在独立机架式服务器上配置远程密钥管理

目录

简介

本文档介绍在独立机架式服务器上配置密钥管理互操作性协议(KMIP)。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科集成管理控制器(CIMC)
- 自加密驱动器(SED)
- KMIP

使用的组件

本文档中的信息基于以下软件和硬件版本：

- UCSC-C220-M4S，CIMC版本：4.1(1h)
- SED驱动器
- 800GB企业性能SAS SED SSD(10 FWPD)- MTFDJAK800MBS
- 驱动器部件ID:UCS-SD800GBEK9
- 供应商：微米
- 型号：S650DC-800FIPS
- Vormetric作为第三方密钥管理器

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

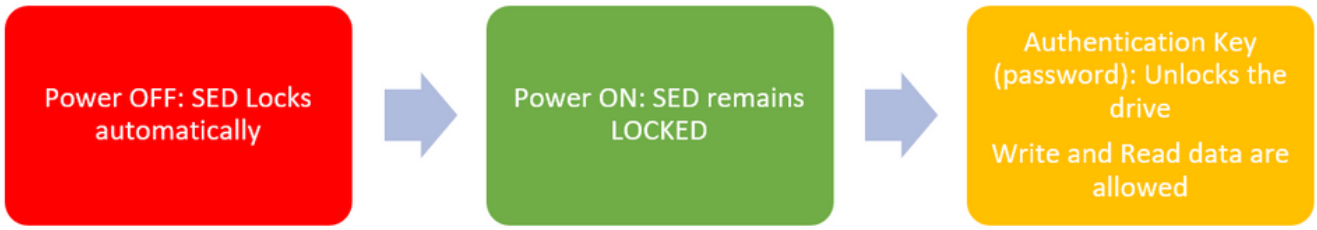
KMIP是一种可扩展的通信协议，它定义了用于在密钥管理服务器上处理加密密钥的消息格式。由于简化了加密密钥管理，这有利于数据加密。

SED驱动器

SED是硬盘驱动器(HDD)或固态驱动器(SSD)，驱动器内置加密电路。它以透明方式加密写入介质的所有数据，并在解锁后以透明方式解密从介质读取的所有数据。

在SED中，加密密钥本身不会离开SED硬件的范围，因此可以安全抵御操作系统级别的攻击。

SED驱动工作流程：



1. SED驱动器流

使用**本地密钥管理**配置可以在本地获取解锁驱动器的密码，用户负责记住密钥信息。它也可以通过远程密钥管理获取，其中从KMIP服务器创建并获取安全密钥，用户负责在CIMC中配置KMIP服务器。

配置

创建客户端私钥和客户端证书

这些命令将使用OpenSSL包在Linux计算机上输入，而不是在Cisco IMC中。确保根CA证书和客户端证书中的公用名相同。

> **注意**：确保Cisco IMC时间设置为当前时间。

1.创建2048位RSA密钥。

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

2.使用已创建的密钥创建自签名证书。

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

3.有关获取根CA证书的详细信息，请参阅KMIP供应商文档。

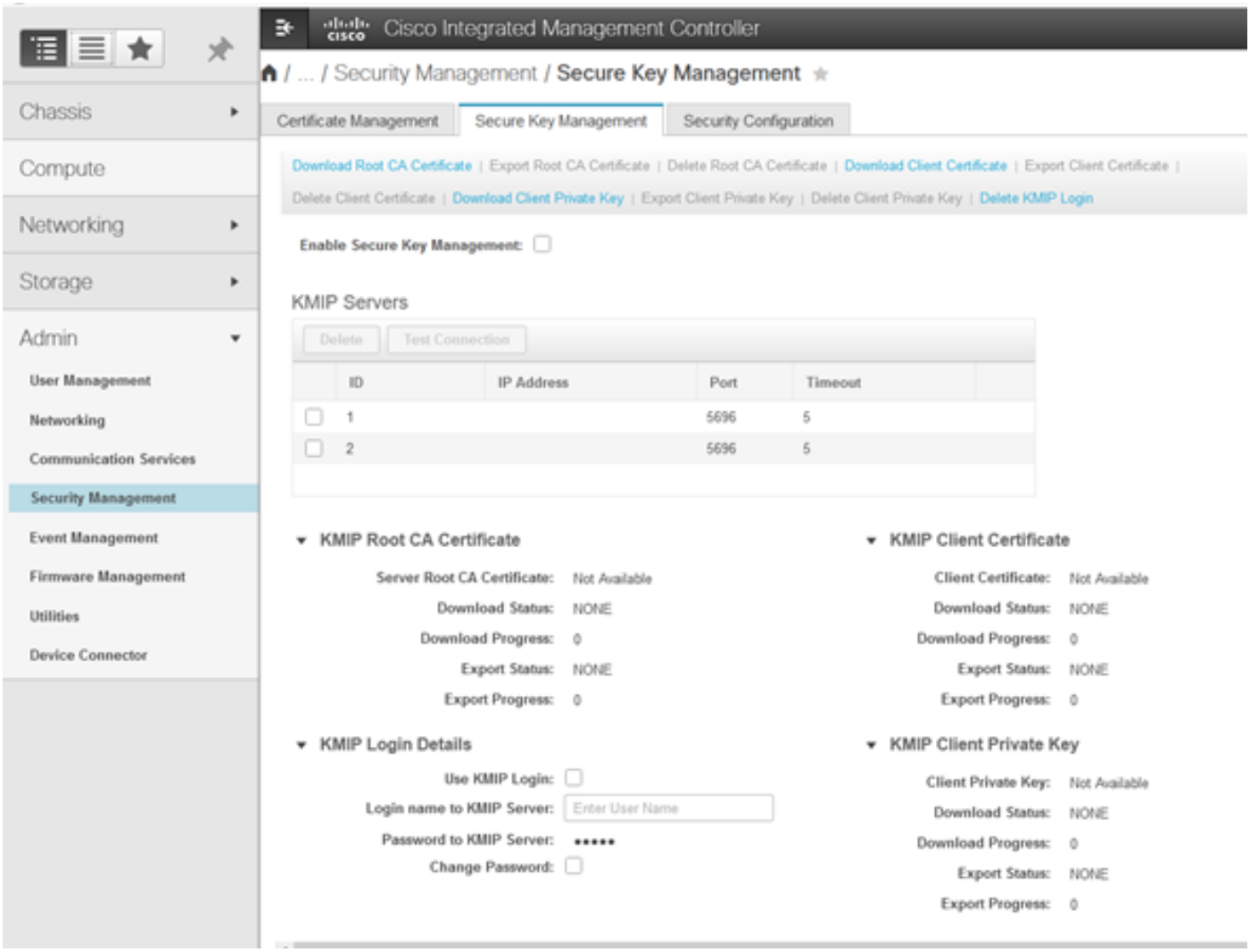
> **注意**：Vormetric要求RootCa证书中的公用名称与Vormetric主机的主机名匹配。

注意：您必须拥有帐户才能访问KMIP供应商的配置指南：
SafeNet
涡度

在CIMC上配置KMIP服务器

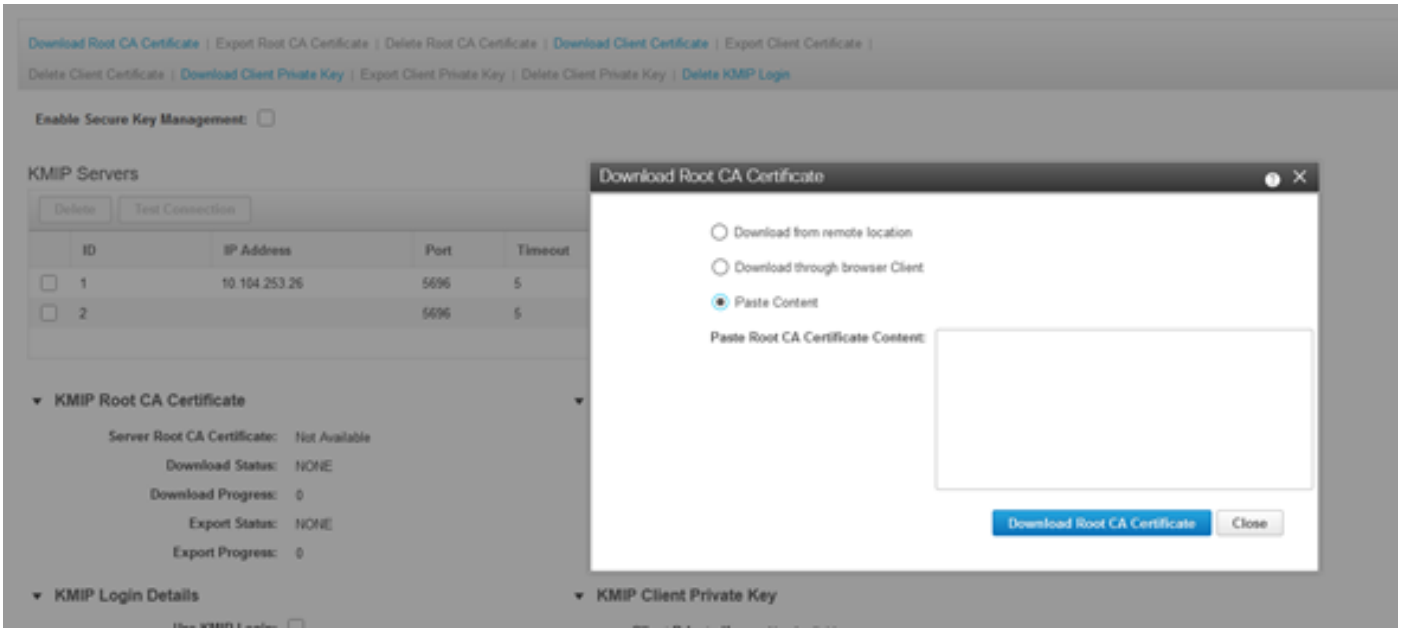
1.导航到**Admin > Security Management > Secure Key Management。**

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



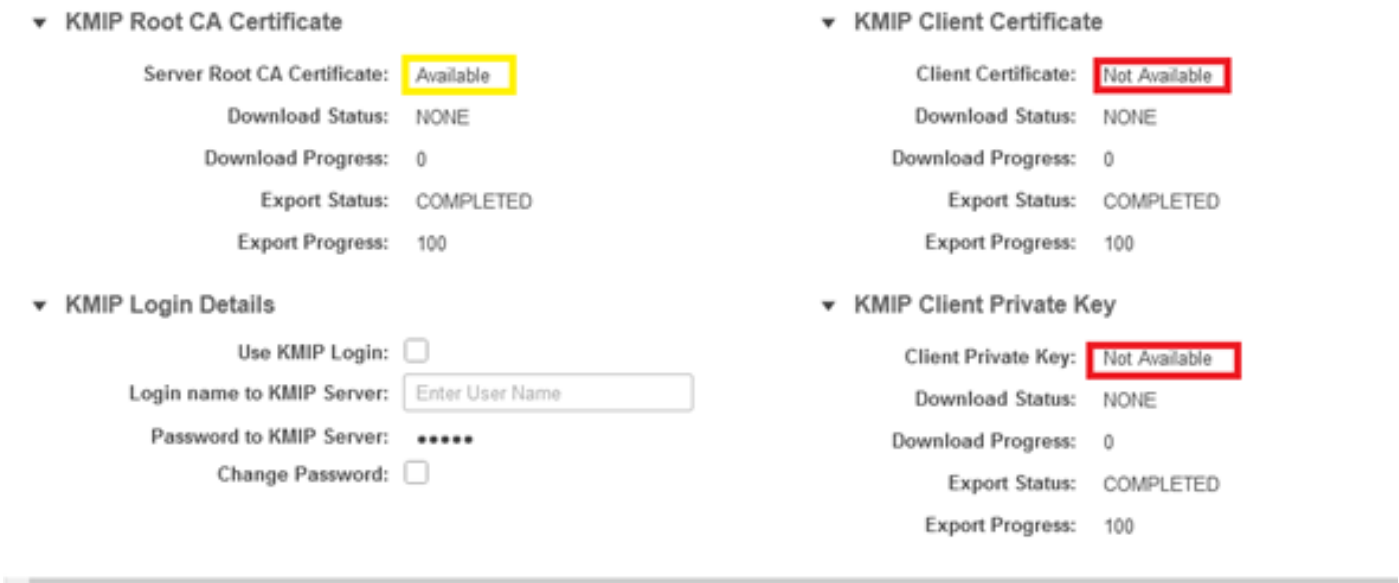
2.单击IP地址并设置KMIP服务器的IP，确保您能够访问它，如果默认端口已被使用，则无需更改任何其他内容，然后保存更改。

3.将证书和私钥下载到服务器。您可以下载 **.pem** file or just paste the content.



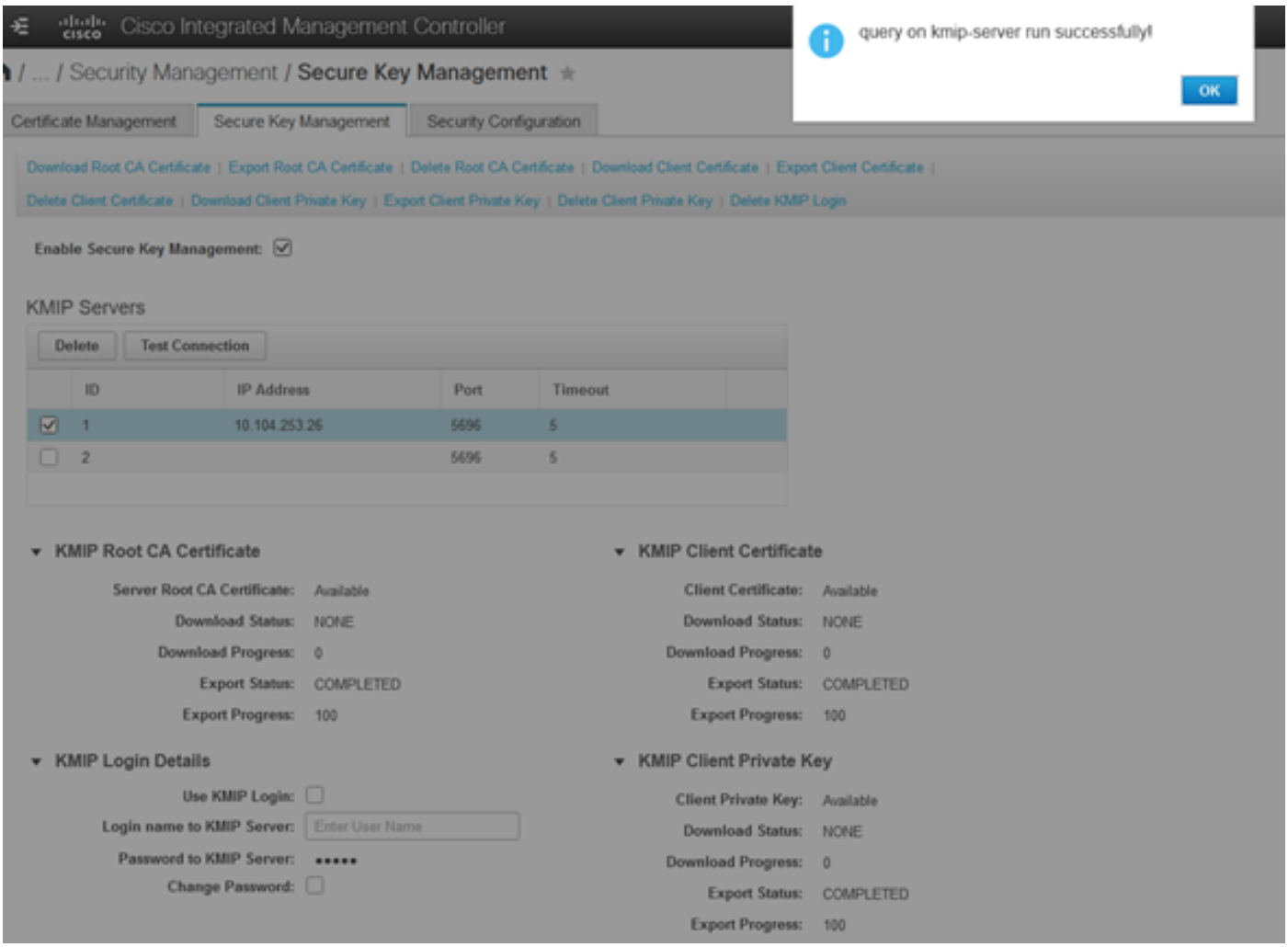
4.上传证书时，您会看到证书显示为**Available**，对于未上传的缺失证书，您会看到**Not Available**。

仅当所有证书和私钥都已成功下载到CIMC时，才能测试连接。



5.（可选）一旦您拥有所有证书，您可以选择添加KMIP服务器的用户和密码，此配置仅作为第三方KMIP服务器受SafeNet支持。

6.测试连接，如果证书正确，并且可以通过配置的端口访问KMIP服务器，则会看到连接成功。

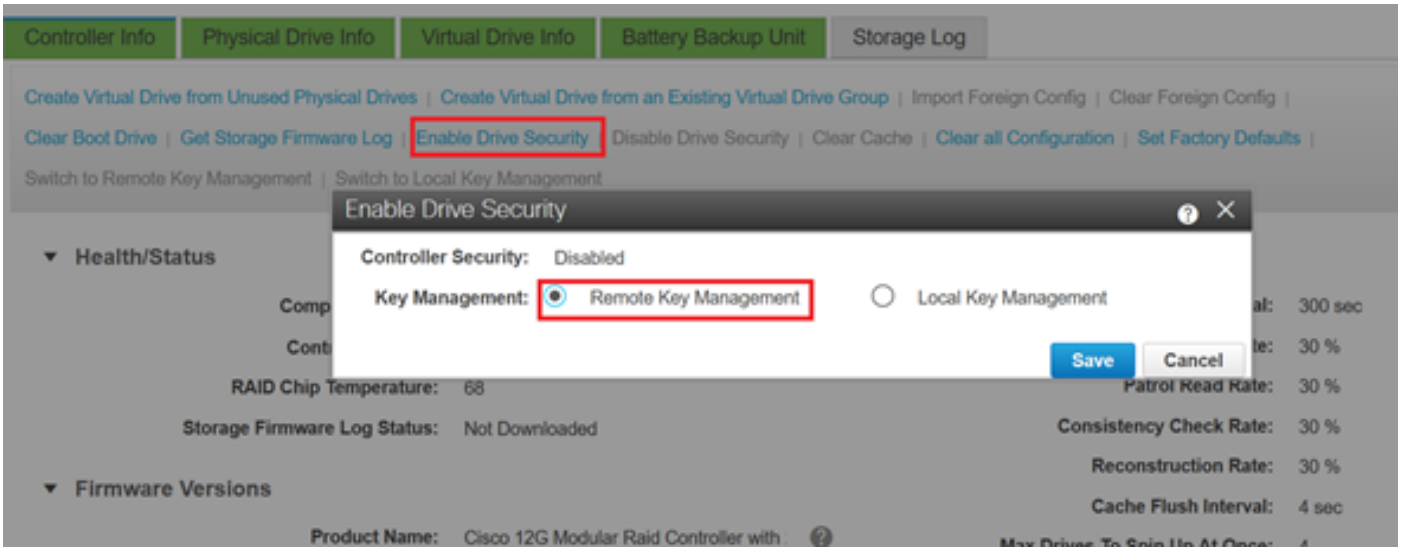


7.一旦我们与KMIP的连接成功，您可以启用远程密钥管理。

导航到**网络>模块化Raid控制器>控制器信息**。

选择**Enable Drive Security**，然后选择**Remote Key Management**。

> **注意：**如果之前启用了**本地密钥管理**，则会要求您输入当前密钥以便进行远程管理



验证

使用本部分可确认配置能否正常运行。

从CLI，您可以验证配置。

1.验证是否已启用KMIP。

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

2.检验IP地址、端口和超时。

```
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.验证证书是否可用。

```
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.验证登录详细信息。

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

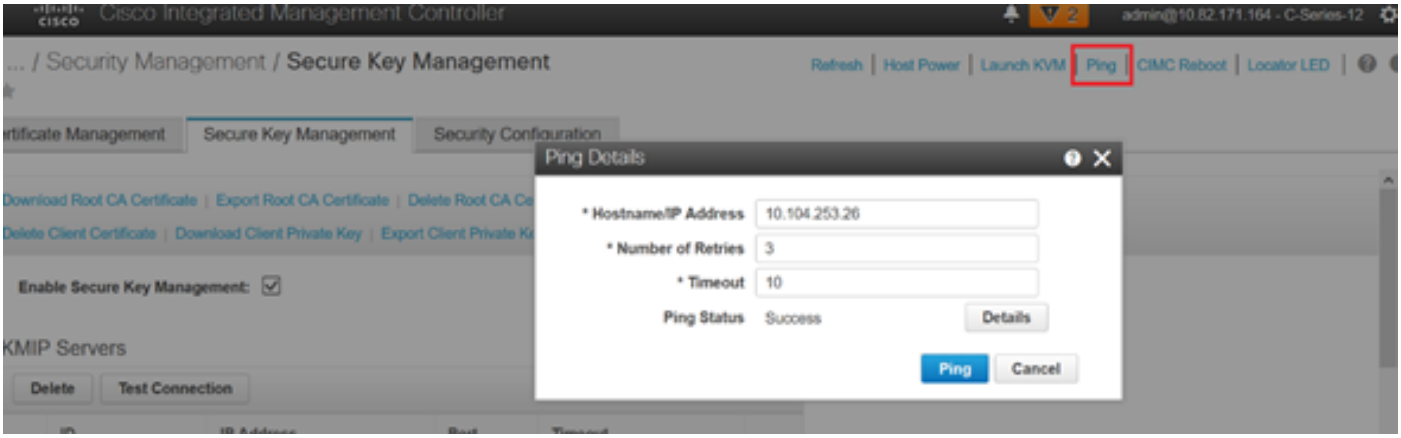
5.测试连接。

```
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!
```

故障排除

目前没有针对此配置的故障排除信息。

如果与KMIP服务器的测试连接失败，请确保可以ping通服务器。



确保在CIMC和KMIP服务器上打开端口5696。您可以在我们的PC上安装NMAP版本，因为此命令在CIMC上不可用。

您可以在本地计算机上安装NMAP，以测试端口是否打开；在文件安装目录下，使用以下命令：

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

输出显示KMIP服务的开放端口：

```
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>
```

输出显示KMIP服务的关闭端口：

```
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
```

相关信息

- C系列配置指南 — 自我加密驱动器
- C系列配置指南 — 密钥管理互操作性协议
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。