安装和配置

IBM

目录

环境概述

IBM Security Key Lifecycle Manager 以解决方案的形式提供了简化的密钥生命周期管理功能，易于安装、部署和管理。

此文档重点描述安装和配置 IBM Security Key Lifecycle Manager 时必须完成的任务。

功能概述

使用 IBM Security Key Lifecycle Manager 来管理密钥的生命周期和企业的证书。可以管理对称密钥、密钥、非对称密钥对和证书。

IBM Security Key Lifecycle Manager 具有以下关键功能部件:

- 基于角色的访问控制，它为特定的设备组提供执行创建、修改和删除等任务的许可权。大多数许可权与特定的设备组相关联。
- 通过使用行业标准的密钥管理互操作性协议 (KMIP) 将存储数据加密并进行对应的密钥管理，扩展对设备的支持。

  您可以使用 IBM Security Key Lifecycle Manager 图形用户界面来创建、配置和搜索加密对象。这些对象用于向符合 KMIP 标准的客户机设备提供加密密钥。
- 为 DS5000 存储服务器提供对称密钥

  对提供给 DS5000 存储服务器的密钥进行管理和不间断维护。限制设备（如磁盘驱动器）可与其相关联的机器集。您可以将设备与 IBM Security Key Lifecycle Manager 数据库中的现有机器相关联。
- IBM Security Key Lifecycle Manager 服务器连接至的一个或多个设备的加密密钥。
- 为您生成的自签名证书、专用密钥和数据库中的密钥元数据存储密钥材料。
- 跨平台备份和复原，用于保护关键数据和其他 IBM Security Key Lifecycle Manager 数据，如配置文件和当前数据库信息。
- 跨平台备份实用程序，用于在 IBM Security Key Lifecycle Manager 先前版本 V1.0、V2.0、V2.0.1、V2.5 以及 IBM Encryption Key Manager V2.1 上运行备份操作。您可以跨操作系统在 IBM Security Key Lifecycle Manager 的当前版本上复原这些备份文件。
- 在安装期间迁移 IBM Security Key Lifecycle Manager 先前版本 V1.0,、V2.0、V2.0.1、V2.5 以及 IBM Encryption Key Manager V2.1 组件。
- 基于所选事件（由于成功操作和/或不成功操作而发生）的审计记录。安装或启动 IBM Security Key Lifecycle Manager 会将构建级别写入审计日志中。
- 支持启用了加密的 3592 磁带机、LTO 磁带机、DS5000 存储服务器、DS8000 Turbo 磁带机 以及其他设备。
- 支持使用硬件安全模块 (HSM) 来存储用于保护存储在数据库中的所有密码和密钥的主密钥。
- 一组用于跨操作系统自动复制当前活动文件和数据的操作。此复制支持以独立于服务器的操作系统和目录结构的方式克隆多个服务器上的 IBM Security Key Lifecycle Manager 环境。

- 支持使用 LDAP（轻量级目录访问协议）服务器进行用户认证。您可以配置任何 LDAP 存储库（如 IBM Security Directory Server 或 Microsoft Active Directory）中的 IBM Security Key Lifecycle Manager 用户。
- 服务器配置向导，用于配置 IBM Security Key Lifecycle Manager 以进行 SSL/TLS 握手。通过 SSL 握手，服务器和客户机设备可以建立用于安全通信的连接。

部署

IBM Security Key Lifecycle Manager 部署由一个安装过程构成，该过程会收集信息以用于数据库准备、用户标识配置以及从 Encryption Key Manager 迁移数据（可选）。

Windows 以及 Linux 或 AIX 等其他系统上的部署

在 Windows 系统以及诸如 Linux 或 AIX 之类的其他系统上，IBM Security Key Lifecycle Manager 安装程序会在同一计算机上部署 IBM Security Key Lifecycle Manager 服务器和必需的中间件组件。您必须确保此计算机具有满足工作负载所需的内存、处理器速度和可用磁盘空间。

IBM Security Key Lifecycle Manager 可在域控制器环境中的成员服务器上运行，但在主域或备份域控制器上不受支持。

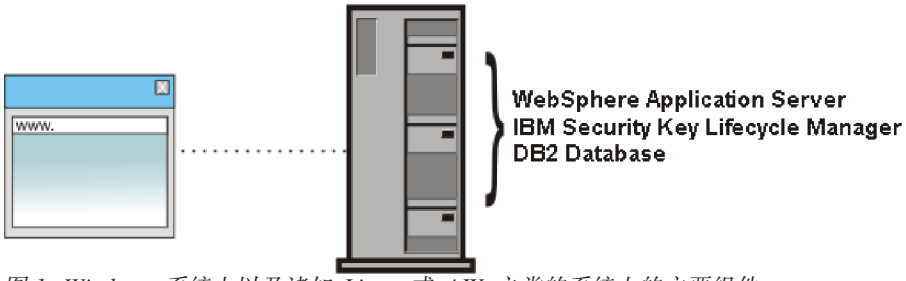

图 1. Windows 系统上以及诸如 Linux 或 AIX 之类的系统上的主要组件

安装概述

IBM Security Key Lifecycle Manager 安装包括准备软件以及之后运行安装程序。

安装 IBM Security Key Lifecycle Manager 的主要步骤是:

1. 规划安装并填写安装工作表。请参阅第 5 页的『规划安装』。
2. 安装和配置 IBM Security Key Lifecycle Manager。安装分为以下阶段:
   a. 介绍阶段，包括语言选择和简介面板以及许可协议面板。
   b. DB2® 和 WebSphere® Application Server 中间件安装阶段，包括收集用于安装 DB2 和 WebSphere Application Server 的信息的面板。在您输入这些信息后，安装程序将在此阶段安装 DB2、中间件和 IBM Security Key Lifecycle Manager。
3. 登录并验证安装，解决所有问题。请参阅第 12 页的『登录 URL 和初始用户标识』和第 90 页的『验证安装』以获取详细信息。

注: 安装时间可能会超过半小时。

安装映像和修订包

对于分布式系统，通过使用 IBM® Passport Advantage® Web 站点来获取 IBM Security Key Lifecycle Manager 安装文件和修订包。还可以通过其他方式来获取文件，例如，通过由 IBM 销售代表提供的 DVD。

Passport Advantage Web 站点提供了软件包，请参阅 eAssemblies 以获取各种 IBM 产品。

“修订中心”Web 站点为系统的软件、硬件和操作系统提供修订和更新。在“修订中心”Web 站点中发布 IBM Security Key Lifecycle Manager 修订包。

IBM Security Key Lifecycle Manager 的 IBM Knowledge Center 上的“安装和配置”部分提供有关安装和配置 IBM Security Key Lifecycle Manager 以及必备中间件产品的指示信息。

安装软件包准备

对于分布式系统，安装软件包可从 DVD 获取，或者通过下载一个或多个压缩文件获取。

从 DVD 安装

对于分布式系统，要从 DVD 安装，请执行以下步骤:

1. 根据操作系统的要求插入或装配 DVD。
2. 在 DVD 的根目录中找到安装脚本。

从下载的软件包安装

分布式系统的安装软件包文件是归档文件，其中包含安装中使用的文件。带有“eImage <*integer*>”标签的软件包需要组合到计算机上的某个临时安装目录中。例如，软件包标签可能是 `eImage 1`。临时安装目录的路径不能包含空格或特殊字符。

要从 eImage 映像进行安装，请遵循以下组合步骤:

1. 将 eImage 软件包文件下载到一个方便的临时目录中。
2. 将 eImage 软件包中的所有压缩文件展开到一个不同的临时目录中。

Windows 系统

将第一个 eImage 软件包解压缩到与第一个 eImage 软件包名称相匹配的临时子目录中。将后续软件包解压缩到与第一个 eImage 软件包名称（而不是后续软件包的名称）相匹配的子目录中。

例如，使用临时目录 `C:\mysklmV26download` 执行以下步骤:

a. 首先，将 eImage 软件包 1 解压缩到某个子目录，例如 `C:\mysklmV26download\CZJF3ML`。

b. 然后，将软件包 2 解压缩到 eImage 软件包 1 创建的同一个子目录，在本示例中为 `C:\mysklmV26download\CZJF3ML`。

c. 将后续软件包解压缩到 eImage 软件包 1 子目录，在本示例中为 `C:\mysklmV26download\CZJF3ML`。

Linux 系统

在 Linux 系统上，压缩文件将直接展开到临时目录中，而不会添加软件包名称。

AIX 系统

在 AIX 系统上，压缩文件将直接展开到临时目录，而不会添加软件包名称。

必须使用 GNU tar 实用程序对 eImage 软件包进行解压缩。请执行以下步骤:

a. 从以下地址下载并安装 GNU tar 实用程序:

   ftp://ftp.software.ibm.com/aix/freeSoftware/aixtoolbox/RPMS/ppc/tar/tar-1.22-1.aix6.1.ppc.rpm

b. 对每个软件包进行解压缩。例如，要对名为 CZJD7ML.tar 的第一个 eImage 进行解压缩，请运行以下命令:

   ```
   /usr/bin/gtar -xvf CZJD7ML.tar
   ```

c. 通过指定其他每个 eImage 重复该命令。

3. 在您展开安装软件包的临时目录中查找并运行安装文件。例如，查找:
   - Windows 系统: launchpad.exe
   - 其他系统: launchpad.sh

   在某些版本的 Linux 操作系统上，当使用 DVD 中的 **launchpad.sh** 命令启动安装程序时，可能会看到以下错误消息:

   ```
   -bash: ./launchpad.sh: /bin/sh: bad interpreter: Permission denied
   ```

   当缺省自动装配设置具有 -noexec 许可权时，会发生此问题。运行安装程序之前，请更改许可权。例如，输入:

   ```
   mount -o remount,exec /media/SKLM_LINUX_Base
   ```

要从修订包映像进行更新，请遵循位于 http://www.ibm.com/support/fixcentral 的 IBM 修订中心 Web 站点上的自述文件指示信息。请使用以下详细信息访问该 Web 站点:

- 产品组: Security Systems
- 产品名称: IBM Security Key Lifecycle Manager

规划安装

必须先规划环境并了解 IBM Security Key Lifecycle Manager 的需求，然后才能安装所需软件。

安装 IBM Security Key Lifecycle Manager 之前，请遵循以下步骤:

- 使用第 93 页的『安装前工作表』中的工作表来帮助进行规划。
- 确定 IBM Security Key Lifecycle Manager 拓扑（在第 2 页的『部署』中有述）。
- 确保系统符合硬件需求。有关更多信息，请参阅
  - 第 7 页的『分布式系统的硬件需求』
- 确保操作系统的级别正确，并且已应用了所有必需的补丁。请参阅第 8 页的『操作系统需求』以获取有关所需操作系统版本的信息。
- 确保需要更新的那些操作系统的内核设置正确。请参阅第 10 页的『DB2 内核设置』以获取详细信息。
- 如果想要使用您自己先前安装的 DB2 版本，请确保 DB2 的副本处于所需的软件级别。请参阅第 9 页的『必备软件』以获取有关受支持的 DB2 版本的信息。
- 确定是否要从较早版本的 Encryption Key Manager 迁移配置。有关迁移的更多信息，请参阅第 21 页的『迁移规划』。
- 决定要用于安装 IBM Security Key Lifecycle Manager 的安装方式: 图形方式或静默方式。请参阅第 41 页的『安装类型』以获取对安装方式的描述。

HOME 和其他目录变量的定义

可以为指定的实施定制 *HOME* 目录。为每个目录变量的定义作出相应的替换。

下表包含在此信息中使用的缺省定义，它表示各种产品安装路径的 *HOME* 目录级别。

这些操作系统（出于方便引用起见，被称为 *distributed systems*）的 *path* 缺省值不同。术语“分布式系统”是指非大型机硬件平台，包括个人计算机和工作站。

- 对于 Windows 系统，缺省值为:
  - DB2

    drive:\Program Files (x86)\IBM
  - 对于除了 DB2 的所有应用程序

    drive:\
- 对于 Linux 和 AIX 系统，缺省路径为 /opt。

表 1. HOME 和其他目录变量

目录变量	缺省定义	描述
DB_HOME	**Windows 系统**: *drive*:\Program Files (x86)\IBM\DB2SKLMV26 **AIX 和 Linux 系统**: /opt/IBM/DB2SKLMV26	包含了 IBM Security Key Lifecycle Manager 的 DB2 应用程序的目录。
DB_INSTANCE_HOME	**Windows** *drive**db2adminID* 例如，如果 *drive* 的值为 C:，并且缺省 DB2 管理员为 sklmdb26，那么 *DB_INSTANCE_HOME* 为 C:\SKLMDB26。 **Linux 和 AIX®** /home/*db2adminID*	包含了 IBM Security Key Lifecycle Manager 的 DB2 数据库实例的目录。
WAS_HOME	**Windows** *drive*:\Program Files (x86)\IBM\WebSphere\AppServer **Linux 和 AIX** *path*/IBM/WebSphere/AppServer 例如: /opt/IBM/WebSphere/AppServer	WebSphere Application Server 主目录。
SKLM_HOME	**Windows** *WAS_HOME*\products\sklm **Linux 和 AIX** *WAS_HOME*/products/sklm	IBM Security Key Lifecycle Manager 主目录。
SKLM_INSTALL_HOME	**Windows** *drive*:\Program Files (x86)\IBM\SKLMV26 **Linux 和 AIX** *path*/IBM/SKLMV26	包含 IBM Security Key Lifecycle Manager 许可证和迁移文件的目录。
IM_INSTALL_DIR	**Windows** *drive*:\ProgramData\IBM\Installation Manager **Linux 和 UNIX** /var/ibm/InstallationManager	IBM Installation Manager 的安装目录。

硬件和软件需求

您的环境必须满足最低系统需求才能安装 IBM Security Key Lifecycle Manager。

发布的硬件和软件需求在发布时是准确的。

另外，请参阅 http://pic.dhe.ibm.com/infocenter/prodguid/v1r0/clarity/softwareReqsForProduct.html 上的详细系统需求文档。

1. 输入 IBM Security Key Lifecycle Manager.
2. 选择产品版本。例如 2.6。
3. 选择操作系统。
4. 单击**提交**。

分布式系统的硬件需求

您必须确保此计算机具有满足工作负载所需的内存、处理器速度和可用磁盘空间。

表 2. 硬件需求

系统组件	最小值*	建议值**
系统内存 (RAM)	4 GB	8 GB
处理器速度	**Linux 和 Windows 系统** 1.0 GHz 单处理器 **AIX 系统** 1.5 GHz（2 路）	**Linux 和 Windows 系统** 3.0 GHz 双处理器 **AIX 系统** 1.5 GHz（4 路）
可用于 IBM Security Key Lifecycle Manager 和必备产品（例如 DB2）的磁盘空间	16 GB	30 GB
/tmp 或 C:\temp 中的可用磁盘空间	4 GB	4 GB
DB2 的 /home 目录中的可用磁盘空间	7 GB	25 GB
DB2 的 /var 目录中的可用磁盘空间	1 GB（Linux 和 UNIX 操作系统上）	1 GB MB（Linux 和 UNIX 操作系统上）

所有文件系统都必须都可以进行写入操作。

* 最小值: 这些值可启用 IBM Security Key Lifecycle Manager 的基本使用。

** 推荐值: 必须使用较大的值以适合于您的生产环境。最关键的需求为提供足够的系统内存、可用磁盘和交换空间。处理器速度相对而言，没之前的因素重要。

在 Linux 和 UNIX 操作系统上，必须将 DB2 产品安装到空目录中。如果指定为安装路径的目录中包含子目录或文件，那么 DB2 安装可能会失败。

在 Linux 和 UNIX 操作系统上，$HOME 目录中需要 4 GB 的可用空间。

在 Windows 操作系统上，除了 DB2 产品所需的可用空间，还需要以下可用空间:

- 40 MB（系统驱动器上）
- 由环境变量 *temp* 指定的 /temp 文件夹中具有 60 MB 空间

不支持安装到映射的网络驱动器/安装的分区中。

如果多个系统组件的安装位置都在同一 Windows 驱动器/UNIX 分区上，那么该驱动器/分区上的可用空间必须能够容纳所有这些组件。

操作系统需求

运行 IBM Security Key Lifecycle Manager 服务器的每种操作系统都具有最低的版本级别需求。

“操作系统需求”表确定了安装的操作系统需求:

表 3. 操作系统需求

操作系统	使用 **DB2 工作组服务器版 V10.5.0.6**
AIX V6.1 和 V7.2（32 位模式）。支持基于 POWER7 处理器的服务器。 • 64 位 AIX 内核是必需的。 • 使用 AIX 6.1 技术级别 7 Service Pack 6。最低 XL C/C++ 运行时级别需要 xlC.rte 12.1.0.0 和 xlC.aix61.rte 12.1.0.0 （或更高版本）文件。这些文件包含在 AIX 软件包的 2008 年 6 月 IBM C++ 运行时环境组件中。	✓
Windows Server 2012 on x86（64 位模式）, 用于: • 标准修订版	✓
Windows Server 2012 **R2** on x86（64 位模式）, 用于: • 标准修订版	✓
Red Hat Enterprise Linux V6.0 Update 6.0 和 V7.0 Update 3 on x86（64 位模式）	✓
Red Hat Enterprise Linux V6.0 Update 6.0 和 V7.0 Update 3 (System z) on x86（64 位模式）	✓
SuSE Linux Enterprise Server V10 和 V11 on x86（64 位模式）	✓
SuSE Linux Enterprise Server V11 (System z) on x86（64 位模式）	✓

注: 不要将 IBM Security Key Lifecycle Manager 安装在具有固化操作系统的系统上。

在 Red Hat Enterprise Linux 操作系统上安装 IBM Security Key Lifecycle Manager 之前，请确保安装以下技术说明中描述的必需库: https://www-304.ibm.com/support/docview.wss?uid=swg21459143

在 AIX 操作系统上安装 IBM Security Key Lifecycle Manager 之前，请确保安装以下技术说明中描述的必需库: http://www-01.ibm.com/support/docview.wss?uid=swg21631478

Linux 软件包

在 Linux 操作系统中，IBM Security Key Lifecycle Manager 需要 `compat-libstdc++` 软件包，其中包含 `libstdc++.so.6`。它还需要 `libaio` 软件包，其中包含 DB2 数据库服务器所需的异步库。

- `libstdc` 软件包

  要确定您是否具有该软件包，请运行以下命令:

  ```
  rpm -qa | grep -i "libstdc"
  ```

  如果未安装该软件包，请在您的原始安装介质上查找 `rpm` 文件，并进行安装。

```
find installation_media -name compat-libstdc++*
rpm -ivh full_path_to_compat-libstdc++_rpm_file
```

- libaio 软件包

  要确定您是否具有该软件包，请运行以下命令:

  ```
  rpm -qa  | grep -i "libaio"
  ```

  如果未安装该软件包，请在您的原始安装介质上查找 rpm 文件，并进行安装。

  ```
  find installation_media -name libaio*
  rpm -ivh full_path_to_libaio_rpm_file
  ```

在 Red Hat Enterprise Linux 64 位系统上，DB2 安装要求在运行 **db2setup** 之前必须安装两个单独的 libaio 程序包。这两个程序包均命名为 libaio。但是，要安装两个不同的 RPM 文件: 其中一个是 i386 RPM 文件，另一个是 x86_64 RPM 文件。

禁用安全增强 Linux

如果启用了安全增强 Linux (SELINUX)，那么会在 Linux 操作系统上会发生 IBM Security Key Lifecycle Manager 问题。

关于此任务

例如，IBM Security Key Lifecycle Manager 服务器 端口可能会发生 TCP/IP 连接问题。要禁用安全增强 Linux，请在安装 Linux 操作系统之后执行以下步骤:

过程

1. 编辑 /etc/selinux/config 文件并设置 SELINUX=disabled。
2. 重新启动系统。
3. 从命令行运行 **sestatus**，确保已禁用 SELinux。

   ```
   [root@localhost ~]$ sestatus
   SELinux status: disabled
   ```

4. 安装 IBM Security Key Lifecycle Manager。

必备软件

IBM Security Key Lifecycle Manager 使用多个支持程序和中间件程序。

- 『Java 运行时环境 (JRE) 需求』
- 第 10 页的『运行时环境需求』
- 第 10 页的『数据库权限和需求』
- 受支持的浏览器（不随产品安装提供）

在分布式系统上，IBM Security Key Lifecycle Manager 将安装所使用的中间件。如果系统上已安装了 DB2，那么请参阅第 10 页的『数据库权限和需求』中的详细信息。

确保在 UNIX 操作系统上安装 IBM Security Key Lifecycle Manager 之前安装 Bash Shell。

Java 运行时环境 (JRE) 需求

Java 运行时环境 版本的 IBM Security Key Lifecycle Manager 需求取决于使用的操作系统。

在分布式系统上:

IBM Java 运行时环境 随 WebSphere Application Server 提供。

在所有系统上，不支持使用来自 IBM 或其他供应商的独立安装的 Java™ 开发工具包。

数据库权限和需求

数据库的 IBM Security Key Lifecycle Manager 需求取决于使用了哪个操作系统。

- 分布式系统:

  运行 IBM Security Key Lifecycle Manager 服务器的同一计算机上的 DB2 工作组服务器版:

  – IBM Security Key Lifecycle Manager 支持的其他分布式操作系统上的 10.5.0.6 和未来修订包。

    注:

    - 必须使用 IBM Security Key Lifecycle Manager 来管理数据库。为避免数据同步问题，请不要使用数据库应用程序可能提供的工具。
    - 为了提高 AIX 系统上 DB2 V10.5.0.6 的性能，请确保您安装并配置了 DB2 文档 (http://www-01.ibm.com/support/knowledgecenter/SSEPGG_10.5.0/com.ibm.db2.luw.admin.perf.doc/doc/t0054518.html) 中描述的 I/O 完成端口 (IOCP) 软件包。
    - 如果以 root 用户的身份在操作系统的正确版本安装了 DB2 工作组服务器版的现有副本，那么可以使用现有的 DB2 工作组服务器版。IBM Security Key Lifecycle Manager 安装程序未检测到存在 DB2。必须指定 DB2 安装路径。

有关 DB2 先决条件的更多信息，请参阅 DB2 文档 (http://www-01.ibm.com/support/knowledgecenter/SSEPGG_10.5.0/com.ibm.db2.luw.admin.cmd.doc/doc/r0059710.html)。

DB2 内核设置:

确保需要更新的那些操作系统（如 Linux 操作系统）的内核设置正确。

安装应用程序之前，请参阅以下 Web 站点上的 DB2 文档以了解这些内核设置:

AIX 系统

不需要任何设置。

Linux 系统

有关在其他受支持的 Linux 系统上修改 DB2 工作组服务器版 V10.5.0.6 的内核参数的更多信息，请参阅 DB2 文档 (http://www-01.ibm.com/support/knowledgecenter/SSEPGG_10.5.0/com.ibm.db2.luw.qb.server.doc/doc/t0008238.html)。

Windows 系统

不需要任何设置。

运行时环境需求

运行时环境的 IBM Security Key Lifecycle Manager 需求取决于使用的操作系统。

在分布式系统上:

WebSphere Application Server 8.5.5.7 和任何适用的修订包或 APAR 需求。

IBM Security Key Lifecycle Manager 包含并安装 WebSphere Application Server。安装期间，IBM Security Key Lifecycle Manager 将修改 WebSphere Application Server。卸载 IBM Security Key Lifecycle Manager 时，此修改将引起使用相同服务器的产品出错。要避免这些问题，请遵循以下指示:

- 不要将 IBM Security Key Lifecycle Manager 安装在其他产品提供的 WebSphere Application Server 实例中。
- 不要将其他产品安装在 IBM Security Key Lifecycle Manager 提供的 WebSphere Application Server 实例中。

浏览器需求

必须在浏览器中启用会话 cookies 和 JavaScript 以建立与 IBM Security Key Lifecycle Manager 的会话。

产品安装中不包含受支持的浏览器。必须在运行 IBM Security Key Lifecycle Manager 的同一计算机上部署浏览器。

表 4. 受支持的浏览器

浏览器	修订包	AIX	Windows Server 2012	Windows Server 2012 R2	Red Hat Enterprise Linux	SuSE Linux Enterprise Server
Microsoft Internet Explorer V9.0	无		✓	✓		
Microsoft Internet Explorer V10.0	无		✓	✓		
Microsoft Internet Explorer V11.0	无		✓	✓		
Firefox ESR V24.0	无	✓	✓	✓	✓	✓
Firefox ESR V31.0	无	✓	✓	✓	✓	✓
Firefox ESR V38.0	无	✓	✓	✓	✓	✓

密钥长度要求

必须先考虑密钥长度需求，然后再安装和配置 IBM Security Key Lifecycle Manager。

受支持的密钥长度以及导入和导出限制

IBM Security Key Lifecycle Manager 可以为设备提供 2048 位或 1024 位的密钥。早期生成的 1024 位密码可以继续使用。

表 5 列出了 IBM Security Key Lifecycle Manager 支持的密钥长度。

表 5. 支持的密钥长度

导入 PKCS#12 文件	导出 PKCS#12 文件	密钥生成大小（位）
是	是	2048

登录 URL 和初始用户标识

要在安装 IBM Security Key Lifecycle Manager 之后快速启动，请获取登录 URL 以及初始 IBM Security Key Lifecycle Manager 的用户标识和密码。

访问需求

以管理员（root 用户）身份安装 IBM Security Key Lifecycle Manager。

只有在 Linux 操作系统上，还可以非 root 用户身份安装 IBM Security Key Lifecycle Manager。

登录 URL

使用登录 URL 访问 IBM Security Key Lifecycle Manager Web 界面。IBM Security Key Lifecycle Manager 的管理控制台的登录 URL 为:

`https://ip-address:port/ibm/SKLM/login.jsp`

ip-address 的值为 IBM Security Key Lifecycle Manager 服务器 的 IP 地址或 DNS 地址。

port 的值是 IBM Security Key Lifecycle Manager 服务器 用于侦听请求的端口号。

如果您使用 HTTPS 地址，那么端口的缺省值为 9080:

`https://ip-address:9080/ibm/SKLM/login.jsp`

不要使用大于 65520 的端口值。

在 Windows 系统上，这些信息位于“开始”菜单上。单击**开始 > 所有程序 > IBM Security Key Lifecycle Manager 2.6**。

WebSphere Application Server 的管理控制台的登录 URL 为:

`https://ip-address:port/ibm/console/logon.jsp`

ip-address 的值为 WebSphere Application Server 的 IP 地址或 DNS 地址。

port 的值是 WebSphere Application Server 用于侦听请求的端口号。

WebSphere Application Server 信息面板上的缺省端口为 9083。在迁移期间，或者如果缺省端口由于其他原因冲突了，那么 WebSphere Application Server 会自动选择另一个可用端口。

“安装完成”面板将指示已为 WebSphere Application Server 配置了端口。Windows 开始菜单包含了一个条目，它使用正确的端口号连接到 WebSphere Application Server。

单击 **IBM WebSphere > IBM WebSphere Application Server V8.5.5 > 概要文件 > KLMProfile > 管理控制台**。

管理员用户标识和密码

安装 IBM Security Key Lifecycle Manager 将提供缺省管理员用户标识 WASAdmin、SKLMAdmin 和 `sklmdb26`。

表 6. 管理员用户标识和密码

程序	用户标识	密码
分布式系统 对于分布式操作系统，安装必须由不是 AIX 或 Linux 系统 root 用户或者 Windows 系统管理员组成员的本地管理标识运行。不要使用域用户标识来安装 IBM Security Key Lifecycle Manager。 可能有以下一个或多个用户标识:		
IBM Security Key Lifecycle Manager 管理员	**SKLMAdmin** 作为对所有操作有完全访问权的主管理员，此用户标识在名为 `klmSecurityOfficerGroup` 的组中具有 `klmSecurityOfficer` 超级用户角色。用户标识不区分大小写。另外，请使用 **sklmadmin**。请使用 SKLMAdmin 用户标识来管理 IBM Security Key Lifecycle Manager。 使用此 SKLMAdmin 用户标识，您可以: • 查看并使用 IBM Security Key Lifecycle Manager 界面。 • 更改 IBM Security Key Lifecycle Manager 管理员的密码。 但是，您不能: • 创建一个或多个其他的 IBM Security Key Lifecycle Manager 管理员用户标识。 • 执行 WebSphere Application Server 管理员任务，比如创建或分配角色。 • 启动或停止服务器。	在安装期间指定并安全存储密码。

表 6. 管理员用户标识和密码 (续)

程序	用户标识	密码
WebSphere Application Server 管理员	**WASAdmin** 用户标识不区分大小写。另外，请使用在安装期间指定的 **wasadmin** 或用户标识。 不要使用: • SKLMAdmin 用户标识来管理 WebSphere Application Server。 • WASAdmin 用户标识来管理 IBM Security Key Lifecycle Manager。WASAdmin 用户标识没有要使用 IBM Security Key Lifecycle Manager 的角色。 此管理员用户标识是 WebSphere Application Server 用户标识。 使用此 wasadmin 用户标识，您可以: • 仅查看并使用 WebSphere Application Server 界面。 • 创建一个或多个其他的 IBM Security Key Lifecycle Manager 管理员用户标识、组和角色。 • 重置所有 IBM Security Key Lifecycle Manager 用户标识（包 括SKLMAdmin 管理员）的密码。 • 启动和停止服务器。 但是，您不能: • 使用 IBM Security Key Lifecycle Manager 完成任务。例如，无法创建 IBM Security Key Lifecycle Manager 设备组。 • 执行其他需要访问 IBM Security Key Lifecycle Manager 数据的任务。wasadmin 用户标识*不能*以超级用户的身份访问 IBM Security Key Lifecycle Manager 数据。	在安装期间指定并安全存储密码。 使用与保护 SKLMAdmin 用户标识的相同方法保护 WASAdmin 用户标识。WASAdmin 用户标识有权重置 SKLMAdmin 密码并为新的 IBM Security Key Lifecycle Manager 用户创建并分配许可权。
IBM Security Key Lifecycle Manager DB2 数据库		

表 6. 管理员用户标识和密码 (续)

程序	用户标识	密码
数据库实例所有者	**Windows 系统以及诸如 AIX 或 Linux 之类的系统:** 缺省值为 sklmdb26。可以在安装期间指定另一个值。此标识是数据库实例所有者的安装缺省用户标识。 不要指定长度大于 8 个字符的用户标识。 实例名称也为 sklmdb26。 如果 DB2 位于 AIX 或 Linux 等系统上，您的用户标识必须位于 bin 或 root 用户组中，或者位于其成员包含 root 用户的其他组中。 如果为 IBM Security Key Lifecycle Manager 数据库使用了现有的用户标识，那么该用户标识不能拥有其他数据库实例。 **注:** 指定 DB2 的现有副本的用户标识时，不要使用连字符 (-) 或下划线 (_) 字符。	在安装期间指定并安全存储密码。此密码是操作系统密码。如果更改了操作系统的密码，那么必须更改此密码。 有关更多信息，请参阅第 58 页的『在分布式系统上重置密码』。.
数据库实例	管理员标识 sklmdb2 拥有名为 sklmdb26 的 DB2 实例。	

审计文件

IBM Security Key Lifecycle Manager 有一个保存审计数据的缺省目录。位置取决于使用的是哪个操作系统。

分布式系统

在 *SKLM_HOME*/config/SKLMConfig.properties文件中，编辑 **Audit.handler.file.name** 属性可设置此目录。缺省值为:

```
Audit.handler.file.name=logs/audit/sklm_audit.log
```

用户角色

IBM Security Key Lifecycle Manager 提供了超级用户（klmSecurityOfficer 和 klmGUICLIAccessGroup）角色并提供了通过指定更多受限管理角色来满足组织需求的方法。缺省情况下，SKLMAdmin 用户标识使用 klmSecurityOfficer 角色。

对于备份和复原任务，IBM Security Key Lifecycle Manager 还安装了初始情况下没有用户标识的 klmBackupRestoreGroup。安装 IBM Security Key Lifecycle Manager 将创建预定义的管理员、操作员和审计员组来管理 LTO 磁带机。

WASAdmin 用户标识有权创建和分配这些角色，并可以更改任何 IBM Security Key Lifecycle Manager 管理员的密码。要为 IBM Security Key Lifecycle Manager 设置管理限制，请使用 WebSphere Integrated Solutions Console 上的 WASAdmin 用户标识来创建角色、用户和组。将角色和用户分配到组。例如，您可能创建了一个组，并分配了

用户和用于限制用户活动的角色，仅为管理 LTO 磁带机。您必须为新用户分配一个角色，然后该用户才能尝试登录 IBM Security Key Lifecycle Manager。

开始之前，请完成以下任务:

- 确定贵组织在设备管理方面所需的限制。

  例如，您可能确定特定设备组具有它自己的管理。
- 估算在一定时间间隔内可能需要多少个管理用户。为方便使用，请考虑指定组和角色来指定他们的任务。

  例如，您可以指定一个具有受限的许可权范围的组以仅管理 3592 磁带机。

可用的许可权

安装 IBM Security Key Lifecycle Manager 将创建 SKLMAdmin 用户标识，该用户标识具有作为缺省超级用户的 `klmSecurityOfficer` 角色。安装流程还向管理角色的 WebSphere Application Server 列表部署了预定义的许可权。

IBM Security Key Lifecycle Manager 中的*许可权*可以启用操作或启用对设备组的使用。IBM Security Key Lifecycle Manager 中的一个*角色*是一个或多个许可权。但是，在 WebSphere Application Server 图形用户界面中，术语*角色*包含 IBM Security Key Lifecycle Manager 许可权和角色。

注: 安装将创建以下缺省组:

klmSecurityOfficerGroup

安装将向此组分配 `klmSecurityOfficer` 角色。`klmSecurityOfficer` 角色将替换名称为 `klmGroup` 的组中先前的 `klmApplicationRole` 角色。`klmSecurityOfficerGroup` 将替换 `klmGroup`。

`klmSecurityOfficer` 角色具有:

- 对 第 17 页的表 7 和 第 18 页的表 8 中描述的整个许可权集合和设备组的 root 访问权。
- 对可能创建的任何角色或设备组的许可权。
- `suppressmonitor` 角色。

  WebSphere Application Server 提供 `suppressmonitor` 角色以在 WebSphere Integrated Solutions Console 的左窗格中隐藏 IBM Security Key Lifecycle Manager 管理员不使用的任务。隐藏的项与应用程序服务器相关联，包括安全性、故障诊断和用户和组文件夹中的 WebSphere Application Server 管理任务。

klmBackupRestoreGroup

备份和复原 IBM Security Key Lifecycle Manager。

LTOAdmin

使用包括创建、查看、修改、删除、获取（导出）、备份和配置在内的操作管理 LTO 设备系列中的设备。

LTOOperator

使用包括创建、查看、修改和备份在内的操作对 LTO 设备系列中的设备进行操作。

LTOAuditor

使用包括查看和审计在内的操作对 LTO 设备系列中的设备进行审计。

klmGUICLIAccessGroup

向用户提供 IBM Security Key Lifecycle Manager 图形用户界面和命令行界面的访问权。每个产品用户都必须属于该组。

注: 除了对此组的访问权，还必须向用户提供其他访问权以使其成为功能产品用户。

具有 表 7 中的任意一个许可权的用户可以查看:

- SKLMConfig.properties 文件中定义的 IBM Security Key Lifecycle Manager 全局配置参数。
- 密钥服务器和上次备份日期。

表 7. 操作许可权

许可权	启用以下操作	与设备组不相关	与设备组相关联
klmCreate	创建，而不是查看、修改或删除对象。		✓
klmDelete	删除对象，而不是查看、修改或创建对象。		✓
klmGet	导出客户机设备的密钥或证书。		✓
klmModify	修改对象，而不是查看、创建或删除对象。		✓
klmView	查看对象，但不能创建、删除或修改对象。例如，您必须具有此许可权才能查看要在图形用户界面上执行的任务。		✓
klmAdminDeviceGroup	管理。创建设备组，设置缺省参数，查看和删除空的设备组。此许可权不提供对设备、密钥或证书的访问权。	✓	
klmAudit	通过使用 **tklmServedDataList** 命令来查看审核数据。	✓	
klmBackup	创建和删除 IBM Security Key Lifecycle Manager 数据的备份。	✓	
klmConfigure	阅读和更改 IBM Security Key Lifecycle Manager 配置属性，或在 SSL 证书上操作。添加、查看、更新或删除密钥库。	✓	
klmRestore	复原 IBM Security Key Lifecycle Manager 数据的之前的备份副本。	✓	

klmSecurityOfficer 角色还对所有设备组的许可权具有 root 访问权。

表 8. 设备组

许可权	允许对以下对象进行操作
LTO	LTO 设备系列
TS3592	3592 设备系列
DS5000	DS5000 设备系列
DS8000	DS8000 设备系列
BRCD_ENCRYPTOR	BRCD_ENCRYPTOR 设备组
ONESECURE	ONESECURE 设备组
ETERNUS_DX	ETERNUS_DX 设备组
XIV	XIV 设备组
IBM_SYSTEM_X_SED	IBM_SYSTEM_X_SED 设备组
IBM Spectrum Scale（前身为 GPFS）	IBM Spectrum Scale 设备组
GENERIC	GENERIC 设备系列中的对象。
userdevicegroup	根据 LTO 之类的预定义设备系列手动创建的用户定义的实例，例如，myLTO。

IBM Security Key Lifecycle Manager 与 LDAP 的集成

您可以将 IBM Security Key Lifecycle Manager 与 LDAP 用户存储库集成。必须配置 LDAP 存储库以访问 IBM Security Key Lifecycle Manager 服务器、服务器 API 和 CLI。

您可以配置任何 LDAP 存储库（如 IBM Security Directory Server 或 Microsoft Active Directory）中的 IBM Security Key Lifecycle Manager 用户，以访问 IBM Security Key Lifecycle Manager 服务器并调用服务器 API 和 CLI。必须将 LDAP 用户存储库添加到 WebSphere Application Server 的联合存储库并进行配置。IBM Security Key Lifecycle Manager 使用应用程序组对 IBM Security Key Lifecycle Manager 功能强制实施基于角色的授权。为使 IBM Security Key Lifecycle Manager 用户在 LDAP 用户存储库中运行 IBM Security Key Lifecycle Manager 功能，该用户必须是特定 IBM Security Key Lifecycle Manager 应用程序组的成员。

安装 IBM Security Key Lifecycle Manager 时，将在 WebSphere Application Server 联合存储库中的基于文件的缺省存储库内创建应用程序组和用户。向 WebSphere Application Server 联合存储库中添加 LDAP 用户存储库后，必须使 LDAP 用户成为 IBM Security Key Lifecycle Manager 应用程序组的成员。无法使 LDAP 用户成为缺省基于文件的存储库中组的成员。

在基于文件的存储库和 LDAP 存储库之间不可能存在跨存储库组成员资格。但是，跨 LDAP 存储库和基于数据库的存储库可能存在跨存储库组成员资格。因此，请创建基于数据库的存储库并在此存储库中创建所有 IBM Security Key Lifecycle Manager 应用程序。将会除去基于文件的存储库中存在的应用程序组。

一旦创建基于数据库的存储库并将 IBM Security Key Lifecycle Manager 应用程序组添加到此存储库，即可使 LDAP 存储库中的用户成为基于数据库的存储库中 IBM Secu-

rity Key Lifecycle Manager 应用程序组的成员。然后，用户可以登录到 IBM Security Key Lifecycle Manager 应用程序并运行 IBM Security Key Lifecycle Manager 应用程序功能。

有关 LDAP 配置任务的信息，请参阅“管理”部分。

迁移规划

安装此版本的 IBM Security Key Lifecycle Manager 之前，请确定迁移先前版本的 IBM Security Key Lifecycle Manager，还是迁移 Java 平台的 Encryption Key Manager 组件中的先前配置数据。

您还可以使用跨平台备份实用程序对 IBM Security Key Lifecycle Manager V1.0、V2.0、V2.0.1 和 V2.5 等旧版以及 Encryption Key Manager V2.1 运行备份操作以备份关键数据。您可以在 IBM Security Key Lifecycle Manager V2.6 上将这些备份文件复原到与备份来源不同的操作系统。有关更多信息，请参阅旧版 IBM Security Key Lifecycle Manager 的备份和复原操作。

注: Encryption Key Manager 组件仅支持 English 语言环境。因此，必须在英语语言环境中执行从 Encryption Key Manager 到 IBM Security Key Lifecycle Manager 的迁移。

- IBM Security Key Lifecycle Manager V2.5 FP3 或更新版本。

  安装 IBM Security Key Lifecycle Manager V2.6 时检测到较早版本的 IBM Security Key Lifecycle Manager。安装会自动迁移其数据。

  如果 IBM Security Key Lifecycle Manager V2.5 迁移失败，那么会保留成功迁移步骤的记录。运行迁移恢复脚本将从迁移过程中发生错误的点开始。

  注: 从 IBM Security Key Lifecycle Manager V2.5 迁移到 V2.6 时，必须将 IBM Security Key Lifecycle Manager 服务器端口号从 `9080` 更改为可用的任何其他端口号，例如，`9180`。还必须更改 WebSphere Application Server 的安装目录名称，例如，`WebSphere26`。
- IBM Security Key Lifecycle Manager V2.0.1 或更高版本的修订包。

  安装 IBM Security Key Lifecycle Manager V2.6 时检测到较早版本的 IBM Security Key Lifecycle Manager。安装会自动迁移其数据。

  如果 IBM Security Key Lifecycle Manager V2.0.1 迁移失败，那么会保留成功迁移步骤的记录。运行迁移恢复脚本将从迁移过程中发生错误的点开始。
- IBM Security Key Lifecycle Manager V2 修订包 4 或更高版本。

  安装 IBM Security Key Lifecycle Manager V2.6 时检测到较早版本的 IBM Security Key Lifecycle Manager。安装会自动迁移其数据。

  如果 IBM Security Key Lifecycle Manager V2.0 迁移失败，那么会保留成功迁移步骤的记录。运行迁移恢复脚本将从迁移过程中发生错误的点开始。
- IBM Security Key Lifecycle Manager V1 修订包 3 或更高版本。

  安装 IBM Security Key Lifecycle Manager V2.6 时检测到较早版本的 IBM Security Key Lifecycle Manager。安装会自动迁移其数据。

  如果 IBM Security Key Lifecycle Manager V1 迁移失败，那么会保留成功迁移步骤的记录。运行迁移恢复脚本将从迁移过程中发生错误的点开始。

- Encryption Key Manager V2.1

  为 V2.1 启用了迁移，但是没有为更早版本的 Encryption Key Manager 启用迁移。迁移配置的唯一机会是在安装 IBM Security Key Lifecycle Manager 期间，或者在安装后，更改 IBM Security Key Lifecycle Manager 配置之前立即进行迁移。

  如果 Encryption Key Manager V2.1 迁移失败，那么不会将任何数据迁移到 IBM Security Key Lifecycle Manager 数据库。会撤销所有已作出的更改。

如果安装程序迁移失败，那么可以在退出安装后从 *SKLM_HOME*\migration\bin 目录中手动运行 IBM Security Key Lifecycle Manager V2.6 迁移实用程序。

- 运行 **migrate.bat** 或 **migrate.sh** 以将 Encryption Key Manager V2.1 迁移到 IBM Security Key Lifecycle Manager。在诸如 Linux 或 AIX 之类的系统上，请确保以 root 用户身份登录，然后再运行 **migrate.sh**。
- 在 *SKLM_HOME*\migration 目录中运行 **migrateToSKLM.bat** 或 **migrateToSKLM.sh** 以将 IBM Security Key Lifecycle Manager 先前版本迁移到 V2.6。在诸如 Linux 或 AIX 之类的系统上运行 **migrateToSKLM.sh** 之前，请确保您以 root 用户身份登录。

请不要运行可能在此目录中看到的其他 ***.bat** 实用程序。这些实用程序仅供自动安装流程使用。

迁移前

开始之前，请确保您的企业允许临时暂停密钥提供活动一段时间。

还需要用于测试的时间窗来确保新的 IBM Security Key Lifecycle Manager 具有期望的密钥和您想要迁移的其他配置属性。

请完成以下初步任务:

磁盘空间需求

将 IBM Security Key Lifecycle Manager 先前版本迁移到 IBM Security Key Lifecycle Manager V2.6 之前，请验证系统上是否有足够的磁盘空间。

这些磁盘空间需求是额外的，不包含在安装程序所确定的用于安装 IBM Security Key Lifecycle Manager V2.6 及其必备软件 WebSphere Application Server 和 DB2 的磁盘空间需求中。

需要额外的磁盘空间，因为迁移程序将运行以下任务:

- 将用户从先前版本迁移到 V2.6。
- 将先前版本的数据库中的数据移动到新的 IBM Security Key Lifecycle Manager 数据库。
- 将密钥库中的所有密钥移动到 IBM Security Key Lifecycle Manager 数据库。

如果您确定磁盘空间不足，请增加分区上的磁盘空间或盘符。必须确定磁盘空间需求，这包括确定密钥数量和所处理的数据量。

确定磁盘空间需求

要确定磁盘空间需求，请执行以下步骤:

Windows 系统

1. 通过输入文件 %SYSTEMDRIVE%\tklmtemp\db2srcit.txt 的内容来确定 IBM Security Key Lifecycle Manager 先前版本 V1.0、V2.0、V2.0.1 或 V2.5 安装中的以下属性。例如:

   ```
   DB2ADMIN=tklmdb2
   DB2DBNAME=tklmdb
   DB2ADMINID=tklmdb2
   DB2PORTSTART=50010
   DB2INSTALLDIR=C:\IBM\tklmV2db2\
   INSTANCEHOME=C:
   ```

2. 确定 IBM Security Key Lifecycle Manager 先前版本安装数据库所在的盘符。即，INSTANCEHOME 属性的值。使用 Windows 资源管理器，确定名称为 TKLMDB2 的文件夹的大小。

   注: 计算具有数据库的驱动器中要用于迁移的额外空间是否为 TKLMDB2 文件夹的三倍。

3. 使用第 24 页的『确定密钥数和提供的数据』中的步骤来确定密钥数和设备审核数据。迁移密钥和提供的数据时会在 *<IM App Data Dir>*/logs/sklmLogs 文件夹中生成日志。

   注: 计算安装了 IBM Security Key Lifecycle Manager V2.6 的 Windows 驱动器上所需的额外空间是否为以下两个运算的结果之和:

   - 密钥数乘以 5 KB
   - 提供的数据数乘以 1 KB

   在典型安装中，迁移其他项（例如，设备和组）不会生成额外的磁盘空间需求。

诸如 Linux 或 AIX 之类的系统

1. 通过输入文件 /tklmtemp/db2unix.srcit 的内容来确定 IBM Security Key Lifecycle Manager 先前版本 V1.0、V2.0、V2.0.1 或 V2.5 安装中的以下属性。

   典型文件中可能包含以下条目:

   ```
   export DB2ADMIN=tklmdb2
   export DB2DBNAME=tklmdb
   export INSTANCEHOME=/home/tklmdb2
   ```

2. 检查 **INSTANCEHOME** 属性的值来确定数据库所有者的主目录。输入以下命令来确定主目录中的磁盘空间:

   ```
   du –k /home/sklmdb2/sklmdb2
   ```

   注:
   计算具有数据库的磁盘分区中要用于迁移的额外空间是否为 /home/sklmdb2/sklmdb2 文件夹的三倍。

3. 使用第 24 页的『确定密钥数和提供的数据』中的步骤来确定密钥数和设备审核数据。迁移密钥和提供的数据时会在 *<IM App Data Dir>*/logs/sklmLogs 文件夹中生成日志。

注: 计算安装了 IBM Security Key Lifecycle Manager V2.6 的计算机上的磁盘分区中所需的额外空间是否是以下两个操作的总和:

- 密钥数乘以 5 KB
- 提供的数据数乘以 1 KB

在典型安装中，迁移其他项（例如，设备和组）不会生成额外的磁盘空间需求。

确定密钥数和提供的数据

要确定密钥数和提供的数据，请执行以下步骤:

Windows 系统

1. 输入:

   ```
   d2cmd
   set DB2INSTANCE=sklmdb2
   db2 connect to tklmdb user sklmdb2 using password
   ```

   其中:

   tklmdb
   由 **DB2DBNAME** 属性确定。

   sklmdb2
   由 **DB2ADMIN** 属性确定

   password
   数据库的密码。
2. 确定要迁移的密钥数。输入:

   ```
   db2 "SELECT COUNT(UUID) FROM KMT_KEY"
   ```
3. 确定迁移所涉及的处理数据量。输入:

   ```
   db2 "SELECT COUNT(*) FROM KMT_DEVAUDIT"
   ```
4. 退出会话。输入:

   ```
   db2 terminate
   ```

诸如 Linux 或 AIX 之类的系统

1. 输入:

   ```
   . ~sklmdb2/sqllib/db2profile
   db2 connect to tklmdb user sklmdb2 using password
   ```

   其中:

   tklmdb
   由 **DB2DBNAME** 属性确定。

   sklmdb2
   由 **DB2ADMIN** 属性确定

   password
   数据库的密码。
2. 确定要迁移的密钥数。输入:

   ```
   db2 "SELECT COUNT(UUID) FROM KMT_KEY"
   ```
3. 确定迁移所涉及的处理数据量。输入:

```
db2 "SELECT COUNT(*) FROM KMT_DEVAUDIT"
```

4. 退出会话。输入:

```
db2 terminate
```

示例计算

假设 IBM Security Key Lifecycle Manager V2.6 安装在缺省位置 /opt/IBM/WebSphere/AppServer 中，并且磁盘分区为 /opt。数据库实例所有者的主目录为 /home/sklmdb2，磁盘分区为 /home。

确定以下值:

- 数据库中的密钥数 = 84000
- 提供的数据列表 = 100000
- 输入命令 du -k /home/sklmdb2/sklmdb2 将返回值 173712。

计算所需的额外磁盘空间:

- 在 /opt 分区中

  (84000 * 5) + (100000 * 1) = 520000 KB

- 在 /home 分区中

  (3 * 173712) = 521136 KB

数据量

确定是否存在大量数据需要迁移。在迁移活动期间，迁移现有数据库可能最多需要当前磁盘空间使用量的 4 倍。

此磁盘空间的大部分是在迁移成功后释放的。您可能还需要更改 第 7 页的『分布式系统的硬件需求』 中所述的内存设置。

Encryption Key Manager 配置

迁移之前，必须已正确设置 Encryption Key Manager 配置，并且必须是正常运行的配置。

请执行以下步骤:

- 刷新并停止 Encryption Key Manager 服务器以确保没有丢失数据。
- 备份具有您想要迁移的配置数据的服务器。迁移的数据中包含以下文件:
  - 配置属性文件
  - 由配置属性文件引用的密钥和证书
  - 驱动器表
  - 配置属性文件指向的可选元数据文件
  - 可选密钥组文件
- 停止 Encryption Key Manager。迁移期间密钥提供不能处于活动状态。

IBM Security Key Lifecycle Manager V2.6 需求

迁移之前，请确保 IBM Security Key Lifecycle Manager V2.6 满足以下先决条件:

迁移前，请执行以下步骤:

- 确保已对要迁移的版本的 IBM Security Key Lifecycle Manager 应用了最新的修订包。
- 备份 IBM Security Key Lifecycle Manager 先前版本 V1.0、V2.0、V2.0.1 或 V2.5。此外，备份所有副本。如果迁移失败，您可能需要从备份副本复原 IBM Security Key Lifecycle Manager 先前版本。

  注: 将 IBM Security Key Lifecycle Manager 成功迁移到 V2.6 之后，通过使用 CLI 命令、图形用户界面或 REST 接口创建的先前版本备份文件无法用于复原 IBM Security Key Lifecycle Manager V2.6。

  您可以使用 IBM Security Key Lifecycle Manager V2.6 的备份实用程序为先前版本创建跨平台兼容备份文件。然后，可以在 IBM Security Key Lifecycle Manager V2.6 系统上从先前版本复原这些备份文件。
- 验证是否具有正常运行的 IBM Security Key Lifecycle Manager 先前版本 V1.0、V2.0 或 V2.0.1 系统以及已配置的密钥库。如果未配置密钥库，那么迁移将失败。
- 当 V2.6 安装过程除去 IBM Security Key Lifecycle Manager 先前版本时，迁移过程不会除去先前版本的备份目录。

  但是，如果 IBM Security Key Lifecycle Manager 先前版本的备份目录是 Tivoli Integrated Portal 服务器 目录路径中的子文件夹，那么卸载 Tivoli Integrated Portal 时也会除去 IBM Security Key Lifecycle Manager 备份目录。
- 迁移过程不会除去 IBM Security Key Lifecycle Manager 的先前版本。要除去先前版本，请遵循作为迁移源的 IBM Security Key Lifecycle Manager 版本的卸载指示信息。

  注: 因为 IP 端口在两个版本间共享，所以请勿同时运行两个版本。
- 停止 IBM Security Key Lifecycle Manager 和所有副本服务器。迁移期间密钥提供不能处于活动状态。
- 不能对 IBM Security Key Lifecycle Manager 数据库使用带有特殊字符的密码。您只能使用字母字符（A-Z 和 a-z）、数字字符 (0-9)、下划线 (_) 和连字符 (-)。如果您之前修改了密码，那么请在迁移前更改密码以仅使用迁移允许的字符集。迁移后，您可以重置密码来使用特殊字符。
- 迁移期间，请经常检查 `<IM App Data Dir>/logs/sklmLogs/migration.log` 文件以确定迁移的进度。如果迁移失败，请运行迁移实用程序来将消息发送到 `migration.log` 文件和命令行界面。
- 要避免在迁移过程中发生错误，请不要在迁移过程之外启动或停止 DB2 服务器 或 Tivoli Integrated Portal 服务器。请勿中断迁移过程。
- 无论在静默安装方式还是图形安装方式下的迁移过程中，Tivoli Integrated Portal 服务器、Tivoli Key Lifecycle Manager 服务器和 Tivoli Key Lifecycle Manager DB2 数据库服务器都必须处于运行状态。

IBM Security Key Lifecycle Manager V2.5 到 V2.6 迁移

如果要在 Windows 或 Linux 系统（其中安装了 32 位的 Installation Manger）上从 V2.5 迁移，请完成以下步骤。

图形方式安装

1. 下载安装包，并将其解压缩到您选择的目录中。
2. 打开命令提示符。

3. 转到 disk1 目录，并在指定 **reinstallIM** 参数的情况下运行 **reinstallIM** 脚本。

   Windows

   ```
   C:\disk1> reinstallIM.bat -reinstallIM
   ```

   Linux

   ```
   /opt/disk1> reinstallIM.sh -reinstallIM
   ```

4. 接收到消息“Execution Completed”之后，请运行以下命令以安装 V2.6。

   Windows

   ```
   C:\disk1> install.bat
   ```

   Linux

   ```
   /opt/disk1> install.sh
   ```

静默安装

1. 下载安装包，并将其解压缩到您选择的目录中。
2. 打开命令提示符。
3. 转到 disk1 目录，并在指定 **reinstallIM** 参数的情况下运行 **reinstallIM** 脚本。

   Windows

   ```
   C:\disk1> reinstallIM.bat -reinstallIM
   ```

   Linux

   ```
   /opt/disk1> reinstallIM.sh -reinstallIM
   ```

4. 接收到消息“Execution Completed”之后，请运行以下命令以执行静默安装。

   注: 您必须更新迁移响应文件中的参数，使其与迁移设置匹配。

   Windows

   ```
   C:\disk1> silent_install.bat <migration_response_file>
   ```

   Linux

   ```
   /opt/disk1> silent_install.sh <migration_response_file>
   ```

Encryption Key Manager 的迁移需求

可以从 Encryption Key Manager 迁移到 IBM Security Key Lifecycle Manager 之前，需要满足一些特定需求。您可以仅迁移 Encryption Key Manager V2.1。

- 将 Encryption Key Manager 配置文件和所有其他相关文件复制到已安装 IBM Security Key Lifecycle Manager V2.6 的目标系统上。
- 编辑 Encryption Key Manager 配置文件，将参数的相对文件路径更改为绝对路径。
- 仅将一个 Encryption Key Manager 服务器迁移到一个 IBM Security Key Lifecycle Manager 服务器。要迁移第二个 Encryption Key Manager，请使用第二个 IBM Security Key Lifecycle Manager 服务器。
- Encryption Key Manager 服务器和接收迁移的数据的 IBM Security Key Lifecycle Manager 服务器必须在相同的主机上。迁移后，IBM Security Key Lifecycle Manager 服务器 会使用 Encryption Key Manager 服务器之前使用的密钥库、TCP 端口和 SSL 端口。
- 迁移需要两个属性:

- **config.keystore.file**
- **TransportListener.ssl.keystore.name**

- 要迁移密钥文件，如果您的 Encryption Key Manager 配置为将密钥组与 LTO 磁带机配合使用，那么请确保 **config.keygroup.xml.file** 属性存在于 Encryption Key Manager 属性文件中，并且指定为绝对路径。

  此属性可能不在该属性文件中，因为 Encryption Key Manager 可能使用从中启动 Encryption Key Manager 的缺省目录中的文件。

注:

您还可以使用跨平台备份实用程序对 IBM Security Key Lifecycle Manager V1.0、V2.0、V2.0.1 和 V2.5 等旧版以及 Encryption Key Manager V2.1 运行备份操作以备份关键数据。您可以在 IBM Security Key Lifecycle Manager V2.6 上将这些备份文件复原到与备份来源不同的操作系统。有关更多信息，请参阅旧版 IBM Security Key Lifecycle Manager 的备份和复原操作。

从 IBM i 系统迁移 Encryption Key Manager

您可能需要先将 Encryption Key Manager 从诸如 IBM i 之类的系统迁移到其他操作系统，然后才能将 Encryption Key Manager 迁移到 IBM Security Key Lifecycle Manager。

请执行以下步骤:

1. 在 IBM i 系统上，密钥必须位于 JCEKS 密钥库中。否则，您必须先将密钥移动到 JCEKS 密钥库。
2. 将必须为新操作系统更新的 JCEKS 密钥库和 Encryption Key Manager 属性文件从 IBM i 系统移至 IBM Security Key Lifecycle Manager V2.6 支持的系统。
3. 使用所移动的密钥库和已修改属性文件在 IBM Security Key Lifecycle Manager V2.6 支持的系统上设置 Encryption Key Manager。
4. 请确保 Encryption Key Manager 能够在新的系统上正常运行。
5. 在安装 IBM Security Key Lifecycle Manager V2.6 的过程中，从新的 Encryption Key Manager 迁移到 IBM Security Key Lifecycle Manager V2.6。您可以仅迁移 Encryption Key Manager V2.1。

注: 要获取 Encryption Key Manager V2.1，请联系 IBM 软件支持，地址为: http://www.ibm.com/software/support

从不受支持的 Linux 操作系统迁移

使用“迁移备份工具”实用程序对 IBM Security Key Lifecycle Manager V2.6 不支持的操作系统 Red Hat Enterprise Linux V4.0、V5.0 和 SuSE Linux Enterprise Server V9.0 上运行的先前版本 V2.0 或 V2.0.1 进行迁移。

迁移过程

必须执行以下步骤才能迁移到 IBM Security Key Lifecycle Manager V2.6:

1. 确保先前版本 V2.0 或 V2.0.1 在不受支持的操作系统上已安装且正在运行。

2. 运行迁移备份工具。请参阅第 30 页的『运行迁移备份工具』。

   此步骤将创建一个迁移备份 JAR 文件。
3. 在受支持的操作系统 Red Hat Enterprise Linux V5.0 或 SuSE Linux Enterprise Server V10 上安装 IBM Security Key Lifecycle Manager 先前版本 V2.0 或 V2.0.1。受支持的操作系统上的用户、密码和安装位置等设置必须类似于不受支持的操作系统上的设置。
4. 将迁移备份 JAR 文件复制到受支持的操作系统上的系统中。
5. 使用图形用户界面或命令行界面对迁移备份 JAR 文件执行复原操作。请参阅第 30 页的『复原迁移备份文件』。
6. 安装 IBM Security Key Lifecycle Manager V2.6 时会检测此系统中预安装的先前版本 V2.0 或 V2.0.1 并运行迁移过程。

迁移备份工具的位置

解压缩 IBM Security Key Lifecycle Manager 安装程序映像 **sklm_v26_linux_64.tar.gz**，可以在 `/disk1/UnsupportedPlatformMig` 文件夹中找到迁移备份工具。请将 **UnsupportedPlatMig.jar** 和 **dbmigbackup.sh** 文件复制到不受支持的操作系统上的系统中。将 **dbtklmrestore.sh** 文件复制到受支持的操作系统上的系统中。

来自迁移备份工具的返回码

迁移备份工具会返回以下某个返回码:

返回码	描述
0	成功
1	指定的备份文件为空、目录或不存在。
2	无法创建临时目录。
3	从备份 jar 解压缩文件时发生 IO 错误。密码可能不正确。
4	读取备份文件中的清单时发生错误。该文件可能不是备份文件。
5	无法读取 TIP 属性。
6	运行迁移数据库备份脚本时发生错误。请检查 `dbmigbackup.log` 文件是否存在问题。
80	删除临时目录时发生错误。
99	用法不正确。参数为备份文件名称和路径（备份的密码）和可选的 `WAS_HOME`（即 TKLM 的安装目录）。
100	发生了意外的异常。

如果返回码为 `0`，那么迁移备份工具会在原始备份 JAR 文件所在的位置创建一个迁移备份 JAR 文件，例如:

`tklm_v2.0.1.0_20130318223754+0530_backup_mig.jar`。

如果返回码不是 `0`，那么请与服务团队联系以获取支持。必须将以下日志文件发送给支持团队:

调试 生成在 `/UnsupportedPlatformMig/logs` 目录中。

dbmigbackup
生成在 `/UnsupportedPlatformMig` 目录中。

运行迁移备份工具

如果 IBM Security Key Lifecycle Manager 先前版本 V2.0 或 V2.0.1 安装在不受支持的操作系统上，那么必须在系统中运行迁移备份工具。运行此工具时，会生成一个迁移备份 JAR 文件。

关于此任务

必须为以下参数指定值:

- 备份文件名和路径
- 备份文件的密码
- WAS_HOME，IBM Security Key Lifecycle Manager 先前版本的安装目录（可选参数）。

过程

1. 下载 IBM Security Key Lifecycle Manager Linux 安装程序映像并将其解压缩。
2. 如果 IBM Security Key Lifecycle Manager 先前版本 V2.0 或 V2.0.1 安装在不受支持的操作系统中，那么请将 **UnsupportedPlatMig_1.0.0.jar** 和 **dbmigbackup.sh** 文件复制到系统中。
3. 设置环境变量 JAVA_HOME 和 CLASSPATH 并运行该工具。

```
export JAVA_HOME=/opt/ibm/java2-i386-50
export PATH=$JAVA_HOME/bin:$PATH
export CLASSPATH=/UnsupportedPlatformMig/UnsupportedPlatMig_1.0.0.jar:
$CLASSPATH
```

示例

```
[root@sourceRHL4U8 /]# cd /UnsupportedPlatformMig/
[root@sourceRHL4U8 UnsupportedPlatformMig]#
java com.ibm.tklm.migration.unsupportedplatmig.MigrationBackup
/Backup/tklm_v2.0.1.0_20130318223754+0530_backup.jar passw0rd
/opt/IBM/tivoli/tiptklmV2/
0
```

下一步做什么

运行复原操作。请参阅『复原迁移备份文件』。

复原迁移备份文件

如果 IBM Security Key Lifecycle Manager 先前版本 V2.0 或 V2.0.1 安装在受支持的操作系统上，那么您必须复原迁移备份 JAR 文件。

开始之前

如果 IBM Security Key Lifecycle Manager 先前版本 V2.0 或 V2.0.1 安装在不受支持的操作系统上，那么请确保在系统中运行迁移备份工具时已创建了迁移备份 JAR 文件。

过程

1. 下载 IBM Security Key Lifecycle Manager Linux 安装程序映像并将其解压缩。
2. 将 **db2tklmrestore.sh** 重命名为 **db2tklmrestore.sh.bkup**

   可以在以下位置找到 **db2tklmrestore.sh** 文件: /disk1/UnsupportedPlatformMig
3. 将 **db2tklmrestore.sh.bkup** 复制到 <tip_home>/products/tklm/bin/db 目录中。

4. 如果 IBM Security Key Lifecycle Manager 先前版本 V2.0 或 V2.0.1 安装在受支持的操作系统上，请将迁移备份 JAR 文件复制到系统中。
5. 使用图形用户界面或命令行界面执行复原操作。

注:

- 如果您是在不受支持的操作系统（Red Hat Enterprise Linux Version 4.0、SuSE Linux Enterprise Server V9.0、AIX 5.3 和 Windows 2003）上使用 V1.0，那么必须首先迁移到 IBM Security Key Lifecycle Manager 先前版本 V2.0 或 V2.0.1。
- 如果 V2.0 或 V2.0.1 安装在受支持的操作系统上，那么 IBM Security Key Lifecycle Manager 安装程序会检测已安装的版本并执行迁移任务。

从不受支持的 Windows、AIX 和 Solaris 操作系统迁移

使用备份和复原操作可对 V2.6 不支持的操作系统上运行的 IBM Security Key Lifecycle Manager 先前版本 V2.0 或 V2.0.1 进行迁移。不受支持的操作系统为 Windows 2003 R2、Windows 2008、Windows 2008 R2、AIX 5.3 和 Sun Server Solaris V9.0。

注:

您可以使用跨平台备份实用程序对 IBM Security Key Lifecycle Manager V1.0、V2.0、V2.0.1 和 V2.5 等旧版以及 Encryption Key Manager V2.1 运行备份操作以备份关键数据。您可以在 IBM Security Key Lifecycle Manager V2.6 上将这些备份文件复原到与备份来源不同的操作系统。有关更多信息，请参阅旧版 IBM Security Key Lifecycle Manager 的备份和复原操作。

迁移过程

必须执行以下步骤才能迁移到 IBM Security Key Lifecycle Manager V2.6:

1. 确保 IBM Security Key Lifecycle Manager 先前版本 V2.0 或 V2.0.1 在不受支持的操作系统上已安装且正在运行。
2. 通过使用图形用户界面或命令行界面在不受支持的操作系统上运行备份操作来为先前版本生成备份文件。
3. 在受支持的操作系统 Windows Server 2008 R2 或 Sun Server Solaris V10 上安装 IBM Security Key Lifecycle Manager 先前版本 V2.0 或 V2.0.1。受支持的操作系统上的用户、密码和安装位置等设置必须类似于不受支持的操作系统上的设置。

   注: 目标系统上的操作系统（其中操作系统版本受支持）必须与源系统的操作系统为同一操作系统（不受支持的操作系统版本）。例如，如果源系统是在 Windows 上运行，那么目标系统也必须是在 Windows 上运行。
4. 将备份文件复制到受支持的操作系统上的系统中。
5. 通过使用图形用户界面或命令行界面在受支持的操作系统上运行备份文件的复原操作。
6. 在受支持的操作系统上安装 IBM Security Key Lifecycle Manager V2.6 会检测此系统中预安装的先前版本 V2.0 或 V2.0.1 并运行迁移过程。

注:

- 如果您在不受支持的操作系统（SuSE Linux Enterprise Server V9.0、AIX 5.3、Solaris 9、Windows 2003 R2、Windows 2008 和 Windows 2008 R2）上使用的是 IBM Secu-

rity Key Lifecycle Manager 先前版本 V1.0，那么必须先迁移到 IBM Security Key Lifecycle Manager 先前版本 V2.0 或 V2.0.1。

- 如果 V2.0 或 V2.0.1 安装在受支持的操作系统上，那么 IBM Security Key Lifecycle Manager 安装程序会检测已安装的版本并执行迁移任务。

操作系统迁移矩阵

下表列出了各种版本的 IBM Security Key Lifecycle Manager 和 Encryption Key Manager V2.1 支持的操作系统:

操作系统	Encryption Key Manager V2.1	Tivoli Key Lifecycle Manager V1.0	Tivoli Key Lifecycle Manager V2.0	Tivoli Key Lifecycle Manager V2.0.1	IBM Security Key Lifecycle Manager V2.5
Windows Server 2003 R2 32 位	✓	✓	✓	✓	
Windows Server 2003 R2 64 位（32 位方式应用程序）	✓	✓	✓	✓	
Windows Server 2008 32 位	✓	✓	✓	✓	
Windows Server 2008 64 位（32 位方式应用程序）	✓	✓	✓	✓	
Windows Server 2008 R2 64 位（32 位方式应用程序）	✓		✓	✓	✓
Windows Server 2012 64 位（32 位方式应用程序）					✓
Windows Server 2012 R2 64 位（32 位方式应用程序）					✓
AIX 5.3 64 位	✓	✓ 使用技术级别 5300-04 和 Service Pack 5300-04-02	✓ 使用技术级别 9 和 Service Pack 2。最低 C++ 运行时级别需要 xlC.rte 9.0.0.8 和 xlC.aix50.rte 9.0.0.8（或更高版本）文件集。这些文件集包含在 June 2008 IBM® C++ Runtime Environment Components for AIX 软件包中。	✓ 使用技术级别 9 和 Service Pack 2。最低 C++ 运行时级别需要 xlC.rte 9.0.0.8 和 xlC.aix50.rte 9.0.0.8（或更高版本）文件集。这些文件集包含在 June 2008 IBM® C++ Runtime Environment Components for AIX 软件包中。	

操作系统	Encryption Key Manager V2.1	Tivoli Key Lifecycle Manager V1.0	Tivoli Key Lifecycle Manager V2.0	Tivoli Key Lifecycle Manager V2.0.1	IBM Security Key Lifecycle Manager V2.5
AIX 6.1 64 位	✓	✓	✓ 使用 AIX 6.1 技术级别 2。最低 C++ 运行时级别需要 xlC.rte 9.0.0.8 和 xlC.aix61.rte 9.0.0.8（或更高版本）文件集。这些文件集包含在 June 2008 IBM C++ Runtime Environment Components for AIX 软件包中。	✓ 使用 AIX 6.1 技术级别 2。最低 C++ 运行时级别需要 xlC.rte 9.0.0.8 和 xlC.aix61.rte 9.0.0.8（或更高版本）文件集。这些文件集包含在 June 2008 IBM C++ Runtime Environment Components for AIX 软件包中。	✓
AIX 7.1 64 位	✓		✓	✓	✓
Sun Server Solaris 9（SPARC 64 位）	✓	✓	✓ 应用补丁 111711-12 和 111712-12（如果使用原始设备），并应用补丁 122300-11。	✓ 应用补丁 111711-12 和 111712-12（如果使用原始设备），并应用补丁 122300-11。	
Sun Server Solaris 10（SPARC 64 位）	✓	✓	✓ 如果使用原始设备，请应用补丁 125100-07。	✓ 如果使用原始设备，请应用补丁 125100-07。	✓
SuSE Linux Enterprise Server V9 on x86（32 位）	✓	✓	✓	✓	
SuSE Linux Enterprise Server V10 on x86（32 位）	✓	✓	✓ SLES10 SP2	✓ SLES10 SP2	
SuSE Linux Enterprise Server V10 x86_64（32 位方式应用程序）	✓	✓	✓ 使用 Service Pack 2	✓ 使用 Service Pack 2	✓
SuSE Linux Enterprise Server V11 on x86	✓		✓	✓	

操作系统	Encryption Key Manager V2.1	Tivoli Key Lifecycle Manager V1.0	Tivoli Key Lifecycle Manager V2.0	Tivoli Key Lifecycle Manager V2.0.1	IBM Security Key Lifecycle Manager V2.5
SuSE Linux Enterprise Server V11 (System z) on x86_64	✓		✓	✓	✓
Red Hat Enterprise Linux AS 4.0 on x86	✓	✓	✓	✓	
Red Hat Enterprise Linux 5.0 on x86	✓	✓	✓ 使用 Update 2	✓	
Red Hat Enterprise Linux 5.0 on x86_64（32 位方式应用程序）	✓	✓	✓ 使用 Update 2	✓	✓
Red Hat Enterprise Linux 5.0 (System z) on x86_64	✓		✓	✓ 使用 Update 1	✓
Red Hat Enterprise Linux 6 on x86	✓				
Red Hat Enterprise Linux 6 on x86_64	✓				✓
Red Hat Enterprise Linux 6 (System z) on x86_64	✓				✓
要从不受支持的 Linux 操作系统迁移，请参阅第 28 页的『从不受支持的 Linux 操作系统迁移』主题。					

获取 Encryption Key Manager

您只能将 Encryption Key Manager V2.1 迁移到 IBM Security Key Lifecycle Manager V2.6。

关于此任务

如果您使用的是 Encryption Key Manager 的先前版本，请升级到 V2.1。要获取 Encryption Key Manager V2.1，请联系 IBM 软件支持，地址为: http://www.ibm.com/software/support

Encryption Key Manager 的迁移限制

可以从 Encryption Key Manager 迁移哪些内容具有特定限制。

- 迁移管理员 SSL 密钥库和信任库不受支持。IBM Security Key Lifecycle Manager 服务器不支持管理员同步功能。
- 迁移 PKCS11Impl 密钥库和信任库不受支持。IBM Security Key Lifecycle Manager 服务器不支持 PKCS11Impl 密钥库。
- IBM Security Key Lifecycle Manager 不支持在多个组中使用密钥，不同于支持在多个组中使用密钥的 Encryption Key Manager。

将 KeyGroup.xml 中的密钥数据从 Encryption Key Manager 迁移到 IBM Security Key Lifecycle Manager 时，每个密钥都连接到一个组。仅在 IBM Security Key Lifecycle Manager 中的一个组中创建之前在 Encryption Key Manager 中的多个组中的密钥。

迁移过程会记录未在多个组中创建密钥的事件，并继续。如果 symmetricKeySet 属性指定了列表、范围或密钥，而不是组，那么 symmetricKeySet 指定的所有密钥都迁移到名称为 DefaultMigrateGroup 的密钥组。如果作为其他组的一部分来创建 symmetricKeySet 中的密钥，并且名称为 DefaultMigrateGroup 的密钥组为空，那么 IBM Security Key Lifecycle Manager 不会创建 DefaultMigrateGroup 密钥组，并且不会迁移 symmetricKeySet 属性。

要解决该问题，请使用 IBM Security Key Lifecycle Manager 图形或命令行界面为 LTO 磁带机 等定义缺省密钥组。

迁移 Encryption Key Manager 后

迁移 Encryption Key Manager 后，必须验证配置并保护数据。

- 不要运行 Encryption Key Manager。迁移后，Encryption Key Manager 保留了提供密钥的功能。
- 使用证书和密钥来解决可能的问题。

  Encryption Key Manager 不会限制证书及其密钥可以与其进行关联的设备组。迁移到 IBM Security Key Lifecycle Manager V2.6 之后，属于多个设备类型的证书和密钥将标记为 CONFLICTED。您无法将它们的设备组更改为另一个设备组。IBM Security Key Lifecycle Manager 可以使用标记为 CONFLICTED 的证书或密钥进行读写操作。

  迁移可能还会导致证书在 IBM Security Key Lifecycle Manager 图形用户界面中显示带有 UNKNOWN 标签。
  - 未知证书可用作回滚证书。作为回滚进行调度后，未知证书将更新为回滚的特定设备组。带有 UNKNOWN 标签的 SSL 服务器证书会更新为 SSL 证书。
  - 暂挂的证书可能与具有 UNKNOWN 状态的设备组一起列出在图形用户界面上。首先，接受暂挂证书，然后该证书将具有 UNKNOWN 状态。然后，使用 **tklmCertUpdate** 命令将证书使用情况更新到特定的设备组。该更新将证书状态更改为诸如“有效”之类的状态
  - 迁移完成后，一个或多个设备可能与 UNKNOWN 设备组相关联。您可以将 UNKNOWN 设备的设备组指定为新组，或允许在这些设备发出第一个密钥服务请求时确定该组。

  使用 **tklmCertList** 命令可查找标记为 CONFLICTED 或 UNKNOWN 的证书。不指定 **-usage** 参数的值，或者指定参数值 3592、DS8000 或 SSLSERVER。例如，以下 Jython 格式的命令列出了 3592 设备组的所有证书:

  ```
  print AdminTask.tklmCertList('[-usage 3592 -v y]')
  ```

- 请验证迁移的 Encryption Key Manager 配置是否已处于您期望的状态，然后再对 IBM Security Key Lifecycle Manager 进行任何更新或配置更改。

  迁移完成后，Encryption Key Manager 配置密钥库将成为 IBM Security Key Lifecycle Manager 密钥库。不能将 Encryption Key Manager 服务器数据第二次迁移到相同的 IBM Security Key Lifecycle Manager 服务器。

如果迁移失败，并且您选择完成剩余的 IBM Security Key Lifecycle Manager 安装流程，那么只有在还未对 IBM Security Key Lifecycle Manager 配置进行任何更新或更改时才能启动独立迁移恢复脚本。有关更多信息，请参阅第 73 页的『从故障迁移恢复』。

迁移 IBM Security Key Lifecycle Manager 后

迁移 IBM Security Key Lifecycle Manager 后，必须验证配置并保护数据。

- 安装 IBM Security Key Lifecycle Manager V2.6 之后，请立即对 IBM Security Key Lifecycle Manager V2.6 运行备份操作。如果使用 CLI 命令、图形用户界面或 REST 接口创建了备份文件，那么无法将先前版本的备份复原到 V2.6 环境。

  迁移到 V2.6 不会除去 IBM Security Key Lifecycle Manager 的先前版本。为避免端口冲突，不得同时运行两个版本。

  注：在 Windows 平台上，将 IBM Security Key Lifecycle Manager 先前版本（1.0、2.0、2.0.1 或 2.5）迁移到 V2.6 之后，如果在卸载先前版本之前卸载 IBM Security Key Lifecycle Manager V2.6，那么与先前版本关联的 DB2 可能不会启动。

  如果迁移失败，并且选择完成剩余的 IBM Security Key Lifecycle Manager 安装过程，那么只有在尚未对 IBM Security Key Lifecycle Manager 配置进行任何更新或更改时才能启动独立迁移恢复脚本。有关更多信息，请参阅第 73 页的『从故障迁移恢复』。必须先完成迁移恢复过程，然后才能使用 IBM Security Key Lifecycle Manager V2.6。
- 保留但不运行 IBM Security Key Lifecycle Manager 先前版本的副本，以确保在验证确定 V2.6 有问题的情况下具有先前版本的环境和数据。
- 使用证书和密钥来解决可能的问题。

  IBM Security Key Lifecycle Manager 先前版本 V1.0、V2.0、V2.0.1 或 V2.5 不限制证书及其密钥可以关联到的设备组。在 V1.0、V2.0、V2.0.1 或 V2.5 中属于多个设备类型的证书和密钥在 V2.6 中标记为 `CONFLICTED`。您无法将它们的设备组更改为另一个设备组。IBM Security Key Lifecycle Manager 可以使用标记为 `CONFLICTED` 的证书或密钥进行读写操作。
- 迁移完成后，一个或多个设备可能与 `UNKNOWN` 设备组相关联。您可以将 `UNKNOWN` 设备的设备组指定为新组，或允许在这些设备发出第一个密钥服务请求时确定该组。
- 将 IBM Security Key Lifecycle Manager 先前版本迁移到 V2.6 完成后，迁移程序将不会除去先前版本。要除去先前版本，请遵循已作为迁移源的产品版本的卸载指示信息。

  注：因为 IP 端口在两个版本间共享，所以请勿同时运行两个版本。如果迁移无法完成这些步骤，那么迁移过程会发出警告消息以及已成功完成消息。检查 *<IM App Data Dir>*`/logs/sklmLogs/migration.log` 文件中的消息并执行相应的手动操作。
- 在 IBM Security Key Lifecycle Manager 先前版本中出于将来用于管理的目的，您可能已将证书标记为用作 3592 回滚条目，也可能已将密钥组标记为用作 LTO 回滚条目。如果为回滚安排的将来日期早于迁移时间，那么迁移程序会添加相应的消息并且不迁移这些回滚项。成功安装 IBM Security Key Lifecycle Manager V2.6 之后，使用命令行界面或图形用户界面来手动添加这些回滚条目。

- 您无法使用图形用户界面删除通过命令行界面使用 **tklmCertDefaultRolloverAdd** 或 **tklmKeyGroupDefaultRolloverAdd** 命令添加的已迁移滚动更新。 使用命令行界面可删除使用命令行界面创建的已迁移滚动更新。
- 确保主 IBM Security Key Lifecycle Manager V2.6 已配置且处于正常运行状态，备份 IBM Security Key Lifecycle Manager 服务器 V2.6 并在副本计算机上安装备份。
  - 验证 V2.6 副本计算机是否已配置且处于正常运行状态。
  - 在 IBM Security Key Lifecycle Manager V2.6 目录路径以外的其他位置中保留 V2.6 备份文件的副本。独立的位置可以确保如果除去了 IBM Security Key Lifecycle Manager，其他进程无法除去备份文件。

    此外，请保留 *<IM App Data Dir>*/logs/sklmLogs/migration.log 文件以便将来参考。

从 Encryption Key Manager 迁移的数据对象和属性

还将从 Encryption Key Manager 迁移数据对象和属性。

Encryption Key Manager 配置文件中必须具有的属性包括:

- Audit.metadata.file.name

  文件必须存在于配置文件本身所处的相同目录中，并且必须已启用读操作。
- config.drivetable.file.url

  文件必须存在于配置文件本身所处的相同目录中，并且必须已启用读操作。
- config.keystore.file

  文件必须存在于配置文件本身所处的相同目录中，并且必须已启用写操作。
- config.keystore.password.obfuscated
- config.keystore.type

  密钥库类型不能为 PKCS11IMPLKS。
- TransportListener.ssl.keystore.name

  文件必须存在于配置文件本身所处的相同目录中，并且必须已启用读操作。
- TransportListener.ssl.keystore.password.obfuscated
- TransportListener.ssl.keystore.type

  密钥库类型不能为 PKCS11IMPLKS。
- TransportListener.ssl.port

  该值必须是 1 和 65535 之间的正整数，并且不能等于 TransportListener.tcp.port 的值。
- TransportListener.ssl.truststore.type

  密钥库类型不能为 PKCS11IMPLKS。
- TransportListener.tcp.port

  该值必须是 1 和 65535 之间的正整数，并且不能等于 TransportListener.ssl.port 的值。

迁移包含以下数据对象:

密钥库 IBM Security Key Lifecycle Manager 在数据库中存储所有密钥和证书。迁移期间，两个 Encryption Key Manager 密钥库 `Config` 和 `TransportListner` 中的密钥和证书将全部复制到 IBM Security Key Lifecycle Manager 数据库中。将从 `Config` 密钥库复制密钥和证书。将从 `TransportListner` 信任库复制证书。

来自 `TransportListener` 密钥库的某个证书将设置为 IBM Security Key Lifecycle Manager 的 SSL 证书。**`config.keystore.ssl.certalias`** 属性将使用此证书的别名进行更新。

不会使用其他 Encryption Key Manager 密钥库。

设备 从 config.drivetable.file.url 属性指向的驱动表读取所有设备信息，将在 IBM Security Key Lifecycle Manager 数据库中输入这些设备信息。如果驱动器具有已定义的 symalias 属性，那么该驱动器类型设置为 LTO。如果驱动器具有已定义的别名，那么驱动器类型设置为 3592。迁移为不具有这些已定义的属性并且不具有已确定的类型的驱动器设置类型 UNKNOWN。

密钥组 解析由 config.keygroup.xml.file 属性指向的 keygroup.xml 文件，并将密钥组信息存储在 IBM Security Key Lifecycle Manager 数据库中。还将迁移所有组成员和组关系。

如果 symmetricKeySet 属性具有别名列表或具有一系列别名，那么将创建名称为 DefaultMigrationGroup 的缺省密钥组，所有别名都将作为该组的成员。在此情况中，symmetricKeySet 属性设置为 DefaultMigrationGroup。如果 symmetricKeySet 属性已是组别名，那么不会创建缺省迁移组。

元数据 由 Audit.metadata.file.name 属性指向的所有元数据信息都将迁移到 IBM Security Key Lifecycle Manager 数据库中。

从 Encryption Key Manager 配置文件迁移到 SKLMConfig.properties 文件的属性可能包括:

- Audit.eventQueue.max
- Audit.handler.file.size
- Audit.event.outcome
- Audit.event.types
- config.keystore.name（设置为 `defaultKeyStore`）
- cert.valiDATE
- drive.acceptUnknownDrives 作为指定设备组中的缺省项迁移到数据库中。
- fips
- TransportListener.ssl.ciphersuites
- TransportListener.ssl.clientauthentication
- TransportListener.ssl.port
- TransportListener.ssl.protocols
- TransportListener.ssl.timeout
- TransportListener.tcp.port
- TransportListener.tcp.timeout
- useSKIDefaultLabels

- zOSCompatibility

以下属性**将**从 Encryption Key Manager 配置文件迁移到 IBM Security Key Lifecycle Manager 数据库:

- **drive.default.alias1**
- **drive.default.alias2**
- **symmetricKeySet**（设置为已指定的组别名，或设置为 **DefaultMigrationGroup**）

从 IBM Security Key Lifecycle Manager 迁移的数据对象和属性

还将从 IBM Security Key Lifecycle Manager 先前版本 V1.0、V2.0、V2.0.1 和 V2.5 迁移数据对象和属性。

密钥库 密钥库（包括先前版本中的所有证书和元数据）会添加到 IBM Security Key Lifecycle Manager V2.6 数据库中。密钥库由 SKLMConfig.properties 文件中的 **config.keystore.name** 属性确定。

设备 从 IBM Security Key Lifecycle Manager 数据库读取所有设备信息。

密钥组 从 IBM Security Key Lifecycle Manager 数据库读取密钥组信息。

回滚证书和密钥组

可能会对来自先前版本的证书和密钥组进行标记以便将来的 3592 管理。迁移程序会检测并标记这些回滚，以便将来使用 IBM Security Key Lifecycle Manager V2.6 进行管理。

元数据 所有元数据信息都迁移自先前版本数据库，并且可供 IBM Security Key Lifecycle Manager V2.6 数据库使用。

属性 SKLMConfig.properties 文件中的属性是从 IBM Security Key Lifecycle Manager 数据库迁移过来的。将迁移 `datastore.properties` 文件。

在 SKLMConfig.properties V2.6 文件中会替换以下属性:

- **ds8k.acceptUnknownDrives**

  device.AutoPendingAutoDiscovery 属性将替换此属性。
- **drive.acceptUnknownDrives**

  IBM Security Key Lifecycle Manager 数据库中的 **device.AutoPendingAutoDiscovery** 属性将替换此属性。

以下 IBM Security Key Lifecycle Manager V2.0.1 属性已过时，不会进行迁移:

- **tklm.internal.gui.jagworkflow**
- **tklm.internal.gui.lto4workflow**

这些属性从 SKLMConfig.properties V2.6 文件迁移到 IBM Security Key Lifecycle Manager 数据库:

- **drive.default.alias1**
- **drive.default.alias2**
- **symmetricKeySet**（已从 SKLMConfig.properties 文件中除去并替换为表示 IBM Security Key Lifecycle Manager 数据库中设备组的条目）

安装类型

有多个用于安装 IBM Security Key Lifecycle Manager 的选项。

在分布式系统上，您可以使用以下一种安装方式:

- 基于图形用户界面的安装，由向导驱动。
- 静默安装，在无人照管的情况下运行，使用响应文件来指定配置选项。

注: IBM Security Key Lifecycle Manager 不支持控制台方式的安装。

在 Red Hat Enterprise Linux 系统上安装所需的库

在运行针对图形或静默安装方式的安装命令之前，必须先在 x86 64 位 Red Hat Enterprise Linux V6.0 和 Red Hat Enterprise Linux V7.0 系统上安装必需的库。

过程

1. 将 Red Hat Enterprise Linux 6.0/6.1 分发版 DVD 安装到系统。将该 DVD 插入 DVD 驱动器中。
2. 以 root 用户身份打开终端窗口。
3. 执行以下命令:

   ```
   [root@localhost]# mkdir /mnt/cdrom
   [root@localhost]# mount -o ro /dev/cdrom /mnt/cdrom
   ```

4. 在 /etc/yum.repos.d 目录中创建文本文件 server.repo。

   注: 要使用 gedit:

   a. 请执行以下命令:

      ```
      [root@localhost]# gedit /etc/yum.repos.d/server.repo
      ```

   b. 将以下文本添加至该文件:

      ```
      [server]
      name=server
      baseurl=file:///mnt/cdrom/Workstation
      enabled=1
      ```

      其中 baseurl 取决于安装点和 Red Hat Enterprise Linux 分发版。

      在此示例中，安装点是 cdrom，而 Red Hat Enterprise Linux 分发版是 Workstation，但是也可以是 sever。

5. 执行命令:

   ```
   [root@localhost]# yum clean all
   ```

6. 执行以下命令以导入相关的公用密钥:

   ```
   [root@localhost]# rpm --import /mnt/cdrom/*GPG*
   ```

7. 执行以下命令以安装必需的库:

   ```
   [root@localhost]# yum install gtk2.i686
   [root@localhost]# yum install libXtst.i686
   ```

如果您收到上述关于缺少 libstdc++ 的消息，请安装 libstdc++ 库:

```
[root@localhost]# yum install compat-libstdc++
```

在安装期间，可能会收到与示例类似的提示。请回答“y”。

示例:

```
Total download size: 15 M
Installed size: 47 M
Is this ok [y/N]: y
```

注: 命令中的软件包扩展名 (.i686) 可能有所不同，这取决于您所使用的硬件平台。下表列出了有效的软件包扩展名值。不同平台上的 Red Hat Enterprise Linux 6.0 软件包扩展名:

平台	32 位	64 位
x86/x86_64	i686	x86_64
ppc/ppc64	ppc	ppc64
s390/s390x	s390	s390x

安装程序的语法和参数

必须使用安装命令来安装 IBM Security Key Lifecycle Manager。

静默安装

```
silent_install.sh full_path_to_response_file
```

silent_install.bat（在 Windows 系统上）。

silent_install.sh（在诸如 Linux 或 AIX 等系统上）。

图形方式安装

```
install_program
```

其中 *install_program* 是

launchpad.exe（在 Windows 系统上）。

launchpad.sh（在诸如 Linux、Linux for System z 或 AIX 等系统上）。

注: 请不要从网络驱动器或装配驱动器进行安装。例如，请不要指定以下任一 **net use** 语句作为目录位置并尝试安装:

```
net use z: \\server\share
net use \\server\share
```

图形方式安装

IBM Security Key Lifecycle Manager 提供了图形用户界面安装程序。IBM Installation Manager 用于安装 IBM Security Key Lifecycle Manager 及其组件。它提供了一系列面板，这些面板会提示您提供安装所需的信息。

以下步骤以图形方式安装 IBM Security Key Lifecycle Manager。

- 启动安装向导。
- 通过输入配置选项完成各个安装向导页面。有关详细信息，请参阅第 47 页的『分布式系统上的安装』。

- 验证 IBM Security Key Lifecycle Manager 服务器是否可运行。有关详细信息，请参阅第 90 页的『验证安装』。

用于启动图形安装的命令

要启动安装向导，请浏览至已存储安装文件的目录并运行安装命令。

install_program

其中 *install_program* 是:

launchpad.exe（在 Windows 系统上）。

launchpad.sh（在诸如 Linux、Linux for System z 或 AIX 等系统上）。

有关安装程序语法和标志的详细信息，请参阅第 42 页的『安装程序的语法和参数』。

安装和迁移面板

以图形方式安装 IBM Security Key Lifecycle Manager 需要您启动安装向导，浏览一系列安装面板并提供必需信息。

在安装期间，您可能会看到以下面板:

1. 语言选择和简介
2. 包含安装软件包（例如 IBM Installation Manager、IBM DB2、IBM WebSphere Application Server 和 IBM Security Key Lifecycle Manager）的 Installation Manager 窗口
3. 软件许可协议
4. 选择 IBM Installation Manager 和其他安装软件包的安装目录。
5. 选择软件包翻译语言
6. 选择要安装的软件包功能部件
7. DB2 配置选项
8. IBM Security Key Lifecycle Manager 配置选项
9. Encryption Key Manager 迁移选择
10. 安装软件包预览
11. IBM Security Key Lifecycle Manager 的安装进度
12. 安装摘要

注意:

- 当您安装 IBM Security Key Lifecycle Manager 时，请保持**共享资源目录**的缺省路径。IBM Installation Manager 使用此位置下载工件和存储关于已安装软件包的信息。
- 安装完成后，将出现一个页面，其中显示安装状态和已安装软件包的列表。必须选择**无**以指示安装程序不创建概要文件，然后单击**完成**。

在安装期间进行迁移时，您可能会看到以下面板:

1. 语言选择
2. 简介
3. 软件许可协议
4. DB2 目录

5. **迁移信息**
6. **迁移摘要**
7. 必备软件的摘要
8. DB2 的安装进度
9. 开始 IBM Security Key Lifecycle Manager 安装
10. IBM Security Key Lifecycle Manager 和 WebSphere Application Server 的安装目录
11. WebSphere Application Server 信息
12. SKLMAdmin 密码
13. 安装前摘要
14. IBM Security Key Lifecycle Manager 的迁移进度
15. 安装摘要

静默安装

静默式安装是非交互式安装，由提供安装设置的响应文件驱动。

静默安装期间无需用户输入任何信息。在诸如数据中心的环境中，要在多个相同系统上安装 IBM Security Key Lifecycle Manager，此安装类型非常有用。

注: 静默方式安装使用可能包含密码信息的响应文件。要提高安全性，请在安装 IBM Security Key Lifecycle Manager 后立即删除响应文件。

您必须将加密密码添加到响应文件的相关元素。使用 IBM Installation Manager 实用程序来创建加密密码。

Windows

例如，如果将 IBM Security Key Lifecycle Manager 产品映像抽取到 C:\SKLM\disk1 目录，请运行以下命令来创建加密密码。

```
cd C:\SKLM\disk1\im\tools
imcl.exe encryptString password
```

添加您在响应文件中创建的加密密码，如以下示例中所示。

```
<data key='user.DB2_ADMIN_PWD,com.ibm.db2.ofng'
value='<encrypted password>'/>
<data key='user.CONFIRM_PASSWORD,com.ibm.db2.ofng'
value='<encrypted password>'/>
...
<data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm.win32'
value='<encrypted password>'/>
<data key='user.WAS_ADMIN_CONF_PWD,com.ibm.sklm.win32'
value='<encrypted password>'/>
...
<data key='user.SKLM_ADMIN_PASSWORD,com.ibm.sklm.win32'
value='<encrypted password>'/>
<data key='user.SKLM_ADMIN_CONF_PWD,com.ibm.sklm.win32'
value='<encrypted password>'/>
```

Linux 例如，如果将 IBM Security Key Lifecycle Manager 产品映像抽取到 /SKLM/disk1 目录，请运行以下命令来创建加密密码。

```
cd /SKLM/disk1/im/tools
./imcl encryptString password
```

添加您在响应文件中创建的加密密码，如以下示例中所示。

```
<data key='user.DB2_ADMIN_PWD,com.ibm.db2.aix.ofng'
value='<encrypted password>'/>
<data key='user.CONFIRM_PASSWORD,com.ibm.db2.aix.ofng'
value='<encrypted password>'/>
...
<data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm.aix'
value='<encrypted password>'/>
<data key='user.WAS_ADMIN_CONF_PWD,com.ibm.sklm.aix'
value='<encrypted password>'/>
...
<data key='user.SKLM_ADMIN_PASSWORD,com.ibm.sklm.aix'
value='<encrypted password>'/>
<data key='user.SKLM_ADMIN_CONF_PWD,com.ibm.sklm.aix'
value='<encrypted password>'/>
```

可以为每个用户创建不同的加密密码。

要使用响应文件以静默方式启动安装程序，请输入以下命令:

`silent_install.sh` *full_path_to_response_file*

silent_install.bat（在 Windows 系统上）。

silent_install.sh（在诸如 Linux 或 AIX 等系统上）。

注: 如果为 *full_path_to_response_file* 参数输入无效值（例如不完整的路径），那么安装程序将退出。不会显示或记录任何错误消息。

样本响应文件

IBM Security Key Lifecycle Manager 包含多个样本响应文件，创建您自己的响应文件时可将这些样本文件用作模板。在使用样本文件之前，必须先根据您环境的具体情况进行修改。

样本响应文件位于安装软件包所在的目录中。

- 第 95 页的『在 Windows 系统上新安装 V2.6』
- 第 96 页的『在 Linux 系统上新安装 V2.6』
- 第 98 页的『在 Linux for System z 上新安装 V2.6』
- 第 99 页的『在 AIX 系统上新安装 V2.6』
- 第 100 页的『在 Windows 系统上从先前版本迁移到 V2.6』
- 第 102 页的『在 Linux 系统上从先前版本迁移到 V2.6』
- 第 103 页的『在 Linux for System z 上将先前版本迁移到 V2.6』
- 第 105 页的『在 AIX 系统上从先前版本迁移到 V2.6』
- 第 106 页的『Windows 系统上的卸载』
- 第 107 页的『Linux 系统上的卸载』
- 第 107 页的『Linux for System z 上的卸载』
- 第 107 页的『AIX 系统上的卸载』

分布式系统上的安装

以图形方式安装期间，系统将提示您输入安装 IBM Security Key Lifecycle Manager 及其使用的必备软件所需的配置信息。

注意：请记住以下几项重要注意事项:

- 安装时间可能会超过一小时。
- 请不要从网络驱动器或装配驱动器进行安装。例如，请不要指定以下任一 *net use* 语句作为目录位置并尝试安装:

  ```
  net use z: \\server\share
  net use \\server\share
  ```

- 请确保在安装期间出现提示时选择正确的语言。更正语言环境错误需要卸载并重新安装 IBM Security Key Lifecycle Manager 和 DB2。
- 安装 IBM Security Key Lifecycle Manager 时，指定的 DB2 密码必须遵守底层操作系统的密码策略。
- 如果您是使用现有用户作为 DB2 管理员，请确保正确指定密码。
- 在诸如 Linux 之类的系统上安装 IBM Security Key Lifecycle Manager 时，安装期间进行的某些 DB2 配置更改可能需要重新启动系统。在您重新启动系统之前，请关闭任何其他应用程序。在系统重新启动之后，请再次运行安装程序。
- 确保正确设置系统的主机名。
- 所有字段的输入内容只能为字母字符（A-Z 和 a-z）、数字字符 (0-9) 和下划线字符 (_)。该限制也适用于静默安装所用响应文件中的值。
- 确保安装路径中不包含 Unicode 字符。
- 确保安装路径中不包含非 ASCII 字符。
- 如果在环境中具有 IBM Security Key Lifecycle Manager 先前版本，请在安装和迁移到 V2.6 之前考虑以下准则:
  - 获取 IBM Security Key Lifecycle Manager 先前版本的管理员密码。
  - 向 IBM Security Key Lifecycle Manager 先前版本应用最新的修订包。
  - 在 Windows 系统上，请确保 IBM ADE Service 已启动。

    在 Windows 系统上，请打开“服务”控制台。验证 IBM ADE Service 是否已启动。如果该服务未启动，请选择并启动该服务。

安装期间的 DB2 配置

IBM Security Key Lifecycle Manager 要求 DB2 工作组服务器版 为某个 V10.5.0.6 级别，具体级别取决于操作系统。

安装程序将运行以下一项操作:

- 如果已在正确的操作系统的版本上以 root 用户身份安装了 DB2 工作组服务器版 副本，那么可以使用此现有的 DB2 工作组服务器版。IBM Security Key Lifecycle Manager 安装程序未检测到存在 DB2。必须指定 DB2 安装路径。

您还可以安装新的 DB2 工作组服务器版 副本。现有的 DB2 必须安装在系统本地，而不能安装在网络驱动器或共享驱动器上。

在 Windows 系统上，如果安装了新的 DB2 副本，那么 DB2_COPY_NAME 会设置为 DBSKLMV26。

- 如果系统上存在 IBM Security Key Lifecycle Manager 先前版本和 DB2 先前版本，那么该过程会以 V10.5.0.6 级别安装 DB2 工作组服务器版，具体视操作系统而定。您还可以使用其他已安装且级别正确的现有 DB2 10.5.0.6 版本。

  安装过程还会将数据从先前版本的 IBM Security Key Lifecycle Manager 迁移到新版本。例如:

  – 新的 DB2 工作组服务器版 副本将使用先前的 db2admin 用户标识和密码。
  – 在 Windows 系统上，如果安装了新的 DB2 副本，那么 DB2_COPY_NAME 会设置为 DBSKLMV26。
- 如果系统上既不存在 IBM Security Key Lifecycle Manager，也不存在 DB2 的副本或先前版本，那么安装过程将以 V10.5.0.6 级别进行安装，具体视操作系统而定。

  不会进行任何 DB2 升级。

在 DB2 配置期间，系统将提示您输入以下信息，实际信息可能与以下列表有所不同，这取决于操作系统以及 IBM Security Key Lifecycle Manager 要安装新的 DB2 还是使用现有副本:

DB2 选择

DB2 安装目录。

在诸如 AIX 或 Linux 等系统上，该条目的起点必须为根目录。该条目中的第一个字符必须为正斜杠（“/”）。

安装过程会提供缺省值。请参阅第 5 页的『*HOME* 和其他目录变量的定义』。

DB2 管理员标识

本地 DB2 管理员用户标识。安装过程会提供具有必要许可权的缺省管理员用户标识。请不要将域用户标识用作 DB2 管理员。不要指定长度大于 8 个字符的用户标识。

注: 指定 DB2 的现有副本的用户标识时，不要使用连字符 (-) 或下划线 (_) 字符。

在 Windows 系统上，DB2 管理员用户标识必须是 Administrator 组的成员。该用户标识必须符合 Windows 系统上活动的安全策略。

在诸如 Linux 或 AIX 等系统上，IBM Security Key Lifecycle Manager DB2 实例所有者的用户标识必须也是 root 用户标识所属组的成员。如果 bin 可用，请使用 bin 作为该组。如果 bin 不可用，请向系统管理员询问要使用的通用组的名称。

注: 管理员标识不能是 DB2 保留字，例如 db2、users、admins、guests、public、private、properties、local 或 root。

DB2 管理员密码

管理员的密码。最大长度为 20 个字符。

DB2 管理员用户标识的密码必须符合系统上的活动安全策略。此外，DB2 管理员用户标识的登录密码和该用户标识的 DB2 密码必须相同。更改其中之一时，必须更改另一个。

注: 如果您是使用现有用户作为 DB2 管理员，请确保安装期间正确指定密码。

数据库名称

IBM Security Key Lifecycle Manager 数据库的名称，即 SKLMDB26。

DB2 端口

DB2 使用的端口。

管理员组

管理员用户标识所在的访问组。如果 DB2 位于 AIX 或 Linux 等系统上，您的用户标识必须位于 bin 或 root 用户组中，或者位于其成员包含 root 用户的其他组中。

管理员主目录/数据库主目录

在其中创建 IBM Security Key Lifecycle Manager 所使用数据库实例和格式化表的目录（AIX 或 Linux 系统）或驱动器（Windows 系统）。

注意:

- 所有字段的输入内容只能为字母字符（A-Z 和 a-z）、数字字符 (0-9) 和下划线字符 (_)。该限制也适用于静默安装所用响应文件中的值。
- 请不要在任何目录路径或文件名中指定空格。
- 在其中安装 DB2 的计算机的名称不能以“ibm”、“sql”、或“sys”开头，无论大小写。该计算机的名称也不能包含下划线字符 (_)。
- 如果您是使用现有用户作为 DB2 管理员，请确保安装期间正确指定密码。

Windows 系统上的 DB2 密码安全性问题

在 Windows 系统上，DB2 管理员用户标识和密码必须符合系统上的活动安全策略。

如果存在已生效的密码有效期限制，那么必须在超过有效期之前更改管理员用户标识的登录密码和 DB2 密码。

此外，DB2 管理员用户标识的登录密码和 WebSphere Application Server 使用的 DB2 数据源密码必须相同。更改其中之一时，必须更改另一个。

要更改 DB2 数据库密码，请执行以下步骤:

1. 停止 WebSphere Application Server 及*所有*与 DB2 相关的 Windows 服务。
2. 打开控制面板并单击**管理工具 > 计算机管理 > 本地用户和组 > 用户**以打开 Windows 用户管理工具。
3. 更改 IBM Security Key Lifecycle Manager 数据库所有者的密码。
4. 打开控制面板并单击**管理工具 > 计算机管理**以打开“Windows 服务”控制台。
5. 在以下服务上，使用**属性**对话框的**登录**选项卡更改密码:
   - DB2 - DBSKLMV26 - *sklminstance*

     例如，*sklminstance* 的值可能是:

     ```
     DB2 - DBSKLMV26 - DBSKLM26
     DB2 - DBSKLMV26 - SKLMDB26
     ```

例如，使用缺省实例名称时，*sklminstance* 的值可能是:

```
DB2 - DBSKLMV26 - SKLMDB26
```

- DB2 Governor (DBSKLMV26)
- DB Remote Command Server (DBSKLMV26)
- DB2DAS - DB2DAS00

所有服务的密码均已更改时，请重新启动这些服务。

必须停止并重新启动以下服务。无须更改密码:

- DB2 License Server (DBSKLMV26)
- DB2 Management Service (DBSKLMV26)

6. 启动 WebSphere Application Server。
7. 使用 WebSphere Application Server 提供的 **wsadmin** 界面指定 Jython 语法。

   ```
   wsadmin -username WASAdmin -password mypwd -lang jython
   ```

8. 使用 **wsadmin** 命令更改 WebSphere Application Server 数据源的密码:
   a. 以下命令列出了 JAASAuthData 条目:

      ```
      wsadmin>print AdminConfig.list('JAASAuthData')
      ```

      结果可能为:

      ```
      (cells/SKLMCell|security.xml#JAASAuthData_1379859888963)
      ```

   b. 识别其别名与字符串 sklm_db 相匹配的数据源标识。另外，识别其别名与字符串 sklmdb 相匹配的数据源标识:

      ```
      print AdminConfig.showAttribute('JAASAuthData_list_entry', 'alias')
      ```

      例如，在一行上输入:

      ```
      print AdminConfig.showAttribute
      ('(cells/SKLMCell|security.xml#JAASAuthData_1379859888963)', 'alias')
      ```

      结果为:

      ```
      sklm_db
      ```

   c. 更改 sklm_db 别名的密码，并在一行上输入以下命令:

      ```
      print AdminConfig.modify('JAASAuthData_list_entry',
        '[[password newpassword]]'
      ```

      如果在密码中指定特殊字符，请在指定密码值时使用引号作为定界符。

      例如，在一行上输入:

      ```
      print AdminConfig.modify
      ('(cells/SKLMCell|security.xml#JAASAuthData_1379859888963)',
      '[[password tucs0naz]]')
      ```

   d. 保存更改:

      ```
      print AdminConfig.save()
      ```

   e. 使用 **stopServer** 和 **startServer** 命令停止并重新启动 IBM Security Key Lifecycle Manager 服务器。

      或者，通过使用 Windows 计算机管理来停止并重新启动 IBM Security Key Lifecycle Manager 服务器。

1) 打开控制面板并单击**管理工具 > 计算机管理 > 服务和应用程序 > 服务**。
2) 停止然后启动其名称类似于 IBM WebSphere Application Server V8.5 - SKLM26Server 的 IBM Security Key Lifecycle Manager 服务器服务。

f. 验证是否可以使用 WebSphere Application Server 数据源连接到数据库。

1) 首先，请输入:

```
print AdminConfig.list('DataSource')
```

结果可能为:

```
"Default Datasource(cells/SKLMCell/nodes/SKLMNode/servers/server1|
resources.xml#DataSource_1183122153625)"
"SKLM DataSource(cells/SKLMCell/nodes/SKLMNode/servers/server1|
resources.xml#DataSource_1379859893896)"
"SKLM scheduler XA Datasource(cells/SKLMCell/nodes/SKLMNode/servers/
server1|resources.xml#DataSource_1379859896273)"
DefaultEJBTimerDataSource(cells/SKLMCell/nodes/SKLMNode/servers/
server1|resources.xml#DataSource_1000001
```

2) 在第一个数据源上测试连接。例如，输入:

```
print AdminControl.testConnection('SKLM DataSource(cells....)')
```

例如，在一行上输入:

```
print AdminControl.testConnection
('(SKLM DataSource(cells/SKLMCell/nodes/SKLMNode/servers/server1|
resources.xml#DataSource_1379859893896)')
```

3) 在其余的数据源上测试连接。例如，输入:

```
print AdminControl.testConnection
('(SKLM scheduler XA Datasource(cells/SKLMCell/nodes/SKLMNode/
servers/server1|resources.xml#DataSource_1379859896273)')
```

4) 在这两种情况下，您都会收到消息，表明与数据源的连接已成功。例如:

```
WASX7217I: Connection to provided datasource was successful.
```

现在，您可以运行 IBM Security Key Lifecycle Manager 操作。

诸如 Linux 或 AIX 等系统上的 DB2 密码安全性问题

在诸如 Linux 或 AIX 等系统上，您可能需要更改 DB2 管理员用户标识的密码。DB2 管理员用户标识的登录密码和该用户标识的 DB2 密码必须相同。

IBM Security Key Lifecycle Manager 安装程序将安装 DB2，并提示安装人员为名为 sklmdb26 的用户输入密码。此外，DB2 应用程序还会创建名为 sklmdb26 的操作系统用户条目。例如，此用户的密码可能到期，需要您对两个用户标识的密码都进行再同步。

必须先更改系统用户条目的密码，然后才能更改 DB2 管理员用户标识的密码。请执行以下步骤:

1. 以 root 用户身份登录 IBM Security Key Lifecycle Manager 服务器。
2. 将用户更改为 sklmdb26 系统用户条目。输入:

```
su sklmdb26
```

3. 更改密码。输入:

```
passwd
```

指定新密码。

4. 退回为 root 用户。

   ```
   exit
   ```

5. 在 *WAS_HOME*/bin 目录中，使用 WebSphere Application Server 提供的 **wsadmin** 界面来指定 Jython 语法。

   ```
   ./wsadmin.sh -username WASAdmin -password mypwd -lang jython
   ```

6. 更改 WebSphere Application Server 数据源的密码:

   a. 以下命令将列出 JAASAuthData 条目:

      ```
      wsadmin>print AdminConfig.list('JAASAuthData')
      ```

      结果可能类似于以下示例:

      ```
      (cells/SKLMCell|security.xml#JAASAuthData_1228871756187)
      (cells/SKLMCell|security.xml#JAASAuthData_1228871757843)
      ```

   b. 根据每个条目输入 **AdminConfig.showall** 命令以查找别名 sklm_db。例如，在一行上输入:

      ```
      print AdminConfig.showall
        ('(cells/SKLMCell|security.xml#JAASAuthData_1228871756187)')
      ```

      结果类似于以下示例:

      ```
      {alias sklm_db}
      {description "SKLM database user j2c authentication alias"}
      {password *****}
      {userId sklmdb26}
      ```

      同时在一行上输入:

      ```
      print AdminConfig.showall
        ('(cells/SKLMCell|security.xml#JAASAuthData_1228871757843)')
      ```

      结果类似于以下示例:

      ```
      {alias sklmdb}
      {description "SKLM database user J2C authentication alias"}
      {password *****}
      {userId sklmdb26}
      ```

   c. 更改标识为 JAASAuthData_**1228871756187** 的 sklm_db 别名的密码:

      ```
      print AdminConfig.modify('JAASAuthData_list_entry', '[[password passw0rdc]]'
      ```

      例如，在一行上输入:

      ```
      print AdminConfig.modify
      ('(cells/SKLMCell|security.xml#JAASAuthData_1228871756187)',
      '[[password tucs0naz]]')
      ```

   d. 更改标识为 JAASAuthData_**1228871757843** 的 sklmdb 别名的密码:

      ```
      print AdminConfig.modify('JAASAuthData_list_entry', '[[password passw0rdc]]'
      ```

      例如，在一行上输入:

      ```
      print AdminConfig.modify
      ('(cells/SKLMCell|security.xml#JAASAuthData_1228871757843)',
      '[[password tucs0naz]]')
      ```

   e. 保存更改:

      ```
      print AdminConfig.save()
      ```

   f. 退回为 root 用户。

```
exit
```

g. 在 *WAS_HOME*/bin 目录中，停止 WebSphere Application Server 应用程序。例如，以 WASAdmin 身份在一行上输入:

```
stopServer.sh server1 -username wasadmin -password passw0rd
```

结果类似于以下示例:

```
ADMU0116I: Tool information is being logged in file
//opt/IBM/WebSphere/AppServer/profiles/KLMProfile/logs/server1/stopServer.log
ADMU0128I: Starting tool with the WASProfile profile
ADMU3100I: Reading configuration for server: server1
ADMU3201I: Server stop request issued. Waiting for stop status.
ADMU4000I: Server server1 stop completed.
```

h. 启动 WebSphere Application Server 应用程序。以 WebSphere Application Server 管理员身份在一行上输入:

```
 startServer.sh server1
```

i. 在 *WAS_HOME*/bin 目录中，使用 WebSphere Application Server 提供的 **wsadmin** 界面来指定 Jython 语法。

```
./wsadmin.sh -username wasadmin -password mypwd -lang jython
```

j. 验证是否可以使用 WebSphere Application Server 数据源连接到数据库。

1) 首先，查询数据源的列表。输入:

```
print AdminConfig.list('DataSource')
```

结果可能类似于以下示例:

```
"SKLM DataSource(cells/SKLMCell/nodes/SKLMNode/
  servers/server1|resources.xml#DataSource_1228871762031)"
"SKLM scheduler XA Datasource(cells/SKLMCell/nodes/SKLMNode/
  servers/server1|resources.xml#DataSource_1228871766562)"
"Tivoli Common Reporting Data Source(cells/SKLMCell|resources.xml#
  DataSource_1227211230078)"
DefaultEJBTimerDataSource(cells/SKLMCell/nodes/SKLMNode/
  servers/server1|resources.xml#DataSource_1000001)
ttssdb(cells/SKLMCell|resources.xml#DataSource_1227211144390)
```

2) 输入:

```
print AdminControl.testConnection('SKLM DataSource(cells....)')
```

例如，在一行上输入:

```
print AdminControl.testConnection
  ('SKLMDataSource(cells/SKLMCell/nodes/SKLMNode/
  servers/server1|resources.xml#DataSource_1228871762031)')
```

3) 在其余的数据源上测试连接。例如，输入:

```
print AdminControl.testConnection
 ('SKLM scheduler XA Datasource(cells/SKLMCell/nodes/SKLMNode/
  servers/server1|resources.xml#DataSource_1228871766562)')
```

4) 在这两种情况下，您都会收到消息，表明与数据源的连接已成功。例如:

```
WASX7217I: Connection to provided data source was successful.
```

安装期间的中间件配置

安装向导会收集 IBM Security Key Lifecycle Manager 和 WebSphere Application Server 运行时环境的信息。

安装向导需要您为以下字段提供信息:

- 请仅使用字母字符（A-Z 和 a-z）、数字字符 (0-9) 和下划线字符 (_)。该限制也适用于静默安装期间的响应文件中的值。

  名称字符串不能以空格开头或结尾，且不能包含以下字符:

  / 正斜杠
  \ 反斜杠
  * 星号
  , 逗号
  : 冒号
  ; 分号
  = 等号
  + 加号
  ? 问号
  | 竖线
  < 左尖括号
  > 右尖括号
  & 与符号
  % 百分号
  ' 单引号
  " 双引号
  ]]> 此字符组合无特定名称。
  . 句点（如果是第一个字符则无效；如果是后面的字符则有效）
  # 散列标记
  $ 美元符号
  ~ 波浪线
  (左圆括号
) 右圆括号

- 对 WebSphere Application Server 的安装位置请求做出响应时请选择新位置。

  如果系统上已安装了 WebSphere Application Server，那么***请勿***使用现有的 Key Lifecycle Manager 概要文件。

WebSphere Application Server 目录名称
指定期望的 WebSphere Application Server 安装目录。请勿在目录路径中使用空格。

用户标识
指定 Key Lifecycle Manager 管理员概要文件的 WebSphere Application Server 登录用户标识。

密码 指定 Key Lifecycle Manager 概要文件的 WebSphere Application Server 密码。

端口号 指定 Key Lifecycle Manager 概要文件的 WebSphere Application Server 端口。请勿使用大于 65520 的端口值。

迁移 Encryption Key Manager 配置

安装提供了将现有 Encryption Key Manager 配置迁移到 IBM Security Key Lifecycle Manager 的选项。

注:

您还可以使用跨平台备份实用程序对 IBM Security Key Lifecycle Manager V1.0、V2.0、V2.0.1 和 V2.5 等旧版以及 Encryption Key Manager V2.1 运行备份操作以备份关键数据。您可以在 IBM Security Key Lifecycle Manager V2.6 上将这些备份文件复原到与备份来源不同的操作系统。有关更多信息，请参阅旧版 IBM Security Key Lifecycle Manager 的备份和复原操作。

开始之前，请先获取登录 Encryption Key Manager 服务器 的密码。

要迁移现有配置，请选择以下选项:

迁移 Encryption Key Manager

如果有旧的 Encryption Key Manager 属性文件要迁移到 IBM Security Key Lifecycle Manager，那么请选中此框。如果选中此复选框，那么必须指定先前 Encryption Key Manager 系统中的属性文件。

可以从 Encryption Key Manager V2.1 迁移。

进行迁移时，Encryption Key Manager 必须处于不活动状态。要停止正在运行的 Encryption Key Manager 进程，请完成以下步骤:

1. 启动管理会话。在 V2.1 中，输入以下命令:

   ```
   java com.ibm.keymanager.KMSAdminCmd KeyManagerConfig.properties -i
   ```

2. 管理会话启动后，请完成以下步骤:
   a. 使用 login 命令向 Encryption Key Manager 服务器认证。输入:

      ```
      login -ekmuser EKMAdmin -password password
      ```

   b. 停止服务器。输入:

      ```
      stopekm
      ```

3. 退出会话。

有关迁移的限制，请参阅第 21 页的『迁移规划』。

在 Linux 系统上进行 IBM Security Key Lifecycle Manager 的非 root 用户安装

您可以在 Linux 操作系统上以非 root 用户身份安装 IBM Security Key Lifecycle Manager。

在 Linux 系统上进行 IBM Security Key Lifecycle Manager 的非 root 用户安装的最佳实践

计划在 Linux 系统上进行 IBM Security Key Lifecycle Manager 的非 root 用户安装时，可以考虑多项最佳实践。在开始安装之前，请查看这些最佳实践。

- 确保非 root 用户属于非 root 用户主组。root 用户必须具有 guests、admins、users 和 local 以外的主组。

- 非 root 用户的主目录 (`$HOME`) 必须指向正确的位置。例如: `/home/<user_name>`
- 如果系统中先前曾安装 IBM Security Key Lifecycle Manager 和 DB2，请确认已将其完全除去，而未遗留任何内容。
- 安装 IBM Security Key Lifecycle Manager 时，针对非 root 用户安装执行的 Prerequisite Scanner 可能会失败。请确保满足 Prerequisite Scanner 检查中指示的所有先决条件（管理员权限需求除外），然后再继续安装。

  要解决管理员权限问题并继续安装，请跳过运行 Prerequisite Scanner。要跳过先决条件扫描，请使用以下属性在 `/tmp` 目录中创建 `sklmInstall.properties` 文件。

  ```
  SKIP_PREREQ=true
  ```
- 请确保用于 DB2 安装的操作系统级别内核设置正确。有关 DB2 内核设置的更多信息，请参阅 DB2 文档: http://www-01.ibm.com/support/knowledgecenter/SSEPGG_10.5.0/com.ibm.db2.luw.qb.server.doc/doc/t0008238.html
- 在安装期间，数据库管理员标识必须与登录系统以执行安装的非 root 用户相同。请确保满足数据库管理员标识的以下需求:
  - 数据库管理员标识的密码必须与非 root 用户的操作系统级别密码相同。
  - 数据库管理员组与操作系统级别非 root 用户的主组相同。
  - 数据库主目录指向非 root 用户的主目录。
- 静默方式不支持非 root 用户安装。
- 不支持从 IBM Security Key Lifecycle Manager 先前版本 1.0、2.0、2.0.1 和 2.5 以及加密密钥管理器迁移到 V2.6 的非 root 用户安装。
- 以非 root 用户身份进行安装时，无法在系统引导时启动 DB2。通过在启动 WebSphere Application Server 之前启动 DB2来解决此问题。在安装程序完成安装之后，运行 `nonrootconfig.sh` 脚本。

在 Linux 系统上以非 root 用户身份安装 IBM Security Key Lifecycle Manager

您可以在 Linux 操作系统上以非 root 用户身份安装 IBM Security Key Lifecycle Manager。IBM Security Key Lifecycle Manager 非 root 安装以非 root 用户身份安装 DB2 和 WebSphere Application Server。

关于此任务

注:

- 如果您以非 root 用户身份安装 IBM Security Key Lifecycle Manager，那么无法将 IBM Security Key Lifecycle Manager 先前版本 V1.0、V2.0 和 V2.0.1、V2.5 以及 Encryption Key Manager 迁移到 V2.6。
- 在静默方式下无法以非 root 用户身份安装 IBM Security Key Lifecycle Manager。

过程

1. 确保目标环境满足 IBM Security Key Lifecycle Manager 安装先决条件。请参阅第 5 页的『规划安装』。
2. 创建非 root 用户标识。确保该用户标识具有 `guests`、`admins`、`users` 和 `local` 以外的主组。
3. 运行 **launchpad.sh**。

4. 指定 DB2 配置参数。请参阅『进行非 root 安装期间配置 DB2』。
5. 指定 WebSphere Application Server 配置参数。
6. 在 IBM Security Key Lifecycle Manager 过程完成之后，必须停止 WebSphere Application Server 和 DB2。

   运行以下命令以停止 WebSphere Application Server。

   ```
   cd <WAS_HOME>/bin
   ./stopServer.sh <server name> -username <WAS Admin User ID>
   -password <WAS Admin password>
   ```

   ```
   ./stopServer.sh server1 -username wasadmin -password wasadmin_pwd
   ```

   运行以下命令以停止 DB2。

   ```
   cd ~/sqllib/adm
   ./db2stop
   ```

7. 打开 /home/username/sklmV26properties/scripts 并运行以下命令。

   非 root DB2 安装需要 root 访问权以配置 DB2 实例使用特定的端口号和服务名称。

   ```
   sudo nonrootconfig.sh <instance_home> <user_name> <port_number>
   ```

8. 重新启动 WebSphere Application Server。

   ```
   cd <WAS_HOME>/bin
   ./startServer.sh <server name>
   ```

   ```
   ./startServer.sh server1
   ```

下一步做什么

在 *SKLM_HOME*/config/SKLMConfig.properties 文件中，更新大于 1024 的 SSL 端口号。例如:

```
TransportListener.ssl.port property =4411
```

安装后，您必须以非 root 用户身份登录才能启动或停止 IBM Security Key Lifecycle Manager 服务器和 DB2 服务器。

进行非 root 安装期间配置 DB2

IBM Security Key Lifecycle Manager 要求 DB2 工作组服务器版 处于 V10.5.5 级别，具体视操作系统而定。

在配置 DB2 期间，会提示您提供以下信息:

DB2 管理员标识

本地 DB2 管理员用户标识。因为非 root DB2 用户可以具有单个实例，所以 DB2 管理员标识必须与登录系统的用户标识相同。

用户标识具有下列限制和要求:

- 必须具有 guests、admins、users 和 local 以外的主组。
- 可以包含小写字母 (a-z)、数字 (0-9) 和下划线字符 (_)。
- 长度不能超过 8 个字符。
- 不能以 IBM、SYS、SQL 或数字开头
- 不能是 DB2 保留字（USERS、ADMINS、GUESTS、PUBLIC 或 LOCAL）或 SQL 保留字

- 不能使用任何具有 root 用户特权的用户标识作为 DB2 实例标识、DAS 标识或受防护标识。
- 不能包含重音字符。

DB2 管理员密码

管理员的密码。最大长度为 20 个字符。

DB2 管理员用户标识的密码必须符合系统上的活动安全策略。DB2 管理员标识的密码必须与登录系统的非 root 用户的操作系统级别密码相同。更改其中之一时，必须更改另一个。

数据库名称

IBM Security Key Lifecycle Manager 数据库的名称，即 SKLMDB26。

DB2 端口

DB2 使用的端口。

管理员组

管理员用户标识所在的访问组。数据库管理员组必须与操作系统级别的非 root 用户的主组相同。

管理员主目录/数据库主目录

该目录中创建了数据库实例以及 IBM Security Key Lifecycle Manager 所使用的格式化表。数据库主目录必须指向非 root 用户的主目录。

注意:

1. 所有字段的输入内容只能为字母字符（A-Z 和 a-z）、数字字符 (0-9) 和下划线字符 (_)。该限制也适用于静默安装所用响应文件中的值。
2. 请不要在任何目录路径或文件名中指定空格。
3. 在其中安装 DB2 的计算机的名称不能以小写或大写的“ibm”、“sql”或“sys”开头。该计算机的名称也不能包含下划线字符 (_)。

有关如何修改内核参数和非 root 安装的更多信息，请参阅 DB2 文档。

- http://www-01.ibm.com/support/knowledgecenter/SSEPGG_10.5.0/com.ibm.db2.luw.qb.server.doc/doc/t0008238.html
- http://www-01.ibm.com/support/knowledgecenter/SSEPGG_10.5.0/com.ibm.db2.luw.qb.server.doc/doc/t0050571.html

在分布式系统上重置密码

必须是管理员才能为 IBM Security Key Lifecycle Manager 或 WebSphere Application Server 重置密码。

关于此任务

可以在运行 IBM Security Key Lifecycle Manager 的计算机上重置密码。仅当用户密码丢失时使用这些步骤。在所有其他情况下，请使用图形用户界面更新密码。

过程

1. 使用本地管理员用户标识进行登录。
2. 备份 *WAS_HOME*/profiles/KLMProfile/config/cells/SKLMCell/fileRegistry.xml文件。更改密码值将更改此注册表文件。

3. 更改密码。
   - Windows 系统
     a. 使用 Jython 语法启动 **wsadmin** 会话。例如，输入:

        ```
        WAS_HOME/bin/wsadmin -conntype none -profileName KLMProfile -lang jython
        ```

     b. 重置 SKLMAdmin 用户标识的密码:

        ```
        wsadmin>print AdminTask.changeFileRegistryAccountPassword
         ('-userId SKLMAdmin -password newpassword')
        ```

        注:

        – 只有 WASAdmin 用户标识或拥有 WebSphere Application Server 管理权限的另一个用户标识可以使用 **AdminTask.changeFileRegistryAccountPassword** 命令更改密码。
        – 使用 **AdminTask.changeFileRegistryAccountPassword** 命令创建的密码不能根据 IBM Security Key Lifecycle Manager 提供的已配置的密码策略进行验证。

          在重置丢失的密码之后，用户必须使用图形用户界面设置密码。

     c. 保存更改并退出:

        ```
        wsadmin>print AdminConfig.save()
        wsadmin>exit
        ```

   - 诸如 Linux 或 AIX 之类的系统
     a. 使用 Jython 语法启动 **wsadmin** 会话。例如，在一行上输入:

        ```
        WAS_HOME/bin/wsadmin.sh -conntype none
           -profileName KLMProfile -lang jython
        ```

     b. 重置 SKLMAdmin 用户标识的密码:

        ```
        wsadmin>print AdminTask.changeFileRegistryAccountPassword
         ('-userId SKLMAdmin -password newpassword')
        ```

        注:

        – 只有 WASAdmin 用户标识或拥有 IBM Security Key Lifecycle Manager 管理权限的另一个用户标识可以使用 **AdminTask.changeFileRegistryAccountPassword** 命令更改密码。
        – 使用 **AdminTask.changeFileRegistryAccountPassword** 命令创建的密码不能根据 IBM Security Key Lifecycle Manager 提供的已配置的密码策略进行验证。

          在重置丢失的密码之后，用户必须使用图形用户界面设置密码。

     c. 保存更改并退出:

        ```
        wsadmin>print AdminConfig.save()
        wsadmin>exit
        ```

4. 停止和启动服务器。
   - 停止

     在 Windows 系统上:

     ```
     stopServer.bat server1
     ```

     在诸如 Linux 或 AIX 的系统上:

     ```
     ./stopServer.sh server1
     ```

- 启动

  在 Windows 系统上:

  ```
  startServer.bat server1
  ```

  在诸如 Linux 或 AIX 的系统上:

  ```
  ./startServer.sh server1
  ```

5. 请验证是否可以使用新的密码已指定的管理员身份登录。

分布式系统上的卸载

在分布式系统上，卸载 IBM Security Key Lifecycle Manager 有以下注意事项:

- 缺省卸载方式与用于安装 IBM Security Key Lifecycle Manager 的方式相同。还可以使用其他方式进行卸载。有关更多信息，请参阅『卸载程序的语法和参数』。
- 如果在安装 IBM Security Key Lifecycle Manager 之前已安装了 DB2，那么卸载 IBM Security Key Lifecycle Manager 时不会卸载 DB2。此任务是单独的可选步骤。有关信息，请参阅第 67 页的『DB2 卸载』。

  此外，虽然卸载 IBM Security Key Lifecycle Manager 会使 DB2 数据库实例与用于 IBM Security Key Lifecycle Manager DB2 实例所有者的用户标识取消关联，但是仍需要在单独的步骤中删除该用户标识。有关信息，请参阅第 69 页的『从 DB2 实例所有者除去用户标识』。

  卸载不成功可能表示需要返回到已知的 IBM Security Key Lifecycle Manager V2.0.1 状态。有关更多信息，请参阅第 65 页的『在迁移反复失败后重新安装先前版本』。

卸载程序的语法和参数

必须使用卸载命令来卸载 IBM Security Key Lifecycle Manager。

静默卸载

```
imcl -input full_path_to_response_file -silent
```

-input 使用要在静默卸载期间使用的卸载选项指定响应文件的完整路径和文件名称。

-silent
指定 IBM Installation Manager 安装程序必须以静默方式运行。

以图形方式卸载

uninstall_program

其中 *uninstall_program* 是:

***<IM_INSTALL_DIR>*\IBMIM.exe**（在 Windows 系统上）。

***<IM_INSTALL_DIR>*\IBMIM**（在诸如 Linux 或 AIX 之类的系统上）。

在 Windows 系统上卸载

使用 IBM Installation Manager 卸载 IBM Security Key Lifecycle Manager、DB2 和 WebSphere Application Server。

开始之前

在卸载 IBM Security Key Lifecycle Manager 之前停止 WebSphere Application Server。如果在卸载 IBM Security Key Lifecycle Manager 之前 WebSphere Application Server 未停止，那么步骤 4 之后将显示以下错误消息。

```
Running processes have been detected that may interfere with the current
operation. Stop all WebSphere and related processes before continue.
```

单击**重新检查状态**以继续执行卸载任务。

过程

1. 浏览至 *<IM_INSTALL_DIR>* 并双击 **IBMIM** 来以 GUI 方式启动 IBM Installation Manager。
2. 在 IBM Installation Manager 中，单击**卸载**。将打开“卸载软件包”窗口。
3. 选择复选框卸载 IBM Security Key Lifecycle Manager、DB2 和 WebSphere Application Server。
4. 单击**下一步**。输入 WebSphere Application Server 管理员用户标识和密码。
5. 单击**下一步**。 将打开“摘要面板”窗口。
6. 查看要卸载的软件包及其安装目录，然后单击**卸载**。

下一步做什么

注: 卸载 IBM Security Key Lifecycle Manager 之后，请删除 `C:\Program Files (x86)\IBM\WebSphere` 和`C:\Program Files (x86)\DB2SKLMV26` 目录（如果这些目录尚未除去）。

在 Windows 系统上从失败的卸载恢复

必须从在 Windows 系统上卸载 IBM Security Key Lifecycle Manager 的失败尝试中恢复。

关于此任务

此任务假定卸载程序未成功完成。请执行以下恢复步骤:

过程

1. 停止 WebSphere Application Server 服务。
   a. 通过打开“控制面板”并单击**管理工具 > 服务**，打开 Windows 服务控制台。
   b. 查找 WebSphere Application Server 服务。

      例如: `IBM WebSphere Application Server V8.5 - SKLM26Server`
   c. 打开此服务的**属性**对话框。如果**服务状态**不处于“已停止”状态，请单击**停止**。
   d. 单击**确定**管理对话框，然后退出 Windows 服务控制台。

   如果无法从 Windows 服务控制台中停止服务，请打开命令提示符，然后输入这些命令手动停止服务:

   ```
   cd WAS_HOME\bin
   WASService -stop SKLMServer
   ```
2. 如果尚未除去 WebSphere Application Server 服务，请除去它。 打开命令提示符，然后输入以下命令:

   ```
   cd WAS_HOME\bin
   WASService -remove SKLMServer
   ```
3. 卸载 WebSphere Application Server（如果存在并且其他产品未在对其进行使用）。

   有关卸载指示信息，请参阅以下链接:

图形用户界面

http://www-01.ibm.com/support/knowledgecenter/SSAW57_8.5.5/com.ibm.websphere.installation.nd.doc/ae/tins_uninstallation_dist_gui.html

命令行界面

http://www-01.ibm.com/support/knowledgecenter/SSAW57_8.5.5/com.ibm.websphere.installation.nd.doc/ae/tins_uninstallation_dist_cl.html

如果已除去 *WAS_HOME* 或 *WAS_HOME*\bin 目录，请跳过步骤 1、2 和 3。

4. 卸载 DB2（如果存在并且其他产品未在对其进行使用）。

   有关卸载指示信息，请参阅第 67 页的『除去 DB2（可选）』。

5. 在文本编辑器中打开 C:\ProgramData\IBM\Installation Manager\installRegistry.xml 文件。

   注: 备份 installRegistry.xml 文件。

6. 除去只与 IBM Security Key Lifecycle Manager 相关的条目。 例如:

```
<profile id='IBM Security Key Lifecycle Manager v2.6' kind='product'>
  ....
</profile>
```

7. 除去此目录中的安装日志文件:

   \<*IM App Data Dir*>\logs

8. 除去**控制面板** > **添加/删除程序** > **IBM Installation Manager**。
9. 除去以下文件夹（如果存在）:
   - C:\Program Files (x86)\IBM\DB2SKLMV26
   - C:\Program Files (x86)\IBM\WebSphere
   - C:\Program Files (x86)\IBM\SKLMV26
   - C:\Program Files (x86)\IBM\Installation Manager
   - C:\Program Files (x86)\IBM\IBMIMShared
10. 重新启动计算机。

在 Linux 和 AIX 等系统上卸载

必须在卸载 IBM Security Key Lifecycle Manager 之前停止 WebSphere Application Server。

开始之前

要在系统（比如 Linux 或 AIX）上卸载 IBM Security Key Lifecycle Manager 时，请执行以下步骤。

过程

1. 浏览至 <*IM_INSTALL_DIR*> 并运行 **IBMIM**。
2. 在 IBM Installation Manager 中，单击**卸载**。将打开“卸载软件包”窗口。
3. 选择复选框卸载 IBM Security Key Lifecycle Manager、DB2 和 WebSphere Application Server。
4. 单击**下一步**。输入 WebSphere Application Server 管理员用户标识和密码。

5. 单击**下一步**。 此时将打开摘要面板。
6. 查看要卸载的软件包及其安装目录。
7. 单击**卸载**。

从在系统（比如 Linux 或 AIX）上失败的安装中恢复

可能想要从在系统（比如 Linux 或 AIX）上卸载 IBM Security Key Lifecycle Manager 的失败尝试中恢复。

关于此任务

此任务假定卸载程序未成功完成。请执行以下恢复步骤:

过程

1. 以 root 用户的身份登录。
2. 停止 WebSphere Application Server 进程（如果其正在运行）。

   ```
   cd WAS_HOME/profiles/KLMProfile/bin
   ./stopServer.sh server1
   ```

3. 卸载 WebSphere Application Server（如果存在并且其他产品未在对其进行使用）。

   有关卸载指示信息，请参阅以下链接:

   图形用户界面

   http://www-01.ibm.com/support/knowledgecenter/SSAW57_8.5.5/com.ibm.websphere.installation.nd.doc/ae/tins_uninstallation_dist_gui.html

   命令行界面

   http://www-01.ibm.com/support/knowledgecenter/SSAW57_8.5.5/com.ibm.websphere.installation.nd.doc/ae/tins_uninstallation_dist_cl.html

   如果已除去 *WAS_HOME* 或 *WAS_HOME*/bin 目录，请跳过步骤 2 和 3。
4. 卸载 DB2（如果存在并且其他产品未在对其进行使用）。

   有关卸载指示信息，请参阅第 67 页的『除去 DB2（可选）』。
5. 打开 /var/ibm/InstallationManager/installRegistry.xml 文件。

   注: 备份 installRegistry.xml 文件。
6. 除去**只**与 IBM Security Key Lifecycle Manager 相关的条目。 例如:

   ```
   <profile id='IBM Security Key Lifecycle Manager v2.6' kind='product'>
     ....
   </profile>
   ```

7. 使用以下命令从 /var/ibm/InstallationManager/logs 目录中除去安装日志文件:

   ```
   rm -rf /var/ibm/InstallationManager/logs
   ```

8. 卸载 IBM Installation Manger。
9. 除去以下文件夹（如果存在）:
   - opt/IBM/DB2SKLMV26
   - opt/IBM/WebSphere
   - opt/IBM/SKLMV26
   - opt/IBM/Installation Manager

- opt/IBM/IBMIMShared

10. 重新启动计算机。

在迁移反复失败后重新安装先前版本

迁移过程不会影响 IBM Security Key Lifecycle Manager 的先前版本。如果迁移过程仍然失败，请卸载 IBM Security Key Lifecycle Manager V2.6 并继续运行先前版本。

注: 在 Windows 平台上，将 IBM Security Key Lifecycle Manager 先前版本（1.0、2.0、2.0.1 或 2.5）迁移到 V2.6 之后，如果在卸载先前版本之前卸载 IBM Security Key Lifecycle Manager V2.6，那么与先前版本关联的 DB2 可能不会启动。

可以按照第 61 页的『分布式系统上的卸载』中的步骤卸载 IBM Security Key Lifecycle Manager V2.6。

除去 DB2（可选）

卸载 IBM Security Key Lifecycle Manager 之后，您可以选择保留已安装的 DB2 或卸载该程序。

如果在安装 IBM Security Key Lifecycle Manager 之前已安装 DB2，那么卸载 IBM Security Key Lifecycle Manager 不会将 DB2 卸载。如果 DB2 是通过 IBM Security Key Lifecycle Manager 安装程序进行安装的，那么卸载 IBM Security Key Lifecycle Manager 时将会卸载 DB2。您可能还需确保相关的自动启动服务已禁用。

DB2 卸载

卸载 IBM Security Key Lifecycle Manager 之后，可以选择保留已安装的 DB2 或卸载该程序。

如果选择保留已安装的 DB2，那么可以选择保留或除去 IBM Security Key Lifecycle Manager DB2 实例所有者。除非您有特定的原因需要保留实例所有者（例如要保持与数据库的连接），否则请解除该用户标识与 DB2 数据库实例的关联。有关更多信息，请参阅第 68 页的『从 DB2 实例解除用户标识的关联』。

如果选择卸载 DB2，请遵循以下步骤:

Windows 系统:

打开控制面板。

Windows Server 2008: 单击**程序和功能**。查找 DB2 的条目，然后单击**删除**以将其卸载。

注: 卸载 DB2 之后，可能还需要完成额外的步骤才能除去 DB2 工件。

1. 要删除用于 IBM Security Key Lifecycle Manager DB2 实例所有者的用户标识，请打开控制面板并单击**管理工具 > 计算机管理 > 本地用户和组 > 用户**。

   复查用户标识的列表。如果 IBM Security Key Lifecycle Manager DB2 实例所有者的用户标识仍存在，请将其删除。

   关闭“计算机管理”控制台。
2. 复查条目并验证 DB2 端口的条目是否已从 `C:\WINDOWS\system32\drivers\etc\services` 文件中除去。编辑文件并搜索 DB2 使用的端口号。如果找到任何此类端口号，请将相应条目从文件中除去。
3. 打开控制面板并单击**管理工具 > 计算机管理 > 服务**。复查服务列表并验证与 DB2 相关的服务条目是否已除去。完成后关闭“服务”控制台。
4. 如果 DB2 安装目录尚未除去，请将该目录除去。

有关在 Windows 系统上卸载 DB2 的更多信息，请参阅 DB2 文档 (http://www-01.ibm.com/support/knowledgecenter/SSEPGG_10.5.0/com.ibm.db2.luw.qb.server.doc/doc/t0007436.html)。

AIX 和 Linux 系统:

1. 以 root 用户身份登录。
2. 除去 IBM Security Key Lifecycle Manager DB2 实例所有者的用户标识:
   a. 更改为 IBM Security Key Lifecycle Manager DB2 实例所有者的用户标识，对该实例所有者用户标识运行 **db2istop** 命令，然后回退到 root 用户标识:

      ```
      su - sklm_instance_owner_userid

      cd DB_HOME/instance
      ./db2istop sklm_instance_owner_userid /home/sklm_instance_owner_userid

      exit
      ```

   b. 对实例所有者用户标识运行 **db2idrop** 命令:

      ```
      cd DB_HOME/instance
      ./db2idrop sklm_instance_owner_userid
      ```

   c. 从系统中除去该用户标识:

      ```
      userdel -r sklm_instance_owner_userid
      ```

3. 从系统中除去 DB2:

   ```
   cd DB_HOME/install/
   ./db2_deinstall -a
   ```

4. 编辑服务文件:

   ```
   vi /etc/services
   ```

   找到 DB2 使用的端口号，并将这些条目从文件中除去。
5. 如果 DB2 安装目录尚未除去，请将其除去。

有关在诸如 Linux 和 AIX 等系统上卸载 DB2 的更多信息，请参阅 DB2 文档 (http://www-01.ibm.com/support/knowledgecenter/SSEPGG_10.5.0/com.ibm.db2.luw.qb.server.doc/doc/t0007439.html)。

以下示例显示所涉及的步骤，其中使用缺省的 DB2 实例所有者用户标识 sklmdb26 和缺省的 DB2 目录 /opt/IBM/DB2SKLMV26。

以 root 用户身份开始，输入:

```
su - sklmdb2
cd /opt/IBM/DB2SKLMV26/instance
./db2istop sklmdb26/home/sklmdb26
exit
# Exit back to root.
cd /opt/IBM/DB2SKLMV26/instance
./db2idrop sklmdb26
userdel -r sklmdb26
cd /opt/IBM/DB2SKLMV26/install
./db2_deinstall -a
vi /etc/services
# Locate and remove the DB2 port entries in the services file.
rm -rf /opt/IBM/DB2SKLMV26
```

从 DB2 实例解除用户标识的关联

可以从 IBM Security Key Lifecycle Manager DB2 实例解除用户标识的关联。

如果用户标识已从 DB2 实例解除关联，某个步骤可能会返回一条消息说明未找到该用户。如果收到此消息，请继续下一步。

- **Windows 系统**:

1. 打开“Windows 服务”控制台，然后停止 IBM Security Key Lifecycle Manager 实例所有者的 DB2 服务。

   要查找 DB2 实例服务，请搜索以“DB2”开头的服务的服务列表。实例服务的条目包含 IBM Security Key Lifecycle Manager DB2 实例所有者的用户标识，将其作为部分服务名称。例如，**DB2 - DBSKLMV26 - SKLMDB26**。

   打开服务的属性对话框，将**服务状态**设置为已停止，并将**启动类型**设置为手动。
2. 单击**开始> 程序 > IBM DB2 > *instance_owner* > 命令行工具 > 命令窗口** 以打开 DB2 命令窗口，然后输入:

   ```
   db2idrop db databasename
   db2idrop sklm_instance_owner_userid
   ```
3. 如果 C:*sklm_instance_owner_user_id* 目录仍然存在，请将其除去:

   ```
   del /s /q  C:\sklm_instance_owner_user_id
   ```

- **AIX 和 Linux 系统**:

  以 root 用户的身份进行登录，然后执行以下步骤。
  1. 更改为 IBM Security Key Lifecycle Manager DB2 实例所有者的用户标识，对该实例所有者用户标识运行 **db2istop** 命令，然后回退到 root 用户标识:

     ```
     su - sklm_instance_owner_userid

     cd DB_HOME/instance
     ./db2istop sklm_instance_owner_userid /home/sklm_instance_owner_userid

     exit
     ```
  2. 对实例所有者用户标识运行 **db2idrop** 命令:

     ```
     cd DB_HOME/instance
     ./db2idrop sklm_instance_owner_userid
     ```
  3. 如果 *sklm_instance_owner_user_id*/sqllib 目录仍然存在，请将其除去:

     ```
     rm -rf sklm_instance_owner_user_id/sqllib
     ```

从 DB2 实例所有者除去用户标识

要除去用作 IBM Security Key Lifecycle Manager DB2 实例所有者的用户标识，请使用操作系统的用户管理实用程序来删除该用户标识。

删除用作 IBM Security Key Lifecycle Manager 数据库的实例所有者的用户标识之前，请确保该用户标识不再与 DB2 实例关联。

请遵循第 68 页的『从 DB2 实例解除用户标识的关联』中的步骤。如果用户标识已从 DB2 实例解除关联，某个步骤可能会返回一条消息说明未找到该用户。如果收到此消息，请继续下一步。

验证用户标识与 DB2 数据库实例不再关联之后，请按照以下步骤从系统除去该用户标识:

- **Windows 系统**:

  使用您运行的 Windows 版本的用户管理工具来从系统删除 DB2 管理用户。例如，在 Windows 的某些版本上，请执行以下步骤:
  1. 打开控制面板。

2. 单击**管理工具 > 计算机管理 > 本地用户和组 > 用户**。
3. 从系统删除用户。

- **AIX 和 Linux 系统**:

  以 root 用户的身份进行登录，然后输入以下命令来删除用户标识:

  ```
  userdel -r sklm_instance_owner_userid
  ```

禁用自动服务

IBM Security Key Lifecycle Manager 卸载过程将禁用与 IBM Security Key Lifecycle Manager 关联的 DB2 和 WebSphere Application Server 服务。要更正错误条件，您可能还需要确保已禁用这些服务。

Windows 系统

在 Windows 系统上，使用“Windows 服务”控制台可阻止与 IBM Security Key Lifecycle Manager 关联的 DB2 和 WebSphere Application Server 服务自动启动。

打开“Windows 服务”控制台并在以下列表中查找服务。针对列表中的每个服务，打开该服务的“属性”对话框，并确保**启动类型**设置为已禁用，且**服务状态**字段设置为已停止。

DB2 - *db2 副本名称 - SKLM_INSTANCE_OWNER*
例如，**DB2 - DBSKLMV26 - SKLMDB6**

DB2 Governor (*db2 副本名称*)
例如，**DB2 Governor (DBSKLMV26)**

DB2 License Server (*db2 副本名称*)
例如，**DB2 License Server (DBSKLMV26)**

DB2 Management Service (*db2 副本名称*)
例如，**DB2 Management Service (DBSKLMV26)**

DB2 Remote Command Server (*db2 副本名称*)
例如，**DB2 Remote Command Server (DBSKLMV26)**

DB2DAS - *DB2DAS_entry*
例如，**DB2DAS - DB2DAS00**

注: 仅当 DAS 服务托管于 Windows 服务中时，才禁用 DB2 Administration Server (DAS)。

AIX 和 Linux 系统

在 AIX 或 Linux 系统上，输入以下命令对 IBM Security Key Lifecycle Manager DB2 实例所有者进行配置，以使其不会自动启动:

```
. ~sklmdb2/sqllib/db2profile
DB_HOME/instance/db2iauto -off sklmdb26
```

其中，`sklmdb2` 是缺省实例所有者用户标识。如果在安装期间更改了该用户标识，请改用更改后的用户标识。

接着，编辑 /etc/inittab 文件并除去自动启动 WebSphere Application Server 服务器的条目。

```
/opt/IBM/WebSphere/AppServer/bin/startServer.sh server1
```

从故障迁移恢复

可以为失败执行迁移恢复步骤来迁移 Encryption Key Manager 或 IBM Security Key Lifecycle Manager。

从 Encryption Key Manager 的迁移失败进行恢复

迁移 Encryption Key Manager 期间可能会发生错误。

安装流程完成了 IBM Security Key Lifecycle Manager 的安装步骤，并开始迁移步骤以将数据从 Encryption Key Manager 迁移到 IBM Security Key Lifecycle Manager。

- 迁移开始时，安装程序验证 Encryption Key Manager 属性文件中的值时可能会发生错误，可能会出现以下情况:
  - 无法读取属性文件，因为没有足够的访问许可权。
  - 必需的属性不存在或不具有值。
  - 属性值的格式不正确。
  - 属性指向的文件不存在，或由于没有足够的访问许可权而无法读取。
- 迁移操作完成重要活动后可能会发生错误。在此情况下，请查看错误日志文件:

  Windows 系统:

  ```
  <IM App Data Dir>\logs\sklmLogs\migration.log
  ```

  AIX 和 Linux 系统:

  ```
  <IM App Data Dir>/logs/sklmLogs/migration.log
  ```

如果 Encryption Key Manager 迁移失败，并且您选择完成剩余的迁移过程，那么如果在运行迁移恢复脚本之前未更改或配置 IBM Security Key Lifecycle Manager 服务器，那么可以启动该迁移恢复脚本。

如果 Encryption Key Manager 迁移失败而未迁移任何数据，那么请除去 `tklmKeystore.jceks` 文件以重新开始迁移过程。您可以在 `WAS_HOME\products\sklm\keystore` 目录中找到该文件。

Encryption Key Manager 的迁移恢复脚本

如果您未在运行迁移恢复脚本之前对 IBM Security Key Lifecycle Manager 服务器作出任何更改或配置，那么可以为 Encryption Key Manager 启动迁移恢复脚本。例如，未在系统上明显地更改可用磁盘空间。

迁移脚本位于 *SKLM_HOME*`\migration\bin` 目录中。用于运行该脚本的命令为:

Windows 系统:

```
cd SKLM_HOME\migration\bin
.\migrate.bat sklm_instance_owner_password
```

Linux 和 AIX 系统:

```
cd SKLM_HOME/migration/bin
./migrate.sh sklm_instance_owner_password
```

在诸如 Linux 或 AIX 之类的系统上，请确保以 root 用户身份登录，然后再运行 migrate.sh。

其中，*sklm_instance_owner_password* 参数是 IBM Security Key Lifecycle Manager 服务器 DB2 实例所有者的密码。

SKLM_HOME 参数仅在 Windows 系统上使用，并且必须用引号括起来。

Windows 系统:

```
cd "C:\Program Files (x86)\IBM\SKLMV26\migration\bin"

.\bin\migrate.bat password
echo %ERRORLEVEL%
```

注:

- 如果不想将密码作为参数来进行指定，那么请省略该密码。恢复脚本将提示您输入值。该密码不是以明文显示的。例如:

  ```
  migrate.bat
  echo $?
  ```

- 在其运行时过程中，迁移恢复脚本会创建一个 migration.log 文件。
- 如果 migrate.bat 或 migrate.sh 不可用,
  1. 请将 migrate.bat.template 或 migrate.sh.template 复制到 migrate.bat 或 migrate.sh。
  2. 指定必需参数。
  3. 运行该文件。

Linux 和 AIX 系统:

```
cd /opt/IBM/SKLMV26/migration/bin
./bin/migrate.sh password
echo $?
```

在诸如 Linux 或 AIX 之类的系统上，请确保以 root 用户身份登录，然后再运行 migrate.sh。

从 IBM Security Key Lifecycle Manager 的迁移失败进行恢复

迁移 IBM Security Key Lifecycle Manager 期间可能会发生以下错误场景:

- 迁移开始时，以下的一种或多种情况可能会导致发出错误消息:
  - 没有足够的访问许可权来读取所需文件，或者缺少属性或文件。
  - 其他应用程序在使用所需文件。
  - DB2 服务器 迁移期间，WebSphere Application Server 意外停止运行。
- 迁移完成后，或已执行重要活动，迁移操作开始后可能会发生错误。

安装程序将显示错误消息。在此情况下，请查看错误日志文件:

Windows 系统:

<*IM App Data Dir*>\logs\sklmLogs\migration.log

AIX 和 Linux 系统:

<*IM App Data Dir*>/logs/sklmLogs/migration.log

如果您反复运行迁移程序均失败而选择回到先前版本，那么请对新版本的 DB2 完成以下任务:

- 卸载 IBM Security Key Lifecycle Manager 先前版本。在诸如 AIX 或 Linux 之类的系统上，浏览至实例所有者的主目录，如 /home/sklmdb26。如果 sqllib_v91 目录存在，请除去该目录。
- 重新启动计算机。
- 重新安装 IBM Security Key Lifecycle Manager 先前版本并复原最近的备份。应用最新的修订包。

IBM Security Key Lifecycle Manager 的迁移恢复脚本

如果您未在运行迁移恢复脚本之前对 IBM Security Key Lifecycle Manager 服务器作出任何更改或配置，那么可以为 IBM Security Key Lifecycle Manager 启动迁移恢复脚本。例如，未在系统上明显地更改可用磁盘空间。

迁移实用程序会在 *<IM App Data Dir>\logs\sklmLogs* 目录中创建 migration.log 文件。

迁移脚本位于 *SKLM_HOME*\migration 目录中。运行迁移脚本之前，请确保正确设置 JAVA_HOME。以下示例显示 JAVA_HOME 的路径:

Windows 系统

```
C:\Program Files (x86)\IBM\WebSphere\AppServer\java\jre
```

Linux 和 AIX 系统

```
/opt/IBM/WebSphere/AppServer/java/jre
```

用于运行该迁移脚本的命令为:

Windows 系统

```
cd SKLM_HOME\migration
.\migrateToSKLM.bat
```

注: 必须为 migration.properties 文件（该文件存在于 *SKLM_HOME*\migration 目录下）中的迁移参数指定值。

例如:

```
cd "C:\Program Files (x86)\IBM\SKLMv26\migration"
.\migrateToSKLM.bat
```

Linux 和 AIX 系统

```
cd SKLM_HOME/migration
./migrateToSKLM.sh
```

注: 必须为 migration.properties 文件（该文件存在于 *SKLM_HOME*/migration 目录下）中的迁移参数指定值。

例如:

```
cd /opt/IBM/SKLMV26/migration
./migrateToSKLM.sh
```

在诸如 Linux 或 AIX 之类的系统上运行 **migrateToSKLM.sh** 之前，请确保您以 root 用户身份登录。

注: 运行迁移恢复脚本之后，请手动重新启动 WebSphere Application Server。

migration.properties 文件中的参数

WAS_HOME

WebSphere Application Server for IBM Security Key Lifecycle Manager V2.6 的安装目录。

TKLM_TIP_HOME

Tivoli Integrated Portal for IBM Security Key Lifecycle Manager 先前版本 V1.0、V2.0 或 V2.0.1 的安装目录。对于 V2.5，您还可以使用此参数来设置 `<WAS_HOME>`。

WAS_ADMIN_ID

先前版本的 Tivoli Integrated Portal 管理员用户名。

WAS_ADMIN_PASSWORD

Tivoli Integrated Portal 管理员用户名的密码。

SKLM_INSTALL_PATH

安装 IBM Security Key Lifecycle Manager 的目录。

SKLM_ADMIN_USER

IBM Security Key Lifecycle Manager 先前版本的管理员用户名。该用户名必须为 `TKLMAdmin`。

MIG_LOG_PATH

存储 `migration.log` 的文件路径。

TKLM_VERSION

系统上安装的 IBM Security Key Lifecycle Manager 先前版本的版本号。

TKLM_DB_PWD

IBM Security Key Lifecycle Manager 先前版本的 DB2 管理员密码。

KEYSTORE_PWD

IBM Security Key Lifecycle Manager 先前版本 V1.0、V2.0 或 V2.0.1 的密钥存储库密码。对于 V2.5，不需要此参数。

IM_INSTALL_DIR

IBM Installation Manager 的安装目录。

注: 除了密码以外的所有其他值都预先填写在该属性文件中。请勿修改除空白字段以外的任何值。

DB2 启用自动启动

如果以恢复方式运行迁移脚本完成了失败的迁移，那么计算机重新启动时必须启用 DB2 自动启动。

Windows 系统

在 Windows 系统上，执行以下步骤来自动启动 DB2:

1. 打开“控制面板”并单击**开始 > 控制面板 > 管理工具 > 服务**。
2. 右键单击 **DB2 - DBSKMV26 - SKLMDB26** 服务，然后右键单击**属性**。
3. 在“属性”对话框的**常规**选项卡上，将**启动类型**更改为**自动**，并单击**应用**。
4. 重新启动系统以验证数据库服务器是否会自动启动。

AIX 和 Linux 系统

如果您在 IBM Security Key Lifecycle Manager V1 中启用了 crontab，那么请输入以下命令来启用 DB2 自动启动。

```
. <DB_home_dir>/sqllib/db2profile
DB_HOME/instance/db2iauto -on sklmdb26
```

其中 sklmdb26 是缺省实例所有者用户标识。如果在安装期间更改了该值，请改用该更改后的用户标识。

迁移属性文件

IBM Security Key Lifecycle Manager 服务器迁移实用程序保留了 *SKLM_HOME*/migration/migratestatus.properties 文件来跟踪已完成的任务。

如果迁移失败，会保留属性文件以用于调试。迁移实用程序还使用保留的文件来确定从哪个点开始新的迁移过程。如果您意外地再次运行迁移，那么实用程序将使用该属性文件来确定迁移是否已成功。

安装后步骤

安装 IBM Security Key Lifecycle Manager 之后，请确保 DB2 和 WebSphere Application Server 服务已正确配置。

仅在使用因特网协议 V6 (IPv6) 的系统上，安装结束时显示的统一资源定位符为 IPv4 URL。在访问 IBM Security Key Lifecycle Manager 之前，请将该 URL 更改为您已知的 IPv6 URL。

服务、端口和进程

安装 IBM Security Key Lifecycle Manager 服务器 之后，请验证所需服务、端口和进程是否正在运行。

Windows 系统:

- 服务
  - WebSphere Application Server: IBM WebSphere Application Server V8.5 - SKLM26Server
  - DB2: DBSKLMV26 - SKLMDB26
- 端口

  注: 所有以下端口都必须处于打开状态且未由任何其他进程使用。
  - 用于访问 IBM Security Key Lifecycle Manager 图形用户界面和 REST 服务的 HTTPS 端口: **9080**
  - 用于访问 WebSphere Integrated Solutions Console 的 HTTPS 端口: **9083**
  - DB2: 缺省值为 **50020**。

    这是针对 DB2 的缺省值。您可以在 IBM Security Key Lifecycle Manager 安装时配置此端口。此值可能是其他端口号，具体取决于安装设置。还存在与缺省端口号关联的其他端口。
  - 用于侦听 KMIP 消息的缺省安装时 SSL 端口: **5696**
  - 用于侦听设备消息的 SSL 端口: **441**
  - 用于侦听设备消息的 TCP 端口: **3801**
  - WebSphere Application Server: **9080 - 9099**

    WebSphere Application Server 安装针对其提供的各种服务必需这些端口。
  - 主服务器和克隆服务器的复制配置文件中用户配置的复制端口。如果在主服务器和克隆服务器之间使用了防火墙，那么该防火墙必须配置为传递因特网控制报文协议 (ICMP)。
- 进程
  - IBM Security Key Lifecycle Manager: `WASService.exe java.exe`
  - DB2: `db2fmp64.exe db2syscs.exe`

如果 V2.6 迁移自 V1.0、V2.0 或 2.0.1:

- 服务
  - Tivoli Integrated Portal: TIPProfile_Port_16340
  - DB2: DB2TKLMV2 - TKLMDB2
- 端口
  - IBM Security Key Lifecycle Manager: 16340、16341、16342、16343、16345、16346、16350、16352、16353
  - DB2: 端口号与 IBM Security Key Lifecycle Manager V1 上的 DB2 端口号相同。还存在与缺省端口号关联的其他端口。
- 进程
  - IBM Security Key Lifecycle Manager: `WASService.exe java.exe`
  - DB2: `db2fmp.exe db2syscs.exe`

AIX 或 Linux 等系统:

- 端口

  注: 所有以下端口都必须处于打开状态且未由任何其他进程使用。
  - 用于访问 IBM Security Key Lifecycle Manager 图形用户界面和 REST 服务的 HTTPS 端口: **9080**
  - 用于访问 WebSphere Integrated Solutions Console 的 HTTPS 端口: **9083**
  - DB2: 缺省值为 **50020**。

    这是针对 DB2 的缺省值。您可以在 IBM Security Key Lifecycle Manager 安装时配置此端口。此值可能是其他端口号，具体取决于安装设置。还存在与缺省端口号关联的其他端口。
  - 用于侦听 KMIP 消息的缺省安装时 SSL 端口: **5696**
  - 用于侦听设备消息的 SSL 端口: **441**
  - 用于侦听设备消息的 TCP 端口: **3801**
  - WebSphere Application Server: **9080 - 9099**

    WebSphere Application Server 安装针对其提供的各种服务必需这些端口。
  - 主服务器和克隆服务器的复制配置文件中用户配置的复制端口。如果在主服务器和克隆服务器之间使用了防火墙，那么该防火墙必须配置为传递因特网控制报文协议 (ICMP)。
- 进程
  - IBM Security Key Lifecycle Manager: WebSphere Application Server 和 Java
  - DB2: `db2fmp64 db2syscs`

安装后的安全性

安装 IBM Security Key Lifecycle Manager 之后，您必须执行若干步骤以确保您的浏览器可识别证书，并保护敏感的用户标识和密码。

指定用于浏览器访问的证书

所有浏览器会触发一个必须覆盖以获取对 WebSphere Application Server 的访问权的证书错误。

关于此任务

因为内部证书的所有者不在签署权限的可信列表中而发生错误。在每个用于访问 IBM Security Key Lifecycle Manager 的浏览器中安装证书。可以使用 WebSphere Application Server 用户界面覆盖证书。

要配置证书，请执行以下步骤:

过程

1. 使用 WASAdmin 用户标识登录 IBM Security Key Lifecycle Manager 服务器。
2. 在“安全性”选项卡上，单击**SSL 证书和密钥管理**。
3. 在“SSL 证书和密钥管理”页面上，单击**管理端点安全配置 -> server1**。 在本地拓扑树中，可能需要单击 **SKLMCell > 节点 > SKLMNode > 服务器 > server1** 来展开树，然后在出站分支中查找 server1。
4. 要设置此端点的特定 SSL 配置，请单击**管理证书**。
5. *解压缩*证书。

   浏览器只需要证书。解压缩操作会检索证书（公用密钥），并将它存储为一个文件。不要导出证书，因为会同时获取公用和专用密钥。
6. 将证书导入浏览器。
   - Firefox
     a. 单击**工具 > 选项 > 高级 > 加密**。
     b. 选择**查看证书 > 导入**按钮。
     c. 导航至导出证书的目标位置。选择证书，然后单击**打开**。
     d. 在“证书管理器”对话框中，选择已导入的证书，然后单击**编辑**。
     e. 在“编辑 Web 站点证书信任设置”对话框中，选择**信任此证书的发布机构**，然后单击**确定**。
     f. 在“证书管理器”对话框中，单击**确定**。
     g. 在“选项”对话框中，单击**确定**。
   - Internet Explorer
     a. 单击**工具 > Internet 选项**。
     b. 选择**内容**选项卡，然后单击**证书**按钮。
     c. 选择**受信任的根证书发布机构**选项卡，然后单击**导入**按钮。
     d. 在“证书导入向导”对话框中，单击**下一步**。
     e. 浏览以查找证书，然后单击**下一步**。
     f. 输入证书的密码，然后单击**下一步**。
     g. 完成向导提供的剩余步骤。
     h. 在“安全警告”对话框中，阅读警告。如果同意，请单击**是**。
7. 在浏览器地址字段，输入指向 IBM Security Key Lifecycle Manager 服务器 的标准的全球资源定位器 (URL)。按下 **Enter** 键。

更改 WebSphere Application Server 密钥库密码

浏览器的 SSL 证书存储在 WebSphere Application Server 密钥库中。在 WebSphere Application Server 上，这些密钥库密码是公共的并且必须进行更改。

关于此任务

当安装应用程序服务器时，每个服务器会为 WebAS 中使用缺省密码值的缺省 SSL 配置创建密钥库和信任库。

过程

1. 使用图形用户界面更改密码:
   a. 使用 WASAdmin 用户标识登录 WebSphere 集成解决方案控制台。
      `https://localhost:9083/ibm/console/logon.jsp`
   b. 在“安全性”选项卡上，单击**SSL 证书和密钥管理**。
   c. 在“SSL 证书和密钥管理”页面上，单击**密钥库和证书 > NodeDefaultKeyStore**。
   d. 更改密钥库密码。
   e. 在“SSL 证书和密钥管理”页面上，单击**密钥库 > NodeDefaultTrustStore**。
   f. 更改信任库密码。
2. 在安全的位置保存密码。

WebSphere Application Server 安全性

必须执行若干步骤以确保 WebSphere Application Server 敏感信息的安全性。

支持人员可能确定需要通过跟踪来调试 **WASService.exe** 命令运行的功能中的问题。对此功能开启跟踪会将可能敏感的跟踪信息写入 Windows 根目录中的 WASService.Trace 文件中。请使用适用于您站点的信息保护步骤来保护 WASService.Trace 文件。

此外，运行 **stopServer** 命令时请小心。不要直接在命令行上输入密码。而应在出现提示时输入 WebSphere Application Server 管理员的用户名和密码。

例如，要停止绑定到 *WAS_HOME* 的所有进程，请输入:

```
stopServer server1
```

出现提示时，请输入用户名和密码。

应避免在命令中包含用户标识和密码。例如，请不要输入:

在 Windows 系统上:

```
stopServer.bat server1 -username wasadmin -password mypwd
```

在诸如 Linux 或 AIX 的系统上:

```
./stopServer.sh server1  -username wasadmin -password mypwd
```

在运行 **ps -aef** 命令以显示关于活动进程的信息之后，可能会显示 WebSphere Application Server 密码。

安装期间的安装错误

安装期间可能会发生必须更正的错误。许多错误消息包含的信息足以更正引起错误的情况。但是，有些错误情况需要更多信息才能更正。

静默安装可能在未显示任何错误消息的情况下退出，但是在日志文件中确实存在错误。 如果静默安装退出时显示返回码零，也请检查日志文件中是否包含错误消息。

Windows 系统:

\<*IM App Data Dir*>\logs

AIX 或 Linux 等系统:

/<*IM App Data Dir*>/logs

如果看到有错误消息显示磁盘或文件系统没有足够的可用磁盘空间:

请除去文件以释放空间，或向系统添加存储器以扩展文件系统的大小。

请不要在安装程序运行时更正该问题。请在进行更正之前先退出安装程序，并在进行更正之后重新启动安装程序。

请参阅第 7 页的『分布式系统的硬件需求』以获取有关磁盘空间和其他硬件需求的信息。

如果在从 Linux 系统向本地机器导出显示内容时，在本地机器上使用 Exceed X 服务器安装 IBM Security Key Lifecycle Manager，那么请不要拒绝许可协议。

如果拒绝许可协议，系统可能会将安装程序视为无响应。请接受许可协议，或者改为使用 Cygwin X 服务器或虚拟网络连接。

使用 Windows 用户和组管理工具除去 sklmdb2 管理员时，在重新安装 IBM Security Key Lifecycle Manager 和 DB2 之前需要先除去先前的 sklmdb2 子目录。

在 IBM Security Key Lifecycle Manager 安装期间，如果先前已使用 Windows 用户和组管理工具删除了作为 DB2 管理员的 sklmdb26 用户标识，那么可能会遇到问题。之后重新安装 IBM Security Key Lifecycle Manager 时将无法安装 DB2。

要修正该问题，请执行以下步骤:

1. 切换到相应的子目录:
   - Windows Server 2012: *drive*:\Users
2. 除去 sklmdb26 子目录。
3. 重新安装 IBM Security Key Lifecycle Manager。使用 Windows 用户和组管理工具来删除用户帐户 sklmdb26 时，不会自动除去 sklmdb26 子目录。

启用自动服务

IBM Security Key Lifecycle Manager 安装过程会启动 IBM Security Key Lifecycle Manager 所需的 DB2 和 WebSphere Application Server 服务。安装过程还会将这些服务设置为自动启动。但是，您可能需要更正自动启动服务产生的错误情况。

Windows 系统

在 Windows 系统上，请使用“Windows 服务”控制台将服务配置为自动启动。

找到以下列表中的服务。对于列表中的每个服务，打开服务的“属性”对话框，并确保**启动类型**设置为自动。如果**服务状态**字段的值为已停止，请单击**启动**以启动该服务。

DB2 - *db2 副本名称 - SKLM_INSTANCE_OWNER*
例如，**DB2 - DBSKLMV26 - SKLMDB6**

DB2 Governor（*db2 副本名称*）
例如，**DB2 Governor (DBSKLMV26)**

DB2 License Server（*db2 副本名称*）
例如，**DB2 License Server (DBSKLMV26)**

DB2 Management Service（*db2 副本名称*）
例如，**DB2 Management Service (DBSKLMV26)**

DB2 Remote Command Server（*db2 副本名称*）
例如，**DB2 Remote Command Server (DBSKLMV26)**

DB2DAS - *DB2DAS_entry*
例如，**DB2DAS - DB2DAS00**

注: 仅当 DAS 服务托管于 Windows 服务中时，才禁用 DB2 Administration Server (DAS)。

WAS 服务 - IBM Security Key Lifecycle Manager
例如，**IBM WebSphere Application Server V8.5 - SKLM26Server**

Linux 系统

在 Linux 系统上，输入以下命令以将 IBM Security Key Lifecycle Manager DB2 实例所有者配置为自动启动:

```
<DB_home_dir>/sqllib/db2profile
DB_HOME/instance/db2iauto -on sklmdb26
```

其中，sklmdb2 是缺省实例所有者用户标识。如果在安装期间更改了该值，请改用该更改后的用户标识。

在 Linux 系统上安装 IBM Security Key Lifecycle Manager 会向 /etc/inittab 文件中添加用于启动 WebSphere Application Server 的命令。在 Linux 系统中，安装程序会在 /etc/init.d 中创建 SecurityKeyLifecycleManager_was.init 文件。您可以在 /etc/initttab 文件中添加类似的命令:

```
slp:2345:wait:/bin/sleep 60
tt:23456789:wait:WAS_HOME/bin/startServer.sh server1
```

AIX 系统

在 AIX 系统上，输入以下命令来将 IBM Security Key Lifecycle Manager DB2 实例所有者配置为自动启动:

```
<DB_home_dir>/sqllib/db2profile
DB_HOME/instance/db2iauto -on sklmdb26
```

其中，sklmdb2 是缺省实例所有者用户标识。如果在安装期间更改了该用户标识，请改用更改后的用户标识。

在 AIX 系统上安装 IBM Security Key Lifecycle Manager 会向 /etc/inittab 文件中添加用于启动 WebSphere Application Server 的命令。您可以编辑 /etc/inittab 文件中的以下命令:

```
sl:2345:wait:/bin/sleep 60
tt:23456:wait:WAS_HOME/bin/startServer.sh server1
```

要将 WebSphere Application Server 配置为自动启动，请遵循 *IBM WebSphere Application Server V6.1 on the Solaris 10 Operating System* 红皮书出版物中描述如何创建 SMF 服务定义的部分中所述的步骤。此文档可从 http://www.redbooks.ibm.com/abstracts/sg247584.html 获取。

将该 Web 页面上的信息改写为基于您的 IBM Security Key Lifecycle Manager 安装的值。例如，在以下脚本中使用您系统中的目录:

```
WAS_DIR="//opt/IBM/WebSphere/AppServer/profiles/KLMProfile"
```

在某些系统上，可能需要将清单文件中的超时值从 60 增加到 300。

设置会话超时时间间隔

IBM Security Key Lifecycle Manager 用户界面会话可以配置为在三十分钟处于不活动状态后超时，或者没有任何时间限制始终保持活动状态。

过程

1. 可以使用图形用户界面来设置会话超时时间间隔:
   a. 使用 WASAdmin 用户标识登录 WebSphere 集成解决方案控制台。

      ```
      https://localhost:9083/ibm/console/logon.jsp
      ```

   b. 在**应用程序**选项卡上，单击**应用程序类型 > WebSphere 企业应用程序**。
   c. 在“企业应用程序”页面上，单击 **sklm_kms**。
   d. 在“Web 模块属性”部分中，单击**会话管理**。
   e. 在“常规属性”部分中，选择**覆盖会话管理**。
   f. 在“会话超时”部分中，选择**无超时**以时刻保持活动状态而无超时。
   g. 要以分钟为单位设置不活动超时，请选择**设置超时**并指定所需的不活动超时值。
2. 单击**应用**。
3. 单击**确定**。

设置最大事务超时值

总事务超时值设置为 600 秒。根据设置的不同，某些长时间运行的 IBM Security Key Lifecycle Manager 操作可能超时。

关于此任务

长时间运行的 IBM Security Key Lifecycle Manager 操作可能会超时，报告的错误消息如下例所示:

```
[10/21/08 14:28:41:693 CDT] 00000020 TimeoutManage I
WTRN0006W: Transaction 00000110001 has timed out after xxx seconds.
```

要将事务超时时间间隔配置为一个更大的值，请执行以下步骤:

过程

1. 停止服务器。
   - Windows 系统:

     在 *WAS_HOME*\bin 属性中，输入:

     ```
     stopServer.bat server1
     ```
   - AIX 和 Linux 系统:

     在 *WAS_HOME*/bin 目录中，输入:

     ```
     ./stopServer.sh server1
     ```
2. 编辑此文件:

   ```
   ..\profiles\KLMProfile\config\cells\SKLMCell\nodes\SKLMNode\
     servers\server1\server.xml
   ```
3. 将 **propogatedOrBMTTranLifetimeTimeout** 参数更改为一个更大的值。
4. 保存文件。
5. 启动服务器。
   - Windows 系统:

     在 *WAS_HOME*\bin 属性中，输入:

     ```
     startServer.bat server1
     ```
   - AIX 和 Linux 系统:

     在 *WAS_HOME*/bin 目录中，输入:

     ```
     ./startServer.sh server1
     ```

确保迁移后的 DB2 版本正确

在连接到 IBM Security Key Lifecycle Manager 数据库之前，请确保使用的是 DB2 的当前版本。

关于此任务

将 IBM Security Key Lifecycle Manager 从 V1.0、V2.0、V2.0.1 或 V2.5 迁移到 V2.6 之后，DB2 的过时版本 10.1 和更高版本均可用。

请执行以下步骤:

过程

1. 以 AIX 或 Linux 之类的系统的数据库实例所有者或 Windows 系统上的 DB2 管理员的身份登录。
2. 请确保 DB2 的当前版本可用。请执行以下步骤:

   Windows 系统:
   - 单击**开始 > IBM DB2 > DB2SKLMV26 > 命令行工具 > 命令行处理器**。请指定:

     ```
     set DB2INSTANCE=sklmdb26
     ```
   - 导航至 *drive*:\Program Files (x86)\IBM\DB2SKLMV26\bin 目录，并确保可以成功运行 DB2 命令。例如，输入:

```
db2cmd
db2stop
db2start
```

AIX 或 Linux 等系统:

- 导航至 /opt/IBM/DB2SKLMV26/bin 目录。
- 请确保可以成功运行 DB2 命令。例如，输入:

```
<DB_home_dir>/sqllib/db2profile
db2stop
db2start
```

3. 启动 IBM Security Key Lifecycle Manager V2.6。

更改 DB2 服务器 主机名

在更改 IBM Security Key Lifecycle Manager 系统主机名之后，可能需要更改 DB2 服务器 的主机名。

关于此任务

从位于以下 Web 地址的技术说明中获取用于更改您的 DB2 服务器 级别的主机名的最新步骤: http://www.ibm.com/support/docview.wss?rs=71&context=SSEPGG&context=SSEPDU&context=SSVGXH&context=SSVGZB&context=SSFHEG&context=SSYK8P&context=SSTLZ9&q1=db2+change+hostname&uid=swg21258834&loc=en_US&cs=utf-8&lang=en

更改现有的 WebSphere Application Server 主机名

在更改系统主机名之前，必须先更改 WebSphere Application Server 的主机名。

过程

1. 更改 WebSphere Application Server 的主机名。有关如何更改主机名的更多信息，请参阅 IBM WebSphere Application Server 文档 (http://www-01.ibm.com/support/knowledgecenter/SSEQTP_8.5.5/com.ibm.websphere.base.iseries.doc/ae/tagt_hostname.html)。
2. 此任务成功后，请更改 DB2 服务器的主机名。有关更多信息，请参阅『更改 DB2 服务器 主机名』。

停止 DB2 服务器

要停止数据库服务器，先停止 WebSphere Application Server，然后停止 DB2 服务器。

关于此任务

您必须为 AIX 或 Linux 等系统的数据库实例所有者，或者 Windows 系统的本地管理员。

要停止数据库服务器，请执行以下步骤:

过程

1. 以 AIX 或 Linux 等系统的数据库实例所有者或 Windows 系统的本地管理员的身份登录。

2. 停止 WebSphere Application Server。请输入此命令:

   Windows 系统:

   ```
   cd C:\Program Files (x86)\IBM\WebSphere\AppServer\bin
   .\stopServer.bat server1 -username wasadmin -password mysecretpwd
   ```

   AIX 或 Linux 等系统:

   ```
    /opt/IBM/WebSphere/AppServer/bin/stopServer.sh server1
   -username wasadmin
     -password mysecretpwd
   ```

3. 停止 DB2 服务器。请输入以下命令:

   Windows 系统:

   ```
   set DB2INSTANCE=sklmdb26
   db2stop
   ```

   AIX 或 Linux 等系统:

   ```
   su -sklmdb26
   db2stop
   ```

配置 SSL

在安装了 IBM Security Key Lifecycle Manager 之后，可能要使用 SSL 配置安全通信。

关于此任务

此选项由 *SKLM_HOME*/config/SKLMConfig.properties 文件中的 **config.keystore.ssl.certalias** 属性控制。

如果指定了传输端口，此别名指向一个现有的证书，它用于驱动器和 IBM Security Key Lifecycle Manager 服务器 之间的安全通信的 SSL 认证。

如果从 Encryption Key Manager 迁移数据，那么 TransportListener 信任库中的所有证书都将导入 IBM Security Key Lifecycle Manager 密钥库。

来自 TransportListener *密钥库*的证书已设置为 IBM Security Key Lifecycle Manager 的 SSL 证书。**config.keystore.ssl.certalias** 属性将使用此证书的别名进行更新。

要配置用于安全通信的 SSL，请执行以下步骤:

过程

1. 导航至相应的的页面或目录。
   - 图形用户界面:

     登录图形用户界面。您可以选择以下任一路径:
     - 单击 **IBM Security Key Lifecycle Manager > 配置 > SSL/KMIP**。
     - **IBM Security Key Lifecycle Manager > 高级配置 > 服务器证书**。
   - 命令行界面:

     在 *WAS_HOME*/bin 目录中，使用 Jython 启动 **wsadmin** 会话。使用授权的用户标识（例如，SKLMAdmin 用户标识）登录到 **wsadmin**。例如，在 Windows 系统上，浏览至 *drive*:\Program Files (x86)\IBM\WebSphere\AppServer\bin 目录并输入:

– Windows 系统:

```
wsadmin -username SKLMAdmin -password mypwd -lang jython
```

– AIX 或 Linux 等系统:

```
./wsadmin.sh -username SKLMAdmin -password mypwd -lang jython
```

2. 指定用于 SSL 通信的证书。
   - 图形用户界面:

     指定一个证书作为 SSL 证书:

     – 在“用于提供密钥的 SSL/KMIP”页面上，选择将密钥库中的现有证书用作 SSL 证书的选项。选择一个证书，然后单击**确定**。
     – 另外，在“管理服务器证书”页面上，选择一个现有证书并单击**修改**。指定此证书是当前正在使用的证书，然后单击**修改证书**。
   - 命令行界面:
     – 要查看属性值，请使用 **tklmConfigGetEntry** 命令。例如，可能想要验证已迁移的证书是否设置为 SSL 证书。

       此 Jython 格式的命令会获取 **config.keystore.ssl.certalias** 属性的当前值。

       ```
       wsadmin>print AdminTask.tklmConfigGetEntry
        ('[-name config.keystore.ssl.certalias]')
       ```

     – 要更改属性值，请使用 **tklmConfigUpdateEntry** 命令指定 IBM Security Key Lifecycle Manager 服务器 使用的证书。

     例如，此 Jython 格式的命令示例会更改 **config.keystore.ssl.certalias** 属性的值。

     ```
     print AdminTask.tklmConfigUpdateEntry
       ('[-name config.keystore.ssl.certalias
        -value mycert]')
     ```

3. 成功指示符会根据界面的不同而不同:
   - 图形用户界面:

     在“成功”页面上的“下一步”中，单击要执行的相关任务。
   - 命令行界面:

     完成消息表示成功。

确定当前端口号

完成 IBM Security Key Lifecycle Manager 服务器 安装之后，可能需要确定 IBM Security Key Lifecycle Manager 服务器 和 WebSphere Integrated Solutions Console 的安全端口号。

关于此任务

这些端口号的值由 *WAS_HOME*/profiles/KLMProfile/properties/portdef.props 文件中的 **WC_defaulthost_secure** 或 **WC_adminhost_secure** 属性指定。例如，文件可以指定这些值:

```
WC_defaulthost_secure=9080
WC_adminhost_secure=9083
```

WC_defaulthost_secure 属性值对应于 IBM Security Key Lifecycle Manager 服务器安全端口，而 **WC_adminhost_secure** 属性值对应于 WebSphere Integrated Solutions Console 安全端口。

验证安装

在分布式系统进行安装之后，请验证 IBM Security Key Lifecycle Manager 安装是否成功。

执行以下操作以验证分布式系统上的安装:

1. 启动和停止服务器。请参阅第 91 页的『在分布式系统上启动和停止 IBM Security Key Lifecycle Manager 服务器』以获取详细信息。
2. 在 Web 浏览器中打开 IBM Security Key Lifecycle Manager。
   a. 使用登录 URL 访问 IBM Security Key Lifecycle Manager Web 界面。

      ```
      https://ip-address:port/ibm/SKLM/login.jsp
      ```

      ip-address 的值为 IBM Security Key Lifecycle Manager 服务器 的 IP 地址或 DNS 地址。

      port 的值是 IBM Security Key Lifecycle Manager 服务器 用于侦听请求的端口号。缺省值为 9080。

      在 Windows 系统上，这些信息位于“开始”菜单上。单击**开始 > 所有程序 > IBM Security Key Lifecycle Manager 2.6**。
   b. 使用凭证登录并确保显示 IBM Security Key Lifecycle Manager 欢迎页面。
3. 使用命令行界面列出 IBM Security Key Lifecycle Manager 命令组。例如，从 *WAS_HOME*/bin 输入:

   ```
   ./wsadmin.sh -username <sklmadmin id> -password <sklmadmin passwd> -lang jython
   ```

   当 **wsadmin** 工具发出提示时，请输入以下命令:

   ```
   wsadmin>print AdminTask.help("-commandGroups")
   ```

   将显示 IBM Security Key Lifecycle Manager 命令组。例如，列表将包含备份命令和其他命令组:

   ```
   TKLMBackupCommands - IBM Security Key Lifecycle Manager backup/restore commands
   ```

启用 Internet Explorer V9.0、V10 和 V11 的脚本设置

确保已启用 Internet Explorer V9.0 和 V10.0 的脚本编制设置。

关于此任务

除非已为 Internet Explorer V9.0、V10 和 11.0 启用了特定的脚本编制设置，否则稍后可能无法创建 IBM Security Key Lifecycle Manager 用户。

请确保已启用了以下浏览器设置:

- 允许在脚本中的状态栏更新
- 活动脚本
- Java applet 的脚本编制

过程

1. 打开浏览器，然后单击**工具 > Internet 选项 > 安全性**。
2. 滚动“脚本编制”选项的安全设置列表，确保已启用了以下设置:
   - 允许在脚本中的状态栏更新
   - 活动脚本
   - Java applet 的脚本编制
3. 单击**确定**。

在分布式系统上启动和停止 IBM Security Key Lifecycle Manager 服务器

可能想要使用 **startServer** 或 **stopServer** 命令启动或停止 IBM Security Key Lifecycle Manager 服务器。例如，在复原任务完成之后，重新启动 IBM Security Key Lifecycle Manager 服务器。

关于此任务

当 SKLMConfig.properties 文件中的 **autoRestartAfterRestore** 属性值为 true（缺省值）时，复原备份文件后，IBM Security Key Lifecycle Manager 服务器会自动重新启动。

用于启动和停止 IBM Security Key Lifecycle Manager 服务器 的脚本在 *WAS_HOME*/bin 目录中。

过程

1. 导航至 *WAS_HOME*/bin 目录。
2. 启动或停止服务器。
   - 启动

     在 Windows 系统上:
     ```
     startServer.bat server1
     ```
     在诸如 Linux 或 AIX 的系统上:
     ```
     ./startServer.sh server1
     ```
   - 停止

     在 Windows 系统上:
     ```
     stopServer.bat server1
     ```
     在诸如 Linux 或 AIX 的系统上:
     ```
     ./stopServer.sh server1
     ```

   缺省情况下，将启用全局安全性。请输入 WebSphere Application Server 管理员的用户标识和密码，作为 stopServer 的参数。当省略这些参数时，脚本会提示您输入参数，但是可以在命令行上指定:

   在 Windows 系统上:
   ```
   stopServer.bat server1 -username wasadmin -password mypwd
   ```
   在诸如 Linux 或 AIX 的系统上:
   ```
   ./stopServer.sh server1  -username wasadmin -password mypwd
   ```

下一步做什么

确定 IBM Security Key Lifecycle Manager 是否正在运行。例如，在 Web 浏览器中打开 IBM Security Key Lifecycle Manager，然后登录。

启用全局安全性

可能发生必须启用全局安全性的情况。

关于此任务

当使用 IBM Security Key Lifecycle Manager 时，不要禁用全局安全性。

过程

1. 要启用全局安全性，请以 WebSphere Application Server 管理员 WASAdmin 的身份登录。
2. 在导航栏中，单击**安全性**。
3. 单击**保证管理、应用程序和基础结构的安全**。
4. 勾选**启用管理安全性**复选框。

   请确保也选择了**启用应用程序安全性**，并且未选择**使用 Java 2 安全性限制对本地资源的应用程序访问**。
5. 单击**应用**。
6. 在“消息”框中单击**保存**。单击**注销**。
7. 停止并重新启动服务器。
8. 重新装入 IBM Security Key Lifecycle Manager 登录页面。验证该页面是否需要密码。

禁用全局安全性

可能发生必须禁用全局安全性的情况。

关于此任务

当使用 IBM Security Key Lifecycle Manager 时，不要禁用全局安全性。

过程

1. 要禁用全局安全性，请以 WebSphere Application Server 管理员 WASAdmin 的身份登录。
2. 在导航栏中，单击**安全性**。
3. 单击**保证管理、应用程序和基础结构的安全**。
4. 清除**启用管理安全性**复选框。
5. 单击**应用**。
6. 在“消息”框中单击**保存**。单击**注销**。
7. 停止并重新启动服务器。
8. 重新装入 IBM Security Key Lifecycle Manager 登录页面。验证页面是否不需要密码。

安装前工作表

在开始安装和配置 IBM Security Key Lifecycle Manager 之前，您可以完成以下工作表以识别完成 IBM Security Key Lifecycle Manager 安装所需的配置参数。

常规安装参数

使用工作表可记录一般安装参数。

表 9. 常规安装参数

选项	描述	缺省值或示例值	您的值
安装方式	运行安装程序的方式。	gui（缺省值） silent	
重要步骤: 检查可用磁盘空间	确保具有足够的可用磁盘空间。	请参阅第 7 页的『分布式系统的硬件需求』以了解值。	

DB2 配置参数

使用工作表可记录与 DB2 安装和配置相关的条目。

表 10. DB2 配置参数

字段名称	描述	缺省值或示例值	您的值
DB2 目标	要安装 DB2 的目录	**Windows 系统:** *drive*:\Program Files (x86)\IBM\DB2SKLMV26 **AIX 和 Linux 系统:** /opt/IBM/DB2SKLMV26	
DB2 管理员标识	IBM Security Key Lifecycle Manager 数据库管理员（也称为实例所有者）的用户标识	sklmdb26	
DB2 管理员密码	数据库管理员用户标识的密码		
数据库名称	IBM Security Key Lifecycle Manager 数据库的名称	SKLMDB26	
DB2 端口	DB2 服务侦听端口	50020	
管理员主目录/数据库主目录	创建数据库实例和格式化表的目录	C:	

表 10. DB2 配置参数 (续)

字段名称	描述	缺省值或示例值	您的值
管理员组	数据库的实例所有者所属的组。	如果 DB2 位于 AIX 或 Linux 等系统上，您的用户标识必须位于 bin 或 root 用户组中，或者位于其成员包含 root 用户的其他组中。	
实例盘符	要安装 DB2 的驱动器（仅限 Windows 系统）	C:	

样本响应文件

您可能需要对 Windows 和其他系统使用样本响应文件。安装之前，您还必须阅读并同意此产品的许可条款。要查找响应文件和许可条款文件，请查看安装映像文件的根目录。/license 子目录中包含文本格式的许可证文件。

除非您执行以下步骤，否则安装将失败。

在响应文件中，对指定许可证的行进行以下更改:

- 将缺省值设置为 true 以表示您同意许可证的条款。
- 除去行首的井字符 (#) 来对该行取消注释。

在 Windows 系统上新安装 V2.6

此示例响应文件包含响应信息，用于在 Windows 系统上安装 IBM Security Key Lifecycle Manager V2.6，或者进行要迁移 Encryption Key Manager 的安装。

```
<?xml version='1.0' encoding='UTF-8'?>
<agent-input>
  <server>
    <repository location='C:\disk1\im'/>
    <repository location='C:\disk1'/>
  </server>
  <profile id='IBM Installation Manager' installLocation='C:\Program Files <x86>
\IBM\Installation Manager\eclipse' kind='self'>
    <data key='eclipseLocation' value='C:\Program Files <x86>\IBM\Installation Manager\eclipse'/>
    <data key='user.import.profile' value='false'/>
    <data key='cic.selector.os' value='win32'/>
    <data key='cic.selector.arch' value='x86_64'/>
    <data key='cic.selector.ws' value='win32'/>
  </profile>
  <install modify='false'>
    <!-- IBMÂ® Installation Manager 1.8.2 -->
    <offering profile='IBM Installation Manager' id='com.ibm.cic.agent'
features='agent_core,agent_jre,agent_web' installFixes='none'/>
 <!-- IBM DB2 10.5.0.0 -->
    <offering profile='IBM DB2' id='com.ibm.db2.ofng' features='com.ibm.db2.ofng'
 installFixes='none'/>
 <!-- IBM WebSphere Application Server 8.5.5.7 -->
    <offering profile='IBM WebSphere Application Server V8.5' id=
'com.ibm.websphere.BASE.v85' features='core.feature,ejbdeploy,thinclient,
embeddablecontainer,com.ibm.sdk.6_32bit' installFixes='none'/>
    <!-- IBM WebSphere SDK Java Technology Edition <Optional> 7.0.4.1 -->
    <offering profile='IBM WebSphere Application Server V8.5' id=
'com.ibm.websphere.IBMJAVA.v70' features='com.ibm.sdk.7' installFixes='none'/>
  <!-- IBM Security Key Lifecycle Manager 2.6.0.0 -->
    <offering profile='IBM Security Key Lifecycle Manager v2.6' id=
'com.ibm.sklm26.win32' features='main.feature' installFixes='none'/>
  </install>
  <profile id='IBM DB2' installLocation='C:\Program Files <x86>\IBM\DB2SKLMV26'>
    <data key='eclipseLocation' value='C:\Program Files <x86>\IBM\DB2SKLMV26'/>
    <data key='user.import.profile' value='false'/>
    <data key='cic.selector.os' value='win32'/>
    <data key='cic.selector.arch' value='x86'/>
    <data key='cic.selector.ws' value='win32'/>
    <data key='user.DB2_ADMIN_ID,com.ibm.db2.ofng' value='sklmdb26'/>
    <data key='user.DB2_ADMIN_PWD,com.ibm.db2.ofng' value='5CWzYx4KYl0tqj
/VbyOrug=='/>
    <data key='user.CONFIRM_PASSWORD,com.ibm.db2.ofng' value='5CWzYx4KYl0tqj
/VbyOrug=='/>
    <data key='user.DB2_DB_HOME,com.ibm.db2.ofng' value='C:'/>
    <data key='user.DB2_DB_NAME,com.ibm.db2.ofng' value='SKLMDB26'/>
    <data key='user.DB2_DB_PORT,com.ibm.db2.ofng' value='50020'/>
    <data key='user.DB2_EXISTS,com.ibm.db2.ofng' value='false'/>
    <data key='user.DB2_LOCATION,com.ibm.db2.ofng' value='C:\\Program Files <x86>
```

```
\\IBM\\DB2SKLMV26'/>
    <data key='cic.selector.nl' value='en'/>
  </profile>
  <profile id='IBM WebSphere Application Server V8.5' installLocation=
'C:\Program Files <x86>\IBM\WebSphere\AppServer'>
    <data key='eclipseLocation' value='C:\Program Files <x86>\IBM\WebSphere\AppServer'/>
    <data key='user.import.profile' value='false'/>
    <data key='cic.selector.os' value='win32'/>
    <data key='cic.selector.arch' value='x86'/>
    <data key='cic.selector.ws' value='win32'/>
    <data key='cic.selector.nl' value='en'/>
  </profile>

  <profile id='IBM Security Key Lifecycle Manager v2.6' installLocation=
'C:\Program Files <x86>\IBM\SKLMV26'>
    <data key='eclipseLocation' value='C:\Program Files <x86>\IBM\SKLMV26'/>
    <data key='user.import.profile' value='false'/>
    <data key='cic.selector.os' value='win32'/>
    <data key='cic.selector.arch' value='x86'/>
    <data key='cic.selector.ws' value='win32'/>
    <data key='user.IS_SILENT_MODE,com.ibm.sklm26.win32' value='false'/>
    <data key='user.EKM_PROPFILE,com.ibm.sklm26.win32'
value='C:\KeyManagerConfig.properties'/>
    <data key='user.EKM_MIGRATION,com.ibm.sklm26.win32' value='false'/>
    <data key='user.PROFILE_NAME,com.ibm.sklm26.win32' value='KLMProfile'/>
    <data key='user.WAS_ADMIN_ID,com.ibm.sklm26.win32' value='wasadmin'/>
    <data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm26.win32' value='zN39fpCc9SqIryGJM7+02A=='/>
    <data key='user.WAS_ADMIN_CONF_PWD,com.ibm.sklm26.win32'
value='zN39fpCc9SqIryGJM7+02A=='/>
    <data key='user.SKLM_ADMIN_USER,com.ibm.sklm26.win32' value='SKLMAdmin'/>
    <data key='user.SKLM_ADMIN_PASSWORD,com.ibm.sklm26.win32'
value='mIk4YV2XPl82kE7evFjqmw=='/>
    <data key='user.SKLM_ADMIN_CONF_PWD,com.ibm.sklm26.win32'
value='mIk4YV2XPl82kE7evFjqmw=='/>
    <
data key='user.SKLM_APP_PORT,com.ibm.sklm26.win32' value='9080'/>
    <data key='cic.selector.nl' value='en'/>
  </profile>
  <preference name='com.ibm.cic.common.core.preferences.eclipseCache'
value='C:\Program Files <x86>\IBM\IBMIMShared'/>
  <preference name='com.ibm.cic.common.core.preferences.connectTimeout'
value='30'/>
  <preference name='com.ibm.cic.common.core.preferences.readTimeout' value='45'/>
  <preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount'
value='0'/>
  <preference name='offering.service.repositories.areUsed' value='true'/>
  <preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false'/>
  <preference name='com.ibm.cic.common.core.preferences.http.
disablePreemptiveAuthentication' value='false'/>
  <preference name='http.ntlm.auth.kind' value='NTLM'/>
  <preference name='http.ntlm.auth.enableIntegrated.win32' value='true'/>
  <preference name='com.ibm.cic.common.core.preferences.
preserveDownloadedArtifacts' value='true'/>
  <preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false'/>
  <preference name='PassportAdvantageIsEnabled' value='false'/>
  <preference name='com.ibm.cic.common.core.preferences.searchForUpdates'
value='false'/>
  <preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false'/>
  <preference name='com.ibm.cic.common.sharedUI.showErrorLog' value='true'/>
  <preference name='com.ibm.cic.common.sharedUI.showWarningLog' value='true'/>
  <preference name='com.ibm.cic.common.sharedUI.showNoteLog' value='true'/>
</agent-input>
```

在 Linux 系统上新安装 V2.6

此示例响应文件包含响应信息，用于在 Linux 之类的系统上安装 IBM Security Key Lifecycle Manager V2.6，或者进行要迁移 Encryption Key Manager 的安装。

```
<?xml version='1.0' encoding='UTF-8'?>
<agent-input>
  <server>
    <repository location='/disk1/im'/>
    <repository location='/disk1/'/>
  </server>
  <profile id='IBM Installation Manager' installLocation='/opt/IBM/
InstallationManager/eclipse' kind='self'>
    <data key='eclipseLocation' value='/opt/IBM/InstallationManager/eclipse'/>
```

```
    <data key='user.import.profile' value='false'/>
    <data key='cic.selector.os' value='linux'/>
    <data key='cic.selector.arch' value='x86_64'/>
    <data key='cic.selector.ws' value='gtk'/>
  </profile>
  <install modify='false'>
    <offering profile='IBM Installation Manager' id='com.ibm.cic.agent'
features='agent_core,agent_jre,agent_web' installFixes='none'/>
 <offering profile='IBM DB2' id='com.ibm.db2.linux.ofng' features=
'com.ibm.com.ibm.db2.linux' installFixes='none'/>
 <offering profile='IBM WebSphere Application Server V8.5' id=
'com.ibm.websphere.BASE.v85' features='core.feature,ejbdeploy,thinclient,
embeddablecontainer,com.ibm.sdk.6_32bit' installFixes='none'/>
 <offering profile='IBM WebSphere Application Server V8.5' id='com.ibm.
websphere.IBMJAVA.v70' features='com.ibm.sdk.7' installFixes='none'/>
 <offering profile='IBM Security Key Lifecycle Manager v2.6' id=
'com.ibm.sklm26.linux' features='main.feature' installFixes='none'/>
  </install>
  <profile id='IBM DB2' installLocation='/opt/IBM/DB2SKLMV26'>
    <data key='eclipseLocation' value='/opt/IBM/DB2SKLMV26'/>
    <data key='user.import.profile' value='false'/>
    <data key='cic.selector.os' value='linux'/>
    <data key='cic.selector.arch' value='x86_64'/>
    <data key='cic.selector.ws' value='gtk'/>
    <data key='user.DB2_ADMIN_ID,com.ibm.db2.linux.ofng' value='sklmdb26'/>
    <data key='user.DB2_ADMIN_PWD,com.ibm.db2.linux.ofng' value='5CWzYx4KYl0tqj/
VbyOrug=='/>
    <data key='user.CONFIRM_PASSWORD,com.ibm.db2.linux.ofng' value=
'5CWzYx4KYl0tqj/VbyOrug=='/>
    <data key='user.DB2_DB_HOME,com.ibm.db2.linux.ofng' value='/home/sklmdb26'/>
    <data key='user.DB2_DB_NAME,com.ibm.db2.linux.ofng' value='SKLMDB26'/>
    <data key='user.DB2_DB_PORT,com.ibm.db2.linux.ofng' value='50020'/>
    <data key='user.DB2_EXISTS,com.ibm.db2.linux.ofng' value='false'/>
    <data key='user.DB2_LOCATION,com.ibm.db2.linux.ofng' value='/opt/IBM/DB2SKLMV26'/>
    <data key='user.DB2_DB_LHOME,com.ibm.db2.linux.ofng' value='/home/sklmdb26'/>
    <data key='user.DB2_ADMIN_GRP,com.ibm.db2.linux.ofng' value='root'/>
    <data key='cic.selector.nl' value='en'/>
  </profile>
  <profile id='IBM WebSphere Application Server V8.5' installLocation=
'/opt/IBM/
WebSphere/AppServer'>
    <data key='eclipseLocation' value='/opt/IBM/WebSphere/AppServer'/>
    <data key='user.import.profile' value='false'/>
    <data key='cic.selector.os' value='linux'/>
    <data key='cic.selector.arch' value='x86'/>
    <data key='cic.selector.ws' value='gtk'/>
    <data key='cic.selector.nl' value='en'/>
  </profile>
  <profile id='IBM Security Key Lifecycle Manager v2.6' installLocation='/opt/IBM/SKLMV26'>
    <data key='eclipseLocation' value='/opt/IBM/SKLMV26'/>
    <data key='user.import.profile' value='false'/>
    <data key='cic.selector.os' value='linux'/>
    <data key='cic.selector.arch' value='x86_64'/>
    <data key='cic.selector.ws' value='gtk'/>
    <data key='user.IS_SILENT_MODE,com.ibm.sklm26.linux' value='false'/>
    <data key='user.EKM_PROPFILE,com.ibm.sklm26.linux' value='/opt/IBM/
KeyManagerConfig.properties'/>
    <data key='user.EKM_MIGRATION,com.ibm.sklm26.linux' value='false'/>
    <data key='user.PROFILE_NAME,com.ibm.sklm26.linux' value='KLMProfile'/>
    <data key='user.WAS_ADMIN_ID,com.ibm.sklm26.linux' value='wasadmin'/>
    <data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm26.linux' value='zN39fpCc9SqIryGJM7+02A=='/>
    <data key='user.WAS_ADMIN_CONF_PWD,com.ibm.sklm26.linux' value='zN39fpCc9SqIryGJM7+02A=='/>
    <data key='user.SKLM_ADMIN_USER,com.ibm.sklm26.linux' value='SKLMAdmin'/>
    <data key='user.SKLM_ADMIN_PASSWORD,com.ibm.sklm26.linux' value=
'mIk4YV2XPl82kE7evFjqmw=='/>
    <data key='user.SKLM_ADMIN_CONF_PWD,com.ibm.sklm26.linux' value=
'mIk4YV2XPl82kE7evFjqmw=='/>
    <data key='user.SKLM_APP_PORT,com.ibm.sklm26.linux' value='9080'/>
    <data key='cic.selector.nl' value='en'/>
  </profile>
  <preference name='com.ibm.cic.common.core.preferences.eclipseCache'
value='/opt/IBM/IBMIMShared'/>
  <preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30'/>
  <preference name='com.ibm.cic.common.core.preferences.readTimeout' value='45'/>
  <preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0'/>
  <preference name='offering.service.repositories.areUsed' value='true'/>
  <preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false'/>
  <preference name='com.ibm.cic.common.core.preferences.http.
disablePreemptiveAuthentication' value='false'/>
  <preference name='http.ntlm.auth.kind' value='NTLM'/>
```

```
  <preference name='http.ntlm.auth.enableIntegrated.win32' value='true'/>
  <preference name='com.ibm.cic.common.core.preferences.
preserveDownloadedArtifacts' value='true'/>
  <preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false'/>
  <preference name='PassportAdvantageIsEnabled' value='false'/>
  <preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false'/>
  <preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false'/>
  <preference name='com.ibm.cic.common.sharedUI.showErrorLog' value='true'/>
  <preference name='com.ibm.cic.common.sharedUI.showWarningLog' value='true'/>
  <preference name='com.ibm.cic.common.sharedUI.showNoteLog' value='true'/>
</agent-input>
```

在 Linux for System z 上新安装 V2.6

此示例响应文件包含响应信息，用于在 Linux for System z 上安装 IBM Security Key Lifecycle Manager V2.6，或者进行要迁移 Encryption Key Manager 的安装。

```
<?xml version="1.0" encoding="UTF-8"?>
<!--The "acceptLicense" attribute has been deprecated. Use "-acceptLicense"
command line option to accept license agreements.-->
<agent-input acceptLicense='true'>
 <server>
  <repository location='/disk1/im'/>
  <repository location='/disk1/'/>
 </server>
 <profile id='IBM Installation Manager' installLocation='/opt/IBM/
InstallationManager/eclipse' kind='self'>
  <data key='eclipseLocation' value='/opt/IBM/InstallationManager/eclipse'/>
  <data key='user.import.profile' value='false'/>
  <data key='cic.selector.os' value='linux'/>
  <data key='cic.selector.arch' value='s390'/>
  <data key='cic.selector.ws' value='gtk'/>
 </profile>
 <install modify='false'>
  <offering id='com.ibm.cic.agent'  profile='IBM Installation Manager'
features='agent_core,agent_jre' installFixes='none'/>
  <offering id='com.ibm.db2.linux.ofng'  profile='IBM DB2' features=
'com.ibm.com.ibm.db2.linux' installFixes='none'/>
  <offering id='com.ibm.websphere.BASE.v85'  profile='IBM WebSphere
Application Server V8.5' features='core.feature,ejbdeploy,thinclient,
embeddablecontainer,com.ibm.sdk.6_32bit' installFixes='none'/>
  <offering profile='IBM WebSphere Application Server V8.5' id=
'com.ibm.websphere.IBMJAVA.v70' features='com.ibm.sdk.7' installFixes='none'/>
  <offering id='com.ibm.sklm26.linux'  profile='IBM Security Key Lifecycle
Manager v2.6' features='main.feature' installFixes='none'/>
 </install>
 <profile id='IBM DB2' installLocation='/opt/IBM/DB2SKLMV26'>
  <data key='eclipseLocation' value='/opt/IBM/DB2SKLMV26'/>
  <data key='user.import.profile' value='false'/>
  <data key='cic.selector.os' value='linux'/>
  <data key='cic.selector.arch' value='s390'/>
  <data key='cic.selector.ws' value='gtk'/>
  <data key='user.DB2_ADMIN_ID,com.ibm.db2.linux.ofng' value='sklmdb26'/>
  <data key='user.DB2_ADMIN_GRP,com.ibm.db2.linux.ofng' value='root'/>
  <data key='user.DB2_ADMIN_PWD,com.ibm.db2.linux.ofng' value=
'SwIhGBTDHcJok80Ux4Sb3g=='/>
  <data key='user.CONFIRM_PASSWORD,com.ibm.db2.linux.ofng' value='SwIhGBTDHcJok80Ux4Sb3g=='/>
  <data key='user.DB2_DB_HOME,com.ibm.db2.linux.ofng' value='/home/sklmdb26'/>
  <data key='user.DB2_DB_LHOME,com.ibm.db2.linux.ofng' value='/home/sklmdb26'/>
  <data key='user.DB2_DB_NAME,com.ibm.db2.linux.ofng' value='SKLMDB26'/>
  <data key='user.DB2_DB_PORT,com.ibm.db2.linux.ofng' value='50020'/>
  <data key='user.DB2_EXISTS,com.ibm.db2.linux.ofng' value='false'/>
  <data key='user.DB2_LOCATION,com.ibm.db2.linux.ofng' value='/opt/IBM/DB2SKLMV26'/>
  <data key='cic.selector.nl' value='en'/>
 </profile>
 <profile id='IBM WebSphere Application Server V8.5' installLocation=
'/opt/IBM/WebSphere/AppServer'>
  <data key='eclipseLocation' value='/opt/IBM/WebSphere/AppServer'/>
  <data key='user.import.profile' value='false'/>
  <data key='cic.selector.os' value='linux'/>
  <data key='cic.selector.arch' value='s390'/>
  <data key='cic.selector.ws' value='gtk'/>
  <data key='cic.selector.nl' value='en'/>
 </profile>
 <profile id='IBM Security Key Lifecycle Manager v2.6' installLocation='/opt/IBM/SKLMV26'>
  <data key='eclipseLocation' value='/opt/IBM/SKLMV26'/>
  <data key='user.import.profile' value='false'/>
```

```
  <data key='cic.selector.os' value='linux'/>
  <data key='cic.selector.arch' value='s390'/>
  <data key='cic.selector.ws' value='gtk'/>
  <data key='user.IS_SILENT_MODE,com.ibm.sklm26.linux' value='false'/>
  <data key='user.EKM_PROPFILE,com.ibm.sklm26.linux' value='/opt/IBM/KeyManagerConfig.properties'/>
  <data key='user.EKM_MIGRATION,com.ibm.sklm26.linux' value='false'/>
  <data key='user.PROFILE_NAME,com.ibm.sklm26.linux' value='KLMProfile'/>
  <data key='user.WAS_ADMIN_ID,com.ibm.sklm26.linux' value='wasadmin'/>
  <data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm26.linux' value='zN39fpCc9SqIryGJM7+02A=='/>
  <data key='user.WAS_ADMIN_CONF_PWD,com.ibm.sklm26.linux' value='zN39fpCc9SqIryGJM7+02A=='/>
  <data key='user.SKLM_ADMIN_USER,com.ibm.sklm26.linux' value='SKLMAdmin'/>
  <data key='user.SKLM_ADMIN_PASSWORD,com.ibm.sklm26.linux' value='94FrH/Ll220hVIYc9TflNQ=='/>
  <data key='user.SKLM_ADMIN_CONF_PWD,com.ibm.sklm26.linux' value='94FrH/Ll220hVIYc9TflNQ=='/>
  <data key='user.SKLM_APP_PORT,com.ibm.sklm26.linux' value='9080'/>

  <data key='cic.selector.nl' value='en'/>
 </profile>
 <preference name='com.ibm.cic.common.core.preferences.eclipseCache'
value='/opt/IBM/IBMIMShared'/>
 <preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30'/>
 <preference name='com.ibm.cic.common.core.preferences.readTimeout' value='45'/>
 <preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0'/>
 <preference name='offering.service.repositories.areUsed' value='true'/>
 <preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false'/>
 <preference name='com.ibm.cic.common.core.preferences.http.
disablePreemptiveAuthentication' value='false'/>
 <preference name='http.ntlm.auth.kind' value='NTLM'/>
 <preference name='http.ntlm.auth.enableIntegrated.win32' value='true'/>
 <preference name='com.ibm.cic.common.core.preferences.
preserveDownloadedArtifacts' value='true'/>
 <preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false'/>
 <preference name='PassportAdvantageIsEnabled' value='false'/>
 <preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false'/>
 <preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false'/>
 <preference name='com.ibm.cic.common.sharedUI.showErrorLog' value='true'/>
 <preference name='com.ibm.cic.common.sharedUI.showWarningLog' value='true'/>
 <preference name='com.ibm.cic.common.sharedUI.showNoteLog' value='true'/>
 </agent-input>
```

在 AIX 系统上新安装 V2.6

此示例响应文件包含响应信息，用于在 AIX 系统上安装 IBM Security Key Lifecycle Manager V2.6，或者进行要迁移 Encryption Key Manager 的安装。

```
(?xml version="1.0" encoding="UTF-8"?)
(!--The "acceptLicense" attribute has been deprecated. Use "-acceptLicense"
command line option to accept license agreements.--)
(agent-input acceptLicense='true')
(server)
 (repository location='/disk1/im'/)
 (repository location='/disk1/'/)
(/server)
(profile id='IBM Installation Manager' installLocation='/opt/IBM/
InstallationManager/eclipse' kind='self')
 (data key='eclipseLocation' value='/opt/IBM/InstallationManager/eclipse'/)
 (data key='user.import.profile' value='false'/)
 (data key='cic.selector.os' value='aix'/)
 (data key='cic.selector.arch' value='ppc'/)
 (data key='cic.selector.ws' value='motif'/)
(/profile)
(install modify='false')
(offering id='com.ibm.cic.agent'  profile='IBM Installation Manager'
features='agent_core,agent_jre' installFixes='none'/)
(offering id='com.ibm.db2.aix.ofng'  profile='IBM DB2' features='main.feature'
installFixes='none'/)
(offering id='com.ibm.websphere.BASE.v85'  profile='IBM WebSphere Application
Server V8.5' features='core.feature,ejbdeploy,thinclient,embeddablecontainer,
com.ibm.sdk.6_32bit' installFixes='none'/)
(offering profile='IBM WebSphere Application Server V8.5' id=
'com.ibm.websphere.IBMJAVA.v70' features='com.ibm.sdk.7' installFixes='none'/)
(offering id='com.ibm.sklm26.aix'  profile='IBM Security Key Lifecycle Manager
v2.6' features='main.feature' installFixes='none'/)
(/install)
(profile id='IBM DB2' installLocation='/opt/IBM/DB2SKLMV26')
(data key='eclipseLocation' value='/opt/IBM/DB2SKLMV26'/)
(data key='user.import.profile' value='false'/)
(data key='cic.selector.os' value='aix'/)
```

```
(data key='cic.selector.arch' value='ppc'/)
(data key='cic.selector.ws' value='motif'/)
(data key='user.DB2_ADMIN_ID,com.ibm.db2.aix.ofng' value='sklmdb26'/)
(data key='user.DB2_ADMIN_GRP,com.ibm.db2.aix.ofng' value='bin'/)
(data key='user.DB2_ADMIN_PWD,com.ibm.db2.aix.ofng' value='SwIhGBTDHcJok80Ux4Sb3g=='/)
(data key='user.CONFIRM_PASSWORD,com.ibm.db2.aix.ofng' value='SwIhGBTDHcJok80Ux4Sb3g=='/)
(data key='user.DB2_DB_HOME,com.ibm.db2.aix.ofng' value='/home/sklmdb26'/)
(data key='user.DB2_DB_NAME,com.ibm.db2.aix.ofng' value='SKLMDB26'/)
(data key='user.DB2_DB_PORT,com.ibm.db2.aix.ofng' value='50020'/)
(data key='user.DB2_EXISTS,com.ibm.db2.aix.ofng' value='false'/)
(data key='user.DB2_LOCATION,com.ibm.db2.aix.ofng' value='/opt/IBM/DB2SKLMV26'/)
(data key='cic.selector.nl' value='en'/)
(/profile)
(profile id='IBM WebSphere Application Server V8.5' installLocation=
'/opt/IBM/WebSphere/AppServer')
(data key='eclipseLocation' value='/opt/IBM/WebSphere/AppServer'/)
(data key='user.import.profile' value='false'/)
(data key='cic.selector.os' value='aix'/)
(data key='cic.selector.arch' value='ppc'/)
(data key='cic.selector.ws' value='motif'/)
(data key='cic.selector.nl' value='en'/)
(/profile)
(profile id='IBM Security Key Lifecycle Manager v2.6' installLocation='/opt/IBM/SKLMV26')
(data key='eclipseLocation' value='/opt/IBM/SKLMV26'/)
(data key='user.import.profile' value='false'/)
(data key='cic.selector.os' value='aix'/)
(data key='cic.selector.arch' value='ppc'/)
(data key='cic.selector.ws' value='motif'/)
(data key='user.IS_SILENT_MODE,com.ibm.sklm26.linux' value='false'/)
(data key='user.EKM_PROPFILE,com.ibm.sklm26.aix' value='/opt/IBM/
KeyManagerConfig.properties'/)
(data key='user.EKM_MIGRATION,com.ibm.sklm26.aix' value='false'/)
(data key='user.PROFILE_NAME,com.ibm.sklm26.aix' value='KLMProfile'/)
(data key='user.WAS_ADMIN_ID,com.ibm.sklm26.aix' value='wasadmin'/)
(data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm26.aix' value=
'zN39fpCc9SqIryGJM7+02A=='/)
(data key='user.WAS_ADMIN_CONF_PWD,com.ibm.sklm26.aix' value=
'zN39fpCc9SqIryGJM7+02A=='/)
(data key='user.SKLM_ADMIN_USER,com.ibm.sklm26.aix' value='SKLMAdmin'/)
(data key='user.SKLM_ADMIN_PASSWORD,com.ibm.sklm26.aix' value=
'94FrH/Ll220hVIYc9TflNQ=='/)
(data key='user.SKLM_ADMIN_CONF_PWD,com.ibm.sklm26.aix' value=
'94FrH/Ll220hVIYc9TflNQ=='/)
(data key='user.SKLM_APP_PORT,com.ibm.sklm26.aix' value='9080'/)
 (data key='cic.selector.nl' value='en'/)
(/profile)
(preference name='com.ibm.cic.common.core.preferences.eclipseCache'
value='/opt/IBM/IBMIMShared'/)
(preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30'/)
(preference name='com.ibm.cic.common.core.preferences.readTimeout' value='45'/)
(preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0'/)
(preference name='offering.service.repositories.areUsed' value='true'/)
(preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false'/)
(preference name='com.ibm.cic.common.core.preferences.http.
disablePreemptiveAuthentication' value='false'/)
(preference name='http.ntlm.auth.kind' value='NTLM'/)
(preference name='http.ntlm.auth.enableIntegrated.win32' value='true'/)
(preference name='com.ibm.cic.common.core.preferences.
preserveDownloadedArtifacts' value='true'/)
(preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false'/)
(preference name='PassportAdvantageIsEnabled' value='false'/)
(preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false'/)
(preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false'/)
(preference name='com.ibm.cic.common.sharedUI.showErrorLog' value='true'/)
(preference name='com.ibm.cic.common.sharedUI.showWarningLog' value='true'/)
(preference name='com.ibm.cic.common.sharedUI.showNoteLog' value='true'/)
(/agent-input)
```

在 Windows 系统上从先前版本迁移到 V2.6

此示例响应文件包含响应信息，用于在 Windows 系统上进行要将 IBM Security Key Lifecycle Manager 从先前版本迁移到 V2.6 的安装。

注: 要确定 IBM Security Key Lifecycle Manager 较早版本是否存在并且是否需要迁移，请使用 **tklmVersionInfo** 命令。例如，在 Jython 会话中输入以下命令:

```
print AdminTask.tklmVersionInfo<>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<!--The "acceptLicense" attribute has been deprecated. Use "-acceptLicense"
command line option to accept license agreements.-->
<agent-input acceptLicense='true'>
<server>
<repository location='C:\disk1\im'/>
<repository location='C:\disk1\'/>
</server>
<profile id='IBM Installation Manager' installLocation=
'C:\Program Files <x86>\IBM\Installation Manager\eclipse' kind='self'>
<data key='eclipseLocation' value='C:\Program Files <x86>\IBM\Installation Manager\eclipse'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='win32'/>
<data key='cic.selector.arch' value='x86_64'/>
<data key='cic.selector.ws' value='win32'/>
</profile>
<install modify='false'>
<offering profile='IBM Installation Manager' id='com.ibm.cic.agent' features=
'agent_core,agent_jre,agent_web' installFixes='none'/>
<offering profile='IBM DB2' id='com.ibm.db2.ofng' features='com.ibm.db2.ofng'
installFixes='none'/>
<offering profile='IBM WebSphere Application Server V8.5' id=
'com.ibm.websphere.BASE.v85' features='core.feature,ejbdeploy,thinclient,
embeddablecontainer,com.ibm.sdk.6_32bit' installFixes='none'/>
<offering profile='IBM WebSphere Application Server V8.5' id=
'com.ibm.websphere.IBMJAVA.v70' features='com.ibm.sdk.7' installFixes='none'/>
<offering profile='IBM Security Key Lifecycle Manager v2.6' id=
'com.ibm.sklm26.win32' features='main.feature' installFixes='none'/>
</install>
<profile id='IBM DB2' installLocation='C:\Program Files <x86>\IBM\DB2SKLMV26'>
<data key='eclipseLocation' value='C:\Program Files <x86>\IBM\DB2SKLMV26'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='win32'/>
<data key='cic.selector.arch' value='x86'/>
<data key='cic.selector.ws' value='win32'/>
<data key='user.DB2_ADMIN_ID,com.ibm.db2.ofng' value='sklmdb26'/>
<data key='user.DB2_ADMIN_PWD,com.ibm.db2.ofng' value='SwIhGBTDHcJok80Ux4Sb3g=='/>
<data key='user.CONFIRM_PASSWORD,com.ibm.db2.ofng' value='SwIhGBTDHcJok80Ux4Sb3g='/>
<data key='user.DB2_DB_HOME,com.ibm.db2.ofng' value='C:'/>
<data key='user.DB2_DB_NAME,com.ibm.db2.ofng' value='SKLMDB26'/>
<data key='user.DB2_DB_PORT,com.ibm.db2.ofng' value='50020'/>
<data key='user.DB2_EXISTS,com.ibm.db2.ofng' value='false'/>
<data key='user.DB2_LOCATION,com.ibm.db2.ofng' value='C:\\Program Files <x86>\\
IBM\\DB2SKLMV26'/>
<data key='cic.selector.nl' value='en'/>
</profile>
<profile id='IBM WebSphere Application Server V8.5' installLocation=
'C:\Program Files <x86>\IBM\WebSphere\AppServer'>
<data key='eclipseLocation' value='C:\Program Files <x86>\IBM\WebSphere\AppServer'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='win32'/>
<data key='cic.selector.arch' value='x86'/>
<data key='cic.selector.ws' value='win32'/>
<data key='cic.selector.nl' value='en'/>
</profile>
<profile id='IBM Security Key Lifecycle Manager v2.6' installLocation=
'C:\Program Files <x86>\IBM\SKLMV26'>
<data key='eclipseLocation' value='C:\Program Files <x86>\IBM\SKLMV26'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='win32'/>
<data key='cic.selector.arch' value='x86'/>
<data key='cic.selector.ws' value='win32'/>
<data key='user.EKM_PROPFILE,com.ibm.sklm26.win32' value=
'C:\KeyManagerConfig.properties'/>
<data key='user.EKM_MIGRATION,com.ibm.sklm26.win32' value='false'/>
<data key='user.PROFILE_NAME,com.ibm.sklm26.win32' value='KLMProfile'/>
<data key='user.WAS_ADMIN_ID,com.ibm.sklm26.win32' value='tipadmin'/>
<data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm26.win32' value='L7vybdrE8dgbdNodwJIkQQ=='/>
<data key='user.WAS_ADMIN_CONF_PWD,com.ibm.sklm26.win32' value='L7vybdrE8dgbdNodwJIkQQ=='/>
<data key='user.SKLM_ADMIN_USER,com.ibm.sklm26.win32' value='TKLMAdmin'/>
<data key='user.SKLM_ADMIN_PASSWORD,com.ibm.sklm26.win32' value='now6wpN1MFAVFGfIB1r9+Q=='/>
<data key='user.SKLM_ADMIN_CONF_PWD,com.ibm.sklm26.win32' value='now6wpN1MFAVFGfIB1r9+Q=='/>
<data key='user.SKLM_APP_PORT,com.ibm.sklm26.win32' value='9080'/>
<data key='user.TKLM_VERSION,com.ibm.sklm26.win32' value='2.0.1'/>
<data key='user.TKLM_TIP_HOME,com.ibm.sklm26.win32' value='C:\IBM\tivoli\tiptklmV2'/>
<data key='user.TKLM_INSTALLED,com.ibm.sklm26.win32' value='true'/>
<data key='user.TKLM_DB_PWD,com.ibm.sklm26.win32' value='/6vJK3fcU3QxHY+RVfCFVw=='/>
<data key='user.TKLM_KEYSTORE_PWD,com.ibm.sklm26.win32' value='fufgZbY47EfxLYarBAIxeQ=='/>
```

```
<data key='cic.selector.nl' value='en'/>
</profile>
<preference name='com.ibm.cic.common.core.preferences.eclipseCache'
value='C:\Program Files <x86>\IBM\IBMIMShared'/>
<preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30'/>
<preference name='com.ibm.cic.common.core.preferences.readTimeout' value='45'/>
<preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount'
value='0'/>
<preference name='offering.service.repositories.areUsed' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.http.
disablePreemptiveAuthentication' value='false'/>
<preference name='http.ntlm.auth.kind' value='NTLM'/>
<preference name='http.ntlm.auth.enableIntegrated.win32' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false'/>
<preference name='PassportAdvantageIsEnabled' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false'/>
<preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false'/>
<preference name='com.ibm.cic.common.sharedUI.showErrorLog' value='true'/>
<preference name='com.ibm.cic.common.sharedUI.showWarningLog' value='true'/>
<preference name='com.ibm.cic.common.sharedUI.showNoteLog' value='true'/>
</agent-input>
```

在 Linux 系统上从先前版本迁移到 V2.6

此示例响应文件包含响应信息，用于在 Linux 系统上进行要将 IBM Security Key Lifecycle Manager 从先前版本迁移到 V2.6 的安装。

注: 要确定 IBM Security Key Lifecycle Manager 较早版本是否存在并且是否需要迁移，请使用 **tklmVersionInfo** 命令。例如，在 Jython 会话中输入以下命令:

```
print AdminTask.tklmVersionInfo<>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<!--The "acceptLicense" attribute has been deprecated. Use "-acceptLicense"
command line option to accept license agreements.-->
<agent-input acceptLicense='true'>
<server>

<repository location='/disk1/im'/>
<repository location='/disk1/'/>
</server>
<profile id='IBM DB2' installLocation='/opt/IBM/DB2SKLMV26'>
<data key='eclipseLocation' value='/opt/IBM/DB2SKLMV26'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='linux'/>
<data key='cic.selector.arch' value='x86_64'/>
<data key='cic.selector.ws' value='gtk'/>
<data key='user.DB2_ADMIN_ID,com.ibm.db2.linux.ofng' value='sklmdb26'/>
<data key='user.DB2_ADMIN_GRP,com.ibm.db2.linux.ofng' value='root'/>
<data key='user.DB2_ADMIN_PWD,com.ibm.db2.linux.ofng' value='SwIhGBTDHcJok80Ux4Sb3g=='/>
<data key='user.CONFIRM_PASSWORD,com.ibm.db2.linux.ofng' value='SwIhGBTDHcJok80Ux4Sb3g=='/>
<data key='user.DB2_DB_LHOME,com.ibm.db2.linux.ofng' value='/home/sklmdb26'/>
<data key='user.DB2_DB_NAME,com.ibm.db2.linux.ofng' value='SKLMDB26'/>
<data key='user.DB2_DB_PORT,com.ibm.db2.linux.ofng' value='50020'/>
<data key='user.DB2_EXISTS,com.ibm.db2.linux.ofng' value='false'/>
<data key='user.DB2_LOCATION,com.ibm.db2.linux.ofng' value='/opt/IBM/DB2SKLMV26'/>
<data key='cic.selector.nl' value='en'/>
</profile>
<install modify='false'>
<offering profile='IBM Installation Manager'  id='com.ibm.cic.agent'
features='agent_core,agent_jre,agent_web' installFixes='none'/>
<offering profile='IBM DB2' features='com.ibm.com.ibm.db2.linux'
id='com.ibm.db2.linux.ofng' installFixes='none'/>
<offering profile='IBM WebSphere Application Server V8.5'
id='com.ibm.websphere.BASE.v85' features='core.feature,ejbdeploy,thinclient,
embeddablecontainer,com.ibm.sdk.6_32bit' installFixes='none'/>
<offering profile='IBM WebSphere Application Server V8.5'
id='com.ibm.websphere.IBMJAVA.v70' features='com.ibm.sdk.7' installFixes='none'/>
<offering profile='IBM Security Key Lifecycle Manager v2.6'
id='com.ibm.sklm26.linux' features='main.feature' installFixes='none'/>
</install>
<profile id='IBM Installation Manager' installLocation=
'/opt/IBM/InstallationManager/eclipse' kind='self'>
<data key='eclipseLocation' value='/opt/IBM/InstallationManager/eclipse'/>
```

```
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='linux'/>
<data key='cic.selector.arch' value='x86_64'/>
<data key='cic.selector.ws' value='gtk'/>
</profile>
<profile id='IBM WebSphere Application Server V8.5' installLocation=
'/opt/IBM/WebSphere/AppServer'>
<data key='eclipseLocation' value='/opt/IBM/WebSphere/AppServer'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='linux'/>
<data key='cic.selector.arch' value='x86'/>
<data key='cic.selector.ws' value='gtk'/>
<data key='cic.selector.nl' value='en'/>
</profile>
<profile id='IBM Security Key Lifecycle Manager v2.6' installLocation='/opt/IBM/SKLMV26'>
<data key='eclipseLocation' value='/opt/IBM/SKLMV26'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='linux'/>
<data key='cic.selector.arch' value='x86'/>
<data key='cic.selector.ws' value='gtk'/>
<data key='user.EKM_PROPFILE,com.ibm.sklm26.linux' value='/opt/IBM/
KeyManagerConfig.properties'/>
<data key='user.EKM_MIGRATION,com.ibm.sklm26.linux' value='false'/>
<data key='user.PROFILE_NAME,com.ibm.sklm26.linux' value='KLMProfile'/>
<data key='user.WAS_ADMIN_ID,com.ibm.sklm26.linux' value='tipadmin'/>
<data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm26.linux' value='L7vybdrE8dgbdNodwJIkQQ=='/>
<data key='user.WAS_ADMIN_CONF_PWD,com.ibm.sklm26.linux' value='L7vybdrE8dgbdNodwJIkQQ=='/>
<data key='user.SKLM_ADMIN_USER,com.ibm.sklm26.linux' value='TKLMAdmin'/>
<data key='user.SKLM_ADMIN_PASSWORD,com.ibm.sklm26.linux' value='now6wpN1MFAVFGfIB1r9+Q=='/>
<data key='user.SKLM_ADMIN_CONF_PWD,com.ibm.sklm26.linux' value='now6wpN1MFAVFGfIB1r9+Q=='/>
<data key='user.SKLM_APP_PORT,com.ibm.sklm26.linux' value='9080'/>
<data key='user.TKLM_VERSION,com.ibm.sklm26.linux' value='2.0.1'/>
<data key='user.TKLM_TIP_HOME,com.ibm.sklm26.linux' value='/opt/IBM/tivoli/tiptklmV2/'/>
<data key='user.TKLM_INSTALLED,com.ibm.sklm26.linux' value='true'/>
<data key='user.TKLM_DB_PWD,com.ibm.sklm26.linux' value='/6vJK3fcU3QxHY+RVfCFVw=='/>
<data key='user.TKLM_KEYSTORE_PWD,com.ibm.sklm26.linux' value='fufgZbY47EfxLYarBAIxeQ=='/>
<data key='cic.selector.nl' value='en'/>
</profile>
<preference name='com.ibm.cic.common.core.preferences.eclipseCache'
value='/opt/IBM/IBMIMShared'/>
<preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30'/>
<preference name='com.ibm.cic.common.core.preferences.readTimeout' value='45'/>
<preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0'/>
<preference name='offering.service.repositories.areUsed' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.http.
disablePreemptiveAuthentication' value='false'/>
<preference name='http.ntlm.auth.kind' value='NTLM'/>
<preference name='http.ntlm.auth.enableIntegrated.win32' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.
preserveDownloadedArtifacts' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false'/>
<preference name='PassportAdvantageIsEnabled' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false'/>
<preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false'/>
<preference name='com.ibm.cic.common.sharedUI.showErrorLog' value='true'/>
<preference name='com.ibm.cic.common.sharedUI.showWarningLog' value='true'/>
<preference name='com.ibm.cic.common.sharedUI.showNoteLog' value='true'/>
</agent-input>
```

在 Linux for System z 上将先前版本迁移到 V2.6

此示例响应文件包含响应信息，用于在 Linux for System z 上进行要将 IBM Security Key Lifecycle Manager 从先前版本迁移到 V2.6 的安装。

注: 要确定 IBM Security Key Lifecycle Manager 较早版本是否存在并且是否需要迁移，请使用 **tklmVersionInfo** 命令。例如，在 Jython 会话中输入以下命令:

```
print AdminTask.tklmVersionInfo<>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<!--The "acceptLicense" attribute has been deprecated. Use "-acceptLicense"
command line option to accept license agreements.-->
<agent-input acceptLicense='true'>
<server>
```

```
<repository location='/disk1/im'/>
<repository location='/disk1/'/>

</server>
<profile id='IBM DB2' installLocation='/opt/IBM/DB2SKLMV26'>
<data key='eclipseLocation' value='/opt/IBM/DB2SKLMV26'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='linux'/>
<data key='cic.selector.arch' value='s390'/>
<data key='cic.selector.ws' value='gtk'/>
<data key='user.DB2_ADMIN_ID,com.ibm.db2.linux.ofng' value='sklmdb26'/>
<data key='user.DB2_ADMIN_GRP,com.ibm.db2.linux.ofng' value='root'/>
<data key='user.DB2_ADMIN_PWD,com.ibm.db2.linux.ofng' value='SwIhGBTDHcJok80Ux4Sb3g=='/>
<data key='user.CONFIRM_PASSWORD,com.ibm.db2.linux.ofng' value='SwIhGBTDHcJok80Ux4Sb3g=='/>
<data key='user.DB2_DB_LHOME,com.ibm.db2.linux.ofng' value='/home/sklmdb26'/>
<data key='user.DB2_DB_NAME,com.ibm.db2.linux.ofng' value='SKLMDB26'/>
<data key='user.DB2_DB_PORT,com.ibm.db2.linux.ofng' value='50020'/>
<data key='user.DB2_EXISTS,com.ibm.db2.linux.ofng' value='false'/>
<data key='user.DB2_LOCATION,com.ibm.db2.linux.ofng' value='/opt/IBM/DB2SKLMV26'/>
<data key='cic.selector.nl' value='en'/>
</profile>
<install modify='false'>
<offering profile='IBM Installation Manager' id='com.ibm.cic.agent'
features='agent_core,agent_jre' installFixes='none'/>
<offering profile='IBM DB2' id='com.ibm.db2.linux.ofng'
features='com.ibm.com.ibm.db2.linux' installFixes='none'/>
<offering profile='IBM WebSphere Application Server V8.5'
id='com.ibm.websphere.BASE.v85' features='core.feature,ejbdeploy,thinclient,
embeddablecontainer,com.ibm.sdk.6_32bit' installFixes='none'/>
<offering profile='IBM WebSphere Application Server V8.5'
id='com.ibm.websphere.IBMJAVA.v70' features='com.ibm.sdk.7' installFixes='none'/>
<offering id='com.ibm.sklm26.linux'  profile='IBM Security Key Lifecycle Manager v2.6'
features='main.feature' installFixes='none'/>
</install>
<profile id='IBM Installation Manager' installLocation=
'/opt/IBM/InstallationManager/eclipse' kind='self'>
<data key='eclipseLocation' value='/opt/IBM/InstallationManager/eclipse'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='linux'/>
<data key='cic.selector.arch' value='s390'/>
<data key='cic.selector.ws' value='gtk'/>
</profile>
<profile id='IBM WebSphere Application Server V8.5' installLocation=
'/opt/IBM/WebSphere/AppServer'>
<data key='eclipseLocation' value='/opt/IBM/WebSphere/AppServer'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='linux'/>
<data key='cic.selector.arch' value='s390'/>
<data key='cic.selector.ws' value='gtk'/>
<data key='cic.selector.nl' value='en'/>
</profile>
<profile id='IBM Security Key Lifecycle Manager v2.6' installLocation=
'/opt/IBM/SKLMV26'>
<data key='eclipseLocation' value='/opt/IBM/SKLMV26'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='linux'/>
<data key='cic.selector.arch' value='s390'/>
<data key='cic.selector.ws' value='gtk'/>
<data key='user.EKM_PROPFILE,com.ibm.sklm26.linux' value=
'/opt/IBM/KeyManagerConfig.properties'/>
<data key='user.EKM_MIGRATION,com.ibm.sklm26.linux' value='false'/>
<data key='user.PROFILE_NAME,com.ibm.sklm26.linux' value='KLMProfile'/>
<data key='user.WAS_ADMIN_ID,com.ibm.sklm26.linux' value='tipadmin'/>
<data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm26.linux' value='L7vybdrE8dgbdNodwJIkQQ=='/>
<data key='user.WAS_ADMIN_CONF_PWD,com.ibm.sklm26.linux' value='L7vybdrE8dgbdNodwJIkQQ=='/>
<data key='user.SKLM_ADMIN_USER,com.ibm.sklm26.linux' value='TKLMAdmin'/>
<data key='user.SKLM_ADMIN_PASSWORD,com.ibm.sklm26.linux' value='now6wpN1MFAVFGfIB1r9+Q=='/>
<data key='user.SKLM_ADMIN_CONF_PWD,com.ibm.sklm26.linux' value='now6wpN1MFAVFGfIB1r9+Q=='/>
<data key='user.SKLM_APP_PORT,com.ibm.sklm26.linux' value='9080'/>
<data key='user.TKLM_VERSION,com.ibm.sklm26.linux' value='2.0.1'/>
<data key='user.TKLM_TIP_HOME,com.ibm.sklm26.linux' value='/opt/IBM/tivoli/tiptklmV2/'/>
<data key='user.TKLM_INSTALLED,com.ibm.sklm26.linux' value='true'/>
<data key='user.TKLM_DB_PWD,com.ibm.sklm26.linux' value='/6vJK3fcU3QxHY+RVfCFVw=='/>
<data key='user.TKLM_KEYSTORE_PWD,com.ibm.sklm26.linux' value='fufgZbY47EfxLYarBAIxeQ=='/>
<data key='cic.selector.nl' value='en'/>
</profile>
<preference name='com.ibm.cic.common.core.preferences.eclipseCache'
value='/opt/IBM/IBMIMShared'/>
<preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30'/>
<preference name='com.ibm.cic.common.core.preferences.readTimeout' value='45'/>
```

```
<preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0'/>
<preference name='offering.service.repositories.areUsed' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.http.
disablePreemptiveAuthentication' value='false'/>
<preference name='http.ntlm.auth.kind' value='NTLM'/>
<preference name='http.ntlm.auth.enableIntegrated.win32' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.
preserveDownloadedArtifacts' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false'/>
<preference name='PassportAdvantageIsEnabled' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false'/>
<preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false'/>
<preference name='com.ibm.cic.common.sharedUI.showErrorLog' value='true'/>
<preference name='com.ibm.cic.common.sharedUI.showWarningLog' value='true'/>
<preference name='com.ibm.cic.common.sharedUI.showNoteLog' value='true'/>
</agent-input>
```

在 AIX 系统上从先前版本迁移到 V2.6

此示例响应文件包含响应信息，用于在 AIX 系统上进行要将 IBM Security Key Lifecycle Manager 从先前版本迁移到 V2.6 的安装。

注: 要确定 IBM Security Key Lifecycle Manager 较早版本是否存在并且是否需要迁移，请使用 **tklmVersionInfo** 命令。例如，在 Jython 会话中输入以下命令:

```
print AdminTask.tklmVersionInfo<>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<!--The "acceptLicense" attribute has been deprecated. Use "-acceptLicense"
command line option to accept license agreements.-->
<agent-input acceptLicense='true'>
<server>

<repository location='/disk1/im'/>
<repository location='/disk1/'/>

</server>
<profile id='IBM DB2' installLocation='/opt/IBM/DB2SKLMV26'>
<data key='eclipseLocation' value='/opt/IBM/DB2SKLMV26'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='aix'/>
<data key='cic.selector.arch' value='ppc'/>
<data key='cic.selector.ws' value='motif'/>
<data key='user.DB2_ADMIN_ID,com.ibm.db2.aix.ofng' value='sklmdb26'/>
<data key='user.DB2_ADMIN_GRP,com.ibm.db2.aix.ofng' value='bin'/>
<data key='user.DB2_ADMIN_PWD,com.ibm.db2.aix.ofng' value='SwIhGBTDHcJok80Ux4Sb3g=='/>
<data key='user.CONFIRM_PASSWORD,com.ibm.db2.aix.ofng' value='SwIhGBTDHcJok80Ux4Sb3g=='/>
<data key='user.DB2_DB_HOME,com.ibm.db2.aix.ofng' value='/home/sklmdb26'/>
<data key='user.DB2_DB_NAME,com.ibm.db2.aix.ofng' value='SKLMDB26'/>
<data key='user.DB2_DB_PORT,com.ibm.db2.aix.ofng' value='50020'/>
<data key='user.DB2_EXISTS,com.ibm.db2.aix.ofng' value='false'/>
<data key='user.DB2_LOCATION,com.ibm.db2.aix.ofng' value='/opt/IBM/DB2SKLMV26'/>
<data key='cic.selector.nl' value='en'/>
</profile>
<install modify='false'>
<offering profile='IBM Installation Manager' id='com.ibm.cic.agent'
features='agent_core,agent_jre' installFixes='none'/>
<offering profile='IBM DB2' id='com.ibm.db2.aix.ofng'
features='main.feature' installFixes='none'/>
<offering profile='IBM WebSphere Application Server V8.5'
id='com.ibm.websphere.BASE.v85' features='core.feature,ejbdeploy,thinclient,
embeddablecontainer,com.ibm.sdk.6_32bit' installFixes='none'/>
<offering profile='IBM WebSphere Application Server V8.5'
id='com.ibm.websphere.IBMJAVA.v70' features='com.ibm.sdk.7' installFixes='none'/>
<offering profile='IBM Security Key Lifecycle Manager v2.6'
id='com.ibm.sklm26.aix' features='main.feature' installFixes='none'/>
</install>
<profile id='IBM Installation Manager' installLocation=
'/opt/IBM/InstallationManager/eclipse' kind='self'>
<data key='eclipseLocation' value='/opt/IBM/InstallationManager/eclipse'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='aix'/>
<data key='cic.selector.arch' value='ppc'/>
<data key='cic.selector.ws' value='motif'/>
</profile>
```

```
<profile id='IBM WebSphere Application Server V8.5' installLocation=
'/opt/IBM/WebSphere/AppServer'>
<data key='eclipseLocation' value='/opt/IBM/WebSphere/AppServer'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='aix'/>
<data key='cic.selector.arch' value='ppc'/>
<data key='cic.selector.ws' value='motif'/>
<data key='cic.selector.nl' value='en'/>
</profile>
<profile id='IBM Security Key Lifecycle Manager v2.6' installLocation=
'/opt/IBM/SKLMV26'>
<data key='eclipseLocation' value='/opt/IBM/SKLMV26'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='aix'/>
<data key='cic.selector.arch' value='ppc'/>
<data key='cic.selector.ws' value='motif'/>
<data key='user.EKM_PROPFILE,com.ibm.sklm26.aix'
value='/opt/IBM/KeyManagerConfig.properties'/>
<data key='user.EKM_MIGRATION,com.ibm.sklm26.aix' value='false'/>
<data key='user.PROFILE_NAME,com.ibm.sklm26.aix' value='KLMProfile'/>
<data key='user.WAS_ADMIN_ID,com.ibm.sklm26.aix' value='tipadmin'/>
<data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm26.aix' value='L7vybdrE8dgbdNodwJIkQQ=='/>
<data key='user.WAS_ADMIN_CONF_PWD,com.ibm.sklm26.aix' value='L7vybdrE8dgbdNodwJIkQQ=='/>
<data key='user.SKLM_ADMIN_USER,com.ibm.sklm26.aix' value='TKLMAdmin'/>
<data key='user.SKLM_ADMIN_PASSWORD,com.ibm.sklm26.aix' value='now6wpN1MFAVFGfIB1r9+Q=='/>
<data key='user.SKLM_ADMIN_CONF_PWD,com.ibm.sklm26.aix' value='now6wpN1MFAVFGfIB1r9+Q=='/>
<data key='user.SKLM_APP_PORT,com.ibm.sklm26.aix' value='9080'/>
<data key='user.TKLM_VERSION,com.ibm.sklm26.aix' value='2.0.1'/>
<data key='user.TKLM_TIP_HOME,com.ibm.sklm26.aix' value='/opt/IBM/tivoli/tiptklmV2/'/>
<data key='user.TKLM_INSTALLED,com.ibm.sklm26.aix' value='true'/>
<data key='user.TKLM_DB_PWD,com.ibm.sklm26.aix' value='/6vJK3fcU3QxHY+RVfCFVw=='/>
<data key='user.TKLM_KEYSTORE_PWD,com.ibm.sklm26.aix' value='fufgZbY47EfxLYarBAIxeQ=='/>
<data key='cic.selector.nl' value='en'/>
</profile>
<preference name='com.ibm.cic.common.core.preferences.eclipseCache'
value='/opt/IBM/IBMIMShared'/>
<preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30'/>
<preference name='com.ibm.cic.common.core.preferences.readTimeout' value='45'/>
<preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0'/>
<preference name='offering.service.repositories.areUsed' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.http.disablePreemptiveAuthentication'
value='false'/>
<preference name='http.ntlm.auth.kind' value='NTLM'/>
<preference name='http.ntlm.auth.enableIntegrated.win32' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false'/>
<preference name='PassportAdvantageIsEnabled' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false'/>
<preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false'/>
<preference name='com.ibm.cic.common.sharedUI.showErrorLog' value='true'/>
<preference name='com.ibm.cic.common.sharedUI.showWarningLog' value='true'/>
<preference name='com.ibm.cic.common.sharedUI.showNoteLog' value='true'/>
</agent-input>
```

Windows 系统上的卸载

此示例响应文件包含响应信息，用于在 Windows 系统上执行卸载。

```
<?xml version="1.0" encoding="UTF-8"?>
<agent-input>
<profile id='IBM Security Key Lifecycle Manager v2.6'>
<data key='user.WAS_ADMIN_ID,com.ibm.sklm26.win32' value='wasadmin'/>
<data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm26.win32'
value='zN39fpCc9SqIryGJM7+02A=='/>
</profile>
<uninstall modify='false'>
<offering id='com.ibm.sklm26.win32'  profile='IBM Security Key Lifecycle Manager
v2.6' features='main.feature'/>
<offering id='com.ibm.websphere.BASE.v85'  profile='IBM WebSphere Application
Server V8.5' features='core.feature,ejbdeploy,thinclient,embeddablecontainer,
samples,com.ibm.sdk.6_32bit,com.ibm.sdk.6_64bit'/>
<offering id='com.ibm.db2.ofng'  profile='IBM DB2' features='com.ibm.db2.ofng'/>
</uninstall>
</agent-input>
```

Linux 系统上的卸载

此示例响应文件包含响应信息，用于在 Linux 系统上进行卸载。

```
<?xml version="1.0" encoding="UTF-8"?>
<agent-input>
<profile id='IBM Security Key Lifecycle Manager v2.6'>
<data key='user.WAS_ADMIN_ID,com.ibm.sklm26.linux' value='wasadmin'/>
<data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm26.linux'
value='zN39fpCc9SqIryGJM7+02A=='/>
</profile>
<uninstall modify='false'>
<offering id='com.ibm.sklm26.linux'  profile='IBM Security Key Lifecycle
Manager v2.6' features='main.feature'/>
<offering id='com.ibm.websphere.BASE.v85'  profile='IBM WebSphere Application
Server V8.5' features='core.feature,ejbdeploy,thinclient,embeddablecontainer,
samples,com.ibm.sdk.6_32bit,com.ibm.sdk.6_64bit'/>
<offering id='com.ibm.db2.linux.ofng'  profile='IBM DB2' features=
'com.ibm.com.ibm.db2.linux'/>
</uninstall>
</agent-input>
```

Linux for System z 上的卸载

此示例响应文件包含响应信息，用于在 Linux for System z 上进行卸载。

```
<?xml version="1.0" encoding="UTF-8"?>
<agent-input>
<profile id='IBM Security Key Lifecycle Manager v2.6'>
<data key='user.WAS_ADMIN_ID,com.ibm.sklm26.linux' value='wasadmin'/>
<data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm26.linux'
value='zN39fpCc9SqIryGJM7+02A=='/>
</profile>
<uninstall modify='false'>
<offering id='com.ibm.sklm26.linux'  profile='IBM Security Key Lifecycle
Manager v2.6' features='main.feature'/>
<offering id='com.ibm.websphere.BASE.v85'  profile='IBM WebSphere Application
Server V8.5' features='core.feature,ejbdeploy,thinclient,embeddablecontainer,
samples,com.ibm.sdk.6_32bit,com.ibm.sdk.6_64bit'/>
<offering id='com.ibm.db2.linux.ofng'  profile='IBM DB2' features=
'com.ibm.com.ibm.db2.linux'/>
</uninstall>
</agent-input>
```

AIX 系统上的卸载

此示例响应文件包含响应信息，用于在 AIX 系统上进行卸载。

```
<?xml version="1.0" encoding="UTF-8"?>
<agent-input>
<profile id='IBM Security Key Lifecycle Manager v2.6'>
<data key='user.WAS_ADMIN_ID,com.ibm.sklm26.aix' value='wasadmin'/>
<data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm26.aix'
value='zN39fpCc9SqIryGJM7+02A=='/>
</profile>
<uninstall modify='false'>
<offering id='com.ibm.sklm26.aix'  profile='IBM Security Key Lifecycle Manager
v2.6' features='main.feature'/>
<offering id='com.ibm.websphere.BASE.v85'  profile='IBM WebSphere Application
Server V8.5' features='core.feature,ejbdeploy,thinclient,embeddablecontainer,
samples,com.ibm.sdk.6_32bit,com.ibm.sdk.6_32bit'/>
<offering id='com.ibm.db2.aix.ofng'  profile='IBM DB2' features='main.feature'/>
</uninstall>
</agent-input>
```

安装错误消息

根据操作结果，IBM Security Key Lifecycle Manager 可能会提供参考、警告或错误消息。

消息格式

由 IBM Security Key Lifecycle Manager 遵循 Tivoli Message Standard 记录的消息。每个消息由消息标识及其伴随的消息文本组成。

消息具有以下语法:

CTG*UUXXXXZ*

其中:

CTG 识别 IBM Security Key Lifecycle Manager 产品。

UU 识别 IBM Security Key Lifecycle Manager 的组件或子系统。例如:

- **KM** IBM Security Key Lifecycle Manager 服务器 消息。
- **KO** 密码策略消息。
- **KS** IBM Security Key Lifecycle Manager 密钥服务器消息。

XXXX 指示序列号或消息号，比如 0001。

Z 一个字符类型的代码指示消息的严重性:

- I 表示参考消息
- W 表示警告消息
- E 表示错误消息
-

例如:

CTGKM0545E: 导出证书时发生错误。

错误和警告消息

IBM Security Key Lifecycle Manager 会根据您执行的操作生成错误和警告消息。

CTGKM9002E 管理员标识必须等于或小于 8 个字符。

说明: 用户标识的最大长度限制为 8 个字符。

系统操作: 更正错误之前无法继续安装。

用户响应: 请选择另一个等于或小于 8 个字符的用户标识。

CTGKM9003E 管理员标识必须以字母字符开头。

说明: 用户标识必需以字母开头。

另外，用户标识只能使用字母字符、数字字符以及下划线（A-Z、a-z、0–9 和 _）。

系统操作: 更正错误之前无法继续安装。

用户响应: 请选择另一个以字母开头的用户标识。

CTGKM9004E 管理员标识不能以 ibm、sql 或 sys 开头。

说明: 管理员用户标识不能以“ibm”、“sql”或“sys”开头。

系统操作: 更正错误之前无法继续安装。

用户响应: 请选择另一个不以某个限制字符串开头的用户标识。

CTGKM9005E 管理员标识不能是: db2、users、admins、guests、public、private、properties、local 或 root。

说明: 不能使用 DB2 的保留关键字作为管理员用户标识。

系统操作: 更正错误之前无法继续安装。

用户响应: 请选择另一个不是 DB2 关键字的用户标识。

CTGKM9006E 管理员标识是必填字段。

说明: 必需指定管理员用户标识。

系统操作: 在字段中输入值之前无法继续安装。

用户响应: 请在“管理员标识”字段中输入用户标识。

CTGKM9007E 密码是必填字段。

说明: 必须指定密码。

系统操作: 在字段中输入值之前无法继续安装。

用户响应: 请输入用户标识的密码。

CTGKM9010E 密码确认字段是必填字段。

说明: 必须指定密码。

系统操作: 在字段中输入值之前无法继续安装。

用户响应: 请输入用户标识的密码。

CTGKM9011E 数据库主目录是必填字段。

说明: 必须指定数据库主目录。

系统操作: 在字段中输入值之前无法继续安装。

用户响应: 请输入用于存储数据库文件的目录。

CTGKM9012E 数据库名称是必填字段。

说明: 必须指定数据库名称。

系统操作: 在字段中输入值之前无法继续安装。

用户响应: 请输入数据库的名称。

CTGKM9037E 端口必须是介于 1024 和 65536 之间的正整数。

说明: 端口号必须介于 1024 和 65536 之间。

系统操作: 更正错误之前无法继续安装。

用户响应: 请输入介于 1024 和 65536 之间的端口号。

CTGKM9038E 端口是必填字段。

说明: 必须指定端口。

系统操作: 在字段中输入值之前无法继续安装。

用户响应: 请输入端口号。

CTGKM9041E 密码和密码确认字段不匹配。请为这两个字段重新输入匹配的密码。

说明: 两个字段中的密码必须匹配。

系统操作: 更正错误之前无法继续安装。

用户响应: 请在字段中重新输入值。

CTGKM9042I 密码不能包含空格。

说明: 密码只能包含字母数字字符和下划线（a-z、A-Z、0–9 和 _）。

系统操作: 更正错误之前无法继续安装。

用户响应: 请输入另一个符合规则的密码。

CTGKM9044I “管理员标识”不能是 SQL 保留字。

说明: “管理员标识”不能是 SQL 保留字。

系统操作: 更正错误之前无法继续安装。

用户响应: 请为管理员标识输入另一个值。

CTGKM9049I Windows DB2“数据库主目录”字段必须为盘符名 [A-Z] 后跟一个冒号。

说明: 在 Windows 系统上，必须选择用于安装 IBM Security Key Lifecycle Manager 数据库的驱动器。Windows 驱动器指示符是一个字母，后面跟一个冒号 (:)。例如 C: 。

系统操作: 更正错误之前无法继续安装。

用户响应: 请输入格式正确的驱动器盘符。

CTGKM9050E 数据名称必须小于等于 8 个字符。

说明: 数据名称必须小于等于 8 个字符。

系统操作: 更正错误之前无法继续安装。

用户响应: 请选择另一个名称。

CTGKM9050I Windows DB2“数据库主目录”字段必须是可写入的驱动器盘符。

说明: 驱动器必须可写才能继续安装。

系统操作: 更正错误之前无法继续安装。

用户响应: 使用操作系统实用程序使驱动器可写，或者选择另一个驱动器。

CTGKM9051E 数据库名称不能包含特殊字符。

说明: 名称包含了一个或多个不正确的字符。

用户响应: 请重新输入名称并重试。

CTGKM9052E 数据库名称必须以字母字符开头。

说明: 数据库名称只能包含字母字符、数字字符和下划线（A-Z、a-z、0–9 和 _）。

系统操作: 更正错误之前无法继续安装。

用户响应: 请选择另一个名称。

CTGKM9053E 不支持当前选择使用的 DB2 版本。支持的版本为 10.1 以及更高版本。

说明: IBM Security Key Lifecycle Manager 需要受支持版本的 DB2。

系统操作: 安装任务失败。

用户响应: 请获取受支持版本的 DB2。然后重试。

CTGKM9054E 指定的位置不是有效的 DB2 安装目录。

说明: 指定的目录不包含现有 DB2 安装。

用户响应: 请选择一个有效的 DB2 安装目录。

CTGKM9055E “用户名”/“密码”字段不能超过 {0} 个字符。

说明: 您指定的值超出最大长度。

系统操作: 更正错误之前无法继续安装。

用户响应: 指定不超过限制的值。然后重试操作。

CTGKM9056E {0} 的密码和确认密码不匹配。

说明: “密码”和“确认密码”字段的值必须相同。

系统操作: 更正错误之前无法继续安装。

用户响应: 为“密码”和“确认密码”字段指定相同的值，然后重试操作。

CTGKM9057E “Application Server 管理员确认密码”字段为空。

说明: 用户未指定密码确认值。

系统操作: 更正错误之前无法继续安装。

用户响应: 在“确认密码”字段中输入值。然后重试。

CTGKM9058E “Application Server 管理员用户”字段为空。

说明: 当“Application Server 管理员用户”字段为空时会显示此消息。

系统操作: 更正错误之前无法继续安装。

用户响应: 指定值并重试。

CTGKM9059E “IBM Security Key Lifecycle Manager 管理员用户”字段为空。

说明: 当“IBM Security Key Lifecycle Manager 管理员用户”字段为空时会显示此消息。

系统操作: 更正错误之前无法继续安装。

用户响应: 指定值并重试。

CTGKM9060E “用户名”字段不能包含任何特殊字符。

说明: 用户名中包含一个或多个不正确的字符。

系统操作: 更正错误之前无法继续安装。

用户响应: 使用有效字符重新输入用户名并重试。

CTGKM9061E 指定的端口已在使用。

说明: 输入的端口号必须可供使用。端口号已在使用中。

系统操作: 更正错误之前无法继续安装。

用户响应: 请选择另一个端口号。确保指定的端口号可用。

CTGKM9062E “IBM Security Key Lifecycle Manager 管理员密码”字段为空。

说明: 当“IBM Security Key Lifecycle Manager 管理员密码”字段为空时会显示此消息。

系统操作: 更正错误之前无法继续安装。

用户响应: 指定值并重试。

CTGKM9063E “Application Server 管理员密码”字段为空。

说明: 当“Application Server 管理员密码”字段为空时会显示此消息。

系统操作: 更正错误之前无法继续安装。

用户响应: 指定值并重试。

CTGKM9064E “Encryption Key Manager 属性文件”字段为空。

说明: 当“Encryption Key Manager 属性文件”字段为空时会显示此消息。

系统操作: 更正错误之前无法继续安装。

用户响应: 请指定值。

CTGKM9065E “IBM Security Key Lifecycle Manager 管理员确认密码”字段为空。

说明: 用户未指定密码确认值。

系统操作: 更正错误之前无法继续安装。

用户响应: 指定值并重试。

CTGKM9066E “IBM Security Key Lifecycle Manager 应用程序端口号”为空。

说明: 当“IBM Security Key Lifecycle Manager 应用程序端口号”字段为空时会显示此消息。

系统操作: 更正错误之前无法继续安装。

用户响应: 指定值并重试。

CTGKM9067E “数据库管理员密码”字段为空。

说明: 当“数据库管理员密码”字段为空时会显示此消息。

系统操作: 更正错误之前无法继续安装。

用户响应: 指定值并重试。

CTGKM9068E 密钥库的密码为空。

说明: 必须指定密钥库的密码。

用户响应: 指定密钥库的密码并重试。

CTGKM9069E 用户名 {0} 或密码无效。

说明: 该操作需要有效的用户名和密码。

系统操作: 操作失败。

用户响应: 指定有效的用户名和密码。然后重试。

CTGKM9070E 此刻无法验证这些凭证。

说明: 指定的凭证可能不正确。

系统操作: 更正错误之前无法继续安装。

用户响应: 参阅 WebSphere Application Server 日志以获取更多信息，然后更正问题。

CTGKM9071E 无法启动 WebSphere Application Server 实例。

说明: 无法启动 WebSphere Application Server 实例。

系统操作: 更正错误之前无法继续安装。

用户响应: 参阅 WebSphere Application Server 日志以获取更多信息，然后更正问题。

CTGKM9072E 找不到 DB2 安装详细信息文件 {0}。

说明: 找不到 DB2 实例数据文件。

系统操作: 更正错误之前无法继续安装。

用户响应: 确保以下文件存在。

Windows 系统

以下目录中是否存在 `db2srcit.txt` 文件:

- `C:\tklmtemp`
- `C:\sklmV26properties`

Linux 和 AIX 系统

检查以下目录下的 `db2unix.srcit` 文件中是否缺少属性:

- `/tklmtemp`
- `/root/sklmV26properties`

CTGKM9073E DB2InstallResponseUpdater 至少需要 {0} 个参数。只有 {1} 个参数。

说明: 安装程序未对正在尝试执行的二进制文件传入正确的参数。这是 Installation Manager 无法解决的内部错误。

系统操作: 安装失败。

用户响应: 查看安装历史记录，找出有问题的软件包。在 Installation Manager 中，单击**文件 > 安装历史记录**。在控制台方式下，在主菜单中输入“S”以选择“查看安装历史记录”。与 IBM 客户支持联系。

CTGKM9074E 文件 {0} 不存在。

说明: 安装程序正在执行的二进制文件试图访问不存在的文件。这是 Installation Manager 无法解决的内部错误。

系统操作: 安装失败。

用户响应: 查看安装历史记录，找出有问题的软件包。在 Installation Manager 中，单击**文件 > 安装历史记录**。在控制台方式下，在主菜单中输入 S 以选择“查看安装历史记录”。与 IBM 客户支持联系。

CTGKM9075E 文件 {0} 是不可写的。

说明: 安装程序正在执行的二进制文件试图修改只读文件。这是 Installation Manager 无法解决的内部错误。

系统操作: 安装失败。

用户响应: 查看安装历史记录，找出有问题的软件包。在 Installation Manager 中，单击**文件 > 安装历史记录**。在控制台方式下，在主菜单中输入 S 以选择“查看安装历史记录”。与 IBM 客户支持联系。

CTGKM9076E 现已安装的 DB2 的指定路径无效。

说明: 现已安装的 DB2 的指定路径不正确。

系统操作: 更正错误之前无法继续安装。

用户响应: 请指定正确的路径。然后重试。

CTGKM9077E 响应文件对象为空。

说明: 必须指定响应文件。

用户响应: 请指定一个值。然后重试。

CTGKM9078E {0} 需要 {1} 个参数。只有 {2} 个参数。

说明: 安装程序未对正在尝试执行的二进制文件传入正确的参数。这是 Installation Manager 无法解决的内部错误。

系统操作: 安装失败。

用户响应: 查看安装历史记录，找出有问题的软件包。在 Installation Manager 中，单击**文件 > 安装历史记录**。在控制台方式下，在主菜单中输入 S 以选择“查看安装历史记录”。与 IBM 客户支持联系。

CTGKM9079E 文件系统中不存在路径 {0} 所指定的文件/文件夹。

说明: 安装程序正在执行的二进制文件试图访问不存在的文件。这是 Installation Manager 无法解决的内部错误。

系统操作: 安装失败。

用户响应: 查看安装历史记录，找出有问题的软件包。在 Installation Manager 中，单击**文件 > 安装历史记录**。在控制台方式下，在主菜单中输入 S 以选择“查看安装历史记录”。与 IBM 客户支持联系。

CTGKM9080E 在系统上检测到 IBM Tivoli Key Lifecycle Manager 服务器 V{0}。此版本无法升级到 V2.6。要继续安装，请将 IBM Tivoli Key Lifecycle Manager 升级到 V{1}。

说明: 安装失败。

系统操作: 更正错误之前无法继续安装。

用户响应: 将 IBM Tivoli Key Lifecycle Manager 升级到受支持的版本。

CTGKM9081E 执行 {0} 命令时出现错误

说明: 运行指定的命令时发生问题。

系统操作: 安装失败。

用户响应: 检查 Installation Manager 日志文件并执行必要的更正操作。然后重试。

CTGKM9082E 找不到正在运行的服务器进程。

说明: 尝试停止 WebSphere Application Server 时发生问题。

系统操作: 安装失败。

用户响应: 手动启动服务器并重试。

CTGKM9083E 无法确定 WebSphere Application Server V8.5 的安装位置。

说明: 安装程序无法确定 WebSphere Application Server V8.5 的位置。

系统操作: 安装失败。

用户响应: 卸载 Installation Manager 并重新运行安装过程。

CTGKM9084E DB2 安装详细信息文件无效。找不到 {0} 的条目。

说明: DB2 实例数据文件中存在的详细信息不正确。

系统操作: 安装失败。

用户响应:

Windows 系统

检查以下目录下的 `db2srcit.txt` 文件中是否缺少属性:

- `C:\tklmv2properties`
- `C:\tklmtemp`
- `C:\sklmV25properties`

Linux 和 AIX 系统

检查以下目录下的 `db2unix.srcit` 文件中是否缺少属性:

- `/tklmv2properties`
- `/tklmtemp`
- `/root/sklmV25properties`

CTGKM9085E 找不到 DB2 安装详细信息文件 {0}。

说明: 找不到 DB2 实例数据文件。

系统操作: 更正错误之前无法继续安装。

用户响应: 确保以下文件存在。

Windows 系统

以下目录中是否存在 db2srcit.txt 文件:

- C:\tklmtemp
- C:\sklmV26properties

Linux 和 AIX 系统

检查以下目录下的 db2unix.srcit 文件中是否缺少属性:

- /tklmtemp
- /root/sklmV26properties

CTGKM9086E 在注册表中找不到已安装的 WebSphere Application Server。

说明: 在安装注册表中找不到 WebSphere Application Server V8.5 的实例。

系统操作: 更正错误之前无法继续安装。

用户响应: 卸载 Installation Manager 并重新运行安装程序。

CTGKM9087E 无法从端口定义文件 {0} 装入数据。

说明: 无法读取 WebSphere Application Server 的端口定义文件。

系统操作: 更正错误之前无法继续安装。

用户响应: 清除一切现有安装并重新运行安装程序。

CTGKM9088E 端口定义文件 {0} 未包含必需的键 - {1}。

说明: 端口定义文件中的详细信息不正确。

系统操作: 更正错误之前无法继续安装。

用户响应: 清除一切现有安装并重新运行安装程序。

CTGKM9089E 无法获取密钥库文件位置。

说明: 找不到密钥库位置。

系统操作: 安装失败。

用户响应: 确保 Tivoli Key Lifecycle Manager 数据库已启动且正在运行，然后重新运行安装程序。

CTGKM9090E 必须选择 IBM DB2 和 IBM WebSphere Application Server 产品才能继续进行 IBM Security Key Lifecycle Manager 安装。请返回到上一个屏幕，然后选择 IBM DB2 V10.5.5 和 IBM WebSphere Application Server V8.5.5.6 产品。

说明: 您指定的详细信息不正确。

用户响应: 请指定正确的值。

CTGKM9091E 必须选择与 IBM Security Key Lifecycle Manager 关联的 IBM DB2 和 IBM WebSphere Application Server 产品才能继续进行 IBM Security Key Lifecycle Manager 卸载。请返回到上一个屏幕，然后选择 IBM DB2 V10.5.5 和 IBM WebSphere Application Server V8.5.5.6 产品。

说明: 您指定的详细信息不正确。

系统操作: 更正错误之前，无法继续卸载。

用户响应: 请指定正确的值。

CTGKM9092E 一个或多个先决条件未满足需求。下面给出了报告。

说明: 未满足安装先决条件需求。要进行安装，必须满足所有先决条件。

系统操作: 更正错误之前无法继续安装。

用户响应: 执行更正操作以满足需求。然后重试。

CTGKM9093E 系统上的驱动器均不具有安装该产品所需的空间 ({0})。

说明: 系统中不具有安装该产品所需的最小空间。

系统操作: 更正错误之前无法继续安装。

用户响应: 将指定驱动器上的可用空间量增加到所需的最小空间量。然后重试。

CTGKM9094E 无法读取 Prerequisite Scanner 结果。

说明: 运行 Prerequisite Scanner 后找不到先决条件输出文件。

系统操作: 更正错误之前无法继续安装。

用户响应: 在不从系统中删除任何文件的情况下重新运行安装程序。

CTGKM9095E 密码不符合操作系统密码策略需求。请检查最小密码长度和密码复杂性需求。

说明: 指定的密码违反密码规则。

系统操作: 密码在服务器上未更新。

用户响应: 请检查最小密码长度、密码复杂性和密码历史记录需求。

CTGKM9096E 为 WebSphere Application Server 管理员提供的凭证无效。

说明: 为 WebSphere Application Server 管理员指定了不正确的凭证。

系统操作: 更正错误之前无法继续安装。

用户响应: 为 WebSphere Application Server 管理员指定正确的用户名和密码。然后重试。

CTGKM9099E 需要 WebSphere 管理员凭证才能继续进行卸载。

说明: WebSphere Application Server 的用户名或密码未指定或不正确。

用户响应: 指定正确的 WebSphere Application Server 管理员用户名和密码，然后重试。

CTGKM9100E 找不到 DB2 安装详细信息文件 {0}

说明: 找不到 DB2 实例数据文件。

系统操作: 更正错误之前无法继续安装。

用户响应: 确保以下文件存在。

Windows 系统

以下目录中是否存在 db2srcit.txt 文件:

- C:\tklmtemp
- C:\sklmV26properties

Linux 和 AIX 系统

检查以下目录下的 db2unix.srcit 文件中是否缺少属性:

- /tklmtemp
- /root/sklmV26properties

CTGKM9101E 路径“<Variable formatSpec="{0}">VALUE_0</Variable>”位于网络文件系统上或不可写。请选择本地文件系统路径用于安装。

说明: 试图在不位于系统本地硬盘上的某个位置进行安装。

系统操作: 更正错误之前无法继续安装。

用户响应: 更改安装路径并指定系统上的本地路径。

CTGKM9102E 路径“<Variable formatSpec="{0}">VALUE_0</Variable>”位于网络驱动器上或不可写。请选择本地驱动器用于安装。

说明: 试图在不位于系统本地硬盘上的某个位置进行安装。

系统操作: 更正错误之前无法继续安装。

用户响应: 更改安装路径并指定系统上的本地路径。

CTGKM9103E 找不到 Prerequisite Scanner 工具的位置。

说明: 找不到 Prerequisite Scanner 的位置。

系统操作: 更正错误之前无法继续安装。

用户响应: 在不从系统中删除任何文件的情况下重新运行安装程序。

安装和迁移日志文件

如果安装或迁移时遇到意外的错误情况，请使用日志文件来确定问题的原因。

背景信息

在安装期间，安装程序会使用多个子程序、组件和子系统。许多错误情况是由于子程序故障而发生。

安装子程序、组件和系统

您可能会在日志文件中看到以下名称或缩写:

- DB2
- IBM Installation Manager (IM)

安装阶段

发生的错误情况和向您提供的日志文件取决于发生错误的阶段:

1. 介绍阶段，包含“语言选择”面板、“简介”面板以及“许可协议”面板。
2. DB2 安装阶段，包含收集用于安装 DB2 的信息的面板。输入这些信息后，安装程序将安装 DB2。
3. 中间件安装阶段，包含收集用于安装 WebSphere Application Server 中间件的信息的面板。输入这些信息后，安装程序将安装中间件。

   IBM Security Key Lifecycle Manager 在此阶段安装。

错误报告最有可能紧随 DB2 阶段和中间件安装阶段出现。

重要的日志文件

安装错误日志提供关键信息。

db2_install.log
DB2 安装日志文件。

db_config.log
包含关于 IBM Security Key Lifecycle Manager 数据库创建和表创建的信息。

***.out 和 *.err**
如果 **.err** 文件表示的操作成功，那么这些文件的大小为零字节。请检查大小大于零字节的错误文件。

首先使用的日志文件

了解错误发生时间可使您确定要首先使用的日志文件。DB2 阶段刚结束以及中间件阶段刚结束是最有可能发生错误的时候。使用以下列表可确定首先要使用的日志文件。

在 DB2 安装阶段中或刚结束时

1. 如果错误在早期发生，那么唯一可用的日志为: db2_install.log。
2. 如果错误在此阶段晚期发生，那么 sklmV26properties 目录可能包含某些 DB2 配置的结果或在此阶段运行的其他子程序的结果。
3. 错误日志文件的位置可能各不相同，这取决于错误发生在 DB2 阶段中，还是发生在 DB2 阶段结束时。

   在 DB2 阶段结束时，日志文件会从 sklmV26properties 目录复制到 *<IM logs>*\sklmLogs 目录。请参阅表 11 以了解这些文件的位置。

在中间件安装阶段中或紧随其后

要在其中检查错误的第一个日志文件为 db_config.log。

日志文件的名称和位置

安装完成之后，大部分错误日志位于 *WAS_HOME*\logs 目录中。

有关使用安装期间所产生错误文件的大致顺序，请参阅表 11。

如果发生迁移，那么在 *<IM App Data Dir>*\logs\sklmLogs\migration.log 目录中还有几个文件。

表 11. 安装日志文件的位置

日志文件	描述	位置
db2_install.log	DB2 安装日志。	在安装早期，此文件位于以下位置: **Windows 系统**: C:*<IM App Data Dir>*\logs\sklmLogs **AIX 和 Linux 系统**: /*<IM App Data Dir>*/logs/sklmLogs
db_config.log	包含关于数据库创建和表创建的信息。	**Windows 系统**: C:*<IM App Data Dir>*\logs\sklmLogs **AIX 和 Linux 系统**: /*<IM App Data Dir>*/logs/sklmLogs
各种 *.xml 和 *.log 文件	IBM Security Key Lifecycle Manager 安装日志文件。	**Windows 系统**: C:*<IM App Data Dir>*\logs **AIX 和 Linux 系统**: /*<IM App Data Dir>*/logs
各种 *.out 和 *.err 文件	安装期间生成的 STDOUT 和 STDERR 文件。	*WAS_HOME*\logs
migration.log	迁移事件。	*<IM App Data Dir>*\logs\sklmLogs\migration.log
results.txt	包含 Prerequisite Scanner 的结果。	%temp%/sklmPRS/results.txt

迁移日志文件的名称和位置

在迁移过程中，迁移程序调用其他程序或工具时会创建日志文件。

如果迁移失败，那么请检查 *<IM App Data Dir>*\logs\sklmLogs\migration.log 目录中的迁移日志文件。

检查错误日志文件

必须查看日志文件以检查错误日志文件。

过程

1. 查看日志文件列表 从哪个日志文件开始取决于操作系统和安装阶段。第 117 页的『首先使用的日志文件』 中的列表可以提供一个起始点: 可以在找到具有错误消息的一个日志文件之前检查几个日志文件。
2. 转至日志文件所在的目录，然后使用文本编辑器打开目录。 在 Windows 系统上，使用可以处理 UNIX 样式的换行符字符的文本编辑器，比如 Microsoft WordPad。
3. 最新的日志条目位于文件的末尾。从日志文件中的最后一个条目开始，检查每个条目。 注意所涉及的程序以及该条目的时间戳记（如有）。

   在查看了最后一条条目后，查看倒数第二条条目。就像查看之前的条目一样查看此条目。扫描在两个地方提到的任何内容，比如文件名或错误条件。

   重复之前的步骤，在日志文件中向上移动。可能有好几条具有与此错误条件相关的信息的条目。如果此日志文件中的信息不足，请查看其他的日志文件以获取更多信息。

   如果没有有关错误的任何消息，请转至另一个日志文件。

其他要收集的信息

您必须执行可能提供更多信息的若干操作以验证安装。

- 检查可用磁盘空间。请参阅第 7 页的『分布式系统的硬件需求』以了解最低空间需求。
- 确定 DB2 实例是否已创建。如果已创建，即证明 DB2 安装成功。

  要验证 DB2 实例是否已创建，请以 IBM Security Key Lifecycle Manager DB2 实例所有者的身份登录，浏览至 *DB_INSTANCE_HOME* 目录，然后运行:

  ```
  db2ilist
  ```

  此时将显示已配置实例的列表。IBM Security Key Lifecycle Manager 的实例名称（例如 sklmdb2）通常位于该列表中。
- 使用实例所有者用户标识启动和停止 IBM Security Key Lifecycle Manager 数据库服务器。此操作可验证数据库创建。

  要启动和停止数据库，请以 IBM Security Key Lifecycle Manager DB2 实例所有者的身份登录，浏览至 *DB_INSTANCE_HOME* 目录，然后对数据库运行 **db2start** 和 **db2stop** 命令。
- 显示 DB2 数据库中表的列表。此操作可验证“动态数据语言”进程。

要显示表的列表，请以 IBM Security Key Lifecycle Manager DB2 实例所有者的身份登录，浏览至 *DB_INSTANCE_HOME* 目录，然后运行以下命令:

```
db2 connect to sklm_database user sklm_instance_owner_userid \
using sklm_instance_owner_passwd

db2 list tables

db2 describe table table_name
```

- 确定 WebSphere Application Server 的 Java 进程是否正在运行。如果该进程正在运行，即证明 WebSphere Application Server 安装成功。

  要验证该 Java 进程是否正在运行，请浏览至 *WAS_HOME*/bin 目录并运行以下命令以停止并重新启动服务器:

  ```
  stopServer.sh server1
  startServer.sh server1
  ```

  如果已启用全局安全性，请向这些命令中添加以下参数以停止并重新启动服务器:

  ```
  -username was_admin_id -password was_admin_passwd
  ```

  在 Windows 系统上，还可以打开“Windows 服务”控制台并验证 KLMProfile 的服务是否已启动。
- 启动 IBM Security Key Lifecycle Manager 应用程序以验证 IBM Security Key Lifecycle Manager 安装以及总体安装。

  要启动 IBM Security Key Lifecycle Manager 应用程序，请启动 WebSphere Application Server，然后查找 IBM Security Key Lifecycle Manager 任务。

声明

本信息是为在美国国内供应的产品和服务而编写的。IBM 可能在其他国家或地区不提供本文档中讨论的产品、服务或功能特性。有关您当前所在区域的产品和服务的信息，请向您当地的 IBM 代表咨询。任何对 IBM 产品、程序或服务的引用并非意在明示或暗示只能使用 IBM 的产品、程序或服务。只要不侵犯 IBM 的知识产权，任何同等功能的产品、程序或服务，都可以代替 IBM 产品、程序或服务。但是，评估和验证任何非 IBM 产品、程序或服务，则由用户自行负责。

IBM 公司可能已拥有或正在申请与本文档内容有关的各项专利。提供本文档并未授予用户使用这些专利的任何许可。您可以用书面方式将许可查询寄往:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

有关双字节字符集 (DBCS) 信息的许可查询，请与您所在国家或地区的 IBM 知识产权部门联系，或用书面方式将查询寄往:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

本条款不适用英国或任何这样的条款与当地法律不一致的国家或地区:

International Business Machines Corporation“按现状”提供本出版物，不附有任何种类的（无论是明示的还是暗含的）保证，包括但不限于暗含的有关非侵权、适销和适用于某种特定用途的保证。

某些国家或地区在某些交易中不允许免除明示或暗含的保证。因此本条款可能不适用于您。

本信息中可能包含技术方面不够准确的地方或印刷错误。此处的信息将定期更改；这些更改将编入本资料的新版本中。IBM 可以随时对本资料中描述的产品和/或程序进行改进和/或更改，而不另行通知。

本信息中对非 IBM Web 站点的任何引用都只是为了方便起见才提供的，不以任何方式充当对那些 Web 站点的保证。那些 Web 站点中的资料不是 IBM 产品资料的一部分，使用那些 Web 站点带来的风险将由您自行承担。

IBM 可以按它认为适当的任何方式使用或分发您所提供的任何信息而无须对您承担任何责任。

本程序的被许可方如果要了解有关程序的信息以达到如下目的: (i) 允许在独立创建的程序和其他程序（包括本程序）之间进行信息交换，以及 (ii) 允许对已经交换的信息进行相互使用，请与下列地址联系:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

只要遵守适当的条件和条款，包括某些情形下的一定数量的付费， 都可获得这方面的信息。

本资料中描述的许可程序及其所有可用的许可资料均由 IBM 依据 IBM 客户协议、IBM 国际软件许可协议或任何同等协议中的条款提供。

此处包含的任何性能数据都是在受控环境中测得的。因此，在其他操作环境中获得的数据可能会有明显的不同。有些测量可能是在开发级的系统上进行的，因此不保证与一般可用系统上进行的测量结果相同。此外，有些测量是通过推算而估计的， 实际结果可能会有差异。本文档的用户应当验证其特定环境的适用数据。

涉及非 IBM 产品的信息可从这些产品的供应商、其出版说明或其他可公开获得的资料中获取。IBM 没有对这些产品进行测试，也无法确认其性能的精确性、兼容性或任何其他关于非 IBM 产品的声明。有关非 IBM 产品性能的问题应当向这些产品的供应商提出。

所有关于 IBM 未来方向或意向的声明都可随时更改或收回，而不另行通知，它们仅仅表示了目标和意愿而已。

所有 IBM 的价格均是 IBM 当前的建议零售价，可随时更改而不另行通知。经销商的价格可与此不同。

本信息仅用于规划的目的。在所描述的产品上市之前，此处的信息会有更改。

本信息包括日常业务运作中使用的数据和报告的示例。为了尽可能完整地说明这些示例，示例中可能会包括个人、公司、品牌和产品的名称。所有这些名称均是虚构的，如与实际商业企业使用的名称和地址雷同，纯属巧合。

版权许可:

本信息包括源语言形式的样本应用程序，这些样本说明不同操作平台上的编程方法。如果是为按照在编写样本程序的操作平台上的应用程序编程接口 (API) 进行应用程序的开发、使用、经销或分发为目的，您可以任何形式对这些样本程序进行复制、修改、分发，而无须向 IBM 付费。这些示例并未在所有条件下作全面测试。因此，IBM 不能担保或暗示这些程序的可靠性、可维护性或功能。用户如果是为了按照 IBM 应用程序编程接口开发、使用、经销或分发应用程序，则可以任何形式复制、修改和分发这些样本程序，而无须向 IBM 付费。

凡这些实例程序的每份拷贝或其任何部分或任何衍生产品，都必须包括如下版权声明:

©（贵公司的名称）（年）。此部分代码是根据 IBM 公司的样本程序衍生出来的。© Copyright IBM Corp. （输入年份）. All rights reserved.

如果您正在查看本信息的软拷贝格式，图片和彩色图例可能无法显示。

产品文档的条款和条件

这些出版物的使用权是依据下列条款和条件而授予。

适用性 这些条款和条件是对 IBM Web 站点的任何使用条款的补充。

个人使用

您可以复制这些出版物以供您个人非商业性使用，但必须保留全部所有权声明。未经 IBM 明确同意，您不得分发、显示或衍生这些出版物或其中的任何部分。

商业使用

您只能在企业内复制、分发和显示这些出版物，但必须保留全部所有权声明。未经 IBM 明确同意，您不得在企业外部衍生这些出版物，也不得复制、分发或显示这些出版物或其中的任何部分。

权利 除本许可权中明确授予的权限以外，未授予对出版物或其中所含任何信息、数据、软件或其他智慧财产的任何其他明示或默示许可权、许可证或权利。

IBM 保留在出版物的使用损害其利益或者上述指示未得到正确遵循（由 IBM 确定）时自行撤回此处所授予许可权的权利。

除非完全符合所有适用的法律法规，包括美国的所有出口法律及法规，否则不得下载、出口或再出口此信息

IBM 不对这些出版物的内容作任何保证。这些出版物“按现状”提供，不附有任何种类的（无论是明示的还是暗含的）保证，包括但不限于暗含的有关适销、不侵权和适用于某种特定用途的保证。

商标

IBM、IBM 徽标和 ibm.com 是 International Business Machines Corp. 在全世界许多司法辖区注册的注册商标或商标。其他产品和服务名称可能是 IBM 或其他公司的商标。IBM 商标的当前列表可以从 Web 上获得 (http://www.ibm.com/legal/copytrade.shtml)。

Adobe、Acrobat、PostScript 和所有基于 Adobe 的商标是 Adobe Systems Incorporated 在美国和/或其他国家或地区的注册商标或商标。

IT Infrastructure Library 是 Central Computer and Telecommunications Agency（它现在是 Office of Government Commerce 的一部分）的注册商标。

Intel、Intel 徽标、Intel Inside、Intel Inside 徽标、Intel Centrino、Intel Centrino 徽标、Celeron、Intel Xeon、Intel SpeedStep、Itanium 和 Pentium 是 Intel Corporation 或其子公司在美国和其他国家或地区的商标或注册商标。

Linux 是 Linus Torvalds 在美国和/或其他国家或地区的商标。

Microsoft、Windows、Windows NT 以及 Windows 徽标是 Microsoft Corporation 在美国和/或其他国家或地区的商标。

ITIL 是英国政府商务部的注册商标和欧盟注册商标，且已在美国专利和商标局注册。

UNIX 是 The Open Group 在美国和其他国家或地区的注册商标。

Java 和所有基于 Java 的商标和徽标是 Oracle 和/或其子公司的商标或注册商标。

Cell Broadband Engine 是 Sony Computer Entertainment Inc. 在美国和/或其他国家或地区的商标并且在当地许可证下使用。

Linear Tape-Open、LTO、LTO 徽标、Ultrium 和 Ultrium 徽标是 HP、IBM Corp. 和 Quantum 在美国和/或其他国家或地区的商标。

索引

[A]

[B]

[C]

[D]

[F]

[G]

[H]

[J]

[K]

[L]

[M]

[P]

[Q]

[R]

[S]

[T]

[W]

[X]

[Y]

[Z]

[数字]

A

B

D

E

F

G

I

J

K

L

M

O

P

R

S

T