構成と管理
StorageGRID 11.5

NetApp
April 11, 2024

目次

構成と管理

StorageGRID の管理

StorageGRID システムの設定方法について説明します。

- "StorageGRID システムの管理"
- "StorageGRID への管理者アクセスの制御"
- "キー管理サーバを設定しています"
- "テナントの管理"
- "S3およびSwiftクライアント接続の設定"
- "StorageGRID ネットワークと接続の管理"
- "AutoSupport を設定しています"
- "ストレージノードの管理"
- "管理ノードの管理"
- "アーカイブノードの管理"
- "StorageGRID へのデータの移行"

StorageGRID システムの管理

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

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

> 情報ライフサイクル管理（ ILM ）ルールとポリシーを含むオブジェクトを管理する手順は、に移動されました"ILM を使用してオブジェクトを管理する"。

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

必要なもの

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

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	87
Microsoft Edge の場合	87
Mozilla Firefox	84

ブラウザウィンドウの幅を推奨される値に設定してください。

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

Grid Managerにサインインします

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

必要なもの

- ログインクレデンシャルが必要です。
- Grid ManagerのURLが必要です。
- 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 ブラウザでクッキーが有効になっている必要があります。
- 特定のアクセス権限が必要です。

このタスクについて

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

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

管理ノードがハイアベイラビリティ（ HA ）グループに含まれている場合は、 HA グループの仮想 IP アドレスまたは仮想 IP アドレスにマッピングされる完全修飾ドメイン名を使用して接続します。プライマリ管理ノードが使用できない場合を除いてプライマリ管理ノード上のグリッドManagerにアクセスするよう、プライマリ管理ノードをグループの優先マスターとして選択してください。

手順

1. サポートされている Web ブラウザを起動します。

2. ブラウザのアドレスバーに、 Grid Manager の URL を入力します。

   `https://FQDN_or_Admin_Node_IP/`

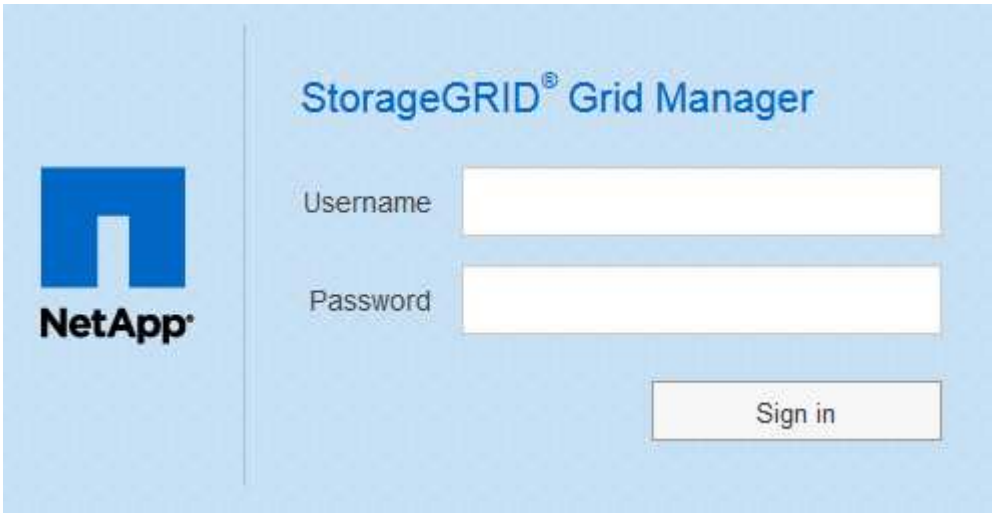
   ここで、 *FQDN_or_Admin_Node_IP* は、管理ノードの完全修飾ドメイン名またはIPアドレス、あるいは管理ノードのHAグループの仮想IPアドレスです。

   HTTPS（443）の標準ポート以外のポートでGrid Managerにアクセスする必要がある場合は、次のように入力します *FQDN_or_Admin_Node_IP* は完全修飾ドメイン名またはIPアドレス、portはポート番号です。

   `https://FQDN_or_Admin_Node_IP:port/`

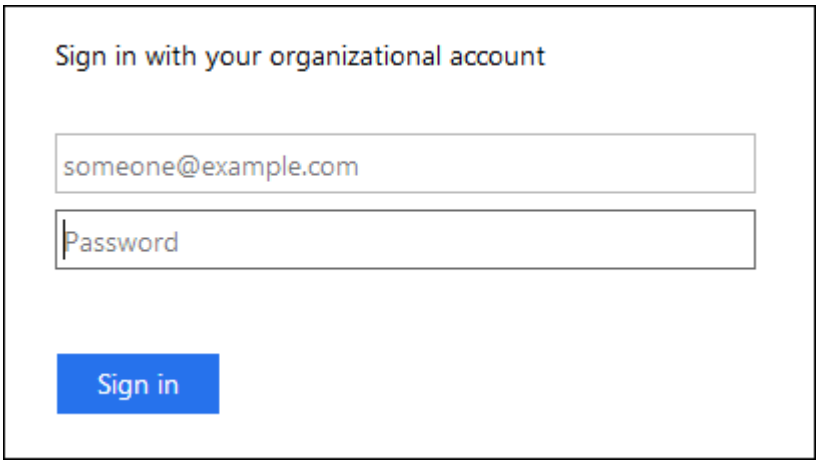
3. セキュリティアラートが表示された場合は、ブラウザのインストールウィザードを使用して証明書をインストールします。
4. Grid Manager にサインインします。

   - StorageGRID システムでシングルサインオン（ SSO ）が使用されていない場合は、次の手順を実行します。
     i. Grid Manager のユーザ名とパスワードを入力します。
     ii. [* サインイン *] をクリックします。

   - StorageGRID システムで SSO が有効になっており、このブラウザで初めて URL にアクセスした場合は、次の手順を実行します。
     i. [* サインイン *] をクリックします。[アカウント ID] フィールドは空白のままにできます。

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

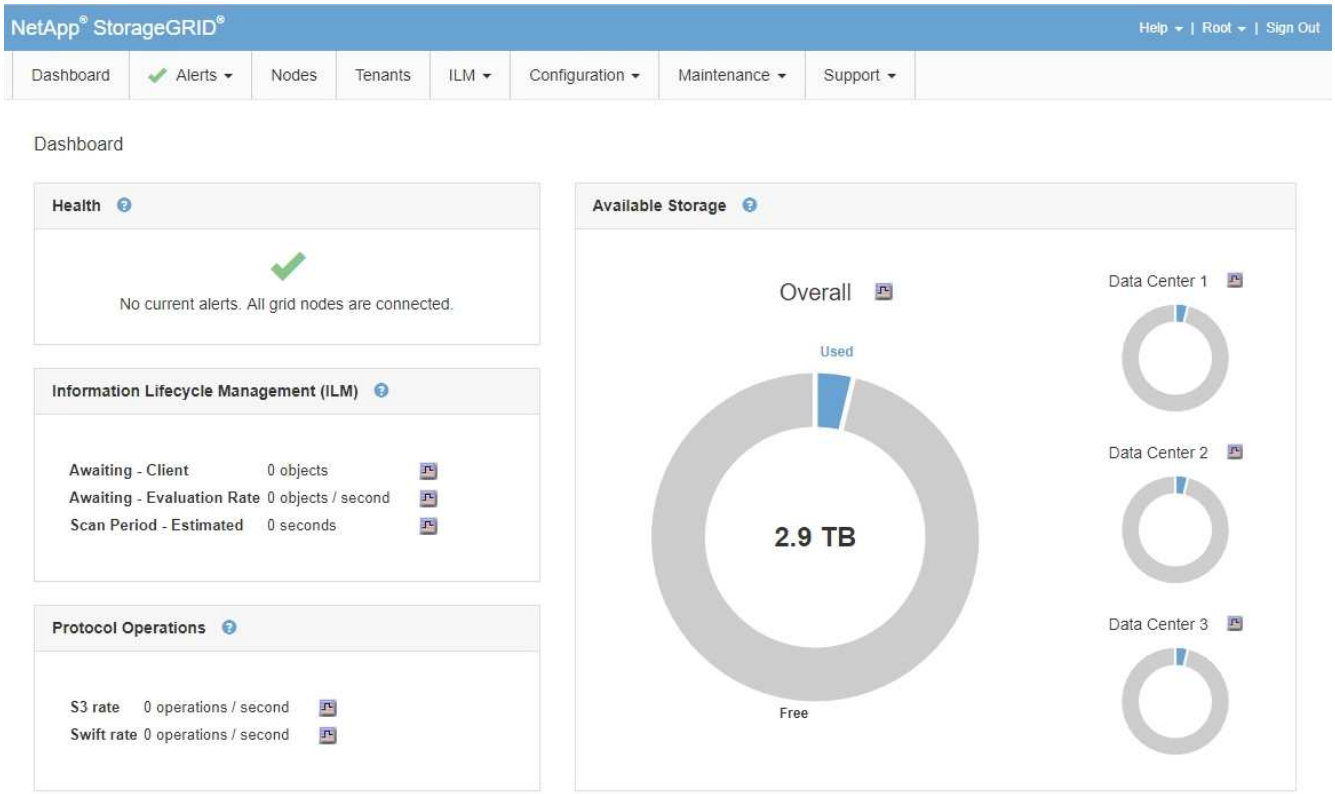


◦ StorageGRID システムで SSO が有効になっており、 Grid Manager またはテナントアカウントに以前にアクセスしたことがある場合は、次の手順を実行します。

i. 次のいずれかを実行します。

- 「* 0 *」（Grid ManagerのアカウントID）と入力し、*サインイン*をクリックします。
- 最近のアカウントのリストに* Grid Manager *が表示されている場合は、*サインイン*をクリックします。

ii. 組織の SSO サインインページで通常使用している SSO クレデンシャルを使用してサインインします。サインインすると、ダッシュボードが含まれた Grid Manager のホームページが表示されます。表示される情報については、StorageGRID の監視とトラブルシューティングの手順の「ダッシュボードの表示」を参照してください。



5. 別の管理ノードにサインインする場合は、次の手順を実行します。

オプション	手順
SSO が有効になっていない	a. ブラウザのアドレスバーに、他の管理ノードの完全修飾ドメイン名または IP アドレスを入力します。必要に応じてポート番号を追加します。 b. Grid Manager のユーザ名とパスワードを入力します。 c. [* サインイン *] をクリックします。

オプション	手順
SSO が有効です	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。 1 つの管理ノードにサインインしたら、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。ただし、 SSO セッションが期限切れになると、クレデンシャルの再入力を求められます。 • 注： SSO は制限された Grid Manager ポートでは使用できません。ユーザをシングルサインオンで認証する場合は、デフォルトの HTTPS ポート（ 443 ）を使用する必要があります。

関連情報

"Web ブラウザの要件"

"ファイアウォールによるアクセス制御"

"サーバ証明書の設定"

"シングルサインオンを設定しています"

"管理者グループの管理"

"ハイアベイラビリティグループの管理"

"テナントアカウントを使用する"

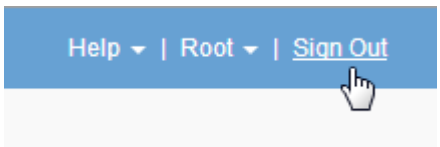
"トラブルシューティングを監視します"

Grid Managerからサインアウトします

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

手順

1. ユーザインターフェイスの右上隅にある [**Sign Out**] リンクを探します。



2. [サインアウト]をクリックします。

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

関連情報

"シングルサインオンを設定しています"

"テナントアカウントを使用する"

パスワードを変更しています

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

必要なもの

Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

このタスクについて

フェデレーテッドユーザとして StorageGRID にサインインする場合、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できません。代わりに、 Active Directory や OpenLDAP などの外部 ID ソースでパスワードを変更する必要があります。

手順

1. Grid Managerのヘッダーで、*自分の名前>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ます。
3. 新しいパスワードを入力します。

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

4. 新しいパスワードをもう一度入力します。

5. [保存（ Save ）] をクリックします。

プロビジョニングパスフレーズを変更しています

この手順 を使用して、 StorageGRID プロビジョニングパスフレーズを変更します。パスフレーズは、リカバリ、拡張、およびメンテナンスの手順で必要になります。StorageGRID システムのグリッドトポロジ情報と暗号化キーを含むリカバリパッケージのバックアップをダウンロードする場合も、パスフレーズが必要です。

必要なもの

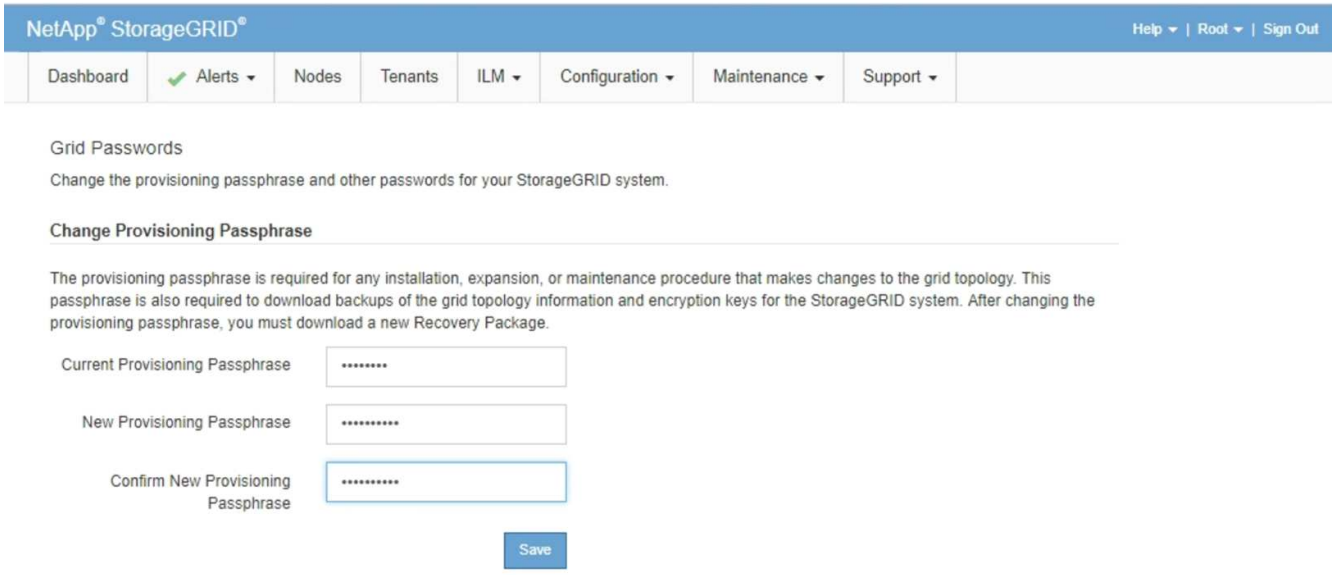
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- MaintenanceまたはRoot Access権限が必要です。
- 現在のプロビジョニングパスフレーズが必要です。

このタスクについて

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

手順

1. [構成（Configuration ）**]>[***アクセス制御（* Access Control ）**]>[** Gridパスワード*（* Grid

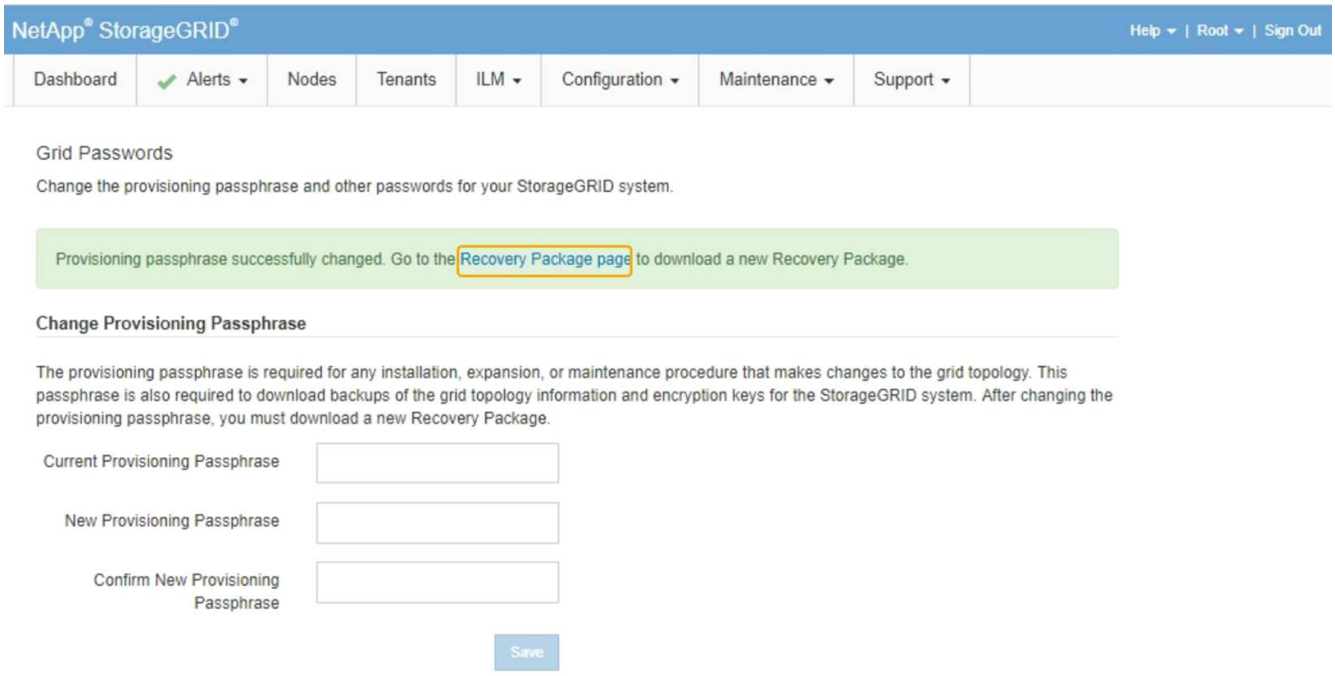


2. 現在のプロビジョニングパスフレーズを入力します。
3. 新しいリンフレーズを入力してください。パスフレーズには8文字以上32文字以下の文字列を含める必要があります。パスフレーズでは大文字と小文字が区別されます。

> 新しいプロビジョニングパスフレーズを安全な場所に保存します。インストール、拡張、およびメンテナンスの手順を実行する必要があります。

4. 新しいパスフレーズをもう一度入力し、*保存*をクリックします。

プロビジョニングパスフレーズの変更が完了すると、成功を示す緑のバナーが表示されます。変更には1分未満かかります。



5. 成功バナー内の*リカバリパッケージページ*リンクを選択します。
6. Grid Manager から新しいリカバリパッケージをダウンロードします。[* Maintenance **>]>[** Recovery Package]を選択し、新しいプロビジョニングパスフレーズを入力します。

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

ブラウザセッションのタイムアウトを変更する

Grid Manager ユーザと Tenant Manager ユーザが一定期間非アクティブになった場合にサインアウトするかどうかを制御できます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

このタスクについて

GUI の非アクティブ時のタイムアウトのデフォルト値は 900 秒（ 15 分）です。ユーザのブラウザセッションがこの時間以上アクティブでない場合、セッションはタイムアウトします。

必要に応じて、 GUI の Inactivity Timeout 表示オプションを設定して、タイムアウト時間を増減できます。

シングルサインオン（SSO）が有効になっていて、ユーザーのブラウザーセッションがタイムアウトした場合、システムはユーザーが手動で「サインアウト」をクリックしたかのように動作します。StorageGRID に再度アクセスするには、ユーザが SSO クレデンシャルを再入力する必要があります。

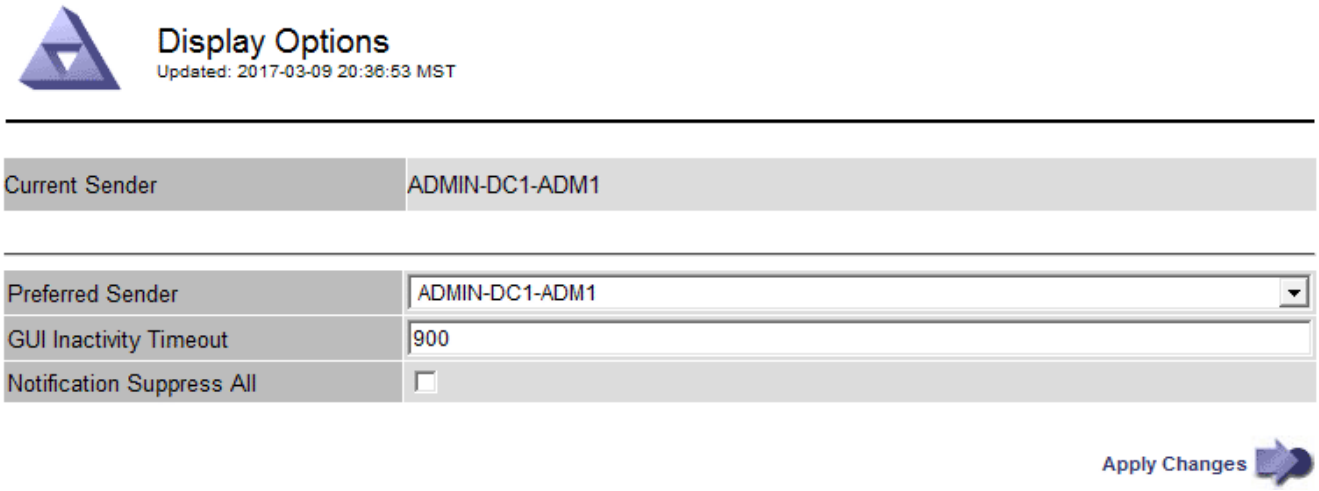
ユーザセッションのタイムアウトは、次の方法でも制御できます。

- システムセキュリティ用の、個別の設定不可能な StorageGRID タイマー。デフォルトでは、各ユーザの認証トークンはユーザがサインインしてから 16 時間後に期限切れになります。ユーザの認証が期限切れになると、 GUI の非アクティブ時のタイムアウト値に達していなくても、そのユーザは自動的にサインアウトされます。トークンを更新するには、再度サインインする必要があります。
- SSO が有効になっている StorageGRID では、アイデンティティプロバイダのタイムアウト設定が使用されます。

手順

1. * Configuration > System Settings > Display Options *を選択します。
2. * GUI の非アクティブ時のタイムアウト * には、 60 秒以上のタイムアウト時間を入力します。

   この機能を使用しない場合は、このフィールドを 0 に設定します。ユーザは、サインインしてから 16 時間後、認証トークンが期限切れになった時点でサインアウトされます。



3. [変更の適用 *] をクリックします。

   新しい設定は、現在サインインしているユーザには影響しません。新しいタイムアウト設定を有効にするには、ユーザが再度サインインするか、ブラウザを更新する必要があります。

関連情報

"シングルサインオンの仕組み"

"テナントアカウントを使用する"

StorageGRID ライセンス情報の表示

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

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

このタスクについて

この StorageGRID システムのソフトウェアライセンスを含む問題 がある場合、ダッシュボードのヘルスパネルにはライセンスステータスアイコンと * ライセンス * リンクが表示されます。この数値は、ライセンス関連の問題の数を示しています。

ステップ

ライセンスを表示するには、次のいずれかを実行します。

- ダッシュボードの正常性パネルで、ライセンスステータスアイコンまたは*ライセンス*リンクをクリックします。このリンクは、ライセンスを持つ問題 が存在する場合にのみ表示されます。
- [* Maintenance ** System * License（メンテナンス*システム*ライセンス）]を選択します。

ライセンスページが表示され、現在のライセンスに関する次の読み取り専用情報が提供されます。

- StorageGRID システム ID 。この StorageGRID インストールの一意の ID 番号です
- ライセンスのシリアル番号
- グリッドのライセンスが付与されているストレージ容量
- ソフトウェアライセンスの終了日
- サポートサービス契約の終了日
- ライセンステキストファイルの内容

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

StorageGRID ライセンス情報を更新しています

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

必要なもの

- StorageGRID システムに適用する新しいライセンスファイルが必要です。
- 特定のアクセス権限が必要です。
- プロビジョニングパスフレーズが必要です。

手順

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

   新しいライセンスファイルが検証され、表示されます。

5. [保存（ Save ）] をクリックします。

グリッド管理**API**を使用する

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

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

トップレベルのリソース

グリッド管理 API で使用可能な最上位のリソースは次のとおりです。

- `/grid`：Grid Managerユーザのみがアクセスでき、設定されているグループ権限に基づいてアクセスが制限されます。
- `/org`：テナントアカウントのローカルまたはフェデレーテッドLDAPグループに属するユーザのみがアクセスできます。詳細については、テナントアカウントの使用に関する情報を参照してください。
- `/private`：Grid Managerユーザのみがアクセスでき、設定されているグループ権限に基づいてアクセスが制限されます。これらのAPIは内部使用のみを目的としており、正式にドキュメント化されていません。また、これらのAPIは予告なく変更される場合があります。

関連情報

"テナントアカウントを使用する"

"Prometheus：クエリの基本"

グリッド管理 **API** の処理

グリッド管理 API では、使用可能な API 処理が次のセクションに分類されます。

- *accounts * — 新規アカウントの作成や特定の使用状況の取得など ' ストレージ・テナント・アカウントを管理するためのオペレーション
- * alarms * - 現在のアラーム（レガシーシステム）をリストし、現在のアラートやノード接続状態の概要など、グリッドの健全性に関する情報を返す処理。
- *alert-history * — 解決済みアラートに関する操作。
- *alert-Receiver * — アラート通知受信者（電子メール）に関する操作。
- *alert-rules * — アラートルールに関する操作
- *alert-silences *-- アラートのサイレンスに関するオペレーション。
- * alerts * — アラートの処理。
- * audit * — 監査構成をリストおよび更新する処理。
- **auth** — ユーザセッション認証を実行するための操作。

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

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

  認証セキュリティの向上については、「クロスサイトリクエストフォージェリに対する保護」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設定する処理。
- **config** — 製品リリースと Grid Management API のバージョンに関連する操作。製品のリリースバージョンおよびそのリリースでサポートされているグリッド管理 API のメジャーバージョンをリストし、廃止されたバージョンの API を無効にすることができます。
- * deactivated-features * — 非アクティブ化された可能性のある機能を表示する操作。
- *dns-servers * — 設定済みの外部 DNS サーバをリストおよび変更する処理。
- * endpoint-domain-names * — エンドポイントドメイン名をリストおよび変更する処理。
- * erasure-coding * — イレイジャーコーディングプロファイルに対する処理。
- *expansion *-- 拡張の操作 (プロシージャレベル) 。
- * expansion-nodes * - 拡張処理（ノードレベル）。
- * expansion-sitites * — 拡張の操作（サイトレベル）。
- * grid-networks * — グリッドネットワークリストをリストおよび変更する処理。
- * grid-password* - 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、フェデレーテッドグリッド管理者グループを外部 LDAP サーバから取得するための処理。
- * identity-source * — 外部のアイデンティティソースを設定する処理、およびフェデレーテッドグループとユーザ情報を手動で同期する処理。

- *ilm * — 情報ライフサイクル管理 (ILM; 情報ライフサイクル管理) の操作。
- **license** — StorageGRID ライセンスを取得および更新する処理。
- **logs** — ログファイルを収集してダウンロードするための操作。
- * メトリクス * — ある時点での瞬時の指標クエリや、一定期間にわたる指標クエリなど、 StorageGRID メトリックに対する処理。グリッド管理 API は、バックエンドのデータソースとして Prometheus システム監視ツールを使用します。Prometheus クエリの構築については、 Prometheus の Web サイトを参照してください。

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

- * node-health * - ノードのヘルスステータスに関する処理。
- *ntp-servers * — 外部ネットワークタイムプロトコル（ NTP ）サーバをリストまたは更新する処理。
- * objects * — オブジェクトおよびオブジェクトメタデータに対する処理。
- **recovery** — リカバリ手順 の処理。
- * recovery-package * — リカバリパッケージをダウンロードする処理。
- *regions * — 領域の表示と作成のための操作。
- *s3-object-lock * — グローバルな S3 オブジェクトロック設定に対する処理。
- *server-certificate * — Grid Manager サーバ証明書を表示および更新する処理。
- *snmp * — 現在の SNMP 設定に対する操作。
- *traffic-classes *-- トラフィック分類ポリシーの操作。
- *untrusted-client-network * — 信頼されていないクライアントネットワーク構成に対する操作。
- * users * — Grid Manager ユーザーを表示および管理する操作。

API要求の実行

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

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

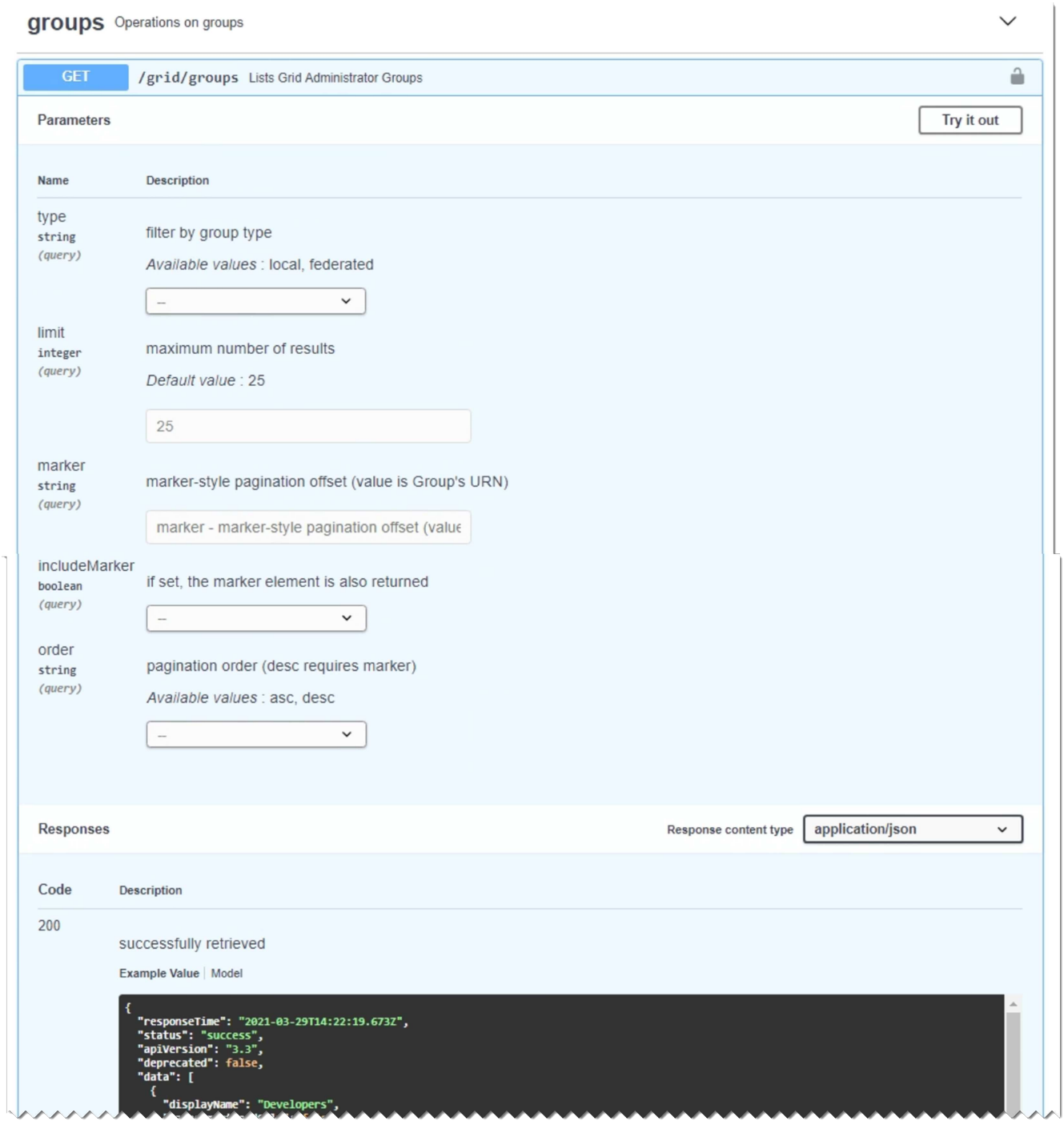
> API Docs Web ページを使用して実行する API 処理はすべてその場で実行されます。設定データやその他のデータを誤って作成、更新、または削除しないように注意してください。

手順

1. Grid Managerヘッダーから* Help > API Documentation *を選択します。
2. 目的の処理を選択します。

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

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



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

9. 応答コードを確認し、要求が成功したかどうかを判断します。

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

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

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

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

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

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

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

古い要求は、次の方法で廃止とマークされます。

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

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

現在のリリースでサポートされている**API**バージョンを確認します

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

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

要求の**API**バージョンの指定

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

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

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

クロスサイトリクエストフォージェリ（**CSRF**）の防止

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

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

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

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

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

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

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

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

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

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

シングルサインオンが有効な場合は、**API**を使用します

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、標準の認証API要求を使用してグリッド管理APIまたはテナント管理APIにサインインおよびサインアウトすることはできません。

シングルサインオンが有効な場合は、**API**へのサインイン

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で有効なAD FSから認証トークンを取得するための一連のAPI要求を問題 で処理する必要があります。

必要なもの

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

このタスクについて

認証トークンを取得するには、次のいずれかの例を使用します。

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

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

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

URLエンコード問題 がある場合は、「Unsupported SAML version」というエラーが表示される可能性があり

ます。

手順

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

   プロンプトが表示されたら、次の引数の値を入力します。

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

   [+]
   ```
   python3 /tmp/storagegrid-ssoauth.py
   saml_user: my-sso-username
   saml_domain: my-domain
   sg_address: storagegrid.example.com
   tenant_account_id: 12345
   Enter the user's SAML password:
   ********************************************************************************

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

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

3. cURL 要求を使用する場合は、次の手順 を使用します。

   a. サインインに必要な変数を宣言します。

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

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

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

次の例は、の署名付き認証URLに対するPOST要求を示しています `TENANTACCOUNTID`。結果は python-m json ツールに渡され、 JSON エンコードが削除されます。

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

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

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

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

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

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

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

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

応答にはクライアント要求 ID が含まれています。

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

e. 応答からクライアント要求 ID を保存します。

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

f. 前の応答のフォームアクションにクレデンシャルを送信します。

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

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

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

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

g. を保存します `MSISAuth` 応答からのCookie。

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

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

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

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

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

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

i. を保存します `SAMLResponse` 非表示フィールドから：

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

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

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

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

応答には認証トークンが含まれています。

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

a. 認証トークンを応答にという名前で保存します `MYTOKEN`。

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

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

シングルサインオンが有効な場合は、**API**からのサインアウト

シングルサインオン（ SSO ）が有効になっている場合は、グリッド管理 API またはテナント管理 API からサインアウトするための一連の API 要求を問題 で処理する必要があります。

このタスクについて

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

手順

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

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

ログアウト URL が返されます。

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

2. ログアウト URL を保存します。

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

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

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

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

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

4. StorageGRID Bearer トークンを削除します。

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

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

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

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

StorageGRID セキュリティ証明書を使用する

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セキュアで信頼された接続の確立に使用される小さいデータファイルです。

StorageGRID では、 2 種類のセキュリティ証明書が使用されます。

- * HTTPS 接続を使用する場合は、サーバー証明書 * が必要です。サーバ証明書は、クライアントとサーバ間のセキュアな接続を確立し、クライアントに対するサーバの ID を認証し、データのセキュアな通信パスを提供するために使用されます。サーバとクライアントには、それぞれ証明書のコピーがあります。
- * クライアント証明書 * は、クライアントまたはユーザー ID をサーバーに対して認証し、パスワードだけではなく、より安全な認証を提供します。クライアント証明書はデータを暗号化しません。

クライアントが HTTPS を使用してサーバに接続すると、サーバはサーバ証明書を返します。このサーバ証明書には公開鍵が含まれています。クライアントは、サーバの署名と証明書のコピーの署名を比較して、この証明書を検証します。署名が一致した場合、クライアントは同じ公開鍵を使用してサーバとのセッションを開始します。

StorageGRID は、一部の接続（ロードバランサエンドポイントなど）のサーバとして、または他の接続（ CloudMirror レプリケーションサービスなど）のクライアントとして機能します。

外部の認証局（ CA ）は、組織の情報セキュリティポリシーに完全に準拠した問題 カスタム証明書を作成できます。StorageGRID には、システムのインストール時に内部CA証明書を生成するCAも組み込まれています。デフォルトでは、これらの内部CA証明書を使用して、内部StorageGRID トラフィックが保護されます。非本番環境では内部CA証明書を使用できますが、本番環境では外部の認証局が署名したカスタム証明書を使用することを推奨します。証明書なしのセキュアでない接続もサポートされますが、推奨されません。

- カスタム CA 証明書では内部証明書は削除されませんが、カスタム証明書にはサーバ接続の検証用の証明書を指定する必要があります。
- すべてのカスタム証明書が、サーバ証明書のシステム強化ガイドラインを満たしている必要があります。

  "システムの保護対策"

- StorageGRID では、 CA からの証明書を 1 つのファイル（ CA 証明書バンドル）にバンドルすることがサポートされています。

> StorageGRID には、すべてのグリッドで同じオペレーティングシステムの CA 証明書も含まれています。本番環境では、オペレーティングシステムの CA 証明書の代わりに、外部の認証局によって署名されたカスタム証明書を指定してください。

サーバ証明書とクライアント証明書のタイプのバリエーションは、いくつかの方法で実装されます。システムを設定する前に、特定の StorageGRID 構成に必要なすべての証明書を準備しておく必要があります。

証明書	証明書のタイプ	説明	ナビゲーションの場所	詳細
管理者クライアント証明書	クライアント	StorageGRID が外部クライアントアクセスを認証できるように、各クライアントにインストールします。 • 許可された外部クライアントから StorageGRID Prometheus データベースにアクセスできるようにします。 • 外部ツールを使用して StorageGRID をセキュアに監視できます。	設定>*アクセス制御*>*クライアント証明書*	"管理者クライアント証明書の設定"
アイデンティティフェデレーション証明書	サーバ	StorageGRID と外部のActive Directory、OpenLDAP、またはOracle Directory Server間の接続が認証されます。アイデンティティフェデレーションに使用され、管理者グループとユーザを外部システムで管理できます。	設定>*アクセス制御*>*アイデンティティフェデレーション*	"アイデンティティフェデレーションを使用する"
シングルサインオン（ SSO ）証明書	サーバ	シングルサインオン（SSO）要求に使用されるActive Directoryフェデレーションサービス（AD FS）とStorageGRID 間の接続を認証します。	環境設定>*アクセスコントロール*>*シングルサインオン*	"シングルサインオンを設定しています"

証明書	証明書のタイプ	説明	ナビゲーションの場所	詳細
キー管理サーバ（ KMS ）の証明書	サーバとクライアント	StorageGRID と外部キー管理サーバ（ KMS ）の間の接続を認証します。この接続により、 StorageGRID アプライアンスノードに暗号化キーが提供されます。	構成>*システム設定*>*キー管理サーバ*	"キー管理サーバの追加（KMS）"
E メールアラート通知の証明書	サーバとクライアント	アラート通知に使用される SMTP E メールサーバと StorageGRID 間の接続を認証します。 • SMTP サーバとの通信に Transport Layer Security （ TLS ）が必要な場合は、 E メールサーバの CA 証明書を指定する必要があります。 • SMTP E メールサーバで認証用のクライアント証明書が必要な場合にのみ、クライアント証明書を指定してください。	アラート>*電子メールの設定*	"トラブルシューティングを監視します"

証明書	証明書のタイプ	説明	ナビゲーションの場所	詳細
ロードバランサエンドポイントの証明書	サーバ	S3またはSwiftクライアントとゲートウェイノードまたは管理ノード上のStorageGRID ロードバランササービスの間の接続を認証します。ロードバランサエンドポイントを設定する際に、ロードバランサ証明書をアップロードまたは生成します。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読み出す際にロードバランサ証明書を使用します。 *注：*ロードバランサ証明書は、通常のStorageGRID 処理で最も使用される証明書です。	設定>*ネットワーク設定*>*ロードバランサエンドポイント*	• "ロードバランサエンドポイントの設定" • FabricPool のロードバランサエンドポイントの作成 "StorageGRID for FabricPool を設定します"
管理インターフェイスのサーバ証明書	サーバ	クライアントの Web ブラウザと StorageGRID 管理インターフェイスの間の接続を認証することで、ユーザがセキュリティの警告なしで Grid Manager とテナントマネージャにアクセスできるようにします。 この証明書は、 Grid 管理 API 接続とテナント管理 API 接続も認証します。 内部のCA証明書を使用するか、カスタム証明書をアップロードすることができます。	構成>*ネットワーク設定*>*サーバー証明書*	• "サーバ証明書の設定" • "Grid ManagerおよびTenant Manager用のカスタムサーバ証明書を設定する"

証明書	証明書のタイプ	説明	ナビゲーションの場所	詳細
クラウドストレージプールのエンドポイントの証明書	サーバ	StorageGRID クラウドストレージプールから外部ストレージ（S3 GlacierやMicrosoft Azure BLOBストレージなど）への接続を認証します。クラウドプロバイダのタイプごとに別の証明書が必要です。	• ilm >*ストレージ・プール	"ILM を使用してオブジェクトを管理する"
プラットフォームサービスのエンドポイント証明書	サーバ	StorageGRID プラットフォームサービスから S3 ストレージリソースへの接続を認証します。	• Tenant Manager * > * storage （ S3 ） * > * Platform services endpoints *	"テナントアカウントを使用する"
Object Storage API Service Endpoint Server証明書	サーバ	ストレージノード上のLocal Distribution Router（LDR）サービスまたはゲートウェイノード上の廃止されたConnection Load Balancer（CLB）サービスへのセキュアなS3またはSwiftクライアント接続を認証します。	設定>*ネットワーク設定*>*ロードバランサエンドポイント*	"ストレージノードまたはCLBサービスへの接続用のカスタムサーバ証明書を設定する"

例 **1** ：ロードバランササービス

この例では、 StorageGRID がサーバとして機能します。

1. ロードバランサエンドポイントを設定し、 StorageGRID でサーバ証明書をアップロードまたは生成します。
2. S3 または Swift クライアント接続をロードバランサエンドポイントに設定し、同じ証明書をクライアントにアップロードします。
3. クライアントは、データを保存または取得する際に HTTPS を使用してロードバランサエンドポイントに接続します。
4. StorageGRID は、公開鍵を含むサーバ証明書と、秘密鍵に基づく署名を返します。
5. クライアントは、サーバの署名と証明書のコピーの署名を比較して、この証明書を検証します。署名が一致した場合、クライアントは同じ公開鍵を使用してセッションを開始します。
6. クライアントがオブジェクトデータを StorageGRID に送信

例 2 ：外部キー管理サーバ（ KMS ）

この例では、 StorageGRID がクライアントとして機能します。

1. 外部キー管理サーバソフトウェアを使用する場合は、 StorageGRID を KMS クライアントとして設定し、 CA 署名済みサーバ証明書、パブリッククライアント証明書、およびクライアント証明書の秘密鍵を取得します。
2. Grid Manager を使用して KMS サーバを設定し、サーバ証明書とクライアント証明書およびクライアント秘密鍵をアップロードします。
3. StorageGRID ノードで暗号化キーが必要な場合、証明書からのデータと秘密鍵に基づく署名を含む KMS サーバに要求が送信されます。
4. KMS サーバは証明書の署名を検証し、 StorageGRID を信頼できることを決定します。
5. KMS サーバは、検証済みの接続を使用して応答します。

StorageGRID への管理者アクセスの制御

StorageGRID システムへの管理者アクセスは、ファイアウォールポートを開くか閉じ、管理者グループとユーザを管理し、シングルサインオン（SSO）を設定し、StorageGRID 指標へのセキュアな外部アクセスを許可するクライアント証明書を提供することによって制御できます。

- "ファイアウォールによるアクセス制御"
- "アイデンティティフェデレーションを使用する"
- "管理者グループの管理"
- "ローカルユーザの管理"
- "StorageGRID にシングルサインオン（SSO）を使用する"
- "管理者クライアント証明書の設定"

ファイアウォールによるアクセス制御

ファイアウォールでアクセスを制御するには、外部ファイアウォールで特定のポートを開くか、または閉じます。

外部ファイアウォールでのアクセス制御

StorageGRID 管理ノード上のユーザインターフェイスと API へのアクセスは、外部ファイアウォールで特定のポートを開くか、または閉じることで制御できます。たとえば、システムアクセスを制御する他の方法に加えて、ファイアウォールでテナントが Grid Manager に接続できないようにすることができます。

ポート	説明	ポートが開いている場合
443	管理ノードのデフォルトの HTTPS ポート	Web ブラウザと管理 API クライアントは、 Grid Manager 、 Grid 管理 API 、 Tenant Manager 、およびテナント管理 API にアクセスできます。 • 注： * ポート 443 は一部の内部トラフィックにも使用されます。
8443	管理ノード上の制限された Grid Manager ポート	• Web ブラウザと管理 API クライアントは、 HTTPS を使用して Grid Manager とグリッド管理 API にアクセスできます。 • Web ブラウザと管理 API クライアントは、 Tenant Manager またはテナント管理 API にはアクセスできません。 • 内部コンテンツに対する要求は拒否されます。
ポート 1	管理ノード上の制限された Tenant Manager ポート	• Web ブラウザと管理 API クライアントは HTTPS を使用して Tenant Manager とテナント管理 API にアクセスできます。 • Web ブラウザと管理 API クライアントは、 Grid Manager またはグリッド管理 API にはアクセスできません。 • 内部コンテンツに対する要求は拒否されます。

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

関連情報

"Grid Managerにサインインします"

"StorageGRID がSSOを使用していない場合のテナントアカウントの作成"

"Summary ：クライアント接続の IP アドレスとポート"

"信頼されていないクライアントネットワークの管理"

"Ubuntu または Debian をインストールします"

"VMware をインストールする"

"Red Hat Enterprise Linux または CentOS をインストールします"

アイデンティティフェデレーションを使用する

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

できます。

アイデンティティフェデレーションの設定

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

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。
- シングルサインオン（SSO）を有効にする場合は、Active Directoryをフェデレーテッドアイデンティティソースとして使用し、AD FSをアイデンティティプロバイダとして使用する必要があります。「シングルサインオンの使用要件」を参照してください。
- アイデンティティプロバイダとしてActive Directory、OpenLDAP、またはOracle Directory Serverを使用している必要があります。

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

- LDAP サーバとの通信に Transport Layer Security （ TLS ）を使用する場合は、アイデンティティプロバイダが TLS 1.2 または 1.3 を使用している必要があります。

このタスクについて

次の種類のフェデレーテッドグループをインポートする場合は、Grid Managerのアイデンティティソースを設定する必要があります。

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

手順

1. [設定（Configuration ）**]>[***アクセス制御（* Access Control ）**]>[***アイデンティティフェデレーション
2. ［ * アイデンティティフェデレーションを有効にする * ］ を選択

   LDAPサーバを設定するためのフィールドが表示されます。

3. LDAP サービスタイプセクションで、設定する LDAP サービスのタイプを選択します。

   Active Directory 、 OpenLDAP 、または Other *を選択できます。

   > OpenLDAP *を選択した場合は、OpenLDAPサーバを設定する必要があります。OpenLDAPサーバの設定に関するガイドラインを参照してください。

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

4. [* その他 *] を選択した場合は、 [LDAP 属性] セクションのフィールドに入力します。
   - * User Unique Name * ： LDAP ユーザの一意な ID が含まれている属性の名前。この属性はと同じです `sAMAccountName` Active Directoryおよびの場合 `uid` OpenLDAPの場合。Oracle Directory Server を設定する場合は、と入力します `uid`。
   - * User UUID * ： LDAP ユーザの永続的な一意な ID が含まれている属性の名前。この属性はと同じです `objectGUID` Active Directoryおよびの場合 `entryUUID` OpenLDAPの場合。Oracle Directory Serverを設定する場合は、と入力します `nsuniqueid`。指定した属性の各ユーザの値は、 16 バイトまたは文字列形式の 32 桁の 16 進数である必要があります。ハイフンは無視されます。
   - * Group Unique name *：LDAPグループの一意なIDが含まれている属性の名前。この属性はと同じです `sAMAccountName` Active Directoryおよびの場合 `cn` OpenLDAPの場合。Oracle Directory Serverを設定する場合は、と入力します `cn`。
   - * グループ UUID * ： LDAP グループの永続的な一意な ID が含まれている属性の名前。この属性はと同じです `objectGUID` Active Directoryおよびの場合 `entryUUID` OpenLDAPの場合。Oracle Directory Serverを設定する場合は、と入力します `nsuniqueid`。指定した属性の各グループの値は、16 バイトまたは文字列形式の 32 桁の 16 進数である必要があります。ハイフンは無視されます。
5. Configure LDAP server（LDAPサーバの設定）セクションで、必要なLDAPサーバおよびネットワーク接続情報を入力します。
   - * Hostname *：LDAPサーバのホスト名またはIPアドレス。
   - * Port * ： LDAP サーバへの接続に使用するポート。

     STARTTLS のデフォルトポートは 389 、 LDAPS のデフォルトポートは 636 です。ただし、ファイアウォールが正しく設定されていれば、任意のポートを使用できます。
   - * Username * ： LDAP サーバに接続するユーザの識別名（ DN ）の完全パス。

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

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

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

     *グループの一意な名前*値は、所属する*グループのベースDN *内で一意である必要があります。
   - * User base DN*：ユーザを検索するLDAPサブツリーの識別名（DN）の完全パス。

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

6. [* Transport Layer Security（TLS）*]セクションで、セキュリティ設定を選択します。
   - * STARTTLSを使用（推奨）*：STARTTLSを使用してLDAPサーバとの通信を保護します。これが推奨されるオプションです。
   - * LDAPS を使用 * ： LDAPS （ LDAP over SSL ）オプションでは、 TLS を使用して LDAP サーバへの接続を確立します。このオプションは互換性を確保するためにサポートされています。
   - * TLS を使用しないでください * ： StorageGRID システムと LDAP サーバの間のネットワークトラフィックは保護されません。

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

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

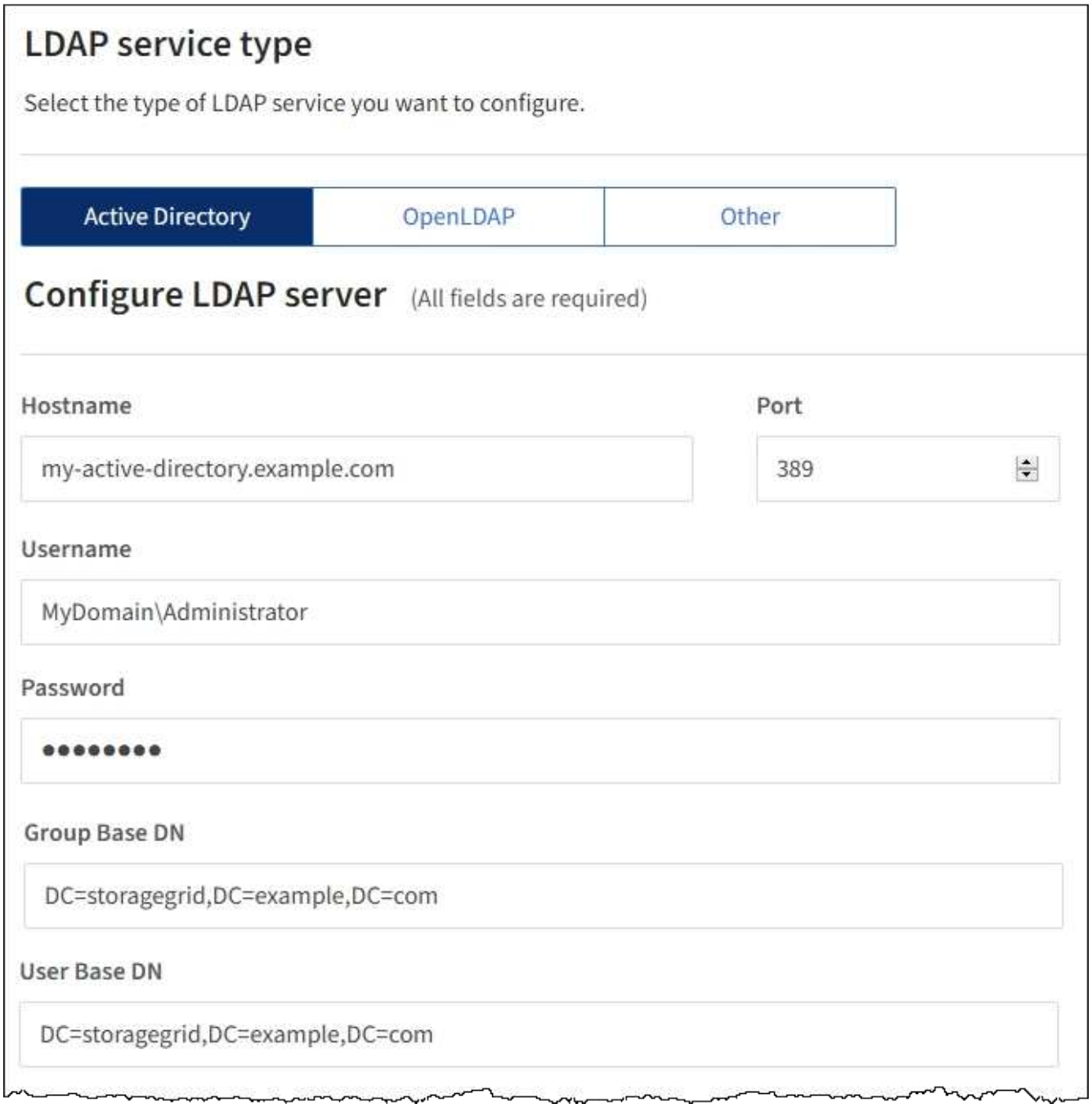
     この設定を選択した場合は、カスタムセキュリティ証明書をコピーして CA 証明書テキストボックスに貼り付けます。

8. 必要に応じて、*接続のテスト*を選択して、LDAPサーバーの接続設定を検証します。

   接続が有効な場合は、ページの右上に確認メッセージが表示されます。

9. 接続が有効な場合は、*保存*を選択します。

   次のスクリーンショットは、Active Directoryを使用するLDAPサーバの設定例を示しています。



関連情報

"発信 TLS 接続でサポートされる暗号"

"シングルサインオンの使用要件"

"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使用する"

OpenLDAP サーバの設定に関するガイドライン

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

memberof オーバーレイと **refint** オーバーレイ

memberof オーバーレイと refint オーバーレイを有効にする必要があります。詳細については、OpenLDAPの管理者ガイドのリバースグループメンバーシップのメンテナンス手順を参照してください。

インデックス作成

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

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

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

OpenLDAPの管理者ガイドのリバースグループメンバーシップのメンテナンスに関する情報を参照してください。

関連情報

"OpenLDAP のドキュメント：バージョン 2.4 管理者ガイド"

アイデンティティソースとの強制同期

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

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。
- アイデンティティソースが有効になっている必要があります。

手順

1. [設定（Configuration ）]>[*アクセス制御（* Access Control ）]>[*アイデンティティフェデレーション

   アイデンティティフェデレーションページが表示されます。「* Synchronize *」ボタンは、ページの下部にあります。

2. [同期化（Synchronize）]をクリックします

   同期が開始されたことを示す確認メッセージが表示されます。環境によっては、同期プロセスにしばらく

時間がかかることがあります。

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

アイデンティティフェデレーションの無効化

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

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

このタスクについて

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

- フェデレーテッドユーザはサインインできなくなります。
- 現在サインインしているフェデレーテッドユーザは、セッションが有効な間は StorageGRID システムに引き続きアクセスできますが、セッションが期限切れになると以降はサインインできなくなります。
- StorageGRID システムとアイデンティティソース間の同期は行われず、同期されていないアカウントに対してはアラートやアラームが生成されません。
- シングルサインオン（SSO）が*有効*または*サンドボックスモード*に設定されている場合、*アイデンティティフェデレーションを有効にする*チェックボックスは無効になります。アイデンティティフェデレーションを無効にするには、シングルサインオンページの SSO ステータスが * 無効 * になっている必要があります。

手順

1. [設定（Configuration ）**]>[***アクセス制御（* Access Control ）**]>[***アイデンティティフェデレーション
2. [アイデンティティフェデレーションを有効にする*]チェックボックスをオフにします。
3. [保存（ Save ）] をクリックします。

関連情報

"シングルサインオンを無効にしています"

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

管理者グループの作成

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

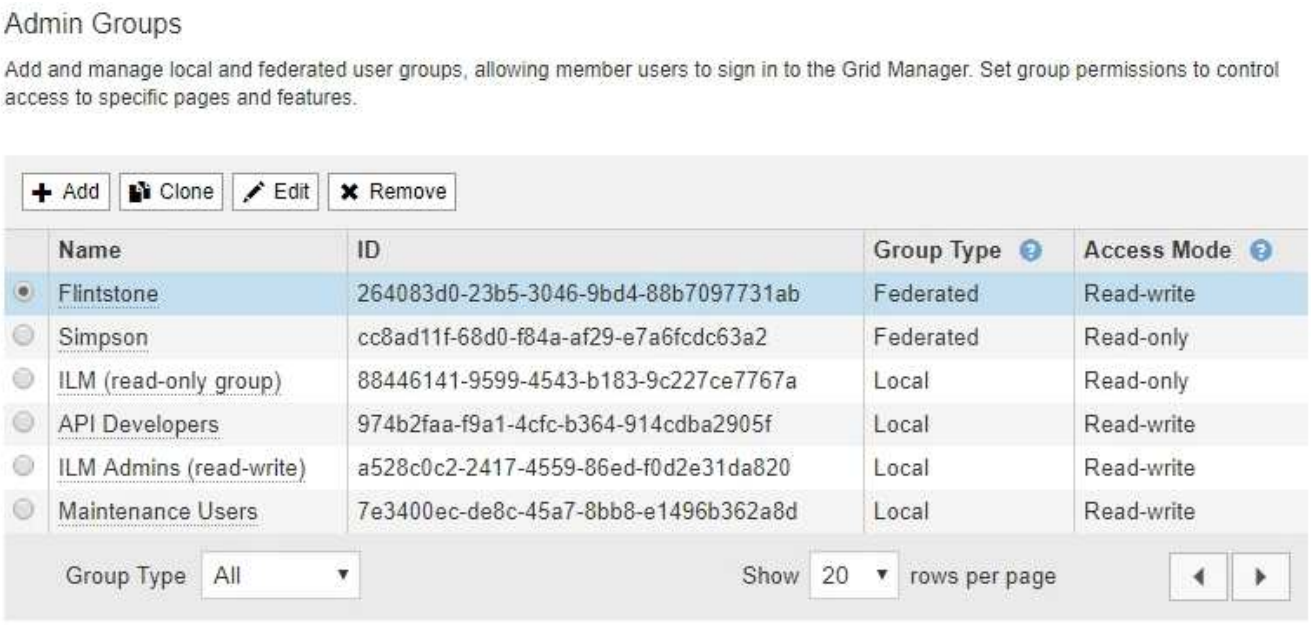
必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。
- フェデレーテッドグループをインポートする場合は、アイデンティティフェデレーションを設定済みで、インポートするフェデレーテッドグループが設定済みのアイデンティティソースにあらかじめ存在している必要があります。

手順

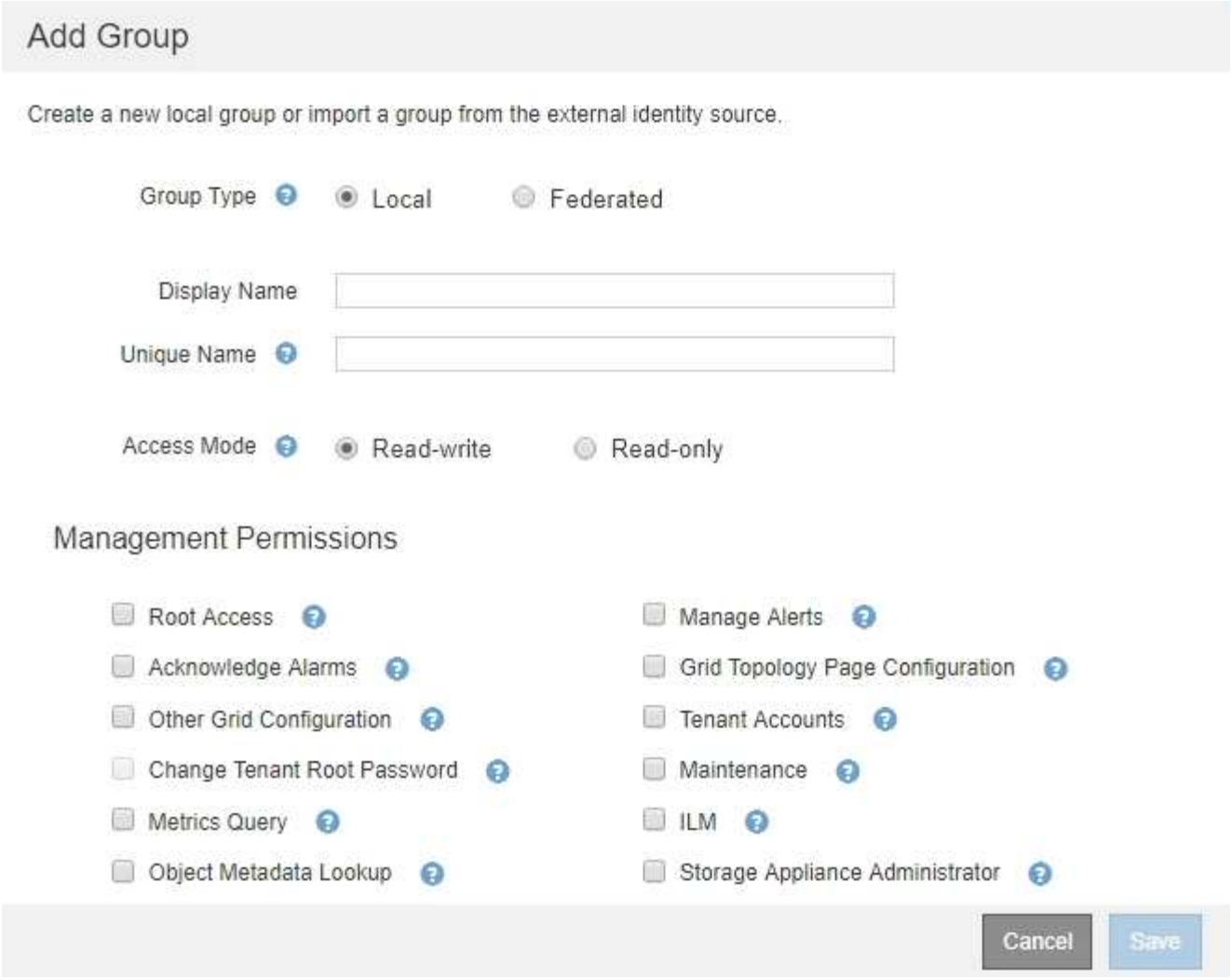
1. [構成アクセス制御管理者グループ*]を選択します。

   Admin Groupsページが表示され、既存の管理者グループが一覧表示されます。



2. 「 * 追加」を選択します。

   [Add Group]ダイアログボックスが表示されます。



3. [グループタイプ]で、StorageGRID 内でのみ使用されるグループを作成する場合は[ローカル*]を、アイデンティティソースからグループをインポートする場合は[フェデレーション*]を選択します。
4. 「ローカル」を選択した場合は、グループの表示名を入力します。表示名は、Grid Managerに表示される名前です。たとえば、「 Maintenance Users 」または「 ILM Administrators 」のようになります。
5. グループの一意の名前を入力します。
   - ローカル：任意の一意の名前を入力します。たとえば'ILM Administrators.`と入力します
   - * Federated *：設定されているアイデンティティソースに表示されるとおりにグループの名前を入力します。
6. *アクセスモード*では、グループ内のユーザがGrid ManagerおよびGrid管理APIで設定の変更や操作を実行できるかどうか、あるいは設定や機能のみを表示できるかどうかを選択します。
   - * 読み取り / 書き込み *（デフォルト）：ユーザは設定を変更し、管理権限で許可されている操作を実行できます。
   - * 読み取り専用 * ：ユーザーは設定と機能のみを表示できます。Grid Manager API や Grid 管理 API で変更や処理を行うことはできません。ローカルの読み取り専用ユーザは自分のパスワードを変更できます。

ユーザーが複数のグループに属していて、いずれかのグループが * 読み取り専用 * に設定されている場合、ユーザーは選択したすべての設定と機能に読み取り専用でアクセスできます。

7. 管理権限を1つ以上選択します。

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

8. [保存（ Save ）] を選択します。

   新しいグループが作成されます。ローカルグループの場合は、ユーザを追加できます。フェデレーテッドグループの場合は、どのユーザがグループに属するかはアイデンティティソースが管理します。

関連情報

"ローカルユーザの管理"

管理者グループの権限

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

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

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

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

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

ルートアクセス（ **Root Access** ）

この権限は、すべてのグリッド管理機能へのアクセスを許可します。

アラートの管理

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

アラームの確認（レガシーシステム）

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

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

Gridトポロジページの設定

この権限では、次のメニューオプションにアクセスできます。

- サポート*ツール*グリッドトポロジ*の各ページにある構成タブを参照してください。
- イベントカウントのリセット[ノード*イベント*]タブのリンク。

その他の**Grid**設定

この権限で、追加のグリッド設定オプションにアクセスできます。

> これらの追加オプションを表示するには、ユーザにGrid Topology Page Configuration権限が付与されている必要もあります。

- アラーム（レガシー・システム）：
  - グローバルアラーム
  - 従来のEメール設定
- * ILM * ：
  - ストレージプール
  - ストレージグレード
- 構成*ネットワーク設定
  - リンクコスト
- 環境設定*システム設定：
  - 表示オプション（Display Options）
  - グリッドオプション（Grid Options）
  - ストレージオプション
- コンフィグレーション*モニタリング：
  - イベント
- サポート：
  - AutoSupport

テナントアカウント

この権限は、* tenants * Tenant Accounts *ページへのアクセスを許可します。

> Grid管理APIのバージョン1（すでに廃止）では、この権限を使用してテナントグループのポリシーの管理、Swift管理者パスワードのリセット、およびrootユーザのS3アクセスキーの管理を行います。

テナントの**root**パスワードを変更

この権限は、テナントアカウントページの* rootパスワードの変更*オプションにアクセスして、テナントのローカルrootユーザのパスワードを変更できるユーザを制御することを可能にします。この権限を持たないユーザには、*Change Root Password *オプションは表示されません。

> この権限を割り当てるには、Tenant Accounts権限がグループに割り当てられている必要があります。

メンテナンス

この権限では、次のメニューオプションにアクセスできます。

- 環境設定*システム設定：
  - ドメイン名*
  - サーバ証明書*
- コンフィグレーション*モニタリング：
  - 監査*
- 設定*アクセス制御：
  - Gridのパスワード
- メンテナンス*メンテナンスタスク
  - 運用停止
  - 拡張
  - リカバリ
- メンテナンス*ネットワーク*：
  - DNSサーバ*
  - Gridネットワーク*
  - NTPサーバ*
- メンテナンス*システム*：
  - ライセンス*
  - リカバリパッケージ
  - ソフトウェア・アップデート
- サポート*ツール*：

- ログ

- Maintenance権限がないユーザは、アスタリスクの付いたページを表示できますが、編集することはできません。

指標クエリ

この権限は、[*Support*Tools*Metrics *]ページへのアクセスを提供します。また、グリッド管理 API の「指標」セクションを使用して、カスタムの Prometheus 指標クエリにアクセスすることもできます。

ILM

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

- イレイジャーコーディング
- ルール
- * ポリシー *
- リージョン

> 「* ILM ストレージ・プール」および「ILM ストレージ・グレード」メニュー・オプションへのアクセスは、「その他のGrid設定」および「Gridトポロジ・ページの設定」権限によって制御されます。

オブジェクトメタデータの検索

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

ストレージアプライアンス管理者

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

権限とアクセスモードの相互作用

すべての権限について、グループのアクセスモード設定は、ユーザが設定を変更して処理を実行できるかどうか、またはユーザが関連する設定と機能のみを表示できるかどうかを決定します。ユーザーが複数のグループに属していて、いずれかのグループが * 読み取り専用 * に設定されている場合、ユーザーは選択したすべての設定と機能に読み取り専用でアクセスできます。

グリッド管理**API**からの機能の非アクティブ化

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

このタスクについて

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

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

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

_ 企業 A は、グリッド管理 API で Deactivate Features システムを使用することで、この目的を達成できます。Grid Manager（UIとAPIの両方）で* Change Tenant Root Password *機能を完全に非アクティブにすることで、A社はすべてのテナントアカウントのrootユーザのパスワードを変更できるようになります。_

非アクティブ化した機能の再アクティブ

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

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

詳細については、S3またはSwiftクライアントアプリケーションを実装する手順を参照してください。

手順

1. Swagger のグリッド管理 API のドキュメントにアクセスします。
2. Deactivate Features エンドポイントを探します。
3. * Change Tenant Root Password *などの機能を非アクティブ化するには、次のようにAPIに本文を送信します。

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

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

4. すべての機能を再アクティブ化するには、次のような本文を API に送信します。

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

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

前述の例は、 _all_deactivated 機能を再アクティブ化します。非アクティブ化したままにする必要がある他の機能が非アクティブ化されている場合は、 PUT 要求でそれらを明示的に指定する必要があります。たとえば、Change Tenant Root Password機能を再アクティブ化して、Alarm Acknowledgment機能を非アクティブなままにするには、次のPUT要求を送信します。

```
{ "grid": { "alarmAcknowledgment": true } }
```

関連情報

"グリッド管理APIを使用する"

管理者グループの変更

管理者グループを変更して、グループに関連付けられている権限を変更できます。ローカル管理者グループについては、表示名を更新することもできます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

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. グループを選択します。

   システムに20個を超えるアイテムが含まれている場合は、各ページに一度に表示する行数を指定できます。その後、ブラウザの検索機能を使用して、現在表示されている行の特定の項目を検索できます。

3. [編集（ Edit ）] をクリックします。
4. オプションで'ローカル・グループの場合は'たとえばMaintenance Usersのように'ユーザーに表示されるグループの名前を入力します

   一意の名前は内部グループ名であるため、変更できません。

5. 必要に応じて、グループのアクセスモードを変更します。
   - * 読み取り / 書き込み * （デフォルト）：ユーザは設定を変更し、管理権限で許可されている操作を実行できます。
   - * 読み取り専用 * ：ユーザーは設定と機能のみを表示できます。Grid Manager API や Grid 管理 API で変更や処理を行うことはできません。ローカルの読み取り専用ユーザは自分のパスワードを変更できます。

   ユーザーが複数のグループに属していて、いずれかのグループが * 読み取り専用 * に設定されている場合、ユーザーは選択したすべての設定と機能に読み取り専用でアクセスできます。

6. 必要に応じて、グループ権限を追加または削除します。

管理者グループの権限に関する情報を参照してください。

7. [保存（ Save ）] を選択します。

関連情報

[管理者グループの権限]

管理者グループを削除しています

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

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

このタスクについて

グループを削除すると、そのグループに割り当てられているユーザは、別のグループから権限が付与されていないかぎり、Grid Managerへのすべてのアクセス権限を失います。

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. グループの名前を選択します。

   システムに20個を超えるアイテムが含まれている場合は、各ページに一度に表示する行数を指定できます。その後、ブラウザの検索機能を使用して、現在表示されている行の特定の項目を検索できます。

3. 「 * 削除」を選択します。
4. 「 * OK 」を選択します。

ローカルユーザの管理

ローカルユーザを作成してローカル管理者グループに割り当て、そのユーザがアクセスできるGrid Manager機能を決定することができます。

Grid Managerには'ルートという名前の'事前定義されたローカル・ユーザが1つ含まれていますローカルユーザは追加および削除できますが、rootユーザ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、ローカルユーザはStorageGRID にサインインできません。

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

ローカルユーザを作成しています

ローカル管理者グループを作成した場合は、1人以上のローカルユーザを作成し、各ユーザを1つ以上のグル

ープに割り当てることができます。このグループの権限は、ユーザがアクセスできるGrid Manager機能を制御します。

このタスクについて

作成できるのはローカルユーザだけで、作成したユーザはローカル管理者グループにのみ割り当てることができます。フェデレーテッドユーザとフェデレーテッドグループは、外部のアイデンティティソースを使用して管理されます。

手順

1. [構成（Configuration ）]>[*アクセス制御（* Access Control ）]>[*管理者ユーザー（* Admin Users *）
2. [作成（ Create ）] をクリックします。
3. ユーザの表示名、一意の名前、およびパスワードを入力します。
4. アクセス権限を制御する1つ以上のグループにユーザを割り当てます。

   グループ名のリストは'グループ(Groups)テーブルから生成されます

5. [保存（ Save ）] をクリックします。

関連情報

"管理者グループの管理"

ローカルユーザアカウントの変更

ローカル管理者ユーザのアカウントを変更して、ユーザの表示名またはグループメンバーシップを更新できます。ユーザが一時的にシステムにアクセスできないように設定することもできます。

このタスクについて

編集できるのはローカルユーザのみです。フェデレーテッドユーザの詳細は、外部のアイデンティティソースと自動的に同期されます。

手順

1. [構成（Configuration ）]>[*アクセス制御（* Access Control ）]>[*管理者ユーザー（* Admin Users *）
2. 編集するユーザを選択します。

   システムに20個を超えるアイテムが含まれている場合は、各ページに一度に表示する行数を指定できます。その後、ブラウザの検索機能を使用して、現在表示されている行の特定の項目を検索できます。

3. [編集（ Edit ）] をクリックします。
4. 必要に応じて、名前またはグループメンバーシップを変更します。
5. 必要に応じて、ユーザが一時的にシステムにアクセスできないようにするには、*アクセス拒否*をオンにします。
6. [保存（ Save ）] をクリックします。

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

ローカルユーザのアカウントを削除する

Grid Managerへのアクセスが不要になったローカルユーザのアカウントを削除できます。

手順

1. [構成（Configuration ）]>[*アクセス制御（* Access Control ）]>[*管理者ユーザー（* Admin Users *）
2. 削除するローカルユーザを選択します。

   事前定義されたrootローカルユーザは削除できません。

   システムに20個を超えるアイテムが含まれている場合は、各ページに一度に表示する行数を指定できます。その後、ブラウザの検索機能を使用して、現在表示されている行の特定の項目を検索できます。

3. [削除（ Remove ）] をクリックします。
4. [OK] をクリックします。

ローカルユーザのパスワードを変更する

ローカルユーザは、 Grid Manager のバナーで * Change Password * 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。また、Admin Usersページへのアクセス権を持つユーザは、他のローカルユーザのパスワードを変更できます。

このタスクについて

変更できるのはローカルユーザのパスワードのみです。フェデレーテッドユーザは、自分のパスワードを外部のアイデンティティソース内で変更する必要があります。

手順

1. [構成（Configuration ）]>[*アクセス制御（* Access Control ）]>[*管理者ユーザー（* Admin Users *）
2. [ユーザー]ページで、ユーザーを選択します。

   システムに20個を超えるアイテムが含まれている場合は、各ページに一度に表示する行数を指定できます。その後、ブラウザの検索機能を使用して、現在表示されている行の特定の項目を検索できます。

3. [パスワードの変更*]をクリックします。
4. パスワードを入力して確認し、*保存*をクリックします。

StorageGRID にシングルサインオン（SSO）を使用する

StorageGRID システムでは、 Security Assertion Markup Language 2.0 （ SAML 2.0 ）標準を使用したシングルサインオン（ SSO ）がサポートされます。SSO が有効な場合は、 Grid Manager 、 Tenant Manager 、 Grid 管理 API 、またはテナント管理 API にアクセスするすべてのユーザを外部のアイデンティティプロバイダによって認証する必要があります。ローカルユーザは StorageGRID にサインインできません。

- "シングルサインオンの仕組み"
- "シングルサインオンの使用要件"
- "シングルサインオンを設定しています"

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

SSOが有効な場合はサインインします

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

手順

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

   StorageGRID のサインインページが表示されます。

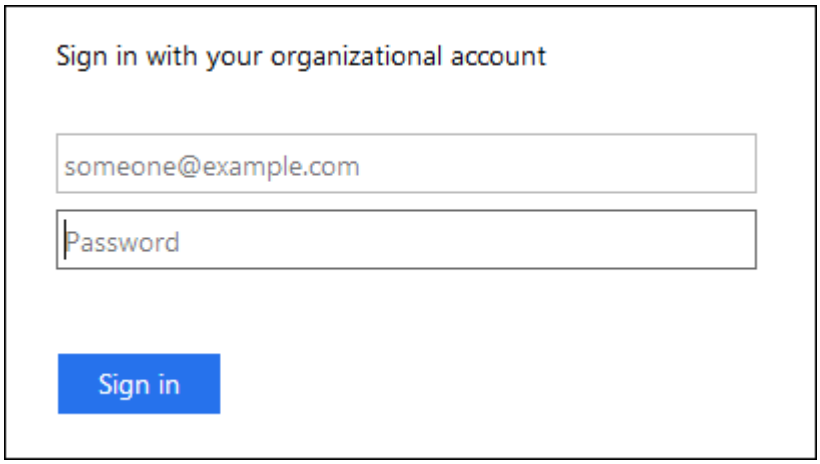
   - このブラウザで初めて URL にアクセスした場合は、アカウント ID の入力を求められます。

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

テナントアカウントの完全なURL（完全修飾ドメイン名またはIPアドレスのあとにを追加したもの）を入力すると、StorageGRID のサインインページは表示されません `/?accountId=20-digit-account-id`）。代わりに、組織の SSO サインインページがすぐに表示されます。このページでは、を実行できます SSO クレデンシャルを使用してサインインします。

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

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



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

   SSO クレデンシャルが正しい場合：

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

   SSO クレデンシャルを再入力する必要はありません。

SSOが有効な場合はサインアウトします

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

手順

1. ユーザインターフェイスの右上隅にある [**Sign Out**] リンクを探します。
2. [サインアウト]をクリックします。

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

サインイン先	サインアウト元	サインアウトされる対象
1 つ以上の管理ノードでグリッドマネージャを使用します	任意の管理ノード上の Grid Manager	すべての管理ノード上の Grid Manager
1 つ以上の管理ノード上の Tenant Manager	任意の管理ノード上の Tenant Manager	すべての管理ノード上の Tenant Manager
Grid Manager と Tenant Manager の両方	Grid Manager の略	Grid Manager のみ。SSO からサインアウトするには、 Tenant Manager からもサインアウトする必要があります。

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

シングルサインオンの使用要件

StorageGRID システムでシングルサインオン（ SSO ）を有効にする前に、このセクションの要件を確認してください。

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

アイデンティティプロバイダの要件

SSOのアイデンティティプロバイダ（IdP）は、次の要件を満たしている必要があります。

- 次のいずれかのバージョンのActive Directoryフェデレーションサービス（AD FS）
  - AD FS 4.0はWindows Server 2016に付属しています

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

  - AD FS 3.0 （ Windows Server 2012 R2 Update 以降に付属）。
- Transport Layer Security （ TLS ） 1.2 または 1.3
- Microsoft .NET Framework バージョン 3.5.1 以降

サーバ証明書の要件

StorageGRID は、各管理ノード上の管理インターフェイスのサーバ証明書を使用して、Grid Manager、テナントマネージャ、グリッド管理API、およびテナント管理APIへのアクセスを保護します。AD FS でStorageGRID 用にSSOの証明書利用者信頼を設定する際には、このサーバ証明書をAD FSへのStorageGRID 要求の署名証明書として使用します。

管理インターフェイス用のカスタムサーバ証明書をまだインストールしていない場合は、インストールしてください。インストールしたカスタムサーバ証明書はすべての管理ノードで使用され、すべてのStorageGRID 証明書利用者信頼で使用できます。

> 管理ノードのデフォルトサーバ証明書をAD FSの証明書利用者信頼に使用することは推奨されません。ノードに障害が発生した場合にそのノードをリカバリすると、新しいデフォルトサーバ証明書が生成されます。リカバリしたノードにサインインするには、AD FSの証明書利用者信頼を新しい証明書で更新する必要があります。

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

関連情報

"ファイアウォールによるアクセス制御"

"Grid ManagerおよびTenant Manager用のカスタムサーバ証明書を設定する"

シングルサインオンを設定しています

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

- "フェデレーテッドユーザがサインインできることを確認しておき"
- "サンドボックスモードの使用"
- "AD FSでの証明書利用者信頼の作成"
- "証明書利用者信頼のテスト"
- "シングルサインオンの有効化"
- "シングルサインオンを無効にしています"
- "1つの管理ノードのシングルサインオンの一時的な無効化と再有効化"

フェデレーテッドユーザがサインインできることを確認しておき

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

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。
- Active Directoryをフェデレーテッドアイデンティティソースとして使用し、AD FSをアイデンティティプロバイダとして使用している。

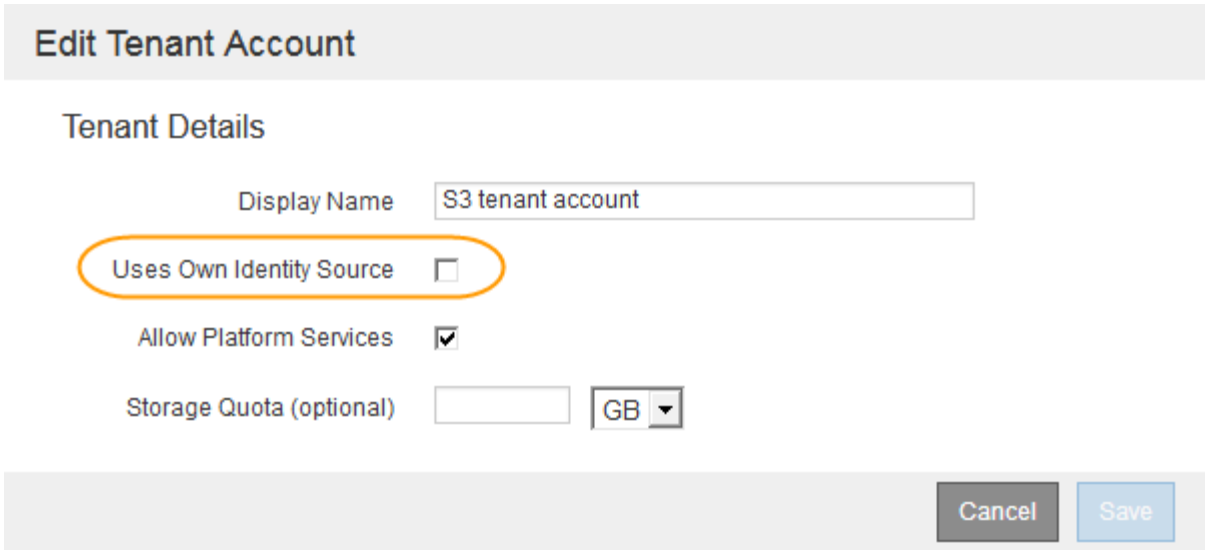
  "シングルサインオンの使用要件"

手順

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

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

   a. 各テナントアカウントの Tenant Manager にサインインします。
   b. アクセス制御*>*アイデンティティフェデレーション*を選択します。
   c. ［アイデンティティフェデレーションを有効にする］チェックボックスがオフになっていることを確認します。
   d. その場合は、このテナントアカウントに使用されている可能性のあるフェデレーテッドグループが不要になっ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*をクリックします。
2. フェデレーテッドユーザが Grid Manager にアクセスできることを確認します。
   a. Grid Managerから* Configuration > Access Control > Admin Groups *を選択します。
   b. Active Directoryアイデンティティソースから少なくとも1つのフェデレーテッドグループがインポートされていて、そのグループにRoot Access権限が割り当てられていることを確認します。
   c. サインアウトします。
   d. フェデレーテッドグループ内のユーザとして Grid Manager に再度サインインできることを確認します。
3. 既存のテナントアカウントがある場合は、Root Access権限を持つフェデレーテッドユーザがサインインできることを確認します。
   a. Grid Managerから* tenants *を選択します。
   b. テナントアカウントを選択し、*アカウントの編集*をクリックします。
   c. [独自のアイデンティティソースを使用する*]チェックボックスがオンになっている場合は、チェックボックスをオフにして、[保存*]をクリックします。



Tenant Accountsページが表示されます。

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

b. Tenant Managerで、* Access Control > Groups *をクリックします。

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

d. サインアウトします。

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

関連情報

"シングルサインオンの使用要件"

"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の使用

サンドボックスモードを使用すると、StorageGRID ユーザにシングルサインオン（SSO）を適用する前に、Active Directoryフェデレーションサービス（AD FS）の証明書利用者信頼を設定およびテストできます。SSOを有効にしたあとにサンドボックスモードを再度有効にすると、新規および既存の証明書利用者信頼を設定またはテストできます。サンドボックスモードを再度有効にすると、StorageGRID ユーザーのSSOは一時的に無効に

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

このタスクについて

SSOが有効な場合、ユーザが管理ノードにサインインしようとすると、StorageGRID からAD FSに認証要求が送信されます。次に、AD FS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。要求が成功した場合、応答にはユーザのUniversally Unique Identifier（UUID）が含まれます。

StorageGRID （サービスプロバイダ）とAD FS（アイデンティティプロバイダ）がユーザの認証要求を安全にやり取りできるようにするには、StorageGRID で特定の設定を行う必要があります。次に、AD FSを使用して、管理ノードごとに証明書利用者信頼を作成します。最後に、 StorageGRID に戻って SSO を有効にする必要があります。

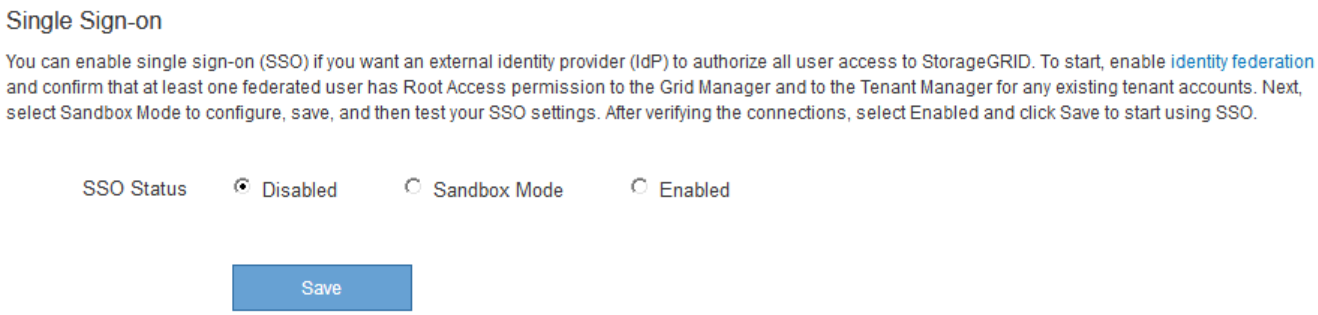
サンドボックスモードでは、 SSO を有効にする前に、この手順を簡単に実行し、すべての設定をテストできます。

サンドボックスモードは使用することを推奨しますが、必須ではありません。StorageGRID でSSOを設定した直後にAD FSの証明書利用者信頼を作成する準備ができている場合は、また、管理ノードごとにSSOプロセスとシングルログアウト（SLO）プロセスをテストする必要はありません。* enabled をクリックし、**StorageGRID** 設定を入力して、**AD FS**内の管理ノードごとに証明書利用者信頼を作成し、 Save *をクリックしてSSOを有効にします。

手順

1. 「* Configuration * Access Control * Single Sign-On *」を選択します。

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



   SSO Statusオプションが表示されない場合は、Active Directoryがフェデレーテッドアイデンティティソースとして設定されていることを確認します。「シングルサインオンの使用要件」を参照してください。

2. [サンドボックスモード]オプションを選択します。

   アイデンティティプロバイダと証明書利用者の設定が表示されます。［アイデンティティプロバイダ］セクションでは、［サービスタイプ］フィールドは読み取り専用です。ここには、使用しているアイデンティティフェデレーションサービスのタイプ（Active Directoryなど）が表示されます。

3. アイデンティティプロバイダセクションで、次の手順を実行します。

   a. フェデレーションサービス名をAD FSに表示されているとおりに入力します。

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

b. StorageGRID 要求への応答としてアイデンティティプロバイダがSSO設定情報を送信するときに、Transport Layer Security（TLS）を使用して接続を保護するかどうかを指定します。

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

  この設定を選択した場合は、証明書を* CA証明書*テキストボックスにコピーして貼り付けます。

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

4. 証明書利用者セクションで、StorageGRID 管理ノードに使用する証明書利用者信頼を設定するときに使用する証明書利用者IDを指定します。

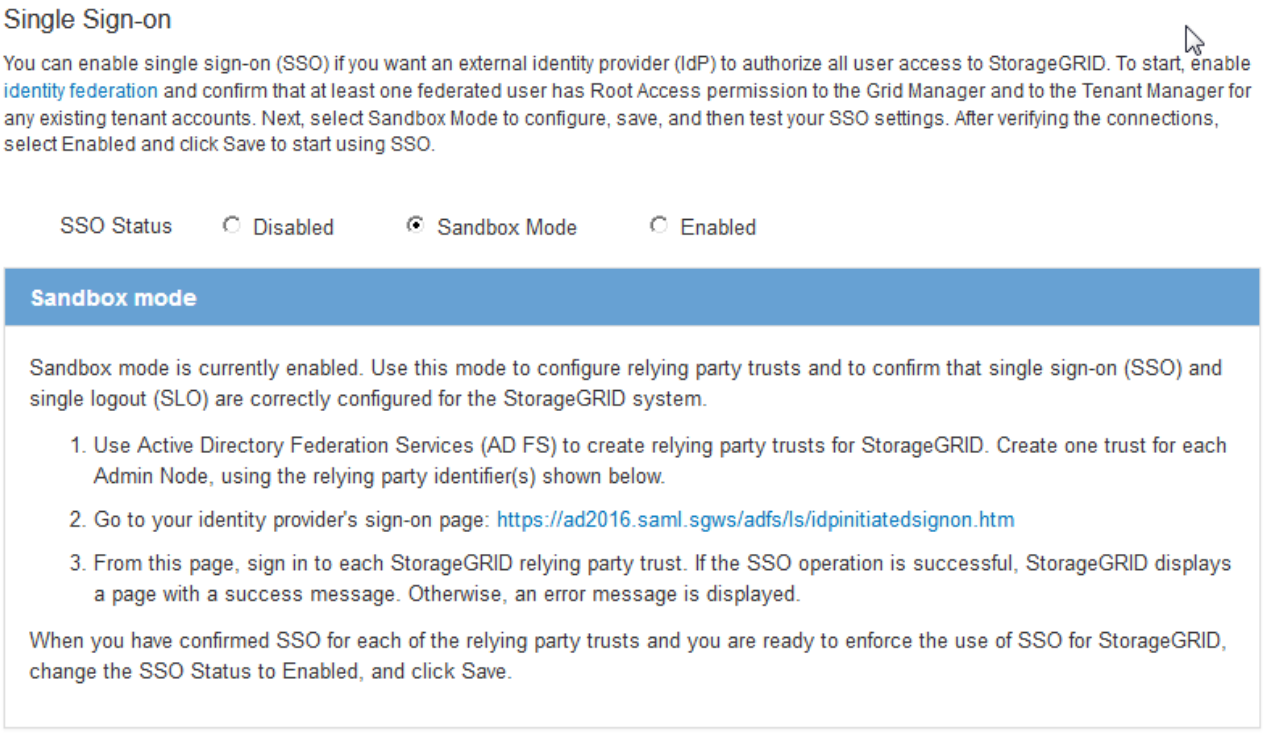
◦ たとえば、グリッドに管理ノードが1つしかなく、今後管理ノードを追加する予定がない場合は、と入力します `SG` または `StorageGRID`。

◦ グリッドに複数の管理ノードがある場合は、という文字列を含めます `[HOSTNAME]` を入力します。例： `SG-[HOSTNAME]`。これにより、管理ノードのホスト名に基づいて、各管理ノードの証明書利用者IDを含むテーブルが生成されます。+注：証明書利用者信頼はStorageGRID システム内の管理ノードごとに作成する必要があります。管理ノードごとに証明書利用者信頼を作成することで、ユーザは管理ノードに対して安全にサインイン / サインアウトすることができます。

5. [保存（ Save ）] をクリックします。

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

◦ サンドボックスモードの確認メッセージが表示され、サンドボックスモードが有効になっていることが確認されます。AD FSの使用時にもこのモードを使用して、管理ノードごとに証明書利用者信頼を設定し、シングルサインイン（SSO）プロセスとシングルログアウト（SLO）プロセスをテストできます。



関連情報

"シングルサインオンの使用要件"

AD FSでの証明書利用者信頼の作成

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

Windows PowerShellを使用した証明書利用者信頼の作成

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

必要なもの

- StorageGRID でSSOを設定し、システム内の各管理ノードの完全修飾ドメイン名（またはIPアドレス）と証明書利用者IDを確認しておきます。

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

- AD FS での証明書利用者信頼の作成経験があるか、または Microsoft AD FS のドキュメントを参照できる必要があります。
- AD FS 管理スナップインを使用していて、 Administrators グループに属している必要があります。

このタスクについて

以下の手順は、Windows Server 2016に付属のAD FS 4.0での手順です。Windows Server 2012 R2に含まれているAD FS 3.0を使用している場合は、手順 にわずかな違いがあります。不明な点がある場合は、Microsoft AD FS のドキュメントを参照してください。

手順

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

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

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

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

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

      たとえば、 **ObjectGUID to Name ID** と入力します。
   f. 属性ストアで、 * Active Directory * を選択します。
   g. マッピングテーブルの LDAP 属性列に、 * objectGUID * と入力します。
   h. マッピングテーブルの発信クレームタイプ列で、ドロップダウンリストから * 名前 ID * を選択します。

i. [完了]をクリックし、[OK]をクリックします。

7. メタデータが正常にインポートされたことを確認します。
   a. 証明書利用者信頼を右クリックしてプロパティを開きます。
   b. [**Endpoints**] 、 [***Identifiers**] 、および [**Signature**] タブのフィールドに値が入力されていることを確認します。

      メタデータがない場合は、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. 上記の手順を繰り返して、 StorageGRID システム内のすべての管理ノードに対して証明書利用者信頼を設定します。
9. 完了したら、StorageGRID およびに戻ります "すべての証明書利用者信頼をテストします" 正しく設定されていることを確認します。

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

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

必要なもの

- StorageGRID でSSOを設定し、システム内の各管理ノードの完全修飾ドメイン名（またはIPアドレス）と証明書利用者IDを確認しておきます。

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

- AD FS での証明書利用者信頼の作成経験があるか、または Microsoft AD FS のドキュメントを参照できる必要があります。
- AD FS 管理スナップインを使用していて、 Administrators グループに属している必要があります。

このタスクについて

以下の手順は、Windows Server 2016に付属のAD FS 4.0での手順です。Windows Server 2012 R2に含まれているAD FS 3.0を使用している場合は、手順 にわずかな違いがあります。不明な点がある場合は、 Microsoft AD FS のドキュメントを参照してください。

手順

1. Windows Server Managerで、* Tools をクリックし、 AD FS Management *を選択します。
2. Actions（アクション）で、* Add（証明書利用者信頼の追加）*をクリックします。
3. [ようこそ]ページで、[クレーム対応]を選択し、[開始]をクリックします。
4. [* オンラインまたはローカルネットワーク上で公開されている証明書利用者に関するデータをインポートする *] を選択します。
5. * フェデレーションメタデータアドレス（ホスト名または URL ） * に、この管理ノードの SAML メタデータの場所を入力します。

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

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

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

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

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

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

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

      メタデータがない場合は、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. 上記の手順を繰り返して、 StorageGRID システム内のすべての管理ノードに対して証明書利用者信頼を設定します。
10. 完了したら、StorageGRID およびに戻ります "すべての証明書利用者信頼をテストします" 正しく設定されていることを確認します。

証明書利用者信頼の手動作成

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

必要なもの

- StorageGRID でSSOを設定し、システム内の各管理ノードの完全修飾ドメイン名（またはIPアドレス）と証明書利用者IDを確認しておきます。

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

- StorageGRID 管理インターフェイス用にカスタム証明書をアップロードしておきます。または、コマンドシェルから管理ノードにログインする方法を確認しておきます。
- AD FS での証明書利用者信頼の作成経験があるか、または Microsoft AD FS のドキュメントを参照できる必要があります。
- AD FS 管理スナップインを使用していて、 Administrators グループに属している必要があります。

このタスクについて

以下の手順は、Windows Server 2016に付属のAD FS 4.0での手順です。Windows Server 2012 R2に含まれているAD FS 3.0を使用している場合は、手順 にわずかな違いがあります。不明な点がある場合は、 Microsoft AD FS のドキュメントを参照してください。

手順

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

   a. この管理ノードの表示名を入力します。

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

   b. オプションのトークン暗号化証明書を設定する手順は省略してください。

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

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

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

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

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

      Admin_Node_Identifier

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

   f. 設定を確認し、証明書利用者信頼を保存して、ウィザードを閉じます。

[クレーム発行ポリシーの編集] ダイアログボックスが表示されます。

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

6. ［クレームルール］ウィザードを開始するには、［ルールの追加］をクリックします。
   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］をクリックします。
   b. ［ ルールの設定 ］ ページで、このルールの表示名を入力します。

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

   c. 属性ストアで、 * Active Directory * を選択します。
   d. マッピングテーブルの LDAP 属性列に、 * objectGUID * と入力します。
   e. マッピングテーブルの発信クレームタイプ列で、ドロップダウンリストから * 名前 ID * を選択します。
   f. [完了]をクリックし、[OK]をクリックします。
7. 証明書利用者信頼を右クリックしてプロパティを開きます。
8. [* Endpoints] タブで、シングルログアウト（ SLO ）のエンドポイントを設定します。
   a. * SAMLの追加*をクリックします。
   b. [* Endpoint Type*>*SAML Logout*] を選択します。
   c. 「 * Binding * > * Redirect * 」を選択します。
   d. [**Trusted URL**] フィールドに、この管理ノードからのシングルログアウト（ SLO ）に使用する URL を入力します。

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

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

   a. [OK] をクリックします。
9. [* Signature*] タブで、この証明書利用者信頼の署名証明書を指定します。
   a. カスタム証明書を追加します。
      - StorageGRID にアップロードしたカスタム管理証明書がある場合は、その証明書を選択します。
      - カスタム証明書がない場合は、管理ノードにログインしてに進みます `/var/local/mgmt-api` 管理ノードのディレクトリにを追加します `custom-server.crt` 証明書ファイル。

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

   b. [*適用（Apply）]をクリックし、[OK]をクリックします。

証明書利用者のプロパティが保存されて閉じられます。

10. 上記の手順を繰り返して、 StorageGRID システム内のすべての管理ノードに対して証明書利用者信頼を設定します。
11. 完了したら、StorageGRID およびに戻ります "すべての証明書利用者信頼をテストします" 正しく設定されていることを確認します。

証明書利用者信頼のテスト

StorageGRID に対するシングルサインオン（SSO）の使用を適用する前に、シングルサインオンとシングルログアウト（SLO）が正しく設定されていることを確認します。管理ノードごとに証明書利用者信頼を作成した場合は、管理ノードごとにSSOとSLOを使用できることを確認します。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。
- AD FSに1つ以上の証明書利用者信頼を設定しておきます。

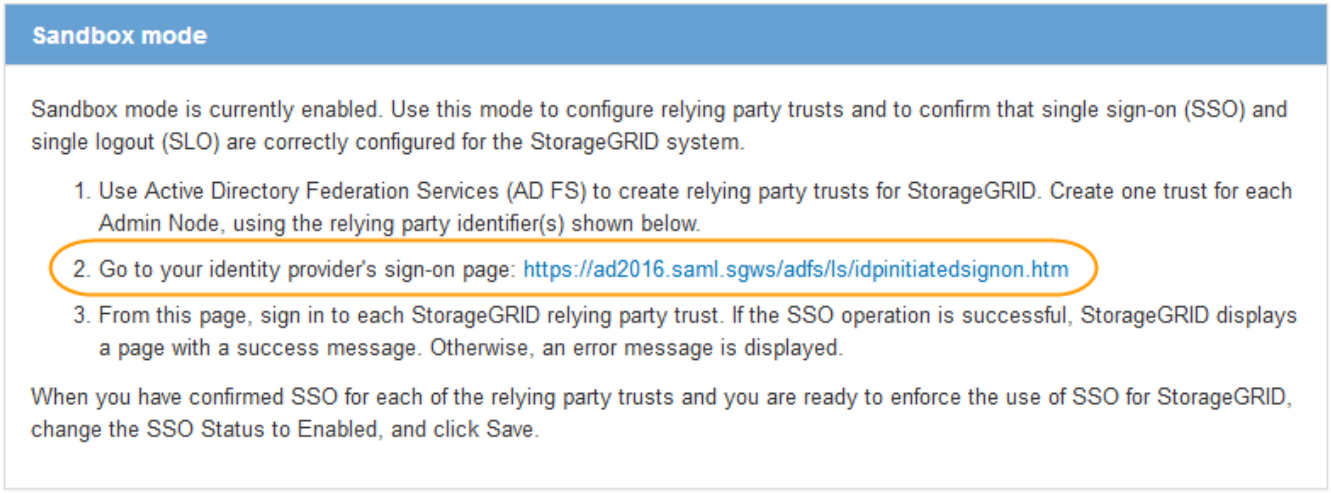
手順

1. 「* Configuration * Access Control * Single Sign-On *」を選択します。

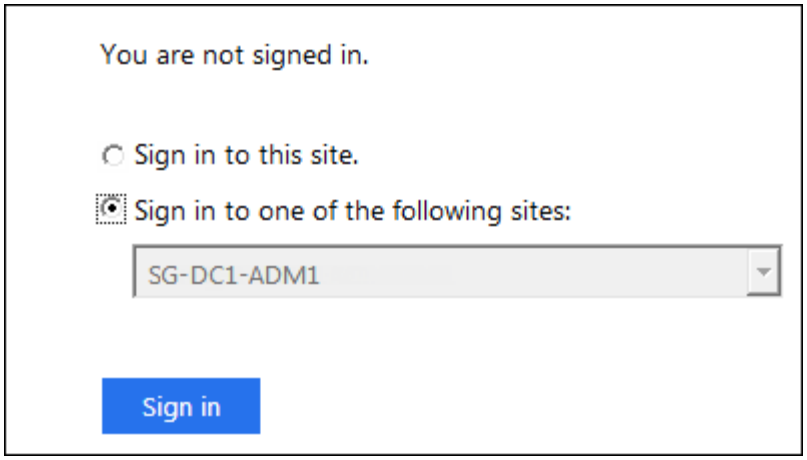
   [シングルサインオン]ページが表示され、[サンドボックスモード]オプションが選択されます。

2. サンドボックスモードの手順で、アイデンティティプロバイダのサインオンページへのリンクを探します。

   このURLは、[**Federated Service Name**]フィールドに入力した値から取得されます。



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



ユーザ名とパスワードの入力を求めるプロンプトが表示されます。

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

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

   - SSO 処理が失敗すると、エラーメッセージが表示されます。問題 を修正し、ブラウザのクッキーを消去してやり直してください。
6. 上記の手順を繰り返して、他のすべての管理ノードにサインインできることを確認します。

   すべてのSSOサインインおよびログアウト処理が成功したら、SSOを有効にすることができます。

シングルサインオンの有効化

サンドボックスモードを使用してすべてのStorageGRID 証明書利用者信頼をテストしたら、シングルサインオン（SSO）を有効にすることができます。

必要なもの

- アイデンティティソースから少なくとも1つのフェデレーテッドグループをインポートして、そのグループにRoot Access管理権限を割り当てておく必要があります。既存のテナントアカウントに対して、少なくとも1人のフェデレーテッドユーザがGrid ManagerとTenant ManagerへのRoot Access権限を持っていることを確認する必要があります。
- サンドボックスモードを使用して、すべての証明書利用者信頼をテストしておく必要があります。

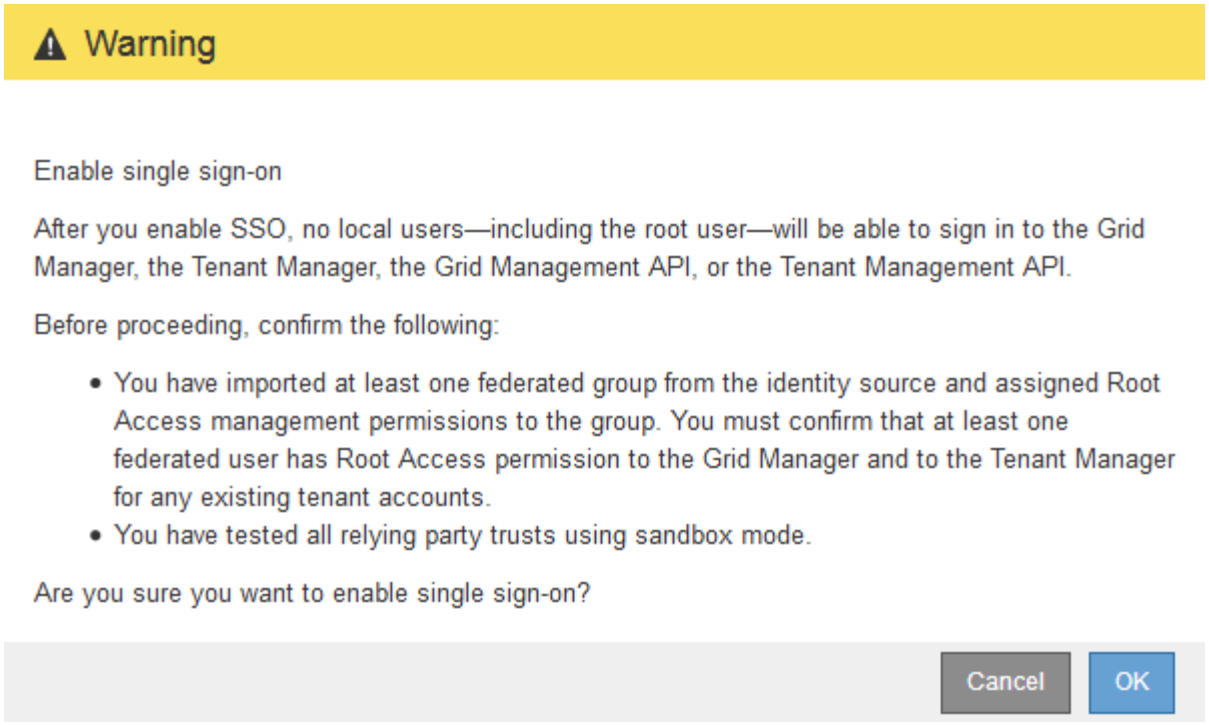
手順

1. 「* Configuration * Access Control * Single Sign-On *」を選択します。

   [シングルサインオン]ページが開き、[サンドボックスモード]が選択されます。

2. SSO ステータスを * Enabled * に変更します。
3. [保存（ Save ）] をクリックします。

   警告メッセージが表示されます。



4. 警告を確認し、* OK *をクリックします。

   シングルサインオンが有効になりました。

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

シングルサインオンを無効にしています

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

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

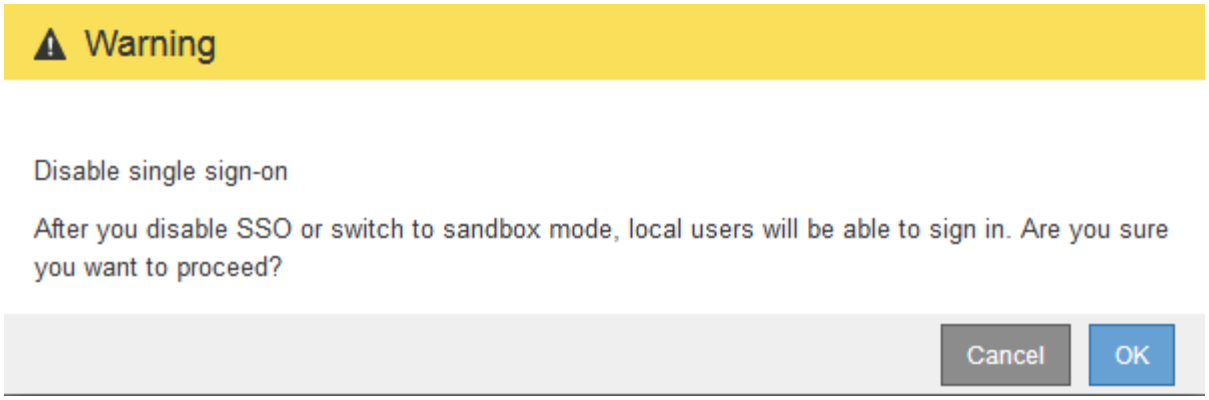
手順

1. 「* Configuration * Access Control * Single Sign-On *」を選択します。

   [Single Sign-On] ページが表示されます。

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

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



4. [OK] をクリックします。

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

1つの管理ノードのシングルサインオンの一時的な無効化と再有効化

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

必要なもの

- 特定のアクセス権限が必要です。
- を用意しておく必要があります `Passwords.txt` ファイル。
- ローカルのrootユーザのパスワードを確認しておく必要があります。

このタスクについて

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

> 1 つの管理ノードに対して SSO を無効にしても、グリッド内の他の管理ノードの SSO 設定には影響しません。Grid Manager の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オンのままで、既存の SSO 設定はすべて更新しないかぎり維持されます。

手順

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

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

2. 次のコマンドを実行します。`disable-saml`

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

3. SSO を無効にすることを確認します。

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

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

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

5. ユーザ名「 root 」とローカルの root ユーザのパスワードを使用してサインインします。
6. SSO 設定の修正が必要なために SSO を一時的に無効にした場合は、次の手順を実行します
   a. 「* Configuration * Access Control * Single Sign-On *」を選択します。
   b. 正しくない SSO 設定または古い SSO 設定を変更します。
   c. [保存（ Save ）] をクリックします。

      シングルサインオンページで* Save *をクリックすると、グリッド全体でSSOが自動的に再有効化されます。

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

      - 次のコマンドを実行します。 `enable-saml`

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

      SSO を有効にすることを確認します。

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

   - グリッドノードをリブートします。 `reboot`

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

関連情報

"シングルサインオンを設定しています"

管理者クライアント証明書の設定

クライアント証明書を使用すると、許可された外部クライアントがStorageGRID

Prometheusデータベースにアクセスできるようになります。クライアント証明書は、外部ツールを使用してStorageGRID を監視するためのセキュアな方法を提供します。

外部の監視ツールを使用してStorageGRID にアクセスする必要がある場合は、グリッドマネージャを使用してクライアント証明書をアップロードまたは生成し、証明書の情報を外部ツールにコピーする必要があります。

管理者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、独自の証明書を指定するか、またはGrid Managerを使用して証明書を生成します。

必要なもの

- Root Access 権限が必要です。
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 管理ノードのIPアドレスまたはドメイン名を確認しておく必要があります。
- StorageGRID 管理インターフェイスのサーバ証明書を設定し、対応するCAバンドルを用意しておく必要があります
- 独自の証明書をアップロードする場合は、証明書の公開鍵と秘密鍵がローカルコンピュータ上にある必要があります。

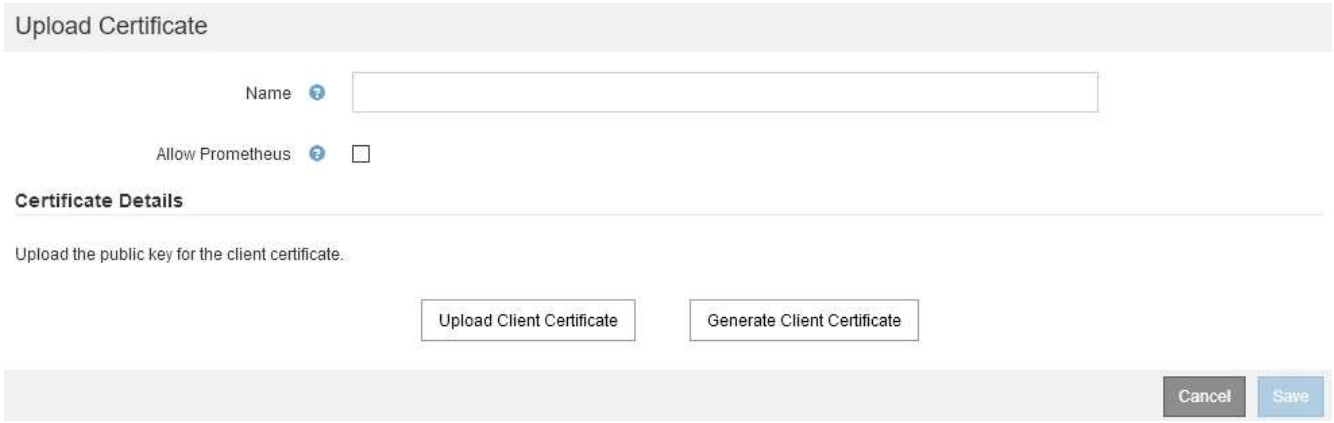
手順

1. Grid Managerで、* Configuration **>** Access Control **>** Client Certificates *を選択します。

   [Client Certificates]ページが表示されます。

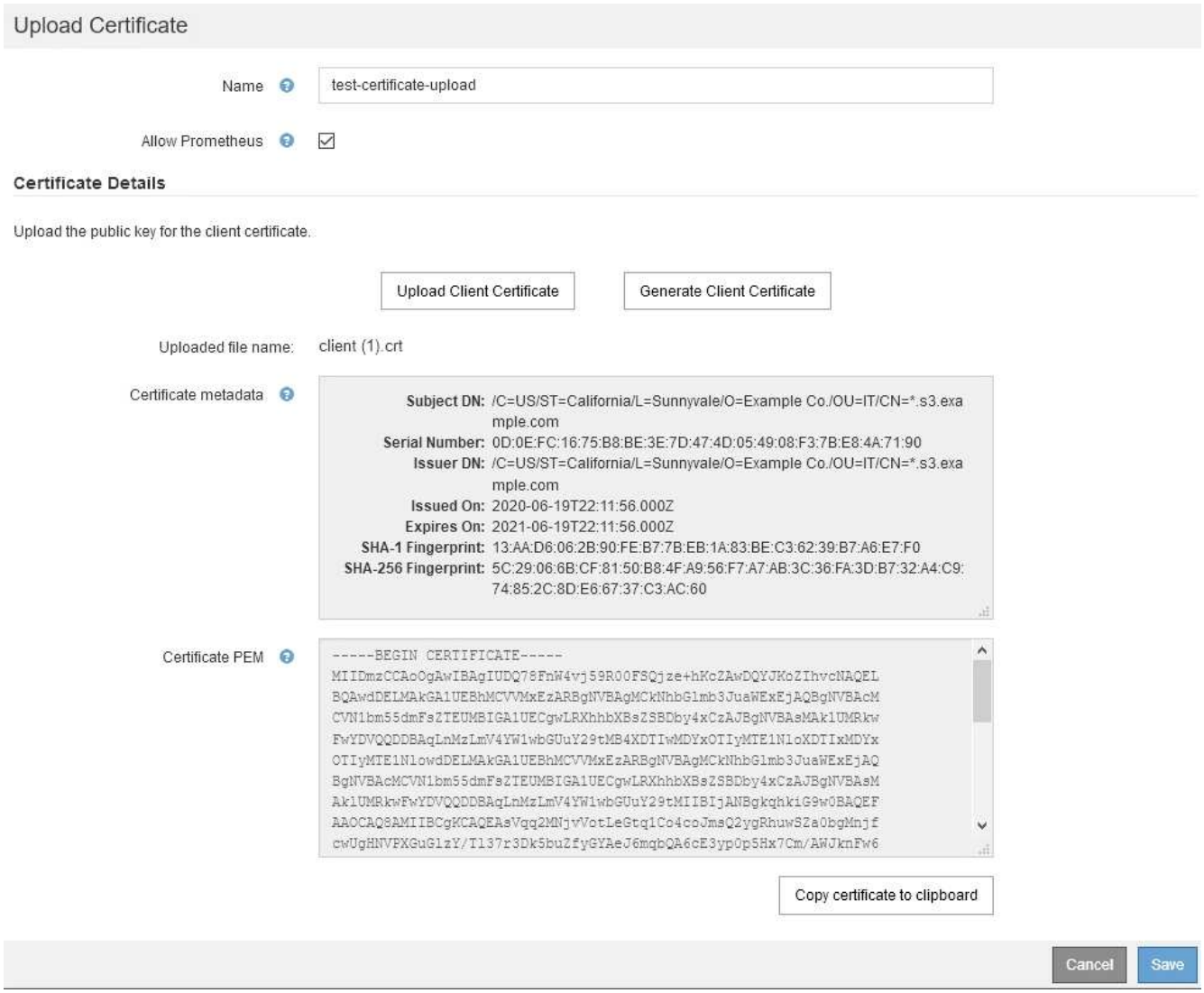
2. 「 * 追加」を選択します。

   証明書のアップロードページが表示されます。



3. 証明書の名前を1～32文字で入力します。
4. 外部の監視ツールを使用してPrometheus指標にアクセスするには、* Prometheus *を許可するチェックボックスをオンにします。
5. 証明書をアップロードまたは生成します。
   a. 証明書をアップロードするには、に進みます こちらをご覧ください。
   b. 証明書を生成するには、に進みます こちらをご覧ください。
6. [upload_cert]]証明書をアップロードするには、次の手順を実行します。
   a. [クライアント証明書のアップロード]を選択します。
   b. 証明書の公開鍵を参照します。

      証明書の公開鍵をアップロードすると、「Certificate metadata」フィールドと「Certificate PEM」フィールドに値が入力されます。



a. [証明書をクリップボードにコピーする*]を選択し、証明書を外部監視ツールに貼り付けます。

b. 編集ツールを使用して、秘密鍵をコピーして外部の監視ツールに貼り付けます。

c. 証明書をGrid Managerに保存するには、* Save *を選択します。

7. [generate-cert]]証明書を生成するには、次の手順を実行します。

a. [クライアント証明書の生成]を選択します。

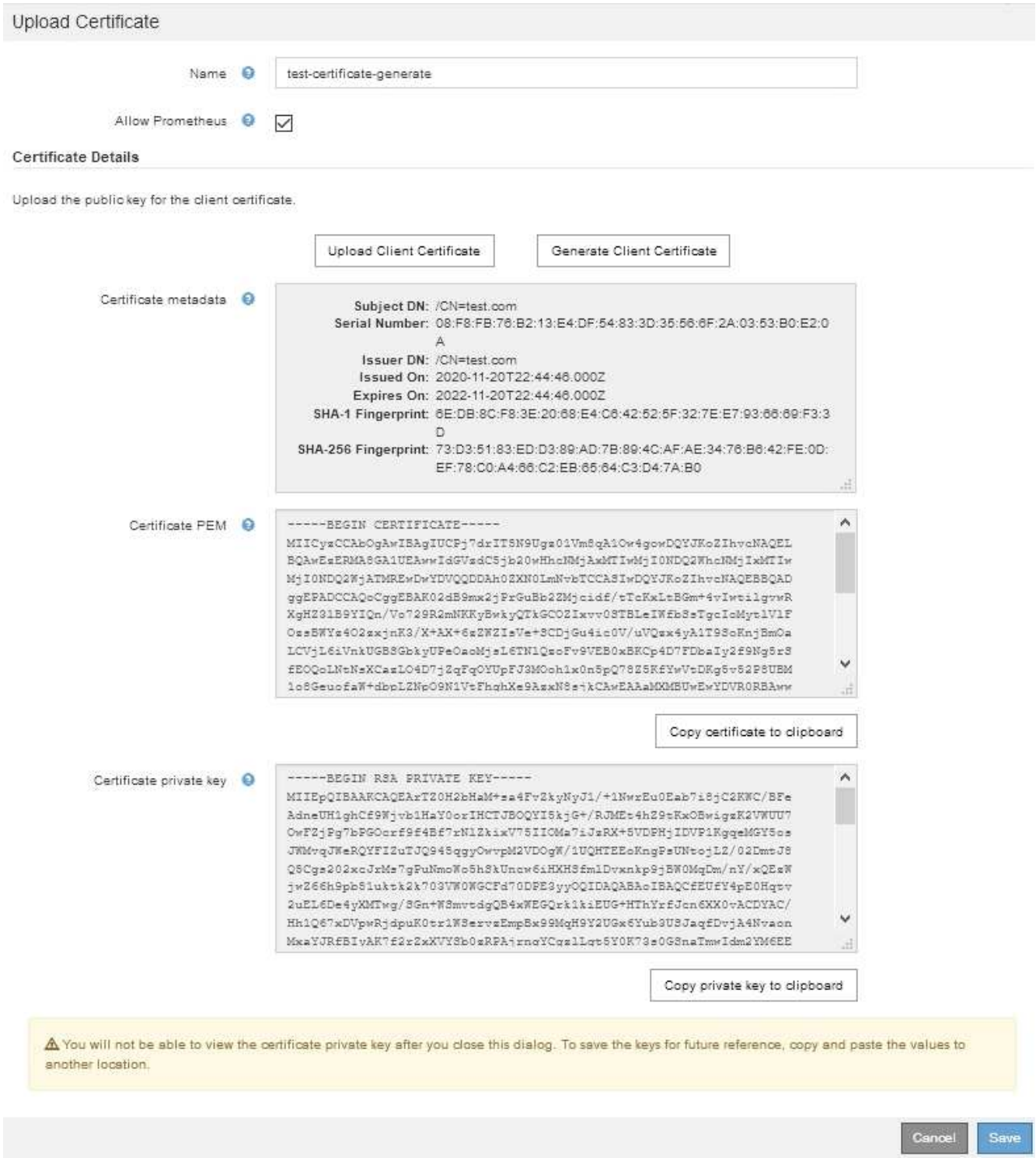
b. 管理ノードのドメイン名またはIPアドレスを入力します。

c. 必要に応じて、証明書を所有する管理者を識別するために、[X.509 subject（Distinguished Name（DN;認定者名）]とも呼ばれる）を入力します。

d. 必要に応じて、証明書の有効日数を選択します。デフォルトは730日です。

e. [*Generate （生成）] を選択します

「* Certificate metadata 」、「 Certificate PEM *」、および「Certificate private key *」の各フィールドに値が入力されます。



a. [証明書をクリップボードにコピーする*]を選択し、証明書を外部監視ツールに貼り付けます。

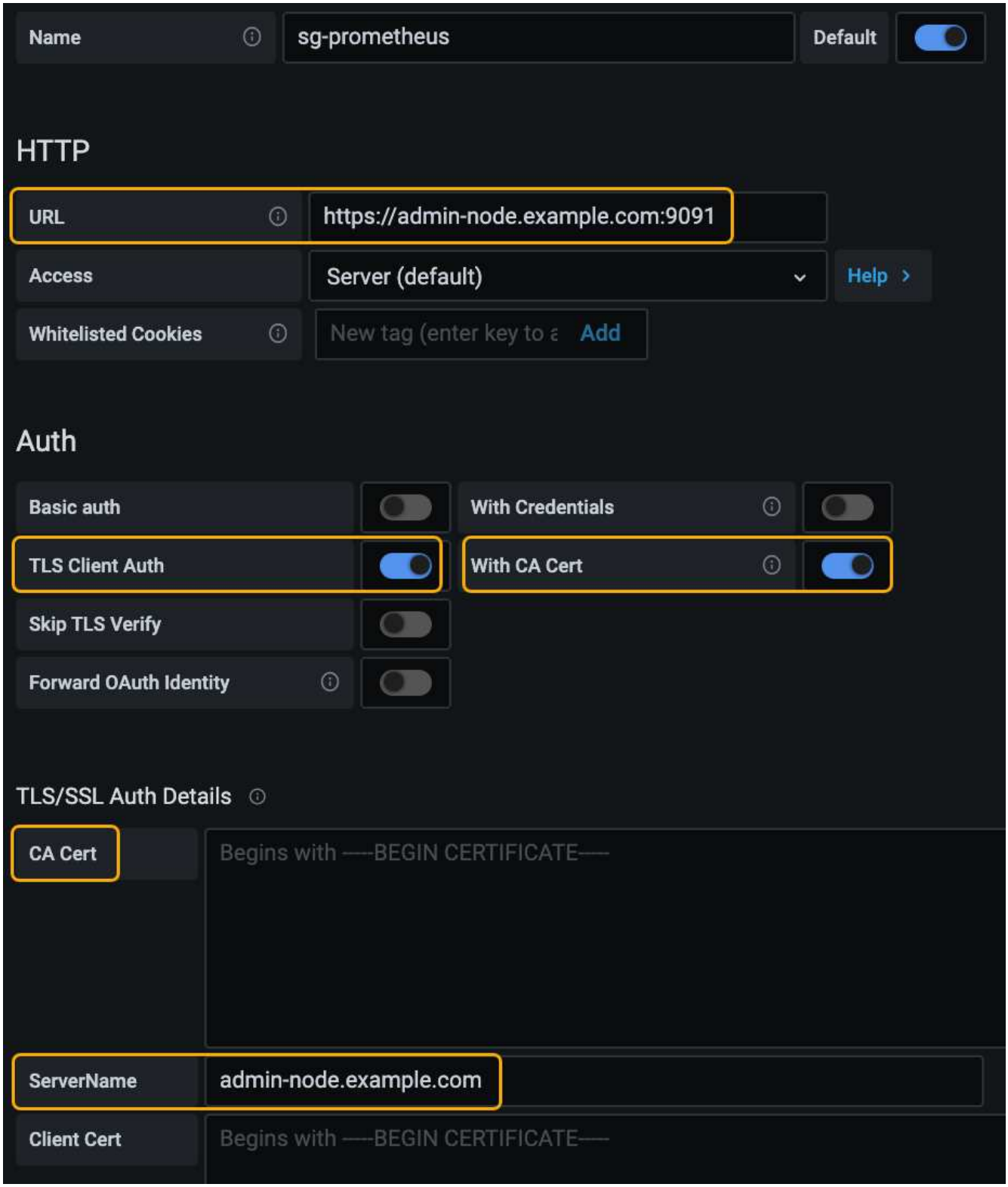
b. 秘密鍵をクリップボードにコピー*を選択し、外部監視ツールに貼り付けます。

> このダイアログボックスを閉じると、秘密鍵を表示できなくなります。キーを安全な場所にコピーします。

c. 証明書をGrid Managerに保存するには、* Save *を選択します。

8. Grafana などの外部監視ツールで次の設定を行います。

Grafana の例は次のスクリーンショットで示されています。



a. * 名前 * ：接続の名前を入力します。

   StorageGRID ではこの情報は必要ありませんが、接続をテストするための名前を指定する必要があります。

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

ます。

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

c. CA証明書を使用して、* TLSクライアント認証*および*を有効にします。

d. TLS/SSL Auth Detailsの下で、管理インターフェイスのサーバ証明書またはCAバンドルを**CA Cert**にコピーして貼り付けます。

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のサーバ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。

f. StorageGRID またはローカルファイルからコピーした証明書と秘密鍵を保存してテストします。

これで、外部の監視ツールを使用して StorageGRID から Prometheus 指標にアクセスできるようになります。

指標の詳細については、StorageGRID の監視とトラブルシューティングの手順を参照してください。

関連情報

"StorageGRID セキュリティ証明書を使用する"

"Grid ManagerおよびTenant Manager用のカスタムサーバ証明書を設定する"

"トラブルシューティングを監視します"

管理者クライアント証明書の編集

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

必要なもの

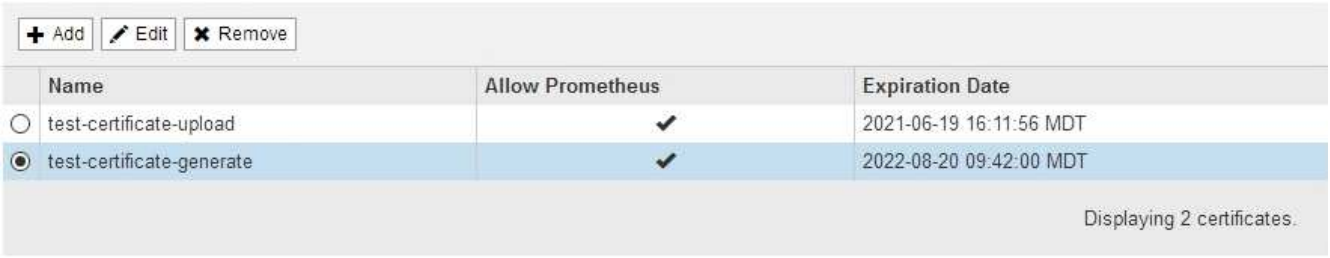
- Root Access 権限が必要です。
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 管理ノードのIPアドレスまたはドメイン名を確認しておく必要があります。
- 新しい証明書と秘密鍵をアップロードする場合は、ローカルコンピュータ上でそれらの証明書が使用可能である必要があります。

手順

1. [* Configuration > Access Control > Client Certificates *]を選択します。

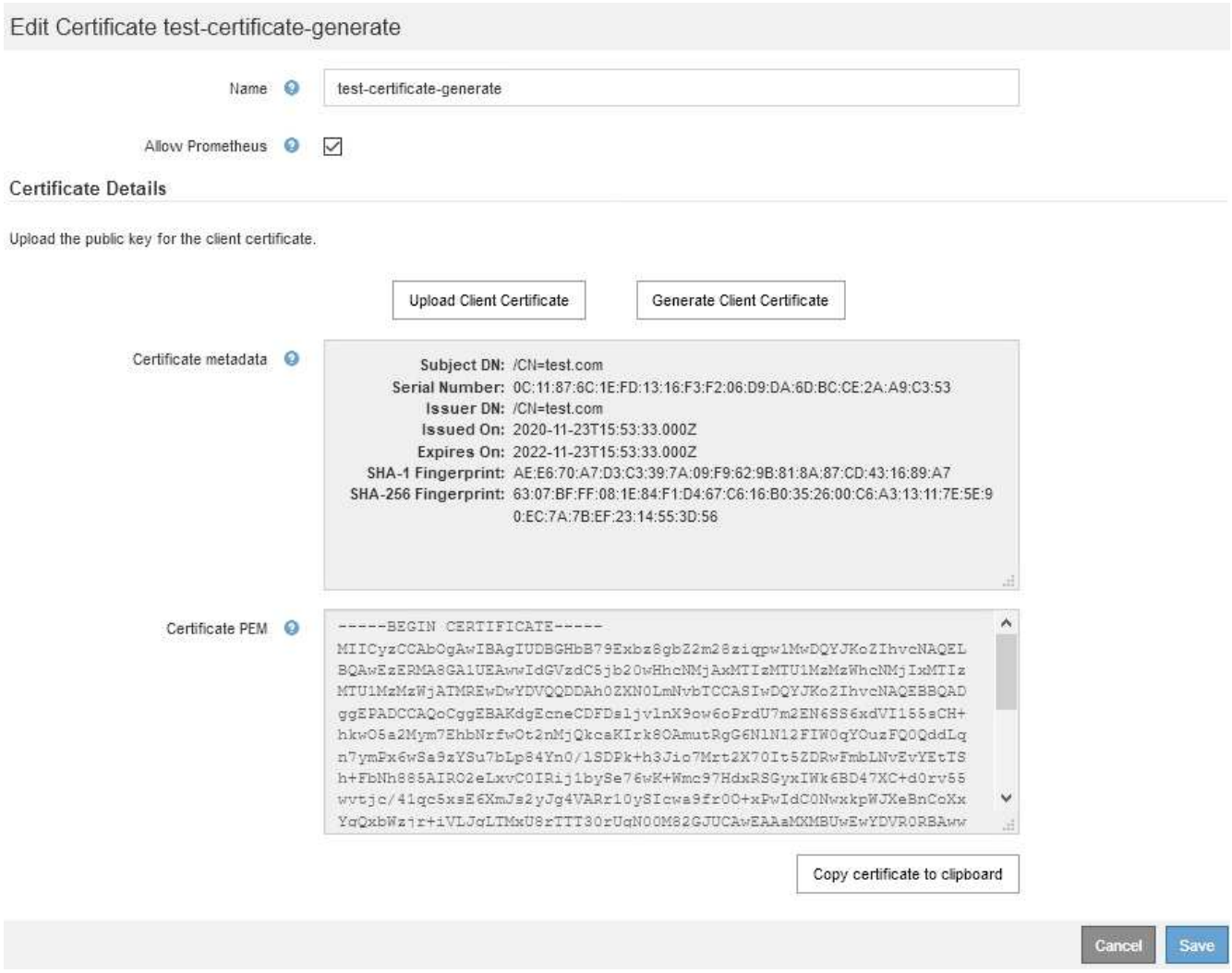
[Client Certificates]ページが表示されます。既存の証明書のリストが表示されます。

証明書の有効期限が表に記載されています。証明書の有効期限が近づいた場合、またはすでに有効期限が切れた場合は、メッセージが表に表示され、アラートがトリガーされます。



2. 編集する証明書の左側にあるオプションボタンを選択します。
3. 「 * 編集 * 」を選択します。

   [Edit Certificate]ダイアログボックスが表示されます。



4. 証明書に必要な変更を加えます。
5. 証明書をGrid Managerに保存するには、* Save *を選択します。
6. 新しい証明書をアップロードした場合：
   a. [証明書をクリップボードにコピーする*]を選択して、証明書を外部監視ツールに貼り付けます。
   b. 編集ツールを使用して、新しい秘密鍵をコピーして外部の監視ツールに貼り付けます。
   c. 外部の監視ツールで証明書と秘密鍵を保存してテストします。

7. 新しい証明書を生成した場合：
   a. [証明書をクリップボードにコピーする*]を選択して、証明書を外部監視ツールに貼り付けます。
   b. [プライベートキーをクリップボードにコピーする*]を選択して、証明書を外部監視ツールに貼り付けます。

      このダイアログボックスを閉じると、秘密鍵を表示したりコピーしたりすることはできなくなります。キーを安全な場所にコピーします。

   c. 外部の監視ツールで証明書と秘密鍵を保存してテストします。

管理者クライアント証明書を削除しています

不要になった証明書は削除できます。

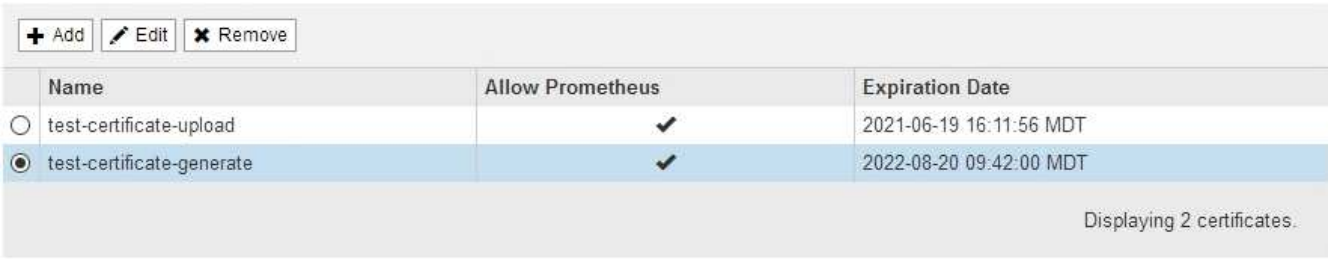
必要なもの

- Root Access 権限が必要です。
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

手順

1. [* Configuration > Access Control > Client Certificates *]を選択します。

   [Client Certificates]ページが表示されます。既存の証明書のリストが表示されます。



2. 削除する証明書の左側にあるオプションボタンを選択します。
3. 「 * 削除」を選択します。

   確認のダイアログボックスが表示されます。

4. 「 * OK 」を選択します。

証明書が削除されます。

キー管理サーバを設定しています

1 つ以上の外部キー管理サーバ（ KMS ）を設定して、特別に設定したアプライアンスノード上のデータを保護することができます。

キー管理サーバ（ **KMS** ）とは何ですか？

キー管理サーバ（ KMS ）は、関連する StorageGRID サイトの StorageGRID アプライアンスノードに Key Management Interoperability Protocol （ KMIP ）を使用して暗号化キーを提供する外部のサードパーティシステムです。

インストール時にノード暗号化 * 設定が有効になっている StorageGRID アプライアンスノードのノード暗号化キーを管理するには、 1 つ以上のキー管理サーバを使用します。これらのアプライアンスノードでキー管理サーバを使用すると、アプライアンスをデータセンターから削除した場合でも、データを保護できます。アプライアンスのボリュームを暗号化すると、ノードが KMS と通信できないかぎり、アプライアンスのデータにアクセスすることはできません。

> StorageGRID では、アプライアンスノードの暗号化と復号化に使用する外部キーは作成も管理もされません。外部キー管理サーバを使用して StorageGRID データを保護する場合は、そのサーバの設定方法を理解し、暗号化キーの管理方法を理解しておく必要があります。キー管理タスクの実行については、この手順では説明していません。サポートが必要な場合は、キー管理サーバのドキュメントを参照するか、テクニカルサポートにお問い合わせください。

StorageGRID 暗号化方式の確認

StorageGRID には、データを暗号化するためのさまざまなオプションがあります。使用可能な方法を確認して、データ保護の要件を満たす方法を決定する必要があります。

次の表に、 StorageGRID で使用できる暗号化方式の概要を示します。

暗号化オプション	動作の仕組み	環境
Grid Manager からキー管理サーバ（ KMS ）を取得します	StorageGRID サイト用のキー管理サーバ（* Configuration > System Settings > Key Management Server *）を設定し、アプライアンスでノード暗号化を有効にします。次に、アプライアンスノードが KMS に接続して、 Key Encryption Key （ KEK ；キー暗号化キー）を要求します。このキーは、各ボリュームのデータ暗号化キー（ DEK ）を暗号化および復号化します。	インストール中にノード暗号化 * が有効になっているアプライアンスノード。アプライアンスのすべてのデータは、物理的な損失やデータセンターからの削除から保護されます。一部の StorageGRID ストレージおよびサービスアプライアンスで使用できます。

暗号化オプション	動作の仕組み	環境
SANtricity System Manager のドライブセキュリティ	ストレージアプライアンスでドライブセキュリティ機能が有効になっている場合は、 SANtricity System Manager を使用してセキュリティキーを作成および管理できます。このキーは、セキュリティ保護されたドライブ上のデータにアクセスするために必要です。	Full Disk Encryption （ FDE ）ドライブまたは連邦情報処理標準（ FIPS ）ドライブが搭載されたストレージアプライアンス。セキュリティ保護されたドライブ上のデータは、すべて物理的な損失やデータセンターからの削除から保護されます。一部のストレージアプライアンスまたはサービスアプライアンスでは使用できません。 "SG6000 ストレージアプライアンス" "SG5700 ストレージアプライアンス" "SG5600 ストレージアプライアンス"
格納オブジェクトの暗号化グリッドオプション	• Stored Object Encryption オプションは**Grid Manager**で有効にできます（ Configuration > System Settings > Grid Options *）。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。	新たに取り込まれたS3およびSwiftオブジェクトデータ。格納されている既存のオブジェクトは暗号化されません。オブジェクトメタデータやその他の機密データは暗号化されません。 "格納オブジェクトの暗号化を設定する"
S3 バケットの暗号化	バケットの暗号化を有効にするには、 PUT Bucket 暗号化要求を問題 に設定します。オブジェクトレベルで暗号化されていない新しいオブジェクトは取り込み時に暗号化されます。	新たに取り込まれたS3オブジェクトデータのみ。バケットに暗号化を指定する必要があります。既存のバケットオブジェクトは暗号化されません。オブジェクトメタデータやその他の機密データは暗号化されません。 "S3 を使用する"

暗号化オプション	動作の仕組み	環境
S3 オブジェクトのサーバ側の暗号化（ SSE ）	オブジェクトを格納してを含めるS3要求を問題 した `x-amz-server-side-encryption` 要求ヘッダー。	新たに取り込まれたS3オブジェクトデータのみ。オブジェクトに暗号化を指定する必要があります。オブジェクトメタデータやその他の機密データは暗号化されません。 キーは StorageGRID で管理されます。 "S3 を使用する"
ユーザ指定のキーによる S3 オブジェクトのサーバ側暗号化（ SSE-C ）	オブジェクトを格納する S3 要求を問題 し、 3 つの要求ヘッダーを含めます。 • `x-amz-server-side-encryption-customer-algorithm` • `x-amz-server-side-encryption-customer-key` • `x-amz-server-side-encryption-customer-key-MD5`	新たに取り込まれたS3オブジェクトデータのみ。オブジェクトに暗号化を指定する必要があります。オブジェクトメタデータやその他の機密データは暗号化されません。 キーは StorageGRID の外部で管理されます。 "S3 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暗号化がサポートされている場合は、StorageGRID の外部の暗号化方式を使用して、ボリュームまたはデータストア全体を暗号化できます。	すべてのボリュームまたはデータストアが暗号化されていることを前提として、すべてのオブジェクトデータ、メタデータ、およびシステム構成データ。 外部暗号化方式を使用すると、暗号化アルゴリズムと暗号キーを厳密に制御できます。は、記載されている他の方法と組み合わせることができます。

暗号化オプション	動作の仕組み	環境
StorageGRID の外部でのオブジェクトの暗号化	StorageGRID に取り込まれる前にオブジェクトデータとメタデータを暗号化するには、 StorageGRID の外部の暗号化メソッドを使用します。	オブジェクトデータとメタデータのみ（システム設定データは暗号化されません）。 外部暗号化方式を使用すると、暗号化アルゴリズムと暗号キーを厳密に制御できます。は、記載されている他の方法と組み合わせることができます。 "Amazon Simple Storage Service - Developer Guide ：クライアント側の暗号化を使用したデータの保護"

複数の暗号化方式を使用する

要件に応じて、一度に複数の暗号化方式を使用できます。例：

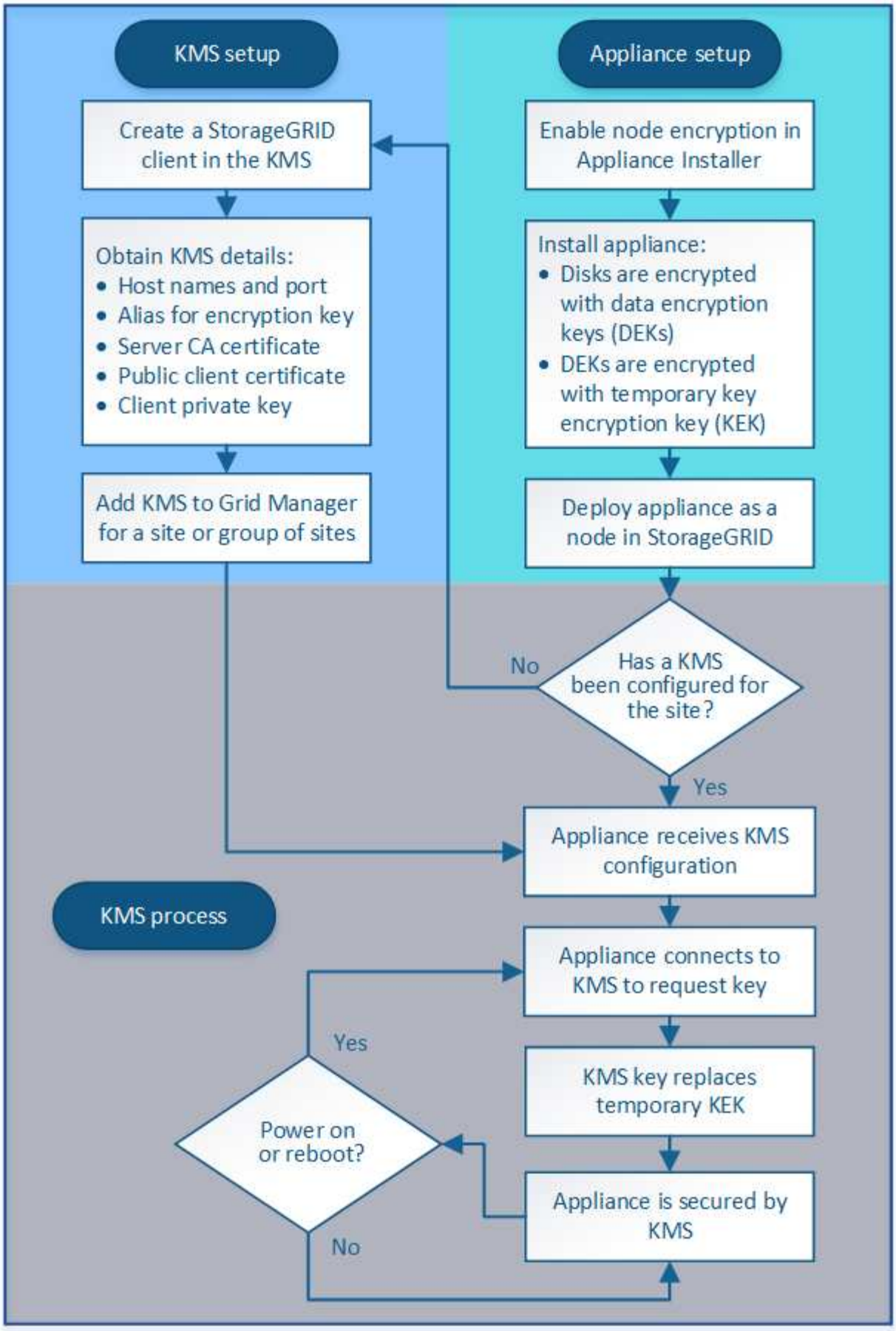
- KMS を使用してアプライアンスノードを保護したり、 SANtricity システムマネージャのドライブセキュリティ機能を使用して、同じアプライアンス内の自己暗号化ドライブ上のデータを「二重に暗号化」することもできます。
- KMS を使用してアプライアンスノード上のデータを保護したり、格納されているオブジェクト暗号化グリッドオプションを使用してすべてのオブジェクトを取り込み時に暗号化することもできます。

暗号化を必要とするオブジェクトがごく一部しかない場合は、暗号化をバケットレベルまたは個々のオブジェクトレベルで制御することを検討してください。複数レベルの暗号化を有効にすると、パフォーマンスコストが増加します。

KMS とアプライアンスの設定の概要

キー管理サーバ（ KMS ）を使用してアプライアンスノード上の StorageGRID データを保護する前に、 1 つ以上の KMS サーバを設定してアプライアンスノードのノード暗号化を有効にするという 2 つの設定タスクを完了しておく必要があります。これらの 2 つの設定タスクが完了すると、キー管理プロセスが自動的に実行されます。

フローチャートは、 KMS を使用してアプライアンスノード上の StorageGRID データを保護する手順の概要を示しています。



フローチャートには、 KMS のセットアップとアプライアンスのセットアップが並行して行われていることが

示されています。ただし、要件に基づいて、新しいアプライアンスノードのノード暗号化を有効にする前後にキー管理サーバをセットアップできます。

キー管理サーバのセットアップ（KMS）

キー管理サーバのセットアップには、主に次の手順が含まれます。

ステップ	を参照してください
KMS ソフトウェアにアクセスし、各 KMS または KMS クラスタに StorageGRID 用のクライアントを追加します。	"KMSでクライアントとしてStorageGRID を設定する"
KMS で StorageGRID クライアントの必要な情報を入手します。	"KMSでクライアントとしてStorageGRID を設定する"
Grid Manager に KMS を追加して 1 つのサイトまたはデフォルトのサイトグループに割り当て、必要な証明書をアップロードして、 KMS の設定を保存します。	"キー管理サーバの追加（KMS）"

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セットアップするには、次の手順に従います。

1. アプライアンスのハードウェア構成フェーズでは、 StorageGRID アプライアンスインストーラを使用してアプライアンスのノード暗号化 * 設定を有効にします。

   > グリッドにアプライアンスを追加したあとに * Node Encryption * 設定を有効にすることはできません。また、ノード暗号化が有効になっていないアプライアンスでは外部キー管理を使用できません。

2. StorageGRID アプライアンスインストーラを実行します。インストール時に、次のように各アプライアンスボリュームにランダムデータ暗号化キー（ DEK ）が割り当てられます。
   - DEK は、各ボリュームのデータの暗号化に使用されます。これらのキーは、アプライアンス OS で Linux Unified Key Setup （ LUKS ； Linux Unified Key Setup ）ディスク暗号化を使用して生成され、変更することはできません。
   - 各 DEK は、 KEK （ Master Key Encryption Key ）によって暗号化されます。最初の KEK は、アプライアンスが KMS に接続できるまで DEK を暗号化する一時キーです。
3. StorageGRID にアプライアンスノードを追加します。

詳細については、次を参照してください。

- "SG100 SG1000サービスアプライアンス"
- "SG6000 ストレージアプライアンス"
- "SG5700 ストレージアプライアンス"
- "SG5600 ストレージアプライアンス"

キー管理の暗号化プロセス（自動的に実行）

キー管理の暗号化には、次の高度な手順が含まれています。これらの手順は自動的に実行されます。

1. ノードの暗号化が有効になっているアプライアンスをグリッドにインストールすると、 StorageGRID は、新しいノードを含むサイトに KMS 設定が存在するかどうかを確認します。
   - KMS がすでにサイト用に設定されている場合、アプライアンスは KMS の設定を受信します。
   - KMS がサイト用にまだ設定されていない場合は、サイトに KMS を設定し、アプライアンスが KMS の設定を受信するまで、アプライアンス上のデータは一時的な KEK によって暗号化されたままになります。
2. アプライアンスは KMS 設定を使用して KMS に接続し、暗号化キーを要求します。
3. KMS は暗号化キーをアプライアンスに送信します。KMS の新しいキーは一時的な KEK に代わるものであり、アプライアンスボリュームの DEK の暗号化と復号化に使用されるようになりました。

   暗号化されたアプライアンスノードから設定された KMS に接続する前に存在するデータは、すべて一時キーで暗号化されます。ただし、一時キーを KMS 暗号化キーに置き換えるまでは、アプライアンスボリュームをデータセンターから削除できないようにする必要があります。

4. アプライアンスの電源をオンにするか再接続すると、 KMS に接続してキーを要求します。揮発性メモリに保存されたキーは、停電や再起動の際に存続することはできません。

キー管理サーバを使用する際の考慮事項と要件

外部キー管理サーバ（ KMS ）を設定する前に、考慮事項と要件を確認しておく必要があります。

KMIP の要件

StorageGRID は KMIP バージョン 1.4 をサポートしています。

"Key Management Interoperability Protocol （キー管理相互運用性プロトコル）仕様バージョン 1.4"

アプライアンスノードと設定された KMS の間の通信には、セキュアな TLS 接続が使用されます。StorageGRID では、 KMIP で次の TLS v1.2 暗号をサポートしています。

- TLS_ECDHE_RSA_with _AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_With _AES_256_GCM_SHA384

ノード暗号化を使用する各アプライアンスノードに、サイト用に設定した KMS または KMS クラスタへのネットワークアクセスがあることを確認してください。

ネットワークのファイアウォールの設定で、各アプライアンスノードが Key Management Interoperability Protocol （ KMIP ）の通信に使用するポートを介して通信できるようにする必要があります。デフォルトの KMIP ポートは 5696 です。

サポートされているアプライアンスはどれですか。

キー管理サーバ（ KMS ）を使用して、「ノード暗号化 * 」が有効になっているグリッド内の StorageGRID アプライアンスの暗号化キーを管理できます。この設定は、 StorageGRID アプライアンスインストーラを使

用してアプライアンスをインストールするハードウェア構成の段階でのみ有効にできます。

> グリッドにアプライアンスを追加したあとにノードの暗号化を有効にすることはできません。また、ノード暗号化が有効になっていないアプライアンスでは外部キー管理を使用できません。

設定されている KMS は、次の StorageGRID アプライアンスおよびアプライアンスノードで使用できます。

アプライアンス	ノードタイプ
SG1000 サービスアプライアンス	管理ノードまたはゲートウェイノード
SG100 サービスアプライアンス	管理ノードまたはゲートウェイノード
SG6000 ストレージアプライアンス	ストレージノード
SG5700 ストレージアプライアンス	ストレージノード
SG5600 ストレージアプライアンス	ストレージノード

次のようなソフトウェアベース（非アプライアンス）のノードでは、設定された KMS を使用することはできません。

- 仮想マシン（ VM ）として導入されたノード
- Linuxホスト上のDockerコンテナ内に導入されたノード

これらの他のプラットフォームに導入されたノードでは、データストアまたはディスクレベルで StorageGRID 外部の暗号化を使用できます。

キー管理サーバを設定する必要があるのはいつですか？

新規インストールの場合は、テナントを作成する前に Grid Manager で 1 つ以上のキー管理サーバをセットアップするのが一般的です。この順序により、ノード上に格納されるオブジェクトデータよりも先にノードが保護されます。

Grid Manager では、アプライアンスノードのインストール前またはインストール後にキー管理サーバを設定できます。

必要なキー管理サーバの数

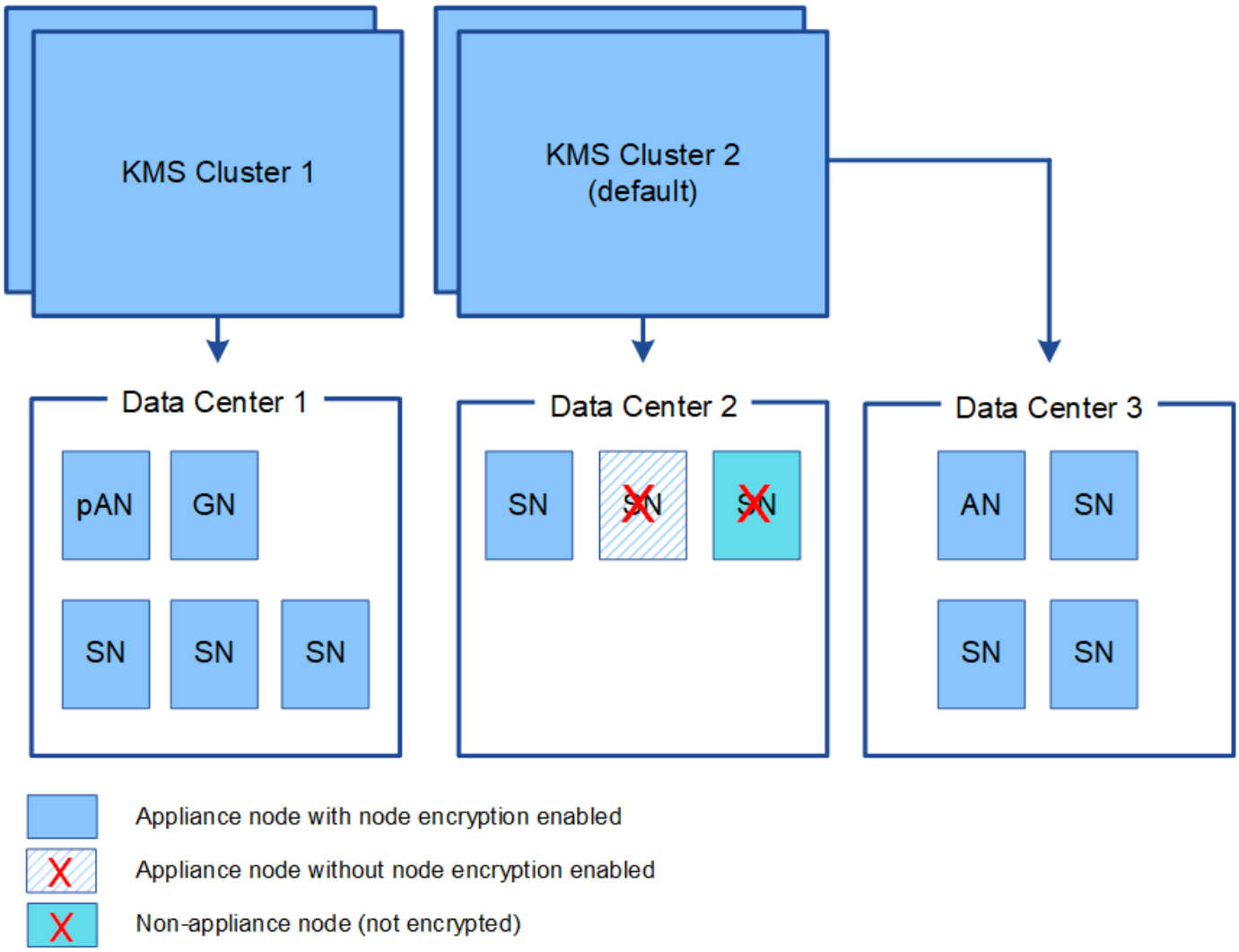
1 つ以上の外部キー管理サーバを設定して、 StorageGRID システム内のアプライアンスノードに暗号化キーを提供できます。各 KMS は、 1 つのサイトまたはサイトグループにある StorageGRID アプライアンスノードに単一の暗号化キーを提供します。

StorageGRID は KMS クラスタの使用をサポートしています。各 KMS クラスタには、設定と暗号化キーを共有するレプリケートされた複数のキー管理サーバが含まれます。高可用性構成のフェイルオーバー機能が向上するため、 KMS クラスタをキー管理に使用することを推奨します。

たとえば、 StorageGRID システムに 3 つのデータセンターサイトがあるとします。1 つの KMS クラスタを設定して、データセンター 1 のすべてのアプライアンスノードともう 1 つの KMS クラスタのキーを取得し、

他のすべてのサイトにあるすべてのアプライアンスノードのキーを取得することができます。2 つ目の KMS クラスタを追加すると、データセンター 2 とデータセンター 3 にデフォルトの KMS を設定できます。

非アプライアンスノードや、インストール時に * Node Encryption * が有効になっていない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どうなりますか。

セキュリティのベストプラクティスとして、設定された各 KMS で使用される暗号化キーを定期的にローテーションすることを推奨します。

暗号化キーをローテーションするときは、 KMS ソフトウェアを使用して、最後に使用したバージョンのキーを同じキーの新しいバージョンにローテーションします。完全に別のキーに回転させないでください。

> キーのローテーションは、 Grid Manager 内の KMS のキー名（エイリアス）を変更しては実行しないでください。代わりに、 KMS ソフトウェアのキーバージョンを更新してキーをローテーションしてください。以前のキーに使用したものと同じキーエイリアスを新しいキーに使用します。設定されている KMS のキーエイリアスを変更すると、 StorageGRID がデータを復号化できなくなる可能性があります。

新しいキーバージョンが利用可能になった場合：

- このサービスは、 KMS に関連付けられているサイトにある暗号化されたアプライアンスノードに自動的に配信されます。キーが回転した後 1 時間以内に分配が行われる必要があります。
- 新しいキーバージョンが配布されたときに暗号化アプライアンスノードがオフラインになっている場合、ノードはリブート後すぐに新しいキーを受け取ります。
- 何らかの理由でアプライアンスボリュームの暗号化に新しいキーバージョンを使用できない場合は、アプライアンスノードに対して * KMS 暗号化キーローテーション failed * アラートがトリガーされます。このアラートの解決方法については、テクニカルサポートへの問い合わせが必要になることがあります。

アプライアンスノードは暗号化したあとに再利用できますか。

暗号化されたアプライアンスを別の StorageGRID システムにインストールする必要がある場合は、先にグリッドノードの運用を停止して、オブジェクトデータを別のノードに移動しておく必要があります。その後、StorageGRID アプライアンスインストーラを使用して KMS の設定をクリアします。KMS の設定をクリアすると、「ノード暗号化 * 」設定が無効になり、アプライアンスノードと StorageGRID サイトの KMS 設定の間の関連付けが解除されます。

KMS 暗号化キーにアクセスできないため、アプライアンスに残っているデータにはアクセスできなくなり、永続的にロックされます。

"SG100 SG1000サービスアプライアンス"

"SG6000 ストレージアプライアンス"

"SG5700 ストレージアプライアンス"

"SG5600 ストレージアプライアンス"

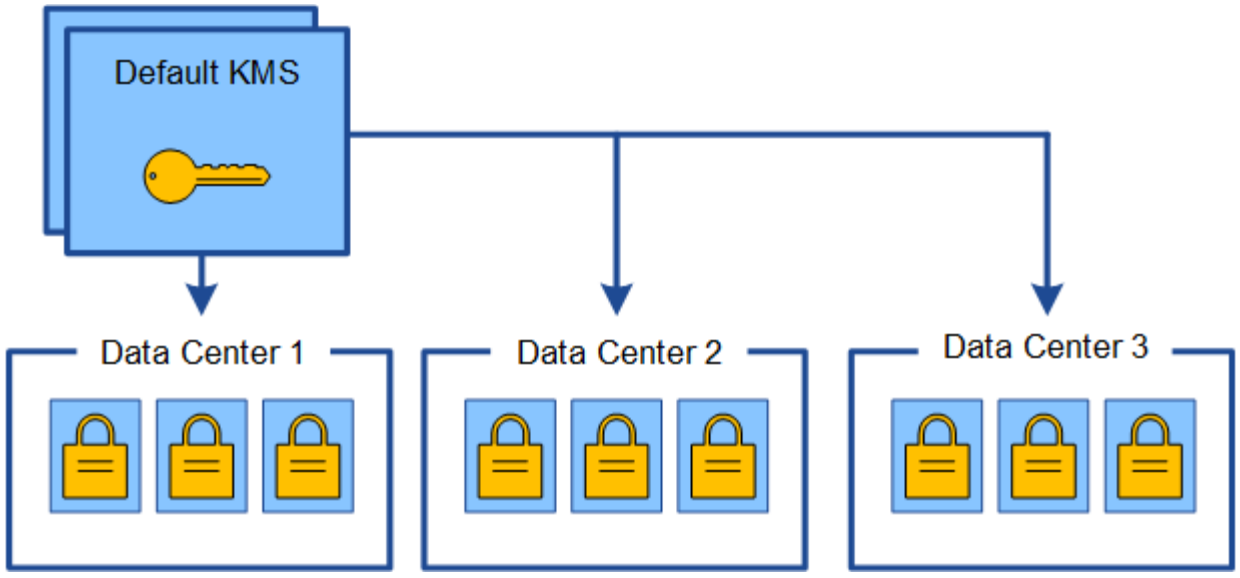
サイトの **KMS** を変更する際の考慮事項

各キー管理サーバ（ KMS ）または KMS クラスタは、 1 つのサイトまたはサイトグループにあるすべてのアプライアンスノードに暗号化キーを提供します。サイトで使用する KMS を変更する必要がある場合は、暗号化キーを KMS から別の KMS にコピーする必要があります。

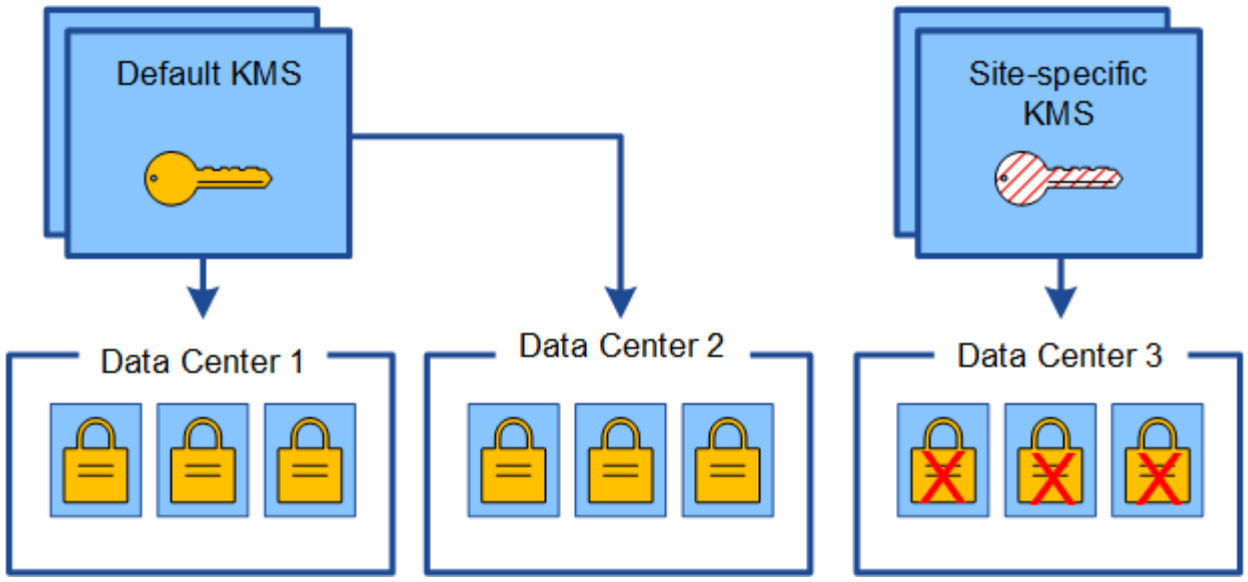
サイトで使用されている KMS を変更する場合は、そのサイトで以前に暗号化したアプライアンスノードを新しい KMS に格納されているキーを使用して復号化できることを確認する必要があります。場合によっては、暗号化キーの現在のバージョンを元の KMS から新しい KMS にコピーする必要があります。サイトで暗号化されたアプライアンスノードを復号化するために、 KMS に正しいキーがあることを確認する必要があります。

例：

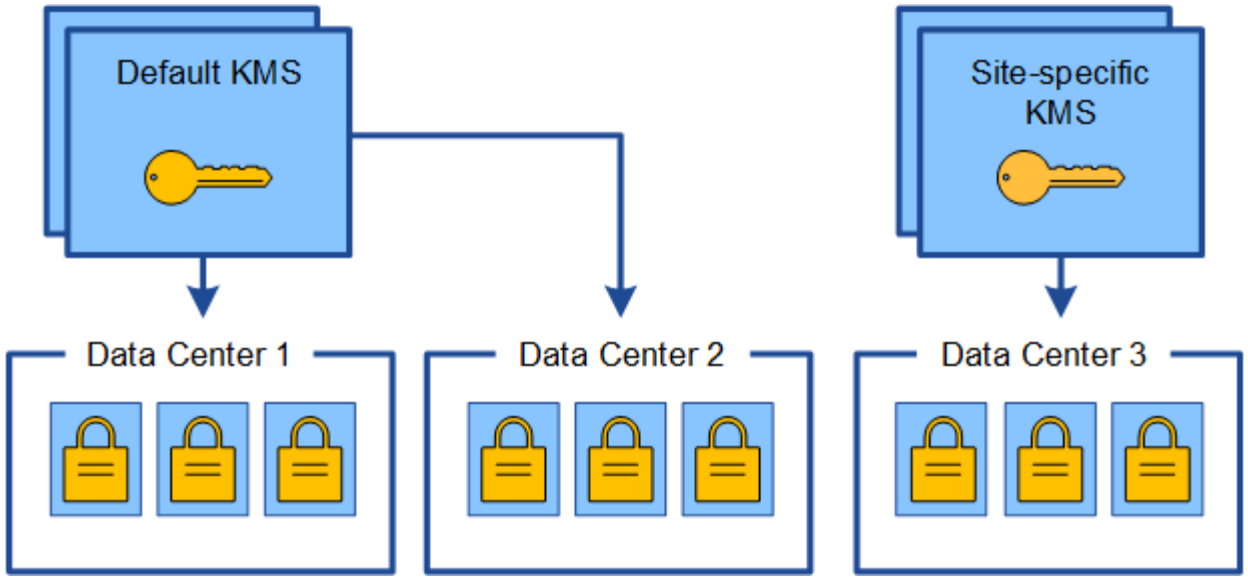
1. 最初に、専用の KMS がない環境 のすべてのサイトを設定します。
2. KMS を保存すると、「 Node Encryption * 」設定が有効になっているすべてのアプライアンスノードが KMS に接続して暗号化キーを要求します。このキーは、すべてのサイトのアプライアンスノードの暗号化に使用されます。同じキーを使用して、これらのアプライアンスを復号化する必要もあります。



3. 1 つのサイト（図のデータセンター 3 ）にサイト固有の KMS を追加することにしました。ただし、アプライアンスノードはすでに暗号化されているため、サイト固有の KMS の設定を保存しようとすると検証エラーが発生します。このエラーは、サイト固有の KMS に、そのサイトでノードを復号化するための正しいキーがないことが原因で発生します。



4. 問題 に対応するには、現在のバージョンの暗号化キーをデフォルトの KMS から新しい KMS にコピーします。（技術的には、元のキーを同じエイリアスを持つ新しいキーにコピーします。元のキーが新しいキーの前のバージョンになります）。 サイト固有の KMS に、データセンター 3 でアプライアンスノードを復号化するための正しいキーが付与されるようになり、 StorageGRID に保存できるようになりました。



サイトに使用する **KMS** を変更するユースケース

次の表に、サイトの KMS を変更する一般的なケースに必要な手順をまとめます。

サイトの **KMS** を変更するユースケース	必要な手順
サイト固有の KMS エントリが 1 つ以上あり、それらのエントリの 1 つをデフォルトの KMS として使用する必要があります。	サイト固有の KMS を編集します。[* キー管理対象 *] フィールドで、別の KMS （デフォルト KMS ）で管理されていないサイト * を選択します。サイト固有の KMS がデフォルトの KMS として使用されるようになります。専用の KMS を使用していないサイトにも適用されます。 "キー管理サーバの編集（KMS）"
デフォルトの KMS を使用して、拡張時に新しいサイトを追加する必要があります。新しいサイトにはデフォルトの KMS を使用しないでください。	1. 新しいサイトにあるアプライアンスノードがデフォルトの KMS によって暗号化済みの場合は、KMS ソフトウェアを使用して、現在のバージョンの暗号化キーをデフォルトの KMS から新しい KMS にコピーします。 2. Grid Manager を使用して新しい KMS を追加し、サイトを選択します。 "キー管理サーバの追加（KMS）"

サイトの **KMS** を変更するユースケース	必要な手順
サイトの KMS で別のサーバを使用するとします。	1. サイトのアプライアンスノードが既存の KMS によって暗号化済みの場合は、 KMS ソフトウェアを使用して、既存の KMS から新しい KMS に暗号化キーの現在のバージョンをコピーします。 2. Grid Manager を使用して既存の KMS 設定を編集し、新しいホスト名または IP アドレスを入力します。 "キー管理サーバの追加（KMS）"

KMSでクライアントとして**StorageGRID** を設定する

KMS を StorageGRID に追加する前に、各外部キー管理サーバまたは KMS クラスタのクライアントとして StorageGRID を設定する必要があります。

このタスクについて

これらの手順は、 Thales CipherTrust Manager k170v 、バージョン 2.0 、 2.1 、および 2.2 に適用されます。StorageGRID で別のキー管理サーバを使用する方法については、テクニカルサポートにお問い合わせください。

"Thales CipherTrust マネージャ"

手順

1. KMS ソフトウェアから、使用する KMS または KMS クラスタごとに StorageGRID クライアントを作成します。

   各 KMS は、 1 つのサイトまたはサイトグループにある StorageGRID アプライアンスノードの単一の暗号化キーを管理します。

2. KMS ソフトウェアから、 KMS または KMS クラスタごとに AES 暗号化キーを作成します。

   暗号化キーはエクスポート可能である必要があります。

3. KMS または KMS クラスタごとに次の情報を記録します。

   この情報は、 KMS を StorageGRID に追加するときに必要になります。

   - 各サーバのホスト名または IP アドレス。
   - KMS で使用される KMIP ポート。
   - KMS 内の暗号化キーのキーエイリアス。

   > ⓘ 暗号化キーは KMS にすでに存在している必要があります。StorageGRID は KMS キーを作成または管理しません。

4. KMS または KMS クラスタごとに、認証局（ CA ）が署名したサーバ証明書または PEM でエンコードされた各 CA 証明書ファイルを含む証明書バンドルを、証明書チェーンの順序で連結して取得します。

サーバ証明書を使用すると、外部 KMS は StorageGRID に対して自身を認証できます。

- 証明書では、 Privacy Enhanced Mail （ PEM ） Base-64 エンコード X.509 形式を使用する必要があります。
- 各サーバ証明書の Subject Alternative Name （ SAN ）フィールドには、 StorageGRID が接続する完全修飾ドメイン名（ FQDN ）または IP アドレスを含める必要があります。

> StorageGRID で KMS を設定する場合は、「 * Hostname * 」フィールドに同じ FQDN または IP アドレスを入力する必要があります。

- サーバ証明書は、 KMS の KMIP インターフェイスで使用されている証明書と一致する必要があります。通常はポート 5696 が使用されます。

5. 外部 KMS によって StorageGRID に発行されたパブリッククライアント証明書とクライアント証明書の秘密鍵を取得します。

   クライアント証明書は、 StorageGRID が KMS に対して自身を認証することを許可します。

キー管理サーバの追加（**KMS**）

StorageGRID キー管理サーバウィザードを使用して、各 KMS または KMS クラスタを追加します。

必要なもの

- を確認しておく必要があります "キー管理サーバを使用する際の考慮事項と要件"。
- が必要です "KMS でクライアントとして StorageGRID を設定"をクリックし、KMSまたはKMSクラスタごとに必要な情報を確認しておく必要があります
- Root Access 権限が必要です。
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

このタスクについて

可能環境 であれば、サイト固有のキー管理サーバを設定してから、別の KMS で管理されていないデフォルトの KMS を設定してください。最初にデフォルトの KMS を作成すると、グリッド内のノードで暗号化されたすべてのアプライアンスがデフォルトの KMS で暗号化されます。サイト固有の KMS をあとで作成するには、まず、暗号化キーの現在のバージョンをデフォルトの KMS から新しい KMS にコピーする必要があります。

"サイトの KMS を変更する際の考慮事項"

手順

1. "手順 1 ： KMS の詳細を入力します"
2. "手順 2 ：サーバ証明書をアップロードする"
3. "手順 3 ：クライアント証明書をアップロードする"

手順 **1** ： **KMS** の詳細を入力します

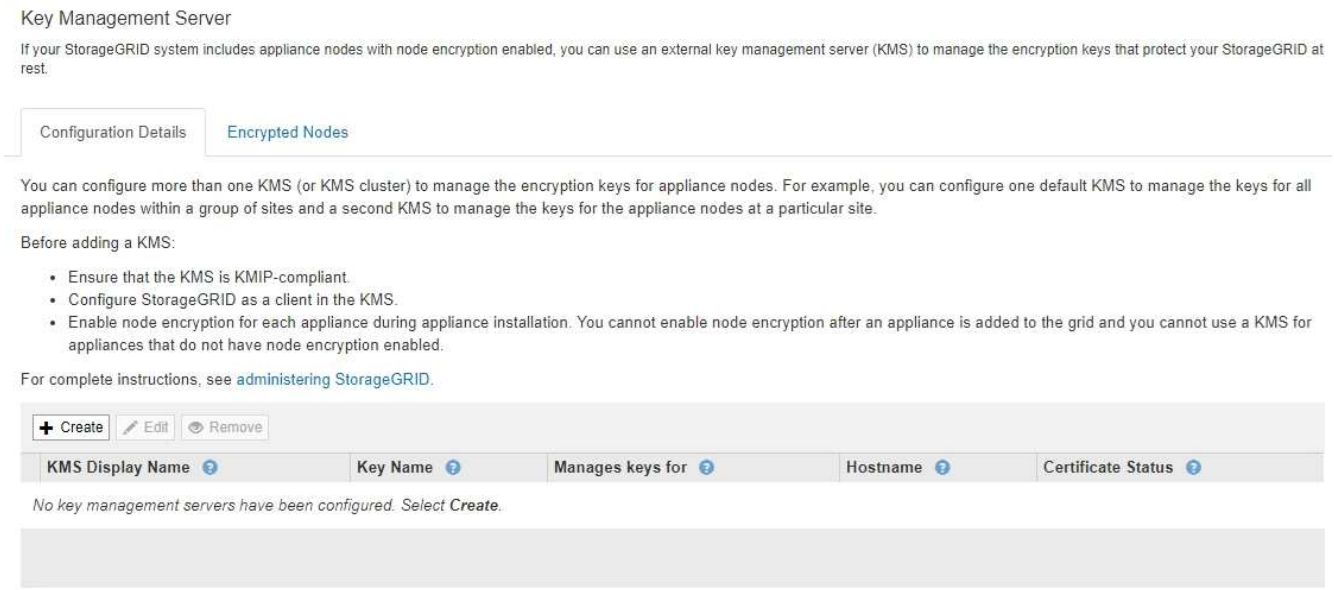
キー管理サーバの追加ウィザードの手順 1 （ KMS の詳細を入力）で、 KMS または

KMS クラスタの詳細を指定します。

手順

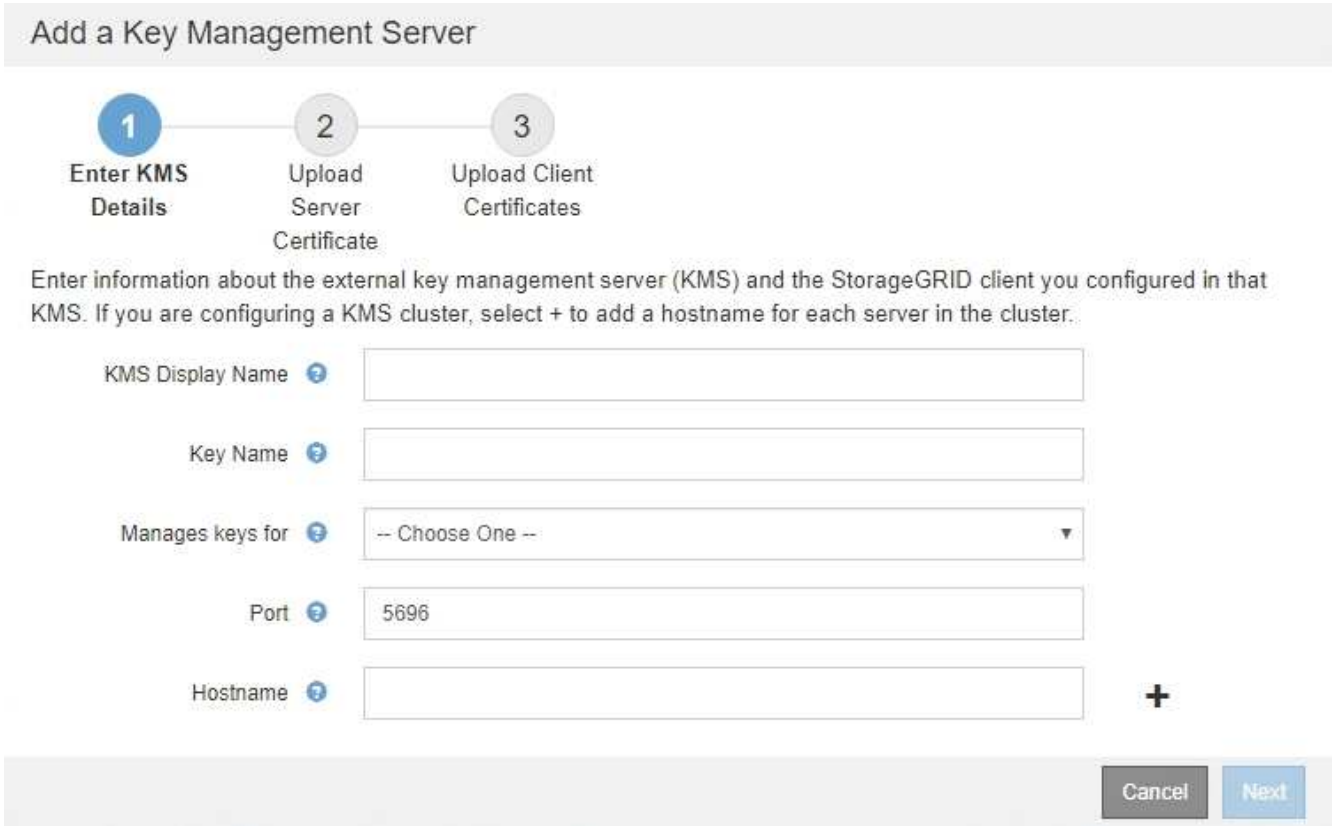
1. 「* Configuration * System Settings ** Key Management Server *」を選択します。

   [Key Management Server] ページが表示され、 [Configuration] [Details] タブが選択されます。



2. 「 * Create * 」を選択します。

   Add a Key Management Server （キー管理サーバの追加）ウィザードの手順 1 （ KMS の詳細を入力）が表示されます。



3. KMS および設定した StorageGRID クライアントの情報を KMS で入力します。

フィールド	説明
KMS 表示名	この KMS を特定するのに役立つわかりやすい名前。1~64 文字で指定します。
キー名	KMS 内の StorageGRID クライアントの正確なキーエイリアス。1~255 文字で指定する必要があります。
のキーを管理します	この KMS に関連する StorageGRID サイトを参照してください。可能であれば、サイト固有のキー管理サーバを設定してから、環境 で他の KMS で管理されていないすべてのサイトをデフォルトの KMS で設定する必要があります。 • 特定のサイトのアプライアンスノードの暗号化キーをこの KMS で管理する場合は、サイトを選択します。 • 「 * Sites not managed by another KMS （デフォルト KMS ） * 」を選択して、専用の KMS とその後の拡張で追加したサイトに適用されるデフォルトの KMS を設定します。 ◦ 注： * 以前にデフォルト KMS で暗号化されていたサイトを選択しても、新しい KMS に元の暗号化キーの現在のバージョンを提供しなかった場合、 KMS の設定を保存すると、検証エラーが発生します。
ポート	KMS サーバが Key Management Interoperability Protocol （ KMIP ）の通信に使用するポート。デフォルトでは、 KMIP 標準ポートである 5696 が使用されます。
ホスト名	KMS の完全修飾ドメイン名または IP アドレス。 • 注： * サーバ証明書の SAN フィールドには、ここに入力する FQDN または IP アドレスを含める必要があります。そうしないと、StorageGRID は KMS クラスタ内のすべてのサーバに接続できなくなります。

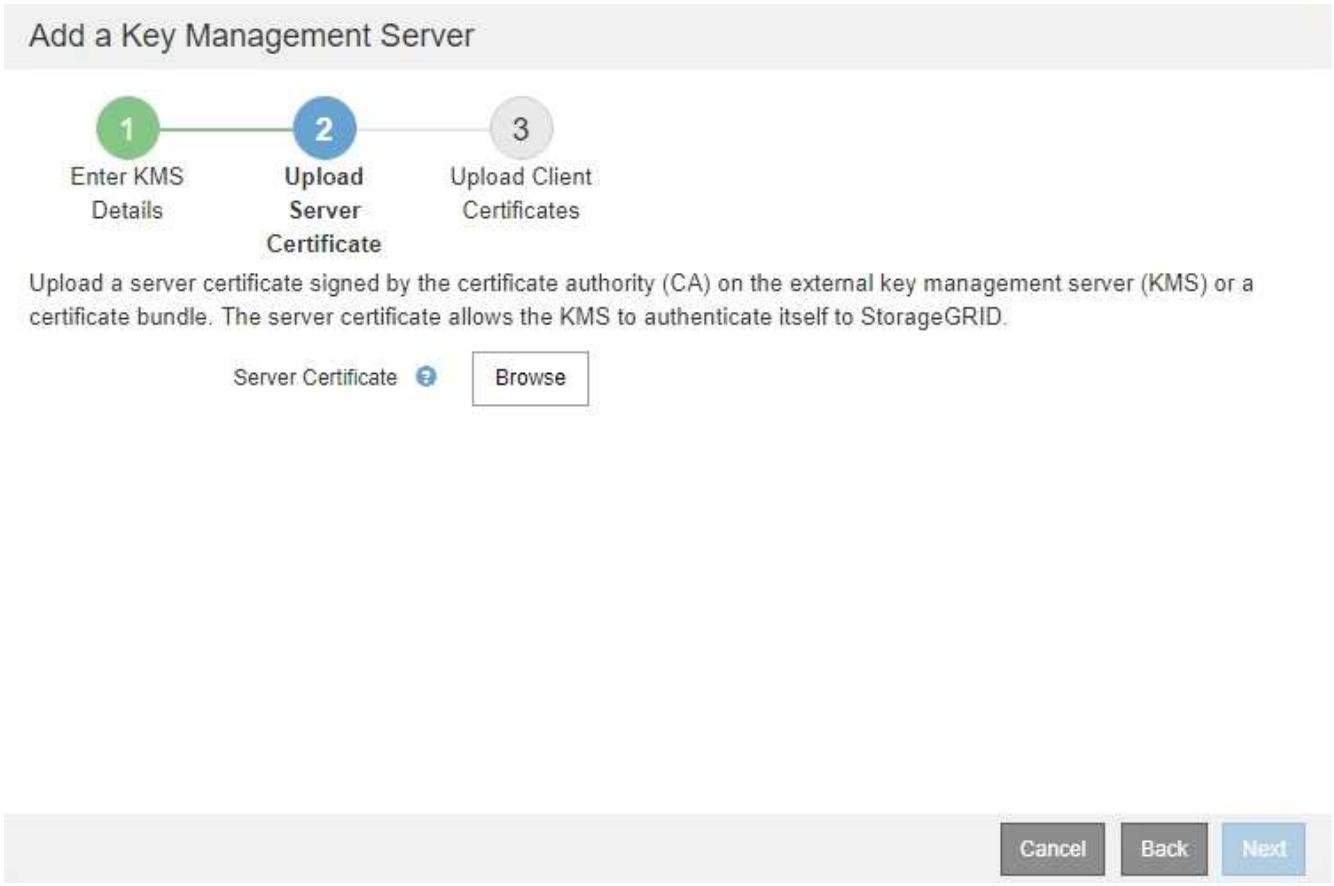
4. KMS クラスタを使用している場合は、プラス記号を選択します ➕ クラスタ内の各サーバのホスト名を追加します。
5. 「 * 次へ * 」を選択します。

   キー管理サーバの追加ウィザードの手順2（サーバ証明書をアップロード）が表示されます。

キー管理サーバの追加ウィザードの手順 2 （サーバ証明書をアップロード）で、 KMS のサーバ証明書（または証明書バンドル）をアップロードします。サーバ証明書を使用すると、外部 KMS は StorageGRID に対して自身を認証できます。

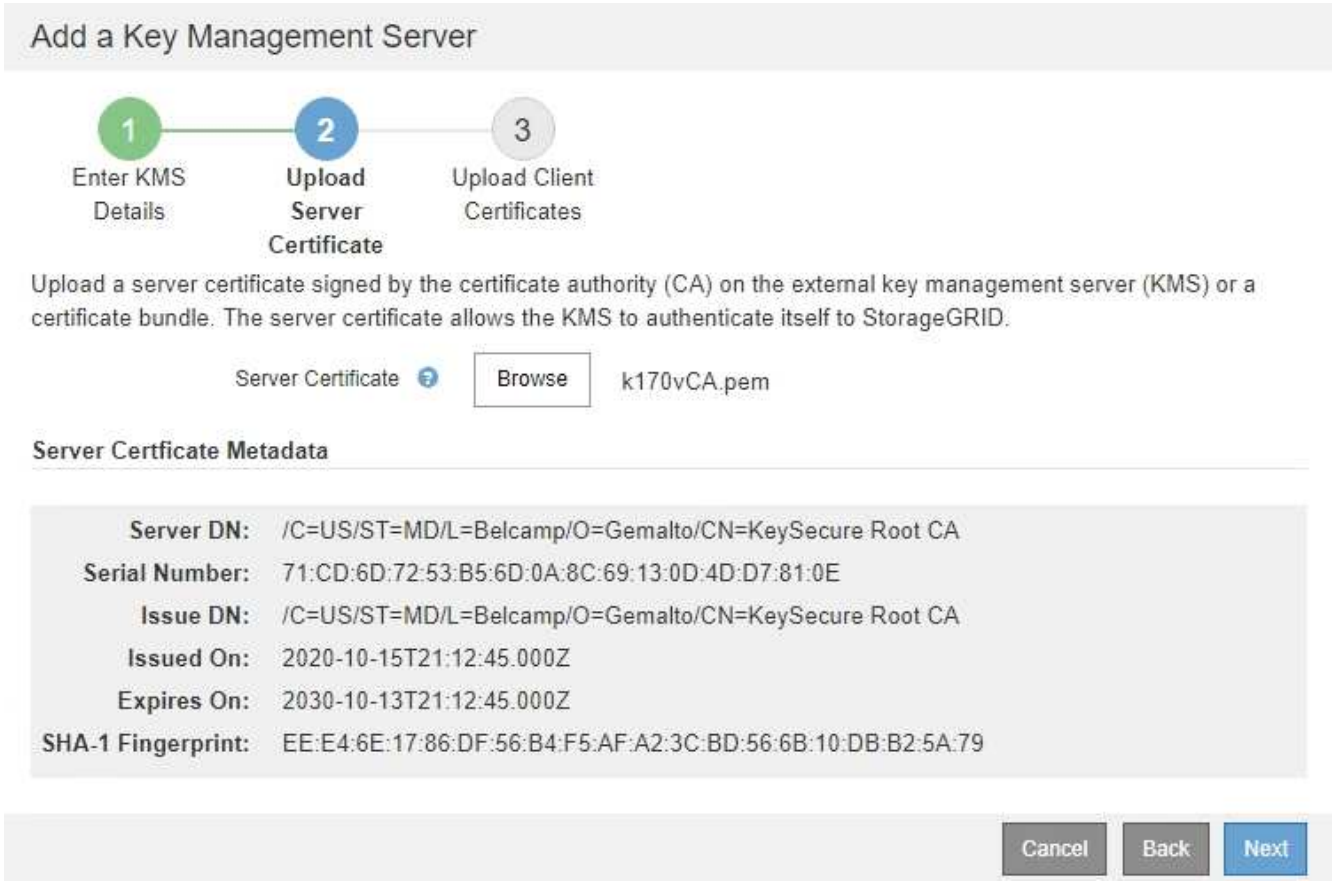
手順

1. 手順 2 （サーバー証明書のアップロード） * から、保存されている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。

   サーバ証明書のメタデータが表示されます。



証明書バンドルをアップロードした場合は、各証明書のメタデータが独自のタブに表示されます。

3. 「 * 次へ * 」を選択します。

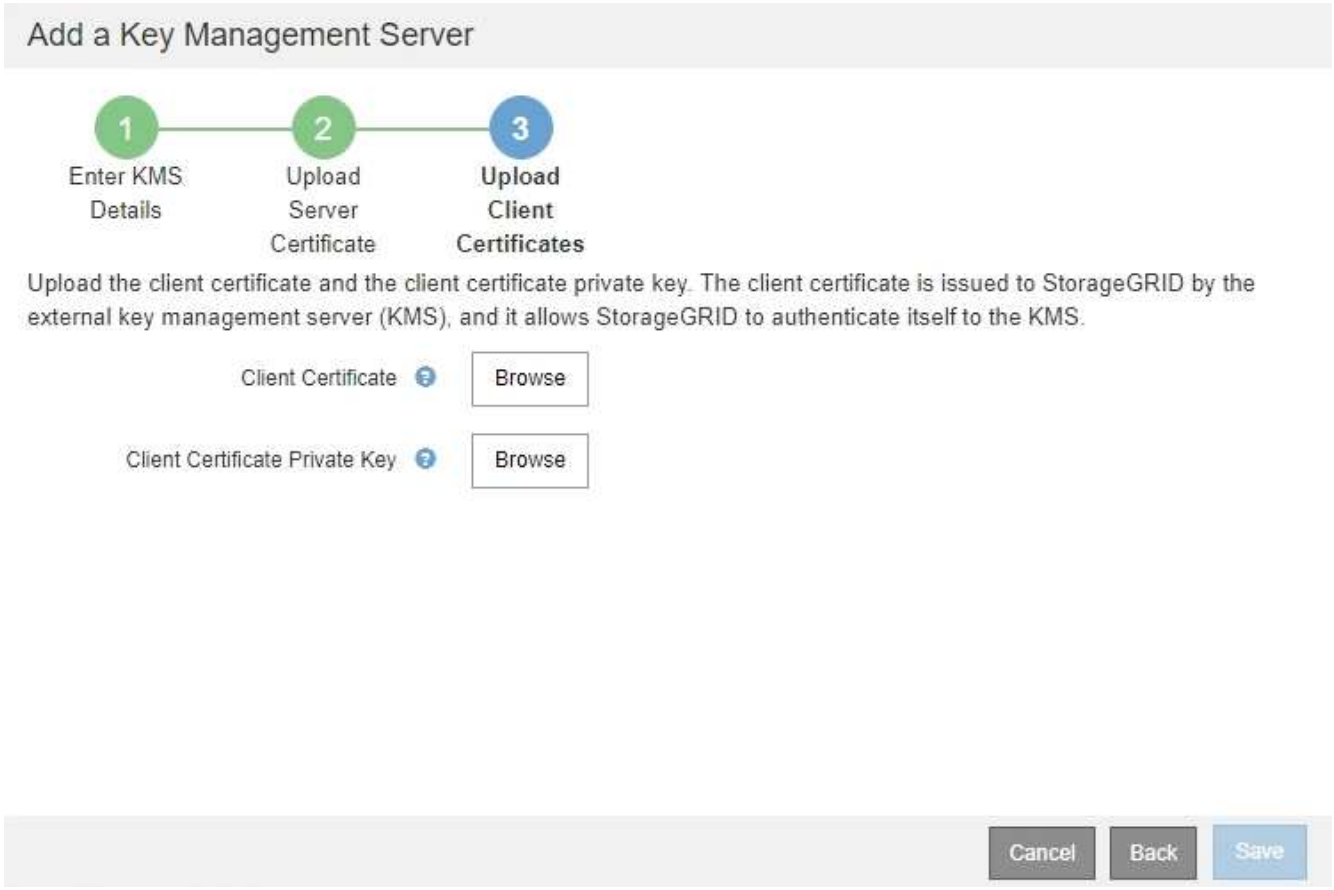
   Add a Key Management Serverウィザードの手順3（クライアント証明書をアップロード）が表示されます。

手順 **3** ：クライアント証明書をアップロードする

キー管理サーバの追加ウィザードの手順 3 （クライアント証明書をアップロード）で、クライアント証明書とクライアント証明書の秘密鍵をアップロードします。クライアント証明書は、 StorageGRID が KMS に対して自身を認証することを許可します。

手順

1. * 手順 3 （クライアント証明書をアップロード） * から、クライアント証明書の場所を参照します。

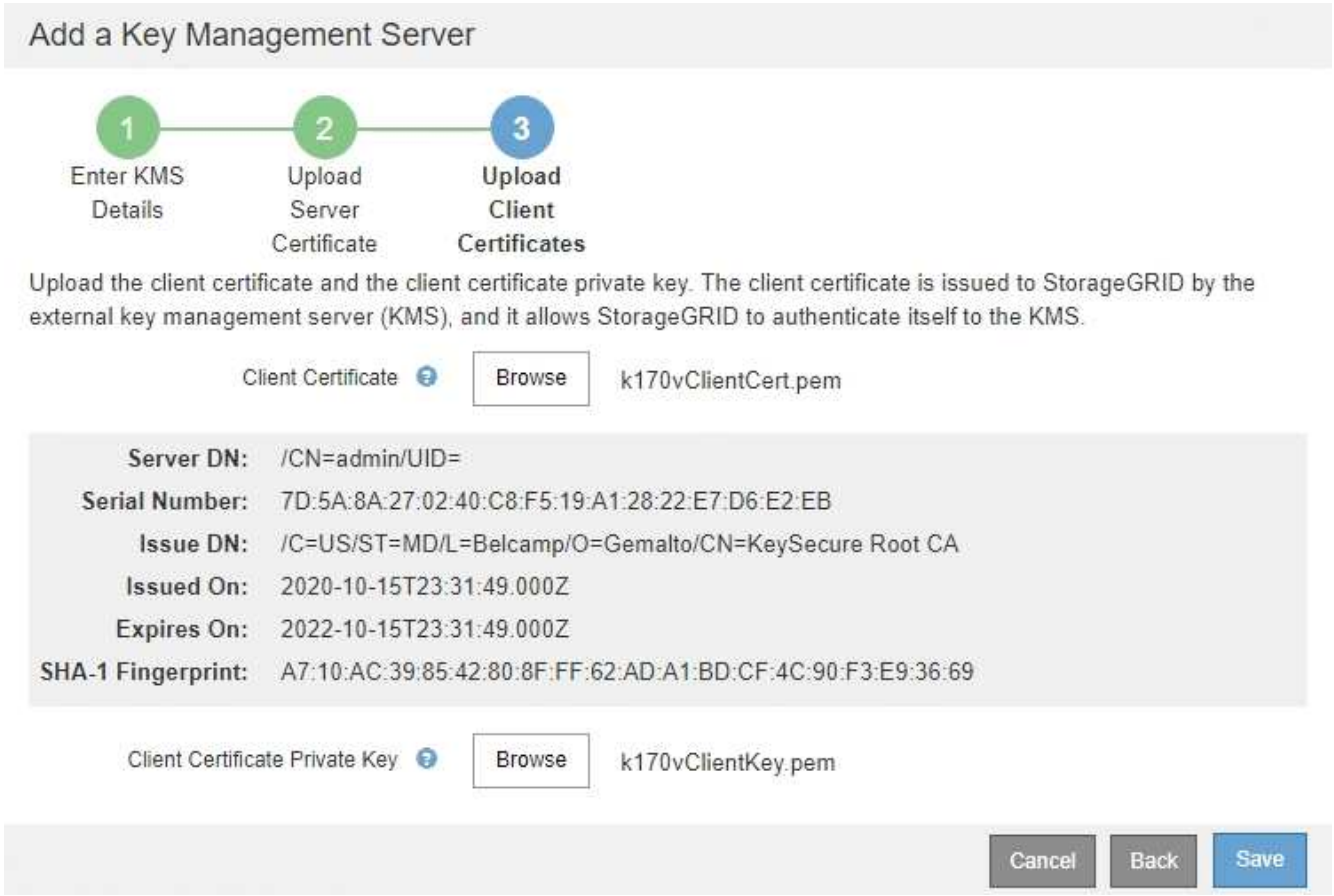


2. クライアント証明書ファイルをアップロードします。

   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鍵の場所を参照します。
4. 秘密鍵ファイルをアップロードします。

   クライアント証明書とクライアント証明書の秘密鍵のメタデータが表示されます。



5. [保存（ Save ）] を選択します。

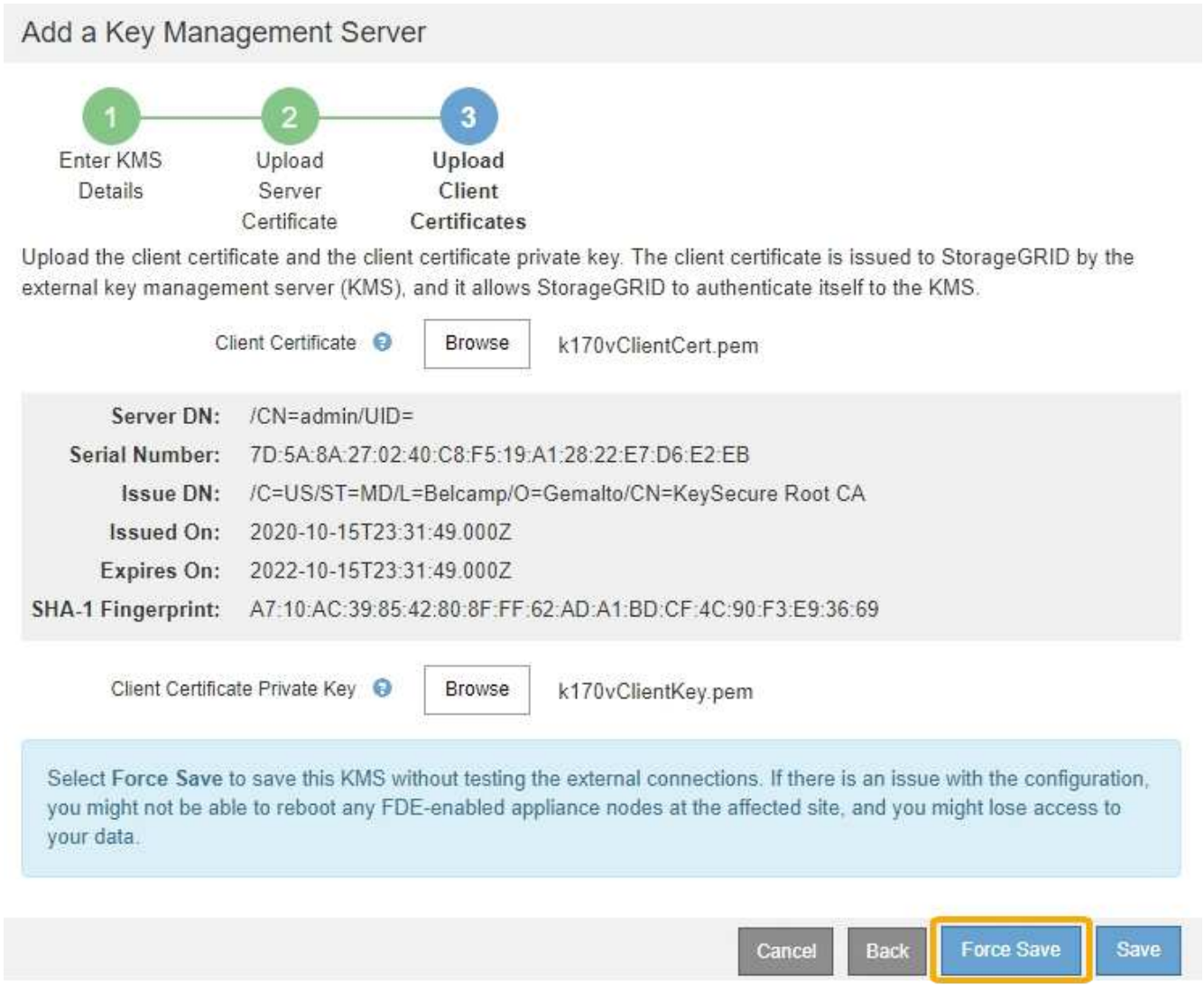
   キー管理サーバとアプライアンスノードの間の接続をテストします。すべての接続が有効で、正しいキーが KMS にある場合は、新しいキー管理サーバが Key Management Server ページの表に追加されます。

   > KMS を追加すると、すぐに [Key Management Server] ページの証明書ステータスが [Unknown （不明）] と表示されます。各証明書の実際のステータスの StorageGRID 取得には 30 分程度かかる場合があります。最新のステータスを表示するには、 Web ブラウザの表示を更新する必要があります。

6. 「 * Save * （保存）」を選択したときにエラーメッセージが表示された場合は、メッセージの詳細を確認し、「 * OK * 」を選択します。

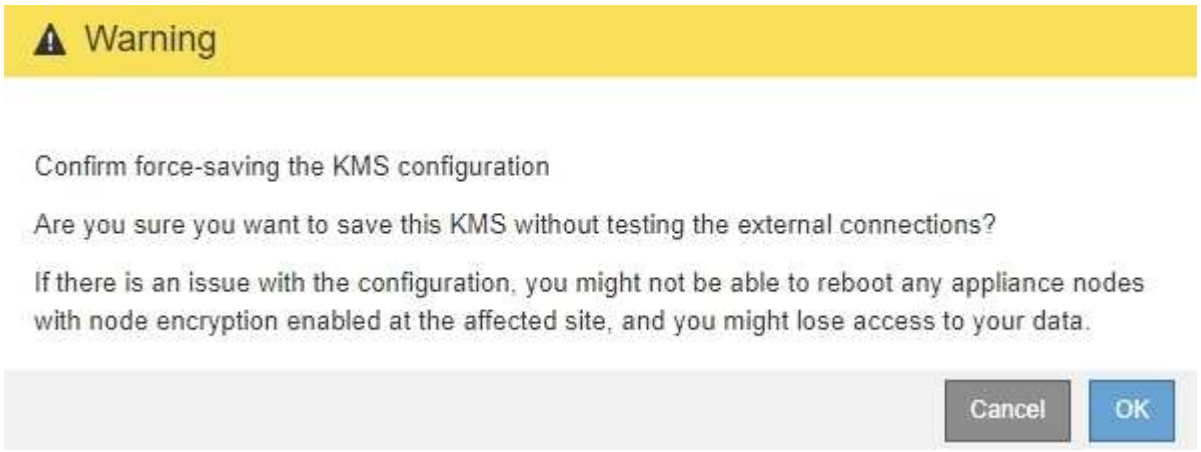
   たとえば、接続テストに失敗した場合は、 422 ： Unprocessable Entity エラーが返されることがあります。

7. 外部接続をテストせずに現在の設定を保存する必要がある場合は、 * 強制保存 * を選択します。



[強制保存] を選択すると KMS の設定が保存されますが、各アプライアンスからその KMS への外部接続はテストされません。構成を含む問題 がある場合、該当するサイトでノード暗号化が有効になっているアプライアンスノードをリブートできない可能性があります。問題が解決するまでデータにアクセスできなくなる可能性があります。

8. 確認の警告を確認し、設定を強制的に保存する場合は、「 * OK 」を選択します。



KMS の設定は保存されますが、 KMS への接続はテストされません。

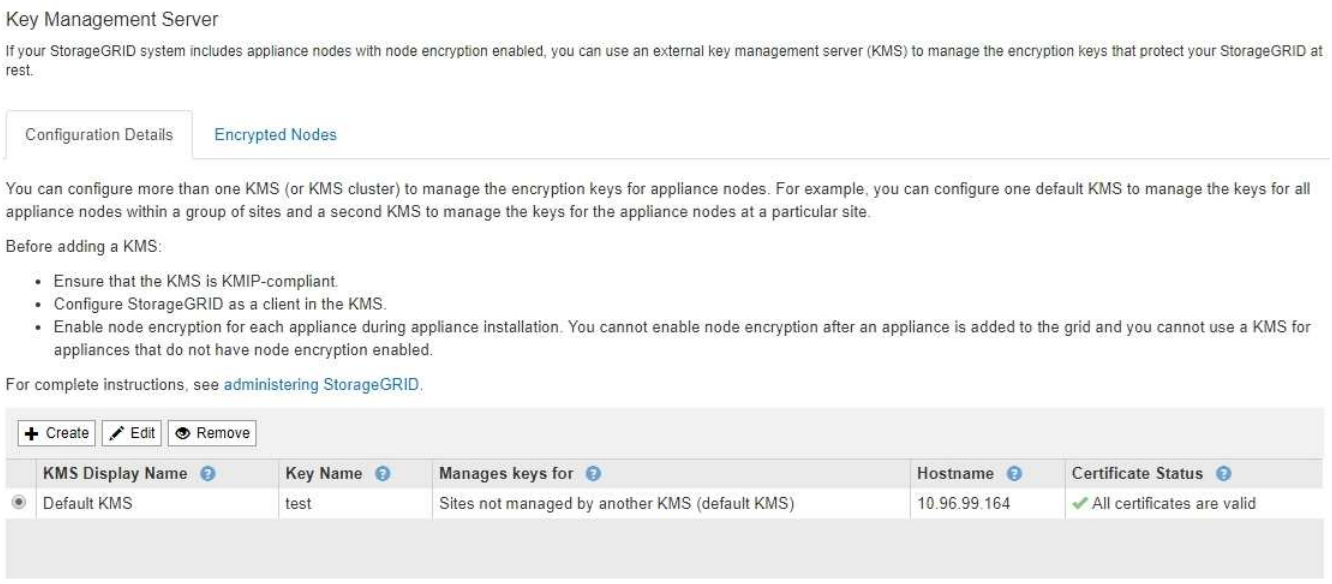
KMSの詳細を確認する

StorageGRID システム内の各キー管理サーバ（ KMS ）に関する情報を確認することができます。これには、サーバ証明書とクライアント証明書の現在のステータスも含まれます。

手順

1. 「* Configuration * System Settings ** Key Management Server *」を選択します。

   [Key Management Server] ページが表示されます。Configuration Details タブには、設定されているすべてのキー管理サーバが表示されます。



2. 各 KMS について、表の情報を確認します。

フィールド	説明
KMS 表示名	KMS の説明的な名前。
キー名	KMS 内の StorageGRID クライアントのキーエイリアス。
のキーを管理します	KMS に関連付けられている StorageGRID サイト。 このフィールドには、特定の StorageGRID サイトの名前、または別の KMS （デフォルト KMS ）で管理されていないサイト * が表示されます

フィールド	説明
ホスト名	KMS の完全修飾ドメイン名または IP アドレス。 2 台のキー管理サーバからなるクラスタがある場合は、両方のサーバの完全修飾ドメイン名または IP アドレスが表示されます。クラスタに複数のキー管理サーバがある場合は、最初の KMS の完全修飾ドメイン名または IP アドレスと、クラスタ内の追加のキー管理サーバの数が表示されます。 例： `10.10.10.10 and 10.10.10.11` または `10.10.10.10 and 2 others`。 クラスタ内のすべてのホスト名を表示するには、KMS を選択して「 * Edit * 」を選択します。
証明書のステータス	サーバ証明書、オプションの CA 証明書、およびクライアント証明書の現在の状態：有効、期限が切れている、期限が近づいている、または不明。 • 注： StorageGRID * 証明書のステータスが更新されるまで 30 分程度かかる場合があります。現在の値を表示するには、 Web ブラウザの表示を更新する必要があります。

3. 証明書のステータスが不明の場合は、 30 分ほど待ってから Web ブラウザを更新してください。

> KMS を追加すると、すぐに [Key Management Server] ページの証明書ステータスが [Unknown （不明）] と表示されます。各証明書の実際のステータスの StorageGRID 取得には 30 分程度かかる場合があります。実際のステータスを確認するには、 Web ブラウザの表示を更新する必要があります。

4. 証明書のステータス列に、証明書の有効期限が切れている、または有効期限が近づいていることが示されている場合は、できるだけ早く問題 に対処してください。

   StorageGRID の監視とトラブルシューティングの手順で、* 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サーバ証明書の有効期限*アラートの推奨される対処方法を参照してください。

> データアクセスを維持するために、証明書の問題はできるだけ早く対処する必要があります。

関連情報

"トラブルシューティングを監視します"

暗号化されたノードの表示

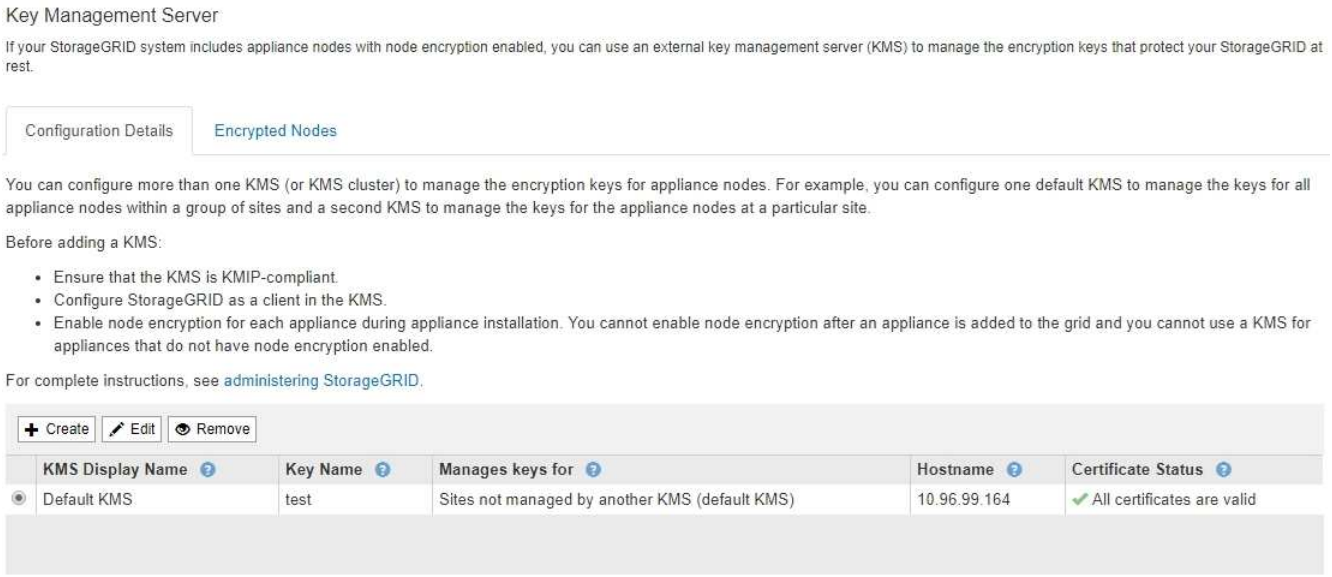
StorageGRID システムでノード暗号化 * 設定が有効になっているアプライアンスノード

に関する情報を表示できます。

手順

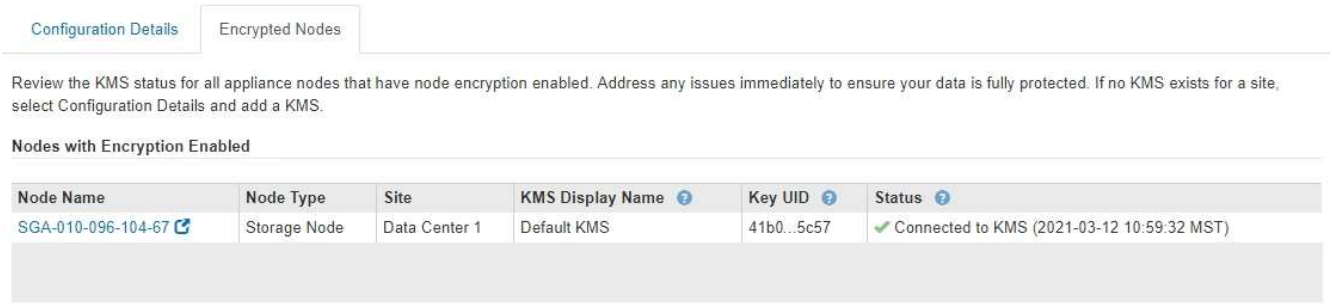
1. 「* Configuration * System Settings ** Key Management Server *」を選択します。

   [Key Management Server] ページが表示されます。Configuration Details タブには、設定済みのすべてのキー管理サーバが表示されます。



2. ページの上部から、 [* 暗号化されたノード *] タブを選択します。

   [Encrypted Nodes] タブには、 StorageGRID システムでノード暗号化 * 設定が有効になっているアプライアンスノードが表示されます。



3. 各アプライアンスノードについて、表の情報を確認します。

列（ **Column** ）	説明
ノード名	アプライアンスノードの名前。
ノードタイプ（ Node Type ）	ノードのタイプ。 Storage 、 Admin 、または Gateway 。
サイト	ノードがインストールされている StorageGRID サイトの名前。
KMS 表示名	ノードに使用される KMS の説明的な名前。 KMS が表示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 "キー管理サーバの追加（KMS）"
キー UID	アプライアンスノードでデータの暗号化と復号化に使用する暗号化キーの一意の ID 。キー UID 全体を表示するには、セルにカーソルを合わせます。 ダッシュ（ - - ）は、キー UID が不明であることを示します。アプライアンスノードと KMS 間の接続問題 が原因である可能性があります。
ステータス	KMS とアプライアンスノード間の接続のステータス。ノードが接続されている場合は、タイムスタンプが 30 分ごとに更新されます。KMS の設定変更後に接続ステータスが更新されるまで数分かかることがあります。 • 注： * 新しい値を表示するには、 Web ブラウザを更新する必要があります。

4. ステータス列に KMS 問題 と表示されている場合は、問題 にすぐに対処してください。

   通常の KMS 操作中、ステータスは * KMS * に接続されます。ノードがグリッドから切断されると、ノードの接続状態が（意図的に停止しているか不明である）と表示されます。

   その他のステータスメッセージは、同じ名前の StorageGRID アラートに対応します。

   ◦ KMS の設定をロードできませんでした
   ◦ KMS 接続エラー
   ◦ KMS 暗号化キー名が見つかりません
   ◦ KMS 暗号化キーのローテーションに失敗しました
   ◦ KMS キーでアプライアンスボリュームを復号化できませんでした
   ◦ KMSが構成されていませんStorageGRID の監視とトラブルシューティングの手順で、これらのアラートに対する推奨される対処方法を確認してください。

問題が発生した場合は、データを完全に保護するために、すぐに対処する必要があります。

関連情報

"トラブルシューティングを監視します"

キー管理サーバの編集（**KMS**）

証明書の有効期限が近づいている場合など、キー管理サーバの設定の編集が必要になることがあります。

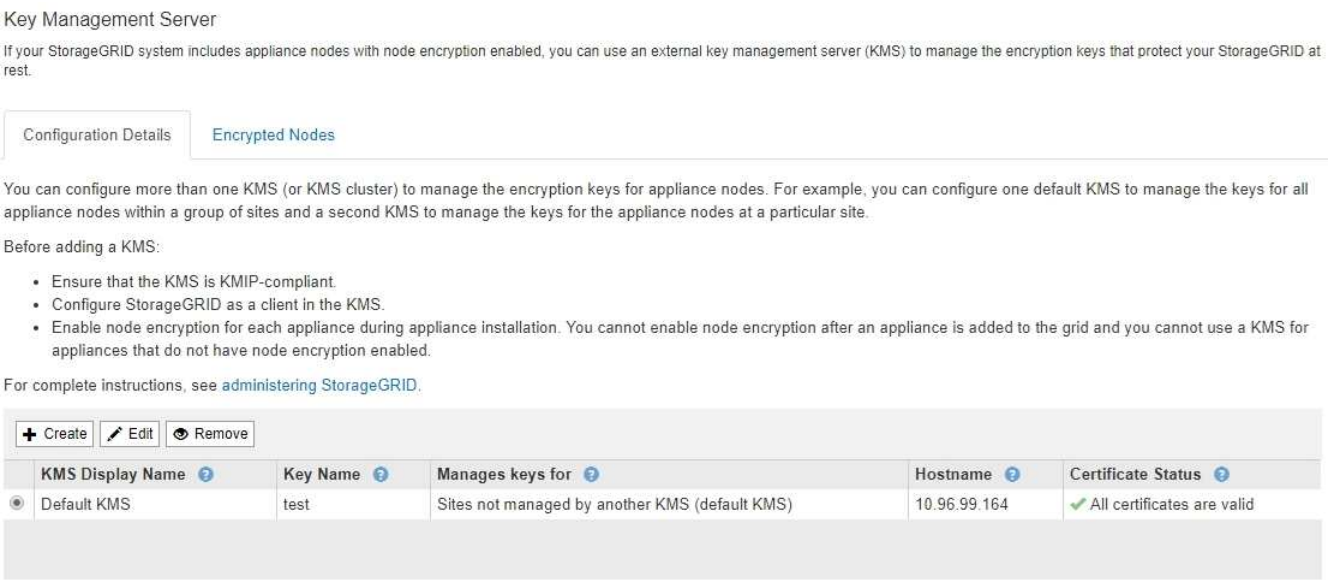
必要なもの

- を確認しておく必要があります "キー管理サーバを使用する際の考慮事項と要件"。
- KMS用に選択したサイトを更新する予定がある場合は、を確認しておく必要があります "サイトの KMS を変更する際の考慮事項"。
- Root Access 権限が必要です。
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

手順

1. 「* Configuration * System Settings ** Key Management Server *」を選択します。

   Key Management Server ページが表示され、設定済みのすべてのキー管理サーバが表示されます。



2. 編集する KMS を選択し、「 * 編集」を選択します。
3. 必要に応じて、キー管理サーバの編集ウィザードの * 手順 1 （ KMS の詳細を入力） * で詳細を更新します。

フィールド	説明
KMS 表示名	この KMS を特定するのに役立つわかりやすい名前。1~64 文字で指定します。
キー名	KMS 内の StorageGRID クライアントの正確なキーエイリアス。1~255 文字で指定する必要があります。 キー名の編集が必要になることはほとんどありません。たとえば、エイリアスの名前が KMS で変更された場合や、以前のキーのすべてのバージョンが新しいエイリアスのバージョン履歴にコピーされている場合は、キー名を編集する必要があります。 KMS のキー名 (エイリアス) を変更して、キーの回転を試みないでください。代わりに、 KMS ソフトウェアのキーバージョンを更新してキーをローテーションしてください。StorageGRID では、以前に使用されていたすべてのキーバージョン（および今後使用するすべてのバージョン）に、同じキーエイリアスを使用して KMS からアクセスできることが必要です。設定されている KMS のキーエイリアスを変更すると、StorageGRID がデータを復号化できなくなる可能性があります。 "キー管理サーバを使用する際の考慮事項と要件"
のキーを管理します	サイト固有の KMS を編集していて ' デフォルトの KMS がまだない場合は ' オプションで ' 別の KMS (デフォルト KMS) で管理されていないサイト * を選択しますこの選択により、サイト固有の KMS がデフォルトの KMS に変換されます。これは、専用の KMS を持たないすべてのサイトと、拡張時に追加されたサイトに適用されます。 • 注： * サイト固有の KMS を編集している場合、別のサイトを選択することはできません。デフォルトの KMS を編集する場合は ' 特定のサイトを選択することはできません
ポート	KMS サーバが Key Management Interoperability Protocol （ KMIP ）の通信に使用するポート。デフォルトでは、 KMIP 標準ポートである 5696 が使用されます。
ホスト名	KMS の完全修飾ドメイン名または IP アドレス。 • 注： * サーバ証明書の SAN フィールドには、ここに入力する FQDN または IP アドレスを含める必要があります。そうしないと、 StorageGRID は KMS クラスタ内のすべてのサーバに接続できなくなります。

4. KMS クラスタを構成する場合は、プラス記号を選択します ➕ クラスタ内の各サーバのホスト名を追加します。
5. 「 * 次へ * 」を選択します。

キー管理サーバの編集ウィザードの手順 2 （サーバ証明書をアップロード）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. 「 * 次へ * 」を選択します。

   キー管理サーバの編集ウィザードの手順 3 （クライアント証明書をアップロード）が表示されます。

8. クライアント証明書とクライアント証明書の秘密鍵を置き換える必要がある場合は、 * 参照 * を選択して新しいファイルをアップロードします。
9. [保存（ Save ）] を選択します。

   キー管理サーバと影響を受けるサイトのすべてのノード暗号化アプライアンスノードの間の接続をテストします。すべてのノード接続が有効で、 KMS に正しいキーがある場合は、キー管理サーバが Key Management Server ページの表に追加されます。

10. エラーメッセージが表示された場合は、メッセージの詳細を確認し、「 * OK * 」を選択します。

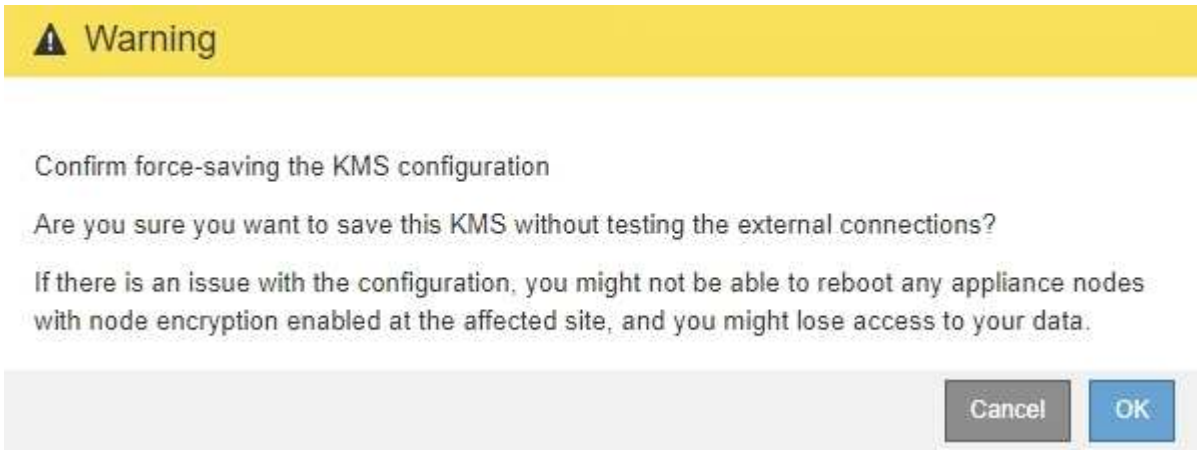
    たとえば、この KMS 用に選択したサイトが別の KMS によってすでに管理されている場合や、接続テストに失敗した場合は、「 422 ： Unprocessable Entity 」というエラーが表示されます。

11. 接続エラーを解決する前に現在の設定を保存する必要がある場合は、 * 強制保存 * を選択します。

    [強制保存] を選択すると KMS の設定が保存されますが、各アプライアンスからその KMS への外部接続はテストされません。構成を含む問題 がある場合、該当するサイトでノード暗号化が有効になっているアプライアンスノードをリブートできない可能性があります。問題が解決するまでデータにアクセスできなくなる可能性があります。

    KMS の設定が保存されます。

12. 確認の警告を確認し、設定を強制的に保存する場合は、「 * OK 」を選択します。



KMS の設定は保存されますが、 KMS への接続はテストされません。

キー管理サーバの削除（**KMS**）

場合によっては、キー管理サーバの削除が必要になることがあります。たとえば、サイ

トの運用を停止した場合は、サイト固有の KMS を削除できます。

必要なもの

- を確認しておく必要があります "キー管理サーバを使用する際の考慮事項と要件"。
- Root Access 権限が必要です。
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

このタスクについて

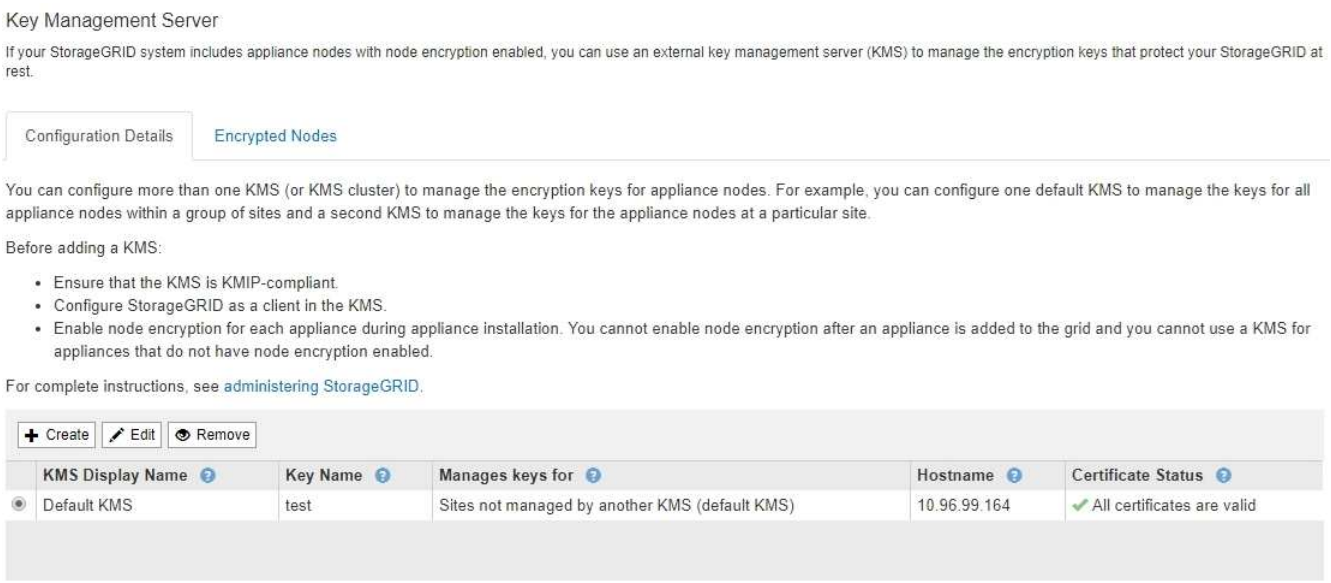
KMS は以下の場合に削除できます。

- サイトの運用が停止された場合や、ノードの暗号化が有効なアプライアンスノードがサイトに含まれていない場合は、サイト固有の KMS を削除できます。
- ノード暗号化が有効なアプライアンスノードがあるサイトごとにサイト固有の KMS がすでに存在する場合は、デフォルトの KMS を削除できます。

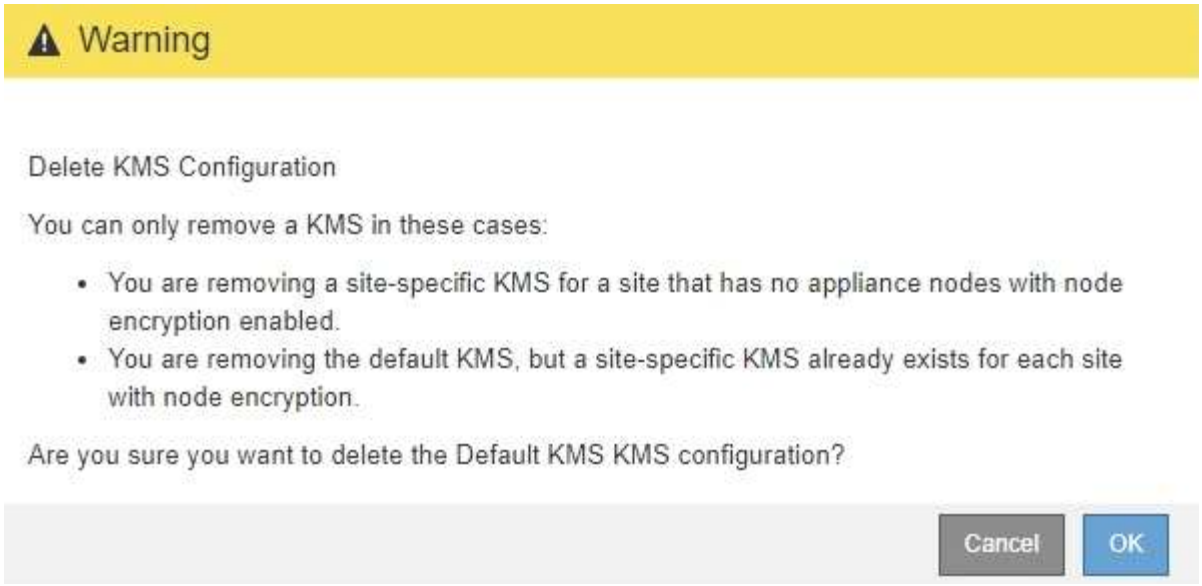
手順

1. 「* Configuration * System Settings ** Key Management Server *」を選択します。

   Key Management Server ページが表示され、設定済みのすべてのキー管理サーバが表示されます。



2. 削除する KMS のラジオボタンを選択し、「 * Remove * 」を選択します。
3. 警告ダイアログで考慮事項を確認します。



4. 「 * OK 」を選択します。

KMS の設定は削除されます。

テナントの管理

グリッド管理者は、 S3 および Swift クライアントがオブジェクトの格納と読み出し、ストレージ使用状況の監視、および StorageGRID システムを使用してクライアントが実行できる操作の管理に使用するテナントアカウントを作成して管理します。

テナントアカウントとは

テナントアカウントは、 Simple Storage Service （ S3 ） REST API または Swift REST API を使用するクライアントアプリケーションが、 StorageGRID でオブジェクトの格納や読み出しを行うことを可能にします。

各テナントアカウントで使用できるプロトコルは 1 つで、アカウントの作成時に指定します。両方のプロトコルを使用して StorageGRID システムにオブジェクトの格納や読み出しを行うには、テナントアカウントを 2 つ作成する必要があります。 1 つは S3 バケットとオブジェクト用、もう 1 つは Swift コンテナとオブジェクト用です。各テナントアカウントには、専用のアカウント ID 、許可されたグループとユーザ、バケットまたはコンテナ、およびオブジェクトがあります。

必要に応じて、システムに格納されているオブジェクトをエンティティごとに分ける場合は、追加のテナントアカウントを作成します。たとえば、次のようなユースケースでは複数のテナントアカウントをセットアップできます。

- * エンタープライズのユースケース：エンタープライズアプリケーションで StorageGRID システムを管理する場合は、組織内の部門ごとにグリッドのオブジェクトストレージを分離する必要があります。この場合は、マーケティング部門、カスタマーサポート部門、人事部門などのテナントアカウントを作成できます。

> S3 クライアントプロトコルを使用する場合は、 S3 バケットとバケットポリシーを使用してエンタープライズ内の部門間でオブジェクトを分離できます。テナントアカウントを使用する必要はありません。詳細については、 S3 クライアントアプリケーションを実装する手順を参照してください。

- * サービスプロバイダのユースケース：サービスプロバイダとして StorageGRID システムを管理する場合は、グリッド上のストレージをリースするエンティティごとにグリッドのオブジェクトストレージを分離できます。この場合は、 A 社、 B 社、 C 社などのテナントアカウントを作成します。

テナントアカウントを作成および設定する

テナントアカウントを作成する際には次の情報を指定します。

- テナントアカウントの表示名。
- テナントアカウントで使用されるクライアントプロトコル（ S3 または Swift ）。
- S3 テナントアカウントの場合：テナントアカウントに S3 バケットで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。テナントアカウ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を使用できるようグリッドを設定する必要があります。「プラットフォームサービスの管理」を参照してください。
- 必要に応じて、テナントアカウントのストレージクォータ — テナントのオブジェクトで使用可能な最大ギガバイト数、テラバイト数、ペタバイト数。クォータを超過すると、テナントは新しいオブジェクトを作成できなくなります。

> テナントのストレージクォータは、物理容量（ディスクのサイズ）ではなく、論理容量（オブジェクトのサイズ）を表します。

- StorageGRID システムでアイデンティティフェデレーションが有効になっている場合は、テナントアカウントを設定するための Root Access 権限が割り当てられているフェデレーテッドグループ。
- StorageGRID システムでシングルサインオン（ SSO ）が使用されていない場合は、テナントアカウントが独自のアイデンティティソースを使用するか、グリッドのアイデンティティソースを共有するか、およびテナントのローカル root ユーザの初期パスワード。

テナントアカウントが作成されたら、次のタスクを実行できます。

- * グリッドのプラットフォームサービスの管理 * ：テナントアカウントでプラットフォームサービスを有効にする場合は、プラットフォームサービスメッセージの配信方法と、 StorageGRID 環境でプラットフォームサービスを使用する際のネットワーク要件を理解しておく必要があります。
- * テナントアカウントのストレージ使用状況を監視 * ：テナントがアカウントの使用を開始したら、 Grid Manager を使用して各テナントが消費するストレージ容量を監視できます。

  テナントにクォータを設定している場合は、「テナントクォータ使用率が高い * 」アラートを有効にして、テナントがクォータを消費しているかどうかを確認できます。有効にすると、テナントのクォータの 90% が使用されたときにこのアラートがトリガーされます。詳細については、 StorageGRID の監視とトラブルシューティングの手順にあるアラートリファレンスを参照してください。

- * クライアント処理の設定 * ：一部のタイプのクライアント処理が禁止されているかどうかを設定できます。

S3テナントを設定する

S3 テナントアカウントが作成されたら、テナントユーザは Tenant Manager にアクセス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の設定（グリッドとアイデンティティソースを共有する場合を除く）、およびローカルグループとユーザの作成

- S3 アクセスキーの管理
- S3 バケットの作成と管理を行う
- ストレージ使用状況を監視しています
- プラットフォームサービスの使用（有効な場合）

> S3 テナントユーザは、 Tenant Manager を使用して S3 アクセスキーとバケットを作成および管理できますが、オブジェクトを取り込みおよび管理するには S3 クライアントアプリケーションを使用する必要があります。

Swiftテナントを設定します

Swift テナントアカウントが作成されたら、テナントの root ユーザは Tenant Manager にアクセス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の設定（グリッドとアイデンティティソースを共有する場合を除く）、およびローカルグループとユーザの作成
- ストレージ使用状況を監視しています

> Swift ユーザが Tenant Manager にアクセスするには、 Root Access 権限が必要です。ただし Root Access 権限では、 Swift REST API に認証してコンテナを作成したりオブジェクトを取り込んだりすることはできません。Swift REST API に認証するには、 Swift 管理者の権限が必要です。

関連情報

"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します

StorageGRID システム内のストレージへのアクセスを制御するために、少なくとも 1 つのテナントアカウントを作成する必要があります。

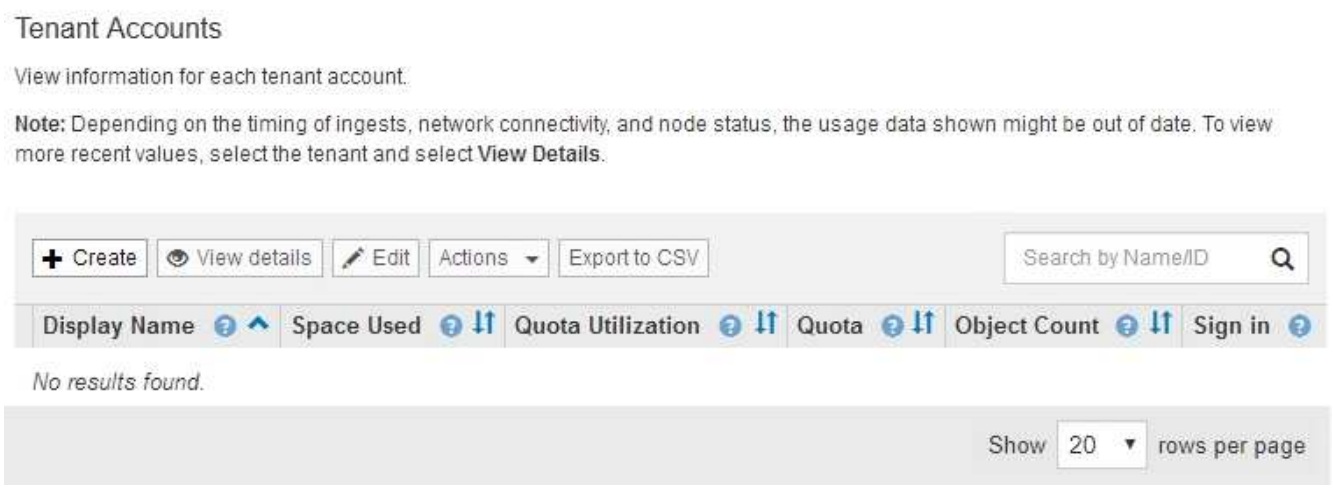
必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

手順

1. 「* tenants *」を選択します

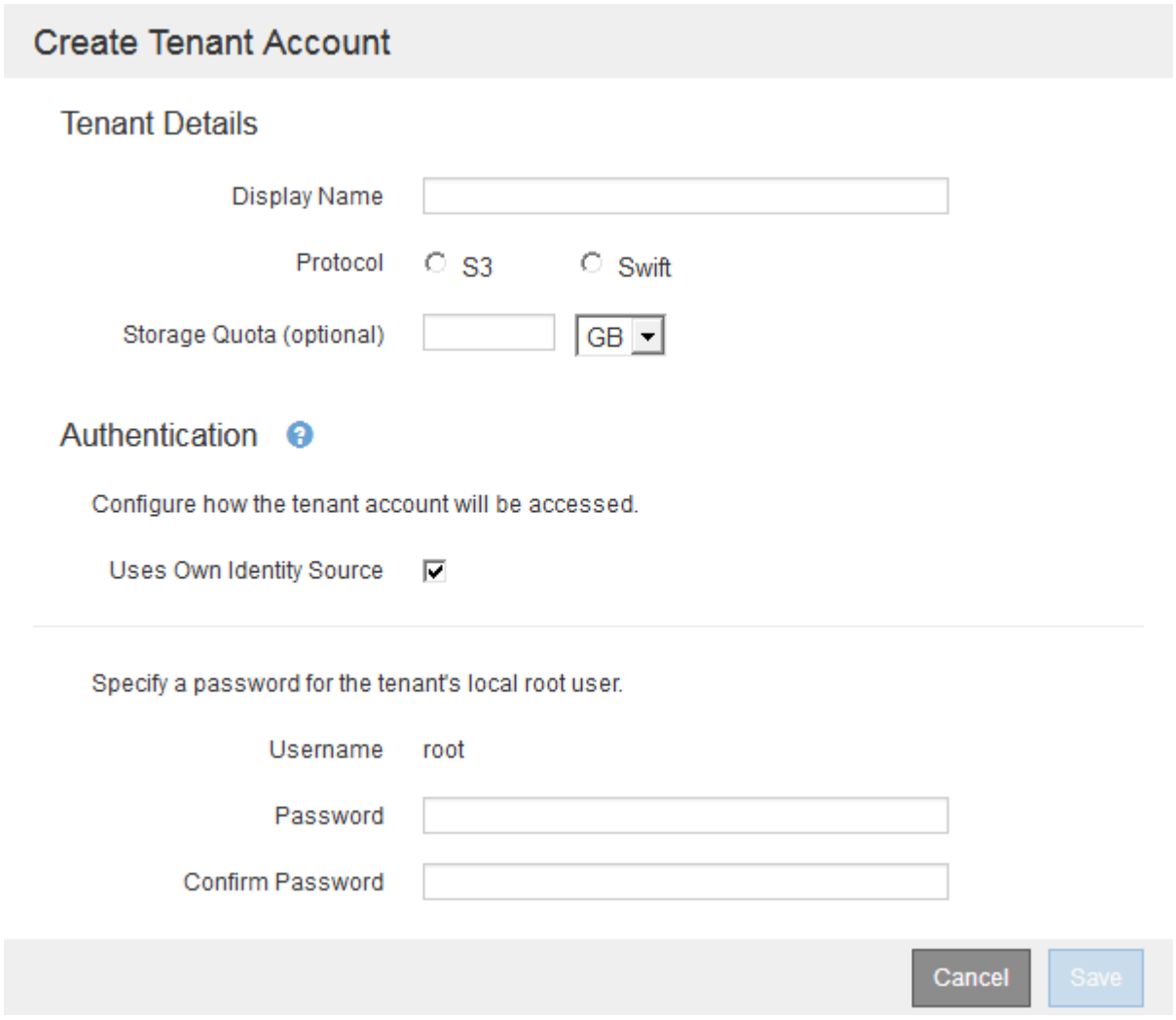
   Tenant Accountsページが表示され、既存のテナントアカウントの一覧が表示されます。



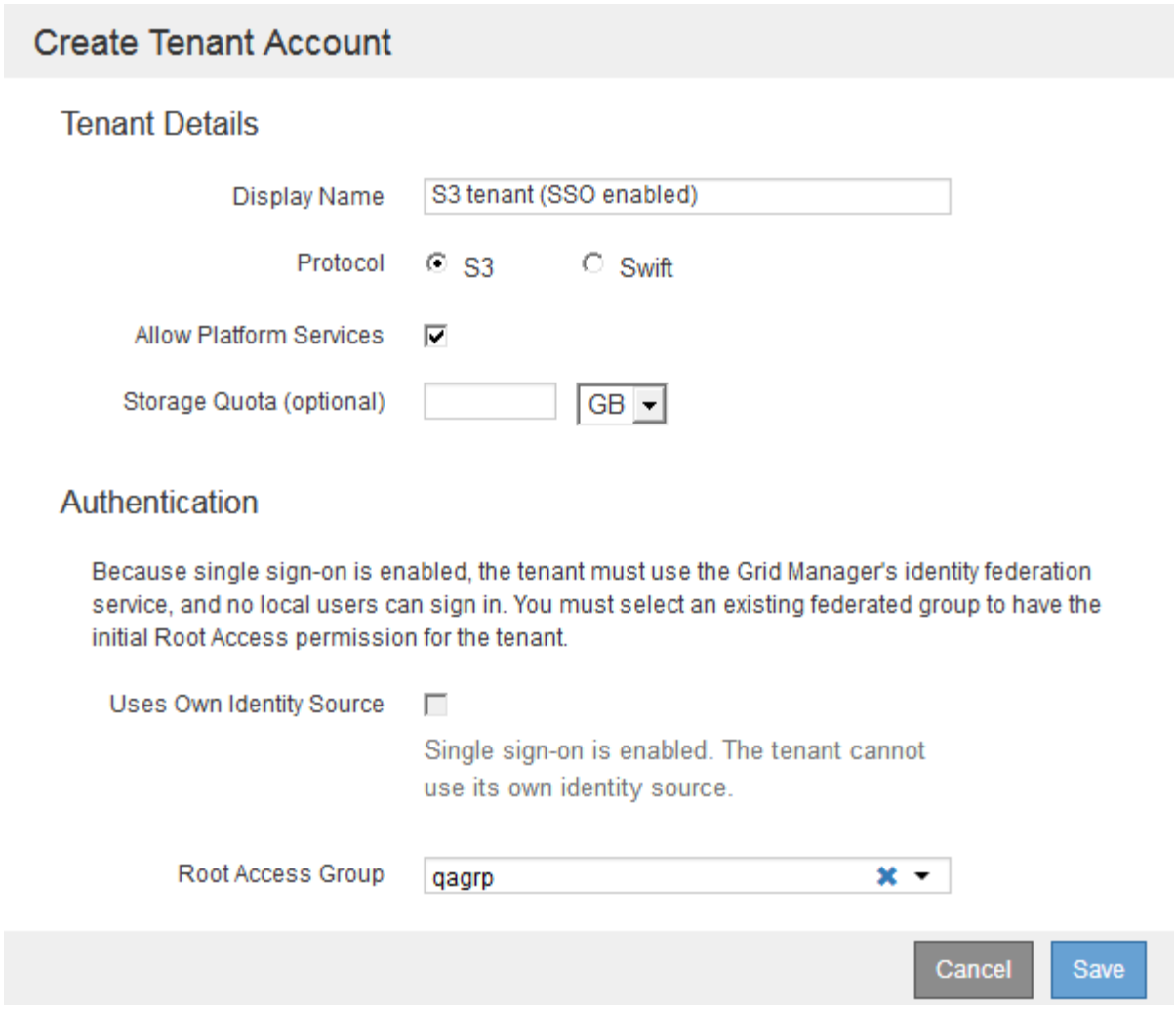
2. 「 * Create * 」を選択します。

Create Tenant Accountページが表示されます。このページに表示されるフィールドは、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かどうかによって異なります。

- SSOを使用していない場合、Create Tenant Accountページは次のようになります。



- SSOが有効な場合、Create Tenant Accountページは次のようになります。



関連情報

"アイデンティティフェデレーションを使用する"

"シングルサインオンを設定しています"

StorageGRID が**SSO**を使用していない場合のテナントアカウントの作成

テナントアカウントを作成する際は、名前、クライアントプロトコル、およびオプションでストレージクォータを指定します。StorageGRID がシングルサインオン（SSO）を使用していない場合は、テナントアカウントが独自のアイデンティティソースを使用するかどうかを指定し、テナントのローカルrootユーザの初期パスワードを設定する必要があります。

このタスクについて

Grid Manager用に設定されているアイデンティティソースをテナントアカウントで使用し、テナントアカウントにフェデレーテッドグループへのRoot Access権限を付与する場合は、そのフェデレーテッドグループをGrid Managerにインポートしておく必要があります。この管理グループに Grid Manager の権限を割り当てる必要はありません。の手順を参照してください "管理者グループの管理"。

手順

1. [表示名]テキストボックスに、このテナントアカウントの表示名を入力します。

   表示名は一意である必要はありません。作成したテナントアカウントには、一意の数値アカウントIDが割り当てられます。

2. このテナントアカウントで使用するクライアントプロトコルとして、* S3 または Swift *を選択します。
3. S3テナントアカウントの場合は、このテナントでS3バケットにプラットフォームサービスを使用しないようにする場合を除き、プラットフォームサービスの許可*チェックボックスをオンのままにしておきます。

   プラットフォームサービスが有効になっている場合、テナントは外部サービスにアクセスするCloudMirror レプリケーションなどの機能を使用できます。これらの機能の使用を無効にすることで、テナントが消費するネットワーク帯域幅またはその他のリソースの量を制限できます。「プラットフォームサービスの管理」を参照してください。

4. [ストレージクォータ]テキストボックスに、このテナントのオブジェクトで使用可能にする最大ギガバイト数、テラバイト数、またはペタバイト数をオプションで入力します。次に、ドロップダウンリストから単位を選択します。

   このテナントのクォータを無制限にする場合は、このフィールドを空白のままにします。

   テナントのストレージクォータは、物理容量（ディスクのサイズ）ではなく、論理容量（オブジェクトのサイズ）を表します。ILMのコピーおよびイレイジャーコーディングは、クォータの使用量にはカウントされません。クォータを超過すると、テナントアカウントは新しいオブジェクトを作成できなくなります。

   各テナントアカウントのストレージ使用状況を監視するには、「使用状況」を選択します。テナントアカウントは、Tenant Managerのダッシュボードまたはテナント管理APIを使用してストレージ使用状況を監視することもできます。ノードがグリッド内の他のノードから切断されていると、テナントのストレージ使用状況の値が最新ではなくなる場合があります。合計はネットワーク接続が回復すると更新されます。

5. テナントで独自のグループとユーザを管理する場合は、次の手順を実行します。
   a. [独自のアイデンティティソースを使用する*]チェックボックスをオンにします(デフォルト)。

      このチェックボックスをオンにしてテナントグループとユーザにアイデンティティフェデレーションを使用する場合、テナントが独自のアイデンティティソースを設定する必要があります。テナントアカウントを使用する手順を参照してください。

   b. テナントのローカルrootユーザのパスワードを指定します。
6. テナントがGrid Manager用に設定されたグループとユーザを使用する場合は、次の手順を実行します。
   a. [独自のアイデンティティソースを使用する*]チェックボックスをオフにします。
   b. 次のいずれか、または両方を実行します。
      - Root Access Groupフィールドで、テナントに対する最初のRoot Access権限を持つ既存のフェデレーテッドグループをGrid Managerから選択します。

適切な権限がある場合は、フィールドをクリックすると、Grid Managerから既存のフェデレーテッドグループが表示されます。それ以外の場合は、グループの一意の名前を入力します。

- テナントのローカルrootユーザのパスワードを指定します。

7. [保存（ Save ）] をクリックします。

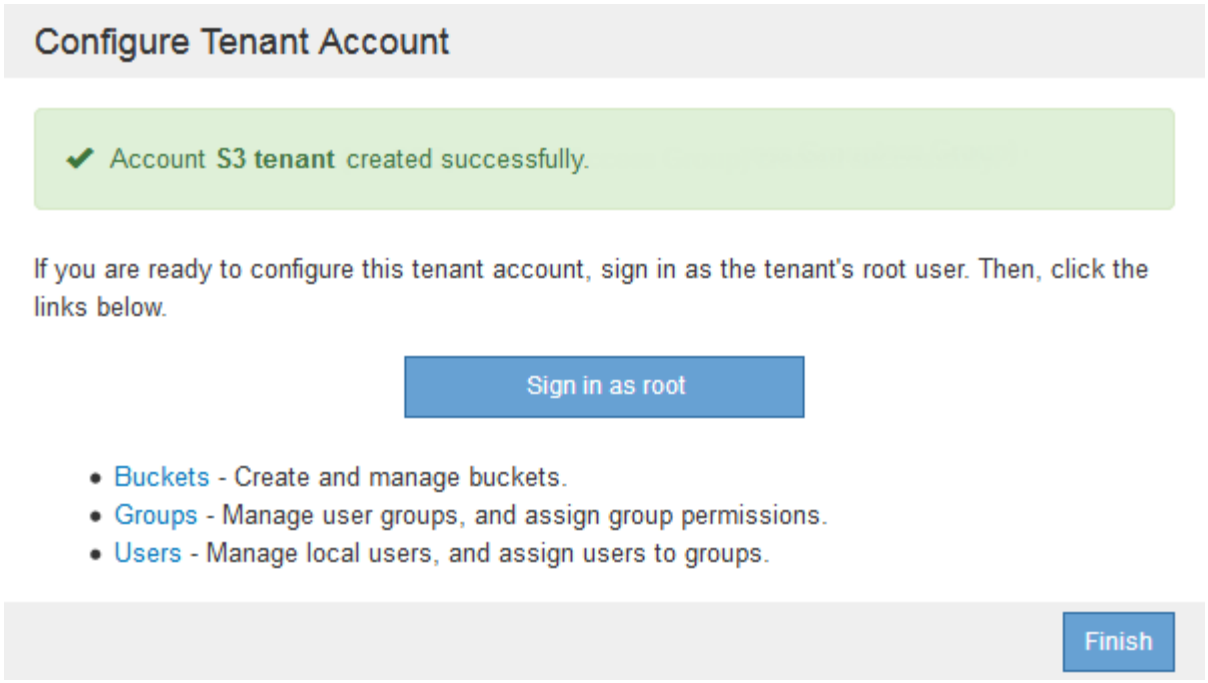
   テナントアカウントが作成されます。

8. 必要に応じて、新しいテナントにアクセスします。それ以外の場合は、の手順に進みます テナントへのアクセスはあとで行います。

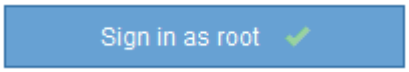
実行する作業	手順
制限されたポートでGrid Managerにアクセスします	このテナントアカウントへのアクセス方法の詳細については、「* Restricted *」をクリックしてください。 Tenant Manager の URL の形式は次のとおりです。 `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/` • *FQDN_or_Admin_Node_IP* は、管理ノードの完全修飾ドメイン名またはIPアドレスです • *port* は、テナント専用ポートです • *20-digit-account-id* は、テナントの一意のアカウントIDです
ポート443でGrid Managerにアクセスしているが、ローカルrootユーザのパスワードを設定していない	[サインイン]をクリックし、ルートアクセスフェデレーテッドグループにユーザのクレデンシャルを入力します。
ポート443でGrid Managerにアクセスし、ローカルrootユーザのパスワードを設定した	次の手順に進みます rootとしてサインインします。

9. rootとしてテナントにサインインします。

   a. Configure Tenant Account（テナントアカウントの設定）ダイアログボックスで、* Sign in as root（**root**としてサインイン）ボタンをクリックします。



緑のチェックマークがボタン上に表示されます。これは、rootユーザとしてテナントアカウントにサインインしていることを示しています。



a. リンクをクリックしてテナントアカウントを設定します。

   各リンクをクリックすると、 Tenant Manager の対応するページが開きます。このページの手順については、テナントアカウントの使用手順を参照してください。

b. [完了] をクリックします。

10. あとでテナントにアクセスするには、次の手順を実行します。

使用するポート	次のいずれかを実行 ...
ポート 443	• Grid Managerで* tenants を選択し、テナント名の右側にある Sign In *をクリックします。 • Web ブラウザにテナントの URL を入力します。 `https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/` ◦ *FQDN_or_Admin_Node_IP* は、管理ノードの完全修飾ドメイン名またはIPアドレスです ◦ *20-digit-account-id* は、テナントの一意のアカウントIDです

使用するポート	次のいずれかを実行 ...
制限されたポート	• Grid Managerから* tenants を選択し、 Restricted *をクリックします。 • Web ブラウザにテナントの URL を入力します。 `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id` ◦ *FQDN_or_Admin_Node_IP* は、管理ノードの完全修飾ドメイン名またはIPアドレスです ◦ *port* は、テナント専用の制限付きポートです ◦ *20-digit-account-id* は、テナントの一意のアカウントIDです

関連情報

"ファイアウォールによるアクセス制御"

"S3テナントアカウント用のプラットフォームサービスの管理"

"テナントアカウントを使用する"

SSOが有効な場合のテナントアカウントの作成

テナントアカウントを作成する際は、名前、クライアントプロトコル、およびオプションでストレージクォータを指定します。StorageGRID でシングルサインオン（SSO）が有効になっている場合は、テナントアカウントを設定するためのRoot Access権限が割り当てられているフェデレーテッドグループも指定します。

手順

1. [表示名]テキストボックスに、このテナントアカウントの表示名を入力します。

   表示名は一意である必要はありません。作成したテナントアカウントには、一意の数値アカウントIDが割り当てられます。

2. このテナントアカウントで使用するクライアントプロトコルとして、* S3 または Swift *を選択します。
3. S3テナントアカウントの場合は、このテナントでS3バケットにプラットフォームサービスを使用しないようにする場合を除き、プラットフォームサービスの許可*チェックボックスをオンのままにしておきます。

   プラットフォームサービスが有効になっている場合、テナントは外部サービスにアクセスする CloudMirror レプリケーションなどの機能を使用できます。これらの機能の使用を無効にすることで、テナントが消費するネットワーク帯域幅またはその他のリソースの量を制限できます。「プラットフォームサービスの管理」を参照してください。

4. [ストレージクォータ]テキストボックスに、このテナントのオブジェクトで使用可能にする最大ギガバイト数、テラバイト数、またはペタバイト数をオプションで入力します。次に、ドロップダウンリストから単位を選択します。

このテナントのクォータを無制限にする場合は、このフィールドを空白のままにします。

テナントのストレージクォータは、物理容量（ディスクのサイズ）ではなく、論理容量（オブジェクトのサイズ）を表します。ILMのコピーおよびイレイジャーコーディングは、クォータの使用量にはカウントされません。クォータを超過すると、テナントアカウントは新しいオブジェクトを作成できなくなります。

各テナントアカウントのストレージ使用状況を監視するには、「使用状況」を選択します。テナントアカウントは、Tenant Managerのダッシュボードまたはテナント管理APIを使用してストレージ使用状況を監視することもできます。ノードがグリッド内の他のノードから切断されていると、テナントのストレージ使用状況の値が最新ではなくなる場合があります。合計はネットワーク接続が回復すると更新されます。

5. [独自のアイデンティティソースを使用する*]チェックボックスがオフになっており、無効になっていることに注意してください。

   SSOが有効であるため、テナントはGrid Manager用に設定されたアイデンティティソースを使用する必要があります。ローカルユーザはサインインできません。

6. [* Root Access Group]フィールドで、テナントに対する最初のRoot Access権限を持つ既存のフェデレーテッドグループをGrid Managerから選択します。

   適切な権限がある場合は、フィールドをクリックすると、Grid Managerから既存のフェデレーテッドグループが表示されます。それ以外の場合は、グループの一意の名前を入力します。

7. [保存（ Save ）] をクリックします。

   テナントアカウントが作成されます。Tenant Accountsページが表示され、新しいテナントの行が追加されます。

8. Root Accessグループのユーザは、必要に応じて新しいテナントの* Sign In *リンクをクリックしてTenant Managerにすぐにアクセスし、テナントを設定できます。それ以外の場合は、テナントアカウントの管理者に*サインイン*リンクのURLを提供します。（テナントのURLは、いずれかの管理ノードの完全修飾ドメイン名またはIPアドレスのあとにを追加したものです `/?accountId=20-digit-account-id`.）

   テナントアカウントのRoot Accessグループに属していない場合は、* Sign In *をクリックするとアクセス拒否のメッセージが表示されます。

関連情報

"シングルサインオンを設定しています"

"S3テナントアカウント用のプラットフォームサービスの管理"

"テナントアカウントを使用する"

テナントのローカル**root**ユーザのパスワードを変更する

テナントのローカル root ユーザがアカウントからロックアウトされた場合は、 root ユー

ザのパスワード変更が必要になることがあります。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

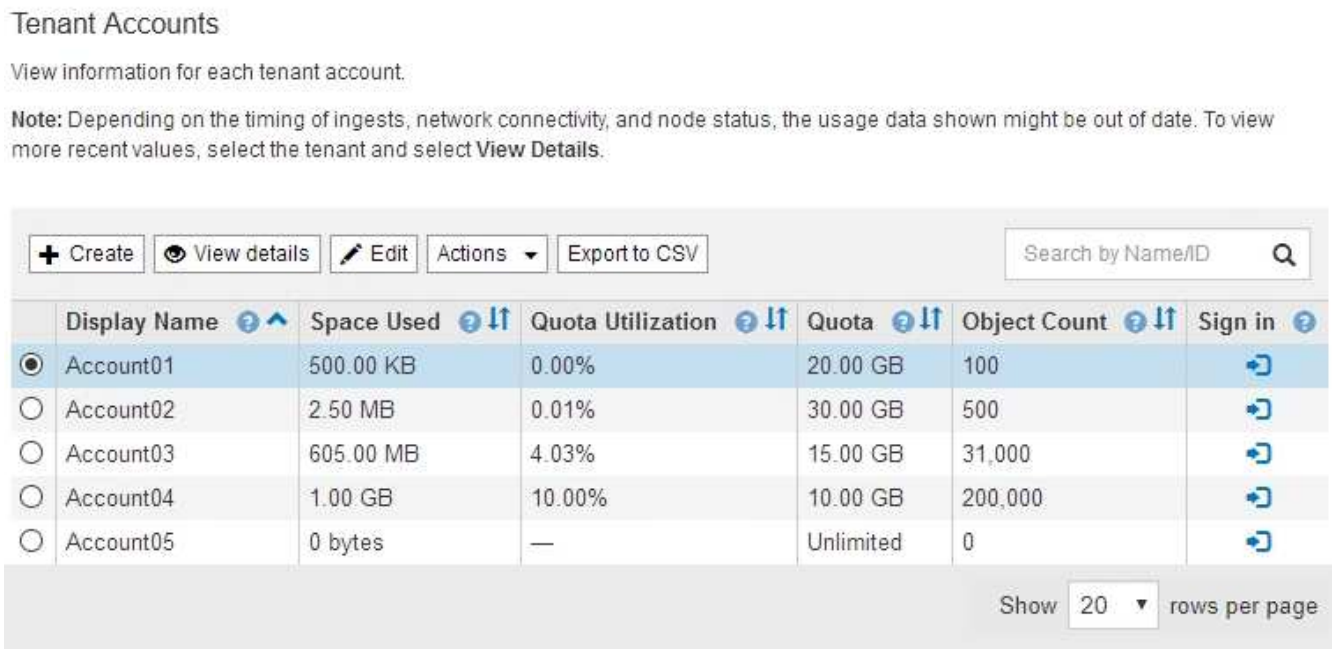
このタスクについて

StorageGRID システムでシングルサインオン（ SSO ）が有効になっている場合、ローカル root ユーザはテナントアカウントにサインインできません。rootユーザのタスクを実行するには、テナントのRoot Access権限を持つフェデレーテッドグループにユーザが属している必要があります。

手順

1. 「* tenants *」を選択します

   Tenant Accountsページが表示され、既存のテナントアカウントがすべてリストされます。

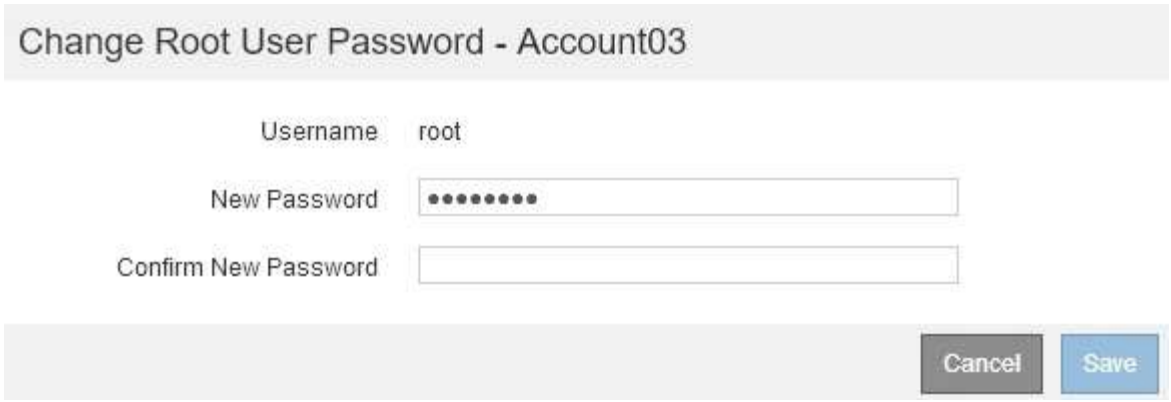


2. 編集するテナントアカウントを選択します。

   システムに20個を超えるアイテムが含まれている場合は、各ページに一度に表示する行数を指定できます。検索ボックスを使用して、表示名またはテナントIDでテナントアカウントを検索します。

   [詳細の表示]、[編集]、[アクション]ボタンが有効になります。

3. [アクション（* Actions ）]ドロップダウンから、[*ルートパスワードの変更（Change Root Password）]を選択します。



4. テナントアカウントの新しいパスワードを入力します。
5. [保存（ Save ）] を選択します。

関連情報

"StorageGRID への管理者アクセスの制御"

テナントアカウントを編集する

テナントアカウントを編集して、表示名の変更、アイデンティティソース設定の変更、プラットフォームサービスの許可または禁止、ストレージクォータの入力を行うことができます。

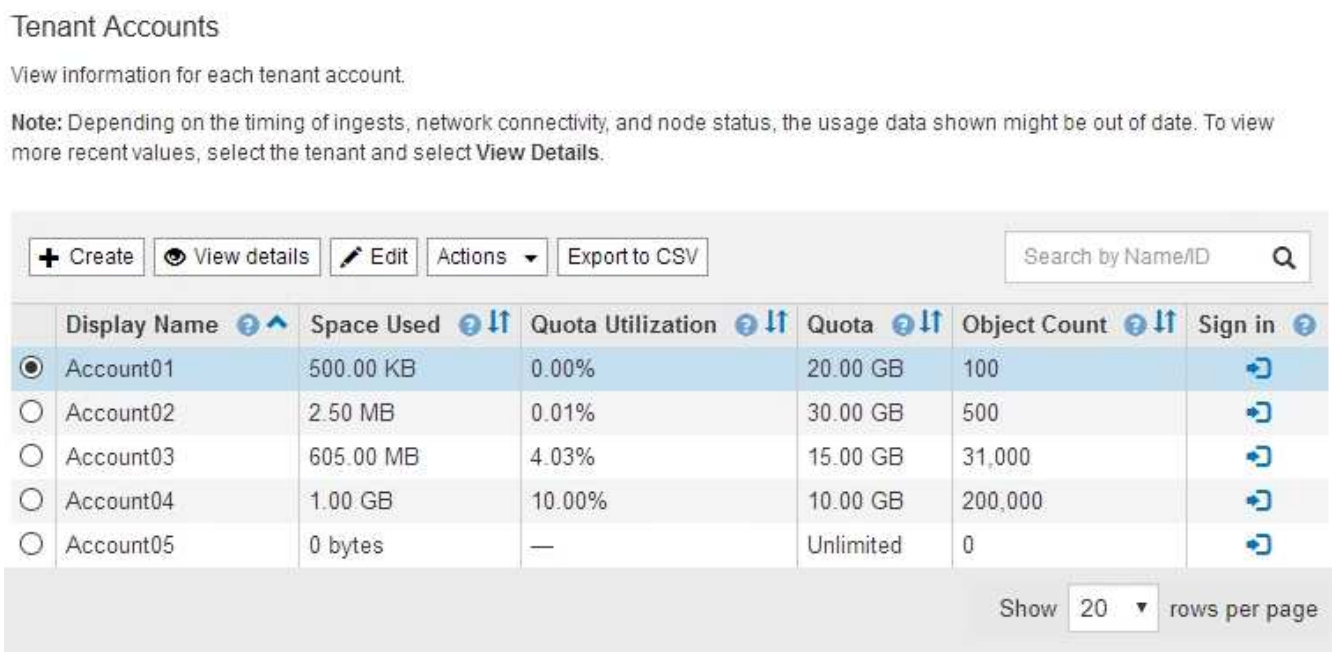
必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

手順

1. 「* tenants *」を選択します

   Tenant Accountsページが表示され、既存のテナントアカウントがすべてリストされます。

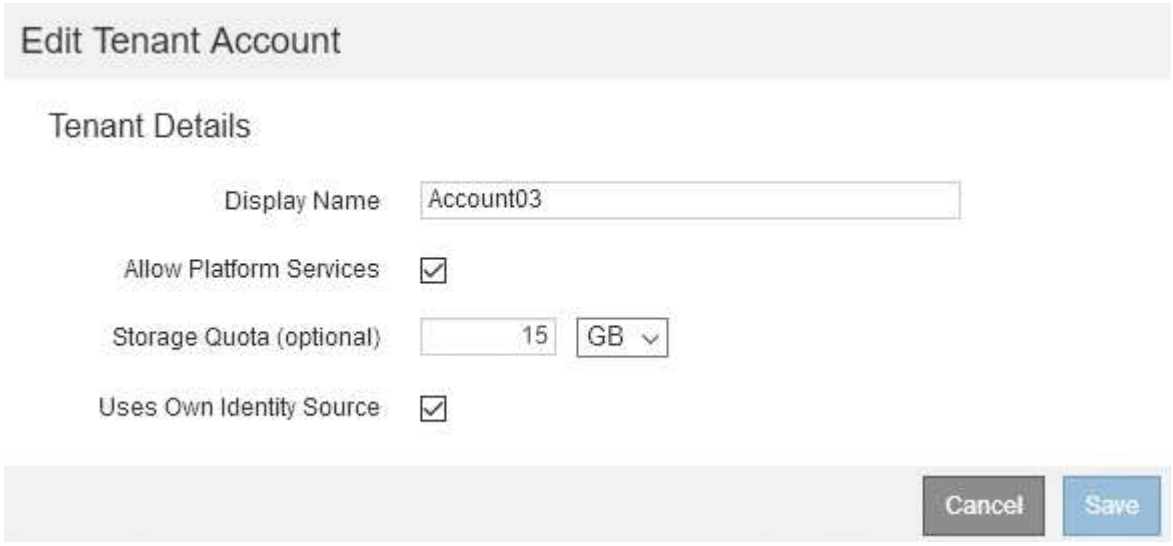


2. 編集するテナントアカウントを選択します。

   システムに20個を超えるアイテムが含まれている場合は、各ページに一度に表示する行数を指定できます。検索ボックスを使用して、表示名またはテナントIDでテナントアカウントを検索します。

3. 「 * 編集 * 」を選択します。

   Edit Tenant Accountページが表示されます。この例は、シングルサインオン（ SSO ）を使用しないグリッドを対象としています。このテナントアカウントには、独自のアイデンティティソースが設定されていません。



4. 必要に応じて、フィールドの値を変更します。
   a. このテナントアカウントの表示名を変更します。
   b. テナントアカウントがS3バケットにプラットフォームサービスを使用できるかどうかを確認するには、プラットフォームサービスを許可する*チェックボックスの設定を変更します。

プラットフォームサービスをすでに使用しているテナントに対してこのオプションを無効にすると、テナントがS3バケット用に設定しているサービスが停止します。エラーメッセージはテナントに送信されません。たとえば、テナントで S3 バケットに CloudMirror レプリケーションが設定されている場合は、引き続きバケットにオブジェクトを格納できますが、エンドポイントとして設定された外部の S3 バケットにはこれらのオブジェクトのコピーが作成されなくなります。

c. ストレージクォータ*の場合、このテナントのオブジェクトで使用可能な最大ギガバイト数、テラバイト数、またはペタバイト数を変更します。このテナントのクォータを無制限にする場合は、このフィールドを空白のままにします。

   テナントのストレージクォータは、物理容量（ディスクのサイズ）ではなく、論理容量（オブジェクトのサイズ）を表します。ILMのコピーおよびイレイジャーコーディングは、クォータの使用量にはカウントされません。

   各テナントアカウントのストレージ使用状況を監視するには、「使用状況」を選択します。テナントアカウントは、Tenant Managerのダッシュボードまたはテナント管理APIを使用して自分の使用状況を監視することもできます。ノードがグリッド内の他のノードから切断されていると、テナントのストレージ使用状況の値が最新ではなくなる場合があります。合計はネットワーク接続が回復すると更新されます。

d. テナントアカウントで独自のアイデンティティソースを使用するか、Grid Manager用に設定されたアイデンティティソースを使用するかを決定するには、* Use own Identity Source *チェックボックスの設定を変更します。

   [独自のアイデンティティソースを使用する]チェックボックスが次の場合：

   - 無効にしてオンにした場合、テナントでは独自のアイデンティティソースがすでに有効になっています。Grid Manager 用に設定されたアイデンティティソースを使用するには、テナント側で独自のアイデンティティソースを無効にする必要があります。
   - StorageGRID システムで SSO が有効になっている場合は、無効にしてオフにします。テナントは、 Grid Manager 用に設定されたアイデンティティソースを使用する必要があります。

5. [保存（ Save ）] を選択します。

関連情報

"S3テナントアカウント用のプラットフォームサービスの管理"

"テナントアカウントを使用する"

テナントアカウントを削除する

システムに対するテナントのアクセス権を完全に削除する場合は、テナントアカウントを削除します。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。
- テナントアカウントに関連付けられているすべてのバケット（ S3 ）、コンテナ（ Swift ）、およびオブ

ジェクトを削除しておく必要があります。

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選択します。

   システムに20個を超えるアイテムが含まれている場合は、各ページに一度に表示する行数を指定できます。検索ボックスを使用して、表示名またはテナントIDでテナントアカウントを検索します。

3. [アクション（* Actions ）]ドロップダウンから、[*削除（ Remove）]を選択します。
4. 「 * OK 」を選択します。

関連情報

"StorageGRID への管理者アクセスの制御"

S3テナントアカウント用のプラットフォームサービスの管理

S3 テナントアカウントでプラットフォームサービスを有効にする場合は、テナントがそのサービスの使用に必要な外部リソースにアクセスできるようにグリッドを設定する必要があります。

- "プラットフォームサービスとは"
- "プラットフォームサービス用のネットワークとポート"
- "サイト単位のプラットフォームサービスメッセージの配信"
- "プラットフォームサービスのトラブルシューティング"

プラットフォームサービスとは

プラットフォームサービスには、 CloudMirror レプリケーション、イベント通知、および検索統合サービスがあります。

これらのサービスを使用すると、テナントの S3 バケットで次の機能を使用できます。

- * CloudMirror レプリケーション * ： StorageGRID CloudMirror レプリケーションサービスは、 StorageGRID バケットから指定された外部のデスティネーションに特定のオブジェクトをミラーリングするために使用します。

  たとえば、 CloudMirror レプリケーションを使用して特定の顧客レコードを Amazon S3 にミラーリングし、 AWS サービスを利用してデータを分析することができます。

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

- * 通知 * ：バケット単位のイベント通知は、オブジェクトに対して実行された特定の処理に関する通知を、指定された外部の Amazon Simple Notification Service ™（ SNS ）に送信するために使用します。

  たとえば、バケットに追加された各オブジェクトについてアラートが管理者に送信されるように設定できます。この場合、オブジェクトは重大なシステムイベントに関連付けられているログファイルです。

S3 オブジェクトのロックが有効になっているバケットでイベント通知を設定することはできますが、オブジェクトの S3 オブジェクトロックメタデータ（ Retain Until Date および Legal Hold のステータスを含む）は通知メッセージに含まれません。

- * 検索統合サービス * ：検索統合サービスは、外部サービスを使用してメタデータを検索または分析できるように、指定された Elasticsearch インデックスに S3 オブジェクトメタデータを送信するために使用します。

  たとえば、リモートの Elasticsearch サービスに S3 オブジェクトメタデータを送信するようにバケットを設定できます。次に、 Elasticsearch を使用してバケット間で検索を実行し、オブジェクトメタデータのパターンに対して高度な分析を実行できます。

  S3 オブジェクトロックが有効なバケットでは Elasticsearch 統合を設定できますが、オブジェクトの S3 オブジェクトロックメタデータ（ Retain Until Date および Legal Hold のステータスを含む）は通知メッセージに含まれません。

プラットフォームサービスを使用すると、テナントで、外部ストレージリソース、通知サービス、データの検索または分析サービスを利用できるようになります。通常、プラットフォームサービスのターゲットは StorageGRID 環境の外部にあるため、テナントにこれらのサービスの使用を許可するかどうかを決める必要があります。この方法を使用する場合は、テナントアカウントを作成または編集するときにプラットフォームサービスの使用を有効にする必要があります。テナントで生成されたプラットフォームサービスのメッセージが宛先に届くようにネットワークを設定する必要もあります。

プラットフォームサービスの使用に関する推奨事項

プラットフォームサービスを使用する前に、次の推奨事項を確認してください。

- CloudMirror のレプリケーション、通知、検索統合を必要とする S3 要求ではアクティブなテナントが 100 個を超えないようにします。アクティブなテナントが 100 を超えると、 S3 クライアントのパフォーマンスが低下する可能性があります。
- StorageGRID システムの S3 バケットで、バージョン管理と CloudMirror レプリケーションの両方が有効になっている場合は、デスティネーションエンドポイントでも S3 バケットのバージョン管理を有効にします。これにより、 CloudMirror レプリケーションでエンドポイントに同様のオブジェクトバージョンを生成できます。

関連情報

"テナントアカウントを使用する"

"ストレージプロキシを設定しています"

"トラブルシューティングを監視します"

プラットフォームサービス用のネットワークとポート

S3 テナントにプラットフォームサービスの使用を許可する場合は、プラットフォームサービスのメッセージがデスティネーションに配信されるようにグリッドのネットワークを設定する必要があります。

テナントアカウントを作成または更新する際に、 S3 テナントアカウントのプラットフォームサービスを有効にできます。プラットフォームサービスが有効になっている場合、テナントは、その S3 バケットからの

CloudMirror レプリケーション、イベント通知、または検索統合のメッセージのデスティネーションとして機能するエンドポイントを作成できます。これらのプラットフォームサービスメッセージは、 ADC サービスを実行しているストレージノードからデスティネーションエンドポイントに送信されます。

たとえば、テナントは次のタイプのデスティネーションエンドポイントを設定できます。

- ローカルでホストされる Elasticsearch クラスタ
- Simple Notification Service （ SNS ）メッセージの受信をサポートするローカルアプリケーション
- StorageGRID の同じインスタンス上または別のインスタンス上の、ローカルにホストされる S3 バケット
- Amazon Web Services 上のエンドポイントなどの外部エンドポイント。

プラットフォームサービスメッセージが確実に配信されるように、 ADC ストレージノードが含まれるネットワークを設定する必要があります。デスティネーションエンドポイントへのプラットフォームサービスメッセージの送信に、次のポートを使用できることを確認する必要があります。

デフォルトでは、プラットフォームサービスメッセージは次のポートで送信されます。

- **80** ：エンドポイント URI が http で始まる場合
- **442** ： https で始まるエンドポイント URI の場合

エンドポイントの作成や編集を行う際に、テナントで別のポートを指定できます。

> StorageGRID 環境が CloudMirror レプリケーションのデスティネーションとして使用されている場合は、ポート 80 または 443 以外のポートにレプリケーションメッセージが送信される可能性があります。デスティネーション StorageGRID 環境で S3 に使用されているポートがエンドポイントで指定されていることを確認してください。

非透過型プロキシサーバを使用する場合は、ストレージプロキシの設定で、インターネット上のエンドポイントなどの外部エンドポイントへのメッセージの送信を許可する必要もあります。

関連情報

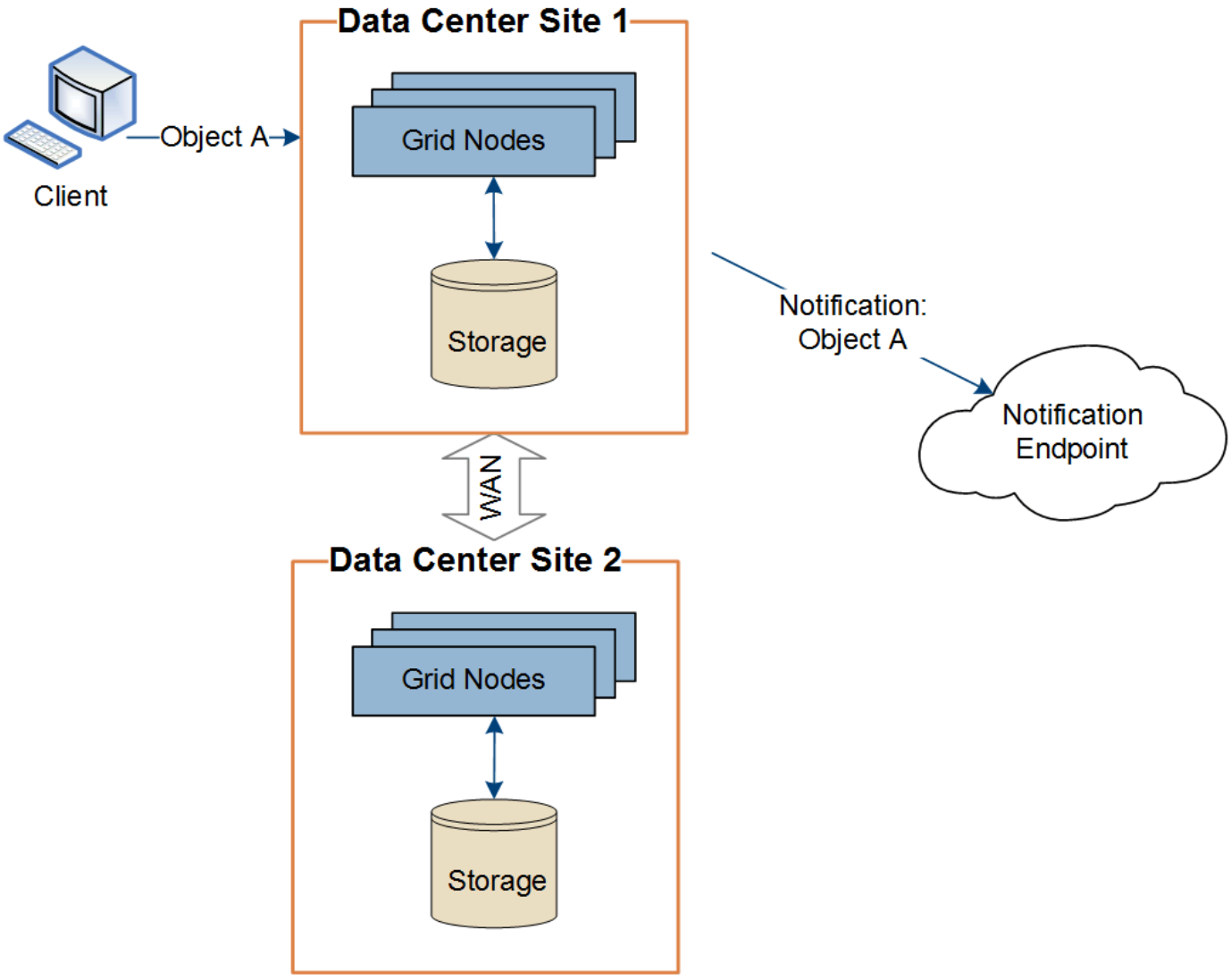
"ストレージプロキシを設定しています"

"テナントアカウントを使用する"

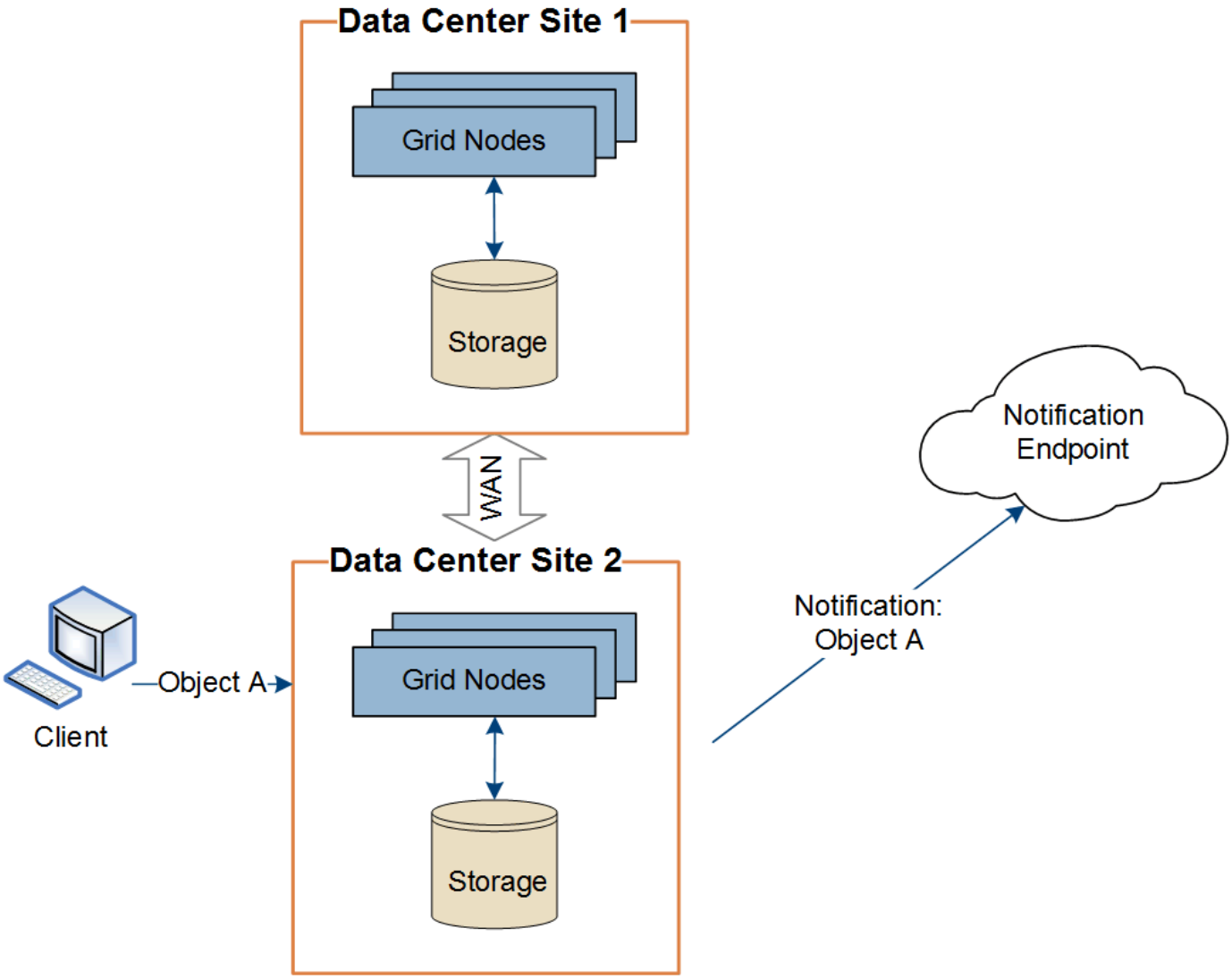
サイト単位のプラットフォームサービスメッセージの配信

プラットフォームサービスの処理はすべてサイト単位で実行されます。

つまり、テナントがクライアントを使用してデータセンターサイト 1 のゲートウェイノードに接続し、オブジェクトに対して S3 API の Create 処理を実行すると、その処理に関する通知はデータセンターサイト 1 からトリガーされて送信されます。



クライアントが続けてデータセンターサイト 2 から同じオブジェクトに対して S3 API の Delete 処理を実行すると、その処理に関する通知はデータセンターサイト 2 からトリガーされて送信されます。



プラットフォームサービスメッセージを宛先に配信できるように、各サイトのネットワークが設定されていることを確認します。

プラットフォームサービスのトラブルシューティング

プラットフォームサービスで使用されるエンドポイントは、テナントユーザが Tenant Manager で作成および管理します。ただし、テナントでプラットフォームサービスの設定または使用に関する問題がテナントで発生した場合は、グリッドマネージャを使用して問題 を解決できる可能性があります。

新しいエンドポイントに関する問題

テナントでプラットフォームサービスを使用するには、 Tenant Manager を使用してエンドポイントを 1 つ以上作成する必要があります。各エンドポイントは、 StorageGRID S3 バケット、 Amazon Web Services バケット、 Simple Notification Service トピック、ローカルまたは AWS でホストされる Elasticsearch クラスタなど、 1 つのプラットフォームサービスの外部のデスティネーションを表します。各エンドポイントには、外部リソースの場所と、そのリソースへのアクセスに必要なクレデンシャルが含まれます。

テナントでエンドポイントを作成すると、 StorageGRID システムによって、そのエンドポイントが存在するかどうかと、指定されたクレデンシャルでアクセスできるかどうかが検証されます。エンドポイントへの接続

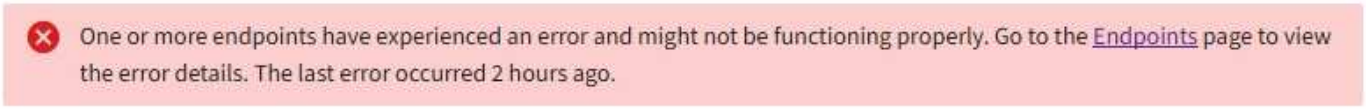
は、各サイトの 1 つのノードから検証されます。

エンドポイントの検証が失敗した場合は、その理由を記載したエラーメッセージが表示されます。テナントユーザは、問題 を解決してから、エンドポイントの作成をもう一度実行する必要があります。

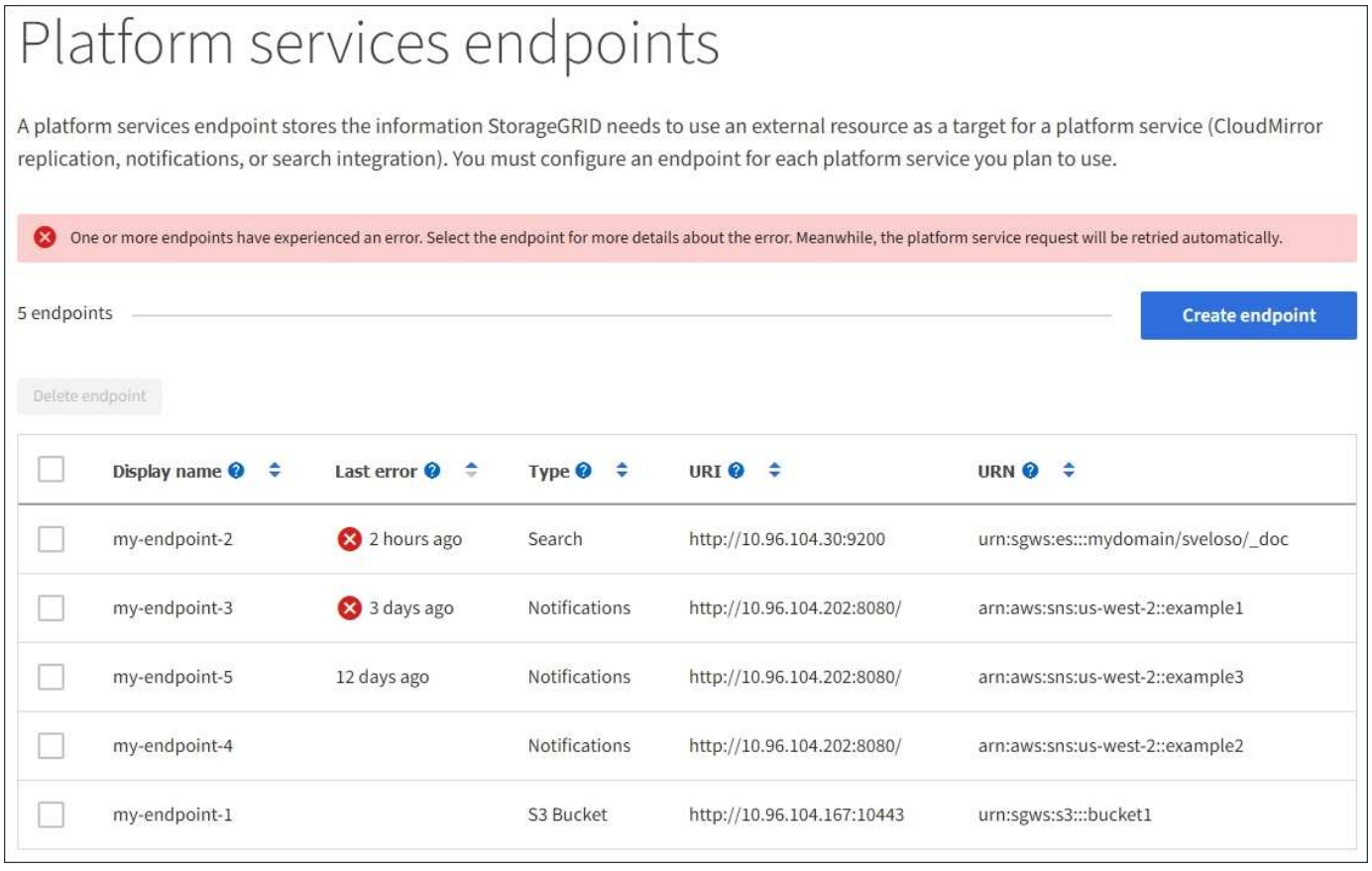
テナントアカウントでプラットフォームサービスが有効でない場合は、エンドポイントの作成が失敗します。

既存のエンドポイントに関する問題

StorageGRID が既存のエンドポイントにアクセスしようとしたときにエラーが発生した場合は、テナントマネージャのダッシュボードにメッセージが表示されます。



テナントユーザは、エンドポイントページに移動して各エンドポイントの最新のエラーメッセージを確認し、エラーが発生してからの時間を特定できます。[* Last error*] 列には、各エンドポイントの最新のエラーメッセージとエラーが発生してからの経過時間が表示されます。が含まれるエラーです アイコンは過去 7 日以内に発生しました。



「 * Last error * 」列の一部のエラーメッセージには、かっこ内にログ ID が含まれている場合があります。グリッド管理者やテクニカルサポートは、この ID を使用して、 bycast.log のエラーに関する詳細情報を確認できます。

プロキシサーバに関連する問題

ストレージノードとプラットフォームサービスエンドポイントの間にストレージプロキシを設定している場合、プロキシサービスで StorageGRID からのメッセージが許可されていないとエラーが発生する可能性があります。これらの問題を解決するには、プロキシサーバの設定を調べて、プラットフォームサービス関連のメッセージがブロックされていないことを確認してください。

エラーが発生したかどうかを確認しています

過去 7 日間にエンドポイントエラーが発生した場合は、 Tenant Manager のダッシュボードにアラートメッセージが表示されます。エラーの詳細を確認するには、エンドポイントのページに移動します。

クライアント処理が失敗する

一部のプラットフォームサービスの問題により、 S3 バケットに対する原因 クライアント処理が失敗することがあります。たとえば、内部の Replicated State Machine （ RSM ）サービスが停止した場合や、配信のためにキューに登録されたプラットフォームサービスメッセージが多すぎる場合は、 S3 クライアント処理が失敗します。

サービスのステータスを確認するには、次の手順に従います。

1. Support **>** Tools **>** Grid Topology *を選択します。
2. [***site *>*_Storage Node***>*SSM*>*Services] を選択します。

リカバリ可能なエンドポイントエラーとリカバリ不能なエンドポイントエラー

エンドポイントの作成後に、さまざまな理由からプラットフォームサービス要求のエラーが発生することがあります。一部のエラーは、ユーザが対処することでリカバリできます。たとえば、リカバリ可能なエラーは次のような原因で発生する可能性があります。

- ユーザのクレデンシャルが削除されたか、期限切れになっています。
- デスティネーションバケットが存在しません。
- 通知を配信できません。

StorageGRID でリカバリ可能なエラーが発生した場合は、成功するまでプラットフォームサービス要求が再試行されます。

その他のエラーはリカバリできません。たとえば、エンドポイントが削除されるとリカバリ不能なエラーが発生します。

StorageGRID でリカバリ不能なエンドポイントのエラーが発生すると、Grid ManagerでTotal Events（SMTT）アラームが生成されます。Total Eventsアラームを表示するには、次の手順を実行し

1. [ノード（ Nodes）]を選択し
2. 「***site *>* grid node_name >*** Events *」を選択します。
3. 表の一番上に Last Event が表示されます。

   イベントメッセージは、にも表示されます `/var/local/log/bycast-err.log`。

4. SMTT アラームに記載されている指示に従って問題 を修正します。

5. [イベントカウントのリセット]をクリックします。
6. プラットフォームサービスメッセージが配信されていないオブジェクトについてテナントに通知します。
7. テナントで、オブジェクトのメタデータまたはタグを更新することで、失敗したレプリケーションまたは通知を再度トリガーするよう指定します。

   テナントでは、既存の値を再送信し、不要な変更を回避できます。

プラットフォームサービスメッセージを配信できません

デスティネーションでプラットフォームサービスメッセージの受信を妨げる問題 が検出された場合、バケットに対する処理は成功しますが、プラットフォームサービスメッセージは配信されません。たとえば、デスティネーションでクレデンシャルが更新されたため StorageGRID がデスティネーションサービスを認証できなくなった場合に、このエラーが発生することがあります。

リカバリ不能なエラーによってプラットフォームサービスメッセージを配信できない場合は、Grid ManagerでTotal Events（SMTT）アラームが生成されます。

プラットフォームサービス要求のパフォーマンスが低下します

要求が送信されるペースがデスティネーションエンドポイントで要求を受信できるペースを超えると、StorageGRID ソフトウェアはバケットの受信 S3 要求を調整する場合があります。スロットルは、デスティネーションエンドポイントへの送信を待機している要求のバックログが生じている場合にのみ発生します。

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

通常、 CloudMirror 要求には、検索統合やイベント通知の要求よりも多くのデータ転送が含まれるため、デスティネーションエンドポイントのパフォーマンスによる影響を受ける可能性が高くなります。

プラットフォームサービス要求が失敗しました

プラットフォームサービスの要求の失敗率を表示するには、次の手順を実行します。

1. [ノード（ Nodes）]を選択し
2. [**_site *>*Platform Services**] を選択します。
3. ［障害発生率の要求］チャートを表示します。

Platform services unavailable アラート

「 * Platform services unavailable * 」アラートは、実行中または使用可能な RSM サービスがあるストレージノードが少なすぎるために、サイトでプラットフォームサービスの処理を実行できないことを示しています。

RSM サービスは、プラットフォームサービス要求がそれぞれのエンドポイントに確実に送信されるようにします。

このアラートを解決するには、サイトのどのストレージノードに RSM サービスが含まれているかを特定します（ RSM サービスは、 ADC サービスがあるストレージノードにあります）。 そのあと、それらのストレージノードの過半数が稼働していて使用可能であることを確認します。

RSM サービスを含む複数のストレージノードでサイトで障害が発生すると、そのサイトに対する保留中のプラットフォームサービス要求はすべて失われます。

プラットフォームサービスエンドポイントに関するその他のトラブルシューティングガイダンス

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に関する追加情報 の詳細については、テナントアカウントの使用手順を参照してください。

"テナントアカウントを使用する"

関連情報

"トラブルシューティングを監視します"

"ストレージプロキシを設定しています"

S3およびSwiftクライアント接続の設定

グリッド管理者は設定オプションを管理して、 S3 および Swift テナントがクライアントアプリケーションを StorageGRID システムに接続してデータの格納と読み出しを行う方法を制御します。クライアントとテナントのさまざまな要件を満たすために、多数のオプションが用意されています。

クライアントアプリケーションは、次のいずれかに接続することで、オブジェクトを格納または読み出すことができます。

- 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、または必要に応じて、管理ノードまたはゲートウェイノードのハイアベイラビリティ（ HA ）グループの仮想 IP アドレス
- ゲートウェイノード上の CLB サービス、または必要に応じて、ゲートウェイノードのハイアベイラビリティグループの仮想 IP アドレス

CLB サービスは廃止されました。StorageGRID 11.3 より前に設定されたクライアントは、ゲートウェイノード上の CLB サービスを引き続き使用できます。ロードバランシングに StorageGRID を使用する他のすべてのクライアントアプリケーションは、ロードバランササービスを使用して接続する必要があります。

- 外部ロードバランサを使用するかどうかに関係なく、ストレージノードに追加されます

StorageGRID システムには、必要に応じて次の機能も設定できます。

- ロードバランササービス：クライアントがロードバランササービスを使用できるようにするには、クライアント接続用のロードバランサエンドポイントを作成します。ロードバランサエンドポイントを作成する際には、ポート番号、エンドポイントで HTTP / HTTPS 接続を許可するかどうか、エンドポイントを使用するクライアントのタイプ（ S3 または Swift ）、 HTTPS 接続に使用する証明書（該当する場合）を指定します。
- * 信頼されていないクライアントネットワーク * ：信頼されていないクライアントネットワークとして設定することで、クライアントネットワークのセキュリティを強化できます。クライアントネットワークが信頼されていない場合、クライアントはロードバランサエンドポイントを使用して接続する必要があります。
- ハイアベイラビリティグループ：ゲートウェイノードまたは管理ノードのHAグループを作成してアクテ

ィブ/バックアップ構成を作成できます。また、ラウンドロビンDNSや他社製ロードバランサと複数のHAグループを使用してアクティブ/アクティブ構成を実現することもできます。クライアント接続は、 HA グループの仮想 IP アドレスを使用して確立されます。

ストレージノードに直接接続するか、 CLB サービス（廃止予定）を使用して StorageGRID に接続するクライアントに対しては、 HTTP の使用を有効にし、 S3 クライアントには S3 API エンドポイントのドメイン名を設定できます。

Summary ：クライアント接続の **IP** アドレスとポート

クライアントアプリケーションは、グリッドノードの IP アドレスおよび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。ハイアベイラビリティ（ HA ）グループが設定されている場合は、 HA グループの仮想 IP アドレスを使用してクライアントアプリケーションを接続できます。

このタスクについて

次の表に、クライアントが StorageGRID に接続できるさまざまな方法、および接続のタイプごとに使用される IP アドレスとポートを示します。以下の手順では、ロードバランサエンドポイントとハイアベイラビリティ（ HA ）グループがすでに設定されている場合に Grid Manager でこの情報を検索する方法について説明します。

接続が確立される場所	クライアントが接続するサービス	**IP** アドレス	ポート
HA グループ	ロードバランサ	HA グループの仮想 IP アドレス	• ロードバランサエンドポイントのポート
HA グループ	CLB の機能です • 注： * CLB サービスは廃止されました。	HA グループの仮想 IP アドレス	デフォルトの S3 ポート： • HTTPS ： 8082 • HTTP ： 8084 デフォルトの Swift ポート： • HTTPS ： 8083 • HTTP ： 8085
管理ノード	ロードバランサ	管理ノードの IP アドレス	• ロードバランサエンドポイントのポート
ゲートウェイノード	ロードバランサ	ゲートウェイノードの IP アドレス	• ロードバランサエンドポイントのポート

接続が確立される場所	クライアントが接続するサービス	**IP** アドレス	ポート
ゲートウェイノード	CLB の機能です • 注： * CLB サービスは廃止されました。	ゲートウェイノードの IP アドレス • 注：デフォルトでは、 CLB および LDR の HTTP ポートは有効になっていません。	デフォルトの S3 ポート： • HTTPS ： 8082 • HTTP ： 8084 デフォルトの Swift ポート： • HTTPS ： 8083 • HTTP ： 8085
ストレージノード	LDR	ストレージノードの IP アドレス	デフォルトの S3 ポート： • HTTPS ： 18082 • HTTP ： 18084 デフォルトの Swift ポート： • HTTPS ： 18083 • HTTP ： 18085

例

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 S3 クライアントを接続するには、次のように構造化された 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 S3 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、 S3 クライアントは次の URL を使用して StorageGRID に接続できます。

- `https://192.0.2.5:10443`

Swift クライアントをゲートウェイノードの HA グループのロードバランサエンドポイントに接続するには、次のように構造化された 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 192.0.2.6 で、 Swift ロードバランサエンドポイントのポート番号が 10444 の場合、 Swift クライアントは次の URL を使用して StorageGRID に接続できます。

- `https://192.0.2.6:10444`

クライアントが StorageGRID への接続に使用する IP アドレスに DNS 名を設定できます。ローカルネットワーク管理者にお問い合わせください。

手順

1. サポートされているブラウザを使用してGrid Managerにサインインします。
2. グリッドノードの IP アドレスを確認するには、次の手順を実行します。
   a. [ノード（ Nodes）]を選択し
   b. 接続する管理ノード、ゲートウェイノード、またはストレージノードを選択します。
   c. [* Overview * （概要 * ）] タブを選択します。
   d. Node Information セクションで、ノードの IP アドレスを確認します。
   e. Show More *をクリックして、IPv6アドレスとインターフェイスマッピングを表示します。

      クライアントアプリケーションから、リスト内の任意の IP アドレスへの接続を確立できます。

      - * eth0 ： * グリッドネットワーク
      - * eth1 ： * 管理ネットワーク（オプション）
      - * eth2 ： * クライアントネットワーク（オプション）

      表示されている管理ノードまたはゲートウェイノードがハイアベイラビリティグループのアクティブノードである場合は、 HA グループの仮想 IP アドレスが eth2 に表示されます。

3. ハイアベイラビリティグループの仮想 IP アドレスを検索するには、次の手順を実行します。
   a. * Configuration > Network Settings > High Availability Groups *を選択します。
   b. HA グループの仮想 IP アドレスを表で確認します。
4. ロードバランサエンドポイントのポート番号を確認するには、次の手順を実行します。
   a. [* Configuration > Network Settings > Load Balancer Endpoints *]を選択します。

      Load Balancer Endpoints ページが表示され、設定済みのエンドポイントのリストが表示されます。

   b. エンドポイントを選択し、*エンドポイントの編集*をクリックします。

      [Edit Endpoint] ウィンドウが開き、エンドポイントに関する追加の詳細が表示されます。

   c. 選択したエンドポイントが正しいプロトコル（S3またはSwift）で使用するように設定されていることを確認し、* Cancel *をクリックします。
   d. クライアント接続に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にのみ設定されます。それ以外のポートはすべて、ゲートウェイノードと管理ノードの両方に設定されます。

負荷分散の管理

StorageGRID のロードバランシング機能を使用して、 S3 / Swift クライアントからの取り込み / 読み出しワークロードを処理できます。ロードバランシングは、複数のストレ

ージノードにワークロードと接続を分散することで、速度と接続容量を最大化します。

StorageGRID システムでは、次の方法でロードバランシングを実現できます。

- 管理ノードとゲートウェイノードにインストールされているロードバランササービスを使用します。ロードバランササービスはレイヤ 7 のロードバランシングを提供し、クライアント要求の TLS ターミネーション、要求の検査、およびストレージノードへの新しいセキュアな接続の確立を実施します。これは推奨されるロードバランシングメカニズムです。
- ゲートウェイノードにのみインストールされているConnection Load Balancer（CLB）サービスを使用します。CLB サービスはレイヤ 4 のロードバランシングを提供し、リンクコストをサポートします。

  CLB サービスは廃止されました。

- サードパーティ製ロードバランサを統合します。詳細については、ネットアップのアカウント担当者にお問い合わせください。

ロードバランシングの仕組み - ロードバランササービス

ロードバランササービスは、クライアントアプリケーションからの受信ネットワーク接続を複数のストレージノードに分散します。ロードバランシングを有効にするには、Grid Manager を使用してロードバランサエンドポイントを設定する必要があります。

ロードバランサエンドポイントは管理ノードまたはゲートウェイノードにのみ設定できます。これらのノードタイプにはロードバランササービスが含まれているためです。ストレージノードまたはアーカイブノードにエンドポイントを設定することはできません。

各ロードバランサエンドポイントは、ポート、プロトコル（HTTPまたはHTTPS）、サービスタイプ（S3またはSwift）、およびバインドモードを指定します。HTTPS エンドポイントにはサーバ証明書が必要です。バインドモードでは、エンドポイントポートのアクセスを次のように制限できます。

- 特定のハイアベイラビリティ（HA）仮想IPアドレス（VIP）
- 特定のノードの特定のネットワークインターフェイス

ポートに関する考慮事項

クライアントは、ロードバランササービスを実行しているノードに設定された任意のエンドポイントにアクセスできます。ただしポート 80 と 443 は例外で、管理ノードではこれらのノードが予約されているため、これらのポートに設定されたエンドポイントはゲートウェイノードでのみロードバランシング処理をサポートします。

ポートを再マッピングした場合、同じポートを使用してロードバランサエンドポイントを設定することはできません。再マッピングしたポートを使用してエンドポイントを作成できますが、これらのエンドポイントはロードバランササービスではなく、元の CLB ポートおよびサービスに再マッピングされます。ポートの再マッピングを削除するには、リカバリとメンテナンスの手順に従ってください。

CLB サービスは廃止されました。

CPU の可用性

S3 / Swift トラフィックをストレージノードに転送する際、各管理ノードおよびゲートウェイノード上のロー

ドバランササービスは独立して動作します。重み付きのプロセスを使用すると、ロードバランササービスは、より多くの要求をより多くの CPU を使用可能なストレージノードにルーティングします。ノード CPU 負荷情報は数分ごとに更新されますが、重み付けがより頻繁に更新される場合があります。ノードの使用率が 100% になった場合や、ノードの利用率のレポートに失敗した場合でも、すべてのストレージノードには最小限のベースとなる重みの値が割り当てられます。

CPU の可用性に関する情報が、ロードバランササービスが配置されているサイトに制限されている場合があります。

関連情報

""

ロードバランサエンドポイントの設定

ロードバランサエンドポイントを作成、編集、および削除できます。

ロードバランサエンドポイントの作成

各ロードバランサエンドポイントは、ポート、ネットワークプロトコル（HTTPまたはHTTPS）、およびサービスタイプ（S3またはSwift）を指定します。HTTPSエンドポイントを作成する場合は、サーバ証明書をアップロードまたは生成する必要があります。

必要なもの

- Root Access 権限が必要です。
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- ロードバランササービスに使用するポートをすでに再マッピングしている場合は、再マッピングを削除しておく必要があります。

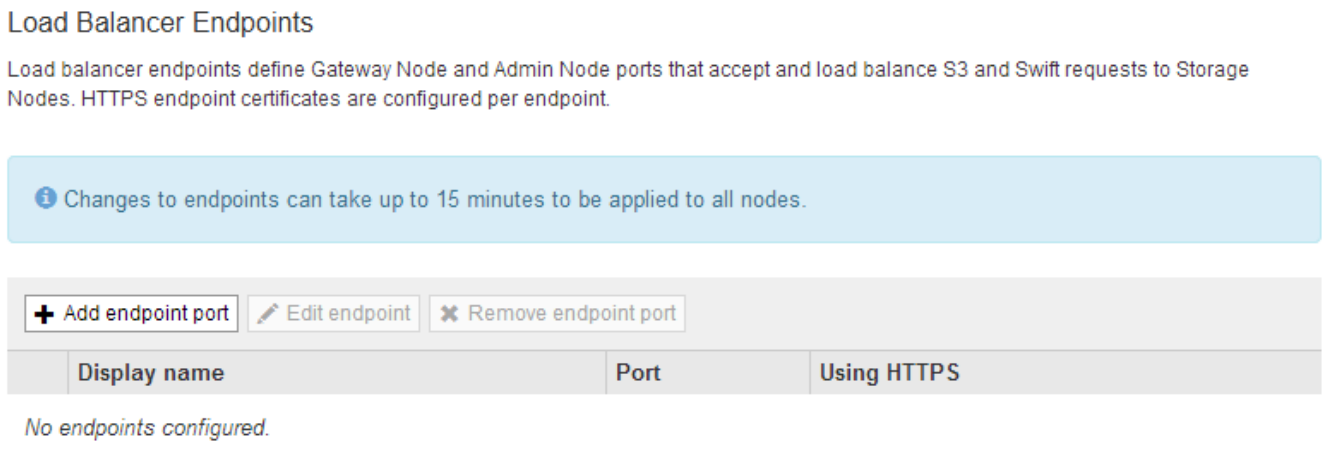
> ポートを再マッピングした場合、同じポートを使用してロードバランサエンドポイントを設定することはできません。再マッピングしたポートを使用してエンドポイントを作成できますが、これらのエンドポイントはロードバランササービスではなく、元の CLB ポートおよびサービスに再マッピングされます。ポートの再マッピングを削除するには、リカバリとメンテナンスの手順に従ってください。

> CLB サービスは廃止されました。

手順

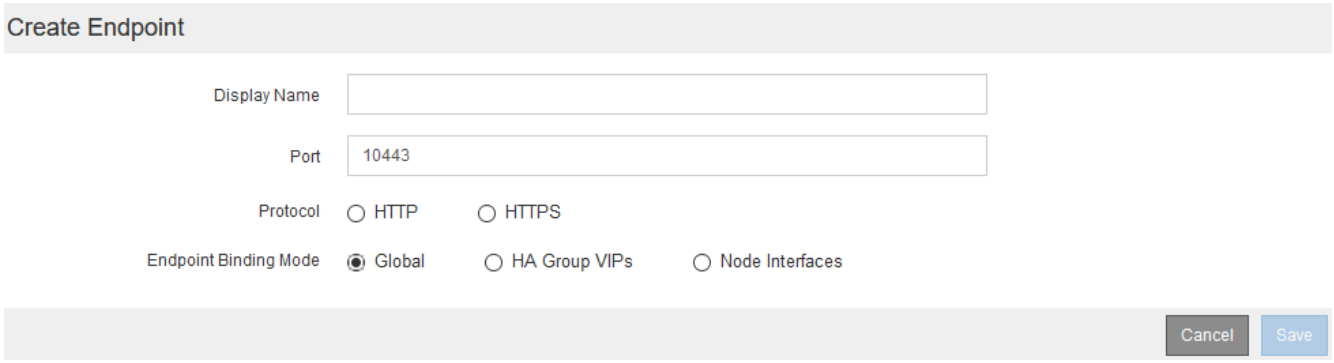
1. [* Configuration > Network Settings > Load Balancer Endpoints *]を選択します。

   Load Balancer Endpointsページが表示されます。



2. [エンドポイントの追加]を選択します。

   [Create Endpoint]ダイアログボックスが表示されます。



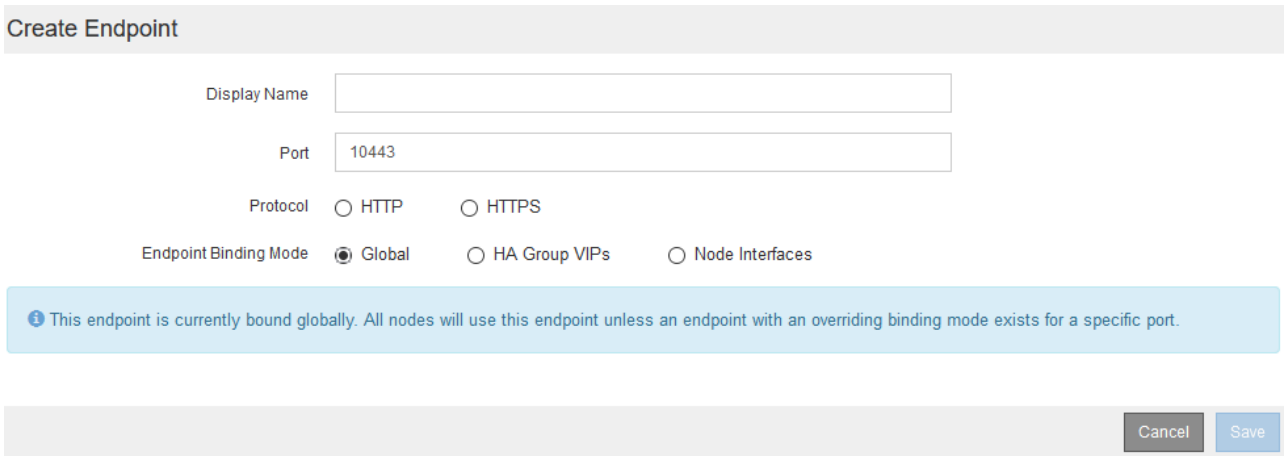
3. ロードバランサエンドポイントのページのリストに表示されるエンドポイントの表示名を入力します。
4. ポート番号を入力するか、あらかじめ入力されているポート番号をそのまま使用します。

   ポート番号80または443は管理ノードで予約されているため、これらのポートを入力すると、エンドポイントはゲートウェイノードにのみ設定されます。

   他のグリッドサービスで使用されているポートは使用できません。内部および外部の通信に使用されるポートの一覧については、ネットワークのガイドラインを参照してください。

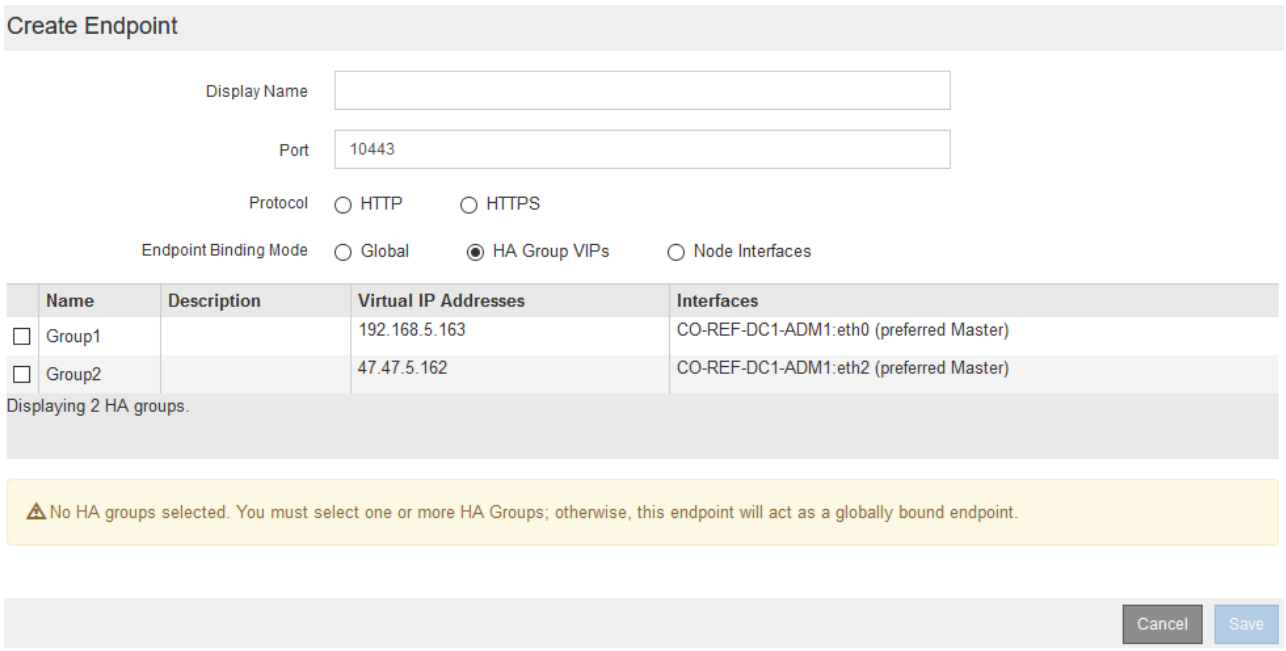
5. このエンドポイントのネットワークプロトコルを指定するには、「* HTTP 」または「 HTTPS *」を選択します。
6. エンドポイントバインディングモードを選択します。

   - * Global *（デフォルト）：指定したポート番号のすべてのゲートウェイノードと管理ノードでエンドポイントにアクセスできます。



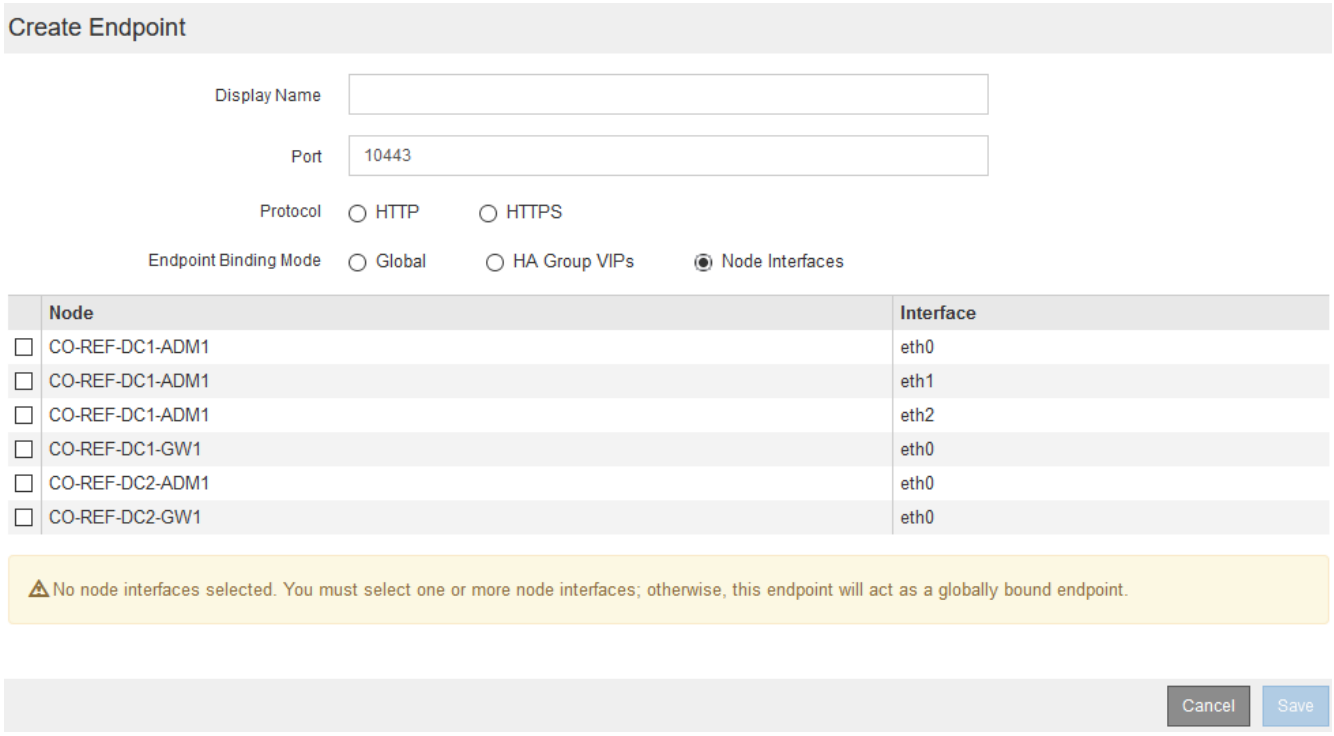
- * HA Group VIP *：エンドポイントには、選択したHAグループに定義された仮想IPアドレスからのみアクセスできます。このモードで定義されたエンドポイントは、エンドポイントによって定義されたHAグループが互いに重複しないかぎり、同じポート番号を再利用できます。

  仮想IPアドレスが割り当てられたエンドポイントを表示するHAグループを選択します。



- ノードインターフェイス：エンドポイントには、指定したノードとネットワークインターフェイスでのみアクセスできます。このモードで定義されたエンドポイントは、相互に重複しないかぎり、同じポート番号を再利用できます。

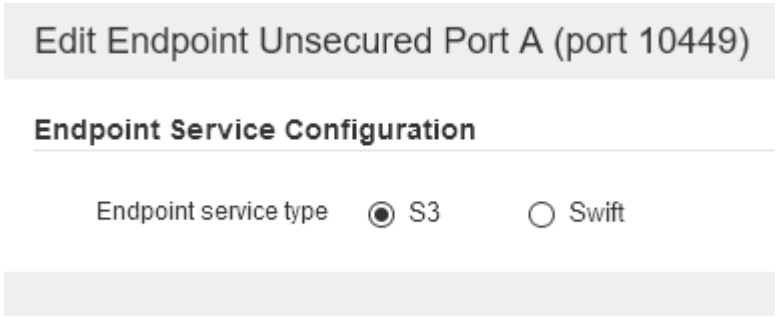
  エンドポイントを表示するノードインターフェイスを選択します。



7. [保存（ Save ）] を選択します。

   [Edit Endpoint]ダイアログボックスが表示されます。

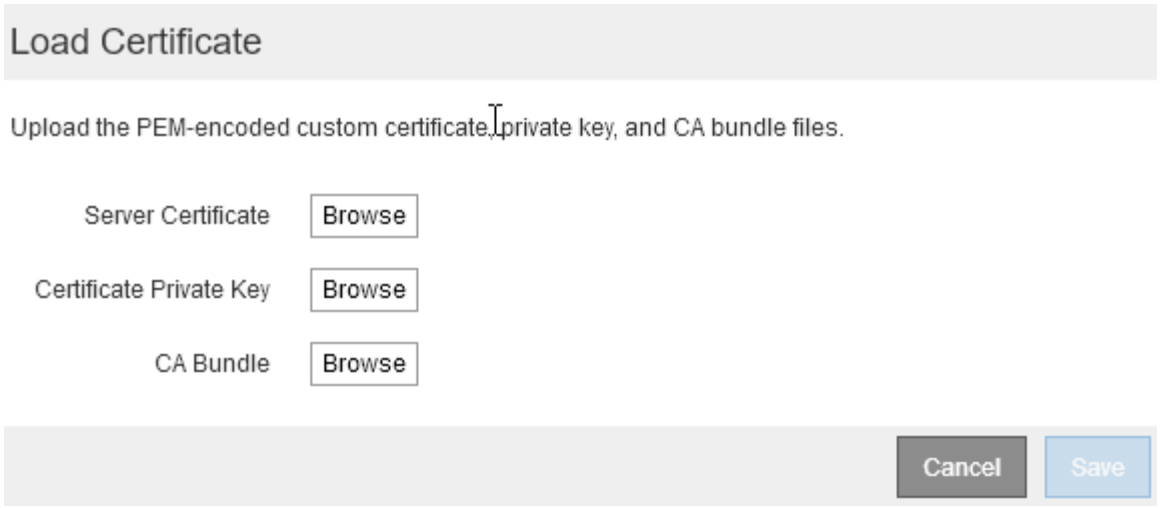
8. エンドポイントで処理するトラフィックのタイプを指定するには、「* S3 」または「 Swift *」を選択します。



9. *HTTP*を選択した場合は、*Save*を選択します。

   セキュアでないエンドポイントが作成されます。ロードバランサエンドポイントのページのテーブルには、エンドポイントの表示名、ポート番号、プロトコル、およびエンドポイントIDが表示されます。

10. [* HTTPS*]を選択し、証明書をアップロードする場合は、[証明書のアップロード]を選択します。



a. サーバ証明書と証明書の秘密鍵を参照します。

   S3クライアントがS3 APIエンドポイントのドメイン名を使用して接続できるようにするには、クライアントがグリッドへの接続に使用する可能性のあるすべてのドメイン名に一致するマルチドメイン証明書またはワイルドカード証明書を使用します。たとえば、サーバ証明書でドメイン名を使用しているとします `*.example.com`。

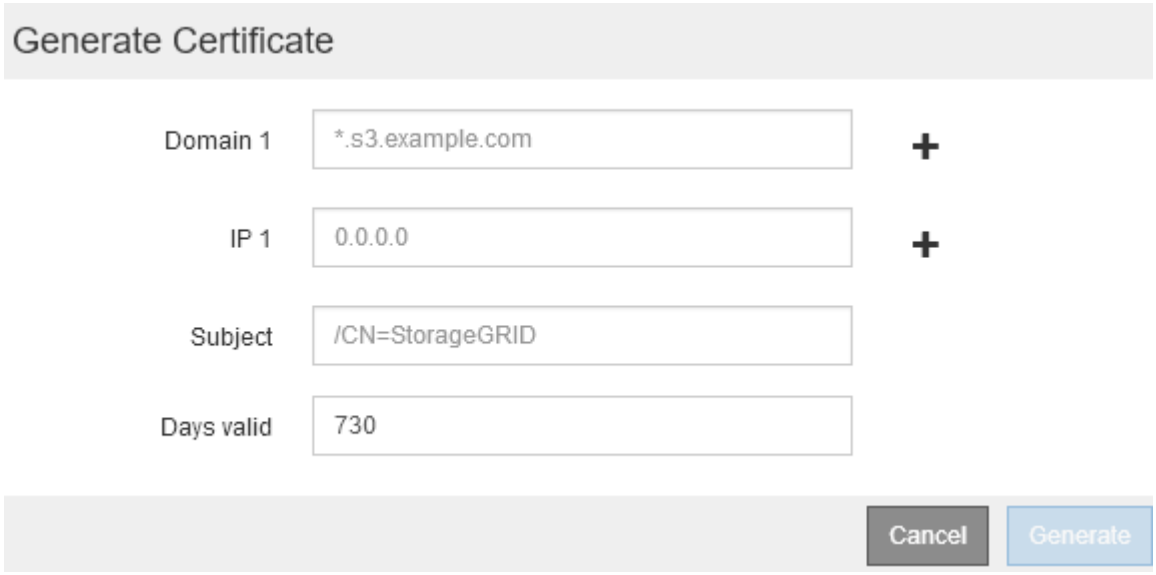
"S3 APIエンドポイントのドメイン名を設定しています"

a. 必要に応じて、CAバンドルを参照します。

b. [保存（ Save ）] を選択します。

   エンドポイントのPEMでエンコードされた証明書データが表示されます。

11. [* HTTPS*]を選択し、証明書を生成する場合は、[証明書の生成]を選択します。



a. ドメイン名またはIPアドレスを入力します。

   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： `*.sgws.foo.com` ワイルドカード*を

使用して表します `gn1.sgws.foo.com` および `gn2.sgws.foo.com`。

"S3 APIエンドポイントのドメイン名を設定しています"

a. 選択するオプション ➕ をクリックして、他のドメイン名またはIPアドレスを追加します。

   ハイアベイラビリティ（HA）グループを使用する場合は、HA仮想IPのドメイン名とIPアドレスを追加します。

b. 必要に応じて、証明書を所有するユーザを識別するために、[X.509 subject]（識別名（DN）とも呼ばれる）を入力します。

c. 必要に応じて、証明書の有効日数を選択します。デフォルトは730日です。

d. [*Generate （生成）] を選択します

   エンドポイントの証明書メタデータとPEMでエンコードされた証明書データが表示されます。

12. [保存（ Save ）] をクリックします。

    エンドポイントが作成されます。ロードバランサエンドポイントのページのテーブルには、エンドポイントの表示名、ポート番号、プロトコル、およびエンドポイントIDが表示されます。

関連情報

""

"ネットワークガイドライン"

"ハイアベイラビリティグループの管理"

"信頼されていないクライアントネットワークの管理"

ロードバランサエンドポイントの編集

セキュアでない（HTTP）エンドポイントの場合、エンドポイントのサービスタイプ（S3またはSwift）を変更できます。セキュアな（HTTPS）エンドポイントの場合、エンドポイントのサービスタイプを編集して、セキュリティ証明書を表示または変更できます。

必要なもの

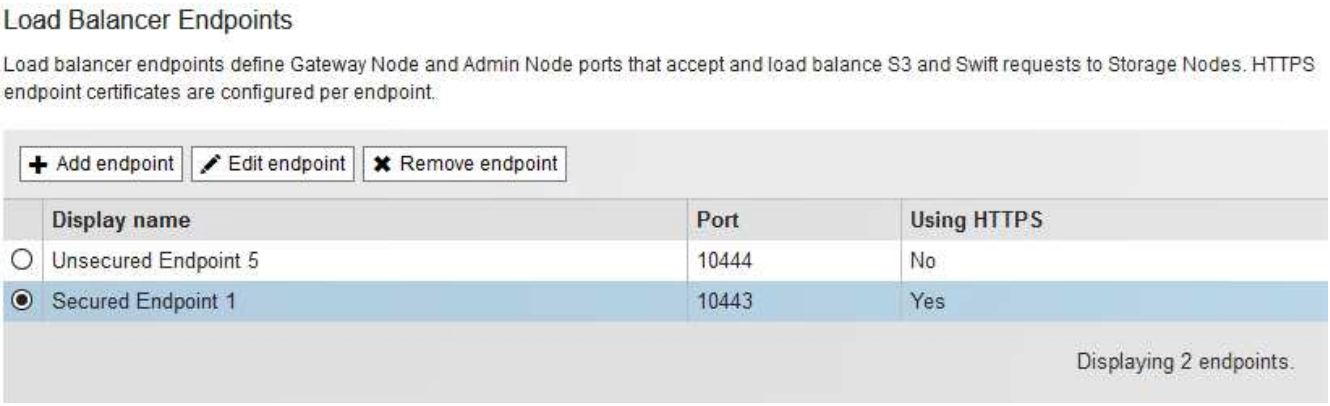
- Root Access 権限が必要です。
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

手順

1. [* Configuration > Network Settings > Load Balancer Endpoints *]を選択します。

   Load Balancer Endpointsページが表示されます。既存のエンドポイントがテーブルに表示されます。

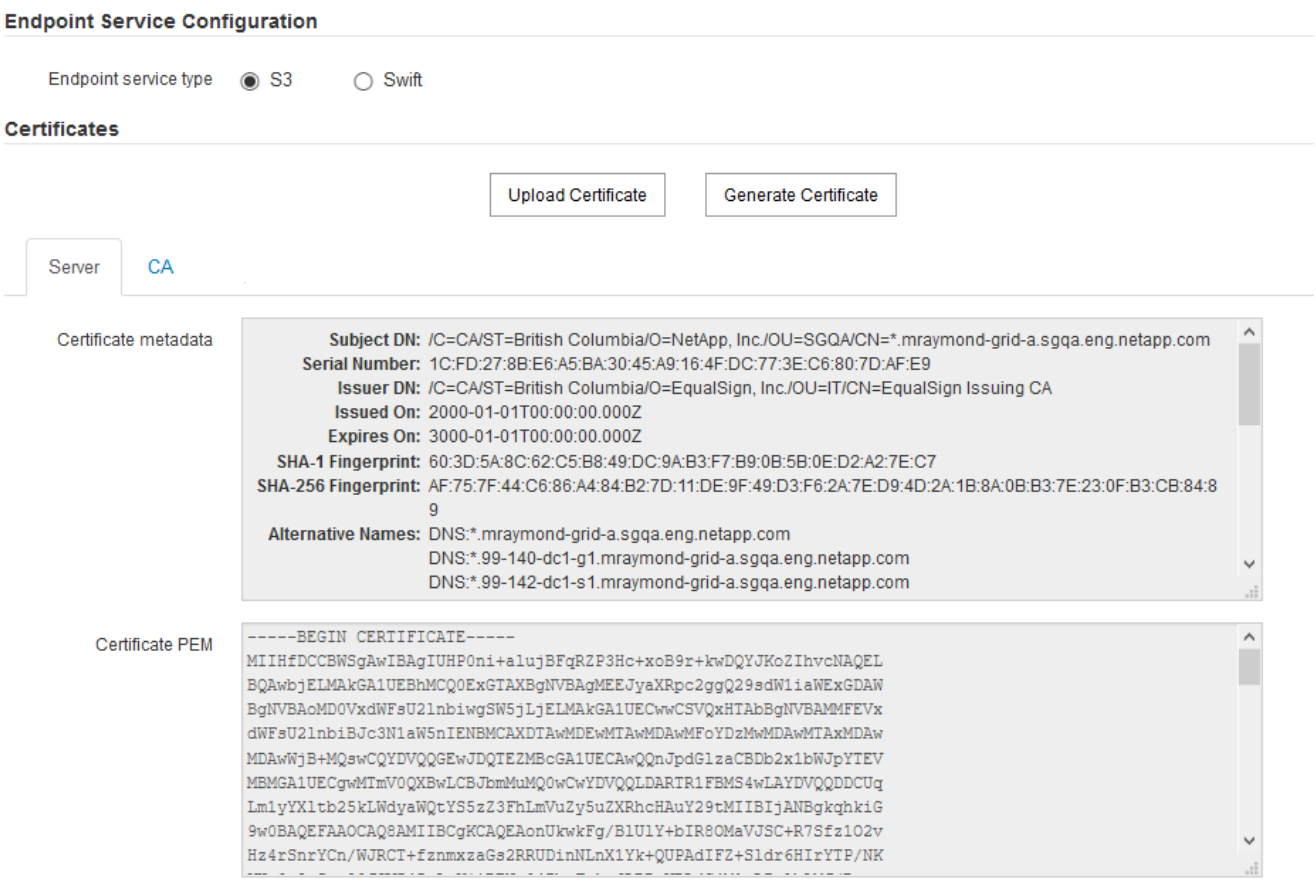
   まもなく期限切れになる証明書を含むエンドポイントが表に示されます。



2. 編集するエンドポイントを選択します。
3. *エンドポイントの編集*をクリックします。

   [Edit Endpoint]ダイアログボックスが表示されます。

   セキュアでない（HTTP）エンドポイントの場合は、ダイアログボックスの[Endpoint Service Configuration]セクションだけが表示されます。セキュア（HTTPS）エンドポイントの場合、次の例に示すように、ダイアログボックスの[Endpoint Service Configuration]セクションと[Certificates]セクションが表示されます。



4. エンドポイントに必要な変更を加えます。

   セキュアでない（HTTP）エンドポイントの場合、次の操作を実行できます。

- エンドポイントのサービスタイプをS3またはSwiftに変更します。
- エンドポイントバインディングモードを変更します。セキュアな（HTTPS）エンドポイントの場合、次の操作を実行できます。
- エンドポイントのサービスタイプをS3またはSwiftに変更します。
- エンドポイントバインディングモードを変更します。
- セキュリティ証明書を表示します。
- 現在の証明書の有効期限が切れたとき、または有効期限が近づいたときに、新しいセキュリティ証明書をアップロードまたは生成します。

  タブを選択して、デフォルトのStorageGRID サーバ証明書またはアップロードされたCA署名証明書に関する詳細情報を表示します。

> 既存のエンドポイントのプロトコルを変更する場合は、たとえばHTTPからHTTPSに変更する場合は、新しいエンドポイントを作成する必要があります。ロードバランサエンドポイントの作成手順に従って、必要なプロトコルを選択します。

5. [保存（ Save ）] をクリックします。

関連情報

[ロードバランサエンドポイントの作成]

ロードバランサエンドポイントの削除

不要になったロードバランサエンドポイントは削除できます。

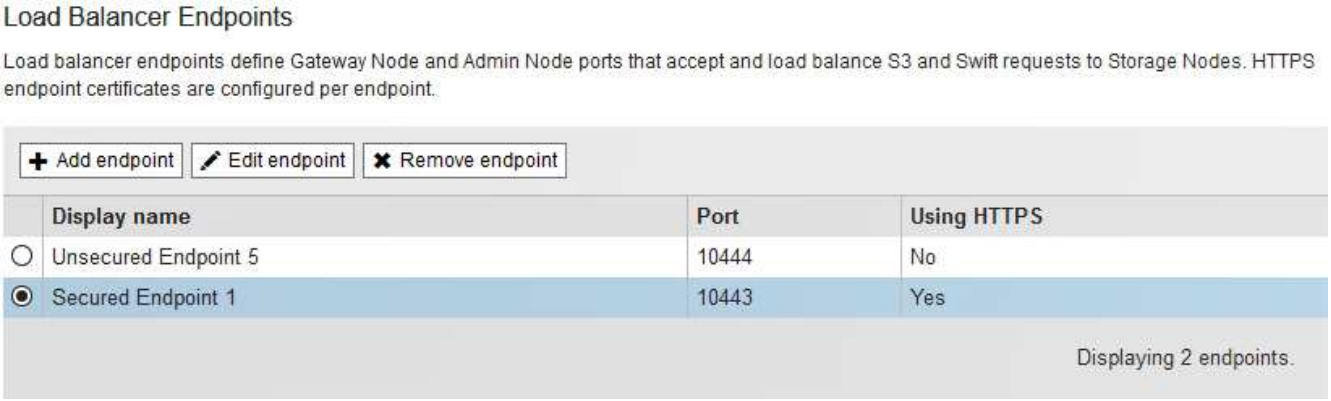
必要なもの

- Root Access 権限が必要です。
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

手順

1. [* Configuration > Network Settings > Load Balancer Endpoints *]を選択します。

   Load Balancer Endpointsページが表示されます。既存のエンドポイントがテーブルに表示されます。



2. 削除するエンドポイントの左側にあるオプションボタンを選択します。

3. [エンドポイントの削除*]をクリックします。

   確認のダイアログボックスが表示されます。

4. [OK] をクリックします。

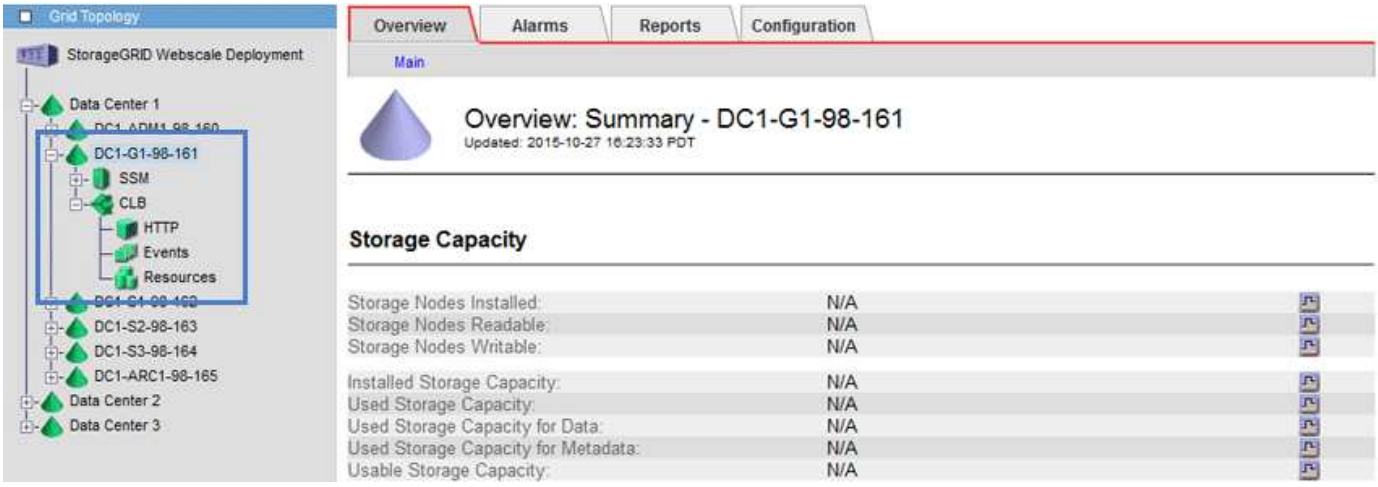
   エンドポイントが削除されます。

ロードバランシングの仕組み **- CLB** サービス

ゲートウェイノード上の Connection Load Balancer （ CLB ）サービスは廃止されました。ロードバランササービスが推奨されるロードバランシングメカニズムになりました。

CLB サービスはレイヤ 4 ロードバランシングを使用して、可用性、システムの負荷、および管理者が設定したリンクコストに基づいて、クライアントアプリケーションからの受信 TCP ネットワーク接続を最適なストレージノードに分散します。最適なストレージノードが選択されると、 CLB サービスは双方向のネットワーク接続を確立し、選択されたノードとの間でトラフィックを転送します。CLB は、受信ネットワーク接続を転送するときにグリッドネットワーク設定を考慮しません。

CLBサービスに関する情報を表示するには、* Support **>** Tools **>** Grid Topology を選択し、 CLB *とその下のオプションを選択できるようになるまでゲートウェイノードを拡張します。



CLB サービスを使用する場合は、 StorageGRID システムのリンクコストを設定することを検討してください。

関連情報

"リンクコストとは"

"リンクコストを更新しています"

信頼されていないクライアントネットワークの管理

クライアントネットワークを使用している場合は、明示的に設定されたエンドポイントでのみインバウンドクライアントトラフィックを受け入れることで、悪意のある攻撃から StorageGRID を保護できます。

デフォルトでは、各グリッドノードのクライアントネットワークは *trusted_* です。つまり、StorageGRID は、使用可能なすべての外部ポートでの各グリッドノードへのインバウンド接続をデフォルトで信頼します（ネットワークガイドラインの外部通信に関する情報を参照）。

各ノードのクライアントネットワークを「 *untrusted_* 」に指定することで、 StorageGRID システムに対する悪意ある攻撃の脅威を軽減できます。ノードのクライアントネットワークが信頼されていない場合、ノードはロードバランサエンドポイントとして明示的に設定されたポートのインバウンド接続だけを受け入れます。

例 **1** ：ゲートウェイノードが **HTTPS S3** 要求のみを受け入れる

ゲートウェイノードで、 HTTPS S3 要求を除くクライアントネットワーク上のすべてのインバウンドトラフィックを拒否するとします。この場合、次の一般的な手順を実行します。

1. Load Balancer Endpoints ページで、ポート 443 で S3 over HTTPS のロードバランサエンドポイントを設定します。
2. Untrusted Client Networks ページで、ゲートウェイ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ことを指定します。

設定を保存すると、ポート 443 での HTTPS S3 要求と ICMP エコー（ ping ）要求を除き、ゲートウェイノードのクライアントネットワーク上のすべてのインバウンドトラフィックが破棄されます。

例 **2** ：ストレージノードが **S3** プラットフォームサービス要求を送信する

あるストレージノードからのアウトバウンド S3 プラットフォームサービストラフィックは有効にするが、クライアントネットワークでそのストレージノードへのインバウンド接続は禁止するとします。この場合は、次の手順を実行します。

- Untrusted Client Networks ページで、ストレージノード上のクライアントネットワークが信頼されていないことを指定します。

設定を保存すると、ストレージノードはクライアントネットワークで受信トラフィックを受け入れなくなりますが、 Amazon Web Services へのアウトバウンド要求は引き続き許可します。

関連情報

"ネットワークガイドライン"

"ロードバランサエンドポイントの設定"

ノードのクライアントネットワークの指定は信頼されていません

クライアントネットワークを使用している場合は、各ノードのクライアントネットワー

クが信頼されているかどうかを指定できます。拡張で追加し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。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限が必要です。
- 管理ノードまたはゲートウェイノードが明示的に設定されたエンドポイントでのみインバウンドトラフィックを受け入れるように設定する場合は、ロードバランサエンドポイントを定義しておきます。

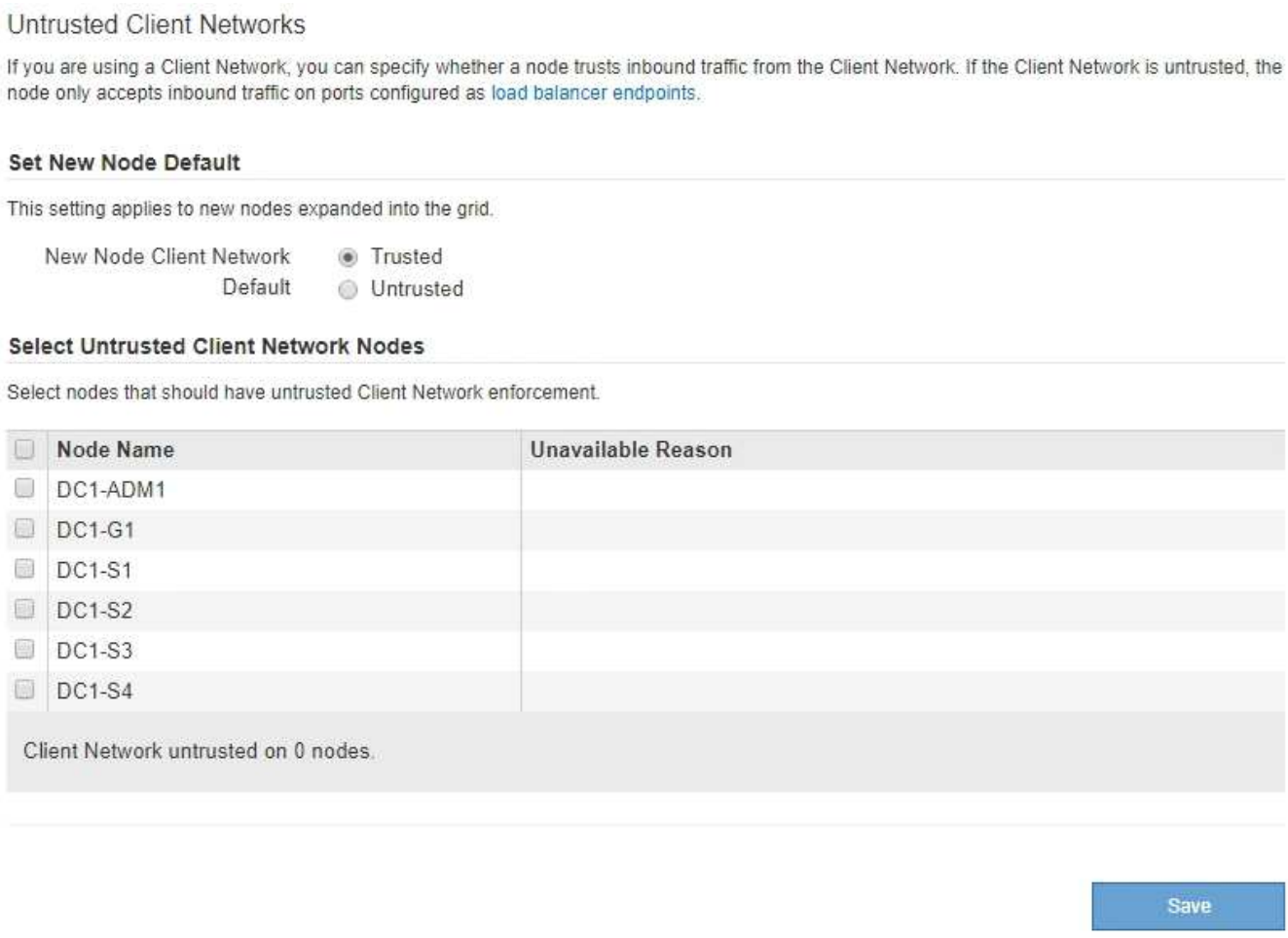
> ロードバランサエンドポイントが設定されていないと、既存のクライアント接続が失敗する可能性があります。

手順

1. 「* Configuration * Network Settings * Untrusted Client Network *」を選択します。

   [Untrusted Client Networks]ページが表示されます。

   このページには、StorageGRID システム内のすべてのノードが表示されます。ノードのクライアントネットワークが信頼されている必要がある場合は、 Unavailable Reason 列にエントリが表示されます。



2. Set New Node Default * セクションで、拡張手順 で新しいノードをグリッドに追加するときのデフォルト設定を指定します。

- * Trusted * ：拡張でノードが追加されるときに、そのクライアントネットワークが信頼されます。
- * Untrusted * ：拡張でノードが追加されるときに、そのクライアントネットワークは信頼されません。必要に応じて、このページに戻って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. Select Untrusted Client Network Nodes * セクションで、明示的に設定されたロードバランサエンドポイントでのみクライアント接続を許可するノードを選択します。

   タイトルのチェックボックスをオンまたはオフにすると、すべてのノードを選択または選択解除できます。

4. [保存（ Save ）] をクリックします。

   新しいファイアウォールルールがすぐに追加され、適用されます。ロードバランサエンドポイントが設定されていないと、既存のクライアント接続が失敗する可能性があります。

関連情報

"ロードバランサエンドポイントの設定"

ハイアベイラビリティグループの管理

ハイアベイラビリティ（HA）グループを使用して、S3 / Swiftクライアントに可用性の高いデータ接続を提供できます。HAグループを使用して、Grid ManagerとTenant Managerへの可用性の高い接続を提供することもできます。

- "HAグループとは"
- "HAグループの使用方法"
- "HA グループの設定オプション"
- "ハイアベイラビリティグループを作成する"
- "ハイアベイラビリティグループの編集"
- "ハイアベイラビリティグループを削除しています"

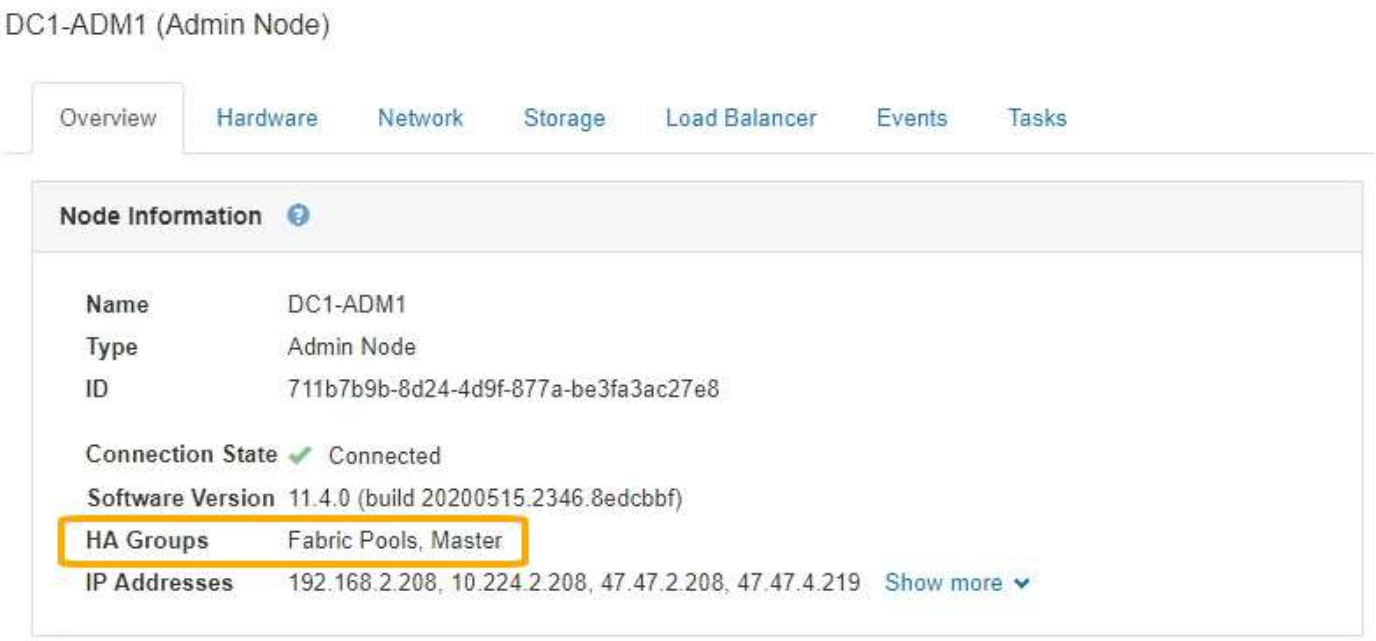
HAグループとは

ハイアベイラビリティグループは、仮想IPアドレス（VIP）を使用してゲートウェイノードまたは管理ノードサービスへのアクティブ/バックアップアクセスを提供します。

HAグループは、管理ノードとゲートウェイノード上の1つ以上のネットワークインターフェイスで構成されます。HAグループを作成するときは、グリッドネットワーク（eth0）またはクライアントネットワーク（eth2）に属するネットワークインターフェイスを選択します。HAグループ内のすべてのインターフェイスは、同じネットワークサブネット内に存在する必要があります。

HAグループは、グループ内のアクティブインターフェイスに追加された仮想IPアドレスを1つ以上維持します。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、仮想IPアドレスは別のインターフェイスに移動します。このフェイルオーバープロセスにかかる時間は通常数秒です。クライアントアプリケーションへの影響はほとんどなく、通常の再試行で処理を続行できます。

HAグループ内のアクティブインターフェイスがマスターに、他のすべてのインターフェイスは、バックアップとして指定されます。これらの指定を表示するには、* Nodes **>*_node_name >** Overview *を選択します。



HAグループを作成する際には、1つのインターフェイスを優先マスターに指定します。優先マスターは、障害が発生してVIPアドレスがバックアップインターフェイスに再割り当てされない限り、アクティブインターフェイスです。障害が解決されると、VIPアドレスは自動的に優先マスターに戻されます。

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停止する。
- インターフェイスが設定されているノードと他のすべてのノードとの接続が少なくとも2分間失われます
- アクティブインターフェイスが停止する。
- ロードバランササービスが停止する。
- ハイアベイラビリティサービスが停止します。

> アクティブインターフェイスをホストするノードの外部でネットワーク障害が発生した場合、フェイルオーバーがトリガーされないことがあります。同様に、 CLB サービス（廃止予定）の障害、またはグリッドマネージャまたはテナントマネージャのサービスの障害によって、フェイルオーバーはトリガーされません。

HAグループに3つ以上のノードのインターフェイスが含まれている場合、フェイルオーバー中にアクティブインターフェイスは他のノードのインターフェイスに移動する可能性があります。

HAグループの使用方法

ハイアベイラビリティ（HA）グループはいくつかの理由で使用できます。

- HA グループは、 Grid Manager または Tenant Manager への可用性の高い管理接続を提供します。
- HA グループは、 S3 / Swift クライアントに可用性の高いデータ接続を提供できます。
- インターフェイスが 1 つしかない HA グループでは、多数の VIP アドレスを指定したり、 IPv6 アドレス

を明示的に設定したりできます。

HA グループは、グループに含まれるすべてのノードが同じサービスを提供する場合にのみ高可用性を提供できます。HA グループを作成するときは、必要なサービスを提供するタイプのノードからインターフェイスを追加してください。

- * 管理ノード * ：ロードバランササービスが含まれ、 Grid Manager またはテナントマネージャへのアクセスを有効にします。
- * ゲートウェイノード * ：ロードバランササービスと CLB サービス（廃止）が含まれます。

HA グループの目的	このタイプのノードを **HA** グループに追加します
Grid Manager へのアクセス	• プライマリ管理ノード（優先マスター） • 非プライマリ管理ノード *注：*プライマリ管理ノードが優先マスターである必要があります。一部のメンテナンス手順は、プライマリ管理ノードでしか実行できません。
Tenant Manager のみにアクセスします	• プライマリ管理ノードまたは非プライマリ管理ノード
S3 または Swift クライアントアクセス - ロードバランササービス	• 管理ノード • ゲートウェイノード
S3 または Swift クライアントアクセス - CLB サービス • 注： * CLB サービスは廃止されました。	• ゲートウェイノード

Grid Manager または **Tenant Manager** で **HA** グループを使用する場合の制限事項

Grid ManagerまたはTenant Managerのサービスで障害が発生しても、HAグループ内でフェイルオーバーはトリガーされません。

フェイルオーバーの発生時に Grid Manager または Tenant Manager にサインインしている場合はサインアウトされるため、再度サインインしてタスクを再開する必要があります。

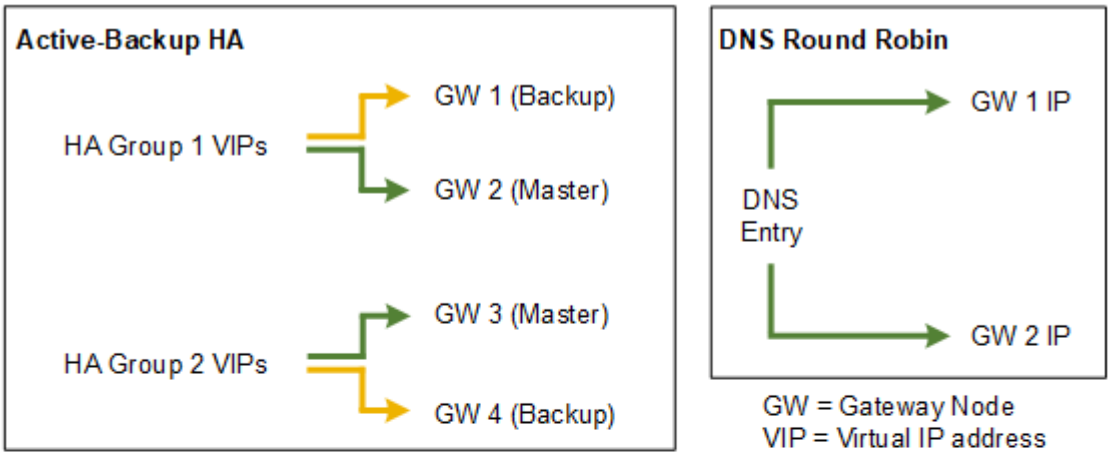
プライマリ管理ノードを使用できない場合は、一部のメンテナンス手順を実行できません。フェイルオーバー中は、 Grid Manager を使用して StorageGRID システムを監視できます。

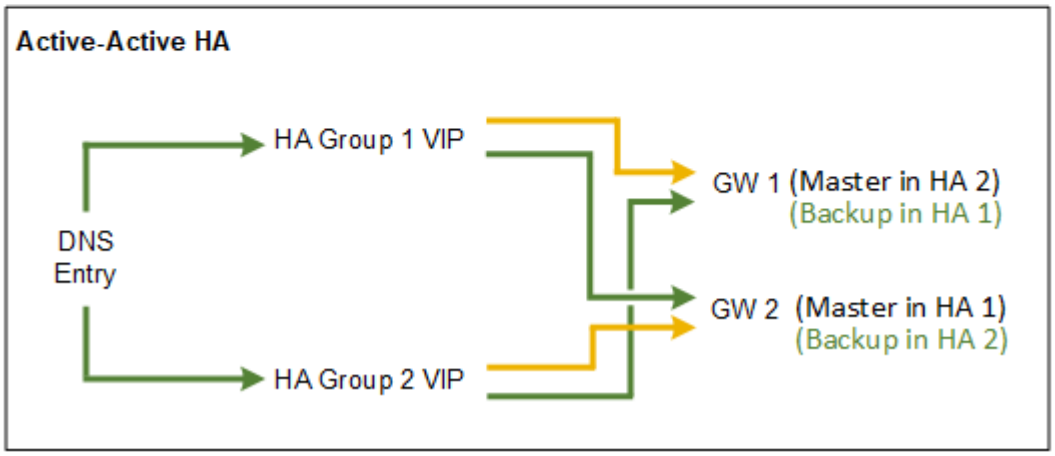
CLB サービスで **HA** グループを使用する場合の制限事項

CLB サービスに障害が発生しても、 HA グループ内でフェイルオーバーはトリガーされません。

CLB サービスは廃止されました。

次の図は、 HA グループのさまざまな構成例を示しています。各オプションには長所と短所があります。





「アクティブ/アクティブHA」の例に示すように、複数の重複するHAグループを作成する場合、合計スループットはノード数とHAグループ数が増えるほど上昇します。ノードとHAグループをそれぞれ3つ以上配置すると、1つのノードをオフラインにする必要があるメンテナンス手順の実行中も、いずれかのVIPを使用して処理を継続できます。

次の表は、図に示す各 HA 構成のメリットをまとめたものです。

設定	利点	欠点
アクティブ / バックアップ HA	• StorageGRID で管理され、外部のコンポーネントを必要としません。 • 高速フェイルオーバー。	• HA グループ内の 1 つのノードだけがアクティブです。各 HA グループで少なくとも 1 つのノードがアイドル状態になります。

設定	利点	欠点
DNS ラウンドロビン	• 総スループットが向上します。 • アイドル状態のホストはありません。	• クライアントの動作によってはフェイルオーバーが低速になる可能性があります。 • StorageGRID の外部でハードウェアを構成する必要があります。 • ユーザによる健全性チェックが必要です。
アクティブ/アクティブ	• トラフィックが複数の HA グループに分散されます。 • HA グループの数が増えるほど総スループットが向上します。 • 高速フェイルオーバー。	• 設定がより複雑になります。 • StorageGRID の外部でハードウェアを構成する必要があります。 • ユーザによる健全性チェックが必要です。

ハイアベイラビリティグループを作成する

1つ以上のハイアベイラビリティ（HA）グループを作成して、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可用性の高いアクセスを提供できます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限が必要です。

このタスクについて

HAグループに追加するインターフェイスは次の条件を満たしている必要があります。

- インターフェイスは、ゲートウェイノードまたは管理ノードのものである必要があります。
- インターフェイスはグリッドネットワーク（eth0）またはクライアントネットワーク（eth2）に属している必要があります。
- インターフェイスには、DHCPではなく固定IPアドレスまたは静的IPアドレスを設定する必要があります。

手順

1. * Configuration > Network Settings > High Availability Groups *を選択します。

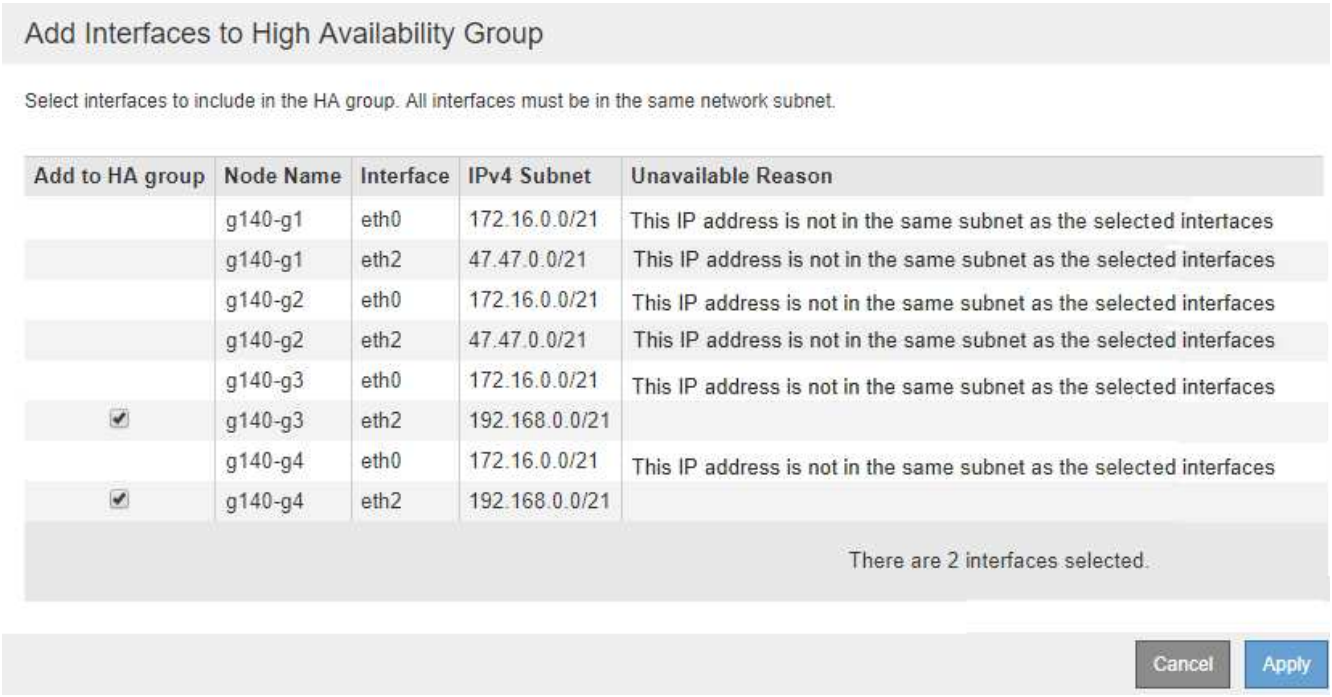
   [High Availability Groups]ページが表示されます。

2. [作成（ Create ）] をクリックします。

   Create High Availability Groupダイアログボックスが表示されます。

3. HAグループの名前を入力し、必要に応じて概要 を入力します。
4. [Select Interfaces]をクリックします。

   Add Interfaces to High Availability Groupダイアログボックスが表示されます。この表には、使用可能なノード、インターフェイス、およびIPv4サブネットが表示されます。



   IPアドレスがDHCPによって割り当てられている場合、インターフェイスはリストに表示されません。

5. Add to HA group *列で、HAグループに追加するインターフェイスのチェックボックスを選択します。

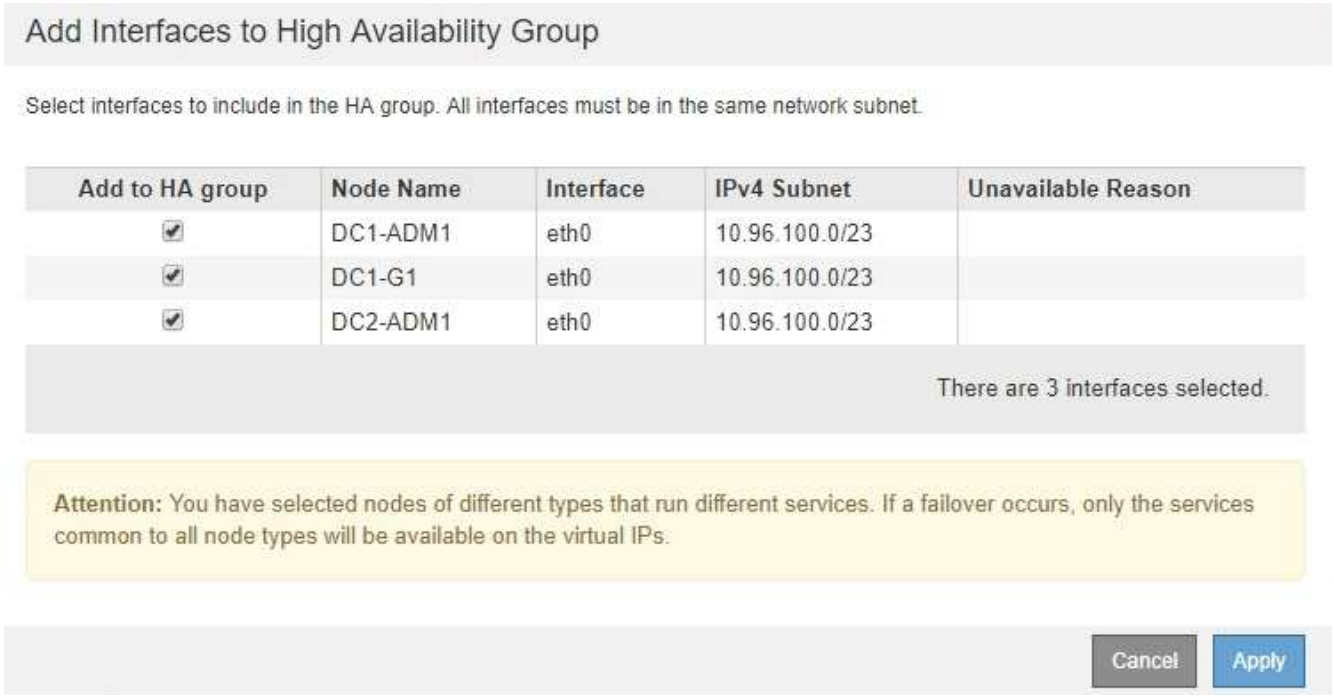
   インターフェイスの選択に関する次のガイドラインに注意してください。

   - インターフェイスを少なくとも 1 つ選択してください。
   - 複数のインターフェイスを選択する場合は、すべてのインターフェイスがグリッドネットワーク（eth0）またはクライアントネットワーク（eth2）上に存在する必要があります。
   - すべてのインターフェイスは、同じサブネット内または共通のプレフィックスを持つサブネット内に存在する必要があります。

IPアドレスは最小のサブネット（最大のプレフィックスを持つサブネット）に制限されます。

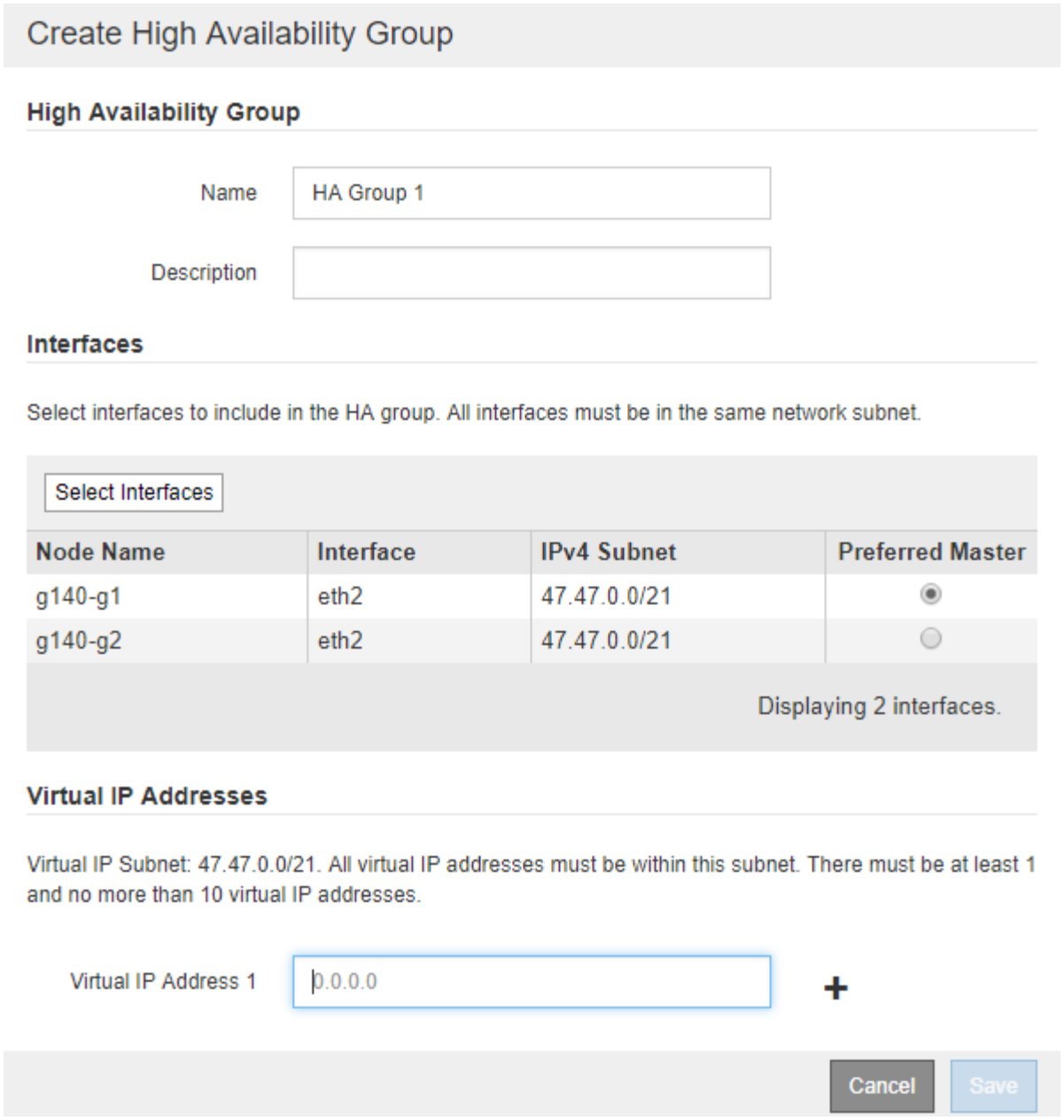
- 異なるタイプのノード上のインターフェイスを選択した場合、フェイルオーバーが発生すると、選択したノードに共通するサービスのみが仮想IPで使用可能になります。
  - Grid ManagerまたはTenant ManagerのHA保護用に2つ以上の管理ノードを選択します。
  - ロードバランササービスのHA保護を利用する場合は、管理ノード、ゲートウェイノード、またはその両方を2つ以上選択します。
  - CLBサービスのHA保護を行うゲートウェイノードを2つ以上選択します。

    CLB サービスは廃止されました。



6. [適用（ Apply ）] をクリックします。

選択したインターフェイスは、Create High Availability GroupページのInterfacesセクションに表示されます。デフォルトでは、リストの最初のインターフェイスが優先マスターとして選択されます。



7. 別のインターフェイスを優先マスターにする場合は、[* Preferred Master*（優先マスター*）]列でそのインターフェイスを選択します。

   優先マスターは、障害が発生してVIPアドレスがバックアップインターフェイスに再割り当てされない限り、アクティブインターフェイスです。

   HAグループがGrid Managerへのアクセスを提供する場合は、プライマリ管理ノード上のインターフェイスを優先マスター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でしか実行できません。

8. ページの仮想IPアドレスセクションに、HAグループの仮想IPアドレスを1~10個入力します。プラス記号（+）をクリックして、複数のIPアドレスを追加します。

   IPv4 アドレスを少なくとも 1 つ指定する必要があります。必要に応じて、追加の IPv4 アドレスと IPv6 アドレスを指定できます。

IPv4アドレスは、すべてのメンバーインターフェイスで共有されるIPv4サブネット内にある必要があります。

9. [保存（ Save ）] をクリックします。

   HA グループが作成され、設定済みの仮想 IP アドレスを使用できるようになります。

関連情報

"Red Hat Enterprise Linux または CentOS をインストールします"

"VMware をインストールする"

"Ubuntu または Debian をインストールします"

"負荷分散の管理"

ハイアベイラビリティグループの編集

ハイアベイラビリティ（HA）グループを編集して、グループ名や概要 を変更したり、インターフェイスを追加または削除したり、仮想IPアドレスを追加または更新したりできます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限が必要です。

このタスクについて

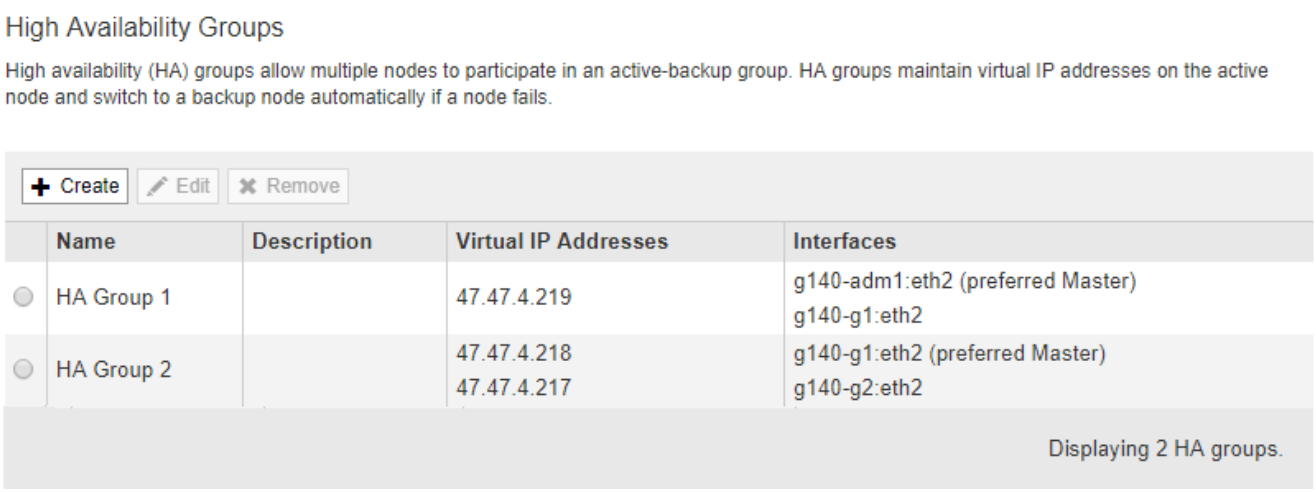
HAグループを編集する理由には、次のようなものがあります。

- 既存のグループにインターフェイスを追加しています。すでにグループに割り当てられている他のインターフェイスと同じサブネット内のインターフェイスのIPアドレスを指定する必要があります。
- HAグループからのインターフェイスの削除たとえば、グリッドネットワークまたはクライアントネットワークのノードのインターフェイスがHAグループで使用されている場合、サイトの開始や手順 のノードの運用停止はできません。

手順

1. * Configuration > Network Settings > High Availability Groups *を選択します。

   [High Availability Groups]ページが表示されます。

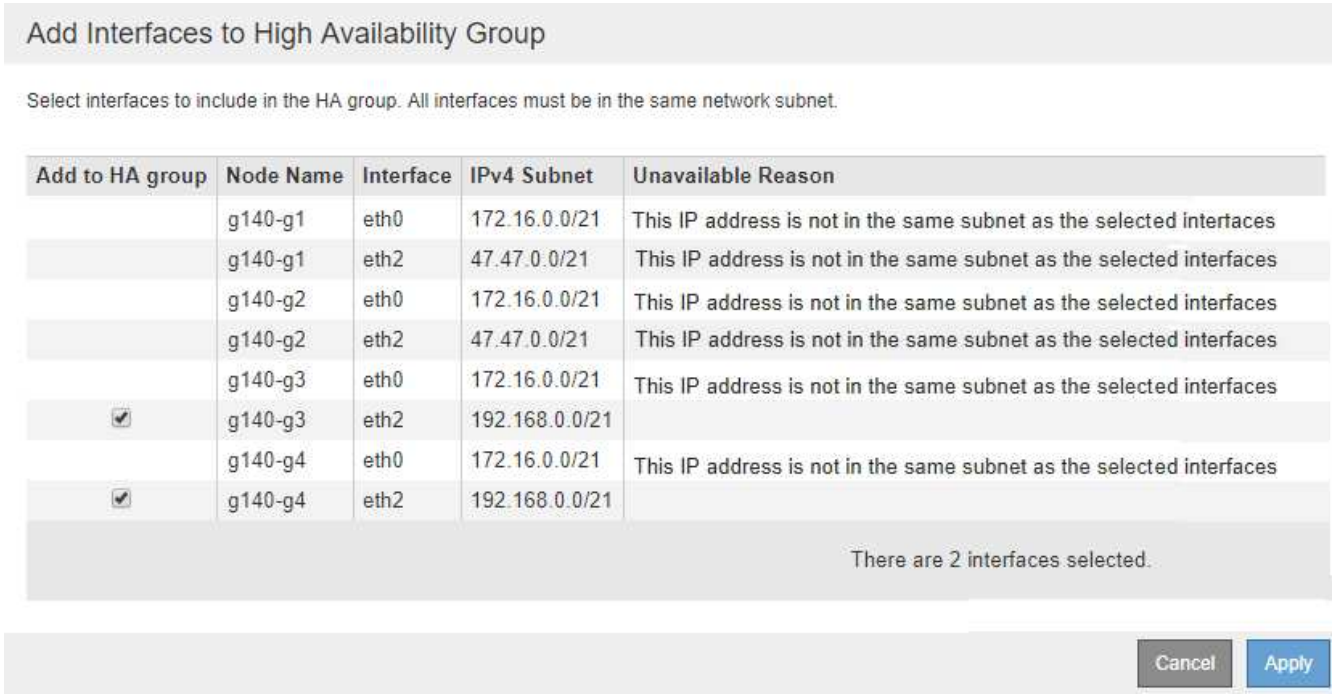


2. 編集するHAグループを選択し、* Edit *をクリックします。

   Edit High Availability Groupダイアログボックスが表示されます。

3. 必要に応じて、グループの名前または概要 を更新します。
4. 必要に応じて、* Select interfaces *をクリックして、HAグループのインターフェイスを変更します。

   Add Interfaces to High Availability Groupダイアログボックスが表示されます。



   IPアドレスがDHCPによって割り当てられている場合、インターフェイスはリストに表示されません。

5. チェックボックスをオンまたはオフにして、インターフェイスを追加または削除します。

   インターフェイスの選択に関する次のガイドラインに注意してください。

   ◦ インターフェイスを少なくとも 1 つ選択してください。

- 複数のインターフェイスを選択する場合は、すべてのインターフェイスがグリッドネットワーク（eth0）またはクライアントネットワーク（eth2）上に存在する必要があります。
- すべてのインターフェイスは、同じサブネット内または共通のプレフィックスを持つサブネット内に存在する必要があります。

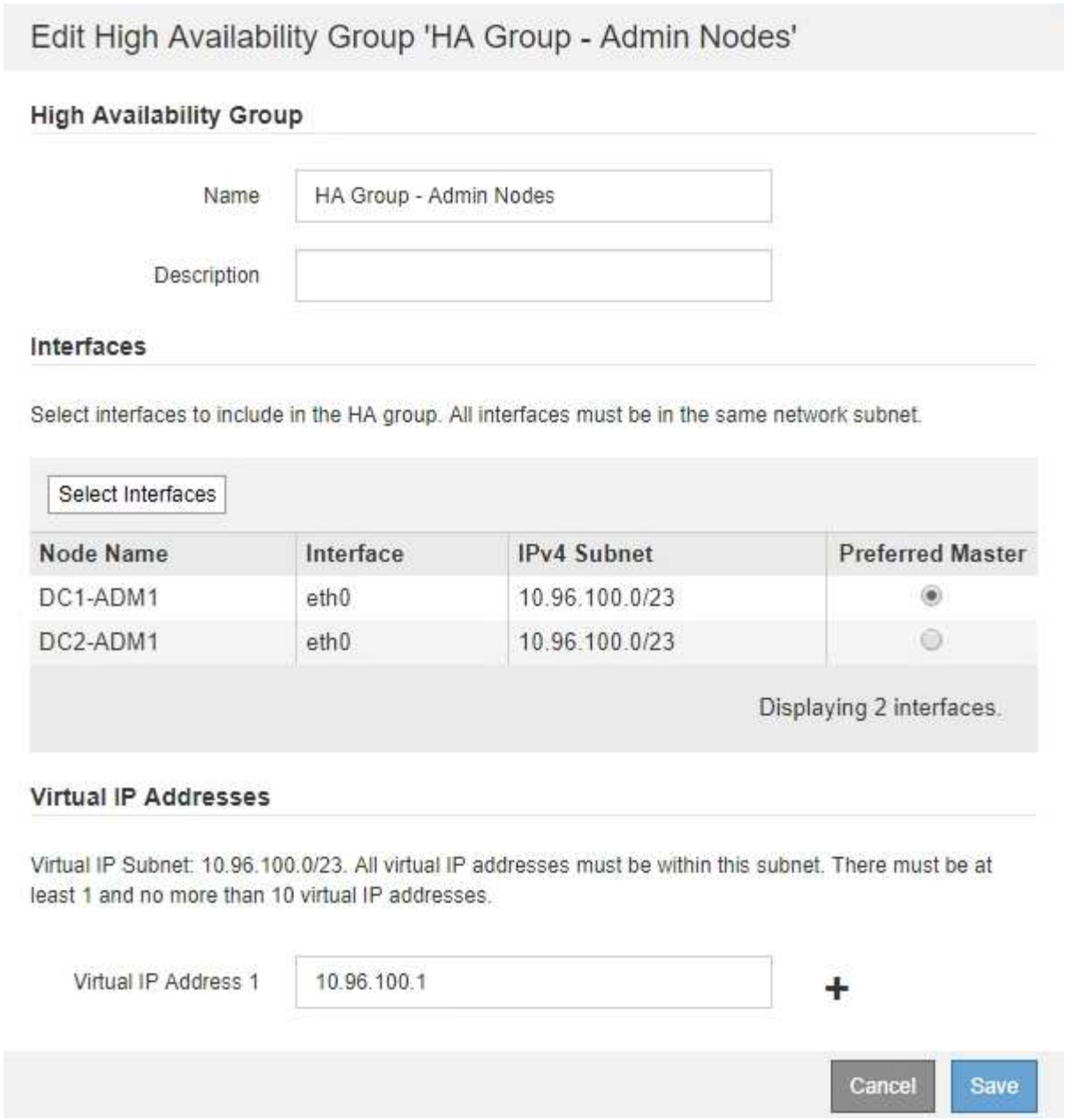
  IPアドレスは最小のサブネット（最大のプレフィックスを持つサブネット）に制限されます。

- 異なるタイプのノード上のインターフェイスを選択した場合、フェイルオーバーが発生すると、選択したノードに共通するサービスのみが仮想IPで使用可能になります。
  - Grid ManagerまたはTenant ManagerのHA保護用に2つ以上の管理ノードを選択します。
  - ロードバランササービスのHA保護を利用する場合は、管理ノード、ゲートウェイノード、またはその両方を2つ以上選択します。
  - CLBサービスのHA保護を行うゲートウェイノードを2つ以上選択します。

    CLB サービスは廃止されました。

6. [適用（ Apply ）] をクリックします。

   選択したインターフェイスがページのインターフェイスセクションに表示されます。デフォルトでは、リストの最初のインターフェイスが優先マスターとして選択されます。



7. 別のインターフェイスを優先マスターにする場合は、[* Preferred Master*（優先マスター*）]列でそのインターフェイスを選択します。

   優先マスターは、障害が発生してVIPアドレスがバックアップインターフェイスに再割り当てされない限り、アクティブインターフェイスです。

   HAグループがGrid Managerへのアクセスを提供する場合は、プライマリ管理ノード上のインターフェイスを優先マスター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でしか実行できません。

8. 必要に応じて、HAグループの仮想IPアドレスを更新します。

   IPv4 アドレスを少なくとも 1 つ指定する必要があります。必要に応じて、追加の IPv4 アドレスと IPv6 アドレスを指定できます。

   IPv4アドレスは、すべてのメンバーインターフェイスで共有されるIPv4サブネット内にある必要がありま

す。

9. [保存（ Save ）] をクリックします。

   HAグループが更新されました。

ハイアベイラビリティグループを削除しています

使用しなくなったハイアベイラビリティ（HA）グループを削除できます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限が必要です。

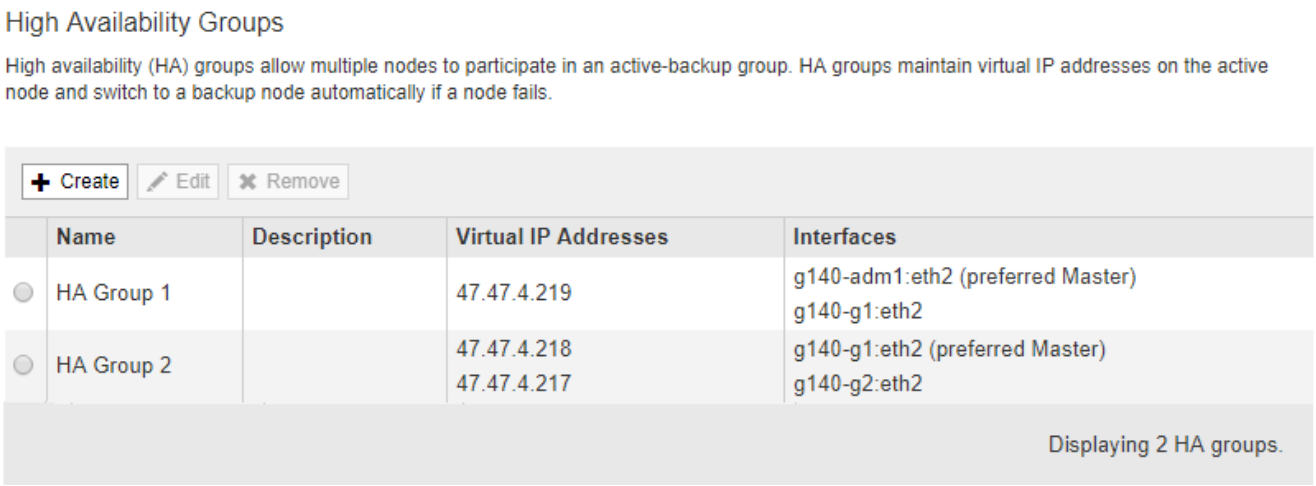
このタスクを実行します

HAグループを削除すると、そのグループのいずれかの仮想IPアドレスを使用するように設定されているS3またはSwiftクライアントはStorageGRID に接続できなくなります。クライアントの停止を回避するには、該当するS3またはSwiftクライアントアプリケーションをすべて更新してからHAグループを削除する必要があります。各クライアントを更新して、別のIPアドレスを使用して接続します。たとえば、別のHAグループの仮想IPアドレスや、インストール時またはDHCPを使用してインターフェイスに設定されたIPアドレスなどです。

手順

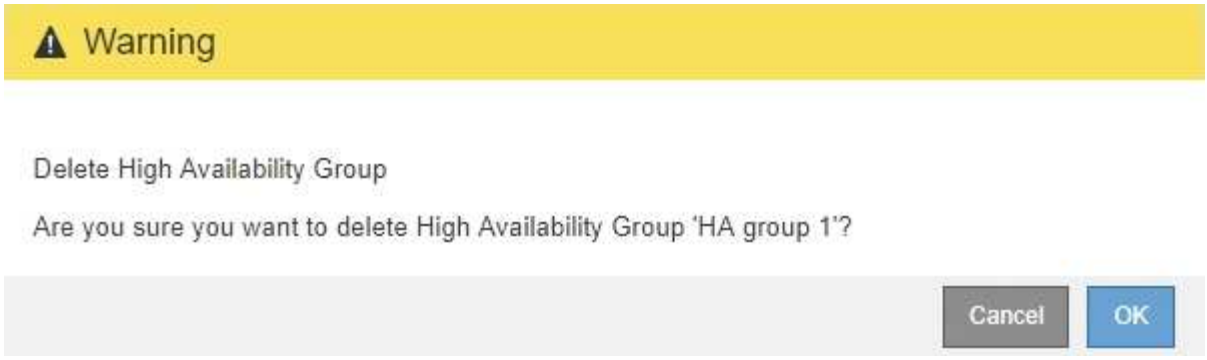
1. * Configuration > Network Settings > High Availability Groups *を選択します。

   [High Availability Groups]ページが表示されます。



2. 削除するHAグループを選択し、* Remove *をクリックします。

   Delete High Availability Groupという警告が表示されます。



3. [OK] をクリックします。

   HAグループが削除されます。

S3 APIエンドポイントのドメイン名を設定しています

S3 仮想ホスト形式の要求をサポートするには、 Grid Manager を使用して、 S3 クライアントの接続先となるエンドポイントのドメイン名のリストを設定する必要があります。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。
- グリッドのアップグレードが進行中でないことを確認しておく必要があります。

  ドメイン名の設定は、グリッドのアップグレードの進行中は変更しないでください。

このタスクについて

クライアントがS3エンドポイントのドメイン名を使用できるようにするには、次の作業をすべて実行する必要があります。

- Grid Manager を使用して、 S3 エンドポイントのドメイン名を StorageGRID システムに追加します。
- クライアントが StorageGRID への HTTPS 接続に使用する証明書が、クライアントが必要とするすべてのドメイン名に対して署名されていることを確認します。

  たとえば、エンドポイントがの場合などです `s3.company.com`、HTTPS接続に使用する証明書にが含まれていることを確認する必要があります `s3.company.com` エンドポイントとエンドポイントのワイルドカードSubject Alternative Name（SAN）： `*.s3.company.com`。

- クライアントが使用する DNS サーバを設定します。クライアントが接続に使用する IP アドレスの DNS レコードを含め、ワイルドカード名を含む必要なすべてのエンドポイントドメイン名をレコードが参照するようにします。

クライアントは、ゲートウェイノード、管理ノード、またはストレージノードの IP アドレスを使用するか、ハイアベイラビリティグループの仮想 IP アドレスに接続することで、StorageGRID に接続できます。DNS レコードに正しい IP アドレスを追加するためには、クライアントアプリケーションがグリッドに接続する方法を理解しておく必要があります。

クライアントがHTTPS接続に使用する証明書は、クライアントがグリッドに接続する方法によって異なります。

- ロードバランササービスを使用して接続する場合、クライアントは特定のロードバランサエンドポイント用の証明書を使用します。

  各ロードバランサエンドポイントには独自の証明書があり、異なるエンドポイントドメイン名を認識するように各エンドポイントを設定できます。

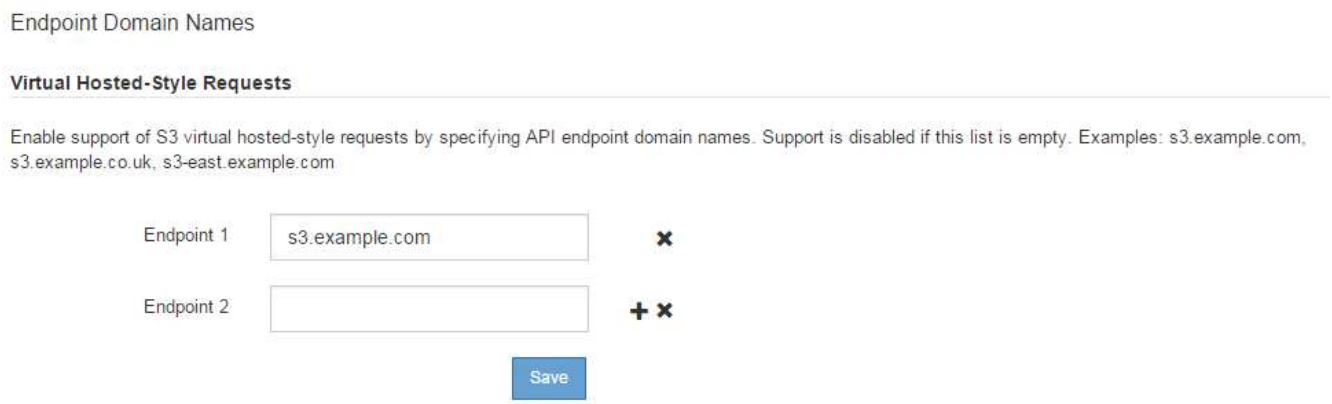
- クライアントがストレージノードまたはゲートウェイノード上のCLBサービスに接続する場合、クライアントは、必要なエンドポイントのドメイン名をすべて追加して更新されたグリッドのカスタムサーバ証明書を使用します。

  CLB サービスは廃止されました。

手順

1. [環境設定]>[ネットワーク設定]>[ドメイン名]を選択します。

   [Endpoint Domain Names] ページが表示されます。



2. （+）アイコンを使用してフィールドを追加し、* Endpoint *フィールドにS3 APIエンドポイントのドメイン名のリストを入力します。

   このリストが空の場合、 S3 仮想ホスト形式の要求のサポートは無効になります。

3. [保存（ Save ）] をクリックします。
4. クライアントが使用するサーバ証明書が、必要なエンドポイントのドメイン名と一致していることを確認します。
   - ロードバランササービスを使用するクライアントの場合は、クライアントが接続するロードバランサエンドポイントに関連付けられている証明書を更新します。

◦ ストレージノードに直接接続するクライアント、またはゲートウェイノード上のCLBサービスを使用するクライアントの場合は、グリッドのカスタムサーバ証明書を更新します。

5. エンドポイントのドメイン名要求を解決するために必要な DNS レコードを追加します。

結果

これで、クライアントがエンドポイントを使用するようになります `bucket.s3.company.com`を指定すると、DNSサーバが正しいエンドポイントに解決され、証明書がエンドポイントを認証します。

関連情報

"S3 を使用する"

"IPアドレスを表示しています"

"ハイアベイラビリティグループを作成する"

"ストレージノードまたはCLBサービスへの接続用のカスタムサーバ証明書を設定する"

"ロードバランサエンドポイントの設定"

クライアント通信での**HTTP**の有効化

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すべての接続、またはゲートウェイノード上の廃止された CLB サービスへのすべての接続に、HTTPS ネットワークプロトコルを使用します。非本番環境のグリッドのテストなどの目的で、これらの接続に対して HTTP を有効にすることもできます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

このタスクについて

S3 / Swift クライアントがストレージノードへの HTTP 接続を直接確立する必要がある場合、またはゲートウェイノード上の廃止された CLB サービスへの HTTP 接続を確立する必要がある場合にのみ、このタスクを実行します。

HTTPS 接続のみを使用するクライアント、またはロードバランササービスに接続するクライアントでは、（各ロードバランサエンドポイントで HTTP または HTTPS を使用するように設定できるため）このタスクを実行する必要はありません。詳細については、ロードバランサエンドポイントの設定に関する情報を参照してください。

を参照してください "Summary ：クライアント接続の IP アドレスとポート" ストレージノードへの接続時、または HTTP または HTTPS を使用して廃止された CLB サービスへの接続時に使用するポート S3 および Swift クライアントを取得する

> 要求が暗号化されずに送信されるため、本番環境のグリッドで HTTP を有効にする場合は注意してください。

手順

1. 「環境設定*システム設定*グリッドオプション*」を選択します。

2. [ネットワークオプション] セクションで、 [* HTTP 接続を有効にする *] チェックボックスをオンにします。

3. [保存（ Save ）] をクリックします。

関連情報

"ロードバランサエンドポイントの設定"

"S3 を使用する"

"Swift を使用します"

許可するクライアント処理の制御

PreventClientModification グリッドオプションを選択して、特定の HTTP クライアント処理を拒否することができます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

このタスクについて

クライアント変更の禁止は、システム全体の設定です。[クライアント変更を禁止する] オプションを選択すると、次の要求が拒否されます。

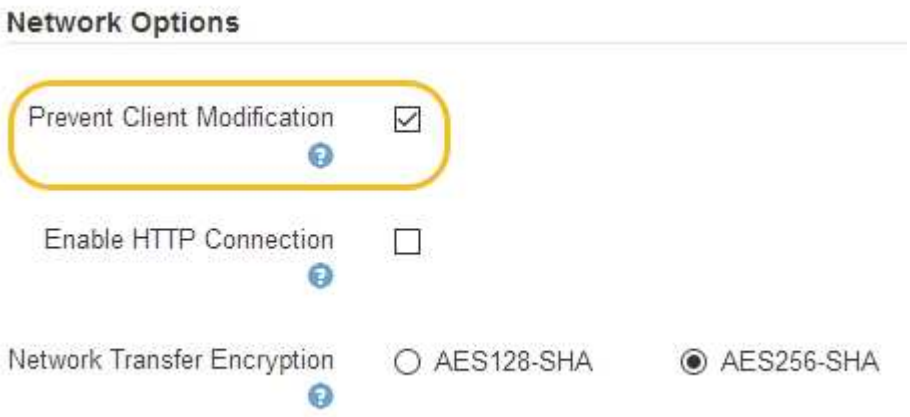
- * S3 REST API *
  - バケットの削除要求
  - 既存オブジェクトのデータ、ユーザ定義メタデータ、または S3 オブジェクトのタグを変更するすべての要求

> この設定は、バージョン管理が有効なバケットには適用されません。バージョン管理によって、すでにオブジェクトデータ、ユーザ定義メタデータ、オブジェクトのタグを変更できないようになっています。

- * Swift REST API *
  - コンテナの削除要求
  - 既存のオブジェクトを変更する要求。たとえば、 Put Overwrite 、 Delete 、 Metadata Update などの処理が拒否されます。

手順

1. 「環境設定*システム設定*グリッドオプション*」を選択します。
2. [ネットワークオプション] セクションで、 [クライアントの変更を禁止する *] チェックボックスをオンにします。



3. [保存（ Save ）] をクリックします。

StorageGRID ネットワークと接続の管理

グリッドマネージャを使用して、 StorageGRID のネットワークと接続を設定および管理できます。

を参照してください "S3およびSwiftクライアント接続の設定" を参照して、 S3 または Swift クライアントを接続する方法を確認してください。

- "StorageGRID ネットワークのガイドライン"
- "IPアドレスを表示しています"
- "発信 TLS 接続でサポートされる暗号"
- "ネットワーク転送の暗号化の変更"
- "サーバ証明書の設定"
- "ストレージプロキシを設定しています"
- "管理プロキシの設定"
- "トラフィック分類ポリシーの管理"
- "リンクコストとは"

StorageGRID ネットワークのガイドライン

StorageGRID では、グリッドノードあたり最大 3 つのネットワークインターフェイスがサポートされ、各グリッドノードのネットワークをセキュリティやアクセスの要件に応じて設定することができます。

グリッドノードのネットワークを変更または追加するには、リカバリとメンテナンスの手順を参照してください。ネットワークトポロジの詳細については、ネットワークの手順を参照してください。

Grid ネットワーク

必須グリッドネットワークは、すべての内部 StorageGRID トラフィックに使用されます。このネットワークによって、グリッド内のすべてのノードが、すべてのサイトおよびサブネットにわたって相互に接続されます。

管理ネットワーク

任意。通常、管理ネットワークはシステムの管理とメンテナンスに使用されます。クライアントプロトコルアクセスにも使用できます。管理ネットワークは通常はプライベートネットワークであり、サイト間でルーティング可能にする必要はありません。

クライアントネットワーク

任意。クライアントネットワークはオープンネットワークで、主に S3 および Swift クライアントアプリケーションへのアクセスに使用されます。そのため、グリッドネットワークを分離してセキュリティを確保できます。クライアントネットワークは、ローカルゲートウェイ経由でアクセス可能なすべてのサブネットと通信できます。

ガイドライン

- 各 StorageGRID グリッドノードには、割り当て先のネットワークごとに専用のネットワークインターフェイス、 IP アドレス、サブネットマスク、およびゲートウェイが必要です。
- 1 つのグリッドノードに複数のインターフェイスを設定することはできません。
- 各ネットワークのグリッドノードごとに、単一のゲートウェイがサポートされます。このゲートウェイはノードと同じサブネット上に配置する必要があります。必要に応じて、より複雑なルーティングをゲートウェイに実装できます。
- 各ノードでは、各ネットワークが特定のネットワークインターフェイスにマッピングされます。

ネットワーク	インターフェイス名
グリッド（ Grid ）	eth0
管理（オプション）	Eth1
クライアント（オプション）	eth2

- ノードが StorageGRID アプライアンスに接続されている場合は、ネットワークごとに特定のポートが使用されます。詳細については、使用しているアプライアンスのインストール手順を参照してください。
- デフォルトルートはノードごとに自動的に生成されます。eth2 が有効な場合、 0.0.0.0/0 は eth2 のクライアントネットワークを使用します。eth2 が無効な場合、 0.0.0.0/0 は eth0 のグリッドネットワークを使用します。
- クライアントネットワークは、グリッドノードがグリッドに参加するまで動作状態になりません
- グリッドが完全にインストールされる前にインストールユーザインターフェイスにアクセスできるよう

に、グリッドノード導入時に管理ネットワークを設定できます。

関連情報

""

"ネットワークガイドライン"

IPアドレスを表示しています

StorageGRID システムの各グリッドノードの IP アドレスを表示できます。コマンドラインでこの IP アドレスを使用して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。

必要なもの

Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

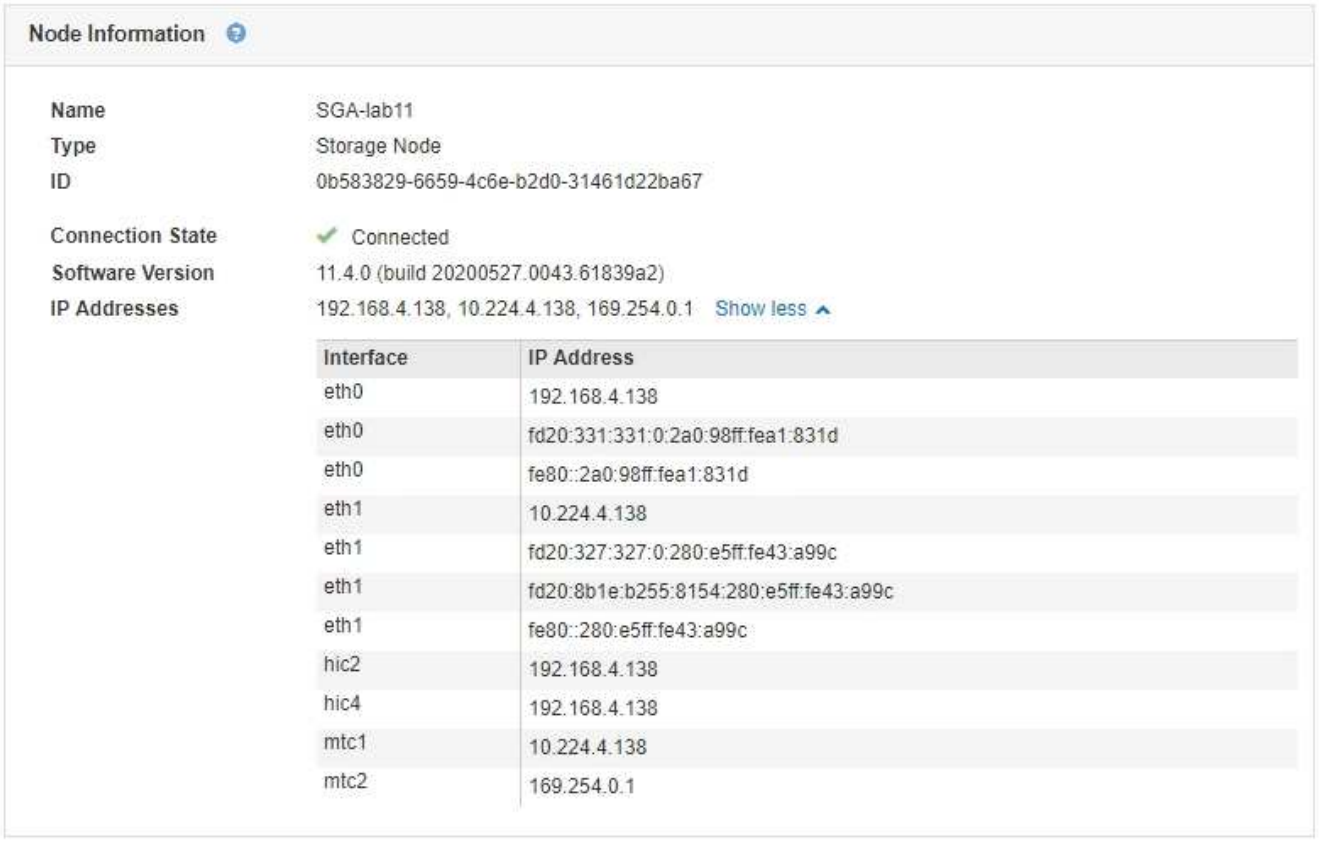
このタスクについて

IPアドレス変更の詳細については、リカバリおよびメンテナンスの手順を参照してください。

手順

1. ノード*>**grid node**>* Overview *を選択します。
2. [IP Addresses]のタイトルの右にある[**Show More**]をクリックします。

   このグリッドノードの IP アドレスがテーブルに表示されます。



関連情報

""

発信 **TLS** 接続でサポートされる暗号

StorageGRID システムでは、アイデンティティフェデレーションとクラウドストレージプールに使用される外部システムへの Transport Layer Security （ TLS ）接続でサポートされる暗号スイートに制限があります。

サポートされる **TLS** のバージョン

StorageGRID では、アイデンティティフェデレーションとクラウドストレージプールに使用される外部システムへの接続で TLS 1.2 と TLS 1.3 がサポートされます。

外部システムとの互換性を確保するために、外部システムとの使用がサポートされている TLS 暗号が選択されています。S3 または Swift クライアントアプリケーションで使用できる暗号のリストは、このリストよりも大容量です。

> プロトコルのバージョン、暗号、鍵交換アルゴリズム、 MAC アルゴリズムなどの TLS 設定オプションは、 StorageGRID では設定できません。これらの設定について具体的なご要望がある場合は、ネットアップのアカウント担当者にお問い合わせください。

サポートされている **TLS 1.2** 暗号スイート

次の TLS 1.2 暗号スイートがサポートされています。

- TLS_ECDHE_RSA_With _AES_128_GCM_SHA256
- TLS_ECDHE_RSA_with _AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_With _AES_128_GG_SHA256
- TLS_ECDHE_ECDSA_With _AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305
- TLS_RSA_With _AES_128_GCM _SHA256
- TLS_RSA_With _AES_256_GCM_SHA384

サポートされている **TLS 1.3** 暗号スイート

次の TLS 1.3 暗号スイートがサポートされています。

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM _SHA256

ネットワーク転送の暗号化の変更

StorageGRID システムでは、 Transport Layer Security （ TLS ）を使用して、グリッドノード間の内部制御トラフィックを保護します。Network Transfer Encryption オプショ

ンは、グリッドノード間の制御トラフィックを暗号化するために TLS で使用されるアルゴリズムを設定します。この設定はデータ暗号化には影響しません。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

このタスクについて

デフォルトでは、ネットワーク転送の暗号化には AES256-SHA アルゴリズムが使用されます。AES128-SHA アルゴリズムを使用して暗号化することもできます。

手順

1. 「環境設定*システム設定*グリッドオプション*」を選択します。
2. ネットワークオプションセクションで、ネットワーク転送の暗号化を * AES128-SHA * または * AES256-SHA * （デフォルト）に変更します。

3. [保存（ Save ）] をクリックします。

サーバ証明書の設定

StorageGRID システムで使用されるサーバ証明書をカスタマイズできます。

StorageGRID システムは、用途が異なる複数のセキュリティ証明書を使用します。

- 管理インターフェイスのサーバ証明書：Grid Manager、Tenant Manager、Grid管理API、およびテナント管理APIへのアクセスを保護するために使用します。
- ストレージAPIのサーバ証明書：ストレージノードおよびゲートウェイノードへのアクセスを保護するために使用します。これらのノードは、APIクライアントアプリケーションがオブジェクトデータをアップロードおよびダウンロードするために使用します。

インストール時に作成されたデフォルトの証明書を使用できるほか、デフォルトの証明書のいずれか、または両方を独自のカスタム証明書に置き換えることもできます。

サポートされているカスタムサーバ証明書のタイプ

StorageGRID システムでは、RSAまたはECDSA（Elliptic Curve Digital Signature Algorithm）で暗号化されたカスタムサーバ証明書がサポートされます。

StorageGRID でREST APIのクライアント接続を保護する方法の詳細については、S3またはSwiftの実装ガイドを参照してください。

ロードバランサエンドポイントの証明書

StorageGRID では、ロードバランサエンドポイントに使用する証明書は別に管理されます。ロードバランサ証明書を設定するには、ロードバランサエンドポイントの設定手順を参照してください。

関連情報

"S3 を使用する"

"Swift を使用します"

"ロードバランサエンドポイントの設定"

Grid Managerおよび**Tenant Manager**用のカスタムサーバ証明書を設定する

デフォルトの StorageGRID サーバ証明書を単一のカスタムサーバ証明書に置き換えると、ユーザがグリッドマネージャとテナントマネージャにアクセスする際にセキュリティの警告が表示されなくなります。

このタスクについて

デフォルトでは、管理ノードごとに、グリッド CA によって署名された証明書が 1 つずつ発行されます。これらの CA 署名証明書は、単一の共通するカスタムサーバ証明書および対応する秘密鍵で置き換えることができます。

1つのカスタムサーバ証明書がすべての管理ノードに対して使用されるため、Grid ManagerおよびTenant Managerへの接続時にクライアントがホスト名を確認する必要がある場合は、ワイルドカード証明書またはマルチドメイン証明書として指定する必要があります。グリッド内のすべての管理ノードに一致するカスタム証明書を定義してください。

設定はサーバ上で行う必要があります。また、使用しているルート認証局（CA）によっては、ユーザがGrid ManagerおよびTenant Managerへのアクセスに使用するWebブラウザにルートCA証明書をインストールすることも必要になります。

サーバ証明書の問題によって処理が中断されないようにするために、このサーバ証明書の有効期限が近づくと、Expiration of server certificate for Management Interface アラートと**Legacy Management Interface Certificate Expiry**（**MCEP**）アラームの両方がトリガーされます。必要に応じて、 Support **>** Tools **>** Grid Topology を選択することにより、現在のサービス証明書が期限切れになるまでの日数を表示できます。次に、「***_ primary Admin Node_***>* CMN **>** Resources *」を選択します。

IP アドレスではなくドメイン名を使用して Grid Manager または Tenant Manager にアクセスする場合は、次のいずれかの場合に証明書のエラーが表示され、バイパスするオプションはありません。

- カスタム管理インターフェイスサーバ証明書の有効期限が切れます。
- カスタムの管理インターフェイスサーバ証明書をデフォルトのサーバ証明書に戻した場合。

手順

1. [* Configuration **]>[** Network Settings **]>[** Server Certificates*]を選択します。
2. Management Interface Server Certificateセクションで、* Install Custom Certificate *をクリックします。

3. 必要なサーバ証明書ファイルをアップロードします。
   - サーバー証明書：カスタムサーバー証明書ファイル（`.crt`）。
   - * Server Certificate Private Key *：カスタムサーバ証明書の秘密鍵ファイル（`.key`）。

     EC 秘密鍵は 224 ビット以上である必要があります。RSA 秘密鍵は 2048 ビット以上にする必要があります。

   - **CA Bundle**：各中間発行認証局（CA）の証明書を含む単一のファイル。このファイルには、 PEM でエンコードされた各 CA 証明書ファイルが、証明書チェーンの順序で連結して含まれている必要があります。
4. [保存（ Save ）] をクリックします。

   以降すべての新しいクライアント接続には、カスタムサーバ証明書が使用されます。

   タブを選択して、デフォルトのStorageGRID サーバ証明書またはアップロードされたCA署名証明書に関する詳細情報を表示します。

   新しい証明書をアップロードしたあと、関連する証明書の有効期限アラート（またはレガシーアラーム）がクリアされるまでに最大1日かかります。

5. Web ブラウザが更新されたことを確認するには、ページをリフレッシュしてください。

Grid Managerおよび**Tenant Manager**用のデフォルトのサーバ証明書のリストア

Grid ManagerおよびTenant Managerでデフォルトのサーバ証明書を使用するように戻すことができます。

手順

1. [* Configuration **]>[** Network Settings **]>[** Server Certificates*]を選択します。
2. Manage Interface Server Certificateセクションで、* Use Default Certificates *をクリックします。
3. 確認ダイアログボックスで * OK * をクリックする。

   デフォルトのサーバ証明書をリストアすると、設定したカスタムサーバ証明書ファイルは削除され、システムからはリカバリできなくなります。以降すべての新しいクライアント接続には、デフォルトのサーバ証明書が使用されます。

4. Web ブラウザが更新されたことを確認するには、ページをリフレッシュしてください。

ストレージノードまたは**CLB**サービスへの接続用のカスタムサーバ証明書を設定する

ストレージノードまたはゲートウェイノード上のCLBサービス（廃止）へのS3またはSwiftクライアント接続に使用するサーバ証明書は、置き換えることができます。置き換え用のカスタムサーバ証明書は組織に固有のものです。

このタスクについて

デフォルトでは、すべてのストレージノードに、グリッド CA によって署名された X.509 サーバ証明書が発行されます。これらの CA 署名証明書は、単一の共通するカスタムサーバ証明書および対応する秘密鍵で置き

換えることができます。

1 つのカスタムサーバ証明書がすべてのストレージノードに対して使用されるため、ストレージエンドポイントへの接続時にクライアントがホスト名を確認する必要がある場合は、ワイルドカード証明書またはマルチドメイン証明書として指定する必要があります。グリッド内のすべてのストレージノードに一致するカスタム証明書を定義してください。

サーバでの設定が完了したら、使用しているルート認証局（CA）によっては、ユーザがシステムへのアクセスに使用するS3またはSwift APIクライアントにルートCA証明書をインストールすることも必要になる場合があります。

> サーバ証明書の問題によって処理が中断されないようにするために、Expiration of server certificate for Storage API Endpoints アラートと、ルートサーバ証明書の有効期限が近づくと従来の**Storage API Service Endpoints Certificate Expiry**（**SCEP**）アラームの両方がトリガーされます。必要に応じて、「 Support **Tools * Grid Topology *** 」を選択することにより、現在のサービス証明書が期限切れになるまでの日数を表示できます。次に、「***_ primary Admin Node_** CMN * Resources *」を選択します。

カスタム証明書は、クライアントがゲートウェイノード上の廃止されたCLBサービスを使用してStorageGRIDに接続する場合、またはクライアントがストレージノードに直接接続する場合にのみ使用されます。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を使用してStorageGRID に接続するS3またはSwiftクライアントは、ロードバランサエンドポイント用に設定された証明書を使用します。

> *ロードバランサエンドポイント証明書の有効期限*アラートは、まもなく期限切れになるロードバランサエンドポイントに対してトリガーされます。

手順

1. [* Configuration **]>[** Network Settings **]>[** Server Certificates*]を選択します。
2. Object Storage API Service Endpoints Server Certificateセクションで、* Install Custom Certificate *をクリックします。
3. 必要なサーバ証明書ファイルをアップロードします。
   - サーバー証明書：カスタムサーバー証明書ファイル（`.crt`）。
   - * Server Certificate Private Key *：カスタムサーバ証明書の秘密鍵ファイル（`.key`）。

     > EC 秘密鍵は 224 ビット以上である必要があります。RSA 秘密鍵は 2048 ビット以上にする必要があります。

   - **CA Bundle**：各中間発行認証局（CA）の証明書を含む単一のファイル。このファイルには、 PEM でエンコードされた各 CA 証明書ファイルが、証明書チェーンの順序で連結して含まれている必要があります。
4. [保存（ Save ）] をクリックします。

   以降すべての新しいAPIクライアント接続には、カスタムサーバ証明書が使用されます。

   タブを選択して、デフォルトのStorageGRID サーバ証明書またはアップロードされたCA署名証明書に関する詳細情報を表示します。

新しい証明書をアップロードしたあと、関連する証明書の有効期限アラート（またはレガシーアラーム）がクリアされるまでに最大1日かかります。

5. Web ブラウザが更新されたことを確認するには、ページをリフレッシュしてください。

関連情報

"S3 を使用する"

"Swift を使用します"

"S3 APIエンドポイントのドメイン名を設定しています"

S3および**Swift**の**REST API**エンドポイント用のデフォルトサーバ証明書のリストア

S3およびSwiftのREST APIエンドポイント用のデフォルトサーバ証明書を使用する設定に戻すことができます。

手順

1. [* Configuration **]>[** Network Settings **]>[** Server Certificates*]を選択します。
2. Object Storage API Service Endpoints Server Certificateセクションで、* Use Default Certificates *をクリックします。
3. 確認ダイアログボックスで * OK * をクリックする。

   オブジェクトストレージAPIエンドポイント用のデフォルトサーバ証明書をリストアすると、設定したカスタムサーバ証明書ファイルは削除され、システムからはリカバリできなくなります。以降すべての新しいAPIクライアント接続には、デフォルトのサーバ証明書が使用されます。

4. Web ブラウザが更新されたことを確認するには、ページをリフレッシュしてください。

StorageGRID システムの**CA**証明書をコピーしています

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

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

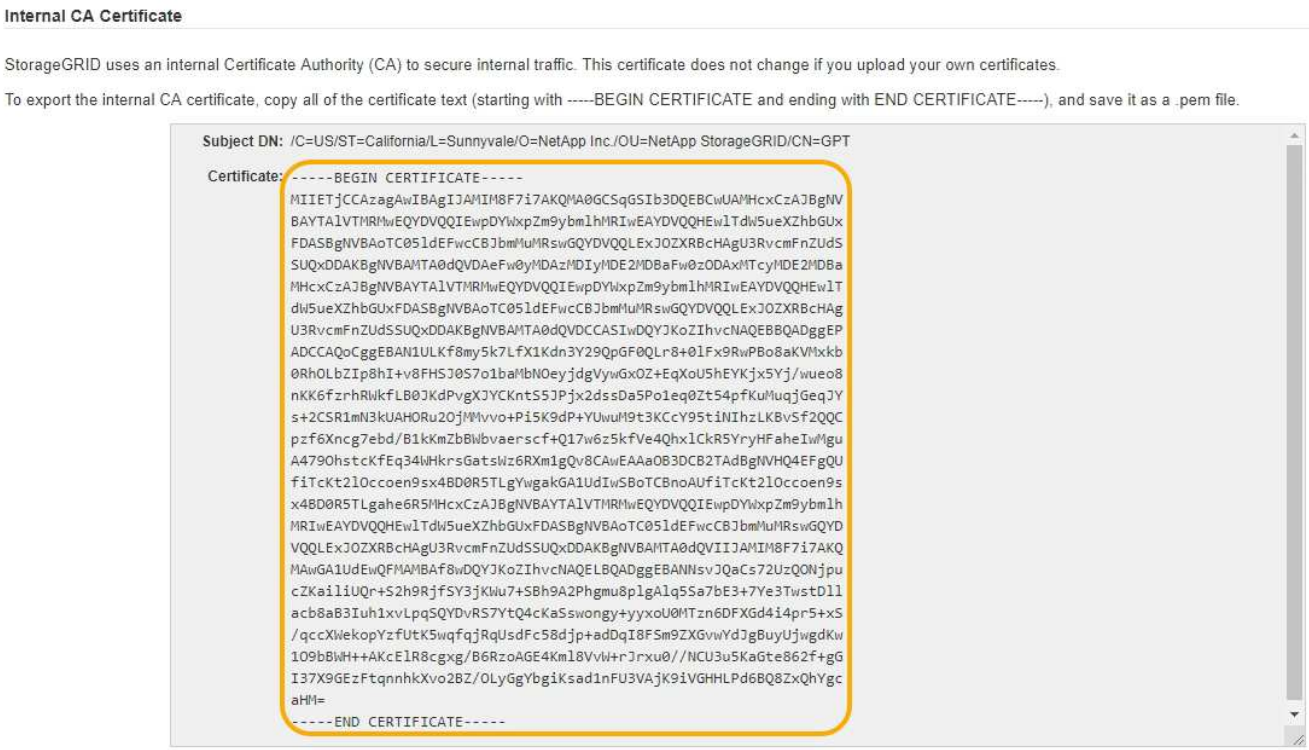
このタスクについて

カスタムサーバ証明書が設定されている場合、クライアントアプリケーションはカスタムサーバ証明書を使用してサーバを検証する必要があります。StorageGRID システムから CA 証明書をコピーしない。

手順

1. [* Configuration **]>[** Network Settings **]>[** Server Certificates*]を選択します。
2. [内部**CA**証明書（* Internal CA Certificate *）]セクションで、すべての証明書テキストを選択します。

   を含める必要があります `-----BEGIN CERTIFICATE-----` および `-----END CERTIFICATE-----` を選択します。



3. 選択したテキストを右クリックし、*コピー*を選択します。
4. コピーした証明書をテキストエディタに貼り付けます。
5. 拡張子を付けてファイルを保存します `.pem`。

   例： `storagegrid_certificate.pem`

FabricPool 用の**StorageGRID** 証明書を設定しています

厳密なホスト名検証を実行する S3 クライアントでは、 FabricPool を使用する ONTAP クライアントなどの厳密なホスト名検証の無効化をサポートしていない場合は、ロードバランサエンドポイントの設定時にサーバ証明書を生成またはアップロードできます。

必要なもの

- 特定のアクセス権限が必要です。
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

このタスクについて

ロードバランサエンドポイントを作成する際には、自己署名サーバ証明書を生成するか、既知の認証局（CA）によって署名された証明書をアップロードできます。本番環境では、既知の CA によって署名された証明書を使用する必要があります。CA によって署名された証明書は、システムを停止することなくローテーションできます。また、中間者攻撃に対する保護としても優れているため、セキュリティも強化されます。

次の手順は、 FabricPool を使用する S3 クライアントを対象とした一般的なガイドラインです。詳細な情報と手順については、StorageGRID for FabricPool の設定手順を参照してください。

ゲートウェイノード上の別の Connection Load Balancer （ CLB ）サービスは廃止され、 FabricPool での使用は推奨されなくなりました。

手順

1. 必要に応じて、 FabricPool で使用するハイアベイラビリティ（ HA ）グループを設定します。
2. FabricPool で使用する S3 ロードバランサエンドポイントを作成します。

   HTTPSロードバランサエンドポイントを作成する際に、サーバ証明書、証明書の秘密鍵、およびCAバンドルのアップロードを求めるプロンプトが表示されます。

3. ONTAP でクラウド階層として StorageGRID を接続します。

   ロードバランサエンドポイントのポートと、アップロードした CA 証明書で使用する完全修飾ドメイン名を指定します。次に、 CA 証明書を指定します。

   > ⓘ 中間 CA が StorageGRID 証明書を発行した場合は、中間 CA 証明書を指定する必要があります。StorageGRID 証明書がルート CA によって直接発行された場合は、ルート CA 証明書を指定する必要があります。

関連情報

"StorageGRID for FabricPool を設定します"

管理インターフェイス用の自己署名サーバ証明書の生成

スクリプトを使用して、ホスト名の厳密な検証が必要な管理APIクライアント用の自己署名サーバ証明書を生成できます。

必要なもの

- 特定のアクセス権限が必要です。
- を用意しておく必要があります `Passwords.txt` ファイル。

このタスクについて

本番環境では、既知の認証局（CA）によって署名された証明書を使用する必要があります。CA によって署名された証明書は、システムを停止することなくローテーションできます。また、中間者攻撃に対する保護としても優れているため、セキュリティも強化されます。

手順

1. 各管理ノードの完全修飾ドメイン名（ FQDN ）を取得します。
2. プライマリ管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@primary_Admin_Node_IP`
   b. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

      rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。
3. 新しい自己署名証明書を使用して StorageGRID を設定します。

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

- の場合 `--domains`、ワイルドカードを使用して、すべての管理ノードの完全修飾ドメイン名を表します。例： `*.ui.storagegrid.example.com` ワイルドカード*を使用して表します `admin1.ui.storagegrid.example.com` および `admin2.ui.storagegrid.example.com`。
- 設定 `--type` 終了： `management` Grid ManagerおよびTenant Managerで使用される証明書を設定するため。
- デフォルトでは、生成された証明書の有効期間は 1 年間（ 365 日）です。この期間を過ぎる前に証明書を再作成する必要があります。を使用できます `--days` デフォルトの有効期間を上書きする引数。

> ⓘ 証明書の有効期間は、で始まります `make-certificate` を実行します。管理APIクライアントがStorageGRID と同じ時間ソースと同期されるようにしてください。同期されていないと、クライアントが証明書を拒否する可能性があります。

```
$ sudo make-certificate --domains *.ui.storagegrid.example.com --type
management --days 365
```

出力には、管理 API クライアントで必要なパブリック証明書が含まれています。

4. 証明書を選択してコピーします。

   BEGIN タグと END タグも含めて選択してください。

5. コマンドシェルからログアウトします。 `$ exit`
6. 証明書が設定されたことを確認します。
   a. Grid Manager にアクセスします。
   b. 「* Configuration * Server Certificates * Management Interface Server Certificate *」を選択します。
7. コピーしたパブリック証明書を使用するように管理APIクライアントを設定します。BEGIN タグと END タグを含めてください。

ストレージプロキシを設定しています

プラットフォームサービスまたはクラウドストレージプールを使用している場合は、ストレージノードと外部の S3 エンドポイントの間に非透過型プロキシを設定できます。たとえば、インターネット上のエンドポイントなどの外部エンドポイントへプラットフォームサービスメッセージを送信する場合などには、非透過型プロキシが必要です。

必要なもの

- 特定のアクセス権限が必要です。
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

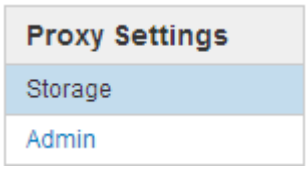
このタスクについて

設定できるストレージプロキシは 1 つです。

手順

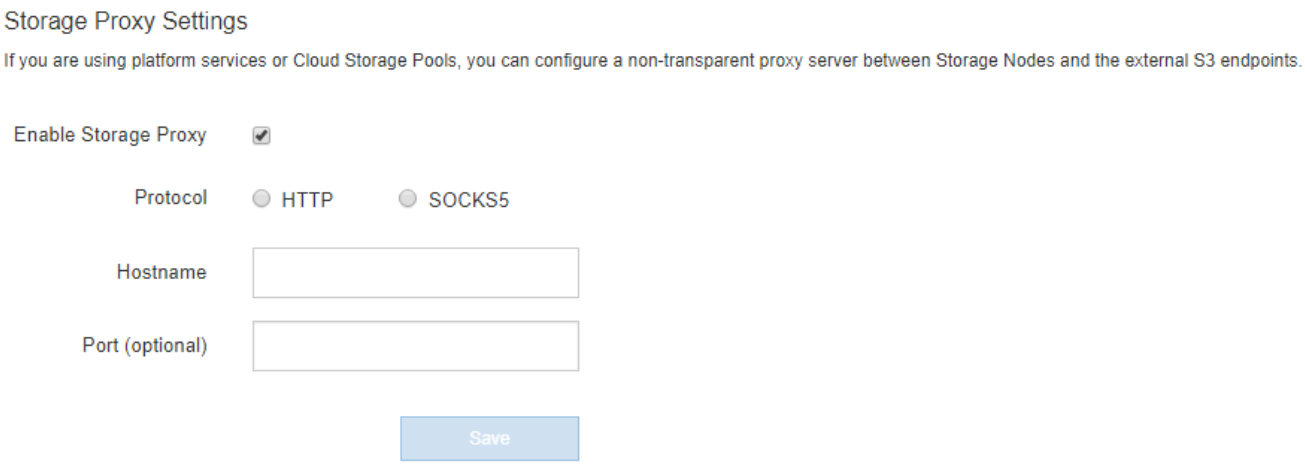
1. [環境設定*ネットワーク設定*プロキシ設定]を選択します。

   ストレージプロキシの設定ページが表示されます。デフォルトでは、サイドバーメニューで「 * Storage * 」が選択されています。



2. Enable Storage Proxy （ストレージプロキシの有効化）チェックボックスを選択します。

   ストレージプロキシを設定するためのフィールドが表示されます。



3. 非透過型ストレージプロキシのプロトコルを選択します。
4. プロキシサーバのホスト名または IP アドレスを入力します。
5. 必要に応じて、プロキシサーバへの接続に使用するポートを入力します。

   プロトコルにデフォルトのポート 80 を使用する場合は、このフィールドを空白のままにできます。 HTTP の場合は 80 、 SOCKS5 の場合は 1080 です。

6. [保存（ Save ）] をクリックします。

   ストレージプロキシが保存されたら、プラットフォームサービスまたはクラウドストレージプールの新しいエンドポイントを設定してテストできます。

   プロキシの変更が有効になるまでに最大 10 分かかることがあります。

7. プロキシサーバの設定をチェックして、 StorageGRID からのプラットフォームサービス関連メッセージがブロックされないようにします。

完了後

ストレージプロキシを無効にする必要がある場合は、*ストレージプロキシを有効にする*チェックボックスの選択を解除し、*保存*をクリックします。

関連情報

"プラットフォームサービス用のネットワークとポート"

"ILM を使用してオブジェクトを管理する"

管理プロキシの設定

HTTPまたはHTTPSを使用してAutoSupport メッセージを送信する場合は、管理ノードとテクニカルサポート（AutoSupport ）の間に非透過型プロキシサーバを設定できます。

必要なもの

- 特定のアクセス権限が必要です。
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

このタスクについて

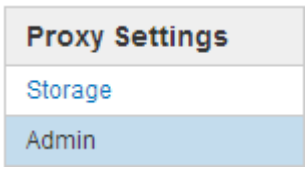
設定できる管理プロキシは 1 つです。

手順

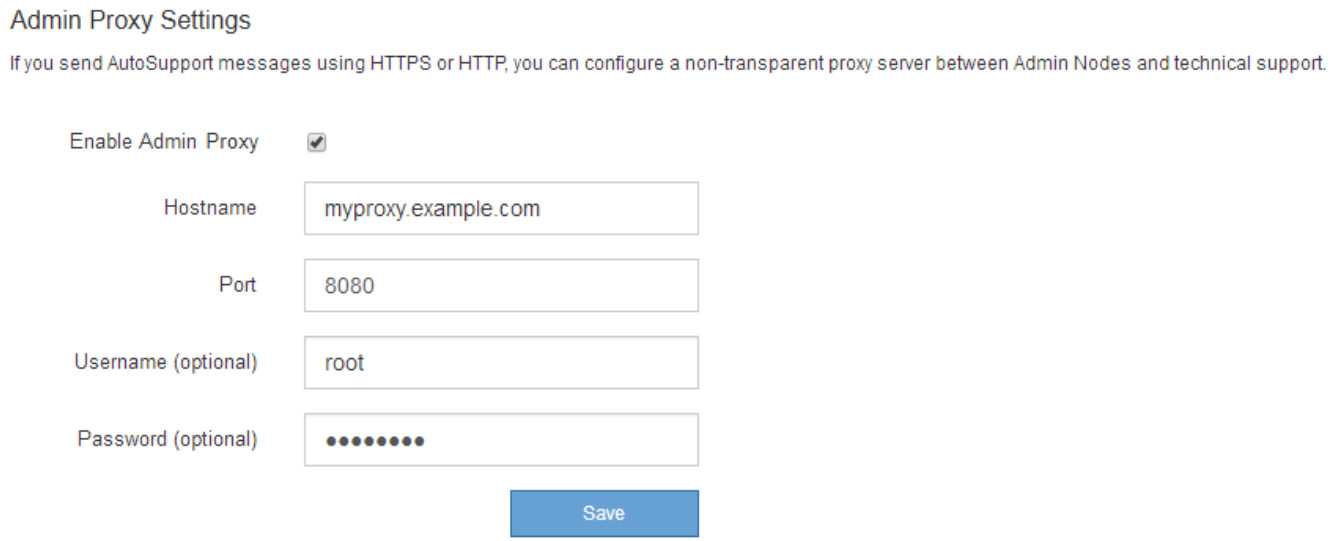
1. [環境設定*ネットワーク設定*プロキシ設定]を選択します。

   Admin Proxy Settings ページが表示されます。デフォルトでは、サイドバーメニューで「 * Storage * 」が選択されています。

2. サイドバーのメニューから、 **Admin** を選択します。



3. [管理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。



4. プロキシサーバのホスト名または IP アドレスを入力します。

5. プロキシサーバへの接続に使用するポートを入力します。
6. 必要に応じて、プロキシユーザ名を入力します。

   プロキシサーバでユーザ名が不要な場合は、このフィールドを空白のままにします。

7. 必要に応じて、プロキシパスワードを入力します。

   プロキシサーバでパスワードが不要な場合は、このフィールドを空白のままにします。

8. [保存（ Save ）] をクリックします。

   管理プロキシが保存されると、管理ノードとテクニカルサポートの間にプロキシサーバが設定されます。

   プロキシの変更が有効になるまでに最大 10 分かかることがあります。

9. プロキシを無効にする必要がある場合は、*管理者プロキシを有効にする*チェックボックスの選択を解除し、*保存*をクリックします。

関連情報

"AutoSupport メッセージのプロトコルの指定"

トラフィック分類ポリシーの管理

サービス品質（ QoS ）サービスを強化するために、トラフィック分類ポリシーを作成して、さまざまなタイプのネットワークトラフィックを識別および監視できます。これらのポリシーは、トラフィックの制限と監視に役立ちます。

トラフィック分類ポリシーは、ゲートウェイノードおよび管理ノードの StorageGRID ロードバランササービス上のエンドポイントに適用されます。トラフィック分類ポリシーを作成するには、ロードバランサエンドポイントを作成しておく必要があります。

ルールとオプションの制限を一致させる

各トラフィック分類ポリシーには、次のエンティティに関連するネットワークトラフィックを識別する 1 つ以上の一致ルールが含まれています。

- バケット
- テナント
- サブネット（クライアントを含む IPv4 サブネット）
- エンドポイント（ロードバランサエンドポイント）

StorageGRID は、ルールの目的に応じて、ポリシー内のルールに一致するトラフィックを監視します。ポリシーのルールに一致するトラフィックは、そのポリシーによって処理されます。逆に、指定されたエンティティを除くすべてのトラフィックを照合するルールを設定できます。

必要に応じて、次のパラメータに基づいてポリシーの制限を設定できます。

- 総帯域幅

- 総帯域幅アウト
- 同時読み取り要求
- 同時書き込み要求
- での要求ごとの帯域幅
- 要求ごとの帯域幅アウト
- 読み取り要求レート
- 書き込み要求の速度

> ポリシーを作成して、アグリゲートの帯域幅を制限したり、要求ごとの帯域幅を制限したりできます。ただし、 StorageGRID では、両方のタイプの帯域幅を同時に制限することはできません。アグリゲートの帯域幅の制限により、制限のないトラフィックにパフォーマンスが若干低下する可能性があります。

トラフィック制限

トラフィック分類ポリシーを作成した場合、トラフィックは設定したルールおよび制限のタイプに応じて制限されます。集約または要求ごとの帯域幅制限の場合、要求は、設定したレートでストリームインまたはアウトされます。StorageGRID では 1 つの速度しか適用できないため、最も特定のポリシーがマッチするのはマッチャーのタイプです。それ以外のすべての制限タイプでは、クライアント要求は 250 ミリ秒遅延し、一致するポリシー制限を超える要求に対しては 503 スローダウン応答を受信します。

Grid Manager では、トラフィックチャートを表示して、ポリシーが想定したトラフィック制限を適用していることを確認できます。

SLAでの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ともに使用して、容量、データ保護、およびパフォーマンスに固有のサービスレベル契約（ SLA ）を適用できます。

トラフィック分類の制限は、ロードバランサごとに実装されます。複数のロードバランサに同時にトラフィックが分散されている場合、合計最大速度は指定した速度制限の倍数になります。

次の例は、 SLA の 3 つの階層を示しています。トラフィック分類ポリシーを作成して、各 SLA 層のパフォーマンス目標を達成できます。

サービスレベル階層	容量	データ保護	パフォーマンス	コスト
ゴールド	1 PB のストレージを使用できます	3 コピーの ILM ルール	25 、 000 要求 / 秒 5 GB/ 秒（ 40 Gbps ）の帯域幅	$$/ 月
シルバー	250 TB のストレージを使用できます	2 コピーの ILM ルール	10 K 要求 / 秒 1.25 GB/ 秒（ 10 Gbps ）の帯域幅	$/ 月

サービスレベル階層	容量	データ保護	パフォーマンス	コスト
ブロンズ	100TB のストレージを使用できます	2 コピーの ILM ルール	5 、 000 要求 / 秒 1 GB/ 秒（ 8 Gbps ）の帯域幅	月あたりのコスト

トラフィック分類ポリシーの作成

バケット、テナント、 IP サブネット、またはロードバランサエンドポイントごとにネットワークトラフィックを監視し、必要に応じて制限する場合は、トラフィック分類ポリシーを作成します。必要に応じて、帯域幅、同時要求数、または要求速度に基づいてポリシーの制限を設定できます。

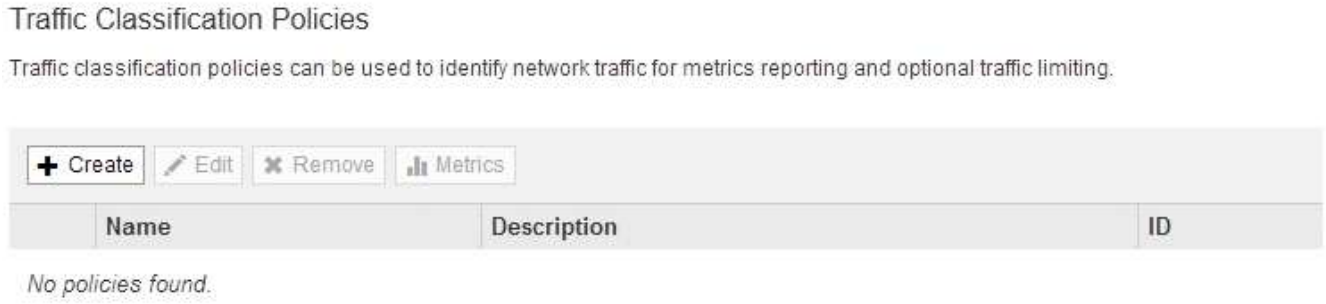
必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限が必要です。
- 照合するロードバランサエンドポイントを作成しておく必要があります。
- 該当するテナントを作成しておく必要があります。

手順

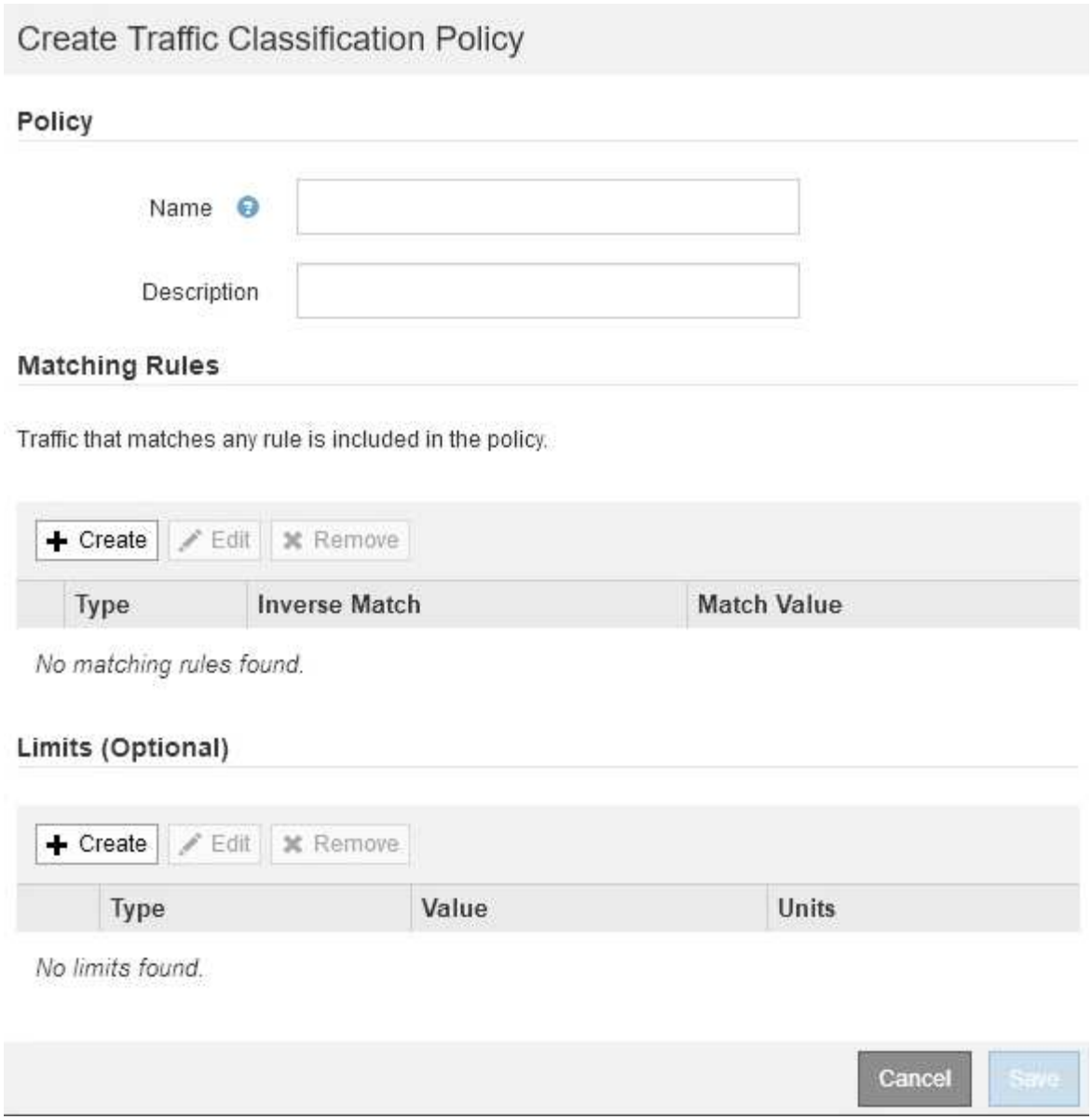
1. [* Configuration **]>[** Network Settings **]>[** Traffic Classification]を選択します。

   [Traffic Classification Policies] ページが表示されます。



2. [作成（ Create ）] をクリックします。

   Create Traffic Classification Policy ダイアログボックスが表示されます。



3. [* 名前 *] フィールドに、ポリシーの名前を入力します。

   ポリシーを識別できるように、わかりやすい名前を入力します。

4. 必要に応じて、 * 概要 * フィールドにポリシーの概要 を追加します。

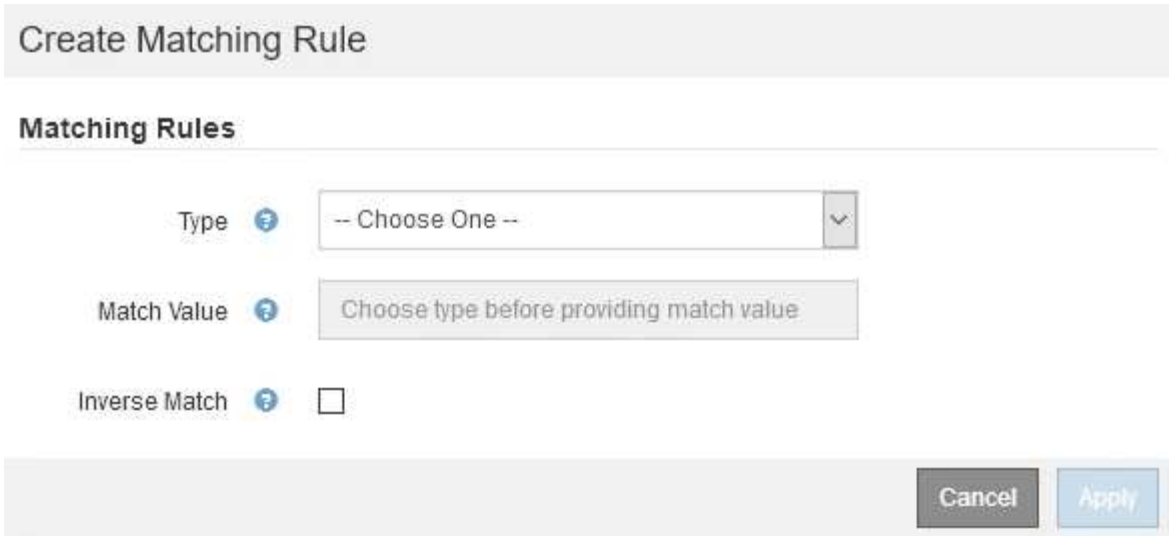
   たとえば、このトラフィック分類ポリシー環境 の内容と制限する内容を説明します。

5. ポリシーに一致するルールを 1 つ以上作成します。

   一致ルールは、このトラフィック分類ポリシーの影響を受けるエンティティを制御します。たとえば、このポリシーを特定のテナントのネットワークトラフィックに適用する場合は、テナントを選択します。または、このポリシーを特定のロードバランサエンドポイントのネットワークトラフィックに適用する場合は、 [Endpoint] を選択します。

   a. [マッチングルール（Matching Rules *）]セクションで[*作成（Create *）]をクリックし

      [Create Matching Rule] ダイアログボックスが表示されます。



b. [* タイプ *] ドロップダウンから、一致するルールに含めるエンティティのタイプを選択します。

c. [**match value**] フィールドに、選択したエンティティのタイプに基づいて照合値を入力します。

   - Bucket ：バケット名を入力します。
   - Bucket Regex ：一連のバケット名と一致するために使用される正規表現を入力します。

     正規表現は固定されていません。バケット名の先頭にある ｛キャレット｝ アンカーを使用し、名前の末尾に $ アンカーを使用します。

   - CIDR ： IPv4 サブネットを CIDR 表記で入力し、目的のサブネットと一致させます。
   - Endpoint ：既存のエンドポイントのリストからエンドポイントを選択します。これは、ロードバランサエンドポイントのページで定義したロードバランサエンドポイントです。
   - テナント：既存のテナントのリストからテナントを選択します。テナントの一致は、アクセス対象のバケットの所有権に基づきます。バケットへの匿名アクセスは、バケットを所有するテナントと一致します。

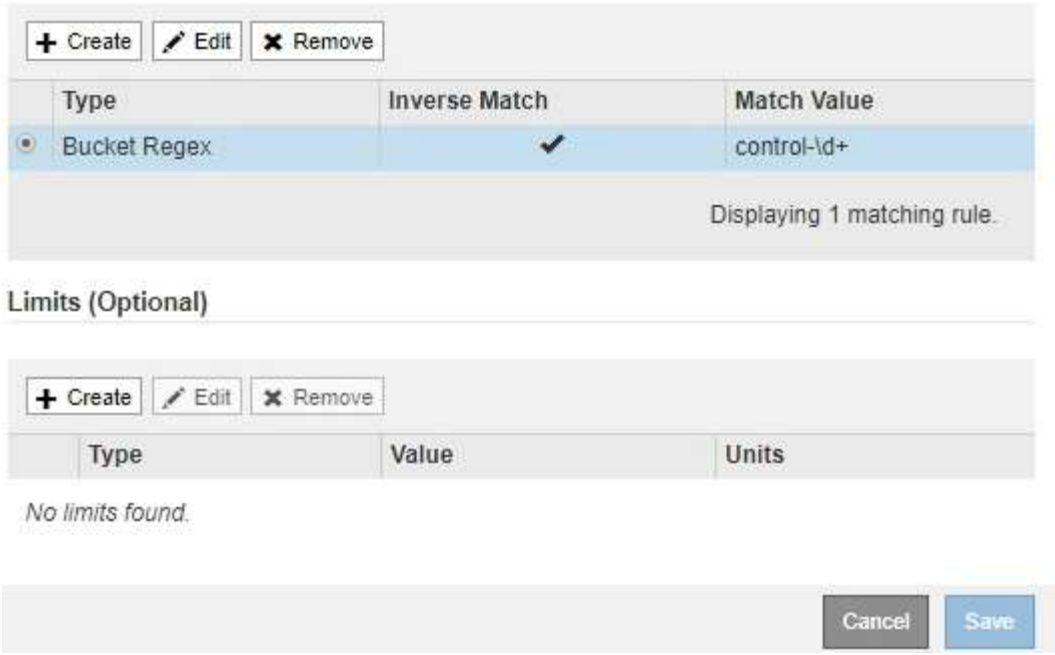
d. 定義した Type および Match 値と一致するすべての TRAFFER_EXCEPT _Traffic を照合する場合は、* Inverse * チェックボックスをオンにします。それ以外の場合は、このチェックボックスをオフのままにします。

   たとえば、このポリシーをいずれかのロードバランサエンドポイントを除くすべてのエンドポイントに適用する場合は、除外するロードバランサエンドポイントを指定し、 * Inverse * を選択します。

   > 少なくとも 1 つが逆マッチャーである複数のマッチャーを含むポリシーの場合、すべてのリクエストに一致するポリシーを作成しないように注意してください。

e. [適用（ Apply ）] をクリックします。

   ルールが作成され、 [Matching Rules] テーブルに表示されます。



a. ポリシーに対して作成するルールごとに上記の手順を繰り返します。

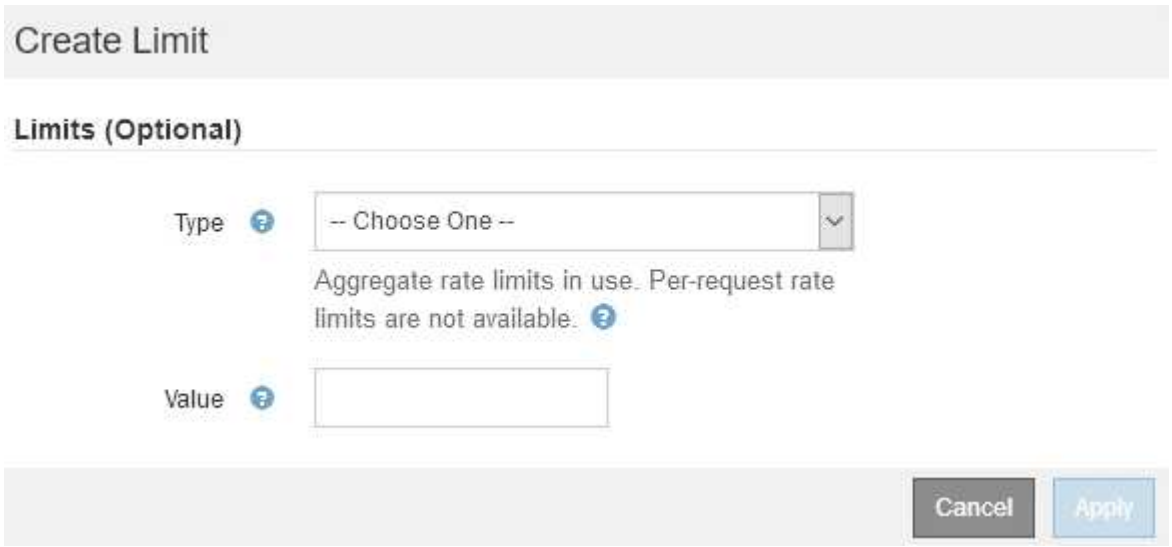
ルールに一致するトラフィックは、ポリシーによって処理されます。

6. 必要に応じて、ポリシーの制限を作成します。

制限を作成しない場合でも、ポリシーに一致するネットワークトラフィックを監視できるように StorageGRID で指標が収集されます。

a. 「制限」セクションで「*作成」をクリックします。

境界を作成（ Create Limit ）ダイアログボックスが表示されます。



b. [* タイプ *] ドロップダウンから、ポリシーに適用する制限のタイプを選択します。

次のリストの * in * は S3 または Swift クライアントから StorageGRID ロードバランサへのトラフィ

ックを表し、 * out * はロードバランサから S3 または Swift クライアントへのトラフィックを表しています。

- 総帯域幅
- 総帯域幅アウト
- 同時読み取り要求
- 同時書き込み要求
- での要求ごとの帯域幅
- 要求ごとの帯域幅アウト
- 読み取り要求レート
- 書き込み要求の速度

> ポリシーを作成して、アグリゲートの帯域幅を制限したり、要求ごとの帯域幅を制限したりできます。ただし、 StorageGRID では、両方のタイプの帯域幅を同時に制限することはできません。アグリゲートの帯域幅の制限により、制限のないトラフィックにパフォーマンスが若干低下する可能性があります。

帯域幅の制限については、設定された制限のタイプに最も一致するポリシーが StorageGRID によって適用されます。たとえば、トラフィックを一方向のみに制限するポリシーがある場合、帯域幅制限が設定されている他のポリシーと一致するトラフィックがあっても、反対方向のトラフィックは無制限になります。StorageGRID は、帯域幅制限の「ベスト」マッチを次の順序で実装します。

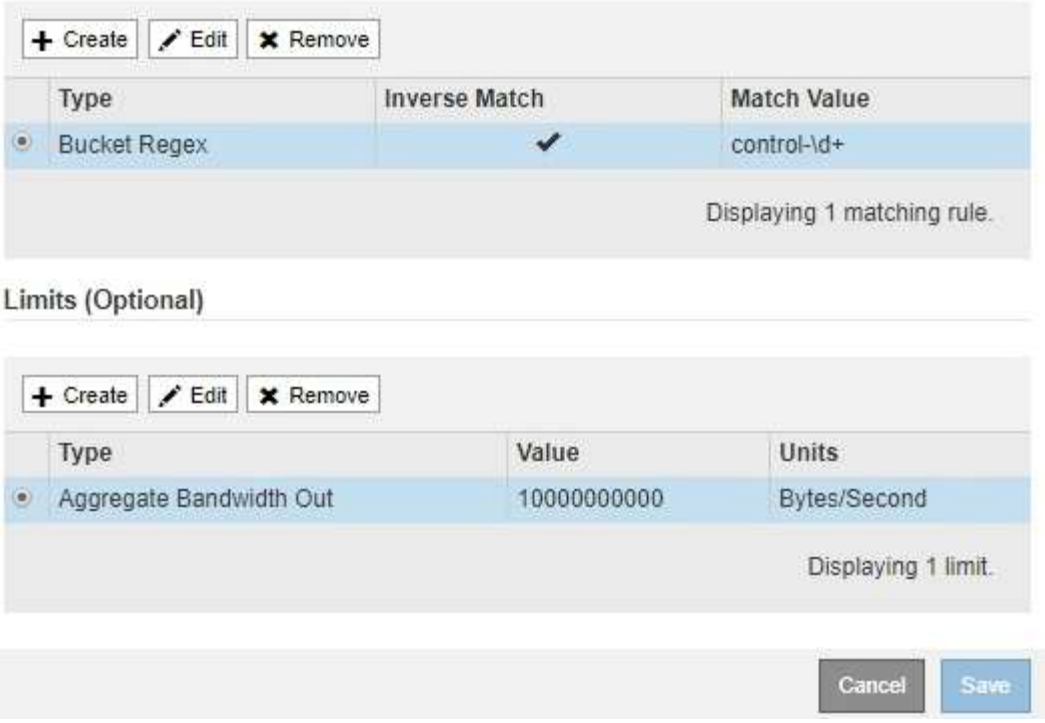
- 正確な IP アドレス（ /32 マスク）
- 正確なバケット名
- バケットの正規表現
- テナント
- エンドポイント
- 正確でない CIDR の一致（ /32 ではない）
- 逆一致

c. [* 値 *] フィールドに、選択した制限のタイプの数値を入力します。

制限を選択すると、想定される単位が表示されます。

d. [適用（ Apply ）] をクリックします。

境界が作成され、 [境界（ Limits ）] テーブルにリストされます。



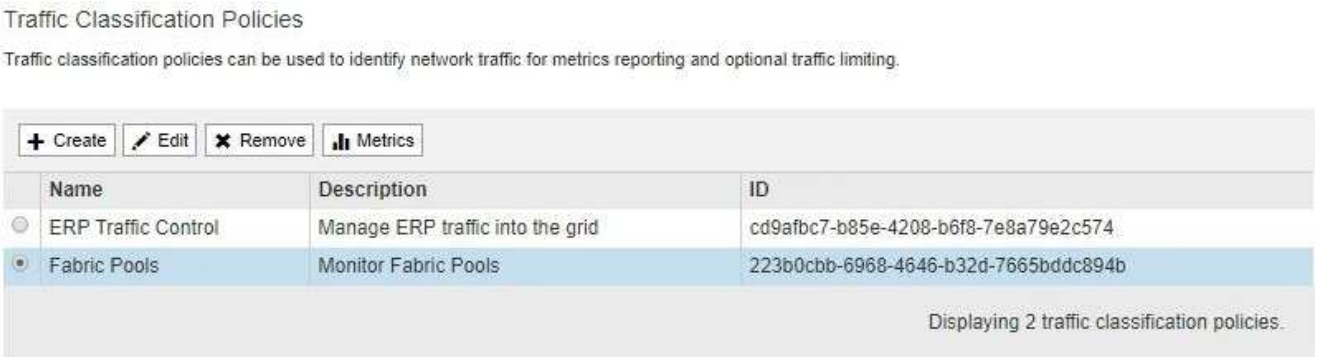
e. ポリシーに追加する上限ごとに、上記の手順を繰り返します。

たとえば、 SLA 階層に 40Gbps の帯域幅制限を作成する場合は、制限されたアグリゲート帯域幅と合計帯域幅の制限を作成し、各帯域幅を 40Gbps に設定します。

1 秒あたりのメガバイト数をギガビット / 秒に変換するには、 8 倍にします。たとえば、 125 MB/ 秒は 1 、 000 Mbps または 1 Gbps に相当します。

7. ルールと制限の作成が完了したら、*保存*をクリックします。

ポリシーが保存され、 Traffic Classification Policies テーブルにリストされます。



S3 および Swift クライアントトラフィックがトラフィック分類ポリシーに従って処理されるようになりました。トラフィックチャートを表示して、ポリシーが想定したトラフィック制限を適用していることを確認できます。

関連情報

"負荷分散の管理"

"ネットワークトラフィックメトリックの表示"

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、その名前または概要 を変更したり、ポリシーのルールや制限を作成、編集、削除したりできます。

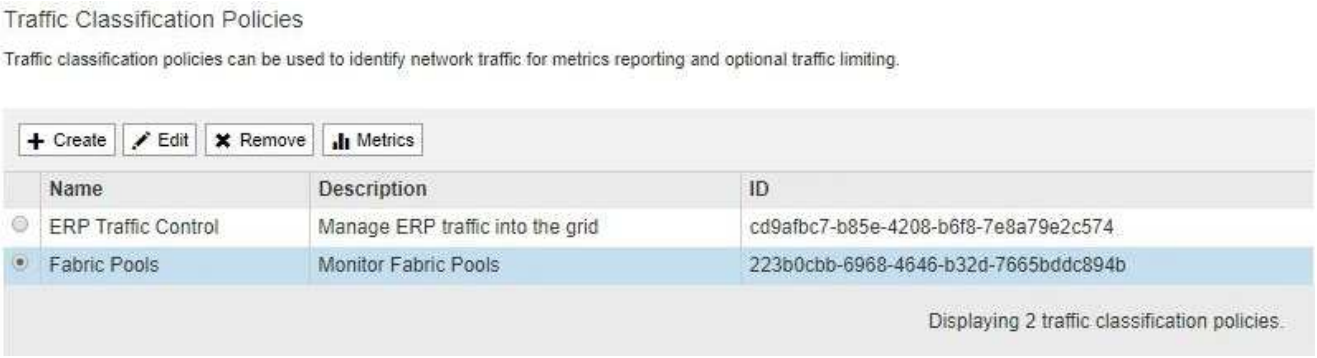
必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限が必要です。

手順

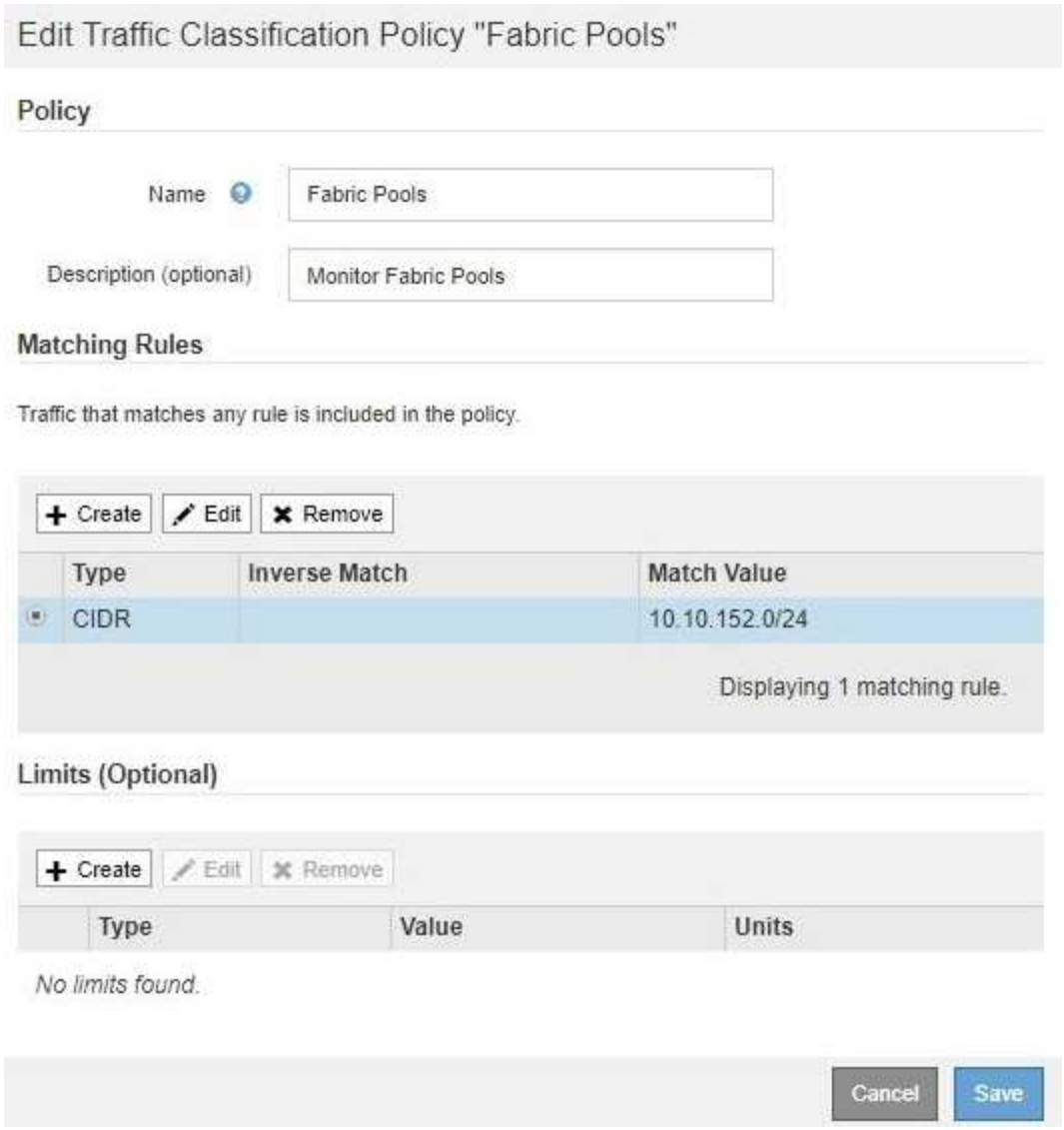
1. [* Configuration **]>[** Network Settings **]>[** Traffic Classification]を選択します。

   [Traffic Classification Policies] ページが表示され、既存のポリシーがテーブルにリストされます。



2. 編集するポリシーの左側にあるオプションボタンを選択します。
3. [編集（ Edit ）] をクリックします。

   Edit Traffic Classification Policy ダイアログボックスが表示されます。



4. 必要に応じて、一致するルールと制限を作成、編集、または削除します。
   a. 一致するルールまたは制限を作成するには、*作成*をクリックし、ルールの作成または制限の作成の手順に従います。
   b. 一致するルールまたは制限を編集するには、ルールまたは制限のラジオボタンを選択し、[一致するルール*]セクションまたは[制限]セクションで[編集]をクリックして、ルールの作成または制限の作成の手順に従います。
   c. 一致するルールまたは制限を削除するには、ルールまたは制限のラジオボタンを選択し、*削除*をクリックします。次に、[OK]をクリックして、ルールまたは制限を削除することを確認します。
5. ルールまたは制限の作成または編集が終了したら、*適用*をクリックします。
6. ポリシーの編集が完了したら、*保存*をクリックします。

   ポリシーに加えた変更が保存され、ネットワークトラフィックはトラフィック分類ポリシーに従って処理されるようになりました。トラフィックチャートを表示して、ポリシーが想定したトラフィック制限を適用していることを確認できます。

トラフィック分類ポリシーを削除する

トラフィック分類ポリシーが不要になった場合は、削除できます。

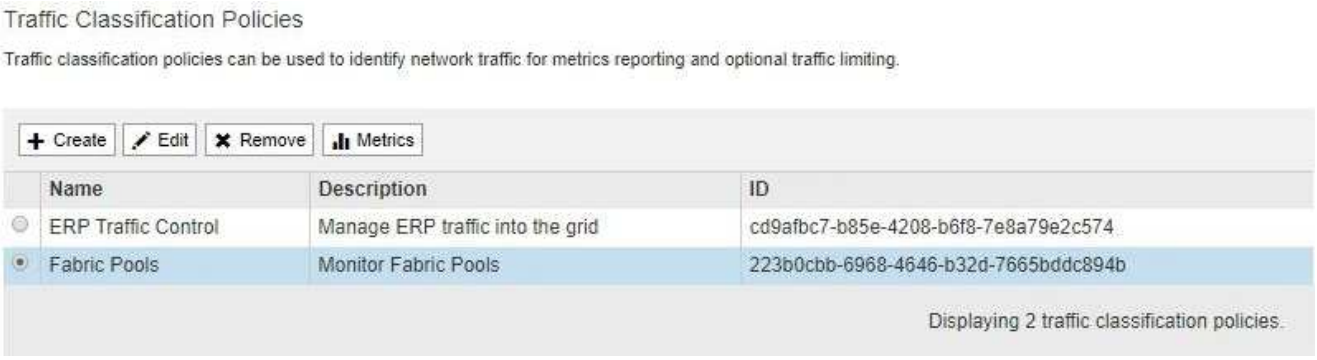
必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限が必要です。

手順

1. [* Configuration **]>[** Network Settings **]>[** Traffic Classification]を選択します。

   [Traffic Classification Policies] ページが表示され、既存のポリシーがテーブルにリストされます。



2. 削除するポリシーの左側にあるオプションボタンを選択します。
3. [削除（ Remove ）] をクリックします。

   警告ダイアログボックスが表示されます。

4. [OK]をクリックして、ポリシーを削除することを確認します。

   ポリシーが削除されます。

ネットワークトラフィックメトリックの表示

Traffic Classification Policies ページから使用可能なグラフを表示することで、ネットワークトラフィックを監視できます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

- Root Access 権限が必要です。

このタスクについて

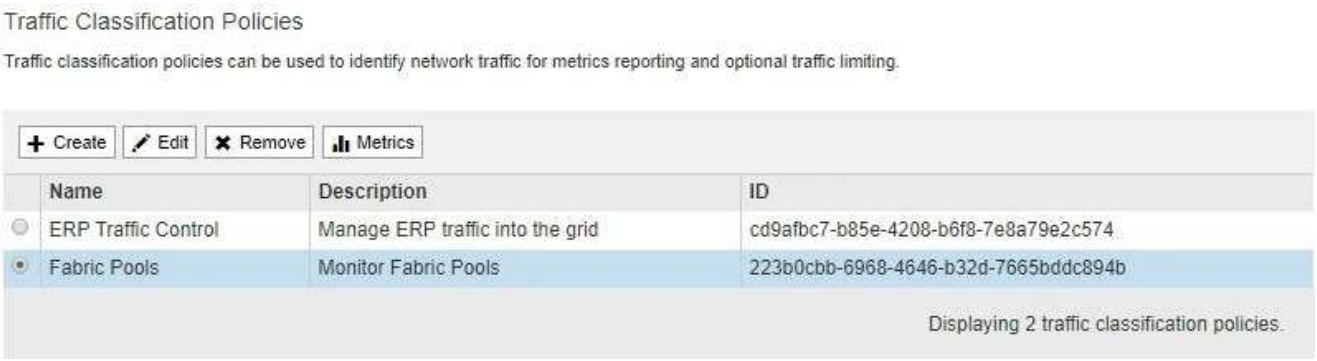
既存のトラフィック分類ポリシーでは、ロードバランササービスのメトリックを表示して、ポリシーがネットワーク全体のトラフィックを正常に制限しているかどうかを判断できます。グラフ内のデータは、ポリシーの調整が必要かどうかを判断するのに役立ちます。

トラフィック分類ポリシーに制限が設定されていない場合でも、メトリックが収集され、グラフにはトラフィックの傾向を把握するのに役立つ情報が表示されます。

手順

1. [* Configuration **]>[** Network Settings **]>[** Traffic Classification]を選択します。

   [Traffic Classification Policies] ページが表示され、既存のポリシーがテーブルにリストされます。



2. 指標を表示するポリシーの左側にあるラジオボタンを選択します。
3. [メトリクス]をクリックします。

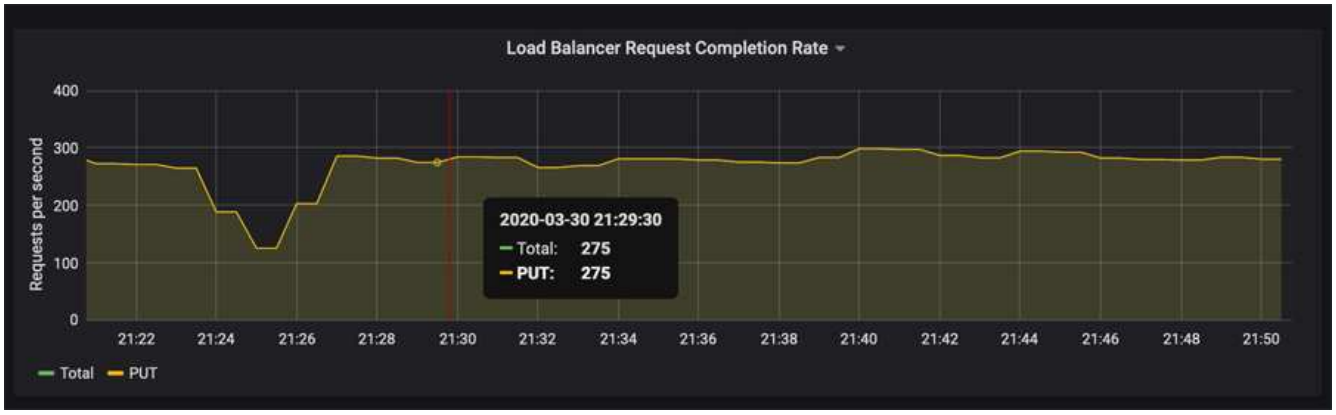
   新しいブラウザウィンドウが開き、 Traffic Classification Policy グラフが表示されます。このグラフには、選択したポリシーに一致するトラフィックのメトリックだけが表示されます。

   その他のポリシーを選択して表示するには、 * policy * プルダウンを使用します。

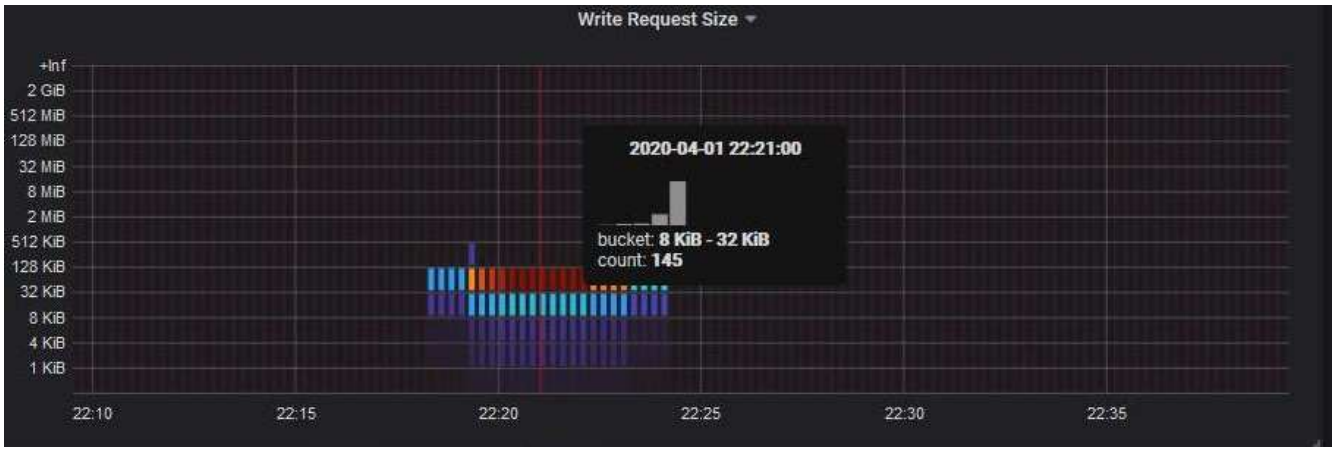
Web ページには次のグラフが表示されます。

- ロードバランサ要求トラフィック：このグラフは、ロードバランサエンドポイントと要求を送信しているクライアントの間で伝送されるデータのスループットを、 1 秒あたりのビット数で 3 分間の移動平均を提供します。
- ロードバランサの要求完了率：このグラフには、 1 秒あたりの完了済み要求数の 3 分間の移動平均が、要求タイプ（ GET 、 PUT 、 HEAD 、 DELETE ）別に示されます。この値は、新しい要求のヘッダーが検証されると更新されます。
- Error Response Rate ：このグラフには、 1 秒あたりにクライアントに返されたエラー応答数の 3 分間の移動平均が、エラー応答コード別に示されます。
- Average Request Duration （ Non-Error ）：このグラフには、要求期間の 3 分間の移動平均が、要求タイプ（ GET 、 PUT 、 HEAD 、 DELETE ）別に示されます。要求期間は、要求ヘッダーがロードバランササービスによって解析された時点から始まり、完全な応答本文がクライアントに返された時点で終了します。
- オブジェクトサイズ別の書き込み要求速度：このヒートマップは、オブジェクトサイズに基づいて書き込み要求が完了した時点での 3 分間の移動平均を提供します。この場合、書き込み要求は PUT 要求のみを参照します。
- オブジェクトサイズ別の読み取り要求速度：このヒートマップでは、オブジェクトサイズに基づいて読み取り要求が完了した時点での 3 分間の移動平均が提供されます。この場合、読み取り要求は GET 要求のみを参照します。ヒートマップの色は、個々のグラフ内のオブジェクトサイズの相対的な頻度を示します。クーラの色（紫や青など）は相対レートが低いことを示し、暖色の色（オレンジや赤など）は相対レートが高いことを示します。

4. 折れ線グラフにカーソルを合わせると、グラフの特定の部分の値がポップアップで表示されます。



5. ヒートマップにカーソルを合わせると、サンプルの日時、カウントに集約されたオブジェクトサイズ、およびその期間の 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。



6. 左上の * Policy * プルダウンを使用して、別のポリシーを選択します。

   選択したポリシーのグラフが表示されます。

7. または、* Support *メニューからグラフにアクセスします。
   a. [* Support*]>[* Tools]>[* Metrics]を選択します。
   b. ページの * Grafana * セクションで、 * Traffic Classification Policy * を選択します。
   c. ページ左上のプルダウンからポリシーを選択します。

      トラフィック分類ポリシーは、その ID によって識別されます。ポリシー ID は、 Traffic Classification Policies ページにリストされます。

8. 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。

関連情報

"トラブルシューティングを監視します"

リンクコストとは

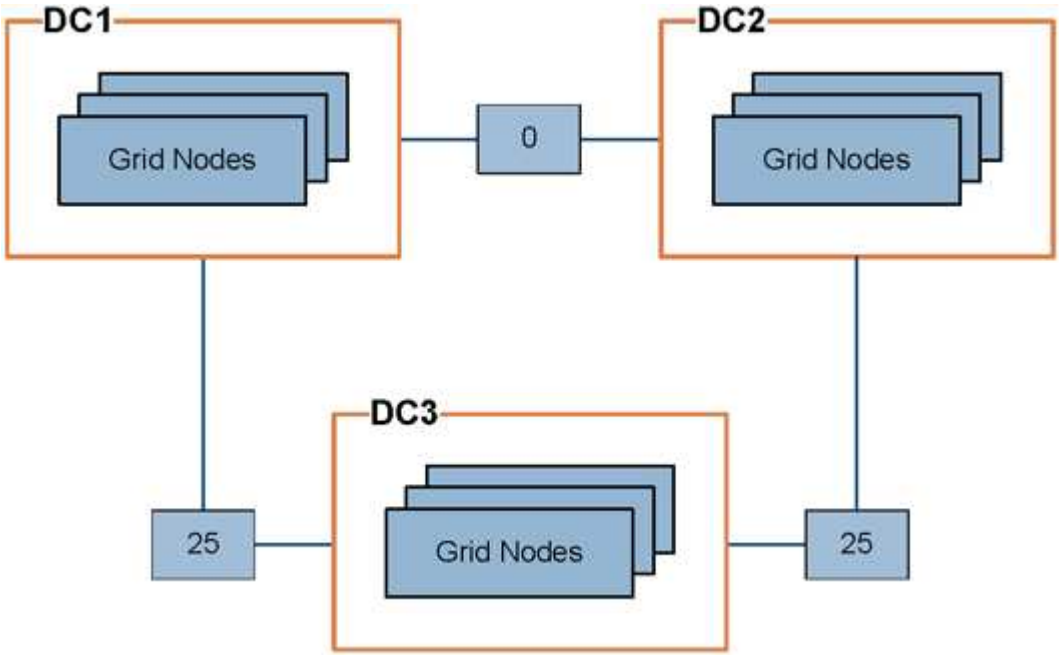
リンクコストを使用すると、複数のデータセンターサイトが存在する場合に、要求されたサービスを提供するデータセンターサイトの優先順位を決定できます。サイト間のレ

イテンシに合わせてリンクコストを調整できます。

- リンクコストは、オブジェクトの読み出しにどのオブジェクトコピーを使用するかを優先的に処理するために使用されます。
- リンクコストは、グリッド管理 API およびテナント管理 API で、使用する内部 StorageGRID サービスを決定するために使用されます。
- リンクコストは、ゲートウェイノード上のCLBサービスがクライアント接続を転送するために使用します。

> CLB サービスは廃止されました。

次の図は、サイト間でリンクコストが設定されている 3 つのサイトグリッドを示しています。



- ゲートウェイノード上の CLB サービスは、同じデータセンターサイトにあるすべてのストレージノード、およびリンクコストが 0 のデータセンターサイトにクライアント接続を均等に分散します。

  この例で、データセンターサイト 1 （ DC1 ）にあるゲートウェイノードは、 DC1 にあるストレージノードと DC2 にあるストレージノードにクライアント接続を均等に分散します。DC3 にあるゲートウェイノードは、 DC3 にあるストレージノードにのみクライアント接続を送信します。

- 複数のレプリケートコピーが存在するオブジェクトを読み出す場合、 StorageGRID はリンクコストが最も低いデータセンターにあるコピーを読み出します。

  この例で、 DC2 にあるクライアントアプリケーションが DC1 と DC3 の両方に格納されているオブジェクトを読み出す場合、 DC1 から DC2 へのリンクコストは 0 で、 DC3 から DC2 へのリンクコスト（ 25 ）よりも低いため、オブジェクトは DC1 から読み出されます。

リンクコストは、測定単位を伴わない任意の相対的な数値です。たとえば、使用にあたってリンクコスト 50 の優先度はリンクコスト 25 よりも低くなります。次の表に、よく使用されるリンクコストを示します。

リンク	リンクコスト	注：
物理データセンターサイト間	25 （デフォルト）	WAN リンクで接続されたデータセンター。
同じ物理的な場所にある論理データセンターサイト間	0	同じ物理ビルディングまたはキャンパスにある論理データセンターを LAN で接続します。

関連情報

"ロードバランシングの仕組み - CLB サービス"

リンクコストを更新しています

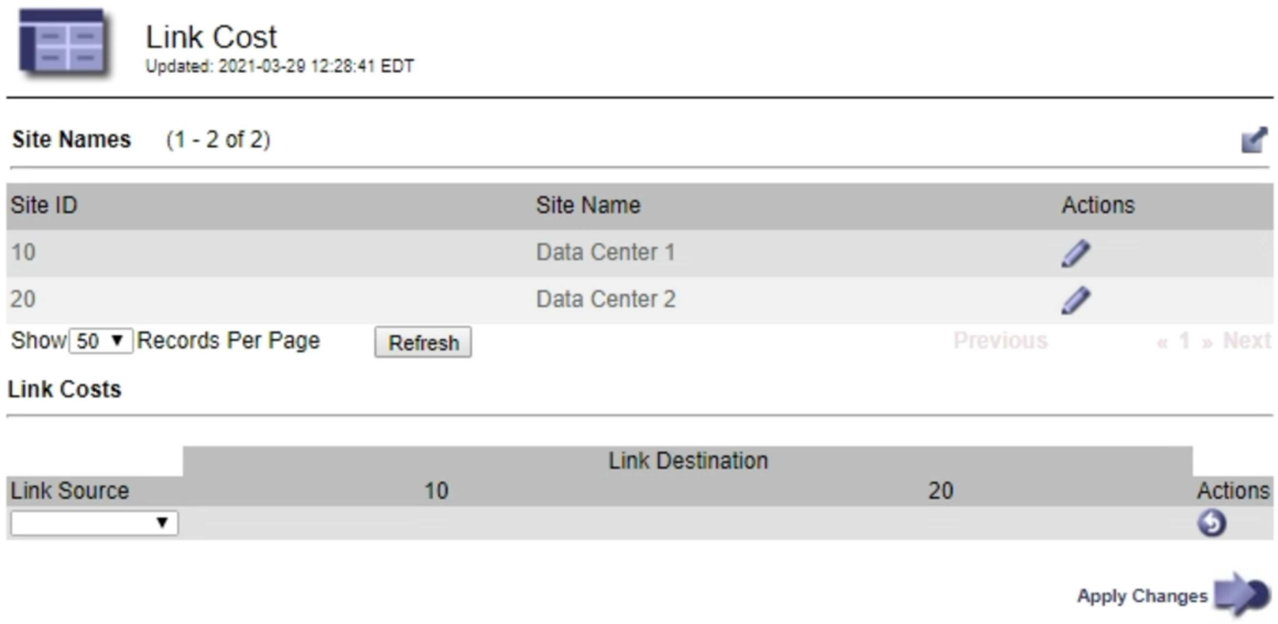
データセンターサイト間のリンクコストを更新して、サイト間のレイテンシを反映させることができます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Grid Topology Page Configuration権限が必要です。

手順

1. [環境設定]>[ネットワーク設定]>[リンクコスト]を選択します。



2. [リンク先 *] でサイトを選択し、 [リンク先 *] に 0 ～ 100 のコスト値を入力します。

   リンク元がリンク先と同じ場合は、リンクコストを変更できません。

   変更をキャンセルするには、をクリックします * 復帰 * 。

3. [変更の適用 *] をクリックします。

AutoSupport を設定しています

AutoSupport 機能を使用すると、 StorageGRID システムのヘルスメッセージおよびステータスメッセージをテクニカルサポートに送信できます。AutoSupport を使用すると、問題の特定と解決にかかる時間を大幅に短縮できます。また、システムのストレージニーズを監視し、新しいノードやサイトを追加する必要があるかどうかを判断するための支援も行います。必要に応じて、 1 つの別の送信先に AutoSupport メッセージを送信するように設定できます。

AutoSupport メッセージに含まれる情報

AutoSupport メッセージには次のような情報が含まれます。

- StorageGRID ソフトウェアのバージョン
- オペレーティングシステムのバージョン
- システムレベルおよび場所レベルの属性情報
- 最新のアラートとアラーム（従来型システム）
- 履歴データを含む、すべてのグリッドタスクの現在のステータス
- ノード*グリッドノード**イベント*ページに表示されるイベント情報
- 管理ノードデータベースの使用率
- 失われた、または欠落しているオブジェクトの数
- Grid の設定
- NMS エンティティ
- アクティブな ILM ポリシー
- プロビジョニングされたグリッド仕様ファイル
- 診断メトリック

AutoSupport 機能および個々の AutoSupport オプションは、 StorageGRID の初回インストール時に有効にするか、あとから有効にすることができます。AutoSupport が有効になっていない場合は、Grid ManagerDashboardにメッセージが表示されます。このメッセージには、 AutoSupport 設定ページへのリンクが含まれています。

「x」記号を選択できます をクリックしてメッセージを閉じます。このメッセージは、AutoSupport が無効なままであっても、ブラウザキャッシュがクリアされるまで表示されません。

Active IQ を使用する

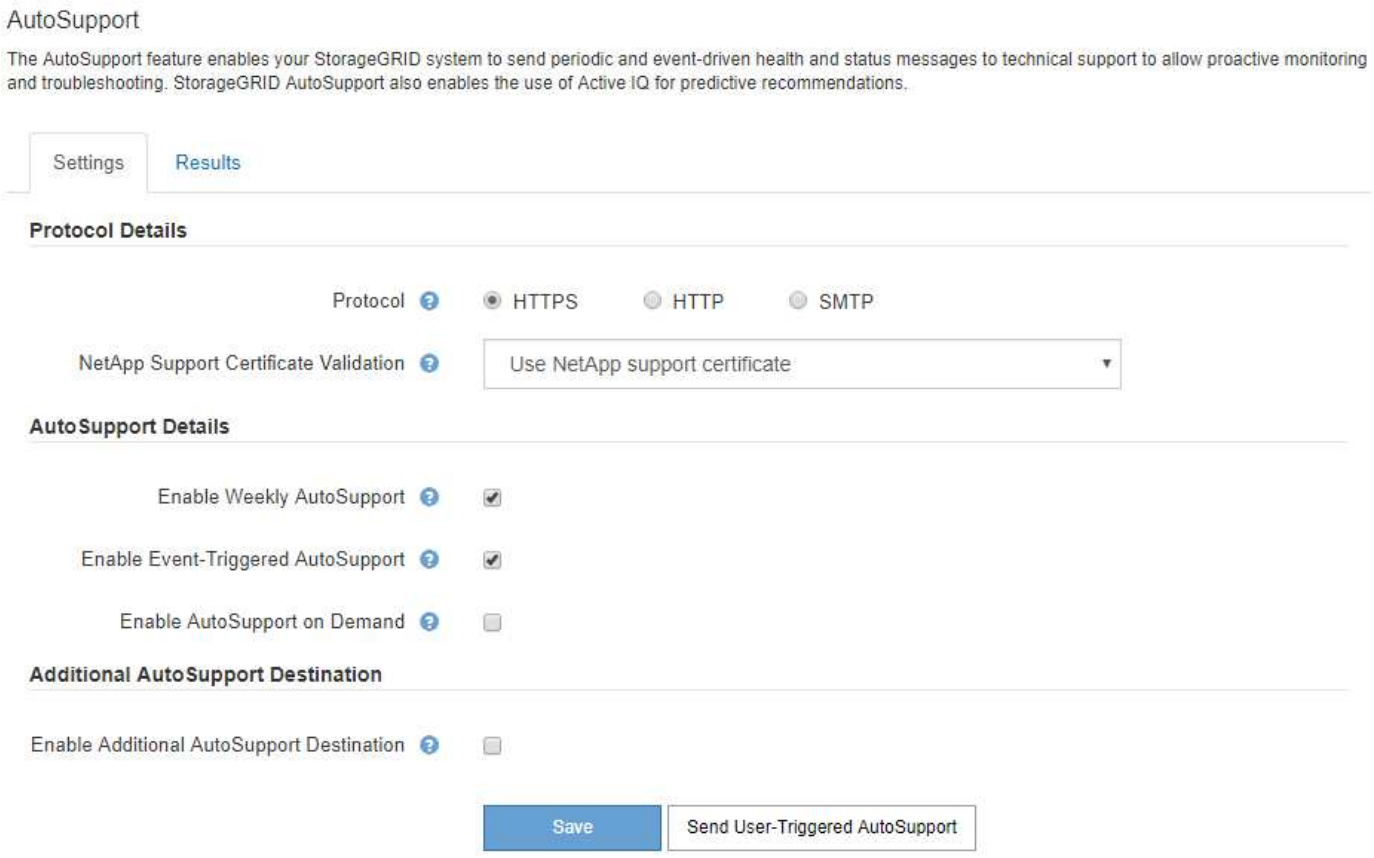
Active IQ は、ネットアップのインストールベースが提供する予測分析と集合知を活用する、クラウドベースのデジタルアドバイザです。継続的なリスク評価、予測アラート、規範となるガイダンス、自動化されたアクションによって、問題が発生する前に予防できます。これにより、システムの健全性が向上し、システムの可用性が向上します。

NetApp Support Siteの 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 IQ Digital Advisorのドキュメント"

AutoSupport 設定にアクセスしています

AutoSupport はGrid Manager（* Support > Tools > AutoSupport *）を使用して設定します。「 * AutoSupport * 」ページには、 * 設定 * と * 結果 * の 2 つのタブがあります。



AutoSupport メッセージを送信するためのプロトコル

AutoSupport メッセージの送信には、次の 3 つのプロトコルのいずれかを選択できます。

- HTTPS
- HTTP
- SMTP

HTTPS または HTTP を使用して AutoSupport メッセージを送信する場合は、管理ノードとテクニカルサポートの間に非透過型プロキシサーバを設定できます。

SMTP を AutoSupport メッセージのプロトコルとして使用する場合は、 SMTP メールサーバを設定する必要があります。

AutoSupport オプション

AutoSupport メッセージをテクニカルサポートに送信するには、次のオプションを任意に組み合わせて使用できます。

- * 週単位 * ： AutoSupport メッセージを週に 1 回自動的に送信します。デフォルト設定： Enabled （有効）。
- * イベントトリガー型 * ： 1 時間ごと、または重大なシステムイベントが発生したときに、 AutoSupport メッセージを自動的に送信します。デフォルト設定： Enabled （有効）。
- * On Demand * ： StorageGRID システムが AutoSupport メッセージを自動的に送信するようテクニカルサポートから要求できます。これは、問題 がアクティブに機能している場合に便利です（ HTTPS AutoSupport 転送プロトコルが必要）。デフォルト設定： Disabled （無効）。
- * User-triggered * ： AutoSupport メッセージをいつでも手動で送信します。

関連情報

"ネットアップサポート"

AutoSupport メッセージのプロトコルの指定

AutoSupport メッセージの送信には、3つのプロトコルのいずれかを使用できます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限または Other Grid Configuration 権限が必要です。
- AutoSupport メッセージの送信用にHTTPSプロトコルまたはHTTPプロトコルを使用する場合は、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提供するか、プロキシサーバを使用して提供しておく必要があります（インバウンド接続は不要です）。
- HTTPSまたはHTTPプロトコルの使用時にプロキシサーバを使用する場合は、管理プロキシサーバを設定しておく必要があります。
- AutoSupport メッセージのプロトコルとしてSMTPを使用する場合は、SMTPメールサーバを設定しておく必要があります。アラームの E メール通知には同じメールサーバ設定（従来のシステム）が使用されます。

このタスクについて

AutoSupport メッセージは、次のいずれかのプロトコルを使用して送信できます。

- * HTTPS * ：これはデフォルトで、新規インストールに推奨される設定です。HTTPS プロトコルはポート 443 を使用します。AutoSupport On Demand 機能を有効にする場合は、 HTTPS プロトコルを使用する必要があります。
- * HTTP * ：このプロトコルは、インターネット経由でデータを送信する際にプロキシサーバーが HTTPS に変換する信頼された環境で使用されない限り、安全ではありません。HTTP プロトコルはポート 80 を使用します。
- * SMTP * ： AutoSupport メッセージを E メールで送信する場合は、このオプションを使用します。SMTPをAutoSupport メッセージのプロトコルとして使用する場合は、[Legacy Email Setup]ページ

（* Support * Alarms（レガシー）* **Legacy Email Setup**）でSMTPメールサーバを設定する必要があります。

> StorageGRID 11.2 より前のリリースでは、 SMTP が AutoSupport メッセージに使用できる唯一のプロトコルでした。以前のバージョンの StorageGRID をインストールしていた場合は、 SMTP がプロトコルとして選択されている可能性があります。

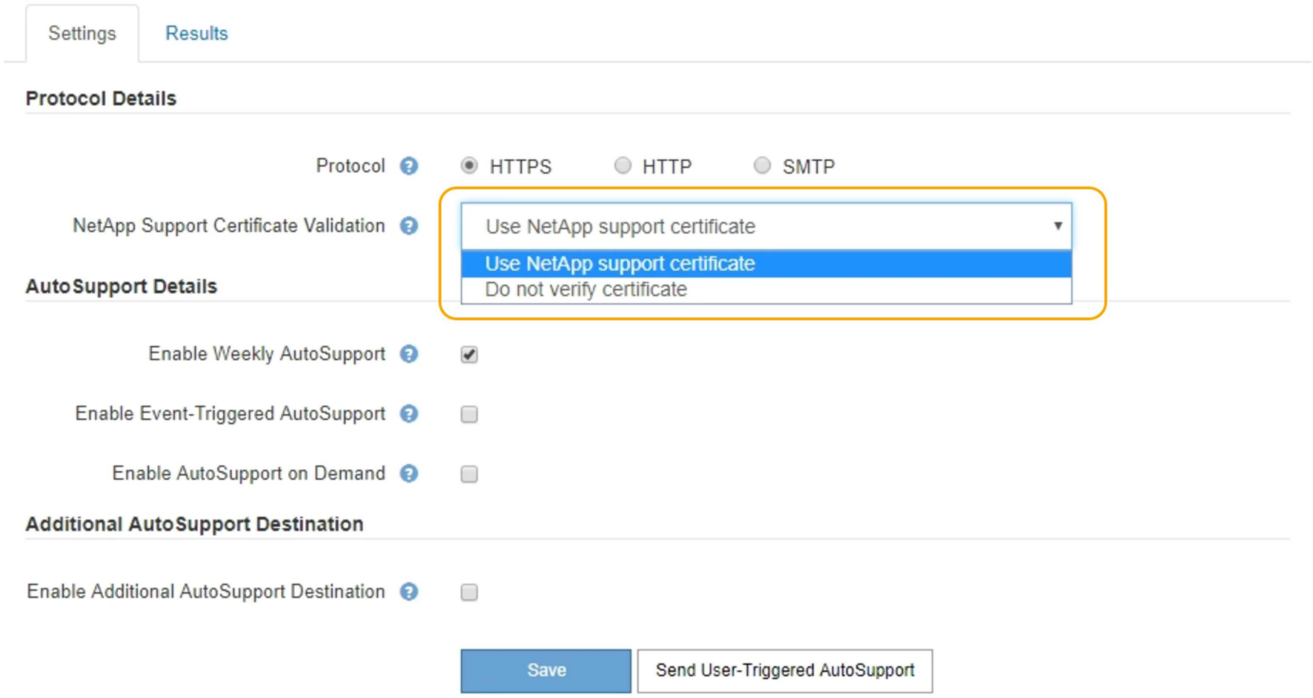
設定したプロトコルは、すべてのタイプの AutoSupport メッセージの送信に使用されます。

手順

1. [サポート（Support ）**]>[***ツール（* Tools ）**]>[** AutoSupport （*）]

   AutoSupport ページが表示され、 * 設定 * タブが選択されます。

2. AutoSupport メッセージの送信に使用するプロトコルを選択します。



3. ネットアップサポート証明書の検証*を選択します。

   - ネットアップサポート証明書を使用（デフォルト）：証明書の検証により、AutoSupport メッセージの送信がセキュアになります。ネットアップサポート証明書は、 StorageGRID ソフトウェアとともにすでにインストールされています。
   - Do not verify certificate（証明書を検証しない）：このオプションは、証明書の一時的な問題が発生した場合など、証明書の検証を使用しない十分な理由がある場合にのみ選択します。

4. [保存（ Save ）] を選択します。

   毎週、ユーザトリガー型、およびイベントトリガー型のすべてのメッセージが選択したプロトコルを使用して送信されます。

関連情報

"管理プロキシの設定"

AutoSupport On Demandの有効化

AutoSupport On Demand は、テクニカルサポートが問題解決に積極的に取り組んでいる場合に役立ちます。AutoSupport On Demandを有効にすると、テクニカルサポートはユーザの介入を必要とせずにAutoSupport メッセージの送信を要求できます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限または Other Grid Configuration 権限が必要です。
- 週次AutoSupport メッセージを有効にしておく必要があります。
- 転送プロトコルをHTTPSに設定しておく必要があります。

このタスクについて

この機能を有効にすると、テクニカルサポートは、StorageGRID システムに対してAutoSupport メッセージを自動的に送信するよう要求できます。テクニカルサポートは、 AutoSupport On Demand クエリのポーリング間隔も設定できます。

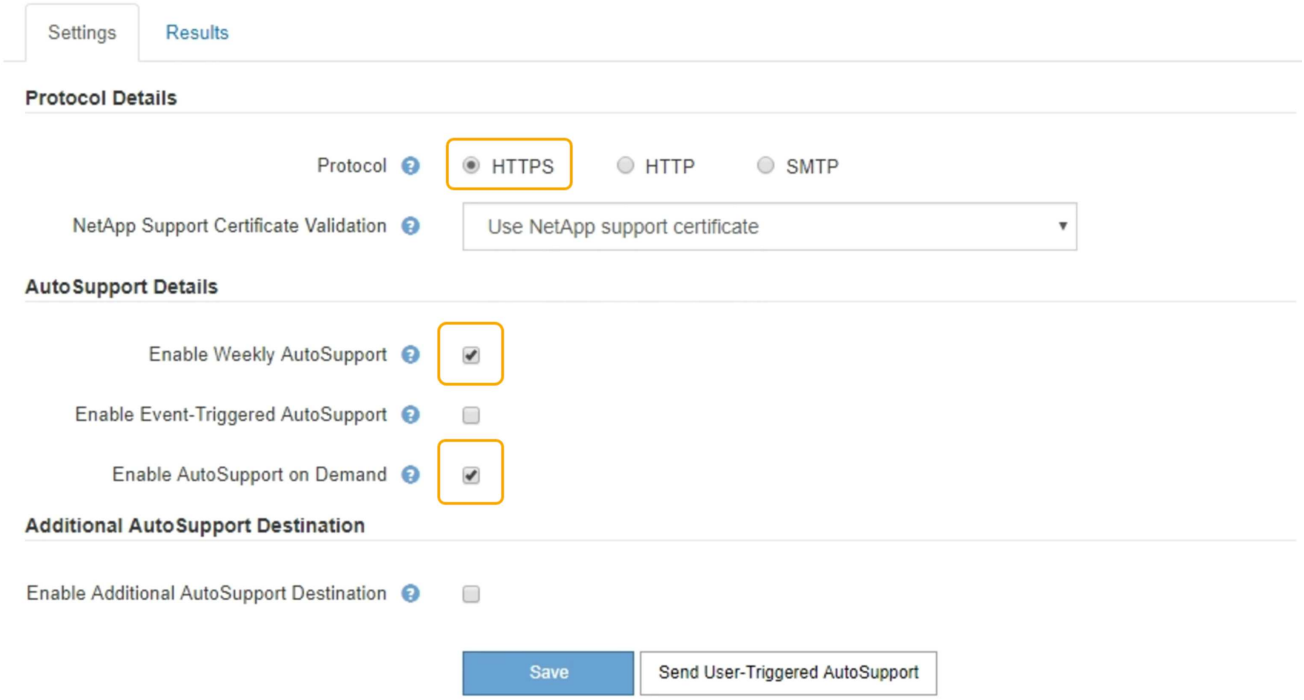
テクニカルサポートは、 AutoSupport On Demand を有効または無効にすることはできません。

手順

1. [サポート（Support ）**]>[***ツール（* Tools ）**]>[** AutoSupport （*）]

   AutoSupport ページが表示され、 * 設定 * タブが選択されます。

2. ページの「* Protocol Details *」セクションで、「HTTPS」ラジオボタンを選択します。



3. [週次 AutoSupport を有効にする *] チェックボックスをオンにします。
4. [オンデマンド AutoSupport を有効にする *] チェックボックスをオンにします。

5. [保存（ Save ）] を選択します。

   AutoSupport On Demand は有効になっており、テクニカルサポートは AutoSupport On Demand 要求を StorageGRID に送信できます。

週次**AutoSupport** メッセージの無効化

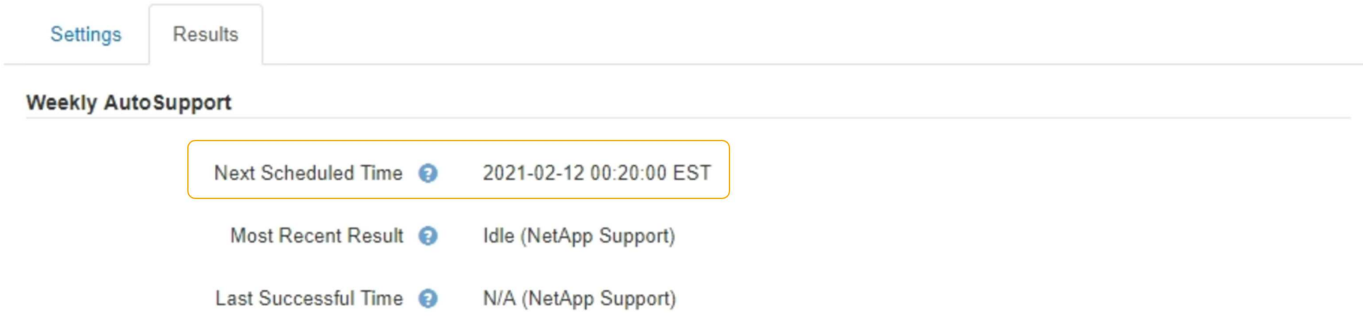
デフォルトでは、 StorageGRID システムは週に 1 回ネットアップサポートに AutoSupport メッセージを送信するように設定されています。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限または Other Grid Configuration 権限が必要です。

このタスクについて

週次AutoSupport メッセージが送信されるタイミングを確認するには、「* AutoSupport **>** Results 」ページの「 Weekly AutoSupport 」の「 Next Scheduled Time *」を参照してください。



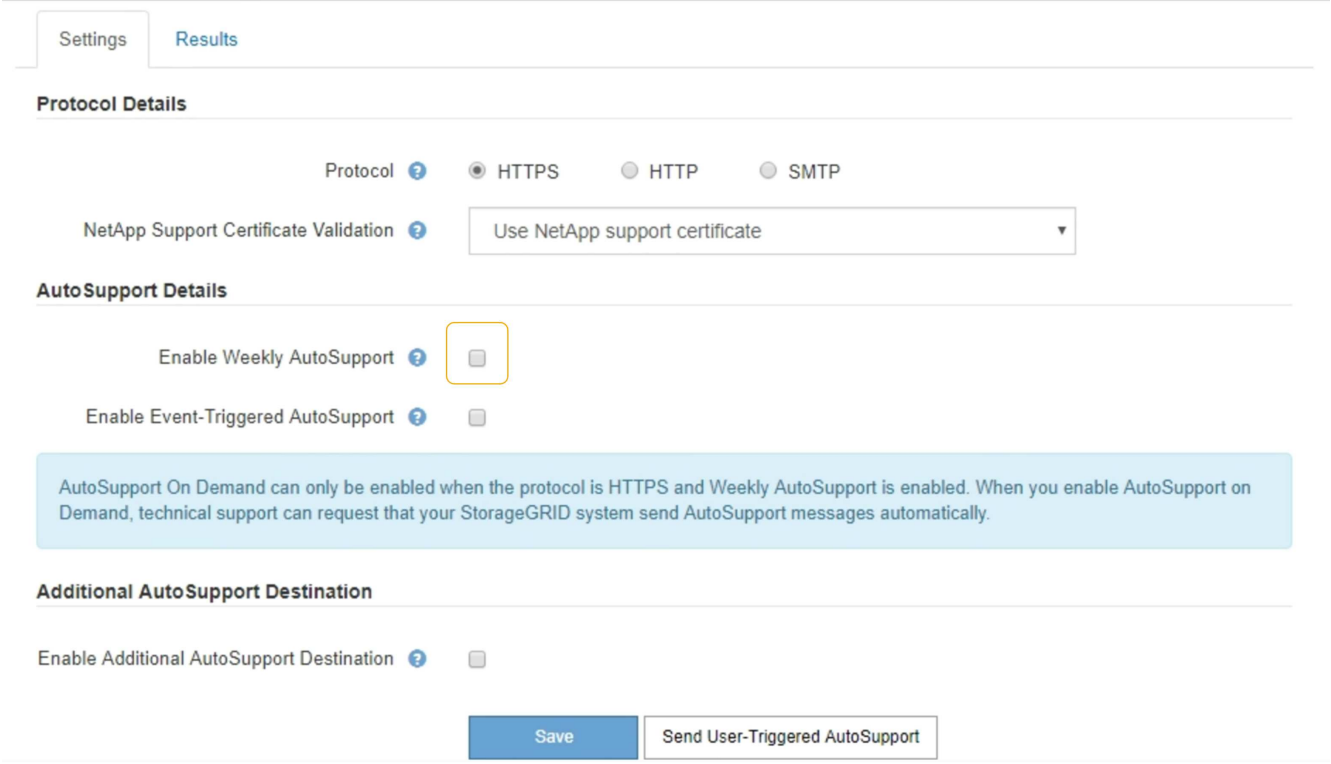
AutoSupport メッセージの自動送信はいつでも無効にすることができます。

手順

1. [サポート（Support ）**]>[***ツール（* Tools ）**]>[** AutoSupport （*）]

   AutoSupport ページが表示され、 * 設定 * タブが選択されます。

2. [毎週AutoSupport を有効にする*]チェックボックスをオフにします。



3. [保存（ Save ）] を選択します。

イベントトリガー型**AutoSupport** メッセージを無効にします

デフォルトでは、 StorageGRID システムは、重要なアラートやその他の重大なシステムイベントが発生したときに AutoSupport メッセージをネットアップサポートに送信するように設定されています。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限または Other Grid Configuration 権限が必要です。

このタスクについて

イベントトリガー型 AutoSupport メッセージはいつでも無効にすることができます。

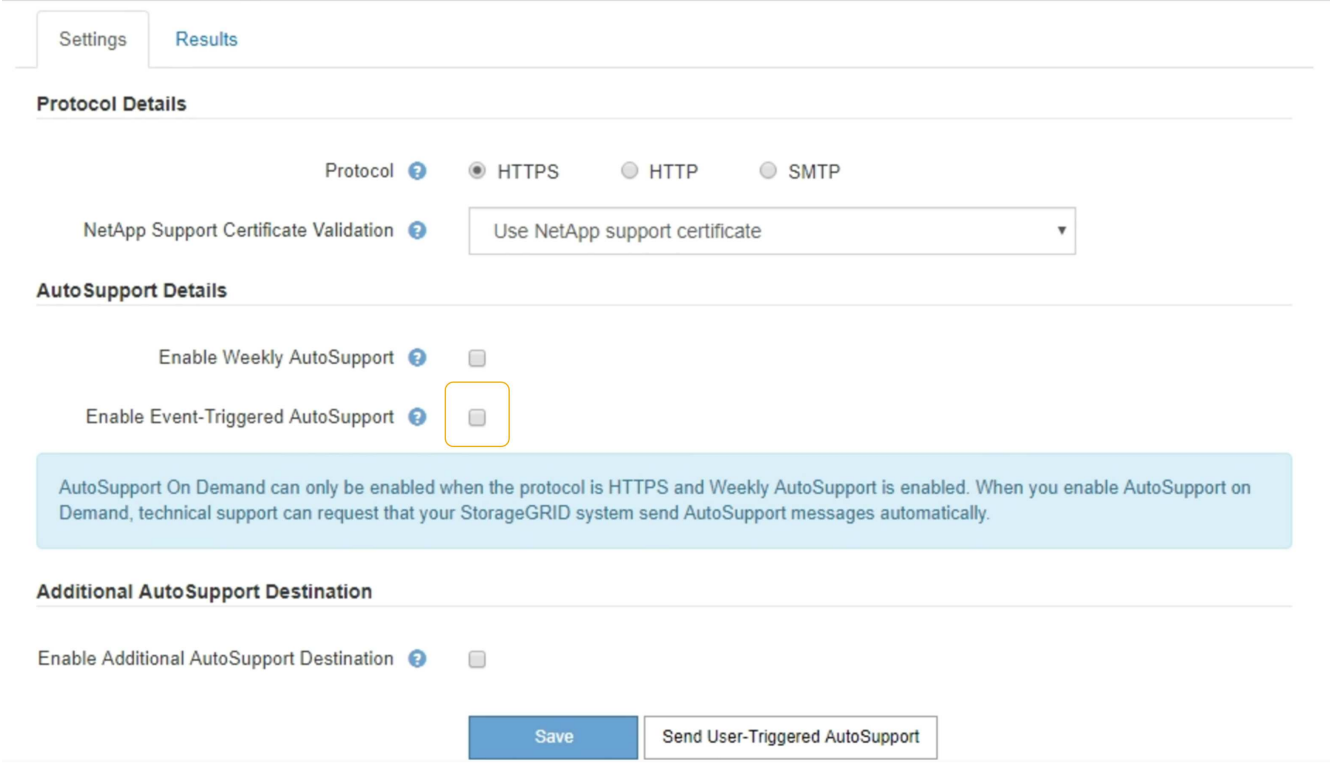
> システム全体で E メール通知を停止した場合は、イベントトリガー型 AutoSupport メッセージも生成されません。（「* Configuration * **System Settings * Display Options *」**（設定*システム設定*表示オプション）を選択します。次に、 [* 通知（ Notification ）] [すべてを抑制（ Suppress All ）] を選択

手順

1. [サポート（Support ）**]>[***ツール（* Tools ）**]>[** AutoSupport （*）]

   AutoSupport ページが表示され、 * 設定 * タブが選択されます。

2. Enable Event-triggered AutoSupport *チェックボックスをオフにします。



3. [保存（ Save ）] を選択します。

手動での**AutoSupport** メッセージのトリガー

テクニカルサポートによる StorageGRID システムの問題のトラブルシューティングを支援するために、 AutoSupport メッセージの送信を手動でトリガーできます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限または Other Grid Configuration 権限が必要です。

手順

1. [サポート（Support ）**]>[***ツール（* Tools ）**]>[** AutoSupport （*）]

   AutoSupport ページが表示され、 * 設定 * タブが選択されます。

2. [ユーザー起動 AutoSupport 送信] を選択します。

   StorageGRID は、テクニカルサポートに AutoSupport メッセージを送信しようとします。試行に成功した場合は、 [結果（ Results ）] タブの [最新結果（ Recent Result ）] * 値と [前回成功した時間（ Last Successful Time ）] * 値が更新されます。問題がある場合、「最新の結果 * 」の値が「失敗」に更新され、 StorageGRID は AutoSupport メッセージの送信を再試行しません。

   ユーザトリガー型 AutoSupport メッセージを送信したあと、 1 分後にブラウザの AutoSupport ページを更新して最新の結果にアクセスします。

AutoSupport デスティネーションを追加しています

AutoSupport を有効にすると、ヘルスメッセージとステータスメッセージがネットアップサポートに送信されます。すべての AutoSupport メッセージに対して、追加の送信先を 1 つ指定できます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限または Other Grid Configuration 権限が必要です。

このタスクについて

AutoSupport メッセージの送信に使用されるプロトコルの確認または変更については、AutoSupport プロトコルの指定手順を参照してください。

SMTP プロトコルを使用して、 AutoSupport メッセージを追加の送信先に送信することはできません。

"AutoSupport メッセージのプロトコルの指定"

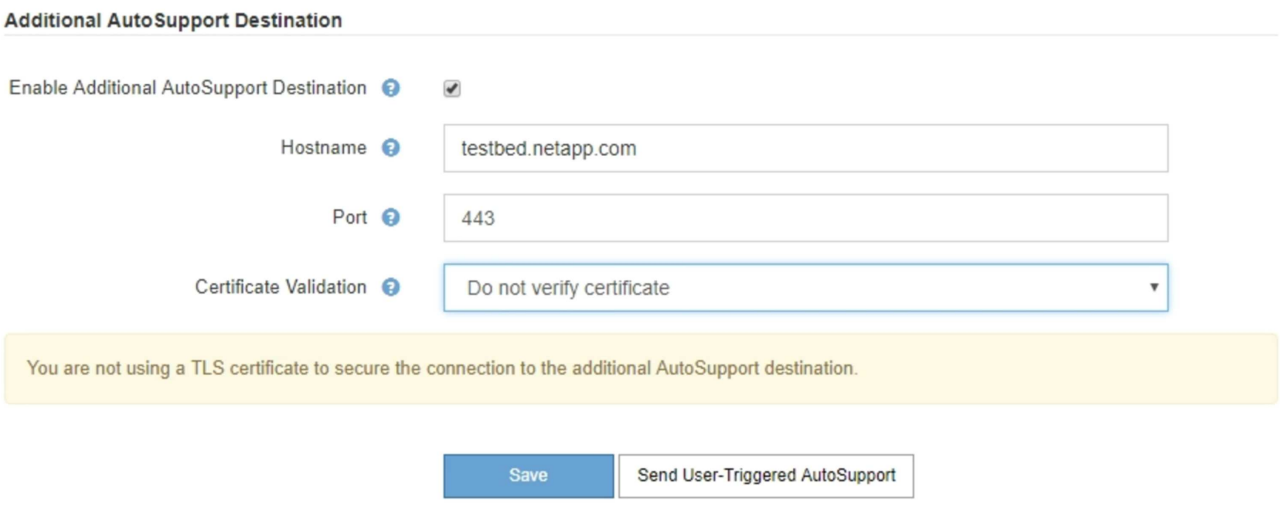
手順

1. [サポート（Support ）**]>[***ツール（* Tools ）**]>[** AutoSupport （*）]

   AutoSupport ページが表示され、 * 設定 * タブが選択されます。

2. [追加の AutoSupport 送信先を有効にする *] を選択します。

   追加の AutoSupport Destination フィールドが表示されます。

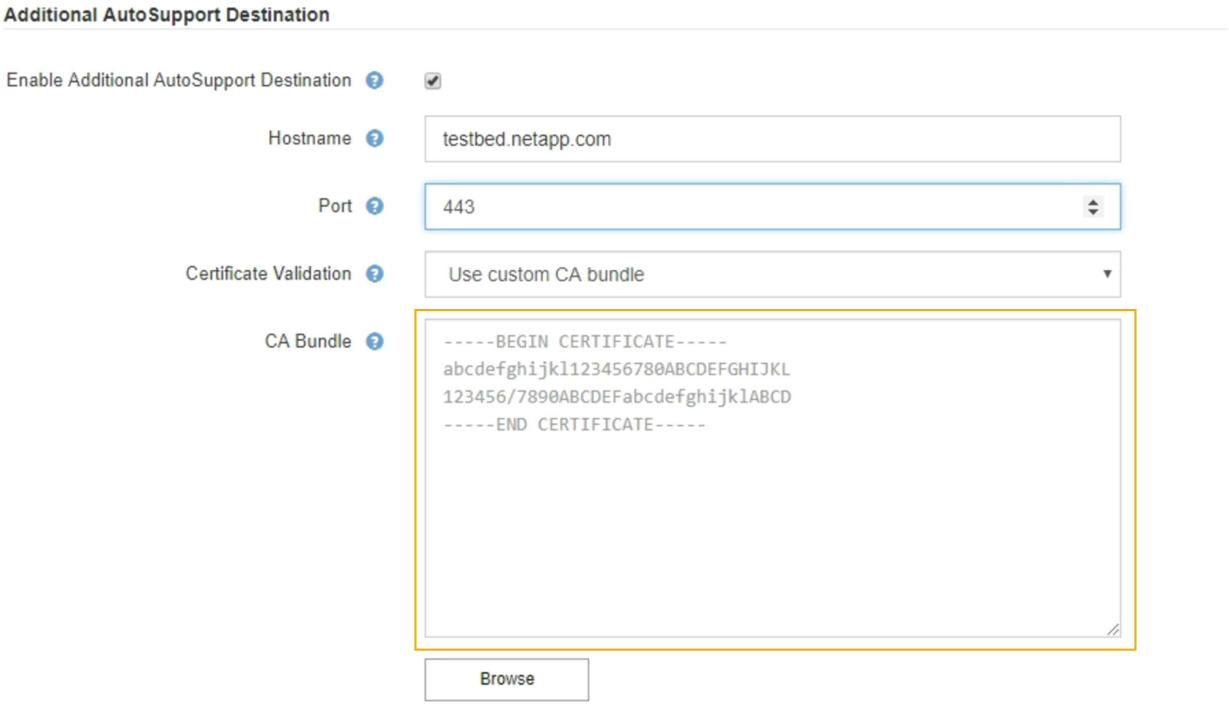


3. 追加の AutoSupport デスティネーションサーバのサーバホスト名または IP アドレスを入力します。

   追加の送信先は 1 つだけ入力できます。

4. 追加の AutoSupport デスティネーションサーバへの接続に使用するポートを入力します（デフォルトは、 HTTP の場合はポート 80 、 HTTPS の場合はポート 443 ）。

5. 証明書の検証とともに AutoSupport メッセージを送信するには、 [証明書の検証 *] ドロップダウンで [カスタム CA バンドルを使用する *] を選択します。次に、次のいずれかを実行します。
   - 編集ツールを使用して、 PEM でエンコードされた各 CA 証明書ファイルのすべての内容を、証明書チェーンの順序で連結された * CA Bundle* フィールドにコピーして貼り付けます。を含める必要があります `----BEGIN CERTIFICATE----` および `----END CERTIFICATE----` を選択します。



   - [* 参照 *] を選択し、証明書が含まれているファイルに移動し、 [* 開く *] を選択してファイルをアップロードします。証明書の検証により、 AutoSupport メッセージの送信を安全に行うことができます。
6. 証明書の検証を行わずに AutoSupport メッセージを送信するには、 [証明書の検証 *] ドロップダウンで [証明書を検証しない *] を選択します。

   このオプションは、証明書の検証を使用しない理由がある場合（証明書に一時的な問題がある場合など）にのみ選択してください。

   「 You are not using a TLS certificate to secure connection to the additional AutoSupport destination. 」というメッセージが表示されます。

7. [保存（ Save ）] を選択します。

   それ以降に送信される毎週、イベントトリガー型、およびユーザトリガー型の AutoSupport メッセージは、すべて追加の送信先に送信されます。

StorageGRID 経由でのEシリーズAutoSupport メッセージの送信

EシリーズSANtricity System ManagerのAutoSupport メッセージは、ストレージアプライアンスの管理ポートではなくStorageGRID 管理ノードからテクニカルサポートに送信できます。

必要なもの

- Grid Managerにはサポートされているwebブラウザを使用してサインインします。
- Storage Appliance Administrator権限またはRoot Access権限が必要です。

> Grid Manager を使用して SANtricity System Manager にアクセスするには、 SANtricity ファームウェア 8.70 以降が必要です。

このタスクについて

E シリーズ AutoSupport メッセージには、ストレージハードウェアの詳細が記載されており、 StorageGRID システムから送信される他の AutoSupport メッセージよりも具体的です。

SANtricity System Manager で特殊なプロキシサーバアドレスを設定して、アプライアンスの管理ポートを使用せずに StorageGRID 管理ノード経由で送信される AutoSupport メッセージを原因 に設定します。この方法で送信される AutoSupport メッセージは、 Grid Manager で設定されている可能性がある優先送信者と管理者のプロキシ設定に基づいています。

Grid Managerで管理プロキシサーバを設定する場合は、管理プロキシの設定手順を参照してください。

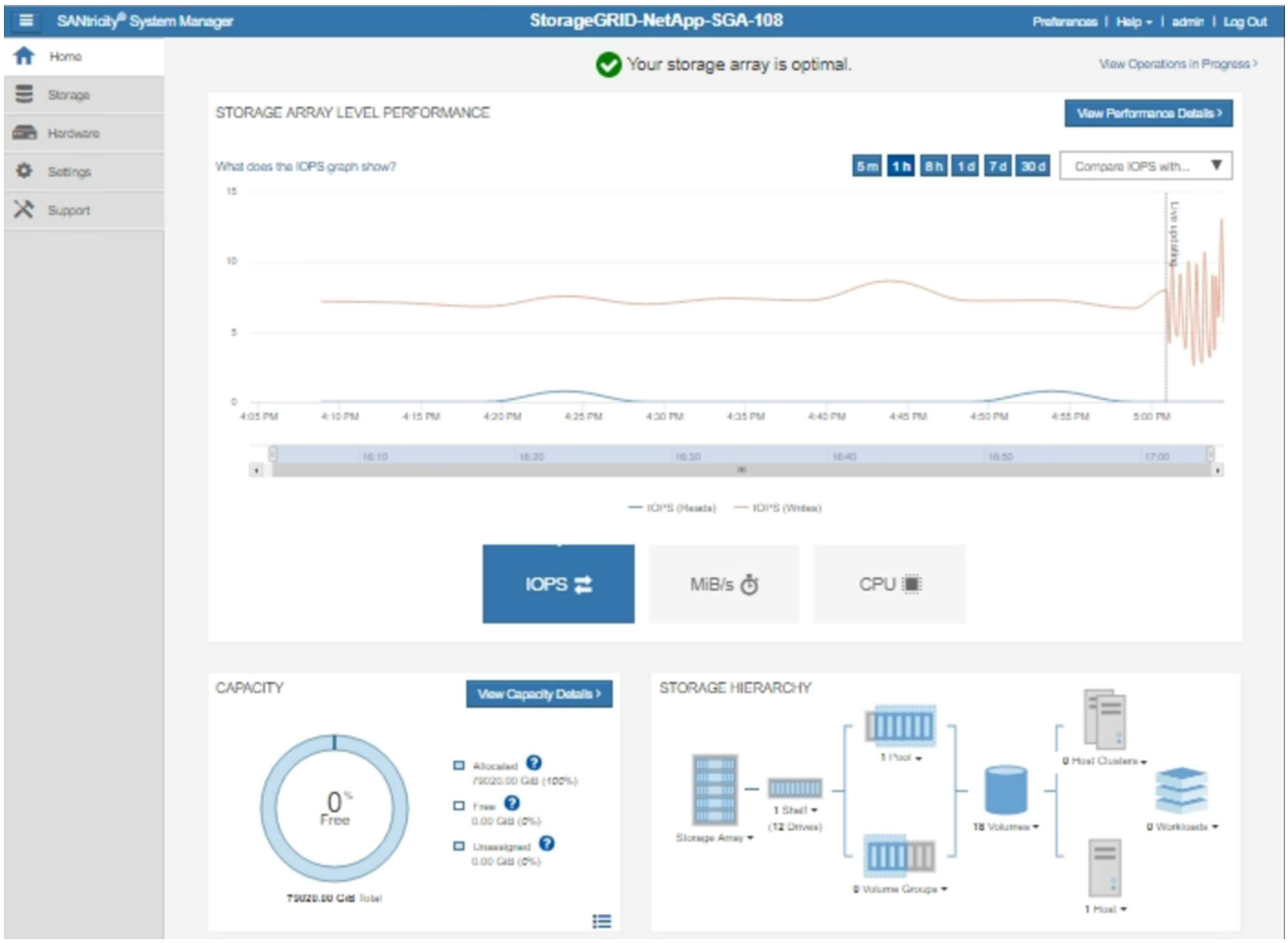
"管理プロキシの設定"

> この手順 は、 E シリーズ AutoSupport メッセージ用に StorageGRID プロキシサーバを設定するためだけに使用します。EシリーズAutoSupport の設定情報の詳細については、Eシリーズのドキュメントセンターを参照してください。
>
> "NetApp Eシリーズシステムのドキュメントセンター"

手順

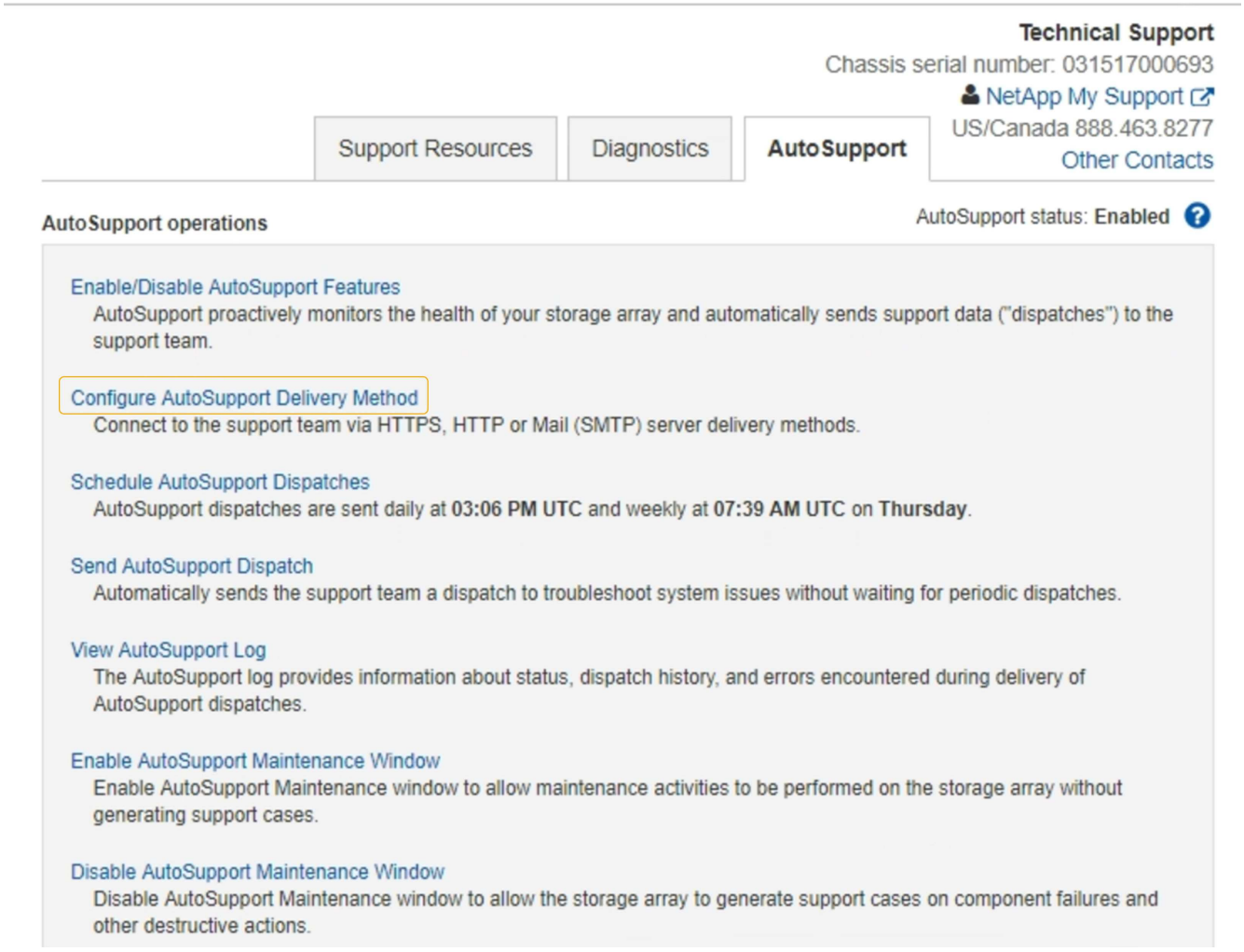
1. Grid Managerで、* Nodes *を選択します。
2. 左側のノードのリストから、設定するストレージアプライアンスノードを選択します。
3. SANtricity System Manager* を選択します。

   SANtricity の System Manager ホームページが表示されます。



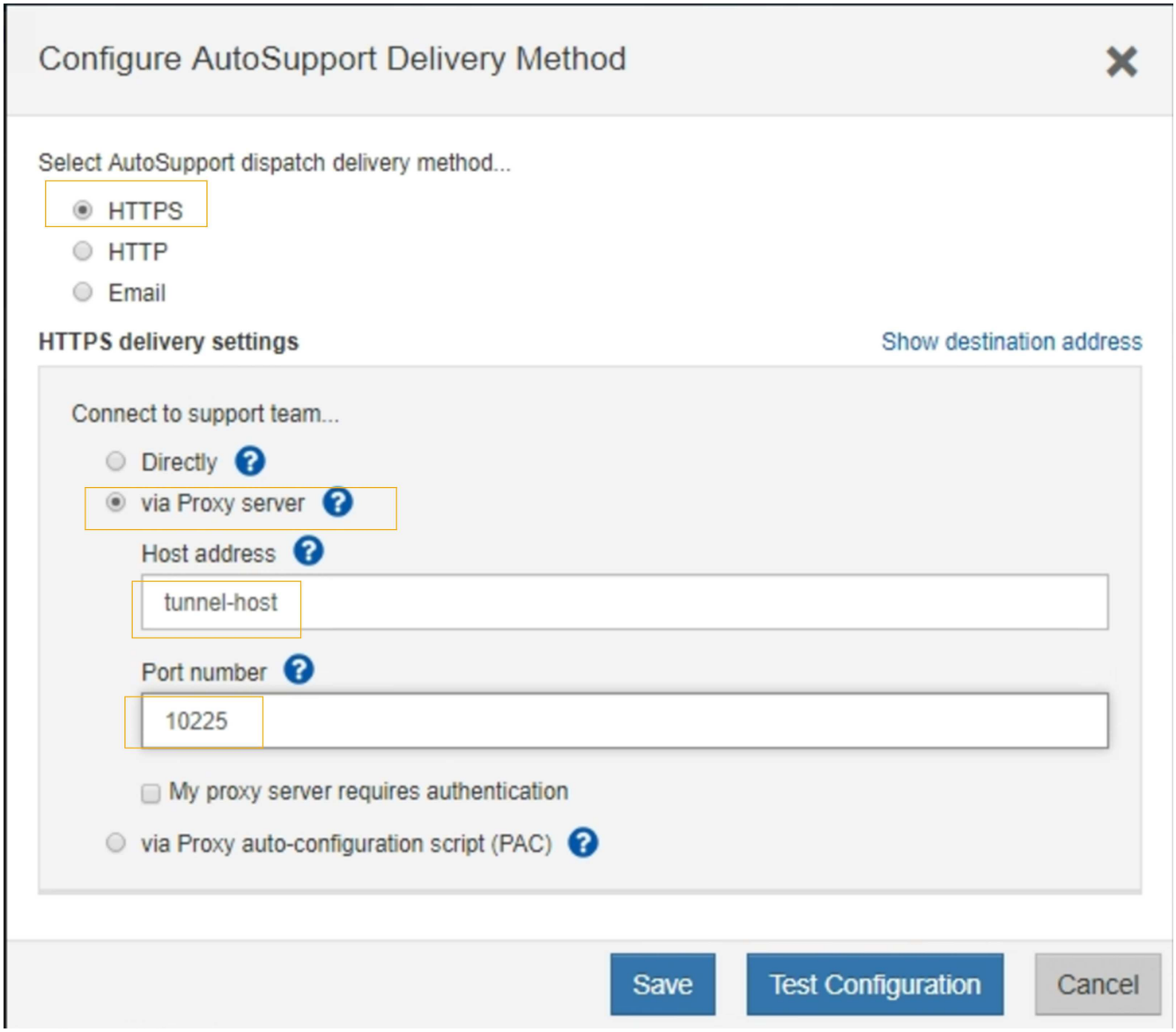
4. [* Support*>]>[* Support center*]>[* AutoSupport *]を選択します。

   AutoSupport operations ページが表示されます。



5. AutoSupport 配信方法の設定 * を選択します。

   AutoSupport 配信方法の設定ページが表示されます。



6. 配信方法として「 * HTTPS * 」を選択します。

   HTTPS プロトコルを有効にする証明書が事前にインストールされています。

7. プロキシサーバー経由 * を選択します。
8. 入力するコマンド `tunnel-host` を入力します。

   `tunnel-host` は、管理ノードを使用してEシリーズAutoSupport メッセージを送信する特別なアドレスです。

9. 入力するコマンド `10225` をクリックします。

   `10225` は、アプライアンスのEシリーズコントローラからAutoSupport メッセージを受信するStorageGRID プロキシサーバのポート番号です。

10. AutoSupport プロキシサーバーのルーティングと設定をテストするには、 * テスト構成 * を選択します。

    正しい場合は、緑色のバナーのメッセージ「 AutoSupport 設定が確認されました。」が表示されます。

テストに失敗した場合は、赤いバナーが表示されます。StorageGRID の DNS 設定とネットワークを確認し、優先送信者である管理ノードがNetApp Support Siteに接続できることを確認してから、もう一度テストを実行してください。

11. [保存（ Save ）] を選択します。

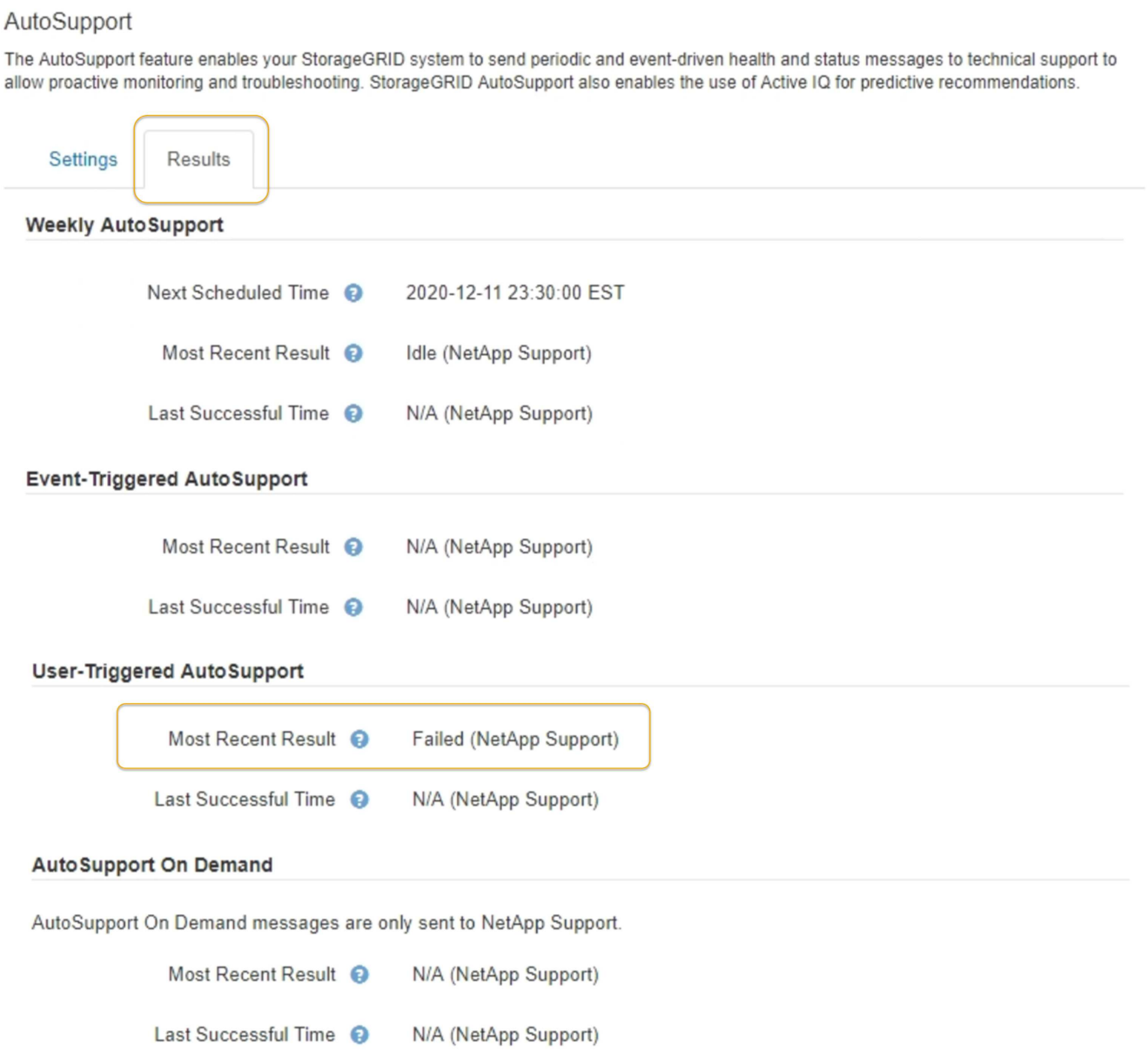
構成が保存され ' AutoSupport 配信方法が構成されましたという確認メッセージが表示されます

AutoSupport メッセージのトラブルシューティング

AutoSupport メッセージの送信が失敗すると、 StorageGRID システムは AutoSupport メッセージのタイプに応じて異なる処理を行います。AutoSupport メッセージのステータスを確認するには、サポート*ツール AutoSupport *結果*を選択します。

E メール通知をシステム全体で停止した場合は、イベントトリガー型 AutoSupport メッセージが生成されなくなります。（「* Configuration * **System Settings** * **Display Options** *」（設定*システム設定*表示オプション）を選択します。次に、 [* 通知（ Notification ）] [すべてを抑制（ Suppress All ）] を選択

AutoSupport メッセージの送信に失敗すると、 AutoSupport ページの * Results * タブに「 Failed 」と表示されます。



週次 **AutoSupport** メッセージのエラーです

週単位の AutoSupport メッセージの送信に失敗した場合、 StorageGRID システムは次の処理を行います。

1. 最新の結果属性を更新して再試行します。
2. 4 分間隔で 15 回、 1 時間 AutoSupport メッセージの再送信を試みます。
3. 送信エラーが 1 時間発生した後、最新の結果属性を失敗に更新します。
4. AutoSupport メッセージの送信を、次にスケジュールされた時刻に再試行します。
5. NMS サービスが利用できないことが原因でメッセージの送信が失敗した場合、および 7 日以内にメッセージが送信された場合は、 AutoSupport の定期送信スケジュールを維持します。
6. 7 日以上メッセージが送信されていない場合は、 NMS サービスが使用可能な状態に戻った時点で AutoSupport メッセージが送信されます。

ユーザトリガー型またはイベントトリガー型の **AutoSupport** メッセージのエラーです

ユーザトリガー型またはイベントトリガー型の AutoSupport メッセージの送信に失敗した場合、StorageGRID システムは次の処理を行います。

1. 既知のエラーの場合は、エラーメッセージが表示されます。たとえば、ユーザが正しいEメール設定を指定せずにSMTPプロトコルを選択した場合、次のエラーが表示されます。 `AutoSupport messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`
2. メッセージの再送信は試行されません。
3. にエラーを記録します `nms.log`。

プロトコルとしてSMTPが選択されている場合に問題が発生した場合は、StorageGRID システムのEメールサーバが正しく設定されていることと、Eメールサーバが実行されていることを確認します（* Support アラーム（レガシー） Legacy Email Setup *）。AutoSupport ページに次のエラーメッセージが表示される場合があります。 `AutoSupport messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

E メールサーバの設定方法については、を参照してください "監視とトラブルシューティングの手順"。

AutoSupport メッセージのエラーの修正

プロトコルとして SMTP が選択されている状況で問題が発生した場合は、 StorageGRID システムの E メールサーバが正しく設定されていることと、 E メールサーバが実行されていることを確認します。AutoSupport ページに次のエラーメッセージが表示される場合があります。 `AutoSupport messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

関連情報

"トラブルシューティングを監視します"

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の容量とサービスを提供します。ストレージノードを管理するには、各ノードの使用可能なスペース量を監視し、しきい値を設定し、ストレージノードの設定を適用します。

- "ストレージノードとは"
- "ストレージオプションの管理"
- "オブジェクトメタデータストレージの管理"
- "格納オブジェクトのグローバル設定"
- "ストレージノード設定"
- "容量が上限に達したストレージノードの管理"

ストレージノードとは

ストレージノードは、オブジェクトデータとメタデータを管理および格納します。各 StorageGRID システムには、少なくとも 3 つのストレージノードが必要です。サイトが

複数ある場合は、 StorageGRID システム内の各サイトにも 3 つのストレージノードが必要です。

ストレージノードには、ディスク上のオブジェクトデータとメタデータを格納、移動、検証し、読み出すために必要なサービスとプロセスを提供します。ストレージノードに関する詳細情報は、* Nodes *ページで確認できます。

ADCサービスとは

Administrative Domain Controller （ ADC ）サービスは、グリッドノードとその相互接続を認証します。ADC サービスは、サイトにある最初の 3 つのストレージノード上でホストされます。

ADC サービスは、サービスの場所や可用性などのトポロジ情報を管理します。あるグリッドノードが別のグリッドノードからの情報を必要とする場合や、別のグリッドノードによる処理を必要とする場合、そのグリッドノードは ADC サービスにアクセスして要求に最適なグリッドノードを見つけます。また、ADCサービスはStorageGRID 環境の設定バンドルのコピーを保持するため、すべてのグリッドノードは現在の設定情報を取得できます。ストレージノードのADC情報は、グリッドトポロジのページ（サポート*グリッドトポロジ）で表示できます。

分散された処理および孤立した処理に対応するため、各 ADC サービスは、証明書、設定バンドル、およびサービスやトポロジに関する情報を、 StorageGRID システム内の他の ADC サービスと同期します。

一般に、すべてのグリッドノードは少なくとも 1 つの ADC サービスへの接続を維持し、これにより、グリッドノードは常に最新情報にアクセスします。ADC サービスに接続したグリッドノードは他のグリッドノードの証明書をキャッシュするため、ある ADC サービスが利用できない場合でも既知のグリッドノードを使用して引き続き機能できます。新しいグリッドノードが接続を確立するためには、 ADC サービスを使用する必要があります。

ADC サービスは接続された各グリッドノードからトポロジ情報を収集します。このグリッドノード情報には、 CPU 負荷、使用可能なディスクスペース（ストレージがある場合）、サポートされているサービス、およびグリッドノードのサイト ID が含まれます。その他のサービスは、トポロジクエリを介して ADC サービスにトポロジ情報を要求します。ADC サービスは、 StorageGRID システムから受信した最新情報で各クエリに応答します。

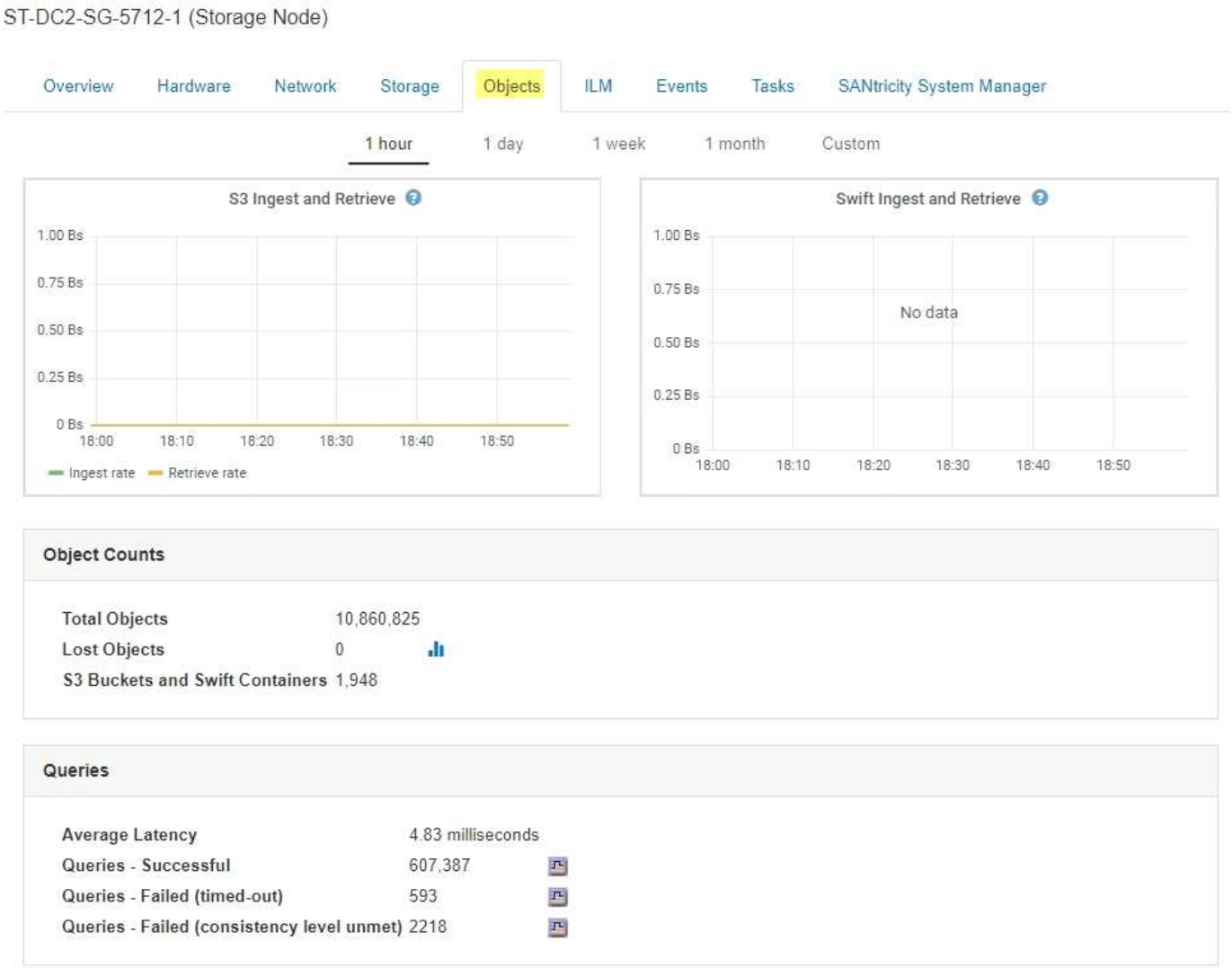
DDSサービスとは

Distributed Data Store （ DDS ）サービスはストレージノードによってホストされ、 Cassandra データベースとのインターフェイスを提供して、 StorageGRID システムに格納されているオブジェクトメタデータに対してバックグラウンドタスクを実行します。

オブジェクト数

DDS サービスは、 StorageGRID システムに取り込まれたオブジェクトの合計数と、システムでサポートされている各インターフェイス（ S3 または Swift ）を使用して取り込まれたオブジェクトの合計数を追跡します。

任意のストレージノードのNodesページのObjectsタブには、Total Objectsの数が表示されます。



クエリ

特定の DDS サービスを使用したメタデータストアに対するクエリの平均実行時間、成功したクエリの合計数、およびタイムアウト問題 が原因で失敗したクエリの合計数を特定できます。

クエリ情報を確認して、メタデータストアである Cassandra の健常性を監視できます。これは、システムの取り込みと読み出しのパフォーマンスに影響します。たとえば、平均的なクエリのレイテンシが遅く、タイムアウトが原因で失敗したクエリの数が多い場合は、メタデータストアの負荷が高いか、または別の処理を実行中である可能性があります。

整合性の問題が原因で失敗したクエリの合計数を確認することもできます。整合性レベルの問題は、特定の DDS サービスを使用してクエリを実行した際に使用可能なメタデータストアの数が不足しているために発生します。

診断ページを使用すると、グリッドの現在の状態の追加情報 を取得できます。を参照してください "診断の実行"。

整合性の保証と制御

StorageGRID は、新しく作成されたオブジェクトのリードアフターライト整合性を保証します。正常に完了した PUT 処理に続く GET 処理では、新しく書き込まれたデータを読み取ることができます。既存のオブジ

ェクトの上書き、メタデータの更新、および削除の整合性レベルは、結果整合性です。

LDRサービスとは

Local Distribution Router （ LDR ）サービスは各ストレージノードによってホストされ、 StorageGRID システムのコンテンツ転送を処理します。コンテンツ転送には、データストレージ、ルーティング、要求処理など、多数のタスクが含まれます。LDR サービスは、データ転送の負荷とデータトラフィック機能を処理し、StorageGRID システムの作業の大部分を担います。

LDR サービスは次のタスクを処理します。

- クエリ
- 情報ライフサイクル管理（ ILM ）のアクティビティ
- オブジェクトの削除
- オブジェクトデータのストレージ
- 別の LDR サービス（ストレージノード）からのオブジェクトデータの転送
- データストレージ管理
- プロトコルインターフェイス（ S3 および Swift ）

また、 LDR サービスは、 StorageGRID システムが取り込まれた各オブジェクトに割り当てる一意な「コンテンツハンドル」（ UUID ）と S3 および Swift オブジェクトのマッピングを管理します。

クエリ

LDR クエリには、読み出しおよびアーカイブ処理におけるオブジェクトの場所のクエリが含まれます。クエリの平均実行時間、成功したクエリの合計数、およびタイムアウト問題 が原因で失敗したクエリの合計数を特定できます。

クエリ情報を確認して、メタデータストアの健常性を監視できます。メタデータストアの健常性は、システムの取り込みと読み出しのパフォーマンスに影響します。たとえば、平均的なクエリのレイテンシが遅く、タイムアウトが原因で失敗したクエリの数が多い場合は、メタデータストアの負荷が高いか、または別の処理を実行中である可能性があります。

整合性の問題が原因で失敗したクエリの合計数を確認することもできます。整合性レベルの問題は、特定の LDR サービスを使用してクエリを実行した際に使用可能なメタデータストアの数が不足しているために発生します。

診断ページを使用すると、グリッドの現在の状態の追加情報 を取得できます。を参照してください "診断の実行"。

ILM アクティビティ

情報ライフサイクル管理（ ILM ）指標を使用すると、 ILM 実装に対してオブジェクトが評価される速度を監視できます。これらの指標は、ダッシュボードまたは各ストレージノードのノードページのILMタブで確認できます。

オブジェクトストア

LDR サービスの基盤となるデータストレージは、一定数のオブジェクトストア（ストレージボリュームとも呼ばれます）に分割されます。各オブジェクトストアは個別のマウントポイントです。

ストレージノードのオブジェクトストアは、ノードページのストレージタブで確認できます。

Object Stores

ID	Size	Available	Replicated Data	EC Data	Object Data (%)	Health
0000	4.40 TB	1.35 TB	43.99 GB	0 bytes	1.00%	No Errors
0001	1.97 TB	1.57 TB	44.76 GB	351.14 GB	20.09%	No Errors
0002	1.97 TB	1.46 TB	43.29 GB	465.20 GB	25.81%	No Errors
0003	1.97 TB	1.70 TB	43.51 GB	223.98 GB	13.58%	No Errors
0004	1.97 TB	1.92 TB	44.03 GB	0 bytes	2.23%	No Errors
0005	1.97 TB	1.46 TB	43.67 GB	463.36 GB	25.73%	No Errors
0006	1.97 TB	1.92 TB	43.10 GB	1.61 GB	2.27%	No Errors
0007	1.97 TB	1.35 TB	46.05 GB	575.24 GB	31.53%	No Errors
0008	1.97 TB	1.81 TB	46.00 GB	112.84 GB	8.06%	No Errors
0009	1.97 TB	1.57 TB	43.91 GB	352.72 GB	20.13%	No Errors
000A	1.97 TB	1.70 TB	44.31 GB	226.81 GB	13.76%	No Errors
000B	1.97 TB	1.92 TB	43.17 GB	780.07 MB	2.23%	No Errors
000C	1.97 TB	1.58 TB	44.32 GB	339.56 GB	19.48%	No Errors
000D	1.97 TB	1.82 TB	44.47 GB	107.34 GB	7.70%	No Errors
000E	1.97 TB	1.68 TB	43.07 GB	241.70 GB	14.45%	No Errors
000F	2.03 TB	1.50 TB	44.57 GB	475.47 GB	25.67%	No Errors

ストレージノード内のオブジェクトストアは、ボリューム ID と呼ばれる 0000 ~ 002F の 16 進数で識別されます。最初のオブジェクトストア（ボリューム 0 ）では、 Cassandra データベースのオブジェクトメタデータ用にスペースがリザーブされます。このボリュームの残りのスペースはオブジェクトデータに使用されます。他のすべてのオブジェクトストアはオブジェクトデータ専用です。オブジェクトデータにはレプリケートコピーとイレイジャーコーディングフラグメントがあります。

レプリケートコピーのスペース使用量を均等にするために、特定のオブジェクトのオブジェクトデータは、使用可能なストレージスペースに基づいて 1 つのオブジェクトストアに格納されます。1 つ以上のオブジェクトストアの容量を使い果たした場合は、ストレージノード上の容量がなくなるまで、残りのオブジェクトストアが引き続きオブジェクトを格納します。

メタデータの保護

オブジェクトメタデータは、オブジェクトの変更時刻や格納場所など、オブジェクトに関連する情報またはオブジェクトの概要 です。StorageGRID は Cassandra データベースにオブジェクトメタデータを格納します。Cassandra データベースは LDR サービスと連携します。

冗長性を確保してオブジェクトメタデータを損失から保護するために、各サイトでオブジェクトメタデータのコピーが 3 つ保持されます。各サイトのすべてのストレージノードに均等にコピーが分散されます。このレプリケーションは設定できず、自動的に実行されます。

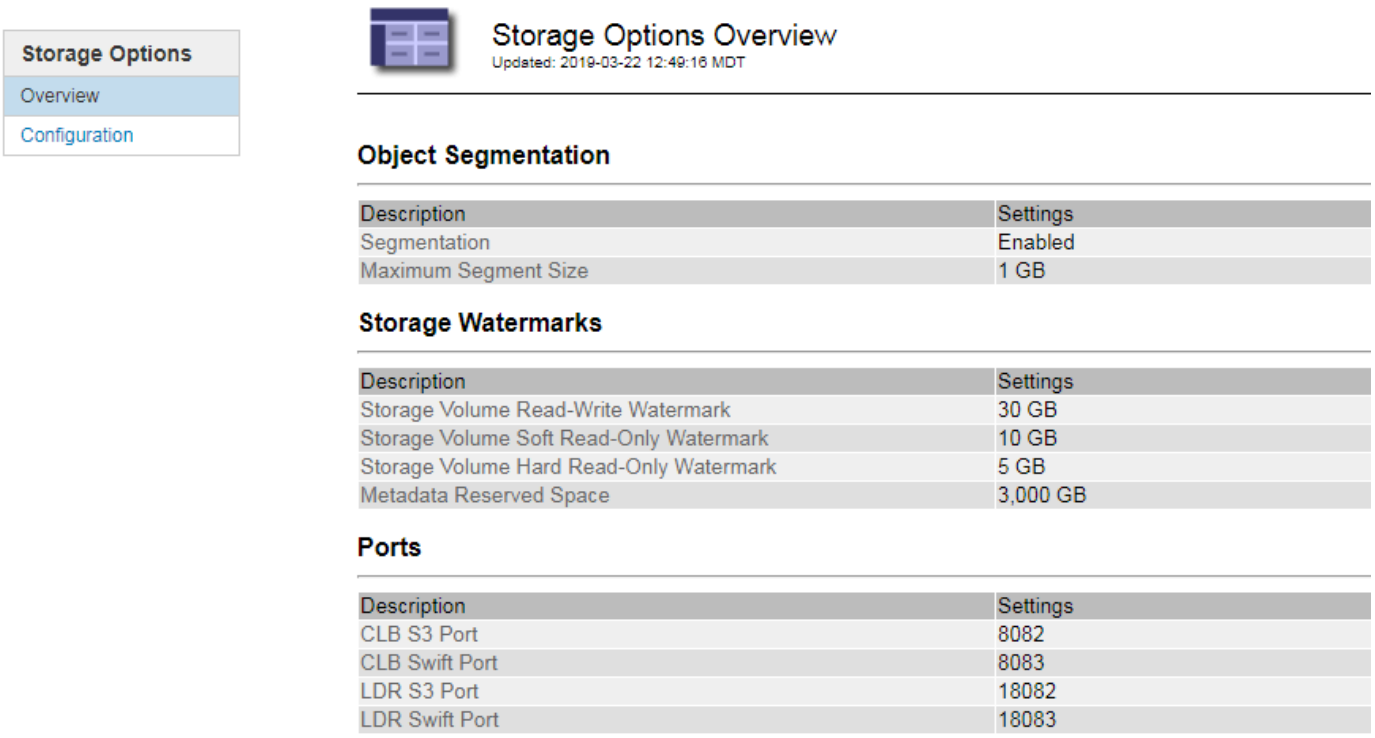
"オブジェクトメタデータストレージの管理"

ストレージオプションの管理

ストレージオプションは、Grid Managerの設定メニューを使用して表示および設定できます。ストレージオプションには、オブジェクトのセグメント化設定と、ストレージウォーターマークの現在の値が含まれます。ゲートウェイノード上の廃止された CLB サー

ビスおよびストレージノード上の LDR サービスで使用されている S3 および Swift ポートを表示することもできます。

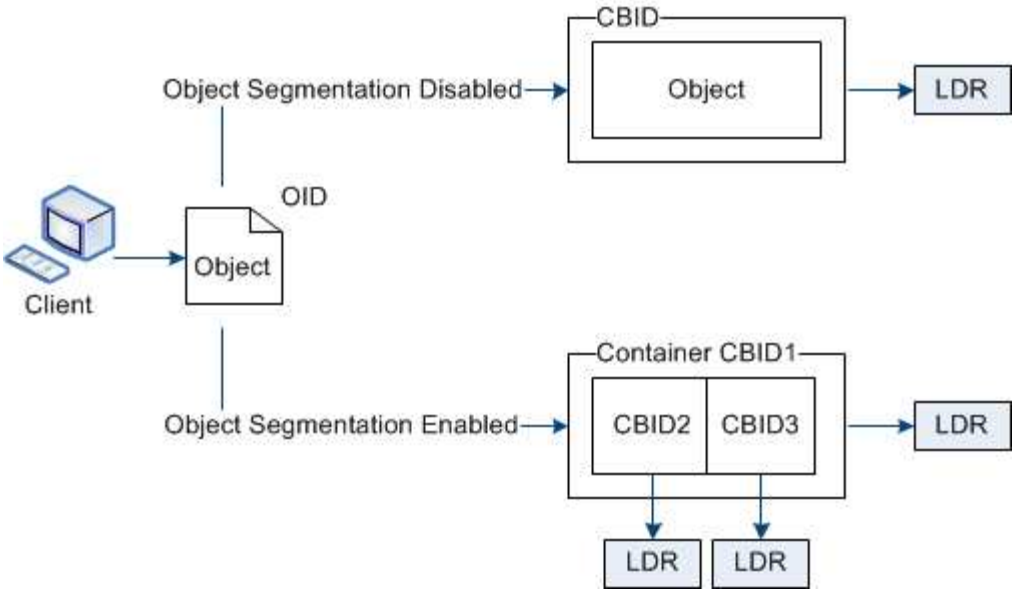
ポート割り当ての詳細については、を参照してください "Summary ：クライアント接続の IP アドレスとポート"。



オブジェクトのセグメント化とは

オブジェクトのセグメント化は、 1 つのオブジェクトを小さな固定サイズのオブジェクトに分割して、大きいオブジェクトによるストレージとリソースの使用を最適化するプロセスです。S3 のマルチパートアップロードでもセグメント化されたオブジェクトが作成され、各パートを表すオブジェクトが 1 つ作成されます。

オブジェクトが StorageGRID システムに取り込まれると、 LDR サービスはオブジェクトを複数のセグメントに分割し、すべてのセグメントのヘッダー情報をコンテンツとして表示するセグメントコンテナを作成します。



StorageGRID システムに、ターゲットタイプが「Cloud Tiering - Simple Storage Service」で、ターゲットのアーカイブストレージシステムがAmazon Web Services（AWS）のアーカイブノードが含まれている場合、最大セグメントサイズは4.5GiB（4、831、838、208バイト）以下にする必要があります。これは、AWS PUTの最大サイズである5GBを超えないようにするための上限です。この値を超えるAWSへの要求は失敗します。

セグメントコンテナを読み出す際、 LDR サービスは各セグメントから元のオブジェクトを組み立て、クライアントに返します。

コンテナとセグメントは同じストレージノードに格納する必要はありません。コンテナとセグメントは任意のストレージノードに格納できます。

各セグメントは StorageGRID システムによって個別に処理され、 Managed Objects や Stored Objects などの属性の対象としてカウントされます。たとえば、 StorageGRID システムに格納されているオブジェクトが 2 つのセグメントに分割された場合、取り込みが完了すると次のように Managed Objects の値が 3 つ増えます。

セグメントコンテナ + セグメント 1 + セグメント 2 = 3 個の格納オブジェクト

大きいオブジェクトを処理する際のパフォーマンスを向上させるには、次の点を確認します。

- 各ゲートウェイおよびストレージノードに、必要なスループットに十分なネットワーク帯域幅があること。たとえば、グリッドネットワークとクライアントネットワークは 10Gbps イーサネットインターフェイス上に別々に設定します。
- 必要なスループットに十分な数のゲートウェイノードとストレージノードが導入されていること。
- 各ストレージノードのディスク IO パフォーマンスが、必要なスループットに対して十分であること。

ストレージボリュームのウォーターマークとは

StorageGRID では、ストレージボリュームのウォーターマークを使用して、ストレージノードで使用可能なスペースの量を監視できます。ノードで使用可能なスペース量が設定されたウォーターマークよりも少なくなると、Storage Status（SSTS）アラームがトリガーされて、ストレージノードを追加する必要があるかどうかを判断できます。

ストレージ・ボリューム・ウォーターマークの現在の設定を表示するには'[構成*ストレージ・オプション*概要*]を選択します

Storage Options Overview

Updated: 2019-10-09 13:09:30 MDT

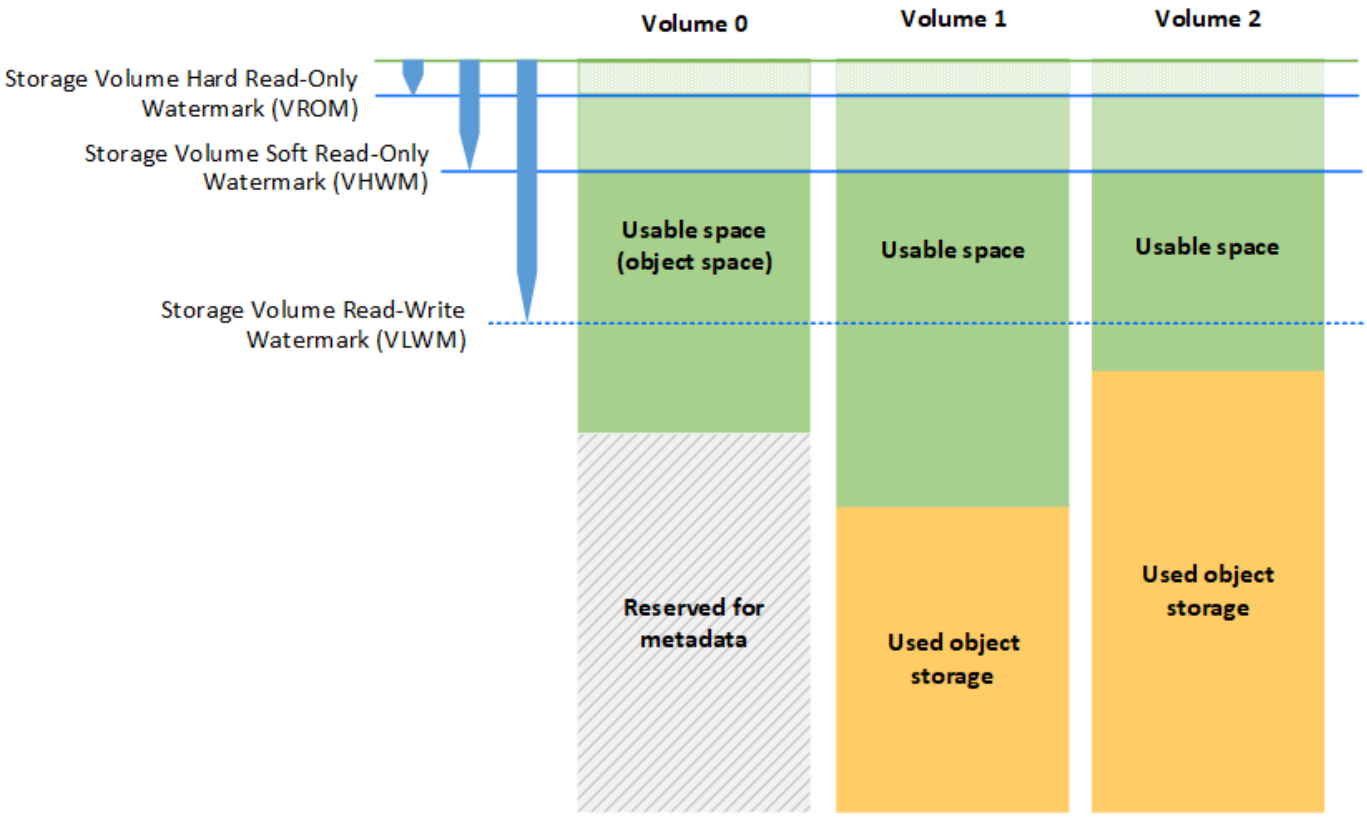
Object Segmentation

Description	Settings
Segmentation	Enabled
Maximum Segment Size	1 GB

Storage Watermarks

Description	Settings
Storage Volume Read-Write Watermark	30 GB
Storage Volume Soft Read-Only Watermark	10 GB
Storage Volume Hard Read-Only Watermark	5 GB
Metadata Reserved Space	3,000 GB

次の図は、ボリュームを3つ含むストレージノードでの、3つのストレージボリュームウォーターマークの相対的な位置を示しています。各ストレージノード内で、StorageGRID がオブジェクトメタデータ用にボリューム0のスペースをリザーブし、そのボリュームの残りのスペースはオブジェクトデータに使用されます。他のすべてのボリュームはオブジェクトデータ専用のボリュームです。オブジェクトデータにはレプリケートコピーとイレイジャーコーディングフラグメントがあります。



ストレージボリュームウォーターマークは、ストレージノード内の各ボリュームに必要な最小空きスペースを示すシステム全体のデフォルト値で、この値を超えると、StorageGRID によってノードの読み取り/書き込み動作が変更されたり、アラームがトリガーされたりします。StorageGRID が処理を実行するには、すべてのボリュームがウォーターマークに達する必要があります。一部のボリュームに必要な最小空きスペース量を超えると、アラームはトリガーされず、ノードの読み取り/書き込み動作も変更されません。

Storage Volume Soft Read-Only Watermark（Vhwm）

Storage Volume Soft Read-Only Watermarkは、オブジェクトデータに使用可能なノードのスペースがフルに近づいていることを示す最初のウォーターマークです。このウォーターマークは'ノードがソフト読み取り専用モードにならないようにするために'ストレージ・ノード内の各ボリュームに必要な空きスペースの量を表しますソフト読み取り専用モードでは、ストレージノードはStorageGRID システムの他の要素にサービスが読み取り専用であることをアドバタイズしますが、保留中の書き込み要求はすべて実行します。

各ボリュームの空きスペース量がこのウォーターマークを下回ると、Storage Status（SSTS）アラームがNoticeレベルでトリガーされ、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。

たとえば、 Storage Volume Soft Read-Only Watermark がデフォルト値の 10GB に設定されているとします。ストレージノード内の各ボリュームの空きスペースが10GB未満になると、SSTSアラームがNoticeレベルでトリガーされ、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。

Storage Volume Hard Read-Only Watermark（VROM）

Storage Volume Hard Read-Only Watermarkは、オブジェクトデータに使用可能なノードのスペースがフルに近づいていることを示す2つ目のウォーターマークです。このウォーターマークは'ノードがハード読み取り専用モードにならないようにするために'ストレージ・ノード内の各ボリュームに必要な空きスペースの量を表しますハード読み取り専用モードでは、ストレージノードは読み取り専用となり、書き込み要求を受け付けません。

ストレージノード内のすべてのボリュームの空きスペース量がこのウォーターマークを下回ると、Storage Status（SSTS）アラームがMajorレベルでトリガーされ、ストレージノードはハード読み取り専用モードに移行します。

たとえば、Storage Volume Hard Read-Only Watermarkがデフォルト値の5GBに設定されているとします。ストレージノード内の各ストレージボリュームの空きスペースが5GB未満になると、SSTSアラームがMajorレベルでトリガーされ、ストレージノードはハード読み取り専用モードに移行します。

Storage Volume Hard Read-Only Watermarkの値は、Storage Volume Soft Read-Only Watermarkの値より小さくする必要があります。

Storage Volume Read-Write Watermark（VLWM）

読み取り専用モードに移行したストレージボリューム読み取り/書き込みウォーターマークのみの環境 ストレージノード。このウォーターマークは、ストレージノードが再度読み取り/書き込み可能になるタイミングを決定します。

たとえば、あるストレージノードがハード読み取り専用モードに移行したとします。Storage Volume Read-Write Watermarkが30GB（デフォルト）に設定されている場合、ノードが再度読み取り/書き込み可能になるためには、ストレージノード内の各ストレージボリュームの空きスペースが5GBから30GBに増える必要があります。

Storage Volume Read-Write Watermarkの値は、Storage Volume Soft Read-Only Watermarkの値より大きくする必要があります。

関連情報

"容量が上限に達したストレージノードの管理"

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、そのシステムに格納できるオブジェクトの最大数を制御します。StorageGRID システムに新しいオブジェクトを格納するための十分なスペースを確保するには、 StorageGRID がオブジェクトメタデータを格納する場所と方法を理解する必要があります。

オブジェクトメタデータとは

オブジェクトメタデータは、オブジェクトについて記述された任意の情報です。StorageGRID では、オブジェクトメタデータを使用してグリッド全体のすべてのオブジェクトの場所を追跡し、各オブジェクトのライフサイクルを継続的に管理します。

StorageGRID のオブジェクトの場合、オブジェクトメタデータには次の種類の情報が含まれます。

- システムメタデータ（各オブジェクトの一意の ID （ UUID ）、オブジェクト名、 S3 バケットまたは

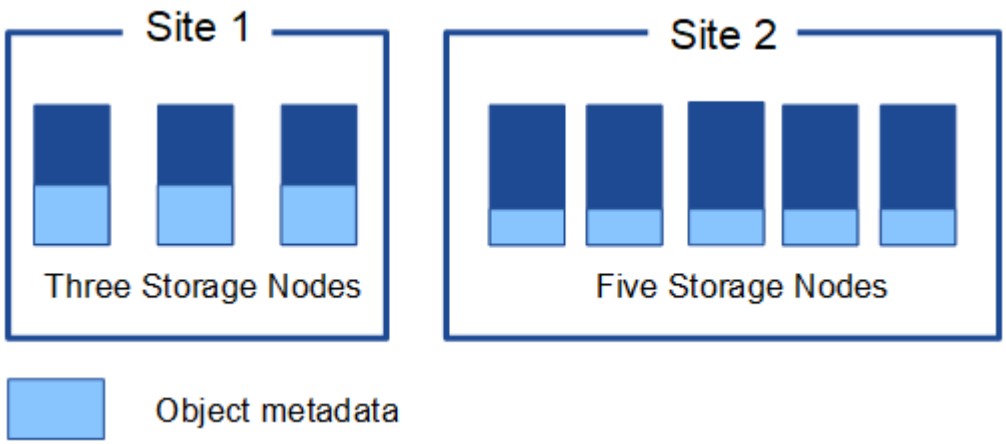
Swift コンテナの名前、テナントアカウントの名前または ID 、オブジェクトの論理サイズ、オブジェクトの作成日時など）、 オブジェクトが最後に変更された日時。

- オブジェクトに関連付けられているカスタムユーザメタデータのキーと値のペア。
- S3 オブジェクトの場合、オブジェクトに関連付けられているオブジェクトタグのキーと値のペア。
- レプリケートオブジェクトコピーの場合、各コピーの現在の格納場所。
- イレイジャーコーディングオブジェクトコピーの場合、各フラグメントの現在の格納場所。
- クラウドストレージプール内のオブジェクトコピーの場合、外部バケットの名前とオブジェクトの一意の識別子を含むオブジェクトの場所。
- セグメント化されたオブジェクトやマルチパートオブジェクトの場合、セグメント ID とデータサイズ。

オブジェクトメタデータの格納方法

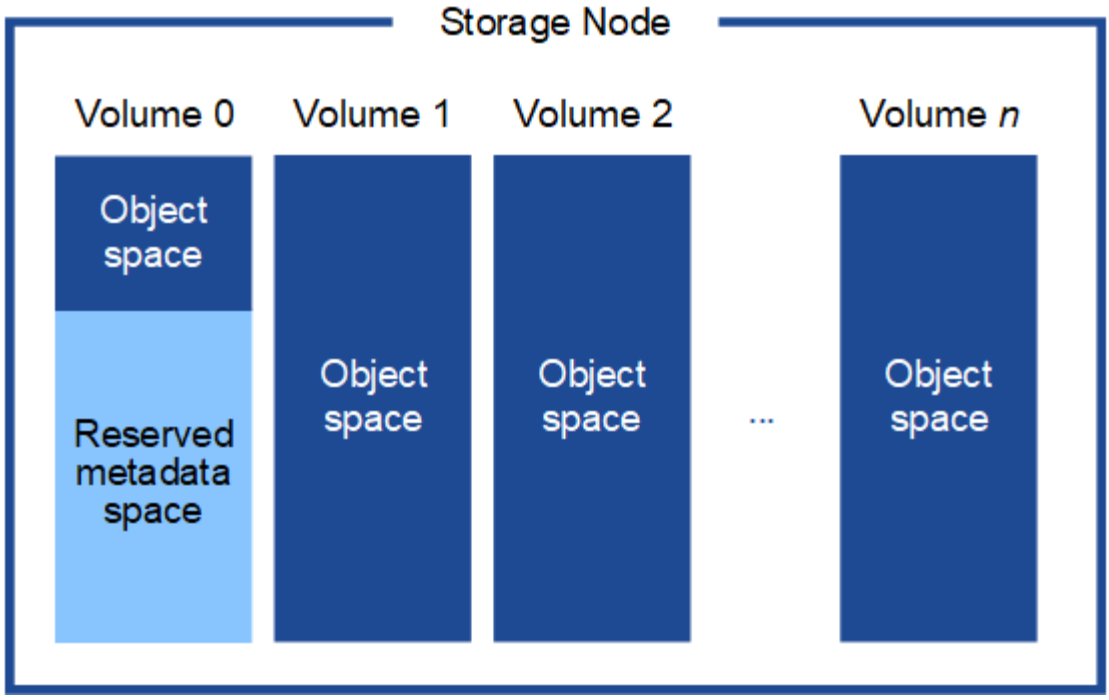
StorageGRID は Cassandra データベースにオブジェクトメタデータを保持し、 Cassandra データベースはオブジェクトデータとは別に格納されます。冗長性を確保し、オブジェクトメタデータを損失から保護するために、 StorageGRID は各サイトのシステム内のすべてのオブジェクトにメタデータのコピーを 3 つずつ格納します。オブジェクトメタデータの 3 つのコピーが各サイトのすべてのストレージノードに均等に分散されます。

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。各サイトに同じ量のオブジェクトメタデータがあり、そのサイトのストレージノード間で均等に分散されます。



オブジェクトメタデータの格納先

この図は、単一のストレージノードのストレージボリュームを表しています。



図に示すように、 StorageGRID は各ストレージノードのストレージボリューム 0 にオブジェクトメタデータ用のスペースをリザーブします。リザーブスペースを使用してオブジェクトメタデータを格納し、重要なデータベース処理を実行します。ストレージボリューム 0 の残りのスペースとストレージノード内のその他すべてのストレージボリュームは、オブジェクトデータ（レプリケートコピーとイレイジャーコーディングフラグメント）専用に使用されます。

特定のストレージノードでオブジェクトメタデータ用にリザーブされているスペースの量は、次に示すいくつかの要因によって決まります。

Metadata Reserved Space の設定

Metadata Reserved Space _ は、各ストレージノードのボリューム 0 でメタデータ用にリザーブされるスペースの量を表すシステム全体の設定です。次の表に、StorageGRID 11.5のこの設定のデフォルト値を示します。

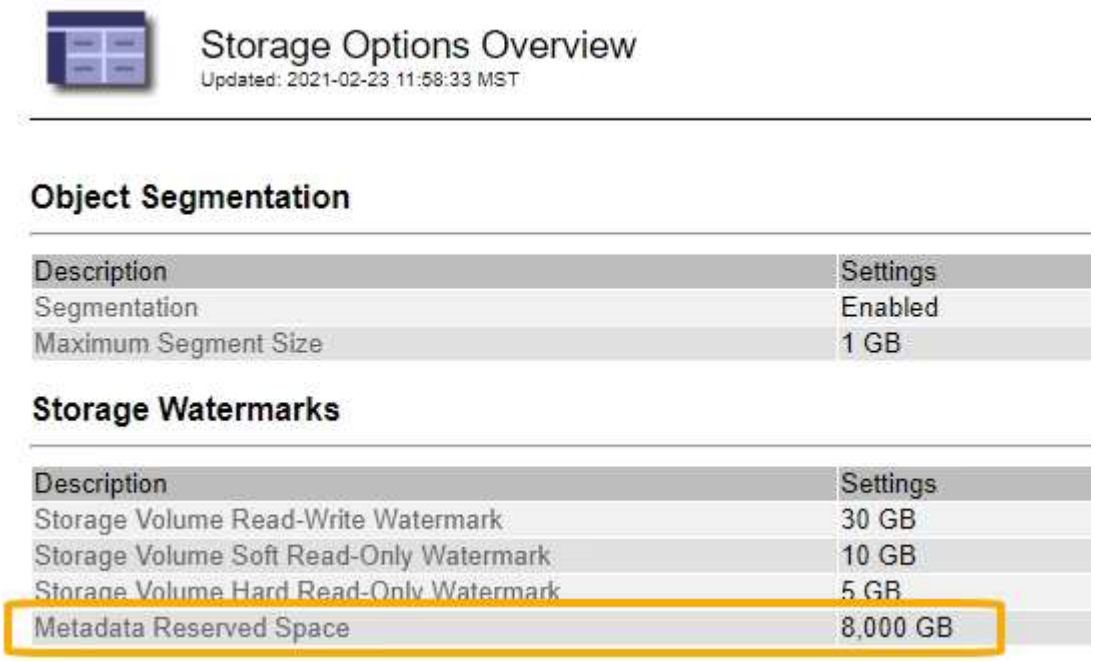
- StorageGRID の最初のインストール時に使用していたソフトウェアバージョン。
- 各ストレージノード上の RAM の容量。

StorageGRID の初期インストールに使用するバージョン	ストレージノード上の **RAM** の容量	**StorageGRID 11.5** のデフォルトの**Metadata Reserved Space**設定
11.5	グリッド内の各ストレージノードで 128GB 以上	8 TB （ 8 、 000 GB ）
	グリッド内の任意のストレージノードで 128GB 未満	3TB （ 3 、 000GB ）
11.1 ～ 11.4	いずれかのサイトの各ストレージノードで 128GB 以上	4TB （ 4 、 000GB ）

StorageGRID の初期インストールに使用するバージョン	ストレージノード上の **RAM** の容量	**StorageGRID 11.5** のデフォルトの**Metadata Reserved Space**設定
	各サイトのストレージノードで 128GB 未満	3TB （ 3 、 000GB ）
11.0 以前	任意の金額	2TB （ 2 、 000 GB ）

StorageGRID システムの Metadata Reserved Space 設定を表示するには、次の手順を実行します。

1. * Configuration **>** System Settings **>** Storage Options *を選択します。
2. Storage Watermarks テーブルで、 * Metadata Reserved Space * を探します。



スクリーンショットでは、「 * Metadata Reserved Space * 」の値が 8 、 000 GB （ 8 TB ）になっています。StorageGRID 11.5の新規インストールでは、各ストレージノードに128GB以上のRAMが搭載されます。

メタデータ用にリザーブされている実際のスペース

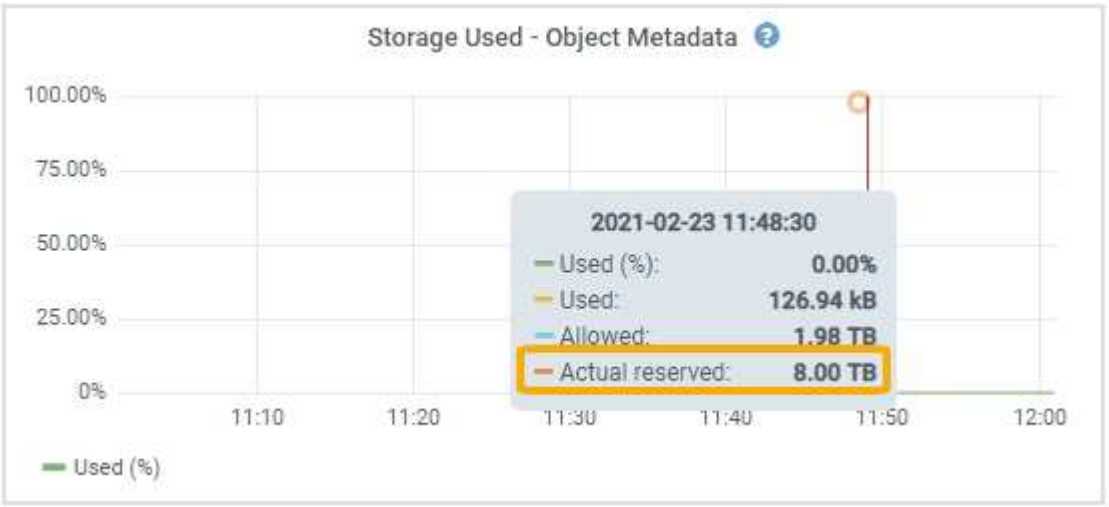
システム全体の Metadata Reserved Space 設定とは異なり、オブジェクトメタデータ用の実際のリザーブスペースは、ストレージノードごとに決定されます。ある特定のストレージノードについて、メタデータ用に実際にリザーブされるスペースは、ノードのボリューム 0 のサイズとシステム全体の * Metadata Reserved Space * 設定によって異なります。

ノードのボリューム **0** のサイズ	メタデータ用にリザーブされている実際のスペース
500GB 未満（非本番環境で使用）	ボリューム 0 の 10%

ノードのボリューム **0** のサイズ	メタデータ用にリザーブされている実際のスペース
500GB 以上	次の値のうち小さい方： • ボリューム 0 • Metadata Reserved Space の設定

特定のストレージノードでメタデータ用にリザーブされている実際のスペースを表示するには、次の手順を実行します

1. Grid Managerから* Nodes *>*_ Storage Node_*を選択します。
2. [* ストレージ *] タブを選択します。
3. 「使用済みストレージ — オブジェクトメタデータ」グラフにカーソルを合わせ、「実際に予約されている容量 * 」の値を探します。



スクリーンショットでは、実際の予約数 * の値は 8TB です。このスクリーンショットは、StorageGRID 11.5 を新規にインストールした大規模ストレージノードを示しています。システム全体の Metadata Reserved Space 設定がこのストレージノードのボリューム 0 よりも小さいため、このノードの実際のリザーブスペースは Metadata Reserved Space 設定と同じです。

actual reserved *値は次のPrometheus指標に対応します。

```
storagegrid_storage_utilization_metadata_reserved_bytes
```

実際にリザーブされているメタデータスペースの例

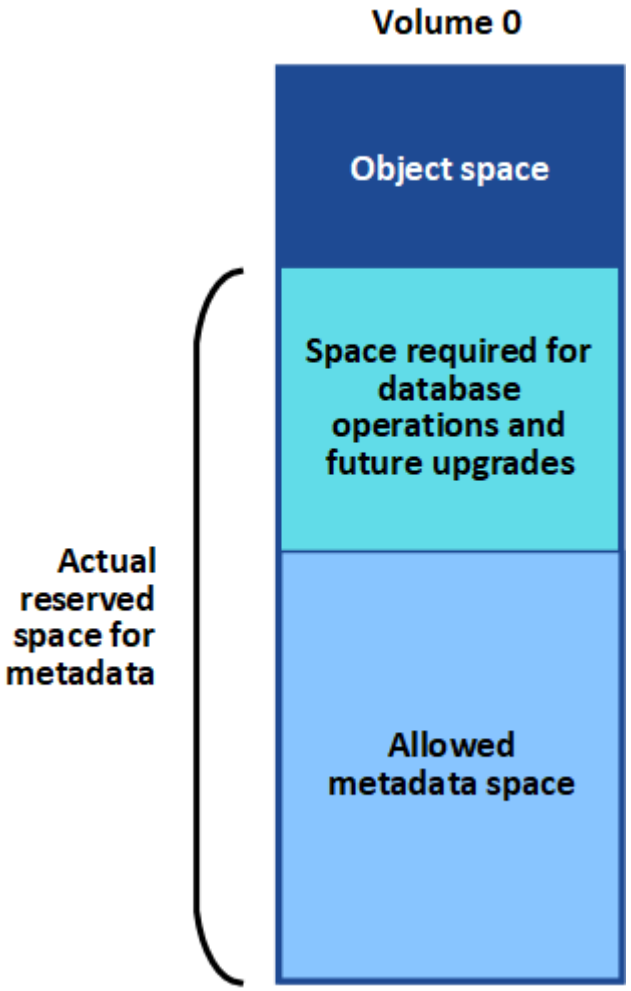
バージョン11.5を使用して新しいStorageGRID システムをインストールするとします。この例では、各ストレージノードの RAM が 128GB を超え、ストレージノード 1 （ SN1 ）のボリューム 0 が 6TB であるとします。次の値に基づきます。

- システム全体の * Metadata Reserved Space * が 8TB に設定されている（ストレージノードごとに128GBを超えるRAMが搭載されている場合、この値はStorageGRID 11.5の新規インストールでのデフォルト値です）。

- SN1 のメタデータ用にリザーブされている実際のスペースは 6TB です。（ボリューム 0 が * Metadata Reserved Space * 設定より小さいため、ボリューム全体がリザーブされます）。

許可されているメタデータスペースです

メタデータ用に実際に予約されている各ストレージノードは、オブジェクトメタデータに使用できるスペース（許容されるメタデータスペース _ ）と、重要なデータベース処理（コンパクションや修復など）や将来のハードウェアおよびソフトウェアのアップグレードに必要なスペースに分割されます。許可されるメタデータスペースは、オブジェクトの全体的な容量を決定します。



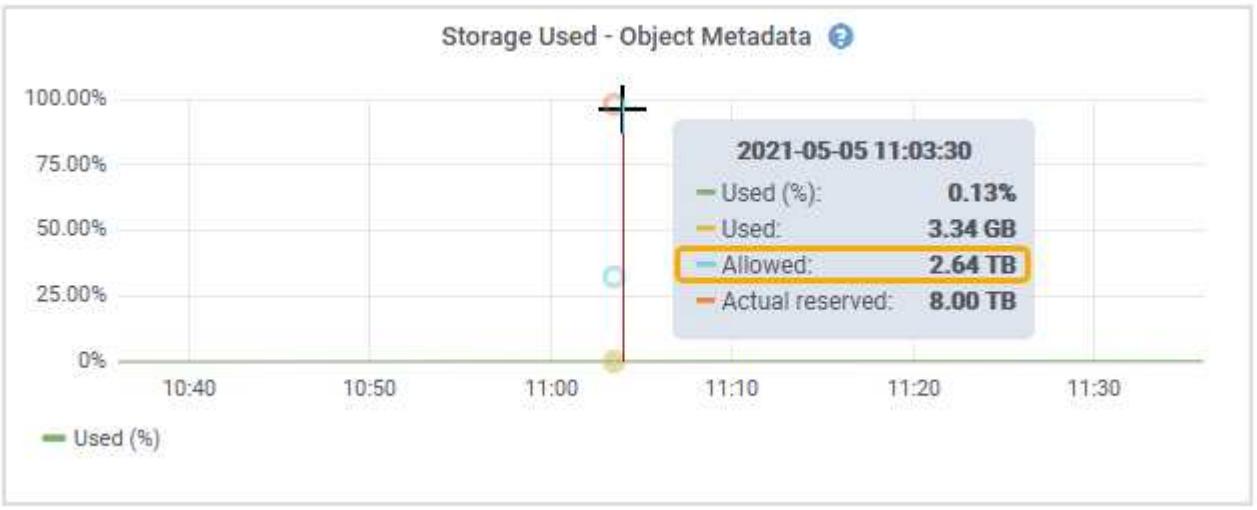
次の表は、 StorageGRID がストレージノードで許可されるメタデータスペースの値をどのように決定するかを示しています。

メタデータ用にリザーブされている実際のスペース	許可されているメタデータスペースです
4TB以下	メタデータ用にリザーブされている実際のスペースの 60% 。最大 1.98 TB
4TBを超える	（メタデータ用に実際にリザーブされるスペース−1TB）×60%、最大2.64 TB

StorageGRID システムで任意のストレージノードに2.64TBを超えるメタデータを格納（または格納する予定がある場合）がある場合、許可されるメタデータスペースが増加することがあります。各ストレージノードのRAMが128GBを超え、かつストレージボリューム0に空きスペースがある場合は、ネットアップの営業担当者にお問い合わせください。要件を確認し、可能であれば各ストレージノードで許可されているメタデータスペースを増やします。

ストレージノードで使用可能なメタデータスペースを表示するには、次の手順を実行します。

1. Grid Managerから* Node *>*_ 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」グラフにカーソルを合わせ、「使用可能な値 * 」を探します。



スクリーンショットでは、「許可」の値は 2.64TB です。これは、メタデータ用に実際にリザーブされているスペースが 4TB を超えるストレージノードの最大値です。

「 * Allowed * 」の値は、次の Prometheus 指標に対応します。

```
storagegrid_storage_utilization_metadata_allowed_bytes
```

許可されるメタデータスペースの例

バージョン11.5を使用してStorageGRID システムをインストールするとします。この例では、各ストレージノードの RAM が 128GB を超え、ストレージノード 1 （ SN1 ）のボリューム 0 が 6TB であるとします。次の値に基づきます。

- システム全体の * Metadata Reserved Space * が 8TB に設定されている（各ストレージノードのRAMが128GBを超えている場合、StorageGRID 11.5のデフォルト値です）。
- SN1 のメタデータ用にリザーブされている実際のスペースは 6TB です。（ボリューム 0 が * Metadata Reserved Space * 設定より小さいため、ボリューム全体がリザーブされます）。
- SN1 でメタデータに使用できるスペースは 2.64 TB です。（実際のリザーブスペースの最大値です）。

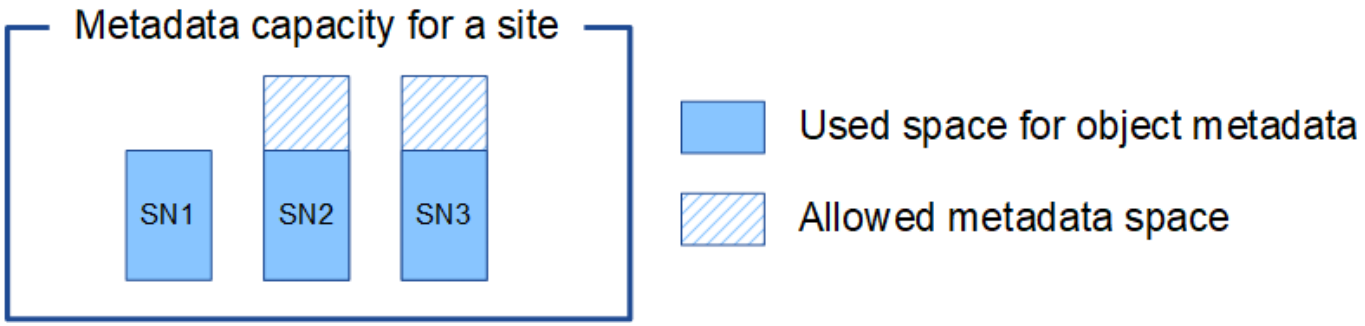
前述したように、 StorageGRID は各サイトのストレージノードにオブジェクトメタデータを均等に分散します。このため、サイトにサイズが異なるストレージノードがある場合、サイトで一番小さいノードがサイトのメタデータ容量を決定します。

次の例を考えてみましょう。

- サイズの異なる 3 つのストレージノードを含む単一サイトのグリッドがある。
- Metadata Reserved Space * の設定は 4TB です。
- ストレージノードには、リザーブされている実際のメタデータスペースと許可されているメタデータスペースについて、次の値があります。

ストレージノード	ボリューム **0** のサイズ	リザーブされている実際のメタデータスペースです	許可されているメタデータスペースです
SN1.	2.2 TB	2.2 TB	1.32TB をサポートします
SN2.	5 TB	4 TB	1.98 TB
SN3	6TB	4 TB	1.98 TB

オブジェクトメタデータはサイトのストレージノード間で均等に分散されるため、この例の各ノードが格納できるメタデータは 1.32TB です。SN2 と SN3 で許可されるメタデータスペースのうち、 0.66TB を追加で使用することはできません。



同様に、 StorageGRID は各サイトで StorageGRID システムのすべてのオブジェクトメタデータを管理するため、 StorageGRID システム全体のメタデータ容量は最小サイトのオブジェクトメタデータ容量で決まります。

また、オブジェクトメタデータの容量はオブジェクトの最大数に制御されるため、一方のノードがメタデータの容量を超えると、実質的にグリッドがフルになります。

関連情報

- 各ストレージノードのオブジェクトメタデータ容量を監視する方法については、次の資料を参照してください。

  "トラブルシューティングを監視します"

- システムのオブジェクトメタデータ容量を増やすには、新しいストレージノードを追加する必要があります。

  "グリッドを展開します"

格納オブジェクトのグローバル設定

グリッドオプションを使用すると、 StorageGRID システムに格納されているすべてのオブジェクトについて、格納オブジェクトの圧縮や格納オブジェクトの暗号化などの設定を行うことができます。設定を行うことができます。

- "格納オブジェクトの圧縮を設定しています"
- "格納オブジェクトの暗号化を設定する"
- "格納オブジェクトのハッシュの設定"

格納オブジェクトの圧縮を設定しています

[格納オブジェクトの圧縮] グリッドオプションを使用すると、 StorageGRID に格納されているオブジェクトのサイズを縮小して、オブジェクトのストレージ消費量を抑えることができます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

このタスクについて

デフォルトでは、 [格納オブジェクトの圧縮] グリッドオプションは無効になっています。このオプションを有効にすると、 StorageGRID は、ロスレス圧縮を使用して各オブジェクトを保存時に圧縮します。

この設定を変更すると、新しい設定が適用されるまで約 1 分かかります。設定した値は、パフォーマンスと拡張用にキャッシュされます。

このオプションを有効にする前に、次の点に注意してください。

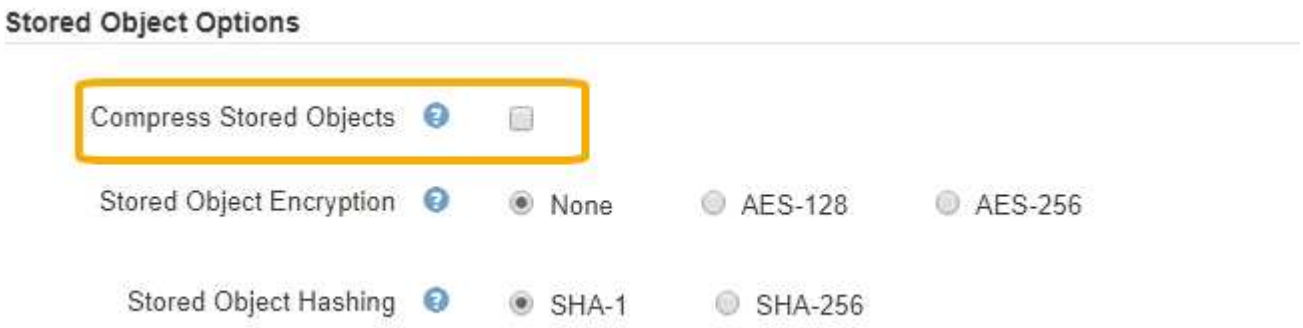
- 格納されるデータの圧縮率がわかっている場合を除き、圧縮を有効にしないでください。
- StorageGRID にオブジェクトを保存するアプリケーションは、オブジェクトを圧縮してから保存することがあります。クライアントアプリケーションがオブジェクトを StorageGRID に保存する前に圧縮している場合は、 [格納オブジェクトの圧縮] を有効にしてもオブジェクトのサイズはさらに縮小されません。
- NetApp FabricPool と StorageGRID を併用する場合は、圧縮を有効にしないでください。
- Compress Stored Objects グリッドオプションを有効にした場合は、 S3 および Swift クライアントアプリケーションでバイト範囲を指定した GET Object 処理を実行しないでください。StorageGRID は要求されたバイトにアクセスするためにオブジェクトを圧縮解除する必要があるため ' これらの “range read” 操作は非効率的です非常に大きなオブジェクトから小さい範囲のバイト数を要求する GET Object 処理は特に効率が悪く、たとえば、 50GB の圧縮オブジェクトから 10MB の範囲を読み取る処理は非効率的です。

  圧縮オブジェクトから範囲を読み取ると、クライアント要求がタイムアウトする可能性があります。

オブジェクトを圧縮する必要があり、クライアントアプリケーションが範囲読み取りを使用する必要がある場合は、アプリケーションの読み取りタイムアウトを増やしてください。

手順

1. 「環境設定*システム設定*グリッドオプション*」を選択します。
2. [格納オブジェクトのオプション] セクションで、 [格納オブジェクトの圧縮 *] チェックボックスをオンにします。



3. [保存（ Save ）] をクリックします。

格納オブジェクトの暗号化を設定する

オブジェクトストアが侵害された場合に読み取り可能な形式でデータを読み出せないようにするには、格納オブジェクトを暗号化します。デフォルトでは、オブジェクトは暗号化されません。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

このタスクについて

格納オブジェクトの暗号化を使用すると、 S3 または Swift 経由で取り込まれたすべてのオブジェクトデータを暗号化できます。この設定を有効にすると、新たに取り込まれたすべてのオブジェクトが暗号化されますが、既存の格納オブジェクトに対する変更はありません。暗号化を無効にすると、現在暗号化されているオブジェクトは暗号化されたままですが、新しく取り込まれたオブジェクトは暗号化されませ

この設定を変更すると、新しい設定が適用されるまで約 1 分かかります。設定した値は、パフォーマンスと拡張用にキャッシュされます。

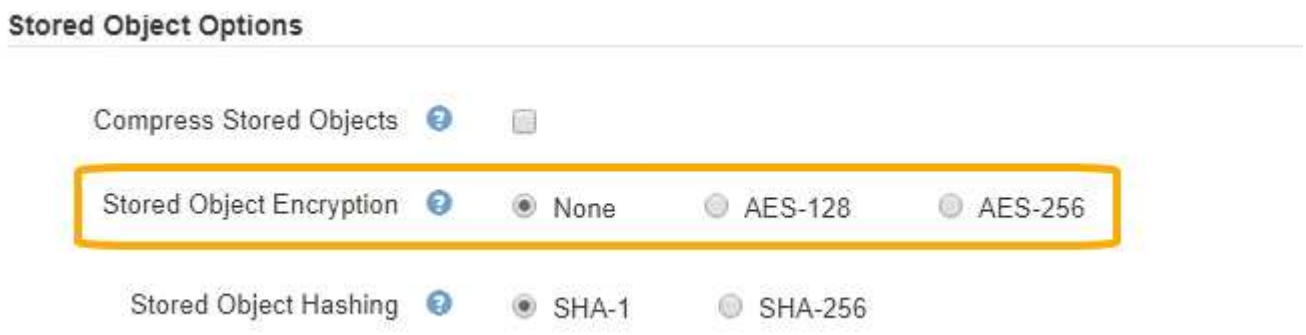
格納オブジェクトは、 AES - 128 または AES - 256 暗号化アルゴリズムを使用して暗号化できます。

格納オブジェクトの暗号化設定は、バケットレベルまたはオブジェクトレベルの暗号化で暗号化されていない S3 オブジェクトにのみ適用されます。

手順

1. 「環境設定*システム設定*グリッドオプション*」を選択します。

2. [格納オブジェクトのオプション] セクションで、 [格納オブジェクトの暗号化] を [* なし * （デフォルト）] 、 [* AES-128 *] 、または [* AES-256 *] に変更します。



3. [保存（ Save ）] をクリックします。

格納オブジェクトのハッシュの設定

格納オブジェクトのハッシュオプションは、オブジェクトの整合性の検証に使用するハッシュアルゴリズムを指定します。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

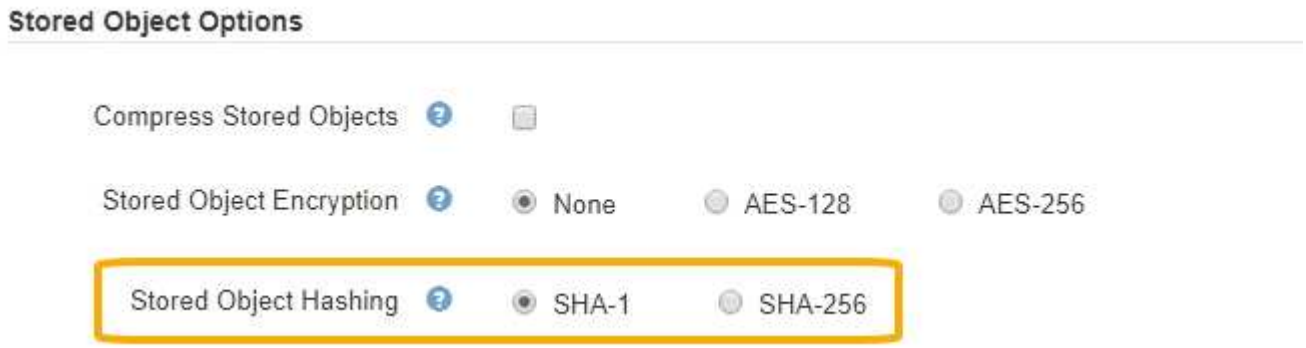
このタスクについて

デフォルトでは、オブジェクトデータはSHA-1アルゴリズムを使用してハッシュされます。SHA-256 アルゴリズムには追加の CPU リソースが必要で、整合性検証には一般的に推奨されていません。

この設定を変更すると、新しい設定が適用されるまで約 1 分かかります。設定した値は、パフォーマンスと拡張用にキャッシュされます。

手順

1. 「環境設定*システム設定*グリッドオプション*」を選択します。
2. 格納オブジェクトのオプションセクションで、格納オブジェクトのハッシュを * SHA-1 * （デフォルト）または * SHA-256 * に変更します。



3. [保存（ Save ）] をクリックします。

各ストレージノードは、いくつかの設定とカウンタを使用します。アラーム（従来のシステム）をクリアするには、現在の設定の表示またはカウンタのリセットが必要になる場合があります。

ドキュメントで特に指示された場合を除き、ストレージノード設定を変更する前にテクニカルサポートにお問い合わせください。必要に応じて、イベントカウンタをリセットしてレガシーアラームをクリアできます。

ストレージノードの設定とカウンタにアクセスするには、次の手順を実行します。

1. Support **>** Tools **>** Grid Topology *を選択します。
2. 「 * *site* * > * _ *Storage Node** 」を選択します。
3. ストレージノードを展開し、サービスまたはコンポーネントを選択します。
4. [* 構成 *] タブを選択します。

次の表に、ストレージノードの構成設定をまとめます。

LDR

属性名（**Attribute Name**）	コード	説明
HTTP State のことです	HSTE	S3 、 Swift 、およびその他の内部 StorageGRID トラフィックの HTTP プロトコルの現在の状態。 • Offline ：処理は許可されず、クライアントアプリケーションが LDR サービスへの HTTP セッションを開こうとするとエラーメッセージが表示されます。アクティブなセッションは正常終了します。 • Online ：処理は正常に続行されます
HTTP を自動起動します	HTAS	• このオプションを選択すると、再起動時のシステムの状態は * LDR * > * Storage * コンポーネントの状態によって異なります。再起動時に * ldr*>* Storage* コンポーネントが読み取り専用の場合、 HTTP インターフェイスも読み取り専用です。LDR * > * Storage * コンポーネントが Online の場合、 HTTP も Online になります。それ以外の場合は、 HTTP インターフェイスは Offline 状態のままです。 • 選択しない場合、 HTTP インターフェイスは明示的に有効にするまで Offline のままです。

LDR> データストア

属性名（**Attribute Name**）	コード	説明
Lost Objects 数をリセットします	RCOR	このサービス上にある損失オブジェクト数のカウンタをリセットします。

LDR > Storage の順にクリックします

属性名（**Attribute Name**）	コード	説明
ストレージの状態 — 望ましい	SSD	ストレージコンポーネントに求める状態をユーザが設定できます。LDR サービスはこの値を読み取り、指定されたステータスに一致するように試みます。この値は、再起動後も維持されます。 たとえば、この設定を使用すると、使用可能なストレージスペースが十分にある場合でも、ストレージを強制的に読み取り専用にすることができます。これはトラブルシューティングに役立ちます。 この属性には次のいずれかの値を指定できます。 • Offline ：目的の状態が Offline の場合、 LDR サービスは * LDR * > * Storage * コンポーネントをオフラインにします。 • Read-only ： LDR サービスはストレージを読み取り専用にし、新しいコンテンツの受け入れを停止します。開いているセッションが閉じられるまでの短時間の間、コンテンツが引き続きストレージノードに保存される可能性があります。 • Online ：通常のシステム運用中は、値を Online のままにします。ストレージの状態 — ストレージコンポーネントの現在の状態は ' 使用可能なオブジェクトストレージ容量などの LDR サービスの状態に基づいてサービスによって動的に設定されますスペースが少ない場合、コンポーネントは読み取り専用になります。
ヘルスチェックタイムアウト	SHCT	ストレージボリュームが正常であるとみなされるために、ヘルスチェックテストが完了する必要のある秒数。この値は、サポートから指示があった場合にのみ変更してください。

LDR > Verification の順に選択します

属性名（**Attribute Name**）	コード	説明
欠落オブジェクト数のリセット	VCMI	OMIS （ Missing Objects Detected ）の数をリセットします。フォアグラウンド検証の完了後にのみ使用してください。欠落しているレプリケートオブジェクトデータは、 StorageGRID システムによって自動的にリストアされます。
確認します	FVOV	フォアグラウンド検証を実行するオブジェクトストアを選択します。
検証レート	VPRI （ VPRI ）	バックグラウンド検証を実行する際のレートを設定します。バックグラウンド検証レートの設定に関する情報を参照してください。
破損オブジェクト数のリセット	VCCR	バックグラウンド検証中に見つかった、破損しているレプリケートされたオブジェクトデータのカウンタをリセットします。このオプションを使用すると、 OCOR （ Corrupt Objects Detected ）アラームの状態をクリアできます。詳細については、 StorageGRID の監視とトラブルシューティングの手順を参照してください。
隔離オブジェクトを削除します	OQRT の場合	破損したオブジェクトを隔離ディレクトリから削除し、隔離されたオブジェクトの数をゼロにリセットして、 Quarantined Objects Detected （ OQRT ）アラームをクリアします。このオプションは、破損したオブジェクトが StorageGRID システムによって自動的にリストアされたあとに使用します。 Lost Objects アラームがトリガーされた場合、テクニカルサポートが隔離されたオブジェクトにアクセスを試みる可能性があります。隔離されたオブジェクトが、データのリカバリや、オブジェクトコピーの破損の原因となった根本的な問題のデバッグに役立つ場合があります。

LDR> イレイジャーコーディング

属性名（**Attribute Name**）	コード	説明
書き込みエラー数をリセットします	RSWF	イレイジャーコーディングオブジェクトデータのストレージノードへの書き込みエラーのカウンタをリセットします。
読み取りエラー数をリセットします	RSRF	イレイジャーコーディングオブジェクトデータのストレージノードからの読み取りエラーのカウンタをリセットします。

属性名（**Attribute Name**）	コード	説明
Reset Deletes Failure Count （エラーカウントをリセット）	自衛隊	イレイジャーコーディングオブジェクトデータのストレージノードからの削除エラーのカウンタをリセットします。
破損コピーのリセット検出数	RSCC	ストレージノード上にあるイレイジャーコーディングオブジェクトデータの破損コピー数のカウンタをリセットします。
破損フラグメントのリセット検出数	RSCD	ストレージノード上にあるイレイジャーコーディングオブジェクトデータの破損フラグメントのカウンタをリセットします。
欠落フラグメントの検出数をリセットします	RSMD	ストレージノード上にあるイレイジャーコーディングオブジェクトデータの欠落フラグメントのカウンタをリセットします。フォアグラウンド検証の完了後にのみ使用してください。

LDR > Replication の順に選択します

属性名（**Attribute Name**）	コード	説明
インバウンドレプリケーションエラー数をリセットします	RICR	インバウンドレプリケーションエラーのカウンタをリセットします。これを使用すると、 RIRF （ Inbound Replication - - Failed ）アラームをクリアできます。
アウトバウンドレプリケーションのエラー数をリセットします	ROCR	アウトバウンドレプリケーションエラーのカウンタをリセットします。これを使用すると、 RORF （ Outbound Replications - - Failed ）アラームをクリアできます。
インバウンドレプリケーションを無効にします	DSIR	メンテナンスまたは手順 のテストの一環としてインバウンドレプリケーションを無効にする場合に選択します。通常の運用中はオフのままにします。 インバウンドレプリケーションを無効にすると、オブジェクトをストレージノードから読み出して StorageGRID システム内の別の場所へコピーすることはできますが、他の場所からこのストレージノードへオブジェクトをコピーすることはできません。つまり、 LDR サービスは読み取り専用です。

属性名（**Attribute Name**）	コード	説明
アウトバウンドレプリケーションを無効にします	DSOR	メンテナンスまたは手順 のテストの一環としてアウトバウンドレプリケーション（ HTTP 読み出し用のコンテンツ要求を含む）を無効にする場合に選択します。通常の運用中はオフのままにします。 アウトバウンドレプリケーションを無効にすると、このストレージノードにオブジェクトをコピーすることはできますが、ストレージノードからオブジェクトを読み出して StorageGRID システム内の別の場所へコピーすることはできません。LDR サービスは書き込み専用です。

関連情報

"トラブルシューティングを監視します"

容量が上限に達したストレージノードの管理

ストレージノードの容量が上限に達した場合は、新しいストレージを追加して StorageGRID システムを拡張する必要があります。ストレージボリュームの追加、ストレージ拡張シェルフの追加、ストレージノードの追加の 3 つのオプションがあります。

ストレージボリュームを追加しています

各ストレージノードは最大数のストレージボリュームをサポートします。定義されている最大値はプラットフォームによって異なります。ストレージノードのストレージボリュームが最大数より少ない場合は、ボリュームを追加して容量を増やすことができます。StorageGRID システムの拡張手順を参照してください。

ストレージ拡張シェルフの追加

SG6060 などの一部の StorageGRID アプライアンスストレージノードで、追加のストレージシェルフがサポートされます。拡張機能が最大容量まで拡張されていない StorageGRID アプライアンスがある場合は、ストレージシェルフを追加して容量を増やすことができます。StorageGRID システムの拡張手順を参照してください。

ストレージノードの追加

ストレージノードを追加してストレージ容量を増やすことができます。ストレージを追加する場合は、現在アクティブな ILM ルールと容量の要件について慎重に検討する必要があります。StorageGRID システムの拡張手順を参照してください。

関連情報

"グリッドを展開します"

管理ノードの管理

StorageGRID 環境の各サイトには管理ノードを1つ以上配置できます。

- "管理ノードとは"
- "複数の管理ノードを使用する"
- "プライマリ管理ノードの特定"
- "優先送信者を選択しています"
- "通知のステータスとキューの表示"
- "管理ノードによる確認済みアラームの表示（従来のシステム）"
- "監査クライアントアクセスを設定しています"

管理ノードとは

管理ノードは、システムの設定、監視、ロギングなどの管理サービスを提供します。各グリッドにはプライマリ管理ノードが 1 つ必要で、冗長性を確保するために任意の数の非プライマリ管理ノードを設定できます。

Grid Manager または Tenant Manager にサインインすると、管理ノードに接続されます。どの管理ノードにも接続が可能で、各管理ノードに表示される StorageGRID システムのビューもほぼ同じです。ただし、メンテナンス手順はプライマリ管理ノードを使用して実行する必要があります。

管理ノードを使用して、 S3 および Swift クライアントトラフィックの負荷を分散することもできます。

管理ノードは次のサービスをホストします。

- AMS サービス
- CMN サービス
- NMS サービス
- Prometheus サービス
- ロードバランササービスとハイアベイラビリティサービス（ S3 および Swift クライアントトラフィックをサポート）

管理ノードは、グリッド管理 API とテナント管理 API からの要求を処理する管理アプリケーションプログラムインターフェイス（ mgmt-api ）もサポートします。

AMS サービスとは

Audit Management System （ AMS ）サービスは、システムアクティビティとイベントを追跡します。

CMN サービスとは

Configuration Management Node （ CMN ）サービスは、すべてのサービスで必要とされる接続およびプロトコルの機能について、システム全体での設定を管理します。CMN サービスはグリッドタスクの実行および監視にも使用されます。StorageGRID 環境ごとに CMN サービスは 1 つだけです。CMN サービスをホストする管理ノードをプライマリ管理ノードと呼びます。

NMS サービスとは

Network Management System （ NMS ）サービスは、 StorageGRID システムのブラウザベースのインターフェイスであるグリッドマネージャに表示される、監視、レポート、および設定のオプションを提供します。

Prometheus サービスとは

Prometheus サービスは、すべてのノードのサービスから時系列の指標を収集します。

関連情報

"グリッド管理APIを使用する"

"テナントアカウントを使用する"

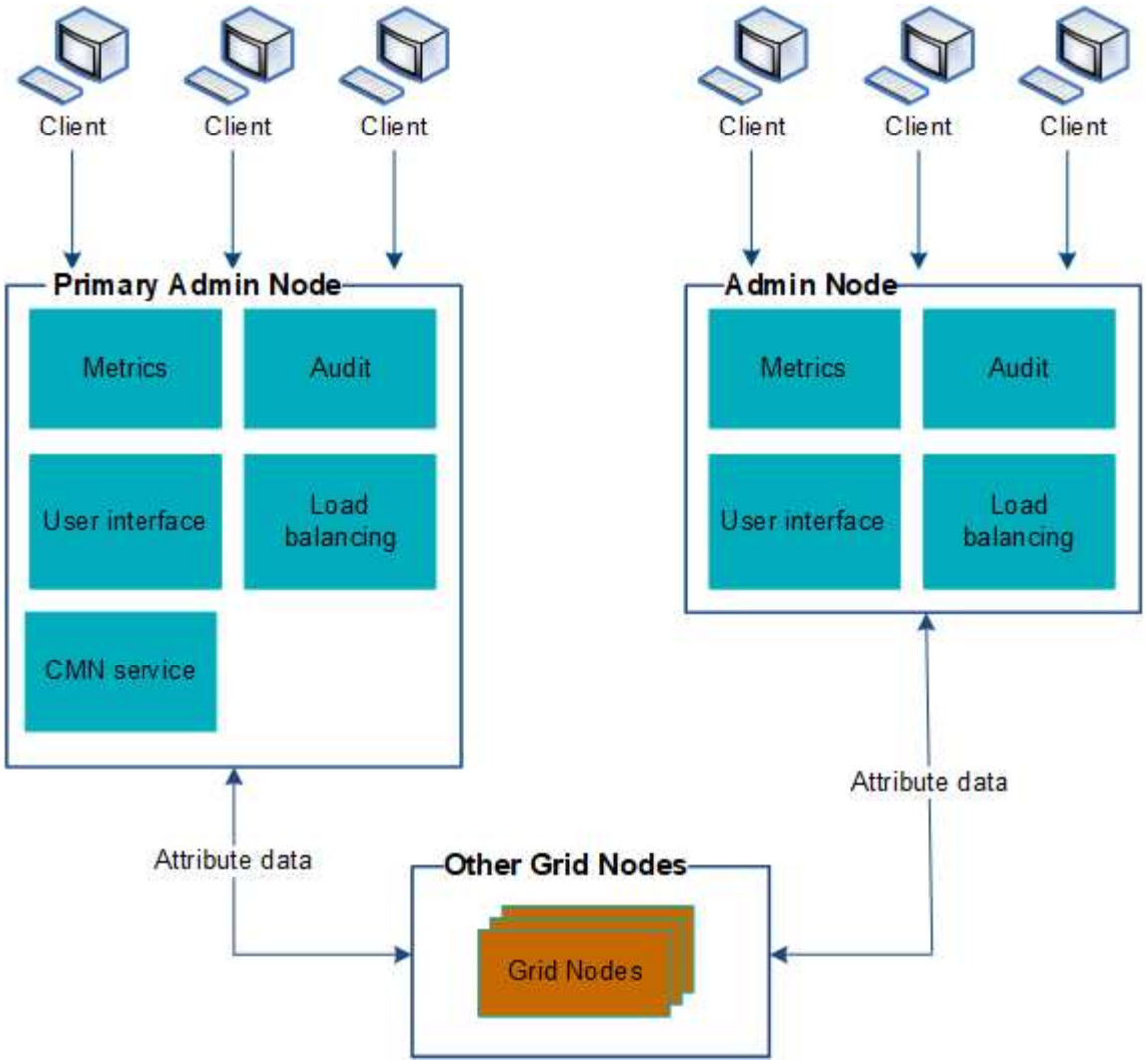
"負荷分散の管理"

"ハイアベイラビリティグループの管理"

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ます。これにより、 1 つの管理ノードに障害が発生した場合でも、 StorageGRID システムを継続的に監視して設定することができます。

ある管理ノードが使用できなくなっても属性の処理は続行され、アラートとアラーム（従来のシステム）は引き続きトリガーされ、 E メール通知と AutoSupport メッセージは引き続き送信されます。ただし、通知と AutoSupport メッセージ以外のフェイルオーバー保護は提供されません。特に、ある管理ノードからのアラームの確認応答は他の管理ノードにはコピーされません。



管理ノードに障害が発生した場合、次の 2 つの方法で StorageGRID システムを引き続き表示および設定することができます。

- Web クライアントは使用可能な他の管理ノードに再接続できます。
- システム管理者が管理ノードのハイアベイラビリティグループを設定している場合、 Web クライアントは HA グループの仮想 IP アドレスを使用して引き続き Grid Manager または Tenant Manager にアクセスできます。

> HA グループを使用している場合、マスター管理ノードに障害が発生するとアクセスが中断します。ユーザは、 HA グループの仮想 IP アドレスがグループ内の別の管理ノードにフェイルオーバーしたあとで、再度サインインする必要があります。

一部のメンテナンスタスクはプライマリ管理ノードでしか実行できません。プライマリ管理ノードに障害が発生した場合、そのノードをリカバリするまでは、 StorageGRID システムは完全に機能している状態ではありません。

関連情報

"ハイアベイラビリティグループの管理"

プライマリ管理ノードの特定

プライマリ管理ノードは CMN サービスをホストします。一部のメンテナンス手順は、プライマリ管理ノードでしか実行できません。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

手順

1. Support **>** Tools **>** Grid Topology *を選択します。
2. [**_site **管理ノード]を選択し、をクリックします ➕ をクリックしてトポロジツリーを展開し、この管理ノードでホストされているサービスを表示します。

   プライマリ管理ノードは CMN サービスをホストします。

3. この管理ノードが CMN サービスをホストしていない場合、他の管理ノードを確認します。

優先送信者を選択しています

StorageGRID 環境に複数の管理ノードが含まれている場合は、通知の優先送信者となる管理ノードを選択できます。デフォルトでは、プライマリ管理ノードが選択されますが、任意の管理ノードを優先送信者にすることができます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

このタスクについて

「* Configuration * System Settings * Display Options *」ページに、現在優先送信者として選択されている管理ノードが表示されます。デフォルトでは、プライマリ管理ノードが選択されます。

通常のシステム運用では、優先送信者のみが次の通知を送信します。

- AutoSupport メッセージ
- SNMP 通知
- アラート E メール
- アラーム E メール（レガシーシステム）

ただし、他のすべての管理ノード（スタンバイ送信者）が優先送信者を監視します。問題が検出された場合は、スタンバイ送信者もこれらの通知を送信できます。

次の場合、優先送信者とスタンバイ送信者の両方が通知を送信することがあります。

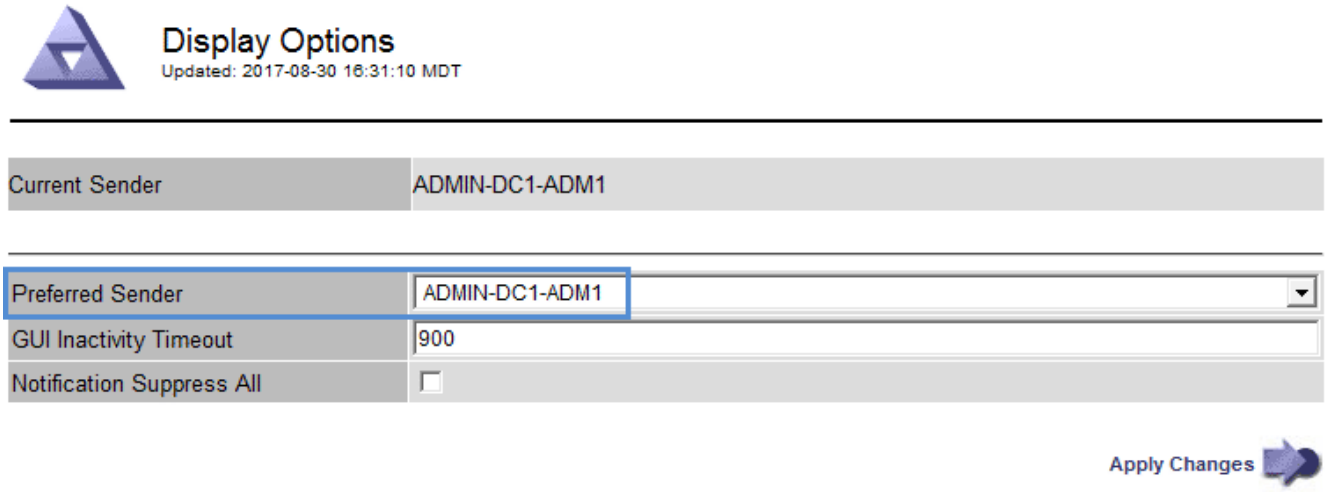
- 管理ノードどうしが「孤立した」状態になると、優先送信者とスタンバイ送信者の両方が通知の送信を試み、通知が重複して届く可能性があります。
- スタンバイ送信者が優先送信者に関する問題を検出して通知の送信を開始したあとで、優先送信者が通知

を再び送信できるようになることがあります。この場合、重複する通知が送信される可能性があります。優先送信者に関するエラーが検出されなくなると、スタンバイ送信者は通知の送信を停止します。

アラーム通知と AutoSupport メッセージをテストするときは、すべての管理ノードからテスト E メールが送信されます。アラート通知をテストするときは、すべての管理ノードにサインインして接続を確認する必要があります。

手順

1. * Configuration > System Settings > Display Options *を選択します。
2. [表示オプション] メニューから、 [* オプション *] を選択します。
3. 優先送信者として設定する管理ノードをドロップダウンリストから選択します。



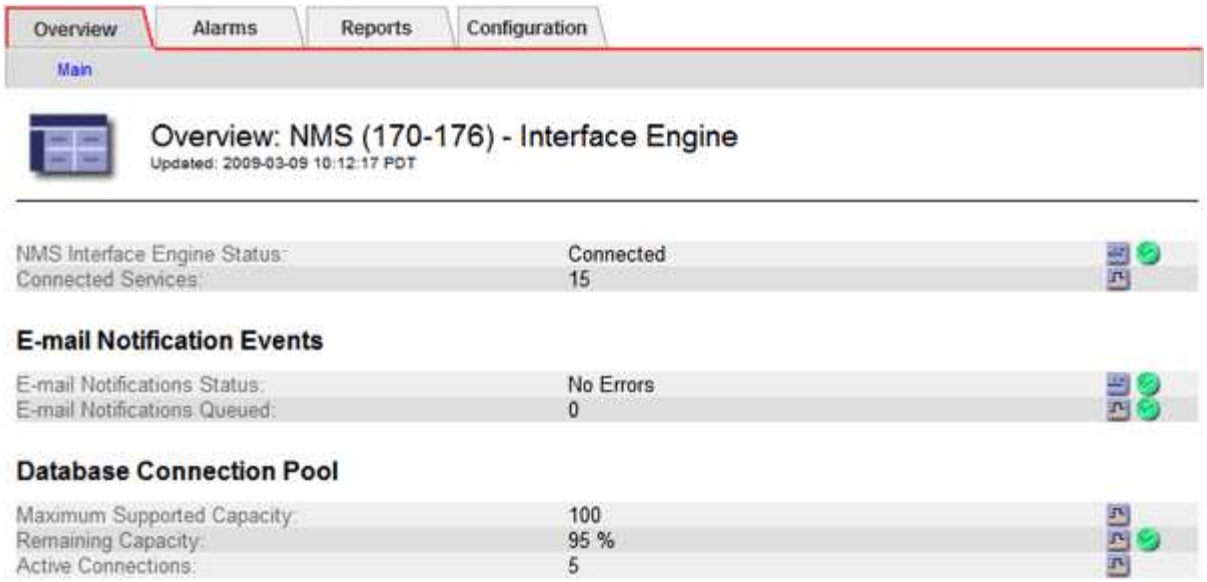
4. [変更の適用 *] をクリックします。

   管理ノードが通知の優先送信者として設定されます。

通知のステータスとキューの表示

管理ノードのNMSサービスは、メールサーバに通知を送信します。NMS サービスの現在のステータスとその通知キューのサイズは、 Interface Engine ページで確認できます。

Interface Engineページにアクセスするには、* Support > Tools > Grid Topology を選択します。最後に、 ***site _ * > * _Admin Node*** > * NMS * > * Interface Engine * を選択します。

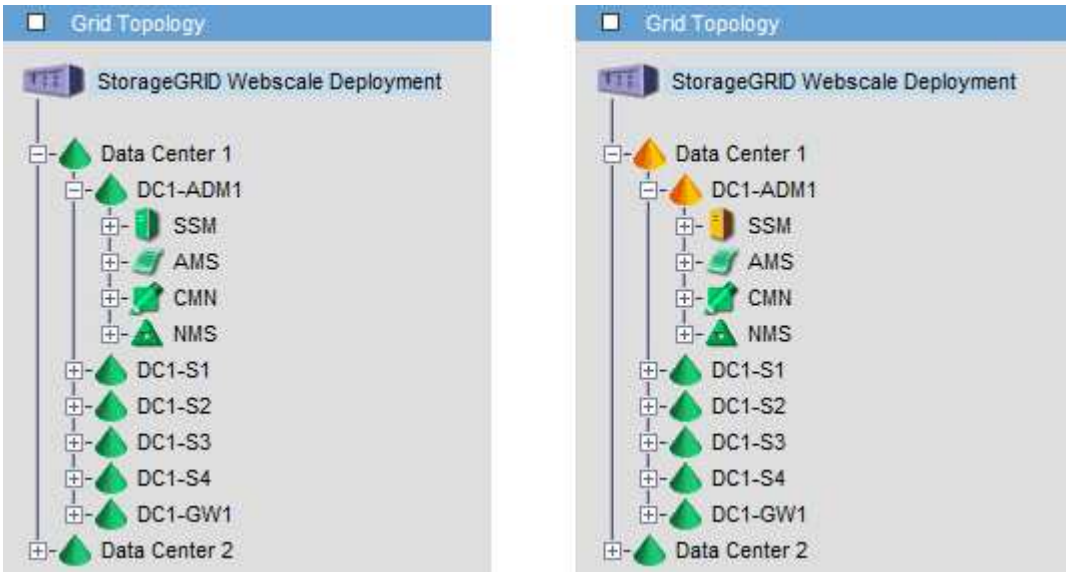


通知は E メール通知キューを通じて処理され、トリガーされた順にメールサーバに送信されます。通知の送信時に問題（ネットワーク接続エラーなど）が発生してメールサーバが使用できなくなった場合は、メールサーバへの再送信が 60 秒間試行されます。60 秒経ってもメールサーバに送信されなかった通知は通知キューから破棄され、キュー内の次の通知の送信が試行されます。通知が送信されずに通知キューから破棄されることがあるため、通知が送信されずにアラームがトリガーされる可能性があります。通知が送信されずにキューから破棄された場合は、 MINS （ E メール通知ステータス） Minor アラームがトリガーされます。

管理ノードによる確認済みアラームの表示（従来のシステム）

ある管理ノードのアラームを確認しても、確認済みのアラームは他の管理ノードにはコピーされません。確認応答は他の管理ノードにはコピーされないため、グリッドトポロジツリーでは各管理ノードで同じように表示されない場合があります。

この違いは、 Web クライアントに接続する場合に役立ちます。Web クライアントでは、管理者のニーズに基づいて、 StorageGRID システムをさまざまな方法で表示できます。



通知は、確認応答が発生した管理ノードから送信されます。

監査クライアントアクセスを設定しています

管理ノードは、 Audit Management System （ AMS ）サービスを介して、監査対象のすべてのシステムイベントを、監査共有からアクセス可能なログファイルに記録します。監査共有はインストール時に各管理ノードに追加されます。監査ログへのアクセスを簡単にするためには、 CIFS と NFS の両方についてクライアントから監査共有へのアクセスを設定します。

StorageGRID システムは、確認応答を使用して、ログファイルに書き込まれる前に監査メッセージが失われないようにします。AMS サービスまたは中間の監査リレーサービスがメッセージの制御を確認するまで、メッセージはサービスのキューに残ります。

詳細については、監査メッセージを確認する手順を参照してください。

CIFS または NFS を使用するオプションがある場合は、 nfs を選択します。

CIFS / Samba を使用した監査エクスポートは廃止されており、 StorageGRID の今後のリリースで削除される予定です。

関連情報

"管理ノードとは"

"監査ログを確認します"

"ソフトウェアをアップグレードする"

CIFSの監査クライアントを設定しています

監査クライアントの設定に使用する手順 は、認証方式 (Windows ワークグループまたは Windows Active Directory) によって異なります。追加した監査共有は、読み取り専用の共有として自動的に有効になります。

CIFS / Samba を使用した監査エクスポートは廃止されており、 StorageGRID の今後のリリースで削除される予定です。

関連情報

"ソフトウェアをアップグレードする"

ワークグループの監査クライアントの設定

この手順 は、監査メッセージの取得先である StorageGRID 環境内の管理ノードごとに実行します。

必要なもの

- を用意しておく必要があります `Passwords.txt` root / adminアカウントのパスワードを含むファイル（SAIDパッケージ内にあります）。
- を用意しておく必要があります `Configuration.txt` ファイル（SAIDパッケージ内にあります）。

このタスクについて

CIFS / Samba を使用した監査エクスポートは廃止されており、 StorageGRID の今後のリリースで削除される予定です。

手順

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

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

2. すべてのサービスの状態が「Running」または「Verified」であることを確認します。 `storagegrid-status`

   すべてのサービスが「 Running 」または「 Verified 」でない場合は、問題を解決してから続行してください。

3. コマンドラインに戻り、 * Ctrl * + * C * を押します。
4. CIFS設定ユーティリティを起動します。 `config_cifs.rb`

```
------------------------------------------------------------------
| Shares                  | Authentication         | Config          |
------------------------------------------------------------------
| add-audit-share         | set-authentication     | validate-config |
| enable-disable-share    | set-netbios-name       | help            |
| add-user-to-share       | join-domain            | exit            |
| remove-user-from-share  | add-password-server    |                 |
| modify-group            | remove-password-server |                 |
|                         | add-wins-server        |                 |
|                         | remove-wins-server     |                 |
------------------------------------------------------------------
```

5. Windows ワークグループの認証を設定します。

   認証がすでに設定されている場合は、確認メッセージが表示されます。認証がすでに設定されている場合は、次の手順に進みます。

   a. 入力するコマンド `set-authentication`
   b. WindowsワークグループまたはActive Directoryのインストールを求めるプロンプトが表示されたら、次のように入力します。 `workgroup`
   c. プロンプトが表示されたら、ワークグループの名前を入力します。 *`workgroup_name`*
   d. プロンプトが表示されたら、わかりやすいNetBIOS名を設定します。 *`netbios_name`*

または

Enter * キーを押して管理ノードのホスト名を NetBIOS 名として使用します。

スクリプトによって Samba サーバが再起動され、変更が適用されます。この処理にかかる時間は 1 分未満です。認証を設定したら、監査クライアントを追加します。

a. プロンプトが表示されたら、 * Enter * を押します。

CIFS 設定ユーティリティが表示されます。

6. 監査クライアントを追加します。

a. 入力するコマンド `add-audit-share`

共有は読み取り専用として自動的に追加されます。

b. プロンプトが表示されたら、ユーザまたはグループを追加します。 *`user`*

c. プロンプトが表示されたら、監査ユーザ名を入力します。 *`audit_user_name`*

d. プロンプトが表示されたら、監査ユーザのパスワードを入力します。 *`password`*

e. プロンプトが表示されたら、確認のためにもう一度同じパスワードを入力します。 *`password`*

f. プロンプトが表示されたら、 * Enter * を押します。

CIFS 設定ユーティリティが表示されます。

ディレクトリを入力する必要はありません。監査ディレクトリ名は事前に定義されています。

7. 複数のユーザまたはグループが監査共有へのアクセスを許可されている場合は、ユーザを追加します。

a. 入力するコマンド `add-user-to-share`

有効な共有に番号が振られ、リストに表示されます。

b. プロンプトが表示されたら、監査エクスポート共有の番号を入力します。 *`share_number`*

c. プロンプトが表示されたら、ユーザまたはグループを追加します。 `user`

または `group`

d. プロンプトが表示されたら、監査ユーザまたはグループの名前を入力します。 *`audit_user or audit_group`*

e. プロンプトが表示されたら、 * Enter * を押します。

CIFS 設定ユーティリティが表示されます。

f. 監査共有に追加するユーザまたはグループごとに、上記の手順を繰り返します。

8. 必要に応じて、設定を確認します。 `validate-config`

サービスがチェックされて表示されます。次のメッセージは無視してかまいません。

```
Can't find include file /etc/samba/includes/cifs-interfaces.inc
Can't find include file /etc/samba/includes/cifs-filesystem.inc
Can't find include file /etc/samba/includes/cifs-custom-config.inc
Can't find include file /etc/samba/includes/cifs-shares.inc
rlimit_max: increasing rlimit_max (1024) to minimum Windows limit
(16384)
```

a. プロンプトが表示されたら、 * Enter * を押します。

監査クライアント設定が表示されます。

b. プロンプトが表示されたら、 * Enter * を押します。

CIFS 設定ユーティリティが表示されます。

9. CIFS設定ユーティリティを閉じます。 `exit`
10. Sambaサービスを開始します。 `service smbd start`
11. StorageGRID 環境が単一サイトの場合は、次の手順に進みます。

または

StorageGRID 環境で他のサイトに管理ノードが含まれている場合は、必要に応じてこれらの監査共有を有効にします。

a. サイトの管理ノードにリモートからログインします。
   i. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
   ii. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   iii. 次のコマンドを入力してrootに切り替えます。 `su -`
   iv. に記載されているパスワードを入力します `Passwords.txt` ファイル。
b. 同じ手順を繰り返して、追加の管理ノードごとに監査共有を設定します。
c. リモート管理ノードへのリモートのSecure Shellログインを終了します。 `exit`
12. コマンドシェルからログアウトします。 `exit`

関連情報

"ソフトウェアをアップグレードする"

Active Directoryの監査クライアントを設定しています

この手順 は、監査メッセージの取得先である StorageGRID 環境内の管理ノードごとに実行します。

必要なもの

- を用意しておく必要があります `Passwords.txt` root / adminアカウントのパスワードを含むファイル（SAIDパッケージ内にあります）。
- CIFS Active Directoryのユーザ名とパスワードが必要です。
- を用意しておく必要があります `Configuration.txt` ファイル（SAIDパッケージ内にあります）。

CIFS / Samba を使用した監査エクスポートは廃止されており、 StorageGRID の今後のリリースで削除される予定です。

手順

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

   rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。
2. すべてのサービスの状態が「Running」または「Verified」であることを確認します。 `storagegrid-status`

   すべてのサービスが「 Running 」または「 Verified 」でない場合は、問題を解決してから続行してください。
3. コマンドラインに戻り、 * Ctrl * + * C * を押します。
4. CIFS設定ユーティリティを起動します。 `config_cifs.rb`

```
------------------------------------------------------------------
| Shares                  | Authentication         | Config          |
------------------------------------------------------------------
| add-audit-share         | set-authentication     | validate-config |
| enable-disable-share    | set-netbios-name       | help            |
| add-user-to-share       | join-domain            | exit            |
| remove-user-from-share  | add-password-server    |                 |
| modify-group            | remove-password-server |                 |
|                         | add-wins-server        |                 |
|                         | remove-wins-server     |                 |
------------------------------------------------------------------
```

5. Active Directoryの認証を設定します。 `set-authentication`

   ほとんどの環境では、監査クライアントを追加する前に認証を設定する必要があります。認証がすでに設定されている場合は、確認メッセージが表示されます。認証がすでに設定されている場合は、次の手順に進みます。

a. ワークグループまたはActive Directoryのインストールを求めるプロンプトが表示されたら、次のよう `ad`

b. プロンプトが表示されたら、 AD ドメインの名前（短いドメイン名）を入力します。

c. プロンプトが表示されたら、ドメインコントローラの IP アドレスまたは DNS ホスト名を入力します。

d. プロンプトが表示されたら、完全なドメインレルム名を入力します。

大文字を使用します。

e. winbind サポートの有効化を求めるプロンプトが表示されたら、「 * y * 」と入力します。

Winbind は AD サーバのユーザおよびグループの情報を解決するために使用されます。

f. プロンプトが表示されたら、 NetBIOS 名を入力します。

g. プロンプトが表示されたら、 * Enter * を押します。

CIFS 設定ユーティリティが表示されます。

6. ドメインに参加します。

a. CIFS設定ユーティリティが起動していない場合は、起動します。 `config_cifs.rb`

b. ドメインに参加します。 `join-domain`

c. 管理ノードが現在ドメインの有効なメンバーかどうかテストするよう求めるプロンプトが表示されます。この管理ノードがドメインに参加していない場合は、次のように入力します。 `no`

d. プロンプトが表示されたら、管理者のユーザ名を指定します。 *`administrator_username`*

ここで、 *`administrator_username`* は、StorageGRID ユーザ名ではなく、CIFS Active Directoryのユーザ名です。

e. プロンプトが表示されたら、管理者のパスワードを入力します。 *`administrator_password`*

はい *`administrator_password`* は、StorageGRID パスワードではなく、CIFS Active Directoryのユーザ名です。

f. プロンプトが表示されたら、 * Enter * を押します。

CIFS 設定ユーティリティが表示されます。

7. ドメインに参加したことを確認します。

a. ドメインに参加します。 `join-domain`

b. サーバが現在ドメインの有効なメンバーかどうかをテストするよう求められたら、次のように入力します。 `y`

「 Join is OK 」というメッセージが表示される場合は、ドメインに正常に参加しています。このメッセージが表示されない場合は、もう一度認証を設定してドメインに参加してください。

c. プロンプトが表示されたら、 * Enter * を押します。

CIFS 設定ユーティリティが表示されます。

8. 監査クライアントを追加します。 `add-audit-share`
   a. ユーザまたはグループの追加を求めるプロンプトが表示されたら、次のように入力します。 `user`
   b. 監査ユーザ名の入力を求めるプロンプトが表示されたら、監査ユーザ名を入力します。
   c. プロンプトが表示されたら、 * Enter * を押します。

      CIFS 設定ユーティリティが表示されます。

9. 複数のユーザまたはグループが監査共有へのアクセスを許可されている場合は、ユーザを追加します。 `add-user-to-share`

   有効な共有に番号が振られ、リストに表示されます。

   a. 監査エクスポート共有の数を入力します。
   b. ユーザまたはグループの追加を求めるプロンプトが表示されたら、次のように入力します。 `group`

      監査グループ名の入力を求められます。

   c. 監査グループ名を求めるプロンプトが表示されたら、監査ユーザグループの名前を入力します。
   d. プロンプトが表示されたら、 * Enter * を押します。

      CIFS 設定ユーティリティが表示されます。

   e. 監査共有に追加するユーザまたはグループごとに、この手順を繰り返します。

10. 必要に応じて、設定を確認します。 `validate-config`

    サービスがチェックされて表示されます。次のメッセージは無視してかまいません。

    - インクルードファイルが見つかりません `/etc/samba/includes/cifs-interfaces.inc`
    - インクルードファイルが見つかりません `/etc/samba/includes/cifs-filesystem.inc`
    - インクルードファイルが見つかりません `/etc/samba/includes/cifs-interfaces.inc`
    - インクルードファイルが見つかりません `/etc/samba/includes/cifs-custom-config.inc`
    - インクルードファイルが見つかりません `/etc/samba/includes/cifs-shares.inc`
    - RLIMIT_max ： rlimit_max （ 1024 ）を Windows の最小制限（ 16384 ）に増やす

      「 security=ads 」と「 password server 」パラメータは同時に指定しないでください（ Samba は、接続する正しい DC を自動的に検出します）。

      i. プロンプトが表示されたら、 * Enter * を押して監査クライアントの設定を表示します。
      ii. プロンプトが表示されたら、 * Enter * を押します。

      CIFS 設定ユーティリティが表示されます。

11. CIFS設定ユーティリティを閉じます。 `exit`

12. StorageGRID 環境が単一サイトの場合は、次の手順に進みます。

    または

    StorageGRID 環境で他のサイトに管理ノードが含まれている場合は、必要に応じてこれらの監査共有を有効にします。

    a. サイトの管理ノードにリモートからログインします。
        i. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
        ii. に記載されているパスワードを入力します `Passwords.txt` ファイル。
        iii. 次のコマンドを入力してrootに切り替えます。 `su -`
        iv. に記載されているパスワードを入力します `Passwords.txt` ファイル。
    b. 同じ手順を繰り返して、管理ノードごとに監査共有を設定します。
    c. 管理ノードへのリモートのSecure Shellログインを終了します。 `exit`

13. コマンドシェルからログアウトします。 `exit`

関連情報

"ソフトウェアをアップグレードする"

CIFS監査共有へのユーザまたはグループの追加

AD 認証と統合されている CIFS 監査共有にユーザまたはグループを追加できます。

必要なもの

- を用意しておく必要があります `Passwords.txt` root / adminアカウントのパスワードを含むファイル（SAIDパッケージ内にあります）。
- を用意しておく必要があります `Configuration.txt` ファイル（SAIDパッケージ内にあります）。

このタスクについて

次の手順 は、 AD 認証と統合されている監査共有用です。

> CIFS / Samba を使用した監査エクスポートは廃止されており、 StorageGRID の今後のリリースで削除される予定です。

手順

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

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

2. すべてのサービスの状態が「 Running 」または「 Verified 」であることを確認します。入力するコマンド `storagegrid-status`

   すべてのサービスが「 Running 」または「 Verified 」でない場合は、問題を解決してから続行してください。

3. コマンドラインに戻り、 * Ctrl * + * C * を押します。
4. CIFS設定ユーティリティを起動します。 `config_cifs.rb`

```
------------------------------------------------------------------
| Shares                  | Authentication         | Config          |
------------------------------------------------------------------
| add-audit-share         | set-authentication     | validate-config |
| enable-disable-share    | set-netbios-name       | help            |
| add-user-to-share       | join-domain            | exit            |
| remove-user-from-share  | add-password-server    |                 |
| modify-group            | remove-password-server |                 |
|                         | add-wins-server        |                 |
|                         | remove-wins-server     |                 |
------------------------------------------------------------------
```

5. ユーザまたはグループの追加を開始します。 `add-user-to-share`

   設定済みの監査共有に番号が振られ、リストに表示されます。

6. プロンプトが表示されたら、監査共有（audit-export）の番号を入力します。 *`audit_share_number`*

   この監査共有へのアクセスをユーザまたはグループに許可するかどうかの確認を求められます。

7. プロンプトが表示されたら、ユーザまたはグループを追加します。 `user` または `group`
8. プロンプトが表示されたら、この AD 監査共有のユーザまたはグループ名を入力します。

   サーバのオペレーティングシステムと CIFS サービスの両方で、ユーザまたはグループが読み取り専用として監査共有に追加されます。Samba 設定がリロードされ、ユーザまたはグループが監査クライアント共有にアクセスできるようになります。

9. プロンプトが表示されたら、 * Enter * を押します。

   CIFS 設定ユーティリティが表示されます。

10. 監査共有に追加するユーザまたはグループごとに、上記の手順を繰り返します。
11. 必要に応じて、設定を確認します。 `validate-config`

    サービスがチェックされて表示されます。次のメッセージは無視してかまいません。

    - include ファイル /etc/samba/include/cifs-interfaces.in が見つかりません
    - include ファイル /etc/samba/include/cifs-filesystem.in が見つかりません

- include ファイル /etc/samba/include/cifs-custom-config.in が見つかりません
- include ファイル /etc/samba/include/cifs-shares.in が見つかりません
  i. プロンプトが表示されたら、 * Enter * を押して監査クライアントの設定を表示します。
  ii. プロンプトが表示されたら、 * Enter * を押します。

12. CIFS設定ユーティリティを閉じます。 `exit`
13. 次の状況に応じて、追加の監査共有を有効にする必要があるかどうかを判断します。
    - StorageGRID 環境が単一サイトの場合は、次の手順に進みます。
    - StorageGRID 環境で他のサイトに管理ノードが含まれている場合は、必要に応じてこれらの監査共有を有効にします。
      i. サイトの管理ノードにリモートからログインします。
         A. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
         B. に記載されているパスワードを入力します `Passwords.txt` ファイル。
         C. 次のコマンドを入力してrootに切り替えます。 `su -`
         D. に記載されているパスワードを入力します `Passwords.txt` ファイル。
      ii. 同じ手順を繰り返して、管理ノードごとに監査共有を設定します。
      iii. リモート管理ノードへのリモートのSecure Shellログインを終了します。 `exit`
14. コマンドシェルからログアウトします。 `exit`

CIFS監査共有からのユーザまたはグループの削除

監査共有にアクセス可能な最後のユーザまたはグループを削除することはできません。

必要なもの

- を用意しておく必要があります `Passwords.txt` rootアカウントのパスワードを含むファイル（SAIDパッケージ内にあります）。
- を用意しておく必要があります `Configuration.txt` ファイル（SAIDパッケージ内にあります）。

このタスクについて

CIFS / Samba を使用した監査エクスポートは廃止されており、 StorageGRID の今後のリリースで削除される予定です。

手順

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

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

2. CIFS設定ユーティリティを起動します。 `config_cifs.rb`

```
------------------------------------------------------------------
| Shares                 | Authentication         | Config          |
------------------------------------------------------------------
| add-audit-share        | set-authentication     | validate-config |
| enable-disable-share   | set-netbios-name       | help            |
| add-user-to-share      | join-domain            | exit            |
| remove-user-from-share | add-password-server    |                 |
| modify-group           | remove-password-server |                 |
|                        | add-wins-server        |                 |
|                        | remove-wins-server     |                 |
------------------------------------------------------------------
```

3. ユーザまたはグループの削除を開始します。 `remove-user-from-share`

   管理ノードで使用可能な監査共有に番号が振られ、リストに表示されます。監査共有には「 audit-export 」というラベルが付けられています。

4. 監査共有の番号を入力します。 *`audit_share_number`*
5. ユーザまたはグループの削除を求めるプロンプトが表示されたら、次のように入力します `user` または `group`

   監査共有のユーザまたはグループに番号が振られ、リストに表示されます。

6. 削除するユーザまたはグループに対応する番号を入力します。 *`number`*

   監査共有が更新され、ユーザまたはグループは監査共有にアクセスできなくなります。例：

```
Enabled shares
 1. audit-export
Select the share to change: 1
Remove user or group? [User/group]: User
Valid users for this share
1. audituser
2. newaudituser
Select the user to remove: 1

Removed user "audituser" from share "audit-export".

Press return to continue.
```

7. CIFS設定ユーティリティを閉じます。 `exit`
8. StorageGRID 環境で他のサイトに管理ノードが含まれている場合は、必要に応じて各サイトで監査共有を無効にします。

9. 設定が完了したら、各コマンドシェルからログアウトします。 `exit`

関連情報

"ソフトウェアをアップグレードする"

CIFS監査共有のユーザ名またはグループ名を変更する

CIFS 監査共有のユーザまたはグループの名前を変更するには、新しいユーザまたはグループを追加してから古いユーザまたはグループを削除します。

このタスクについて

CIFS / Samba を使用した監査エクスポートは廃止されており、 StorageGRID の今後のリリースで削除される予定です。

手順

1. 名前を更新した新しいユーザまたはグループを監査共有に追加します。
2. 古いユーザ名またはグループ名を削除します。

関連情報

"ソフトウェアをアップグレードする"

"CIFS監査共有へのユーザまたはグループの追加"

"CIFS監査共有からのユーザまたはグループの削除"

CIFS監査の統合の検証

監査共有は読み取り専用です。ログファイルはコンピュータアプリケーションによって読み取られることを目的としていますが、ファイルを開けるかどうかは検証の対象に含まれていません。Windows のエクスプローラウィンドウに監査ログファイルが表示されれば、検証は十分とみなされます。接続を検証したら、すべてのウィンドウを閉じます。

NFSの監査クライアントの設定

監査共有は読み取り専用の共有として自動的に有効になります。

必要なもの

- を用意しておく必要があります `Passwords.txt` rootまたはadminのパスワードを含むファイル（SAIDパッケージ内にあります）。
- を用意しておく必要があります `Configuration.txt` ファイル（SAIDパッケージ内にあります）。
- 監査クライアントがNFSバージョン3（NFSv3）を使用している必要があります。

このタスクについて

この手順 は、監査メッセージの取得先である StorageGRID 環境内の管理ノードごとに実行します。

手順

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

      rootとしてログインすると、プロンプトがから変わります `$` 終了： `#`。
2. すべてのサービスの状態が「 Running 」または「 Verified 」であることを確認します。入力するコマンド `storagegrid-status`

   「 Running 」または「 Verified 」でないサービスがある場合は、問題を解決してから続行してください。
3. コマンドラインに戻ります。Ctrl キーを押しながら * C キーを押します。
4. NFS 設定ユーティリティを起動します。入力するコマンド `config_nfs.rb`

```
----------------------------------------------------------------------
| Shares                | Clients               | Config           |
----------------------------------------------------------------------
| add-audit-share       | add-ip-to-share       | validate-config  |
| enable-disable-share  | remove-ip-from-share  | refresh-config   |
|                       |                       | help             |
|                       |                       | exit             |
----------------------------------------------------------------------
```

5. 監査クライアントを追加します。 `add-audit-share`
   a. プロンプトが表示されたら、監査共有用の監査クライアントのIPアドレスまたはIPアドレス範囲を入力します。 `client_IP_address`
   b. プロンプトが表示されたら、 * Enter * を押します。
6. 複数の監査クライアントに監査共有へのアクセスを許可する場合は、ユーザのIPアドレスを追加します。 `add-ip-to-share`
   a. 監査共有の番号を入力します。 *`audit_share_number`*
   b. プロンプトが表示されたら、監査共有用の監査クライアントのIPアドレスまたはIPアドレス範囲を入力します。 *`client_IP_address`*
   c. プロンプトが表示されたら、 * Enter * を押します。

      NFS 設定ユーティリティが表示されます。
   d. 監査共有に追加する監査クライアントごとに、上記の手順を繰り返します。
7. 必要に応じて、設定を確認します。
   a. 次のように入力します。 `validate-config`

サービスがチェックされて表示されます。

b. プロンプトが表示されたら、 * Enter * を押します。

NFS 設定ユーティリティが表示されます。

c. NFS設定ユーティリティを閉じます。 `exit`

8. 他のサイトで監査共有を有効にする必要があるかどうかを確認します。
   - StorageGRID 環境が単一サイトの場合は、次の手順に進みます。
   - StorageGRID 環境で他のサイトに管理ノードが含まれている場合は、必要に応じてこれらの監査共有を有効にします。
     i. サイトの管理ノードにリモートからログインします。
        A. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
        B. に記載されているパスワードを入力します `Passwords.txt` ファイル。
        C. 次のコマンドを入力してrootに切り替えます。 `su -`
        D. に記載されているパスワードを入力します `Passwords.txt` ファイル。
     ii. 同じ手順を繰り返して、追加の管理ノードごとに監査共有を設定します。
     iii. リモート管理ノードへのリモートの Secure Shell ログインを終了します。入力するコマンド `exit`
9. コマンドシェルからログアウトします。 `exit`

NFS 監査クライアントは、 IP アドレスに基づいて監査共有へのアクセスが許可されます。新しい NFS 監査クライアントに共有に IP アドレスを追加して監査共有へのアクセスを許可するか、または IP アドレスを削除して既存の監査クライアントを削除します。

監査共有への**NFS**監査クライアントの追加

NFS 監査クライアントは、 IP アドレスに基づいて監査共有へのアクセスが許可されます。新しい NFS 監査クライアントに監査共有へのアクセスを許可するには、そのクライアントの IP アドレスを監査共有に追加します。

必要なもの

- を用意しておく必要があります `Passwords.txt` root / adminアカウントのパスワードを含むファイル（SAIDパッケージ内にあります）。
- を用意しておく必要があります `Configuration.txt` ファイル（SAIDパッケージ内にあります）。
- 監査クライアントがNFSバージョン3（NFSv3）を使用している必要があります。

手順

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

d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

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

2. NFS設定ユーティリティを起動します。 `config_nfs.rb`

```
----------------------------------------------------------------------
| Shares                | Clients               | Config           |
----------------------------------------------------------------------
| add-audit-share       | add-ip-to-share       | validate-config  |
| enable-disable-share  | remove-ip-from-share  | refresh-config   |
|                       |                       | help             |
|                       |                       | exit             |
----------------------------------------------------------------------
```

3. 入力するコマンド `add-ip-to-share`

管理ノードで有効になっている NFS 監査共有のリストが表示されます。監査共有はのように表示されます。 `/var/local/audit/export`

4. 監査共有の番号を入力します。 *`audit_share_number`*
5. プロンプトが表示されたら、監査共有用の監査クライアントのIPアドレスまたはIPアドレス範囲を入力します。 *`client_IP_address`*

監査クライアントが監査共有に追加されます。

6. プロンプトが表示されたら、 * Enter * を押します。

NFS 設定ユーティリティが表示されます。

7. 監査共有に追加する監査クライアントごとに、この手順を繰り返します。
8. 必要に応じて、設定を確認します。 `validate-config`

サービスがチェックされて表示されます。

a. プロンプトが表示されたら、 * Enter * を押します。

NFS 設定ユーティリティが表示されます。

9. NFS設定ユーティリティを閉じます。 `exit`
10. StorageGRID 環境が単一サイトの場合は、次の手順に進みます。

StorageGRID 環境で他のサイトに管理ノードが含まれている場合は、必要に応じてこれらの監査共有を有効にします。

a. サイトの管理ノードにリモートからログインします。

i. 次のコマンドを入力します。 `ssh admin@`*`grid_node_IP`*

ii. に記載されているパスワードを入力します `Passwords.txt` ファイル。

iii. 次のコマンドを入力してrootに切り替えます。 `su -`

iv. に記載されているパスワードを入力します `Passwords.txt` ファイル。

b. 同じ手順を繰り返して、管理ノードごとに監査共有を設定します。

c. リモート管理ノードへのリモートのSecure Shellログインを終了します。 `exit`

11. コマンドシェルからログアウトします。 `exit`

NFS監査の統合の検証

監査共有を設定して NFS 監査クライアントを追加したら、監査クライアント共有をマウントし、監査共有のファイルにアクセスできることを確認します。

手順

1. AMS サービスをホストしている管理ノードのクライアント側 IP アドレスを使用して、接続（またはクライアントシステムでの操作）を検証します。入力するコマンド `ping IP_address`

   サーバが応答して接続を示していることを確認します。

2. クライアントのオペレーティングシステムに適したコマンドを使用して、読み取り専用の監査共有をマウントします。Linux コマンドの例は次のとおりです（ 1 行で入力します）。

   ```
   mount -t nfs -o hard,intr Admin_Node_IP_address:/var/local/audit/export
   myAudit
   ```

   AMS サービスをホストしている管理ノードの IP アドレスと、監査システムの事前定義された共有名を使用します。マウントポイントには、クライアントが選択した任意の名前を使用できます（例： *myAudit* 前のコマンドを参照）。

3. 監査共有のファイルにアクセスできることを確認します。入力するコマンド `ls myAudit /*`

   ここで、 *myAudit* は、監査共有のマウントポイントです。少なくとも 1 つのログファイルが表示されている必要があります。

監査共有からの**NFS**監査クライアントの削除

NFS 監査クライアントは、 IP アドレスに基づいて監査共有へのアクセスが許可されます。既存の監査クライアントを削除するには、その IP アドレスを削除します。

必要なもの

- を用意しておく必要があります `Passwords.txt` root / adminアカウントのパスワードを含むファイル（SAIDパッケージ内にあります）。
- を用意しておく必要があります `Configuration.txt` ファイル（SAIDパッケージ内にあります）。

このタスクについて

監査共有にアクセス可能な最後の IP アドレスを削除することはできません。

手順

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

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

2. NFS設定ユーティリティを起動します。 `config_nfs.rb`

```
------------------------------------------------------------------
| Shares                | Clients               | Config          |
------------------------------------------------------------------
| add-audit-share       | add-ip-to-share       | validate-config |
| enable-disable-share  | remove-ip-from-share  | refresh-config  |
|                       |                       | help            |
|                       |                       | exit            |
------------------------------------------------------------------
```

3. 監査共有からIPアドレスを削除します。 `remove-ip-from-share`

   サーバで設定されている監査共有に番号が振られ、リストに表示されます。監査共有はのように表示されます。 `/var/local/audit/export`

4. 監査共有に対応する番号を入力します。 *`audit_share_number`*

   監査共有へのアクセスを許可している IP アドレスに番号が振られ、リストに表示されます。

5. 削除する IP アドレスに対応する番号を入力します。

   監査共有が更新され、この IP アドレスの監査クライアントからのアクセスは許可されなくなります。

6. プロンプトが表示されたら、 * Enter * を押します。

   NFS 設定ユーティリティが表示されます。

7. NFS設定ユーティリティを閉じます。 `exit`
8. StorageGRID 環境が複数データセンターサイトの環境であり、他のサイトにも管理ノードが含まれている場合は、必要に応じてこれらの監査共有を無効にします。
   a. 各サイトの管理ノードにリモートからログインします。
      i. 次のコマンドを入力します。 `ssh admin@grid_node_IP`
      ii. に記載されているパスワードを入力します `Passwords.txt` ファイル。
      iii. 次のコマンドを入力してrootに切り替えます。 `su -`

iv. に記載されているパスワードを入力します `Passwords.txt` ファイル。

b. 同じ手順を繰り返して、追加の管理ノードごとに監査共有を設定します。

c. リモート管理ノードへのリモートのSecure Shellログインを終了します。 `exit`

9. コマンドシェルからログアウトします。 `exit`

NFS監査クライアントの**IP**アドレスの変更

1. 既存の NFS 監査共有に新しい IP アドレスを追加します。
2. 元の IP アドレスを削除します。

関連情報

"監査共有へのNFS監査クライアントの追加"

"監査共有からのNFS監査クライアントの削除"

アーカイブノードの管理

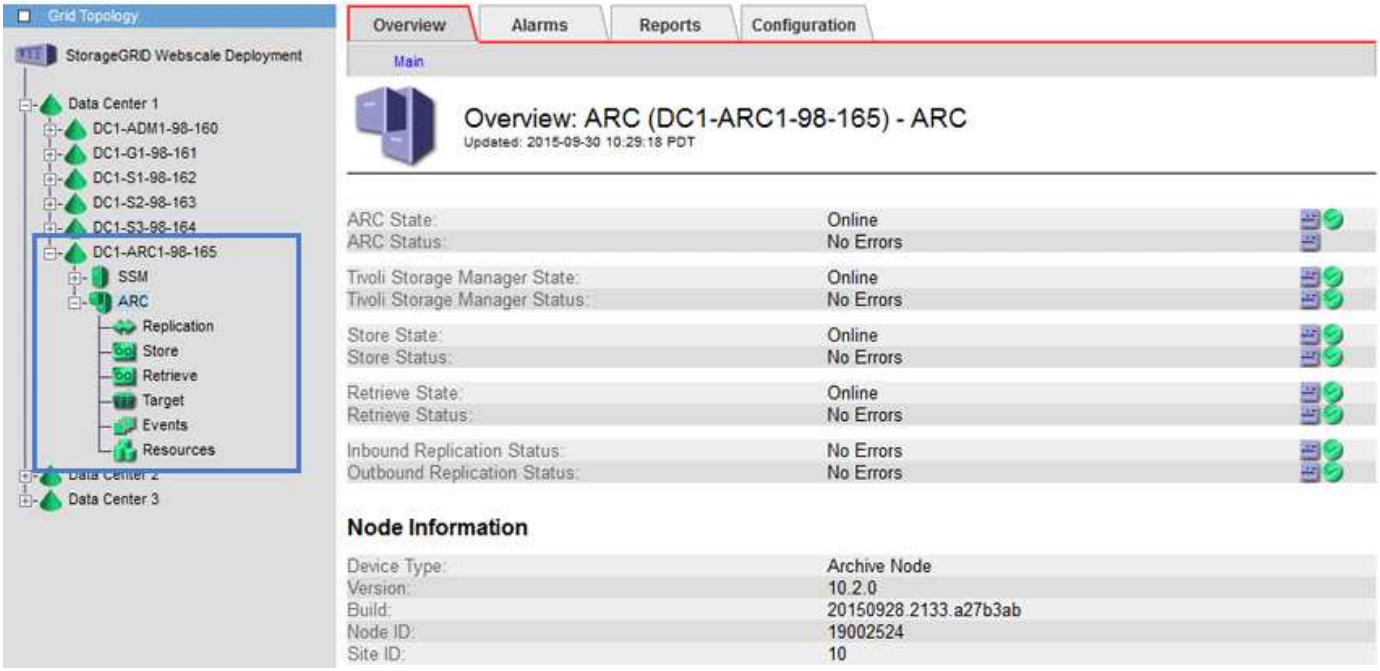
必要に応じて、StorageGRID システムの各データセンターサイトにアーカイブノードを導入して、Tivoli Storage Manager（TSM）などの外部アーカイブストレージシステムに接続できます。

外部ターゲットへの接続を設定したあと、 TSM のパフォーマンスを最適化するようにアーカイブノードを設定できます。 TSM サーバの容量が上限に近づいている場合や TSM サーバを使用できない場合は、アーカイブノードをオフラインにできます。また、レプリケーションと読み出しを設定できます。アーカイブノードにカスタムアラームを設定することもできます。

- "アーカイブノードとは"
- "アーカイブストレージへのアーカイブノード接続を設定しています"
- "アーカイブノード用のカスタムアラームの設定"
- "Tivoli Storage Managerを統合する"

アーカイブノードとは

アーカイブノードは、オブジェクトデータの長期保管用に外部アーカイブストレージシステムをターゲットとするインターフェイスを提供します。また、この接続、および StorageGRID システムとターゲットの外部アーカイブストレージシステム間でのオブジェクトデータ転送も監視します。



削除はできないが定期的にはアクセスされないオブジェクトデータは、ストレージノードの回転式ディスクから、クラウドやテープなどの外部アーカイブストレージにいつでも移動できます。オブジェクトデータをこのようにアーカイブするには、データセンターサイトのアーカイブノードを設定し、次にこのアーカイブノードをコンテンツ配置手順の「ターゲット」として選択した ILM ルールを設定します。アーカイブノードは、アーカイブされたオブジェクトデータ自体の管理は行いません。これは外部アーカイブデバイスによって行われます。

オブジェクトメタデータはアーカイブされず、ストレージノードに残ります。

ARC サービスとは

Archive Node's Archive（ARC）サービスは、TSMミドルウェア経由のテープなど、外部アーカイブストレージへの接続を設定できる管理インターフェイスです。

ARC サービスは、外部のアーカイブストレージシステムと連携することにより、ニアラインストレージ用にオブジェクトデータを送信し、クライアントアプリケーションがアーカイブされたオブジェクトを要求したときに読み出しを実行します。クライアントアプリケーションがアーカイブされたオブジェクトを要求すると、ストレージノードは ARC サービスからオブジェクトデータを要求します。ARC サービスは外部のアーカイブストレージシステムに要求を送信し、アーカイブストレージシステムは要求されたオブジェクトデータを読み出して ARC サービスに送信します。ARC サービスはオブジェクトデータを検証してストレージノードに転送し、ストレージノードは要求元のクライアントアプリケーションにオブジェクトを返します。

TSM ミドルウェア経由でテープにアーカイブされたオブジェクトデータに対する要求は、読み出し効率が向上するように管理されます。要求は、テープに格納されているオブジェクトの順番と同じになるように順序が調整されたうえで、ストレージデバイスへの送信用のキューに登録されます。アーカイブデバイスによっては、異なるボリューム上のオブジェクトに対する複数の要求を同時に処理できます。

アーカイブストレージへのアーカイブノード接続を設定しています

外部アーカイブに接続するようにアーカイブノードを設定する場合は、ターゲットタイプを選択する必要があります。

StorageGRID システムでは、S3インターフェイスを使用したクラウドへのオブジェクトデータのアーカイブ、またはTivoli Storage Manager（TSM）ミドルウェアを使用したテープへのオブジェクトデータのアーカイブがサポートされます。

アーカイブノードにアーカイブターゲットのタイプを設定したあとに、そのタイプを変更することはできません。

- "S3 APIを使用したクラウドへのアーカイブ"
- "TSMミドルウェア経由でテープにアーカイブ"
- "アーカイブノードの読み出し設定を構成しています"
- "アーカイブノードのレプリケーションを設定しています"

S3 APIを使用したクラウドへのアーカイブ

アーカイブノードは、 Amazon Web Services （ AWS ）に直接接続するように設定することも、 S3 API を使用して StorageGRID システムと連携可能な他のシステムに接続するように設定することもできます。

S3 API を使用してアーカイブノードから外部のアーカイブストレージシステムにオブジェクトを移動する処理は、より多くの機能を提供する ILM Cloud Storage Pools に置き換えられました。Cloud Tiering - Simple Storage Service （ S3 ） * オプションは引き続きサポートされていますが、代わりにクラウドストレージプールの実装を推奨します。

「 Cloud Tiering - Simple Storage Service （ S3 ） * 」オプションを指定してアーカイブノードを現在使用している場合は、クラウドストレージプールへのオブジェクトの移行を検討してください。情報ライフサイクル管理を使用してオブジェクトを管理する手順を参照してください。

関連情報

"ILM を使用してオブジェクトを管理する"

S3 APIの接続を設定します

S3 インターフェイスを使用してアーカイブノードに接続する場合は、 S3 API の接続を設定する必要があります。これらの設定が完了するまで ARC サービスは外部アーカイブストレージシステムと通信できないため、 Major アラーム状態のままです。

S3 API を使用してアーカイブノードから外部のアーカイブストレージシステムにオブジェクトを移動する処理は、より多くの機能を提供する ILM Cloud Storage Pools に置き換えられました。Cloud Tiering - Simple Storage Service （ S3 ） * オプションは引き続きサポートされていますが、代わりにクラウドストレージプールの実装を推奨します。

「 Cloud Tiering - Simple Storage Service （ S3 ） * 」オプションを指定してアーカイブノードを現在使用している場合は、クラウドストレージプールへのオブジェクトの移行を検討してください。情報ライフサイクル管理を使用してオブジェクトを管理する手順を参照してください。

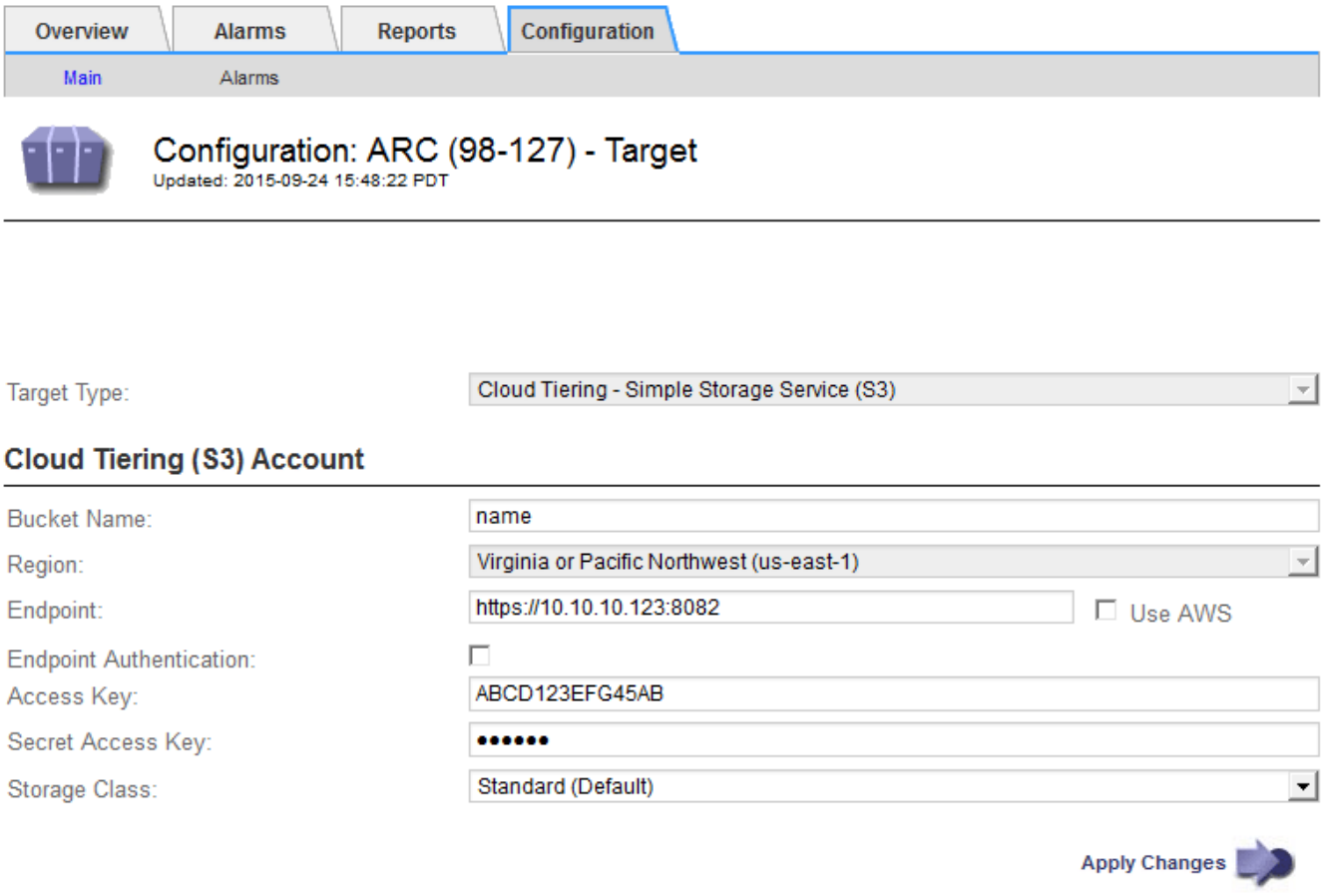
必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

- 特定のアクセス権限が必要です。
- ターゲットのアーカイブストレージシステム上にバケットを作成しておく必要があります。
  - このバケットは1つのアーカイブノード専用にする必要があります。他のアーカイブノードやアプリケーションでは使用できません。
  - バケットには、場所に応じた適切なリージョンを選択する必要があります。
  - バケットのバージョン管理は一時停止に設定する必要があります。
- オブジェクトのセグメント化を有効にして、最大セグメントサイズは4.5GiB（4、831、838、208バイト）以下にする必要があります。S3 が外部アーカイブストレージシステムとして使用されている場合、この値を超える S3 API 要求は失敗します。

手順

1. Support > Tools > Grid Topology *を選択します。
2. アーカイブノード* ARC *ターゲット*を選択します。
3. * Configuration * > * Main * を選択します。



4. ターゲットタイプドロップダウンリストから * Cloud Tiering - Simple Storage Service （ S3 ） * を選択します。

ターゲットタイプを選択するまで、構成設定は使用できません。

5. アーカイブノードからターゲットの外部の S3 対応アーカイブストレージシステムへの接続に使用するクラウドの階層化（ S3 ）アカウントを設定します。

このページのフィールドのほとんどはわかりやすいもので、説明を必要としません。以下は、説明が必要なフィールドです。

- * Region * ： * Use AWS * が選択されている場合にのみ選択できます。バケットのリージョンと同じリージョンを選択する必要があります。
- * Endpoint * および * Use AWS * ： Amazon Web Services （ AWS ）の場合は、「 * Use AWS * 」を選択します。* エンドポイント * には、バケット名属性とリージョン属性に基づいてエンドポイント URL が自動的に入力されます。例：

  ```
  https://bucket.region.amazonaws.com
  ```

  AWS 以外のターゲットの場合は、ポート番号を含め、バケットをホストしているシステムの URL を入力します。例：

```
https://system.com:1080
```

- * エンドポイント認証 *: デフォルトで有効になっています。外部アーカイブストレージシステムへのネットワークが信頼されている場合は、チェックボックスをオフにして、対象の外部アーカイブストレージシステムのエンドポイントの SSL 証明書およびホスト名検証を無効にすることができます。StorageGRID システムの別のインスタンスがターゲットのアーカイブストレージデバイスであり、システムに公開署名された証明書が設定されている場合、このチェックボックスはオンのままでかまいません。
- * ストレージクラス * ：通常のストレージには「 * Standard （デフォルト） * 」を選択します。簡単に再作成できるオブジェクトに対してのみ、「冗長性の低下」を選択します。* 冗長性の低下 * 信頼性の低い低コストのストレージを提供します。ターゲットのアーカイブストレージシステムが StorageGRID システムの別のインスタンスの場合、ストレージクラス * はオブジェクトの取り込み時に実行されるオブジェクトの中間コピー数を、デュアルコミットがオブジェクトの取り込み時に使用される場合にターゲットシステムで制御します。

6. [変更の適用 *] をクリックします。

   指定した設定が検証され、 StorageGRID システムに適用されます。いったん設定したターゲットは変更できません。

関連情報

"ILM を使用してオブジェクトを管理する"

S3 APIの接続設定の変更

S3 API を使用して外部のアーカイブストレージシステムに接続するようにアーカイブノードを設定したあとで接続が変更された場合、一部の設定を変更できます。

必要なもの

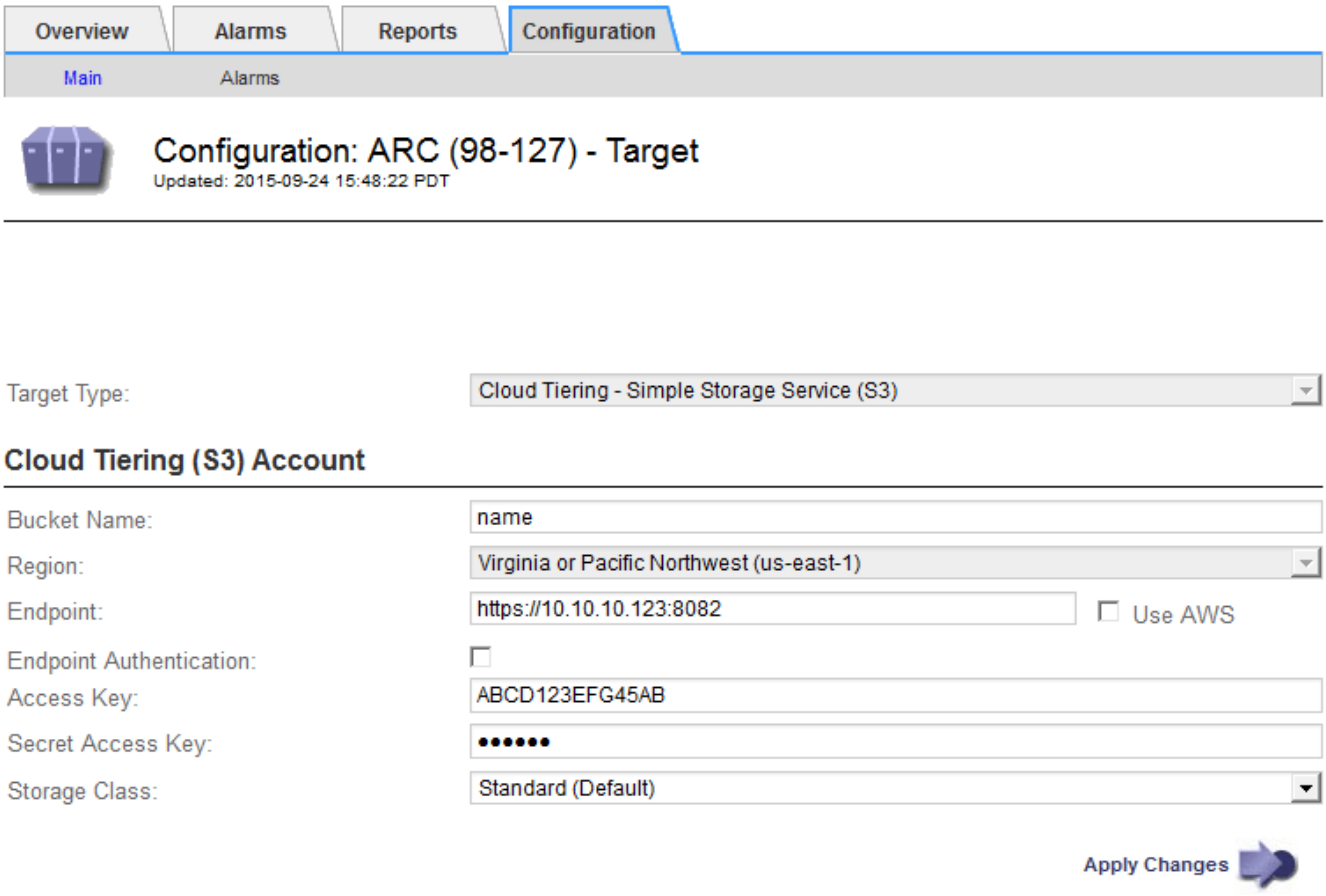
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

このタスクについて

クラウドの階層化（ S3 ）アカウントを変更した場合は、アーカイブノードによって以前にバケットに取り込まれたすべてのオブジェクトを含む、バケットへの読み取り / 書き込みアクセスがユーザアクセスクレデンシャルに割り当てられている必要があります。

手順

1. Support > Tools > Grid Topology *を選択します。
2. 「アーカイブノード **ARC** ターゲット」を選択します。
3. * Configuration * > * Main * を選択します。



4. 必要に応じて、アカウント情報を変更します。

   ストレージクラスを変更すると、新しいオブジェクトデータは新しいストレージクラスで格納されます。既存のオブジェクトは、引き続き取り込み時に設定したストレージクラスで格納されます。

   バケット名、リージョン、およびエンドポイントは AWS の値を使用し、変更することはできません。

5. [変更の適用 *] をクリックします。

クラウドの階層化サービスの状態を変更しています

クラウドの階層化サービスの状態を変更することで、 S3 API を使用して接続する外部のアーカイブストレージシステムに対してアーカイブノードが読み取り / 書き込みできるかどうかを制御できます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

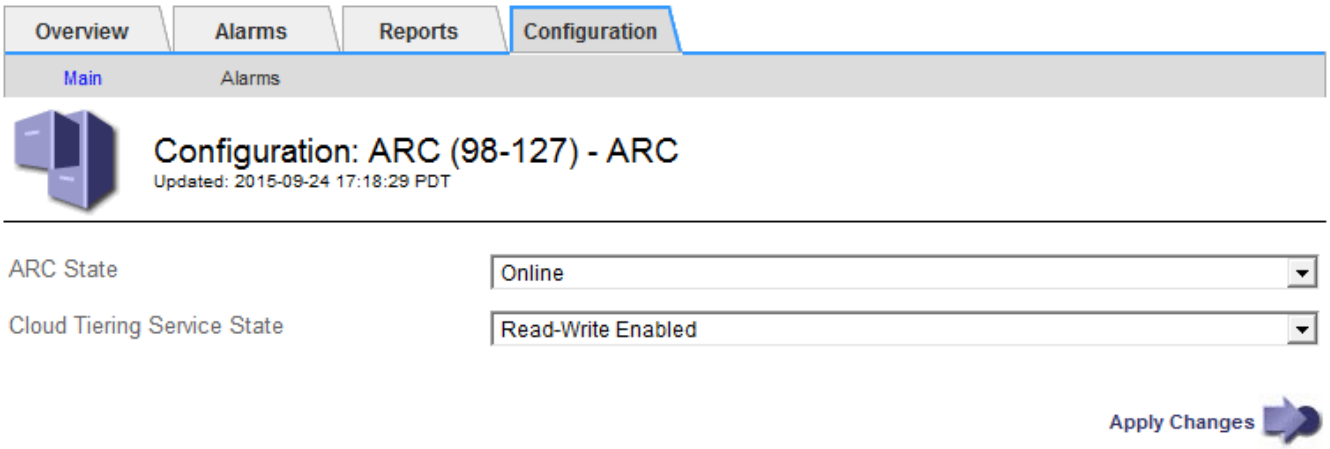
- 特定のアクセス権限が必要です。
- アーカイブノードが設定されている必要があります。

このタスクについて

クラウドの階層化サービスの状態を「 * Read-Write Disabled 」に変更すると、アーカイブノードを効果的にオフラインにできます。

手順

1. Support **>** Tools **>** Grid Topology *を選択します。
2. 「 * _ アーカイブノード _ * > * ARC * 」を選択します。
3. * Configuration * > * Main * を選択します。



4. クラウドの階層化サービスの状態 * を選択します。
5. [変更の適用 *] をクリックします。

S3 API接続のストア障害数のリセット

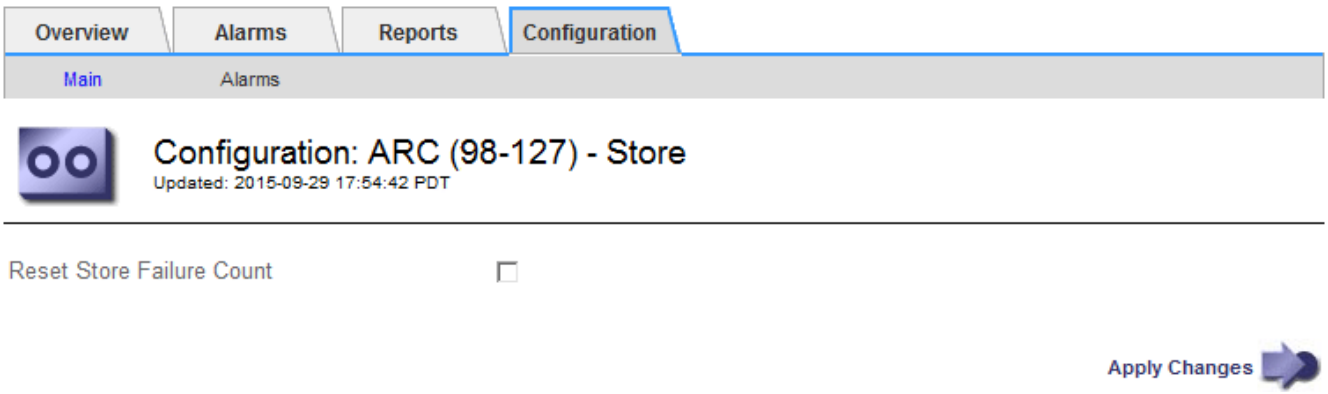
アーカイブノードが S3 API 経由でアーカイブストレージシステムに接続している場合は、ストア障害数をリセットでき、 ARVF （ Store Failures ）アラームをクリアできます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

手順

1. Support **>** Tools **>** Grid Topology *を選択します。
2. 「*アーカイブノード **ARC** Store *」を選択します。
3. * Configuration * > * Main * を選択します。



4. 「 Reset Store Failure Count 」を選択します。
5. [変更の適用 *] をクリックします。

   Store Failures 属性がゼロにリセットされます。

「**Cloud Tiering - S3**」からクラウドストレージプールへのオブジェクトの移行

現在 Cloud Tiering - Simple Storage Service （ S3 ） * 機能を使用してオブジェクトデータを S3 バケットに階層化している場合は、代わりにクラウドストレージプールへのオブジェクトの移行を検討してください。クラウドストレージプールは拡張性に優れたアプローチを提供し、 StorageGRID システム内のすべてのストレージノードを活用します。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。
- クラウド階層化用に設定された S3 バケットにオブジェクトが格納済みである。

> オブジェクトデータを移行する前に、ネットアップのアカウント担当者に問い合わせて関連するコストについて把握してください。

このタスクについて

ILM から見た場合、クラウドストレージプールはストレージプールに似ています。ただし、ストレージプールは StorageGRID システム内のストレージノードまたはアーカイブノードで構成されますが、クラウドストレージプールは外部の S3 バケットで構成されます。

オブジェクトを「 Cloud Tiering - S3 」からクラウドストレージプールに移行する前に、 S3 バケットを作成し、 StorageGRID にクラウドストレージプールを作成する必要があります。次に、新しい ILM ポリシーを作成し、クラウド階層化バケットにオブジェクトを格納するために使用していた ILM ルールをコピーし、同じオブジェクトをクラウドストレージプールに格納するように変更します。

オブジェクトがクラウドストレージプールに格納されている場合、それらのオブジェクトのコピーを StorageGRID にも格納することはできません。現在クラウド階層化に使用している ILM ルールが複数の場所に同時にオブジェクトを格納するように設定されている場合は、その機能が失われるため、このオプションの移行を引き続き実行するかどうかを検討してください。移行を続行する場合は、既存のルールをコピーするのではなく、新しいルールを作成する必要があります。

手順

1. クラウドストレージプールを作成

   クラウドストレージプールに新しい S3 バケットを使用して、クラウドストレージプールで管理されるデータのみが含まれるようにします。

2. クラウド階層化バケットに格納する原因 オブジェクトをアクティブな ILM ポリシーで特定します。
3. 該当するルールをコピーします。
4. コピーしたルールで、配置場所を新しいクラウドストレージプールに変更します。
5. コピーしたルールを保存します。
6. 新しいルールを使用する新しいポリシーを作成します。
7. 新しいポリシーをシミュレートしてアクティブ化します。

   新しいポリシーがアクティブ化されて ILM 評価が実行されると、クラウド階層化用に設定された S3 バケットからクラウドストレージプール用に設定された S3 バケットにオブジェクトが移動します。グリッド上の使用可能なスペースに影響はありません。クラウドストレージプールに移動されたオブジェクトは、クラウド階層化バケットから削除されます。

関連情報

"ILM を使用してオブジェクトを管理する"

TSMミドルウェア経由でのテープへのアーカイブ

Tivoli Storage Manager （ TSM ）サーバをターゲットとするようにアーカイブノードを構成できます。 TSM サーバは、テープライブラリを含むランダムまたはシーケンシャルアクセスのストレージデバイスとの間でオブジェクトデータを格納および読み出すための論理インターフェイスです。

アーカイブノードの ARC サービスは TSM サーバに対するクライアントとして機能し、 Tivoli Storage Manager をアーカイブストレージシステムと通信するためのミドルウェアとして使用します。

TSM 管理クラス

TSM ミドルウェアによって定義された管理クラスは、 TSM のバックアップおよびアーカイブ処理がどのように機能するかを示します。この管理クラスを使用して、 TSM サーバによって適用されるコンテンツ用のルールを指定できます。これらのルールは StorageGRID システムの ILM ポリシーとは独立して機能します。オブジェクトは永続的に格納され、アーカイブノードによっていつでも読み出し可能であるという StorageGRID システムの要件と矛盾しないことが必要です。アーカイブノードから TSM サーバにオブジェクトデータが送信されたあと、 TSM サーバが管理するテープにオブジェクトデータが格納される間、 TSM のライフサイクルと保持のルールが適用されます。

TSM 管理クラスは、アーカイブノードから TSM サーバにオブジェクトデータが送信されたあと、データの場所または保持のルールを適用するために TSM サーバで使用されます。たとえば、データベースのバックアップとして識別されたオブジェクト（新しいデータで上書き可能な一時的コンテンツ）を、アプリケーションデータ（無期限に保持する必要のある固定コンテンツ）とは別の方法で処理できます。

TSMミドルウェアへの接続を設定しています

アーカイブノードが Tivoli Storage Manager （ TSM ）ミドルウェアと通信するためには、いくつかの設定を行う必要があります。

必要なもの

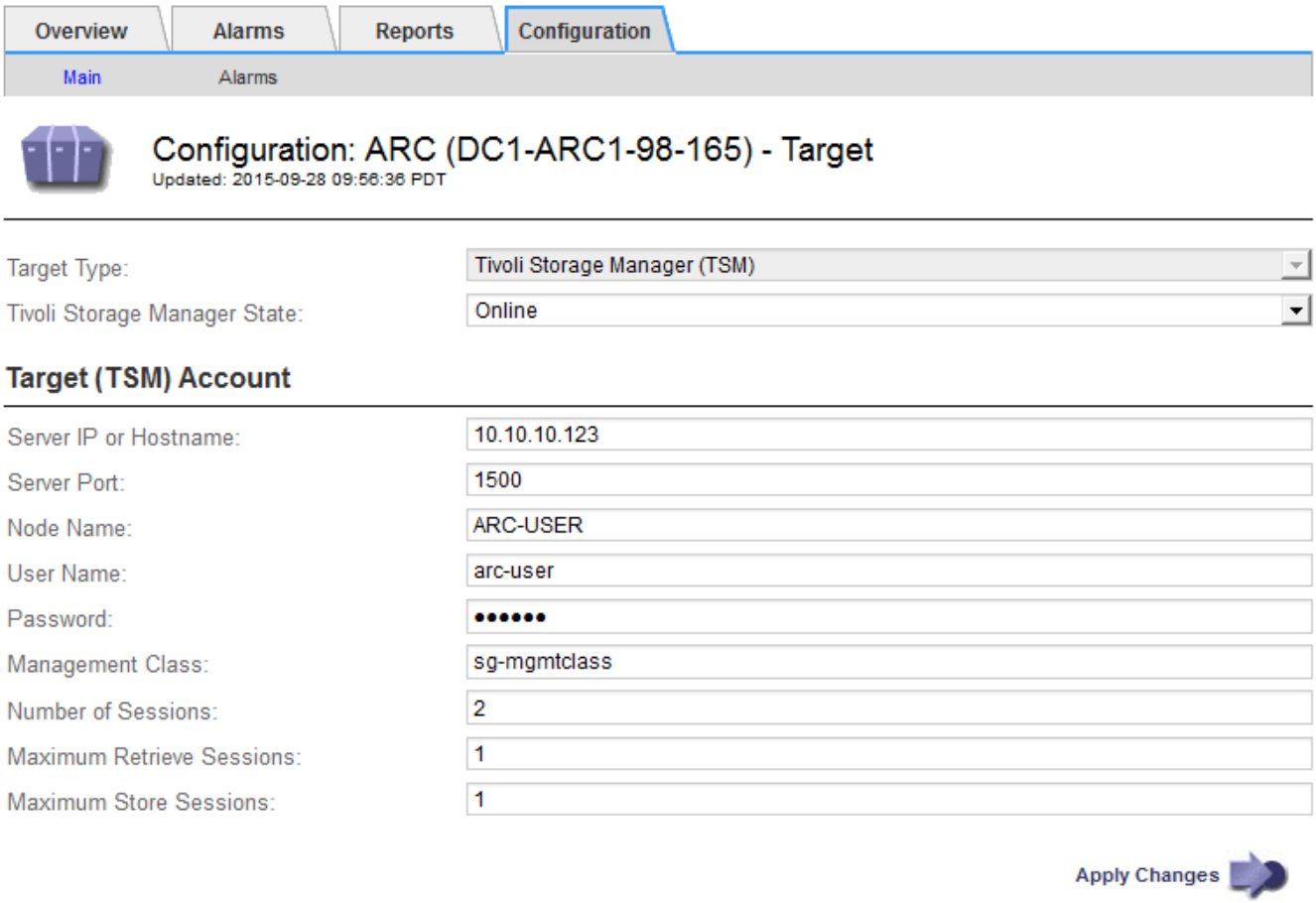
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

このタスクについて

これらの設定が完了するまで ARC サービスは Tivoli Storage Manager と通信できないため、 Major アラーム状態のままです。

手順

1. Support **>** Tools **>** Grid Topology *を選択します。
2. 「アーカイブノード **ARC** ターゲット」を選択します。
3. * Configuration * > * Main * を選択します。



4. [ターゲット・タイプ **]** ドロップダウン・リストから **'[** Tivoli Storage Manager(TSM)*] を選択します
5. Tivoli Storage Manager State * では、 TSM ミドルウェアサーバからの読み出しを防ぐために「 * Offline * 」を選択します。

   デフォルトでは、「 Tivoli Storage Manager State 」は「 Online 」に設定されています。つまり、アーカイブノードは TSM ミドルウェアサーバからオブジェクトデータを読み出すことができます。

6. 次の情報を入力します。

   - * Server IP or Hostname * ： ARC サービスが使用する TSM ミドルウェアサーバの IP アドレスまたは完全修飾ドメイン名を指定します。デフォルトの IP アドレスは 127.0.0.1 です。
   - * Server Port * ： ARC サービスの接続先の TSM ミドルウェアサーバ上のポート番号を指定します。デフォルトは 1500 です。
   - * Node Name * ：アーカイブノードの名前を指定します。TSM ミドルウェアサーバに登録した名前（ arc - user ）を入力する必要があります。
   - * User Name * ： ARC サービスが TSM サーバへのログインに使用するユーザ名を指定します。デフォルトのユーザ名（ arc - user ）またはアーカイブノード用に指定した管理ユーザを入力します。
   - * Password * ： ARC サービスが TSM サーバへのログインに使用するパスワードを指定します。
   - * 管理クラス * ：オブジェクトが StorageGRID システムに保存されるときに管理クラスが指定されていない場合や、指定した管理クラスが TSM ミドルウェアサーバ上で定義されていない場合に使用するデフォルトの管理クラスを指定します。
   - * Number of Sessions * ： TSM ミドルウェアサーバ上にあるアーカイブノード専用のテープドライブの数を指定します。アーカイブノードは、最大でマウントポイントごとに 1 つのセッションと少数（ 5 つ未満）の追加セッションを同時に作成します。

     アーカイブノードを登録または更新したときには、この値を MAXNUMMP （マウントポイントの最大数）と同じ値に変更する必要があります（登録コマンドでは、値が設定されていない場合の MAXNUMMP のデフォルト値は 1 です）。

   また、 TSM サーバの MAXSESSIONS の値を、 ARC サービス用に設定されている Sessions の数以上の数値に変更する必要があります。TSM サーバ上の MAXSESSIONS のデフォルト値は 25 です。

   - * Maximum Retrieve Sessions * ： ARC サービスが読み出し処理用に TSM ミドルウェアサーバに対して開くことができるセッションの最大数を指定します。ほとんどの場合、適切な値は「セッション数 - ストアセッションの最大数」です。1 つのテープ・ドライブを共有してストレージと取得を行う必要がある場合は ' セッション数に等しい値を指定します
   - * Maximum Store Sessions * ： ARC サービスがアーカイブ処理用に TSM ミドルウェアサーバに対して開くことができる同時セッションの最大数を指定します。

     この値は、対象のアーカイブストレージシステムが一杯で、読み出しのみが可能な場合を除き、 1 に設定する必要があります。すべてのセッションを読み出しに使用するには、この値を 0 に設定します。

7. [変更の適用 *] をクリックします。

TSMミドルウェアセッション用のアーカイブノードの最適化

アーカイブノードのセッションを設定することで、 Tivoli Server Manager （ TSM ）に

接続するアーカイブノードのパフォーマンスを最適化できます。

必要なもの

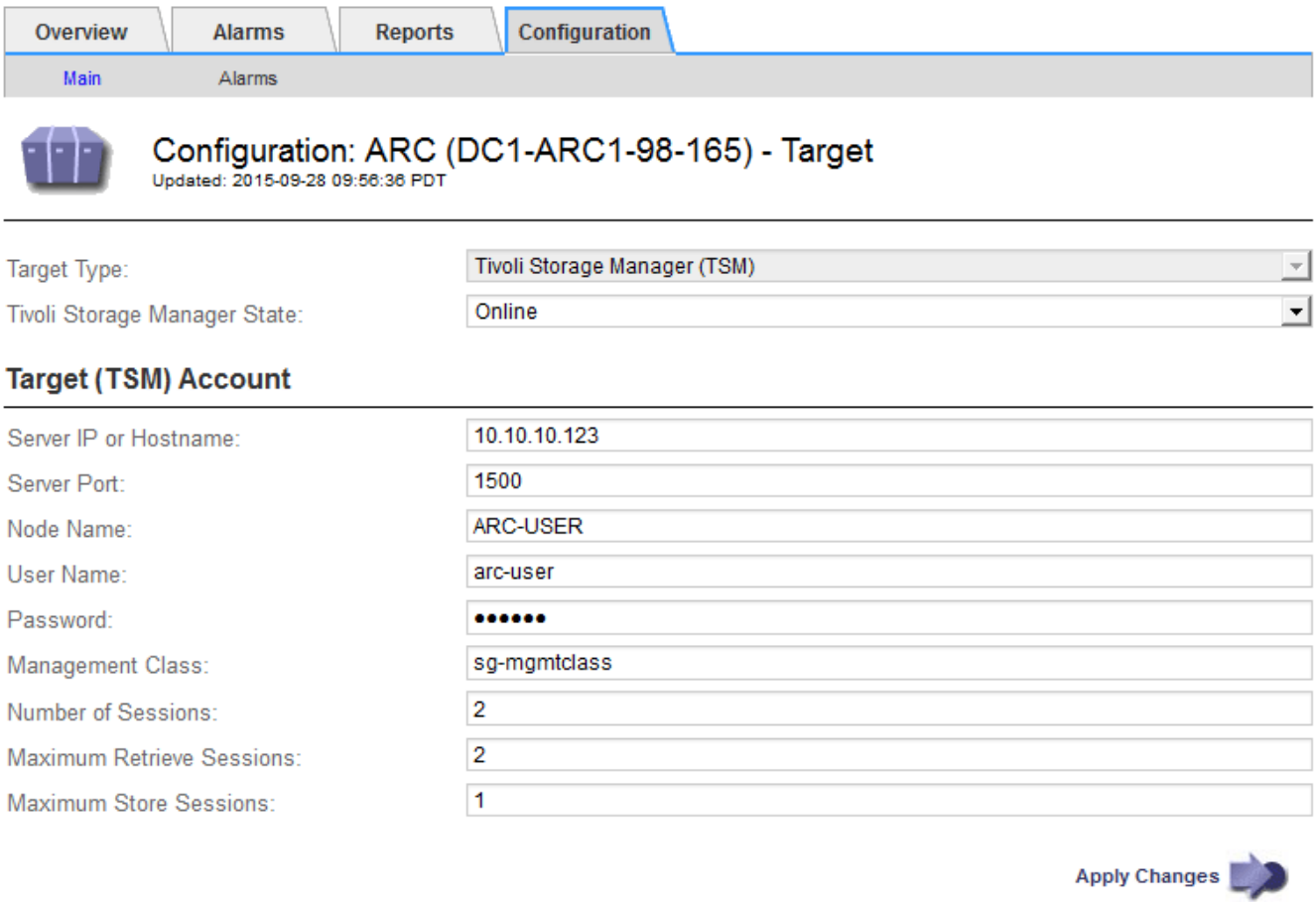
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

このタスクについて

通常、アーカイブノードが TSM ミドルウェアサーバに対して同時に開くことができるセッションの数は、TSM サーバが所有するアーカイブノード専用のテープドライブの数に設定されます。1 本のテープドライブがストレージ用に割り当てられ、残りは読み出し用に割り当てられます。ただし、ストレージノードがアーカイブノードのコピーからリビルドされている場合や、アーカイブノードが読み取り専用モードで動作している場合は、読み出しセッションの最大数を同時セッション数と同じに設定することで、 TSM サーバのパフォーマンスを最適化できます。したがって、すべてのドライブを同時に読み出しに使用できます。また、必要に応じて、これらのドライブのうち 1 つをストレージに使用することもできます。

手順

1. Support **>** Tools **>** Grid Topology *を選択します。
2. 「アーカイブノード **ARC** ターゲット」を選択します。
3. * Configuration * > * Main * を選択します。
4. Maximum Retrieve Sessions * を Number of Sessions * と同じに変更します。



5. [変更の適用 *] をクリックします。

TSMのアーカイブ状態とカウンタの設定

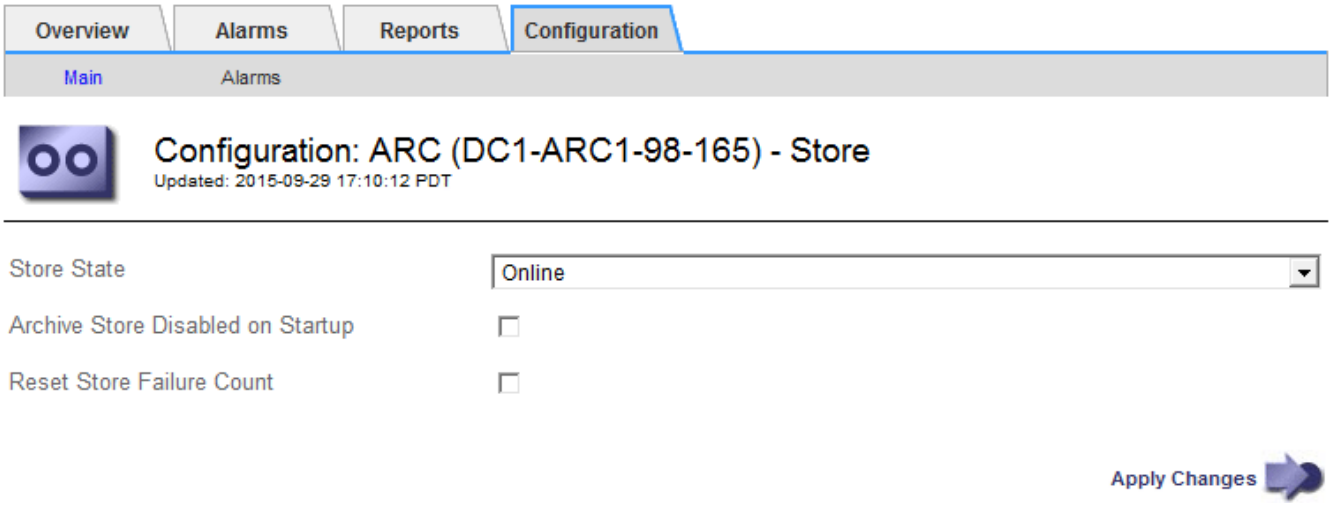
アーカイブノードが TSM ミドルウェアサーバに接続している場合は、アーカイブノードのアーカイブストアの状態をオンラインまたはオフラインに設定できます。また、アーカイブノードの初回起動時にアーカイブストアを無効にしたり、関連するアラーム用に追跡されているエラー数をリセットしたりすることもできます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

手順

1. Support **>** Tools **>** Grid Topology *を選択します。
2. 「*アーカイブノード **ARC** Store *」を選択します。
3. * Configuration * > * Main * を選択します。



4. 必要に応じて次の設定を変更します。
   - Store State ：コンポーネントの状態を次のいずれかに設定します。
     - Online ：アーカイブノードはオブジェクトデータを処理してアーカイブストレージシステムに格納できます。
     - Offline ：アーカイブノードはオブジェクトデータを処理してアーカイブストレージシステムに格納できません。
   - Archive Store Disabled on Startup ：オンにすると、アーカイブストアコンポーネントは再起動後も読み取り専用のままになります。ターゲットのアーカイブストレージシステムへの格納を継続的に無効にする場合に使用します。対象のアーカイブストレージシステムでコンテンツを受け入れられない場合に便利です。
   - Reset Store Failure Count ：ストア障害のカウンタをリセットします。この設定を使用して、 ARVF （ Stores Failure ） アラームをクリアできます。
5. [変更の適用 *] をクリックします。

関連情報

"TSMサーバの容量が上限に達した場合のアーカイブノードの管理"

TSMサーバの容量が上限に達した場合のアーカイブノードの管理

TSM サーバには、管理対象の TSM データベースまたはアーカイブメディアストレージの容量が上限に近づいている場合にアーカイブノードに通知する手段がありません。アーカイブノードは、 TSM サーバが新しいコンテンツの受け入れを停止したあとも引き続き TSM サーバに転送するオブジェクトデータを受け入れますが、TSM サーバが管理するメディアにこのコンテンツを書き込むことはできません。アラームがトリガーされます。この状況を回避するには、 TSM サーバをプロアクティブに監視します。

必要なもの

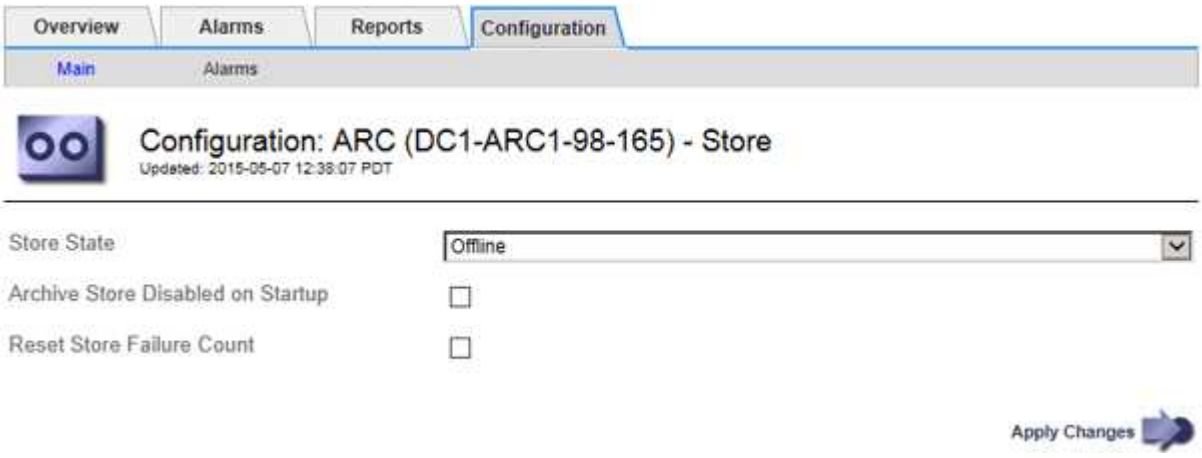
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

このタスクについて

ARCサービスからTSMサーバにさらにコンテンツが送信されないようにするには、* ARC * Store *コンポーネントをオフラインにします。この手順 は、 TSM サーバがメンテナンスに使用できないときにアラームを生成しない場合にも役立ちます。

手順

1. Support **>** Tools **>** Grid Topology *を選択します。
2. 「*アーカイブノード **ARC** Store *」を選択します。
3. * Configuration * > * Main * を選択します。



4. 「Store State」を「」に変更します `Offline`。
5. 「 Archive Store Disabled on Startup * 」を選択します。
6. [変更の適用 *] をクリックします。

TSMミドルウェアが容量の限界に達した場合にアーカイブノードを読み取り専用に設定

ターゲットの TSM ミドルウェアサーバが容量の限界に達した場合、読み出しのみを実行するようにアーカイブノードを最適化できます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

手順

1. Support > Tools > Grid Topology *を選択します。
2. 「アーカイブノード **ARC** ターゲット」を選択します。
3. * Configuration * > * Main * を選択します。
4. Maximum Retrieve Sessions を Number of Sessions に示されている同時セッション数と同じ数に変更します
5. 最大ストアセッション数を 0 に変更します。

> アーカイブノードが読み取り専用の場合、最大ストアセッション数を 0 に変更する必要はありません。ストアセッションは作成されません。

6. [変更の適用 *] をクリックします。

アーカイブノードの読み出し設定を構成しています

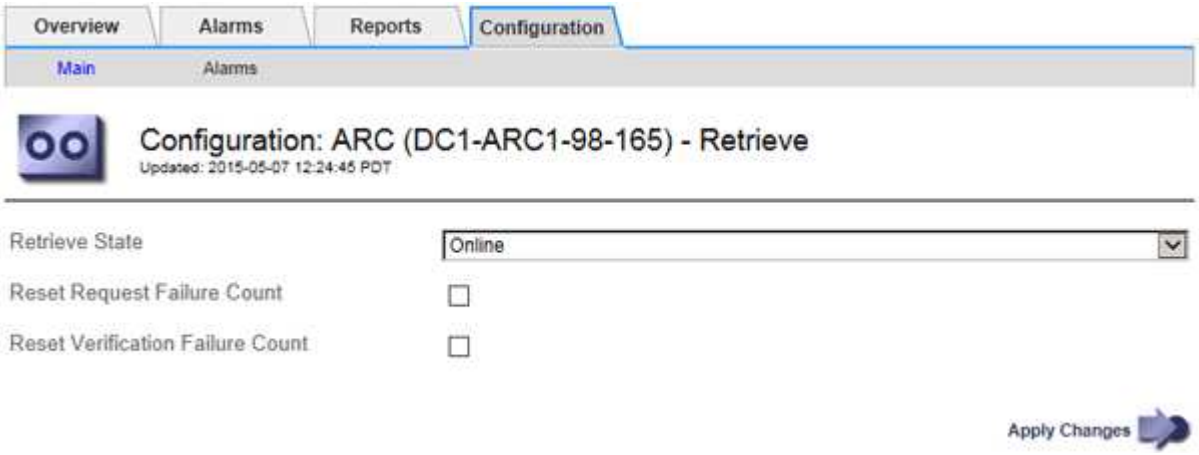
アーカイブノードの読み出し設定を行って、状態をオンラインまたはオフラインに設定したり、関連するアラームで追跡されているエラー数をリセットしたりできます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

手順

1. Support > Tools > Grid Topology *を選択します。
2. アーカイブノード* ARC *読み出し*を選択します。
3. * Configuration * > * Main * を選択します。



4. 必要に応じて次の設定を変更します。

- * Retrieve State * ：コンポーネントの状態を次のいずれかに設定します。
  - Online ：グリッドノードがアーカイブメディアデバイスからオブジェクトデータを読み出すことができます。
  - Offline ：グリッドノードはオブジェクトデータを読み出すことができません。
- Reset Request Failures Count ：オンにすると、要求エラーのカウンタがリセットされます。この設定を使用して、 ARRF （ Request Failures ）アラームをクリアできます。
- Reset Verification Failure Count ：オンにすると、読み出したオブジェクトデータの検証エラーのカウンタがリセットされます。この設定を使用して、 ARRV （ Verification Failures ）アラームをクリアできます。

5. [変更の適用 *] をクリックします。

アーカイブノードのレプリケーションを設定しています

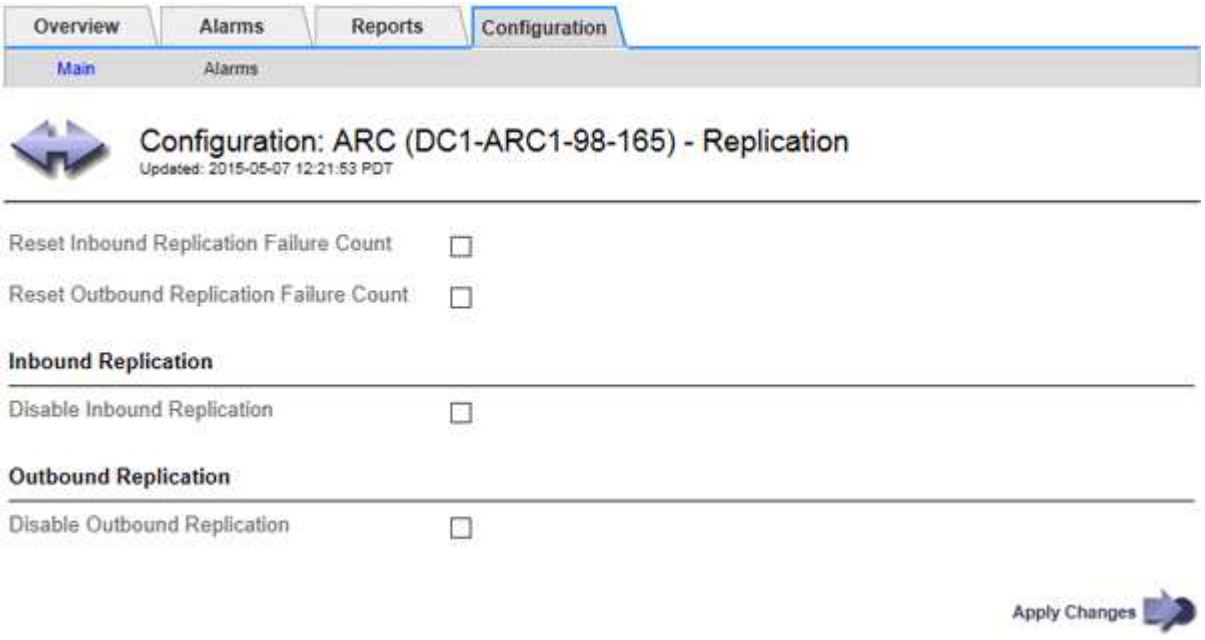
アーカイブノードのレプリケーション設定を行って、インバウンドおよびアウトバウンドのレプリケーションを無効にしたり、関連するアラームで追跡されているエラー数をリセットしたりできます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

手順

1. Support **>** Tools **>** Grid Topology *を選択します。
2. 「 * _ アーカイブノード _ * > * ARC * > * レプリケーション * 」を選択します。
3. * Configuration * > * Main * を選択します。



4. 必要に応じて次の設定を変更します。
   - * Reset Inbound Replication Failure Count * ：インバウンドレプリケーションエラーのカウンタをリセ

ットする場合に選択します。この設定を使用して、 RIRF （ Inbound Replications - - Failed ）アラームをクリアできます。

- **Reset Outbound Replication Failure Count** ：アウトバウンドレプリケーションエラーのカウンタをリセットする場合に選択します。これを使用すると、 RORF （ Outbound Replications - - Failed ）アラームをクリアできます。
- * インバウンド複製を無効にする *: メンテナンスまたは手順 のテストの一環としてインバウンド複製を無効にする場合に選択します。通常の運用中はオフのままにします。

  インバウンドレプリケーションを無効にすると、 ARC サービスからオブジェクトデータを読み出して StorageGRID システム内の別の場所へレプリケートすることはできますが、システム内の別の場所からこの ARC サービスにオブジェクトをレプリケートすることはできません。ARC サービスは読み取り専用です。

- * アウトバウンドレプリケーションの無効化 * ：メンテナンスまたはテスト用手順 の一環としてアウトバウンドレプリケーション（ HTTP 読み出し用のコンテンツ要求を含む）を無効にする場合は、このチェックボックスを選択します。通常の運用中はオフのままにします。

  アウトバウンドレプリケーションを無効にすると、この ARC サービスにオブジェクトデータをコピーして ILM ルールに従うことはできますが、 ARC サービスからオブジェクトデータを読み出して StorageGRID システム内の別の場所へコピーすることはできません。ARC サービスは書き込み専用です。

5. [変更の適用 *] をクリックします。

アーカイブノード用のカスタムアラームの設定

ARQL 属性と ARRL 属性のカスタムアラームを設定する必要があります。これらの属性は、アーカイブノードがアーカイブストレージシステムからオブジェクトデータを読み出す際の速度と効率を監視します。

- ARQL ：平均キュー長。アーカイブストレージシステムから読み出し用にキューに登録されたオブジェクトデータの平均時間（マイクロ秒）。
- ARRL ：平均リクエストレイテンシ。アーカイブノードがアーカイブストレージシステムからオブジェクトデータを読み出すために必要な平均時間（マイクロ秒）。

これらの属性の許容値は、アーカイブストレージシステムの設定および使用方法によって異なります。（ * ARC * > * Retrieve * > * Overview * > * Main * に移動します）。 要求のタイムアウトに設定された値や、取得要求に使用できるセッション数は特に影響を受けます。

統合が完了したら、アーカイブノードによるオブジェクトデータの読み出しを監視して、通常の読み出し時間およびキューの長さを確認します。次に、異常な動作状態が発生した場合にトリガーされる、 ARQL と ARRL のカスタムアラームを作成します。

関連情報

"トラブルシューティングを監視します"

Tivoli Storage Managerを統合する

ここでは、アーカイブノードをTivoli Storage Manager（TSM）サーバと統合する際のベストプラクティスとセットアップ情報について、TSMサーバの設定に影響を及ぼすアー

カイブノードの動作の詳細も含めて説明します。

- "アーカイブノードの設定と処理"
- "構成のベストプラクティス"
- "アーカイブノードのセットアップを完了します"

アーカイブノードの設定と処理

StorageGRID システムは、オブジェクトが無期限に保存され、常にアクセス可能な場所として、アーカイブノードを管理します。

オブジェクトが取り込まれると、 StorageGRID システムに対して定義されている情報ライフサイクル管理（ ILM ）ルールに基づいて、アーカイブノードを含む必要なすべての場所にコピーが作成されます。アーカイブノードは TSM サーバに対するクライアントとして機能し、 StorageGRID ソフトウェアのインストール時に TSM クライアントライブラリがアーカイブノードにインストールされます。ストレージ用にアーカイブノードに転送されたオブジェクトデータは、 TSM サーバに直接保存されます。TSM サーバへの保存前にアーカイブノードがオブジェクトデータをステージングしたり、オブジェクトを集約したりすることはありません。ただし、データ速度が保証されれば、アーカイブノードから TSM サーバに 1 回のトランザクションで複数のコピーを送信できます。

アーカイブノードから TSM サーバに保存されたオブジェクトデータは、ライフサイクル / 保持ポリシーに従って TSM サーバで管理されます。これらの保持ポリシーは、アーカイブノードの処理に対応するように定義する必要があります。つまり、アーカイブノードによって保存されたオブジェクトデータは、アーカイブノードによって削除されないかぎり、無期限に保存されていつでもアーカイブノードからアクセスできる必要があります。

StorageGRID システムの ILM ルールと TSM サーバのライフサイクル / 保持ポリシーの間に接続は確立されていません。それぞれが互いに独立して動作します。ただし、各オブジェクトが StorageGRID システムに取り込まれる際に、そのオブジェクトに TSM 管理クラスを割り当てることができます。この管理クラスは、オブジェクトデータとともに TSM サーバに渡されます。オブジェクトタイプごとに異なる管理クラスを割り当てると、オブジェクトデータを別々のストレージプールに配置したり、必要に応じて異なる移行ポリシーや保持ポリシーを適用したりするように TSM サーバを設定できます。たとえば、データベースのバックアップとして識別されたオブジェクト（新しいデータで上書き可能な一時的コンテンツ）を、アプリケーションデータ（無期限に保持する必要のある固定コンテンツ）とは別の方法で処理できます。

アーカイブノードは新規または既存の TSM サーバと統合でき、専用の TSM サーバは必要ありません。TSM サーバは、サイズが予想される最大負荷に対応していれば、他のクライアントと共有できます。TSM は、アーカイブノードとは別のサーバまたは仮想マシンにインストールする必要があります。

複数のアーカイブノードから同じ TSM サーバに書き込むように設定できますが、この設定が推奨されるのは、アーカイブノードが異なるデータセットを TSM サーバに書き込む場合のみです。各アーカイブノードが同じオブジェクトデータのコピーをアーカイブに書き込む場合は、複数のアーカイブノードを同じ TSM サーバに書き込む設定は推奨されません。後者のシナリオでは、本来ならばオブジェクトデータの独立した、冗長コピーとなるはずが、両方のコピーが単一点障害（ TSM サーバ）となります。

アーカイブノードは、 TSM の Hierarchical Storage Management （ HSM ；階層型ストレージ管理）コンポーネントは使用しません。

構成のベストプラクティス

TSM サーバをサイジングおよび設定する場合、アーカイブノードとの連携を最適化する

ベストプラクティスがあります。

TSM サーバをサイジングおよび設定する際には、次の点を考慮する必要があります。

- アーカイブノードは TSM サーバに保存する前にオブジェクトを集約しないため、アーカイブノードに書き込まれるすべてのオブジェクトへの参照を格納できるように TSM データベースをサイジングする必要があります。
- アーカイブノードソフトウェアでは、テープまたはその他のリムーバブルメディアにオブジェクトを直接書き込む際のレイテンシが許容されません。したがって TSM サーバには、リムーバブルメディアが使用されるたびにアーカイブノードが最初にデータを保存する初期ストレージ用のディスクストレージプールを設定する必要があります。
- イベントベースの保持を使用するには、 TSM の保持ポリシーを設定する必要があります。アーカイブノードでは、作成ベースの TSM 保持ポリシーはサポートされません。保持ポリシーでは、推奨設定である retmin=0 および retver=0 （アーカイブノードが保持イベントをトリガーしたときに保持が開始され、その後 0 日間保持される）を使用してください。ただし、これらの retmin 値および retver 値はオプションです。

ディスクプールは、テーププールにデータを移行するように設定する必要があります（つまり、テーププールをディスクプールの NXTSTGPOOL に設定します）。テーププールは、両方のプールに同時に書き込むディスクプールのコピープールとしては設定しないでください（つまり、テーププールをディスクプールの COPYSTGPOOL にすることはできません）。アーカイブノードデータを含むテープのオフラインコピーを作成するには、 TSM サーバの 2 つ目のテーププールとして、アーカイブノードのデータ用に使用されるテーププールのコピープールを設定します。

アーカイブノードのセットアップを完了します

インストールプロセスを完了した時点ではアーカイブノードは機能していません。StorageGRID システムが TSM アーカイブノードにオブジェクトを保存できるようにするには、 TSM サーバのインストールと設定を完了し、 TSM サーバと通信するようにアーカイブノードを設定する必要があります。

TSMの読み出しおよび格納セッションを最適化する方法については、アーカイブストレージの管理に関する情報を参照してください。

- "アーカイブノードの管理"

必要に応じて次の IBM のドキュメントを参照し、 StorageGRID システムでアーカイブノードと TSM サーバを統合する準備をしてください。

- "『 IBM Tape Device Drivers Installation and User's Guide 』（ IBM テープデバイスドライバインストールおよびユーザーズガイド）"
- "IBM Tape Device Drivers Programming Reference"

新しい**TSM**サーバをインストールしています

アーカイブノードを新規または既存の TSM サーバと統合できます。新しい TSM サーバをインストールする場合は、 TSM のドキュメントの指示に従ってインストールを完了してください。

アーカイブノードを TSM サーバと同じマシンでホストすることはできません。

TSMサーバの設定

このセクションでは、 TSM のベストプラクティスに従って TSM サーバを準備する手順を記載します。

次の手順では、のプロセスについて説明します。

- TSM サーバ上でディスクストレージプール、およびテープストレージプール（必要な場合）を定義します
- アーカイブノードから保存されたデータ用に TSM 管理クラスを使用するドメインポリシーを定義し、そのドメインポリシーを使用するようにノードを登録します

これらの手順はあくまで参考であり、 TSM のドキュメントに代わるものでも、すべての構成に適した完全な手順がすべて記載されているわけでもありません。環境に固有の手順は、詳細な要件を把握し、 TSM サーバのすべてのドキュメントに精通している TSM 管理者に確認する必要があります。

TSMテープストレージプールとディスクストレージプールを定義する

アーカイブノードはディスクストレージプールに書き込みます。コンテンツをテープにアーカイブするには、コンテンツをテープストレージプールに移動するようにディスクストレージプールを設定する必要があります。

このタスクについて

1 台の TSM サーバに対し、 Tivoli Storage Manager でテープストレージプールとディスクストレージプールを定義する必要があります。ディスクプールを定義したら、ディスクボリュームを作成してディスクプールに割り当てます。TSM サーバでディスクのみのストレージを使用する場合、テーププールは必要ありません。

テープストレージプールを作成する前に、 TSM サーバでいくつかの手順を完了しておく必要があります。（テープライブラリを作成し、テープライブラリにドライブを少なくとも 1 本作成します。サーバからライブラリへのパスとサーバからドライブへのパスを定義し、ドライブのデバイスクラスを定義します）。 これらの手順の詳細は、サイトのハードウェア構成とストレージ要件によって異なります。詳細については、 TSM のドキュメントを参照してください。

以下に、このプロセスの手順を示します。サイトの要件は導入の要件によって異なることに注意してください。設定の詳細および手順については、 TSM のドキュメントを参照してください。

以下のコマンドを実行するには、管理者権限を使用してサーバにログオンし、 dsmadmc ツールを使用する必要があります。

手順

1. テープライブラリを作成します。

   ```
   define library tapelibrary libtype=scsi
   ```

   ここで *tapelibrary* はテープライブラリの任意の名前で、の値です `libtype` テープライブラリのタイプによって異なる場合があります。

2. サーバからテープライブラリへのパスを定義します。

   ```
   define path servername tapelibrary srctype=server desttype=library device=lib-devicename
   ```

   - *servername* はTSMサーバの名前です
   - *tapelibrary* は、定義したテープライブラリの名前です
   - *lib-devicename* は、テープライブラリのデバイス名です

3. ライブラリのドライブを定義します。

   ```
   define drive tapelibrary drivename
   ```

   - *drivename* は、ドライブに指定する名前です
   - *tapelibrary* は、定義したテープライブラリの名前です

     ハードウェア構成によっては、追加のドライブを設定することが必要になる場合があります。（たとえば、 1 つのテープライブラリからの入力が 2 つあるファイバチャネルスイッチに TSM サーバが接続されている場合は、入力ごとにドライブを定義します）。

4. サーバから定義したドライブへのパスを定義します。

   ```
   define path servername drivename srctype=server desttype=drive library=tapelibrary device=drive-dname
   ```

   - *drive-dname* は、ドライブのデバイス名です
   - *tapelibrary* は、定義したテープライブラリの名前です

     テープライブラリ用に定義したドライブごとに、別のを使用してこの手順を繰り返します *drivename* および *drive-dname* をクリックします。

5. ドライブのデバイスクラスを定義します。

   ```
   define devclass DeviceClassName devtype=lto library=tapelibrary format=tapetype
   ```

   - *DeviceClassName* は、デバイスクラスの名前です
   - *lto* は、サーバに接続されているドライブのタイプです
   - *tapelibrary* は、定義したテープライブラリの名前です
   - *tapetype* は、テープのタイプです。たとえば、ultrium3です

6. ライブラリのインベントリにテープボリュームを追加します。

   ```
   checkin libvolume tapelibrary
   ```

   tapelibrary は、定義したテープライブラリの名前です。

7. プライマリテープストレージプールを作成します。

```
define stgpool SGWSTapePool DeviceClassName description=description
collocate=filespace maxscratch=XX
```

- *SGWSTapePool* はアーカイブノードのテープストレージプールの名前です。テープストレージプールには（ TSM サーバが想定する命名規則に沿ってさえいれば）任意の名前を選択できます。
- *DeviceClassName* は、テープライブラリのデバイスクラス名です。
- *description* はストレージプールの概要 で、を使用してTSMサーバに表示できます `query stgpool` コマンドを実行しますたとえば ' アーカイブ・ノード用のテープ・ストレージ・プールなどです
- *collocate=filespace* は、TSMサーバが同じファイルスペースのオブジェクトを1つのテープに書き込む必要があることを指定します。
- XX は次のいずれかです。
  - テープライブラリ内の空のテープの数（アーカイブノードだけがライブラリを使用している場合）。
  - StorageGRID システム用に割り当てられているテープの数（テープライブラリが共有されている場合）。

8. TSM サーバで、ディスクストレージプールを作成します。TSM サーバの管理コンソールで、と入力します

```
define stgpool SGWSDiskPool disk description=description
maxsize=maximum_file_size nextstgpool=SGWSTapePool highmig=percent_high
lowmig=percent_low
```

- *SGWSDiskPool* はアーカイブノードのディスクプールの名前です。ディスクストレージプールには（ TSM が想定する命名規則に沿ってさえいれば）任意の名前を選択できます。
- *description* はストレージプールの概要 で、を使用してTSMサーバに表示できます `query stgpool` コマンドを実行しますたとえば ' アーカイブ・ノード用のディスク・ストレージ・プールなどです
- *maximum_file_size* ディスクプールにキャッシュされるのではなく、このサイズよりも大きいオブジェクトをテープに直接書き込みます。を設定することを推奨します *maximum_file_size* を10 GBに設定します。
- *nextstgpool=SGWSTapePool* は、ディスクストレージプールをアーカイブノード用に定義したテープストレージプールと関連付けます。
- *percent_high* ディスクプールの内容のテーププールへの移行を開始する値を設定します。を設定することを推奨します *percent_high* を0に設定すると、データがすぐに移行されます
- *percent_low* テープ・プールへの移行を停止する値を設定します。を設定することを推奨します *percent_low* を0に設定して、ディスクプールをクリアします。

9. TSM サーバで、 1 つ以上のディスクボリュームを作成してディスクプールに割り当てます。

```
define volume SGWSDiskPool volume_name formatsize=size
```

- *SGWSDiskPool* はディスクプール名です。
- *volume_name* はボリュームの完全パスです（例： `/var/local/arc/stage6.dsm`）をテープに転送する準備として、TSMサーバ上でディスクプールの内容を書き込みます。
- *size* は、ディスクボリュームのサイズ（MB単位）です。

たとえば、テープボリュームの容量が 200GB の場合、ディスクプールのコンテンツで 1 つのテープを使い切るようなディスクボリュームを 1 個作成するには、 size の値を 200000 に設定します。

ただし、 TSM サーバがディスクプール内の各ボリュームに書き込むことができるため、小さいサイズのディスクボリュームを複数作成する方がよい場合もあります。たとえばテープサイズが 250GB の場合、 10GB （ 10000 ）のディスクボリュームを 25 個作成します。

TSM サーバは、ディスクボリューム用にディレクトリ内のスペースを事前に割り当てます。この処理には、完了までに時間がかかることがあります（ 200GB のディスクボリュームの場合は 3 時間以上）。

ドメインポリシーの定義とノードの登録

アーカイブノードから保存されたデータ用に TSM 管理クラスを使用するドメインポリシーを定義し、そのドメインポリシーを使用するようにノードを登録する必要があります。

Tivoli Storage Manager （ TSM ）でアーカイブノードのクライアントパスワードの期限が切れると、アーカイブノードのプロセスでメモリリークが発生する可能性があります。アーカイブノードのクライアントユーザ名 / パスワードの期限が切れないように TSM サーバを設定してください。

アーカイブノードとして使用するノードを TSM サーバに登録する（または既存のノードを更新する）場合は、そのノードが書き込み処理に使用できるマウントポイントの数を指定する必要があります。そのためには、 REGISTER NODE コマンドで MAXNUMMP パラメータを指定します。通常、マウントポイントの数は、アーカイブノードに割り当てられているテープドライブのヘッド数と同じです。TSM サーバの MAXNUMMP に指定する数は、アーカイブノードの *ARC * > * Target * > * Configuration * > * Main * > * Maximum Store Sessions * に設定された値以上である必要があります 同時ストアセッション数はアーカイブノードでサポートされないため、値は 0 または 1 に設定されます。

TSM サーバ用に設定した MAXSESSIONS の値によって、すべてのクライアントアプリケーションが TSM サーバに対して開くことのできる最大セッション数が制御されます。TSM で指定する MAXSESSIONS の値は、アーカイブノードの Grid Manager で * ARC * > * Target * > * Configuration * > * Main * > * Sessions * に指定されている値以上である必要があります。アーカイブノードは、最大でマウントポイントごとに 1 つのセッションと少数（ 5 つ未満）の追加セッションを同時に作成します。

アーカイブノードに割り当てられているTSMノードは、カスタムドメインポリシーを使用します `tsm-domain`。。 `tsm-domain` ドメイン・ポリシーは'標準ドメイン・ポリシーの変更バージョンであり'テープに書き込むように構成され'アーカイブ先がStorageGRID システムのストレージ・プールに設定されています（*`SGWSDiskPool`*）。

ドメインポリシーを作成およびアクティブ化するには、管理者権限を使用して TSM サーバにログインし、 dsmadmc ツールを使用する必要があります。

ドメインポリシーを作成してアクティブ化します

アーカイブノードから送信されたデータを保存するように TSM サーバを設定するには、ドメインポリシーを作成してアクティブ化する必要があります。

手順

1. ドメインポリシーを作成します。

```
copy domain standard tsm-domain
```

2. 既存の管理クラスを使用しない場合は、次のいずれかを入力します。

```
define policyset tsm-domain standard

define mgmtclass tsm-domain standard default
```

default は、導入用のデフォルトの管理クラスです。

3. 適切なストレージプールにコピーグループを作成します。（ 1 行に）次のように入力します。

```
define copygroup tsm-domain standard default type=archive
destination=SGWSDiskPool retinit=event retmin=0 retver=0
```

default は、アーカイブノードのデフォルトの管理クラスです。の値 `retinit`、 `retmin`および `retver` アーカイブノードで現在使用されている保持動作を反映するように選択されています

> 設定しないでください `retinit` 終了： `retinit=create`。設定 `retinit=create` 保持イベントを使用してTSMサーバからコンテンツが削除されるため、アーカイブノードからコンテンツが削除されないようにします。

4. 管理クラスをデフォルトに割り当てます。

```
assign defmgmtclass tsm-domain standard default
```

5. 新しいポリシーセットをアクティブに設定します。

```
activate policyset tsm-domain standard
```

activate コマンドを入力したときに表示される「 no backup copy group 」警告は無視してください。

6. 新しいポリシーセットを使用するノードを TSM サーバに登録します。TSM サーバで、次のように（ 1 行に）入力します。

```
register node arc-user arc-password passexp=0 domain=tsm-domain
MAXNUMMP=number-of-sessions
```

aarc-user と arc-password は、アーカイブノードで定義したクライアントノード名とパスワードです。また、 MAXNUMMP の値は、アーカイブノードの格納セッション用に予約されているテープドライブの数に設定されます。

> デフォルトでは、ノードを登録すると、管理ユーザ ID がクライアント所有者の権限で作成され、パスワードが定義されます。

StorageGRID へのデータの移行

日常業務に StorageGRID システムを使用しながら、同時に StorageGRID システムに大量のデータを移行できます。

次のセクションでは、 StorageGRID システムへの大量のデータ移行について、その概要と計画方法を説明します。データ移行の一般的なガイドではなく、移行を実行するための詳細な手順も記載されていません。このセクションのガイドラインと手順に従って、日常業務を中断せずに StorageGRID システムにデータを効率的に移行し、移行したデータが StorageGRID システムによって適切に処理されるようにしてください。

- "StorageGRID システムの容量の確認"
- "移行データのILMポリシーの決定"
- "移行が処理に及ぼす影響"
- "データ移行のスケジュール設定"
- "データ移行の監視"
- "移行アラーム用のカスタム通知の作成"

StorageGRID システムの容量の確認

StorageGRID システムに大量のデータを移行する前に、予想されるボリュームを処理できるディスク容量が StorageGRID システムにあることを確認します。

StorageGRID システムにアーカイブノードが含まれていて、移行するオブジェクトのコピーをニアラインストレージ（テープなど）に保存する場合は、アーカイブノードのストレージに予想される移行量に対応する十分な容量があることを確認します。

容量評価の一環として、移行を計画しているオブジェクトのデータプロファイルを確認し、必要なディスク容量を計算します。StorageGRID システムのディスク容量の監視に関する詳細については、StorageGRID の監視とトラブルシューティングの手順を参照してください。

関連情報

"トラブルシューティングを監視します"

"ストレージノードの管理"

移行データの**ILM**ポリシーの決定

StorageGRID システムの ILM ポリシーは、作成されるコピーの数とその格納先、および保持期間を決定します。ILM ポリシーは、オブジェクトをフィルタリングする方法、および一定の期間にわたってオブジェクトデータを管理する方法を記述した一連の ILM ルールで構成されます。

移行データの使用方法およびその要件によっては、日常業務に使用する ILM ルールとは別の、移行データに固有の ILM ルールを定義することができます。たとえば、日常的なデータ管理と移行対象のデータに異なる規制要件が適用される場合、異なるグレードのストレージに異なる数の移行データのコピーが必要となる可能性があります。

移行データと日常業務で保存されるオブジェクトデータを一意に区別できる場合は、移行データにのみ適用されるルールを設定できます。

いずれかのメタデータ条件を使用してデータのタイプを確実に識別できる場合は、この条件を使用して移行データにのみ適用される ILM ルールを定義できます。

データ移行を開始する前に、 StorageGRID システムの ILM ポリシーとそのポリシーが移行データにどのよう

に適用されるかを確認し、 ILM ポリシーへの変更があればテストしておく必要があります。

> ILM ポリシーが正しく指定されていないと、原因 によるリカバリ不能なデータ損失が発生する可能性があります。ポリシーを想定どおりに機能させるには、 ILM ポリシーをアクティブ化する前に、 ILM ポリシーに加えたすべての変更をよく確認してください。

関連情報

"ILM を使用してオブジェクトを管理する"

移行が処理に及ぼす影響

StorageGRID システムは、オブジェクトを効率的に格納して読み出せるようにすること、およびオブジェクトデータとメタデータの冗長コピーをシームレスに作成することでデータ損失に対する優れた保護を提供することを目的に設計されています。

ただし、日常的なシステム運用に影響が及ばないように、または極端なケースでは StorageGRID システムに障害が発生してデータが失われないように、この章の手順に従ってデータ移行を慎重に管理する必要があります。

大量のデータを移行すると、システムに新たな負荷がかかります。StorageGRID システムの負荷が高い場合は、オブジェクトの格納および読み出し要求への応答が遅くなります。その結果、日常業務に不可欠な格納および読み出し要求が影響を受ける可能性があります。移行は、原因 のその他の運用上の問題にもなります。たとえば、ストレージノードの容量が上限に近づい原因 ている場合は、一括取り込みによって断続的に大きな負荷がかかると、ストレージノードが読み取り専用と読み書き可能の間で何度も切り替わり、そのたびに通知が生成されます。

負荷の高い状態が続く場合、オブジェクトデータとメタデータの完全な冗長性を確保するために StorageGRID システムが実行する必要のあるさまざまな処理がキューに溜まっていきます。

移行中に StorageGRID システムを安全かつ効率的に運用するためには、本書のガイドラインに従ってデータ移行を慎重に管理する必要があります。データの移行にあたっては、オブジェクトを複数のバッチで取り込むか、または取り込み量を常に調整します。そのうえで、 StorageGRID システムを常時監視し、さまざまな属性値が超えようにします。

データ移行のスケジュール設定

主要な業務時間中はデータを移行しないでください。データの移行は、夕方や週末など、システムの使用率が低い時間帯にのみ実施してください。

アクティビティが高い期間には、できるだけデータ移行をスケジュールしないでください。ただし、アクティビティレベルが高い期間を完全に回避することが現実的でない場合はそのまま進めてかまいません。その場合は、関連する属性を注意深く監視し、許容値を超えた場合に対処する必要があります。

関連情報

"データ移行の監視"

データ移行の監視

所定の期間内にILMポリシーに従ってデータが配置されるよう、必要に応じてデータ移行を監視し、調整する必要があります。

次の表に、データ移行中に監視する必要がある属性とその内容を示します。

取り込み速度を抑制するためにレート制限を指定したトラフィック分類ポリシーを使用する場合は、次の表に示す統計情報とともに、観察されたレートを監視し、必要に応じて制限を減らすことができます。

モニタ	説明
ILM による評価を待機しているオブジェクトの数	1. Support **>** Tools **>** Grid Topology *を選択します。 2. [***deployment***概要***Main***]を選択します。 3. ILM アクティビティセクションで、次の属性について表示されるオブジェクトの数を監視します。 ◦ * Awaiting - All （ XQUZ ） * ： ILM による評価を待機しているオブジェクトの合計数です。 ◦ * Awaiting - Client （ XCQZ ） * ：クライアント処理（取り込みなど）から ILM による評価を待機しているオブジェクトの合計数です。 4. これらの属性のどちらかに対して表示されるオブジェクトの数が 100 、 000 を超えた場合は、オブジェクトの取り込み速度を調整して、 StorageGRID システムへの負荷を軽減してください。
ターゲットアーカイブシステムのストレージ容量	ILM ポリシーによって、移行対象データのコピーがターゲットアーカイブストレージシステム（テープまたはクラウド）に保存される場合は、ターゲットアーカイブストレージシステムの容量を監視して、移行対象データ用の十分な容量が確保されていることを確認してください。
アーカイブノード ARC * Store *	「 Store Failures （ ARVF ） * 」属性のアラームがトリガーされた場合、対象のアーカイブストレージシステムの容量が上限に達している可能性があります。ターゲットアーカイブストレージシステムをチェックして、アラームをトリガーした問題を解決してください。

移行アラーム用のカスタム通知の作成

StorageGRID では、特定の値が推奨されるしきい値を超えた場合に移行を監視するシステム管理者にアラート通知またはアラーム（従来のシステム）通知を送信することができます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。
- アラート（またはアラーム）通知のEメールを設定しておく必要があります。

手順

1. データ移行中に監視するPrometheusの指標またはStorageGRID 属性ごとに、カスタムのアラートルールまたはグローバルカスタムアラームを作成します。

   アラートはPrometheusの指標値に基づいてトリガーされます。属性値に基づいてアラームがトリガーさ

れます。詳細については、StorageGRID の監視とトラブルシューティングの手順を参照してください。

2. データ移行が完了したら、カスタムのアラートルールまたはグローバルカスタムアラームを無効にします。

   グローバルカスタムアラームはデフォルトアラームを上書きします。

関連情報

"トラブルシューティングを監視します"

ILM を使用してオブジェクトを管理する

情報ライフサイクルルールとポリシーを使用してオブジェクトを管理する方法、およびS3オブジェクトロックを使用してオブジェクト保持に関する規制に準拠する方法について説明します。

- "情報ライフサイクル管理によるオブジェクトの管理"
- "S3オブジェクトロックでオブジェクトを管理する"
- "ILM ルールとポリシーの例"

情報ライフサイクル管理によるオブジェクトの管理

StorageGRID システムのオブジェクトを管理するには、情報ライフサイクル管理（ ILM ）ルールとポリシーを設定します。ILM ルールとポリシーは、オブジェクトデータのコピーを作成して分散し、一定の期間にわたって管理する方法を StorageGRID に指示します。

ILM ルールと ILM ポリシーを設計して実装するには、慎重な計画が必要です。運用要件、 StorageGRID システムのトポロジ、オブジェクト保護のニーズ、使用可能なストレージタイプについて理解しておく必要があります。次に、さまざまなタイプのオブジェクトをどのようにコピー、分散、および格納するかを決定する必要があります。

- "オブジェクトのライフサイクル全体にわたる ILM の動作"
- "ILM ポリシーとは"
- "ILM ルールとは"
- "ストレージグレード、ストレージプール、ECプロファイル、リージョンを作成する"
- "ILMルールを作成する"
- "ILMポリシーを作成する"
- "ILMルールおよびILMポリシーの操作"

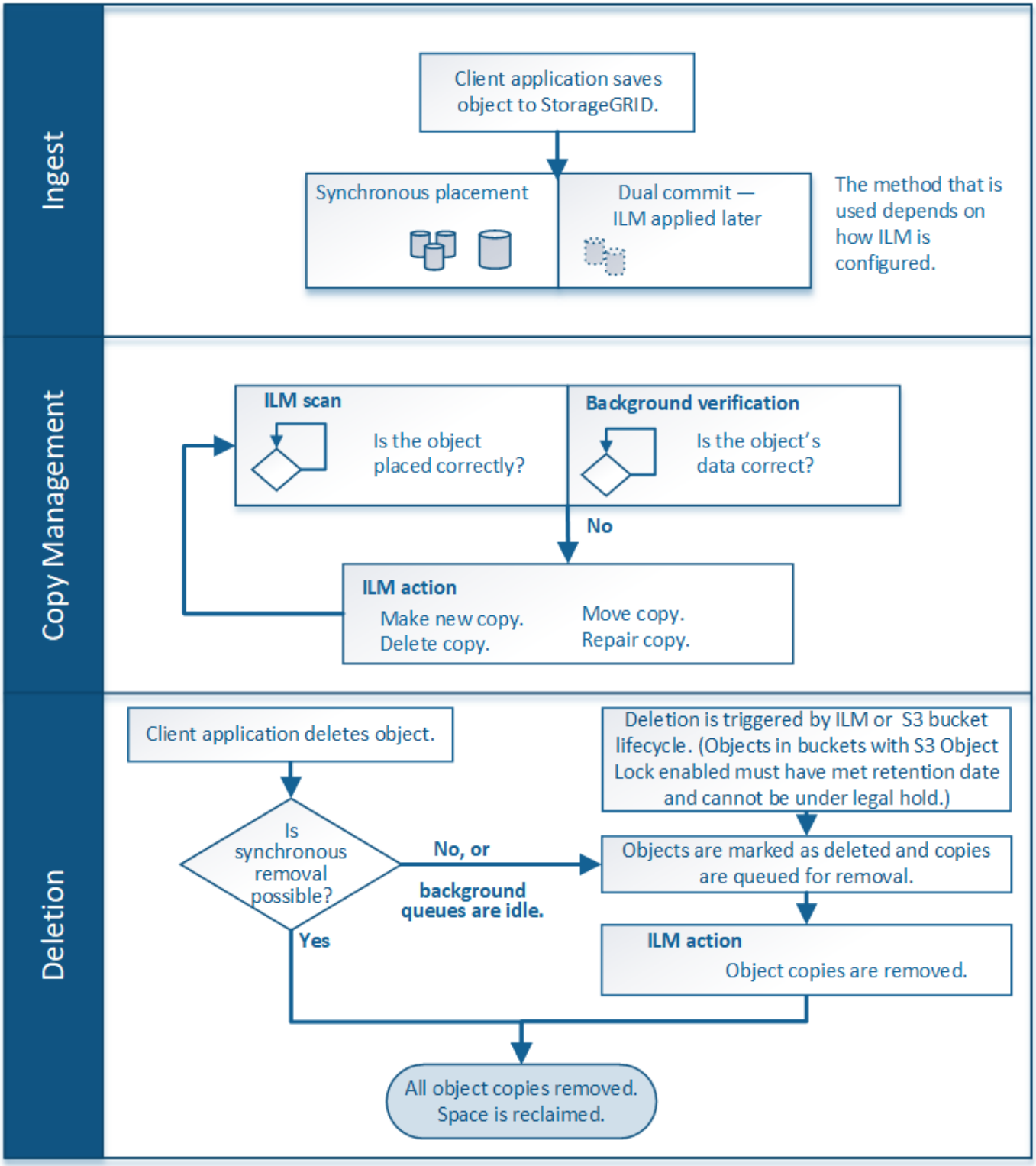
オブジェクトのライフサイクル全体にわたる **ILM** の動作

StorageGRID での ILM を使用したオブジェクト管理方法を理解することは、ポリシーをより効果的に設計するうえで役立ちます。

- * 取り込み： S3 または Swift クライアントアプリケーションが StorageGRID システムへの接続を確立してオブジェクトを保存すると取り込みが開始され、 StorageGRID がクライアントに「 ingest successful 」メッセージを返すと取り込みが完了します。ILM 要件の指定方法に応じて、 ILM の手順を即座に適用（同期配置）するか、中間コピーを作成して ILM をあとから適用（デュアルコミット）することで、オブジェクトデータは取り込み時に保護されます。
- * コピー管理 * ： ILM の配置手順に指定された数とタイプのオブジェクトコピーを作成すると、 StorageGRID はオブジェクトの場所を管理し、オブジェクトを損失から保護します。
  - ILM のスキャンと評価： StorageGRID は、グリッドに格納されているオブジェクトのリストを継続的にスキャンし、現在のコピーが ILM 要件を満たしているかどうかを確認します。タイプ、数、または場所が異なるオブジェクトコピーが必要となった場合、 StorageGRID は必要に応じてコピーを作成、削除、または移動します。
  - バックグラウンド検証： StorageGRID は、バックグラウンド検証を継続的に実行して、オブジェクトデータの整合性をチェックします。問題が検出されると、 StorageGRID は、現在の ILM 要件を満たす場所に、新しいオブジェクトコピーまたは置き換え用のイレイジャーコーディングオブジェクトフラグメントを自動的に作成します。StorageGRID の監視とトラブルシューティングの手順を参照してください。
- * オブジェクトの削除 * ： StorageGRID システムからすべてのコピーが削除されると、オブジェクトの管理は終了します。オブジェクトは、クライアントによる削除要求、または S3 バケットライフサイクルの終了が原因の ILM による削除または削除が原因で削除されます。

> S3 オブジェクトロックが有効になっているバケット内のオブジェクトがリーガルホールドの対象である場合、または retain-until date が指定されていても未達成の場合、オブジェクトを削除することはできません。

次の図は、オブジェクトのライフサイクル全体にわたる ILM の動作をまとめたものです。



関連情報

"トラブルシューティングを監視します"

オブジェクトの取り込み方法

StorageGRID は、オブジェクトに一致するILMルールの指定に従って、同期配置またはデュアルコミットを実行し、取り込み時にオブジェクトを保護します。

S3またはSwiftクライアントがオブジェクトをグリッドに格納すると、次のどちらかの方法でStorageGRIDにオブジェクトが取り込まれます。

- 同期配置：StorageGRID は、ILM要件を満たすために必要なすべてのオブジェクトコピーをただちに作成します。すべてのコピーが作成されると、StorageGRID は「ingest successful」メッセージをクライアントに送信します。

  StorageGRID は、すべてのオブジェクトコピーをただちに作成できない場合（必要な場所が一時的に使用できない場合など）、クライアントに「ingest failed」というメッセージを送信します。または、ILMルールの作成時に選択した内容に応じて、中間オブジェクトコピーの作成とILMの評価を実行します。

- デュアル・コミット：StorageGRID は'それぞれ異なるストレージ・ノード上に'オブジェクトの中間コピーを2つ作成し'クライアントにingest successfulメッセージを送信します次に、StorageGRID はオブジェクトをILM評価のキューに登録します。

  StorageGRID によるILM評価では、中間コピーがILMルールの配置手順を満たしているかどうかが最初にチェックされます。たとえば、2つの中間コピーが2コピーのILMルールの手順を満たしていても、イレイジャーコーディングルールの手順を満たしていない場合があります。中間コピーがILMの手順を満たしていない場合、StorageGRID は新しいオブジェクトコピーを作成し、不要な中間コピーをすべて削除します。

  StorageGRID が中間コピーを2つ作成できない場合（ネットワーク問題 が2つ目のコピーを作成できない場合など）、StorageGRID は再試行しません。取り込みは失敗します。

> S3 / Swiftクライアントでは、を指定することで、StorageGRID が取り込み時に1つの中間コピーを作成するように指定できます `REDUCED_REDUNDANCY` ストレージクラス。詳細については、S3 / Swiftクライアントを実装する手順を参照してください。

デフォルトでは、StorageGRID は同期配置を使用して取り込み時にオブジェクトを保護します。

関連情報

"取り込みのデータ保護オプション"

"S3 を使用する"

"Swift を使用します"

取り込みのデータ保護オプション

ILM ルールを作成する際には、取り込み時にオブジェクトを保護するためのオプションとして、 Dual commit 、 Balanced 、または Strict のいずれかを指定します。選択したオプションに応じて、 StorageGRID は、中間コピーを作成してオブジェクトをキューに登録し、あとで ILM 評価を実行するか、または同期配置を使用してコピーをただちに作成して ILM 要件を満たします。

デュアルコミット

Dual commit オプションを選択すると、 StorageGRID は 2 つの異なるストレージノード上に中間オブジェクトコピーをただちに作成し、「 ingest successful 」メッセージをクライアントに返します。オブジェクトは ILM 評価のキューに登録され、ルールの配置手順を満たすコピーはあとで作成されます。

Dual commit オプションを使用する状況

次のいずれかの場合に Dual commit オプションを使用します。

- マルチサイトの ILM ルールを使用しており、クライアントの取り込みレイテンシを考慮する必要があります。Dual commit を使用する場合は、 ILM を満たしていないデュアルコミットコピーの作成と削除の作業をグリッドで確実に実行できるようにする必要があります。具体的には、
  - ILM のバックログが発生しないように、グリッドの負荷が十分に低い必要があります。
  - グリッドにハードウェアリソース（ IOPS 、 CPU 、メモリ、ネットワーク帯域幅など）が余剰である。
- マルチサイトの ILM ルールを使用していて、通常はサイト間の WAN 接続のレイテンシが高くなっているか、帯域幅が制限されている。このシナリオでは、 Dual commit オプションを使用するとクライアントのタイムアウトを回避できます。Dual commit オプションを選択する前に、現実的なワークロードでクライアントアプリケーションをテストする必要があります。

strict

Strict オプションを選択すると、 StorageGRID は取り込み時に同期配置を使用してルールの配置手順で指定されたすべてのオブジェクトコピーをただちに作成します。必要なストレージの場所が一時的に使用できないなどの理由で、 StorageGRID がすべてのコピーを作成できない場合は、取り込みが失敗します。クライアントは処理を再試行する必要があります。

Strict オプションを使用する場合

Strict オプションは、 ILM ルールに指定された場所にのみオブジェクトをただちに格納するための運用または規制上の要件がある場合に使用してください。たとえば、規制要件を満たすために、 Strict オプションと Location Constraint 高度なフィルタを使用して、オブジェクトが特定のデータセンターに格納されないようにする必要があります。

"例 5 ：取り込み動作が Strict の場合の ILM ルールとポリシー"

中間（ Balanced ）

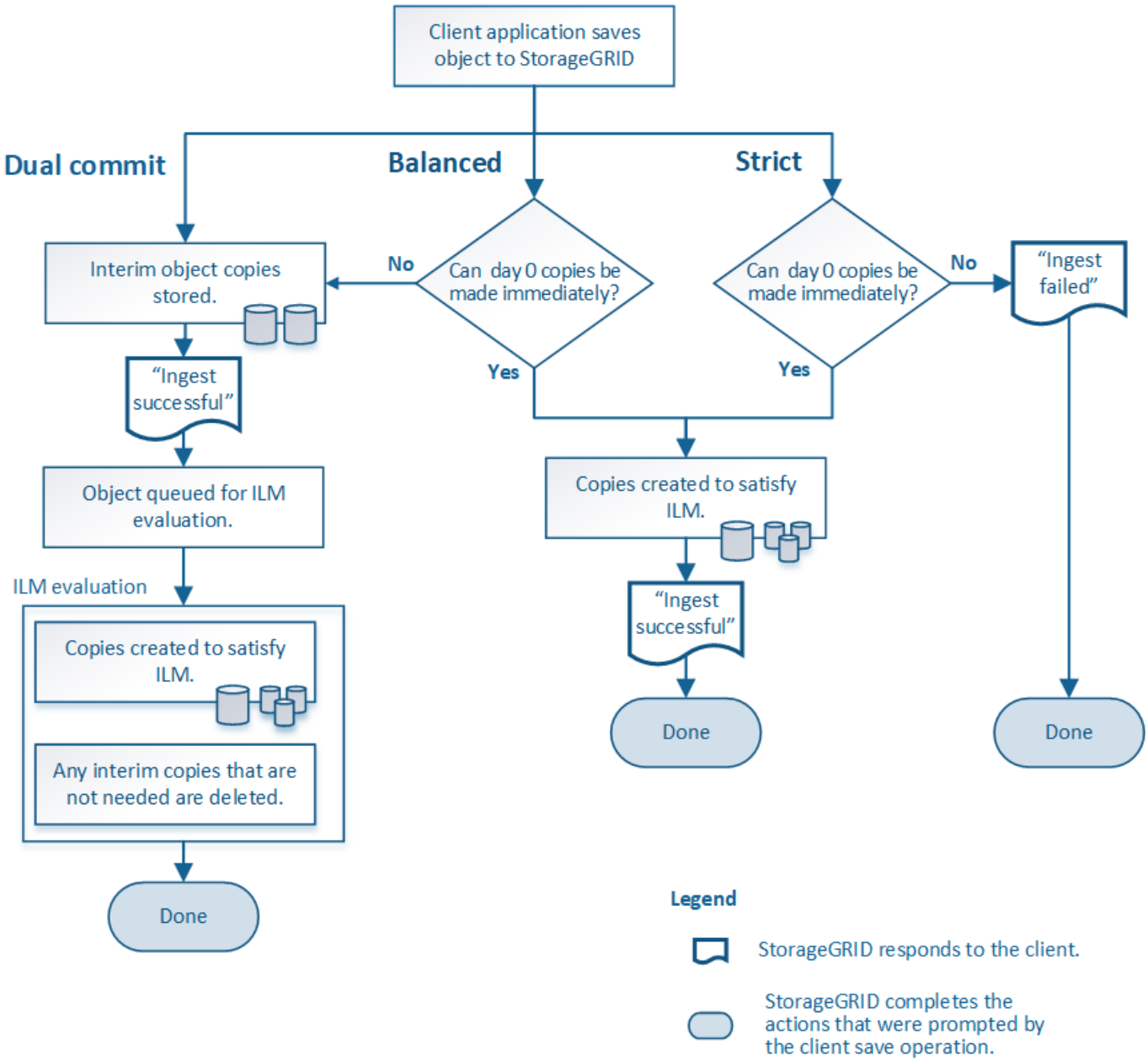
Balanced オプションを選択した場合も、 StorageGRID は、取り込み時に同期配置を使用してルールの配置手順で指定されたすべてのコピーをただちに作成します。Strict オプションと違い、 StorageGRID がすべてのコピーをただちに作成できない場合は、代わりに Dual commit を使用します。

Balanced オプションを使用する状況

Balanced オプションは、データ保護、グリッドパフォーマンス、および取り込みの成功の最適な組み合わせを実現するために使用します。Balanced は、 ILM ルールウィザードのデフォルトオプションです。

3 つの取り込みオプションのフローチャート

フローチャートは、次のいずれかの取り込みオプションを使用するILMルールにオブジェクトが一致した場合の動作を示しています。



関連情報

"オブジェクトの取り込み方法"

データ保護オプションのメリット、デメリット、および制限事項

取り込み時にデータを保護するための 3 つのオプション（ Balanced 、 Strict 、 Dual commit ）のそれぞれのメリットとデメリットを理解することは、 ILM ルールに選択するオプションを決定する際に役立ちます。

Balanced オプションと **Strict** オプションのメリット

取り込み時に中間コピーを作成する Dual commit と比較すると、 2 つの同期配置オプションには次のメリットがあります。

- * Better データ セキュリティ * ：オブジェクトデータは、 ILM ルールの配置手順に従ってただちに保護さ

れます。配置手順は、複数の格納場所の障害など、さまざまな障害状況からオブジェクトを保護するように設定できます。Dual commit で保護できるのは、単一のローカルコピーの損失のみです。

- * グリッド処理の効率化 * ：各オブジェクトは、取り込み時に 1 回だけ処理されます。StorageGRID システムで中間コピーを追跡または削除する必要がないため、処理の負荷が軽減され、消費されるデータベーススペースも少なくてすみます。
- * （ Balanced ） Recommended * ： Balanced オプションは、最適な ILM 効率を実現します。Strict 取り込み動作が必要であるか、グリッドが Dual commit に使用するためのすべての条件を満たしていないかぎり、 Balanced オプションを使用することを推奨します。
- * （ Strict ）オブジェクトの場所が明らか * ： Strict オプションは、 ILM ルールの配置手順に従ってオブジェクトがただちに格納されることを保証します。

Balanced オプションと **Strict** オプションのデメリット

Dual commit と比較すると、 Balanced オプションと Strict オプションにはいくつかのデメリットがあります。

- * クライアントの取り込み時間が長くなる * ：クライアントの取り込みレイテンシが長くなる可能性があります。Balanced オプションと Strict オプションを使用する場合、すべてのイレイジャーコーディングフラグメントまたはレプリケートコピーが作成されて格納されるまで、「 ingest successful 」メッセージはクライアントに返されません。しかし、ほとんどの場合、オブジェクトデータは最終的な配置までの時間をはるかに短縮できます。
- * （ Strict ）取り込みエラーの増加 * ： Strict オプションでは、 StorageGRID が ILM ルールに指定されたすべてのコピーをただちに作成できないと取り込みが失敗します。必要なストレージの場所が一時的にオフラインになっている場合や、ネットワークでサイト間のオブジェクトコピーが原因 で遅延している場合には、取り込みに失敗する可能性が高くなります。
- * （ Strict ） S3 マルチパートアップロードでは、状況によっては想定どおりに配置されない可能性がある * ： Strict では、オブジェクトが ILM ルールの指定どおりに配置されるか、あるいは取り込みが失敗するかのどちらかの結果が想定されます。ところが、 S3 マルチパートアップロードの場合、オブジェクトの各パートの取り込み時に ILM が評価され、マルチパートアップロードが完了した時点でオブジェクト全体に対して ILM が評価されます。そのため、次の状況では想定どおりに配置されないことがあります。
  - * S3 マルチパートアップロードの実行中に ILM が変更された場合 * ：各パートはその取り込み時にアクティブなルールに従って配置されるため、マルチパートアップロードが完了した時点でオブジェクトの一部のパートが現在の ILM 要件を満たしていない可能性があります。この場合、オブジェクトの取り込みは失敗しません。代わりに、正しく配置されていないパートは ILM ルールによる再評価の対象としてキューに登録され、あとで正しい場所に移動されます。
  - * ILM ルールがサイズでフィルタリングする場合 * ：パーツに対して ILM を評価する際、 StorageGRID はオブジェクトのサイズではなくパーツのサイズでフィルタリングします。つまり、オブジェクト全体としては ILM 要件を満たしていない場所にオブジェクトのパーツが格納される可能性があります。たとえば、 10GB 以上のオブジェクトをすべて DC1 に格納し、それより小さいオブジェクトをすべて DC2 に格納するルールの場合、 10 パートからなるマルチパートアップロードの 1GB の各パートは取り込み時に DC2 に格納されます。オブジェクトに対して ILM が評価されると、オブジェクトのすべてのパートが DC1 に移動されます。
- * （ Strict ）オブジェクトタグまたはメタデータが更新され、新たに必要となった配置を実行できなくても取り込みが失敗しない * ： Strict では、オブジェクトが ILM ルールの指定どおりに配置されるか、あるいは取り込みが失敗するかのどちらかの結果が想定されます。ただし、グリッドにすでに格納されているオブジェクトのメタデータまたはタグを更新しても、オブジェクトは再取り込みされません。そのため、更新によってトリガーされるオブジェクト配置の変更は、すぐには実行されず、通常のバックグラウンド ILM プロセスで ILM が再評価されると、配置変更が行われます。必要な配置変更を行えない場合（新たに必要となった場所が使用できない場合など）は、更新されたオブジェクトは配置変更が可能になるまで現在の場所に残ります。

Balanced オプションと **Strict** オプションを使用したオブジェクトの配置に関する制限事項

次のいずれかの配置手順を含む ILM ルールには、 Balanced オプションまたは Strict オプションを使用できません。

- クラウドストレージプールへの配置： 0 日目
- アーカイブノードへの配置： 0 日目
- ルールの参照時間としてユーザ定義の作成時間が設定されている場合のクラウドストレージプールまたはアーカイブノードでの配置

StorageGRID ではクラウドストレージプールまたはアーカイブノードにコピーを同期的に作成できず、ユーザ定義の作成時間が現在の状態に解決される場合があるため、このような制限があります。

ILM ルールと整合性制御がデータ保護に与える影響

ILM ルールと選択した整合性制御は、どちらもオブジェクトの保護方法に影響します。これらの設定は対話的に操作できます。

たとえば、 ILM ルールに対して選択した取り込み動作はオブジェクトコピーの初期配置に影響し、オブジェクトの格納時に使用される整合性制御はオブジェクトメタデータの初期配置に影響します。StorageGRID では、クライアント要求に対応するためにオブジェクトのメタデータとそのデータの両方にアクセスする必要があるため、整合性レベルと取り込み動作に一致する保護レベルを選択することで、より適切な初期データ保護と予測可能なシステム応答を実現できます。

StorageGRID で使用できる整合性制御の概要を以下に示します。

- * all * ：すべてのノードが即座にオブジェクトメタデータを受け取り、受け取れない場合は要求が失敗します。
- * strong-global * ：オブジェクトのメタデータがすべてのサイトにただちに分散されます。すべてのサイトのすべてのクライアント要求について、リードアフターライト整合性が保証されます。
- * strong-site * ：オブジェクトのメタデータがただちにサイトの他のノードに分散されます。1 つのサイト内のすべてのクライアント要求について、リードアフターライト整合性が保証されます。
- * read-after-new-write * ：新規オブジェクトについてはリードアフターライト整合性が提供され、オブジェクトの更新については結果整合性が提供されます。高可用性が確保され、データ保護が保証されます。
- * available * （ HEAD オペレーションについては結果整合性）：「 read-after-new-write 」整合性レベルと動作は同じですが、 HEAD オペレーションについては結果整合性のみを提供します。

> 整合性レベルを選択する前に、S3またはSwiftクライアントアプリケーションの作成手順の設定の完全な概要 を確認してください。デフォルト値を変更する前に、利点と制限事項を理解しておく必要があります。

整合性制御と **ILM** ルールの連動の例

次の ILM ルールと次の整合性レベル設定の 2 サイトグリッドがあるとします。

- * ILM ルール * ：ローカルサイトとリモートサイトに 1 つずつ、 2 つのオブジェクトコピーを作成します。Strict 取り込み動作が選択されています。
- * 整合性レベル *:"Strong-GLOBAL" (オブジェクトメタデータはすべてのサイトにただちに分散されます)

クライアントがオブジェクトをグリッドに格納すると、 StorageGRID は両方のオブジェクトをコピーし、両方のサイトにメタデータを分散してからクライアントに成功を返します。

オブジェクトは、取り込みが成功したことを示すメッセージが表示された時点で損失から完全に保護されます。たとえば、取り込み直後にローカルサイトが失われた場合、オブジェクトデータとオブジェクトメタデータの両方のコピーがリモートサイトに残っています。オブジェクトを完全に読み出し可能にしている。

代わりに同じ ILM ルールと「 strong-site 」整合性レベルを使用する場合は、オブジェクトデータがリモートサイトにレプリケートされたあとで、オブジェクトメタデータがそこに分散される前に、クライアントに成功メッセージが送信される可能性があります。この場合、オブジェクトメタデータの保護レベルがオブジェクトデータの保護レベルと一致しません。取り込み直後にローカルサイトが失われると、オブジェクトメタデータが失われます。オブジェクトを読み出すことができません。

整合性レベルと ILM ルールの間の関係は複雑になる可能性があります。サポートが必要な場合は、ネットアップにお問い合わせください。

関連情報

"レプリケーションとは"

"イレイジャーコーディングとは"

"イレイジャーコーディングスキームとは"

"例 5 ：取り込み動作が Strict の場合の ILM ルールとポリシー"

"S3 を使用する"

"Swift を使用します"

オブジェクトの格納方法（レプリケーションまたはイレイジャーコーディング）

StorageGRID では、レプリケートコピーを格納するかイレイジャーコーディングコピーを格納することで、オブジェクトを損失から保護できます。作成するコピーのタイプは、ILMルールの配置手順で指定します。

- "レプリケーションとは"
- "シングルコピーレプリケーションを使用しない理由"
- "イレイジャーコーディングとは"
- "イレイジャーコーディングスキームとは"
- "イレイジャーコーディングのメリット、デメリット、および要件"

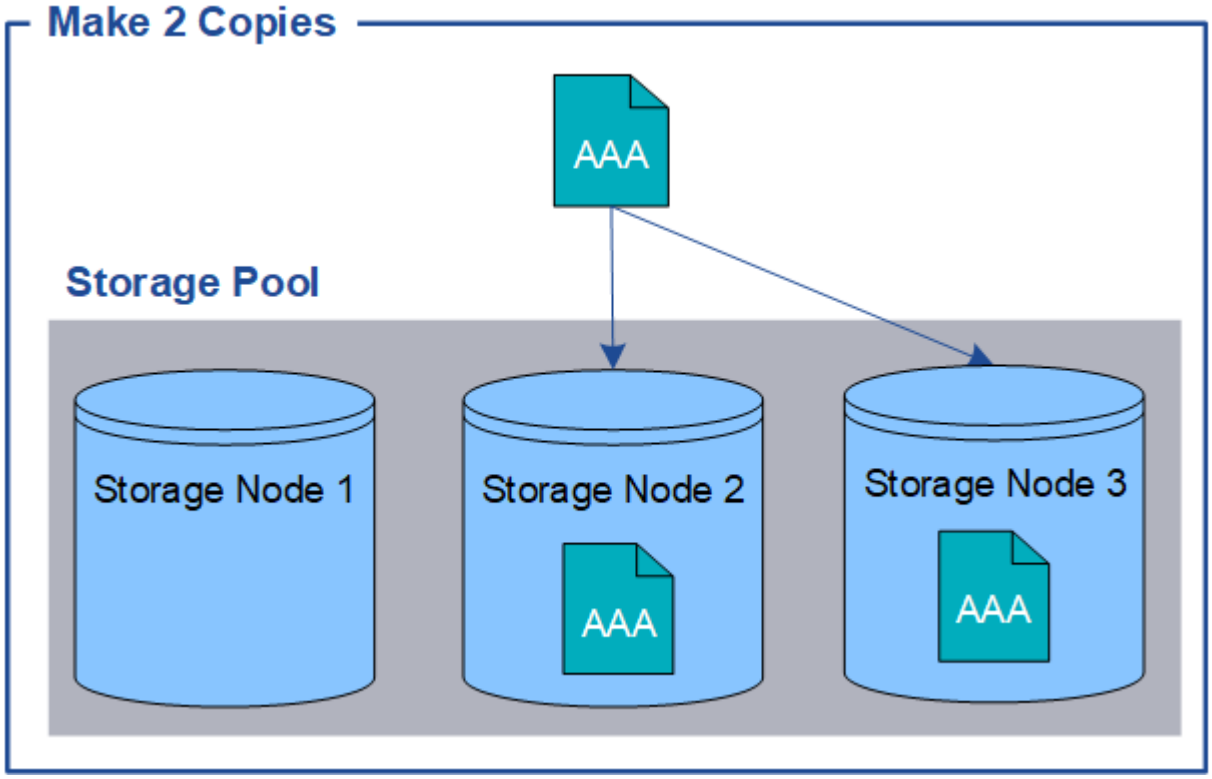
レプリケーションとは

レプリケーションは、 StorageGRID がオブジェクトデータを格納するために使用する 2 つの方法のうちの 1 つです。レプリケーションを使用する ILM ルールにオブジェクトが一致すると、オブジェクトデータの完全なコピーが作成され、ストレージノードまたはアーカイブノードに格納されます。

レプリケートコピーを作成するように ILM ルールを設定する場合は、作成するコピーの数、コピーを配置す

る場所、およびそれぞれの場所にコピーを格納する期間を指定します。

次の例の ILM ルールは、各オブジェクトのレプリケートコピーを 2 つずつ、 3 つのストレージノードからなるストレージプールに配置するように指定されています。



このルールにオブジェクトが一致した場合、 StorageGRID はオブジェクトのコピーを 2 つ作成して、ストレージプール内の別々のストレージノードにそれぞれのコピーを配置します。この 2 つのコピーは、使用可能な 3 つのストレージノードのうちのいずれか 2 つに配置されます。この場合、ストレージノード 2 と 3 に配置されています。コピーは 2 つあるため、ストレージプール内のいずれかのノードで障害が発生した場合でもオブジェクトを読み出すことができます。

StorageGRID が任意のストレージノードに格納できるレプリケートコピーは 1 つのオブジェクトにつき 1 つだけです。グリッドにストレージノードが 3 つあり、 4 コピーの ILM ルールを作成した場合、作成されるコピーはストレージノードごとに 1 つだけになります。ILM placement unAchievable * アラートがトリガーされ、 ILM ルールを完全に適用できなかったことを示します。

関連情報

"ストレージプールとは"

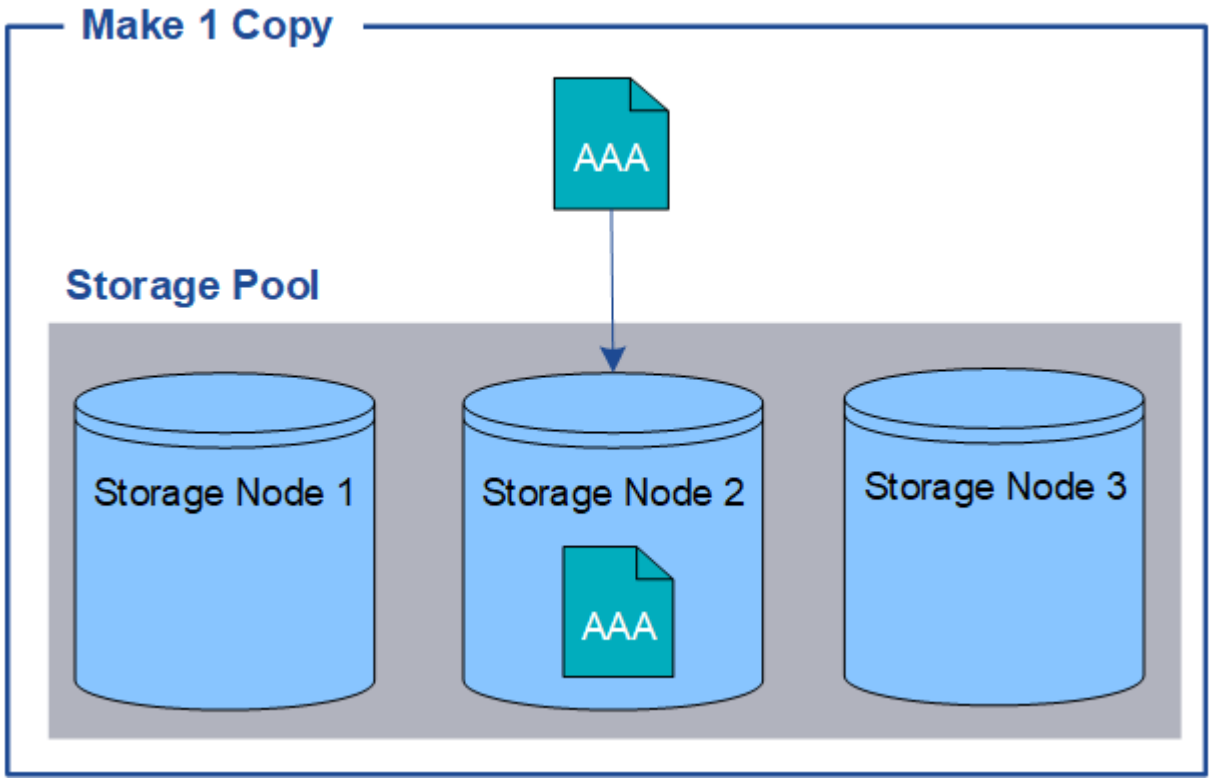
"複数のストレージプールを使用したサイト間レプリケーション"

シングルコピーレプリケーションを使用しない理由

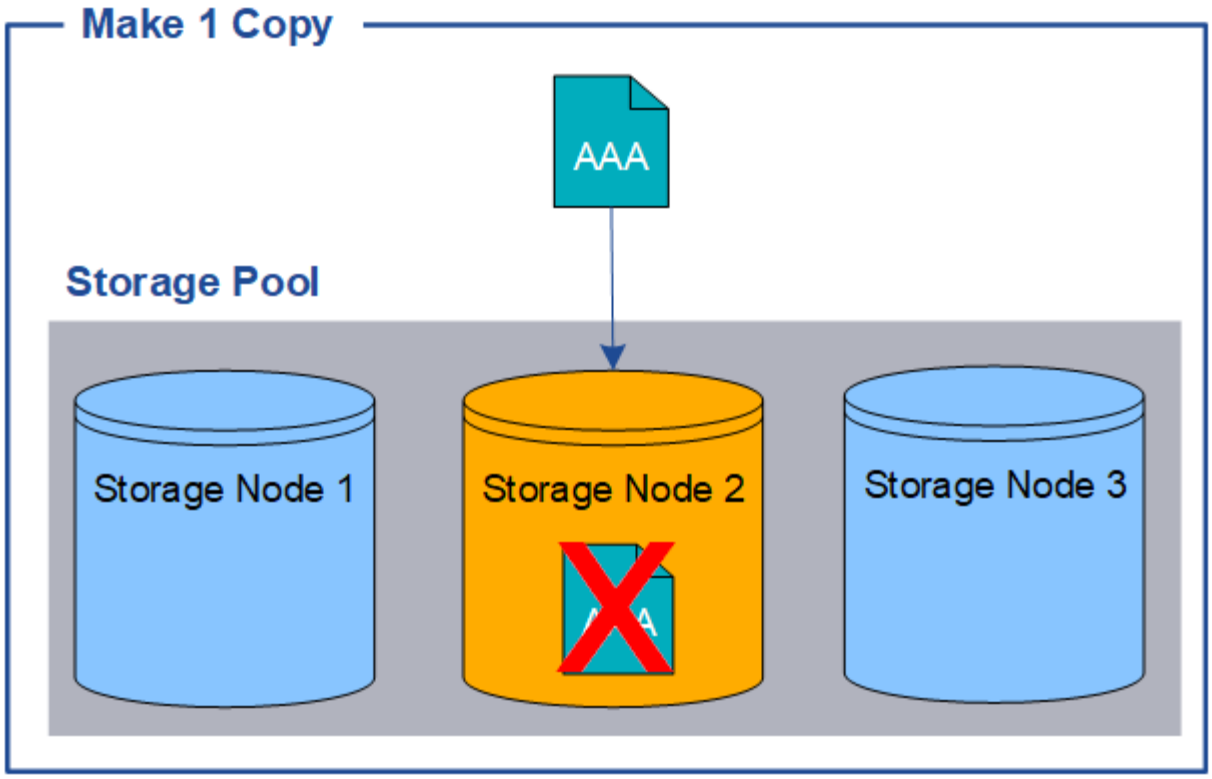
レプリケートコピーを作成する ILM ルールを作成するときは、配置手順の任意の期間に少なくとも 2 つのコピーを指定する必要があります。

レプリケートコピーを 1 つだけ作成する ILM ルールは、どの期間も使用しないでください。オブジェクトのレプリケートコピーが 1 つしかない場合、ストレージノードに障害が発生したり、重大なエラーが発生すると、そのオブジェクトは失われます。また、アップグレードなどのメンテナンス作業中は、オブジェクトへのアクセスが一時的に失われます。

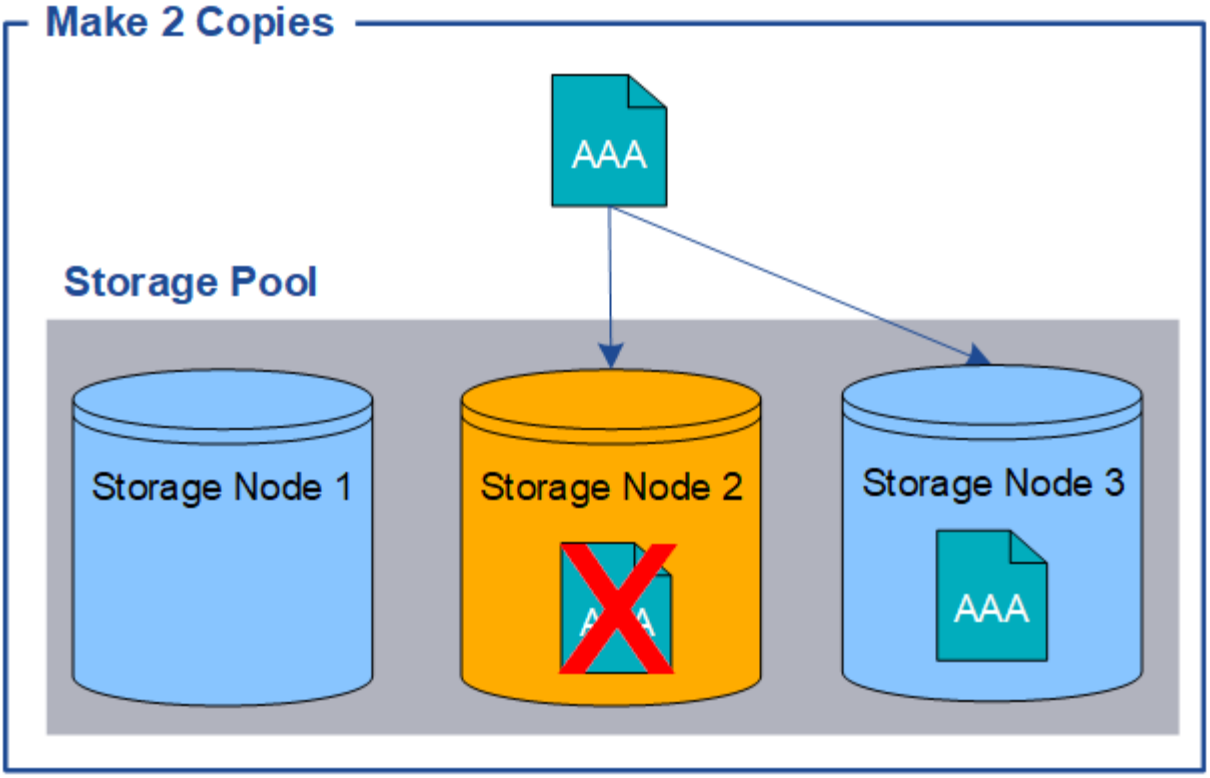
次の例では、 Make 1 Copy ILM ルールによって、 1 つのオブジェクトのレプリケートコピーを 3 つのストレージノードからなるストレージプールに配置するように指定しています。このルールに一致するオブジェクトが取り込まれると、 StorageGRID は 1 つのストレージノードにのみコピーを配置します。



ILM ルールにオブジェクトのレプリケートコピーが 1 つしか作成されていない場合、ストレージノードが使用できなくなるとオブジェクトにアクセスできなくなります。この例では、アップグレードやその他のメンテナンス手順 の実行中など、ストレージノード 2 がオフラインになるとオブジェクト AAA へのアクセスが一時的に失われます。ストレージノード 2 で障害が発生すると、オブジェクト AAA が完全に失われます。



オブジェクトデータの損失を防ぐには、レプリケーションで保護するすべてのオブジェクトのコピーを常に 2 つ以上作成する必要があります。コピーが複数ある場合も、 1 つのストレージノードに障害が発生した場合やオフラインになった場合でもオブジェクトにアクセスできます。

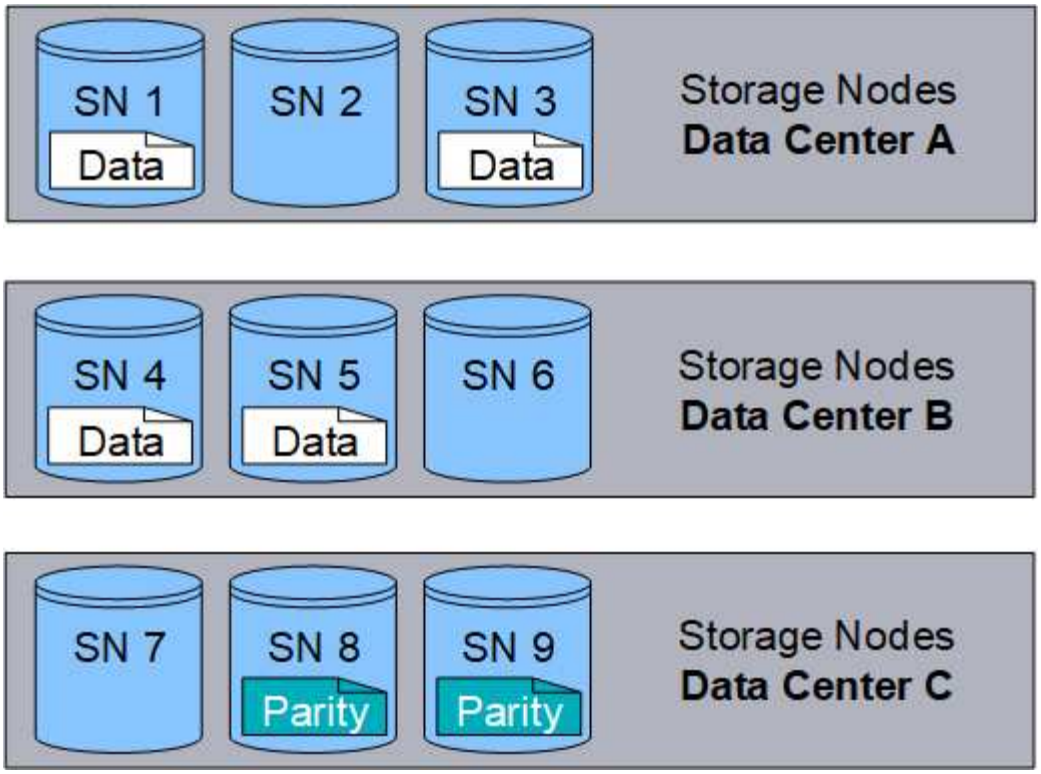


イレイジャーコーディングとは

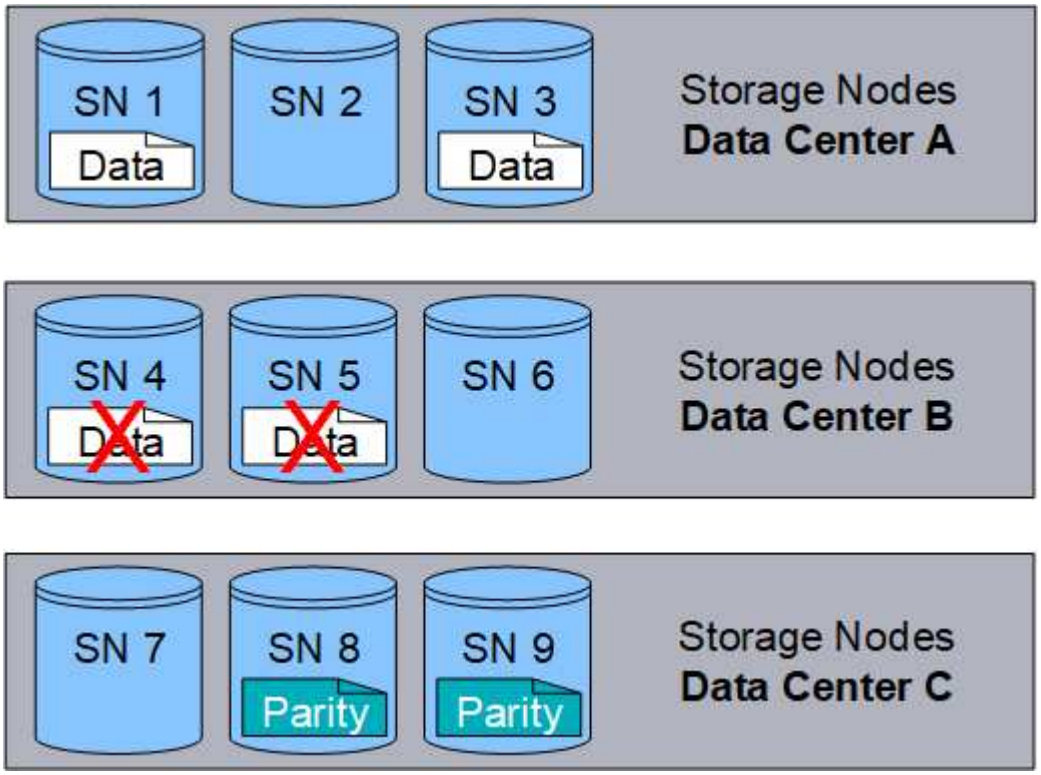
イレイジャーコーディングとは

イレイジャーコーディングは、オブジェクトデータを格納するために StorageGRID で使用される 2 つ目の方法です。StorageGRID がイレイジャーコーディングコピーを作成するために設定された ILM ルールとオブジェクトを照合する場合は、オブジェクトデータを複数のデータフラグメントに分割し、追加のパリティフラグメントを計算して、各フラグメントを別のストレージノードに格納します。アクセスされたオブジェクトは、格納されたフラグメントを使用して再アセンブルされます。データフラグメントまたはパリティフラグメントが破損したり失われたりしても、イレイジャーコーディングアルゴリズムが残りのデータフラグメントとパリティフラグメントを使用してそのフラグメントを再作成します。

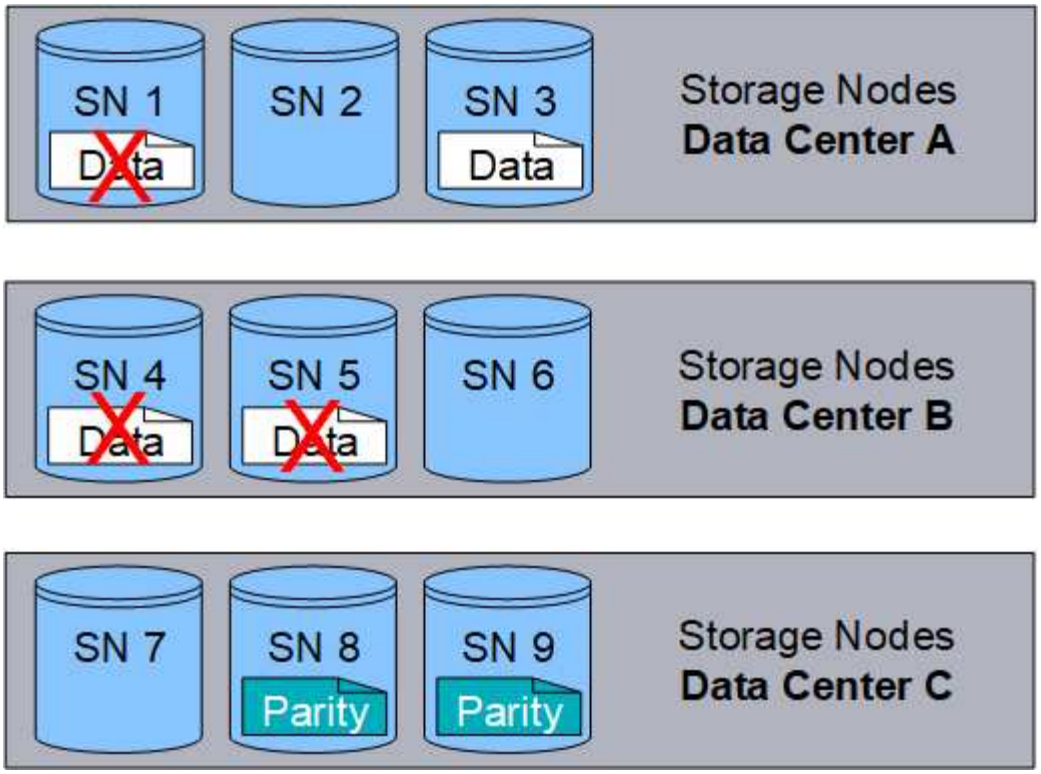
次の例は、オブジェクトのデータに対するイレイジャーコーディングアルゴリズムの使用方法を示しています。この例の ILM ルールでは 4+2 のイレイジャーコーディングスキームを使用します。各オブジェクトは 4 つのデータフラグメントに等分され、オブジェクトデータから 2 つのパリティフラグメントが計算されます。ノードやサイトの障害時にもデータが保護されるよう、 6 つの各フラグメントは 3 つのデータセンターサイトの別々のノードに格納されます。



4+2 のイレイジャーコーディングスキームでは、少なくとも 9 個のストレージノードが必要です。このノードには、 3 つのサイトそれぞれに 3 個のストレージノードが必要です。6 つのうちのいずれか 4 つのフラグメント（データまたはパリティ）が使用可能であれば、オブジェクトを読み出すことができます。最大 2 つのフラグメントが失われても、オブジェクトデータが失われることはありません。データセンターサイト全体で障害が発生した場合でも、他のすべてのフラグメントに引き続きアクセスできれば、オブジェクトの読み出しまたは修復が可能です。



3 つ以上のストレージノードが失われると、オブジェクトを読み出せなくなります。



関連情報

"ストレージプールとは"

"イレイジャーコーディングスキームとは"

"イレイジャーコーディングプロファイルの設定"

イレイジャーコーディングスキームとは

ILM ルールにイレイジャーコーディングプロファイルを設定する場合は、使用するストレージプールを構成するストレージノードとサイトの数に基づいて、使用可能なイレイジャーコーディングスキームを選択します。イレイジャーコーディングスキームは、各オブジェクト用に作成されるデータフラグメントとパリティフラグメントの数を制御します。

StorageGRID システムは、 Reed-Solomon イレイジャーコーディングアルゴリズムを使用します。このアルゴリズムは、オブジェクトを k 個のデータフラグメントに分割して、 m 個のパリティフラグメントを計算します。k + m = n 個のフラグメントが n 個のストレージノードに分散され、データ保護を提供します。失われたフラグメントまたは破損したフラグメントは、オブジェクトが保持できる最大 m 個です。k 個のフラグメントがオブジェクトの読み出しまたは修復に必要です。

イレイジャーコーディングプロファイルを設定する場合は、ストレージプールについて次のガイドラインに従ってください。

- ストレージプールには 3 つ以上のサイト、または 1 つのサイトだけが含まれている必要があります。

> ストレージプールにサイトが 2 つ含まれている場合、イレイジャーコーディングプロファイルは設定できません。

- 3 つ以上のサイトを含むストレージプールのイレイジャーコーディングスキーム
- 1 サイトのストレージプールのイレイジャーコーディングスキーム

- デフォルトのストレージプール、すべてのストレージノード、またはデフォルトサイトであるすべてのサイトを含むストレージプールは使用しないでください。
- ストレージプールには少なくとも *k* + *m*+1 ストレージノードを含める必要があります。

  必要なストレージノードの最小数は、 _ k + m_. です。ただし、必要なストレージノードが一時的に使用できない場合に、少なくとも 1 つのストレージノードを追加することで、取り込みエラーや ILM バックログが発生するのを防ぐことができます。

イレイジャーコーディングスキームのストレージオーバーヘッドは、パリティフラグメントの数（ *m*） をデータフラグメントの数（ *k* ）で割ることによって計算されます。ストレージオーバーヘッドを使用して、各イレイジャーコーディングオブジェクトに必要なディスクスペースを計算できます。

```
disk space = object size + (object size * storage overhead)
```

たとえば、 4+2 スキームを使用して 10MB のオブジェクト（ストレージオーバーヘッドが 50% ）を格納すると、そのオブジェクトが消費するグリッドストレージは 15MB です。6+3 のストレージオーバーヘッドを含む 6+2 スキームを使用して同じ 10MB のオブジェクトを格納すると、オブジェクトが消費するサイズは約 13.3 MB になります。

合計値が最も小さいイレイジャーコーディングスキーム（ _k + m_that ）をニーズに合わせて選択します。フラグメント数が少ないイレイジャーコーディングスキームは全体的に計算効率が高く、 1 つのオブジェクトに作成されて分散（または取得）されるフラグメント数が少なくて済むため、フラグメントサイズが大きいためパフォーマンスが向上し、ストレージの追加が必要になった場合に拡張時に必要なノード数が少なくて済みます。（ストレージ拡張の計画については、 StorageGRID の拡張手順を参照してください）。

3 つ以上のサイトを含むストレージプールのイレイジャーコーディングスキーム

次の表に、 3 つ以上のサイトを含むストレージプールについて、 StorageGRID で現在サポートされているイレイジャーコーディングスキームを示します。これらの方式はいずれもサイト障害からの保護を提供します。1 つのサイトが失われてもオブジェクトには引き続きアクセスできます。

サイト損失の保護を提供するイレイジャーコーディングスキームの場合、ストレージプールに推奨されるストレージノードの数は各サイトに少なくとも 3 つのストレージノードが必要なため _ k + m_+1 を超えています。

イレイジャーコーディングスキーム（ *k* + *m*）	サイトの最小数	各サイトで推奨されるストレージノードの数	推奨されるストレージノードの総数	サイト障害からの保護	ストレージオーバーヘッド
4+2	3.	3.	9.	はい。	50%
6+2	4.	3.	12.	はい。	33%
8+2	5.	3.	15	はい。	25%
6 + 3	3.	4.	12.	はい。	50%

イレイジャーコーディングスキーム（ *k* + *m*）	サイトの最小数	各サイトで推奨されるストレージノードの数	推奨されるストレージノードの総数	サイト障害からの保護	ストレージオーバーヘッド
9 + 3	4.	4.	16	はい。	33%
2+1	3.	3.	9.	はい。	50%
4+1	5.	3.	15	はい。	25%
6+1	7.	3.	21	はい。	17%
7+5	3.	5.	15	はい。	71%

StorageGRID では、サイトごとに少なくとも 3 つのストレージノードが必要です。7+5 スキームを使用するには、各サイトに少なくとも 4 つのストレージノードが必要。サイトごとに 5 つのストレージノードを使用することを推奨します。

サイト保護を提供するイレイジャーコーディングスキームを選択する場合は、次の要素の相対的な重要性を調整します。

- * フラグメント数 * ：フラグメントの総数が少ないほど、一般にパフォーマンスと拡張の柔軟性が向上します。
- * フォールトトレランス * ：パリティセグメントの数を増やすことでフォールトトレランスが向上します（ _m_の 値が大きい場合）。
- * ネットワーク・トラフィック *: 障害から回復する場合、フラグメント数の多いスキーム（つまり、 *k* + *m*） を使用すると、より多くのネットワーク・トラフィックが生成されます。
- * ストレージ・オーバーヘッド * ：オーバーヘッドの大きいスキームでは、オブジェクトごとにより多くのストレージ・スペースが必要です。

たとえば、 4+2 と 6+3 のどちらかのスキーム（どちらも 50% のストレージオーバーヘッドがある）を選ぶ場合、フォールトトレランスをさらに高める必要がある場合は 6+3 のスキームを選択します。ネットワークリソースが制限されている場合は、 4+2 のスキームを選択します。他のすべての要素が等しい場合は、フラグメントの合計数が少ないため、 4+2 を選択します。

使用するスキームが不明な場合は、 4+2 または 6+3 を選択するか、テクニカルサポートにお問い合わせください。

1 サイトのストレージプールのイレイジャーコーディングスキーム

1 サイトのストレージプールでは、サイトに十分な数のストレージノードがある場合、 3 つ以上のサイト用に定義されたすべてのイレイジャーコーディングスキームがサポートされます。

必要なストレージノードの最小数は *k* + *m_1* ですが、 *_k* + *m*+1 ストレージノードを含むストレージプールを推奨します。たとえば、 2+1 イレイジャーコーディングスキームには少なくとも 3 つのストレージノードからなるストレージプールが必要ですが、推奨されるストレージノード数は 4 つです。

イレイジャーコーディングスキーム（ *k* + *m*）	ストレージノードの最小数	推奨されるストレージノードの数	ストレージオーバーヘッド
4+2	6.	7.	50%
6+2	8.	9.	33%
8+2	10.	11.	25%
6 + 3	9.	10.	50%
9 + 3	12.	13	33%
2+1	3.	4.	50%
4+1	5.	6.	25%
6+1	7.	8.	17%
7+5	12.	13	71%

関連情報

"グリッドを展開します"

イレイジャーコーディングのメリット、デメリット、および要件

レプリケーションとイレイジャーコーディングのどちらを使用してオブジェクトデータを損失から保護するかを決定する前に、イレイジャーコーディングのメリット、デメリット、および要件を理解しておく必要があります。

イレイジャーコーディングのメリット

イレイジャーコーディングは、レプリケーションに比べて信頼性、可用性、ストレージ効率に優れています。

- * 信頼性 * ：信頼性はフォールトトレランス、つまり同時にデータを失うことなく維持できる障害の数によって判断されます。レプリケーションでは、複数の同一コピーが異なるノード上およびサイト間に格納されます。イレイジャーコーディングの場合、オブジェクトはデータフラグメントとパリティフラグメントにエンコードされ、多数のノードとサイトに分散されます。この分散によってサイトとノード両方の障害からの保護を提供します。イレイジャーコーディングは、同等のストレージコストでレプリケーションよりも優れた信頼性を提供します。
- * 可用性 * ：可用性は、ストレージノードに障害が発生した場合や、ノードにアクセスできなくなった場合にオブジェクトを読み出すことができるかどうかによって定義されます。イレイジャーコーディングは、同等のストレージコストでレプリケーションよりも優れた可用性を提供します。
- * Storage Efficiency * ：可用性と信頼性が同等レベルの場合、イレイジャーコーディングで保護されたオブジェクトが消費するディスクスペースは、同じオブジェクトをレプリケーションで保護する場合よりも少なくなります。たとえば、 10MB のオブジェクトを 2 つのサイトにレプリケートするとディスクスペースを 20MB （ 2 つのコピー）消費しますが、 6+3 のイレイジャーコーディングスキームを使用して 3 つ

のサイトにイレイジャーコーディングされたオブジェクトが消費するディスクスペースは 15MB のみです。

> イレイジャーコーディングオブジェクトのディスクスペースは、オブジェクトサイズにストレージオーバーヘッドを加えたものです。ストレージオーバーヘッドの割合は、パリティフラグメント数をデータフラグメント数で割って算出します。

イレイジャーコーディングのデメリット

レプリケーションと比較した場合のイレイジャーコーディングのデメリットは次のとおりです。

- より多くのストレージノードとサイトが必要です。たとえば、 6+3 のイレイジャーコーディングスキームを使用する場合は、 3 つのサイトに少なくとも 3 つのストレージノードが必要です。一方、オブジェクトデータをレプリケートする場合は、各コピーに必要なストレージノードは 1 つだけです。
- ストレージの拡張にかかるコストと複雑さが増大します。レプリケーションを使用する環境を拡張するには、オブジェクトコピーを作成するすべての場所にストレージ容量を追加するだけです。イレイジャーコーディングを使用する環境を拡張する場合は、使用中のイレイジャーコーディングスキームと、既存のストレージノードの使用率の両方を考慮する必要があります。たとえば、既存のノードが 100% フルになるまで待つ場合は、少なくとも _k + m_Storage ノードを追加する必要があります。ただし、既存のノードが 70% フルになった時点で拡張する場合は、サイトごとに 2 つのノードを追加し、使用可能なストレージ容量を最大化できます。詳細については、StorageGRID の拡張手順を参照してください。
- 地理的に分散したサイトでイレイジャーコーディングを使用する場合は、読み出しのレイテンシが上昇します。イレイジャーコーディングされてリモートサイトに分散されたオブジェクトのフラグメントを WAN 接続経由で読み出す場合、レプリケートされてローカル（クライアントの接続先と同じサイト）で利用可能なオブジェクトよりも時間がかかります。
- 地理的に分散したサイトでイレイジャーコーディングを使用する場合は、特に WAN ネットワーク接続経由でオブジェクトを頻繁に読み出したり修復したりするケースでは読み出しと修復の WAN ネットワークトラフィックが増大します。
- サイト間でイレイジャーコーディングを使用する場合は、サイト間のネットワークレイテンシの上昇に伴ってオブジェクトの最大スループットが大幅に低下します。この最大スループットの低下は TCP ネットワークのスループットが低下したことによるもので、 StorageGRID システムによるオブジェクトフラグメントの格納 / 読み出し速度に影響します。
- コンピューティングリソースの利用率が向上します。

イレイジャーコーディングを使用する状況

イレイジャーコーディングは次の要件に最適です。

- 1MBを超えるオブジェクト

> イレイジャーコーディングコピーに関連付けられているフラグメント数の管理でオーバーヘッドが発生するため、200KB以下のオブジェクトにはイレイジャーコーディングを使用しないでください。

- 頻繁に読み出されないコンテンツの長期保存またはコールドストレージ。
- 高いデータ可用性と信頼性。
- サイトやノードの障害に対する保護

- ストレージ効率
- 複数のレプリケートコピーではなく 1 つのイレイジャーコーディングコピーのみを使用して効率的にデータを保護する必要のある単一サイト環境
- サイト間レイテンシが 100 ミリ秒未満の複数サイト環境

関連情報

"グリッドを展開します"

オブジェクト保持期間の決定方法

StorageGRID には、グリッド管理者と個々のテナントユーザが、オブジェクトを格納する期間を指定するためのオプションがあります。通常、テナントユーザが指定した保持手順は、グリッド管理者が指定した保持手順よりも優先されます。

テナントユーザによるオブジェクト保持期間の制御方法

テナントユーザは、主に次の 3 つの方法でオブジェクトを StorageGRID に格納する期間を制御できます。

- グリッドでグローバルな S3 オブジェクトのロック設定が有効になっている場合、 S3 テナントユーザは S3 オブジェクトのロックを有効にしたバケットを作成し、 S3 REST API を使用して、そのバケットに追加された各オブジェクトバージョンの最新の保持設定とリーガルホールド設定を指定できます。
  - リーガルホールドの対象になっているオブジェクトバージョンは、どの方法でも削除できません。
  - オブジェクトバージョンの retain-until - date に到達するまでは、どのメソッドでもそのバージョンを削除することはできません。
  - S3 オブジェクトロックが有効なバケット内のオブジェクトは ILM によって「無期限」に保持されます。 ただし、それまでの保持期間が終了したあとは、クライアント要求やバケットライフサイクルの終了によってオブジェクトバージョンを削除できます。

    "S3オブジェクトロックでオブジェクトを管理する"

- S3 テナントユーザは、 Expiration アクションを指定するライフサイクル設定をバケットに追加できます。バケットライフサイクルが存在する場合、クライアントがオブジェクトを削除しないかぎり、StorageGRID は Expiration アクションで指定された日付または日数が経過するまでオブジェクトを格納します。
- S3 / Swift クライアントは、オブジェクトの削除要求を問題 に送信できます。StorageGRID は、オブジェクトを削除するか保持するかを決定する際に、常に S3 バケットライフサイクルまたは ILM よりもクライアントの削除要求を優先します。

グリッド管理者によるオブジェクト保持期間の制御方法

グリッド管理者は、 ILM の配置手順を使用してオブジェクトの格納期間を制御します。オブジェクトが ILM ルールに一致した場合、 StorageGRID は ILM ルールの最後の期間が経過するまでそのオブジェクトを格納します。配置手順に「 forever 」が指定されている場合、オブジェクトは無期限に保持されます。

オブジェクトの保持期間を誰が制御するかに関係なく、格納するオブジェクトコピーのタイプ（レプリケートまたはイレイジャーコーディング）とコピーの場所（ストレージノード、クラウドストレージプール、またはアーカイブノード）は ILM 設定によって制御されます。

S3 バケットライフサイクルと ILM の相互作用

S3 バケットライフサイクルの Expiration アクションは、常に ILM 設定よりも優先されます。その結果、 ILM のオブジェクト配置手順がすべて終了したあとも、オブジェクトがグリッドに保持されることがあります。

オブジェクト保持の例

S3 オブジェクトロック、バケットライフサイクル設定、クライアントの削除要求、 ILM の相互作用について、より深く理解するために次の例を検討してください。

例 1 ： S3 バケットライフサイクルのオブジェクト保持期間が ILM よりも長い

ILM

2 つのコピーを 1 年間保存（ 365 日）

バケットライフサイクル

2 年（ 730 日）でオブジェクトが期限切れになる

結果

StorageGRID はオブジェクトを 730 日間格納します。StorageGRID は、バケットライフサイクル設定を使用して、オブジェクトを削除するか保持するかを決定します。

> ILM よりもバケットライフサイクルのオブジェクト保持期間の方が長い場合でも、格納するコピーの数とタイプを決定する際には引き続き StorageGRID の配置手順が使用されます。この例では、 366 日目から 730 日目までの間、オブジェクトの 2 つのコピーが StorageGRID に引き続き格納されます。

例 2 ： S3 バケットライフサイクルのオブジェクト保持期間よりも短い

ILM

2 つのコピーを 2 年間（ 730 日）格納する

バケットライフサイクル

1 年（ 365 日）でオブジェクトを期限切れにする

結果

StorageGRID は 365 日目にオブジェクトのコピーを両方削除します。

例 3 ：クライアントによる削除は、バケットライフサイクルと ILM よりも優先されます

ILM

2 つのコピーをストレージ・ノードに無期限に保存

バケットライフサイクル

2 年（ 730 日）でオブジェクトが期限切れになる

クライアントの削除要求

発行日： 400 日目

結果

StorageGRID は、クライアントの削除要求に応じて 400 日目にオブジェクトのコピーを両方削除します。

例 **4** ： **S3** オブジェクトロックはクライアントの削除要求を上書きします

S3 オブジェクトのロック

オブジェクトバージョンの retain-until は、 2026-03-31 です。リーガルホールドは有効ではありません。

準拠 **ILM** ルール

2 つのコピーをストレージ・ノードに無期限に保存します

クライアントの削除要求

2024-03-331 発行。

結果

retain-until はまだ 2 年前の時点であるため、 StorageGRID はオブジェクトバージョンを削除しません。

関連情報

"S3オブジェクトロックでオブジェクトを管理する"

"S3 を使用する"

"ILM ルールの配置手順とは"

オブジェクトの削除方法

StorageGRID は、クライアント要求に直接応答してオブジェクトを削除するか、 S3 バケットライフサイクルの終了または ILM ポリシーの要件に応じて自動的にオブジェクトを削除します。オブジェクトのさまざまな削除方法と StorageGRID による削除要求の処理方法を理解しておくと、オブジェクトをより効率的に管理できるようになります。

StorageGRID では、次のいずれかの方法でオブジェクトを削除できます。

- 同期削除： StorageGRID がクライアントの削除要求を受け取ると、すべてのオブジェクトコピーがただちに削除されます。コピーが削除されると、削除が成功したことがクライアントに通知されます。
- オブジェクトは削除キューに登録されます。 StorageGRID が削除要求を受け取ると、オブジェクトは削除キューに登録され、削除が成功したことがクライアントにすぐに通知されます。オブジェクトコピーは、あとでバックグラウンド ILM 処理によって削除されます。

StorageGRID では、オブジェクトを削除する際に、削除のパフォーマンスを最適化し、削除のバックログを最小限に抑え、スペースを最も早く解放する方法を使用します。

次の表は、 StorageGRID がどのような場合に各メソッドを使用するかを

削除方法	使用時
オブジェクトは削除キューに登録されます	次の条件のいずれか * が当てはまる場合： • 次のいずれかのイベントによってオブジェクトの自動削除がトリガーされた： ◦ S3 バケットのライフサイクル設定の有効期限または日数に達した。 ◦ ILM ルールに指定された最後の期間が経過した。 • 注： S3 オブジェクトのロックが有効になっているバケット内のオブジェクトは、リーガルホールドの対象である場合や、 retain-until date を指定したものの、まだ満たされていない場合は削除できません。 • S3 / Swift クライアントが削除を要求し、次の条件を 1 つ以上満たしている： ◦ オブジェクトの場所が一時的に使用できないなどの理由で、 30 秒以内にコピーを削除できない。 ◦ バックグラウンド削除キューがアイドル状態である。
オブジェクトをただちに削除（同期削除）	S3 / Swift クライアントが削除要求を行い、次の * すべての条件が満たされている場合： • すべてのコピーを 30 秒以内に削除できる。 • バックグラウンド削除キューには処理するオブジェクトが含まれています。

S3 / Swift クライアントが削除要求を行うと、 StorageGRID はまずオブジェクトを削除キューに追加します。その後、同期削除の実行に切り替えます。処理対象となるオブジェクトがバックグラウンド削除キューに含まれていることを確認することで、 StorageGRID は、クライアントによる削除のバックログが発生しないようにしつつ、特に同時実行性の低いクライアントに対してより効率的に削除を処理できます。

StorageGRID によるオブジェクトの削除方法が及ぼす影響を理解しておく必要があります

StorageGRID によるオブジェクトの削除方法は、システムの動作に影響を及ぼす可能性があります。

- StorageGRID StorageGRID で同期削除が実行されると、結果がクライアントに返されるまでに最大 30 秒かかることがあります。つまり、実際には StorageGRID がオブジェクトを削除キューに登録する場合よりも短時間でコピーが削除されるにもかかわらず、より長くかかっているという印象をクライアントに与える可能性があります。
- 一括削除の実行中にそのパフォーマンスを注意深く監視していると、一定数のオブジェクトが削除されたあとに削除の速度が遅くなったように見えることがあります。この変更は、 StorageGRID がオブジェクトを削除キューへ登録する方法から同期削除に切り替えたときに発生します。削除速度が低下したように見えても、オブジェクトコピーの削除速度が遅くなったわけではありません。一方で、スペースの開放にかかる時間は、平均すると短くなっています。

大量のオブジェクトを削除する場合に、スペースを短時間で解放することが優先されるのであれば、 ILM などの方法を使用してオブジェクトを削除するのではなく、クライアント要求を使用することを検討してください。一般に、クライアントによって削除が実行された場合、 StorageGRID は同期削除を使用できるため、ス

ペースはより短時間で解放されます。

オブジェクトの削除後にスペースを解放するために必要な時間は、次の要因によって異なります。

- オブジェクトコピーが同期的に削除されるか、またはキューに登録されたあとで削除されるか（クライアントの削除要求の場合）。
- グリッド内のオブジェクトの数や、オブジェクトコピーが削除対象キューに登録される場合のグリッドリソースの可用性などのその他の要因（クライアントによる削除およびその他の方法の場合）。

S3 バージョン管理オブジェクトの削除方法

S3 バケットでバージョン管理が有効になっている場合、 StorageGRID は、削除要求に応答する際、要求が S3 クライアント、 S3 バケットライフサイクルの終了、 ILM ポリシーの要件のいずれによるものであるかにかかわらず、 Amazon S3 の動作に従います。

オブジェクトがバージョン管理されている場合、オブジェクトの削除要求は現在のバージョンのオブジェクトを削除せず、スペースも解放しません。代わりに ' オブジェクト削除要求は ' 最新バージョンのオブジェクトとして削除マーカーを作成するだけで ' 以前のバージョンのオブジェクトは noncurrent になります

オブジェクトが削除されていなくても、 StorageGRID は現在のバージョンのオブジェクトが使用できなくなったかのように動作します。そのオブジェクトに対する要求は 404 NotFound を返します。ただし、最新でないオブジェクトデータは削除されていないため、最新でないバージョンのオブジェクトを指定する要求は成功します。

バージョン管理オブジェクトを削除するときにスペースを解放するには、次のいずれかを実行する必要があります。

- * S3クライアント要求*：S3 DELETE Object要求でオブジェクトのバージョン番号を指定します (`DELETE /object?versionId=ID`）。この要求は、指定したバージョンのオブジェクトコピーだけを削除します（他のバージョンは引き続きスペースを消費します）。
- バケットライフサイクル：を使用します `NoncurrentVersionExpiration` をクリックします。NoncurrentDays で指定した日数に達すると、 StorageGRID は最新でないオブジェクトバージョンのコピーをすべて完全に削除します。これらのオブジェクトバージョンはリカバリできません。
- * ILM * ： ILM ポリシーに 2 つの ILM ルールを追加します。最新でないバージョンのオブジェクトに一致する場合は、最初のルールで「 * noncurrent Time * 」を参照時間として使用します。2 つ目のルールの * 取り込み時間 * を現在のバージョンと一致させます。「 * noncurrent Time * 」ルールは、「 * Ingest Time * 」ルールの上のポリシーに含める必要があります。

関連情報

"S3 を使用する"

"例 4 ： S3 バージョン管理オブジェクトの ILM ルールとポリシー"

ILM ポリシーとは

情報ライフサイクル管理（ ILM ）ポリシーは、優先順位が付けられた一連の ILM ルールです。 StorageGRID システムが時間の経過に伴ってオブジェクトデータを管理する方法を決定します。

ILM ポリシーによるオブジェクトの評価方法

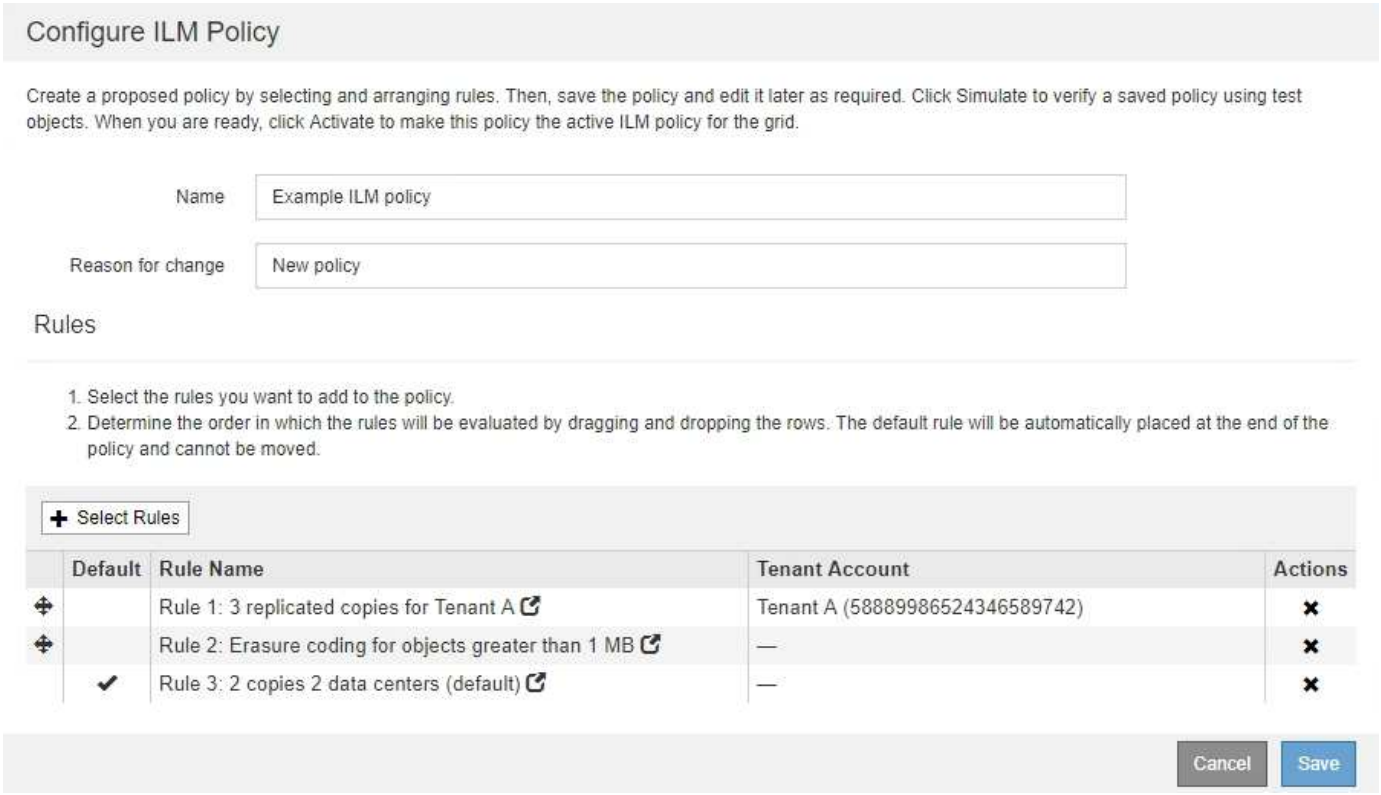
StorageGRID システムのアクティブな ILM ポリシーは、すべてのオブジェクトの配置、期間、データ保護を制御します。

クライアントがオブジェクトを StorageGRID に保存すると、オブジェクトはアクティブポリシー内の順序付けられた ILM ルールに照らして次のように評価されます。

1. ポリシー内の最初のルールのフィルタがオブジェクトに一致すると、オブジェクトはそのルールの取り込み動作に従って取り込まれ、そのルールの配置手順に従って格納されます。
2. 最初のルールのフィルタがオブジェクトに一致しない場合、オブジェクトは一致が見つかるまでポリシー内の後続の各ルールに照らして評価されます。
3. どのルールもオブジェクトに一致しない場合は、ポリシー内のデフォルトルールの取り込み動作と配置手順が適用されます。デフォルトルールはポリシー内の最後のルールであり、フィルタは使用できません。

ILM ポリシーの例

この例の ILM ポリシーは 3 つの ILM ルールを使用します。

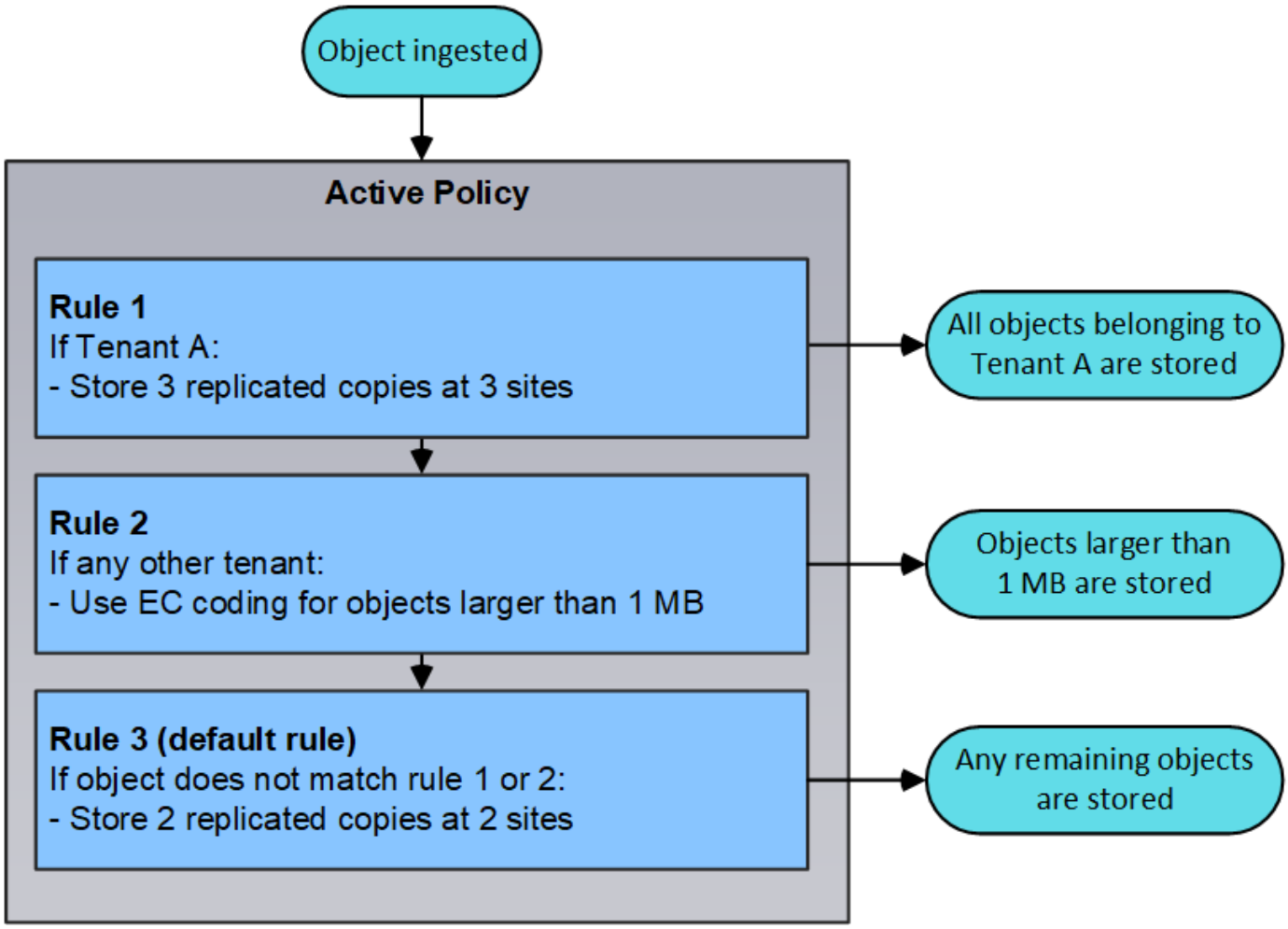


この例では、ルール 1 はテナント A に属するすべてのオブジェクトに一致しますこれらのオブジェクトは、3 つのサイトに 3 つのレプリケートコピーとして格納されます。他のテナントに属するオブジェクトはルール 1 に一致しないため、ルール 2 に照らして評価されます。

ルール2では、他のテナントのすべてのオブジェクトが一致しますが、1MBより大きいオブジェクトのみが該当します。これらのオブジェクトは、 3 つのサイトで 6+3 のイレイジャーコーディングを使用して格納されます。ルール 2 がオブジェクト 1MB 以下に一致しないため、これらのオブジェクトはルール 3 に照らして評価されます。

ルール 3 はポリシー内の最後のルールで、デフォルトのルールであり、フィルタは使用しません。ルール 3

では、ルール 1 またはルール 2 に一致しないすべてのオブジェクトのレプリケートコピーを 2 つ作成します（ 1MB 以下のテナント A に属していないオブジェクト）。



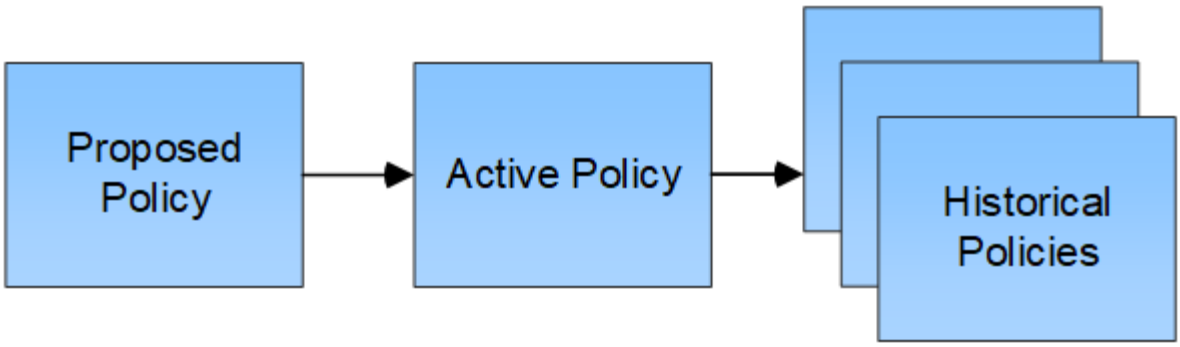
ドラフトポリシー、アクティブポリシー、履歴ポリシーとは

各 StorageGRID システムには、アクティブな ILM ポリシーが 1 つ必要です。StorageGRID システムでは、ドラフトの ILM ポリシーを 1 つと任意の数の履歴ポリシーを使用できます。

初めて ILM ポリシーを作成するときは、 ILM ルールを 1 つ以上選択して特定の順序で並べ、ドラフトポリシーを作成します。ドラフトポリシーをシミュレートして動作を確認したら、そのポリシーをアクティブ化してアクティブポリシーを作成します。

新しい ILM ポリシーをアクティブ StorageGRID 化すると、そのポリシーを使用して、既存のオブジェクトと新たに取り込まれたオブジェクトを含むすべてのオブジェクトが管理されます。新しいポリシーの ILM ルールが実装されたときに、既存のオブジェクトが新しい場所に移動されることがあります。

ドラフトポリシーをアクティブ化すると、それまでのアクティブポリシーは履歴ポリシーになります。ILM 履歴ポリシーは削除できません。



関連情報

"ILMポリシーを作成する"

ILM ルールとは

オブジェクトを管理するには、一連の情報ライフサイクル管理（ ILM ）ルールを作成して 1 つの ILM ポリシーにまとめます。システムに取り込まれた各オブジェクトは、アクティブポリシーに照らして評価されます。ポリシー内のルールがオブジェクトのメタデータに一致すると、ルールの手順に従って、 StorageGRID がそのオブジェクトをコピーして格納します。

ILM ルールでは次の項目を定義

- 格納するオブジェクト。ルールはすべてのオブジェクトに適用することも、ルール環境 を構成するオブジェクトを特定するフィルタを指定することもできます。たとえば、特定のテナントアカウント、特定の S3 バケットまたは Swift コンテナ、または特定のメタデータ値に関連付けられたオブジェクトにのみルールを適用できます。
- ストレージのタイプと場所。オブジェクトは、ストレージノード、クラウドストレージプール、またはアーカイブノードに格納できます。
- 作成するオブジェクトコピーのタイプ。コピーはレプリケートまたはイレイジャーコーディングできます。
- レプリケートコピーの場合は、作成されるコピーの数。
- イレイジャーコーディングコピーにはイレイジャーコーディングスキームを使用します。
- オブジェクトのストレージの場所とコピーのタイプの経時的変化。
- オブジェクトがグリッドに取り込まれるときにオブジェクトデータを保護する方法（同期配置またはデュアルコミット）。

オブジェクトメタデータは ILM ルールによって管理されません。代わりに、オブジェクトメタデータはメタデータストア内の Cassandra データベースに格納されます。データを損失から保護するために、オブジェクトメタデータの 3 つのコピーが各サイトで自動的に維持されます。コピーはすべてのストレージノードに均等に分散されます。

ILM ルールの要素

ILM ルールには次の 3 つの要素があります。

- * フィルタ条件 * ：ルールの基本フィルタと高度なフィルタにより、ルール環境 で使用するオブジェクトが定義されます。オブジェクトがすべてのフィルタに一致する場合、 StorageGRID はルールを適用し、

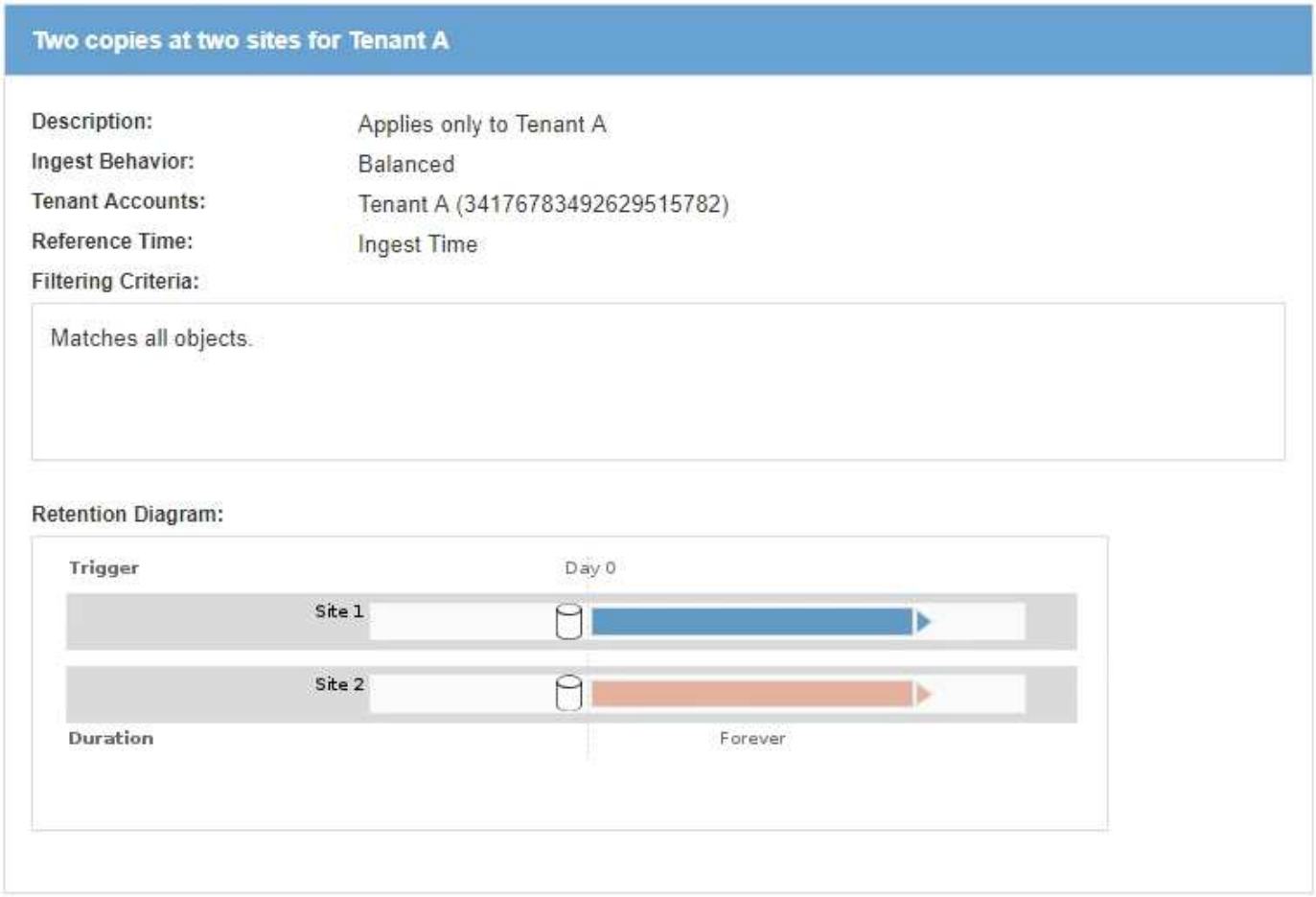
ルールの配置手順で指定されたオブジェクトコピーを作成します。

- * 配置手順 * ：ルールの配置手順によって、オブジェクトコピーの数、タイプ、および場所が定義されます。各ルールに一連の配置手順を含めることで、時間の経過に伴うオブジェクトコピーの数、タイプ、場所を変更することができます。1 つの配置の期間が終了すると、次の配置手順が次の ILM 評価で自動的に適用されます。
- * 取り込み動作 * ：ルールの取り込み動作は、 S3 または Swift クライアントがオブジェクトをグリッドに保存する際の処理を定義します。取り込み動作は、ルールの手順に従ってオブジェクトコピーがすぐに配置されるか、または中間コピーが作成されて配置手順があとから適用されるかを制御します。

ILM ルールの例

次の ILM ルールの例では、テナント A に属するオブジェクトの環境 を設定しますこれらのオブジェクトのレプリケートコピーを 2 つ作成し、各コピーを別々のサイトに格納します。この 2 つのコピーは「無期限」に保持されます。つまり、 StorageGRID はこれらのコピーを自動的に削除しません。これらのオブジェクトは、クライアントの削除要求によって削除されるか、バケットライフサイクルが終了するまで、 StorageGRID によって保持されます。

このルールでは、取り込み動作に Balanced オプションが使用されます。 2 つのサイトの配置手順は、テナント A がオブジェクトを StorageGRID に保存するとすぐに適用されます。ただし、両方の必要なコピーをただちに作成することはできません。たとえば、テナント A がオブジェクトを保存したときにサイト 2 に到達できない場合、 StorageGRID はサイト 1 のストレージノードに 2 つの中間コピーを作成します。サイト 2 が使用可能になると、 StorageGRID はそのサイトで必要なコピーを作成します。



関連情報

"取り込みのデータ保護オプション"

"ストレージプールとは"

"クラウドストレージプールとは"

"オブジェクトの格納方法（レプリケーションまたはイレイジャーコーディング）"

"ILM ルールのフィルタリングとは"

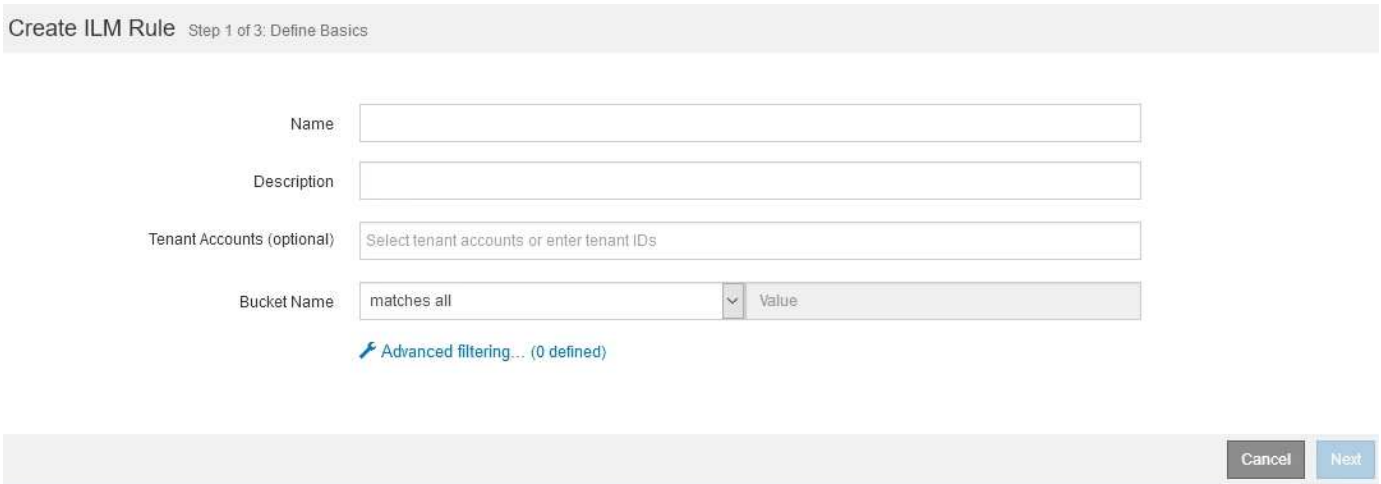
"ILM ルールの配置手順とは"

ILM ルールのフィルタリングとは

ILM ルールを作成する際には、フィルタを指定して環境 ルールを構成するオブジェクトを特定します。

最も単純なケースは、ルールでフィルタを使用しない場合です。環境 のすべてのオブジェクトでフィルタを使用しないルールがある場合は、 ILM ポリシーの最後の（デフォルト）ルールである必要があります。デフォルトルールは、別のルールのフィルタに一致しないオブジェクトに対するストレージの手順を提供します。

基本フィルタを使用すると、大規模なオブジェクトグループに異なるルールを適用できます。Create ILM Rule ウィザードの Define Basics ページの基本フィルタを使用して、特定のテナントアカウント、特定の S3 バケットまたは Swift コンテナ、あるいはその両方にルールを適用できます。



これらの基本フィルタを使用すると、多数のオブジェクトに異なるルールを簡単に適用できます。たとえば、会社の財務記録は規制要件を満たすために保存し、マーケティング部門のデータは日々の業務を円滑に進めるために保存しなければならない場合があります。部門ごとに別々のテナントアカウントを作成するか、またはデータを部門ごとに別々の S3 バケットに分離したあとで、すべての財務記録を環境 で処理するルールを 1 つ作成し、環境 ですべてのマーケティングデータを処理するもう 1 つのルールを作成することができます。

Create ILM Rule ウィザードの * Advanced Filtering * ページでは、詳細な制御を行うことができます。次のオブジェクトプロパティに基づいてオブジェクトを選択するフィルタを作成できます。

- 取り込み時間
- 最終アクセス時間
- オブジェクト名のすべてまたは一部（キー）
- S3 バケットのリージョン（場所の制約）

- オブジェクトのサイズ
- ユーザメタデータ
- S3 オブジェクトタグ

非常に特定の条件でオブジェクトをフィルタリングできます。たとえば、病院の画像診断部門が保管するオブジェクトは、 30 日以内に頻繁に使用され、その後はあまり使用されない可能性があります。一方、患者の通院情報を格納するオブジェクトは、医療ネットワークの本部請求部門にコピーする必要があります。オブジェクト名、サイズ、 S3 オブジェクトタグ、またはその他の関連条件に基づいて各タイプのオブジェクトを識別するフィルタを作成してから、それぞれのオブジェクトセットを適切に格納するルールを別々に作成できます。

必要に応じて、基本フィルタと高度なフィルタを 1 つのルールにまとめることもできます。たとえば、マーケティング部門では、サイズの大きな画像ファイルをベンダーレコードとは異なる方法で格納しなければならない場合があります。一方、人事部門では、特定の地域の人事レコードとポリシー情報を一元的に格納する必要があります。この場合は、テナントアカウントでフィルタリングするルールを作成して各部門からレコードを分離し、各ルールで高度なフィルタを使用してルール環境 に固有のタイプのオブジェクトを識別します。

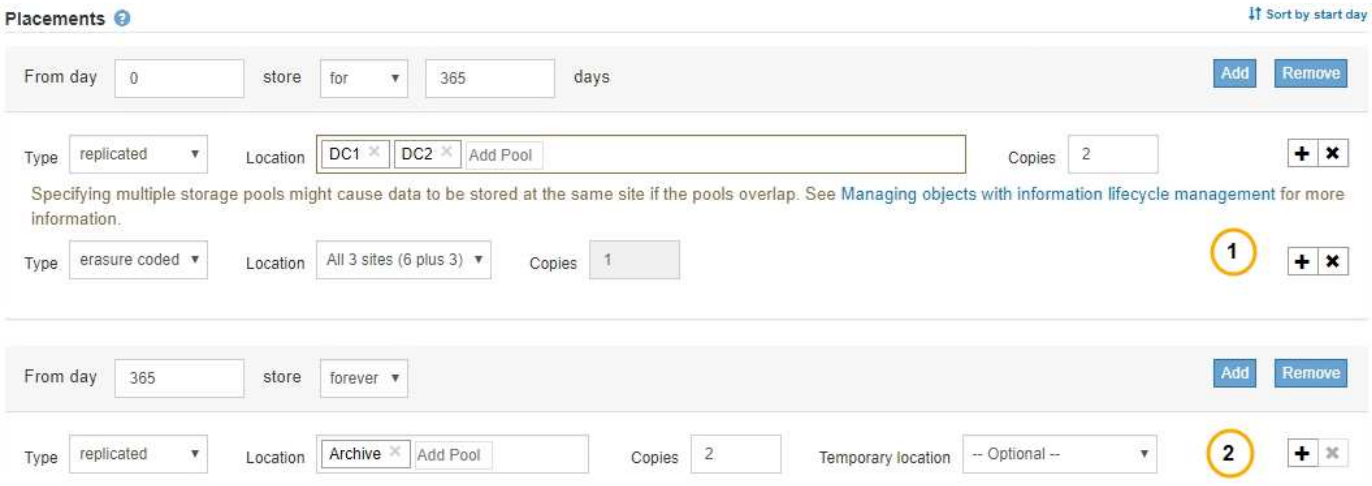
ILM ルールの配置手順とは

配置手順は、オブジェクトデータを格納する場所、タイミング、および方法を決定します。ILM ルールには 1 つ以上の配置手順を含めることができます。各配置手順環境 は一定期間です。

配置手順を作成するには、配置を適用するタイミング（期間）、作成するコピーのタイプ（レプリケートまたはイレイジャーコーディング）、およびコピーの格納先（1つ以上のストレージの場所）を指定します。単一のルール内で、1つの期間に複数の配置を指定でき、また複数の期間にそれぞれ違う配置手順を指定できます。

- 1つの期間に複数のオブジェクト配置を指定するには、プラス記号アイコンをクリックします ➕ をクリックして、期間に複数の行を追加します。
- 複数の期間にオブジェクト配置を指定するには、*追加*ボタンをクリックして次の期間を追加します。次に、期間内に 1 行以上の行を指定します。

この例は、 Create ILM Rule ウィザードの Define PI配置 ページを示しています。



1	1 つ目の配置手順には、 1 年目に 2 つの行があります。 1. 1 行目では、 2 つのデータセンターサイトに 2 つのレプリケートオブジェクトコピーが作成されます。 2. 2 行目には、 3 つのデータセンターサイトを使用して 6+3 のイレイジャーコーディングコピーが作成されます。
2	2 つ目の配置手順では、 1 年後にアーカイブコピーを 2 つ作成し、それらのコピーを無期限に保持します。

ルールに一連の配置手順を定義する場合は、少なくとも 1 つの配置手順が 0 日目に開始し、定義した期間の間にギャップがないことを確認する必要があります。 そして、最終的な配置手順は無期限またはオブジェクトコピーが不要になるまで継続されます。

ルールの各期間が終了すると、次の期間のコンテンツ配置手順が適用されます。新しいオブジェクトコピーが作成され、不要なコピーは削除されます。

ストレージグレード、ストレージプール、**EC**プロファイル、リージョンを作成する

StorageGRID システム用のILMルールを作成する前に、オブジェクトの格納場所を定義し、希望するコピーのタイプを決め、必要に応じてS3リージョンを設定する必要があります。

- "ストレージグレードを作成して割り当てます"
- "ストレージプールを設定しています"
- "クラウドストレージプールの使用"
- "イレイジャーコーディングプロファイルの設定"
- "リージョンの設定（オプション、S3のみ）"

ストレージグレードを作成して割り当てます

ストレージグレードは、ストレージノードで使用されているストレージのタイプを表します。サイトのすべてのノードではなく、特定のストレージノードに特定のオブジェクトを配置するように ILM ルールを設定する場合は、ストレージグレードを作成します。たとえば、 StorageGRID オールフラッシュストレージアプライアンスなどの最速のストレージノードに特定のオブジェクトを格納できます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

このタスクについて

複数のタイプのストレージを使用する場合は、各タイプを識別するストレージグレードを必要に応じて作成できます。ストレージグレードを作成すると、ストレージプールの構成時に特定のタイプのストレージノードを選択できるようになります。

ストレージグレードが重要でない場合（すべてのストレージノードが同じ場合など）は、この手順 をスキップし、ストレージプールの構成時にデフォルトのストレージグレードである All Storage Nodes を使用できます。

拡張で新しいストレージノードを追加すると、そのノードが「すべてのストレージノード」のデフォルトのストレージグレードに追加されます。その結果、次のようになります

- 「 All Storage Nodes 」グレードのストレージプールを使用する ILM ルールの場合、拡張の完了後すぐに新しいノードを使用できます。
- カスタムのストレージグレードを含むストレージプールを使用する ILM ルールの場合、以下に示すようにカスタムのストレージグレードをノードに手動で割り当てるまで新しいノードは使用されません。

> ストレージグレードは必要以上に作成しないでください。たとえば、ストレージノードごとにストレージグレードを作成するのではなく、各ストレージグレードを複数のノードに割り当てます。ストレージグレードを 1 つのノードにしか割り当てていない場合、そのノードが使用できなくなると原因 のバックログが発生する可能性があります。

手順

1. 「* ILM > Storage Grades *」を選択します。
2. ストレージグレードを作成します。

   a. 定義する必要があるストレージグレードごとに、*挿入*をクリックします アイコン"] をクリックして行を追加し、ストレージグレードのラベルを入力します。

      デフォルトのストレージグレードは変更できません。StorageGRID システムの拡張時に追加される新しいストレージノード用に予約されています。

Storage Grades

Updated: 2017-05-26 11:22:39 MDT

Storage Grade Definitions

Storage Grade	Label	Actions
0	Default	
1	disk	

Storage Grades

LDR	Storage Grade	Actions
Data Center 1/DC1-S1/LDR	Default	
Data Center 1/DC1-S2/LDR	Default	
Data Center 1/DC1-S3/LDR	Default	
Data Center 2/DC2-S1/LDR	Default	
Data Center 2/DC2-S2/LDR	Default	
Data Center 2/DC2-S3/LDR	Default	
Data Center 3/DC3-S1/LDR	Default	
Data Center 3/DC3-S2/LDR	Default	
Data Center 3/DC3-S3/LDR	Default	

Apply Changes

a. 既存のストレージグレードを編集するには、*編集*をクリックします をクリックし、必要に応じてラベルを変更します。

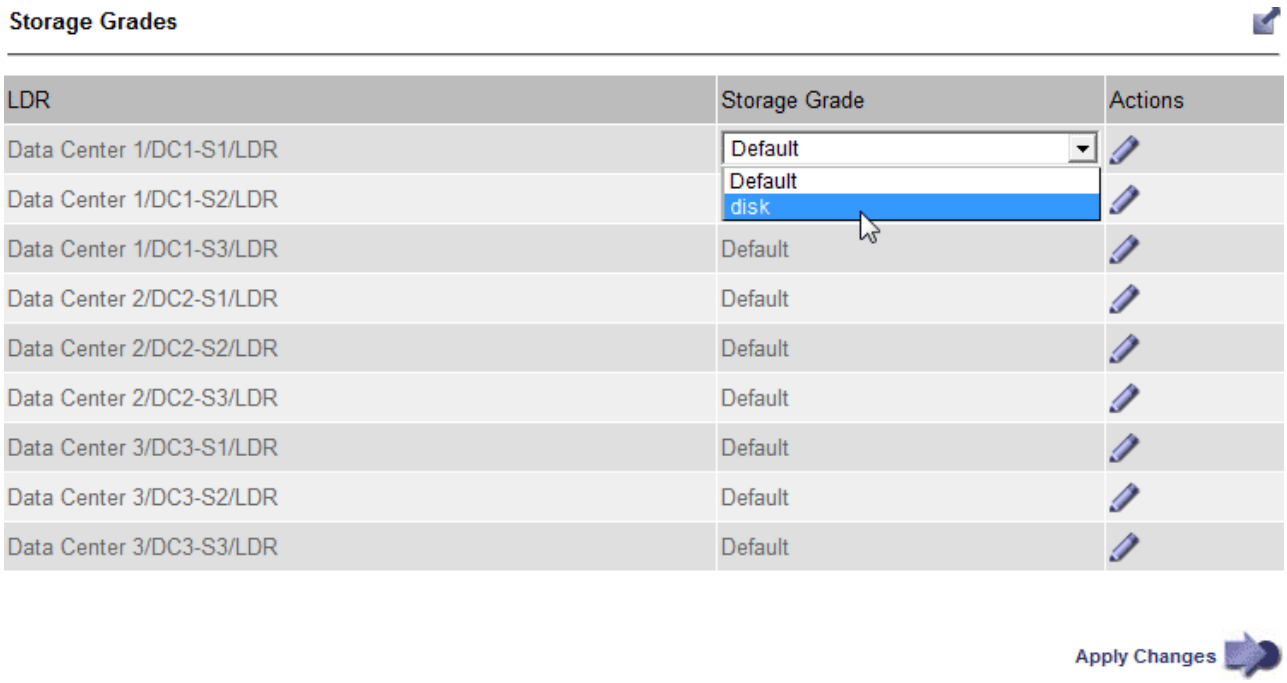
ストレージグレードを削除することはできません。

b. [変更の適用 *] をクリックします。

これで、ストレージグレードをストレージノードに割り当てることができます。

3. ストレージノードにストレージグレードを割り当てます。

a. 各ストレージノードのLDRサービスで、* Edit *をクリックします をクリックし、リストからストレージグレードを選択します。



特定のストレージノードにストレージグレードを割り当てることができるのは 1 回だけです。障害からリカバリしたストレージノードでは、以前に割り当てられていたストレージグレードが維持されます。ILM ポリシーをアクティブ化したあとに、この割り当てを変更しないでください。割り当てが変更されると、新しいストレージグレードに基づいてデータが格納されます。

a. [変更の適用 *] をクリックします。

ストレージプールを設定しています

ILMルールを定義する際には、ストレージプールを使用してオブジェクトの格納場所を指定します。ストレージプールを作成する前に、ストレージプールに関するガイドラインを確認してください。

- "ストレージプールとは"
- "ストレージプールの作成に関するガイドラインを次に示します"
- "複数のストレージプールを使用したサイト間レプリケーション"
- "一時的な場所としてのストレージプールの使用（廃止）"
- "ストレージプールを作成します"
- "ストレージプールの詳細を表示しています"
- "ストレージプールを編集する"
- "ストレージプールを削除しています"

ストレージプールとは

ストレージプールは、ストレージノードまたはアーカイブノードを論理的にグループ化したものです。ストレージプールの設定で、 StorageGRID システムがオブジェクトデー

タを格納する場所と、使用するストレージのタイプを決定します。

ストレージプールには 2 つの属性があります。

- * ストレージグレード * ：ストレージノードの場合は、バッキングストレージの相対的なパフォーマンス。
- * サイト * ：オブジェクトを格納するデータセンター。

ストレージプールは、オブジェクトデータの格納先を決定するために ILM ルールで使用されます。レプリケーションのための ILM ルールを設定する際は、ストレージノードまたはアーカイブノードを含むストレージプールを 1 つ以上選択します。イレイジャーコーディングプロファイルを作成する際は、ストレージノードを含むストレージプールを選択します。

ストレージプールの作成に関するガイドラインを次に示します

ストレージプールを設定して使用する場合は、次のガイドラインに従ってください。

すべてのストレージプールのガイドライン

- StorageGRID には、デフォルトのストレージプールとすべてのストレージノードが含まれ、デフォルトサイト、すべてのサイト、およびデフォルトのストレージグレードであるすべてのストレージノードが使用されます。新しいデータセンターサイトを追加するたびに、 All Storage Nodes ストレージプールが自動的に更新されます。

> ⓘ All Storage Nodes ストレージプールまたはすべてのサイトサイトサイトは、拡張に追加する新しいサイトが自動的に更新されて追加されるため、推奨されません。これは動作ではない可能性があります。All Storage Nodes ストレージプールまたはデフォルトサイトを使用する前に、レプリケートコピーとイレイジャーコーディングコピーに関するガイドラインをよく確認してください。

- ストレージプールの設定は可能なかぎりシンプルにします。必要以上に多くのストレージプールを作成しないでください。
- できるだけ多くのノードを含むストレージプールを作成します。各ストレージプールには 2 つ以上のノードを含める必要があります。ノードが不十分なストレージプールでは、ノードが使用できなくなった場合に原因 ILM バックログが発生する可能性があります。
- 重複する（ 1 つ以上の同じノードを含む）ストレージプールを作成または使用することは避けてください。ストレージプールが重複していると、オブジェクトデータの複数のコピーが同じノードに保存される可能性があります。

レプリケートコピーに使用するストレージプールのガイドライン

- サイトごとに異なるストレージプールを作成します。次に、ルールごとに配置手順でサイト固有のストレージプールを 1 つ以上指定します。各サイトにストレージプールを使用すると、レプリケートされたオブジェクトコピーが想定どおりに配置されるようになります（たとえば、サイト障害から保護するために、各サイトのすべてのオブジェクトのコピーが 1 つずつ）。
- 拡張でサイトを追加する場合は、新しいサイト用の新しいストレージプールを作成します。次に、新しいサイトに格納するオブジェクトを制御するために ILM ルールを更新します。
- 通常は、デフォルトのストレージプール、すべてのストレージノード、またはデフォルトサイトであるすべてのサイトを含むストレージプールを使用しないでください。

イレイジャーコーディングされたコピーに使用するストレージプールのガイドラインを次に示します

- イレイジャーコーディングデータ用にアーカイブノードを使用することはできません。
- ストレージプールに含まれるストレージノードとサイトの数によって、使用できるイレイジャーコーディングスキームが決まります。
- ストレージプールにサイトが 2 つしかない場合、そのストレージプールをイレイジャーコーディングに使用することはできません。2 つのサイトを含むストレージプールではイレイジャーコーディングスキームを使用できません。
- 通常は、デフォルトのストレージプール、すべてのストレージノード、またはデフォルトサイトを含むすべてのサイトのいずれかのイレイジャーコーディングプロファイル内のストレージプールを使用しないでください。

> グリッドにサイトが 1 つしかない場合、イレイジャーコーディングプロファイルに「すべてのストレージノード」ストレージプールまたは「すべてのサイト」デフォルトサイトを使用することはできません。これにより、 2 つ目のサイトが追加された場合にイレイジャーコーディングプロファイルが無効になるのを防ぐことができます。

- 高スループットが必要な場合、サイト間のネットワークレイテンシが 100 ミリ秒を超える状況では、複数のサイトを含むストレージプールを作成することは推奨されません。レイテンシが上昇すると TCP ネットワークのスループットが低下するため、 StorageGRID がオブジェクトフラグメントを作成、配置、読み出す速度は大幅に低下します。スループットの低下は、オブジェクトの取り込みと読み出しの達成可能な最大速度に影響する（ Strict または Balanced が取り込み動作として選択されている場合）か、 ILM キューのバックログが発生する可能性があります（ Dual Commit が取り込み動作として選択されている場合）。
- 可能であれば、選択するイレイジャーコーディングスキームに必要な最小数よりも多くのストレージノードをストレージプールに含めてください。たとえば、 6+3 のイレイジャーコーディングスキームを使用する場合は、 9 個以上のストレージノードが必要です。ただし、サイトごとに少なくとも 1 つのストレージノードを追加することを推奨します。
- ストレージノードはサイト間にできるだけ均等に分散します。たとえば、 6+3 のイレイジャーコーディングスキームをサポートするには、 3 つのサイトにそれぞれ 1 つ以上のストレージノードを含むストレージプールを設定します。

アーカイブされたコピーに使用するストレージプールのガイドラインを次に示します

- ストレージノードとアーカイブノードの両方を含むストレージプールは作成できません。アーカイブされたコピーには、アーカイブノードのみを含むストレージプールが必要です。
- アーカイブノードが含まれたストレージプールを使用する場合は、ストレージノードが含まれたストレージプール上に、 1 つ以上のレプリケートコピーまたはイレイジャーコーディングコピーを保持する必要もあります。
- グローバルな S3 オブジェクトロック設定が有効になっていて準拠 ILM ルールを作成する場合は、アーカイブノードが含まれたストレージプールを使用できません。S3 オブジェクトロックを使用してオブジェクトを管理する手順を参照してください。
- アーカイブノードの Target Type が「 Cloud Tiering - Simple Storage Service （ S3 ）」の場合、そのアーカイブノードは自身のストレージプールに含まれている必要があります。StorageGRID の管理手順を参照してください。

関連情報

"レプリケーションとは"

"イレイジャーコーディングとは"

"イレイジャーコーディングスキームとは"

"複数のストレージプールを使用したサイト間レプリケーション"

"一時的な場所としてのストレージプールの使用（廃止）"

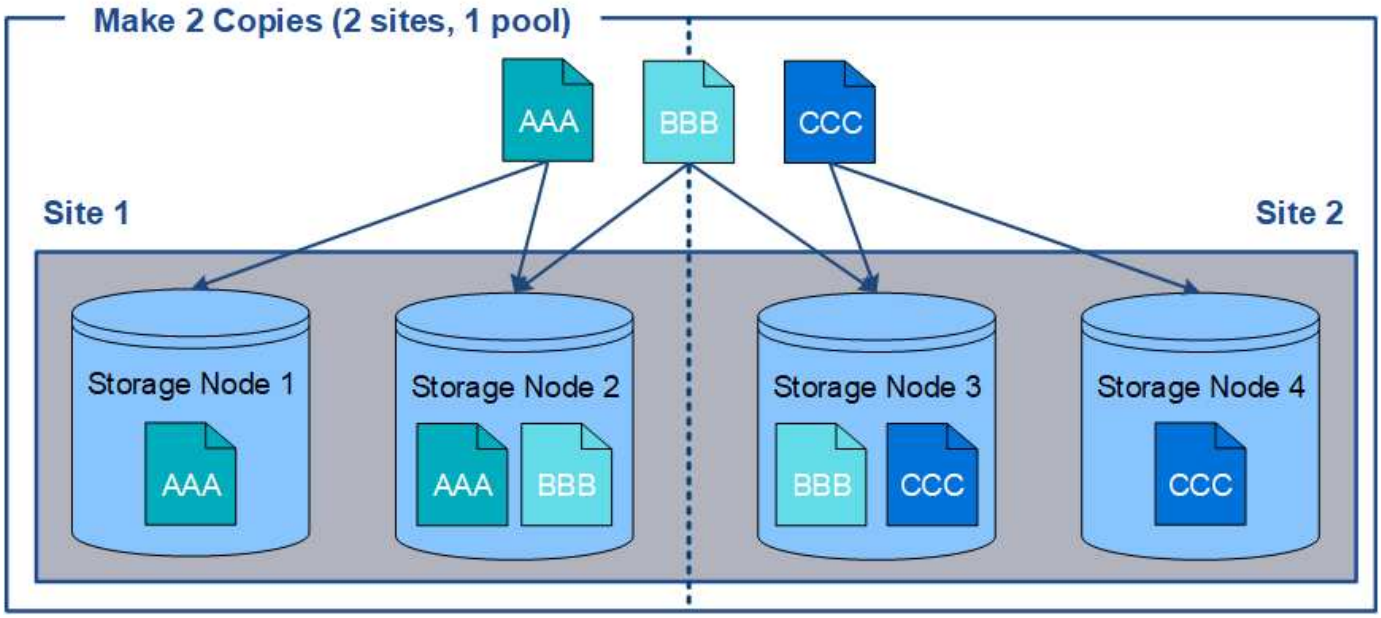
"S3オブジェクトロックでオブジェクトを管理する"

"StorageGRID の管理"

複数のストレージプールを使用したサイト間レプリケーション

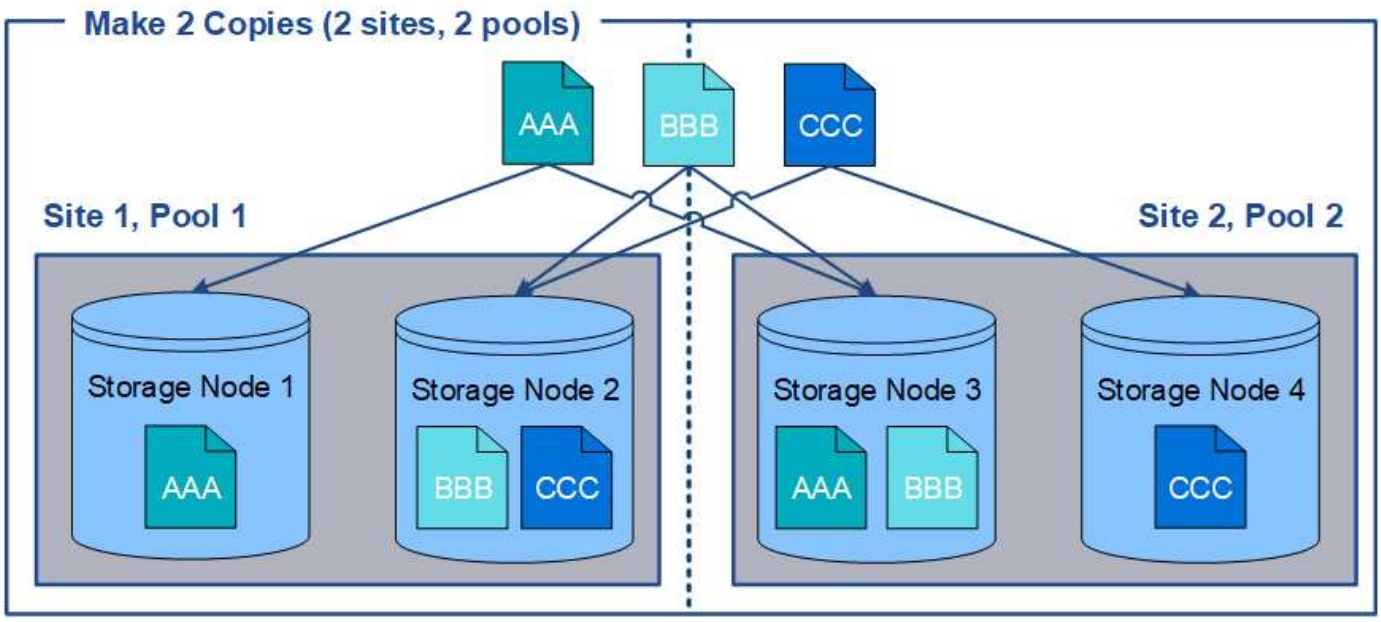
StorageGRID 環境に複数のサイトが含まれている場合は、各サイトにストレージプールを 1 つずつ作成し、ルールの配置手順に両方のストレージプールを指定することで、サイト障害から保護できます。たとえば、 2 つのレプリケートコピーを作成する ILM ルールを設定して、 2 つのサイトのストレージプールを指定すると、各オブジェクトのコピーが各サイトに 1 つずつ配置されます。2 つのコピーを作成するルールを設定して 3 つのストレージプールを指定すると、 2 つのコピーが別々のサイトに格納される際、ストレージプール間のディスク使用量のバランスを保つようにコピーが分散されます。

次の例は、 ILM ルールによって 2 つのサイトのストレージノードを含む単一のストレージプールにレプリケートオブジェクトコピーが配置された場合にどうなるかを示しています。レプリケートコピーがストレージプール内の使用可能な任意のノードに配置されるため、一部のオブジェクトのすべてのコピーが 1 つのサイト内にのみ配置される可能性があります。この例では、システムはオブジェクト AAA の 2 つのコピーをサイト 1 の別々のストレージノードに、オブジェクト CCC の 2 つのコピーをサイト 2 の別々のストレージノードに格納しています。いずれかのサイトで障害が発生したりアクセスできなくなった場合、保護されるのはオブジェクト BBB だけです。



一方、この例は、複数のストレージプールを使用した場合のオブジェクトの格納方法を示しています。この例の ILM ルールは、各オブジェクトのレプリケートコピーを 2 つ作成して 2 つのストレージプールに分散するように指定されています。各ストレージプールには一方のサイトのすべてのストレージノードが含まれていま

す。各オブジェクトのコピーは各サイトに格納されるため、オブジェクトデータはサイトの障害やサイトへのアクセス障害から保護されます。



複数のストレージプールを使用する場合は、次の点に注意してください。

- n 個のコピーを作成する場合は、 n 個以上のストレージプールを追加する必要があります。たとえば、 3 つのコピーを作成するようにルールが設定されている場合は、ストレージプールを 3 つ以上指定する必要があります。
- コピーの数がストレージプールの数と同じ場合は、オブジェクトのコピーが 1 つずつ各ストレージプールに格納されます。
- コピーの数がストレージプールの数より少ない場合、プール間のディスク使用量のバランスを維持し、複数のコピーが同じストレージプールに格納されないようにコピーが分散されます。
- ストレージプールが重複している（同じストレージノードを含んでいる）場合は、オブジェクトのすべてのコピーが 1 つのサイトにのみ保存される可能性があります。選択したストレージプールに同じストレージノードが含まれていないことを確認する必要があります。

一時的な場所としてのストレージプールの使用（廃止）

ストレージプールを 1 つ含むオブジェクトの配置を使用して ILM ルールを作成する場合は、一時的な場所として使用する 2 つ目のストレージプールを指定するように求められます。

一時的な場所は廃止されており、今後のリリースで削除される予定です。ストレージプールは、新しい ILM ルールの一時的な場所として選択しないでください。

Strict 取り込み動作を選択した場合（ Create ILM Rule ウィザードのステップ 3 ）、一時的な場所は無視されます。

関連情報

"取り込みのデータ保護オプション"

ストレージプールを作成することで、 StorageGRID システムがオブジェクトデータを格納する場所と、使用するストレージのタイプを決定します。各ストレージプールには、サイトとストレージグレードがそれぞれ 1 つ以上含まれています。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。
- ストレージプールの作成に関するガイドラインを確認しておく必要があります。

このタスクについて

ストレージプールは、オブジェクトデータの格納場所を決定します。必要なストレージプールの数は、グリッド内のサイトの数と、レプリケートコピーまたはイレイジャーコーディングコピーのタイプによって異なります。

- レプリケーションおよび単一サイトのイレイジャーコーディングの場合は、サイトごとにストレージプールを作成します。たとえば、レプリケートオブジェクトコピーを 3 つのサイトに格納する場合は、ストレージプールを 3 つ作成します。
- 3 つ以上のサイトでイレイジャーコーディングする場合は、サイトごとに 1 つのエントリを含むストレージプールを 1 つ作成します。たとえば、 3 つのサイトにまたがるオブジェクトをイレイジャーコーディングする場合は、ストレージプールを 1 つ作成します。プラスアイコンを選択します ➕ アイコン"] をクリックして、各サイトのエントリを追加します。

> ⓘ イレイジャーコーディングプロファイルで使用されるストレージプールには、デフォルトの All Sites サイトを含めないでください。代わりに、イレイジャーコーディングデータを格納するサイトごとにストレージプールにエントリを追加します。を参照してください この手順を実行します たとえば、のように指定します。

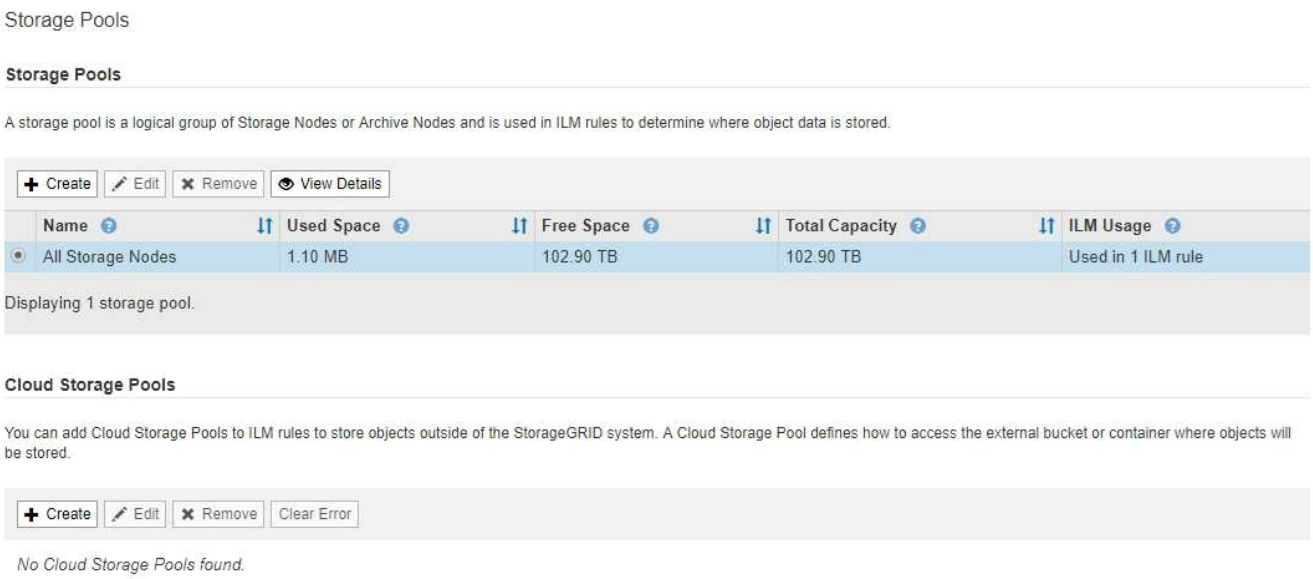
- ストレージグレードが複数ある場合は、 1 つのサイトに異なるストレージグレードを含むストレージプールを作成しないでください。

  "ストレージプールの作成に関するガイドラインを次に示します"

手順

1. ILM > Storage Pools *を選択します。

   Storage Pools （ストレージプール）ページが表示され、定義済みのすべてのストレージプールがリストされます。

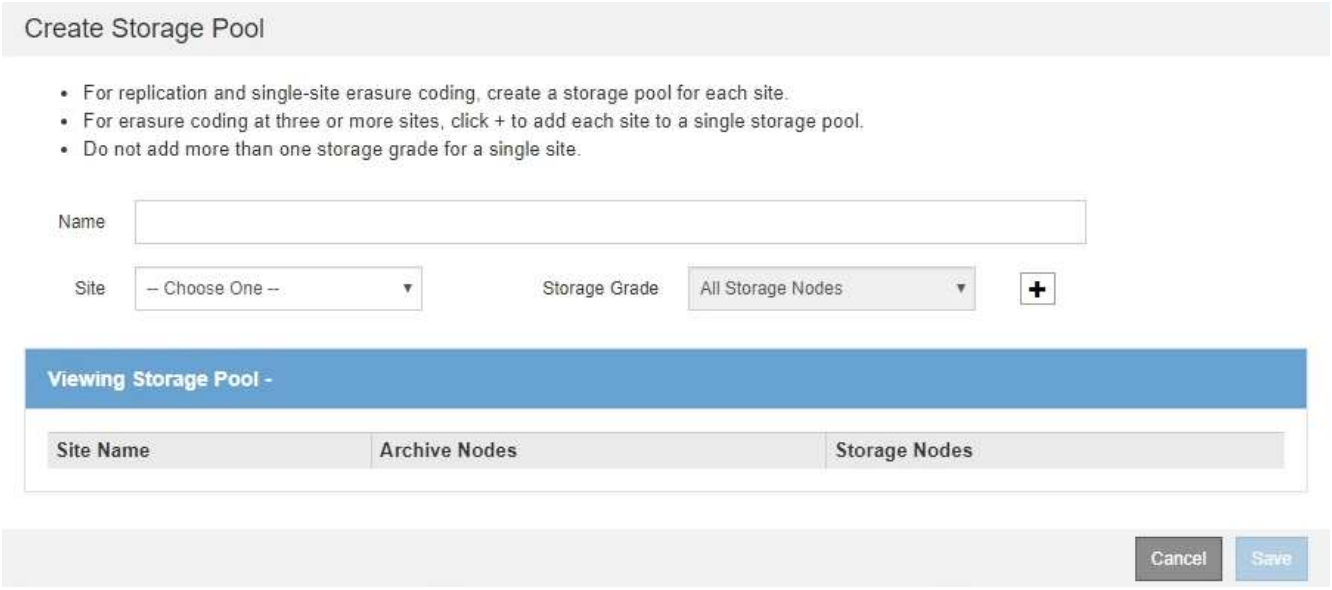


リストには、システムデフォルトのストレージプール、システムデフォルトサイトのすべてのサイトを使用するすべてのストレージノード、およびデフォルトのストレージグレードであるすべてのストレージノードが含まれます。

> All Storage Nodes ストレージプールは、新しいデータセンターサイトを追加するたびに自動的に更新されるため、 ILM ルールでこのストレージプールを使用することは推奨されません。

2. 新しいストレージプールを作成するには、「 * 作成」を選択します。

   Create Storage Pool （ストレージプールの作成）ダイアログボックスが表示されます。



3. ストレージプールの一意の名前を入力します。

   イレイジャーコーディングプロファイルと ILM ルールを設定するときに識別しやすい名前を使用してください。

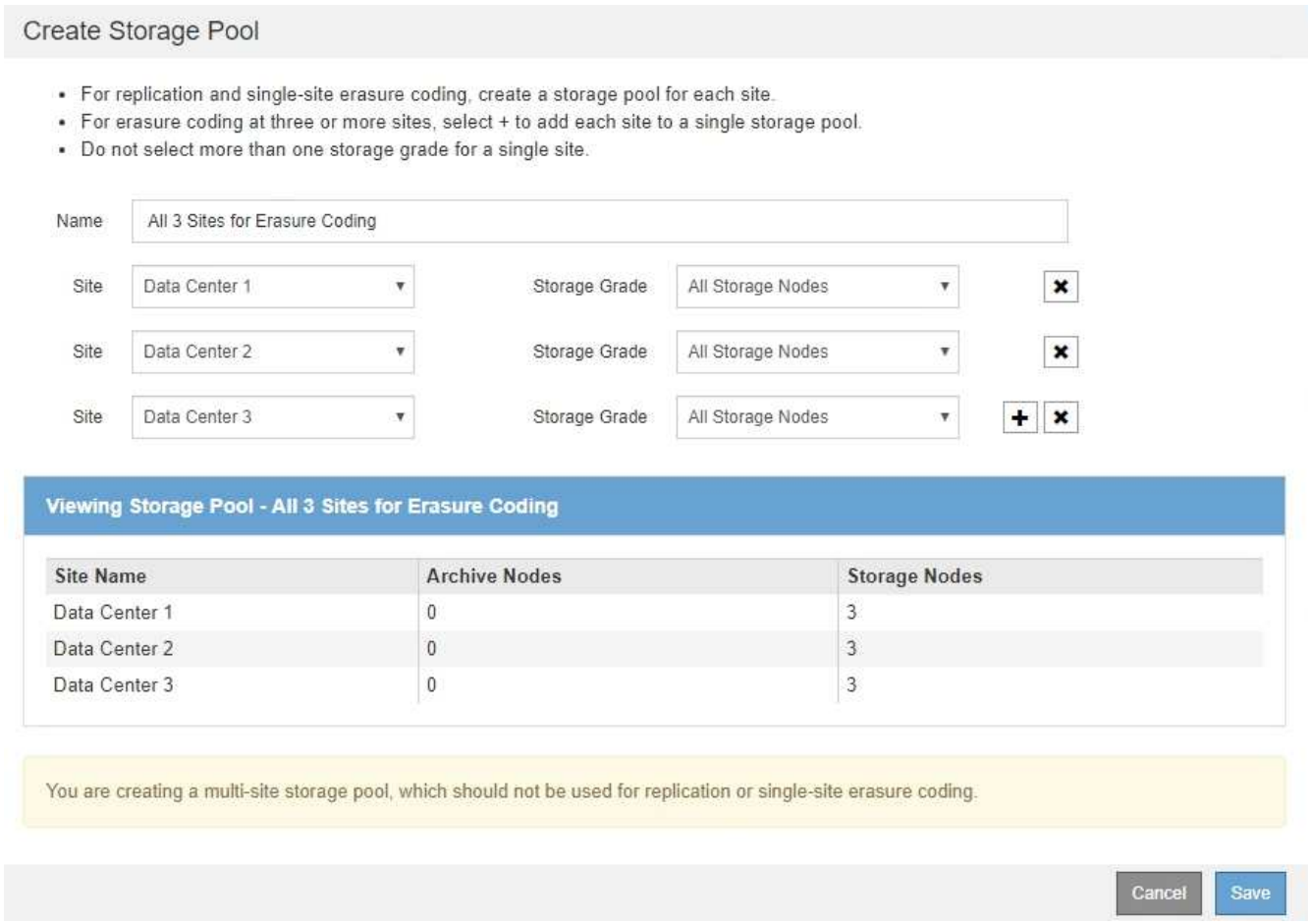
4. [*Site *] ドロップダウン・リストから ' このストレージ・プールのサイトを選択します

   サイトを選択すると、表内のストレージノードとアーカイブノードの数が自動的に更新されます。

5. ストレージグレード * ドロップダウンリストから、 ILM ルールでこのストレージプールを使用する場合に使用するストレージのタイプを選択します。

   デフォルトの All Storage Nodes ストレージグレードには、選択したサイトのすべてのストレージノードが含まれます。Default Archive Nodes ストレージグレードには、選択したサイトのすべてのアーカイブノードが含まれます。グリッド内のストレージノード用にストレージグレードを追加で作成している場合、そのグレードもドロップダウンに表示されます。

6. [[entries]]] マルチサイトイレイジャーコーディングプロファイルでストレージプールを使用する場合は、を選択します ➕ アイコン"] をクリックして、各サイトのエントリをストレージプールに追加します。



> 重複するエントリを作成したり、 * アーカイブノード * ストレージグレードとストレージノードを含むストレージグレードの両方を含むストレージプールを作成したりすることはできません。
>
> サイトに複数のエントリを追加しても、ストレージグレードが異なる場合は警告が表示されます。

   エントリを削除するには、を選択します ✖。

7. 選択に問題がなければ、 * 保存 * を選択します。

新しいストレージプールがリストに追加されます。

関連情報

"ストレージプールの作成に関するガイドラインを次に示します"

ストレージプールの詳細を表示しています

ストレージプールの詳細を表示して、ストレージプールの使用場所を確認したり、含まれているノードやストレージグレードを確認したりできます。

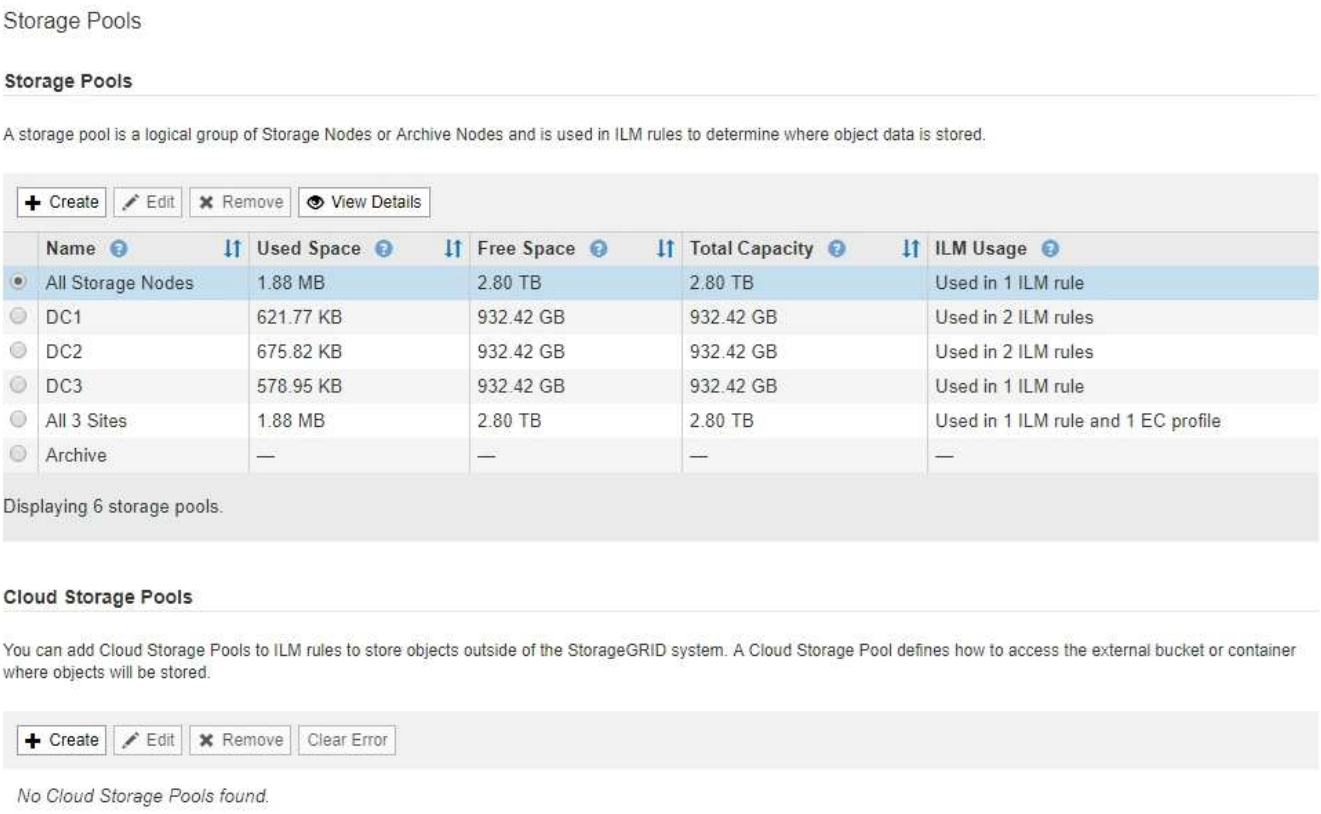
必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

手順

1. ILM > Storage Pools *を選択します。

   Storage Pools （ストレージプール）ページが表示されます。このページには、定義済みのストレージプールがすべて表示されます。



   この表には、ストレージノードを含む各ストレージプールに関する次の情報が含まれています。

   - * Name * ：ストレージプールの一意の表示名。
   - * Used Space * ：ストレージプールにオブジェクトを格納するために現在使用されているスペースの量。

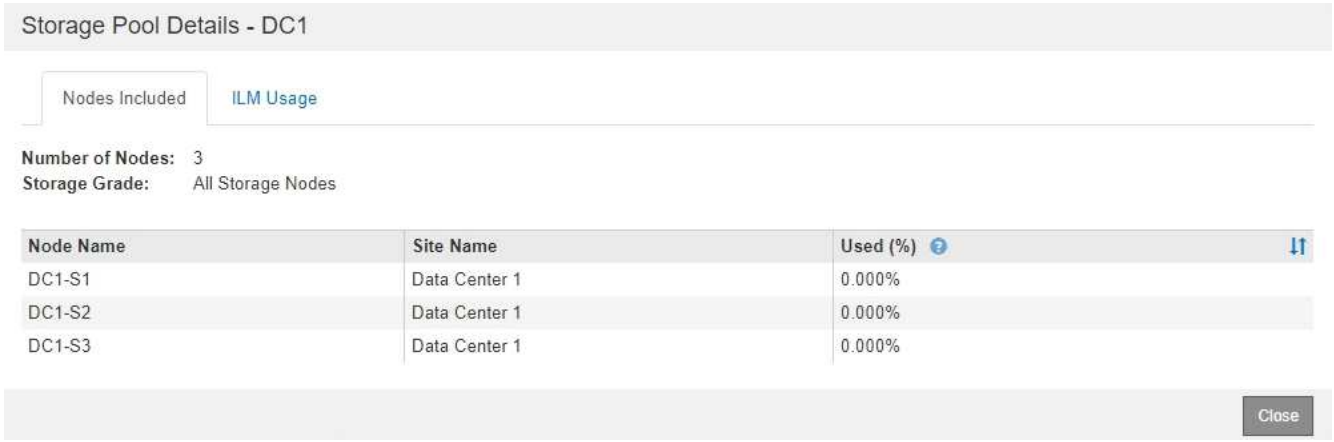
- * Free Space * ：ストレージプールにオブジェクトを格納するために使用可能な残りのスペース。
- * Total Capacity * ：ストレージプールのサイズ。ストレージプール内のすべてのノードのオブジェクトデータに使用可能なスペースの合計に相当します。
- * ILM Usage * ：ストレージプールの現在の使用状況。ストレージプールは、使用されていない場合や、 1 つ以上の ILM ルール、イレイジャーコーディングプロファイル、またはその両方で使用されている場合があります。

> 使用中のストレージプールは削除できません。

2. 特定のストレージプールの詳細を表示するには、そのラジオボタンを選択し、「 * 詳細を表示 * 」を選択します。

   Storage Pool Details モーダルが表示されます。

3. 「 Nodes included * 」タブを表示して、ストレージプールに含まれるストレージノードまたはアーカイブノードについて確認します。



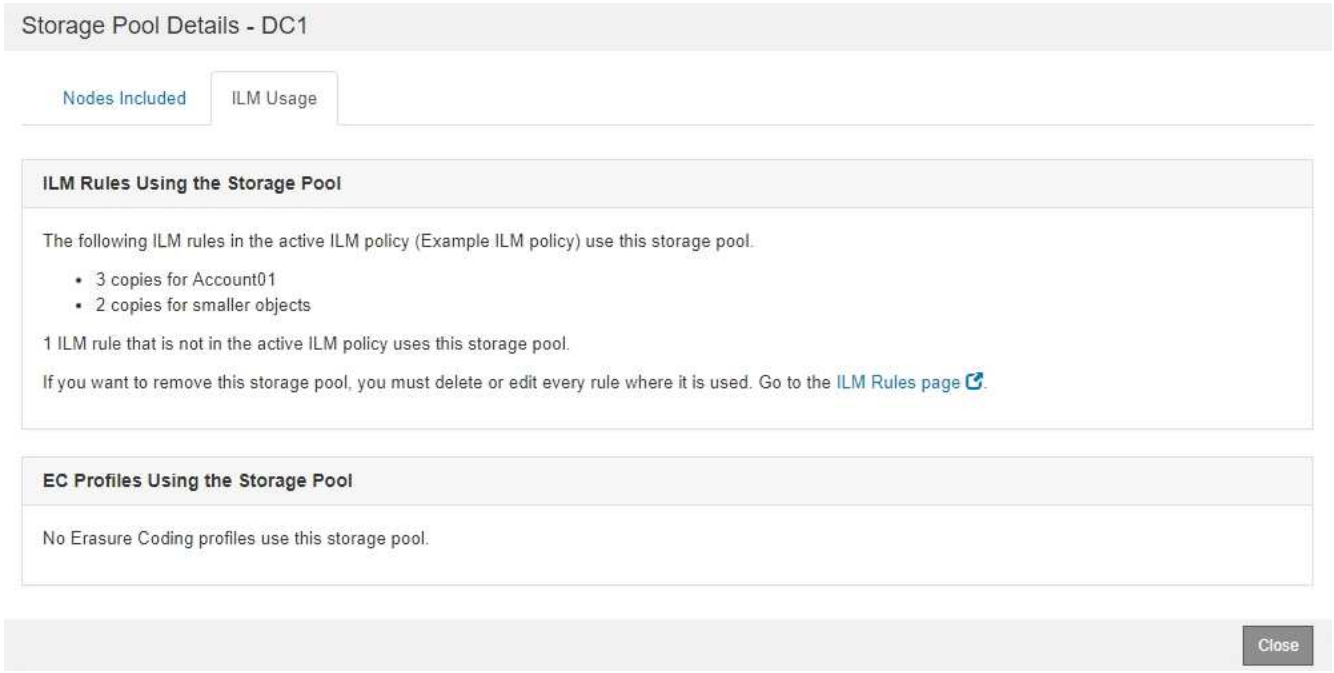
   この表には、ノードごとに次の情報が記載されています。

   - ノード名
   - サイト名
   - 使用済み（ % ）：ストレージノードの場合、オブジェクトデータに使用されている合計使用可能スペースの割合。この値にはオブジェクトメタデータは含まれません。

> 各ストレージノードのStorage Used - Object Dataチャートにも同じ使用済み（%）値が表示されます（* Nodes ***>*Storage Node***>* Storage *）。

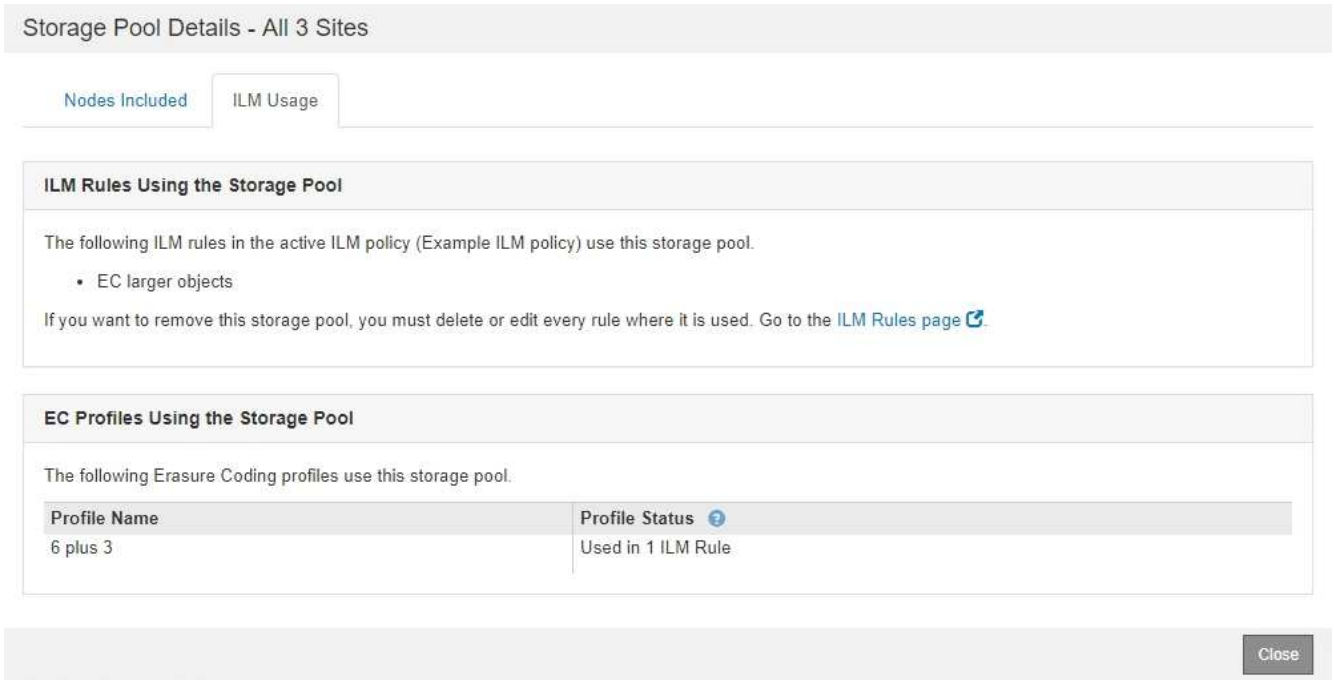
4. 「 * ILM Usage * 」タブを選択して、ストレージプールが現在 ILM ルールやイレイジャーコーディングプロファイルで使用されているかどうかを確認します。

   この例では、 DC1 ストレージプールは、アクティブな ILM ポリシーに含まれる 2 つのルールとアクティブなポリシーに含まれない 1 つのルールという 3 つの ILM ルールで使用されます。



ILM ルールで使用されているストレージプールは削除できません。

この例では、 All 3 Sites ストレージプールがイレイジャーコーディングプロファイルで使用されています。そのイレイジャーコーディングプロファイルは、アクティブな ILM ポリシー内の 1 つの ILM ルールによって使用されます。



イレイジャーコーディングプロファイルで使用されているストレージプールは削除できません。

5. 必要に応じて、 * ILM Rules ページ * に移動し、ストレージプールを使用するルールの確認と管理を行います。

ILM ルールの操作手順を参照してください。

6. ストレージプールの詳細の表示が完了したら、「 * 閉じる * 」を選択します。

関連情報

"ILMルールおよびILMポリシーの操作"

ストレージプールを編集する

ストレージプールを編集して、名前を変更したり、サイトやストレージグレードを更新したりできます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。
- ストレージプールの作成に関するガイドラインを確認しておく必要があります。
- アクティブなILMポリシーのルールで使用されているストレージプールを編集する場合は、変更がオブジェクトデータの配置にどのように影響するかを考慮する必要があります。

このタスクについて

アクティブな ILM ポリシーで使用されているストレージプールに新しいストレージグレードを追加する場合は、新しいストレージグレードのストレージノードが自動的には使用されないことに注意してください。StorageGRID で新しいストレージグレードを強制的に使用するには、編集したストレージプールを保存したあとに新しい ILM ポリシーをアクティブ化する必要があります。

手順

1. ILM > Storage Pools *を選択します。

   Storage Pools （ストレージプール）ページが表示されます。

2. 編集するストレージプールのラジオボタンを選択します。

   All Storage Nodes ストレージプールは編集できません。

3. 「 * 編集 * 」を選択します。
4. 必要に応じて、ストレージプール名を変更します。
5. 必要に応じて、他のサイトとストレージグレードを選択します。

   ストレージプール原因 がイレイジャーコーディングプロファイルで使用されている場合や、イレイジャーコーディングスキームを無効に変更する場合、サイトまたはストレージグレードを変更することはできません。たとえば、イレイジャーコーディングプロファイルで使用されているストレージプールにサイトが 1 つしかないストレージグレードが含まれている場合、サイトが 2 つのストレージグレードを使用することはできません。これは、変更によってイレイジャーコーディングスキームが無効になるためです。

6. [保存（ Save ）] を選択します。

完了後

アクティブな ILM ポリシーで使用されているストレージプールに新しいストレージグレードを追加した場合は、新しい ILM ポリシーをアクティブ化して StorageGRID に新しいストレージグレードを強制的に使用させます。たとえば、既存の ILM ポリシーのクローンを作成し、そのクローンをアクティブ化します。

ストレージプールを削除しています

使用されていないストレージプールは削除できます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

手順

1. ILM > Storage Pools *を選択します。

   Storage Pools （ストレージプール）ページが表示されます。

2. テーブルの ILM Usage 列を参照して、ストレージプールを削除できるかどうかを確認します。

   ストレージプールが ILM ルールまたはイレイジャーコーディングプロファイルで使用されている場合、ストレージプールを削除することはできません。必要に応じて、 * View Details * > * ILM Usage * の順に選択して、ストレージプールの使用場所を決定します。

3. 削除するストレージプールが使用されていない場合は、ラジオボタンを選択します。
4. 「 * 削除」を選択します。
5. 「 * OK 」を選択します。

クラウドストレージプールの使用

クラウドストレージプールを使用して、StorageGRID オブジェクトをS3 GlacierやMicrosoft Azure BLOBストレージなどの外部ストレージに移動できます。オブジェクトをグリッドの外部に移動すると、低コストのストレージ階層を活用した長期間のアーカイブが可能になります。

- "クラウドストレージプールとは"
- "クラウドストレージプールオブジェクトのライフサイクル"
- "クラウドストレージプールを使用する状況"
- "クラウドストレージプールに関する考慮事項"
- "クラウドストレージプールと CloudMirror レプリケーションを比較しています"
- "クラウドストレージプールの作成"
- "クラウドストレージプールの編集"
- "クラウドストレージプールの削除"
- "クラウドストレージプールのトラブルシューティング"

クラウドストレージプールとは

クラウドストレージプールでは、 ILM を使用して StorageGRID システムの外部にオブジェクトデータを移動できます。たとえば、 Amazon S3 Glacier 、 S3 Glacier Deep Archive 、 Microsoft Azure Blob Storage のアーカイブアクセス階層など、アクセス頻度の低いオブジェクトを低コストのクラウドストレージに移動できます。または、 StorageGRID オブジェクトのクラウドバックアップを保持して、ディザスタリカバリを強化することもできます。

ILM から見た場合、クラウドストレージプールはストレージプールに似ています。どちらの場所にオブジェクトを格納する場合も、 ILM ルールの配置手順の作成時にプールを選択します。ただし、ストレージプールは StorageGRID システム内のストレージノードまたはアーカイブノードで構成されますが、クラウドストレージプールは外部のバケット（ S3 ）またはコンテナ（ Azure BLOB ストレージ）で構成されます。

次の表に、ストレージプールとクラウドストレージプールの比較と、類似点と相違点を示します。

	ストレージプール	クラウドストレージプール
作成方法	Grid Managerで* ILM *>*ストレージプール*オプションを使用する。 ストレージプールを作成する前に、ストレージグレードをセットアップする必要があります。	Grid Managerで* ILM *>*ストレージプール*オプションを使用する。 クラウドストレージプールを作成する前に、外部のバケットまたはコンテナをセットアップする必要があります。
作成できるプール数	無制限。	最大 10 個。

	ストレージプール	クラウドストレージプール
オブジェクトの格納先	StorageGRID 内の 1 つ以上のストレージノードまたはアーカイブノード。	StorageGRID システムの外部にある Amazon S3 バケットまたは Azure BLOB ストレージコンテナ。 クラウドストレージプールが Amazon S3 バケットの場合： • 必要に応じて、 Amazon S3 Glacier や S3 Glacier Deep Archive などの低コストの長期保存用ストレージにオブジェクトを移行するようにバケットライフサイクルを設定できます。外部ストレージシステムが Glacier ストレージクラスと S3 POST Object restore API をサポートしている必要があります。 • AWS Commercial クラウド サービス（ C2S ）で使用するクラウドストレージプールを作成できます。 C2S は AWS Secret Region をサポートします。 クラウドストレージプールが Azure BLOB ストレージコンテナの場合、 StorageGRID はオブジェクトをアーカイブ層に移行します。 • 注：一般に、クラウドストレージプールに使用するコンテナには Azure Blob Storage のライフサイクル管理を設定しないでください。クラウドストレージプール内のオブジェクトに対する POST Object restore 処理が、設定されたライフサイクルの影響を受ける可能性があります。
オブジェクトの配置を制御する要素	アクティブな ILM ポリシーの ILM ルール。	アクティブな ILM ポリシーの ILM ルール。
使用されるデータ保護方法	レプリケーションまたはイレイジャーコーディング。	レプリケーション：
各オブジェクトに許可されるコピー数	複数。	クラウドストレージプールに 1 つ、また必要に応じて StorageGRID に 1 つ以上のコピーを作成します。 • 注： * 1 つのオブジェクトを複数のクラウドストレージプールに一度に格納することはできません。

	ストレージプール	クラウドストレージプール
利点は何ですか？	オブジェクトにいつでもすばやくアクセスできる。	低コストのストレージ。

クラウドストレージプールオブジェクトのライフサイクル

クラウドストレージプールを実装する前に、クラウドストレージプールのタイプごとに格納されているオブジェクトのライフサイクルを確認してください。

関連情報

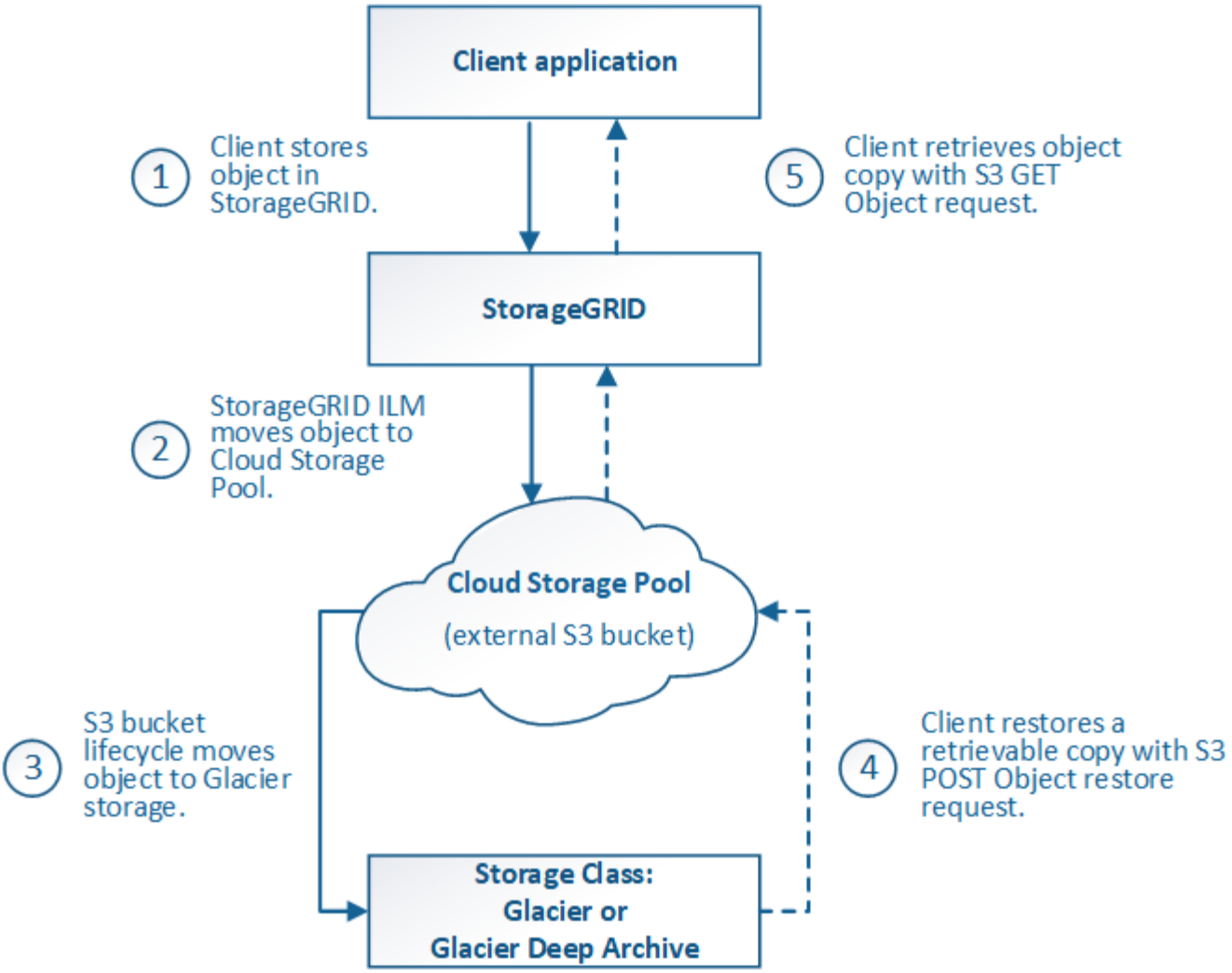
S3 ：クラウドストレージプールオブジェクトのライフサイクル

Azure ：クラウドストレージプールオブジェクトのライフサイクル]

S3 ：クラウドストレージプールオブジェクトのライフサイクル

次の図は、 S3 クラウドストレージプールに格納されているオブジェクトのライフサイクルステージを示しています。

この図と説明にある「 Glacier 」は、 Glacier ストレージクラスと Glacier Deep Archive ストレージクラスの両方を意味します。ただし例外が 1 つあり、 Glacier Deep Archive ストレージクラスでは Expedited リストア階層はサポートされず、Bulk または Standard のみがサポートされます。



1. * StorageGRID * に格納されているオブジェクト

   ライフサイクルを開始するために、クライアントアプリケーションがオブジェクトを StorageGRID に格納します。

2. * オブジェクトを S3 クラウドストレージプールに移動 *

   - S3 クラウドストレージプールを配置場所として使用する ILM ルールにオブジェクトが一致した場合、 StorageGRID はクラウドストレージプールで指定された外部の S3 バケットにオブジェクトを移動します。
   - オブジェクトが S3 クラウドストレージプールに移動されると、クライアントアプリケーションは、オブジェクトが Glacier ストレージに移行されていないかぎり、 StorageGRID から S3 GET Object 要求を使用してオブジェクトを読み出すことができます。

3. * オブジェクトを Glacier に移行（読み出し不可の状態） *

   - 必要に応じて、オブジェクトを Glacier ストレージに移行できます。たとえば外部の S3 バケットが、ライフサイクル設定を使用してオブジェクトを即座または数日後に Glacier ストレージに移行できます。

オブジェクトを移行する場合は、外部の S3 バケット用のライフサイクル設定を作成する必要があります。また、 Glacier ストレージクラスを実装し、 S3 POST Object restore API をサポートするストレージ解決策 を使用する必要があります。

Swift クライアントによって取り込まれたオブジェクトには、クラウドストレージプールを使用しないでください。Swift では POST Object restore 要求がサポートされないため、StorageGRID は S3 Glacier ストレージに移行された Swift オブジェクトを読み出せません。これらのオブジェクトを読み出す Swift GET object 要求は失敗します（ 403 Forbidden ）。

- 移行中、クライアントアプリケーションは S3 HEAD Object 要求を使用してオブジェクトのステータスを監視できます。

4. * Glacier ストレージからオブジェクトをリストア *

   オブジェクトが Glacier ストレージに移行されている場合、クライアントアプリケーションは S3 POST Object restore 要求を問題 で実行して、読み出し可能なコピーを S3 クラウドストレージプールにリストアできます。要求では、クラウドストレージプールでコピーを利用できる日数と、リストア処理に使用するデータアクセス階層（ Expedited 、 Standard 、 Bulk ）を指定します。読み出し可能なコピーの有効期限に達すると、コピーは自動的に読み出し不可能な状態に戻ります。

   StorageGRID 内のストレージノードにもオブジェクトのコピーが存在する場合、 POST Object restore 要求を実行して Glacier からオブジェクトをリストアする必要はありません。GET Object 要求を使用してローカルコピーを直接読み出すことができます。

5. * オブジェクトが取得されました *

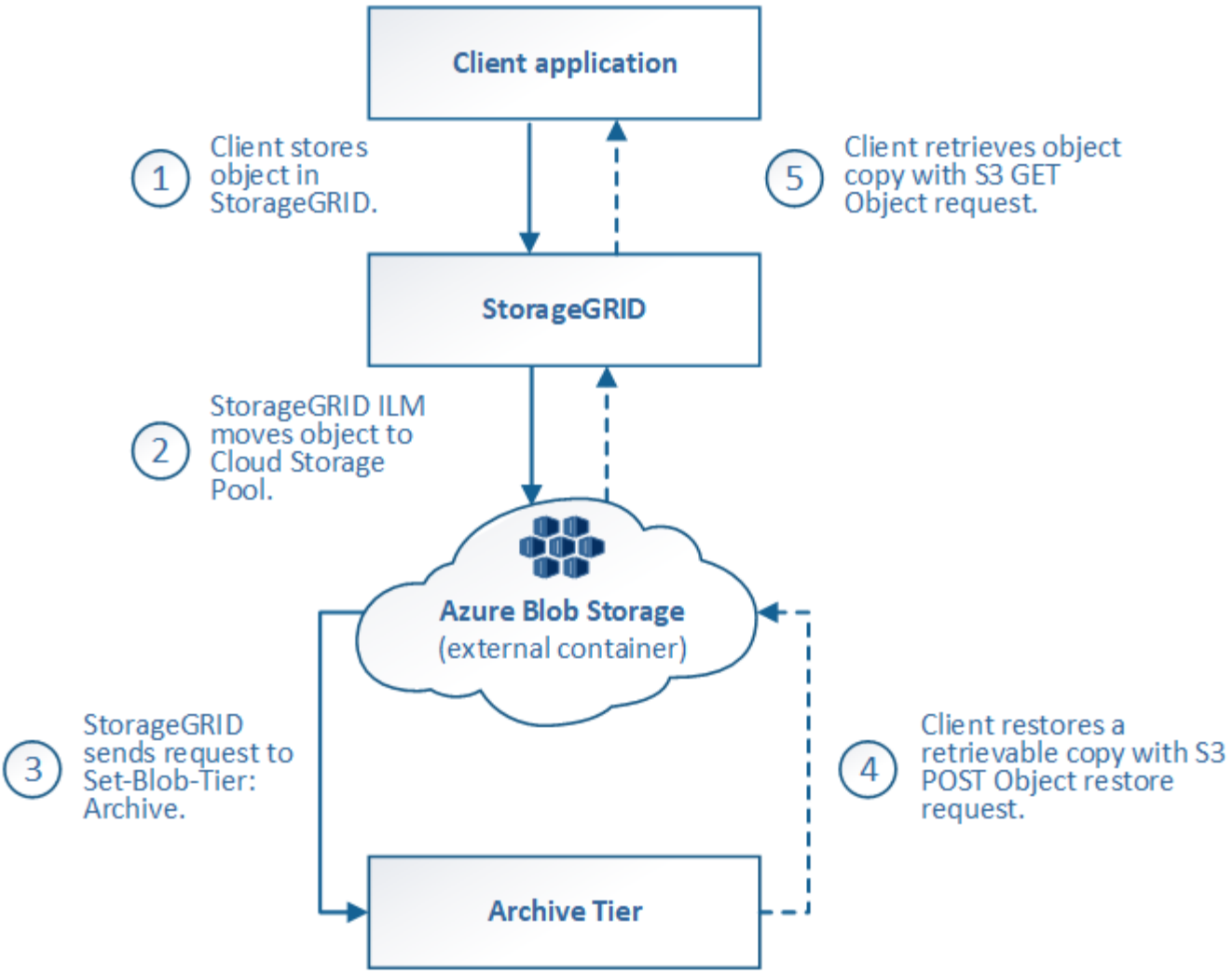
   オブジェクトがリストアされると、クライアントアプリケーションは GET Object 要求を問題 で実行して、リストアされたオブジェクトを読み出すことができます。

関連情報

"S3 を使用する"

Azure ：クラウドストレージプールオブジェクトのライフサイクル

次の図は、 Azure クラウドストレージプールに格納されているオブジェクトのライフサイクルステージを示しています。



1. * StorageGRID * に格納されているオブジェクト

   ライフサイクルを開始するために、クライアントアプリケーションがオブジェクトを StorageGRID に格納します。

2. * オブジェクトを Azure クラウドストレージプールに移動 *

   Azure クラウドストレージプールを配置場所として使用する ILM ルールにオブジェクトが一致した場合、StorageGRID はクラウドストレージプールで指定された外部の Azure BLOB ストレージコンテナにオブジェクトを移動します

   > Swift クライアントによって取り込まれたオブジェクトには、クラウドストレージプールを使用しないでください。Swift では POST Object restore 要求がサポートされないため、StorageGRID は Azure BLOB ストレージのアーカイブ層に移行された Swift オブジェクトを読み出せません。これらのオブジェクトを読み出す Swift GET object 要求は失敗します（ 403 Forbidden ）。

3. * オブジェクトをアーカイブ層に移行（読み出し不可の状態） *

   オブジェクトを Azure クラウドストレージプールに移動すると、 StorageGRID は自動的にオブジェクトを Azure BLOB ストレージのアーカイブ層に移行します。

4. * アーカイブ層からオブジェクトを復元 *

   オブジェクトがアーカイブ層に移行されている場合、クライアントアプリケーションは S3 POST Object restore 要求を問題 で実行して、読み出し可能なコピーを Azure クラウドストレージプールにリストアできます。

   POST Object Restore を受け取った StorageGRID は、オブジェクトを一時的に Azure BLOB ストレージのクール層に移行します。POST Object restore 要求の有効期限に達すると、 StorageGRID はオブジェクトをアーカイブ層に戻します。

   > StorageGRID 内のストレージノードにもオブジェクトのコピーが存在する場合、 POST Object restore 要求を実行してアーカイブアクセス階層からオブジェクトをリストアする必要はありません。GET Object 要求を使用してローカルコピーを直接読み出すことができます。

5. * オブジェクトが取得されました *

   オブジェクトが Azure クラウドストレージプールにリストアされると、クライアントアプリケーションは、リストアされたオブジェクトを読み出すための GET Object 要求を問題 に送信できます。

クラウドストレージプールを使用する状況

クラウドストレージプールは、いくつかのユースケースで大きなメリットをもたらします。

外部の場所にある **StorageGRID** データのバックアップ

クラウドストレージプールを使用して、 StorageGRID オブジェクトを外部の場所にバックアップできます。

StorageGRID 内のコピーにアクセスできない場合は、クラウドストレージプール内のオブジェクトデータを使用してクライアント要求を処理できます。ただし、クラウドストレージプール内のバックアップオブジェクトコピーにアクセスするには、問題 S3 POST Object restore 要求が必要になる場合があります。

クラウドストレージプール内のオブジェクトデータは、ストレージボリュームまたはストレージノードの障害が原因で失われたデータを StorageGRID からリカバリする場合にも使用できます。オブジェクトのコピーがクラウドストレージプールにしか残っていない場合、 StorageGRID はオブジェクトを一時的にリストアして、リカバリされたストレージノードに新しいコピーを作成します。

バックアップ解決策 を実装するには

1. 単一のクラウドストレージプールを作成する。
2. ストレージノードにオブジェクトコピーを（レプリケートコピーまたはイレイジャーコーディングコピーとして）同時に格納し、クラウドストレージプールにオブジェクトコピーを 1 つ格納する ILM ルールを設定します。
3. ルールを ILM ポリシーに追加します。次に、ポリシーをシミュレートしてアクティブ化します。

StorageGRID から外部の場所へのデータの階層化

クラウドストレージプールを使用して、 StorageGRID システムの外部にオブジェクトを格納できます。たとえば、保持する必要のあるオブジェクトが多数あり、それらのオブジェクトにアクセスすることはほとんどありません。クラウドストレージプールを使用してオブジェクトを低コストのストレージに階層化し、

StorageGRID のスペースを解放できます。

階層化解決策 を実装するには：

1. 単一のクラウドストレージプールを作成する。
2. 使用頻度の低いオブジェクトをストレージノードからクラウドストレージプールに移動する ILM ルールを設定します。
3. ルールを ILM ポリシーに追加します。次に、ポリシーをシミュレートしてアクティブ化します。

複数のクラウドエンドポイントを維持する

複数のクラウドにオブジェクトデータを階層化またはバックアップする場合は、複数のクラウドストレージプールを設定できます。ILM ルールのフィルタを使用して、各クラウドストレージプールに格納するオブジェクトを指定できます。たとえば、一部のテナントやバケットのオブジェクトを Amazon S3 Glacier に格納し、その他のテナントやバケットのオブジェクトを Azure BLOB ストレージに格納することができます。または、 Amazon S3 Glacier と Azure BLOB ストレージ間でデータを移動することもできます。複数のクラウドストレージプールを使用する場合、オブジェクトを格納できるクラウドストレージプールは一度に 1 つだけであることに注意してください。

複数のクラウドエンドポイントを実装するには、次

1. 最大 10 個のクラウドストレージプールを作成できます。
2. 適切なタイミングで適切なオブジェクトデータを各クラウドストレージプールに格納する ILM ルールを設定します。たとえば、バケット A のオブジェクトをクラウドストレージプール A に格納し、バケット B のオブジェクトをクラウドストレージプール B に格納しますまたは、オブジェクトを Cloud Storage Pool A に一定期間保存してから、クラウドストレージプール B に移動します
3. ルールを ILM ポリシーに追加します。次に、ポリシーをシミュレートしてアクティブ化します。

クラウドストレージプールに関する考慮事項

クラウドストレージプールを使用して StorageGRID システムからオブジェクトを移動する場合は、クラウドストレージプールの設定と使用に関する考慮事項を確認しておく必要があります。

一般的な考慮事項

- 一般に、 Amazon S3 Glacier や Azure BLOB ストレージなどのクラウドアーカイブストレージにはオブジェクトデータを低コストで格納することができます。ただし、クラウドアーカイブストレージからデータを読み出すコストは比較的高くなります。全体的なコストを最小限に抑えるには、クラウドストレージプール内のオブジェクトにアクセスするタイミングと頻度を考慮する必要があります。クラウドストレージプールの使用は、アクセス頻度の低いコンテンツにのみ推奨されます。
- Swift クライアントによって取り込まれたオブジェクトには、クラウドストレージプールを使用しないでください。Swift では POST Object restore 要求がサポートされないため、 StorageGRID は S3 Glacier ストレージや Azure BLOB ストレージのアーカイブ層に移行された Swift オブジェクトを読み出せません。これらのオブジェクトを読み出す Swift GET object 要求は失敗します（ 403 Forbidden ）。
- クラウドストレージプールターゲットからオブジェクトを読み出すレイテンシが増加しているため、FabricPool でクラウドストレージプールを使用することはサポートされていません。

クラウドストレージプールの作成に必要な情報

クラウドストレージプールを作成する前に、クラウドストレージプールに使用する外部の S3 バケットまたは Azure BLOB ストレージコンテナを作成する必要があります。その後、 StorageGRID でクラウドストレージプールを作成する際に、次の情報を指定する必要があります。

- プロバイダタイプ： Amazon S3 または Azure BLOB ストレージ。
- Amazon S3 を選択した場合は、クラウドストレージプールが AWS Secret Region （ * CAP （ C2S Access Portal ） * ）で使用するかどうかを示します。
- バケットまたはコンテナの正確な名前。
- バケットまたはコンテナへのアクセスに必要なサービスエンドポイント。
- バケットまたはコンテナへのアクセスに必要な認証。
  - * S3 * ：必要に応じて、アクセスキー ID とシークレットアクセスキー。
  - *C2S * ： CAP サーバから一時的なクレデンシャルを取得するための完全な URL 。サーバ CA 証明書、クライアント証明書、クライアント証明書の秘密鍵、および秘密鍵が暗号化されている場合は復号化するためのパスフレーズ。
  - *Azure BLOB ストレージ * ：アカウント名とアカウントキー。これらのクレデンシャルにはコンテナに対する完全な権限が必要です。
- 必要に応じて、バケットまたはコンテナへの TLS 接続を検証するカスタム CA 証明書を指定します。

クラウドストレージプールに使用するポートに関する考慮事項

指定したクラウドストレージプールとの間でオブジェクトを ILM ルールによって移動できるようにするには、システムのストレージノードが含まれるネットワークを設定する必要があります。次のポートがクラウドストレージプールと通信できることを確認してください。

デフォルトでは、クラウドストレージプールは次のポートを使用します。

- **80** ：エンドポイント URI が http で始まる場合
- **442** ： https で始まるエンドポイント URI の場合

クラウドストレージプール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。

非透過型プロキシサーバを使用する場合は、ストレージプロキシの設定で、インターネット上のエンドポイントなどの外部エンドポイントへのメッセージの送信を許可する必要もあります。

コストに関する考慮事項

クラウドストレージプールを使用してクラウド内のストレージにアクセスするには、クラウドへのネットワーク接続が必要です。クラウドストレージプールを使用して StorageGRID とクラウドの間で移動するデータ量の予測に基づいて、クラウドへのアクセスに使用するネットワークインフラのコストを考慮し、適切にプロビジョニングする必要があります。

StorageGRID が外部のクラウドストレージプールエンドポイントに接続すると、さまざまな要求を実行して接続を監視し、必要な処理を確実に実行できるようにします。これらの要求には追加コストが伴いますが、クラウドストレージプールの監視にかかるコストは、 S3 または Azure にオブジェクトを格納する場合の全体的なコストのごくわずかです。

外部クラウドストレージプールのエンドポイントから StorageGRID にオブジェクトを戻す必要がある場合、より大きなコストが発生する可能性があります。次のいずれかの場合、オブジェクトが StorageGRID に戻ることがあります。

- オブジェクトの唯一のコピーがクラウドストレージプールにあり、オブジェクトを StorageGRID に格納することにした場合。その場合は、 ILM ルールとポリシーを再設定するだけです。ILM 評価が実行されると、 StorageGRID はクラウドストレージプールからオブジェクトを読み出す要求を複数実行します。次に、 StorageGRID は指定された数のレプリケートコピーまたはイレイジャーコーディングコピーをローカルに作成します。オブジェクトが StorageGRID に戻ると、クラウドストレージプール内のコピーは削除されます。
- ストレージノードの障害が原因でオブジェクトが失われた場合。オブジェクトのコピーがクラウドストレージプールにしか残っていない場合、 StorageGRID はオブジェクトを一時的にリストアして、リカバリされたストレージノードに新しいコピーを作成します。

> オブジェクトがクラウドストレージプールから StorageGRID に戻ると、 StorageGRID は各オブジェクトに対してクラウドストレージプールエンドポイントに対して複数の要求を実行します。大量のオブジェクトを移動する場合は、事前にテクニカルサポートに問い合わせて、期間と関連コストの見積もりを依頼してください。

S3 ：クラウドストレージプールバケットに必要な権限

クラウドストレージプールに使用される外部の S3 バケットポリシーで、バケットへのオブジェクトの移動、オブジェクトのステータスの取得、必要に応じた Glacier ストレージからのオブジェクトのリストアなどを行うために、 StorageGRID 権限を付与する必要があります。理想的には、StorageGRID にはバケットへのフルコントロールアクセスが必要です (`s3:*`）。ただし、これができない場合は、バケットポリシーで次のS3権限をStorageGRID に付与する必要があります。

- `s3:AbortMultipartUpload`
- `s3:DeleteObject`
- `s3:GetObject`
- `s3:ListBucket`
- `s3:ListBucketMultipartUploads`
- `s3:ListMultipartUploadParts`
- `s3:PutObject`
- `s3:RestoreObject`

S3：外部バケットのライフサイクルに関する考慮事項

StorageGRID とクラウドストレージプールに指定された外部の S3 バケット間のオブジェクトの移動は、StorageGRID の ILM ルールとアクティブな ILM ポリシーによって制御されます。一方、クラウドストレージプールに指定された外部の S3 バケットから Amazon S3 Glacier または S3 Glacier Deep Archive （あるいは Glacier ストレージクラスを実装するストレージ解決策 ）へのオブジェクトの移行は、そのバケットのライフサイクル設定によって制御されます。

クラウドストレージプールからオブジェクトを移行する場合は、外部の S3 バケットに適切なライフサイクル設定を作成する必要があります。また、 Glacier ストレージクラスを実装し、かつ S3 POST Object restore API をサポートするストレージ解決策 を使用する必要があります。

たとえば、 StorageGRID からクラウドストレージプールに移動されたすべてのオブジェクトをすぐに Amazon S3 Glacier ストレージに移行するとします。この場合、単一のアクション（ * Transition * ）を指定する外部の S3 バケットでライフサイクル設定を次のように作成します。

```
<LifecycleConfiguration>
  <Rule>
    <ID>Transition Rule</ID>
    <Filter>
       <Prefix></Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>0</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
  </Rule>
</LifecycleConfiguration>
```

このルールは、すべてのバケットオブジェクトを作成された日（ StorageGRID からクラウドストレージプールに移動された日）に Amazon S3 Glacier に移行します。

> 外部バケットのライフサイクルを設定する場合、 * Expiration * アクションを使用してオブジェクトの期限を定義しないでください。Expiration アクション期限切れのオブジェクトを削除するために、外部ストレージシステムを原因 します。期限切れのオブジェクトにあとで StorageGRID からアクセスしようとしても、削除されたオブジェクトは見つかりません。

クラウドストレージプール内のオブジェクトを（Amazon S3 Glacierではなく）S3 Glacier Deep Archiveに移行する場合は、と指定します `<StorageClass>DEEP_ARCHIVE</StorageClass>` をバケットライフサイクルに追加します。ただし、を使用できないことに注意してください `Expedited` S3 Glacier Deep Archiveからオブジェクトをリストアする階層。

Azure ：アクセス層に関する考慮事項

Azure ストレージアカウントを設定する場合は、デフォルトのアクセス層をホットまたはクールに設定できます。クラウドストレージプールで使用するストレージアカウントを作成する場合は、デフォルト階層としてホット階層を使用する必要があります。StorageGRID はオブジェクトをクラウドストレージプールに移動するとすぐに階層をアーカイブに設定しますが、デフォルト設定をホットにしておくことで、最低期間の 30 日前にクール階層から削除されたオブジェクトに対する早期削除料金が発生しません。

Azure ：ライフサイクル管理はサポートされていません

クラウドストレージプールで使用するコンテナには Azure BLOB ストレージのライフサイクル管理を使用しないでください。ライフサイクル処理が Cloud Storage Pool の処理の妨げになることがあります。

関連情報

"クラウドストレージプールの作成"

"S3 ：クラウドストレージプールの認証情報の指定"

"C2S S3 ：クラウドストレージプールの認証情報の指定"

"Azure：クラウドストレージプールの認証情報の指定"

"StorageGRID の管理"

クラウドストレージプールと **CloudMirror** レプリケーションを比較しています

クラウドストレージプールの使用を開始するにあたって、クラウドストレージプールとStorageGRID CloudMirror レプリケーションサービスの類似点と相違点を理解しておくと役立ちます。

	クラウドストレージプール	**CloudMirror** レプリケーションサービス
主な目的は何ですか？	クラウドストレージプールはアーカイブターゲットとして機能します。クラウドストレージプール内のオブジェクトコピーは、オブジェクトの唯一のコピーにすることも、追加のコピーにすることもできます。つまり、オンプレミスに 2 つのコピーを保持するのではなく、 StorageGRID 内に保持できるコピーは 1 つだけで、クラウドストレージプールにコピーを送信できます。	CloudMirror レプリケーションサービスを使用すると、テナントで、 StorageGRID （ソース）内のバケットから外部の S3 バケット（デスティネーション）にオブジェクトを自動的にレプリケートできます。CloudMirror レプリケーションでは、独立した S3 インフラにオブジェクトの独立したコピーが作成されます。
セットアップ方法は？	クラウドストレージプールは、グリッドマネージャまたはグリッド管理 API を使用して、ストレージプールと同じ方法で定義されます。クラウドストレージプールは、 ILM ルールの配置先として選択できます。ストレージプールはストレージノードのグループで構成されますが、クラウドストレージプールはリモートの S3 または Azure エンドポイント（ IP アドレス、クレデンシャルなど）を使用して定義されます。	テナントユーザは、Tenant ManagerまたはS3 APIを使用してCloudMirrorエンドポイント（IPアドレス、クレデンシャルなど）を定義することによってCloudMirrorレプリケーションを設定します。CloudMirror エンドポイントのセットアップ後、そのテナントアカウントが所有するバケットは、 CloudMirror エンドポイントを参照するように設定できます。
設定は誰が担当しますか？	通常はグリッド管理者	通常はテナントユーザ
デスティネーションは何ですか？	• 互換性のある任意の S3 インフラ（ Amazon S3 を含む） • Azure BLOB アーカイブ層	• 互換性のある任意の S3 インフラ（ Amazon S3 を含む）
オブジェクトをデスティネーションに移動する原因は何ですか？	アクティブな ILM ポリシー内の 1 つ以上の ILM ルール。ILM ルールは、 StorageGRID がクラウドストレージプールに移動するオブジェクトとオブジェクトを移動するタイミングを定義します。	CloudMirror エンドポイントを使用して設定されたソースバケットに新しいオブジェクトを取り込む処理。 CloudMirror エンドポイントを使用してバケットが設定される前のソースバケットに含まれていたオブジェクトは、変更されていないかぎりレプリケートされません。

	クラウドストレージプール	**CloudMirror** レプリケーションサービス
オブジェクトの読み出し方法	アプリケーションは、クラウドストレージプールに移動されたオブジェクトを読み出すために、 StorageGRID への要求を行う必要があります。オブジェクトの唯一のコピーがアーカイブストレージに移行された場合、StorageGRID はオブジェクトのリストアプロセスを管理して読み出し可能にします。	デスティネーションバケット内のミラーコピーは独立したコピーであるため、アプリケーションは、 StorageGRID または S3 デスティネーションに要求を行うことでオブジェクトを読み出すことができます。たとえば、CloudMirror レプリケーションを使用してパートナー組織にオブジェクトをミラーリングするとします。パートナーは、独自のアプリケーションを使用して、 S3 デスティネーションからオブジェクトを直接読み取ったり更新したりできます。StorageGRID を使用する必要はありません。
デスティネーションから直接読み取ることはできますか。	いいえクラウドストレージプールに移動されるオブジェクトは StorageGRID によって管理されます。読み取り要求は StorageGRID に転送する必要があります（ StorageGRID がクラウドストレージプールからの読み出しを実行します）。	はい。ミラーコピーは独立したコピーであるためです。
オブジェクトがソースから削除された場合はどうなりますか？	オブジェクトもクラウドストレージプールから削除されます。	削除操作は複製されません。削除したオブジェクトは StorageGRID バケットには存在しなくなりますが、デスティネーションバケットには引き続き存在します。同様に、デスティネーションバケット内のオブジェクトもソースに影響を与えることなく削除できます。
災害後（ StorageGRID システムが動作していない）にどのようにしてオブジェクトにアクセスしますか。	障害が発生した StorageGRID ノードをリカバリする必要があります。このプロセスでは、レプリケートされたオブジェクトのコピーをクラウドストレージプールのコピーを使用してリストアすることができます。	CloudMirror デスティネーション内のオブジェクトコピーは StorageGRID から独立しているため、 StorageGRID ノードがリカバリされる前に直接アクセスできます。

関連情報

"StorageGRID の管理"

クラウドストレージプールの作成

クラウドストレージプールを作成 StorageGRID する際には、 StorageGRID がオブジェクトの格納に使用する外部バケットまたはコンテナの名前と場所、クラウドプロバイダのタイプ（ Amazon S3 または Azure Blob Storage ）、および外部のバケットまたはコンテナにアクセスするために必要な情報を指定します。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。
- クラウドストレージプールの設定に関するガイドラインを確認しておく必要があります。
- クラウドストレージプールが参照する外部のバケットまたはコンテナが存在している必要があります。
- バケットまたはコンテナにアクセスするためのすべての認証情報が必要です。

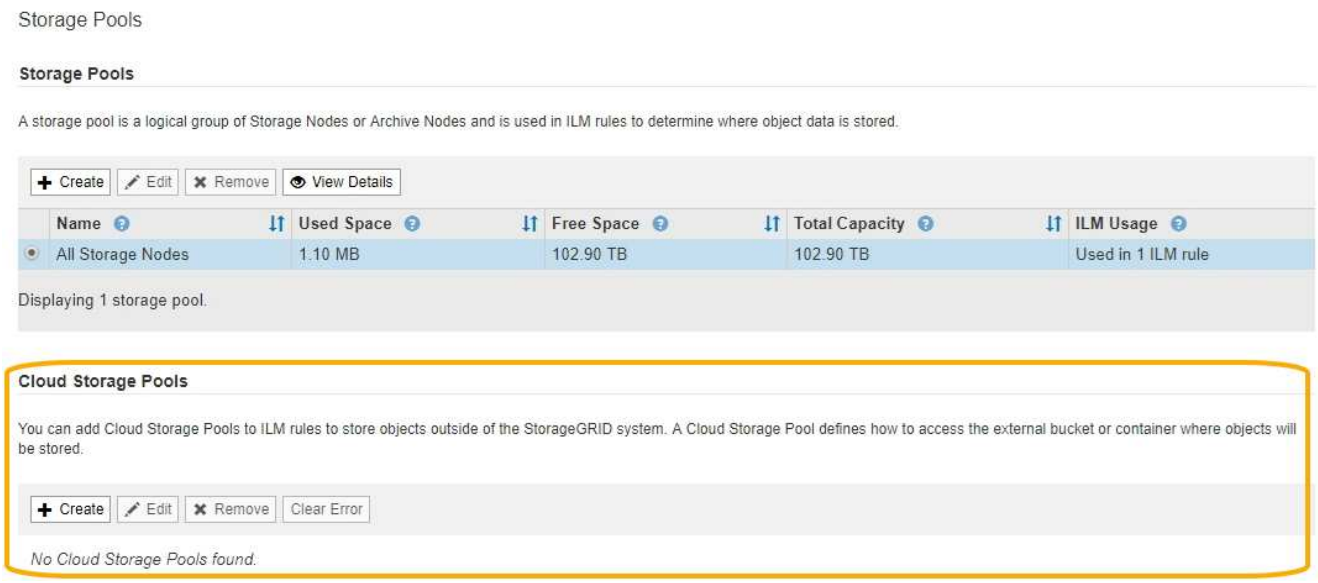
このタスクについて

クラウドストレージプールは、単一の外部の S3 バケットまたは Azure BLOB ストレージコンテナを指定します。クラウドストレージプールは保存後すぐに StorageGRID で検証されます。そのため、クラウドストレージプールに指定されたバケットまたはコンテナが存在し、アクセス可能であることを確認しておく必要があります。

手順

1. ILM > Storage Pools *を選択します。

   Storage Pools （ストレージプール）ページが表示されます。このページには、ストレージプールとクラウドストレージプールの 2 つのセクションがあります。



2. ページのクラウドストレージプールセクションで、*作成*をクリックします。

   Create Cloud Storage Pool （クラウドストレージプールの作成）ダイアログボックスが表示されます。

3. 次の情報を入力します。

フィールド	説明
表示名	クラウドストレージプールとその目的を簡単に説明する名前。ILM ルールを設定するときに識別しやすい名前を使用してください。
プロバイダタイプ	このクラウドストレージプールに使用するクラウドプロバイダ： • Amazon S3（S3またはC2S S3クラウドストレージプールの場合はこのオプションを選択します） • Azure BLOBストレージ ◦ 注：[プロバイダタイプ] を選択すると、ページの下部に [サービスエンドポイント] 、 [認証] 、および [サーバ検証] セクションが表示されます。
バケットまたはコンテナ	クラウドストレージプール用に作成された外部の S3 バケットまたは Azure コンテナの名前。バケットまたはコンテナの名前は正確に指定する必要があります。一致していないと、クラウドストレージプールの作成が失敗します。クラウドストレージプールの保存後にこの値を変更することはできません。

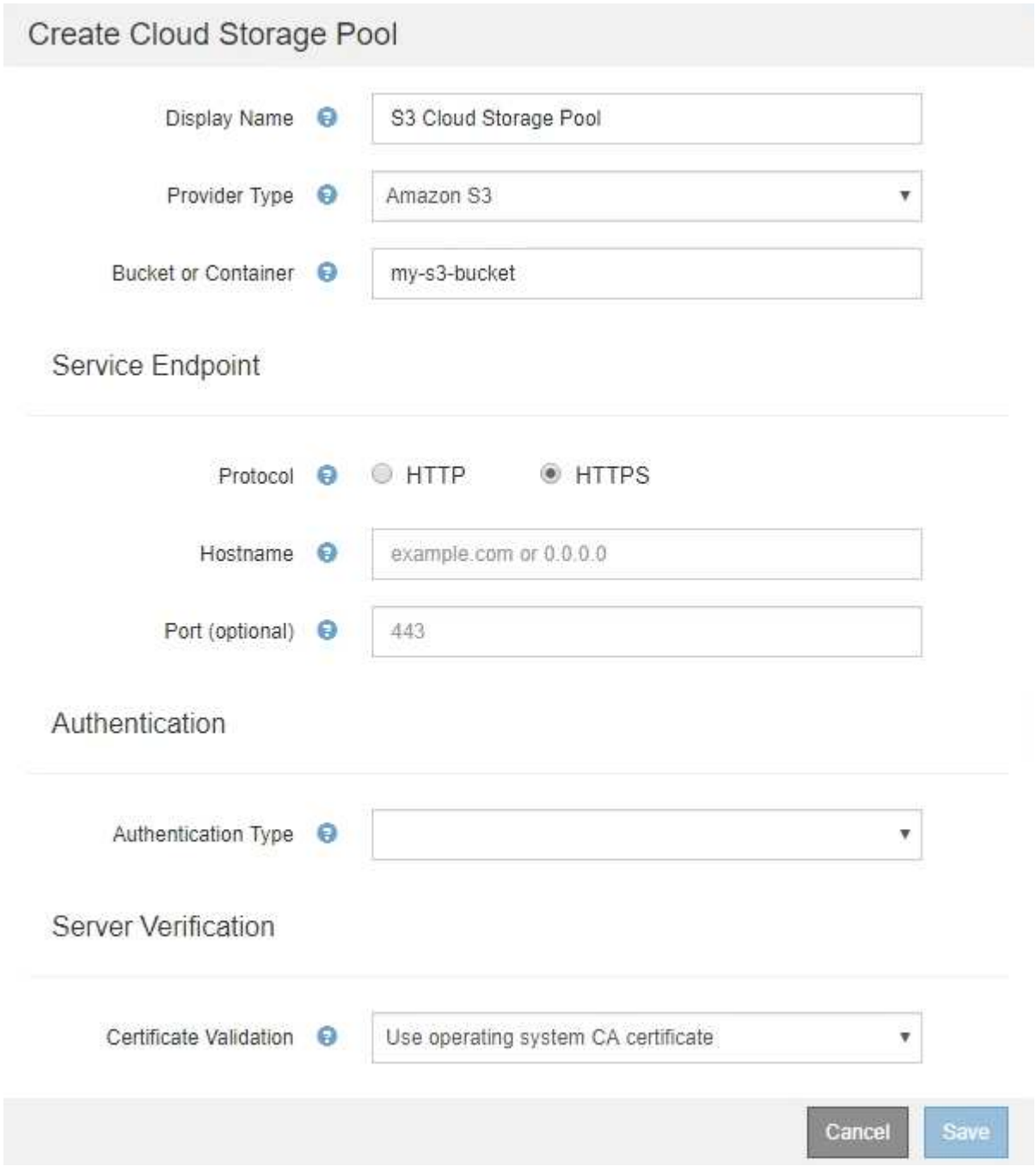
4. 選択したプロバイダータイプに基づいて、ページの [Service Endpoint] 、 [Authentication] 、および [Server Verification] セクションを完了します。
   - "S3 ：クラウドストレージプールの認証情報の指定"
   - "C2S S3 ：クラウドストレージプールの認証情報の指定"
   - "Azure：クラウドストレージプールの認証情報の指定"

S3 ：クラウドストレージプールの認証情報の指定

S3 用のクラウドストレージプールを作成する場合は、クラウドストレージプールのエンドポイントで必要な認証のタイプを選択する必要があります。匿名を指定するか、アクセスキー ID とシークレットアクセスキーを入力できます。

必要なもの

- クラウドストレージプールの基本情報を入力し、プロバイダタイプとして* Amazon S3 *を指定しておく必要があります。



- アクセスキー認証を使用している場合は、外部のS3バケットのアクセスキーIDとシークレットアクセスキーを把握しておく必要があります。

手順

1. 「 * Service Endpoint * 」セクションで、次の情報を入力します。

   a. クラウドストレージプールに接続するときに使用するプロトコルを選択します。

      デフォルトのプロトコルは HTTPS です。

b. クラウドストレージプールのサーバのホスト名または IP アドレスを入力します。

例：

```
s3-aws-region.amazonaws.com
```

バケット名はこのフィールドに含めないでください。バケット名は「 * Bucket 」フィールドまたは「 Container * 」フィールドに入力します。

a. 必要に応じて、クラウドストレージプールへの接続時に使用するポートを指定します。

デフォルトのポート（ HTTPS の場合はポート 443 、 HTTP の場合はポート 80 ）を使用する場合は、このフィールドを空白のままにします。

2. [* 認証 *] セクションで、クラウドストレージプールエンドポイントに必要な認証のタイプを選択します。

オプション	説明
アクセスキー	Cloud Storage Pool バケットにアクセスするには、アクセスキー ID とシークレットアクセスキーが必要です。
匿名	すべてのユーザが Cloud Storage Pool バケットにアクセスできます。アクセスキー ID とシークレットアクセスキーは不要です。
CAP （ C2S Access Portal ）	C2S S3 にのみ使用されます。に進みます "C2S S3 ：クラウドストレージプールの認証情報の指定"。

3. アクセスキーを選択した場合は、次の情報を入力します。

オプション	説明
アクセスキー ID	外部バケットを所有するアカウントのアクセスキー ID 。
シークレットアクセスキー	関連付けられているシークレットアクセスキー。

4. Server Verification セクションで、クラウドストレージプールへの TLS 接続用の証明書を検証する方法を選択します。

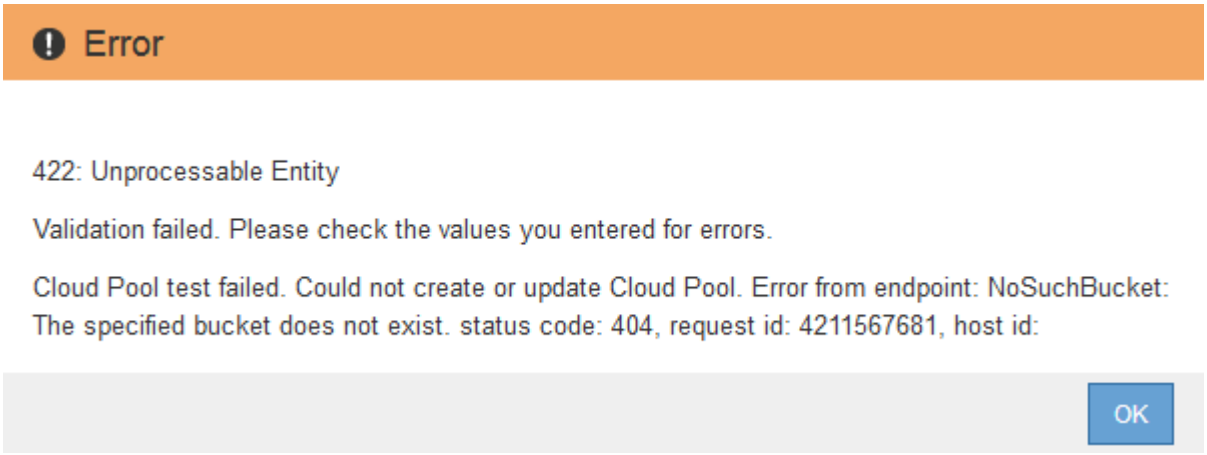
オプション	説明
オペレーティングシステムの CA 証明書を使用します	オペレーティングシステムにインストールされているデフォルトのCA証明書を使用して接続を保護します。
カスタム CA 証明書を使用する	カスタム CA 証明書を使用する。Select New *をクリックし、PEMでエンコードされたCA証明書をアップロードします。
証明書を検証しないでください	TLS 接続に使用される証明書は検証されません。

5. [保存（ Save ）] をクリックします。

クラウドストレージプールを保存すると、 StorageGRID では次の処理が実行されます。

- バケットとサービスエンドポイントが存在し、指定したクレデンシャルを使用してそれらにアクセスできることを検証します。
- バケットをクラウドストレージプールとして識別するために、バケットにマーカーファイルを書き込みます。このファイルは削除しないでください `x-ntap-sgws-cloud-pool-uuid`。

クラウドストレージプールの検証に失敗すると、その理由を記載したエラーメッセージが表示されます。たとえば、証明書エラーが発生した場合や、指定したバケットが存在しない場合などにエラーが報告されます。



クラウドストレージプールのトラブルシューティングの手順を参照し、問題 を解決してから、クラウドストレージプールをもう一度保存してください。

関連情報

"クラウドストレージプールのトラブルシューティング"

C2S S3 ：クラウドストレージプールの認証情報の指定

Commercial クラウド サービス （ C2S ） S3 サービスをクラウドストレージプールとして使用するには、認証タイプとして C2S Access Portal （ CAP ）を設定し、StorageGRID が C2S アカウント内の S3 バケットにアクセスするための一時的なクレデンシャルを要求できるようにする必要があります。

必要なもの

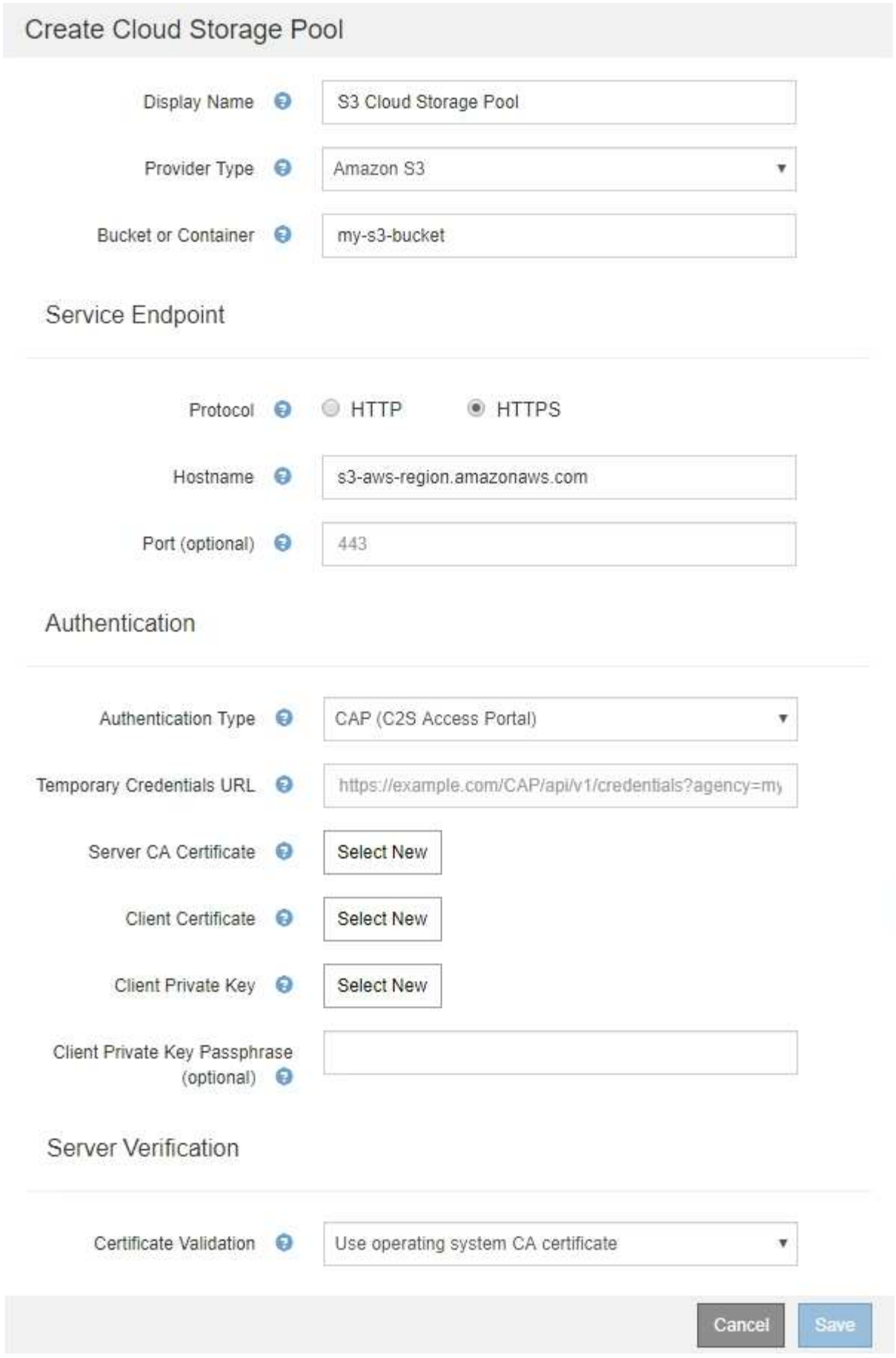
- サービスエンドポイントを含むAmazon S3クラウドストレージプールの基本情報を入力しておく必要があります。
- StorageGRID がCAPサーバから一時的なクレデンシャルを取得するために使用する、C2Sアカウントに割り当てられている必須/オプションのAPIパラメータをすべて含む完全なURLが必要です。
- 該当する公的認証局（CA）が発行したサーバCA証明書が必要です。StorageGRID は、この証明書を使用して CAP サーバの識別情報を確認します。サーバ CA 証明書は PEM エンコードを使用している必要があります。
- 該当する公的認証局（CA）が発行したクライアント証明書が必要です。StorageGRID は、この証明書を使用して CAP サーバに対して自身を識別します。クライアント証明書は PEM エンコードを使用し、C2S アカウントへのアクセスが許可されている必要があります。

- クライアント証明書のPEMでエンコードされた秘密鍵が必要です。
- クライアント証明書の秘密鍵が暗号化されている場合は、復号化用のパスフレーズが必要です。

手順

1. [* 認証 **]** セクションで、 **[** 認証タイプ **]** ドロップダウンから ***CAP (C2S Access Portal)*** を選択します。

   CAP C2S の認証フィールドが表示されます。


Create Cloud Storage Pool
Display Name
S3 Cloud Storage Pool
Provider Type
Amazon S3
Bucket or Container
my-s3-bucket
Service Endpoint
Protocol
HTTP
HTTPS
Hostname
s3-aws-region.amazonaws.com
Port (optional)
443
Authentication
Authentication Type
CAP (C2S Access Portal)
Temporary Credentials URL
https://example.com/CAP/api/v1/credentials?agency=my
Server CA Certificate
Select New
Client Certificate
Select New
Client Private Key
Select New
Client Private Key Passphrase (optional)
Server Verification
Certificate Validation
Use operating system CA certificate
Cancel
Save

2. 次の情報を入力します。

   a. [*Temporary Credentials URL] には、 StorageGRID が CAP サーバから一時的なクレデンシャルを取得するために使用する完全な URL を入力します。これには、 C2S アカウントに割り当てられている必須およびオプションの API パラメータがすべて含まれます。

   b. サーバーCA証明書*の場合は、*新規選択*をクリックし、StorageGRID がCAPサーバーの検証に使用するPEMでエンコードされたCA証明書をアップロードします。

   c. *クライアント証明書*の場合は、*新しい*を選択をクリックし、StorageGRID がCAPサーバに対して自身を識別するために使用するPEMでエンコードされた証明書をアップロードします。

   d. *クライアント秘密鍵*の場合は、*新規選択*をクリックし、クライアント証明書のPEMでエンコードされた秘密鍵をアップロードします。

      秘密鍵が暗号化されている場合は、従来の形式を使用する必要があります。（ PKCS #8 で暗号化された形式はサポートされていません）。

   e. クライアントの秘密鍵が暗号化されている場合は、クライアントの秘密鍵を復号化するためのパスフレーズを入力します。それ以外の場合は、 [* クライアント秘密キーのパスフレーズ *] フィールドを空白のままにします。

3. Server Verification セクションで、次の情報を指定します。

   a. 「 * 証明書の検証 * 」で、「 * カスタム CA 証明書を使用する * 」を選択します。

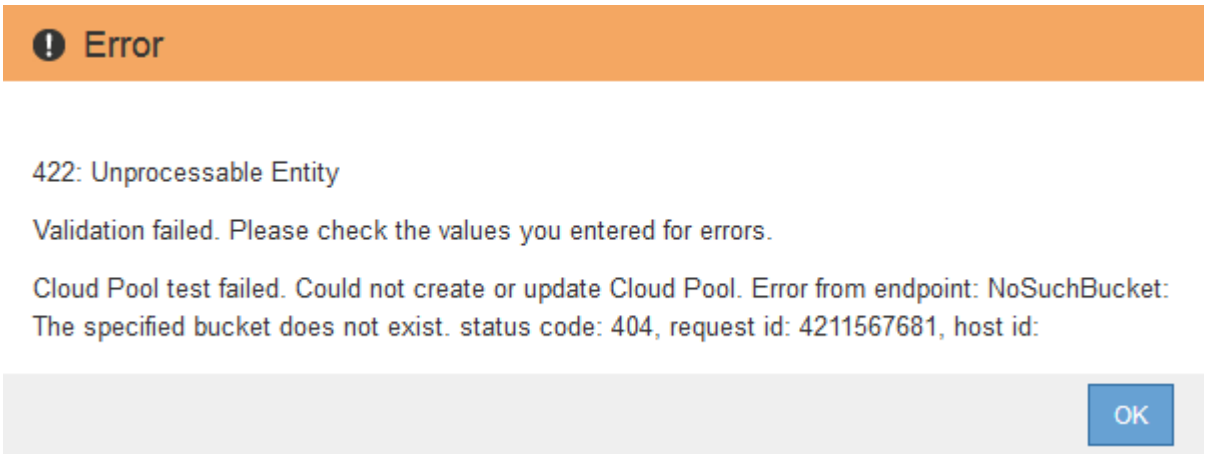
   b. Select New *をクリックし、PEMでエンコードされたCA証明書をアップロードします。

4. [保存（ Save ）] をクリックします。

クラウドストレージプールを保存すると、 StorageGRID では次の処理が実行されます。

- バケットとサービスエンドポイントが存在し、指定したクレデンシャルを使用してそれらにアクセスできることを検証します。
- バケットをクラウドストレージプールとして識別するために、バケットにマーカーファイルを書き込みます。このファイルは削除しないでください `x-ntap-sgws-cloud-pool-uuid`。

クラウドストレージプールの検証に失敗すると、その理由を記載したエラーメッセージが表示されます。たとえば、証明書エラーが発生した場合や、指定したバケットが存在しない場合などにエラーが報告されます。



クラウドストレージプールのトラブルシューティングの手順を参照し、問題 を解決してから、クラウドストレージプールをもう一度保存してください。

関連情報

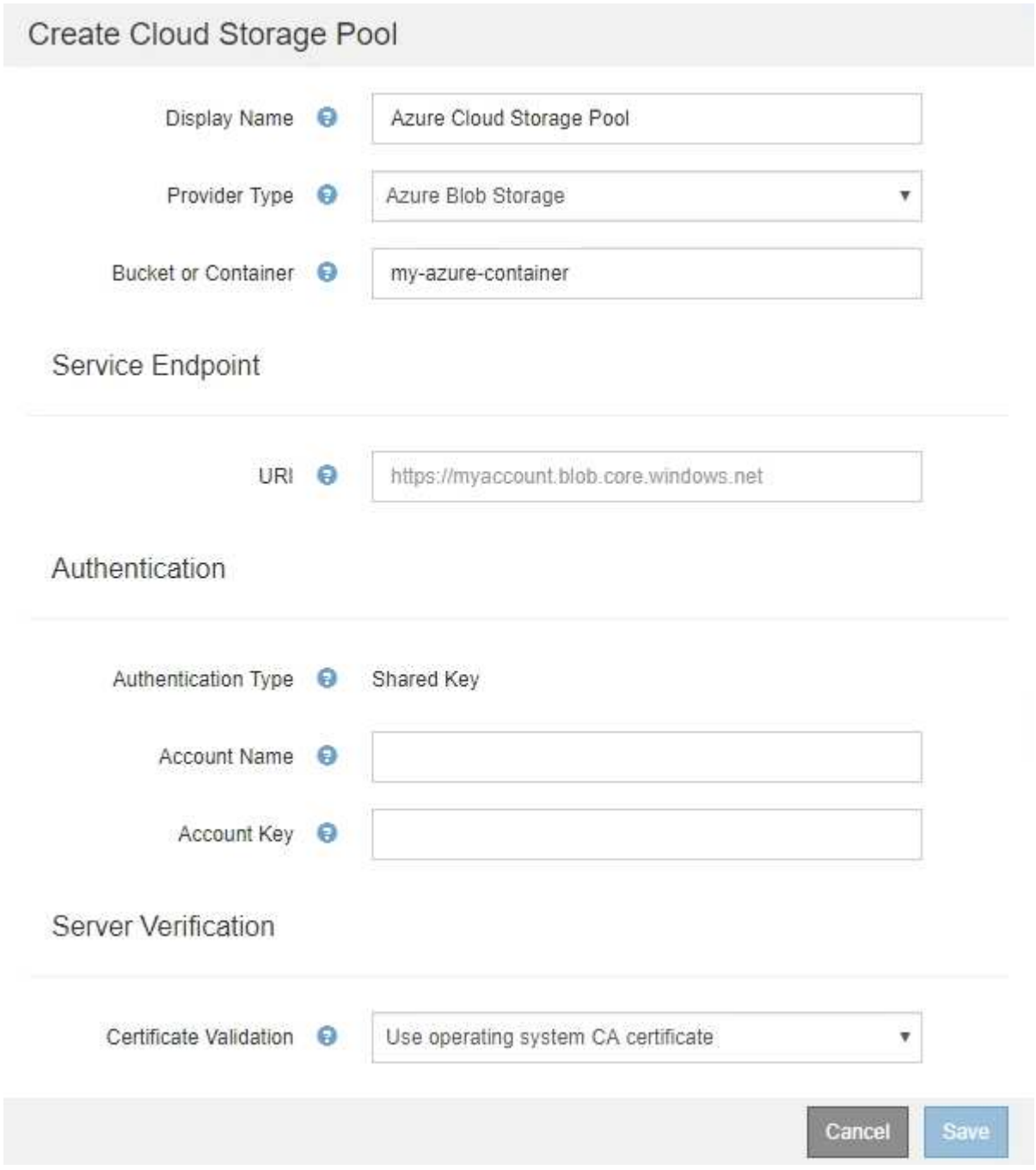
"クラウドストレージプールのトラブルシューティング"

Azure：クラウドストレージプールの認証情報の指定

Azure BLOB ストレージ用のクラウドストレージプールを作成する場合は、StorageGRID がオブジェクトの格納に使用する外部コンテナのアカウント名とアカウントキーを指定する必要があります。

必要なもの

- クラウドストレージプールの基本情報を入力し、プロバイダタイプとして「* Azure Blob Storage 」を指定しておく必要があります。***Authentication Type** フィールドに Shared Key* が表示されます。



- クラウドストレージプールに使用されるBLOBストレージコンテナへのアクセスに使用するUniform Resource Identifier（URI）を確認しておく必要があります。
- ストレージアカウントの名前とシークレットキーを把握しておく必要があります。これらの値は Azure portal を使用して確認できます。

手順

1. 「 * サービスエンドポイント * 」セクションで、クラウドストレージプールに使用される BLOB ストレージコンテナへのアクセスに使用する Uniform Resource Identifier （ URI ）を入力します。

   次のいずれかの形式で指定します。

   - `https://host:port`
   - `http://host:port`

   ポートを指定しない場合、デフォルトでは HTTPS URI にはポート 443 が、 HTTP URI にはポート 80 が使用されます。* Azure BLOBストレージコンテナのURIの例* ： `https://myaccount.blob.core.windows.net`

2. [* 認証 * （ * Authentication * ）] セクションで、次の情報を入力します。

   a. **Account Name** に、外部サービスコンテナを所有する BLOB ストレージアカウントの名前を入力します。

   b. 「 * Account Key * 」に、 BLOB ストレージアカウントのシークレットキーを入力します。

   Azure エンドポイントの場合は、共有キー認証を使用する必要があります。

3. [サーバ検証 *] セクションで、クラウドストレージプールへの TLS 接続用証明書の検証に使用する方法を選択します。

オプション	説明
オペレーティングシステムの CA 証明書を使用します	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 証明書を使用する。[Select New]をクリックし、PEMでエンコードされた証明書をアップロードします。
証明書を検証しないでください	TLS 接続に使用される証明書は検証されません。

4. [保存（ Save ）] をクリックします。

クラウドストレージプールを保存すると、 StorageGRID では次の処理が実行されます。

- コンテナと URI が存在し、指定したクレデンシャルを使用してアクセスできることを検証します。
- クラウドストレージプールとして識別するためにコンテナにマーカーファイルを書き込みます。このファイルは削除しないでください `x-ntap-sgws-cloud-pool-uuid`。

クラウドストレージプールの検証に失敗すると、その理由を記載したエラーメッセージが表示されます。たとえば、証明書エラーが発生した場合や、指定したコンテナが存在しない場合などにエラーが報告されます。

クラウドストレージプールのトラブルシューティングの手順を参照し、問題 を解決してから、クラウドストレージプールをもう一度保存してください。

関連情報

"クラウドストレージプールのトラブルシューティング"

クラウドストレージプールの編集

クラウドストレージプールを編集して、名前、サービスエンドポイント、またはその他の詳細を変更できます。ただし、クラウドストレージプールの S3 バケットまたは Azure コンテナを変更することはできません。

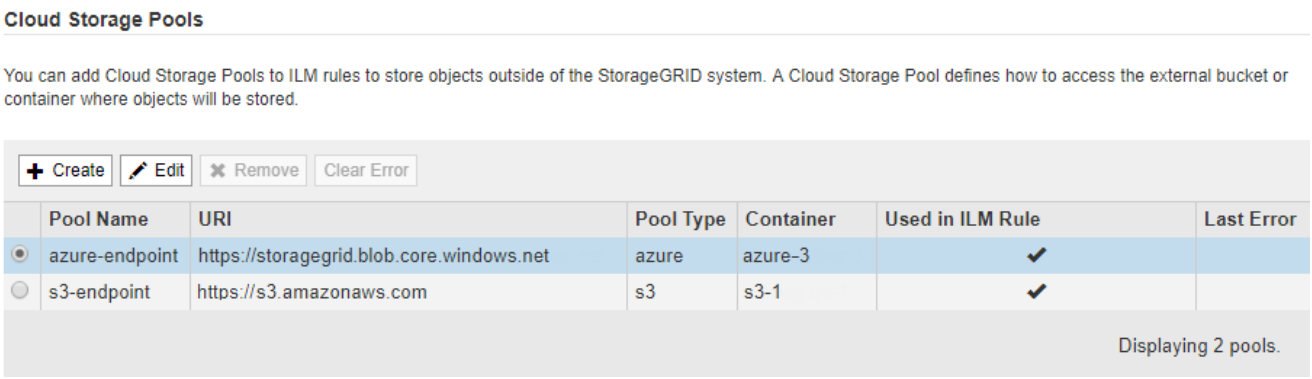
必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。
- クラウドストレージプールの設定に関するガイドラインを確認しておく必要があります。

手順

1. ILM > Storage Pools *を選択します。

   Storage Pools （ストレージプール）ページが表示されます。Cloud Storage Pools テーブルには、既存のクラウドストレージプールが表示されます。



2. 編集するクラウドストレージプールのラジオボタンを選択します。
3. [編集（ Edit ）] をクリックします。
4. 必要に応じて、表示名、サービスエンドポイント、認証クレデンシャル、または証明書の検証方法を変更します。

   クラウドストレージプールのプロバイダタイプ、 S3 バケット、 Azure コンテナを変更することはできません。

   以前にサーバ証明書またはクライアント証明書をアップロードした場合は、現在使用中の証明書を確認するために [現在の証明書を表示] を選択できます。

5. [保存（ Save ）] をクリックします。

   クラウドストレージプールを保存すると、バケットまたはコンテナとサービスエンドポイントが存在し、

指定したクレデンシャルでそれらにアクセスできることが StorageGRID によって検証されます。

クラウドストレージプールの検証が失敗すると、エラーメッセージが表示されます。たとえば、証明書エラーが発生した場合はエラーが報告されます。

クラウドストレージプールのトラブルシューティングの手順を参照し、問題 を解決してから、クラウドストレージプールをもう一度保存してください。

関連情報

"クラウドストレージプールに関する考慮事項"

"クラウドストレージプールのトラブルシューティング"

クラウドストレージプールの削除

ILM ルールで使用されておらず、オブジェクトデータが含まれていないクラウドストレージプールを削除できます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。
- S3 バケットまたは Azure コンテナにオブジェクトが含まれていないことを確認します。クラウドストレージプールにオブジェクトが含まれている場合、そのストレージプールを削除しようとするとエラーが発生します。「クラウドストレージプールのトラブルシューティング」を参照してください。

> クラウドストレージプールを作成すると、 StorageGRID はバケットまたはコンテナにマーカーファイルを書き込み、クラウドストレージプールとして識別します。このファイルは削除しないでください `x-ntap-sgws-cloud-pool-uuid`。

- プールを使用している可能性のある ILM ルールを削除しておきます。

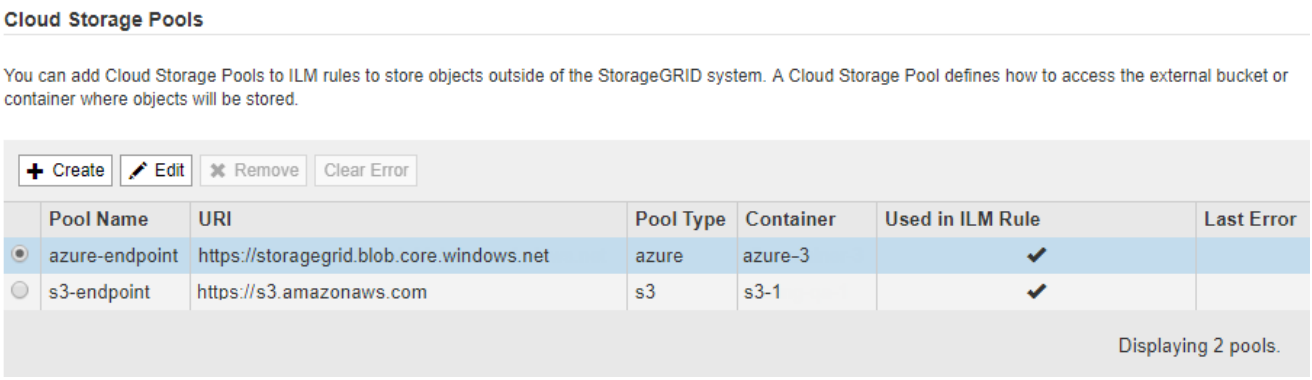
手順

1. ILM > Storage Pools *を選択します。

   Storage Pools （ストレージプール）ページが表示されます。

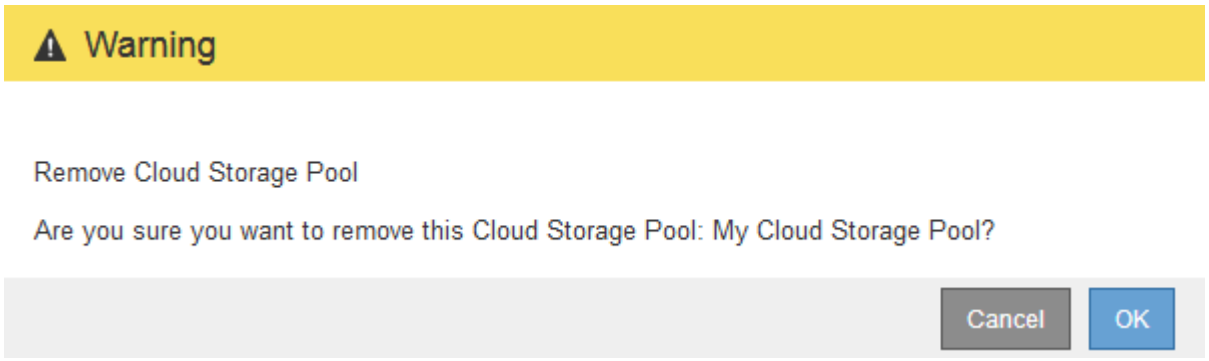
2. ILM ルールで現在使用されていないクラウドストレージプールのラジオボタンを選択します。

   ILM ルールで使用されているクラウドストレージプールは削除できません。「 * 削除」ボタンは無効になっています。



3. [削除（ Remove ）] をクリックします。

   確認の警告が表示されます。



4. [OK] をクリックします。

   クラウドストレージプールが削除されます。

関連情報

"クラウドストレージプールのトラブルシューティング"

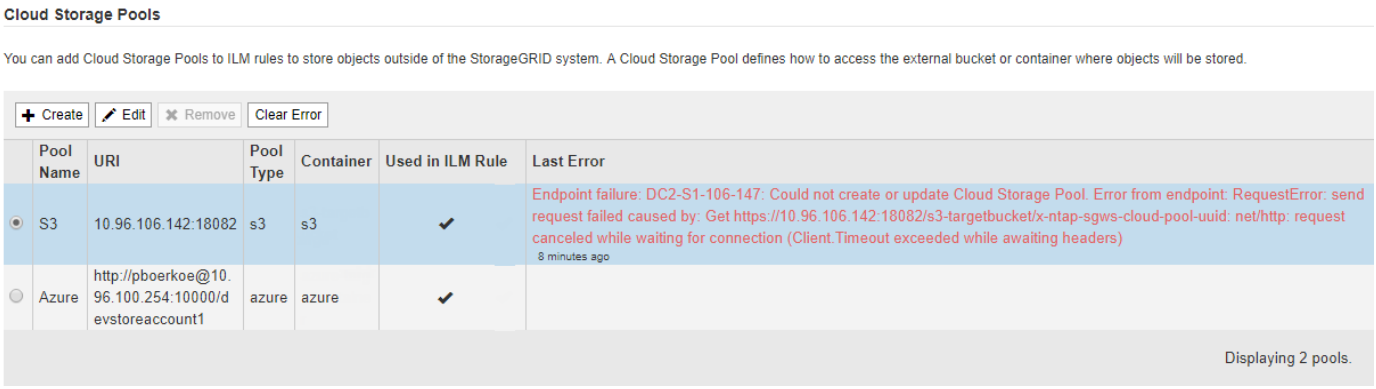
クラウドストレージプールのトラブルシューティング

クラウドストレージプールの作成、編集、削除時にエラーが発生した場合は、以下のトラブルシューティング手順を使用して問題 を解決してください。

エラーが発生したかどうかを確認しています

StorageGRID では、すべてのクラウドストレージプールの健全性チェックを 1 分に 1 回実行して、クラウドストレージプールにアクセスできること、およびプールが正常に機能していることを確認します。健全性チェックで問題 が検出されると、ストレージプールページのクラウドストレージプールテーブルの前回のエラー列にメッセージが表示されます。

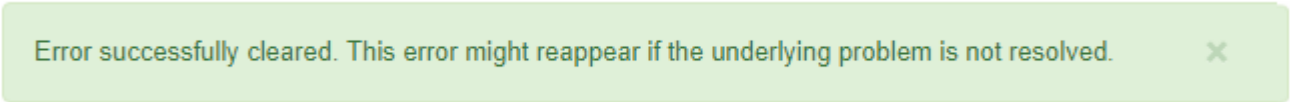
次の表は、各クラウドストレージプールで検出された最新のエラーと、エラーが発生してからの時間を示しています。



また、過去 5 分以内に新しいクラウドストレージプールのエラーが発生したことが健全性チェックで検出されると、 * クラウドストレージプール接続エラー * アラートがトリガーされます。このアラートのEメール通知を受信した場合は、ストレージプールのページ（* ILM *>*ストレージプール*を選択）に移動し、Last Error 列のエラーメッセージを確認して、以下のトラブルシューティング・ガイドラインを参照してください。

エラーが解決されたかどうかを確認しています

エラーの原因となっている問題を解決したら、エラーが解決されたかどうかを確認できます。Cloud Storage Poolページで、エンドポイントのオプションボタンを選択し、* Clear Error *をクリックします。StorageGRID がクラウドストレージプールのエラーをクリアしたことを示す確認メッセージが表示されます。



原因となっている問題が解決されると、エラーメッセージは表示されなくなります。ただし、根本的な問題が修正されていない場合（または別のエラーが発生した場合）は、数分以内に Last Error 列にエラーメッセージが表示されます。

エラー：このクラウドストレージプールには予期しないコンテンツが含まれています

クラウドストレージプールを作成、編集、または削除しようとすると、このエラーが発生する場合があります。このエラーは、バケットまたはコンテナにが含まれている場合に発生します `x-ntap-sgws-cloud-pool-uuid` マーカーファイルですが、想定されるUUIDがファイルにありません。

通常、このエラーが表示されるのは、新しいクラウドストレージプールを作成していて、 StorageGRID の別のインスタンスがすでに同じクラウドストレージプールを使用している場合のみです。

問題 を修正するには、次の手順を実行します。

- 組織内のユーザがこのクラウドストレージプールを使用していないことを確認します。
- を削除します `x-ntap-sgws-cloud-pool-uuid` ファイルして、クラウドストレージプールの設定を再試行してください。

エラー：クラウドストレージプールを作成または更新できませんでした。エンドポイントからのエラーです

クラウドストレージプールを作成または編集しようとすると、このエラーが発生する場合があります。このエラーは、何らかの接続または構成の問題 が原因で StorageGRID がクラウドストレージプールに書き込めないことを示しています。

問題 を修正するには、エンドポイントからのエラーメッセージを確認します。

- エラーメッセージにが含まれている場合 `Get *url*: EOF`をクリックし、クラウドストレージプールに使用されるサービスエンドポイントが、HTTPSを必要とするコンテナまたはバケットにHTTPプロトコルを使用していないことを確認します。
- エラーメッセージにが含まれている場合 `Get *url*: net/http: request canceled while waiting for connection` をクリックして、ストレージノードがクラウドストレージプールに使用するサービスエンドポイントにアクセスできるようにネットワーク設定で許可されていることを確認します。
- その他のすべてのエンドポイントエラーメッセージについては、次のいずれか、または複数の操作を試してください。
  - クラウドストレージプール用に入力した名前と同じ名前の外部コンテナまたはバケットを作成して、新しいクラウドストレージプールを再度保存します。
  - クラウドストレージプール用に指定したコンテナまたはバケット名を修正して、新しいクラウドストレージプールを再度保存します。

エラー： **CA** 証明書を解析できませんでした

クラウドストレージプールを作成または編集しようとすると、このエラーが発生する場合があります。このエラーは、クラウドストレージプールの設定時に入力した証明書を StorageGRID が解析できなかった場合に発生します。

問題 を修正するには、指定した CA 証明書に問題がないかどうかを確認します。

エラー：この **ID** のクラウドストレージプールが見つかりませんでした

クラウドストレージプールを編集または削除しようとすると、このエラーが発生する場合があります。このエラーは、次のいずれかの理由でエンドポイントが 404 応答を返した場合に発生します。

- クラウドストレージプールに使用されたクレデンシャルに、バケットの読み取り権限がありません。
- クラウドストレージプールに使用されるバケットにはが含まれません `x-ntap-sgws-cloud-pool-uuid` マーカーファイル。

問題 を修正するには、次の手順をいくつか実行します。

- 設定したアクセスキーに関連付けられているユーザに必要な権限があることを確認します。
- 必要な権限があるクレデンシャルを使用してクラウドストレージプールを編集します。
- 権限が正しい場合は、サポートにお問い合わせください。

エラー：クラウドストレージプールの内容を確認できませんでした。エンドポイントからのエラーです

クラウドストレージプールを削除しようとすると、このエラーが発生する場合があります。このエラーは、何らかの接続または設定問題 が原因で、 StorageGRID がクラウドストレージプールバケットのコンテンツを読み取れないことを示しています。

問題 を修正するには、エンドポイントからのエラーメッセージを確認します。

エラー： **Objects have already been placed in this bucket**

クラウドストレージプールを削除しようとすると、このエラーが発生する場合があります。ILM によって移動されたデータ、クラウドストレージプールの設定前にバケットに配置されていたデータ、またはクラウドストレージプールの作成後に他のソースによってバケットに配置されたデータが含まれているクラウドストレージプールは削除できません。

問題 を修正するには、次の手順をいくつか実行します。

- 「クラウドストレージプールオブジェクトのライフサイクル」の手順に従って、オブジェクトを StorageGRID に戻します。
- 残りのオブジェクトが ILM によってクラウドストレージプールに配置されていないことが確実な場合は、バケットからオブジェクトを手動で削除します。

> ILM によって配置された可能性のあるクラウドストレージプールからは、オブジェクトを手動で削除しないでください。手動で削除したオブジェクトにあとで StorageGRID からアクセスしようとしても、削除したオブジェクトは見つかりません。

エラー：クラウドストレージプールにアクセスしようとして、プロキシで外部エラーが発生しました

ストレージノードとクラウドストレージプールに使用する外部の S3 エンドポイントの間に非透過型ストレージプロキシを設定した場合に、このエラーが発生する可能性があります。このエラーは、外部プロキシサーバがクラウドストレージプールのエンドポイントに到達できない場合に発生します。たとえば、 DNS サーバがホスト名を解決できない場合や、外部ネットワークの問題 が存在する場合があります。

問題 を修正するには、次の手順をいくつか実行します。

- クラウドストレージプールの設定（* ILM **>***ストレージプール）を確認します。
- ストレージプロキシサーバのネットワーク設定を確認します。

関連情報

"クラウドストレージプールオブジェクトのライフサイクル"

イレイジャーコーディングプロファイルの設定

イレイジャーコーディングプロファイルを設定するには、ストレージプールを6+3などのイレイジャーコーディングスキームと関連付けます。これにより、ILMルールの配置手順を設定する際に、イレイジャーコーディングプロファイルを選択できるようになります。オブジェクトがルールに一致すると、イレイジャーコーディングスキームに従ってデータフラグメントとパリティフラグメントが作成され、ストレージプール内の格納場所に分散されます。

- "イレイジャーコーディングプロファイルの作成"
- "イレイジャーコーディングプロファイルの名前変更"
- "イレイジャーコーディングプロファイルを非アクティブ化する"

イレイジャーコーディングプロファイルを作成するには、ストレージノードを含むストレージプールをイレイジャーコーディングスキームに関連付けます。この関連付けにより、作成されるデータフラグメントおよびパリティフラグメントの数と、各フラグメントをどこに分散配置するかが決まります。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。
- サイトを1つだけ含むストレージプール、または3つ以上のサイトを含むストレージプールを作成しておく必要があります。サイトが 2 つだけのストレージプールではイレイジャーコーディングスキームを使用できません。

このタスクについて

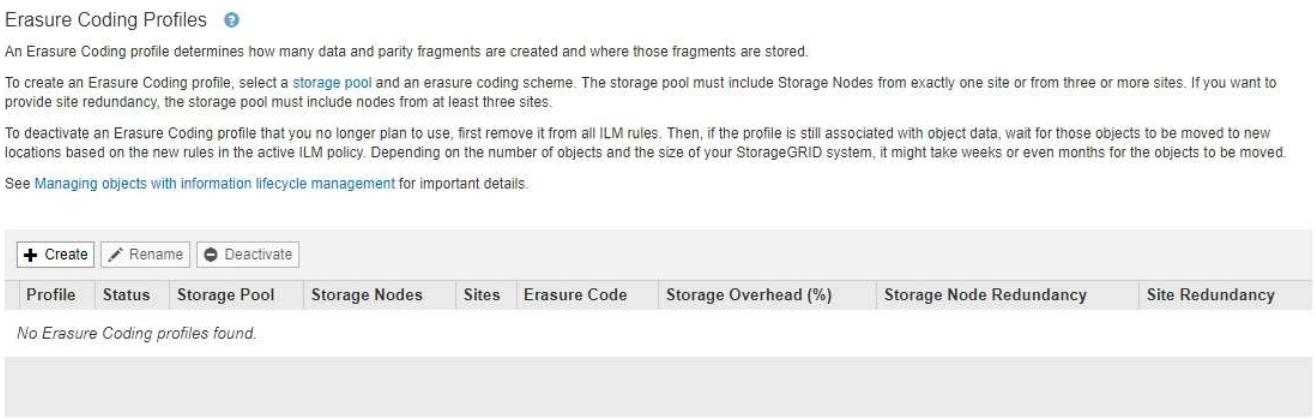
イレイジャーコーディングプロファイルで使用するストレージプールには、サイトが 1 つだけ、または 3 つ以上含まれている必要があります。サイトの冗長性を確保するには、ストレージプールにサイトが少なくとも 3 つ必要です。

ストレージノードを含むストレージプールを選択する必要があります。イレイジャーコーディングデータ用にアーカイブノードを使用することはできません。

手順

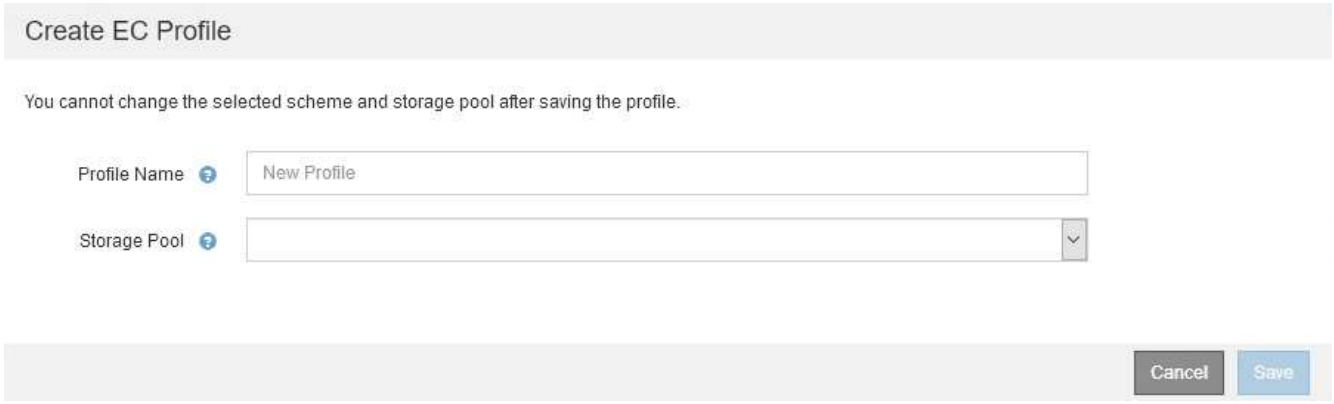
1. ILM * > * イレイジャーコーディング * を選択します。

   イレイジャーコーディングのプロファイルページが表示されます。



2. [作成（ Create ）] をクリックします。

   EC プロファイルの作成ダイアログボックスが表示されます。



3. イレイジャーコーディングプロファイルの一意の名前を入力します。

   イレイジャーコーディングプロファイル名は一意である必要があります。既存のプロファイルの名前を使用すると、そのプロファイルが非アクティブ化されていても、検証エラーが発生します。

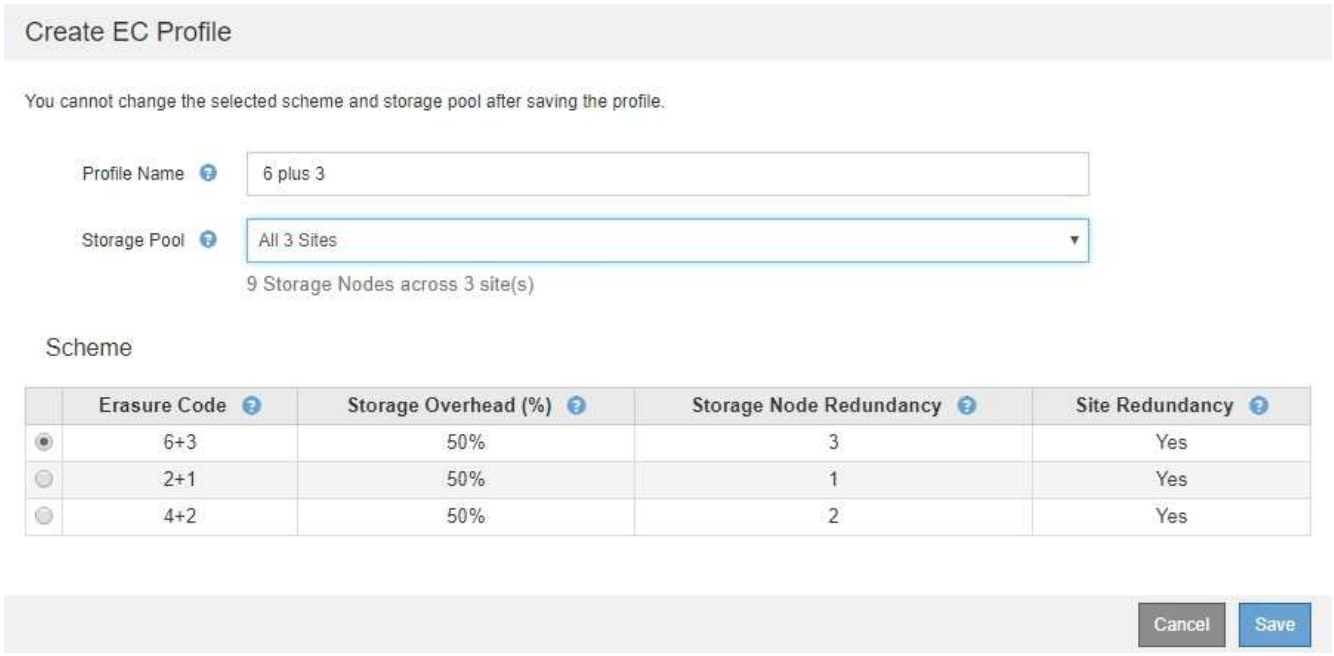
   > ILM ルールの配置手順で、イレイジャーコーディングプロファイル名がストレージプール名に追加されます。

4. このイレイジャーコーディングプロファイル用に作成したストレージプールを選択します。

   > グリッドにサイトが 1 つしかない場合、デフォルトのストレージプール、すべてのストレージノード、またはデフォルトサイトであるすべてのサイトを含むストレージプールは使用できません。これにより、 2 つ目のサイトが追加された場合にイレイジャーコーディングプロファイルが無効になるのを防ぐことができます。

   > ストレージプールにサイトが 2 つだけ含まれている場合、そのストレージプールをイレイジャーコーディングに使用することはできません。2 つのサイトを含むストレージプールではイレイジャーコーディングスキームを使用できません。

   ストレージプールを選択すると、プール内のストレージノードとサイトの数に基づいて、使用可能なイレイジャーコーディングスキームのリストが表示されます。



使用可能な各イレイジャーコーディングスキームについて次の情報が表示されます。

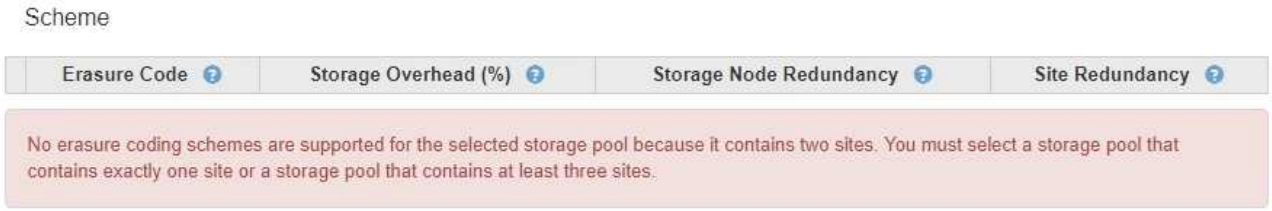
- * イレイジャーコーディングコード * ：イレイジャーコーディングスキームの名前。データフラグメント + パリティフラグメントの形式で表されます。
- * ストレージオーバーヘッド（ % ） * ：オブジェクトのデータサイズを基準とした、パリティフラグメントに必要な追加のストレージ。ストレージオーバーヘッド = パリティフラグメントの総数 / データフラグメントの総数。
- * ストレージノードの冗長性 * ：オブジェクトデータの読み出しが可能な状態で、損失が許容されるストレージノードの数。
- * Site Redundancy * ：選択したイレイジャーコーディングで、サイトが 1 つ失われてもオブジェクトデータの読み出しが可能かどうかを示します。

  サイトの冗長化を確保するには、選択したストレージプールに複数のサイトが含まれていて、どのサイトが失われても十分な数のストレージノードが各サイトに配置されている必要があります。たとえば、 6+3 のイレイジャーコーディングスキームを使用してサイトの冗長化を確保するためには、選択したストレージプールにサイトが 3 つ以上含まれていて、各サイトにストレージノードが 3 つ以上含まれている必要があります。

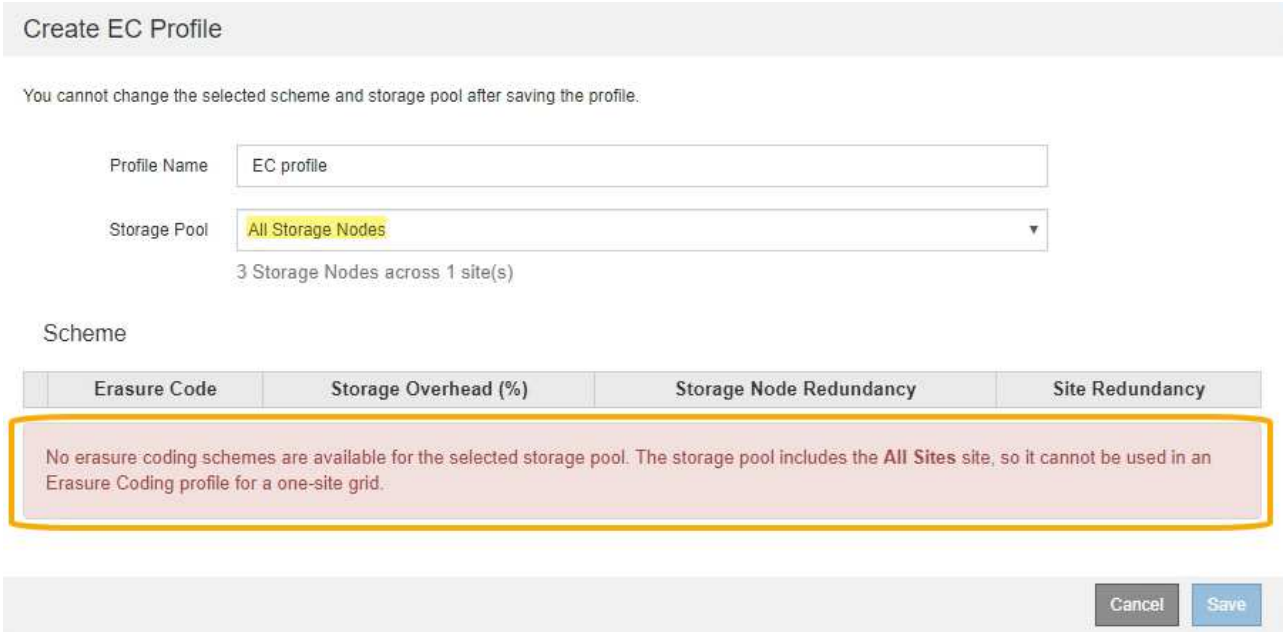
  メッセージは次の場合に表示されます。

- 選択したストレージプールではサイトの冗長性が確保されません。選択したストレージプールに含まれているサイトが 1 つだけの場合は、次のメッセージが表示されます。ノードを障害から保護する場合は、 ILM ルールでこのイレイジャーコーディングプロファイルを使用できます。

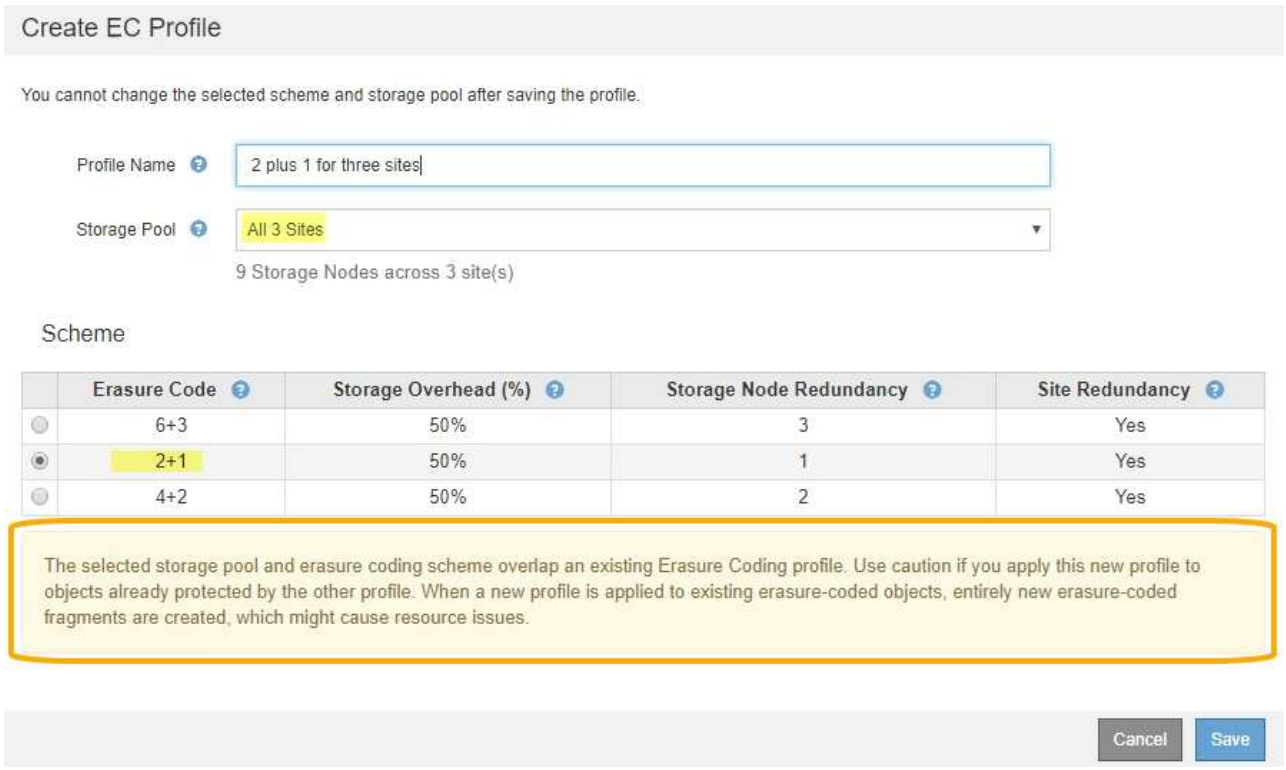
- 選択したストレージプールがイレイジャーコーディングスキームの要件を満たしていません。たとえば、選択したストレージプールに含まれているサイトが 2 つだけの場合は、次のメッセージが表示されます。イレイジャーコーディングを使用してオブジェクトデータを保護する場合は、サイトが 1 つだけ、または 3 つ以上のストレージプールを選択する必要があります。



- グリッドに含まれるサイトが 1 つだけで、デフォルトのストレージプールかすべてのストレージノード、またはデフォルトサイトであるすべてのサイトを含むストレージプールを選択した場合。



- 選択したイレイジャーコーディングスキームとストレージプールが、別のイレイジャーコーディングプロファイルと重複しています。



この例では、別のイレイジャーコーディングプロファイルで 2+1 スキームを使用しており、他のプロファイルのストレージプールでも All 3 Sites ストレージプールのいずれかのサイトを使用しているため、警告メッセージが表示されます。

この新しいプロファイルを作成することはできませんが、 ILM ポリシーでプロファイルの使用を開始する際は十分に注意する必要があります。この新しいプロファイルを他のプロファイルですでに保護されている既存のイレイジャーコーディングオブジェクトに適用すると、 StorageGRID によって完全に新しいオブジェクトフラグメントのセットが作成されます。既存の 2+1 フラグメントは再利用されない。イレイジャーコーディングスキームが同じであっても、あるイレイジャーコーディングプロファイルから別のプロファイルに移行すると、リソースの問題が発生する可能性があります。

5. 複数のイレイジャーコーディングスキームが表示される場合は、使用するスキームを 1 つ選択します。

   どのイレイジャーコーディングスキームを使用するかを決めるにあたっては、フォールトトレランス（パリティセグメントの数が多いほど高くなる）と修復に必要なネットワークトラフィック（フラグメントの数が多いほどネットワークトラフィックも増加する）のバランスを考慮する必要があります。たとえば、4+2 と 6+3 のどちらかのスキームを選ぶ場合、パリティを増やしてフォールトトレランスを向上させる必要がある場合は 6+3 のスキームを選択します。ノード修復時のネットワーク使用量を削減するためにネットワークリソースが制限されている場合は、 4+2 のスキームを選択します。

6. [保存（ Save ）] をクリックします。

イレイジャーコーディングプロファイルの名前変更

イレイジャーコーディングプロファイルの名前を変更して、プロファイルの内容をより明確にすることができます。

必要なもの

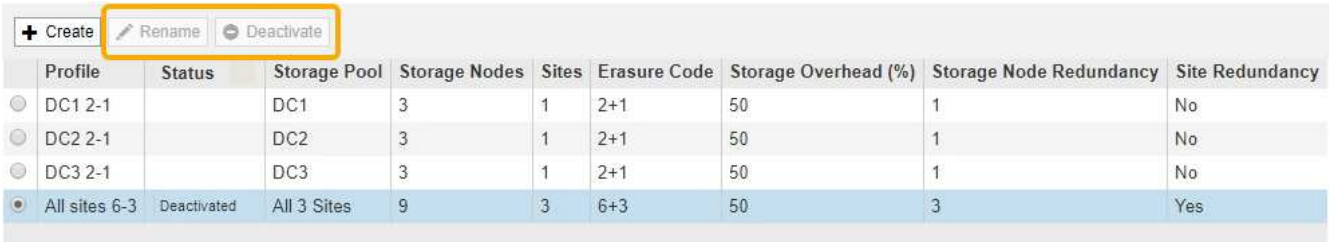
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

- 特定のアクセス権限が必要です。

手順

1. ILM * > * イレイジャーコーディング * を選択します。

   イレイジャーコーディングのプロファイルページが表示されます。[名前の変更 * （ Rename * ）] ボタンと [非活動化 * （ Deactivate * ）] ボタンの両方が無効



2. 名前を変更するプロファイルを選択します。

   [名前の変更 * （ Rename * ）] ボタンと [非活動化 * （ Deactivate * ）] ボタンが有効

3. [名前の変更 *] をクリックします。

   EC プロファイルの名前変更ダイアログボックスが表示されます。

4. イレイジャーコーディングプロファイルの一意の名前を入力します。

   ILM ルールの配置手順で、イレイジャーコーディングプロファイル名がストレージプール名に追加されます。

   イレイジャーコーディングプロファイル名は一意である必要があります。既存のプロファイルの名前を使用すると、そのプロファイルが非アクティブ化されていても、検証エラーが発生します。

5. [保存（ Save ）] をクリックします。

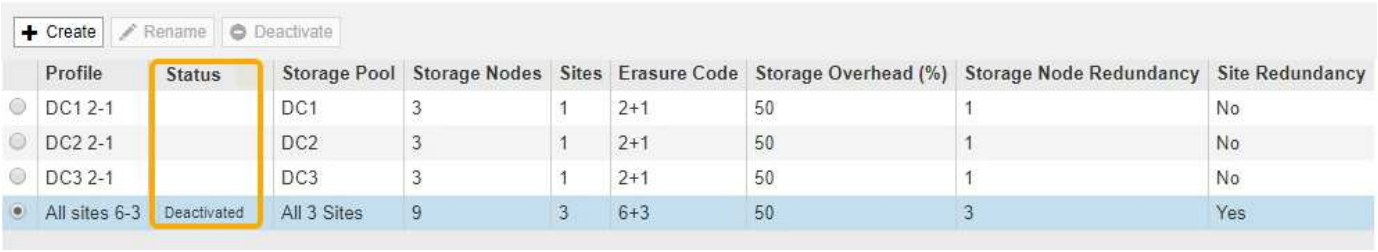
使用する予定がなくなったイレイジャーコーディングプロファイルや、プロファイルが現在どの ILM ルールでも使用されていないプロファイルは、非アクティブ化できます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。
- イレイジャーコーディングされたデータ修復処理または運用停止手順が実行中でないことを確認しておく必要があります。いずれかの処理の実行中にイレイジャーコーディングプロファイルを非アクティブ化しようとすると、エラーメッセージが返されます。

このタスクについて

イレイジャーコーディングプロファイルを非アクティブ化しても、プロファイルはイレイジャーコーディングのプロファイルページに表示されますが、ステータスは * deactivated* になります。



Profile	Status	Storage Pool	Storage Nodes	Sites	Erasure Code	Storage Overhead (%)	Storage Node Redundancy	Site Redundancy
DC1 2-1		DC1	3	1	2+1	50	1	No
DC2 2-1		DC2	3	1	2+1	50	1	No
DC3 2-1		DC3	3	1	2+1	50	1	No
All sites 6-3	Deactivated	All 3 Sites	9	3	6+3	50	3	Yes

非アクティブ化されたイレイジャーコーディングプロファイルは使用できなくなります。非アクティブ化したプロファイルは、 ILM ルールの配置手順の作成時に表示されません。非アクティブ化したプロファイルは再アクティブ化できません。

StorageGRID では、次のいずれかに該当する場合はイレイジャーコーディングプロファイルを非アクティブ化できません。

- イレイジャーコーディングプロファイルは現在 ILM ルールで使用されています。
- ILM ルールではイレイジャーコーディングプロファイルが使用されなくなりましたが、プロファイルのオブジェクトデータとパリティのフラグメントはまだ存在します。

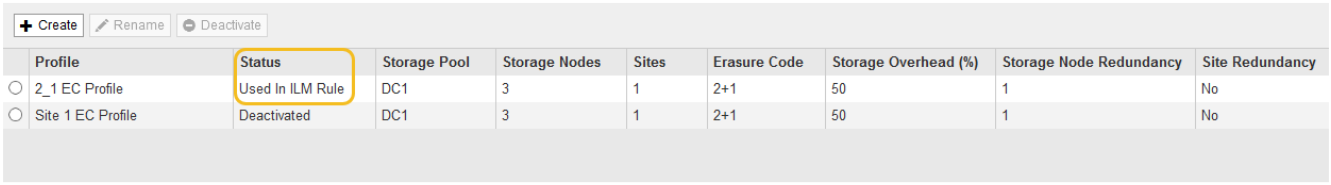
手順

1. ILM * > * イレイジャーコーディング * を選択します。

   イレイジャーコーディングのプロファイルページが表示されます。[名前の変更 * （ Rename * ）] ボタンと [非活動化 * （ Deactivate * ）] ボタンの両方が無効

2. ステータス * 列を確認して、非アクティブ化するイレイジャーコーディングプロファイルが ILM ルールで使用されていないことを確認します。

   ILM ルールで使用されているイレイジャーコーディングプロファイルは非アクティブ化できません。この例では、少なくとも 1 つの ILM ルールで * 2_1 EC プロファイル * が使用されています。

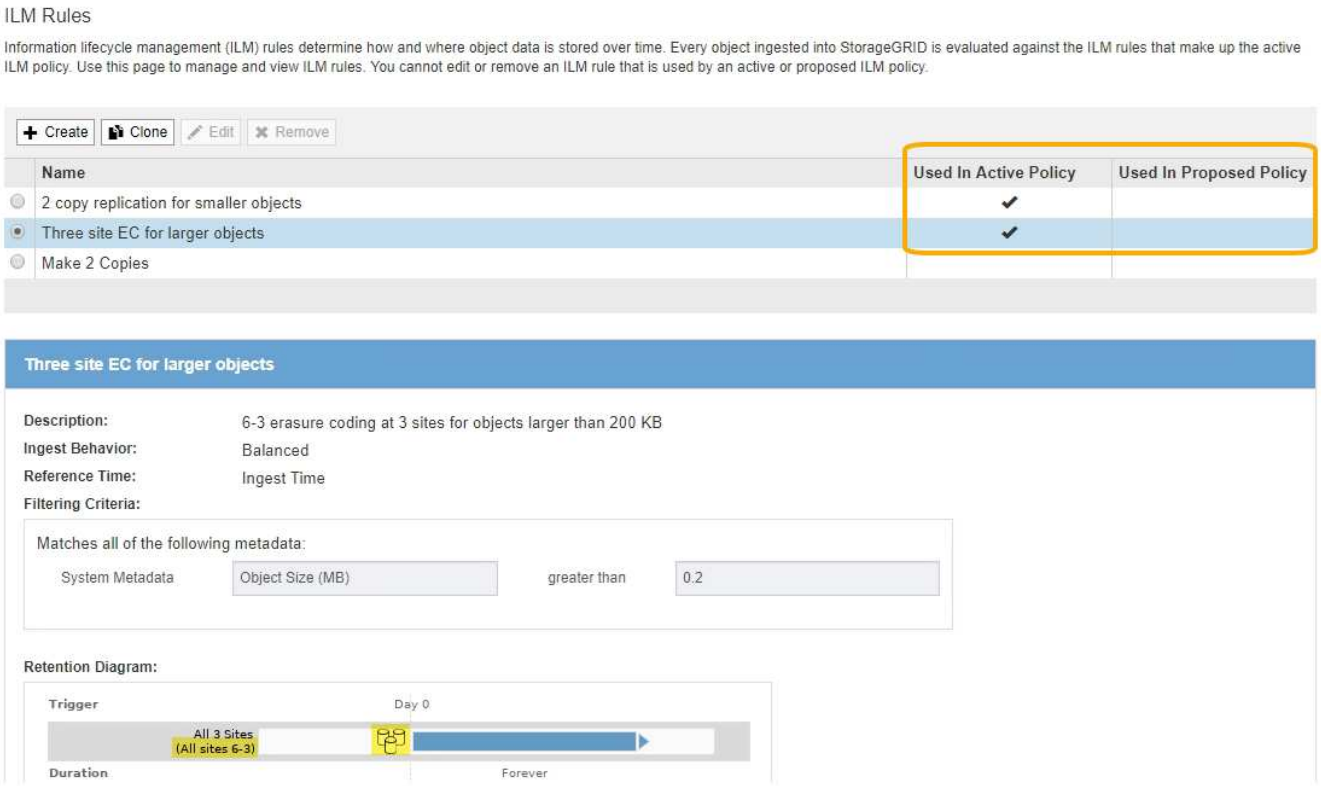


3. プロファイルが ILM ルールで使用されている場合は、次の手順を実行します。

   a. [* ILM*>* Rules] を選択します。

   b. 表示されているルールごとに、オプションボタンを選択し、保持図を確認して、非アクティブ化するイレイジャーコーディングプロファイルがルールで使用されているかどうかを判断します。

      この例では、「 3 サイト EC for larger objects 」ルールで、「 * All 3 Sites * 」というストレージプールと「 * all sites 6+3 * イレイジャーコーディングプロファイル」を使用しています。イレイジャーコーディングプロファイルは次のアイコンで表されます。 



   a. 非アクティブ化するイレイジャーコーディングプロファイルを ILM ルールが使用している場合は、そのルールがアクティブな ILM ポリシーとドラフトポリシーのどちらで使用されているかを確認します。

      この例では、アクティブな ILM ポリシーで大容量オブジェクト * ルール用の * 3 サイト EC が使用されています。

   b. イレイジャーコーディングプロファイルの使用場所に基づいて、表に記載された追加の手順を実行します。

プロファイルはどこで使用されていますか？	プロファイルを非アクティブ化する前に実行する追加手順	追加の手順を参照してください
ILM ルールでは使用されません	追加の手順は必要ありません。この手順に進みます。	_ なし _
ILM ポリシーで使用されたことのない ILM ルール	i. 該当する ILM ルールをすべて編集または削除します。ルールを編集する場合は、イレイジャーコーディングプロファイルを使用するすべての配置を削除します。 ii. この手順に進みます。	"ILMルールおよびILMポリシーの操作"
アクティブな ILM ポリシーに現在含まれている ILM ルール	i. アクティブポリシーのクローンを作成します。 ii. イレイジャーコーディングプロファイルを使用する ILM ルールを削除します。 iii. オブジェクトを確実に保護するために、新しい ILM ルールを 1 つ以上追加します。 iv. 新しいポリシーを保存、シミュレート、およびアクティブ化します。 v. 新しいポリシーが適用され、追加した新しいルールに基づいて既存のオブジェクトが新しい場所に移動されるまで待ちます。 ◦ 注： StorageGRID システムのオブジェクト数とサイズによっては、新しい ILM ルールに基づいてオブジェクトを新しい場所に移動するのに数週間から数カ月かかる場合があります。 データに関連付けられたままイレイジャーコーディングプロファイルを安全に非アクティブ化しようとしても、非アクティブ化処理は失敗します。プロファイルを非アクティブ化する準備ができていない場合は、エラーメッセージが表示されます。 vi. ポリシーから削除したルールを編集または削除します。ルールを編集する場合は、イレイジャーコーディングプロファイルを使用するすべての配置を削除します。 vii. この手順に進みます。	• "ILMポリシーを作成する" • "ILMルールおよびILMポリシーの操作"

プロファイルはどこで使用されていますか？	プロファイルを非アクティブ化する前に実行する追加手順	追加の手順を参照してください
ドラフトの ILM ポリシーに現在含まれている ILM ルール	i. ドラフトポリシーを編集します。 ii. イレイジャーコーディングプロファイルを使用する ILM ルールを削除します。 iii. すべてのオブジェクトが保護されるように 1 つ以上の新しい ILM ルールを追加します。 iv. ドラフトポリシーを保存します。 v. ポリシーから削除したルールを編集または削除します。ルールを編集する場合は、イレイジャーコーディングプロファイルを使用するすべての配置を削除します。 vi. この手順に進みます。	• "ILMポリシーを作成する" • "ILMルールおよびILMポリシーの操作"
ILM 履歴ポリシー内の ILM ルール	i. ルールを編集または削除します。ルールを編集する場合は、イレイジャーコーディングプロファイルを使用するすべての配置を削除します。（このルールは履歴ポリシーに履歴ルールとして表示されます）。 ii. この手順に進みます。	• "ILMルールおよびILMポリシーの操作"

c. プロファイルが ILM ルールで使用されていないことを確認するには、イレイジャーコーディングのプロファイルページをリフレッシュしてください。

4. プロファイルが ILM ルールで使用されていない場合は、ラジオボタンを選択し、 * Deactivate * を選択します。

[EC プロファイルを非活動化（ Deactivate EC Profile ）] ダイアログボックスが表示

5. プロファイルを非活動化してもよい場合は、 [* 非活動化 * （ * Deactivate * ）] を選択します。

◦ StorageGRID でイレイジャーコーディングプロファイルを非アクティブ化できる場合、ステータスは * deactivated* になります。これで、どの ILM ルールにもこのプロファイルを選択できなくなりました。

◦ StorageGRID がプロファイルを非アクティブ化できない場合は、エラー・メッセージが表示されます。たとえば、オブジェクトデータがまだこのプロファイルに関連付けられている場合は、エラーメ

ッセージが表示されます。無効化プロセスを再度実行する前に、数週間待つ必要がある場合があります。

リージョンの設定（オプション、**S3**のみ）

ILM ルールは S3 バケットが作成されたリージョンに基づいてオブジェクトをフィルタリングできるため、オブジェクトのリージョンによって異なるストレージに格納できます。S3 バケットのリージョンをルールのフィルタとして使用する場合は、システム内のバケットで使用できるリージョンを最初に作成しておく必要があります。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

このタスクについて

S3 バケットを作成する際は、特定のリージョンにバケットを作成するように指定できます。リージョンを指定すると地理的にユーザにより近い場所にバケットを配置でき、レイテンシの最適化、コストの最小化、規制要件への対応を実現できます。

ILM ルールの作成時には、 S3 バケットに関連付けられているリージョンを高度なフィルタとして使用できます。たとえば、 us-west-2 リージョンで作成された S3 バケット内のオブジェクトにのみ適用するルールを作成できます。そのうえで、そのリージョン内のデータセンターサイトにあるストレージノードにオブジェクトのコピーを配置してレイテンシを最適化するように指定できます。

リージョンを設定する場合は、次の注意事項に従ってください。

- デフォルトでは、すべてのバケットが us-east-1 リージョンに属しているとみなされます。
- Tenant Manager またはテナント管理 API を使用してバケットを作成するとき、または S3 の PUT Bucket API 要求の LocationConstraint 要求要素を使用してバケットを作成するときにデフォルト以外のリージョンを指定する前に、 Grid Manager を使用してリージョンを作成する必要があります。StorageGRID で定義されていないリージョンを PUT Bucket 要求で使用すると、エラーが発生します。
- S3 バケットの作成時には正確なリージョン名を使用する必要があります。リージョン名では大文字と小文字が区別されます。 2 文字以上 32 文字以下にする必要があります。有効な文字は、数字、アルファベット、およびハイフンです。

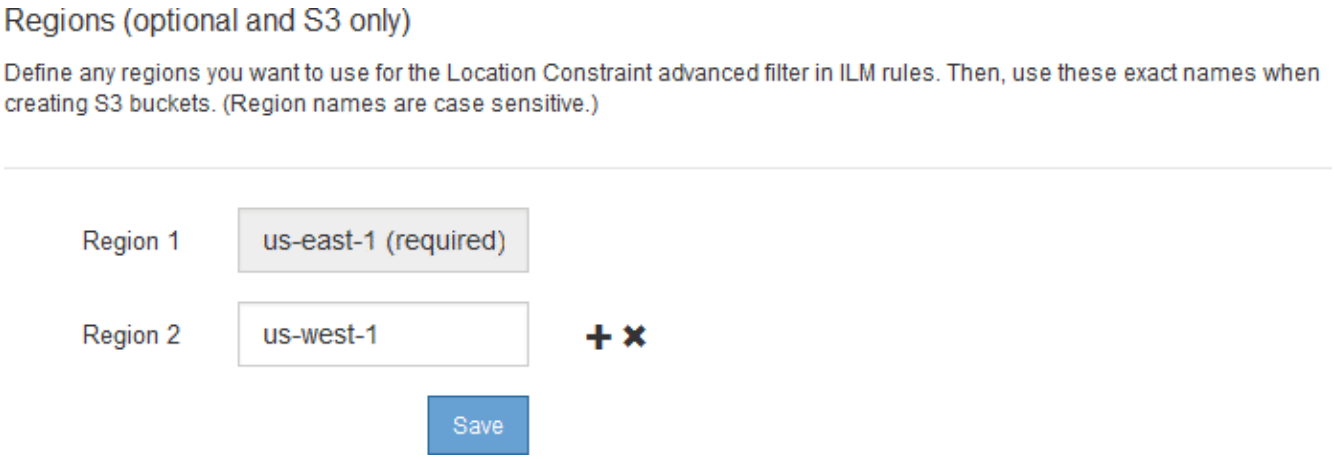
> EU は、 eu-west-1 のエイリアスとはみなされません。EU または eu-west-1 リージョンを使用する場合は、正確な名前を使用する必要があります。

- アクティブな ILM ポリシーやドラフトの ILM ポリシー内で現在使用されているリージョンを削除または変更することはできません。
- ILM ルールで高度なフィルタとして使用されているリージョンが無効な場合でも、そのルールをドラフトポリシーに追加できます。ただし、ドラフトポリシーを保存またはアクティブ化しようとするとエラーが発生します。（無効なリージョンは、 ILM ルールで高度なフィルタとして使用しているリージョンをあとで削除した場合や、グリッド管理 API を使用してルールを作成し、定義していないリージョンを指定した場合に発生することがあります）。
- あるリージョンを使用して S3 バケットを作成したあとにそのリージョンを削除した場合、高度なフィルタ「 Location Constraint 」を使用してそのバケット内のオブジェクトを検索するにはリージョンを再び追加する必要があります。

手順

1. [* ILM*>* Regions*] を選択します。

   Regions ページが表示され、現在定義されているリージョンがリストされます。*領域1 *はデフォルト領域を示します。 `us-east-1`（変更または削除できません）。

2. リージョンを追加するには：

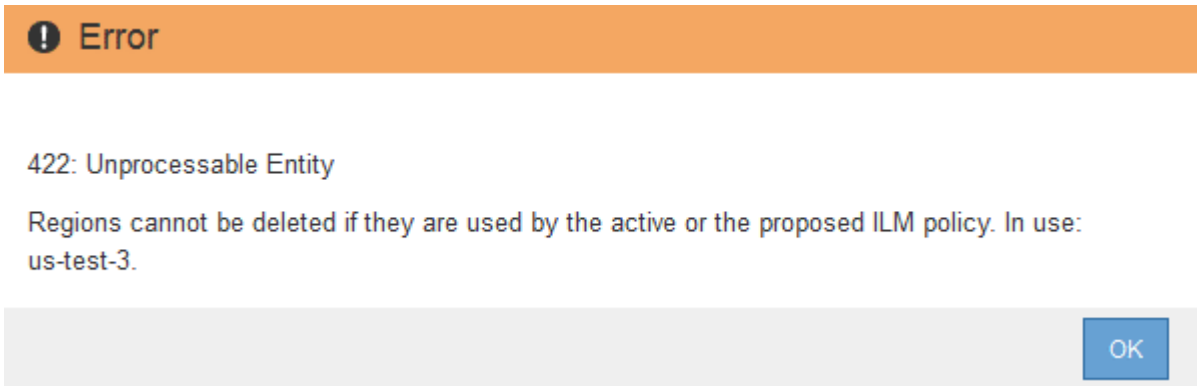
   a. 挿入アイコンをクリックします ✚ アイコン"] をクリックします。

   b. S3 バケットの作成時に使用するリージョンの名前を入力します。

      対応する S3 バケットの作成時には、正確なリージョン名を LocationConstraint 要求の要素として使用する必要があります。

3. 未使用の領域を削除するには、削除アイコンをクリックします ✖。

   アクティブポリシーまたはドラフトポリシーで現在使用されているリージョンを削除しようとすると、エラーメッセージが表示されます。

4. 変更が完了したら、*保存*をクリックします。

   Create ILM Rule ウィザードの Advanced Filtering ページの * Location Constraint * リストからこれらのリージョンを選択できるようになりました。

関連情報

"ILMルールで高度なフィルタを使用する"

ILM ルールを使用して、時間の経過に伴うオブジェクトデータの配置を管理できます。ILM ルールを作成するには、 Create ILM Rule ウィザードを使用します。

作業を開始する前に

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。
- このルール環境 を使用するテナントアカウントを指定する場合は、Tenant Accounts権限が必要です。または、各アカウントのアカウントIDを確認しておく必要があります。
- 最終アクセス時間のメタデータでオブジェクトをフィルタリングするルールの場合、 S3 の場合はバケットで、 Swift の場合はコンテナで最終アクセス時間の更新が有効になっている必要があります。
- レプリケートコピーを作成する場合は、使用するストレージプールまたはクラウドストレージプールを設定しておく必要があります。
- イレイジャーコーディングコピーを作成する場合は、イレイジャーコーディングプロファイルを設定しておく必要があります。
- に精通している必要があります "取り込みのデータ保護オプション"。
- S3オブジェクトロックで使用する準拠ルールを作成する必要がある場合は、を参照しておく必要があります "S3 オブジェクトのロックの要件"。

> ポリシーのデフォルトのILMルールを作成するには、代わりに次の手順 を使用します。 "デフォルトのILMルールを作成する"。

このタスクについて

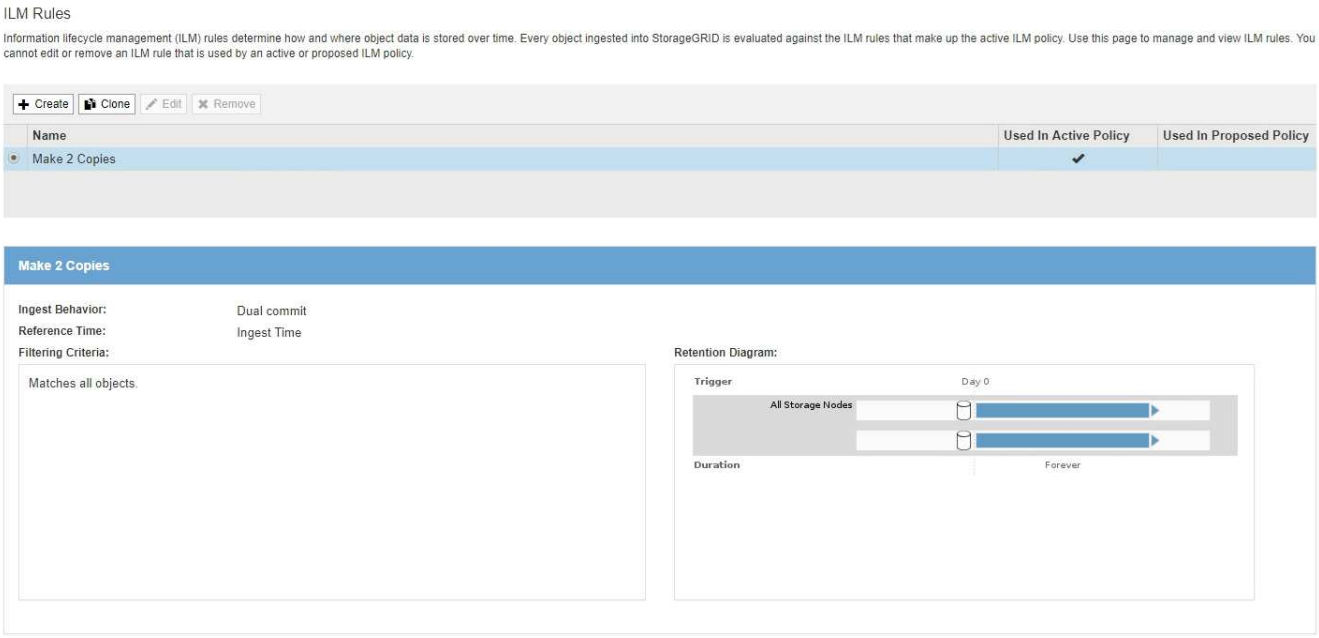
ILM ルールを作成する場合は、次の点

- StorageGRID システムのトポロジとストレージ構成を考慮します。
- 作成するオブジェクトコピーのタイプ（レプリケートまたはイレイジャーコーディング）および各オブジェクトに必要なコピー数を検討します。
- StorageGRID システムに接続するアプリケーションで使用されるオブジェクトメタデータのタイプを決定します。ILM ルールは、メタデータに基づいてオブジェクトをフィルタリングします。
- 時間の経過に伴うオブジェクトコピーの配置先を検討します。
- 取り込み時のデータ保護に使用するオプション（Balanced、Strict、Dual commit）を決定します。

手順

1. [* ILM*>* Rules] を選択します。

   ILM ルールページが表示され、組み込みのルールである Make 2 Copies が選択されます。



StorageGRID システムでグローバルな S3 オブジェクトのロック設定が有効になっている場合、 ILM ルールページの外観は少し異なります。サマリテーブルには * 準拠 * 列が含まれ、選択したルールの詳細には * 準拠 * フィールドが含まれます。

2. 「 * Create * 」を選択します。

   Create ILM Rule ウィザードの Step 1 （ Define Basics ）が表示されます。基本の定義ページを使用して、ルール環境 で使用するオブジェクトを定義します。

関連情報

"S3 を使用する"

"Swift を使用します"

"イレイジャーコーディングプロファイルの設定"

"ストレージプールを設定しています"

"クラウドストレージプールの使用"

"取り込みのデータ保護オプション"

"S3オブジェクトロックでオブジェクトを管理する"

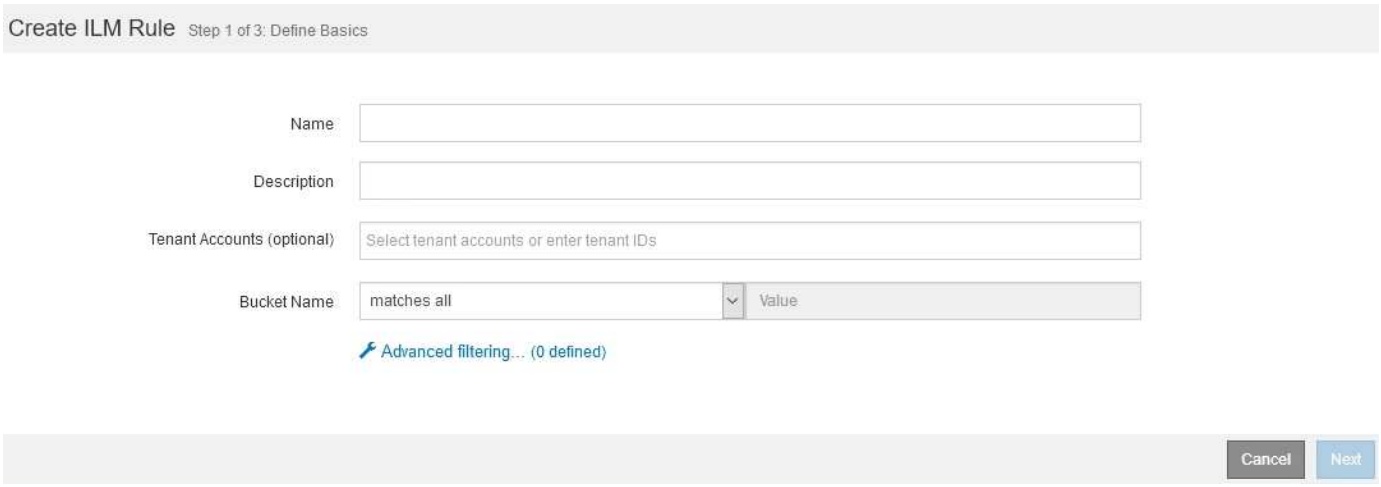
ステップ **1/3** ：基本事項を定義します

Create ILM Rule ウィザードのステップ 1 （ Define Basics ）では、ルールの基本フィルタと高度なフィルタを定義できます。

このタスクについて

StorageGRID は、 ILM ルールに照らしてオブジェクトを評価する際に、オブジェクトメタデータをルールのフィルタと比較します。オブジェクトメタデータがすべてのフィルタに一致した場合、 StorageGRID はルー

ルを使用してオブジェクトを配置します。すべてのオブジェクトに適用するルールを設計したり、 1 つ以上のテナントアカウントやバケット名などの基本的なフィルタや、オブジェクトのサイズやユーザメタデータなどの高度なフィルタを指定したりできます。



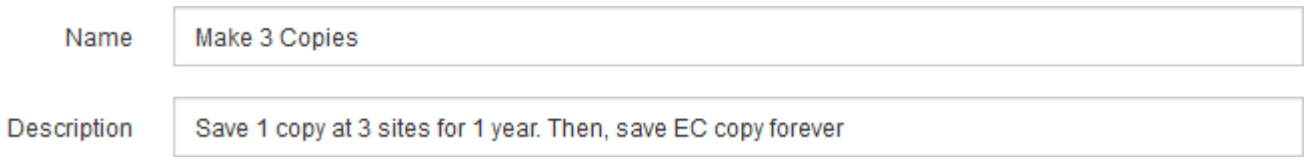
手順

1. [* 名前 *] フィールドに、ルールの一意の名前を入力します。

   1~64 文字で指定する必要があります。

2. 必要に応じて、ルールの短い概要 を * 概要 * フィールドに入力します。

   あとから識別しやすいように、ルールの目的や機能を指定してください。



3. 必要に応じて、このルールを適用する S3 または Swift テナントアカウントを 1 つ以上選択します。このルールですべてのテナントを環境 に設定する場合は、このフィールドを空白のままにします。

   Root Access権限またはTenant Accounts権限がない場合は、リストからテナントを選択できません。代わりに、テナント ID を入力するか、複数の ID をカンマで区切って入力します。

4. 必要に応じて、このルールを適用する S3 バケットまたは Swift コンテナを指定します。

   「 * matches all * 」が選択されている場合（デフォルト）、「環境 all S3 bucketes 」または「 Swift containers 」というルールが適用されます。

5. 必要に応じて、 ［ * 高度なフィルタリング * ］ を選択し、追加のフィルタを指定します。

   高度なフィルタを設定しない場合は、基本フィルタに一致するすべてのオブジェクトを環境 ルールに追加します。

> このルールでイレイジャーコーディングコピーを作成する場合は、「高度なフィルタリング」を選択します。次に、高度なフィルタ「* Object Size（MB）」を追加し、「 greater than 0.2 *」に設定します。サイズフィルタを使用すると、2MB以下のオブジェクトはイレイジャーコーディングされません。

6. 「 * 次へ * 」を選択します。

ステップ 2 （配置を定義）が表示されます。

関連情報

"ILM ルールのフィルタリングとは"

"ILMルールで高度なフィルタを使用する"

"ステップ 2 / 3 ：配置を定義する"

ILMルールで高度なフィルタを使用する

高度なフィルタを使用すると、メタデータに基づいて特定のオブジェクトにのみ適用する ILM ルールを作成できます。ルールに対して高度なフィルタを設定するには、照合するメタデータのタイプを選択し、演算子を選択して、メタデータ値を指定します。オブジェクトが評価されると、高度なフィルタに一致するメタデータを含むオブジェクトにのみ ILM ルールが適用されます。

次の表に、高度なフィルタで指定できるメタデータタイプ、各タイプのメタデータに使用できる演算子、および想定されるメタデータ値を示します。

メタデータタイプ	サポートされる演算子	メタデータ値
取り込み時間（マイクロ秒）	• が等しい • が同じではありません • より小さい • が次の値以下です • が次の値より大きい • が次の値以上である	オブジェクトが取り込まれた日時。 • 注：新しい ILM ポリシーをアクティブ化する際にリソースの問題が発生しないように、既存のオブジェクトの数が多い場合は、ルールで取り込み時間の高度なフィルタを使用することができます。既存のオブジェクトが不必要に移動されないようにするために、新しいポリシーが適用されるおおよその時間よりも長くなるように取り込み時間を設定します。
キーを押します	• が等しい • が同じではありません • が含まれます • にはを含めません • がで始まります • で始まるものではありません • が次の値で終わる • で終わることはありません	一意の S3 または Swift オブジェクトキーのすべてまたは一部。 たとえば、で終わるオブジェクトを照合できます `.txt` またはで開始します `test-object/`。

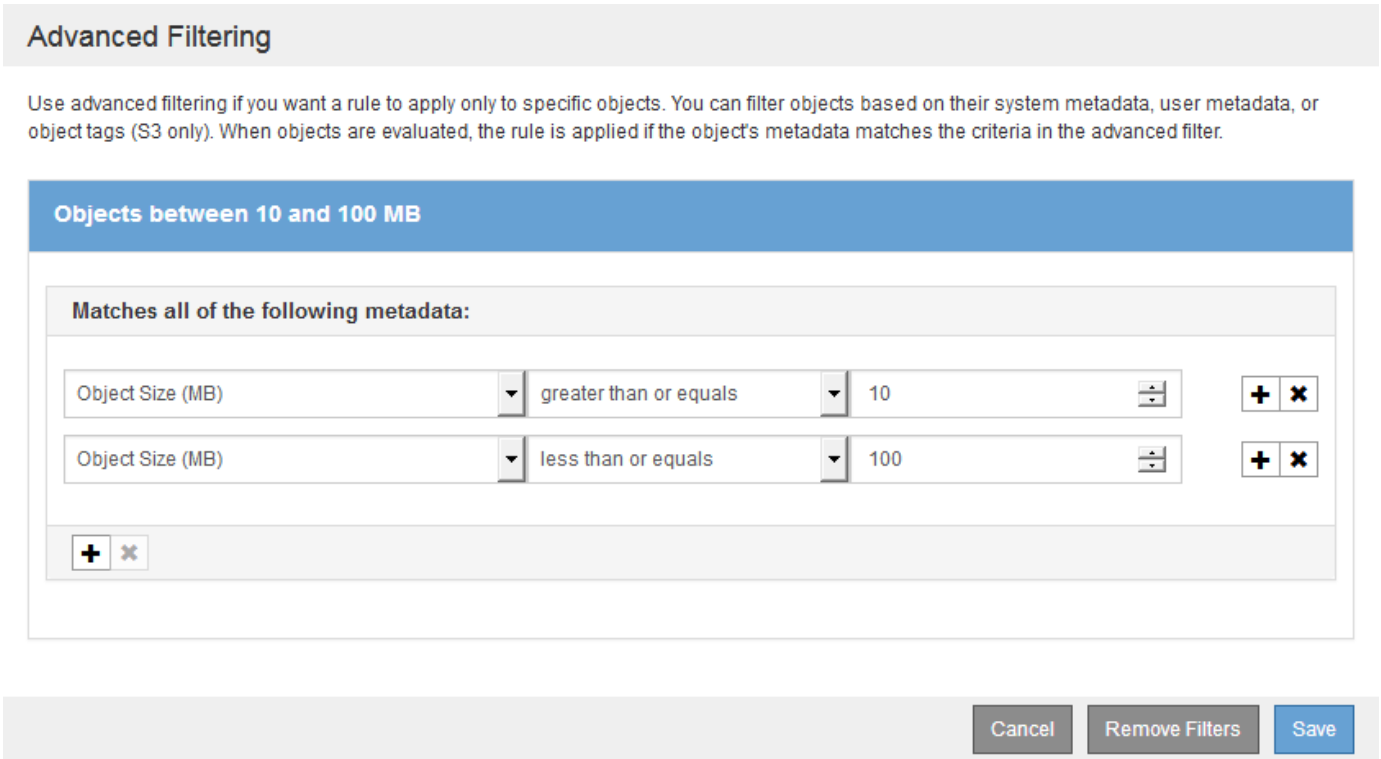
メタデータタイプ	サポートされる演算子	メタデータ値
最終アクセス時間（マイクロ秒）	• が等しい • が同じではありません • より小さい • が次の値以下です • が次の値より大きい • が次の値以上である • が存在します • は存在しません	オブジェクトが最後に読み出された（読み取られた、または表示された）日時。 • 注：最終アクセス時間を高度なフィルタとして使用する場合は、 S3 バケットまたは Swift コンテナに対して最終アクセス時間の更新を有効にする必要があります。 "ILMルールで最終アクセス日時を使用する"
場所の制約（ S3 のみ）	• が等しい • が同じではありません	S3 バケットが作成されたリージョン。表示されるリージョンを定義するには、 * ilm * > * Regions * を使用します。 • 注： us-east-1 の値は、 us-east-1 リージョンで作成されたバケット内のオブジェクト、およびリージョンが指定されていないバケット内のオブジェクトに一致します。 "リージョンの設定（オプション、S3のみ）"
オブジェクトサイズ（ MB ）	• が等しい • が次の値と等しくない • より小さい • が次の値以下です • が次の値より大きい • が次の値以上である	オブジェクトのサイズ（ MB 単位）。 1MB未満のオブジェクトサイズでフィルタリングするには、10進値を入力します。たとえば、イレイジャーコーディングコピーを作成するルールの場合は、「* Object Size（MB）* advanced filter」を「* greater than 0.2 *」に設定します。この設定により、200KB以下のオブジェクトにイレイジャーコーディングが使用されることはありません。 *注意：*ブラウザの種類とロケールの設定によって、小数点としてピリオドまたはカンマを使用する必要があるかどうかが制御されます。

メタデータタイプ	サポートされる演算子	メタデータ値
ユーザメタデータ	• が含まれます • が次の値で終わる • が等しい • が存在します • にはを含めません • で終わることはありません • が同じではありません • は存在しません • で始まるものではありません • がで始まります	キーと値のペア。 * User Metadata Name * はキー、 * User Metadata Value * は値です。 たとえば、ユーザメタデータがあるオブジェクトでフィルタリングするには、のように指定します `color=blue`、を指定します `color` ユーザーメタデータ名*の場合、 `equals` 演算子の場合は、および `blue` For * User Metadata Value *を参照してください。 • 注： * ユーザメタデータ名では大文字と小文字は区別されませんが、値では大文字と小文字が区別されます。
オブジェクトタグ（ S3 のみ）	• が含まれます • が次の値で終わる • が等しい • が存在します • にはを含めません • で終わることはありません • が同じではありません • は存在しません • で始まるものではありません • がで始まります	キーと値のペア。 * オブジェクトタグ名 * はキー、 * オブジェクトタグ値 * は値です。 たとえば、オブジェクトタグがのオブジェクトでフィルタリングする場合などです `Image=True`、を指定します `Image` *オブジェクトタグ名*の場合、 `equals` 演算子の場合は、および `True` for * Object Tag value *。 • 注： * オブジェクトタグ名とオブジェクトタグ値では、大文字と小文字が区別されます。これらの項目は、オブジェクトに対して定義されたとおりに正確に入力する必要があります。

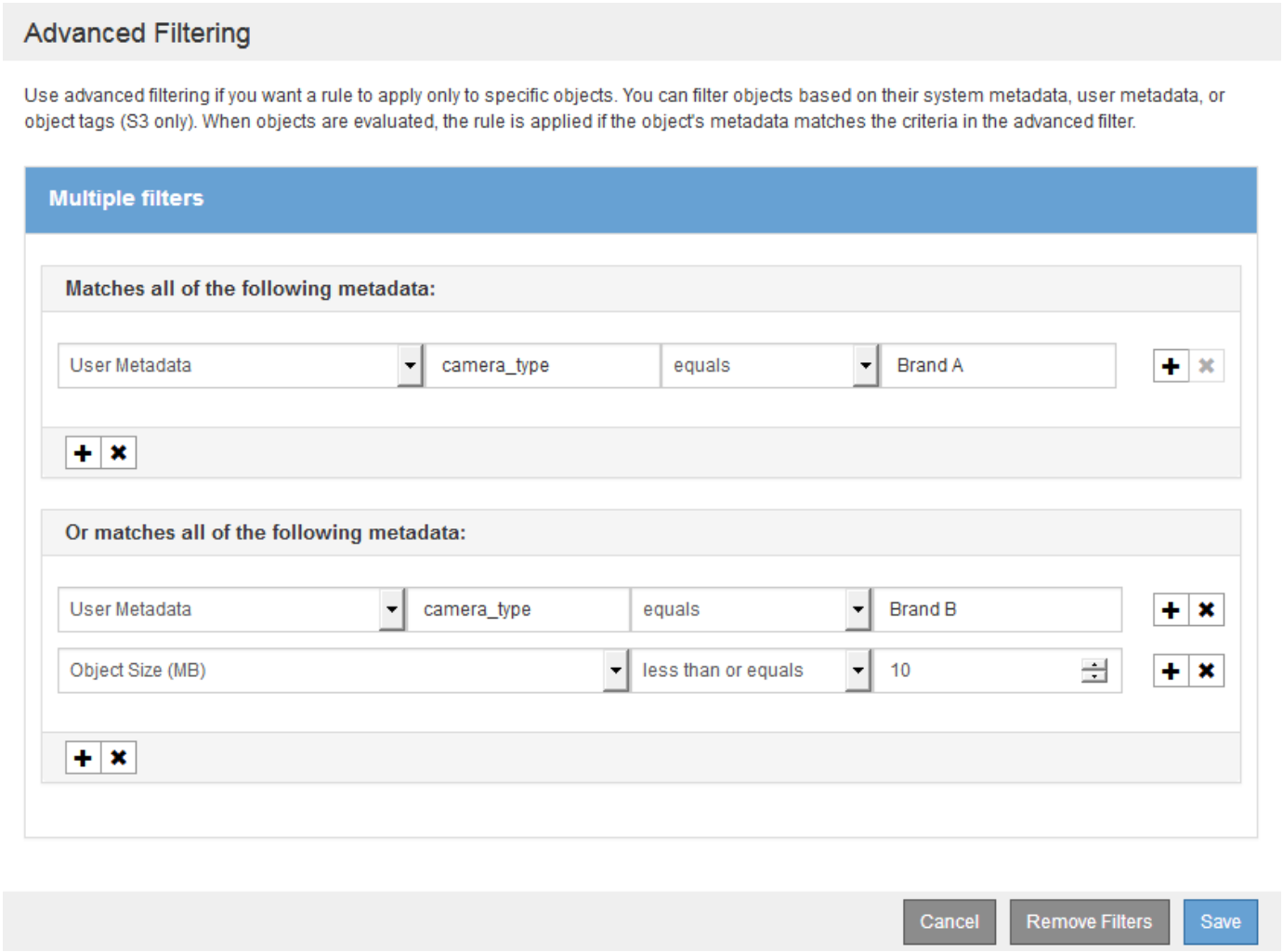
複数のメタデータタイプと値を指定する

高度なフィルタを定義する場合は、複数のタイプのメタデータと複数のメタデータ値を指定できます。たとえば、サイズが 10~100MB のオブジェクトに一致するルールを設定するには、 * Object Size * メタデータタイプを選択し、 2 つのメタデータ値を指定します。

- 最初のメタデータ値で 10MB 以上のオブジェクトを指定します。
- 2 番目のメタデータ値で 100MB 以下のオブジェクトを指定します。



複数のエントリを使用すると、照合するオブジェクトを正確に制御できます。次の例では、 camera_type ユーザメタデータの値が Brand A または Brand B の環境 オブジェクトをルールします。ただし、ルールでは、10MB より小さい Brand B のオブジェクトのみが環境 されます。



関連情報

"ILMルールで最終アクセス日時を使用する"

"リージョンの設定（オプション、S3のみ）"

ステップ **2 / 3** ：配置を定義する

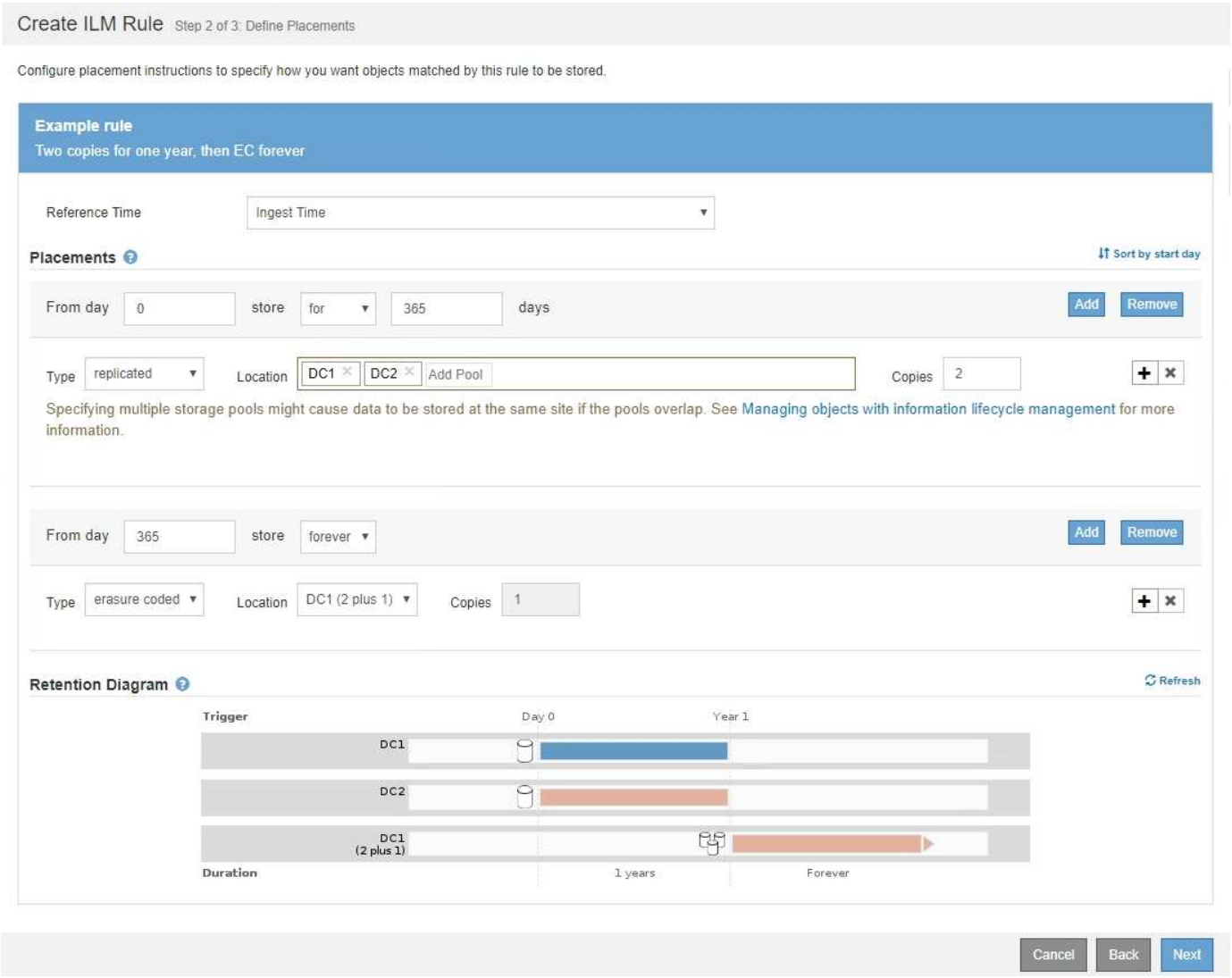
Create ILM Rule ウィザードのステップ 2 （配置を定義）では、オブジェクトを格納する期間、コピーのタイプ（レプリケートまたはイレイジャーコーディング）、格納場所、およびコピーの数を決定する配置手順を定義できます。

このタスクについて

ILM ルールには 1 つ以上の配置手順を含めることができます。各配置手順環境 は一定期間です。複数の手順を使用する場合は、期間が連続していて、少なくとも 1 つの手順が 0 日目に開始されている必要があります。手順は無期限に、またはオブジェクトコピーが不要になるまで継続できます。

複数のタイプのコピーを作成する場合や、期間中に別々の場所を使用する場合は、各配置手順に複数の行を追加することができます。

この ILM ルールの例では、最初の 1 年間にレプリケートコピーを 2 つ作成します。各コピーは、別々のサイトのストレージプールに保存されます。1 年後、 2+1 のイレイジャーコーディングコピーが作成され、 1 つのサイトにのみ保存されます。



手順

1. [* 基準時間 * （ * Reference Time * ）] で、配置手順の開始時間の計算に使用する時間のタイプを選択します。

オプション	説明
取り込み時間	オブジェクトが取り込まれた時間。
最終アクセス時間	オブジェクトが最後に読み出された（読み取られた、または表示された）時間。 • 注：このオプションを使用するには、 S3 バケットまたは Swift コンテナに対する最終アクセス時間の更新が有効になっている必要があります。 "ILMルールで最終アクセス日時を使用する"

オプション	説明
最新でなくなった時間	新しいバージョンが取り込まれて最新バージョンになったことが原因で、あるオブジェクトバージョンが最新でなくなった時間。 • 注：最新でない時間は、バージョン管理が有効なバケット内の S3 オブジェクトにのみ適用されます。 このオプションを使用すると、最新でないオブジェクトバージョンをフィルタリングすることで、バージョン管理オブジェクトによるストレージへの影響を軽減できます。「例4：S3バージョン管理オブジェクトのILMルールとポリシー」を参照してください。
ユーザ定義の作成時間	ユーザ定義のメタデータで指定された時間。

準拠ルールを作成する場合は、 * 取り込み時間 * を選択する必要があります。

2. [配置（ Plations] ）セクションで、最初の期間の開始時間と期間を選択します。

   たとえば ' 最初の年のオブジェクトを格納する場所を指定することができます ("365 日の場合は 0 日 ")少なくとも 1 つの手順は 0 日目から開始する必要があります。

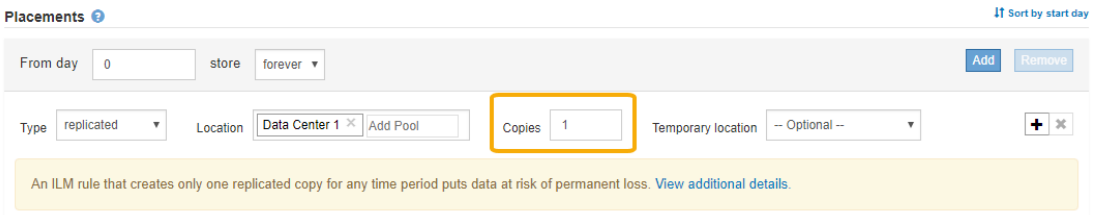
3. レプリケートコピーを作成する場合は、次の手順を実行します。
   a. [* タイプ **]** ドロップダウンリストから、 **[*Replicated-]** を選択します。
   b. ［ * 場所 * ］ フィールドで、追加するストレージ・プールごとに ［ * プールの追加 * ］ を選択します。
      - ストレージプールを 1 つしか指定しない場合、 StorageGRID は 1 つのオブジェクトのレプリケートコピーを任意のストレージノードに 1 つだけ格納できます。グリッドにストレージノードが 3 つある場合は、コピー数として 4 を選択すると、各ストレージノードにコピーが 1 つずつ、合計 3 つだけ作成されます。

        ILM placement unAchievable * アラートがトリガーされ、 ILM ルールを完全に適用できなかったことを示します。

      - 複数のストレージプールを指定する場合は、次の点に注意してください。 *
        - コピー数をストレージプール数よりも多くすることはできません。
        - コピーの数がストレージプールの数と同じ場合は、オブジェクトのコピーが 1 つずつ各ストレージプールに格納されます。
        - コピーの数がストレージプールの数より少ない場合、プール間のディスク使用量のバランスを維持し、サイトがオブジェクトのコピーを複数取得しないようにコピーが分散されます。
        - ストレージプールが重複している（同じストレージノードを含んでいる）場合は、オブジェクトのすべてのコピーが 1 つのサイトにのみ保存される可能性があります。そのため、デフォルトの All Storage Nodes ストレージプールと別のストレージプールは指定しないでください。

c. 作成するコピーの数を選択します。

コピー数を 1 に変更すると、警告が表示されます。ある期間にレプリケートコピーを 1 つしか作成しない ILM ルールには、データが永続的に失われるリスクがあります。ある期間にオブジェクトのレプリケートコピーが1つしか存在しない場合、ストレージノードに障害が発生したり、重大なエラーが発生すると、そのオブジェクトは失われます。また、アップグレードなどのメンテナンス作業中は、オブジェクトへのアクセスが一時的に失われます。



これらのリスクを回避するには、次のいずれかの操作を行います。

- 期間のコピー数を増やします。
- プラス記号アイコンをクリックします ➕ 期間中に追加のコピーを作成します。次に、別のストレージプールまたはクラウドストレージプールを選択します。
- 「 * Replicated * 」ではなく、「 * erasure Coded * 」を選択します。このルールですべての期間に対して複数のコピーを作成するようすでに定義されている場合は、この警告を無視してかまいません。

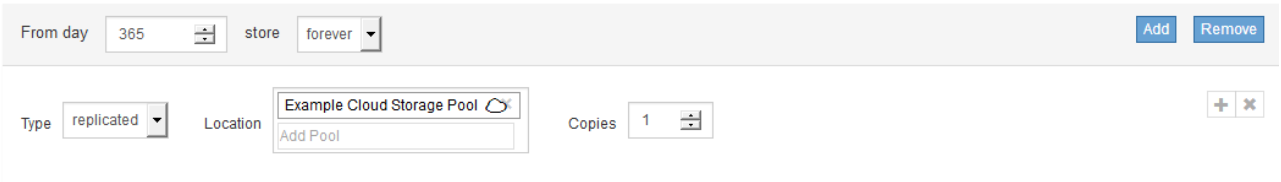
d. ストレージプールを 1 つしか指定していない場合は、「 * 一時的な場所 * 」フィールドは無視してください。

一時的な場所は廃止され、今後のリリースで削除される予定です。

4. オブジェクトをクラウドストレージプールに格納する場合は、次の手順を実行します。

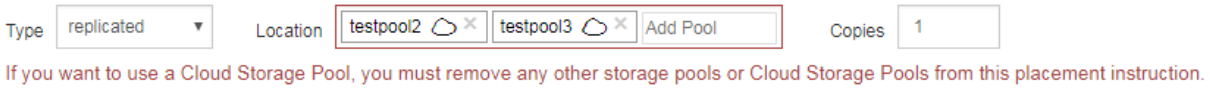
a. [* タイプ] ドロップダウンリストから、 **[*Replicated-]** を選択します。

b. [* 場所 *] フィールドで、 [* プールの追加 *] を選択します。次に、クラウドストレージプールを選択します。

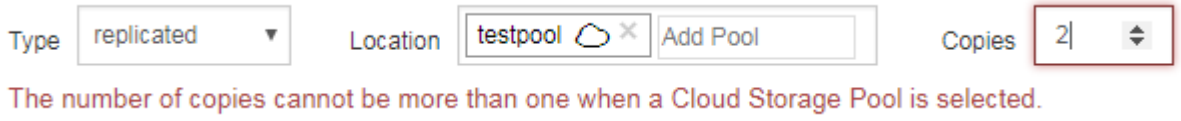


クラウドストレージプールを使用する場合は、次の点に注意してください。

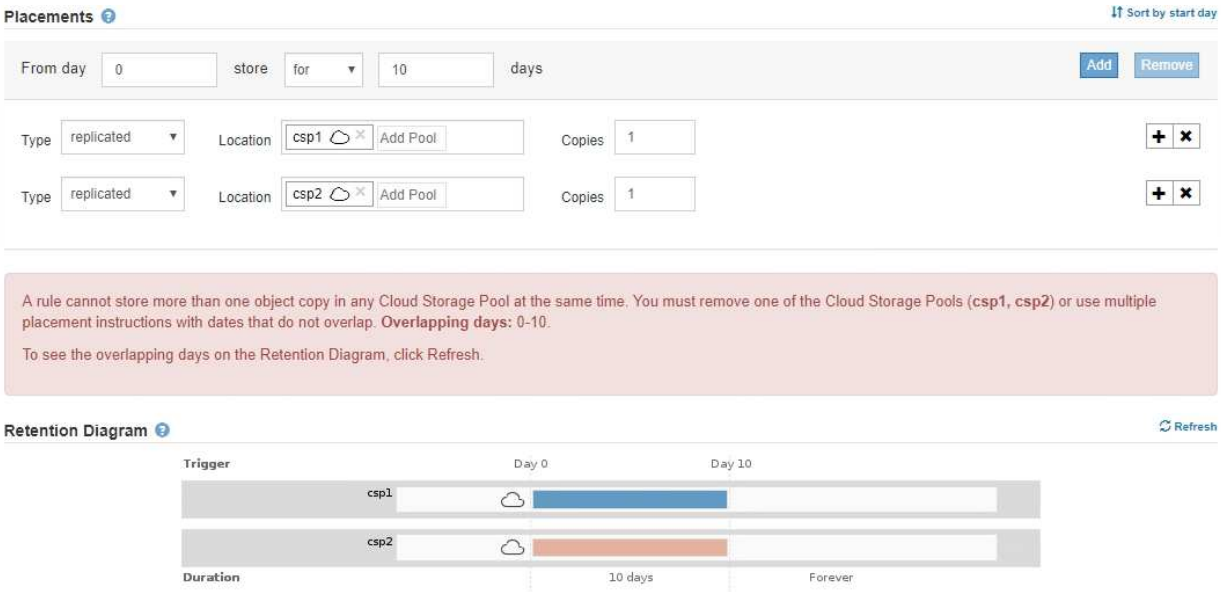
- 1 つの配置手順で複数のクラウドストレージプールを選択することはできません。同様に、クラウドストレージプールとストレージプールを同じ配置手順で選択することはできません。



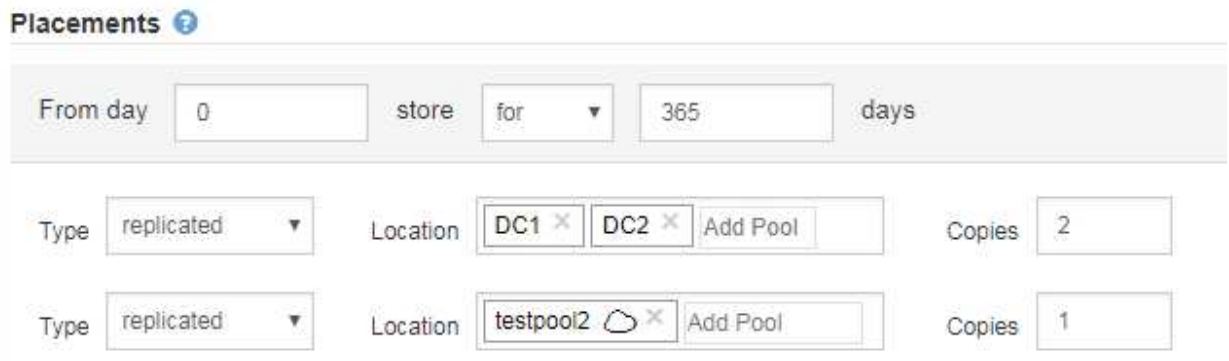
- 任意のクラウドストレージプールに格納できるオブジェクトのコピーは 1 つだけです。「 * Copies * 」を 2 以上に設定すると、エラーメッセージが表示されます。



- どのクラウドストレージプールにも、複数のオブジェクトコピーを同時に格納することはできません。クラウドストレージプールを使用する複数の配置で日付が重複している場合や、同じ配置内の複数の行でクラウドストレージプールを使用している場合は、エラーメッセージが表示されます。



- オブジェクトをレプリケートコピーまたはイレイジャーコーディングコピーとして StorageGRID に格納するときに、オブジェクトをクラウドストレージプールに格納することができます。ただし、この例に示すように、各場所のコピーの数とタイプを指定できるように、配置手順には複数の行を含める必要があります。



5. イレイジャーコーディングコピーを作成する場合は、次の手順を実行します。

   a. [* タイプ * （ * Type * ）] ドロップダウンリストから [* イレイジャーコーディング * （ * erasure Coded * ）] を選択

      コピーの数が 1 に変わります。200KB 以下のオブジェクトを無視する高度なフィルタがルールに含まれていない場合は警告が表示されます。

      Do not use erasure coding for objects that are 200 KB or smaller. Select **Back** to return to Step 1. Then, use **Advanced filtering** to set the Object Size (MB) filter to "greater than 0.2".

      200KB 未満のオブジェクトにはイレイジャーコーディングを使用しないでください。イレイジャーコーディングされた非常に小さなフラグメントを管理するオーバーヘッドは発生しません。

   b. オブジェクトサイズの警告が表示された場合は、次の手順に従ってクリアします。

      i. 「戻る」を選択して、ステップ1に戻ります。

      ii. 「高度なフィルタリング」を選択します。

      iii. [オブジェクトサイズ(MB)]フィルタを「0.2より大きい」に設定します。

   c. 格納場所を選択します。

      イレイジャーコーディングコピーの格納場所には、ストレージプール名とイレイジャーコーディングプロファイル名が続けて含まれます。

6. 必要に応じて、別の期間を追加するか、別の場所に追加のコピーを作成します。

   ◦ プラスアイコンをクリックして、同じ期間に追加のコピーを別の場所に作成します。

   ◦ 別の期間を配置手順に追加するには、* Add *をクリックします。

      最終期間が * forever * で終わる場合を除き、オブジェクトは最終期間の終了時に自動的に削除されます。

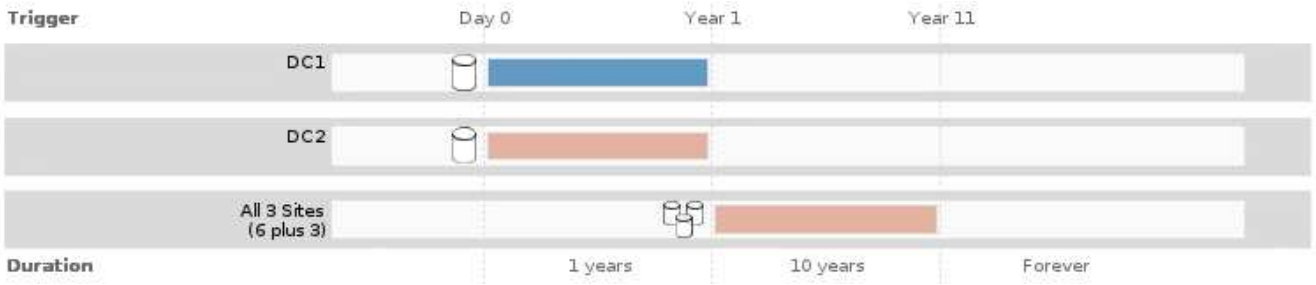
7. [更新]をクリックして保持図を更新し'配置手順を確認します

   図の中の各ラインは、オブジェクトコピーをいつどこに配置するかを示しています。コピーのタイプは次のいずれかのアイコンで表されます。

	レプリケートコピー
	イレイジャーコーディングコピー

	クラウドストレージプールのコピー

この例では、 2 つのレプリケートコピーが 2 つのストレージプール（ DC1 と DC2 ）に 1 年間保存されます。その後、 3 つのサイトで 6+3 のイレイジャーコーディングスキームを使用して、イレイジャーコーディングコピーがさらに 10 年間保存されます。11 年後、オブジェクトは StorageGRID から削除されます。



8. 「 * 次へ * 」をクリックします。

ステップ 3 （取り込み動作の定義）が表示されます。

関連情報

"ILM ルールの配置手順とは"

"例 4 ： S3 バージョン管理オブジェクトの ILM ルールとポリシー"

"シングルコピーレプリケーションを使用しない理由"

"S3オブジェクトロックでオブジェクトを管理する"

"一時的な場所としてのストレージプールの使用（廃止）"

"ステップ 3 / 3 ：取り込み動作を定義する"

ILMルールで最終アクセス日時を使用する

最終アクセス時間を ILM ルールの参照時間として使用できます。たとえば、過去 3 カ月間に表示されたオブジェクトをローカルストレージノードに残しておき、最近表示されていないオブジェクトをオフサイトの場所に移動することができます。特定の日付に最後にアクセスされたオブジェクトにのみ ILM ルールを適用する場合は、高度なフィルタとして最終アクセス時間を使用することもできます。

このタスクについて

ILM ルールで最終アクセス日時を使用する前に、次の考慮事項を確認してください。

- 参照時間として最終アクセス時間を使用する場合、オブジェクトの最終アクセス時間を変更しても ILM 評価はすぐには開始されない点に注意してください。オブジェクトの配置が評価され、バックグラウンド ILM がオブジェクトを評価したときに必要に応じてオブジェクトが移動されます。この処理には、オブジェクトがアクセスされてから 2 週間以上かかる場合があります。

  最終アクセス時間に基づいて ILM ルールを作成する際には、このレイテンシを考慮し、短い期間（ 1 カ月

未満）を使用する配置は避けてください。

- 高度なフィルタまたは参照時間として最終アクセス時間を使用する場合は、 S3 バケットに対して最終アクセス時間の更新を有効にしておく必要があります。Tenant Manager またはテナント管理 API を使用できます。

> 最終アクセス時間の更新は Swift コンテナでは常に有効ですが、 S3 バケットではデフォルトで無効になっています。

> 最終アクセス時間の更新を有効にすると、特に小さなオブジェクトを含むシステムのパフォーマンスが低下する可能性があります。これは、オブジェクトが読み出されるたびに StorageGRID が新しいタイムスタンプでオブジェクトを更新する必要があるためです。

次の表に、バケット内のすべてのオブジェクトについて、さまざまなタイプの要求について最終アクセス時間が更新されるかどうかを示します。

要求のタイプ	最終アクセス時間の更新が無効になったときに最終アクセス時間を更新するかどうか	最終アクセス時間の更新が有効になったときに最終アクセス時間を更新するかどうか
オブジェクト、そのアクセス制御リスト、またはメタデータの読み出し要求	いいえ	はい。
オブジェクトメタデータの更新要求	はい。	はい。
バケット間でのオブジェクトのコピー要求	• ソースコピーに対しては、「いいえ」と指定します • デスティネーションコピーについては、はい	• ソースコピーについては、はい • デスティネーションコピーについては、はい
マルチパートアップロードの完了要求	はい、アセンブルされたオブジェクトの場合	はい、アセンブルされたオブジェクトの場合

関連情報

"S3 を使用する"

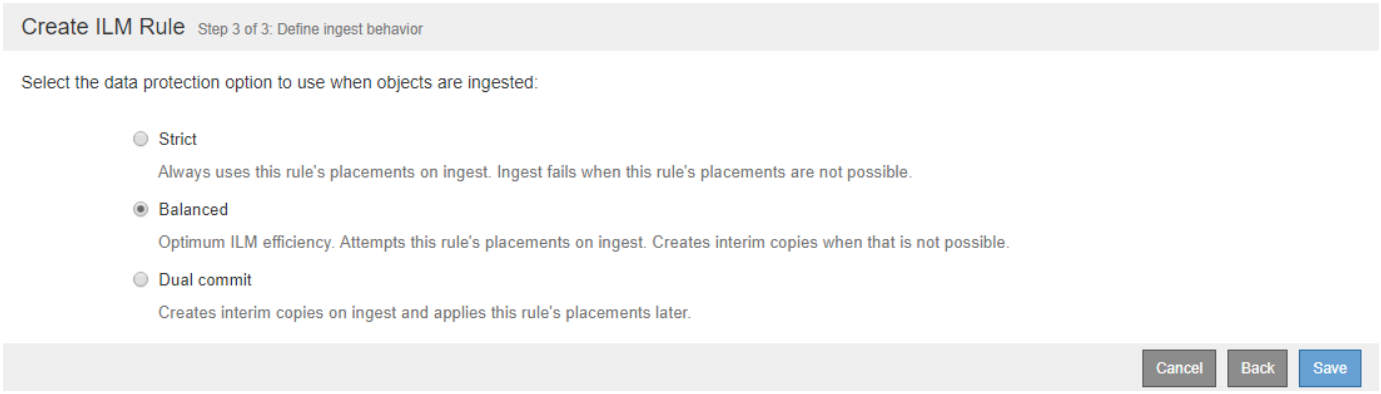
"テナントアカウントを使用する"

ステップ **3 / 3** ：取り込み動作を定義する

Create ILM Rule ウィザードのステップ 3 （取り込み動作の定義）では、このルールでフィルタリングされたオブジェクトを取り込み時に保護する方法を選択できます。

このタスクについて

StorageGRID は、中間コピーを作成してオブジェクトをキューに登録し、あとで ILM 評価を実行するか、またはコピーを作成してルールの配置手順をすぐに満たすことができます。



手順

1. オブジェクトの取り込み時に使用するデータ保護オプションを選択します。

オプション	説明
strict	取り込み時に必ずこのルールの配置手順を使用します。このルールの配置手順が不可能な場合、取り込みは失敗します。
中間（ Balanced ）	最適な ILM 効率取り込み時にこのルールの配置手順を試行し、不可能な場合に中間コピーを作成します。
デュアルコミット	取り込み時に中間コピーを作成し、このルールの配置手順をあとで適用します。

「 Balanced 」は、ほとんどの場合に適した データ セキュリティ と効率性を組み合わせたソリューションです。「 Strict 」または「 Dual commit 」は一般に特定の要件を満たすために使用します。

詳細については、「取り込みのデータ保護オプションとは」および「各データ保護オプションの長所と短所」を参照してください。

Strict オプションまたは Balanced オプションを選択してルールで次のいずれかの配置を使用している場合は、エラーメッセージが表示されます。

- クラウドストレージプール： 0 日目
- アーカイブノード： 0 日目
- ルールでユーザ定義の作成時間を参照時間として使用する場合は、クラウドストレージプールまたはアーカイブノード

2. [保存（ Save ）] をクリックします。

ILM ルールが保存されます。ルールは、 ILM ポリシーに追加されてアクティブ化されるまでは有効になりません。

関連情報

"取り込みのデータ保護オプション"

"データ保護オプションのメリット、デメリット、および制限事項"

"例 5 ：取り込み動作が Strict の場合の ILM ルールとポリシー"

"ILMポリシーを作成する"

デフォルトの**ILM**ルールを作成する

すべてのILMポリシーに、オブジェクトをフィルタリングしないデフォルトルールが設定されている必要があります。ILMポリシーを作成する前に、ポリシーのデフォルトルールとして使用できるILMルールを少なくとも1つ作成する必要があります。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

このタスクについて

デフォルトルールは、ILMポリシーで評価される最後のルールであるため、フィルタは使用できません。デフォルトルールの配置手順は、ポリシー内の別のルールに一致しないオブジェクトに適用されます。

次のポリシーの例では、最初のルールがテナント A に属するオブジェクトにのみ適用されますデフォルトルールである最後のルールは、他のすべてのテナントアカウントに属する環境 オブジェクトです。

デフォルトルールを作成するときは、次の要件に注意してください。

- デフォルトのルールは、ポリシーの最後のルールとして自動的に配置されます。
- デフォルトルールでは、基本フィルタまたは詳細フィルタは使用できません。
- デフォルトのルールでレプリケートコピーを作成する必要があります。

> イレイジャーコーディングコピーを作成するルールはポリシーのデフォルトルールとして使用しないでください。イレイジャーコーディングルールでは、高度なフィルタを使用して、小さなオブジェクトがイレイジャーコーディングされないようにします。

- 一般に、デフォルトルールではオブジェクトを無期限に保持する必要があります。
- S3 オブジェクトのグローバルロック設定を使用している（または有効にする）場合は、アクティブポリシーまたはドラフトポリシーのデフォルトルールが準拠している必要があります。

手順

1. [* ILM*>* Rules] を選択します。

   ILM ルールページが表示されます。

2. 「 * Create * 」を選択します。

Create ILM Rule ウィザードの Step 1 （ Define Basics ）が表示されます。

3. [* 名前 *] フィールドに、ルールの一意の名前を入力します。
4. 必要に応じて、ルールの短い概要 を * 概要 * フィールドに入力します。
5. [* Tenant Accounts] フィールドは空白のままにします。

   デフォルトのルールをすべてのテナントアカウントに適用する必要があります。

6. Bucket Name * フィールドは空白のままにします。

   デフォルトルールは、すべての S3 バケットと Swift コンテナに適用する必要があります。

7. 「 * 高度なフィルタリング * 」は選択しないでください

   デフォルトルールでフィルタを指定することはできません。

8. 「 * 次へ * 」を選択します。

   ステップ 2 （配置を定義）が表示されます。

9. デフォルトルールの配置手順を指定します。
   - デフォルトルールではオブジェクトを無期限に保持する必要があります。デフォルトルールによってオブジェクトが無期限に保持されない場合、新しいポリシーをアクティブ化すると警告が表示されます。これが想定どおりの動作であることを確認する必要があります。
   - デフォルトのルールでレプリケートコピーを作成する必要があります。

     イレイジャーコーディングコピーを作成するルールはポリシーのデフォルトルールとして使用しないでください。イレイジャーコーディングルールでは、高度なフィルタ「 * Object Size （ MB ） than 0.2 」を含めて、小さいオブジェクトがイレイジャーコーディングされないようにします。

   - S3 オブジェクトのグローバルロック設定を使用している（または有効にする）場合は、デフォルトルールが準拠している必要があります。
     - 2 つ以上のレプリケートオブジェクトコピーまたは 1 つのイレイジャーコーディングコピーを作成する。
     - これらのコピーが、配置手順の各ラインの間、ストレージノード上に存在している必要があります。
     - オブジェクトコピーをクラウドストレージプールに保存することはできません。
     - オブジェクトコピーをアーカイブノードに保存することはできません。
     - 配置手順の少なくとも 1 行は、参照時間として取り込み時間を使用して 0 日目から開始する必要があります。
     - 配置手順の少なくとも 1 行は「無期限」である必要があります。
10. [更新]をクリックして保持図を更新し’配置手順を確認します
11. 「 * 次へ * 」をクリックします。

    ステップ 3 （取り込み動作の定義）が表示されます。

12. オブジェクトの取り込み時に使用するデータ保護オプションを選択し、 * 保存 * を選択します。

ILMポリシーを作成する

ILM ポリシーを作成するには、最初に ILM ルールを選択して配置します。次に、以前に取り込まれたオブジェクトに対してドラフトポリシーをシミュレートし、その動作を確認します。ドラフトポリシーが意図したとおりに機能していることを確認したら、そのポリシーをアクティブ化してアクティブポリシーを作成できます。

> ILM ポリシーが正しく設定されていないと、リカバリできないデータ損失が発生する可能性があります。ILM ポリシーをアクティブ化する前に、 ILM ポリシーおよびその ILM ルールを慎重に確認し、次に ILM ポリシーをシミュレートします。ILM ポリシーが意図したとおりに機能することを必ず確認してください。

ILM ポリシーの作成に関する考慮事項

- システムに組み込まれているポリシーである Baseline 2 Copies Policy をテストシステムでのみ使用します。このポリシーの Make 2 Copies ルールは、すべてのサイトを含む All Storage Nodes ストレージプールを使用します。StorageGRID システムに複数のサイトがある場合は、 1 つのオブジェクトのコピーが同じサイトに 2 つ配置される可能性があります。
- 新しいポリシーを設計する際には、グリッドに取り込まれる可能性のあるさまざまなタイプのオブジェクトをすべて考慮してください。それらのオブジェクトに一致し、必要に応じて配置するルールがポリシーに含まれていることを確認してください。
- ILM ポリシーはできるだけシンプルにします。これにより、時間が経って StorageGRID システムに変更が加えられ、オブジェクトデータが意図したとおりに保護されないという危険な状況を回避できます。
- ポリシー内のルールの順序が正しいことを確認してください。ポリシーをアクティブ化すると、新規および既存のオブジェクトがリスト内の順にルールによって評価されます。たとえば、ポリシー内の最初のルールがオブジェクトに一致する場合、そのルールは他のルールによって評価されません。
- すべての ILM ポリシーの最後のルールはデフォルトの ILM ルールであり、フィルタを使用することはできません。オブジェクトが別のルールに一致していない場合は、デフォルトルールによって、そのオブジェクトの配置場所と保持期間が制御されます。
- 新しいポリシーをアクティブ化する前に、ポリシーによって既存のオブジェクトの配置が変更されていないかどうかを確認します。既存のオブジェクトの場所を変更すると、新しい配置が評価されて実装される際に一時的なリソースの問題が発生する可能性があります。

関連情報

"ILM ポリシーとは"

"例 6 ： ILM ポリシーを変更する"

ドラフトのILMポリシーを作成します

ドラフトの ILM ポリシーを新規に作成できます。同じルールセットを使用する場合は、現在のアクティブポリシーをクローニングして作成できます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

- 特定のアクセス権限が必要です。
- ドラフトポリシーに追加するILMルールを作成しておく必要があります。必要に応じて、ドラフトポリシーを保存して追加のルールを作成し、ドラフトポリシーを編集して新しいルールを追加できます。
- フィルタを含まないポリシー用のデフォルトのILMルールを作成しておく必要があります。

  "デフォルトのILMルールを作成する"

このタスクについて

ドラフトの ILM ポリシーを作成する主な理由は次のとおりです。

- 新しいサイトを追加した場合、そのサイトにオブジェクトを配置するために新しい ILM ルールを使用する必要があります。
- サイトの運用を停止しているときは、そのサイトを参照するすべてのルールを削除する必要があります。
- 新しいテナントには特別なデータ保護要件があります。
- クラウドストレージプールの使用を開始した。

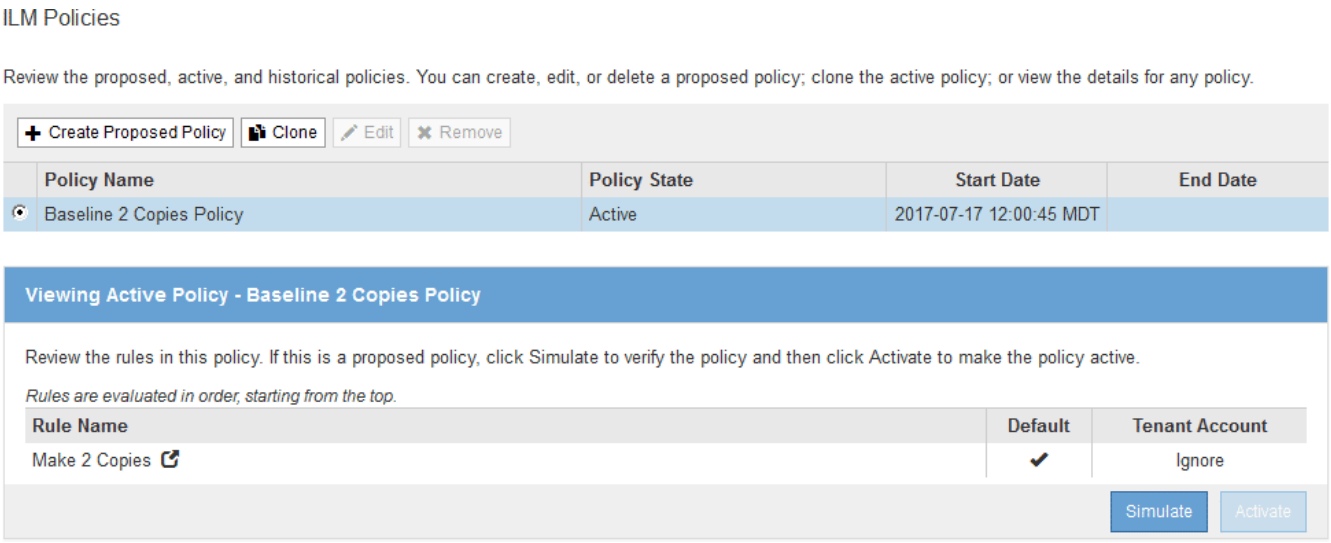
> システムに組み込まれているポリシーである Baseline 2 Copies Policy をテストシステムでのみ使用します。このポリシーの Make 2 Copies ルールは、すべてのサイトを含む All Storage Nodes ストレージプールを使用します。StorageGRID システムに複数のサイトがある場合は、1 つのオブジェクトのコピーが同じサイトに 2 つ配置される可能性があります。

> グローバルなS3オブジェクトのロック設定が有効になっている場合は、ポリシーの作成手順が少し異なります。S3 オブジェクトロックが有効になっているバケットの要件を ILM ポリシーが準拠していることを確認する必要があります。
>
> "S3オブジェクトのロックが有効になったあとのILMポリシーの作成"

手順

1. 「 * ILM * > * Policies * 」を選択します。

   ILM ポリシーページが表示されます。このページでは、ドラフトポリシー、アクティブポリシー、履歴ポリシーのリストを確認し、 または、ドラフトポリシーを削除するか、アクティブポリシーをクローニングするか、すべてのポリシーの詳細を表示します。

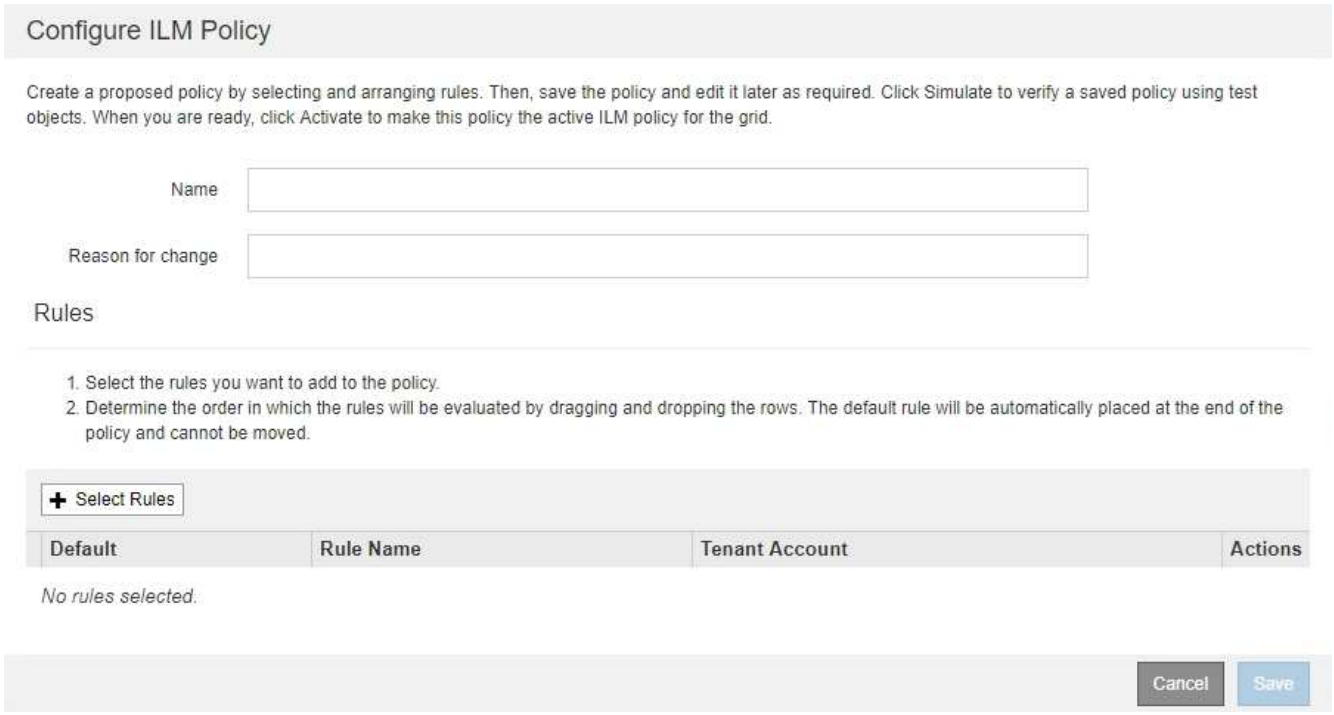


2. ドラフトの ILM ポリシーを作成する方法を決定します。

オプション	手順
ルールが選択されていない新しいドラフトポリシーを作成します	a. ドラフトのILMポリシーが現在存在する場合は、そのポリシーを選択し、*削除*をクリックします。 既存のドラフトポリシーがある場合、新しいドラフトポリシーを作成することはできません。 b. [ドラフトポリシーの作成]をクリックします。
アクティブポリシーに基づいてドラフトポリシーを作成します	a. ドラフトのILMポリシーが現在存在する場合は、そのポリシーを選択し、*削除*をクリックします。 すでにドラフトポリシーが存在する場合、アクティブポリシーをクローニングすることはできません。 b. テーブルからアクティブポリシーを選択します。 c. [* Clone*] をクリックします。
既存のドラフトポリシーを編集します	a. テーブルからドラフトポリシーを選択します。 b. [編集（ Edit ）] をクリックします。

Configure ILM Policy （ ILM ポリシーの設定）ダイアログボックスが表示されます。

新しいドラフトポリシーを作成する場合は、すべてのフィールドが空白になり、ルールは選択されません。



アクティブなポリシーを複製する場合、 * 名前 * フィールドにはアクティブなポリシーの名前が表示され、バージョン番号（この例では「 v2 」）が付加されます。アクティブポリシーで使用されているルールが選択され、現在の順序で表示されます。

3. [* 名前 *] フィールドに、ドラフトポリシーの一意の名前を入力します。

   1 文字以上 64 文字以下で入力する必要があります。アクティブポリシーをクローニングする場合は、現在の名前にバージョン番号を付加したものを使用することも、新しい名前を入力することもできます。

4. [変更理由（ Reason for change ）] フィールドに、新しいドラフトポリシーを作成する理由を入力します。

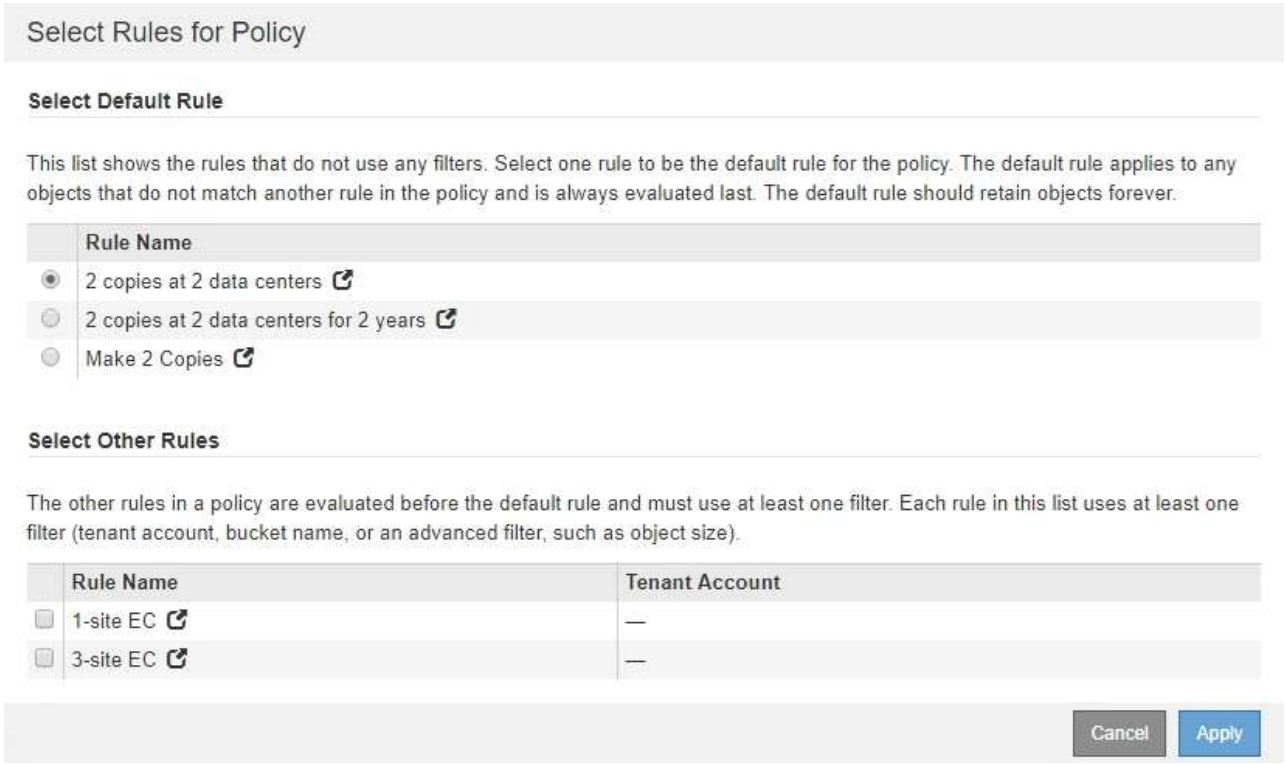
   1 文字以上 128 文字以下で入力する必要があります。

5. ポリシーにルールを追加するには、 * ルールの選択 * を選択します。

   [Select Rules for Policy] ダイアログボックスが表示され、定義済みのすべてのルールが一覧表示されます。ポリシーをクローニングする場合は、次の手順を実行します。

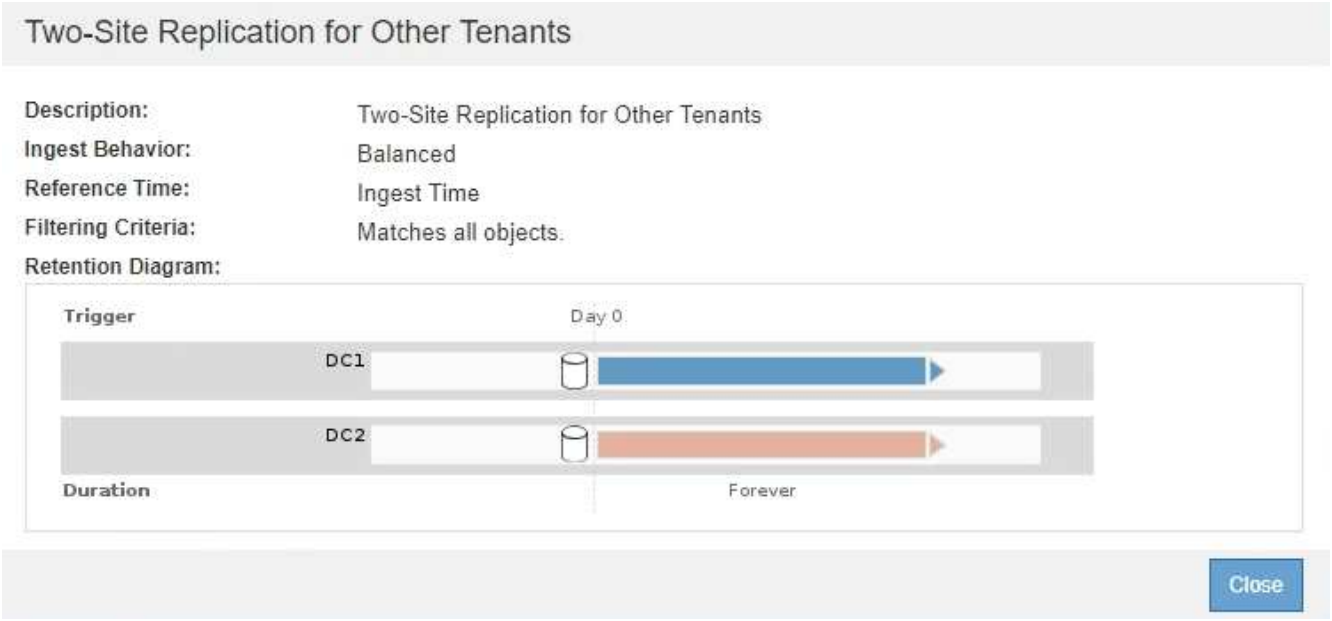
   - クローニングするポリシーで使用されているルールが選択されます。
   - クローニングするポリシーで、デフォルトルールではないフィルタを使用していないルールが使用されている場合は、それらのルールを 1 つだけ残して、それを除くすべてのルールを削除するように求められます。
   - デフォルトルールでフィルタを使用している場合は、新しいデフォルトルールを選択するように求められます。

◦ デフォルトルールが最後のルールではない場合は、ボタンを使用して新しいポリシーの末尾にルールを移動できま
す。



6. ルール名または詳細アイコンを選択します をクリックすると、そのルールの設定が表示されます。

この例は、 2 つのレプリケートコピーを 2 つのサイトに作成する ILM ルールの詳細を示しています。



7. [デフォルトルールを選択（ * Select Default Rule ）] セクションで、ドラフトポリシーにデフォルトルールを 1 つ選択します。

デフォルトルールは、ポリシー内の別のルールに一致しないオブジェクトの環境 を作成します。デフォルトルールではフィルタを使用できず、常に最後に評価されます。

ルールが[Select Default Rule]セクションに表示されない場合は、ILMポリシーページを終了してデフォルトルールを作成する必要があります。

"デフォルトのILMルールを作成する"

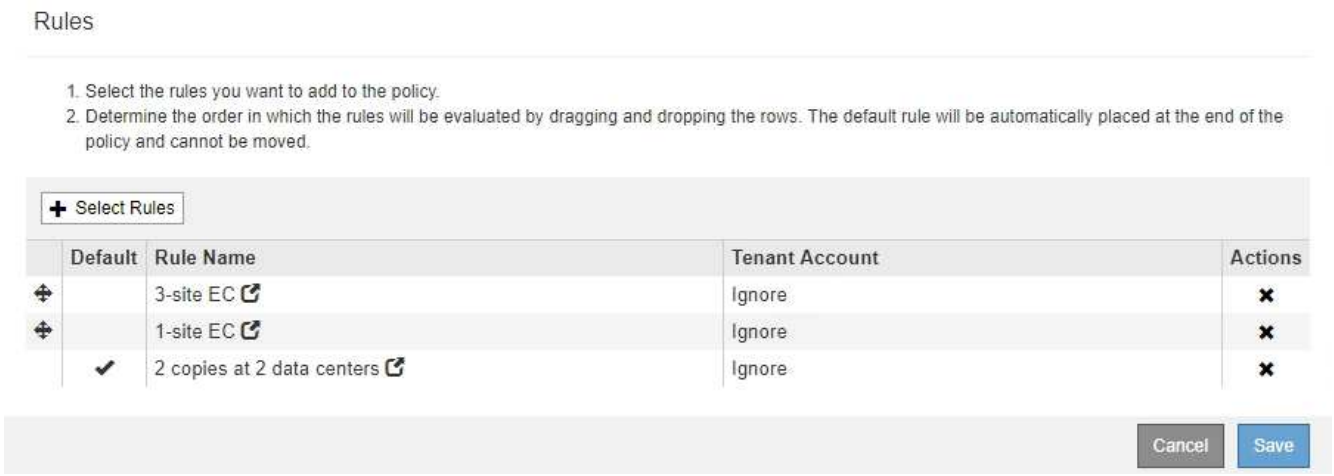
Make 2 Copies ルールをポリシーのデフォルトルールとして使用しないでください。Make 2 Copies ルールは、 1 つのストレージプールであるすべてのストレージノードを使用します。このプールにはすべてのサイトが含まれています。StorageGRID システムに複数のサイトがある場合は、 1 つのオブジェクトのコピーが同じサイトに 2 つ配置される可能性があります。

8. [その他のルールを選択してください] セクションで、ポリシーに含める他のルールを選択します。

   他のルールはデフォルトルールの前に評価され、少なくとも1つのフィルタ（テナントアカウント、バケット名、オブジェクトサイズなどの高度なフィルタ）を使用する必要があります。

9. ルールの選択が完了したら、 * 適用 * を選択します。

   選択したルールが表示されます。デフォルトのルールは末尾にあり、その上に他のルールがあります。



デフォルトルールによってオブジェクトが無期限に保持されない場合は、警告が表示されます。このポリシーをアクティブ化するときは、デフォルトルールの配置手順を経過したとき（バケットライフサイクルによってオブジェクトが長期間保持されないかぎり）に StorageGRID がオブジェクトを削除することを確認する必要があります。

10. デフォルト以外のルールの行をドラッグアンドドロップして、ルールが評価される順序を決定します。

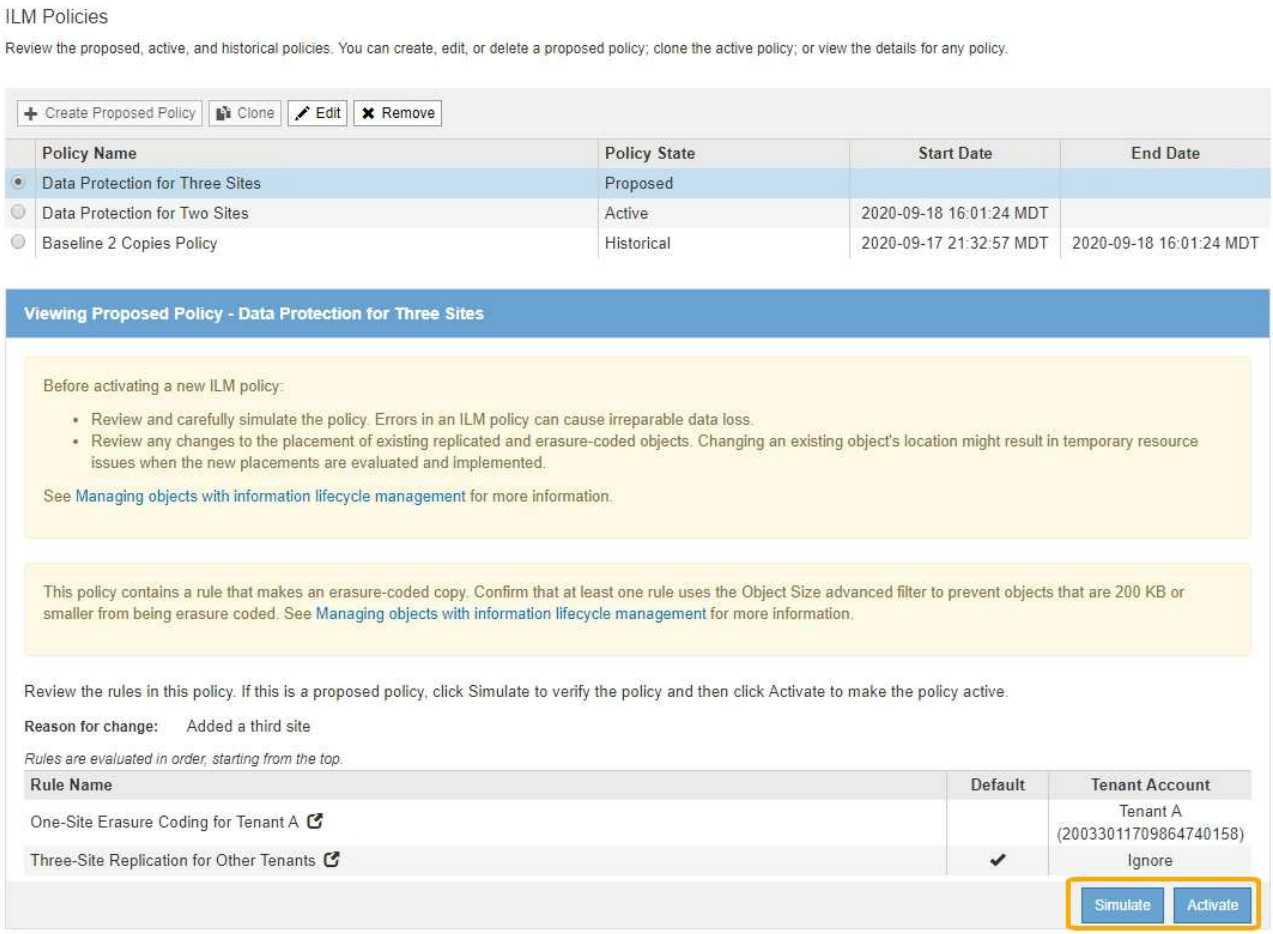
    デフォルトのルールは移動できません。

ILM ルールの順序が正しいことを確認してください。ポリシーをアクティブ化すると、新規および既存のオブジェクトがリスト内の順にルールによって評価されます。

11. 必要に応じて、削除アイコンをクリックします ✖ ポリシーに不要なルールを削除するには、 [ルールの選択] を選択してルールを追加します。
12. 完了したら、 * 保存 * を選択します。

    ILM ポリシーページが更新されます。

    - 保存したポリシーがドラフトとして表示されます。ドラフトポリシーには開始日と終了日がありません。
    - [シミュレート（ Simulate ）] および [活動化（ Activate ）] * ボタンが有効になります。



13. に進みます "ILMポリシーをシミュレートする"。

関連情報

"ILM ポリシーとは"

"S3オブジェクトロックでオブジェクトを管理する"

S3オブジェクトのロックが有効になったあとの**ILM**ポリシーの作成

グローバルな S3 オブジェクトのロック設定が有効になっている場合は、ポリシーの作成手順が少し異なります。S3 オブジェクトロックが有効になっているバケットの要件を

ILM ポリシーが準拠していることを確認する必要があります。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。
- StorageGRID システムでグローバルなS3オブジェクトロック設定が有効になっている必要があります。

> グローバルなS3オブジェクトのロック設定が有効になっていない場合は、代わりにドラフトポリシーの作成手順を使用してください。
>
> "ドラフトのILMポリシーを作成します"

- ドラフトポリシーに追加する準拠ILMルールと非準拠ILMルールを作成しておく必要があります。必要に応じて、ドラフトポリシーを保存して追加のルールを作成し、ドラフトポリシーを編集して新しいルールを追加できます。

  "例 7 ： S3 オブジェクトロックの準拠 ILM ポリシー"

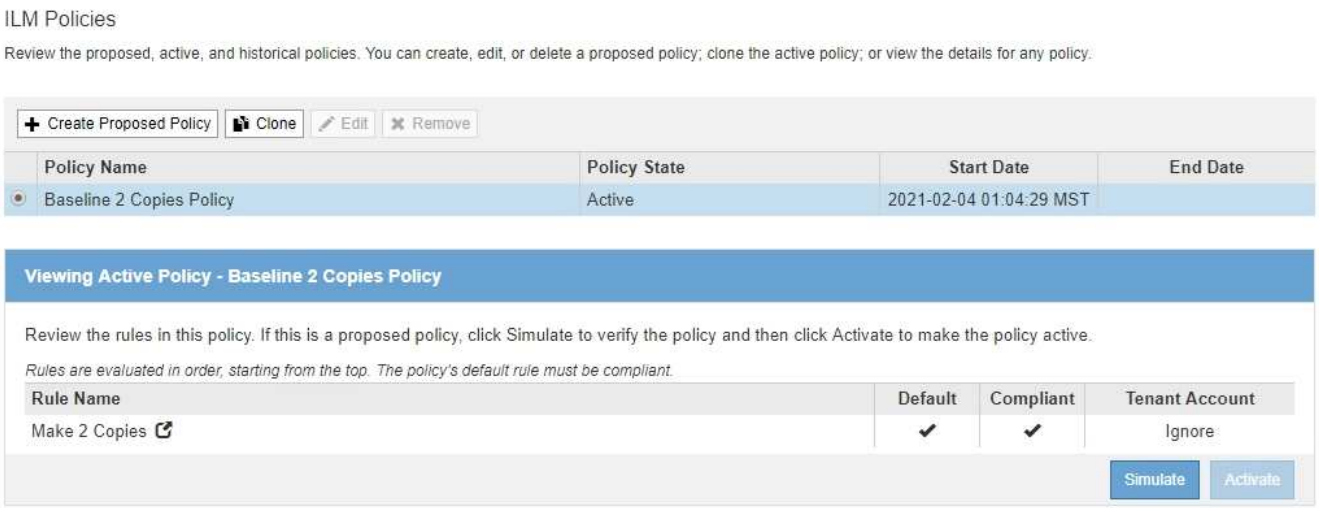
- ポリシーの準拠デフォルトのILMルールを作成しておく必要があります。

  "デフォルトのILMルールを作成する"

手順

1. 「 * ILM * > * Policies * 」を選択します。

   ILM ポリシーページが表示されます。グローバルな S3 オブジェクトのロック設定が有効になっている場合は、 ILM ポリシーページに準拠している ILM ルールが表示されます。



2. [* 名前 *] フィールドに、ドラフトポリシーの一意の名前を入力します。

   1 文字以上 64 文字以下で入力する必要があります。

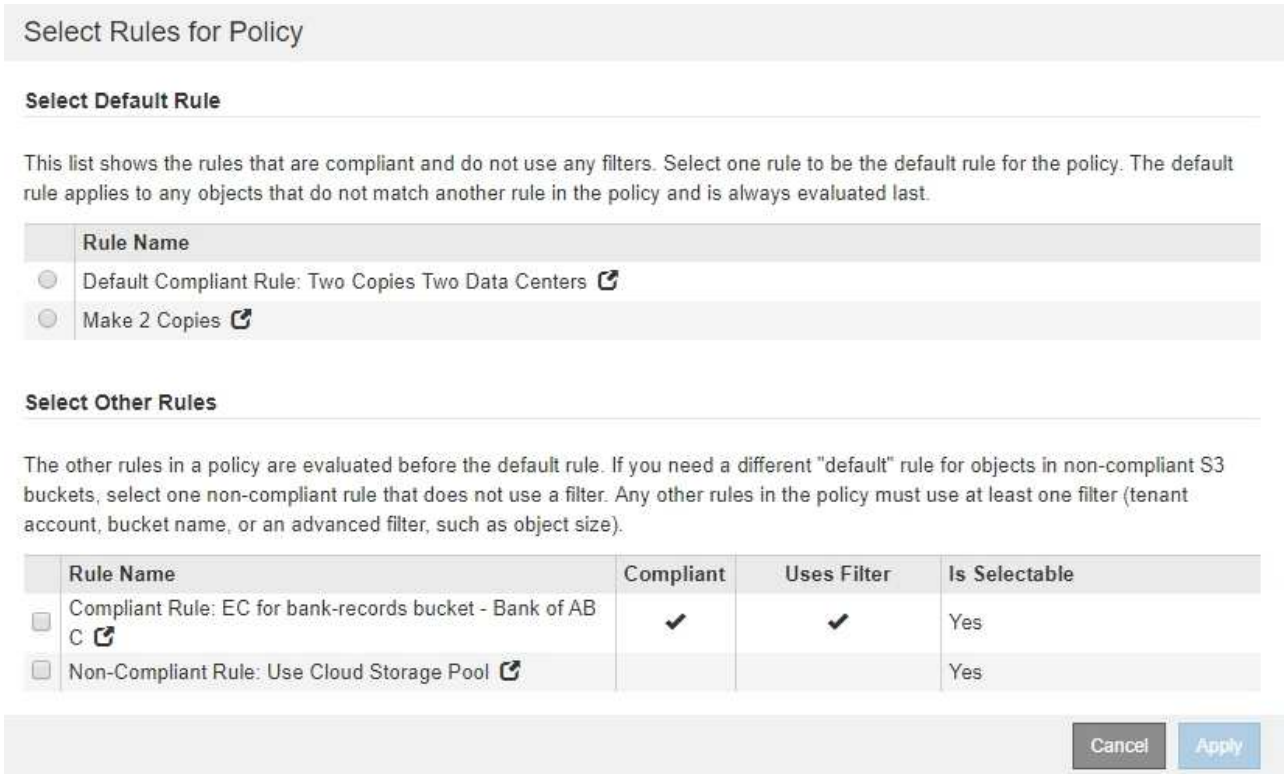
3. [変更理由（ Reason for change ）] フィールドに、新しいドラフトポリシーを作成する理由を入力します。

1 文字以上 128 文字以下で入力する必要があります。

4. ポリシーにルールを追加するには、 * ルールの選択 * を選択します。

   [Select Rules for Policy] ダイアログボックスが表示され、定義済みのすべてのルールが一覧表示されます。

   - ［ デフォルトルールの選択 ］ セクションには、準拠ポリシーのデフォルトになるルールがリストされます。フィルタを使用しない準拠ルールが含まれています。
   - [その他のルールの選択] セクションには、このポリシーに選択できる他の準拠ルールと非準拠ルールが一覧表示されま
     す。



5. ルール名または詳細アイコンを選択します をクリックすると、そのルールの設定が表示されます。
6. [デフォルトルールを選択（ * Select Default Rule ）] セクションで、ドラフトポリシーにデフォルトルールを 1 つ選択します。

   このセクションの表には、準拠ルールのみが表示され、フィルタは使用されません。

   ルールが[Select Default Rule]セクションに表示されない場合は、ILMポリシーページを終了して、準拠するデフォルトルールを作成する必要があります。

   "デフォルトのILMルールを作成する"

   Make 2 Copies ルールをポリシーのデフォルトルールとして使用しないでください。Make 2 Copies ルールは、 1 つのストレージプールであるすべてのストレージノードを使用します。このプールにはすべてのサイトが含まれています。このルールを使用すると、 1 つのオブジェクトの複数のコピーが同じサイトに配置される場合があります。

7. [その他のルールを選択してください] セクションで、ポリシーに含める他のルールを選択します。

a. 非準拠 S3 バケット内のオブジェクトに別の「デフォルト」ルールが必要な場合は、必要に応じて、フィルタを使用しない非準拠ルールを 1 つ選択します。

   たとえば、クラウドストレージプールやアーカイブノードを使用して、 S3 オブジェクトロックが有効になっていないバケットにオブジェクトを格納できます。

   フィルタを使用しない非準拠ルールは 1 つだけ選択できます。1 つのルールを選択すると、 [選択可能] 列には、フィルタのない他の非準拠ルールについては [* いいえ] と表示されます。

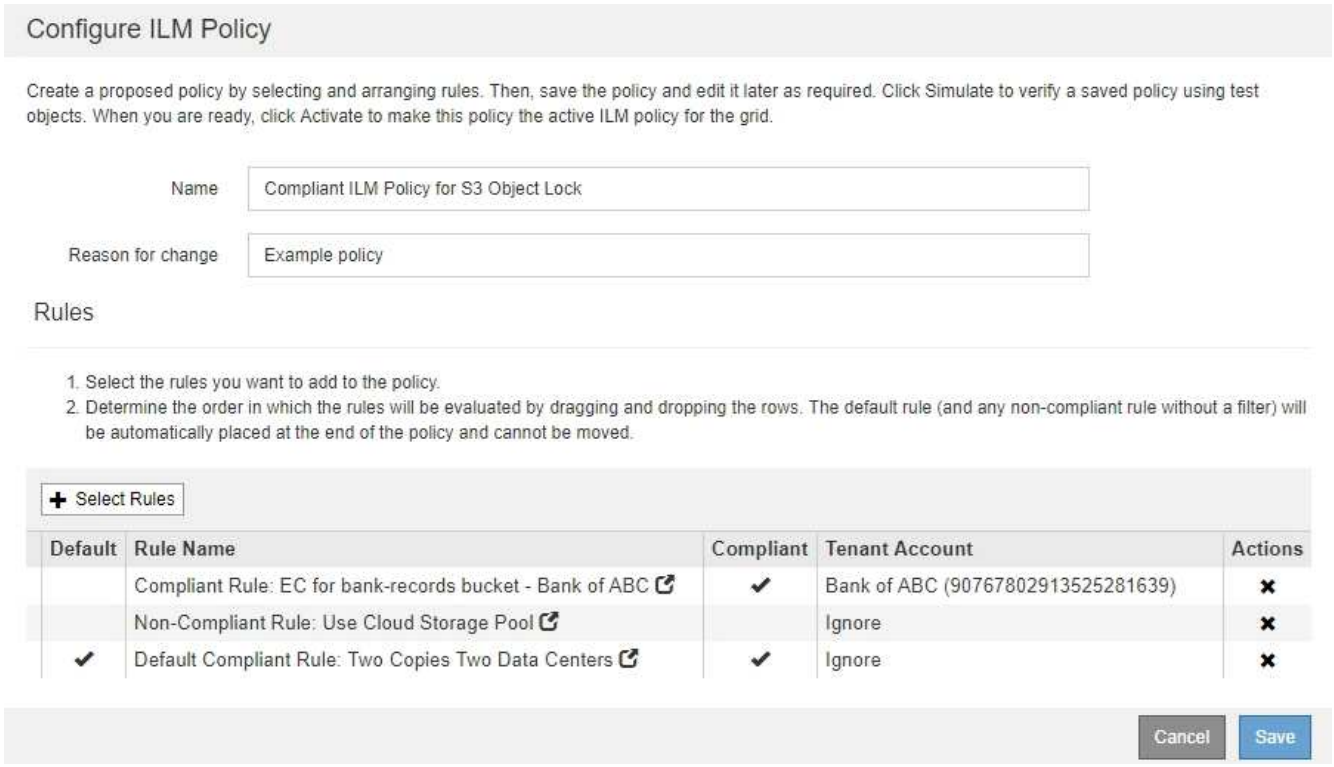
a. ポリシーで使用する他の準拠ルールと非準拠ルールを選択します。

   他のルールでは、少なくとも 1 つのフィルタ（テナントアカウント、バケット名、オブジェクトサイズなどの高度なフィルタ）を使用する必要があります。

8. ルールの選択が完了したら、 * 適用 * を選択します。

   選択したルールが表示されます。デフォルトのルールは末尾にあり、その上に他のルールがあります。非準拠の「デフォルト」ルールも選択した場合、そのルールはポリシーの 2 番目から最後までのルールとして追加されます。

   この例では、最後のルール「 2 Copies 2 Data Center 」がデフォルトルールで、準拠ルールでフィルタがありません。2 番目から最後までのルールである Cloud Storage Pool にもフィルタはありませんが、準拠していません。



。

9. デフォルト以外のルールの行をドラッグアンドドロップして、ルールが評価される順序を決定します。

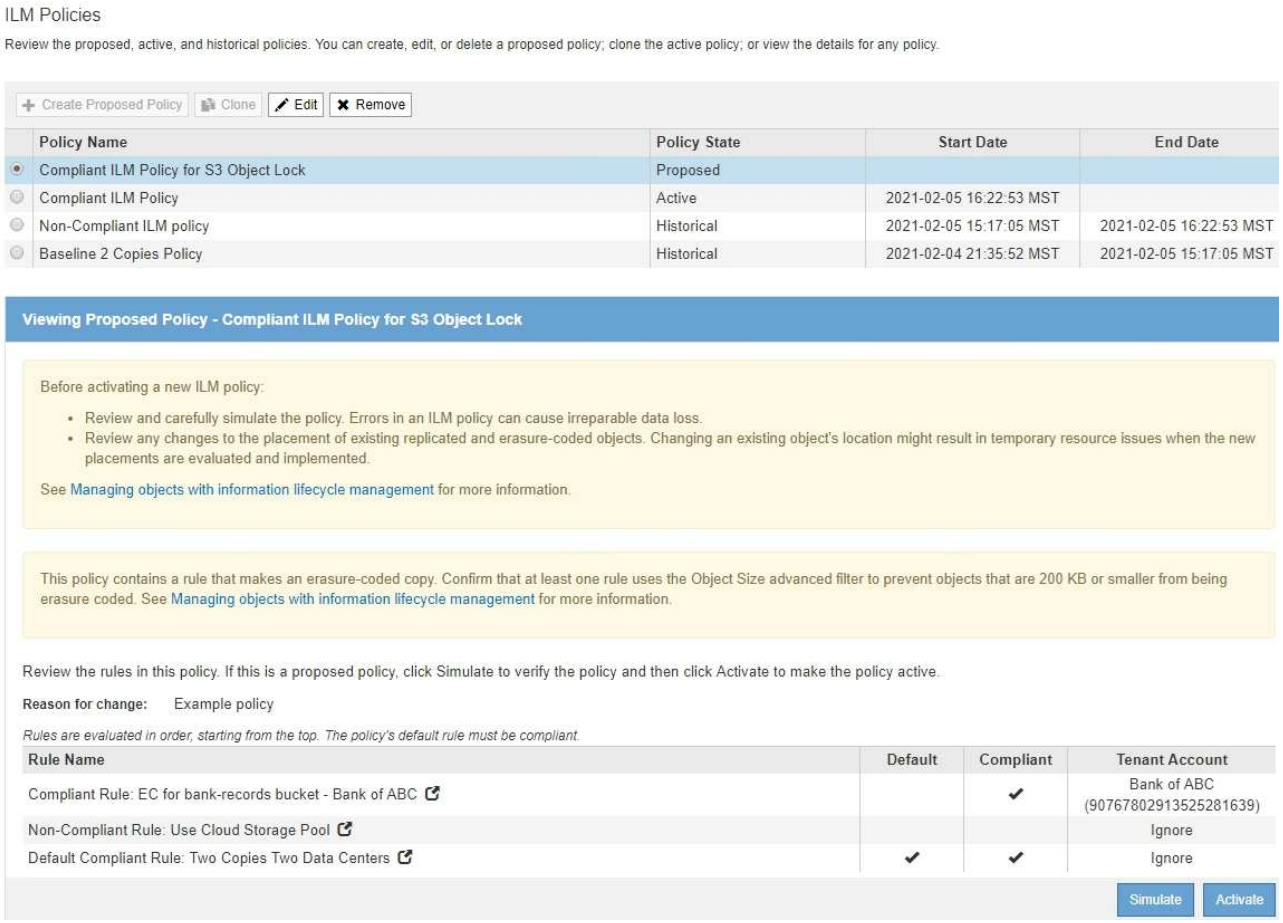
   デフォルトのルールまたは非準拠の「デフォルト」ルールは移動できません。

ILM ルールの順序が正しいことを確認してください。ポリシーをアクティブ化すると、新規および既存のオブジェクトがリスト内の順にルールによって評価されます。

10. 必要に応じて、削除アイコンをクリックします ポリシーに不要なルールを削除するには、 [ルールの選択] を選択してルールを追加します。
11. 完了したら、 * 保存 * を選択します。

    ILM ポリシーページが更新されます。

    - 保存したポリシーがドラフトとして表示されます。ドラフトポリシーには開始日と終了日がありません。
    - [シミュレート（ Simulate ）] および [活動化（ Activate ）] * ボタンが有効になります。



12. に進みます "ILMポリシーをシミュレートする"。

ILMポリシーをシミュレートする

ポリシーをアクティブ化して本番環境のデータに適用する前に、テストオブジェクトでドラフトポリシーをシミュレートする必要があります。シミュレーション期間は、アクティブ化して本番環境のデータに適用する前にポリシーを安全にテストするための、スタンドアロン環境を提供します。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。
- テストする各オブジェクトのS3バケット/オブジェクトキーまたはSwiftコンテナ/オブジェクト名を確認しておく必要があります。また、それらのオブジェクトを取り込んでおく必要があります。

このタスクについて

ドラフトポリシーをテストするオブジェクトは慎重に選択する必要があります。ポリシーを確実にシミュレートするには、各ルールのフィルタごとに少なくとも 1 つのオブジェクトをテストする必要があります。

たとえば、バケット A のオブジェクトに一致するルールとバケット B のオブジェクトに一致するルールを含むポリシーを確実にテストするためには、少なくともバケット A から 1 つとバケット B から 1 つオブジェクトを選択する必要があります。ポリシーに他のすべてのオブジェクトを配置するデフォルトルールが含まれている場合は、別のバケットのオブジェクトを少なくとも1つテストする必要があります。

ポリシーをシミュレートする場合は、次の点を考慮します。

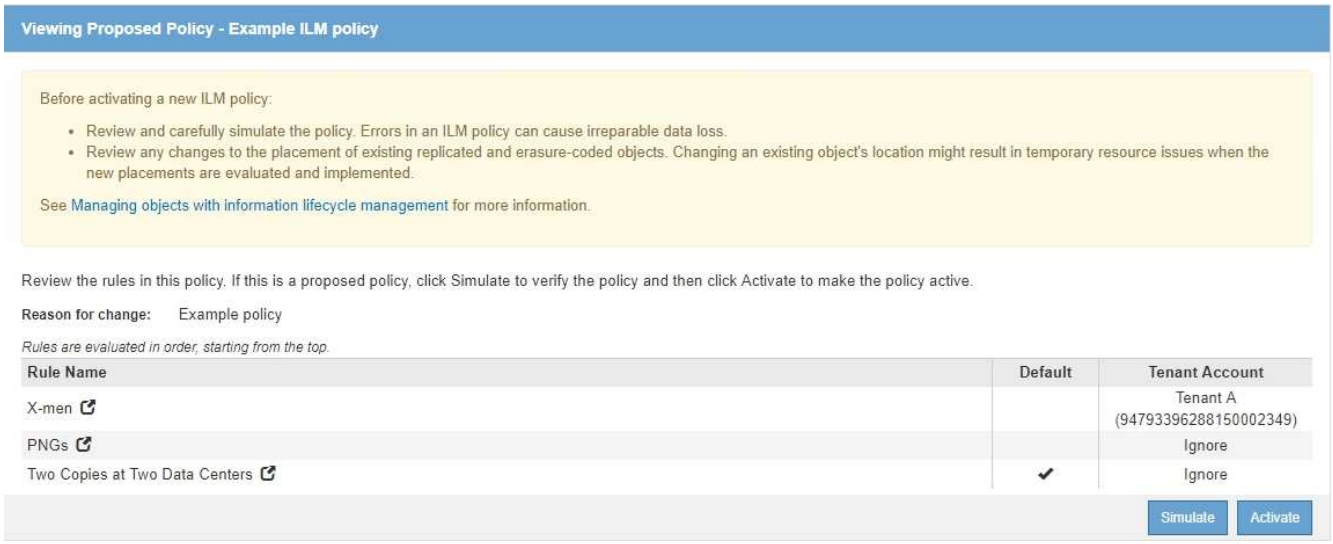
- ポリシーを変更したら、ドラフトポリシーを保存します。次に、保存したドラフトポリシーの動作をシミュレートします。
- ポリシーをシミュレートするとポリシー内の ILM ルールがテストオブジェクトをフィルタリングするため、各オブジェクトにどのルールが適用されたかを確認できます。ただし、オブジェクトのコピーは作成されず、配置もされません。シミュレーションを実行しても、データ、ルール、ポリシーはいっさい変更されません。
- シミュレーションページでは、 ILM ポリシーページを閉じるか別のページに移動するか更新するまで、テストしたオブジェクトが保持されます。
- シミュレーションは、一致したルールの名前を返します。どのストレージプールまたはイレイジャーコーディングプロファイルが有効かを確認するには、ルール名または詳細アイコンをクリックして保持図を表示します。
- S3 のバージョン管理が有効な場合、ポリシーはオブジェクトの現在のバージョンに対してのみシミュレートされます。

手順

1. ルールを選択して配置し、ドラフトポリシーを保存します。

   この例のポリシーには 3 つのルールがあります。

ルール名	フィルタ	コピーのタイプ	保持
男性用	• テナント A • ユーザメタデータ（シリーズ = x-men ）	2 つのデータセンターに 2 つのコピーを保持	2 年
PNGs	キーの末尾は .png です	2 つのデータセンターに 2 つのコピーを保持	5 年
2 つのコピーで 2 つのデータセンターを構成し	_ なし _	2 つのデータセンターに 2 つのコピーを保持	永遠に

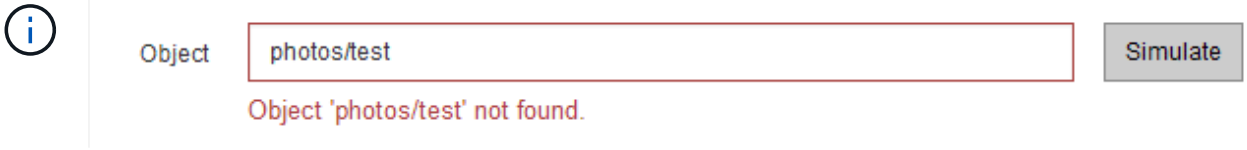


2. * Simulate *をクリックします。

   Simulation ILM Policy （シミュレーション ILM ポリシー）ダイアログボックスが表示されます。

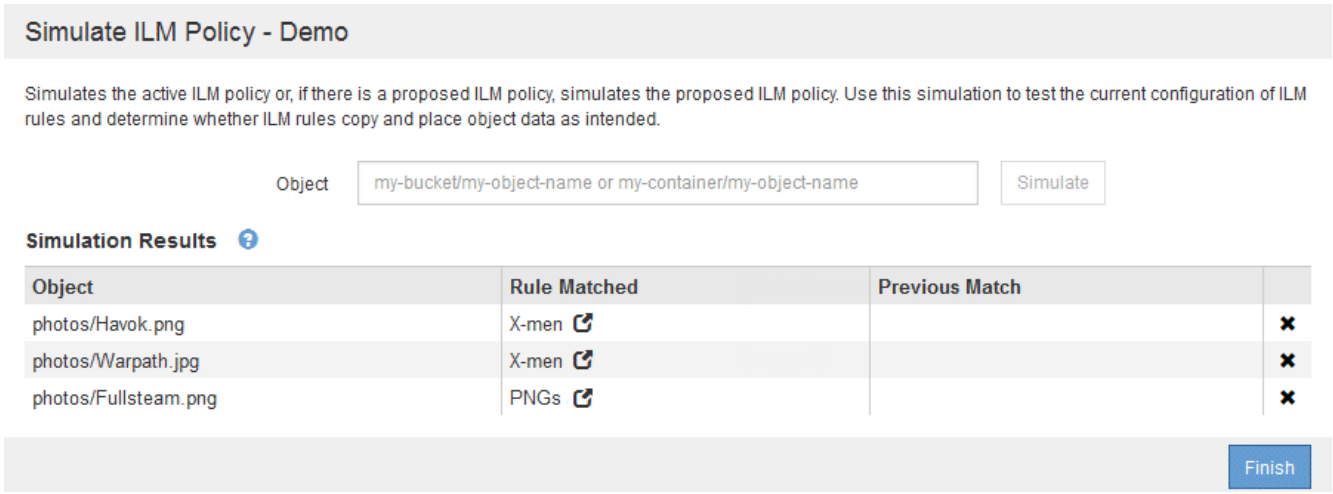
3. * Object フィールドに、テストオブジェクトの**S3**バケット/オブジェクトキーまたは**Swift**コンテナ/オブジェクト名を入力し、 Simulate *をクリックします。

   取り込まれていないオブジェクトを指定するとメッセージが表示されます。



4. [* シミュレーション結果 * （ Simulation Results ）] で、各オブジェクトが正しいルールに一致していることを確認します。

   この例では、を使用しています `Havok.png` および `Warpath.jpg` オブジェクトが「X-men」ルールに正しく一致しました。。 `Fullsteam.png` オブジェクト。には含まれません `series=x-men` ユーザメタデータは「X-men」ルールには一致しませんでしたが、「PNGs」ルールに正しく一致しました。3 つのオブジェクトがすべて他のルールに一致したため、デフォルトルールは使用されませんでした。



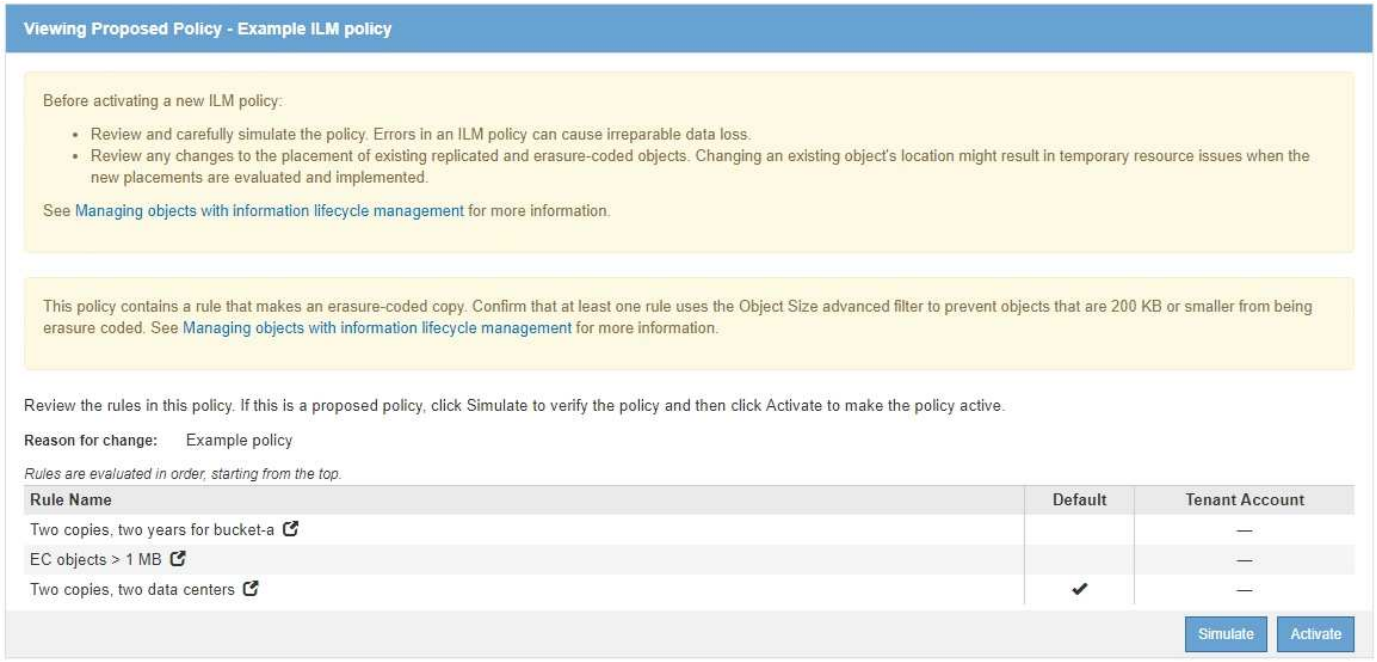
以下の例は、ILMポリシーをアクティブ化する前にシミュレートして、ILMルールを確認する方法を示しています。

例**1**：ドラフトの**ILM**ポリシーをシミュレートしてルールを確認する

この例は、ドラフトポリシーをシミュレートしてルールを確認する方法を示しています。

この例では、 2 つのバケットに取り込まれたオブジェクトに対して * サンプルの ILM ポリシー * をシミュレートします。このポリシーには、次の 3 つのルールが含まれています。

- 最初のルール「 * 2 copies 、 buckets-a * 」の 2 年間は、 bucket-a のオブジェクトにのみ適用されます
- 2番目のルールのメニュー：ECオブジェクト[1MB]、環境 Allバケット。ただし1MBを超えるオブジェクトでフィルタリングします。
- 3番目のルールはデフォルトルールであり、フィルタは含まれません。



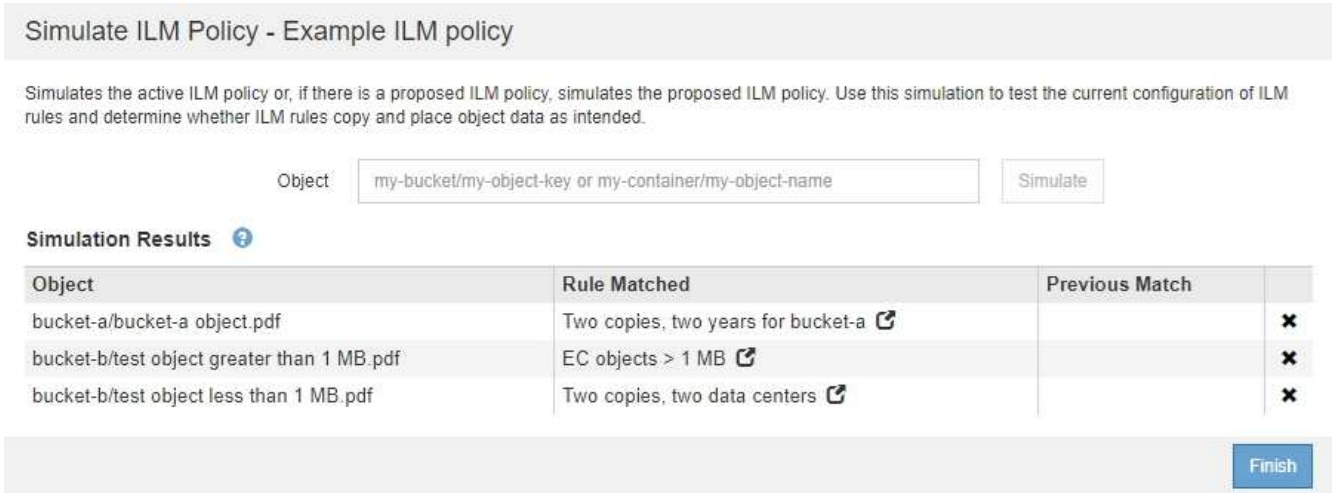
手順

1. ルールを追加してポリシーを保存したら、* Simulate *をクリックします。

   Simulate ILM Policy ダイアログボックスが表示されます。

2. * Object フィールドに、テストオブジェクトの**S3**バケット/オブジェクトキーまたは**Swift**コンテナ/オブジェクト名を入力し、 Simulate *をクリックします。

   シミュレーション結果が表示され、ポリシー内のどのルールがテストした各オブジェクトに一致したかが示されます。



3. 各オブジェクトが正しいルールに一致したことを確認します。

   次の例では、

   a. `bucket-a/bucket-a object.pdf` のオブジェクトをフィルタリングする最初のルールを正しくマッチングしました `bucket-a`。

   b. `bucket-b/test object greater than 1 MB.pdf` がにあります `bucket-b`では、最初のルールと一致しませんでした。代わりに、 1MB を超えるオブジェクトをフィルタリングする 2 つ目のルールに正しく一致しました。

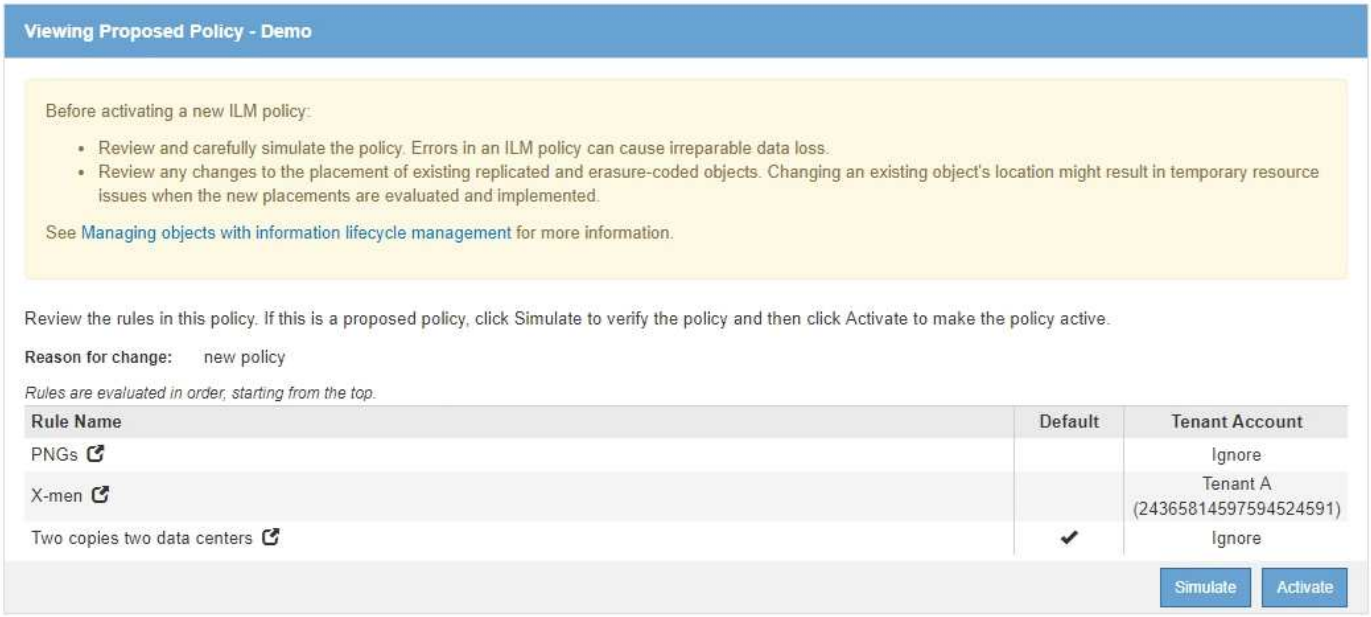
   c. `bucket-b/test object less than 1 MB.pdf` 最初の2つのルールのフィルタに一致しなかったため、フィルタが含まれていないデフォルトルールによって配置されます。

例 **2** ：ドラフトの **ILM** ポリシーをシミュレートする際にルールの順序を変更する

この例では、ポリシーをシミュレートする際に、ルールの順序を変更して結果を変更する方法を示します。

この例では、 * Demo * ポリシーをシミュレートします。このポリシーの目的は次の 3 つのルールで、 series = x -men ユーザメタデータを含むオブジェクトを検索することです。

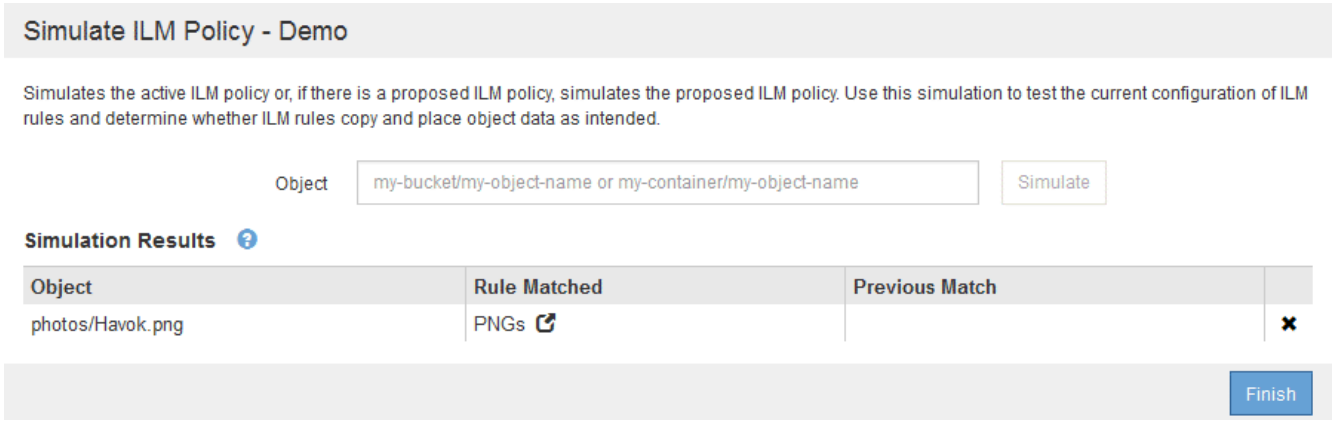
- 最初のルール「* PNGs *」はで終わるキー名に対してフィルタを適用します `.png`。
- 2つ目のルール「* X-men」はテナントAのオブジェクトにのみ適用され、フィルタを適用します `series=x-men` ユーザメタデータ。
- 最後のルール「 * 2 Copies 2 data centers * 」はデフォルトルールで、最初の 2 つのルールに一致しないオブジェクトに一致します。



手順

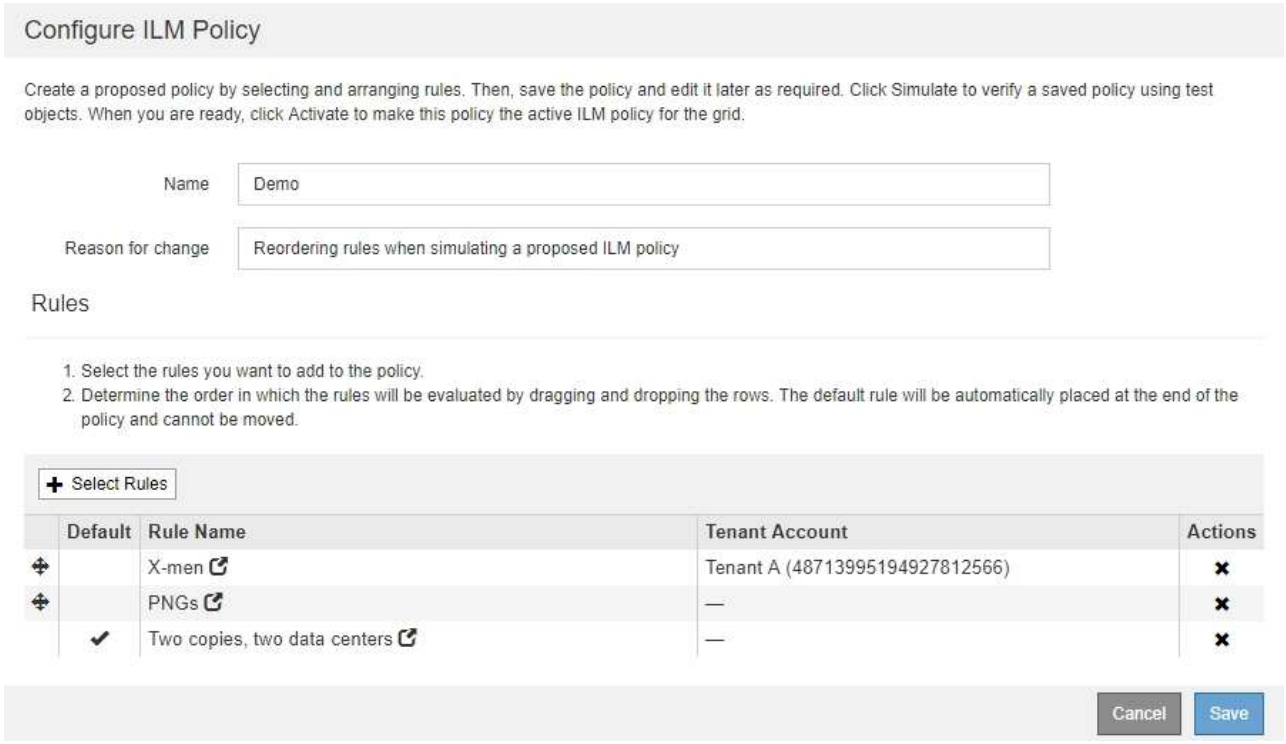
1. ルールを追加してポリシーを保存したら、* Simulate *をクリックします。
2. * Object フィールドに、テストオブジェクトの**S3**バケット/オブジェクトキーまたは**Swift**コンテナ/オブジェクト名を入力し、 Simulate *をクリックします。

   シミュレーション結果が表示され、が表示されます `Havok.png` オブジェクトは「* PNGs *」ルールに一致しました。



   ただし、そのルールはです `Havok.png` オブジェクトは* X-men *ルールをテストすることを意図していました。

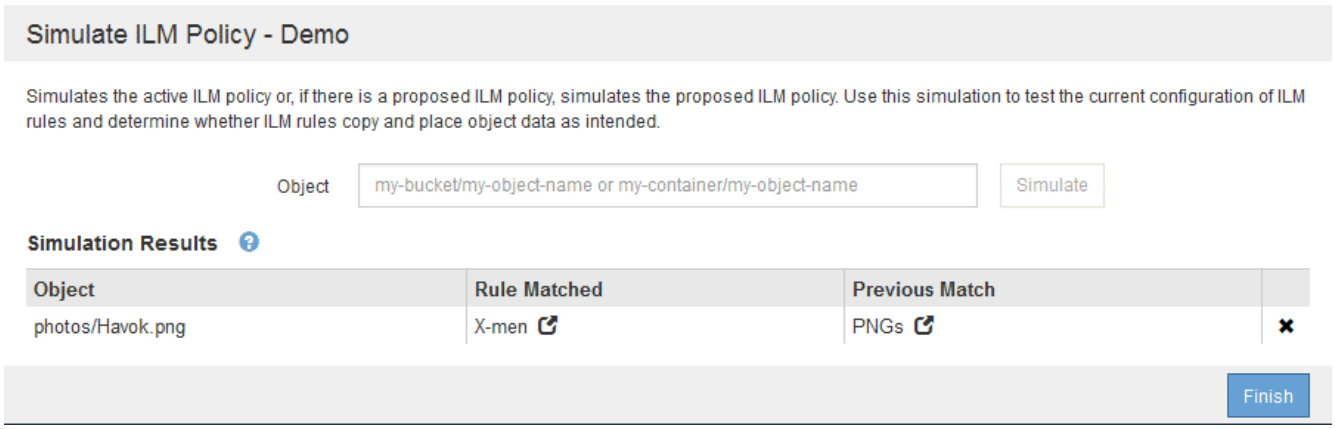
3. 問題 を解決するには、ルールの順序を変更します。
   a. Finish *をクリックして、Simulate ILM Policyページを閉じます。
   b. * Edit *をクリックして、ポリシーを編集します。
   c. 「 * X-men 」ルールをリストの先頭にドラッグします。



d. [保存（ Save ）] をクリックします。

4. * Simulate *をクリックします。

以前にテストしたオブジェクトが更新したポリシーに照らして再評価され、新しいシミュレーション結果が表示されます。この例では、Rule Matched列にが表示されています `Havok.png` 想定どおりに「X-men」メタデータルールに一致します。以前の一致列には、 PNGs ルールが以前のシミュレーションでオブジェクトに一致したことが示されます。



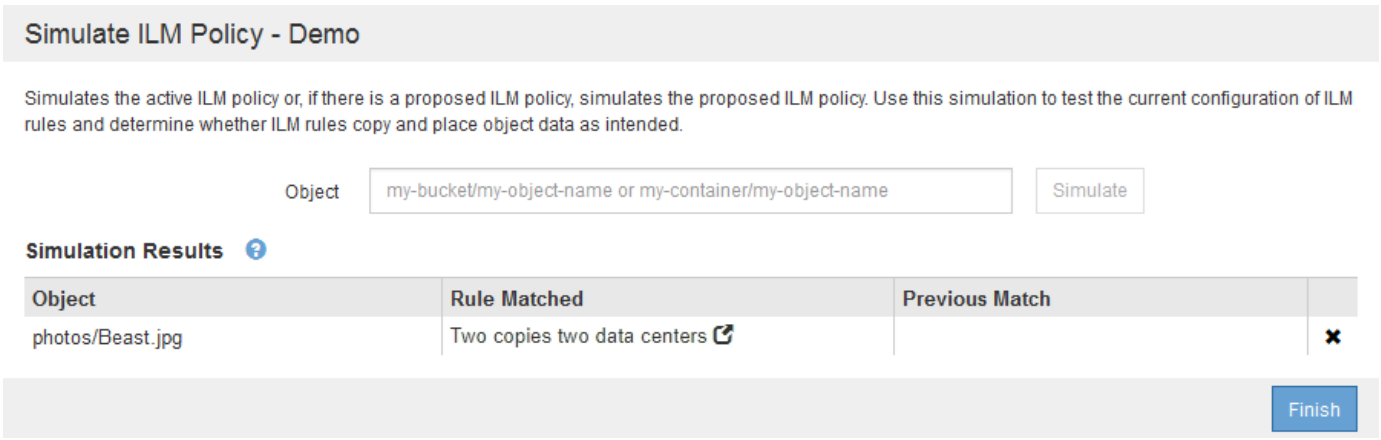
[ポリシーの設定] ページを開いたままにしておくと、テストオブジェクトの名前を再入力しなくても、変更後にポリシーを再シミュレートできます。

例 **3** ：ドラフトの **ILM** ポリシーをシミュレートする際にルールを修正する

この例では、ポリシーをシミュレートしてポリシー内のルールを修正し、シミュレーションを続行する方法を示します。

この例では、 * Demo * ポリシーをシミュレートします。このポリシーの目的は、が含まれるオブジェクトを

検索することです `series=x-men` ユーザメタデータ。ただし、に対してシミュレートしたところ予期しない結果が発生しました `Beast.jpg` オブジェクト。オブジェクトが「 X-men 」メタデータルールではなくデフォルトルールに一致しましたが、 2 つのデータセンターがコピーされています。

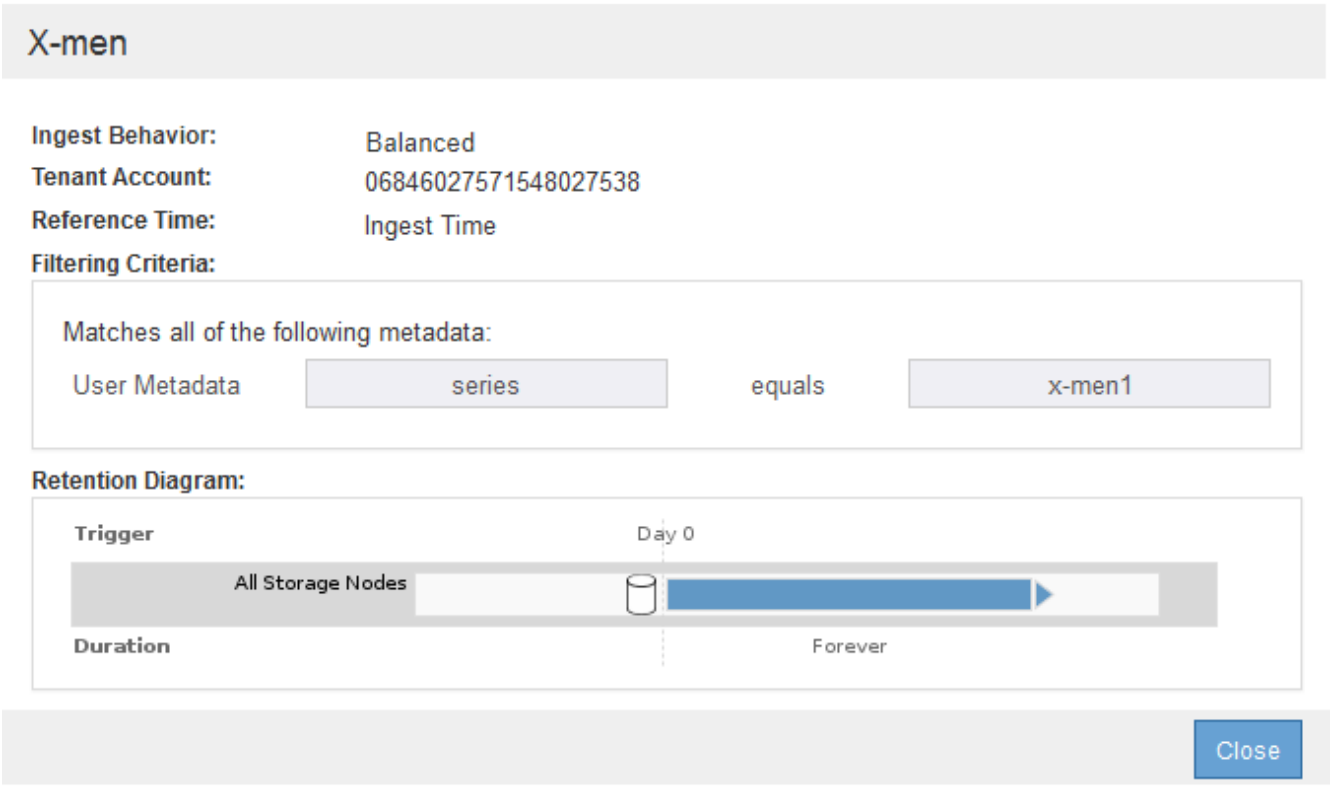


テストオブジェクトがポリシー内の想定したルールに一致しない場合は、ポリシー内の各ルールを調べてエラーを修正する必要があります。

手順

1. ポリシー内のルールごとに、ルール名または詳細アイコンをクリックしてルール設定を確認します をクリックします。
2. ルールのテナントアカウント、参照時間、およびフィルタ条件を確認します。

   この例では、「 X-men 」ルールのメタデータにエラーがあります。メタデータ値は「 x-men. 」ではなく「 x-men1 」として入力されました。



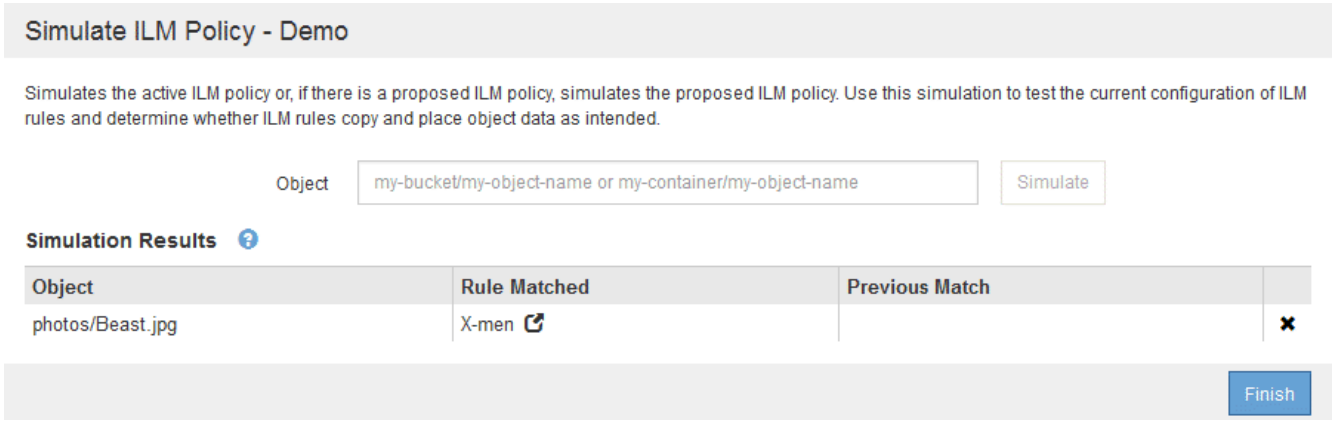
3. このエラーを解決するには、次のようにルールを修正します。
   - ルールがドラフトポリシーに含まれている場合は、ルールをクローニングするか、ポリシーから削除してポリシーを編集できます。
   - ルールがアクティブポリシーに含まれている場合は、ルールをクローニングする必要があります。アクティブポリシーのルールは編集または削除できません。

オプション	説明
ルールをクローニングしています	i. [* ILM*>* Rules] を選択します。 ii. 不正なルールを選択し、* Clone *をクリックします。 iii. 誤った情報を変更して、*保存*をクリックします。 iv. 「 * ILM * > * Policies * 」を選択します。 v. ドラフトポリシーを選択し、* Edit *をクリックします。 vi. [ルールの選択]をクリックします。 vii. 新しいルールのチェックボックスをオンにし、元のルールのチェックボックスをオフにして、*適用*をクリックします。 viii. [保存（ Save ）] をクリックします。
ルールを編集しています	i. ドラフトポリシーを選択し、* Edit *をクリックします。 ii. 削除アイコンをクリックします ✖ 誤ったルールを削除するには、*保存*をクリックします。 iii. [* ILM*>* Rules] を選択します。 iv. 不正なルールを選択し、*編集*をクリックします。 v. 誤った情報を変更して、*保存*をクリックします。 vi. 「 * ILM * > * Policies * 」を選択します。 vii. ドラフトポリシーを選択し、* Edit *をクリックします。 viii. 修正したルールを選択し、*適用*をクリックして、*保存*をクリックします。

4. もう一度シミュレーションを実行します。

> ILM ポリシーページから移動してルールを編集したため、以前にシミュレーションで入力したオブジェクトは表示されなくなりました。オブジェクトの名前を再入力する必要があります。

この例では、修正した「X-men」ルールがに一致します `Beast.jpg` に基づくオブジェクト `series=x-men` ユーザメタデータ（期待どおり）。



ILMポリシーをアクティブ化します

ドラフトの ILM ポリシーに ILM ルールを追加してポリシーをシミュレートし、ポリシーが想定どおりに動作することを確認したら、ドラフトポリシーをアクティブ化できます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。
- ドラフトのILMポリシーを保存し、シミュレートしておく必要があります。

> 原因 ポリシーにエラーがあると、回復不能なデータ損失が発生する可能性があります。ポリシーをアクティブ化する前によく確認およびシミュレートし、想定どおりに機能することを確認してください。

> 新しい ILM ポリシーをアクティブ化すると、 StorageGRID は、そのポリシーを使用して、既存のオブジェクトと新たに取り込まれたオブジェクトを含むすべてのオブジェクトを管理します。新しい ILM ポリシーをアクティブ化する前に、既存のレプリケートオブジェクトとイレイジャーコーディングオブジェクトの配置に対する変更を確認してください。既存のオブジェクトの場所を変更すると、新しい配置が評価されて実装される際に一時的なリソースの問題が発生する可能性があります。

このタスクについて

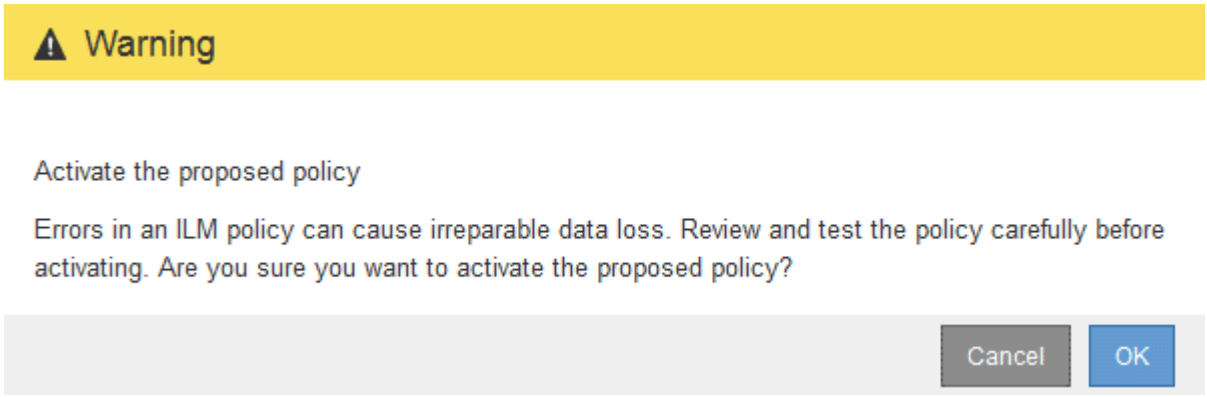
ILM ポリシーをアクティブ化すると、システムは新しいポリシーをすべてのノードに配布します。ただし、すべてのグリッドノードが新しいアクティブポリシーを受信できるようになるまで、新しいポリシーが実際には有効にならない場合があります。グリッドオブジェクトが誤って削除されないように、システムが新しいアクティブポリシーの実装を待機する場合もあります。

- データの冗長性や耐久性を向上させる変更をポリシーに加えた場合、変更内容はすぐに実装されます。たとえば、 2 コピーのルールではなく 3 コピーのルールを含む新しいポリシーをアクティブ化した場合、そのポリシーはすぐに実装されます。これは、データの冗長性が向上するためです。
- データの冗長性や耐久性を低下させる可能性のある変更をポリシーに加えた場合、変更内容はすべてのグリッドノードが使用可能になるまで実装されません。たとえば、 3 コピーのルールではなく 2 コピーのルールを使用する新しいポリシーをアクティブ化すると、新しいポリシーは「 Active 」とマークされますが、すべてのノードがオンラインで使用可能になるまで有効になりません。

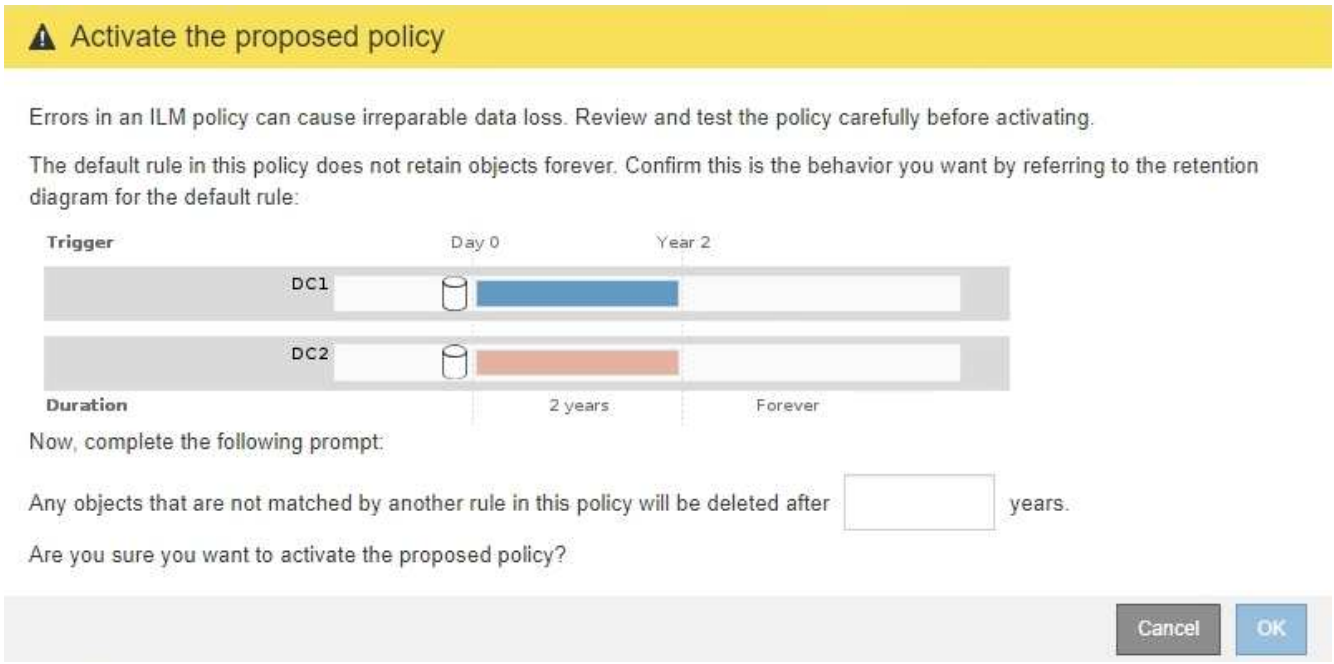
手順

1. ドラフトポリシーをアクティブ化する準備ができたら、ILMポリシーページでポリシーを選択し、*アクティブ化*をクリックします。

   警告メッセージが表示され、ドラフトポリシーをアクティブ化するかどうかの確認を求められます。



   ポリシーのデフォルトルールがオブジェクトを無期限に保持しない場合は、警告メッセージにプロンプトが表示されます。この例の保持図では、デフォルトルールによって 2 年後にオブジェクトが削除されることが示されています。テキストボックスに「 * 2 * 」と入力して、ポリシー内の別のルールに一致しないオブジェクトが 2 年後に StorageGRID から削除されることを確認する必要があります。

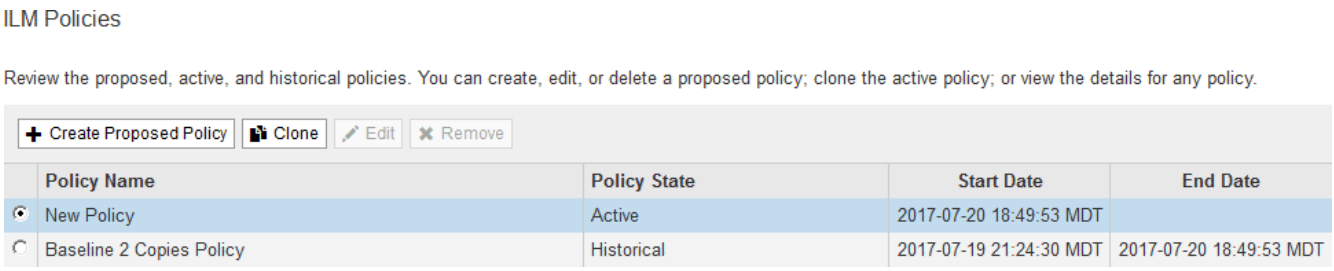


2. [OK] をクリックします。

結果

新しい ILM ポリシーがアクティブ化されると次のようになります。

- ポリシーのポリシーの状態がアクティブと表示されます。[開始日] エントリには、ポリシーがアクティブ化された日時が表示されます。



- 以前にアクティブだったポリシーが、ポリシーの状態が Historical と表示されます。[開始日] と [終了日] のエントリは、ポリシーがアクティブになった日時と、ポリシーが有効でなくなった日時を示します。

関連情報

"例 6 ： ILM ポリシーを変更する"

オブジェクトメタデータの検索による**ILM**ポリシーの検証

ILM ポリシーをアクティブ化したら、そのポリシーを表すテストオブジェクトを StorageGRID システムに取り込む必要があります。次に、オブジェクトメタデータの検索を実行して、コピーが意図したとおりに作成され、正しい場所に配置されていることを確認します。

必要なもの

- 次のいずれかのオブジェクト ID が必要です。
  - **UUID** ：オブジェクトの Universally Unique Identifier です。UUID はすべて大文字で入力します。
  - * CBID * ： StorageGRID 内のオブジェクトの一意の識別子。監査ログからオブジェクトの CBID を取得できます。CBID はすべて大文字で入力します。
  - * S3 のバケットとオブジェクトキー * ：オブジェクトが S3 インターフェイスから取り込まれた場合、クライアントアプリケーションはバケットとオブジェクトキーの組み合わせを使用してオブジェクトを格納および識別します。
  - * Swift のコンテナとオブジェクト名 * ：オブジェクトが Swift インターフェイスから取り込まれた場合、クライアントアプリケーションはコンテナとオブジェクト名の組み合わせを使用してオブジェクトを格納および識別します。

手順

1. オブジェクトを取り込みます。
2. 「* ILM > Object Metadata Lookup *」を選択します。
3. [* 識別子 * （ * Identifier * ）] フィールドにオブジェクトの識別子を入力します。

   UUID 、 CBID 、 S3 バケット / オブジェクトキー、または Swift コンテナ / オブジェクト名を入力できます。

4. [*検索（Look Up）]をクリックします。

   オブジェクトメタデータの検索結果が表示されます。このページには、次の種類の情報が表示されます。

   - システムメタデータ（オブジェクト ID （ UUID ）、オブジェクト名、コンテナの名前、テナントアカウントの名前または ID 、オブジェクトの論理サイズ、オブジェクトの作成日時、オブジェクトの最終変更日時など）。
   - オブジェクトに関連付けられているカスタムユーザメタデータのキーと値のペア。
   - S3 オブジェクトの場合、オブジェクトに関連付けられているオブジェクトタグのキーと値のペア。
   - レプリケートオブジェクトコピーの場合、各コピーの現在の格納場所。
   - イレイジャーコーディングオブジェクトコピーの場合、各フラグメントの現在の格納場所。
   - クラウドストレージプール内のオブジェクトコピーの場合、外部バケットの名前とオブジェクトの一意の識別子を含むオブジェクトの場所。
   - セグメント化されたオブジェクトとマルチパートオブジェクトの場合、セグメント ID とデータサイズを含むオブジェクトセグメントのリスト。100 個を超えるセグメントを持つオブジェクトの場合は、最初の 100 個のセグメントだけが表示されます。
   - 未処理の内部ストレージ形式のすべてのオブジェクトメタデータ。この未加工のメタデータには、リリース間で維持されるとはかぎらない内部のシステムメタデータが含まれます。

     次の例では、 2 つのレプリケートコピーとして格納された S3 テストオブジェクトのオブジェクトメタデータの検索結果が表示されています。

System Metadata

Object ID	A12E96FF-B13F-4905-9E9E-45373F6E7DA8
Name	testobject
Container	source
Account	t-1582139188
Size	5.24 MB
Creation Time	2020-02-19 12:15:59 PST
Modified Time	2020-02-19 12:15:59 PST

Replicated Copies

Node	Disk Path
99-97	/var/local/rangedb/2/p/06/0B/00nM8H$|TFbnQQ}|CV2E
99-99	/var/local/rangedb/1/p/12/0A/00nM8H$|TFboW28|CXG%

Raw Metadata


```
{
    "TYPE": "CTNT",
    "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
    "NAME": "testobject",
    "CBID": "0x8823DE7EC7C10416",
    "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
    "PPTH": "source",
    "META": {
        "BASE": {
            "PAWS": "2",
```


5. オブジェクトが正しい場所に格納され、コピーのタイプが正しいことを確認します。

監査オプションが有効になっている場合は、監査ログを監視して「 ORLM Object Rules Met 」というメッセージを探すこともできます。ORLM 監査メッセージからは、 ILM 評価プロセスのより詳細なステータスを確認できますが、オブジェクトデータの配置が正しいかどうかや、 ILM ポリシーが完全かどうかに関する情報は得られません。これは自分で評価する必要があります。詳細については、監査メッセージに関する情報を参照してください。

関連情報

"監査ログを確認します"

"S3 を使用する"

"Swift を使用します"

ILM ルールと ILM ポリシーを作成したあとも、引き続きストレージ要件の変化に合わせて設定を変更できます。

ILMルールを削除する

ILM ルールのリストを管理しやすくするためには、使用しない ILM ルールを削除してください。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

> ILM ルールは、アクティブポリシーまたはドラフトポリシーで現在使用されている場合は削除できません。ポリシーを使用している ILM ルールを削除する必要がある場合は、まず次の手順を実行する必要があります。
>
> 1. アクティブポリシーをクローニングするか、ドラフトポリシーを編集します。
> 2. ポリシーから ILM ルールを削除します。
> 3. 新しいポリシーを保存、シミュレート、およびアクティブ化して、オブジェクトが想定どおりに保護されるようにします。

手順

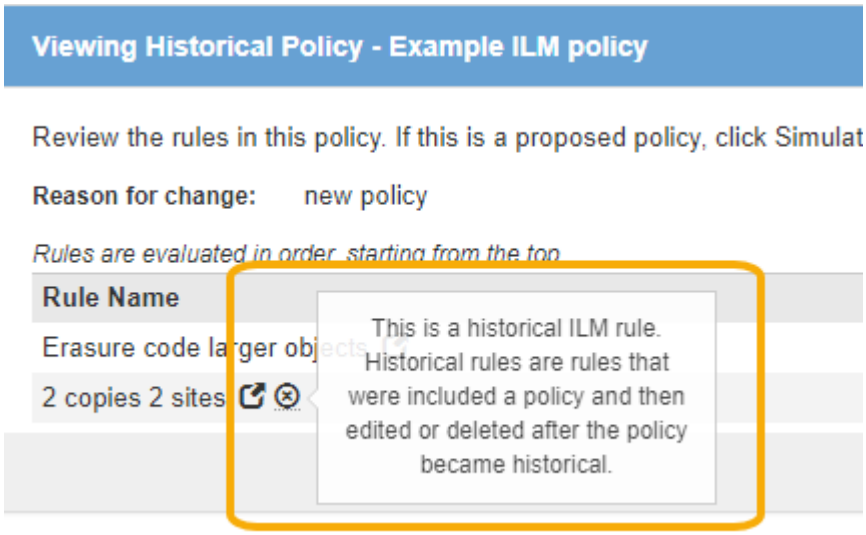
1. [* ILM*>* Rules] を選択します。
2. 削除するルールのテーブルエントリを確認します。

   ルールがアクティブな ILM ポリシーまたはドラフトの ILM ポリシーで使用されていないことを確認します。

3. 削除するルールが使用されていない場合は、ラジオボタンを選択し、 * 削除 * を選択します。
4. 「 * OK 」を選択して、 ILM ルールを削除することを確認します。

   ILM ルールが削除されます。

履歴ポリシーで使用されているルールを削除すると、が削除されます ⊗ ポリシーを表示するとルールのアイコンが表示されます。これは、ルールが履歴ルールになったことを示します。



関連情報

"ILMポリシーを作成する"

ILMルールを編集する

ILM ルールを編集して、フィルタまたは配置手順を変更しなければならない場合があります。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

このタスクについて

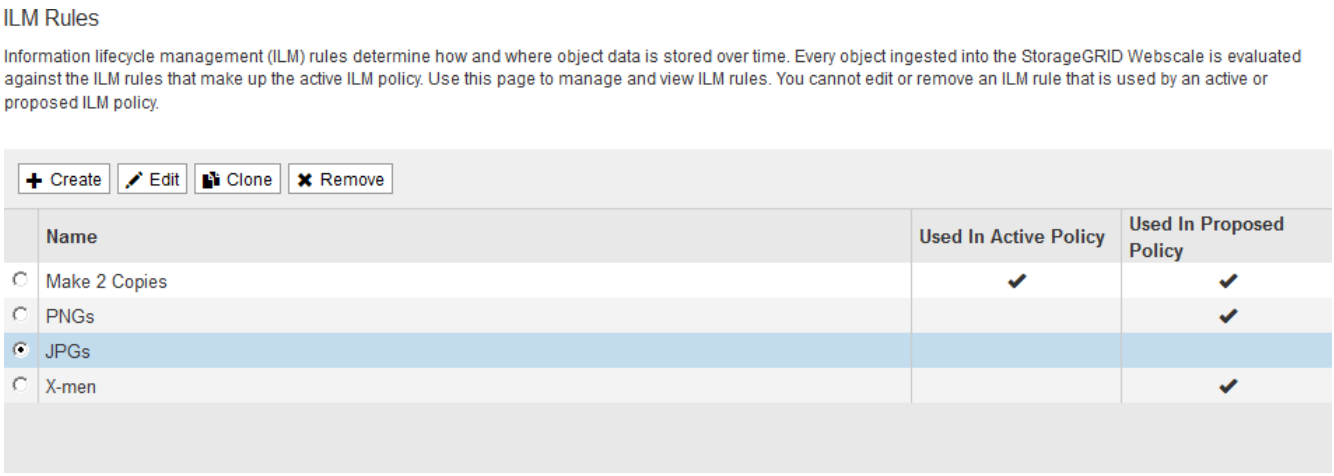
ドラフトの ILM ポリシーまたはアクティブな ILM ポリシーで使用されているルールを編集することはできません。代わりに、これらのルールをクローニングして、クローニングしたコピーに必要な変更を加えることができます。組み込みの ILM ルール（ Make 2 Copies ）や StorageGRID バージョン 10.3 より前に作成された ILM ルールも編集できません。

編集原因 したルールをアクティブな ILM ポリシーに追加する前に、オブジェクトの配置手順の変更によってシステムの負荷が増大する可能性があることに注意してください。

手順

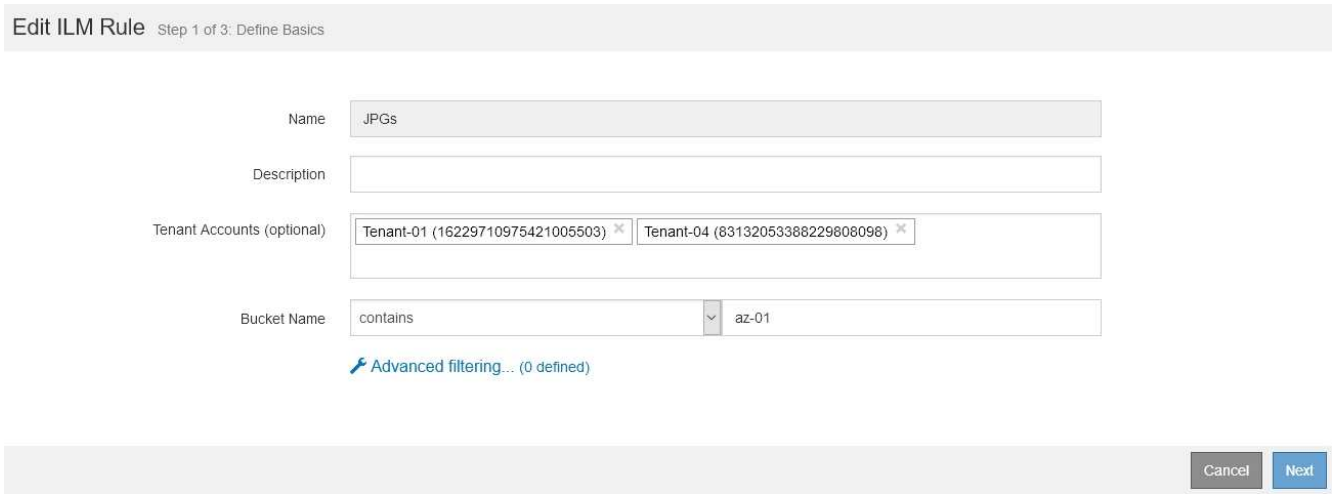
1. [* ILM*>* Rules] を選択します。

   ILM ルールページが表示されます。このページには、使用可能なすべてのルールと、アクティブポリシーまたはドラフトポリシーで使用されているルールが表示されます。



2. 使用されていないルールを選択し、*編集*をクリックします。

   ILM ルールの編集ウィザードが開きます。

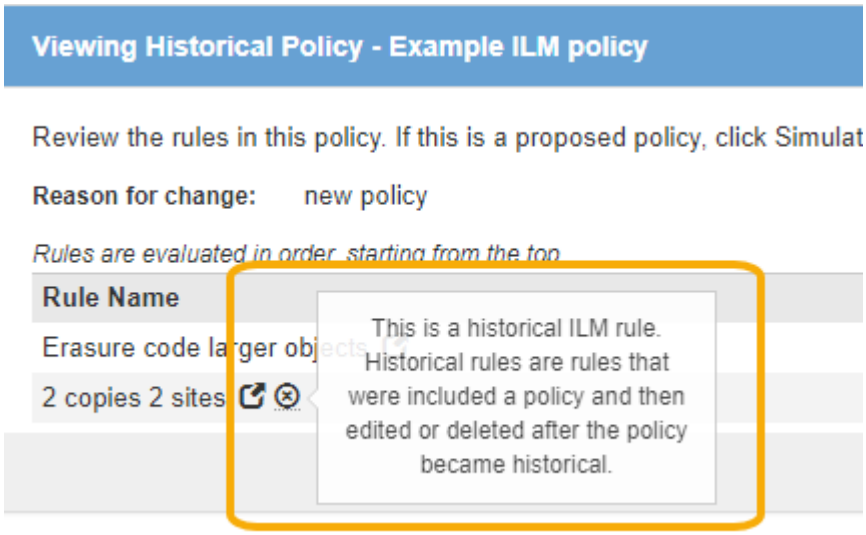


3. ILMルールの作成手順と高度なフィルタを使用する手順に従って、Edit ILM Ruleウィザードの各ページのオプションを設定します。

   ILM ルールの編集時に、 ILM ルールの名前を変更することはできません。

4. [保存（ Save ）] をクリックします。

履歴ポリシーで使用されているルールを編集すると、が表示されます ⊗ ポリシーを表示するとルールのアイコンが表示されます。これは、ルールが履歴ルールになったことを示します。



関連情報

"ILMルールを作成する"

"ILMルールで高度なフィルタを使用する"

ILMルールをクローニングする

ドラフトの ILM ポリシーまたはアクティブな ILM ポリシーで使用されているルールを編集することはできません。代わりに、ルールをクローニングして、クローニングしたコピーに必要な変更を加えることができます。その後、必要に応じてドラフトポリシーから元のルールを削除し、変更後のバージョンに置き換えることができます。バージョン 10.2 以前の StorageGRID を使用して作成された ILM ルールはクローニングできません。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

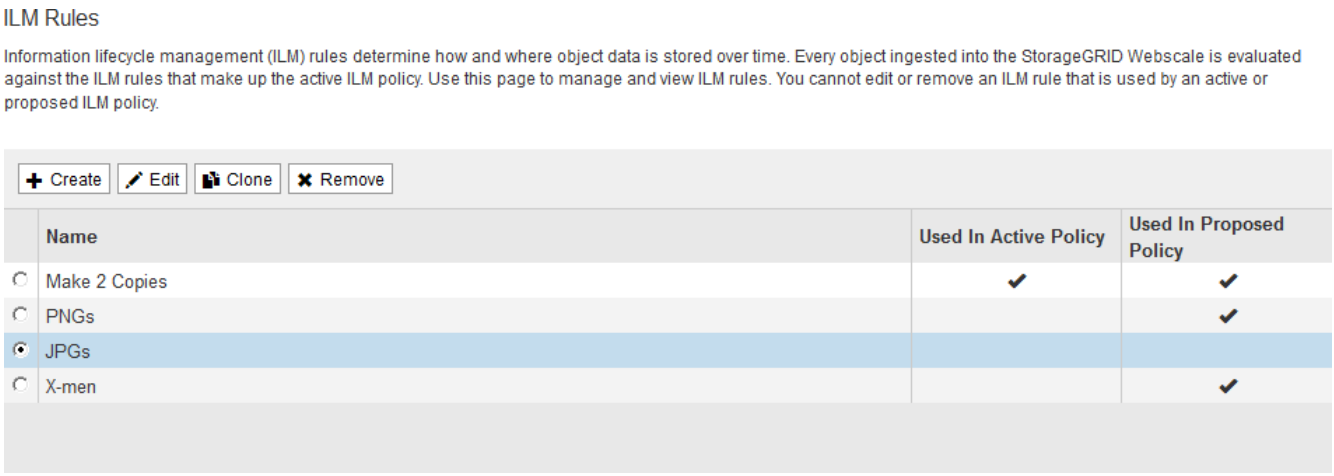
このタスクについて

アクティブな ILM ポリシー原因 にクローニングされたルールを追加する前に、オブジェクトの配置手順の変更によってシステムの負荷が増加する可能性があることに注意してください。

手順

1. [* ILM*>* Rules] を選択します。

   ILM ルールページが表示されます。



2. クローニングするILMルールを選択し、* Clone *をクリックします。

   Create ILM Rule ウィザードが開きます。

3. ILM ルールの編集手順に従い、高度なフィルタを使用して、クローニングされたルールを更新します。

   ILM ルールをクローニングする場合は、新しい名前を入力する必要があります。

4. [保存（ Save ）] をクリックします。

   新しい ILM ルールが作成されます。

関連情報

"ILMルールおよびILMポリシーの操作"

"ILMルールで高度なフィルタを使用する"

ILMポリシーアクティビティキューの表示

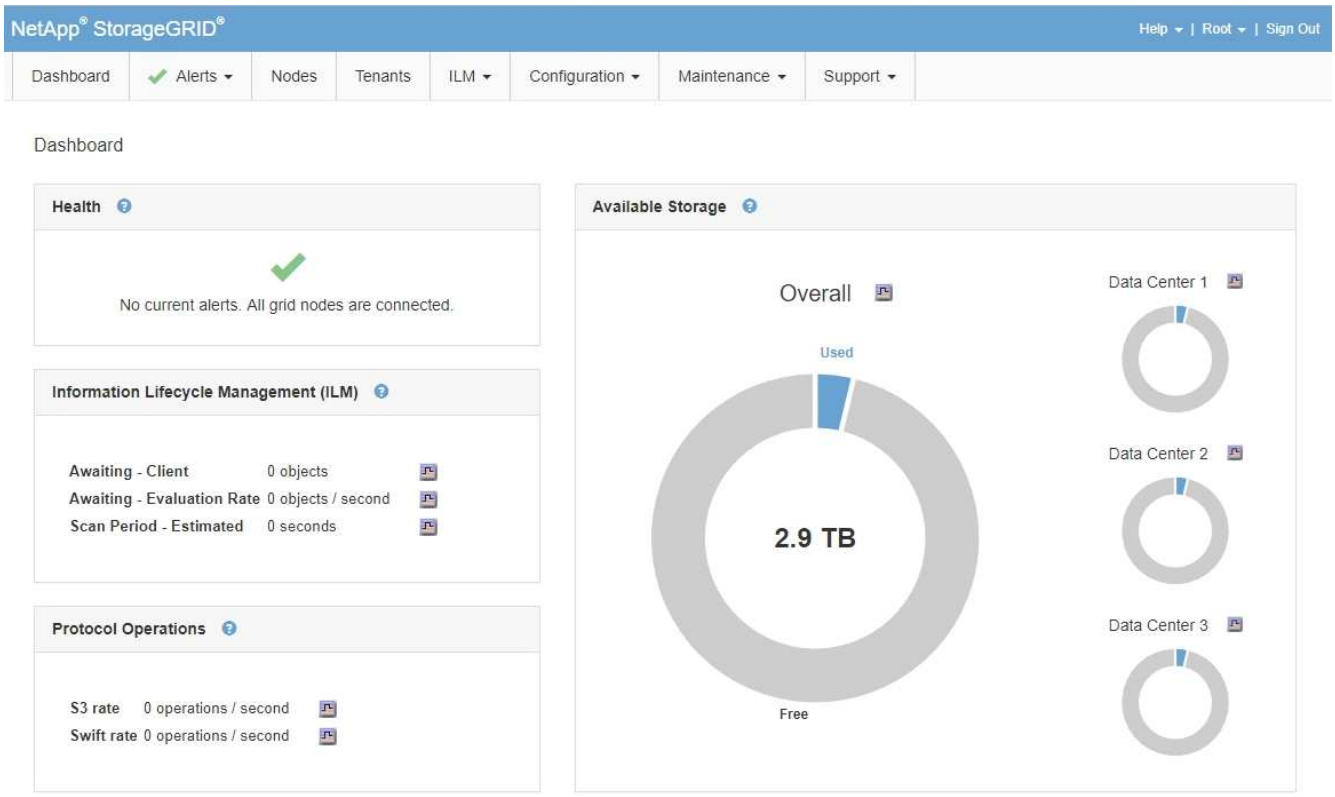
ILM ポリシーに対する評価を待機している、キュー内のオブジェクトの数をいつでも表示できます。システムパフォーマンスを確認するために、 ILM 処理キューの監視が必要になる場合があります。キューが大きい場合は、システムが取り込み速度に対応できていない、クライアントアプリケーションからの負荷が大きすぎる、何らかの異常な状態が存在する、などが考えられます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

手順

1. 「 * ダッシュボード * 」を選択します。



2. 情報ライフサイクル管理（ ILM ）セクションを監視する。

   疑問符をクリックできます をクリックすると、このセクションの項目の概要 が表示されます。

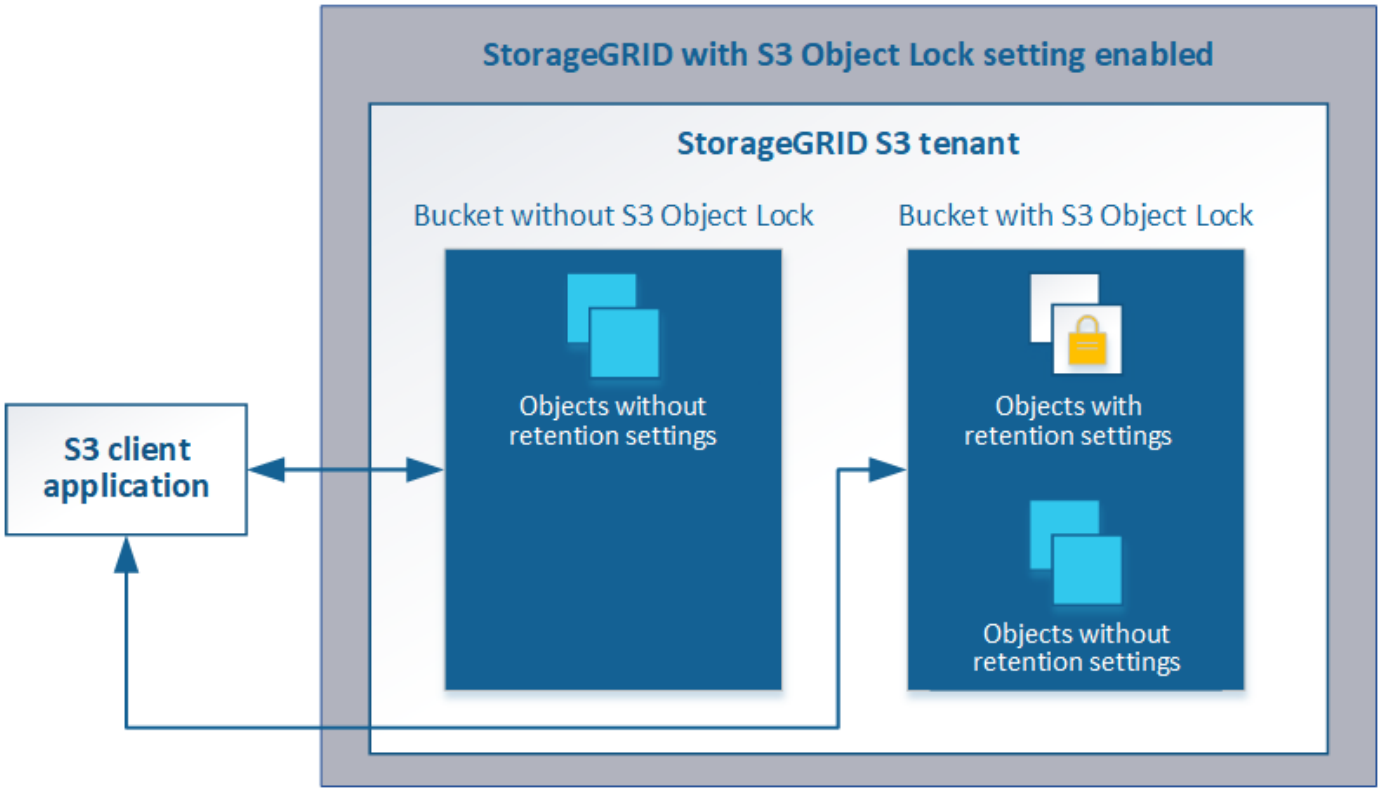
S3オブジェクトロックでオブジェクトを管理する

グリッド管理者は、 StorageGRID システムで S3 オブジェクトロックを有効にし、準拠 ILM ポリシーを実装して、特定の S3 バケット内のオブジェクトが指定した期間にわたって削除または上書きされないようにすることができます。

S3 オブジェクトのロックとは何ですか？

StorageGRID S3 オブジェクトロック機能は、 Amazon Simple Storage Service （Amazon S3 ）での S3 オブジェクトロックに相当するオブジェクト保護解決策 です。

図に示すように、 StorageGRID システムでグローバルな S3 オブジェクトのロック設定が有効になっている場合、 S3 テナントアカウントでは、 S3 オブジェクトのロックを有効にしているかどうかに関係なくバケットを作成できます。バケットで S3 オブジェクトのロックが有効になっている場合、 S3 クライアントアプリケーションは、そのバケット内の任意のオブジェクトバージョンの保持設定を必要に応じて指定できます。オブジェクトのバージョンには、 S3 オブジェクトロックで保護するように指定された保持設定が必要です。



StorageGRID S3 オブジェクトロック機能は、 Amazon S3 準拠モードと同等の単一の保持モードを提供します。デフォルトでは、保護されたオブジェクトバージョンは、どのユーザーでも上書きまたは削除できません。StorageGRID S3 オブジェクトのロック機能では、ガバナンスモードはサポートされず、特別な権限を持つユーザは保持設定を省略したり保護されたオブジェクトを削除したりすることはできません。

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、 S3 クライアントアプリケーションは、オブジェクトの作成時または更新時に、次のオブジェクトレベルの保持設定のいずれか、または両方を必要に応じて指定できます。

- **Retain Until - date** ：オブジェクトバージョンの retain-until - date が将来の日付である場合、オブジェクトは読み出し可能ですが、変更または削除することはできません。必要に応じて、オブジェクトの retain-date を増やすことはできますが、この日付を減らすことはできません。
- * リーガルホールド * ：オブジェクトバージョンにリーガルホールドを適用すると、そのオブジェクトがただちにロックされます。たとえば、調査または法的紛争に関連するオブジェクトにリーガルホールドを設定する必要がある場合があります。リーガルホールドには有効期限はありませんが、明示的に削除されるまで保持されます。リーガルホールドは、それまでの保持期間とは関係ありません。

これらの設定の詳細については、の「Using S3 object lock」を参照してください "S3 REST API のサポートされる処理と制限事項"。

S3 オブジェクトロックと従来の準拠の比較

StorageGRID 11.5のS3オブジェクトロック機能は、以前のバージョンのStorageGRID で使用できた準拠機能に代わる機能です。新しいS3オブジェクトロック機能はAmazon S3の要件に準拠しているため、「従来のコンプライアンス」と呼ばれる独自のStorageGRID 準拠機能は廃止されています。

グローバル準拠設定を有効にしている場合は、StorageGRID 11.5にアップグレードすると、新しいグローバ

ルS3オブジェクトロック設定が自動的に有効になります。テナントユーザは、StorageGRID 11.5で準拠を有効にした新しいバケットを作成できなくなります。ただし、必要に応じて、テナントユーザは既存の従来の準拠バケットを引き続き使用および管理できます。これには次のタスクの実行が含まれます。

- 従来の準拠が有効になっている既存のバケットに新しいオブジェクトを取り込む。
- 従来の準拠が有効になっている既存のバケットの保持期間を延長する。
- 従来の準拠が有効になっている既存のバケットの自動削除設定を変更する。
- 従来の準拠が有効になっている既存のバケットにリーガルホールドを適用する。
- リーガルホールドを解除する。

"ネットアップのナレッジベース： StorageGRID 11.5 でレガシー準拠バケットを管理する方法"

以前のバージョンの StorageGRID で従来の準拠機能を使用していた場合、次の表を参照して、 StorageGRID の S3 オブジェクトロック機能と比較する方法を確認してください。

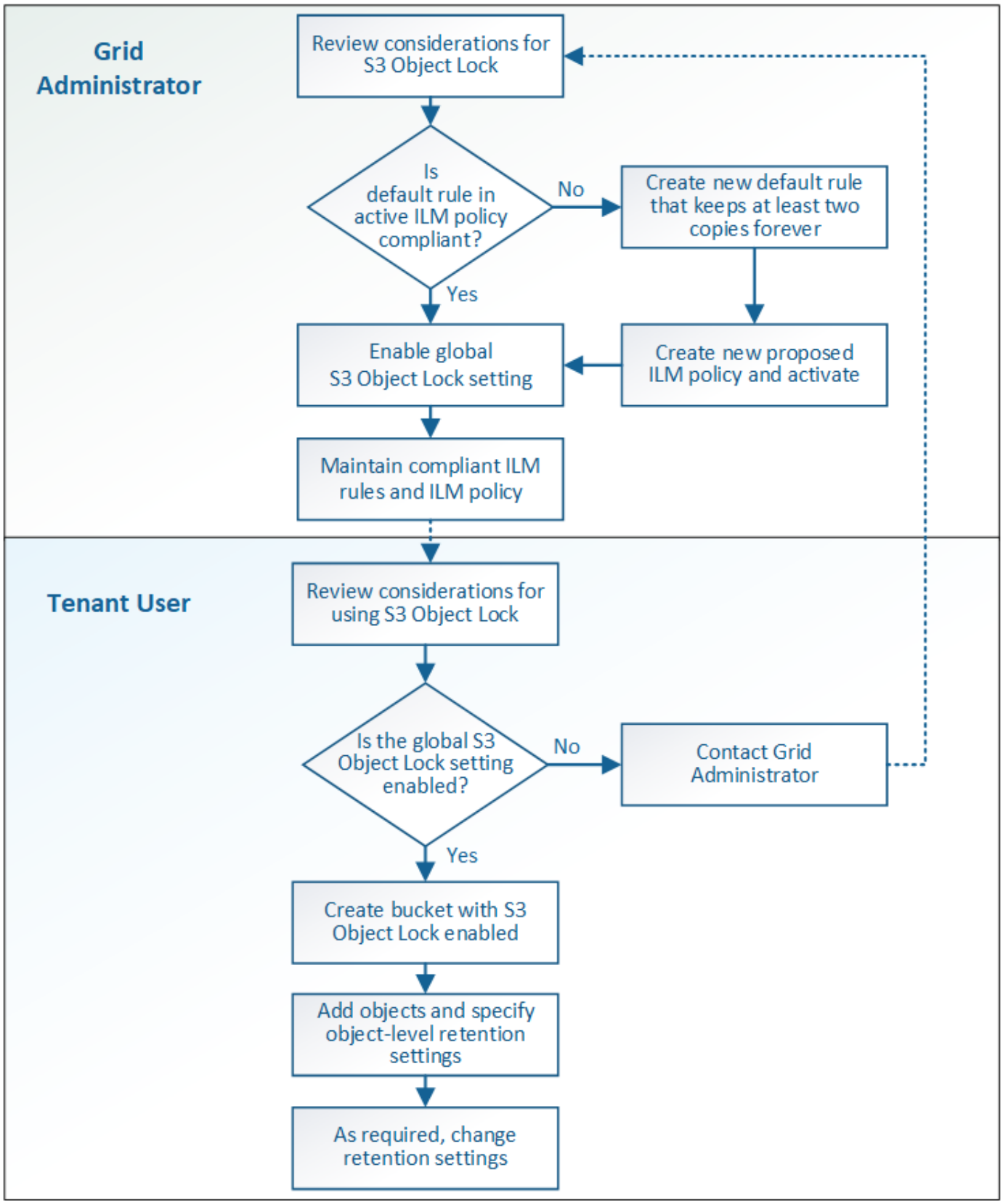
	S3 オブジェクトロック（新規）	コンプライアンス（レガシー）
この機能はグローバルにどのように有効になりますか。	Grid Managerから* Configuration > System Settings > S3 Object Lock *を選択します。	サポートは終了しました。 *注：グローバル準拠設定を有効にしている場合、StorageGRID 11.5にアップグレードすると、グローバルなS3オブジェクトロック設定が自動的に有効になります。
バケットで機能を有効にするにはどうすればよいですか？	Tenant Manager 、テナント管理 API 、または S3 REST API を使用して新しいバケットを作成するときは、 S3 オブジェクトロックを有効にする必要があります。	準拠を有効にした新しいバケットを作成することはできなくなりました。ただし、既存の準拠バケットには引き続き新しいオブジェクトを追加できます。
バケットのバージョン管理はサポートされているか	はい。バケットのバージョン管理は必須であり、バケットで S3 オブジェクトのロックが有効になっている場合は自動的に有効になります。	いいえ従来の準拠機能では、バケットのバージョン管理は許可されていません。
オブジェクト保持はどのように設定されますか。	ユーザーは、オブジェクトバージョンごとに retain-until date を設定できます。	ユーザはバケット全体の保持期間を設定する必要があります。保持期間を指定すると、バケット内のすべてのオブジェクトが環境 で保持されます。
バケットには保持とリーガルホールドのデフォルト設定を適用できるか。	いいえS3オブジェクトのロックが有効になっているStorageGRID バケットでは、デフォルトの保持期間は使用されません。代わりに、オブジェクトバージョンごとにretain-dateを指定できます。	はい。

	S3 オブジェクトロック（新規）	コンプライアンス（レガシー）
保持期間は変更できますか。	オブジェクトバージョンの retain-until は、上げることはできますが、減らすことはできません。	バケットの保持期間は、増やすことはできますが、減らすことはできません。
リーガルホールドはどこで制御されますか？	バケット内のオブジェクトバージョンにリーガルホールドを適用したり、リーガルホールドを解除したりできます。	リーガルホールドはバケットに適用され、バケット内のすべてのオブジェクトに適用されます。
オブジェクトを削除できるのはいつですか。	オブジェクトがリーガルホールドの対象でない場合は、 retain-until 日に達したあとでオブジェクトバージョンを削除できます。	バケットがリーガルホールドの対象でない場合は、保持期間が過ぎたあとにオブジェクトを削除できます。オブジェクトは自動または手動で削除できます。
バケットライフサイクル設定はサポートされていますか。	はい。	いいえ

S3 オブジェクトロックのワークフロー

グリッド管理者は、テナントユーザと緊密に連携し、保持要件に応じてオブジェクトが保護されるようにする必要があります。

次のワークフロー図は、 S3 オブジェクトロックの使用手順の概要を示しています。以下の手順は、グリッド管理者およびテナントユーザが実行します。



Grid 管理者タスク

ワークフロー図に示されているように、 S3 テナントユーザが S3 オブジェクトロックを使用できるようにするには、グリッド管理者が次の 2 つのタスクを実行する必要があります。

1. 準拠 ILM ルールを少なくとも 1 つ作成し、アクティブな ILM ポリシー内のデフォルトルールに設定します。
2. StorageGRID システム全体で、グローバルな S3 オブジェクトロック設定を有効にします。

テナントユーザタスク

グローバルな S3 オブジェクトのロック設定を有効にしたあと、テナントは次のタスクを実行できます。

1. S3 オブジェクトのロックを有効にしたバケットを作成する。
2. これらのバケットにオブジェクトを追加し、オブジェクトレベルの保持期間とリーガルホールドの設定を指定します。
3. 必要に応じて、個々のオブジェクトの保持期間を更新するか、リーガルホールド設定を変更します。

関連情報

"テナントアカウントを使用する"

"S3 を使用する"

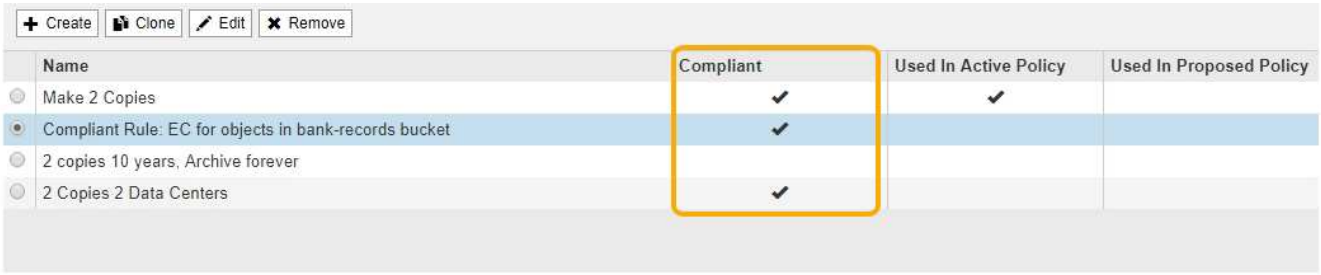
S3 オブジェクトのロックの要件

グローバルな S3 オブジェクトのロック設定を有効にするための要件、準拠 ILM ルールおよび ILM ポリシーを作成するための要件、および StorageGRID が S3 オブジェクトロックを使用するバケットとオブジェクトに適用する制限事項を確認しておく必要があります。

グローバルな **S3** オブジェクトロック設定を使用するための要件

- S3 テナントが S3 オブジェクトロックを有効にしてバケットを作成できるようにするには、 Grid Manager またはグリッド管理 API を使用してグローバルな S3 オブジェクトロック設定を有効にする必要があります。
- グローバルな S3 オブジェクトのロック設定を有効にすると、すべての S3 テナントアカウントで S3 オブジェクトのロックを有効にしてバケットを作成できるようになります。
- グローバルな S3 オブジェクトのロック設定を有効にしたあとに、設定を無効にすることはできません。
- アクティブなILMポリシーのデフォルトルールが_Compliant _でないとグローバルなS3オブジェクトロックを有効にすることはできません（つまり、デフォルトルールはS3オブジェクトロックが有効になっているバケットの要件を満たす必要があります）。
- グローバルな S3 オブジェクトのロック設定が有効になっている場合、ポリシーのデフォルトルールが準拠していないと、ドラフトの ILM ポリシーを新規作成したり、既存のドラフトの ILM ポリシーをアクティブ化したりすることはできません。グローバルな S3 オブジェクトのロック設定を有効にすると、 ILM ルールおよび ILM ポリシーのページに、準拠している ILM ルールが表示されます。

  次の例では、 ILM ルールページに、 S3 オブジェクトのロックが有効になっているバケットに準拠した 3 つのルールが表示されています。

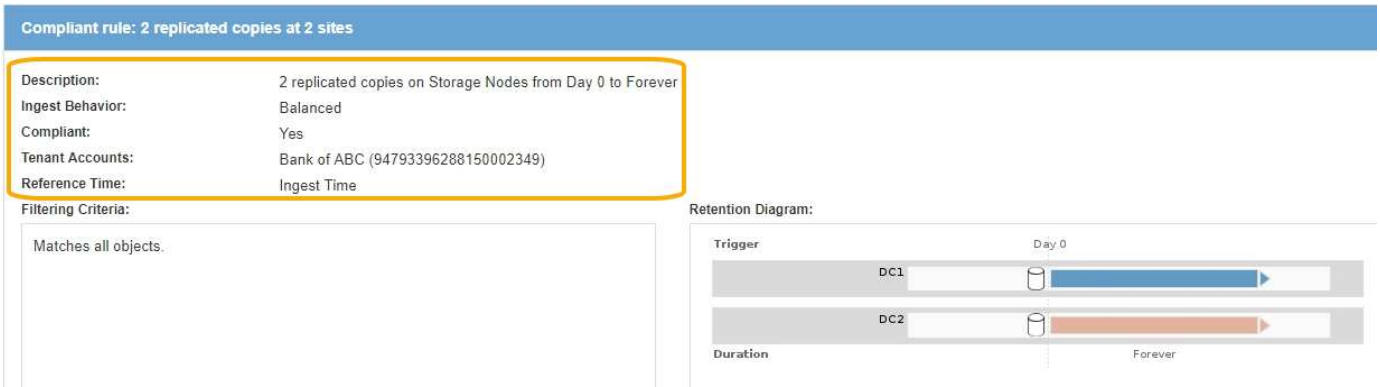


準拠 **ILM** ルールの要件

グローバルな S3 オブジェクトのロック設定を有効にする場合は、アクティブな ILM ポリシーのデフォルトルールが準拠していることを確認する必要があります。準拠ルールは、 S3 オブジェクトのロックが有効になっているバケットと従来の準拠が有効になっている既存のバケットの両方の要件を満たします。

- 2 つ以上のレプリケートオブジェクトコピーまたは 1 つのイレイジャーコーディングコピーを作成する。
- これらのコピーが、配置手順の各ラインの間、ストレージノード上に存在している必要があります。
- オブジェクトコピーをクラウドストレージプールに保存することはできません。
- オブジェクトコピーをアーカイブノードに保存することはできません。
- 配置手順の 1 行以上が、参照時間として * 取り込み時間 * を使用して 0 日目から開始されている必要があります。
- 配置手順の少なくとも 1 行は「無期限」である必要があります。

たとえば、次のルールは S3 オブジェクトのロックを有効にしたバケットの要件を満たしています。2 つの複製オブジェクト・コピーを取り込み時（ 0 日目）から「無期限」に格納します。 オブジェクトは 2 つのデータセンターのストレージノードに格納されます。



アクティブな **ILM** ポリシーとドラフトの **ILM** ポリシーの要件

グローバルな S3 オブジェクトのロック設定が有効になっている場合は、アクティブな ILM ポリシーとドラフ

トの ILM ポリシーに、準拠ルールと非準拠ルールの両方を含めることができます。

- アクティブな ILM ポリシーまたはドラフトの ILM ポリシーのデフォルトルールは、準拠ルールである必要があります。
- 非準拠ルールは、 S3 オブジェクトロックが有効になっていないバケット内のオブジェクト、または従来の準拠機能が有効になっていないオブジェクトのみに適用されます。
- 準拠ルールは任意のバケット内のオブジェクトに適用できます。 S3 オブジェクトのロックや従来の準拠を有効にする必要はありません。

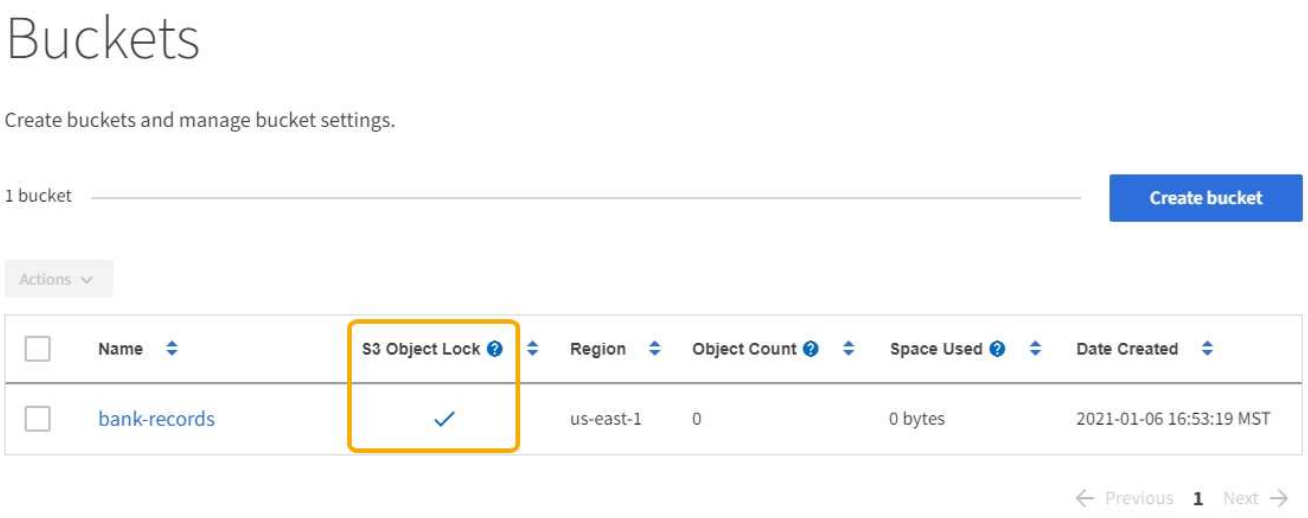
準拠 ILM ポリシーには、次の 3 つのルールが含まれる場合があります。

1. S3 オブジェクトのロックが有効な特定のバケット内にオブジェクトのイレイジャーコーディングコピーを作成する準拠ルール。EC コピーは、 0 日目から無期限にストレージノードに格納されます。
2. 2 つのレプリケートオブジェクトコピーを作成してストレージノードに 1 年間保存したあと、 1 つのオブジェクトコピーをアーカイブノードに移動して無期限に格納する非準拠ルール。このルールでは、 S3 オブジェクトロックまたはレガシー準拠が有効になっていない環境 バケットのみが無期限に格納され、アーカイブノードを使用するため、バケットのみが有効になります。
3. 2 つのレプリケートオブジェクトコピーを 0 日目からストレージノードに無期限に作成するデフォルトの準拠ルール。このルールは、最初の 2 つのルールでフィルタリングされなかったすべてのバケットのオブジェクトを環境 します。

S3 オブジェクトのロックを有効にした場合のバケットの要件

- StorageGRID システムでグローバルな S3 オブジェクトロック設定が有効になっている場合は、テナントマネージャ、テナント管理 API 、または S3 REST API を使用して、 S3 オブジェクトロックを有効にしたバケットを作成できます。

  次の Tenant Manager の例では、 S3 オブジェクトのロックが有効になっているバケットを示しています。



- S3 オブジェクトのロックを使用する場合は、バケットの作成時に S3 オブジェクトのロックを有効にする必要があります。既存のバケットに対して S3 オブジェクトロックを有効にすることはできません。
- S3 オブジェクトロックでは、バケットのバージョン管理が必要です。バケットで S3 オブジェクトのロックが有効になっている場合は、そのバケットのバージョン管理が StorageGRID で自動的に有効になります。

- S3 オブジェクトのロックを有効にしてバケットを作成したあとに、そのバケットの S3 オブジェクトのロックを無効にしたりバージョン管理を一時停止したりすることはできません。
- S3オブジェクトのロックが有効になっているStorageGRID バケットでは、デフォルトの保持期間はありません。代わりに、S3クライアントアプリケーションは、そのバケットに追加されるオブジェクトバージョンごとに保持期限とリーガルホールド設定を指定できます。
- バケットライフサイクル設定は S3 オブジェクトライフサイクルバケットでサポートされます。
- CloudMirror レプリケーションは、 S3 オブジェクトロックが有効になっているバケットではサポートされません。

S3 オブジェクトのロックが有効になっているバケット内のオブジェクトの要件

- S3クライアントアプリケーションは、S3オブジェクトのロックで保護する必要があるオブジェクトごとに保持設定を指定する必要があります。
- オブジェクトバージョンの retain-until date は増やすことができますが、この値を減らすことはできません。
- 係争中の訴訟や規制上の調査に関する通知があった場合、オブジェクトバージョンをリーガルホールドの対象にすることで関連情報を保持できます。オブジェクトバージョンがリーガルホールドの対象になっている場合は、それが retain-until 日に達しても、そのオブジェクトを StorageGRID から削除することはできません。リーガルホールドを解除すると、それまで保持期限に達した場合にオブジェクトバージョンを削除できるようになります。
- S3 オブジェクトロックにはバージョン管理されたバケットを使用する必要があります。保持設定はオブジェクトのバージョンごとに適用されます。オブジェクトバージョンには、 retain-until date 設定とリーガルホールド設定の両方を設定できます。ただし、オブジェクトバージョンを保持することはできません。また、どちらも保持することはできません。オブジェクトの retain-une-date 設定またはリーガルホールド設定を指定すると、要求で指定されたバージョンのみが保護されます。オブジェクトの以前のバージョンはロックされたまま、オブジェクトの新しいバージョンを作成できます。

S3 オブジェクトのロックが有効なバケット内のオブジェクトのライフサイクル

S3 オブジェクトのロックが有効になっているバケットに保存された各オブジェクトは、次の 3 つの段階を経て処理されます。

1. * オブジェクトの取り込み *
    - S3 オブジェクトのロックが有効になっているバケットにオブジェクトのバージョンを追加するときに、 S3 クライアントアプリケーションはオプションでオブジェクトの保持設定を指定できます（ retain-until date 、 legal hold 、または both ）。StorageGRID は、そのオブジェクトのメタデータを生成します。これには、一意のオブジェクト ID （ UUID ）と取り込み日時が含まれます。
    - 保持設定のあるオブジェクトのバージョンが取り込まれたあとに、そのデータと S3 ユーザ定義メタデータを変更することはできません。
    - StorageGRID は、オブジェクトメタデータをオブジェクトデータとは別に格納します。各サイトですべてのオブジェクトメタデータのコピーを 3 つ保持します。
2. * オブジェクト保持 *
    - オブジェクトの複数のコピーが StorageGRID によって格納される。コピーの正確な数、タイプ、格納場所は、アクティブな ILM ポリシーの準拠ルールによって決まります。
3. * オブジェクトの削除 *
    - オブジェクトは、 retain-until - date に到達したときに削除できます。

- リーガルホールドの対象になっているオブジェクトは削除できません。

関連情報

"テナントアカウントを使用する"

"S3 を使用する"

"S3 オブジェクトロックと従来の準拠の比較"

"例 7 ： S3 オブジェクトロックの準拠 ILM ポリシー"

"監査ログを確認します"

S3オブジェクトのロックをグローバルに有効にする

オブジェクトデータの保存時に 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 システム全体で S3 オブジェクトのロックを有効にする必要があります。グローバルな S3 オブジェクトのロック設定を有効にすると、 S3 テナントユーザは S3 オブジェクトのロックでバケットとオブジェクトを作成および管理できるようになります。

必要なもの

- Root Access 権限が必要です。
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- S3オブジェクトロックのワークフローを確認し、考慮事項を把握しておく必要があります。
- アクティブなILMポリシーのデフォルトルールは準拠ルールである必要があります。

  "デフォルトのILMルールを作成する"

  "ILMポリシーを作成する"

このタスクについて

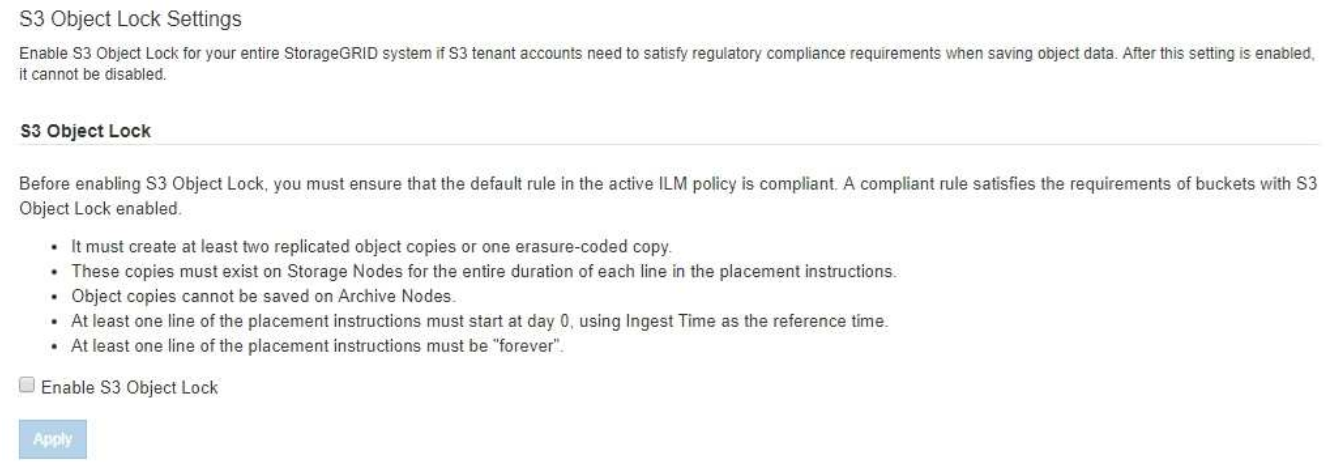
テナントユーザが S3 オブジェクトのロックを有効にした新しいバケットを作成できるようにするには、グリッド管理者がグローバルな S3 オブジェクトロック設定を有効にする必要があります。この設定を有効にすると、あとで無効にすることはできません。

> 以前のバージョンのStorageGRID を使用してグローバル準拠設定を有効にした場合は、StorageGRID バージョン11.5にアップグレードすると新しいS3オブジェクトロック設定が自動的に有効になります。既存の準拠バケットの設定の管理には引き続きStorageGRID を使用できますが、新しい準拠バケットを作成することはできません。
>
> "ネットアップのナレッジベース： StorageGRID 11.5 でレガシー準拠バケットを管理する方法"

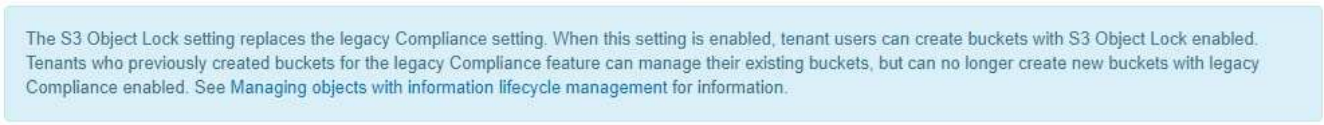
手順

1. * Configuration > System Settings > S3 Object Lock *を選択します。

   S3 Object Lock Settings （ S3 オブジェクトロック設定）ページが表示されます。

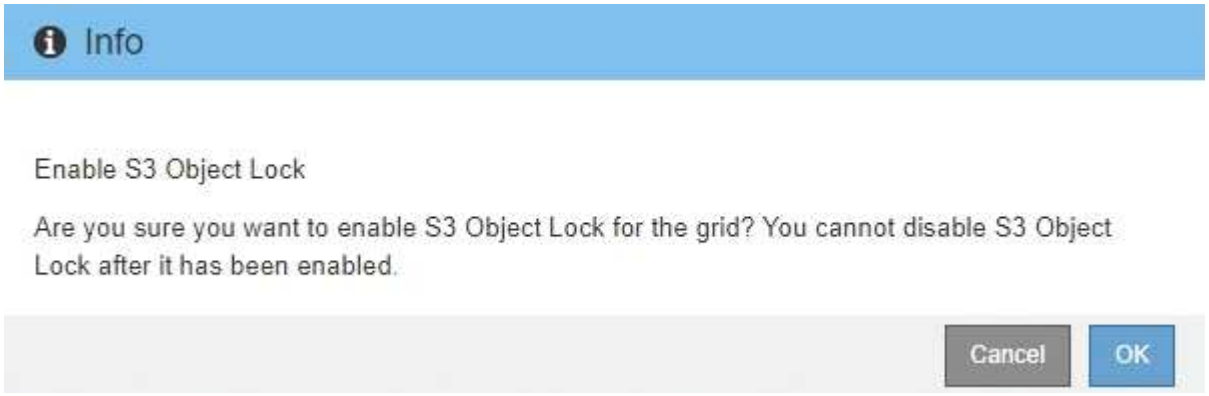


以前のバージョンの StorageGRID を使用してグローバル準拠設定を有効にした場合、ページには次の注が表示されます。



2. S3 オブジェクトロックを有効にする * を選択します。
3. * 適用 * を選択します。

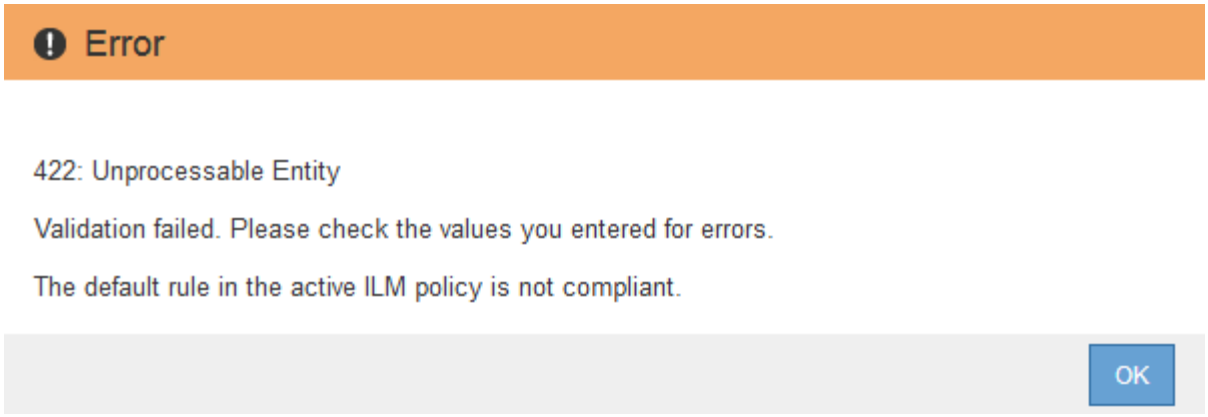
   確認のダイアログボックスが表示され、有効にした S3 オブジェクトのロックを無効にできないことを通知するメッセージが表示されます。



4. システム全体に対して S3 オブジェクトロックを永続的に有効にしてもよろしいですか？ * OK * を選択します。

   「 * OK * 」を選択した場合：

   - アクティブな ILM ポリシーのデフォルトルールが準拠している場合は、グリッド全体で S3 オブジェクトのロックが有効になり、無効にすることはできません。
   - デフォルトルールが準拠していない場合は、準拠ルールをデフォルトルールとして含む新しい ILM ポリシーを作成してアクティブ化する必要があることを示すエラーメッセージが表示されます。「 * OK 」を選択し、新しいドラフトポリシーを作成してシミュレートし、アクティブ化します。



完了後

グローバルなS3オブジェクトのロック設定を有効にしたあとで、新しいILMポリシーを作成できます。設定を有効にすると、 ILM ポリシーに、準拠デフォルトルールと非準拠デフォルトルールの両方をオプションで含めることができます。たとえば、 S3 オブジェクトロックが有効になっていないバケット内のオブジェクトに対してフィルタが適用されていない非準拠ルールを使用できます。

関連情報

"S3オブジェクトのロックが有効になったあとのILMポリシーの作成"

"ILMルールを作成する"

"ILMポリシーを作成する"

"S3 オブジェクトロックと従来の準拠の比較"

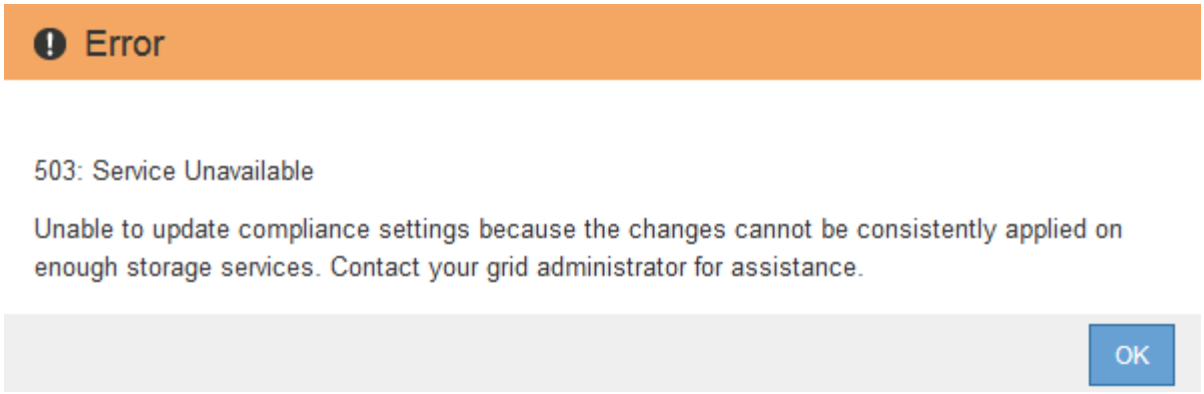
S3オブジェクトロックまたは従来の準拠設定の更新時に発生した整合性エラーを解決する

データセンターサイトまたはサイトの複数のストレージノードが使用できなくなった場合は、 S3 テナントユーザが S3 オブジェクトロックまたは従来の準拠設定に変更を適用できるよう支援する必要があります。

S3 オブジェクトロック（または従来の準拠）が有効になっているバケットを使用するテナントユーザは、特定の設定を変更できます。たとえば、 S3 オブジェクトロックを使用するテナントユーザがオブジェクトのバージョンをリーガルホールドの対象にする必要がある場合があります。

テナントユーザが S3 バケットまたはオブジェクトバージョンの設定を更新すると、 StorageGRID はグリッド全体ですぐにバケットまたはオブジェクトメタデータを更新します。データセンターサイトまたは複数のストレージノードが使用できないためにメタデータを更新できない場合は、エラーメッセージが表示されます。具体的には、

- Tenant Manager ユーザには次のエラーメッセージが表示されます。



- テナント管理APIユーザとS3 APIユーザは、の応答コードを受け取ります `503 Service Unavailable` 同様のメッセージテキストを含む。

このエラーを解決するには、次の手順を実行します。

1. できるだけ早く、すべてのストレージノードまたはサイトを利用できる状態に戻します。
2. 各サイトで十分な数のストレージノードを利用可能にできない場合は、テクニカルサポートに問い合わせて、ノードをリカバリし、変更がグリッド全体に一貫して適用されるようにしてください。
3. 基盤となる問題 が解決されたら、テナントユーザに設定の変更を再試行するよう通知してください。

関連情報

"テナントアカウントを使用する"

"S3 を使用する"

""

ILM ルールとポリシーの例

このセクションの例は、独自のILMルールとポリシーのベースとして使用できます。

- "例 1 ：オブジェクトストレージの ILM ルールとポリシー"
- "例 2 ： EC オブジェクトサイズのフィルタリング用の ILM ルールとポリシー"
- "例 3 ：画像ファイルの保護を強化する ILM ルールとポリシー"
- "例 4 ： S3 バージョン管理オブジェクトの ILM ルールとポリシー"
- "例 5 ：取り込み動作が Strict の場合の ILM ルールとポリシー"
- "例 6 ： ILM ポリシーを変更する"
- "例 7 ： S3 オブジェクトロックの準拠 ILM ポリシー"

例 1 ：オブジェクトストレージの ILM ルールとポリシー

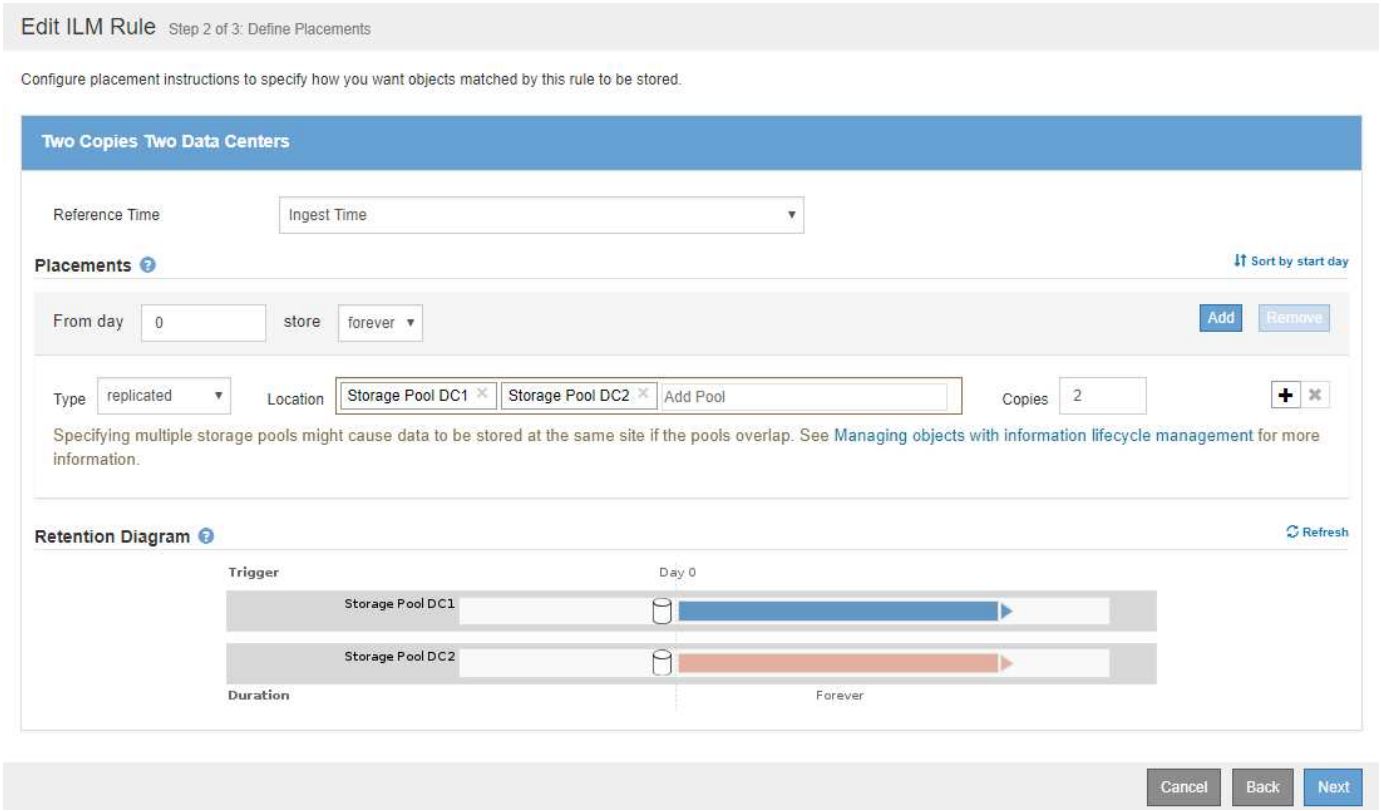
以下に記載するサンプルルールとポリシーをベースに、それぞれのオブジェクトの保護および保持要件を満たす ILM ポリシーを定義できます。

以下の ILM ルールとポリシーは一例にすぎません。ILM ルールを設定する方法は多数あります。新しいポリシーをアクティブ化する前に、ドラフトポリシーをシミュレートして、コンテンツの損失を防ぐためにドラフトポリシーが想定どおりに機能することを確認してください。

例 **1** の **ILM** ルール **1** ： **2** つのデータセンターへのオブジェクトデータのコピー

この ILM ルールの例では、 2 つのデータセンター内のストレージプールにオブジェクトデータをコピーします。

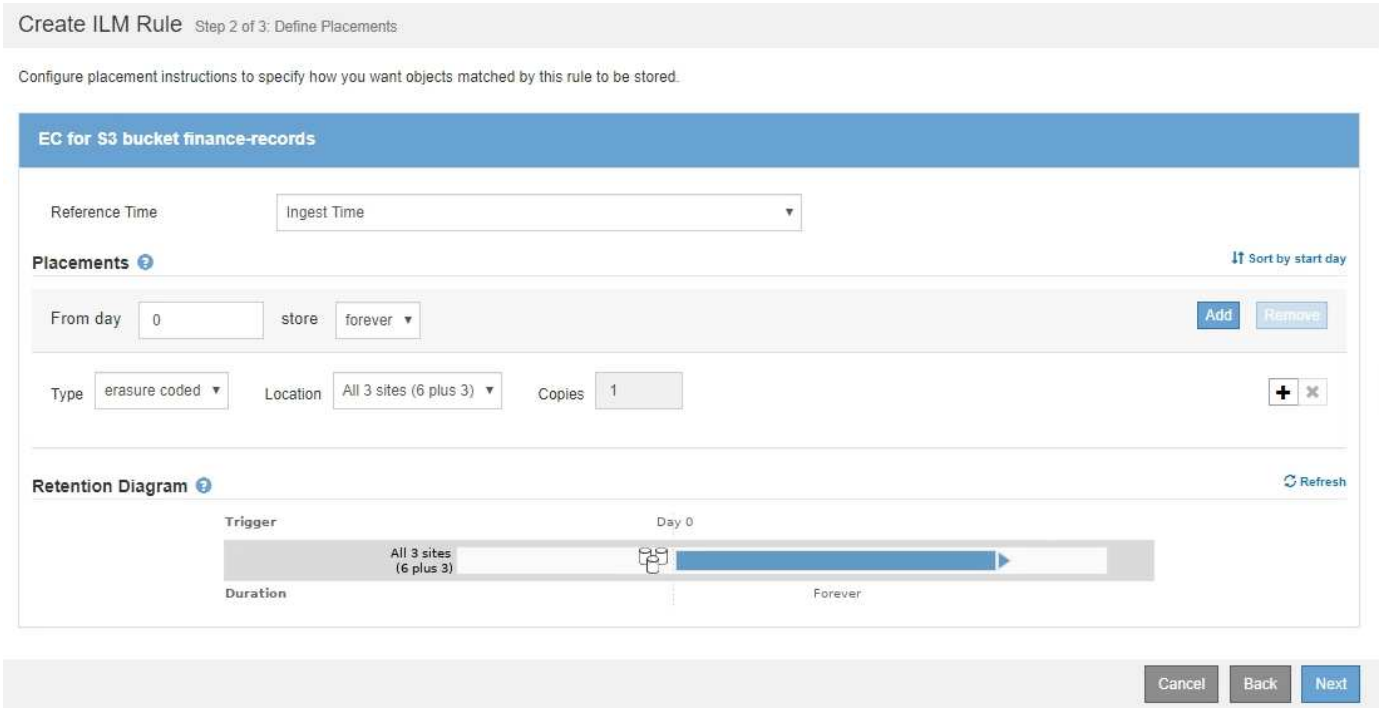
ルール定義	値の例
ストレージプール	別々のデータセンターに 2 つのストレージプール、 Storage Pool DC1 および Storage Pool DC2
ルール名	2 つのコピーで 2 つのデータセンターを構成し
参照時間	取り込み時間
コンテンツ配置	0 日目にレプリケートされたコピーを 2 つ無期限に保存 — Storage Pool DC1 に 1 つ、 Storage Pool DC2 に 1 つ。



例 **1** の **ILM** ルール **2** ：イレイジャーコーディングプロファイルとバケットの照合

この ILM ルールの例では、イレイジャーコーディングプロファイルと S3 バケットを使用して、オブジェクトの格納先と格納期間を決定します。

ルール定義	値の例
イレイジャーコーディングプロファイル	• 3 つのデータセンター（ 3 つすべてのサイト）にまたがる 1 つのストレージプール • 6+3 イレイジャーコーディングスキームを使用
ルール名	S3 バケット finance-records の EC
参照時間	取り込み時間
コンテンツ配置	finance-records という名前の S3 バケット内のオブジェクトに対し、イレイジャーコーディングコピーをイレイジャーコーディングプロファイルで指定されたプールに 1 つ作成します。このコピーを無期限に保持します。

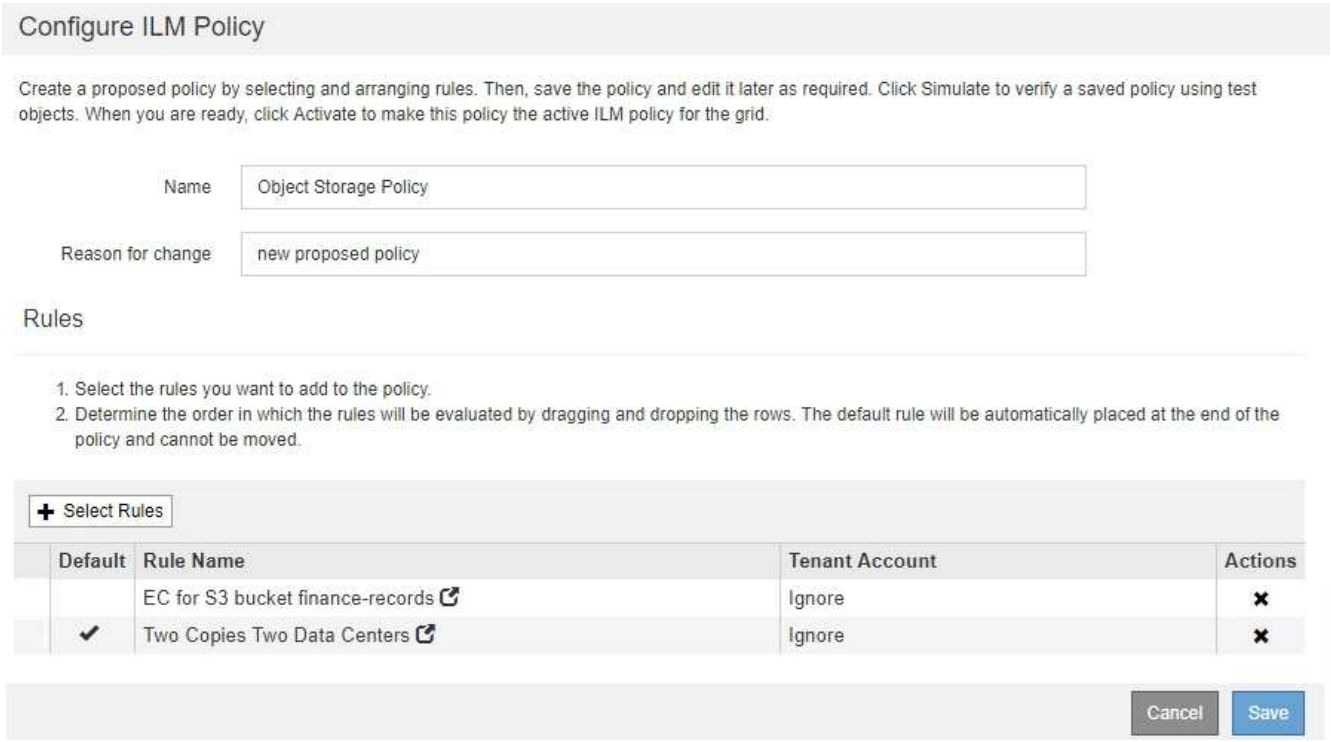


例 **1** の **ILM** ポリシー

StorageGRID システムでは、高度で複雑な ILM ポリシーを設計できますが、実際には、ほとんどの ILM ポリシーはシンプルです。

マルチサイトトポロジの一般的な ILM ポリシーには、次のような ILM ルールが含まれています。

- 取り込み時に、6+3イレイジャーコーディングを使用して、という名前のS3バケットに属するすべてのオブジェクトを格納します `finance-records` 3箇所のデータセンターに分散
- オブジェクトが最初の ILM ルールに一致しない場合は、ポリシーのデフォルトの ILM ルールである 2 つのデータセンターを使用して、 DC1 と DC2 の 2 つのデータセンターにそのオブジェクトのコピーを格納します。



例 **2** ： **EC** オブジェクトサイズのフィルタリング用の **ILM** ルールとポリシー

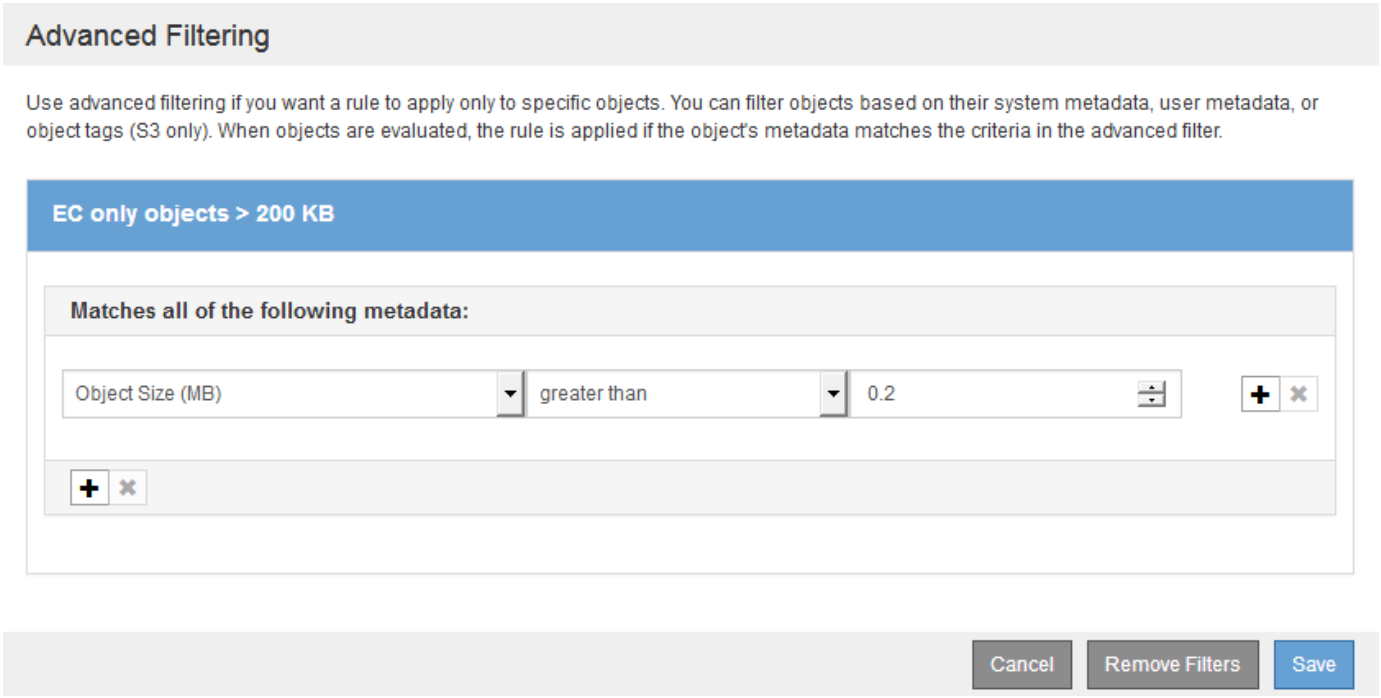
以下に記載するサンプルルールとポリシーをベースに、オブジェクトサイズでフィルタリングして EC の推奨要件を満たす ILM ポリシーを定義できます。

以下の ILM ルールとポリシーは一例にすぎません。ILM ルールを設定する方法は多数あります。新しいポリシーをアクティブ化する前に、ドラフトポリシーをシミュレートして、コンテンツの損失を防ぐためにドラフトポリシーが想定どおりに機能することを確認してください。

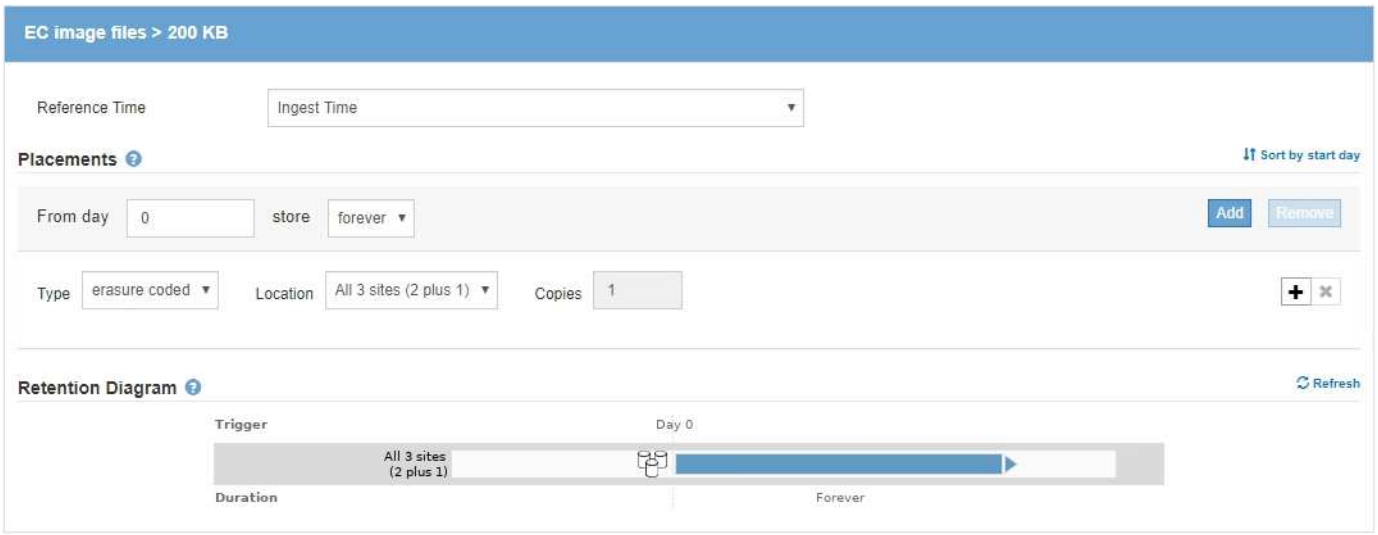
例**2**の**ILM**ルール**1**：**200KB**を超えるすべてのオブジェクトにイレイジャーコーディングを使用します

このILMルールの例では、200KB（0.20MB）を超えるすべてのオブジェクトをイレイジャーコーディングします。

ルール定義	値の例
ルール名	ECのみのオブジェクト>200KB
参照時間	取り込み時間
オブジェクトサイズの高度なフィルタリング	オブジェクトサイズ（MB）が0.20より大きい
コンテンツ配置	3 つのサイトを使用して 2+1 のイレイジャーコーディングコピーを作成



配置手順は、3つのサイトすべてを使用して2+1のイレイジャーコーディングコピーを作成するように指定します。

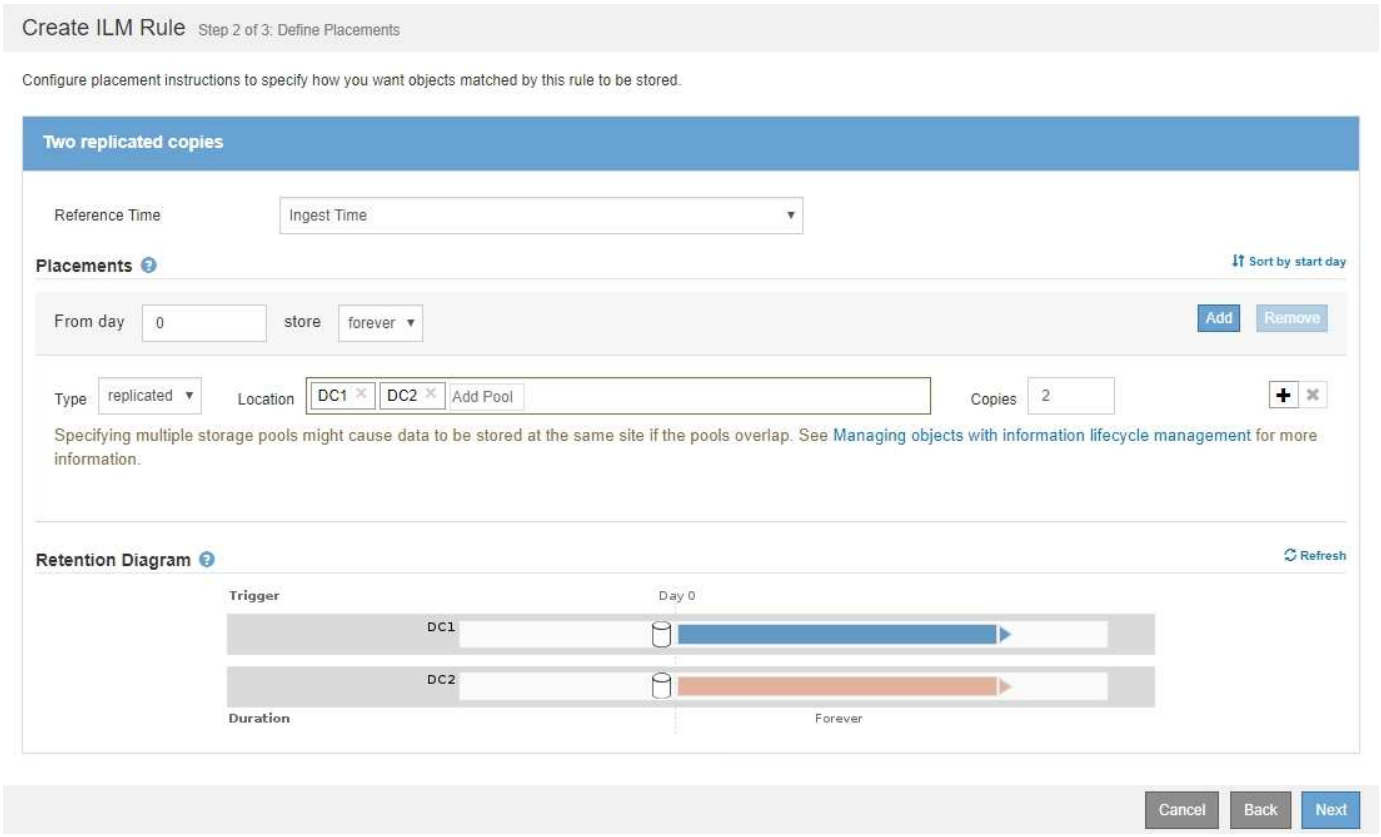


例 **2** の **ILM** ルール **2** ：レプリケートされたコピーを **2** つ

この ILM ルールの例では、レプリケートコピーを 2 つ作成し、オブジェクトサイズではフィルタリングしません。このルールはポリシー内の2番目のルールです。例2のILMルール1が200KBを超えるすべてのオブジェクトを除外するため、例2のILMルール2は200KB以下の環境 オブジェクトのみを除外します。

ルール定義	値の例
ルール名	2 つのレプリケートコピー
参照時間	取り込み時間

ルール定義	値の例
オブジェクトサイズの高度なフィルタリング	なし
コンテンツ配置	レプリケートコピーを 2 つ作成して、 DC1 と DC2 の 2 つのデータセンターに保存します

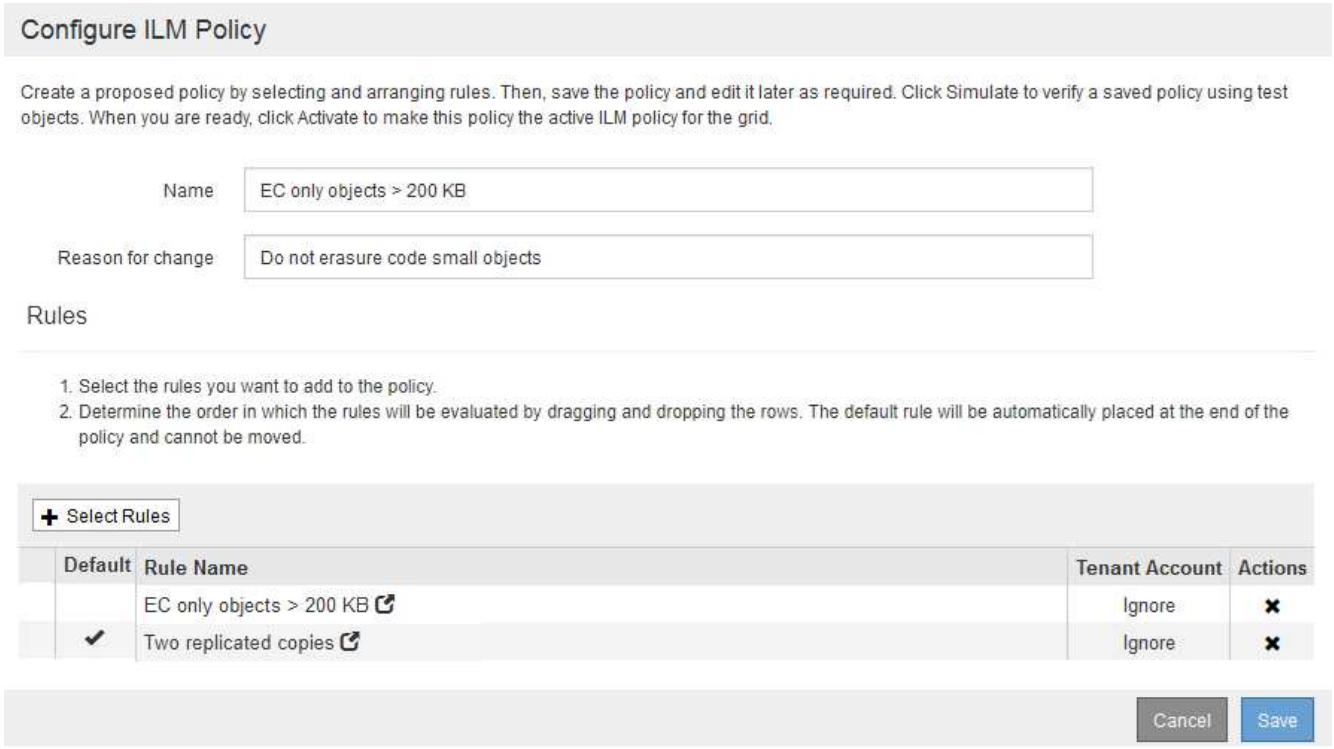


例2のILMポリシー：200KBを超えるオブジェクトにイレイジャーコーディングを使用

このポリシーの例では、200KBを超えるオブジェクトがイレイジャーコーディングされます。他のすべてのオブジェクトから2つのレプリケートコピーが作成されます。

この例のILMポリシーには、次のILMルールが含まれています。

- 200KBを超えるすべてのオブジェクトをイレイジャーコーディングします。
- オブジェクトが最初のILMルールに一致しない場合は、デフォルトのILMルールを使用して、そのオブジェクトのレプリケートコピーを2つ作成します。200KBを超えるオブジェクトはルール1で除外されているため、ルール2では200KB以下の環境 オブジェクトのみが除外されます。



例 **3** ：画像ファイルの保護を強化する **ILM** ルールとポリシー

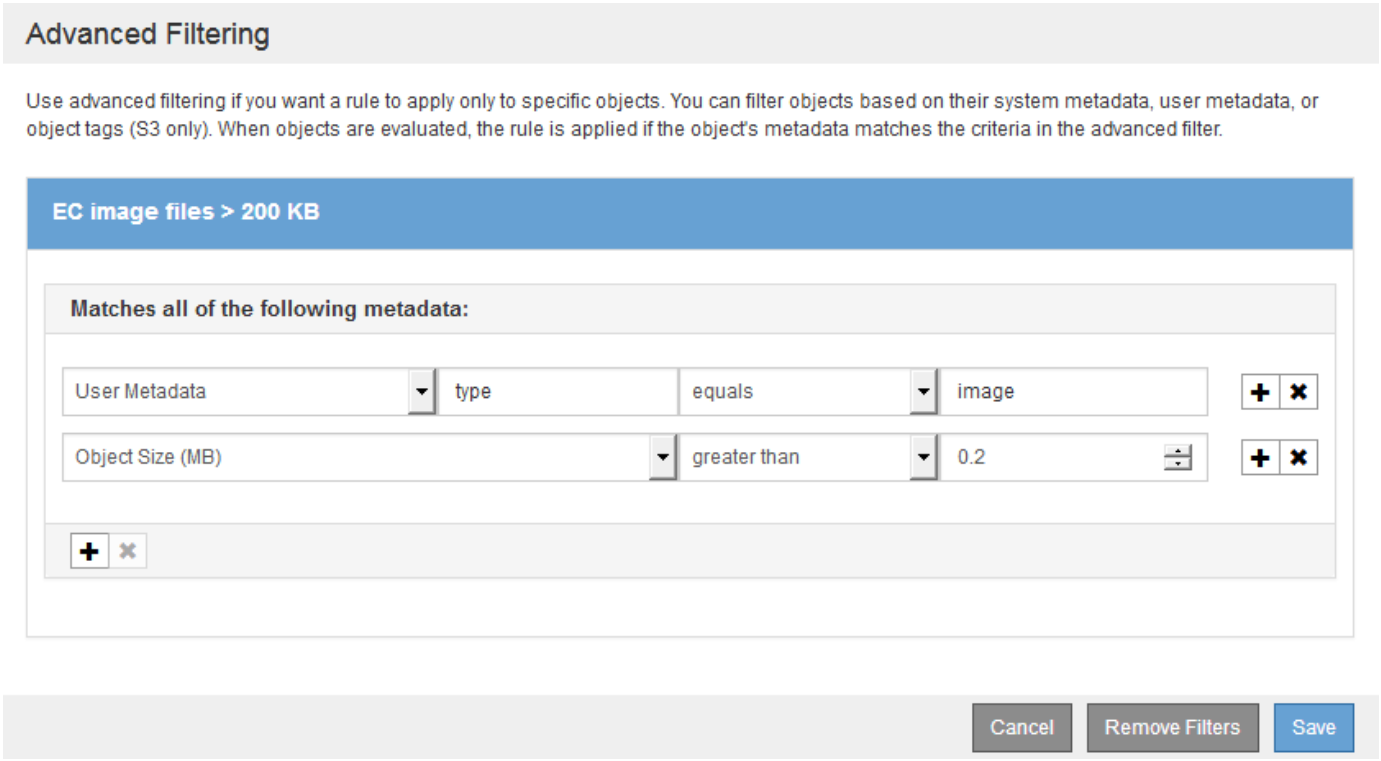
以下に記載するサンプルルールとポリシーを使用して、200KBを超える画像をイレイジャーコーディングし、200KB以下の画像からコピーを3つ作成できます。

以下の ILM ルールとポリシーは一例にすぎません。ILM ルールを設定する方法は多数あります。新しいポリシーをアクティブ化する前に、ドラフトポリシーをシミュレートして、コンテンツの損失を防ぐためにドラフトポリシーが想定どおりに機能することを確認してください。

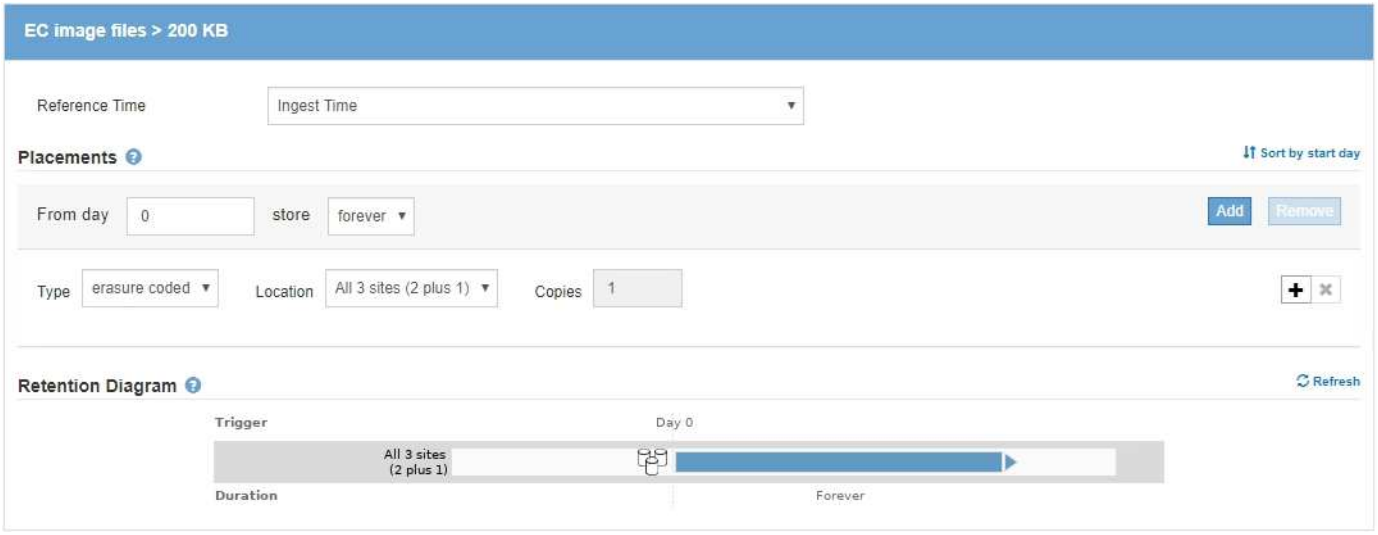
例**3**の**ILM**ルール**1**：**200KB**を超える画像ファイルにイレイジャーコーディングを使用

このILMルールの例では、高度なフィルタリングを使用して、200KBを超えるすべての画像ファイルをイレイジャーコーディングします。

ルール定義	値の例
ルール名	ECイメージファイル>200KB
参照時間	取り込み時間
ユーザメタデータの高度なフィルタリング	ユーザメタデータタイプはイメージファイルと同じです
オブジェクトサイズの高度なフィルタリング	オブジェクトサイズ（MB）が0.2より大きい
コンテンツ配置	3 つのサイトを使用して 2+1 のイレイジャーコーディングコピーを作成



このルールはポリシー内の最初のルールとして設定されているため、イレイジャーコーディングの配置手順では200KBを超える環境 イメージのみが使用されます。

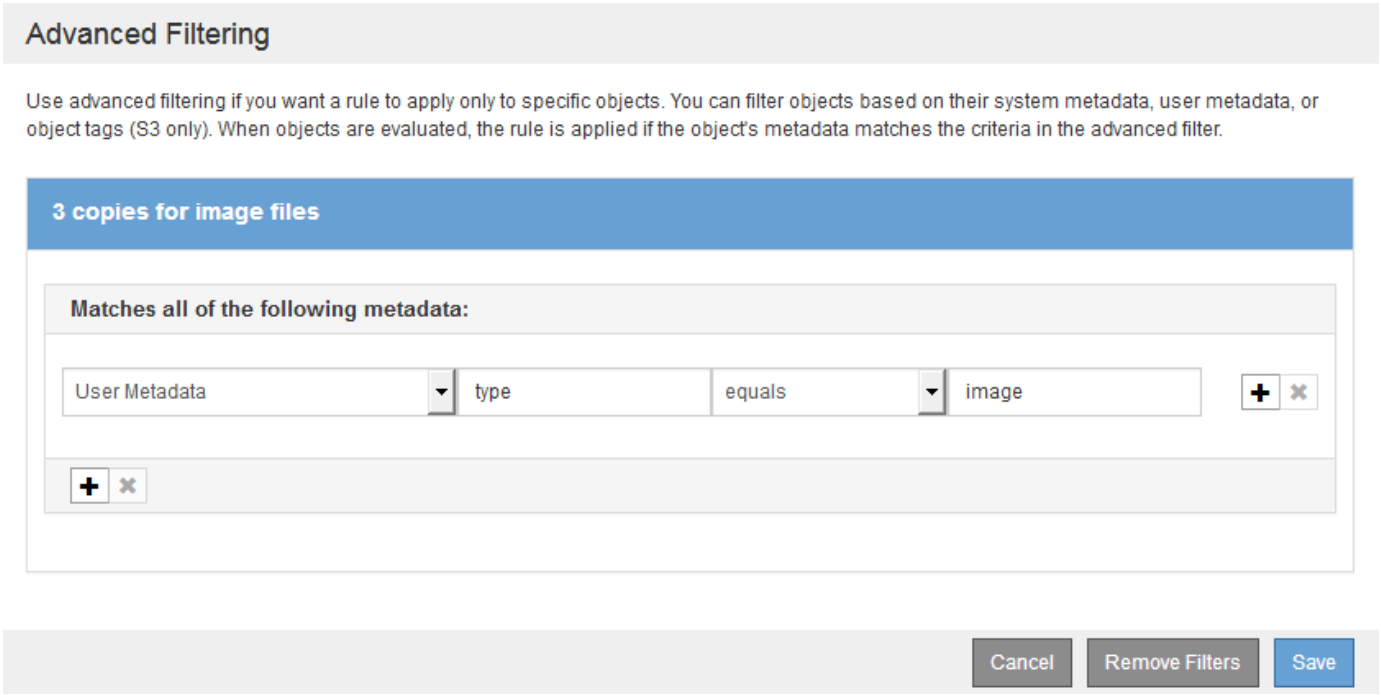


例**3**の**ILM**ルール**2**：残りのすべてのイメージファイルのコピーを**3**つレプリケートします

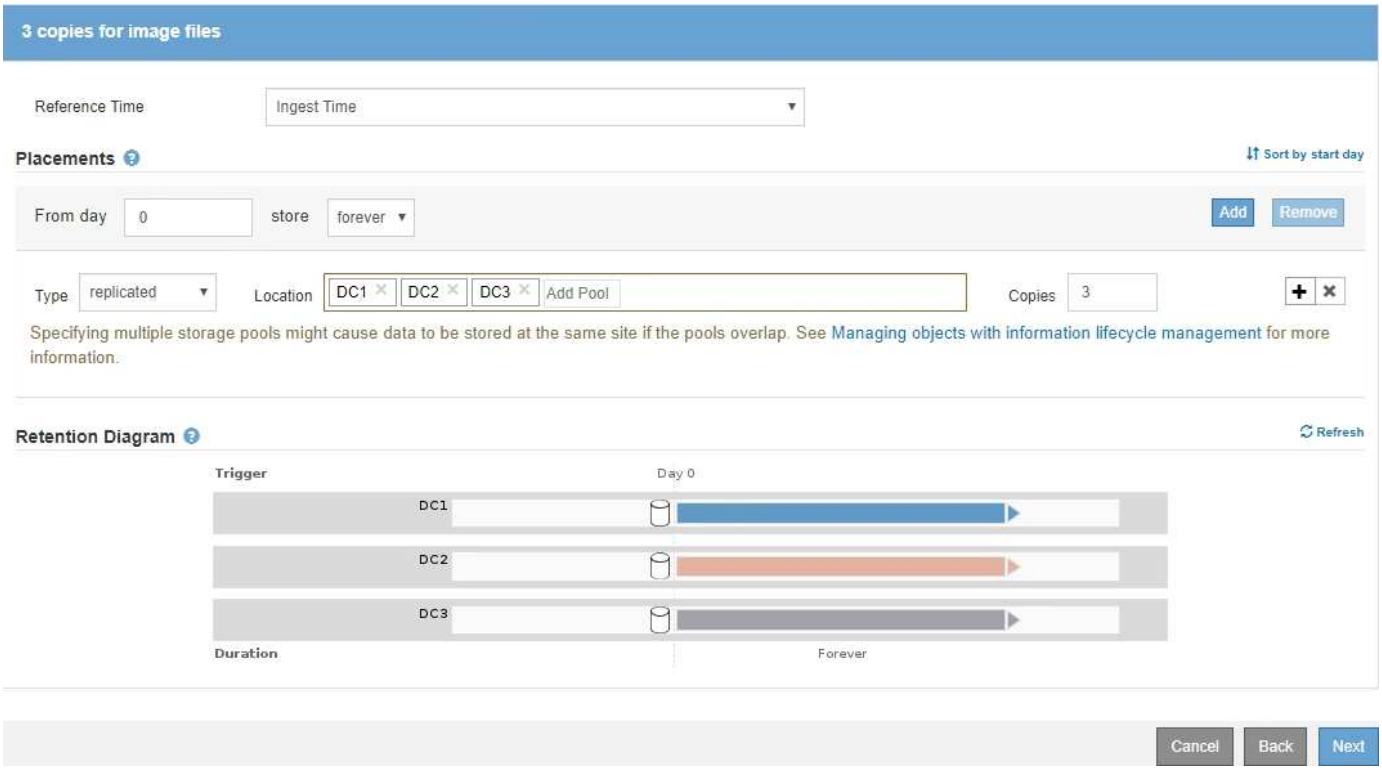
このILMルールの例では、高度なフィルタリングを使用して、イメージファイルをレプリケートするように指定します。

ルール定義	値の例
ルール名	画像ファイル用に3つのコピー
参照時間	取り込み時間

ルール定義	値の例
ユーザメタデータの高度なフィルタリング	ユーザメタデータタイプはイメージファイルと同じです
コンテンツ配置	レプリケートされたコピーをすべてのストレージノードに3つ作成します



ポリシー内の最初のルールは200KBを超える画像ファイルにすでに一致しているため、この配置手順は200KB以下の画像ファイルにのみ適用されます。

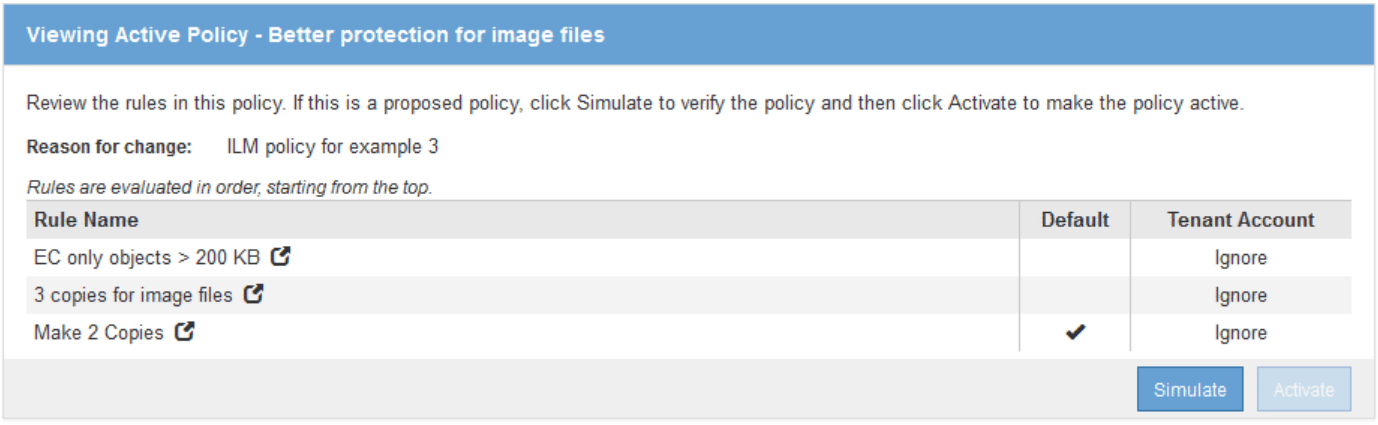


例 **3** の **ILM** ポリシー：画像ファイルの保護の強化

この例では、ILMポリシーで3つのILMルールを使用して、200KB（0.2MB）を超える画像ファイルをイレイジャーコーディングし、200KB以下の画像ファイルのレプリケートコピーを作成し、画像以外のファイルについては2つのレプリケートコピーを作成するポリシーを作成します。

この例のILMポリシーには、次の処理を実行するルールが含まれています。

- 200KBを超えるすべての画像ファイルをイレイジャーコーディングします。
- 残りの（200KB以下の）画像ファイルのコピーを3つ作成します。
- 残りのすべてのオブジェクト（つまり、すべての非イメージファイル）にデフォルトルールを適用します。



例 **4** ： **S3** バージョン管理オブジェクトの **ILM** ルールとポリシー

バージョン管理が有効になっている S3 バケットがある場合は、参照時間として *

noncurrent time * を使用する ILM ポリシーにルールを含めることで、最新でないオブジェクトバージョンを管理できます。

この例に示すように、バージョン管理オブジェクトで使用されるストレージの量を制御するには、最新でないオブジェクトバージョンに別々の配置手順を使用します。

以下の ILM ルールとポリシーは一例にすぎません。ILM ルールを設定する方法は多数あります。新しいポリシーをアクティブ化する前に、ドラフトポリシーをシミュレートして、コンテンツの損失を防ぐためにドラフトポリシーが想定どおりに機能することを確認してください。

最新でないオブジェクトバージョンを管理するための ILM ポリシーを作成する場合は、ポリシーをシミュレートするためにオブジェクトバージョンの UUID または CBID が必要です。オブジェクトの UUID と CBID を確認するには、オブジェクトが最新の間にオブジェクトメタデータを検索します。

関連情報

"S3 バージョン管理オブジェクトの削除方法"

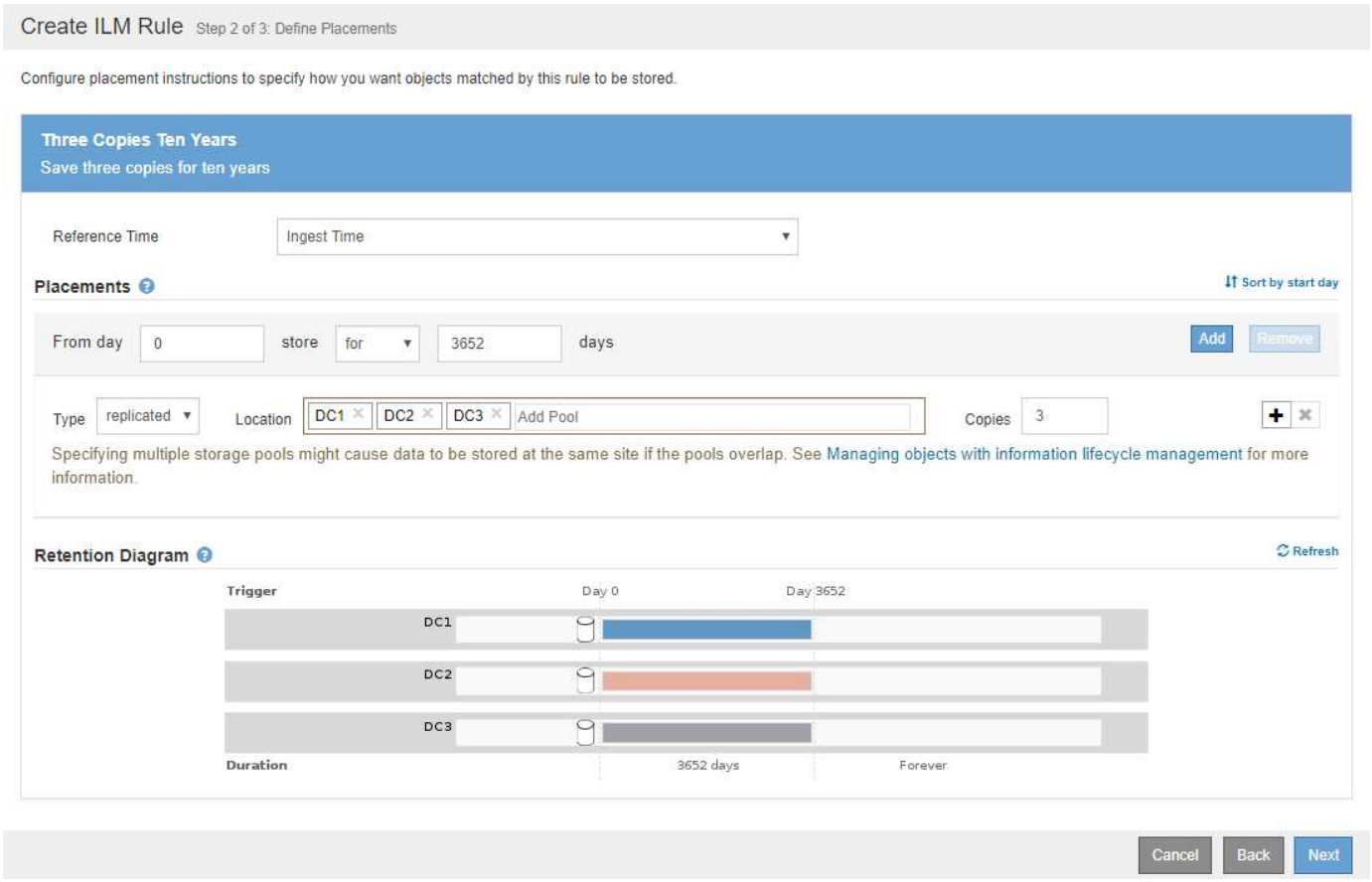
"オブジェクトメタデータの検索によるILMポリシーの検証"

例 4 の ILM ルール 1 ：コピーを 3 つ、 10 年間保存します

この例では、 3 つのデータセンターに各オブジェクトのコピーを 10 年間格納します。

このルールは、オブジェクトがバージョン管理されているかどうかに関係なく、すべてのオブジェクトを環境します。

ルール定義	値の例
ストレージプール	別々のデータセンターにある 3 つのストレージプール、 DC1 、 DC2 、 DC3 。
ルール名	3 つのコピー 10 年
参照時間	取り込み時間
コンテンツ配置	0 日目から、 3 つのレプリケートコピーを 10 年間（ 3 、 652 日）格納（ DC1 、 DC2 、 DC3 に 1 つずつ）。10 年後にオブジェクトのコピーをすべて削除する。



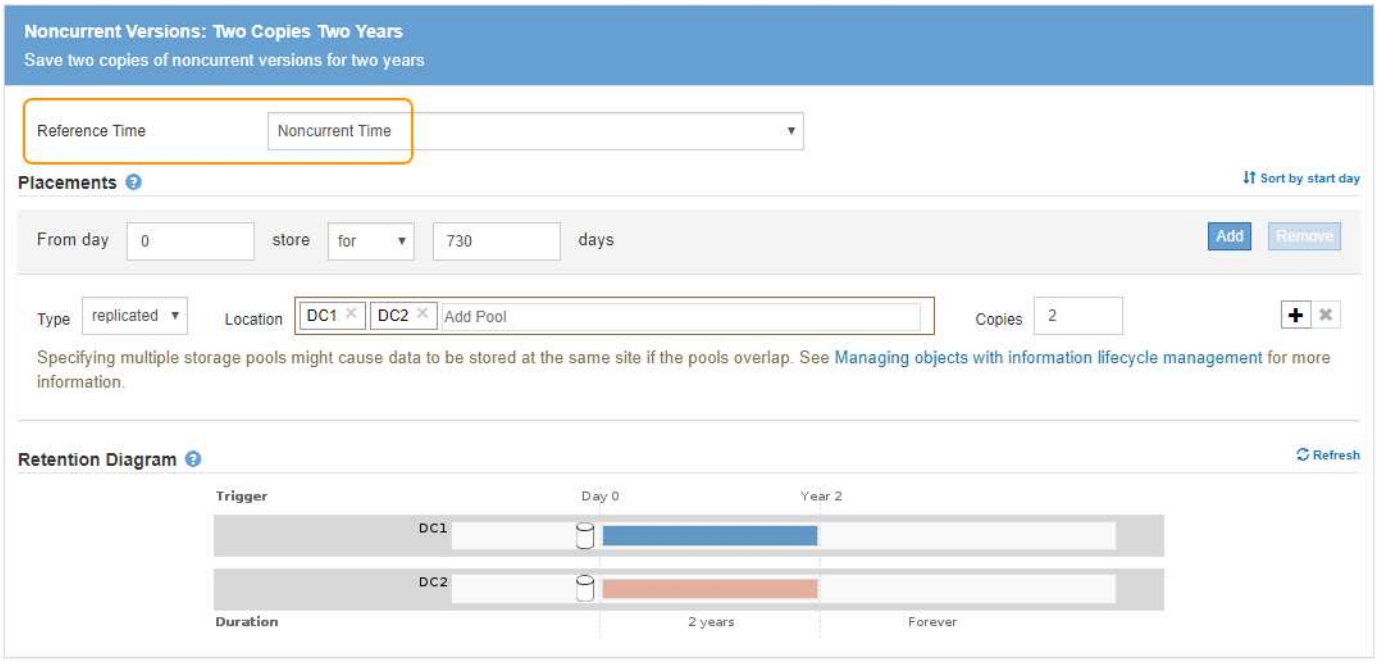
例 **4** の **ILM** ルール **2** ：最新でないバージョンのコピーを **2** つ、 **2** 年間保存します

この例では、最新でないバージョンの S3 バージョン管理オブジェクトのコピーを 2 つ、 2 年間格納します。

ILM ルール 1 ではすべてのバージョンのオブジェクトが環境 されるため、最新でないバージョンをすべて除外する別のルールを作成する必要があります。このルールでは、参照時間に * noncurrent Time * オプションを使用します。

この例では、最新でないバージョンのコピーが 2 つだけ格納され、その期間は 2 年間です。

ルール定義	値の例
ストレージプール	別々のデータセンターにある 2 つのストレージプール、 DC1 および DC2
ルール名	最新でないバージョン： 2 コピー 2 年
参照時間	最新でなくなった時間
コンテンツ配置	0 日目から最新でない時間（オブジェクトバージョンが最新でないバージョンになる日から）を基準に、最新でないオブジェクトバージョンのレプリケートコピーを 2 つ（ 730 日）保持し、 DC1 と DC2 に 1 つずつ保持します。2 年後に最新でないバージョンを削除します。



例 **4** の **ILM** ポリシー： **S3** バージョン管理オブジェクト

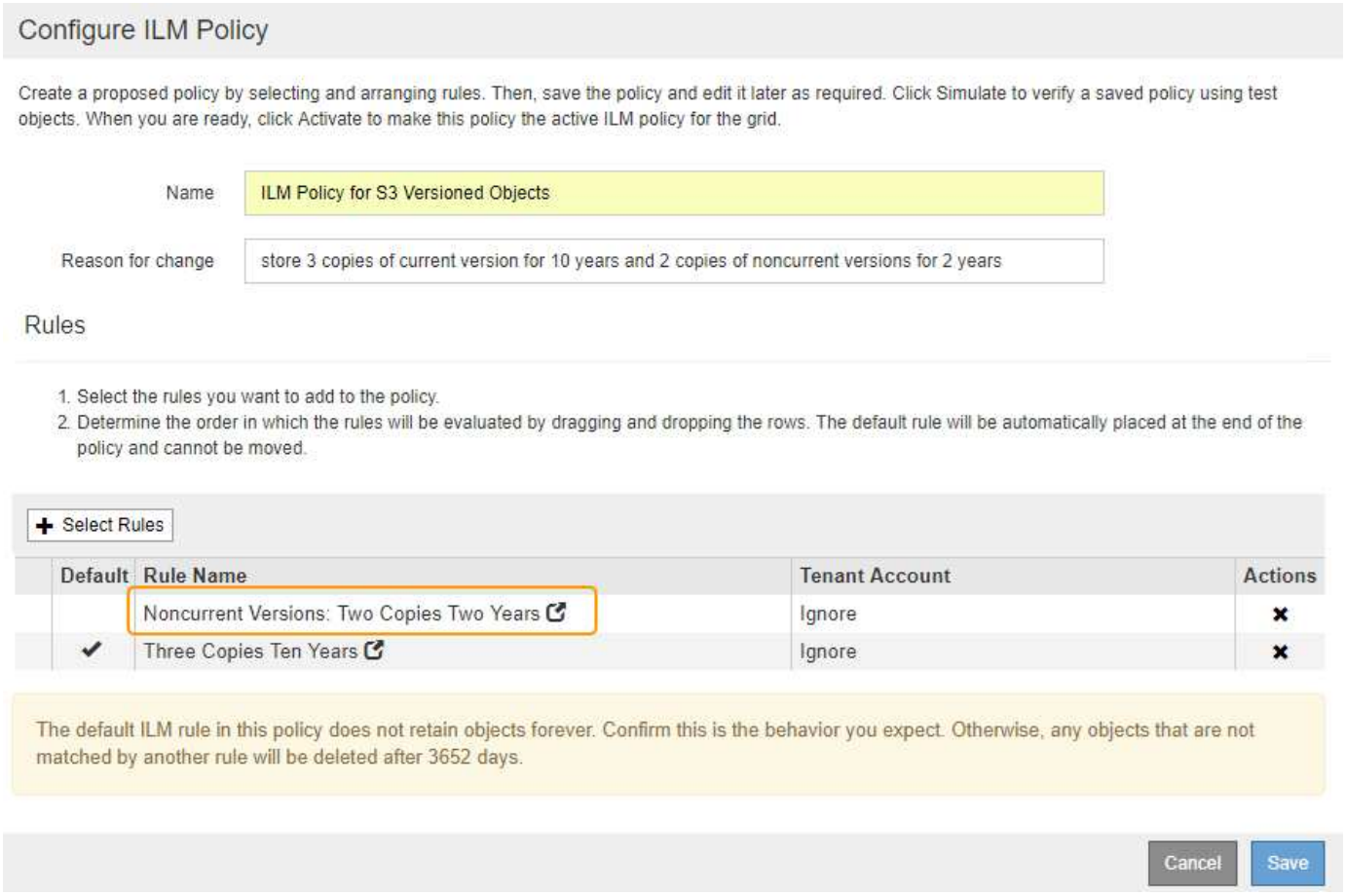
最新バージョンとは異なる古いバージョンのオブジェクトを管理する場合は、現在のオブジェクトバージョンに適用されるルールを開始する前に、参照時間として * noncurrent Time * を使用するルールを ILM ポリシーに含める必要があります。

S3 バージョン管理オブジェクトの ILM ポリシーには、次のような ILM ルールが含まれます。

- 古い（最新でない）バージョンの各オブジェクトを、そのバージョンが最新でなくなった日から 2 年間保持します。

> 最新でない時間ルールは、現在のオブジェクトバージョンに適用されるルールより前にポリシーに表示される必要があります。それ以外の場合、最新でないオブジェクトバージョンは noncurrent Time ルールに一致しません。

- 取り込み時に、レプリケートコピーを 3 つ作成して、 3 つのデータセンターに 1 つずつ格納します。最新のオブジェクトバージョンのコピーを 10 年間保持します。



この例のポリシーをシミュレートすると、テストオブジェクトは次のように評価されます。

- 最新でないオブジェクトバージョンがすべて最初のルールに一致します。最新でないオブジェクトバージョンが 2 年以上経過している場合は、 ILM によって完全に削除されます（最新でないバージョンのコピーがすべてグリッドから削除されます）。

> 最新でないオブジェクトバージョンをシミュレートするには、そのバージョンの UUID または CBID を使用する必要があります。オブジェクトが最新の間であれば、 Object Metadata Lookup を使用して UUID と CBID を検索できます。

- 現在のオブジェクトバージョンが 2 つ目のルールに一致します。最新のオブジェクトバージョンが 10 年間保存されると 'ILM プロセスはオブジェクトの最新バージョンとして削除マーカーを追加し ' 以前のオブジェクトバージョンを「 noncurrent 」にします 次回の ILM 評価では、この最新でないバージョンは最初のルールに一致します。その結果、 DC3 にあるコピーがパージされ、 DC1 と DC2 にある 2 つのコピーがさらに 2 年間格納されます。

関連情報

"オブジェクトメタデータの検索によるILMポリシーの検証"

例 **5** ：取り込み動作が **Strict** の場合の **ILM** ルールとポリシー

ルールで場所フィルタと Strict 取り込み動作を使用すると、特定のデータセンターの場所にオブジェクトが保存されないようにすることができます。

この例では、規制上の問題により、パリベースのテナントは EU の外部に一部のオブジェクトを格納しないよ

うにしています。他のテナントアカウントのすべてのオブジェクトを含むその他のオブジェクトは、パリデータセンターまたは米国のデータセンターに格納できます。

以下の ILM ルールとポリシーは一例にすぎません。ILM ルールを設定する方法は多数あります。新しいポリシーをアクティブ化する前に、ドラフトポリシーをシミュレートして、コンテンツの損失を防ぐためにドラフトポリシーが想定どおりに機能することを確認してください。

関連情報

"オブジェクトの取り込み方法"

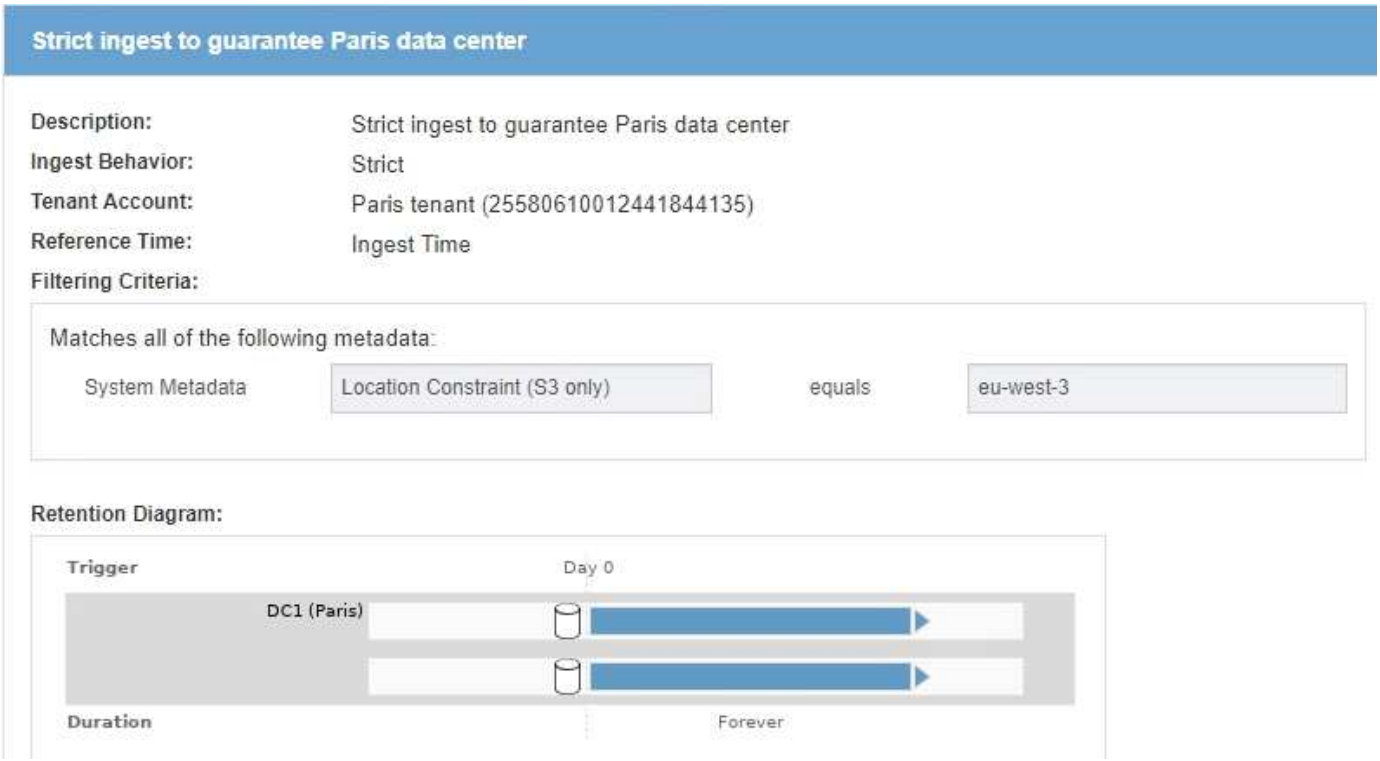
"ステップ 3 / 3 ：取り込み動作を定義する"

例 **5** の **ILM** ルール **1** ：パリデータセンターを確保するための **Strict** 取り込み

この ILM ルールの例では Strict 取り込み動作を使用して、パリベースのテナントによって S3 バケットに保存されたオブジェクトのリージョンが eu-west-3 リージョン（パリ）に設定されたものが米国のデータセンターに格納されないようにします。

このルールは、パリテナントに属し、 S3 バケットリージョンが eu-west-3 （パリ）に設定されている環境 オブジェクトを示します。

ルール定義	値の例
テナントアカウント	パリのテナント
高度なフィルタリング	場所制約は eu-west-3 に相当します
ストレージプール	DC1 （パリ）
ルール名	厳格な取り込みにより、パリのデータセンターを保証します
参照時間	取り込み時間
コンテンツ配置	0 日目から、 2 つのレプリケートコピーを DC1 （パリ）に保存
取り込み動作	strict 。取り込み時に必ずこのルールの配置手順を使用してください。パリデータセンターにオブジェクトのコピーを 2 つ保存できない場合、取り込みは失敗します。



例 **5** の **ILM** ルール **2** ：他のオブジェクトに対してバランスのとれた取り込み

この ILM ルールの例では、 Balanced 取り込み動作を使用して、最初のルールに一致しないオブジェクトの ILM 効率が最適化されます。このルールに一致するすべてのオブジェクトのコピーが 2 つ保存されます。 1 つは米国データセンターに、もう 1 つはパリデータセンターに格納されます。ルールをすぐに完了できない場合は、使用可能な任意の場所に中間コピーが格納されます。

このルールは、任意のテナントおよびすべてのリージョンに属する環境 オブジェクトを対象としています。

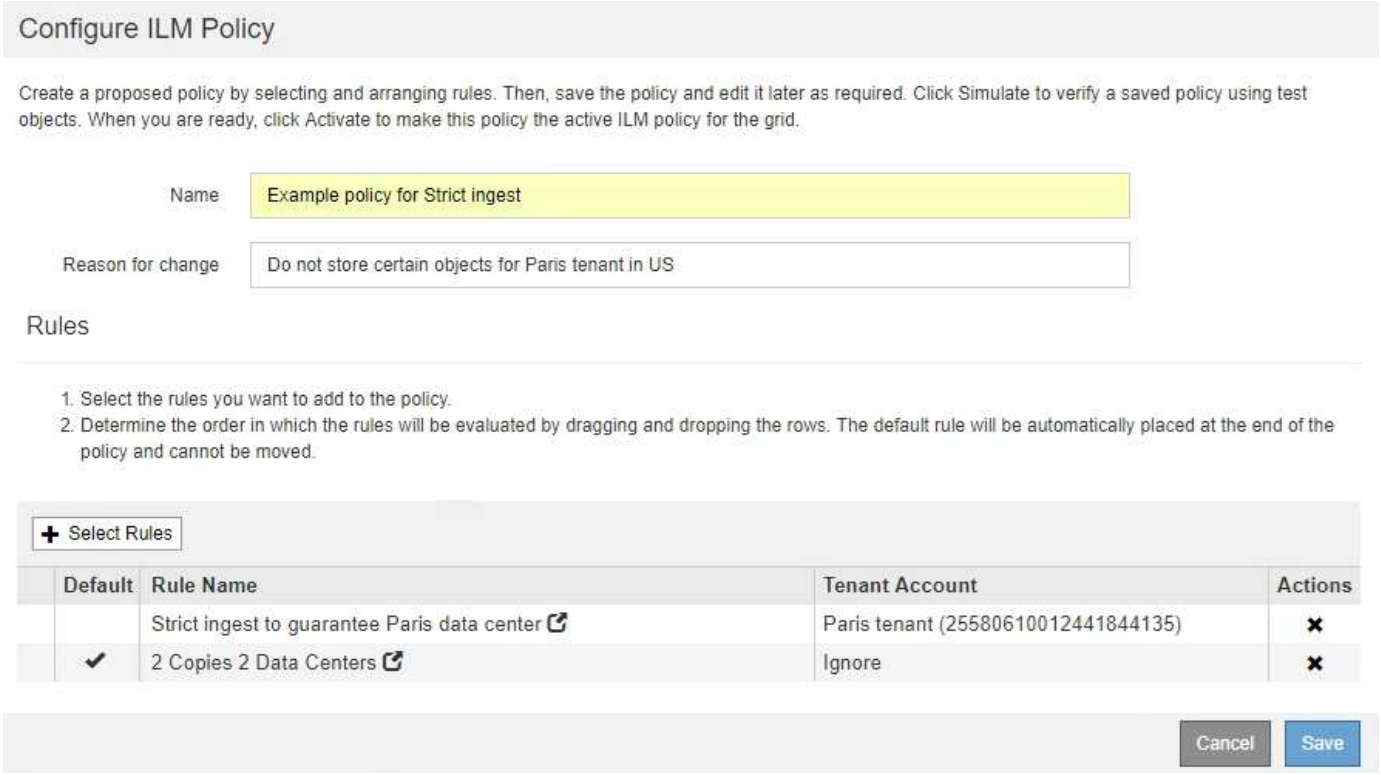
ルール定義	値の例
テナントアカウント	無視します
高度なフィルタリング	_ 指定されていません _
ストレージプール	DC1 （パリ）および DC2 （米国）
ルール名	2 つのコピーで 2 つのデータセンター
参照時間	取り込み時間
コンテンツ配置	0 日目から、 2 つのレプリケートコピーを 2 つのデータセンターに無期限に格納します
取り込み動作	中間（ Balanced ）：このルールに一致するオブジェクトは、可能であればルールの配置手順に従って配置されます。それ以外の場合、中間コピーは任意の空き場所で作成されます。

例 **5** の **ILM** ポリシー：取り込み動作を組み合わせたもの

この例の ILM ポリシーには、取り込み動作が異なる 2 つのルールが含まれています。

2 つの異なる取り込み動作を使用する ILM ポリシーには、次のような ILM ルールが含まれる場合があります。

- パリのテナントに属し、かつ S3 バケットリージョンがパリのデータセンター内でのみ eu-west-3 （パリ）に設定されているオブジェクトを格納します。パリのデータセンターが利用できない場合は取り込みに失敗します。
- その他のすべてのオブジェクト（パリテナントに属しているものの、バケットリージョンが異なるオブジェクトを含む）は、米国のデータセンターとパリのデータセンターの両方に保存します。配置手順を満たすことができない場合は、使用可能な任意の場所に中間コピーを作成します。



この例のポリシーをシミュレートすると、テストオブジェクトは次のように評価されます。

- パリのテナントに属し、 S3 バケットリージョンが eu-west-3 に設定されているオブジェクトはすべて最初のルールに一致し、パリのデータセンターに格納されます。最初のルールでは Strict 取り込みが使用されるため、これらのオブジェクトが米国のデータセンターに格納されることはありません。パリデータセンターのストレージノードを使用できない場合、取り込みは失敗します。
- 他のすべてのオブジェクトは、パリテナントに属するオブジェクトや S3 バケットリージョンが eu-west-3 に設定されていないオブジェクトを含む 2 番目のルールに一致します。各オブジェクトのコピーが各データセンターに 1 つずつ保存されます。ただし、 2 つ目のルールでは Balanced ing(バランスの取れた取り込み) が使用されるため、 1 つのデータセンターが使用できない場合は、使用可能な任意の場所に 2 つの中間コピーが保存されます。

例 **6** ： **ILM** ポリシーを変更する

データ保護のニーズが変わった場合や新しいサイトを追加した場合は、新しい ILM ポリシーの作成とアクティブ化が必要になることがあります。

ポリシーを変更する前に、 ILM の配置変更が一時的に StorageGRID システムの全体的なパフォーマンスに及ぼす影響について理解しておく必要があります。

この例では、拡張時に新しい StorageGRID サイトが追加され、新しいサイトにデータを格納するためにアクティブな ILM ポリシーを変更する必要があります。

以下の ILM ルールとポリシーは一例にすぎません。ILM ルールを設定する方法は多数あります。新しいポリシーをアクティブ化する前に、ドラフトポリシーをシミュレートして、コンテンツの損失を防ぐためにドラフトポリシーが想定どおりに機能することを確認してください。

ILM ポリシーの変更がパフォーマンスに与える影響

新しい ILM ポリシーをアクティブ化すると、特に新しいポリシーの配置手順で多数の既存オブジェクトの新しい場所への移動が必要になった場合には、 StorageGRID システムのパフォーマンスに一時的に影響する可能性があります。

> 新しい ILM ポリシーをアクティブ化すると、 StorageGRID は、そのポリシーを使用して、既存のオブジェクトと新たに取り込まれたオブジェクトを含むすべてのオブジェクトを管理します。新しい ILM ポリシーをアクティブ化する前に、既存のレプリケートオブジェクトとイレイジャーコーディングオブジェクトの配置に対する変更を確認してください。既存のオブジェクトの場所を変更すると、新しい配置が評価されて実装される際に一時的なリソースの問題が発生する可能性があります。

StorageGRID のパフォーマンスに一時的に影響する可能性がある ILM ポリシーの変更には、次のようなものがあります。

- 既存のイレイジャーコーディングオブジェクトへの別のイレイジャーコーディングプロファイルの適用

> StorageGRID では、各イレイジャーコーディングプロファイルは一意とみなされ、新しいプロファイルを使用する場合はイレイジャーコーディングフラグメントが再利用されません。

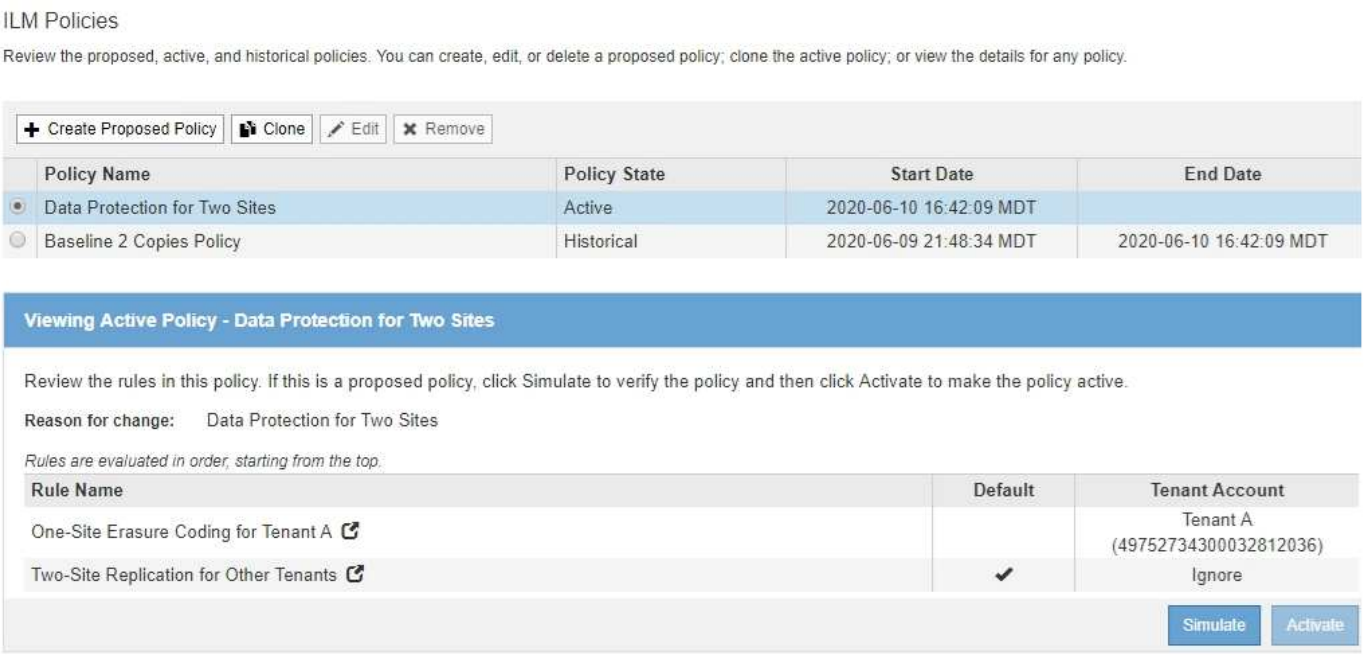
- 既存のオブジェクトに必要なコピーのタイプを変更する。たとえば、大部分のレプリケートオブジェクトをイレイジャーコーディングオブジェクトに変換する場合などです。
- 既存のオブジェクトのコピーをまったく別の場所に移動する。たとえば、クラウドストレージプールとリモートサイトの間で多数のオブジェクトを移動する場合などです。

関連情報

"ILMポリシーを作成する"

例 6 のアクティブな ILM ポリシー： 2 つのサイトでのデータ保護

この例では、アクティブな ILM ポリシーは最初に 2 サイトの StorageGRID システム用に設計され、 2 つの ILM ルールを使用しています。



この ILM ポリシーでは、テナント A に属するオブジェクトが 1 つのサイトで 2+1 のイレイジャーコーディングによって保護され、一方他のすべてのテナントに属するオブジェクトは 2-copy レプリケーションを使用して 2 つのサイト間で保護されます。

> この例の最初のルールでは、高度なフィルタを使用して、イレイジャーコーディングが小さいオブジェクトには使用されないようにしています。200KB未満のテナントAのオブジェクトは、レプリケーションを使用する2つ目のルールによって保護されます。

ルール **1** ：テナント **A** に **1** つのサイトのイレイジャーコーディング

ルール定義	値の例
ルール名	テナント A の 1 サイトのイレイジャーコーディング
テナントアカウント	テナント A
ストレージプール	データセンター 1
コンテンツ配置	データセンター 1 の 2+1 イレイジャーコーディングを 0 日目から無期限に実行

ルール **2** ：他のテナントに **2** つのサイトをレプリケートする

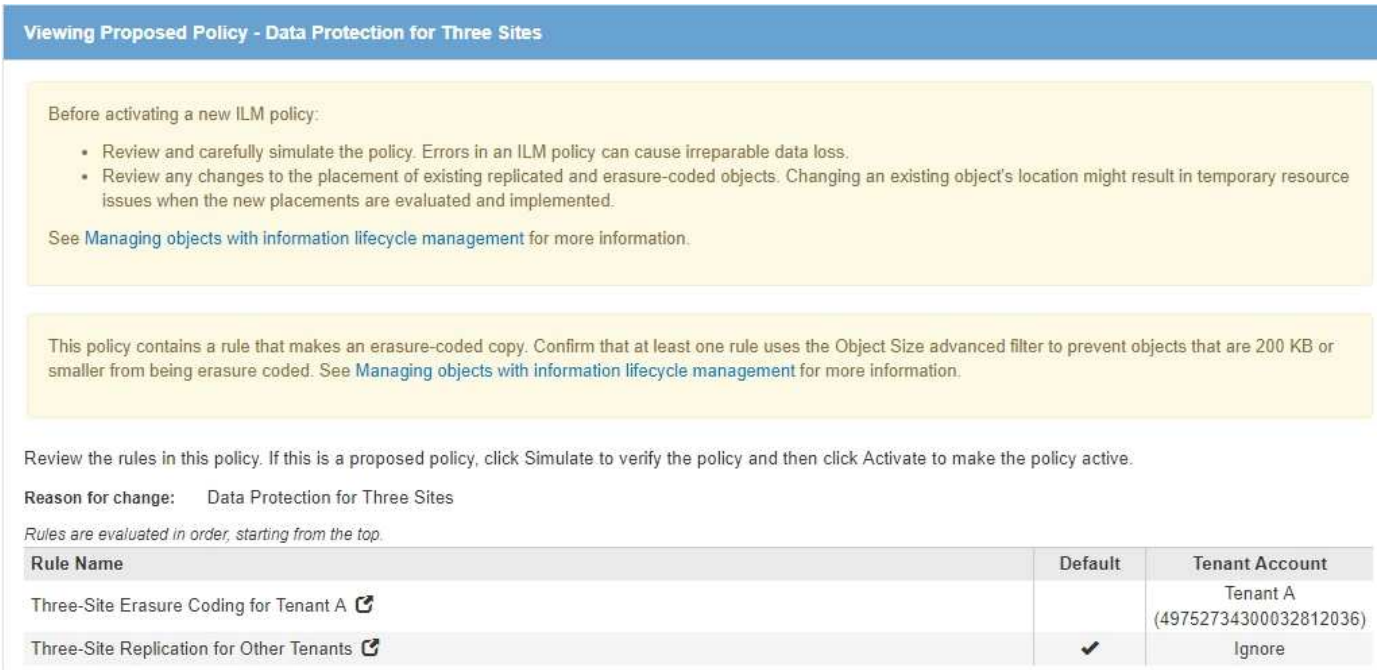
ルール定義	値の例
ルール名	他のテナント用の 2 サイトレプリケーション
テナントアカウント	無視します

ルール定義	値の例
ストレージプール	データセンター 1 とデータセンター 2
コンテンツ配置	0 日目から無期限にレプリケートされたコピー × 2 ：データセンター 1 に 1 つ、データセンター 2 に 1 つ。

例 **6** の **ILM** ポリシーとして、 **3** つのサイトのデータ保護が提案されています

この例では、 3 サイトの StorageGRID システムの ILM ポリシーを更新しています。

新しいサイトを追加するための拡張を行ったあと、グリッド管理者は 2 つの新しいストレージプールを作成しました。 1 つは Data Center 3 用のストレージプール、もう 1 つは 3 つのサイトすべてを含むストレージプール（「すべてのストレージノードのデフォルトのストレージプールとは異なる」）です。その後、管理者は 2 つの新しい ILM ルールと、 3 つのサイトすべてのデータを保護するために作成された新しいドラフトの ILM ポリシーを作成しました。



この新しい ILM ポリシーがアクティブ化されると、テナント A に属するオブジェクトが 3 つのサイトで 2+1 イレイジャーコーディングによって保護され、他のテナント（およびテナント A に属する小さいオブジェクト）に属するオブジェクトは 3 つのサイト間で 3 コピーレプリケーションによって保護されるようになります。

ルール **1** ：テナント **A** に **3** サイトイレイジャーコーディング

ルール定義	値の例
ルール名	テナント A の 3 サイトイレイジャーコーディング
テナントアカウント	テナント A

ルール定義	値の例
ストレージプール	3 つのデータセンターすべて（データセンター 1 、データセンター 2 、データセンター 3 を含む）
コンテンツ配置	0 日目から無期限に 3 つのデータセンターすべてに 2+1 のイレイジャーコーディングを実行

ルール **2** ：他のテナントに **3** つのサイトをレプリケーションする

ルール定義	値の例
ルール名	他のテナント用に 3 つのサイトにレプリケーション
テナントアカウント	無視します
ストレージプール	データセンター 1 、データセンター 2 、データセンター 3
コンテンツ配置	0 日目から無期限にレプリケートされたコピー 3 つ：データセンター 1 に 1 つ、データセンター 2 に 1 つ、データセンター 3 に 1 つ、

例 **6** のドラフト **ILM** ポリシーをアクティブ化しています

新しいドラフト ILM ポリシーをアクティブ化すると、既存のオブジェクトが新しい場所に移動されたり、新規または更新されたルールの配置手順に基づいて既存のオブジェクトの新しいオブジェクトコピーが作成されたりする可能性があります。

原因 ポリシーにエラーがあると、回復不能なデータ損失が発生する可能性があります。ポリシーをアクティブ化する前によく確認およびシミュレートし、想定どおりに機能することを確認してください。

新しい ILM ポリシーをアクティブ化すると、 StorageGRID は、そのポリシーを使用して、既存のオブジェクトと新たに取り込まれたオブジェクトを含むすべてのオブジェクトを管理します。新しい ILM ポリシーをアクティブ化する前に、既存のレプリケートオブジェクトとイレイジャーコーディングオブジェクトの配置に対する変更を確認してください。既存のオブジェクトの場所を変更すると、新しい配置が評価されて実装される際に一時的なリソースの問題が発生する可能性があります。

イレイジャーコーディングの手順が変わったときの動作

この例の現在アクティブな ILM ポリシーでは、テナント A に属するオブジェクトがデータセンター 1 で 2+1 のイレイジャーコーディングを使用して保護されます。新しいドラフトの ILM ポリシーでは、テナント A に属するオブジェクトがデータセンター 1 、 2 、 3 で 2+1 イレイジャーコーディングを使用して保護されます。

新しい ILM ポリシーがアクティブ化されると、次の ILM 処理が実行されます。

- テナント A で取り込まれた新しいオブジェクトは 2 つのデータフラグメントに分割され、 1 つのパリテ

ィフラグメントが追加される。その後、 3 つのフラグメントそれぞれが別々のデータセンターに格納されます。

- テナント A に属する既存のオブジェクトは、実行中の ILM スキャンプロセスで再評価されます。ILM の配置手順では新しいイレイジャーコーディングプロファイルが使用されるため、完全に新しいイレイジャーコーディングされたフラグメントが作成され、 3 つのデータセンターに分散されます。

> データセンター 1 の既存の 2+1 フラグメントは再利用されません。StorageGRID では、各イレイジャーコーディングプロファイルは一意とみなされ、新しいプロファイルを使用する場合はイレイジャーコーディングフラグメントが再利用されません。

レプリケーション手順が変わったときの動作

この例の現在アクティブな ILM ポリシーでは、他のテナントに属するオブジェクトは、データセンター 1 と 2 のストレージプール内の 2 つのレプリケートコピーを使用して保護されます。新しいドラフトの ILM ポリシーでは、他のテナントに属するオブジェクトが、データセンター 1 、 2 、 3 のストレージプール内の 3 つのレプリケートコピーを使用して保護されます。

新しい ILM ポリシーがアクティブ化されると、次の ILM 処理が実行されます。

- テナント A 以外のテナントに新しいオブジェクトが追加されると、 StorageGRID は 3 つのコピーを作成し、各データセンターに 1 つずつコピーを保存します。
- それらの他のテナントに属する既存のオブジェクトは、 ILM のスキャンプロセスの実行中に再評価されます。データセンター 1 とデータセンター 2 にある既存のオブジェクトコピーが新しい ILM ルールのレプリケーション要件を引き続き満たしているため、 StorageGRID はデータセンター 3 にオブジェクトの新しいコピーを 1 つ作成するだけで済みます。

このポリシーをアクティブ化した場合のパフォーマンスへの影響

この例でドラフトの ILM ポリシーをアクティブ化すると、この StorageGRID システムの全体的なパフォーマンスに一時的に影響します。テナント A の既存オブジェクト用に新しいイレイジャーコーディングフラグメントを作成し、他のテナントの既存オブジェクト用にデータセンター 3 に新しいレプリケートコピーを作成するには、通常よりも高いレベルのグリッドリソースが必要になります。

ILM ポリシーが変更されたため、クライアントの読み取り要求と書き込み要求が一時的に通常よりもレイテンシが高くなる可能性があります。配置手順がグリッド全体に完全に実装されたあと、レイテンシは通常レベルに戻ります。

新しい ILM ポリシーをアクティブ化する際のリソースの問題を回避するには、既存のオブジェクトの数が多い場合にルールで取り込み時間の高度なフィルタを使用します。既存のオブジェクトが不必要に移動されないようにするために、新しいポリシーが適用されるおおよその時間よりも長くなるように取り込み時間を設定します。

> ILM ポリシーの変更後にオブジェクトが処理される速度を遅くしたり、上げたりする必要がある場合は、テクニカルサポートにお問い合わせください。

例 **7** ： **S3** オブジェクトロックの準拠 **ILM** ポリシー

S3 オブジェクトのロックが有効なバケット内のオブジェクトの保護および保持の要件を満たす ILM ポリシーを定義する際は、以下の例の S3 バケット、 ILM ルール、 ILM ポリシーをベースとして使用できます。

以前の StorageGRID リリースで従来の準拠機能を使用していた場合、この例を使用して、従来の準拠機能が有効になっている既存のバケットを管理することもできます。

以下の ILM ルールとポリシーは一例にすぎません。ILM ルールを設定する方法は多数あります。新しいポリシーをアクティブ化する前に、ドラフトポリシーをシミュレートして、コンテンツの損失を防ぐためにドラフトポリシーが想定どおりに機能することを確認してください。

関連情報

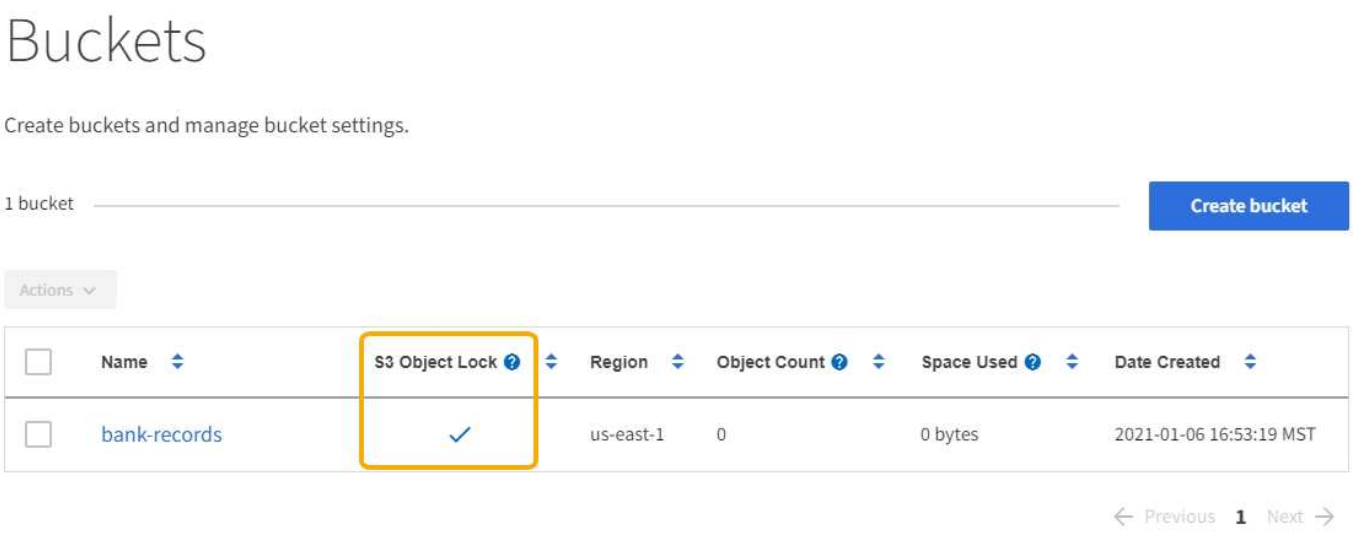
"S3オブジェクトロックでオブジェクトを管理する"

"ILMポリシーを作成する"

S3 オブジェクトのロックのバケットとオブジェクトの例

次の例では、 Bank of ABC という名前の S3 テナントアカウントで、 Tenant Manager を使用して、重要な銀行記録を格納するために S3 オブジェクトロックを有効にしたバケットを作成しています。

バケットの定義	値の例
テナントアカウント名	ABC 銀行
バケット名	銀行記録
バケットのリージョン	us-east-1 （デフォルト）



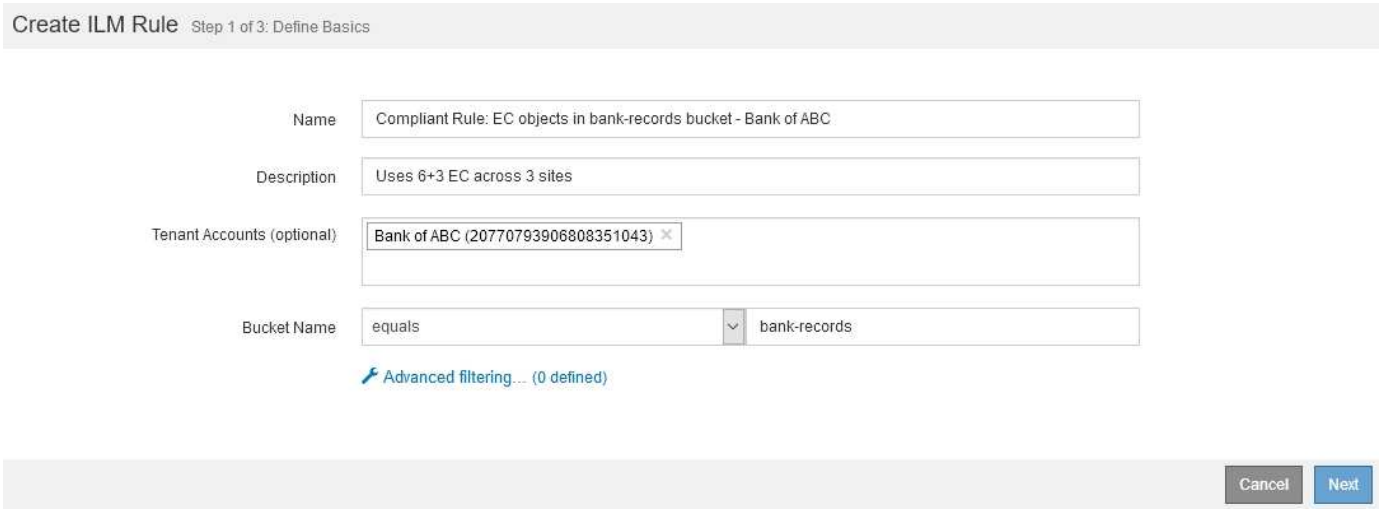
bank-recordsバケットに追加されるオブジェクトとオブジェクトのバージョンには、次の値が使用されます `retain-until-date` および `legal hold` 設定：

オブジェクトごとに設定します	値の例
`retain-until-date`	`"2030-12-30T23:59:59Z"` （12月30日、2030日） 各オブジェクトバージョンには独自のバージョンがあります `retain-until-date` 設定：この設定は、上げることはできますが、下げることはできません。
`legal hold`	`"OFF"` （無効） リーガルホールドは、保持期間中いつでも任意のオブジェクトバージョンに適用または解除できます。オブジェクトがリーガルホールドの対象になっている場合は、たとえであってもそのオブジェクトを削除することはできません `retain-until-date` に到達しました。

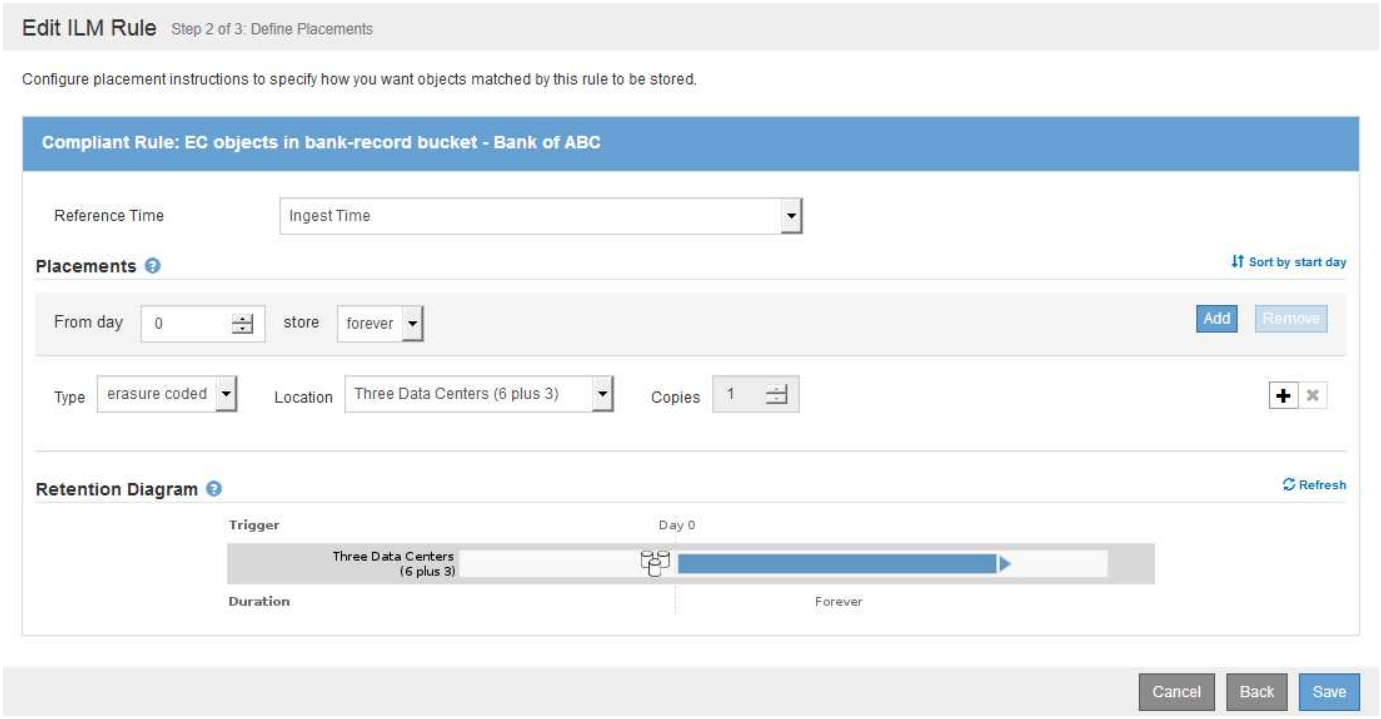
S3 オブジェクトのロックの **ILM** ルール **1** の例：イレイジャーコーディングプロファイルとバケットの照合

この例の ILM ルールは、 Bank of ABC という名前の S3 テナントアカウントのみに適用されます。内のすべてのオブジェクトに一致します `bank-records` その後、バケットとイレイジャーコーディングを使用して、6+3のイレイジャーコーディングプロファイルを使用して、3つのデータセンターサイトのストレージノードにオブジェクトを格納します。このルールは、 S3 オブジェクトロックが有効なバケットの要件を満たしています。イレイジャーコーディングコピーが 0 日目から無期限にストレージノードに保持され、参照時間として取り込み時間が使用されます。

ルール定義	値の例
ルール名	準拠ルール： Bank of ABC の銀行記録バケットの EC オブジェクト
テナントアカウント	ABC 銀行
バケット名	`bank-records`
高度なフィルタリング	オブジェクトサイズ（MB）が0.20より大きい *注：このフィルタは、200KB以下のオブジェクトにイレイジャーコーディングが使用されないようにします。



ルール定義	値の例
参照時間	取り込み時間
配置	0 日目のストアから永遠に
イレイジャーコーディングプロファイル	• 3 つのデータセンターサイトのストレージノードにイレイジャーコーディングコピーを作成します • 6+3 イレイジャーコーディングスキームを使用

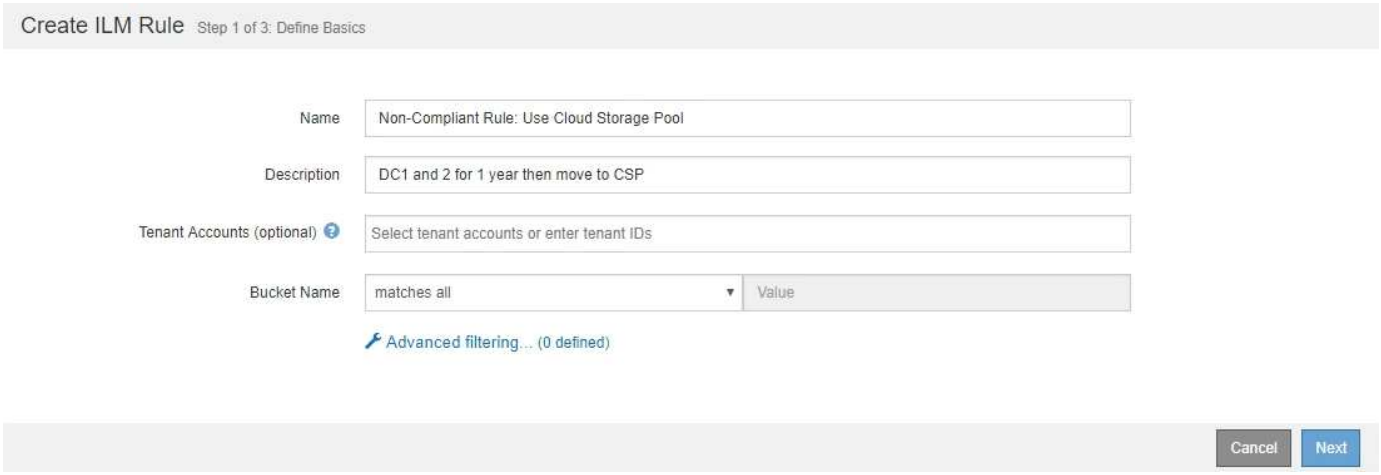


S3 オブジェクトのロックの例の **ILM** ルール **2** ：非準拠ルール

この例の ILM ルールでは、 2 つのレプリケートオブジェクトコピーをストレージノードに最初に格納します。1 年後、クラウドストレージプールに 1 つのコピーを無期限に格納します。このルールはクラウドストレ

ージプールを使用するため、非準拠となり、 S3 オブジェクトロックが有効になっているバケット内のオブジェクトには適用されません。

ルール定義	値の例
ルール名	非準拠ルール：クラウドストレージプールを使用
テナントアカウント	指定されていません
バケット名	指定されていませんが、 S3 オブジェクトロック（または従来の準拠機能）が有効になっていないバケットのみに適用されます。
高度なフィルタリング	指定されていません



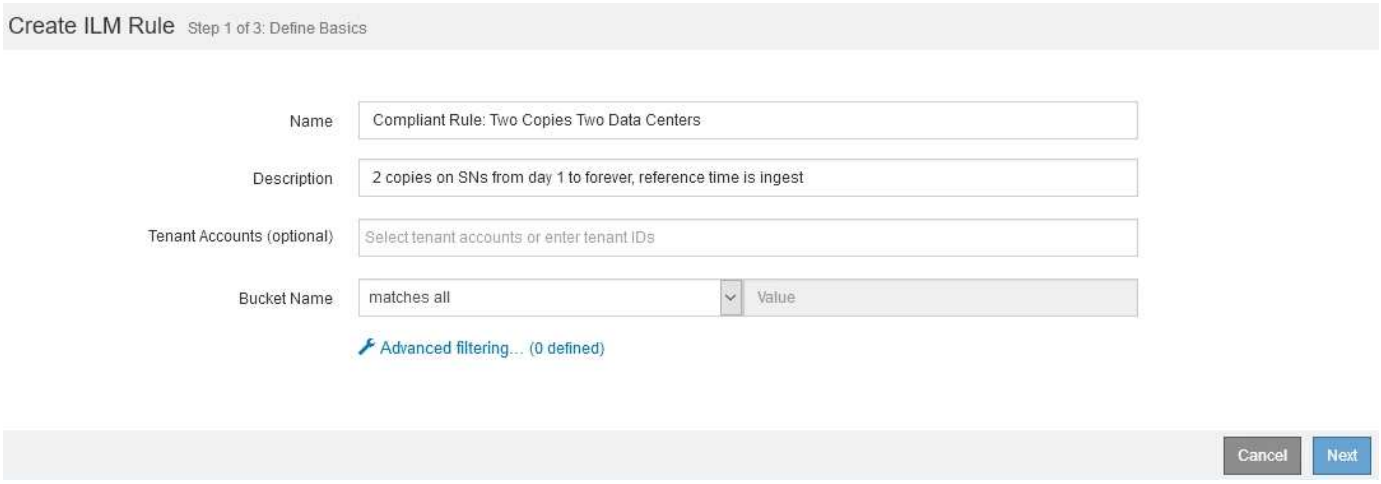
ルール定義	値の例
参照時間	取り込み時間
配置	• 0 日目から、 2 つのレプリケートコピーをデータセンター 1 とデータセンター 2 のストレージノードに 365 日間格納します • 1 年後、レプリケートコピーを 1 つクラウドストレージプールに無期限に格納します

S3 オブジェクトのロックの例の **ILM** ルール **3** ：デフォルトルール

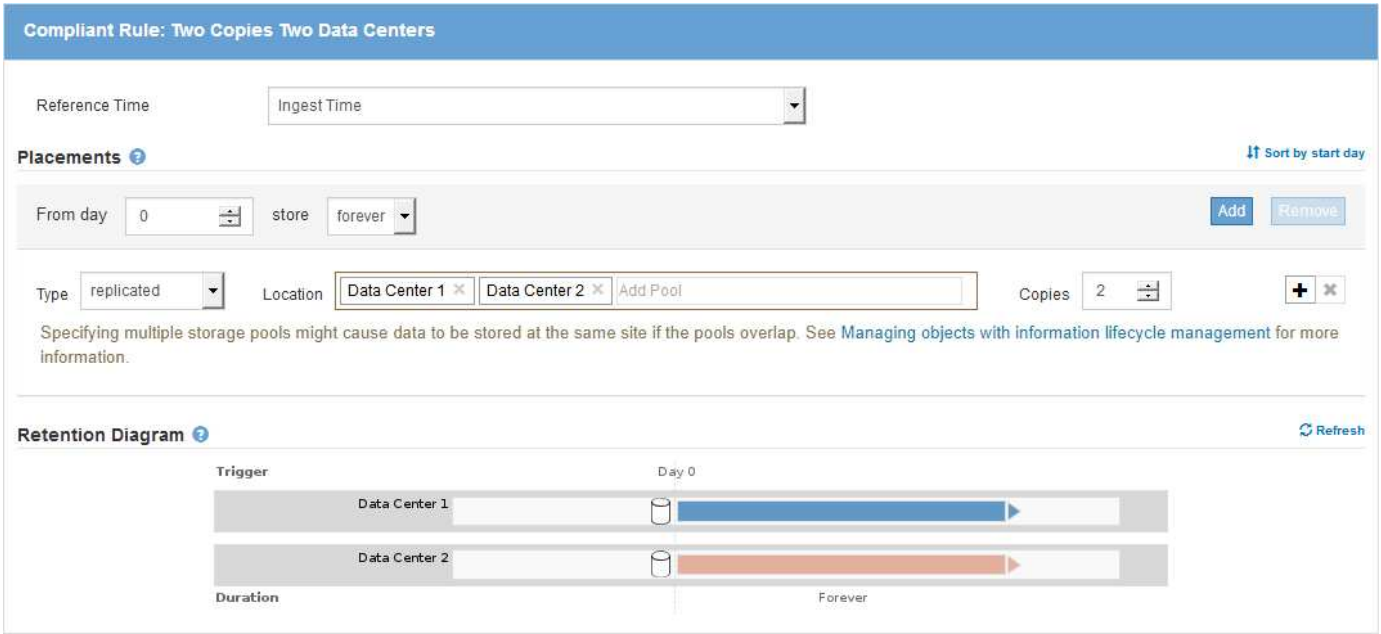
この ILM ルールの例では、 2 つのデータセンター内のストレージプールにオブジェクトデータをコピーします。この準拠ルールは、 ILM ポリシーのデフォルトルールとして設計されています。このルールにはフィルタは含まれておらず、S3オブジェクトロックが有効なバケットの要件を満たしています。参照時間として取り込みを使用して、2つのオブジェクトコピーが0日目から無期限にストレージノードに保持されます。

ルール定義	値の例
ルール名	デフォルトの準拠ルール： 2 つのコピーが 2 つのデータセンターを作成します

ルール定義	値の例
テナントアカウント	指定されていません
バケット名	指定されていません
高度なフィルタリング	指定されていません



ルール定義	値の例
参照時間	取り込み時間
配置	0 日目から無期限に、 2 つのレプリケートコピーを保持します。 1 つはデータセンター 1 のストレージノードに、もう 1 つはデータセンター 2 のストレージノードに保持します。

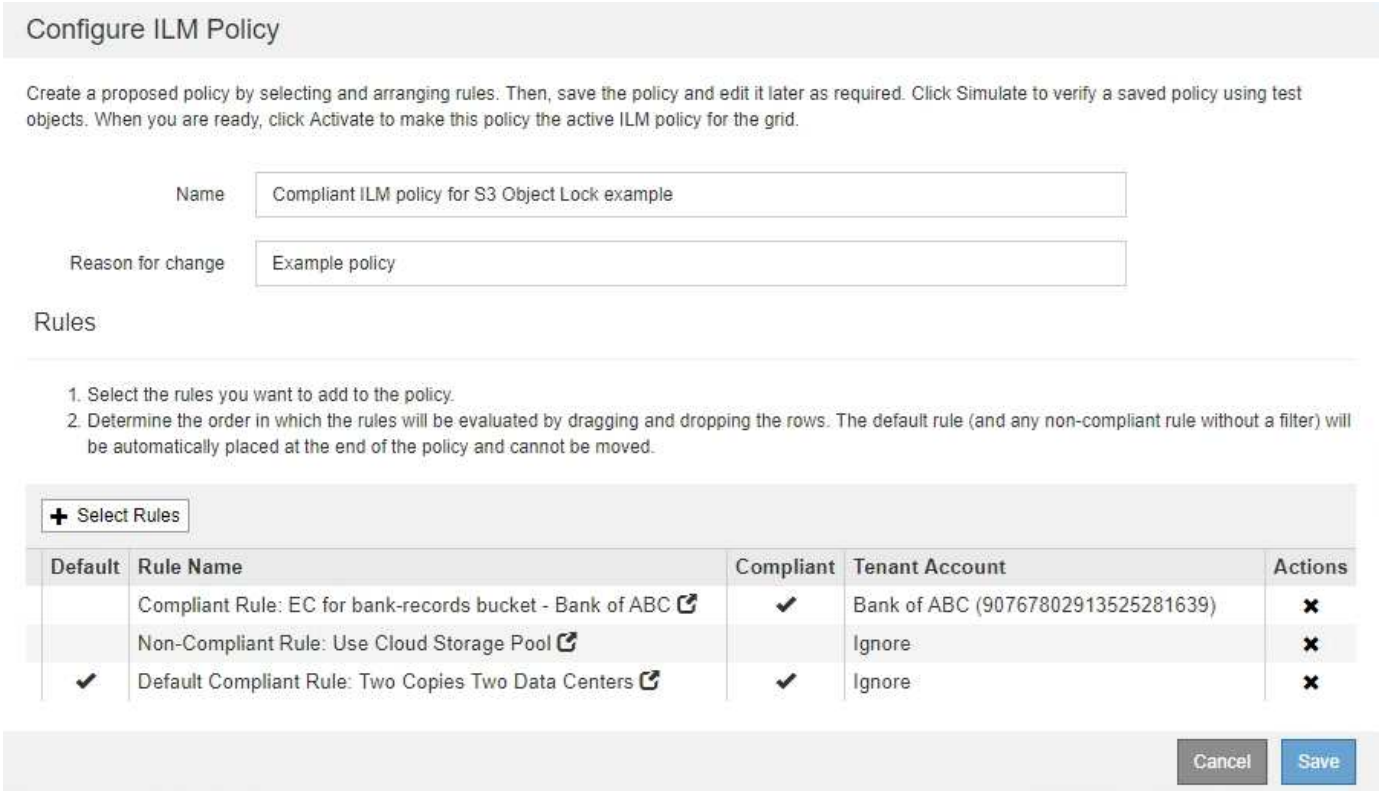


S3 オブジェクトロックが有効になっているバケット内のオブジェクトを含め、システム内のすべてのオブジェクトを効果的に保護する ILM ポリシーを作成するには、すべてのオブジェクトのストレージ要件を満たす ILM ルールを選択する必要があります。その後、ドラフトポリシーをシミュレートしてアクティブ化する必要があります。

ポリシーにルールを追加しています

この例では、 ILM ポリシーに、次の順序で 3 つの ILM ルールが含まれています。

1. S3オブジェクトロックが有効な特定のバケットで、イレイジャーコーディングを使用して200KBを超えるオブジェクトを保護する準拠ルール。オブジェクトは 0 日目から無期限にストレージノードに格納されます。
2. 2 つのレプリケートオブジェクトコピーを作成してストレージノードに 1 年間保存したあと、 1 つのオブジェクトコピーをクラウドストレージプールに無期限に移動する非準拠ルール。S3 オブジェクトロックが有効になっているバケットでは、クラウドストレージプールを使用するため、このルールは適用されません。
3. 2 つのレプリケートオブジェクトコピーを 0 日目からストレージノードに無期限に作成するデフォルトの準拠ルール。



ドラフトポリシーをシミュレートする

ドラフトポリシーにルールを追加してデフォルトの準拠ルールを選択し、他のルールを配置したら、 S3 オブジェクトロックを有効にしたバケットおよび他のバケットのオブジェクトをテストしてポリシーをシミュレートする必要があります。たとえば、この例のポリシーをシミュレートすると、テストオブジェクトは次のように評価されます。

- 最初のルールは、Bank of ABCテナントのバケットバンクレコードで200KBを超えるテストオブジェクト

のみに一致します。

- 2 番目のルールは、他のすべてのテナントアカウントの非準拠バケット内のすべてのオブジェクトに一致します。
- デフォルトのルールは次のオブジェクトに一致します。
  - バケットバンク内の200KB以下のオブジェクト- Bank of ABCテナントのレコード。
  - 他のすべてのテナントアカウントで S3 オブジェクトロックが有効になっている他のバケット内のオブジェクト。

ポリシーをアクティブ化しています

新しいポリシーによってオブジェクトデータが適切に保護されることを確認したら、アクティブ化します。

システムの保護対策

StorageGRID システムをセキュリティの脅威から保護するためのシステム設定、ベストプラクティス、および推奨事項について説明します。

- "StorageGRID システムのセキュリティ強化"
- "ソフトウェアアップグレードの強化に関するガイドライン"
- "StorageGRID ネットワークのセキュリティ強化のガイドライン"
- "StorageGRID ノードの保護対策のガイドライン"
- "サーバ証明書のセキュリティ強化ガイドライン"
- "その他のセキュリティ強化に関するガイドライン"]

StorageGRID システムのセキュリティ強化

システムのセキュリティ強化とは、 StorageGRID システムからできるだけ多くのセキュリティリスクを排除するプロセスです。

このドキュメントでは、 StorageGRID 固有の強化ガイドラインの概要を説明します。これらのガイドラインは、システム強化に関する業界標準のベストプラクティスを補足するものです。たとえば、次のガイドラインでは、 StorageGRID に強力なパスワードを使用し、 HTTP ではなく HTTPS を使用し、可能な場合は証明書ベースの認証を有効にすることを前提としています。

StorageGRID をインストールして構成する際に、これらのガイドラインを使用して、情報システムの機密性、整合性、可用性に関する規定のセキュリティ目標を達成できます。

StorageGRID は、 _NetApp 脆弱性処理ポリシー _ に従います。報告された脆弱性は、製品セキュリティインシデント対応プロセスに従って検証および解決されます。

StorageGRID システムを強化するための一般的な考慮事項

StorageGRID システムを強化する際は、次の点を考慮する必要があります。

- 実装した 3 つの StorageGRID ネットワークのうち、どれですか。すべての StorageGRID システムでグリッドネットワークを使用する必要がありますが、管理ネットワーク、クライアントネットワーク、または

その両方を使用することもできます。ネットワークごとにセキュリティに関する考慮事項が異なります。

- StorageGRID システムの個々のノードで使用するプラットフォームのタイプ。StorageGRID ノードは、VMware仮想マシン、Linuxホスト上のDockerコンテナ内に導入できるほか、専用のハードウェアアプライアンスとして導入することもできます。プラットフォームのタイプごとに、強化に関するベストプラクティスがあります。
- テナントアカウントが信頼されている方法。テナントアカウントを信頼しないサービスプロバイダである場合は、信頼できる社内テナントのみを使用した場合とはセキュリティ上の問題が異なります。
- どのセキュリティ要件および規則に準拠しているか。特定の規制や企業の要件に準拠しなければならない場合があります。

関連情報

"脆弱性対策ポリシー"

ソフトウェアアップグレードの強化に関するガイドライン

攻撃を防御するには、 StorageGRID システムおよび関連サービスを最新の状態に保つ必要があります。

StorageGRID ソフトウェアへのアップグレード

StorageGRID ソフトウェアは、可能なかぎり、最新のメジャーリリースまたは以前のメジャーリリースにアップグレードする必要があります。StorageGRID を最新の状態に保つことで、既知の脆弱性がアクティブになる時間を短縮し、攻撃対象領域全体を削減できます。また、 StorageGRID の最新リリースには、以前のリリースには含まれていないセキュリティ強化機能が含まれていることがよくあります。

ホットフィックスが必要になったときに、ネットアップは最新リリースの更新プログラムの作成に優先順位を付けます。一部のパッチは、以前のリリースと互換性がない場合があります。

StorageGRID の最新のリリースやホットフィックスをダウンロードするには、 StorageGRID のソフトウェアダウンロードページにアクセスします。StorageGRID ソフトウェアのアップグレード手順については、StorageGRID のアップグレード手順を参照してください。ホットフィックスの適用手順については、リカバリとメンテナンスの手順を参照してください。

外部サービスへのアップグレード

外部サービスには、 StorageGRID に間接的に影響する脆弱性が存在する場合がありますStorageGRID が依存するサービスが最新の状態に保たれていることを確認してください。LDAP 、 KMS （ KMIP サーバ）、 DNS 、 NTP などのサービスを利用できます。

サポートされているバージョンの一覧については、 NetApp Interoperability Matrix Tool を参照してください。

ハイパーバイザーのアップグレード

StorageGRID ノードが VMware または別のハイパーバイザーで実行されている場合は、ハイパーバイザーのソフトウェアとファームウェアが最新であることを確認する必要があります。

サポートされているバージョンの一覧については、 NetApp Interoperability Matrix Tool を参照してください。

*** Linuxノードへのアップグレード***

StorageGRID ノードで Linux ホストプラットフォームを使用している場合は、セキュリティ更新とカーネル更新がホスト OS に適用されていることを確認する必要があります。また、これらの更新プログラムが利用可能になった場合は、脆弱なハードウェアにファームウェアの更新プログラムを適用する必要があります。

サポートされているバージョンの一覧については、 NetApp Interoperability Matrix Tool を参照してください。

関連情報

"ネットアップのダウンロード： StorageGRID"

"ソフトウェアをアップグレードする"

""

"NetApp Interoperability Matrix Tool で確認できます"

StorageGRID ネットワークのセキュリティ強化のガイドライン

StorageGRID システムでは、グリッドノードあたり最大 3 つのネットワークインターフェイスがサポートされ、各グリッドノードのネットワークをセキュリティやアクセスの要件に応じて設定することができます。

グリッドネットワークのガイドライン

グリッドネットワークはすべての内部 StorageGRID トラフィック用に設定する必要があります。グリッドネットワークのグリッドノードは、いずれも他のすべてのノードと通信できなければなりません。

グリッドネットワークを設定する際は、次のガイドラインに従ってください。

- オープンインターネット上のクライアントなど、信頼できないクライアントからネットワークが保護されていることを確認します。
- 可能な場合は、グリッドネットワークを内部トラフィック専用にします。管理ネットワークとクライアントネットワークの両方に、内部サービスへの外部トラフィックをブロックするファイアウォール制限が追加されています。グリッドネットワークを使用した外部クライアントトラフィックの処理はサポートされていますが、この使用によって保護レイヤが少なくなります。
- StorageGRID 環境が複数のデータセンターにまたがっている場合は、仮想プライベートネットワーク（ VPN ）またはグリッドネットワーク上で同等の機能を使用して、内部トラフィックをさらに保護します。
- 一部のメンテナンス手順では、プライマリ管理ノードと他のすべてのグリッドノードの間のポート 22 で Secure Shell （ SSH ）アクセスが必要です。外部ファイアウォールを使用して、信頼できるクライアントへの SSH アクセスを制限します。

管理ネットワークのガイドライン

管理ネットワークは、通常、管理タスク（ Grid Manager または SSH を使用する信頼できる従業員）および LDAP 、 DNS 、 NTP 、 KMS （ KMIP サーバ）などの信頼された他のサービスとの通信に使用します。ただし、 StorageGRID ではこの使用が内部的に適用されることはありません。

管理ネットワークを使用する場合は、次のガイドラインに従ってください。

- 管理ネットワーク上のすべての内部トラフィックポートをブロックします。使用するプラットフォームに対応したインストールガイドの内部ポートの一覧を参照してください。
- 信頼されていないクライアントが管理ネットワークにアクセスできる場合は、外部ファイアウォールで管理ネットワーク上の StorageGRID へのアクセスをブロックします。

クライアントネットワークのガイドライン

クライアントネットワークは、通常、テナント、および CloudMirror レプリケーションサービスや別のプラットフォームサービスなどの外部サービスとの通信に使用されます。ただし、 StorageGRID ではこの使用が内部的に適用されることはありません。

クライアントネットワークを使用する場合は、次のガイドラインに従ってください。

- クライアントネットワーク上のすべての内部トラフィックポートをブロックします。使用するプラットフォームに対応したインストールガイドの内部ポートの一覧を参照してください。
- 明示的に設定されたエンドポイントでのみ、インバウンドクライアントトラフィックを受け入れます。StorageGRID の管理手順の信頼されていないクライアントネットワークの管理に関する情報を参照してください。

関連情報

"ネットワークガイドライン"

"グリッド入門"

"StorageGRID の管理"

"Red Hat Enterprise Linux または CentOS をインストールします"

"Ubuntu または Debian をインストールします"

"VMware をインストールする"

StorageGRID ノードの保護対策のガイドライン

StorageGRID ノードは、VMware仮想マシン、Linuxホスト上のDockerコンテナ内に導入できるほか、専用のハードウェアアプライアンスとして導入することもできます。プラットフォームのタイプとノードのタイプにはそれぞれ、強化に関するベストプラクティスがあります。

ファイアウォールの設定

システム強化プロセスの一環として、外部ファイアウォールの設定を確認し、 IP アドレスとそれが厳密に必要なポートからのみトラフィックが許可されるように変更する必要があります。

VMwareプラットフォームおよびStorageGRID アプライアンスで実行されるノードは、自動的に管理される内部ファイアウォールを使用します。この内部ファイアウォールは、一部の一般的な脅威に対する追加の保護レイヤを提供しますが、外部ファイアウォールの必要性は排除されません。

StorageGRID で使用されるすべての内部ポートと外部ポートの一覧については、ご使用のプラットフォームのインストールガイドを参照してください。

仮想化、コンテナ、共有ハードウェア

すべての StorageGRID ノードで、信頼されていないソフトウェアと同じ物理ハードウェア上で StorageGRID を実行しないでください。StorageGRID とマルウェアの両方が同じ物理ハードウェア上に存在する場合、ハイパーバイザーによる保護によって、 StorageGRID で保護されたデータへのマルウェアのアクセスが防止されるとは限りません。たとえば、 Meltdown と Specter 攻撃は、最新のプロセッサに存在する重要な脆弱性を悪用し、プログラムが同じコンピュータ上のメモリにデータを盗むことを可能にします。

未使用のサービスを無効にします

すべての StorageGRID ノードについて、未使用のサービスへのアクセスを無効化またはブロックする必要があります。たとえば、 CIFS または NFS 用の監査共有へのクライアントアクセスを設定しない場合は、これらのサービスへのアクセスをブロックするか無効にします。

インストール中にノードを保護

信頼されていないユーザが、ノードのインストール時にネットワーク経由で StorageGRID ノードにアクセスすることを許可しないでください。ノードは、グリッドに参加するまで完全にはセキュアではありません。

管理ノードのガイドライン

管理ノードは、システムの設定、監視、ロギングなどの管理サービスを提供します。Grid Manager または Tenant Manager にサインインすると、管理ノードに接続されます。

StorageGRID システムで管理ノードを保護するには、次のガイドラインに従います。

- 開いているインターネット上の管理ノードなど、信頼されていないクライアントからすべての管理ノードを保護します。グリッドネットワーク上、管理ネットワーク上、またはクライアントネットワーク上のどの管理ノードにも、信頼されていないクライアントがアクセスできないようにします。
- StorageGRID グループは Grid Manager とテナントマネージャの機能へのアクセスを制御します。各ユーザグループにロールに最低限必要な権限を付与し、読み取り専用アクセスモードを使用してユーザによる設定変更を防止します。
- StorageGRID ロードバランサエンドポイントを使用する場合は、信頼されないクライアントトラフィックに管理ノードの代わりにゲートウェイノードを使用します。
- 信頼されていないテナントがある場合は、テナントマネージャやテナント管理 API に直接アクセスすることを許可しないでください。代わりに、信頼されていないテナントがテナントポータルまたはテナント管理 API と連動する外部テナント管理システムを使用するようにします。
- 必要に応じて、管理ノードからネットアップサポートへの AutoSupport 通信をより細かく制御するために管理プロキシを使用します。StorageGRID の管理手順の管理プロキシの作成手順を参照してください。
- 必要に応じて、制限された 8443 ポートと 9443 ポートを使用して Grid Manager と Tenant Manager の通信を分離します。共有ポート 443 をブロックして、テナント要求をポート 9443 に制限して追加の保護を確保します。
- 必要に応じて、グリッド管理者とテナントユーザには別々の管理ノードを使用します。

詳細については、 StorageGRID の管理手順を参照してください。

ストレージノードに関するガイドライン

ストレージノードは、オブジェクトデータとメタデータを管理および格納します。StorageGRID システムでストレージノードを保護するには、次のガイドラインに従います。

- 信頼されていないテナントのアウトバウンドサービスは有効にしないでください。たとえば、信頼されていないテナントのアカウントを作成する場合は、テナントが独自のアイデンティティソースを使用することを許可せず、プラットフォームサービスの使用も許可しないでください。StorageGRID の管理手順に従って、テナントアカウントを作成する手順を参照してください。
- 信頼されないクライアントトラフィックには、サードパーティのロードバランサを使用します。サードパーティ製のロードバランシングにより、攻撃に対する制御性が向上し、追加の保護レイヤが提供されます。
- 必要に応じて、ストレージプロキシを使用して、クラウドストレージプールとプラットフォームサービスのストレージノードから外部サービスへの通信をより細かく制御します。StorageGRID の管理手順のストレージプロキシの作成手順を参照してください。
- 必要に応じて、クライアントネットワークを使用して外部サービスに接続します。次に、「* Configuration > Network Settings > Untrusted Client Network *」を選択し、ストレージノード上のクライアントネットワークが信頼されていないことを示します。ストレージノードはクライアントネットワーク上の受信トラフィックを受け入れなくなりますが、プラットフォームサービスへのアウトバウンド要求は引き続き許可します。

ゲートウェイノードのガイドライン

ゲートウェイノードは、クライアントアプリケーションが StorageGRID への接続に使用できるオプションのロードバランシングインターフェイスです。StorageGRID システムにゲートウェイノードを保護するには、次のガイドラインに従います。

- ゲートウェイノード上の CLB サービスを使用する代わりに、ロードバランサエンドポイントを設定して使用する。StorageGRID の管理手順のロードバランシングの管理手順を参照してください。

  CLB サービスは廃止されました。

- クライアントとゲートウェイノードまたはストレージノードの間で、信頼されていないクライアントトラフィックにサードパーティのロードバランサを使用します。サードパーティ製のロードバランシングにより、攻撃に対する制御性が向上し、追加の保護レイヤが提供されます。サードパーティのロードバランサを使用する場合でも、内部のロードバランサエンドポイントを経由するようにネットワークトラフィックを設定したり、ストレージノードに直接送信したりすることができます。
- ロードバランサエンドポイントを使用している場合は、必要に応じてクライアントネットワーク経由で接続します。次に、「* Configuration > Network Settings > Untrusted Client Network *」を選択し、ゲートウェイノード上のクライアントネットワークが信頼されていないことを示します。ゲートウェイノードは、ロードバランサエンドポイントとして明示的に設定されたポートのインバウンドトラフィックのみを受け入れます。

ハードウェアアプライアンスノードのガイドライン

StorageGRID ハードウェアアプライアンスは、 StorageGRID システム専用に設計されています。一部のアプライアンスはストレージノードとして使用できます。その他のアプライアンスは、管理ノードまたはゲートウェイノードとして使用できます。アプライアンスノードをソフトウェアベースのノードと組み合わせることも、自社開発の全アプライアンスグリッドを導入することもできます。

StorageGRID システムにハードウェアアプライアンスノードを固定するには、次のガイドラインに従います。

- アプライアンスでストレージコントローラの管理に SANtricity System Manager を使用している場合は、信頼されていないクライアントからネットワーク経由で SANtricity System Manager にアクセスできないようにします。

- アプライアンスに Baseboard Management Controller （ BMC ；ベースボード管理コントローラ）が搭載されている場合は、 BMC 管理ポートで下位レベルのハードウェアアクセスが許可されることに注意してください。BMC 管理ポートは、信頼されているセキュアな内部管理ネットワークにのみ接続してください。該当するネットワークがない場合は、テクニカルサポートから BMC 接続の要請があった場合を除き、 BMC 管理ポートを接続しないか、またはブロックしたままにしてください。
- アプライアンスが Intelligent Platform Management Interface （ IPMI ）標準を使用したイーサネット経由でのコントローラハードウェアのリモート管理をサポートする場合は、ポート 623 での信頼されていないトラフィックをブロックします。
- アプライアンスのストレージコントローラに FDE または FIPS ドライブが搭載されていて、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 を使用してドライブセキュリティキーを設定します。
- FDE または FIPS ドライブが搭載されていないアプライアンスの場合は、 Key Management Server （ KMS ）を使用してノード暗号化を有効にします。

使用している StorageGRID ハードウェアアプライアンスのインストールとメンテナンスの手順を参照してください。

関連情報

"Red Hat Enterprise Linux または CentOS をインストールします"

"Ubuntu または Debian をインストールします"

"VMware をインストールする"

"StorageGRID の管理"

"テナントアカウントを使用する"

"SG100 SG1000サービスアプライアンス"

"SG5600 ストレージアプライアンス"

"SG5700 ストレージアプライアンス"

"SG6000 ストレージアプライアンス"

サーバ証明書のセキュリティ強化ガイドライン

インストール時に作成されたデフォルトの証明書を独自のカスタム証明書に置き換える必要があります。

多くの組織では、 StorageGRID Web アクセス用の自己署名デジタル証明書が、情報セキュリティポリシーに準拠していません。本番用システムでは、 StorageGRID の認証に使用する CA 署名デジタル証明書をインストールする必要があります。

具体的には、次のデフォルト証明書ではなくカスタムサーバ証明書を使用する必要があります。

- 管理インターフェイスのサーバ証明書：Grid Manager、テナントマネージャ、Grid管理API、テナント管理APIへのアクセスを保護するために使用されます。
- * Object Storage API Service Endpoints Server Certificate *：ストレージノードおよびゲートウェイノード

へのアクセスを保護するために使用します。これらのノードは、S3およびSwiftクライアントアプリケーションがオブジェクトデータをアップロードおよびダウンロードするために使用します。

> StorageGRID では、ロードバランサエンドポイントに使用する証明書は別に管理されます。ロードバランサ証明書を設定するには、 StorageGRID の管理手順でロードバランサエンドポイントの設定手順を参照してください。

カスタムサーバ証明書を使用する場合は、次のガイドラインに従ってください。

- 証明書にはが必要です *subjectAltName* StorageGRID のDNSエントリと同じです。詳細については、のセクション 4.2.1.6 「 Subject Alternative Name 」を参照してください "RFC 5280: PKIX 証明書と CRL プロファイル"。
- 可能であれば、ワイルドカード証明書は使用しないでください。このガイドラインの例外は、 S3 仮想ホスト形式のエンドポイントの証明書です。バケット名が事前に不明な場合は、ワイルドカードを使用する必要があります。
- 証明書にワイルドカードを使用する必要がある場合は、リスクを軽減するために追加の手順を実行する必要があります。などのワイルドカードパターンを使用します `*.s3.example.com`を使用せずに、を使用してください `s3.example.com` その他のアプリケーションのサフィックス。このパターンは、などのパス形式のS3アクセスでも機能します `dc1-s1.s3.example.com/mybucket`。
- 証明書の有効期限を短く（ 2 カ月など）設定し、グリッド管理 API を使用して証明書のローテーションを自動化します。これは、ワイルドカード証明書で特に重要です。

また、クライアントは StorageGRID との通信に厳密なホスト名チェックを使用する必要があります。

その他のセキュリティ強化に関するガイドライン

StorageGRID ネットワークおよびノードに対する強化ガイドラインに加えて、StorageGRID システムの他の領域に対する強化ガイドラインに従う必要があります。

ログと監査メッセージ

StorageGRID ログおよび監査メッセージ出力は必ず安全な方法で保護してください。StorageGRID のログと監査メッセージは、サポートやシステム可用性の観点から非常に重要な情報を提供します。また、StorageGRID のログおよび監査メッセージの出力に含まれる情報や詳細情報は、一般に機密性が高いため、

StorageGRID ログの詳細については、監視とトラブルシューティングの手順を参照してください。StorageGRID 監査メッセージの詳細については、監査メッセージに関する手順を参照してください。

NetApp AutoSupport

StorageGRID の AutoSupport 機能を使用すると、システムの状態をプロアクティブに監視し、ネットアップテクニカルサポート、組織の社内サポートチーム、またはサポートパートナーにメッセージと詳細を自動的に送信できます。デフォルトでは、 StorageGRID を初めて設定した場合、ネットアップテクニカルサポートへの AutoSupport メッセージが有効になります。

AutoSupport 機能は無効にすることができます。ただし、 StorageGRID システムで問題 に障害が発生した場合には、 AutoSupport を使用して迅速に問題を識別し解決できるため、ネットアップではこの機能を有効にすることを推奨してい

AutoSupport は、転送プロトコルとして HTTPS 、 HTTP 、 SMTP をサポートしています。AutoSupport メッ

セージは機密性が高いため、ネットアップでは、 AutoSupport メッセージをネットアップサポートに送信する際のデフォルト転送プロトコルとして HTTPS を使用することを強く推奨しています。

必要に応じて、管理ノードからネットアップテクニカルサポートへの AutoSupport 通信をより細かく制御するための管理プロキシを設定できます。StorageGRID の管理手順の管理プロキシの作成手順を参照してください。

Cross-Origin Resource Sharing （ CORS ）

S3 バケットとバケット内のオブジェクトに他のドメインにある Web アプリケーションからアクセスできるようにする必要がある場合は、そのバケットに Cross-Origin Resource Sharing （ CORS ）を設定できます。一般に、 CORS は必要でないかぎり有効にしないでください。CORS が必要な場合は、信頼できるオリジンに制限します。

テナントアカウントの使用手順の Cross-Origin Resource Sharing （ CORS ）の設定手順を参照してください。

外部セキュリティデバイス

完全なセキュリティ強化解決策 は、 StorageGRID 以外のセキュリティメカニズムに対応する必要があります。StorageGRID へのアクセスをフィルタリングおよび制限するために追加のインフラデバイスを使用すると、厳格なセキュリティ体制を確立し、維持するための効果的な方法となります。これらの外部セキュリティデバイスには、ファイアウォール、 Intrusion Prevention System （ IPS ；侵入防御システム）、およびその他のセキュリティデバイスが含まれます。

信頼されないクライアントトラフィックには、サードパーティのロードバランサを使用することを推奨します。サードパーティ製のロードバランシングにより、攻撃に対する制御性が向上し、追加の保護レイヤが提供されます。

関連情報

"トラブルシューティングを監視します"

"監査ログを確認します"

"テナントアカウントを使用する"

"StorageGRID の管理"

StorageGRID for FabricPool を設定します

StorageGRID をNetApp FabricPool クラウド階層として設定する方法について説明します。

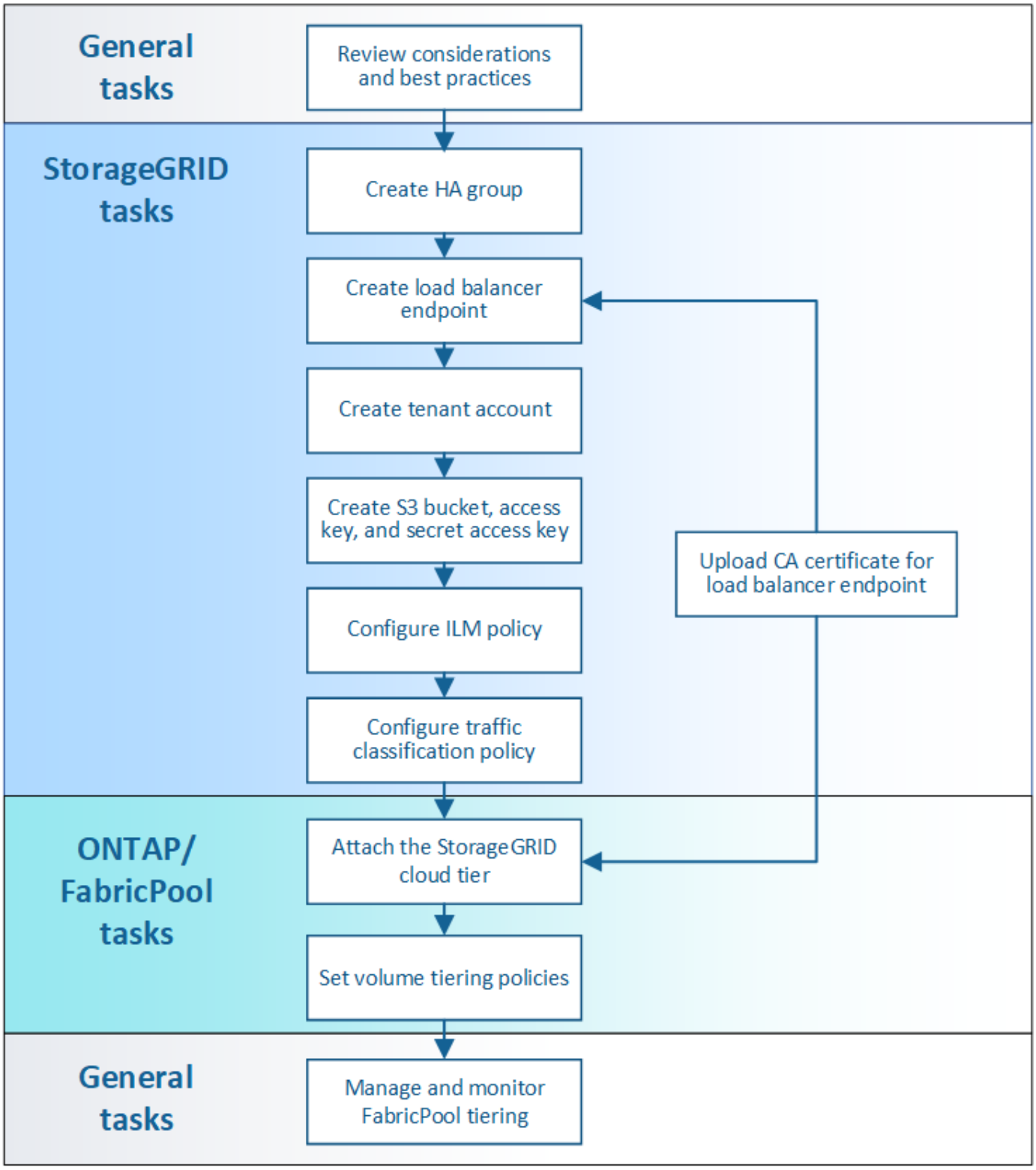
- "StorageGRID for FabricPool を設定しています"
- "StorageGRID をクラウド階層として接続するために必要な情報"
- "StorageGRID の情報ライフサイクル管理とFabricPool のデータを使用する"
- "FabricPool のトラフィック分類ポリシーを作成する"
- "StorageGRID および FabricPool に関するその他のベストプラクティスです"

StorageGRID for FabricPool を設定しています

NetApp ONTAP ソフトウェアを使用すると、 NetApp FabricPool を使用して、アクセス頻度の低いデータやコールドデータを NetApp StorageGRID オブジェクトストレージシステムに階層化できます。

次の手順に従って、次の操作を行います

- FabricPool で使用する StorageGRID オブジェクトストレージシステムの設定の概要について説明します。
- StorageGRID を FabricPool クラウド階層として接続した場合に ONTAP に入力する情報の入手方法について説明します。
- StorageGRID 情報ライフサイクル管理（ ILM ）ポリシー、 StorageGRID トラフィック分類ポリシー、および FabricPool ワークロードのその他の StorageGRID オプションを設定するためのベストプラクティスについて説明します。



必要なもの

これらの手順を使用する前に、次の

- アクセス頻度の低い ONTAP データを StorageGRID に階層化するときに使用する FabricPool ボリューム階層化ポリシーを決定します。
- ストレージ容量とパフォーマンスのニーズを満たす StorageGRID システムを計画して設置します。
- Grid Manager や Tenant Manager を含む StorageGRID システムソフトウェアの理解

関連情報

- "TR-4598：『FabricPool Best Practices for ONTAP 9.8』"
- "ONTAP 9 ドキュメンテーション・センター"

FabricPool とは

FabricPool は、ハイパフォーマンスのフラッシュアグリゲートを高パフォーマンス階層として、オブジェクトストアをクラウド階層として使用する ONTAP ハイブリッドストレージ解決策 です。FabricPool 内のデータは、アクセス頻度に応じてどちらかの階層に格納されます。FabricPool を使用すると、パフォーマンス、効率、保護を犠牲にすることなくストレージコストを削減できます。

アーキテクチャを変更する必要はなく、中央のONTAP ストレージシステムからデータベースとアプリケーションの環境を引き続き管理できます。

オブジェクトストレージとは

オブジェクトストレージは、ファイルストレージやブロックストレージなどの他のストレージアーキテクチャとは対照的に、データをオブジェクトとして管理するストレージアーキテクチャです。オブジェクトは単一のコンテナ（バケットなど）内に保持され、他のディレクトリ内のディレクトリにファイルとしてネストされることはありません。一般にオブジェクトストレージはファイルストレージやブロックストレージよりもパフォーマンスは低くなりますが、拡張性は大幅に向上します。StorageGRID バケットはペタバイト単位のデータを保持できます。

StorageGRID を**FabricPool** クラウド階層として使用する

FabricPool では、 ONTAP データを StorageGRID などの多数のオブジェクトストアプロバイダに階層化できます。サポートされる 1 秒あたりの最大入出力処理数（ IOPS ）をバケットレベルまたはコンテナレベルで設定する可能性があるパブリッククラウドとは異なり、 StorageGRID のパフォーマンスはシステム内のノード数に応じて拡張されます。StorageGRID を FabricPool クラウド階層として使用すると、コールドデータをプライベートクラウド内に保持することで、最高のパフォーマンスと完全なデータ管理を実現できます。

また、 StorageGRID をクラウド階層として使用する場合は、 FabricPool ライセンスは必要ありません。

StorageGRID で複数の**ONTAP** クラスタを使用する

以下の手順では、 StorageGRID を単一の ONTAP クラスタに接続する方法について説明します。ただし、同じ StorageGRID システムを複数の ONTAP クラスタに接続することができます。

複数の ONTAP クラスタから単一の StorageGRID システムにデータを階層化する場合は、クラスタごとに異なる S3 バケットを使用する必要があります。要件に応じて、すべてのクラスタに同じハイアベイラビリティ（ HA ）グループ、ロードバランサエンドポイント、およびテナントアカウントを使用するか、またはクラスタごとにこれらの項目をそれぞれ設定できます。

StorageGRID をクラウド階層として接続するために必要な情報

StorageGRID をFabricPool のクラウド階層として接続する前に、StorageGRID でいくつかの設定手順を実行して特定の値を取得する必要があります。

このタスクについて

次の表に、 FabricPool のクラウド階層として StorageGRID を接続する場合に ONTAP に入力する必要がある情報を示します。このセクションのトピックでは、 StorageGRID のグリッドマネージャとテナントマネージ

ャを使用して必要な情報を取得する方法について説明します。

表示されるフィールド名と ONTAP で必要な値の入力プロセスは、 ONTAP CLI （ storage aggregate object-store config create ）と ONTAP System Manager （ * Storage * > * Aggregates & Disks * > * Cloud Tier * ）のどちらを使用しているかによって異なります。

詳細については、以下を参照してください。

- "TR-4598：『FabricPool Best Practices for ONTAP 9.8』"
- "ONTAP 9 ドキュメンテーション・センター"

ONTAP フィールド	説明
オブジェクトストア名	一意でわかりやすい名前。例： `StorageGRID_Cloud_Tier`。
プロバイダタイプ	StorageGRID （System Manager）または `SGWS` （CLI）。
ポート	FabricPool が StorageGRID に接続するときに使用するポート。StorageGRID ロードバランサエンドポイントを定義する際に使用するポート番号を指定します。 "FabricPool のロードバランサエンドポイントの作成"
サーバ名	StorageGRID ロードバランサエンドポイントの完全修飾ドメイン名（ FQDN ）。例： `s3.storagegrid.company.com`。 次の点に注意してください。 • ここで指定するドメイン名は、 StorageGRID ロードバランサエンドポイント用にアップロードする CA 証明書のドメイン名と一致する必要があります。 • このドメイン名の DNS レコードは、 StorageGRID への接続に使用する各 IP アドレスにマッピングする必要があります。 "StorageGRID IPアドレス用のDNSサーバを設定する"
コンテナ名	この ONTAP クラスタで使用する StorageGRID バケットの名前。例： `fabricpool-bucket`。このバケットはTenant Managerで作成します。 次の点に注意してください。 • 設定の作成後にバケット名を変更することはできません。 • バケットでバージョン管理を有効にすることはできません。 • データを StorageGRID に階層化する ONTAP クラスタごとに異なるバケットを使用する必要があります。 "S3バケットを作成してアクセスキーを取得する"

ONTAP フィールド	説明
アクセスキーとシークレットのパスワード	StorageGRID テナントアカウントのアクセスキーとシークレットアクセスキー。 これらの値は Tenant Manager で生成します。 "S3バケットを作成してアクセスキーを取得する"
SSL	有効にする必要があります。
オブジェクトストアの証明書	StorageGRID ロードバランサエンドポイントの作成時にアップロードした CA 証明書。 • 注：中間 CA が StorageGRID 証明書を発行した場合は、中間 CA 証明書を指定する必要があります。StorageGRID 証明書がルート CA によって直接発行された場合は、ルート CA 証明書を指定する必要があります。 "FabricPool のロードバランサエンドポイントの作成"

完了後

必要な StorageGRID 情報を取得したら、 ONTAP にアクセスしてクラウド階層として StorageGRID を追加し、クラウド階層をアグリゲートとして追加し、ボリューム階層化ポリシーを設定できます。

ロードバランシングのベストプラクティスを参照してください

StorageGRID をFabricPool クラウド階層として接続する前に、StorageGRID グリッドマネージャを使用して少なくとも1つのロードバランサエンドポイントを設定します。

ロードバランシングとは

データを FabricPool から StorageGRID システムに階層化すると、 StorageGRID はロードバランサを使用して取り込みと読み出しのワークロードを管理します。ロードバランシングは、 FabricPool ワークロードを複数のストレージノードに分散することで、速度と接続容量を最大化します。

StorageGRID ロードバランササービスはすべての管理ノードとすべてのゲートウェイノードにインストールされ、レイヤ 7 のロードバランシングを提供します。クライアント要求の Transport Layer Security （ TLS ）終了を実行し、要求を検査し、ストレージノードへの新しいセキュアな接続を確立します。

各ノード上のロードバランササービスは、クライアントトラフィックをストレージノードに転送する際に独立して動作します。重み付きのプロセスを使用すると、ロードバランササービスは、より多くの要求をより多くの CPU を使用可能なストレージノードにルーティングします。

推奨されるロードバランシングメカニズムは StorageGRID ロードバランササービスですが、代わりにサードパーティのロードバランサを統合することもできます。詳細については、ネットアップのアカウント担当者にお問い合わせいただくか、次のテクニカルレポートを参照してください。

"StorageGRID ロードバランサオプション"

ゲートウェイノード上の別の Connection Load Balancer （ CLB ）サービスは廃止され、FabricPool での使用は推奨されなくなりました。

StorageGRID ロードバランシングのベストプラクティスを参照してください

一般的なベストプラクティスとして、 StorageGRID システムの各サイトにロードバランササービスを使用するノードが 2 つ以上必要です。たとえば、サイトには管理ノードとゲートウェイノードの両方、または管理ノードが2つ含まれている場合があります。SG100 または SG100 サービスアプライアンス、ベアメタルノード、仮想マシン（ VM ）ベースのノードのいずれを使用しているかに関係なく、各ロードバランシングノードに適切なネットワーク、ハードウェア、または仮想化インフラがあることを確認します。

StorageGRID ロードバランサエンドポイントを設定して、ゲートウェイノードと管理ノードが FabricPool の受信要求と送信要求に使用するポートを定義する必要があります。

ロードバランサエンドポイント証明書のベストプラクティス

FabricPool で使用するロードバランサエンドポイントを作成する際には、プロトコルとしてHTTPSを使用する必要があります。その後、公開された信頼された証明書またはプライベート認証局（CA）によって署名された証明書をアップロードするか、自己署名証明書を生成できます。この証明書は、 ONTAP が StorageGRID で認証することを許可します。

ベストプラクティスとして、 CA サーバ証明書を使用して接続を保護することを推奨します。CA によって署名された証明書は、無停止でローテーションできます。

ロードバランサエンドポイントで使用する CA 証明書を要求する場合は、証明書のドメイン名が、そのロードバランサエンドポイント用に ONTAP に入力するサーバ名と一致していることを確認してください。可能であれば、ワイルドカード（ * ）を使用して仮想ホスト形式の URL を許可します。例：

```
*.s3.storagegrid.company.com
```

StorageGRID を FabricPool クラウド階層として追加する場合は、 ONTAP クラスタにも同じ証明書をインストールする必要があります。また、ルート証明書と下位の認証局（ CA ）証明書もインストールする必要があります。

StorageGRID では、さまざまな目的でサーバ証明書が使用されます。ロードバランササービスに接続する場合は、Object Storage APIサービスエンドポイントのサーバ証明書をアップロードする必要はありません。

ロードバランシングエンドポイントのサーバ証明書の詳細を確認するには、次の手順を実行します。

- "負荷分散の管理"
- "サーバ証明書のセキュリティ強化ガイドライン"

ハイアベイラビリティグループのベストプラクティス

StorageGRID をFabricPool クラウド階層として接続する前に、StorageGRID グリッドマネージャを使用してハイアベイラビリティ（HA）グループを設定します。

ハイアベイラビリティ（**HA**）グループとは

FabricPool データの管理に常にロードバランササービスを使用できるようにするには、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 1 つのエンティティ（ハイアベイラビリティ（ HA ）グループと呼ばれます）にグループ化します。HA グループのアクティブノードで障害が発生した場合、グループ内の別のノードがワークロードの管理を続行できます。

各 HA グループは、関連付けられたノード上の共有サービスへの可用性の高いアクセスを提供します。たとえば、すべての管理ノードで構成されるHAグループは、一部の管理ノード管理サービスとロードバランササービスへの高可用性アクセスを提供します。ゲートウェイノードのみ、または管理ノードとゲートウェイノードの両方で構成されるHAグループは、共有ロードバランササービスへの可用性の高いアクセスを提供します。

HAグループを作成するときは、グリッドネットワーク（eth0）またはクライアントネットワーク（eth2）に属するネットワークインターフェイスを選択します。HAグループ内のすべてのインターフェイスは、同じネットワークサブネット内に存在する必要があります。

HAグループは、グループ内のアクティブインターフェイスに追加された仮想IPアドレスを1つ以上維持します。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、仮想IPアドレスは別のインターフェイスに移動します。このフェイルオーバープロセスにかかる時間は通常数秒です。クライアントアプリケーションへの影響はほとんどなく、通常の再試行で処理を続行できます。

ロードバランシングノードのHAグループを設定すると、FabricPool はそのHAグループの仮想IPアドレスに接続します。

ハイアベイラビリティ（ **HA** ）グループのベストプラクティス

FabricPool 用の StorageGRID HA グループを作成する際のベストプラクティスは、次のワークロードによって異なります。

- プライマリワークロードのデータで FabricPool を使用する場合は、データの取得の中断を回避するために、ロードバランシングノードを少なくとも 2 つ含む HA グループを作成する必要があります。
- FabricPool の snapshot-only のボリューム階層化ポリシーまたは非プライマリのローカルのパフォーマンス階層（ディザスタリカバリ先や NetApp SnapMirror ® デスティネーションなど）を使用する予定の場合は、 1 つのノードだけで HA グループを設定できます。

ここでは、アクティブ / バックアップ HA の HA グループの設定（一方のノードがアクティブでもう一方のノードがバックアップ）について説明します。ただし、 DNS ラウンドロビンまたはアクティブ / アクティブ HA を使用することもできます。これらの他の HA 構成のメリットについては、を参照してください "HA グループの設定オプション"。

StorageGRID IPアドレス用の**DNS**サーバを設定する

ハイアベイラビリティグループとロードバランサエンドポイントを設定したら、 ONTAP システムのドメインネームシステム（ DNS ）に、 FabricPool が接続に使用する IP アドレスに StorageGRID サーバ名（完全修飾ドメイン名）を関連付けるレコードが含まれていることを確認する必要があります。

DNS レコードに入力する IP アドレスは、負荷分散ノードの HA グループを使用しているかどうかによって異なります。

- HA グループを設定している場合、 FabricPool 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、 FabricPool は、任意のゲートウェイノードまたは管理ノードの IP アドレスを使用して StorageGRID ロードバランササービスに接続できます。

また、 DNS レコードが、ワイルドカード名を含む、必要なすべてのエンドポイントドメイン名を参照していることを確認する必要があります。

FabricPool のハイアベイラビリティ（HA）グループの作成

FabricPool で使用するように StorageGRID を設定する場合は、必要に応じて 1 つ以上のハイアベイラビリティ（ HA ）グループを作成できます。HA グループは、管理ノード、ゲートウェイノード、またはその両方の 1 つ以上のネットワークインターフェイスで構成されます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限が必要です。

このタスクについて

各 HA グループは、仮想 IP アドレス（ VIP ）を使用して、関連付けられたノード上の共有サービスへの可用性の高いアクセスを提供します。

詳細については、を参照してください。を参照してください "ハイアベイラビリティグループの管理"。

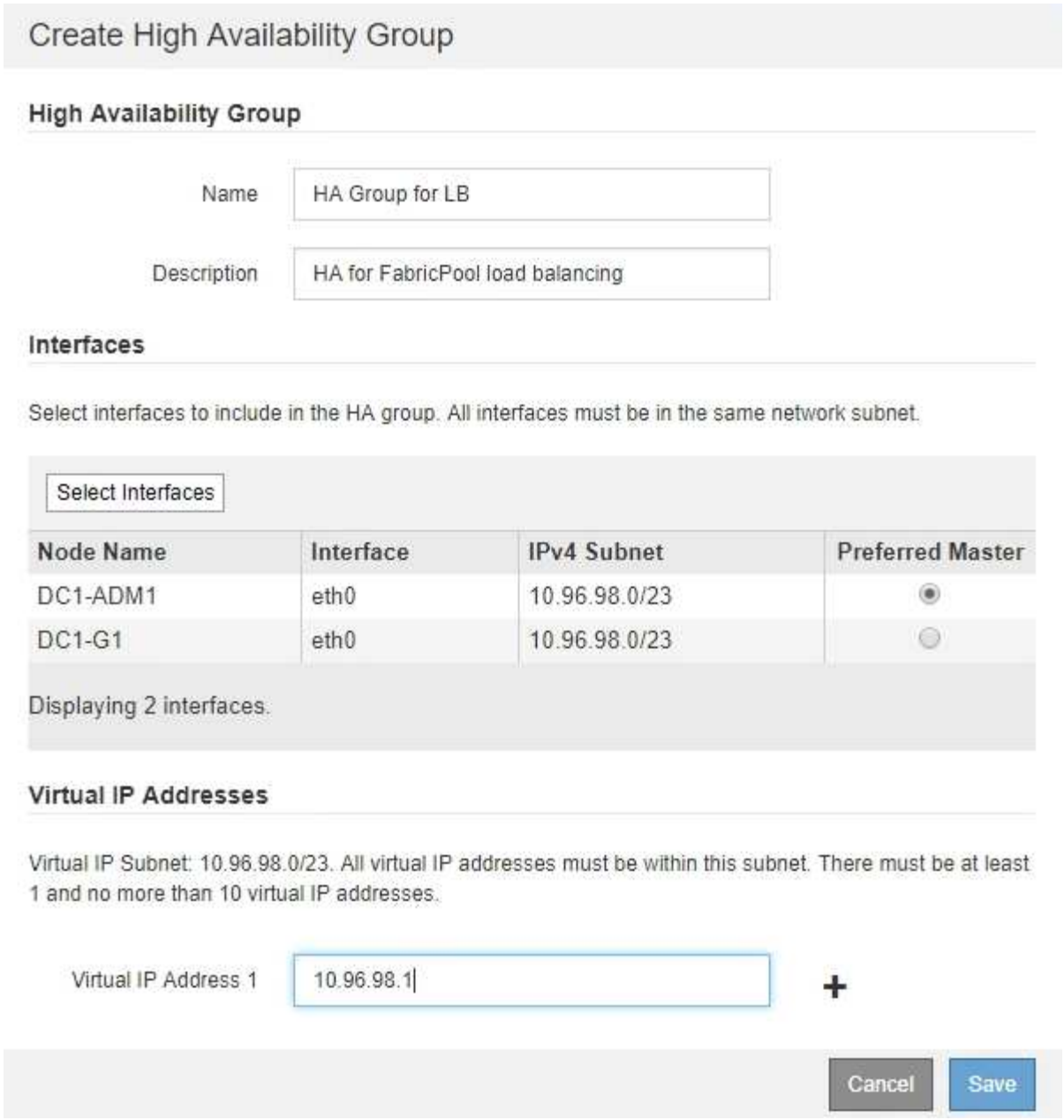
手順

1. * Configuration > Network Settings > High Availability Groups *を選択します。
2. ネットワークインターフェイスを1つ以上選択してください。ネットワークインターフェイスは、グリッドネットワーク（eth0）またはクライアントネットワーク（eth2）上の同じサブネットに属している必要があります。
3. 1つのノードを優先マスターに割り当てます。

   優先マスターは、障害が発生してVIPアドレスがバックアップインターフェイスに再割り当てされない限り、アクティブインターフェイスです。

4. HAグループのIPv4アドレスを10個まで入力します。

   すべてのメンバーインターフェイスで共有するIPv4サブネット内のアドレスを指定する必要があります。



FabricPool のロードバランサエンドポイントの作成

FabricPool で使用するStorageGRID を設定する場合は、ロードバランサエンドポイントを設定し、ロードバランサエンドポイント証明書をアップロードします。この証明書は、ONTAP とStorageGRID 間の接続を保護するために使用されます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- Root Access 権限が必要です。
- 次のファイルが必要です。
  - Server Certificate ：カスタムサーバ証明書ファイル。
  - Server Certificate Private Key ：カスタムサーバ証明書の秘密鍵ファイル。

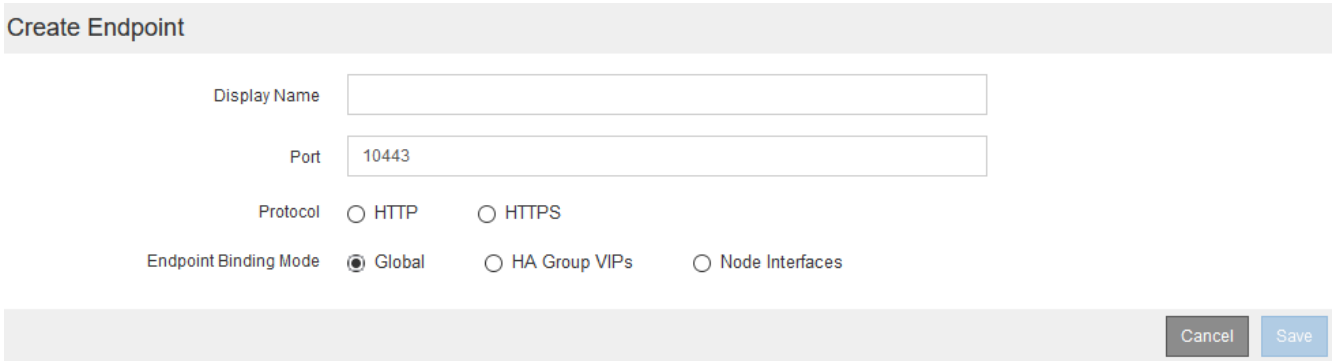
◦ CA Bundle：各中間発行認証局（CA）の証明書を含む単一のファイル。このファイルには、 PEM でエンコードされた各 CA 証明書ファイルが、証明書チェーンの順序で連結して含まれている必要があります。

このタスクについて

このタスクの詳細については、を参照してください "ロードバランサエンドポイントの設定"。

手順

1. [* Configuration > Network Settings > Load Balancer Endpoints *]を選択します。



2. [エンドポイントの追加]を選択します。
3. 次の情報を入力します。

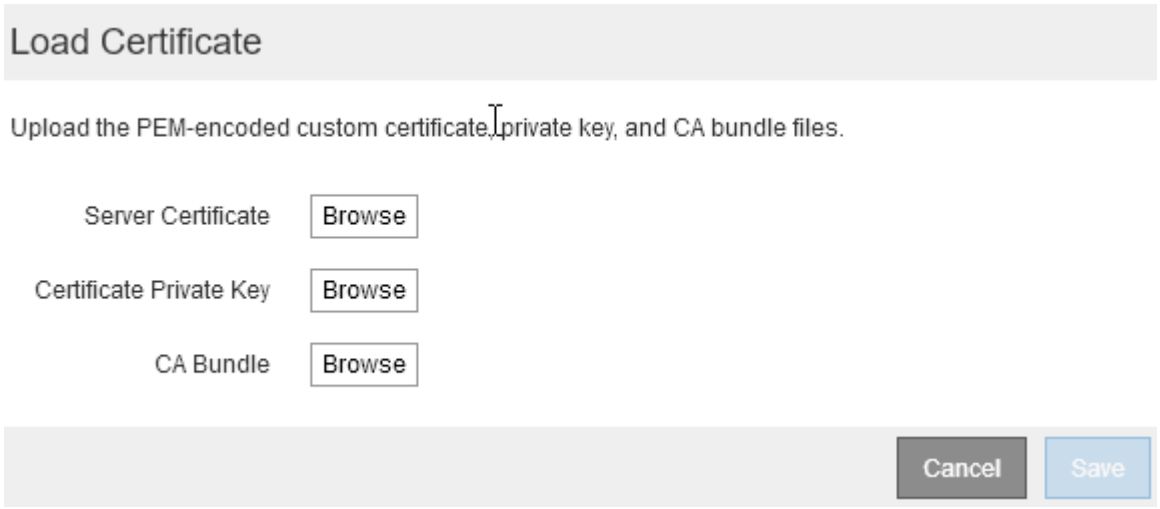
フィールド	説明
表示名	エンドポイントのわかりやすい名前
ポート	ロードバランシングに使用する StorageGRID ポート。このフィールドのデフォルト値は 10433 ですが、未使用の外部ポートを入力することもできます。80 または 443 と入力すると、エンドポイントは管理ノードで予約されているため、ゲートウェイノードにのみ設定されます。 • 注： * 他のグリッドサービスで使用されているポートは使用できません。内部および外部の通信に使用されるポートのリストを参照してください。 "ネットワークポートのリファレンス" StorageGRID を FabricPool クラウド階層として接続する場合は、 ONTAP に同じポート番号を指定する必要があります。
プロトコル	は* HTTPS *にする必要があります。

フィールド	説明
エンドポイントバインドモード	[グローバル * （ Global * ）] 設定を使用するか（推奨）、このエンドポイントのアクセス性を次のいずれかに制限します。 • 特定のハイアベイラビリティ（ HA ）仮想 IP アドレス（ VIP ）。このオプションは、ワークロードの分離レベルを大幅に高める必要がある場合にのみ使用してください。 • 特定のノードの特定のネットワークインターフェイス。

4. [保存（ Save ）] を選択します。

   [Edit Endpoint]ダイアログボックスが表示されます。

5. 「* Endpoint Service Type 」で「 S3 *」を選択します。
6. [証明書のアップロード*(推奨)]を選択し、サーバ証明書、証明書の秘密鍵、およびCAバンドルを参照します。



7. [保存（ Save ）] を選択します。

FabricPool のテナントアカウントの作成

Grid Manager で FabricPool 用のテナントアカウントを作成する必要があります。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

このタスクについて

テナントアカウントを使用すると、クライアントアプリケーションで StorageGRID に対してオブジェクトの格納や読み出しを行うことができます。各テナントアカウントには、専用のアカウント ID 、許可されたグループとユーザ、バケット、オブジェクトがあります。

複数の ONTAP クラスタに同じテナントアカウントを使用できます。また、必要に応じて、 ONTAP クラスタごとに専用のテナントアカウントを作成することもできます。

> この手順は、 Grid Manager にシングルサインオン（ SSO ）が設定されていることを前提としています。SSOを使用していない場合は、の手順を使用します "StorageGRID がSSOを使用していない場合のテナントアカウントの作成"。

手順

1. 「* tenants *」を選択します
2. 「 * Create * 」を選択します。
3. FabricPool テナントアカウントの表示名を入力します。
4. S3 を選択します。
5. プラットフォームサービスの使用を有効にするには、[プラットフォームサービスを許可]チェックボックスをオンのままにします。

   プラットフォームサービスが有効になっている場合、テナントは外部サービスにアクセスする CloudMirror レプリケーションなどの機能を使用できます。
6. Storage Quota *フィールドは空白のままにします。
7. [* Root Access Group]フィールドで、テナントに対する最初のRoot Access権限を持つ既存のフェデレーテッドグループをGrid Managerから選択します。
8. [保存（ Save ）] を選択します。

S3バケットを作成してアクセスキーを取得する

FabricPool ワークロードで StorageGRID を使用する前に、 FabricPool データ用の S3 バケットを作成する必要があります。また、 FabricPool に使用するテナントアカウントのアクセスキーとシークレットアクセスキーを取得する必要があります。

必要なもの

- FabricPool で使用するテナントアカウントを作成しておく必要があります。

このタスクについて

ここでは、 StorageGRID テナントマネージャを使用してバケットを作成し、アクセスキーを取得する方法について説明します。テナント管理 API または StorageGRID S3 REST API を使用してこれらのタスクを実行することもできます。

詳細については、以下をご覧ください。

- "テナントアカウントを使用する"
- "S3 を使用する"

手順

1. Tenant Manager にサインインします。

   次のいずれかを実行できます。

- Grid Manager の Tenant Accounts ページで、テナントの * Sign In * リンクを選択し、クレデンシャルを入力します。
- Web ブラウザでテナントアカウントの URL を入力し、クレデンシャルを入力します。

2. FabricPool データ用の S3 バケットを作成する。

   使用する ONTAP クラスタごとに一意のバケットを作成する必要があります。

   a. ストレージ（ S3 ） * > * バケット * を選択します。
   b. [* バケットの作成 *] を選択します。
   c. FabricPool で使用する StorageGRID バケットの名前を入力します。例： `fabricpool-bucket`。

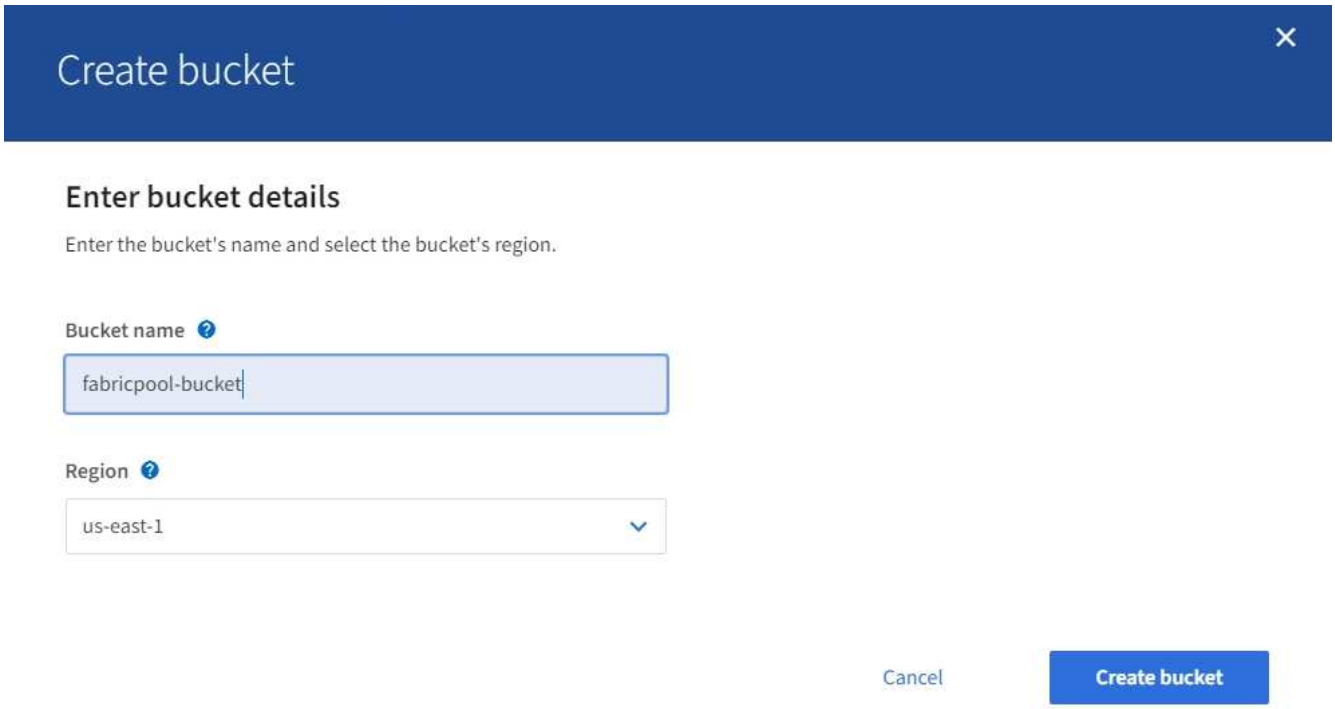
      バケットの作成後にバケット名を変更することはできません。

      バケット名は次のルールを満たす必要があります。

      - StorageGRID システム全体で（テナントアカウント内だけではなく）一意である必要があります。
      - DNS に準拠している必要があります。
      - 3 文字以上 63 文字以下にする必要があります。
      - 1 つ以上のラベルを連続して指定できます。隣接するラベルはピリオドで区切ります。各ラベルの先頭と末尾の文字は小文字のアルファベットか数字にする必要があり、使用できる文字は小文字のアルファベット、数字、ハイフンのみです。
      - テキスト形式の IP アドレスのようにはできません。
      - 仮想ホスト形式の要求でピリオドを使用しないでください。ピリオドを使用すると、サーバワイルドカード証明書の検証で原因 の問題が発生します。

   d. このバケットのリージョンを選択します。

      デフォルトでは、すべてのバケットがに作成されます `us-east-1` リージョン：



a. [* バケットの作成 *] を選択します。

3. アクセスキーとシークレットアクセスキーを作成します。

a. 「 * storage （ S3 ） * > * My access keys * 」を選択します。

b. 「 * キーの作成 * 」を選択します。

c. [アクセスキーの作成 *] を選択します。

d. アクセスキー ID とシークレットアクセスキーを安全な場所にコピーするか、「 * Download.csv * 」を選択してアクセスキー ID とシークレットアクセスキーを含むスプレッドシートファイルを保存します。

これらの値は、 ONTAP で StorageGRID を FabricPool クラウド階層として設定するときに入力します。

今後新しいアクセスキーとシークレットアクセスキー StorageGRID を作成する場合は、 ONTAP がデータの格納と読み出しを中断なく行えるように、 ONTAP で対応する値をただちに更新する必要があります。

StorageGRID の情報ライフサイクル管理とFabricPool のデータを使用する

FabricPool を使用して StorageGRID にデータを階層化する場合は、 StorageGRID 情報ライフサイクル管理（ ILM ）ルールの作成要件と、 FabricPool データを管理するための ILM ポリシーの作成要件を理解しておく必要があります。FabricPool データに適用される ILM ルールがシステム停止を伴わないようにする必要があります。

FabricPool は、 StorageGRID の ILM ルールやポリシーを認識しません。StorageGRID の ILM ポリシーの設定ミスが原因でデータが失われる可能性があります。

詳細については、以下をご覧ください。 "ILM を使用してオブジェクトを管理する"

FabricPool データに関する**ILM**のガイドライン

以下のガイドラインを確認し、 ILM ルールと ILM ポリシーが FabricPool データとビジネス要件に適していることを確認してください。すでに StorageGRID ILM を使用している場合は、次のガイドラインに従って、アクティブな ILM ポリシーの更新が必要になることがあります。

- レプリケーションルールとイレイジャーコーディングルールを任意に組み合わせて、クラウド階層のデータを保護できます。

  コスト効率に優れたデータ保護を実現するために、サイト内で 2+1 のイレイジャーコーディングを使用することを推奨します。イレイジャーコーディングは、レプリケーションよりも多くのCPUを使用しますが、ストレージ容量は大幅に少なくなります。4+1スキームと6+1スキームは2+1よりも少ない容量を使用しますが、グリッド拡張時にストレージノードを追加する場合にスループットが低下し、柔軟性が低下します。

- FabricPool データに適用するルールは、イレイジャーコーディングを使用するか、少なくとも 2 つのレプリケートコピーを作成する必要があります。

  ある期間にレプリケートコピーを 1 つしか作成しない ILM ルールには、データが永続的に失われるリスクがあります。オブジェクトのレプリケートコピーが 1 つしかない場合、ストレージノードに障害が発生したり、重大なエラーが発生すると、そのオブジェクトは失われます。また、アップグレードなどのメンテナンス作業中は、オブジェクトへのアクセスが一時的に失われます。

- FabricPool クラウド階層のデータが期限切れになる、または削除される ILM ルールは使用しないでください。StorageGRID ILM によって FabricPool オブジェクトが削除されないように、各 ILM ルールの保持期間を「 forever 」に設定します。
- FabricPool クラウド階層のデータをバケットから別の場所に移動するルールは作成しないでください。ILMルールを使用して、アーカイブノードを使用してFabricPool データをテープにアーカイブしたり、クラウドストレージプールを使用してFabricPool データをGlacierに移動したりすることはできません。

  クラウドストレージプールターゲットからオブジェクトを読み出すレイテンシが増加しているため、 FabricPool でクラウドストレージプールを使用することはサポートされていません。

- ONTAP 9.8 以降では、オプションでオブジェクトタグを作成して階層化データを分類およびソートし、管理を容易にすることができます。たとえば、タグを設定できるのは、 StorageGRID に接続されている FabricPool ボリュームのみです。次に、 StorageGRID で ILM ルールを作成する際に、高度なフィルタ「オブジェクトタグ」を使用してこのデータを選択し、配置します。

FabricPool データ用の **ILM** ポリシーの例

以下に記載するシンプルなポリシーの例をベースに、独自の ILM ルールとポリシーを作成します。

この例では、コロラド州デンバーの 1 つのデータセンターに 4 つのストレージノードがある StorageGRID システムの ILM ルールと ILM ポリシーを設計していることを前提としています。この例のFabricPool データは、というバケットを使用しています `fabricpool-bucket`。

> 以下の ILM ルールとポリシーは一例にすぎません。ILM ルールを設定する方法は多数あります。新しいポリシーをアクティブ化する前に、ドラフトポリシーをシミュレートして、コンテンツの損失を防ぐためにドラフトポリシーが想定どおりに機能することを確認してください。
>
> 詳細については、以下をご覧ください。 "ILM を使用してオブジェクトを管理する"

手順

1. *Den という名前のストレージプールを作成します。Denver サイトを選択します。
2. 2 plus 1 * という名前のイレイジャーコーディングプロファイルを作成します。2+1 イレイジャーコーディングスキームと *Den * ストレージプールを選択します。
3. のデータにのみ適用されるILMルールを作成します `fabricpool-bucket`。次のルール例では、イレイジャーコーディングコピーを作成します。

ルール定義	値の例
ルール名	FabricPool データ用の 2+1 のイレイジャーコーディング
バケット名	`fabricpool-bucket` FabricPool テナントアカウントでフィルタリングすることもできます。
高度なフィルタリング	オブジェクトサイズ（ MB ）が 0.2 MB を超えています。 • 注： * FabricPool は 4MB のオブジェクトのみを書き込みますが、このルールではイレイジャーコーディングを使用するため、オブジェクトサイズフィルタを追加する必要があります。
参照時間	取り込み時間
配置	0 日目のストアから永遠に
を入力します	イレイジャーコーディング
場所	デン (2 プラス 1)
取り込み動作	中間（ Balanced ）

4. 最初のルールに一致しないオブジェクトのレプリケートコピーを 2 つ作成する ILM ルールを作成します。基本フィルタ（テナントアカウントまたはバケット名）や高度なフィルタは選択しないでください。

ルール定義	値の例
ルール名	2 つのレプリケートコピー
バケット名	_ なし _
高度なフィルタリング	_ なし _
参照時間	取り込み時間
配置	0 日目のストアから永遠に
を入力します	レプリケート
場所	デン
コピー	2.
取り込み動作	中間（ Balanced ）

5. ドラフトの ILM ポリシーを作成して 2 つのルールを選択レプリケーションルールではフィルタを使用しないため、ポリシーのデフォルト（最後の）ルールを使用できます。
6. テストオブジェクトをグリッドに取り込みます。
7. ポリシーをテストオブジェクトでシミュレートして動作を確認します。
8. ポリシーをアクティブ化する。

このポリシーをアクティブ化すると、 StorageGRID はオブジェクトデータを次のように配置します。

- のFabricPool から階層化されたデータ `fabricpool-bucket` 2+1イレイジャーコーディングスキームを使用してイレイジャーコーディングされます。2 つのデータフラグメントと 1 つのパリティフラグメントが 3 つの異なるストレージノードに配置されます。
- 他のすべてのバケット内のオブジェクトがレプリケートされます。2 つのコピーが作成され、 2 つの異なるストレージノードに配置されます。
- イレイジャーコーディングコピーとレプリケートコピーは、 S3 クライアントによって削除されるまで StorageGRID に保持されます。StorageGRID ILM によってこれらの項目が削除されることはありません。

FabricPool のトラフィック分類ポリシーを作成する

必要に応じて、 StorageGRID トラフィック分類ポリシーを設計して、 FabricPool ワークロードのサービス品質を最適化できます。

必要なもの

- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。

- Root Access 権限が必要です。

このタスクについて

FabricPool のトラフィック分類ポリシーを作成する場合のベストプラクティスは、次のようにワークロードによって異なります。

- FabricPool のプライマリワークロードのデータを StorageGRID に階層化する場合は、 FabricPool ワークロードの帯域幅が大半であることを確認する必要があります。トラフィック分類ポリシーを作成して、他のすべてのワークロードを制限できます。

  一般に、 FabricPool の読み取り処理は、書き込み処理よりも優先順位を付けることが重要です。

  たとえば、他の S3 クライアントがこの StorageGRID システムを使用している場合は、トラフィック分類ポリシーを作成する必要があります。他のバケット、テナント、 IP サブネット、またはロードバランサエンドポイントのネットワークトラフィックを制限できます。

- 原則として、どの FabricPool ワークロードにも QoS 制限を課すべきではなく、他のワークロードに限定するだけです。
- 他のワークロードで設定されている制限は、ワークロードの動作が不明な場合に適用される範囲内である必要があります。また、グリッドのサイジングと機能、および想定される利用率に応じて、制限が適用されます。

詳細については、以下をご覧ください。 "トラフィック分類ポリシーの管理"

手順

1. [* Configuration **]>[** Network Settings **]>[** Traffic Classification]を選択します。
2. 名前と概要 を入力します。
3. [一致ルール] セクションで、少なくとも 1 つのルールを作成します。
   a. 「 * Create * 」を選択します。
   b. [* Endpoint] を選択し、 FabricPool 用に作成したロードバランサエンドポイントを選択します。

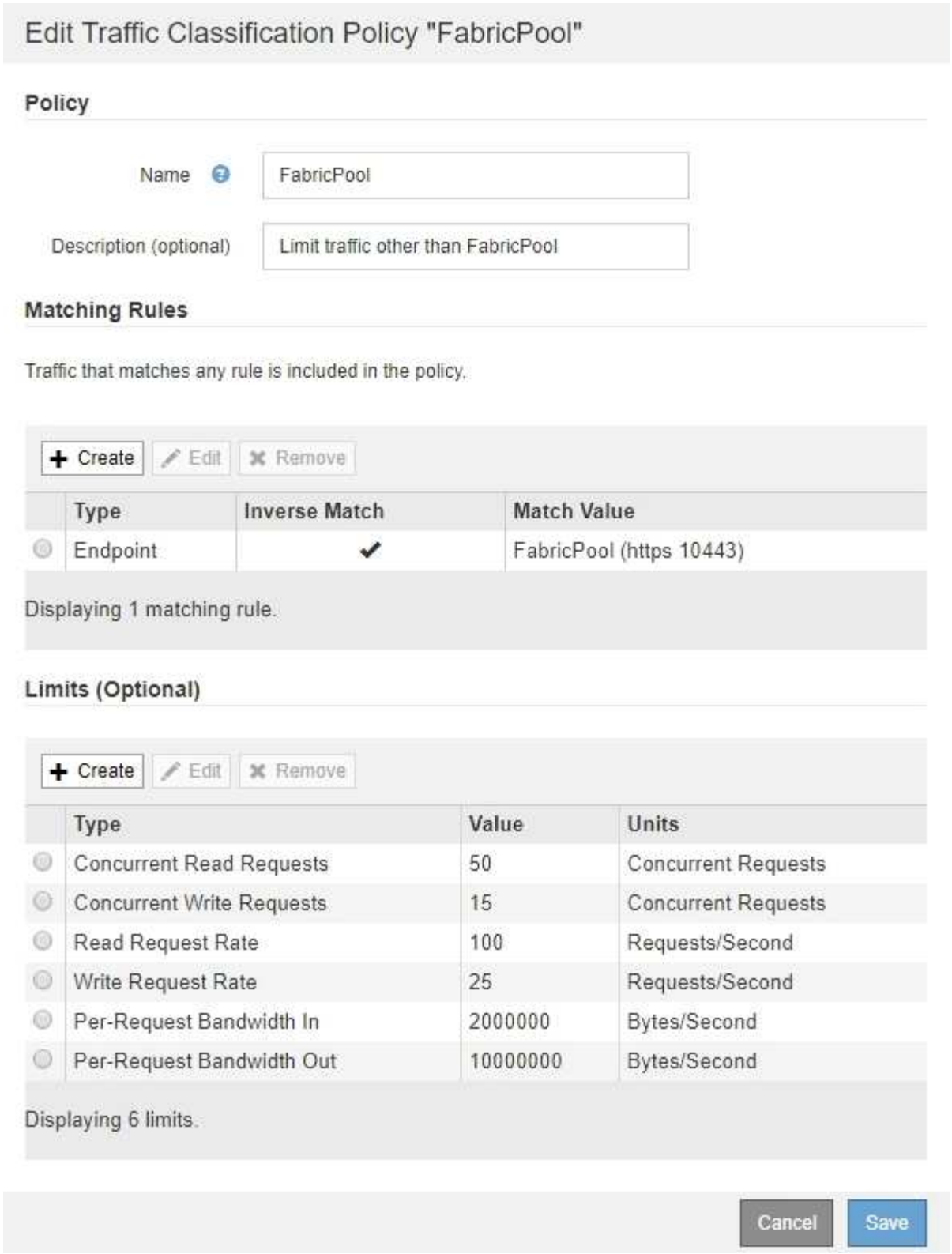
      FabricPool テナントアカウントまたはバケットを選択することもできます。

   c. このトラフィックポリシーで他のエンドポイントのトラフィックを制限する場合は、 [* 逆一致 * （ Inverse match * ）] を選択します。
4. 必要に応じて、 1 つ以上の制限を作成します。

   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、トラフィックの傾向を把握できるようにメトリックが収集されます。

   a. 「 * Create * 」を選択します。
   b. 制限するトラフィックのタイプと適用する制限を選択します。

      次に、FabricPool トラフィック分類の例では、制限できるネットワークトラフィックのタイプと、選択できる値のタイプを示します。実際のポリシーのトラフィックタイプと値は、固有の要件に基づいています。



5. トラフィック分類ポリシーを作成した後、ポリシーを選択し、 [*Metrics] を選択して、ポリシーがトラフィックを想定どおりに制限しているかどうかを確認します。

StorageGRID および FabricPool に関するその他のベストプラクティスです

FabricPool で使用する StorageGRID システムを設定する場合は、データの保存方法に影響する可能性があるグローバルオプションを設定しないでください。

オブジェクトの暗号化

StorageGRID の設定時に、他のStorageGRID クライアント（* Configuration > System Settings > Grid Options *）でデータ暗号化が必要な場合は、グローバル*格納オブジェクト暗号化*設定をオプションで有効にできます。FabricPool から StorageGRID に階層化されたデータはすでに暗号化されているため、StorageGRID 設定を有効にする必要はありません。クライアント側の暗号化キーは ONTAP が所有します。

オブジェクトの圧縮

StorageGRID を設定する場合は、グローバル*保存オブジェクトの圧縮*設定（構成>*システム設定*>*グリッドオプション*）を有効にしないでください。FabricPool から StorageGRID に階層化されたデータはすでに圧縮されています。「格納オブジェクトの圧縮」を有効にしても、オブジェクトのサイズはこれ以上縮小されません。

整合性レベル

FabricPool バケットの場合、推奨されるバケットの整合性レベルは* Read-after-new-write で、新しいバケットのデフォルトの設定です。**FabricPool** バケットを編集して available *やその他の整合性レベルを使用しないでください。

FabricPool による階層化

StorageGRID ノードが NetApp AFF システムから割り当てられたストレージを使用している場合は、ボリュームで FabricPool 階層化ポリシーが有効になっていないことを確認してください。たとえば、 StorageGRID ノードが VMware ホストで実行されている場合は、 StorageGRID ノードのデータストアの作成元ボリュームで FabricPool 階層化ポリシーが有効になっていないことを確認します。StorageGRID ノードで使用するボリュームで FabricPool による階層化を無効にすることで、トラブルシューティングとストレージの処理がシンプルになります。

StorageGRID を使用して StorageGRID に関連するデータを FabricPool 自体に階層化しないでください。StorageGRID データを StorageGRID に階層化すると、トラブルシューティングと運用がより複雑になります。

著作権に関する情報

商標に関する情報