キー管理サーバーを構成する

StorageGRID software

NetApp
December 03, 2025

目次

キー管理サーバーを構成する

キー管理サーバー (KMS) とは何ですか?

キー管理サーバー (KMS) は、キー管理相互運用性プロトコル (KMIP) を使用して、関連付けられたStorageGRIDサイトのStorageGRIDアプライアンス ノードに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。

StorageGRID は特定のキー管理サーバーのみをサポートします。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、 "NetApp Interoperability Matrix Tool（IMT）" 。

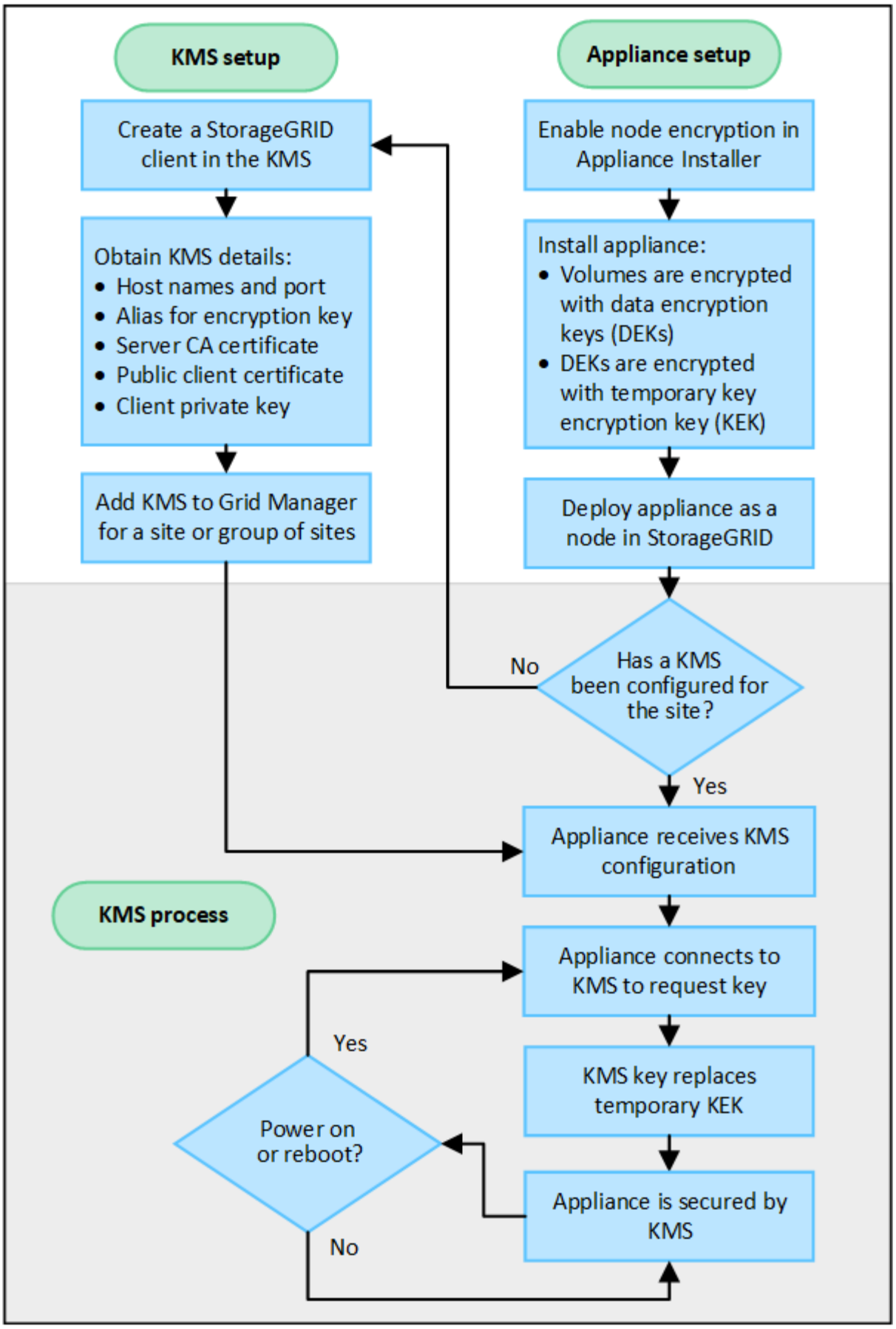
インストール中に ノード暗号化 設定が有効になっているStorageGRIDアプライアンス ノードのノード暗号化キーを管理するには、1 つ以上のキー管理サーバーを使用できます。これらのアプライアンス ノードでキー管理サーバーを使用すると、アプライアンスがデータ センターから削除された場合でもデータを保護できます。アプライアンス ボリュームが暗号化された後は、ノードが KMS と通信できない限り、アプライアンス上のデータにアクセスできなくなります。

> StorageGRID は、アプライアンス ノードの暗号化と復号化に使用される外部キーを作成または管理しません。 StorageGRIDデータを保護するために外部のキー管理サーバを使用する予定の場合は、そのサーバの設定方法と暗号化キーの管理方法を理解している必要があります。キー管理タスクの実行は、これらの手順の範囲外です。ヘルプが必要な場合は、キー管理サーバー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構成

キー管理サーバー (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 サーバーを設定し、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 つの構成タスクを完了する必要があります。これら 2 つの構成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。

このフローチャートは、KMS を使用してアプライアンス ノード上のStorageGRIDデータを保護するための大まかな手順を示しています。



フローチャートでは、KMS セットアップとアプライアンス セットアップが並行して行われていることを示し

ています。ただし、要件に応じて、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または後に、キー管理サーバーをセットアップできます。

キー管理サーバー（KMS）をセットアップする

キー管理サーバーの設定には、次の大まかな手順が含まれます。

手順	参照
KMS ソフトウェアにアクセスし、各 KMS または KMS クラスターにStorageGRIDのクライアントを追加します。	"StorageGRIDをKMSのクライアントとして設定する"
KMS 上のStorageGRIDクライアントに必要な情報を取得します。	"StorageGRIDをKMSのクライアントとして設定する"
KMS を Grid Manager に追加し、単一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 構成を保存します。	"キー管理サーバー（KMS）を追加する"

アプライアンスのセットアップ

KMS を使用するためにアプライアンス ノードを設定するには、次の大まかな手順が含まれます。

1. アプライアンスのインストールのハードウェア構成段階で、 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された後は、*ノード暗号化*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することはできません。

2. StorageGRIDアプライアンス インストーラを実行します。インストール中に、次のようにランダム データ暗号化キー (DEK) が各アプライアンス ボリュームに割り当てられます。
   - DEK は各ボリューム上のデータを暗号化するために使用されます。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、変更できません。
   - 個々の DEK は、マスター キー暗号化キー (KEK) によって暗号化されます。初期 KEK は、アプライアンスが KMS に接続できるようになるまで DEK を暗号化する一時的なキーです。
3. アプライアンス ノードをStorageGRIDに追加します。

見る "ノード暗号化を有効にする"詳細については。

キー管理暗号化プロセス（自動的に実行）

キー管理暗号化には、自動的に実行される次の高レベルの手順が含まれます。

1. ノード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 構成が存在するかどうかを判断します。

- サイトに KMS がすでに構成されている場合、アプライアンスは KMS 構成を受け取ります。
- サイトに KMS がまだ構成されていない場合は、サイトに KMS が構成され、アプライアンスが KMS 構成を受信するまで、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続けます。

2. アプライアンスは KMS 構成を使用して KMS に接続し、暗号化キーを要求します。
3. KMS はアプライアンスに暗号化キーを送信します。 KMS からの新しいキーは一時的な KEK に置き換えられ、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 ノードが構成された KMS に接続する前に存在するすべてのデータは、一時キーで暗号化されます。ただし、一時キーが KMS 暗号化キーに置き換えられるまで、アプライアンス ボリュームはデータ センターからの削除から保護されているとは見なされません。

4. アプライアンスの電源がオンになったり再起動したりすると、KMS に再接続してキーを要求します。揮発性メモリに保存されるキーは、電源喪失や再起動により失われます。

鍵管理サーバーの使用に関する考慮事項と要件

外部キー管理サーバー (KMS) を構成する前に、考慮事項と要件を理解しておく必要があります。

サポートされている **KMIP** のバージョンは何ですか?

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

"鍵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は何ですか?

ネットワーク ファイアウォール設定では、各アプライアンス ノードがキー管理相互運用性プロトコル (KMIP) 通信に使用され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 ノードが、サイト用に構成した KMS または KMS クラスターへのネットワーク アクセス権を持っていることを確認する必要があります。

どのバージョンの **TLS** がサポートされていますか?

アプライアンス ノードと構成された KMS 間の通信には、安全な TLS 接続が使用されます。 StorageGRID は、KMSまたはKMSクラスタへのKMIP接続を行う際に、KMSがサポートするものと、"TLSおよびSSHポリシー"使用しているもの。

StorageGRID は、接続時に KMS とプロトコルと暗号 (TLS 1.2) または暗号スイート (TLS 1.3) をネゴシエートします。利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 (*[構成] > [セキュリティ] [セキュリティ設定])。

どのアプライアンスがサポートされていますか?

キー管理サーバー (KMS) を使用して、グリッド内の ノード暗号化 設定が有効になっている任意

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たアプライアンスのインストールのハードウェア構成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された後は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することはできません。

構成された KMS は、 StorageGRIDアプライアンスおよびアプライアンス ノードに使用できます。

構成された KMS は、次のようなソフトウェア ベース (アプライアンス以外) のノードには使用できません。

- 仮想マシン (VM) として展開されたノード
- Linuxホスト上のコンテナエンジン内にデプロイされたノード

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

キー管理サーバーはいつ構成すればよいですか?

新規インストールの場合、通常、テナントを作成する前に、グリッド マネージャーで 1 つ以上のキー管理サーバーを設定する必要があります。この順序により、オブジェクト データがノードに保存される前にノードが保護されることが保証されます。

アプライアンス ノードをインストールする前または後に、グリッド マネージャーでキー管理サーバーを構成できます。

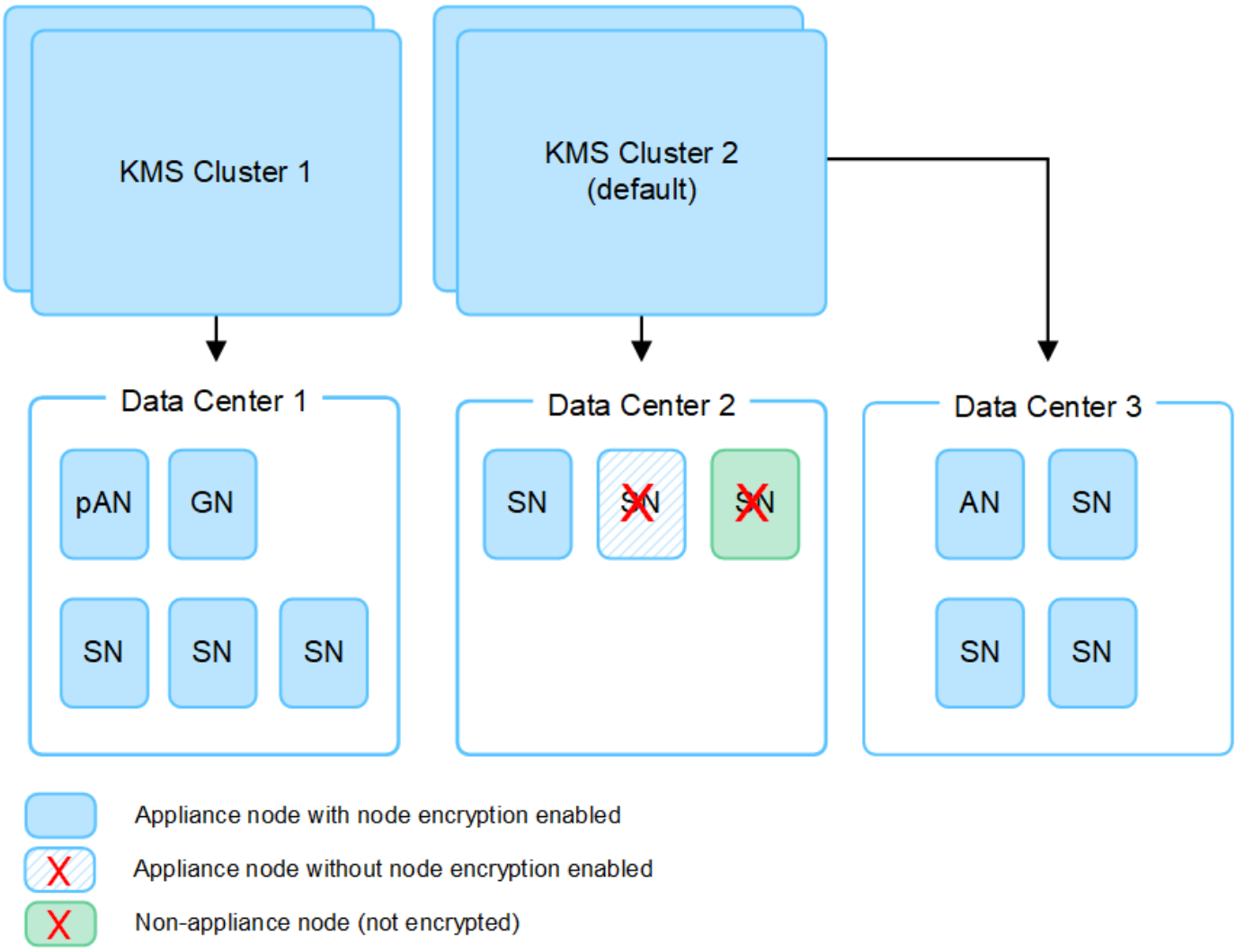
キー管理サーバーは何台必要ですか?

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するように、1 つ以上の外部キー管理サーバーを設定できます。各 KMS は、単一のサイトまたはサイト グループの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 クラスターの使用をサポートしています。各 KMS クラスターには、構成設定と暗号化キーを共有する複数の複製されたキー管理サーバーが含まれています。高可用性構成のフェイルオーバー機能が向上するため、キー管理に KMS クラスターを使用することをお勧めします。

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 クラスターを構成してデータ センター 1 のすべてのアプライアンス ノードにキーを提供し、2 つ目の KMS クラスターを構成して他のすべてのサイトのすべてのアプライアンス ノードにキーを提供するといったことが可能です。 2 番目の KMS クラスターを追加すると、データセンター 2 とデータセンター 3 のデフォルトの KMS を構成できます。

アプライアンス以外のノードや、インストール時に ノード暗号化 設定が有効になっていなかったアプライアンス ノードでは、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何が起こりますか?

セキュリティのベストプラクティスとして、定期的に"暗号化キーをローテーションする"構成された各 KMS によって使用されます。

新しいキー バージョンが利用可能になると、次のようになります。

- これは、KMS に関連付けられたサイトまたはサイト内の暗号化されたアプライアンス ノードに自動的に配布されます。配布は、キーがローテーションされてから 1 時間以内に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されたアプライアンス ノードがオフラインの場合、ノードは再起動すると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キー バージョン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** 暗号化キーのローテーションに失敗しました というアラートがトリガーされます。このアラートを解決するには、テクニカル サポートに問い合わせる必要がある場合があります。

アプライアンス ノードを暗号化した後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、まずグリッド ノードを廃止して、オブジェクト データを別のノードに移動する必要があります。その後、 StorageGRID

アプライアンスインストーラを使用して "KMS構成をクリアする"。 KMS 構成をクリアすると、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 構成間の関連付けが削除されます。

KMS 暗号化キーにアクセスできないと、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、永久にロックされます。

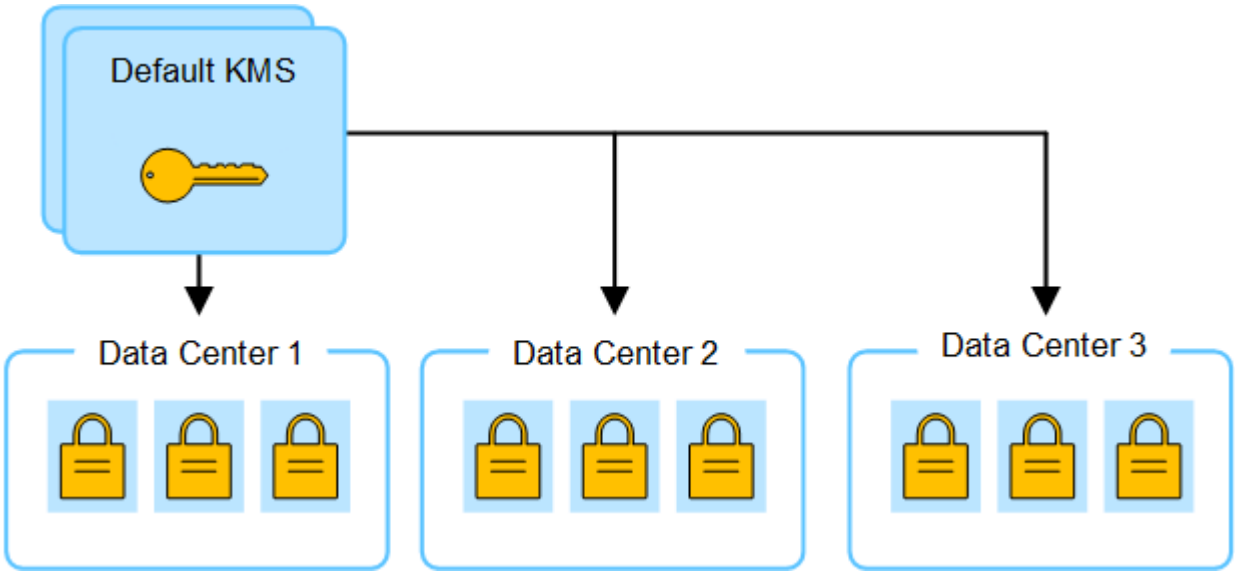
サイトのKMSを変更する際の考慮事項

各キー管理サーバー (KMS) または KMS クラスターは、単一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。サイトに使用する KMS を変更する必要がある場合は、暗号化キーをある KMS から別の KMS にコピーする必要がある場合があります。

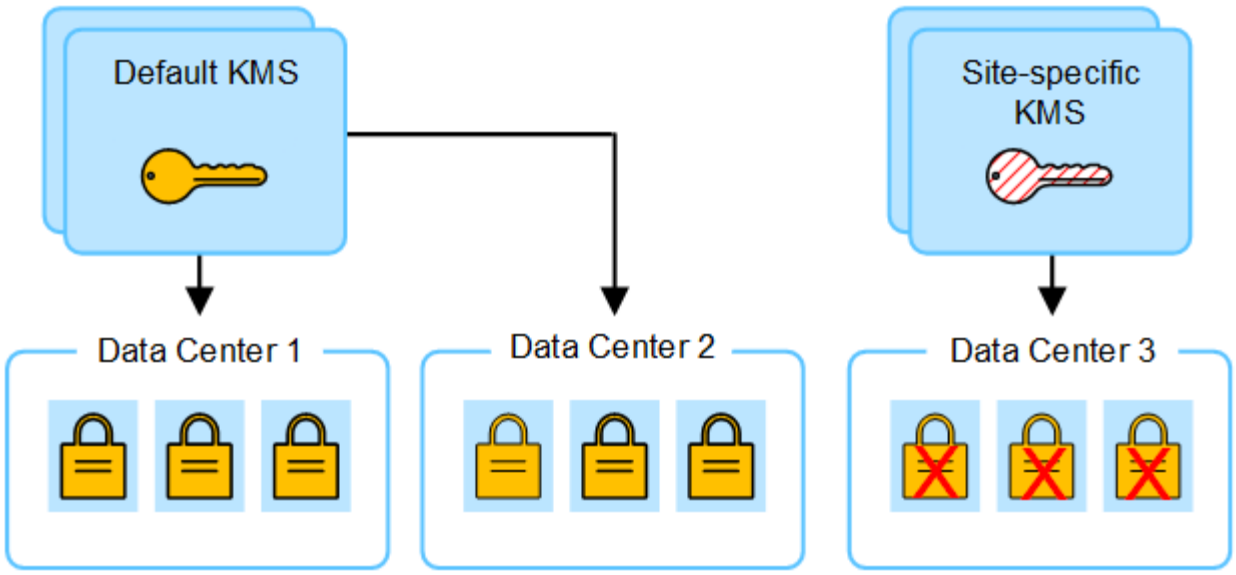
サイトに使用されている KMS を変更する場合は、そのサイトにある以前に暗号化されたアプライアンス ノードを、新しい KMS に保存されているキーを使用して復号化できることを確認する必要があります。場合によっては、現在のバージョンの暗号化キーを元の KMS から新しい KMS にコピーする必要があります。サイトの暗号化されたアプライアンス ノードを復号化するには、KMS に正しいキーがあることを確認する必要があります。

例えば：

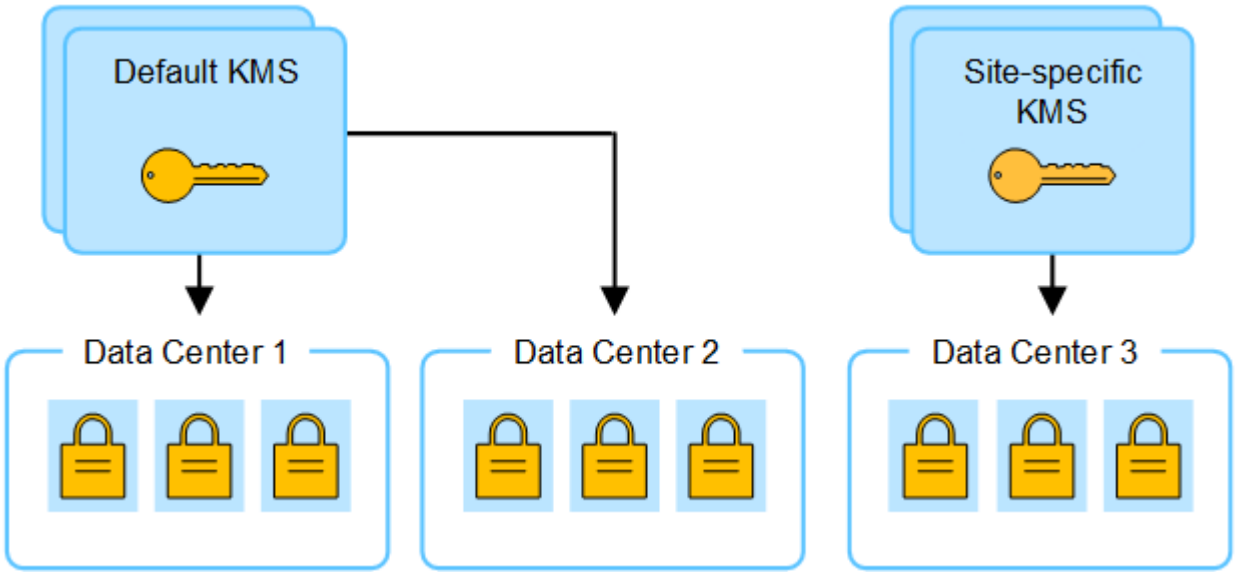
1. 最初に、専用の KMS がないすべてのサイトに適用されるデフォルトの KMS を構成します。
2. KMS が保存されると、*ノード暗号化*設定が有効になっているすべてのアプライアンス ノードが KMS に接続し、暗号化キーを要求します。このキーは、すべてのサイトのアプライアンス ノードを暗号化するために使用されます。これらのアプライアンスを復号化する場合にも、同じキーを使用する必要があります。



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 の構成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 にそのサイトのノードを復号化するための正しいキーがないため発生します。



4. この問題を解決するには、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。元のキーは新しいキーの以前のバージョンになります。サイト固有の KMS には、データセンター 3 のアプライアンス ノードを復号化するための正しいキーが含まれるようになったため、 StorageGRIDに保存できるようになりました。



サイトで使用する **KMS** を変更するユースケース

次の表は、サイトの KMS を変更する最も一般的なケースに必要な手順をまとめたものです。

サイトの **KMS** を変更するユースケース	必要な手順
1 つ以上のサイト固有の KMS エントリがあり、そのうちの 1 つをデフォルトの KMS として使用します。	サイト固有の KMS を編集します。 キーの管理対象 フィールドで、別の **KMS** によって管理されていないサイト **(**デフォルトの **KMS)** 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。これは、専用の KMS を持たないすべてのサイトに適用されます。 "キー管理サーバー（KMS）を編集する"
デフォルトの KMS があり、拡張で新しいサイトを追加します。新しいサイトではデフォルトの KMS を使用しません。	1. 新しいサイトのアプライアンス ノードがすでにデフォルトの KMS によって暗号化されている場合は、KMS ソフトウェアを使用して、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 にコピーします。 2. グリッド マネージャーを使用して、新しい KMS を追加し、サイトを選択します。 "キー管理サーバー（KMS）を追加する"
サイトの KMS で別のサーバーを使用する必要がある。	1. サイトのアプライアンス ノードが既存の KMS によって既に暗号化されている場合は、KMS ソフトウェアを使用して、暗号化キーの現在のバージョンを既存の KMS から新しい KMS にコピーします。 2. グリッド マネージャーを使用して、既存の KMS 構成を編集し、新しいホスト名または IP アドレスを入力します。 "キー管理サーバー（KMS）を追加する"

StorageGRIDをKMSのクライアントとして設定する

KMS をStorageGRIDに追加するには、まず各外部キー管理サーバーまたは KMS クラスターのクライアントとしてStorageGRID を構成する必要があります。

これらの手順は、Thales CipherTrust Manager および 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、 "NetApp Interoperability Matrix Tool（IMT）" 。

手順

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

   各 KMS は、単一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。各 KMS または KMS クラスターに対して 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にキーを作成させます。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. 各 KMS または KMS クラスターについて次の情報を記録します。

   KMS をStorageGRIDに追加するときに、次の情報が必要になります。

   - 各サーバーのホスト名または 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. 各 KMS または KMS クラスターごとに、証明機関 (CA) によって署名されたサーバー証明書、または証明書チェーンの順序で連結された各 PEM エンコードされた CA 証明書ファイルを含む証明書バンドルを取得します。

   サーバー証明書により、外部 KMS はStorageGRIDに対して自身を認証できるようになります。

   - 証明書には、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。
   - 各サーバー証明書のサブジェクト別名 (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 アドレスが含まれている必要があります。

     StorageGRIDで KMS を構成する場合は、ホスト名 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。

   - サーバー証明書は、通常ポート 5696 を使用する KMS の KMIP インターフェイスで使用される証明書と一致する必要があります。

5. 外部 KMS によってStorageGRIDに発行された公開クライアント証明書と、クライアント証明書の秘密キーを取得します。

   クライアント証明書により、 StorageGRID はKMS に対して自身を認証できるようになります。

キー管理サーバー（KMS）を追加する

各 KMS または KMS クラスターを追加するには、 StorageGRIDキー管理サーバ ウィザードを使用します。

開始する前に

- あなたは、"キー管理サーバーの使用に関する考慮事項と要件" 。
- あなたが持っている"StorageGRIDをKMSのクライアントとして構成しました"各 KMS または KMS クラスターの必要な情報が得られます。
- グリッドマネージャにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは"ルートアクセス権限"。

タスク概要

可能であれば、別の KMS によって管理されていないすべてのサイトに適用されるデフォルトの KMS を構成する前に、サイト固有のキー管理サーバーを構成します。最初にデフォルトの KMS を作成すると、グリッド内のすべてのノード暗号化アプライアンスがデフォルトの KMS によって暗号化されます。後でサイト固有の KMS を作成する場合、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。見る"サイトのKMSを変更する際の考慮事項"詳細については。

ステップ1: KMSの詳細

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

手順

1. 構成 > セキュリティ > *キー管理サーバー*を選択します。

   構成の詳細タブが選択された状態で、キー管理サーバー ページが表示されます。

2. *作成*を選択します。

   キー管理サーバーの追加ウィザードのステップ 1 (KMS の詳細) が表示されます。

3. KMS と、その KMS で構成したStorageGRIDクライアントについて、次の情報を入力します。

フィールド	説明
KMS name	この KMS を識別するのに役立つ説明的な名前。 1 ～ 64 文字にする必要があります。
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 文字にする必要があります。 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求められます。
キーを管理します	この KMS に関連付けられるStorageGRIDサイト。可能であれば、別の KMS によって管理されていないすべてのサイトに適用されるデフォルトの KMS を構成する前に、サイト固有のキー管理サーバーを構成する必要があります。 • この KMS が特定のサイトのアプライアンス ノードの暗号化キーを管理する場合は、サイトを選択します。 • 専用の KMS を持たないサイトと、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の KMS を構成するには、[別の KMS によって管理されていないサイト (デフォルトの KMS)] を選択します。 注意: 以前にデフォルトの KMS によって暗号化されたサイトを選択し、元の暗号化キーの現在のバージョンを新しい KMS に提供しなかった場合、KMS 構成を保存するときに検証エラーが発生します。

フィールド	説明
ポート	KMS サーバーがキー管理相互運用性プロトコル (KMIP) 通信に使用するポート。デフォルトは KMIP 標準ポートである 5696 です。
ホスト名	KMS の完全修飾ドメイン名または IP アドレス。 注: サーバー証明書のサブジェクト別名 (SAN) フィールドには、ここで入力する 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 または KMS クラスター内のすべてのサーバーに接続できなくなります。

4. KMS クラスターを構成する場合は、「別のホスト名を追加」を選択して、クラスター内の各サーバーのホスト名を追加します。
5. *続行*を選択します。

ステップ2: サーバー証明書をアップロードする

キー管理サーバーの追加ウィザードの手順 2 (サーバー証明書のアップロード) では、KMS のサーバー証明書 (または証明書バンドル) をアップロードします。サーバー証明書により、外部 KMS はStorageGRIDに対して自身を認証できるようになります。

手順

1. ステップ **2 (**サーバー証明書のアップロード**)** から、保存された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。

   サーバー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、各証明書のメタデータがそれぞれのタブに表示されます。

3. *続行*を選択します。

ステップ3: クライアント証明書をアップロードする

キー管理サーバー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) では、クライアント証明書とクライアント証明書の秘密キーをアップロードします。クライアント証明書により、 StorageGRID はKMS に対して自身を認証できるようになります。

手順

1. ステップ **3 (**クライアント証明書のアップロード**)** 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キー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にキーを作成するように要求されます。

   キー管理サーバーとアプライアンス ノード間の接続がテストされます。すべての接続が有効で、正しいキーが KMS に見つかった場合、新しいキー管理サーバーが [キー管理サーバー] ページのテーブルに追加されます。

   > KMS を追加するとすぐに、[キー管理サーバー] ページの証明書のステータスが [不明] と表示されます。 StorageGRID が各証明書の実際のステータスを取得するには、最大 30 分かかる場合があります。現在のステータスを確認するには、Web ブラウザを更新する必要があります。

6. テストして保存 を選択したときにエラー メッセージが表示される場合は、メッセージの詳細を確認して **OK** を選択します。

   たとえば、接続テストが失敗した場合、「422: 処理できないエンティティ」というエラーが表示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構成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 構成は保存されますが、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。構成に問題がある場合は、影響を受け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 ノードを再起動できない可能性があります。問題が解決されるまで、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、構成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。

KMSを管理する

キー管理サーバー (KMS) の管理には、詳細の表示または編集、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。

開始する前に

- グリッドマネージャにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは"必要なアクセス許可"。

KMSの詳細を表示

StorageGRIDシステム内の各キー管理サーバー (KMS) に関する情報 (キーの詳細、サーバーおよびクライアント証明書の現在のステータスなど) を表示できます。

手順

1. 構成 > セキュリティ > *キー管理サーバー*を選択します。

キー管理サーバー ページが表示され、次の情報が表示されます。

- [構成の詳細] タブには、構成されているキー管理サーバーの一覧が表示されます。
- 「暗号化されたノード」タブには、ノード暗号化が有効になっているノードが一覧表示されます。

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
キーを管理します	KMS に関連付けられた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** によって管理されていないサイト **(**デフォルトの **KMS)** 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 つのキー管理サーバーのクラスターがある場合は、両方のサーバーの完全修飾ドメイン名または IP アドレスがリストされます。クラスター内に 3 台以上のキー管理サーバーが存在する場合、最初の KMS の完全修飾ドメイン名または IP アドレスが、クラスター内の追加のキー管理サーバーの数とともに一覧表示されます。 例えば： `10.10.10.10 and 10.10.10.11`または `10.10.10.10 and 2 others`。 クラスター内のすべてのホスト名を表示するには、KMS を選択し、[編集] または [アクション] > [編集] を選択します。

3. KMS 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	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時。	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、時刻、証明書 PEM など)。	証明書PEM	証明書の PEM (プライバシー強化メール) ファイルの内容。

タブ	フィールド	説明
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、時刻、証明書 PEM など)。

4. 組織のセキュリティ慣行で必要な頻度で、「キーのローテーション」を選択するか、KMS ソフトウェアを使用して新しいバージョンのキーを作成します。

   キーのローテーションが成功すると、キー UID と最終変更日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、最後に使用したキーのバージョンから同じキーの新しいバージョンにローテーションします。まったく異なるキーに回転しないでください。

   KMS のキー名 (エイリアス) を変更してキーをローテーションしないでください。StorageGRID、以前に使用したすべてのキー バージョン (および将来のバージョン) が同じキー エイリアスを使用して KMS からアクセスできる必要があります。構成された KMS のキー エイリアスを変更すると、 StorageGRID はデータを復号化できなくなる可能性があります。

証明書の管理

サーバーまたはクライアント証明書に関する問題があれば速やかに対処してください。可能であれば、証明書の有効期限が切れる前に交換してください。

データ アクセスを維持するには、証明書の問題をできるだけ早く解決する必要があります。

手順

1. 構成 > セキュリティ > *キー管理サーバー*を選択します。
2. 表で、各 KMS の証明書の有効期限の値を確認します。
3. いずれかの KMS の証明書の有効期限が不明な場合は、最大 30 分待ってから 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、有効期限が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. *サーバー証明書*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、サーバー証明書の代わりに*クライアント証明書*を選択します。
5. **KMS CA** 証明書の有効期限、**KMS** クライアント証明書の有効期限、および **KMS** サーバー証明書の有効期限 アラートがトリガーされた場合は、各アラートの説明をメモし、推奨されるアクションを実行してください。

   StorageGRID が証明書の有効期限の更新を取得するには、最大 30 分かかる場合があります。現在の値を表示するには、Web ブラウザを更新してください。

サーバー証明書のステータスが不明 というステータスが表示される場合は、KMS でクライアント証明書を必要とせずにサーバー証明書を取得できることを確認してください。

暗号化されたノードを表示する

*ノード暗号化*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 ノードに関する情報を表示できます。

手順

1. 構成 > セキュリティ > *キー管理サーバー*を選択します。

   キー管理サーバー ページが表示されます。 [構成の詳細] タブには、構成されているキー管理サーバーが表示されます。

2. ページの上部から、[暗号化されたノード] タブを選択します。

   [暗号化されたノード] タブには、 StorageGRIDシステム内の ノード暗号化 設定が有効になっているアプライアンス ノードが一覧表示されます。

3. 各アプライアンス ノードの表の情報を確認します。

列	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: ストレージ、管理、またはゲートウェイ。
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 name	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、[構成の詳細] タブを選択して KMS を追加します。 "キー管理サーバー（KMS）を追加する"
キーUID	アプライアンス ノード上のデータの暗号化と復号化に使用され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。 ダッシュ (--) は、アプライアンス ノードと KMS 間の接続の問題が原因で、キー UID が不明であることを示します。
ステータス	KMS とアプライアンス ノード間の接続の状態。ノードが接続されている場合、タイムスタンプは 30 分ごとに更新されます。 KMS 構成の変更後、接続ステータスが更新されるまでに数分かかる場合があります。 注: 新しい値を表示するには、Web ブラウザを更新してください。

4. ステータス列に KMS の問題が示されている場合は、すぐに問題に対処してください。

通常の KMS 操作中は、ステータスは **KMS** に接続済み になります。ノードがグリッドから切断されている場合、ノードの接続状態 (管理上ダウンまたは不明) が表示されます。

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

- KMS構成の読み込みに失敗しました
- 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 キーがアプライアンス ボリュームの暗号化に失敗しました
- KMSが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アクションを実行します。

データが完全に保護されるようにするには、問題があればすぐに対処する必要があります。

KMSの編集

たとえば、証明書の有効期限が近づいている場合など、キー管理サーバーの構成を編集する必要がある場合があります。

開始する前に

- KMS用に選択したサイトを更新する予定の場合は、"サイトのKMSを変更する際の考慮事項" 。
- グリッドマネージャにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは"ルートアクセス権限"。

手順

1. 構成 > セキュリティ > *キー管理サーバー*を選択します。

   キー管理サーバー ページが表示され、構成されているすべてのキー管理サーバーが表示されます。

2. 編集する KMS を選択し、[アクション] > [編集] を選択します。

   表内の 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、キー管理サーバー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 name	この KMS を識別するのに役立つ説明的な名前。 1 ～ 64 文字にする必要があります。

フィールド	説明
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 文字にする必要があります。 キー名を編集する必要があるのは、まれなケースのみです。たとえば、KMS でエイリアスの名前が変更された場合や、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た場合は、キー名を編集する必要があります。
キーを管理します	サイト固有の KMS を編集していて、デフォルトの KMS がまだない場合は、オプションで 別の **KMS** によって管理されていないサイト **(**デフォルトの **KMS)** を選択します。これを選択すると、サイト固有の KMS がデフォルトの KMS に変換され、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。 注意**:** サイト固有の KMS を編集している場合は、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は、特定のサイトを選択することはできません。
ポート	KMS サーバーがキー管理相互運用性プロトコル (KMIP) 通信に使用するポート。デフォルトは KMIP 標準ポートである 5696 です。
ホスト名	KMS の完全修飾ドメイン名または IP アドレス。 注**:** サーバー証明書のサブジェクト別名 (SAN) フィールドには、ここで入力する 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 または KMS クラスター内のすべてのサーバーに接続できなくなります。

4. KMS クラスターを構成する場合は、「別のホスト名を追加」を選択して、クラスター内の各サーバーのホスト名を追加します。
5. *続行*を選択します。

   キー管理サーバーの編集ウィザードのステップ 2 (サーバー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. *続行*を選択します。

   キー管理サーバーの編集ウィザードのステップ 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キー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。

   影響を受けるサイトにあるキー管理サーバーとすべてのノード暗号化アプライアンス ノード間の接続がテストされます。すべてのノード接続が有効で、正しいキーが KMS 上に見つかった場合、キー管理サーバーが「キー管理サーバー」ページのテーブルに追加されます。

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 に選択したサイトが既に別の KMS によって管理されている場合、または接続テストが失敗した場合は、「422: 処理できないエンティティ」エラーが表示されることがあります。

11. 接続エラーを解決する前に現在の構成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 構成は保存されますが、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。構成に問題がある場合は、影響を受け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 ノードを再起動できない可能性があります。問題が解決されるまで、データにアクセスできなくなる可能性があります。

    KMS 構成が保存されます。

12. 確認の警告を確認し、構成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。

キー管理サーバー（KMS）を削除する

場合によっては、キー管理サーバーを削除する必要がある場合があります。たとえば、サイトを廃止した場合は、サイト固有の KMS を削除する必要がある場合があります。

開始する前に

- あなたは、"キー管理サーバーの使用に関する考慮事項と要件" 。
- グリッドマネージャにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは"ルートアクセス権限"。

タスク概要

次の場合には KMS を削除できます。

- サイトが廃止された場合、またはサイトにノード暗号化が有効になっているアプライアンス ノードが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になっているアプライアンス ノードがある各サイトにサイト固有の 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. 構成 > セキュリティ > *キー管理サーバー*を選択します。

    キー管理サーバー ページが表示され、構成されているすべてのキー管理サーバーが表示されます。

2. 削除する KMS を選択し、[アクション] > [削除] を選択します。

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

3. 次の点を確認してください。
    - ノード暗号化が有効になっているアプライアンス ノードがないサイトのサイト固有の KMS を削除しています。

- デフォルトの KMS を削除していますが、ノード暗号化が行われたサイトごとにサイト固有の KMS が既に存在しています。

4. *はい*を選択してください。

   KMS 構成が削除されます。

著作権に関する情報

商標に関する情報