



キー管理サーバを設定

StorageGRID 11.7

NetApp
April 12, 2024

目次

キー管理サーバを設定	1
キー管理サーバの設定：概要	1
KMS とアプライアンスの設定の概要	1
キー管理サーバを使用する際の考慮事項と要件	4
サイトの KMS を変更する際の考慮事項	7
KMS でクライアントとして StorageGRID を設定します	10
キー管理サーバ（KMS）を追加する	11
KMS の詳細を確認します	18
暗号化されたノードを表示する	19
キー管理サーバ（KMS）を編集する	21
キー管理サーバ（KMS）を削除する	23

キー管理サーバを設定

キー管理サーバの設定：概要

1 つ以上の外部キー管理サーバ（KMS）を設定して、特別に設定したアプライアンスノード上のデータを保護することができます。

キー管理サーバ（KMS）とは何ですか？

キー管理サーバ（KMS）は、関連する StorageGRID サイトの StorageGRID アプライアンスノードに Key Management Interoperability Protocol（KMIP）を使用して暗号化キーを提供する外部のサードパーティシステムです。

インストール時にノード暗号化 * 設定が有効になっている StorageGRID アプライアンスノードのノード暗号化キーを管理するには、1 つ以上のキー管理サーバを使用します。これらのアプライアンスノードでキー管理サーバを使用すると、アプライアンスをデータセンターから削除した場合でも、データを保護できます。アプライアンスボリュームが暗号化されると、ノードがKMSと通信できないかぎり、アプライアンスのデータにアクセスすることはできません。

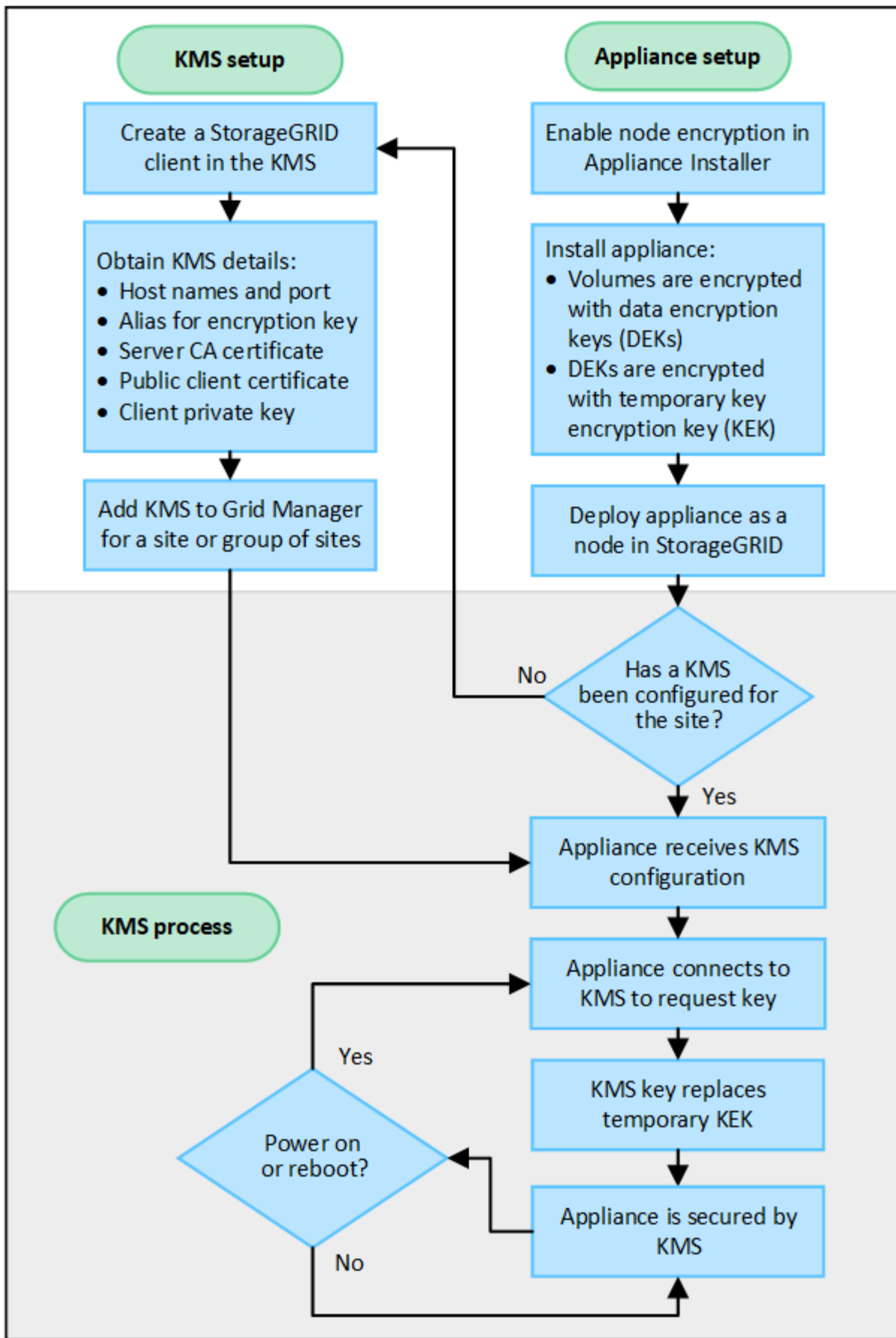


StorageGRID では、アプライアンスノードの暗号化と復号化に使用する外部キーは作成も管理もされません。外部キー管理サーバを使用して StorageGRID データを保護する場合は、そのサーバの設定方法を理解し、暗号化キーの管理方法を理解しておく必要があります。キー管理タスクの実行については、この手順では説明していません。サポートが必要な場合は、キー管理サーバのドキュメントを参照するか、テクニカルサポートにお問い合わせください。

KMS とアプライアンスの設定の概要

キー管理サーバ（KMS）を使用してアプライアンスノード上の StorageGRID データを保護する前に、1 つ以上の KMS サーバを設定してアプライアンスノードのノード暗号化を有効にするという 2 つの設定タスクを完了しておく必要があります。これらの 2 つの設定タスクが完了すると、キー管理プロセスが自動的に実行されます。

フローチャートは、KMS を使用してアプライアンスノード上の StorageGRID データを保護する手順の概要を示しています。



フローチャートには、KMS のセットアップとアプライアンスのセットアップが並行して行われていることが

示されています。ただし、要件に基づいて、新しいアプライアンスノードのノード暗号化を有効にする前後にキー管理サーバをセットアップできます。

キー管理サーバ（KMS）のセットアップ

キー管理サーバのセットアップには、主に次の手順が含まれます。

ステップ	を参照してください
KMS ソフトウェアにアクセスし、各 KMS または KMS クラスタに StorageGRID 用のクライアントを追加します。	"KMS でクライアントとして StorageGRID を設定します"
KMS で StorageGRID クライアントの必要な情報を入手します。	"KMS でクライアントとして StorageGRID を設定します"
Grid Manager に KMS を追加して 1 つのサイトまたはデフォルトのサイトグループに割り当て、必要な証明書をアップロードして、KMS の設定を保存します。	"キー管理サーバ（KMS）を追加する"

アプライアンスをセットアップします

KMS を使用するためにアプライアンスノードをセットアップするには、次の手順に従います。

1. アプライアンスのハードウェア構成フェーズでは、StorageGRID アプライアンスインストーラを使用してアプライアンスのノード暗号化 * 設定を有効にします。



アプライアンスをグリッドに追加したあとに * Node Encryption * 設定を有効にすることはできません。また、ノード暗号化が有効になっていないアプライアンスでは外部キー管理を使用できません。

2. StorageGRID アプライアンスインストーラを実行します。インストール時に、次のように各アプライアンスボリュームにランダムデータ暗号化キー（DEK）が割り当てられます。
 - DEK は、各ボリュームのデータの暗号化に使用されます。これらのキーは、アプライアンス OS の Linux Unified Key Setup（LUKS）ディスク暗号化を使用して生成され、変更することはできません。
 - 各 DEK は、KEK（Master Key Encryption Key）によって暗号化されます。最初の KEK は、アプライアンスが KMS に接続できるまで DEK を暗号化する一時キーです。
3. StorageGRID にアプライアンスノードを追加します。

を参照してください "[ノード暗号化を有効にします](#)" を参照してください。

キー管理の暗号化プロセス（自動的に実行）

キー管理の暗号化には、次の高度な手順が含まれています。これらの手順は自動的に実行されます。

1. ノードの暗号化が有効になっているアプライアンスをグリッドにインストールすると、StorageGRID は、新しいノードを含むサイトに KMS 設定が存在するかどうかを確認します。

- KMS がすでにサイト用に設定されている場合、アプライアンスは KMS の設定を受信します。
 - KMS がサイト用にまだ設定されていない場合は、サイトに KMS を設定し、アプライアンスが KMS の設定を受信するまで、アプライアンス上のデータは一時的な KEK によって暗号化されたままになります。
2. アプライアンスは KMS 設定を使用して KMS に接続し、暗号化キーを要求します。
 3. KMS は暗号化キーをアプライアンスに送信します。KMS の新しいキーは一時的な KEK に代わるものであり、アプライアンスボリュームの DEK の暗号化と復号化に使用されるようになりました。



暗号化されたアプライアンスノードから設定された KMS に接続する前に存在するデータは、すべて一時キーで暗号化されます。ただし、一時キーを KMS 暗号化キーに置き換えるまでは、アプライアンスボリュームをデータセンターから削除できないようにする必要があります。

4. アプライアンスの電源をオンにするか再接続すると、KMS に接続してキーを要求します。揮発性メモリに保存されているキーは、電源の喪失や再起動に耐えられません。

キー管理サーバを使用する際の考慮事項と要件

外部キー管理サーバ（KMS）を設定する前に、考慮事項と要件を確認しておく必要があります。

KMIP の要件

StorageGRID は KMIP バージョン 1.4 をサポートしています。

["Key Management Interoperability Protocol（キー管理相互運用性プロトコル）仕様バージョン 1.4"](#)

アプライアンスノードと設定された KMS の間の通信には、セキュアな TLS 接続が使用されます。StorageGRID では、KMIP で次の TLS v1.2 暗号をサポートしています。

- TLS_ECDHE_RSA_with_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_With_AES_256_GCM_SHA384

ノード暗号化を使用する各アプライアンスノードに、サイト用に設定した KMS または KMS クラスタへのネットワークアクセスがあることを確認してください。

ネットワークのファイアウォールの設定で、各アプライアンスノードが Key Management Interoperability Protocol（KMIP）の通信に使用するポートを介して通信できるようにする必要があります。デフォルトの KMIP ポートは 5696 です。

サポートされているアプライアンスはどれですか。

キー管理サーバ（KMS）を使用して、「ノード暗号化 *」が有効になっているグリッド内の StorageGRID アプライアンスの暗号化キーを管理できます。この設定は、StorageGRID アプライアンスインストーラを使用してアプライアンスをインストールするハードウェア構成の段階でのみ有効にできます。



アプライアンスをグリッドに追加したあとにノード暗号化を有効にすることはできません。また、ノード暗号化が有効になっていないアプライアンスでは、外部キー管理を使用できません。

StorageGRID アプライアンスおよびアプライアンスノードに対して設定したKMSを使用できます。

次のようなソフトウェアベース（アプライアンス以外）のノードでは、設定されたKMSを使用できません。

- 仮想マシン（VM）として導入されたノード
- Linux ホストのコンテナエンジン内に導入されたノード

これらの他のプラットフォームに導入されたノードでは、データストアまたはディスクレベルで StorageGRID 外部の暗号化を使用できます。

キー管理サーバを設定する必要があるのはいつですか？

新規インストールの場合は、テナントを作成する前に Grid Manager で 1 つ以上のキー管理サーバをセットアップするのが一般的です。この順序により、ノード上に格納されるオブジェクトデータよりも先にノードが保護されます。

Grid Manager では、アプライアンスノードのインストール前またはインストール後にキー管理サーバを設定できます。

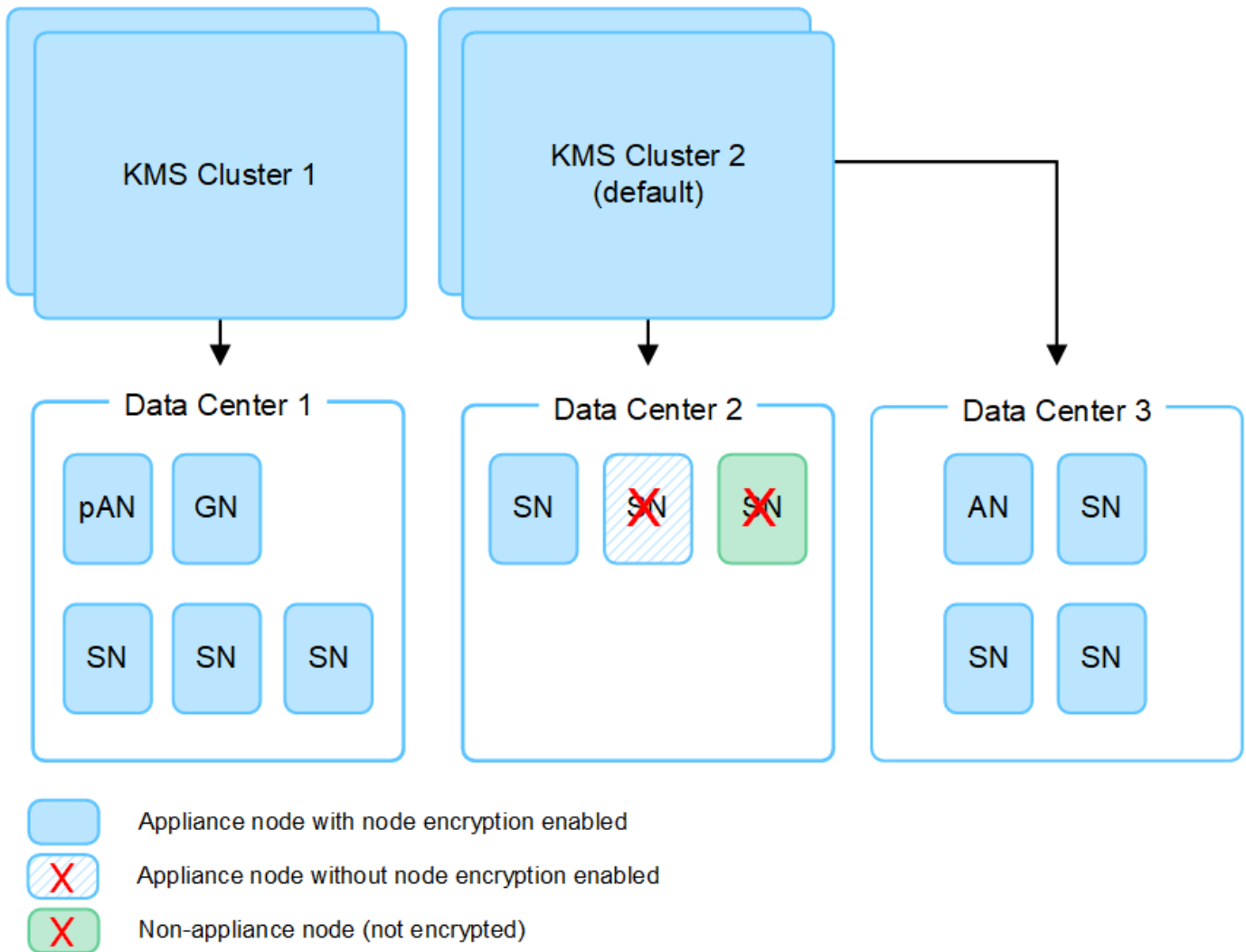
必要なキー管理サーバの数

1 つ以上の外部キー管理サーバを設定して、StorageGRID システム内のアプライアンスノードに暗号化キーを提供できます。各 KMS は、1 つのサイトまたはサイトグループにある StorageGRID アプライアンスノードに単一の暗号化キーを提供します。

StorageGRID は KMS クラスタの使用をサポートしています。各 KMS クラスタには、設定と暗号化キーを共有するレプリケートされた複数のキー管理サーバが含まれます。高可用性構成のフェイルオーバー機能が向上するため、KMS クラスタをキー管理に使用することを推奨します。

たとえば、StorageGRID システムに 3 つのデータセンターサイトがあるとします。1 つの KMS クラスタを設定して、データセンター 1 のすべてのアプライアンスノードともう 1 つの KMS クラスタのキーを取得し、他のすべてのサイトにあるすべてのアプライアンスノードのキーを取得することができます。2 つ目の KMS クラスタを追加すると、データセンター 2 とデータセンター 3 にデフォルトの KMS を設定できます。

非アプライアンスノード、またはインストール時に * Node Encryption * 設定が有効になっていないアプライアンスノードには、KMSを使用できないことに注意してください。



キーをローテーションするとどうなりますか。

セキュリティのベストプラクティスとして、設定された各 KMS で使用される暗号化キーを定期的にローテーションすることを推奨します。

暗号化キーをローテーションするときは、KMS ソフトウェアを使用して、最後に使用したバージョンのキーを同じキーの新しいバージョンにローテーションします。完全に別のキーに回転しないでください。



キーのローテーションは、Grid Manager 内の KMS のキー名（エイリアス）を変更しては実行しないでください。代わりに、KMS ソフトウェアのキーバージョンを更新してキーをローテーションしてください。以前のキーに使用したものと同一キーエイリアスを新しいキーに使用します。設定されている KMS のキーエイリアスを変更すると、StorageGRID がデータを復号化できなくなる可能性があります。

新しいキーバージョンが利用可能になった場合：

- このサービスは、KMS に関連付けられているサイトにある暗号化されたアプライアンスノードに自動的に配信されます。キーが回転した後 1 時間以内に分配が行われる必要があります。
- 新しいキーバージョンが配布されたときに暗号化アプライアンスノードがオフラインになっている場合、ノードはリポート後すぐに新しいキーを受け取ります。

- 何らかの理由で新しいバージョンのキーを使用してアプライアンスボリュームを暗号化できない場合は、アプライアンスノードに対して * kms encryption key rotation failed * アラートがトリガーされます。このアラートの解決方法については、テクニカルサポートへの問い合わせが必要になることがあります。

アプライアンスノードは暗号化したあとに再利用できますか。

暗号化されたアプライアンスを別の StorageGRID システムにインストールする必要がある場合は、先にグリッドノードの運用を停止して、オブジェクトデータを別のノードに移動しておく必要があります。その後、StorageGRID アプライアンスインストーラを使用して実行できます **"KMS構成をクリアします"**。KMS の設定をクリアすると、「ノード暗号化 *」設定が無効になり、アプライアンスノードと StorageGRID サイトの KMS 設定の間の関連付けが解除されます。



KMS 暗号化キーにアクセスできないため、アプライアンスに残っているデータにはアクセスできなくなり、永続的にロックされます。

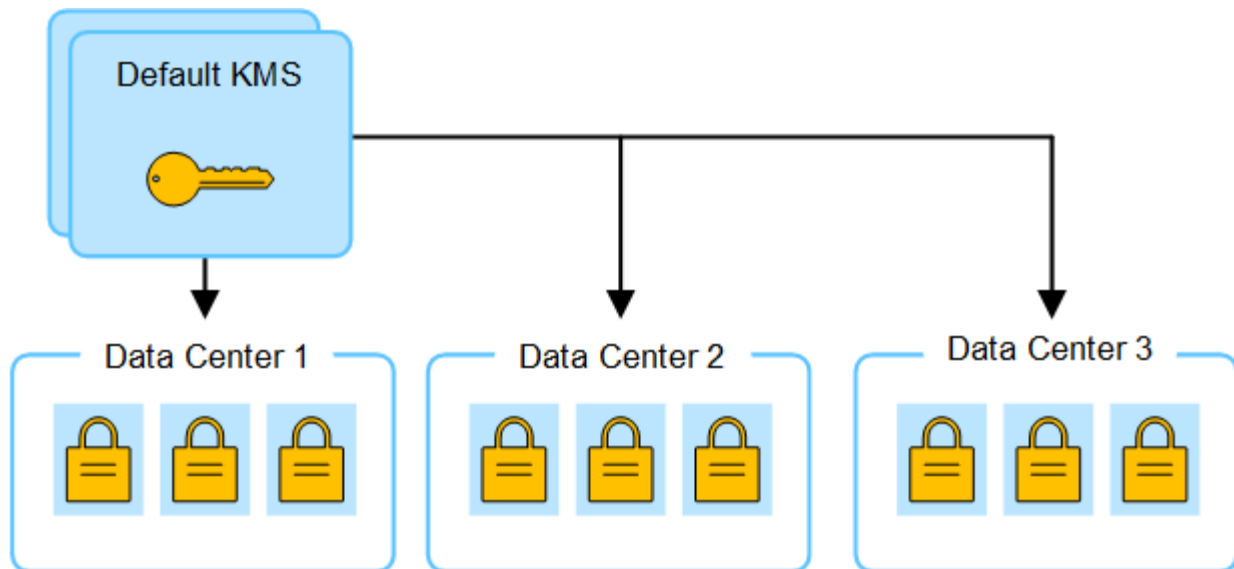
サイトの **KMS** を変更する際の考慮事項

各キー管理サーバ (KMS) または KMS クラスタは、1つのサイトまたはサイトグループにあるすべてのアプライアンスノードに暗号化キーを提供します。サイトで使用する KMS を変更する必要がある場合は、暗号化キーを KMS から別の KMS にコピーする必要があります。

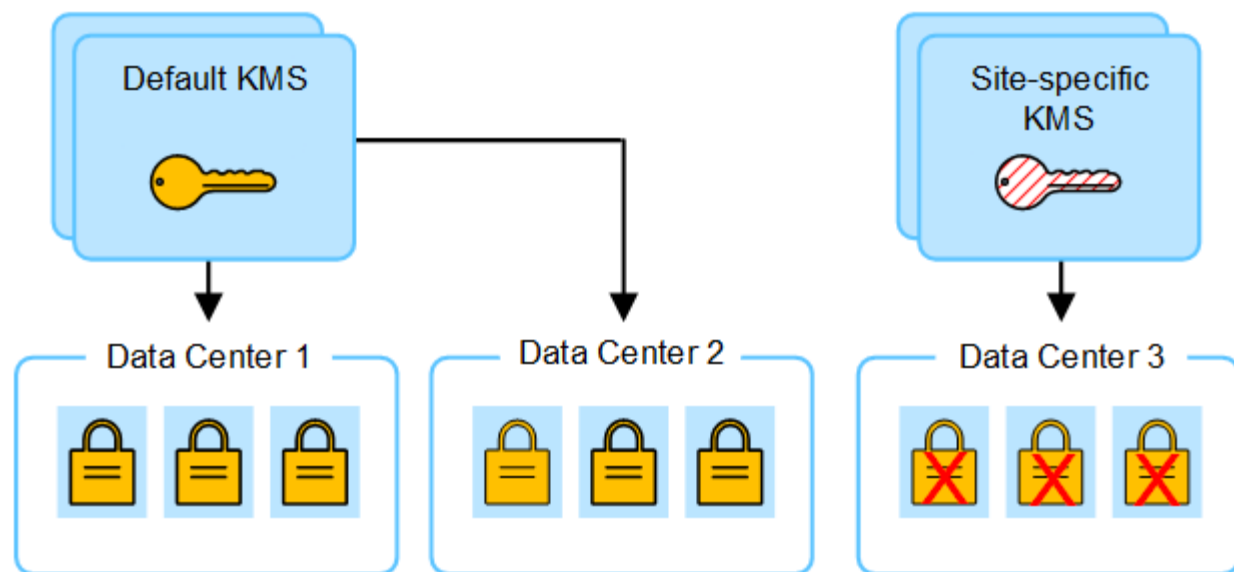
サイトで使用されている KMS を変更する場合は、そのサイトで以前に暗号化したアプライアンスノードを新しい KMS に格納されているキーを使用して復号化できることを確認する必要があります。場合によっては、暗号化キーの現在のバージョンを元の KMS から新しい KMS にコピーする必要があります。サイトで暗号化されたアプライアンスノードを復号化するために、KMS に正しいキーがあることを確認する必要があります。

例：

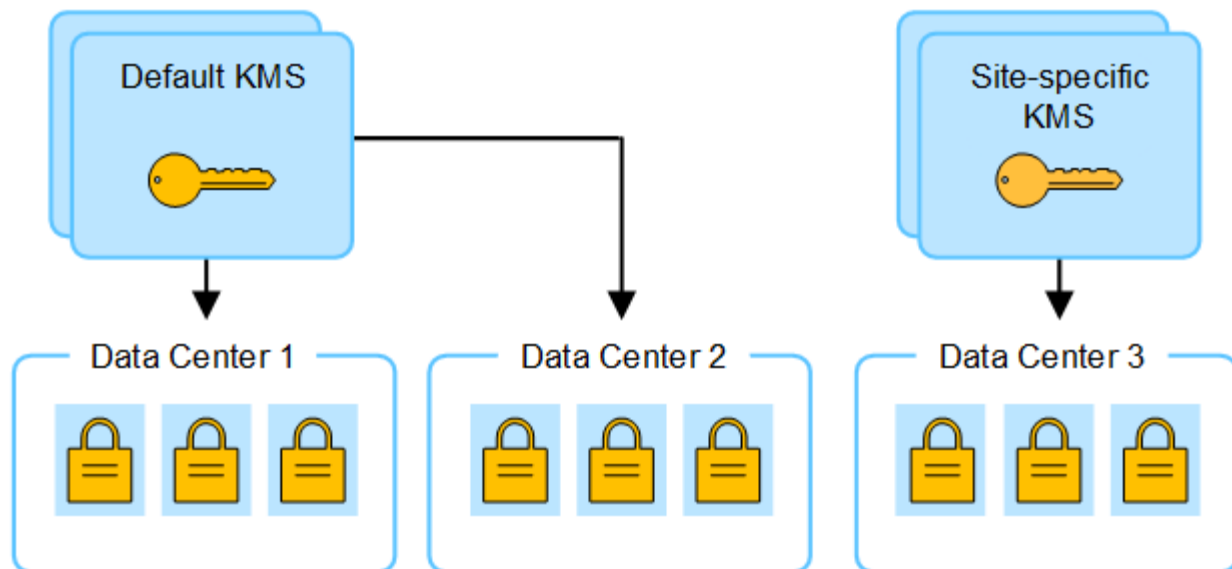
1. 最初に、専用の KMS を持たないすべてのサイトを環境するデフォルト KMS を構成します。
2. KMS を保存すると、「Node Encryption *」設定が有効になっているすべてのアプライアンスノードが KMS に接続して暗号化キーを要求します。このキーは、すべてのサイトのアプライアンスノードの暗号化に使用されます。同じキーを使用して、これらのアプライアンスを復号化する必要があります。



3. 1つのサイト（図のデータセンター3）にサイト固有のKMSを追加することにしました。ただし、アプライアンスノードはすでに暗号化されているため、サイト固有のKMSの設定を保存しようとする時検証エラーが発生します。このエラーは、サイト固有のKMSに、そのサイトでノードを復号化するための正しいキーがないことが原因で発生します。



4. 問題に対応するには、現在のバージョンの暗号化キーをデフォルトのKMSから新しいKMSにコピーします。（技術的には、元のキーを同じエイリアスを持つ新しいキーにコピーします。元のキーが新しいキーの前のバージョンになります）。サイト固有のKMSに、データセンター3でアプライアンスノードを復号化するための正しいキーが付与されるようになり、StorageGRIDに保存できるようになりました。



サイトに使用する **KMS** を変更するユースケース

次の表に、サイトの KMS を変更する一般的なケースに必要な手順をまとめます。

サイトの KMS を変更するユースケース	必要な手順
サイト固有の KMS エントリが 1 つ以上あり、それらのエントリの 1 つをデフォルトの KMS として使用する必要があります。	<p>サイト固有の KMS を編集します。[* キー管理対象 *] フィールドで、別の KMS (デフォルト KMS) で管理されていないサイト * を選択します。サイト固有の KMS がデフォルトの KMS として使用されるようになります。それは専用の KMS を持っていないすべてのサイトに適用されます。</p> <p>"キー管理サーバ (KMS) を編集する"</p>
デフォルトの KMS を使用して、拡張時に新しいサイトを追加する必要があります。新しいサイトにはデフォルトの KMS を使用しないでください。	<ol style="list-style-type: none"> 1. 新しいサイトにあるアプライアンスノードがデフォルトの KMS によって暗号化済みの場合は、KMS ソフトウェアを使用して、現在のバージョンの暗号化キーをデフォルトの KMS から新しい KMS にコピーします。 2. Grid Manager を使用して新しい KMS を追加し、サイトを選択します。 <p>"キー管理サーバ (KMS) を追加する"</p>
サイトの KMS で別のサーバを使用するとします。	<ol style="list-style-type: none"> 1. サイトのアプライアンスノードが既存の KMS によって暗号化済みの場合は、KMS ソフトウェアを使用して、既存の KMS から新しい KMS に暗号化キーの現在のバージョンをコピーします。 2. Grid Manager を使用して既存の KMS 設定を編集し、新しいホスト名または IP アドレスを入力します。 <p>"キー管理サーバ (KMS) を追加する"</p>

KMS でクライアントとして StorageGRID を設定します

KMS を StorageGRID に追加する前に、各外部キー管理サーバまたは KMS クラスタのクライアントとして StorageGRID を設定する必要があります。

このタスクについて

これらの手順はタレスCipherTrust Managerに適用されます。サポートされているバージョンの一覧については、[を参照してください](#) "ネットアップの Interoperability Matrix Tool (IMT)"。

手順

1. KMS ソフトウェアから、使用する KMS または KMS クラスタごとに StorageGRID クライアントを作成します。

各 KMS は、1つのサイトまたはサイトグループにある StorageGRID アプライアンスノードの単一の暗号化キーを管理します。

2. KMS ソフトウェアから、KMS または KMS クラスタごとに AES 暗号化キーを作成します。

暗号化キーは2、048ビット以上で、エクスポート可能である必要があります。

3. KMS または KMS クラスタごとに次の情報を記録します。

この情報は、KMS を StorageGRID に追加するときに必要になります。

- 各サーバのホスト名または IP アドレス。
- KMS で使用される KMIP ポート。
- KMS 内の暗号化キーのキーエイリアス。



暗号化キーは KMS にすでに存在している必要があります。StorageGRID は KMS キーを作成または管理しません。

4. KMS または KMS クラスタごとに、認証局 (CA) が署名したサーバ証明書または PEM でエンコードされた各 CA 証明書ファイルを含む証明書バンドルを、証明書チェーンの順序で連結して取得します。

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。

- 証明書では、Privacy Enhanced Mail (PEM) Base-64 エンコード X.509 形式を使用する必要があります。
- 各サーバ証明書の Subject Alternative Name (SAN) フィールドには、StorageGRID が接続する完全修飾ドメイン名 (FQDN) または IP アドレスを含める必要があります。



StorageGRID で KMS を設定する場合は、「* Hostname *」フィールドに同じ FQDN または IP アドレスを入力する必要があります。

- サーバ証明書は、KMS の KMIP インターフェイスで使用されている証明書と一致する必要があります。通常はポート 5696 が使用されます。
5. 外部 KMS によって StorageGRID に発行されたパブリッククライアント証明書とクライアント証明書の秘密鍵を取得します。

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。

キー管理サーバ（KMS）を追加する

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。

作業を開始する前に

- を確認しておきます ["キー管理サーバを使用する際の考慮事項と要件"](#)。
- これで完了です ["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きます。
- 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"](#)。
- Root アクセス権限が割り当てられている。

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。を参照してください ["サイトの KMS を変更する際の考慮事項"](#) を参照してください。

ステップ1：KMSの詳細

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

手順

1. 設定 * > * セキュリティ * > * キー管理サーバ * を選択します。

[設定の詳細]タブが選択された状態で、[キー管理サーバ]ページが表示されます。

Key management server

If your StorageGRID system includes appliance nodes with node encryption enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID data at rest.

Configuration details

Encrypted nodes

You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

Before adding a KMS:

- Ensure that the KMS is KMIP-compliant.
- Configure StorageGRID as a client in the KMS.
- Enable node encryption for each appliance during appliance installation. You cannot enable node encryption after an appliance is added to the grid and you cannot use a KMS for appliances that do not have node encryption enabled.

For complete instructions, see [Configure key management servers](#).

Create Actions Search... Displaying one result

<input type="checkbox"/>	KMS name	Key name	Manages keys for	Hostname	Certificate expiration
<input type="checkbox"/>	KMS	SG-Global	nmakmipdc1	thales1.vtc.englab.netapp.com and 2 others	✓ All certificates are valid

← Previous 1 Next →

2. 「* Create *」を選択します。

キー管理サーバの追加ウィザードの手順1（KMSの詳細）が表示されます。

Add a Key Management Server ✕

1 KMS Details
 2 Upload server certificate
 3 Upload client certificates

KMS details

Enter information about the external key management server (KMS) and the StorageGRID client you configured in that KMS. If you are configuring a KMS cluster select **Add another hostname** to add a hostname for each server in the cluster.

KMS name ?

Key name ?

Manages keys for ?

▼

Port ?

Hostname ?

[Add another hostname](#)

Cancel
Continue

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。

フィールド	説明
のキーを管理します	<p>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。</p> <ul style="list-style-type: none"> • 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。 • 専用のKMSを持たないサイトや、その後の拡張で追加するサイトに適用されるデフォルトKMSを設定するには、*[別のKMSで管理されていないサイト(デフォルトKMS)]*を選択します。 <ul style="list-style-type: none"> ◦ 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	<p>KMS の完全修飾ドメイン名または IP アドレス。</p> <p>*注：*サーバ証明書のSubject Alternative Name (SAN) フィールドには、ここに入力するFQDNまたはIPアドレスが含まれている必要があります。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。</p>

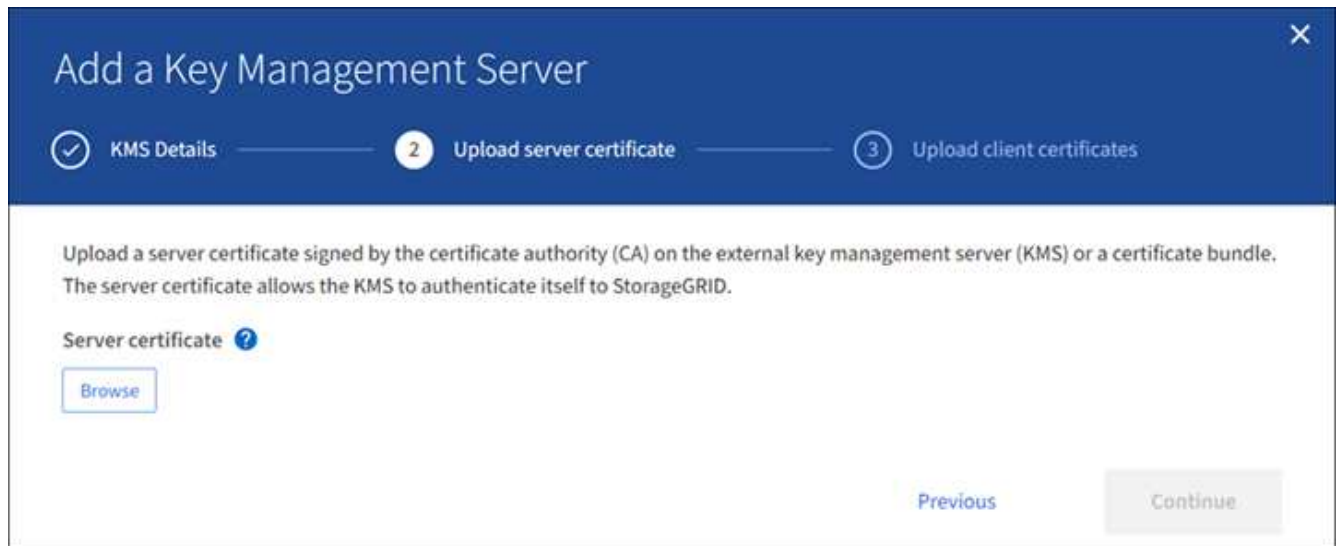
4. KMSクラスタを構成する場合は、*[別のホスト名を追加]*を選択して、クラスタ内の各サーバのホスト名を追加します。
5. 「* Continue *」を選択します。

手順2:サーバ証明書をアップロードします

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）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。

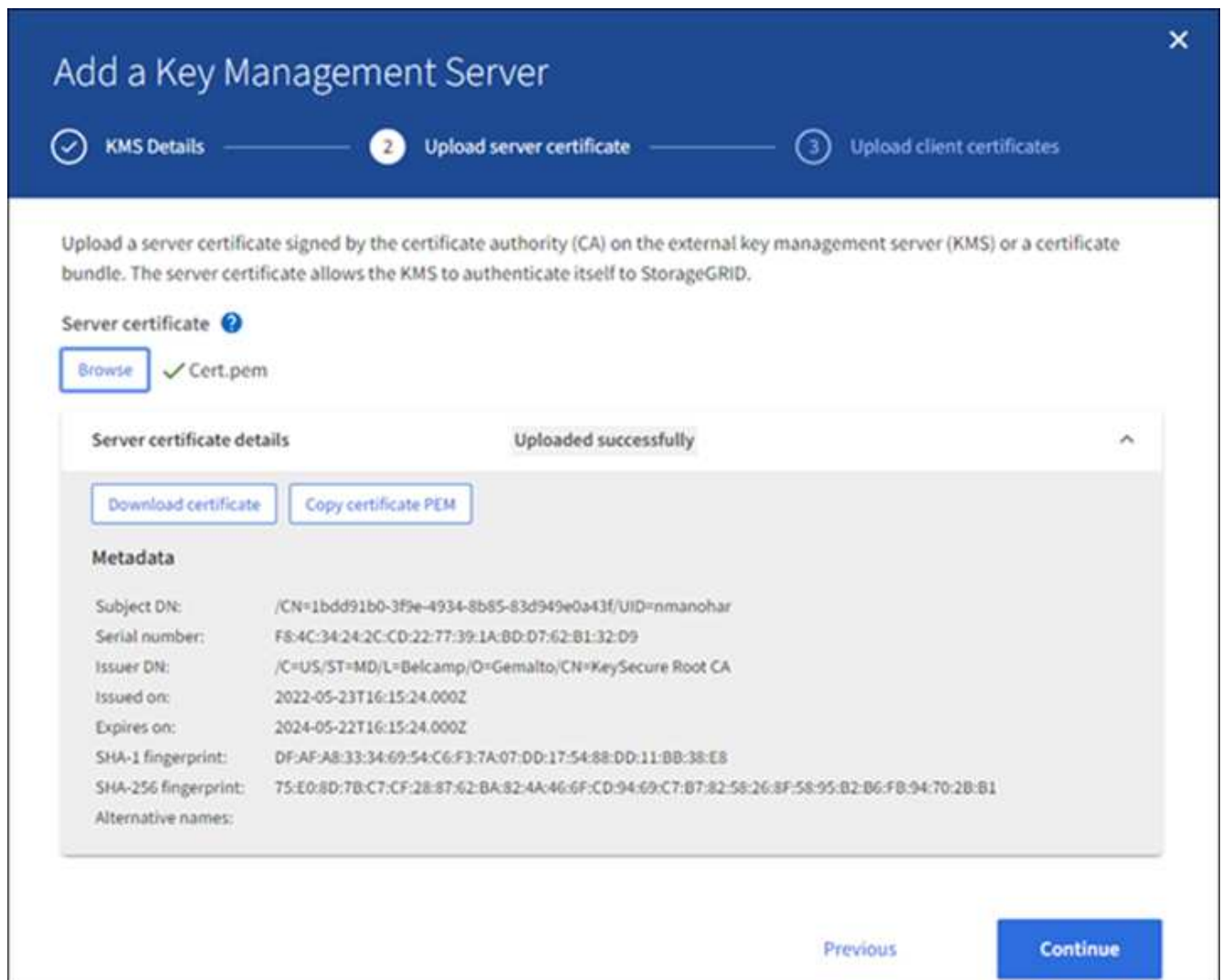
手順

1. [手順2（サーバ証明書のアップロード）]*で、保存されているサーバ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. 「* Continue *」を選択します。

手順3：クライアント証明書をアップロードします

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のアップロード）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. ステップ3（クライアント証明書のアップロード）*で、クライアント証明書の場所を参照します。

The screenshot shows a wizard window titled "Add a Key Management Server". The progress bar at the top indicates three steps: "KMS Details" (completed), "Upload server certificate" (completed), and "3 Upload client certificates" (current step). The main content area contains the following text: "Upload the client certificate and the client certificate private key. The client certificate is issued to StorageGRID by the external key management server (KMS), and it allows StorageGRID to authenticate itself to the KMS." Below this text are two sections: "Client certificate" with a "Browse" button, and "Client certificate private key" with a "Browse" button. At the bottom right, there are two buttons: "Previous" and "Test and save".

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。

5. [テストして保存]*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. 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。



[Force save]*を選択すると、KMSの構成が保存されますが、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ポ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。

KMS の詳細を確認します

StorageGRID システム内の各キー管理サーバ（KMS）に関する情報を確認することができます。これには、サーバ証明書とクライアント証明書の現在のステータスも含まれます。

手順

1. 設定 * > * セキュリティ * > * キー管理サーバ * を選択します。

[Key management server]ページが表示されます。[設定の詳細]タブには、設定済みのキー管理サーバが表示されます。

2. 各 KMS について、表の情報を確認します。

フィールド	説明
KMS名	KMS の説明的な名前。
キー名	KMS 内の StorageGRID クライアントのキーエイリアス。
のキーを管理します	KMS に関連付けられている StorageGRID サイト。 このフィールドには、特定の StorageGRID サイトの名前、または別の KMS（デフォルト KMS）で管理されていないサイト * が表示されます
ホスト名	KMS の完全修飾ドメイン名または IP アドレス。 2 台のキー管理サーバからなるクラスタがある場合は、両方のサーバの完全修飾ドメイン名または IP アドレスが表示されます。クラスタに複数のキー管理サーバがある場合は、最初の KMS の完全修飾ドメイン名または IP アドレスと、クラスタ内の追加のキー管理サーバの数が表示されます。 例： 10.10.10.10 and 10.10.10.11 または 10.10.10.10 and 2 others。 クラスタ内のすべてのホスト名を表示するには、KMSを開き、[編集]*または[アクション]>[編集]*を選択します。

フィールド	説明
証明書の有効期限	<p>サーバ証明書、オプションの CA 証明書、およびクライアント証明書の現在の状態：有効、期限が切れている、期限が近づいている、または不明。</p> <p>*注：*証明書の有効期限の更新を取得するには、StorageGRID が30分ほどかかる場合があります。現在の値を表示するには、Web ブラウザの表示を更新する必要があります。</p>

- 証明書の有効期限が不明な場合は、30分ほど待ってからWebブラウザをリフレッシュしてください。



KMSを追加した直後に、[Key Management Server]ページに証明書の有効期限が[Unknown]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。実際のステータスを確認するには、Web ブラウザの表示を更新する必要があります。

- [証明書の有効期限]列に証明書の有効期限が切れているか、有効期限が近づいていることが示されている場合は、できるだけ早く問題に対処してください。

「* kms CA certificate expiration 」、 「 kms client certificate expiration 」、 「 kms server certificate expiration *」 の各アラートがトリガーされたら、各アラートの概要 をメモして推奨される対処方法を実行します。



データアクセスを維持するために、証明書の問題はできるだけ早く対処する必要があります。

- このKMSの証明書の詳細を表示するには、表からKMS名を選択します。
- KMSの概要ページで、サーバ証明書とクライアント証明書の両方のメタデータと証明書のPEMを確認します。必要に応じて、*[証明書の編集]*を選択して証明書を新しい証明書に置き換えます。

暗号化されたノードを表示する

StorageGRID システムでノード暗号化 * 設定が有効になっているアプライアンスノードに関する情報を表示できます。

手順

- 設定 * > * セキュリティ * > * キー管理サーバ * を選択します。

[Key Management Server] ページが表示されます。Configuration Details タブには、設定済みのすべてのキー管理サーバが表示されます。

- ページの上部で、*[暗号化されたノード]*タブを選択します。

[Encrypted nodes]タブには、*[Node Encryption]*設定が有効になっているStorageGRID システム内のアプライアンスノードが表示されます。

- 各アプライアンスノードについて、表の情報を確認します。

列 (Column)	説明
ノード名	アプライアンスノードの名前。
ノードタイプ	ノードのタイプ。 Storage 、 Admin 、 または Gateway 。
サイト	ノードがインストールされている StorageGRID サイトの名前。
KMS名	ノードに使用される KMS の説明的な名前。 KMSがリストされていない場合は、[Configuration details]タブを選択してKMSを追加します。 "キー管理サーバ (KMS) を追加する"
キー UID	アプライアンスノードでデータの暗号化と復号化に使用する暗号化キーの一意的 ID 。 キーUID全体を表示するには、セルの上にカーソルを置きます。 ダッシュ (--) は、キー UID が不明であることを示します。アプライアンスノードと KMS 間の接続問題 が原因である可能性があります。
ステータス	KMS とアプライアンスノード間の接続のステータス。 ノードが接続されている場合は、タイムスタンプが 30 分ごとに更新されます。 KMS の設定変更後に接続ステータスが更新されるまで数分かかることがあります。 • 注： *新しい値を表示するには、 Web ブラウザを更新する必要があります。

4. ステータス列に KMS 問題 と表示されている場合は、問題 にすぐに対処してください。

通常の KMS 操作中、ステータスは * KMS * に接続されます。ノードがグリッドから切断されると、ノードの接続状態が (意図的に停止しているか不明である) と表示されます。

その他のステータスメッセージは、同じ名前の StorageGRID アラートに対応します。

- KMS の設定をロードできませんでした
- KMS 接続エラー
- KMS 暗号化キー名が見つかりません
- KMS 暗号化キーのローテーションに失敗しました
- KMS キーでアプライアンスボリュームを復号化できませんでした
- KMS は設定されていません

これらのアラートに対して推奨される対処方法を実行します。



問題が発生した場合は、データを完全に保護するために、すぐに対処する必要があります。

キー管理サーバ（KMS）を編集する

証明書の有効期限が近づいている場合など、キー管理サーバの設定の編集が必要になることがあります。

作業を開始する前に

- を確認しておきます ["キー管理サーバを使用する際の考慮事項と要件"](#)。
- KMS 用に選択したサイトを更新する予定がある場合は、を確認してください ["サイトの KMS を変更する際の考慮事項"](#)。
- 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"](#)。
- Root アクセス権限が割り当てられている。

手順

1. 設定 * > * セキュリティ * > * キー管理サーバ * を選択します。


[Key management server]ページが表示され、設定済みのすべてのキー管理サーバが表示されます。

2. 編集するKMSを選択し、[アクション]>[編集]*を選択します。

テーブルでKMS名を選択し、KMS詳細ページで*編集*を選択して、KMSを編集することもできます。

3. 必要に応じて、キー管理サーバの編集ウィザードの*ステップ1（KMSの詳細）*で詳細を更新します。

フィールド	説明
KMS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。

フィールド	説明
キー名	<p>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。</p> <p>キー名の編集が必要になることはほとんどありません。たとえば、エイリアスの名前が KMS で変更された場合や、以前のキーのすべてのバージョンが新しいエイリアスのバージョン履歴にコピーされている場合は、キー名を編集する必要があります。</p> <div style="border: 1px solid gray; padding: 5px; margin: 10px 0;">  <p>KMS のキー名 (エイリアス) を変更して、キーの回転を試みないでください。代わりに、KMS ソフトウェアのキーバージョンを更新してキーをローテーションしてください。StorageGRID では、以前に使用されていたすべてのキーバージョン (および今後使用するすべてのバージョン) に、同じキーエイリアスを使用して KMS からアクセスできることが必要です。設定されている KMS のキーエイリアスを変更すると、StorageGRID がデータを復号化できなくなる可能性があります。</p> <p style="color: blue;">"キー管理サーバを使用する際の考慮事項と要件"</p> </div>
のキーを管理します	<p>サイト固有のKMSを編集していて、まだデフォルトKMSを持っていない場合は、オプションで*[別のKMSで管理されていないサイト(デフォルトKMS)]*を選択します。このオプションを選択すると、サイト固有のKMSがデフォルトのKMSに変換されます。これは、専用のKMSを持たないすべてのサイトと、拡張で追加されたすべてのサイトに適用されます。</p> <p>*注:*サイト固有のKMSを編集している場合、別のサイトを選択することはできません。デフォルトのKMSを編集している場合、特定のサイトを選択することはできません。</p>
ポート	<p>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。</p>
ホスト名	<p>KMS の完全修飾ドメイン名または IP アドレス。</p> <p>*注:*サーバ証明書のSubject Alternative Name (SAN) フィールドには、ここに入力するFQDNまたはIPアドレスが含まれている必要があります。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。</p>

4. KMSクラスタを構成する場合は、*[別のホスト名を追加]*を選択して、クラスタ内の各サーバのホスト名を追加します。
5. 「* Continue *」を選択します。

[キー管理サーバの編集]ウィザードの手順2 (サーバ証明書のアップロード) が表示されます。

6. サーバ証明書を置き換える必要がある場合は、* 参照 * を選択して新しいファイルをアップロードしま

す。

7. 「 * Continue * 」を選択します。

[Edit a Key Management Server]ウィザードの手順3（クライアント証明書のアップロード）が表示されま
す。

8. クライアント証明書とクライアント証明書の秘密鍵を置き換える必要がある場合は、 * 参照 * を選択して
新しいファイルをアップロードします。

9. [テストして保存]*を選択します。

キー管理サーバと影響を受けるサイトのすべてのノード暗号化アプライアンスノードの間の接続をテスト
します。すべてのノード接続が有効で、KMS に正しいキーがある場合は、キー管理サーバが Key
Management Server ページの表に追加されます。

10. 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、この KMS 用に選択したサイトが別の KMS によってすでに管理されている場合や、接続テスト
に失敗した場合は、「422 : Unprocessable Entity」というエラーが表示されます。

11. 接続エラーを解決する前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。



[Force save]*を選択すると、KMSの構成が保存されますが、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レポ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。

KMS の設定が保存されます。

12. 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。

キー管理サーバ（KMS）を削除する

場合によっては、キー管理サーバの削除が必要になることがあります。たとえば、サイ
トの運用を停止した場合は、サイト固有の KMS を削除できます。

作業を開始する前に

- を確認しておきます ["キー管理サーバを使用する際の考慮事項と要件"](#)。
- 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"](#)。
- Root アクセス権限が割り当てられている。

このタスクについて

KMS は以下の場合に削除できます。

- サイトの運用が停止された場合や、ノードの暗号化が有効なアプライアンスノードがサイトに含まれてい
ない場合は、サイト固有の KMS を削除できます。
- ノード暗号化が有効なアプライアンスノードがあるサイトごとにサイト固有の KMS がすでに存在する場

合は、デフォルトの KMS を削除できます。

手順

1. 設定 * > * セキュリティ * > * キー管理サーバ * を選択します。

[Key management server]ページが表示され、設定済みのすべてのキー管理サーバが表示されます。

2. 削除するKMSを選択し、【アクション】>【削除】を選択します。

テーブルでKMS名を選択し、KMS詳細ページで * Remove * を選択して、KMSを削除することもできます。

3. 次の条件に該当することを確認します。

- アプライアンスノードでノード暗号化が有効になっていないサイトのサイト固有のKMSを削除する場合。
- デフォルトのKMSを削除しようとしていますが、ノード暗号化を使用して各サイトにサイト固有のKMSがすでに存在しています。

4. 「 * はい * 」を選択します。

KMS の設定は削除されます。

著作権に関する情報

Copyright © 2024 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。