场景

IBM

目录

场景

场景演示了如何应用技术以实现业务目标并解决问题。 它们描述了将讨论运用到实际中的假设业务情况。

这些场景研究了使用 IBM Security Key Lifecycle Manager 可以执行的某些首要步骤和某些更高级的任务。作为这些场景的必备软件，请安装 IBM Security Key Lifecycle Manager 服务器并验证其组件是否在运行中。

场景: 提供主服务器和副本服务器

要确保有连续的密钥和证书可用于加密设备，请为您的企业配置主 IBM Security Key Lifecycle Manager 服务器和副本 IBM Security Key Lifecycle Manager 服务器。 然后，提供保护关键数据的重复备份和恢复操作。

在 Windows 系统和其他系统上，两个系统必须具有满足工作负载的所需内存、速度和可用磁盘空间。

IBM Security Key Lifecycle Manager 以独立于应用程序的操作系统和目录结构的方式创建备份文件。 您可以将备份文件复原到不同于从其备份的操作系统的操作系统。

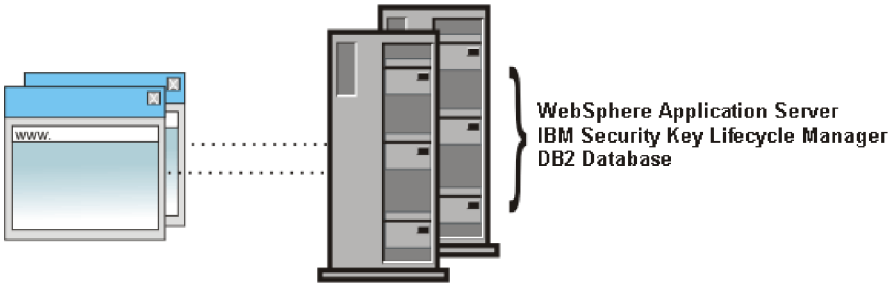

图 1. 主 IBM Security Key Lifecycle Manager 服务器和副本 IBM Security Key Lifecycle Manager 服务器

在创建副本服务器之前，对操作中的需求进行编目，可能包括:

- 站点独有的灾难恢复过程。 此过程可能需要特别的或周期性的活动以确保主 IBM Security Key Lifecycle Manager 服务器和副本 IBM Security Key Lifecycle Manager 服务器同时可用。

  您的站点可能需要定期执行演示主 IBM Security Key Lifecycle Manager 服务器的模拟故障会导致副本的立即响应。

  IBM Security Key Lifecycle Manager 服务器不提供自动故障转移。 您必须单独设置必要的设备控件，以确保在主服务器失败时，副本服务器可用。
- 初始安装和配置IBM Security Key Lifecycle Manager 服务器，以及安装中需要密钥和证书的设备。

您可能还会选择在其他服务器上安装和配置 IBM Security Key Lifecycle Manager 服务器及其必备软件，并设置备份和恢复关键数据的调度。

- 您的组织通常更改密钥和证书的时间周期。

  如果组织每月或每季度替换一次密钥和证书，请确保当新的密钥和证书在开始使用周期之前备份密钥资料和其他数据。
- 导致创建证书请求并将请求发送到认证中心的事件。

  使用站点或认证中心需要的安全通信进程。 直到返回实际的证书之前，请运行备份以保护与证书请求关联的密钥和数据。
- IBM Security Key Lifecycle Manager 服务器的升级和相关的中间件修订包。

  运行备份以确保升级后的 IBM Security Key Lifecycle Manager 服务器使用的密钥和其他关键数据与升级前使用的相同。

备份和复原实践

执行更改（例如，添加或更改设备、密钥和证书）时，必须备份 IBM Security Key Lifecycle Manager 关键数据。 IBM Security Key Lifecycle Manager 提供了创建配置文件的备份文件、数据库和其他数据的任务。 您可以将此备份文件复原到不同于从其备份的操作系统的操作系统。

未能正确备份关键数据可能会导致无法访问所有加密的数据，并且无法恢复对这些数据的访问。 不要对备份文件进行加密，或将备份文件存储在加密设备上。 备份数据失败还可能会导致密钥管理器在以后出现不一致的情况，也可能丢失存储设备上的数据。

可以遵循以下实践:

- 同时维护并发运行的主 IBM Security Key Lifecycle Manager 服务器和至少一个副本 IBM Security Key Lifecycle Manager 服务器。 如果主服务器出现故障，请确保存储设备有权访问它的密钥。

  IBM Security Key Lifecycle Manager 服务器不提供自动故障转移。 您必须单独设置必要的设备控件，以确保在主服务器失败时，副本服务器可用。
- 只要添加或更改设备、密钥或证书，就运行备份任务。 将 IBM Security Key Lifecycle Manager 备份文件恢复到副本 IBM Security Key Lifecycle Manager 服务器中。
- 在主服务器始终可用的正常操作情况下，请不要对副本计算机上的 IBM Security Key Lifecycle Manager 服务器 进行更改。 如果故障事件在主服务器关闭时在副本服务器上发生了重要活动，请备份副本服务器并将备份文件复原到主服务器。
- 只使用 IBM Security Key Lifecycle Manager 备份和恢复任务创建备份文件。 只使用 IBM Security Key Lifecycle Manager 来恢复备份文件包含的数据。 不要采取其他手动步骤来备份或恢复文件。
- 请妥善保存备份文件，保存位置应与运行 IBM Security Key Lifecycle Manager 服务器的计算机不同。如果主 IBM Security Key Lifecycle Manager 服务器上的文件丢失，请确保可以在替换服务器上重新构建该功能。 这些文件可能位于地理上独立的位置。

备份和复原运行时需求

备份和复原 IBM Security Key Lifecycle Manager 备份文件的数据有一些运行时需求。

通过增加允许备份和复原大型密钥填充事务的时间间隔，可避免超时故障。为此文件中的 **totalTranLifetimeTimeout** 设置指定一个更大的值:

WAS_HOME/profiles/KLMProfile/config/cells/
SKLMCell/nodes/SKLMNode/servers/server1/server.xml

此外，必须满足以下条件:

- 确保任务在允许密钥提供活动停止的时间间隔期间执行。
- 对于备份任务，IBM Security Key Lifecycle Manager 服务器必须在正常操作状态下运行。 IBM Security Key Lifecycle Manager 数据库实例必须可用。
- 对于恢复任务，必须可通过 IBM Security Key Lifecycle Manager 数据源访问 IBM Security Key Lifecycle Manager 数据库实例。

  在开始恢复任务之前，请确保您具有创建备份文件时使用的密码。 恢复的文件必须写入先前从中备份数据的相同 IBM Security Key Lifecycle Manager 服务器中。 或者，复原的文件必须写入副本计算机中。
- 请确保与 **tklm.backup.dir** 属性相关联的目录存在。另外，请确保对系统的这些目录以及在 IBM Security Key Lifecycle Manager 服务器和 DB2® 服务器 上运行的 IBM Security Key Lifecycle Manager 管理员账户有读写访问权。

设置副本计算机

IBM Security Key Lifecycle Manager 的副本计算机具有的存储容量和可用磁盘空间必须等于或大于通常运行 IBM Security Key Lifecycle Manager 服务器的主计算机。

关于此任务

使用 IBM Security Key Lifecycle Manager 安装程序并重复在主计算机上执行过的相同步骤。

过程

1. 获取存储容量和可用磁盘空间等于或大于通常运行 IBM Security Key Lifecycle Manager 服务器的计算机的计算机。
2. 在副本计算机上安装和配置操作系统和修订，以与通常运行 IBM Security Key Lifecycle Manager 服务器的计算机上的系统相匹配。
3. 完成 IBM Security Key Lifecycle Manager 的 IBM Knowledge Center 上的“安装和配置”部分中描述的安装步骤和验证步骤。

下一步做什么

在安装和验证通常运行 IBM Security Key Lifecycle Manager 的主计算机后，配置和测试副本计算机。

验证在主 IBM Security Key Lifecycle Manager 服务器上创建的当前备份文件是否在副本计算机成功恢复。

发生重要副本服务器活动后进行响应

主 IBM Security Key Lifecycle Manager 服务器关闭时，副本服务器可能具有重要活动。选择公告的维护时间间隔，以在网络流量停止时，备份副本服务器，并将备份文件恢复到主服务器中。

关于此任务

如果副本服务器提供设备的密钥，那么不会发出任何警报。 验证是否确实需要备份副本计算机，然后将备份文件恢复到主服务器。例如，您可能要确定写请求是否会导致向设备提供密钥。 使用 **tklmServedDataList** 命令查询数据库并列出已提供的数据。 有关来自设备的读请求的不太重要的信息位于审计日志中。

过程

1. 在公告的网络流量停止时间，备份副本计算机。
2. 将副本计算机的备份文件恢复到通常运行 IBM Security Key Lifecycle Manager 服务器的主计算机中。

下一步做什么

验证主 IBM Security Key Lifecycle Manager 服务器是否处于活动状态，以及是否成功恢复备份文件。

场景: 请求第三方证书

IBM Security Key Lifecycle Manager 可以生成一个可发送到认证中心的 PKCS #10 格式的证书请求。 使用返回的 CA 证书可保护支持加密的设备上的数据，或进行 SSL 通信。

1. 在开始之前，确定是将证书用于 SSL 认证，还是用于保护与 3592 磁带机或 DS8000 Turbo 磁带机进行的通信。
2. 对于预期要在下一个业务周期内使用的每个证书，请创建一个证书请求。

   生成的证书请求文件位于 SKLM_HOME 目录中。 例如，生成的证书请求可能是文件，例如 SKLM_HOME\080419154137-sslcert001.csr。

   证书请求文件是已编码的 base64 格式的，编辑器无法读取改文件。

   证书请求文件包含 base64 格式信息，包括:

   - 版本号。
   - 主题名称，即请求者的 X.500 名称。 例如，X.500 名称包含公共名称 (CN) 值、组织和识别主题的其他值。
   - 公用密钥数据和算法唯一标识。 可以使用诸如 RSA 或 ECDSA 之类的算法。
   - 由用户专用密钥签名的已生成的数据签名。

   密钥库数据库包含用于生成证书请求签名的专用密钥。

   此外，与证书请求相关的信息会存储在数据库中。 这些信息包括 X.500 主题名称、开始日期、截止日期和停用日期，以及通常为证书指定的其他属性的其他值（包括证书请求的暂挂状态）。 这些值会在导入返回的证书时进行更新。
3. 在证书返回之前保护证书请求。 对于在创建并发送证书请求后以及在密钥库数据库中更改实际密钥或证书时来说，对密钥库数据库运行备份任务十分重要。
4. 在确保备份文件准备妥当之后，请使用站点或认证中心进行电子邮件或 HTTPS 传输所需的安全通信过程，手动向所选的认证中心发送证书请求。
5. 导入返回的与先前证书请求匹配的证书。

在收到有效的请求后，认证中心将返回 DER 或 base64 编码的证书。 该证书包含在证书请求中提供的公用密钥以及认证中心的签名，这说明公用密钥是有效的并且您的企业是真正的所有者。 证书主题名称是在证书请求中提供的 X.500 主题名称。

6. 在此备份包含了新证书的密钥库数据库。

创建证书请求

使用“创建证书”对话框、**tklmCertGenRequest** 命令或“**证书生成请求 REST 服务**”来创建证书请求。

关于此任务

在开始之前，确定用于获取由认证中心发出的证书的站点策略和过程。

过程

1. 浏览至相应的页面或目录:
   - 图形用户界面:
     a. 登录图形用户界面。
     b. 在“欢迎”页面的“密钥和设备管理”部分，选择 **3592** 或 **DS8000** 设备组。
     c. 单击**转至 > 根据指导创建密钥和设备**。
     d. 或者，右键单击 **3592** 或 **DS8000**，然后选择**根据指导创建密钥和设备**。
   - 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
       ```

   - REST 界面:
     – 打开 REST 客户机。
2. 请求证书:
   - 图形用户界面:
     a. 在“步骤 1: 创建证书”页面上，单击**创建**。
     b. 在“创建证书”对话框中，选择第三方提供程序的证书请求。
     c. 指定必需和可选参数的值。
     d. 单击**创建证书**。
   - 命令行界面:

     输入 tklmCertGenRequest 以创建证书请求文件。 例如:
     – SSL 通信

```
print AdminTask.tklmCertGenRequest('[-alias sklmSSLCertificate1
 -cn sklm -ou sales -o myCompanyName -locality myLocation
  -country US -validity 999 -keyStoreName defaultKeyStore
   -fileName mySSLCertRequest1.crt -usage SSLSERVER]')
```

– 3592 磁带机

```
print AdminTask.tklmCertGenRequest('[-alias sklmCertificate1
 -cn sklm -ou marketing -o CompanyName -locality myLocation
  -country US -validity 999 -keyStoreName defaultKeyStore
   -fileName myCertRequest1.crt -usage 3592]')
```

– DS8000 Turbo 磁带机

```
print AdminTask.tklmCertGenRequest('[-alias sklmCertificate3
 -cn sklm -ou sales -o myCompanyName -locality myLocation
  -country US -validity 999 -keyStoreName defaultKeyStore
   -fileName myCertRequest3.crt -usage DS8000]')
```

- REST 界面:

a. 获取唯一的用户认证标识以访问 IBM Security Key Lifecycle Manager REST 服务。有关认证过程的更多信息，请参阅REST 服务的认证过程。

b. 要调用**证书生成请求 REST 服务**，请发送 HTTP POST 请求。请随请求消息一起传递您在步骤 a 中获得的用户认证标识，如以下示例所示。

– SSL 通信

```
POST https://localhost:9080/SKLM/rest/v1/certificates
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth authId=139aeh34567m
{"type":"certreq","alias":"sklmSSLCertificate1","cn":"sklm","ou":
"sales","o":
"myCompanyName","usage":"SSLSERVER","country":"US","validity":"999",
"fileName":
"mySSLCertRequest1.crt","algorithm":"ECDSA"}
```

– 3592 磁带机

```
POST https://localhost:9080/SKLM/rest/v1/certificates
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth authId=139aeh34567m
{"type":"certreq","alias":"sklmCertificate1","cn":"sklm","ou":
"sales","o":
"myCompanyName","usage":"3592","country":"US","validity":"999",
"fileName":
"myCertRequest1.crt","algorithm":"ECDSA"}
```

– DS8000 Turbo 磁带机

```
POST https://localhost:9080/SKLM/rest/v1/certificates
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth authId=139aeh34567m
{"type":"certreq","alias":"sklmCertificate3","cn":"sklm","ou":
"sales","o":
"myCompanyName","usage":"DS8000","country":"US","validity":"999",
"fileName":
"myCertRequest1.crt","algorithm":"ECDSA"}
```

3. 成功指示符会根据界面的不同而不同:

- 图形用户界面:

  证书或证书请求会显示为**证书**表中的项。返回“欢迎”页面。 在“欢迎”页面的**操作项**中，证书请求会显示在**暂挂证书**表中。

- 命令行界面:

完成消息表示成功。

- REST 界面:

  状态码 200 OK 表示成功。

下一步做什么

通过组织提供的安全通信过程，手动向认证中心发送证书请求。 此外，保留证书请求的别名值以在导入返回的证书时使用，返回的证书必须与证书请求匹配。

导入证书

可以使用图形用户界面的“欢迎”页面上的暂挂证书链接、**tklmCertImport** CLI命令或“**证书导入 REST 服务**”，导入先前从认证中心请求的证书。

关于此任务

在开始之前，确保入局证书的别名与先前的证书请求别名匹配，例如 sklm cert1。 将证书文件写入临时目录。

检索原始证书请求的别名以在导入返回的证书时使用，返回的证书必须指定正确的别名。

要查找主题名称为 X.500 的证书请求以确定它是否与主题名称为 X.500 的证书匹配，请通过将 state 属性的值指定为 pending，运行 **tklmCertList** 命令或“**证书列表 REST 服务**”。

要查看证书文件的主题名称，可以执行以下步骤:

- Windows 系统:

  直接打开证书文件。 Windows 本机实用程序将以可读取的格式显示证书中的信息。

- 其他系统:

  使用新的别名将证书导入 IBM Security Key Lifecycle Manager。 然后，运行 **tklmCertList** 命令或“**证书列表 REST 服务**”并指定别名以查看证书信息。

过程

1. 浏览至相应的页面或目录:
   - 图形用户界面:

     登录图形用户界面。将显示“欢迎”页面。

   - 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
```

- REST 界面:
  - 打开 REST 客户机。

2. 导入证书:
   - 图形用户界面
     a. 在“欢迎”页面“操作项”部分的“密钥组和证书”区域中，单击**您具有暂挂证书**。
     b. 在**暂挂证书**表中，选择相应的暂挂证书。
     c. 单击**导入**。
     d. 在**文件名和位置**字段中，输入由认证中心返回的证书请求文件的路径和文件名。
     e. 或者，单击**浏览**来浏览到证书请求文件。 例如，您可能会浏览到 *drive*:\Program Files (x86)\IBM\WebSphere\AppServer\products\sklm 目录中的暂挂证书。
     f. 单击**导入**。
   - 命令行界面:

     输入 tklmCertImport 以导入证书。 例如:
     - SSL 通信

```
print AdminTask.tklmCertImport
 ('[-fileName myTempPath\\mySSLCertRequest1.cer
   -alias sklmSSLCertificate1 -format base64
     -keyStoreName defaultKeyStore -usage SSLSERVER]')
```

     - 3592 磁带机

```
print AdminTask.tklmCertImport \
 ('[-fileName myTempPath\\myCertRequest2.cer
   -alias sklmCertificate2 -format base64
     -keyStoreName defaultKeyStore -usage 3592]')
```

     - DS8000 Turbo 磁带机

```
print AdminTask.tklmCertImport
 ('[-fileName myTempPath\\myCertRequest3.cer
   -alias sklmCertificate3 -format base64
     -keyStoreName defaultKeyStore -usage DS8000]')
```

   - REST 界面
     a. 获取唯一的用户认证标识以访问 IBM Security Key Lifecycle Manager REST 服务。有关认证过程的更多信息，请参阅REST 服务的认证过程。
     b. 要调用**证书导入 REST 服务**，请发送 HTTP POST 请求。请随请求消息一起传递您在步骤 a 中获得的用户认证标识，如以下示例所示。
        - SSL 通信

```
POST https://localhost:9080/SKLM/rest/v1/certificates/import
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth authId=139aeh34567m
{"fileName":"/mycertfilenam.base64","alias","sklmSSLCertificate1",
"format":"base64",
"usage":"SSLSERVER"}
```

        - 3592 磁带机

```
POST https://localhost:9080/SKLM/rest/v1/certificates/import
Content-Type: application/json
Accept: application/json
Authorization: SKLMAuth authId=139aeh34567m
{"fileName":"/mycertfilenam.base64","alias","sklmSSLCertificate2",
"format":"base64",
"usage":"3592"}
```

– DS8000 Turbo 磁带机

```
POST https://localhost:9080/SKLM/rest/v1/certificates/import
Content-Type: application/json
Accept: application/json
Authorization: SKLMAuth authId=139aeh34567m
{"fileName":"/mycertfilenam.base64","alias","sklmSSLCertificate3",
"format":"base64",
"usage":"DS8000"}
```

3. 成功指示符会根据界面的不同而不同:
   - 图形用户界面:

     暂挂证书条目将从“欢迎”页面的**暂挂证书**表中除去。 如果没有证书要导入，那么**暂挂证书**表将会从“欢迎”页面的“操作项”部分除去。
   - 命令行界面:

     完成消息表示成功。
   - REST 界面:

     状态码 200 OK 表示成功。

下一步做什么

确保备份密钥材料以保护证书。 然后，可能要将证书与一个或多个设备关联。

证书请求问题

您必须解决创建证书请求或启用返回的证书以使用时发生的问题。

- 在创建证书请求之前，请以管理员的身份解决这些问题:
  – **问题**: 您可能没有对证书请求文件的写许可权。 也可能是没有足够的可用磁盘空间，或数据库可能不可用。

    解决方案: 确保您的许可权正确，具有足够的可用磁盘空间，并且数据库连接可用。 否则，请进行相应的更正。 然后重试操作。
  – **问题**: 没有为公共名称指定值。公共名称 (cn) 是证书的唯一标识的一部分。 例如，值cn 用于证书的主题名称，它可以识别正在导入的证书是否与原始证书请求相匹配。

    解决方案: 指定证书的公共名称。然后重试操作。
  – **问题**: 证书请求文件存在。

    解决方案: 证书请求中指定的文件名与现有的证书请求文件名相匹配。 请为证书请求指定不同的文件名。 例如，指定 myUniqueRequest.crt。然后重试操作。
- 当导入已返回的 CA 证书时，请解决以下问题:
  – **问题**: 从认证中心返回的证书的主题名称与原始证书请求中的主题名称不匹配。

解决方案: 更正文件名或别名规范。 然后，重新尝试导入操作。

– **问题**: 验证密钥和证书时出错。向认证中心提交的证书请求与所返回的证书不匹配。

解决方案: 该问题可能是一个内部处理错误。 收集可能位于审计日志中的任何信息，然后联系 IBM 软件支持。

– **问题**: 要导入的证书中的密钥与原始证书请求中的密钥不匹配。

解决方案: 您尝试将返回的证书与不正确的证书请求相匹配。 使用与此响应对应的别名导入证书。 然后重试操作。

– **问题**: 导入到期年限超过 50 年的证书时，您可能会看到以下消息:

使用命令行界面

```
CTGKM0002E Command failed: javax.management.MBeanException:
RuntimeException thrown in RequiredModelMBean while trying to invoke
operation importCertificate
```

使用图形用户界面

```
Cannot import certificate to the keystore.
javax.management.MBeanException: RuntimeException thrown in
RequiredModelMBean while trying to invoke operation
importCertificate
```

变通方法: 证书到期年限不能超过 50 年。 要修改到期年限，请更改 SKLMConfig.properties 文件中的 **maximum.keycert.expiration.period.in.years** 参数值。

场景: IBM Security Key Lifecycle Manager 批量复制设置

可以使用 IBM Security Key Lifecycle Manager 将密钥资料、配置文件和其他关键信息从第一主服务器自动复制到最多 20 个辅助克隆服务器中。 此自动复制可确保密钥和证书持续可供加密设备使用。

注: 仅在添加新密钥时才能运行自动复制过程。

数据复制可实现将 IBM Security Key Lifecycle Manager 环境以独立于服务器的操作系统和目录结构的方式克隆到多个服务器。

自动复制确保在主 IBM Security Key Lifecycle Manager 实例不可用时可使用备份系统。备份系统包含所有必需的密钥及其关联的数据。 您可以使用图形用户界面、CLI 命令或 REST 界面执行以下复制任务:

- 安排复制过程
- 启动和停止复制任务
- 提供复制任务的状态
- 执行复制配置文件功能

复制配置文件

您可以将 IBM Security Key Lifecycle Manager 复制作为一个独立任务来运行。 必须提供了有效复制配置文件，以在添加新密钥时启动自动化复制过程。

IBM Security Key Lifecycle Manager 使用 <*SKLM_HOME*>\config\ReplicationSKLMConfig.properties 配置文件中的属性来控制复制过程。 例如，C:\Program Files (x86)\IBM\WebSphere\AppServer\products\sklm\config\ReplicationSKLMConfig.properties。您可以使用 IBM Security Key Lifecycle Manager 图形用户界面、命令行界面或 REST 界面，更改复制配置文件的属性。

您可以对每个系统进行以下分类:

- 主控 - 将要被复制的主系统。
- 克隆 - 将要被复制到的辅助系统

主系统的复制文件可以至多指定 20 个克隆系统。 每个克隆系统通过 IP 地址或主机名以及端口号进行识别。 您可以将 IBM Security Key Lifecycle Manager 环境以独立于服务器的操作系统和目录结构的方式复制到多个克隆服务器。

注释:

- 仅当在主系统中添加新密钥时才会执行已计划的复制。
- 一个主系统最多可以带 20 个克隆系统。不支持多个主系统。

您可以使用 IBM Security Key Lifecycle Manager 复制程序来安排自动备份操作。 必须仅配置主服务器的属性以定期备份数据。

主配置文件样本

```
replication.role=master
replication.auditLogName=replication.log
replication.MaxLogFileSize=1000
replication.MaxBackupNum=10
replication.MaxLogFileNum=5
replication.BackupDestDir=C\:\\IBM\WebSphere\\AppServer\\products\\sklm\\restore
backup.ClientIP1=myhost1
backup.ClientPort1=2222
backup.EncryptionPassword=password
backup.ReleaseKeysOnSuccessfulBackup=false
backup.CheckFrequency=60
backup.TLSCertAlias=ssl_cert
replication.MasterListenPort=1111
```

- *主控*是缺省的复制角色。 对其进行指定以避免混淆。
- 用 **backup.ClientIPn** 和 **backup.ClientPortn** 参数至少指定一个克隆系统。
- 请确保指定的端口可用，并且当前没有 IBM Security Key Lifecycle Manager 或其他进程在使用该端口。
- 最多可以指定 20 个克隆系统。
- **backup.TLSCertAlias** 参数必须指定主控系统及所有克隆系统中存在的证书。
- 指定加密和解密备份的密码。 当 IBM Security Key Lifecycle Manager 对该密码进行首次读取之后，其在复制配置文件中会成为隐式密码。

克隆配置文件样本

```
replication.role=clone
replication.MasterListenPort=1111
replication.BackupDestDir=C\:\\IBM\WebSphere\\AppServer\\products\\sklm\\restore
replication.MaxLogFileSize=1000
replication.MaxBackupNum=3
replication.MaxLogFileNum=4
restore.ListenPort=2222
```

- 在克隆系统上，指定参数值 replication.role=clone。

- **restore.ListenPort** 参数必须指定在主系统上的 **backup.ClientIPn** 参数中指定的端口号。

有关所有可用复制配置参数的完整详细信息，请参阅 IBM Security Key Lifecycle Manager 文档中的“参考信息”部分。

服务器间通信

传输层安全性 (TLS) 协议用于主系统和克隆系统之间的安全通信。

在主系统及其所有克隆系统的 IBM Security Key Lifecycle Manager 密钥库中必须有可用的现有专用密钥。 必须在 ReplicationSKLMConfig.properties 配置文件的 **backup.TLSCertAlias** 参数中，设置主系统上此密钥的别名。 如果主系统和克隆系统上的密钥不同，那么将无法启动系统间的通信以运行复制任务。 您可以使用图形用户界面、命令行界面或 REST 界面，更改复制配置文件的属性。

复制调度

配置 ReplicationSKLMConfig.properties 文件的属性，以安排 IBM Security Key Lifecycle Manager 自动化复制过程。

使用图形用户界面、命令行界面或 REST 界面，配置复制配置文件的属性以安排复制过程。 仅当在主系统中添加新密钥时才会执行已计划的复制。 还可使用 IBM Security Key Lifecycle Manager 复制程序来安排自动备份操作。 必须仅配置主服务器的属性以定期备份数据。

您可以配置调度，以便让 IBM Security Key Lifecycle Manager 检查是否需要进行定期复制以及是否在更改后启动此过程。 若有需要，您还可以指定运行复制的时间。 配置 **backup.CheckFrequency** 参数来指定 IBM Security Key Lifecycle Manager 检查主系统是否有更新的频率。 执行更新时会引起复制。 该值以小时计，缺省值为 1 小时。

要指定时间，请配置 **backup.DailyStartReplicationBackupTime** 参数。您必须以 24 小时的格式 (HH:MM) 来指定时间。 自上一次复制以来，当主系统进行修改时，会执行复制。

在缺省情况下，一旦克隆系统接收到来自主系统的备份即会还原备份。 要指定还原时间，请在克隆系统的复制配置文件中添加 **restore.DailyStartReplicationRestoreTime** 参数。 您必须以 24 小时的格式 (HH:MM) 来指定时间。

您可以使用“复制”页面来强制对所有已定义的克隆系统进行临时复制或特定复制。或者，可使用以下 CLI 命令或 REST 界面:

- **tklmReplicationNow**
- **Replication Now REST Service**

复制审计记录

IBM Security Key Lifecycle Manager 复制会将审计信息记录到 IBM Security Key Lifecycle Manager 审计日志文件中。

IBM Security Key Lifecycle Manager 复制程序提供了一种功能，它可以将特定于复制的审计记录写入其独立的审计日志文件。 复制审计日志记录与复制过程相关的所有操作。 缺省情况下，复制审计日志文件的位置是 *<SKLM_HOME>*\logs\replication\replication_audit.log。

使用图形用户界面、命令行界面或 REST 界面，在 ReplicationSKLMConfig.properties 文件中设置审计属性。在配置文件中，可以配置审计属性，例如，审计日志文件位置、日志文件名、日志文件大小、要保留的最大日志文件数或要保留的最大备份文件数。

设置复制过程

必须在 IBM Security Key Lifecycle Manager 中设置一个可进行复制过程的基本环境。

关于此任务

本主题描述如何通过使用 IBM Security Key Lifecycle Manager 命令行界面命令和 REST 界面设置复制过程以进行复制。 有关使用图形用户界面进行复制设置的信息，请参阅克隆服务器和主服务器的复制设置。

过程

1. 设置 IBM Security Key Lifecycle Manager 主系统。
2. 添加密钥和设备，以便准备好提供所需的密钥。
3. 指定 SSLSERVER 证书用于复制。 可以使用 GUI、CLI 命令或 REST 界面创建此证书，如下例中所示:

   图形用户界面

   a. 登录图形用户界面。

   b. 单击**高级配置 > 服务器证书**.

   命令行界面

   在一行上输入 **tklmCertCreate** 命令。例如，要创建自签名证书，请输入:

   ```
   print AdminTask.tklmCertCreate('[('[-type selfsigned -alias
   sklmSSLCertificate -cn sklmssl -ou accounting -o myCompanyName
   -country US -keyStoreName defaultKeyStore -usage SSLSERVER
   -validity 999]')
   ```

   REST 界面

   要创建自签名证书，可以使用“**证书生成请求 REST 服务**”。 请使用 REST 客户机发出以下 HTTP 请求:

   ```
   POST https://localhost:9080/SKLM/rest/v1/certificates
   Content-Type: application/json
   Accept: application/json
   Authorization: SKLMAuth authId=139aeh34567m
   Accept-Language : en
   {"type":"selfsigned","alias":"sklmCertificate","cn":"sklm","ou":"sales",
   "o":"myCompanyName","usage":"3592","country":"US","validity":"999", "
   algorithm ": " RSA "  }
   ```

4. 创建主 IBM Security Key Lifecycle Manager 的备份，如下例中所示:

   图形用户界面

   a. 登录图形用户界面。

   b. 单击**备份和恢复**。

命令行界面

输入 **tklmBackupRun** 命令:

```
print AdminTask.tklmBackupRun
('[-backupDirectory C:\\wasbak1\\sklmbackup1 -password myBackupPwd]')
```

REST 界面

要创建备份，请使用“**备份运行 REST 服务**”。请使用 REST 客户机发出以下 HTTP 请求:

```
POST https://localhost:9080/SKLM/rest/v1/ckms/backups
Content-Type: application/json
Accept: application/json
Authorization: SKLMAuth authId=139aeh34567m
Accept-Language : en
{"backupDirectory":"/sklmbackup1","password":"myBackupPwd"}
```

5. 将步骤 2 中创建的备份复制到 IBM Security Key Lifecycle Manager 的每个克隆系统中。 将此备份复原到每个系统中，如以下示例中所示:

图形用户界面

a. 登录图形用户界面。

b. 单击**备份和恢复**。

命令行界面

在一行中输入 **tklmBackupRestoreRun** 命令:

```
print AdminTask.tklmBackupRunRestore
('[-backupFilePath /opt/sklmbackup/sklm_v2.5_20081012074433_backup.jar
  -password myBackupPwd]')
```

REST 界面

要复原备份，可以使用“**备份运行 REST 服务**”。 请使用 REST 客户机发出以下 HTTP 请求:

```
POST https://localhost:9080/SKLM/rest/v1/ckms/restore
Content-Type: application/json
Accept: application/json
Authorization: SKLMAuth authId=139aeh34567m
Accept-Language : en
{"backupFilePath":"/sklmbackup","password":"myBackupPwd"}
```

6. 在主系统中创建 ReplicationSKLMConfig.properties 复制配置文件。 此配置文件必须是文本文件，并且必须将它放在与 IBM Security Key Lifecycle Manager 属性文件所在的目录相同的目录中，例如 C:\Program Files (x86)\IBM\WebSphere\AppServer\products\sklm\config\ReplicationSKLMConfig.properties。

如下示例显示了要允许启动复制任务，主控中所需的字段。 必须执行以下步骤:

- 将角色设置为主控。
- 确定第一个步骤中的证书，并至少提供一个克隆服务器及端口号。
- 定义主侦听端口并选择密码。

```
backup.EncryptionPassword=mypassword
backup.TLSCertAlias=sklmSSLCertificate
backup.ClientIP1=myhostname
backup.ClientPort1=2222
replication.MasterListenPort=1111
```

backup.EncryptionPassword 属性可以包含字符、数字或特殊字符。 当首次运行复制时，该产品将隐藏该属性。 **backup.TLSCertAlias** 属性将指定证书的别名以及在第一个步骤中创建的用于和克隆系统进行通信的专用密钥。

replication.MasterListenPort 属性指定主系统用于侦听克隆系统的某些响应的端口。 **backup.ClientIP1** 和 **backup.ClientPort1** 属性将对克隆系统进行定义。 **backup.ClientIP1** 属性可以是主机名，也可以是 IP 地址。 **backup.ClientPort1** 属性将指定客户机将要侦听的端口。 要定义其他克隆系统，必须指定 **backup.ClientIP*** 和 **backup.ClientPort*** 属性，其中“*”是 2 至 5 之间的一个数字，与您首次设置的值一样。

7. 在克隆系统中创建 ReplicationSKLMConfig.properties 复制配置文件。 此配置文件必须是文本文件，并且必须将它放在与 IBM Security Key Lifecycle Manager 属性文件所在的目录相同的目录中，例如 C:\Program Files (x86)\IBM\WebSphere\AppServer\products\sklm\config\ReplicationSKLMConfig.properties。

   如下示例显示了要允许启动复制任务，克隆系统中所需的字段。 必须执行以下步骤:

   - 将角色设置为克隆。
   - 定义主侦听端口。
   - 定义还原侦听端口。 端口必须与主系统上相应的 **backup.ClientIP*** 参数中编码的端口号相同。

   ```
   replication.role=clone
   backup.TLSCertAlias=sklmSSLCertificate
   replication.MasterListenPort=1111
   restore.ListenPort=2222
   ```

   克隆系统需要 **replication.role** 属性。 在缺省情况下，此属性的值为主控。 **backup.TLSCertAlias** 属性必须设置为第一个步骤中所创建的证书，这与主系统上的一样。当复制被延迟，或者还原过程所花时间比主系统等待响应的时间长时，此属性将用于发送克隆系统的状态。

   当复制被延迟，或者还原过程所花时间比主系统等待响应的时间长时，**replication.MasterListenPort** 属性将指定发送状态的端口。 最后一个属性 **restore.ListenPort** 是克隆系统用于侦听来自主系统的复制请求的端口。

8. 在主系统和克隆系统中重新启动 IBM Security Key Lifecycle Manager。 可以在克隆系统和主系统上查看以下消息: 使用 **tklmReplicationStatus** CLI 命令确保正在运行复制任务。 可以在主系统和克隆系统上查看以下消息:

   命令行界面

   可以使用以下 CLI 命令确保正在运行复制任务:

   ```
   print AdminTask.tklmReplicationStatus()
   ```

   主系统

   ```
   1.CTGKM2215I The Security Key Lifecycle Manager Replication
   task is UP. Role set to: MASTER
   CTGKM2218I The last completed replication took place at
   Thu Jun 19 14:50:59 WST 2015
   CTGKM2217I The next scheduled replication is due at
   Fri Jun 20 17:03:36 WST 2015
   ```

   克隆系统

   ```
   CTGKM2215I The SKLM Replication task is UP. Role set to: CLONE
   CTGKM2220I No previous successful replications.
   CTGKM2221I No replication currently scheduled.
   ```

REST 界面

使用“**复制状态 REST 服务**”确保正在运行复制任务。 请使用 REST 客户机发出以下 HTTP 请求:

```
GET https://localhost:9080/SKLM/rest/v1/replicate/status
Content-Type: application/json
Accept: application/json
Authorization: SKLMAuth authId=139aeh34567m
```

主系统

```
Status Code : 200 OK
Content-Language: en
[
  { code:"CTGKM2215I", "status":"CTGKM2215I The Security Key
Lifecycle Manager  Replication task is UP. Role set to: MASTER"},
  {code:"CTGKM2218I", "status":"CTGKM2218I The last completed
replication took place at Thu Jun 19 14:50:59 WST 2015."} ,
  {code:"CTGKM2217I", "status":"CTGKM2217I The next scheduled
replication is due at Fri Jun 20 17:03:36 WST 2015." }

]
```

克隆系统

```
Status Code : 200 OK
[
  {code:"CTGKM2215I", "status":"CTGKM2215I The Security Key
Lifecycle Manager  Replication task is UP. Role set to: CLONE"}
, { code:"CTGKM2220I", "status":"CTGKM2220I No previous
   successful replications."} ,
  { code:"CTGKM2217I", "status":"CTGKM2221I No replication
   currently scheduled." }

]
```

9. 现在已经设置了复制，并且复制将每隔 60 分钟检查一次是否有修改。 你可以更改此时间间隔，为复制设置一个每天固定的时间来检查是否有修改。 也可以使用 **tklmReplicationNow** CLI 命令或“**立即复制 REST 服务**”来立即运行复制任务。

复制问题和解决方法

当运行 IBM Security Key Lifecycle Manager 复制任务时，必须考虑到在克隆系统和主系统上可能出现的问题。

不完整的复制

- 请确保在 **backup.TLSCertAlias** 参数中指定的 SSL 证书和专用密钥在主服务器和克隆服务器中均可用。
- 请确保其他软件产品当前没有使用为复制通信指定的端口号。
- 检查复制配置文件中指定的服务器名称或 IP 地址是否正确，并且是否可以从主服务器获取。
- 通过运行 **tklmReplicationStatus** 命令或**复制状态 REST 服务**，检查每个服务器上的复制任务是否都已启动，或检查 IBM Security Key Lifecycle Manager 欢迎页面上**复制**部分上的状态。
- 对于 DB2 复制，请确保主服务器和克隆服务器的日期/时间是几乎同步的。 巨大的差异会导致还原失败。
- 检查复制配置文件，确保定义了最少的必需参数，并且没有拼写错误。
- 最多可定义一台主服务器和 10 台相关联的克隆服务器。 至少必须定义一台克隆服务器。

- 检查复制审计文件以获取更多有关复制失败的信息。

在调度的时间未执行复制

- 仅当创建**新的**密钥材料时执行已计划的复制。
- 当在主复制配置文件中设置特定的复制时间和检查时间间隔时，特定的复制时间将覆盖检查时间间隔。

克隆系统复制

- 复制后，克隆系统将会重新启动。
- 维护克隆服务器的可用性。 您可以用 **restore.DailyStartReplicationRestoreTime** 参数指定一个特定的时间来完成复制。例如，无论何时收到备份文件，仅在晚上 11 点运行还原。对配置文件中的以下属性进行编码:

  ```
  restore.DailyStartReplicationRestoreTime=23:00
  ```

场景: 设置 IBM Security Key Lifecycle Manager 服务器与客户机设备之间的 SSL 握手

SSL 握手支持 IBM Security Key Lifecycle Manager 服务器设备和客户机设备建立连接以进行安全通信。 IBM Security Key Lifecycle Manager 提供了服务器配置向导，为 SSL 握手配置服务器和客户机设备。

必须完成向导中的以下步骤以进行 SSL/TLS 握手:

1. 创建自签名 SSL/KMIP 服务器证书。
2. 将步骤 1 中创建的 SSL/KMIP 服务器证书以编码格式导出到证书文件，以供客户机设备使用。还可导出现有证书。
3. 将客户机通信证书导入到 IBM Security Key Lifecycle Manager 服务器。

创建自签名 SSL/KMIP 服务器证书

作为第一项活动，可以创建 SSL/KMIP 服务器证书以用于 IBM Security Key Lifecycle Manager。

过程

1. 登录图形用户界面。
2. 单击**查看配置参数和/或创建 SSL 服务器证书**链接。

   在安装 IBM Security Key Lifecycle Manager 之后，**查看配置参数和/或创建 SSL 服务器证书**链接将立即是唯一可用来配置 IBM Security Key Lifecycle Manager 以便与客户机设备进行 SSL/TLS 握手的选项。如果先前创建了 SSL 服务器证书，那么此链接不可见。
3. 或者，在“欢迎”页面上，单击**配置 > SSL/KMIP > 启动服务器配置向导**。
4. 单击**创建 SSL/KMIP 服务器证书**。
5. 在“添加 SSL/KMIP 证书”对话框中，选择**创建自签名证书**。
6. 根据需要指定参数的值。
7. 单击**创建证书**。

下一步做什么

您可能需要将创建的 IBM Security Key Lifecycle Manager SSL/KMIP 服务器证书以编码格式导出到文件，以供客户机设备使用。单击**导出证书**链接或单击**导出 SSL/KMIP 服务器证书**选项卡。您还可以通过选择**使用现有证书**导出现有的 SSL/KMIP 服务器证书。请参阅『导出服务器证书』。

导出服务器证书

必需将 IBM Security Key Lifecycle Manager SSL/KMIP 服务器证书以编码格式导出到文件，以供客户机设备使用。客户机设备导入此证书，以与服务器进行安全通信。

过程

1. 登录图形用户界面。
2. 在“欢迎”页面上，单击**配置 > SSL/KMIP > 启动服务器配置向导**。
3. 要创建自签名证书，请单击**创建 SSL/KMIP 服务器证书**。 请参阅第 17 页的『创建自签名 SSL/KMIP 服务器证书』主题，以获取更多信息。
4. 单击**导出 SSL/KMIP 服务器证书**。
5. 在“导出证书”对话框，根据需要指定参数的值。例如，可以指定 **BASE64** 或 **DER** 作为证书文件格式。

   注: 如果未指定路径，那么证书将导出到 IBM Security Key Lifecycle Manager 的缺省安装位置。
6. 单击**导出证书**。

下一步做什么

您可以转到下一个步骤以导入客户机设备通信证书，以便在 IBM Security Key Lifecycle Manager 服务器与客户机设备之间进行安全通信。单击**转至下一步**链接或选择**导入 SSL/KMIP 服务器证书**。请参阅『导入客户机通信证书』。

导入客户机通信证书

必须将通信证书导入到 IBM Security Key Lifecycle Manager 服务器，才能与客户机设备进行安全通信。

过程

1. 登录图形用户界面。
2. 在“欢迎”页面上，单击**配置 > SSL/KMIP > 启动服务器配置向导**。
3. 要创建自签名证书，请单击**创建 SSL/KMIP 服务器证书**。 请参阅第 17 页的『创建自签名 SSL/KMIP 服务器证书』主题，以获取更多信息。
4. 单击**导出 SSL/KMIP 服务器证书**以将 IBM Security Key Lifecycle Manager SSL/KMIP 服务器证书以编码格式导出到文件，以供客户机设备使用。请参阅『导出服务器证书』，以获取更多信息。
5. 单击**导入 SSL/KMIP 客户机证书**。
6. 在“导入证书”对话框，根据需要指定参数的值。
7. 单击**导入**。

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。 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。

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。Web 上的“版权和商标信息”(www.ibm.com/legal/copytrade.shtml) 提供了 IBM 商标的最新列表。

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

I

S

T