Dell™ PowerVault™ Encryption Key Manager

Краткое руководство пользователя LTO Ultrium 4 и LTO Ultrium 5

Данное руководство знакомит с ***основной конфигурацией***, необходимой для шифрования на накопителях на магнитной ленте LTO Gen 4 и LTO Gen 5. Загрузите с Web-сайта **http://support.dell.com** последние версии встроенного ПО библиотеки и накопителя перед установкой и настройкой Dell PowerVault Encryption Key Manager, чтобы исключить возможные проблемы.

Dell PowerVault Encryption Key Manager (диспетчер ключей шифрования, EKM) - это программа на основе Java™, которая обеспечивает создание, защиту, хранение и обслуживание ключей шифрования для накопителей на магнитной ленте с возможностью шифрования. Эти ключи используются для шифрования информации, записываемой на ленточные носители LTO, и расшифровки информации, считываемой с таких носителей. Encryption Key Manager работает в операционных системах Linux® и Windows® и предназначен для совместного использования в различных офисах и подразделениях в рамках организации.

В данном документе объясняется, как установить и настроить программу Encryption Key Manager с помощью графического пользовательского интерфейса (GUI) или команд. В нем содержится информация об использовании JCEKS - самого простого из поддерживаемых типов переносимых хранилищ ключей. Чтобы получить дополнительные сведения о конкретной процедуре или другом поддерживаемом типе хранилищ ключей, см. *"Руководство пользователя Dell Encryption Key Manager"*, которое можно найти на Web-сайте **http://support.dell.com** или на диске Dell Encryption Key Manager, прилагающемся к продукту.

Примечание: ВАЖНАЯ ИНФОРМАЦИЯ ПО КОНФИГУРАЦИИ ХОСТ-СЕРВЕРА Encryption Key Manager: Для минимизации риска потери данных на компьютерах с установленными программами Dell Encryption Key Manager рекомендуется использовать память ECC. Encryption Key Manager формирует запросы на генерацию ключей шифрования и их передачу накопителям на магнитной ленте LTO-4 и LTO-5. Encryption Key Manager при обработке ключа хранит его данные в системной памяти в свернутом (зашифрованном) виде. Следует заметить, что данные ключа необходимо передать соответствующему накопителю на магнитной ленте без ошибок, чтобы записанные на кассету данные можно было восстановить (расшифровать). Если по какой-либо причине данные ключа были повреждены из-за ошибок в разрядах системной памяти, но использовались для записи данных на кассету, то записанные на эту кассету данные будут недоступны для восстановления (последующей расшифровки). Существуют различные средства защиты, предотвращающие появление подобных ошибок данных. Однако если компьютер, на котором установлено приложение Encryption Key Manager, не использует память с коррекцией ошибок Error Correction Code (ECC), существует вероятность повреждения хранимых в памяти данных и, в результате, их потери. Вероятность появления таких ошибок достаточно мала, однако на компьютерах, на которых установлены критически важные приложения (например, Encryption Key Manager) всегда рекомендуется использовать память ECC.

Первоначальный этап: установка ПО Encryption Key Manager

1. Вставьте компакт-диск Dell Encryption Key Manager. Если установка в Windows не начинается автоматически, найдите на компакт-диске файл Install_Windows.bat и дважды щелкните по нему.

   В системе Linux установка не начинается автоматически. Перейдите в корневой каталог компакт-диска и запустите файл `Install_Linux.sh`.

   На экране появится лицензия конечного пользователя. Для продолжения установки вам понадобится принять положения этой лицензии.

При установке все содержимое (документация, файлы GUI-интерфейса, файлы свойств конфигурации), соответствующее операционной системе, копируется с компакт-диска на жесткий диск компьютера. Во время установки система проверяется на наличие правильной среды IBM Java Runtime Environment. Если эта среда не обнаружена, она автоматически устанавливается.

По окончании установки запускается графический пользовательский интерфейс (GUI).

Способ 1: Настройка Encryption Key Manager с помощью интерфейса пользователя

Данная процедура позволяет создать основную конфигурацию. После ее успешного выполнения запускается сервер Encryption Key Manager.

1. Если интерфейс не запускается, откройте его следующим образом.

   В операционной системе Windows
   перейдите в каталог c:\ekm\gui и выберите файл `LaunchEKMGui.bat`

   На платформах Linux
   перейдите в каталог /var/ekm/gui и запустите файл `. ./LaunchEKMGui.sh`
   Примечание: Укажите в командной строке оболочки Linux . ./ (точка, пробел, точка, прямая косая черта) перед именем файла, для того чтобы оболочка гарантированно обнаружила сценарий.

2. На странице EKM Server Configuration (Настройка сервера EKM) (рис. 1) введите данные во все обязательные поля (отмечены "звездочкой" (*)). Для получения описания какого-либо поля щелкните по знаку вопроса справа от него. Нажмите кнопку **Next** (Далее), чтобы перейти на страницу EKM Server Certificate Configuration (Настройка сертификата сервера EKM).

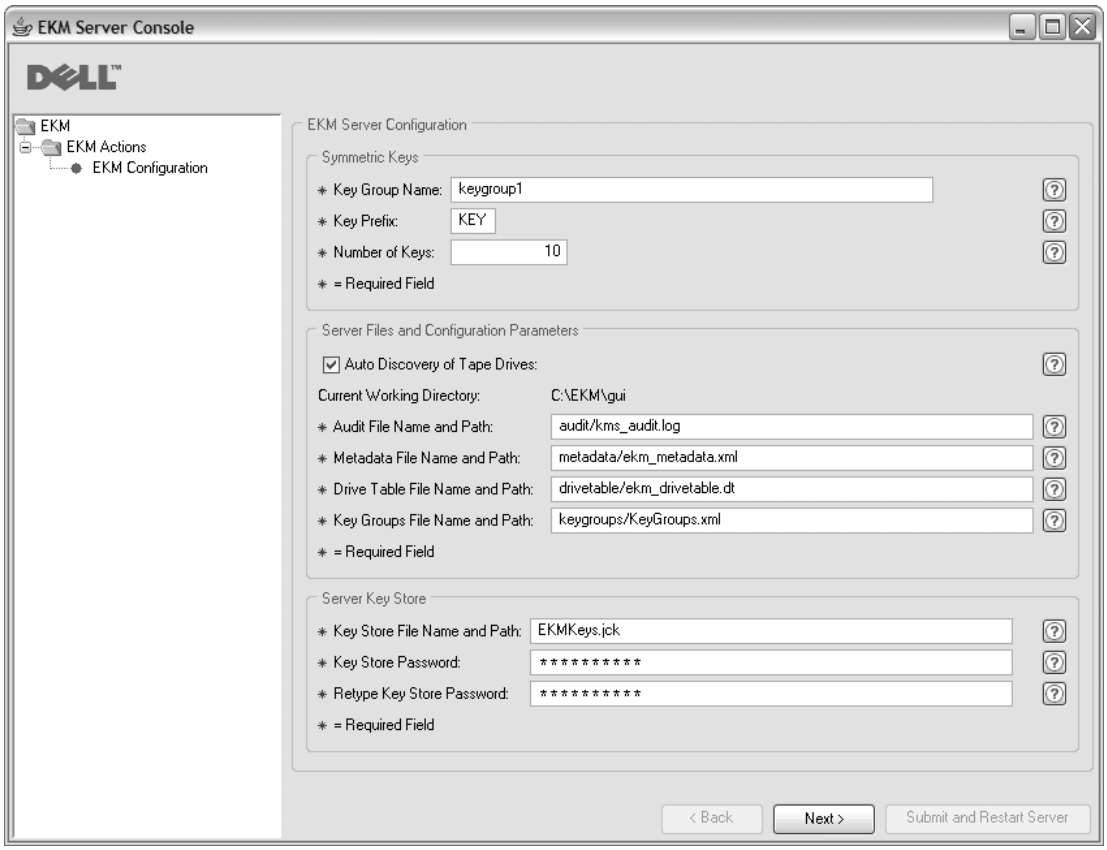

Рисунок 1. Страница EKM Server Configuration (Настройка сервера EKM)

Примечания:

a. После автоматического обнаружения и добавления накопителей сервер Encryption Key Manager необходимо обновить с помощью GUI-интерфейса, чтобы убедиться в том, что они сохранены в таблице накопителей.

b. Задав пароль хранилища ключей, **меняйте его только в том случае**, если нарушена безопасность пароля. Для предотвращения потенциального нарушения безопасности пароли скрываются. Чтобы изменить пароль хранилища ключей, необходимо изменить пароль каждого ключа в этом хранилище

отдельно с помощью команды **keytool**. См. раздел “Изменение паролей хранилищ ключей” в *Руководстве пользователя Dell Encryption Key Manager*.

3. На странице EKM Server Certificate Configuration (Настройка сертификата сервера EKM) (рис. 2) введите псевдоним хранилища ключей, а также заполните дополнительные поля, которые позволят идентифицировать сертификат и его назначение. Щелкните по **Submit and Start Server** (Применить и запустить сервер).

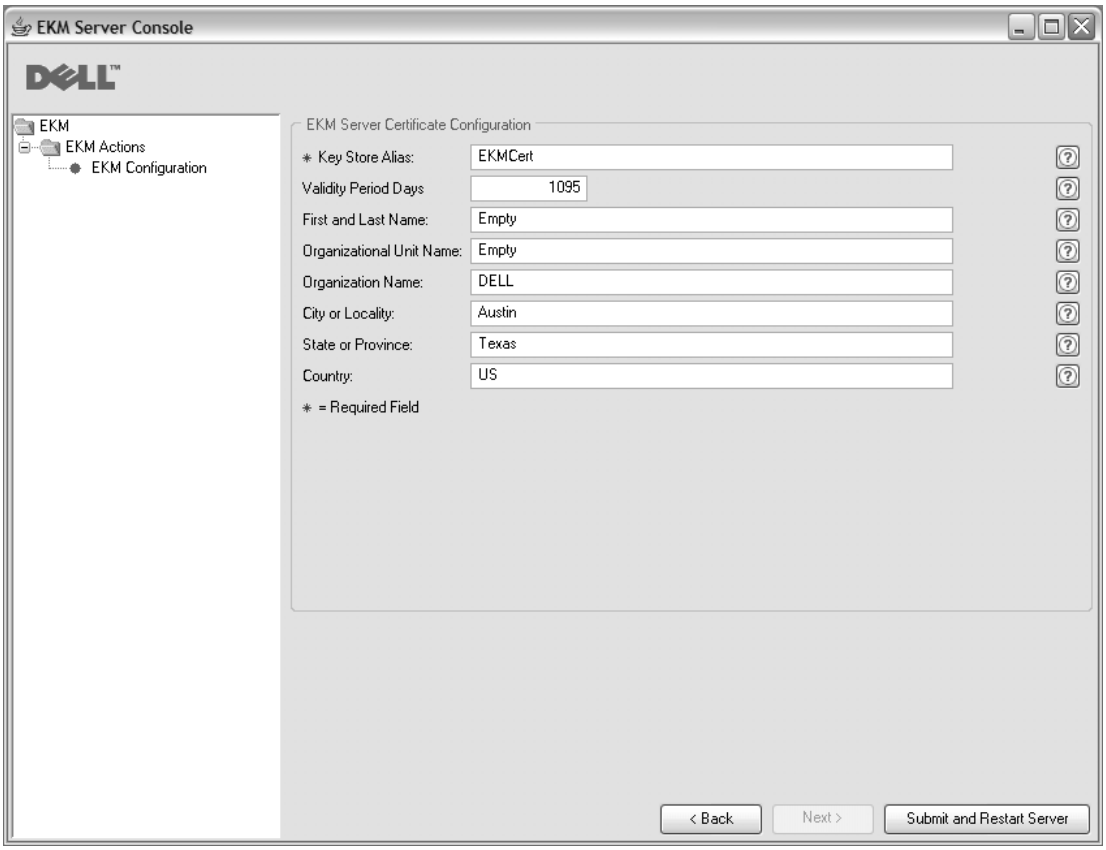

Рисунок 2. Страница EKM Server Certificate Configuration (Настройка сертификата сервера EKM)

Примечание: Если во время создания ключа работа интерфейса Encryption Key Manager будет прервана, то потребуется переустановка Encryption Key Manager.

Если процесс генерации ключа приложением Encryption Key Manager остановлен до его завершения, файл хранилища ключей будет поврежден. Для восстановления в этом случае выполните следующие действия:

- Если была прервана первоначальная установка Encryption Key Manager, перейдите в каталог, куда производилась установка (например x:\ekm). Удалите каталог и повторно запустите установку.
- Если работа Encryption Key Manager была прервана во время добавления новой группы ключей, остановите сервер Encryption Key Manager, восстановите файл хранилища ключей при помощи последней резервной копии хранилища ключей (этот файл находится в папке x:\ekm\gui\backupfiles). Следует учесть, что имя файла резервной копии содержит метку даты и времени его создания (например, 2007_11_19_16_38_31_EKMKeys.jck). После копирования файла в каталог x:\ekm\gui метку даты и времени из имени файла необходимо удалить. Перезапустите сервер Encryption Key Manager и повторите ранее прерванный процесс добавления группы ключей.

4. На экране появится окно резервного копирования (рис. 3), напоминающее о необходимости резервного копирования файлов данных Encryption Key Manager. Введите путь к каталогу, где следует сохранить резервные копии данных. Щелкните по **Backup** (Создать резервную копию).

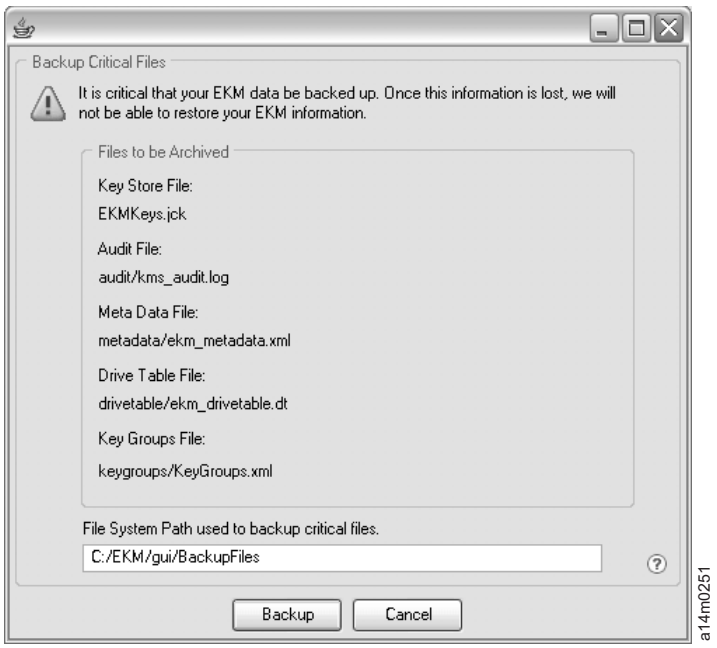

Рисунок 3. Окно Backup Critical Files (Создание резервных копий важных файлов)

5. Появится страница User Login (Вход пользователя). Введите ID пользователя по умолчанию (EKMAdmin) и пароль по умолчанию (changeME). Щелкните по **Login** (Вход).
   Сервер Dell Encryption Key Manager запускается в фоновом режиме.

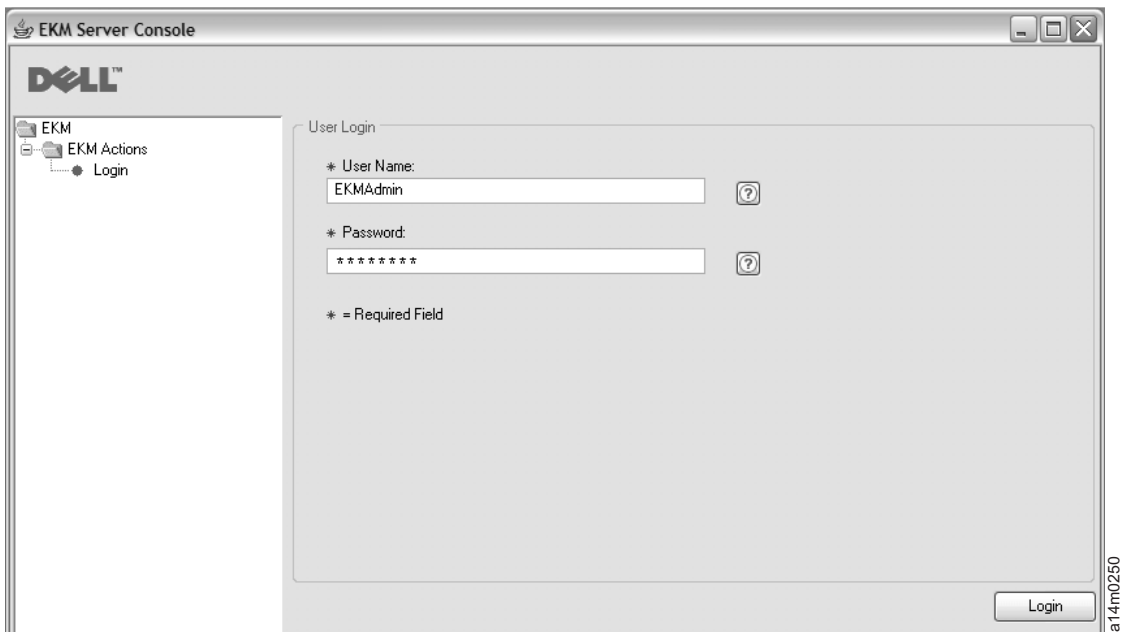

Рисунок 4. Страница User Login (Вход пользователя)

6. Выберите **Server Health Monitor** (Монитор работоспособности сервера) в навигаторе интерфейса и убедитесь, что сервер Encryption Key Manager работает.

Как определить правильный IP-адрес хоста

Ограничения текущего графического пользовательского интерфейса Encryption Key Manager могут не позволить отобразить IP-адрес хоста в мониторе работоспособности сервера:

- Если хост настроен на IPV6-адреса, приложение Encryption Key Manager не сможет отобразить IP-адрес.
- Если приложение Encryption Key Manager установлено в системе Linux, оно отображает адрес localhost, а не фактический активный порт IP.

a. Чтобы получить фактический IP-адрес системы хоста, определите адрес порта IP при помощи конфигурации сети.
   - В ОС Windows откройте командное окно и введите `ipconfig`.
   - В Linux введите `isconfig`.

Как идентифицировать порт SSL в EKM

a. Запустите сервер Encryption Key Manager при помощи командной строки.
   - В Windows перейдите в каталог `c:\ekm` и запустите файл **startServer.bat**
   - На платформах Linux перейдите в каталог `/var/ekm` и введите `startServer.sh`
   - Для более детальной информации см. раздел “Запуск, обновление и остановка сервера диспетчера ключей” в *Руководстве пользователя Dell Encryption Key Manager*.

b. Запустите CLI-клиент из командной строки.
   - В Windows перейдите в каталог `c:\ekm` и запустите файл **startClient.bat**
   - На платформах Linux перейдите в каталог `/var/ekm` и введите `startClient.sh`
   - Для более детальной информации см. раздел “Запуск клиента интерфейса командной строки” *Руководства пользователя Dell Encryption Key Manager*.

c. Войдите в систему клиента CLI на сервере Encryption Key Manager при помощи следующей команды:

   `login -ekmuser` *`ID_пользователя`* `-ekmpassword` ***`пароль`***

   где ID_пользователя = EKMAdmin и пароль = changeME (Это пароль по умолчанию. Если вы ранее изменили пароль по умолчанию, используйте свой новый пароль.)

   После успешного входа в систему отображается сообщение `User successfully logged in (Пользователь успешно вошел в систему)`.

d. Идентифицируйте порт SSL, выполнив следующую команду:

   `status`

   Отображаемый результат должен быть подобен следующему: `server is running. TCP port: 3801, SSL port: 443`.

   Запомните номер порта, настроенного на протокол SSL, и убедитесь, что именно этот порт использован для настройки ваших параметров шифрования, управляемого библиотекой.

e. Выйдите из системы при помощи командной строки. Введите следующую команду:

   `exit`

   Закройте командное окно.

Способ 2: Настройка Encryption Key Manager с помощью команд

Шаг 1. Создание хранилища ключей JCEKS

ВНИМАНИЕ: настоятельно рекомендуется регулярно создавать копии Encryption Key Manager и всех связанных файлов. В случае потери или повреждения ключей шифрования Encryption Key Manager восстановить зашифрованные данные будет невозможно.

Создайте хранилище ключей и поместите в него сертификат и секретный ключ. Сертификат необходим для защиты взаимодействия между серверами Encryption Key Manager и информационного обмена с клиентом интерфейса командной строки (CLI) Encryption Key Manager. Команда **keytool** создает новое хранилище

ключей JCEKS под названием EKMKeys.jck и помещает в него сертификат и секретный ключ с псевдонимом ekmcert. Данный сертификат действует в течение 5 лет. По истечении срока действия сертификата взаимодействие между серверами Encryption Key Manager, а также между CLI-клиентом Encryption Key Manager и сервером Encryption Key Manager может стать невозможным. Удалите старый сертификат с истекшим сроком действия и создайте новый, как описано в данной процедуре.

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

Команда keytool запрашивает информацию, необходимую для создания сертификата, который обеспечивает идентификацию пользователя Encryption Key Manager. Далее приведены подобные запросы с примерами ответов.

```
Ваши имя и фамилия? [Нет данных]: ekmcert
Название вашего подразделения? [Нет данных]: EKM
Название вашей организации? [Нет данных]: Dell
Название вашего города или района? [Нет данных]: Austin
Название вашего штата или провинции? [Нет данных]: TX
Двухбуквенный код страны для этой единицы? [Нет данных]: US
Правильно ли введены данные: CN=ekmcert, OU=EKM, O=Dell, L=Austin, ST=TX, C=US?
   (введите yes (да) или no (нет)):
```

Введите `yes` (да) и нажмите клавишу Enter.

Шаг 2. Создание ключей шифрования

Примечание: Перед тем как применить команду keytool в первый раз во время сеанса, запустите сценарий **updatePath** для настройки правильной среды.

В операционной системе Windows
перейдите в каталог `cd c:\ekm` и выберите файл updatePath.bat

На платформах Linux
перейдите в каталог /var/ekm и запустите файл `. ./updatePath.sh`
Примечание: Укажите в командной строке оболочки Linux . ./ (точка, пробел, точка, прямая косая черта) перед именем файла, для того чтобы оболочка гарантированно обнаружила сценарий.

Для шифрования LTO с помощью Encryption Key Manager необходимо заранее создать несколько симметричных ключей и сохранить их в хранилище ключей. Команда **keytool** генерирует 32 256-разрядных ключа AES и сохраняет их в хранилище, созданном на шаге 1. Запустите эту команду из каталога Encryption Key Manager, чтобы создать в нем файл хранилища ключей. Имена полученных ключей будут иметь вид от key0000000000000000 до key000000000000001f.

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

Эта команда запрашивает пароль хранилища ключей для доступа к хранилищу. Введите необходимый пароль и нажмите клавишу Enter. При запросе пароля ключа снова нажмите клавишу Enter, так как эта информация не требуется. Не вводите новый или измененный пароль. Это приведет к тому, что пароль ключа будет совпадать с паролем хранилища ключей. Запишите введенный пароль хранилища ключей, поскольку он понадобится в дальнейшем при запуске Encryption Key Manager.

Примечание: Задав пароль хранилища ключей, меняйте его только в том случае, если нарушена безопасность пароля. При изменении пароля хранилища ключей необходимо также изменить все свойства пароля в файле конфигурации. Для предотвращения потенциального нарушения безопасности пароли скрываются.

Шаг 3. Запуск сервера Encryption Key Manager

Чтобы запустить сервер Encryption Key Manager без использования графического интерфейса, запустите сценарий startServer:

В операционной системе Windows
перейдите в каталог `c:\ekm\ekmserver` и запустите файл startServer.bat

На платформах Linux
перейдите в каталог /var/ekm/ekmserver и запустите файл `. ./startServer.sh`
Примечание: Укажите в командной строке оболочки Linux . ./ (точка, пробел, точка, прямая косая черта) перед именем файла, для того чтобы оболочка гарантированно обнаружила сценарий.

ВНИМАНИЕ: настоятельно рекомендуется регулярно создавать копии Encryption Key Manager и всех связанных файлов. В случае потери или повреждения ключей шифрования Encryption Key Manager восстановить зашифрованные данные будет невозможно.

Шаг 4. Запуск клиента интерфейса командной строки Encryption Key Manager

Для запуска клиента Encryption Key Manager с интерфейсом командной строки (CLI) запустите сценарий startClient:

В операционной системе Windows
перейдите в каталог `c:\ekm\ekmclient` и запустите файл startClient.bat

На платформах Linux
перейдите в каталог /var/ekm\ekmclient и запустите файл `. ./startClient.sh`
Примечание: Укажите в командной строке оболочки Linux . ./ (точка, пробел, точка, прямая косая черта) перед именем файла, для того чтобы оболочка гарантированно обнаружила сценарий.

После успешного входа CLI-клиента на сервер диспетчера ключей можно выполнять любые команды CLI-интерфейса. Используйте команду quit для завершения работы CLI-клиента. Если клиент не используется в течение 10 минут, его работа завершается автоматически. Сведения о командах интерфейса командной строки (CLI) см. в *Руководстве пользователя Dell Encryption Key Manager*, которое можно найти на Web-сайте **http://support.dell.com** или на диске Dell Encryption Key Manager, прилагающемся к продукту.

Дополнительные сведения

Дополнительная информация приведена в следующих публикациях:

- *Руководство пользователя Dell Encryption Key Manager* (имеется на компакт-диске Dell Encryption Key Manager и доступно на Web-сайте **http://support.dell.com**).
- Технический документ *Library Managed Encryption for Tape*, содержащий рекомендации по шифрованию на лентах LTO (доступен на Web-сайте **http://www.dell.com**).