キー管理サーバの追加（KMS）

StorageGRID 11.5

NetApp
April 11, 2024

目次

キー管理サーバの追加（KMS）

StorageGRID キー管理サーバウィザードを使用して、各 KMS または KMS クラスタを追加します。

必要なもの

- を確認しておく必要があります "キー管理サーバを使用する際の考慮事項と要件"。
- が必要です "KMS でクライアントとして StorageGRID を設定"をクリックし、KMSまたはKMSクラスタごとに必要な情報を確認しておく必要があります
- 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。

このタスクについて

可能環境 であれば、サイト固有のキー管理サーバを設定してから、別の KMS で管理されていないデフォルトの KMS を設定してください。最初にデフォルトの KMS を作成すると、グリッド内のノードで暗号化されたすべてのアプライアンスがデフォルトの KMS で暗号化されます。サイト固有の KMS をあとで作成するには、まず、暗号化キーの現在のバージョンをデフォルトの KMS から新しい KMS にコピーする必要があります。

"サイトの KMS を変更する際の考慮事項"

手順

1. "手順 1 ： KMS の詳細を入力します"
2. "手順 2 ：サーバ証明書をアップロードする"
3. "手順 3 ：クライアント証明書をアップロードする"

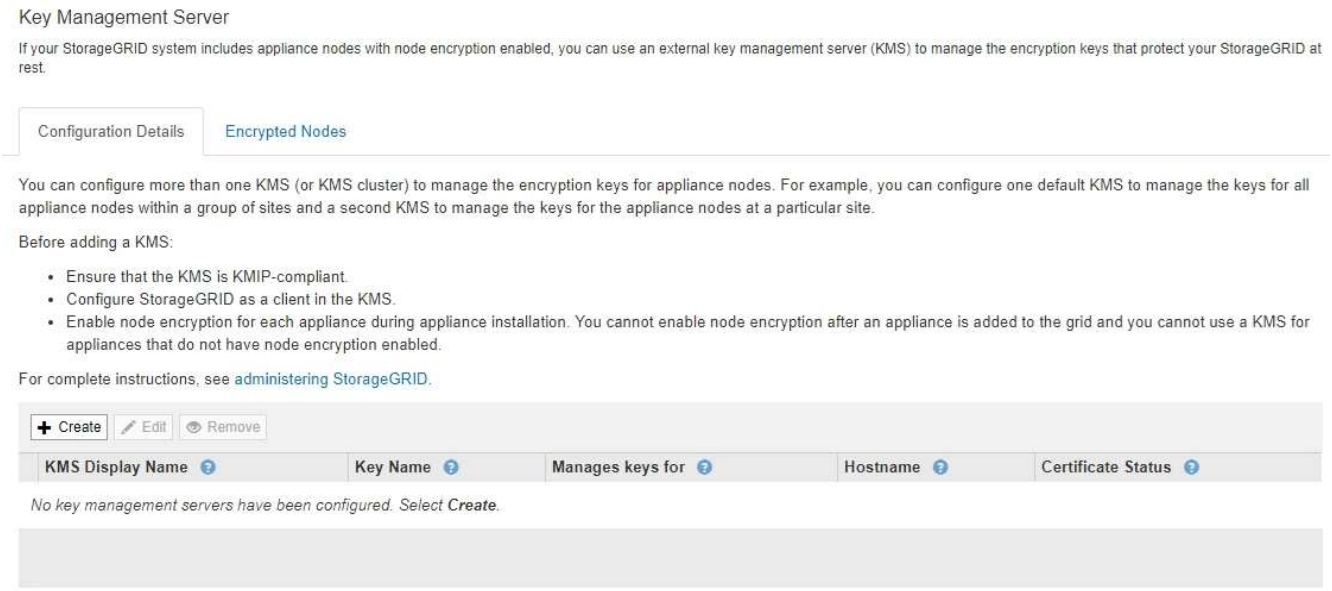
手順 1 ： KMS の詳細を入力します

キー管理サーバの追加ウィザードの手順 1 （ KMS の詳細を入力）で、 KMS または KMS クラスタの詳細を指定します。

手順

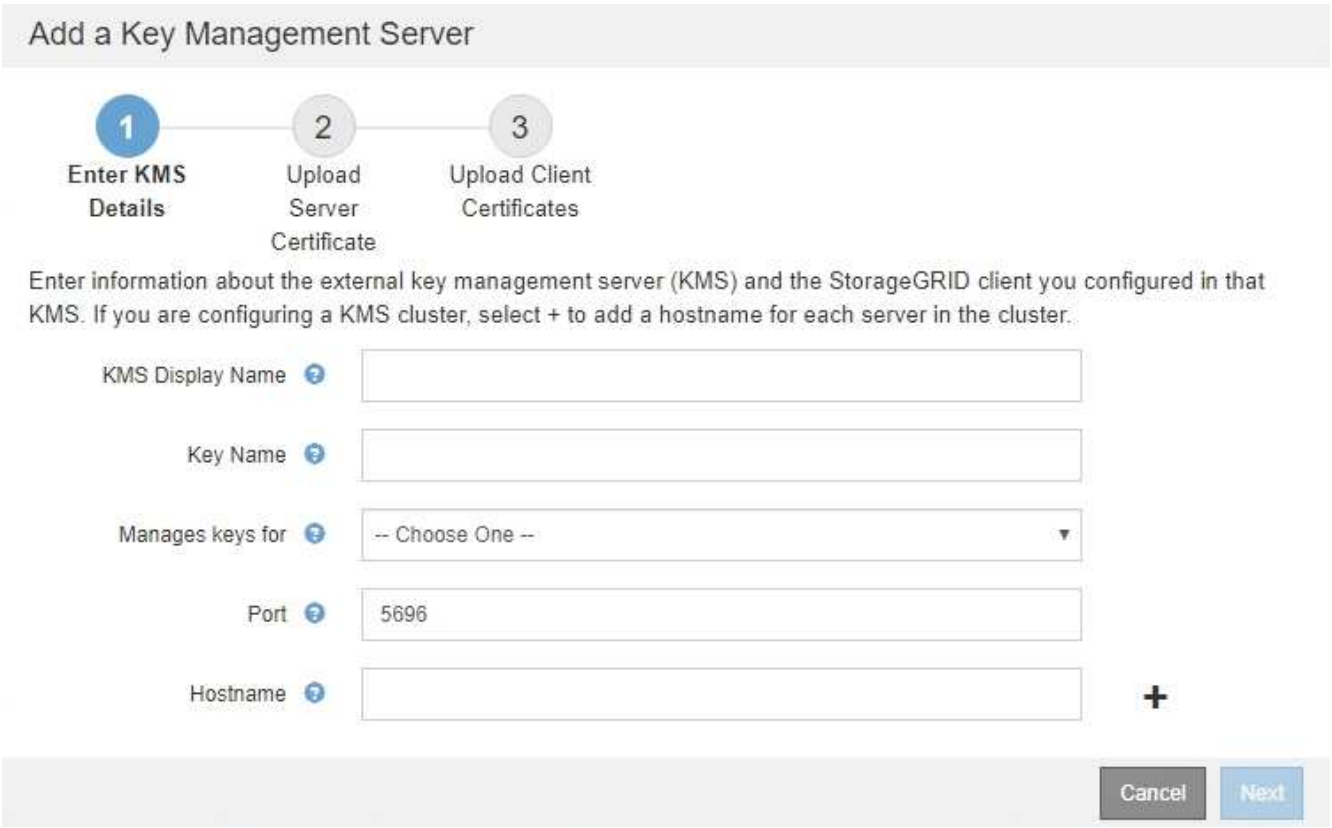
1. 「* Configuration * System Settings ** Key Management Server *」を選択します。

   [Key Management Server] ページが表示され、 [Configuration] [Details] タブが選択されます。



2. 「 * Create * 」を選択します。

Add a Key Management Server （キー管理サーバの追加）ウィザードの手順 1 （ KMS の詳細を入力）が表示されます。



3. KMS および設定した StorageGRID クライアントの情報を KMS で入力します。

フィールド	説明
KMS 表示名	この KMS を特定するのに役立つわかりやすい名前。1~64 文字で指定します。
キー名	KMS 内の StorageGRID クライアントの正確なキーエイリアス。1~255 文字で指定する必要があります。
のキーを管理します	この KMS に関連する StorageGRID サイトを参照してください。可能であれば、サイト固有のキー管理サーバを設定してから、環境 で他の KMS で管理されていないすべてのサイトをデフォルトの KMS で設定する必要があります。 • 特定のサイトのアプライアンスノードの暗号化キーをこの KMS で管理する場合は、サイトを選択します。 • 「 * Sites not managed by another KMS （デフォルト KMS ） * 」を選択して、専用の KMS とその後の拡張で追加したサイトに適用されるデフォルトの KMS を設定します。 ◦ 注： * 以前にデフォルト KMS で暗号化されていたサイトを選択しても、新しい KMS に元の暗号化キーの現在のバージョンを提供しなかった場合、 KMS の設定を保存すると、検証エラーが発生します。
ポート	KMS サーバが Key Management Interoperability Protocol （ KMIP ）の通信に使用するポート。デフォルトでは、 KMIP 標準ポートである 5696 が使用されます。
ホスト名	KMS の完全修飾ドメイン名または IP アドレス。 • 注： * サーバ証明書の SAN フィールドには、ここに入力する FQDN または IP アドレスを含める必要があります。そうしないと、StorageGRID は KMS クラスタ内のすべてのサーバに接続できなくなります。

4. KMS クラスタを使用している場合は、プラス記号を選択します ➕ クラスタ内の各サーバのホスト名を追加します。
5. 「 * 次へ * 」を選択します。

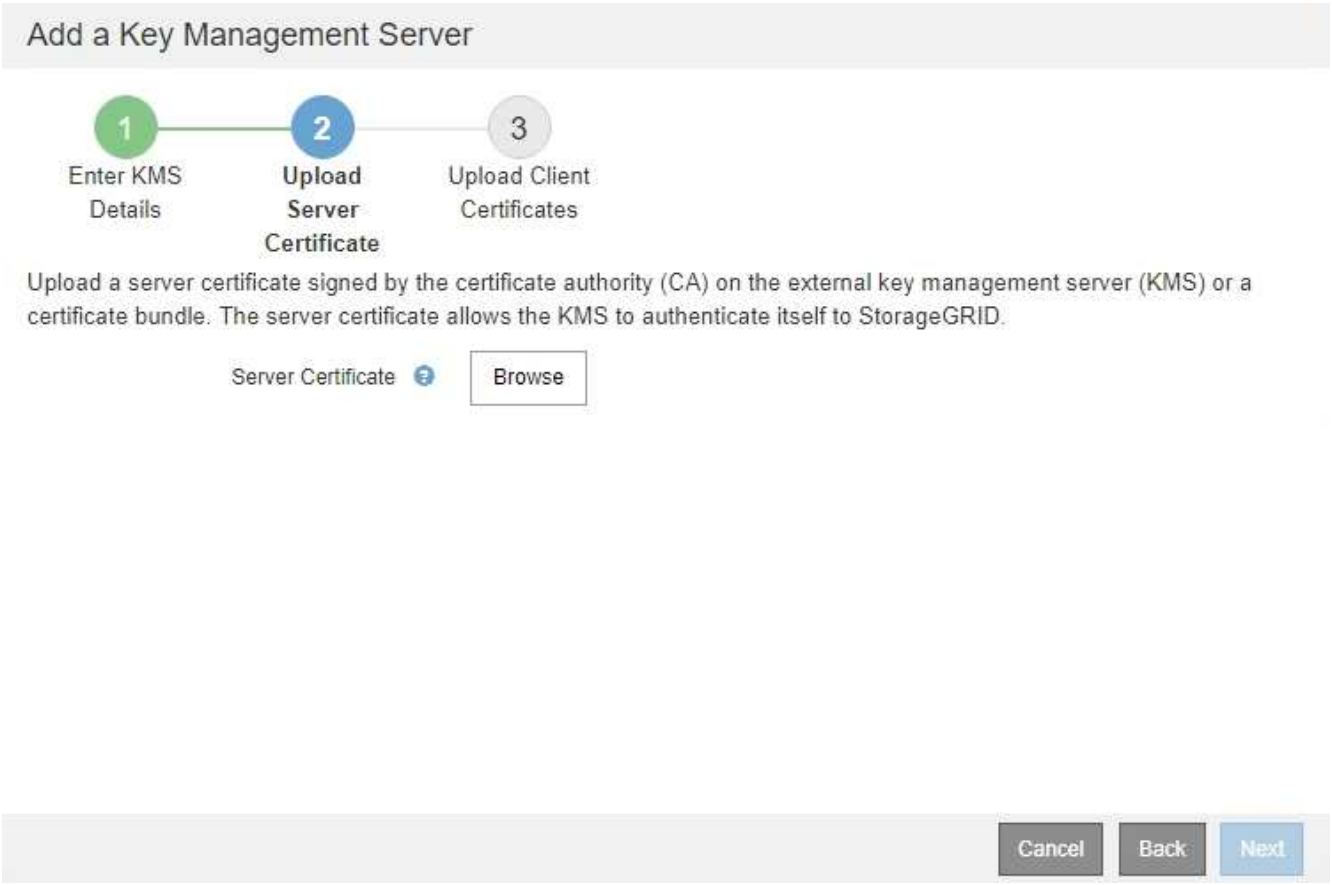
   キー管理サーバの追加ウィザードの手順2（サーバ証明書をアップロード）が表示されます。

手順 2 ：サーバ証明書をアップロードする

キー管理サーバの追加ウィザードの手順 2 （サーバ証明書をアップロード）で、 KMS のサーバ証明書（または証明書バンドル）をアップロードします。サーバ証明書を使用すると、外部 KMS は StorageGRID に対して自身を認証できます。

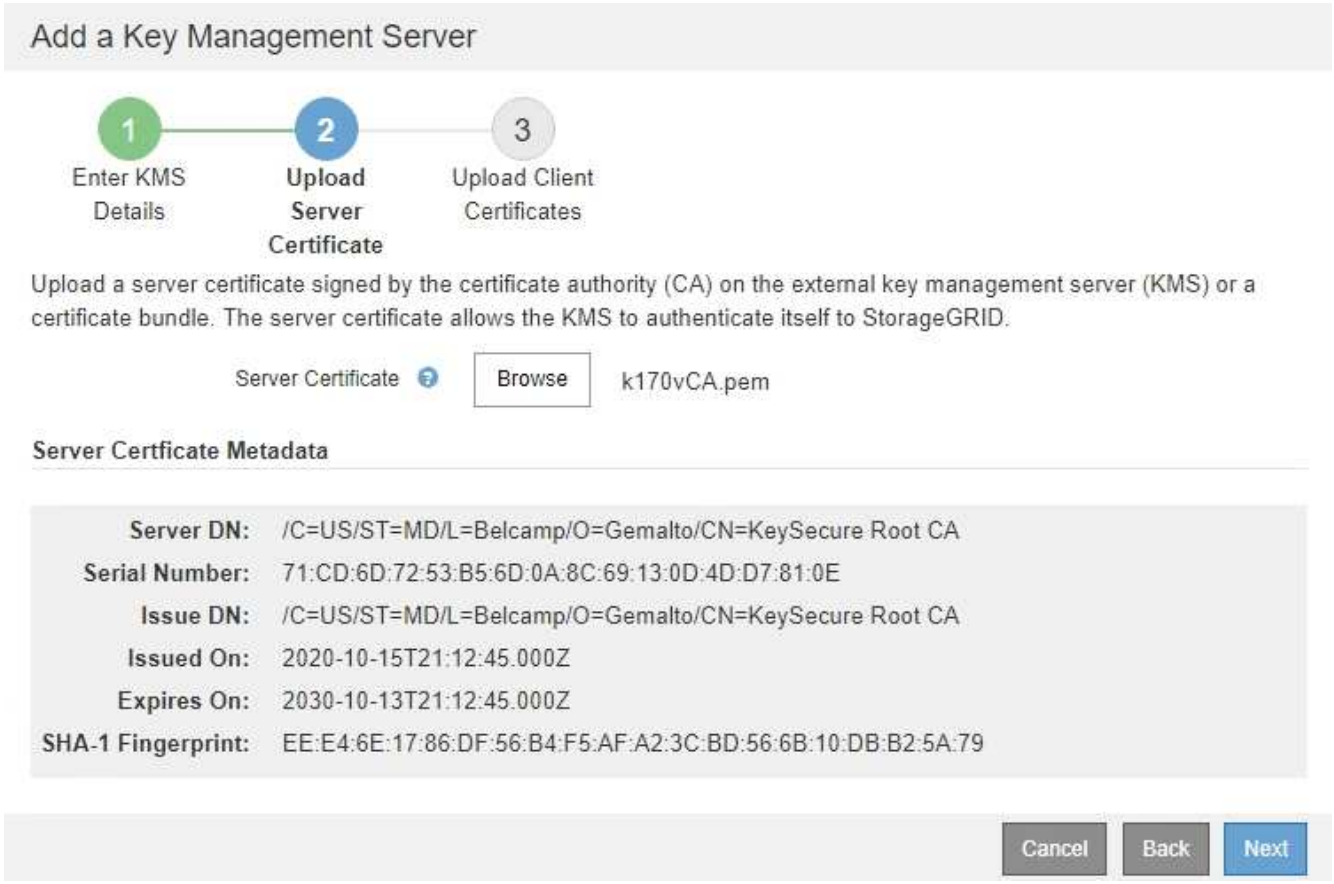
手順

1. 手順 2 （サーバー証明書のアップロード） * から、保存されているサーバー証明書または証明書バンドルの場所を参照します。



2. 証明書ファイルをアップロードします。

   サーバ証明書のメタデータが表示されます。



証明書バンドルをアップロードした場合は、各証明書のメタデータが独自のタブに表示されます。

3. 「 * 次へ * 」を選択します。

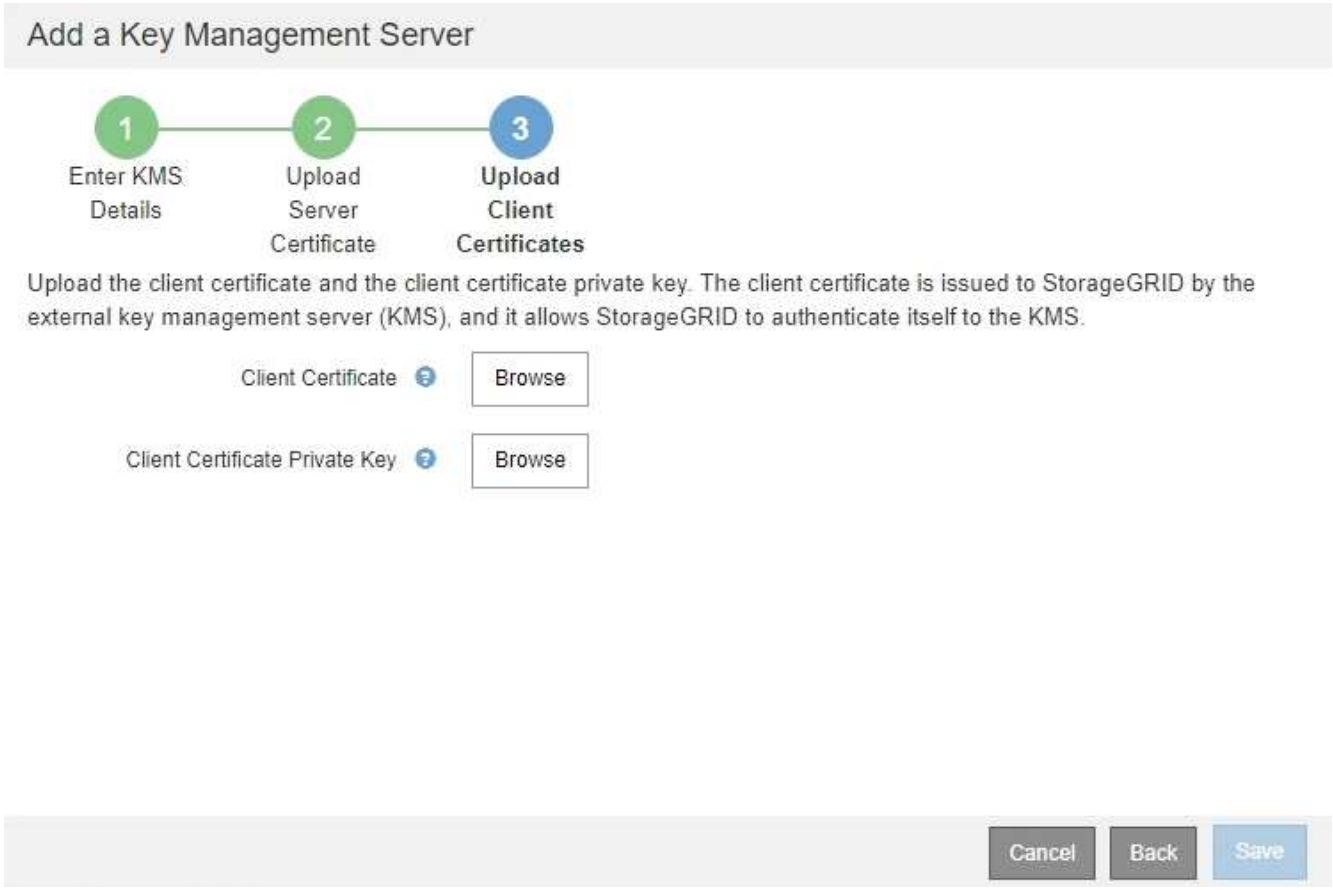
   Add a Key Management Serverウィザードの手順3（クライアント証明書をアップロード）が表示されます。

手順 3 ：クライアント証明書をアップロードする

キー管理サーバの追加ウィザードの手順 3 （クライアント証明書をアップロード）で、クライアント証明書とクライアント証明書の秘密鍵をアップロードします。クライアント証明書は、 StorageGRID が KMS に対して自身を認証することを許可します。

手順

1. * 手順 3 （クライアント証明書をアップロード） * から、クライアント証明書の場所を参照します。

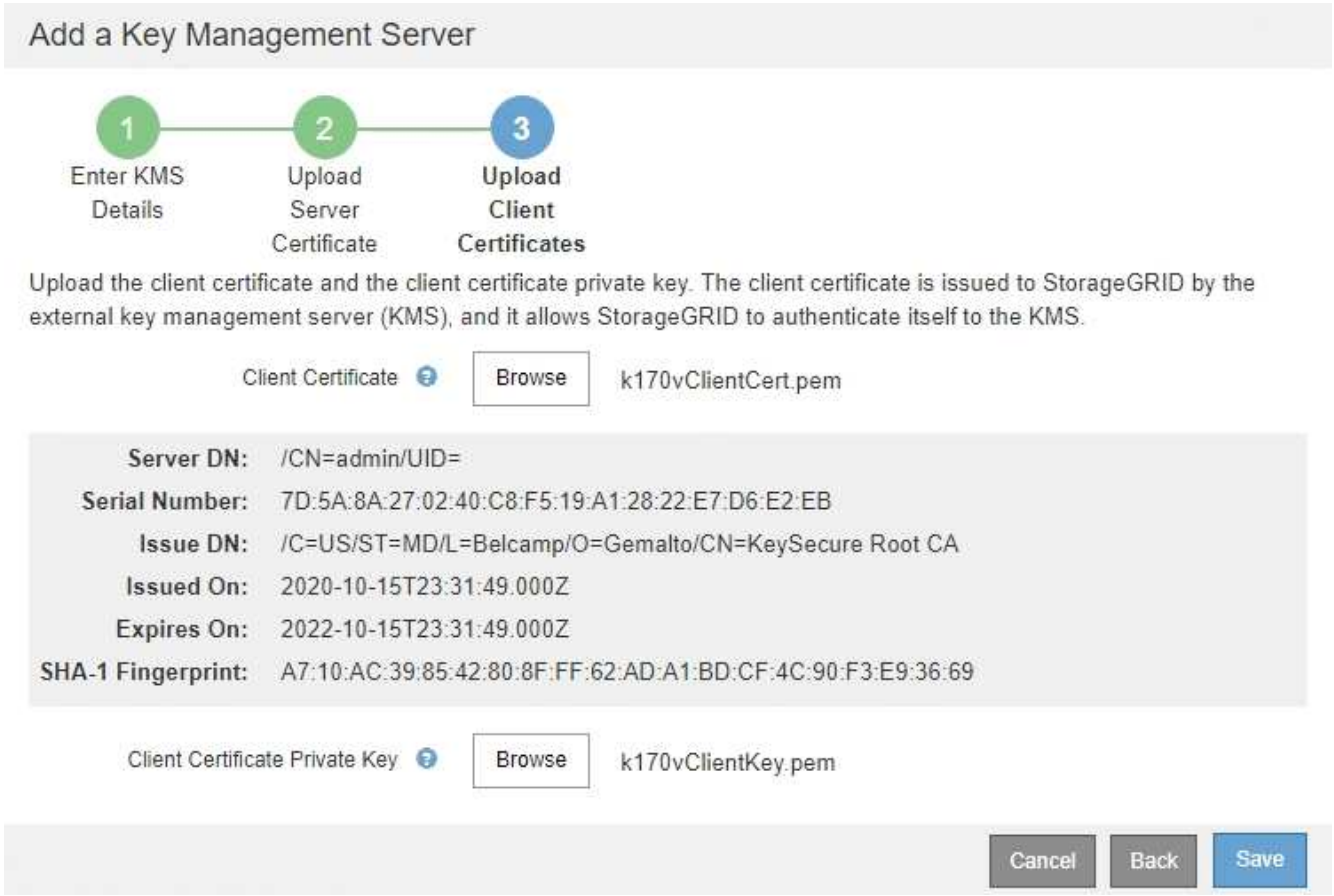


2. クライアント証明書ファイルをアップロードします。

   クライアント証明書のメタデータが表示されます。

3. クライアント証明書の秘密鍵の場所を参照します。
4. 秘密鍵ファイルをアップロードします。

   クライアント証明書とクライアント証明書の秘密鍵のメタデータが表示されます。



5. [保存（ Save ）] を選択します。

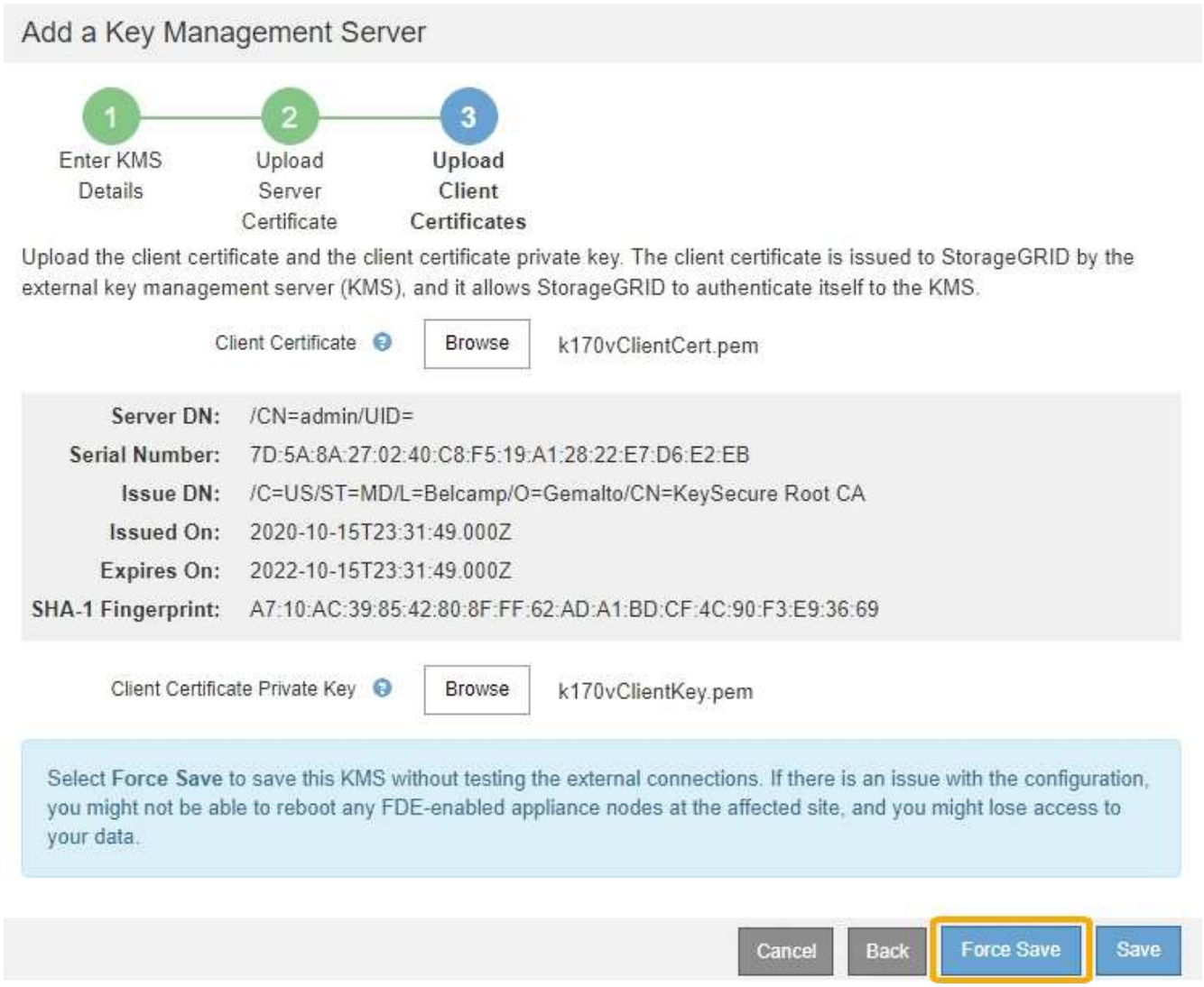
   キー管理サーバとアプライアンスノードの間の接続をテストします。すべての接続が有効で、正しいキーが KMS にある場合は、新しいキー管理サーバが Key Management Server ページの表に追加されます。

   > KMS を追加すると、すぐに [Key Management Server] ページの証明書ステータスが [Unknown （不明）] と表示されます。各証明書の実際のステータスの StorageGRID 取得には 30 分程度かかる場合があります。最新のステータスを表示するには、 Web ブラウザの表示を更新する必要があります。

6. 「 * Save * （保存）」を選択したときにエラーメッセージが表示された場合は、メッセージの詳細を確認し、「 * OK * 」を選択します。

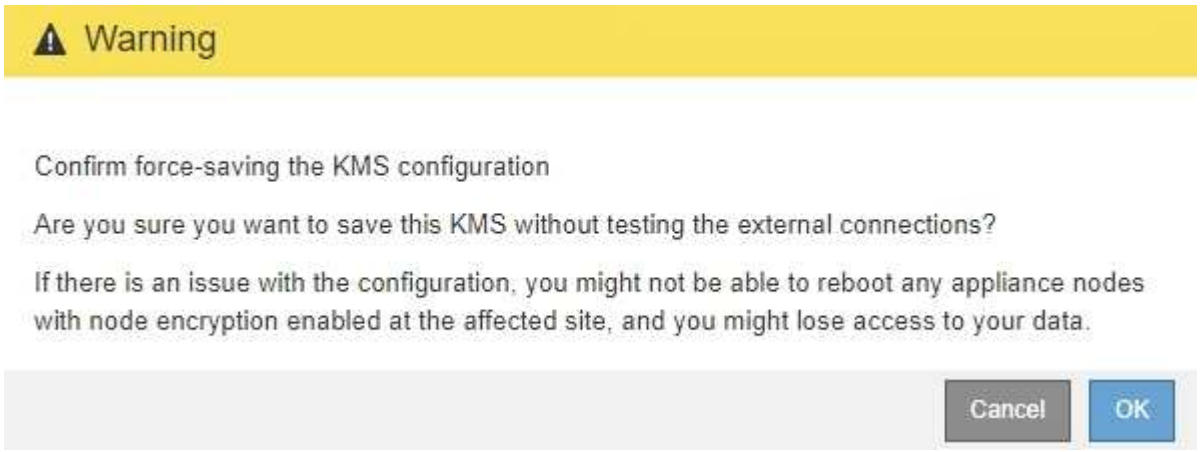
   たとえば、接続テストに失敗した場合は、 422 ： Unprocessable Entity エラーが返されることがあります。

7. 外部接続をテストせずに現在の設定を保存する必要がある場合は、 * 強制保存 * を選択します。



[強制保存] を選択すると KMS の設定が保存されますが、各アプライアンスからその KMS への外部接続はテストされません。構成を含む問題 がある場合、該当するサイトでノード暗号化が有効になっているアプライアンスノードをリブートできない可能性があります。問題が解決するまでデータにアクセスできなくなる可能性があります。

8. 確認の警告を確認し、設定を強制的に保存する場合は、「 * OK 」を選択します。



KMS の設定は保存されますが、 KMS への接続はテストされません。

著作権に関する情報

商標に関する情報