Configurer la gestion des clés à distance sur des serveurs rack autonomes

Contenu

Introduction

Ce document décrit la configuration du protocole KMIP (Key Management Interoperability Protocol) sur des serveurs rack autonomes.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Contrôleur de gestion intégré Cisco (CIMC)
- Lecteur à chiffrement automatique (SED)
- KMIP

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- UCSC-C220-M4S, CIMC Version : 4.1(1h)
- Lecteurs SED
- SSD SAS SED hautes performances 800 Go (10 FWPD) - MTFDJAK800 MBS
- ID de pièce de lecteur : UCS-SD800GBEK9
- Fournisseur : MICRON
- Modèle : S650DC-800FIPS

- Vormetric comme gestionnaire de clés tiers

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 votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

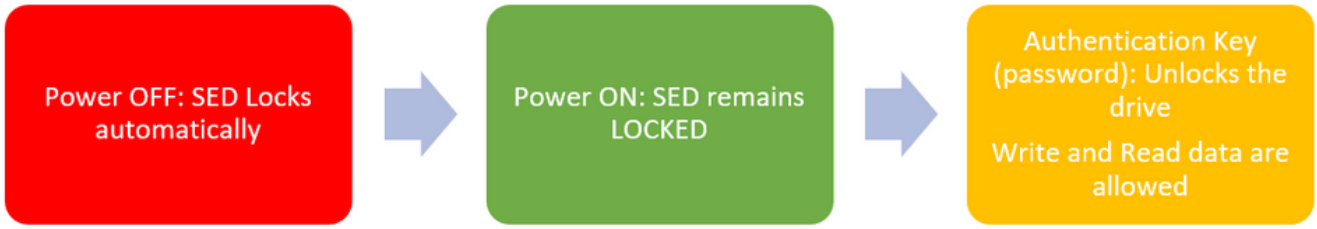
Le protocole KMIP est un protocole de communication extensible qui définit des formats de message pour la manipulation de clés cryptographiques sur un serveur de gestion de clés. Cela facilite le chiffrement des données car simplifie la gestion des clés de chiffrement.

Lecteurs SED

Un SED est un disque dur (HDD) ou un disque SSD (Solid State Drive) avec un circuit de cryptage intégré dans le lecteur. Il chiffre de manière transparente toutes les données écrites sur le support et, lorsqu'il est déverrouillé, déchiffre de manière transparente toutes les données lues sur le support.

Dans un SED, les clés de cryptage elles-mêmes ne quittent jamais les limites du matériel SED et sont donc à l'abri des attaques au niveau du système d'exploitation.

Workflow des lecteurs SED :



1. Flux d'entraînement SED

Le mot de passe pour déverrouiller le lecteur peut être obtenu localement avec la configuration de **gestion de clé locale** où la responsabilité de l'utilisateur est de mémoriser les informations de clé. Il peut également être obtenu avec Remote Key Management où la clé de sécurité est créée et récupérée à partir d'un serveur KMIP et où la responsabilité de l'utilisateur est de configurer le serveur KMIP dans CIMC.

Configuration

Créer une clé privée client et un certificat client

Ces commandes doivent être entrées sur une machine Linux avec le package OpenSSL, et non dans l'IMC Cisco. Assurez-vous que le nom commun est identique dans le certificat de l'autorité de certification racine et dans le certificat du client.

> **Note**: Assurez-vous que l'heure Cisco IMC est définie sur l'heure actuelle.

1. Créez une clé RSA de 2 048 bits.

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

2. Créez un certificat auto-signé avec la clé déjà créée.

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

3. Reportez-vous à la documentation du fournisseur KMIP pour obtenir des détails sur l'obtention du certificat d'autorité de certification racine.

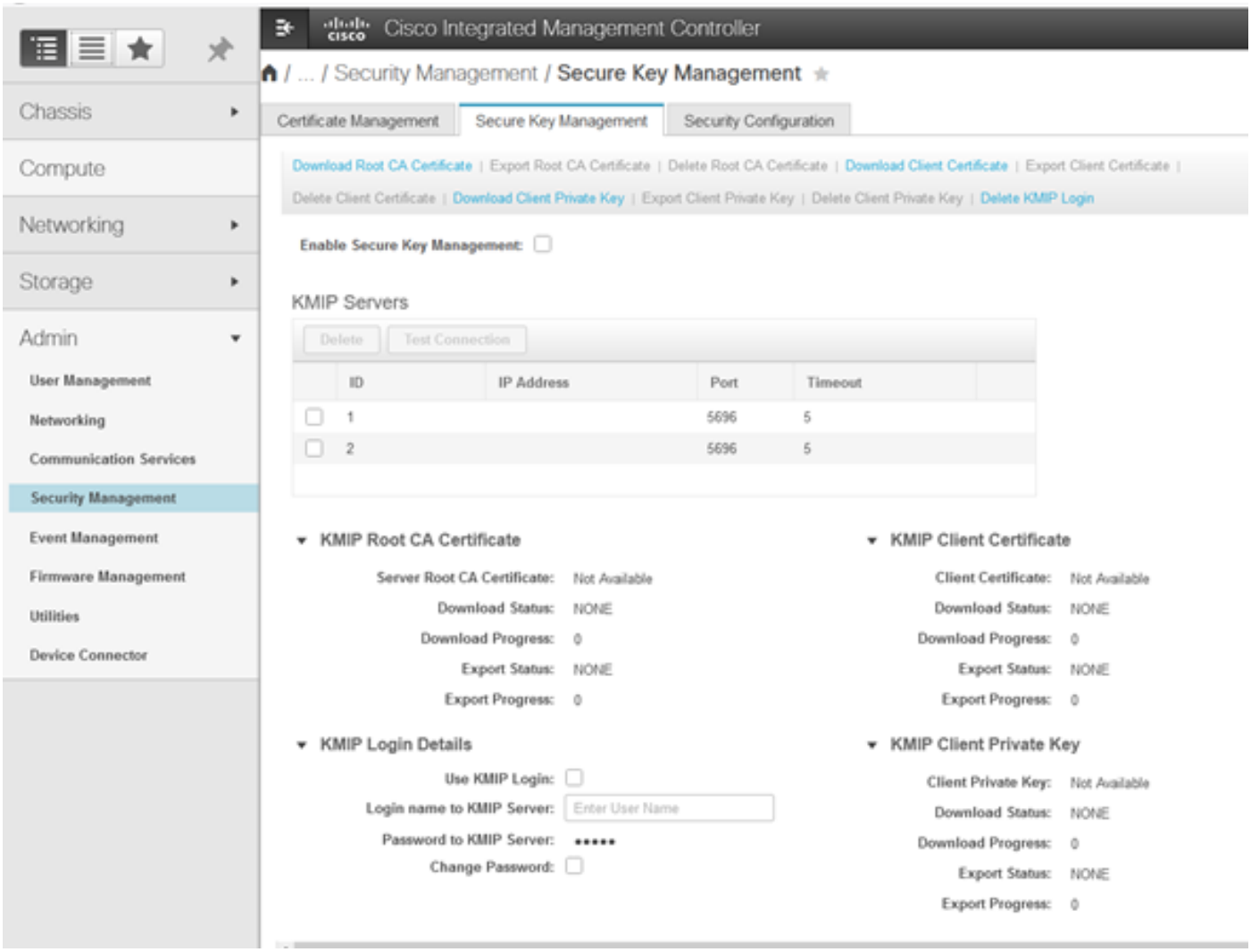
> **Note**: Le Vormetric nécessite que le nom commun dans le certificat RootCa corresponde au nom d'hôte de l'hôte Vormetric.

> **Note**: Vous devez disposer d'un compte pour accéder aux guides de configuration des fournisseurs KMIP :
> SafeNet
> Vormétrique

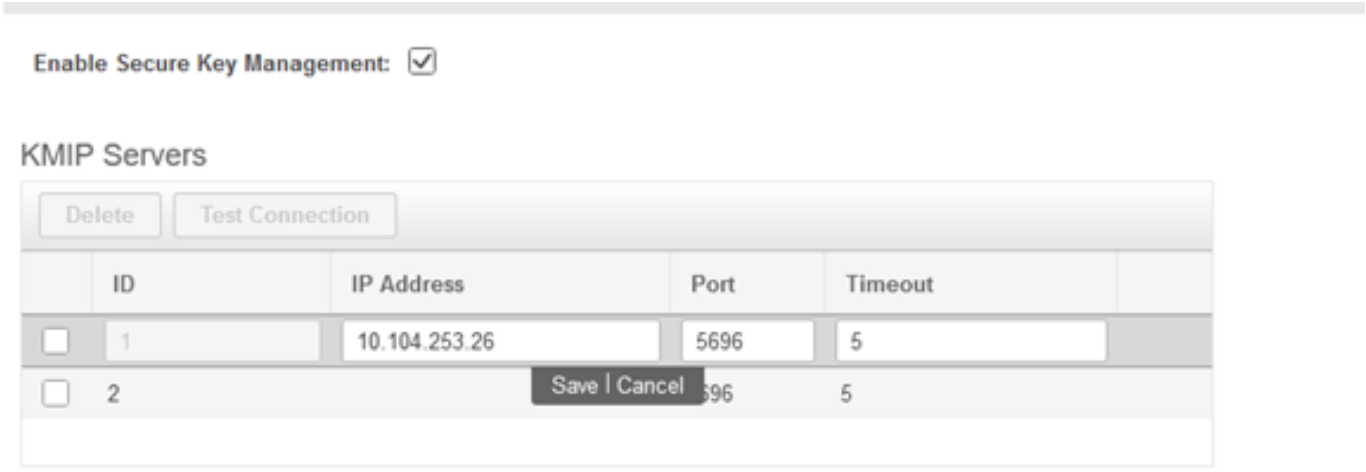
Configurer le serveur KMIP sur CIMC

1. Accédez à **Admin > Security Management > Secure Key Management.**

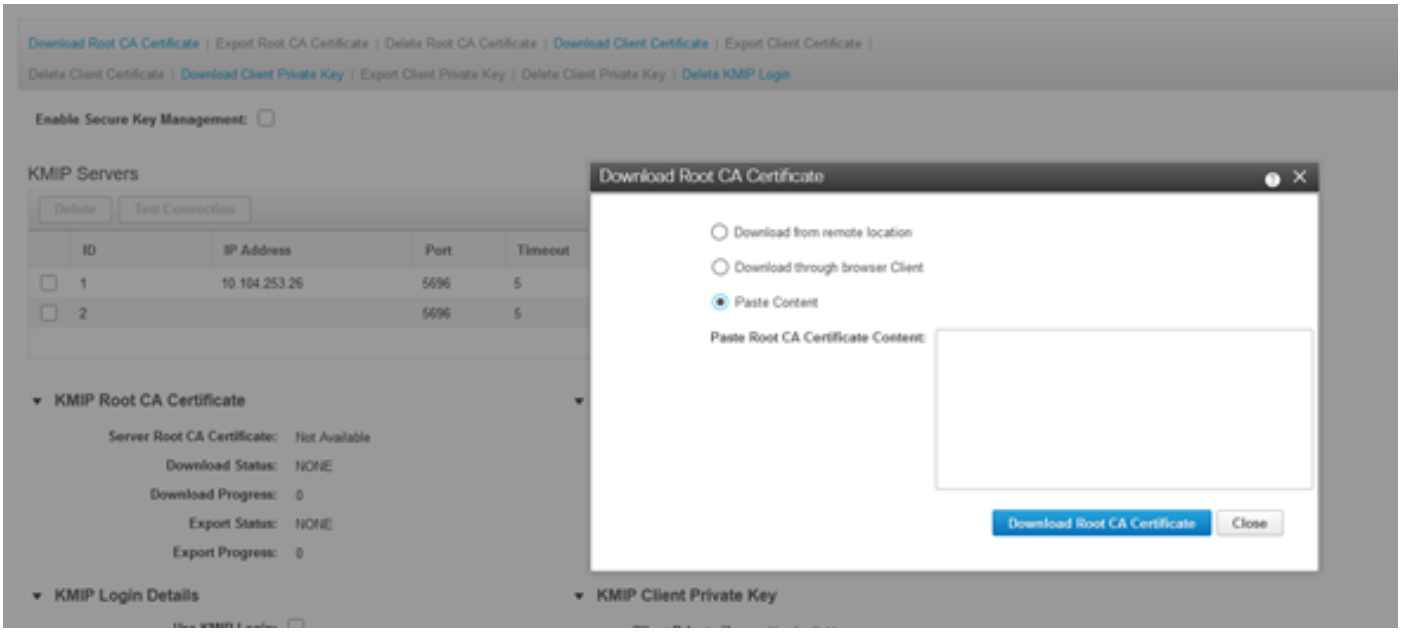
Une configuration claire indique **Export/Delete** buttons grayed out, only **Download** buttons are active.



2. Cliquez sur l'adresse IP et définissez l'adresse IP pour le serveur KMIP, assurez-vous que vous êtes en mesure de l'atteindre et dans le cas où le port par défaut est utilisé rien d'autre ne doit être modifié, puis enregistrez les modifications.



3. Téléchargez les certificats et la clé privée sur le serveur. Vous pouvez télécharger le **.pem** file or just paste the content.

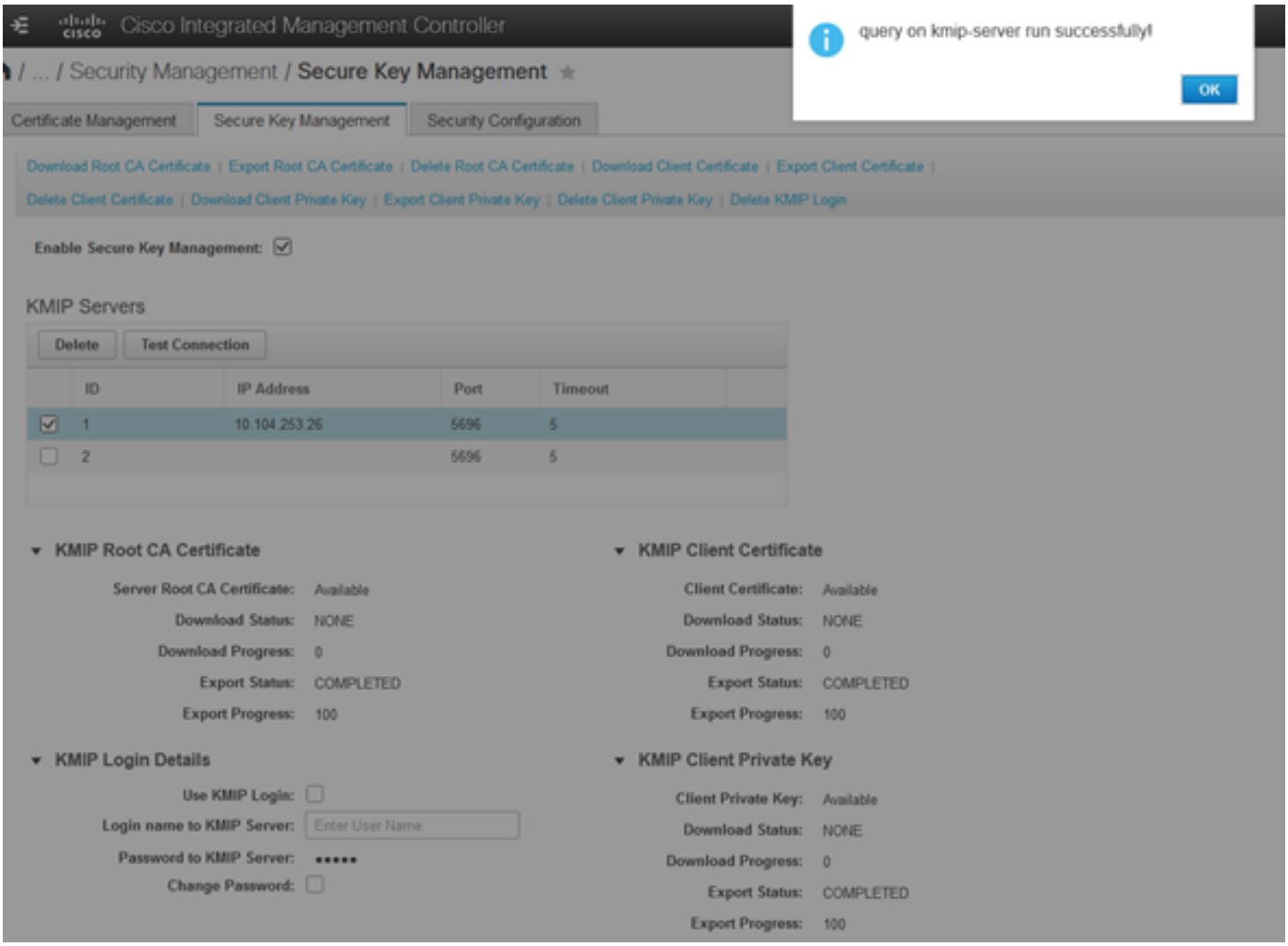


4. Lorsque vous téléchargez les certificats, vous voyez que les certificats s'affichent comme **Disponibles**, pour les certificats manquants qui ne sont pas téléchargés, vous voyez **Non disponible**.

Vous ne pouvez tester la connexion que lorsque tous les certificats et toutes les clés privées ont été téléchargés sur le CIMC.

5. (Facultatif) Une fois que vous disposez de tous les certificats, vous pouvez éventuellement ajouter l'utilisateur et le mot de passe du serveur KMIP. Cette configuration n'est prise en charge que pour SafeNet en tant que serveur KMIP tiers.

6. Testez la connexion et si les certificats sont corrects et que vous pouvez atteindre le serveur KMIP via le port configuré, vous voyez une connexion réussie.

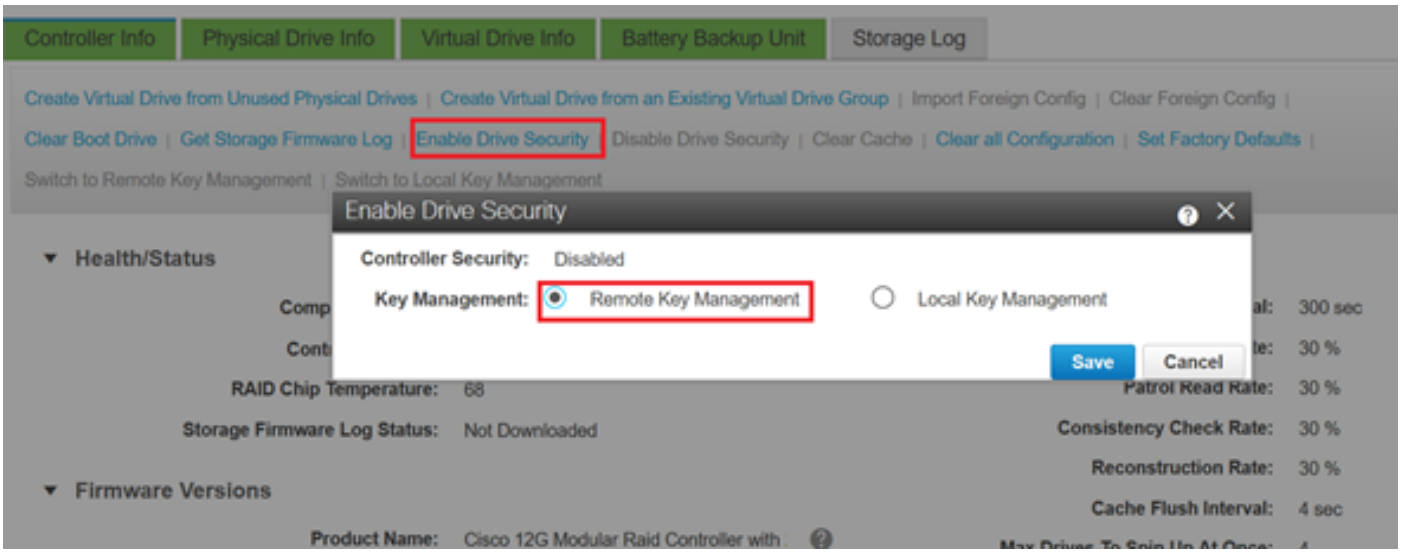


7. Une fois votre connexion avec KMIP établie, vous pouvez activer la gestion des clés à distance.

Accédez à **Networking > Modular Raid Controller > Controller Info**.

Sélectionnez **Enable Drive Security**, puis **Remote Key Management**.

> **Note**: Si la **gestion des clés locales** était activée précédemment, vous êtes invité à saisir la clé actuelle afin de modifier la gestion à distance



Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Vous pouvez vérifier la configuration à partir de l'interface de ligne de commande.

1. Vérifiez si KMIP est activé.

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

2. Vérifiez l'adresse IP, le port et le délai d'attente.

```
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. Vérifiez si les certificats sont 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. Vérifiez les détails de connexion.

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

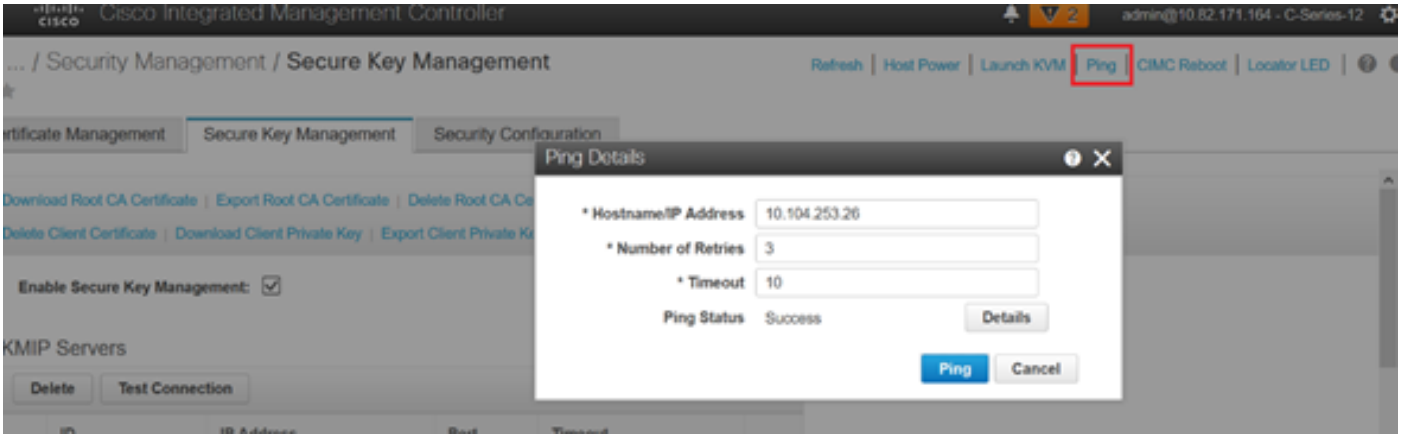
5. Testez la connexion.

```
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!
```

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Si le test de connexion avec le serveur KMIP échoue, assurez-vous que vous pouvez envoyer une requête ping au serveur.

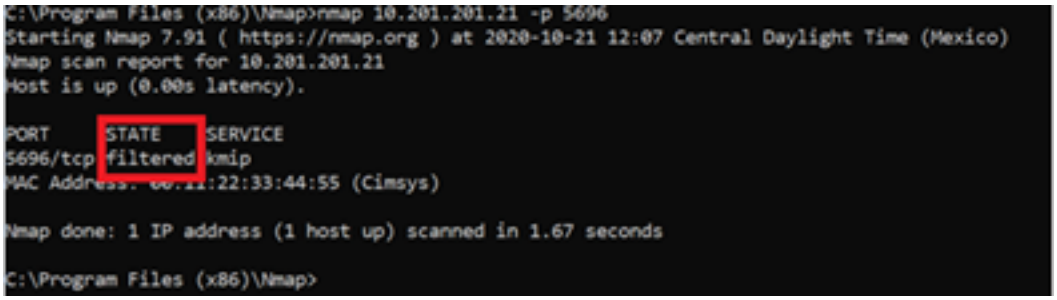


Assurez-vous que le port 5696 est ouvert sur le CIMC et le serveur KMIP. Vous pouvez installer une version NMAP sur votre PC, car cette commande n'est pas disponible sur CIMC.

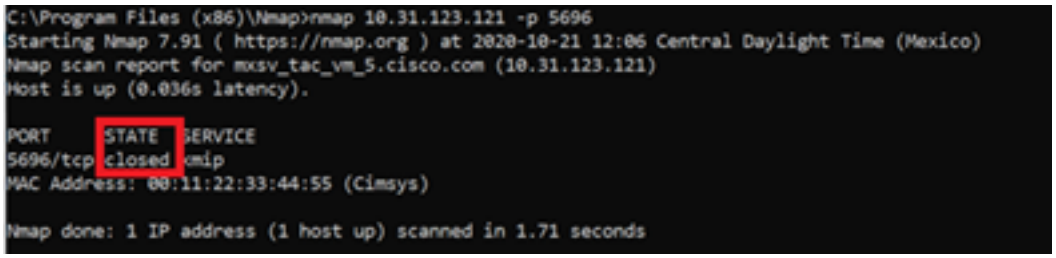
Vous pouvez installer NMAP sur votre machine locale, pour tester si le port est ouvert ; sous le répertoire dans lequel le fichier a été installé, utilisez cette commande :

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

Le résultat montre un port ouvert pour le service KMIP :



Le résultat montre un port fermé pour le service KMIP :



Informations connexes

- Guide de configuration de la gamme C - Disques à chiffrement automatique
- Guide de configuration de la gamme C - Protocole d'interopérabilité de gestion des clés

- Support et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.