StorageGRID システムの管理

StorageGRID

NetApp
October 03, 2025

目次

StorageGRID システムの管理

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

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

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

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

必要なもの

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

Web ブラウザの要件

サポートされている Web ブラウザを使用する必要があります。

Web ブラウザ	サポートされる最小バージョン
Google Chrome	87
Microsoft Edge の場合	87
Mozilla Firefox	84

ブラウザウィンドウの幅を推奨される値に設定してください。

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

Grid Managerにサインインします

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

必要なもの

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

このタスクについて

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

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

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

手順

1. サポートされている Web ブラウザを起動します。
2. ブラウザのアドレスバーに、 Grid Manager の URL を入力します。

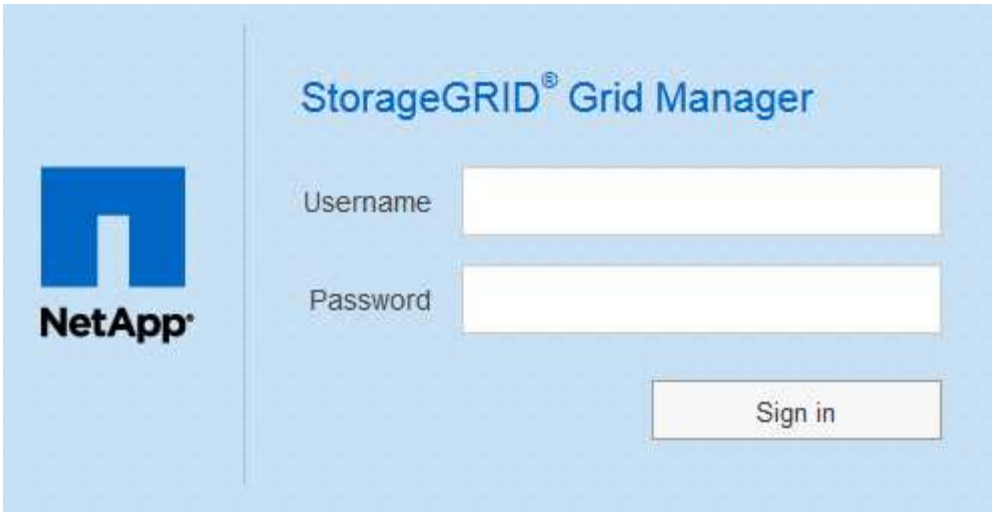
   `https://FQDN_or_Admin_Node_IP/`

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

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

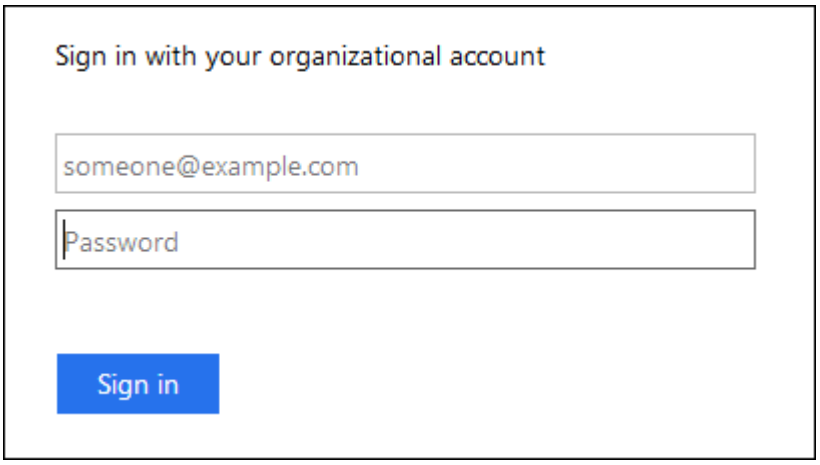
   `https://FQDN_or_Admin_Node_IP:port/`

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



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

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

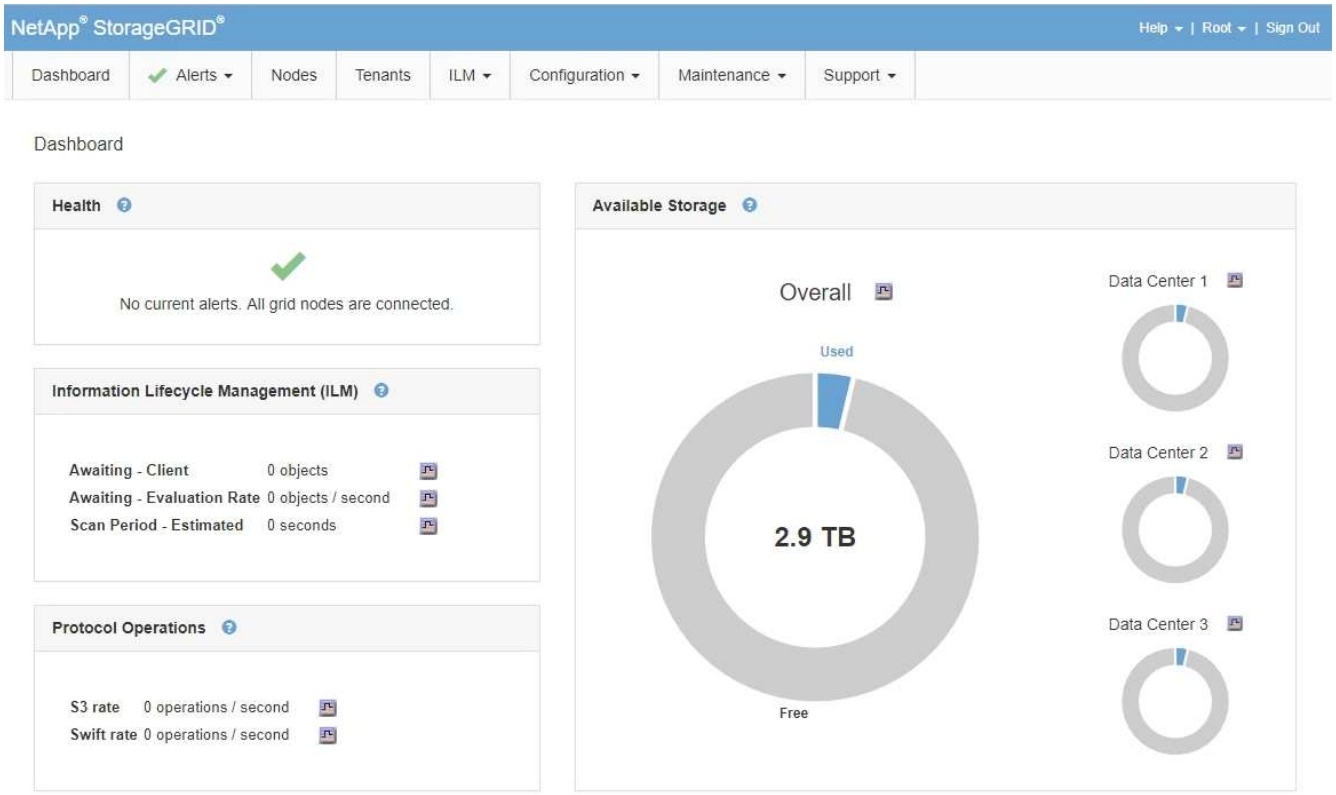


- StorageGRID システムで SSO が有効になっており、 Grid Manager またはテナントアカウントに以前にアクセスしたことがある場合は、次の手順を実行します。

i. 次のいずれかを実行します。

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

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



5. 別の管理ノードにサインインする場合は、次の手順を実行します。

オプション	手順
SSO が有効になっていない	a. ブラウザのアドレスバーに、他の管理ノードの完全修飾ドメイン名または IP アドレスを入力します。必要に応じてポート番号を追加します。 b. Grid Manager のユーザ名とパスワードを入力します。 c. [* サインイン *] をクリックします。
SSO が有効です	ブラウザのアドレスバーに、他の管理ノードの完全修飾ドメイン名または IP アドレスを入力します。 1 つの管理ノードにサインインしたら、再度サインインしなくても他の管理ノードにアクセスできます。ただし、 SSO セッションが期限切れになると、クレデンシャルの再入力を求められます。 • 注： SSO は制限された Grid Manager ポートでは使用できません。ユーザをシングルサインオンで認証する場合は、デフォルトの HTTPS ポート（ 443 ）を使用する必要があります。

関連情報

"Web ブラウザの要件"

"ファイアウォールによるアクセス制御"

"サーバ証明書の設定"

"シングルサインオンを設定しています"

"管理者グループの管理"

"ハイアベイラビリティグループの管理"

"テナントアカウントを使用する"

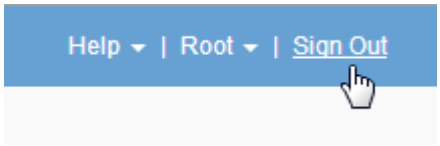
"トラブルシューティングを監視します"

Grid Managerからサインアウトします

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

手順

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



2. [サインアウト]をクリックします。

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

関連情報

"シングルサインオンを設定しています"

"テナントアカウントを使用する"

パスワードを変更しています

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

必要なもの

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

このタスクについて

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

手順

1. Grid Managerのヘッダーで、*自分の名前>パスワードの変更*を選択します。
2. 現在のパスワードを入力します。
3. 新しいパスワードを入力します。

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

4. 新しいパスワードをもう一度入力します。
5. [保存（ Save ）] をクリックします。

プロビジョニングパスフレーズを変更しています

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

必要なもの

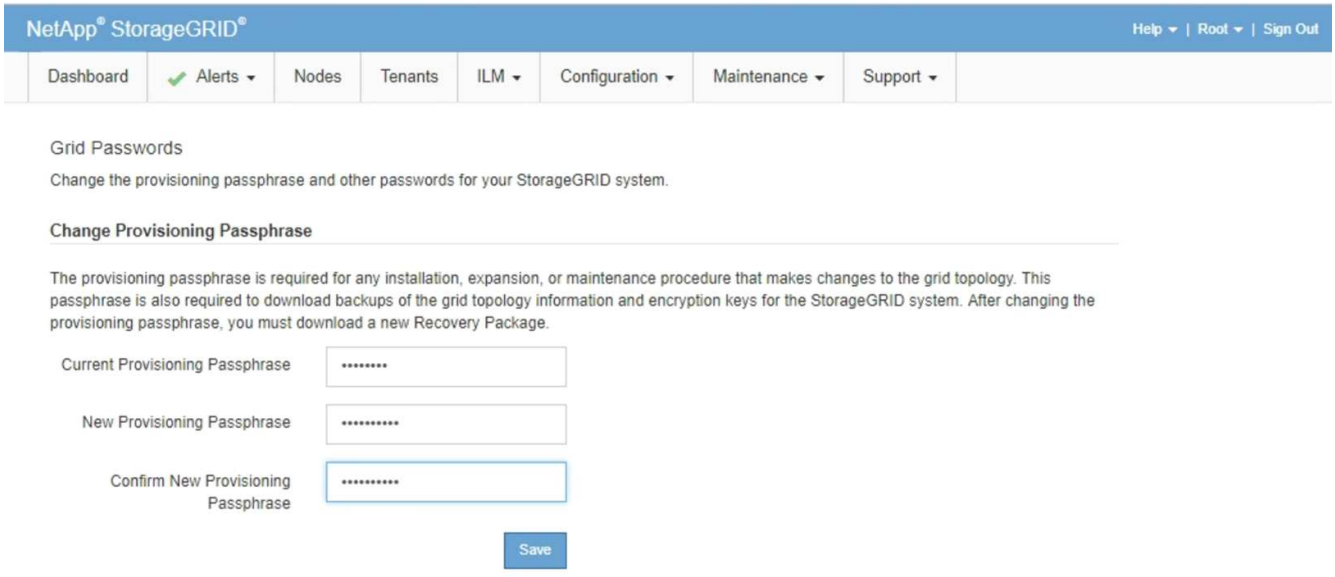
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- MaintenanceまたはRoot Access権限が必要です。
- 現在のプロビジョニングパスフレーズが必要です。

このタスクについて

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

手順

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

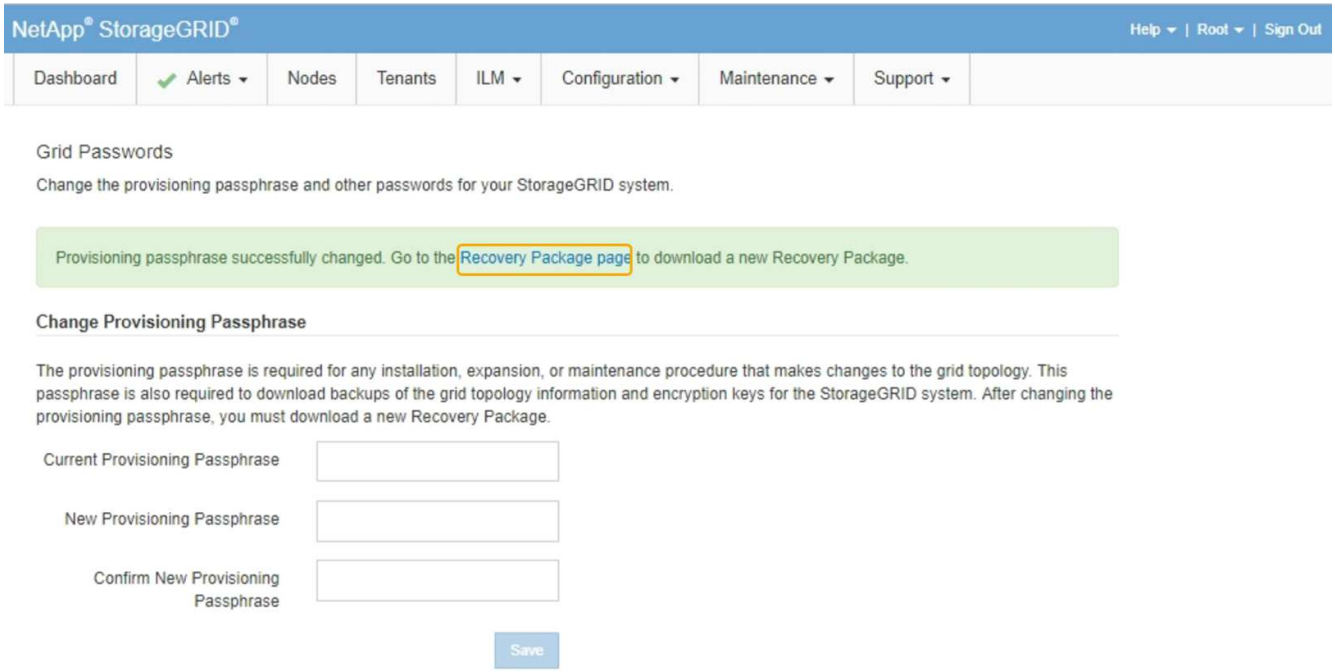


2. 現在のプロビジョニングパスフレーズを入力します。
3. 新しいリンフレーズを入力してください。パスフレーズには8文字以上32文字以下の文字列を含める必要があります。パスフレーズでは大文字と小文字が区別されます。

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

4. 新しいパスフレーズをもう一度入力し、*保存*をクリックします。

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



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

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

ブラウザセッションのタイムアウトを変更する

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

必要なもの

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

このタスクについて

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

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

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

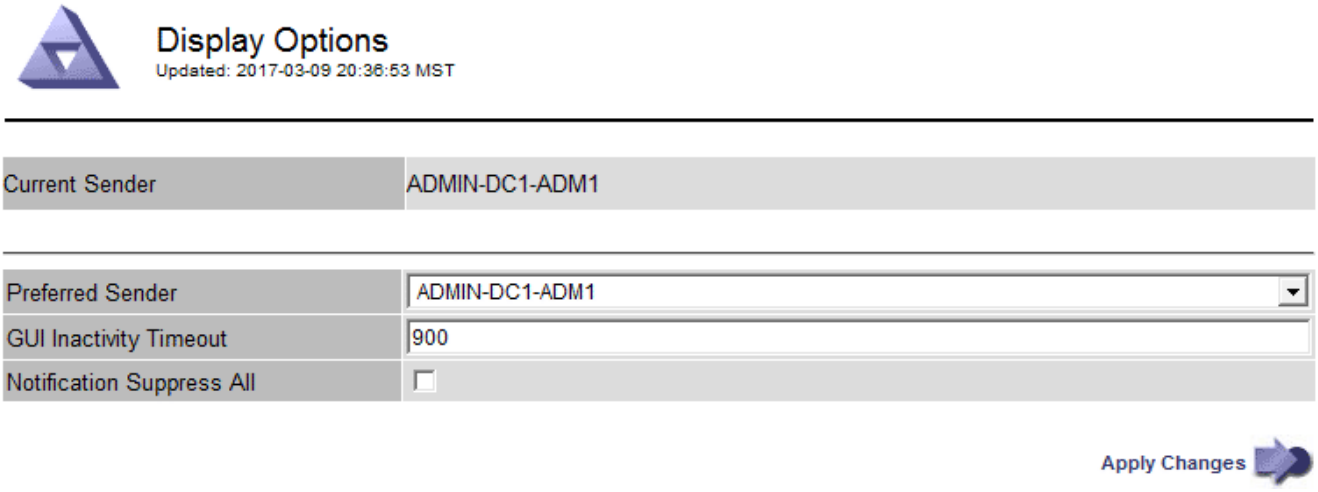
ユーザセッションのタイムアウトは、次の方法でも制御できます。

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

手順

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

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



3. [変更の適用 *] をクリックします。

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

関連情報

"シングルサインオンの仕組み"

StorageGRID ライセンス情報の表示

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

必要なもの

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

このタスクについて

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

ステップ

ライセンスを表示するには、次のいずれかを実行します。

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

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

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

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

StorageGRID ライセンス情報を更新しています

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

必要なもの

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

手順

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

   新しいライセンスファイルが検証され、表示されます。

5. [保存（ Save ）] をクリックします。

グリッド管理APIを使用する

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

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

トップレベルのリソース

グリッド管理 API で使用可能な最上位のリソースは次のとおりです。

- `/grid`：Grid Managerユーザのみがアクセスでき、設定されているグループ権限に基づいてアクセスが制限されます。
- `/org`：テナントアカウントのローカルまたはフェデレーテッドLDAPグループに属するユーザのみがアクセスできます。詳細については、テナントアカウントの使用に関する情報を参照してください。

- `/private`：Grid Managerユーザのみがアクセスでき、設定されているグループ権限に基づいてアクセスが制限されます。これらのAPIは内部使用のみを目的としており、正式にドキュメント化されていません。また、これらのAPIは予告なく変更される場合があります。

関連情報

"テナントアカウントを使用する"

"Prometheus：クエリの基本"

グリッド管理 API の処理

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

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

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

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

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

- * client-certificates * — 外部監視ツールを使用して StorageGRID に安全にアクセスできるようにクライアント証明書を設定する処理。
- **config** — 製品リリースと Grid Management API のバージョンに関連する操作。製品のリリースバージョンおよびそのリリースでサポートされているグリッド管理 API のメジャーバージョンをリストし、廃止されたバージョンの API を無効にすることができます。
- * deactivated-features * — 非アクティブ化された可能性のある機能を表示する操作。
- *dns-servers * — 設定済みの外部 DNS サーバをリストおよび変更する処理。
- * endpoint-domain-names * — エンドポイントドメイン名をリストおよび変更する処理。

- * erasure-coding * — イレイジャーコーディングプロファイルに対する処理。
- *expansion *-- 拡張の操作 (プロシージャレベル) 。
- * expansion-nodes * - 拡張処理（ノードレベル）。
- * expansion-sitites * — 拡張の操作（サイトレベル）。
- * grid-networks * — グリッドネットワークリストをリストおよび変更する処理。
- * grid-password* - グリッドパスワード管理の操作。
- *groups * — ローカルグリッド管理者グループを管理し、フェデレーテッドグリッド管理者グループを外部 LDAP サーバから取得するための処理。
- * identity-source * — 外部のアイデンティティソースを設定する処理、およびフェデレーテッドグループとユーザ情報を手動で同期する処理。
- *ilm * — 情報ライフサイクル管理 (ILM; 情報ライフサイクル管理) の操作。
- **license** — StorageGRID ライセンスを取得および更新する処理。
- **logs** — ログファイルを収集してダウンロードするための操作。
- * メトリクス * — ある時点での瞬時の指標クエリや、一定期間にわたる指標クエリなど、 StorageGRID メトリックに対する処理。グリッド管理 API は、バックエンドのデータソースとして Prometheus システム監視ツールを使用します。Prometheus クエリの構築については、 Prometheus の Web サイトを参照してください。

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

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

API要求の実行

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

必要なもの

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

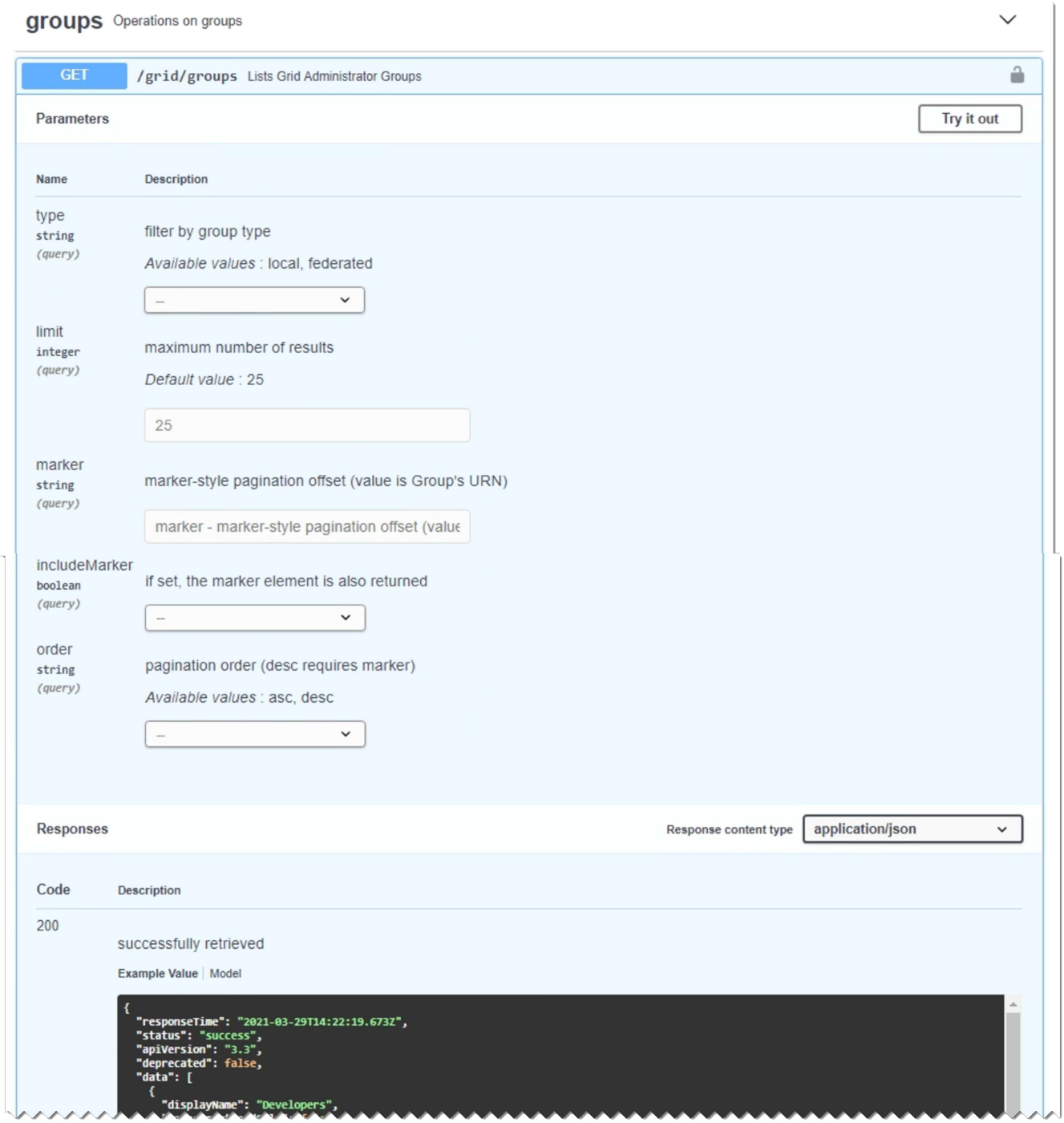
> API Docs Web ページを使用して実行する API 処理はすべてその場で実行されます。設定データやその他のデータを誤って作成、更新、または削除しないように注意してください。

手順

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

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

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



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

グリッド管理 API のバージョン管理

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

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

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

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

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

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

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

古い要求は、次の方法で廃止とマークされます。

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

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

現在のリリースでサポートされている**API**バージョンを確認します

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

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

要求の**API**バージョンの指定

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

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

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

クロスサイトリクエストフォージェリ（**CSRF**）の防止

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

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

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

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

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

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

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

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

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

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

シングルサインオンが有効な場合は、**API**を使用します

StorageGRID システムでシングルサインオン（SSO）が有効になっている場合、標準の認証API要求を使用してグリッド管理APIまたはテナント管理APIにサインインおよびサインアウトすることはできません。

シングルサインオンが有効な場合は、**API**へのサインイン

シングルサインオン（SSO）が有効になっている場合は、グリッド管理APIまたはテナント管理APIで有効なAD FSから認証トークンを取得するための一連のAPI要求を問題 で処理する必要があります。

必要なもの

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

このタスクについて

認証トークンを取得するには、次のいずれかの例を使用します。

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

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

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

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

ます。

手順

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

   プロンプトが表示されたら、次の引数の値を入力します。

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

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

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

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

3. cURL 要求を使用する場合は、次の手順 を使用します。

   a. サインインに必要な変数を宣言します。

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

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

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

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

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

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

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

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

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

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

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

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

応答にはクライアント要求 ID が含まれています。

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

e. 応答からクライアント要求 ID を保存します。

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

f. 前の応答のフォームアクションにクレデンシャルを送信します。

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

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

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

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

g. を保存します `MSISAuth` 応答からのCookie。

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

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

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

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

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

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

i. を保存します `SAMLResponse` 非表示フィールドから：

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

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

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

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

応答には認証トークンが含まれています。

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

a. 認証トークンを応答にという名前で保存します `MYTOKEN`。

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

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

シングルサインオンが有効な場合は、**API**からのサインアウト

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

このタスクについて

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

手順

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

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

ログアウト URL が返されます。

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

2. ログアウト URL を保存します。

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

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

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

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

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

4. StorageGRID Bearer トークンを削除します。

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

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

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

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

StorageGRID セキュリティ証明書を使用する

セキュリティ証明書は、 StorageGRID コンポーネント間、および StorageGRID コンポーネントと外部システム間のセキュアで信頼された接続の確立に使用される小さいデータファイルです。

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

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

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

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

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

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

  "システムの保護対策"

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

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

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

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

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

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

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

例 1 ：ロードバランササービス

この例では、 StorageGRID がサーバとして機能します。

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

例 2 ：外部キー管理サーバ（ KMS ）

この例では、 StorageGRID がクライアントとして機能します。

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

著作権に関する情報

商標に関する情報