Диспетчер ключей шифрования Dell Encryption Key Manager 3.0

Руководство по внедрению

Примечания, предупреждения и предостережения

ПРИМЕЧАНИЕ: ПРИМЕЧАНИЕ. Содержит важную информацию, которая помогает более эффективно работать с компьютером.

ОСТОРОЖНО: Указывает на риск повреждения оборудования или потери данных в случае несоблюдения инструкций.

ПРЕДУПРЕЖДЕНИЕ: ОСТОРОЖНО! Указывает на потенциальную опасность повреждения оборудования, получения травмы или на угрозу для жизни.

2011 – 12

Rev. A00

Содержание

1

Обзор

Диспетчер ключей шифрования Dell Encryption Key Manager (EKM) 3.0 является утилитой шифрования, которая позволяет защитить сохраненные на ленточных кассетах LTO данные при помощи управления ключами шифрования для автоматизированных решений для лент Dell, в том числе для серии ML и TL PowerVault. EKM 3.0 позволяет управлять жизненным циклом ключей шифрования для лент, в том числе их генерирование, распределение, администрирование и удаление.

В данном руководстве описывается способ установки, настройки и порядок выполнения основных операций в диспетчере ключей шифрования Dell Encryption Key Manager 3.0 (EKM 3.0). Компания Dell рекомендует прочитать данный документ перед установкой EKM 3.0.

В данное руководство включена информация о следующем:

- Требования к аппаратному и программному обеспечению для EKM 3.0
- Установка и удаление EKM 3.0 на операционной системе Windows и системах на базе Linux
- Настройка EKM 3.0
- Основные операции в EKM 3.0
- Миграция EKM 2.X во время установки EKM 3.0 и слияние EKM 2.X с настроенным установленным EKM 3.0
- Часто задаваемые вопросы, информация о поиске и устранении неисправностей, обычные сообщения об ошибке, а также контактная информация службы поддержки

ПРИМЕЧАНИЕ: EKM 3.0 основан на диспетчере жизненного цикла ключей IBM Tivoli Key Lifecycle Manager (TKLM) V2 FixPack 2, но был адаптирован для поддержки инфраструктуры ленточных библиотек Dell при помощи выбора подходящей подгруппы параметров TKLM для ленты.

Для получения сведений об использовании EKM 3.0, которые не были рассмотрены в данном руководстве, см. документацию TKLM, которая включает в себя следующее:

- IBM Tivoli Key Manager 2.0 *Quick Start Guide (Краткое руководство пользователя)*
- IBM Tivoli Key Manager 2.0 *Installation and Configuration Guide (Руководство по установке и настройке)*
- IBM Tivoli Key Manager 2.0 *Product Overview/Scenario Guide (Обзор продукта/Руководство по использованию сценариев)*

Для получения сведений о том, как получить доступ к документации TKLM, см. раздел Documentation and Reference Materials (Документация и справочная информация) файла **ReadThisFirst.txt** на установочном носителе EKM 3.0.

Некоторые экраны и функции, рассмотренные в документации IBM TKLM, не включены в Dell EKM 3.0. EKM 3.0 включает в себя только ту подгруппу функций, которая необходима для реализации поддержки ленточных библиотек Dell PowerVault.

ПРИМЕЧАНИЕ: Для получения информации о рекомендованном способе использования и настройке Dell EKM 3.0 см. раздел Best Practices (Передовой опыт) в файле **ReadThisFirst.txt** на установочном носителе EKM 3.0.

ПРИМЕЧАНИЕ: Для получения самой свежей информации, включая сведения об улучшениях и исправлениях ошибок, см. примечания к выпуску по адресу: **support.dell.com/manuals**. Перейдите в раздел **Software (Программное обеспечение) → Systems Management (Управление системой) → Dell Encryption Key Manager** .

Требования к аппаратному и программному обеспечению

Требования к аппаратному обеспечению сервера

Минимальные требования к аппаратному обеспечению сервера управления ключами (аппаратное обеспечение, на котором EKM 3.0 будет установлен):

- ЦП: 2,3 ГГц
- Память: 4 ГБ с коррекцией ошибок
- Доступное пространство на диске (для установки EKM 3.0 и обычного хранения ключей): 5 ГБ

ПРИМЕЧАНИЕ: Если в системе, на которую вы устанавливаете EKM 3.0, имеется 24 или более ЦП, см. примечания к выпуску EKM 3.0 для получения более подробной информации о способе обновления EKM 3.0 после завершения установки. Для получения доступа к примеяаниям к выпуску EKM 3.0 перейдите по адресу **support.dell.com/manuals**, а затем перейдите в раздел **Software (Программное обеспечение) → Systems Management (Управление системой) → Dell Encryption Key Manager**.

Требования к веб-обозреватели

EKM 3.0 поддерживает следующие веб-обозреватели:

- Microsoft Internet Explorer, версия 7.0
- Microsoft Internet Explorer, версия 8.0, режим совместимости
- Firefox, версия 3.0.x (EKM 3.0 не поддерживает Firefox версии 3.5 и выше).

ПРИМЕЧАНИЕ: Для обеспечения работы функций EKM 3.0 должен быть включен JavaScript. Для получения указаний о том, как включить JavaScript, см. документацию на веб-обозреватель.

Требования к операционной системе

EKM 3.0 поддерживает следующие операционные системы:

- Windows Server 2003 R2 с пакетом исправлений 2, 32-бит и 64-бит, версии Standard и Enterprise
- Windows Server 2008 с пакетом исправлений 2, 32-бит и 64-бит, версии Standard и Enterprise
- Windows Server 2008 R2, версии Standard и Enterprise
- Red Hat Enterprise Linux (RHEL) 4.X, Advanced Server (AS), 32-бит
- Red Hat Enterprise Linux (RHEL) 5.X, 32-бит и 64-бит
- SUSE Linux Enterprise Server (SLES) 10 с пакетом исправлений 4, 64-бит
- SUSE Linux Enterprise Server (SLES) 11 с пакетом исправлений 1, 64-бит

ПРИМЕЧАНИЕ: EKM 3.0 не поддерживает VMware или Microsoft Hyper-V Server.

ПРИМЕЧАНИЕ: Для получения информации о требованиям и ограничениям к настройке конфигурации с основным/дополнительным сервером, см. раздел Setting up Primary and Secondary EKM 3.0 Servers (Настройка основного и дополнительного сервера EKM 3.0).

ПРИМЕЧАНИЕ: EKM 3.0 выполняет обязательные проверки системы перед установкой. Для получения более подробной информации см. раздел System Prerequisite Checks (Необходимые проверки системы).

2

Установка EKM 3.0

В настоящей главе описывается порядок установки EKM 3.0 на операционной системе Windows и на системах на базе Linux.

ПРИМЕЧАНИЕ: Если в настоящее время вы используете EKM 2.X, компания Dell рекомендует провести техническое обслуживание вашей текущей инфраструктуры (серверы, операционные системы, ленточные библиотеки и т.д., в которых используется защита EKM 2.X), в противном случае вы не сможете избежать проблем.

EKM 3.0 не поддерживает использование виртуальных машин в качестве хост-систем. Если в качестве хост-системы для EKM 2.X вы используете виртуальную машину, вы можете продолжить использование EKM 2.X, или перейти к использованию физического сервера.

ПРИМЕЧАНИЕ: Если вы планируете мигрировать вашу систему EKM 2.X в EKM 3.0, то перед началом процедуры установки EKM 3.0 см. раздел Migrating an Encryption Key Manager (EKM) 2.X Version during the EKM 3.0 Installation (Миграция диспетчера ключей шифрования (EKM) версии 2.X в процессе установки EKM 3.0).

ПРИМЕЧАНИЕ: Компания Dell рекомендует устанавливать EKM 3.0 на отдельный физический сервер, который не используется для работы каких-либо других служб. Такой вариант позволит гарантировать, что производительность и время отклика EKM 3.0 не будет ухудшено каким-либо другим приложением, запущенным на том же самом физическом сервере.

ОСТОРОЖНО: EKM 3.0 поддерживает установку только напрямую с носителя EKM 3.0. Не копируйте содержимое носителя EKM 3.0 на жесткий диск.

ПРИМЕЧАНИЕ: Для выполнения описанных в данной главе процедур необходимо наличие знаний уровня системного администратора.

Подготовка к установке EKM 3.0 на операционной системе Microsoft Windows

В данной главе описываются действия, выполняемые перед установкой диспетчера ключей шифрования Dell Encryption Key Manager 3.0 на операционной системе Microsoft Windows.

ПРИМЕЧАНИЕ: Процедура установки занимает примерно 45 минут. Не выключайте систему до завершения процедуры установки.

ПРИМЕЧАНИЕ: Для выполнения установки EKM 3.0 вы должны войти в систему как **Administrator (Администратор)**.

ПРИМЕЧАНИЕ: Если вы не хотите использовать сложный пароль для базы данных, отключите настройку **Password must meet complexity requirements (Пароль должен соответствовать требованиям сложности)** в операционной системе перед установкой в дисковод установочного носителя EKM 3.0.

1. Вставьте установочный носитель EKM 3.0 для операционной системы Microsoft Windows в дисковод системы, на которой вы желаете выполнить установку EKM 3.0.
2. Если ваша система настроена на автоматический запуск DVD-диска после его установки в дисковод, подождите некоторое время до появления установщика. Если автоматический запуск на вашей системе не настроен, перейдите к DVD-дисководу и дважды нажмите на DVD-дисковод или файл **install.exe** в корневом каталоге DVD-диска.

   Отобразится экран приветствия **Welcome** мастера установки EKM 3.0.

ПРИМЕЧАНИЕ: Если вы хотите установить EKM 3.0 по сети, не используйте путь доступа формата: \\<*ip_адрес*>*общая_папка_EKM_3.0*. Вместо него укажите сетевой путь к дисководу. В проводнике Windows Explorer воспользуйтесь **Tools (Инструменты)** → **Map Network Drive (Добавить сетевой диск)** для того, чтобы ввести установочный путь доступа <*буква_сетевого_диска*>:\<*носитель_EKM_3.0*>.

Для продолжения перейдите к разделу Performing the EKM 3.0 Installation Procedure (Выполнение процедуры установки EKM 3.0).

Подготовка к установке EKM 3.0 на операционной системе Red Hat Enterprise Linux

В данной главе описываются действия, которые необходимо выполнить перед установкой диспетчера ключей шифрования Dell Encryption Key Manager 3.0 на операционной системе Red Hat Enterprise Linux.

ПРИМЕЧАНИЕ: Процедура установки занимает примерно 45 минут. Не выключайте систему до завершения процедуры установки.

Для подготовки системы к установке EKM 3.0 выполните следующие действия:

1. Вставьте соответствующий вашей операционной системе установочный диска EKM 3.0 в дисковод компьютера, на котором необходимо выполните установку EKM 3.0.
2. Если ваша система настроена на автоматический запуск DVD-диска после его установки в дисковод, дождитесь момента, когда на экране отобразится установщик. Если на вашей системе автоматический запуск не настроен, откройте окно терминала с привилегированными правами и перейдите в папку, в которой смонтирован DVD-диск EKM 3.0. Введите команду **./autorun.sh** и нажмите на кнопку **Enter (Ввод)**.

ПРИМЕЧАНИЕ: Если SELinux установлено и включено, перед началом установки отключите его. См. раздел System Prerequisite Checks (Необходимые проверки системы).

ПРИМЕЧАНИЕ: В операционных системах Red Hat часть имеется набор битов **noexec** для отключения выполнения любых двоичных файлов на смонтированных файловых системах. Если бит **noexec** на смонтированном диске DVD ROM имеет параметр **disable (отключить)**, то установщик EKM 3.0 с DVD-диска не будет запущен. Для запуска установщика EKM 3.0 с DVD-диска выполните следующие действия:

   a) Запустите сеанс терминала с привилегированными правами.
   b) Демонтируйте DVD-диск EKM 3.0.
   c) Повторно смонтируйте DVD-диск EKM 3.0 в режиме **read-only (только для чтения)** с отключенным набором битов **noexec** при помощи ввода следующих команд:

      ```
      mkdir /media/dellmedia mount /dev/<EKM 3.0 device><space>/media/dellmedia
      cd /media/dellmedia
      ```

   d) Для выполнения установочной программы введите команду **./autorun.sh** и нажмите на кнопку **Enter (Ввод)**.

   Отобразится экран приветствия **Welcome** мастера установки EKM 3.0.

Для продолжения перейдите к разделу Performing the EKM 3.0 Installation Procedure (Выполнение процедуры установки EKM 3.0).

Подготовка к установке EKM 3.0 на операционной системе SUSE Linux Enterprise Server

В данной главе описываются действия, которые необходимо выполнить перед установкой диспетчера ключей шифрования Dell Encryption Key Manager 3.0 на операционной системе SUSE Linux Enterprise Server (SLES).

ПРИМЕЧАНИЕ: Процедура установки занимает примерно 45 минут. Не выключайте систему до завершения процедуры установки.

Для подготовки системы к установке EKM 3.0 выполните следующие действия:

1. Вставьте соответствующий вашей операционной системе установочный диска EKM 3.0 в дисковод компьютера, на котором необходимо выполните установку EKM 3.0.
2. Если ваша система настроена на автоматический запуск DVD-диска после его установки в дисковод, дождитесь момента, когда на экране отобразится установщик. Если на вашей системе автоматический запуск не настроен, откройте окно терминала с привилегированными правами и перейдите в папку, в которой смонтирован DVD-диск EKM 3.0. Введите команду **./autorun.sh** и нажмите на кнопку **Enter (Ввод)**.

   Отобразится экран приветствия **Welcome** мастера установки EKM 3.0.

ПРИМЕЧАНИЕ: Если SELinux установлено и включено, перед началом установки отключите его.

3. Откройте порт 50000. Для чего выполните следующие действия:
   a) Перейдите к **Computer (Компьютер)** → **Places (Места)** → **File System (Файловая система)** .
   b) Дважды нажмите на кнопку **etc (Другое)**.
   c) Дважды нажмите на кнопку **Services (Службы)**.
   d) В файле **Services (Службы)** измените строку **50000/tcp** и **50000/udp** на **50100/tcp** и **50100/udp**.
   e) Нажмите на кнопку **Save (Сохранить)**.

Для продолжения перейдите к разделу Performing the EKM 3.0 Installation Procedure (Выполнение процедуры установки EKM 3.0).

Выполнение процедуры установки EKM 3.0

В настоящей главе описывается порядок установки EKM 3.0.

ПРИМЕЧАНИЕ: процедура установки занимает примерно 45 минут. Не выключайте систему до завершения процедуры установки.

ПРИМЕЧАНИЕ: Если EKM 3.0 устанавливается на сервере, который будет использоваться в качестве дополнительного сервера EKM 3.0, то необходимо использовать те же пароли, которые использовались при установке EKM 3.0 на основной сервер.

1. На экране приветствия **Welcome** мастера установки EKM 3.0 нажмите на кнопку **Next (Далее)**.

   Отобразится экран **License Agreement (Лицензионное соглашение)**.
2. Нажмите на переключатель для принятия условий лицензионного соглашения.
3. Нажмите на кнопку **Next (Далее)**.

ПРИМЕЧАНИЕ: Установщик EKM 3.0 выполняет необходимые проверки системы. Установщик проверяет, что система соответствует минимальным требованиям и настраивает EKM 3.0 для вашей системы.

В случае отображения сообщения об ошибке, см раздел System Prerequisite Checks (Необходимые проверки системы).

Отображается экран **Reuse Installation Profile (Повторно использовать профиль установки)**.

4. *Если вы устанавливаете EKM 3.0 впервые*, оставьте пустым флажок **Reuse an EKM 3.0 installation profile (Повторно использовать профиль установки EKM 3.0)**.

   Если вы выполняете повторную установку EKM 3.0 или устанавливаете EKM 3.0 на дополнительный сервер и желаете использовать сохраненный после предыдущей установки профиль, выполните следующие действия:

   a) Установите флажок **Reuse an EKM 3.0 installation profile (Повторно использовать профиль установки EKM 3.0)**. После установки данного флажка становится активным поле **File Location (Местонахождение файла)**.

   b) Нажмите на кнопку **Choose (Выбрать)** и перейдите к профилю установки, который был ранее создан в процессе настройки и установки EKM 3.0 (например, **E:\EKM_config.txt** для операционной системы Windows, или **/tmp/ekm_config** в системах а базе Linux).

      Для переноса профиля установки из места его хранения можно использовать съемный диск или сетевую общую папку.

ПРИМЕЧАНИЕ: В графическом пользовательском интерфейсе установки профиль установки во все поля, за исключением полей для ввода паролей, заносит всю информацию, которая была использована во время предыдущей установки. В случае использования профиля установки необходимо повторно ввести все пароли.

ПРИМЕЧАНИЕ: Если выполняется установка EKM 3.0 на дополнительный сервер, следует повторно использовать профиль установки основного сервера EKM 3.0 для того, чтобы гарантировать совпадение всех вводимых параметров.

5. Нажмите на кнопку **Next (Далее)**.

   Откроется экран **Database (База данных)**. В данном экране создается учетная запись администратора базы данных EKM DB2.

ПРИМЕЧАНИЕ: В данном экране и каждом из двух последующих экранов создается отдельная учетная запись. Запишите все имена пользователей и пароли, которые вы создаете для данных учетных записей.

6. По умолчанию в поле **Database Location (Расположение базы данных)** указывается заранее введенное место. Компания Dell рекомендует не изменять место расположения по умолчанию. Это папка, в которую установщик выполнит установку программного обеспечения EKM 3.0 DB2.

7. В поле **Database User Name (Имя пользователя базы данных)** введите имя пользователя, которое соответствует следующим критериям:

   - может содержать только строчные буквы (a–z), цифры (0–9) и символ подчеркивания (_)
   - Не может включать более восьми символов
   - Не может начинаться с “ibm,” “sys,” “sql,” или цифры
   - Не может начинаться или заканчиваться на символ подчеркивания (_)
   - Не может быть словом, зарезервированным для DB2 (например, “users,” “admins,” “guests,” “public” и “local”), или словом, зарезервированным для SQL
   - Не может совпадать с именем существующего пользователя системы

   Это идентификатор учетной записи администратора базы данных EKM 3.0 DB2. EKM 3.0 создает локальную учетную запись пользователя в вашей системе с таким именем пользователя.

8. В поле **Database Password (Пароль базы данных)** введите пароль для учетной записи администратора базы данных EKM DB2. В поле **Confirm Database Password (Повторить пароль базы данных)** введите пароль повторно.

ПРИМЕЧАНИЕ: Все пароли чувствительны к регистру.

ПРИМЕЧАНИЕ: Компания Dell рекомендует использовать надежные пароли для всех учетных записей EKM 3.0.

9. В поле **Database Data Drive (Диск хранения базы данных)** укажите диск для хранения базы данных. В данной папке будут сохранены данные EKM 3.0 DB2. Для операционной системы Windows введите букву диска и двоеточие (:). Для систем на базе Linux введите путь к папке, например, **/home/ekmdb2**.
10. В поле **Database Name (Имя базы данных)** укажите имя для базы данных EKM 3.0 DB2.
11. В поле **Database Port (Порт базы данных)** по умолчанию указано значение **50010** для операционной системы Windows, и значение **50000** для систем на базе Linux.

    Для всех портов, используемых в EKM 3.0 и настраиваемых в процессе установки EKM 3.0, указывается заранее введенные рекомендованные адреса. Компания Dell настоятельно рекомендует использовать данные рекомендованные адреса портов. Если планируется использование дополнительного сервера и адрес какого-либо порта изменяется в процессе установки EKM 3.0, то адрес данного порта должен совпадать как для основного, так и для дополнительного сервера EKM 3.0.

ПРИМЕЧАНИЕ: Все использованные в процессе установки порты должны быть открыты для выполнения установки EKM 3.0. Убедитесь в том, что они открыты:

Для проверки того, что порты являются открытыми, в операционной системе Windows,

a. Перейдите по адресу: **<*root*>:\Windows\System32\drivers\etc**.
b. Откройте текстовый файл **Services**.
c. Изучите содержимое файла и убедитесь в том, что номер порта, который планируется указать в поле **Database Port (Порт базы данных)** присутствует. Если порт доступен, то его в списке не будет.

Для проверки того, что порты являются открытыми, в системах на базе Linux,

a. Откройте файл **/etc/services**.
b. Изучите содержимое файла и убедитесь в том, что номер порта, который планируется указать в поле **Database Port (Порт базы данных)** присутствует. Если порт доступен, то его в списке не будет.

12. Нажмите на кнопку **Next (Далее)**.

    Откроется экран **EKM Administrator (Администратор EKM)**. В данном экране вы создаете учетную запись администратора EKM 3.0 (суперпользователя). Данная учетная запись используется для создания новых пользователей, новых групп и назначения для них прав доступа.
13. В поле **Administrator Username (Имя администратора)** введите имя пользователя для администратора EKM 3.0 (Может быть любым за исключением **tklmadmin**).
14. В поле **Password (Пароль)** введите пароль для учетной записи администратора EKM 3.0. В поле **Confirm Password (Повторить пароль)** введите пароль повторно.
15. Нажмите на кнопку **Next (Далее)**.

    Откроется экран **Encryption Manager (Диспетчер шифрования)**. В данном экране создается учетная запись диспетчера шифрования EKM 3.0 Encryption Manager (TKLMAdmin). Данная учетная запись является обычной. Она используется для ежедневного управления ключами. В поле **TKLMAdmin Username (Имя пользователя TKLMAdmin)** заранее введено значение **tklmadmin**. Данное имя пользователя является обязательным для диспетчера шифрования EKM Encryption Manager.
16. В поле **TKLMAdmin password (Пароль TKLMAdmin)** введите пароль для учетной записи диспетчера шифрования Encryption Manager EKM 3.0. В поле **TKLMAdmin Confirm Password (Повторить пароль TKLMAdmin)** введите пароль повторно.
17. В операционной системе Windows и в системах на базе Linux **EKM Port (Порт EKM)** по умолчанию назначен **16310**. Рекомендуется использовать данный порт. Нажмите на кнопку **Next (Далее)**.

ПРИМЕЧАНИЕ: Если указанный порт используется другой службой, то установщик EKM 3.0 предложит вам выбрать другой порт. Для определения используемых портов используйте команду **netstat**, после чего выберите свободный порт. Запишите его номер. Данный порт будет использоваться для осуществления доступа к порталу EKM 3.0.

Откроется экран **Migration (Миграция)**. Данный экран применяется для миграции с EKM 2.X на EKM 3.0.

Если у вас имеется версия EKM 2.X, которую вы желаете мигрировать в EKM 3.0, то выполнить данную процедуру следует сейчас. См. раздел Migrating an Encryption Key Manager (EKM) 2.X Version during the EKM 3.0 Installation (Миграция диспетчера ключей шифрования (EKM) версии 2.X в процессе установки EKM 3.0)..

ПРИМЕЧАНИЕ: Можно выполнить миграцию только версии EKM 2.X, которая использовалась для создания ключей.

Если версии EKM 2.X для миграции в EKM 3.0 не имеется,

a) Оставьте свободным флажок **Migrate from EKM 2.X to EKM 3.0 (Мигрировать с EKM 2.X на EKM 3.0)** и нажмите на кнопку **Next (Далее)**.

   Откроется всплывающее окно с запросом на проверку.

b) Если выбран вариант без миграции с версии EKM 2.X, нажмите на кнопку **Yes (Да)** во всплывающем окне с подтверждением того, что миграция с версии EKM 2.X не выполняется.

   Откроется экран **Configuration Summary (Обзор конфигурации)**.

18. На экране **Configuration Summary (Обзор конфигурации)** отметьте флажок **Save profile (Сохранить профиль)**.

    Станет активным поле **File Directory (Папка для файла)**.

ПРИМЕЧАНИЕ: Компания Dell рекомендует сохранить профиль установки на тот случае, когда потребуется повторная установка EKM 3.0 для устранения последствий аварии. Сохраненный профиль установки необходим для создания дополнительного сервера EKM 3.0.

ПРИМЕЧАНИЕ: Компания Dell рекомендует использовать для сохранения файла съемный диск. В случае использования съемного диска его следует подключить до нажатия на кнопку **Next**. Съемный диск должен оставаться подключенным к системе до завершения процесса установки. В другом случае можно сохранить данный файл на локальном диске, позже скопировать его на съемный диск.

ПРИМЕЧАНИЕ: Вводимый в данное поле путь должен включать имя файла. Не указывайте только имя папки. Путь вплоть до имени папки должен существовать, а имя файла для профиля установки существовать не должно.

19. В поле **File Directory (Папка для файла)** введите место хранения и имя файла создаваемого профиля установки, или нажмите на кнопку **Choose (Выбрать)** и выберите место расположения и введите имя файла.

    В данной папке будет сохранен профиль установки с указанным именем файла.

    EKM 3.0 сохраняет профиль установки после завершения процедуры установки EKM 3.0. Если используется конфигурация основного/дополнительного сервера, необходимо использовать профиль установки основного сервера EKM 3.0 в процессе установки дополнительного сервера EKM 3.0 для автоматического заполнения полей для ввода информации во время установки.

    Аналогично, если установка выполняется на том же сервере и вам необходимо использовать те же поля, то можно использовать данный профиль установки для автоматического заполнения полей для ввода информации для установки.

ПРИМЕЧАНИЕ: Компания Dell рекомендует сделать снимок или распечатать экран **Configuration Summary (Обзор конфигурации)** для использования в дальнейшем.

20. На экране **Configuration Summary (Обзор конфигурации)** нажмите на кнопку **Next (Далее)**.

    Откроется экран **Installation Summary(Обзор установочной информации)**.

21. Проверьте правильность информации на экране **Installation Summary (Обзор установочной информации)**.

22. Нажмите на кнопку **Install (Установить)**.

ПРИМЕЧАНИЕ: Процедура установки программного обеспечения занимает примерно 45 минут. Не выключайте систему до завершения процедуры установки.

ПРИМЕЧАНИЕ: Если вы планируете настроить дополнительный сервер EKM 3.0, не устанавливайте EKM 3.0 на дополнительный сервер до тех пор, пока не завершиться процесс установки EKM 3.0 на основном сервере.

23. После завершения процесса установки нажмите на кнопку **Done (Готово)**.

ПРИМЕЧАНИЕ: Если была выполнена миграция версии EKM 2.X на новую установку EKM 3.0, то компания Dell настоятельно рекомендует создать резервную копию EKM 3.0 для того, чтобы гарантировать сохранность новых ключей. См. раздел Creating a Backup of the Keystore (Создание резервной копии хранилища ключей).

ПРИМЕЧАНИЕ: Если в процессе повторной установки EKM 3.0 происходит ошибка установки из-за ее прерывания, то удаление следует выполнить вручную. См. раздел Manually Uninstalling EKM 3.0 in Windows (Ручное удаление EKM 3.0 в операционной системе Windows).

3

Настройка основного и дополнительного сервера EKM 3.0

В данной главе описывается способ установки, использования и удаления EKM 3.0 на основном и дополнительном сервере.

ОСТОРОЖНО: Чтобы предотвратить возможную потерю данных из-за отказа сервера EKM 3.0, компания Dell рекомендует использовать конфигурацию с основным и дополнительным сервером EKM 3.0. Такая конфигурация обеспечивает избыточность в случае, когда основной сервер EKM 3.0 не работает или недоступен.

ПРИМЕЧАНИЕ: Невозможно иметь сервер EKM 3.0 в качестве основного, и сервер EKM 2.X в качестве дополнительного, или наоборот.

Установка EKM 3.0 на основной сервер

В процессе установки EKM 3.0 на основной сервер необходимо выбрать вариант с сохранением профиля установки. После завершения процедуры установки EKM 3.0 на основном сервере скопируйте сохраненный профиль установки на переносной диск или в совместно используемую папку на сервере. См. раздел Installing EKM 3.0 (Установка EKM 3.0).

Использование EKM 3.0 на основном сервере

Основным считается тот сервер EKM 3.0, на котором выполняются все задания по управлению ключами шифрования. По умолчанию основной сервер EKM 3.0 имеет следующую настройку: **Automatically accept all new device requests for communication (Автоматический прием запросов на установление связи от всех новых устройств)**. Подробную информацию о том, как просматривать или изменять данную настройку, см. раздел Configuring EKM 3.0 to Accept Devices that Contact EKM 3.0 for Keys (Настройка EKM 3.0 для принятия устройств, обращающихся к EKM 3.0 для получения ключей). Компания Dell рекомендует регулярно создавать резервные копии данных основного сервера EKM 3.0. См. раздел Performing Backups and Restoring from a Backup (Создание резервной копии и восстановление с помощью резервной копии).

Если по какой-либо причине необходимо заменить основной сервер EKM 3.0, установите EKM 3.0 на новый физический сервер с использованием профиля установки, созданного в процессе установки первого основного сервера EKM 3.0. Восстановите данные на новом основном сервере EKM 3.0 с помощью самой свежей резервной копии, затем обновите все устройства для того, чтобы они могли отправлять свои запросы на получение ключей в новый основной сервер EKM 3.0. Смотрите руководство пользователя на вашу ленточную библиотеку для получения информации о том, как изменить IP-адрес сервера EKM 3.0, используемого для отправки запросов на получение ключей. Для поиска руководства пользователя ленточной библиотекой см. раздел Documentation and Reference Materials (Документация и справочная информация) файл **ReadThisFirst.txt** на установочном носителе EKM 3.0.

Установка EKM 3.0 на дополнительном сервере

ПРИМЕЧАНИЕ: Не устанавливайте EKM 3.0 на дополнительном сервере до тех пор, пока не закончится установка EKM 3.0 на основном сервере не будет завершена.

На системе, на которой EKM 3.0 установлен в качестве дополнительного сервера, должна использоваться такая же версия операционной системе, что и установленная на основном сервере EKM 3.0. EKM 3.0 не поддерживает возможность использования разных операционных систем на основных и дополнительных серверах.

Установите EKM 3.0 на дополнительный сервер согласно процедур, описанных в разделе Installing EKM 3.0 (Установка EKM 3.0). Используйте профиль установки, сохраненный во время установки EKM 3.0 на основной сервер. Вы должны вручную ввести те же самые пароли, что были использованы во время установки EKM 3.0 на основной сервер.

Использование EKM 3.0 на дополнительном сервере

Дополнительный сервер EKM 3.0 применяется для обеспечения избыточности на тот случай, когда основной сервер EKM 3.0 не работает или недоступен.

Регулярно используйте резервную копию, созданную на основном сервере EKM 3.0, для выполнению операции восстановления на дополнительном сервере EKM 3.0 для обеспечения синхронизации данных на основном и дополнительном сервере EKM 3.0. См. раздел Performing Backups and Restoring from a Backup (Создание резервной копии и восстановление из резервной копии).

По умолчанию дополнительный сервер EKM 3.0 также настроен на **Automatically accept all new device requests for communication (Автоматический прием запросов на установление связи от всех новых устройств)**. Компания Dell рекомендует изменять данный параметр на **Only accept manually added devices for communication (Принимать запросы только от вручную указанных устройств)** после каждой операции восстановления. Такая настройка позволит не допустить выдачу ключей дополнительным сервером EKM 3.0 новым устройствам, которые не добавлены в основной сервер EKM 3.0. Для получения подробной информации о том, как просматривать или изменять данную настройку см. раздел Configuring EKM 3.0 to Accept Devices that Contact EKM 3.0 for Keys (Настройка EKM 3.0 для принятия запросов от устройств, обращающихся к EKM 3.0 для получения ключей).

Если основной сервер EKM 3.0 временно не работает или недоступен, необходимо выполнить операцию восстановления на дополнительном сервере EKM 3.0 с использованием самой свежей резервной копии данных основного сервера EKM 3.0.

ПРИМЕЧАНИЕ: Когда основной сервер EKM 3.0 не работает или недоступен, а дополнительный сервер EKM 3.0 используется для обслуживания запросов устройств на получения ключей, компания Dell рекомендует не выполнять на дополнительном сервере EKM 3.0 какие-либо работы по управлению работой системы или текущие задачи.

Удаление EKM 3.0 с основного и дополнительного сервера

Порядок действий при удалении EKM 3.0 с основного и дополнительного сервера см. в разделе Uninstalling EKM 3.0 (Удаление EKM 3.0).

4

Создание резервной копии и восстановление с помощью резервной копии

Процедуру создания резервной копии можно провести в любой момент. В результате выполнения данной процедуры создается резервная копия файла с хранилищем ключей с устройствами и ключами.

В резервные копии не включаются группы устройств, пользователи или группы пользователей. База данных DB2 содержится здесь.

Провести восстановление данных с помощью резервной копии можно в любой момент.

ПРИМЕЧАНИЕ: Если резервная копия ключей не создана, ключи не будут обслуживаться. Если ключи недоступны для обслуживания, то задания по созданию зашифрованных резервных копий завершаться ошибкой.

Создание резервной копии хранилища ключей

В данной главе описывается способ создания резервной копии хранилища ключей.

1. Войдите в портал EKM 3.0. См. Вход в портал диспетчера ключей шифрования Encryption Key Manager 3.0.

   Откроется окно приветствия **Welcome to Dell Encryption Key Manager**.
2. В панели навигации перейдите к **Dell Encryption Key Manager (Диспетчер ключей шифрования Dell)** → **Backup and Restore (Резервное копирование и восстановление данных)** .

   Откроется окно **Backup and Restore (Резервное копирование и восстановление данных)**.
3. Нажмите на кнопку **Browse (Обзор)** рядом с полем **Backup repository location (Расположение архива с резервной копией)** и перейдите к папке, в которой желаете сохранить файл резервной копии (например, **C:\EKM_Backup** для операционной системы Windows, или **/root/EKM_Backup** на платформах с Linux).

ПРИМЕЧАНИЕ: Данная папка должна быть создана до начала процесса создания резервной копии, или процесс будет прекращен. Если вы желаете использовать новую папку, то создайте ее до начала процесса создания резервной копии.

4. Нажмите на кнопку **Select (Выбрать)** во всплывающем окне **Browse Directory (Обзор каталога)** для возврата к экрану **Backup and Restore (Резервное копирование и восстановление данных)**.
5. Нажмите на кнопку **Create Backup (Создать резервную копию)**.

   Отобразится экран **Create Backup (Создать резервную копию)**.
6. В поле **Create password (Создать пароль)** укажите пароль к резервной копии. Данный пароль должен состоять не менее чем из шести символов.

ПРИМЕЧАНИЕ: Компания Dell рекомендует использовать надежные пароли во всех связанных с EKM 3.0 случаях.

7. В поле **Retype Password (Повторить пароль)** повторно ведите пароль.
8. (Дополнительно) В поле **Backup description (Описание резервной копии)** ведите описание для файла резервной копии. Если описание не указано, то для файла резервной копии применяется описание по умолчанию.

ПРИМЕЧАНИЕ: В некоторых версиях приложений для просмотра веб-страниц поле с используемым по умолчанию описанием защищено от редактирования. Более подробную информацию см. разделе Known Issues and Their Resolutions (Известные проблемы и методы их решения).

9. Нажмите на кнопку **Create Backup (Создать резервную копию)**.

   Откроется всплывающее окно с запросом на подтверждение.

10. Во всплывающем окне с запросом на подтверждение нажмите на кнопку **OK**. Начнется выполнения процесса создание резервной копии.

ПРИМЕЧАНИЕ: Не используйте систему в процессе создания резервной копии. Если окно EKM 3.0 остается выделенным серым цветом в течение продолжительного времени, в приложении для просмотра веб-страниц нажмите на кнопку "Обновить".

11. После создания файла резервной копии отобразится всплывающее окно **Information (Информация)** с подтверждением успешного создания файла. Во всплывающем окне нажмите на кнопку **OK**. Созданный вами файл резервной копии отображается в таблице на экране **Backup and Restore (Резервное копирование и восстановление данных)**.

12. Нажмите на кнопку **Return home (Вернуться в начало)** в нижней части экрана.

    Откроется окно приветствия **Welcome to Dell Encryption Key Manager**.

Восстановление из резервной копии

Можно восстановить данные из резервной копии. Резервную копию можно применить для создания дополнительных серверов управления ключами, а также для повторного создания сервера EKM 3.0 в случае восстановления при отказе.

ОСТОРОЖНО: Выполняйте восстановление данных только из такой резервной копии, которая была создана на текущей системе, или с помощью другого сервера EKM 3.0, установленного с использованием текущего профиля установки. Невозможно выполнить восстановление данных из резервной копии, которая была создана на отличной от текущей системе с другими установочными параметрами.

1. Войдите в портал EKM 3.0. См. Вход в портал диспетчера ключей шифрования Encryption Key Manager 3.0.

   Откроется окно приветствия **Welcome to Dell Encryption Key Manager**.

2. В панели навигации перейдите к **Dell Encryption Key Manager (Диспетчер ключей шифрования Dell)** → **Backup and Restore (Резервное копирование и восстановление данных)** .

   Откроется окно **Backup and Restore (Резервное копирование и восстановление данных)**.

3. Выберите файл резервной копии для восстановления.

4. Нажмите кнопку **Restore From Backup (Восстановить из резервной копии)** в верхней части таблицы.

   Откроется подокно **Restore From Backup (Восстановить из резервной копии)**.

5. Введите пароль к файлу резервной копии.

6. Нажмите кнопку **Restore Backup (Восстановить резервную копию)**.

   Откроется всплывающее окно с запросом на подтверждение.

ОСТОРОЖНО: Все ключи, созданные после создания резервной копии, будут потеряны, так же как и доступ к любым данным, зашифрованным с применением данных ключей. Потерянные или удаленные ключи восстановить каким бы то ни было способом невозможно.

7. Во всплывающем окне с запросом на подтверждение нажмите кнопку **OK**.

8. После восстановления данных с помощью резервной копии следует вручную остановить и запустить сервер EKM 3.0. См. Запуск и остановка сервера EKM 3.0 в Windows или Запуск и остановка сервера EKM 3.0 в Linux.

5

Использование EKM 3.0

В данной главе описываются некоторые основные операции EKM 3.0.

ПРИМЕЧАНИЕ: EKM 3.0 основан на диспетчере жизненного цикла ключей IBM Tivoli Key Lifecycle Manager (TKLM) V2 FixPack 2, но был адаптирован для поддержки инфраструктуры ленточных библиотек Dell при помощи выбора подходящей подгруппы параметров TKLM для ленты.

Для получения сведений об использовании EKM 3.0, которые не были рассмотрены в данном руководстве, см. документацию TKLM, которая включает в себя следующее:

- IBM Tivoli Key Manager 2.0 *Quick Start Guide (Краткое руководство пользователя)*
- IBM Tivoli Key Manager 2.0 *Installation and Configuration Guide (Руководство по установке и настройке)*
- IBM Tivoli Key Manager 2.0 *Product Overview/Scenario Guide (Обзор продукта/Руководство по использованию сценариев)*

Для получения сведений о том, как получить доступ к документации TKLM, см. раздел Documentation and Reference Materials (Документация и справочная информация) файла **ReadThisFirst.txt** на установочном носителе EKM 3.0.

Некоторые экраны и функции, рассмотренные в документации IBM TKLM, не включены в Dell EKM 3.0. EKM 3.0 включает в себя только ту подгруппу функций, которая необходима для реализации поддержки ленточных библиотек Dell PowerVault.

Вход в портал диспетчера ключей шифрования Encryption Key Manager 3.0

Для входа в портал Encryption Key Manager 3.0 выполните следующие шаги:

1. Откройте веб-обозреватель и для открытия портала EKM 3.0 введите следующий указатель URL:

   http://<*IP_адрес_сервера_EKM 3.0*>:<*номер_порта_EKM_3.0*>

ПРИМЕЧАНИЕ: Указанный номер порта совпадает с указанным вами в процессе установки EKM 3.0. Значением по умолчанию является **16310**.

Если номер порта не известен, см. следующее:

В операционной системе Windows	См. значение свойства **WC_defaulthost** в следующем файле: **<*root*>:\Dell \EKM\profiles\TIPProfile\properties\portdef.props**.
На платформах Linux	См. значение свойства **WC_defaulthost** в следующем файле: **/opt/dell/ekm/profiles/ TIPProfile/properties/portdef.props**.

ПРИМЕЧАНИЕ: Если отображается сообщение об ошибке с текстом, что страницу найти невозможно, это может говорить о том, что служба EKM 3.0 не запущена. См. Запуск и остановка сервера EKM 3.0 в Windows или Запуск и остановка сервера EKM 3.0 в Linux.

Отображается окно входа в EKM 3.0.

2. Войдите в EKM 3.0 с помощью имени пользователя диспетчера шифрования EKM 3.0 Encryption Manager (**tklmadmin**) и пароля дисптчера шифрования EKM 3.0 Encryption Manager, указанного в процессе установки EKM 3.0.

   Откроется окно приветствия **Welcome to Dell Encryption Key Manager**.

Создание главного хранилища ключей

В данной главе описывается способ создания главного хранилища ключей. Во время первого входа в EKM 3.0 вы должны создать главное хранилище ключей.

ПРИМЕЧАНИЕ: Если вы мигрировали хранилище ключей EKM 2.X в процессе установки EKM 3.0, то хранилище ключей уже создано, и данную процедуру можно пропустить.

ПРИМЕЧАНИЕ: В дальнейшем, если вы желаете создать добавочные ключи и (или) группы ключей, см. раздел Creating Key Groups for the Device Group (Создание групп ключей для группы устройств).

Для создания главного хранилища ключей выполните следующие действия:

1. На экране приветствия диспетчера ключей шифрования **Welcome to Dell Encryption Key Manager** нажмите на **click here to create the master keystore (Нажмите для создания главного хранилища ключей)**.

   Появится экран **Keystore (Хранилище ключей)**.

2. Сохраните значения по умолчанию для полей **Keystore type (Тип хранилища ключей)**, **Keystore path (Путь к хранилищу ключей)** и **Keystore name (Имя хранилища ключей)**.

   Значения по умолчанию: **Keystore type (Тип хранилища ключей)**: JCEKS, и **Keystore name (Имя хранилища ключей)**: defaultKeyStore. Значение по умолчанию для поля **Keystore path (Путь к хранилищу ключей)** для операционной системы Windows: **<*root*>:\Dell\EKM\products\tklm\keystore**. Значение по умолчанию для поля **Keystore path (Путь к хранилищу ключей)** для систем на базе Linux: **/opt/dell/ekm/products/tklm/keystore**.

3. В поле **Password (Пароль)** укажите пароль к хранилищу ключей по умолчанию. Данный пароль должен состоять не менее чем из шести символов.

4. В поле **Retype Password (Повторить пароль)** повторно ведите пароль.

5. Нажмите на кнопку **OK**.

   На экране **Keystore (Хранилище ключей)** отображается подтверждение успешного создания хранилища ключей.

6. Создайте резервную копию хранилища ключей. См. раздел Performing Backups and Restoring from a Backup (Создание резервной копии и восстановление с помощью резервной копии).

Включение брандмауэра на сервере EKM 3.0

ПРИМЕЧАНИЕ: Указания по настройке вашего брандмауэра см. в документации к вашей операционной системе.

EKM 3.0 обменивается данными с ленточной библиотекой по сети. Если на системе, на которой установлен EKM 3.0, включен брандмауэр и необходимые порты не были открыты, обмен данными между EKM 3.0 и ленточной библиотекой будет нарушено. Если брандмауэр должен быть включен на системе, на которой установлен EKM 3.0, то для восстановления обмена данными между EKM 3.0 и ленточной библиотекой выполните следующие действия:

ПРИМЕЧАНИЕ: Эти порты используются в EKM 3.0 по умолчанию. Если ваша ленточная библиотека настроена на использование других портов, убедитесь в том, что при настройке брандмауэра и EKM 3.0 используются данные номера портов.

ПРИМЕЧАНИЕ: Если для EKM 3.0 используется конфигурация основного/дополнительного сервера, то повторите данную процедуру для дополнительного сервера.

1. Откройте следующие порты для соответствующих протоколов:
   - TCP: 3801
   - SSL: 443
2. Если ваш брандмауэр настроен только на пропускание определенных IP-адресов и/или масок подсети для передачи данных по вышеуказанным портам, то убедитесь в том, что IP-адрес и/или маска подсети вашей ленточной библиотеки включены в список разрешенных IP-адресов и/или масок подсети.

   Для получения доступа к сетевым настройкам ленточной библиотеки, войдите в станцию дистанционного управления ленточной библиотекой (RMU) и откройте сетевые настройки. Более подробную информацию см. в руководстве пользователя ленточной библиотекой. Для поиска руководства пользователя ленточной библиотекой см. раздел Documentation and Reference Materials (Документация и справочная информация) файл **ReadThisFirst.txt** на установочном носителе EKM 3.0.
3. Если позже вы захотите изменить настройки портов для обмена данных между EKM 3.0 и ленточной библиотекой, убедитесь в том, что данные порты изменены в настройках ленточной библиотеки, EKM 3.0 и брандмауэра на той системе, на которой установлен EKM 3.0.

Настройка EKM 3.0 для принятия устройств, обращающихся к EKM 3.0 для получения ключей

В данной главе описывается способ настройки поведения EKM 3.0 для обработки запросов от устройств, пытающихся подключиться к EKM 3.0 для отправки запроса на получения ключей. Подробную информацию о том, как подключиться к EKM 3.0 для отправки запросов на получение ключей см. в руководстве пользователя к вашему устройству.

1. Войдите в портал EKM 3.0. См. Вход в портал диспетчера ключей шифрования Encryption Key Manager 3.0.

   Откроется окно приветствия **Welcome to Dell Encryption Key Manager**.
2. В панели навигации перейдите к **Dell Encryption Key Manager (Диспетчер ключей шифрования Dell) → Key and Device Management (Управление ключами и устройствами)** .

   Появится экран **Key and Device Management (Управление ключами и устройствами)**.
3. В выпадающем меню **Manage keys and devices (Управлять ключами и устройствами)** выберите **LTO** и нажмите на кнопку **Go (Выполнить)**.

ПРИМЕЧАНИЕ: Для получения более подробных сведений о том, как получить доступ к документации TKLM, см. раздел Documentation and Reference Materials (Документация и справочная информация) файла **ReadThisFirst.txt** на установочном носителе EKM 3.0.

4. В выпадающем меню в нижней части таблицы выберите один из следующих вариантов:

Automatically accept all new device requests for communication (Автоматический прием запросов на установление связи от всех новых устройств)	Ключи будут автоматически выдаваться новым устройствам. Это настройка EKM 3.0 по умолчанию. Компания Dell рекомендует сохранить данную настройку для основного сервера EKM 3.0, но не для дополнительного, если он настроен.

Only accept manually added devices for communication (Принимать запросы только от вручную указанных устройств)	Ключи не будут выдаваться устройством, за исключением случаев, когда устройства добавлены вручную. Если вы настраиваете дополнительный сервер EKM 3.0, компания Dell рекомендует использовать данную настройку для того, чтобы дополнительный сервер EKM 3.0 не выдавал автоматически ключи новым устройствам.
Hold new device requests pending my approval (Задерживать запросы от новых устройств до принятия решения)	Обращающиеся к EKM 3.0 устройства добавляются в список ожидания.

Создание группы устройств

Данная процедура позволяет создать группу устройств. Если используется группа устройств по умолчанию, пропустите данный раздел.

Группы устройств используются для управления Ключами, которые обслуживают одно или более устройств. Компания Dell рекомендует использовать группы устройств для управления подгруппы устройств исходя их нужд своей организации.

Для создания новой группы устройств выполните следующие действия:

1. Войдите в портал EKM 3.0. См. Вход в портал диспетчера ключей шифрования Encryption Key Manager 3.0.

   Откроется окно приветствия **Welcome to Dell Encryption Key Manager**.
2. В панели навигации перейдите к **Dell Encryption Key Manager (Диспетчер ключей шифрования Dell) → Advanced Configuration (Дополнительная настройка) → Device Group (Группа устройств)**.

   Появится экран **Manage Device Groups (Управлять группой устройств)**.
3. Нажмите кнопку **Create (Создать)** в верхней части таблицы.

   Откроется подокно **Create Device Group (Создать группу устройств)**.
4. Под полем **Device family (Семейство устройства)** выберите зависимый переключатель **LTO**.
5. В поле **Device group name (Имя группы устройств)** введите имя для группы устройств. Компания Dell рекомендует водить имя, которое отражает назначение данной группы устройств, например, **Accounting (Учет)**.
6. Нажмите на кнопку **Create (Создать)**.

   Во всплывающем окне **Information (Информация)** указываются настройки семейства устройства.
7. Во всплывающем окне **Information (Информация)** нажмите на кнопку **OK**.

   Группа устройств создана. Новая группа устройств отражается в списке на экране **Manage Device Groups (Управлять группой устройств)**.

Создание групп ключей для группы устройств

Группы ключей – это объединенные в группы ключи для определенного устройства. В данной главе описывается способ создания и настройки групп ключей для определенного устройства. Группы ключей, которые были настроены для одного устройства, не могут использоваться с другим устройством.

Для создания групп ключей для группы устройств выполните следующие действия:

1. Войдите в портал EKM 3.0. См. Вход в портал диспетчера ключей шифрования Encryption Key Manager 3.0.

   Откроется окно приветствия **Welcome to Dell Encryption Key Manager**.
2. В панели навигации перейдите к **Dell Encryption Key Manager (Диспетчер ключей шифрования Dell) → Key and Device Management (Управление ключами и устройствами)** .

Появится экран **Key and Device Management (Управление ключами и устройствами)**.

3. В выпадающем меню **Manage keys and devices (Управлять ключами и устройствами)** выберите имя группы устройств, в которую вы желаете добавить группу ключей.
4. Рядом с **Key and Device Management (Управление ключами и устройствами)** нажмите на кнопку **Go (Приступить)**.

   В утилите **Key and Device Management (Управление ключами и устройствами)** откроется страница для выбранной группы устройств. На данной странице перечисляются любые группы ключей и устройств, которые входят в данную группу устройств.
5. В таблице нажмите на кнопку **Add (Добавить)**, а затем выберите **Key Group (Группа ключей)**.

   Откроется подокно **Create Key Group (Создать группу ключей)**.
6. В поле **Key group name (Имя группы ключей)** введите имя группы ключей.
7. В поле **Number of keys to create (Количество создаваемых ключей)** введите количество создаваемых ключей.
8. В поле **First three letters of key name (Первые три буквы имени ключа)** введите префикс из трех любых букв для имени ключа.
9. Если необходимо сделать данную группу ключей группой ключей по умолчанию, отметьте флажок **Make this the default key group (Сделать группой ключей по умолчанию)**.
10. Нажмите на **Create Key Group (Создать группу ключей)**.

    Отобразится всплывающее окно **Warning (Предупреждение)**.
11. Если вы хотите создать резервную копию, нажмите на ссылку голубого цвета во всплывающем окне **Warning (Предупреждение)** для перенаправления на экран **Backup and Restore (Резервное копирование и восстановление данных)**. См. раздел Performing Backups and Restoring from a Backup (Создание резервной копии и восстановление с помощью резервной копии). После создания реервной копии вернитесь на экран **Key and Device Management (Управление ключами и устройствами)**. Если создавать резервную копию в этот раз не требуется, то переходите к следующему действию.

ПРИМЕЧАНИЕ: Компания Dell рекомендует создавать резервную копию данных всякий раз, когда в ключи, группы ключей или группы устройств вносятся изменения.

12. Нажмите на кнопку **OK** во всплывающем окне **Warning (Предупреждение)**.

    Группа ключей создана. В окне **Key and Device Management (Управление ключами и устройствами)** отображаются группы ключей.
13. Данное действие выполнять не обязательно. Убедитесь в том, что ключи были созданы, для чего выполните действия, приведенные на экране **Key and Device Management (Управление ключами и устройствами)**:
    a) В выпадающем меню в верхней части таблицы выберите **View Keys, Key Group Membership and Drives (Показать ключи, состав группы ключей и диски)**.

       В таблице отобразятся ключи.
    b) Прокрутите список вниз для обнаружения новых ключей.

Добавление устройства в группу устройств

В данной главе описывается порядок добавления устройства в существующую группу устройств.

ПРИМЕЧАНИЕ: В EKM 3.0 группами устройств по умолчанию являются **FUTURE_DEVICES** и **LTO**.

ПРИМЕЧАНИЕ: Для автоматического добавления устройств в какую-либо группу устройств, необходимо создать группу ключей и резервную копию, или в противном случае проведение проверки пути к ключу библиотеки завершиться ошибкой и устройство добавлено не будет. Более подробную информацию см. в разделе Creating Key Groups for a Device Group (Создание групп ключей для группы устройств) и Creating a Backup of the Keystore (Создание резервной копии хранилища ключей).

1. Войдите в портал EKM 3.0. См. Вход в портал диспетчера ключей шифрования Encryption Key Manager 3.0.

   Откроется окно приветствия **Welcome to Dell Encryption Key Manager**.
2. Под **Key and Device Management (Управление ключами и устройствами)** в выпадающем меню **Manage keys and devices (Управлять ключами и устройствами)** выберите группу устройств для использования.
3. Нажмите **Go (Вперед)**.

   В утилите **Key and Device Management (Управление ключами и устройствами)** откроется страница для выбранной группы устройств. На данной странице перечисляются любые группы ключей и устройств, которые входят в данную группу устройств.
4. Для открытия выпадающего меню в нижней части страницы выберите **Automatically accept all new device requests for communication (Автоматический прием запросов на установление связи от всех новых устройств)**.
5. Настройте ленточную библиотеку на подключение к серверу EKM 3.0.

   Более подробную информацию см. в руководстве пользователя ленточной библиотеки. Руководство пользователя ленточной библиотеки см. в разделе Documentation and Reference Materials (Документация и справочная информация) файла **ReadThisFirst.txt** на установочном носителе EKM 3.0.
6. Запустите проверку пути к ключу в станции дистанционного управления ленточной библиотекой (RMU). Более подробную информацию см. в руководстве пользователя ленточной библиотеки.

   Новое устройство отображается на экране **Key and Device Management (Управление ключами и устройствами)**.

ПРИМЕЧАНИЕ: Если вы желаете добавить устройство вручную, см. документацию TKLM. Для получения сведений о том, как получить доступ к документации TKLM, см. раздел Documentation and Reference Materials (Документация и справочная информация) файла **ReadThisFirst.txt** на установочном носителе EKM 3.0.

Удаление и добавление ключей в группы ключей

В данной главе описывается способ добавления и удаления ключей из групп ключей.

ПРИМЕЧАНИЕ: В результате удаления ключа из группы ключей сам ключ не удаляется; ключ просто перестает входить в группу ключей. Если необходимо удалить один ключ, то см. раздел Deleting a Specific Key (Удаление определенного ключа).

ПРИМЕЧАНИЕ: Указания по открытию окна **Key and Device Management (Управление ключами и устройствами)** см. в разделе Creating Key Groups for the Device СозGroup (Создание групп ключей для группы устройств).

1. Войдите в портал EKM 3.0. См. Вход в портал диспетчера ключей шифрования Encryption Key Manager 3.0.

   Откроется окно приветствия **Welcome to Dell Encryption Key Manager**.
2. В панели навигации перейдите к **Dell Encryption Key Manager (Диспетчер ключей шифрования Dell) → Key and Device Management (Управление ключами и устройствами)** .

   Появится экран **Key and Device Management (Управление ключами и устройствами)**.
3. В выпадающем меню **Manage keys and devices (Управлять ключами и устройствами)** выберите имя группы устройств, в которую вы желаете добавить группу ключей.
4. Рядом с **Key and Device Management (Управление ключами и устройствами)** нажмите на кнопку **Go (Приступить)**.

   В утилите **Key and Device Management (Управление ключами и устройствами)** откроется страница для выбранной группы устройств. На данной странице перечисляются любые группы ключей и устройств, которые входят в данную группу устройств.
5. Выберите группу ключей для изменения.

6. Нажмите кнопку **Modify (Изменить)** в верхней части таблицы.

   Откроется подокно **Modify Key Group (Изменить группу ключей)**.

7. В подокне **Modify Key Group (Изменить группу ключей)** выберите требуемый зависимый переключатель.

   Если вы выбрали зависимый переключатель **Create additional keys in key group (Создать добавочные ключи в группе ключей)**, введите количество ключей для добавления в группу ключей в поле **Number of keys to create (Количество создаваемых ключей)**. В поле **First three letters of key name (Первые три буквы имени ключа)** введите три буквы, которые в новых ключах будут использоваться как префикс.

   Если вы выбрали поле **Delete key from key group (Удалить ключ из группы ключей)**, то введите псевдоним ключа в текстовое поле.

8. Выберите **Modify Key Group (Изменить группу ключей)**.

   Группа ключей изменяется и отражает внесенные изменения.

Удаление групп ключей

В данной главе описывается способ удаления группы ключей.

ОСТОРОЖНО: В результате удаления группы ключей удаляются все включенные в данную группу ключи. Удаление ключа эквивалентно удалению любых данных, защищенных с помощью данного ключа, так как к этим данным невозможно будет получить доступ. Для обеспечения безопасности удаленные ключи невозможно восстановить каким-либо способом.

ПРИМЕЧАНИЕ: Нельзя удалить группу ключей по умолчанию для группы устройств.

Для удаления группы ключей выполните следующие действия:

1. Войдите в портал EKM 3.0. См. Вход в портал диспетчера ключей шифрования Encryption Key Manager 3.0.

   Откроется окно приветствия **Welcome to Dell Encryption Key Manager**.

2. В панели навигации перейдите к **Dell Encryption Key Manager (Диспетчер ключей шифрования Dell) → Key and Device Management (Управление ключами и устройствами)** .

   Появится экран **Key and Device Management (Управление ключами и устройствами)**.

3. В выпадающем меню **Manage keys and devices (Управлять ключами и устройствами)** выберите имя группы устройств, в которую вы желаете добавить группу ключей.

4. Рядом с **Key and Device Management (Управление ключами и устройствами)** нажмите на кнопку **Go (Приступить)**.

   В утилите **Key and Device Management (Управление ключами и устройствами)** откроется страница для выбранной группы устройств. На данной странице перечисляются любые группы ключей и устройств, которые входят в данную группу устройств.

5. Убедитесь в том, что предназначенная для удаления группа ключей не является группой ключей по умолчанию. В противном случае измените группу ключей таким образом, чтобы она перестала быть группой ключей по умолчанию:

   a) В таблице **Key Group (Группа ключей)** правой кнопкой мыши нажмите на группу ключей, которую необходимо удалить.

      Откроется всплывающее меню.

   b) Во всплывающем меню выберите **Modify (Изменить)**.

      Откроется подокно **Modify Key Group (Изменить группу ключей)**.

   c) Снимите флажок **Make this the default key group (Сделать группой ключей по умолчанию)**.

   d) Нажать на **Modify Key Group (Изменить группу ключей)**.

      Появится экран **Key and Device Management (Управление ключами и устройствами)**.

6. Нажмите предназначенную для удаления группу ключей для ее выделения, а затем нажмите на кнопку **Delete (Удалить)**.

Откроется всплывающее окно с запросом на подтверждение.

7. Во всплывающем окне с запросом на подтверждение нажмите кнопку **OK**.

   Группа ключей и все ключи, связанные с данной группой ключей, удалены.

Проверка сертификата сервера

В данной главе описывается способ проверки того, что запланированный для использования сертификат сервера является сертификатом сервера. Для этого выполните следующие действия:

1. Войдите в портал EKM 3.0. См. Вход в портал диспетчера ключей шифрования Encryption Key Manager 3.0.

   Откроется окно приветствия **Welcome to Dell Encryption Key Manager**.

2. В панели навигации перейдите к **Dell Encryption Key Manager (Диспетчер ключей шифрования Dell) → Advanced Configuration (Дополнительная настройка) → Server Certificates (Сертификаты сервера)**.

   Откроется окно **Administer Server Certificates (Администрация сертификатов сервера)**.

3. Убедитесь в том, что в столбце **In Use (Используется)** установлен флажок для сертификата, который планируется использовать.

   *Если в столбце **In Use (Используется)** для сертификата, который планируется использовать, уже стоит флажок,* то данная процедура считается завершенной.

   *Если в столбце **In Use (Используется)** для сертификата, который планируется использовать, флажок не стоит,* выполните следующие действия:

   a) Нажмите на предназначенный для использования сертификат для его выделения.
   b) Нажмите кнопку **Modify (Изменить)** в верхней части таблицы.

      Откроется подокно **Modify SSL/KMIP (Изменить SSL/KMIP)**.

   c) Выберите флажок **Current certificate in use (Текущий сертификат используется)**.
   d) Нажмите на **Modify Certificate (Изменить сертификат)**.

      Отобразится всплывающее окно **Warning (Предупреждение)**.

   e) Нажмите на кнопку **OK** во всплывающем окне **Warning (Предупреждение)**.
   f) Остановите и запустите сервер. См. Запуск и остановка сервера EKM 3.0 в Windows или Запуск и остановка сервера EKM 3.0 в Linux.

ПРИМЕЧАНИЕ: Невозможно изменить сертификат каким-либо образом, кроме как установить для него параметр **In Use (Используется)**.

Просмотр подробной информации о сертификате сервера

Если необходимо ознакомиться с подробной информацией о сертификате сервера, выполните следующие действия:

1. Нажмите на сертификат для его выделения:
2. Нажмите кнопку **Modify (Изменить)** в верхней части таблицы.

   Откроется подокно **Modify SSL/KMIP Certificate (Изменить сертификат SSL/KMIP)**.

3. Ознакомьтесь с подробной информацией о сертификате. Для просмотра любых дополнительных параметров можно также нажать на кнопку **Optional Certificate Parameters (Дополнительные параметры Сертификата)**.

Вход на сервер WebSphere

В процессе выполнения некоторых процедур вам требуется входить на сервер WebSphere. В данной главе описывается порядок входа на сервер WebSphere в операционной системе Windows и системах на базе Linux. Входить на сервер WebSphere следует только когда данное действие указано в какой-либо процедуре.

Для входа в сервер WebSphere с помощью команды **wsadmin**:

1. *В операционной системе Windows* в командной строке перейдите к **<*root*>:\Dell\EKM\bin**. *В системах на базе Linux* в окне терминала перейдите к **/opt/dell/ekm/bin**.
2. *Для операционной системы Windows* введите следующую команду:
   ```
   wsadmin -username tklmadmin -password <tklm password> -lang jython
   ```
   Для систем на базе Linux введите следующую команду:
   ```
   ./wsadmin.sh -username tklmadmin -password <tklm password> -lang jython
   ```
   Нажмите на кнопку **Enter (Ввод)**. Команда выполняется в течение непродолжительного времени, и отображается командная строка **wsadmin**.

ПРИМЕЧАНИЕ: Команды чувствительны к регистру. Вокруг круглых или квадратных скобок пробелов нет. Не вводите символы "больше" или "меньше" (< >) вокруг переменных величин.

ПРИМЕЧАНИЕ: Для выхода с сервера WebSphere введите команду **Exit** и нажмите на кнопку **Enter (Ввод)**.

Запуск и остановка сервера EKM 3.0 в Windows

В данной главе описывается порядок запуска и остановки сервера EKM 3.0 в операционной системе Windows/

1. В командной строке перейдите к **<*root*>:\Dell\EKM\bin**.
2. Для запуска сервера введите следующую команду:
   ```
   startserver server1
   ```
   Для остановки сервера введите следующую команду:
   ```
   stopserver server1
   ```
3. Нажмите на кнопку **Enter (Ввод)**.
   Программа выполняется и в командной строке отображается сообщение с подтверждением:
   ```
   Server server1 open for e-business
   ```
   или
   ```
   Server server1 stop completed
   ```

Запуск и остановка сервера EKM 3.0 в Linux

В данной главе описывается порядок запуска и остановки сервера EKM 3.0 на системах на базе Linux.

ПРИМЕЧАНИЕ: Для запуска и остановки сервера вы должны войти в систему как привилегированный пользователь.

1. В окне терминала перейдите к **/opt/dell/ekm/bin**.
2. Для запуска сервера введите следующую команду:
   ```
   ./startserver.sh server1
   ```

Для остановки сервера введите следующую команду:

```
./stopserver.sh server1
```

ПРИМЕЧАНИЕ: Для выполнения остановки сервера вам потребуется ввести имя пользователя и пароль администратора EKM 3.0.

3. Нажмите на кнопку **Enter (Ввод)**.

   Программа выполняется и в окне терминала отображается сообщение с подтверждением:

   ```
   Server server1 open for e-business
   ```

   или

   ```
   Server server1 stop completed
   ```

6

Миграция и слияние

Во время установки EKM 3.0 вы можете выполнить миграцию EKM 2.X в EKM 3.0.

После установки EKM 3.0 вы можете выполнить слияние EKM 2.X с EKM 3.0.

В данной главе описываются процедуры слияния и миграции.

ПРИМЕЧАНИЕ: Можно выполнить миграцию или слияние только для версии EKM 2.X, которая использовалась для создания ключей.

Миграция диспетчера ключей шифрования (EKM) версии 2.X в процессе установки EKM 3.0

Выполняйте данную процедуру только если вы выполняете настройку экрана **Migration (Миграция)** в процессе установки EKM 3.0. Экран **Migration (Миграция)** предназначен для миграции диспетчера ключей шифрования (EKM) версии 2.X в EKM 3.0.

ПРИМЕЧАНИЕ: Если в настоящее время вы используете EKM 2.X, компания Dell рекомендует провести техническое обслуживание вашей текущей инфраструктуры (серверы, операционные системы, ленточные библиотеки и т.д., в которых используется защита EKM 2.X), в противном случае вы не сможете избежать проблем.

Если вам необходимо выполнить миграцию версию EKM 2.X в EKM 3.0, компания Dell рекомендует выполнить процедуру миграции сейчас.

ПРИМЕЧАНИЕ: Если в качестве хост-системы для EKM 2.X вы используете виртуальную машину, вы можете продолжить использование EKM 2.X, или перейти к использованию физического сервера. EKM 3.0 не поддерживает использование виртуальных машин в качестве хост-систем.

ПРИМЕЧАНИЕ: В процессе установки EKM 3.0 можно выполнить миграцию только одной версии EKM 2.X. Если имеется более одной версии EKM 2.X для переноса в EKM 3.0, то выполните миграцию первой с помощью данной процедуры, а затем, когда установка буде завершена, для слияния добавочных версий см. раздел Merging Additional EKM 2.X Versions into EKM 3.0 (Миграция добавочных версий EKM 2.X в EKM 3.0).

Можно выполнить *слияние* версии EKM 2.X с EKM 3.0 после завершения установки EKM 3.0 при помощи утилиты слияния EKM 2.X с EKM 3.0, но компания Dell настоятельно рекомендует выполнить слияние в данный момент.

ПРИМЕЧАНИЕ: Если используется конфигурация с основным/дополнительным сервером EKM 3.0, то процедуру миграции следует выполнить только на основном сервере EKM 3.0.

После завершения миграции создайте резервную копию сервера EKM 3.0 и используйте данный резервный файл для восстановления на дополнительном сервере EKM 3.0 и обеспечения соответствия данных содержимому основного сервера EKM 3.0.

Для выполнения миграции с EKM 2.X в процессе установки EKM 3.0, перейдите к разделу EKM 2.X to EKM 3.0 Migration Procedure (Процедура миграции EKM 2.X в EKM 3.0).

Процедура миграции EKM 2.X в EKM 3.0

Для миграции версии EKM 2.X в EKM 3.0 из окна **Migration (Миграция)** в процессе установки EKM 3.0 выполните следующие действия:

1. Войдите в консоль EKM 2.X, создайте резервную копию хранилища ключей EKM 2.X, остановите сервер EKM 2.X и выйдите из консоли EKM 2.X. Более подробную информацию см. в руководстве пользователя EKM 2.X.
2. Скопируйте папку EKM 2.X:

   Если ваш сервер EKM 2.X установлен не на одной с конечным устанавливаемым EKM 3.0 машине, скопируйте папку EKM 2.X на сервере EKM 2.X во временную папку на сервере EKM 3.0 (например, **C:\temp \MyEKM2** для операционной системы Windows, или **/opt/myekm2** для платформ на основе Linux).

   Если ваш сервер EKM 2.X установлен на одной с конечным устанавливаемым EKM 3.0 машине, все равно необходимо создать копию папки EKM 2.X на данной машине.
3. В окне **Migration (Миграция)** в процессе установки EKM 3.0 установите отметку для флажка **Migrate from EKM 2.X to EKM 3.0 (Мигрировать из EKM 2.X в EKM 3.0)**.

4. Нажмите **Choose (Выбрать)** и перейдите в каталог, в который ранее была скопирована папка EKM 2.X. Не выбирайте что-либо ниже данной папки.

ОСТОРОЖНО: Если ваш сервер EKM 2.X установлен на одной с конечным устанавливаемым EKM 3.0 машине, то не выполняйте переход в каталог, в который установлен EKM 2.X, так как установщик EKM 3.0 определяет использованную для установки папку. Перейдите в копию каталога EKM 2.X, которая была создана ранее.

5. Нажмите на кнопку **Next (Далее)**.

   Откроется экран **Configuration Summary (Обзор конфигурации)**.

ПРИМЕЧАНИЕ: В случае отображения сообщения об ошибке проверьте путь к разделу EKM 2.X.

6. Продолжайте процедуру установки EKM 3.0. См. раздел Performing the EKM 3.0 Installation Procedure (Выполнение процедуры установки EKM 3.0).

ПРИМЕЧАНИЕ: Пароль к новому хранилищу паролей EKM 3.0 является тот же пароль, который был назначен для хранилища ключа мигрируемого EKM 2.X.

ОСТОРОЖНО: Не запускайте EKM 2.X после миграции его ключей в EKM 3.0. При необходимости можно удалить EKM 2.X после успешного завершения миграции из EKM 2.X в EKM 3.0. Компания Dell рекомендует создать резервную копию файлов EKM 2.X перед удалением EKM 2.X.

Слияние диспетчера ключей шифрования (EKM) 2.X с EKM 3.0 после установки EKM 3.0

В данной главе описывается процедура слияния EKM 2.X с EKM 3.0 после завершения процедуры установки для операционной системы Windows и систем на базе Linux. В данной процедуре используется утилита слияния EKM 2.X с EKM 3.0.

Применяйте данную процедуру, если EKM 3.0 уже установлен и настроен, а вы хотите выполнить слияние EKM 2.X с EKM 3.0.

ПРИМЕЧАНИЕ: Если используется конфигурация с основным/дополнительным сервером EKM 3.0, то процедуру слияния следует выполнить только на основном сервере EKM 3.0. После завершения процедуры слияния на основном сервере EKM 3.0, выполните процедуру создания резервной копии, а затем восстановите данные из данного файла резервной копии на дополнительном сервере EKM 3.0. См. раздел Performing Backups and Restoring from a Backup (Создание резервной копии и восстановление с помощью резервной копии).

ПРИМЕЧАНИЕ: Если EKM 3.0 еще не установлен, компания Dell рекомендует выполнять слияние EKM 2.X с EKM 3.0 в процессе выполнения установки EKM 3.0. См. раздел Performing the EKM 3.0 Installation Procedure (Выполнение процедуры установки EKM 3.0).

В качестве примеров в данном документе приведены стандартные для операционной системы Windows пути (например, **C:\<*имя папки*>**). Вставьте соответствующую букву диска или путь Linux для вашей системы.

Необходимые условия для утилиты миграции

Перед запуском утилиты миграции убедитесь в том, что выполнены следующие требования:

- EKM 3.0 должен быть установлен и главное хранилище ключей должно быть создано, иначе процедура слияния закончится ошибкой. См. раздел Creating a Master Keystore (Создание главного хранилища ключей).
- В случае миграции EKM 2.X в EKM 3.0, как EKM 2.X, так и EKM 3.0 должны быть установлены в операционной системе одной версии.
- Если вы ранее выполняли процесс слияния или миграции EKM 2.X в EKM 3.0, то полученный в результате миграции сертификат **ekmcert** по прежнему будет сохранен на сервере EKM 3.0, и может быть сохранен даже после выполнения восстановления из предыдущей резервной копии. Необходимо удалить сертификат **ekmcert** с сервера EKM 3.0 до выполнения процедуры слияния. См. раздел Deleting the ekmcert Certificate, Keys, and Key Groups, and Renaming Devices (Удаление сертификата ekmcert, ключей и групп ключей, а также переименование устройств).
- Необходимо переименовать дубликаты ключей, групп ключей и устройств в EKM 2.X до их миграции в EKM 3.0. См. руководство пользователя EKM 2.X.
  - Совпадений псевдонимов/имен ключа из исходного EKM 2.X в конечном EKM 3.0 быть не может. Каждый входящий ключ должен иметь уникальный псевдоним/имя, в противном случае процедура слияния завершиться ошибкой.
  - Совпадений псевдонимов/имен *группы* ключа из исходного EKM 2.X в конечном EKM 3.0 быть не может. Каждая входящая группа ключа должна иметь уникальный псевдоним/имя, в противном случае процедура слияния завершиться ошибкой.
  - Совпадений устройств из исходного EKM 2.X в конечном EKM 3.0 быть не может, в противном случае процедура слияния завершиться ошибкой

Процедура слияния EKM 2.X с EKM 3.0

Для запуска утилиты миграции выполните следующие действия:

1. Войдите в портал EKM 3.0. См. Вход в портал диспетчера ключей шифрования Encryption Key Manager 3.0.

   Откроется окно приветствия **Welcome to Dell Encryption Key Manager**.
2. На сервере EKM 3.0 создайте резервную копию EKM 3.0. Информацию о процедуре по созданию резервных копий см. в разделе Performing Backups and Restoring from a Backup (Создание резервной копии и восстановление с помощью резервной копии).

   Если работа утилиты слияния завершается ошибкой или повреждением каких-либо данных EKM 3.0, можно использовать данную резервную копию для восстановления любой потерянной информации.
3. Выйдите из EKM 3.0.
4. Остановите сервер EKM 3.0 перед запуском утилиты слияния. См. раздел Starting and Stopping the EKM 3.0 Server in Windows (Запуск и остановка сервера EKM 3.0 в Windows) или Starting and Stopping the EKM 3.0 Server in Linux (Запуск и остановка сервера EKM 3.0 в Linux).
5. На системном диске сервера EKM 3.0 создайте подходящую папку (например, **C:\EKM_Files** для ОС Windows, или **/opt/EKM_Files** для систем на базе Linux).
6. Войдите в консоль EKM 2.X, создайте резервную копию хранилища ключей EKM 2.X, остановите сервер EKM 2.X и выйдите из консоли EKM 2.X. См. руководство пользователя EKM 2.X.
7. Из места установки EKM 2.X скопируйте следующие файлы в папку, созданную на сервере EKM 3.0 во время предыдущего действия. Если EKM 2.X установлена на другой физической системе, используйте съемный диск или сетевую папку сервера той же операционной системы.
   - В операционной системе Windows из **<*root*>:\ekm\gui** скопируйте **EKMKeys.jck**. В системе на базе Linux данный файл расположен в **/var/ekm/gui**.

- В операционной системе Windows из **<*root*>:\ekm\gui** скопируйте **KeyManagerConfig.properties** (это файл конфигурации EKM). В системе на базе Linux данный файл расположен в **/var/ekm/gui**.
- В операционной системе Windows из **<*root*>:\ekm\gui\keygroups** скопируйте **keygroup.xml**. В системе на базе Linux данный файл расположен в **/var/ekm/gui/keygroups**.
- В операционной системе Windows из **<*root*>:\ekm\gui\drivetable** скопируйте **ekm_drivetable.dt**. В системе на базе Linux данный файл расположен в **/var/ekm/gui/drivetable**.

ОСТОРОЖНО: В операционной системе Windows для создания или редактирования текстовых файлов используйте приложение Notepad (Блокнот). В случае использования приложения Wordpad данная процедура завершиться ошибкой.

8. Измените файл **KeyManagerConfig.properties** таким образом, чтобы он содержал только следующие параметры:

   - **config.keygroup.xml.file**
   - **config.keystore.password.obfuscated**
   - **config.keystore.file**
   - **config.drivetable.file.url**

   Остальные строки удалите. Пример см. в Пример кода в данной процедуре.

9. Добавьте в новый файл **KeyManagerConfig.properties** следующие параметры DB2:

   - jdbcURL = jdbc:db2://localhost:<порт базы данных *EKM 3.0 DB2 database port*>/<*имя базы данных EKM 3.0 DB2*>

     или

     jdbcURL = jdbc:db2://<*IP-адрес сервера EKM 3.0*>:<*порт базы данных EKM 3.0 DB2*>/<*имя базы данных EKM 3.0 DB2*>
   - jdbcUID = <*имя пользователя администратора DB2*>
   - jdbcPW = <*пароль администратора DB2*>
   - dbType = DB2

   Пример см. в Пример кода в данной процедуре.

ПРИМЕЧАНИЕ: Переменные величины – это настраиваемые в процессе установки EKM 3.0 параметры. Не вводите символы больше или меньше (< >) вокруг переменных величин. Переменные величины, имена пользователей и пароли чувствительны к регистру.

10. Добавьте строку пароля для хранилища ключей EKM 3.0 по умолчанию в файл **KeyManagerConfig.properties**. Строка пароля следующая:

    tklm.encryption.password = <*пароль хранилища ключей ekm 3.0*>.

    Обновленный файл **KeyManagerConfig.properties** должен выглядеть аналогично следующему примеру:

Пример кода для операционной системы Windows

```
config.keygroup.xml.file = File:c:\\<EKM_Files>\
\KeyGroups.xml config.keystore.password.obfuscated =
38087C9DA4A4696A6B6C config.keystore.file = c:\
\<EKM_Files>\\EKMKeys.jck config.drivetable.file.url =
File:c:\\<EKM_Files>\\ekm_drivetable.dt jdbcURL =
jdbc:db2://localhost:50010/ekm_dell jdbcUID = ekmdell1
jdbcPW = Dell1234 dbType = DB2 tklm.encryption.password =
Dell1234
```

Где *EKM_Files* – это папка, которая была создана ранее.

Пример кода для системы на базе Linux

```
config.keygroup.xml.file = File:/opt/<EKM_Files>/KeyGroups.xml
config.keystore.password.obfuscated = 38087C9DA4A4696A6B6C
config.keystore.file = /opt/<EKM_Files>/EKMKeys.jck
config.drivetable.file.url = File:/opt/<EKM_Files>/
ekm_drivetable.dt jdbcURL = jdbc:db2://localhost:50010/
ekm_dell jdbcUID = ekmdell1 jdbcPW = Dell1234 dbType = DB2
tklm.encryption.password = Dell1234
```

Где *EKM_Files* – это папка, которая была создана ранее.

11. Перейдите в папку **EKM2DKMMerge** на установочном носителе EKM 3.0. Из папки **EKM2DKMMerge** скопируйте файл **EKM2DKMMerge.jar** в папку, которая была создана ранее во время выполнения данного действия (например, C:\EKM_Files для операционной системы Windows, или /opt/EKM_Files для системы на базе Linux).

ПРИМЕЧАНИЕ: Для всех следующих действий необходимо использовать одну командную строку или окно терминала. Если изменить командные строки или окна терминалов, настраиваемый CLASSPATH не будет автоматически применен к другим командным строкам или окнам терминала.

12. На сервере EKM 3.0 настройте пути доступа для WAS и TIP, которые необходимы для работы утилиты слияния.

В операционной системе Windows:

a. В командной строке перейдите к **<*root*>:\Dell\EKM\bin**.

b. Для запуска сценария командной строки введите следующую команду:

```
setupCmdLine.bat
```

Пример:

```
C:\Dell\EKM\bin\setupCmdLine.bat
```

c. Нажмите на кнопку **Enter (Ввод)**. Команда выполняется и система отображает следующее сообщение в последней строке:

```
goto :EOF
```

На платформах Linux:

a. В окне терминала перейдите к **/opt/dell/ekm/bin**.

b. Введите следующую команду:

```
. setupCmdLine.sh
```

c. Команда выполняется. После успешного выполнения команды в системе на базе Linux отображается пустая строка. Индикатор завершения работы команды отсутствует.

ПРИМЕЧАНИЕ: У сценария **setupCmdLine.sh** должны быть полномочия на выполнение.

13. Создайте пакетный файл (.bat) командной строки (для систем на базе Linux, .sh) для получения доступа к необходимым для утилиты слияния .jar-файлам и для настройки дополнительных параметров для CLASSPATH:

a) Скопируйте следующую временную настройку CLASSPATH в текстовый файл и присвойте имя <*filename*>.bat или для системы на базе Linux, <*filename*>.sh (например, **setupclasspath.bat** для операционной системы Windows, или **setupclasspath.sh** для системы на базе Linux).

b) Сохраните файл .bat/.sh в созданной ранее во время выполнения данного действия папке, например, C:\EKM_Files или /opt/EKM_Files.

ОСТОРОЖНО: В операционной системе Windows для создания или редактирования текстовых файлов используйте приложение Notepad (Блокнот). В случае использования приложения Wordpad данная процедура завершиться ошибкой.

c) Измените пакетный файл:

Для операционной системы Windows, измените пакетный файл таким образом, чтобы заменить ***c:\EKM\Needed*** на путь к месту, в который вы поместили файл **EKM2DKMMerge.jar**, например **c:\EKM_Files**.

Для систем на базе Linux, измените сценарий командного процессора таким образом, чтобы заменить **/opt/EKM_Files** на путь к месту, в которое вы поместили файл **EKM2DKMMerge.jar**.

Временная настройка CLASSPATH для операционной системы Windows

```
set JAVA_HOME=%WAS_HOME%\java set PATH=%JAVA_HOME%\bin;%JAVA_HOME%\jre
\bin;%PATH% set CLASSPATH=c:\EKM\Needed\EKM2DKMMerge.jar;%CLASSPATH% set
CLASSPATH=.;%WAS_HOME%\plugins\com.ibm.icu_3.4.5.jar;%WAS_HOME%\products
\tklm\migration\j2ee.jar;%WAS_HOME%\plugins\com.ibm.tklm.commands.jar;
%WAS_HOME%\products\tklm\migration\com.ibm.tklm.kmip.adapter.jar;%WAS_HOME
%\profiles\TIPProfile\installedApps\TIPCell\tklm_kms.ear
\com.ibm.tklm.kmip.jar;"C:\Program Files\Dell\db2dkm\java\db2jcc.jar";"C:
\Program Files\Dell\db2dkm\java\db2jcc_license_cu.jar";%WAS_HOME%\profiles
\TIPProfile\installedApps\TIPCell\tklm_kms.ear\com.ibm.tklm.keyserver.jar;
%WAS_HOME%\profiles\TIPProfile\installedApps\TIPCell\tklm_kms.ear
\com.ibm.tklm.server.api.jar;%WAS_HOME%\profiles\TIPProfile\installedApps
\TIPCell\tklm_kms.ear\com.ibm.tklm.server.db.ejb.jar;%CLASSPATH%
```

ПРИМЕЧАНИЕ: При необходимости, замените буквы дисков.

ПРИМЕЧАНИЕ: Если используется 64–битная версия Windows, измените пакетный файл таким образом, чтобы заменить **Program Files** в CLASSPATH выше на **Program Files (x86)**.

Временная настройка CLASSPATH для системы на базе Linux

```
export JAVA_HOME=$WAS_HOME/java export PATH=${JAVA_HOME}/bin:${JAVA_HOME}
$/jre/bin:$PATH export CLASSPATH=/opt/EKM_Files/EKM2DKMMerge.jar:
$CLASSPATH export CLASSPATH=.:$WAS_HOME/plugins/com.ibm.icu_3.4.5.jar:
$WAS_HOME/products/tklm/migration/j2ee.jar:$WAS_HOME/plugins/
com.ibm.tklm.commands.jar:$WAS_HOME/products/tklm/migration/
com.ibm.tklm.kmip.adapter.jar:$WAS_HOME/profiles/TIPProfile/installedApps/
TIPCell/tklm_kms.ear/com.ibm.tklm.kmip.jar:/opt/dell/db2ekm/java/
db2jcc.jar:/opt/dell/db2ekm/java/db2jcc_license_cu.jar:$WAS_HOME/profiles/
TIPProfile/installedApps/TIPCell/tklm_kms.ear/com.ibm.tklm.keyserver.jar:
$WAS_HOME/profiles/TIPProfile/installedApps/TIPCell/tklm_kms.ear/
com.ibm.tklm.server.api.jar:$WAS_HOME/profiles/TIPProfile/installedApps/
TIPCell/tklm_kms.ear/com.ibm.tklm.server.db.ejb.jar:$CLASSPATH
```

14. Запустите пакетный файл, который вы только что создали. В одной командной строке или окне терминала на сервере EKM 3.0 перейдите в папку, которая была создана ранее во время выполнения данного действия (например, C:\EKM_Files для операционной системы Windows, или /opt/EKM_Files для системы на базе Linux), и выполните пакетный файл, который вы создали во время предыдущего действия. В системе на базе Linux, введите текстовый файл, который был создан ранее, например, . setupclasspath.sh.

15. В одной командной строке или окне терминала на сервере EKM 3.0 выполните следующую команду Java:

```
java<space>com.ibm.tklm.ekm2tklm.MergeEKM2KLM<space>KeyManagerConfig.propert
ies
```

ПРИМЕЧАНИЕ: Команды чувствительны к регистру. Не вводите символы "больше" или "меньше" (< >) вокруг переменных величин.

Файл **KeyManagerConfig.properties** – это тот файл, который вы изменяли ранее во время выполнения данного действия.

Данная команда выполняет слияние EKM 2.X с EKM 3.0.

После успешного выполнения отображается следующее сообщение:

```
TKLM version: 2.0.0.0 201007241325Starting EKM to KLM MergeKMSDebug.init,
debug output filename not specified: using defaultCTGKS0250I: Successfully
migrated the Encryption Key Manager keystores, certificates and
keys.CTGKS0251I: Successfully migrated the Encryption Key Manager key
groups.CTGKS0249I: Successfully migrated the Encryption Key Manager
devices.Migration Complete.
```

ПРИМЕЧАНИЕ: В случае получения ошибок просмотрите журнал для определения причины. Также можно сохранить журнал отладки в другое место или переименовать его для того, чтобы сохранить в статичном виде, в противном случае утилита слияния EKM 2.X с EKM 3.0 будет добавлять в него данные. В операционной системе Windows журнал отладки расположен в следующем каталоге на сервере EKM 3.0: **<*root*>:\Dell\EKM\bin\products\tklm\logs\debug.log**. В системах на базе Linux журнал отладки расположен в следующем каталоге на сервере EKM 3.0: **/opt/dell/ekm/bin/products/tklm/logs/debug.log**.

ПРИМЕЧАНИЕ: Если вы получите следующую ошибку, это значит, что вы пытаетесь выполнить миграцию при наличии дубликата на сервере EKM 2.X и сервере EKM 3.0.

```
Duplicate <item> = <item> Migration failed. Please refer to the debug file
for more information (Дубликат <item> = <item> Ошибка миграции. Более
подробную информацию см. в файле отладки).
```

См. раздел Deleting the ekmcert Certificate, Keys, and Key Groups, and Renaming Devices (Удаление сертификата ekmcert, ключей и групп ключей, а также переименование устройств)

Если вы получите следующее сообщение об ошибке и не желаете удалять ключ вместо его переименования, не закрывайте командную строку или окно терминала. Вам потребуется скопировать псевдоним данного ключа из командной строки или окна терминала.

```
Duplicate Key Alias= <key alias> (Дубликат псевдонима ключа= <псевдоним
ключа> )
```

См. раздел Deleting the ekmcert Certificate, Keys, and Key Groups, and Renaming Devices (Удаление сертификата ekmcert, ключей и групп ключей, а также переименование устройств)

ОСТОРОЖНО: Удаление ключа эквивалентно удалению любых данных, защищенных с помощью данного ключа, так как к этим данным невозможно будет получить доступ. Для обеспечения безопасности удаленные ключи невозможно восстановить каким-либо способом.

16. Запустите сервер EKM 3.0 с помощью команды **startserver**. См. раздел Starting and Stopping the EKM 3.0 Server in Windows (Запуск и остановка сервера EKM 3.0 в Windows) или Starting and Stopping the EKM 3.0 Server in Linux (Запуск и остановка сервера EKM 3.0 в Linux).

17. Убедитесь в том, что группы ключей, ключи и устройства EKM 2.X мигрировали в EKM 3.0. См. раздел Verifying the EKM 2.X to EKM 3.0 Merge or Migration (Проверка выполнения слияния или миграции EKM 2.X в EKM 3.0). Если процедура слияния завершилась успешно, то процедура завершена. Если вы хотите выполнить слияние добавочных версий EKM 2.X в EKM 3.0, см. раздел Merging Additional EKM 2.X Versions into EKM 3.0 (Миграция добавочных версий EKM 2.X в EKM 3.0). Если процедура слияния завершилась ошибкой, см. раздел Merge Failure (Ошибка слияния).

ОСТОРОЖНО: Не запускайте EKM 2.X после слияния его ключей с EKM 3.0. При необходимости можно удалить EKM 2.X после успешного завершения слияния EKM 2.X с EKM 3.0. Компания Dell рекомендует создать резервную копию файлов EKM 2.X перед удалением EKM 2.X.

Проверка выполнения слияния или миграции EKM 2.X в EKM 3.0

В данной главе описывается способ проверки того, процедура слияния или миграции EKM 2.X в EKM 3.0 завершилась успешно, а также что ленточные библиотеки работают исправно.

Для проверки того, что слияние или перенос EKM 2.X в EKM 3.0 завершился успешно, выполните следующие действия:

1. Войдите в портал EKM 3.0. См. Вход в портал диспетчера ключей шифрования Encryption Key Manager 3.0.
   Откроется окно приветствия **Welcome to Dell Encryption Key Manager**.

2. В панели навигации перейдите к **Dell Encryption Key Manager (Диспетчер ключей шифрования Dell) → Key and Device Management (Управление ключами и устройствами)** .

Появится экран **Key and Device Management (Управление ключами и устройствами)**.

3. В выпадающем меню **Manage keys and devices (Управлять ключами и устройствами)** выберите **LTO** и нажмите на кнопку **Go (Выполнить)**.

   На экране **Key and Device Management (Управление ключами и устройствами)** отобразится перенесенная группа (группы) ключей EKM с указанием количества ключей в каждой группе.

4. В выпадающем меню в верхней части таблицы выберите **View Keys, Key Group Membership and Drives (Показать ключи, состав группы ключей и диски)**. Если ключ отображается в левой части таблицы, то процесс слияния завершился успешно.

5. В процессе миграции не происходит импорт настроенный в EKM 2.X устройств. Необходимо выполнить настройку устройств EKM 2.X. См. раздел Adding a Device to a Device Group (Добавление устройства в группу устройства).

6. В портале EKM 3.0 убедитесь в том, что настройка EKM 3.0 допускает автоматический прием запросов от устройств. Настройка на экране **Key and Device Management (Управление ключами и устройствами)** должна быть следующей: **Automatically accept all new device requests for communication (Автоматический прием запросов на установление связи от всех новых устройств)**.

7. Проверьте устройства в вашей библиотеке:
   a) Убедитесь в том, что порт SSL и порт TCP в вашей ленточной библиотеке настроены правильно.
   b) Запустите проведение проверки пути к ключу из вашей ленточной библиотеки для проверки конфигурации ленточной библиотеки.

ПРИМЕЧАНИЕ: Подробную информацию см. в руководстве пользователя ленточной библиотеки. Информацию о расположении руководства пользователя ленточной библиотеки см. раздел Documentation and Reference Materials (Документация и справочная информация) файла **ReadThisFirst.txt** на установочном носителе EKM 3.0.

Ошибка слияния

Если процедура слияния завершается ошибкой, выполните следующие действия:

1. Убедитесь в том, что сервер EKM 3.0 запущен. В противном случае запустите сервер EKM 3.0 с помощью команды **startserver**. См. раздел Starting and Stopping the EKM 3.0 Server in Windows (Запуск и остановка сервера EKM 3.0 в Windows) или Starting and Stopping the EKM 3.0 Server in Linux (Запуск и остановка сервера EKM 3.0 в Linux).

2. Закройте командную строку.

3. Зафиксируйте журнал отладчика, для чего сохраните его в другую папку или переименуйте.

   Журнал отладчика расположен в следующем каталоге: **<*root*>:\Dell\EKM\bin\products\tklm\logs\debug.log** для ОС Windows, или **/opt/dell/ekm/bin/products/tklm/logs/debug.log** для платформ на базе Linux.

4. Восстановите EKM 3.0 через портал EKM 3.0 из резервной копии, которая была создана в процессе выполнения первого действия в EKM 2.X to EKM 3.0 Merge Procedure (Процедура слияния EKM 2.X с EKM 3.0). Для получения указаний по восстановлению данных из резервной копии, см. раздел Restoring from a Backup (Восстановление из резервной копии).

5. Повторите процедуру слияния. См. раздел EKM 2.X to EKM 3.0 Merge Procedure (Процедура слияния EKM 2.X с EKM 3.0).

Миграция добавочных версий EKM 2.X в EKM 3.0

Выполните данную процедуру, если вы выполнили миграцию или слияние EKM 2.X в EKM 3.0, и необходимо мигрировать добавочные версии EKM 2.X в EKM 3.0.

1. Удалите сертификат **ekmcert** из EKM 3.0. См. раздел Deleting the ekmcert Certificate, Keys, and Key Groups, and Renaming Devices (Удаление сертификата ekmcert, ключей и групп ключей, а также переименование устройств.
2. Выполните процедуру слияния для каждой добавочной версии EKM 2.X, которую необходимо объединить. См. раздел EKM 2.X to EKM 3.0 Merge Procedure (Процедура слияния EKM 2.X с EKM 3.0).

Удаление сертификата ekmcert, ключей и групп ключей, а также переименование устройств

В процессе слияния EKM 2.X с EKM 3.0 не допускается наличие дубликатов сертификатов **ekmcert**, псевдонимов ключей, псевдонимов групп ключей или устройств в EKM 2.X и на сервере EKM 3.0.

ПРИМЕЧАНИЕ: Если дубликаты ключей или групп ключей имеются, то компания Dell рекомендует переименовать такие ключи и группы ключей в EKM 2.X до слияния их с EKM 3.0. Для получения более подробной информации см. руководство пользователя EKM 2.X. Если дубликаты ключей или групп ключей не используются, то можно их удалить из EKM 2.X. Однако удаление ключа эквивалентно удалению любых данных, защищенных с помощью данного ключа, так как к этим данным невозможно будет получить доступ. Для обеспечения безопасности удаленные ключи невозможно восстановить каким-либо способом.

Если имеются дубликаты устройств, необходимо удалить их из EKM 2.X.

Если вы получили следующую ошибку в процессе выполнения процедуры слияния, удалите соответствующий объект на основании приведенной в сообщении об ошибке информации.

`Duplicate <item> = <item> Migration failed. Please refer to the debug file for more information (Дубликат <item> = <item> Ошибка миграции. Более подробную информацию см. в файле отладки).`

См. соответствующий раздел:

- Удаление сертификата ekmcert
- Удаление определенного ключа
- Удаление устройства

ekmcert Certificate Deletion (Удаление сертификата ekmcert)

Для каждой установки EKM 2.X имеется один сертификат **ekmcert**. Если вы выполняете слияние или миграцию более одного EKM 2.X в EKM 3.0, необходимо удалить сертификат **ekmcert** в EKM 3.0 до начала процедуры слияния с новым EKM 2.X.

Из-за того, что **ekmcert** является сертификатом, а не ключом, он не входит в какую-либо группу ключей на сервере EKM 3.0. Поэтому, если вы выполнили миграцию версии EKM 2.X в EKM 3.0, а затем удалили группы ключей EKM 2.X из EKM 3.0, полученный в результате миграции сертификат **ekmcert** по прежнему будет сохранен на сервере EKM 3.0, и может быть сохранен даже после выполнения восстановления из предыдущей резервной копии. Из-за того, что утилита миграции пытается повторно добавить сертификат **ekmcert**, процесс миграции будет завершен ошибкой.

Необходимо удалить сертификат **ekmcert** с сервера EKM 3.0 в случае возникновения одной из следующих ситуаций:

- Вы мигрировали EKM 2.X в EKM 3.0 в процессе установки EKM 3.0
- Вы выполняли миграцию EKM 2.X в EKM 3.0 не первый раз
- Вам необходимо удалить ранее мигрированную или мигрированную версию EKM 2.X
- При попытке выполнения процедуры миграции вы получаете следующую ошибку. Данная ошибка указывает на наличие сертификата **ekmcert** в EKM 3.0:

  ```
  Duplicate Key Alias = ekmcert Migration failed (Двойной псевдоним ключа =
  ошибка миграции ekmcert). Более подробную информацию см. в файле
  отладчика.
  ```

Для удаления сертификата **ekmcert** см. раздел Deleting the ekmcert Certificate (Удаление сертификата ekmcert).

Удаление сертификата ekmcert

Для проверки того, что сертификат **ekmcert** имеется в EKM 3.0, и удалить его выполните следующие действия:

1. Войдите в портал EKM 3.0. См. Вход в портал диспетчера ключей шифрования Encryption Key Manager 3.0.

   Откроется окно приветствия **Welcome to Dell Encryption Key Manager**.

2. В панели навигации перейдите к **Dell Encryption Key Manager (Диспетчер ключей шифрования Dell)** → **Advanced Configuration (Дополнительная настройка)** → **Server Certificates (Сертификаты сервера)**.

   Откроется окно **Administer Server Certificates (Администрация сертификатов сервера)**.

3. На экране **Administer Server Certificates (Администрация сертификатов сервера)** убедитесь в том, что сертификат **ekmcert** приведен в списке и в настоящий момент не используется.

   Если сертификат **ekmcert** в настоящий момент не используется, переходите к выполнению следующего действия. Если сертификат **ekmcert** в настоящее время используется, выполните следующие действия:

   a) Выберите сертификат **ekmcert**.
   b) Нажмите на кнопку **Modify (Изменить)**.
   c) Уберите флажок **Current certificate in use (Текущий сертификат используется)**.
   d) Нажмите на **Modify Certificate (Изменить сертификат)**.

      Отобразится окно **Administer Server Certificates (Администрация сертификатов сервера)**. Сертификат отобразится как неиспользуемый.

4. Повторно выберите сертификат **ekmcert**.

5. Нажмите кнопку **Delete (Удалить)** в верхней части таблицы.

   Откроется окно с запросом на подтверждение.

6. Нажмите на кнопку **OK**, чтобы удалить сертификат.

   Сертификат удален из списка.

Удаление определенного ключа

В данной главе описывается способ удаления определенного ключа. Связанный с устройством ключ удалить невозможно.

ОСТОРОЖНО: Удаление ключа эквивалентно удалению любых данных, защищенных с помощью данного ключа, так как к этим данным невозможно будет получить доступ. Для обеспечения безопасности удаленные ключи невозможно восстановить каким-либо способом.

ПРИМЕЧАНИЕ: Если вы получили сообщение об ошибке наличия двух одинаковых ключей во время выполнения миграции из EKM 2.X в EKM 3.0, компания Dell рекомендует переименовать второй ключ в EKM 2.X. Более подробную информацию см. в руководстве пользователя EKM 2.X.

1. Войдите в портал EKM 3.0. См. Вход в портал диспетчера ключей шифрования Encryption Key Manager 3.0.

   Откроется окно приветствия **Welcome to Dell Encryption Key Manager**.
2. В панели навигации перейдите к **Dell Encryption Key Manager (Диспетчер ключей шифрования Dell) → Key and Device Management (Управление ключами и устройствами)** .

   Появится экран **Key and Device Management (Управление ключами и устройствами)**.
3. В выпадающем меню **Manage keys and devices (Управлять ключами и устройствами)** выберите **LTO** и нажмите на кнопку **Go (Выполнить)**.

   Появится экран **Key and Device Management (Управление ключами и устройствами)**.
4. В выпадающем меню в верхней части таблицы выберите **View Keys, Key Group Membership and Drives (Показать ключи, состав группы ключей и диски)**.

   В таблице отобразятся ключи.
5. Нажмите на предназначенный для удаления ключ для его выделения.
6. Нажмите кнопку **Delete (Удалить)** в верхней части таблицы.

   Откроется всплывающее окно с запросом на подтверждение.
7. Если ы уверенны в необходимости удаления выбранного ключа, ,нажмите на кнопку **OK**.

   Ключ удален.

Удаление устройства

В данной главе описывается способ удаления устройства. Устройство – это отдельный диск, установленный в ленточную библиотеку. Серийный номер отображается на правой стороне ленточного диска.

ПРИМЕЧАНИЕ: Если вы получили сообщение об ошибке наличия двух одинаковых устройств во время выполнения миграции из EKM 2.X в EKM 3.0, компания Dell рекомендует удалить устройство в EKM 2.X. Более подробную информацию см. в руководстве пользователя EKM 2.X.

Для удаления устройства из EKM 3.0 выполните следующие действия:

1. Войдите в портал EKM 3.0. См. Вход в портал диспетчера ключей шифрования Encryption Key Manager 3.0.

   Откроется окно приветствия **Welcome to Dell Encryption Key Manager**.
2. В панели навигации перейдите к **Dell Encryption Key Manager (Диспетчер ключей шифрования Dell) → Key and Device Management (Управление ключами и устройствами)** .

   Появится экран **Key and Device Management (Управление ключами и устройствами)**.
3. В выпадающем меню **Manage keys and devices (Управлять ключами и устройствами)** выберите группу устройств, в которую входит предназначенное для удаления устройство.
4. Нажмите **Go (Вперед)**.

   Отображается перечень устройств, входящих в группу устройств.
5. Нажмите на предназначенное для удаления устройство для его выделения.

6. Нажмите кнопку **Delete (Удалить)** в верхней части таблицы.

   Откроется всплывающее окно с запросом на подтверждение.

7. Нажмите на кнопку **OK** во всплывающем окне.

   Устройство удалено.

Проверка удаления библиотеки хранилища ключей EKM 2.X из EKM 3.0

Данная процедура не является обязательной. В данной главе описывается способ проверки удаления всех записей хранилища ключей EKM 2.X (сертификат **ekmcert** и ключи в хранилище ключей EKM 2.X) из сервера EKM 3.0. Для чего выполните следующие действия:

1. В командной строке или окне терминала на сервере EKM 3.0 перейдите в папку, созданную во время процедуры EKM 2.X to EKM 3.0 Merge Procedure (Процедура слияния EKM 2.X с EKM 3.0) (например, **C:\EKM_Files** в операционной системе Windows, или **/opt/EKM_Files** в системах на базе Linux).
2. Убедитесь в том, что утилита Java SDK **keytool** доступна в пути командной строки.
3. Отобразите список содержимого хранилища ключей EKM 2.X с помощью следующей команды:

   ```
   keytool -list -keystore <EKM_2.X_имя_хранилища_ключей> -storetype JCEKS
   ```

   где <*EKM_ 2.X_имя_хранилища_ключей*> – это имя импортируемого хранилища ключей EKM 2.X.

   Например:

   keytool -list -keystore *EKMKeys.jck* -storetype JCEKS

   Система предложит ввести пароль.

4. Введите пароль хранилища ключей EKM 2.X и нажмите на кнопку **Enter (Ввод)**.

   Отображается тип хранилища ключей EKM 2.X, сертификат **ekmcert**, провайдер хранилища ключей, а также ключи в хранилище ключей EKM 2.X. Список ключей будет использован для сравнения с хранилищем ключей EKM 3.0 для проверки того, что данные ключи не находятся в хранилище ключей EKM 3.0.

ПРИМЕЧАНИЕ: Командную строку не закрывайте. На последующем этапе будет выполняться поиск этих ключей и/или сертификата **ekmcert** в хранилище ключей EKM 3.0 для проверки их удаления из EKM 3.0.

5. Запустите сервер EKM 3.0 с помощью команды **startserver**. См. раздел Starting and Stopping the EKM 3.0 Server in Windows (Запуск и остановка сервера EKM 3.0 в Windows) или Starting and Stopping the EKM 3.0 Server in Linux (Запуск и остановка сервера EKM 3.0 в Linux).
6. *В командной строке Windows* перейдите к **<*root*>:\Dell\EKM\bin**. *В системе на базе Linux* перейдите к **/opt/dell/ekm/bin**.
7. Зайдите на сервер WebSphere с помощью команды **wsadmin**. См. раздел Logging onto the WebSphere Server (Вход на сервер WebSphere).
8. В поле **wsadmin** при помощи полученного ранее псевдонима ключа введите одну из следующих команд для вывода определенного ключа или сертификата на сервере EKM 3.0:

   Для ключей:

   ```
   print AdminTask.tklmKeyList('[-alias <псевдоним ключа>]')
   ```

   Для сертификата **ekmcert**:

   ```
   print AdminTask.tklmKeyList('[-alias ekmcert]')
   ```

ПРИМЕЧАНИЕ: Вы получили псевдонимы ключей во время предыдущего действия. В ОС Windows можно копировать псевдонимы с помощью панели инструментов в окне командной строки.

ПРИМЕЧАНИЕ: Если вы хотите визуально сравнить псевдонимы ключей, можно отобразить список всех ключей на сервере EKM 3.0 при помощи следующей команды:

```
print AdminTask.tklmKeyList('[-alias]')
```

9. Нажмите на кнопку **Enter (Ввод)**.

   Команда начнет выполнение.

Если на EKM 3.0 дубликат ключа на найден, отобразится следующее сообщение:

```
Найдено 0 ключей.
```

Если на EKM 3.0 имеется ключ или сертификат, то UUID и псевдоним ключа или сертификата отображается на дисплее.

Если на EKM 3.0 имеется ключ или сертификат, удалите данный ключ или сертификат из EKM 3.0. См. раздел Deleting a Specific Key (Удаление определенного ключа).

Повторите данное действие для каждого дубликата ключа, который был найден ранее.

7

Удаление EKM 3.0

В настоящей главе описывается порядок удаления EKM 3.0 из операционной системы Windows и систем на базе Linux.

ОСТОРОЖНО: В результате удаления EKM 3.0 все зашифрованные данные, записанные в ленточную библиотеку Dell PowerVault при помощи управляемого библиотекой шифрования (LME), станут недоступными для чтения. Перед удалением EKM 3.0 убедитесь в том, что все важные данные дешифрованы. Если существует возможность повторной установки EKM 3.0 в будущем, перед удалением EKM 3.0 создайте резервную копию. Скопируйте резервную копию и профиль установки EKM 3.0 (если профиль установки был сохранен) не внешний носитель перед удалением EKM 3.0. В процессе повторной установки EKM 3.0 используйте данный файл резервной копии для выполнения операции восстановления данных. См. раздел Performing Backups and Restoring from a Backup (Создание резервной копии и восстановление с помощью резервной копии).

ПРИМЕЧАНИЕ: Процедура удаления занимает примерно 35 минут. Не выключайте систему до завершения процедуры удаления.

ПРИМЕЧАНИЕ: В процессе удаления EKM 3.0 также происходит удаление WebSphere и DB2. Если DB2 используется с другими приложениями, компания Dell рекомендует не удалять EKM 3.0. Вместо этого рекомендуется остановить службу EKM 3.0. Для получения информации об остановке службы EKM 3.0 см. разделе Starting and Stopping the EKM 3.0 Server in Windows (Запуск и остановка сервера EKM 3.0 в Windows) или Starting and Stopping the EKM 3.0 Server in Linux (Запуск и остановка сервера EKM 3.0 в Linux).

ПРИМЕЧАНИЕ: Если используется конфигурация с основным/дополнительным сервером, также следует провести процедуру удаления дополнительном сервере EKM 3.0.

ПРИМЕЧАНИЕ: Если вы желаете повторно установить EKM 3.0, см. раздел Reinstalling EKM 3.0 (Повторная установка EKM 3.0).

Удаление EKM 3.0 на операционной системе Windows

В данной процедуре используется программа удаления EKM 3.0 для операционной системы Windows.

ПРИМЕЧАНИЕ: Процедура удаления занимает примерно 35 минут. Не выключайте систему до завершения процедуры установки.

1. На версиях Windows 2008 откройте **Control Panel (Панель управления)** и перейдите в **Programs and Features (Программы и компоненты)**.

   На Windows Server 2003 R2 с пакетом исправлений 2 откройте **Control Panel (Панель управления)** и перейдите в **Add or Remove Programs (Установка и удаление программ)**.
2. Правой кнопкой нажмите на **EKM 3.0** и выберите **Uninstall (Удалить)**.
3. Следуйте отображаемым на экране указаниям.

   После завершения процедуры удаления откроется окно **Uninstall Complete (Удаление завершено)**.
4. В окне **Uninstall Complete (Удаление завершено)** нажмите на кнопку **Done (Готово)**.

   Появится диалоговое окно с сообщением о перезагрузке системы.
5. В диалоговом окне нажмите на кнопку **Done (Готово)** (Если не нажать кнопку **Done (Готово)**, ОС Windows все равно будет перезагружена примерно через минуту).

ПРИМЕЧАНИЕ: Если ОС Windows не перезагружается, выполните перезагрузку машины вручную.

ПРИМЕЧАНИЕ: Если во время выполнения процесса удаления вы столкнулись с ошибками, можно просмотреть главный журнал установки в начальном каталоге пользователя **<*root*>:\Users\Administrator**. Главный журнал установки имеет имя **IA-TIPxxx**. Прокрутите окно к самой нижней строке гласного журнала установки для определения момента остановки процесса или возникновения ошибки. Для получения более подробной информации также можно просматривать файлы журнала в **<*root*>:\tklmv2properties**.

ПРИМЕЧАНИЕ: Если в процессе повторной установки EKM 3.0 происходит ошибка установки из-за ее прерывания, то удаление следует выполнить вручную. См. раздел Manually Uninstalling EKM 3.0 in Windows (Ручное удаление EKM 3.0 в операционной системе Windows).

Удаление EKM 3.0 на платформах на базе Linux

В данной процедуре используется программа удаления EKM 3.0 для платформ на базе Linux.

ПРИМЕЧАНИЕ: Процедура удаления занимает примерно 35 минут. Не выключайте систему до завершения процедуры установки.

1. Откройте сеанс работы с терминалом и перейдите к **/opt/dell/ekm/Uninstall_EKM**.
2. Запустите **Uninstall EKM (Удалить EKM)** при помощи следующей команды:

   ```
   ./Uninstall EKM
   ```

   Откроется всплывающее окно.
3. Нажмите на кнопку **Run (Выполнить)** во всплывающем окне.

   Откроется окно **Uninstall EKM (Удалить EKM)**.
4. Нажмите на кнопку **Uninstall (Удалить)**.

   Начнется выполнение процедуры удаления.
5. После завершения процедуры удаления откроется окно **Uninstall Complete (Удаление завершено)**. Нажмите на кнопку **Done (Готово)**.

   Система выполнит перезагрузку.

ПРИМЕЧАНИЕ: Если в процессе повторной установки EKM 3.0 происходит ошибка установки из-за ее прерывания, то удаление следует выполнить вручную. См. раздел Manually Uninstalling EKM 3.0 in Windows (Удаление EKM 3.0 вручную на платформах на базе Linux).

8

Поиск и устранение неисправностей

В данной главе приводится информация по поиску и устранению неисправностей, частым вопросам, сообщениям распространенных ошибок, а также контактная информация службы поддержки.

ПРИМЕЧАНИЕ: Если в данной главе ваша проблема не рассмотрена, см. руководство по поиску и устранению неисправностей TKLM. Для получения сведений о том, как получить доступ к документации TKLM, см. раздел Documentation and Reference Materials (Документация и справочная информация) файла **ReadThisFirst.txt** на установочном носителе EKM 3.0.

Обращение в компанию Dell

ПРИМЕЧАНИЕ: При отсутствии действующего подключения к Интернету можно найти контактные сведения в счете на приобретенное изделие, упаковочном листе, накладной или каталоге продукции компании Dell.

Компания Dell предоставляет несколько вариантов поддержки и обслуживания через Интернет и по телефону. Доступность служб различается по странам и видам продукции, и некоторые службы могут быть недоступны в вашем регионе. Порядок обращения в компанию Dell по вопросам сбыта, технической поддержки или обслуживания пользователей описан ниже.

1. Перейдите на веб-узел **support.dell.com**.
2. Выберите категорию поддержки.
3. Если вы находитесь не в США, выберите код своей страны в нижней части страницы, либо выберите **All (Все)**, чтобы просмотреть дополнительные варианты.
4. Выберите соответствующую службу или ссылку на ресурс технической поддержки, в зависимости от ваших потребностей.

Необходимые проверки системы

Перед установкой EKM 3.0 выполняет необходимые проверки системы. Если после экрана с лицензионным соглашением **License Agreement** отображается сообщение об ошибке, выполняйте указания, приведенные в сообщении об ошибке. Указания по наиболее распространенным ошибкам см. ниже.

Не пройдена проверка минимальных системных требований

В случае получения ошибки **Minimum System Requirements Failed (Не пройдена проверка минимальных системных требований)** нажмите на кнопку **Cancel and Exit (Отмена и выход)** и убедитесь в том, что ваша система соответствует требованиям. Требования системы см. в разделе Hardware and Software Requirements (Требования к аппаратному и программному обеспечению).

Пользователь не является администратором данной системы

Вы должны быть привилегированным пользователем на платформе на базе Linux или администратором в ОС Windows для того, чтобы устанавливать EKM 3.0.

SELinux должно быть отключено

Если SELinux установлено и включено, перед началом установки отключите SELinux.

Для отключения SELinux в RHEL5 выполните следующие действия:

1. В верхней панели инструментов на рабочем столе перейдите в **System (Система) → Administration (Управление) → Security Level and Firewall (Уровень безопасности и брандмауэр)**.

   Откроется окно **Security Level Configuration (Настройка уровня безопасности)**.
2. Нажмите на вкладку **SELinux**. В окне **SELinux Setting (Настройка SELinux)** нажмите на стрелки и выберите **Disabled (Выключено)**.
3. Нажмите на кнопку **Apply (Применить)**.
4. Нажмите на кнопку **OK**.
5. Для того чтобы изменения вступили в силу, перезагрузите систему.

Для отключения SELinux в RHEL4 выполните следующие действия:

1. Перейдите в **Applications (Приложения) → System Settings (Настройки системы) → Security Level (Уровень безопасности)** .

   Откроется всплывающее окно.
2. Во всплывающем окне выберите вкладку **SELinux**.
3. В выпадающем меню выберите **Disable (Выключить)**.
4. Перезагрузите систему.

compat-libstdc++ Не установлена

Если отображается сообщение об ошибке “compat-libstdc++ Not Installed” (compat-libstdc++ не установлена) см. раздел Installing the compat-libstdc++ Library (Установка библиотеки compat-libstdc++).

Не пройдена проверка минимального объема совместно используемой памяти

Во время установки EKM 3.0 на платформах на базе Linux отображается следующая ошибка:

```
Система не соответствует необходимым для установки требованиям к минимальному
объему совместно используемой памяти. Перед началом установки убедитесь в том,
что ваша система соответствует минимальным требованиям.
```

Для устранения данной проблемы выполните следующие действия:

1. Для увеличения объема совместно используемой памяти до требуемого объема и постоянного уровня откройте сеанс работы с терминалом и введите следующую команду:

   ```
   echo "kernel.msgmni = 1024" >> /etc/sysctl.conf echo "kernel.msgmax =
   65536" >> /etc/sysctl.conf echo "kernel.msgmnb = 65536" >> /etc/sysctl.conf
   echo "kernel.sem = 250 256000 32 1024" >> /etc/sysctl.conf echo
   "kernel.shmmax = 1268435456" >> /etc/sysctl.conf
   ```

ПРИМЕЧАНИЕ: Это минимальные значения, необходимые для установки EKM 3.0 на платформе на базе Linux. Для успешной установки EKM 3.0 может потребоваться больший объем памяти (kernel.shmmax). Если установка завершается неудачей, удалите EKM 3.0, увеличьте kernel.shmmax примерно на 25%, и установите EKM 3.0 повторно. Для удаления EKM 3.0 см. раздел Uninstalling EKM 3.0 (Удаление EKM 3.0).

2. Введите следующую команду для того, чтобы система немедленно начала использовать новый объем совместно используемой памяти (в противном случае необходимо выполнить перезагрузку):

   ```
   sysctl -p
   ```

Пользователь DB2 уже существует как обычный пользователь

Введенное в поле **DB2 User Name (Имя пользователя DB2)** имя пользователя уже используется пользователем в данной системе. Выберите другое имя пользователя.

В системе уже имеется TKLM или EKM 3.0

В системе TKLM или EKM 3.0 уже установлено. Удалите имеющийся экземпляр или установите EKM 3.0 на другую систему.

В системе уже имеется DB2

В системе DB2 уже установлено. Удалите DB2 или установите EKM 3.0 на другую систему.

ksh Не установлен

Установщику EKM 3.0 требуется наличие **ksh**. Установите **ksh** и затем установите EKM 3.0. См. документацию на свою операционную систему.

В имени хост-системы использован специальный символ

Имя хост-системы на вашем компьютере, на который выполняется установка EKM 3.0, не должно содержать пробелы или специальные символы, например, дефисы (-) или знаки подчеркивания (_). EKM 3.0 поддерживает только буквенно-числовые символы в имени хост-системы.

Имя домена

Имя домена на вашем компьютере, на который выполняется установка EKM 3.0, не должно содержать пробелы или специальные символы, например, дефисы (-) или знаки подчеркивания (_). EKM 3.0 поддерживает только буквенно-числовые символы в имени домена.

Недопустимый файл /etc/hosts

В файле **/etc/hosts** должна содержаться правильная запись для IPv4 адреса замыкания на себя. Данная запись должна иметь следующий формат:

```
<IPv4 адреса замыкания на себя><пробел><полное имя хост-
системы><пробел><краткое имя хост-системы>
```

Где <*пробел*> – это знак пробела.

Коды ошибок

Для получения списка кодов ошибок и их описания см. раздел Documentation and Reference Materials (Документация и справочная информация) файла **ReadThisFirst.txt** на установочном носителе EKM 3.0.

Справочные файлы Windows

Можно использовать следующие файлы журнала и файлы ошибок для поиска и устранения проблем в процессе установки EKM 3.0 на ОС Windows:

- **C:\tklm_install.stderr** (стандартный файл журнала ошибок)
- **C:\tklmV2properties*.log** (файл журнала установки DB2)
- **C:\Users\Administrator\IA-TIPInstall-00.txt** (файл журнала установки EKM 3.0)

ПРИМЕЧАНИЕ: Данные пути доступа применимы к версиям Windows Server 2008. Для Windows Server 2003 R2 с пакетом исправлений 2, файл журнала установки EKM 3.0 расположен в **C:\Documents and Settings \Administrator\IA-TIPInstall-00.txt**.

- **C:\Dell\EKM\products\tklm\logs\audit\tklm_audit.txt** (файл аудита) (Кроме возникших во время установки проблем данный файл также может быть использован для поиска и устранения проблем, возникших в процессе использования).

ПРИМЕЧАНИЕ: В приведенных выше путях доступа предполагается, что диск C: является системным диском. Замените букву вашего системного диска на **C:**.

Справочные файлы Linux

Можно использовать следующие файлы журнала и файлы ошибок для поиска и устранения проблем в процессе установки EKM 3.0 на системах на базе Linux:

- **/root/IA-TipInstall_*.log**
- **/tklm_install.stderr** (стандартный файл журнала ошибок)
- **/tklmV2properties/*.log**
- **/opt/dell/ekm/products/tklm/logs/audit/tklm_audit.log**

Удаление EKM 3.0 вручную

Во время удаления EKM 3.0 в сначала используйте автоматическую процедуру удаления. См. раздел Uninstalling EKM 3.0 (Удаление EKM 3.0). Если в результате выполнения автоматической процедуры установки произошла ошибка, удалите EKM 3.0 вручную.

Удаление EKM 3.0 вручную на операционной системе Windows

Если в процессе повторной установки EKM 3.0 происходит ошибка установки из-за ее прерывания, то удаление следует выполнить вручную. Если какие-либо элементы уже удалены, то пропустите данное действие.

ПРИМЕЧАНИЕ: Если имеется возможность переустановить операционную систему на вашем сервере, то компания Dell рекомендует переустановить операционную систему, а затем установить EKM 3.0.

ПРИМЕЧАНИЕ: Путевые имена в данной процедуре указаны для версий Windows Server 2008. Когда возможно, во время выполнения данной процедуры для Windows Server 2003 R2 с пакетом исправлений 2 перейдите в **Start (Пуск) → Control Panel (Панель управления) → Add or Remove Programs (Добавить или удалить программы)**.

1. Перейдите к **Start (Пуск) → Control Panel (Панель управления) → Programs (Программы) (или Programs and Features(программы и компоненты)) → Uninstall a Program (Удалить программу)** . Удалить IBM DB2 (**DB2 Workgroup Server Edition - DB2TKLMV2**).
2. Перейдите к **Start (Пуск) → Control Panel (Панель управления) → Programs (Программы) (или Programs and Features (Программы и компоненты)) → Uninstall a Program (Удалить программу)**.
3. Нажмите на **EKM**.
4. Нажмите **Uninstall/Change (Удалить/изменить)**.

   Отобразится мастер удаления EKM 3.0.
5. Следуйте подсказкам мастера удаления.

   После завершения удаления EKM 3.0 система будет автоматически перезагружена.
6. Перейдите к **Start (Пуск) → Control Panel (Панель управления) → Programs (Программы) → Uninstall a Program (Удалить программу)**. Uninstall (Удалить) **IBM Update Installer for WebSphere software V7.0**.
7. Запустите редактор реестра Windows Registry Editor (Regedit). Перейдите к **HKEY_CURRENT_USER → Software → IBM → DB2 → InstalledCopies**. Удалите папку **DB2TLKMV2**.

ОСТОРОЖНО: Будьте внимательны в процессе внесения изменений в реестр. Если вы внесете неправильное изменение, система может начать работать неустойчиво.

8. В проводнике Windows Explorer перейдите к **<*root*>:\Dell**, если имеется (например, **C:\Dell**). Удалите папку **EKM** (если имеется) и все вложенные папки (**<*root*>:\Dell\EKM**).
9. На корневом диске (например, **C:**), удалите папку **tklmV2properties** (**<*root*>:\tklmV2properties**).
10. На корневом диске удалите папку **tklmdbarchive**. (**<*root*>:\tklmdbarchive**).
11. На корневом диске удалите папку с именем, совпадающем с именем пользователя DB2.
12. На корневом диске удалите файл **tklm_install.stderr** (**<*root*>:\tklm_install.stderr**).
13. В проводнике Windows Explorer перейдите в **<*root*>:\Program Files (x86)\dell**. Удалите установочный каталог DB2 (**<*root*>:\Program Files (x86)\dell\db2dkm**).

ПРИМЕЧАНИЕ: Во время выполнения данного действия и трех последующих, если ваша система является 32-битной операционной системой, замените имя "Program Files (x86)" на имя "Program Files."

14. В проводнике Windows Explorer перейдите в **<*root*>:\Program Files (x86)\ibm**. Удалите папку **Common** (**<*root*>:\Program Files (x86)\ibm\Common**).

15. В проводнике Windows Explorer перейдите в **<*root*>:\Program Files (x86)\ibm**. Удалите папку **gsk8** (**<*root*>:\Program Files (x86)\ibm\gsk8**).
16. Перейдите к **Start (Пуск)** → **Administrative Tools (Администрирование)** → **Computer Management (Управление компьютером)** . В левой панели перейдите в **Local Users and Groups (Локальные пользователи и группы)** → **Users (Пользователи)** . В правой панели удалите учетную запись (записи) администратора DB2.
17. Перейдите к **Start (Пуск)** → **Administrative Tools (Администрирование)** → **Computer Management (Управление компьютером)** . В левой панели перейдите в **Local Users and Groups (Локальные пользователи и группы)** → **Groups (Группы)** . В правой панели удалите группы администраторов DB2 (**DB2ADMINS** и **DB2USERS**).
18. В проводнике Windows Explorer перейдите в **<*root*>:\Users**. Удалите папку, имя которой совпадает с именем пользователя DB2.
19. В проводнике Windows Explorer перейдите в **<*root*>:\Users\Administrator**. Удалите текстовый файл **IA-TIPInstall-xx log**.
20. Остановите и удалите любые из следующих установленных служб Windows EKM 3.0. Для чего введите в командную строку следующие команды из корневого диска (например, **C:**). Если служба уже остановлена, можно пропустить связанное с остановкой действие.

ПРИМЕЧАНИЕ: По желанию можно остановить и удалить службы с помощью утилиты Windows Services

```
sc stop "DBTKLM20" sc delete "DBTKLM20" sc stop "<DB2 user name>" sc delete
"<DB2 user name>" sc stop "DB2GOVERNOR_DB2TKLMV2" sc delete
"DB2GOVERNOR_DB2TKLMV2" sc stop "DB2LICD_DB2TKLMV2" sc delete
"DB2LICD_DB2TKLMV2" sc stop "DB2MGMTSVC_DB2TKLMV2" sc delete
"DB2MGMTSVC_DB2TKLMV2" sc stop "DB2REMOTECMD_DB2TKLMV2" sc delete
"DB2REMOTECMD_DB2TKLMV2" sc stop "DB2DAS00" sc delete "DB2DAS00"
```

ПРИМЕЧАНИЕ: Следующая служба в утилите Windows Services отображается как **Tivoli Integrated Portal - TIPProfile_Port_<*номер порта DB2*>**.

```
sc stop "IBMWAS61Service - TIPProfile_Port_<номер порта DB2>" sc delete
"IBMWAS61Service - TIPProfile_Port_<номер порта DB2>"
```

ПРИМЕЧАНИЕ: По умолчанию номер порта для DB2 используется 16310.

21. Введите следующие команды в корневом диске (например, **C:**):

```
reg delete HKEY_LOCAL_MACHINE\software\classes\installer\Products
\907E425044C581845A83FCBED0CD5771 /f reg delete HKEY_LOCAL_MACHINE\software
\classes\installer\Features\907E425044C581845A83FCBED0CD5771 /f
```

22. Перезагрузите систему.
23. Если желаете повторно установить EKM 3.0, см. раздел Performing the EKM 3.0 Installation Procedure (Выполнение процедуры установки EKM 3.0).

Удаление EKM 3.0 вручную на платформах на базе Linux

Если в процессе повторной установки EKM 3.0 происходит ошибка установки из-за ее прерывания, то удаление следует выполнить вручную. Если какие-либо элементы уже удалены, то пропустите данное действие.

ПРИМЕЧАНИЕ: Если имеется возможность переустановить операционную систему на вашем сервере, то компания Dell рекомендует переустановить операционную систему, а затем установить EKM 3.0.

В следующей процедуре замените следующие переменные (<*переменная*>) на свои пути установки или названия переменных.

- <*DB2_INSTALL_DIR*>: это выбранный вами каталог для установки базы данных.
- <*DB2_ADMIN*>: это идентификатор администратора DB2 (например, **ekm_dell1**).

- <*DB2_ADMIN_HOME*>: это исходный каталог базы данных (также называется место расположения базы данных).
- <*DB2_DB_NAME*>: это имя базы данных.

1. Запустите сеанс терминала.
2. Удалите экземпляр DB2 при помощи ввода следующей команды:

   ```
   cd /opt/dell/ekm/products/tklm/_uninst ./removeDB2Inst.sh
   <DB2_INSTALL_DIR> ./removeDB2Inst.sh <DB2_ADMIN> ./removeDB2Inst.sh
   <DB2_ADMIN_HOME> ./removeDB2Inst.sh <DB2_DB_NAME>
   ```

   Например:

   ```
   ./removeDB2Inst.sh /opt/dell/db2ekm ./removeDB2Inst.sh /ekm_dell1 ./
   removeDB2Inst.sh /home/db2ekm ./removeDB2Inst.sh /db2ekm
   ```

3. Запустите автоматическое удаление TKLM с ответным файлом при помощи ввода следующих команд:

   ```
   /opt/dell/ekm/_uninst/TIPInstall/uninstall -i silent -f /opt/dell/ekm/
   Uninstall_EKM/dkm_uninstall_response.txt
   ```

4. Удалите файлы журнала при помощи ввода следующих команд:

   ```
   rm -rf /tklmV2properties cd /opt/dell/ekm/ rm tklm_install.stderr rm IA-
   TIPIn*.log rm EKM_Install*.log
   ```

5. Удалите идентификатор пользователя DB2 из системы при помощи ввода следующих команд:

   ```
   userdel -r $DB2_ADMIN$
   ```

   Например:

   ```
   userdel -r ekm_dell1
   ```

6. Удалите DB2 из системы при помощи ввода следующих команд:

   ```
   cd /opt/dell/ekm/install ./db2_deinstall -a
   ```

7. Удалите родительский каталог, использованный для слияния/миграции EKM 2.X и установки EKM 3.0.

   ```
   rm -rf /opt/dell/ekm
   ```

8. Перезагрузите машину.
9. Если желаете повторно установить EKM 3.0, см. раздел Performing the EKM 3.0 Installation Procedure (Выполнение процедуры установки EKM 3.0).

Повторная установка EKM 3.0

Для выполнения повторной установки EKM 3.0 выполните следующие действия:

1. Удалите EKM 3.0 согласно процедуре удаления. См. раздел Uninstalling EKM 3.0 (Удаление EKM 3.0).

ПРИМЕЧАНИЕ: Если после удаления EKM 3.0 машина не выполнила перезагрузку автоматически, перезагрузите ее.

2. Повторно установите EKM 3.0 согласно процедуре установки. См. раздел Performing the EKM 3.0 Installation Procedure (Выполнение процедуры установки EKM 3.0).

ПРИМЕЧАНИЕ: Если в процессе первоначальной установки EKM 3.0 был сохранен профиль установки, то его можно использовать для выполнения повторной установки EKM 3.0. Однако, если используется конфигурация с основным/дополнительным сервером, а профиль установки сохранен для дополнительного сервера EKM 3.0, не используйте его для повторной установки EKM 3.0 на основной сервер.

Часто задаваемые вопросы

Можно ли установить EKM 3.0 в операционной системе, которая не включена в перечень в разделе Требования к аппаратному и программному обеспечению?

Нет. EKM 3.0 поддерживает только те операционные системы, их версии, выпуски, пакеты обновления и уровень битов, которые приведены в перечне в разделе Требования к аппаратному и программному обеспечению.

Можно ли скопировать файлы из установщика EKM 3.0 на жесткий диск системы и выполнить установку из системы?

Нет. EKM 3.0 поддерживает только установку с установочных носителей EKM 3.0. См. раздел Установка EKM 3.0.

Что мне делать, если в процессе установки EKM 3.0 я получил сообщение об ошибке автоматической установки?

Более подробную информацию см. в файле **tklm_install.stderr** (файл стандартного журнала ошибок). *В операционной системе Windows* данный файл расположен по адресу **<*root*>:\tklm_install.stderr**. *В системах на базе Linux* он расположен по адресу **/tklm_install.stderr**. Если код ошибки приведен в данном файле, см. раздел Коды ошибок.

После устранения проблемной ситуации, описанной в коде ошибки, выполните ручное удаление приложения. См. раздел Ручное удаление EKM 3.0. Перезагрузите систему после ручного удаления EKM 3.0, а затем повторно установите EKM 3.0.

Что мне делать, если d процессе повторной установки EKM 3.0 я получил сообщение об ошибке автоматической установки?

Выполните ручное удаление приложения. См. раздел Ручное удаление EKM 3.0. Перезагрузите систему после ручного удаления EKM 3.0, а затем повторно установите EKM 3.0.

Что мне делать, если в процессе установки EKM 3.0 я получил сообщение об ошибке с указанием того, что Windows Server 2003 R2 SP2 не установлен?

Список поддерживаемых операционных систем см в разделе Требования к аппаратному и программному обеспечению. После установки Windows Server 2003 R2 со второго компакт-диска, перед установкой EKM 3.0 перезагрузите систему.

ОСТОРОЖНО: Данная операция приведет к перезаписи данных на ленточном носителе. После перезаписи данные на ленточном носителе станут недоступными.

Как можно повторно использовать ранее зашифрованный носитель в качестве незашифрованного носителя или в качестве зашифрованного носителя с другим ключом шифрования.

Для повторного использования ранее зашифрованного носителя необходимо использование рабочей конфигурации EKM 3.0, содержащей ключи для повторно используемых кассет, а также PowerVault TL2000 или TL4000.

Перезаписать кассеты таким образом в PowerVault ML6000 невозможно. Для выполнения такой задачи можно мигрировать кассеты из ML6000 в TL2000 или TL4000. После чего необходимо указать для TL2000 или TL4000 соответствующий сервер EKM 3.0.

Для использования ранее зашифрованного носителя выполните следующие действия:

1. Убедитесь в том, что сервер EKM 3.0 работает и правильно настроен.
2. Зайдите в графический пользовательский интерфейс RMU для TL2000/TL4000 (требуется учетная запись администратора/сервисная учетная запись).
3. Перейдите в **Configure Library (Настроить библиотеку)**.
4. Перейдите в **Encryption (Шифрование)**.
5. Измените настройки **Encryption Policy (Политика шифрования)** на **Internal Label – Selective Encryption (Внутренняя маркировка – Выборочное шифрование)**.
6. Отправьте задачу на запись (например, быстрое стирание, полное стирание или создание резервной копии) на предназначенный для повторного использования носитель.

Для проверки того, что шифрование было перезаписано выполните следующие действия:

1. Войдите в графический пользовательский интерфейс RMU для TL2000/4000.
2. Перейдите в **Monitor Library (Библиотека монитора)**, а затем в **Inventory (Опись)**.
3. Выберите в выпадающем меню соответствующий журнал.
4. Убедитесь в том, что в разделе **Comment (Комментарий)** отображается текст **Not Encrypted (Не зашифровано)**.

Удалить или отменить установку EKM 3.0 можно только после того, как все необходимые носители были перезаписаны. Компания Dell рекомендует создать резервную копию важных файлов графического пользовательского интерфейса EKM 3.0 и сохранить файлы резервных копий на внешний носитель, например на съемный диск. В таком случае EKM 3.0 может быть восстановлена, если необходимо перезаписать добавочные кассеты.

У меня возникли проблемы при установке EKM 3.0 и потребовалась повторная установка. Как определить, выполнял ли EKM 3.0 выдачу каких-либо ключей или нет?

1. Откройте командную строку и перейдите в папку файла контрольного журнала.

   Для операционной системы Windows контрольный журнал расположен по адресу **<*root*>:\Dell\EKM\products\tklm\logs\audit\tklm_audit.txt**.

   Для систем на базе Linux контрольный журнал расположен по адресу: **/opt/dell/ekm/products/tklm/logs/audit/tklm_audit.log**.
2. Скопируйте текущий файл контрольного журнала во временный файл, чтобы его можно было открыть. Текущий файл контрольного журнала используется и не может быть открыт в процессе обновления.
3. Откройте временную копию в текстовом редакторе (например, WordPad). Выполните поиск строки **Drive Serial Number (Серийный номер диска)**. Если запись найдена, то ключ был выдан. Если значение параметра **volser** не заполнено, то это результат проведения проверки пути к ключу, и поэтому для большей уверенности необходимо продолжить поиск в файле дополнительных записей, связанных с серийным номером диска.

ОСТОРОЖНО: Если ключи были присвоены, то перед удалением EKM 3.0 необходимо дешифровать упомянутый носитель.

Как изменяется мое приложения для резервного копирования, когда я настраиваю ленточную библиотеку для шифрования с управлением библиотекой.

После включения управляемого библиотекой шифрования на ленточной библиотеке и настройки конфигурации зашифрованных разделов, вносятся изменения в настройки дисков, на которых размещен данный раздел (разделы). Необходимо остановить и повторно запустить службы приложения для резервного копирования после настройки конфигурации разделов с включенным шифрованием для того, чтобы гарантировать распознавание настроек шифрования на диске (дисках) приложением для резервного копирования.

ПРИМЕЧАНИЕ: Приложение для резервного копирования ленточных носителей не будет отображать **включение** шифрования, если используется управляемое библиотекой шифрование. Ленточная библиотека покажет разделы с **включенным шифрованием**. Для приложения по резервному копированию управляемое библиотекой шифрование является прозрачным. Приложение для резервного копирования ленточных носителей показывает, что шифрование **включено** только в том случае, если приложение (например, Symantec, CommVault т.д.) выдает ключи шифрования диску (дискам).

Как в EKM 3.0 обрабатывается добавление новых дисков или замена неисправного диска?

Можно добавить новые или ремонтные диски на сервер EKM 3.0 при помощи функции автоматического поиска или вручную. Информацию о добавлении дисков при помощи функции автоматического поиска см. в разделе Добавление устройства в группу устройства.

Компания Dell рекомендует использовать функцию автоматического поиска, так как для ручного добавления диска необходимо ввести 12-значный серийный номер диска (10-значный серийный номер плюс два нуля в конце). Если обеспечение безопасности является приоритетом, можно включить автоматическое обнаружение и

запустить контрольное резервное копирование или проверку пути к ключу в ленточной библиотеке для добавления необходимых дисков в перечень дисков. После чего можно выключить автоматическое обнаружение, чтобы не допустить выдачу ключей новым дискам. До тех пор, пока EKM 3.0 способно проверять подлинность цифровых подписей, присвоенных диску изготовителем, EKM 3.0 продолжает принимать запросы на ключи. В хранилище ключей ключи группируются в группы ключей и можно связывать данные группы ключей с новыми/ремонтными дисками после добавления дисков.

ПРИМЕЧАНИЕ: Если вы желаете добавить устройство вручную, см. документацию TKLM. Для получения сведений о том, как получить доступ к документации TKLM, см. раздел Documentation and Reference Materials (Документация и справочная информация) файла **ReadThisFirst.txt** на установочном носителе EKM 3.0.

Как в EKM 3.0 обрабатывается добавление новой ленточной библиотеки или замена неисправной ленточной библиотеки?

Для управляемого библиотекой шифрования ленточная библиотека является всего лишь промежуточным звеном. Можно добавлять или заменять ленточные библиотеки и выдавать ключи до тех пор, пока EKM 3.0 способно проверять подлинность цифровой подписи диска. Ремонтная ленточная библиотека должна иметь лицензию на использование управляемого библиотекой шифрования и быть настроена на работу вместе с имеющимся EKM 3.0.

Какое влияние шифрование оказывает на сжатие и наоборот?

Данные сжимаются до шифрования, так как зашифрованные данные в основном не могут быть сжаты. Поэтому сжатие не оказывает какого-либо влияния на шифрование, и наоборот

Снижает ли шифрование уровень производительности?

Шифрование может незначительно влиять на уровень производительности, но он не приводит к увеличению окна резервного копирования.

Как можно запросить получение и использовать сторонний сертификат?

Создайте запрос на выдачу сертификата в EKM 3.0. Отправьте данный запрос на выдачу сертификата в центр сертификации. Полученный от центра сертификации сертификат можно импортировать в EKM 3.0 использовать для защиты данных на устройстве с включенной функцией шифрования или для передачи данных по протоколу SSL. Для получения более подробной информации о порядке формирования запроса на выдачу сертификата, импорта полученного сертификата и его использования для шифрования см. документацию TKLM. Для получения более подробной информации о получении доступа к документации TKLM, см. раздел Documentation and Reference Materials (Документация и справочная информация файла) **ReadThisFirst.txt** на установочном носителе EKM 3.0.

Известные проблемы и методы их решения

Проблема: невозможно создать резервную копию.

Описание:

С помощью Internet Explorer попытайтесь создать резервную копию хранилища ключей. Когда указывается несуществующее место расположения резервной копии, выполнение процедуры не происходит.

Решение:

Выполнить одно из следующих действий. Если выбранное действие не работает, выполните другое указанное действие:

- Включите JavaScript в используемом приложении для просмотра веб-страниц. Если используется Internet Explorer V8, включите режим представления совместимости Compatibility View.
- Используйте другое поддерживаемое приложение для просмотра веб-страниц. Более подробную информацию см. в разделе Требования к аппаратному и программному обеспечению.

- Укажите существующую папку. Если желаете указать новую папку, создайте ее до создания резервной копии.

Проблема: одновременно создается несколько резервных копий.

Описание:

При попытке создания резервной копии хранилища ключей одновременно создаются несколько файлов резервной копии. Данная ситуация возникает редко.

Решение:

Все файлы резервной копии имеют одинаковое содержание. Любой из данных файлов резервной копии можно использовать для восстановления данных.

Проблема: мне приходится дважды вводить информацию для входа в систему.

Описание:

После истечения времени ожидания для EKM 3.0 (через примерно 30 минут простоя), первая попытка входа в EKM 3.0 отклоняется и необходимо вводить информацию для входа в систему второй раз.

Решение:

Вводите информацию для входа в EKM 3.0 оба раза.

Проблема: правая панель частично скрыта панелью навигации.

Описание:

Вы используете Internet Explorer. Вы открываете экран **Key and Device Management (Управление ключами и устройствами)** EKM 3.0. Вы выбираете группу ключей или ленточный диск. Правая панель частично скрывается панелью навигации.

Решение:

Выполните одно из следующих действий:

- Обновите экран.
- Разверните окно приложения для просмотра веб-страниц.
- Используйте другое поддерживаемое приложение для просмотра веб-страниц. Более подробную информацию см. в разделе Требования к аппаратному и программному обеспечению.

Проблема: в верхней части приложения для просмотра веб-страниц отображается сообщение "Certificate Error" (Ошибка сертификата).

Описание:

Вы используете Internet Explorer 8 в режиме представления совместимости. Вы успешно импортируете выданный службой сертификат, но в верхней части экрана рядом с панелью ввода URL-адреса отображается сообщение **Certificate Error (Ошибка сертификата)**.

Решение:

Выполните одно из следующих действий:

- Игнорируйте ошибку. Данная ошибка не мешает работе EKM 3.0.
- Используйте другое поддерживаемое приложение для просмотра веб-страниц (например, Internet Explorer 6.X или Firefox). См. Требования к аппаратному и программному обеспечению.

Проблема: я не могу сортировать информацию в таблицах.

Описание:

С помощью полей фильтров в верхней части таблиц на экранах **Administer Server Certificates (Администрация сертификатов сервера)**, **Backup and Restore (Резервное копирование и восстановление данных)** и **Credential Store (Хранилище имени пользователя и пароля)** невозможно сортировать содержимое таблиц.

Решение:

Для сортировки содержимого нажмите на строку заголовка каждой колонки.

Проблема: я не могу добавить описание для созданной мной резервной копии.

Описание:

С помощью Firefox в операционной системе Windows вы создаете резервную копию. Вы не можете ввести описание для резервной копии и используется описание по умолчанию.

Решение:

Используйте поддерживаемую версию Internet Explorer. Более подробную информацию см. в разделе Требования к аппаратному и программному обеспечению.

Проблема: определенные действия в графическом пользовательском интерфейсе EKM 3.0 приводят к возникновению ошибок сценариев с отображением всплывающих окон с сообщениями.

Описание

Внутри веб-обозревателя отображаются ошибки сценариев и запрашиваемые действия не выполняются.

Решение:

Выполнить одно из следующих действий. Если выбранное действие не работает, выполните другое действие:

- Включите JavaScript в используемом приложении для просмотра веб-страниц. Если используется Internet Explorer V8, включите режим представления совместимости Compatibility View.

ПРИМЕЧАНИЕ: После входа в EKM 3.0 необходимо включить режим представление совместимости.

- Используйте другое поддерживаемое приложение для просмотра веб-страниц. Более подробную информацию см. в разделе Требования к аппаратному и программному обеспечению.

Проблема: во время удаления индикатор выполнения не точно отображает ход выполнения.

Описание

Индикатор удаления не точно отображает ход выполнения процесса. В начале процесса удаления индикатор переходит примерно к 30% и остается в таком положении во время всего процесса удаления. В конце операции он переходит к значению 100%.

Решение

Это проблема известна и не связана с процессом удаления.

ОСТОРОЖНО: Не перезагружайте систему или отменяйте процессу удаления.

Проблема: настройки для экрана Key and Device Management (Управление ключами и устройствами) не вступают в силу.

Описание

Когда на экране Key and Device Management (Управление ключами и устройствами) я изменяют настройки для передачи данных для диска изменения не вступают в силу.

Решение:

После изменения настроек для передачи данных для диска следует остановить и запустить сервер EKM 3.0. Изменения вступят в силу. Более подробную информацию см. в разделе Запуск и остановка сервера EKM 3.0 в Windows или Запуск и остановка сервера EKM 3.0 в Linux.

Проблема: на сервере под управлением ОС Windows 2008 после завершения установки EKM 3.0 в панели оповещения отображается зеленый значок, обозначающий процедуру установки.

Описание

В панели оповещения отображается зеленый значок.

Решение

Данная проблема является известной и не влияет на характеристики или надежность EKM 3.0. После выхода и повторного входа в систему значок больше не появится.

Проблема: во время настройки процесса установки EKM 3.0 в некоторых полях отображается значение "0".

Описание

Во время настройки процесса установки EKM 3.0 в некоторых полях отображается значение "0". Данная ситуация возникает в случае использования профиля установки для установки EKM 3.0, который является или недействительным, или в нем не все поля заполнены.

Решение

Убедитесь в том, что используете правильный профиль установки.

ПРИМЕЧАНИЕ: Если заполнить все поля вручную, необходимо убедиться в том, что введенные данные точно соответствуют использованным в исходной установке, в противном случае дополнительный сервер невозможно будет использовать в качестве резервного сервера для основного сервера.

Проблема: во время создания резервной копии отображается сообщение об ошибке "software exception" (Исключение программного уровня).

Описание

Когда вы создаете резервную копию, отображается сообщение об ошибке (исключение программного уровня).

Решение

В EKM 3.0 имеется известное ограничение на серверы, в которых используется более 24 ЦП. Для решения данной проблемы необходимо установить самый свежий универсальный пакет исправлений для DB2.

ПРИМЕЧАНИЕ: Для получения более подробной информации см. примечания к выпуску по адресу: **support.dell.com/manuals**. Перейдите в раздел **Software (Программное обеспечение) → Systems Management (Управление системой) → Dell Encryption Key Manager** .

Проблема: я не могу добавить уровни доступа только что созданному пользователю с помощью Internet Explorer V8.

Описание

После входа в EKM 3.0 в качестве администратора создания нового пользователя а затем попытки добавления уровня доступа только что созданному пользователю, отображается ошибка JavaScript и уровень доступа не добавляется.

Решение

Сначала создайте пользователя, затем добавьте уровни доступа для пользователя с помощью экрана **Administrative User Roles (Уровни доступа администратора)**. Чтобы получить доступ к данному экрану в панели навигации перейдите к **Users and Groups (Пользователи и группы) → Administrative User Roles (Уровни доступа администратора)**. Также устранить данную проблему можно, если использовать поддерживаемую версию Firefox.

Проблема: когда я удаляю EKM 3.0, отображается ошибка "stack overflow exception" (Ошибка переполнения стека).

Описание

В процессе удаления EKM 3.0 отображается ошибка Java.

Решение

Удаляйте EKM 3.0 вручную. Более подробную информацию см. в разделе Manually Uninstalling EKM 3.0 (Ручное удаление EKM 3.0).

Проблема: процесс удаления EKM 3.0 продолжается в течение нескольких часов и не завершается.

Описание

При попытки удаления EKM 3.0 процесс не завершается.

Решение

Удаляйте EKM 3.0 вручную. Более подробную информацию см. в разделе Manually Uninstalling EKM 3.0 (Ручное удаление EKM 3.0).

Установка библиотеки compat-libstdc++

Перед установкой EKM 3.0 на платформах под управлением систем на базе Linux необходимо установить библиотеку **compat-libstdc++-33-3.2.3-61** или более позднюю ее версию.

Если в процессе установки EKM 3.0 на системе на базе Linux вы получите такое сообщение об ошибке, необходимо установить **compat-libstdc++**:

```
Your operating system does not have the compat-libstdc++ packaged installed (В
вашей операционной системе не установлен пакет compat-libstdc++).
```

Для установки **compat-libstdc++**:

1. В сеансе терминала перейдите к RPM-файлу **compat-libstdc++** в папке **EKMPREREQLIBS** на установочном носителе EKM 3.0 при помощи следующей команды:

   ```
   cd /<путь_к_установочному_dvd-диску_EKM_3.0>/EKMPREREQLIBS
   ```

2. Установите **compat-libstdc++** при помощи ввода следующей команды:

   ```
   rpm -ivh compat-libstdc++*.rpm
   ```

ПРИМЕЧАНИЕ: Если отображается ошибка с сообщением о том, что RPM-пакет **compat-libstdc++**, который вы пытаетесь установить, конфликтует с пакетом **libstdc++-33**, который уже установлен в системе, выполните следующие действия:

a. Введите следующую команду:

   ```
   rpm -e libstdc++-33
   ```

b. Введите следующую команду:

   ```
   rpm -ivh compat-libstdc++*.rpm
   ```