サーバ証明書を設定
StorageGRID

NetApp
November 04, 2025

目次

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。

セキュリティポリシーの暗号タイプは、サーバ証明書タイプと一致している必要があります。たとえば、RSA暗号にはRSA証明書が必要で、ECDSA暗号にはECDSA証明書が必要です。を参照してください "セキュリティ証明書を管理する"。サーバ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設定する場合は、設定できます "一時的にデフォルトのセキュリティポリシーに戻します"。

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 REST APIのセキュリティを設定" または "Swift REST APIのセキュリティを設定します"。

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）。
- 証明書の秘密鍵：カスタムサーバ証明書の秘密鍵ファイル (`.key`）。

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

- **CA Bundle** ：各中間発行認証局（ CA ）の証明書を含む単一の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。拡張子を付けてファイルを保存します `.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。+ 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。

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（オプション）	証明書所有者のX.509サブジェクト名または識別名（DN）。 このフィールドに値を入力しない場合、生成される証明書では、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。
有効な日数	作成後に証明書の有効期限が切れる日数。
キー使用の拡張機能を追加します	選択されている場合（デフォルトおよび推奨）、キー使用と拡張キー使用拡張が生成された証明書に追加されます。 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:証明書にこれらの拡張機能が含まれている場合、古いクライアントで接続の問題が発生する場合を除き、このチェックボックスをオンのままにします。

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。拡張子を付けてファイルを保存します `.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。

   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。

作業を開始する前に

- 特定のアクセス権限が必要です。
- を使用することができます `Passwords.txt` ファイル。

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. に記載されているパスワードを入力します `Passwords.txt` ファイル。
   c. 次のコマンドを入力してrootに切り替えます。 `su -`
   d. に記載されているパスワードを入力します `Passwords.txt` ファイル。

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

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

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

   - の場合 `--domains`、ワイルドカードを使用して、すべての管理ノードの完全修飾ドメイン名を表します。例： `*.ui.storagegrid.example.com` ワイルドカード*を使用して表します `admin1.ui.storagegrid.example.com` および `admin2.ui.storagegrid.example.com`。
   - 設定 `--type` 終了： `management` 管理インターフェイスの証明書を設定します。この証明書はGrid ManagerとTenant Managerで使用されます。

◦ 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。を使用できます `--days` デフォルトの有効期間を上書きする引数。

> 証明書の有効期間は、で始まります `make-certificate` を実行します。管理クライアントが 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 クライアントで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バンドルをダウンロードします `.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。拡張子を付けてファイルを保存します `.pem`。

   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に貼り付けます。

c. 拡張子を付けてテキストファイルを保存します `.pem`。

   例： `storagegrid_certificate.pem`

S3 および Swift API 証明書を設定する

ストレージノードまたはロードバランサエンドポイントへのS3 / Swiftクライアント接続に使用されるサーバ証明書を置き換えたりリストアしたりできます。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* Expiration of global server certificate for S3 and Swift API *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）。
- 証明書の秘密鍵：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。拡張子を付けてファイルを保存します `.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。

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（オプション）	証明書所有者のX.509サブジェクト名または識別名（DN）。 このフィールドに値を入力しない場合、生成される証明書では、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。
有効な日数	作成後に証明書の有効期限が切れる日数。
キー使用の拡張機能を追加します	選択されている場合（デフォルトおよび推奨）、キー使用と拡張キー使用拡張が生成された証明書に追加されます。 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:証明書にこれらの拡張機能が含まれている場合、古いクライアントで接続の問題が発生する場合を除き、このチェックボックスをオンのままにします。

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。拡張子を付けてファイルを保存します `.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クライアント接続でデフォルトの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。

   S3およびSwift APIのグローバル証明書のデフォルト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、システムからリカバリすることはできません。ストレージノードへの以降の新しいS3およびSwiftクライアント接続には、デフォルトのS3およびSwift API証明書が使用されます。

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バンドルをダウンロードします `.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。拡張子を付けてファイルを保存します `.pem`。

   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に貼り付けます。

c. 拡張子を付けてテキストファイルを保存します `.pem`。

   例： `storagegrid_certificate.pem`

関連情報

- "S3 REST APIを使用する"
- "Swift REST APIを使用する"
- "S3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。

作業を開始する前に

- 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

証明書をダウンロードします `.pem` ファイル。

a. [証明書のダウンロード] を選択します。
b. 証明書ファイルの名前とダウンロード先を指定します。拡張子を付けてファイルを保存します `.pem`。

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. 拡張子を付けてテキストファイルを保存します `.pem`。

例： `storagegrid_certificate.pem`

FabricPool の StorageGRID 証明書を設定します

S3クライアントが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場合（FabricPool を使用するONTAP クライアントなど）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。

作業を開始する前に

- 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"。

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。

著作権に関する情報

商標に関する情報