Configuración de la administración remota de claves en servidores en rack independientes

Contenido

Introducción

Este documento describe la configuración del Protocolo de interoperabilidad de administración de claves (KMIP) en servidores en rack independientes.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Integrated Management Controller (CIMC)
- Unidad de autocifrado (SED)
- KMIP

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- UCSC-C220-M4S, versión de CIMC: 4.1(1 nonies)
- Unidades SED
- SSD SAS SED de rendimiento empresarial de 800 GB (10 FWPD) - MTFDJAK800 MB
- ID de pieza de unidad: UCS-SD800GBEK9
- Proveedor: MICRON
- Modelo: S650DC-800FIPS

- Vormetric como gestor de claves de terceros

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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

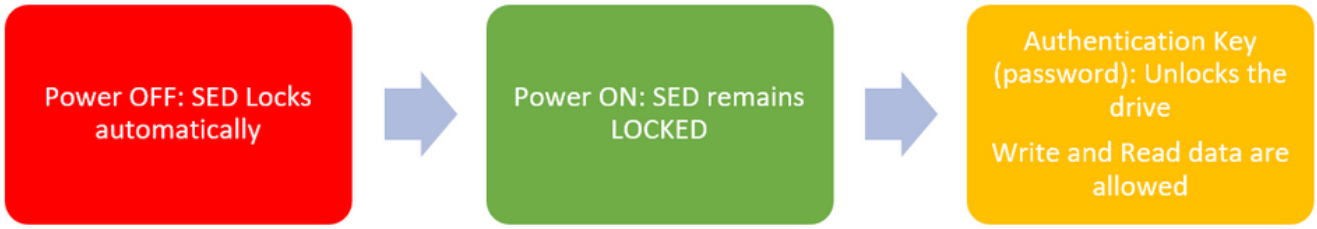
El KMIP es un protocolo de comunicación extensible que define formatos de mensajes para la manipulación de claves criptográficas en un servidor de administración de claves. Esto facilita el cifrado de datos porque simplifica la administración de claves de cifrado.

Unidades SED

Un SED es una unidad de disco duro (HDD) o una unidad de estado sólido (SSD) con un circuito de cifrado integrado en la unidad. Cifra de forma transparente todos los datos escritos en los medios y, cuando se desbloquea, descifra de forma transparente todos los datos leídos desde los medios.

En un SED, las claves de cifrado en sí mismas nunca salen de los confines del hardware SED y, por lo tanto, están a salvo de ataques en el nivel del SO.

Flujo de trabajo de unidades SED:



1. Flujo de unidad SED

La contraseña para desbloquear la unidad se puede obtener localmente con la configuración **Local Key Management** donde la responsabilidad del usuario es recordar la información clave. También se puede obtener con Administración remota de claves, donde la clave de seguridad se crea y obtiene de un servidor KMIP y la responsabilidad del usuario es configurar el servidor KMIP en CIMC.

Configurar

Crear una clave privada de cliente y un certificado de cliente

Estos comandos deben ingresarse en una máquina Linux con el paquete OpenSSL, no en Cisco IMC. Asegúrese de que el nombre común sea el mismo en el certificado de CA raíz y en el certificado de cliente.

> **Nota:** Asegúrese de que la hora de Cisco IMC esté configurada en la hora actual.

1. Cree una clave RSA de 2048 bits.

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

2. Cree un certificado autofirmado con la clave ya creada.

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

3. Consulte la documentación del proveedor de KMIP para obtener detalles sobre la obtención del certificado de CA raíz.

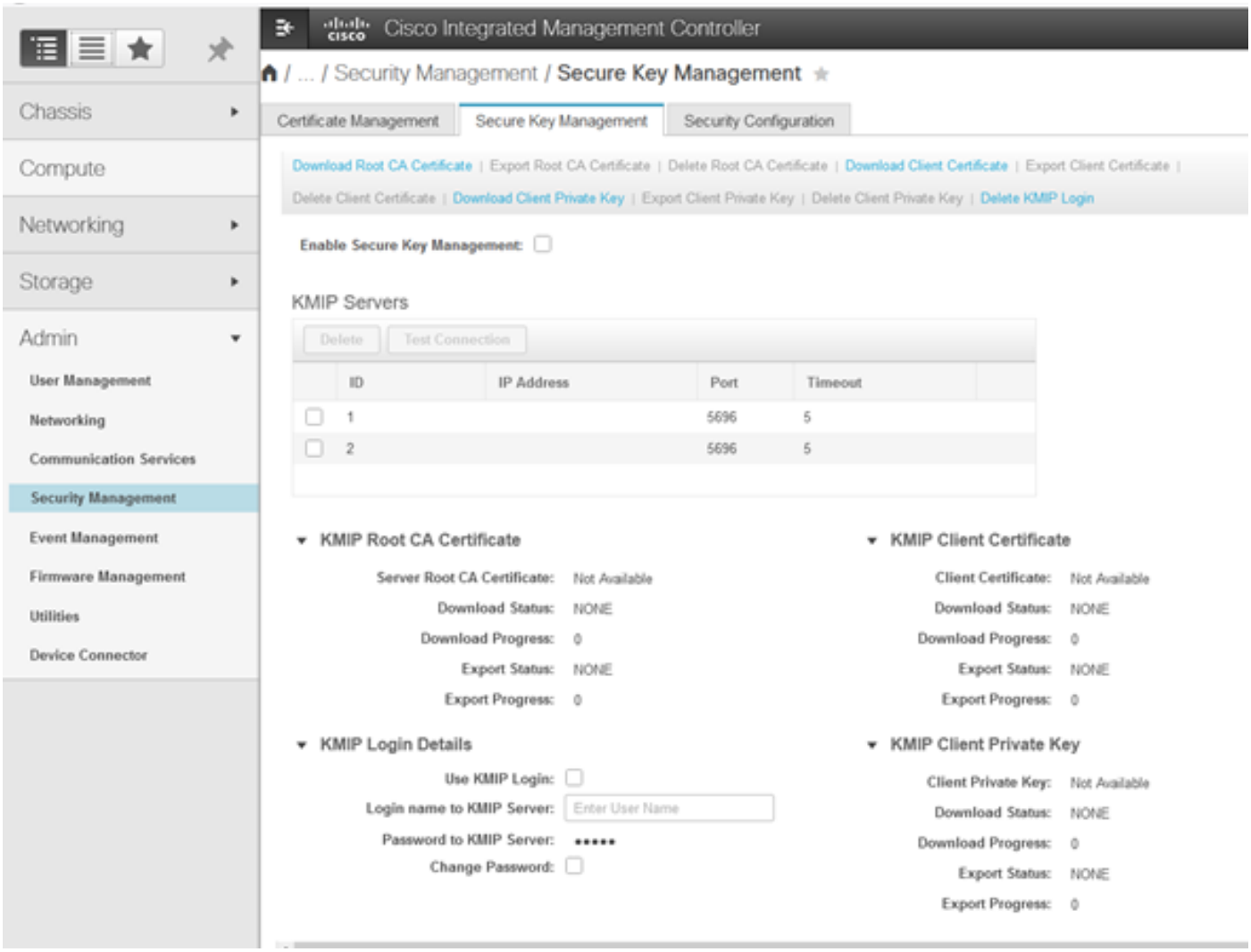
> **Nota:** Vormetric requiere que el nombre común en el certificado RootCa coincida con el nombre de host del host Vormetric.

> **Nota:** Debe tener una cuenta para tener acceso a las guías de configuración de los proveedores de KMIP:
> SafeNet
> Vormétrico

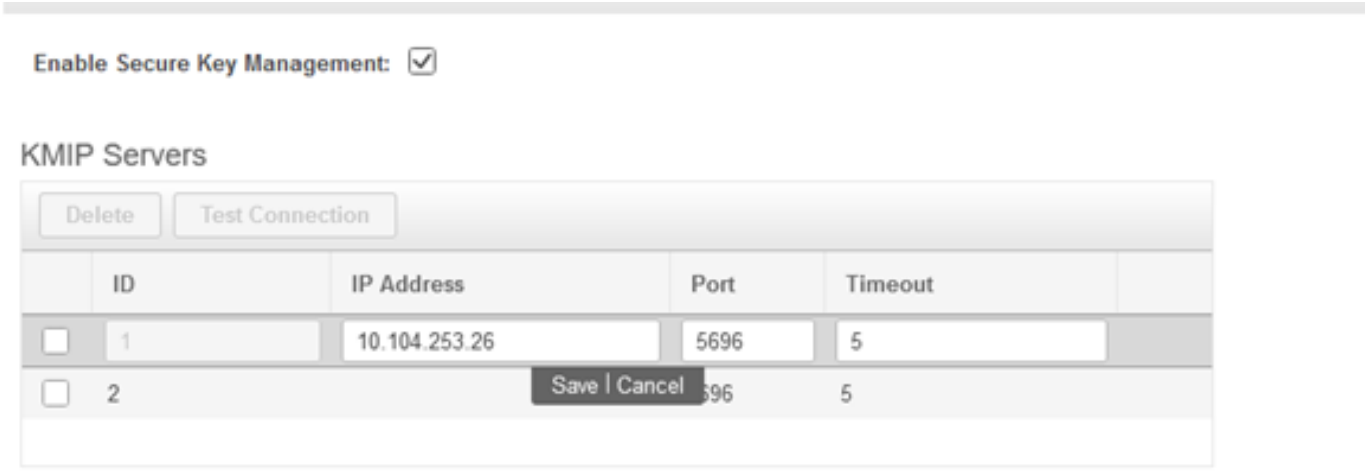
Configuración del servidor KMIP en CIMC

1. Vaya a **Admin > Security Management > Secure Key Management.**

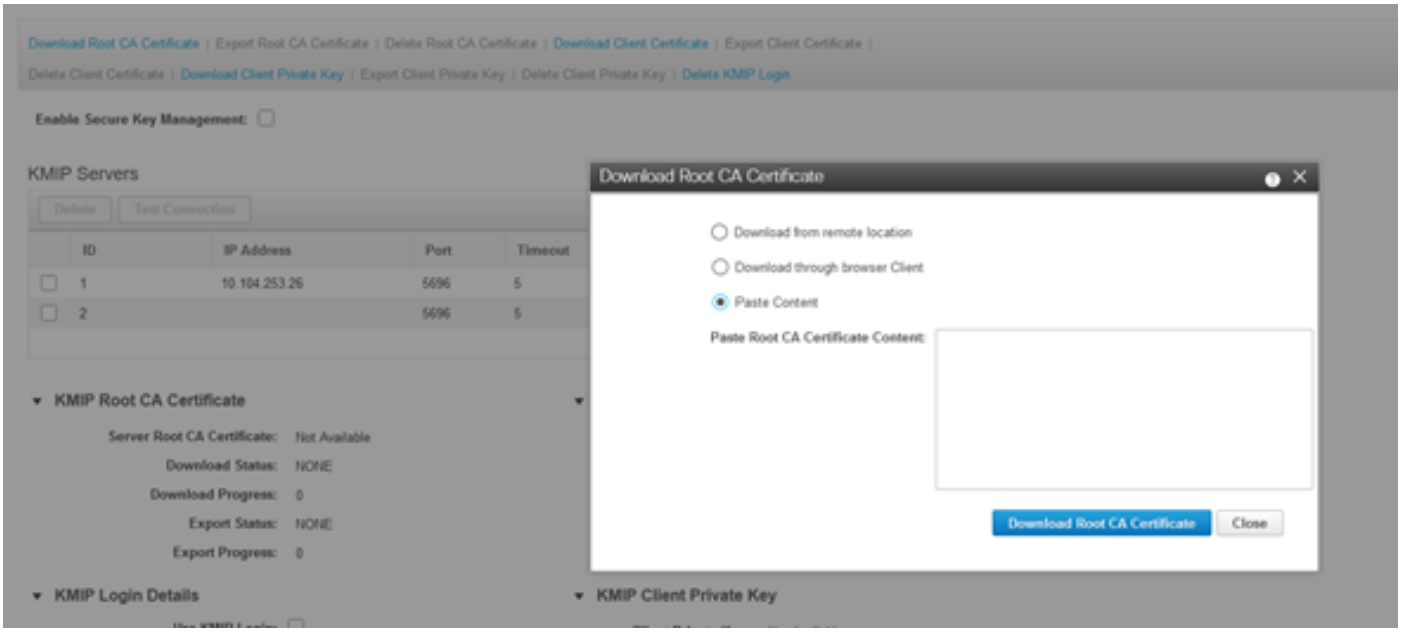
Una configuración clara muestra **Export/Delete** buttons grayed out, only **Download** buttons are active.



2. Haga clic en la dirección IP y establezca la dirección IP para el servidor KMIP, asegúrese de que puede alcanzarla y, en caso de que se utilice el puerto predeterminado, no necesita cambiar nada más, guarde los cambios.



3. Descargue los certificados y la clave privada en el servidor. Puede descargar el **.pem** file or just paste the content.

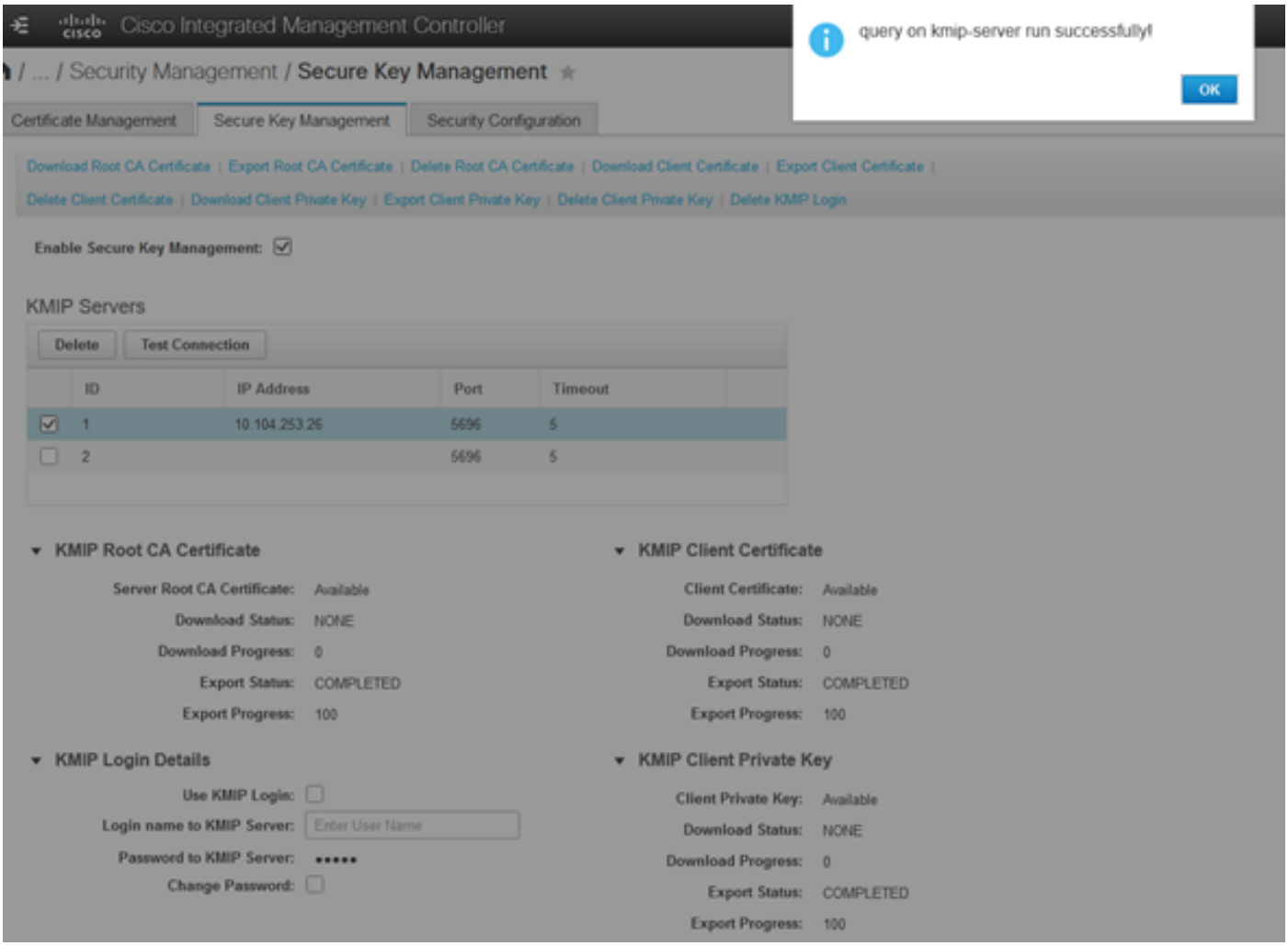


4. Al cargar los certificados, verá que los certificados se muestran como **Disponible**, para los certificados que faltan y que no se cargan, verá **No Disponible**.

Sólo puede probar la conexión cuando todos los certificados y claves privadas se hayan descargado correctamente al CIMC.

5. (opcional) Una vez que tenga todos los certificados, puede agregar opcionalmente el usuario y la contraseña para el servidor KMIP, esta configuración sólo es compatible con SafeNet como servidor KMIP de terceros.

6. Pruebe la conexión y si los certificados son correctos y puede alcanzar el servidor KMIP a través del puerto configurado, verá una conexión exitosa.

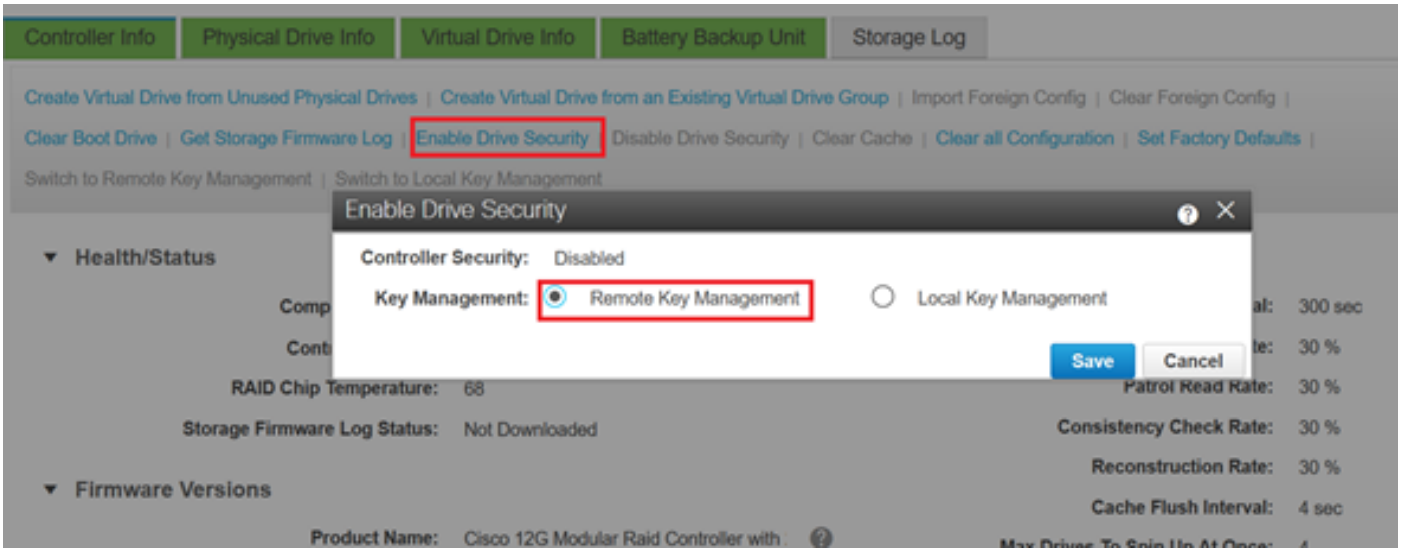


7. Una vez que nuestra conexión con KMIP es exitosa, puede habilitar la administración remota de claves.

Vaya a **Networking > Modular Raid Controller > Controller Info**.

Seleccione **Enable Drive Security** y luego **Remote Key Management**.

> **Nota:** Si anteriormente se habilitó **Local Key Management**, se le solicitará la clave actual para cambiar para administración remota



Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

Desde la CLI puede verificar la configuración.

1. Verifique si KMIP está habilitado.

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

2. Verifique la dirección IP, el puerto y el tiempo de espera.

```
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. Compruebe si los certificados están disponibles.

```
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 los detalles de inicio de sesión.

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

5. Compruebe la conexión.

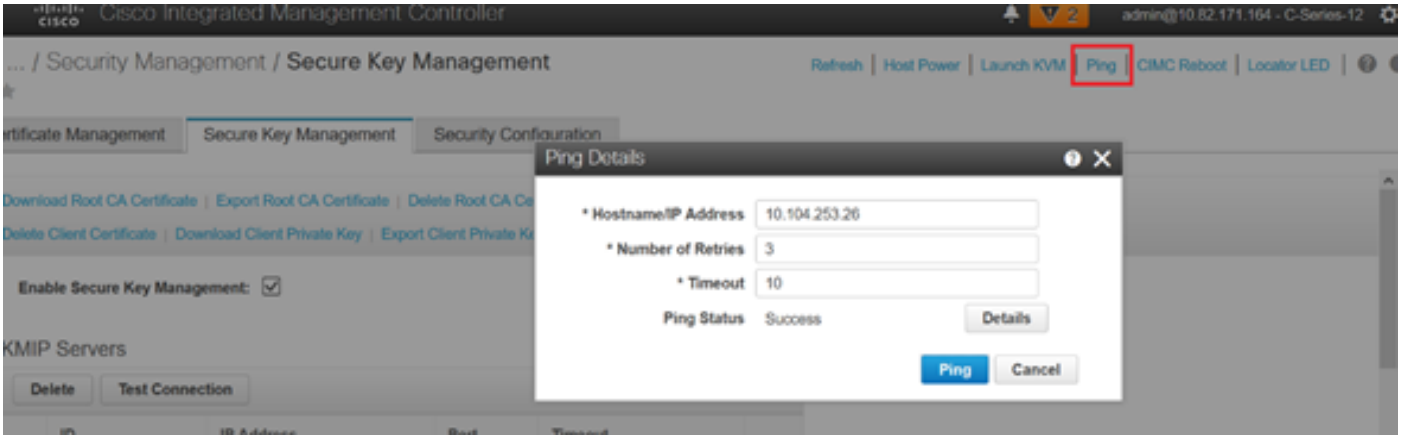
```
C-Series-12 /kmip # C-Series-12 /kmip # scope kmip-server 1 C-Series-12 /kmip/kmip-server #
```

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

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Si la conexión de prueba con el servidor KMIP no se realiza correctamente, asegúrese de que puede hacer ping al servidor.

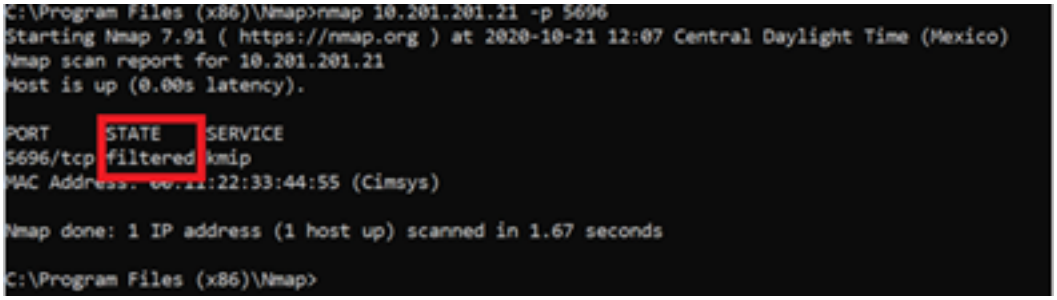


Asegúrese de que el puerto 5696 esté abierto en el CIMC y el servidor KMIP. Puede instalar una versión de NMAP en su PC, ya que este comando no está disponible en CIMC.

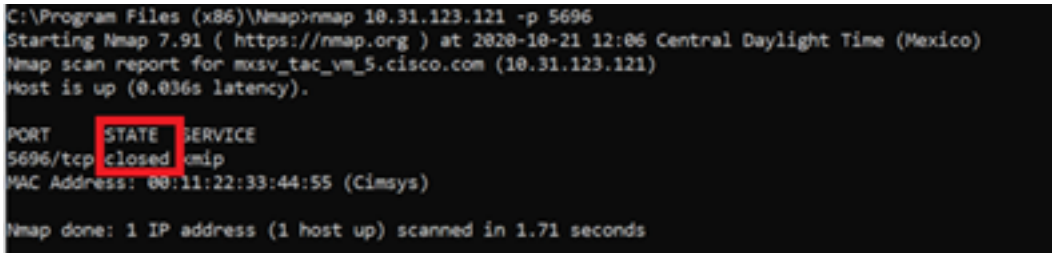
Puede instalar NMAP en su equipo local, para probar si el puerto está abierto; en el directorio donde se instaló el archivo, utilice este comando:

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

El resultado muestra un puerto abierto para el servicio KMIP:



El resultado muestra un puerto cerrado para el servicio KMIP:



Información Relacionada

- Guía de configuración de la serie C: unidades de autocifrado

- Guía de configuración de la serie C: Key Management Interoperability Protocol
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).