Konfigurieren von Schlüsselverwaltungsservern

StorageGRID software

NetApp
October 21, 2025

Inhalt

Konfigurieren von Schlüsselverwaltungsservern

Was ist ein Schlüsselverwaltungsserver (KMS)?

Ein Schlüsselverwaltungsserver (KMS) ist ein externes Drittanbietersystem, das mithilfe des Key Management Interoperability Protocol (KMIP) Verschlüsselungsschlüssel für StorageGRID Appliance-Knoten am zugehörigen StorageGRID Standort bereitstellt.

StorageGRID unterstützt nur bestimmte Schlüsselverwaltungsserver. Eine Liste der unterstützten Produkte und Versionen finden Sie im "NetApp Interoperability Matrix Tool (IMT)" .

Sie können einen oder mehrere Schlüsselverwaltungsserver verwenden, um die Knotenverschlüsselungsschlüssel für alle StorageGRID Appliance-Knoten zu verwalten, bei denen während der Installation die Einstellung **Knotenverschlüsselung** aktiviert wurde. Durch die Verwendung von Schlüsselverwaltungsservern mit diesen Appliance-Knoten können Sie Ihre Daten schützen, selbst wenn eine Appliance aus dem Rechenzentrum entfernt wird. Nachdem die Appliance-Volumes verschlüsselt wurden, können Sie auf keine Daten auf der Appliance zugreifen, es sei denn, der Knoten kann mit dem KMS kommunizieren.

> StorageGRID erstellt oder verwaltet die externen Schlüssel, die zum Verschlüsseln und Entschlüsseln von Appliance-Knoten verwendet werden, nicht. Wenn Sie zum Schutz von StorageGRID -Daten einen externen Schlüsselverwaltungsserver verwenden möchten, müssen Sie wissen, wie dieser Server eingerichtet wird und wie die Verschlüsselungsschlüssel verwaltet werden. Die Durchführung wichtiger Verwaltungsaufgaben geht über den Rahmen dieser Anweisungen hinaus. Wenn Sie Hilfe benötigen, lesen Sie die Dokumentation zu Ihrem Schlüsselverwaltungsserver oder wenden Sie sich an den technischen Support.

KMS- und Appliance-Konfiguration

Bevor Sie einen Schlüsselverwaltungsserver (KMS) zum Sichern von StorageGRID -Daten auf Appliance-Knoten verwenden können, müssen Sie zwei Konfigurationsaufgaben ausführen: Einrichten eines oder mehrerer KMS-Server und Aktivieren der Knotenverschlüsselung für die Appliance-Knoten. Wenn diese beiden Konfigurationsaufgaben abgeschlossen sind, erfolgt der Schlüsselverwaltungsprozess automatisch.

Das Flussdiagramm zeigt die allgemeinen Schritte zur Verwendung eines KMS zum Sichern von StorageGRID -Daten auf Appliance-Knoten.

Das Flussdiagramm zeigt, dass die KMS-Einrichtung und die Einrichtung der Appliance parallel erfolgen. Sie können die Schlüsselverwaltungsserver jedoch je nach Ihren Anforderungen vor oder nach der Aktivierung der Knotenverschlüsselung für neue Appliance-Knoten einrichten.

Einrichten des Schlüsselverwaltungsservers (KMS)

Das Einrichten eines Schlüsselverwaltungsservers umfasst die folgenden allgemeinen Schritte.

Schritt	Siehe
Greifen Sie auf die KMS-Software zu und fügen Sie jedem KMS oder KMS-Cluster einen Client für StorageGRID hinzu.	"Konfigurieren Sie StorageGRID als Client im KMS"
Besorgen Sie sich die erforderlichen Informationen für den StorageGRID -Client auf dem KMS.	"Konfigurieren Sie StorageGRID als Client im KMS"
Fügen Sie das KMS zum Grid Manager hinzu, weisen Sie es einer einzelnen Site oder einer Standardgruppe von Sites zu, laden Sie die erforderlichen Zertifikate hoch und speichern Sie die KMS-Konfiguration.	"Hinzufügen eines Schlüsselverwaltungsservers (KMS)"

Einrichten der Appliance

Das Einrichten eines Appliance-Knotens für die KMS-Verwendung umfasst die folgenden allgemeinen Schritte.

1. Verwenden Sie während der Hardwarekonfigurationsphase der Appliance-Installation das StorageGRID Appliance Installer, um die Einstellung **Knotenverschlüsselung** für die Appliance zu aktivieren.

   > ⓘ Sie können die Einstellung **Knotenverschlüsselung** nicht aktivieren, nachdem eine Appliance zum Grid hinzugefügt wurde, und Sie können die externe Schlüsselverwaltung nicht für Appliances verwenden, bei denen die Knotenverschlüsselung nicht aktiviert ist.

2. Führen Sie das StorageGRID Appliance-Installationsprogramm aus. Während der Installation wird jedem Appliance-Volume wie folgt ein zufälliger Datenverschlüsselungsschlüssel (DEK) zugewiesen:
   - Die DEKs werden zum Verschlüsseln der Daten auf jedem Volume verwendet. Diese Schlüssel werden mithilfe der Linux Unified Key Setup (LUKS)-Festplattenverschlüsselung im Betriebssystem der Appliance generiert und können nicht geändert werden.
   - Jeder einzelne DEK wird durch einen Master-Key-Verschlüsselungsschlüssel (KEK) verschlüsselt. Der anfängliche KEK ist ein temporärer Schlüssel, der die DEKs verschlüsselt, bis das Gerät eine Verbindung zum KMS herstellen kann.
3. Fügen Sie den Appliance-Knoten zu StorageGRID hinzu.

Sehen "Knotenverschlüsselung aktivieren" für Details.

Schlüsselverwaltungs-Verschlüsselungsprozess (erfolgt automatisch)

Die Schlüsselverwaltungsverschlüsselung umfasst die folgenden Schritte auf hoher Ebene, die automatisch ausgeführt werden.

1. Wenn Sie eine Appliance mit aktivierter Knotenverschlüsselung im Grid installieren, ermittelt StorageGRID , ob für die Site, die den neuen Knoten enthält, eine KMS-Konfiguration vorhanden ist.
   - Wenn für die Site bereits ein KMS konfiguriert wurde, erhält die Appliance die KMS-Konfiguration.
   - Wenn für die Site noch kein KMS konfiguriert wurde, werden die Daten auf der Appliance weiterhin durch den temporären KEK verschlüsselt, bis Sie für die Site ein KMS 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. Das KMS sendet einen Verschlüsselungsschlüssel an das Gerät. Der neue Schlüssel vom KMS ersetzt den temporären KEK und wird nun zum Verschlüsseln und Entschlüsseln der DEKs für die Appliance-Volumes verwendet.

> Alle Daten, die vorhanden sind, bevor der verschlüsselte Appliance-Knoten eine Verbindung zum konfigurierten KMS herstellt, werden mit einem temporären Schlüssel verschlüsselt. Allerdings sollten die Appliance-Volumes erst dann als vor der Entfernung aus dem Rechenzentrum geschützt betrachtet werden, wenn der temporäre Schlüssel durch den KMS-Verschlüsselungsschlüssel ersetzt wurde.

4. Wenn das Gerät eingeschaltet oder neu gestartet wird, stellt es erneut eine Verbindung zum KMS her, um den Schlüssel anzufordern. Der im flüchtigen Speicher gespeicherte Schlüssel übersteht einen Stromausfall oder Neustart nicht.

Überlegungen und Anforderungen zur Verwendung eines Schlüsselverwaltungsservers

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

Welche Version von KMIP wird unterstützt?

StorageGRID unterstützt KMIP Version 1.4.

"Key Management Interoperability Protocol-Spezifikation Version 1.4"

Welche Netzwerkaspekte sind zu berücksichtigen?

Die Netzwerk-Firewall-Einstellungen müssen jedem Appliance-Knoten die Kommunikation über den für die KMIP-Kommunikation (Key Management Interoperability Protocol) verwendeten Port ermöglichen. Der Standard-KMIP-Port ist 5696.

Sie müssen sicherstellen, dass jeder Appliance-Knoten, der Knotenverschlüsselung verwendet, Netzwerkzugriff auf den KMS oder KMS-Cluster hat, den Sie für die Site konfiguriert haben.

Welche TLS-Versionen werden unterstützt?

Die Kommunikation zwischen den Appliance-Knoten und dem konfigurierten KMS erfolgt über sichere TLS-Verbindungen. StorageGRID kann entweder das TLS 1.2- oder das TLS 1.3-Protokoll unterstützen, wenn es KMIP-Verbindungen zu einem KMS oder KMS-Cluster herstellt, je nachdem, was das KMS unterstützt und welche"TLS- und SSH-Richtlinie" Sie verwenden.

StorageGRID handelt beim Herstellen der Verbindung das Protokoll und die Verschlüsselung (TLS 1.2) oder die Verschlüsselungssuite (TLS 1.3) mit dem KMS aus. Um zu sehen, welche Protokollversionen und Chiffren/Chiffrensammlungen verfügbar sind, lesen Sie die `tlsOutbound` Abschnitt der aktiven TLS- und SSH-Richtlinie des Grids (**KONFIGURATION** > **Sicherheit Sicherheitseinstellungen**).

Welche Geräte werden unterstützt?

Sie können einen Schlüsselverwaltungsserver (KMS) verwenden, um Verschlüsselungsschlüssel für jedes StorageGRID Gerät in Ihrem Grid zu verwalten, bei dem die Einstellung **Knotenverschlüsselung** aktiviert ist. Diese Einstellung kann nur während der Hardwarekonfigurationsphase der Geräteinstallation mit dem StorageGRID Appliance Installer aktiviert werden.

> Sie können die Knotenverschlüsselung nicht aktivieren, nachdem ein Gerät zum Grid hinzugefügt wurde, und Sie können die externe Schlüsselverwaltung nicht für Geräte verwenden, bei denen die Knotenverschlüsselung nicht aktiviert ist.

Sie können das konfigurierte KMS für StorageGRID -Geräte und Geräteknoten verwenden.

Sie können den konfigurierten KMS nicht für softwarebasierte (nicht-Appliance-)Knoten verwenden, einschließlich der folgenden:

- Als virtuelle Maschinen (VMs) bereitgestellte Knoten
- In Container-Engines auf Linux-Hosts bereitgestellte Knoten

Auf diesen anderen Plattformen bereitgestellte Knoten können die Verschlüsselung außerhalb von StorageGRID auf Datenspeicher- oder Festplattenebene verwenden.

Wann sollte ich Schlüsselverwaltungsserver konfigurieren?

Bei einer Neuinstallation sollten Sie normalerweise einen oder mehrere Schlüsselverwaltungsserver im Grid Manager einrichten, bevor Sie Mandanten erstellen. Diese Reihenfolge stellt sicher, dass die Knoten geschützt sind, bevor Objektdaten auf ihnen gespeichert werden.

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

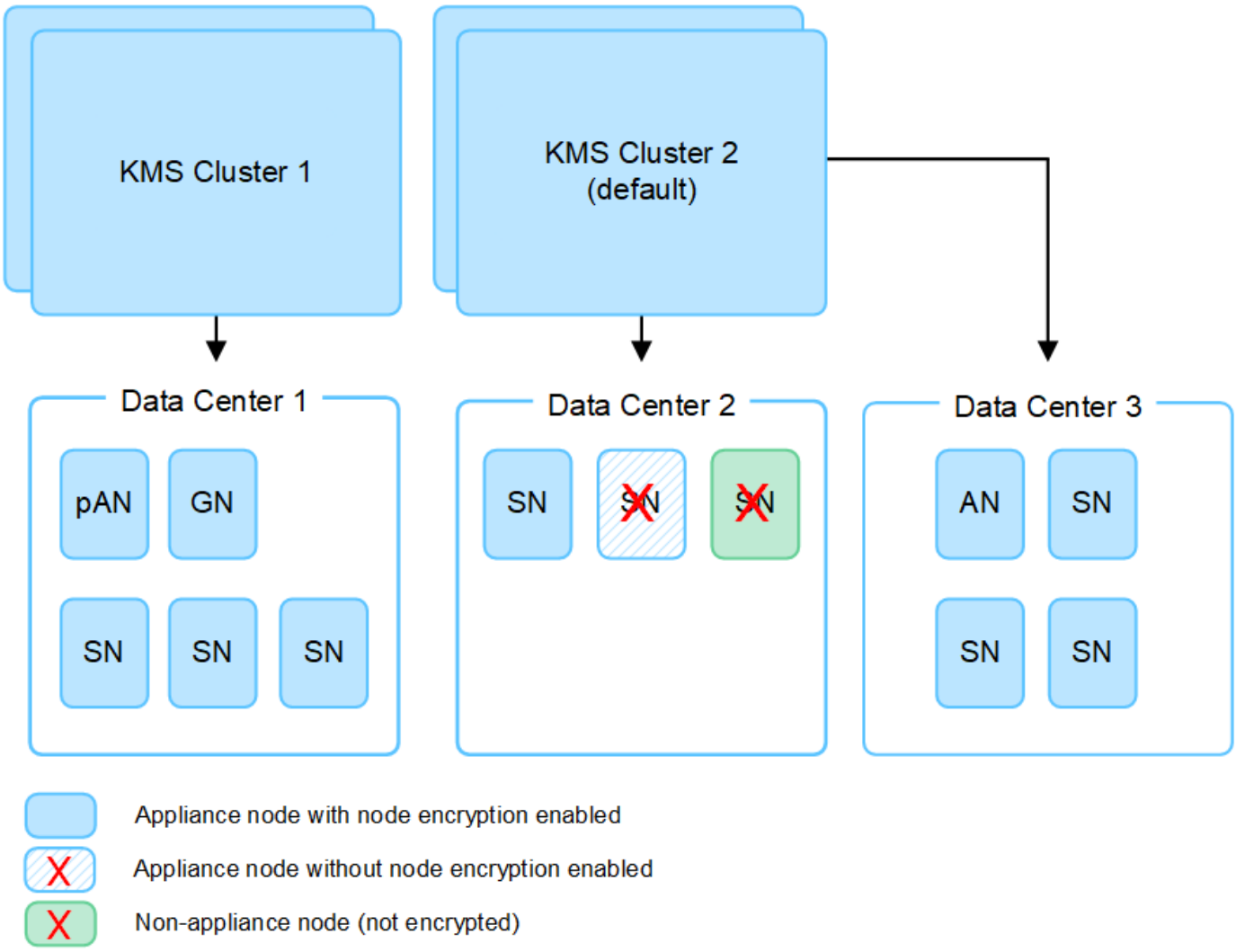
Wie viele Schlüsselverwaltungsserver benötige ich?

Sie können einen oder mehrere externe Schlüsselverwaltungsserver konfigurieren, um den Appliance-Knoten in Ihrem StorageGRID System Verschlüsselungsschlüssel bereitzustellen. Jeder KMS stellt den StorageGRID Appliance-Knoten an einem einzelnen Standort oder einer Gruppe von Standorten einen einzelnen Verschlüsselungsschlüssel bereit.

StorageGRID unterstützt die Verwendung von KMS-Clustern. Jeder KMS-Cluster enthält mehrere replizierte Schlüsselverwaltungsserver, die Konfigurationseinstellungen und Verschlüsselungsschlüssel gemeinsam nutzen. Die Verwendung von KMS-Clustern für die Schlüsselverwaltung wird empfohlen, da dadurch die Failover-Funktionen einer Hochverfügbarkeitskonfiguration verbessert werden.

Nehmen wir beispielsweise an, Ihr StorageGRID -System verfügt über drei Rechenzentrumsstandorte. Sie können einen KMS-Cluster so konfigurieren, dass er allen Appliance-Knoten im Rechenzentrum 1 einen Schlüssel bereitstellt, und einen zweiten KMS-Cluster, der allen Appliance-Knoten an allen anderen Standorten einen Schlüssel bereitstellt. Wenn Sie den zweiten KMS-Cluster hinzufügen, können Sie ein Standard-KMS für Data Center 2 und Data Center 3 konfigurieren.

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



Was passiert, wenn ein Schlüssel rotiert wird?

Als bewährte Sicherheitsmaßnahme sollten Sie regelmäßig"Rotieren Sie den Verschlüsselungsschlüssel" wird von jedem konfigurierten KMS verwendet.

Wenn die neue Schlüsselversion verfügbar ist:

- Es wird automatisch an die verschlüsselten Appliance-Knoten an dem oder den mit dem KMS verbundenen Standorten verteilt. Die Verteilung sollte innerhalb einer Stunde nach der Schlüsselrotation erfolgen.
- Wenn der verschlüsselte Appliance-Knoten offline ist, wenn die neue Schlüsselversion verteilt wird, erhält der Knoten den neuen Schlüssel, sobald er neu gestartet wird.
- Wenn die neue Schlüsselversion aus irgendeinem Grund nicht zum Verschlüsseln von Appliance-Volumes verwendet werden kann, wird für den Appliance-Knoten die Warnung **Rotation des KMS-Verschlüsselungsschlüssels fehlgeschlagen** ausgelöst. Möglicherweise müssen Sie sich an den technischen Support wenden, um Hilfe bei der Lösung dieser Warnung zu erhalten.

Kann ich einen Appliance-Knoten nach der Verschlüsselung wiederverwenden?

Wenn Sie ein verschlüsseltes Gerät in einem anderen StorageGRID -System installieren müssen, müssen Sie zuerst den Grid-Knoten außer Betrieb nehmen, um Objektdaten auf einen anderen Knoten zu verschieben.

Anschließend können Sie den StorageGRID Appliance Installer verwenden, um "Löschen Sie die KMS-Konfiguration" . Durch das Löschen der KMS-Konfiguration wird die Einstellung **Knotenverschlüsselung** deaktiviert und die Verknüpfung zwischen dem Appliance-Knoten und der KMS-Konfiguration für die StorageGRID -Site entfernt.

> Ohne Zugriff auf den KMS-Verschlüsselungsschlüssel sind alle auf dem Gerät verbleibenden Daten nicht mehr zugänglich und dauerhaft gesperrt.

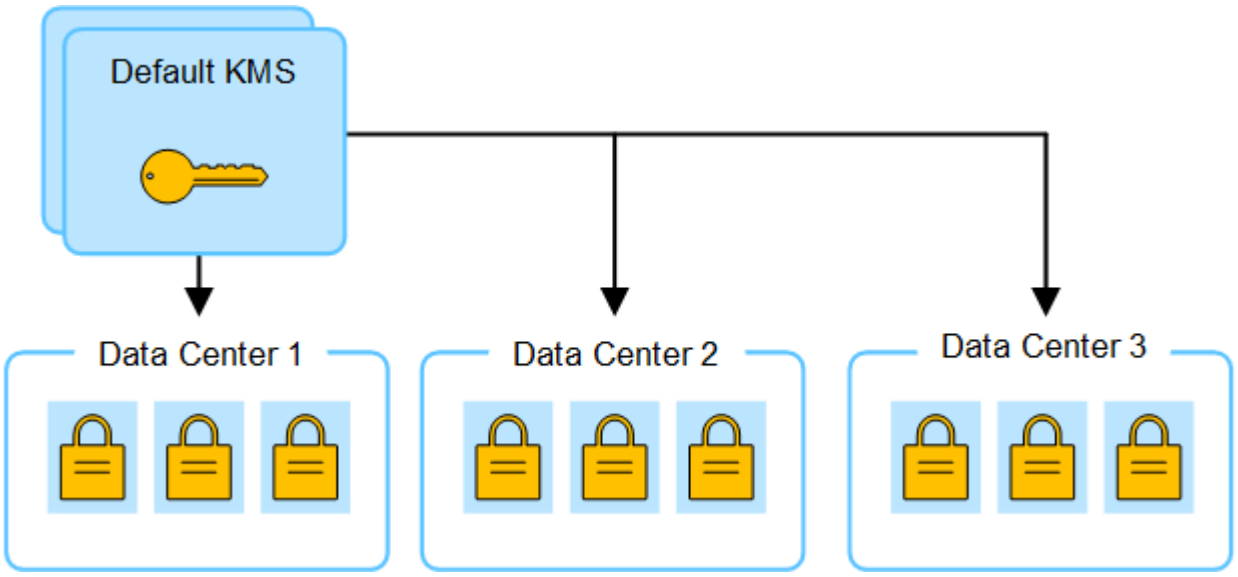
Überlegungen zum Ändern des KMS für eine Site

Jeder Schlüsselverwaltungsserver (KMS) oder KMS-Cluster stellt allen Appliance-Knoten an einem einzelnen Standort oder einer Gruppe von Standorten einen Verschlüsselungsschlüssel bereit. Wenn Sie ändern müssen, welches KMS für eine Site verwendet wird, müssen Sie möglicherweise den Verschlüsselungsschlüssel von einem KMS in ein anderes kopieren.

Wenn Sie das für eine Site verwendete KMS ändern, müssen Sie sicherstellen, dass die zuvor verschlüsselten Appliance-Knoten an dieser Site 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 in das neue KMS kopieren. Sie müssen sicherstellen, dass das KMS über den richtigen Schlüssel zum Entschlüsseln der verschlüsselten Appliance-Knoten am Standort verfügt.

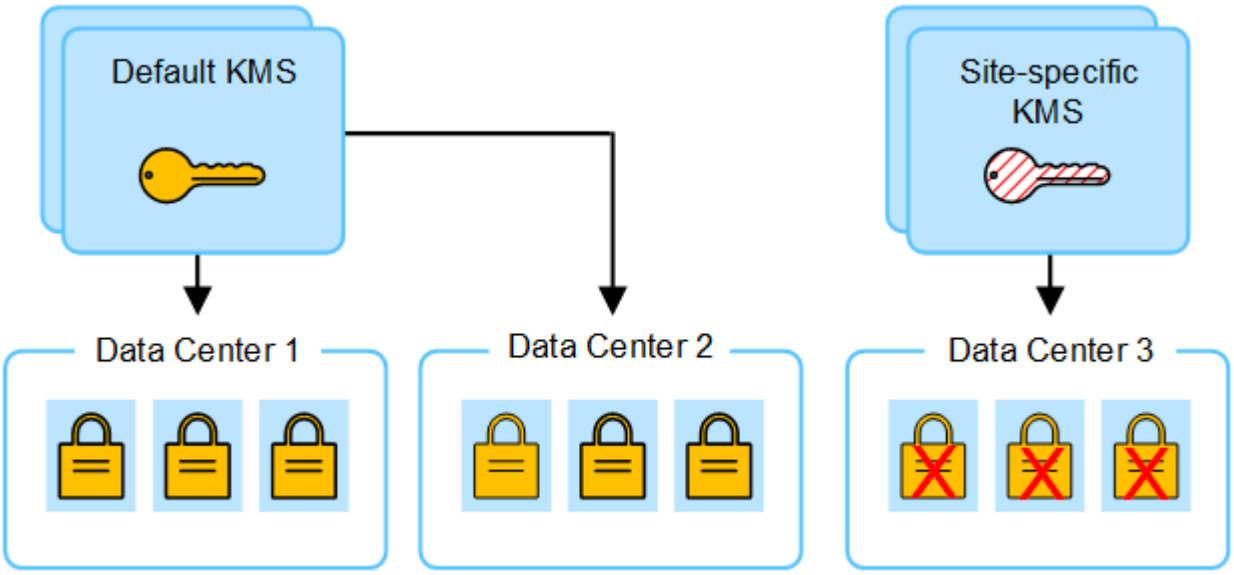
Beispiel:

1. Sie konfigurieren zunächst ein Standard-KMS, das für alle Sites gilt, die nicht über ein dediziertes KMS verfügen.
2. Wenn das KMS gespeichert ist, stellen alle Appliance-Knoten, bei denen die Einstellung **Knotenverschlüsselung** aktiviert ist, eine Verbindung zum KMS her und fordern den Verschlüsselungsschlüssel an. Dieser Schlüssel wird zum Verschlüsseln der Appliance-Knoten an allen Standorten verwendet. Derselbe Schlüssel muss auch zum Entschlüsseln dieser Geräte verwendet werden.

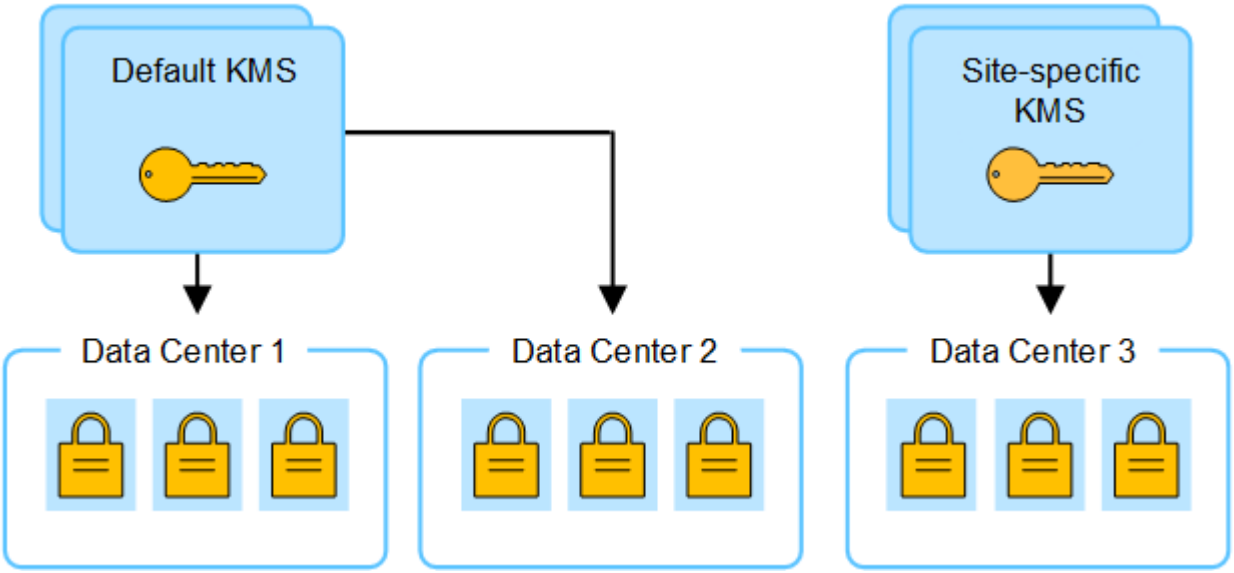


3. Sie entscheiden sich, für einen Standort (Rechenzentrum 3 in der Abbildung) ein standortspezifisches KMS hinzuzufügen. Da die Appliance-Knoten jedoch bereits verschlüsselt sind, tritt ein Validierungsfehler auf, wenn Sie versuchen, die Konfiguration für das standortspezifische KMS zu speichern. Der Fehler tritt

auf, weil das standortspezifische KMS nicht über den richtigen Schlüssel zum Entschlüsseln der Knoten an diesem Standort verfügt.



4. Um das Problem zu beheben, kopieren Sie die aktuelle Version des Verschlüsselungsschlüssels vom Standard-KMS in das neue KMS. (Technisch gesehen kopieren Sie den Originalschlüssel in einen neuen Schlüssel mit demselben Alias. Der Originalschlüssel wird zu einer früheren Version des neuen Schlüssels.) Das standortspezifische KMS verfügt jetzt über den richtigen Schlüssel zum Entschlüsseln der Appliance-Knoten im Rechenzentrum 3, sodass es in StorageGRID gespeichert werden kann.



Anwendungsfälle zum Ändern des für eine Site verwendeten KMS

Die Tabelle fasst die erforderlichen Schritte für die gängigsten Fälle zum Ändern des KMS für eine Site zusammen.

Anwendungsfall zum Ändern des KMS einer Site	Erforderliche Schritte
Sie haben einen oder mehrere standortspezifische KMS-Einträge und möchten einen davon als Standard-KMS verwenden.	Bearbeiten Sie das standortspezifische KMS. Wählen Sie im Feld **Verwaltet Schlüssel für** die Option **Sites, die nicht von einem anderen KMS verwaltet werden (Standard-KMS)** aus. Das standortspezifische KMS wird jetzt als Standard-KMS verwendet. Dies gilt für alle Sites, die nicht über ein dediziertes KMS verfügen. "Bearbeiten eines Schlüsselverwaltungsservers (KMS)"
Sie haben ein Standard-KMS und fügen in einer Erweiterung eine neue Site hinzu. Sie möchten für die neue Site nicht das Standard-KMS verwenden.	1. Wenn die Appliance-Knoten am neuen Standort bereits vom Standard-KMS verschlüsselt wurden, verwenden Sie die KMS-Software, um die aktuelle Version des Verschlüsselungsschlüssels vom Standard-KMS auf ein neues KMS zu kopieren. 2. Fügen Sie mithilfe des Grid Managers das neue KMS hinzu und wählen Sie die Site aus. "Hinzufügen eines Schlüsselverwaltungsservers (KMS)"
Sie möchten, dass das KMS für eine Site einen anderen Server verwendet.	1. Wenn die Appliance-Knoten am Standort bereits vom vorhandenen KMS verschlüsselt wurden, verwenden Sie die KMS-Software, um die aktuelle Version des Verschlüsselungsschlüssels vom vorhandenen KMS auf das neue KMS zu kopieren. 2. Bearbeiten Sie mithilfe des Grid Managers die vorhandene KMS-Konfiguration und geben Sie den neuen Hostnamen oder die neue IP-Adresse ein. "Hinzufügen eines Schlüsselverwaltungsservers (KMS)"

Konfigurieren Sie StorageGRID als Client im KMS

Sie müssen StorageGRID als Client für jeden externen Schlüsselverwaltungsserver oder KMS-Cluster konfigurieren, bevor Sie das KMS zu StorageGRID hinzufügen können.

Diese Anweisungen gelten für Thales CipherTrust Manager und Hashicorp Vault. Eine Liste der unterstützten Produkte und Versionen finden Sie im "NetApp Interoperability Matrix Tool (IMT)" .

Schritte

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

   Jedes KMS verwaltet einen einzelnen Verschlüsselungsschlüssel für die StorageGRID -Geräteknoten an einem einzelnen Standort oder einer Gruppe von Standorten.

2. Erstellen Sie einen Schlüssel mit einer der folgenden beiden Methoden:
   - Verwenden Sie die Schlüsselverwaltungsseite Ihres KMS-Produkts. Erstellen Sie für jeden KMS oder KMS-Cluster einen AES-Verschlüsselungsschlüssel.

     Der Verschlüsselungsschlüssel muss mindestens 2.048 Bit lang sein und exportierbar sein.

- Lassen Sie den Schlüssel von StorageGRID erstellen. Sie werden beim Testen und Speichern danach aufgefordert"Hochladen von Client-Zertifikaten" .

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

   Sie benötigen diese Informationen, wenn Sie das KMS zu StorageGRID hinzufügen:

   - Hostname oder IP-Adresse für jeden Server.
   - Vom KMS verwendeter KMIP-Port.
   - Schlüsselalias für den Verschlüsselungsschlüssel im KMS.

4. Besorgen Sie sich für jeden KMS oder KMS-Cluster ein von einer Zertifizierungsstelle (CA) signiertes Serverzertifikat oder ein Zertifikatspaket, das alle PEM-codierten CA-Zertifikatsdateien enthält, die in der Reihenfolge der Zertifikatskette aneinandergereiht sind.

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

   - Das Zertifikat muss das Base-64-codierte X.509-Format von Privacy Enhanced Mail (PEM) verwenden.
   - Das Feld „Subject Alternative Name“ (SAN) in jedem Serverzertifikat muss den vollqualifizierten 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 in das Feld **Hostname** eingeben.

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

5. Besorgen Sie sich das öffentliche Client-Zertifikat, das vom externen KMS an StorageGRID ausgestellt wurde, und den privaten Schlüssel für das Client-Zertifikat.

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

Hinzufügen eines Schlüsselverwaltungsservers (KMS)

Sie verwenden den StorageGRID Key Management Server-Assistenten, um jeden KMS oder KMS-Cluster hinzuzufügen.

Bevor Sie beginnen

- Sie haben die"Überlegungen und Anforderungen zur Verwendung eines Schlüsselverwaltungsservers" .
- Du hast"StorageGRID als Client im KMS konfiguriert" , und Sie verfügen über die erforderlichen Informationen für jeden KMS oder KMS-Cluster.
- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Root-Zugriffsberechtigung" .

Informationen zu diesem Vorgang

Konfigurieren Sie nach Möglichkeit alle standortspezifischen Schlüsselverwaltungsserver, bevor Sie ein Standard-KMS konfigurieren, das für alle Standorte gilt, die nicht von einem anderen KMS verwaltet werden. Wenn Sie zuerst das Standard-KMS erstellen, werden alle knotenverschlüsselten Appliances im Grid durch das Standard-KMS verschlüsselt. Wenn Sie später ein standortspezifisches KMS erstellen möchten, müssen Sie zunächst die aktuelle Version des Verschlüsselungsschlüssels vom Standard-KMS in das neue KMS

kopieren. Sehen"Überlegungen zum Ändern des KMS für eine Site" für Details.

Schritt 1: KMS-Details

In Schritt 1 (KMS-Details) des Assistenten „Schlüsselverwaltungsserver hinzufügen“ geben Sie Details zum KMS oder KMS-Cluster an.

Schritte

1. Wählen Sie **KONFIGURATION** > **Sicherheit** > **Schlüsselverwaltungsserver**.

   Die Seite „Schlüsselverwaltungsserver“ wird mit der ausgewählten Registerkarte „Konfigurationsdetails“ angezeigt.

2. Wählen Sie **Erstellen**.

   Schritt 1 (KMS-Details) des Assistenten „Schlüsselverwaltungsserver hinzufügen“ wird angezeigt.

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

Feld	Beschreibung
KMS-Name	Ein beschreibender Name, der Ihnen bei der Identifizierung dieses KMS hilft. Muss zwischen 1 und 64 Zeichen lang sein.
Schlüsselname	Der genaue Schlüsselalias für den StorageGRID -Client im KMS. Muss zwischen 1 und 255 Zeichen lang sein. **Hinweis**: Wenn Sie mit Ihrem KMS-Produkt keinen Schlüssel erstellt haben, werden Sie aufgefordert, den Schlüssel von StorageGRID erstellen zu lassen.
Verwaltet Schlüssel für	Die StorageGRID -Site, die mit diesem KMS verknüpft wird. Wenn möglich, sollten Sie alle standortspezifischen Schlüsselverwaltungsserver konfigurieren, bevor Sie ein Standard-KMS konfigurieren, das für alle Standorte gilt, die nicht von einem anderen KMS verwaltet werden. • Wählen Sie einen Standort aus, wenn dieses KMS die Verschlüsselungsschlüssel für die Appliance-Knoten an einem bestimmten Standort verwalten soll. • Wählen Sie **Sites, die nicht von einem anderen KMS verwaltet werden (Standard-KMS)** aus, um ein Standard-KMS zu konfigurieren, das für alle Sites gilt, die nicht über ein dediziertes KMS verfügen, sowie für alle Sites, die Sie in nachfolgenden Erweiterungen hinzufügen. **Hinweis:** Beim Speichern der KMS-Konfiguration tritt ein Validierungsfehler auf, wenn Sie eine Site auswählen, die zuvor vom Standard-KMS verschlüsselt wurde, Sie dem neuen KMS jedoch nicht die aktuelle Version des ursprünglichen Verschlüsselungsschlüssels bereitgestellt haben.

Feld	Beschreibung
Hafen	Der Port, den der KMS-Server für die KMIP-Kommunikation (Key Management Interoperability Protocol) verwendet. Der Standardwert ist 5696, der KMIP-Standardport.
Hostname	Der vollqualifizierte Domänenname oder die IP-Adresse für den KMS. **Hinweis:** Das Feld „Subject Alternative Name“ (SAN) 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 in einem KMS-Cluster herstellen.

4. Wenn Sie einen KMS-Cluster konfigurieren, wählen Sie **Weiteren Hostnamen hinzufügen** aus, um für jeden Server im Cluster einen Hostnamen hinzuzufügen.
5. Wählen Sie **Weiter**.

Schritt 2: Server-Zertifikat hochladen

In Schritt 2 (Serverzertifikat hochladen) des Assistenten „Schlüsselverwaltungsserver hinzufügen“ laden Sie das Serverzertifikat (oder Zertifikatspaket) für den KMS hoch. Das Serverzertifikat ermöglicht dem externen KMS, sich gegenüber StorageGRID zu authentifizieren.

Schritte

1. Navigieren Sie in **Schritt 2 (Serverzertifikat hochladen)** zum Speicherort des gespeicherten Serverzertifikats oder Zertifikatspakets.
2. Laden Sie die Zertifikatsdatei hoch.

   Die Metadaten des Serverzertifikats werden angezeigt.

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

3. Wählen Sie **Weiter**.

Schritt 3: Client-Zertifikate hochladen

In Schritt 3 (Client-Zertifikate hochladen) des Assistenten „Schlüsselverwaltungsserver hinzufügen“ laden Sie das Client-Zertifikat und den privaten Schlüssel des Client-Zertifikats hoch. Das Client-Zertifikat ermöglicht StorageGRID , sich gegenüber dem KMS zu authentifizieren.

Schritte

1. Navigieren Sie in **Schritt 3 (Client-Zertifikate hochladen)** zum Speicherort des Client-Zertifikats.
2. Laden Sie die Client-Zertifikatdatei hoch.

   Die Metadaten des Client-Zertifikats werden angezeigt.

3. Navigieren Sie zum Speicherort des privaten Schlüssels für das Client-Zertifikat.
4. Laden Sie die private Schlüsseldatei hoch.

5. Wählen Sie **Testen und speichern**.

   Wenn kein Schlüssel vorhanden ist, werden Sie aufgefordert, StorageGRID einen erstellen zu lassen.

   Die Verbindungen zwischen dem Schlüsselverwaltungsserver und den Appliance-Knoten werden getestet. Wenn alle Verbindungen gültig sind und der richtige Schlüssel auf dem KMS gefunden wird, wird der neue Schlüsselverwaltungsserver der Tabelle auf der Seite „Schlüsselverwaltungsserver“ hinzugefügt.

   > Unmittelbar nachdem Sie einen KMS hinzugefügt haben, wird der Zertifikatsstatus auf der Seite „Schlüsselverwaltungsserver“ als „Unbekannt“ angezeigt. Es kann bis zu 30 Minuten dauern, bis StorageGRID den tatsächlichen Status jedes Zertifikats abruft. Sie müssen Ihren Webbrowser aktualisieren, um den aktuellen Status anzuzeigen.

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

   Beispielsweise erhalten Sie möglicherweise den Fehler „422: Unprocessable Entity“, wenn ein Verbindungstest fehlgeschlagen ist.

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

   > Durch Auswahl von **Speichern erzwingen** wird die KMS-Konfiguration gespeichert, die externe Verbindung von jedem Gerät zu diesem KMS wird jedoch nicht getestet. Wenn ein Problem mit der Konfiguration vorliegt, können Sie Appliance-Knoten, bei denen die Knotenverschlüsselung am betroffenen Standort aktiviert ist, möglicherweise nicht neu starten. Bis zur Lösung der Probleme verlieren Sie möglicherweise den Zugriff auf Ihre Daten.

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, aber die Verbindung zum KMS wird nicht getestet.

Verwalten eines KMS

Die Verwaltung eines Schlüsselverwaltungsservers (KMS) umfasst das Anzeigen oder Bearbeiten von Details, das Verwalten von Zertifikaten, das Anzeigen verschlüsselter Knoten und das Entfernen eines KMS, wenn dieser nicht mehr benötigt wird.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"erforderliche Zugriffsberechtigung" .

KMS-Details anzeigen

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

Schritte

1. Wählen Sie **KONFIGURATION** > **Sicherheit** > **Schlüsselverwaltungsserver**.

Die Seite „Schlüsselverwaltungsserver“ wird angezeigt und zeigt die folgenden Informationen:

- Auf der Registerkarte „Konfigurationsdetails“ werden alle konfigurierten Schlüsselverwaltungsserver aufgelistet.
- Auf der Registerkarte „Verschlüsselte Knoten“ werden alle Knoten aufgelistet, bei denen die Knotenverschlüsselung aktiviert ist.

2. Um die Details für ein bestimmtes KMS anzuzeigen und Vorgänge auf diesem KMS auszuführen, wählen Sie den Namen des KMS aus. Auf der Detailseite für das KMS sind die folgenden Informationen aufgeführt:

Feld	Beschreibung
Verwaltet Schlüssel für	Die mit dem KMS verknüpfte StorageGRID -Site. In diesem Feld wird der Name einer bestimmten StorageGRID Site oder **Sites angezeigt, die nicht von einem anderen KMS verwaltet werden (Standard-KMS).**
Hostname	Der vollqualifizierte Domänenname oder die IP-Adresse des KMS. Wenn ein Cluster aus zwei Schlüsselverwaltungsservern vorhanden ist, werden die vollqualifizierten Domänennamen oder IP-Adressen beider Server aufgelistet. Wenn in einem Cluster mehr als zwei Schlüsselverwaltungsserver vorhanden sind, wird der vollqualifizierte Domänenname oder die IP-Adresse des ersten KMS zusammen mit der Anzahl der zusätzlichen Schlüsselverwaltungsserver im Cluster aufgelistet. Zum Beispiel: `10.10.10.10 and 10.10.10.11` oder `10.10.10.10 and 2 others`. Um alle Hostnamen in einem Cluster anzuzeigen, wählen Sie ein KMS aus und wählen Sie **Bearbeiten** oder **Aktionen** > **Bearbeiten**.

3. Wählen Sie auf der KMS-Detailseite eine Registerkarte aus, um die folgenden Informationen anzuzeigen:

Tab	Feld	Beschreibung
Wichtige Informationen	Schlüsselname	Der Schlüsselalias für den StorageGRID -Client im KMS.
Schlüssel-UID	Die eindeutige Kennung der neuesten Version des Schlüssels.	Zuletzt geändert
Datum und Uhrzeit der neuesten Version des Schlüssels.	Serverzertifikat	Metadaten

Tab	Feld	Beschreibung
Die Metadaten für das Zertifikat, wie Seriennummer, Ablaufdatum und -uhrzeit sowie das Zertifikat-PEM.	Zertifikat PEM	Der Inhalt der PEM-Datei (Privacy Enhanced Mail) für das Zertifikat.
Client-Zertifikat	Metadaten	Die Metadaten für das Zertifikat, wie Seriennummer, Ablaufdatum und -uhrzeit sowie das Zertifikat-PEM.

4. Wählen Sie so oft wie es die Sicherheitspraktiken Ihres Unternehmens erfordern **Schlüssel rotieren** oder verwenden Sie die KMS-Software, um eine neue Version des Schlüssels zu erstellen.

   Wenn die Schlüsselrotation erfolgreich war, werden die Felder „Schlüssel-UID“ und „Zuletzt geändert“ aktualisiert.

> Wenn Sie den Verschlüsselungsschlüssel mithilfe der KMS-Software rotieren, rotieren Sie ihn von der zuletzt verwendeten Version des Schlüssels zu einer neuen Version desselben Schlüssels. Wechseln Sie nicht zu einem völlig anderen Schlüssel.
>
> Versuchen Sie niemals, einen Schlüssel zu rotieren, indem Sie den Schlüsselnamen (Alias) für das KMS ändern. StorageGRID erfordert, dass alle zuvor verwendeten Schlüsselversionen (sowie alle zukünftigen) vom KMS mit demselben Schlüsselalias aus zugänglich sind. Wenn Sie den Schlüsselalias für ein konfiguriertes KMS ändern, kann StorageGRID Ihre Daten möglicherweise nicht entschlüsseln.

Zertifikate verwalten

Beheben Sie umgehend alle Probleme mit Server- oder Clientzertifikaten. Ersetzen Sie Zertifikate nach Möglichkeit vor ihrem Ablauf.

> Sie müssen alle Zertifikatsprobleme so schnell wie möglich beheben, um den Datenzugriff aufrechtzuerhalten.

Schritte

1. Wählen Sie **KONFIGURATION** > **Sicherheit** > **Schlüsselverwaltungsserver**.
2. Sehen Sie sich in der Tabelle den Wert für den Zertifikatsablauf für jeden KMS an.
3. Wenn das Ablaufdatum des Zertifikats für einen KMS unbekannt ist, warten Sie bis zu 30 Minuten und aktualisieren Sie dann Ihren Webbrowser.
4. Wenn in der Spalte „Zertifikatablauf“ angegeben ist, dass ein Zertifikat abgelaufen ist oder bald abläuft, wählen Sie das KMS aus, um zur KMS-Detailseite zu gelangen.
   a. Wählen Sie **Serverzertifikat** aus und überprüfen Sie den Wert für das Feld „Läuft ab am“.
   b. Um das Zertifikat zu ersetzen, wählen Sie **Zertifikat bearbeiten**, um ein neues Zertifikat hochzuladen.
   c. Wiederholen Sie diese Teilschritte und wählen Sie **Client-Zertifikat** anstelle von Server-Zertifikat.
5. Wenn die Warnungen **Ablauf des KMS-CA-Zertifikats**, **Ablauf des KMS-Client-Zertifikats** und **Ablauf des KMS-Server-Zertifikats** ausgelöst werden, notieren Sie sich die Beschreibung der einzelnen

Warnungen und führen Sie die empfohlenen Aktionen aus.

Es kann bis zu 30 Minuten dauern, bis StorageGRID Aktualisierungen zum Ablauf des Zertifikats erhält. Aktualisieren Sie Ihren Webbrowser, um die aktuellen Werte anzuzeigen.

Wenn Sie den Status „Serverzertifikatstatus unbekannt“ erhalten, stellen Sie sicher, dass Ihr KMS den Erhalt eines Serverzertifikats ohne Clientzertifikat zulässt.

Verschlüsselte Knoten anzeigen

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

Schritte

1. Wählen Sie **KONFIGURATION** > **Sicherheit** > **Schlüsselverwaltungsserver**.

   Die Seite „Schlüsselverwaltungsserver“ 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 Appliance-Knoten in Ihrem StorageGRID -System aufgelistet, für die die Einstellung **Knotenverschlüsselung** aktiviert ist.

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

Spalte	Beschreibung
Knotenname	Der Name des Appliance-Knotens.
Knotentyp	Der Knotentyp: Speicher, Admin oder Gateway.
Website	Der Name der StorageGRID -Site, an der der Knoten installiert ist.
KMS-Name	Der beschreibende Name des für den Knoten verwendeten KMS. Wenn kein KMS aufgeführt ist, wählen Sie die Registerkarte „Konfigurationsdetails“ aus, um ein KMS hinzuzufügen. "Hinzufügen eines Schlüsselverwaltungsservers (KMS)"
Schlüssel-UID	Die eindeutige ID des Verschlüsselungsschlüssels, der zum Verschlüsseln und Entschlüsseln von Daten auf dem Appliance-Knoten verwendet wird. Um eine vollständige Schlüssel-UID anzuzeigen, wählen Sie den Text aus. Ein Bindestrich (--) zeigt an, dass die Schlüssel-UID unbekannt ist, möglicherweise aufgrund eines Verbindungsproblems zwischen dem Appliance-Knoten und dem KMS.

Spalte	Beschreibung
Status	Der Status der Verbindung zwischen dem KMS und dem Appliance-Knoten. Wenn der Knoten verbunden ist, wird der Zeitstempel alle 30 Minuten aktualisiert. Es kann mehrere Minuten dauern, bis der Verbindungsstatus nach Änderungen der KMS-Konfiguration aktualisiert wird. **Hinweis:** Aktualisieren Sie Ihren Webbrowser, um die neuen Werte anzuzeigen.

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

   Während des normalen KMS-Betriebs lautet der Status **Mit KMS verbunden**. Wenn ein Knoten vom Netz getrennt wird, wird der Verbindungsstatus des Knotens angezeigt (Administrativ deaktiviert oder Unbekannt).

   Andere Statusmeldungen entsprechen StorageGRID -Warnungen mit denselben Namen:

   - KMS-Konfiguration konnte nicht geladen werden
   - KMS-Konnektivitätsfehler
   - Name des KMS-Verschlüsselungsschlüssels nicht gefunden
   - Fehler bei der Rotation des KMS-Verschlüsselungsschlüssels
   - KMS-Schlüssel konnte ein Appliance-Volume nicht entschlüsseln
   - KMS ist nicht konfiguriert

   Führen Sie die empfohlenen Aktionen für diese Warnungen aus.

> ! Sie müssen alle Probleme sofort beheben, um sicherzustellen, dass Ihre Daten vollständig geschützt sind.

Bearbeiten eines KMS

Möglicherweise müssen Sie die Konfiguration eines Schlüsselverwaltungsservers bearbeiten, beispielsweise wenn ein Zertifikat bald abläuft.

Bevor Sie beginnen

- Wenn Sie die für ein KMS ausgewählte Site aktualisieren möchten, haben Sie die"Überlegungen zum Ändern des KMS für eine Site" .
- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Root-Zugriffsberechtigung" .

Schritte

1. Wählen Sie **KONFIGURATION** > **Sicherheit** > **Schlüsselverwaltungsserver**.

   Die Seite „Schlüsselverwaltungsserver“ wird angezeigt und zeigt alle konfigurierten Schlüsselverwaltungsserver.

2. Wählen Sie das KMS aus, das Sie bearbeiten möchten, und wählen Sie **Aktionen** > **Bearbeiten**.

   Sie können ein KMS auch bearbeiten, indem Sie den KMS-Namen in der Tabelle auswählen und auf der

KMS-Detailseite **Bearbeiten** auswählen.

3. Aktualisieren Sie optional die Details in **Schritt 1 (KMS-Details)** des Assistenten „Schlüsselverwaltungsserver bearbeiten“.

Feld	Beschreibung
KMS-Name	Ein beschreibender Name, der Ihnen bei der Identifizierung dieses KMS hilft. Muss zwischen 1 und 64 Zeichen lang sein.
Schlüsselname	Der genaue Schlüsselalias für den StorageGRID -Client im KMS. Muss zwischen 1 und 255 Zeichen lang sein. Nur in seltenen Fällen müssen Sie den Schlüsselnamen bearbeiten. Beispielsweise müssen Sie den Schlüsselnamen bearbeiten, wenn der Alias im KMS umbenannt wird oder wenn alle Versionen des vorherigen Schlüssels in den Versionsverlauf des neuen Alias kopiert wurden.
Verwaltet Schlüssel für	Wenn Sie ein standortspezifisches KMS bearbeiten und noch kein Standard-KMS haben, wählen Sie optional **Standorte, die nicht von einem anderen KMS verwaltet werden (Standard-KMS)** aus. Diese Auswahl konvertiert ein standortspezifisches KMS in das Standard-KMS, das für alle Standorte gilt, die kein dediziertes KMS haben, und für alle Standorte, die in einer Erweiterung hinzugefügt werden. **Hinweis:** Wenn Sie ein standortspezifisches KMS bearbeiten, können Sie keine andere Site auswählen. Wenn Sie das Standard-KMS bearbeiten, können Sie keine bestimmte Site auswählen.
Hafen	Der Port, den der KMS-Server für die KMIP-Kommunikation (Key Management Interoperability Protocol) verwendet. Der Standardwert ist 5696, der KMIP-Standardport.
Hostname	Der vollqualifizierte Domänenname oder die IP-Adresse für den KMS. **Hinweis:** Das Feld „Subject Alternative Name“ (SAN) 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 in einem KMS-Cluster herstellen.

4. Wenn Sie einen KMS-Cluster konfigurieren, wählen Sie **Weiteren Hostnamen hinzufügen** aus, um für jeden Server im Cluster einen Hostnamen hinzuzufügen.
5. Wählen Sie **Weiter**.

   Schritt 2 (Serverzertifikat hochladen) des Assistenten „Schlüsselverwaltungsserver 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 (Client-Zertifikate hochladen) des Assistenten „Schlüsselverwaltungsserver bearbeiten“ wird

angezeigt.

8. Wenn Sie das Client-Zertifikat und den privaten Schlüssel des Client-Zertifikats ersetzen müssen, wählen Sie **Durchsuchen** und laden Sie die neuen Dateien hoch.
9. Wählen Sie **Testen und speichern**.

   Die Verbindungen zwischen dem Schlüsselverwaltungsserver und allen knotenverschlüsselten Appliance-Knoten an den betroffenen Standorten werden getestet. Wenn alle Knotenverbindungen gültig sind und der richtige Schlüssel auf dem KMS gefunden wird, wird der Schlüsselverwaltungsserver der Tabelle auf der Seite „Schlüsselverwaltungsserver“ hinzugefügt.

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

    Beispielsweise erhalten Sie möglicherweise den Fehler „422: Unprocessable Entity“, wenn die Site, die Sie für dieses KMS ausgewählt haben, 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 **Speichern erzwingen**.

    > Durch Auswahl von **Speichern erzwingen** wird die KMS-Konfiguration gespeichert, die externe Verbindung von jedem Gerät zu diesem KMS wird jedoch nicht getestet. Wenn ein Problem mit der Konfiguration vorliegt, können Sie Appliance-Knoten, bei denen die Knotenverschlüsselung am betroffenen Standort aktiviert ist, möglicherweise nicht neu starten. Bis zur Lösung der Probleme verlieren Sie möglicherweise den Zugriff auf Ihre Daten.

    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 Schlüsselverwaltungsservers (KMS)

In manchen Fällen möchten Sie möglicherweise einen Schlüsselverwaltungsserver entfernen. Beispielsweise möchten Sie möglicherweise ein standortspezifisches KMS entfernen, wenn Sie die Site außer Betrieb genommen haben.

Bevor Sie beginnen

- Sie haben die"Überlegungen und Anforderungen zur Verwendung eines Schlüsselverwaltungsservers" .
- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"Root-Zugriffsberechtigung" .

Informationen zu diesem Vorgang

Sie können einen KMS in folgenden Fällen entfernen:

- Sie können ein standortspezifisches KMS entfernen, wenn der Standort außer Betrieb genommen wurde oder wenn der Standort keine Appliance-Knoten mit aktivierter Knotenverschlüsselung enthält.
- Sie können das Standard-KMS entfernen, wenn für jeden Standort mit Appliance-Knoten und aktivierter Knotenverschlüsselung bereits ein standortspezifischer KMS vorhanden ist.

Schritte

1. Wählen Sie **KONFIGURATION** > **Sicherheit** > **Schlüsselverwaltungsserver**.

   Die Seite „Schlüsselverwaltungsserver“ wird angezeigt und zeigt alle konfigurierten Schlüsselverwaltungsserver.

2. Wählen Sie das KMS aus, das Sie entfernen möchten, und wählen Sie **Aktionen** > **Entfernen**.

   Sie können ein KMS auch entfernen, indem Sie den KMS-Namen in der Tabelle auswählen und auf der KMS-Detailseite **Entfernen** auswählen.

3. Bestätigen Sie, dass Folgendes zutrifft:
   - Sie entfernen ein standortspezifisches KMS für eine Site, die keinen Appliance-Knoten mit aktivierter Knotenverschlüsselung hat.
   - Sie entfernen das Standard-KMS, aber für jede Site ist bereits ein standortspezifisches KMS mit Knotenverschlüsselung vorhanden.
4. Wählen Sie **Ja**.

   Die KMS-Konfiguration wird entfernt.