Dell™ PowerVault™ Encryption Key Manager

Leitfaden für den Schnelleinstieg in die Arbeit mit LTO Ultrium 4- und LTO Ultrium 5-Bandlaufwerken

In diesem Leitfaden wird eine ***Basiskonfiguration*** für Verschlüsselungen auf LTO 4- und LTO 5-Bandlaufwerken erläutert. Bevor Sie Dell PowerVault Encryption Key Manager installieren und konfigurieren, müssen Sie unter **http://support.dell.com** die aktuelle Firmware für Bandarchive und -laufwerke herunterladen, um sicherzustellen, dass keine Fehler auftreten.

Beim Dell PowerVault Encryption Key Manager (nachfolgend als Encryption Key Manager bezeichnet) handelt es sich um ein Java™-Softwareprogramm, mit dem auf verschlüsselungsfähigen Bandlaufwerken Verschlüsselungsschlüssel generiert, geschützt, gespeichert und verwaltet werden können. Diese Schlüssel werden dazu verwendet, Informationen zu verschlüsseln, die auf LTO-Banddatenträger geschrieben werden, und Informationen zu entschlüsseln, die von diesen Datenträgern gelesen werden. Encryption Key Manager kann unter Linux® und Windows® ausgeführt werden. Diese Software wurde als gemeinsam genutzte Ressource konzipiert, die an mehreren Positionen innerhalb eines Unternehmens implementiert werden kann.

In diesem Dokument wird erläutert, wie Sie Encryption Key Manager schnell über die grafische Benutzerschnittstelle oder über Befehle installieren und konfigurieren können. Des Weiteren wird die Verwendung des Keystores JCEKS erläutert, da dieser Keystore der am einfachsten und am besten zu übertragende Keystore-Typ aller unterstützten Keystores ist. Weitere Informationen zu einem bestimmten Schritt oder einem weiteren unterstützten Keystore-Typ finden Sie im Handbuch *Dell Encryption Key Manager Benutzerhandbuch* unter **http://support.dell.com** oder auf dem EKM-Datenträger von Dell, der im Lieferumfang Ihres Produkts enthalten ist.

Anmerkung: WICHTIGE INFORMATIONEN ZUR KONFIGURATION DES EKM-HOST-SERVERS: Es empfiehlt sich, auf Systemen, auf denen Encryption Key Manager installiert ist, ECC-Speicher (Error Correction Code) zu verwenden, um das Risiko von Datenverlusten auf ein Minimum zu reduzieren. Encryption Key Manager übernimmt die Funktion, das Erstellen von Verschlüsselungsschlüsseln anzufordern und diese an LTO 4- und LTO 5-Bandlaufwerke weiterzuleiten. Die Schlüssel befinden sich während der Verarbeitung durch Encryption Key Manager (in verschlüsselter Form) im Systemspeicher. Sie müssen fehlerfrei an das richtige Bandlaufwerk übertragen werden, damit die auf einer Bandkassette gespeicherten Daten wiederhergestellt (entschlüsselt) werden können. Falls bestimmte Schlüssel auf Grund eines Bitfehlers im Systemspeicher beschädigt und anschließend zum Schreiben von Daten auf eine Bandkassette verwendet werden, können die auf diese Bandkassette geschriebenen Daten nicht wiederhergestellt (d. h. zu einem späteren Zeitpunkt entschlüsselt) werden. Es stehen Sicherheitsfunktionen zur Verfügung, mit denen sichergestellt wird, dass solche Datenfehler nicht auftreten. Wenn das System, auf dem Encryption Key Manager installiert ist, jedoch keinen ECC-Speicher verwendet, besteht weiterhin die Möglichkeit, dass Schlüssel im Systemspeicher beschädigt werden. Diese Beschädigungen können anschließend zu Datenverlusten führen. Die Wahrscheinlichkeit solcher Beschädigungen ist zwar gering, es empfiehlt sich allerdings, auf Systemen, auf denen kritische Anwendungen installiert sind (wie z. B. Encryption Key Manager), ECC-Speicher zu verwenden.

Erster Schritt: Installieren der EKM-Software

1. Legen Sie die CD mit Encryption Key Manager von Dell ein. Falls die Installation nicht automatisch unter Windows startet, wechseln Sie auf das CD-ROM-Laufwerk, und klicken Sie doppelt auf die Datei Install_Windows.bat.

   Unter Linux startet die Installation nicht automatisch. Wechseln Sie in das Stammverzeichnis der CD, und geben Sie `Install_Linux.sh` ein.

   Daraufhin wird eine Endbenutzer-Lizenzvereinbarung angezeigt. Sie müssen dieser Lizenzvereinbarung zustimmen, damit der Installationsvorgang fortgesetzt wird.

   Bei der Installation werden alle Dateien (Dokumentation, GUI-Dateien und Eigenschaftendateien für die Konfiguration), die für das von Ihnen verwendete Betriebssystem benötigt werden, von der CD auf das Festplattenlaufwerk kopiert. Während der Installation wird geprüft, ob auf dem System die richtige IBM Java Runtime Environment installiert ist. Wenn diese Software nicht gefunden werden kann, wird sie automatisch installiert.

   Nach Abschluss der Installation wird die grafische Benutzerschnittstelle (GUI) gestartet.

Methode 1: Konfigurieren von EKM über die grafische Benutzerschnittstelle

Mit dieser Prozedur wird eine Basiskonfiguration erstellt. Nach Abschluss dieser Prozedur wird der EKM-Server gestartet.

1. Wenn die grafische Benutzerschnittstelle nicht gestartet wird, können Sie sie wie folgt aufrufen:
   Unter Windows
   Wechseln Sie in das Verzeichnis c:\ekm\gui, und klicken Sie auf `LaunchEKMGui.bat`.
   Auf Linux-Plattformen
   Wechseln Sie in das Verzeichnis /var/ekm/gui, und geben Sie `. ./LaunchEKMGui.sh` ein.
   Anmerkung: Geben Sie vor dem Linux-Shellbefehl ". ./" ein (zwei durch ein Leerzeichen getrennte Punkte, gefolgt von einem Schrägstrich), um sicherzustellen, dass die Shell das Script findet.
2. Geben Sie auf der Seite **EKM Configuration** (Abb. 1) Daten in alle Felder ein, in denen eine Angabe gemacht werden muss. Diese sind mit einem Stern (*) gekennzeichnet. Wenn Sie auf das Fragezeichen rechts neben einem Datenfeld klicken, wird eine entsprechende Beschreibung angezeigt. Klicken Sie auf **Next**, um auf die Seite **EKM Server Certificate Configuration** zu wechseln.

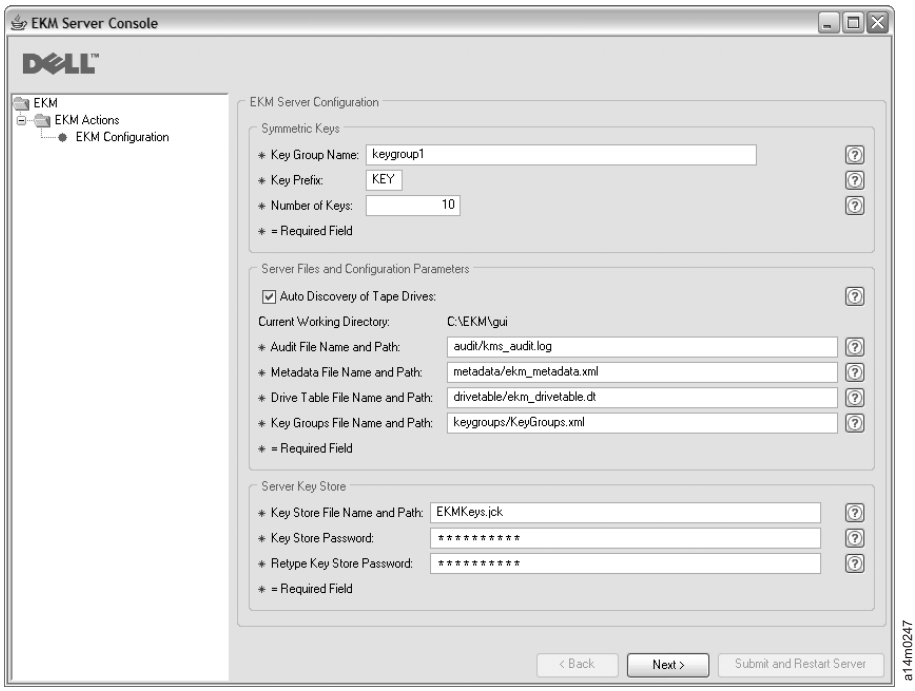

Abbildung 1. Seite "EKM Server Configuration"

Anmerkungen:

a. Der EKM-Server muss über die grafische Benutzerschnittstelle aktualisiert werden, nachdem Laufwerke über die automatische Erkennung hinzugefügt wurden, um sicherzustellen, dass die Laufwerke in der Laufwerktabelle gespeichert werden.

b. Sobald Sie das Keystore-Kennwort festgelegt haben, darf es **nicht mehr geändert werden**, es sei denn, es bietet nicht mehr die nötige Sicherheit. Um Sicherheitsrisiken zu vermeiden, werden die Kennwörter verdeckt angezeigt. Wenn Sie das Keystore-Kennwort ändern, müssen Sie das Kennwort für jeden Schlüssel in diesem Keystore durch Eingabe des Befehls **keytool** einzeln ändern. Siehe hierzu den Abschnitt „Ändern von Keystore-Kennwörtern" im Handbuch *Dell Encryption Key Manager Benutzerhandbuch*.

3. Geben Sie auf der Seite **EKM Server Certificate Configuration** (Abb. 2) den Aliasnamen des Keystores ein, und machen Sie in allen zusätzlichen Feldern Angaben, mit denen das Zertifikat und dessen Zweck identifiziert werden kann. Klicken Sie auf **Submit and Start Server**.

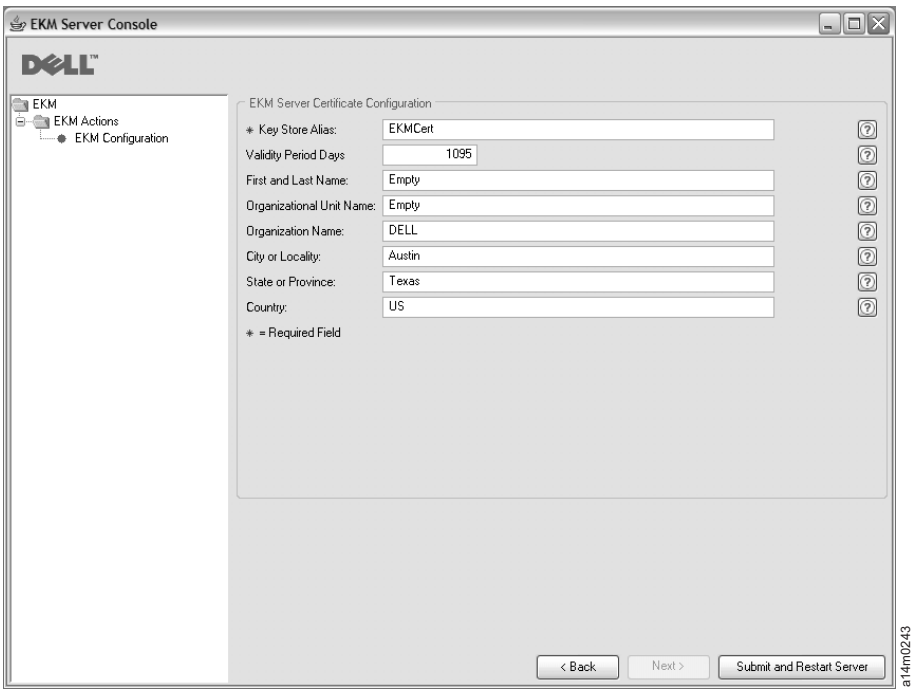

Abbildung 2. Seite "EKM Server Certificate Configuration"

Anmerkung: Wenn die grafische Benutzerschnittstelle des Encryption Key Manager bei der Schlüsselerstellung unterbrochen wird, muss Encryption Key Manager erneut installiert werden.

Die Keystore-Datei wird beschädigt, wenn Sie den Prozess zur Schlüsselerstellung von Encryption Key Manager vor dessen Abschluss stoppen. Führen Sie die nachfolgend aufgeführten Schritte aus, um dieses Problem zu lösen:

- Wenn Encryption Key Manager während der Erstinstallation unterbrochen wurde, wechseln Sie auf das Laufwerk, auf dem sich das zugehörige Verzeichnis befindet (z. B. x:\ekm). Löschen Sie das Verzeichnis, und starten Sie den Installationsvorgang erneut.
- Wenn Encryption Key Manager beim Hinzufügen einer neuen Schlüsselgruppe unterbrochen wurde, stoppen Sie den EKM-Server, und stellen Sie die Keystore-Datei mit Hilfe der neuesten Sicherungsversion des Keystores wieder her (diese Datei befindet sich im Verzeichnis x:\ekm\gui\backupfiles folder). Beachten Sie, dass im Namen der Sicherungsdatei eine Datums- und eine Zeitmarke enthalten sind (z. B. 2007_11_19_16_38_31_EKMKeys.jck). Die Datums- und Zeitmarke muss aus dem Namen entfernt werden, nachdem die Datei in das Verzeichnis x:\ekm\gui kopiert wurde. Starten Sie anschließend den EKM-Server erneut, und fügen Sie die Schlüsselgruppe hinzu, bei der dieser Vorgang zuvor unterbrochen wurde.

4. Über ein Fenster zum Durchführen von Sicherungen (Abb. 3) werden Sie daran erinnert, dass Sie EKM-Datendateien sichern müssen. Geben Sie den Pfad ein, in dem die Sicherungsdaten gespeichert werden sollen. Klicken Sie auf **Backup**.

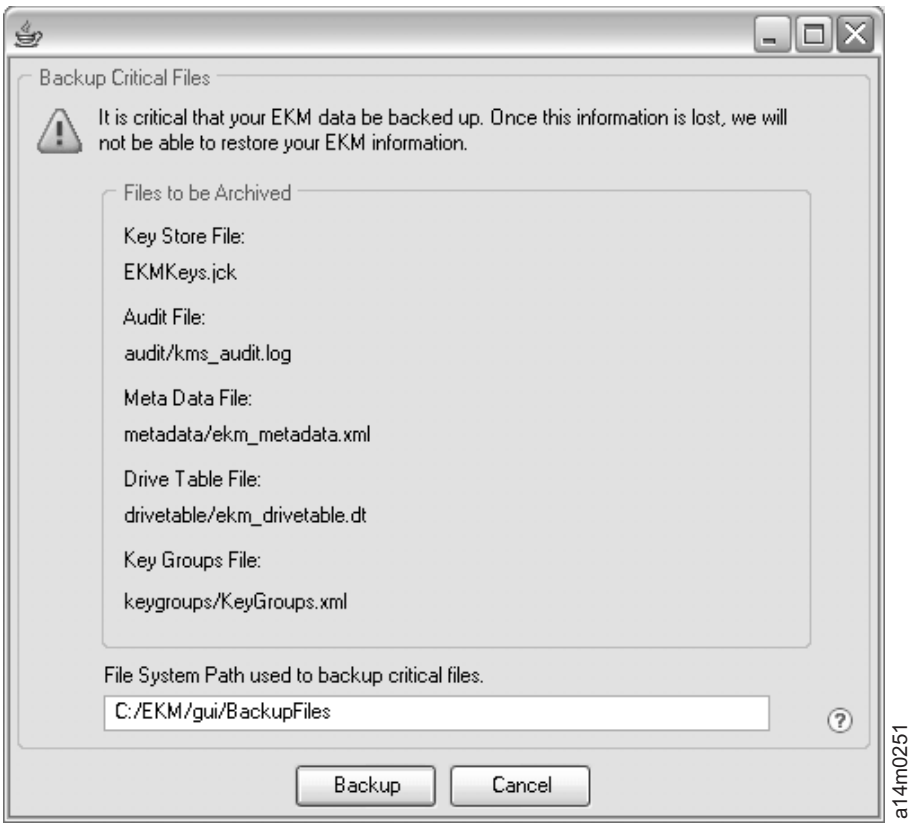

Abbildung 3. Fenster "Backup Critical Files"

5. Daraufhin wird die Seite **User Login** angezeigt. Geben Sie den Standardbenutzernamen EKMAdmin und das Standardkennwort changeME ein. Klicken Sie dann auf **Login**.

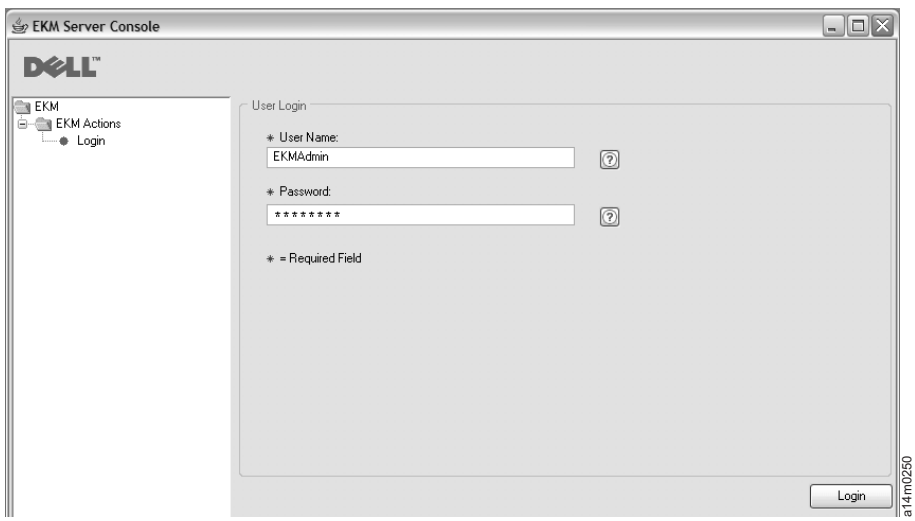

Abbildung 4. Seite "User Login"

Der EKM-Server (Encryption Key Manager) wird im Hintergrund gestartet.

6. Wählen Sie **Server Health Monitor** in der GUI-Navigation aus, um zu prüfen, ob der EKM-Server einsatzbereit ist.

Ermitteln der richtigen Host-IP-Adresse

Einschränkungen in der aktuellen grafischen Benutzerschnittstelle von Encryption Key Manager können dazu führen, dass die Host-IP-Adresse von Encryption Key Manager nicht in der Anzeige "Server Health Monitor" angezeigt wird:

- Wenn der Host unter Verwendung einer IPv6-Adresse konfiguriert wurde, kann die IP-Adresse nicht über Encryption Key Manager angezeigt werden.
- Wenn Encryption Key Manager auf einem Linux-System installiert wurde, zeigt die Anwendung die Adresse des lokalen Hosts an und nicht den tatsächlich aktiven IP-Port.

a. Ermitteln Sie die IP-Portadresse über die Netzwerkkonfiguration, um die tatsächliche IP-Adresse des Hostsystems abzufragen.
   - Rufen Sie auf einem Windows-System ein Befehlsfenster auf, und geben Sie `ipconfig` ein.
   - Geben Sie unter Linux `isconfig` ein.

Identifizieren des EKM SSL-Ports

a. Starten Sie den EKM-Server über eine Befehlszeile.
   - Wechseln Sie unter Windows in das Verzeichnis `c:\ekm`, und klicken Sie auf **startServer.bat**.
   - Wechseln Sie auf Linux-Plattformen in das Verzeichnis `/var/ekm`, und geben Sie `startServer.sh` ein.
   - Weitere Informationen hierzu finden Sie im Abschnitt „Starten, Aktualisieren und Stoppen des EKM-Servers" im Handbuch *Dell Encryption Key Manager Benutzerhandbuch*.

b. Starten Sie den CLI-Client über eine Befehlszeile.
   - Wechseln Sie unter Windows in das Verzeichnis `c:\ekm`, und klicken Sie auf **startClient.bat**.
   - Wechseln Sie auf Linux-Plattformen in das Verzeichnis `/var/ekm`, und geben Sie `startClient.sh` ein.
   - Weitere Informationen hierzu finden Sie im Abschnitt „CLI-Client (Command Line Interface)" im Handbuch *Dell Encryption Key Manager Benutzerhandbuch*.

c. Melden Sie sich mit dem folgenden Befehl bei einem CLI-Client auf dem EKM-Server an:

   `login –ekmuser` *`Benutzer-ID`* `–ekmpassword` ***`Kennwort`***

   Hierbei muss für *Benutzer-ID* EKMAdmin und für *Kennwort* changeME angegeben werden. (Dies ist das Standardkennwort. Wenn Sie das Standardkennwort zuvor geändert haben, geben Sie hier das neue Kennwort ein.)

   Nach der Anmeldung wird die Nachricht `User successfully logged in` angezeigt.

d. Identifizieren Sie den SSL-Port durch Eingabe des folgenden Befehls:

   ```
   status
   ```

   Daraufhin wird eine Nachricht ähnlich der folgenden angezeigt: `server is running. TCP port: 3801, SSL port: 443`.

   Notieren Sie sich den konfigurierten SSL-Port, und stellen Sie sicher, dass dieser Port zur Konfiguration der archiv-verwalteten Verschlüsselungseinstellungen verwendet wurde.

e. Melden Sie sich von der Befehlszeile ab. Geben Sie folgenden Befehl ein:

   ```
   exit
   ```

   Schließen Sie dann das Befehlsfenster.

Methode 2: Konfigurieren von EKM über die Eingabe von Befehlen

Schritt 1. Erstellen eines JCEKS-Keystores

VORSICHT: Es wird dringend empfohlen, regelmäßig eine Sicherungskopie der EKM-Dateien und aller zugehörigen Dateien zu erstellen. Wenn EKM-Verschlüsselungsschlüssel verlorengehen oder beschädigt werden, können die verschlüsselten Daten nicht wiederhergestellt werden.

Erstellen Sie einen Keystore, und nehmen Sie ein Zertifikat und einen privaten Schlüssel auf. Das Zertifikat wird verwendet, um die Kommunikation zwischen EKM-Servern und mit dem EKM CLI-Client (Command Line Interface) sicherzustellen. Mit dem Befehl **keytool** wird ein neuer JCEKS-Keystore mit dem Namen EKMKeys.jck erstellt, und ein Zertifikat und ein privater Schlüssel mit dem Aliasnamen ekmcert werden aufgenommen. Dieses Zertifikat ist fünf Jahre lang gültig. Wenn das Zertifikat abläuft, ist keine Kommunikation zwischen EKM-Servern und zwischen dem EKM CLI-Client und dem EKM-Server mehr möglich. Löschen Sie das abgelaufene Zertifikat, und erstellen Sie ein neues wie in diesem Schritt beschrieben.

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

Wenn Sie den Befehl **keytool** ausführen, werden Sie aufgefordert, Informationen einzugeben, die für die Erstellung eines Zertifikats erforderlich sind, das Ihre EKM-Identifikation ermöglicht. Die Eingabeaufforderungen mit den jeweiligen Beispielantworten sehen ähnlich den folgenden aus:

```
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"):
```

Geben Sie `yes` ein, und drücken Sie die Eingabetaste.

Schritt 2. Erstellen von Verschlüsselungsschlüsseln

Anmerkung: Bevor Sie den Befehl keytool das erste Mal in einer Sitzung verwenden, müssen Sie das Script **updatePath** ausführen, um die richtige Umgebung festzulegen.

Unter Windows
Wechseln Sie in das Verzeichnis `cd c:\ekm`, und klicken Sie auf updatePath.bat.

Auf Linux-Plattformen
Wechseln Sie in das Verzeichnis /var/ekm, und geben Sie `. ./updatePath.sh` ein.
Anmerkung: Geben Sie vor dem Linux-Shellbefehl ". ./" ein (zwei durch ein Leerzeichen getrennte Punkte, gefolgt von einem Schrägstrich), um sicherzustellen, dass die Shell das Script findet.

Für LTO-Verschlüsselungen benötigt Encryption Key Manager eine Reihe symmetrischer Schlüssel, die vorab generiert und in einem Keystore gespeichert werden sollen. Durch Ausführen dieses Befehls **keytool** werden 32 AES-Schlüssel mit 256 Bit erstellt und in dem in Schritt 3 erstellten Keystore gespeichert. Führen Sie diesen Befehl im Verzeichnis EKM aus, damit die Keystore-Datei in diesem Verzeichnis erstellt wird. Die Namen der erstellten Schlüssel lauten key0000000000000000 bis key0000000000000001f.

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

Wenn Sie diesen Befehl ausführen, werden Sie aufgefordert, ein Keystore-Kennwort einzugeben, damit Sie auf den Keystore zugreifen können. Geben Sie das gewünschte Kennwort ein, und drücken Sie die Eingabetaste. Wenn Sie aufgefordert werden, ein Schlüsselkennwort einzugeben, drücken Sie erneut die Eingabetaste, da dies nicht erforderlich ist. Geben Sie kein neues oder anderes Kennwort ein.

Das Schlüsselkennwort entspricht damit dem Keystore-Kennwort. Notieren Sie sich das eben eingegebene Keystore-Kennwort, da es später beim Starten von Encryption Key Manager benötigt wird.

Anmerkung: Sobald Sie das Keystore-Kennwort festgelegt haben, darf es nicht mehr geändert werden, es sei denn, es bietet nicht mehr die nötige Sicherheit. Wenn Sie das Keystore-Kennwort ändern, müssen auch alle Kennworteigenschaften in der Konfigurationsdatei geändert werden. Um Sicherheitsrisiken zu vermeiden, werden die Kennwörter verdeckt angezeigt.

Schritt 3. Starten des EKM-Servers

Starten Sie das Script **startServer**, um den EKM-Server ohne die grafische Benutzerschnittstelle zu starten:

Unter Windows
Wechseln Sie in das Verzeichnis `c:\ekm\ekmserver`, und klicken Sie auf die Datei startServer.bat.

Auf Linux-Plattformen
Wechseln Sie in das Verzeichnis /var/ekm/ekmserver, und geben Sie `. ./startServer.sh` ein.
Anmerkung: Geben Sie vor dem Linux-Shellbefehl ". ./" ein (zwei durch ein Leerzeichen getrennte Punkte, gefolgt von einem Schrägstrich), um sicherzustellen, dass die Shell das Script findet.

VORSICHT: Es wird dringend empfohlen, regelmäßig eine Sicherungskopie der EKM-Dateien und aller zugehörigen Dateien zu erstellen. Wenn EKM-Verschlüsselungsschlüssel verlorengehen oder beschädigt werden, können die verschlüsselten Daten nicht wiederhergestellt werden.

Schritt 4. Starten des EKM CLI-Clients

Wenn Sie den EKM CLI-Client starten möchten, müssen Sie zunächst das Script **startClient** starten:

Unter Windows
Wechseln Sie in das Verzeichnis `c:\ekm\ekmclient`, und klicken Sie auf startClient.bat.

Auf Linux-Plattformen
Wechseln Sie in das Verzeichnis /var/ekm\ekmclient, und geben Sie `. ./startClient.sh` ein.
Anmerkung: Geben Sie vor dem Linux-Shellbefehl ". ./" ein (zwei durch ein Leerzeichen getrennte Punkte, gefolgt von einem Schrägstrich), um sicherzustellen, dass die Shell das Script findet.

Sobald der CLI-Client erfolgreich am EKM-Server angemeldet wurde, können Sie alle CLI-Befehle ausführen. Nach Abschluss des Vorgangs können Sie den CLI-Client mit dem Befehl quit herunterfahren. Wenn der Client 10 Minuten lang nicht verwendet wurde, wird er automatisch heruntergefahren. Informationen zu CLI-Befehlen finden Sie im Handbuch *Dell Encryption Key Manager Benutzerhandbuch* unter **http://support.dell.com** oder auf dem im Lieferumfang des Produkts enthaltenen Datenträger mit Encryption Key Manager von Dell.

Weitere Informationen

Weitere Informationen finden Sie in den folgenden Veröffentlichungen:

- Im *Dell Encryption Key Manager Benutzerhandbuch* (auf der CD mit Encryption Key Manager von Dell enthalten und verfügbar unter **http://support.dell.com**)
- Im White Paper *Library Managed Encryption for Tape* mit Hinweisen zu bewährten Verfahren für die Verschlüsselung von LTO-Bandlaufwerken (verfügbar unter **http://www.dell.com**)