



StorageGRID の管理

StorageGRID 11.5

NetApp
April 11, 2024

目次

StorageGRID の管理	1
StorageGRID システムの管理	1
StorageGRID への管理者アクセスの制御	30
キー管理サーバを設定しています	75
テナントの管理	104
S3およびSwiftクライアント接続の設定	127
StorageGRID ネットワークと接続の管理	160
AutoSupport を設定しています	191
ストレージノードの管理	207
管理ノードの管理	231
アーカイブノードの管理	255
StorageGRID へのデータの移行	278

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。

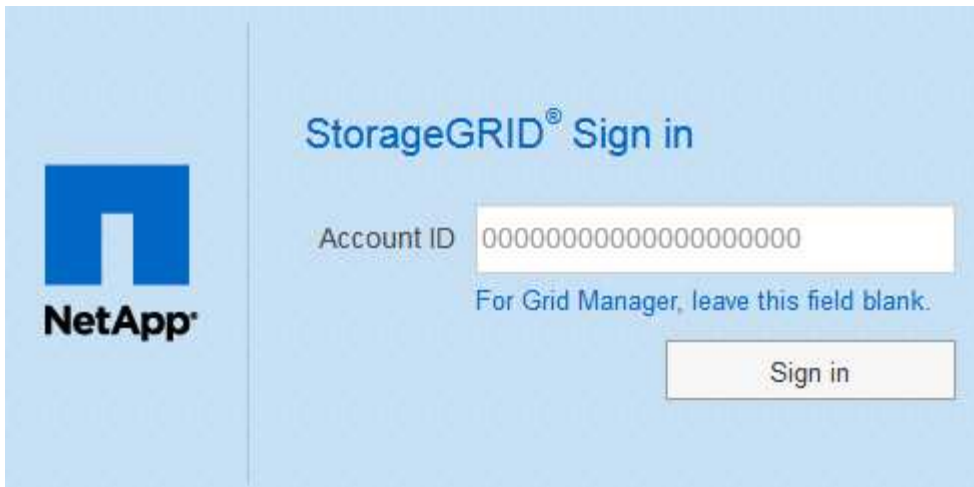
HTTPS (443) の標準ポート以外のポートでGrid Managerにアクセスする必要がある場合は、次のように入力します `FQDN_or_Admin_Node_IP`は完全修飾ドメイン名またはIPアドレス、`port`はポート番号です。

`https://FQDN_or_Admin_Node_IP:port/`

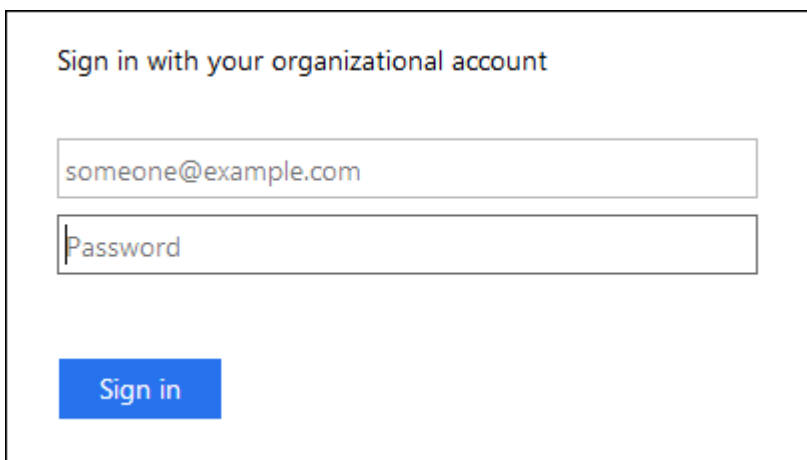
3. セキュリティアラートが表示された場合は、ブラウザのインストールウィザードを使用して証明書をインストールします。
4. Grid Manager にサインインします。
 - StorageGRID システムでシングルサインオン (SSO) が使用されていない場合は、次の手順を実行します。
 - i. Grid Manager のユーザ名とパスワードを入力します。
 - ii. [* サインイン *] をクリックします。



- 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：



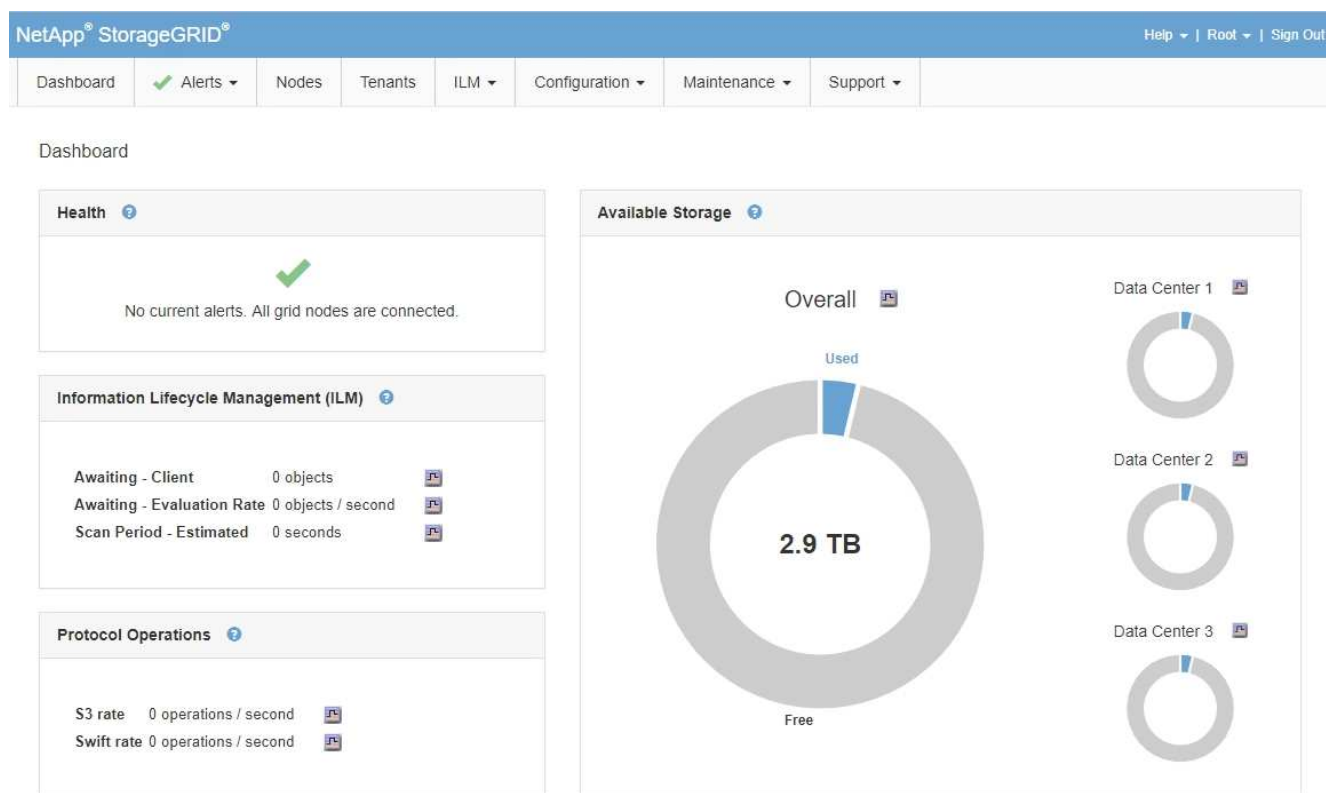
° StorageGRID システムで SSO が有効になっており、Grid Manager またはテナントアカウントに以前にアクセスしたことがある場合は、次の手順を実行します。

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	<ol style="list-style-type: none"> 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。 Grid Manager のユーザ名とパスワードを入力します。 [* 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	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> 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"](#)

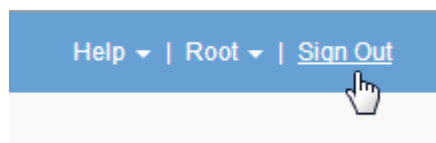
["トラブルシューティングを監視します"](#)

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	<p>管理ノードからサインアウトされます。</p> <p>Grid Manager のサインインページが表示されます。</p> <ul style="list-style-type: none"> 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	<p>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。</p> <ul style="list-style-type: none"> 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、`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

NetApp® StorageGRID® Help | Root | Sign Out

Dashboard Alerts Nodes Tenants ILM Configuration Maintenance Support

Grid Passwords

Change the provisioning passphrase and other passwords for your StorageGRID system.

Change Provisioning Passphrase

The provisioning passphrase is required for any installation, expansion, or maintenance procedure that makes changes to the grid topology. This passphrase is also required to download backups of the grid topology information and encryption keys for the StorageGRID system. After changing the provisioning passphrase, you must download a new Recovery Package.

Current Provisioning Passphrase

New Provisioning Passphrase

Confirm New Provisioning Passphrase

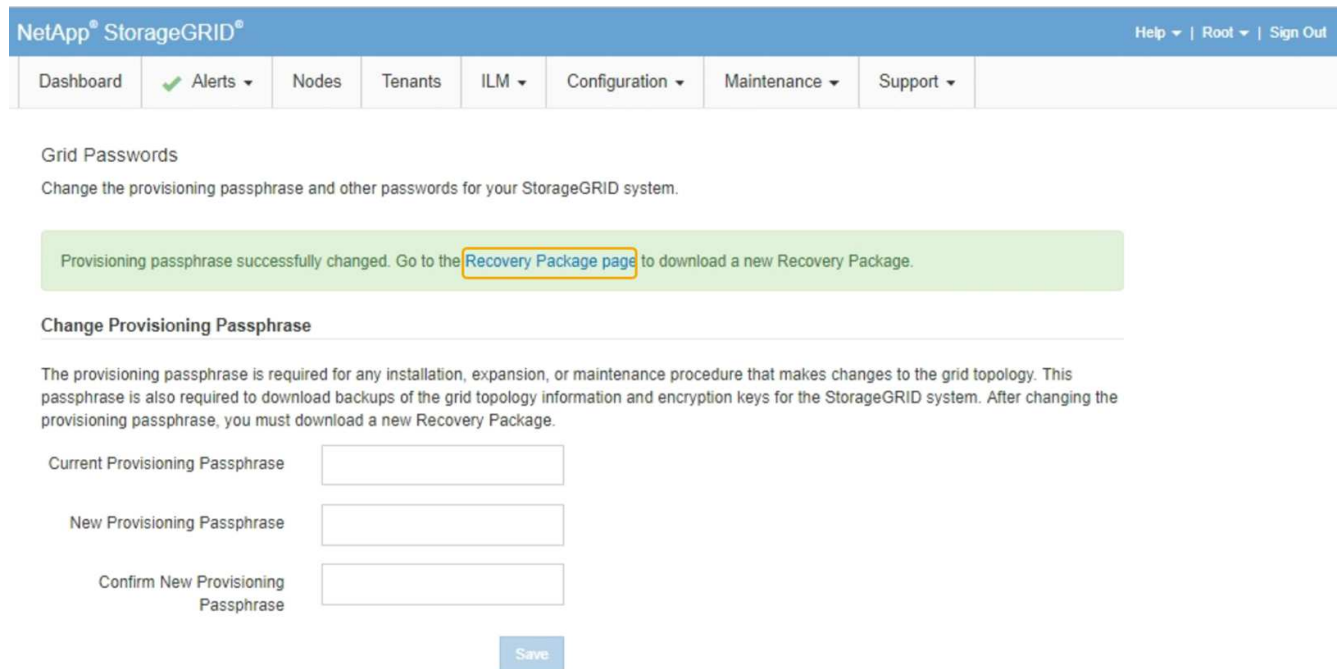
2. 現在のプロビジョニングパスフレーズを入力します。
3. 新しいリンフレーズを入力してください。パスフレーズには8文字以上32文字以下の文字列を含める必要があります。パスフレーズでは大文字と小文字が区別されます。



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. 新しいパスワードをもう一度入力し、*保存*をクリックします。

プロビジョニングパスワード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ワードを入力します。



プロビジョニングパスワードを変更したら、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。



Display Options

Updated: 2017-03-09 20:36:53 MST

Current Sender	ADMIN-DC1-ADM1
Preferred Sender	ADMIN-DC1-ADM1
GUI Inactivity Timeout	900
Notification Suppress All	<input type="checkbox"/>

Apply Changes

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。

Dashboard



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。

groups Operations on groups

GET /grid/groups Lists Grid Administrator Groups

Parameters Try it out

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

Responses Response content type application/json

Code	Description
200	successfully retrieved

Example Value | Model

```
{
  "responseTime": "2021-03-29T14:22:19.673Z",
  "status": "success",
  "apiVersion": "3.3",
  "deprecated": false,
  "data": [
    {
      "displayName": "Developers",
```

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 のバージョン管理

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

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

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

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

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

StorageGRID ソフトウェアを初めてインストールした時点では、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 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

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=fZHRT0MwFIZfhh...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=$SAMPLPASSWORD&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=fZHRTomwFIZfhh...UJikvo
77sXPw%3D%3D&RelayState=12345&client-request-id=00000000-0000-0000-
ee02-0080000000de
Set-Cookie: MSISAuth=AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY=; path=/adfs;
HttpOnly; Secure
Date: Tue, 06 Nov 2018 16:55:05 GMT
```

- g. 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。


```
{
  "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%3D",
  "responseTime": "2018-11-20T22:20:30.839Z",
  "status": "success"
}
```

2. ログアウト URL を保存します。

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

3. 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: MSISignoutProtocol=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。

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 をサーバに対して認証し、パスワードだけでなく、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	<p>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。</p> <ul style="list-style-type: none"> 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、OpenLD AP、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 アプリケーション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。 <ul style="list-style-type: none"> • 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	<p>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。</p> <p>*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。</p>	設定>*ネットワーク設定*>*ロードバランサエンドポイント*	<ul style="list-style-type: none"> • "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 <p>"StorageGRID for FabricPool を設定します"</p>
管理インターフェイスのサーバ証明書	サーバ	<p>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。</p> <p>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。</p> <p>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。</p>	構成>*ネットワーク設定*>*サーバー証明書*	<ul style="list-style-type: none"> • "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。	<ul style="list-style-type: none"> 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。	<ul style="list-style-type: none"> • 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	<p>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。</p> <ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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 ユーザの一意的な 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的な 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 グループの一意的な 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的な 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。



*グループの一意的な名前*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。



*ユーザーの一意的な名前*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。

LDAP service type

Select the type of LDAP service you want to configure.

Active Directory

OpenLDAP

Other

Configure LDAP server (All fields are required)

Hostname

my-active-directory.example.com

Port

389

Username

MyDomain\Administrator

Password

●●●●●●●●

Group Base DN

DC=storagegrid,DC=example,DC=com

User Base DN

DC=storagegrid,DC=example,DC=com

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。

Synchronize

StorageGRID periodically synchronizes federated groups and users from the configured LDAP server. Clicking the button below will immediately start the synchronization process against the saved LDAP server.

Synchronize

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。

Admin Groups

Add and manage local and federated user groups, allowing member users to sign in to the Grid Manager. Set group permissions to control access to specific pages and features.



Name	ID	Group Type	Access Mode
Flintstone	264083d0-23b5-3046-9bd4-88b7097731ab	Federated	Read-write
Simpson	cc8ad11f-68d0-f84a-af29-e7a6fcdc63a2	Federated	Read-only
ILM (read-only group)	88446141-9599-4543-b183-9c227ce7767a	Local	Read-only
API Developers	974b2faa-f9a1-4cfc-b364-914cdba2905f	Local	Read-write
ILM Admins (read-write)	a528c0c2-2417-4559-86ed-f0d2e31da820	Local	Read-write
Maintenance Users	7e3400ec-de8c-45a7-8bb8-e1496b362a8d	Local	Read-write

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。

Add Group

Create a new local group or import a group from the external identity source.

Group Type Local Federated

Display Name

Unique Name

Access Mode Read-write Read-only

Management Permissions

- | | |
|--|---|
| <input type="checkbox"/> Root Access | <input type="checkbox"/> Manage Alerts |
| <input type="checkbox"/> Acknowledge Alarms | <input type="checkbox"/> Grid Topology Page Configuration |
| <input type="checkbox"/> Other Grid Configuration | <input type="checkbox"/> Tenant Accounts |
| <input type="checkbox"/> Change Tenant Root Password | <input type="checkbox"/> Maintenance |
| <input type="checkbox"/> Metrics Query | <input type="checkbox"/> ILM |
| <input type="checkbox"/> Object Metadata Lookup | <input type="checkbox"/> Storage Appliance Administrator |

Cancel

Save

- [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。
- 「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。
- 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。
- *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のままにするには、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の仕組み

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

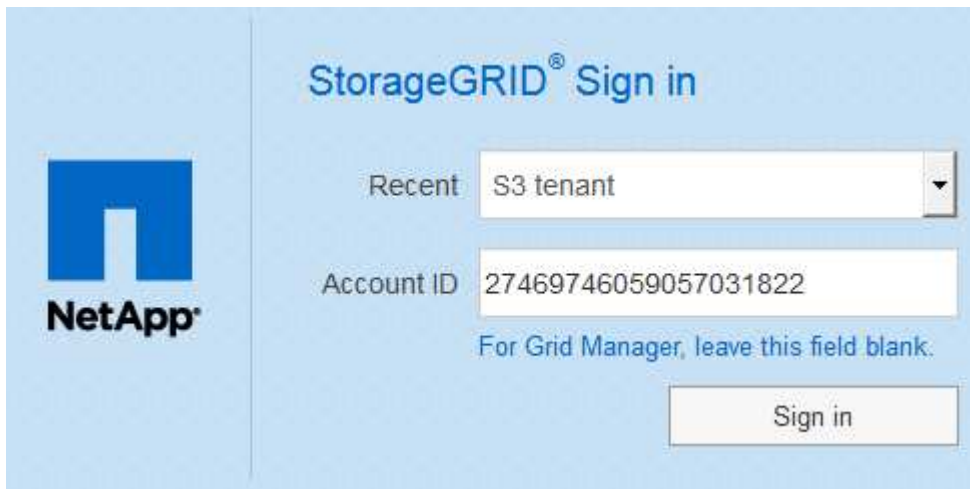
1. Web ブラウザで、StorageGRID 管理ノードの完全修飾ドメイン名または IP アドレスを入力します。

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。



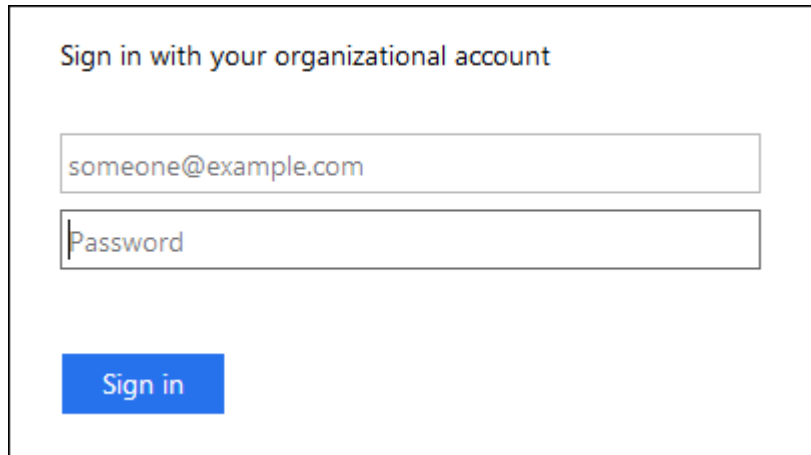
テナントアカウントの完全なURL（完全修飾ドメイン名またはIPアドレスのあとにを追加したもの）を入力すると、StorageGRID のサインインページは表示されません（/?accountId=20-digit-account-id）。代わりに、組織の SSO サインインページがすぐに表示されます。このページでは、を実行できます [SSO クレデンシャルを使用してサインインします](#)。

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 `custom-server.crt`。ノードのデフォルトサーバ証明書の名前は `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く"](#)
- ["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く

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。

Edit Tenant Account

Tenant Details

Display Name

Uses Own Identity Source

Allow Platform Services

Storage Quota (optional)

Cancel

Save

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、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ない場合は、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。

Single Sign-on

You can enable single sign-on (SSO) if you want an external identity provider (IdP) to authorize all user access to StorageGRID. To start, enable [identity federation](#) and confirm that at least one federated user has Root Access permission to the Grid Manager and to the Tenant Manager for any existing tenant accounts. Next, select Sandbox Mode to configure, save, and then test your SSO settings. After verifying the connections, select Enabled and click Save to start using SSO.

SSO Status Disabled Sandbox Mode Enabled

Save



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。ここでは、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、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。

Single Sign-on

You can enable single sign-on (SSO) if you want an external identity provider (IdP) to authorize all user access to StorageGRID. To start, enable [identity federation](#) and confirm that at least one federated user has Root Access permission to the Grid Manager and to the Tenant Manager for any existing tenant accounts. Next, select Sandbox Mode to configure, save, and then test your SSO settings. After verifying the connections, select Enabled and click Save to start using SSO.

SSO Status Disabled Sandbox Mode Enabled

Sandbox mode

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

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

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

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

- 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。
- 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_Identifier" -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）。

- 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。

- 「* 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。

- 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。
 - 作成した証明書利用者信頼を検索します。
 - 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。
 - アクセス制御ポリシーを選択します。
 - [*適用 (Apply)]をクリックし、[OK]をクリックします
- 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。
 - 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。

- 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

- Windows Server Managerで、* Tools をクリックし、AD FS Management *を選択します。
- 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。
- [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。
- [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。
- 証明書利用者信頼の追加ウィザードを実行します。
 - 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。

- 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。
- [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。
- 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。

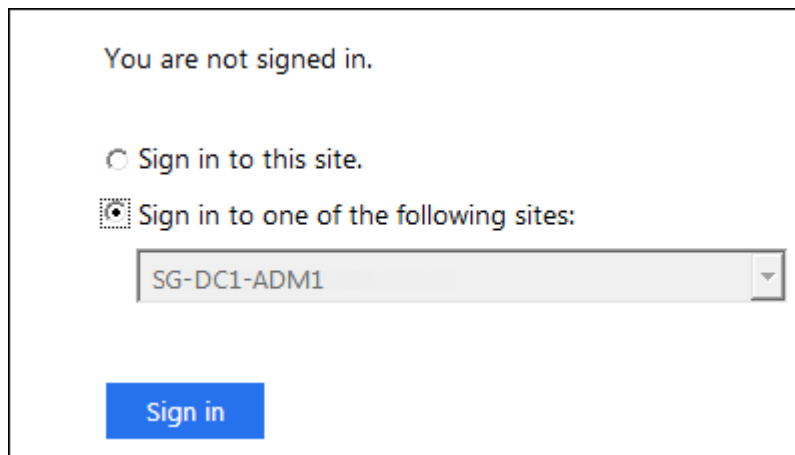
Sandbox mode

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

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

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

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。



The screenshot shows a web interface for signing in. At the top, it says "You are not signed in." Below this, there are two radio button options: "Sign in to this site." (which is unselected) and "Sign in to one of the following sites:" (which is selected). Under the selected option, there is a dropdown menu with "SG-DC1-ADM1" selected. At the bottom left, there is a blue "Sign in" button.

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。

Warning

Enable single sign-on

After you enable SSO, no local users—including the root user—will be able to sign in to the Grid Manager, the Tenant Manager, the Grid Management API, or the Tenant Management API.

Before proceeding, confirm the following:

- You have imported at least one federated group from the identity source and assigned Root Access management permissions to the group. You must confirm that at least one federated user has Root Access permission to the Grid Manager and to the Tenant Manager for any existing tenant accounts.
- You have tested all relying party trusts using sandbox mode.

Are you sure you want to enable single sign-on?

Cancel

OK

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。

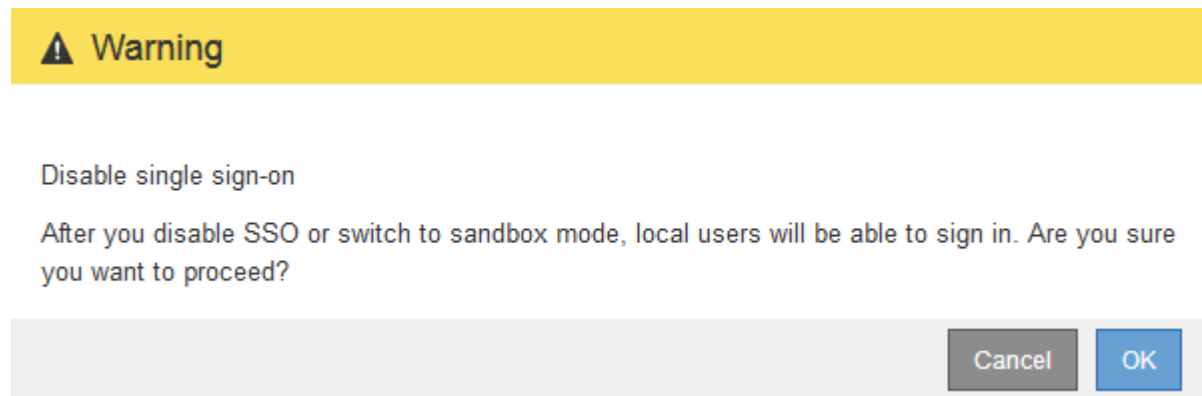
手順

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。

- 次のコマンドを入力します。 `ssh admin@Admin_Node_IP`
- 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。
- 次のコマンドを入力してrootに切り替えます。 `su -`
- 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

- 「* Configuration * Access Control * Single Sign-On *」を選択します。
- 正しくないSSO設定または古いSSO設定を変更します。
- [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。

- 必要なタスクを実行します。
- [サインアウト]をクリックして、Grid Managerを閉じます。
- 管理ノードでSSOを再度有効にします。次のいずれかの手順を実行します。

- 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 クレデンシヤ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。

Client Certificates

You can upload or generate one or more client certificates to allow StorageGRID to authenticate external client access.

Name	Allow Prometheus	Expiration Date
No client certificates configured.		

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。

Upload Certificate

Name

Allow Prometheus

Certificate Details


Upload the public key for the client certificate.

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。

Upload Certificate

Name  test-certificate-upload

Allow Prometheus 


Certificate Details

Upload the public key for the client certificate.

Upload Client Certificate

Generate Client Certificate

Uploaded file name: client (1).crt

Certificate metadata 

```
Subject DN: /C=US/ST=California/L=Sunnyvale/O=Example Co./OU=IT/CN=*.s3.example.com
Serial Number: 0D:0E:FC:16:75:B8:BE:3E:7D:47:4D:05:49:08:F3:7B:E8:4A:71:90
Issuer DN: /C=US/ST=California/L=Sunnyvale/O=Example Co./OU=IT/CN=*.s3.example.com
Issued On: 2020-06-19T22:11:56.000Z
Expires On: 2021-06-19T22:11:56.000Z
SHA-1 Fingerprint: 13:AA:D6:06:2B:90:FE:B7:7B:EB:1A:83:BE:C3:62:39:B7:A6:E7:F0
SHA-256 Fingerprint: 5C:29:06:6B:CF:81:50:B8:4F:A9:56:F7:A7:AB:3C:36:FA:3D:B7:32:A4:C9:74:85:2C:8D:E6:67:37:C3:AC:60
```

Certificate PEM 

```
-----BEGIN CERTIFICATE-----
MIIDmzCCAoQgAwIBAgIUUDQ78FnW4vj59R00FSQjze+hKcoZAwDQYJKoZIhvcNAQEL
BQAwDELMAkGA1UEBhMCVVMxEzARBgNVBAgMCkNhbg1mb3JuaWEuXzAQBgNVBAcM
CVN1bm55dmFsZTEUMBIGA1UECgwLRXhhbXBsZSBDbj4xOzAkJBgNVBAeMAk1UMRkw
FwYDQDDDBAqLnMzLmV4YW1wbGUuY29tMB4XDTEwMDYxOTIyMTE1N1oXDTEwMDYx
OTIyMTE1N1owDELMAkGA1UEBhMCVVMxEzARBgNVBAgMCkNhbg1mb3JuaWEuXzAQBg
NVBAcMVCV1bm55dmFsZTEUMBIGA1UECgwLRXhhbXBsZSBDbj4xOzAkJBgNVBAeM
Ak1UMRkwFwYDQDDDBAqLnMzLmV4YW1wbGUuY29tMIIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEA5Vqq2MnjvVotLeStq1Co4coJmsQ2ygrhuwSza0bgMnjf
cwUgHNVFXGuGlzY/Tl37r3Dk5bu2fyGYAeJ6mqbQA6cE3yp0p5Hw7Cm/AWJknFw6
```

Copy certificate to clipboard

Cancel

Save

- [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。
 - 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。
 - 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。
- [クライアント証明書の生成]を選択します。
 - 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。
 - 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。
 - 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。
 - [*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。

Grafana の例は次のスクリーンショットで示されています。

The screenshot shows the Grafana configuration interface for a Prometheus data source named 'sg-prometheus'. The 'Default' toggle is turned on. Under the 'HTTP' section, the 'URL' is set to 'https://admin-node.example.com:9091'. The 'Access' dropdown is set to 'Server (default)'. Under the 'Auth' section, 'Basic auth' is disabled, 'With Credentials' is disabled, 'TLS Client Auth' is enabled, 'Skip TLS Verify' is disabled, and 'Forward OAuth Identity' is disabled. 'With CA Cert' is also enabled. Under the 'TLS/SSL Auth Details' section, the 'CA Cert' field is highlighted, and the 'ServerName' is set to 'admin-node.example.com'. The 'Client Cert' field is also visible, showing a placeholder for a certificate.

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。

	Name	Allow Prometheus	Expiration Date
<input type="radio"/>	test-certificate-upload	✓	2021-06-19 16:11:56 MDT
<input checked="" type="radio"/>	test-certificate-generate	✓	2022-08-20 09:42:00 MDT

Displaying 2 certificates.

- 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。
- 「* 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。

Edit Certificate test-certificate-generate

Name:

Allow Prometheus:

Certificate Details

Upload the public key for the client certificate.

Upload Client Certificate
Generate Client Certificate

Certificate metadata

```

Subject DN: /CN=test.com
Serial Number: 0C:11:87:6C:1E:FD:13:16:F3:F2:06:D9:DA:6D:BC:CE:2A:A9:C3:53
Issuer DN: /CN=test.com
Issued On: 2020-11-23T15:53:33.000Z
Expires On: 2022-11-23T15:53:33.000Z
SHA-1 Fingerprint: AE:E6:70:A7:D3:C3:39:7A:09:F9:62:9B:81:8A:87:CD:43:16:89:A7
SHA-256 Fingerprint: 63:07:BF:FF:08:1E:84:F1:D4:67:C6:16:B0:35:26:00:C6:A3:13:11:7E:5E:9
0:EC:7A:7B:EF:23:14:55:3D:56

```

Certificate PEM

```

-----BEGIN CERTIFICATE-----
MIICyzCCAbOgAwIBAgIUDBGHbB79Exbz8gbZ2m28ziqpw1MwDQYJKoZIhvcNAQEL
BQAwEzERMASGA1UEAwIdGVzdC5jb20wHhcNMjAxMTIzMTU1MzZWhcNMjAxMTIz
MTU1MzZWhcATMREwDwYDVQQDDAh0ZXN0LmNvbnVhYy9kaWYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBBAKdgEcneCDFDsLjvLnX9ow6oPrdU7m2EN6SS6xdVI155sCH+
hkwO5a2Mym7EhbNrfwOt2nMjQkcaKIrk8QAmutRgG6N1N12FIW0gYQuzFQ0QddLq
n7ymFw6w8a9zYSu7bLp84Yn0/LSDPk+h3Jic7Mrt2X70It5ZDRwFmbLNvEvYEtIS
h+FbNh885AIRO2eLxvCOIRij1bySe76wK+Wmc97HdxR8GyxIWk6BD47XC+dOrv55
wvtjc/41qc5xsE6XmJs2yJg4VARx10y8Icwa9fr00+xPwIdCOwXkpWJXeBnCoKX
YcQxbWz1r+iVLJqLTMxUszTTI30rUgN00M82GJUCAwEAAaMKMBUwEwYDVR0RBAAw

```

Copy certificate to clipboard

Cancel Save

- 証明書に必要な変更を加えます。
- 証明書をGrid Managerに保存するには、* Save *を選択します。
- 新しい証明書をアップロードした場合：
 - [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。
 - 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。
 - 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。

	Name	Allow Prometheus	Expiration Date
<input type="radio"/>	test-certificate-upload	✓	2021-06-19 16:11:56 MDT
<input checked="" type="radio"/>	test-certificate-generate	✓	2022-08-20 09:42:00 MDT

Displaying 2 certificates.

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。

Warning

Delete certificate

Are you sure you want to delete the certificate "test-certificate-generate"?

Cancel OK

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	<p>ストレージ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。</p>	<p>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。一部のストレージプライアンスまたはサービスプライアンスでは使用できません。</p> <p>"SG6000 ストレージプライアンス"</p> <p>"SG5700 ストレージプライアンス"</p> <p>"SG5600 ストレージプライアンス"</p>
格納オブジェクトの暗号化グリッドオプション	<ul style="list-style-type: none"> 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。 	<p>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。</p> <p>"格納オブジェクトの暗号化を設定する"</p>
S3 バケットの暗号化	<p>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。</p>	<p>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。</p> <p>"S3 を使用する"</p>

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)	<p>オブジェクトを格納してを含めるS3要求を問題した <code>x-amz-server-side-encryption</code> 要求ヘッダー。</p>	<p>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。</p> <p>キーは StorageGRID で管理されます。</p> <p>"S3 を使用する"</p>
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)	<p>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。</p> <ul style="list-style-type: none"> • <code>x-amz-server-side-encryption-customer-algorithm</code> • <code>x-amz-server-side-encryption-customer-key</code> • <code>x-amz-server-side-encryption-customer-key-MD5</code> 	<p>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。</p> <p>キーは StorageGRID の外部で管理されます。</p> <p>"S3 を使用する"</p>
外部ボリュームまたはデータストアの暗号化	<p>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。</p>	<p>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。</p> <p>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。</p>

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。	<p>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）。</p> <p>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。</p> <p>"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"</p>

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：

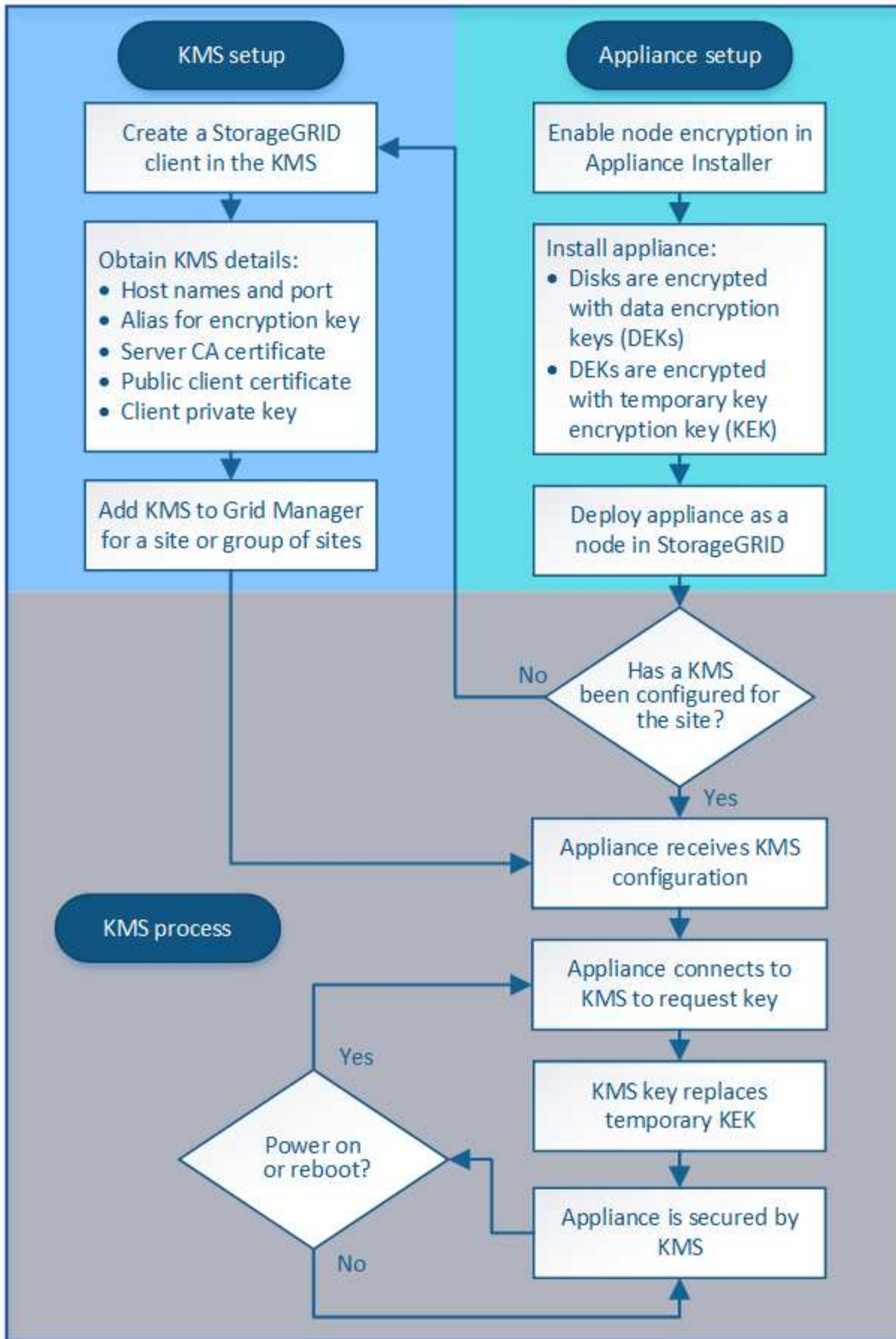
- KMS を使用してアプライアンスノードを保護したり、SANtricity システムマネージャのドライブセキュリティ機能を使用して、同じアプライアンス内の自己暗号化ドライブ上のデータを「二重に暗号化」することもできます。
- KMS を使用してアプライアンスノード上のデータを保護したり、格納されているオブジェクト暗号化グリッドオプションを使用してすべてのオブジェクトを取り込み時に暗号化することもできます。

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力します。	"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。

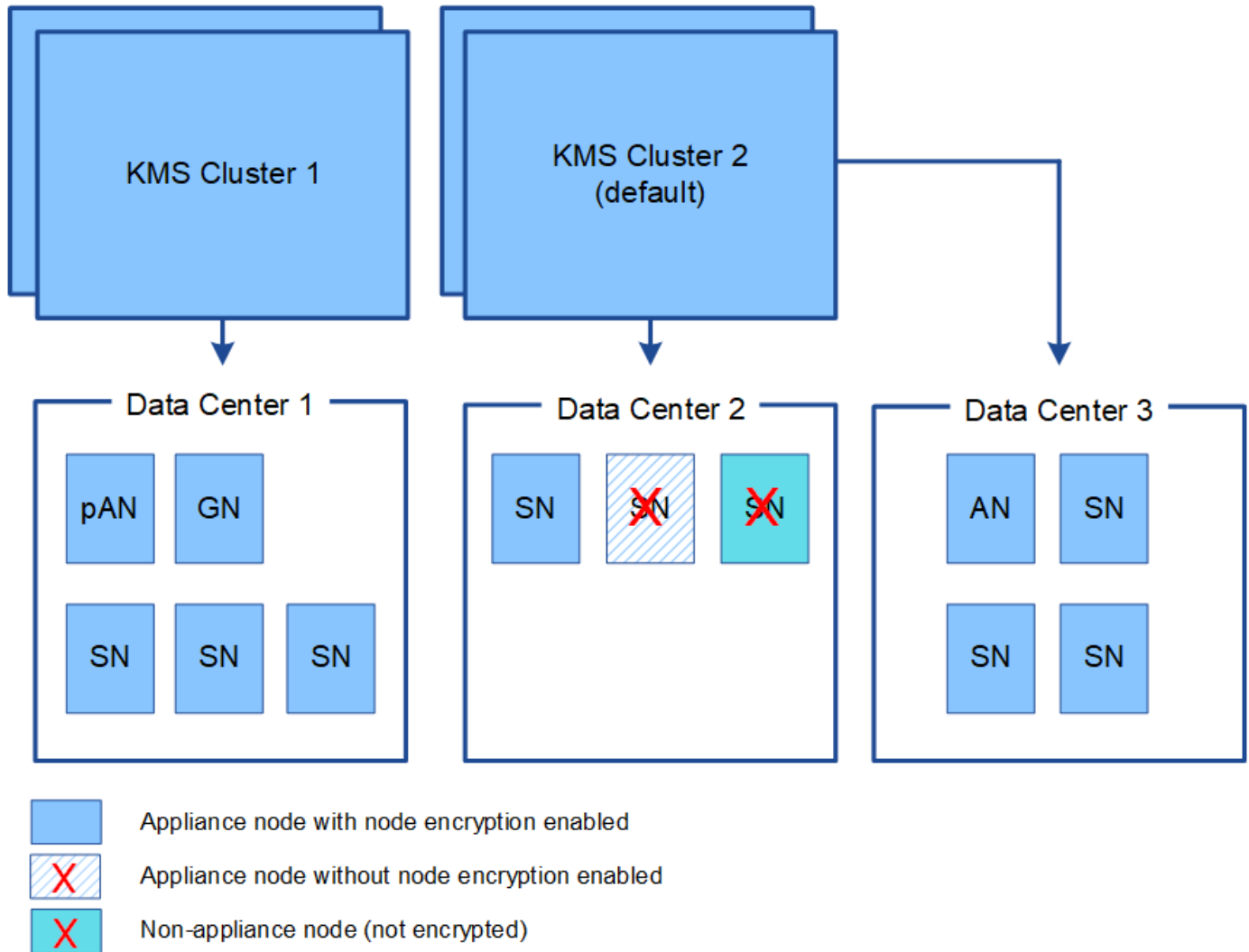
必要なキー管理サーバの数

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一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"](#)

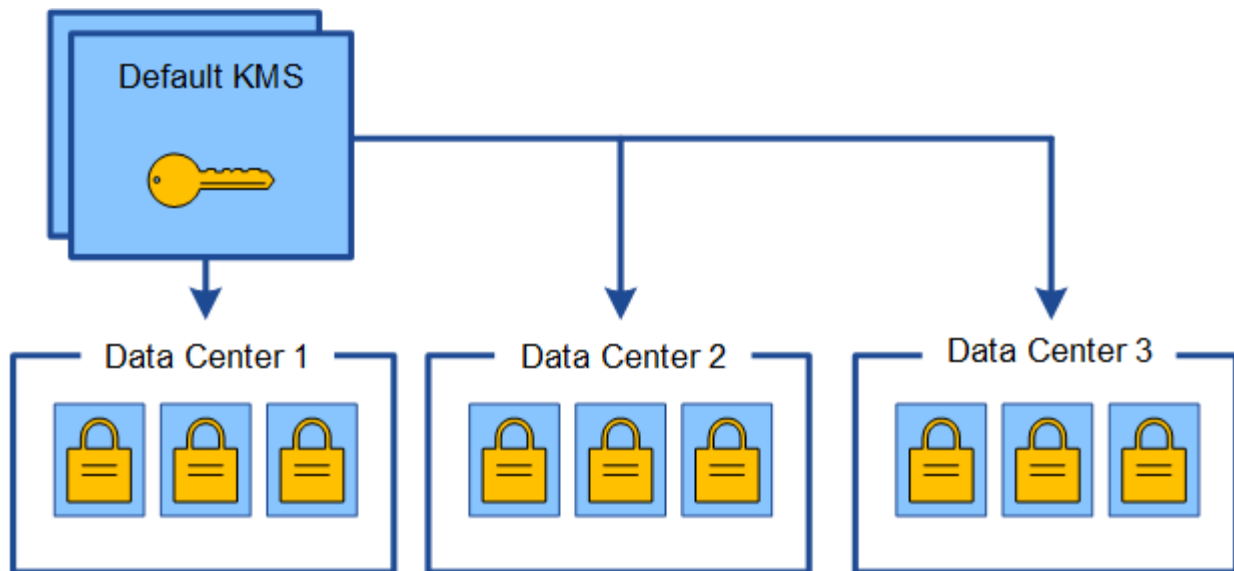
サイトの **KMS** を変更する際の考慮事項

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。

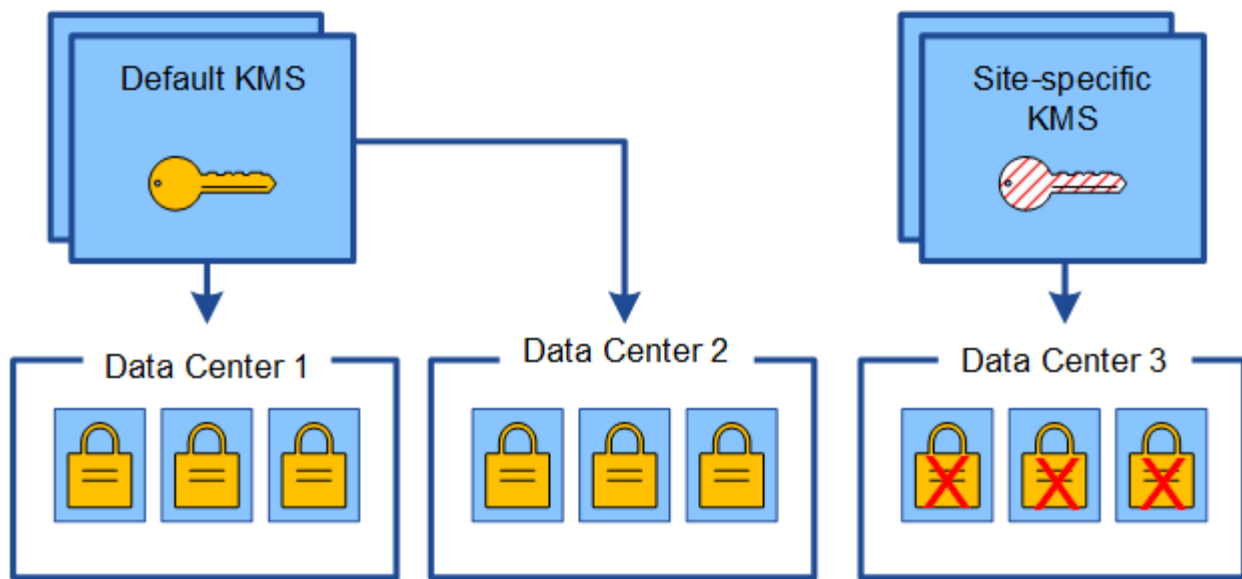
サイトで使用されている KMS を変更する場合は、そのサイトで以前に暗号化したアプライアンスノードを新しい KMS に格納されているキーを使用して復号化できることを確認する必要があります。場合によっては、暗号化キーの現在のバージョンを元の KMS から新しい KMS にコピーする必要があります。サイトで暗号化されたアプライアンスノードを復号化するために、KMS に正しいキーがあることを確認する必要があります。

例：

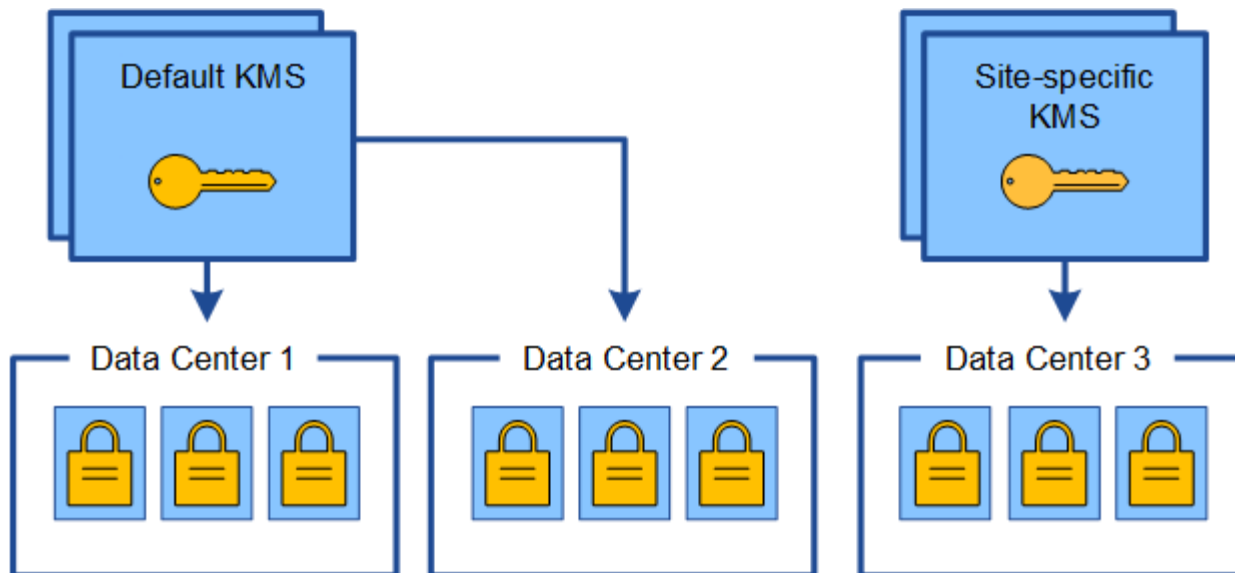
1. 最初に、専用の KMS がない環境のすべてのサイトを設定します。
2. KMS を保存すると、「Node Encryption *」設定が有効になっているすべてのアプライアンスノードが KMS に接続して暗号化キーを要求します。このキーは、すべてのサイトのアプライアンスノードの暗号化に使用されます。同じキーを使用して、これらのアプライアンスを復号化する必要もあります。



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時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
<p>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。</p>	<p>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。</p> <p>"キー管理サーバの編集 (KMS)"</p>
<p>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。</p>	<ol style="list-style-type: none"> 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。 <p>"キー管理サーバの追加 (KMS)"</p>

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。	<ol style="list-style-type: none"> 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。 <p>"キー管理サーバの追加 (KMS) "</p>

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なになります。

- 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。

Key Management Server

If your StorageGRID system includes appliance nodes with node encryption enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID at rest.

Configuration Details Encrypted Nodes

You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

Before adding a KMS:

- Ensure that the KMS is KMIP-compliant.
- Configure StorageGRID as a client in the KMS.
- Enable node encryption for each appliance during appliance installation. You cannot enable node encryption after an appliance is added to the grid and you cannot use a KMS for appliances that do not have node encryption enabled.

For complete instructions, see [administering StorageGRID](#).

+ Create Edit Remove

KMS Display Name	Key Name	Manages keys for	Hostname	Certificate Status
No key management servers have been configured. Select Create .				

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。

Add a Key Management Server

1 Enter KMS Details 2 Upload Server Certificate 3 Upload Client Certificates

Enter information about the external key management server (KMS) and the StorageGRID client you configured in that KMS. If you are configuring a KMS cluster, select + to add a hostname for each server in the cluster.

KMS Display Name

Key Name

Manages keys for

Port

Hostname +

Cancel Next

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	<p>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。</p> <ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> ◦ 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	<p>KMS の完全修飾ドメイン名または IP アドレス。</p> <ul style="list-style-type: none"> • 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。

手順 2：サーバ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 2（サーバ証明書をアップロード）で、KMS のサーバ証明書（または証明書バンドル）をアップロードします。サーバ証明書を使用すると、外部 KMS は StorageGRID に対して自身を認証できます。

手順

1. 手順 2（サーバ証明書のアップロード）* から、保存されているサーバ証明書または証明書バンドルの場所を参照します。

Add a Key Management Server

1 Enter KMS Details 2 Upload Server Certificate 3 Upload Client Certificates

Upload a server certificate signed by the certificate authority (CA) on the external key management server (KMS) or a certificate bundle. The server certificate allows the KMS to authenticate itself to StorageGRID.

Server Certificate

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。

Add a Key Management Server



Upload a server certificate signed by the certificate authority (CA) on the external key management server (KMS) or a certificate bundle. The server certificate allows the KMS to authenticate itself to StorageGRID.

Server Certificate ⓘ k170vCA.pem

Server Certificate Metadata

```
Server DN: /C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA
Serial Number: 71:CD:6D:72:53:B5:6D:0A:8C:69:13:0D:4D:D7:81:0E
Issue DN: /C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA
Issued On: 2020-10-15T21:12:45.000Z
Expires On: 2030-10-13T21:12:45.000Z
SHA-1 Fingerprint: EE:E4:6E:17:86:DF:56:B4:F5:AF:A2:3C:BD:56:6B:10:DB:B2:5A:79
```

Cancel

Back

Next



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）が表示されません。

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。

Add a Key Management Server



Upload the client certificate and the client certificate private key. The client certificate is issued to StorageGRID by the external key management server (KMS), and it allows StorageGRID to authenticate itself to the KMS.

Client Certificate 

Client Certificate Private Key 

Cancel

Back

Save

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。

Add a Key Management Server



Upload the client certificate and the client certificate private key. The client certificate is issued to StorageGRID by the external key management server (KMS), and it allows StorageGRID to authenticate itself to the KMS.

Client Certificate  k170vClientCert.pem

```
Server DN: /CN=admin/UID=  
Serial Number: 7D:5A:8A:27:02:40:C8:F5:19:A1:28:22:E7:D6:E2:EB  
Issue DN: /C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA  
Issued On: 2020-10-15T23:31:49.000Z  
Expires On: 2022-10-15T23:31:49.000Z  
SHA-1 Fingerprint: A7:10:AC:39:85:42:80:8F:FF:62:AD:A1:BD:CF:4C:90:F3:E9:36:69
```

Client Certificate Private Key  k170vClientKey.pem

Cancel

Back

Save

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。

Add a Key Management Server



Upload the client certificate and the client certificate private key. The client certificate is issued to StorageGRID by the external key management server (KMS), and it allows StorageGRID to authenticate itself to the KMS.

Client Certificate ⓘ k170vClientCert.pem

Server DN: /CN=admin/UID=
Serial Number: 7D:5A:8A:27:02:40:C8:F5:19:A1:28:22:E7:D6:E2:EB
Issue DN: /C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA
Issued On: 2020-10-15T23:31:49.000Z
Expires On: 2022-10-15T23:31:49.000Z
SHA-1 Fingerprint: A7:10:AC:39:85:42:80:8F:FF:62:AD:A1:BD:CF:4C:90:F3:E9:36:69

Client Certificate Private Key ⓘ k170vClientKey.pem

Select **Force Save** to save this KMS without testing the external connections. If there is an issue with the configuration, you might not be able to reboot any FDE-enabled appliance nodes at the affected site, and you might lose access to your data.

Cancel

Back

Force Save

Save



[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。

Warning

Confirm force-saving the KMS configuration

Are you sure you want to save this KMS without testing the external connections?

If there is an issue with the configuration, you might not be able to reboot any appliance nodes with node encryption enabled at the affected site, and you might lose access to your data.

Cancel

OK

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。

Key Management Server

If your StorageGRID system includes appliance nodes with node encryption enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID at rest.

Configuration Details Encrypted Nodes

You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

Before adding a KMS:

- Ensure that the KMS is KMIP-compliant.
- Configure StorageGRID as a client in the KMS.
- Enable node encryption for each appliance during appliance installation. You cannot enable node encryption after an appliance is added to the grid and you cannot use a KMS for appliances that do not have node encryption enabled.

For complete instructions, see [administering StorageGRID](#).

+ Create Edit Remove				
KMS Display Name	Key Name	Manages keys for	Hostname	Certificate Status
Default KMS	test	Sites not managed by another KMS (default KMS)	10.96.99.164	✓ All certificates are valid

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	<p>KMS の完全修飾ドメイン名または IP アドレス。</p> <p>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。</p> <p>例： 10.10.10.10 and 10.10.10.11 または 10.10.10.10 and 2 others。</p> <p>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。</p>
証明書のステータス	<p>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。</p> <ul style="list-style-type: none"> 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。

Key Management Server

If your StorageGRID system includes appliance nodes with node encryption enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID at rest.

Configuration Details Encrypted Nodes

You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

Before adding a KMS:

- Ensure that the KMS is KMIP-compliant.
- Configure StorageGRID as a client in the KMS.
- Enable node encryption for each appliance during appliance installation. You cannot enable node encryption after an appliance is added to the grid and you cannot use a KMS for appliances that do not have node encryption enabled.

For complete instructions, see [administering StorageGRID](#).

+ Create Edit Remove				
KMS Display Name	Key Name	Manages keys for	Hostname	Certificate Status
Default KMS	test	Sites not managed by another KMS (default KMS)	10.96.99.164	✓ All certificates are valid

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。

Key Management Server

If your StorageGRID system includes appliance nodes with Full Disk Encryption (FDE) enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID data at rest.

Configuration Details Encrypted Nodes

You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

[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。

Configuration Details Encrypted Nodes

Review the KMS status for all appliance nodes that have node encryption enabled. Address any issues immediately to ensure your data is fully protected. If no KMS exists for a site, select Configuration Details and add a KMS.

Nodes with Encryption Enabled

Node Name	Node Type	Site	KMS Display Name	Key UID	Status
SGA-010-096-104-67	Storage Node	Data Center 1	Default KMS	41b0...5c57	✓ Connected to KMS (2021-03-12 10:59:32 MST)

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的 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。

Key Management Server

If your StorageGRID system includes appliance nodes with node encryption enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID at rest.

Configuration Details

Encrypted Nodes

You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

Before adding a KMS:

- Ensure that the KMS is KMIP-compliant.
- Configure StorageGRID as a client in the KMS.
- Enable node encryption for each appliance during appliance installation. You cannot enable node encryption after an appliance is added to the grid and you cannot use a KMS for appliances that do not have node encryption enabled.

For complete instructions, see [administering StorageGRID](#).

+ Create Edit Remove				
KMS Display Name	Key Name	Manages keys for	Hostname	Certificate Status
Default KMS	test	Sites not managed by another KMS (default KMS)	10.96.99.164	✓ All certificates are valid

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	<p>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。</p> <p>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。</p> <div style="border: 1px solid gray; padding: 10px; margin: 10px 0;">  <p>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。</p> <p>"キー管理サーバを使用する際の考慮事項と要件"</p> </div>
のキーを管理します	<p>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。</p> <ul style="list-style-type: none"> • 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	<p>KMS の完全修飾ドメイン名または IP アドレス。</p> <ul style="list-style-type: none"> • 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。

Warning

Confirm force-saving the KMS configuration

Are you sure you want to save this KMS without testing the external connections?

If there is an issue with the configuration, you might not be able to reboot any appliance nodes with node encryption enabled at the affected site, and you might lose access to your data.

Cancel

OK

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。

Key Management Server

If your StorageGRID system includes appliance nodes with node encryption enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID at rest.

Configuration Details

Encrypted Nodes

You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

Before adding a KMS:

- Ensure that the KMS is KMIP-compliant.
- Configure StorageGRID as a client in the KMS.
- Enable node encryption for each appliance during appliance installation. You cannot enable node encryption after an appliance is added to the grid and you cannot use a KMS for appliances that do not have node encryption enabled.

For complete instructions, see [administering StorageGRID](#).

+ Create Edit Remove				
KMS Display Name	Key Name	Manages keys for	Hostname	Certificate Status
<input checked="" type="radio"/> Default KMS	test	Sites not managed by another KMS (default KMS)	10.96.99.164	✓ All certificates are valid

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。

⚠ Warning

Delete KMS Configuration

You can only remove a KMS in these cases:

- You are removing a site-specific KMS for a site that has no appliance nodes with node encryption enabled.
- You are removing the default KMS, but a site-specific KMS already exists for each site with node encryption.

Are you sure you want to delete the Default KMS KMS configuration?

Cancel

OK

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せん。



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、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。

Tenant Accounts

View information for each tenant account.

Note: Depending on the timing of ingests, network connectivity, and node status, the usage data shown might be out of date. To view more recent values, select the tenant and select **View Details**.

+ Create View details Edit Actions Export to CSV Search by Name/ID

Display Name Space Used Quota Utilization Quota Object Count Sign in

No results found.

Show 20 rows per page

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。

Create Tenant Account

Tenant Details

Display Name

Protocol S3 Swift

Storage Quota (optional) GB

Authentication ?

Configure how the tenant account will be accessed.

Uses Own Identity Source

Specify a password for the tenant's local root user.

Username root

Password

Confirm Password

Cancel Save

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

Create Tenant Account

Tenant Details

Display Name	<input type="text" value="S3 tenant (SSO enabled)"/>
Protocol	<input checked="" type="radio"/> S3 <input type="radio"/> Swift
Allow Platform Services	<input checked="" type="checkbox"/>
Storage Quota (optional)	<input type="text"/> <input type="text" value="GB"/>

Authentication

Because single sign-on is enabled, the tenant must use the Grid Manager's identity federation service, and no local users can sign in. You must select an existing federated group to have the initial Root Access permission for the tenant.

Uses Own Identity Source

Single sign-on is enabled. The tenant cannot use its own identity source.

Root Access Group

Cancel

Save

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トッドグループを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	<p>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。</p> <p>Tenant Manager の URL の形式は次のとおりです。</p> <pre>https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/</pre> <ul style="list-style-type: none"> • <i>FQDN_or_Admin_Node_IP</i> 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 • <i>port</i> は、テナント専用ポートです • <i>20-digit-account-id</i> 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。

- 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。

Configure Tenant Account

✔ Account S3 tenant created successfully.

If you are ready to configure this tenant account, sign in as the tenant's root user. Then, click the links below.

Sign in as root

- [Buckets](#) - Create and manage buckets.
- [Groups](#) - Manage user groups, and assign group permissions.
- [Users](#) - Manage local users, and assign users to groups.

Finish

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。

Sign in as root ✔

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	<ul style="list-style-type: none">• 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。 <p><code>https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/</code></p> <ul style="list-style-type: none">◦ <code>FQDN_or_Admin_Node_IP</code> 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◦ <code>20-digit-account-id</code> 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	<ul style="list-style-type: none"> • 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。 <pre>https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id</pre> <ul style="list-style-type: none"> ◦ <i>FQDN_or_Admin_Node_IP</i> 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 ◦ <i>port</i> は、テナント専用の制限付きポートです ◦ <i>20-digit-account-id</i> 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。

Tenant Accounts

View information for each tenant account.

Note: Depending on the timing of ingests, network connectivity, and node status, the usage data shown might be out of date. To view more recent values, select the tenant and select **View Details**.

	Display Name	Space Used	Quota Utilization	Quota	Object Count	Sign in
<input checked="" type="radio"/>	Account01	500.00 KB	0.00%	20.00 GB	100	
<input type="radio"/>	Account02	2.50 MB	0.01%	30.00 GB	500	
<input type="radio"/>	Account03	605.00 MB	4.03%	15.00 GB	31,000	
<input type="radio"/>	Account04	1.00 GB	10.00%	10.00 GB	200,000	
<input type="radio"/>	Account05	0 bytes	—	Unlimited	0	

Show 20 rows per page

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。

Change Root User Password - Account03

Username	root
New Password	<input type="password" value="●●●●●●"/>
Confirm New Password	<input type="password"/>

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。

Tenant Accounts

View information for each tenant account.

Note: Depending on the timing of ingests, network connectivity, and node status, the usage data shown might be out of date. To view more recent values, select the tenant and select **View Details**.

	Display Name  	Space Used  	Quota Utilization  	Quota  	Object Count  	Sign in 
<input checked="" type="radio"/>	Account01	500.00 KB	0.00%	20.00 GB	100	
<input type="radio"/>	Account02	2.50 MB	0.01%	30.00 GB	500	
<input type="radio"/>	Account03	605.00 MB	4.03%	15.00 GB	31,000	
<input type="radio"/>	Account04	1.00 GB	10.00%	10.00 GB	200,000	
<input type="radio"/>	Account05	0 bytes	—	Unlimited	0	

Show 20 rows per page

- 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。

- 「* 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。

Edit Tenant Account

Tenant Details

Display Name

Allow Platform Services

Storage Quota (optional)

Uses Own Identity Source

Cancel

Save

- 必要に応じて、フィールドの値を変更します。
 - このテナントアカウントの表示名を変更します。
 - 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せん。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せんが、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 クラスター
- 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

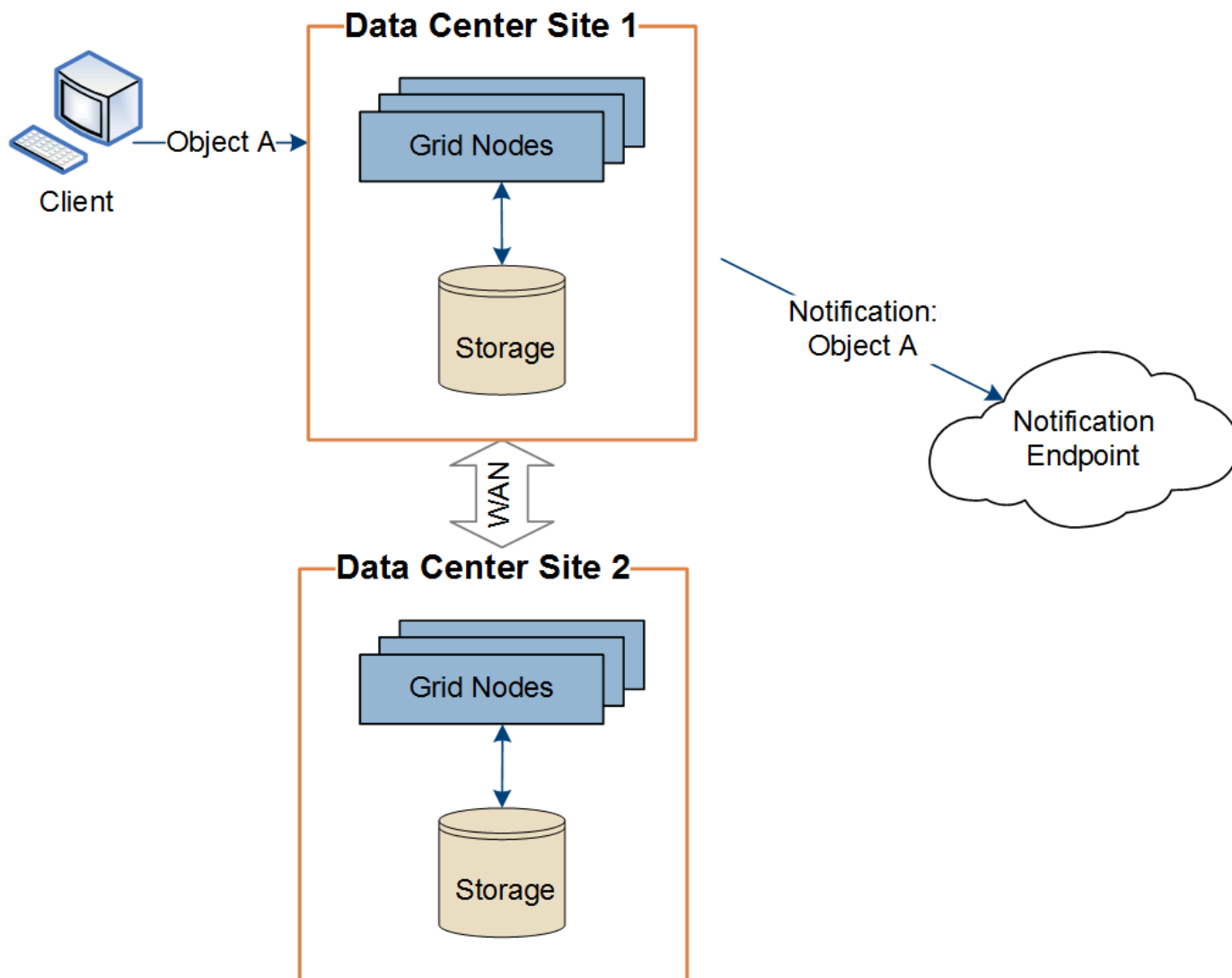
["ストレージプロキシを設定しています"](#)

["テナントアカウントを使用する"](#)

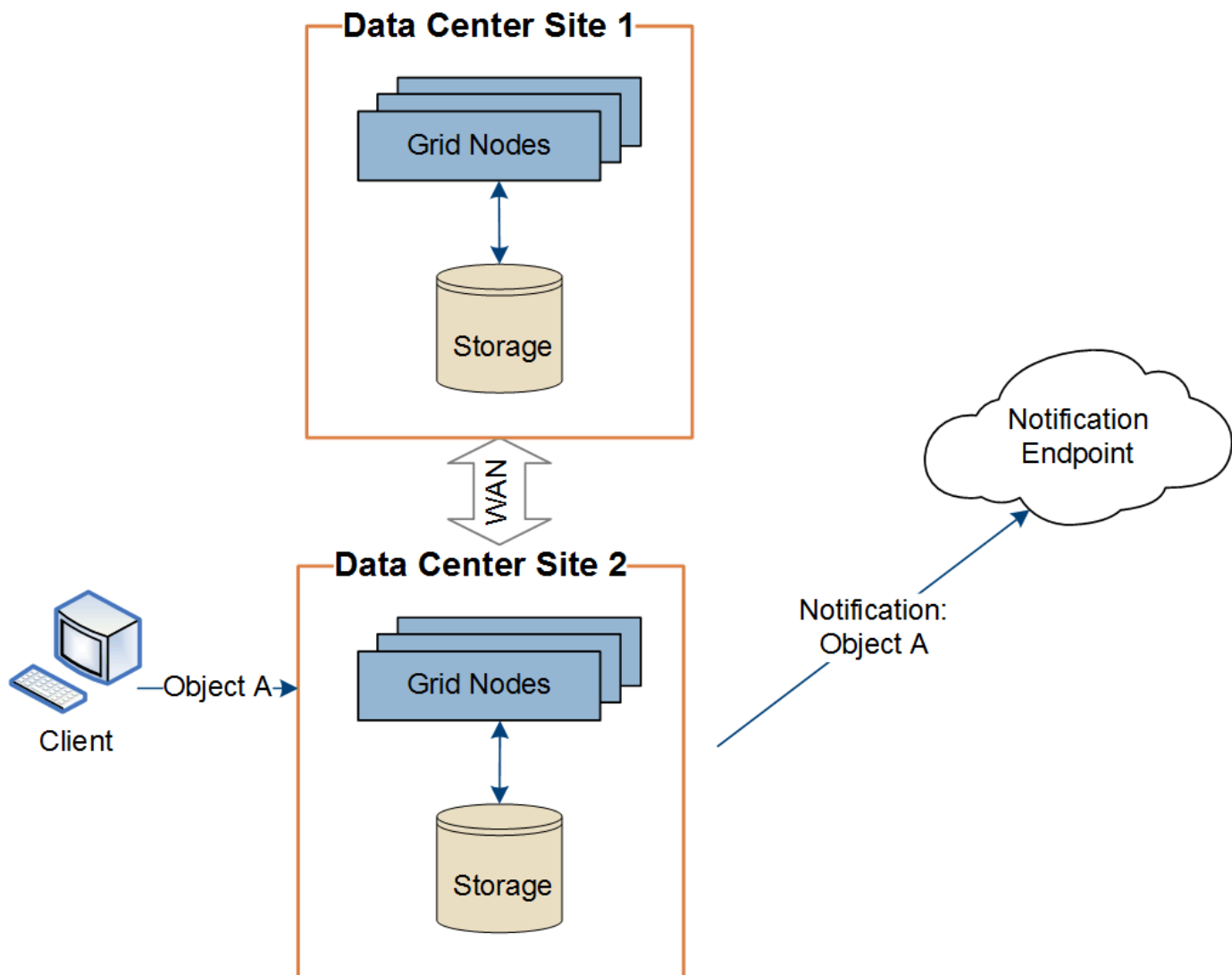
サイト単位のプラットフォームサービスメッセージの配信

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 사용되는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を検証されます。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。



One or more endpoints have experienced an error and might not be functioning properly. Go to the [Endpoints](#) page to view the error details. The last error occurred 2 hours ago.

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

Platform services endpoints

A platform services endpoint stores the information StorageGRID needs to use an external resource as a target for a platform service (CloudMirror replication, notifications, or search integration). You must configure an endpoint for each platform service you plan to use.















One or more endpoints have experienced an error. Select the endpoint for more details about the error. Meanwhile, the platform service request will be retried automatically.

5 endpoints

Create endpoint

Delete endpoint

<input type="checkbox"/>	Display name  	Last error  	Type  	URI  	URN  
<input type="checkbox"/>	my-endpoint-2	 2 hours ago	Search	http://10.96.104.30:9200	urn:sgws:es:::mydomain/sveloso/_doc
<input type="checkbox"/>	my-endpoint-3	 3 days ago	Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example1
<input type="checkbox"/>	my-endpoint-5	12 days ago	Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example3
<input type="checkbox"/>	my-endpoint-4		Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example2
<input type="checkbox"/>	my-endpoint-1		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket1



「* 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）。その後、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ド

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	<ul style="list-style-type: none"> • 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： <ul style="list-style-type: none"> • HTTPS : 8082 • HTTP : 8084 デフォルトの Swift ポート： <ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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。

Load Balancer Endpoints

Load balancer endpoints define Gateway Node and Admin Node ports that accept and load balance S3 and Swift requests to Storage Nodes. HTTPS endpoint certificates are configured per endpoint.

Changes to endpoints can take up to 15 minutes to be applied to all nodes.

+ Add endpoint port Edit endpoint Remove endpoint port

Display name

Port

Using HTTPS

No endpoints configured.

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。

Create Endpoint

Display Name

Port 10443

Protocol HTTP HTTPS

Endpoint Binding Mode Global HA Group VIPs Node Interfaces

Cancel

Save

- 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。
- 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。

- 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。
- 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。

Create Endpoint

Display Name

Port

Protocol HTTP HTTPS

Endpoint Binding Mode Global HA Group VIPs Node Interfaces

i This endpoint is currently bound globally. All nodes will use this endpoint unless an endpoint with an overriding binding mode exists for a specific port.

Cancel Save

- * 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。

Create Endpoint

Display Name

Port

Protocol HTTP HTTPS

Endpoint Binding Mode Global HA Group VIPs Node Interfaces

Name	Description	Virtual IP Addresses	Interfaces
<input type="checkbox"/> Group1		192.168.5.163	CO-REF-DC1-ADM1:eth0 (preferred Master)
<input type="checkbox"/> Group2		47.47.5.162	CO-REF-DC1-ADM1:eth2 (preferred Master)

Displaying 2 HA groups.

⚠ No HA groups selected. You must select one or more HA Groups; otherwise, this endpoint will act as a globally bound endpoint.

Cancel Save

- 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。

Create Endpoint


Display Name

Port

Protocol HTTP HTTPS

Endpoint Binding Mode Global HA Group VIPs Node Interfaces

Node	Interface
<input type="checkbox"/> CO-REF-DC1-ADM1	eth0
<input type="checkbox"/> CO-REF-DC1-ADM1	eth1
<input type="checkbox"/> CO-REF-DC1-ADM1	eth2
<input type="checkbox"/> CO-REF-DC1-GW1	eth0
<input type="checkbox"/> CO-REF-DC2-ADM1	eth0
<input type="checkbox"/> CO-REF-DC2-GW1	eth0

 No node interfaces selected. You must select one or more node interfaces; otherwise, this endpoint will act as a globally bound endpoint.

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。

Edit Endpoint Unsecured Port A (port 10449)

Endpoint Service Configuration

Endpoint service type S3 Swift

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。

Load Certificate

Upload the PEM-encoded custom certificate, private key, and CA bundle files.

Server Certificate	<input type="button" value="Browse"/>
Certificate Private Key	<input type="button" value="Browse"/>
CA Bundle	<input type="button" value="Browse"/>

- 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。

Generate Certificate

Domain 1	<input type="text" value="*.s3.example.com"/>	<input type="button" value="+"/>
IP 1	<input type="text" value="0.0.0.0"/>	<input type="button" value="+"/>
Subject	<input type="text" value="/CN=StorageGRID"/>	
Days valid	<input type="text" value="730"/>	

- 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*

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。

- 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。

Load Balancer Endpoints

Load balancer endpoints define Gateway Node and Admin Node ports that accept and load balance S3 and Swift requests to Storage Nodes. HTTPS endpoint certificates are configured per endpoint.

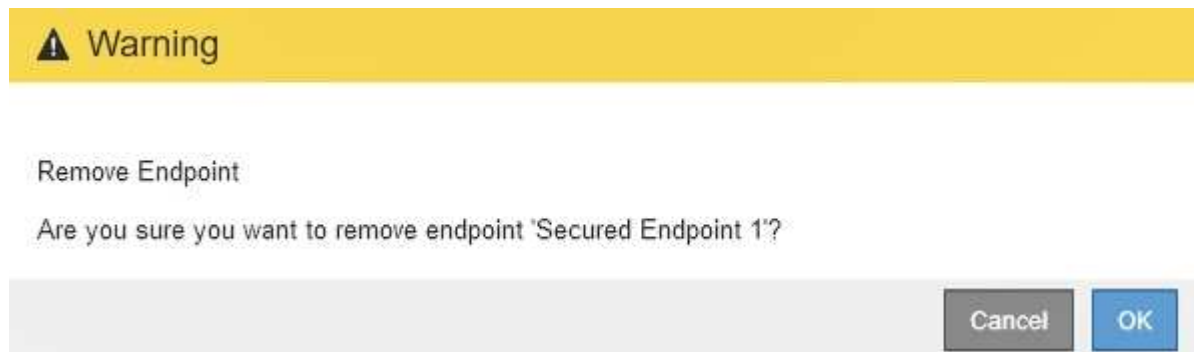
<input type="button" value="+ Add endpoint"/> <input type="button" value="✎ Edit endpoint"/> <input type="button" value="✕ Remove endpoint"/>			
	Display name	Port	Using HTTPS
<input type="radio"/>	Unsecured Endpoint 5	10444	No
<input checked="" type="radio"/>	Secured Endpoint 1	10443	Yes

Displaying 2 endpoints.

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。

The screenshot shows the "Grid Topology" interface. On the left is a tree view of the "StorageGRID Webscale Deployment" with nodes like "Data Center 1", "DC1-ADM1-98-160", "DC1-G1-98-161", "SSM", "CLB", "HTTP", "Events", "Resources", "DC1-G1-98-162", "DC1-S2-98-163", "DC1-S3-98-164", "DC1-ARC1-98-165", "Data Center 2", and "Data Center 3". The "CLB" node is highlighted with a blue box. On the right, the "Overview" tab is active, showing "Main" and "Overview: Summary - DC1-G1-98-161" with an update timestamp of "2015-10-27 16:23:33 PDT". Below this is a "Storage Capacity" section with a table of metrics.

Storage Capacity	
Storage Nodes Installed:	N/A
Storage Nodes Readable:	N/A
Storage Nodes Writable:	N/A
Installed Storage Capacity:	N/A
Used Storage Capacity:	N/A
Used Storage Capacity for Data:	N/A
Used Storage Capacity for Metadata:	N/A
Usable Storage Capacity:	N/A

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。

Untrusted Client Networks

If you are using a Client Network, you can specify whether a node trusts inbound traffic from the Client Network. If the Client Network is untrusted, the node only accepts inbound traffic on ports configured as [load balancer endpoints](#).

Set New Node Default

This setting applies to new nodes expanded into the grid.

New Node Client Network Trusted
Default Untrusted

Select Untrusted Client Network Nodes

Select nodes that should have untrusted Client Network enforcement.

<input type="checkbox"/>	Node Name	Unavailable Reason
<input type="checkbox"/>	DC1-ADM1	
<input type="checkbox"/>	DC1-G1	
<input type="checkbox"/>	DC1-S1	
<input type="checkbox"/>	DC1-S2	
<input type="checkbox"/>	DC1-S3	
<input type="checkbox"/>	DC1-S4	

Client Network untrusted on 0 nodes.

Save

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せん。

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。

DC1-ADM1 (Admin Node)

Overview Hardware Network Storage Load Balancer Events Tasks

Node Information

Name	DC1-ADM1
Type	Admin Node
ID	711b7b9b-8d24-4d9f-877a-be3fa3ac27e8
Connection State	 Connected
Software Version	11.4.0 (build 20200515.2346.8edcbbf)
HA Groups	Fabric Pools, Master
IP Addresses	192.168.2.208, 10.224.2.208, 47.47.2.208, 47.47.4.219 Show more 

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	<ul style="list-style-type: none"> • 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 <p>*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。</p>
Tenant Manager のみにアクセスします	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • ゲートウェイノード <p>• 注: * CLB サービスは廃止されました。</p>

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

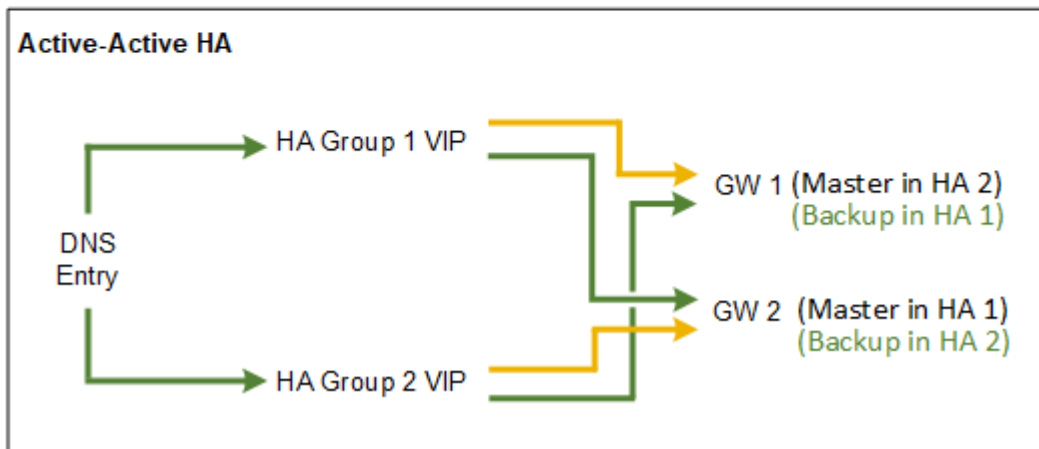
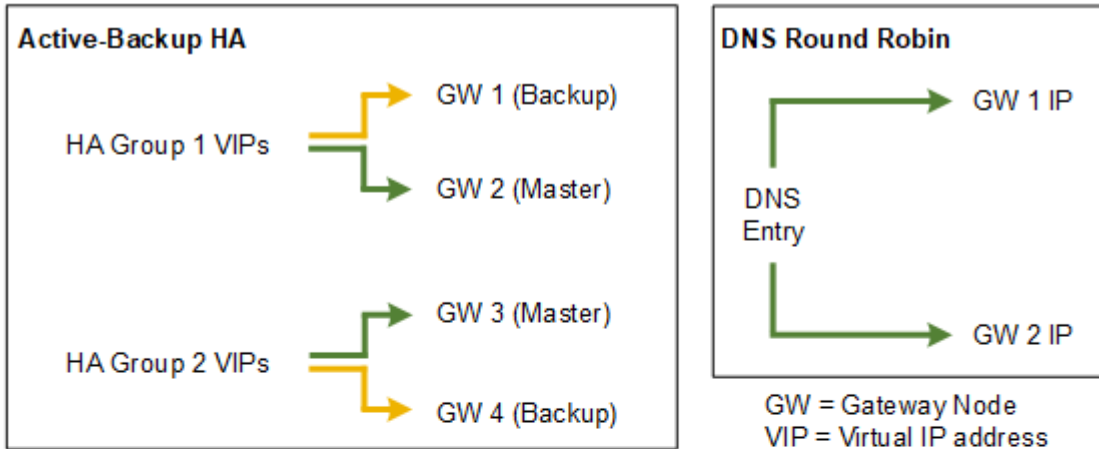
CLB サービスに障害が発生しても、HA グループ内でフェイルオーバーはトリガーされません。



CLB サービスは廃止されました。

HA グループの設定オプション

次の図は、HA グループのさまざまな構成例を示しています。各オプションには長所と短所があります。



「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	<ul style="list-style-type: none"> 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。 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> • 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。 	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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。 	<ul style="list-style-type: none"> • 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。

High Availability Groups

High availability (HA) groups allow multiple nodes to participate in an active-backup group. HA groups maintain virtual IP addresses on the active node and switch to a backup node automatically if a node fails.

+ Create Edit Remove

Name	Description	Virtual IP Addresses	Interfaces
No HA groups found.			

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。

Add Interfaces to High Availability Group

Select interfaces to include in the HA group. All interfaces must be in the same network subnet.

Add to HA group	Node Name	Interface	IPv4 Subnet	Unavailable Reason
	g140-g1	eth0	172.16.0.0/21	This IP address is not in the same subnet as the selected interfaces
	g140-g1	eth2	47.47.0.0/21	This IP address is not in the same subnet as the selected interfaces
	g140-g2	eth0	172.16.0.0/21	This IP address is not in the same subnet as the selected interfaces
	g140-g2	eth2	47.47.0.0/21	This IP address is not in the same subnet as the selected interfaces
	g140-g3	eth0	172.16.0.0/21	This IP address is not in the same subnet as the selected interfaces
<input checked="" type="checkbox"/>	g140-g3	eth2	192.168.0.0/21	
	g140-g4	eth0	172.16.0.0/21	This IP address is not in the same subnet as the selected interfaces
<input checked="" type="checkbox"/>	g140-g4	eth2	192.168.0.0/21	

There are 2 interfaces selected.

Cancel Apply

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。

Add Interfaces to High Availability Group

Select interfaces to include in the HA group. All interfaces must be in the same network subnet.

Add to HA group	Node Name	Interface	IPv4 Subnet	Unavailable Reason
<input checked="" type="checkbox"/>	DC1-ADM1	eth0	10.96.100.0/23	
<input checked="" type="checkbox"/>	DC1-G1	eth0	10.96.100.0/23	
<input checked="" type="checkbox"/>	DC2-ADM1	eth0	10.96.100.0/23	

There are 3 interfaces selected.

Attention: You have selected nodes of different types that run different services. If a failover occurs, only the services common to all node types will be available on the virtual IPs.

Cancel

Apply

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。

Create High Availability Group

High Availability Group

Name

Description

Interfaces

Select interfaces to include in the HA group. All interfaces must be in the same network subnet.

Select Interfaces

Node Name	Interface	IPv4 Subnet	Preferred Master
g140-g1	eth2	47.47.0.0/21	<input checked="" type="radio"/>
g140-g2	eth2	47.47.0.0/21	<input type="radio"/>

Displaying 2 interfaces.

Virtual IP Addresses

Virtual IP Subnet: 47.47.0.0/21. All virtual IP addresses must be within this subnet. There must be at least 1 and no more than 10 virtual IP addresses.

Virtual IP Address 1



Cancel

Save

- 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。

- 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。

High Availability Groups

High availability (HA) groups allow multiple nodes to participate in an active-backup group. HA groups maintain virtual IP addresses on the active node and switch to a backup node automatically if a node fails.

	Name	Description	Virtual IP Addresses	Interfaces
<input type="radio"/>	HA Group 1		47.47.4.219	g140-adm1:eth2 (preferred Master) g140-g1:eth2
<input type="radio"/>	HA Group 2		47.47.4.218 47.47.4.217	g140-g1:eth2 (preferred Master) g140-g2:eth2

Displaying 2 HA groups.

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。

Add Interfaces to High Availability Group

Select interfaces to include in the HA group. All interfaces must be in the same network subnet.

Add to HA group	Node Name	Interface	IPv4 Subnet	Unavailable Reason
<input type="checkbox"/>	g140-g1	eth0	172.16.0.0/21	This IP address is not in the same subnet as the selected interfaces
<input type="checkbox"/>	g140-g1	eth2	47.47.0.0/21	This IP address is not in the same subnet as the selected interfaces
<input type="checkbox"/>	g140-g2	eth0	172.16.0.0/21	This IP address is not in the same subnet as the selected interfaces
<input type="checkbox"/>	g140-g2	eth2	47.47.0.0/21	This IP address is not in the same subnet as the selected interfaces
<input type="checkbox"/>	g140-g3	eth0	172.16.0.0/21	This IP address is not in the same subnet as the selected interfaces
<input checked="" type="checkbox"/>	g140-g3	eth2	192.168.0.0/21	
<input type="checkbox"/>	g140-g4	eth0	172.16.0.0/21	This IP address is not in the same subnet as the selected interfaces
<input checked="" type="checkbox"/>	g140-g4	eth2	192.168.0.0/21	

There are 2 interfaces selected.

Cancel

Apply

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。

Edit High Availability Group 'HA Group - Admin Nodes'

High Availability Group

Name

Description

Interfaces

Select interfaces to include in the HA group. All interfaces must be in the same network subnet.

Node Name	Interface	IPv4 Subnet	Preferred Master
DC1-ADM1	eth0	10.96.100.0/23	<input checked="" type="radio"/>
DC2-ADM1	eth0	10.96.100.0/23	<input type="radio"/>

Displaying 2 interfaces.

Virtual IP Addresses

Virtual IP Subnet: 10.96.100.0/23. All virtual IP addresses must be within this subnet. There must be at least 1 and no more than 10 virtual IP addresses.

Virtual IP Address 1



Cancel

Save

- 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。

- 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。

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。

High Availability Groups

High availability (HA) groups allow multiple nodes to participate in an active-backup group. HA groups maintain virtual IP addresses on the active node and switch to a backup node automatically if a node fails.

	Name	Description	Virtual IP Addresses	Interfaces
<input type="radio"/>	HA Group 1		47.47.4.219	g140-adm1:eth2 (preferred Master) g140-g1:eth2
<input type="radio"/>	HA Group 2		47.47.4.218 47.47.4.217	g140-g1:eth2 (preferred Master) g140-g2:eth2

Displaying 2 HA groups.

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。

⚠ Warning

Delete High Availability Group

Are you sure you want to delete High Availability Group 'HA group 1'?

Cancel

OK

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。

Endpoint Domain Names

Virtual Hosted-Style Requests

Enable support of S3 virtual hosted-style requests by specifying API endpoint domain names. Support is disabled if this list is empty. Examples: s3.example.com, s3.example.co.uk, s3-east.example.com

Endpoint 1 ×

Endpoint 2 + ×

Save

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できるようになります `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。

Network Options



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。

Network Options

Prevent Client Modification

Enable HTTP Connection

Network Transfer Encryption AES128-SHA AES256-SHA

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。

Node Information	
Name	SGA-lab11
Type	Storage Node
ID	0b583829-6659-4c6e-b2d0-31461d22ba67
Connection State	✔ Connected
Software Version	11.4.0 (build 20200527.0043.61839a2)
IP Addresses	192.168.4.138, 10.224.4.138, 169.254.0.1 Show less
Interface	IP Address
eth0	192.168.4.138
eth0	fd20:331:331:0:2a0:98ff:fea1:831d
eth0	fe80::2a0:98ff:fea1:831d
eth1	10.224.4.138
eth1	fd20:327:327:0:280:e5ff:fe43:a99c
eth1	fd20:8b1e:b255:8154:280:e5ff:fe43:a99c
eth1	fe80::280:e5ff:fe43:a99c
hic2	192.168.4.138
hic4	192.168.4.138
mtc1	10.224.4.138
mtc2	169.254.0.1

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。

Network Options

Prevent Client Modification  

Enable HTTP Connection  

Network Transfer Encryption  AES128-SHA AES256-SHA

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。
 - サーバ証明書：カスタムサーバ証明書ファイル (.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あります。

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。
 - サーバ証明書：カスタムサーバ証明書ファイル (.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. 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 クライアントに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。

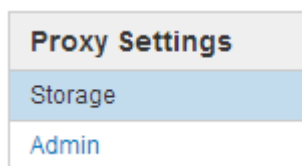
このタスクについて

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。

Storage Proxy Settings

If you are using platform services or Cloud Storage Pools, you can configure a non-transparent proxy server between Storage Nodes and the external S3 endpoints.

Enable Storage Proxy

Protocol HTTP SOCKS5

Hostname

Port (optional)

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せん。

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

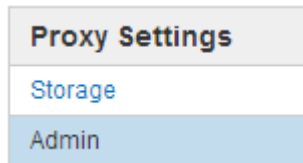
設定できる管理プロキシは1つです。

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。

Admin Proxy Settings

If you send AutoSupport messages using HTTPS or HTTP, you can configure a non-transparent proxy server between Admin Nodes and technical support.

Enable Admin Proxy	<input checked="" type="checkbox"/>
Hostname	<input type="text" value="myproxy.example.com"/>
Port	<input type="text" value="8080"/>
Username (optional)	<input type="text" value="root"/>
Password (optional)	<input type="password" value="••••••••"/>
<input type="button" value="Save"/>	

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
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。

Traffic Classification Policies

Traffic classification policies can be used to identify network traffic for metrics reporting and optional traffic limiting.




The screenshot shows a user interface for managing Traffic Classification Policies. At the top, there is a toolbar with four buttons: '+ Create', 'Edit', 'Remove', and 'Metrics'. Below the toolbar is a table with three columns: 'Name', 'Description', and 'ID'. The table is currently empty, and the text 'No policies found.' is displayed below it.

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。

Create Traffic Classification Policy

Policy

Name 

Description

Matching Rules

Traffic that matches any rule is included in the policy.

Type	Inverse Match	Match Value
------	---------------	-------------

No matching rules found.

Limits (Optional)

Type	Value	Units
------	-------	-------

No limits found.

Cancel

Save

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。



Create Matching Rule

Matching Rules

Type  -- Choose One -- 

Match Value  Choose type before providing match value

Inverse Match 

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。

+ Create Edit Remove		
Type	Inverse Match	Match Value
Bucket Regex	✓	control-ld+


Displaying 1 matching rule.

Limits (Optional)


+ Create Edit Remove			
Type	Value	Type	Units
No limits found.			

Cancel Save

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。

Create Limit

Limits (Optional)

Type 

Aggregate rate limits in use. Per-request rate limits are not available. 

Value 

Cancel Apply

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。

Type	Inverse Match	Match Value
Bucket Regex	✓	control-ld+

Displaying 1 matching rule.

Limits (Optional)

Type	Value	Units
Aggregate Bandwidth Out	10000000000	Bytes/Second

Displaying 1 limit.

Cancel Save

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。

Traffic Classification Policies

Traffic classification policies can be used to identify network traffic for metrics reporting and optional traffic limiting.

Name	Description	ID
ERP Traffic Control	Manage ERP traffic into the grid	cd9afbc7-b85e-4208-b6f8-7e8a79e2c574
Fabric Pools	Monitor Fabric Pools	223b0cbb-6968-4646-b32d-7665bddc894b

Displaying 2 traffic classification policies.

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。

Traffic Classification Policies

Traffic classification policies can be used to identify network traffic for metrics reporting and optional traffic limiting.

<input type="button" value="+ Create"/> <input type="button" value="Edit"/> <input type="button" value="Remove"/> <input type="button" value="Metrics"/>			
	Name	Description	ID
<input type="radio"/>	ERP Traffic Control	Manage ERP traffic into the grid	cd9afbc7-b85e-4208-b6f8-7e8a79e2c574
<input checked="" type="radio"/>	Fabric Pools	Monitor Fabric Pools	223b0cbb-6968-4646-b32d-7665bddc894b

Displaying 2 traffic classification policies.

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。

Edit Traffic Classification Policy "Fabric Pools"

Policy

Name 

Fabric Pools

Description (optional)

Monitor Fabric Pools

Matching Rules

Traffic that matches any rule is included in the policy.

 Create	 Edit	 Remove
Type	Inverse Match	Match Value
<input checked="" type="radio"/> CIDR		10.10.152.0/24
Displaying 1 matching rule.		

Limits (Optional)

 Create	 Edit	 Remove
Type	Value	Units
No limits found.		

Cancel

Save

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。

Traffic Classification Policies

Traffic classification policies can be used to identify network traffic for metrics reporting and optional traffic limiting.

Name	Description	ID
ERP Traffic Control	Manage ERP traffic into the grid	cd9afbc7-b85e-4208-b6f8-7e8a79e2c574
Fabric Pools	Monitor Fabric Pools	223b0cbb-6968-4646-b32d-7665bddc894b

Displaying 2 traffic classification policies.

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。

Traffic Classification Policies

Traffic classification policies can be used to identify network traffic for metrics reporting and optional traffic limiting.

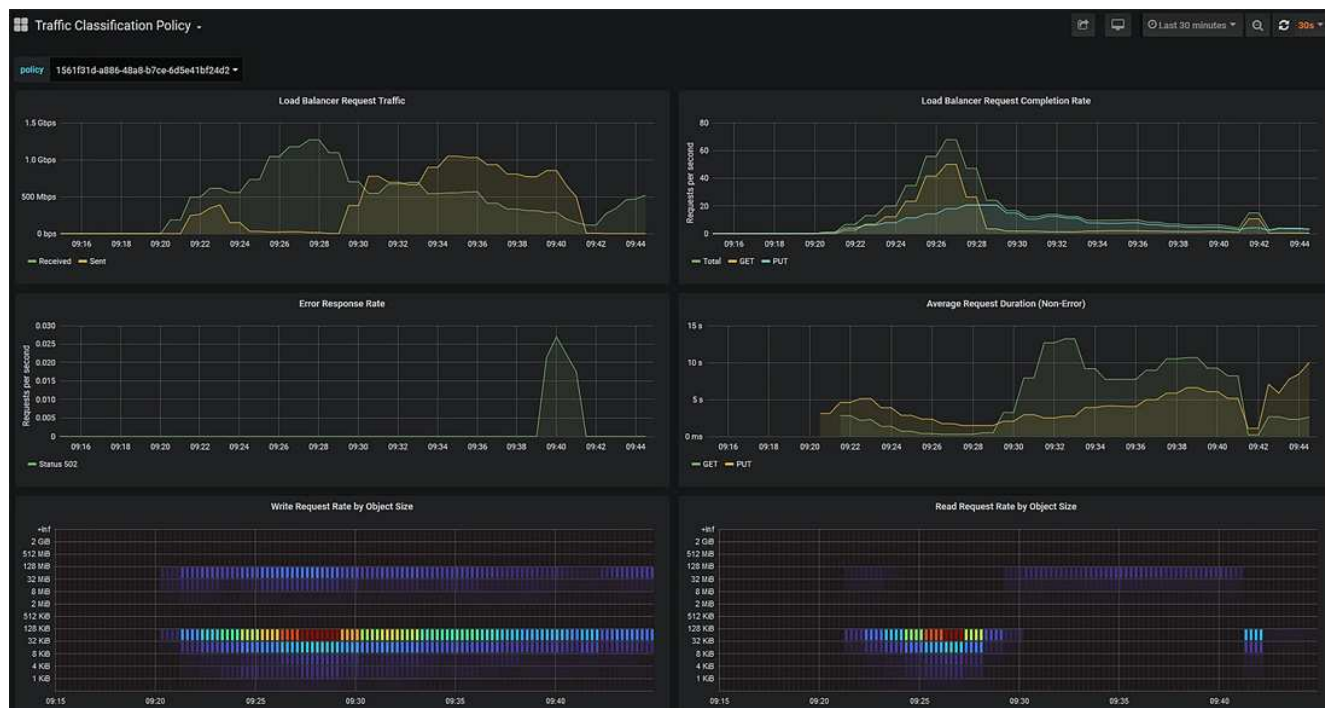


Name	Description	ID
<input type="radio"/> ERP Traffic Control	Manage ERP traffic into the grid	cd9afbc7-b85e-4208-b6f8-7e8a79e2c574
<input checked="" type="radio"/> Fabric Pools	Monitor Fabric Pools	223b0cbb-6968-4646-b32d-7665bddc894b

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。

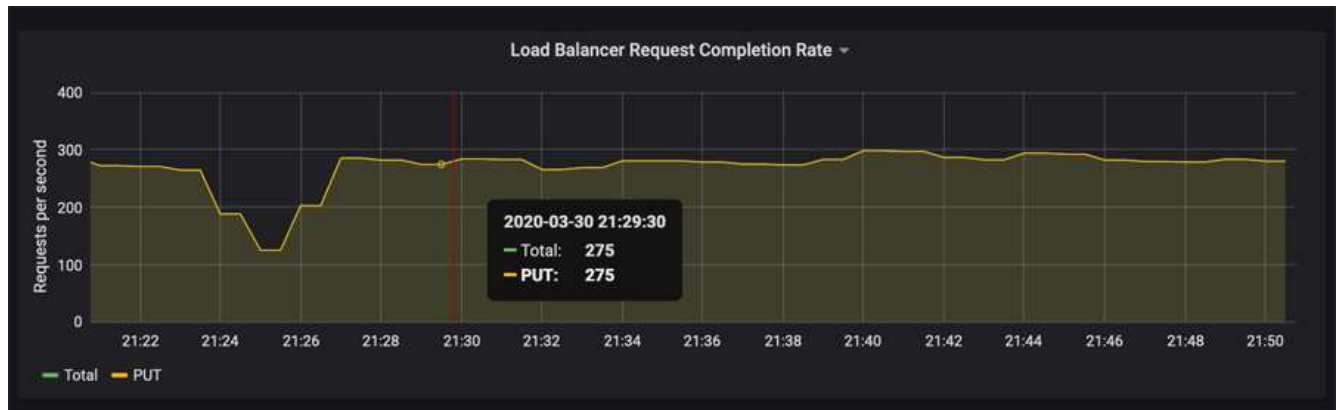
その他のポリシーを選択して表示するには、* policy * プルダウンを使用します。



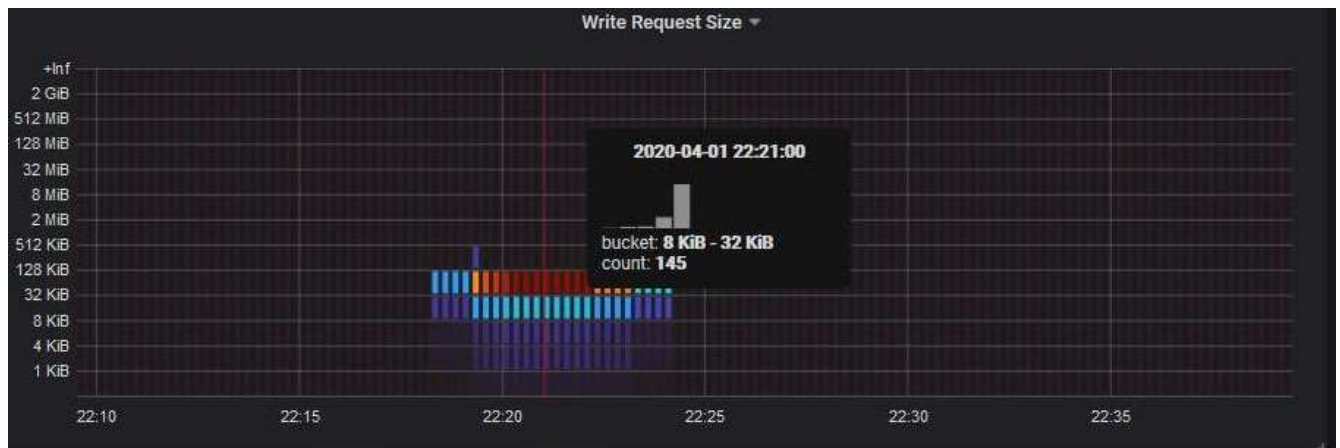
Web ページには次のグラフが表示されます。

- **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（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。



- 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。



- 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。

- または、* Support *メニューからグラフにアクセスします。

- [* Support*]>[* Tools]>[* Metrics]を選択します。
- ページの * Grafana * セクションで、 * Traffic Classification Policy * を選択します。
- 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。

- 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

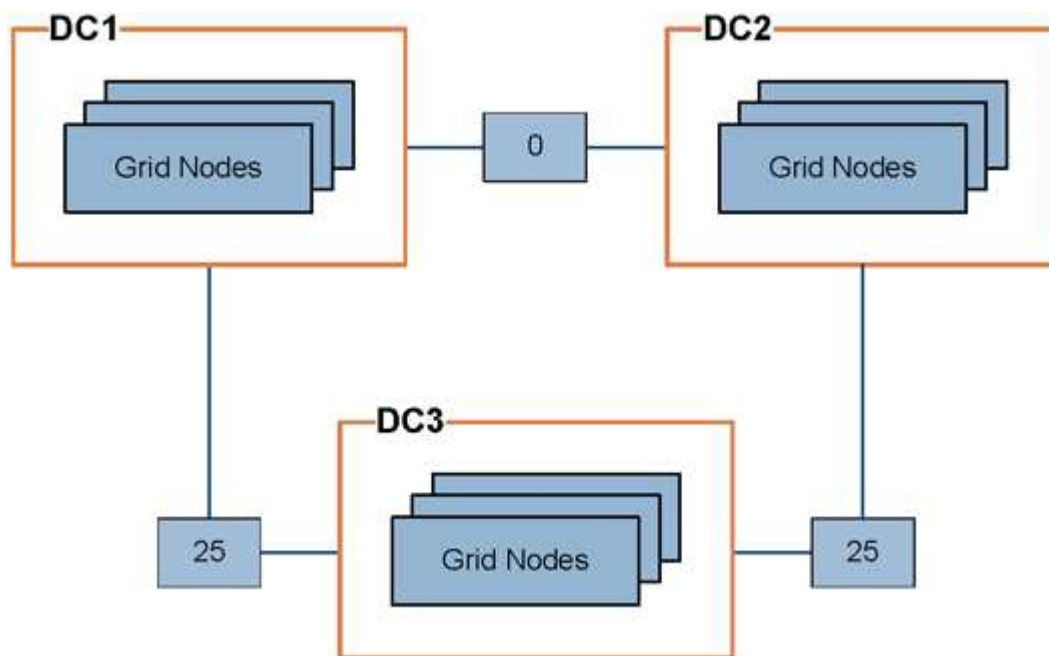
たサービスを提供するデータセンターサイトの優先順位を決定できます。サイト間のレイテンシに合わせてリンクコストを調整できます。

- 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せん。



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。

Link Cost
Updated: 2021-03-29 12:28:41 EDT

Site Names (1 - 2 of 2)

Site ID	Site Name	Actions
10	Data Center 1	
20	Data Center 2	

Show 50 Records Per Page Previous « 1 » Next

Link Costs

Link Source	Link Destination	Link Cost	Actions
10	20	20	

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。

The AutoSupport feature is disabled. You should enable AutoSupport to allow StorageGRID to send health and status messages to technical support for proactive monitoring and troubleshooting.



「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ーです。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

The AutoSupport feature enables your StorageGRID system to send periodic and event-driven health and status messages to technical support to allow proactive monitoring and troubleshooting. StorageGRID AutoSupport also enables the use of Active IQ for predictive recommendations.

Settings Results

Protocol Details

Protocol ? HTTPS HTTP SMTP

NetApp Support Certificate Validation ? Use NetApp support certificate ▼

AutoSupport Details

Enable Weekly AutoSupport ?

Enable Event-Triggered AutoSupport ?

Enable AutoSupport on Demand ?

Additional AutoSupport Destination

Enable Additional AutoSupport Destination ?

Save Send User-Triggered AutoSupport

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

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。

The screenshot shows the 'Settings' tab for AutoSupport. Under 'Protocol Details', the 'Protocol' is set to 'HTTPS'. The 'NetApp Support Certificate Validation' dropdown menu is open, with 'Use NetApp support certificate' selected. Below this, there are three checkboxes under 'AutoSupport Details': 'Enable Weekly AutoSupport' (checked), 'Enable Event-Triggered AutoSupport' (unchecked), and 'Enable AutoSupport on Demand' (unchecked). Under 'Additional AutoSupport Destination', 'Enable Additional AutoSupport Destination' is unchecked. At the bottom, there are 'Save' and 'Send User-Triggered AutoSupport' buttons.

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。

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。

The screenshot shows a web interface for configuring AutoSupport. At the top, there are two tabs: "Settings" and "Results". Below the tabs is a section titled "Protocol Details". In this section, there are three radio buttons for "Protocol": "HTTPS" (which is selected and highlighted with a yellow box), "HTTP", and "SMTP". Below the radio buttons is a dropdown menu for "NetApp Support Certificate Validation" with the selected option "Use NetApp support certificate". Below the "Protocol Details" section is another section titled "AutoSupport Details". In this section, there are three checkboxes: "Enable Weekly AutoSupport" (checked and highlighted with a yellow box), "Enable Event-Triggered AutoSupport" (unchecked), and "Enable AutoSupport on Demand" (checked and highlighted with a yellow box). Below the "AutoSupport Details" section is a section titled "Additional AutoSupport Destination". In this section, there is one checkbox: "Enable Additional AutoSupport Destination" (unchecked). At the bottom of the page, there are two buttons: "Save" and "Send User-Triggered AutoSupport".

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。

Settings	Results
Weekly AutoSupport	
Next Scheduled Time ?	2021-02-12 00:20:00 EST
Most Recent Result ?	Idle (NetApp Support)
Last Successful Time ?	N/A (NetApp Support)

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。

Settings
Results

Protocol Details

Protocol ? HTTPS HTTP SMTP

NetApp Support Certificate Validation ? Use NetApp support certificate ▼

AutoSupport Details

Enable Weekly AutoSupport ?

Enable Event-Triggered AutoSupport ?

AutoSupport On Demand can only be enabled when the protocol is HTTPS and Weekly AutoSupport is enabled. When you enable AutoSupport on Demand, technical support can request that your StorageGRID system send AutoSupport messages automatically.

Additional AutoSupport Destination

Enable Additional AutoSupport Destination ?

Save
Send User-Triggered AutoSupport

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。

Settings
Results

Protocol Details

Protocol ? HTTPS HTTP SMTP

NetApp Support Certificate Validation ? Use NetApp support certificate ▼

AutoSupport Details

Enable Weekly AutoSupport ?

Enable Event-Triggered AutoSupport ?

AutoSupport On Demand can only be enabled when the protocol is HTTPS and Weekly AutoSupport is enabled. When you enable AutoSupport on Demand, technical support can request that your StorageGRID system send AutoSupport messages automatically.

Additional AutoSupport Destination

Enable Additional AutoSupport Destination ?

Save
Send User-Triggered AutoSupport

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。

Additional AutoSupport Destination

Enable Additional AutoSupport Destination

Hostname

Port

Certificate Validation

You are not using a TLS certificate to secure the connection to the additional AutoSupport destination.

Save

Send User-Triggered AutoSupport

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。

Additional AutoSupport Destination

Enable Additional AutoSupport Destination

Hostname

Port

Certificate Validation

CA Bundle

```
-----BEGIN CERTIFICATE-----
abcdefghijklmnopqrstuvwxyz123456780ABCDEFGHIJKL
123456/7890ABCDEFabcdefghijklmnopqrstuvwxyzABCD
-----END CERTIFICATE-----
```

- [* 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、ストレージアプリケーション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"



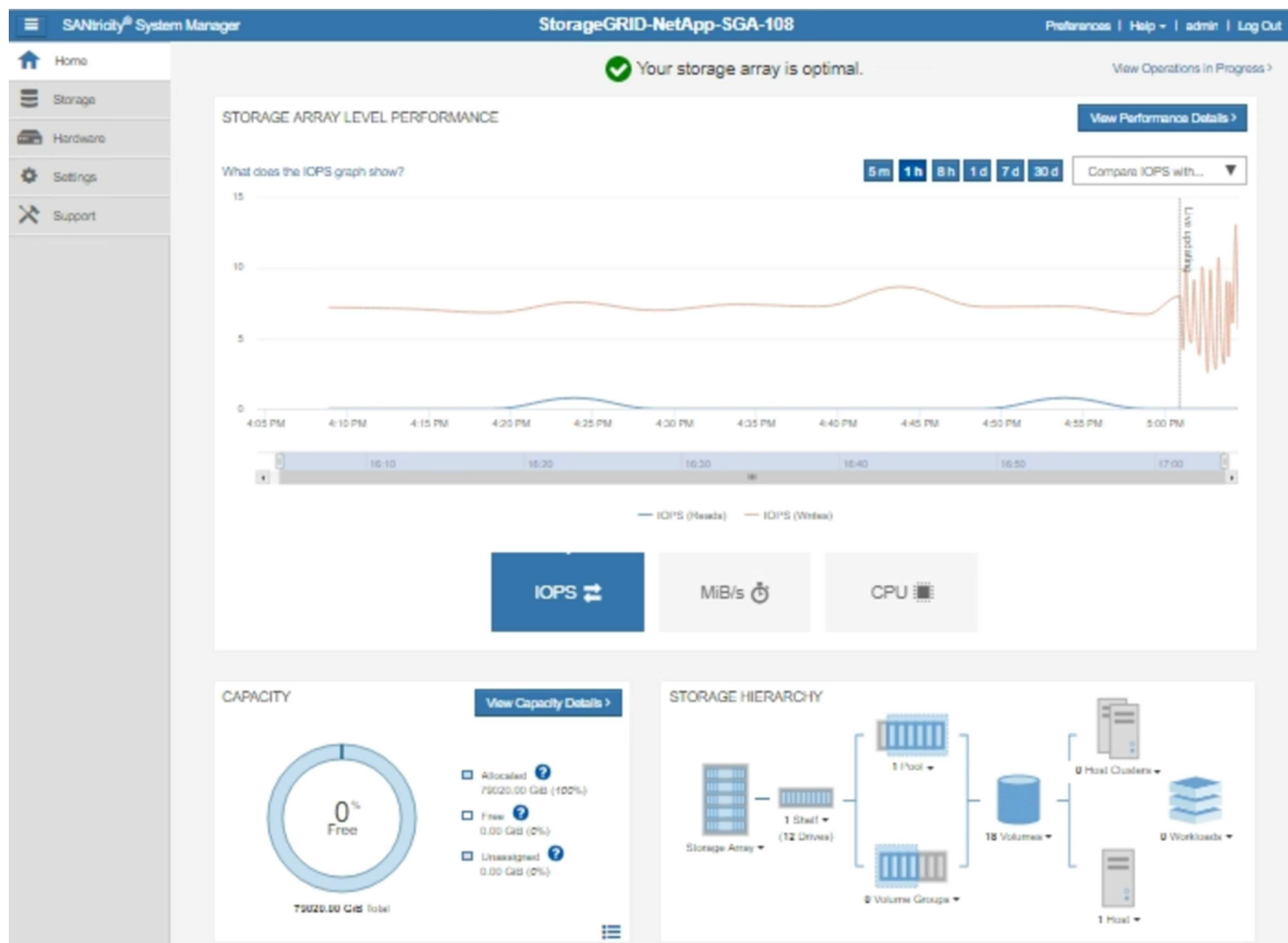
この手順 は、E シリーズ AutoSupport メッセージ用に StorageGRID プロキシサーバを設定するためだけに使用します。EシリーズAutoSupport の設定情報の詳細については、Eシリーズのドキュメントセンターを参照してください。

["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。

Support Resources

Diagnostics

AutoSupport

AutoSupport operations

AutoSupport status: Enabled 

[Enable/Disable AutoSupport Features](#)

AutoSupport proactively monitors the health of your storage array and automatically sends support data ("dispatches") to the support team.

[Configure AutoSupport Delivery Method](#)

Connect to the support team via HTTPS, HTTP or Mail (SMTP) server delivery methods.

[Schedule AutoSupport Dispatches](#)

AutoSupport dispatches are sent daily at 03:06 PM UTC and weekly at 07:39 AM UTC on Thursday.

[Send AutoSupport Dispatch](#)

Automatically sends the support team a dispatch to troubleshoot system issues without waiting for periodic dispatches.

[View AutoSupport Log](#)

The AutoSupport log provides information about status, dispatch history, and errors encountered during delivery of AutoSupport dispatches.

[Enable AutoSupport Maintenance Window](#)

Enable AutoSupport Maintenance window to allow maintenance activities to be performed on the storage array without generating support cases.

[Disable AutoSupport Maintenance Window](#)

Disable AutoSupport Maintenance window to allow the storage array to generate support cases on component failures and other destructive actions.

5. AutoSupport 配信方法の設定 * を選択します。

AutoSupport 配信方法の設定ページが表示されます。

Configure AutoSupport Delivery Method ✕

Select AutoSupport dispatch delivery method...

HTTPS
 HTTP
 Email

HTTPS delivery settings Show destination address

Connect to support team...

Directly ?
 via Proxy server ?

Host address ?

Port number ?

My proxy server requires authentication
 via Proxy auto-configuration script (PAC) ?

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 プロキシサーバーのポート番号です。

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。

AutoSupport

The AutoSupport feature enables your StorageGRID system to send periodic and event-driven health and status messages to technical support to allow proactive monitoring and troubleshooting. StorageGRID AutoSupport also enables the use of Active IQ for predictive recommendations.



The screenshot shows a web interface with two tabs: 'Settings' and 'Results'. The 'Results' tab is selected and highlighted with a yellow border. Below the tabs, there are three sections: 'Weekly AutoSupport', 'Event-Triggered AutoSupport', and 'User-Triggered AutoSupport'. Each section contains two rows of data: 'Most Recent Result' and 'Last Successful Time'. The 'User-Triggered AutoSupport' section has a yellow border around its 'Most Recent Result' row, which shows 'Failed (NetApp Support)'. The 'AutoSupport On Demand' section is at the bottom and contains two rows of data.

Category	Property	Value
Weekly AutoSupport	Next Scheduled Time	2020-12-11 23:30:00 EST
	Most Recent Result	Idle (NetApp Support)
	Last Successful Time	N/A (NetApp Support)
Event-Triggered AutoSupport	Most Recent Result	N/A (NetApp Support)
	Last Successful Time	N/A (NetApp Support)
User-Triggered AutoSupport	Most Recent Result	Failed (NetApp Support)
	Last Successful Time	N/A (NetApp Support)
AutoSupport On Demand	Most Recent Result	N/A (NetApp Support)
	Last Successful Time	N/A (NetApp Support)

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. 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、およびサービスヤ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。

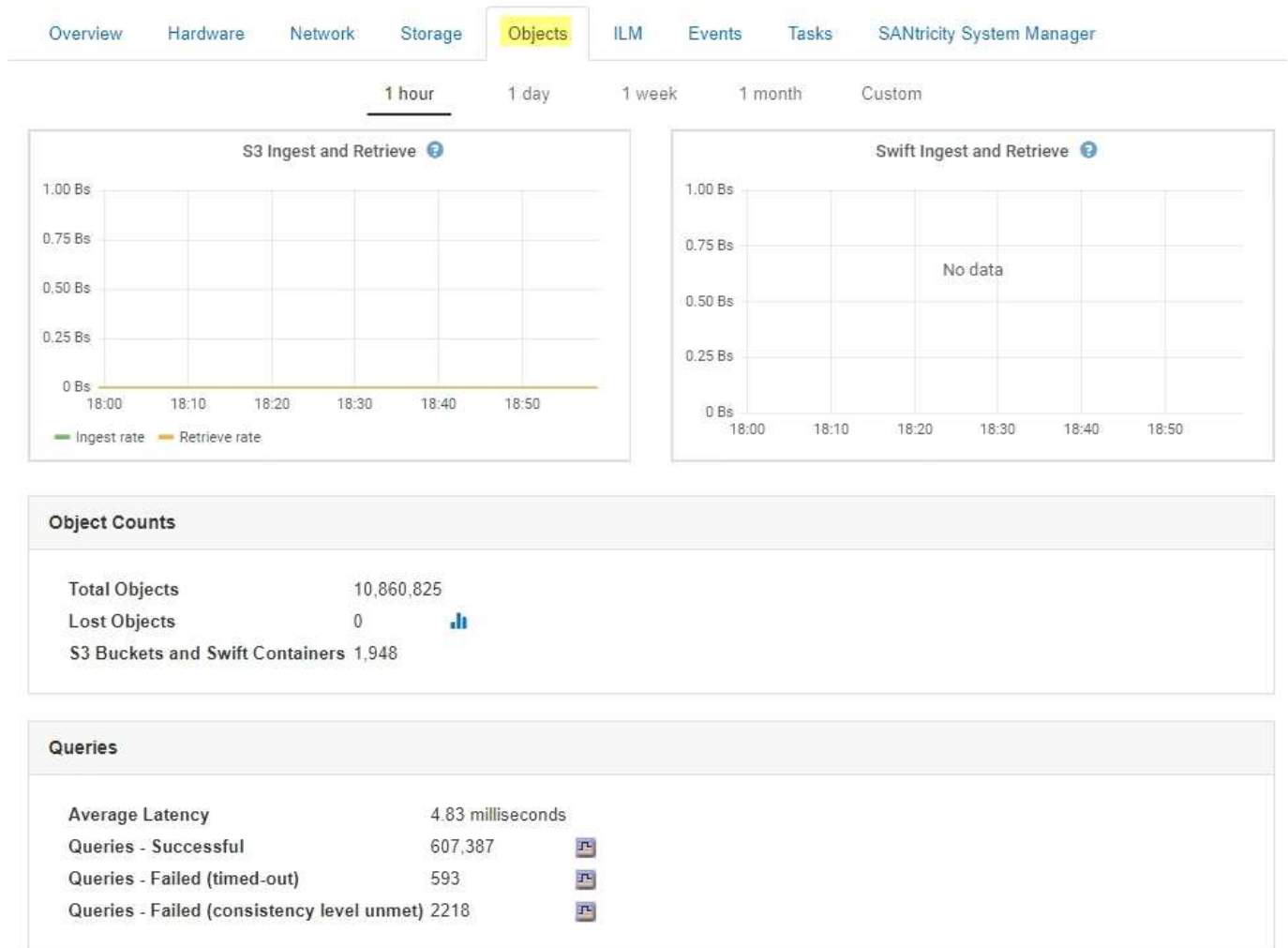
DDS サービスとは

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 の健全性を監視できます。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られている一意な「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全性を監視できます。メタデータストアの健全性は、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](#)".

Storage Options
Overview
Configuration



Storage Options Overview

Updated: 2019-03-22 12:49:16 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

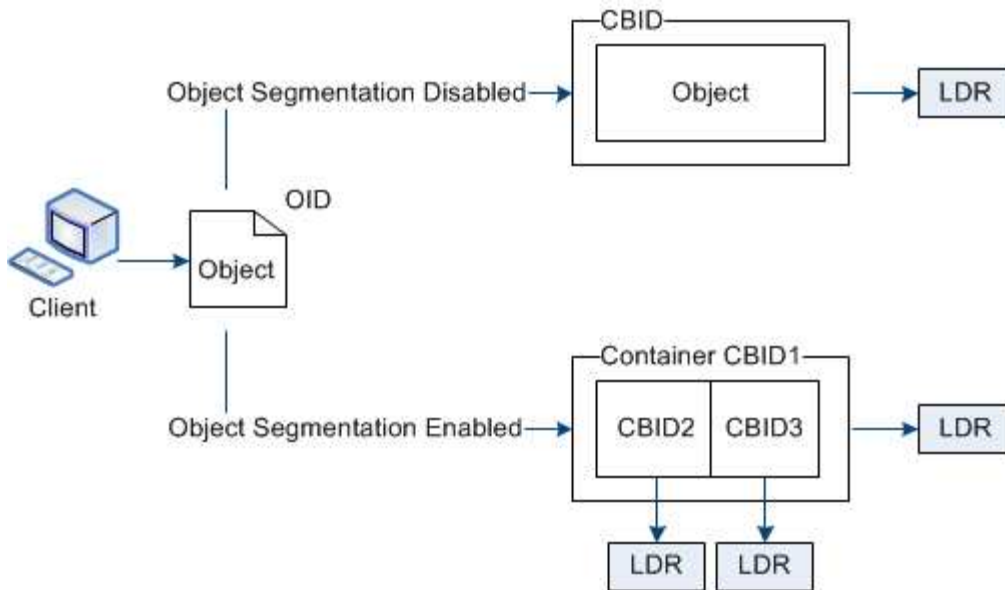
Ports

Description	Settings
CLB S3 Port	8082
CLB Swift Port	8083
LDR S3 Port	18082
LDR Swift Port	18083

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

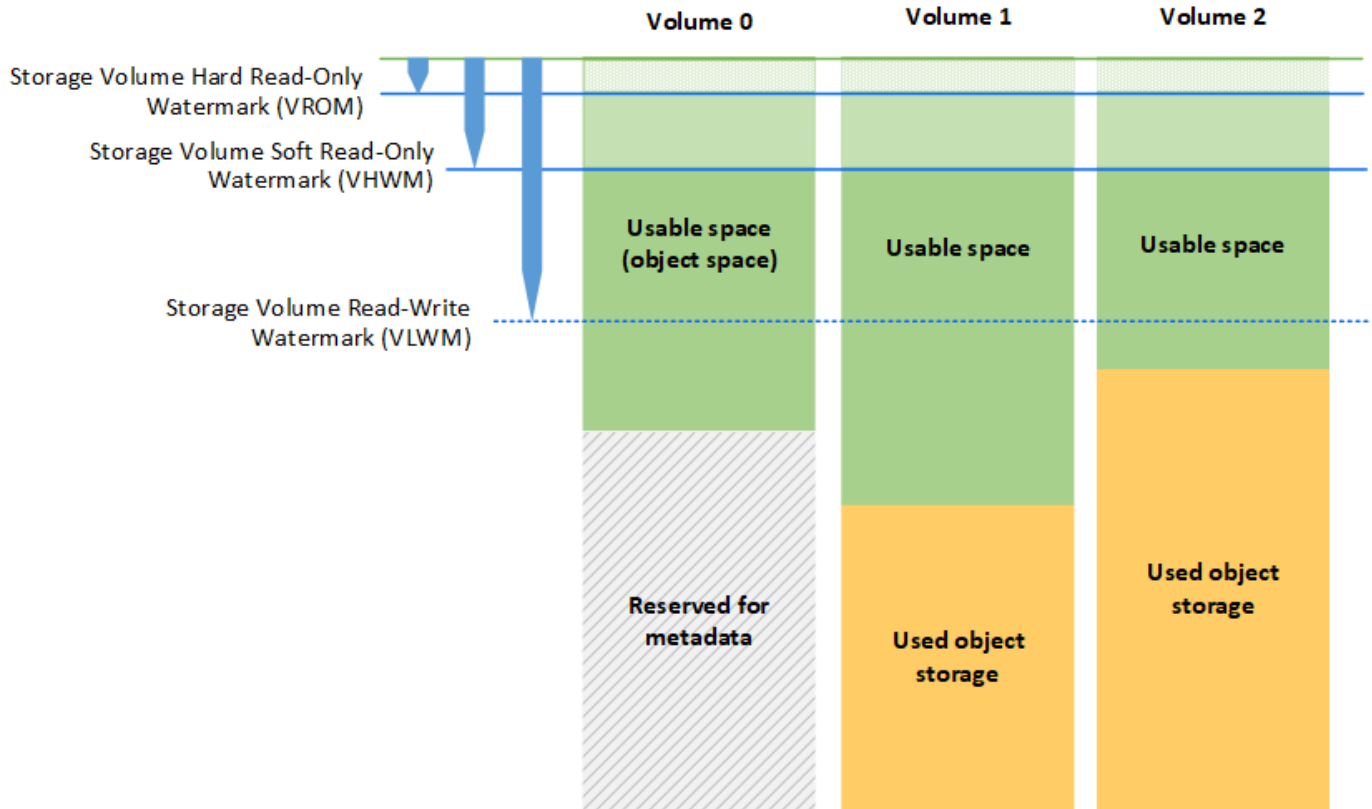
Object Segmentation

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

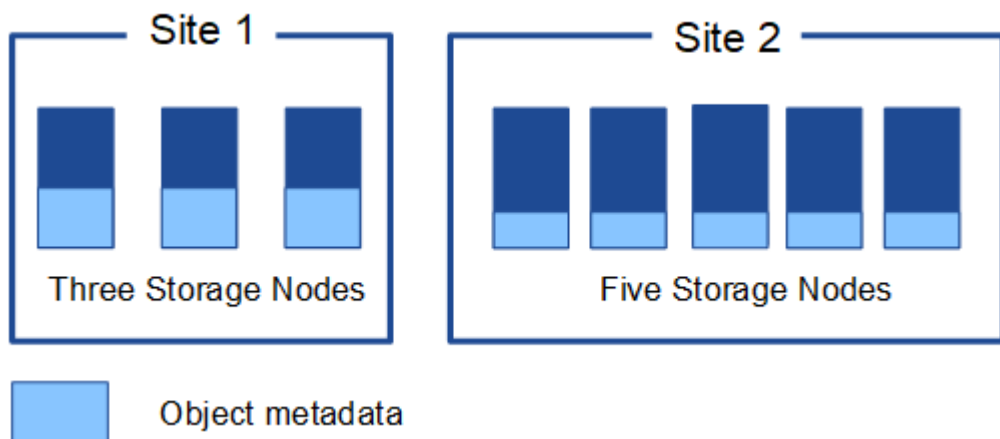
Swift コンテナの名前、テナントアカウントの名前または ID、オブジェクトの論理サイズ、オブジェクトの作成日時など)、オブジェクトが最後に変更された日時。

- 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

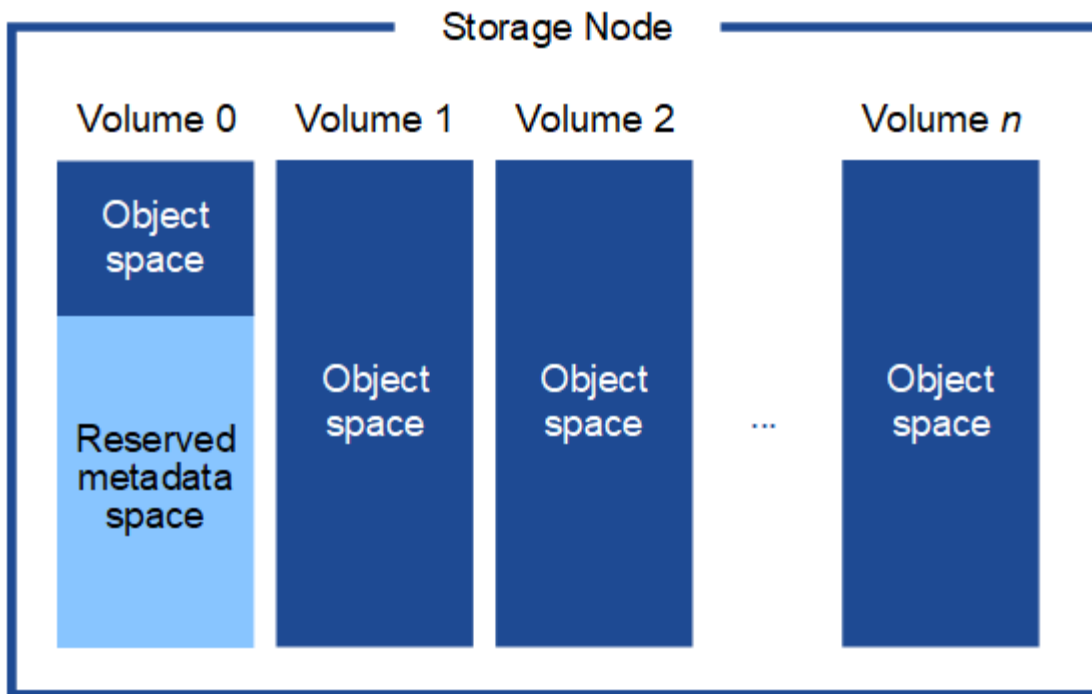
StorageGRID は Cassandra データベースにオブジェクトメタデータを保持し、Cassandra データベースはオブジェクトデータとは別に格納されます。冗長性を確保し、オブジェクトメタデータを損失から保護するために、StorageGRID は各サイトのシステム内のすべてのオブジェクトにメタデータのコピーを 3 つずつ格納します。オブジェクトメタデータの 3 つのコピーが各サイトのすべてのストレージノードに均等に分散されます。

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）専用で使用されます。

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。



Storage Options Overview

Updated: 2021-02-23 11:58:33 MST

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	8,000 GB

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

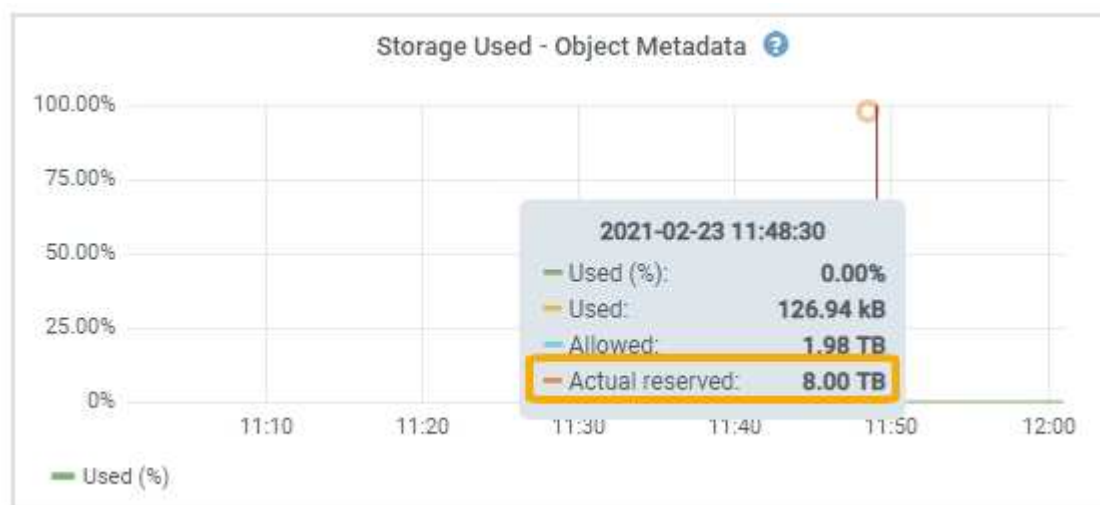
システム全体の Metadata Reserved Space 設定とは異なり、オブジェクトメタデータ用の実際のリザーブスペースは、ストレージノードごとに決定されます。ある特定のストレージノードについて、メタデータ用に実際にリザーブされるスペースは、ノードのボリューム 0 のサイズとシステム全体の * Metadata Reserved Space * 設定によって異なります。

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： <ul style="list-style-type: none"> • 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。

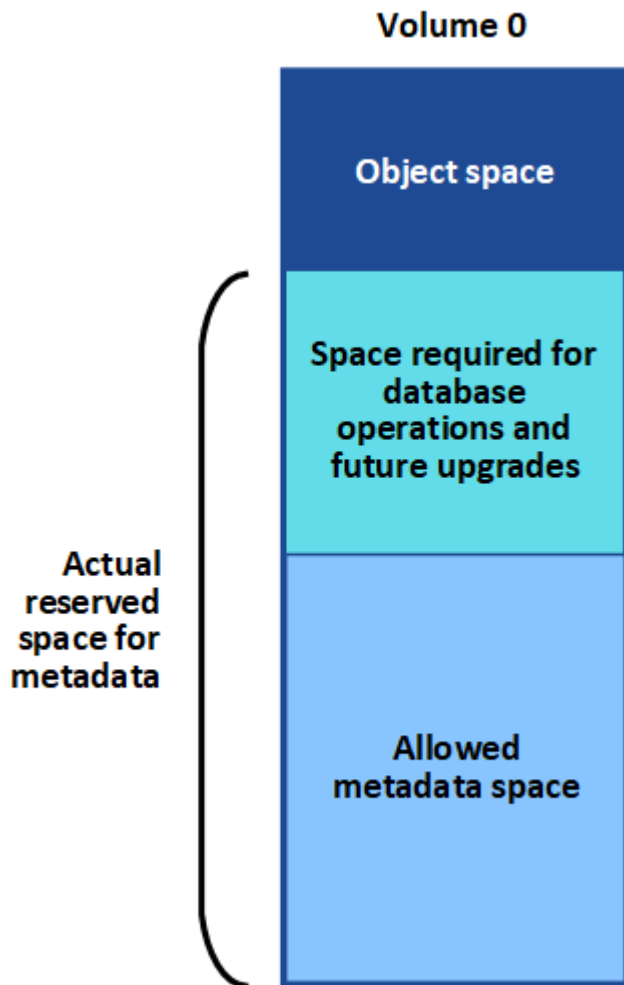
- システム全体の * Metadata Reserved Space * が 8TB に設定されている (ストレージノードごとに128GB を超えるRAMが搭載されている場合、この値はStorageGRID 11.5の新規インストールでのデフォルト値で

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。

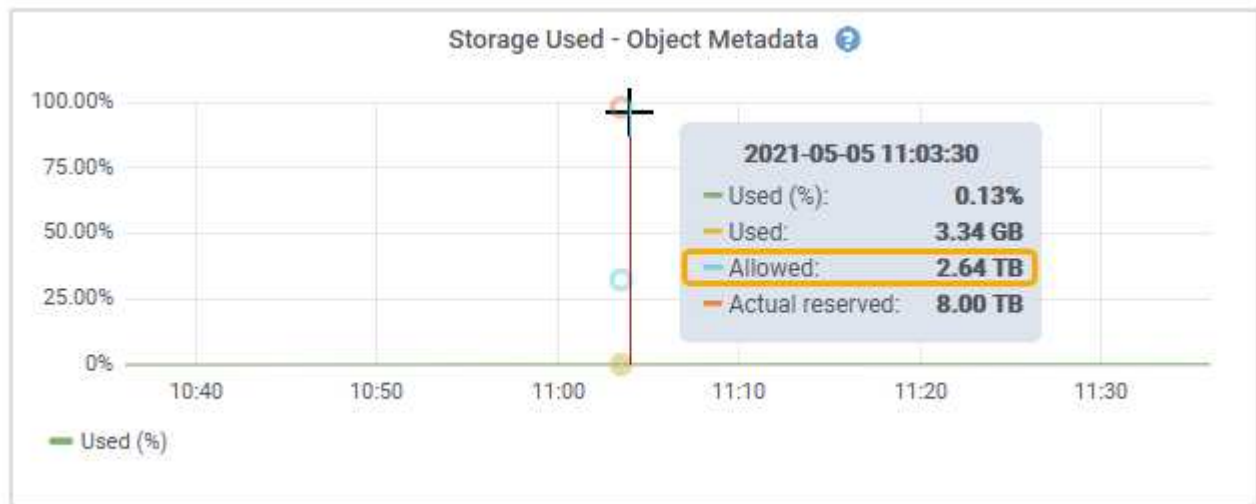
メタデータ用にリザーブされている実際のスペース	許可されているメタデータスペースです
4TB以下	メタデータ用にリザーブされている実際のスペースの 60%。最大 1.98 TB
4TBを超える	(メタデータ用に実際にリザーブされるスペース-1TB) ×60%、最大2.64 TB



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2.64TBです。（実際のリザーブスペースの最大値です）。

サイズの異なるストレージノードがオブジェクト容量に与える影響

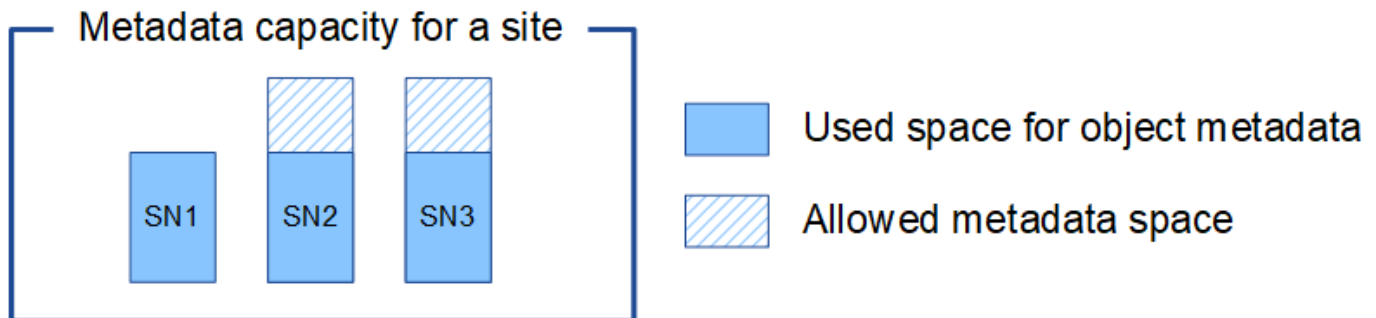
前述したように、StorageGRID は各サイトのストレージノードにオブジェクトメタデータを均等に分散します。このため、サイトにサイズが異なるストレージノードがある場合、サイトで一番小さいノードがサイトのメタデータ容量を決定します。

次の例を考えてみましょう。

- サイズの異なる 3 つのストレージノードを含む単一サイトのグリッドがある。
- Metadata Reserved Space * の設定は 4TB です。
- ストレージノードには、リザーブされている実際のメタデータスペースと許可されているメタデータスペースについて、次の値があります。

ストレージノード	ボリューム 0 のサイズ	リザーブされている実際のメタデータスペースです	許可されているメタデータスペースです
SN1.	2.2 TB	2.2 TB	1.32TB をサポートしません
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。

Stored Object Options

Compress Stored Objects

Stored Object Encryption None AES-128 AES-256

Stored Object Hashing SHA-1 SHA-256

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。

Stored Object Options

Compress Stored Objects  

Stored Object Encryption  None AES-128 AES-256

Stored Object Hashing  SHA-1 SHA-256

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。

Stored Object Options

Compress Stored Objects  

Stored Object Encryption  None AES-128 AES-256

Stored Object Hashing  SHA-1 SHA-256

3. [保存 (Save)]をクリックします。

ストレージノード設定

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。 <ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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	<p>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。</p> <p>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。</p> <p>この属性には次のいずれかの値を指定できます。</p> <ul style="list-style-type: none"> • 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	<p>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がある秒数。この値は、サポートから指示があった場合のみ変更してください。</p>

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	VCM1	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 (エラーカウンタをリセット)	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も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	<p>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。</p> <p>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。</p>

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

エ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"](#)

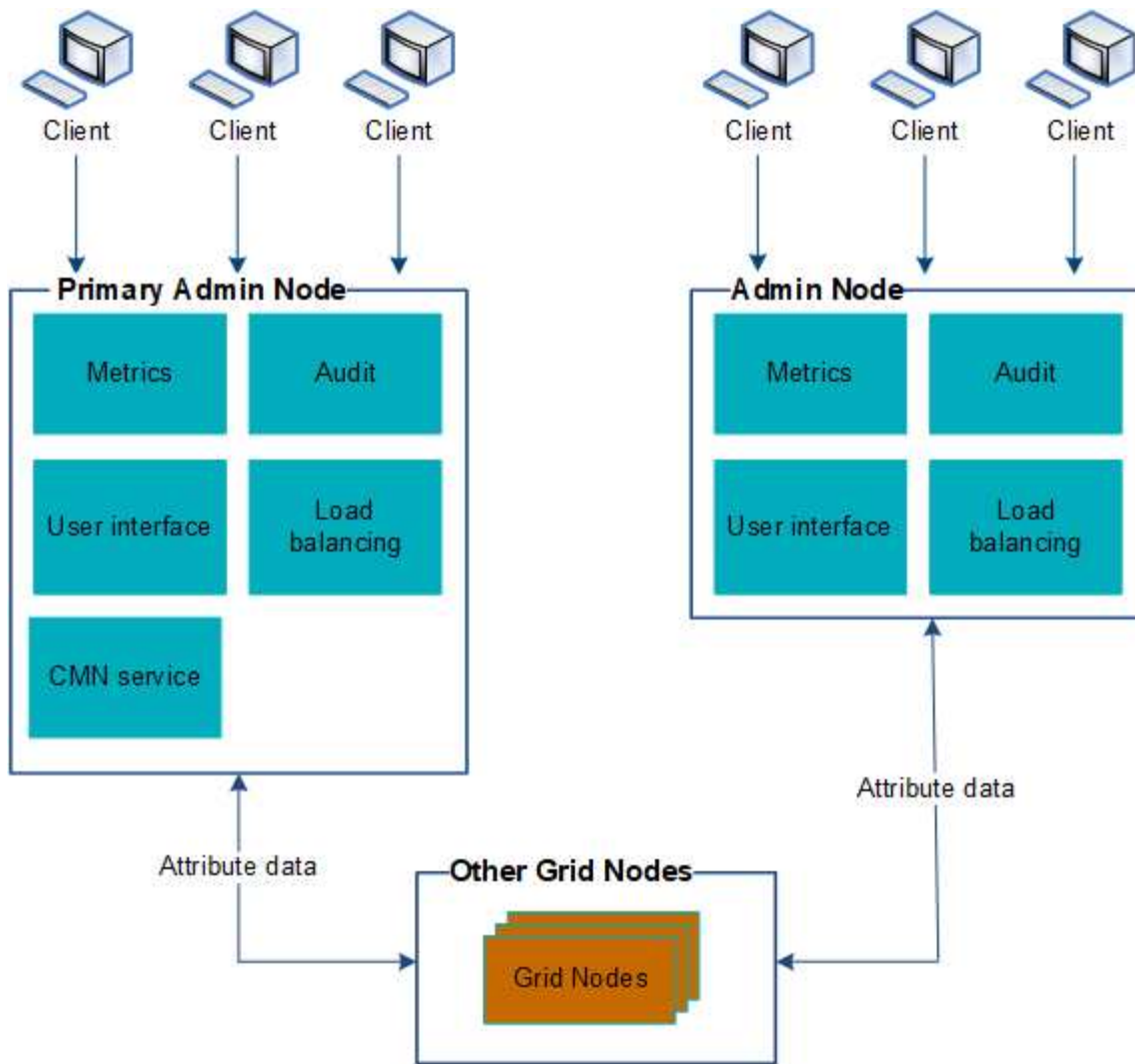
["負荷分散の管理"](#)

["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。



Display Options

Updated: 2017-08-30 16:31:10 MDT

Current Sender	ADMIN-DC1-ADM1
Preferred Sender	ADMIN-DC1-ADM1
GUI Inactivity Timeout	900
Notification Suppress All	<input type="checkbox"/>

Apply Changes

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。

Overview Alarms Reports Configuration


Main


 **Overview: NMS (170-176) - Interface Engine**
Updated: 2009-03-09 10:12:17 PDT

NMS Interface Engine Status: Connected 


Connected Services: 15 


E-mail Notification Events


E-mail Notifications Status: No Errors 

E-mail Notifications Queued: 0 

Database Connection Pool

Maximum Supported Capacity: 100 

Remaining Capacity: 95 % 

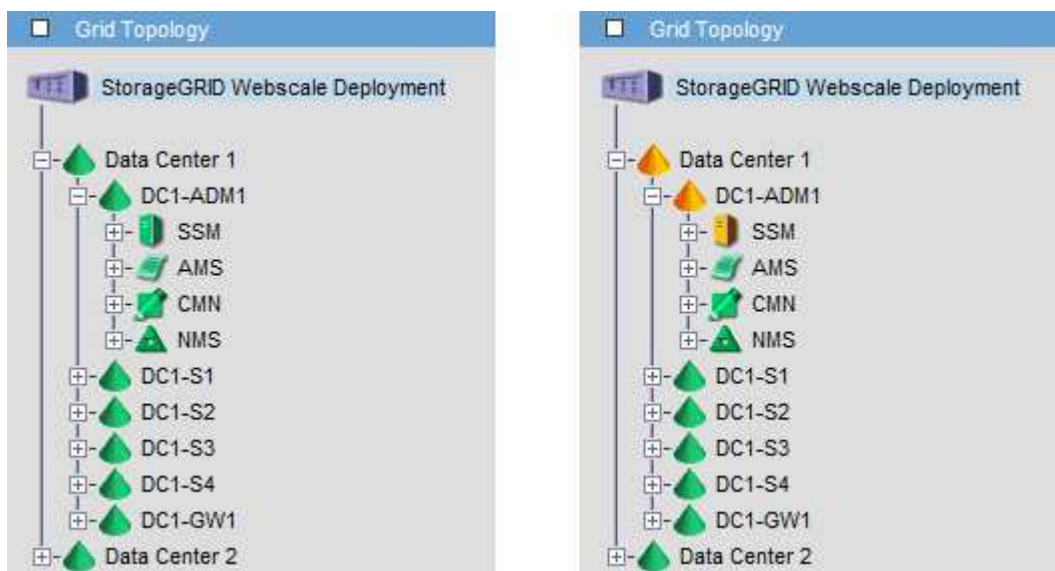
Active Connections: 5 

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 smb 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`
監査グループ名を入力されます。
- 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: #。

- 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。

- コマンドラインに戻り、`* Ctrl * + * C *`を押します。
- 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     |                         |  
-----
```

- 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。

- 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。

- 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`

- 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。

- 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。

- 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。

- 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。

Overview: ARC (DC1-ARC1-98-165) - ARC
Updated: 2015-09-30 10:29:18 PDT

ARC State:	Online	LELE
ARC Status:	No Errors	LELE
Tivoli Storage Manager State:	Online	LELE
Tivoli Storage Manager Status:	No Errors	LELE
Store State:	Online	LELE
Store Status:	No Errors	LELE
Retrieve State:	Online	LELE
Retrieve Status:	No Errors	LELE
Inbound Replication Status:	No Errors	LELE
Outbound Replication Status:	No Errors	LELE

Node Information

Device Type:	Archive Node
Version:	10.2.0
Build:	20150928.2133.a27b3ab
Node ID:	19002524
Site ID:	10

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。

Configuration: ARC (98-127) - Target
Updated: 2015-09-24 15:48:22 PDT

Target Type: Cloud Tiering - Simple Storage Service (S3)

Cloud Tiering (S3) Account

Bucket Name: name

Region: Virginia or Pacific Northwest (us-east-1)

Endpoint: https://10.10.10.123:8082 Use AWS

Endpoint Authentication:

Access Key: ABCD123EFG45AB

Secret Access Key: ●●●●●●

Storage Class: Standard (Default)

Apply Changes

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。

Target Type: Cloud Tying - Simple Storage Service (S3)

Cloud Tying (S3) Account

Bucket Name: name

Region: Virginia or Pacific Northwest (us-east-1)

Endpoint: https://10.10.10.123:8082 Use AWS

Endpoint Authentication:

Access Key: ABCD123EFG45AB

Secret Access Key: ●●●●●●

Storage Class: Standard (Default)

Apply Changes

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。

The screenshot displays the configuration interface for an ARC (Asynchronous Replication Controller). The 'Configuration' tab is active, and the 'Main' sub-tab is selected. The page title is 'Configuration: ARC (98-127) - ARC', with a timestamp 'Updated: 2015-09-24 17:18:29 PDT'. Two configuration items are visible: 'ARC State' is set to 'Online' and 'Cloud Tiering Service State' is set to 'Read-Write Enabled'. An 'Apply Changes' button is located at the bottom right of the configuration area.

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。

Overview Alarms Reports Configuration

Main Alarms

 Configuration: ARC (98-127) - Store
Updated: 2015-09-29 17:54:42 PDT

Reset Store Failure Count

Apply Changes 

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お問い合わせに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

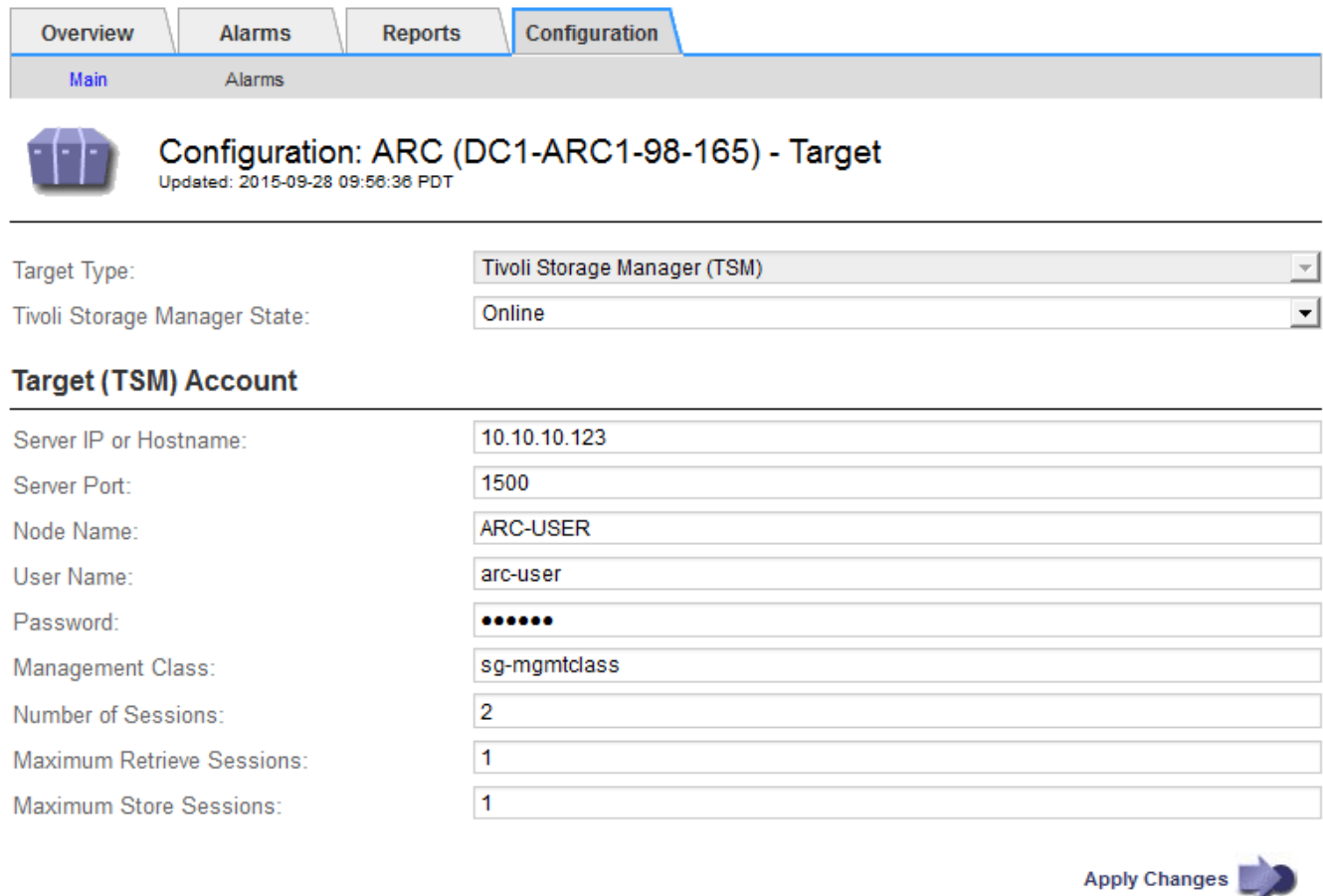
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

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。



The screenshot shows a web interface for configuring a TSM target. At the top, there are tabs for Overview, Alarms, Reports, and Configuration. The Configuration tab is active, and the sub-tab 'Main' is selected. Below the tabs, there is a header for 'Configuration: ARC (DC1-ARC1-98-165) - Target' with an update timestamp of '2015-09-28 09:56:38 PDT'. The main configuration area includes two dropdown menus: 'Target Type' set to 'Tivoli Storage Manager (TSM)' and 'Tivoli Storage Manager State' set to 'Online'. Below these is a section titled 'Target (TSM) Account' with several input fields: 'Server IP or Hostname' (10.10.10.123), 'Server Port' (1500), 'Node Name' (ARC-USER), 'User Name' (arc-user), 'Password' (masked with dots), 'Management Class' (sg-mgmtclass), 'Number of Sessions' (2), 'Maximum Retrieve Sessions' (1), and 'Maximum Store Sessions' (1). At the bottom right, there is an 'Apply Changes' button with a right-pointing arrow.

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。

アーカイブノードに登録または更新したときには、この値を MAXNUMMPP (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 MAXNUMMPP 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

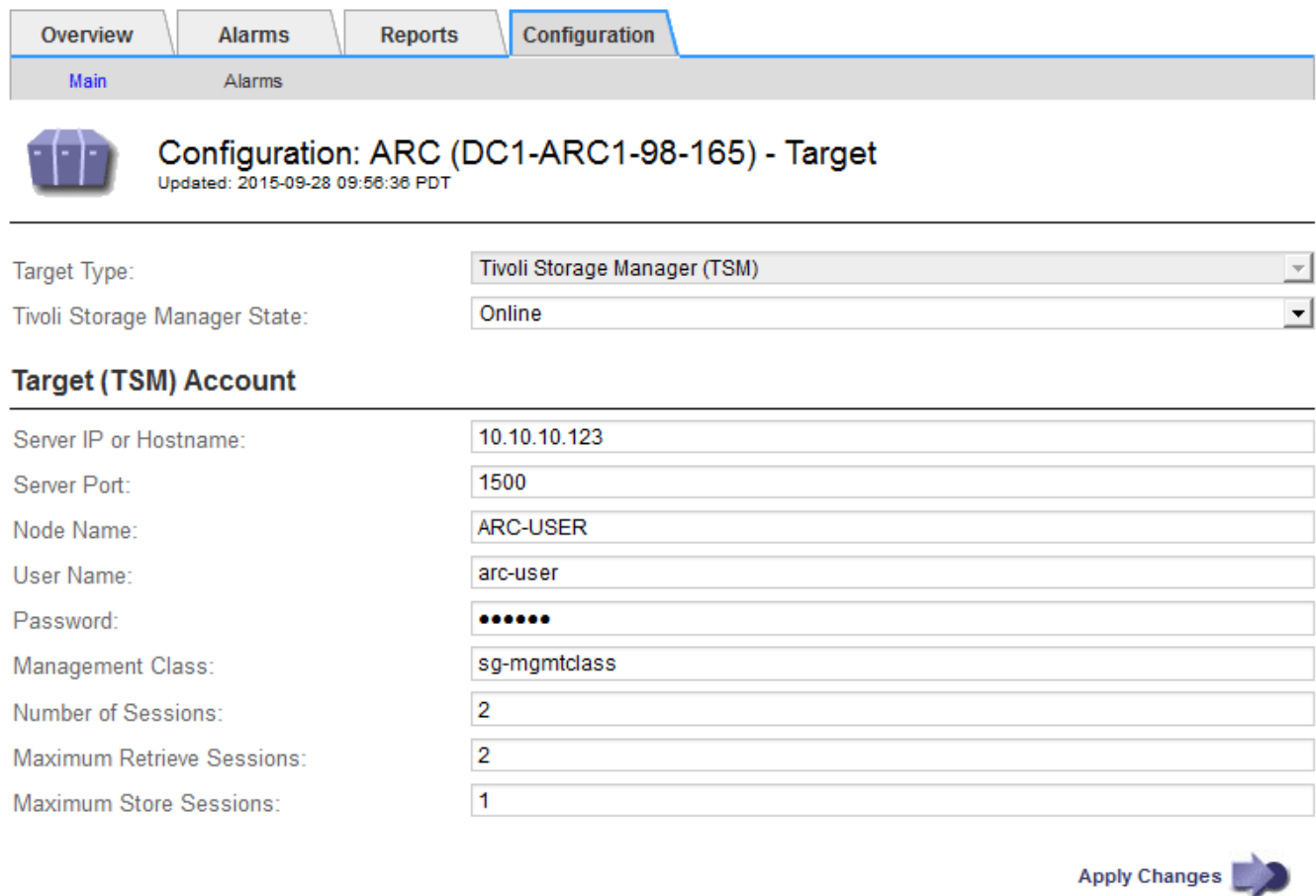
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

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。



The screenshot shows the 'Configuration' tab selected in the Grid Manager interface. The page title is 'Configuration: ARC (DC1-ARC1-98-165) - Target' with a sub-header 'Updated: 2015-09-28 09:56:36 PDT'. Below the title, there are two dropdown menus: 'Target Type' set to 'Tivoli Storage Manager (TSM)' and 'Tivoli Storage Manager State' set to 'Online'. A section titled 'Target (TSM) Account' contains several input fields: 'Server IP or Hostname' (10.10.10.123), 'Server Port' (1500), 'Node Name' (ARC-USER), 'User Name' (arc-user), 'Password' (masked with dots), 'Management Class' (sg-mgmtclass), 'Number of Sessions' (2), 'Maximum Retrieve Sessions' (2), and 'Maximum Store Sessions' (1). At the bottom right of the configuration area, there is an 'Apply Changes' button with a right-pointing arrow.

5. [変更の適用 *] をクリックします。

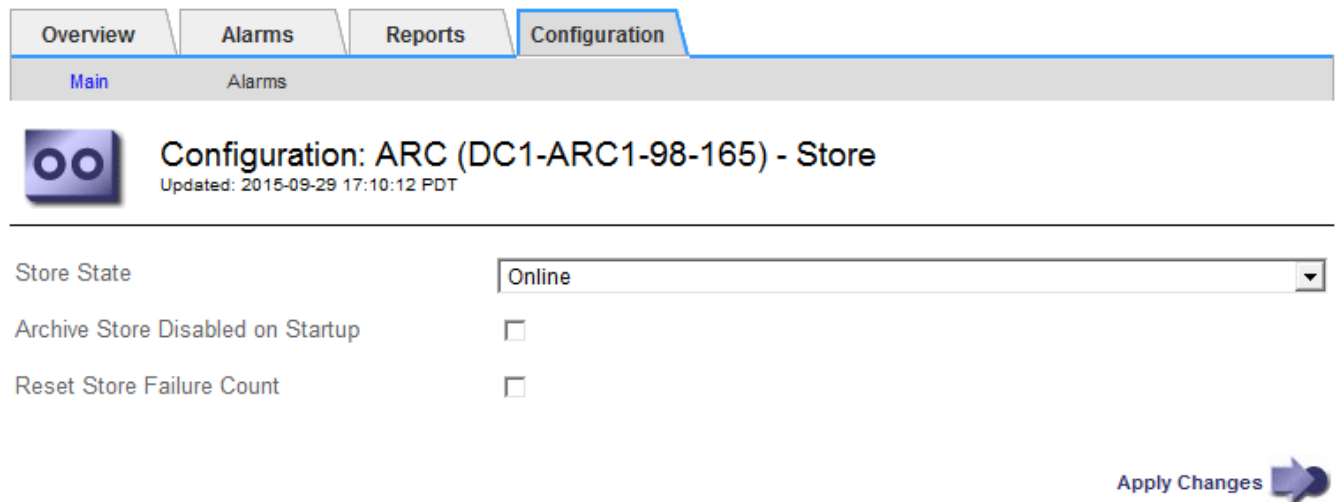
アーカイブノードが TSM ミドルウェアサーバに接続している場合は、アーカイブノードのアーカイブストアの状態をオンラインまたはオフラインに設定できます。また、アーカイブノードの初回起動時にアーカイブストアを無効にしたり、関連するアラーム用に追跡されているエラー数をリセットしたりすることもできます。

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。



Configuration: ARC (DC1-ARC1-98-165) - Store
Updated: 2015-09-29 17:10:12 PDT

Store State	Online
Archive Store Disabled on Startup	<input type="checkbox"/>
Reset Store Failure Count	<input type="checkbox"/>

Apply Changes

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

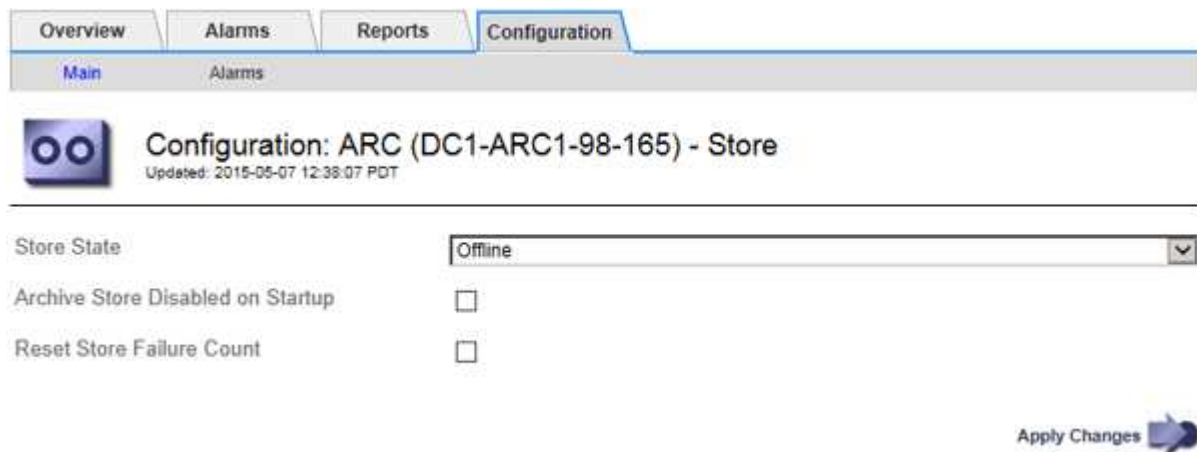
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 特定のアクセス権限が必要です。

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を設定

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。

Configuration: ARC (DC1-ARC1-98-165) - Retrieve
Updated: 2015-05-07 12:24:45 PDT

Retrieve State	Online
Reset Request Failure Count	<input type="checkbox"/>
Reset Verification Failure Count	<input type="checkbox"/>

Apply Changes

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。

The screenshot shows the configuration interface for ARC (DC1-ARC1-98-165) - Replication. The page has a navigation bar with tabs for Overview, Alarms, Reports, and Configuration. Below the navigation bar, there are two sub-tabs: Main and Alarms. The main content area is titled 'Configuration: ARC (DC1-ARC1-98-165) - Replication' and includes a timestamp 'Updated: 2015-05-07 12:21:53 PDT'. There are four checkboxes for configuration options: 'Reset Inbound Replication Failure Count', 'Reset Outbound Replication Failure Count', 'Disable Inbound Replication', and 'Disable Outbound Replication'. An 'Apply Changes' button is located at the bottom right of the configuration area.

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

ットする場合には選択します。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は選択します。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は選択します。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

カイク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、dsmadmcli 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=tape
```

- *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
- *tape* 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 maxxscratch=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、dsmadm 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
```

arc-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	<ol style="list-style-type: none">Support > Tools > Grid Topology *を選択します。[deployment*概要*Main]を選択します。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。<ul style="list-style-type: none">*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。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

- 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"](#)

著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および/または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。