Remote Key Management configureren op standalone rackservers

Inhoud

Inleiding

In dit document wordt de configuratie beschreven van het Key Management Interoperability Protocol (KMIP) op standalone rackservers.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Integrated Management Controller (CIMC)
- Self-encrypting drive (SED)
- KMIP

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- UCS C220-M4S, CIMC-versie: 4.1(1 nonies)
- SED-schijven
- 800 GB Enterprise Performance SAS SED SSD (10 FWPD) - MTFDJAK800MBS
- ID onderdeel station: UCS-SD800G-BEK9 switch
- Verkoper: MICRON
- Model: SG650DC-800FIPS
- Vormetric als third-party key manager

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

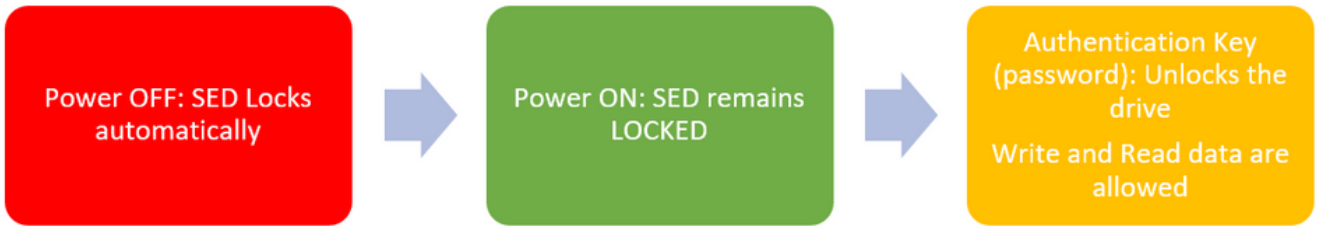
KMIP is een uitbreidbaar communicatieprotocol dat berichtformaten definieert voor de manipulatie van cryptografische sleutels op een sleutelbeheerserver. Dit vergemakkelijkt gegevenscodering omdat encryptie zeer belangrijk beheer vereenvoudigt.

SED-schijven

Een SED is een vaste schijf (HDD) of solid-state drive (SSD) met een encryptie-circuit dat in het station is ingebouwd. Het versleutelt alle gegevens die naar de media zijn geschreven en ontgrendelt alle gegevens die van de media zijn gelezen.

In een SED laten de encryptiesleutels zelf nooit de grenzen van de SED-hardware en zijn daardoor veilig voor aanvallen op OS-niveau.

Werkstroom van SED-schijven:



1. SED-schijf

Het wachtwoord om het station te ontgrendelen kan lokaal worden verkregen met de configuratie **Local Key Management** waarbij de gebruiker verantwoordelijk is om de belangrijkste informatie te onthouden. Het kan ook worden verkregen met Remote Key Management waar de beveiligingssleutel wordt gemaakt en gehaald van een KMIP-server en de gebruiker de verantwoordelijkheid heeft om de KMIP-server te configureren in CIMC.

Configureren

Een client-privésleutel en clientcertificaat maken

Deze opdrachten moeten op een Linux-machine met het OpenSSL-pakket worden ingevoerd, niet in de Cisco IMC. Zorg ervoor dat de algemene naam hetzelfde is in het basiscertificaat van CA en in het clientcertificaat.

> **Opmerking:** Zorg ervoor dat de Cisco IMC-tijd is ingesteld op de huidige tijd.

1. Maak een 2048-bits RSA-toets.

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

2. Maak een zelfondertekend certificaat met de sleutel die al is gemaakt.

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

3. Raadpleeg de KMIP-verkoopdocumentatie voor informatie over het verkrijgen van het Root CA-certificaat.

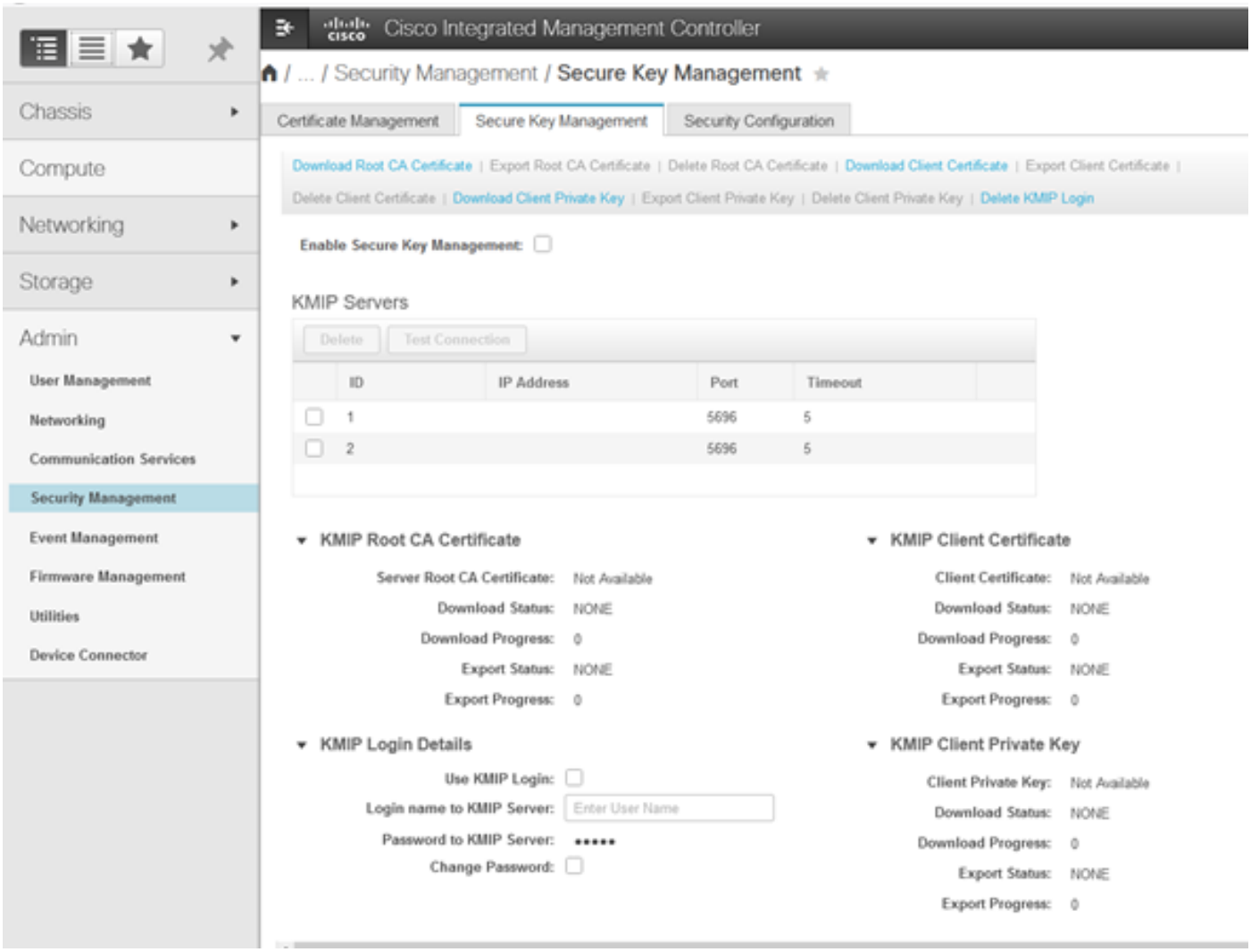
> **Opmerking:** Vormetric vereist dat de gemeenschappelijke naam in het RootCa certificaat overeenkomt met de hostname van de Vormetric host.

> **Opmerking:** U moet een account hebben om toegang te hebben tot de configuratiehandleidingen voor de KMIP-leveranciers:
> SafeNet
> vormetrisch

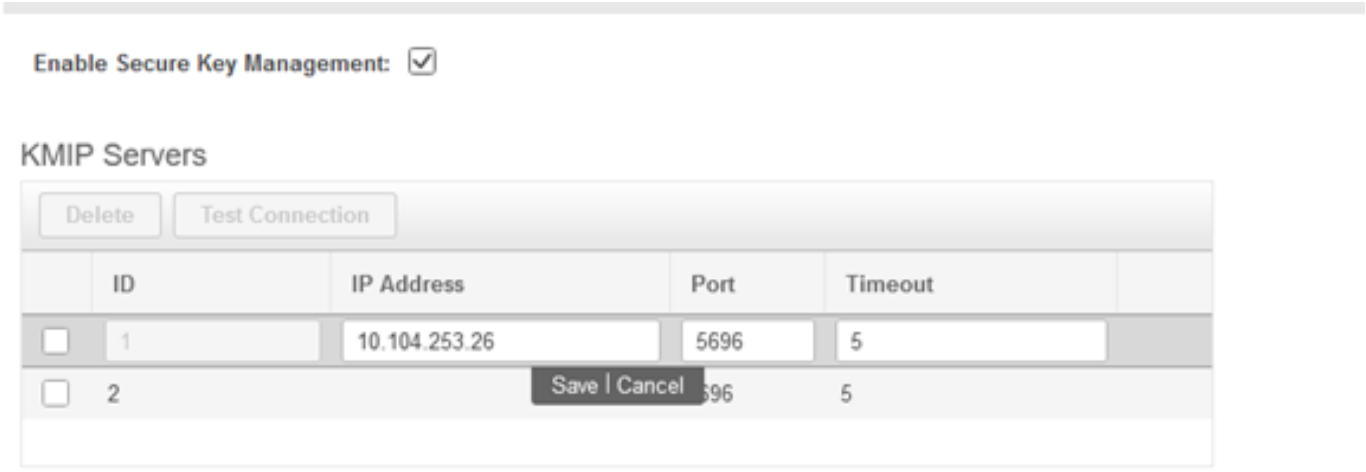
KMIP-server op de CIMC configureren

1. Ga naar **Beheer > Beveiligingsbeheer > Beveiligingsbeheer.**

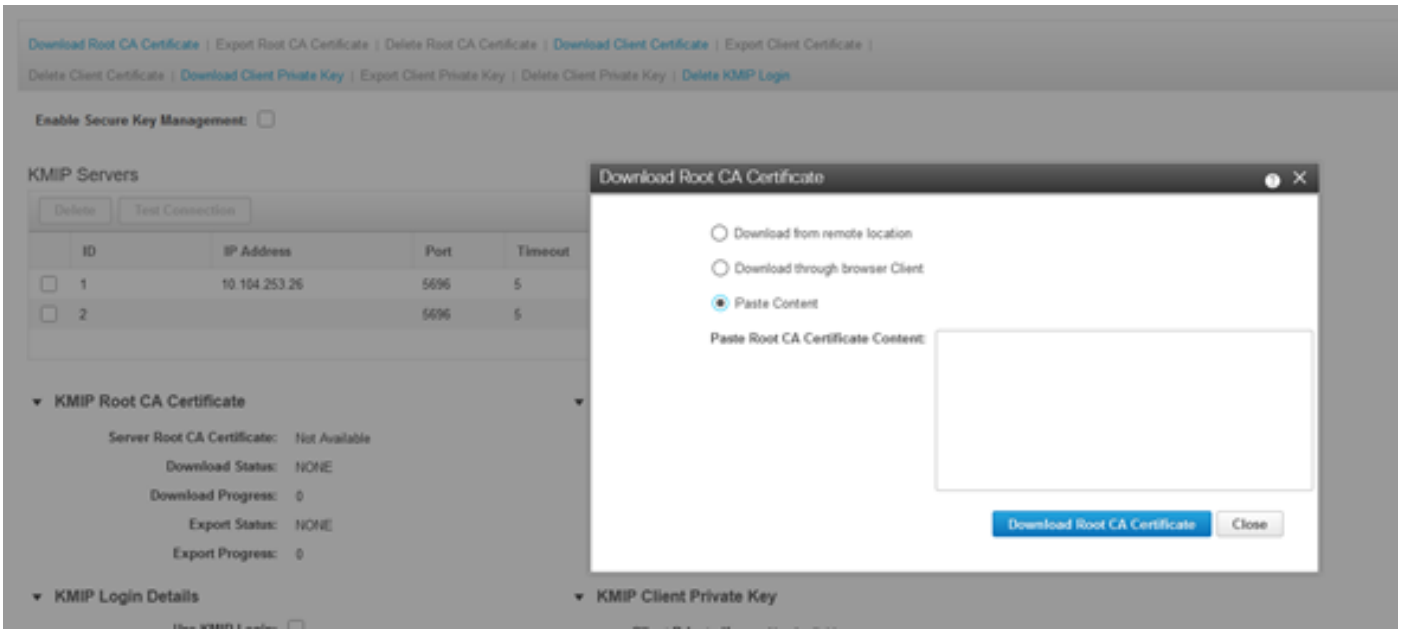
Een duidelijke configuratie toont **Export/Delete** buttons grayed out, only **Download** buttons are active.



2. Klik op het IP-adres en stel het IP voor de KMIP-server in, zorg ervoor dat u het kunt bereiken en, voor het geval dat de standaardpoort wordt gebruikt, hoeft er niets anders te worden gewijzigd, dan slaat u de wijzigingen op.

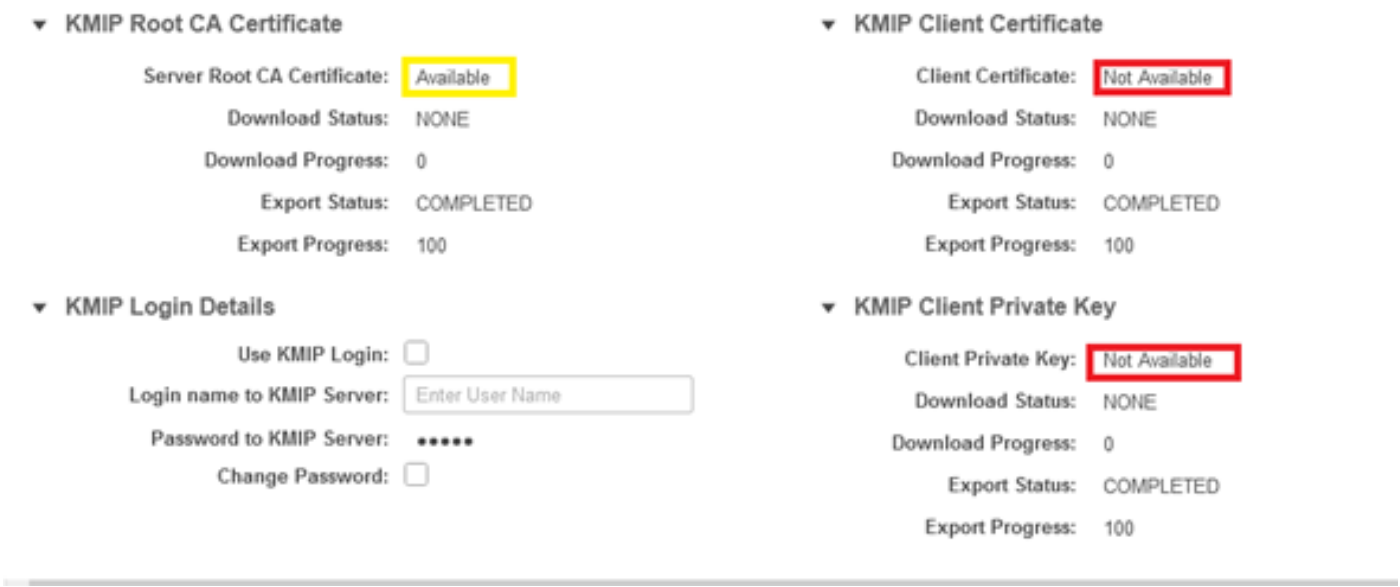


3. Download de certificaten en privé sleutel naar de server. U kunt de **.pem** file or just paste the content.



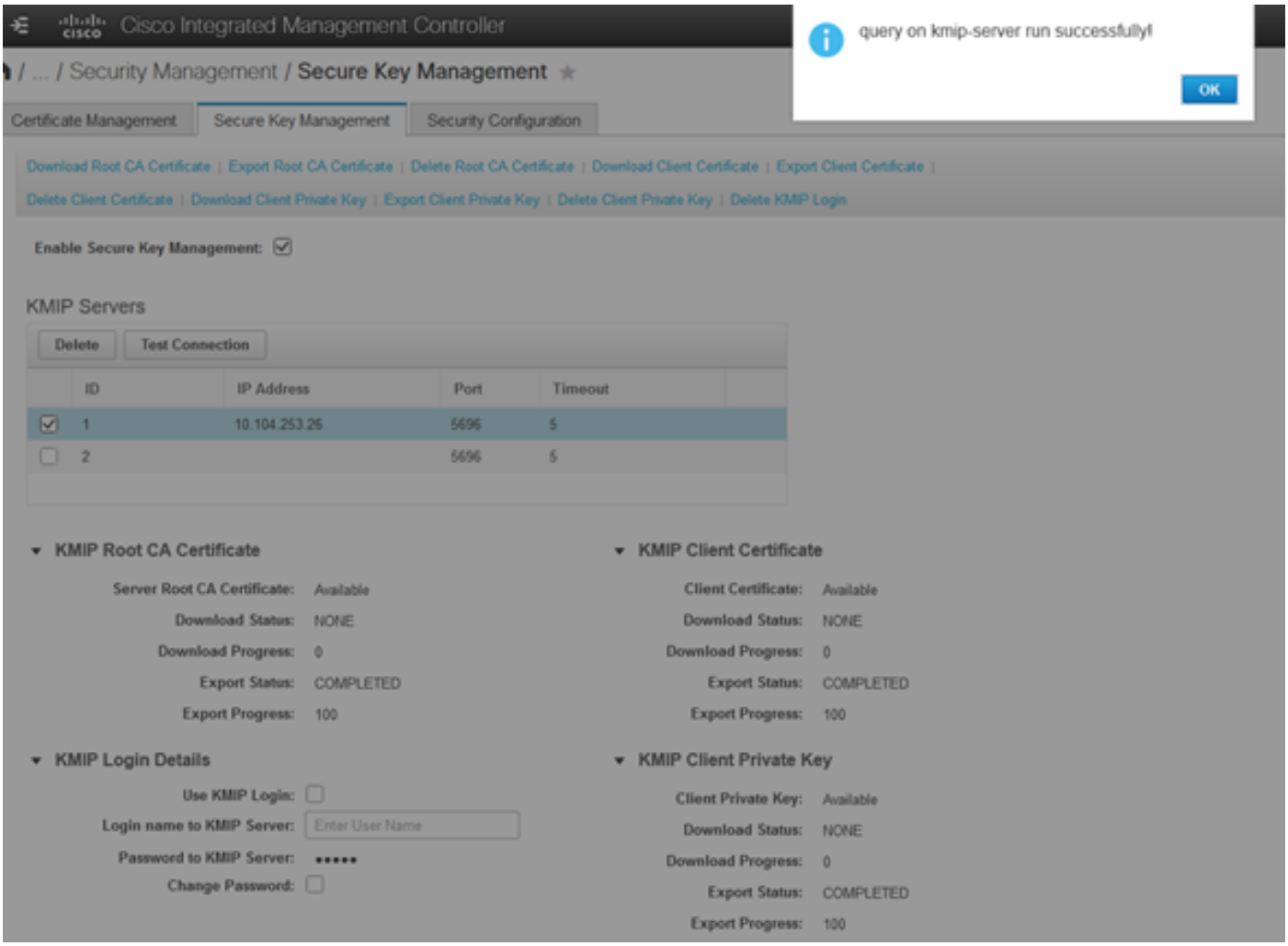
4. Wanneer u de certificaten uploadt, ziet u dat de certificaten als **Beschikbaar** worden weergegeven. Voor de ontbrekende certificaten die niet zijn geüpload, ziet u **Niet beschikbaar**.

U kunt de verbinding alleen testen wanneer alle certificaten en privésleutels zijn gedownload naar de CIMC.



5. (facultatief) Zodra u alle certificaten hebt, kunt u naar keuze de gebruiker en het wachtwoord voor de KMIP-server toevoegen, wordt deze configuratie alleen ondersteund voor SafeNet als een KMIP-server van een derde partij.

6. Test de verbinding en als de certificaten correct zijn en u de KMIP-server kunt bereiken via de geconfigureerde poort, ziet u een succesvolle verbinding.

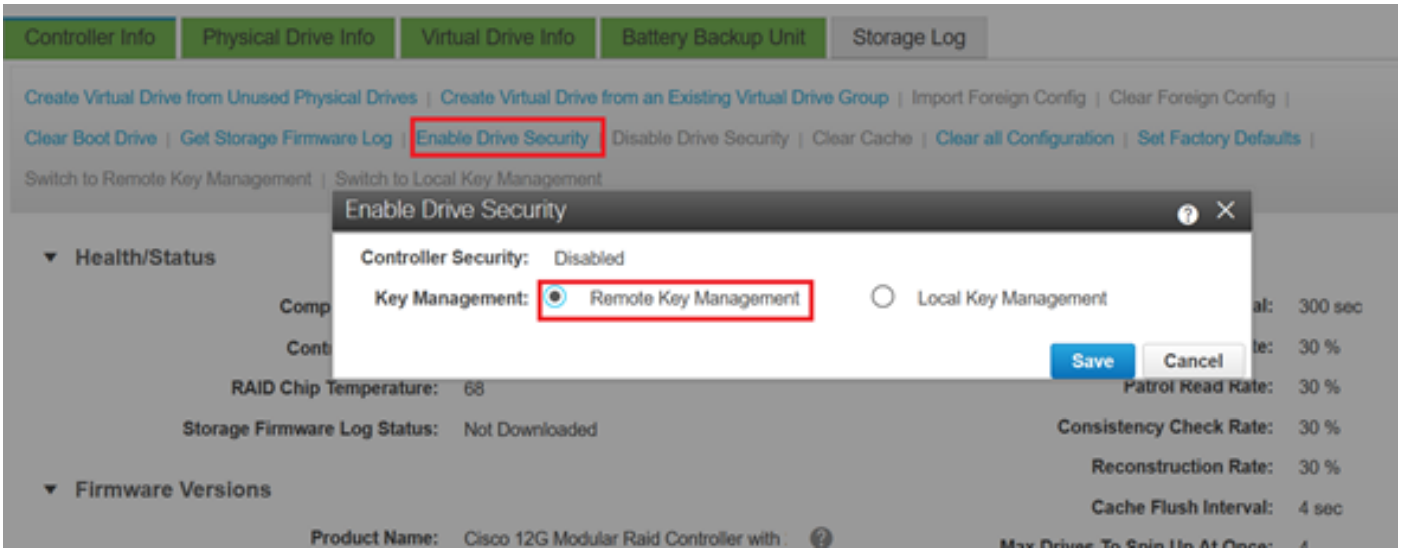


7. Zodra onze verbinding met KMIP succesvol is, kunt u het beheer van externe sleutels inschakelen.

Ga naar **Netwerk > Modular Raid Controller > Controller Info**.

Selecteer **Drive Security inschakelen** en vervolgens **Remote Key Management**.

> **Opmerking:** Als **Local Key Management** eerder is ingeschakeld, wordt u gevraagd om de huidige toets te wijzigen voor extern beheer



Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

Van CLI kunt u de configuratie verifiëren.

1. Controleer of KMIP is ingeschakeld.

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

2. Controleer het IP-adres, de poort en de tijdelijke versie.

```
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. Controleer of de certificaten beschikbaar zijn.

```
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. Controleer de inloggegevens.

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

5. Test de aansluiting.

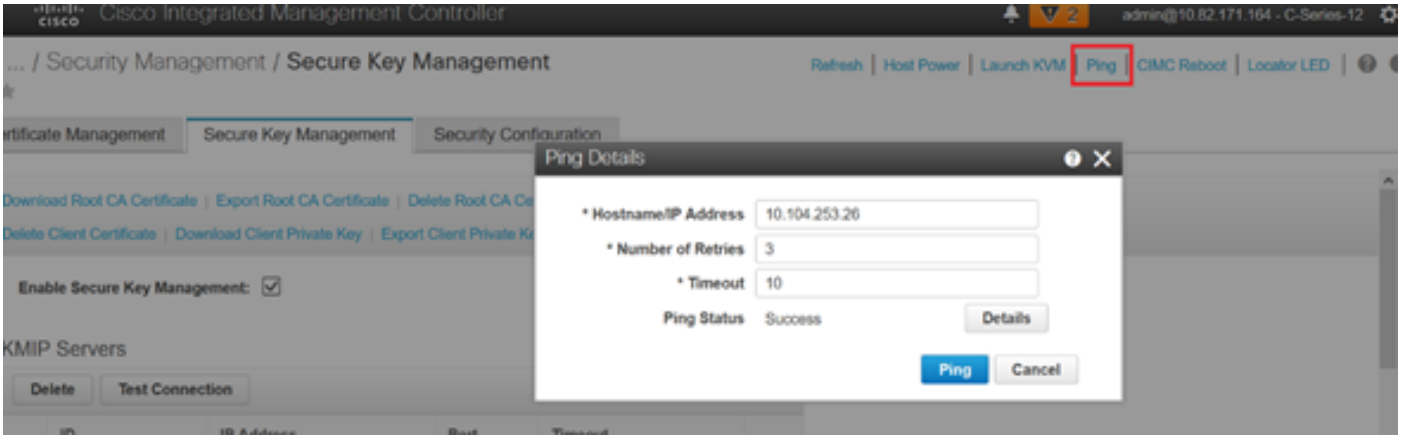
```
C-Series-12 /kmip # C-Series-12 /kmip # scope kmip-server 1 C-Series-12 /kmip/kmip-server #
```

```
test-connectivity Result of test-connectivity: query on kmip-server run successfully!
```

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Als de testverbinding met de KMIP-server niet succesvol is, zorg er dan voor dat u de server kunt pingen.

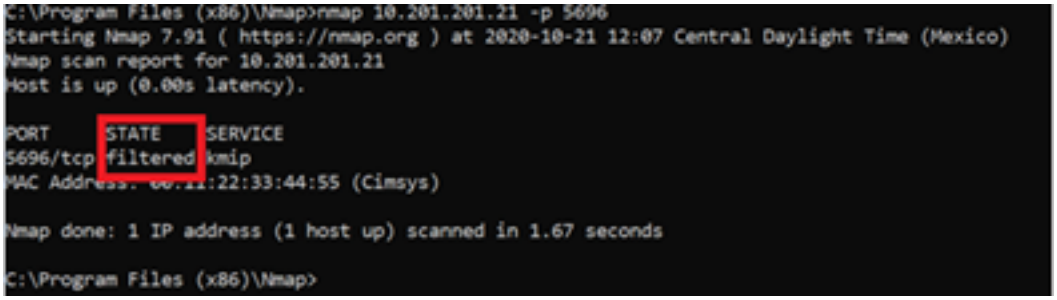


Zorg ervoor dat poort 5696 is geopend op de CIMC- en KMIP-server. U kunt een NMAP-versie op onze pc installeren, aangezien deze opdracht niet beschikbaar is op CIMC.

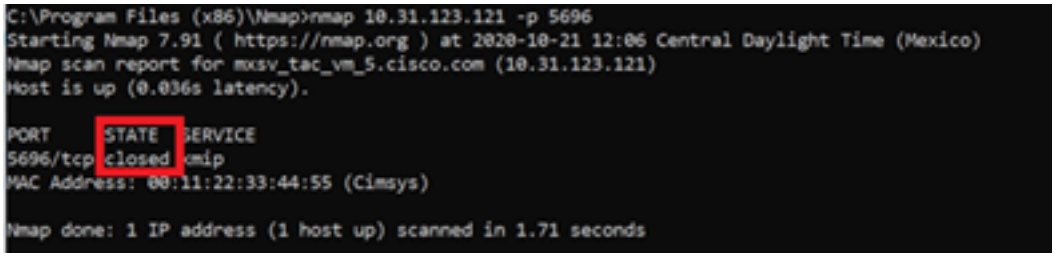
U kunt NMAP installeren op uw lokale machine, om te testen of de poort is geopend; Gebruik deze opdracht in de map waarin het bestand is geïnstalleerd:

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

De output toont een open poort voor KMIP-service:



De output toont een gesloten haven voor de dienst van KMIP:



Gerelateerde informatie

- C Series-configuratiehandleiding - zelfversleutelende stations

- C Series-configuratiehandleiding - Key Management Interoperability Protocol
- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.