在獨立機架式伺服器上配置遠端金鑰管理

目錄

簡介

本檔案介紹在獨立機架式伺服器上設定金鑰管理互通性通訊協定(KMIP)。

必要條件

需求

思科建議您瞭解以下主題：

- 思科整合式管理控制器(CIMC)
- 自我加密驅動器(SED)
- KMIP

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- UCSC-C220-M4S，CIMC版本：4.1(1h)
- SED驅動器
- 800GB企業效能SAS SED SSD(10 FWPD)- MTFDJAK800MBS
- 驅動器部件ID:UCS-SD800GBEK9
- 供應商：微米
- 型號：S650DC-800FIPS
- Vormetric作為第三方金鑰管理器

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

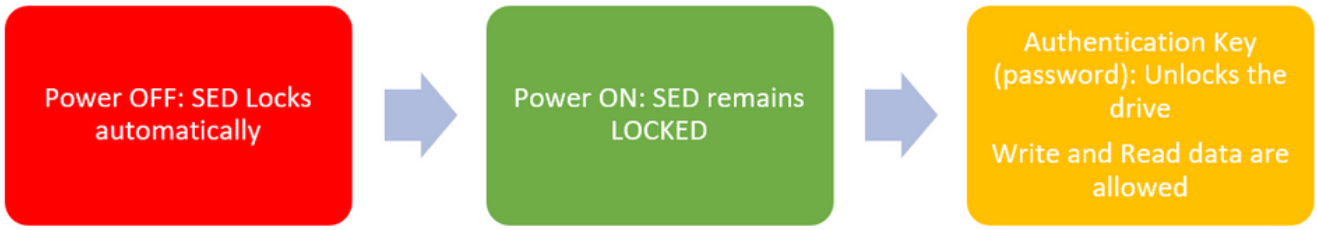
KMIP是一種可擴展的通訊協定，它定義了用於在金鑰管理伺服器上處理金鑰的消息格式。這簡化了加密金鑰管理，從而方便了資料加密。

SED驅動器

SED是硬碟驅動器(HDD)或固態驅動器(SSD)，驅動器內建加密電路。它透明地加密寫入介質的所有資料，並在解鎖後透明地解密從介質讀取的所有資料。

在SED中，加密金鑰本身永遠不會離開SED硬體的限制，因此可以安全抵禦作業系統級別的攻擊。

SED驅動器工作流：



1. SED驅動器流

使用**本地金鑰管理**配置（使用者負責記住金鑰資訊）可在本地獲取解鎖驅動器的密碼。它也可以通過遠端金鑰管理獲取，其中安全金鑰是從KMIP伺服器建立和提取的，使用者負責在CIMC中配置KMIP伺服器。

設定

建立客戶端私鑰和客戶端證書

這些命令將使用OpenSSL包在Linux機器上輸入，而不是在Cisco IMC中。確保根CA證書和客戶端證書中的公用名相同。

> **附註**：確保Cisco IMC時間設定為當前時間。

1.建立2048位RSA金鑰。

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

2.使用已建立的金鑰建立自簽名證書。

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

3.有關獲取根CA證書的詳細資訊，請參閱KMIP供應商文檔。

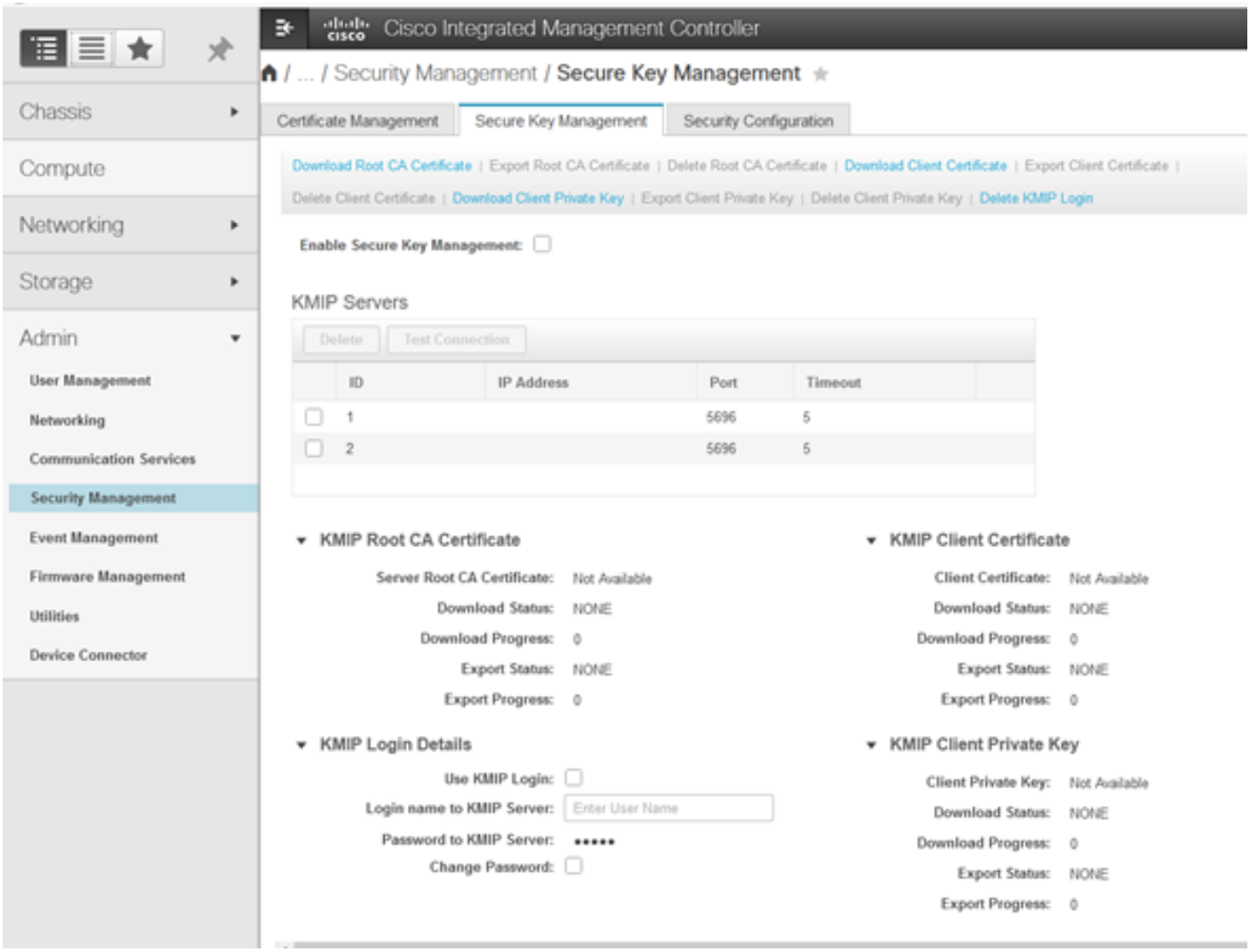
> **附註**：Vormetric要求RootCa證書中的公用名稱與Vormetric主機的主機名匹配。

附註：您必須擁有帳戶才能訪問KMIP供應商的配置指南：
SafeNet
渦度

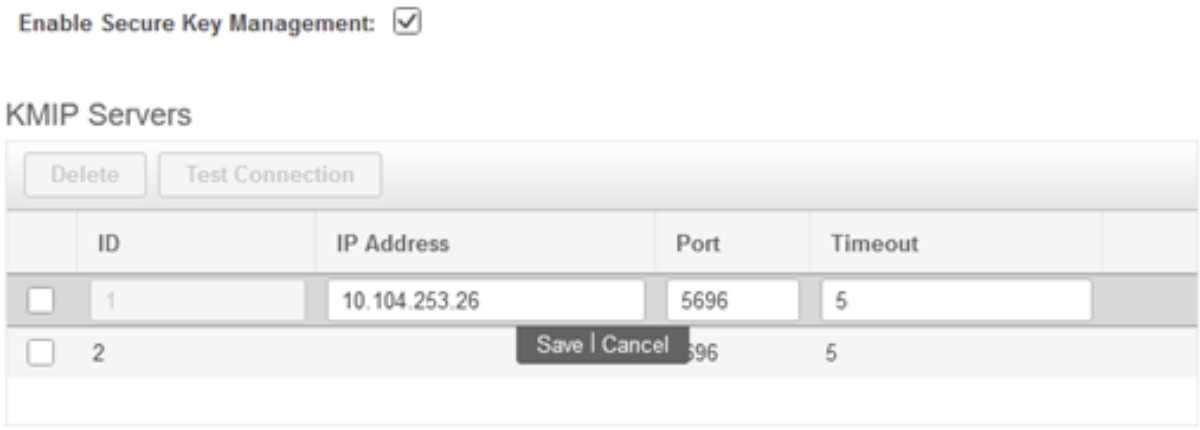
在CIMC上配置KMIP伺服器

1.導航到**Admin > Security Management > Secure Key Management**。

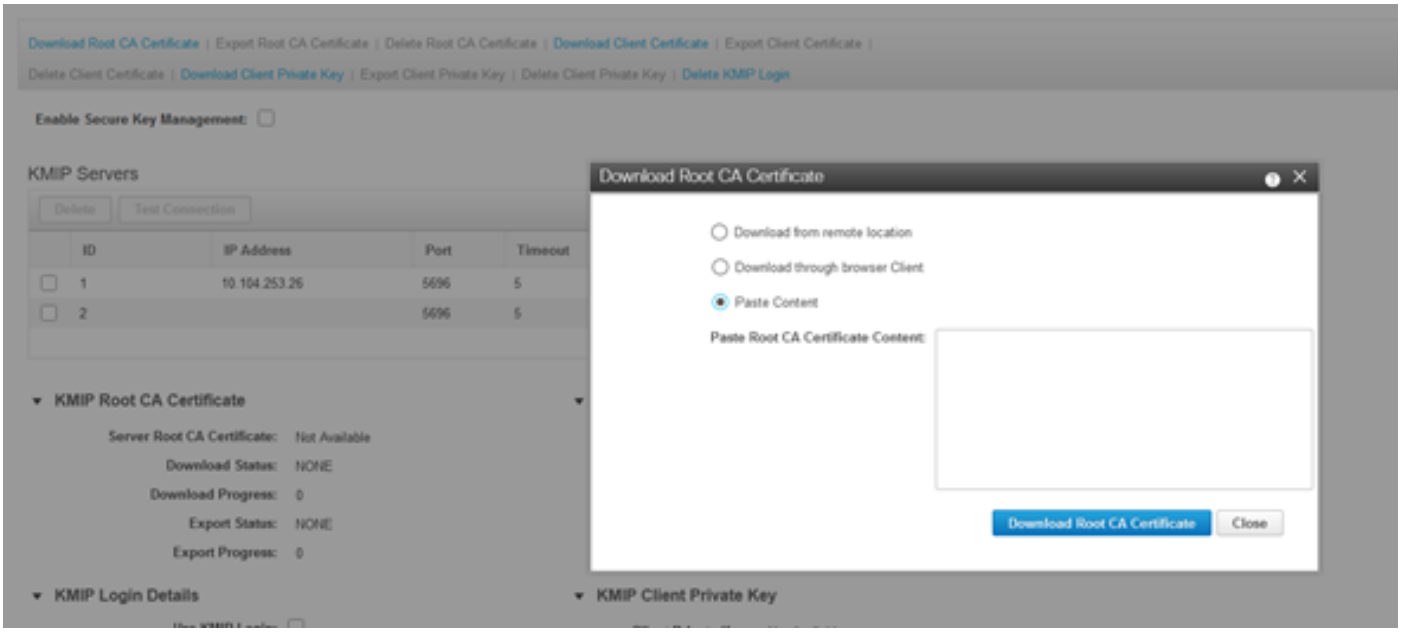
清晰的配置顯示 **Export/Delete** buttons grayed out, only **Download** buttons are active.



2.按一下IP地址並設定KMIP伺服器的IP，確保您能夠訪問它，並且在預設埠被使用時，無需更改任何其他內容，然後儲存更改。

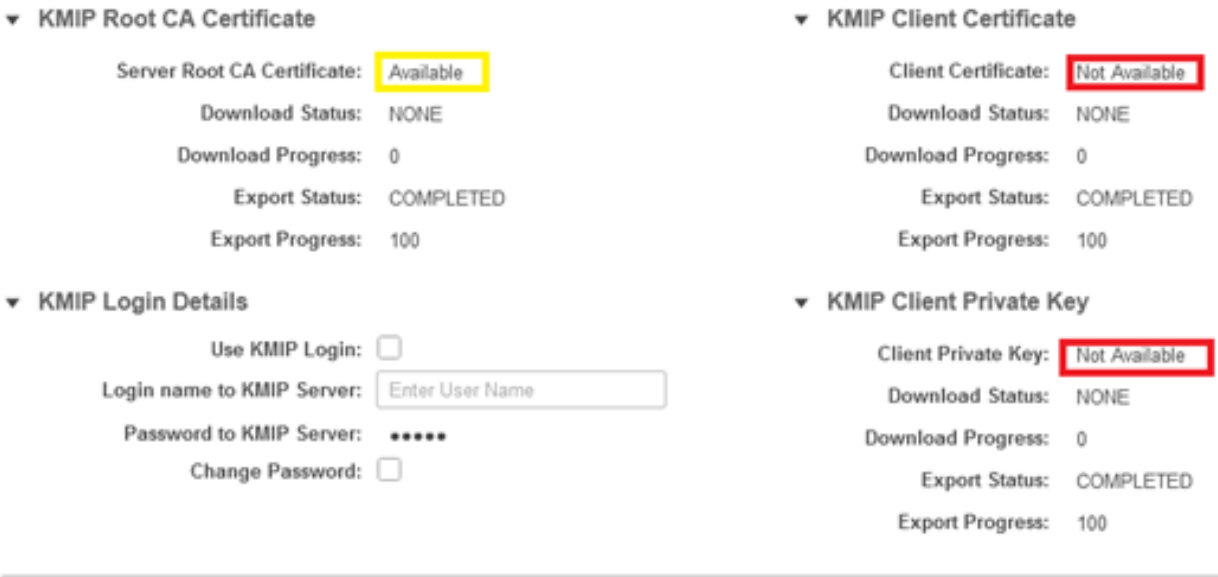


3.將證書和私鑰下載到伺服器。您可以下載 **.pem** file or just paste the content.



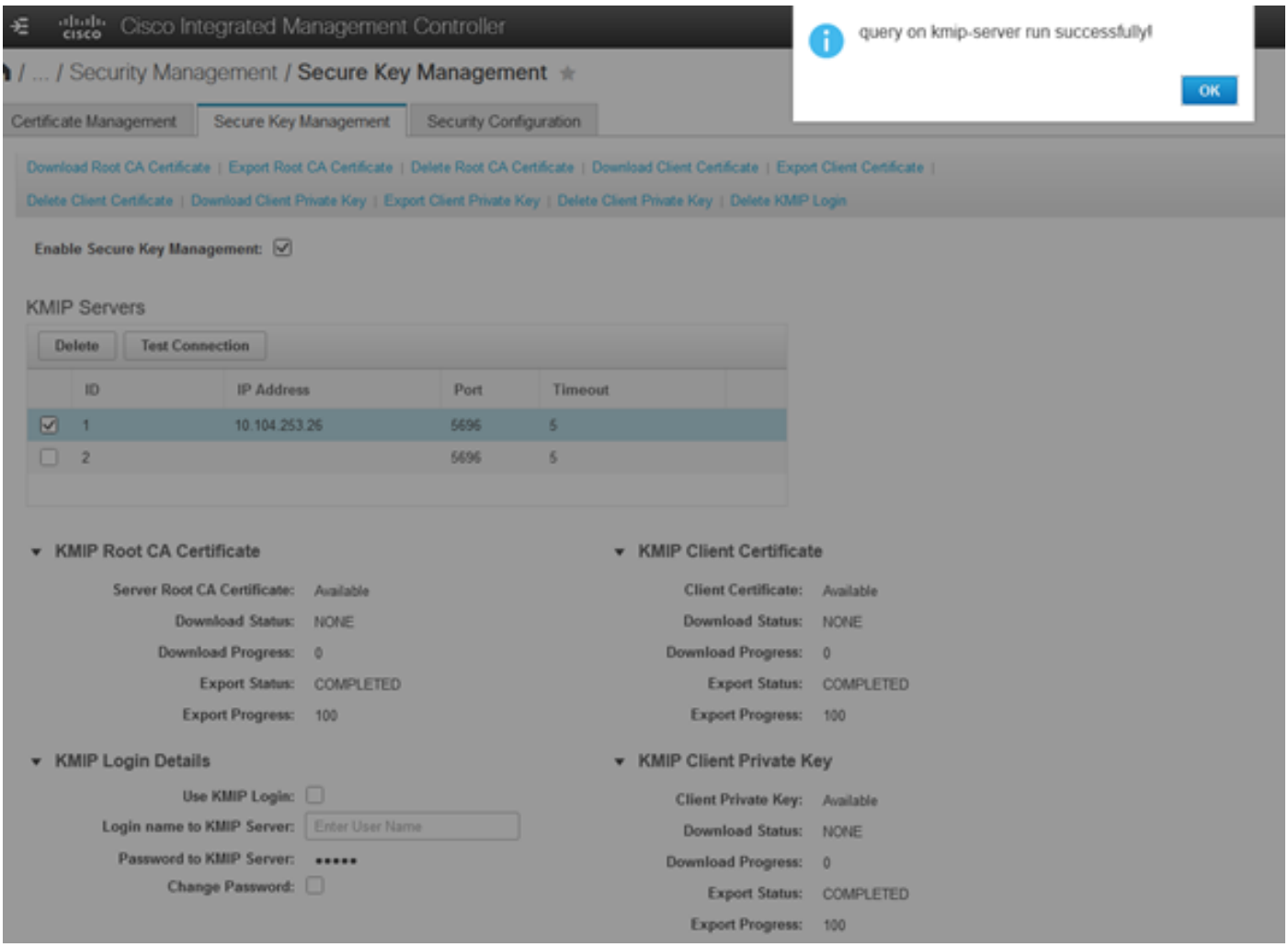
4.上傳證書時，您會看到證書顯示為**Available**，對於未上傳的缺失證書，您會看到**Not Available**。

僅當所有證書和私鑰都已成功下載到CIMC時，才能測試連線。



5.（可選）一旦您擁有所有證書，則可以選擇新增KMIP伺服器的使用者和密碼，只有作為第三方KMIP伺服器的SafeNet才支援此配置。

6.測試連線，如果證書正確，並且可以通過配置的埠訪問KMIP伺服器，則連線成功。

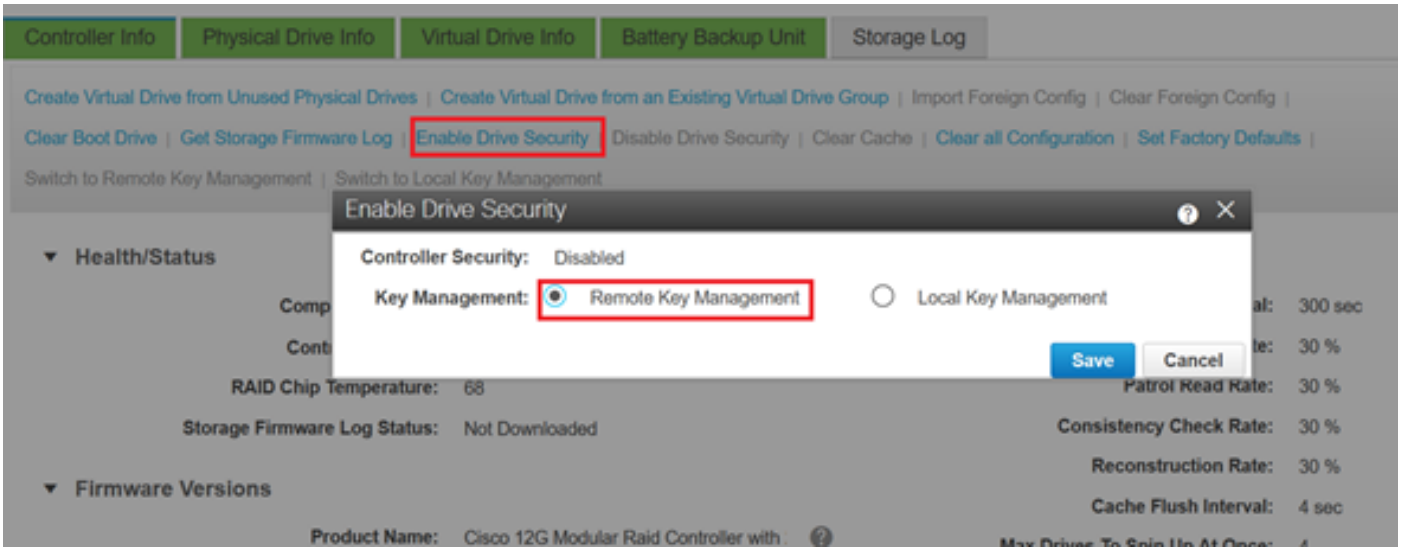


7.一旦我們與KMIP的連線成功，就可以啟用遠端金鑰管理。

導覽至**Networking > Modular Raid Controller > Controller Info**。

選擇**Enable Drive Security**，然後選擇**Remote Key Management**。

> **附註**：如果以前啟用了**Local Key Management**，則會要求您輸入當前金鑰，以便進行遠端管理



驗證

使用本節內容，確認您的組態是否正常運作。

您可以在CLI中驗證設定。

1.驗證是否已啟用KMIP。

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

2.檢驗IP地址、埠和超時。

```
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.驗證證書是否可用。

```
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.驗證登入詳細資訊。

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

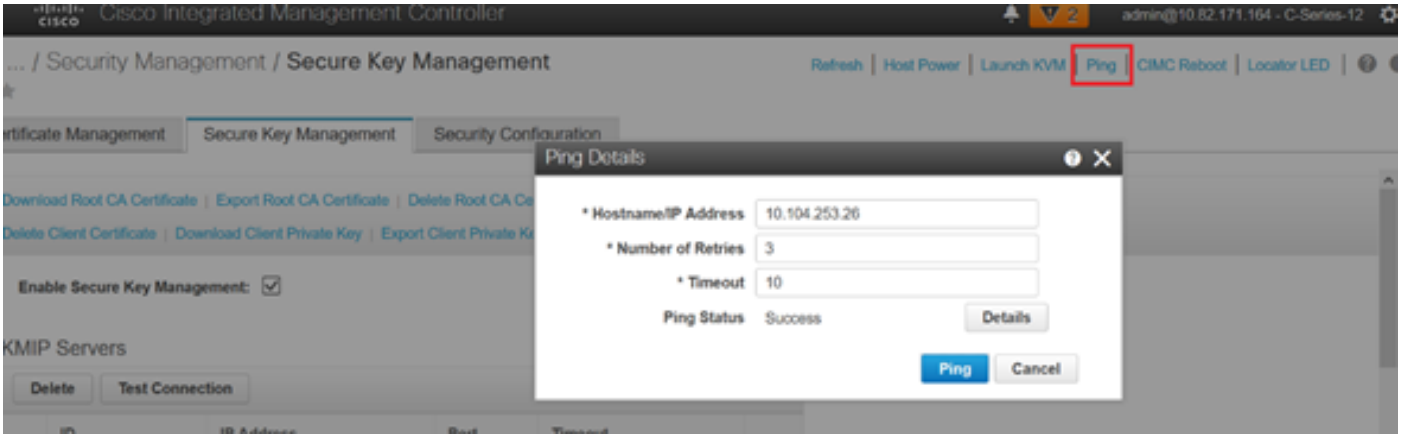
5.測試連線。

```
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!
```

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

如果與KMIP伺服器的測試連線失敗，請確保可以ping通該伺服器。



確保在CIMC和KMIP伺服器上開啟埠5696。您可以在我們的PC上安裝NMAP版本，因為此命令在CIMC上不可用。

可以在本地電腦上安裝NMAP，以測試埠是否開啟；在安裝檔案的目錄下，使用以下命令：

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

輸出顯示KMIP服務的開放埠：

```
C:\Program Files (x86)\Nmap>nmap 10.201.201.21 -p 5696
Starting Nmap 7.91 ( https://nmap.org ) at 2020-10-21 12:07 Central Daylight Time (Mexico)
Nmap scan report for 10.201.201.21
Host is up (0.00s latency).

PORT     STATE    SERVICE
5696/tcp filtered kmip
MAC Address: 00:11:22:33:44:55 (Cimsys)

Nmap done: 1 IP address (1 host up) scanned in 1.67 seconds

C:\Program Files (x86)\Nmap>
```

輸出顯示KMIP服務的關閉埠：

```
C:\Program Files (x86)\Nmap>nmap 10.31.123.121 -p 5696
Starting Nmap 7.91 ( https://nmap.org ) at 2020-10-21 12:06 Central Daylight Time (Mexico)
Nmap scan report for mxsv_tac_vm_5.cisco.com (10.31.123.121)
Host is up (0.036s latency).

PORT     STATE  SERVICE
5696/tcp closed kmip
MAC Address: 00:11:22:33:44:55 (Cimsys)

Nmap done: 1 IP address (1 host up) scanned in 1.71 seconds
```

相關資訊

- C系列配置指南 — 自我加密驅動器
- C系列配置指南 — 金鑰管理互操作性協定
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。