スタンドアロンラックサーバでのリモートキー管理の設定

内容

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[背景説明](#)
[SEDドライブ](#)
[設定](#)
[クライアント秘密キーとクライアント証明書の作成](#)
[CIMCでのKMIPサーバの設定](#)
[確認](#)
[トラブルシュート](#)
[関連情報](#)

概要

このドキュメントでは、スタンドアロンラックサーバでのKey Management Interoperability Protocol(KMIP)の設定について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco インテグレーテッド マネージメント コントローラ（CIMC）
- 自己暗号化ドライブ(SED)
- KMIP

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- UCSC-C220-M4S、CIMCバージョン：4.1(1h)
- SEDドライブ
- 800 GBエンタープライズパフォーマンスSAS SED SSD(10 FWPD) - MTFDJAK800MBS
- ドライブ部品ID:UCS-SD800GBEK9
- ベンダー：ミクロン
- Model:S650DC-800FIPS
- サードパーティのキーマネージャとしてのメトリック

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

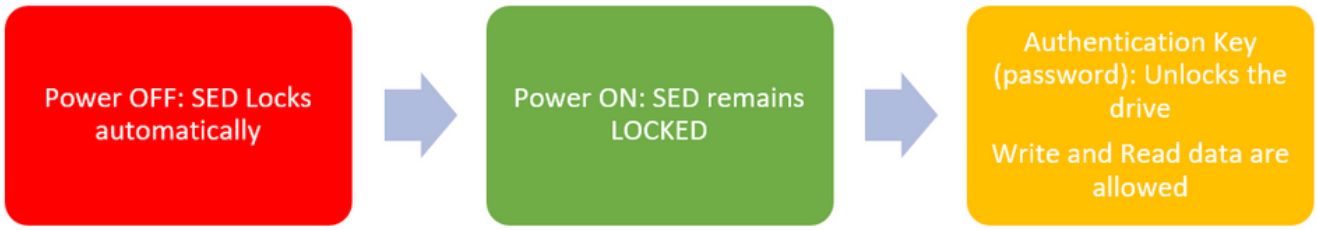
KMIPは、キー管理サーバ上の暗号キーを操作するためのメッセージ形式を定義する拡張可能な通信プロトコルです。これにより、暗号化キーの管理が簡素化されるため、データの暗号化が容易になります。

SEDドライブ

SEDは、暗号化回路が内蔵されたハードディスクドライブ(HDD)またはソリッドステートドライブ(SSD)です。メディアに書き込まれたすべてのデータを透過的に暗号化し、ロック解除されると、メディアから読み取られたすべてのデータを透過的に復号化します。

SEDでは、暗号化キー自体がSEDハードウェアの制約を離れることはないため、OSレベルの攻撃から安全です。

SEDドライブワークフロー：



（ー）SEDドライブフロー

ドライブのロックを解除するためのパスワードは、**ローカルキー管理**設定を使用してローカルで取得できます。この設定では、ユーザがキー情報を記憶する必要があります。また、Remote Key Management(RRM)を使用して、セキュリティキーを作成してKMIPサーバから取得することもできます。ユーザの責任は、CIMCでKMIPサーバを設定することです。

設定

クライアント秘密キーとクライアント証明書の作成

これらのコマンドは、Cisco IMCではなく、OpenSSLパッケージを搭載したLinuxマシンで入力する必要があります。ルートCA証明書とクライアント証明書で共通名が同じであることを確認します。

> **注**：Cisco IMC時間が現在の時間に設定されていることを確認します。

1. 2048ビットのRSAキーを作成します。

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

2.既に作成されているキーを使用して自己署名証明書を作成します。

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

3.ルートCA証明書の取得の詳細については、KMIPベンダーのドキュメントを参照してください。

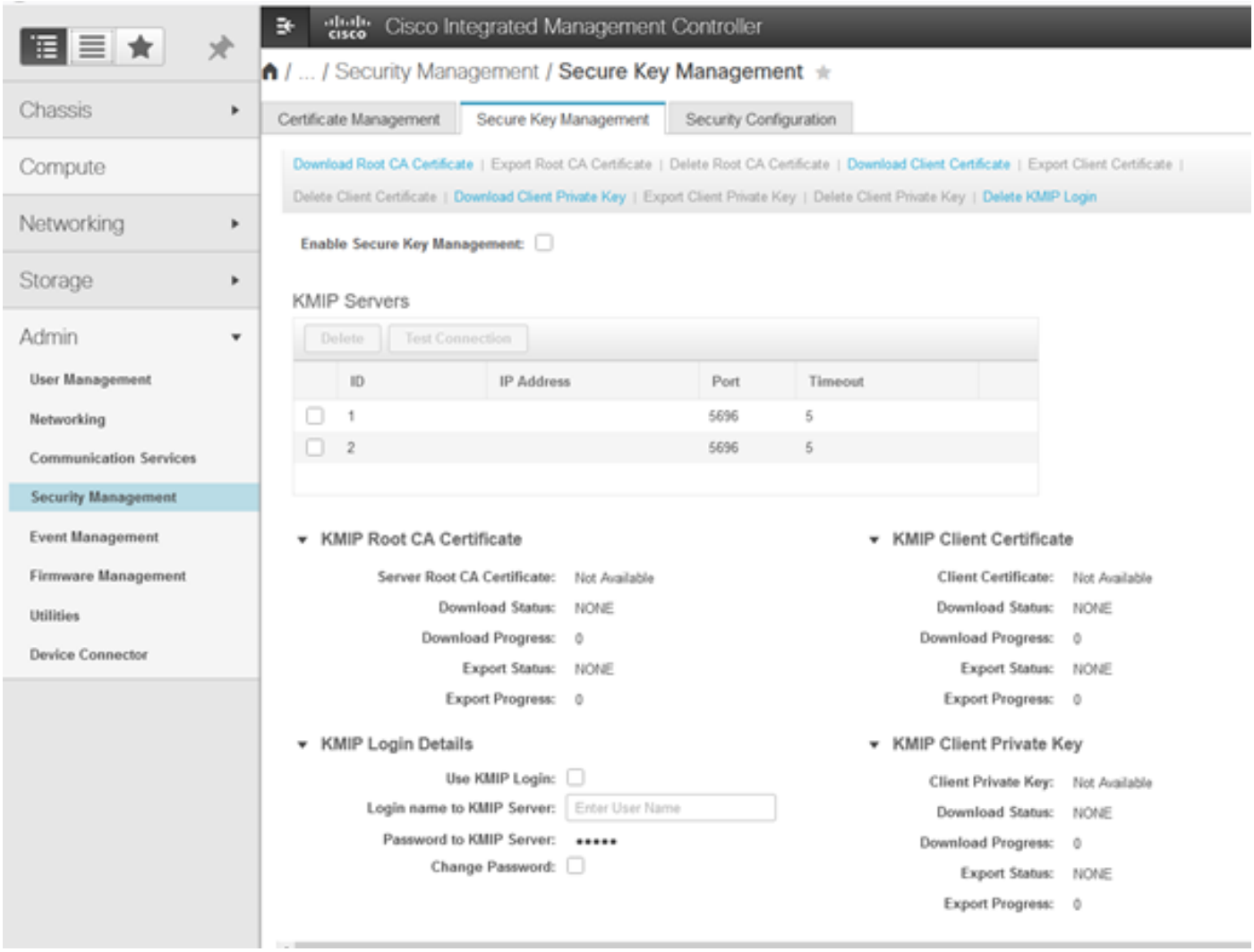
注：Vormetricでは、RootCa証明書内の共通名がVormetricホストのホスト名と一致する必要があります。

注：KMIPベンダーの設定ガイドにアクセスするには、アカウントが必要です。
SafeNet
渦の

CIMCでのKMIPサーバの設定

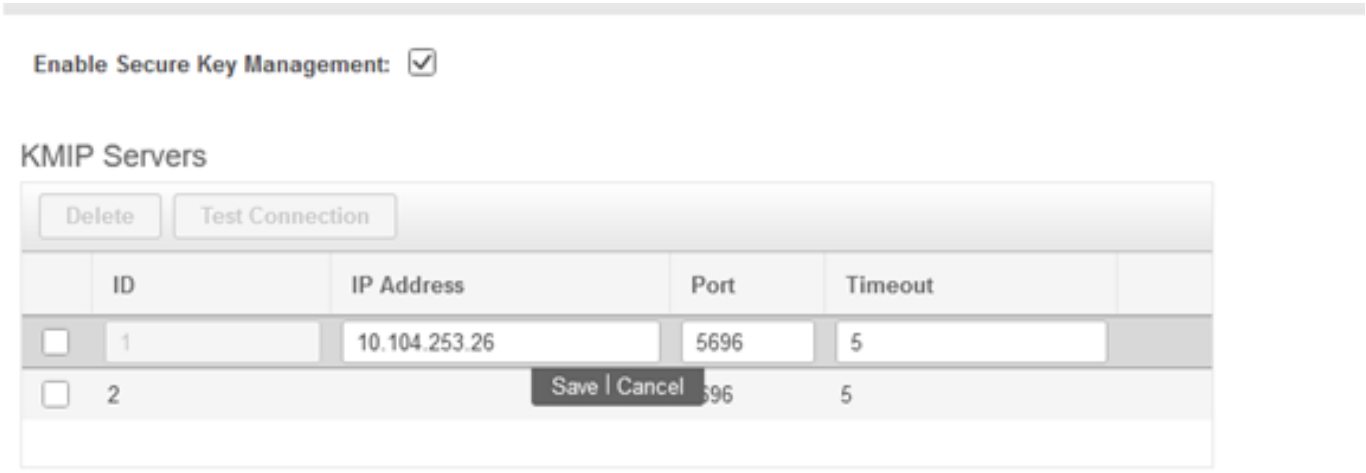
1. [Admin] > [Security Management] > [Secure Key Management] に移動します。

明確な設定は次のとおりです **Export/Delete** buttons grayed out, only **Download** buttons are active.

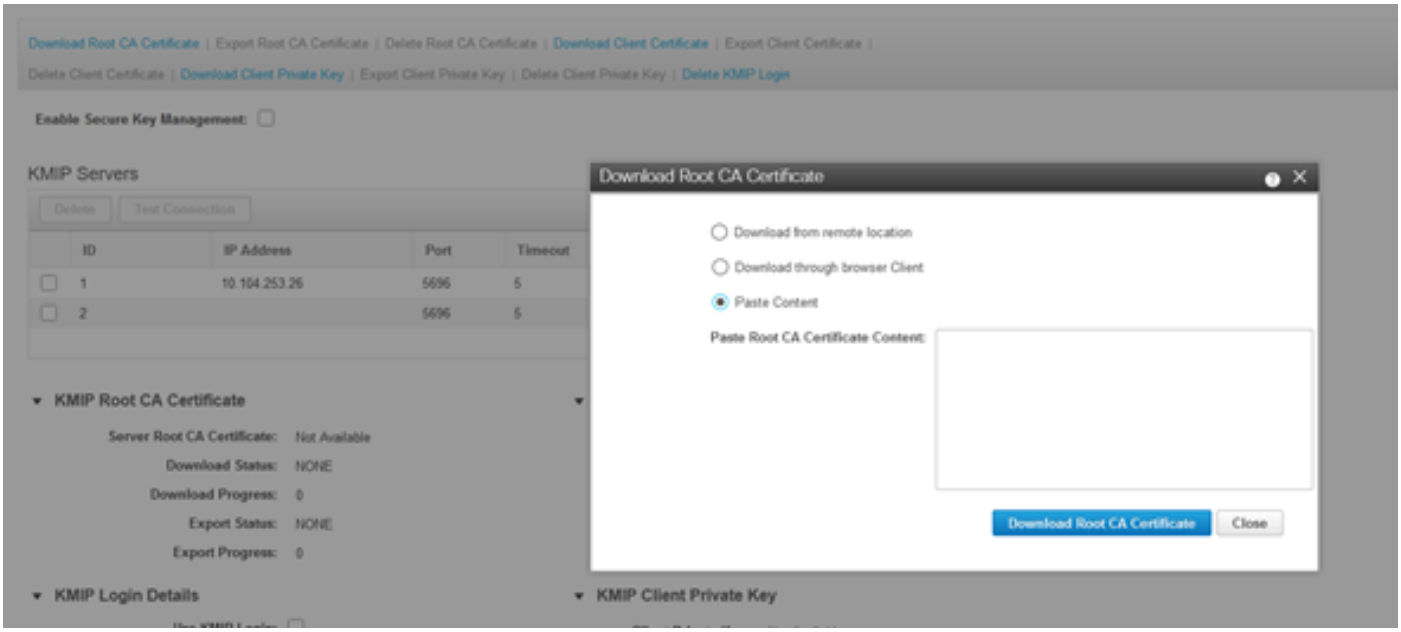


2. IPアドレスをクリックし、KMIPサーバーのIPを設定します。IPアドレスに到達できることを確

認し、デフォルト・ポートが使用されている場合は変更する必要がなければ、変更を保存します。



3.証明書と秘密キーをサーバにダウンロードします。ダウンロード可能な **.pem** file or just paste the content.

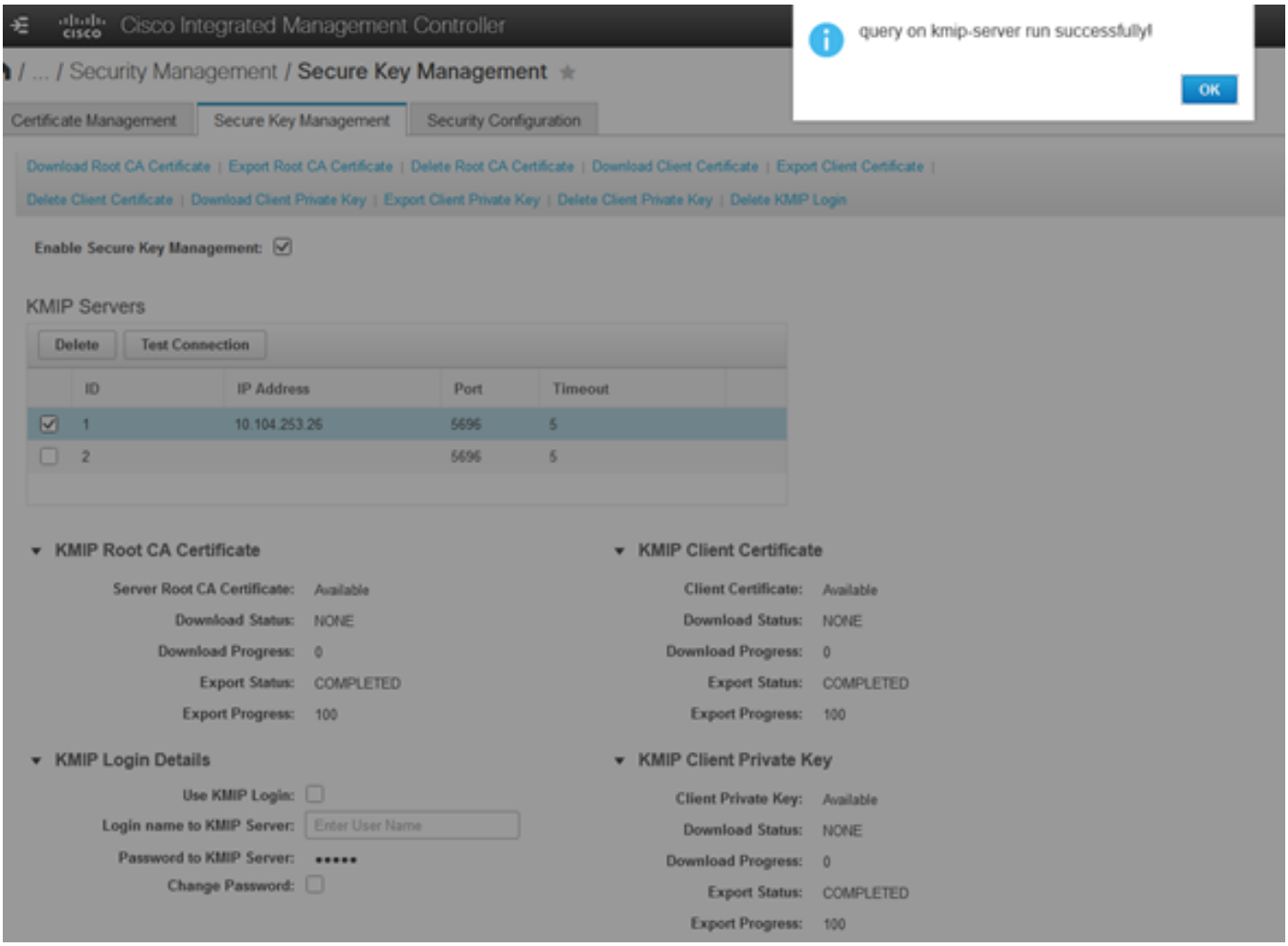


4.証明書をアップロードすると、証明書が[Available] と表示され、アップロードされていない不足している証明書には[Not Available] と表示されます。

接続をテストできるのは、すべての証明書と秘密キーがCIMCに正常にダウンロードされた場合だけです。

5.（オプション）すべての証明書を取得したら、オプションでKMIPサーバのユーザとパスワードを追加できます。この設定は、サードパーティのKMIPサーバとしてのSafeNetに対してのみサポートされます。

6.接続をテストし、証明書が正しく、設定されたポートを介してKMIPサーバに到達できる場合は、正常に接続されていることを確認します。

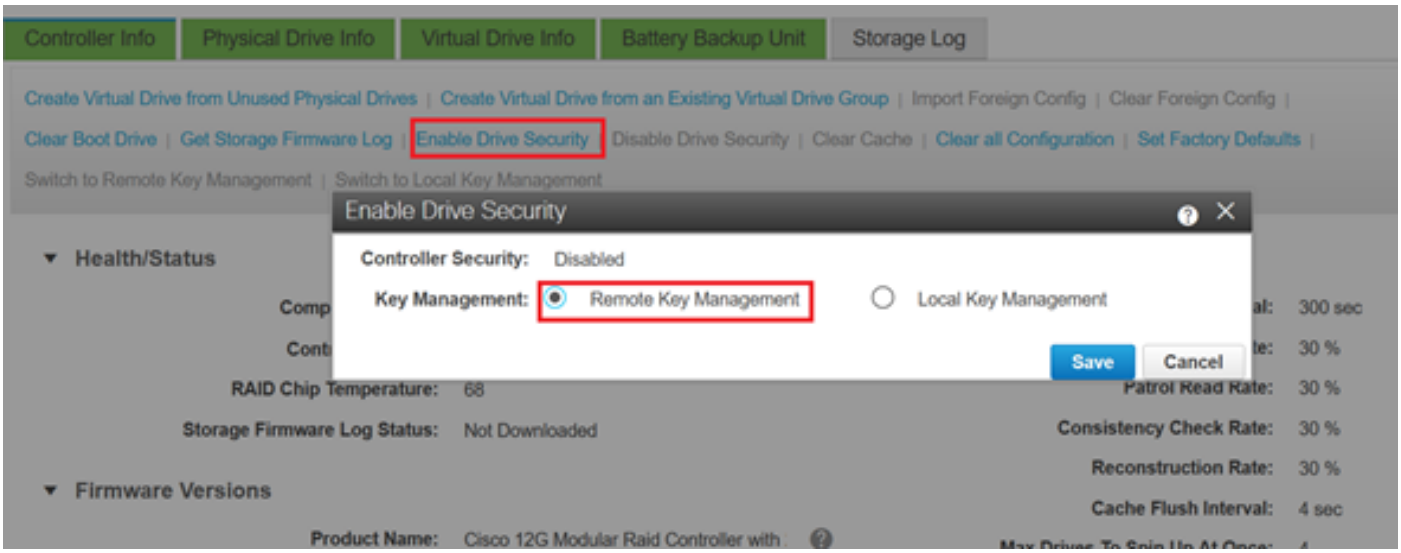


7. KMIPとの接続が成功したら、リモートキー管理を有効にできます。

[Networking] > [Modular Raid Controller] > [Controller Info] に移動します。

[Enable Drive Security] を選択し、次に[Remote Key Management] を選択します。

> **注：以前にローカルキー管理が有効になっていた場合は、リモート管理に変更するために現在のキーを入力するように求められます**



確認

ここでは、設定が正常に機能しているかどうかを確認します。

CLIから設定を確認できます。

1. KMIPが有効かどうかを確認します。

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

2. IPアドレス、ポート、およびタイムアウトを確認します。

```
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.証明書が使用可能かどうかを確認します。

```
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.ログインの詳細を確認します。

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

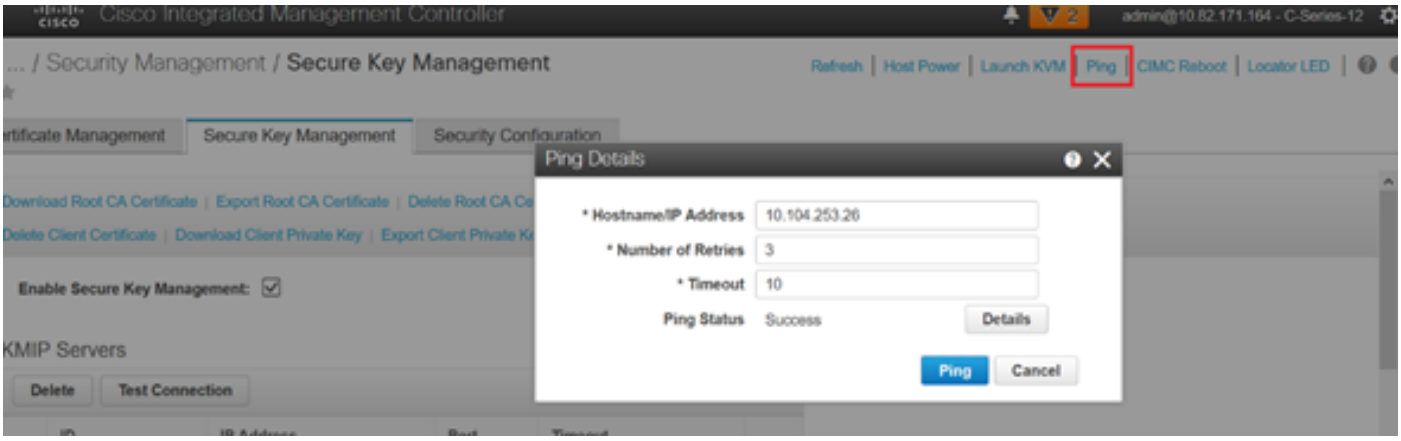
5.接続をテストします。

```
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!
```

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。

KMIPサーバとのテスト接続が成功しない場合は、サーバにpingできることを確認します。



CIMCとKMIPサーバでポート5696が開いていることを確認します。このコマンドはCIMCでは使用できないため、NMAPバージョンをPCにインストールできます。

ローカルマシンにNMAPをインストールして、ポートが開いているかどうかをテストできます。ファイルがインストールされたディレクトリで、次のコマンドを使用します。

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

出力は、KMIPサービスのオープンポートを示しています。

```
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>
```

出力は、KMIPサービスのクローズポートを示しています。

```
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
```

関連情報

- Cシリーズ構成ガイド – 自己暗号化ドライブ
- Cシリーズ構成ガイド – Key Management Interoperability Protocol
- テクニカル サポートとドキュメント – Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。