Dell™ PowerVault™ 加密密钥管理器

LTO Ultrium 4 和 LTO Ultrium 5 的快速入门指南

作为入门方式，本指南提供了在 LTO 第 4 代和 LTO 第 5 代磁带机上进行加密的***基本配置***。安装和配置 Dell PowerVault 加密密钥管理器之前，请访问 **http://support.dell.com** 下载最新的库和驱动器固件以确保不存在任何问题。

Dell PowerVault 加密密钥管理器（现在开始称为加密密钥管理器）是一种 Java™ 软件程序，可以帮助支持加密的磁带机生成、保护、存储和维护加密密钥。这些密钥用于对写入 LTO 磁带介质的信息进行加密，并且对从 LTO 磁带介质读取的信息进行解密。加密密钥管理器在Linux® 和 Windows® 上运行，用作部署在企业内部多个位置的共享资源。

本文档展示了通过使用图形用户界面（GUI）或使用命令，您可以多快的速度安装并设置加密密钥管理器。本文档展示了如何使用 JCEKS 密钥库类型，因为 JCEKS 密钥库类型是最简便且可传输性最好的受支持密钥库。如果需要关于特定步骤或其他受支持密钥库类型的更多信息，请参阅位于以下位置的 *Dell 加密密钥管理器用户指南*：**http://support.dell.com** 或产品随附的 Dell 加密密钥管理器介质。

注： 重要的加密密钥管理器主机服务器配置信息：建议 Dell 加密密钥管理器程序所在的计算机使用 ECC 内存，以便将丢失数据的风险降到最低。加密密钥管理器执行以下功能：请求生成加密密钥并将这些密钥传递给 LTO-4 和 LTO-5 磁带机。在加密密钥管理器进行处理的过程中，密钥材料以打包（加密）格式驻留在系统内存内。请注意，密钥材料必须在不发生任何错误的情况下传递到到相应磁带机中，写入磁带盒的数据才能恢复（解密）。如果因为某种原因，系统内存中的位错误导致密钥材料损坏，而该密钥材料用于将数据写入磁带盒，那么写入该磁带盒的数据将不能恢复（即以后将无法解密）。目前已存在防止发生此类数据错误的安全措施。但是，如果加密密钥管理器所在的计算机不使用纠错编码（ECC）内存，那么密钥材料可能在处于系统内存中时遭到损坏，而损坏则可能导致数据丢失。这种情况发生的几率很小，但是还是始终建议重要程序（如加密密钥管理器）所在的计算机使用 ECC 内存。

初始操作：安装加密密钥管理器软件

1. 插入 Dell 加密密钥管理器 CD。如果在 Windows 中没有自动启动安装，那么浏览到 CD 并双击 Install_Windows.bat。

   对于 Linux，不会自动启动安装。请转至 CD 根目录并输入 `Install_Linux.sh`。

   将显示最终用户许可协议。您必须认可该许可协议，才能继续安装。

   安装过程将把适合您的操作系统的所有内容（文档、GUI 文件和配置属性文件）从 CD 复制到硬盘驱动器。安装期间，将检查您的系统是否具有合适的 IBM Java 运行时环境。如果未找到，那么将自动安装该环境。

   安装完成之后，将启动图形用户界面（GUI）。

方法 1: 使用 GUI 设置加密密钥管理器

此过程创建一个基本配置。一旦成功完成，将启动加密密钥管理器服务器。

1. 如果尚未启动 GUI，按如下方式打开:

   在 Windows 上

   浏览至 c:\ekm\gui 并单击 LaunchEKMGui.bat

   在 Linux 平台上

   浏览至 /var/ekm/gui 并输入 . ./LaunchEKMGui.sh

   注意: 在 Linux shell 命令之前指定 . ./ （句点空格句点正斜杠）以确保该shell 能够找到脚本。

2. 在 EKM 服务器配置页面（图 1）上的所有必填字段（以星号 * 标记）中输入数据。单击任何数据字段右侧的问号标记以获取描述。单击**下一步** 转至EKM 服务器证书配置页面。

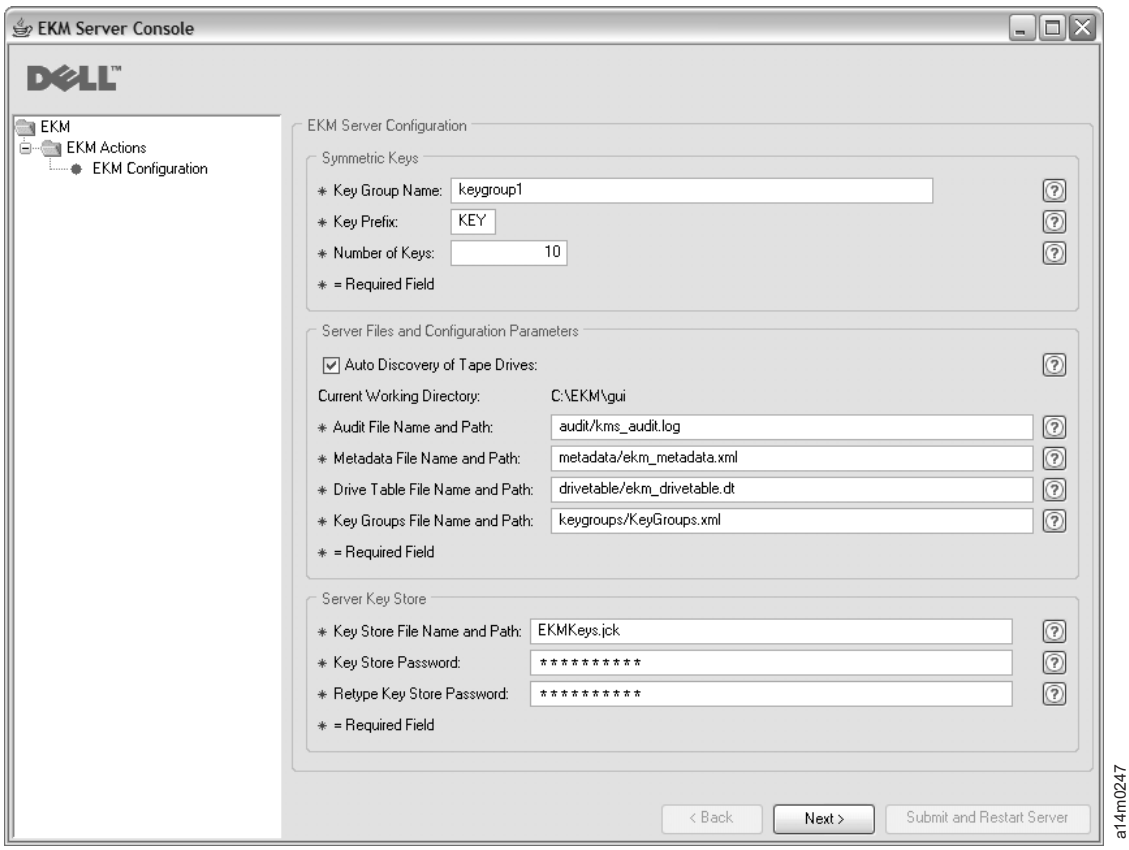

图 1. EKM Server Configuration 页面

注:

a. 通过自动发现添加磁带机之后，应该使用 GUI 刷新加密密钥管理器服务器以确保将它们存储在磁带机表格中。

b. 一旦设置了密钥库密码，除非违反了它的安全性，否则**不要对它进行更改**。密码采用加密形式，以消除安全性风险。更改密钥库密码需要使用 **keytool** 命令分别更改该密钥库中的每一个密码。请参阅 *Dell 加密密钥管理器用户指南* 中的“更改密钥库密码”。

3. 在 EKM 服务器证书配置页面（第 3 页的图 2）输入密钥库别名并填写可能有助于识别证书及其用途的附加字段。单击**提交并启动服务器**。

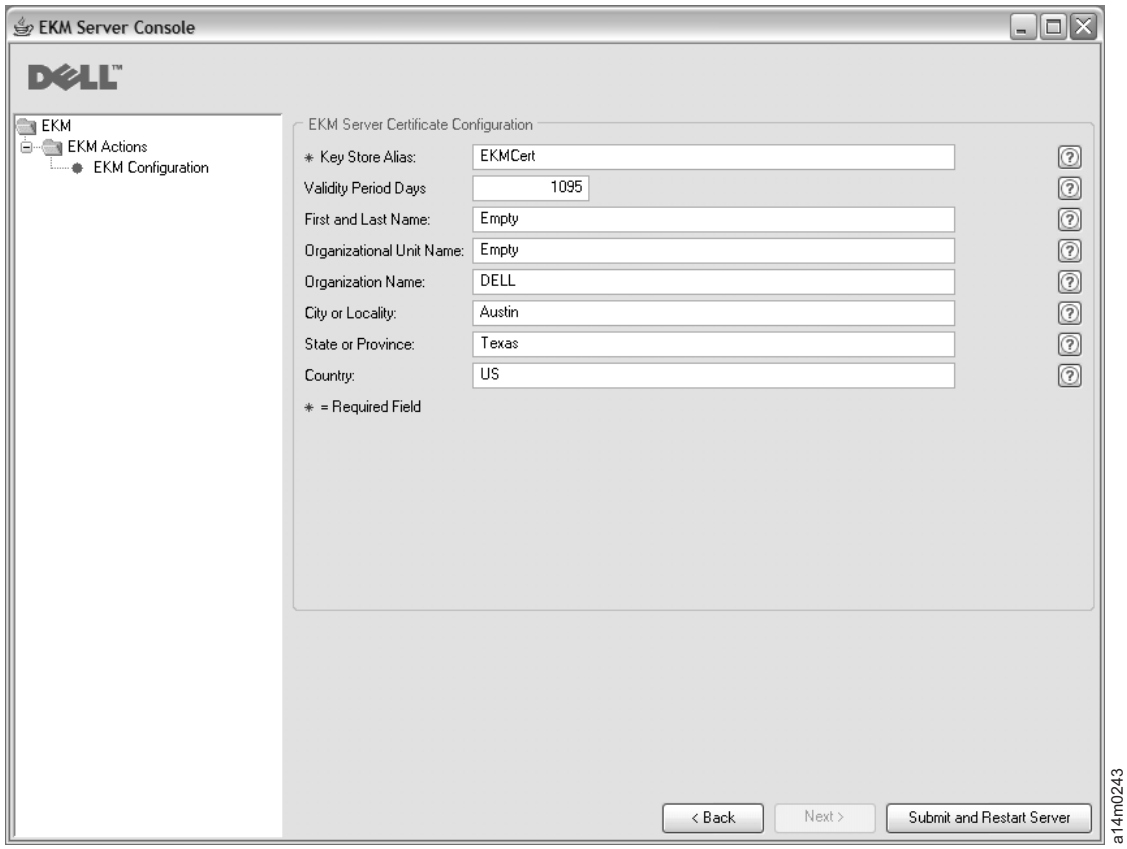

图 2. EKM Server Certificate Configuration 页面

注: 如在密钥生成期间中断加密密钥管理器 GUI，则将需要再次安装加密密钥管理器。

如果在加密密钥管理器密钥生成进程完成之前即将其关闭，那么密钥库文件将被损坏。要防止这种情况，请执行下列步骤:

- 如果加密密钥管理器在初始安装时被中断，请浏览到目录所在的位置（例如，x:\ekm）。删除该目录并重新启动安装。
- 如果添加新密钥组时加密密钥管理器被中断，请关闭加密密钥管理器服务器，并使用最新的备份密钥库（此文件位于 x:\ekm\gui\backupfiles 文件夹中）恢复您的密钥库文件。请注意，该备份文件以文件名一部分的形式包含该日期和时间戳记（例如，2007_11_19_16_38_31_EKMKeys.jck）。日期和时间戳记在文件复制到 x:\ekm\gui 目录中后就必须被除去。重新启动加密密钥管理器服务器并添加之前被中断的密钥组。

4. 将显示备份窗口（图 3），提醒您备份加密密钥管理器数据文件。请输入备份数据的保存路径。单击**备份**。

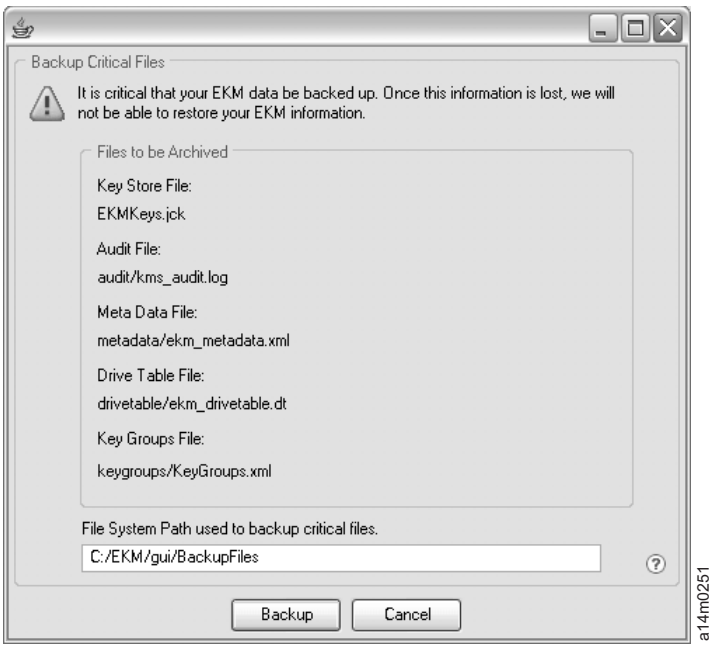

图 3. Backup Critical Files 窗口

5. 将显示用户登录页面。输入缺省用户名 EKMAdmin 和缺省密码 changeME。单击**登录**。

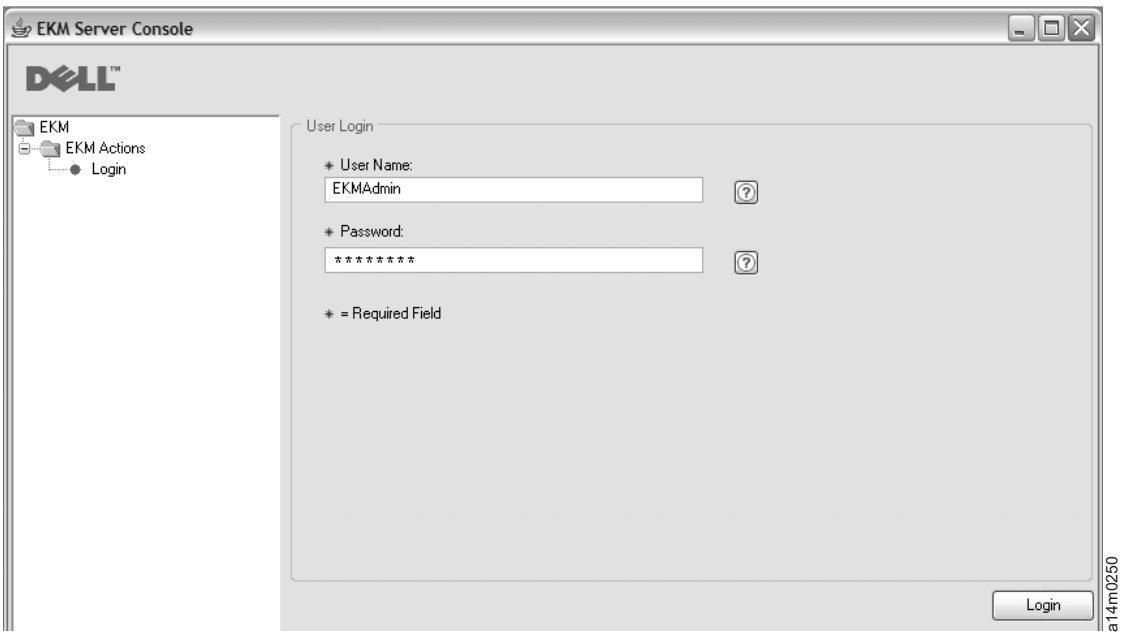

图 4. 用户登录页面

Dell 加密密钥服务器服务器在后台启动。

6. 在 GUI 导航器中选择 **Server Health Monitor** 以验证加密密钥管理器服务器是否已经启动。

如何查找正确的主机 IP 配置:

当前加密密钥管理器 GUI 中的限制可能使其无法在“服务器运行状况监视器”中显示加密密钥管理器主机 IP 地址。

- 如果主机配置为使用 IPv6 地址，那么加密密钥管理器应用程序将无法显示该 IP 地址。
- 如果加密密钥管理器应用程序安装在 Linux 系统中，那么该加密密钥管理器应用程序将显示本地主机地址，而不是实际的活动 IP 端口。

a. 要检索主机系统的实际 IP 地址，请通过访问网络配置查找 IP 端口地址。
   - 在 Windows 系统中，打开命令窗口并输入 `ipconfig`。
   - 对于 Linux，请输入 `isconfig`。

如何识别 EKM SSL 端口

a. 使用命令行启动加密密钥管理器服务器。
   - 在 Windows 上，浏览至 `c:\ekm` 并单击 **startServer.bat**
   - 在 Linux 平台上，浏览至 `/var/ekm` 并输入 `startServer.sh`
   - 有关更多信息，请参阅《*Dell 加密密钥管理器用户指南*》中的“启动、刷新和关闭密钥管理器服务器”。

b. 使用命令行启动 CLI 客户机。
   - 在 Windows 上，浏览至 `c:\ekm` 并单击 **startClient.bat**
   - 在 Linux 平台上，浏览至 `/var/ekm` 并输入 `startClient.sh`
   - 有关更多信息，请参阅《*Dell 加密密钥管理器用户指南*》中的“启动命令行界面客户机”。

c. 使用以下命令登录加密密钥管理器服务器上的 CLI 客户机:

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

   其中，*userID* = EKMAdmin 且 *password* = changeME（此为缺省密码。如果以前更改过缺省密码，请使用新密码。）

   登录如果成功，将显示 `User successfully logged in`。

d. 通过输入以下命令识别 SSL 端口:

   ```
   status
   ```

   显示的响应应类似: `server is running. TCP port: 3801, SSL port: 443.`

   记下 SSL 配置端口并确保该端口为用于配置您的库管理的加密设置的端口。

e. 从命令行注销。输入以下命令:

   ```
   exit
   ```

   关闭命令窗口。

方法 2: 使用命令设置加密密钥管理器

步骤 1. 创建 JCEKS 密钥库

注意: 强烈建议定期复制加密密钥管理器以及所有关联文件。一旦加密密钥管理器加密密钥丢失或损坏，将没有办法恢复加密的数据。

创建密钥库并使用证书和专用密钥对它进行填充。 证书用于保证加密密钥管理器服务器之间及其与加密密钥管理器 CLI 客户机通信的安全性。该 **keytool** 命令将创建名为 EKMKeys.jck 的新 JCEKS 密钥库，并使用别

名为 ekmcert 的证书和专用密钥对它进行填充。该证书的有效期为五年。该证书到期时，加密密钥管理器服务器之间以及加密密钥管理器服务器与加密密钥管理器 CLI 客户机之间的通信将无法再继续进行。请除去旧的到期证书，并按该步骤所指定创建新的证书。

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

该 keytool 命令提示您提供信息，它将使用该信息来创建认可您的加密密钥管理器身份的证书。这些提示以及样本响应类似于以下内容:

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

输入 yes 并按 Enter 键。

步骤 2. 生成加密密钥

注: 在会话中第一次使用 keytool 命令之前，请运行 **updatePath** 脚本以设置正确的环境。

在 Windows 上

浏览至 cd c:\ekm 并单击 click updatePath.bat

在 Linux 平台上

浏览至 /var/ekm 并输入 . ./updatePath.sh

注意: 在 Linux shell 命令之前指定 . ./ （句点空格句点正斜杠）以确保该shell 能够找到脚本。

对于 LTO 加密，加密密钥管理器需要在密钥库中预生成并存储大量对称密钥。该 **keytool** 命令生成 32 个 256 位 AES 密钥，并将它们存储在步骤 3 创建的密钥库中。从加密密钥管理器目录运行此命令，以在该目录中创建密钥库文件。生成密钥的名称将是 key000000000000000000 到 key0000000000000001f。

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

此命令提示您输入用于访问密钥库的密钥库密码。输入所需的密码并按 Enter 键。 当提示输入密钥密码时，再次按 Enter 键，因为不需要该信息。 不要输入新的或不同的密码。这将导致密钥密码与密钥库密码相同。 请记下此处输入的密钥库密码，因为以后启动加密密钥管理器 时将需要该密码。

注: 一旦设置了密钥库密码，除非违反了它的安全性，否则不要对它进行更改。更改密钥库密码还需要更改配置文件中所有的密码属性。密码采用加密形式，以消除安全性风险。

步骤 3. 启动加密密钥管理器服务器

要想不通过 GUI 来启动加密密钥管理器服务器，请启动 startServer 脚本:

在 Windows 上

浏览至 cd c:\ekm\ekmserver 并单击 startServer.bat

在 Linux 平台上

浏览至 /var/ekm/ekmserver 并输入 . ./startServer.sh

注意: 在 Linux shell 命令之前指定 . ./ （句点空格句点正斜杠）以确保该shell 能够找到脚本。

注意: 强烈建议定期复制加密密钥管理器以及所有关联文件。一旦加密密钥管理器加密密钥丢失或损坏，将没有办法恢复加密的数据。

步骤 4. 启动加密密钥管理器命令行界面客户机

要启动加密密钥管理器 CLI 客户机，请启动 startClient 脚本:

在 Windows 上

浏览至 `cd c:\ekm\ekmclient` 并单击 startClient.bat

在 Linux 平台上

浏览至 /var/ekm\ekmclient 并输入 `. ./startClient.sh`

注意: 在 Linux shell 命令之前指定 . ./ （句点空格句点正斜杠）以确保该shell 能够找到脚本。

CLI 客户机成功登录到密钥管理器服务器之后，您可以执行任何 CLI 命令。完成之后，请使用 quit 命令关闭 CLI 客户机。客户机在未用时间达 10 分钟时将自动关闭。关于 CLI 命令信息，请参阅位于以下位置的 *Dell 加密密钥管理器用户指南*: **http://support.dell.com** 或产品随附的 Dell 加密密钥管理器介质上。

更多信息

要获取更多信息，请参阅以下出版物。

- *Dell 加密密钥管理器用户指南*（包含在 Dell 加密密钥管理器 CD 上，并且可从 **http://support.dell.com** 获取）。
- *Library Managed Encryption for Tape* 白皮书，它推荐了关于 LTO 磁带加密的最佳实践（可从 **http://www.dell.com** 获取）。
