规划

IBM

目录

规划

规划是一种活动，在规划中作出的决定会影响到一个或多个后续活动。

规划活动包括一些任务，如选择适当的密钥大小和数据库、预测现有数据是否需要迁移以及确定站点需要的现行常规做法。

站点需求

在安装 IBM Security Key Lifecycle Manager 之前，请考虑站点问题，例如密钥大小的需求，或者是使用 IBM Security Key Lifecycle Manager 提供的 DB2®，还是使用已安装在系统中的现有副本。 可能还需要考虑 Encryption Key Manager 的迁移需求。

密钥大小需求

安装和配置 IBM Security Key Lifecycle Manager 之前，必须考虑密钥大小需求。

受支持的密钥大小和导入及导出限制

IBM Security Key Lifecycle Manager 可为设备提供 2048 或 1024 位的密钥。 可继续使用生成为 1024 位密钥的较旧密钥。

表 1 列出了 IBM Security Key Lifecycle Manager 支持的密钥大小。

表 1. 受支持的密钥大小

导入 PKCS#12 文件	导出 PKCS#12 文件	密钥生成大小（以位为单位）
是	是	2048

DB2 规划

您必须考虑是使用 DB2 工作组服务器版 的现有副本，还是使用 IBM Security Key Lifecycle Manager 安装程序为分布式系统提供的 DB2 版本和修订包。 现有 DB2 必须本地安装在系统上，而不能安装在网络或共享驱动器上。

使用 IBM Security Key Lifecycle Manager 来管理 DB2。

- 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 V10.5.0.6 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。

有关数据库需求的更多信息，请参阅 IBM Security Key Lifecycle Manager 的 IBM Knowledge Center 上的“安装和配置”部分。

迁移规划

安装此版本的 IBM Security Key Lifecycle Manager 之前，请确定是迁移先前版本的 IBM Security Key Lifecycle Manager，还是迁移适用于 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 组件仅支持英语语言环境。 因此，必须在英语语言环境中进行从 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 的迁移失败，会保留成功迁移步骤的记录。 运行迁移恢复脚本时将从迁移过程中发生错误的位置开始。

  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 的迁移失败，会保留成功迁移步骤的记录。 运行迁移恢复脚本时将从迁移过程中发生错误的位置开始。
- IBM Security Key Lifecycle Manager V2 FP4 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 的迁移失败，会保留成功迁移步骤的记录。 运行迁移恢复脚本时将从迁移过程中发生错误的位置开始。

- IBM Security Key Lifecycle Manager V1 FP3 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 的迁移失败，会保留成功迁移步骤的记录。 运行迁移恢复脚本时将从迁移过程中发生错误的位置开始。

- Encryption Key Manager V2.1

  已为 V2.1 启用迁移，但对于早于 V2.1 的版本 Encryption Key Manager 没有启用。迁移配置的唯一机会是在 IBM Security Key Lifecycle Manager 安装过程中，或者是在安装结束后且更改 IBM Security Key Lifecycle Manager 配置之前。

  如果 Encryption Key Manager V2.1 迁移失败，那么不会有任何数据迁移到 IBM Security Key Lifecycle Manager 数据库。将撤销任何已作出的更改。

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 Linux 或 AIX 等系统上运行 **migrate.sh** 之前，请确保您已以 root 用户身份登录。
- 运行 *SKLM_HOME*\migration 目录中的 **migrateToSKLM.bat** 或 **migrateToSKLM.sh** 以将 IBM Security Key Lifecycle Manager 较低版本迁移至 V2.6。 在 Linux 或 AIX 等系统上运行 **migrateToSKLM.sh** 之前，请确保您已以 root 用户身份登录。

不要运行可能在此目录中看到过的其他 ***.bat** 实用程序。 这些实用程序仅供自动安装过程使用。

用于加密数据的证书需求

IBM Security Key Lifecycle Manager 需要至少一个包含了公用/专用密钥对的 X.509 数字证书，从而保护当数据在 3592 磁带机和 DS8000 Turbo 磁带机上加密时 IBM Security Key Lifecycle Manager 服务器创建的数据加密密钥。

IBM Security Key Lifecycle Manager 允许为每个写请求定义两个数字证书别名。创建磁带或磁盘时，指定的两个别名（标签）中有一个必须在 IBM Security Key Lifecycle Manager 密钥库数据库中具有专用密钥。 此密钥使创建者可以读取磁带或磁盘。 其他别名（标签 ）可以是来自合作伙伴的公用密钥，该合作伙伴可以使用其专用密钥对该公用密钥进行解密。 要读取已加密的磁带或磁盘，需要正确的专用密钥。

有两种方法可设置数字证书:

- 创建自己的公用/专用密钥对和对应的证书，用于对稍后可以读取和解密的磁带或磁盘进行写入和加密操作。
- 获取来自合作伙伴的公用密钥和对应的证书，用于对可以由合作伙伴读取并解密的磁带或磁盘进行写入和加密操作。

与其他组织共享磁带

可以出于数据传输、联合开发、合同服务或其他目的与其他组织共享磁带。 对于 3592 磁带机和 LTO 磁带机，用于共享加密磁带的方法有所不同。

如果要将密钥移动到自己的灾难恢复位置，请使用密钥库数据库。 如果要将密钥移动到业务合作伙伴，请提供业务合作伙伴的公用密钥。

通过检查此类证书的信任链并追溯到最终签署该证书的认证中心 (CA)，验证从业务合作伙伴处接收到的任何证书的有效性。 如果信任该 CA，那么可以信任该证书。 或者，也可以在证书传输期间受到安全保护时验证证书的有效性。 如果未能使用上述方法的其中一种来验证证书的有效性，那么将为“中间人”攻击提供机会。

3592 磁带共享

IBM Security Key Lifecycle Manager 可以在 3592 磁带上存储两组打包的加密密钥。此实践允许其他组织可以读取特定的磁带，而无需提供任何共享的秘密信息，也不会降低证书和密钥的安全性。

使用另一个别名（或密钥标签），向 IBM Security Key Lifecycle Manager 密钥库数据库添加其他组织的公用/专用证书的公用部分和密钥。 写入磁带时，加密密钥会存储在磁带上，它受两组公用/专用密钥的保护，一组是您自己的密钥，而另一组属于其他组织。 其他组织必须具有支持加密的 3592 磁带机。 其他组织可使用其 IBM Security Key Lifecycle Manager 及其专用密钥来对允许读取特定磁带的数据密钥进行解包。

IBM Security Key Lifecycle Manager 必须具有合作伙伴组织的证书。 其他组织必须拥有由其他组织运行的 IBM Security Key Lifecycle Manager 使用的密码库中关联的专用密钥。 这种灵活性使提供的磁带可供两个组织读取。 如果要利用此功能，那么必须向您的密钥库数据库中添加其他组织的证书（其中包含公用密钥）。

LTO 磁带共享

要在 LTO 磁带上共享已加密的密钥，其他组织必须可以使用用于加密磁带上的数据的对称密钥副本。 此密钥使他们可以读取磁带。 要共享对称密钥，其他组织必须与您共享其公用密钥。

此公用密钥用于在将对称密钥从 IBM Security Key Lifecycle Manager 密钥库导出时，将对称密钥进行打包。当其他组织将对称密钥导入其 IBM Security Key Lifecycle Manager 密钥库时，将使用对应的专用密钥对该对称密钥进行解包。

此实践确保对称密钥在传输中的安全性，因为只有专用密钥的持有者才能对对称密钥进行解包。 只有使用用于加密 IBM Security Key Lifecycle Manager 密钥库中的数据的对称密钥，其他组织才能读取磁带上的数据。

建议站点实践

规划加密密钥服务器（比如 IBM Security Key Lifecycle Manager）必须考虑站点实践，从第一次实施到建立到行之有效的实践。

表 2 是站点可能要考虑的最佳实践的列表。

表 2. 建议站点实践

主题	建议实践
自签名证书	将自签名证书用于公司内的内部生产和测试用途。
CA 颁发的证书	对于生产环境，请使用 CA 颁发的证书。
证书替换频率	每季度替换一次用于创建新磁带盒的证书。

表 2. 建议站点实践 (续)

主题	建议实践
CA 颁发的最小证书数	最少颁发一个证书，并且假设该证书同时用作缺省证书和合作伙伴证书。
测试和生产环境中磁带机的一般数量	数量范围从几台设备到几百台，设备的中等数量在 100 多台范围内。
远程站点	存在一个或多个远程站点，并且 IBM Security Key Lifecycle Manager 为远程站点提供密钥。
每年发生的泄密证书数	零个证书泄密。
强制故障转移需求	许多站点要求备份加密密钥服务器必须始终在另一个站点上运行。 只要数据发生更改，主站点就会对密钥资料进行备份。 此外，在发生故障转移时，备份的数据能可靠地恢复到非现场副本 IBM Security Key Lifecycle Manager 服务器以供使用。
选择性加密或加密所有数据	必须考虑是选择性加密，还是加密除密钥库数据库以外的所有数据，并且要考虑可能出现的恢复问题。 大部分站点会加密所有除了IBM Security Key Lifecycle Manager 数据及其备份数据之外的所有数据。
备份文件	要获取更多信息，请参阅有关备份和恢复的管理主题。

自签名证书

您必须考虑如何平衡自签名证书的可用性与企业的安全性需求。

确定组织对使用自签名证书以及由认证中心 (CA) 颁发的证书的策略。 可能需要创建自签名证书以用于项目的测试阶段。您可能还要提前向认证中心请求用于生产阶段的证书。

敏感信息的安全性

必须确保只有授权人员才能访问 IBM Security Key Lifecycle Manager 数据库中 IBM Security Key Lifecycle Manager 密钥材料的敏感信息。

站点在职责划分方面各不相同，并且可能没有职责划分。 但是，为了提高安全性，站点可以执行以下步骤:

- 一个人为 IBM Security Key Lifecycle Manager 服务器 提供运行时系统管理员支持。站点具有可运行 IBM Security Key Lifecycle Manager 服务器的系统管理员。
- 另外一个人充当数据库管理员，对 IBM Security Key Lifecycle Manager 所使用的 DB2 用户标识和数据库实例具有受限的访问权。

安全配置

必须最大限度地提供环境、安装、管理和操作中的安全性，以便确保只有授权人员可以访问 IBM Security Key Lifecycle Manager 的敏感信息。

环境

可以配置这些环境元素以实现最高安全性:

- 限制对系统的物理访问，以阻止对服务器硬件的未经授权的访问，从而仅允许授权管理员有权访问系统控制台。
- 确保通信网络安全，防止窃听和电子欺骗。
- 使用防火墙并保持所有端口位于防火墙后面。 仅打开 IBM Security Key Lifecycle Manager 需要的端口。
- 指定文件系统控件以保护 IBM Security Key Lifecycle Manager 系统上的敏感文件。控件必须保护文件的安全，并且必须将访问权限制为只有需要访问的用户才能访问。
- 保护密钥服务器、配置文件、日志文件、审计日志文件、数据库实例和 IBM Security Key Lifecycle Manager 备份文件的安全。
- 确保系统有足够的磁盘空间来存储审计日志。
- 如果在 IBM Security Key Lifecycle Manager 上使用任何一种调试实用程序，那么必须确保输出是安全的。 仅从安全的系统（您了解其中所有已安装的应用程序）访问 IBM Security Key Lifecycle Manager。
- 虽然 IBM Security Key Lifecycle Manager 备份 JAR 文件由密码保护，但是不是 JAR 文件的所有内容都由密码保护，这使该文件容易孙华或故意被破坏。 请保持 JAR 文件的安全。
- 不要编辑包含在备份 JAR 文件中的文件。否则这些文件将变得不可读。 将备份文件保留在由您控制密码的安全位置。 将备份文件的副本保留在 IBM Security Key Lifecycle Manager 计算机和 IBM Security Key Lifecycle Manager 目录路径之外的安全位置。
- 当使用浏览器管理 IBM Security Key Lifecycle Manager 时，通过使用某些 IBM Security Key Lifecycle Manager 面板，可以浏览服务器系统上的目录布局。 IBM Security Key Lifecycle Manager 是以 root 用户身份运行的产品，浏览文件系统时，将使用这些 root 用户许可权。

安装

- 不要安装在域控制器上。
- 不要安装在共享文件系统上。

管理和用户假设

安全地管理管理员:

- 请将管理员权限仅授予那些管理 IBM Security Key Lifecycle Manager、满足站点对于在维护 IBM Security Key Lifecycle Manager 安全性方面可信且称职的人员。
- 管理员必须根据系统文档和 IBM Security Key Lifecycle Manager 文档提供的指导信息进行工作。
- `SKLMAdmin` 是特权用户，对 IBM Security Key Lifecycle Manager 具有无限制的访问权。 只有在获得特权时才能以 `SKLMAdmin` 的身份登录。
- WebSphere Application Server 管理员是特权用户，具有创建用户帐户和授予对 IBM Security Key Lifecycle Manager 的访问权的访问权。 仅为已授权的人员提供 `WASAdmin` 用户标识和密码。
- 系统上的用户标识仅授予有权使用系统上信息的用户。
- 确保对 IBM Security Key Lifecycle Manager 具有访问权的用户怀有合作精神，而没有恶意。

- 不要将操作系统特权授予诸如 LTOAuditor 之类的管理员，他们无需启动或停止 IBM Security Key Lifecycle Manager 服务器。

操作

安全地管理正在进行的操作:

- 启用建议的密码策略。
- 根据密码策略选择并管理用户和管理员密码。
- 启用审计。
- 针对系统安全操作确定和实施必要过程。
- 确保维护过程包括对系统定期进行诊断和审计，包括定期备份以及复查审计文件和错误日志。
- 将密码安全地传输给系统用户。
- 指示用户和管理员不要泄露他们的密码。
- 没有锁定机制用于重复输入错误密码的用户。
- 像保护管理员密码本身那样来严格保护配置文件以防止泄密，包括配置文件内容的所有表现形式，例如打印输出和备份。

配置属性

表 3 描述了一组用于最高安全性设置的配置属性。 使用安全的方法配置属性，但是无需设置用于最高安全性。 提供的以下示例可帮助您了解这些决策。

表 3. 安全配置属性设置

属性	最安全的建议
Audit.event.outcome	指定成功和失败事件数。
Audit.eventQueue.max	设置为值 0。
Audit.event.types	指定除值 none 以外的所有值。
Audit.handler.file.multithreads	对安全性无影响。
Audit.handler.file.name	为文件指定一个有效、安全的位置。
Audit.handler.file.size	对安全性无影响。
Audit.handler.file.threadlifespan	对安全性无影响。
backup.keycert.before.serving	设置为值 true。
cert.valiDATE	设置为值 true。
config.keystore.name	不要更改此值。
config.keystore.ssl.certalias	使用图形用户界面或命令行界面设置协议有效值。
调试（debug）	启用调试记录可能会影响 IBM Security Key Lifecycle Manager 性能。只有在 IBM 支持代表的指导下，才应启用此选项。
device.AutoPendingAutoDiscovery（IBM Security Key Lifecycle Manager 数据库中的一个属性）	设置为值 0（零或手动）或 2（自动暂挂）。
enableClientCertPush	设置为值 false。
enableMachineAffinity（IBM Security Key Lifecycle Manager 数据库中的一个属性）	设置为值 true（已启用）。
fips	设置为值 true（已启用）。

表 3. 安全配置属性设置 (续)

属性	最安全的建议
KMIPListener.ssl.port	设置为有效端口号。
lock.timeout	使用缺省值。
maxPendingClientCerts	使用缺省值。
pcache.refresh.interval	使用缺省值。
tklm.backup.db2.dir	指定一个有效、安全的目录。
tklm.backup.dir	指定一个有效、安全的目录。
tklm.encryption.keysize	使用缺省值。
tklm.encryption.password	此属性供内部使用。不要更改其值。
tklm.encryption.pbe.algorithm	此属性供内部使用。 不要更改其值。
TransportListener.tcp.port	指定有效的端口号。
TransportListener.tcp.timeout	指定有效的超时时间间隔。
TransportListener.ssl.ciphersuites	使用缺省值。
TransportListener.ssl.clientauthentication	指定设备支持的最高值。
TransportListener.ssl.port *	指定有效的端口号。
TransportListener.ssl.protocols	制定值 SSL_TLSv2。
TransportListener.ssl.timeout	指定有效的超时时间间隔。
Transport.ssl.vulnerableciphers.patterns	使用缺省值。
stopRoundRobinKeyGrps	指定值 true，但在某些环境中，false 也可能可以接受。 要获取更多注意事项，请参阅有关 **stopRoundRobinKeyGrps** 属性的参考主题。
useSKIDefaultLabels	对安全性无影响。
zOSCompatibility	对安全性无影响。

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

[数字]

A

B

C

D

E

F

K

L

M

P

S

T

U

Z