概述

目录

产品概述

产品概述主题描述 IBM Security Key Lifecycle Manager 产品（先前称为 IBM Tivoli Key Lifecycle Manager）及其业务和技术背景信息。

它们包含以下内容的相关信息:

- 产品功能部件和功能
- 产品所基于的技术和体系结构
- 作为产品功能部件底层的用户模型和角色
- 支持各种用户角色的图形界面和工具

本发行版中的新增内容

IBM Security Key Lifecycle Manager V2.6.0 提供多个易用性和互操作性改进以供安装、配置和监视 IBM Security Key Lifecycle Manager 基础结构和流程从而本地创建和管理 KMIP 对象的生命周期。

基于独立于操作系统的 UI 的复制配置

为自动复制配置提供图形用户界面。您可以配置复制程序以在将新密钥添加到主服务器时，跨克隆服务器复制 IBM Security Key Lifecycle Manager 关键数据。

自动复制过程支持以独立于操作系统和服务器目录结构的方式将 IBM Security Key Lifecycle Manager 环境克隆至多个服务器。例如，您可以将数据从 Windows 系统上的主服务器复制到 Linux 系统上的克隆服务器。您可以克隆 IBM Security Key Lifecycle Manager 主服务器，最多可达 20 个副本。 要获取更多信息，请参阅克隆服务器和主服务器的复制设置。

独立于操作系统的备份和复原操作

支持跨平台备份和复原功能以保护 IBM Security Key Lifecycle Manager 关键数据。 您可以创建跨平台兼容备份，并跨操作系统复原此备份。 例如，可在 Windows 系统上复原 Linux 系统上的备份，反之亦然。

您可以使用跨平台备份实用程序在早期版本的 IBM Security Key Lifecycle Manager 上运行备份操作来备份关键数据。 您可以在最新版本的 IBM Security Key Lifecycle Manager 上将这些备份文件复原至不同于从中备份这些文件的其他操作系统中。

您还可以配置 IBM Security Key Lifecycle Manager 来调度自动备份操作。 只能针对主服务器配置属性以定期备份数据。 要获取更多信息，请参阅备份和复原。

NSA Suite B 合规性

支持通过符合美国国家安全局 (NSA) Suite B 加密准则的安全套接字进行通信，从而提供增强的安全级别。要获取更多信息，请参阅第 10 页的『IBM Security Key Lifecycle Manager 中 NSA Suite B 加密合规性』。

通过图形用户界面来调试日志记录设置

通过使用图形用户界面来收集调试信息，以支持调试日志记录设置的配置。 调

试日志文件提供额外信息以对 IBM Security Key Lifecycle Manager 问题进行分析和故障诊断。要获取更多信息，请参阅指定调试信息的设置。

通过图形用户界面导出 SSL/KMIP 服务器证书的设置
使用图形用户界面支持以编码格式将 SSL/KMIP 服务器证书导出至文件。 导出的文件可加速部署证书，实现与服务器的安全通信。 要获取更多信息，请参阅导出 SSL/KMIP 服务器证书。

服务器配置向导，用于对 IBM Security Key Lifecycle Manager 进行 SSL/TLS 握手配置 包含“服务器配置向导”，以对 IBM Security Key Lifecycle Manager 服务器和客户机设备进行 SSL/TLS 握手配置。 SSL 握手支持服务器与客户机设备建立连接以实现安全通信。 向导提供了设置 SSL/TLS 握手流程的指导方法。 要获取更多信息，请参阅方案: 在 IBM Security Key Lifecycle Manager 服务器与客户机设备之间设置 SSL 握手。

符合 KIMP 1.2 和 Storage Networking Industry Association Secure Storage Industry Forum (SNIA-SSIF) 证书
符合 Key Management Interoperability Protocol (KMIP) 以及与存储行业有关的其他安全相关标准。

更快且更简单地配置符合 KMIP 的客户机以用于密钥管理操作
IBM Security Key Lifecycle Manager 提供图形用户界面以创建、配置和搜索加密对象。这些对象用于为符合 KMIP 的客户机设备提供加密密钥。有关 KMIP 对象管理的更多信息，请参阅KMIP 对象管理。

安装改进
对安装程序进行了对象改进，以在安装过程中通过执行环境验证和先决条件检查来提供更多用户反馈。

用于数据加密的 AES 256 位主密钥的自动生成
在成功安装 IBM Security Key Lifecycle Manager 之后，自动生成 AES 256 位主密钥用于数据加密。 要符合 PCI DSS 标准并提高数据安全性，请将长度为 256 位的主密钥用于加密 IBM Security Key Lifecycle Manager 敏感数据（如密钥材料）。

注:

- 从 IBM Security Key Lifecycle Manager V2.6 发行版起，不再支持 Solaris 操作系统。
- 不推荐在 IBM Security Key Lifecycle Manager 的未来版本中使用 IBM Security Key Lifecycle Manager 命令行界面命令。使用 REST 界面代替。
- 在 IBM Security Key Lifecycle Manager 的以后版本中不推荐使用图形用户界面、命令行界面和 REST 界面中对密钥和证书的**别名**属性的所有引用。

支持的语言

IBM Security Key Lifecycle Manager 支持各种语言。 用户界面标签、消息和值可显示为英文和非英文。 但是，IBM Security Key Lifecycle Manager 仅支持本地化为单一语言环境的系统。

IBM Security Key Lifecycle Manager 支持以下语言:

- 英语

- 法语
- 德语
- 意大利语
- 日语
- 韩国语
- 简体中文
- 西班牙语
- 繁体中文

功能概述

使用 IBM Security Key Lifecycle Manager 管理企业密钥和证书的生命周期。 您可以管理对称密钥、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) 来扩展对设备的支持，从而对已存储的数据进行加密并进行相应的密钥管理。

  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。这些对象用于为符合 KMIP 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。
- 与 IBM Security Key Lifecycle Manager 服务器连接的一个或多个设备的加密密钥。
- 将您生成的自签名证书的密钥材料、专用密钥以及密钥元数据存储在数据库中。
- 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（例如，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 早期 V1.0、V2.0、V2.0.1、V2.5 版本和 IBM Encryption Key Manager V2.1 上运行备份操作。 您可以在最新版本的 IBM Security Key Lifecycle Manager 上跨操作系统复原这些备份文件。
- 在安装期间迁移 IBM Security Key Lifecycle Manager 早期 V1.0、V2.0、V2.0.1、V2.5 版本和 IBM Encryption Key Manager V2.1 组件。
- 基于因成功操作和/或失败操作而发生的选定事件的审计记录。 安装或启动 IBM Security Key Lifecycle Manager 会将构建级别写入审计日志中。
- 支持能够加密的 3592 磁带机、LTO 磁带机、DS5000 存储服务器、DS8000 Turbo 磁带机 和其他设备。
- 支持使用硬件安全模块 (HSM) 存储用于保护数据库中存储的所有密码和密钥的主密钥。

- 一组用于自动复制操作系统中当前活动文件和数据的操作。 此复制支持以独立于操作系统和服务器目录结构的方式对多个服务器上的 IBM Security Key Lifecycle Manager 环境进行克隆。
- 支持将轻量级目录访问协议 (LDAP) 服务器用于用户认证。 您可以在任何 LDAP 存储库（例如，IBM Security Directory Server 或 Microsoft Active Directory）中配置 IBM Security Key Lifecycle Manager。
- 服务器配置向导，用于对 IBM Security Key Lifecycle Manager 进行 SSL/TLS 握手配置。 SSL 握手支持服务器与客户机设备建立连接以实现安全通信。

密钥提供

IBM Security Key Lifecycle Manager 能够定义并提供密钥。 IBM Security Key Lifecycle Manager 还能定义可与设备相关联的密钥或密钥组。 不同的设备需要不同的密钥类型。在配置设备后，IBM Security Key Lifecycle Manager 会将密钥部署到请求密钥的设备。

密钥组

一个 IBM Security Key Lifecycle Manager 密钥组包含多个密钥。 一个密钥仅可以是一个密钥组的成员。

在分布式系统上，删除密钥组*还会删除密钥组中的所有密钥*。

密钥元数据

IBM Security Key Lifecycle Manager 密钥中包含诸如密钥别名、算法和激活日期等信息。

元数据可能还包括密钥描述、截止日期、停用日期、销毁日期、泄密日期、密钥用途、备份时间和状态（例如，活动）。 IBM Security Key Lifecycle Manager 将密钥的元数据存储在 IBM Security Key Lifecycle Manager 数据库中。

密钥和证书状态

在生存期内，加密对象会经历一系列的状态转变，这些状态依赖于密钥或证书的存在时间长度以及数据是否受保护。 其他因素，例如密钥或证书是否遭到泄露也会影响加密对象的状态。

IBM Security Key Lifecycle Manager 可维护以下密码对象状态。

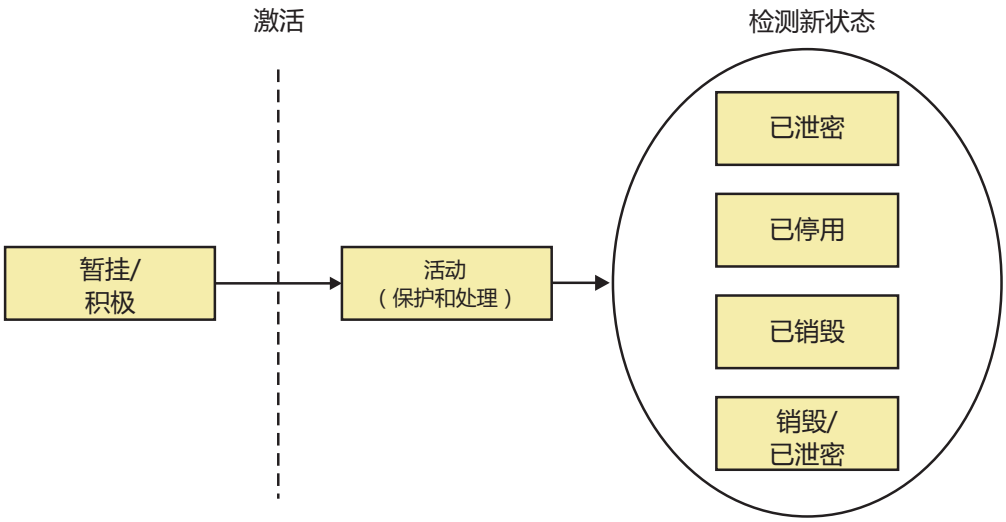

图 1. 密码对象状态

密钥或证书的状态定义了所允许的用途:

pending
证书请求条目正在暂挂由认证中心核准并认证的证书的返回。

pre-active
对象已存在，但是尚无法用于任何加密用途，例如具有未来使用时间戳记的已迁移证书。

active
对象正用于保护和处理数据，期间可能会使用 **Process Start Date** 和 **Protect Stop Date** 属性。 例如，保护包括加密和签名问题。 处理包括解密和签名验证。

compromised
由于某种原因怀疑对象的安全性。 已泄密对象绝不会返回至未泄密状态，并且无法用于保护数据。 该对象仅用于处理客户机中受密码保护的信息，可以依靠该客户机来处理已泄密加密对象。

IBM Security Key Lifecycle Manager 在泄密之前会保留对象的状态。 要处理先前保护的数据，可能要继续使用泄密对象。

deactivated
对象将不用于应用密码保护，例如加密或签名。 但是，如果发生特殊情况，可以通过特殊许可权该对象用于处理密码保护的信息。 例如，处理包括解密或验证。

destroyed
对象不可再用于任何用途。 此状态导致从产品中除去该对象。

destroyed-compromised
对象不可再用于任何用途。 此状态导致从产品中除去该对象。

不再活动的对象的状态可能会发生以下更改:

- 从已停用更改为已销毁。
- 从已停用更改为已泄密。
- 从已泄密更改为已销毁-泄密。

- 从已销毁到已销毁-泄密。

IBM Security Key Lifecycle Manager 密钥库

IBM Security Key Lifecycle Manager 可以存储对称密钥、公用密钥、专用密钥及其关联的证书链和受信任证书。

在 IBM Security Key Lifecycle Manager 生成新的密钥时，该密钥及其元数据存储在 IBM Security Key Lifecycle Manager 数据库中的密钥表中。通过使用主密钥保护密钥数据。在创建证书请求时，IBM Security Key Lifecycle Manager 将创建处于暂挂状态的密钥条目。

通过使用命令行界面可以更改密钥的信息属性。

支持加密的 3592 磁带机和 LTO 磁带机

IBM Security Key Lifecycle Manager 对支持加密的 3592 磁带机和 LTO 磁带机提供支持。 对于不支持加密的磁带机不提供支持。

IBM Security Key Lifecycle Manager 支持以下磁带机类型:

- 3592 磁带机

  TS1120 和 TS1130 磁带机支持数据加密。

- LTO 磁带机

  支持 LTO Ultrium 4 磁带机和 LTO Ultrium 5 磁带机对数据进行加密。

数据压缩后将在磁带机中以全线路速度执行加密。

有关 IBM Security Key Lifecycle Manager 支持的设备的信息，请参阅 http://pic.dhe.ibm.com/infocenter/prodguid/v1r0/clarity/softwareReqsForProduct.html 中的存储器硬件一节。

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**。
5. 在“软件产品兼容性报告”页面，单击 **硬件**。

企业存储: DS8000® 存储控制器（2107、242x）

IBM Security Key Lifecycle Manager 支持 DS8000 存储控制器 (IBM System Storage DS8000 Turbo 磁带机)。

此支持需要 DS8000 存储控制器上具有相应的微代码束版本，许可内码级别为 64.20.xxx.0 或更高级别。

IBM System Storage®: DS5000 存储控制器（1818-51A、1818-53A 和 1814-20A）

IBM Security Key Lifecycle Manager 支持 DS5000 存储服务器 (IBM System Storage DS5000)。

此支持适用于具有自加密光纤通道驱动器（FDE/SED 驱动器）的 DS5000 系列存储系统（DS5100、DS5300 和 DS5020）。另外还必须购买选件 Full-Disk Encryption Premium Feature 并在存储子系统中启用此选件。 系统中包含下列存储控制器:

- 1818-51A、1818-53A、FC 7358 DS5000 磁盘加密激活
- 1814-20A 和 FC 7410 DS5020 磁盘加密激活

请参阅 *IBM DS Storage Manager 10.70 Installation and Host Support Guide* 以获取如何设置 DS5000 存储子系统以支持 IBM Security Key Lifecycle Manager 的更多信息。

备份和恢复

IBM Security Key Lifecycle Manager 提供了跨平台备份和复原功能以保护 IBM Security Key Lifecycle Manager 的关键信息。 您可以创建跨平台兼容备份，并跨操作系统复原此备份。 例如，可在 Windows 系统上复原 Linux 系统上的备份，反之亦然。

使用 IBM Security Key Lifecycle Manager 可通过以下功能保护数据:

备份 备份是需要恢复副本以使用户恢复工作时使用的活动生产信息的辅助副本。 发生灾难时，备份可使业务重新启动并运行。 由于备份的重点是不断变化的业务信息，因此备份是短期信息并且经常被覆盖。 您可以将备份文件的副本保留在地理位置上独立的安全计算机上。

根据您的站点需求，还可以维护提供其他 IBM Security Key Lifecycle Manager 服务器（包括关键数据的备份）的副本计算机。 副本计算机在主 IBM Security Key Lifecycle Manager 服务器不可用时能快速恢复。

恢复 恢复操作使用已备份的生产数据（例如 IBM Security Key Lifecycle Manager 密钥库和其他关键信息）将 IBM Security Key Lifecycle Manager 服务器恢复到已知状态。

审计

IBM Security Key Lifecycle Manager 以公共基本事件 (CBE) 格式在分布式系统上提供审计记录。这些审计记录存储在审计日志中的平面文件中。

IBM Security Key Lifecycle Manager 自动化克隆复制

IBM Security Key Lifecycle Manager 自动克隆复制使用一个程序来克隆 IBM Security Key Lifecycle Manager 主服务器，最多可达 20 个副本。

您可以配置程序来复制密钥和其他配置信息（例如，当新密钥滚动显示）。此程序自动执行所需的复制。自动克隆复制可确保密钥和证书始终可供加密设备使用。

IBM Security Key Lifecycle Manager 提供了一组操作，用于复制所有系统中当前处于活动状态的文件和数据。 此复制支持以独立于操作系统和服务器目录结构的方式将 IBM Security Key Lifecycle Manager 环境克隆至多个服务器。 例如，您可以将数据从 Windows 系统上的主服务器复制到 Linux 系统上的克隆服务器。 运行自动复制程序时，会复制以下 IBM Security Key Lifecycle Manager 数据:

- IBM Security Key Lifecycle Manager 数据库表中的数据。
- IBM Security Key Lifecycle Manager 数据库中的所有密钥材料。
- IBM Security Key Lifecycle Manager 配置文件（复制配置文件除外）。

注: 这些数据将作为 IBM Security Key Lifecycle Manager 备份的组成部分。在复制期间，不会对复制配置文件进行备份并将其传递至克隆。

在 `ReplicationSKLMConfig.properties` 配置文件中定义 IBM Security Key Lifecycle Manager 复制配置参数。您可以使用图形用户界面、命令行界面或 REST 接口来更改复制配置文件的属性。 您必须在复制过程中配置所有系统上的复制配置文件。 每个 IBM Security Key Lifecycle Manager 实例被定义为*主系统*，即要克隆的系统，或者被定义为*克隆系统*，即要将数据复制到的系统。

硬件安全模块中的主密钥

IBM Security Key Lifecycle Manager 支持使用硬件安全模块 (HSM) 存储用于保护数据库中存储的所有密码的主密钥。

HSM 会为主密钥的存储和使用提供额外的保护。 产品数据库中存储的主密钥保护口令。 主口令是客户在产品中配置用于存储在 IBM Security Key Lifecycle Manager 中创建的密钥的密钥库的密码。

LDAP 与 IBM Security Key Lifecycle Manager 服务器 集成

LDAP（轻量级目录访问协议）支持在企业级别管理用户标识和密码，而不是在个别系统上管理这些数据。 您可以将 IBM Security Key Lifecycle Manager 与 LDAP 用户存储库集成。

您可以在任何 LDAP 存储库（例如，IBM Security Directory Server 或 Microsoft Active Directory）中配置 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 或 CLI。 您必须将 LDAP 用户存储库添加并配置到 WebSphere® Application Server 的联合存储库中。 有关 LDAP 配置的更多信息，请参阅：LDAP 配置

服务器配置向导

您可以使用“服务器配置向导”来对服务器和客户机设备进行 SSL/TLS 握手配置。 SSL/TLS 握手支持 IBM Security Key Lifecycle Manager 服务器与客户机设备建立连接以实现安全通信。

在安装 IBM Security Key Lifecycle Manager 后立即出现的唯一可用选项是使用“服务器配置向导”对 IBM Security Key Lifecycle Manager 进行 SSL/TLS 握手配置。 要打开，请单击**查看配置参数和/或创建 SSL 服务器证书**链接。此向导提供了设置 SSL 握手过程的指导方法。 有关 SSL/TLS 握手的更多信息，请参阅：方案：在 IBM Security Key Lifecycle Manager 服务器与客户机设备之间设置 SSL 握手。

技术概述

您可以使用 IBM Security Key Lifecycle Manager 来创建、备份和管理企业使用的密钥及证书的生命周期。 您可以管理对称密钥、非对称密钥对和证书的加密。 IBM Security Key Lifecycle Manager 还提供了图形用户界面、命令行界面和 REST 接口用于管理密钥及证书。

IBM Security Key Lifecycle Manager 等待通过 TCP/IP 通信送达的密钥生成或密钥检索请求并对其作出响应。 此通信可来自磁带库、磁带控制器、磁带子系统、设备驱动器或磁带机。

主 IBM Security Key Lifecycle Manager 提供以下功能:

- 管理对称密钥、非对称密钥对以及 X.509 V3 证书。
- 管理密钥的创建和生命周期，包含有关其目标用途的元数据。
- 为了进行灾难恢复，请提供关键数据的受保护备份。 例如，在分布式系统上，备份包含密钥数据（受管的实际密钥和证书）、有关密钥的元数据和配置文件。
- 要使密钥和证书始终可供加密设备使用，提供自动克隆复制程序来复制密钥和其他配置信息（例如，当新密钥滚动显示）。
- 根据操作系统不同，基于文件的审计日志会有所不同。在分布式系统上，审计日志包含一个平面文件中的数据，该文件基于公共基本事件 (CBE) 安全性事件规范。您还可以配置 IBM Security Key Lifecycle Manager 以生成系统日志搁置的审计记录并将它们发送到系统日志服务器。

密钥概述

加密密钥通常是专为打乱并还原数据而生成的随机位串。 加密密钥使用旨在确保每个密钥的唯一性和不可预测性的算法进行创建。 通过此方式构造的密钥越长，加密代码就越难破解。

IBM Security Key Lifecycle Manager 使用两种加密算法: 对称算法和非对称算法。 对称或密钥加密使用一个密钥进行加密和解密。 对称密钥加密可有效用于大量数据进行加密。

高级加密标准 (AES) 密钥是对称密钥，它可使用三种不同的密钥长度（128 位、192 位或 256 位）。 AES 是美国政府认可并推荐使用的加密标准。 256 位密钥是 AES 允许的最长密钥。 缺省情况下，IBM Security Key Lifecycle Manager 将生成 256 位的 AES 密钥。

非对称或公用/专用加密使用密钥对。使用公用/专用密钥对中的一个密钥加密的数据只能使用该密钥对中的另一个密钥进行解密。 生成非对称密钥对时，通常使用公用密钥进行加密，而使用专用密钥进行解密。

IBM Security Key Lifecycle Manager 同时使用对称和非对称密钥。 对称加密可以对用户或主机数据进行高速加密。 非对称加密（其速度必然较慢）可保护对称密钥。

联邦信息处理标准

联邦政府要求其所有密码提供者都已通过 FIPS 140 认证。 不断成长的私营团体中也已采用此标准。 在这一安全敏感的领域，由第三方根据政府标准对密码功能进行认证具有更高的价值。

如果将专用密钥导出至 PKCS#12 文件，请确保在包含密钥的文件离开计算机之前，使用 FIPS 核准的方法对该文件进行打包。

IBM Security Key Lifecycle Manager 本身不提供密码功能，因此无需也不必获得 FIPS 140-2 认证。 但是，IBM Security Key Lifecycle Manager 会利用 IBM Java 密码术扩展组件中 IBM JVM 的密码功能。 这些功能允许选择并使用 IBMJCEFIPS 密码提供者，后者已通过 FIPS 140-2 一级认证。

有关 IBMJCEFIPS 提供者及其选择和使用方面的更多信息，请参阅 Java 文档的 IBM 安全信息 (http://www-01.ibm.com/support/knowledgecenter/SSYKE2_6.0.0/com.ibm.java.security.component.60.doc/security-component/fips.html)。

有关如何配置 FIPS 的过程，请参阅以下技术说明：http://www-01.ibm.com/support/docview.wss?uid=swg21395541

请参阅特定硬件和软件密码提供者的文档，以获取有关他们的产品是否通过 FIPS 140-2 认证的信息。

注： 将 **fips** 配置属性设置为 on 会使 IBM Security Key Lifecycle Manager 将 IBMJCEFIPS 提供者用于所有加密功能。

IBM Security Key Lifecycle Manager 中 NSA Suite B 加密合规性

您可以配置 IBM Security Key Lifecycle Manager 以符合美国国家安全局 (NSA) 指定的标准来定义加密的安全需求。

NSA Suite B 徐烨哦 TLS 1.2 协议和密码套件，这些是通过将 ECDSA-256 和 ECDSA-384 用于客户机或服务器认证使用最低 128 位安全级别进行配置的。为支持 Suite B 概要文件，提供以下 Java 系统属性：

```
com.ibm.jsse2.suiteB=128|192|false
```

在设置 **com.ibm.jsse2.suiteB** 系统属性时，IBMJSSE2 确保遵守指定的安全级别。IBMJSSE2 验证协议、密钥和证书符合请求的概要文件。要获取更多信息，请参阅https://www-01.ibm.com/support/knowledgecenter/SSYKE2_8.0.0/com.ibm.java.security.component.80.doc/security-component/jsse2Docs/suiteb.html。

要在 IBM Security Key Lifecycle Manager 中启用 Suite B 合规性，您必须使用以下选项配置 SKLMConfig.properties 属性文件：

```
suiteB=128|192
```

在使用值 128 或 192 配置 **suiteB** 时，会将以下属性添加到属性文件或者将更新值（如果属性已存在）：

```
TransportListener.ssl.protocols=SSL_TLSv2
requireSHA2Signatures=true
autoScaleSignatureHash=true
useThisECKeySize=256(if suiteB is 128)|384(if suiteB is 192)
```

配置 IBM Security Key Lifecycle Manager 以实现 Suite B 合规性

1. 停止 IBM Security Key Lifecycle Manager 服务器。有关指示信息，请参阅在分布式系统上启动和停止 IBM Security Key Lifecycle Manager 服务器。
2. 编辑 *SKLM_HOME*/config/SKLMConfig.properties 文件中的以下属性并保存文件：

   ```
   suiteB=128|192
   ```

   - 值 128 指定最低 128 位安全级别。
   - 值 192 指定最低 192 位安全级别。

   您还可以使用 tklmConfigUpdateEntry CLI 命令或 Update Config Property REST Service 来更新 SKLMConfig.properties 文件。
3. 重新启动服务器。

使用密钥管理互操作性协议进行密钥管理

IBM Security Key Lifecycle Manager 服务器支持与客户机进行密钥管理互操作性协议 (KMIP) 通信，从而对密码材料进行密钥管理操作。 这些材料包括对称密钥和非对称密钥、证书，以及用于创建这些密钥和证书并控制其用法的模板。

密钥管理互操作性协议是结构化信息标准促进组织 (OASIS) 标准化项目的一部分，用于对存储的数据进行加密和密钥管理。

有关更多信息，请参阅“密钥管理互操作性协议”文档 (http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=kmip)。

您可以使用 IBM Security Key Lifecycle Manager 图形用户界面来管理和控制服务器支持的加密资料（对象）。有关如何管理 KMIP 对象的更多信息，请参阅KMIP 对象管理。

IBM Security Key Lifecycle Manager 支持的 KMIP 概要文件

IBM Security Key Lifecycle Manager 支持将以下概要文件用于 KMIP 服务器与客户机交互:

- 基本发现版本服务器概要文件
- 基本基线服务器 KMIP 概要文件
- 基本秘密数据服务器 KMIP 概要文件
- 基本对称密钥库和服务器 KMIP 概要文件
- 基本对称密钥铸造间和服务器 KMIP 概要文件
- 基本非对称密钥库服务器 KMIP 概要文件
- 基本非对称密钥和证书库服务器 KMIP 概要文件
- 基本非对称密钥铸造间和服务器 KMIP 概要文件
- 基本证书服务器 KMIP 概要文件（PEM 证书格式除外）
- 基本非对称密钥铸造间和证书服务器 KMIP 概要文件（PEM 证书格式除外）
- 发现版本 TLS 1.2 认证服务器概要文件
- 基线服务器 TLS 1.2 认证 KMIP 概要文件
- 秘密数据服务器 TLS 1.2 认证 KMIP 概要文件
- 对称密钥库和服务器 TLS 1.2 认证 KMIP 概要文件
- 对称密钥铸造间和服务器 TLS 1.2 认证 KMIP 概要文件
- 非对称密钥库服务器 TLS 1.2 认证 KMIP 概要文件
- 非对称密钥和证书库服务器 TLS 1.2 认证 KMIP 概要文件
- 非对称密钥铸造间和服务器 TLS 1.2 认证 KMIP 概要文件
- 证书服务器 TLS 1.2 认证 KMIP 概要文件（PEM 证书格式除外）
- 非对称密钥铸造间和证书服务器 TLS 1.2 认证 KMIP 概要文件（PEM 证书格式除外）

有关概要文件的更多信息，请参阅 KMIP 概要文件 1.2 文档 (http://docs.oasis-open.org/kmip/profiles/v1.2/kmip-profiles-v1.2.pdf)。

密钥和证书的 KMIP 属性

IBM Security Key Lifecycle Manager 支持以下任务:

- 遵循关于 KMIP 图形用户界面的信息进行操作:
  - 是否已配置 KMIP 端口和超时设置。
  - 当前 KMIP 证书，指示正在将哪个证书用于安全服务器或服务器/客户机通信。
  - 为安全通信指定的是 SSL/KMIP 还是 SSL。
- 您可以更新密钥和证书的 KMIP 属性。

  例如，您可以使用 **tklmKeyAttributeUpdate** 命令来更新:

  name
  指定用于标识或查找对象的名称。此属性为密钥管理互操作性协议属性。

  applicationSpecificInformation
  将应用程序名称空间信息指定为密钥管理互操作性协议属性。

  contactInformation
  将联系人信息指定为密钥管理互操作性协议属性。

  cryptoParams *cryptoparameter1, cryptoparameterN*
  使用对象来指定用于加密操作的加密参数。 此属性为密钥管理互操作性协议属性。

  customAttribute
  将字符串格式的定制属性指定为密钥管理互操作性协议属性。特定于客户机的属性必须以字符“x-”（x 连字符）开头，而特定于服务器的属性必须以“y-”（y 连字符）开头。

  link
  指定从一个受管加密对象指向另一个密切相关的目标受管加密对象的链接。 此属性为密钥管理互操作性协议属性。

  objectGroup
  指定此对象可能属于的一个或多个对象组名。 此属性为密钥管理互操作性协议属性。

  processStartDate
  指定对称密钥对象可用于处理的日期。 在该日期之后，您不能更改该值。如果指定的日期早于当前日期，那么该值将设置为当前日期。 此属性为密钥管理互操作性协议属性。

  protectStopDate
  指定对象不能用于处理的日期。 在该日期之后，您不能更改该值。 如果指定的日期早于当前日期，那么该值将设置为当前日期。 此属性为密钥管理互操作性协议属性。

  usageLimits
  将总字节数 (BYTE) 或总对象数 (OBJECT) 指定为密钥管理互操作性协议属性。使用此对象之后，就不能修改此值。 例如，**GetUsageAllocation** 将调用此对象。
- 列出并删除客户机注册的 KMIP 模板。

客户机使用模板以标准化或方便的方式指定新对象的密码属性。 模板是受管对象，包含客户机可为密码对象设置的操作中的属性。 例如，客户机可设置特定于应用程序的信息。

tklmKMIPTemplateList

列出 IBM Security Key Lifecycle Manager 提供的 KMIP 模板。例如，您可以列出所有模板。

tklmKMIPTemplateDelete

删除客户机向 IBM Security Key Lifecycle Manager 注册的 KMIP 模板。

- 列出并删除秘密数据（如密码）或用于生成密钥的种子值。

tklmSecretDataDelete

删除 KMIP 客户机发送至 IBM Security Key Lifecycle Manager 的秘密数据。

tklmSecretDataList

列出 KMIP 客户机发送至 IBM Security Key Lifecycle Manager 的秘密数据。

- 设置缺省端口和超时属性

KMIPListener.ssl.port

指定 IBM Security Key Lifecycle Manager 服务器侦听来自库的请求时使用的端口。 该服务器通过 SSL 套接字并使用密钥管理互操作性协议进行通信。

TransportListener.ssl.port

指定 IBM Security Key Lifecycle Manager 服务器侦听来自磁带库（这些磁带库使用 SSL 协议进行通信）的请求时使用的端口。

TransportListener.ssl.timeout

指定套接字在关闭之前等待 read() 的时间。此属性用于 SSL 套接字。

- 启用或禁用来自 KMIP 客户机的删除请求。

认证过的客户机可请求对密钥可用性、服务器性能和密钥安全性可能有重大影响的删除操作。 使用 **tklmDeviceGroupAttributeUpdate** 或 **tklmDeviceGroupCreate** 命令指定 enableKMIPDelete 属性以确定 IBM Security Key Lifecycle Manager 是否会对这些请求执行操作。

密钥提供管理

IBM Security Key Lifecycle Manager 解决方案可帮助支持 IBM 加密的设备生成、保护、存储和维护加密密钥。 您可以使用这些密钥对写入设备以及从设备中读取的信息进行加密和解密。

IBM Security Key Lifecycle Manager 充当后台进程，等待通过其本身与磁带库、磁带控制器、磁带子系统、设备驱动程序或磁带机之间的 TCP/IP 通信路径发送来的密钥生成请求或密钥检索请求。 当磁带机写入加密数据时，它将首先请求来自 IBM Security Key Lifecycle Manager 的加密密钥。

AES 密钥和 3592 磁带机:

当 3592 磁带机写入加密数据时，它将首先请求来自 IBM Security Key Lifecycle Manager 的加密密钥。

IBM Security Key Lifecycle Manager 收到请求后将生成高级加密标准 (AES) 密钥。 该密钥以两种受保护形式提供给磁带机:

- 使用 Rivest-Shamir-Adleman (RSA) 密钥对加密或打包。 3592 磁带机 将此密钥副本写入盒式磁带的内存中，另外还将其写入盒式磁带内磁带介质上的其他位置以用作冗余备份。
- 单独打包以安全传送至磁带机，送达后对密钥进行解包。 内部密钥用于对写入磁带的数据进行加密。

当 3592 磁带机读取加密的盒式磁带时，会将磁带上受保护的 AES 密钥发送至对打包 AES 密钥进行解包的 IBM Security Key Lifecycle Manager。 然后将使用不同的密钥对 AES 密钥进行打包，以便安全地传送回磁带机。 将对该密钥进行解包并用于对磁带上存储的数据进行解码。 IBM Security Key Lifecycle Manager 还允许对受保护的 AES 密钥进行二次打包，方法是在对磁带进行写入时使用不同于原始 RSA 密钥的 RSA 密钥。当意外地需要将卷导出给业务合作伙伴，而又没有业务伙伴的公用密钥时，对密钥进行二次打包很有用。 此方法不需要重新写入整个磁带，能够使用业务合作伙伴的公用密钥对使盒式磁带的数据密钥进行二次加密。

非对称密钥和 3592 磁带机:

除了 256 位 AES 对称数据密钥之外，IBM Security Key Lifecycle Manager 还使用公用/专用（非对称）密钥密码术来保护对称数据加密密钥。 这些密钥在 IBM Security Key Lifecycle Manager 与 3592 磁带机 之间传递时生成并接受检索。

公用/专用密钥密码术还用于验证 IBM Security Key Lifecycle Manager 为其提供密钥的磁带机的标识。

当 3592 磁带机请求密钥时，IBM Security Key Lifecycle Manager 将生成随机对称数据加密密钥。 请使用公用/专用密钥密码术，通过密钥加密密钥来对数据加密密钥进行打包，其中密钥加密密钥是非对称密钥对的公用密钥。

打包的数据密钥与解包对称密钥所需的专用密钥的相关密钥标签信息，共同组成了一个数字信封，称为外部加密的数据密钥结构。 该结构存储在存放使用此方法加密的数据的任何盒式磁带的磁带头区域中。 用于对数据进行解密的密钥与数据一起存储在磁带本身之中，通过非对称公用/专用密钥打包加以保护。 用于打包数据密钥的公用密钥从以下两个来源之一获取:

- 存储在密钥库中的公用密钥（属于内部生成的公用/专用密钥对）。
- 存储在密钥库中的证书（例如，来自业务合作伙伴的证书）。

存储在密钥库中的证书和密钥是允许磁带机或磁带库对磁带上的数据进行解密的控制点。 没有密钥库中的信息，就无法读取磁带。 防止未授权用户从密钥库获取专用密钥非常重要。 您必须始终使密钥库可用于读取磁带。

数据加密密钥以打包且受保护形式仅存储在磁带上。 当 3592 磁带机要读取加密的磁带时，该磁带机会将外部加密的数据密钥发送至 IBM Security Key Lifecycle Manager。 IBM Security Key Lifecycle Manager 将根据别名或密钥标签来确定使用其密钥库中的哪个专用密钥加密密钥来解包外部加密的数据密钥并恢复数据加密密钥。

恢复数据加密密钥后，将使用磁带机可解密的其他密钥对其进行打包。 然后，该密钥将发送回磁带机，从而使磁带机能够对数据进行解密。

在对 3592 磁带机加密时，IBM Security Key Lifecycle Manager 使用别名（也称为密钥标签）来标识用于打包外部加密数据密钥的公用/专用密钥。 可以使用 IBM Security Key Lifecycle Manager 图形用户界面或命令行界面来为每个磁带设备定义特定的别名。

IBM Security Key Lifecycle Manager 允许为每个加密磁带机定义至少两个别名（证书或密钥标签）。 通过别名可以访问组织内外其他位置上的加密数据。 其中一个别名的专用密钥必须已知。 如果不想指定两个不同的密钥标签或别名，那么可使用相同的值来定义这两个别名。

AES 密钥和 LTO 磁带机:

当 LTO 磁带机写入加密数据时，它将首先请求来自 IBM Security Key Lifecycle Manager 的加密密钥。

收到请求后，IBM Security Key Lifecycle Manager 将从密钥库获取现有 AES 密钥。然后，将打包该密钥以安全传送至磁带机。 随后，将解包该密钥并用于对写入磁带的数据进行解密.

当 LTO 磁带机读取已加密的磁带时，IBM Security Key Lifecycle Manager 将从密钥库获取所需的密钥。 该密钥基于磁带中密钥标识内的信息，并将其打包提供给磁带机，以便进行安全传输。

对称密钥和 LTO 磁带机:

IBM Security Key Lifecycle Manager 仅将对称数据密钥用于 LTO 磁带机上的加密任务。

LTO 磁带机请求密钥时，IBM Security Key Lifecycle Manager 将使用为该磁带机指定的别名。 如果没有为该磁带机指定别名，IBM Security Key Lifecycle Manager 将使用来自密钥组、密钥别名列表或密钥别名范围中的别名。

密钥组中的密钥将以循环方式使用，以帮助更均等地使用密钥。

选定的别名将与预先安装在密钥库中的对称数据密钥相关联。 IBM Security Key Lifecycle Manager 会将此数据密钥发送至 LTO 磁带机以用于对数据进行加密。 选定别名也会转换成称为数据密钥标识的实体，该实体将写入具有已加密数据的磁带中。 读取 LTO 磁带时，IBM Security Key Lifecycle Manager 可使用数据密钥标识来识别对数据进行解密所需的正确数据密钥。

AES 密钥和 DS8000 Turbo 磁带机:

DS8000 Turbo 磁带机启动时，设备将请求来自 IBM Security Key Lifecycle Manager 的解锁密钥。

如果 DS8000 Turbo 磁带机请求新密钥用作其解锁密钥，那么 IBM Security Key Lifecycle Manager 将生成高级加密标准 (AES) 密钥。 然后，该密钥以两种受保护形式提供给磁带机:

- 使用 Rivest-Shamir-Adleman (RSA) 密钥对加密（打包）。 DS8000 Turbo 磁带机会将此密钥副本存储在未加密分区中的数组上。
- 单独打包以便安全地传输到磁带机，到达后会立即解包并使用其中的密钥对数组进行解锁。

如果 DS8000 Turbo 磁带机请求现有的解锁密钥，那么数组上受保护的 AES 密钥将发送至 IBM Security Key Lifecycle Manager，打包的 AES 密钥将在其中解包。 然后将使用不同的密钥对 AES 密钥进行打包，以便安全地传送回 DS8000 Turbo 磁带机。 将解包该密钥，并将其用于对阵列进行解锁。

非对称密钥和 DS8000 Turbo 磁带机:

当 256 位 AES 对称数据加密密钥在 IBM Security Key Lifecycle Manager 和 DS8000 Turbo 磁带机之间传递时，IBM Security Key Lifecycle Manager 还将使用公用/专用（非对称）密钥密码术对其进行保护。

公用/专用密钥密码术还用于验证 IBM Security Key Lifecycle Manager 为其提供密钥的磁带机的标识。 当 DS8000 Turbo 磁带机请求新的密钥时，IBM Security Key Lifecycle Manager 将生成随机对称数据加密密钥。 请使用公用/专用密钥密码术，通过密钥加密密钥来对数据加密密钥进行打包，其中密钥加密密钥是非对称密钥对的公用密钥。

打包的数据密钥与解包对称密钥所需的专用密钥的相关密钥标签信息，共同组成了一个数字信封，称为外部加密的数据密钥结构。该结构存储在保存使用此方法所加密数据的任何盒式磁带的磁带头区域中。 用于对数据进行解密的密钥与数据一起存储在磁带本身之中，通过非对称公用/专用密钥打包加以保护。 用于打包数据密钥的公用密钥从以下两个来源之一获取:

- 存储在密钥库中的证书（例如，来自业务合作伙伴的证书）。
- 存储在密钥库中的公用密钥（属于内部生成的公用/专用密钥对）。

存储在密钥库中的证书和密钥是允许对 DS8000 Turbo 磁带机进行解锁的控制点。 没有密钥库中的信息，就无法对 DS8000 Turbo 磁带机进行解锁。

您必须防止未经授权的用户访问密钥库中的专用密钥，并使密钥库对您自己始终可用以便对阵列进行解锁。 数据加密密钥以打包且受保护形式仅存储在 DS8000 Turbo 磁带机上。

为了对 DS8000 Turbo 磁带机进行解锁，DS8000 Turbo 磁带机 会将外部加密的数据密钥发送给 IBM Security Key Lifecycle Manager。 IBM Security Key Lifecycle Manager 将根据别名或密钥标签来确定使用其密钥库中的哪个专用密钥加密密钥来解包外部加密的数据密钥并恢复数据加密密钥。 恢复数据加密密钥后，将使用磁带机可解密的其他密钥对其进行打包。 然后，该密钥将发送回磁带机，从而使磁带机能够对数据进行解密。

IBM Security Key Lifecycle Manager 使用别名（也称为密钥标签）来识别用于打包解锁密钥的公用/专用密钥。 您可以为每个设备定义特定的别名。 IBM Security Key Lifecycle Manager 允许最多为每个 DS8000 Turbo 磁带机定义两个别名（证书或密钥标签），从而避免发生死锁情况。 IBM Security Key Lifecycle Manager 与 DS8000 Turbo 磁带机必须位于同一系统中。 DS8000 Turbo 磁带机必须先进行解锁，然后 IBM Security Key Lifecycle Manager 才能够运行。 其中一个别名的专用密钥必须已知。 如果不想指定两个不同的密钥标签或别名，那么可使用相同的值来定义这两个别名。

AES 密钥和 DS5000 存储服务器:

DS5000 存储服务器启动时，设备将请求来自 IBM Security Key Lifecycle Manager 的密钥以对磁盘驱动器进行解锁。

作为响应，IBM Security Key Lifecycle Manager 将从密钥库获取一个现有的 AES 密钥。 IBM Security Key Lifecycle Manager 将对该 AES 密钥进行打包，以便安全地传输到 DS5000 存储服务器，后者会对该密钥进行解包以用于解锁磁盘驱动器。

对称密钥和 DS5000 存储服务器:

IBM Security Key Lifecycle Manager 仅将对称数据密钥用作 DS5000 存储服务器的解锁密钥。

DS5000 存储服务器请求密钥时，IBM Security Key Lifecycle Manager 将使用请求指定的别名来获取密钥。 如果 DS5000 存储服务器请求不指定别名，那么 IBM Security Key Lifecycle Manager 将从与请求 DS5000 存储服务器关联的密钥列表中获取别名。 此列表中的密钥将以循环方式提供，以使密钥得到均等使用。

选定的别名将与预先安装在密钥库中的对称数据密钥相关联。 IBM Security Key Lifecycle Manager 将对称数据密钥发送至设备以用于对此数组的磁盘驱动器进行解锁。选定别名也会转换成称为数据密钥标识的 DS5000 存储服务器存储的实体。 IBM Security Key Lifecycle Manager 可在需要时使用数据密钥标识来识别正确的数据密钥。

主要组件

分布式系统上的 IBM Security Key Lifecycle Manager 解决方案包括 IBM Security Key Lifecycle Manager 服务器、WebSphere Application Server 和 DB2®。

在分布式系统上，安装 IBM Security Key Lifecycle Manager 会同时安装这些必备软件。

运行时环境

- 分布式系统

  WebSphere Application Server 运行 Java 虚拟机，该虚拟机为应用程序代码提供运行时环境。 应用程序服务器提供通信安全性、日志记录、消息传递以及 Web 服务。

数据库服务器

IBM Security Key Lifecycle Manager 将密钥材料存储在 DB2 关系数据库中。使用 IBM Security Key Lifecycle Manager 来管理 DB2。

Windows 以及 Linux 或 AIX 等其他系统上的部署

在 Windows 系统以及 Linux 或 AIX 等其他系统上，IBM Security Key Lifecycle Manager 安装程序将 IBM Security Key Lifecycle Manager 服务器和必需的中间件组件部署在同一台计算机上。 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。

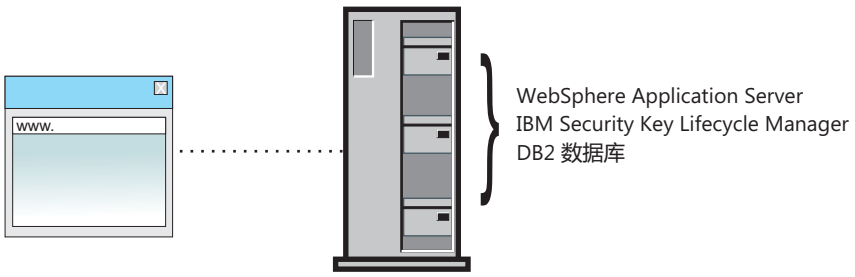

图 2. Windows 系统以及 Linux 或 AIX 等其他系统上的主要组件

部署主服务器和副本服务器

为了确保可用性，请既部署主 IBM Security Key Lifecycle Manager 服务器，又在其他系统上部署主 IBM Security Key Lifecycle Manager 服务器的副本。

在 Windows 系统以及 Linux 或 AIX 等其他系统上，两台计算机必须具有满足工作负载的所需内存、速度和可用磁盘空间。 两台计算机上的操作系统和中间件组件必须相同。 安装路径也必须相同。

图 3. 主 IBM Security Key Lifecycle Manager 服务器和副本 IBM Security Key Lifecycle Manager 服务器

副本系统需求

副本系统必须具有完全相同的操作系统、数据库和 IBM Security Key Lifecycle Manager 应用程序，包括来自当前 IBM Security Key Lifecycle Manager 服务器备份文件的关键数据。 安装路径也必须相同。

确保对于以下需求，在两个系统上具有相同的版本和修订级别:

- 操作系统和修订或补丁。
- DB2 和必需的可用磁盘空间。 数据库必须位于运行 IBM Security Key Lifecycle Manager 服务器的同一系统上。
- IBM Security Key Lifecycle Manager 服务器.

  您必须将当前 IBM Security Key Lifecycle Manager 服务器备份文件手动复制到副本系统。 IBM Security Key Lifecycle Manager 不会自动同步两个 IBM Security Key Lifecycle Manager 服务器之间的数据。

备份和复原

备份和恢复任务提供对关键数据的保护，并且需要考虑站点实践以确保服务器的可用性和运行时能力。

IBM Security Key Lifecycle Manager 会以独立于操作系统和服务器目录结构的方式来创建备份文件。 备份文件包含 IBM Security Key Lifecycle Manager 服务器当前状态的关键数据。 站点实践必须考虑如何确保可以提供密钥。

您可以使用跨平台备份实用程序在早期版本的 IBM Security Key Lifecycle Manager 上运行备份操作来备份关键数据。 您可以在最新版本的 IBM Security Key Lifecycle Manager 上将这些备份文件复原至不同于从中备份这些文件的其他操作系统中。

注: 从 IBM Security Key Lifecycle Manager V2.6 发行版起，不再支持 Solaris 操作系统。 如果您正在 Solaris 系统上使用 IBM Security Key Lifecycle Manager，请使用跨平台备份实用程序来备份数据。 随后，在部署于任何受支持操作系统（例如，Windows、Linux 或 AIX）上的 IBM Security Key Lifecycle Manager V2.6 系统上，您可以运行复原操作以复原这些数据。

IBM Security Key Lifecycle Manager 备份和复原操作支持将 AES 256 位密钥长度用于数据加密/解密，以符合 PCI DSS（支付卡行业数据安全标准）标准，从而提高数据安全性。

仅当使用 AES 256 位主密钥进行数据加密时，备份和复原操作才使用 AES 256 位长度的密钥对数据进行加密或解密。 如果 IBM Security Key Lifecycle Manager 备份操作将 AES 256 位密钥用于数据加密，那么您必须安装 Java 密码术扩展 (JCE) 无限制强度管辖区域策略文件。 有关安装指示信息，请参阅安装 Java 密码术扩展无限制强度管辖区域策略文件。

注: 在最新版本中，安装 IBM Security Key Lifecycle Manager 后，缺省情况下会生成 AES 256 位主密钥，并在服务器中安装 JCE 不受限强度管辖区域策略文件。

备份文件中的数据类别

IBM Security Key Lifecycle Manager 的备份文件包含关键数据。 例如，根据您的配置，它可能包含密钥材料、配置文件和其他信息。

以下类别的数据需要备份保护:

IBM Security Key Lifecycle Manager 配置文件

定义选定 IBM Security Key Lifecycle Manager 活动的属性，例如审计设置和为系统配置定制的其他值。

IBM Security Key Lifecycle Manager 数据库

有关 IBM Security Key Lifecycle Manager 对象（例如设备、密钥组、证书、密钥材料和驱动器）的数据。

备份文件安全性

确保没有意外损坏备份文件或忘记加密密码。

要为备份文件提供安全性:

- 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 目录路径之外的位置。 保存在其他位置可确保在除去 IBM Security Key Lifecycle Manager 时，其他进程不会除去审计日志和备份文件。
- 请勿编辑备份 JAR 文件中的文件。 否则这些文件将变得不可读。
- 确保您保留了用于对备份文件进行加密的密码。 需要相同的密码来解密并恢复文件。

恢复

恢复操作使用已备份的生产数据（例如 IBM Security Key Lifecycle Manager 密钥材料和其他关键信息）将 IBM Security Key Lifecycle Manager 服务器恢复到已知状态。

IBM Security Key Lifecycle Manager 支持跨操作系统执行复原操作。 您可以在不同于从中备份 IBM Security Key Lifecycle Manager 文件的其他操作系统上复原这些备份文件。 例如，您可以将在 Linux 系统上生成的备份复原至 Windows 系统。

从您先前指定的非 IBM Security Key Lifecycle Manager 目录路径的位置检索备份文件的副本。 您还必须知道先前用于对备份文件进行加密的密码。 使用密码可在主 IBM Security Key Lifecycle Manager 服务器上解密和复原文件。

在复原备份文件之前，请确保备份清单文件中列出了归档中的所有 IBM Security Key Lifecycle Manager数据文件。 运行备份操作时，会随备份归档一起创建清单文件。

在启动复原任务之前，请隔离系统以进行维护。 对现有系统进行备份。如果在复原过程中发生任何问题，您就可以使用此备份将系统恢复为原始状态。执行复原后，必须立即重新启动 IBM Security Key Lifecycle Manager 服务器。 请先验证环境，然后再将 IBM Security Key Lifecycle Manager 服务器重新切换为生产环境。

登录 URL 和初始用户标识

要在安装 IBM Security Key Lifecycle Manager 后开始使用该产品，请获取登录 URL 以及初始 IBM Security Key Lifecycle Manager 管理员用户标识和密码。

访问权需求

作为管理员（root 用户）来对 IBM Security Key Lifecycle Manager 进行安装。

您还可以只在 Linux 操作系统中作为非 root 用户来对 IBM Security Key Lifecycle Manager 进行安装。

登录 URL

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

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

ip-address 的值是 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 侦听请求的端口号。

如果使用 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，信息位于开始菜单。单击**开始 > 所有程序 > IBM Security Key Lifecycle Manager 2.6**。

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

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

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

port 的值是 WebSphere Application Server 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，或者在缺省端口由于其他原因而存在冲突时，WebSphere Application Server 会自动选择其他可用端口。

安装完成面板指示为 WebSphere Application Server 配置的端口。 Windows“开始”菜单包含一个条目，用于通过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 WASAdmin、SKLMAdmin 和 `sklmdb26` 的缺省管理员用户标识。

表 1. 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，必须由本地管理标识执行安装，该标识是 AIX 或 Linux 系统的 root 用户标识，或者是 Windows 系统上 Administrators 组的成员。 不要使用域用户标识来安装 IBM Security Key Lifecycle Manager。 您可能具有以下一个或多个用户标识:		

表 1. 管理员用户标识和密码 (续)

程序	用户标识	密码
IBM Security Key Lifecycle Manager 管理员	**SKLMAdmin** 作为对所有操作具有完整访问权的主管理员，此用户标识在名为 `klmSecurityOfficerGroup` 的组中具有 `klmSecurityOfficer` 超级用户角色。此用户标识不区分大小写。 或者，使用 **sklmadmin**。使用 SKLMAdmin 用户标识可管理 IBM Security Key Lifecycle Manager。 使用 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，您无法: • 创建一个或多个额外的 IBM Security Key Lifecycle Manager 管理员用户标识。 • 执行 WebSphere Application Server 管理员任务，例如创建或分配角色。 • 启动或停止服务器。	在安装期间指定并安全存储密码。

表 1. 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** 此用户标识不区分大小写。 或者，使用 **wasadmin** 或安装期间指定的用户标识。 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 用户标识没有使用 IBM Security Key Lifecycle Manager 的角色。 此管理员用户标识是 WebSphere Application Server 管理员用户标识。 使用 wasadmin 用户标识，您可以: • 查看并仅使用 WebSphere Application Server 界面。 • 创建一个或多个额外的 IBM Security Key Lifecycle Manager 管理员用户标识、组和角色。 • 重置任何 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，您无法: • 使用 IBM Security Key Lifecycle Manager 来完成任务。 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*以超级用户身份访问 IBM Security Key Lifecycle Manager。	在安装期间指定并安全存储密码。 使用保护 SKLMAdmin 用户标识的方式来保护 WASAdmin 用户标识。 WASAdmin 用户标识有权重置 SKLMAdmin 密码，也有权创建许可权并将许可权分配给 IBM Security Key Lifecycle Manager 用户。
IBM Security Key Lifecycle Manager DB2 数据库		

表 1. 管理员用户标识和密码 (续)

程序	用户标识	密码
数据库的实例所有者	**Windows 系统以及诸如 AIX 或 Linux 等系统**: 缺省值为 sklmdb26。您可以在安装期间指定不同的值。 该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。 实例名称也是 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。 如果将现有的用户标识用作 IBM Security Key Lifecycle Manager 数据库的实例所有者，那么该用户标识无法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。 如果在操作系统上更改了密码，那么必须更改此密码。 要获取更多信息，请参阅第 29 页的『重置分布式系统上的密码』。.
数据库实例	管理员标识 sklmdb2 拥有名为 sklmdb26 的 DB2 实例。	

HOME 及其他目录变量的定义

您可为特定实现定制 *HOME* 目录。 请相应地替换每个目录变量的定义。

下表包含本资料中用于表示各种产品安装路径的 *HOME* 目录级别的缺省定义。

path 的缺省值对于以下操作系统有所不同，为引用方便，将这些操作系统称为 *distributed systems*。 术语『分布式系统』指的是非大型机硬件平台，包括个人计算机和工作站。

- 对于 Windows系统，缺省路径为:
  - DB2

    drive:\Program Files (x86)\IBM
  - 除 DB2 以外的所有应用程序

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

表 2. HOME 及其他目录变量

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 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 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。

共享浏览器会话的问题

对于使用 WebSphere Application Server 和 IBM Security Key Lifecycle Manager 的共享浏览器会话，必须予以避免，因为此类会话会在服务器上造成不可预料的结果。 在同一客户机上使用多个浏览器窗口时，可以共享会话。

例如，在使用 Firefox 浏览器时，会话始终会共享。 会话可能还在 Internet Explorer 中共享，这取决于注册表设置或打开浏览器窗口的方式。

您必须避免以下情况:

- 多个用户登录同一会话。
- 同一客户机上的多个浏览器窗口访问相同的 WebSphere Application Server。

IBM Security Key Lifecycle Manager 用户的密码策略

应用于新 IBM Security Key Lifecycle Manager 用户的密码的密码策略由 *SKLM_HOME*/config/TKLMPasswordPolicy.xml 文件指定。

策略不会应用于为缺省用户（例如，SKLMAdmin）创建的初始密码。 缺省用户在 IBM Security Key Lifecycle Manager 安装期间创建。

密码策略应用于对缺省用户的密码更改以及新用户的新密码和已更改密码。仅当创建或更改了用户概要文件时，才会执行策略检查。 在新用户尝试登录到 IBM Security Key Lifecycle Manager 之前，必须为该用户指定角色。

缺省情况下将启用密码策略。 您可以使用 XML 或 ASCII 编辑器来更改此文件。 要禁用此策略，请将策略文件中 **enabled** 参数的值更改为 false:

```
PasswordPolicy enabled="true"
```

IBM Security Key Lifecycle Manager 支持以下密码规则:

表 3. 密码规则

规则	缺省值
最小长度	6
最大长度	20
最小数字字符数	2
最小字母字符数	3
同一字符连续出现的最大次数	2
禁止密码中出现用户标识*	已启用
禁止密码中出现用户名*	已启用

* 检测此值是否区分大小写。

注: 要指定该值不区分大小写，请编辑缺省密码策略并为用户标识和用户名指定 CaseInsensitive:

```
<?xml version="1.0" encoding="UTF-8"?>
<PasswordPolicy version="1.0" uuid="" name="Password policy for TKLM"
enabled="true">
    <Description/>
    <PasswordRules><![CDATA[<?xml version="1.0" encoding="UTF-8"?>
 <PasswordRuleSet version="1.0">
     <MinLengthConstraint Min="6"/>
     <MaxLengthConstraint Max="20"/>
     <MaxSequentialChars Max="2"/>
     <MinAlphabeticCharacters Min="3"/>
     <MinDigitCharacters Min="2"/>
     <NotUserIDCaseInsensitive/>
     <NotUserNameCaseInsensitive/>
 </PasswordRuleSet>
]]></PasswordRules>
</PasswordPolicy>
```

更改密码策略

使用编辑器来手动更改 IBM Security Key Lifecycle Manager 提供的密码策略。

关于此任务

确保仅更改密码策略中的元素和属性值，而不是更改元素和属性名称本身。 密码策略应用于对缺省用户的密码更改以及新用户的新密码和已更改密码。 仅当创建或更改了用户概要文件时，才会执行策略检查。

过程

1. 在开始之前，将 *SKLM_HOME*/config/TKLMPasswordPolicy.xml 文件备份到安全位置。如果更改后的密码策略有问题，您可以还原到备份副本。
2. 在文本编辑器中编辑 TKLMPasswordPolicy.xml 文件，仅更改密码策略中 XML 元素和属性的值。
3. 保存已更改的文件。

   策略更改将立即执行。 无需重新启动 IBM Security Key Lifecycle Manager 服务器。
4. 要对更改进行测试，请以 WASAdmin 身份登录 WebSphere Application Server 并为新用户创建用户概要文件。

   确认接受符合策略的密码，而拒绝违反策略的密码。 完成时，如果必要，请删除测试用户概要文件。

更改用户密码

更改后的用户密码必须符合 IBM Security Key Lifecycle Manager 提供的密码策略。

关于此任务

此任务使用 WebSphere 集成解决方案控制台 上的 WASAdmin 用户标识来更改用户的密码，包括 SKLMAdmin 用户标识的密码。

有关用于创建组和用户的命令的更多信息，请参阅 IBM WebSphere Application Server 文档 (http://www-01.ibm.com/support/knowledgecenter/SSAW57_8.5.5/com.ibm.websphere.nd.iseries.doc/ae/rxml_atwimmgt.html)。

过程

1. 登录到 WebSphere 集成解决方案控制台。
   - 图形用户界面:
     a. 在浏览器的欢迎页面上，输入 WASAdmin 的用户标识和密码值，例如 wasadminpw。
     b. 在导航树中，单击**用户和组** > **管理用户**。
   - 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，WASAdmin 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 WASAdmin -password wasadminpw -lang jython
```

– AIX 或 Linux 等系统:

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

2. 更改用户的密码。
   - 图形用户界面:
     a. 在**管理用户 > 搜索用户**对话框，单击**搜索**。
     b. 在搜索条件表中，双击选定的用户标识。例如，双击 myAdmin 将其作为用户标识。
     c. 在“用户属性”对话框中，更改**密码**和**确认密码**字段的值。
     d. 单击**确定**。
   - 命令行界面:
     a. 输入 updateUser 并指定所需的值。 例如，使用 Jython 在一行上输入:

```
print AdminTask.updateUser('-uniqueName uid=test2,
o=defaultWIMFileBasedRealm -password secret12 -confirmPassword secret12')
```

其中,

-uniqueName
指定要为其创建密码的用户的唯一名称。 （字符串，必需）

更改密码之前，可以使用 **searchUsers** 命令来验证该名称是否正确标识了用户。

-password
指定用户的密码。 （字符串，必需）

新密码必须符合 IBM Security Key Lifecycle Manager 提供的密码策略。

-confirmPassword
再次指定密码以验证为密码参数输入的密码。 （字符串，可选）

下一步做什么

接下来，验证该用户是否可以登录。 以 WASAdmin 身份注销。 以该用户身份登录并确认接受已更改的密码。

更改 IBM Security Key Lifecycle Manager 用户密码

您可以使用 IBM Security Key Lifecycle Manager 应用程序用户标识来更改用户密码。更改的密码必须符合 IBM Security Key Lifecycle Manager 提供的密码策略。

关于此任务

有关用于更改密码的命令的更多信息，请参阅 IBM WebSphere Application Server 文档 (http://www-01.ibm.com/support/knowledgecenter/SSAW57_8.5.5/com.ibm.websphere.nd.iseries.doc/ae/rxml_atwimmgt.html)。

过程

1. 导航至相应的页面或目录:
   - 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登录 wsadmin。

Windows

导航至 C: \Program Files (x86)\IBM\WebSphere\AppServer\bin 目录并输入:

```
wsadmin.bat -username <SKLM user> -password <SKLM user passwd>
-lang jython
```

AIX 或 Linux

导航至 /opt/IBM/WebSphere/AppServer/bin 目录并输入:

```
./wsadmin.sh -username <SKLM user> -password <SKLM user passwd>
-lang jython
```

- 图形用户界面:
  – 登录图形用户界面。

2. 更改用户的密码。
   - 命令行界面:
     – 运行以下命令:

```
AdminTask.changeMyPassword('[-oldPassword <oldpasswordvalue>
-newPassword
<newpasswordvalue> -confirmNewPassword <newpasswordvalue>]')
```

示例:

```
AdminTask.changeMyPassword('[-oldPassword sklmadmin -newPassword
Ibm12one
-confirmNewPassword Ibm12One]')
```

   - 图形用户界面:
     a. 在标题栏上，单击 **<SKLM 用户>**链接。
     b. 单击**更改密码**。
     c. 在“更改密码对话框中，输入您的**当前密码**。
     d. 输入您的**新密码**。
     e. 在**确认新密码**字段中再次输入新密码。
     f. 单击**更改密码**。

重置分布式系统上的密码

您必须是管理员才能重置 IBM Security Key Lifecycle Manager 或 WebSphere Application Server 的密码。

关于此任务

您可以对运行 IBM Security Key Lifecycle Manager 的计算机上的密码进行重置。仅当用户的密码丢失时，才应使用以下步骤。 在所有其他情况下，请使用图形用户界面来更新密码。

过程

1. 使用本地管理员用户标识登陆。
2. 备份 *WAS_HOME*/profiles/KLMProfile/config/cells/SKLMCell/fileRegistry.xml 文件。更改密码的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 用户标识或具有 WebSphere Application Server 管理员权限的其他用户标识可以使用 **AdminTask.changeFileRegistryAccountPassword** 命令更改密码。
        - 不会根据 IBM Security Key Lifecycle Manager 提供的已配置密码策略对使用 **AdminTask.changeFileRegistryAccountPassword** 命令创建的密码进行验证。

          在重置丢失的密码后，用户必须使用图形用户界面来设置密码。

     c. 保存更改并退出:

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

   - Linux 或 AIX 等系统
     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 用户标识或具有 IBM Security Key Lifecycle Manager 管理员权限的其他用户标识可以使用 **AdminTask.changeFileRegistryAccountPassword** 命令更改密码。
        - 不会根据 IBM Security Key Lifecycle Manager 提供的已配置密码策略对使用 **AdminTask.changeFileRegistryAccountPassword** 命令创建的密码进行验证。

          在重置丢失的密码后，用户必须使用图形用户界面来设置密码。

     c. 保存更改并退出:

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

4. 停止并启动服务器。
   - 停止

     在 Windows 系统上:

     ```
     stopServer.bat server1
     ```

     在例如 Linux 或 AIX 的系统上:

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

- 开始

  在 Windows 系统上:

  ```
  startServer.bat server1
  ```

  在例如 Linux 或 AIX 的系统上:

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

5. 验证是否可以使用新密码以指定的管理员身份登录。

用户角色

IBM Security Key Lifecycle Manager 提供了一个超级用户（klmSecurityOfficer 和 klmGUICLIAccessGroup）角色以及多种指定受到更多限制的管理角色的方法，可满足您组织的需求。缺省情况下，SKLMAdmin 用户标识具有 klmSecurityOfficer 角色。

对于备份和恢复任务，IBM Security Key Lifecycle Manager 还会安装 klmBackupRestoreGroup，初始情况下其中没有任何用户标识。 安装 IBM Security Key Lifecycle Manager 将创建预定义的管理员、操作员和审计员组以管理 LTO 磁带机。

WASAdmin 用户标识有权创建和分配这些角色，并更改任何 IBM Security Key Lifecycle Manager 管理员的密码。要设置 IBM Security Key Lifecycle Manager 的管理限制，请在 WebSphere Integrated Solutions Console 上使用 WASAdmin 用户标识来创建角色、用户和组。 将角色和用户分配给组。 例如，您可以创建组并分配将用户活动限制为仅管理 LTO 磁带机的用户和角色。 在新用户尝试登录到 IBM Security Key Lifecycle Manager 之前，必须为其分配角色。

开始之前，请完成以下任务:

- 确定您的组织所需的设备管理的限制。

  例如，可能要确定特定的设备组具有其自己的管理。
- 估计在某一时间间隔内可能需要多少管理用户。 为了使用方便，请考虑指定组和角色以指定其任务。

  例如，可以指定一个具有受限范围许可权的组以仅管理 3592 磁带机。

用户、组、角色和受保护对象之间的关系

要对受保护对象执行有用的操作，IBM Security Key Lifecycle Manager 用户必须具有一个或多个角色。 角色必须能够执行操作，例如在 LTO 设备系列中创建对象（例如设备）。

用户可以是组的成员。 组可能具有一个或多个角色。角色用于指定对受保护的对象执行操作的权限。例如，受保护的对象包括设备、设备组、密码对象（证书、密钥、密钥对和密钥组）以及证书和密钥组的滚动设置。

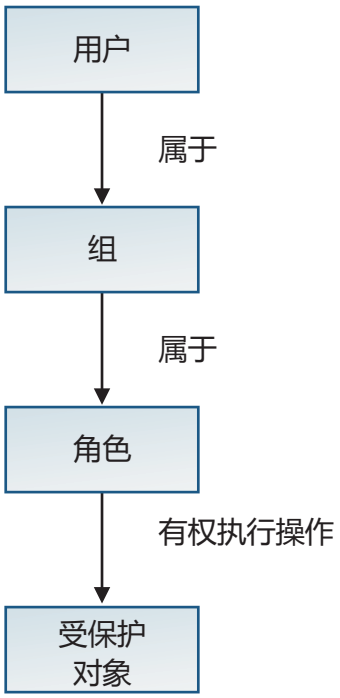

图 4. 用户、组、角色和受保护对象之间的关系

可以使用 WebSphere 集成解决方案控制台 在父组中创建具有不同许可权的子组。但是，IBM Security Key Lifecycle Manager 仅识别父组的许可权，而不识别其子组的许可权。

可用的许可权

安装 IBM Security Key Lifecycle Manager 将创建 SKLMAdmin 用户标识，该标识具有作为缺省超级用户的 `klmSecurityOfficer` 角色。 安装过程还会将预定义的许可权部署到 WebSphere Application Server 管理角色的列表中。

IBM Security Key Lifecycle Manager 的*许可权*启用操作或使用设备组。 IBM Security Key Lifecycle Manager 中的*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*包括 IBM Security Key Lifecycle Manager 许可权和角色。

注: 安装将创建以下缺省组:

klmSecurityOfficerGroup

安装会将 `klmSecurityOfficer` 角色分配给此组。 `klmSecurityOfficer` 角色将替换名为 `klmGroup` 的组中先前的 `klmApplicationRole` 角色。`klmSecurityOfficerGroup` 将替换 `klmGroup`。

`klmSecurityOfficer` 角色具有:

- 对第 33 页的表 4 和第 34 页的表 5 中描述的所有许可权和设备组的 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 提供了 `suppressmonitor` 角色，用于将 IBM Security Key Lifecycle Manager 管理员不使用的任务隐藏在 WebSphere Inte-

grated Solutions Console 的左窗格中。 隐藏项与应用程序服务器相关联，包括安全性、故障诊断以及用户和组文件夹中的 WebSphere Application Server 管理任务。

klmBackupRestoreGroup

备份并恢复 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。

klmGUICLI 访问组

为用户提供到 IBM Security Key Lifecycle Manager 图形用户界面和命令行界面的访问。 每位产品用户必须是该组的一部分。

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产品功能用户。为用户提供其他访问。

具有表 4 中任何一项许可权的用户可以查看:

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

表 4. 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	创建对象，但不能查看、修改或删除对象。		✓
klmDelete	删除对象，但不能查看、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，但不能查看、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、查看和删除空设备组。 此许可权未提供对设备、密钥或证书的访问权。	✓	
klmAudit	使用 **tklmServedDataList** 命令查看审计数据。	✓	

表 4. 操作许可权 (续)

许可权	启用以下操作	与设备组不相关	与设备组相关联
klmBackup	创建和删除 IBM Security Key Lifecycle Manager 数据的备份。	✓	
klmConfigure	读取和更改 IBM Security Key Lifecycle Manager 配置属性，或对 SSL 证书执行操作。 添加、查看、更新或删除密钥库。	✓	
klmRestore	恢复 IBM Security Key Lifecycle Manager 数据的先前备份副本。	✓	

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

表 5. 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（先前称为 GPFS）	IBM Spectrum Scale 设备组
GENERIC	GENERIC 设备系列中的对象。
userdevicegroup	根据预定义的设备系列（例如 LTO）手动创建的用户定义实例，例如 myLTO。

多个许可权

要对设备进行操作，用户必须具有执行一个或多个操作以及访问一个或多个设备组的许可权。

如果用户出现以下情况，可能会发生错误:

具有操作许可权，但没有设备组许可权

例如，用户具有一组操作许可权，包括查看、创建、修改和删除。 但是，用户没有用于接收操作的设备组许可权。

具有设备组许可权，但没有操作许可权

例如，用户具有包括 LTO 和 3592 的设备组许可权。但是，用户没有针对设备组执行操作的许可权。

具有新设备组的新角色，但是没有操作许可权

例如，用户具有为名为 myLTO 的新设备组创建的新角色 myLTO。但是，用户没有其他操作许可权。

许可权可以:

- 直接分配。

  例如，作为用户的角色可能是对特定的设备组具有查看和修改许可权。

- 通过组成员资格获取。

  许可权特定于设备组。 您可能是两个用户组的成员。 例如，一个用户组中的成员资格可能会授予查看和修改许可权以用于 LTO 设备组。而第二个用户组可能会授予查看、创建和修改许可权以用于 3592 设备组。因此您可以查看和修改任一设备组中的设备。 但是，只能对 3592 设备组中的设备完成创建操作。

密钥和证书等数据与设备组相关联。 此类数据仅显示在图形用户界面页面的与数据相关联的设备组中。 具有多个设备组许可权的用户可以更改这些设备组之间数据的关联。

IBM Security Key Lifecycle Manager 数据库中的某些属性与设备组相关联。 例如，IBM Security Key Lifecycle Manager 数据库中的 **symmetricKeySet** 属性与预定义的 LTO 设备组相关联。 要更改该属性，您的角色必须具有执行修改操作的许可权和访问 LTO 设备组的许可权。

用于管理 LTO 磁带机的预定义组

安装 IBM Security Key Lifecycle Manager 将创建用于管理 LTO 磁带机的预定义管理组。 您可以将这些组用作模型以便为其他设备组定义类似的管理组。

LTOAdmin 组:

可以使用 LTOAdmin 组中的成员资格，通过创建、查看、修改、删除、获取（导出）、备份和配置等操作来管理 LTO 设备系列中的设备。

此组包含以下许可权:

表 6. 操作许可权

许可权	启用以下操作
LTO	LTO 设备系列
klmCreate	创建对象，但不能查看、修改或删除对象。
klmDelete	删除对象，但不能查看、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，但不能查看、创建或删除对象。
klmView	查看对象，但不能创建、删除或修改对象。
klmAudit	使用 **tklmServedDataList** 命令查看审计数据。
klmBackup	创建和删除 IBM Security Key Lifecycle Manager 数据的备份。
klmConfigure	读取和更改 IBM Security Key Lifecycle Manager 配置属性，或对 SSL 证书执行操作。
suppressmonitor	将 IBM Security Key Lifecycle Manager 管理员不需要使用的任务隐藏在 WebSphere Integrated Solutions Console 的左窗格中。

LTOOperator 组:

可以使用 LTOOperator 组中的成员资格，通过创建、查看、修改、删除和备份等操作来操作 LTO 设备系列中的设备。

此组包含以下许可权:

表 7. 操作许可权

许可权	启用以下操作
LTO	LTO 设备系列.
klmCreate	创建对象，但不能查看、修改或删除对象。
klmModify	修改对象，但不能查看、创建或删除对象。
klmView	查看对象，但不能创建、删除或修改对象。
klmBackup	创建和删除 IBM Security Key Lifecycle Manager 数据的备份。
suppressmonitor	将 IBM Security Key Lifecycle Manager 管理员不需要使用的任务隐藏在 WebSphere Integrated Solutions Console 的左窗格中。

LTOAuditor 组:

您可以使用 LTOAuditor 组中的成员资格，通过查看和审计等操作对 LTO 设备系列中的设备进行审计。

此组包含以下许可权:

表 8. 操作许可权

许可权	启用以下操作
LTO	LTO 设备系列.
klmView	查看对象，但不能创建、删除或修改对象。
klmAudit	使用 **tklmServedDataList** 命令查看审计数据。
suppressmonitor	将 IBM Security Key Lifecycle Manager 管理员不需要使用的任务隐藏在 WebSphere Integrated Solutions Console 的左窗格中。

WebSphere Application Server 角色

WebSphere Application Server 提供了您可能需要使用的角色。 例如，您可能需要查看或更改 WebSphere Application Server 配置。还可能需要将用户和组分配为管理用户角色和管理组角色。

角色包括监视者、配置者、操作员、管理员、安全管理员和其他角色。

有关更多信息，请在 WebSphere 应用程序服务器文档（http://www-01.ibm.com/support/knowledgecenter/SSAW57_8.5.5/com.ibm.websphere.home.doc_wasinfo_v8r5/welcome_ic_home.html）中搜索*管理角色*。

发行信息

发行信息主题描述特定于此 IBM Security Key Lifecycle Manager 发行版的信息。

系统需求

您的环境必须满足安装 IBM Security Key Lifecycle Manager 的最小系统需求。

有关硬件和软件需求的信息，请参阅 IBM Security Key Lifecycle Manager 的 IBM Knowledge Center 上的“安装和配置”部分。 已发布的硬件和软件需求正值出版物时期。

此外，请参阅系统需求文档的详细信息，地址是 http://pic.dhe.ibm.com/infocenter/prodguid/v1r0/clarity/softwareReqsForProduct.html。

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**。

必备软件

IBM Security Key Lifecycle Manager 具备以下必备软件:

Java 运行时环境 (JRE) 需求

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

在分布式系统上:

IBM Java 运行时环境（包含在 WebSphere Application Server 中）。

在所有系统上，不支持使用由 IBM® 或其他供应商提供的 Java™ 独立安装开发工具包。

运行时环境需求

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

在分布式系统上:

WebSphere Application Server 8.5.5.7 以及所有适用的修订包或 APAR 需求。

IBM Security Key Lifecycle Manager 包含并安装 WebSphere Application Server。在安装期间，IBM Security Key Lifecycle Manager 会修改 WebSphere Application Server。卸载 IBM Security Key Lifecycle Manager 时，此修改行为可能会导致使用相同服务器的产品出现问题。为避免这些问题:

- 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。

数据库权限和需求

IBM Security Key Lifecycle Manager 对数据库的需求取决于使用的操作系统。

- 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 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上安装了 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 必备软件的更多信息，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（例如 Linux 操作系统）的内核设置正确。

在安装应用程序前，请参阅以下 Web 站点上的 DB2 文档以了解这些附加的内核设置:

AIX 系统

不需要。

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）。

Window 系统

不需要。

针对大型环境调整 DB2 缓冲池

您可能需要针对大型环境调整 DB2 缓冲池设置。

使用以下设置:

```
db2 alter bufferpool TKLMBP_LG immediate size 1000 automatic
#---
#--- Use one of the following two statements:
#--- If you migrate from IBM Security Key Lifecycle Manager Version 1,
#--- specify the next statement:
db2 alter bufferpool TKLMBP_4K_IDX immediate size 1000 automatic
#--- Otherwise, omit the statement.

#--- However, if NO migration occurs, specify the next statement:
db2 alter bufferpool TKLMBP_4K_LG_IDX immediate size 1000 automatic
#--- Otherwise, omit the statement.

#---
db2 alter bufferpool TKLMBP_8K_LG immediate size 1000 automatic
```

```
db2 alter bufferpool TKLMBP_32K_LG immediate size 1000 automatic
db2 alter bufferpool TKLMBP_SM immediate size 1000 automatic
db2 alter bufferpool TKLMBP_IDX immediate size 1000 automatic
db2 alter bufferpool TKLMBP_32K_IDX immediate size 1000 automatic
db2 alter bufferpool TKLMBP_SCH immediate size 1000 automatic
```

安装映像和修订包

对于分布式系统，请通过访问 IBM Passport Advantage® Web 站点获取 IBM Security Key Lifecycle Manager 安装文件和修订包。 您还可以使用其他方法（例如 IBM 销售代表提供的 DVD）来获取文件。

Passport Advantage Web 站点为各种 IBM 产品提供称之为 eAssemblies 的软件包。

“修订中心”Web 站点为软件、硬件和您系统的操作系统提供修订和更新。 IBM Security Key Lifecycle Manager 修订包发布在“修订中心”Web 站点。

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。

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

根据以下条款和条件授予使用这些出版物的许可权。

适用性 这些条款和条件以及 IBM Web 站点的任何使用条款。

个人使用

您可以为了个人使用而非商业性使用复制这些出版物，但前提是保留所有专有权声明。未经 IBM 的明确许可，您不得分发、显示这些出版物或其中部分出版物，也不得制作其演绎作品。

商业使用

您仅可在贵公司内部复制、分发和显示这些出版物，但前提是保留所有专有权声明。未经 IBM 的明确许可，您不得制作这些出版物的演绎作品，也不得在贵公司外部复制、分发或显示这些出版物或其部分出版物。

权利 除非本许可权中明确授予，否则不得授予对这些出版物或其中包含的任何信息、数据、软件或其他知识产权的任何许可权、许可证或权利，无论明示的还是暗含的。

只要 IBM 认为这些出版物的使用会损害其利益或者 IBM 判定未正确遵守上述指示信息，IBM 将有权撤销此处授予的许可权。

只有您完全遵循所有适用的法律和法规，包括所有的美国出口法律和法规，您才可以下载、出口或再出口该信息。

IBM 对这些出版物的内容不作任何保证。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性、非侵犯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。Web http://www.ibm.com/legal/copytrade.shtml 上提供了 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

[H]

[J]

[K]

[M]

[P]

[Q]

[S]

[W]