Configurar o gerenciamento remoto de chaves em servidores em rack autônomos

Contents

Introduction

Este documento descreve a configuração do KMIP em servidores rack autônomos.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Controlador de gerenciamento integrado da Cisco (CIMC)
- Unidade com autocriptografia (SED)
- KMIP

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- UCSC-C220-M4S, Versão do CIMC: 4.1 (1h)
- Unidades SED
- SSD SAS SED de desempenho empresarial de 800 GB (10 FWPD) - MTFDJAK800 MBS
- ID da peça da unidade: UCS-SD800GBEK9
- Fornecedor: MÍCRON
- Modelo: S650DC-800FIPS
- Vormétrico como gerenciador de chave de terceiros

The information in this document was created from the devices in a specific lab environment. All of

the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

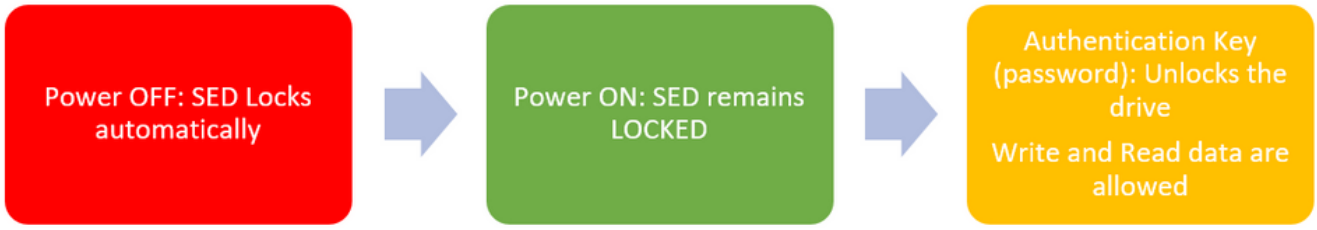
O KMIP é um protocolo de comunicação extensível que define formatos de mensagem para a manipulação de chaves criptográficas em um servidor de gerenciamento de chaves. Isso facilita a criptografia de dados porque simplifica o gerenciamento da chave de criptografia.

Unidades SED

Uma SED é uma unidade de disco rígido (HDD) ou unidade de estado sólido (SSD) com um circuito de criptografia integrado à unidade. Criptografa de forma transparente todos os dados gravados na mídia e, quando desbloqueada, descriptografa de forma transparente todos os dados lidos na mídia.

Em um SED, as próprias chaves de criptografia nunca deixam os limites do hardware do SED e, portanto, estão protegidas de ataques no nível do SO.

Fluxo de trabalho das unidades SED:



1. Fluxo da unidade SED

A senha para desbloquear a unidade pode ser obtida localmente com a configuração **Local Key Management**, onde a responsabilidade do usuário é lembrar as informações da chave. Ele também pode ser obtido com o Gerenciamento remoto de chaves, no qual a chave de segurança é criada e buscada em um servidor KMIP e a responsabilidade do usuário é configurar o servidor KMIP no CIMC.

Configurar

Criar uma chave privada e um certificado de cliente

Esses comandos devem ser inseridos em uma máquina Linux com o pacote OpenSSL, não no Cisco IMC. Verifique se o Nome comum é o mesmo no certificado CA raiz e no certificado do cliente.

> **Note**: Verifique se a hora do Cisco IMC está definida para a hora atual.

1. Crie uma chave RSA de 2048 bits.

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

2. Crie um certificado autoassinado com a chave já criada.

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

3. Consulte a documentação do fornecedor do KMIP para obter detalhes sobre a obtenção do certificado de CA raiz.

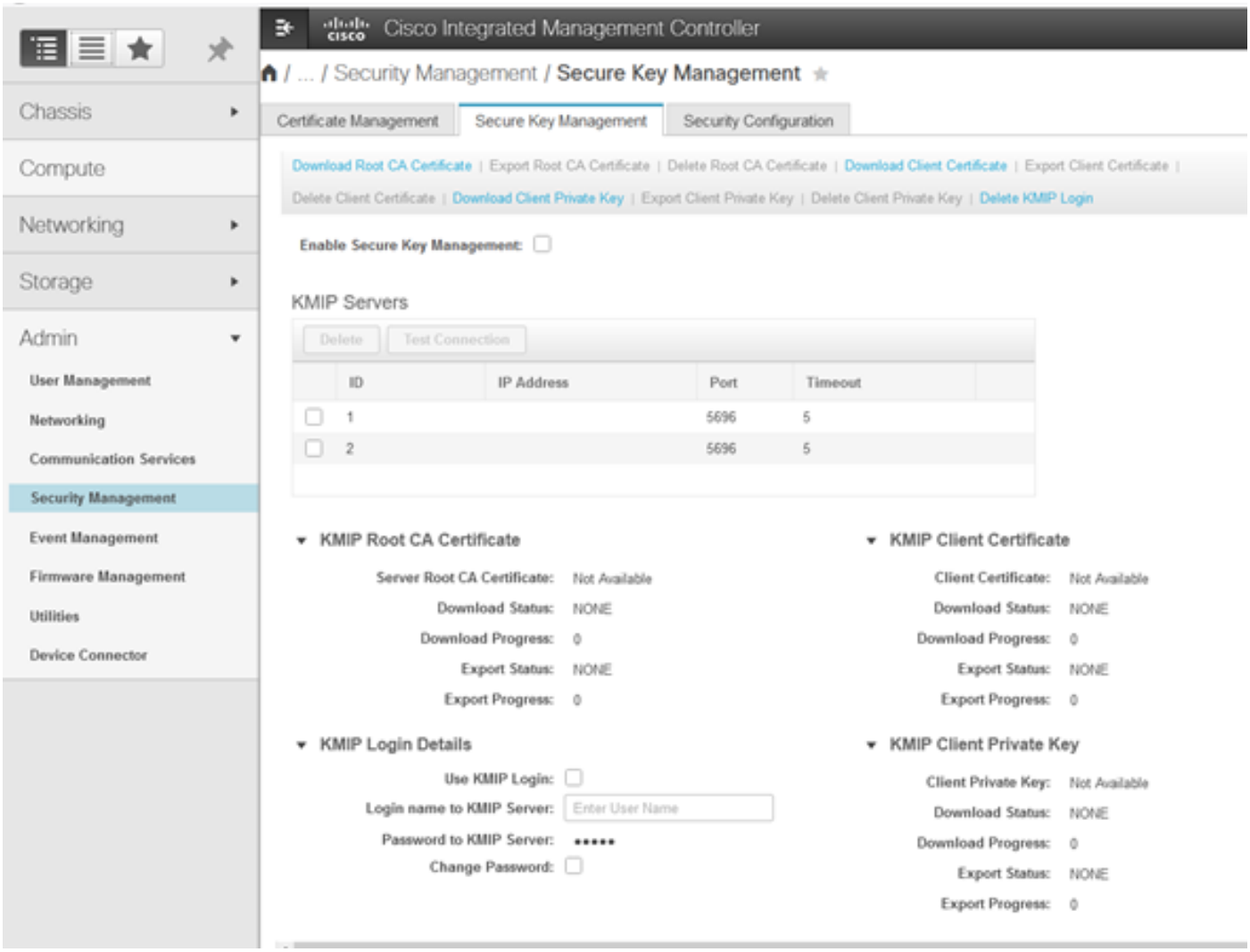
> **Note**: O Vormetric requer que o nome comum no certificado RootCa corresponda ao nome de host do host Vormétrico.

> **Note**: Você deve ter uma conta para ter acesso aos guias de configuração dos fornecedores KMIP:
> SafeNet
> Vormétrico

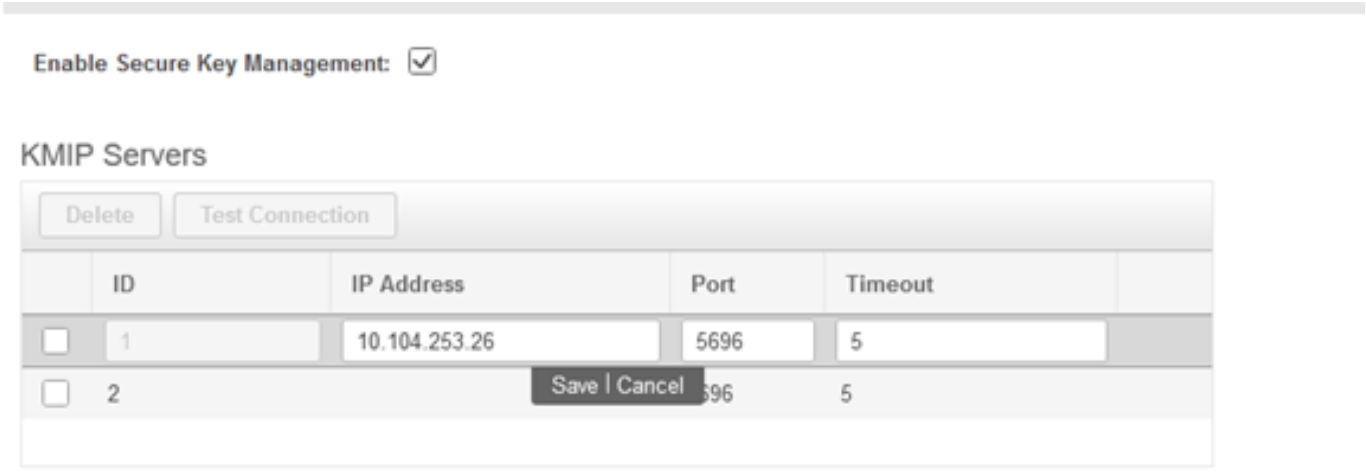
Configurar o servidor KMIP no CIMC

1. Navegue até **Admin > Security Management > Secure Key Management.**

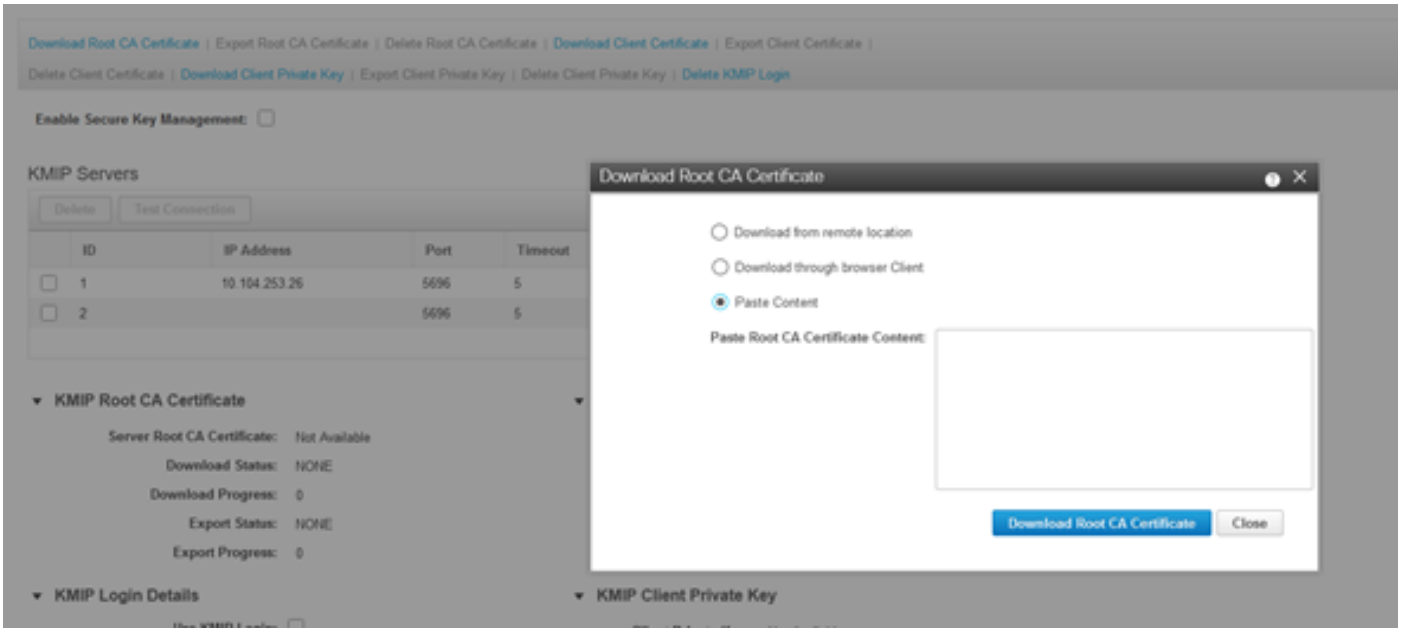
Uma configuração simples mostra **Export/Delete** buttons grayed out, only **Download** buttons are active.



2. Clique no endereço IP e defina o IP para o servidor KMIP, certifique-se de que você pode acessá-lo e, caso a porta padrão seja usada, nada mais precisa ser alterado, então salve as alterações.

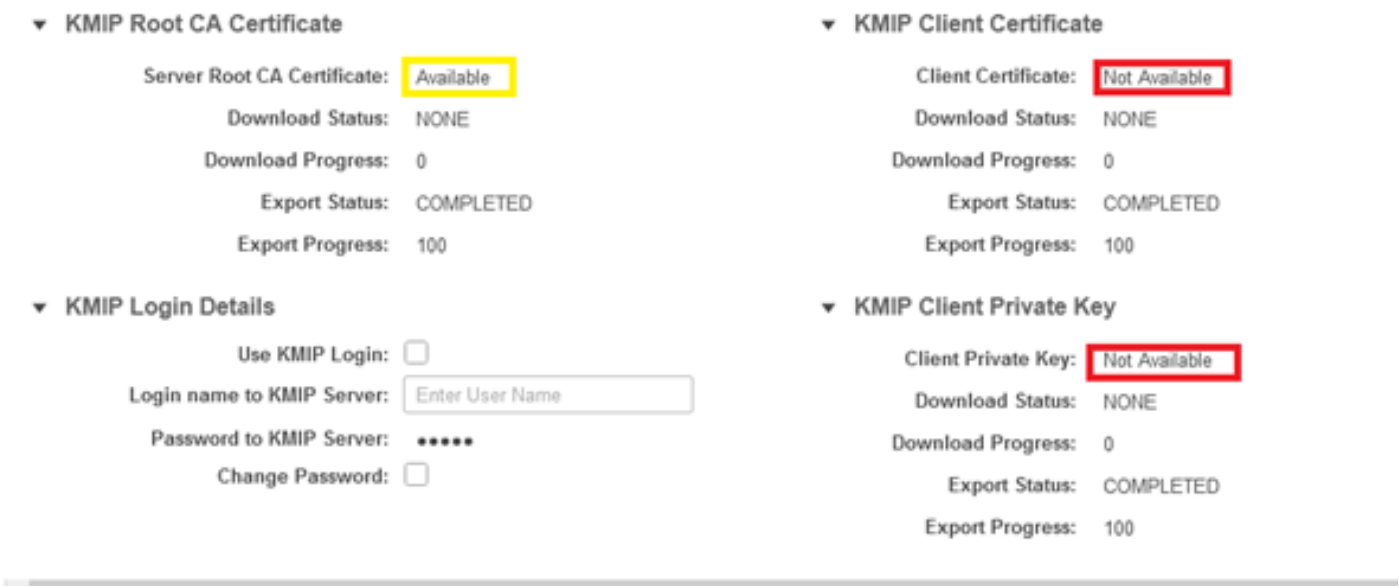


3. Baixe os certificados e a chave privada para o servidor. Você pode baixar o **.pem** file or just paste the content.



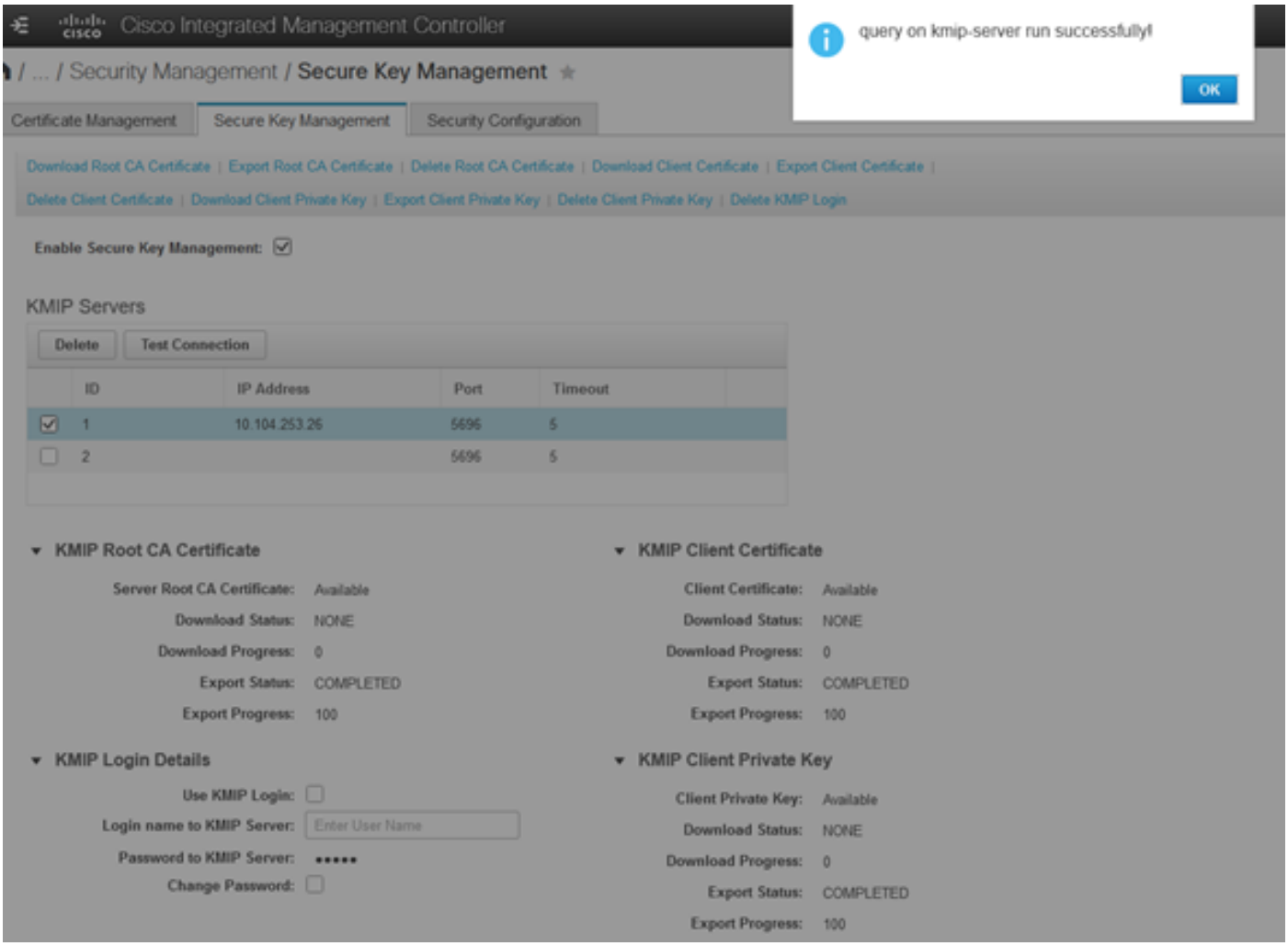
4. Ao fazer upload dos certificados, você verá que os certificados são exibidos como **Disponível**; para os certificados ausentes que não estão carregados, você verá **Não Disponível**.

Você só poderá testar a conexão quando todos os certificados e chaves privadas tiverem sido baixados com êxito no CIMC.



5. (opcional) Depois de ter todos os certificados, você pode opcionalmente adicionar o usuário e senha para o servidor KMIP, esta configuração é suportada somente para o SafeNet como um servidor KMIP de terceiros.

6. Teste a conexão e, se os certificados estiverem corretos e você puder acessar o servidor KMIP através da porta configurada, verá uma conexão bem-sucedida.

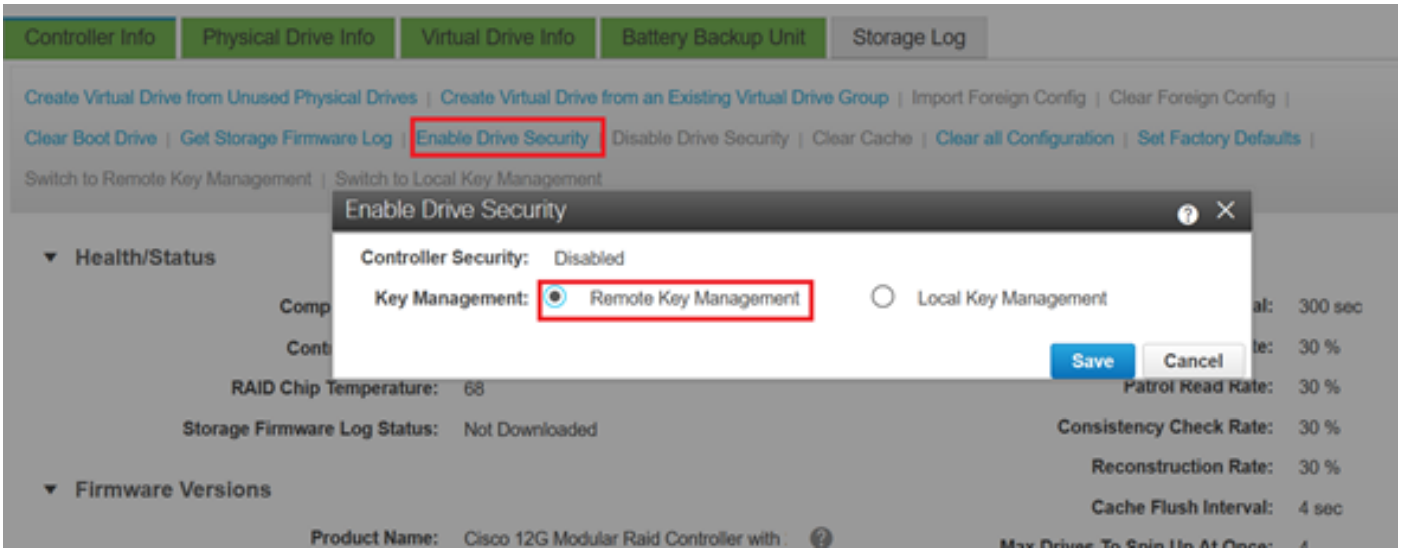


7. Assim que a conexão com o KMIP for bem-sucedida, você poderá ativar o gerenciamento remoto de chaves.

Navegue até **Networking > Modular Raid Controller > Controller Info**.

Selecione **Enable Drive Security** e, em seguida, **Remote Key Management**.

> **Note**: Se anteriormente o **Gerenciamento de chave local** estava habilitado, você será solicitado a fornecer a chave atual para alterar o gerenciamento remoto



Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Na CLI, você pode verificar a configuração.

1. Verifique se o KMIP está habilitado.

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

2. Verifique o endereço IP, a porta e o tempo limite.

```
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. Verifique se os certificados estão disponíveis.

```
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. Verifique os detalhes de login.

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

5. Teste a conexão.

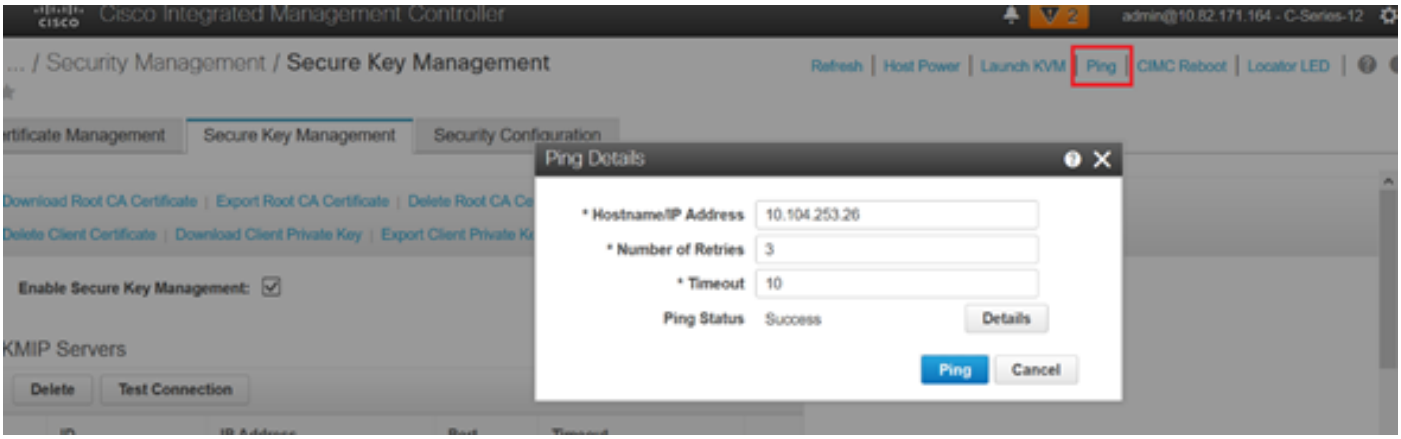
```
C-Series-12 /kmip # C-Series-12 /kmip # scope kmip-server 1 C-Series-12 /kmip/kmip-server #
```

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

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Se o teste de conexão com o servidor KMIP não for bem-sucedido, certifique-se de que você pode fazer ping no servidor.

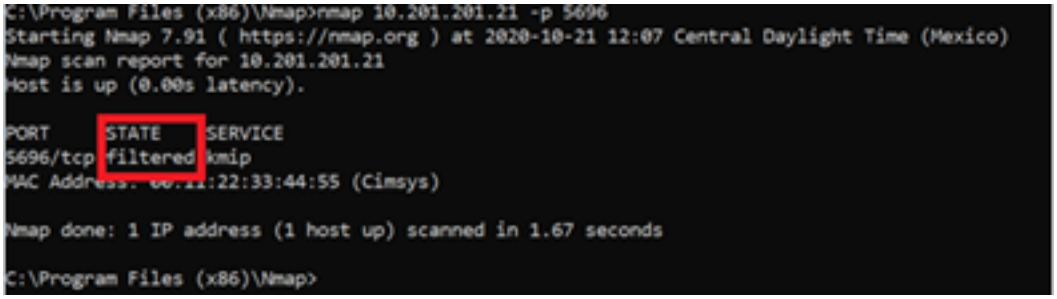


Verifique se a porta 5696 está aberta no CIMC e no servidor KMIP. Você pode instalar uma versão NMAP em seu PC, pois esse comando não está disponível no CIMC.

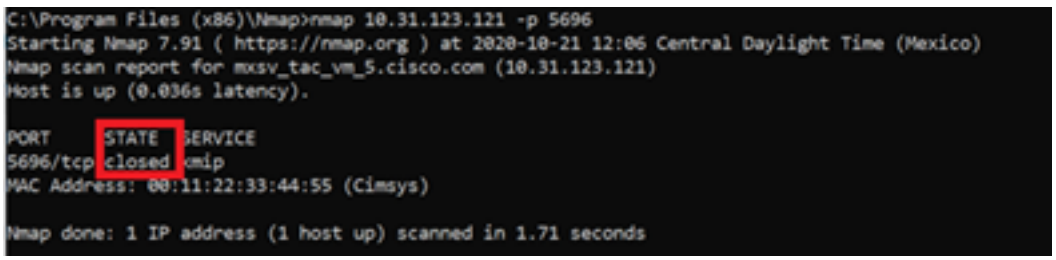
Você pode instalar o NMAP na sua máquina local, para testar se a porta está aberta; no diretório em que o arquivo foi instalado, use este comando:

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

A saída mostra uma porta aberta para o serviço KMIP:



A saída mostra uma porta fechada para o serviço KMIP:



Informações Relacionadas

- Guia de configuração da série C - Unidades com autocriptografia
- Guia de configuração da série C - Key Management Interoperability Protocol
- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.