Remote Key Management auf eigenständigen Rack-Servern konfigurieren

Inhalt

Einleitung

Dieses Dokument beschreibt die Konfiguration des Key Management Interoperability Protocol (KMIP) auf eigenständigen Rack-Servern.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Integrated Management Controller (CIMC)
- Selbstverschlüsselndes Laufwerk (SED)
- KMIP

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- UCSC-C220-M4S, CIMC-Version: 4,1 (1 Std.)
- SED-Laufwerke
- 800 GB Enterprise Performance SAS SED SSD (10 FWPD) - MTFDJAK800MBS
- Laufwerkteil-ID: UCS-SD800GBEK9
- Anbieter: MIKRON
- Modell: S650DC-800FIPS

- Vormetrisch als Drittanbieter-Schlüsselmanager

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

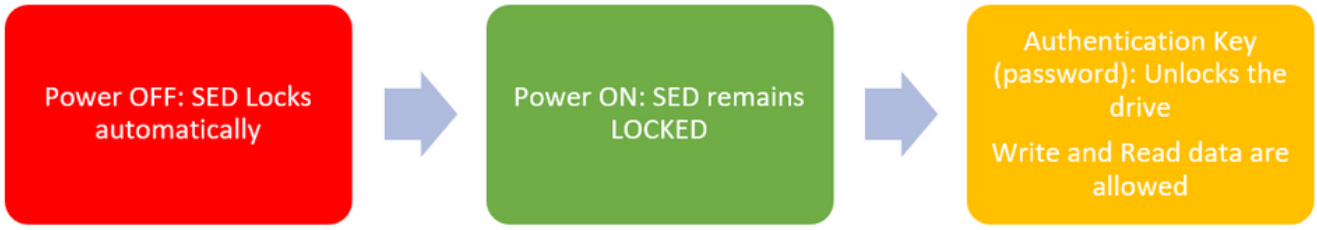
KMIP ist ein erweiterbares Kommunikationsprotokoll, das Nachrichtenformate für die Bearbeitung kryptografischer Schlüssel auf einem Schlüsselverwaltungsserver definiert. Dies erleichtert die Datenverschlüsselung, da die Verschlüsselungsschlüsselverwaltung vereinfacht wird.

SED-Laufwerke

Ein SED ist eine Festplatte (HDD) oder ein Solid-State-Laufwerk (SSD) mit integrierter Verschlüsselungsschaltung. Es verschlüsselt auf transparente Weise alle auf das Medium geschriebenen Daten und entschlüsselt, wenn es entsperrt wird, transparent alle vom Medium gelesenen Daten.

Bei einer SED verlassen die Verschlüsselungsschlüssel selbst nie die Grenzen der SED-Hardware und sind daher vor Angriffen auf Betriebssystemebene sicher.

SED-Laufwerke Workflow:



1. SED-Antriebsfluss

Das Kennwort zum Entsperren des Laufwerks kann lokal über die Konfiguration der **lokalen Schlüsselverwaltung** abgerufen werden, wobei der Benutzer dafür verantwortlich ist, sich die Schlüsselinformationen zu merken. Er kann auch über die Remote Key-Verwaltung abgerufen werden. Dabei wird der Sicherheitsschlüssel von einem KMIP-Server erstellt und abgerufen, und der Benutzer ist dafür verantwortlich, den KMIP-Server im CIMC zu konfigurieren.

Konfigurieren

Erstellen eines privaten Clientschlüssels und eines Clientzertifikats

Diese Befehle müssen auf einem Linux-System mit dem OpenSSL-Paket eingegeben werden, nicht im Cisco IMC. Stellen Sie sicher, dass der Common Name im Root-Zertifizierungsstellenzertifikat und im Clientzertifikat identisch ist.

Anmerkung: Stellen Sie sicher, dass die Cisco IMC-Zeit auf die aktuelle Zeit eingestellt ist.

1. Erstellen Sie einen 2048-Bit-RSA-Schlüssel.

```
openssl genrsa -out client_private.pem 2048
```

2. Erstellen Sie ein selbstsigniertes Zertifikat mit dem bereits erstellten Schlüssel.

```
openssl req -new -x509 -key client_private.pem -out client.pem -days 365
```

3. Weitere Informationen zum Erhalt des Zertifikats der Stammzertifizierungsstelle finden Sie in der Dokumentation des KMIP-Anbieters.

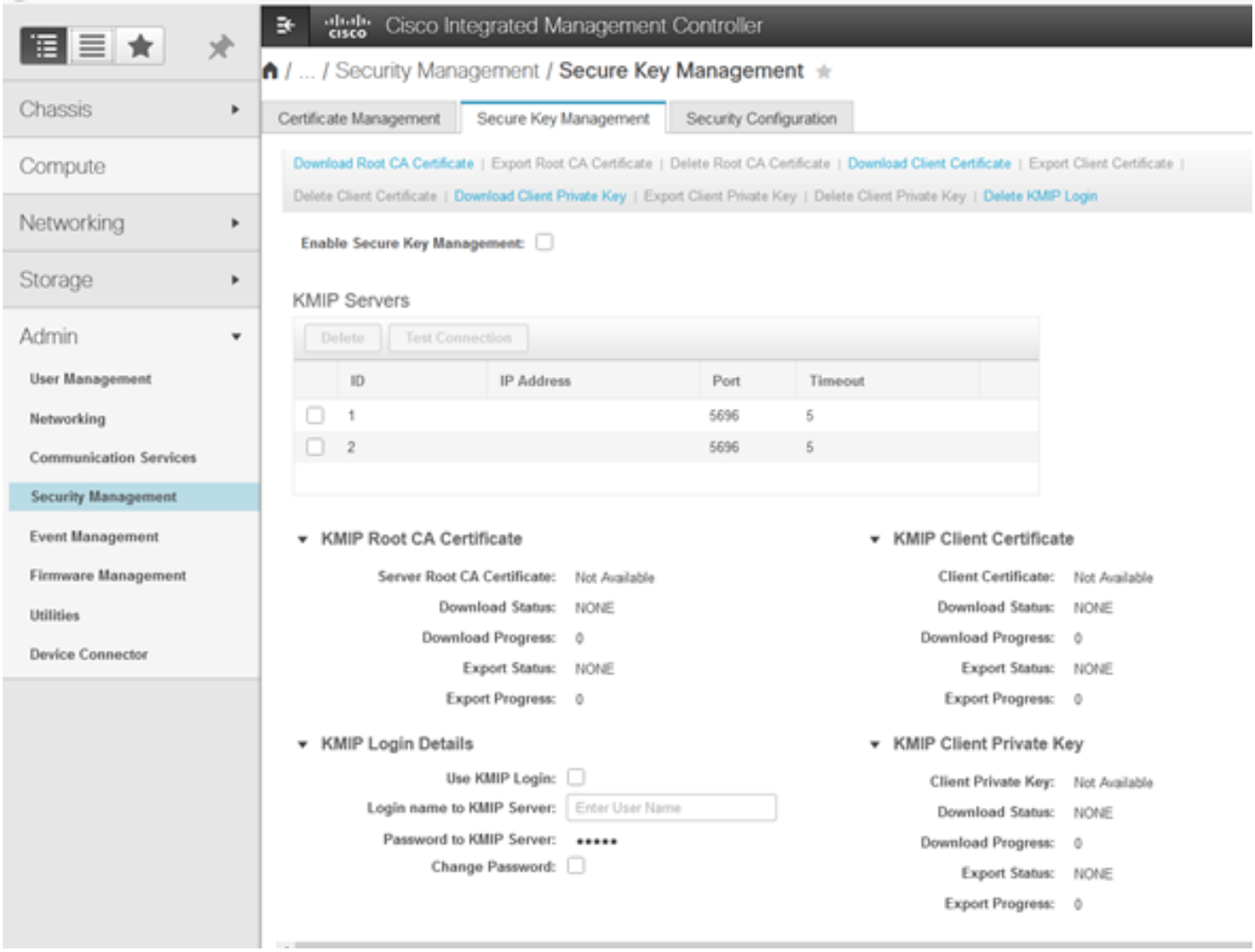
> **Anmerkung:** Für Vormetric muss der allgemeine Name im RootCa-Zertifikat mit dem Hostnamen des Vormetric-Hosts übereinstimmen.

> **Anmerkung:** Sie benötigen ein Konto, um auf die Konfigurationsanleitungen für die KMIP-Anbieter zugreifen zu können:
> SafeNet
> Vormetrisch

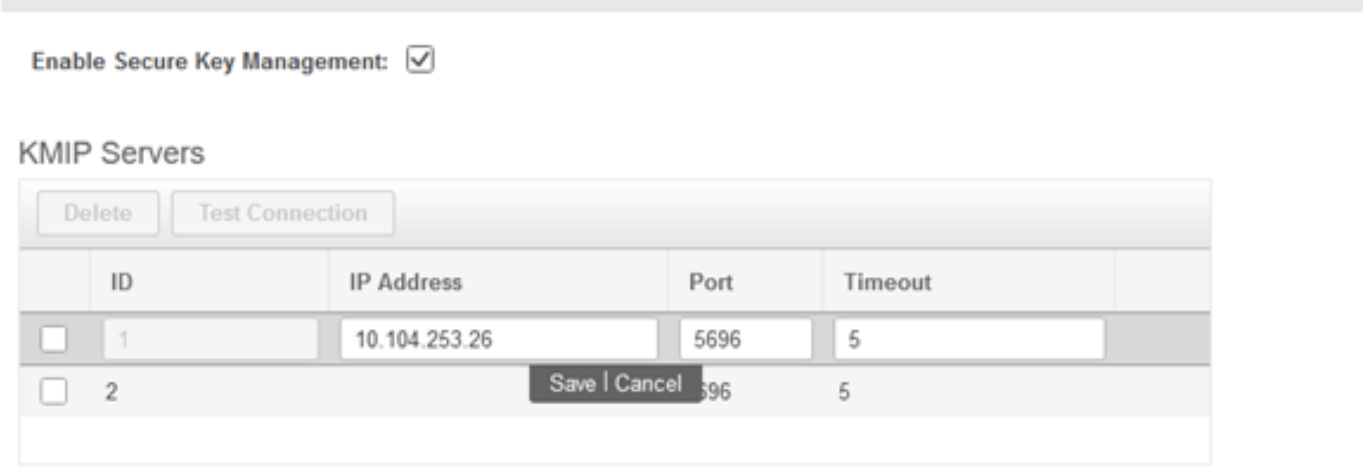
KMIP-Server auf dem CIMC konfigurieren

1. Navigieren Sie zu **Admin > Security Management > Secure Key Management.**

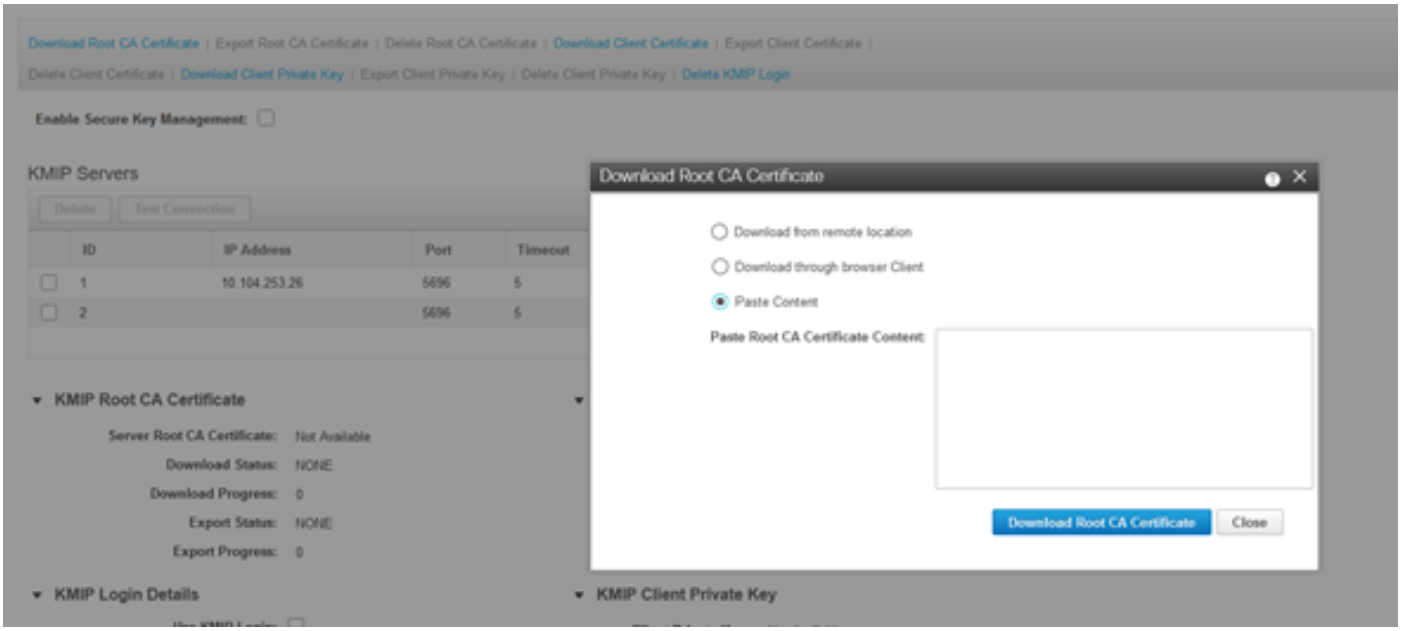
Eine übersichtliche Konfiguration zeigt **Export/Delete** buttons grayed out, only **Download** buttons are active.



2. Klicken Sie auf die IP-Adresse und legen Sie die IP für den KMIP-Server, stellen Sie sicher, dass Sie in der Lage sind, sie zu erreichen und wenn der Standard-Port verwendet wird nichts anderes geändert werden muss, dann speichern Sie die Änderungen.

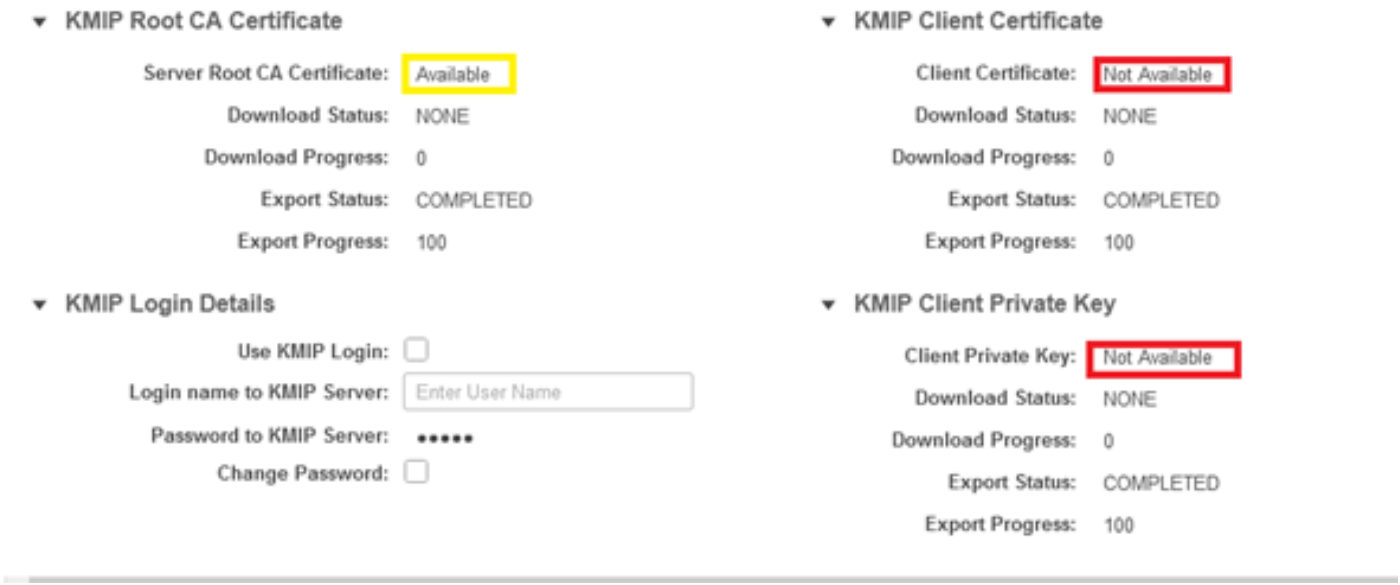


3. Laden Sie die Zertifikate und den privaten Schlüssel auf den Server herunter. Sie können die **.pem** file or just paste the content.



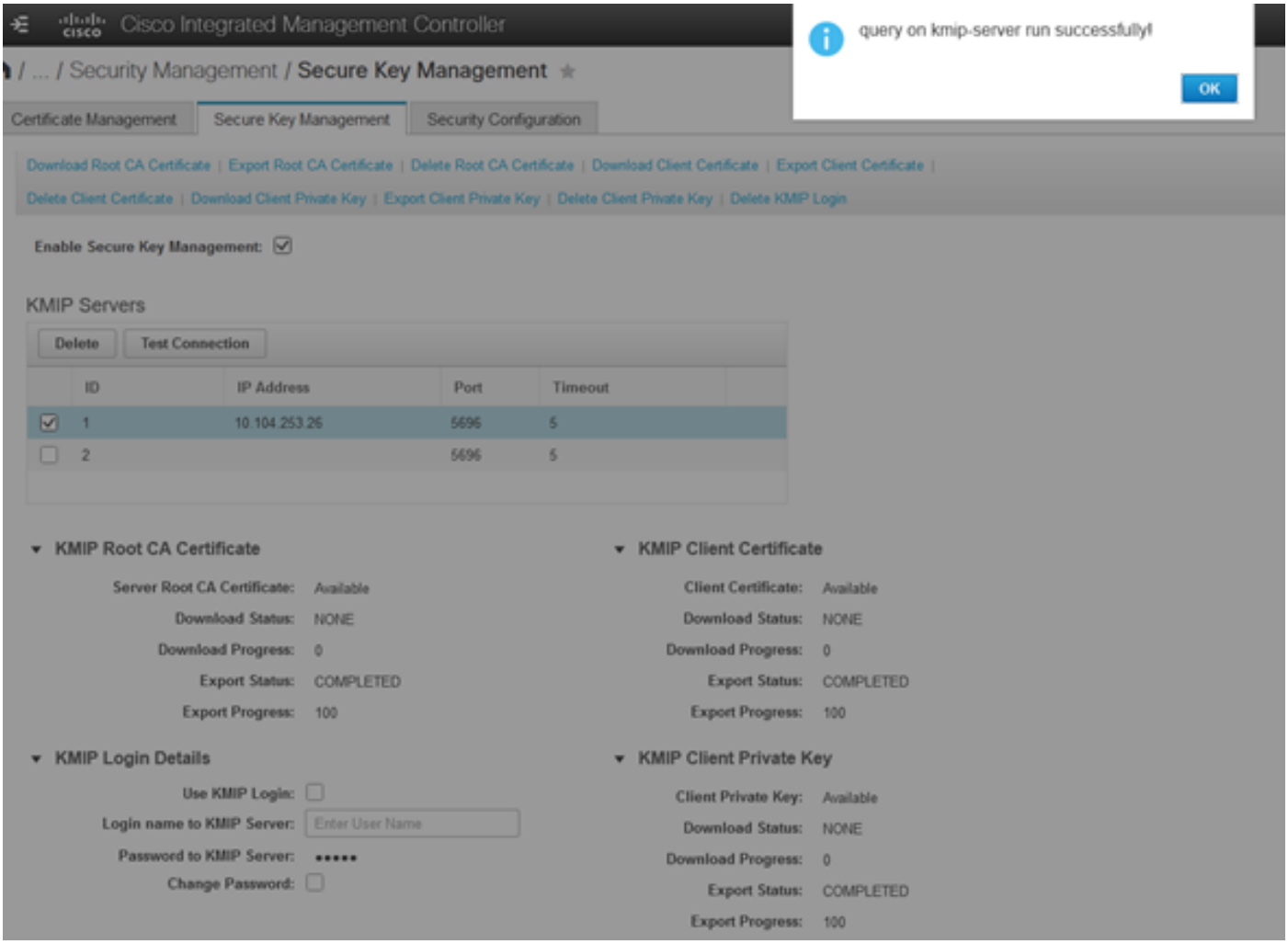
4. Wenn Sie die Zertifikate hochladen, sehen Sie, dass die Zertifikate als **Verfügbar** angezeigt werden. Für die fehlenden Zertifikate, die nicht hochgeladen werden, sehen Sie **Nicht verfügbar**.

Sie können die Verbindung nur testen, wenn alle Zertifikate und privaten Schlüssel erfolgreich auf den CIMC heruntergeladen wurden.



5. (optional) Sobald Sie über alle Zertifikate verfügen, können Sie optional den Benutzer und das Kennwort für den KMIP-Server hinzufügen. Diese Konfiguration wird nur für SafeNet als Drittanbieter-KMIP-Server unterstützt.

6. Testen Sie die Verbindung, und wenn die Zertifikate korrekt sind und Sie den KMIP-Server über den konfigurierten Port erreichen können, wird eine erfolgreiche Verbindung angezeigt.

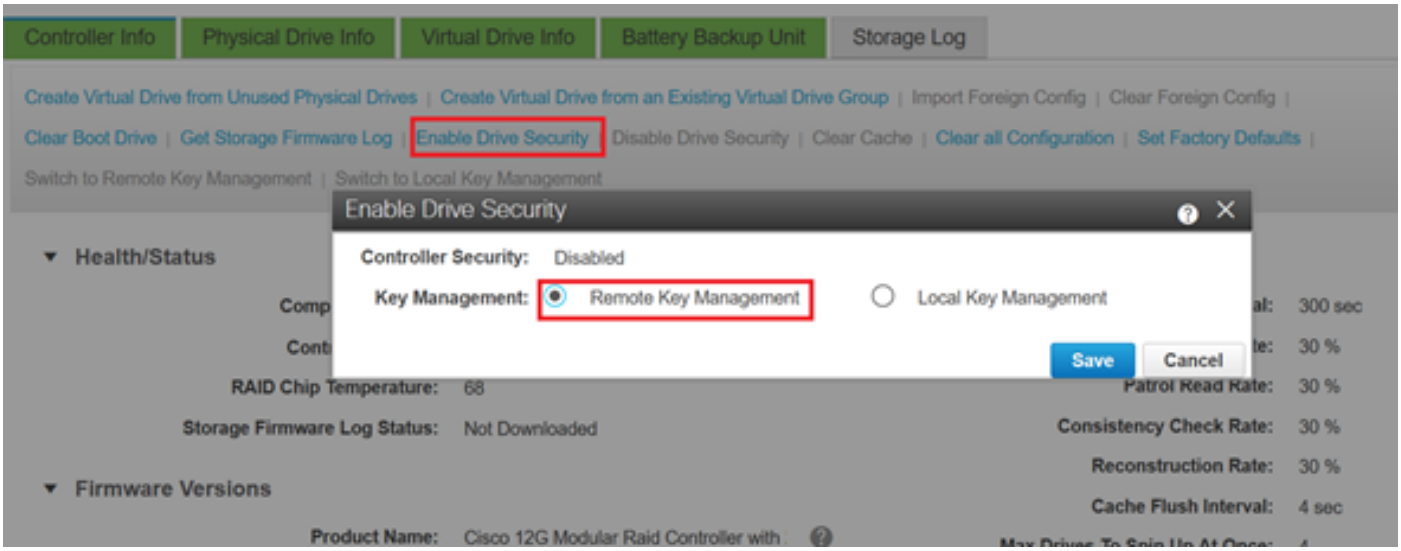


7. Sobald unsere Verbindung mit KMIP erfolgreich ist, können Sie die Remote-Schlüsselverwaltung aktivieren.

Navigieren Sie zu **Networking > Modular Raid Controller > Controller Info**.

Wählen Sie **Laufwerksicherheit aktivieren** und dann **Remote Key Management aus**.

> **Anmerkung:** Wenn die **lokale Schlüsselverwaltung** zuvor aktiviert war, werden Sie aufgefordert, den aktuellen Schlüssel einzugeben, um ihn zur Remote-Verwaltung zu ändern.



Überprüfung

Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Über die CLI können Sie die Konfiguration überprüfen.

1. Überprüfen Sie, ob KMIP aktiviert ist.

```
C-Series-12# scope kmip C-Series-12 /kmip # show detail Enabled: yes
```

2. Überprüfen Sie IP-Adresse, Port und Timeout.

```
C-Series-12 /kmip # show kmip-server Server number Server domain name or IP address Port Timeout
------------ ------------------------------ ------ ------ 1 10.104.253.26 5696 5 2 5696 5
```

3. Überprüfen Sie, ob die Zertifikate verfügbar sind.

```
C-Series-12 /kmip # show kmip-client-certificate KMIP Client Certificate Available: 1 C-Series-
12 /kmip # show kmip-client-private-key KMIP Client Private Key Available: 1 C-Series-12 /kmip #
show kmip-root-ca-certificate KMIP Root CA Certificate Available: 1
```

4. Überprüfen der Anmeldedetails

```
C-Series-12 /kmip # show kmip-login Use KMIP Login Login name to KMIP server Password to KMIP
server ------------------------ ------------------------ -------------------- no ******
```

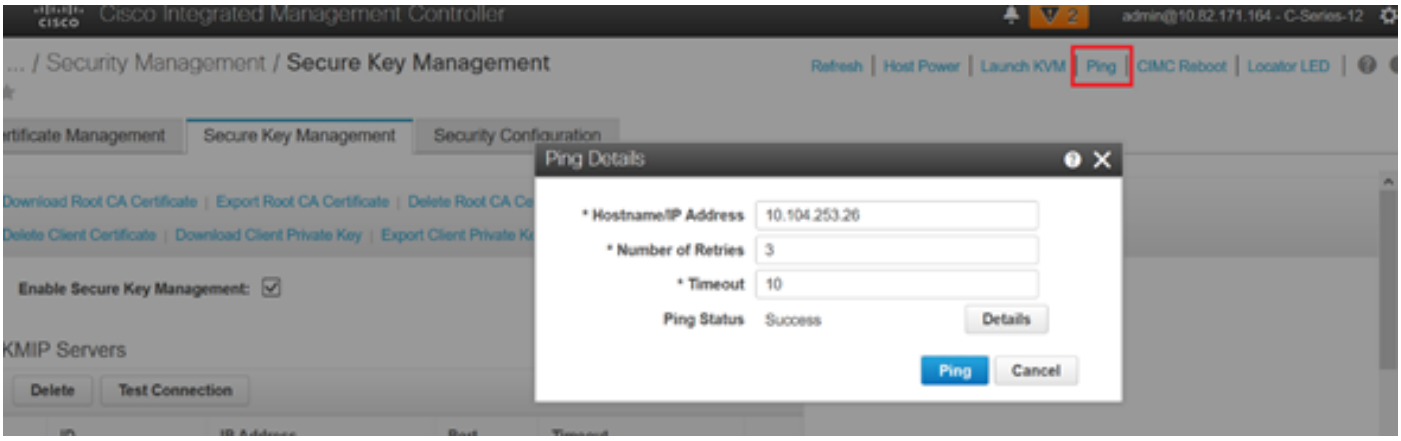
5. Testen Sie die Verbindung.

```
C-Series-12 /kmip # C-Series-12 /kmip # scope kmip-server 1 C-Series-12 /kmip/kmip-server #
test-connectivity Result of test-connectivity: query on kmip-server run successfully!
```

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Wenn die Testverbindung mit dem KMIP-Server nicht erfolgreich hergestellt werden kann, stellen Sie sicher, dass Sie den Server pingen können.

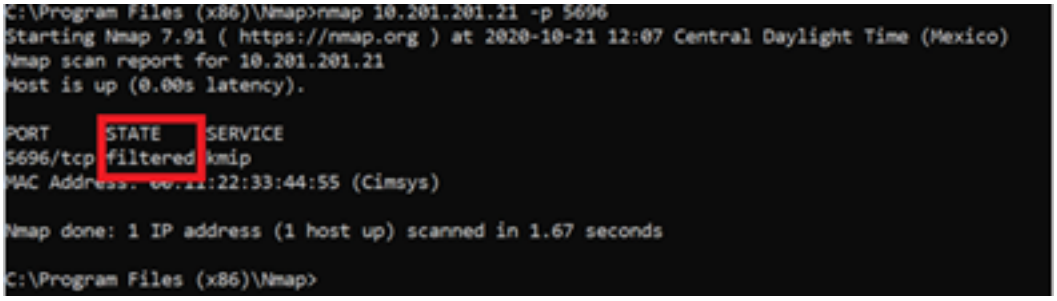


Stellen Sie sicher, dass der Port 5696 auf dem CIMC- und dem KMIP-Server geöffnet ist. Sie können eine NMAP-Version auf unserem PC installieren, da dieser Befehl auf CIMC nicht verfügbar ist.

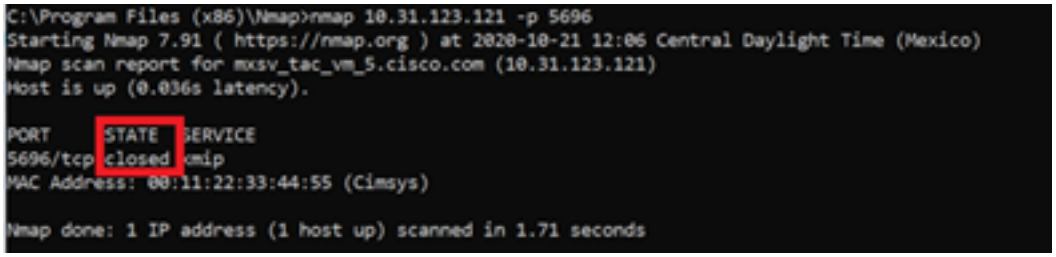
Sie können NMAP auf Ihrem lokalen Computer installieren, um zu testen, ob der Port geöffnet ist. Verwenden Sie in dem Verzeichnis, in dem die Datei installiert wurde, den folgenden Befehl:

```
nmap <ipAddress> -p <port>
```

Die Ausgabe zeigt einen offenen Port für den KMIP-Service:



Die Ausgabe zeigt einen geschlossenen Port für den KMIP-Service:



Zugehörige Informationen

- Konfigurationsanleitung für die C-Serie - Selbstverschlüsselnde Laufwerke
- Konfigurationsanleitung für die C-Serie - Key Management Interoperability Protocol
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.