Configurazione della gestione remota delle chiavi sui server rack standalone

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Premesse](#)
[Unità SED](#)
[Configurazione](#)
[Creare una chiave privata e un certificato client](#)
[Configurazione del server KMIP su CIMC](#)
[Verifica](#)
[Risoluzione dei problemi](#)
[Informazioni correlate](#)

Introduzione

Questo documento descrive la configurazione del protocollo KMIP (Key Management Interoperability Protocol) sui server rack standalone.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Integrated Management Controller (CIMC)
- Unità SED (Self-Encrypting Drive)
- KMIP

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- UCS-C220-M4S, versione CIMC: 4.1(1h)
- Unità SED
- Unità a stato solido SAS SED da 800 GB a elevate prestazioni (10 FWPD) - MTFDJAK800 MBS
- ID parte unità: UCS-SD800GBEK9
- Fornitore: MICRON

- Modello: S650DC-800FIPS
- Vormetrico come key manager di terze parti

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

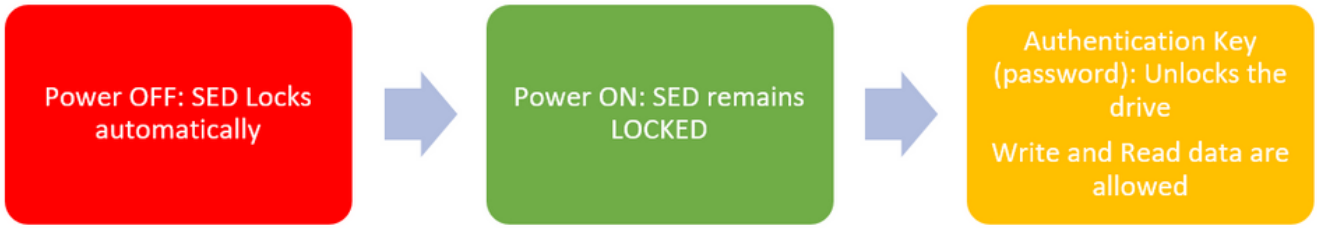
Il KMIP è un protocollo di comunicazione estensibile che definisce i formati dei messaggi per la modifica delle chiavi di crittografia in un server di gestione delle chiavi. Ciò semplifica la crittografia dei dati perché semplifica la gestione delle chiavi di crittografia.

Unità SED

Un SED è un'unità disco rigido (HDD) o a stato solido (SSD) con un circuito di crittografia integrato nell'unità. Crittografa in modo trasparente tutti i dati scritti sul supporto e, quando sbloccato, decrittografa in modo trasparente tutti i dati letti dal supporto.

In un SED, le chiavi di crittografia non superano mai i confini dell'hardware SED e sono quindi al sicuro da attacchi a livello di sistema operativo.

Flusso di lavoro unità SED:



1. Flusso dell'unità SED

La password per sbloccare l'unità può essere ottenuta localmente con la configurazione di **Local Key Management** in cui l'utente è responsabile di ricordare le informazioni chiave. Può essere ottenuto anche con Gestione remota chiavi, in cui la chiave di protezione viene creata e recuperata da un server KMIP e l'utente ha la responsabilità di configurare il server KMIP in CIMC.

Configurazione

Creare una chiave privata e un certificato client

Questi comandi devono essere immessi su un computer Linux con il pacchetto OpenSSL, non su Cisco IMC. Verificare che il nome comune sia lo stesso nel certificato CA radice e nel certificato client.

> **Nota:** Verificare che l'ora Cisco IMC sia impostata sull'ora corrente.

1. Creare una chiave RSA a 2048 bit.

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

2. Creare un certificato autofirmato con la chiave già creata.

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

3. Per ulteriori informazioni sul recupero del certificato CA radice, consultare la documentazione del fornitore del KMIP.

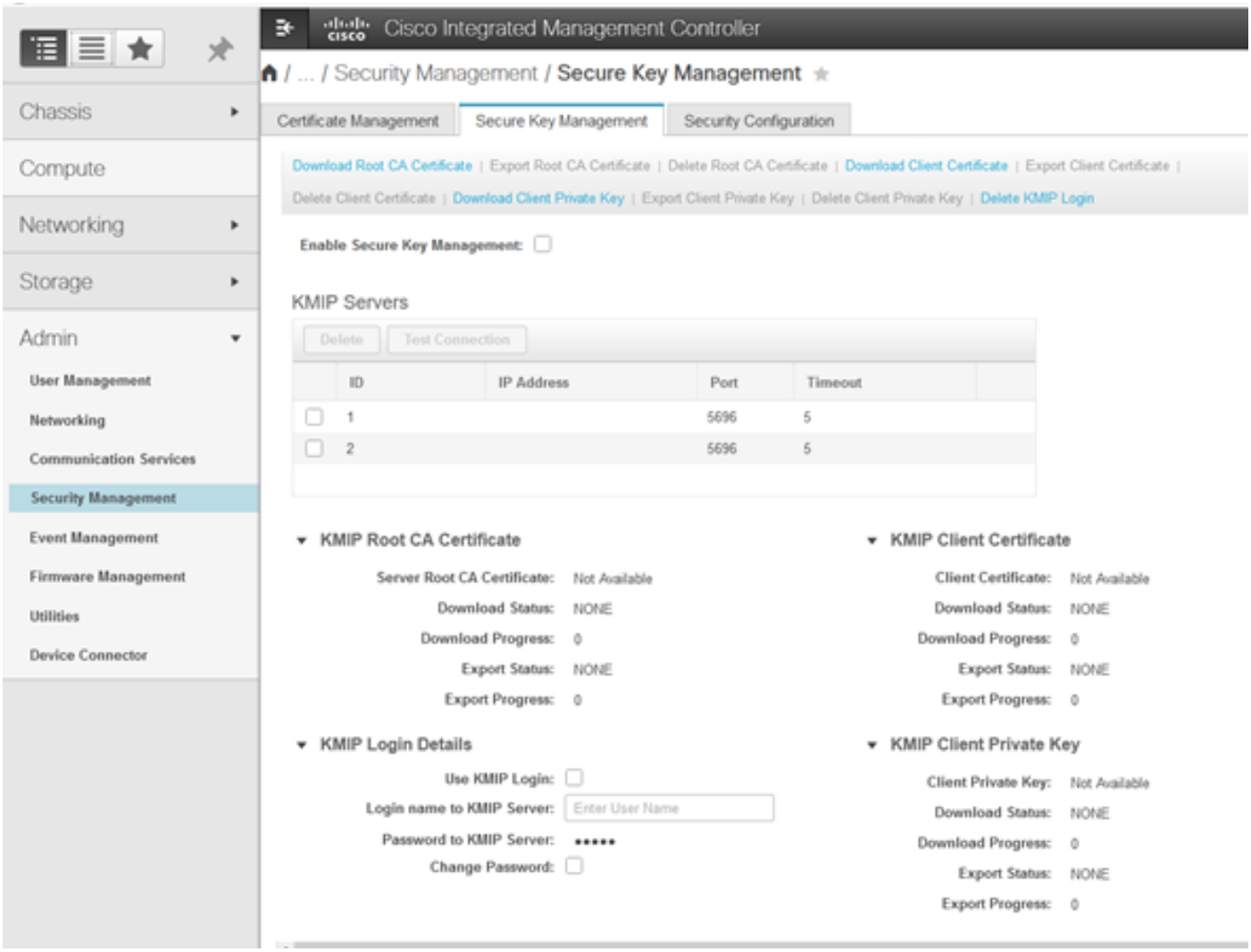
> **Nota:** Vormetric richiede che il nome comune nel certificato RootCa corrisponda al nome host dell'host Vormetric.

> **Nota:** Per accedere alle guide alla configurazione per i fornitori KMIP, è necessario disporre di un account:
> SafeNet
> Vormetrico

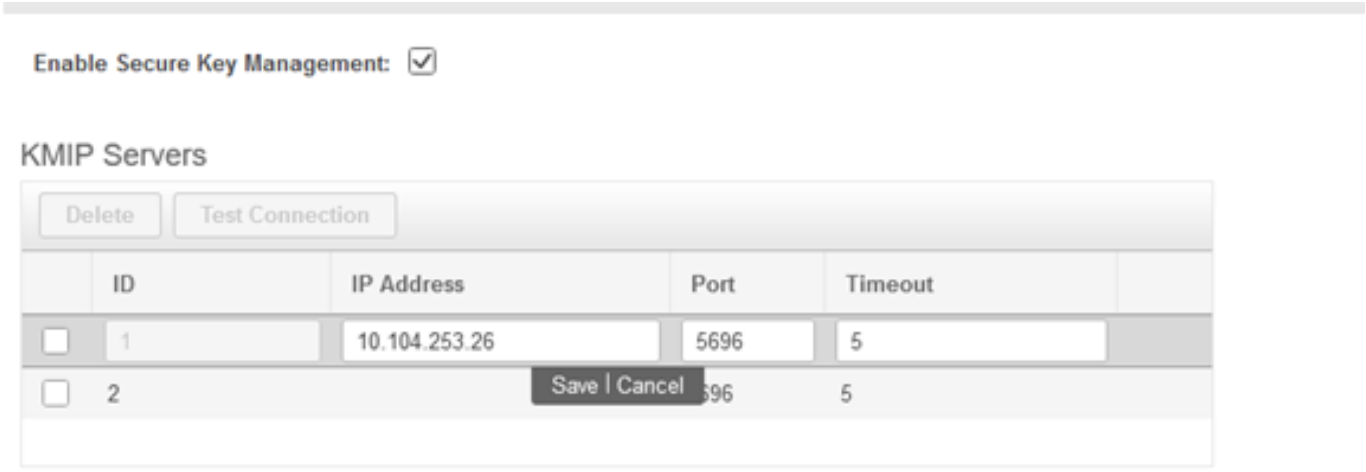
Configurazione del server KMIP su CIMC

1. Passare a **Amministrazione > Gestione sicurezza > Gestione chiavi protette.**

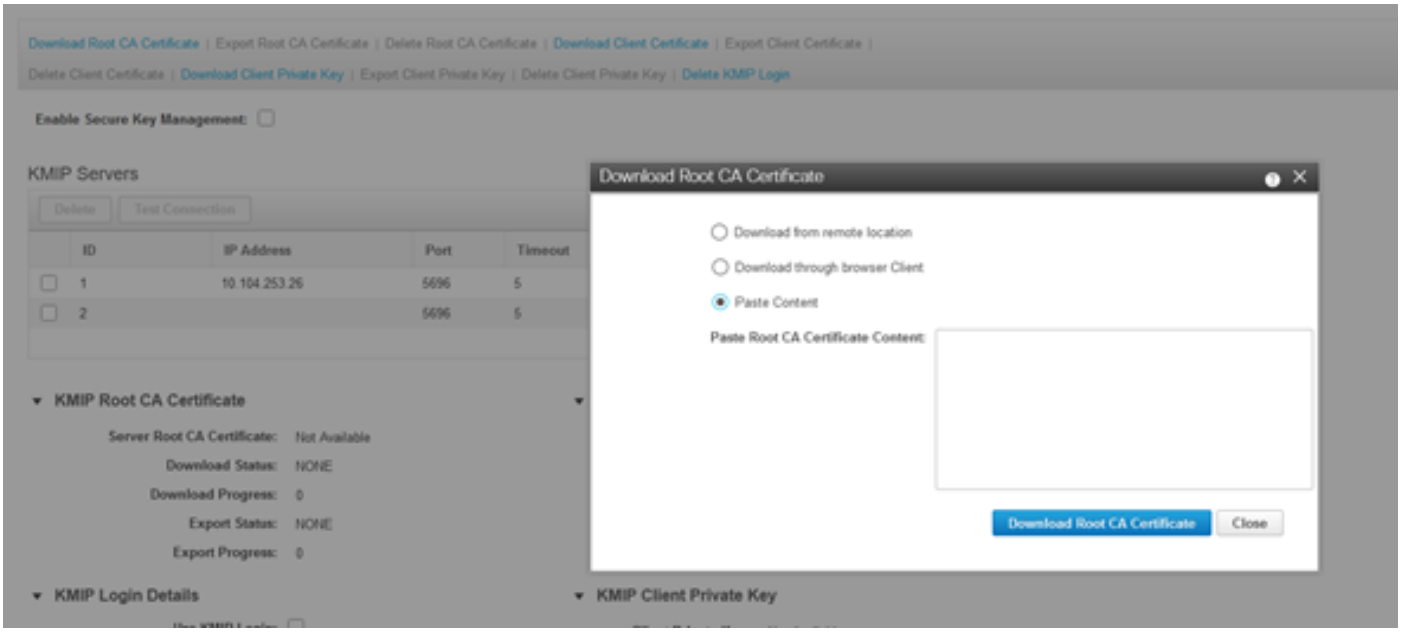
Una configurazione chiara mostra **Export/Delete** buttons grayed out, only **Download** buttons are active.



2. Fare clic sull'indirizzo IP e impostare l'indirizzo IP per il server KMIP, accertarsi di essere in grado di raggiungerlo e, nel caso in cui venga utilizzata la porta predefinita, non è necessario apportare altre modifiche, quindi salvare le modifiche.



3. Scaricare i certificati e la chiave privata nel server. È possibile scaricare **.pem** file or just paste the content.

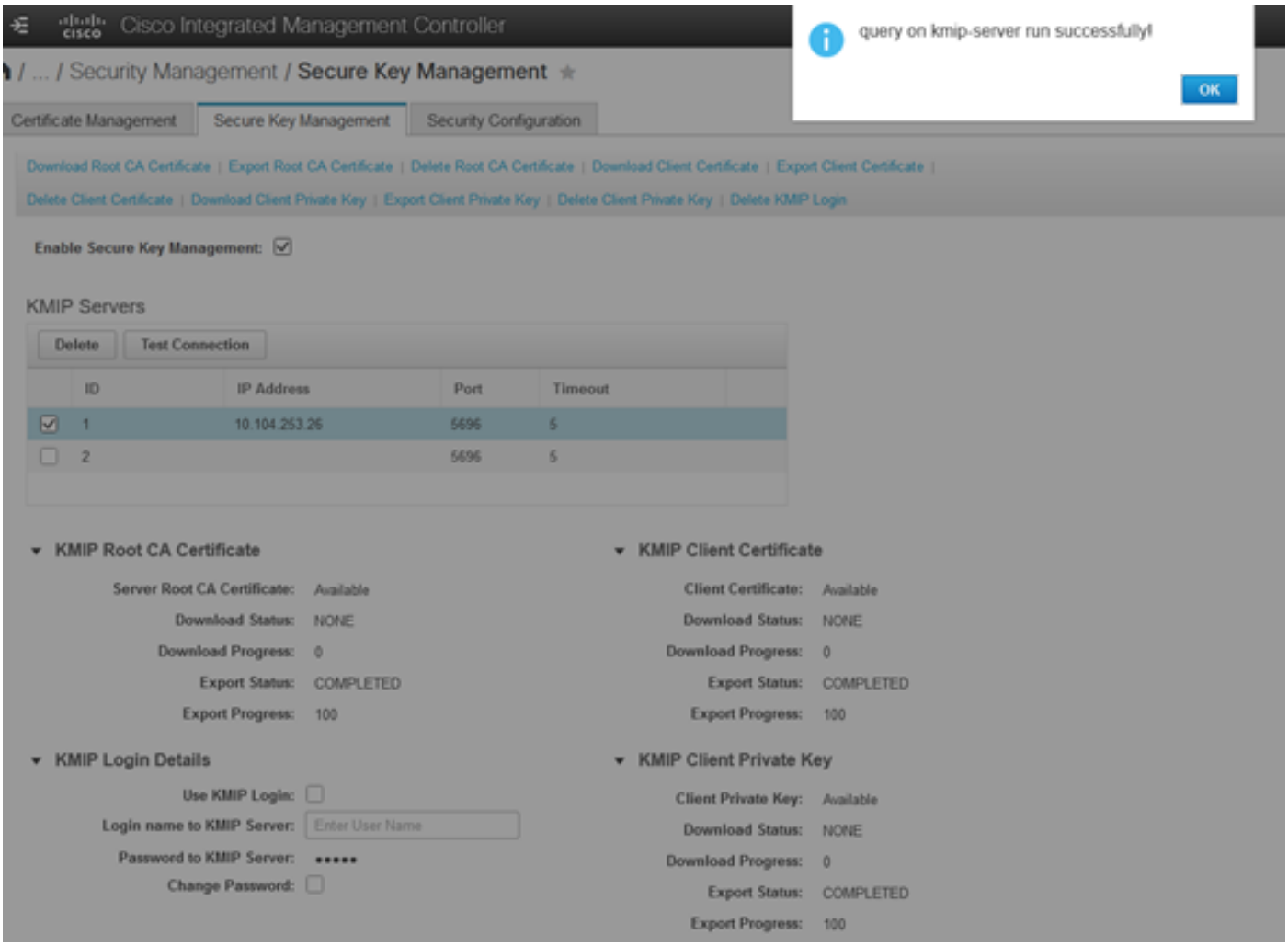


4. Quando si caricano i certificati, viene visualizzato il messaggio **Disponibile** per i certificati mancanti che non sono stati caricati, viene visualizzato **Non disponibile**.

Èpossibile eseguire il test della connessione solo dopo che tutti i certificati e le chiavi private sono stati scaricati correttamente in CIMC.

5. (facoltativo) Dopo aver ottenuto tutti i certificati, è possibile aggiungere l'utente e la password per il server KMIP. Questa configurazione è supportata solo per SafeNet come server KMIP di terze parti.

6. Verificare la connessione. Se i certificati sono corretti e si è in grado di raggiungere il server KMIP tramite la porta configurata, la connessione verrà stabilita correttamente.

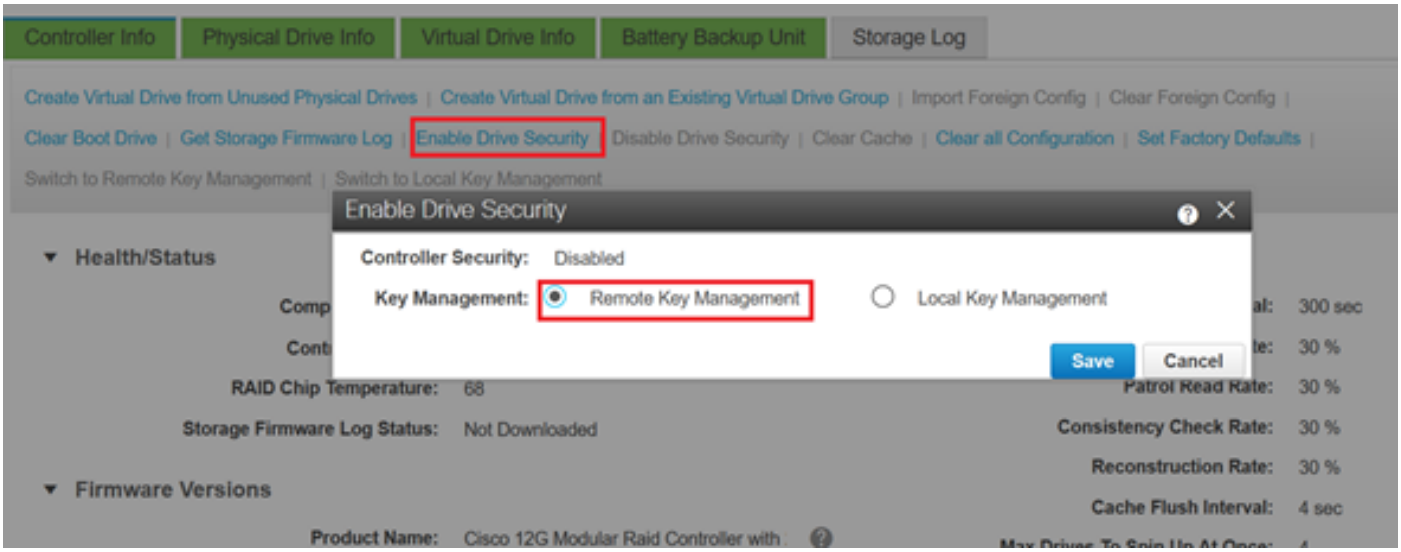


7. Una volta stabilita la connessione con KMIP, sarà possibile abilitare la gestione remota delle chiavi.

Selezionare **Rete > Controller RAID modulare > Informazioni controller**.

Selezionare **Abilita sicurezza unità**, quindi **Gestione chiavi remote**.

> **Nota:** Se in precedenza è stata attivata la **gestione delle chiavi locali**, verrà richiesto di specificare la chiave corrente per modificare la gestione remota



Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Dalla CLI è possibile verificare la configurazione.

1. Verificare se KMIP è abilitato.

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

2. Verificare indirizzo IP, porta e timeout.

```
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. Verificare se i certificati sono disponibili.

```
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. Verificare i dettagli di accesso.

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

5. Verificare la connessione.

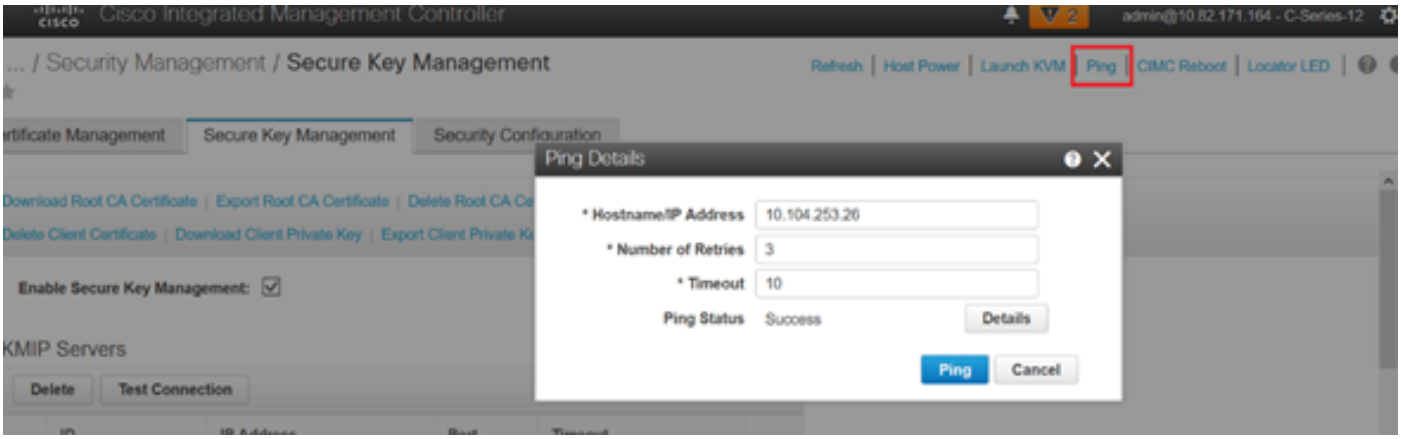
```
C-Series-12 /kmip # C-Series-12 /kmip # scope kmip-server 1 C-Series-12 /kmip/kmip-server #
```

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

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Se la connessione di prova con il server KMIP ha esito negativo, verificare che sia possibile eseguire il ping del server.

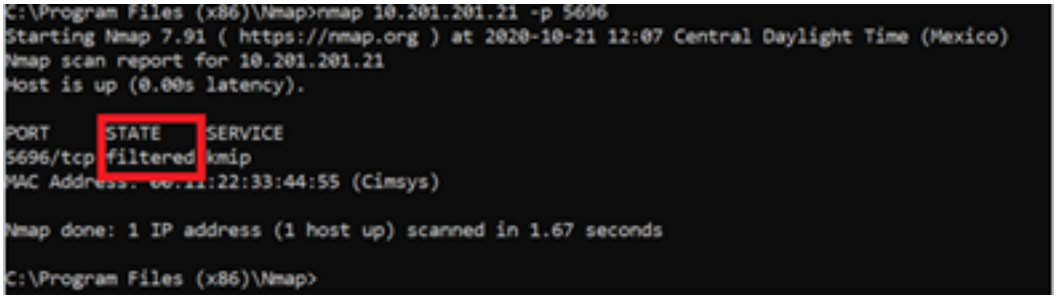


Verificare che la porta 5696 sia aperta sul CIMC e sul server KMIP. È possibile installare una versione NMAP sul PC, poiché questo comando non è disponibile su CIMC.

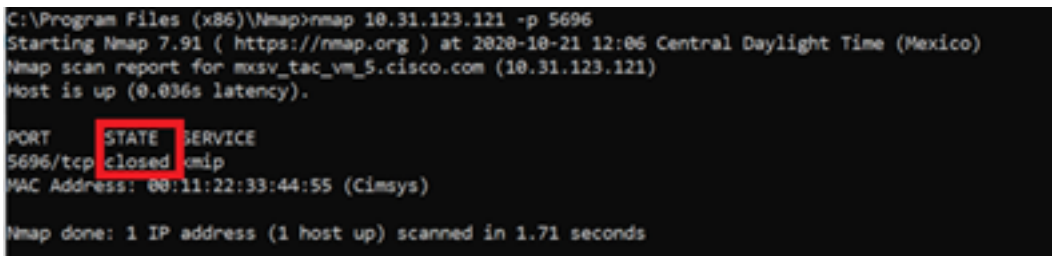
Èpossibile installare NMAP sul computer locale per verificare se la porta è aperta. nella directory in cui è stato installato il file, utilizzare questo comando:

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

Nell'output viene visualizzata una porta aperta per il servizio KMIP:



L'output mostra una porta chiusa per il servizio KMIP:



Informazioni correlate

- Guida alla configurazione della serie C - Unità con crittografia automatica
- Guida alla configurazione della serie C - Protocollo di interoperabilità della gestione delle chiavi
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).