



## 証明書进行管理します StorageGRID

NetApp  
October 03, 2025

# 目次

証明書を管理します	1
セキュリティ証明書について	1
アクセスセキュリティ証明書	2
セキュリティ証明書の詳細	5
証明書の例	11
サーバ証明書を設定	12
サポートされているサーバ証明書のタイプ	12
管理インターフェイス証明書を設定	12
S3 および Swift API 証明書を設定する	17
Grid CA 証明書をコピーする	22
FabricPool の StorageGRID 証明書を設定します	22
クライアント証明書を設定	23
クライアント証明書を追加します	24
クライアント証明書を編集します	28
新しいクライアント証明書を接続します	29
クライアント証明書をダウンロードまたはコピーします	31
クライアント証明書を削除します	31

# 証明書を管理します

## セキュリティ証明書について

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

StorageGRID では、2 種類のセキュリティ証明書が使用されます。

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

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

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

- デフォルトの Grid CA 証明書 \*

StorageGRID には、システムのインストール時に内部のグリッド CA 証明書を生成する認証局（CA）が組み込まれています。デフォルトでは、グリッド 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。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。グリッド CA 証明書は非本番環境で使用できますが、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。
- カスタム証明書はすべてが満たしている必要があります [システムの保護設定のガイドライン](#) サーバ証明書の場合。
- 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。

## アクセスセキュリティ証明書

すべての StorageGRID 証明書に関する情報に一元的にアクセスでき、各証明書の設定ワークフローへのリンクも含まれます。

1. Grid Manager で、 \* configuraton \* > \* Security \* > \* Certificates \* を選択します。

Certificates

View and manage the certificates that secure HTTPS connections between StorageGRID and external clients, such as S3 or Swift, and external servers, such as a key management server (KMS).

Global Grid CA Client Load balancer endpoints Tenants Other

The StorageGRID certificate authority ("grid CA") generates and signs two global certificates during installation. The management interface certificate on Admin Nodes secures the management interface. The S3 and Swift API certificate on Storage and Gateway Nodes secures client access. You should replace each default certificate with your own custom certificate signed by an external certificate authority.

Name	Description	Type	Expiration date
Management interface certificate	Secures the connection between client web browsers and the Grid Manager, Tenant Manager, Grid Management API, and Tenant Management API.	Custom	Jun 4th, 2022
S3 and Swift API certificate	Secures the connections between S3 and Swift clients and Storage Nodes or between clients and the deprecated CLB service on Gateway Nodes. You can optionally use this certificate for a load balancer endpoint as well.	Custom	Jun 4th, 2022

2. [証明書] ページのタブを選択して、各証明書カテゴリの情報を表示し、証明書設定にアクセスします。タブにアクセスできるのは、適切な権限がある場合のみです。

- \* 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。
- \* Grid 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 データベースの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 および Swift 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 \* : アイデンティティフェデレーションサーバー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、証明書の詳細へのリンクを次に示します。

## グローバル

グローバル証明書は、Web ブラウザおよび外部の S3 および Swift API クライアントからの StorageGRID アクセスを保護します。2 つのグローバル証明書は、最初にインストール時に StorageGRID 認証局によって生成されます。本番環境では、外部の認証局によって署名されたカスタム証明書を使用することを推奨します。

- [\[管理インターフェイスの証明書\]](#): クライアントの Web ブラウザ接続を StorageGRID 管理インターフェイスに保護します。
- [S3 および Swift API 証明書](#): ストレージノード、管理ノード、および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。これらのノードは、S3 および Swift クライアントアプリケーションがオブジェクトデータをアップロードおよびダウンロードするために使用します。

インストールされるグローバル証明書には次の情報が含まれます。

- \* 名前 \* : 証明書の管理リンクを持つ証明書の名前。
- \* 概要 \*
- \* タイプ \* : カスタムまたはデフォルト。+グリッドセキュリティを向上させるために、常にカスタム証明書を使用する必要があります。
- \* 失効日 \* : 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。

## 可能です

- グリッドセキュリティを向上させるには、外部の認証局によって署名されたカスタム証明書でデフォルト証明書を置き換えます。
  - [StorageGRID で生成されたデフォルトの管理インターフェイス証明書を置き換えます](#) Grid Manager 接続と Tenant Manager 接続に使用されます。
  - [S3 および Swift API 証明書を置き換えます](#) ストレージノード、CLB サービス（廃止予定）、ロードバランサエンドポイント（オプション）の接続に使用します。
- [管理インターフェイスのデフォルトの証明書をリストア](#)
- [S3 および Swift のデフォルトの API 証明書をリストア](#)
- [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イス証明書を生成します。](#)
- [をコピーまたはダウンロードします](#) [管理インターフェイスの証明書](#) または [S3 および Swift API 証明書](#)。

## Grid CA

◦ [Grid CA 証明書](#)は、StorageGRID のインストール時に StorageGRID 認証局によって生成され、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その内容が含まれます。

可能です [Grid CA 証明書をコピーまたはダウンロードします](#)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](#)は外部の認証局によって生成され、外部の監視ツールと StorageGRID の Prometheus データベースとの間の接続を保護します。

証明書テーブルには、設定されている各クライアント証明書の行があり、証明書の有効期限とともに Prometheus データベースへのアクセスに証明書を使用できるかどうかが表示されます。

可能です

- [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。](#)
- 証明書名を選択して証明書の詳細を表示します。表示される情報は次のとおりです。
  - [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 \\* \(Actions \\*\)](#)] を選択して、すばやく [編集](#)、[添付 \(Attach\)](#) または [取り外します](#) クライアント証明書。最大 10 個のクライアント証明書を選択し、[\\* Actions \\* > \\* Remove \\*](#) を使用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

[ロードバランサエンドポイントの証明書](#) をアップロードまたは生成して、ゲートウェイノードと管理ノード上の S3 / Swift クライアントと StorageGRID ロードバランササービスの間の接続を保護します。

ロードバランサエンドポイントテーブルには、設定されている各ロードバランサエンドポイント用の行があり、グローバルな S3 および Swift API 証明書とカスタムのロードバランサエンドポイント証明書のどちらがエンドポイントに使用されているかを示しています。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 分かかることがあります。

可能です

- [エンドポイント名を選択してブラウザタブを開き、証明書の詳細など、ロードバランサエンドポイントに関する情報を表示します。](#)
- [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。](#)
- [グローバルな S3 および Swift API 証明書を使用します](#) 代わりに、新しいロードバランサエンドポイント証明書を生成します。

テナント

テナントで使用できる [アイデンティティフェデレーションサーバの証明書](#) または [プラットフォームサービスエンドポイントの証明書](#) StorageGRID を使用して接続を保護します。

テナントテーブルには、テナントごとに 1 つの行があり、各テナントに独自のアイデンティティ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。

可能です

- [Tenant Manager にサインインするテナント名を選択します](#)
- [テナントのアイデンティティフェデレーションの詳細を表示するテナント名を選択します](#)

- [テナントプラットフォームサービスの詳細を表示するテナント名を選択します](#)
- [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 では、特定の目的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、機能名で一覧表示されます。その他のセキュリティ証明書には、次のもの

- [アイデンティティフェデレーション証明書](#)
- [クラウドストレージプールの証明書](#)
- [キー管理サーバ（KMS）の証明書](#)
- [シングルサインオン証明書](#)
- [E メールアラート通知の証明書](#)
- [外部 syslog サーバ証明書](#)

情報は、関数が使用する証明書の種類と、そのサーバ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表示およびアクセスできるのは、適切な権限がある場合のみです。

可能です

- [アイデンティティフェデレーション証明書を表示および編集する](#)
- [キー管理サーバ（KMS）のサーバ証明書とクライアント証明書をアップロードします](#)
- [S3、C2S S3、または Azure 用のクラウドストレージプール証明書を指定します](#)
- [証明書利用者信頼の SSO 証明書を手動で指定します](#)
- [アラート E メール通知用の証明書を指定します](#)
- [外部 syslog サーバの証明書を指定します](#)

## セキュリティ証明書の詳細

セキュリティ証明書の種類ごとに、実装手順が記載された記事へのリンクを以下に示します。

### 管理インターフェイスの証明書

証明書のタイプ	説明	ナビゲーションの場所	詳細
サーバ	<p>クライアントの Web ブラウザと StorageGRID 管理インターフェイスの間の接続を認証することで、ユーザがセキュリティの警告なしで Grid Manager とテナントマネージャにアクセスできるようにします。</p> <p>この証明書は、Grid 管理 API 接続とテナント管理 API 接続も認証します。</p> <p>インストール時に作成される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。</p>	<ul style="list-style-type: none"> <li>設定 * &gt; * セキュリティ * &gt; * 証明書 *、* グローバル * タブを選択し、* 管理インターフェイス証明書 * を選択します</li> </ul>	<a href="#">管理インターフェイス証明書を設定</a>

### S3 および Swift API 証明書

証明書のタイプ	説明	ナビゲーションの場所	詳細
サーバ	<p>ストレージノードへのセキュアな S3 または Swift クライアント接続、ゲートウェイノード上の廃止された Connection Load Balancer (CLB) サービス、およびロードバランサエンドポイント (オプション) への接続を認証します。</p>	<ul style="list-style-type: none"> <li>configuration * &gt; * Security * &gt; * Certificates * を選択し、* Global * タブを選択して、* S3 および Swift API certificate * を選択します</li> </ul>	<a href="#">S3 および Swift API 証明書を設定する</a>

### Grid CA 証明書

を参照してください [デフォルトの Grid CA 証明書概要](#)。

### 管理者クライアント証明書

証明書のタイプ	説明	ナビゲーションの場所	詳細
クライアント	<p>StorageGRID が外部クライアントアクセスを認証できるように、各クライアントにインストールします。</p> <ul style="list-style-type: none"> <li>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。</li> <li>外部ツールを使用して StorageGRID をセキュアに監視できます。</li> </ul>	<ul style="list-style-type: none"> <li>設定 * &gt; * セキュリティ * &gt; * 証明書 * を選択し、 * クライアント * タブを選択します</li> </ul>	<a href="#">クライアント証明書を設定</a>

#### ロードバランサエンドポイントの証明書

証明書のタイプ	説明	ナビゲーションの場所	詳細
サーバ	<p>S3 または Swift クライアントと、ゲートウェイノードおよび管理ノード上の StorageGRID ロードバランササービス間の接続を認証します。ロードバランサエンドポイントの設定時に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では、StorageGRID に接続する際にロードバランサ証明書を使用してオブジェクトデータを保存および読み出します。</p> <p>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 <a href="#">S3 および Swift API 証明書</a> ロードバランササービスへの接続を認証する証明書。ロードバランサ接続の認証にグローバル証明書を使用する場合は、ロードバランサ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。</p> <ul style="list-style-type: none"> <li>注： * ロードバランサ認証に使用される証明書は、通常の StorageGRID 処理で最もよく使用される証明書です。</li> </ul>	<ul style="list-style-type: none"> <li>設定 * &gt; * ネットワーク * &gt; * ロードバランサエンドポイント *</li> </ul>	<ul style="list-style-type: none"> <li><a href="#">ロードバランサエンドポイントを設定する</a></li> <li><a href="#">FabricPool のロードバランサエンドポイントを作成します</a></li> </ul>

## アイデンティティフェデレーション証明書

証明書のタイプ	説明	ナビゲーションの場所	詳細
サーバ	Active Directory、OpenLDAP、Oracle Directory Server などの外部のアイデンティティプロバイダと StorageGRID の間の接続を認証します。アイデンティティフェデレーションに使用します。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。	<ul style="list-style-type: none"> <li>設定 * &gt; * アクセス制御 * &gt; * アイデンティティフェデレーション *</li> </ul>	アイデンティティフェデレーションを使用する

#### プラットフォームサービスのエンドポイント証明書

証明書のタイプ	説明	ナビゲーションの場所	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。	<ul style="list-style-type: none"> <li>Tenant Manager * &gt; * storage ( S3 ) * &gt; * Platform services endpoints *</li> </ul>	<p>プラットフォームサービスエンドポイントを作成します</p> <p>プラットフォームサービスエンドポイントを編集します</p>

#### クラウドストレージプールのエンドポイントの証明書

証明書のタイプ	説明	ナビゲーションの場所	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への接続を認証します。クラウドプロバイダのタイプごとに別の証明書が必要です。	<ul style="list-style-type: none"> <li>ilm * &gt; * ストレージ・プール *</li> </ul>	クラウドストレージプールを作成

#### キー管理サーバ ( KMS ) の証明書

証明書のタイプ	説明	ナビゲーションの場所	詳細
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。	<ul style="list-style-type: none"> <li>設定 &gt; *セキュリティ &gt; *キー管理サーバ*</li> </ul>	キー管理サーバの追加（KMS）

### シングルサインオン（SSO）証明書

証明書のタイプ	説明	ナビゲーションの場所	詳細
サーバ	Active Directory フェデレーションサービス（AD FS）やシングルサインオン（SSO）要求に使用される StorageGRID などのアイデンティティフェデレーションサービスとの間の接続を認証します。	<ul style="list-style-type: none"> <li>設定 &gt; *アクセス制御 &gt; *シングルサインオン*</li> </ul>	シングルサインオンを設定します

### E メールアラート通知の証明書

証明書のタイプ	説明	ナビゲーションの場所	詳細
サーバとクライアント	アラート通知に使用される SMTP E メールサーバと StorageGRID 間の接続を認証します。 <ul style="list-style-type: none"> <li>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。</li> <li>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。</li> </ul>	<ul style="list-style-type: none"> <li>アラート &gt; 電子メールセットアップ*</li> </ul>	アラート用の E メール通知を設定します

### 外部 syslog サーバの証明書

証明書のタイプ	説明	ナビゲーションの場所	詳細
サーバ	<p>StorageGRID にイベントを記録する外部 syslog サーバ間で、TLS 接続または RELP/TLS 接続を認証します。</p> <ul style="list-style-type: none"> <li>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。</li> </ul>	<ul style="list-style-type: none"> <li>設定 * &gt; * モニタリング * &gt; * 監査および syslog サーバ * を選択し、* 外部 syslog サーバの設定 * を選択します</li> </ul>	<a href="#">外部 syslog サーバを設定します</a>

## 証明書の例

### 例 1：ロードバランササービス

この例では、StorageGRID がサーバとして機能します。

- 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。
- 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。
- 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。
- 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。
- 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。
- 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。

- 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。
- 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。
- 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。
- 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。
- KMS サーバは、検証済みの接続を使用して応答します。

# サーバ証明書を設定

## サポートされているサーバ証明書のタイプ

StorageGRID システムでは、RSA または ECDSA（Elliptic Curve Digital Signature Algorithm）で暗号化されたカスタム証明書がサポートされます。

StorageGRID で REST API のクライアント接続を保護する方法の詳細については、[を参照してください S3 を使用する](#) または [Swift を使用します](#)。

## 管理インターフェイス証明書を設定

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ると、ユーザがグリッドマネージャとテナントマネージャにアクセスする際にセキュリティの警告が表示されなくなります。デフォルトの管理インターフェイス証明書に戻すか、新しい証明書を生成することもできます。

### このタスクについて

デフォルトでは、管理ノードごとに、グリッド CA によって署名された証明書が 1 つずつ発行されます。これらの CA 署名証明書は、単一の共通するカスタム管理インターフェイス証明書および対応する秘密鍵に置き換えることができます。

Grid Manager および Tenant Manager への接続時にクライアントがホスト名を確認する必要がある場合は、単一のカスタム管理インターフェイスの証明書がすべての管理ノードに対して使用されるため、ワイルドカード証明書またはマルチドメイン証明書として指定する必要があります。グリッド内のすべての管理ノードに一致するカスタム証明書を定義してください。

設定はサーバ上で行う必要があります。また、使用しているルート認証局（CA）によっては、ユーザが Grid Manager および Tenant Manager へのアクセスに使用する Web ブラウザに Grid CA 証明書をインストールすることも必要になります。



サーバ証明書の問題によって処理が中断されないようにするために、このサーバ証明書の有効期限が近づくと、「Expiration of server certificate for Management Interface \*」アラートがトリガーされます。必要に応じて、[グローバル] タブで [\*設定\*] > [\*セキュリティ\*] > [\*証明書\*] を選択し、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 にアクセスする場合は、次のいずれかの場合に証明書のエラーが表示され、バイパスするオプションはありません。

- カスタム管理インターフェイス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イス証明書をデフォルトのサーバ証明書に戻します](#)。

## カスタム管理インターフェイス証明書を追加します

カスタムの管理インターフェイス証明書を追加するには、Grid Manager を使用して独自の証明書を指定するか、証明書を生成します。

## 手順

1. [ \* configuration \* > \* Security \* > \* Certificates \* ] を選択します。
2. [ \* グローバル \* ] タブで、 [ \* 管理インターフェイス証明書 \* ] 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する

必要なサーバ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. 必要なサーバ証明書ファイルをアップロードします。
  - \*サーバ証明書\* : カスタムサーバ証明書ファイル ( PEM エンコード ) 。
  - **Certificate private key**: カスタムサーバ証明書の秘密鍵ファイル ( .key ) 。



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

- 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は、各証明書が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\* を選択します。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。

証明書ファイルの名前とダウンロード先を指定します。ファイルに拡張子「.pem」を付けて保存します。

例: 'storagegrid\_certificate.pem'

- d. [ 保存 ( Save ) ] を選択します。+ 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はカスタムの管理インターフェイス証明書が使用されます。
  - 証明書の内容をコピーして他の場所に貼り付けるには、\*証明書の PEM のコピー\* または \*CA バンドル PEM のコピー\* を選択してください。

## 証明書の生成

サーバ証明書ファイルを生成します。



本番環境では、外部の認証局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を推奨します。

- 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。
  - \* Domain name \* : 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。
  - \* 件名 \* : 証明書所有者の X.509 サブジェクトまたは識別名 ( DN ) 。
  - **days valid**: 証明書の有効期限が切れる作成後の日数

c. [\*Generate (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。

証明書ファイルの名前とダウンロード先を指定します。ファイルに拡張子「.pem」を付けて保存します。

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、\* 証明書の PEM をコピー \* を選択します。

e. [ 保存 ( Save ) ]を選択します。+ 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はカスタムの管理インターフェイス証明書が使用されます。

5. Web ブラウザが更新されたことを確認するには、ページをリフレッシュしてください。



新しい証明書をアップロードまたは生成したあと、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に最大 1 日かかります。

6. カスタムの管理インターフェイス証明書を追加すると、使用中の証明書の詳細な証明書情報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。+ 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。

管理インターフェイスのデフォルトの証明書をリストア

Grid Manager 接続と Tenant Manager 接続での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. [\* configuration \* > \* Security \* > \* Certificates \* ]を選択します。
2. [\* グローバル \* ] タブで、[\* 管理インターフェイス証明書 \* ]を選択します。
3. [\* デフォルト証明書を使用する \* ]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リストアすると、設定したカスタムサーバ証明書ファイルは削除され、システムからはリカバリできなくなります。以降すべての新しいクライアント接続には、デフォルトの管理インターフェイス証明書が使用されます。

4. Web ブラウザが更新されたことを確認するには、ページをリフレッシュしてください。

スクリプトを使用して、新しい自己署名管理インターフェイス証明書を生成します

ホスト名の厳密な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。

必要なもの

- 特定のアクセス権限が必要です。
- 「passwords.txt」ファイルがあります。

このタスクについて

本番環境では、外部の認証局によって署名された証明書を使用することを推奨します。

手順

1. 各管理ノードの完全修飾ドメイン名（FQDN）を取得します。
2. プライマリ管理ノードにログインします。
  - a. 次のコマンドを入力します `ssh admin@primary_Admin_Node_ip`
  - b. 「passwords.txt」ファイルに記載されたパスワードを入力します。
  - c. root に切り替えるには、次のコマンドを入力します
  - d. 「passwords.txt」ファイルに記載されたパスワードを入力します。

root としてログインすると、プロンプトは「\$」から「#」に変わります。

3. 新しい自己署名証明書を使用して StorageGRID を設定します。

```
$sudo make -certificate --domains_wildcard-admin -node-fqdn_ --タイプ管理
```

- 「--domains」の場合、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。たとえば `*.ui.storagegrid.example.com` は `*wildcard` を使用して `admin1.ui.storagegrid.example.com` と `admin2.ui.storagegrid.example.com` を表します
- 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設定するには `--type` を `'management'` に設定します
- 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）です。この期間を過ぎる前に証明書を再作成する必要があります。デフォルトの有効期間を上書きするには `--days` 引数を使用します



証明書の有効期間は 'make -certificate' が実行された時点から始まります管理クライアントが StorageGRID と同じ時間ソースと同期されるようにしてください。同期されていないと、クライアントが証明書を拒否する可能性があります。

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

出力には、管理 API クライアントに必要なパブリック証明書が含まれています。

4. 証明書を選択してコピーします。

BEGIN タグと END タグも含めて選択してください。
5. コマンドシェルからログアウトします。「`$EXIT`」
6. 証明書が設定されたことを確認します。
  - a. Grid Manager にアクセスします。
  - b. `[ * configuration * > * Security * > * Certificates * ]` を選択します
  - c. `[ * グローバル * ]` タブで、`[ * 管理インターフェイス証明書 * ]` を選択します。

7. コピーしたパブリック証明書を使用するように管理クライアントを設定します。BEGIN タグと END タグを含めてください。

管理インターフェイ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. [ \* configuration \* > \* Security \* > \* Certificates \* ] を選択します。
2. [ \* グローバル \* ] タブで、[ \* 管理インターフェイス証明書 \* ] を選択します。
3. [Server] タブまたは [CA Bundle] 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します

証明書または CA バンドルの '.pem' ファイルをダウンロードしますオプションの CA バンドルを使用している場合は、バンドル内の各証明書が独自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にあるすべての証明書が単一のファイルとしてダウンロードされます。

- b. 証明書ファイルの名前とダウンロード先を指定します。ファイルに拡張子「.pem」を付けて保存します。

例： 'storagegrid\_certificate.pem'

証明書または **CA** バンドル **PEM** をコピーしてください

証明書のテキストをコピーして別の場所に貼り付けてください。オプションの CA バンドルを使用している場合は、バンドル内の各証明書が独自のサブタブに表示されます。

- a. [Copy certificate PEM\* (証明書のコピー) ] または [ \* Copy CA bundle PEM\* ( CA バンドル PEM のコピー) ]

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にあるすべての証明書と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に貼り付けます。
- c. テキスト・ファイルに拡張子「.pem」を付けて保存します。

例： 'storagegrid\_certificate.pem'

### S3 および Swift API 証明書を設定する

ストレージノードへの S3 または Swift クライアント接続、ゲートウェイノード上の廃止された Connection Load Balancer (CLB) サービス、またはロードバランサエンドポイントへの S3 または Swift クライアント接続に使用するサーバ証明書を交換またはリス

トアできます。置き換え用のカスタムサーバ証明書は組織に固有のものです。

このタスクについて

デフォルトでは、すべてのストレージノードに、グリッド CA によって署名された X.509 サーバ証明書が発行されます。これらの CA 署名証明書は、単一の共通するカスタムサーバ証明書および対応する秘密鍵で置き換えることができます。

1 つのカスタムサーバ証明書がすべてのストレージノードに対して使用されるため、ストレージエンドポイントへの接続時にクライアントがホスト名を確認する必要がある場合は、ワイルドカード証明書またはマルチドメイン証明書として指定する必要があります。グリッド内のすべてのストレージノードに一致するカスタム証明書を定義してください。

サーバでの設定が完了したら、使用しているルート認証局（CA）によっては、システムへのアクセスに使用する S3 または Swift API クライアントにグリッド CA 証明書をインストールすることも必要になる場合があります。



サーバ証明書の問題によって処理が中断されないようにするために、ルートサーバ証明書の有効期限が近づくと、「S3 および Swift API のグローバルサーバ証明書の有効期限 \*」アラートがトリガーされます。必要に応じて、現在の証明書の有効期限を確認するには、\* configuration \* > \* Security \* > \* Certificates \* を選択し、S3 および Swift API 証明書の有効期限を Global タブで確認します。

S3 および Swift のカスタム API 証明書をアップロードまたは生成できます。

### S3 および Swift のカスタム API 証明書を追加します

手順

1. [\* configuration \* > \* Security \* > \* Certificates \* ] を選択します。
2. Global \* タブで、\* S3 および Swift 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する

必要なサーバ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. 必要なサーバ証明書ファイルをアップロードします。
  - \*サーバ証明書\* : カスタムサーバ証明書ファイル ( PEM エンコード ) 。
  - **Certificate private key**: カスタムサーバ証明書の秘密鍵ファイル (.key) 。



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

- **CA Bundle** : 各中間発行認証局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して含まれている必要があります。
- c. 証明書の詳細を選択して、アップロードしたカスタムの S3 および Swift API 証明書ごとにメタデータと PEM 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は、各証明書が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\* を選択します。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。

証明書ファイルの名前とダウンロード先を指定します。ファイルに拡張子「.pem」を付けて保存します。

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、\*証明書の PEM のコピー\* または \*CA バンドル PEM のコピー\* を選択してください。
- d. [ 保存 ( Save ) ] を選択します。

以降の新しい S3 および Swift クライアント接続には、カスタムサーバ証明書が使用されます。

## 証明書の生成

サーバ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。
  - \*Domain name\* : 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。
  - \*件名\* : 証明書所有者の X.509 サブジェクトまたは識別名 ( DN ) 。
  - **days valid**: 証明書の有効期限が切れる作成後の日数
- c. [\*Generate (生成) ] を選択します
- d. Certificate Details \* を選択して、生成されたカスタムの S3 および Swift API 証明書のメタデータ

と PEM を表示します。

- 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。

証明書ファイルの名前とダウンロード先を指定します。ファイルに拡張子「.pem」を付けて保存します。

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、\* 証明書の PEM をコピー \* を選択します。

e. [ 保存 ( Save ) ] を選択します。

以降の新しい S3 および Swift クライアント接続には、カスタムサーバ証明書が使用されます。

5. タブを選択して、デフォルトの StorageGRID サーバ証明書、アップロードされた CA 署名証明書、または生成されたカスタム証明書のメタデータを表示します。



新しい証明書をアップロードまたは生成したあと、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に最大 1 日かかります。

6. Web ブラウザが更新されたことを確認するには、ページをリフレッシュしてください。
7. カスタムの S3 および Swift API 証明書を追加すると、使用中のカスタムの S3 および Swift API 証明書の詳細な証明書情報が S3 および Swift API の証明書ページに表示されます。+ 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。

### S3 および Swift のデフォルトの API 証明書をリストア

ストレージノードへの S3 および Swift クライアント接続およびゲートウェイノード上の CLB サービスに対する S3 および Swift クライアント接続に、デフォルトの S3 および Swift API 証明書を使用するように戻すことができます。ただし、ロードバランサエンドポイントにはデフォルトの S3 および Swift API 証明書を使用できません。

手順

1. [ \* configuration \* > \* Security \* > \* Certificates \* ] を選択します。
2. Global \* タブで、\* S3 および Swift API 証明書 \* を選択します。
3. [ \* デフォルト証明書を使用する \* ] を選択します。

グローバルな S3 および Swift API 証明書のデフォルトのバージョンをリストアすると、設定したカスタムサーバ証明書ファイルは削除され、システムからはリカバリできなくなります。デフォルトの S3 および Swift API 証明書は、ストレージノードへの以降の新しい S3 および Swift クライアント接続およびゲートウェイノード上の CLB サービスへの以降の新しい接続に使用されます。

4. 警告を確認し、デフォルトの S3 および Swift API 証明書をリストアするには、「\* OK」を選択します。

Root Access 権限がある環境で、S3 および Swift API のカスタム証明書をロードバランサエンドポイントの接続に使用していた場合は、デフォルトの S3 および Swift 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エンドポイントのリストが表示されます。に進みます [ロードバランサエンドポイントを設定する](#) 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. Web ブラウザが更新されたことを確認するには、ページをリフレッシュしてください。

### S3 および Swift API 証明書をダウンロードまたはコピーします

S3 および Swift 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. [ \* configuration \* > \* Security \* > \* Certificates \* ] を選択します。
2. Global \* タブで、 \* S3 および Swift API 証明書 \* を選択します。
3. [Server] タブまたは [CA Bundle] 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します

証明書または CA バンドルの '.pem' ファイルをダウンロードしますオプションの CA バンドルを使用している場合は、バンドル内の各証明書が独自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にあるすべての証明書が単一のファイルとしてダウンロードされます。

- b. 証明書ファイルの名前とダウンロード先を指定します。ファイルに拡張子「.pem」を付けて保存します。

例： 'storagegrid\_certificate.pem'

証明書または **CA** バンドル **PEM** をコピーしてください

証明書のテキストをコピーして別の場所に貼り付けてください。オプションの CA バンドルを使用している場合は、バンドル内の各証明書が独自のサブタブに表示されます。

- a. [Copy certificate PEM\* (証明書のコピー) ] または [\* Copy CA bundle PEM\* (CA バンドル PEM のコピー) ]

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にあるすべての証明書と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に貼り付けます。
- c. テキスト・ファイルに拡張子「.pem」を付けて保存します。

例： 'storagegrid\_certificate.pem'

#### 関連情報

- [S3 を使用する](#)
- [Swift を使用します](#)
- [S3 API エンドポイントのドメイン名を設定](#)

## Grid CA 証明書をコピーする

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

必要なもの

- を使用して Grid Manager にサインインします [サポートされている Web ブラウザ](#)。
- 特定のアクセス権限が必要です。

このタスクについて

カスタムサーバ証明書が設定されている場合、クライアントアプリケーションはカスタムサーバ証明書を使用してサーバを検証する必要があります。StorageGRID システムから CA 証明書をコピーしない。

手順

1. [`* configuration * > * Security * > * Certificates *`] を選択し、 [`* Grid CA *`] タブを選択します。
2. Certificate 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します

証明書「.pem」ファイルをダウンロードします。

- a. [ 証明書のダウンロード ] を選択します。
- b. 証明書ファイルの名前とダウンロード先を指定します。ファイルに拡張子「.pem」を付けて保存します。

例：'storagegrid\_certificate.pem'

証明書 PEM をコピーします

証明書のテキストをコピーして別の場所に貼り付けてください。

- 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に貼り付けます。
- c. テキスト・ファイルに拡張子「.pem」を付けて保存します。

例：'storagegrid\_certificate.pem'

## FabricPool の StorageGRID 証明書を設定します

厳密なホスト名検証を実行する S3 クライアントでは、FabricPool を使用する ONTAP クライアントなどの厳密なホスト名検証の無効化をサポートしていない場合は、ロードバランサエンドポイントの設定時にサーバ証明書を生成またはアップロードできます。

必要なもの

- 特定のアクセス権限が必要です。

- を使用して Grid Manager にサインインします [サポートされている Web ブラウザ](#)。

このタスクについて

ロードバランサエンドポイントを作成する際には、自己署名サーバ証明書を生成するか、既知の認証局（CA）によって署名された証明書をアップロードできます。本番環境では、既知の CA によって署名された証明書を使用する必要があります。CA によって署名された証明書は、システムを停止することなくローテーションできます。また、中間者攻撃に対する保護としても優れているため、セキュリティも強化されます。

次の手順は、FabricPool を使用する S3 クライアントを対象とした一般的なガイドラインです。詳細な情報と手順については、[を参照してください StorageGRID for FabricPool を設定します](#)。



ゲートウェイノード上の別の Connection Load Balancer（CLB）サービスは廃止され、FabricPool での使用は推奨されません。

手順

1. 必要に応じて、FabricPool で使用するハイアベイラビリティ（HA）グループを設定します。
2. FabricPool で使用する S3 ロードバランサエンドポイントを作成します。

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

3. ONTAP でクラウド階層として StorageGRID を接続します。

ロードバランサエンドポイントのポートと、アップロードした CA 証明書で使用する完全修飾ドメイン名を指定します。次に、CA 証明書を指定します。



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

## クライアント証明書を設定

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から StorageGRID の Prometheus データベースにアクセスして、外部ツールで StorageGRID を監視するための安全な方法を提供できます。

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。

の情報を参照してください [一般的なセキュリティ証明書の使用](#) および [カスタムサーバ証明書を設定しています](#)。



サーバ証明書の問題によって処理が中断されないようにするために、このサーバ証明書の有効期限が近づくと、「証明書ページで設定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、[クライアント] タブで [\*設定\*] > [\*セキュリティ\*] > [\*証明書\*] を選択し、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。



特別に設定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（KMS）を使用する場合は、についての具体的な情報を参照してください [KMS クライアント証明書をアップロードする](#)。

#### 必要なもの

- Root Access 権限が割り当てられている。
- を使用して Grid Manager にサインインします [サポートされている Web ブラウザ](#)。
- クライアント証明書を設定するには：
  - 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きます。
  - 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の設定に使用するCA、クライアント証明書、および秘密鍵を用意しておきます。
  - 独自の証明書をアップロードするには、証明書の秘密鍵をローカルコンピュータで使用できます。
  - 秘密鍵は、作成時に保存または記録しておく必要があります。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を確認しておきます。
  - 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、ローカルコンピュータ上で秘密鍵、クライアント証明書、およびCA（使用している場合）を使用できます。

#### クライアント証明書を追加します

シナリオに応じて手順に従って、クライアント証明書を追加します。

- [\[管理インターフェイス証明書はすでに設定されています\]](#)
- [CAによって発行されたクライアント証明書](#)
- [Grid Managerから証明書が生成されました](#)

管理インターフェイス証明書はすでに設定されています

顧客が指定したCA、クライアント証明書、および秘密鍵を使用して管理インターフェイス証明書がすでに設定されている場合は、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. Grid Manager で、\* configuration \* > \* Security \* > \* Certificates \* を選択し、\* Client \* タブを選択します。
2. 「\* 追加」を選択します。
3. 証明書名を1文字以上32文字以下で入力します。
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 \* を許可するを選択します。
5. 「\* Certificate type \*」セクションで、管理インターフェイス証明書「.pem」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、[\[続行\]](#)を選択します。

b. 管理インターフェイス証明書ファイル( '.pem' )をアップロードします

- クライアント証明書の詳細 \* を選択して、証明書メタデータと証明書 PEM を表示します。
- 証明書の内容をコピーして他の場所に貼り付けるには、 \* 証明書の PEM をコピー \* を選択します。

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

新しい証明書が [ クライアント ] タブに表示されます。

6. Grafana などの外部監視ツールで次の設定を行います。

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。

たとえば、「 + <https://admin-node.example.com:9091> + 」と入力します

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、 + をコピーして貼り付けます

- 管理インターフェイスのCA証明書を **CA Cert** に追加します
- クライアント証明書をクライアント証明書に送信します
- クライアントキー\*\*への秘密鍵

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。

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。

これらの指標の詳細については、を参照してください [StorageGRID の監視手順](#)。

## CAによって発行されたクライアント証明書

管理インターフェイス証明書が設定されていない場合や、CAによって発行されたクライアント証明書と秘密鍵を使用するPrometheusのクライアント証明書を追加する場合は、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. 手順~を実行します [管理インターフェイス証明書を設定します](#)。
2. Grid Manager で、 \* configuration \* > \* Security \* > \* Certificates \* を選択し、 \* Client \* タブを選択します。
3. 「 \* 追加 」 を選択します。

4. 証明書名を1文字以上32文字以下で入力します。
5. 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 \* を許可するを選択します。
6. [証明書の種類]セクションで、クライアント証明書、秘密鍵、およびCAバンドルの「.pem」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、[続行]を選択します。
  - b. クライアント証明書、秘密鍵、およびCAバンドルファイル(.pem)をアップロードします。
    - クライアント証明書の詳細 \* を選択して、証明書メタデータと証明書 PEM を表示します。
    - 証明書の内容をコピーして他の場所に貼り付けるには、\* 証明書の PEM をコピー \* を選択します。
  - c. 証明書を Grid Manager に保存するには、\* Create \* を選択します。

新しい証明書が[クライアント]タブに表示されます。

7. Grafana などの外部監視ツールで次の設定を行います。
  - 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。

たとえば、「+ <https://admin-node.example.com:9091>+」と入力します
  - 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、+をコピーして貼り付けます
    - 管理インターフェイスのCA証明書を**CA Cert**に追加します
    - クライアント証明書をクライアント証明書に送信します
    - クライアントキー\*\*への秘密鍵
  - 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。
  - 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。

これらの指標の詳細については、を参照してください [StorageGRID の監視手順](#)。

## Grid Managerから証明書が生成されました

管理インターフェイス証明書が設定されていない場合や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. Grid Manager で、 \* configuration \* > \* Security \* > \* Certificates \* を選択し、 \* Client \* タブを選択します。
2. 「 \* 追加」を選択します。
3. 証明書名を1文字以上32文字以下で入力します。
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 \* を許可するを選択します。
5. [証明書の種類\*]セクションで、[証明書の生成]を選択します。
6. 証明書情報を指定します。
  - \* Domain name \* : 証明書に含める管理ノード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つ以上の管理ノードIPアドレス。
  - \* 件名 \* : 証明書所有者の X.509 サブジェクトまたは識別名 ( DN ) 。
7. [\*Generate (生成) ]を選択します
8. 証明書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、証明書の秘密鍵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、 \* 証明書の PEM をコピー \* 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。

証明書ファイルの名前とダウンロード先を指定します。ファイルに拡張子「 .pem 」を付けて保存します。

例： 'storagegrid\_certificate.pem

- 秘密鍵のコピー \* を選択して、証明書の秘密鍵をコピーして別の場所に貼り付けます。
- 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。

秘密鍵ファイルの名前とダウンロード先を指定します。

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

新しい証明書が [ クライアント ] タブに表示されます。

10. Grid Managerで、 \* configuration > Security > Certificates を選択し、 Global \*タブを選択します。
11. 管理インターフェイス証明書\*を選択します。
12. [\* カスタム証明書を使用する \* ] を選択します。
13. 証明書の .pemファイルとprivate\_key.pemファイルをから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(`.pem`)をアップロードします
- c. 証明書を Grid Manager に保存するには、 \* Create \* を選択します。

新しい証明書が [クライアント] タブに表示されます。

#### 14. Grafana などの外部監視ツールで次の設定を行います。

- 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。

たとえば、「+ <https://admin-node.example.com:9091>+` 」と入力します

- 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、+をコピーして貼り付けます

- 管理インターフェイスクライアント証明書は、**CA Cert**およびクライアント証明書の両方に使用されます
- クライアントキー\*\*への秘密鍵

- 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。

- 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。

これらの指標の詳細については、を参照してください [StorageGRID の監視手順](#)。

## クライアント証明書を編集します

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. [\* configuration\*>] > [\* Security] \* > [\* Certificates\*] を選択し、 [\* Client\*] タブを選択します。

証明書の有効期限と Prometheus のアクセス権限を次の表に示します。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. 編集する証明書を選択します。
3. 「 \* Edit \* 」を選択し、「 \* 名前と権限を編集 \* 」を選択します
4. 証明書名を1文字以上32文字以下で入力します。

5. 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 \* を許可するを選択します。
6. 証明書を Grid Manager に保存するには、「\* Continue \*」を選択します。

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接続します

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できます。

### 手順

1. [\* configuration\*>] > [\* Security] \* > [\* Certificates\*] を選択し、[\* Client\*] タブを選択します。

証明書の有効期限と Prometheus のアクセス権限を次の表に示します。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する

証明書のテキストをコピーして別の場所に貼り付けてください。

- 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 ( '.pem' ) をアップロードします

クライアント証明書の詳細 \* を選択して、証明書メタデータと証明書 PEM を表示します。

- 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。

証明書ファイルの名前とダウンロード先を指定します。ファイルに拡張子「.pem」を付けて保存します。

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、\* 証明書の PEM をコピー \* を選択します。

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

更新された証明書が [ クライアント ] タブに表示されます。

## 証明書の生成

証明書のテキストを生成して他の場所に貼り付けます。

- 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。
  - \* Domain name \* : 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。
  - \* 件名 \* : 証明書所有者の X.509 サブジェクトまたは識別名 ( DN ) 。
  - **days valid**: 証明書の有効期限が切れる作成後の日数
- c. [\*Generate (生成) ] を選択します
- d. クライアント証明書の詳細 \* を選択して、証明書メタデータと証明書 PEM を表示します。



ダイアログを閉じると、証明書の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、\* 証明書の PEM をコピー \* 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。

証明書ファイルの名前とダウンロード先を指定します。ファイルに拡張子「.pem」を付けて保存します。

例： 'storagegrid\_certificate.pem'

- 秘密鍵のコピー \* を選択して、証明書の秘密鍵をコピーして別の場所に貼り付けます。
- 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。

秘密鍵ファイルの名前とダウンロード先を指定します。

- e. 証明書を Grid Manager に保存するには、\* Create \* を選択します。

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します

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

手順

1. [\* configuration\*>] > [\* Security] \* > [\* Certificates\*] を選択し、 [\* Client\*] 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します

証明書「.pem」ファイルをダウンロードします。

- a. [証明書のダウンロード] を選択します。
- b. 証明書ファイルの名前とダウンロード先を指定します。ファイルに拡張子「.pem」を付けて保存します。

例：'storagegrid\_certificate.pem'

証明書をコピーします

証明書のテキストをコピーして別の場所に貼り付けてください。

- 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に貼り付けます。
- c. テキスト・ファイルに拡張子「.pem」を付けて保存します。

例：'storagegrid\_certificate.pem'

## クライアント証明書を削除します

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. [\* configuration\*>] > [\* Security] \* > [\* Certificates\*] を選択し、 [\* Client\*] 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」を選択して確定します。



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。

証明書を削除したあと、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の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

Copyright © 2025 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

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

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

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

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

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

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

## 商標に関する情報

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