# Konfigurieren von Verschlüsselungsmanagement-Servern

StorageGRID 11.5

NetApp
April 11, 2024

# Inhalt

# Konfigurieren von Verschlüsselungsmanagement-Servern

Sie können einen oder mehrere externe Verschlüsselungsmanagement-Server (KMS) konfigurieren, um die Daten auf speziell konfigurierten Appliance-Nodes zu schützen.

## Was ist ein KMS (Key Management Server)?

Ein Verschlüsselungsmanagement-Server (KMS) ist ein externes Drittanbietersystem, das mithilfe des Key Management Interoperability Protocol (KMIP) Verschlüsselungen für die StorageGRID Appliance-Nodes am zugehörigen StorageGRID Standort bereitstellt.

Sie können einen oder mehrere Schlüsselverwaltungsserver verwenden, um die Knotenverschlüsselungsschlüssel für alle StorageGRID Appliance-Knoten zu verwalten, deren **Node-Verschlüsselung**-Einstellung während der Installation aktiviert ist. Durch den Einsatz von Verschlüsselungsmanagement-Servern mit diesen Appliance-Nodes können Sie Ihre Daten selbst dann schützen, wenn eine Appliance aus dem Datacenter entfernt wird. Nachdem die Appliance-Volumes verschlüsselt sind, können Sie erst auf sämtliche Daten auf der Appliance zugreifen, wenn der Node mit dem KMS kommunizieren kann.

> StorageGRID erstellt oder verwaltet keine externen Schlüssel, die zur Verschlüsselung und Entschlüsselung von Appliance-Nodes verwendet werden. Wenn Sie Vorhaben, einen externen Verschlüsselungsmanagementserver zum Schutz von StorageGRID-Daten zu verwenden, müssen Sie wissen, wie Sie diesen Server einrichten, und wissen, wie Sie die Verschlüsselungsschlüssel managen. Die Ausführung wichtiger Managementaufgaben geht über diesen Anweisungen hinaus. Wenn Sie Hilfe benötigen, lesen Sie die Dokumentation für Ihren zentralen Managementserver, oder wenden Sie sich an den technischen Support.

## Überprüfen von StorageGRID Verschlüsselungsmethoden

StorageGRID bietet verschiedene Optionen zur Datenverschlüsselung. Anhand der verfügbaren Methoden können Sie ermitteln, welche Methoden Ihre Datensicherungsanforderungen erfüllen.

Die Tabelle bietet eine allgemeine Zusammenfassung der in StorageGRID verfügbaren Verschlüsselungsmethoden.

| Verschlüsselungsoption | So funktioniert es | Gilt für |
| --- | --- | --- |
| Verschlüsselungsmanagement-Server (KMS) in Grid Manager | Sie konfigurieren einen Schlüsselverwaltungsserver für den StorageGRID-Standort (**Konfiguration** > **Systemeinstellungen** > **Schlüsselverwaltungsserver**) und aktivieren die Knotenverschlüsselung für die Appliance. Anschließend stellt ein Appliance-Node eine Verbindung mit dem KMS her, um einen Schlüsselverschlüsselungsschlüssel (KEK) anzufordern. Dieser Schlüssel verschlüsselt und entschlüsselt den Datenverschlüsselungsschlüssel (DEK) auf jedem Volume. | Appliance-Knoten, deren **Node Encryption** während der Installation aktiviert ist. Alle Daten auf der Appliance sind gegen physischen Verlust oder aus dem Datacenter geschützt. Kann mit einigen StorageGRID Storage und Service Appliances verwendet werden. |
| Laufwerkssicherheit in SANtricity System Manager | Wenn die Laufwerkssicherheitsfunktion für eine Speicher-Appliance aktiviert ist, können Sie den Sicherheitsschlüssel mit SANtricity System Manager erstellen und verwalten. Der Schlüssel ist erforderlich, um auf die Daten auf den gesicherten Laufwerken zuzugreifen. | Storage-Applikationen mit Full Disk Encryption-Laufwerken (FDE) oder FIPS-Laufwerken (Federal Information Processing Standard) Alle Daten auf den gesicherten Laufwerken sind vor physischem Verlust oder Entfernung aus dem Datacenter geschützt. Nicht bei einigen Storage-Appliances oder Service-Appliances verwendet werden können.<br><br>"SG6000 Storage-Appliances"<br><br>"SG5700 Storage-Appliances"<br><br>"SG5600 Storage Appliances" |
| Grid-Option „gespeicherte Objektverschlüsselung“ | Die Option **gespeicherte Objektverschlüsselung** kann im Grid Manager aktiviert werden (**Konfiguration** > **Systemeinstellungen** > **Grid-Optionen**). Bei Aktivierung werden alle neuen Objekte, die nicht auf Bucket-Ebene oder auf Objektebene verschlüsselt sind, während der Aufnahme verschlüsselt. | Neu aufgenommene S3- und Swift-Objektdaten vorhandene gespeicherte Objekte werden nicht verschlüsselt. Objekt-Metadaten und andere sensible Daten sind nicht verschlüsselt.<br><br>"Konfigurieren der gespeicherten Objektverschlüsselung" |

| Verschlüsselungsoption | So funktioniert es | Gilt für |
| --- | --- | --- |
| S3-Bucket-Verschlüsselung | Sie stellen eine PUT-Bucket-Verschlüsselungsanforderung bereit, um die Verschlüsselung für den Bucket zu aktivieren. Neue Objekte, die nicht auf Objektebene verschlüsselt sind, werden bei der Aufnahme verschlüsselt. | Nur neu aufgenommene S3-Objektdaten.Verschlüsselung muss für den Bucket angegeben werden. Vorhandene Bucket-Objekte sind nicht verschlüsselt. Objekt-Metadaten und andere sensible Daten sind nicht verschlüsselt.<br><br>"S3 verwenden" |
| S3-Objektserverseitige Verschlüsselung (SSE) | Sie geben eine S3-Anforderung zum Speichern eines Objekts aus und schließen das ein `x-amz-server-side-encryption` Kopfzeile der Anfrage. | Nur neu aufgenommene S3-Objektdaten.Verschlüsselung muss für das Objekt angegeben werden. Objekt-Metadaten und andere sensible Daten sind nicht verschlüsselt.<br><br>StorageGRID verwaltet die Schlüssel.<br><br>"S3 verwenden" |
| S3 Objektserverseitige Verschlüsselung mit vom Kunden bereitgestellten Schlüsseln (SSE-C) | Sie geben eine S3-Anforderung zum Speichern eines Objekts aus und enthalten drei Anfrageheader.<br><br>• `x-amz-server-side-encryption-customer-algorithm`<br>• `x-amz-server-side-encryption-customer-key`<br>• `x-amz-server-side-encryption-customer-key-MD5` | Nur neu aufgenommene S3-Objektdaten.Verschlüsselung muss für das Objekt angegeben werden. Objekt-Metadaten und andere sensible Daten sind nicht verschlüsselt.<br><br>Schlüssel werden außerhalb von StorageGRID gemanagt.<br><br>"S3 verwenden" |
| Externe Volume- oder Datastore-Verschlüsselung | Sofern die Implementierungsplattform sie unterstützt, verwenden Sie eine Verschlüsselungsmethode außerhalb von StorageGRID, um ein gesamtes Volume oder Datastore zu verschlüsseln. | Alle Objektdaten, Metadaten und Systemkonfigurationsdaten, wobei jedes Volume oder jeder Datastore verschlüsselt ist<br><br>Eine externe Verschlüsselungsmethode bietet eine engere Kontrolle über Verschlüsselungsalgorithmen und -Schlüssel. Kann mit den anderen aufgeführten Methoden kombiniert werden. |

| Verschlüsselungsoption | So funktioniert es | Gilt für |
| --- | --- | --- |
| Objektverschlüsselung außerhalb von StorageGRID | Dabei kommt eine Verschlüsselungsmethode außerhalb von StorageGRID zum Einsatz, um Objektdaten und Metadaten zu verschlüsseln, bevor sie in StorageGRID aufgenommen werden. | Nur Objektdaten und Metadaten (Systemkonfigurationsdaten sind nicht verschlüsselt).<br><br>Eine externe Verschlüsselungsmethode bietet eine engere Kontrolle über Verschlüsselungsalgorithmen und -Schlüssel. Kann mit den anderen aufgeführten Methoden kombiniert werden.<br><br>"Amazon Simple Storage Service – Developer Guide: Schutz von Daten mit Client-seitiger Verschlüsselung" |

### Verwendung mehrerer Verschlüsselungsmethoden

Je nach Ihren Anforderungen können Sie mehrere Verschlüsselungsmethoden gleichzeitig verwenden. Beispiel:

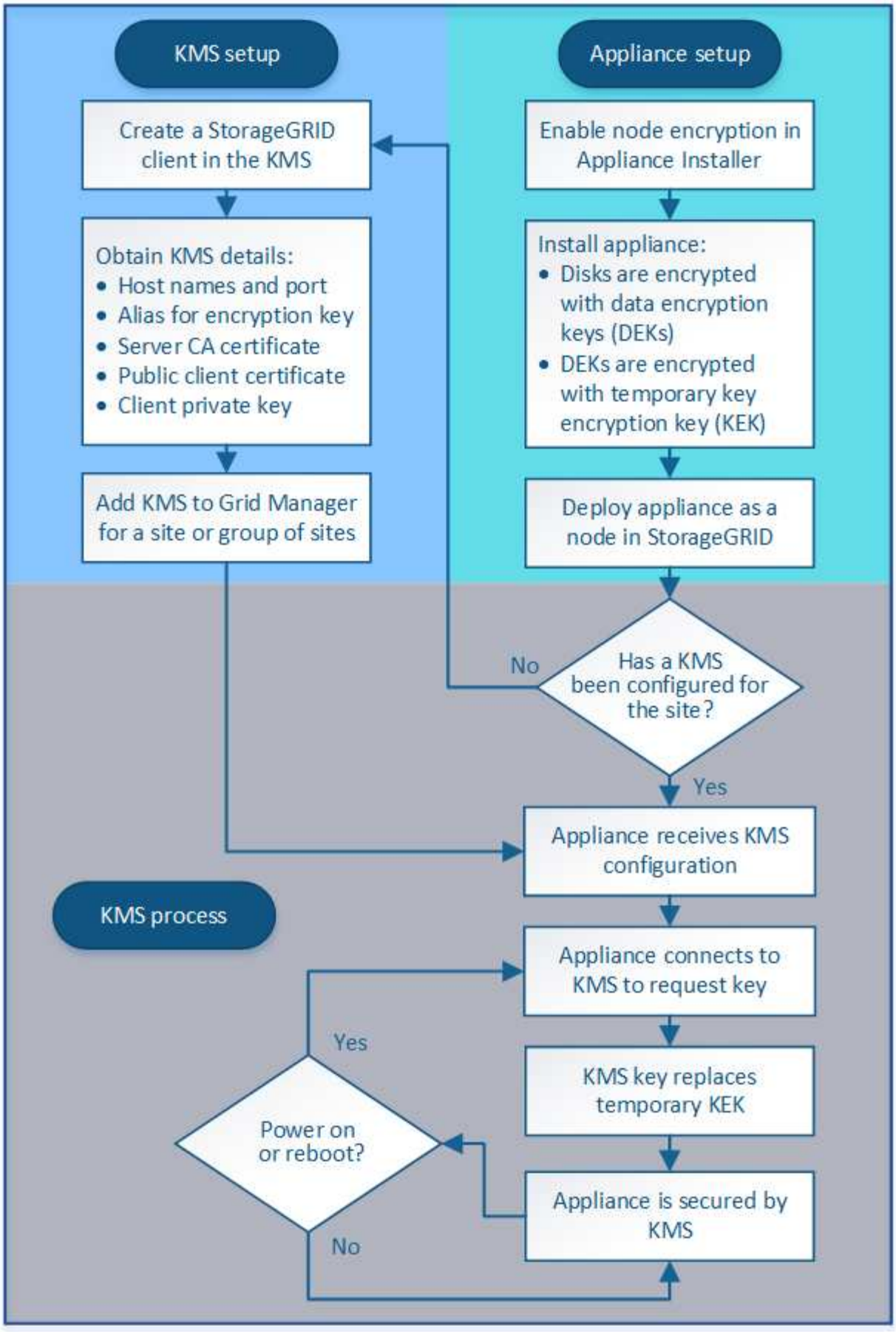
- Mit einem KMS können Appliance-Nodes geschützt werden. Außerdem kann mithilfe der Laufwerksicherheitsfunktion in SANtricity System Manager die Daten „`double verschlüsselte`“ auf den Self-Encrypting Drives in denselben Appliances verschlüsselt werden.
- Mit einem KMS lassen sich Daten auf Appliance-Nodes sichern. Zudem kann die Grid-Option „Speichered Object Encryption“ verwendet werden, um alle Objekte bei der Aufnahme zu verschlüsseln.

Wenn nur ein kleiner Teil Ihrer Objekte eine Verschlüsselung erfordern, sollten Sie stattdessen die Verschlüsselung auf Bucket- oder Objektebene kontrollieren. Durch die Aktivierung diverser Verschlüsselungsstufen entstehen zusätzliche Performance-Kosten.

# Überblick über die KMS- und Appliance-Konfiguration

Bevor der Verschlüsselungsmanagement-Server (KMS) die StorageGRID-Daten auf Appliance-Nodes sichern kann, müssen zwei Konfigurationsaufgaben durchgeführt werden: Ein oder mehrere KMS-Server einrichten und die Node-Verschlüsselung für die Appliance-Nodes aktivieren. Wenn diese beiden Konfigurationsaufgaben abgeschlossen sind, erfolgt automatisch der Verschlüsselungsmanagementprozess.

Das Flussdiagramm zeigt die grundlegenden Schritte bei der Verwendung eines KMS zur Sicherung von StorageGRID-Daten auf Appliance-Nodes.




Das Flussdiagramm zeigt die parallele Einrichtung von KMS und die Einrichtung der Appliance. Sie können

jedoch die Verschlüsselungsmanagement-Server je nach Ihren Anforderungen vor oder nach Aktivierung der Node-Verschlüsselung für neue Appliance-Nodes einrichten.

## Einrichten des Verschlüsselungsmanagement-Servers (KMS)

Die Einrichtung eines Schlüsselverwaltungsservers umfasst die folgenden grundlegenden Schritte.

| Schritt | Siehe |
|---|---|
| Greifen Sie auf die KMS-Software zu und fügen Sie jedem KMS- oder KMS-Cluster einen Client für StorageGRID hinzu. | "Konfigurieren von StorageGRID als Client im KMS" |
| Erhalten Sie die erforderlichen Informationen für den StorageGRID-Client auf dem KMS. | "Konfigurieren von StorageGRID als Client im KMS" |
| Fügen Sie den KMS dem Grid Manager hinzu, weisen Sie ihn einer einzelnen Site oder einer Standardgruppe von Standorten zu, laden Sie die erforderlichen Zertifikate hoch und speichern Sie die KMS-Konfiguration. | "Hinzufügen eines Verschlüsselungsmanagement-Servers (KMS)" |

## Einrichten des Geräts

Die Einrichtung eines Appliance-Nodes für die KMS-Nutzung umfasst die folgenden grundlegenden Schritte.

1. Verwenden Sie während der Hardware-Konfigurationsphase der Appliance-Installation das Installationsprogramm von StorageGRID Appliance, um die Einstellung **Node-Verschlüsselung** für die Appliance zu aktivieren.

   > Sie können die Einstellung **Node Encryption** nicht aktivieren, nachdem ein Gerät zum Grid hinzugefügt wurde, und Sie können keine externe Schlüsselverwaltung für Geräte verwenden, bei denen die Node-Verschlüsselung nicht aktiviert ist.

2. Führen Sie das Installationsprogramm für die StorageGRID-Appliance aus. Während der Installation wird jedem Appliance-Volume ein zufälliger Datenverschlüsselungsschlüssel (random Data Encryption Key, DEK) zugewiesen:
   - Die DEKs werden verwendet, um die Daten auf jedem Volume zu verschlüsseln. Diese Schlüssel werden mit der Linux Unified Key Setup (LUKS) Festplattenverschlüsselung im GerätebOS generiert und können nicht geändert werden.
   - Jede einzelne DEK wird durch einen Master Key Encryption Key (KEK) verschlüsselt. Bei der ersten KEK handelt es sich um einen temporären Schlüssel, der die DEKs verschlüsselt, bis das Gerät eine Verbindung mit dem KMS herstellen kann.
3. Fügen Sie den Appliance-Node StorageGRID hinzu.

Weitere Informationen finden Sie unter:

- "SG100 SG1000 Services-Appliances"
- "SG6000 Storage-Appliances"
- "SG5700 Storage-Appliances"

- "SG5600 Storage Appliances"

### Verschlüsselungsmanagementprozess (wird automatisch durchgeführt)

Die Verschlüsselung des Verschlüsselungsmanagement umfasst die folgenden grundlegenden Schritte, die automatisch durchgeführt werden.

1. Wenn Sie eine Appliance installieren, bei der die Node-Verschlüsselung im Grid aktiviert ist, bestimmt StorageGRID, ob für den Standort, der den neuen Node enthält, eine KMS-Konfiguration vorhanden ist.
   - Wenn bereits ein KMS für den Standort konfiguriert wurde, erhält die Appliance die KMS-Konfiguration.
   - Wenn ein KMS für den Standort noch nicht konfiguriert wurde, werden die Daten auf der Appliance weiterhin durch die temporäre KEK verschlüsselt, bis Sie einen KMS für den Standort konfigurieren und die Appliance die KMS-Konfiguration erhält.
2. Die Appliance verwendet die KMS-Konfiguration, um eine Verbindung zum KMS herzustellen und einen Verschlüsselungsschlüssel anzufordern.
3. Der KMS sendet einen Verschlüsselungsschlüssel an die Appliance. Der neue Schlüssel des KMS ersetzt die temporäre KEK und wird nun zur Verschlüsselung und Entschlüsselung der DEKs für die Appliance-Volumes verwendet.

   > Alle Daten, die vor der Verbindung des verschlüsselten Appliance-Nodes mit dem konfigurierten KMS vorhanden sind, werden mit einem temporären Schlüssel verschlüsselt. Die Appliance-Volumes sollten jedoch erst dann als vor Entfernung aus dem Datacenter geschützt betrachtet werden, wenn der temporäre Schlüssel durch den KMS-Schlüssel ersetzt wird.

4. Wenn die Appliance eingeschaltet oder neu gestartet wird, stellt sie eine Verbindung zum KMS her, um den Schlüssel anzufordern. Der Schlüssel, der im flüchtigen Speicher gespeichert wird, kann keinen Stromausfall oder Neustart überstehen.

# Überlegungen und Anforderungen für die Verwendung eines Verschlüsselungsmanagement-Servers

Bevor Sie einen externen KMS (Key Management Server) konfigurieren, müssen Sie die Überlegungen und Anforderungen verstehen.

### Was sind die KMIP-Anforderungen?

StorageGRID unterstützt KMIP Version 1.4.

"Spezifikation Des Key Management Interoperability Protocol Version 1.4"

Für die Kommunikation zwischen den Appliance-Nodes und dem konfigurierten KMS werden sichere TLS-Verbindungen verwendet. StorageGRID unterstützt die folgenden TLS v1.2-Chiffren für KMIP:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Sie müssen sicherstellen, dass jeder Appliance-Node, der Node-Verschlüsselung verwendet, Netzwerkzugriff auf den für den Standort konfigurierten KMS- oder KMS-Cluster hat.

Die Netzwerk-Firewall-Einstellungen müssen es jedem Appliance-Node ermöglichen, über den Port zu kommunizieren, der für KMIP-Kommunikation (Key Management Interoperability Protocol) verwendet wird. Der KMIP-Standardport ist 5696.

## Welche Appliances werden unterstützt?

Sie können einen Schlüsselverwaltungsserver (KMS) verwenden, um Verschlüsselungsschlüssel für jede StorageGRID-Appliance in Ihrem Grid zu verwalten, auf der die Einstellung **Node-Verschlüsselung** aktiviert ist. Diese Einstellung kann nur während der Hardware-Konfigurationsphase der Appliance-Installation mithilfe des StorageGRID Appliance Installer aktiviert werden.

> ⓘ Nach dem Hinzufügen einer Appliance zum Grid können Sie die Node-Verschlüsselung nicht aktivieren. Appliances, bei denen die Node-Verschlüsselung nicht aktiviert ist, können externes Verschlüsselungsmanagement nicht verwenden.

Der konfigurierte KMS kann für die folgenden StorageGRID Appliances und Appliance-Nodes verwendet werden:

| Appliance | Node-Typ |
|---|---|
| SG1000 Services-Appliance | Admin-Node oder Gateway-Node |
| SG100 Services-Appliance | Admin-Node oder Gateway-Node |
| SG6000 Storage Appliance | Storage-Node |
| SG5700 Storage-Appliance | Storage-Node |
| SG5600 Storage-Appliance | Storage-Node |

Der konfigurierte KMS kann nicht für softwarebasierte (nicht-Appliance-) Nodes verwendet werden, einschließlich folgender Elemente:

- Als Virtual Machines (VMs) implementierte Nodes
- In Docker Containern auf Linux-Hosts implementierte Nodes

Auf diesen anderen Plattformen implementierte Nodes können Verschlüsselung außerhalb von StorageGRID auf Datenspeicher- oder Festplattenebene verwenden.

## Wann sollte ich wichtige Management-Server konfigurieren?

Bei einer neuen Installation sollten Sie in der Regel einen oder mehrere Schlüsselverwaltungsserver im Grid Manager einrichten, bevor Sie Mandanten erstellen. Diese Reihenfolge stellt sicher, dass die Nodes geschützt sind, bevor Objektdaten auf ihnen gespeichert werden.

Sie können die Schlüsselverwaltungsserver im Grid Manager vor oder nach der Installation der Appliance-Knoten konfigurieren.

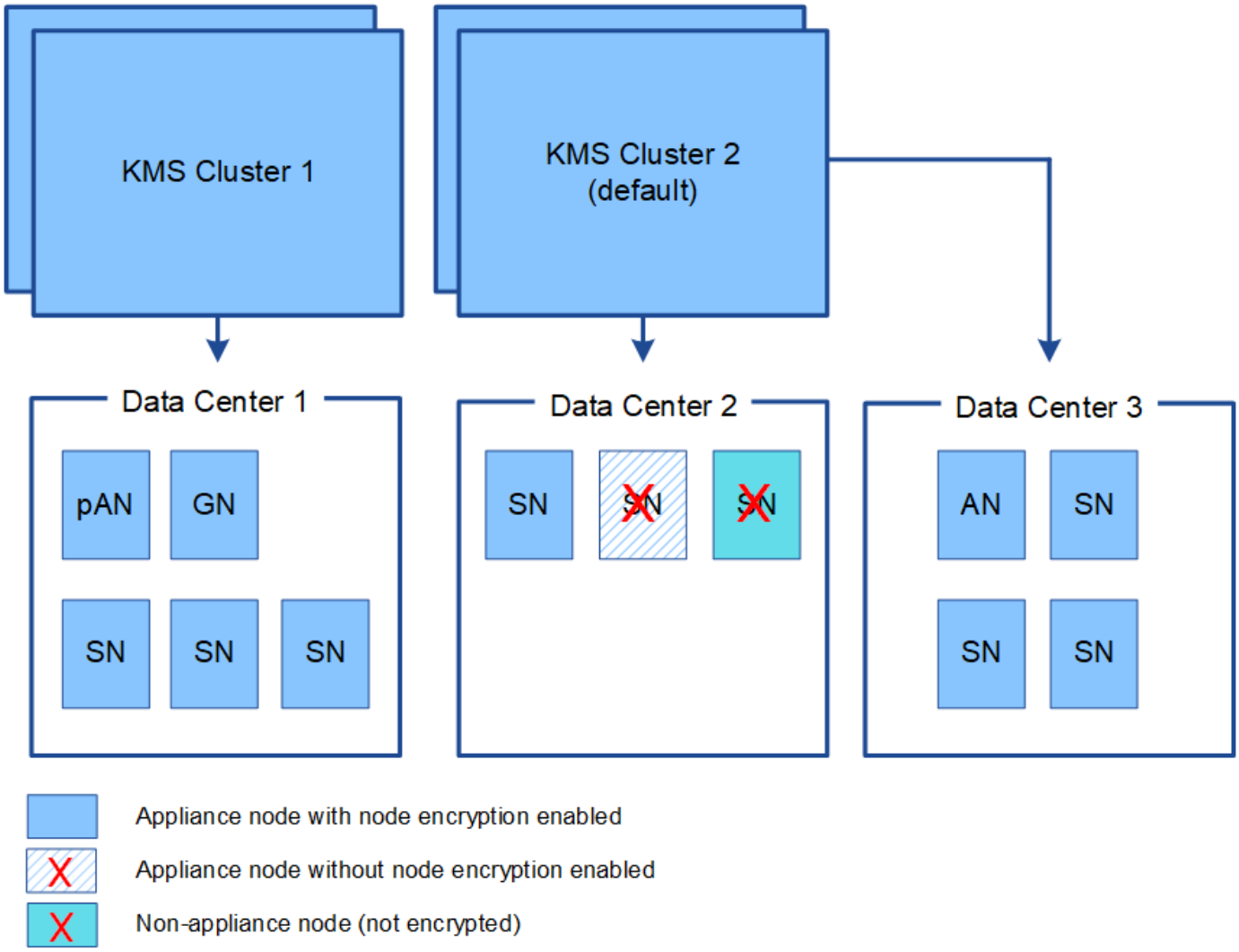
## Wie viele wichtige Management Server brauche ich?

Sie können einen oder mehrere externe Verschlüsselungsmanagementserver konfigurieren, um die Appliance-Nodes in Ihrem StorageGRID-System Verschlüsselungen bereitzustellen. Jeder KMS stellt den StorageGRID Appliance-Nodes an einem einzelnen Standort oder einer Gruppe von Standorten einen einzelnen Verschlüsselungsschlüssel zur Verfügung.

StorageGRID unterstützt die Verwendung von KMS-Clustern. Jeder KMS-Cluster enthält mehrere replizierte Verschlüsselungsmanagement-Server, die Konfigurationseinstellungen und Verschlüsselungen teilen. Die Verwendung von KMS-Clustern für das Verschlüsselungsmanagement wird empfohlen, da dadurch die Failover-Funktionen einer Hochverfügbarkeitskonfiguration verbessert werden.

Nehmen Sie beispielsweise an, Ihr StorageGRID System verfügt über drei Datacenter-Standorte. Sie können ein KMS-Cluster konfigurieren, um allen Appliance-Nodes in Datacenter 1 und einem zweiten KMS-Cluster einen Schlüssel für alle Appliance-Nodes an allen anderen Standorten bereitzustellen. Wenn Sie den zweiten KMS-Cluster hinzufügen, können Sie einen Standard-KMS für Datacenter 2 und Datacenter 3 konfigurieren.

Beachten Sie, dass Sie keinen KMS für nicht-Appliance-Knoten oder für Appliance-Knoten verwenden können, bei denen die **Node Encryption**-Einstellung während der Installation nicht aktiviert war.



### Was passiert, wenn eine Taste gedreht wird?

Als bewährte Sicherheitsmethode sollten Sie den Verschlüsselungsschlüssel, der von jedem konfigurierten KMS verwendet wird, regelmäßig drehen.

Wenn Sie den Verschlüsselungsschlüssel drehen, verwenden Sie die KMS-Software, um von der letzten verwendeten Version des Schlüssels auf eine neue Version desselben Schlüssels zu drehen. Drehen Sie nicht auf einen ganz anderen Schlüssel.

> Versuchen Sie niemals, einen Schlüssel zu drehen, indem Sie den Schlüsselnamen (Alias) für den KMS im Grid Manager ändern. Drehen Sie stattdessen den Schlüssel, indem Sie die Schlüsselversion in der KMS-Software aktualisieren. Verwenden Sie denselben Schlüssel-Alias für neue Schlüssel, wie sie für vorherige Schlüssel verwendet wurden. Wenn Sie den Schlüssel-Alias für einen konfigurierten KMS ändern, kann StorageGRID Ihre Daten möglicherweise nicht entschlüsseln.

Wenn die neue Schlüsselversion verfügbar ist:

- Die Appliance wird automatisch auf die verschlüsselten Appliance-Nodes am Standort oder an den dem KMS zugeordneten Standorten verteilt. Die Verteilung sollte innerhalb einer Stunde erfolgen, wenn der Schlüssel gedreht wird.
- Wenn der Node der verschlüsselten Appliance offline ist, wenn die neue Schlüsselversion verteilt ist, erhält der Node den neuen Schlüssel, sobald er neu gebootet wird.
- Wenn die neue Schlüsselversion nicht zur Verschlüsselung von Appliance-Volumes aus irgendeinem Grund verwendet werden kann, wird für den Appliance-Node die Warnung **KMS-Verschlüsselungsschlüsseldrehung fehlgeschlagen** ausgelöst. Möglicherweise müssen Sie sich an den technischen Support wenden, um Hilfe bei der Lösung dieses Alarms zu erhalten.

### Kann ich einen Appliance-Knoten nach der Verschlüsselung wiederverwenden?

Wenn Sie eine verschlüsselte Appliance in einem anderen StorageGRID System installieren müssen, müssen Sie zuerst den Grid-Node außer Betrieb nehmen, um Objektdaten auf einen anderen Node zu verschieben. Anschließend können Sie die KMS-Konfiguration mit dem Installationsprogramm der StorageGRID-Appliance löschen. Durch das Löschen der KMS-Konfiguration wird die **Node Encryption**-Einstellung deaktiviert und die Zuordnung zwischen dem Appliance-Knoten und der KMS-Konfiguration für den StorageGRID-Standort wird aufgehoben.

> Der Zugriff auf den KMS-Verschlüsselungsschlüssel ist ausgeschlossen, dass alle Daten, die auf der Appliance verbleiben, nicht mehr zugänglich sind und dauerhaft gesperrt werden.

"SG100 SG1000 Services-Appliances"

"SG6000 Storage-Appliances"

"SG5700 Storage-Appliances"

"SG5600 Storage Appliances"

# Überlegungen für das Ändern des KMS für einen Standort

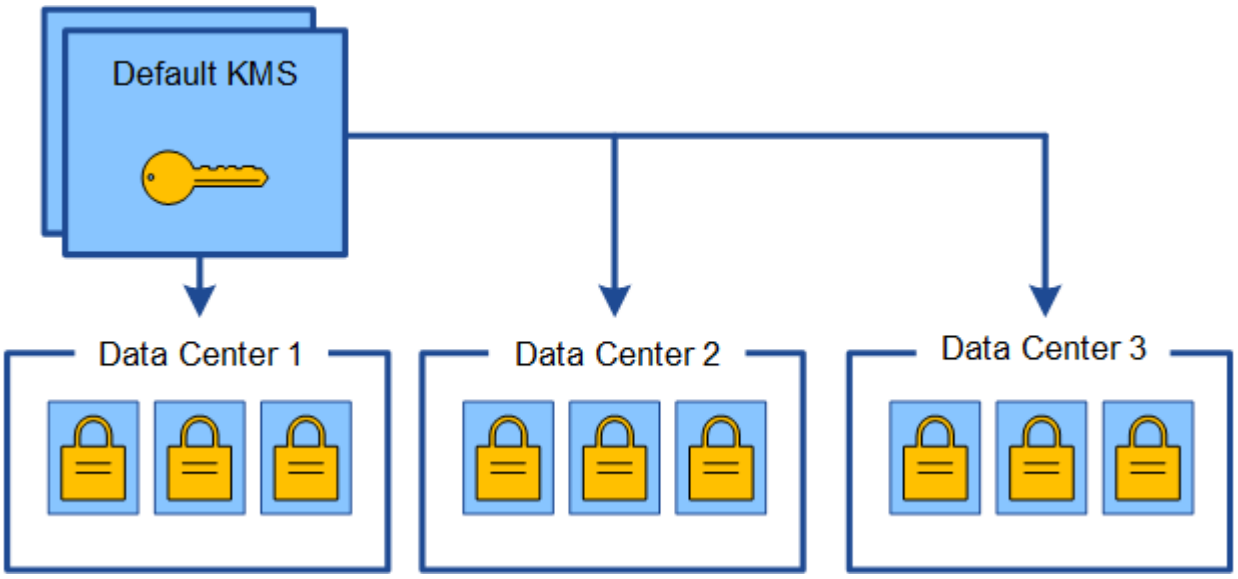
Jeder Verschlüsselungsmanagement-Server (KMS) oder KMS-Cluster gewährt allen Appliance-Nodes an einem einzelnen Standort oder einer Gruppe von Standorten einen

## Verschlüsselungsschlüssel. Wenn Sie ändern müssen, welcher KMS für einen Standort verwendet wird, müssen Sie den Verschlüsselungsschlüssel möglicherweise von einem KMS auf einen anderen kopieren.

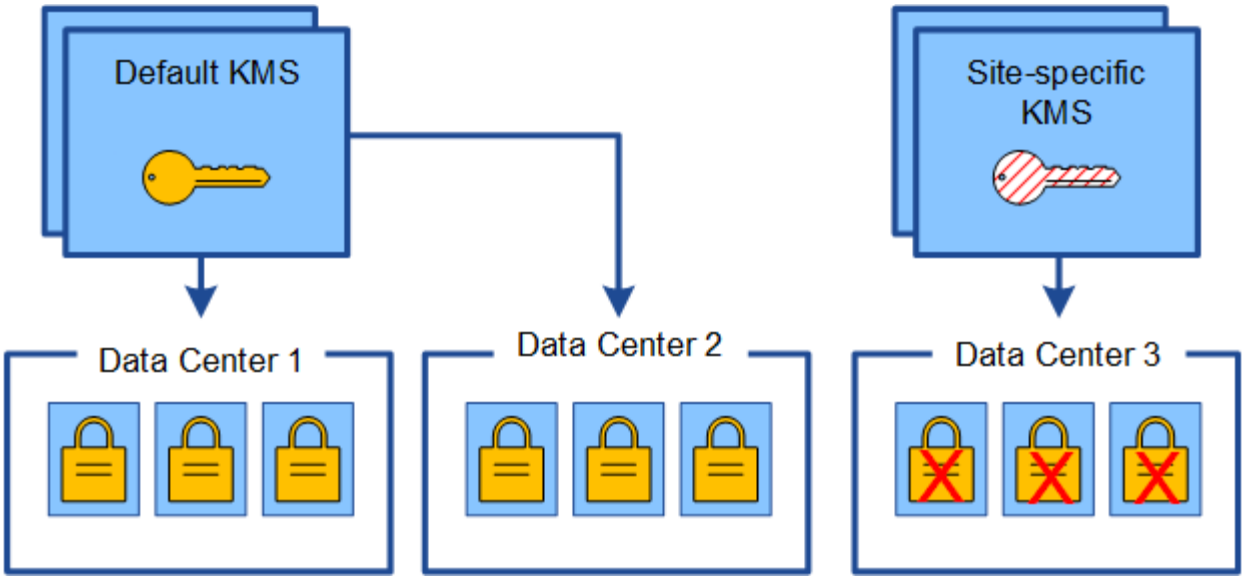
Wenn Sie den KMS ändern, der für einen Standort verwendet wird, müssen Sie sicherstellen, dass die zuvor verschlüsselten Appliance-Nodes an diesem Standort mit dem auf dem neuen KMS gespeicherten Schlüssel entschlüsselt werden können. In einigen Fällen müssen Sie möglicherweise die aktuelle Version des Verschlüsselungsschlüssels vom ursprünglichen KMS auf den neuen KMS kopieren. Sie müssen sicherstellen, dass der KMS über den richtigen Schlüssel verfügt, um die verschlüsselten Appliance-Nodes am Standort zu entschlüsseln.

Beispiel:

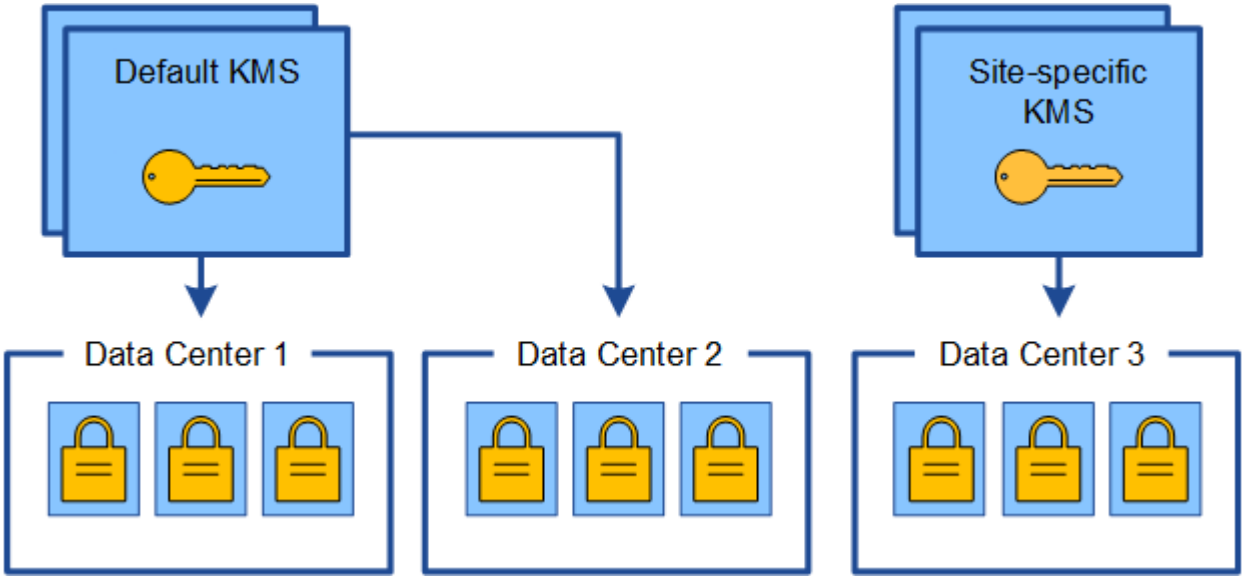
1. Sie konfigurieren zunächst einen Standard-KMS, der für alle Standorte gilt, die keinen dedizierten KMS besitzen.
2. Wenn der KMS gespeichert wird, stellen alle Appliance-Nodes, deren **Node Encryption**-Einstellung aktiviert ist, eine Verbindung zum KMS her und fordern den Verschlüsselungsschlüssel an. Dieser Schlüssel wird verwendet, um die Appliance-Nodes an allen Standorten zu verschlüsseln. Dieser Schlüssel muss auch verwendet werden, um diese Geräte zu entschlüsseln.




3. Sie entscheiden, einen standortspezifischen KMS für einen Standort hinzuzufügen (Datacenter 3 in der Abbildung). Da die Appliance-Nodes jedoch bereits verschlüsselt sind, tritt ein Validierungsfehler auf, wenn Sie versuchen, die Konfiguration für den standortspezifischen KMS zu speichern. Der Fehler tritt auf, weil der standortspezifische KMS nicht über den korrekten Schlüssel verfügt, um die Knoten an diesem Standort zu entschlüsseln.




4. Um das Problem zu beheben, kopieren Sie die aktuelle Version des Verschlüsselungsschlüssels vom Standard-KMS auf den neuen KMS. (Technisch kopieren Sie den Originalschlüssel in einen neuen Schlüssel mit dem gleichen Alias. Der ursprüngliche Schlüssel wird zu einer früheren Version des neuen Schlüssels.) Der standortspezifische KMS hat jetzt den richtigen Schlüssel zur Entschlüsselung der Appliance-Nodes in Datacenter 3, sodass er in StorageGRID gespeichert werden kann.




## Anwendungsfälle für die Änderung, welcher KMS für eine Site verwendet wird

Die Tabelle fasst die erforderlichen Schritte für die häufigsten Fälle zur Änderung des KMS für einen Standort zusammen.

| Anwendungsfall zum Ändern des KMS einer Site | Erforderliche Schritte |
| --- | --- |
| Sie haben einen oder mehrere Site-spezifische KMS-Einträge, und Sie möchten einen von ihnen als Standard-KMS verwenden. | Bearbeiten Sie den Site-spezifischen KMS. Wählen Sie im Feld **verwaltet Schlüssel für** die Option **Sites, die nicht von einem anderen KMS verwaltet werden (Standard KMS)**. Der Site-spezifische KMS wird jetzt als Standard-KMS verwendet. Er gilt für alle Websites, die keinen dedizierten KMS haben.<br><br>"Bearbeiten eines Verschlüsselungsmanagement-Servers (KMS)" |
| Sie haben einen Standard-KMS, und Sie fügen eine neue Site in einer Erweiterung hinzu. Sie möchten den Standard-KMS für die neue Site nicht verwenden. | 1. Wenn die Appliance-Nodes auf dem neuen Standort bereits durch den Standard-KMS verschlüsselt wurden, kopieren Sie mithilfe der KMS-Software die aktuelle Version des Verschlüsselungsschlüssels vom Standard-KMS auf einen neuen KMS.<br>2. Fügen Sie mithilfe des Grid-Managers den neuen KMS hinzu und wählen Sie die Site aus.<br><br>"Hinzufügen eines Verschlüsselungsmanagement-Servers (KMS)" |
| Sie möchten, dass der KMS für eine Site einen anderen Server verwendet. | 1. Wenn die Appliance-Nodes am Standort bereits durch den vorhandenen KMS verschlüsselt wurden, kopieren Sie mithilfe der KMS-Software die aktuelle Version des Verschlüsselungsschlüssels vom bestehenden KMS auf den neuen KMS.<br>2. Bearbeiten Sie mithilfe des Grid Manager die bestehende KMS-Konfiguration und geben Sie den neuen Hostnamen oder die neue IP-Adresse ein.<br><br>"Hinzufügen eines Verschlüsselungsmanagement-Servers (KMS)" |

# Konfigurieren von StorageGRID als Client im KMS

Sie müssen StorageGRID als Client für jeden externen Verschlüsselungsmanagement-Server oder KMS-Cluster konfigurieren, bevor Sie den KMS StorageGRID hinzufügen können.

**Über diese Aufgabe**

Diese Anweisungen gelten für Thales CipherTrust Manager k170v, Versionen 2.0, 2.1 und 2.2. Wenn Sie Fragen zur Verwendung eines anderen Verschlüsselungsmanagementservers mit StorageGRID haben, wenden Sie sich an den technischen Support.

"Thales CipherTrust Manager"

**Schritte**

1. Erstellen Sie von der KMS-Software einen StorageGRID-Client für jeden KMS- oder KMS-Cluster, den Sie verwenden möchten.

   Jeder KMS managt einen einzelnen Verschlüsselungsschlüssel für die Nodes der StorageGRID Appliances an einem einzelnen Standort oder einer Gruppe von Standorten.

2. Erstellen Sie von der KMS-Software einen AES-Verschlüsselungsschlüssel für jedes KMS- oder KMS-Cluster.

   Die Verschlüsselung muss exportierbar sein.

3. Notieren Sie die folgenden Informationen für jeden KMS- oder KMS-Cluster.

   Diese Informationen benötigen Sie, wenn Sie den KMS StorageGRID hinzufügen.

   - Host-Name oder IP-Adresse für jeden Server.
   - Der vom KMS verwendete KMIP-Port.
   - Schlüsselalias für den Verschlüsselungsschlüssel im KMS.

     > Der Verschlüsselungsschlüssel muss bereits im KMS vorhanden sein. StorageGRID erstellt oder managt keine KMS-Schlüssel.

4. Beziehen Sie für jeden KMS- oder KMS-Cluster ein Serverzertifikat, das von einer Zertifizierungsstelle (CA) signiert wurde, oder ein Zertifikatbündel, das jede der PEM-kodierten CA-Zertifikatdateien enthält, die in der Reihenfolge der Zertifikatskette verkettet sind.

   Das Serverzertifikat ermöglicht es dem externen KMS, sich bei StorageGRID zu authentifizieren.

   - Das Zertifikat muss das mit Privacy Enhanced Mail (PEM) Base-64 codierte X.509-Format verwenden.
   - Das Feld für alternativen Servernamen (SAN) in jedem Serverzertifikat muss den vollständig qualifizierten Domänennamen (FQDN) oder die IP-Adresse enthalten, mit der StorageGRID eine Verbindung herstellt.

     > Wenn Sie den KMS in StorageGRID konfigurieren, müssen Sie dieselben FQDNs oder IP-Adressen im Feld **Hostname** eingeben.

   - Das Serverzertifikat muss mit dem Zertifikat übereinstimmen, das von der KMIP-Schnittstelle des KMS verwendet wird. In der Regel wird Port 5696 verwendet.

5. Holen Sie sich das öffentliche Clientzertifikat, das vom externen KMS an StorageGRID ausgestellt wurde, und den privaten Schlüssel für das Clientzertifikat.

   Das Client-Zertifikat ermöglicht StorageGRID, sich am KMS zu authentifizieren.

# Hinzufügen eines Verschlüsselungsmanagement-Servers (KMS)

Mithilfe des Assistenten für den StorageGRID-Verschlüsselungsmanagement-Server können Sie jeden KMS- oder KMS-Cluster hinzufügen.

**Was Sie benötigen**

- Sie müssen den geprüft haben "Überlegungen und Anforderungen für die Verwendung eines Verschlüsselungsmanagement-Servers".
- Dieser muss unbedingt vorhanden sein "StorageGRID wurde als Client im KMS konfiguriert", Und Sie müssen die erforderlichen Informationen für jeden KMS- oder KMS-Cluster haben
- Sie müssen über die Berechtigung Root Access verfügen.
- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

**Über diese Aufgabe**

Konfigurieren Sie, falls möglich, Site-spezifische Verschlüsselungsmanagement-Server, bevor Sie einen Standard-KMS konfigurieren, der für alle Standorte gilt, die nicht von einem anderen KMS gemanagt werden. Wenn Sie zuerst den Standard-KMS erstellen, werden alle Node-verschlüsselten Appliances im Grid durch den Standard-KMS verschlüsselt. Wenn Sie später einen Site-spezifischen KMS erstellen möchten, müssen Sie zuerst die aktuelle Version des Verschlüsselungsschlüssels vom Standard-KMS auf den neuen KMS kopieren.

"Überlegungen für das Ändern des KMS für einen Standort"

**Schritte**

1. "Schritt 1: Geben Sie KMS-Details ein"
2. "Schritt: Serverzertifikat Hochladen"
3. "Schritt 3: Laden Sie Client-Zertifikate Hoch"

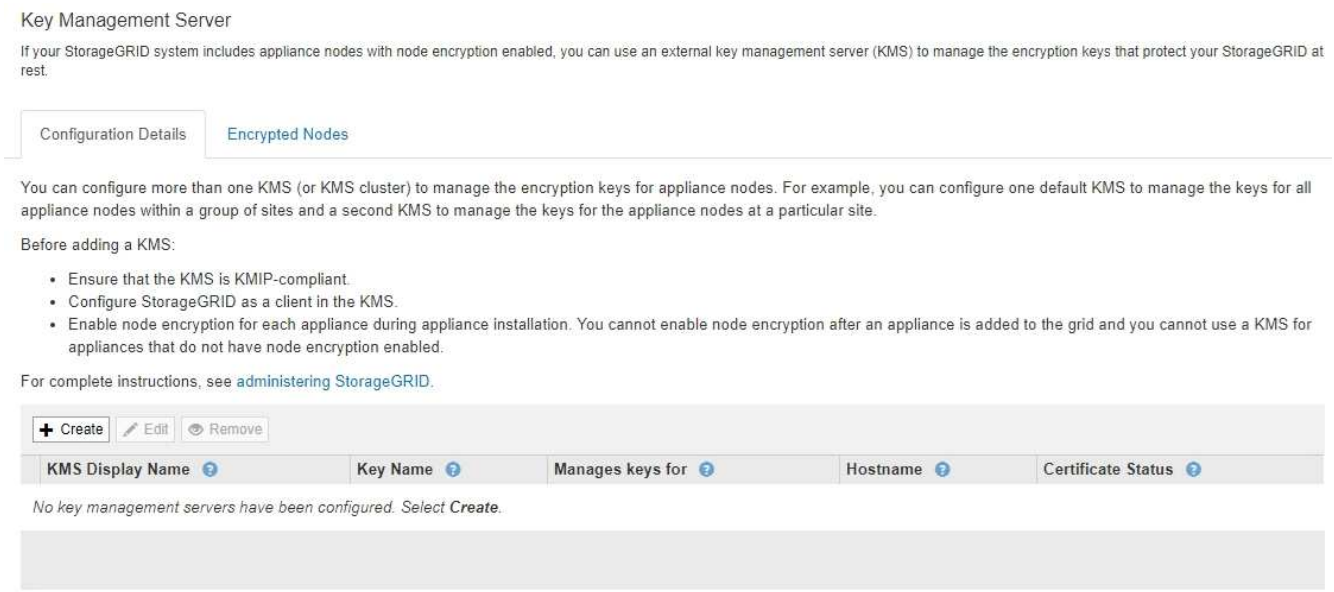
## Schritt 1: Geben Sie KMS-Details ein

In Schritt 1 (KMS-Details eingeben) des Assistenten zum Hinzufügen eines Schlüsselverwaltungsservers geben Sie Details zum KMS- oder KMS-Cluster an.

**Schritte**

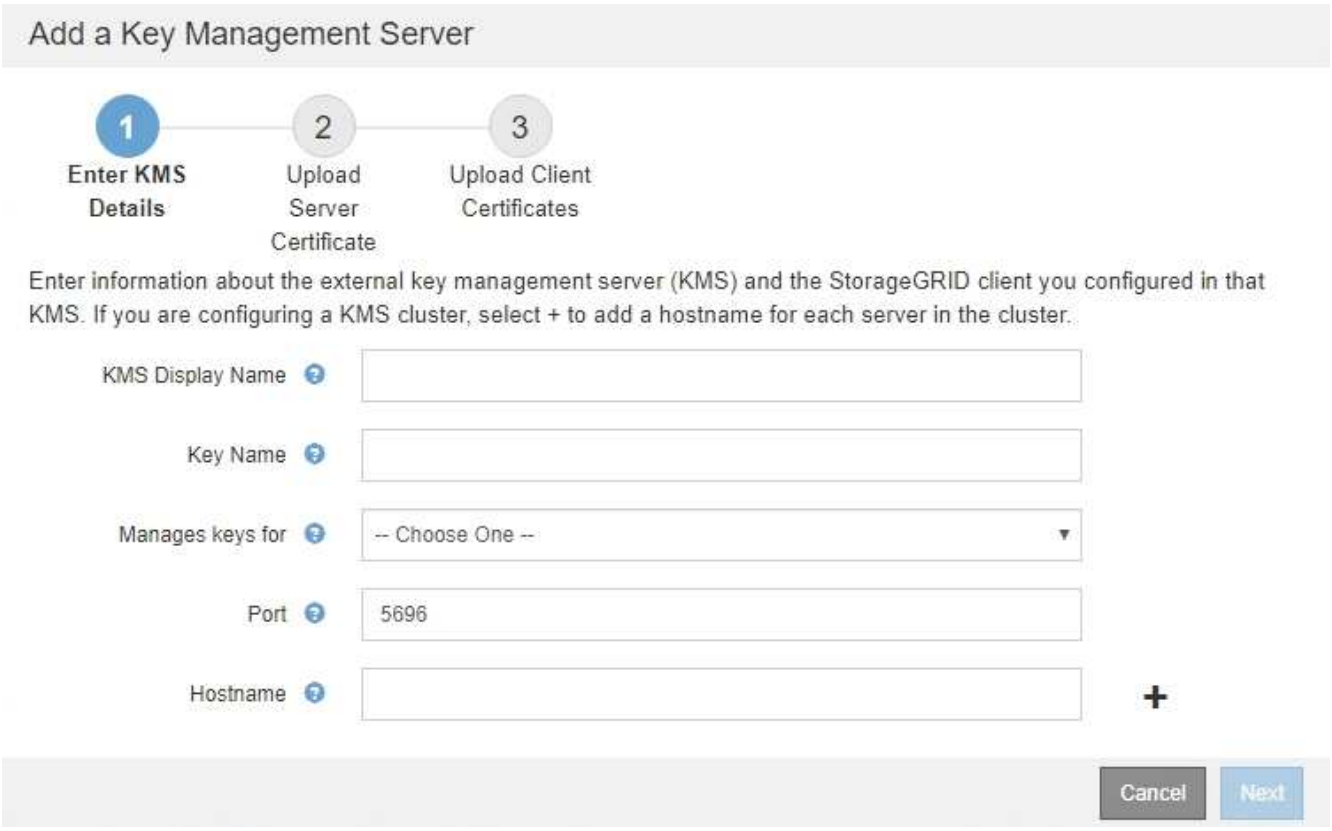
1. Wählen Sie **Konfiguration** > **Systemeinstellungen** > **Schlüsselverwaltungsserver** Aus.

   Die Seite Key Management Server wird angezeigt, wobei die Registerkarte Konfigurationsdetails ausgewählt ist.



2. Wählen Sie **Erstellen**.

   Schritt 1 (KMS-Details eingeben) des Assistenten zum Hinzufügen eines Schlüsselverwaltungsservers wird angezeigt.




3. Geben Sie die folgenden Informationen für den KMS und den StorageGRID-Client ein, den Sie in diesem KMS konfiguriert haben.

| Feld | Beschreibung |
|---|---|
| KMS-Anzeigename | Einen beschreibenden Namen, der Ihnen bei der Identifizierung dieses KMS hilft. Muss zwischen 1 und 64 Zeichen liegen. |
| Schlüsselname | Der exakte Schlüssel-Alias für den StorageGRID-Client im KMS. Muss zwischen 1 und 255 Zeichen liegen. |

| Feld | Beschreibung |
| --- | --- |
| Verwaltet Schlüssel für | Der StorageGRID-Site, die diesem KMS zugeordnet wird. Wenn möglich, sollten Sie alle standortspezifischen Verschlüsselungsmanagement-Server konfigurieren, bevor Sie einen Standard-KMS konfigurieren, der für alle Standorte gilt, die nicht von einem anderen KMS verwaltet werden.<br>• Wählen Sie einen Standort aus, wenn dieser KMS Verschlüsselungen für die Appliance-Nodes an einem bestimmten Standort managt.<br>• Wählen Sie **Sites, die nicht von einem anderen KMS (Standard KMS)** verwaltet werden, um einen Standard-KMS zu konfigurieren, der für alle Sites gilt, die keinen dedizierten KMS haben, und für alle Sites, die Sie in nachfolgenden Erweiterungen hinzufügen.<br>**Hinweis:** beim Speichern der KMS-Konfiguration Tritt Ein Validierungsfehler auf, wenn Sie eine Site auswählen, die zuvor durch den Standard-KMS verschlüsselt wurde, aber Sie haben die aktuelle Version des ursprünglichen Verschlüsselungsschlüssels nicht dem neuen KMS zur Verfügung gestellt. |
| Port | Der Port, den der KMS-Server für die KMIP-Kommunikation (Key Management Interoperability Protocol) verwendet. Die Standardeinstellung ist 5696, d. h. der KMIP-Standardport. |
| Hostname | Der vollständig qualifizierte Domänenname oder die IP-Adresse für den KMS.<br>**Hinweis:** das SAN-Feld des Serverzertifikats muss den FQDN oder die IP-Adresse enthalten, die Sie hier eingeben. Andernfalls kann StorageGRID keine Verbindung zum KMS oder zu allen Servern eines KMS-Clusters herstellen. |

4. Wenn Sie einen KMS-Cluster verwenden, wählen Sie das Pluszeichen aus + Um einen Hostnamen für jeden Server im Cluster hinzuzufügen.
5. Wählen Sie **Weiter**.

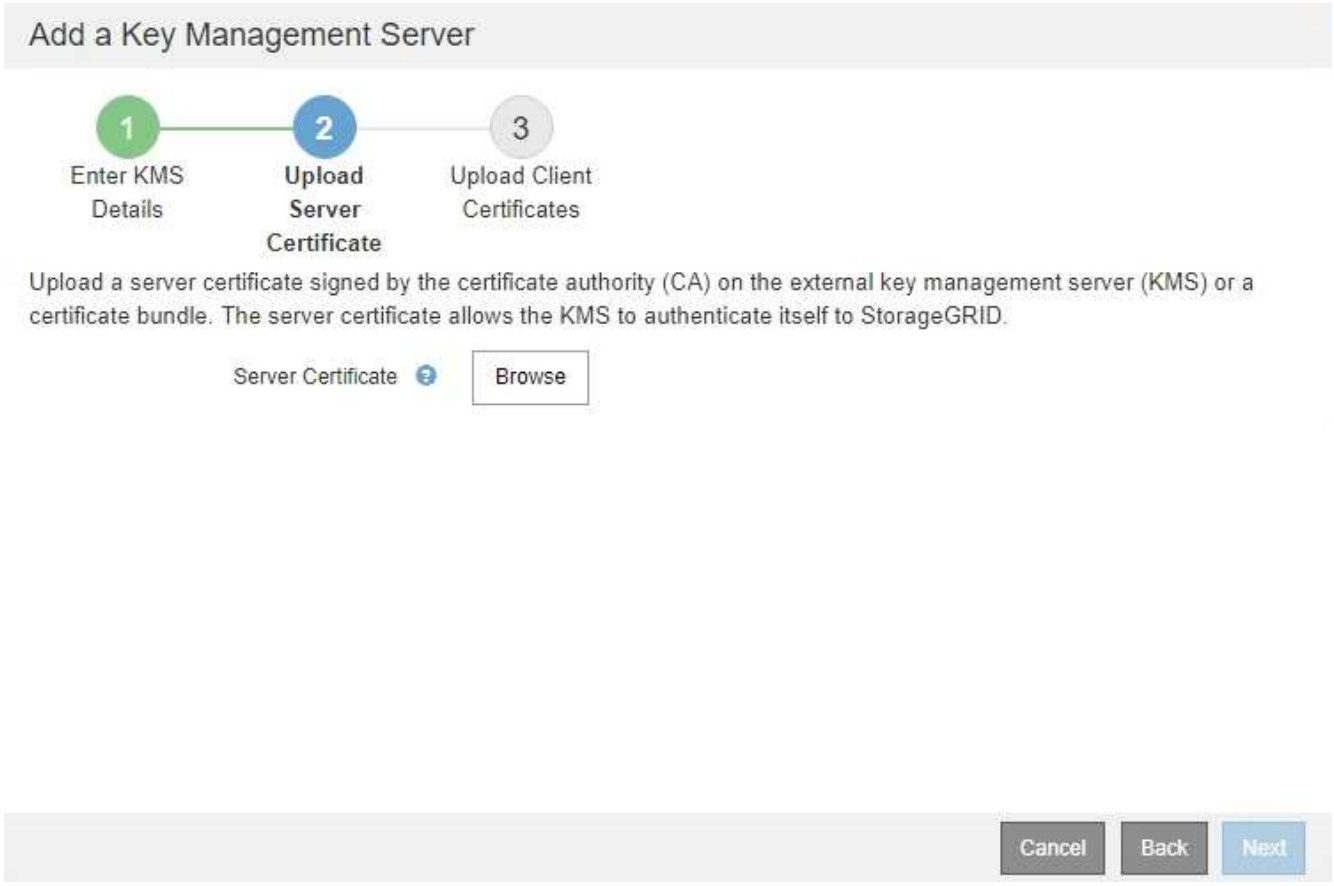
   Schritt 2 (Serverzertifikat hochladen) des Assistenten zum Hinzufügen eines Schlüsselverwaltungsservers wird angezeigt.

## Schritt: Serverzertifikat Hochladen

In Schritt 2 (Serverzertifikat hochladen) des Assistenten zum Hinzufügen eines Schlüsselverwaltungsservers laden Sie das Serverzertifikat (oder das Zertifikatspaket) für den KMS hoch. Das Serverzertifikat ermöglicht es dem externen KMS, sich bei StorageGRID zu authentifizieren.

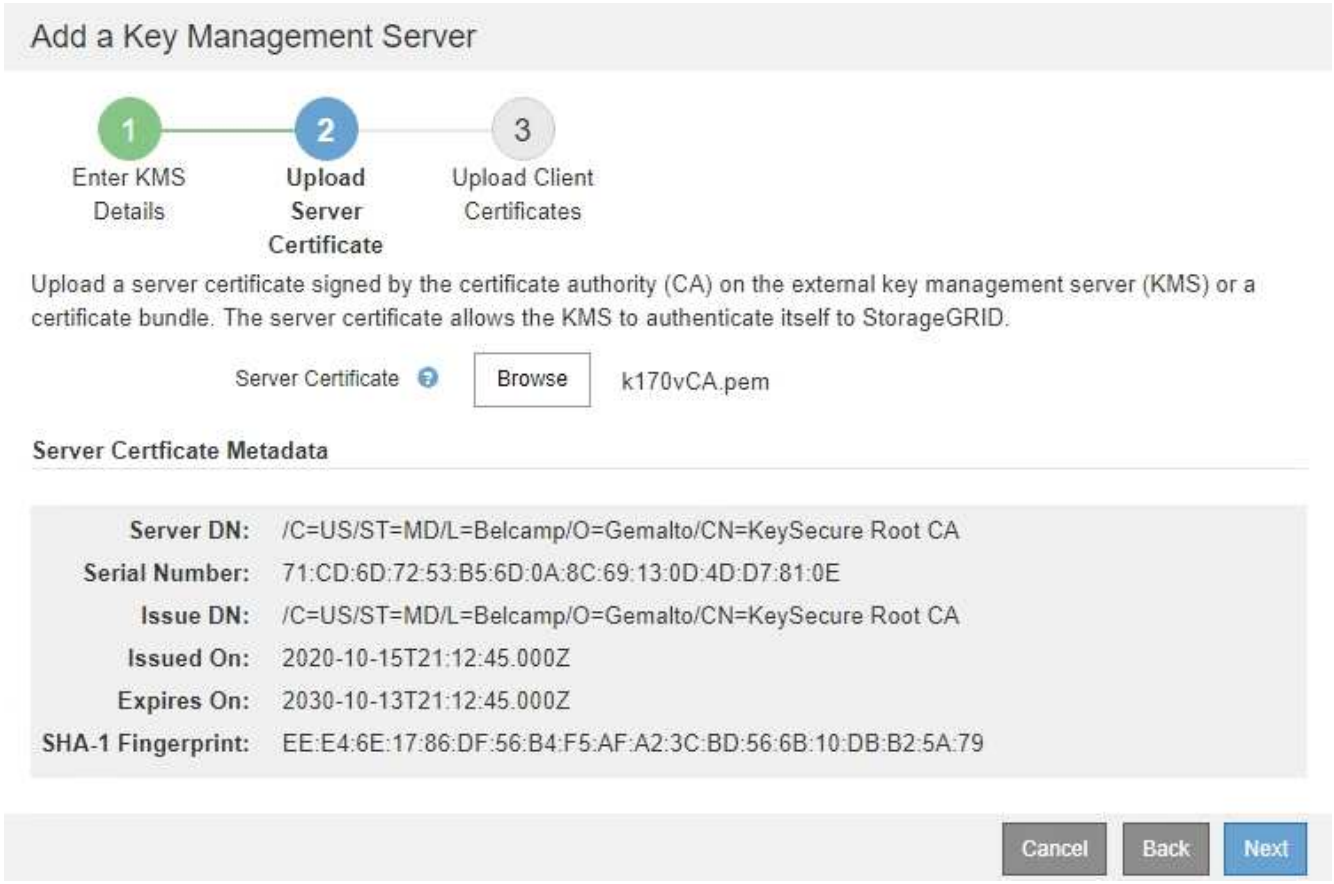
**Schritte**

1. Navigieren Sie ab **Schritt 2 (Serverzertifikat hochladen)** zum Speicherort des gespeicherten Serverzertifikats oder Zertifikatpakets.




2. Laden Sie die Zertifikatdatei hoch.

   Die Metadaten des Serverzertifikats werden angezeigt.




Wenn Sie ein Zertifikatbündel hochgeladen haben, werden die Metadaten für jedes Zertifikat auf der eigenen Registerkarte angezeigt.

3. Wählen Sie **Weiter**.

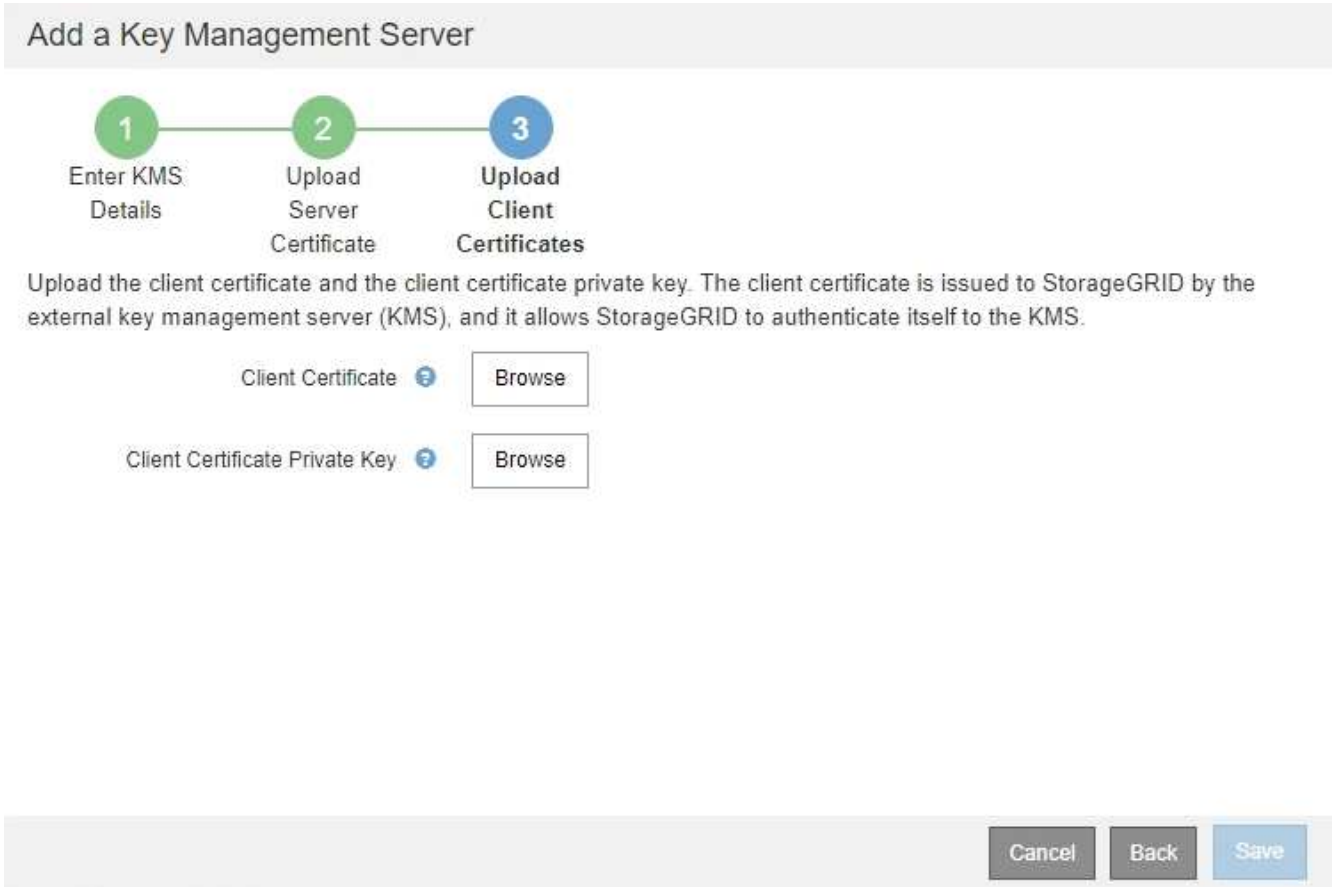
   Schritt 3 (Upload Client Certificates) des Assistenten Add a Key Management Server wird angezeigt.

## Schritt 3: Laden Sie Client-Zertifikate Hoch

In Schritt 3 (Upload Client Certificates) des Assistenten Add a Key Management Server laden Sie das Clientzertifikat und den privaten Schlüssel des Clientzertifikats hoch. Das Client-Zertifikat ermöglicht StorageGRID, sich am KMS zu authentifizieren.

**Schritte**

1. Ab **Schritt 3 (Upload Client Certificates)** navigieren Sie zum Speicherort des Clientzertifikats.

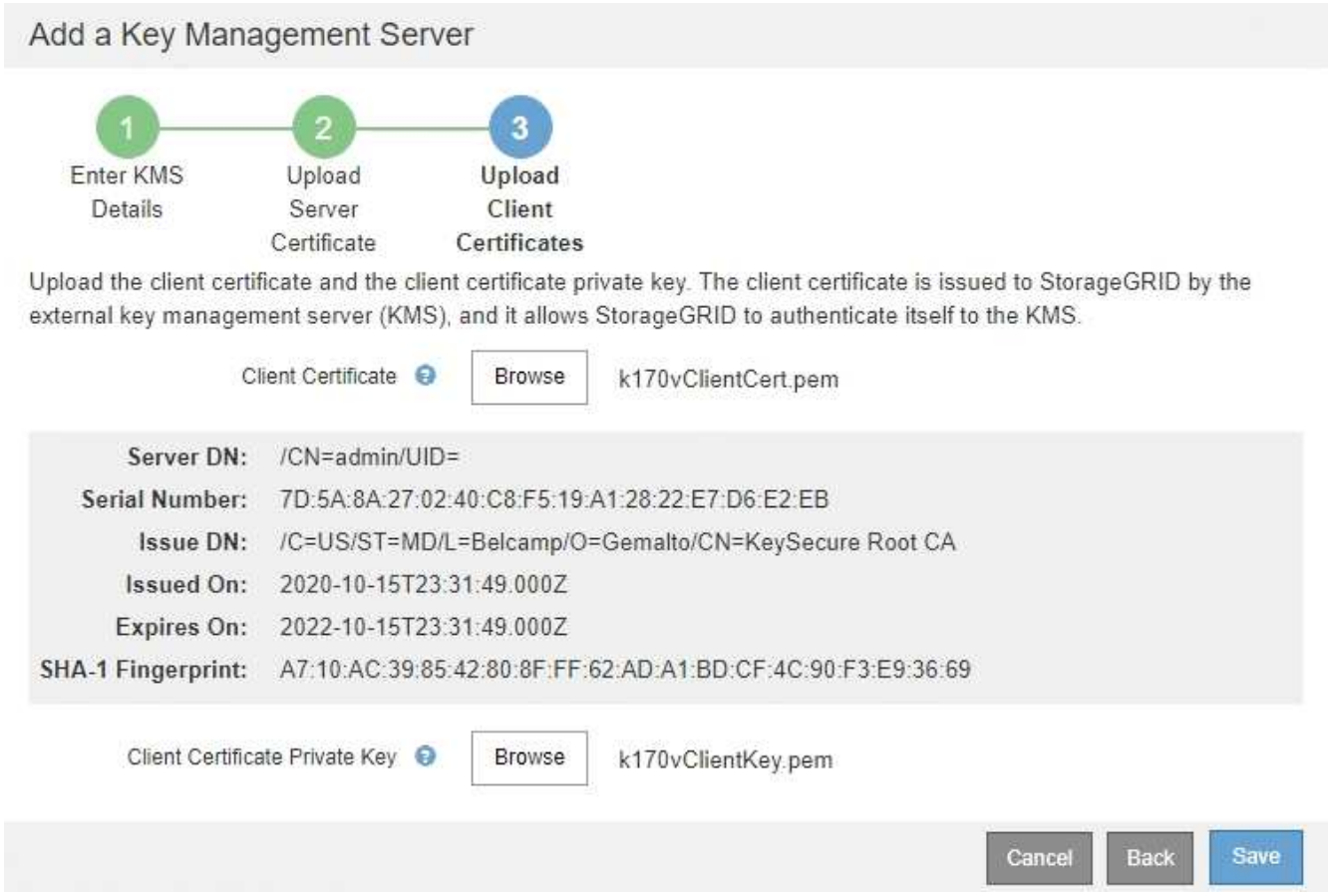



2. Laden Sie die Clientzertifikatdatei hoch.

   Die Metadaten des Client-Zertifikats werden angezeigt.

3. Navigieren Sie zum Speicherort des privaten Schlüssels für das Clientzertifikat.
4. Laden Sie die Datei mit dem privaten Schlüssel hoch.

   Die Metadaten für das Clientzertifikat und der private Schlüssel für das Clientzertifikat werden angezeigt.




5. Wählen Sie **Speichern**.

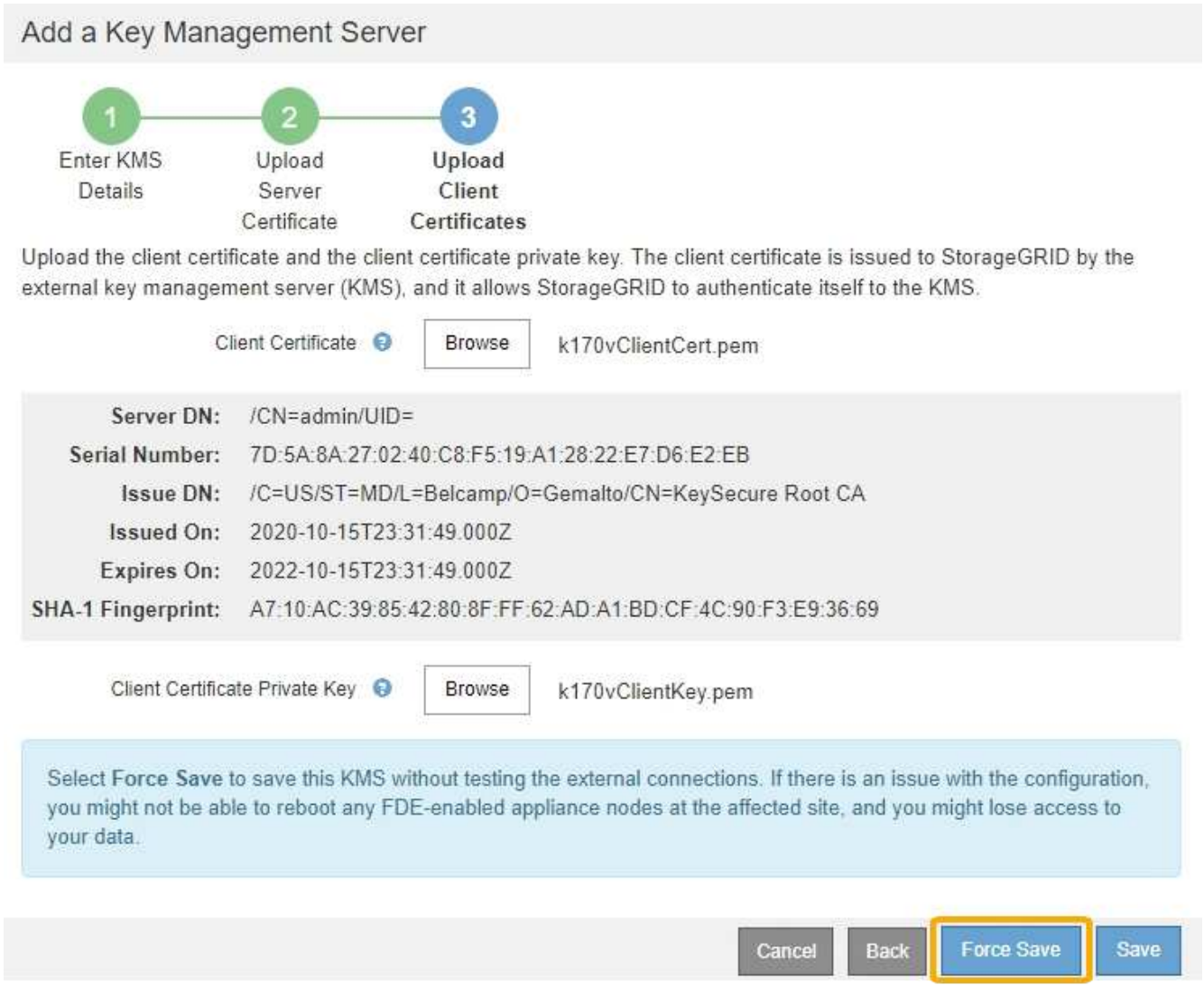
   Die Verbindungen zwischen dem Verschlüsselungsmanagement-Server und den Appliance-Nodes werden getestet. Wenn alle Verbindungen gültig sind und der korrekte Schlüssel auf dem KMS gefunden wird, wird der neue Schlüsselverwaltungsserver der Tabelle auf der Seite des Key Management Servers hinzugefügt.

   > Unmittelbar nach dem Hinzufügen eines KMS wird der Zertifikatsstatus auf der Seite Key Management Server als Unbekannt angezeigt. Es kann StorageGRID bis zu 30 Minuten dauern, bis der aktuelle Status eines jeden Zertifikats angezeigt wird. Sie müssen Ihren Webbrowser aktualisieren, um den aktuellen Status anzuzeigen.

6. Wenn beim Auswählen von **Speichern** eine Fehlermeldung angezeigt wird, überprüfen Sie die Nachrichtendetails und wählen Sie dann **OK** aus.

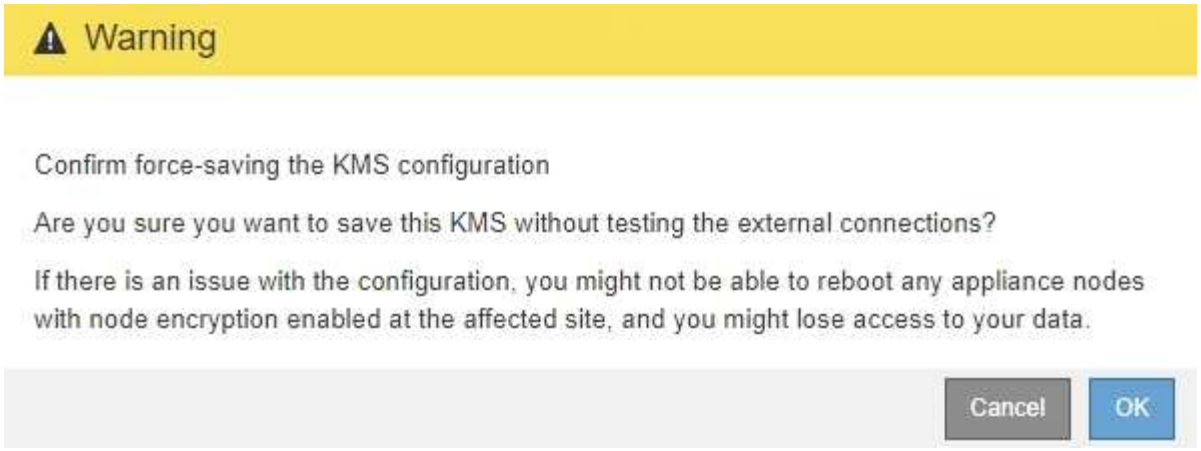
   Beispiel: Wenn ein Verbindungstest fehlgeschlagen ist, können Sie einen Fehler bei unbearbeitbarer Einheit mit 422: Nicht verarbeitbarer Einheit erhalten.

7. Wenn Sie die aktuelle Konfiguration speichern müssen, ohne die externe Verbindung zu testen, wählen Sie **Erzwingen Sie Speichern**.




Durch die Auswahl von **Erzwingen speichern** wird die KMS-Konfiguration gespeichert, die externe Verbindung von jedem Gerät zu diesem KMS wird jedoch nicht getestet. Wenn Probleme mit der Konfiguration bestehen, können Sie Appliance-Nodes, für die die Node-Verschlüsselung am betroffenen Standort aktiviert ist, möglicherweise nicht neu starten. Wenn der Zugriff auf Ihre Daten nicht mehr vollständig ist, können Sie diese Probleme beheben.

8. Überprüfen Sie die Bestätigungswarnung, und wählen Sie **OK**, wenn Sie sicher sind, dass Sie das Speichern der Konfiguration erzwingen möchten.




Die KMS-Konfiguration wird gespeichert, die Verbindung zum KMS wird jedoch nicht getestet.

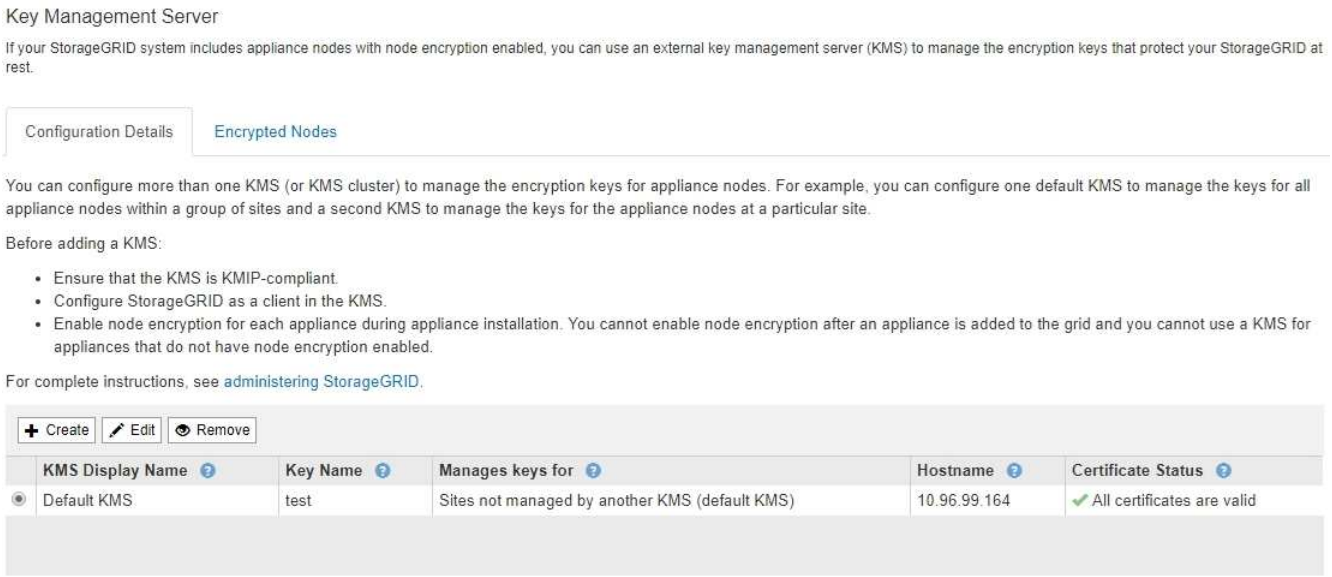
# Anzeigen von KMS-Details

Sie können Informationen zu jedem Schlüsselverwaltungsserver (KMS) in Ihrem StorageGRID-System anzeigen, einschließlich des aktuellen Status des Servers und der Clientzertifikate.

**Schritte**

1. Wählen Sie **Konfiguration** > **Systemeinstellungen** > **Schlüsselverwaltungsserver** Aus.

   Die Seite Key Management Server wird angezeigt. Auf der Registerkarte Konfigurationsdetails werden alle konfigurierten Schlüsselverwaltungsserver angezeigt.




2. Überprüfen Sie die Informationen in der Tabelle für jeden KMS.

| Feld | Beschreibung |
| --- | --- |
| KMS-Anzeigename | Der beschreibende Name des KMS. |

| Feld | Beschreibung |
| --- | --- |
| Schlüsselname | Der Schlüsselalias für den StorageGRID-Client im KMS. |
| Verwaltet Schlüssel für | Der dem KMS zugeordnete StorageGRID-Site.<br><br>Dieses Feld zeigt den Namen einer bestimmten StorageGRID-Site oder **Sites an, die nicht von einem anderen KMS verwaltet werden (Standard-KMS).** |
| Hostname | Der vollständig qualifizierte Domänenname oder die IP-Adresse des KMS.<br><br>Wenn ein Cluster von zwei Schlüsselverwaltungsservern vorhanden ist, werden der vollständig qualifizierte Domänenname oder die IP-Adresse beider Server aufgelistet. Wenn mehr als zwei Schlüsselverwaltungsserver in einem Cluster vorhanden sind, wird der vollständig qualifizierte Domänenname oder die IP-Adresse des ersten KMS zusammen mit der Anzahl der zusätzlichen Schlüsselverwaltungsserver im Cluster aufgelistet.<br><br>Beispiel: `10.10.10.10 and 10.10.10.11` Oder `10.10.10.10 and 2 others`.<br><br>Um alle Hostnamen in einem Cluster anzuzeigen, wählen Sie einen KMS aus, und wählen Sie dann **Bearbeiten** aus. |
| Zertifikatsstatus | Aktueller Status des Serverzertifikats, des optionalen CA-Zertifikats und des Client-Zertifikats: Gültig, abgelaufen, bald abgelaufen oder unbekannt.<br><br>**Hinweis:** möglicherweise dauert StorageGRID bis zu 30 Minuten, um Updates zum Zertifikatsstatus zu erhalten. Sie müssen Ihren Webbrowser aktualisieren, um die aktuellen Werte anzuzeigen. |

3. Wenn der Zertifikatsstatus unbekannt ist, warten Sie bis zu 30 Minuten, und aktualisieren Sie dann Ihren Webbrowser.

> Unmittelbar nach dem Hinzufügen eines KMS wird der Zertifikatsstatus auf der Seite Key Management Server als Unbekannt angezeigt. Es kann StorageGRID bis zu 30 Minuten dauern, bis der aktuelle Status eines jeden Zertifikats angezeigt wird. Sie müssen Ihren Webbrowser aktualisieren, um den aktuellen Status anzuzeigen.

4. Wenn in der Spalte „Zertifikatsstatus“ angegeben ist, dass ein Zertifikat abgelaufen ist oder sich dem

Ablauf nähert, beheben Sie das Problem so schnell wie möglich.

Lesen Sie die empfohlenen Aktionen für den Ablauf des **KMS CA-Zertifikats**, **KMS-Clientzertifikats-Ablauf** und **KMS-Serverzertifikate-Ablauf**-Alarme in den Anweisungen zur Überwachung und Fehlerbehebung von StorageGRID.

> ⓘ Sie müssen Probleme mit dem Zertifikat so schnell wie möglich beheben, um den Datenzugriff aufrechtzuerhalten.

**Verwandte Informationen**

"Monitor Fehlerbehebung"

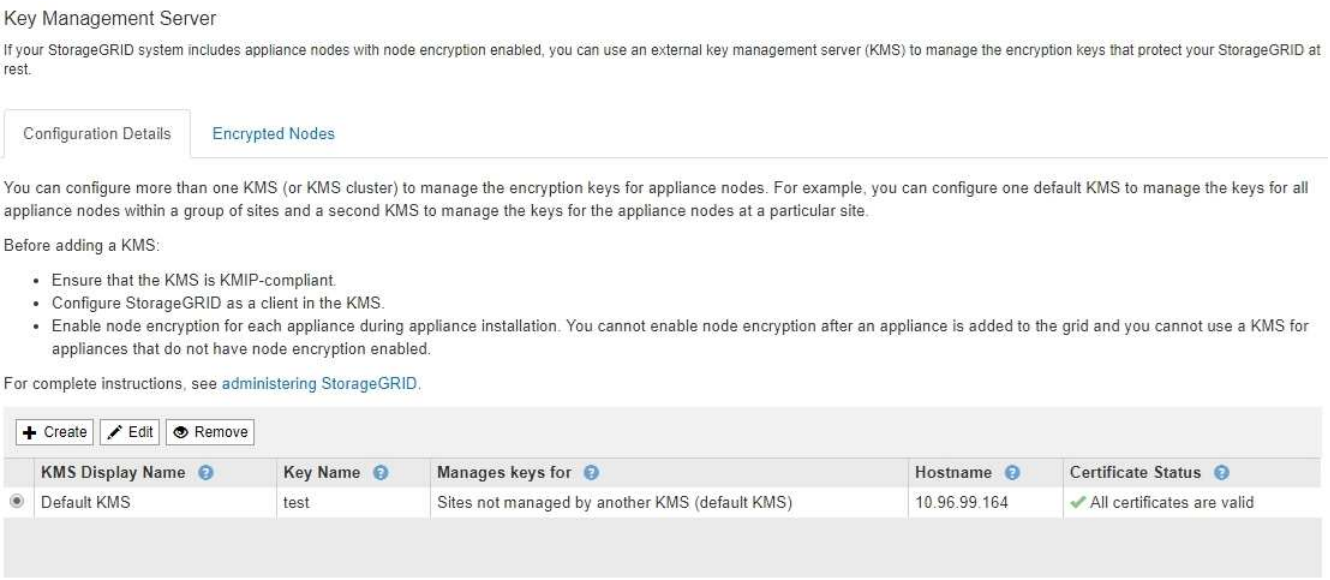
# Anzeigen verschlüsselter Nodes

Sie können Informationen zu den Appliance-Knoten in Ihrem StorageGRID-System anzeigen, bei denen die Einstellung **Node-Verschlüsselung** aktiviert ist.

**Schritte**

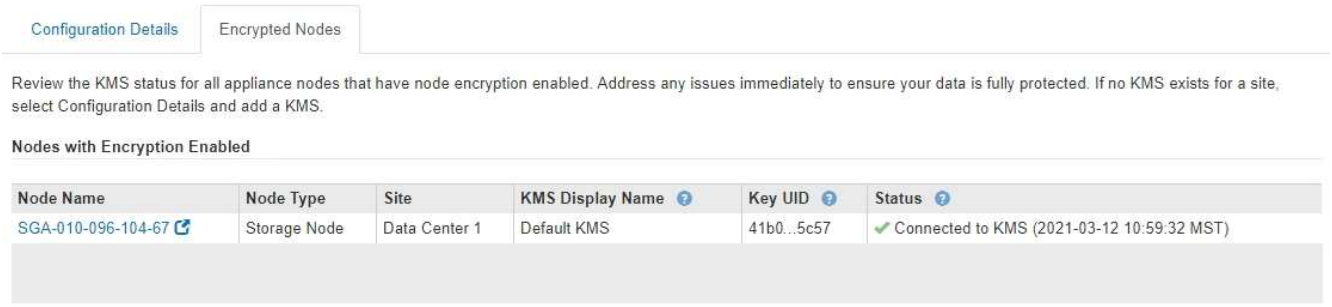
1. Wählen Sie **Konfiguration** > **Systemeinstellungen** > **Schlüsselverwaltungsserver** Aus.

   Die Seite Key Management Server wird angezeigt. Auf der Registerkarte Konfigurationsdetails werden alle konfigurierten Schlüsselverwaltungsserver angezeigt.




2. Wählen Sie oben auf der Seite die Registerkarte **verschlüsselte Knoten** aus.

Auf der Registerkarte verschlüsselte Knoten werden die Geräteknoten in Ihrem StorageGRID-System aufgelistet, bei denen die Einstellung **Knotenverschlüsselung** aktiviert ist.




3. Überprüfen Sie die Informationen in der Tabelle für jeden Appliance-Node.

| Spalte | Beschreibung |
|---|---|
| Node-Name | Der Name des Appliance-Node. |
| Node-Typ | Der Node-Typ: Storage, Admin oder Gateway. |
| Standort | Der Name der StorageGRID-Site, auf der der Node installiert ist. |
| KMS-Anzeigename | Der beschreibende Name des für den Knoten verwendeten KMS.<br><br>Wenn kein KMS aufgeführt ist, wählen Sie die Registerkarte Konfigurationsdetails aus, um einen KMS hinzuzufügen.<br><br>"Hinzufügen eines Verschlüsselungsmanagement-Servers (KMS)" |
| Schlüssel-UID | Die eindeutige ID des Verschlüsselungsschlüssels, der zur Verschlüsselung und Entschlüsselung von Daten auf dem Appliance-Node verwendet wird. Wenn Sie eine vollständige Schlüssel-UID anzeigen möchten, bewegen Sie den Mauszeiger über die Zelle.<br><br>Ein Bindestrich (-) gibt an, dass die Schlüssel-UID unbekannt ist, möglicherweise wegen eines Verbindungsproblem zwischen dem Appliance-Node und dem KMS. |
| Status | Der Status der Verbindung zwischen dem KMS und dem Appliance-Node. Wenn der Knoten verbunden ist, wird der Zeitstempel alle 30 Minuten aktualisiert. Nach einer Änderung der KMS-Konfiguration kann es mehrere Minuten dauern, bis der Verbindungsstatus aktualisiert wird.<br><br>**Hinweis:** Sie müssen Ihren Webbrowser aktualisieren, um die neuen Werte zu sehen. |

4. Wenn in der Spalte Status ein KMS-Problem angezeigt wird, beheben Sie das Problem sofort.

   Während normaler KMS-Vorgänge wird der Status **mit KMS** verbunden. Wenn ein Knoten von der Tabelle getrennt wird, wird der Verbindungsstatus des Knotens angezeigt (administrativ ausgefallen oder

unbekannt).

Andere Statusmeldungen entsprechen StorageGRID Meldungen mit denselben Namen:

- KMS-Konfiguration konnte nicht geladen werden
- KMS-Verbindungsfehler
- DER VERSCHLÜSSELUNGSSCHLÜSSELNAME VON KMS wurde nicht gefunden
- DIE Drehung des VERSCHLÜSSELUNGSSCHLÜSSELS ist fehlgeschlagen
- KMS-Schlüssel konnte ein Appliance-Volume nicht entschlüsseln
- KMS ist nicht konfiguriert Siehe die empfohlenen Aktionen für diese Warnmeldungen in den Anweisungen für Monitoring und Fehlerbehebung StorageGRID.

Sämtliche Probleme müssen sofort behoben werden, um einen vollständigen Schutz Ihrer Daten zu gewährleisten.

**Verwandte Informationen**

"Monitor Fehlerbehebung"

# Bearbeiten eines Verschlüsselungsmanagement-Servers (KMS)

Möglicherweise müssen Sie die Konfiguration eines Schlüsselverwaltungsservers bearbeiten, z. B. wenn ein Zertifikat kurz vor dem Ablauf steht.

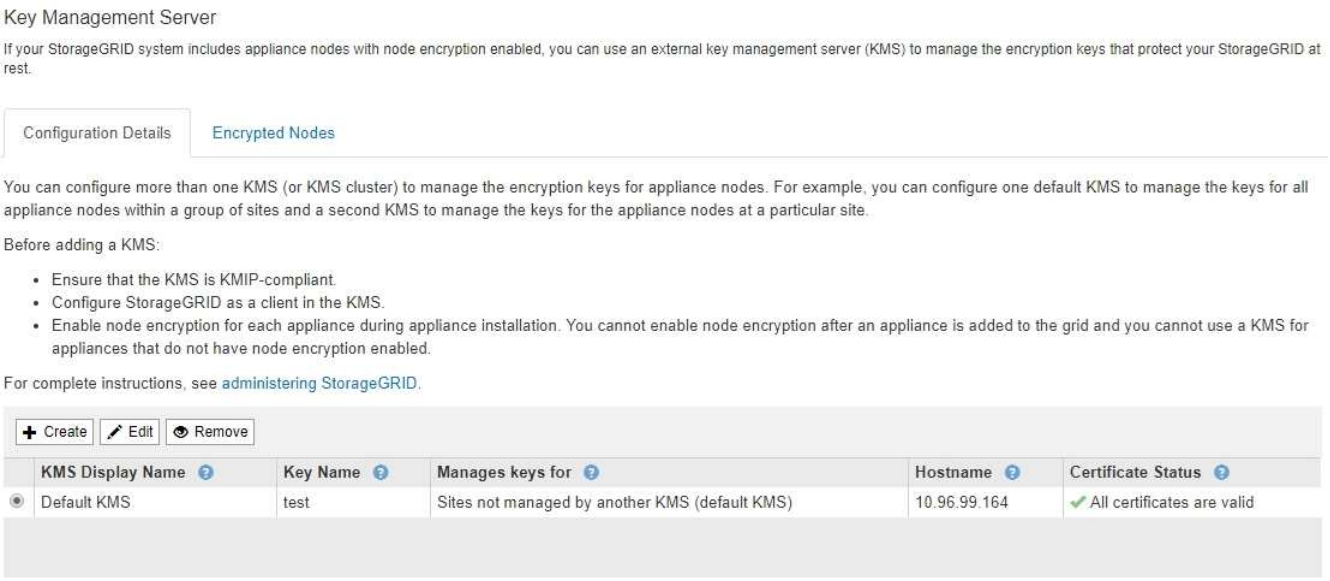
**Was Sie benötigen**

- Sie müssen den geprüft haben "Überlegungen und Anforderungen für die Verwendung eines Verschlüsselungsmanagement-Servers".
- Wenn Sie planen, die für einen KMS ausgewählte Site zu aktualisieren, müssen Sie den geprüft haben "Überlegungen für das Ändern des KMS für einen Standort".
- Sie müssen über die Berechtigung Root Access verfügen.
- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

**Schritte**

1. Wählen Sie **Konfiguration** > **Systemeinstellungen** > **Schlüsselverwaltungsserver** Aus.

   Die Seite Key Management Server wird angezeigt und zeigt alle konfigurierten Schlüsselverwaltungsserver an.




2. Wählen Sie den KMS aus, den Sie bearbeiten möchten, und wählen Sie **Bearbeiten**.
3. Aktualisieren Sie optional die Details in **Schritt 1 (KMS-Details eingeben)** des Assistenten zum Bearbeiten eines Schlüsselverwaltungsservers.

| Feld | Beschreibung |
|---|---|
| KMS-Anzeigename | Einen beschreibenden Namen, der Ihnen bei der Identifizierung dieses KMS hilft. Muss zwischen 1 und 64 Zeichen liegen. |
| Schlüsselname | Der exakte Schlüssel-Alias für den StorageGRID-Client im KMS. Muss zwischen 1 und 255 Zeichen liegen.<br><br>In seltenen Fällen müssen Sie nur den Schlüsselnamen bearbeiten. Sie müssen beispielsweise den Schlüsselnamen bearbeiten, wenn der Alias im KMS umbenannt wird oder alle Versionen des vorherigen Schlüssels in die Versionsgeschichte des neuen Alias kopiert wurden.<br><br>Versuchen Sie niemals, einen Schlüssel zu drehen, indem Sie den Schlüsselnamen (Alias) für den KMS ändern. Drehen Sie stattdessen den Schlüssel, indem Sie die Schlüsselversion in der KMS-Software aktualisieren. Für StorageGRID müssen alle zuvor verwendeten Schlüsselversionen (sowie zukünftige Versionen) vom KMS mit demselben Schlüsselalias zugänglich sein. Wenn Sie den Schlüssel-Alias für einen konfigurierten KMS ändern, kann StorageGRID Ihre Daten möglicherweise nicht entschlüsseln.<br><br>"Überlegungen und Anforderungen für die Verwendung eines Verschlüsselungsmanagement-Servers" |

| Feld | Beschreibung |
| --- | --- |
| Verwaltet Schlüssel für | Wenn Sie einen Site-spezifischen KMS bearbeiten und noch keinen Standard-KMS haben, wählen Sie optional **Sites, die nicht von einem anderen KMS (Standard KMS)** verwaltet werden. Diese Auswahl konvertiert einen standortspezifischen KMS in den Standard-KMS, der für alle Sites gilt, die keinen dedizierten KMS haben, und für alle Sites, die in einer Erweiterung hinzugefügt wurden.<br><br>**Hinweis:** Wenn Sie einen Site-spezifischen KMS bearbeiten, können Sie keine andere Site auswählen. Wenn Sie den Standard-KMS bearbeiten, können Sie keine bestimmte Site auswählen. |
| Port | Der Port, den der KMS-Server für die KMIP-Kommunikation (Key Management Interoperability Protocol) verwendet. Die Standardeinstellung ist 5696, d. h. der KMIP-Standardport. |
| Hostname | Der vollständig qualifizierte Domänenname oder die IP-Adresse für den KMS.<br><br>**Hinweis:** das SAN-Feld des Serverzertifikats muss den FQDN oder die IP-Adresse enthalten, die Sie hier eingeben. Andernfalls kann StorageGRID keine Verbindung zum KMS oder zu allen Servern eines KMS-Clusters herstellen. |

4. Wenn Sie einen KMS-Cluster konfigurieren, wählen Sie das Pluszeichen aus ➕ Um einen Hostnamen für jeden Server im Cluster hinzuzufügen.
5. Wählen Sie **Weiter**.

   Schritt 2 (Serverzertifikat hochladen) des Assistenten „Schlüssel-Management-Server bearbeiten“ wird angezeigt.

6. Wenn Sie das Serverzertifikat ersetzen müssen, wählen Sie **Durchsuchen** und laden Sie die neue Datei hoch.
7. Wählen Sie **Weiter**.

   Schritt 3 (Upload Client Certificates) des Assistenten Edit a Key Management Server wird angezeigt.

8. Wenn Sie das Clientzertifikat und den privaten Schlüssel des Clientzertifikats ersetzen müssen, wählen Sie **Durchsuchen** und laden Sie die neuen Dateien hoch.
9. Wählen Sie **Speichern**.

   Die Verbindungen zwischen dem Verschlüsselungsmanagement-Server und allen Node-verschlüsselten Appliance-Nodes an den betroffenen Standorten werden getestet. Wenn alle Knotenverbindungen gültig sind und der korrekte Schlüssel auf dem KMS gefunden wird, wird der Schlüsselverwaltungsserver der Tabelle auf der Seite des Key Management Servers hinzugefügt.

10. Wenn eine Fehlermeldung angezeigt wird, überprüfen Sie die Nachrichtendetails, und wählen Sie **OK**.

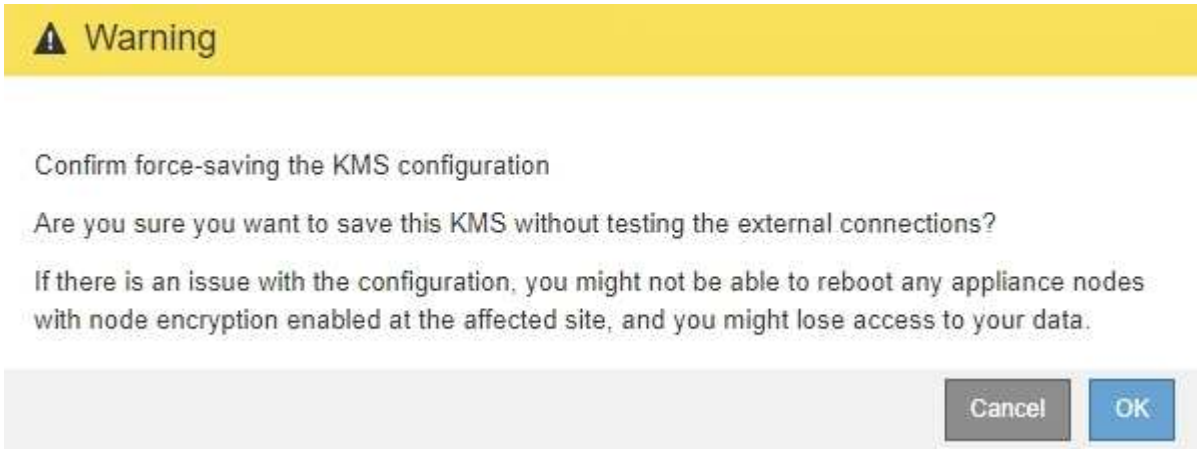
    Sie können beispielsweise einen Fehler bei der nicht verarbeitbaren Einheit von 422 erhalten, wenn die für diesen KMS ausgewählte Site bereits von einem anderen KMS verwaltet wird oder wenn ein Verbindungstest fehlgeschlagen ist.

11. Wenn Sie die aktuelle Konfiguration speichern müssen, bevor Sie die Verbindungsfehler beheben, wählen Sie **Erzwingen Sie Speichern**.

> Durch die Auswahl von **Erzwingen speichern** wird die KMS-Konfiguration gespeichert, die externe Verbindung von jedem Gerät zu diesem KMS wird jedoch nicht getestet. Wenn Probleme mit der Konfiguration bestehen, können Sie Appliance-Nodes, für die die Node-Verschlüsselung am betroffenen Standort aktiviert ist, möglicherweise nicht neu starten. Wenn der Zugriff auf Ihre Daten nicht mehr vollständig ist, können Sie diese Probleme beheben.

Die KMS-Konfiguration wird gespeichert.

12. Überprüfen Sie die Bestätigungswarnung, und wählen Sie **OK**, wenn Sie sicher sind, dass Sie das Speichern der Konfiguration erzwingen möchten.




Die KMS-Konfiguration wird gespeichert, die Verbindung zum KMS wird jedoch nicht getestet.

# Entfernen eines Verschlüsselungsmanagement-Servers (KMS)

In einigen Fällen möchten Sie einen Schlüsselverwaltungsserver entfernen. Sie können beispielsweise einen standortspezifischen KMS entfernen, wenn Sie den Standort deaktiviert haben.

**Was Sie benötigen**

- Sie müssen den geprüft haben "Überlegungen und Anforderungen für die Verwendung eines Verschlüsselungsmanagement-Servers".
- Sie müssen über die Berechtigung Root Access verfügen.
- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

**Über diese Aufgabe**

In diesen Fällen können Sie einen KMS entfernen:

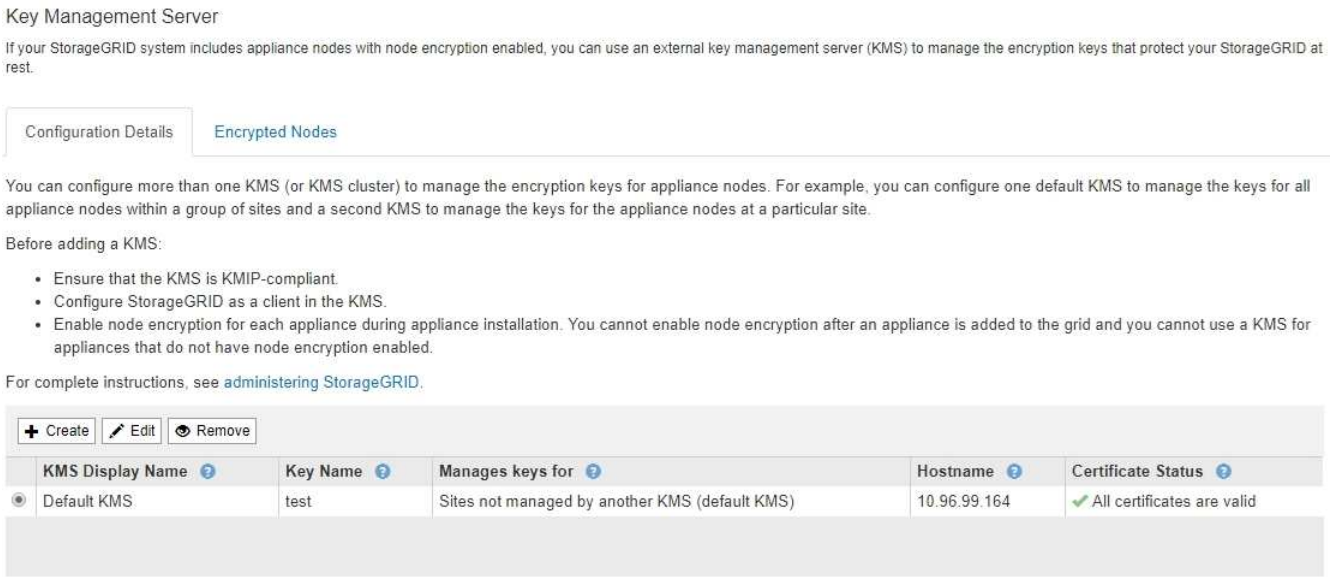
- Wenn der Standort außer Betrieb genommen wurde oder wenn der Standort keine Appliance-Nodes mit aktivierter Node-Verschlüsselung enthält, können Sie einen standortspezifischen KMS entfernen.
- Der Standard-KMS kann entfernt werden, wenn für jeden Standort bereits ein standortspezifischer KMS

vorhanden ist, bei dem Appliance-Nodes mit aktivierter Node-Verschlüsselung vorhanden sind.

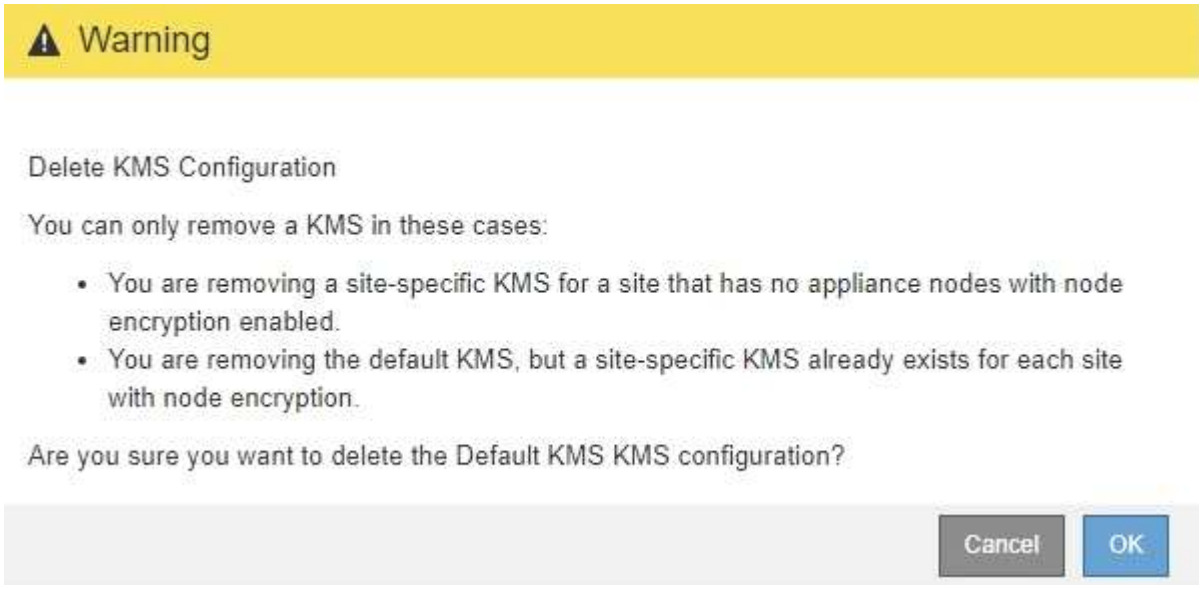
**Schritte**

1. Wählen Sie **Konfiguration** > **Systemeinstellungen** > **Schlüsselverwaltungsserver** Aus.

   Die Seite Key Management Server wird angezeigt und zeigt alle konfigurierten Schlüsselverwaltungsserver an.




2. Wählen Sie das Optionsfeld für den KMS, den Sie entfernen möchten, und wählen Sie **Entfernen**.
3. Prüfen Sie die Überlegungen im Warndialogfeld.




4. Wählen Sie **OK**.

   Die KMS-Konfiguration wurde entfernt.