# キー管理サーバを設定

StorageGRID 11.8

NetApp
March 19, 2024

# 目次

# 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。

StorageGRIDでは、特定のキー管理サーバのみがサポートされます。サポートされている製品とバージョンのリストについては、 "ネットアップの Interoperability Matrix Tool （ IMT ）"。

### 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。

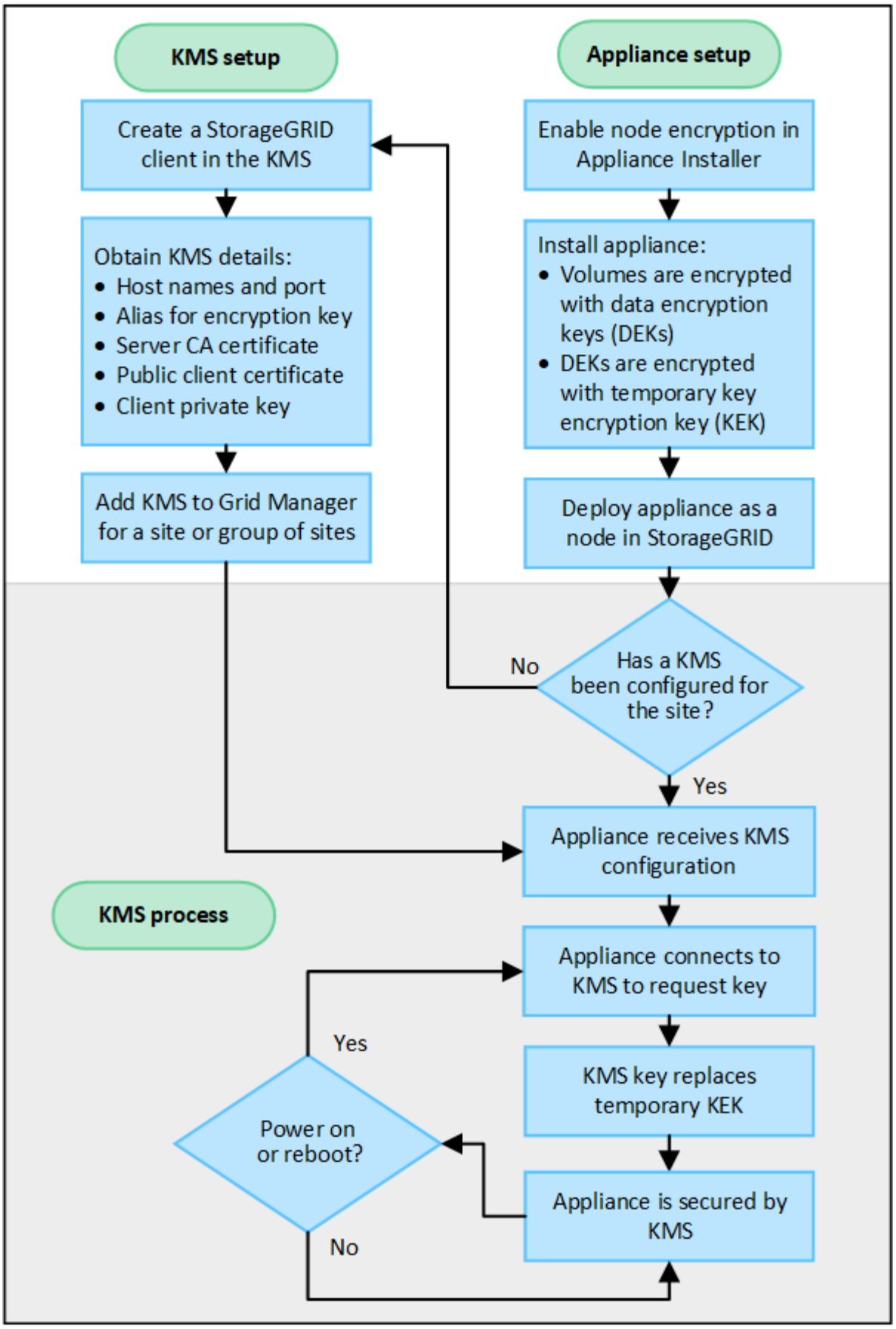
インストール時にノード暗号化 * 設定が有効になっている StorageGRID アプライアンスノードのノード暗号化キーを管理するには、 1 つ以上のキー管理サーバを使用します。これらのアプライアンスノードでキー管理サーバを使用すると、アプライアンスをデータセンターから削除した場合でも、データを保護できます。アプライアンスボリュームが暗号化されると、ノードがKMSと通信できないかぎり、アプライアンスのデータにアクセスすることはできません。

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。

## サポートされている**KMIP**のバージョンを教えてください。

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"

## ネットワークに関する考慮事項

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。

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。

## サポートされている**TLS**のバージョンを教えてください。

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、KMSまたはKMSクラスタへのKMIP接続を確立する際に、どのKMSがサポートしているかに基づいて、TLS 1.2またはTLS 1.3のいずれかのプロトコルをサポートできます。 "TLSおよびSSHポリシー" を使用しています。

StorageGRIDは、接続時にプロトコルと暗号（TLS 1.2）または暗号スイート（TLS 1.3）をKMSとネゴシエートします。使用可能なプロトコルバージョンと暗号/暗号スイートを確認するには、 `tlsOutbound` グリッドのアクティブなTLSおよびSSHポリシーのセクション（* configuration > Security * Security settings *）。

## 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。

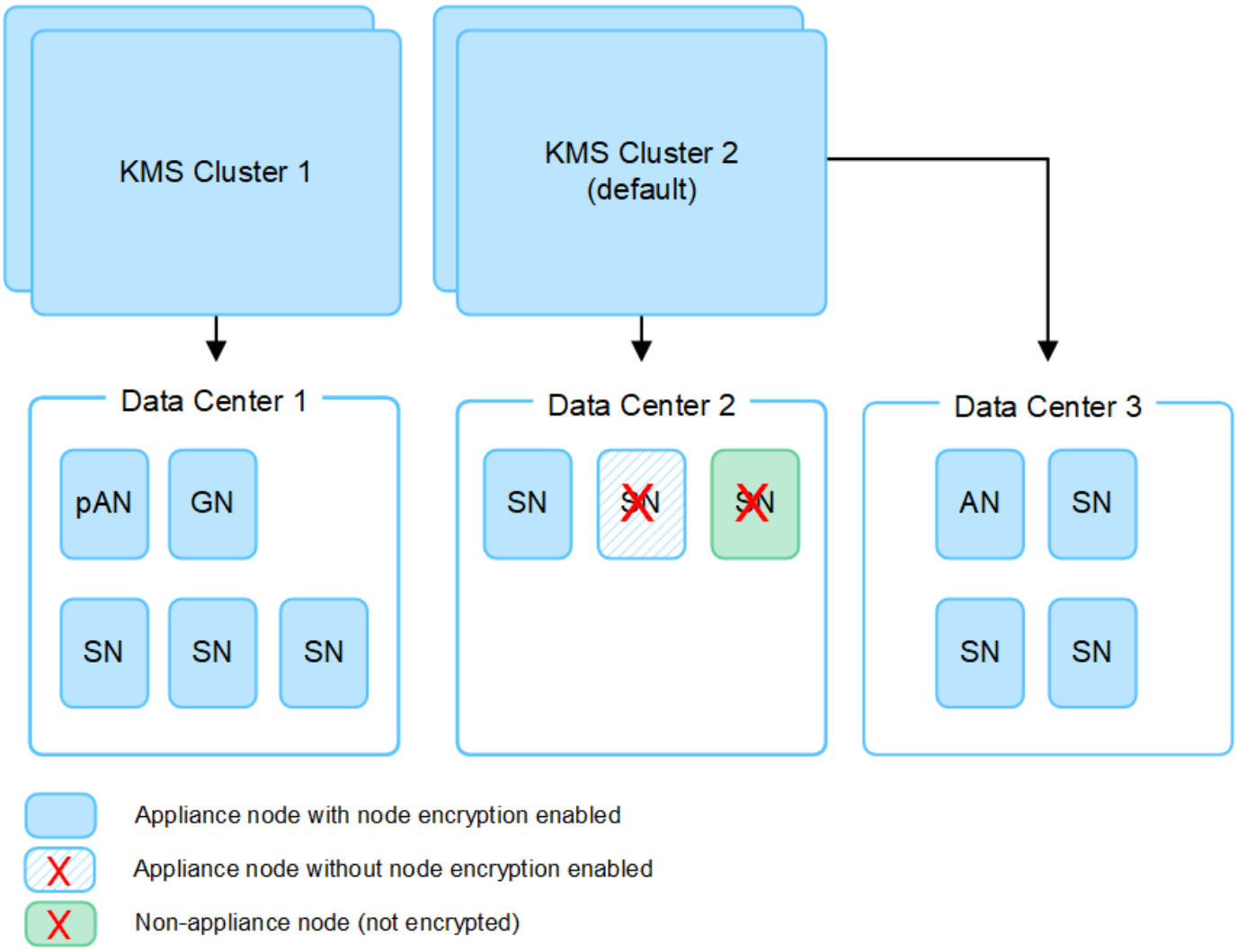
## 必要なキー管理サーバの数

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、定期的に "暗号化キーのローテーション" 設定された各KMSで使用されます。

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、ノードはリブ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を実行できます "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。

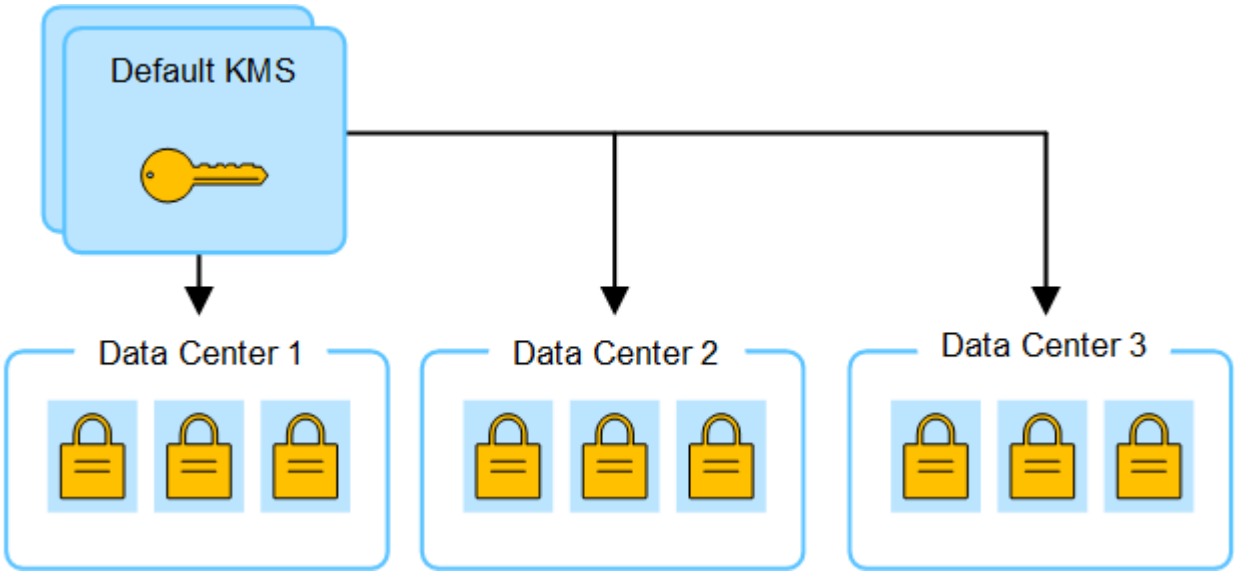
# サイトの KMS を変更する際の考慮事項

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。

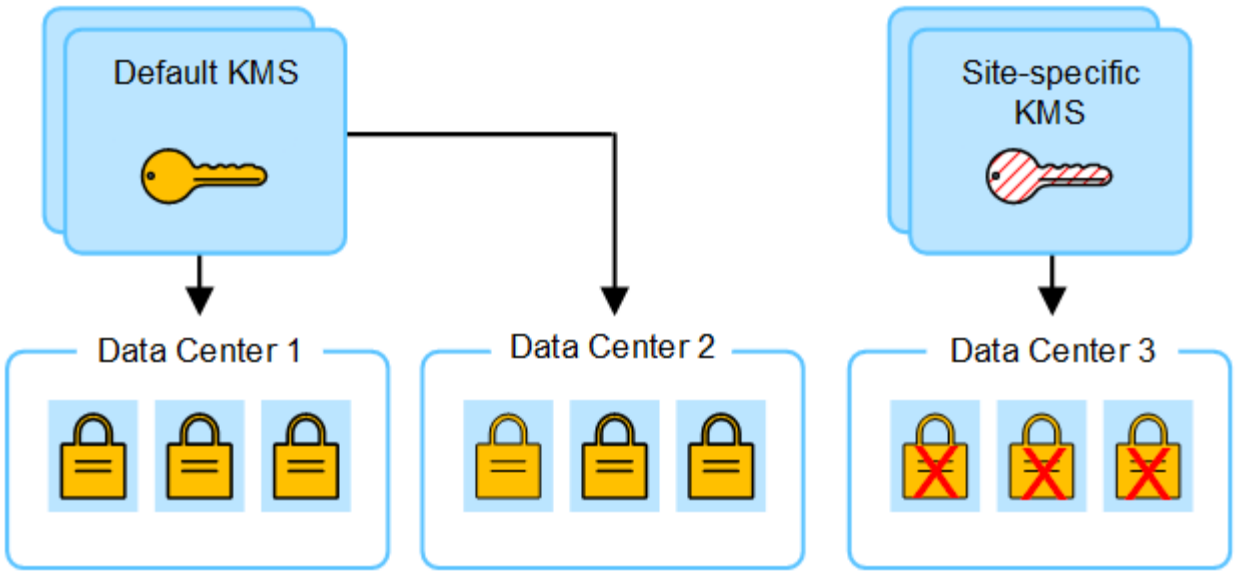
サイトで使用されている KMS を変更する場合は、そのサイトで以前に暗号化したアプライアンスノードを新しい KMS に格納されているキーを使用して復号化できることを確認する必要があります。場合によっては、暗号化キーの現在のバージョンを元の KMS から新しい KMS にコピーする必要があります。サイトで暗号化されたアプライアンスノードを復号化するために、 KMS に正しいキーがあることを確認する必要があります。

例：

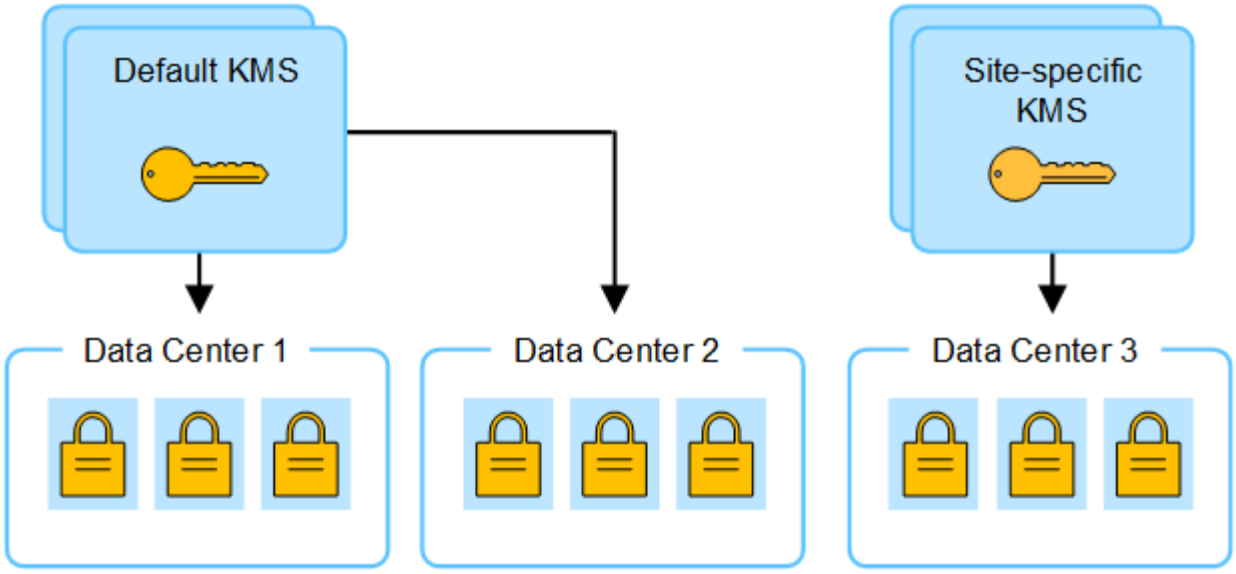
1. 最初に、専用のKMSを持たないすべてのサイトを環境 するデフォルトKMSを構成します。
2. KMS を保存すると、「 Node Encryption * 」設定が有効になっているすべてのアプライアンスノードが KMS に接続して暗号化キーを要求します。このキーは、すべてのサイトのアプライアンスノードの暗号化に使用されます。同じキーを使用して、これらのアプライアンスを復号化する必要もあります。




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と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。 | 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。<br><br>"キー管理サーバ（ KMS ）を編集する" |
| 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。 | 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。<br>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。<br><br>"キー管理サーバ（ KMS ）を追加する" |
| サイトの KMS で別のサーバを使用するとします。 | 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。<br>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。<br><br>"キー管理サーバ（ KMS ）を追加する" |

# 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。

これらの手順は、タレスCipherTrust ManagerとHashicorp Vaultに適用されます。サポートされている製品とバージョンのリストについては、 "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. 次の2つの方法のいずれかを使用してキーを作成します。

   - KMS製品のキー管理ページを使用します。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。

- StorageGRIDにキーを作成してもらいます。次の後にテストして保存すると、プロンプトが表示されます。 "クライアント証明書のアップロード"。

3. KMS または KMS クラスタごとに次の情報を記録します。

   KMSをStorageGRIDに追加するときは、次の情報が必要です。

   - 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。

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"。
- を使用することができます "rootアクセス権限"。

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。

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。

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。<br><br>注: KMS製品を使用してキーを作成していない場合は、StorageGRIDでキーを作成するように要求されます。 |
| 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。<br><br>• 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。<br>• 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。<br>◦ 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。 |

| フィールド | 説明 |
| --- | --- |
| ホスト名 | KMS の完全修飾ドメイン名または IP アドレス。<br><br>*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。 |

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:サーバー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。
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。

キーが存在しない場合は、StorageGRIDでキーを作成するように求めるメッセージが表示されます。

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。

# KMSの管理

## キー管理サーバ（KMS）の管理には、詳細の表示と編集、証明書の管理、暗号化されたノードの表示、不要になったKMSの削除が含まれます。

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"。
- を使用することができます "必要なアクセス権限"。

### KMS の詳細を確認します

キーの詳細、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など、StorageGRIDシステム内の各キー管理サーバ（KMS）に関する情報を表示できます。

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]ページに次の情報が表示されます。

   - [Configuration details]タブには、設定済みのキー管理サーバが表示されます。
   - [Encrypted nodes]タブには、ノード暗号化が有効になっているノードが表示されます。

2. 特定のKMSの詳細を表示し、そのKMSに対して操作を実行するには、KMSの名前を選択します。KMSの詳細ページには、次の情報が表示されます。

| フィールド | 説明 |
| --- | --- |
| のキーを管理します | KMS に関連付けられている StorageGRID サイト。<br><br>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。<br><br>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。<br><br>例： `10.10.10.10 and 10.10.10.11` または `10.10.10.10 and 2 others`。<br><br>クラスタ内のすべてのホスト名を表示するには、KMSを選択して*または[アクション]>[編集]*を選択します。 |

3. KMSの詳細ページでタブを選択すると、次の情報が表示されます。

| タブをクリックする | フィールド | 説明 |
| --- | --- | --- |
| 主な詳細 | キー名 | KMS 内の StorageGRID クライアントのキーエイリアス。 |
| キー UID | キーの最新バージョンの一意の識別子。 | 最終更新日 |
| キーの最新バージョンの日付と時刻。 | サーバ証明書 | メタデータ |
| 証明書のメタデータ（シリアル番号、有効期限の日時、証明書PEMなど）。 | 証明書PEM | 証明書のPEM（Privacy Enhanced Mail）ファイルの内容。 |
| クライアント証明書 | メタデータ | 証明書のメタデータ（シリアル番号、有効期限の日時、証明書PEMなど）。 |

4. 組織のセキュリティ対策で必要に応じて、*[Rotate key]*を選択するか、KMSソフトウェアを使用してキーの新しいバージョンを作成します。

   キーのローテーションが成功すると、[Key UID]フィールドと[Last modified]フィールドが更新されます。

KMSソフトウェアを使用して暗号化キーをローテーションする場合は、最後に使用したバージョンのキーから新しいバージョンの同じキー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。

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。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。

## 証明書を管理します

サーバ証明書またはクライアント証明書の問題に迅速に対処します。可能であれば、有効期限が切れる前に証明書を交換してください。

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。

手順

1. 設定 * > * セキュリティ * > * キー管理サーバ * を選択します。
2. 表で、KMSごとの証明書有効期限の値を確認します。
3. 任意のKMSの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ブラウザを更新してください。
4. [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に近づいていることが示されている場合は、KMSを選択してKMSの詳細ページに移動します。
   a. [サーバ証明書]*を選択し、[有効期限]フィールドの値を確認します。
   b. 証明書を置き換えるには、*[証明書の編集]*を選択して新しい証明書をアップロードします。
   c. これらのサブステップを繰り返し、サーバー証明書ではなく*クライアント証明書*を選択します。
5. 「* 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。

証明書の有効期限の更新がStorageGRIDで取得されるまでに30分ほどかかることがあります。現在の値を確認するには、Webブラウザをリフレッシュしてください。

## 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

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。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。

2. 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。

3. 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。<br><br>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。<br><br>"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の ID 。キーUID全体を表示するには、テキストを選択します。<br><br>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。<br><br>*注：*新しい値を表示するには、Webブラウザを更新してください。 |

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。

## KMSの編集

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

- 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"。
- を使用することができます "rootアクセス権限"。

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。 |
| 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。<br><br>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。 |
| のキーを管理します | 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。<br><br>*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。 |

| フィールド | 説明 |
| --- | --- |
| 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。<br><br>*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。 |

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. サーバー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。

    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構成は保存されますが、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"。
- を使用することができます "rootアクセス権限"。

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



## 商標に関する情報