StorageGRID への管理者アクセスの制御

StorageGRID 11.5

NetApp
April 11, 2024

目次

StorageGRID への管理者アクセスの制御

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

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

ファイアウォールによるアクセス制御

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

外部ファイアウォールでのアクセス制御

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

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

ポート	説明	ポートが開いている場合
ポート 1	管理ノード上の制限された Tenant Manager ポート	• Web ブラウザと管理 API クライアントは HTTPS を使用して Tenant Manager とテナント管理 API にアクセスできます。 • Web ブラウザと管理 API クライアントは、 Grid Manager またはグリッド管理 API にはアクセスできません。 • 内部コンテンツに対する要求は拒否されます。

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

関連情報

"Grid Managerにサインインします"

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

"Summary ：クライアント接続の IP アドレスとポート"

"信頼されていないクライアントネットワークの管理"

"Ubuntu または Debian をインストールします"

"VMware をインストールする"

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

アイデンティティフェデレーションを使用する

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

アイデンティティフェデレーションの設定

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

必要なもの

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

- アイデンティティプロバイダとしてActive Directory、OpenLDAP、またはOracle Directory Serverを使用している必要があります。

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

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

このタスクについて

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

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

手順

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

   LDAPサーバを設定するためのフィールドが表示されます。

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

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

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

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

4. [* その他 *] を選択した場合は、 [LDAP 属性] セクションのフィールドに入力します。
   - * User Unique Name * ： LDAP ユーザの一意な ID が含まれている属性の名前。この属性はと同じです `sAMAccountName` Active Directoryおよびの場合 `uid` OpenLDAPの場合。Oracle Directory Serverを設定する場合は、と入力します `uid`。
   - * User UUID * ： LDAP ユーザの永続的な一意な ID が含まれている属性の名前。この属性はと同じです `objectGUID` Active Directoryおよびの場合 `entryUUID` OpenLDAPの場合。Oracle Directory Serverを設定する場合は、と入力します `nsuniqueid`。指定した属性の各ユーザの値は、 16 バイトまたは文字列形式の 32 桁の 16 進数である必要があります。ハイフンは無視されます。
   - * Group Unique name *：LDAPグループの一意なIDが含まれている属性の名前。この属性はと同じです `sAMAccountName` Active Directoryおよびの場合 `cn` OpenLDAPの場合。Oracle Directory Serverを設定する場合は、と入力します `cn`。
   - * グループ UUID * ： LDAP グループの永続的な一意な ID が含まれている属性の名前。この属性はと

同じです `objectGUID` Active Directoryおよびの場合 `entryUUID` OpenLDAPの場合。Oracle Directory Serverを設定する場合は、と入力します `nsuniqueid`。指定した属性の各グループの値は、16 バイトまたは文字列形式の 32 桁の 16 進数である必要があります。ハイフンは無視されます。

5. Configure LDAP server（LDAPサーバの設定）セクションで、必要なLDAPサーバおよびネットワーク接続情報を入力します。
   - * Hostname *：LDAPサーバのホスト名またはIPアドレス。
   - * Port * ： LDAP サーバへの接続に使用するポート。

     STARTTLS のデフォルトポートは 389 、 LDAPS のデフォルトポートは 636 です。ただし、ファイアウォールが正しく設定されていれば、任意のポートを使用できます。

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

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

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

     - `sAMAccountName` または `uid`
     - `objectGUID`、 `entryUUID`または `nsuniqueid`
     - `cn`
     - `memberOf` または `isMemberOf`

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

     *グループの一意な名前*値は、所属する*グループのベースDN *内で一意である必要があります。

   - * User base DN*：ユーザを検索するLDAPサブツリーの識別名（DN）の完全パス。

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

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

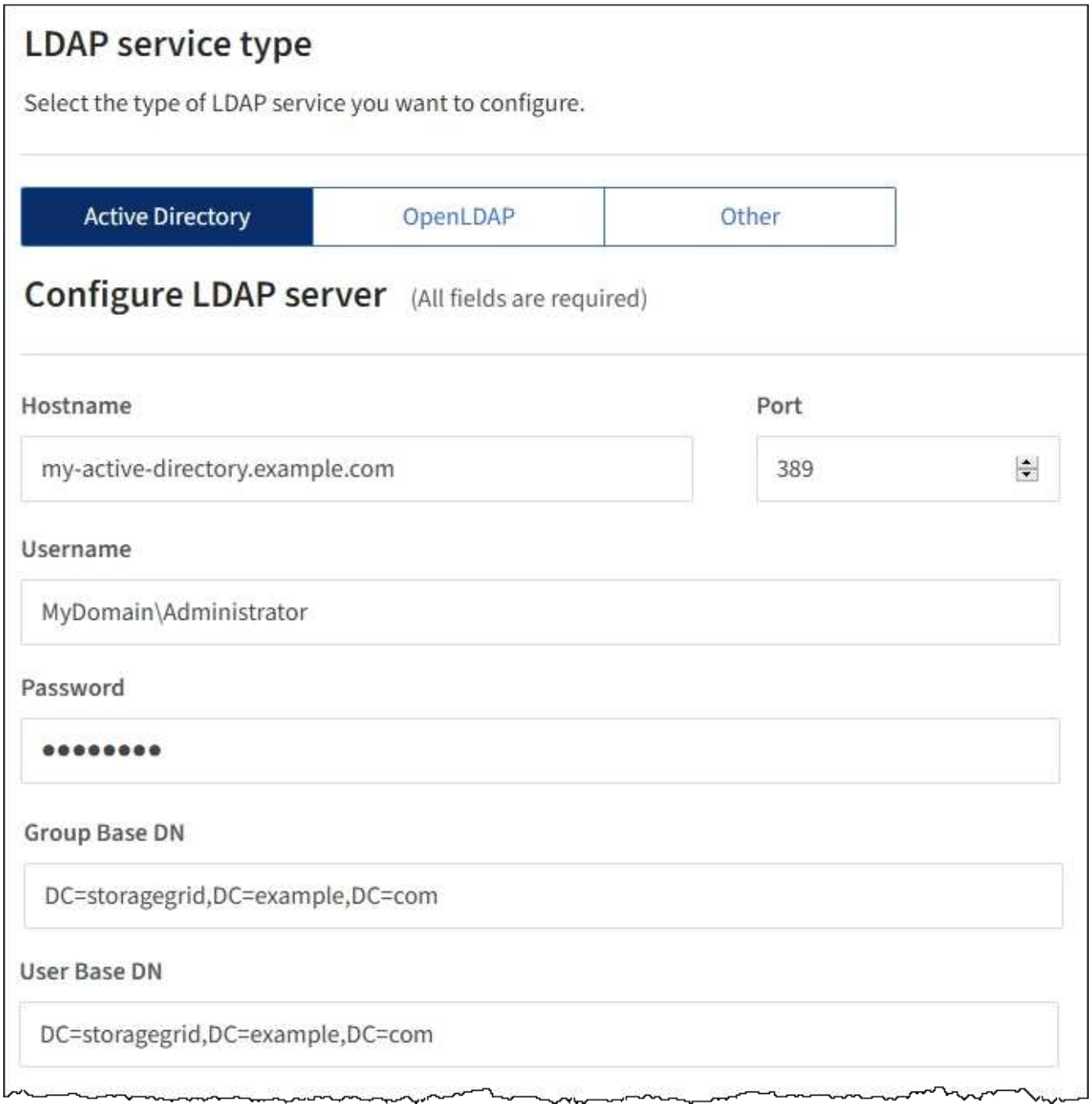
Active Directory サーバで LDAP 署名が適用される場合、 [TLS を使用しない] オプションの使用はサポートされていません。STARTTLS または LDAPS を使用する必要があります。

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

     この設定を選択した場合は、カスタムセキュリティ証明書をコピーして CA 証明書テキストボックスに貼り付けます。
8. 必要に応じて、*接続のテスト*を選択して、LDAPサーバーの接続設定を検証します。

   接続が有効な場合は、ページの右上に確認メッセージが表示されます。
9. 接続が有効な場合は、*保存*を選択します。

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



関連情報

"発信 TLS 接続でサポートされる暗号"

"シングルサインオンの使用要件"

"テナントアカウントを作成します"

"テナントアカウントを使用する"

OpenLDAP サーバの設定に関するガイドライン

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

memberof オーバーレイと **refint** オーバーレイ

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

インデックス作成

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

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

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

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

関連情報

"OpenLDAP のドキュメント：バージョン 2.4 管理者ガイド"

アイデンティティソースとの強制同期

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

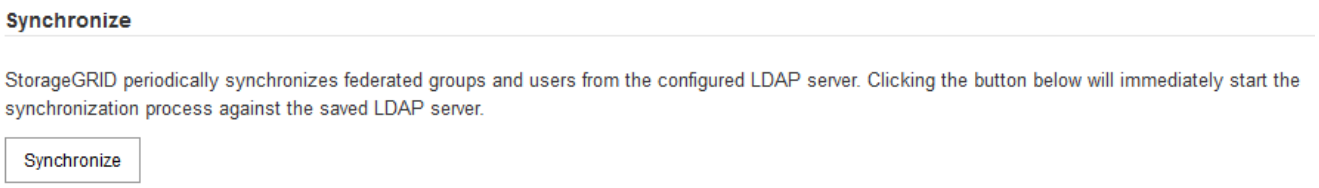
必要なもの

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

手順

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

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

2. [同期化（Synchronize）]をクリックします

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

時間がかかることがあります。

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

アイデンティティフェデレーションの無効化

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

必要なもの

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

このタスクについて

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

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

手順

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

関連情報

"シングルサインオンを無効にしています"

管理者グループの管理

管理者グループを作成して、 1 人以上の管理者ユーザのセキュリティ権限を管理できます。StorageGRID システムへのアクセスを許可するには、ユーザがグループに属している必要があります。

管理者グループの作成

管理者グループを使用すると、 Grid Manager およびグリッド管理 API のどのユーザがどの機能や処理にアク

セスできるかを決定できます。

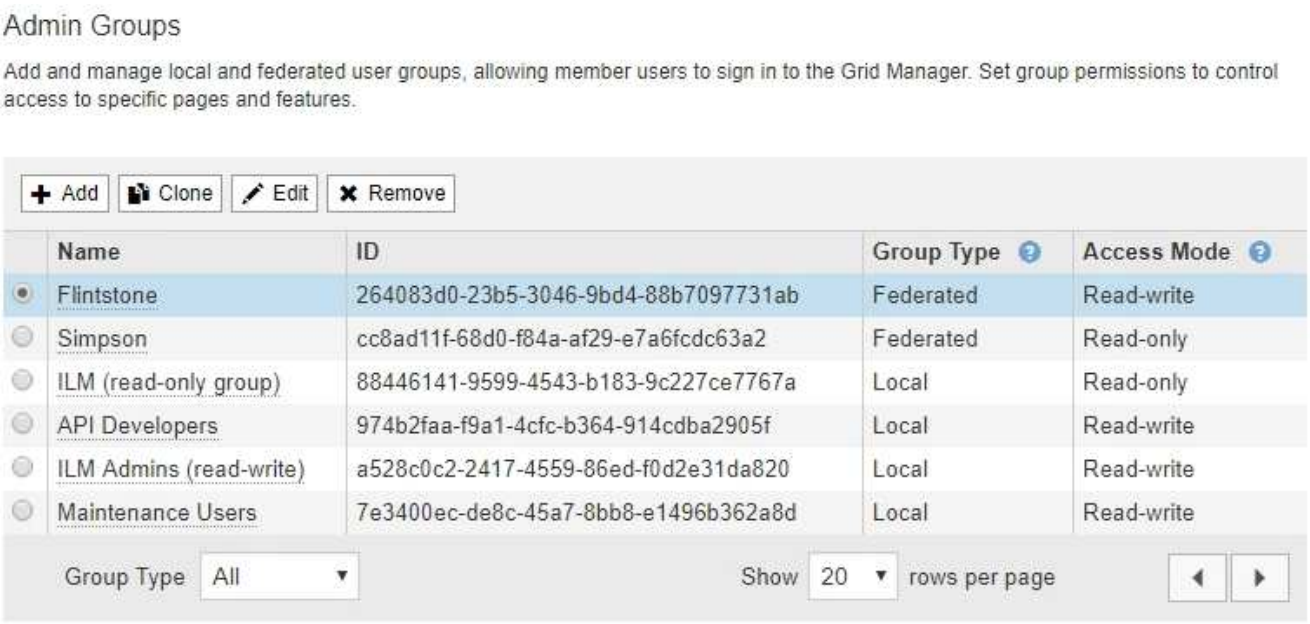
必要なもの

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

手順

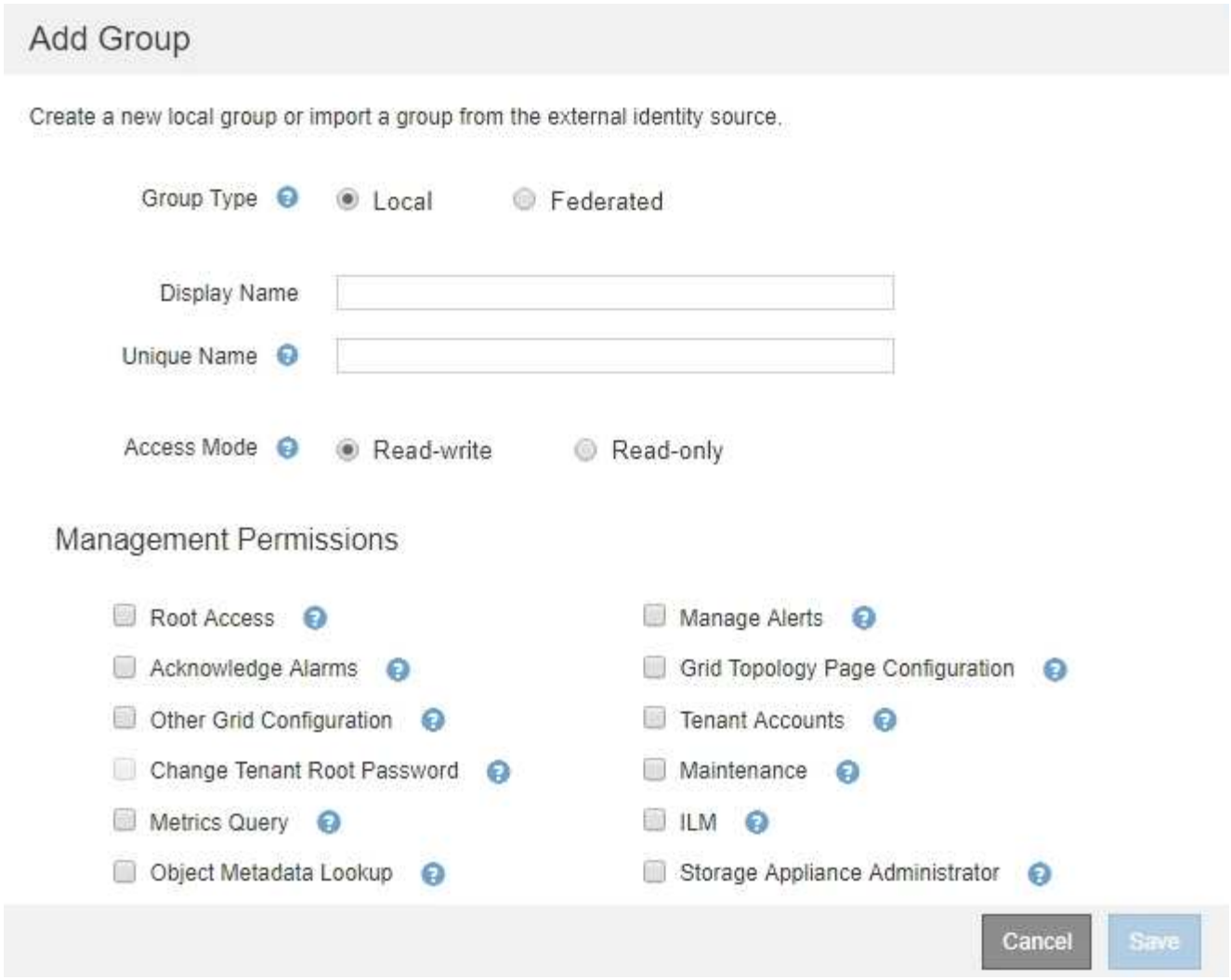
1. [構成アクセス制御管理者グループ*]を選択します。

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



2. 「 * 追加」を選択します。

   [Add Group]ダイアログボックスが表示されます。



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

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

7. 管理権限を1つ以上選択します。

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

8. [保存（ Save ）] を選択します。

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

関連情報

"ローカルユーザの管理"

管理者グループの権限

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

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

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

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

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

ルートアクセス（ **Root Access** ）

この権限は、すべてのグリッド管理機能へのアクセスを許可します。

アラートの管理

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

アラームの確認（レガシーシステム）

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

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

Gridトポロジページの設定

この権限では、次のメニューオプションにアクセスできます。

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

その他の**Grid**設定

この権限で、追加のグリッド設定オプションにアクセスできます。

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

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

テナントアカウント

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

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

テナントの**root**パスワードを変更

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

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

メンテナンス

この権限では、次のメニューオプションにアクセスできます。

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

- ログ

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

指標クエリ

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

ILM

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

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

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

オブジェクトメタデータの検索

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

ストレージアプライアンス管理者

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

権限とアクセスモードの相互作用

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

グリッド管理**API**からの機能の非アクティブ化

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

このタスクについて

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

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

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

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

非アクティブ化した機能の再アクティブ

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

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

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

手順

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

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

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

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

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

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

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

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

関連情報

"グリッド管理APIを使用する"

管理者グループの変更

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

必要なもの

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

手順

1. [構成アクセス制御管理者グループ*]を選択します。
2. グループを選択します。

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

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

   一意の名前は内部グループ名であるため、変更できません。

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

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

6. 必要に応じて、グループ権限を追加または削除します。

管理者グループの権限に関する情報を参照してください。

7. [保存（ Save ）] を選択します。

関連情報

[管理者グループの権限]

管理者グループを削除しています

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

必要なもの

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

このタスクについて

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

手順

1. [構成アクセス制御管理者グループ*]を選択します。
2. グループの名前を選択します。

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

3. 「 * 削除」を選択します。
4. 「 * OK 」を選択します。

ローカルユーザの管理

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

Grid Managerには'ルートという名前の'事前定義されたローカル・ユーザが1つ含まれていますローカルユーザは追加および削除できますが、rootユーザを削除することはできません。

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

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

ローカルユーザを作成しています

ローカル管理者グループを作成した場合は、1人以上のローカルユーザを作成し、各ユーザを1つ以上のグループに割り当てることができます。このグループの権限は、ユーザがアクセスできるGrid Manager機能を制御します。

このタスクについて

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

手順

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

   グループ名のリストは'グループ(Groups)テーブルから生成されます
5. [保存（ Save ）] をクリックします。

関連情報

"管理者グループの管理"

ローカルユーザアカウントの変更

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

このタスクについて

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

手順

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

   システムに20個を超えるアイテムが含まれている場合は、各ページに一度に表示する行数を指定できます。その後、ブラウザの検索機能を使用して、現在表示されている行の特定の項目を検索できます。
3. [編集（ Edit ）] をクリックします。
4. 必要に応じて、名前またはグループメンバーシップを変更します。
5. 必要に応じて、ユーザが一時的にシステムにアクセスできないようにするには、*アクセス拒否*をオンにします。
6. [保存（ Save ）] をクリックします。

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

れます。

ローカルユーザのアカウントを削除する

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

手順

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

   事前定義されたrootローカルユーザは削除できません。

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

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

ローカルユーザのパスワードを変更する

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

このタスクについて

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

手順

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

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

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

StorageGRID にシングルサインオン（SSO）を使用する

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

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

シングルサインオンの仕組み

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。

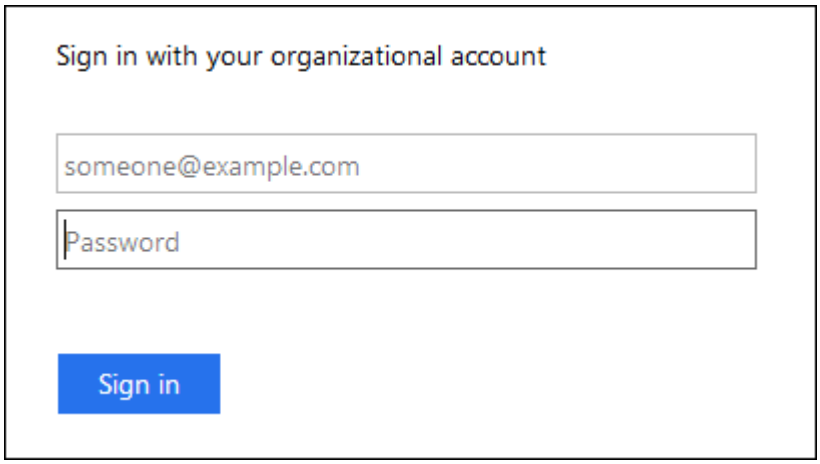
   - このブラウザで初めて URL にアクセスした場合は、アカウント ID の入力を求められます。

   - 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に移動します `/var/local/mgmt-api` ディレクトリ。カスタムサーバ証明書の名前はです `custom-server.crt`。ノードのデフォルトサーバ証明書の名前はです `server.crt`。

関連情報

"ファイアウォールによるアクセス制御"

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

シングルサインオンを設定しています

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

- "フェデレーテッドユーザがサインインできることを確認しておき"
- "サンドボックスモードの使用"

- "AD FSでの証明書利用者信頼の作成"
- "証明書利用者信頼のテスト"
- "シングルサインオンの有効化"
- "シングルサインオンを無効にしています"
- "1つの管理ノードのシングルサインオンの一時的な無効化と再有効化"

フェデレーテッドユーザがサインインできることを確認しておき

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

必要なもの

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

  "シングルサインオンの使用要件"

手順

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

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

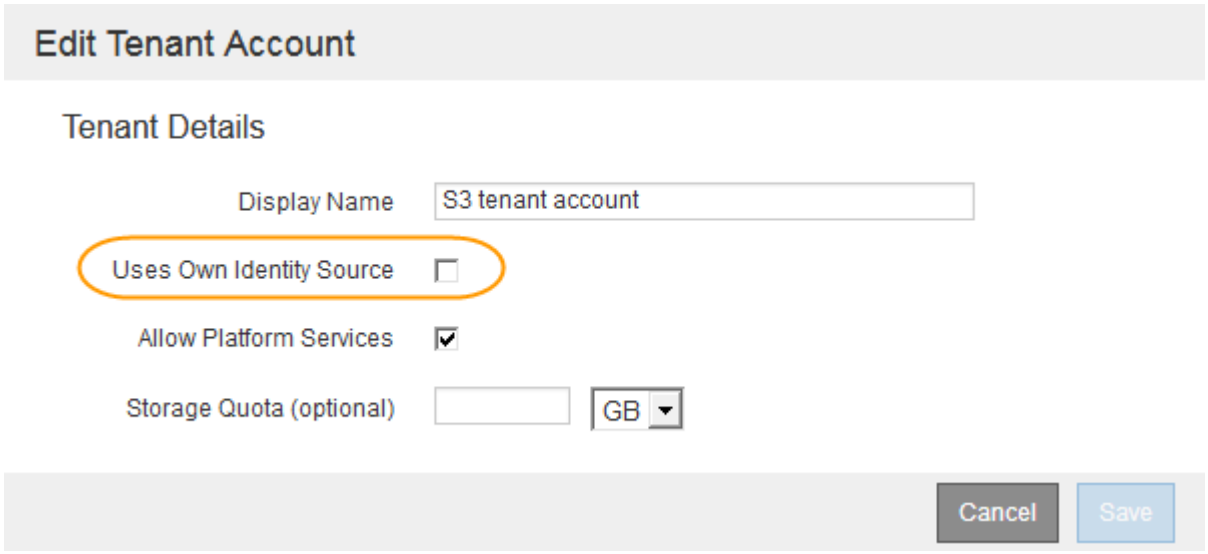
   a. 各テナントアカウントの Tenant Manager にサインインします。
   b. アクセス制御*>*アイデンティティフェデレーションを選択します。
   c. ［アイデンティティフェデレーションを有効にする］チェックボックスがオフになっていることを確認します。
   d. その場合は、このテナントアカウントに使用されている可能性のあるフェデレーテッドグループが不要になっていることを確認し、チェックボックスをオフにして*保存*をクリックします。
2. フェデレーテッドユーザが Grid Manager にアクセスできることを確認します。
   a. Grid Managerから* Configuration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

3. 既存のテナントアカウントがある場合は、Root Access権限を持つフェデレーテッドユーザがサインインできることを確認します。

   a. Grid Managerから* tenants *を選択します。

   b. テナントアカウントを選択し、*アカウントの編集*をクリックします。

   c. [独自のアイデンティティソースを使用する*]チェックボックスがオンになっている場合は、チェックボックスをオフにして、[保存*]をクリックします。



   Tenant Accountsページが表示されます。

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

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

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

   d. サインアウトします。

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

関連情報

"シングルサインオンの使用要件"

"管理者グループの管理"

"テナントアカウントを使用する"

サンドボックスモードの使用

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

効に

必要なもの

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

このタスクについて

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

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

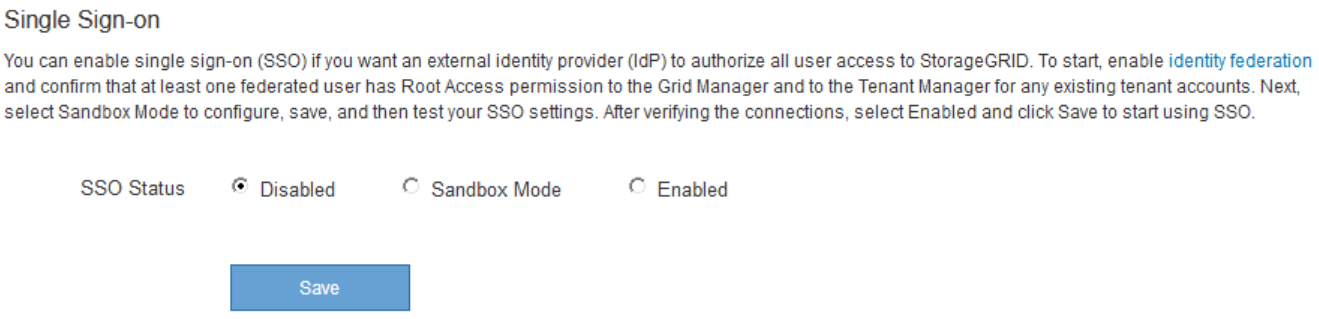
サンドボックスモードでは、 SSO を有効にする前に、この手順を簡単に実行し、すべての設定をテストできます。

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

手順

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

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



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

2. [サンドボックスモード]オプションを選択します。

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

3. アイデンティティプロバイダセクションで、次の手順を実行します。

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

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

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

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

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

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

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

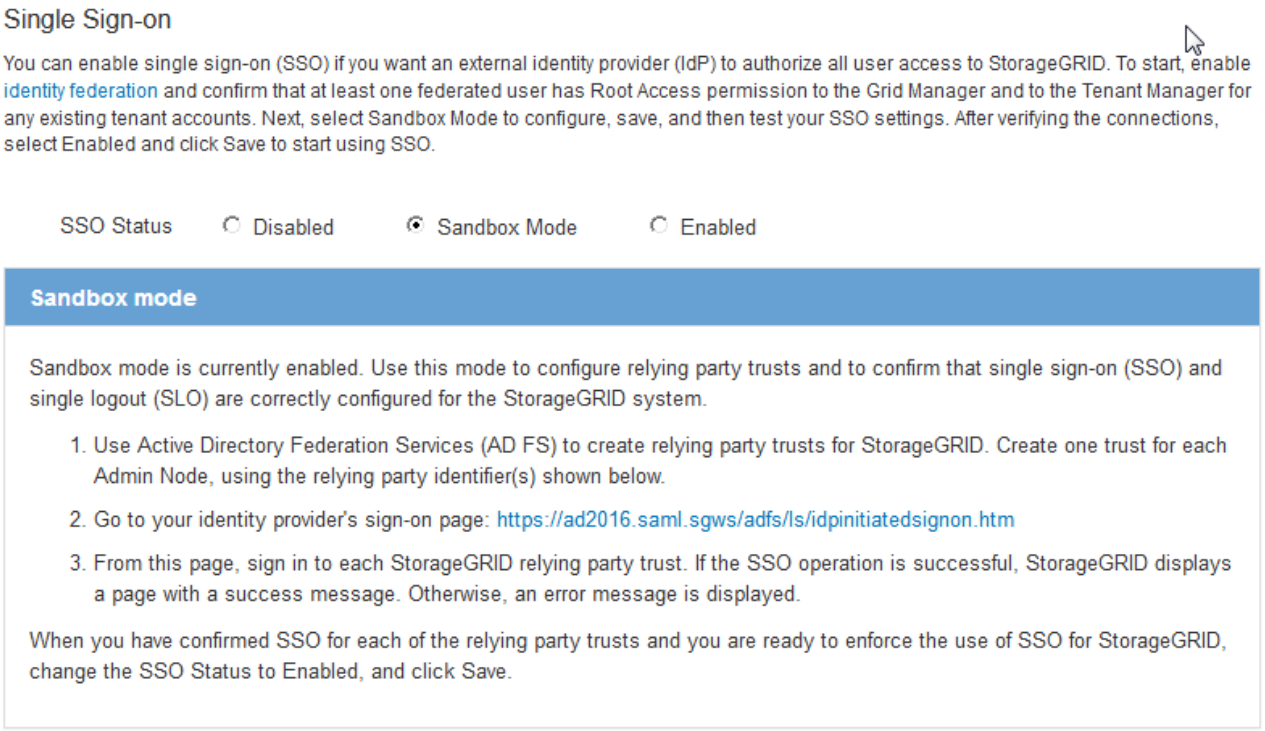
   - たとえば、グリッドに管理ノードが1つしかなく、今後管理ノードを追加する予定がない場合は、と入力します `SG` または `StorageGRID`。
   - グリッドに複数の管理ノードがある場合は、という文字列を含めます `[HOSTNAME]` を入力します。例： `SG-[HOSTNAME]`。これにより、管理ノードのホスト名に基づいて、各管理ノードの証明書利用者IDを含むテーブルが生成されます。+注：証明書利用者信頼はStorageGRID システム内の管理ノードごとに作成する必要があります。管理ノードごとに証明書利用者信頼を作成することで、ユーザは管理ノードに対して安全にサインイン / サインアウトすることができます。

5. [保存（ Save ）] をクリックします。

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

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



関連情報

"シングルサインオンの使用要件"

AD FSでの証明書利用者信頼の作成

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

Windows PowerShellを使用した証明書利用者信頼の作成

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

必要なもの

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

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

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

このタスクについて

以下の手順は、Windows Server 2016に付属のAD FS 4.0での手順です。Windows Server 2012 R2に含まれて

いるAD FS 3.0を使用している場合は、手順 にわずかな違いがあります。不明な点がある場合は、 Microsoft AD FS のドキュメントを参照してください。

手順

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

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

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

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

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

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

i. [完了]をクリックし、[OK]をクリックします。

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

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

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

フェデレーションメタデータをインポートして証明書利用者信頼を作成する

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

必要なもの

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

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

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

このタスクについて

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

手順

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

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

   の場合 `Admin_Node_FQDN` をクリックし、同じ管理ノードの完全修飾ドメイン名を入力します。（必要

に応じて、ノードの IP アドレスを代わりに使用できます。ただし、 IP アドレスを入力した場合、その IP アドレスが変わったときには証明書利用者信頼を更新または再作成する必要があります）。

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

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

7. クレームルールを追加します。
   a. 信頼を右クリックし、 ［ * クレーム発行ポリシーの編集 * ］ を選択します。
   b. [ルールの追加：]をクリックします。
   c. ［ルールテンプレートの選択］ページで、リストから［* LDAP属性をクレームとして送信*］を選択し、［次へ］をクリックします。
   d. ［ ルールの設定 ］ ページで、このルールの表示名を入力します。

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

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

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

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

証明書利用者信頼の手動作成

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

必要なもの

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

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

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

このタスクについて

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

手順

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

   a. この管理ノードの表示名を入力します。

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

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

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

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

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

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

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

      Admin_Node_Identifier

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

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

[クレーム発行ポリシーの編集] ダイアログボックスが表示されます。

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

6. ［クレームルール］ウィザードを開始するには、［ルールの追加］をクリックします。
   a. ［ルールテンプレートの選択］ページで、リストから［* LDAP属性をクレームとして送信*］を選択し、［次へ］をクリックします。
   b. ［ ルールの設定 ］ ページで、このルールの表示名を入力します。

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

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

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

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

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

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

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

証明書利用者のプロパティが保存されて閉じられます。

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

証明書利用者信頼のテスト

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

必要なもの

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

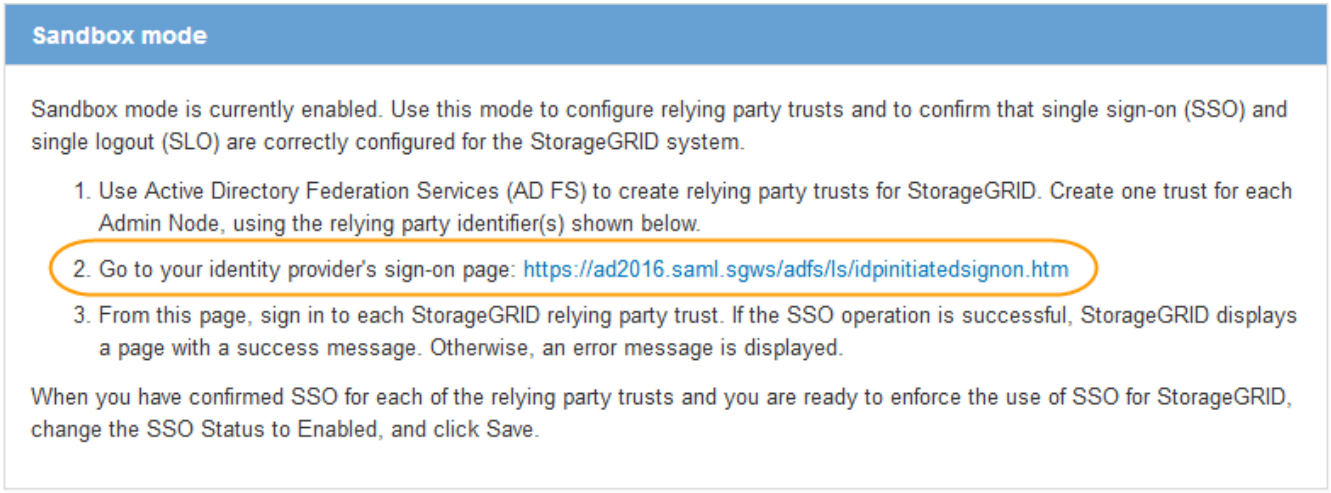
手順

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

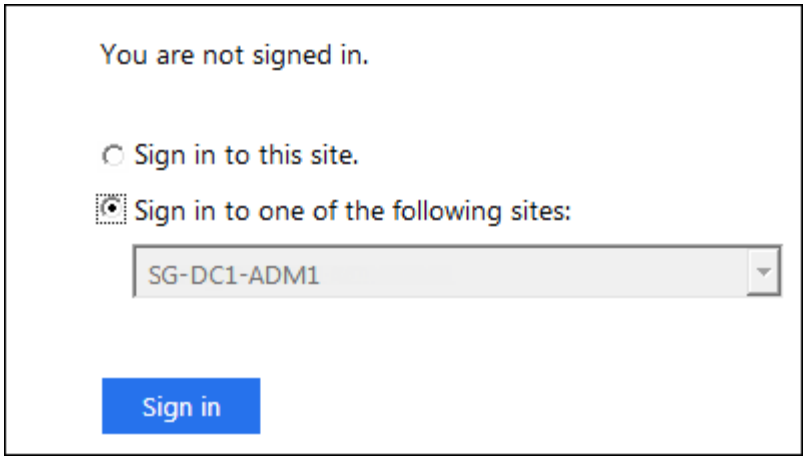
   [シングルサインオン]ページが表示され、[サンドボックスモード]オプションが選択されます。

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

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



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



ユーザ名とパスワードの入力を求めるプロンプトが表示されます。

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

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

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

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

シングルサインオンの有効化

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

必要なもの

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

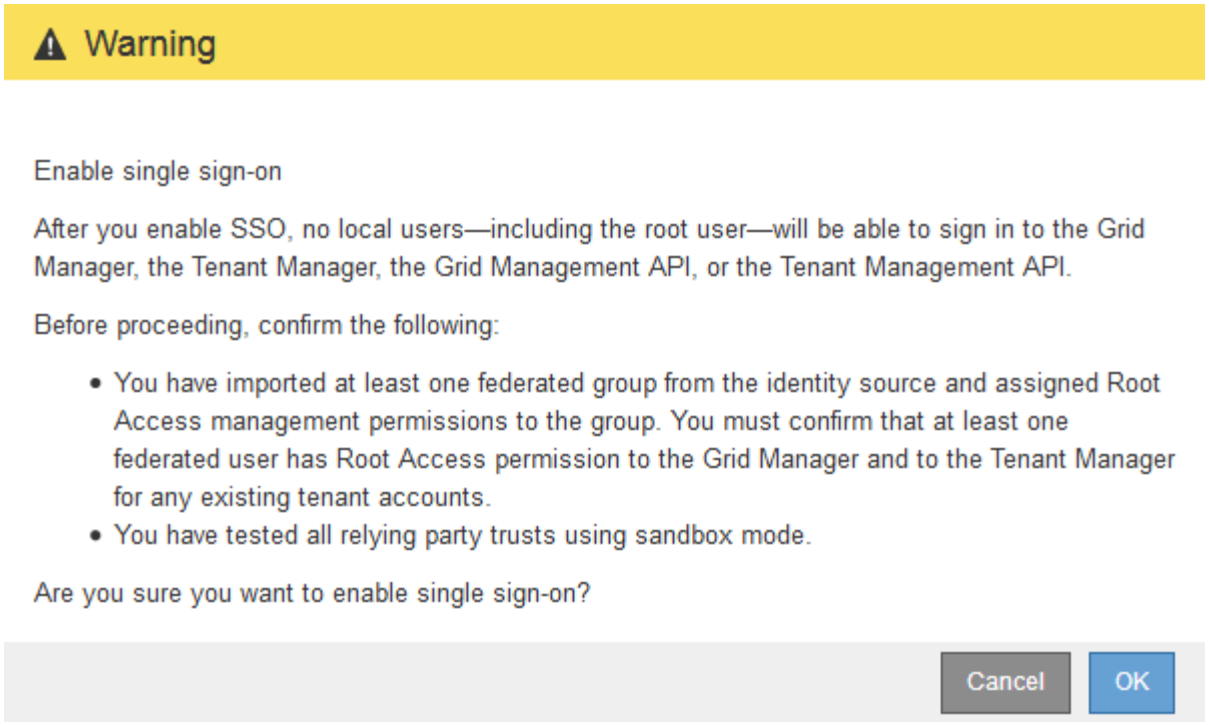
手順

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

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

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

   警告メッセージが表示されます。



4. 警告を確認し、* OK *をクリックします。

   シングルサインオンが有効になりました。

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

シングルサインオンを無効にしています

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

必要なもの

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

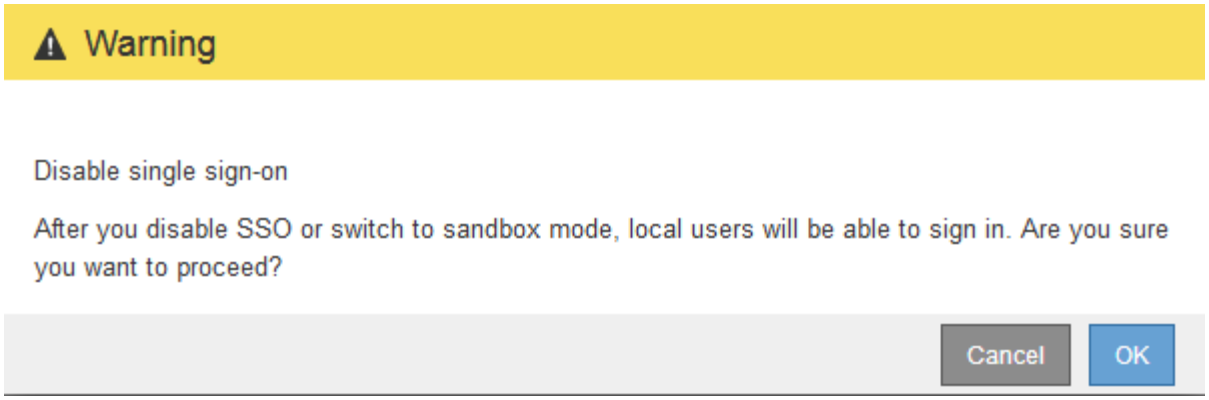
手順

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

   [Single Sign-On] ページが表示されます。

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

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



4. [OK] をクリックします。

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

1つの管理ノードのシングルサインオンの一時的な無効化と再有効化

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

必要なもの

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

このタスクについて

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

> 1 つの管理ノードに対して SSO を無効にしても、グリッド内の他の管理ノードの SSO 設定には影響しません。Grid Manager のシングルサインオンページの * SSO * を有効にするチェックボックスはオンのままで、既存の SSO 設定はすべて更新しないかぎり維持されます。

手順

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

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

2. 次のコマンドを実行します。`disable-saml`

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

3. SSO を無効にすることを確認します。

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

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

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

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

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

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

      - 次のコマンドを実行します。 `enable-saml`

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

      SSO を有効にすることを確認します。

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

   - グリッドノードをリブートします。 `reboot`

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

関連情報

"シングルサインオンを設定しています"

管理者クライアント証明書の設定

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

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

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

管理者クライアント証明書を追加する

クライアント証明書を追加するには、独自の証明書を指定するか、またはGrid Managerを使用して証明書を生成します。

必要なもの

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

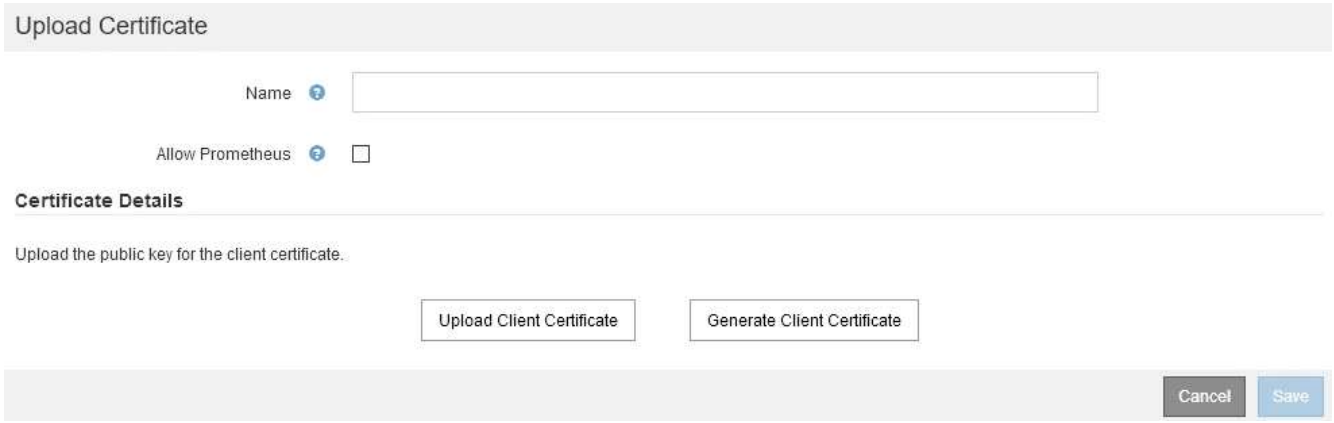
手順

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

   [Client Certificates]ページが表示されます。

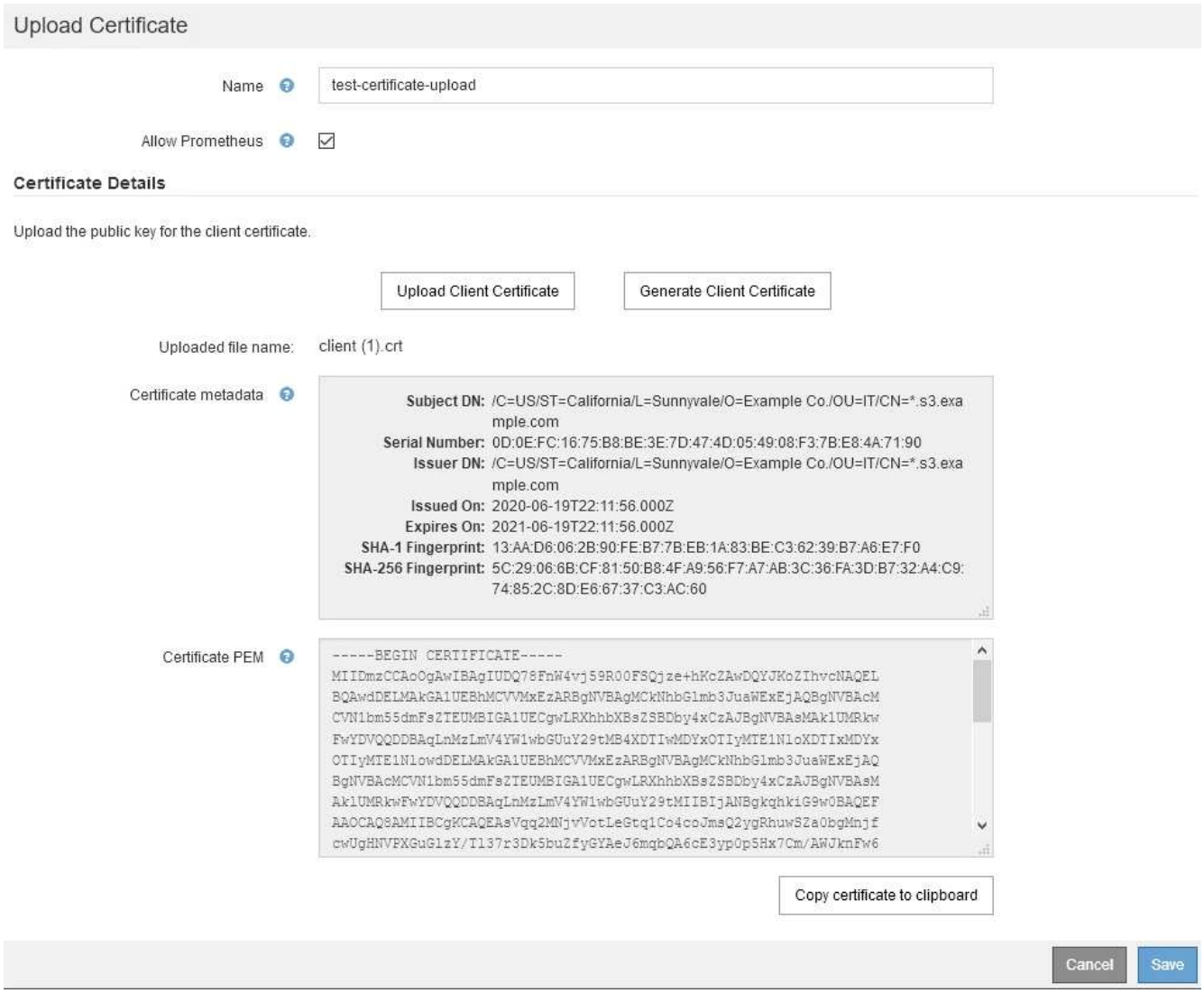
2. 「 * 追加」を選択します。

   証明書のアップロードページが表示されます。



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

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



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

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

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

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

a. [クライアント証明書の生成]を選択します。

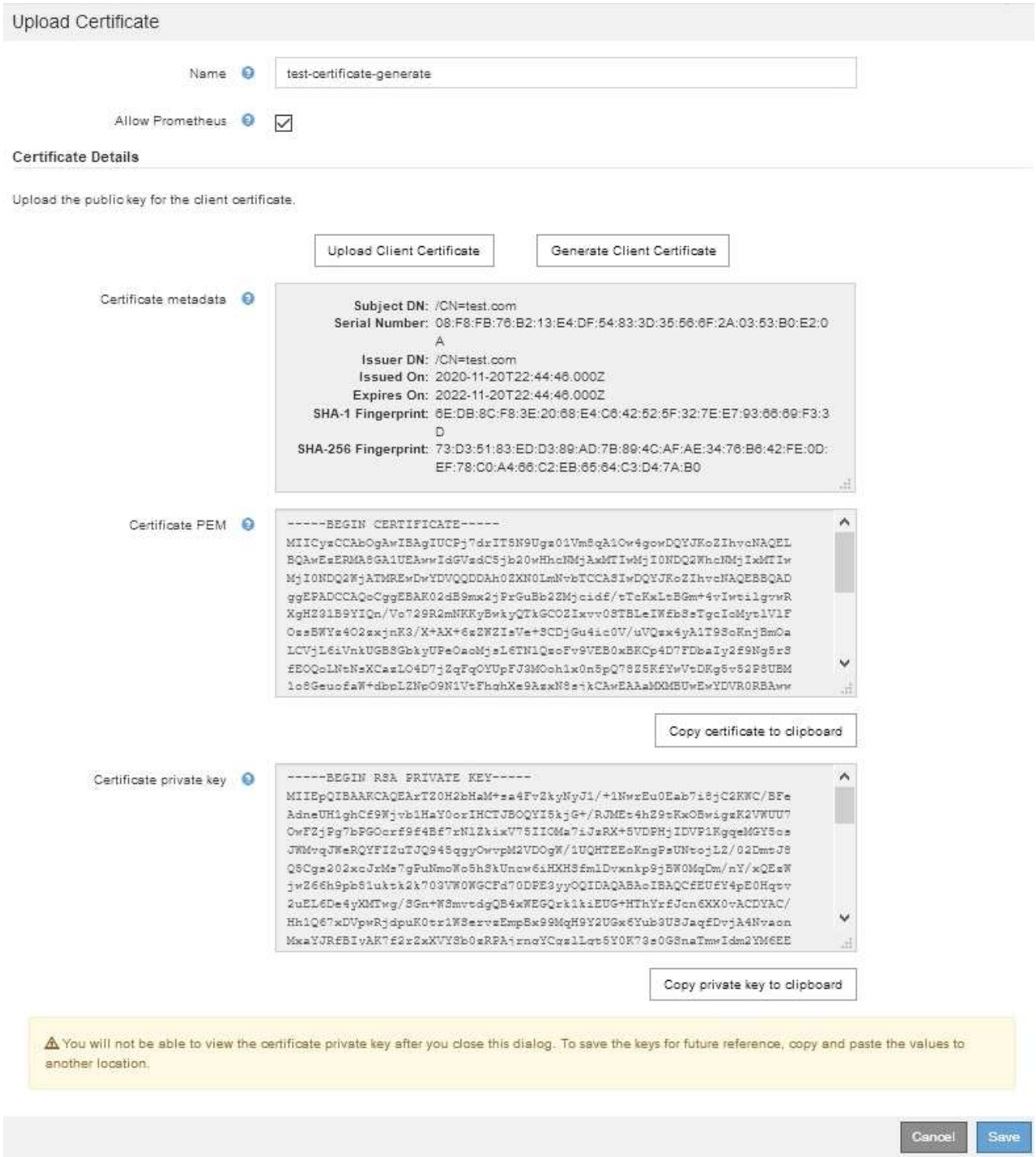
b. 管理ノードのドメイン名またはIPアドレスを入力します。

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

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

e. [*Generate （生成）] を選択します

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



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

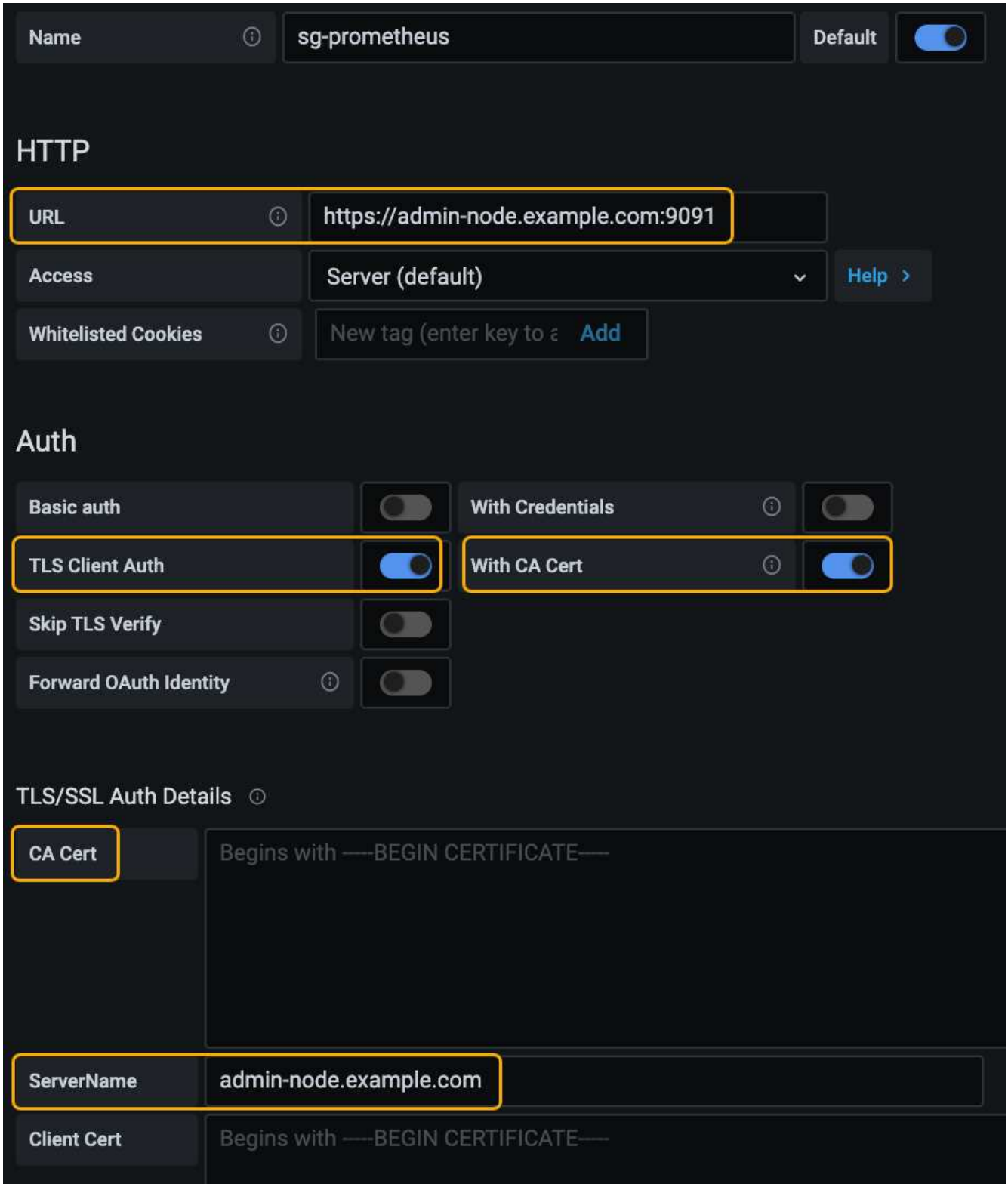
b. 秘密鍵をクリップボードにコピー*を選択し、外部監視ツールに貼り付けます。

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

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

8. Grafana などの外部監視ツールで次の設定を行います。

Grafana の例は次のスクリーンショットで示されています。



a. * 名前 * ：接続の名前を入力します。

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

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

ます。

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

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

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

e. * ServerName* ：管理ノードのドメイン名を入力します。

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

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

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

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

関連情報

"StorageGRID セキュリティ証明書を使用する"

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

"トラブルシューティングを監視します"

管理者クライアント証明書の編集

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

必要なもの

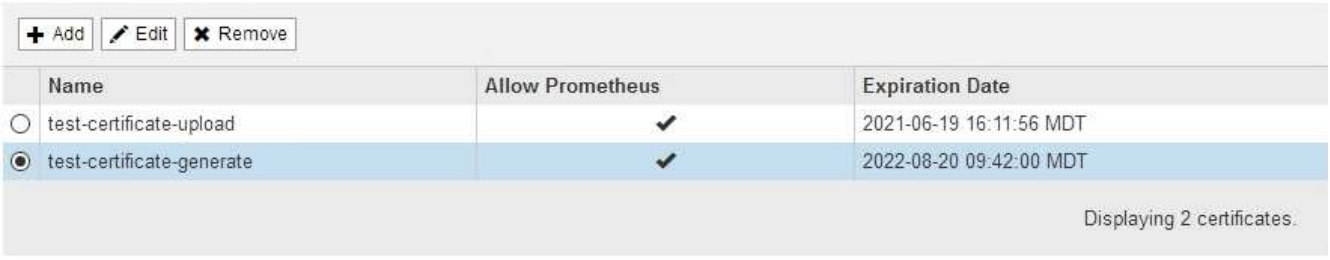
- Root Access 権限が必要です。
- Grid Managerにはサポートされているブラウザを使用してサインインする必要があります。
- 管理ノードのIPアドレスまたはドメイン名を確認しておく必要があります。
- 新しい証明書と秘密鍵をアップロードする場合は、ローカルコンピュータ上でそれらの証明書が使用可能である必要があります。

手順

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

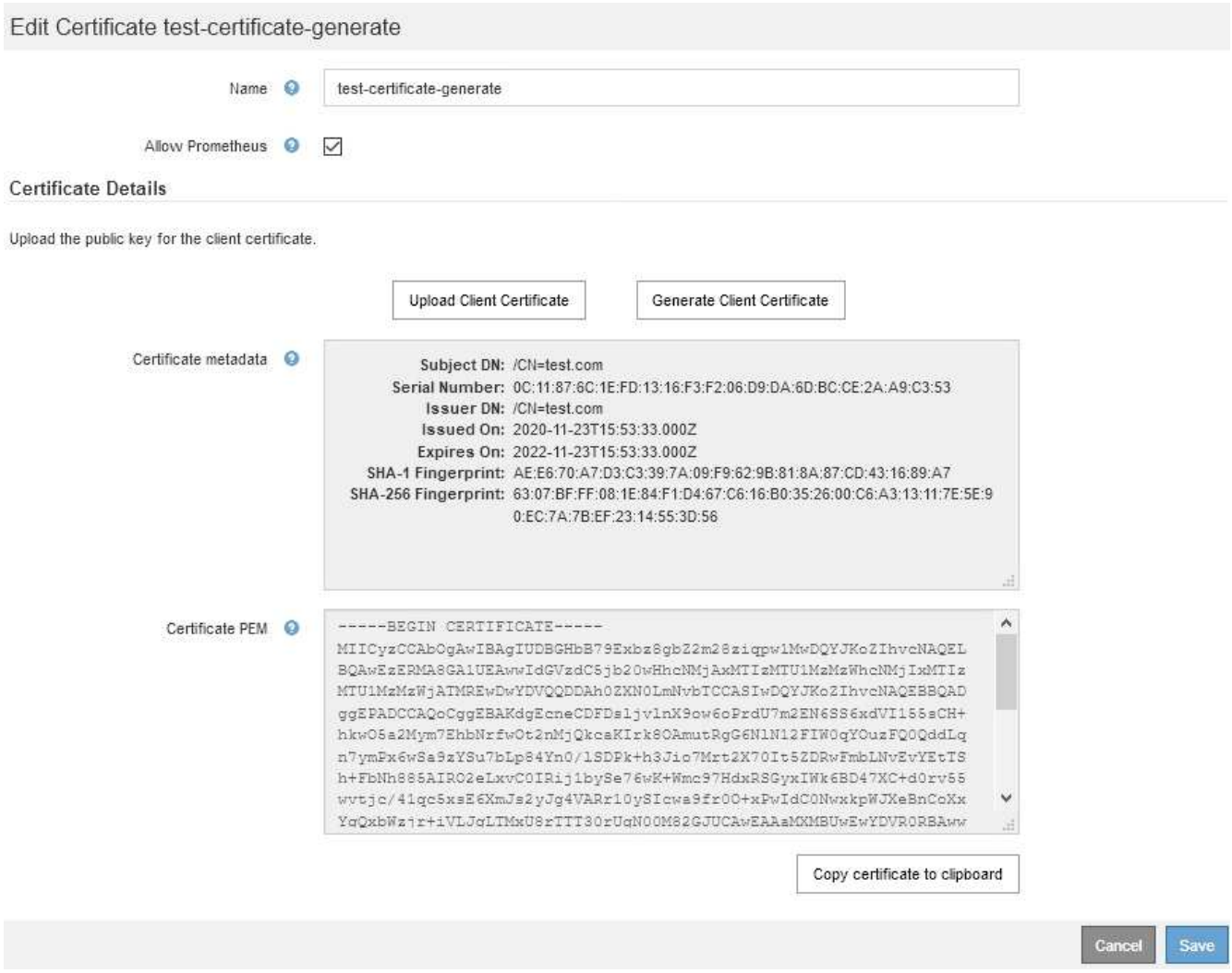
[Client Certificates]ページが表示されます。既存の証明書のリストが表示されます。

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



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

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



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

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

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

   c. 外部の監視ツールで証明書と秘密鍵を保存してテストします。

管理者クライアント証明書を削除しています

不要になった証明書は削除できます。

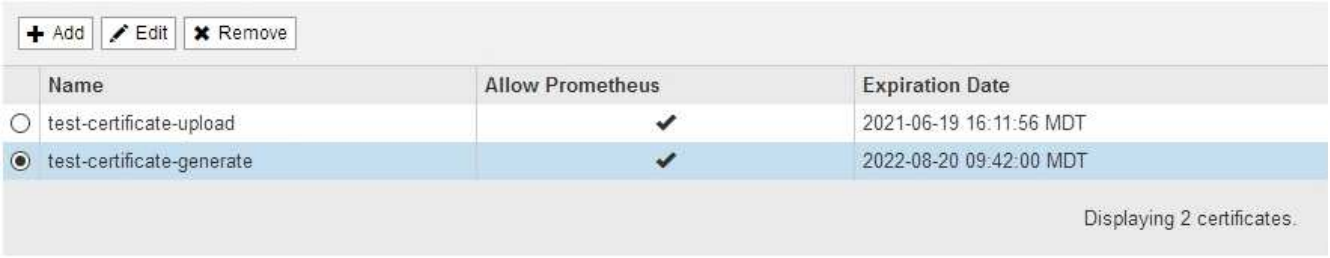
必要なもの

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

手順

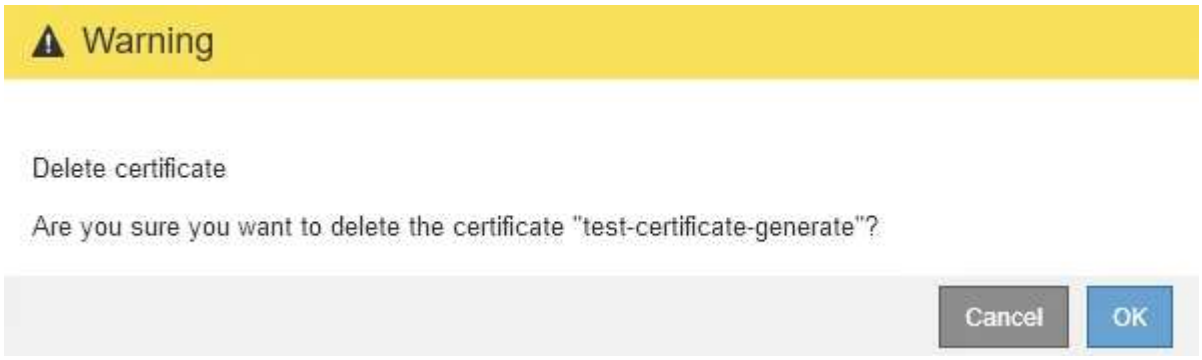
1. [* Configuration > Access Control > Client Certificates *]を選択します。

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



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

   確認のダイアログボックスが表示されます。



4. 「 * OK 」を選択します。

証明書が削除されます。

著作権に関する情報

商標に関する情報