독립형 랙 서버에서 원격 키 관리 구성

목차

소개

이 문서에서는 독립형 랙 서버의 KMIP(Key Management Interoperability Protocol) 컨피그레이션에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- CIMC(Cisco Integrated Management Controller)
- 자체 암호화 드라이브(SED)
- KMIP

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- UCSC-C220-M4S, CIMC 버전: 4.1(1시간)
- SED 드라이브
- 800GB 엔터프라이즈 성능 SAS SED SSD(10 FWPD) - MTFDJAK800MBS
- 드라이브 부품 ID: UCS-SD800GBEK9
- 공급업체: 미크론
- 모델: S650DC-800FIPS
- 서드파티 키 관리자로서 Vormetric

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든

명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

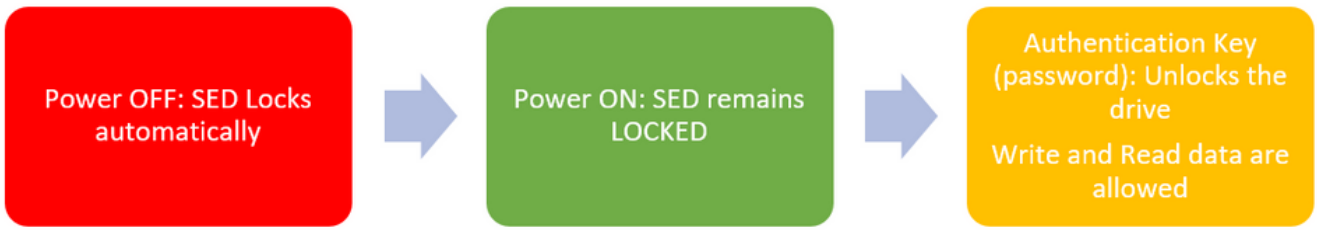
KMIP는 키 관리 서버에서 암호화 키를 조작하기 위한 메시지 형식을 정의하는 확장 가능한 통신 프로토콜입니다. 따라서 암호화 키 관리가 간소화되므로 데이터 암호화가 용이합니다.

SED 드라이브

SED는 하드 디스크 드라이브(HDD) 또는 SSD(Solid-State Drive)로, 드라이브에 암호화 회로가 내장되어 있습니다. 미디어에 기록된 모든 데이터를 투명하게 암호화하고, 잠금을 해제할 경우 미디어에서 읽은 모든 데이터를 투명하게 해독합니다.

SED에서 암호화 키 자체는 SED 하드웨어의 범위를 벗어나지 않으므로 OS 레벨 공격으로부터 안전합니다.

SED 드라이브 워크플로:



1. SED 드라이브 흐름

드라이브의 잠금을 해제하기 위한 비밀번호는 **로컬 키 관리 컨피그레이션**을 통해 로컬에서 얻을 수 있으며, 여기서 사용자의 권한은 키 정보를 기억해야 합니다. 또한 원격 키 관리에서 보안 키를 생성하여 KMIP 서버에서 가져오고 사용자는 CIMC에서 KMIP 서버를 구성해야 합니다.

구성

클라이언트 개인 키 및 클라이언트 인증서 만들기

이러한 명령은 Cisco IMC가 아니라 OpenSSL 패키지가 있는 Linux 시스템에서 입력해야 합니다. Common Name(공통 이름)이 루트 CA 인증서 및 클라이언트 인증서에서 동일한지 확인합니다.

> **참고:** Cisco IMC 시간이 현재 시간으로 설정되어 있는지 확인합니다.

1. 2048비트 RSA 키를 만듭니다.

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

2. 이미 생성한 키로 자체 서명 인증서를 생성합니다.

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

3. 루트 CA 인증서 취득에 대한 자세한 내용은 KMIP 공급업체 설명서를 참조하십시오.

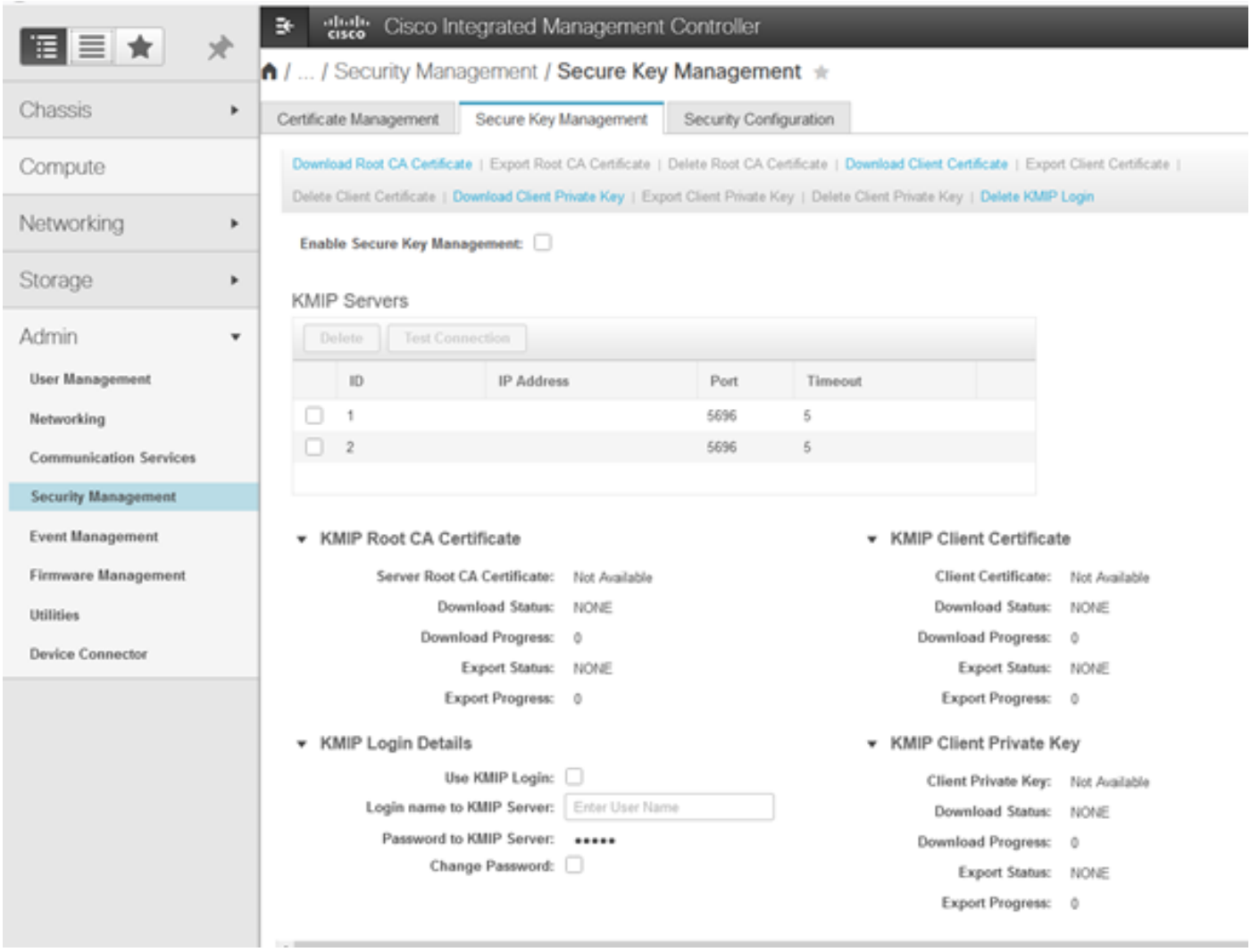
참고: Vormetric을 사용하려면 RootCa 인증서의 일반 이름이 Vormetric 호스트의 호스트 이름과 일치해야 합니다.

참고: KMIP 벤더의 컨피그레이션 가이드에 액세스하려면 계정이 있어야 합니다.
세이프넷
소용돌이

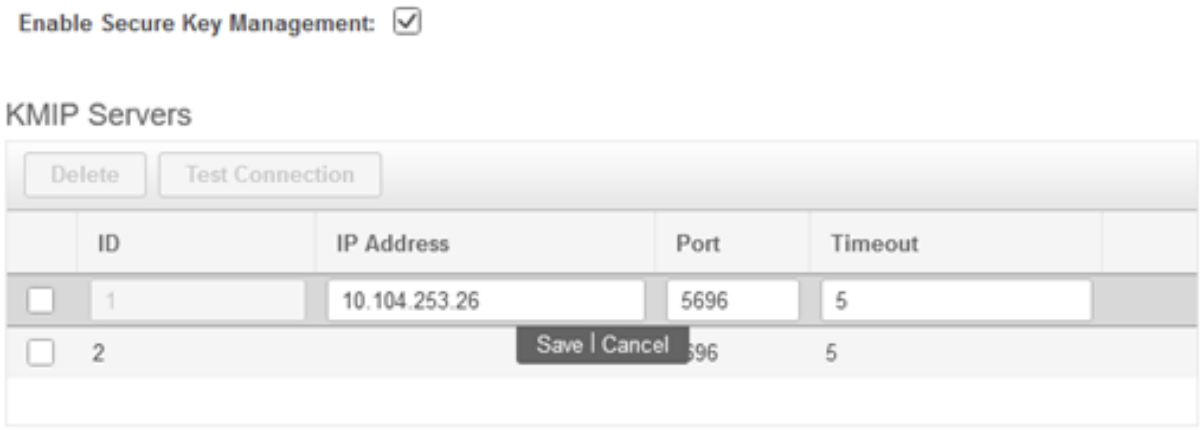
CIMC에서 KMIP 서버 구성

1. Admin(관리) **> Security Management(보안 관리) > Secure Key Management(보안 키 관리)로 이동합니다.**

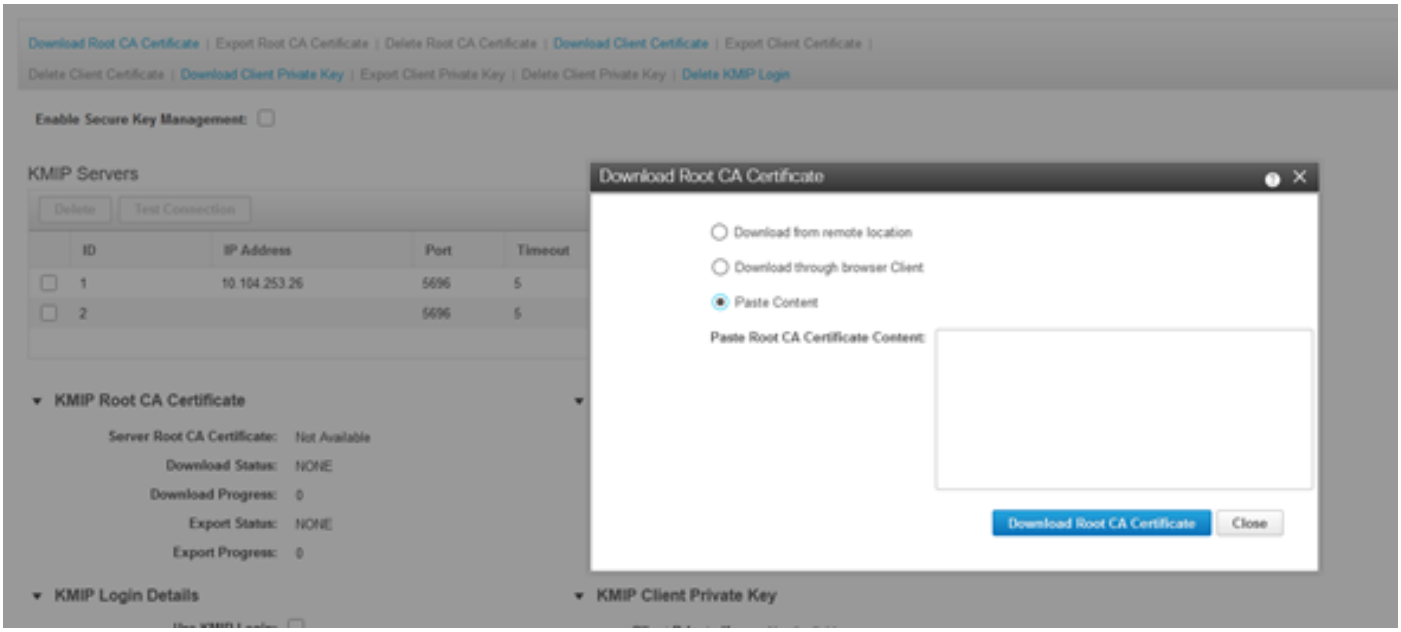
명확한 컨피그레이션이 표시됩니다 **Export/Delete** buttons grayed out, only **Download** buttons are active.



2. IP 주소를 클릭하고 KMIP 서버에 대한 IP를 설정하고, KMIP 서버에 연결할 수 있는지 확인하고, 기본 포트가 사용되는 경우 다른 항목을 변경할 필요가 없으면 변경 사항을 저장합니다.

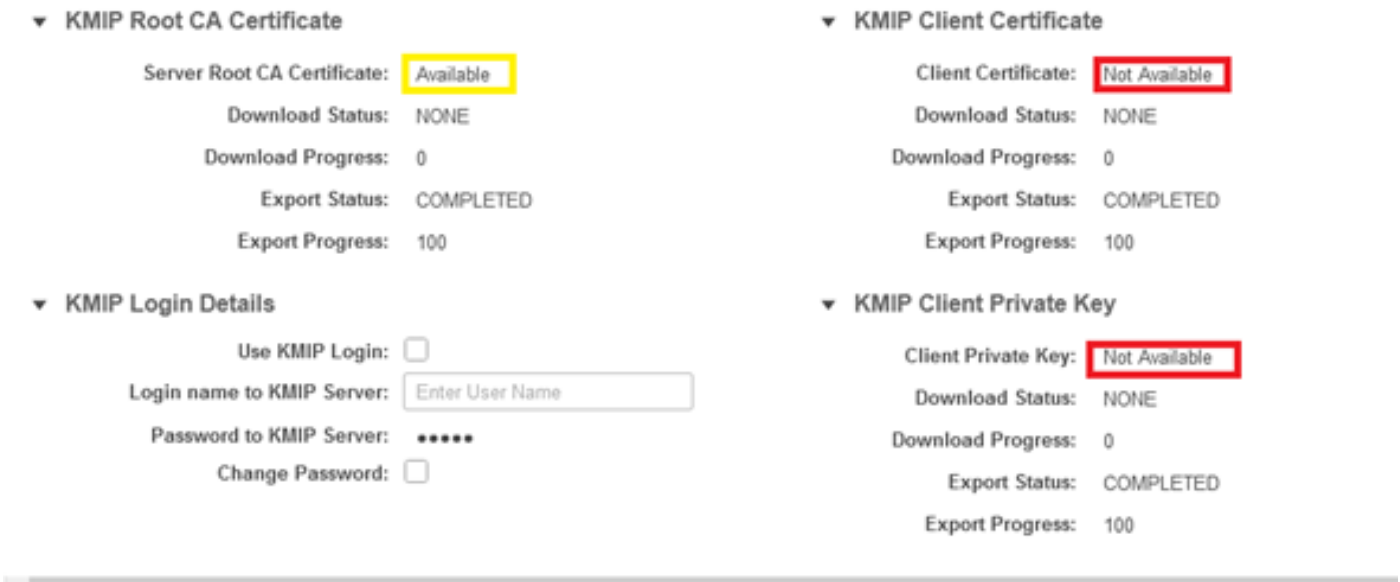


3. 인증서 및 개인 키를 서버에 다운로드합니다. 다운로드 **.pem** file or just paste the content.



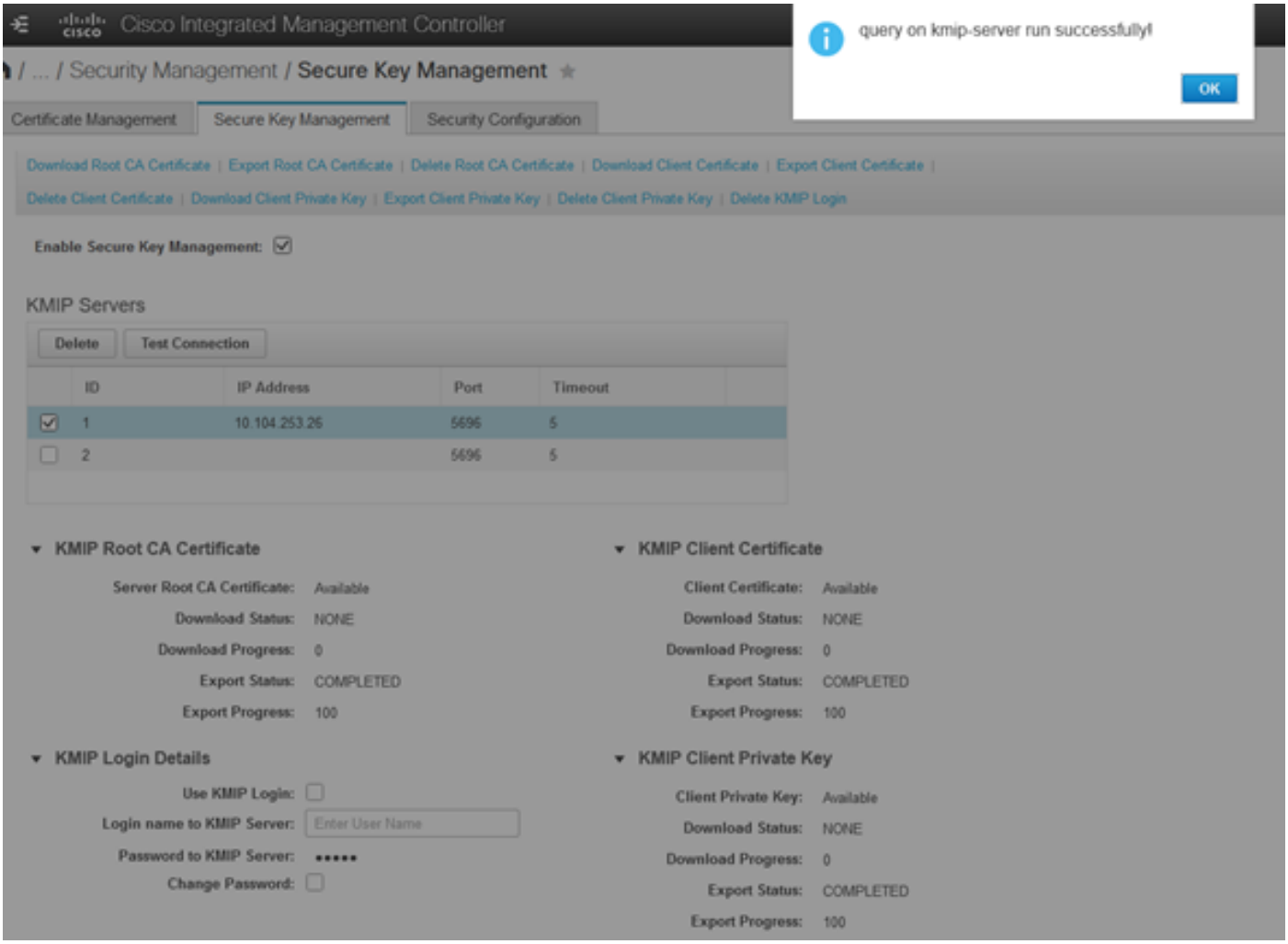
4. 인증서를 업로드하면 인증서가 사용 가능으로 표시되므로, 업로드되지 않은 누락 인증서에 대해서는 사용 불가능으로 **표시됩니다**.

모든 인증서 및 개인 키가 CIMC에 성공적으로 다운로드된 경우에만 연결을 테스트할 수 있습니다.



5. (선택 사항) 모든 인증서가 있는 경우 선택적으로 KMIP 서버에 대한 사용자 및 비밀번호를 추가할 수 있습니다. 이 컨피그레이션은 SafeNet을 서드파티 KMIP 서버로만 지원합니다.

6. 연결을 테스트하고 인증서가 올바르며 구성된 포트를 통해 KMIP 서버에 연결할 수 있으면 연결에 성공했음을 확인합니다.

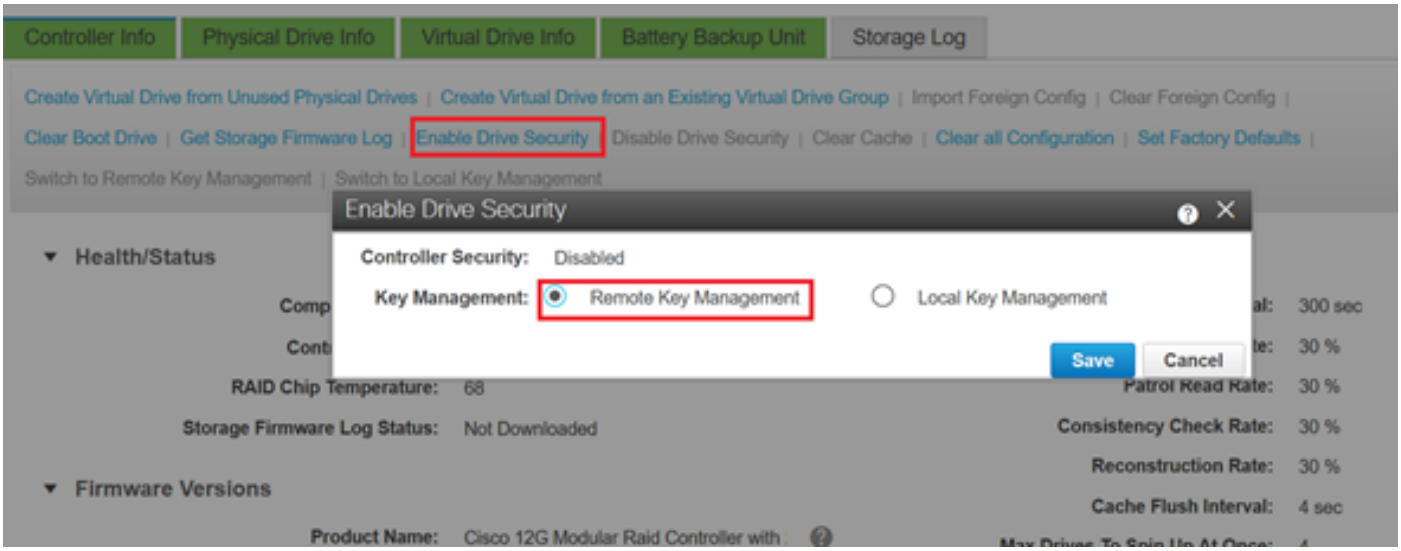


7. KMIP와의 연결에 성공하면 원격 키 관리를 활성화할 수 있습니다.

Networking(네트워킹) **> Modular Raid Controller(모듈형 Raid 컨트롤러) > Controller Info(컨트롤러 정보)로 이동합니다**.

Enable **Drive Security(드라이브 보안 활성화)**를 선택한 다음 **Remote Key Management(원격 키 관리)를 선택합니다**.

> **참고:** 이전에 **로컬 키 관리**를 활성화한 경우 원격 관리를 위해 변경하기 위해 현재 키를 묻는 메시지가 표시됩니다



다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

CLI에서 컨피그레이션을 확인할 수 있습니다.

1. KMIP가 활성화되어 있는지 확인합니다.

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

2. IP 주소, 포트 및 시간 제한을 확인합니다.

```
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. 인증서를 사용할 수 있는지 확인합니다.

```
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. 로그인 세부 정보를 확인합니다.

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

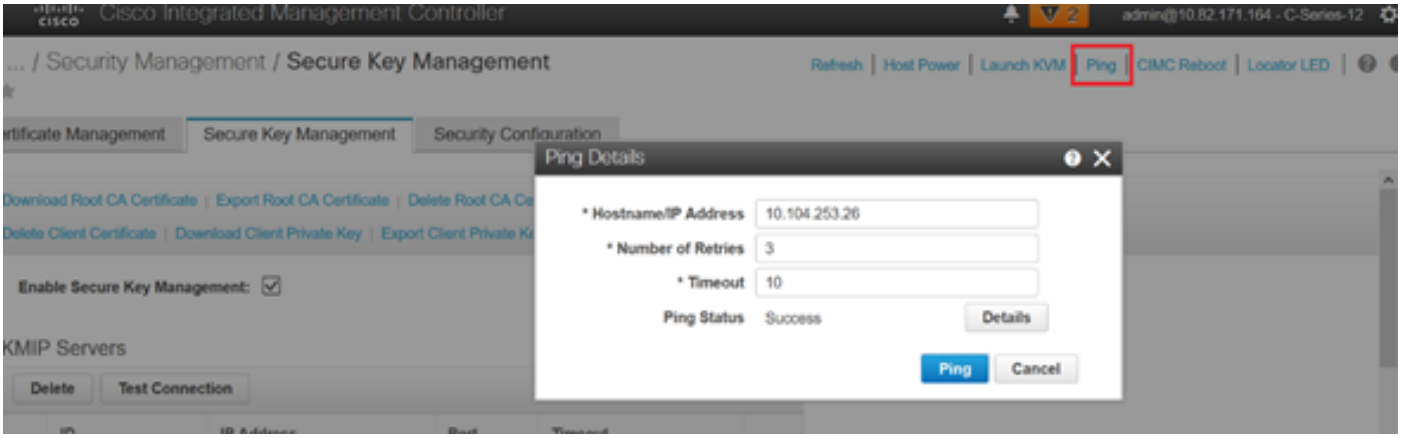
5. 연결을 테스트합니다.

```
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!
```

문제 해결

현재 이 설정에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

KMIP 서버와의 테스트 연결이 성공하지 못하면 서버를 ping할 수 있는지 확인합니다.

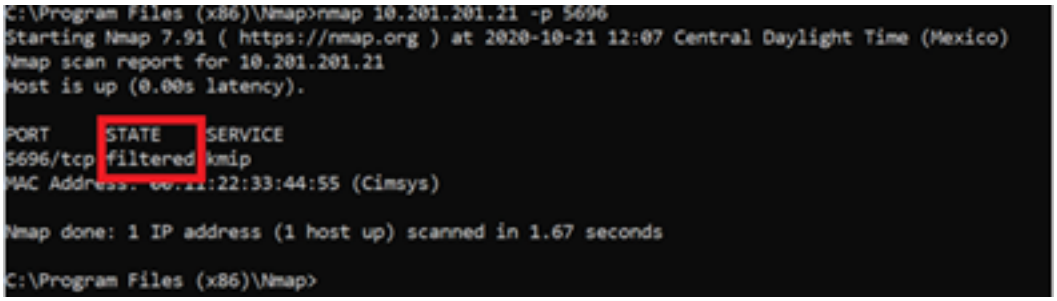


포트 5696이 CIMC 및 KMIP 서버에서 열려 있는지 확인합니다. CIMC에서는 이 명령을 사용할 수 없으므로 PC에 NMAP 버전을 설치할 수 있습니다.

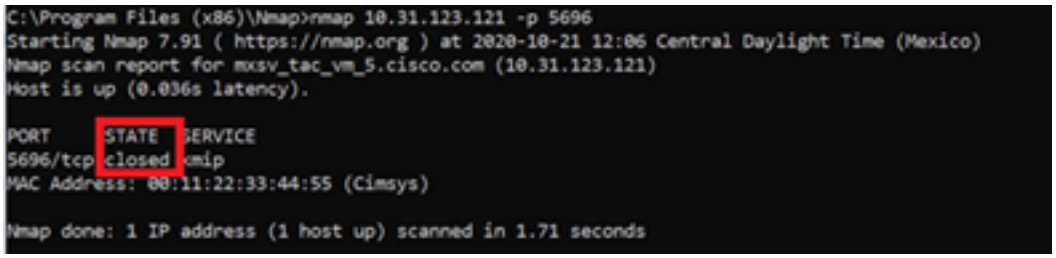
NMAP을 로컬 시스템에 설치하여 포트가 열려 있는지 테스트할 수 있습니다. 파일이 설치된 디렉토리에서 다음 명령을 사용합니다.

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

이 출력은 KMIP 서비스에 대한 오픈 포트를 보여줍니다.



이 출력은 KMIP 서비스에 대한 닫힌 포트를 보여줍니다.



관련 정보

- C 시리즈 구성 가이드 - 자체 암호화 드라이브
- C 시리즈 구성 가이드 - 키 관리 상호 운용성 프로토콜
- 기술 지원 및 문서 – Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.