Dell™ PowerVault™ 加密密钥管理器

用户指南

Dell™ PowerVault™ 加密密钥管理器

用户指南

目录

图 v

表 vii

前言 ix

关于本书 ix
应阅读该书的读者 ix
本书中使用的约定和术语 ix
注意声明 ix
相关出版物 x
Linux 信息 x
Microsoft Windows 信息 x
在线支持. x

请先阅读 xi

联系 Dell xi

第 1 章 磁带机加密概述 1-1

组件 1-1
管理加密 1-2
应用程序管理的磁带加密 1-4
库管理磁带加密 1-5
关于加密密钥 1-5

第 2 章 规划加密密钥管理器环境. . . . 2-1

加密设置任务一览 2-1
加密密钥管理器设置任务 2-1
规划库管理的磁带加密 2-1
硬件和软件需求 2-2
Linux 解决方案组件 2-2
Windows 解决方案组件 2-3
密钥库注意事项 2-3
JCEKS 密钥库 2-3
加密密钥与 LTO 4 和 LTO 5 磁带机 2-4
备份密钥库数据 2-5
实现冗余的多个密钥管理器 2-6
加密密钥管理器服务器配置 2-7
灾难恢复站点注意事项 2-8
异地共享加密磁带的注意事项 2-9
联邦信息处理标准 140-2 注意事项 2-9

第 3 章 安装加密密钥管理器和密钥库 3-1

下载最新版密钥管理器 ISO 映像 3-1
在 Linux 上安装加密密钥管理器 3-1
在 Windows 上安装加密密钥管理器 3-2
使用 GUI 来创建配置文件、密钥库以及证书 . . . 3-5
在 LTO 4 和 LTO 5上生成加密密钥和别名 . . . 3-9
密钥组的创建与管理 3-13

第 4 章 配置加密密钥管理器 4-1

使用 GUI 来配置加密密钥管理器 4-1
配置策略 4-1
自动更新磁带机表 4-1
同步两个密钥管理器服务器之间的数据 4-2
配置基础 4-3

第 5 章 管理加密密钥管理器 5-1

启动、刷新和关闭密钥管理器服务器 5-1
命令行界面客户机 5-5
CLI 命令 5-7

第 6 章 问题确定 6-1

检查这些重要文件以确定加密密钥管理器服务器问题 6-1
调试 CLI 客户机和 EKM 服务器之间的通信问题 6-2
调试密钥管理器服务器问题 6-2
加密密钥管理器报告的错误 6-4
消息 6-7
未指定配置文件. 6-8
未能添加磁带机. 6-8
未能归档日志文件 6-8
未能删除配置 6-8
未能删除磁带机条目 6-9
未能导入 6-9
未能修改配置 6-9
文件名不能为空 6-10
文件大小限值不能是负数 6-10
未使任何数据同步. 6-10
输出无效. 6-11
配置文件中 SSL 端口号无效 6-11
配置文件中 TCP 端口号无效 6-11
必须在配置文件中指定 SSL 端口号 6-12
必须在配置文件中指定 TCP 端口号 6-12
服务器未能启动 6-12
Sync 失败 6-13
指定的审计日志文件仅可读. 6-13
无法装入 Admin 密钥库 6-13
无法装入密钥库 6-14
无法装入传输密钥库 6-14
不受支持的操作 6-14

第 7 章 审计记录 7-1

审计概述 7-1
审计配置参数 7-1
Audit.event.types 7-1
Audit.event.outcome 7-2
Audit.eventQueue.max 7-2
Audit.handler.file.directory 7-2
Audit.handler.file.size 7-3
Audit.handler.file.name 7-3
Audit.handler.file.multithreads 7-3
Audit.handler.file.threadlifespan 7-4
审计记录格式 7-4

加密密钥管理器中的审计要点 7-4
审计记录属性 7-5
审计事件 7-6

第 8 章 使用元数据 8-1

附录 A. 文件示例 A-1
启动守护程序脚本样本 A-1
Linux 平台 A-1
配置文件示例 A-1

附录 B. 加密密钥管理器配置属性文件 B-1
加密密钥管理器服务器配置属性文件 B-1
CLI 客户机配置属性文件 B-8

附录 C. 常见问题解答 C-1

声明 D-1
商标 D-1

词汇表. E-1

索引 X-1

图

1-1. 加密密钥管理器的四个主组件 1-2
1-2. 加密策略引擎和密钥管理的两个可能位置: 1-4
1-3. 使用对称加密密钥的加密 1-6
2-1. LTO 4 或 LTO 5 磁带机请求加密写操作 2-4
2-2. LTO 4 或 LTO 5 磁带机请求加密读操作 2-5
2-3. Backup Critical Files 窗口 2-6
2-4. 单服务器配置 2-7
2-5. 两个带有共享配置的服务器 2-8
2-6. 两个配置不同的服务器访问相同的设备 2-8
3-1. Choose Destination Location 窗口 3-3
3-2. 将该版本的 JVM 设置为缺省 3-3
3-3. Start Copying Files 窗口 3-4
3-4. EKM Server Configuration 页面 3-6
3-5. EKM Server Certificate Configuration 页面 3-7
3-6. Backup Critical Files 窗口 3-7
3-7. 创建密钥组 3-14
3-8. 更改缺省写密钥组 3-15
3-9. 将组指定给磁带机 3-16
3-10. 删除磁带机 3-17
5-1. 服务器状态 5-1
5-2. Login 窗口 5-2

表

1. 本书中使用的印刷体约定 ix
1-1. 加密密钥摘要 1-6
2-1. Linux 的最小软件需求 2-2
2-2. Windows 的最小软件需求 2-3
6-1. 加密密钥管理器报告的错误 6-5
7-1. 加密密钥管理器写入审计文件的审计记录类型 7-4
7-2. 依照审计事件的审计记录类型 7-6
8-1. 元数据查询输出格式 8-2

前言

关于本书

本手册包含了 Dell™ 加密密钥管理器的安装和操作所需的信息和指示信息。它包含关于以下内容的概念和过程:

- 可加密 LTO 4 和 LTO 5 磁带机
- 密钥
- 数字证书

应阅读该书的读者

本书用于负责重要数据安全和备份的存储和安全管理员，以及协助在操作环境中安装和维护加密密钥管理器服务器的所有人员。它假定读者具有关于存储设备和网络的工作经验和知识。

本书中使用的约定和术语

本书使用以下印刷体约定:

表 1. 本书中使用的印刷体约定

约定	用途
粗体	**粗体**单词或字符代表必须按字面使用的系统元素，例如命令名称、文件名、标志名称、路径名和选定菜单选项。
固定宽度	示例、用户指定的文本和系统显示的信息以固定宽度字型显示。
斜体	*斜体*单词或字符代表必须提供的变量值。
[项]	指示可选项。
{项}	对列表加上括号，您必须从列表的格式和语法描述中选择某项。
|	竖线用于分隔选项列表中的各项。
<键>	指示所按的键。

注意声明

注意声明指示可能对程序、设备、系统或数据造成危害的可能性。惊叹号可能伴随着注意声明，但这不是必需的。注意声明示例如下所示:

警告: 如果使用电动螺丝刀来执行此过程，那么可能损坏磁带。

相关出版物

有关更多信息，请参阅以下出版物:

- *Getting Started with the Dell™ PowerVault™ TL2000 and TL4000 Tape Libraries* 提供了安装信息。
- *Dell™ PowerVault™ TL2000 Tape Library and TL4000 Tape Library SCSI Reference* 提供了管理 SCSI 接口行为的受支持 SCSI 命令和协议。

Linux 信息

Red Hat 信息

以下 URL 与 Red Hat Linux® 系统相关:

- **http://www.redhat.com**

SuSE 信息

以下 URL 与 SuSE Linux 系统相关:

- **http://www.suse.com**

Microsoft Windows 信息

以下 URL 使您能够访问关于 Microsoft® Windows® 系统的信息:

- **http://www.microsoft.com**

在线支持

请访问 **http://support.dell.com** 以获取以下相关出版物:

Dell Encryption Key Manager Quick Start Guide 提供关于设置基本配置的信息。

请访问 **http://support.dell.com** 以获取以下相关出版物:

Library Managed Encryption for Tape 白皮书提出了 LTO 磁带加密的最佳实践。

请先阅读

联系 Dell

美国客户可以致电：800-WWW-DELL（800-999-3355）。

注: 如果您不可用因特网连接，可以在您的购买发票、装箱单、帐单或 Dell 产品目录上找到联系信息。

Dell 提供了几个在线和电话支持和服务选项。每个国家和产品的可用性是不同的，在您所在的区域中一些服务可能是没有的。要想联系 Dell 获得有关销售、技术支持或客户服务问题的信息，

1. 请访问 **http://support.dell.com**。
2. 在页面下方的**选择一个国家/地区**下拉菜单验证您的国家或地区。
3. 单击页面左边的**联系我们**。
4. 根据您的需要选择合适的服务或支持连接。
5. 选择适合您的联系方法来联系 Dell。

第 1 章 磁带机加密概述

数据在竞争激烈的商业环境中是最宝贵的资源。在今天对安全非常敏感的世界中，保持数据可用性的同时保护数据、控制对数据的访问和验证数据真实性是我们的优先工作目标。数据加密是响应这些需求的一个工具。Dell 加密密钥管理器（以下称为加密密钥管理器）简化了加密任务。

LTO 4 和 LTO 5 磁带机能够加密写到任何 LTO 4 和 LTO 5 数据盒带上的数据。该新功能将更严格的安全措施添加到已存储数据，而不会由于在服务器上执行加密而增加处理开销或降低处理速度，或支付专用设备的开销。

磁带机加密解决方案由以下 3 个主要元素组成:

支持加密的磁带机

所有 LTO 4 和 LTO 5 磁带机都必须通过库接口启用。

关于磁带机的更多信息，请参阅第 2-2 页的『硬件和软件需求』。

加密密钥管理

加密包括在多个连续层中使用若干种密钥。这些密钥的生成、维护、控制和传输依赖于安装了加密磁带机的操作环境。有些应用程序，能够执行密钥管理。对于没有此类应用程序的环境或要求使用应用程序不可知加密的环境， Dell 加密密钥管理器执行所有必需的密钥管理任务。 第 1-2 页的『管理加密』更详细地描述这些任务。

加密策略

加密策略指的是用于实施加密的方法。它包括规定加密哪些卷和密钥选择机制的规则。设置这些规则的方式和位置取决于操作环境。关于更多信息，请参阅第 1-2 页的『管理加密』。

组件

加密密钥管理器是 Java 环境的一部分，并将 Java Security 组件用于它的加密功能。（有关 Java Security 组件的更多信息，请参阅相关的出版物部分。）加密密钥管理器具有三个用来控制其行为的主组件。这些组件是:

Java 安全性密钥库

密钥库被定义为 Java 密码术扩展（JCE）的一部分和 Java 安全性组件的一个元素，它们反过来又是 Java 运行时环境的一部分。密钥库保存有加密密钥管理器用于执行加密操作的证书和密钥（或者指向证书和密钥的指针）。可支持几种类型的 Java 密钥库，用于提供不同的操作功能，以满足您的需求。这些特征在第 2-3 页的『密钥库注意事项』中进行了详细讨论。

保留密钥库数据的重要性并不是夸张。如果未访问密钥库，那么将无法解密您的加密磁带。请仔细阅读以下主题以理解可用来保护密钥库数据的方法。

配置文件

配置文件使您能够定制加密密钥管理器的行为以满足组织的需要。本文档对这

些行为选项进行了大量描述，首先在第 2-1 页的第 2 章，『规划加密密钥管理器环境』，其次在第 4-1 页的第 4 章，『配置加密密钥管理器』，之后在描述一组完整配置选项的附录 B 中进行了描述。

磁带机表格

磁带机表格由加密密钥管理器用于跟踪其支持的磁带设备。磁带机表格是一个非编辑的二进制文件，其位置指定在配置文件中。可以更改其位置来满足您的需要。

KeyGroups.xml 文件

该保护密码的文件包含所有加密密钥组的名称，以及与每个密钥组关联的加密密钥的别名。

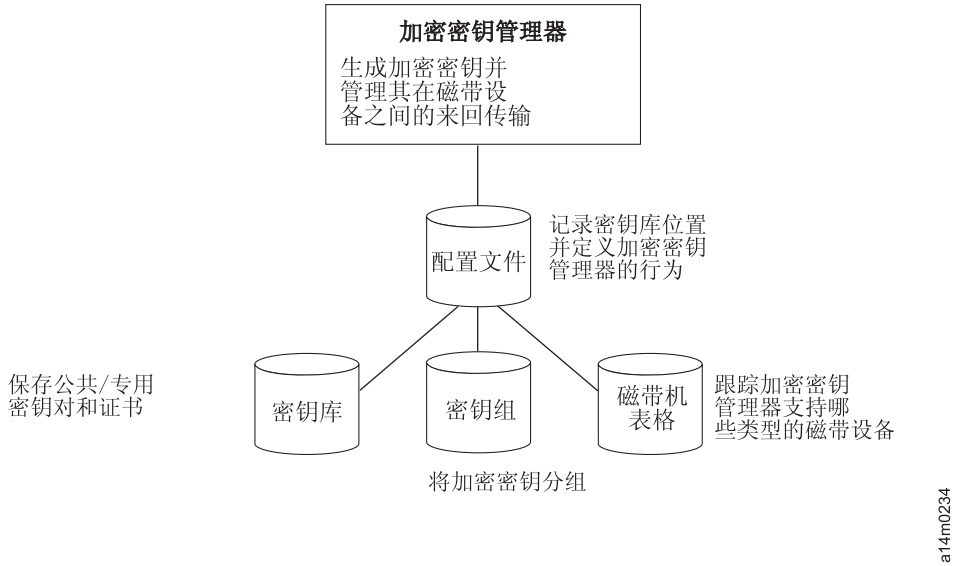

图 1-1. 加密密钥管理器的四个主组件

管理加密

Dell 加密密钥管理器是一种 Java™ 软件程序，该程序用于在 支持加密的磁带机上生成、保护、存储和维护加密密钥，该加密密钥用于对写到磁带介质（磁带和盒带格式）的信息进行加密以及对从磁带介质读取的数据进行解密。加密密钥管理器运行于 Linux（SLES 和 RHEL） 和 Windows 上，旨在作为部署在企业中多个位置的共享资源，并在后台运行。命令行界面客户机提供了丰富的命令集，用于针对您的环境定制加密密钥管理器，并监视其运行。许多定制和监视功能可以通过 Dell 加密密钥管理器图形用户界面（GUI）获取。加密密钥管理器使用一个或多个密钥库来保存所有加密任务所必需的证书和密钥（或指向证书和密钥的链接）。详细信息请参阅第 2-3 页的『密钥库注意事项』。

重要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。

加密密钥管理器作为后台进程运行，该进程等待通过 TCP/IP 通信路径发送到该进程的密钥生成或密钥抽取请求，该 TCP/IP 通信路径位于进程本身和磁带库。磁带机写加密的数据时，它将首先从加密密钥管理器请求获得一个加密密钥。收到请求时，加密密钥管理器将执行以下任务:

加密密钥管理器从密钥库获取已存在的 AES 密钥，并对它进行绑定，以安全地传输到磁带机，并在到达磁带机后被解开，用于对写到磁带的数据进行加密。

加密磁带由 LTO 4 或 LTO 5 磁带机读取时，加密密钥管理器根据磁带上密钥标识中的信息从密钥库获取必需的密钥，对密钥进行绑定，以将它安全地传送到磁带机。

有两种加密管理方法可供选择。这些方法的区别在于：加密测量引擎所在位置、为解决方案执行密钥管理的位置，以及加密密钥管理器与磁带机的连接方式。您的操作环境决定哪种方法最适合您。密钥管理和加密策略引擎可能位于以下两个环境层的其中一个中。

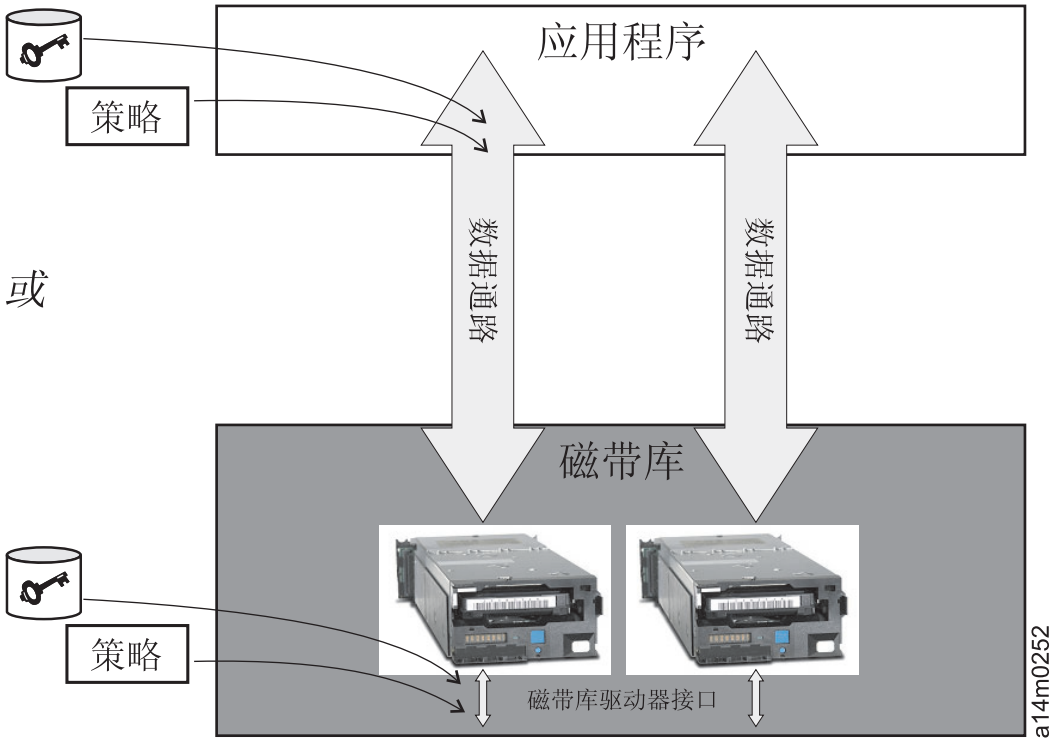

图 1-2. 加密策略引擎和密钥管理的两个可能位置:

应用程序层

一个应用程序，独立于密钥管理器，用于启动磁带存储器的数据传输。关于受支持的应用程序，请参阅『应用程序管理的磁带加密』。

库层

磁带存储器的外壳，比如 Dell PowerVault TL2000/TL4000 和 ML6000 系列。最新的磁带库在磁带库内的每个磁带机上都含有一个内部接口。

应用程序管理的磁带加密

当操作环境运行的应用程序已能够生成和管理加密策略和密钥时，此方法最适用。指定何时使用加密的策略可通过应用程序界面进行定义。策略和密钥通过应用层和加密磁带机之间的数据通路. 加密是应用程序和支持加密的磁带机之间进行交互的结果，并且不需要对系统和库层进行任何更改。由于应用程序管理加密密钥，因而使用应用程序方法写入和加密的卷只能通过写入它们的相同应用程序，使用应用程序管理的加密方法进行读取。

应用程序管理的磁带加密不需要，也不使用 **加密密钥管理器。**

以下最小版本的应用程序可用来管理加密:

- CommVault Galaxy 7.0 SP1
- Symantec Backup Exec 12

应用程序管理的磁带加密在以下产品的 LTO 4 和 LTO 5 磁带机中受到支持:

- Dell™ PowerVault™ TL2000 Tape Library
- Dell™ PowerVault™ TL4000 Tape Library
- Dell™ PowerVault™ ML6000 Tape Library

请参阅磁带备份软件应用程序文档以了解如何管理加密策略和密钥。

库管理磁带加密

针对 Dell™ PowerVault™ TL2000 Tape Library、Dell™ PowerVault™ TL4000 Tape Library或 Dell™ PowerVault™ ML6000 Tape Library 中的 LTO 4 和 LTO 5 磁带机使用该方法。 密钥的生成和管理通过在附带库主机上运行的 Java 应用程序加密密钥管理器来实现。策略控制和密钥经由库 – 磁带机接口，因此对应用程序来说，加密是透明的。

关于加密密钥

加密密钥是特别生成的随机的位串以加密和解密数据。使用设计的算法来创建加密密钥以确保每个密钥的唯一性和不可预测性。通过这种方式构造的密钥越长，中断加密代码将越难。IBM 和 T10 加密的方法都使用 256 位的 AES 算法密钥以加密数据。256 位 AES 是美国政府当前认可和建议使用的加密标准，它允许三个不同的密钥长度。256 位密钥是 AES 允许的最长密钥。

加密密钥管理器使用两类加密算法: 对称算法和非对称算法。对称或者秘密密钥加密使用一个密钥进行加密和解密。一般情况下，使用对称密钥加密可有效地加密大量数据。256 位 AES 密钥是对称密钥。非对称，或者公用/专用加密使用一对密钥。对于使用一个密钥加密的数据，您只能使用公用/专用密钥对的其他密钥进行解密。生成非对称密钥对之后，公用密钥将用来加密，而专用密钥将用来解密。

加密密钥管理器同时使用对称和非对称密钥; 用户或主机数据高速加密的对称加密，以及用来保护对称密钥的非对称加密（必须较慢）。

加密密钥管理器 的加密密钥可以由实用程序（例如 Keytool）生成。负责生成 AES 密钥和采用何种方式将它们传送到磁带机将取决于加密管理的方法。但是，理解加密密钥管理器对加密密钥的使用方式和其他应用程序对加密密钥的使用方式之间的区别，将有所帮助。

Dell 加密密钥管理器处理的加密密钥

在库管理的磁带加密中，未加密数据将发送到 LTO 4 或 LTO 5 磁带机，并使用预生成的对称数据密钥 (DK) 从可用于加密密钥管理器的密钥库中转换为密文，然后写入磁带。加密密钥管理器以循环算法的方式选择预生成的 DK。预生成的 DK 数量不足时，将在多个盒式磁带上重新使用 DK。DK 由加密密钥管理器以加密或打包的格式发送到 LTO 4 或 LTO 5 磁带机。LTO 4 和 LTO 5 磁带机对该 DK 进行解包，并使用它进行加密或解密。但是，在 LTO 4 或 LTO 5 盒式磁带上未存储任何打包的密钥。 写入加密卷之后，您必须根据别名或密钥标注来访问 DK，并且该 DK 必须用于加密密钥管理器以读取卷。第 1-6 页的图 1-3显示此过程。

Dell 加密密钥管理器还使您能够将 LTO 加密的对称密钥组织到密钥组中。使用此方法，您可以根据加密数据的类型、访问加密数据的用户或任何其他有意义的特性来组织密钥。请参阅第 3-13 页的『密钥组的创建与管理』，以了解更多信息。

其他应用程序处理的加密密钥

在应用程序管理的磁带加密中，未加密数据将发送到 LTO 4 和 LTO 5 磁带机，并使用应用程序所提供的对称 DK 转换为密文，然后写入磁带。在盒式磁带上的任何地方未存储 DK。写入加密卷之后，DK 必须处于可用于应用程序（例如，服务器数据库）的某个位置以读取卷。

LTO 4 和 LTO 5 磁带机可以使用应用程序（例如，Yosemite（针对 Dell PowerVault TL2000 和 TL4000 磁带库）、CommVault 和 Symantec Backup Exec）以进行应用程序管理的加密。

或者，LTO 4 和 LTO 5 磁带机可以由采用 T10 命令集以执行加密的应用程序使用。T10 命令集使用应用程序提供的对称 256 位 AES 密钥。T10 可以为每个盒式磁带使用多个和唯一的 DK，甚至可以将加密数据和清除数据写入同一盒式磁带中。应用程序对盒式磁带进行加密时，它将采用应用程序确定的方法选择或生成 DK，然后将它发送到磁带机。**未**使用非对称公用密钥对密钥进行打包，也**未**在盒式磁带上对其进行存储。将加密数据写入磁带之后，DK 必须处于可用于应用程序的某个位置以读取数据。

图 1-3显示应用程序管理和库管理加密的磁带加密的过程。

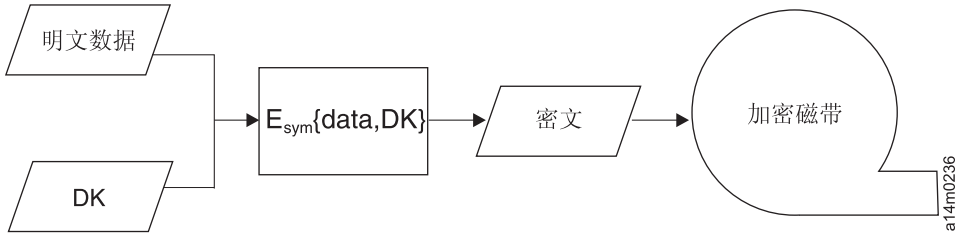

图 1-3. 使用对称加密密钥的加密. LTO 4 和 LTO 5 磁带机上的库管理和应用程序管理的加密。

总而言之

可用于每卷的加密密钥的数量取决于磁带机、加密标准和用来管理加密的方法。对于 LTO 4 和 LTO 5的透明加密（也就是说，通过加密密钥管理器使用库管理的加密），DK 的唯一性取决于加密密钥管理器可以使用的预生成密钥的数量是否充足。

表 1-1. 加密密钥摘要

	密钥使用对象	
加密管理方法	**IBM 加密**	**T10 加密**
库管理的加密	1 DK/磁带盒	不适用
应用程序管理的加密	多个 DK/磁带盒	多个 DK/磁带盒
DK 即对称 AES 256 位的 DK		

第 2 章 规划加密密钥管理器环境

本部分旨在提供信息以使您能够确定满足您的需求的最佳加密密钥管理器配置。规划如何设置加密策略时，您必须考虑多个因素。

加密设置任务一览

可以使用磁带机的加密功能之前，您必须满足某些软件和硬件的需求。以下核对表旨在帮助您满足这些需求。

加密密钥管理器设置任务

在您加密磁带之前，必须先配置好并运行加密密钥管理器，以便它与加密磁带机进行通信。在安装磁带机时，不需要运行加密密钥管理器，但在执行加密时必须使其运行。

- 选择使用何种系统平台作为加密密钥管理器服务器。
- 如有必要，请升级服务器操作系统。（请参阅第 2-2 页的『硬件和软件需求』。）
- 安装 Java 自由策略文件。（请参阅第 2-2 页的『硬件和软件需求』。）
- 升级加密密钥管理器 JAR。（请参阅 第 3-1 页的『下载最新版密钥管理器 ISO 映像』。）
- 创建密钥、证书以及密钥组。

  第 3-5 页的『使用 GUI 来创建配置文件、密钥库以及证书』

  第 3-13 页的『密钥组的创建与管理』
- 如果您遵循第 3-5 页的『使用 GUI 来创建配置文件、密钥库以及证书』中的步骤，这些步骤不再需要，除非您想利用其他配置选项:
  - 如果需要，请导入密钥和证书。（请参阅第 3-11 页的『使用 Keytool -importseckey 导入数据密钥』。）
  - 定义配置属性文件。（请参阅第 4-1 页的第 4 章，『配置加密密钥管理器』。）
  - 定义磁带机加密密钥管理器或设置 **drive.acceptUnknownDrives** 配置属性值为有效状态。（请参阅第 5-7 页的『adddrive』以明确定义磁带机,或参阅第 4-1 页的『自动更新磁带机表』。）
  - 启动加密密钥管理器服务器。（请参阅第 5-1 页的『启动、刷新和关闭密钥管理器服务器』。）
  - 启动命令行界面客户机。（请参阅第 5-5 页的『命令行界面客户机』。）

规划库管理的磁带加密

要执行加密操作，您需要:

- 可加密 LTO 4 和 LTO 5 磁带机
- 密钥库
- Dell 加密密钥管理器

库管理的磁带加密任务

1. 安装和启用 LTO 4 和 LTO 5 磁带机。
   - 更新库固件（在必要时，TL2000、TL4000 和 ML6000）。请访问 **http://support.dell.com**。
     - Dell™ PowerVault™ TL2000 Tape Library 所需的最小固件版本是 5.xx。
     - Dell™ PowerVault™ TL4000 Tape Library 所需的最小固件版本是 5.xx。
     - Dell™ PowerVault™ ML6000 Tape Library 所需的最小固件版本系列是 415G.xxx。
   - 如有必要，更新磁带机固件。所需的最小固件版本是 77B5。
2. 启用 LTO 4 和 LTO 5 磁带机和磁带库，以进行库管理的磁带加密 （请参阅 Dell 磁带库信息以了解详细情况）。
   - 添加加密密钥管理器 服务器 IP 地址
3. 使用库诊断行为以验证加密密钥管理器路径和加密配置（请参阅 Dell 磁带库信息以了解详细情况）。

硬件和软件需求

注: 对于以下各个平台，只有 IBM 版本的 Java 运行时环境（JRE）才支持加密密钥管理器。

Linux 解决方案组件

操作系统

- RHEL 4
- RHEL 5
- SLES 9
- SLES 10
- SLES 11

加密密钥管理器（在 Linux 上运行）

表 2-1. Linux 的最小软件需求

平台	IBM Software Developer Kit	可用于:
64 位 AMD/Opteron/EM64T	Java 6.0 SR5	**http://support.dell.com**
32 位可兼容的 Intel®		

磁带库

对于 Dell PowerVault TL2000 磁带库、TL4000 磁带库和 ML6000 磁带库，确保固件为最新可用级别。有关固件更新的信息，请访问 **http://support.dell.com**。

磁带机

对于 LTO 4 和 LTO 5 磁带机，确保固件为最新可用级别。有关固件更新的信息，请访问 **http://support.dell.com**。

Windows 解决方案组件

操作系统

Windows Server 2003、2008 和 2008 R2

Dell 加密密钥管理器

所需的加密密钥管理器最小版本是 2.1，构建日期是 20070914 或更晚，并处于以下某一个 IBM 运行时环境:

表 2-2. Windows 的最小软件需求

操作系统	IBM 运行时环境
Windows 2003	• IBM® 64-bit Runtime Environment for Windows on AMD64/EM64T architecture, Java 2 Technology Edition, V5.0 SR5 • IBM 32-bit Runtime Environment for Windows, Java 2 Technology Edition, V5.0 SR5
Windows 2008 和 2008 R2	IBM 64-bit Runtime Environment for Windows on AMD64/EM64T architecture, Java 2 Technology Edition, V6.0 SR5

磁带库

对于 Dell™ PowerVault™ TL2000 Tape Library、 Dell™ PowerVault™ TL4000 Tape Library和 Dell™ PowerVault™ ML6000 Tape Library，确保固件为最新可用级别。有关固件更新的信息，请访问 **http://support.dell.com**。

磁带机

对于 LTO 4 和 LTO 5 磁带机，确保固件为最新可用级别。有关固件更新的信息，请访问 **http://support.dell.com**。

密钥库注意事项

保留密钥库数据至关重要。如果未访问密钥库，那么将无法解密您的加密磁带。仔细阅读以下主题以理解可用来保护密钥库数据的方法。

JCEKS 密钥库

EKM 支持 JCEKS 密钥库类型。

JCEKS（基于 Unix 系统服务 文件）是 基于文件的密钥库，它在运行 EKM 的所有平台上均受支持。因此，复制此密钥库的内容以进行备份和恢复，以及使两个 EKM 实例在故障转移时保持同步是相对容易的。出于安全方面的考虑，JCEKS 对密钥库内容提供了基于密码的保护，并提供了相对较好的性能。可以使用诸如 FTP 的文件复制方法。

加密密钥与 LTO 4 和 LTO 5 磁带机

Dell 加密密钥管理器 及其支持的磁带机都使用对称的 256 位 AES 密钥来加密数据。该主题解释您应了解关于这些密钥和证书的哪些内容。

在使用 LTO 盒式磁带的 LTO 4 或 LTO 5 磁带机上执行加密任务时，加密密钥管理器仅使用 256 位 AES 对称数据密钥。

在 LTO 4 或 LTO 5 请求密钥时，加密密钥管理器使用为磁带机指定的别名。如果未为磁带机指定任何别名，那么将使用一个来自 symmetricKeySet 配置属性中指定的密钥组、密钥别名列表或密钥别名范围的别名。如果磁带机缺少特定的别名，那么将以循环法从其他实体选择别名，以均衡地使用密钥。

选定的别名与预装入到密钥库中的对称数据密钥（DK）相关联。加密密钥管理器将把用磁带机可以解密的不同密钥打包的该 DK 发送到 LTO 4 或 LTO 5 磁带机以加密数据。该 DK 不是通过 TCP/IP 明文传送。选定的别名也将转换为称为“数据密钥标识符（DKi）”的实体，该实体将用加密数据写到磁带。通过这种方式，加密密钥管理器可以使用 DKi 来识别读取 LTO 4 或 LTO 5 磁带时解密数据所需要的正确 DK。

第 5-7 页的『CLI 命令』中的 **adddrive** 和 **moddrive** 主题说明如何为磁带机指定别名。请参阅第 3-9 页的『在 LTO 4 和 LTO 5上生成加密密钥和别名』，它含有关于在 symmetricKeySet 配置属性中导入密钥、导出密钥和指定缺省别名的信息。第 3-13 页的『密钥组的创建与管理』说明如何定义密钥组和用密钥库中的别名填充该密钥组。

图 2-1说明执行加密写操作时如何处理密钥。

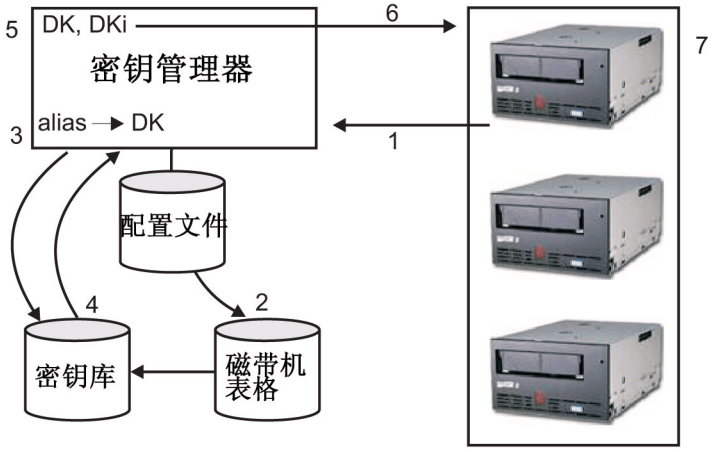

图 2-1. LTO 4 或 LTO 5 磁带机请求加密写操作

1. 磁带机请求对磁带加密的密钥
2. 加密密钥管理器验证磁带机表格中的磁带设备
3. 如果请求中未指定任何别名，且磁带机表格中未指定任何别名，加密密钥管理器将从 keyAliasList 中的别名集或密钥组选择一个别名。
4. 加密密钥管理器从密钥库获取相应的 DK。
5. 加密密钥管理器将该别名转换为 DKi，并将该 DK 与磁带机可以解密的密钥打包在一起
6. 加密密钥管理器将 DK 和 DKi 发送到磁带机

7. 磁带机解开 DK 并将加密数据和 DKi 写到磁带

图 2-2说明执行加密读操作时如何处理密钥。

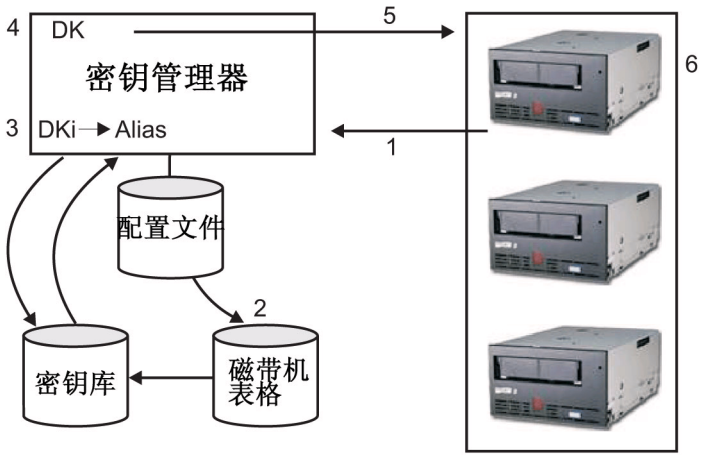

图 2-2. LTO 4 或 LTO 5 磁带机请求加密读操作

1. 磁带机收到读请求，并将 DKi 发送到加密密钥管理器
2. 加密密钥管理器验证磁带机表格中的磁带设备
3. 加密密钥管理器将 DKi 转译为别名并从密钥库获取相应的 DK
4. 加密密钥管理器将该 DK 与磁带机可以解密的密钥打包在一起
5. 加密密钥管理器将打包的 DK 发送到磁带机
6. 磁带机解开 DK 并用它来解密数据

备份密钥库数据

注: 由于密钥库中密钥的临界性质，您需要在非加密盘上备份此数据，这一点是十分重要的，这样您就可以在需要时恢复数据，并且能够使用与磁带机或库关联的那些证书读出加密磁带。备份密钥库失败将会导致不可撤消的丧失所有加密数据的访问权。

备份密钥库信息有许多方法。每个密钥库类型都有其独立的特征。中有较为详细的论述。这些一般的指导方针适用于所有类型:

- 保存所有装入到密钥库的证书的副本（通常是 PKCS12 格式文件）。
- 使用系统备份功能（例如 RACF）来创建密钥库信息的备份副本（注意不要用加密磁带机加密此副本，因为如果这样做，就不可能解密副本以进行恢复）。
- 维护主要和辅助的加密密钥管理器以及密钥库副本（用于备份和故障转移冗余）。备份主要和辅助的密钥库以用于添加冗余。
- 对于 JCEKS 密钥库，仅复制密钥库文件并将清晰的（未加密的）副本存储到安全的位置，例如保险库文件（注意不要用加密磁带机加密此副本，因为如果这样做，就不可能解密副本以进行恢复）。

至少，当您更改密钥库数据时，应该随时进行备份。加密密钥管理器并不修改密钥库数据。唯一能改变密钥库的，就是您对其进行的更改，所以请确保一旦更改了密钥库，立即对其进行复制。

用 GUI 备份文件

1. 打开 GUI（如果它并未启动）：

   Windows 上

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

   Linux 平台上

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

2. 在加密密钥管理器 GUI 左边的导航器中选择 **Backup Critical Files**。
3. 在显示的对话中输入备份数据的路径（图 2-3）。

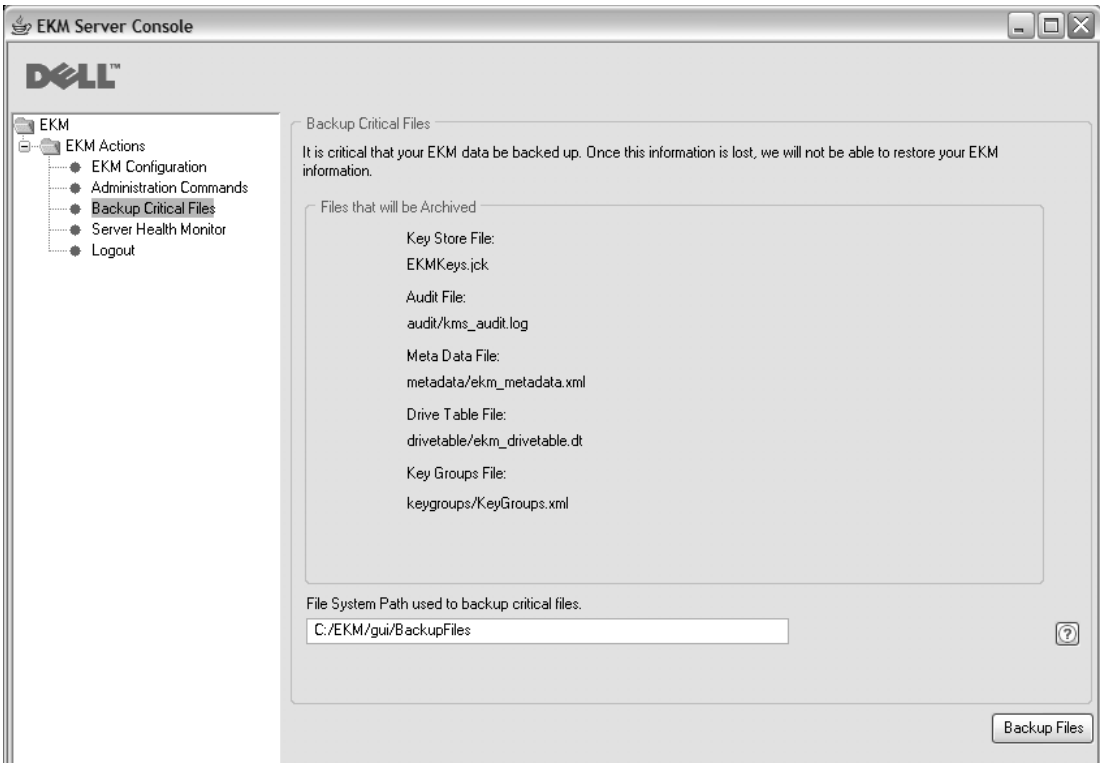

图 2-3. Backup Critical Files 窗口

4. 单击 **Backup Files**。
5. 将有一条参考消息显示结果。

实现冗余的多个密钥管理器

加密密钥管理器被设计用于磁带机和磁带库，以实现冗余，并因此获得更高的可用性，以使您拥有用于同一磁带机和磁带库的多个密钥管理器。但是，这些密钥管理器无需与磁带机和磁带库位于同样的系统上。密钥管理器的最大数取决于磁带库或代理。唯一的要求是这些密钥管理器必须通过 TCP/IP 连接用于磁带机上。

这样就使您拥有两个加密密钥管理器，两者是彼此之间的镜像，并具有密钥库重要信息的内置备份，以及在一个密钥管理器不可用时发挥作用的故障转移功能。配置设备（或代理）时，您可以将它指向两个密钥管理器。如果其中一个密钥管理器由于任何原因而变得不可用，您的设备（或磁带库）将立马启用备用的密钥管理器。

您还可以保持两个加密密钥管理器的同步。需要时利用该功能非常重要，这不仅由于它对重要数据进行内置备份，还由于其能够防止磁道运行被中断的故障转移功能。请参阅第 4-2 页的『同步两个密钥管理器服务器之间的数据』。

注: 同步不包括密钥库。您必须对它们进行手动复制。

加密密钥管理器服务器配置

加密密钥管理器可安装在单个或多个服务器上。以下示例说明一个密钥和两个密钥的管理器配置，但您的库可能允许配置更多。

单服务器配置

单服务器配置（如图 2-4中显示）是最简单的加密密钥管理器配置。但是，由于缺乏冗余，建议您不要使用该服务器配置。在此配置中，所有磁带机均依赖于不带任何备份的单密钥管理器服务器。一旦服务器关闭，那么密钥库、配置文件、KeyGroups.xml file, 和磁带机表格将无法使用，导致所有加密磁带无法读取。在单服务器配置中，您必须确保密钥库、配置文件、KeyGroups.xml 文件，以及磁带机表格的备份副本保留在安全的位置（不同于加密密钥管理器），以便在丢失服务器副本的情况下，可以在替换服务器上重新构建其功能。

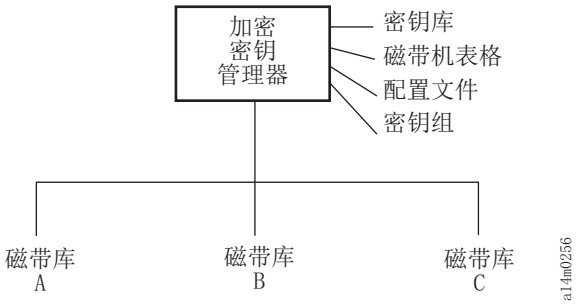

图 2-4. 单服务器配置

两个服务器的配置

建议使用两个服务器的配置。如果由于某种原因无法访问主密钥管理器，那么该加密密钥管理器配置将自动故障转移到辅助密钥管理器。

注: 使用不同的加密密钥管理器服务器处理一组相同磁带机的请求时，关联密钥库中的信息必须完全相同。要求做到这一点是为了，无论联系哪一个密钥管理器服务器，信息必须可用来支持磁带机的请求。

相同配置: 在两个具有相同配置的加密密钥管理器服务器的环境中（例如，第 2-8 页的图 2-5中显示的服务器），如果主密钥管理器当机，那么处理将自动故障转移到辅密钥管理器。在此类配置中，必须使两个密钥管理器服务器同步。配置文件更新和一个密钥管理器服务器的磁带机表格更新可以复制到自动使用 **sync** 命令的其他密钥管理器服务器，但是一个密钥库更新必须复制到使用某些方法的其他密钥库（这些方法特定于正在使用的密钥库）。必须手动复制密钥库和密钥组 XML 文件。请参阅第 4-2 页的『同步两个密钥管理器服务器之间的数据』以获取更多信息。

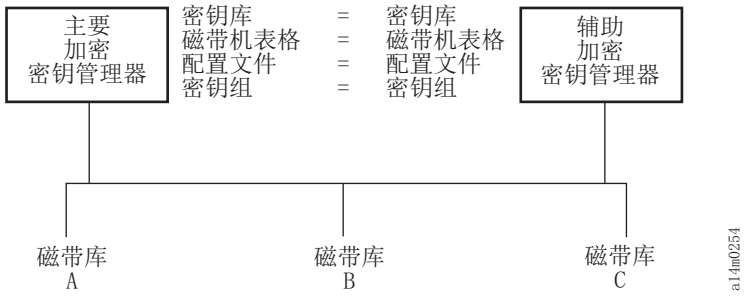

图 2-5. 两个带有共享配置的服务器

不同配置: 两个加密密钥管理器服务器可能共享一个公用密钥库和磁带机表格，但是也可能具有两个不同的配置文件和两组不同的密钥组，正如在它们的 XML 文件中所定义的一样。唯一的需求是用来服务于公共磁带机的密钥针对每个服务器必须相同。这使每个密钥管理器服务器均能够具有自身的属性组。在此类配置中（如图 2-6中显示），在密钥管理器服务器之间应仅对磁带机表格进行同步。（请参阅第 4-2 页的『同步两个密钥管理器服务器之间的数据』以获取更多信息。）确保指定 `sync.type = drivetab`（请不要指定 config 或 all）以防止配置文件被覆盖。

注: 无法部分共享服务器之间的配置。

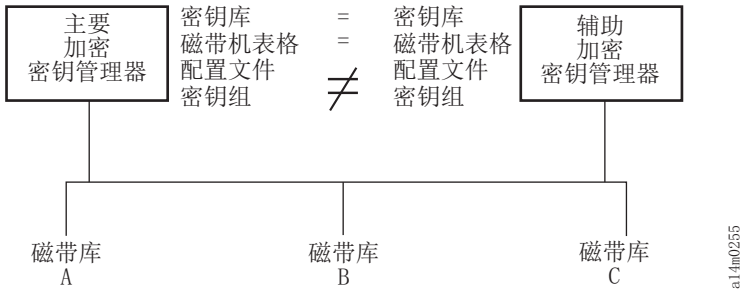

图 2-6. 两个配置不同的服务器访问相同的设备

灾难恢复站点注意事项

如果计划使用灾难恢复（DR）站点，那么加密密钥管理器将提供若干选项，以支持该站点读取和写入加密磁带。这些选项是:

- 在 DR 站点上创建一个重复的加密密钥管理器。

  在 DR 站点使用与您的本地加密密钥管理器相同的信息来设置一个重复的加密密钥管理器（配置文件、磁带机表格、密钥组 XML 文件和密钥库）。那么，此密钥管理器将正常工作，并且能够接管其中一个现有的生产密钥管理器来读取和写入加密磁带。
- 创建三个加密密钥管理器数据文件的备份副本，以便能够按需恢复。

  如果创建加密密钥管理器需要的四个数据元素的当前副本（配置文件、磁带机表格、密钥组 XML 文件，和密钥库），那么您将能够在 DR 站点随时启动密钥管理器，以充当一个重复实体。（请记住不应使用加密密钥管理器来对这些文件的副本进

行加密，因为如果没有密钥管理器就无法对其解密。）如果 DR 站点从您的主站点使用不同的磁带机，那么配置文件和磁带机表格必须包含 DR 站点的正确信息。

异地共享加密磁带的注意事项

注: 对于通过检查此类证书的信任链从业务合作伙伴获取的任何证书到最终签署某个证书的认证中心（CA），验证这些证书的有效性非常重要。如果信任 CA，那么您可以信任该证书。或者，如果某个证书在转换过程中受到安全保护，那么您可以验证该证书的有效性。未使用其中一个方法验证某个证书的有效性可能导致『中间人』攻击。

共享 LTO 4 和 LTO 5 磁带

为了在 LTO 4 或 LTO 5 磁带上共享加密数据，在磁带上用来加密数据的对称密钥的副本必须用于其他组织以使它们能够读取磁带。为共享对称密钥，其他组织必须与您共享它们的公用密钥。使用 keytool 从加密密钥管理器密钥库中导出该公用密钥时，它将用来打包对称密钥（请参阅第 3-12 页的『使用 Keytool -exportseckey 导出数据密钥』）。当其他组织将对称密钥导入到它们的加密密钥管理器密钥库时，将使用相应的专用密钥对它进行解包（请参阅第 3-11 页的『使用 Keytool -importseckey 导入数据密钥』）。这确保对称密钥在转换中是安全的，因为只有专用密钥的持有者才能够解包对称密钥。如果通过在加密密钥管理器密钥库中用来加密数据的对称密钥，其他组织将能够在磁带上读取数据。

联邦信息处理标准 140-2 注意事项

联邦信息处理标准 140-2 非常重要，因为联邦政府要求它的所有加密提供程序获取 FIPS 140 认证。此标准还用于日益私人化的扇区团体。在这个安全意识日渐重要的世界中，由第三方依据政府标准执行的加密功能的认证具有更大的价值。

加密密钥管理器自身不提供加密功能，因而它不需要也不允许获取 FIPS 140-2 认证。但是，加密密钥管理器利用 IBM Java 加密扩展组件中 IBM JVM 的加密功能优势，允许选择和使用具有 FIPS 140-2 第 1 级别认证的 IBMJCEFIPS 加密提供程序。通过将配置属性文件中的 **fips** 配置参数设置为 **on**，您可以使加密密钥管理器为所有加密功能使用 IBMJCEFIPS 提供程序。

请参阅特定硬件和软件加密提供程序的文档，以了解有关其产品是否获取 FIPS 140-2 认证的信息。

第 3 章 安装加密密钥管理器和密钥库

加密密钥管理器随附 IBM Java 虚拟机一起销售，并需要 IBM Software Developer Kit for Linux 和 IBM Runtime Environment for Windows（请参阅第 2-2 页的『硬件和软件需求』）。请遵循适合于您的操作系统的步骤:

- 『在 Linux 上安装加密密钥管理器』
- 第 3-2 页的『在 Windows 上安装加密密钥管理器』

如果您不确定是否已安装了最新版本的加密密钥管理器，『下载最新版密钥管理器 ISO 映像』说明了如何了解较新版本是否可用。最好获得您的 Java 安装版中可能没有的最新版加密密钥管理器。 更多信息请访问 **http://support.dell.com**。

重要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。

下载最新版密钥管理器 ISO 映像

要下载最新版的 Dell ISO 映像，请访问 http://support.dell.com。

在 Linux 上安装加密密钥管理器

通过 CD 在 Linux 上安装加密密钥管理器

1. 插入 Dell 加密密钥管理器 CD 并通过 CD 的根目录输入 `Install_Linux`。

   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。

   安装完成后将启动图形用户界面（GUI）。

在 Linux 上手动安装 Software Developer Kit

如果您不想通过 CD 安装，请执行以下步骤。

1. 根据您的操作系统，从 **http://support.dell.com**下载针对 Java 的适当 运行时环境:
   - Java 6 SR 5（32 位）或更高版本
   - Java 6 SR 5（64 位）或更高版本

2. 将 Java linux rpm 文件放置在工作目录中:

```
mordor:~ #/tape/Encryption/java/1.6.0# pwd
/tape/Encryption/java/1.6.0
mordor:~ #/tape/Encryption/java/1.6.0# ls
ibm-java-i386-jre-6.0-5.0.i386.rpm
```

3. 安装 rpm 软件包:

```
mordor:~ #rpm -ivh -nodeps ibm-java-i386-jre-6.0-5.0.i386.rpm
```

以下命令将把文件放置在 **/opt/ibm/java-i386-60/** 目录中:

```
mordor:~ #/opt/ibm/java-i386-60/jre # ls
.systemPrefs  bin  javaws  lib
```

4. 用 JAVA_HOME、CLASSPATH 以及您为 Java 安装的 bin 目录来编辑（或在需要时创建）文件 **/etc/profile.local**。添加以下 3 行:

```
JAVA_HOME=/opt/ibm/java-i386-60/jre
CLASSPATH=/opt/ibm/java-i386-60/jre/lib
PATH=$JAVA_HOME:opt/ibm/java-i386-60/jre/bin/:$PATH
```

5. 注销并重新登录主机，以使 **/etc/profile.local** 条目生效，或发出导出命令行命令:

```
mordor:~ # export JAVA_HOME=/opt/ibm/java-i386-60/jre
mordor:~ # export CLASSPATH=/opt/ibm/java-i386-60/jre/lib
mordor:~ # export PATH=/opt/ibm/java-i386-60/jre/bin/:$PATH
```

6. 重新登录后，发出 **java -version** 命令。您应该看到以下结果:

```
mordor:~ # java -version
java version "1.6.0"
Java(TM) SE Runtime Environment (build pmz60sr5-20090529(SR5))
IBM J9 VM (build 2.4, J2RE 1.6.0 IBM J9 2.4 Linux x86-32 jvmxi3260-20090519_35743 (JIT enabled)
...
mordor:~ # which java
/opt/ibm/java-i386-60/jre/bin/java
```

在 Windows 上安装加密密钥管理器

1. 插入 Dell 加密密钥管理器 CD。

   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。

   安装完成后将启动图形用户界面（GUI）。

2. InstallShield 向导打开时，单击 **Next**。
3. 阅读许可协议并单击 **Yes**。
4. Choose Destination Location 窗口打开时（第 3-3 页的图 3-1），请选择一个文件夹并记下该文件夹。您需要此 Java 路径才能启动加密密钥管理器。

图 3-1. Choose Destination Location 窗口

单击 **Next**。

5. 随之打开一个窗口，询问您是否要将该 Java 运行时环境用作缺省的系统 JVM（图 3-2）。

图 3-2. 将该版本的 JVM 设置为缺省

单击 **No**。

6. Start Copying Files 窗口随之打开（第 3-4 页的图 3-3）。确认您已记下目标路径。

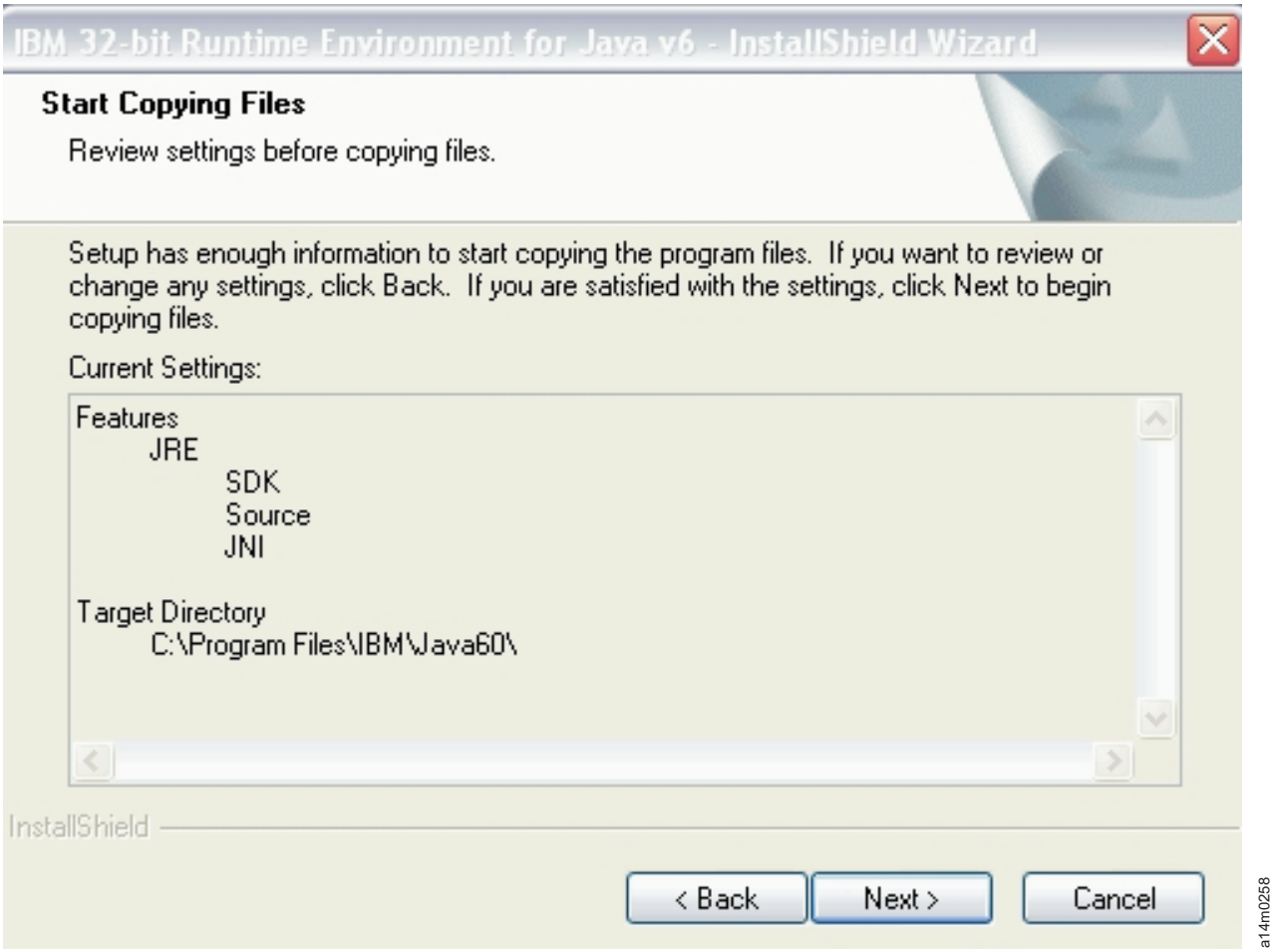

图 3-3. Start Copying Files 窗口

单击 **Next**。

7. 该状态窗口指示安装进度。
8. Browser Registration 窗口打开。选择用于加密密钥管理器的浏览器。单击 **Next**。
9. InstallShield 向导已完成窗口打开时，单击 **Finish**。

   安装后，您可以打开一个命令提示符窗口，以查询已安装 Java 的版本:

```
C:\WinEKM>C:\"Program Files"\IBM\Java60\jre\bin\java -version
java version "1.6.0"
Java(TM) SE Runtime Environment (build pwi3260sr5-20090529_04(SR5))
IBM J9 VM (build 2.4, J2RE 1.6.0 IBM J9 2.4 Windows Server 2003 x86-32 j9vmwi3223-20090
519_35743 (JIT enabled, AOT enabled)
...
```

10. 如下所示更新 PATH 变量: （对于 加密密钥管理器 2.1，是必需的；但是对于 05032007 及更早的构建日期来说是可选的。）

    如果想通过命令窗口调用 Java SDK 时，那么您可能想设置 PATH 变量，以便能够通过任何目录运行 Java JRE 可执行文件 (java.exe)，而无需输入完整的命令路径。如果您不设置 PATH 变量，那么必须在每次运行可执行文件是指定可执行文件的完整路径，比如:

```
C:>\Program Files\IBM\Java60\jre\bin\java ...
```

要永久地设置 PATH（对于加密密钥管理器 2.1，是必需的），请向 PATH 变量添加 java bin 目录的完整路径。通常该完整路径类似于

```
C:\Program Files\IBM\Java60\jre\bin
```

要在 Microsoft Windows 2003、2008 和 2008 R2 中永久设置 PATH:

注: 无法从命令行设置 PATH 变量。

a. 从“开始”菜单中选择**设置**，然后选择**控制面板**。
b. 双击**系统**。
c. 单击**高级**选项卡。
d. 单击**环境变量**。
e. 将系统变量列表向下滚动至 Path 变量，然后单击**编辑**。
f. 将 IBM JVM 路径添加到 Path 变量的开头。

   缺省安装目录为 C:\PROGRA~1\IBM\Java60\jre\bin。

   特别注意: 在路径结尾部分插入一个分号，将其与路径列表中的其他目录隔开。
g. 单击**确定**。

使用 GUI 来创建配置文件、密钥库以及证书

在启动加密密钥管理器之前，必须至少创建一个新密钥库和一份自签名证书。您可以使用 Dell 加密密钥管理器服务器图形用户界面（GUI）来创建加密密钥管理器配置属性文件、密钥库、证书和密钥。作为此进程的结果，还创建了一个简单的 CLI 配置属性文件。

1. 打开 GUI（如果它并未启动）:

   Windows 上

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

   Linux 平台上

   浏览至 /var/ekm/gui 并输入 `. ./LaunchEKMGui.sh`
2. 在 GUI 左边的导航器中选择 **EKM Configuration**。
3. 在“EKM Server Configuration”页面（第 3-6 页的图 3-4）上的所有必填字段（以星号 * 标记）中输入数据。为方便起见，某些字段已填好。单击任何数据字段右侧的问号标记以获取描述。单击 **Next**。

   注: 一旦您设定密钥库密码后，除非其安全性被破坏，否则 **不要更改**该密码。将模糊密码以降低任何安全性暴露。更改密钥库密码需要使用 **keytool** 命令单独更改密钥库中的所有密码。请参阅第 3-11 页的『更改密钥库密码（Changing Keystore Passwords）』。

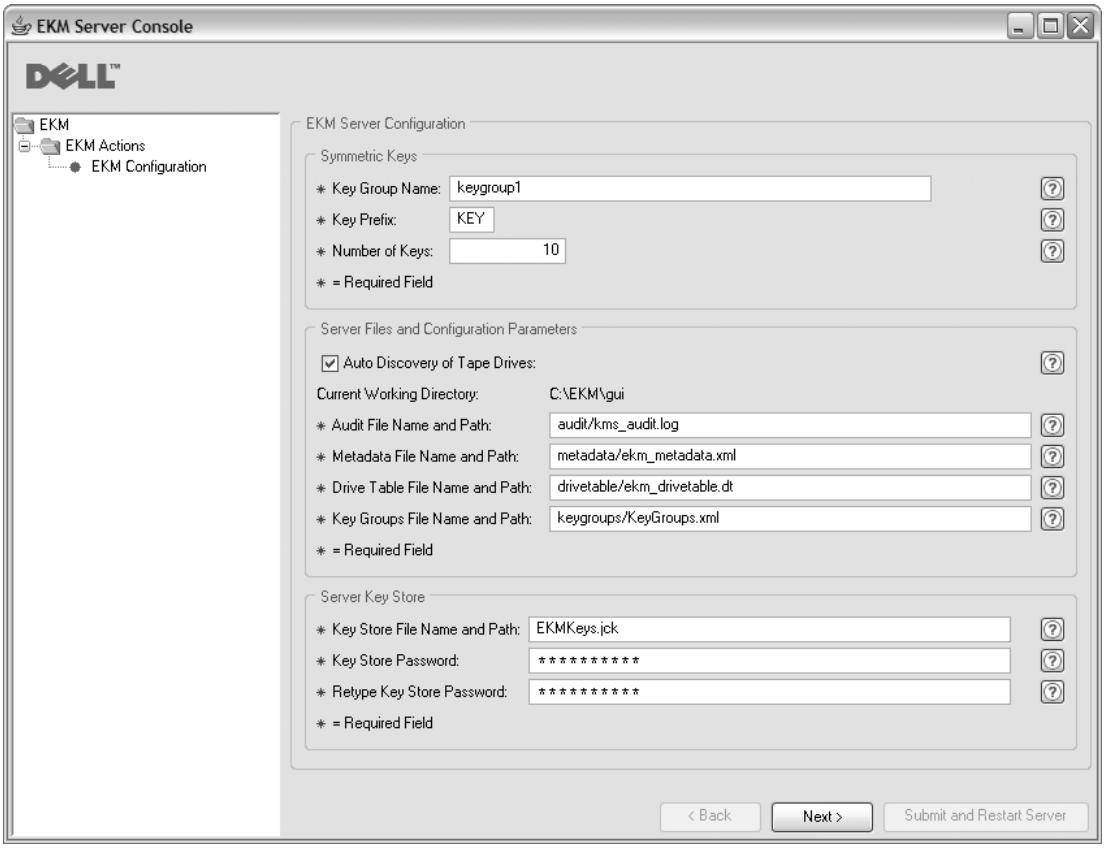

图 3-4. EKM Server Configuration 页面

尽管可以为 Dell 加密密钥管理器密钥库生成的密钥数没有限制，但是生成密钥的时间仍然会增加，具体取决于请求的密钥数量。加密密钥管理器生成 10 个密钥需要 15 秒钟，生成 10000 个密钥则需要 30 分钟以上的时间。请注意，密钥数受到主机服务器资源（服务器中的内存）的限制。加密密钥管理器应用程序运行时在系统内存中维护密钥库列表，以便能够在库从磁带机发送密钥请求时快速访问这些密钥。

注: 如果密钥生成过程中加密密钥管理器 GUI 被中断，那么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加密密钥管理器安装时被中断，请浏览到加密密钥管理器目录所在的目录（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. 在“EKM Server Certificate Configuration”页面（第 3-7 页的图 3-5）上，输入密钥库别名及其他要输入的数据。单击 **Submit and Restart Server**。

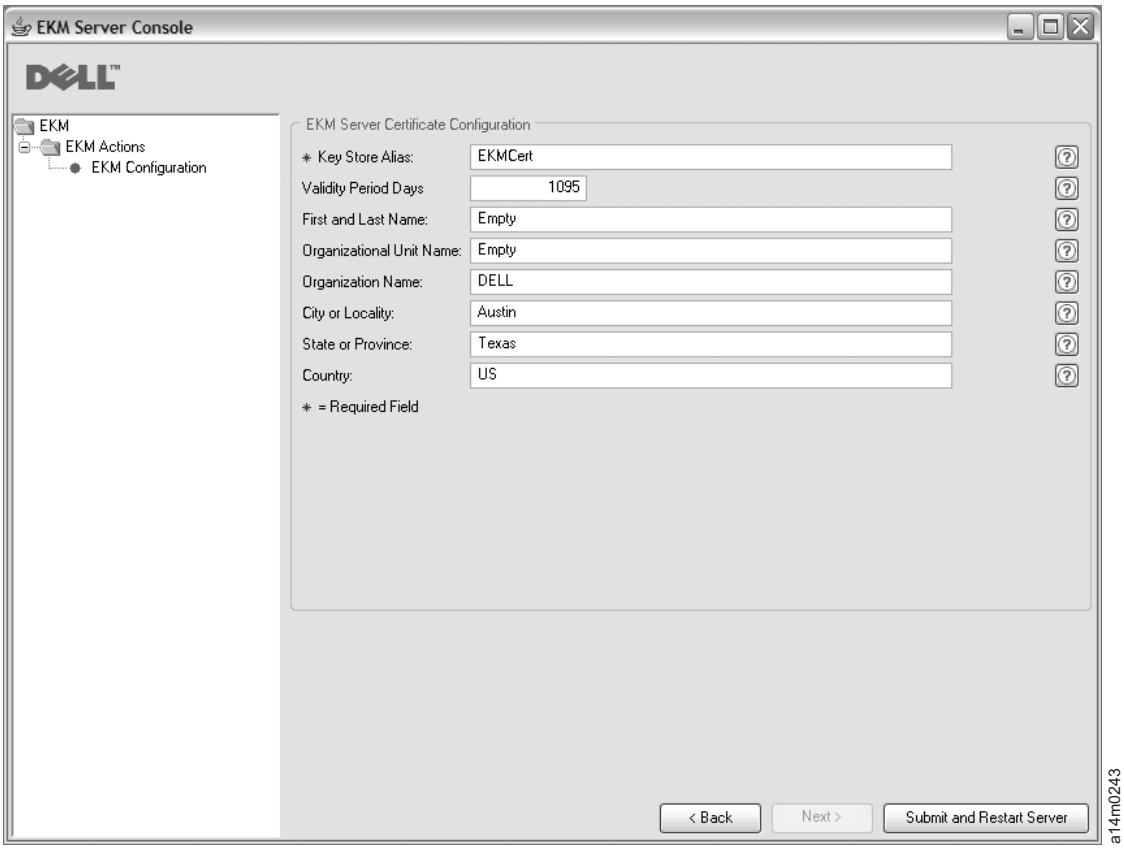

图 3-5. EKM Server Certificate Configuration 页面

5. 将打开一个『Backup Critical Files』窗口（图 3-6），提醒您备份加密密钥管理器数据文件。

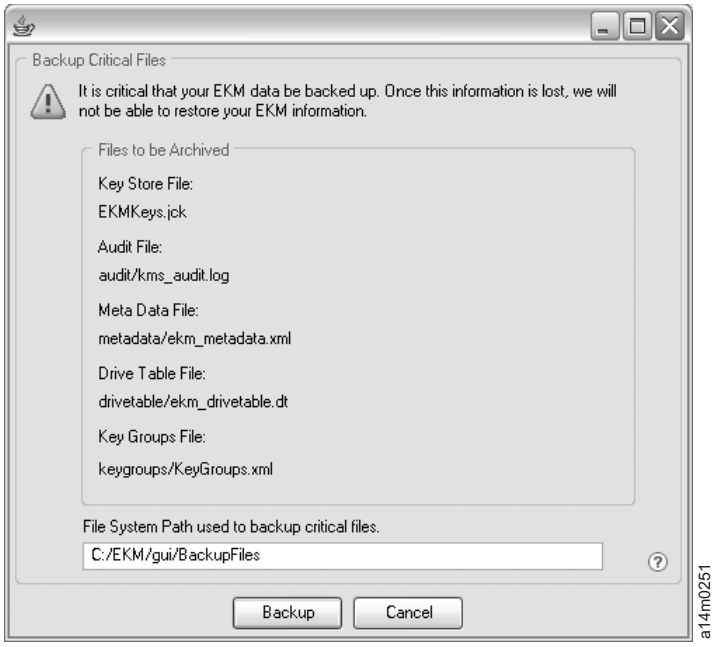

图 3-6. Backup Critical Files 窗口

验证路径并单击 **Backup**。Dell 加密密钥管理器服务器在后台启动。

只要更改加密密钥管理器服务器配置时单击了**确定**，或在 『Backup Critical Files』窗口中单击了 **Backup**，加密密钥管理器就将生成一组备份文件。作为*要归档的文件*列出的文件将保存到 c:/ekm/gui/BackupFlies 目录中。每个文件名都附加了日期和时间。例如，一组在 2007 年 11 月 26 日下午 2 点 58 分 46 秒备份的一组文件在其名称的开始部分将具有以下日期与时间戳记：“2007_11_26_14_58_46_FileName”。备份文件将不会被覆盖。

6. 在 GUI 导航器中选择**服务器运行状况监视器**以验证加密密钥管理器服务器是否已经启动。

要将密钥添加到现有密钥库中，请参阅第 3-13 页的『使用 GUI 定义密钥组并创建密钥』。

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。

1. 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

1. 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`
   - 关于更多信息，请参阅第 5-1 页的『启动、刷新和关闭密钥管理器服务器』。
2. 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`
   - 关于更多信息，请参阅第 5-5 页的『命令行界面客户机』。
3. 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。）

   登录成功后将显示 `User successfully logged in`。
4. 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。

5. 从命令行注销。输入以下命令:

   ```
   exit
   ```

   关闭命令窗口。

在 LTO 4 和 LTO 5上生成加密密钥和别名

Dell 加密密钥管理器Server GUI 是生成对称加密密钥的最简单方法（请参阅第 3-5 页的『使用 GUI 来创建配置文件、密钥库以及证书』）。您也可以使用 Keytool 实用程序来生成对称加密密钥。Keytool 对于在不同密钥之间导入和导出密钥特别有用。详细信息请参阅第 3-11 页的『使用 Keytool -importseckey 导入数据密钥』和第 3-12 页的『使用 Keytool -exportseckey 导出数据密钥』。

Keytool 是用于管理密钥、证书和别名的实用程序。 它用于生成、导入和导出加密数据密钥并将密钥保存在密钥库中。

密钥库中的每个数据密钥都可以通过一个唯一别名进行访问。别名是一个字符串，比如 `123456tape`。在 JCEKS 密钥库中，`123456Tape` 相当于 `123456tape`，并允许访问密钥库中的同一个条目。使用 **keytool -genseckey** 命令来生成数据密钥时，您应在同一命令中指定相应的别名。别名使您能够在正确的密钥组和密钥库中识别正确的密钥，以用于读写 LTO 4 和 LTO 5 磁带上的加密数据。

注: 各个别名和别名范围必须具有唯一性。该唯一性在密钥于给定密钥库/加密密钥管理器实例上生成时强制实现。但是，在多个加密密钥管理器/密钥库环境中，您应该使用一个命名约定，该约定在需要在实例之间传输密钥并同时维持引用的唯一性时保持多个实例的唯一性。

生成密钥和别名后，更新 KeyManagerConfig.properties 文件中的 symmetricKeySet 属性，以指定新的别名、别名范围、密钥组的 GroupID、存储对称密钥的文件的名称以及定义密钥组的文件的名称。（详细信息请参阅第 3-13 页的『密钥组的创建与管理』。）只有 symmetricKeySet 中的指定密钥才会被验证（检查一个已存在别名和一个对称密钥的大小和算法是否恰当）。如果该属性中指定了无效密钥，密钥管理器将无法启动，并创建一条审计记录。

Keytool 实用程序也可以用于将数据密钥导出到其他密钥库或从其他密钥库导入数据密钥。之后将概述每个任务。您可以发出 **keytool -ekmhelp** 命令，以显示所有以下讨论中与密钥管理器相关的参数。

编辑配置属性文件

要对 KeyManagerConfig.properties 或 ClientKeyManagerConfig.properties 文件进行更改:

1. 关闭加密密钥管理器服务器。
2. 使用所选文本编辑器打开 KeyManagerConfig.properties 文件对服务器配置进行更改，或打开 ClientKeyManagerConfig.properties 文件对客户机配置进行更改。对于 Linux 机器，不要因为 ^M 而用 Windows 来编辑文件。如果使用 Windows，请使用 gvim/vim 编辑文件。
3. 根据此文档中提供的指示更改这些属性值。
4. 保存文件。

5. 重新启动加密密钥管理器服务器。

如果不使用 Keytool

如果不使用 keytool 或 GUI 来生成密钥和别名，那么无法生成与加密密钥管理器相兼容的密钥范围。要生成与加密密钥管理器相兼容的单独密钥，就要确保使用以下格式之一指定别名:

- 12 个可打印字符或更少（如 abcdefghijk）
- 3 个可打印字符，后跟两个 0，接着是 16 位十六进制数（如 ABC000000000000000001），总共正好为 21 个字符

使用 Keytool -genseckey 生成数据密钥和别名

注: 在任何会话中首次使用 **keytool** 命令之前，请运行 updatePath 脚本，以设置正确的环境。

Windows 上

浏览至 cd c:\ekm 并单击 **updatePath.bat**

Linux 平台上

浏览至 /var/ekm 并输入 **. ./updatePath.sh**

Keytool 实用程序在使用 LTO 4 和 LTO 5 磁带的 LTO 4 和 LTO 5 磁带机上生成用于加密的别名和对称密钥。使用 **keytool -genseckey** 命令来生成一个或多个密钥并将它们存储在指定密钥库中。**keytool -genseckey** 使用以下参数:

```
-genseckey      [-v] [-protected]
                  [-alias <alias> | aliasrange <aliasRange>] [-keypass <keypass>]
                  [-keyalg <keyalg>] [-keysize <keysize>]
                  [-keystore <keystore>] [-storepass <storepass>]
                  [-storetype <storetype>] [-providerName <name>]
                  [-providerClass <provider_class_name> [-providerArg <arg>] ...
                  [-providerPath <pathlist>]
```

这些参数特别重要，它们用于生成加密密钥管理器的数据密钥，以便在 LTO 4 和 LTO 5 磁带机上进行磁带加密:

-alias

为单个数据密钥指定最多可以有 12 个可打印字符的 *alias* 值（例如 abcfrg 或 key123tape）。

-aliasrange

生成多个数据密钥时，*aliasrange* 被指定为一个 3 个字符的字母前缀，其后跟着一串 16 个字符（十六进制），字符串开头被自动填充以零，以构成长度为 21 个字符的别名。例如，指定 key1-a 将获得一系列从 KEY000000000000000001 到 KEY00000000000000000A 的别名。指定 xyz01-FF 的 *aliasrange* 值将获得 XYZ000000000000000001 到 XYZ0000000000000000FF，该值将生成 255 个对称密钥。

-keypass

指定用于保护数据密钥的密码。该密码**必须完全相同于**密钥库密码。如果未指定任何密码，您将获得指定密钥的提示。如果您在获得提示时按 **Enter**，密钥密钥经被设定为与密钥库使用的相同的密码。*keypass* 长度必须至少为 6 个字符。

注: 一旦您设定密钥库密码后，除非其安全性被破坏，否则 **不要更改**该密码。请参阅『更改密钥库密码（Changing Keystore Passwords）』。

-keyalg

指定用于生成数据密钥的算法。该值必须指定为 AES。

-keysize

指定要生成数据密钥的大小。 密钥大小必须指定为 256。

可以与对称密钥关联的可接受别名示例:

```
abc000000000000000001
abc00a0120fa000000001
```

不会被密钥管理器接受的别名示例:

```
abcefghij1234567 ? wrong lengthabcg0000000000000001 ? prefix is longer than 3 characters
```

如果密钥库中已存在一个别名，Keytool 将抛出一个异常并停止运行。

更改密钥库密码（Changing Keystore Passwords）

注: 一旦您设定密钥库密码后，除非其安全性被破坏，否则 **不要更改**该密码。将模糊密码以降低任何安全性暴露。更改密钥库密码需要通过使用下面的 **keytool** 命令分别更改该密钥库中每一个密钥上的密码。

要更改密钥库密码，请输入:

```
keytool -keypasswd  -keypass old_passwd -new new_passwd -alias alias
        -keystore keystorename -storetype keystoretype
```

您还必须编辑 KeyManagerConfig.properties，以更改每个服务器配置文件属性中的密钥库密钥，该密钥在前述属性中用以下方法指定:

- 删除整个模糊化密码并允许加密密钥管理器在下次启动时发出提示。
- 删除整个模糊密码并键入明文新秘密。该密码将在下次启动时被模糊化。

使用 Keytool -importseckey 导入数据密钥

使用 Keytool -importseckey 命令来从导入文件导入一个或一批密钥。**keytool -importseckey** 使用以下参数:

```
-importseckey          [-v]
                  [-keyalias <keyalias>] [-keypass <keypass>]
                  [-keystore <keystore>] [-storepass <storepass>]
                  [-storetype <storetype>] [-providerName <name>]
                  [-importfile <importfile>] [-providerClass <provider_class_name>]
                  [providerArg <arg>]
```

这些参数特别重要，它们用于导入加密密钥管理器的数据密钥，以便在 LTO 4 和 LTO 5 磁带机上进行磁带加密:

-keyalias

指定密钥库中密钥的别名，以便对 *importfile* 中的所有数据密钥进行解密。

-importfile

指定含有待导入数据密钥的文件。

使用 Keytool -exportseckey 导出数据密钥

使用 Keytool -exportseckey 命令，将一个或一批密钥导出到导出文件中。**keytool -exportseckey** 使用以下参数:

```
-exportseckey        [-v]
                     [-alias <alias> | aliasrange <aliasRange>] [-keyalias <keyalias>]
                     [-keystore <keystore>] [-storepass <storepass>]
                     [-storetype <storetype>] [-providerName <name>]
                     [-exportfile <exportfile>] [-providerClass <provider_class_name>]
                     [providerArg <arg>]
```

这些参数特别重要，它们用于导出加密密钥管理器的数据密钥，以便在 LTO 4 和 LTO 5 磁带机上进行磁带加密:

-alias

为单个数据密钥指定最多可以有 12 个可打印字符的 *alias* 值（例如 `abcfrg` 或 `key123tape`）。

-aliasrange

导出多个数据密钥时，*aliasrange* 被指定为一个 3 个字符的字母前缀，其后跟着一串 16 个字符（十六进制），字符串开头被自动填充以零，以构成长度为 21 个字符的别名。例如，指定 `key1-a` 将获得一系列从 `KEY000000000000000001` 到 `KEY00000000000000000A` 的别名。指定 `xyz01-FF` 的 *aliasrange* 值将获得 `XYZ000000000000000001` 到 `XYZ0000000000000000FF`

-exportfile

指定数据密钥被导出时存储这些密钥的文件。

-keyalias

指定密钥库中公用密钥的别名，以便对所有数据密钥进行解密。请确保 从其导入对称（数据）密钥的密钥库含有对应的专用密钥。

使用 JCEKS 密钥库进行 LTO 4 和 LTO 5 加密的别名和对称密钥设置样本

通过 `-aliasrange` 选项调用 **KeyTool**。

注意: 密钥算法（-keyalg）必须按以下方式被指定为 AES，并且密钥大小（-keysize）必须被指定为 256:

```
/bin/keytool –genseckey –v –aliasrange AES01-FF –keyalg AES –keysize 256
–keypass password -storetype jceks –keystore path/filename.jceks
```

这些 KeyTool 调用将生成在 AES000000000000000001 到 AES0000000000000000FF 的范围内的 255 个有顺序的别名和关联的 AES 256 位对称密钥。别名和密钥都可以按需要累加重复多次，以设置有效密钥管理器操作所需要的完整数量的范围和单独密钥别名。例如，要为 LTO 4 和 LTO 5 生成一个额外的别名和对称密钥:

```
/bin/keytool –genseckey –v –alias abcfrg –keyalg AES –keysize 256
–keypass password -storetype jceks –keystore path/filename.jceks
```

该调用将单独别名 `abcfrg` 累加式地添加到指定的密钥库，该密钥库已含有上述 调用所生成的 255 个别名，从而在 –keystore 选项中指定的 jceks 文件中生成 256 位对称密钥。

更新 KeyManagerConfig.properties 文件中的 symmetricKeySet 属性，添加以下行，以便与以上使用的任何和所有别名范围以及存储对称密钥文件的名称相匹配。注意：如果指定的别名无效，加密密钥管理器可能无法启动。验证失败的其他原因可能包括不正确的位大小（AES keysize 必须为 256）或无效的平台算法。-keyalg 必须为 AES，且 -keysize 必须为 256。**config.keystore.file** 中指定的文件名应该与 KeyTool 调用中 –keystore <filename> 指定的名称相匹配:

symmetricKeySet = AES01-FF,abcfrg
config.keystore.file = <filename>.jceks

只有 symmetricKeySet 中的指定密钥才会被验证（检查一个已存在别名和一个对称密钥的大小和算法是否恰当）。如果在该属性中指定了无效的密钥，加密密钥管理器将无法启动并创建一条审计记录。

密钥组的创建与管理

加密密钥管理器允许您组织 LTO 4 和 LTO 5 的对称密钥并将其加密为密钥组。使用此方法，您可以根据加密数据的类型、访问加密数据的用户或任何其他有意义的特性来组织密钥。一旦创建了密钥组，您可以使用 **adddrive** 命令中的 -symrec 关键字使其与特定磁带机相关联。请参阅第 5-7 页的『adddrive』获取语法信息。

要构建密钥组，必须在 KeyGroups.xml 文件中对其进行定义。如果您遵照的是第 3-5 页的『使用 GUI 来创建配置文件、密钥库以及证书』中的过程，那么此文件的位置就被指定在 EKM 配置页上。If 如果您是手动创建配置文件，KeyGroups.xml 文件的位置就被指定在如下所示的配置属性文件中:

```
config.keygroup.xml.file = FILE:KeyGroups.xml
```

如果未指定此参数，那么将缺省使用加密密钥管理器启动位置的工作目录下的 KeyGroups.xml 文件。如果此文件不存在，那么将创建一个空 KeyGroups.xml 文件。下一次启动加密密钥管理器服务器时，**native_stderr.log** 中可能显示以下消息: `[Fatal Error] :-1:-1: Premature end of file`。这是解析这个空 KeyGroups.xml 文件时产生的错误，不会妨碍加密密钥管理器服务器的启动，除非加密密钥管理器已被配置为使用密钥组。

密钥组是使用 Dell 加密密钥管理器服务器 GUI 或以下的 CLI 客户机命令来构建的（请参阅第 5-7 页的『CLI 命令』获取语法信息）:

使用 GUI 定义密钥组并创建密钥

您可以使用 GUI 来执行管理密钥组所需的全部任务您也可以使用 GUI 来创建其他密钥。

注: 执行以下任何任务过程中单击 **Submit Changes** 时，将会打开一个备份对话窗口（第 3-7 页的图 3-6），提醒您备份加密密钥管理器数据文件。输入保存备份数据位置的路径。单击 **Submit**。然后验证备份路径并单击 **OK**。

创建密钥组并用密钥对其进行填充、或向现有密钥组添加密钥:

1. 打开 GUI（如果它并未启动）:

   Windows 上

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

Linux 平台上

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

2. 在 GUI 左边的导航器中选择 **Administration Commands**。
3. 单击窗口底部的 **Create a Group of Keys** （图 3-7）。

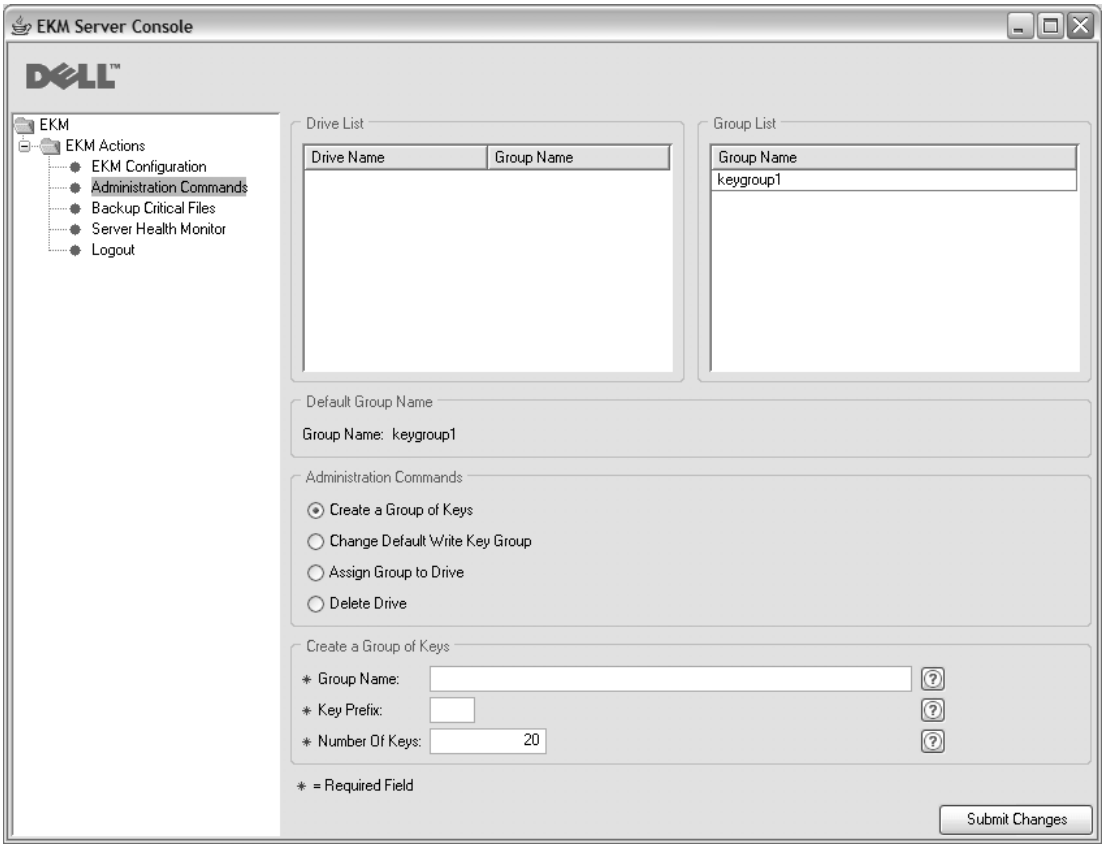

图 3-7. 创建密钥组

4. 输入新密钥组的名称、用于密钥别名的前缀以及组要包含的关键字数目。单击 **Submit Changes**。

更改缺省密钥组:

1. 在 GUI 左边的导航器中选择 **Administration Commands**。
2. 单击窗口底部的 **Change Default Write Key Group**（第 3-15 页的图 3-8）。

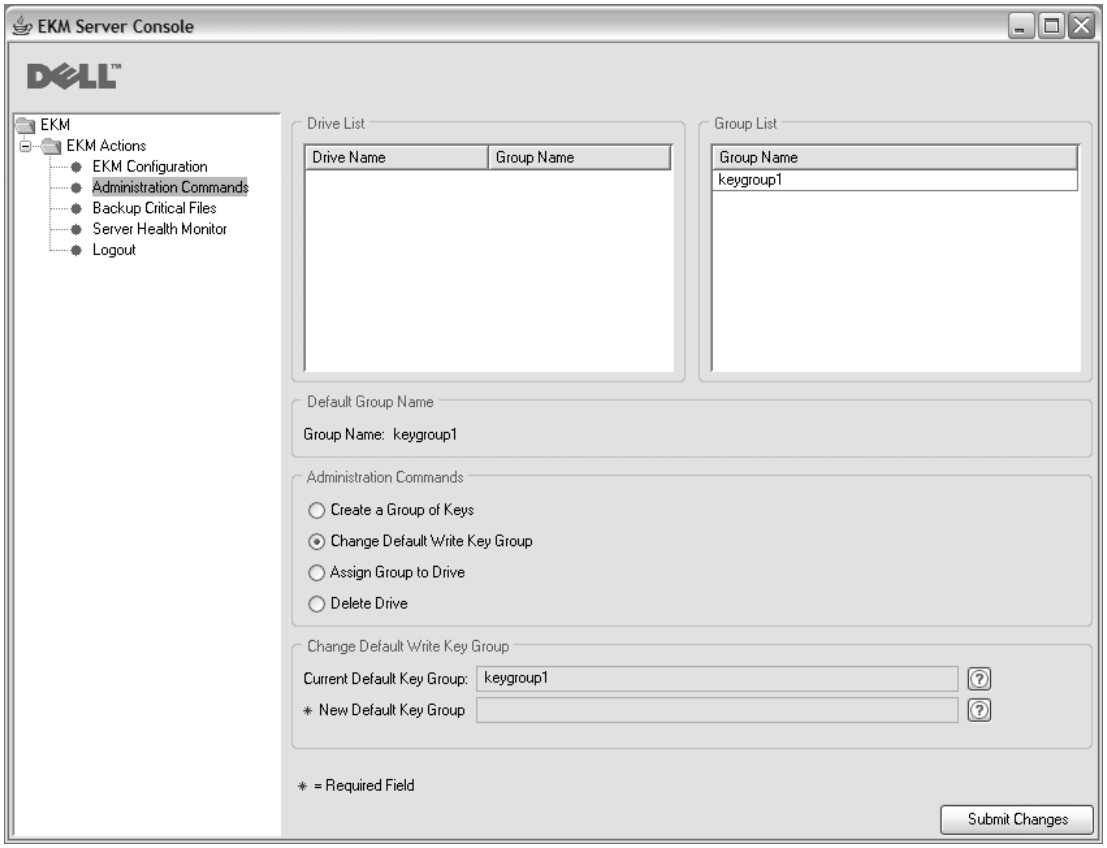

图 3-8. 更改缺省写密钥组

3. 从右侧的组列表中选择新的缺省密钥组。
4. 验证窗口底部的当前密钥组和新的缺省密钥组，并单击 **Submit Changes**。

将特定密钥组指定给特定的磁带机:

1. 在 GUI 左边的导航器中选择 **Administration Commands**。
2. 单击窗口底部的 **Assign Group to Drive**（第 3-16 页的图 3-9）。

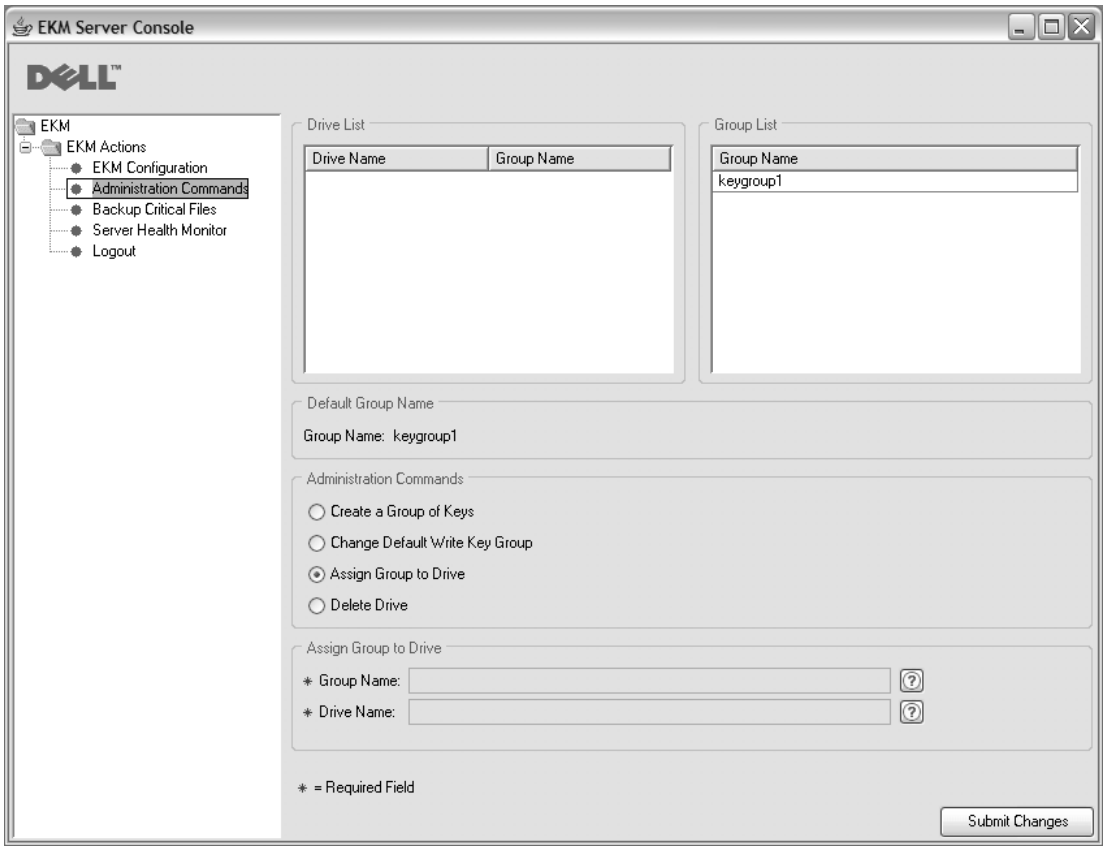

图 3-9. 将组指定给磁带机

3. 从磁带机列表中选择磁带机。
4. 从组列表中选择密钥组。
5. 验证窗口底部的磁带机和密钥组并单击 **Submit Changes**。

从磁带机表格中删除磁带机:

1. 在 GUI 左边的导航器中选择 **Administration Commands**。
2. 单击窗口底部的窗口 **Delete Drive**（第 3-17 页的图 3-10）。

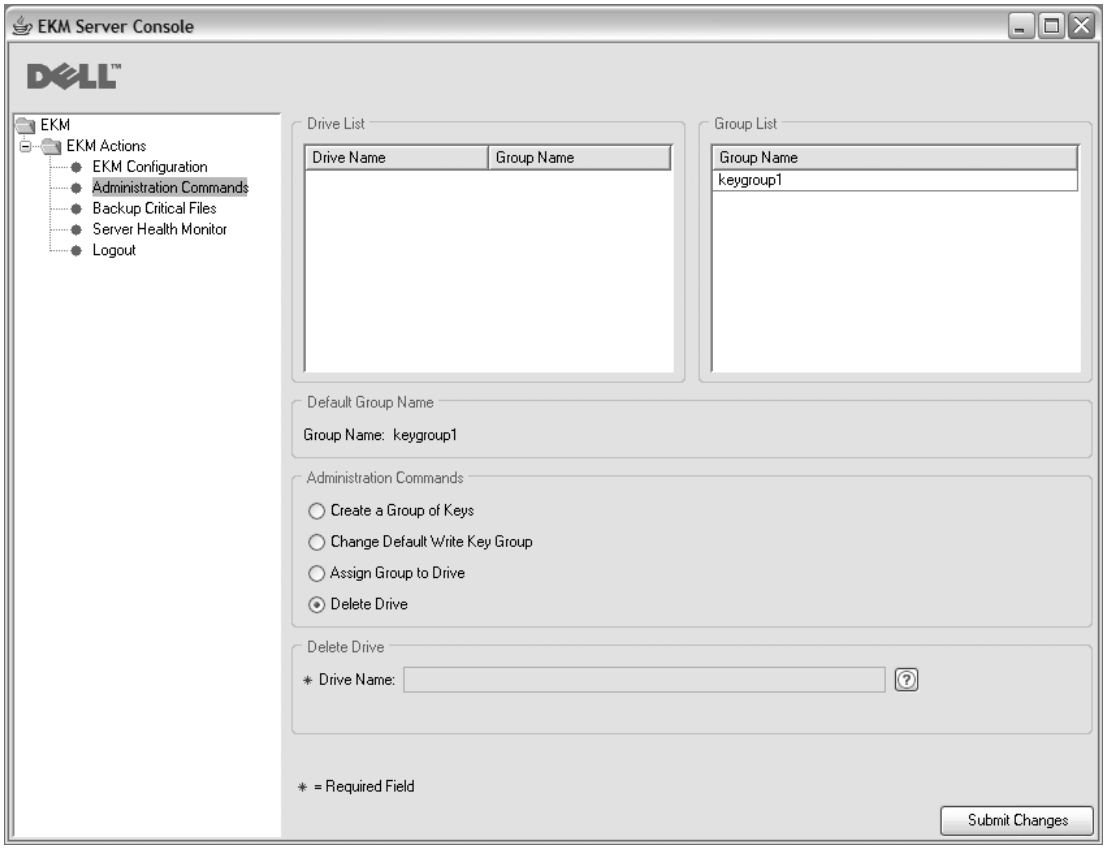

图 3-10. 删除磁带机

3. 从磁带机列表中选择磁带机。
4. 验证窗口底部的磁带机名称并单击 **Submit Changes**。

使用 CLI 命令定义密钥组

加密密钥管理器拥有的密钥组功能使您能够组织密钥组。

一旦安装并配置了加密密钥管理器应用程序（密钥库和密钥已生成）且加密密钥管理器服务器已经启动，那么请使用客户机登录该服务器，并执行以下步骤:

1. 运行 **createkeygroup** 命令。

   此命令可在 KeyGroups.xml 文件中创建初始密钥组对象。仅运行一次此命令。

   语法: **createkeygroup -password** *password*

   -password
   用于加密 KeyGroups.xml 文件中的密钥库密码的*密码*，以备将来的恢复操作。密钥库加密密钥组的密钥，而密钥组的密钥依次加密各个单独密钥组别名密码。因而 KeyGroups.xml 文件中的密钥全都是不清晰的。

   示例: createkeygroup -password a75xynrd
2. 运行 **addkeygroup** 命令。

   此命令在 KeyGroups.xml 中创建具有唯一组标识的密钥组实例。

语法: **addkeygroup -groupID** *groupname*

-groupID
用于识别 KeyGroups.xml 文件中的组的唯一*组名*。

示例: addkeygroup -groupID keygroup1

3. 运行 **addkeygroupalias** 命令。

此命令为密钥库中现有的密钥别名创建新的别名，用于添加到特定密钥组标识。

语法: **addkeygroupalias -alias** *aliasname* **-groupID** *groupname*

-alias
密钥的新*别名*。此名称必须是完全的键名，即，Key00 必须依照 key000000000000000000 输入。

-groupID
用于识别 KeyGroups.xml 文件中的组的唯一*组名*。

示例: addkeygroupalias -alias key000000000000000000 -groupID keygroup1

注: 在使用此 CLI 命令时，您可以一次只添加一个密钥。对于每个需要添加到密钥组的单独密钥，必须运行此命令。

4. 将密钥组与新的或现有的磁带机相关联。
   a. 运行 **moddrive** 命令使密钥组与现有磁带机相关联。

此命令可修改磁带机表格中的磁带机信息。

语法: **moddrive -drivename** *drivename* **-symrec** *alias*

-drivename
drivename 指定磁带机的序列号。

-symrec
指定对称密钥的*别名*或磁带机的密钥组名。

示例: moddrive -drivename 000123456789 -symrec keygroup1

   b. 运行 **adddrive** 命令向磁带机表格添加磁带机并使其与密钥组相关联。

此命令使您能够添加磁带机并使其与特定的密钥组相关联。

语法: **adddrive -drivename** *drivename* **-symrec** *alias*

-drivename
drivename 指定要添加的磁带机的 12 位序列号。

注: 必须在 10 位序列号前加两个 0，以达到 12 位。

-symrec
指定对称密钥的*别名*或磁带机的组标识。。

示例: adddrive -drivename 000123456789 -symrec keygroup1

当没有为磁带机定义别名时，要为缺省使用指定一个密钥组，请将配置属性文件的 symmetrickeySet 属性设置为您希望使用的密钥组的组标识。例如,

```
symmetricKeySet = keygroup1
```

组标识必须与 KeyGroups.xml 文件中的现有密钥组标识相匹配。如果不匹配，那么加密密钥管理器服务器将不启动。加密密钥管理器会在密钥组中跟踪密钥用途。当您指定了有效的组标识，加密密钥管理器会记录最后使用的密钥，然后在指定的密钥组中选择任意一个密钥。

将密钥从一个密钥组复制到另一个密钥组

运行 **addaliastogroup** 命令。

此命令将现有（源）密钥组中的特定别名复制到新的（目标）密钥组。

语法：**addaliastogroup -aliasID** *aliasname* **-sourceGroupID** *groupname* **-targetGroupID** *groupname*

-aliasID
要添加的密钥的*别名*。

-sourceGroupID
用于识别别名要复制到的目标组的唯一*组名*。

-targetGroupID
用于识别别名要添加到的目标组的唯一*组名*。

示例：addaliastogroup -aliasID aliasname -sourceGroupID keygroup1 -targetGroupID keygroup2

注：密钥在两个密钥组中都是可用的。

第 4 章 配置加密密钥管理器

使用 GUI 来配置加密密钥管理器

创建配置属性文件最简单的方法就是使用 Dell 加密密钥管理器 GUI 遵照第 3-5 页的『使用 GUI 来创建配置文件、密钥库以及证书』中的过程进行操作。如果您执行了这些操作，那么您就已创建了配置文件并且不需要进行其他的配置。如果您想利用其他的加密密钥管理器配置选项，以下信息可能会有对您有所帮助。

配置策略

在 KeyManagerConfig.properties 文件中的某些配置设置提供了快捷方式，您应该对这些快捷方式的作用有一定的了解。

自动更新磁带机表

加密密钥管理器在配置文件中提供了一个变量（drive.acceptUnknownDrives），如果它已设置为值 `true`，那么将在新的磁带机与 Dell 加密密钥管理器 联系时自动填充磁带机表。此操作避免了为每个磁带机或库使用 **adddrive** 命令的需求。在此方式中，其中每个设备的 10 位 序列号都不需要使用 CLI 客户机命令来输入。 新的磁带机要进行标准公共/专用密钥密码术的交换以验证磁带设备的标识。一旦此验证完成，新设备就可以根据磁带上存储的 密钥标识来读现有磁带（假定在已配置的密钥库中找到了相应的密钥信息）。

注: 在自动添加磁带机后，应该使用 GUI 或命令第 5-12 页的『refresh』对加密密钥管理器服务器进行刷新，以确保它们已存储在磁带机表格中。

对于 LTO 4 和 LTO 5 磁带机，您可以设置缺省对称密钥池 (symmetricKeySet) 以对新添加的设备进行加密。换言之，当设备进行联系时，您可以使用相关密钥材料通过加密密钥管理器对设备进行完整配置。如果设备添加到磁带机表格上时您不选择这样操作，那么可以在磁带机已添加到磁带机表格中后，使用 **moddrive** 命令来执行此操作。

除了使管理员免于为加密密钥管理器将服务的各个磁带机输入 10 位序列号之外，它还允许在配置大系统时使用缺省环境。

应该注意这些便利所付出代价是降低了安全性。因为设备是自动添加的并且可以用证书别名进行关联（能用此证书别名对磁带进行写入），当跳过手动添加设备时，管理员会执行添加的安全检查您需要对此选项的优点和缺点进行估计，这点是十分重要的，以确定是否要自动添加磁带机信息到磁带机表格，并且绝对相信新设备访问证书信息是可接受的安全风险。

注: drive.acceptUnknownDrives 属性在缺省情况下设为 `false`。因而，加密密钥管理器不会将新磁带机自动添加到磁带机表格。选择您希望操作的方式并据此来更改配置。请参阅请参阅 B 获取详细信息。

同步两个密钥管理器服务器之间的数据

可以在两个加密密钥管理器服务器之间对磁带机表格和配置属性文件进行同步。您可以通过手动使用 CLI 客户机 **sync** 命令或自动设置 KeyManagerConfig.properties 文件中的四个属性来执行此操作。

注意

两个同步方法在密钥库或密钥组 XML 文件中均不能有效使用。您必须对它们进行手动复制。

只有在 KeyManagerConfig.properties 文件的 sync.ipaddress 属性中指定有效的 IP 地址，您才可以启用自动同步功能。请参阅『自动同步』。

手动同步

手动方法涉及执行 CLI 客户机 **sync** 命令。语法如下所示:

sync {**-all** | **-config** | **-drivetab**} **-ipaddr** *ip_addr* :*sslport* [**-merge** | **-rewrite**]

该命令将配置文件属性和/或磁带机表格信息从源（或发送）服务器发送到 **–ipaddr** 参数指定的目标（或接收）服务器。接收的加密密钥管理器服务器必须启动和运行。

所需字段

-all
将配置属性文件和磁带机表格信息同时发送到 **-ipaddr** 指定的服务器。

-config
仅将配置属性文件发送到 **-ipaddr** 指定的服务器。

-drivetab
仅将磁带机表格信息发送到 **-ipaddr** 指定的服务器。

-ipaddr
ip_addr:sslport 指定接收服务器的地址和 ssl 端口。*sslport* 应与接收服务器的 KeyManagerConfig.properties 文件中为『TransportListener.ssl.port』指定的值相匹配。

可选字段

-merge
使用接收服务器上的当前数据合并（添加）新的磁带机表格数据。（配置文件始终是一个重写文件。）这（重写）是缺省值。

-rewrite
使用新数据替换接收服务器上的当前数据。

自动同步

磁带机表格和属性文件可以从主密钥管理器自动发送到辅助服务器。必须运行辅助服务器以实现数据同步。要对数据从主服务器到辅助服务器进行同步，您必须指定主服务器 KeyManagerConfig.properties 文件中的以下四个属性。无需对辅助或接收服务器属性文件进行任何更改。

sync.ipaddress
（例如）指定接收服务器的地址和 ssl 端口。

```
sync.ipaddress = backupekm.server.ibm.com:1443
```

如果该属性未指定或者指定错误，那么系统将禁用自动同步。

sync.action

合并或重写接收服务器中的现有数据。有效值是**合并**（缺省值）和**重写**。同步配置属性始终生成一个重写文件。

sync.timeinhours

发送数据的频率。按整数（小时数）指定值。启动服务器时将出现时间间隔，也就是说，在服务器运行了指定的小时数之后，将出现同步。缺省值是 24。

sync.type

应发送哪些数据。有效值是 **drivetab**（缺省值）、**config** 和 **all**。

配置基础

注: 如果您按照第 3-5 页的『使用 GUI 来创建配置文件、密钥库以及证书』中的过程执行操作，那么您就已经创建了基本的配置并且不需要执行以下的任何步骤。该信息说明如何不使用 GUI 来执行这些任务，并且如果您想要利用其他配置选项，那么该信息是很有用的。

Windows 用户请注意: Windows 不接受包含空白目录路径的命令。在输入命令时，需要为这一目录指定短名称，例如: `progra~1` 而不是 `Program Files`。要列出目录的短名称，发出 **dir /x** 命令。

此过程包含配置加密密钥管理器所需的最少步骤。附录 A 包含服务器配置属性文件的示例。有关服务器和客户机配置的所有属性的完整列表，请参阅附录 B。

1. 使用 **keytool** 管理 JCEKS 密钥库。在创建密钥库时，请注意路径和文件名以及赋予证书与密钥的名称。本信息将用在稍后的步骤中。
2. 创建密钥库（如果密钥库不存在）。将要与磁带机配合使用的证书和密钥添加或导入到新的密钥库。（请参阅第 3-9 页的『在 LTO 4 和 LTO 5上生成加密密钥和别名』。）请注意赋予证书与密钥的名称。本信息将用在稍后的步骤中。
3. 创建密钥组并填充密钥别名。请参阅第 3-13 页的『密钥组的创建与管理』。
4. 使用所选文本编辑器打开 **KeyManagerConfig.properties** 以指定下列属性。请注意服务器的当前设计是非常严谨的。对于 Linux 机器，不要因为 ^M 而用 Windows 来编辑文件。如果使用 Windows，用 gvim/vim 编辑文件。

   Windows 用户请注意: 即使是在 Windows 上运行，Java SDK 仍然使用正斜杠。在指定 **KeyManagerConfig.properties** 文件中的路径时，请确保使用正斜杠。当在命令窗口中指定标准路径名时，针对 Windows 以标准方式使用反斜杠。

   a. **Audit.Handler.File.Directory** – 指定审计日志的存储位置。
   b. **Audit.metadata.file.name** – 为元数据 XML 文件指定标准路径和文件名。
   c. **Config.drivetable.file.url** – 为对加密密钥管理器已知的磁带机的相关信息指定一个位置。在启动服务器或 CLI 客户机之前，不需要此文件。如果文件不存在，那么它将在加密密钥管理器服务器关闭期间创建。
   d. **TransportListener.ssl.keystore.name** – 指定在步骤 1 中创建的密钥库的路径和文件名。

e. **TransportListener.ssl.truststore.name** – 指定在步骤 1 中创建的密钥库的路径和文件名。

f. **Admin.ssl.keystore.name** – 指定在步骤 1 中创建的密钥库的路径和文件名。

g. **Admin.ssl.truststore.name** – 指定在步骤 1 中创建的密钥库的路径和文件名。

h. **config.keystore.file** – 指定在步骤 1 中创建的密钥库的路径和文件名。

i. **drive.acceptUnknownDrives** – 指定 true 或 false。如值为 true，那么允许将与加密密钥管理器联系的新磁带机自动添加到磁带机表格。缺省值为 false。

5. 可添加或省略以下可选密码条目。如果在 **KeyManagerConfig.properties** 中未指定这些条目，那么加密密钥管理器在启动服务器期间将提示输入密钥库密码。

   a. **Admin.ssl.keystore.password** – 指定在步骤 1 中创建的密钥库的密码。

   b. **config.keystore.password** – 指定在步骤 1 中创建的密钥库的密码。

   c. **TransportListener.ssl.keystore.password** – 指定在步骤 1 中创建的密钥库的密码。

   当添加到 **KeyManagerConfig.properties** 文件中时，加密密钥管理器会模糊化这些密码，以增强安全性。

6. 如果要对本地操作系统注册表执行 CLI 客户机认证操作，那么可选择将 **Server.authMechanism** 属性设置为值 LocalOS。如未指定属性值（或将其设置为 EKM），那么缺省情况下，CLI 客户机用户使用 usr/passwd 作为 EKMAdmin/changeME 登录到密钥管理器服务器。（此密码可用 **chgpasswd** 命令更改。）

   当 **Server.authMechanism** 属性设置为 LocalOS 时，Linux 平台需要其他设置。请参阅 **http://support.dell.com** 或产品随附的 Dell 加密密钥管理器介质上的自述文件获取更多信息。第 5-5 页的『对 CLI 客户机用户进行认证』 包含了较多信息。

7. 保存对 **KeyManagerConfig.properties** 的更改。

8. 启动加密密钥管理器服务器。要不通过 GUI 启动服务器，

   Windows 上

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

   Linux 平台上

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

   请参阅第 5-1 页的『启动、刷新和关闭密钥管理器服务器』获取详细说明。

9. 启动 CLI 客户机:

   Windows 上

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

   Linux 平台上

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

   请参阅第 5-5 页的『命令行界面客户机』获取详细说明。

10. 如果在步骤 4（i）中指定 **drive.acceptUnknownDrives = false**，那么通过输入以 # 作为提示符的以下命令来配置磁带机:

    ```
    adddrive -drivename drive_name -rec1 cert_name -rec2 cert_name
    ```

    例如:

    ```
    # adddrive -drivename 000001365054 -rec1 key1c1 -rec2 key1c2
    ```

后接

```
# listdrives -drivename 000001365054
```

返回

```
Entry Key:  SerialNumber = 000001365054

Entry Key:  AliasTwo = key1c2

Entry Key:  AliasOne = key1c1
 Deleted : false
 Updated : true
 TimeStamp : Sun Jul 03 17:34:44 MST 2007
```

11. 以 # 作为提示符输入 **listdrives** 命令以确保磁带机已成功添加。

第 5 章 管理加密密钥管理器

启动、刷新和关闭密钥管理器服务器

启动和关闭加密密钥管理器服务器非常方便。

刷新服务器可以使加密密钥管理器将内存中其密钥库、磁带机表格和配置信息的当前内容转储到各自的文件，然后将它们重新装入到内存。使用 CLI 客户机对这些组件进行任何更改之后，发出刷新将非常有用。虽然在加密密钥管理器服务器关闭时系统将自动保存此类更改，但是如果系统崩溃或电源中断，发出服务器刷新将防止这些更改丢失。

从 Dell 加密密钥管理器 GUI 启动加密密钥管理器服务器:

1. 打开 GUI（如果它并未启动）:

   Windows 上

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

   Linux 平台上

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

2. 在 GUI 左边的导航器中单击 **Server Health Monitor**。
3. 在“Server Status”页面（图 5-1）上，单击 **Start Server** 或 **Refresh Server**。

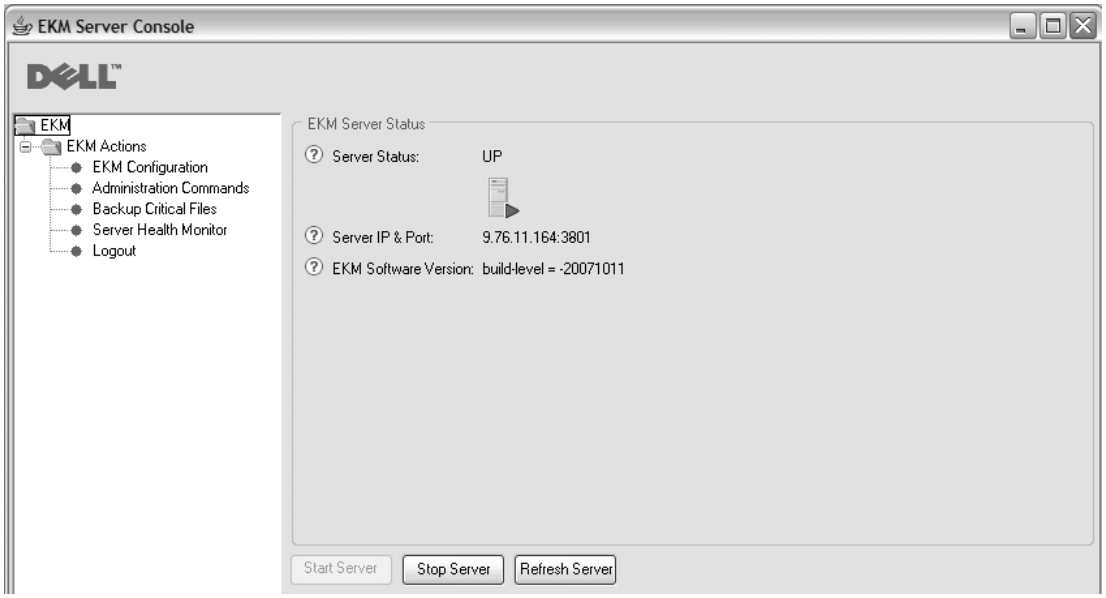

图 5-1. 服务器状态

4. 在“服务器状态”窗口上显示服务器状态的更改。请参阅图 5-1。
5. 将显示 Login 窗口（第 5-2 页的图 5-2）。

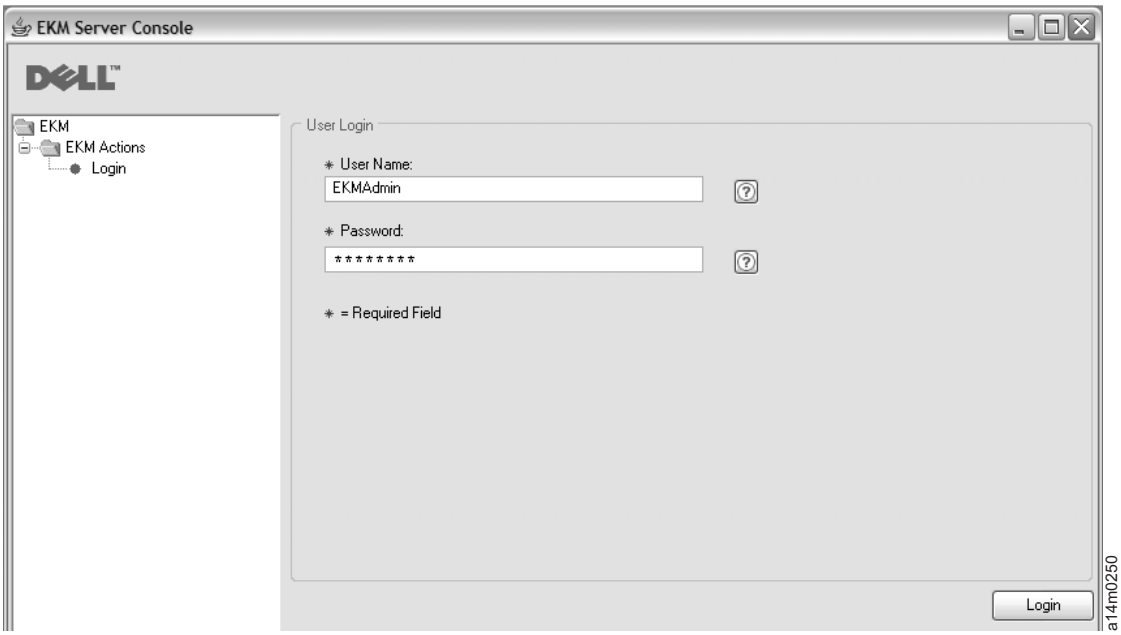

图 5-2. Login 窗口

输入用户名的 EKMAdmin。初始密码是 changeME。登录之后，您可以使用 **chgpasswd** 命令来更改密码。请参阅第 5-8 页的『chgpasswd』。

注: • Dell 加密密钥管理器 GUI 可能无法显示主机 IP 地址

目前的 GUI 的两项局限性使其无法在**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:

- 当前应用程序无法识别 IPV6。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 IP 地址。
- 如果加密密钥管理器应用程序安装在 Linux 系统中，那么该应用程序将显示本地主机地址，而不是实际的活动 IP 端口。

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。

6. 单击 **Login**。

使用相同的"服务器状态"页面可关闭服务器。

使用脚本启动密钥管理器服务器

Windows 上

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

Linux 平台上

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

要关闭服务器，在第 5-5 页的『命令行界面客户机』使用下面描述的任意方法来发出 **stopekm** 命令。其他方法是向密钥管理器过程发送 **sigterm**。这使服务器能够完全关闭和终止运行。请不要向密钥管理器过程发送 **sigkill**。**sigkill** 将不会完全关闭过程。例如，在 Linux 系统，输入 kill -SIGTERM *pid* 或者 kill -15 *pid*。

从命令提示符启动和关闭密钥管理器服务器

要从任何命令窗口或 shell 启动加密密钥管理器服务器，请输入:

```
java com.ibm.keymanager.EKMLaunch KeymanagerConfig.properties
```

此操作将在后台启动加密密钥管理器服务器。正确启动时，使用 `ps -ef | grep java` 命令（ Linux 平台）或使用 Windows 任务管理器可以显示加密密钥管理器Java 进程。作为 Windows 服务运行时，它将显示为 LaunchEKMService。

要关闭服务器，在第 5-5 页的『命令行界面客户机』使用下面描述的任意方法来发出 **stopekm** 命令。其他方法是向密钥管理器过程发送 **sigterm**。这使服务器能够完全关闭和终止运行。请不要向密钥管理器过程发送 **sigkill**。**sigkill** 将不会完全关闭过程。例如，在 Linux 系统，输入 `kill -SIGTERM pid` 或者 `kill -15 pid`。

在 Windows 平台，启动 Dell 加密密钥管理器 作为 Windows 服务时，您可以从控制面板使它停止运行。

将密钥管理器服务器安装为 Window 服务

将加密密钥管理器服务器在主机服务器中安装为服务可以确保主机服务器重新引导时，加密密钥管理器服务器应用程序将启动。

1. 将从 Dell 支持 Web 站点（**http://support.dell.com**）下载的可执行文件 LaunchEKMService.exe 文件解压到临时目录中。
2. 要使该服务正常运行，必须设置某些环境变量。
   a. 从“开始”菜单，单击**控制面板**。
   b. 双击**系统**。
   c. 单击**高级**选项卡。
   d. 单击**环境变量**。
   e. 在“系统变量”列表下面，单击**新建**。
   f. 将 `JAVA_HOME` 指定为变量名称，然后输入 IBM JVM 目录。缺省安装目录为 `C:\PROGRA~1\IBM\Java60`
   g. 单击**确定**。
3. 使用该过程编辑系统 PATH 变量。

   注: 无法从命令行设置 PATH 变量。
   a. 从“开始”菜单，单击**控制面板**。
   b. 双击**系统**。
   c. 单击**高级**选项卡。
   d. 单击**环境变量**。
   e. 滚动**路径**变量的系统变量列表，然后单击**编辑**。
   f. 将 IBM JVM 路径添加到 Path 变量的开头。缺省安装目录为 `C:\PROGRA~1\IBM\Java60\jre\bin`

      注: 在路径结尾部分插入一个分号，将其与路径列表中的其他目录隔开。
   g. 单击**确定**。

4. 确保加密密钥管理器服务器配置属性文件中的路径是全限定的。该文件的名称为 KeyManagerConfig.properties，位于 C:\ekm\gui 目录中。应检查文件中下面的所有路径并将其更新，以确保具有全限定路径（例如，使用 c:\ekm\gui\EKMKeys.jck，而不要使用 gui\EKMKeys.jck）。有关使用缺省安装时如何更改路径，请参阅下列示例。

   这些是属性和使用缺省安装和密钥库名称时应指向的全限定路径。每个这些项都可以在 KeyManagerConfig.properties 文件中找到。

   config.keygroup.xml.file
   路径应更改为：FILE:C:/ekm/gui/keygroups/KeyGroups.xml

   Admin.ssl.keystore.name
   路径应更改为：C:/ekm/gui/EKMKeys.jck

   TransportListener.ssl.truststore.name
   路径应更改为：C:/ekm/gui/EKMKeys.jck

   Audit.metadata.file.name
   路径应更改为：C:/ekm/gui/metadata/ekm_metadata.xml

   Audit.handler.file.directory
   路径应更改为：C:/ekm/gui/audit

   config.keystore.file
   路径应更改为：C:/ekm/gui/EKMKeys.jck

   TransportListener.ssl.keystore.name
   路径应更改为：C:/ekm/gui/EKMKeys.jck

   config.drivetable.file.url
   路径应更改为：FILE:C:/ekm/gui/drivetable/ekm_drivetable.dt

   Admin.ssl.truststore.name
   路径应更改为：C:/ekm/gui/EKMKeys.jck

5. **LaunchEKMServices.exe** 文件必须从命令提示符运行。在 Windows 中可以通过 **开始 > 程序 > 附件 > 命令提示符**来访问命令提示符。
6. 从命令提示符浏览到抽取 **LaunchEKMService.exe** 的临时目录。使用下列选项作为参考运行 **LaunchEKMService.exe** 文件。

   LaunchEKMService {**-help** | **-i** *config_file* | **-u**}

   -help
   显示用途信息。

   -i 将加密密钥管理器安装为 Windows 服务。此选项要求将配置属性文件的完整路径名作为参数传递进来。缺省路径和文件名为 C:\ekm\gui\KeyManagerConfig.properties。

   -u 如果不再需要将其作为服务运行，请卸载密钥管理器 Windows 服务。请注意，EKMServer 服务必须先停止运行，才能卸载。运行此命令时，可能还将显示以下错误消息：Could not remove EKMServer. Error 0。但是，该服务可能仍将被卸载。

   要将加密密钥管理器安装为 Windows 服务，请发出命令：

   ```
   LaunchEKMService.exe -i config file
   ```

7. 使用上面的命令安装服务之后，EKMServer 将出现在服务控制面板中，您可以使用“服务控制面板”启动和关闭加密密钥管理器。

   注: 第一次使用时，必须使用控制面板手动启动该 Windows 服务。

命令行界面客户机

启动加密密钥管理器服务器之后，您就可以在本地或远程通过客户机界面发出 CLI 命令。要发出 CLI 命令，您必须首先启动 CLI 客户机。

对 CLI 客户机用户进行认证

配置文件中的 Server.authMechanism 属性指定认证机制以与本地/远程客户机一起使用。当值设置为 EKM 时，CLI 客户机用户必须将 EKMAdmin/changeME 用作用户/密码来登录到服务器。（使用 **chgpasswd** 命令可以更改此密码。请参阅第 5-8 页的『chgpasswd』。）Server.authMechanism 属性的缺省设置是 EKM。

在 KeyManagerConfig.properties 文件中将 Server.authMechanism 属性值指定为 LocalOS 时，针对本地操作系统注册表来执行客户机认证。CLI 客户机用户必须使用操作系统的用户/密码登录到服务器。请注意，只有允许登录和向服务器提交命令的用户/密码才是运行服务器且同时具有超级用户/root 权限的用户标识。

重要: 对加密密钥管理器配置文件进行这些更改时，必须关闭加密密钥管理器服务器和该 GUI。

对于 Windows 中基于本地操作系统的认证，请将 KeyManagerConfig.properties 中的 Server.authMechanism=LocalOS 设置如下:

1. 找到 KeyManagerConfig.properties 文件（c:\ekm\gui 目录）。
2. 使用所选文本编辑器打开文件（建议使用写字板）。
3. 找到 Server.authMechanism 字符串。如果该字符串不存在，请严格按照 Server.authMechanism=LocalOS 的格式将其添加到该文件中。
4. 保存文件。

现在您用于加密密钥管理器服务器的用户标识和密码与 OS 用户帐户相匹配。请注意，只有有权登录服务器并向服务器提交命令且具有管理员特权的用户才能管理加密密钥管理器服务器。

对于 Linux 平台上基于本地操作系统的认证，需要完成更多步骤:

1. 从 **http://support.dell.com** 下载 Dell Release R175158（EKMServicesAndSamples），并将文件抽取到所选目录中。
2. 在下载中找到 LocalOS 目录。
3. 将 libjaasauth.so 文件从平台上相应的 JVM-JaasSetup 目录复制到 *java_home*/jre/bin 中。
   - 在 32 位 Intel Linux 环境中，将 LocalOS-setup/linux_ia32/libjaasauth.so 文件复制到 *java_home*/jre/bin/ 目录中，其中 *java_home* 通常为 *java_install_path*/IBMJava-i386-60（对于运行 1.6 JVM 的 32 位 Intel Linux 内核）。
   - 在 64 位 AMD64 Linux 环境中，将 LocalOS-setup/linux-x86_64/libjaasauth.so 文件复制到 *java_home*/jre/bin/ 目录中，其中*java_home* 通常为 *java_install_path*/IBMJava-x86_64-60（对于运行 1.6 JVM 的 64 位 Linux 内核）。

对于 Windows 平台，该文件不是必需的。

安装完成之后，可以启动加密密钥管理器服务器。加密密钥管理器客户机现在可以使用基于操作系统的用户/密码登录。请注意，只有允许登录和向服务器提交命令的用户标识才是运行服务器且同时具有超级用户/root 权限的用户标识。

可从 Dell 产品介质以及加密密钥管理器 Web 站点上的 **http://support.dell.com**，以了解更多安装详细信息。

启动命令行界面客户机

注: 必须将加密密钥管理器服务器和加密密钥管理器 CLI 客户机属性文件中的 TransportListener.ssl.port 属性同时设置为相同的值，否则它们将无法通信。如果发生问题，请参阅第 6-2 页的『调试 CLI 客户机和 EKM 服务器之间的通信问题』。

加密密钥管理器 CLI 客户机和加密密钥管理器服务器使用 SSL 来保护其通信。使用不进行客户机认证的缺省 JSSE 配置时，加密密钥管理器服务器上 TransportListener.ssl.keystore 内的证书必须存在于 TransportListener.ssl.truststore 中。这样，客户机才可以信任该服务器。如果加密密钥管理器 CLI 客户机与加密密钥管理器服务器在同一个系统上运行，那么可以使用相同的配置属性文件。这样加密密钥管理器 CLI 客户机就可以使用与加密密钥管理器服务器相同的密钥库/信任密钥库配置。如果不在同一个系统上，或者您希望客户机使用不同的密钥库，那么必须将证书从加密密钥管理器服务器配置属性文件中指定的 TransportListener.ssl.keystore 中导出。必须将这些证书导入加密密钥管理器 CLI 属性文件中的 TransportListener.ssl.truststore 指定的信任密钥库中。

您可以通过四种方式启动 CLI 客户机和发出 CLI 命令。无论选择哪一种，您必须指定 CLI 配置文件的名称。请参阅附录 B 以获取详细信息。

使用脚本

Windows 上

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

Linux 平台上

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

交换方式

要从任何命令窗口或 shell 中交互地运行命令，请输入:

```
java com.ibm.keymanager.KMSAdminCmd CLIconfiglfile_name -i
```

此时会显示 # 提示符。提交任何命令之前，您必须使用以下命令将 CLI 客户机登录到密钥管理器服务器:

```
#login –ekmuser EKMAdmin –ekmpassword changeME
```

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，使用 **quit** 或 **logout** 命令以关闭 CLI 客户机。缺省情况下，如果客户机闲置十分钟，加密密钥管理器服务器将关闭通信套接字。之后，尝试输入命令将导致客户机退出。要为加密密钥管理器服务器/客户机套接字指定更长的超时周期，请修改 KeyManagerConfig.properties 文件中的 theTransportListener.ssl.timeout 属性。

使用命令文件

要将文件中的批处理命令提交到密钥管理器服务器，请创建包含要发出命令的文

件，例如 *clifile*。该文件的第一个命令必须是 **login** 命令，因为在执行任何命令之前要求客户机登录。例如，clifile 可能包含以下内容:

```
login -ekmuser EKMAdmin -ekmpassword changeME
listdrives
```

然后，要执行此命令文件，请启动 CLI 客户机:

```
java com.ibm.keymanager.admin.KMSAdminCmd CLIconfiglfile_name –filename clifile
```

一次执行一个命令

通过指定每个命令的 CLI userid_ID 和密码，您可以一次运行一个命令。从任何命令窗口或 shell 中，输入:

```
java com.ibm.keymanager.KMSAdminCmd ClientConfig.properties_name -listdrives
    -ekmuser EKMAdmin -ekmpassword changeME
```

（使用 **chgpasswd** 命令可以更改此密码。）此时将运行命令，并且客户机会话将终止运行。

CLI 命令

加密密钥管理器提供的命令集可用于通过命令行界面客户端与加密密钥管理器服务器交互，其中包括以下命令。

addaliastogroup

将现有（源）密钥组中的特定别名复制到新的（目标）密钥组。当您想将已存在于一个密钥组中的别名添加到另一密钥组时，此命令是很有用的。

addaliastogroup -aliasID *aliasname* **-sourceGroupID** *groupname* **-targetGroupID** *groupname*

-aliasID
要添加的密钥的*别名*。

-sourceGroupID
用于识别别名要复制到的目标组的唯一*组名*。

-targetGroupID
用于识别别名要添加到的目标组的唯一*组名*。

示例: addaliastogroup -aliasID aliasname -sourceGroupID keygroup1 -targetGroupID keygroup2

adddrive

将新磁带机添加到密钥管理器磁带机表格。请参阅第 4-1 页的『自动更新磁带机表』了解如何将磁带机自动添加到磁带机表格。请参阅第 2-4 页的『加密密钥与 LTO 4 和 LTO 5 磁带机』以获取别名要求信息。

adddrive -drivename *drivename* [**-rec1** *alias*] [**-rec2** *alias*][**-symrec** *alias*]

-drivename
drivename 指定要添加的磁带机的 12 位序列号。

注: 必须在 10 位序列号前加两个 0，以达到 12 位。

-rec1
指定磁带机的证书*别名*（或密钥标注）。

-rec2
指定磁带机证书的第二个*别名*（或密钥标注）。

-symrec
指定对称密钥的*别名*或磁带机的密钥组名。

示例: adddrive -drivename 000123456789 -rec1 alias1 -rec2 alias2

addkeygroup

在密钥组 XML 中创建具有唯一组标识的密钥组实例。

addkeygroup -groupID *groupname*

-groupID
用于识别密钥组 XML 文件中的组的唯一*组名*。

示例: addkeygroup -groupID keygroup1

addkeygroupalias

为密钥库中现有的密钥别名创建新的别名，用于添加到特定密钥组标识。

addkeygroupalias -alias *aliasname* **-groupID** *groupname*

-alias
密钥的新*别名*。

-groupID
用于识别密钥组 XML 文件中的组的唯一*组名*。

示例: addkeygroupalias -alias aliasname -groupID keygroup1

chgpasswd

更改 CLI 客户机的用户（EKMAdmin）缺省密码。

chgpasswd -new *password*

-new
替换先前密码的新*密码*。

示例: chgpasswd -new ebw74jxr

createkeygroup

在 KeyGroups.xml 文件中创建初始密钥组对象。仅运行一次。

createkeygroup -password *password*

-password
用于加密 KeyGroups.xml 文件中的密钥库密码的*密码*，以备将来的恢复操作。密钥库加密密钥组的密钥，而密钥组的密钥依次加密各个单独密钥组别名密码。因而 KeyGroups.xml 文件中的密钥全都是不清晰的。

示例: createkeygroup -password password

deletedrive

从密钥管理器磁带机表格删除磁带机。等同的命令有 **deldrive** 和 **removedrive**。

deletedrive -drivename *drivename*

-drivename
drivename 指定要删除的磁带机的序列号。

示例: deletedrive -drivename 000123456789

delgroupalias

从密钥组删除密钥别名。

delgroupalias -groupID *groupname* **-alias** *aliasname*

-groupID
用于识别 KeyGroups.xml 文件中的组的唯一*组名*。

-alias
要除去的密钥别名的*别名*。

示例: delgroupalias -groupID keygroup1 -alias aliasname

delkeygroup

删除整个密钥组。

delkeygroup -groupID *groupname*

-groupID
用于识别 KeyGroups.xml 文件中的组的唯一*组名*。

示例: delkeygroup -groupID keygroup1

exit

退出 CLI 客户机并关闭加密密钥管理器服务器。等同的命令有 **quit**。

示例: **exit**

export

将磁带机表格或加密密钥管理器服务器配置文件导出到指定的 URL。

export {**-drivetab**|**-config**} **-url** *urlname*

-drivetab
导出磁带机表格。

-config
导出加密密钥管理器服务器的配置文件。

-url
urlname 指定文件要写入的目标位置。

示例: export -drivetab -url FILE:///keymanager/data/export.table

help

显示命令行界面命令名和语法。等同的命令是 **?**。

help

import

从指定的 URL 导入磁带机表格或配置文件。

import {**-merge**|**-rewrite**} {**-drivetab**|**-config**} **-url** *urlname*

-merge
将新数据与当前数据合并。

-rewrite
用新数据替换当前数据。

-drivetab
导入磁带机表格。

-config
导入配置文件。

-url
urlname 指定要从中获取新数据的目标位置。

示例: import -merge -drivetab -url FILE:///keymanager/data/export.table

list

通过 config.keystore.file property 列出密钥库中包含的证书。

list [**-cert** |**-key**|**-keysym**][**-alias** *alias* **-verbose** |**-v**]

-cert
列出指定密钥库中的证书。

-key
列出指定密钥库的所有密钥。

-keysym
列出指定密钥库的对称密钥。

-alias
*别名*将特定证书指定给列表。

-verbose|-v
显示与证书有关的更多信息。

示例:

`list -v` 列举密钥库中的所有信息。

`list -alias mycert -v` 如果 mycert 存在于 config.keystore.file 密钥库中, 为 mycer 别名列举所有可用数据,

listcerts

通过 config.keystore.file property 列出密钥库中包含的证书。

listcerts [**-alias** *alias* **-verbose** |**-v**]

-alias
*别名*将特定证书指定给列表。

-verbose|-v
显示与证书有关的更多信息。

示例: listcerts -alias alias1 -v

listconfig

列出存储器中的加密密钥管理器EKM 服务器配置属性，以反映 KeyManagerConfig.properties 文件的当前内容和由 **modconfig** 命令所做的任何更新。

listconfig

listdrives

列出磁带机表格中的磁带机。

listdrives [**-drivename** *drivename*]

-drivename
drivename 指定列举的磁带机的序列号。

-verbose|-v
显示与磁带机有关的更多信息。

示例: listdrives -drivename 000123456789

login

登录加密密钥管理器服务器上的 CLI 客户机。

login -ekmuser *userID* **-ekmpassword** *password*

-ekmuser
根据所使用的认证类型，为*用户标识*指定 EKMadmin 或 localOS 用户标识值（请参阅第 5-5 页的『对 CLI 客户机用户进行认证』）。

-ekmpassword
用户标识的密码无效。

示例: login -ekmuser EKMAdmin -ekmpassword changeME

logout

注销当前用户。等同的命令有 **logoff**。只有当客户机会话已启用时，这些命令才有用。

示例: **logout**

modconfig

修改加密密钥管理器服务器配置属性文件（即 KeyManagerConfig.properties）中的属性。等同的命令有 **modifyconfig**。

modconfig {**-set** | **-unset**} **-property** *name* **-value** *value*

-set
将指定的属性设置为指定值。

-unset
除去指定的属性。

-property
name 指定目标属性的名称。

-value
value 当已指定了 **-set** 时，为目标属性指定新的值。

示例: modconfig -set -property sync.timeinhours -value 24

moddrive

修改磁带机表格中的磁带机信息。等同的命令有 **modifydrive**。

moddrive -drivename *drivename* {**-rec1** [*alias*] | **-rec2** [*alias*]| **-symrec** [*alias*]}

-drivename
drivename 指定磁带机的序列号。

-rec1
指定磁带机的证书*别名*（或密钥标注）。

-rec2
指定磁带机证书的第二个*别名*（或密钥标注）。

-symrec
指定对称密钥的*别名*或磁带机的密钥组名。

示例: moddrive -drivename 000123456789 -rec1 newalias1

refresh

指令加密密钥管理器用最新配置参数刷新调试、审计和磁带机表格值。

示例: **refresh**

refreshks

刷新密钥库。如果在加密密钥管理器服务器正在运行时对密钥库进行了修改，那么请使用此命令重新装入 **config.keystore.file** 中指定的密钥库。仅在需要时使用此命令，因为此操作可能会降低性能。

示例: **refreshks**

status

显示密钥管理器是启动着的还是关闭着的。

示例: **status**

stopekm

关闭加密密钥管理器服务器。

示例: **stopekm**

sync

将另一台加密密钥管理器服务器上的配置文件属性和/或磁带机表格信息与发布发布命令的密钥管理器服务器上的配置文件属性和/或磁带机表格信息进行同步。

注: 无论在密钥库还是 KeyGroups.xml 文件上，同步方法都不起作用。这些都必须手动复制。

sync {**-all** | **-config** | **-drivetab**} **-ipaddr** *ip_addr* :*ssl*:*port* [**-merge** | **-rewrite**]

-all
将配置属性文件和磁带机表格信息同时发送到 **-ipaddr** 指定的加密密钥管理器服务器。

-config
仅将配置属性文件发送到 **-ipaddr** 指定的加密密钥管理器服务器。

-drivetab
仅将磁带机表格信息发送到 **-ipaddr** 指定的加密密钥管理器服务器。

-ipaddr
ip_addr:ssl:port 指定接收加密密钥管理器服务器的地址和 ssl 端口。*ssl:port* 应与在接收服务器的 KeyManagerConfig.properties 文件中为“TransportListener.ssl.port”指定的值相匹配。

-merge
合并新磁带机表格数据与当前数据。（配置文件始终是一个重写文件。）这（重写）是缺省值。

-rewrite
用新数据替换当前数据。

示例: sync -drivetab -ipaddr remoteekm.ibm.com:443 -merge

version

显示加密密钥管理器服务器的版本。

示例: **version**

第 6 章 问题确定

您可以启用加密密钥管理器的单个组件、多个组件，或者所有组件的调试功能。

检查这些重要文件以确定加密密钥管理器服务器问题

当加密密钥管理器无法启动时，可以检查三个文件来确定问题的根源。

- **native_stdout.log** 和 **native_stderr.log**
  - 由于加密密钥管理器服务器在后台进程中运行，因此没有控制台来显示其常规的通知消息和错误消息。这些消息将记录到这两个文件中。
  - 如果加密密钥管理器服务器属性文件包含属性 **debug.output.file**，那么这两个文件将创建在与调试日志相同的目录中。
  - 如果加密密钥管理器服务器属性文件不包含属性 **debug.output.file**，那么这两个文件将创建在工作目录中。
  - 每次启动加密密钥管理器服务器时，都将删除并重新创建这两个文件。
- 审计日志
  - 审计日志包含加密密钥管理器进行处理时记录的记录。
  - 该文件的位置由加密密钥管理器服务器配置属性文件（即 **KeyManagerConfig.properties**）中的两个属性来指定。
    - Audit.handler.file.directory — 指定审计日志的保存位置
    - Audit.handler.file.name — 指定审计日志的文件名。
  - 有关审计的更多信息，请参阅第 7-1 页的第 7 章，『审计记录』。

大于 127 个字符的密钥库密码日志条目

当加密密钥管理器作为一项 Windows 服务进行安装，而 KeyManagerConfig.properties 文件中的密钥库密码长度大于等于 128 个字符时，加密密钥管理器将无法启动，这是因为无法提示输入可接受长度的密码。本机加密密钥管理器日志包含类似以下内容的条目:

native_stdout.log

```
Server initialized
```

native_stderr.log

```
at com.ibm.keymanager.KeyManagerException: Default keystore failed to load
at com.ibm.keymanager.keygroups.KeyGroupManager.loadDefaultKeyStore(KeyGroupManager.java:145)
at com.ibm.keymanager.keygroups.KeyGroupManager.init(KeyGroupManager.java:605)
at com.ibm.keymanager.EKMServer.c(EKMServer.java:243)
at com.ibm.keymanager.EKMServer.<init>(EKMServer.java:753)
at com.ibm.keymanager.EKMServer.a(EKMServer.java:716)
at com.ibm.keymanager.EKMServer.main(EKMServer.java:129)
```

调试 CLI 客户机和 EKM 服务器之间的通信问题

EKM CLI 客户机和 EKM 服务器之间的通信是在服务器和客户机配置属性文件中的 TransportListener.ssl.port 属性中指定的端口上进行的，而且通过 SSL 对其进行保护。

以下是客户机无法连接到 EKM 服务器的可能原因的列表。它包含显示如何确定问题并更正问题的各个步骤。

- EKM 服务器未在运行，因此客户机没有要进行通信的对象。
  1. 从命令窗口发出 **netstat –an**，并确认是否显示 EKM 服务器属性文件中的 TransportListener.ssl.port 和 TransportListener.tcp.portfrom 属性指定的端口。如果没有显示端口，那么服务器不在运行
- EKM CLI 客户机属性文件中的 TransportListener.ssl.host 属性不指向运行 EKM 服务器的正确主机。
  1. EKM CLI 客户机属性文件中的 TransportListener.ssl.host 属性的值缺省设置为 `localhost`。将该属性的值修改为指向正确主机。
- EKM 服务器和 EKM CLI 客户机不在同一端口上对话。
  1. 请检查 EKM 服务器和 EKM CLI 客户机属性文件中的 TransportListener.ssl.port 属性以确认它们是否都设置为同一值。
- EKM 服务器和 EKM CLI 客户机无法找到用于安全通信的公共证书。
  1. 确保 TransportListener.ssl.keystore 和 TransportListener.ssl.truststore CLI 客户机属性中指定的密钥库包含的证书与服务器属性中的 Admin.ssl.keystore 和 Admin.ssl.truststore 密钥库的证书相同。
  2. 确保客户机属性中的 TransportListener.ssl.keystore.password 具有正确的密码。
  3. 确保这些密钥库中的证书均未过期。JSSE 将不使用过期的证书来确保通信安全。
- EKM CLI 客户机属性文件是只读的。
  1. 请检查文件的属性和许可权以确保运行 EKM CLI 客户机的用户具有访问和修改文件的许可权。
- EKM 服务器属性文件具有 Server.authMechanism = LocalOS，但来自 EKMServicesAndSamples 软件包中的必需文件还未安装，或安装在错误的位置。
  1. 请参阅 EKMServiceAndSamples 软件包中包含的自述文件以获取关于认证的更多信息。

调试密钥管理器服务器问题

大部分有关密钥管理器的问题是关于配置或启动密钥管理器服务器。关于说明调试属性的信息，请参阅附录 B: 缺省配置文件。

如果加密密钥管理器无法启动，请检查防火墙。

软件防火墙或硬件防火墙可能会阻止加密密钥管理器访问端口。

EKM 服务器未启动。无法装入或找到 EKM.properties config。

1. 如果未指定 **KeyManagerConfig.properties** 的完整路径（属性文件没有位于缺省路径）就启动 KMSAdminCmd 或 EKMLaunch，那么会发生此错误。

   在 Windows 上，缺省路径是 **C:/Program Files/IBM/KeyManagerServer/**

   在 Linux 平台上缺省路径是 **/opt/ibm/KeyManagerServer/**

2. 重新输入命令以启动 KMSAdminCmd 并包括 **KeyManagerConfig.properties** 文件的完整路径。请参阅附录 B，“加密密钥管理器配置属性文件”以获取更多信息。

EKM 服务器未启动。XML 元数据文件的文件名需要在配置文件中指定。

配置文件中缺少 Audit.metadata.file.name 条目。

要纠正此问题，将 Audit.metadata.file.name 属性添加到 **KeyManagerConfig.properties** 配置文件。

无法启动 EKM.Mykeys。系统未找到指定的文件。

1. 当 **KeyManagerConfig.properties** 中的密钥库条目没有指向现有的文件时会出现此错误消息。
2. 要纠正此问题，请确保以下 **KeyManagerConfig.properties** 文件中的条目指向现有的、有效的密钥库文件:

   Admin.ssl.keystore.name

   TransportListener.ssl.truststore.name

   TransportListener.ssl.keystore.name

   Admin.ssl.truststore.name

   请参阅附录 B，“加密密钥管理器配置属性文件”以获取更多信息。

无法启动 EKM。文件不存在 = safkeyring://xxx/yyy

发生此错误的原因可能是因为在加密密钥管理器环境 shell 脚本中的 IJO 变量内指定了错误的提供程序。

对于 JCECCARACFKS 密钥库，请使用:

```
-Djava.protocol.handler.pkgs=com.ibm.crypto.hdwrCCA.provider
```

对于 JCERACFKS 密钥库，请使用:

```
-Djava.protocol.handler.pkgs=com.ibm.crypto.provider
```

无法启动 EKM。密钥库被篡改或密码不正确。

1. 如果属性文件中的一个或多个这些条目（请参阅附录 B，“加密密钥管理器配置属性文件”）的值不正确就会发生此错误:

   config.keystore.password（对应于 config.keystore.file）

   admin.keystore.password （对应于 admin.keystore.name）

   transportListener.keystore.password （对应于 transportListener.keystore.name）
2. 如果启动服务器时，在密码提示中输入了错误的密码，就会发生此错误。
3. 如在配置中没有一个密码，系统会三次提示您（前提是属性文件中所有的 3 个密钥库条目都是唯一的）。如果属性中所有的条目都是相同的，那么系统将只提示您一次。

无法启动 EKM。密钥库格式无效。

1. 当为属性文件的其中一个密钥库条目指定了错误的密钥库类型时，发生此错误。
2. 如果属性文件中的所有密钥库条目都指向同一个文件，那么加密密钥管理器将使用 config.keystore.type 值作为所有密钥库的密钥库类型。

3. 当属性文件中特殊的密钥库没有类型条目时，加密密钥管理器假定其类型为 jceks。

无法启动服务器。侦听器线程并未启动和运行。

发生此错误的一些原因有:

1. **KeyManagerConfig.properties** 文件中的以下两个条目指向了相同的端口:

   TransportListener.ssl.port

   TransportListener.tcp.port

   每个传输侦听器都必须配置到各自端口的侦听上。
2. 这些条目中的一个或两个被配置到其他服务（此服务与密钥管理器服务器在同一机器上运行）正在使用的端口上。找出其他服务没有在使用的端口并使用这些端口配置密钥管理器服务器。
3. 在运行 Linux 操作系统的系统上，如果端口中的一个或两个低于 1024，并且启动密钥管理器服务器的用户不是根用户，那么会发生此错误。修改 **KeyManagerConfig.properties** 中的传输侦听器条目以使用 1024 以上的端口。

native_stderr.log 中的消息: "[Fatal Error] :-1:-1: Premature end of file."

加密密钥管理器装入了空密钥组文件时，将产生此消息。此消息来自 XML 解析器，不会妨碍加密密钥管理器的启动，除非它被配置为使用密钥组，并且 **KeyManagerConfig.properties** 中的 config.keygroup.xml.file 属性指定的文件（加密密钥管理器服务器属性文件）已损坏。

错误: 在配置密钥库中找不到别名为: MyKey 的密钥。

属性文件中的 symmetricKeySet 条目含有在 config.keystore.file 中不存在的密钥别名。

要纠正此问题，将配置文件中的 symmetricKeySet 条目修改为仅包含存在于密钥库文件的别名，并且此密钥库文件由 **KeyManagerConfig.properties** 中的 config.keystore.file 条目指定，或者将缺少的对称密钥添加到密钥库。请参阅附录 B, "加密密钥管理器配置属性文件"以获取更多信息。

symmetricKeySet 中没有对称密钥，不支持 LTO 磁带机。

这是参考消息。加密密钥管理器服务器仍将启动，但是在此加密密钥管理器实例中不支持 LTO 磁带机。如果未配置 LTO 磁带机与此加密密钥管理器通信，那么这一点就不构成问题。

加密密钥管理器报告的错误

该小节定义加密密钥管理器报告并返回到磁带机检测数据中的错误消息。这些消息通常被称为故障症状代码或 FSC。以下表格包括错误编号、故障的简短描述和纠正操作。关于说明调试属性的信息，请参阅附录 B: 缺省配置文件。

表 6-1. 加密密钥管理器报告的错误

错误编号	描述	操作
EE02	加密读取消息失败: DriverErrorNotifyParameterError: “收到无效的 ASC & ASCQ。ASC & ASCQ 与密钥创建/密钥转译/密钥获取的其中一个操作不相匹配。”	磁带机请求了不受支持的操作。请确保运行了最新版本的加密密钥管理器（请参阅第 3-1 页的『下载最新版密钥管理器 ISO 映像』以确定最新版本）。请检查磁带机或代理服务器固件的版本并根据需要将其更新为最新版。启用密钥管理器服务器上的调试跟踪。尝试重新创建问题并收集调试日志。如果问题仍然存在，请参阅本出版物前面“请先阅读”一节中的“联系 Dell”，以获取关于技术帮助的信息。
EE0F	加密逻辑错误: 内部错误: “意外错误。EKM 中发生内部编程错误。”	请确保运行了最新版本的加密密钥管理器 （请参阅第 3-1 页的『下载最新版密钥管理器 ISO 映像』以确定最新版本）。请检查磁带机或代理服务器固件的版本并根据需要将其更新为最新版。启用密钥管理器服务器上的调试跟踪。尝试重新创建问题并收集调试日志。如果问题仍然存在，请参阅本出版物前面“请先阅读”一节中的“联系 Dell”，以获取关于技术帮助的信息。
	错误: 来自调用 CSNDDSV returnCode 12 reasonCode 0 的硬件错误。	如果使用硬件加密，请确保启动了 ICSF。
EE23	加密读取消息错误: 内部错误: “意外错误 .....”	从磁带机或代理服务器收到的消息由于常规错误而无法被语法分析。请确保运行了最新版本的加密密钥管理器 （请参阅第 3-1 页的『下载最新版密钥管理器 ISO 映像』以确定最新版本）。启用密钥管理器服务器上的调试。尝试重新创建问题并收集调试日志。如果问题仍然存在，请参阅本出版物前面“请先阅读”一节中的“联系 Dell”，以获取关于技术帮助的信息。
EE25	加密配置问题: 发生了与磁带机表格相关的错误。	如果提供了 config.drivetable.file.url 参数，请确认 KeyManagerConfig.properties 文件中的该参数是否正确。在加密密钥管理器服务器上运行 `listdrives -drivename <drivename>` 命令，以验证磁带机的配置是否正确（例如，磁带机系列号、别名和证书是否正确）。请确保运行了最新版本的加密密钥管理器 （请参阅第 3-1 页的『下载最新版密钥管理器 ISO 映像』以确定最新版本）。请检查磁带机或代理服务器固件的版本并根据需要将其更新为最新版。启用调试跟踪并尝试重新执行该操作。如果问题仍然存在，请参阅本出版物前面“请先阅读”一节中的“联系 Dell”，以获取关于技术帮助的信息。

表 6-1. 加密密钥管理器报告的错误 (续)

错误编号	描述	操作
EE29	加密读取消息失败: 无效的签名	从磁带机或代理服务器收到的消息与消息上的签名不相匹配。请确保运行了最新版本的加密密钥管理器 （请参阅第 3-1 页的『下载最新版密钥管理器 ISO 映像』以确定最新版本）。启用密钥管理器服务器上的调试。尝试重新创建问题并收集调试日志。如果问题仍然存在，请参阅本出版物前面“请先阅读”一节中的“联系 Dell”，以获取关于技术帮助的信息。
EE2B	加密读取消息错误: “DSK 中不存在签名，或无法验证 DSK 中的签名。”	请确保运行了最新版本的加密密钥管理器 （请参阅第 3-1 页的『下载最新版密钥管理器 ISO 映像』以确定最新版本）。请检查磁带机或代理服务器固件的版本并根据需要将其更新为最新版。启用密钥管理器服务器上的调试跟踪。尝试重新创建问题并收集调试日志。如果问题仍然存在，请参阅本出版物前面“请先阅读”一节中的“联系 Dell”，以获取关于技术帮助的信息。
EE2C	加密读取消息失败: QueryDSKParameterError: “对来自设备的 QueryDSKMessage 进行语法分析时出错。意外的 dsk 计数或意外的有效负载。”	磁带机请求加密密钥管理器执行不受支持的功能。请确保运行了最新版本的加密密钥管理器（请参阅第 3-1 页的『下载最新版密钥管理器 ISO 映像』以确定最新版本）。请检查磁带机或代理服务器固件的版本并根据需要将其更新为最新版。启用密钥管理器服务器上的调试跟踪。尝试重新创建问题并收集调试日志。如果问题仍然存在，请参阅本出版物前面“请先阅读”一节中的“联系 Dell”，以获取关于技术帮助的信息。
EE2D	加密读取消息失败: 无效的消息类型	加密密钥管理器收到顺序错乱的消息或收到无法处理的消息。请确保运行了最新版本的加密密钥管理器 （请参阅第 3-1 页的『下载最新版密钥管理器 ISO 映像』以确定最新版本）。启用密钥管理器服务器上的调试。尝试重新创建问题并收集调试日志。如果问题仍然存在，请参阅本出版物前面“请先阅读”一节中的“联系 Dell”，以获取关于技术帮助的信息。
EE2E	加密读取消息失败: 内部错误: 意外错误: 无效的签名类型	从磁带机或代理服务器收到的消息不存在有效的签名类型。请确保运行了最新版本的加密密钥管理器 （请参阅第 3-1 页的『下载最新版密钥管理器 ISO 映像』以确定最新版本）。启用密钥管理器服务器上的调试。尝试重新创建问题并收集调试日志。如果问题仍然存在，请参阅本出版物前面“请先阅读”一节中的“联系 Dell”，以获取关于技术帮助的信息。
EE30	禁止的请求。	对磁带机请求了不受支持的操作。对目标磁带机输入正确和受支持的命令。

表 6-1. 加密密钥管理器报告的错误 (续)

错误编号	描述	操作
EE31	加密配置问题: 发生了与密钥库相关的错误。	请检查您试图使用或为缺省值配置的密钥标签。您可以通过使用 listcerts 命令，列出加密密钥管理器可以使用的证书。如果您知道自己在试图使用缺省值，那么请在加密密钥管理器服务器上运行 -drivename *磁带机名称* 命令，以验证磁带机的配置是否准确（例如，磁带机系列号和关联别名/密钥标签是否正确）。如果上述磁带机没有关联的别名/密钥标签，那么请检查 default.drive.alias1 和 default.drive.alias2 的值。如果该操作没有效果或别名/密钥标签存在，那么请收集调试日志并请参阅本出版物前面“请先阅读”一节中的“联系 Dell”，以获取关于技术帮助的信息。
EE32	与密钥库有关的问题。	很可能是因为该磁带已损坏，因为使用了带不同密钥的另一个加密密钥管理器，或者是因为用于加密该磁带的密钥已经被重命名或从密钥库中删除。请发出 `list -keysym` 命令并确保密钥库中包含请求的别名。
EEE1	加密逻辑错误: 内部错误: “意外错误: EK/EEDK 标志与子页相冲突。”	请确保运行了最新版本的加密密钥管理器 （请参阅第 3-1 页的『下载最新版密钥管理器 ISO 映像』以确定最新版本）。请检查磁带机或代理服务器固件的版本并根据需要将其更新为最新版。启用密钥管理器服务器上的调试。尝试重新创建问题并收集调试日志。如果问题仍然存在，请参阅本出版物前面“请先阅读”一节中的“联系 Dell”，以获取关于技术帮助的信息。
EF01	加密配置问题: “磁带机未配置。”	磁带机表格中不存在试图与加密密钥管理器通信的磁带机。如果提供了 config.drivetable.file.url 参数，请确认 KeyManagerConfig.properties 文件中的该参数是否正确。运行 `listdrives` 命令，以检查磁带机是否存在于列表中。如果不存在，请使用正确的磁带机信息通过 `adddrive` 命令，手动配置磁带机，或使用 `modconfig` 命令，将“drive.acceptUnknownDrives”属性设置为 true。启用调试跟踪并尝试重新执行该操作。如果问题仍然存在， 请参阅本出版物前面“请先阅读”一节中的“联系 Dell”，以获取关于技术帮助的信息。

消息

加密密钥管理器可以生成以下消息并将它们显示在管理员控制台上。

未指定配置文件

文本

```
Configuration file not specified:  KeyManager Configuration file not speci-
fied when starting EKM.
```

说明

KMSAdmin 命令要求配置文件作为命令行参数进行传递。

系统响应

程序停止运行。

操作员响应

请提供配置文件并重新尝试命令。

未能添加磁带机

文本

```
Failed to add drive. Drive already exists.
```

说明

因为磁带机已配置了加密密钥管理器并已存在于磁带机表格中，所以 **adddrive** 命令未能执行。

操作员响应

运行 **listdrives** 命令，以检查磁带机是否已配置了加密密钥管理器。如果磁带机已存在，那么可以使用 **moddrive** 命令来更改磁带机配置。运行 **help**，以获取更多信息。

未能归档日志文件

文本

```
Failed to archive the log file.
```

说明

无法重命名日志文件。

操作员响应

检查文件权限和磁带机上的空间。

未能删除配置

文本

```
"modconfig" command failed.
```

说明

未能通过 **modconfig** 命令删除加密密钥管理器配置。

操作员响应

使用 **help** 检查命令语法，以确认提供的参数是否正确。请检查审计日志，获取更多信息。

未能删除磁带机条目

文本

```
"deldrive" command failed.
```

说明

deldrive 命令未能从磁带机表格删除磁带机条目。

操作员响应

使用 **help** 检查命令语法，以确认提供的参数是否正确。使用 **listdrives** 命令确认磁带机已配置了加密密钥管理器。请检查审计日志，获取更多信息。

未能导入

文本

```
"import" command failed.
```

说明

无法导入磁带机表格或配置文件。

系统响应

加密密钥管理器服务器无法启动。

操作员响应

确认指定的 URL 是否存在并拥有读权限。使用 **help** 检查命令语法。确认参数是否正确，然后重试。

未能修改配置

文本

```
"modconfig" command failed.
```

说明

未能通过 **modconfig** 命令修改加密密钥管理器配置。

操作员响应

使用 **help** 检查命令语法，以确认提供的参数是否正确。请检查审计日志，获取更多信息。

文件名不能为空

文本

```
File name was not supplied for audit log file.
```

说明

审计文件名未通过加密密钥管理器的配置属性提供。此参数为必需的配置参数。

系统响应

程序停止运行。

操作员响应

检查向加密密钥管理器提供的配置属性文件中是否定义了属性 Audit.handler.file.name，并尝试重新启动。

文件大小限值不能是负数

文本

```
Maximum file size for audit log can not be a negative number.
```

说明

加密密钥管理器配置文件中的 Audit.handler.file.size 属性值必须是正数。

系统响应

加密密钥管理器未启动。

操作员响应

请为 Audit.handler.file.size 指定一个有效数值并尝试重新启动加密密钥管理器。

未使任何数据同步

文本

```
No data can be found to be synchronized with "sync".
```

说明

sync 命令无法识别任何要同步的数据。

操作员响应

检查是否存在所提供的配置文件，以及使用 *config.drivetable.file.url* 检查配置文件中是否正确配置了磁带机表格。使用**帮助**检查语法，然后重试 **sync** 命令。

输出无效

文本

```
Invalid input parameters for the CLI.
```

说明

特定的命令语法可能不正确。

操作员响应

确认输入的命令是否正确。使用 **help** 检查命令语法。确认提供的参数是否正确并重试。

配置文件中 SSL 端口号无效

文本

```
Invalid SSL port number specified in the EKM configuration file.
```

说明

配置文件中提供的 SSL 端口号不是有效的数值。

系统响应

加密密钥管理器未启动。

操作员响应

启动加密密钥管理器时为配置文件中的 TransportListener.ssl.port 属性指定有效的端口号并尝试重新启动。

配置文件中 TCP 端口号无效

文本

```
Invalid TCP port number specified in the EKM configuration file.
```

说明

配置文件中提供的 TCP 端口号不是有效的数值。

系统响应

加密密钥管理器未启动。

操作员响应

启动加密密钥管理器时为配置文件中的 TransportListener.tcp.port 属性指定有效的端口号并尝试重新启动。缺省 TCP 端口号为 3801。

必须在配置文件中指定 SSL 端口号

文本

```
SSL port number is not configured in the properties file.
```

说明

SSL 端口号是在配置属性文件中需要配置的属性。它将用于多个服务器环境中加密密钥管理器服务器之间的通信。

系统响应

加密密钥管理器未启动。

操作员响应

指定 TransportListener.ssl.port 属性的有效端口号，然后尝试重新启动加密密钥管理器。

必须在配置文件中指定 TCP 端口号

文本

```
TCP port number is not configured in the properties file.
```

说明

TCP 端口号是在配置属性文件中需要配置的属性。它将用于磁带机和加密密钥管理器之间的通信。

系统响应

加密密钥管理器未启动。

操作员响应

指定 TransportListener.tcp.port 属性的有效端口号，然后尝试重新启动加密密钥管理器。缺省 TCP 端口号为 3801。

服务器未能启动

文本

```
EKM server failed to start.
```

说明

加密密钥管理器服务器由于配置问题而无法启动。

操作员响应

检查配置文件中提供的参数。请检查日志，获取更多信息。

Sync 失败

文本

```
"sync" command failed.
```

说明

同步两个加密密钥管理器服务器之间数据的 Sync 操作失败。

操作员响应

确保为远程加密密钥管理器服务器指定的 IP 地址正确，并且可以访问该计算机。确保配置文件存在，并包含正确的磁带机表格信息。使用**帮助**检查 **sync** 命令语法。查看日志以了解更多信息。

指定的审计日志文件仅可读

文本

```
The audit log file can not be opened for writing.
```

说明

属性 Audit.handler.file.name 指定的加密密钥管理器配置中的审计日志文件不能打开，无法进行写入。

系统响应

加密密钥管理器未启动。

操作员响应

请检查所给审计文件和目录的许可并尝试重新启动加密密钥管理器。

无法装入 Admin 密钥库

文本

```
Keystore for Admin cannot be loaded.
```

说明

无法装入提供给加密密钥管理器的 admin 密钥库。Admin 密钥库用于多个服务器环境中加密密钥管理器服务器之间的服务器端通信。

系统响应

加密密钥管理器未启动。

操作员响应

检查配置文件设置。确保加密密钥管理器配置文件中的属性 admin.keystore.file、admin.keystore.provider 和 admin.keystore.type 正确（请参阅附录 B），密钥库文件存在，并具有读许可权。确保通过 admin.keystore.password 属性为 admin 密钥

库提供的密码或在命令行上输入的密码正确。尝试重新启动加密密钥管理器。

无法装入密钥库

文本

```
Keystore for EKM can not be loaded.
```

说明

无法装入指定给加密密钥管理器的密钥库。

系统响应

加密密钥管理器未启动。

操作员响应

检查配置文件设置。确保加密密钥管理器配置文件中的属性 config.keystore.file、config.keystore.provider 和 config.keystore.type 正确，密钥库文件存在，并具有读许可权。确保通过 config.keystore.password 属性为加密密钥管理器密钥库提供的密码或在命令行上输入的密码正确。尝试重新启动。

无法装入传输密钥库

文本

```
Transport keystore cannot be loaded.
```

说明

无法装入提供给加密密钥管理器的传输密钥库。传输密钥库用于多个服务器环境中加密密钥管理器服务器之间的客户机端通信。

系统响应

加密密钥管理器未启动。

操作员响应

检查配置文件设置。确保加密密钥管理器配置文件中的属性 transport.keystore.file、transport.keystore.provider 和 transport.keystore.type 正确，密钥库文件存在，并具有读许可权。确保通过 transport.keystore.password 属性为 admin 密钥库提供的密码或在命令行上输入的密码正确。尝试重新启动加密密钥管理器。

不受支持的操作

文本

```
User entered action for the CLI which is not supported for EKM.
```

说明

加密密钥管理器不支持或无法识别为 **sync** 命令提供的操作。有效操作是“合并”或“重写”。

操作员响应

使用**帮助**检查命令语法，然后重试。

第 7 章 审计记录

注: 本章中所描述的审计记录格式并不适合程序界面。这些记录的格式可能会随发行版的不同而有所改变。本章中对格式进行了记录，以满足某些审计记录的语法分析的需求。

审计概述

当加密密钥管理器处理请求期间发生各种审计事件时，审计子系统将文本审计记录写入到一组顺序文件中。审计子系统写入到的文件其目录和文件名是可配置的。这些文件的文件大小也是可配置的。随着记录被写入到文件中，文件的大小也随之达到可配置大小，此后文件将被关闭，且按照当前时间戳记重新命名。接着打开另一个文件，记录就写入到新创建的文件中。因而，审计记录的全部记录被分隔成可配置大小的文件，它们的名称按照文件大小超出可配置大小时的时间戳记来排列。

要防止所有审计日志（包括已创建的全部的顺序文件）中的信息量增长得太大而超出文件系统的可用空间，您可能要考虑创建脚本或程序来监控已配置的审计目录/文件夹/容器中的一组文件。当文件被关闭并按照时间戳记命名时，应当复制文件的内容并将其附加到期望的长期、持续的日志位置然后清除文件。注意运行时不要除去或更改加密密钥管理器正写入记录的文件（此文件在文件名中没有时间戳记）。

审计配置参数

以下参数在加密密钥管理器的配置文件中用来控制要记入到审计日志的事件、审计日志文件的写入位置以及审计日志文件的最大大小。

Audit.event.types

语法

Audit.event.types={*type*[;*type*]}

用途

用于指定应该发送到审计日志的审计类型。配置参数可能的值有:

全部	全部事件类型
authentication	认证事件
data_synchronization	加密密钥管理器服务器之间进行信息同步期间所发生的事件
runtime	部分处理操作和请求被发送到加密密钥管理器时所发生的事件
configuration_management	对配置进行更改时所发生的事件
resource_management	对加密密钥管理器中的资源（磁带机）设置进行更改时所发生的事件

示例

此配置值的一个示范为:

```
Audit.event.types=all
```

另一示例为:

```
Audit.event.types=authentication;runtime;resource_management
```

Audit.event.outcome

语法

Audit.event.outcome={*outcome*[;*outcome*]}

用途

用于指示事件的发生是由于操作成功或操作失败还是两者都应该审查。将由于操作成功而发生的要记入日志的事件指定为 **success**。将由于操作失败而发生的要记入日志的事件指定为 **failure**。

示例

此配置值的一个示范为:

```
Audit.event.outcome=failure
```

要启用成功和失败两个事例:

```
Audit.event.outcome=success;failure
```

Audit.eventQueue.max

语法

Audit.eventQueue.max=*number_events*

用途

用于设置存储器队列中能保存的事件对象的最大数目。此参数是可选的但建议您对其进行设置。缺省值是零。

示例

```
Audit.eventQueue.max=8
```

Audit.handler.file.directory

语法

Audit.handler.file.directory=*directoryName*

用途

此参数用于指示审计记录文件应该写到哪个目录下。请注意: 如果目录不存在，加密密钥管理器将尝试创建目录。但是，如果未成功创建目录，加密密钥管理器将不会启动。建议在运行加密密钥管理器之前先创建目录。还请注意: 运行加密密钥管理器时使用的用户标识必须对指定的目录拥有写访问权。

示例

将目录设置到 **/var/ekm/ekm1/audit**:

```
Audit.handler.file.directory=/var/ekm/ekm1/audit
```

Audit.handler.file.size

语法

Audit.handler.file.size=*sizeInKiloBytes*

用途

此参数用于指示审计文件关闭后写入新的审计文件时的大小限制。请注意: 最后的审计文件可能会超出此值几个字节，因为文件是在已超出此大小限制后才关闭的。

示例

要将最大文件大小设置为大约 2 兆字节，请输入:

```
Audit.handler.file.size=2000
```

Audit.handler.file.name

语法

Audit.handler.file.name=*fileName*

用途

使用此参数来指定基本文件名，在指定的审计目录中此文件名用作创建审计日志文件时的基本名称。请注意，此参数必须仅包含基本文件名，不能包含全限定路径名。审计日志文件的全名将附加有与文件写入的时间相对应的值。

为了说明这一点，我们假定在一个示例中 Audit.handler.file.name 的值被设置为 **ekm.log**。那么文件的全名应该是像这样的: ekm.log.2315003554。附加的字符串可用于 帮助确定审计日志文件的创建顺序 - 数字值越高，说明审计日志文件越是新近创建的。

示例

将基本名称设置为 **ekm.log** 的例子是:

```
Audit.handler.file.name=ekm.log
```

Audit.handler.file.multithreads

语法

Audit.handler.file.multithreads={**yes**|**true**|**no**|**false**}

用途

若参数指定为 **true**，那么单独的线程将用于把事件数据写入到审计日志，而允许当前执行的（操作）线程继续工作，不用等待写入审计日志完成。缺省行为是使用多个线程。

示例

将基本名称设置为 **true** 的例子是:

```
Audit.handler.file.multithreads=true
```

Audit.handler.file.threadlifespan

语法

Audit.handler.file.threadlifespan=*timeInSeconds*

用途

此参数用于指定为写入审计日志条目，期望线程具有的最长时间。此值在整理进程期间使用，使线程能够在中断之前完成工作。如果后台线程在由 threadlifespan 参数指定的时间内还没有完成其工作，那么在整理进程时，线程将被中断。

示例

要将写入审计日志的线程的期望时间设置为 10 秒，指定:

```
Audit.handler.file.threadlifespan=10
```

审计记录格式

所有的审计记录都使用此处所描述的相似的输出格式。所有的审计记录都包含一些公共信息包括时间戳记和记录类型以及特定于发生的审计事件的信息。此处显示了审计记录的一般格式:

```
AuditRecordType:[
  timestamp=timestamp
  Attribute Name=Attribute Value
  ...
  ]
```

每个记录都横跨了文件中的多行，记录的第一行以审计记录类型的第一个字符开始，后面接着的是冒号（: ）和开始的左括号（[）。与相同审计记录关联的后续行则缩排两（2）个空格以帮助您阅读日志记录。单一审计记录的最后一行包含了缩排两（2）个空格的结束右括号。每个审计记录的行数根据审计记录类型和审计记录提供的其他属性信息而有所不同。

审计记录的时间戳记基于在加密密钥管理器上运行的系统的时钟。如果这些记录根据时间戳记要与其他系统上发生的事件相关联，那么应该使用某类时间同步来确保环境中各种系统的时钟同步达到可接受的精确水平。

加密密钥管理器中的审计要点

根据配置，加密密钥管理器可以为处理请求期间发生的许多事件写审计记录。 这本节中，可审计的一组事件连同审计记录配置类别一起描述。要将这些审计记录写入到审计文件，必须启用审计记录配置类别。(请参阅表 7-1)。

表 7-1. 加密密钥管理器写入审计文件的审计记录类型

审计记录类型	审计类型	描述
认证	authentication	用于记录认证事件

表 7-1. 加密密钥管理器写入审计文件的审计记录类型 (续)

审计记录类型	审计类型	描述
数据同步	data_synchronization	用于记录数据同步处理
运行时	runtime	用于记录在处理请求时加密密钥管理器服务器中发生的各种重要处理事件
资源管理	resource_management	用于记录将资源配置到加密密钥管理器时进行的更改
配置管理	configuration_management	用于记录对加密密钥管理器服务器的配置所进行的更改

审计记录属性

以下列表说明了每种审计记录类型的可用属性。

认证事件

这些记录的格式是:

```
Authentication event:[
  timestamp=timestamp
  event source=source
  outcome=outcome
  event type=SECURITY_AUTHN
  message=message
  authentication type=type
  users=users
  ]
```

请注意: message 值仅在其信息可用时才显示。

数据同步事件

这些记录的格式是:

```
数据同步事件:
  timestamp=timestamp
  event source=source
  outcome=outcome
  event type=SECURITY_DATA_SYNC
  message=message
  action=action
  resource=resource
  user=user
  ]
```

请注意 message 和 user 值仅在其信息可用时才显示。

运行时事件

这些记录的格式是:

```
运行时事件:
  timestamp=timestamp
  event source=source
  outcome=outcome
  event type=SECURITY_RUNTIME
  message=message
```

```
  resource=resource
  action=action
  user=user
  ]
```

请注意 message 和 user 值仅在其信息可用时才显示。

资源管理事件

这些记录的格式是:

```
资源管理事件:
  timestamp=timestamp
  event source=source
  outcome=outcome
  event type=SECURITY_MGMT_RESOURCE
  message=message
  action=action
  user=user
  resource=resource
  ]
```

请注意: message 值仅在其信息可用时才显示。

配置管理事件

这些记录的格式是:

```
配置管理事件:
  timestamp=timestamp
  event source=source
  outcome=outcome
  event type=SECURITY_MGMT_CONFIG
  message=message
  action=action
  command type=type
  user=user
  ]
```

请注意: message 值仅在其信息可用时才显示。

审计事件

表 7-2 描述了导致创建审计记录的事件。该表列举了此事件发生时被记入日志的审计记录类型。

表 7-2. 依照审计事件的审计记录类型

审计事件	审计记录类型
用户认证成功	authentication
用户认证失败	authentication
数据成功发送至其他 EKM	data_synchronization
将数据发送至 EKM 时出错	data_synchronization
同步命令处理	data_synchronization
处理同步命令时出错	data_synchronization
已启动命令行处理	runtime
已接收退出命令	runtime
输入了未知命令	runtime

表 7-2. 依照审计事件的审计记录类型 (续)

审计事件	审计记录类型
从磁带机接收到消息	runtime
处理来自磁带机的消息时出错	runtime
从磁带机接收的消息出错	runtime
使用从磁带机接收到的信息更新磁带机表格时出错	runtime
检索磁带机表格的信息时出错	runtime
检索密钥库的信息时出错	runtime
处理密钥库的证书时出错	runtime
查找密钥库的专用密钥时出错	runtime
计算密码值时出错	runtime
已成功处理消息交换	runtime
已启动消息处理	runtime
已启动命令行处理	runtime
使用密码服务时发现问题	runtime
发现新的磁带机	runtime
将磁带机配置到磁带机表格时出错	runtime
已成功开始处理磁带机的消息	runtime
已接收并处理 stopekm 命令	runtime
从磁带机表格中除去磁带机	resource_management
从磁带机表格中除去磁带机时出错	resource_management
成功导入磁带机表格	resource_management
导入磁带机表格时出错	resource_management
成功导出磁带机表格	resource_management
成功导出磁带机表格	resource_management
listcerts 命令成功	resource_management
成功将磁带机添加到磁带机表格	resource_management
将磁带机添加到磁带机表格时出错	resource_management
listdrives 命令成功	resource_management
处理 listdrives 命令时出错	resource_management
成功修改磁带机表格	resource_management
修改磁带机表格时出错	resource_management
成功打开密钥库	resource_management
打开密钥库时出错	resource_management
配置属性已更改	configuration_management
更改配置属性时出错	configuration_management
配置属性已删除	configuration_management
删除配置删除时出错	configuration_management
成功导入配置	configuration_management
导入配置时出错	configuration_management
成功导出配置	configuration_management

表 7-2. 依照审计事件的审计记录类型 (续)

审计事件	审计记录类型
导出配置时出错	configuration_management
listconfig 命令成功	configuration_management

第 8 章 使用元数据

必须对加密密钥管理器进行配置，才能创建用于在数据被加密和写到磁带时捕获重要信息的 XML 文件。该文件可通过卷系列号进行查询，以显示用于卷的别名或密钥标签。相反地，该文件也可以通过别名进行查询，以显示与密钥标签/别名关联的所有卷。

注: 如果您未配置元数据文件，加密密钥管理器将无法启动。

执行加密处理时，加密密钥管理器将收集以下数据:

- 磁带机序列号
- 磁带机全球名称
- 创建日期
- 密钥别名 1
- 密钥别名 2
- DKi
- 卷系列号

收集的数据达到一定限制时，将被写到 XML 文件。可在加密密钥管理器属性文件（KeyManagerConfig.properties）中进行设置的缺省限制值为 100 条记录。文件被写后，只要加密密钥管理器处于运行状态，就可以被查询。为了防止文件变得过大，将在达到最大文件大小后，自动转存到另一个新文件中。转存的缺省最大文件大小为 1 MB，它也可以在加密密钥管理器属性文件中进行设置。只保存当前和一个以前的文件版本。在加密密钥管理器配置属性文件中设置的值为:

Audit.metadata.file.name
保存元数据的 XML 文件的名称。它为必需项。

Audit.metadata.file.size
从当前版本文件转存到以前版本文件之前的最大文件大小，用千字节表示。它为可选项。缺省值为 1024（1MB）。

Audit.metadata.file.cachecount
写元数据文件之前被缓存记录的数量。它为可选项。缺省值为 100。

XML 文件格式

该文件含有以下格式的记录。

```
<KeyUsageEvent>
 <DriveSSN>FVTDRIVE0000</driveSSN>          - 磁带机序列号
 <VolSer>TESTER</volSer>                    - 卷序列号
 <DriveWWN>57574E414D453030</driveWWN>      - 磁带机全球通用名称
 <keyAlias2>cert2</keyAlias2>               - 密钥别名 1
 <keyAlias1>cert1</keyAlias1>               - 密钥别名 2
 <dateTime>Tue Feb 20 09:18:07 CST 2007</dateTime>   - 创建日期
</KeyUsageEvent>
```

注意: 对于 LTO 4 和 LTO 5 磁带机，将只有 <keyAlias1></keyAlias1> 记录以及将记录 DKi。

查询元数据 XML 文件

使用 EKMDataParser 工具来查询元数据文件。该工具将使用文档对象模型（DOM）方法对 XML 文件进行语法分析，并且无法通过加密密钥管理器命令行界面运行。它按照以下方式进行调用:

java com.ibm.keymanager.tools.EKMDataParser -filename *full_path_to_metadata_file* {**-volser** *volser* | **-keyalias** *alias*}

metadata_path
该目录路径与为 **KeyManagerConfig.properties** 文件 Audit.metadata.file.name 中的元数据文件指定的目录路径相同。

-filename
filename 是必需项，并且必须是 XML 元数据文件的名称。该名称通常与 **KeyManagerConfig.properties** 文件 Audit.metadata.file.name 属性中指定的名称相匹配。

-volser
XML 文件中您搜索的盒式磁带的卷系列号。必须指定 **-volser** 和 **-keyalias** 两者的其中之一。

-keyalias
XML 文件中您搜索的别名的密钥标签。必须指定 **-volser** 和 **-keyalias** 两者的其中之一。

示例

假定 **KeyManagerConfig.properties** 中的元数据文件名属性（Audit.metadata.file.name）被设置为 metadata，并且该文件位于运行加密密钥管理器的本地目录中，那么以下命令将只过滤出（显示）与卷系列号 72448 相关的 XML 记录:

```
<jvm_path>/bin/java com.ibm.keymanager.tools.EKMDataParser -filename metadata -volser 72448
```

输出的格式如下:

表 8-1. 元数据查询输出格式

keyalias1	keyalias2	volSer	dateTime	driveSSN	dki
cert1	cert2	72448	Wed Mar 14 10:31:32 CDT 2007	FVTDRIVE0004	

从损坏的元数据文件恢复

如果加密密钥管理器关闭方式不正确或运行加密密钥管理器的系统崩溃，加密密钥管理器元数据文件可能损坏。对元数据文件的不当编辑或修改也有可能致使文件损坏。EKMDataParser 解析元数据文件之前，损坏难以察觉。EKMDataParser 可能失败，并生成类似如下的错误:

```
[Fatal Error] EKMData.xml:290:16: The end-tag for element type "KeyUsageEvent" must
 end with a '>' delimiter.
org.xml.sax.SAXParseException: The end-tag for element type "KeyUsageEvent" must
 end with a '>' delimiter.
at org.apache.xerces.parsers.DOMParser.parse(Unknown Source)
at org.apache.xerces.jaxp.DocumentBuilderImpl.parse(Unknown Source)
```

```
at javax.xml.parsers.DocumentBuilder.parse(Unknown Source)
at com.ibm.keymanager.tools.EKMDataParser.a(EKMDataParser.java:136)
at com.ibm.keymanager.tools.EKMDataParser.a(EKMDataParser.java:26)
at com.ibm.keymanager.tools.EKMDataParser.main(EKMDataParser.java:93)
```

如果此错误发生，那么是由于某个元素缺少 XML 结束标记。可以恢复加密密钥管理器元数据文件，以便 EKMDataParser 再次解析该文件。

1. 创建加密密钥管理器元数据文件的备份副本。
2. 编辑该加密密钥管理器元数据文件。
3. 在 XML 中，每个数据或事件段应该有一个初始标记和一个相应的结束标记。
   - 下面是一个初始标记的一些示例:
     - <KeyUsageEvent>
     - <driveSSN>
     - <keyAlias1>
   - 下面是一个结束标记的一些示例:
     - </KeyUsageEvent>
     - </driveSSN>
     - </keyAlias1>
4. 扫描文件并查找不匹配的标记。来自 EKMDataParser 的错误消息列出哪个标记缺少结束标记。这样搜索就轻松得多。
5. 找到不匹配的标记时，将临时删除事件或添加必要的标记以完成事件。
   - 例如，来自一个加密密钥管理器元数据文件的以下摘录显示了没有结束标记的第一个 KeyUsageEvent:

     ```
     <KeyUsageEvent>
     <driveSSN>001310000109</driveSSN>
     <volSer>      </volSer>
     <driveWWN>5005076312418B07</driveWWN>
     <keyAlias1>key0000000000000000F</keyAlias1>
     <dki>6B65790000000000000000F</dki>
     <dateTime>Thu Aug 30 09:50:53 MDT 2007</dateTime>
     <KeyUsageEvent>
     <driveSSN>001310000100</driveSSN>
     <volSer>      </volSer>
     <driveWWN>5005076312418ABB</driveWWN>
     <keyAlias1>key00000000000000000</keyAlias1>
     <dki>6B6579000000000000000000</dki>
     <dateTime>Thu Sep 06 16:49:39 MDT 2007</dateTime>
     </KeyUsageEvent>
     ```

     在行 <dateTime>Thu Aug 30 09:50:53 MDT 2007</dateTime> 和 <KeyUsageEvent> 之间添加一个 </KeyUsageEvent> 将完成第一个 <KeyUsageEvent>。

修复文件损坏将使 EKMDataParser 可以成功解析数据。

附录 A. 文件示例

启动守护程序脚本样本

警告: 不能夸张地描述保留密钥库数据的重要性。如果没有对密钥库的访问权，那么将不能够对已加密磁带解密。请确保保存密钥库和密码信息。

Linux 平台

以下是使您能够以允许的方式去掉后台中的 EKM 的样本脚本。该脚本启动 EKM，并通过脚本传入密钥库密码 *keystore_password*。通过这种方法，密钥库密码就无需出现在 EKM 配置中。（请参阅下面的说明）。以下内容应包含在脚本文件中:

```
java com.ibm.keymanager.KMSAdminCmd KeyManagerConfig.properties <<EOF
startekm
keystore_password
status
EOF
```

注: 如果通过脚本将密钥库密码输入到 EKM 中（即 EKM 配置文件不包含密钥库密码），那么在备份 EKM 时，无需将这些文件（配置文件、磁带机表格和密钥库备份文件）视为机密文件，但是**必须**安全而且可复原地存储包含密钥库密码的脚本（例如，在多个位置存放多个副本）。密钥库密码是机密信息，而且必须以此方法进行处理。安全地备份脚本文件时的选项与备份包含密钥库密码的配置文件的选项相同。但是可从 EKM 备份文件秘密、单独地备份并存储/传输脚本，那么将会增加安全性的间接级别。最后，必须强调，虽然存储了密钥库密码（存储在脚本或 EKM 的配置文件中），还必须对其进行安全、可复原的存储，这样始终都可以恢复密钥库密码。**丢失所有密钥库密码副本将导致丢失密钥库中的所有密钥，而且没有途径可进行恢复。**.

配置文件示例

以下是 EKM 属性文件的示例，它具有指向同一软件密钥库的所有密钥库条目:

```
Admin.ssl.keystore.name = /keymanager/testkeys
Admin.ssl.keystore.type = jceks
Admin.ssl.truststore.name = /keymanager/testkeys
Admin.ssl.truststore.type = jceks
Audit.event.outcome = success,failure
Audit.event.types = all
Audit.eventQueue.max = 0
Audit.handler.file.directory = /keymanager/audit
Audit.handler.file.name = kms_audit.log
Audit.handler.file.size = 10000
Audit.metadata.file.name = /keymanager/metafile.xml
config.drivetable.file.url = FILE:///keymanager/drivetable
config.keystore.file = /keymanager/testkeys
config.keystore.provider = IBMJCE
config.keystore.type = jceks
fips = Off
TransportListener.ssl.ciphersuites = JSSE_ALL
```

```
TransportListener.ssl.clientauthentication = 0
TransportListener.ssl.keystore.name = /keymanager/testkeys
TransportListener.ssl.keystore.type = jceks
TransportListener.ssl.port = 443
TransportListener.ssl.protocols = SSL_TLS
TransportListener.ssl.truststore.name = /keymanager/testkeys
TransportListener.ssl.truststore.type = jceks
TransportListener.tcp.port = 3801
```

这是 EKM 属性文件的示例，它具有指向不同密钥库的所有密钥库条目。粗体的条目与上面第一个示例属性文件不同。

```
Admin.ssl.keystore.name = /keymanager/adminkeys.jceks
Admin.ssl.keystore.type = jceks
Admin.ssl.truststore.name = /keymanager/admintrustkeys
Admin.ssl.truststore.type = jceks
Audit.event.outcome = success,failure
Audit.event.types = all
Audit.eventQueue.max = 0
Audit.handler.file.directory = /keymanager/audit
Audit.handler.file.name = kms_audit.log
Audit.handler.file.size = 10000
Audit.metadata.file.name = /keymanager/metafile.xml
config.drivetable.file.url = FILE:///keymanager/drivetable
config.keystore.file = /keymanager/drive.keys
config.keystore.provider = IBMJCE
config.keystore.type = jceks
fips = Off
TransportListener.ssl.ciphersuites = JSSE_ALL
TransportListener.ssl.clientauthentication = 0
TransportListener.ssl.keystore.name = /keymanager/sslkeys
TransportListener.ssl.keystore.type = jceks
TransportListener.ssl.port = 443
TransportListener.ssl.protocols = SSL_TLS
TransportListener.ssl.truststore.name = /keymanager/ssltrustkeys
TransportListener.ssl.truststore.type = jceks
TransportListener.tcp.port = 3801
```

附录 B. 加密密钥管理器配置属性文件

加密密钥管理器需要两个配置属性文件: 一个用于加密密钥管理器服务器，一个用于 CLI 客户机。每个文件都会被视为 Java.util.Properties 加载文件并进行语法分析，这对属性的格式和规范有一定的限制:

- 每行记录一个配置属性。给定属性的值扩展至行末。
- 含有空格的属性值（如密码）无需用引号括起来。
- 密钥库密码长度不得大于 127 个字符。
- 行末的附属空格可被解释为属性值的一部分。

可从 **http://support.dell.com** 下载的 EKMServicesandSamples 文件中获取一些样本配置属性文件。

加密密钥管理器服务器配置属性文件

以下加密密钥管理器服务器配置文件（KeyManagerConfig.properties）包含了一套完整的属性。文件中的属性设置订单无关。文件中可能出现注释。要想添加一个注释，请使用一行的第一列中的 『#』。

注: 对 KeyManagerConfig.properties 文件所做的修改可能在关闭的时候有所丢失。因此请确保在编辑配置属性前没有运行加密密钥管理器服务器。要关闭加密密钥管理器服务器，请从 CLI 客户机发出 **stopekm** 命令。当重新启动加密密钥管理器服务器时您的更改将被激活。

Admin.ssl.ciphersuites = *value*

指定用于加密密钥管理器服务器之间通信的密码套件。密码套件描述了用于数据传输的密码算法、握手协议传输层安全性（TLS）和安全套接字层（SSL）。

必需 可选。

值 可用值为任何 IBMJSSE2 支持的密码套件。

缺省值 JSSE_ALL

Admin.ssl.keystore.name = *value*

这是用于加密密钥管理器服务器间 **sync** 命令等安全套接字层客户机操作的密钥对和证书数据库名称。在一个 sync 操作中安全套接字服务器发送至安全套接字服务器的证书是来自该密钥库的。

必需 可选。仅用于 **sync** 命令。缺省设置为 **config.keystore.file** 属性的值。

Admin.ssl.keystore.password = password

访问 Admin.ssl.keystore.name 的密码

必需 可选。如果未提供的话，那么会在加密密钥管理器刚启动时跳出一个提示。指定此属性值时，属性的值将被模糊化，以提高安全性，并且属性文件的节名称本身将被替换为名为 “Admin.ssl.keystore.password.obfuscated” 的新节。

Admin.ssl.keystore.type = *value*

所使用的密钥库类型。

必需 可选。

缺省值 jceks

Admin.ssl.protocols = *value*

安全协议。

必需 可选。

值 SSL_TLS | SSL | TLS

缺省值 SSL_TLS

Admin.ssl.timeout = *value*

设定套接字在扔弃套接字时间超出异常之前等待的时间。

必需 可选。

值 请设定分钟数。0 意味着没有超时

缺省值 1

Admin.ssl.truststore.name = *value*

这是数据库文件的名称，该数据库文件用于检查服务器向安全套接字客户机提供的安全套接字服务器证书的信用。

必需 可选。仅用于 **sync** 命令。缺省设置为 **config.keystore.file** 属性的值。

Admin.ssl.truststore.type = *value*

所使用的密钥库类型。

必需 可选。

缺省值 jceks

Audit.event.outcome = *value*

仅记录指定结果中生成的审计事件

必需 是。

值 成功 | 失败。可指定两者，并需要使用逗号或分号隔开。

缺省值 成功

Audit.event.Queue.max = 0

在将审计内存队列中的事件对象清空到文件之前的最大事件对象数。

必需 可选。建议。

值 0 - ？（0 表示立即清空。）

缺省值 0

Audit.event.types = *value*

仅记录指定结果中生成的审计事件

必需 是。

值 全部 | 认证 | 权限 | 数据同步 | 运行时 | 审计管理 | 权限终止 | 配置管理 |资源管理 | 无。可指定多个值，中间以逗号或分号分隔。

缺省值 全部

Audit.handler.file.directory = ../audit

将存放 Audit.handler.file.name 的目录

必需 可选。建议。

Audit.handler.file.multithreads = *value*

指定审计处理程序是否应将单独的线程分派给进程审计记录。

必需 可选。

值 true | false

缺省值 true

Audit.handler.file.name = kms_audit.log

将记录审计条目的文件名。

必需 是。

Audit.handler.file.size = 100

Audit.Handler.file.name 在开始覆盖之前将增大到的大小

必需 可选。建议。

值 0 - ?（以千字节为单位指定。）

缺省值 100

Audit.handler.file.threadlifespan = *value*

限制审计记录处理线程的生存期。仅当 audit.handler.file.multithreads= true 时有用。

必需 可选。

值 以毫秒为单位指定。

缺省值 10000

Audit.metadata.file.cachecount = 100

指定在写入元数据文件之前要在内存中存储的记录数。

必需 否

缺省值 100

Audit.metadata.file.name = *value*

指定要保存元数据记录的 XML 文件的名称。

必需 是。

Audit.metadata.file.size = 1024

指定 XML 元数据文件在关闭文件并启动新文件之前可能达到的最大文件大小（以 KB 为单位指定）。仅保存当前版本和先前版本的文件。

必需 否

缺省值 1024

config.drivetable.file.url = FILE:../filedrive.table

包含关于磁带机的信息（例如序列号、证书等）的文件。

必需 是。

config.keygroup.xml.file = *value*

指定按密钥组存储各个别名的 XML 文件的名称。

必需 可选。

config.keystore.file = *value*

指定要使用的密钥库。

必需 是。

config.keystore.password = password

访问 config.keystore.file 的密码。在指定密码时，该属性的值对于其他安全性是比较模糊的，属性文件中的节名称本身将被命名为 “config.keystore.password.obfuscated” 的新节替换。

必需 可选。如果未提供，将在加密密钥管理器刚启动时跳出一个提示。

config.keystore.provider = IBMJCE

必需 可选。

config.keystore.type = jceks

必需 可选。建议。

缺省值 jceks

debug = *value*

启用指定加密密钥管理器组件的调试。

必需 可选。

值 全部 | 审计 | 服务器 | 可驱动 | config | admin | 传输 | 逻辑 | 密钥库 | 控制台 | 无。可采用多个由逗号隔开的值。

缺省值 无

debug.output = *value*

将调试输出路由至指定位置。

必需 可选。

值 simple_file | 控制台（不推荐）。

debug.output.file = debug

将写入调试输出的路径和文件名。

必需 可选。当 debug.output = simple_file 时是必需的。文件的路径必须存在。

drive.acceptUnknownDrives = *value*

自动将与加密密钥管理器关联的新磁带机添加到磁带机表格

必需 是。

值 true | false

缺省值 false

安全性说明 – 与有效 drive.default.alias1 设置结合使用该设置使磁带机能够连接到加密密钥管理器并可操作，而无需管理员验证添加。有关更多信息，请参阅第 3 章中的『自动更新磁带机表格』。

fips = *value*

联邦信息处理标准。有关更多信息，请参阅第 2 章的 “联邦信息处理标准 140-2 注意事项”。

必需 可选。

值 打开 | 关闭

缺省值 关闭

maximum.threads = 200

加密密钥管理器可创建的最大线程数。

必需 可选。

Server.authMechanism = *value*

指定将用于本地/远程客户机的认证机制。当值设置为 EKM 时，CLI 客户机用户必须使用 usr/passwd 作为 EKMAdmin/changeME 来登录到服务器。（可使用 chgpasswd 命令更改该密码。）当值指定为 LocalOS 时，将完成对本地操作系统注册表的客户机认证。（更改 KeyManagerConfig.properties 文件之前，请务必关闭加密密钥管理器服务器。）CLI 客户机用户必须使用 OS usr/passwd 登录到服务器。对于基于 Linux

1. 从 **http://support.dell.com** 下载 Dell Release R175158（EKMServicesAndSamples）并将文件抽取到所选的目录中。
2. 将 EKMServiceAndSamples.jar（包含在 Dell 产品介质上并可从 **http://support.dell.com** 获取）的内容导入到临时目录中。
3. 将 libjaasauth.so 文件从平台上对应的 LocalOS-setup 目录复制到 *java_home*/jre/bin。
   - 在 32 位 Intel Linux 环境中，将 LocalOS-setup/linux_ia32/libjaasauth.so 文件复制到 *java_home*/jre/bin/ 目录中，其中 *java_home* 通常为 *java_install_path*/IBMJava2-i386-142（对于运行 1.4.2 JVM 的 32 位 Intel Linux 内核）。
   - 在 64 位 AMD64 Linux 环境中，将 LocalOS-setup/linux-x86_64/libjaasauth.so 文件复制到 *java_home*/jre/bin/ 目录中，其中 *java_home* 通常为 *java_install_path*/IBMJava2-amd64-142（对于运行 1.4.2 JVM 的 64 位 AMD Linux 内核）。

对于 Windows 平台，该文件不是必需的。

安装完成之后，可以启动加密密钥管理器服务器。加密密钥管理器客户机现在可以使用基于操作系统的用户/密码登录。请注意，只有允许登录和向服务器提交命令的用户标识才是运行服务器且同时具有超级用户/root 权限的用户标识。

可从 Dell 产品介质以及加密密钥管理器 Web 站点上的 **http://support.dell.com**，以了解更多安装详细信息。

必需 可选。

值 EKM | LocalOS

缺省值 EKM

Server.password = *value*

内部属性。请勿编辑。

symmetricKeySet = {GroupID | keyAliasList [, keyAliasList,]}

指定要用于 LTO 4 和 LTO 5 磁带机的对称密钥别名和密钥组。

必需 可选。仅适用于 LTO 4 和 LTO 5 盒式磁带。

值

为 *GroupID* 指定一个值，或为 *keyAliasList* 指定一个或多个值。

GroupID 指定要构成对称密钥列表的密钥组名称，并在没有为磁带机指定别名时充当缺省名称。*GroupID* 必须与 KeyGroups.xml 文件中的现有密钥组标识匹配。如果不匹配，那么将返回 KeyManageException。如果指定了多个 *GroupID*，那么将返回 KeyManagerException。当您指定有效的 *GroupID* 时，将跟踪密钥组 XML 中使用的上一个密钥，并在每次从对称密钥组列表的 KeyGroups.xml 调用 getKey 时随机选择使用下一个密钥。*keyAliasList* 的每个规范包含 *keyAlias* 或 *keyAliasRange* 的值。

keyAlias 指定最多 12 个字符的 Backus-Naur 表单（BNF）作为密钥库中对称密钥的名称或别名，或指定刚好 21 个字符的 sequentialKeyID。

keyAliasRange 指定最多 18 个字符的 sequentialKeyID 和十六进制数字，以连字符（-）隔开。如果指定 18 个字符，那么前两个字符必须是 00。必须指定在一行上，而且不得包含 cr-lf。

GroupID 指定别名组的名称。

示例 `symmetricKeySet = KMA0238ab34,KMB0000034acd2345678a,THZ001-FF` 这指示加密密钥管理器使用别名 KMA0238ab34 和 KMB0000034acd2345678a，而且当密钥用于 LTO 4 和 LTO 5 时，别名的范围是从 THZ000000000000000001 到 THZ0000000000000000FF。这些密钥必须存在于由属性文件中的 **config.keystore.file** 指定的密钥库中。

sync.action = *value*

指定自动同步期间应对数据完成的操作。

必需 可选。

值 重新写入 | 合并

缺省值 合并

注：合并配置信息与重新写入配置信息相同。

sync.ipaddress = *ip_addr:ssl*

指定要进行自动同步的远程加密密钥管理器的 IP 地址和端口。

必需 可选。如果该属性未指定或以错误方式指定，那么将禁用同步函数。

值 远程服务器的 IP 地址：SSL 端口号

sync.timeinhours = *value*

指定对远程加密密钥管理器执行自动同步之前需要等待的小时数。

必需 可选。

值 以小时为单位指定。

缺省值 24

sync.type = *value*

指定要执行自动同步的数据。

必需 可选。

值 config | drivetab | 全部

缺省值 drivetab

TransportListener.ssl.ciphersuites = JSSE_ALL

用于在加密密钥管理器服务器之间进行通信的密码套件。密码套件描述了用于数据传输的密码算法、握手协议传输层安全性（TLS）和安全套接字层（SSL）。

必需 可选。

值 值 – IBMJSSE2 支持的所有密码套件。

TransportListener.ssl.clientauthentication = 0

在加密密钥管理器服务器之间进行通信所需要的 SSL 认证。

必需 可选。

值 0 - 无客户机认证（缺省）
1 - 服务器需要对客户机执行客户机认证
2 - 服务器必须对客户机执行客户机认证

TransportListener.ssl.keystore.name = *value*

加密密钥管理器服务器用于保存安全套接字服务器的证书和专用密钥的数据库名称。该证书提供给安全套接字客户机以进行认证和信用检查。加密密钥管理器客户机还使用该密钥库与加密密钥管理器服务器对话，并充当安全套接字客户机。

必需 是。

TransportListener.ssl.keystore.password = password

访问 TransportListener.ssl.keystore.name 的密码。指定此属性值时，属性的值将被模糊化，以提高安全性，并且属性文件的节名称本身将被替换为名为 “TransportListener.ssl.keystore.password.obfuscated” 的新节。

必需 可选。

TransportListener.ssl.keystore.type = jceks

必需 可选。建议。

值 JCEKS

TransportListener.ssl.port = *value*

加密密钥管理器服务器将在上面侦听来自其他加密密钥管理器服务器或加密密钥管理器 CLI 客户机的请求的端口。

必需 是。

值 端口号，例如 443。这必须与 CLI 客户机配置属性文件中的 TransportListener.ssl.port 属性匹配。

TransportListener.ssl.protocols = SSL_TLS

安全协议

必需 可选。

值 SSL_TLS（缺省值）| SSL | TLS

TransportListener.ssl.timeout = 10

指定在丢弃 SocketTimeoutException 之前套接字等到 read() 的时间。

必需 可选。

值 请设定分钟数。

缺省值 1

TransportListener.ssl.truststore.name = *value*

用于验证其他客户机和服务器的公用密钥和签名证书的数据库的名称。如果 TransportListener.ssl.clientauthentication 属性**未**设置为缺省值 0（无客户机认证），那么充当安全套接字服务器的加密密钥管理器服务器必须使用此文件认证客户机。加密密钥管理器客户机还使用该信任密钥库与加密密钥管理器服务器对话，并充当安全套接字客户机。

必需 是。

TransportListener.ssl.truststore.type = jceks

必需 可选。建议。

值 JCEKS

TransportListener.tcp.port = *value*

加密密钥管理器服务器将在上面侦听来自磁带机的请求的端口。缺省 TCP 端口号为 3801。

必需 是。

值 端口号，例如 10。

TransportListener.tcp.timeout = *value*

指定在丢弃 SocketTimeoutException 之前套接字等到 read() 的时间。

必需 可选。

值 以分钟为单位指定。0 表示无超时。

缺省值 10

CLI 客户机配置属性文件

该文件（ClientKeyManagerConfig.properties）包含了 KeyManagerConfig.properties 文件中的属性的子集。该子集包含以下属性。

TransportListener.ssl.ciphersuites = JSSE_ALL

用于在加密密钥管理器服务器与 CLI 客户机之间通信的密码套件。密码套件描述了用于数据传输的密码算法、握手协议传输层安全性（TLS）和安全套接字层（SSL）。

必需 可选。

值 该值必须与为加密密钥管理器服务器属性文件

（KeyManagerConfig.properties）中的 TransportListener.ssl.ciphersuites 指定的值相匹配。

TransportListener.ssl.host = *value*

确定加密密钥管理器 CLI 客户机的加密密钥管理器服务器。

必需 可选。

值 IP 地址或主机名

缺省值 本地主机

示例
```
TransportListener.ssl.host = 9.24.136.444
TransportListener.ssl.host = ekmsvr02
```

注: 不在 KeyManagerConfig.properties 文件中使用。

TransportListener.ssl.keystore.name = *value*

加密密钥管理器客户机还使用该密钥库与加密密钥管理器服务器对话，并充当安全套接字客户机。

必需 是。

TransportListener.ssl.keystore.type = jceks

密钥库的类型。

必需 可选。建议。

缺省值 jceks

TransportListener.ssl.port = *value*

这是 CLI 客户机将用于与加密密钥管理器服务器通信的端口。

必需 是。

值 该值必须与为加密密钥管理器服务器属性文件（KeyManagerConfig.properties）中的 TransportListener.ssl.port 指定的值相匹配。

TransportListener.ssl.protocols = SSL_TLS

安全协议

必需 可选。

值 该值必须与为加密密钥管理器服务器属性文件（KeyManagerConfig.properties）中的 TransportListener.ssl.protocols 指定的值相匹配。

TransportListener.ssl.truststore.name = *value*

用于验证其他客户机和服务器的公用密钥和签名证书的数据库的名称。

必需 是。

TransportListener.ssl.truststore.type = jceks

信任密钥库的类型。

必需 可选。建议。

缺省值 jceks

可从 **http://support.dell.com** 上的 EKMServicesAndSamples 文件中下载样本配置属性文件。

附录 C. 常见问题解答

是否可以组合使用基于应用程序的密钥管理和系统管理的加密或库管理的加密?

不能。当使用应用程序管理的加密时，加密在库层上是透明的。同样，当使用库管理的加密时，此过程在其他层上是透明的。加密管理方法之间是互斥的。对于 库管理的加密，无需更改应用程序。

必须在每个可能生成磁带加密或解密请求的系统上安装和运行加密密钥管理器吗?

通过库管理的加密，生成磁带机写入请求的系统无需是运行加密密钥管理器的系统。此外，加密密钥管理器的实例无需在访问加密磁带机的每个系统上运行。

如果我包含了“drive.acceptUnknownDrives = True”参数，是否仍需要在配置文件中包含“config.drivetable.file.url = FILE:/filename”参数?

必须始终指定 **config.drivetable.file.url**。这是磁带机信息所在的位置。如果设置 `drive.acceptUnknownDrives = True`，那么也可指定 `drive.default.alias1` 和 `drive.default.alias2` 变量来更正证书别名/密钥标签。

FILE:/filename 是 `config.drivetable.file.url` 属性的正确语法吗? FILE:/// filename 出现在样本文件中，而 FILE:../ 出现在描述中。

示例是正确的。这是 URL 规范，而不是所需的目录结构规范。

当在 KeyManagerConfig.properties 文件中为 Windows 上运行的加密密钥管理器指定标准路径时，我必须使用正斜杠还是反斜杠?

因为 KeyManagerConfig.properties 是 Java 属性文件，所以只能识别路径名中的正斜杠，即使在 Windows 中也是如此。如果在 KeyManagerConfig.properties 文件中使用反斜杠，那么将发生错误。

加密密钥管理器是否要执行任何证书撤回列表（CRL）检查?

不，加密密钥管理器不执行任何 CRL 检查。

当用于对磁带加密的证书过期时会出现什么情况? 加密密钥管理器将读取先前加密的磁带吗?

证书是否过期不会对加密密钥管理器产生什么影响。它将继续认可这些证书并读取先前加密的磁带。但是，过期的证书必须保留在密钥库中，这样才能读取或附加先前加密的磁带。

加密密钥管理器将需要对证书重命名或更新证书吗?

缺省情况下，加密密钥管理器配置为使用过期证书认可新的密钥请求。如果以这种方式配置加密密钥管理器，那么无需更新证书。如果禁用此功能，但必须继续对新密钥请求使用这个专用密钥/证书对，那么用户必须更新证书。将仅更新证书（有效日期）而不更新相关联的密钥。

以后版本的加密密钥管理器仍可以读取使用较早版本软件创建的加密磁带吗?

是。加密密钥管理器将认可证书，而不考虑发行版。

声明

商标

本文中使用的商标: Dell、Dell 徽标和 PowerVault 均是属于 Dell Inc. 的商标。Microsoft 和 Windows 是 Microsoft Corporation 的注册商标。在本文档中可能还使用了其他商标和商品名称来指声明拥有该标记与名称的实体或其产品。Dell Inc. 放弃非本公司的商标和商品名称的专有利益。

词汇表

本词汇表定义了本出版物和其他相关出版物中使用的特殊术语、缩写和首字母缩写词。

〔B〕

别名（alias）： 请参阅密钥标签（key label）。

〔G〕

公用密钥（public key）： 非对称密钥对中的某个密钥，通常用于加密。加密密钥管理器在将 AES 数据密钥存储到盒式磁带之前使用公用密钥来打包（保护）这些密钥。

〔J〕

加密（encryption）： 从数据到密码的转换。需要密钥来对数据进行加密和解密。加密可防止人员或软件在没有密钥的情况下尝试访问数据。

〔M〕

密钥标签: 用于将 EEDK 与打开受保护对称数据密钥所需的专用密钥（KEK）匹配的唯一标识。根据所使用的密钥库，也称为别名或证书标签。

密钥二次加密（rekey）： 更改非对称加密密钥（保护已加密磁带上存储的数据密钥（DK））的过程，这使不同实体可访问数据。

密钥环（key ring）： 请参阅密钥库（keystore）。

密钥库（keystore）： 用于认证相应公用密钥的专用密钥及其相关联 X.509 数字证书链的数据库。在某些环境中也称为证书库或密钥环。

〔Z〕

证书级别（certificate label）： 请参阅密钥标签（key label）。

证书库（certificate store）： 请参阅密钥库（keystore）。

证书（certificate）： 将公用密钥绑定到证书所有者身份的数字文档，因此能启用对证书所有者的认证。

专用密钥（private key）： 非对称密钥对中的某个密钥，通常用于解密。加密密钥管理器在解密之前使用专用密钥打开受保护的 AES 数据密钥。

A

AES: 高级加密标准。美国政府采用作为加密标准的分组密码。

D

DK: 数据密钥。用于加密数据的字母数字字符串。

E

EEDK: 外部加密数据密钥。在存储到数据盒带中之前已由密钥加密密钥加密（打包）的数据密钥。请参阅 KEK。

K

KEK: 密钥加密密钥。用于加密数据密钥的字母数字、非对称密钥。请参阅 EEDK。

P

PKDS: 公用密钥数据集。也称为 PKA 密钥数据集。

R

RSA: Rivest-Shamir-Adleman 算法。用于加密和认证的非对称、公用密钥密码术的系统。它是 Ron Rivest、Adi Shamir 和 Leonard Adleman 在 1977 年发明的。系统的安全性取决于生产两种大量产品的难易程度。

索引

[A]

安装和配置 4-1
安装（install）Linux（Intel） 3-1

[B]

必备（软件）
  硬件和软件 2-2
  Linux 2-2
  Windows 2-3

[C]

出版物
  联机（online） x
  相关 x
  Linux x
  Windows x
创建密钥库
  加密密钥管理器 GUI 3-5
词汇表 E-1
磁盘驱动器，受支持 2-2
错误（errors）
  加密密钥管理器报告的（reported） 6-5

[D]

调试 B-4

[F]

服务器（server）
  配置（configurations） 2-7
  与其他服务器同步 4-2

[G]

更改密钥库秘密（changing keystore passwords） 3-11
共享磁带 2-9
管理 5-1
规划 2-1
规划注意事项
  加密 2-1
  库管理 2-1

[J]

加密
  对称加密 1-5
  非对称加密 1-5
  公用密钥 1-5
  规划 2-1
  库管理 1-5
  密钥 1-5
  密钥包装 1-5
  密钥加密密钥 1-5
  数据密钥 1-5
  算法 1-5
  外部加密数据密钥 1-5
  应用程序管理 1-4
  专用密钥 1-5
加密密钥管理器
  规划 2-1
加密密钥管理器报告的错误（reported error） 6-5
加密（encryption）
  加密密钥管理器报告的错误（reported error） 6-5
解决问题
  加密（with encryption） 6-5

[K]

库管理磁带加密 1-5

[M]

密钥管理器
  组件 1-1
密钥库密码（keystore passwords） 3-11
密钥组
  创建 3-13
密钥（keys）
  在 LTO 上对称 3-9
命令行界面 5-7
  启动 5-5

[P]

配置
  单服务器 2-7
  两个服务器 2-7
配置加密密钥管理器
  加密密钥管理器属性设置 B-1
配置属性
  服务器 B-1
  客户机 B-8
配置（configure）
  密钥管理器 4-3

[Q]

启动
  命令行界面 5-5
启动和关闭
  服务器（server） 5-1

[R]

软件开发人员工具包（software developer kit）
  安装（install）Linux（Intel） 3-1
  安装（install）Windows 3-2
软件需求 2-2

[S]

商标 D-1
审计 7-1
  参数 7-1
    Audit.eventQueue.max 7-2
    Audit.event.outcome 7-2
    Audit.event.types 7-1
    Audit.handler.file.directory 7-2
    Audit.handler.file.multithreads 7-3
    Audit.handler.file.name 7-3
    Audit.handler.file.size 7-3
    Audit.handler.file.threadlifespan 7-4
  概述 7-1
  记录格式 7-4
  事件 7-6
  属性 7-5
  要点 7-4
声明 D-1
识别主机 IP 地址 3-8
识别 SSL 端口 3-8
属性设置 B-1
  编辑 3-9
术语 E-1

[T]

同步服务器 4-2

[W]

问题确定 6-1
  要检查的文件 6-1
问题，确定和解决（problems, determining and resolving）
  加密（with encryption） 6-5

[X]

消息
  必须在 config 文件中指定 SSL 端口号 6-12
  必须在 config 文件中指定 TCP 端口号 6-12
  不受支持的操作 6-14
  未使任何数据实现同步 6-10
  未指定配置文件 6-8
  无法装入传输密钥库 6-14
  无法装入密钥库 6-14
  无法装入 admin 密钥库 6-13
  指定的审计日志文件仅可读 6-13
  sync 失败 6-13
消息（messages） 6-7
  服务器未能启动（Server failed to start） 6-12
  配置文件中 SSL 端口号无效（Invalid SSL port number in config file） 6-11
  配置文件中 TCP 端口号无效（Invalid TCP port number in config file） 6-11
  输出无效（invalid input） 6-11
  未能导入（Failed to import） 6-9
  未能归档日志文件（failed to archive the log file） 6-8
  未能删除磁带机条目（Failed to delete the drive entry） 6-9
  未能删除配置（Failed to delete the configuration） 6-8
  未能添加磁带机（Failed to add drive） 6-8
  未能修改配置（Failed to modify the configuration） 6-9
  文件大小限值不能是负数（File size limit cannot be a negative number） 6-10
  文件名不能为空（File name cannot be null） 6-10
需求
  硬件和软件 2-2

[Y]

应用程序管理的加密 1-4
硬件需求 2-2
元数据（metadata） 8-1

[Z]

灾难恢复站点
  规划 2-8
主机 IP 地址
  识别 3-8
专用/公用密钥 2-9

A

Audit.eventQueue.max 7-2
Audit.event.outcome 7-2
Audit.event.types 7-1
Audit.handler.file.directory 7-2
Audit.handler.file.multithreads 7-3
Audit.handler.file.name 7-3
Audit.handler.file.size 7-3
Audit.handler.file.threadlifespan 7-4

C

CLI
  调试 6-2
  启动 5-5
ClientKeyManagerConfig.properties B-8
  编辑 3-9

F

FIPS 140-2 2-9

J

JCEKS 2-3

K

KeyManagerConfig.properties B-1
  编辑 3-9

L

Linux
  必备（软件） 2-2
LTO 3-9
  密钥和别名（keys and aliases） 3-9

S

SSL 端口
  识别 3-8

W

Windows
  必备（软件） 2-3

X

XML 元数据文件（XML metadata file） 8-1