# Dell™ PowerVault™ Encryption Key Manager

## LTO Ultrium 4와 LTO Ultrium 5의 빠른 시작 안내서

이 안내서를 사용하여 LTO Gen 5 테이프 드라이브에서의 암호화에 대한 *기본 구성*을 시작할 수 있습니다. 문제점이 없는지 확인하기 위해 Dell PowerVault Encryption Key Manager를 설치 및 구성하기 전에 **http://support.dell.com**에 방문하여 최신 라이브러리와 드라이브 펌웨어를 다운로드하십시오.

Dell PowerVault Encryption Key Manager(이후로는 Encryption Key Manager라 지칭함)는 암호화 가능한 테이프 드라이브를 사용하여 암호화 키를 생성, 보호, 저장 및 유지보수하는 데 도움을 주는 Java™ 소프트웨어 프로그램입니다. 이 키는 LTO 테이프 매체에 기록하는 정보를 암호화하고 그 매체에서 읽는 정보를 해독하는 데 사용됩니다. Encryption Key Manager는 Linux® 및 Windows®에서 작동하며 엔터프라이즈 내의 여러 위치에 전개되는 공유 자원이 되도록 설계되어 있습니다.

이 문서에서는 그래픽 사용자 인터페이스(GUI) 또는 명령을 사용하여 Encryption Key Manager를 신속하게 설치 및 설정하는 방법을 설명합니다. 이 문서에서는 JCEKS 키 저장소 유형을 사용하는 방법에 대해 설명합니다. (JCEKS 키 저장소 유형이 지원되는 키 저장소 중 가장 쉽고 가장 전송 가능성이 좋은 유형이기 때문입니다.) 특정 단계나 지원되는 다른 키 저장소 유형에 대한 자세한 정보는 웹 사이트 **http://support.dell.com** 또는 제품과 함께 제공되는 Dell Encryption Key Manager 매체

**주:** 에 있는 *Dell Encryption Key Manager 사용자 안내서*를 참조하십시오. 중요한 Encryption Key Manager 호스트 서버 구성 정보: Dell Encryption Key Manager 프로그램을 호스트하는 시스템은 데이터 유실의 위험을 최소화하기 위해 ECC 메모리를 사용할 것을 권장합니다. Encryption Key Manager는 암호화 키의 생성을 요청하고 이들 키를 LTO-4 및 LTO 5 테이프 드라이브에 전달하는 기능을 수행합니다. 랩된(암호화된) 키는 처리 중 Encryption Key Manager가 시스템 메모리에 배치합니다. 카트리지에 기록된 데이터를 복구(암호 해독)할 수 있으려면 오류 없이 키를 적절한 테이프 드라이브에 전송해야 합니다. 시스템 메모리의 비트 오류로 키가 손상되었고 카트리지에 데이터를 쓸 때 이 키를 사용하는 경우, 해당 카트리지에 쓰여진 데이터는 복구할 수 없습니다. (즉, 차후에 암호를 해독할 수 없습니다.) 이러한 데이터 오류가 발생하지 않도록 하는 보호 장치가 마련되어 있습니다. 그러나 Encryption Key Manager를 호스트하는 시스템이 ECC(Error Correction Code) 메모리를 사용하지 않는 경우, 시스템 메모리에 있는 동안 키가 손상되고 이러한 손상으로 데이터 유실이 발생할 수 있는 가능성은 남아 있습니다. 이와 같은 데이터 유실 가능성은 적지만 중요 응용프로그램(예: Encryption Key Manager)을 호스트하는 시스템은 ECC 메모리를 사용할 것을 권장합니다.

## 첫 번째 수행 작업: Encryption Key Manager 소프트웨어 설치

1. Dell Encryption Key Manager CD를 삽입하십시오. Windows에서 자동으로 설치가 시작되지 않는 경우, CD를 탐색하여 Install_Windows.bat을 두 번 누르십시오.

Linux의 경우, 설치는 자동으로 시작되지 않습니다. CD 루트 디렉토리로 가서 `Install_Linux.sh`를 입력하십시오.

일반 사용자 라이센스 계약이 표시됩니다. 설치를 계속하려면 이 라이센스 계약을 승인해야 합니다.

설치 프로그램이 CD에서 하드 드라이브로 운영 체제에 적합한 모든 내용(문서, GUI 파일 및 구성 등록 정보 파일)을 복사합니다. 설치 중 시스템에서는 올바른 IBM JRE(Java Runtime Environment)가 있는지 확인합니다. 찾지 못하면 자동으로 설치됩니다.

설치가 완료되면 그래픽 사용자 인터페이스(GUI)가 시작됩니다.

## 방법 1: GUI를 사용하여 Encryption Key Manager 설정

이 프로시저는 기본 구성을 작성합니다. 성공적으로 완료하면 Encryption Key Manager 서버가 시작됩니다.

1. GUI가 시작되지 않으면 다음과 같이 여십시오.

   **Windows**

   c:\ekm\gui를 탐색하고 `LaunchEKMGui.bat`를 누르십시오.

   **Linux 플랫폼**

   /var/ekm/gui를 탐색하고 `. ./LaunchEKMGui.sh`를 입력하십시오.

   참고: Linux 쉘이 스크립트를 찾을 수 있도록 Linux 쉘 명령 앞에 . ./(마침표 공백 마침표 정방향 슬래시)를 지정하십시오.

2. EKM 서버 구성 페이지(그림 1)에서 별표(*)로 표시된 모든 필수 필드에 데이터를 입력하십시오. 필드에 대한 설명을 보려면 데이터 필드 오른쪽에 있는 물음표를 누르십시오. EKM 서버 인증서 구성 페이지로 이동하려면 **다음(Next)**을 누르십시오.

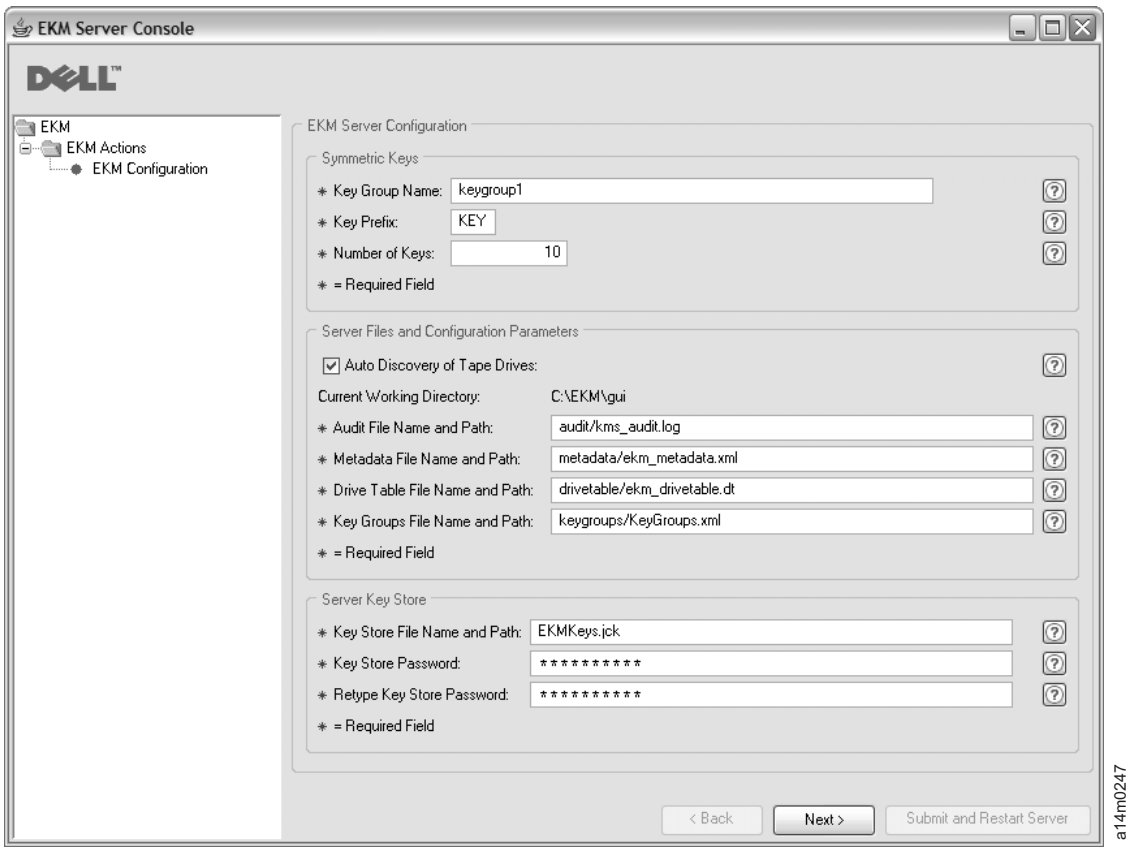


*그림 1. EKM 서버 구성 페이지*

**주:**

a. 드라이브가 드라이브 테이블에 저장되었는지 확인하려면 자동 검색을 통해 드라이브가 추가된 이후에 GUI를 사용하여 Encryption Key Manager 서버를 새로 고쳐야 합니다.

b. 키 저장소 암호를 설정하면 보안을 위반하지 않는 한 **변경하지 마십시오**. 보안 노출 위험을 없애기 위해 암호는 인식하기 어렵게 만들어집니다. 키 저장소 암호를 변경하려면 **keytool** 명령을 사용하여 개별적으로 해당 키 저장소의 모든 키에 대한 암호를 변경해야 합니다. *Dell Encryption Key Manager 사용자 안내서*에 있는 『키 저장소 암호 변경』을 참조하십시오.

3. EKM 서버 인증서 구성 페이지(그림 2)에서 키 저장소 별명을 입력하고 인증서 및 인증 용도 식별에 사용하는 추가 필드를 모두 채우십시오. **제출 및 서버 다시 시작(Submit and Restart Server)**을 누르십시오.

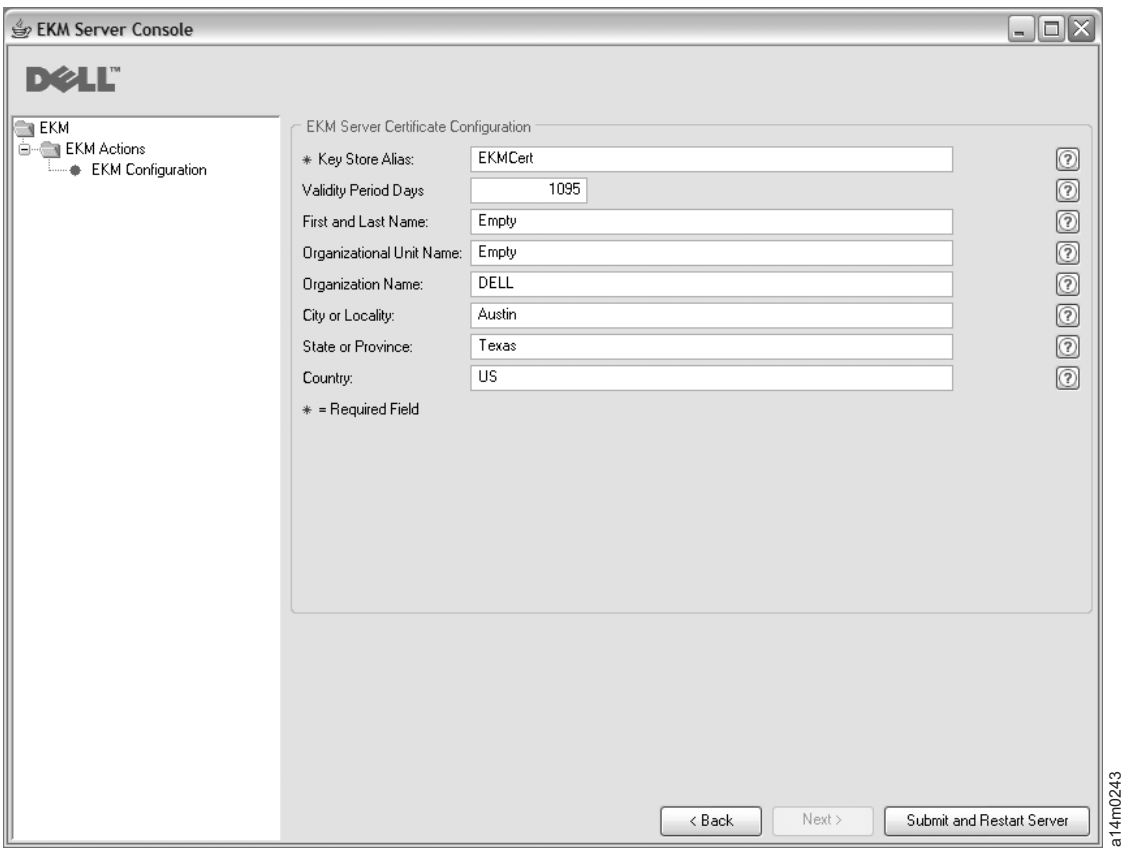


*그림 2. EKM 서버 인증서 구성(EKM Server Certificate Configuration) 페이지*

**주:** 키 생성 중 Encryption Key Manager GUI가 인터럽트되는 경우, Encryption Key Manager를 다시 설치해야 합니다.

Encryption Key Manager의 키 생성 프로세스가 완료되기 전에 이를 중지하는 경우, 키 저장소 파일이 손상될 수 있습니다. 이러한 손상을 복구하려면 다음 단계를 따르십시오.

- 최초 설치 중에 Encryption Key Manager가 인터럽트된 경우, 디렉토리가 위치한 디렉토리(예: x:\ekm)로 이동하십시오. 디렉토리를 삭제하고 설치를 다시 시작하십시오.
- 새로운 키 그룹을 추가하는 중에 Encryption Key Manager가 인터럽트된 경우 Encryption Key Manager 서버를 중지하고 최신 백업 키 저장소(파일 위치는 x:\ekm\gui\backupfiles 폴더임)를 사용하여 키 저장소 파일을 복원하십시오. 백업 파일의 파일 이름에는 날짜와 시간 소인

(예: 2007_11_19_16_38_31_EKMKeys.jck)이 포함되어 있습니다. 파일이 x:\ekm\gui 디렉토리에 복사되면 날짜와 시간 소인을 제거해야 합니다. Encryption Key Manager 서버를 다시 시작하고 이전에 인터럽트된 키 그룹을 추가하십시오.

4. Encryption Key Manager 데이터 파일을 백업해야 함을 알리는 백업 창(그림 3)이 표시됩니다. 백업 데이터를 저장할 경로를 입력하십시오. **백업(Backup)**을 누르십시오.

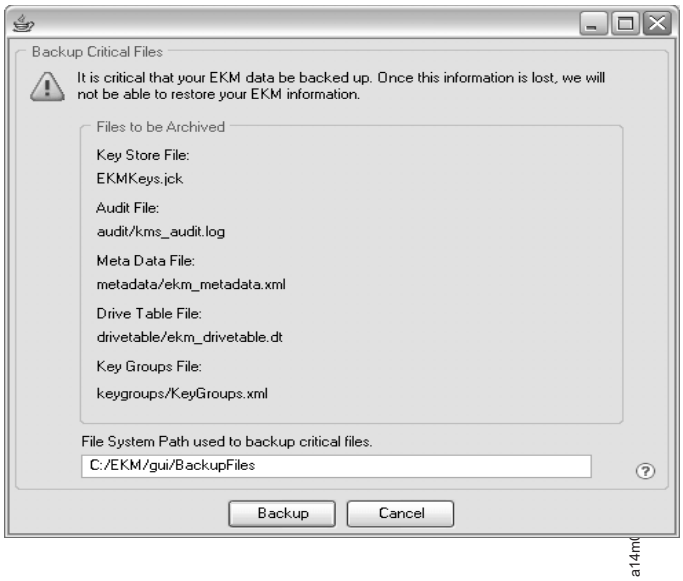


*그림 3. 중요 파일 백업 창*

5. 사용자 로그인 페이지가 표시됩니다. 기본 사용자 이름 EKMAdmin 및 기본 암호 changeME를 입력하십시오. **로그인(Login)**을 누르십시오.

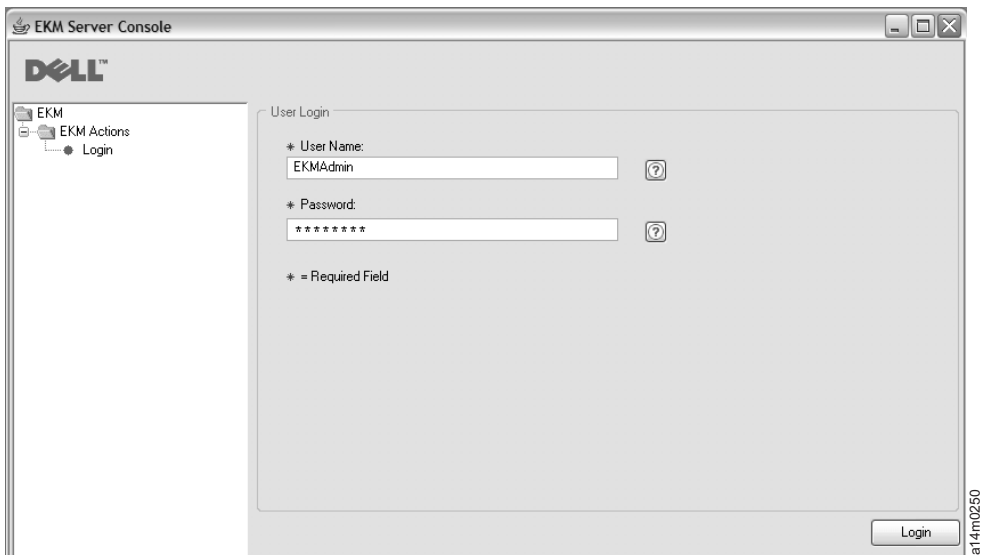


*그림 4. 사용자 로그인 페이지*

Dell Encryption Key Manager 서버가 백그라운드에서 실행됩니다.

6. GUI 탐색기에서 **서버 상태 모니터(Server Health Monitor)**를 선택하고 Encryption Key Manager 서버가 가동 중인지 확인하십시오.

**올바른 호스트 IP 주소를 찾는 방법**

현재 Encryption Key Manager GUI에 적용되는 제한사항 때문에 서버 상태 모니터(Server Health Monitor)에 Encryption Key Manager 호스트 IP 주소를 표시할 수 없습니다.

- IPv6 주소를 사용하여 호스트를 구성하는 경우 Encryption Key Manager 응용프로그램이 IP 주소를 표시할 수 없습니다.
- Encryption Key Manager 응용프로그램이 Linux 시스템에 설치된 경우 Encryption Key Manager 응용프로그램은 로컬 호스트 주소는 표시하지만 실제의 활성 IP 포트는 표시하지 않습니다.

a. 호스트 시스템의 실제 IP 주소를 검색하려면 네트워크 구성에 액세스하여 IP 포트 주소를 찾으십시오.
   - Windows 시스템의 경우 명령 창을 열고 `ipconfig`를 입력하십시오.
   - Linux의 경우 `isconfig`를 입력하십시오.

**EKM SSL 포트를 식별하는 방법**

a. 명령행을 사용하여 Encryption Key Manager 서버를 시작하십시오.
   - Windows의 경우 CD의 `c:\ekm`으로 이동하여 **startServer.bat**을 누르십시오.
   - Linux 플랫폼의 경우 `/var/ekm`으로 이동하여 `startServer.sh`를 입력하십시오.
   - 자세한 정보는 *Dell Encryption Key Manager 사용자 안내서*의 『Key Manager 서버 시작, 새로 고침 및 중지』를 참조하십시오.

b. 명령행을 사용하여 CLI 클라이언트를 시작하십시오.
   - Windows의 경우 CD의 `c:\ekm`으로 이동하여 **startClient.bat**을 누르십시오.
   - Linux 플랫폼의 경우 `/var/ekm`으로 이동하여 `startClient.sh`를 입력하십시오.
   - 자세한 정보는 *Dell Encryption Key Manager 사용자 안내서*의 『명령행 인터페이스 클라이언트 시작』을 참조하십시오.

c. 다음 명령을 사용하여 Encryption Key Manager 서버의 CLI 클라이언트에 로그인하십시오.

   `login –ekmuser` *`userID`* `–ekmpassword` ***`password`***

   여기서, *userID*는 EKMAdmin이고 *password*는 changeME입니다. (이것이 기본 암호입니다. 이전에 기본 암호를 변경한 경우 새 암호를 사용하십시오.)

   로그인에 성공하면 `User successfully logged in`이 표시됩니다.

d. 다음 명령을 입력하여 SSL 포트를 식별하십시오.

   `status`

   표시되는 응답이 다음과 유사해야 합니다. `server is running. TCP port: 3801, SSL port: 443.`

   SSL 구성 포트를 기록해두고 라이브러리 관리 암호화 설정을 구성할 때 이 포트를 사용했는지 확인하십시오.

e. 명령행에서 로그아웃하십시오. 다음 명령을 입력하십시오.

```
exit
```

명령 창을 닫으십시오.

---

## 방법 2: 명령을 사용하여 Encryption Key Manager 설정

### 1 단계. JCEKS 키 저장소 작성

**주의:** Encryption Key Manager 및 모든 연관된 파일의 사본을 정기적으로 작성해야 합니다. Encryption Key Manager 암호화 키가 유실되거나 손상되면 암호화 데이터를 복구할 방법이 없습니다.

키 저장소를 작성하고 인증서 및 개인용 키로 채우십시오. 인증은 Encryption Key Manager 서버 사이의 통신과 Encryption Key Manager CLI 클라이언트와의 통신 보안을 위해 사용됩니다. 이 **keytool** 명령은 EKMKeys.jck라고 하는 새 JCEKS 키스토어를 작성하고 별명이 ekmcert인 개인용 키 및 인증으로 채웁니다. 이 인증은 5년 동안 유효합니다. 인증이 만료되면 Encryption Key Manager 서버 사이의 통신과 Encryption Key Manager CLI 클라이언트 및 Encryption Key Manager 서버 사이의 통신이 작동하지 않을 수 있습니다. 만기된 이전 인증을 제거하고 이 단계에 지정된 대로 인증을 새로 작성하십시오.

```
keytool -keystore EKMKeys.jck -storetype jceks -genkey -alias ekmcert -keyAlg RSA -keysize 2048
–validity 1825
```

keytool 명령을 사용할 경우 Encryption Key Manager ID를 허용하는 인증 작성에 사용되는 정보를 입력하라는 프롬프트가 표시됩니다. 샘플 응답이 있는 프롬프트는 다음과 유사합니다.

```
What is your first and last name? [Unknown]:  ekmcert
What is the name of your organizational unit?   [Unknown]:  EKM
What is the name of your organization? [Unknown]:  Dell
What is the name of your City or Locality?   [Unknown]: Austin
What is the name of your State or Province?   [Unknown]:  TX
What is the two-letter country code for this unit? [Unknown]:  US
Is CN=ekmcert, OU=EKM, O=Dell, L=Austin, ST=TX, C=US correct?(type "yes" or "no"):
```

yes를 입력하고 Enter를 누르십시오.

### 2 단계. 암호화 키 생성

**주:** 세션에서 처음 keytool 명령을 사용하려면 먼저 **updatePath** 스크립트를 실행하여 올바른 환경을 설정해야 합니다.

**Windows**

cd c:\ekm를 탐색하고 updatePath.bat를 누르십시오.

**Linux 플랫폼**

/var/ekm을 탐색하고 . ./updatePath.sh를 입력하십시오.

참고: Linux 쉘이 스크립트를 찾을 수 있도록 Linux 쉘 명령 앞에 . ./(마침표 공백 마침표 정방향 슬래시)를 지정하십시오.

LTO 암호화의 경우, Encryption Key Manager에서 여러 개의 대칭 키를 사전에 생성하여 키 저장소에 저장해야 합니다. 다음 **keytool** 명령은 32개의 256비트 AES 키를 생성하여 3단계에서 작성하는 키 저장소에 저장합니다. Encryption Key Manager 디렉토리에서 이 명령을 실행하여 해당 디렉토리에 키 저장소가 작성되도록 하십시오. 결과 키는 key00000000000000000부터 key0000000000000001f까지의 이름을 포함하게 됩니다.

```
keytool –keystore EKMKeys.jck –storetype jceks –genseckey –keyAlg aes –keysize 256 –aliasrange
key00-1f
```

이 명령은 키 저장소에 액세스하기 위해 키 저장소 암호를 입력하도록 요청하는 프롬프트를 표시합니다. 원하는 암호를 입력한 후 Enter를 누르십시오. 키 암호에 대해 정보가 필요하지 않은 것으로 프롬프트가 표시된 경우 다시 Enter를 누르십시오. 새 암호나 다른 암호를 입력하지 마십시오. 그러면 키 암호는 키 저장소 암호와 같게 됩니다. 여기에 입력한 키 저장소 암호를 기록해 두십시오. 나중에 Encryption Key Manager를 시작할 때 필요합니다.

**주:** 키 저장소 암호를 설정하고 나면 보안 위반이 발생하지 않는 한 변경하지 마십시오. 키 저장소 암호를 변경하면 구성 파일에 있는 모든 암호 특성도 변경해야 합니다. 보안 노출 위험을 없애기 위해 암호는 인식하기 어렵게 만들어집니다.

## 3 단계. Encryption Key Manager 서버 시작

GUI를 사용하지 않고 Encryption Key Manager 서버를 시작하려면 startServer 스크립트를 실행하십시오.

**Windows**

`cd c:\ekm\ekmserver`를 탐색하고 startServer.bat를 누르십시오.

**Linux 플랫폼**

/var/ekm/ekmserver를 탐색하고 `. ./startServer.sh`를 입력하십시오.

참고: Linux 쉘이 스크립트를 찾을 수 있도록 Linux 쉘 명령 앞에 . ./(마침표 공백 마침표 정방향 슬래시)를 지정하십시오.

**주의:** Encryption Key Manager 및 모든 연관된 파일의 사본을 정기적으로 작성해야 합니다. Encryption Key Manager 암호화 키가 유실되거나 손상되면 암호화 데이터를 복구할 방법이 없습니다.

## 4 단계. Encryption Key Manager 명령행 인터페이스 클라이언트 시작

Encryption Key Manager CLI 클라이언트를 시작하려면 startClient 스크립트를 실행하십시오.

**Windows**

`cd c:\ekm\ekmclient`를 탐색하고 startClient.bat를 누르십시오.

**Linux 플랫폼**

/var/ekm\ekmclient를 탐색하고 `. ./startClient.sh`를 입력하십시오.

참고: Linux 쉘이 스크립트를 찾을 수 있도록 Linux 쉘 명령 앞에 . ./(마침표 공백 마침표 정방향 슬래시)를 지정하십시오.

CLI 클라이언트가 Key Manager 서버에 로그인하면 CLI 명령을 실행할 수 있습니다. 완료할 때 CLI 클라이언트를 종료하려면 quit 명령을 사용하십시오. 클라이언트는 10분 동안 사용하지 않는 경우에 자동으로 종료됩니다. CLI 명령 정보에 대해서는 웹 사이트 **http://support.dell.com** 또는 제품과 함께 제공되는 Dell Encryption Key Manager 매체에 있는 *Dell Encryption Key Manager 사용자 안내서*를 참조하십시오.

## 자세한 정보

자세한 정보는 다음 서적을 참조하십시오.

- *Dell Encryption Key Manager 사용자 안내서*(Dell Encryption Key Manager CD에 포함되어 있으며 **http://support.dell.com**에서도 제공됨).
- *Library Managed Encryption for Tape* 백서 - LTO 테이프 암호화에 대한 최적 사례를 제시합니다 (**http://www.dell.com**에서도 제공됨).