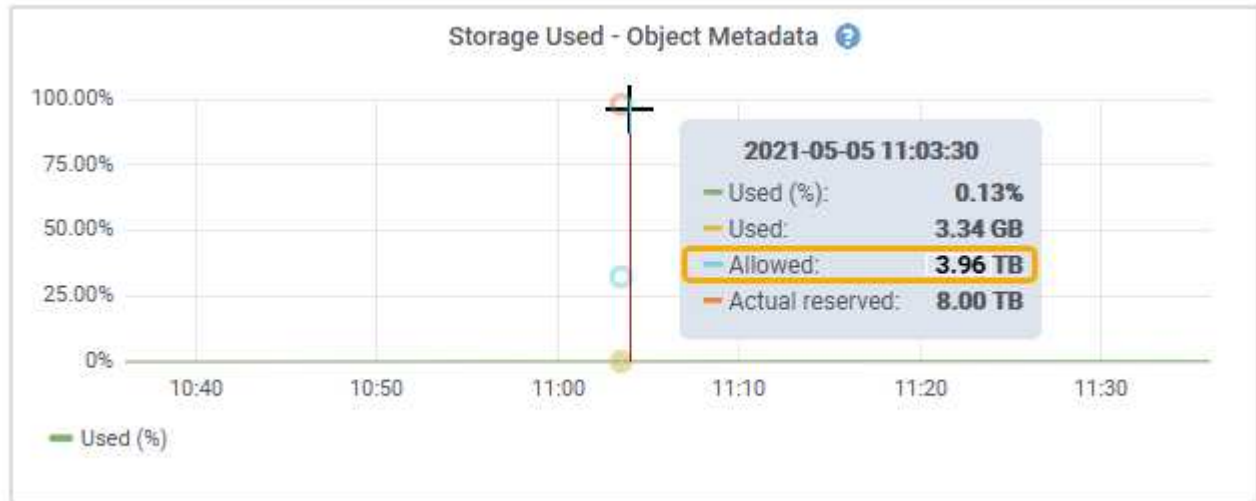
許可されたメタデータスペースを表示

ストレージ ノードに許可されているメタデータ領域を表示するには、次の手順に従います。

手順

1. グリッド マネージャーから、**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. 使用済みストレージ - オブジェクト メタデータ チャートの上にカーソルを置き、許可 値を見つけます。



スクリーンショットでは、「許可された」値は 3.96 TB です。これは、メタデータ用に実際に予約されたスペースが 4 TB を超えるストレージ ノードの最大値です。

Allowed 値は、次の Prometheus メトリックに対応します。

`storagegrid_storage_utilization_metadata_allowed_bytes`

許可された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 があり、ストレージ ノード 1 (SN1) のボリューム 0 が 6 TB であると想定します。これらの値に基づきます：

- システム全体の*メタデータ予約領域*は 8 TB に設定されています。(これは、各ストレージ ノードに 128 GB を超える RAM がある場合のStorageGRID 11.6 以降のデフォルト値です。)
- SN1 のメタデータ用に実際に予約されているスペースは 6 TB です。(ボリューム 0 は メタデータ予約領域 の設定よりも小さいため、ボリューム全体が予約されます。)
- SN1のメタデータに許容されるスペースは、以下の計算に基づいて3TBです。[メタデータに許可されたスペースの表](#):(メタデータ用に実際に予約されている領域 - 1 TB) × 60%、最大 3.96 TB。

異なるサイズのストレージノードがオブジェクト容量に与える影響

前述のように、StorageGRID は各サイトのストレージ ノード全体にオブジェクト メタデータを均等に分散します。このため、サイトに異なるサイズのストレージ ノードが含まれている場合、サイトの最小のノードによってサイトのメタデータ容量が決まります。

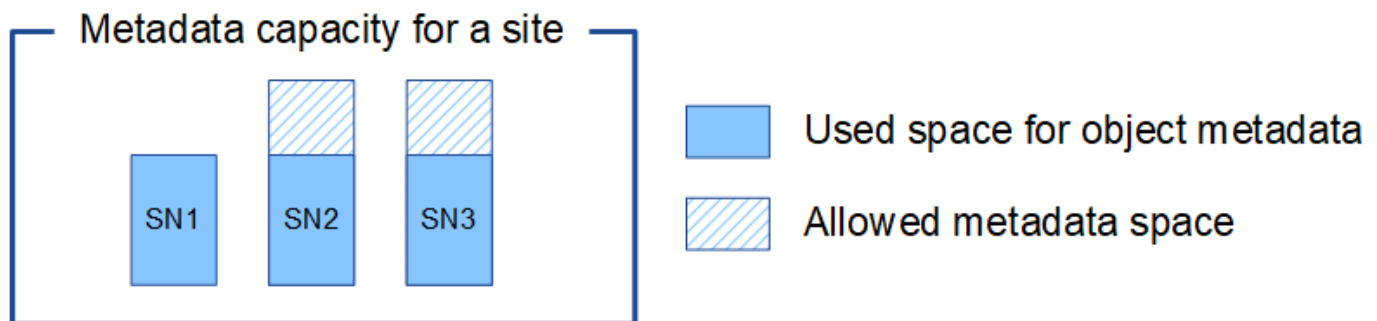
次の例を考えてみましょう。

- 異なるサイズの 3 つのストレージ ノードを含む単一サイト グリッドがあります。

- *メタデータ予約領域*の設定は 4 TB です。
- ストレージ ノードには、実際に予約されているメタデータ領域と許可されているメタデータ領域について次の値が設定されます。

ストレージ ノード	ボリュームのサイズ 0	実際に予約されているメタデータ領域	許可されたメタデータスペース
SN1	2.2 TB	2.2 TB	1.32 TB
SN2	5 TB	4 TB	1.98 TB
SN3	6 TB	4 TB	1.98 TB

オブジェクト 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 のみです。SN2 および SN3 に許可されている追加のメタデータ領域 0.66 TB 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 メタデータを維持するため、StorageGRIDシステムの全体的なメタデータ容量は、最小の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。

また、オブジェクトのメタデータ容量によって最大オブジェクト数が制御されるため、1 つのノードのメタデータ容量が不足すると、グリッドは事実上いっぱいになります。

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](#)"。
- システムのオブジェクトメタデータ容量を増やすには、"[グリッドを展開する](#)"新しいストレージノードを追加します。

メタデータ予約領域設定を増やす

ストレージ ノードが RAM と使用可能なスペースに関する特定の要件を満たしている場合は、メタデータ予約済みスペースのシステム設定を増やすことができる可能性があります。

要件

- グリッドマネージャにサインインするには、"[サポートされているウェブブラウザ](#)"。

- あなたは["ルートアクセス権限またはグリッドトポロジページ構成およびその他のグリッド構成権限"](#)。



グリッド トポロジ ページは非推奨となり、将来のリリースで削除される予定です。

タスク概要

システム全体のメタデータ予約領域設定を手動で最大 8 TB まで増やせる可能性があります。

次の両方の条件が満たされている場合にのみ、システム全体のメタデータ予約領域設定の値を増やすことができます。

- システム内のどのサイトにあるストレージ ノードにも、それぞれ 128 GB 以上の RAM が搭載されています。
- システム内のどのサイトにあるストレージ ノードでも、ストレージ ボリューム 0 に十分な空き容量があります。

この設定を増やすと、すべてのストレージ ノードのストレージ ボリューム 0 上のオブジェクト ストレージに使用可能なスペースが同時に減少することに注意してください。このため、予想されるオブジェクト メタデータの要件に基づいて、メタデータ予約領域を 8 TB 未満の値に設定することをお勧めします。



一般的に、低い値よりも高い値を使用する方が適切です。メタデータ予約領域の設定が大きすぎる場合は、後で減らすことができます。一方、後で値を増やすと、スペースを解放するためにシステムがオブジェクト データを移動する必要がある場合があります。

メタデータ予約領域設定が特定のストレージノード上のオブジェクトメタデータストレージに許可される領域にどのように影響するかの詳細については、以下を参照してください。["オブジェクトメタデータストレージの管理"](#)。

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. 構成 > システム > ストレージ オプション を選択します。
 - b. ストレージ ウォーターマーク セクションで、メタデータ予約済み領域 の値をメモします。
2. この値を増やすには、各ストレージ ノードのストレージ ボリューム 0 に十分な空き容量があることを確認してください。
 - a. 「NODES」を選択します。
 - b. グリッド内の最初のストレージ ノードを選択します。
 - c. ストレージタブを選択します。
 - d. ボリューム セクションで、`/var/local/rangedb/0` エントリを見つけます。
 - e. 使用可能な値が、使用する新しい値と現在のメタデータ予約済みスペースの値の差以上であることを確認します。

たとえば、メタデータ予約済み領域の設定が現在 4 TB で、これを 6 TB に増やしたい場合、使用可能な値は 2 TB 以上である必要があります。

- f. すべてのストレージ ノードに対してこれらの手順を繰り返します。
 - 1 つ以上のストレージ ノードに十分な空き領域がない場合は、メタデータ予約済み領域の値を増やすことはできません。以降の手順には進まないでください。

- 各ストレージ ノードのボリューム 0 に十分な使用可能領域がある場合は、次の手順に進みます。

3. 各ストレージ ノードに少なくとも 128 GB の RAM があることを確認してください。

- 「NODES」を選択します。
- グリッド内の最初のストレージ ノードを選択します。
- *ハードウェア*タブを選択します。
- メモリ使用量グラフの上にカーソルを置きます。*合計メモリ*が少なくとも 128 GB であることを確認してください。
- すべてのストレージ ノードに対してこれらの手順を繰り返します。

- 1 つ以上のストレージ ノードに使用可能な合計メモリが十分でない場合は、メタデータ予約済みスペースの値を増やすことはできません。以降の手順には進まないでください。

- 各ストレージ ノードの合計メモリが 128 GB 以上の場合は、次の手順に進みます。

4. メタデータ予約領域の設定を更新します。

- 構成 > システム > ストレージ オプション を選択します。
- [構成]タブを選択します。
- ストレージ ウォーターマーク セクションで、メタデータ予約済み領域 を選択します。
- 新しい値を入力します。

たとえば、サポートされている最大値である 8 TB を入力するには、**8000000000000** (8 の後に 12 個のゼロが続く) と入力します。

Storage Options

Overview

Configuration



Configure Storage Options
Updated: 2021-12-10 13:48:23 MST

Object Segmentation

Description	Settings
Segmentation	Enabled
Maximum Segment Size	1000000000

Storage Watermarks

Description	Settings
Storage Volume Read-Write Watermark Override	0
Storage Volume Soft Read-Only Watermark Override	0
Storage Volume Hard Read-Only Watermark Override	0
Metadata Reserved Space	8000000000000

Apply Changes


- *変更を適用*を選択します。

保存されたオブジェクトを圧縮する

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が縮小され、オブジェクトが消費するストレージが少なくなります。

開始する前に

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

タスク概要

デフォルトでは、オブジェクトの圧縮は無効になっています。圧縮を有効にすると、StorageGRID は保存時にロスレス圧縮を使用して各オブジェクトを圧縮しようとします。



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。構成された値は、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、次の点に注意してください。

- 保存されるデータが圧縮可能であることがわかっていない限り、[保存されたオブジェクトの圧縮] を選択しないでください。
- オブジェクトをStorageGRIDに保存するアプリケーションは、保存する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オブジェクトをStorageGRIDに保存する前にすでに圧縮している場合は、このオプションを選択してもオブジェクトのサイズはさらに縮小されません。
- StorageGRIDでNetApp FabricPoolを使用している場合は、「保存されたオブジェクトの圧縮」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を選択した場合、S3 クライアント アプリケーションは、返されるバイトの範囲を指定する GetObject 操作の実行を回避する必要があります。これらの「範囲読み取り」操作は、StorageGRID が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効果的に解凍する必要があるため、非効率的です。非常に大きなオブジェクトから小さな範囲のバイトを要求する GetObject 操作は特に非効率的です。たとえば、50 GB の圧縮されたオブジェクトから 10 MB の範囲を読み取るのは非効率的です。

範囲が圧縮されたオブジェクトから読み取られる場合、クライアント要求がタイムアウトする可能性があります。



オブジェクトを圧縮する必要があり、クライアント アプリケーションで範囲読み取りを使用する必要がある場合は、アプリケーションの読み取りタイムアウトを増やします。

手順

1. 構成 > システム > ストレージ設定 > *オブジェクト圧縮*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。

完全なストレージノードを管理する

ストレージ ノードの容量が限界に達したら、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。利用可能なオプションは、ストレージ ボリュームの追加、ストレージ拡張シェルフの追加、ストレージ ノードの追加の 3 つです。

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。定義される最大値はプラットフォームによって異なります。ストレージ ノードに含まれるストレージ ボリュームの数が最大数より少ない場合は、ボリュームを追加して容量を増やすことができます。説明書をご覧ください["StorageGRIDシステムの拡張"](#)。

ストレージ拡張棚を追加する

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アプライアンスがあり、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。説明書をご覧ください["StorageGRIDシステムの拡張"](#)。

ストレージノードの追加

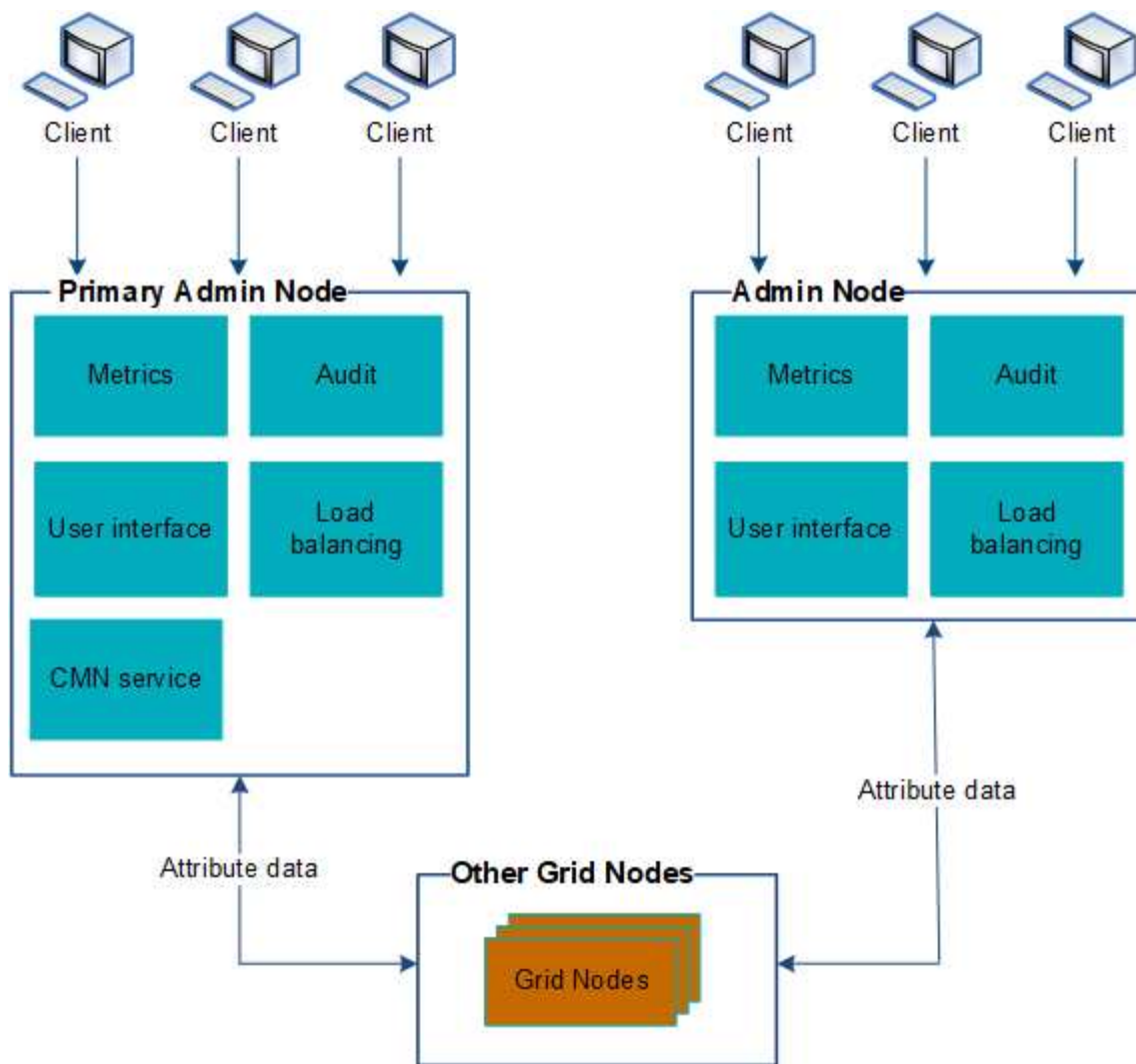
ストレージノードを追加することでストレージ容量を増やすことができます。ストレージを追加するときは、現在アクティブな ILM ルールと容量要件を慎重に考慮する必要があります。説明書をご覧ください["StorageGRIDシステムの拡張"](#)。

管理ノードの管理

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構成できます。

管理ノードが使用できなくなった場合でも、属性処理は続行され、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パッケージを除いて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でも、StorageGRIDシステムの表示と構成を続行するには、次の2つのオプションがあります。

- Web クライアントは、他の利用可能な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構成している場合、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、グリッド マネージャまたはテナント マネージャに引き続きアクセスできます。見る["高可用性グループの管理"](#)。



HA グループを使用する場合、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ールオーバーした後、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 タスクは、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、StorageGRIDシステムが再び完全に機能する前に、プライマリ管理ノードを回復する必要があります。

プライマリ管理ノードを特定する

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。たとえば、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。

ります。

管理ノードの詳細については、以下を参照してください。"管理ノードとは"。

開始する前に

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

手順

1. 「NODES」を選択します。
2. 検索ボックスに「primary」と入力します。

検索結果で、タイプ列に「プライマリ管理ノード」が表示されているノードを特定します。1つのプライマリ管理ノードがリストされる必要があります。

通知ステータスとキューを表示する

管理ノード上のネットワーク管理システム (NMS) サービスは、メール サーバーに通知を送信します。インターフェイス エンジン ページで、NMS サービスの現在のステータスと通知キューのサイズを表示できます。

インターフェイス エンジン ページにアクセスするには、サポート > ツール > グリッド トポロジ を選択します。次に、**site > Admin Node > NMS > Interface Engine** を選択します。

The screenshot displays the 'Overview: NMS (170-176) - Interface Engine' page. At the top, there are tabs for 'Overview', 'Alarms', 'Reports', and 'Configuration'. Below the tabs, the page title is 'Overview: NMS (170-176) - Interface Engine' with a timestamp 'Updated: 2009-03-09 10:12:17 PDT'. The main content area is divided into three sections:

- NMS Interface Engine Status:** Shows 'Connected' with a green status icon and 'Connected Services: 15'.
- E-mail Notification Events:** Shows 'E-mail Notifications Status: No Errors' and 'E-mail Notifications Queued: 0' with a green status icon.
- Database Connection Pool:** Shows 'Maximum Supported Capacity: 100', 'Remaining Capacity: 95 %', and 'Active Connections: 5' with a green status icon.

通知は電子メール通知キューを通じて処理され、トリガーされた順序で次々にメール サーバーに送信されます。問題 (ネットワーク接続エラーなど) が発生し、通知の送信時にメール サーバーが利用できない場合は、メール サーバーに通知を再送信するためのベスト エフォートの試行が 60 秒間継続されます。通知が 60 秒経過してもメール サーバーに送信されない場合、通知は通知キューから削除され、キュー内の次の通知の送信が試行されます。

著作権に関する情報

Copyright © 2025 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。