



Konfigurieren von Verschlüsselungsmanagement-Servern

StorageGRID 11.7

NetApp
April 12, 2024

Inhalt

Konfigurieren von Verschlüsselungsmanagement-Servern	1
Key Management-Server konfigurieren: Übersicht	1
Überblick über die KMS- und Appliance-Konfiguration	1
Überlegungen und Anforderungen für die Verwendung eines Verschlüsselungsmanagement-Servers	4
Überlegungen für das Ändern des KMS für einen Standort	7
Konfigurieren Sie StorageGRID als Client im KMS	10
Hinzufügen eines Verschlüsselungsmanagement-Servers (KMS)	11
KMS-Details anzeigen	18
Verschlüsselte Nodes anzeigen	20
Bearbeiten eines Verschlüsselungsmanagement-Servers (KMS)	21
Entfernen eines Verschlüsselungsmanagement-Servers (KMS)	23

Konfigurieren von Verschlüsselungsmanagement-Servern

Key Management-Server konfigurieren: Übersicht

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 wurden, können Sie nur auf Daten auf der Appliance zugreifen, wenn der Node mit dem KMS kommunizieren kann.

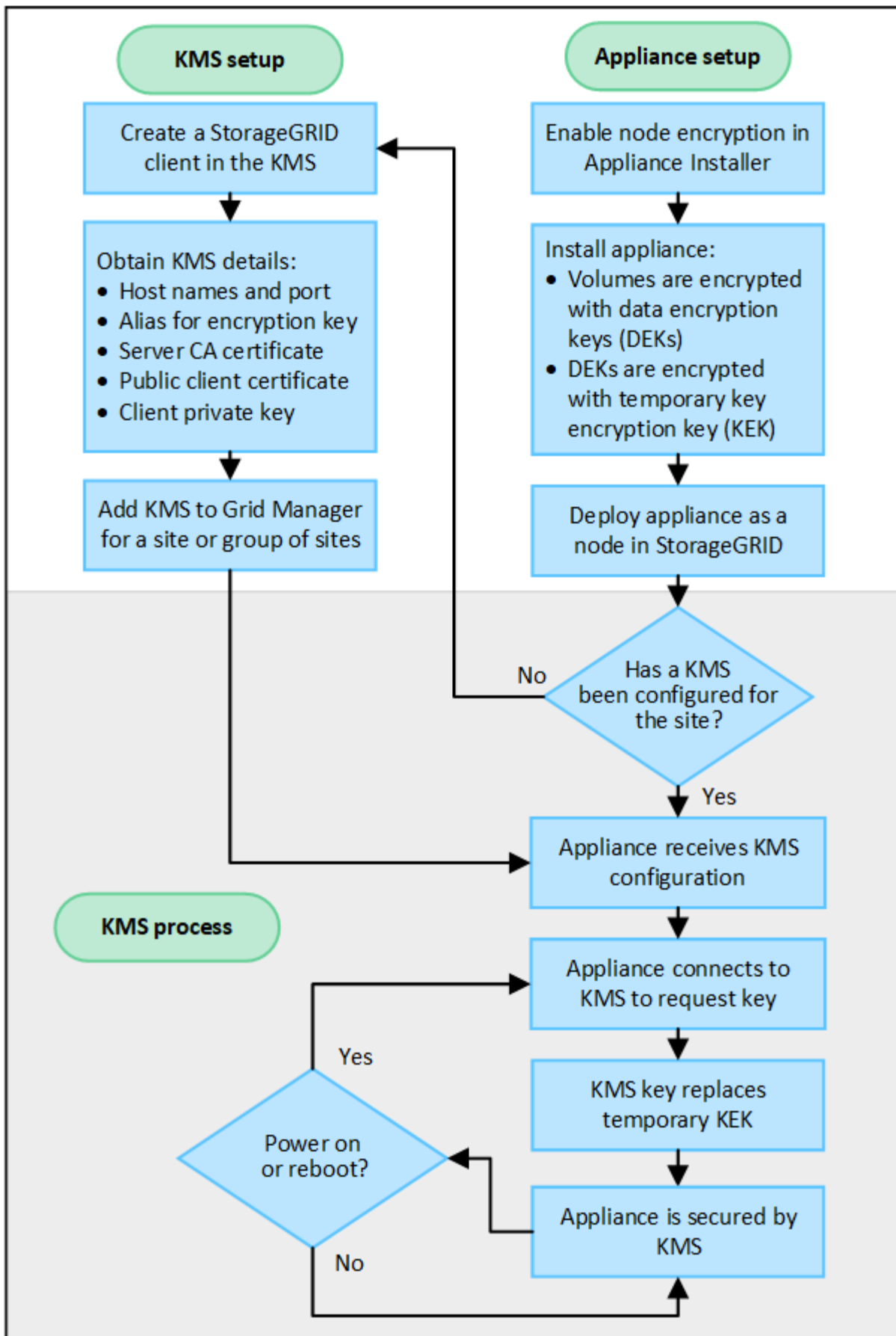


StorageGRID erstellt oder verwaltet keine externen Schlüssel, die zur Verschlüsselung und Entschlüsselung von Appliance-Nodes verwendet werden. Wenn Sie Vorhaben, einen externen Verschlüsselungsmanagementserver zum Schutz von StorageGRID-Daten zu verwenden, müssen Sie wissen, wie Sie diesen Server einrichten, 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.

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 Sie StorageGRID als Client im KMS"
Erhalten Sie die erforderlichen Informationen für den StorageGRID-Client auf dem KMS.	"Konfigurieren Sie 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)"

Richten Sie das Gerät ein

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 eine Appliance zum Grid hinzugefügt wurde, und Sie können keine externe Schlüsselverwaltung für Geräte verwenden, für die keine Knotenverschlüsselung 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 Betriebssystem der Appliance 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.

Siehe ["Aktivieren Sie die Node-Verschlüsselung"](#) Entsprechende Details.

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 ist, kann einen Stromausfall oder einen Neustart nicht überleben.

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 kann die Node-Verschlüsselung nicht aktiviert werden. Zudem kann kein externes Verschlüsselungsmanagement für Appliances verwendet werden, bei denen die Node-Verschlüsselung nicht aktiviert ist.

Sie können das konfigurierte KMS für StorageGRID-Appliances und Appliance-Nodes verwenden.

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

- Als Virtual Machines (VMs) implementierte Nodes
- Nodes, die in Container-Engines auf Linux Hosts implementiert sind

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.

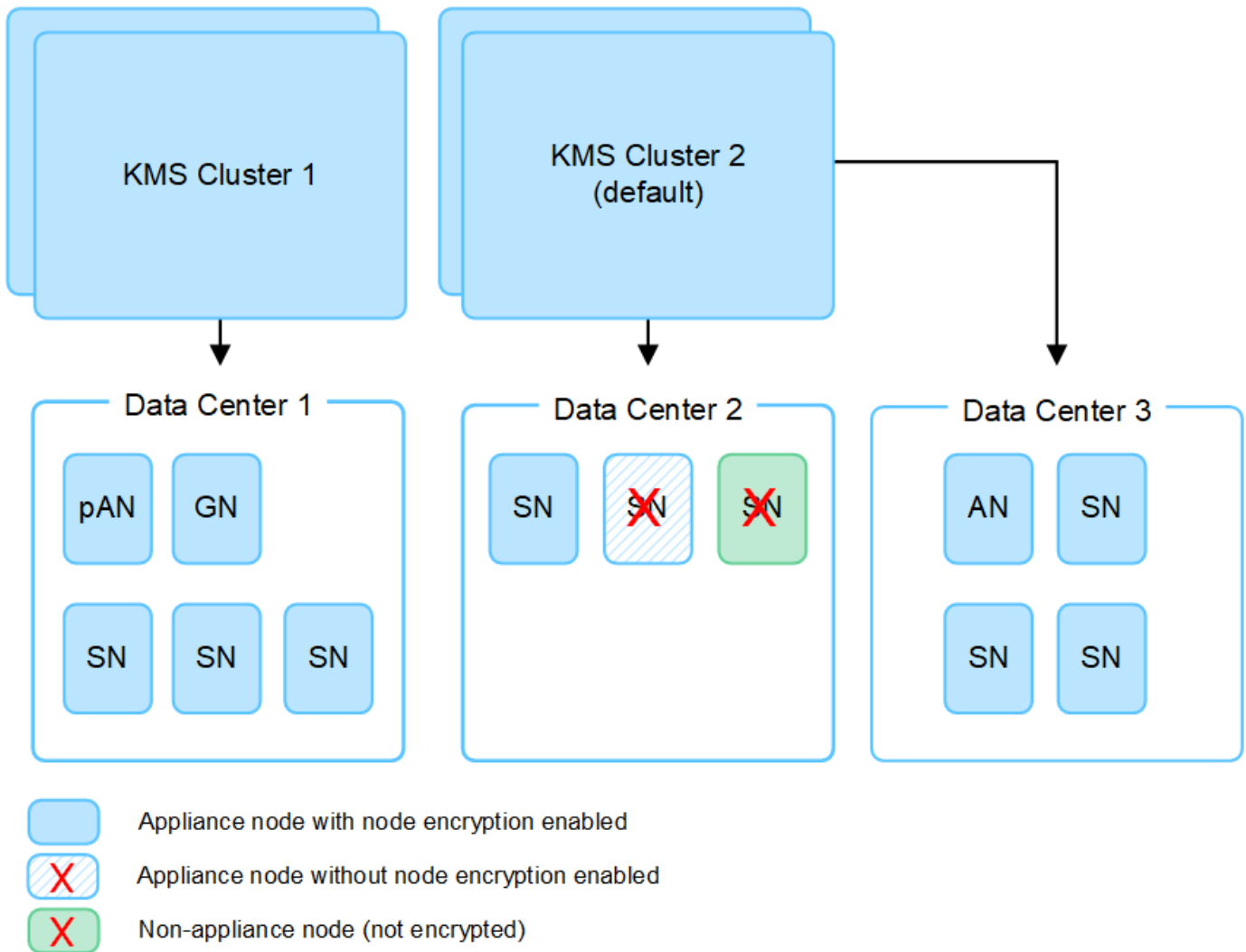
Wie viele wichtige Management Server brauche ich?

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 kein KMS für nicht-Appliance-Knoten oder für alle Appliance-Knoten verwenden können, für die die Einstellung **Node Encryption** 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 zu einer ganz anderen Taste.



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 aus irgendeinem Grund nicht zur Verschlüsselung von Appliance-Volumes verwendet werden kann, wird der Alarm **KMS-Schlüsselrotation fehlgeschlagen** für den Appliance-Knoten 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 das Installationsprogramm der StorageGRID-Appliance für verwenden "[Löschen Sie die KMS-Konfiguration](#)". 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.

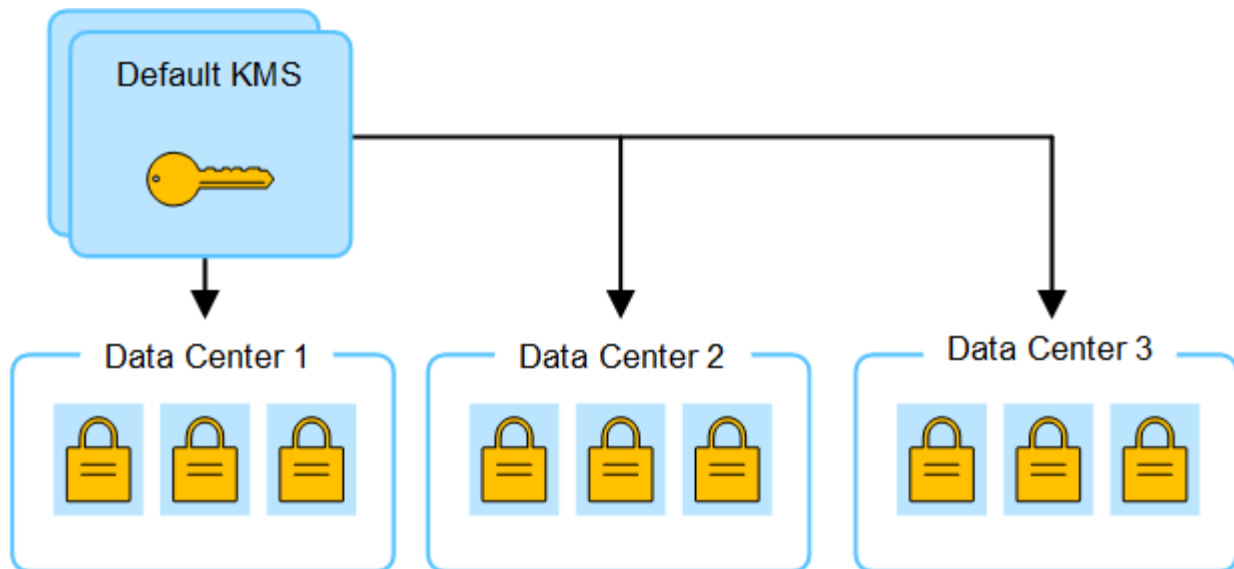
Überlegungen für das Ändern des KMS für einen Standort

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.

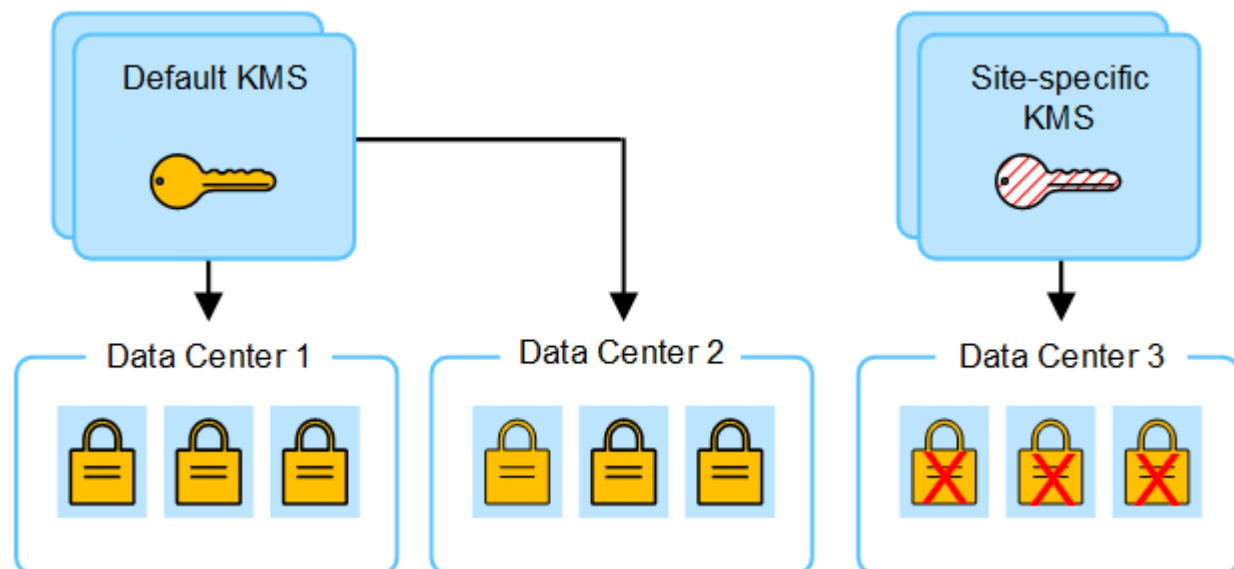
Wenn Sie den KMS ändern, der für einen Standort verwendet wird, müssen Sie sicherstellen, dass die zuvor verschlüsselten Appliance-Nodes an diesem Standort mit dem auf dem neuen KMS gespeicherten Schlüssel entschlüsselt werden können. In einigen Fällen müssen Sie möglicherweise die aktuelle Version des 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:

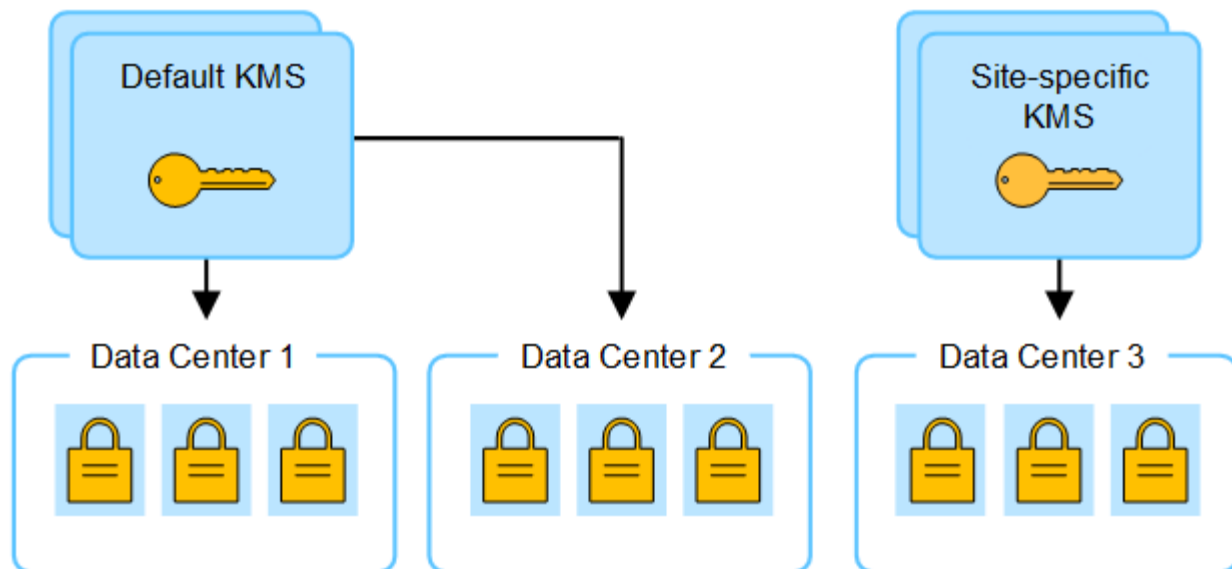
1. Sie konfigurieren zunächst ein Standard-KMS, das für alle Standorte gilt, die kein dediziertes KMS haben.
2. Wenn der KMS gespeichert wird, stellen alle Appliance-Nodes, deren **Node Encryption**-Einstellung aktiviert ist, eine Verbindung zum KMS her und fordern den Verschlüsselungsschlüssel an. Dieser 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.	<p>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. Sie gilt für alle Standorte, die kein dediziertes KMS haben.</p> <p>"Bearbeiten eines Verschlüsselungsmanagement-Servers (KMS)"</p>
Sie haben einen Standard-KMS, und Sie fügen eine neue Site in einer Erweiterung hinzu. Sie möchten nicht das Standard-KMS für den neuen Standort verwenden.	<ol style="list-style-type: none"> 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. 2. Fügen Sie mithilfe des Grid-Managers den neuen KMS hinzu und wählen Sie die Site aus. <p>"Hinzufügen eines Verschlüsselungsmanagement-Servers (KMS)"</p>
Sie möchten, dass der KMS für eine Site einen anderen Server verwendet.	<ol style="list-style-type: none"> 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. 2. Bearbeiten Sie mithilfe des Grid Manager die bestehende KMS-Konfiguration und geben Sie den neuen Hostnamen oder die neue IP-Adresse ein. <p>"Hinzufügen eines Verschlüsselungsmanagement-Servers (KMS)"</p>

Konfigurieren Sie 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. Eine Liste der unterstützten Versionen finden Sie unter "[NetApp Interoperabilitäts-Matrix-Tool \(IMT\)](#)".

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.

Der Verschlüsselungsschlüssel muss mindestens 2,048 Bit haben und 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 Domännennamen (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.

Bevor Sie beginnen

- Sie haben die geprüft "[Überlegungen und Anforderungen für die Verwendung eines Verschlüsselungsmanagement-Servers](#)".
- Das ist schon "[StorageGRID wurde als Client im KMS konfiguriert](#)", Und Sie haben die erforderlichen Informationen für jeden KMS- oder KMS-Cluster.
- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben die Root-Zugriffsberechtigung.

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. Siehe "[Überlegungen für das Ändern des KMS für einen Standort](#)" Entsprechende Details.

Schritt 1: KM Details

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

Schritte

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

Die Seite Key Management Server wird angezeigt, und die Registerkarte Configuration Details ist ausgewählt.

Key management server

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

Configuration details**Encrypted nodes**

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

Before adding a KMS:

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

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

Create Actions Search... Displaying one result

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

← Previous 1 Next →

2. Wählen Sie **Erstellen**.

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

Add a Key Management Server ✕

1 KMS Details
 2 Upload server certificate
 3 Upload client certificates

KMS details

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

KMS name ?

Key name ?

Manages keys for ?

▼

Port ?

Hostname ?

[Add another hostname](#)

Cancel
Continue

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

Feld	Beschreibung
KMS-Name	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	<p>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.</p> <ul style="list-style-type: none"> • Wählen Sie einen Standort aus, wenn dieser KMS Verschlüsselungen für die Appliance-Nodes an einem bestimmten Standort managt. • Wählen Sie Sites Not Managed by another KMS (default KMS) aus, um ein Standard-KMS zu konfigurieren, das für alle Sites gilt, die kein dediziertes KMS haben, und für alle Sites, die Sie in nachfolgenden Erweiterungen hinzufügen. <p>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.</p>
Port	<p>Der Port, den der KMS-Server für die KMIP-Kommunikation (Key Management Interoperability Protocol) verwendet. Die Standardeinstellung ist 5696, d. h. der KMIP-Standardport.</p>
Hostname	<p>Der vollständig qualifizierte Domänenname oder die IP-Adresse für den KMS.</p> <p>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 eines KMS-Clusters herstellen.</p>

4. Wenn Sie einen KMS-Cluster konfigurieren, wählen Sie **Add another hostname**, um einen Hostnamen für jeden Server im Cluster hinzuzufügen.
5. Wählen Sie **Weiter**.

Schritt 2: Serverzertifikat hochladen

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

Schritte

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

Add a Key Management Server

1 KMS Details ————— **2 Upload server certificate** ————— 3 Upload client certificates

Upload a server certificate signed by the certificate authority (CA) on the external key management server (KMS) or a certificate bundle. The server certificate allows the KMS to authenticate itself to StorageGRID.

Server certificate ?

2. Laden Sie die Zertifikatdatei hoch.

Die Metadaten des Serverzertifikats werden angezeigt.

Add a Key Management Server

1 KMS Details ————— **2 Upload server certificate** ————— 3 Upload client certificates

Upload a server certificate signed by the certificate authority (CA) on the external key management server (KMS) or a certificate bundle. The server certificate allows the KMS to authenticate itself to StorageGRID.

Server certificate ?

✓ Cert.pem

Server certificate details Uploaded successfully

Metadata

Subject DN:	/CN=1bdd91b0-3f9e-4934-8b85-83d949e0a43f/UID=nmanohar
Serial number:	F8-4C:34-24-2C-CD-22:77-39-1A-BD-07:62-B1-32-D9
Issuer DN:	/C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA
Issued on:	2022-05-23T16:15:24.000Z
Expires on:	2024-05-22T16:15:24.000Z
SHA-1 fingerprint:	DF:AF:A8:33:34:69:54:C6:F3:7A:07:DD:17:54:88:DD:11:BB:38:E8
SHA-256 fingerprint:	75:E0:8D:7B:C7:CF:28:87:62:BA:82:4A:46:6F:CD:94:69:C7:B7:82:58:26:8F:58:95:B2:06:FB:94:70:2B:81
Alternative names:	



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

3. Wählen Sie **Weiter**.

Schritt 3: Laden Sie Clientzertifikate hoch

In Schritt 3 (Clientzertifikate hochladen) des Assistenten zum Hinzufügen eines Schlüsselverwaltungsservers laden Sie das Clientzertifikat und den privaten Schlüssel des Clientzertifikats hoch. Das Client-Zertifikat ermöglicht StorageGRID, sich am KMS zu authentifizieren.

Schritte

1. Navigieren Sie unter **Schritt 3 (Client-Zertifikate hochladen)** zum Speicherort des Client-Zertifikats.

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

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.

5. Wählen Sie **Test und 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 bei der Auswahl von **Test und 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 **Speichern erzwingen**.



Wenn Sie **Force save** auswählen, wird die KMS-Konfiguration gespeichert, aber die externe Verbindung von jedem Gerät zu diesem KMS wird 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.

- 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.

KMS-Details anzeigen

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

Schritte

- Wählen Sie **KONFIGURATION > Sicherheit > Schlüsselverwaltungsserver** aus.

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

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

Feld	Beschreibung
KMS-Name	Der beschreibende Name des KMS.
Schlüsselname	Der Schlüsselalias für den StorageGRID-Client im KMS.
Verwaltet Schlüssel für	Der dem KMS zugeordnete StorageGRID-Site. Dieses Feld zeigt den Namen einer bestimmten StorageGRID-Site oder Sites an, die nicht von einem anderen KMS verwaltet werden (Standard-KMS) .

Feld	Beschreibung
Hostname	<p>Der vollständig qualifizierte Domänenname oder die IP-Adresse des KMS.</p> <p>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.</p> <p>Beispiel: 10.10.10.10 and 10.10.10.11 Oder 10.10.10.10 and 2 others.</p> <p>Um alle Hostnamen in einem Cluster anzuzeigen, öffnen Sie ein KMS und wählen Bearbeiten oder Aktionen > Bearbeiten.</p>
Ablauf des Zertifikats	<p>Aktueller Status des Serverzertifikats, des optionalen CA-Zertifikats und des Client-Zertifikats: Gültig, abgelaufen, bald abgelaufen oder unbekannt.</p> <p>Hinweis: Es kann StorageGRID so lange wie 30 Minuten dauern, bis Updates zum Ablauf des Zertifikats erhalten. Sie müssen Ihren Webbrowser aktualisieren, um die aktuellen Werte anzuzeigen.</p>

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



Unmittelbar nach dem Hinzufügen eines KMS wird der Ablauf des Zertifikats 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 Zertifikatablauf angezeigt wird, dass ein Zertifikat abgelaufen ist oder kurz vor dem Ablaufdatum steht, beheben Sie das Problem so schnell wie möglich.

Wenn die Warnungen **KMS CA Certificate Expiration**, **KMS Client Certificate Expiration** und **KMS Server Certificate Expiration** ausgelöst werden, notieren Sie sich die Beschreibung der einzelnen Warnungen und führen Sie die empfohlenen Aktionen durch.



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

5. Um die Zertifikatdetails für dieses KMS anzuzeigen, wählen Sie den KMS-Namen aus der Tabelle aus.
6. Überprüfen Sie auf der KMS-Übersichtsseite die Metadaten und das Zertifikat-PEM sowohl für das Serverzertifikat als auch für das Clientzertifikat. Wählen Sie bei Bedarf **Zertifikat bearbeiten**, um ein Zertifikat durch ein neues zu ersetzen.

Verschlüsselte Nodes anzeigen

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 > Sicherheit > 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, für die 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-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 Verschlüsselungsmanagement-Servers (KMS)"
Schlüssel-UID	Die eindeutige ID des Verschlüsselungsschlüssels, der zur Verschlüsselung und Entschlüsselung von Daten auf dem Appliance-Node verwendet wird. Um eine gesamte Schlüssel-UID anzuzeigen, setzen Sie den Cursor über die Zelle. 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. 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
- KM ist nicht konfiguriert

Führen Sie die empfohlenen Aktionen für diese Warnmeldungen aus.



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

Bearbeiten eines Verschlüsselungsmanagement-Servers (KMS)

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

Bevor Sie beginnen

- Sie haben die geprüft "[Überlegungen und Anforderungen für die Verwendung eines Verschlüsselungsmanagement-Servers](#)".
- Wenn Sie die für einen KMS ausgewählte Site aktualisieren möchten, haben Sie die geprüft "[Überlegungen für das Ändern des KMS für einen Standort](#)".
- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben die Root-Zugriffsberechtigung.

Schritte


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

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

2. Wählen Sie den KMS aus, den Sie bearbeiten möchten, und wählen Sie **actions > Edit**.

Sie können einen 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 zum Bearbeiten eines Schlüsselverwaltungsservers.

Feld	Beschreibung
KMS-Name	Einen beschreibenden Namen, der Ihnen bei der Identifizierung dieses KMS hilft. Muss zwischen 1 und 64 Zeichen liegen.
Schlüsselname	<p>Der exakte Schlüssel-Alias für den StorageGRID-Client im KMS. Muss zwischen 1 und 255 Zeichen liegen.</p> <p>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.</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;">  <p>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.</p> <p>"Überlegungen und Anforderungen für die Verwendung eines Verschlüsselungsmanagement-Servers"</p> </div>
Verwaltet Schlüssel für	<p>Wenn Sie ein standortspezifisches KMS bearbeiten und noch kein Standard-KMS haben, wählen Sie optional Sites Not Managed by another KMS (default 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 Sites, die in einer Erweiterung hinzugefügt wurden.</p> <p>Hinweis: Wenn Sie eine Site-spezifische KMS bearbeiten, können Sie keine andere Site auswählen. Wenn Sie das Standard-KMS bearbeiten, können Sie keine bestimmte Site auswählen.</p>
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	<p>Der vollständig qualifizierte Domänenname oder die IP-Adresse für den KMS.</p> <p>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 eines KMS-Clusters herstellen.</p>

4. Wenn Sie einen KMS-Cluster konfigurieren, wählen Sie **Add another hostname**, um einen Hostnamen für jeden Server im Cluster hinzuzufügen.
5. Wählen Sie **Weiter**.

Schritt 2 (Serverzertifikat hochladen) des Assistenten zum Bearbeiten eines Schlüsselverwaltungsservers 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 zum Bearbeiten eines Schlüsselverwaltungsservers 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 **Test und 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 **Speichern erzwingen**.



Wenn Sie **Force save** auswählen, wird die KMS-Konfiguration gespeichert, aber die externe Verbindung von jedem Gerät zu diesem KMS wird 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.

Bevor Sie beginnen

- Sie haben die geprüft "[Überlegungen und Anforderungen für die Verwendung eines Verschlüsselungsmanagement-Servers](#)".

- Sie sind mit einem bei Grid Manager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben die Root-Zugriffsberechtigung.

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 > Sicherheit > Schlüsselverwaltungsserver** aus.

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

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

Sie können 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 einen Standort, der keinen Appliance-Knoten mit aktivierter Knotenverschlüsselung hat.
- Sie entfernen den Standard-KMS, aber für jeden Standort mit Knotenverschlüsselung ist bereits ein standortspezifisches KMS vorhanden.

4. Wählen Sie **Ja**.

Die KMS-Konfiguration wurde entfernt.

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFT SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.