証明書の管理
StorageGRID software

NetApp
December 03, 2025

目次

証明書の管理 1
- セキュリティ証明書を管理する 1
  - セキュリティ証明書にアクセスする 2
  - セキュリティ証明書の詳細 5
  - 証明書の例 11
- サポートされているサーバー証明書の種類 12
- 管理インターフェース証明書を構成する 12
  - カスタム管理インターフェース証明書を追加する 13
  - デフォルトの管理インターフェース証明書を復元する 16
  - スクリプトを使用して新しい自己署名管理インターフェース証明書を生成する 16
  - 管理インターフェース証明書をダウンロードまたはコピーします 17
- S3 API証明書を設定する 18
  - カスタムS3 API証明書を追加する 19
  - デフォルトのS3 API証明書を復元する 22
  - S3 API証明書をダウンロードまたはコピーします 22
- グリッドCA証明書をコピーする 23
- FabricPoolのStorageGRID証明書を構成する 24
- クライアント証明書を構成する 25
  - クライアント証明書を追加する 26
  - クライアント証明書を編集する 29
  - 新しいクライアント証明書を添付する 29
  - クライアント証明書をダウンロードまたはコピーする 32
  - クライアント証明書を削除する 33

証明書の管理

セキュリティ証明書を管理する

セキュリティ証明書は、 StorageGRIDコンポーネント間およびStorageGRIDコンポーネントと外部システム間の安全で信頼できる接続を作成するために使用される小さなデータ ファイルです。

StorageGRID は2 種類のセキュリティ証明書を使用します。

- HTTPS 接続を使用する場合は、サーバー証明書 が必要です。サーバー証明書は、クライアントとサーバー間の安全な接続を確立し、クライアントに対してサーバーの ID を認証し、データの安全な通信パスを提供するために使用されます。サーバーとクライアントはそれぞれ証明書のコピーを持ちます。
- クライアント証明書 は、クライアントまたはユーザーの ID をサーバーに対して認証し、パスワードのみを使用する場合よりも安全な認証を提供します。クライアント証明書はデータを暗号化しません。

クライアントが HTTPS を使用してサーバーに接続すると、サーバーは公開キーを含むサーバー証明書で応答します。クライアントは、サーバーの署名を証明書のコピーの署名と比較することによって、この証明書を検証します。署名が一致する場合、クライアントは同じ公開鍵を使用してサーバーとのセッションを開始します。

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

デフォルトのグリッド**CA**証明書

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

- カスタム CA 証明書では内部証明書は削除されませんが、カスタム証明書はサーバー接続の検証用に指定する必要があります。
- すべてのカスタム証明書は、"サーバー証明書のシステム強化ガイドライン" 。
- StorageGRID は、CA からの証明書を 1 つのファイルにバンドルすること (CA 証明書バンドルと呼ばれる) をサポートしています。

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

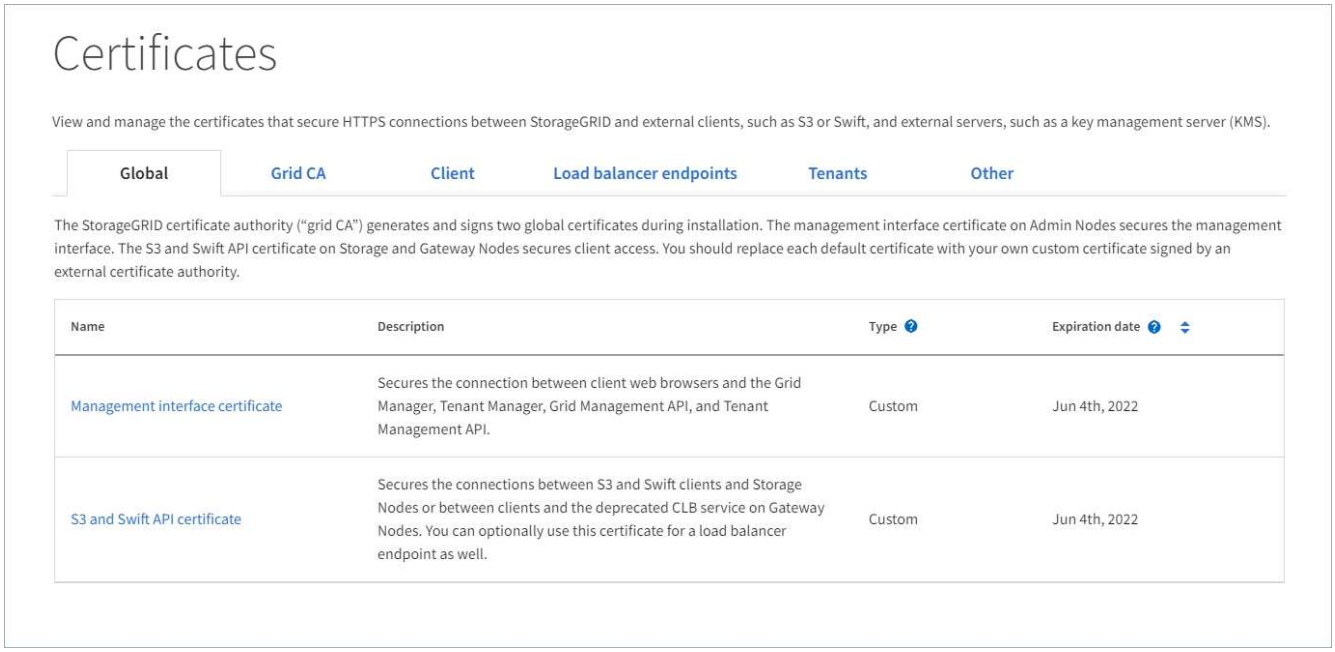
サーバー証明書とクライアント証明書の種類のバリエーションは、いくつかの方法で実装されます。システムを構成する前に、特定のStorageGRID構成に必要なすべての証明書を準備しておく必要があります。

セキュリティ証明書にアクセスする

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

手順

1. Grid Manager から、構成 > セキュリティ > 証明書 を選択します。



2. 各証明書カテゴリに関する情報や証明書設定にアクセスするには、「証明書」ページのタブを選択します。タブにアクセスするには、"適切な許可" 。

   - グローバル: Web ブラウザおよび外部 API クライアントからのStorageGRIDアクセスを保護します。
   - グリッド **CA**: 内部StorageGRIDトラフィックを保護します。
   - クライアント: 外部クライアントとStorageGRID Prometheus データベース間の接続を保護します。
   - ロード バランサ エンドポイント: S3 クライアントとStorageGRIDロード バランサ間の接続を保護します。
   - テナント: ID フェデレーション サーバーへの接続、またはプラットフォーム サービス エンドポイントから S3 ストレージ リソースへの接続を保護します。
   - その他: 特定の証明書を必要とするStorageGRID接続を保護します。

     各タブについては、追加の証明書の詳細へのリンクとともに以下で説明します。

グローバル

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

- [管理インターフェース証明書]: StorageGRID管理インターフェイスへのクライアント Web ブラウザ接続を保護します。
- S3 API証明書: S3 クライアント アプリケーションがオブジェクト データのアップロードとダウンロードに使用するストレージ ノード、管理ノード、ゲートウェイ ノードへのクライアント API 接続を保護します。

インストールされているグローバル証明書に関する情報は次のとおりです。

- 名前: 証明書を管理するためのリンクを含む証明書の名前。
- 説明
- タイプ: カスタムまたはデフォルト。 + グリッドのセキュリティを強化するには、常にカスタム証明書を使用する必要があります。
- 有効期限: デフォルトの証明書を使用している場合、有効期限は表示されません。

次の操作を実行できます。

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

グリッド**CA**

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

証明書情報には、証明書の有効期限と証明書の内容が含まれます。

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

クライアント

クライアント証明書外部証明機関によって生成された証明書は、外部監視ツールとStorageGRID Prometheus データベース間の接続を保護します。

証明書テーブルには、構成されたクライアント証明書ごとに行があり、証明書の有効期限とともに、証明書が Prometheus データベース アクセスに使用できるかどうかが示されます。

次の操作を実行できます。

- "新しいクライアント証明書をアップロードまたは生成します。"
- 証明書名を選択すると、証明書の詳細が表示され、次の操作を実行できます。
  - "クライアント証明書の名前を変更します。"
  - "Prometheus のアクセス権限を設定します。"
  - "クライアント証明書をアップロードして置き換えます。"
  - "クライアント証明書をコピーまたはダウンロードします。"
  - "クライアント証明書を削除します。"
- アクション*を選択してすぐに"編集"、"添付する" 、 または"削除"クライアント証明書。 *アクション > 削除 を使用して、最大 10 個のクライアント証明書を選択して一度に削除できます。

ロード バランサ エンドポイント

ロードバランサのエンドポイント証明書ゲートウェイ ノードおよび管理ノード上の S3 クライアントとStorageGRIDロード バランサ サービス間の接続を保護します。

ロード バランサー エンドポイント テーブルには、構成されたロード バランサー エンドポイントごとに 1 行あり、エンドポイントにグローバル S3 API 証明書が使用されているか、カスタム ロード バランサー エンドポイント証明書が使用されているかを示します。各証明書の有効期限も表示されます。

> エンドポイント証明書の変更がすべてのノードに適用されるまでに最大 15 分かかる場合があります。

次の操作を実行できます。

- "ロードバランサのエンドポイントを表示する"（証明書の詳細を含む）
- "FabricPoolのロード バランサ エンドポイント証明書を指定します。"
- "グローバルS3 API証明書を使用する"新しいロードバランサのエンドポイント証明書を生成する代わりに。

テナント

テナントはIDフェデレーションサーバー証明書またはプラットフォームサービスエンドポイント証明書StorageGRIDとの接続を保護します。

テナント テーブルにはテナントごとに 1 行あり、各テナントに独自の ID ソースまたはプラットフォーム サービスを使用する権限があるかどうかを示します。

次の操作を実行できます。

- "テナント名を選択してテナント マネージャーにサインインします"
- "テナントIDフェデレーションの詳細を表示するには、テナント名を選択してください"
- "テナント名を選択して、テナント プラットフォーム サービスの詳細を表示します。"

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

その他

StorageGRID は特定の目的のために他のセキュリティ証明書を使用します。これらの証明書は機能名別にリストされています。その他のセキュリティ証明書には次のものがあります:

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

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

他の証明書の情報を閲覧したりアクセスしたりするには、"適切な許可" 。

次の操作を実行できます。

- "S3、C2S S3、またはAzureのクラウドストレージプール証明書を指定します"
- "アラートメール通知用の証明書を指定する"
- "外部Syslogサーバーの証明書を使用する"
- "グリッドフェデレーション接続証明書のローテーション"
- "ID フェデレーション証明書の表示と編集"
- "キー管理サーバー（KMS）のサーバー証明書とクライアント証明書をアップロードする"
- "証明書利用者信頼の SSO 証明書を手動で指定する"

セキュリティ証明書の詳細

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

管理インターフェース証明書

証明書の種類	説明	ナビゲーション位置	詳細
サーバ	クライアント Web ブラウザとStorageGRID管理インターフェイス間の接続を認証し、ユーザーがセキュリティ警告なしで Grid Manager および Tenant Manager にアクセスできるようにします。 この証明書は、グリッド管理 API およびテナント管理 API 接続も認証します。 インストール中に作成されたデフォルトの証明書を使用することも、カスタム証明書をアップロードすることもできます。	構成 > セキュリティ > *証明書*で、*グローバル*タブを選択し、*管理インターフェース証明書*を選択します。	"管理インターフェース証明書を構成する"

S3 API証明書

証明書の種類	説明	ナビゲーション位置	詳細
サーバ	ストレージ ノードおよびロード バランサ エンドポイントへの安全な S3 クライアント接続を認証します (オプション)。	構成 > セキュリティ > 証明書、*グローバル*タブを選択し、*S3 API証明書*を選択します。	"S3 API証明書を設定する"

グリッド **CA** 証明書

参照デフォルトのグリッドCA証明書の説明。

管理者クライアント証明書

証明書の種類	説明	ナビゲーション位置	詳細
クライアント	各クライアントにインストールされ、StorageGRID が外部クライアント アクセスを認証できるようになります。 • 承認された外部クライアントがStorageGRID Prometheus データベースにアクセスできるようにします。 • 外部ツールを使用してStorageGRIDを安全に監視できます。	構成 > セキュリティ > 証明書 を選択し、クライアント タブを選択します。	"クライアント証明書を構成する"

ロードバランサのエンドポイント証明書

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

クラウド ストレージ プールのエンドポイント証明書

証明書の種類	説明	ナビゲーション位置	詳細
サーバ	StorageGRIDクラウド ストレージ プールから S3 Glacier や Microsoft Azure Blob ストレージなどの外部ストレージの場所への接続を認証します。クラウド プロバイダーの種類ごとに異なる証明書が必要です。	**ILM** > ストレージプール	"クラウドストレージプールを作成する"

電子メールアラート通知証明書

証明書の種類	説明	ナビゲーション位置	詳細
サーバーとクライアント	アラート通知に使用される SMTP 電子メール サーバーとStorageGRID間の接続を認証します。 • SMTP サーバーとの通信にトランスポート層セキュリティ (TLS) が必要な場合は、電子メール サーバーの CA 証明書を指定する必要があります。 • SMTP 電子メール サーバーが認証にクライアント証明書を必要とする場合にのみ、クライアント証明書を指定します。	アラート > メール設定	"アラートのメール通知を設定する"

外部 **syslog** サーバー証明書

証明書の種類	説明	ナビゲーション位置	詳細
サーバ	StorageGRIDにイベントを記録する外部 syslog サーバー間の TLS または RELP/TLS 接続を認証します。 注: 外部 syslog サーバへの TCP、RELP/TCP、および UDP 接続には、外部 syslog サーバ証明書は必要ありません。	構成 > 監視 > 監査および**Syslog**サーバー	"外部のSyslogサーバーを使用する"

グリッドフェデレーション接続証明書

証明書の種類	説明	ナビゲーション位置	詳細
サーバーとクライアント	現在のStorageGRIDシステムとグリッド フェデレーション接続内の別のグリッド間で送信される情報を認証および暗号化します。	構成 > システム > グリッドフェデレーション	• "グリッドフェデレーション接続を作成する" • "接続証明書をローテーションする"

アイデンティティフェデレーション証明書

証明書の種類	説明	ナビゲーション位置	詳細
サーバ	StorageGRIDと Active Directory、OpenLDAP、Oracle Directory Server などの外部 ID プロバイダー間の接続を認証します。管理者グループとユーザーを外部システムで管理できるようにする ID フェデレーションに使用されます。	構成 > アクセス制御 > アイデンティティ連携	"アイデンティティフェデレーションを使用する"

キー管理サーバー（**KMS**）証明書

証明書の種類	説明	ナビゲーション位置	詳細
サーバーとクライアント	StorageGRIDと、StorageGRIDアプライアンス ノードに暗号化キーを提供する外部キー管理サーバー (KMS) 間の接続を認証します。	構成 > セキュリティ > キー管理サーバー	"キー管理サーバー（KMS）を追加する"

プラットフォーム サービス エンドポイント証明書

証明書の種類	説明	ナビゲーション位置	詳細
サーバ	StorageGRIDプラットフォーム サービスから S3 ストレージ リソースへの接続を認証します。	テナント マネージャー > ストレージ **(S3)** > プラットフォーム サービス エンドポイント	"プラットフォーム サービス エンドポイントを作成する" "プラットフォーム サービス エンドポイントを編集する"

シングルサインオン（**SSO**）証明書

証明書の種類	説明	ナビゲーション位置	詳細
サーバ	Active Directory フェデレーション サービス (AD FS) などの ID フェデレーション サービスと、シングル サインオン (SSO) 要求に使用されるStorageGRID間の接続を認証します。	設定 > アクセス制御 > シングルサインオン	"シングルサインオンを構成する"

証明書の例

例**1:** ロードバランササービス

この例では、 StorageGRID がサーバーとして機能します。

1. ロード バランサのエンドポイントを構成し、 StorageGRIDでサーバー証明書をアップロードまたは生成します。
2. ロードバランサーエンドポイントへの S3 クライアント接続を構成し、同じ証明書をクライアントにアップロードします。
3. クライアントがデータを保存または取得する場合、HTTPS を使用してロード バランサー エンドポイントに接続します。
4. StorageGRID は、公開キーを含むサーバー証明書と、秘密キーに基づく署名で応答します。
5. クライアントは、サーバーの署名を証明書のコピーの署名と比較することによって、この証明書を検証します。署名が一致する場合、クライアントは同じ公開鍵を使用してセッションを開始します。
6. クライアントはオブジェクト データをStorageGRIDに送信します。

例**2:** 外部キー管理サーバー **(KMS)**

この例では、 StorageGRID がクライアントとして機能します。

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

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

サポートされているサーバー証明書の種類

StorageGRIDシステムは、RSA または ECDSA (楕円曲線デジタル署名アルゴリズム) で暗号化されたカスタム証明書をサポートします。

> セキュリティ ポリシーの暗号タイプは、サーバー証明書タイプと一致する必要があります。たとえば、RSA 暗号には RSA 証明書が必要であり、ECDSA 暗号には ECDSA 証明書が必要です。見る"セキュリティ証明書を管理する" 。サーバー証明書と互換性のないカスタムセキュリティポリシーを構成する場合は、"一時的にデフォルトのセキュリティポリシーに戻す" 。

StorageGRIDがクライアント接続を保護する方法の詳細については、以下を参照してください。"S3 クライアントのセキュリティ" 。

管理インターフェース証明書を構成する

デフォルトの管理インターフェイス証明書を単一のカスタム証明書に置き換えて、ユーザーがセキュリティ警告に遭遇することなく Grid Manager および Tenant Manager にアクセスできるようにすることができます。デフォルトの管理インターフェイス証明書に戻したり、新しい証明書を生成したりすることもできます。

タスク概要

デフォルトでは、すべての管理ノードにグリッド CA によって署名された証明書が発行されます。これらの CA 署名付き証明書は、単一の共通カスタム管理インターフェイス証明書と対応する秘密キーに置き換えることができます。

すべての管理ノードに単一のカスタム管理インターフェイス証明書が使用されるため、クライアントが Grid Manager および Tenant Manager に接続するときにホスト名を検証する必要がある場合は、証明書をワイルドカードまたはマルチドメイン証明書として指定する必要があります。グリッド内のすべての管理ノードと一致するようにカスタム証明書を定義します。

サーバー上で構成を完了する必要があります。また、使用しているルート証明機関 (CA) によっては、ユーザーが Grid Manager および Tenant Manager にアクセスするために使用する Web ブラウザーに Grid CA 証明書をインストールする必要もあります。

> 失敗したサーバー証明書によって操作が中断されないように、このサーバー証明書の有効期限が近づくと、管理インターフェイスのサーバー証明書の有効期限*アラートがトリガーされます。必要に応じて、**[*CONFIGURATION]** > [**Security**] > [**Certificates**] を選択し、[Global] タブで管理インターフェイス証明書の有効期限を確認することで、現在の証明書の有効期限を確認できます。

IP アドレスではなくドメイン名を使用して Grid Manager または Tenant Manager にアクセスしている場合、次のいずれかが発生すると、ブラウザにバイパス オプションのない証明書エラーが表示されます。

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

カスタム管理インターフェース証明書を追加する

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

手順

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

証明書をアップロード

必要なサーバー証明書ファイルをアップロードします。

a. *証明書のアップロード*を選択します。

b. 必要なサーバー証明書ファイルをアップロードします。

- サーバー証明書: カスタム サーバー証明書ファイル (PEM エンコード)。
- 証明書の秘密鍵: カスタムサーバー証明書の秘密鍵ファイル(`.key`）。

> EC 秘密鍵は 224 ビット以上である必要があります。 RSA 秘密鍵は 2048 ビット以上である必要があります。

- **CA** バンドル: 各中間発行証明機関 (CA) からの証明書を含む単一のオプション ファイル。このファイルには、PEM でエンコードされた各 CA 証明書ファイルが、証明書チェーンの順序で連結されて含まれている必要があります。

c. *証明書の詳細*を展開して、アップロードした各証明書のメタデータを表示します。オプションの CA バンドルをアップロードした場合、各証明書は独自のタブに表示されます。

- 証明書ファイルを保存するには 証明書のダウンロード を選択するか、証明書バンドルを保存するには **CA** バンドルのダウンロード を選択します。

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

  例： `storagegrid_certificate.pem`

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

d. *保存*を選択します。+ カスタム管理インターフェイス証明書は、Grid Manager、Tenant Manager、Grid Manager API、または Tenant Manager API への以降のすべての新しい接続に使用されます。

証明書を生成する

サーバー証明書ファイルを生成します。

> 実稼働環境でのベスト プラクティスは、外部証明機関によって署名されたカスタム管理インターフェイス証明書を使用することです。

a. *証明書の生成*を選択します。

b. 証明書情報を指定します。

フィールド	説明
ドメイン名	証明書に含める 1 つ以上の完全修飾ドメイン名。複数のドメイン名を表すには、ワイルドカードとして * を使用します。

フィールド	説明
IP	証明書に含める 1 つ以上の IP アドレス。
件名（任意）	証明書所有者の X.509 サブジェクトまたは識別名 (DN)。 このフィールドに値が入力されない場合、生成された証明書では、最初のドメイン名または IP アドレスがサブジェクト共通名 (CN) として使用されます。
有効日数	証明書の有効期限が切れるまでの作成後日数。
キー使用拡張機能を追加する	選択した場合 (デフォルト、推奨)、生成された証明書にキー使用法と拡張キー使用法の拡張機能が追加されます。 これらの拡張機能は、証明書に含まれるキーの目的を定義します。 注意: 証明書にこれらの拡張機能が含まれている場合に古いクライアントとの接続の問題が発生しない限り、このチェックボックスをオンのままにしておきます。

c. *生成*を選択します。

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

   - 証明書ファイルを保存するには、[証明書のダウンロード] を選択します。

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

   例： `storagegrid_certificate.pem`

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

e. *保存*を選択します。+ カスタム管理インターフェイス証明書は、Grid Manager、Tenant Manager、Grid Manager API、または Tenant Manager API への以降のすべての新しい接続に使用されます。

5. ページを更新して、Web ブラウザが更新されていることを確認します。

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

6. カスタム管理インターフェイス証明書を追加すると、管理インターフェイス証明書ページに、使用中の証明書の詳細な証明書情報が表示されます。 + 必要に応じて証明書 PEM をダウンロードまたはコピーできます。

デフォルトの管理インターフェース証明書を復元する

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

手順

1. 構成 > セキュリティ > *証明書*を選択します。
2. *グローバル*タブで、*管理インターフェース証明書*を選択します。
3. *デフォルトの証明書を使用する*を選択します。

   デフォルトの管理インターフェイス証明書を復元すると、構成したカスタム サーバー証明書ファイルが削除され、システムから回復できなくなります。以降のすべての新しいクライアント接続には、デフォルトの管理インターフェイス証明書が使用されます。

4. ページを更新して、Web ブラウザが更新されていることを確認します。

スクリプトを使用して新しい自己署名管理インターフェース証明書を生成する

厳密なホスト名検証が必要な場合は、スクリプトを使用して管理インターフェイス証明書を生成できます。

開始する前に

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

タスク概要

実稼働環境でのベストプラクティスは、外部の証明機関によって署名された証明書を使用することです。

手順

1. 各管理ノードの完全修飾ドメイン名 (FQDN) を取得します。
2. プライマリ管理ノードにログインします。
   a. 次のコマンドを入力します。 `ssh admin@primary_Admin_Node_IP`
   b. 記載されているパスワードを入力してください `Passwords.txt`ファイル。
   c. ルートに切り替えるには、次のコマンドを入力します。 `su -`
   d. 記載されているパスワードを入力してください `Passwords.txt`ファイル。

      ルートとしてログインすると、プロンプトは `$`に `#`。

3. 新しい自己署名証明書を使用してStorageGRIDを構成します。

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

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

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

> ⓘ 証明書の有効期間は、 `make-certificate`実行されます。管理クライアントがStorageGRIDと同じタイム ソースに同期されていることを確認する必要があります。そうでない場合、クライアントは証明書を拒否する可能性があります。

```
$ sudo make-certificate --domains *.ui.storagegrid.example.com --type
management --days 720
```

結果の出力には、管理 API クライアントに必要な公開証明書が含まれます。

4. 証明書を選択してコピーします。

   選択範囲に BEGIN タグと END タグを含めます。

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

管理インターフェース証明書をダウンロードまたはコピーします

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

手順

1. 構成 > セキュリティ > *証明書*を選択します。
2. *グローバル*タブで、*管理インターフェース証明書*を選択します。
3. *サーバー*または*CAバンドル*タブを選択し、証明書をダウンロードまたはコピーします。

証明書ファイルまたは**CA**バンドルをダウンロードする

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

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

   CA バンドルをダウンロードする場合、CA バンドルのセカンダリ タブ内のすべての証明書が 1 つのファイルとしてダウンロードされます。

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

   例： `storagegrid_certificate.pem`

証明書または**CA**バンドル**PEM**のコピー

証明書のテキストをコピーして他の場所に貼り付けます。オプションの CA バンドルを使用している場合、バンドル内の各証明書はそれぞれのサブタブに表示されます。

a. 証明書 **PEM** のコピー または **CA** バンドル **PEM** のコピー を選択します。

   CA バンドルをコピーする場合、CA バンドルのセカンダリ タブ内のすべての証明書が一緒にコピーされます。

b. コピーした証明書をテキスト エディターに貼り付けます。

c. 拡張子をつけてテキストファイルを保存する `.pem`。

   例： `storagegrid_certificate.pem`

S3 API証明書を設定する

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

このバージョンのドキュメント サイトから Swift の詳細は削除されました。見る "StorageGRID 11.8: S3およびSwift API証明書の設定"。

タスク概要

デフォルトでは、すべてのストレージ ノードにグリッド CA によって署名された X.509 サーバー証明書が発行されます。これらの CA 署名付き証明書は、単一の共通カスタム サーバー証明書と対応する秘密キーに置き換えることができます。

すべてのストレージ ノードに単一のカスタム サーバー証明書が使用されるため、クライアントがストレージ エンドポイントに接続するときにホスト名を検証する必要がある場合は、証明書をワイルドカードまたはマルチドメイン証明書として指定する必要があります。グリッド内のすべてのストレージ ノードに一致するようにカスタム証明書を定義します。

サーバーでの設定が完了したら、使用しているルート証明機関 (CA) に応じて、システムにアクセスするために使用する S3 API クライアントに Grid CA 証明書をインストールする必要もあります。

> ⓘ 失敗したサーバー証明書によって操作が中断されないように、ルート サーバー証明書の有効期限が切れそうになると、**S3 API** のグローバル サーバー証明書の有効期限切れ アラートがトリガーされます。必要に応じて、[設定] > [セキュリティ] > [証明書] を選択し、[グローバル] タブで S3 API 証明書の有効期限を確認することで、現在の証明書の有効期限を確認できます。

カスタム S3 API 証明書をアップロードまたは生成できます。

カスタム**S3 API**証明書を追加する

手順

1. 構成 > セキュリティ > *証明書*を選択します。
2. *グローバル*タブで、*S3 API証明書*を選択します。
3. *カスタム証明書を使用する*を選択します。
4. 証明書をアップロードまたは生成します。

証明書をアップロード

必要なサーバー証明書ファイルをアップロードします。

a. *証明書のアップロード*を選択します。

b. 必要なサーバー証明書ファイルをアップロードします。

   - サーバー証明書: カスタム サーバー証明書ファイル (PEM エンコード)。
   - 証明書の秘密鍵: カスタムサーバー証明書の秘密鍵ファイル(`.key`）。

   > EC 秘密鍵は 224 ビット以上である必要があります。 RSA 秘密鍵は 2048 ビット以上である必要があります。

   - **CA** バンドル: 各中間発行証明機関からの証明書を含む単一のオプション ファイル。このファイルには、PEM でエンコードされた各 CA 証明書ファイルが、証明書チェーンの順序で連結されて含まれている必要があります。

c. 証明書の詳細を選択すると、アップロードされた各カスタム S3 API 証明書のメタデータと PEM が表示されます。オプションの CA バンドルをアップロードした場合、各証明書は独自のタブに表示されます。

   - 証明書ファイルを保存するには 証明書のダウンロード を選択するか、証明書バンドルを保存するには **CA** バンドルのダウンロード を選択します。

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

   例： `storagegrid_certificate.pem`

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

d. *保存*を選択します。

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

証明書を生成する

サーバー証明書ファイルを生成します。

a. *証明書の生成*を選択します。

b. 証明書情報を指定します。

フィールド	説明
ドメイン名	証明書に含める 1 つ以上の完全修飾ドメイン名。複数のドメイン名を表すには、ワイルドカードとして * を使用します。
IP	証明書に含める 1 つ以上の IP アドレス。

フィールド	説明
件名（任意）	証明書所有者の X.509 サブジェクトまたは識別名 (DN)。 このフィールドに値が入力されない場合、生成された証明書では、最初のドメイン名または IP アドレスがサブジェクト共通名 (CN) として使用されます。
有効日数	証明書の有効期限が切れるまでの作成後日数。
キー使用拡張機能を追加する	選択した場合 (デフォルト、推奨)、生成された証明書にキー使用法と拡張キー使用法の拡張機能が追加されます。 これらの拡張機能は、証明書に含まれるキーの目的を定義します。 注意: 証明書にこれらの拡張機能が含まれている場合に古いクライアントとの接続の問題が発生しない限り、このチェックボックスをオンのままにしておきます。

c. *生成*を選択します。

d. 証明書の詳細 を選択すると、生成されたカスタム S3 API 証明書のメタデータと PEM が表示されます。

- 証明書ファイルを保存するには、[証明書のダウンロード] を選択します。

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

例： `storagegrid_certificate.pem`

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

e. *保存*を選択します。

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

5. タブを選択すると、デフォルトのStorageGRIDサーバー証明書、アップロードされた CA 署名付き証明書、または生成されたカスタム証明書のメタデータが表示されます。

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

6. ページを更新して、Web ブラウザが更新されていることを確認します。

7. カスタム S3 API 証明書を追加すると、S3 API 証明書ページに、使用中のカスタム S3 API 証明書の詳細な証明書情報が表示されます。 + 必要に応じて証明書 PEM をダウンロードまたはコピーできます。

デフォルトのS3 API証明書を復元する

ストレージノードへの S3 クライアント接続にデフォルトの S3 API 証明書を使用するように戻すことができます。ただし、ロードバランサーエンドポイントにはデフォルトの S3 API 証明書は使用できません。

手順

1. 構成 > セキュリティ > *証明書*を選択します。
2. *グローバル*タブで、*S3 API証明書*を選択します。
3. *デフォルトの証明書を使用する*を選択します。

   グローバル S3 API 証明書のデフォルト バージョンを復元すると、設定したカスタム サーバー証明書ファイルが削除され、システムから復元できなくなります。デフォルトの S3 API 証明書は、ストレージ ノードへの後続の新しい S3 クライアント接続に使用されます。

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

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

5. ページを更新して、Web ブラウザが更新されていることを確認します。

S3 API証明書をダウンロードまたはコピーします

S3 API 証明書の内容を保存またはコピーして、他の場所で使用することができます。

手順

1. 構成 > セキュリティ > *証明書*を選択します。
2. *グローバル*タブで、*S3 API証明書*を選択します。
3. *サーバー*または*CAバンドル*タブを選択し、証明書をダウンロードまたはコピーします。

証明書ファイルまたは**CA**バンドルをダウンロードする

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

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

   CA バンドルをダウンロードする場合、CA バンドルのセカンダリ タブ内のすべての証明書が 1 つのファイルとしてダウンロードされます。

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

   例： `storagegrid_certificate.pem`

証明書または**CA**バンドル**PEM**のコピー

証明書のテキストをコピーして他の場所に貼り付けます。オプションの CA バンドルを使用している場合、バンドル内の各証明書はそれぞれのサブタブに表示されます。

a. 証明書 **PEM** のコピー または **CA** バンドル **PEM** のコピー を選択します。

   CA バンドルをコピーする場合、CA バンドルのセカンダリ タブ内のすべての証明書が一緒にコピーされます。

b. コピーした証明書をテキスト エディターに貼り付けます。

c. 拡張子をつけてテキストファイルを保存する `.pem`。

   例： `storagegrid_certificate.pem`

関連情報

- "S3 REST APIを使用する"
- "S3エンドポイントのドメイン名を設定する"

グリッド**CA**証明書をコピーする

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

開始する前に

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

タスク概要

カスタム サーバー証明書が構成されている場合、クライアント アプリケーションはカスタム サーバー証明書を使用してサーバーを検証する必要があります。 StorageGRIDシステムから CA 証明書をコピーしないでください。

手順

1. 構成 > セキュリティ > 証明書 を選択し、グリッド **CA** タブを選択します。
2. 証明書 **PEM** セクションで、証明書をダウンロードまたはコピーします。

証明書ファイルをダウンロード

証明書をダウンロードする `.pem`ファイル。

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

例： `storagegrid_certificate.pem`

証明書**PEM**のコピー

証明書のテキストをコピーして他の場所に貼り付けます。

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

例： `storagegrid_certificate.pem`

FabricPoolのStorageGRID証明書を構成する

FabricPoolを使用するONTAPクライアントなど、厳密なホスト名検証を実行し、厳密なホスト名検証の無効化をサポートしていない S3 クライアントの場合は、ロードバランサのエンドポイントを設定するときにサーバ証明書を生成またはアップロードできます。

開始する前に

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

タスク概要

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

次の手順は、 FabricPoolを使用する S3 クライアントの一般的なガイドラインを示しています。詳しい情報と手順については、"FabricPool用にStorageGRIDを構成する" 。

手順

1. 必要に応じて、 FabricPoolが使用する高可用性 (HA) グループを構成します。
2. FabricPoolが使用する S3 ロード バランサ エンドポイントを作成します。

   HTTPS ロード バランサ エンドポイントを作成すると、サーバー証明書、証明書の秘密キー、およびオプションの CA バンドルをアップロードするように求められます。

3. StorageGRID をONTAPのクラウド層として接続します。

   アップロードした CA 証明書で使用されるロード バランサーのエンドポイント ポートと完全修飾ドメイン名を指定します。次に、CA 証明書を提供します。

   中間 CA がStorageGRID証明書を発行した場合は、中間 CA 証明書を提供する必要があります。 StorageGRID証明書がルート CA によって直接発行された場合は、ルート CA 証明書を提供する必要があります。

クライアント証明書を構成する

クライアント証明書により、承認された外部クライアントがStorageGRID Prometheusデータベースにアクセスできるようになり、外部ツールがStorageGRID を安全に監視できるようになります。

外部監視ツールを使用してStorageGRIDにアクセスする必要がある場合は、Grid Manager を使用してクライアント証明書をアップロードまたは生成し、証明書情報を外部ツールにコピーする必要があります。

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

失敗したサーバー証明書によって操作が中断されないように、このサーバー証明書の有効期限が近づくと、*証明書ページで構成されたクライアント証明書の有効期限*アラートがトリガーされます。必要に応じて、[構成] > [セキュリティ] > [証明書] を選択し、[クライアント] タブでクライアント証明書の有効期限を確認することで、現在の証明書の有効期限を確認できます。

特別に構成されたアプライアンスノード上のデータを保護するためにキー管理サーバー（KMS）を使用している場合は、"KMSクライアント証明書のアップロード" 。

開始する前に

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

- クライアント証明書を編集するには:
  - 管理ノードの IP アドレスまたはドメイン名があります。
  - 独自の証明書または新しい証明書をアップロードするには、秘密キー、クライアント証明書、および CA (使用されている場合) がローカル コンピューター上で使用可能です。

クライアント証明書を追加する

クライアント証明書を追加するには、次のいずれかの手順を使用します。

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

管理インターフェース証明書はすでに構成されています

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

手順

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

      新しい証明書が [クライアント] タブに表示されます。
7. 外部監視ツールを構成するGrafana など。

CA発行のクライアント証明書

管理インターフェース証明書が設定されておらず、CA 発行のクライアント証明書と秘密キーを使用する Prometheus のクライアント証明書を追加する予定の場合は、この手順を使用して管理者クライアント証明書を追加します。

手順

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

      新しい証明書が [クライアント] タブに表示されます。
8. 外部監視ツールを構成するGrafana など。

グリッドマネージャーから生成された証明書

管理インターフェース証明書が構成されておらず、Grid Manager の証明書生成機能を使用する Prometheus のクライアント証明書を追加する予定の場合は、この手順を使用して管理者クライアント証明書を追加します。

手順

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

     これらの拡張機能は、証明書に含まれるキーの目的を定義します。

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

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

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

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

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

     例： `storagegrid_certificate.pem`

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

     秘密鍵ファイル名とダウンロード場所を指定します。

10. 作成 を選択して、証明書をグリッド マネージャーに保存します。

    新しい証明書が [クライアント] タブに表示されます。

11. グリッド マネージャーで、[構成] > [セキュリティ] > [証明書] を選択し、[グローバル] タブを選択します。
12. *管理インターフェイス証明書*を選択します。
13. *カスタム証明書を使用する*を選択します。
14. certificate.pemとprivate_key.pemファイルをアップロードします。クライアント証明書の詳細ステップ。CA バンドルをアップロードする必要はありません。
    a. *証明書のアップロード*を選択し、*続行*を選択します。
    b. 各証明書ファイルをアップロードする(`.pem`）。
    c. 保存 を選択して、証明書をグリッド マネージャーに保存します。

       新しい証明書が管理インターフェイスの証明書ページに表示されます。

15. 外部監視ツールを構成するGrafana など。

外部監視ツールを設定する

手順

1. Grafana などの外部監視ツールで次の設定を構成します。
   a. 名前: 接続の名前を入力します。

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

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

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

c. **TLS** クライアント認証 と **CA** 証明書 を有効にします。

d. TLS/SSL認証の詳細の下に、以下の内容をコピーして貼り付けます:

   - 管理インターフェース CA 証明書を **CA Cert** へ
   - **Client Cert** へのクライアント証明書
   - クライアントキーの秘密鍵

e. **ServerName**: 管理ノードのドメイン名を入力します。

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

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

   外部監視ツールを使用して、 StorageGRIDから Prometheus メトリックにアクセスできるようになりました。

   指標の詳細については、"StorageGRIDの監視手順" 。

クライアント証明書を編集する

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

手順

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

   証明書の有効期限と Prometheus のアクセス権限が表にリストされています。証明書の有効期限が間もなく切れるか、すでに切れている場合は、テーブルにメッセージが表示され、アラートがトリガーされます。

2. 編集する証明書を選択します。
3. *編集*を選択し、*名前と権限の編集*を選択します。
4. 証明書名を入力します。
5. 外部監視ツールを使用して Prometheus メトリックにアクセスするには、**Prometheus** を許可 を選択します。
6. *続行*を選択して、グリッド マネージャーに証明書を保存します。

   更新された証明書が [クライアント] タブに表示されます。

新しいクライアント証明書を添付する

現在の証明書の有効期限が切れた場合は、新しい証明書をアップロードできます。

手順

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

   証明書の有効期限と Prometheus のアクセス権限が表にリストされています。証明書の有効期限が間もなく切れるか、すでに切れている場合は、テーブルにメッセージが表示され、アラートがトリガーされます。

2. 編集する証明書を選択します。
3. *編集*を選択し、編集オプションを選択します。

証明書をアップロード

証明書のテキストをコピーして他の場所に貼り付けます。

a. *証明書のアップロード*を選択し、*続行*を選択します。

b. クライアント証明書名をアップロードする(`.pem`）。

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

   - 証明書ファイルを保存するには、[証明書のダウンロード] を選択します。

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

   例： `storagegrid_certificate.pem`

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

c. 作成 を選択して、証明書をグリッド マネージャーに保存します。

   更新された証明書が [クライアント] タブに表示されます。

証明書を生成する

他の場所に貼り付けるための証明書テキストを生成します。

a. *証明書の生成*を選択します。

b. 証明書情報を指定します。

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

     これらの拡張機能は、証明書に含まれるキーの目的を定義します。

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

c. *生成*を選択します。

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

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

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

- 証明書ファイルを保存するには、[証明書のダウンロード] を選択します。

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

  例： `storagegrid_certificate.pem`

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

  秘密鍵ファイル名とダウンロード場所を指定します。

e. 作成 を選択して、証明書をグリッド マネージャーに保存します。

新しい証明書が [クライアント] タブに表示されます。

クライアント証明書をダウンロードまたはコピーする

他の場所で使用するためにクライアント証明書をダウンロードまたはコピーすることができます。

手順

1. 構成 > セキュリティ > 証明書 を選択し、クライアント タブを選択します。
2. コピーまたはダウンロードする証明書を選択します。
3. 証明書をダウンロードまたはコピーします。

証明書ファイルをダウンロード

証明書をダウンロードする `.pem`ファイル。

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

   例： `storagegrid_certificate.pem`

証明書のコピー

証明書のテキストをコピーして他の場所に貼り付けます。

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

   例： `storagegrid_certificate.pem`

クライアント証明書を削除する

管理者クライアント証明書が不要になった場合は、削除できます。

手順

1. 構成 > セキュリティ > 証明書 を選択し、クライアント タブを選択します。
2. 削除する証明書を選択します。
3. *削除*を選択して確認します。

> 最大 10 個の証明書を削除するには、[クライアント] タブで削除する各証明書を選択し、[アクション] > [削除] を選択します。

証明書が削除された後、その証明書を使用していたクライアントは、 StorageGRID Prometheus データベースにアクセスするために新しいクライアント証明書を指定する必要があります。

著作権に関する情報

商標に関する情報