管理

IBM

目录

管理

管理是一组任务，通过完成这些任务，您可以准备然后监视 IBM Security Key Lifecycle Manager 环境。

管理活动包括管理密钥、证书和设备之类的任务。

配置设置

IBM Security Key Lifecycle Manager 提供了一组操作，用于更改 IBM Security Key Lifecycle Manager 配置。

例如，您可以更改下列过程的缺省值:

- 用于 TCP 和 SSL 通信的端口或超时值
- 提供了更多日志信息的审计级别
- 用于生成调试日志的调试设置
- 针对自动克隆复制的配置设置

指定 SSL 或 KMIP 证书

您必须指定要用作服务器通信证书的自签名证书。另外，您可以创建证书请求并手动将请求发送到认证中心 (CA) 以进行签名。例如，您可以使用证书向 IBM Security Key Lifecycle Manager 与磁带库之间的通信添加保护。 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。

关于此任务

您可以使用“用于密钥提供的 SSL/KMIP”页面来指定 IBM Security Key Lifecycle Manager 所使用的证书的类型。另外，您还可以使用下列任何 CLI 命令或 REST 界面:

- **tklmCertCreate** 或 **tklmCertGenRequest**
- **Certificate Generate Request REST Service** 或 **Create Certificate REST Service**

您的角色必须具有执行配置操作的许可权，才能创建 SSL 或 KMIP 证书。

开始之前，请确定:

- 您能否在项目中的某个阶段（例如测试阶段）使用自签名证书。
- 发送请求之后，接收 CA 发放的证书所需的时间间隔。 您必须手动向发放中心发送证书请求。
- 您的站点是否需要合作伙伴证书，以便将其用于业务合作伙伴或供应商，或者实现灾难复原目的。
- 证书有效性时间间隔的常规设置（以天计）。

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。 单击 **IBM Security Key Lifecycle Manager** > **配置** > **SSL/KMIP**。
   - 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. 创建一个或多个证书或证书请求:
   - 图形用户界面

     选择是生成自签名证书，还是请求从第三方提供者获取证书。另外，还有一个证书选项，即，使用密钥库中的现有证书。 请填写必填字段和可选字段，然后单击**确定**。
   - 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]')
     ```

     您也可以请求从认证中心获取证书。例如，输入:

     ```
     print AdminTask.tklmCertGenRequest('[-alias sklmSSLCertificate1
      -cn sklm -ou sales -o myCompanyName -locality myLocation
       -country US -validity 999 -keyStoreName defaultKeyStore
        -fileName mySSLCertRequest1.crt -usage SSLSERVER]')
     ```
   - REST 界面
     a. 获取用于访问 IBM Security Key Lifecycle Manager REST 服务的唯一用户认证标识。 有关认证过程的更多信息，请参阅 REST 服务的验证流程。
     b. 要调用 **Certificate Generate Request REST Service**，请发送 HTTP POST 请求。请将您在步骤 a 中获取的用户认证标识随请求消息一起传递，如以下示例所示。

        ```
        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 "  }
```

请发送以下 HTTP 请求，以便从认证中心获取证书:

```
POST https://localhost:9080/SKLM/rest/v1/certificates
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth authId=139aeh34567m
{"type":"certreq","alias":"sklmCert","cn":"sklm",
"ou":"sales","o":
"myCompanyName","usage":"3592","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:

     在“成功”页面上的“下一步”中，单击要执行的相关任务。如果创建自签名证书，那么可能要重新启动服务器并创建备份来确保可以复原此数据。
   - 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

转至“欢迎”页面，并配置组织需要的磁带机类型以及密钥或证书。

指定审计信息的级别

您可以更改 IBM Security Key Lifecycle Manager 用于收集审计信息的缺省设置。

关于此任务

您可以使用“审计”页面来更改写入审计日志的信息级别。 另外，您还可以使用下列 CLI 命令或 REST 界面来列出或更改 SKLMConfig.properties 文件中的 **Audit.event.types** 特性:

- **tklmConfigGetEntry** 和 **tklmConfigUpdateEntry**
- **Get Single Config Property REST Service** 和 **Update Config Property REST Service**

您的角色必须具有执行配置操作的许可权。

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。 单击 **IBM Security Key Lifecycle Manager** > **配置** > **审计和调试**。
   - 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. 更改审计信息级别的值:
   - 在图形用户界面中，为“审计”设置选择“低”、“中等”或“高”值，然后单击**确定**。

     低 存储最少的审计记录。

     选择**低**会在 SKLMConfig.properties 文件中设置下列特性值:

     – Audit.event.types = runtime, authorization, authorization_terminate, resource_management, key_management

     – Audit.event.outcome = failure

     中等（缺省值）
     存储中间数目的审计记录。

     选择**中等**会在 SKLMConfig.properties 文件中设置下列特性值:

     – Audit.event.types = runtime,authorization,authorization_terminate, resource_management, key_management

     – Audit.event.outcome = success,failure

     高 存储最大数目的审计记录。

     选择**高**会在 SKLMConfig.properties 文件中设置下列特性值:

     – Audit.event.types = all

     – Audit.event.outcome = success,failure

   - 命令行界面:
     a. 在一行上输入 **tklmConfigGetEntry** 命令，以获取 SKLMConfig.properties 文件中的目标特性的当前值。例如，要确定将包含在审计日志中的事件类型，请在一行上输入以下命令:

     ```
     wsadmin>print AdminTask.tklmConfigGetEntry
      ('[-name Audit.event.types]')
     ```

     示例响应可能如下:

     ```
     All
     ```

     b. 指定必需更改。 例如，要将选择限制为两种要存储在审计日志中的事件类型，请在一行上输入以下命令:

     ```
     print AdminTask.tklmConfigUpdateEntry
      ('[-name Audit.event.types -value runtime,audit_management]')
     ```

   - REST 界面:

a. 获取用于访问 IBM Security Key Lifecycle Manager REST 服务的唯一用户认证标识。 有关认证过程的更多信息，请参阅 REST 服务的验证流程。

b. 要调用 **Get Single Config Property REST Service**，请发送 HTTP GET 请求。请将您在步骤 a 中获取的用户认证标识随请求消息一起传递，如以下示例所示。

```
GET https://localhost:9080/SKLM/rest/v1/configProperties/
Audit.event.types
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth userAuthId=139aeh34567m
Accept-Language : en
```

成功响应可能如下:

```
Status Code : 200 OK
Content-Language: en
{"property":"Audit.event.types","value":"all"}
```

c. 指定必需更改。 例如，您可以通过发送以下 HTTP 请求，使用 **Update Config Property REST Service** 将选择限制为两种要存储在审计日志中的事件类型:

```
PUT https://localhost:9080/SKLM/rest/v1/configProperties
Content-Type: application/json
Accept: application/json
Authorization: SKLMAuth authId=139aeh34567m
Accept-Language: en
{ "Audit.event.types": "runtime,audit_management"}
```

3. 成功指示符会根据界面的不同而不同:

- 图形用户界面

  在“成功”页面上的“下一步”中，单击要执行的相关任务。

- 命令行界面

  完成消息表示成功。

- REST 界面:

  状态码 200 OK 表示成功。

下一步做什么

您可以重新运行先前返回了错误的操作。 然后，查看审计日志以获取更多信息。 有关审计记录的详细信息，请参阅 IBM Security Key Lifecycle Manager 文档中的“分布式系统上的审计记录”主题。

生成系统日志格式的审计记录

您可以生成系统日志格式的审计记录，然后将这些记录发送到系统日志服务器。 使用 IBM Security Key Lifecycle Manager 图形用户界面来进行配置，以生成系统日志格式的审计记录。

关于此任务

在下列情况下，审计日志消息将以系统日志格式写入已配置的本地审计文件:

- 对审计消息启用了系统日志格式。
- 启用了系统日志格式，并且未指定系统日志服务器主机名和端口号。

- 启用了系统日志格式，指定了系统日志服务器主机名和端口号，但无法访问该服务器主机名或端口号。

过程

1. 登录图形用户界面。
2. 单击 **IBM Security Key Lifecycle Manager** > **配置** > **审计和调试**。
3. 选择**使用系统日志格式**。
4. 在**系统日志服务器主机**中指定服务器主机名或 IP 地址。
5. 在**系统日志服务器端口**中指定系统日志服务器用于侦听请求的端口号。
6. 如果需要使用 SSL/TLS 传输协议来实现审计信息到系统日志服务器的安全传输，请选择**使用 SSL/TLS**。
7. 单击**确定**。

下一步做什么

使用必需参数对审计记录启用系统日志格式之后，仅当您选择了**使用 SSL/TLS** 时，才必须运行下列步骤:

1. 如果尚未创建 IBM Security Key Lifecycle Manager SSL 服务器证书，请创建该证书。要创建证书，您可以使用图形用户界面上的“用于提供密钥的 SSL/KMIP”页面、**Create Certificate REST Service** 或 **tklmCertCreate** CLI 命令。
2. 将 IBM Security Key Lifecycle Manager SSL 服务器证书导出到文件。 要导出证书，您可以使用 **Certificate Export REST Service** 或 **tklmCertExport** CLI 命令。

   要导出服务器证书，而尚未创建证书，请从步骤 1 中获取服务器证书别名。 如果已创建证书，请从图形用户界面转至**高级配置** > **服务器证书**。 别名是标记为正在使用的证书的**证书**列值。
3. 以文件形式获取系统日志服务器证书并将其导入，然后在 IBM Security Key Lifecycle Manager 服务器中信任该系统日志服务器证书。使用 **tklmCertImport** CLI 命令或 **Certificate Import REST Service** 可以通过使用 SYSLOG 导入该证书。
4. 将 IBM Security Key Lifecycle Manager 服务器证书导入到系统日志服务器。 请使用步骤 2 中创建的证书文件。
5. 在配置属性文件中设置IBM Security Key Lifecycle Manager SSL 服务器证书别名。

   注: 如果 IBM Security Key Lifecycle Manager SSL 服务器证书是使用图形用户界面创建的，那么无需执行此步骤。
   例如:

   命令行界面

   ```
   print AdminTask.tklmConfigUpdateEntry('[-name config.keystore.ssl.
   certalias -value <alias of the server certificate that is
   created in Step 1>]')
   ```

   REST 界面

   ```
   PUT https://localhost:9080/SKLM/rest/v1/configProperties
   Content-Type: application/json
   Accept : application/json
   Authorization: SKLMAuth userAuthId=139aeh34567m
   Accept-Language : en
   { "config.keystore.ssl.certalias" : "<alias of the server
   certificate that is created in Step 1>"}
   ```

6. 重新启动 IBM Security Key Lifecycle Manager 服务器。

指定调试信息设置

您可以更改 IBM Security Key Lifecycle Manager 用于收集调试信息的缺省设置。 调试日志文件提供附加信息来分析 IBM Security Key Lifecycle Manager 问题并对这些问题进行故障诊断。

关于此任务

您可以使用“审计”页面的“调试”部分来指定用于生成调试信息的设置。 另外，您还可以使用下列 CLI 命令或 REST 界面来列出或更改 SKLMConfig.properties 文件中的 **debug** 特性:

- **tklmConfigGetEntry** 和 **tklmConfigUpdateEntry**
- **Get Single Config Property REST Service** 和 **Update Config Property REST Service**

您的角色必须具有执行配置操作的许可权。

注: 启用调试日志记录可能会影响 IBM Security Key Lifecycle Manager 性能。请仅在 IBM 支持代表提供指导的情况下启用此选项。

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。 单击 **IBM Security Key Lifecycle Manager** > **配置** > **审计和调试**。
   - 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. 更改设置以生成调试信息:
   - 在图形用户界面中:
     a. 选择**启用调试**，以便在 SKLMConfig.properties 文件中设置下列特性值:

        ```
        debug=all
        ```
     b. 单击**确定**。
   - 命令行界面:

a. 在一行上输入 **tklmConfigGetEntry** 命令，以获取 SKLMConfig.properties 文件中的目标特性的当前值。例如，要确定 debug 的值，请在一行上输入以下命令:

```
wsadmin>print AdminTask.tklmConfigGetEntry
 ('[-name debug]')
```

示例响应可能如下:

```
none
```

b. 指定新的特性值。 例如，要指定值 all 以生成调试日志，请在一行上输入以下命令:

```
print AdminTask.tklmConfigUpdateEntry
 ('[-name debug -value all]')
```

- REST 界面:

a. 获取用于访问 IBM Security Key Lifecycle Manager REST 服务的唯一用户认证标识。 有关认证过程的更多信息，请参阅 REST 服务的验证流程。

b. 要调用 **Get Single Config Property REST Service**，请发送 HTTP GET 请求。请将您在步骤 a 中获取的用户认证标识随请求消息一起传递，如以下示例所示。

```
GET https://localhost:9080/SKLM/rest/v1/configProperties/debug
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth userAuthId=139aeh34567m
Accept-Language : en
```

成功响应可能如下:

```
Status Code : 200 OK
Content-Language: en
{"property":"debug","value":"none"}
```

c. 指定新的特性值。 然后，发送以下 HTTP 请求:

```
PUT https://localhost:9080/SKLM/rest/v1/configProperties
Content-Type: application/json
Accept: application/json
Authorization: SKLMAuth authId=139aeh34567m
Accept-Language: en
{ "debug": "all"}
```

3. 成功指示符会根据界面的不同而不同:

- 图形用户界面

在“成功”页面上的“后续步骤”下，单击要运行的相关任务。

- 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。

指定密钥提供参数

您可以更改 IBM Security Key Lifecycle Manager 提供的缺省证书设置。

关于此任务

使用“密钥提供参数”页面来更改证书设置。 另外，您还可以使用下列 CLI 命令或 REST 界面来列出或更改 SKLMConfig.properties 文件中的相应特性:

- **tklmConfigGetEntry** 和 **tklmConfigUpdateEntry**
- **Get Single Config Property REST Service** 和 **Update Config Property REST Service**

您的角色必须具有执行配置操作的许可权。

开始之前，请确定:

- 是否在提供密钥之前执行证书日期验证。执行验证可以确认证书有效且未到期。
- 是否使用证书中存储的主体密钥标识来标识证书。

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。 单击 **IBM Security Key Lifecycle Manager** > **配置** > **密钥提供参数**。
   - 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. 更改一项或多项证书设置的值:
   - 在图形用户界面中，更改下列一项或多项设置，然后单击**确定**:

     对于写请求或数据写入，不要使用到期证书。

     提供密钥前，请确认包含此密钥的一个或多个证书未到期。到期证书仅用于读请求。 启用此设置时，到期证书将不会用于写请求。 选中此复选框会将 SKLMConfig.properties 文件中 **cert.valiDATE** 属性的值更改为 true。

     保持暂挂客户机设备通信证书。

     在接受来自客户机设备的通信证书以用于设备与 IBM Security Key Lifecycle Manager 服务器 之间的安全通信之前，使这些证书保持暂挂。如果禁用此设置，那么必须手动导入客户机设备通信证书。 此配置参数与 SKLMConfig.properties 文件中处于暂挂状态的客户机设备的 **enableClientCertPush** 属性值相关联。

用证书名称来识别证书。

使用存储在证书中的证书名称（而不是使用主题密钥标识）来识别证书。 您可以在创建证书时指定证书名称。 此功能可用于解密已写入设备的数据。

如果禁用此项，读取盒带或其他设备上的数据时，将使用“主题密钥标识”来确定要使用的证书。 此配置参数与 SKLMConfig.properties 文件中 **useSKIDefaultLabels** 属性的值相关联。

- 命令行界面:
  a. 在一行上输入 **tklmConfigGetEntry** 命令，以获取 SKLMConfig.properties 文件中的目标特性的当前值。例如，输入:

     ```
     wsadmin>print AdminTask.tklmConfigGetEntry
      ('[-name zOSCompatibility]')
     ```

     示例响应可能如下:

     ```
     False
     ```

  b. 指定必需更改。 例如，要将 **zOSCompatibility** 特性的值更改为 true，请在一行上输入以下命令:

     ```
     print AdminTask.tklmConfigUpdateEntry
      ('[-name zOSCompatibility -value true]')
     ```

- REST 界面:
  a. 获取用于访问 IBM Security Key Lifecycle Manager REST 服务的唯一用户认证标识。 有关认证过程的更多信息，请参阅 REST 服务的验证流程。
  b. 要调用 **Get Single Config Property REST Service**，请发送 HTTP GET 请求。请将您在步骤 a 中获取的用户认证标识随请求消息一起传递，如以下示例所示。

     服务请求

     ```
     GET https://localhost:9080/SKLM/rest/v1/configProperties/
     zOSCompatibility
     Content-Type: application/json
     Accept: application/json
     Authorization: SKLMAuth userAuthId=139aeh34567m
     Accept-Language: en
     ```

     成功响应

     ```
     Status Code : 200 OK
     Content-Language: en
     {"zOSCompatibility" : "False"}
     ```

  c. 指定必需更改。 例如，您可以发送以下服务请求，以便将 **zOSCompatibility** 特性的值更改为 true:

     ```
     PUT https://localhost:9080/SKLM/rest/v1/configProperties
     Content-Type: application/json
     Accept: application/json
     Authorization: SKLMAuth authId=139aeh34567m
     Accept-Language: en
     { "zOSCompatibility": "true"}
     ```

3. 成功指示符会根据界面的不同而不同:
   - 图形用户界面:

     在“成功”页面上的“下一步”中，单击要执行的相关任务。

   - 命令行界面:

完成消息表示成功。

- REST 界面:

  状态码 200 OK 表示成功。

下一步做什么

对证书设置的更改以动态方式发生。 接下来，您可以创建所需证书并将其与特定设备进行关联。

确定当前端口号

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

关于此任务

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

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

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

指定端口和超时设置

您可以更改 IBM Security Key Lifecycle Manager 提供的缺省端口和超时设置。

关于此任务

您可以使用“密钥提供参数”页面来更改端口和超时设置。 另外，您还可以使用下列 CLI 命令或 REST 服务来列出和更改 SKLMConfig.properties 文件中的相应特性:

- **tklmConfigGetEntry** 和 **tklmConfigUpdateEntry**
- **Get Single Config Property REST Service** 和 **Update Config Property REST Service**

开始之前，请确定站点中是否存在阻止使用 IBM Security Key Lifecycle Manager 缺省值的端口或超时冲突。 您的角色必须具有执行配置操作的许可权。

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。 单击 **IBM Security Key Lifecycle Manager** > **配置** > **密钥提供端口**。
   - 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. 更改端口或超时设置的值:
   - 在图形用户界面中，更改下列一项或多项设置，然后单击**确定**:

     TCP 端口

     IBM Security Key Lifecycle Manager 使用缺省端口 3801。 值范围从 1 到 65535。 您设置的值也将更改 SKLMConfig.properties 文件中 **TransportListener.tcp.port** 属性的值。您必须确保没有其他应用程序已经在使用该端口。

     TCP 超时（以分钟为单位）

     IBM Security Key Lifecycle Manager 使用缺省超时值 10 分钟。 值范围从 1 到 120。 您设置的值也将更改 SKLMConfig.properties 文件中 **TransportListener.tcp.timeout** 属性的值。

     SSL 端口

     IBM Security Key Lifecycle Manager 使用缺省端口 441。 值范围从 1 到 65535。 您设置的值也将更改 SKLMConfig.properties 文件中 **TransportListener.ssl.port** 属性的值。

     SSL 超时（以分钟为单位）

     IBM Security Key Lifecycle Manager 使用缺省超时值 10 分钟。 值范围从 1 到 120。 此配置参数与 SKLMConfig.properties 文件中 **TransportListener.ssl.timeout** 属性的值相关联。

     KMIP SSL 端口

     KMIP 使用缺省端口 5696。值的范围为 1 到 65535。 此配置参数与 SKLMConfig.properties 文件中 **KMIPListener.ssl.port** 属性的值相关联。

   - 命令行界面:
     a. 在一行上输入 **tklmConfigGetEntry** 命令，以获取 SKLMConfig.properties 文件中的目标特性的当前值。例如，在一行上输入:

     ```
     wsadmin>print AdminTask.tklmConfigGetEntry
      ('[-name TransportListener.tcp.port]')
     ```

     示例响应可能如下:

     ```
     3801
     ```

     b. 指定必需更改。 例如，要指定另一 TCP 端口号，请在一行上输入以下命令:

     ```
     print AdminTask.tklmConfigUpdateEntry
      ('[-name TransportListener.tcp.port -value 3802]')
     ```

- REST 界面:
  a. 获取用于访问 IBM Security Key Lifecycle Manager REST 服务的唯一用户认证标识。 有关认证过程的更多信息，请参阅 REST 服务的验证流程。
  b. 要调用 **Get Single Config Property REST Service**，请发送 HTTP GET 请求。请将您在步骤 a 中获取的用户认证标识随请求消息一起传递，如以下示例所示。

     服务请求

     ```
     GET https://localhost:9080/SKLM/rest/v1/configProperties/
     TransportListener.tcp.port
     Content-Type: application/json
     Accept: application/json
     Authorization: SKLMAuth userAuthId=139aeh34567m
     Accept-Language: en
     ```

     成功响应

     ```
     Status Code : 200 OK
     Content-Language: en
     {"TransportListener.tcp.port" : "3801"}
     ```

  c. 指定必需更改。 例如，要指定另一 TCP 端口号，请发送以下服务请求:

     ```
     PUT https://localhost:9080/SKLM/rest/v1/configProperties
     Content-Type: application/json
     Accept: application/json
     Authorization: SKLMAuth authId=139aeh34567m
     Accept-Language: en
     {"TransportListener.tcp.port": "3802"}
     ```

3. 成功指示符会根据界面的不同而不同:
   - 图形用户界面:

     更新页面会显示您输入的信息。
   - 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

要使端口号之类的更改生效，请重新启动 IBM Security Key Lifecycle Manager 服务器。

克隆服务器和主服务器的复制设置

要设置 IBM Security Key Lifecycle Manager 自动克隆复制过程，您必须针对主服务器和克隆服务器配置复制参数。

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服务器的操作系统和目录结构的方式将 IBM Security Key Lifecycle Manager 环境克隆到多台服务器。 例如，可以将 Windows 系统上的主服务器中的数据复制到 Linux 系统上的克隆服务器。

主服务器配置

主服务器是将要复制的主系统。 仅当向主服务器添加了新密钥时，才会触发复制过程。 您最多可以与 20 台克隆服务器一起复制主服务器。每台克隆服务器通过 IP 地址或主机名以及端口号进行标识。 该服务器使用 ReplicationSKLMConfig.properties 文件中的特性来控制复制过程。 有关复制配置文件的更多信息，请参阅复制配置文件。

您还可以使用 IBM Security Key Lifecycle Manager 复制程序来安排自动备份操作。 必须仅针对主服务器配置特性以定期备份数据。

克隆服务器配置

复制过程支持将 IBM Security Key Lifecycle Manager 环境从主服务器克隆到多台克隆服务器。 克隆服务器使用 ReplicationSKLMConfig.properties文件中的特性来控制复制过程。 触发复制过程后，以下数据将复制到克隆服务器:

- IBM Security Key Lifecycle Manager 数据库表中的数据
- 信任库以及主密钥所在的密钥库
- IBM Security Key Lifecycle Manager 配置文件

指定主服务器的复制参数

您可以更改主服务器的缺省设置以便与克隆服务器通信，从而复制 IBM Security Key Lifecycle Manager 数据。

关于此任务

使用“自动克隆复制配置”页面来配置复制设置。 另外，您还可以使用下列 CLI 命令或 REST 界面来更改 ReplicationSKLMConfig.properties 配置文件中的相应特性:

- **tklmReplicationConfigGetEntry** 和 **tklmReplicationConfigUpdateEntry**
- **Get Single Replication Config Properties REST Service** 和 **Update Replication Config Property REST Service**

注: 仅当向主服务器添加了新密钥时，才会将数据复制到克隆服务器。

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. 单击 **IBM Security Key Lifecycle Manager** > **配置** > **复制**。
   - 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. 更改主服务器的一项或多项设置的值:
   - 在图形用户界面中:
     a. 选择**主**。
     b. 指定相应的设置:

基本特性

来自密钥库的证书	从列表中选择证书。 SSL/TLS 证书必须在主系统以及所有进行了复制配置的克隆系统上存在。
复制备份加密口令	这是备份文件的加密密码，用于确保数据安全。 您需要同一密码来解密和复原文件。
确认复制备份加密口令	再次指定同一密码以验证输入是否正确。
主侦听端口	发生非序列化或延迟复制时，用于通信的端口号。 缺省主侦听端口为 1111。
克隆 - 1 IP 或主机名	克隆服务器的 IP 地址或主机名。您只能在一台主服务器与多达 20 台克隆服务器之间进行复制。 单击**添加克隆**链接可以为多个克隆配置复制设置。
克隆 - 1 端口	这是用于将备份文件发送到克隆服务器的端口号。 每台克隆服务器都通过端口号进行标识。克隆服务器的缺省端口号为 2222。

高级特性

复制备份目标目录	这是用于存储备份文件的位置。 缺省目标目录为 *<WAS_HOME>*\products\sklm\restores。
在回滚之前要保留的最大复制文件数	您希望保留的最大复制文件数。 值必须是介于 2 与 10 之间的正整数。文件数超出指定限制后，系统将删除最旧的文件。
复制频率（以小时计）	这是检查是否需要执行备份操作的频率。 缺省值设置为 1 小时。 如果设置了**每天开始复制时间**值，那么将忽略此参数。
每天复制时间（格式为 HH:MM）	每天运行复制任务的时间，格式为 HH:MM。
复制日志文件名	复制日志文件的名称和位置。此参数的缺省值为 *<WAS_HOME>*\products\sklm\logs\replication。
最大日志文件大小 (KB)	发生回滚之前，日志文件的最大大小。缺省值为 1000 KB（千字节）。 文件达到最大大小后，系统将创建新的日志文件。
要保留的最大日志文件数	您希望保留的最大日志文件数。 缺省情况下，IBM Security Key Lifecycle Manager 保留最后 3 个日志文件。 文件数超出指定限制后，系统将删除最旧的文件。

     c. 单击**确定**。
   - 命令行界面:
     a. 在一行上输入 **tklmReplicationConfigGetEntry** 命令，以获取 ReplicationSKLMConfig.properties 文件中的目标特性的当前值。例如，输入以下命令:

```
wsadmin>print AdminTask.tklmReplicationConfigGetEntry
 ('[-name replication.role]')
```

示例响应可能如下:

```
none
```

b. 指定更改。 例如，要将 **replication.role** 特性的值更改为 master，请在一行上输入以下命令:

```
print AdminTask.tklmReplicationConfigUpdateEntry
 ('[-name replication.role -value master]')
```

- REST 界面:

a. 获取用于访问 IBM Security Key Lifecycle Manager REST 服务的唯一用户认证标识。 有关认证过程的更多信息，请参阅 REST 服务的验证流程。

b. 要调用 **Get Single Config Property REST Service**，请发送 HTTP GET 请求。请将您在步骤 a 中获取的用户认证标识随请求消息一起传递，如以下示例所示。

服务请求

```
GET https://localhost:9080/SKLM/rest/v1/configProperties/
replication.role
Content-Type: application/json
Accept: application/json
Authorization: SKLMAuth userAuthId=139aeh34567m
Accept-Language: en
```

成功响应

```
Status Code : 200 OK
Content-Language: en
{"replication.role" : "none"}
```

c. 指定更改。 例如，您可以使用 **Update Replication Config Property REST Service** 发送以下服务请求，以更改 **replication.role** 特性的值。

```
PUT https://localhost:9080/SKLM/rest/v1/configProperties
Content-Type: application/json
Accept: application/json
Authorization: SKLMAuth authId=139aeh34567m
Accept-Language: en
{ "replication.role": "master"}
```

3. 成功指示符会根据界面的不同而不同:

- 图形用户界面:

  主服务器的“自动克隆复制配置”页面上显示更新后的配置信息。

- 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

您可能希望更改克隆服务器的设置，使其接收来自主服务器的备份文件。

指定克隆服务器的复制参数

您可以更改克隆服务器的缺省设置，使其在用户将新密钥添加到主服务器时自动接收来自主服务器的备份文件。

关于此任务

使用“自动克隆复制配置”页面来更改复制设置。 另外，您还可以使用下列 CLI 命令或 REST 界面来列出或更改 ReplicationSKLMConfig.properties 配置文件中的相应特性:

- **tklmReplicationConfigGetEntry** 和 **tklmReplicationConfigUpdateEntry**
- **Get Single Replication Config Properties REST Service** 和 **Update Replication Config Property REST Service**

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. 单击 **IBM Security Key Lifecycle Manager** > **配置** > **复制**。
   - 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. 更改克隆服务器的一项或多项设置的值:
   - 在图形用户界面中:
     a. 选择**克隆**。
     b. 指定相应的设置:

基本特性

克隆侦听端口	克隆服务器必须进行侦听以接收备份文件的端口号。 缺省端口号为 2222。
主侦听端口	发生非序列化或延迟复制时，用于通信的端口号。 缺省主侦听端口为 1111。

高级特性

复原失败时的重试次数	第一次复原操作失败之后，允许的最大重试次数。 值必须是介于 0 与 2 之间的正整数。
复制日志文件名	复制日志文件的名称和位置。此参数的缺省值为 *<WAS_HOME>*\products\sklm\logs\replication。
最大日志文件大小 (KB)	发生回滚之前，日志文件的最大大小。缺省值为 1000 KB（千字节）。 文件达到最大大小后，系统将创建新的日志文件。

要保留的最大日志文件数	您希望保留的最大日志文件数。 缺省情况下，IBM Security Key Lifecycle Manager 保留最后 3 个日志文件。 文件数超出指定限制后，系统将删除最旧的文件。

c. 单击**确定**。

- 命令行界面:

a. 在一行上输入 **tklmReplicationConfigGetEntry** 命令，以获取 ReplicationSKLMConfig.properties 文件中的目标特性的当前值。例如，输入以下命令:

```
wsadmin>print AdminTask.tklmReplicationConfigGetEntry
 ('[-name replication.role]')
```

示例响应可能如下:

```
none
```

b. 指定更改。 例如，要将 **replication.role** 特性的值更改为 clone，请在一行上输入以下命令:

```
print AdminTask.tklmReplicationConfigUpdateEntry
 ('[-name replication.role -value clone]')
```

- REST 界面:

a. 获取用于访问 IBM Security Key Lifecycle Manager REST 服务的唯一用户认证标识。 有关认证过程的更多信息，请参阅 REST 服务的验证流程。

b. 要调用 **Get Single Config Property REST Service**，请发送 HTTP GET 请求。请将您在步骤 a 中获取的用户认证标识随请求消息一起传递，如以下示例所示。

服务请求

```
GET https://localhost:9080/SKLM/rest/v1/configProperties/
replication.role
Content-Type: application/json
Accept: application/json
Authorization: SKLMAuth userAuthId=139aeh34567m
Accept-Language: en
```

成功响应

```
Status Code : 200 OK
Content-Language: en
{"replication.role" : "none"}
```

c. 指定更改。 例如，您可以使用 **Update Replication Config Property REST Service** 发送以下服务请求，以更改 **replication.role** 特性的值。

```
PUT https://localhost:9080/SKLM/rest/v1/configProperties
Content-Type: application/json
Accept: application/json
Authorization: SKLMAuth authId=139aeh34567m
Accept-Language: en
{ "replication.role": "clone"}
```

3. 成功指示符会根据界面的不同而不同:

- 克隆服务器的“自动克隆复制配置”页面上显示更新后的配置信息。
- 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

您可能希望更改其他克隆服务器的设置。 您可以将 IBM Security Key Lifecycle Manager 数据从主要主服务器复制到多达 20 台辅助克隆服务器。

安排自动备份操作

您可以配置复制设置以自动运行备份操作，从而确保定期备份 IBM Security Key Lifecycle Manager 关键数据。

关于此任务

您可以使用 IBM Security Key Lifecycle Manager 复制程序来安排自动备份操作。 必须仅针对主服务器配置特性以定期备份数据。

使用“自动克隆复制配置”页面来针对主服务器配置设置。 另外，您还可以使用下列 CLI 命令或 REST 界面来更改 ReplicationSKLMConfig.properties 配置文件中的相应特性:

- **tklmReplicationConfigGetEntry** 和 **tklmReplicationConfigUpdateEntry**
- **Get Single Replication Config Properties REST Service** 和 **Update Replication Config Property REST Service**

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. 单击 **IBM Security Key Lifecycle Manager** > **配置** > **复制**。
   - 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. 更改主服务器的一项或多项设置的值:
   - 在图形用户界面中:
     – 选择**主**。
     – 配置设置:

       基本特性

来自密钥库的证书	从列表中选择证书。 SSL/TLS 证书必须在主系统以及所有进行了复制配置的克隆系统上存在。
复制备份加密口令	这是备份文件的加密密码，用于确保数据安全。 您需要同一密码来解密和复原文件。
确认复制备份加密口令	再次指定同一密码以验证输入是否正确。
主侦听端口	发生非序列化或延迟复制时，用于通信的端口号。 缺省主侦听端口为 1111。

高级特性

复制备份目标目录	这是用于存储备份文件的位置。 缺省目标目录为 *<WAS_HOME>*\products\sklm\restores。
在回滚之前要保留的最大复制文件数	您希望保留的最大复制文件数。 值必须是介于 2 与 10 之间的正整数。文件数超出指定限制后，系统将删除最旧的文件。
复制频率（以小时计）	这是检查是否需要执行备份操作的频率。 缺省值设置为 1 小时。 如果设置了**每天开始复制时间**值，那么将忽略此参数。
每天复制时间（格式为 HH:MM）	每天运行复制任务的时间，格式为 HH:MM。
复制日志文件名	复制日志文件的名称和位置。此参数的缺省值为 *<WAS_HOME>*\products\sklm\logs\replication。
最大日志文件大小 (KB)	发生回滚之前，日志文件的最大大小。缺省值为 1000 KB（千字节）。 文件达到最大大小后，系统将创建新的日志文件。
要保留的最大日志文件数	您希望保留的最大日志文件数。 缺省情况下，IBM Security Key Lifecycle Manager 保留最后 3 个日志文件。 文件数超出指定限制后，系统将删除最旧的文件。

– 单击**确定**。

- 命令行界面:
  a. 在一行上输入 **tklmReplicationConfigGetEntry** 命令，以获取 ReplicationSKLMConfig.properties 文件中的目标特性的当前值。例如，输入:

     ```
     wsadmin>print AdminTask.tklmReplicationConfigGetEntry
      ('[-name replication.role]')
     ```

     示例响应可能如下:

     ```
     none
     ```

  b. 指定更改。 例如，要将 **replication.role** 特性的值更改为 master，请在一行上输入以下命令:

     ```
     print AdminTask.tklmReplicationConfigUpdateEntry
      ('[-name replication.role -value master]')
     ```

- REST 界面:
  a. 获取用于访问 IBM Security Key Lifecycle Manager REST 服务的唯一用户认证标识。 有关认证过程的更多信息，请参阅 REST 服务的验证流程。
  b. 要调用 **Get Single Config Property REST Service**，请发送 HTTP GET 请求。请将您在步骤 a 中获取的用户认证标识随请求消息一起传递，如以下示例所示。

服务请求

```
GET https://localhost:9080/SKLM/rest/v1/configProperties/
replication.role
Content-Type: application/json
Accept: application/json
Authorization: SKLMAuth userAuthId=139aeh34567m
Accept-Language: en
```

成功响应

```
Status Code : 200 OK
Content-Language: en
{"replication.role" : "none"}
```

c. 指定更改。 例如，您可以使用 **Update Replication Config Property REST Service** 发送以下服务请求，以更改 **replication.role** 特性的值。

```
PUT https://localhost:9080/SKLM/rest/v1/configProperties
Content-Type: application/json
Accept: application/json
Authorization: SKLMAuth authId=139aeh34567m
Accept-Language: en
{ "replication.role": "master"}
```

3. 成功指示符会根据界面的不同而不同:
   - 图形用户界面:

     主服务器的“自动克隆复制配置”页面上显示更新后的配置信息。
   - 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。

管理组、用户和角色

您可以限制管理员在您的组织中能够执行的活动的范围。

为了保持长期效率，请考虑创建一个组，然后向该组分配角色和用户，而不是直接将角色分配给个别用户。 您可以轻松地更改具有相似职责的人员的角色，并且在将用户分配给另一部门时避免返工。

例如，您可以指定以下活动范围:

- 对于某些角色，未提供任何访问权。 例如，组织可能希望将备份文件和复原文件的职责分离。
- 某些任务隐藏在 WebSphere® 集成解决方案控制台 上。
- 管理只能发生于 LTO 磁带机。

创建组

您可以创建一个组，用来对某些系统管理员指定限制。 必须在预定义 LTO 组后对该组进行建模。

关于此任务

此任务使用 WebSphere 集成解决方案控制台 上的 WASAdmin 用户标识来创建管理组。

注: 要访问 IBM Security Key Lifecycle Manager 图形用户界面或命令行界面，必须将用户分配到以下组: `klmGUICLIAccessGroup`

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)。

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。

过程

1. 登录 WebSphere 集成解决方案控制台 (`https://localhost:9083/ibm/console/logon.jsp`)。
   - 图形用户界面:
     a. 在浏览器的"欢迎"页面上，输入用户标识 `WASAdmin` 以及此管理员的密码。
     b. 在导航树中，单击**用户和组** > **管理组**。
   - 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. 创建组:
   - 图形用户界面:
     a. 在"管理组"页面上，单击**创建**。
     b. 在**组名**字段中，指定组名。 例如，输入 `DS5000Admin`。
     c. 在**描述**字段中，指定更多有关要创建的组的信息。
     d. 单击**创建**。
   - 命令行界面:
     a. 创建授权组。
     b. 创建组。

     输入 `createGroup` 并指定创建组所需的值。 例如，使用 Jython 输入:

     ```
     print AdminTask.createGroup
       ('[-cn DS5000Admin -description DS5000_LocalAdmins]')
     ```

     其中:

     -cn 必需（字符串）。 指定要创建的组的公共名称。 此参数映射到虚拟成员管理器中的 **cn** 特性。

     -description
     可选（字符串）。 指定更多有关要创建的组的信息。

3. 保存您的工作。
   - 图形用户界面:

     使用图形用户界面提供的提示来确认任务是否已完成。
   - 命令行界面:

     保存配置。 例如，使用 Jython 输入:

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

下一步做什么

接下来，向组分配一个或多个许可权或角色。

分配许可权

您可以将管理组映射到受限制的许可权集。

关于此任务

此任务使用 WebSphere 集成解决方案控制台 上的 WASAdmin 用户标识将组映射到受限制的操作集，以管理 DS5000 存储服务器。

有关用于将组映射到角色的命令的更多信息，请参阅 IBM WebSphere Application Server 文档 (http://www-01.ibm.com/support/knowledgecenter/SSAW57_8.5.5/com.ibm.websphere.nd.doc/ae/rxml_atauthorizationgroup.html)。

过程

1. 登录 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. 在图形用户界面中，单击**用户和组 > 管理组角色**。
     c. 单击**添加**。
   - 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. 将受限制的角色集映射到组。
   - 图形用户界面:
     a. 在“管理组角色”页面中的“常规特性”部分中，单击**输入组名**。在**组名**字段中，输入组的名称。 例如，输入 `DS5000Admin`。

b. 在“常规特性”部分中，从**角色**列表中选择所需角色子集。 例如，执行下列步骤:

   – 禁止访问某些角色。 例如，组织可能希望将复原文件的职责分离。 在这种情况下，请勿选择列表中的 klmRestore 项。

   – 确定是否要隐藏 WebSphere 集成解决方案控制台 上的其他任务。如果要隐藏任务，请选择 **suppressmonitor** 作为角色。

   – 将管理仅限制到 DS5000 存储服务器。例如，选择 **DS5000**。

     另外，如果您的任务针对新的设备组（例如 myDS5000）定义管理活动，那么您可以选择先前创建的 myDS5000。

   – 按住 Ctrl 键并选择适用于 IBM Security Key Lifecycle Manager 的角色:

     klmBackup
     创建和删除数据的备份。

     klmRestore
     复原数据的先前备份副本。

     klmConfigure
     阅读或更改特性，或对证书执行操作。

     klmAudit
     查看审计数据。

     klmView
     查看对象。

     klmCreate
     创建对象。

     klmModify
     修改对象。

     klmDelete
     删除对象。

     klmGet
     导出密钥或证书。

     suppressmonitor
     隐藏 WebSphere 集成解决方案控制台 上的其他任务。

     DS5000
     允许对 DS5000 存储服务器执行操作。

c. 单击**确定**。

d. 单击**保存**以将更改直接保存到主配置。

- 命令行界面:

  输入 mapGroupsToAdminRole，并指定将组映射到特定管理角色所需的值。 例如，使用 Jython 将多个角色指定到组，输入一系列命令，并在输入每个命令之后按 **Enter** 键。

  – 为组指定第一个角色:

```
print AdminTask.mapGroupsToAdminRole('[-roleName suppressmonitor
 -groupids DS5000Admin]')
```

– 为组指定下一个角色:

```
print AdminTask.mapGroupsToAdminRole('[-roleName klmConfigure
 -groupids DS5000Admin]')
```

– 通过对每个角色使用单独的声明，为组指定其余角色:

```
print AdminTask.mapGroupsToAdminRole('[-roleName klmBackup
 -groupids DS5000Admin]')
print AdminTask.mapGroupsToAdminRole('[-roleName klmAudit
 -groupids DS5000Admin]')
print AdminTask.mapGroupsToAdminRole('[-roleName klmView
 -groupids DS5000Admin]')
print AdminTask.mapGroupsToAdminRole('[-roleName klmCreate
 -groupids DS5000Admin]')
print AdminTask.mapGroupsToAdminRole('[-roleName klmModify
 -groupids DS5000Admin]')
print AdminTask.mapGroupsToAdminRole('[-roleName klmDelete
 -groupids DS5000Admin]')
print AdminTask.mapGroupsToAdminRole('[-roleName klmGet
 -groupids DS5000Admin]')
print AdminTask.mapGroupsToAdminRole('[-roleName DS5000
 -groupids DS5000Admin]')
```

其中:

- authorizationGroupName

这是授权组的名称。 如果您不指定此参数，那么假定授权组为单元级别授权组。 （字符串，可选）

- roleName

这是管理角色的名称。 （字符串，必需）

- groupids

这是映射到管理角色的组标识的列表。（字符串，[]）

3. 保存您的工作。
   - 图形用户界面:

     使用图形用户界面提供的提示来确认任务是否已完成。
   - 命令行界面:

     保存配置。 例如，使用 Jython 输入:

     ```
     print AdminConfig.save()
     ```
4. 确保您保存到组的角色已进行分配。
   - 图形用户界面

     退出然后重新进入“管理组角色”页面。 将显示其他角色。
   - 命令行界面

     使用 Jython 语法输入以下命令:

     ```
     print AdminTask.listGroupIDsOfAuthorizationGroup()
     ```

下一步做什么

接下来，指定您的组织可能需要的其他组。 例如，指定用于执行操作员任务的管理组。

在组中创建用户

创建用户并将用户的成员资格分配到系统管理员组。

关于此任务

此任务使用 WebSphere 集成解决方案控制台 上的 WASAdmin 用户标识来创建用户并将该用户添加到组。

注: 要访问 IBM Security Key Lifecycle Manager 图形用户界面或命令行界面，必须将用户分配到以下组: `klmGUICLIAccessGroup`

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. 通过在新组中指定成员资格来创建用户。
   - 图形用户界面:
     a. 在“管理用户”页面上，单击**创建**。
     b. 在“创建用户”页面上，指定必需信息，例如用户标识和密码。 例如，输入 `myAdmin` 作为用户标识，`mypwd` 作为密码。
     c. 单击**创建**。
     d. 单击指向新用户标识的链接以显示用户特性。
     e. 在“用户特性”对话框上，单击**组**。
     f. 单击**添加**。
     g. 在“将用户添加到组”对话框上，单击**搜索**。
     h. 在组表中，选择您之前创建的组，并单击**添加**。
     i. 阅读关于用户已添加到组的确认消息，然后单击**关闭**。
   - 命令行界面:

a. 首先，创建用户。 输入 createUser 并指定创建用户所需的值。 例如，使用 Jython 输入:

```
print AdminTask.createUser ('[-uid myAdmin -password tempPass
  -confirmPassword tempPass -cn myAdmin -sn JDoe]')
```

其中:

-uid 指定要创建的用户的唯一标识。（字符串，必需）

-password
指定用户的密码。 （字符串，必需）

-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）

-cn 指定用户的名字。 （字符串，可选）

-sn 指定用户的姓氏。 （字符串，可选）

b. 添加该用户作为组的成员。 例如，在 Jython 中，输入以下命令:

```
print AdminTask.addMemberToGroup('[-memberUniqueName
 uid=myAdmin,o=defaultWIMFileBasedRealm
  -groupUniqueName cn=DS5000Admin,o=defaultWIMFileBasedRealm]')
```

其中:

memberUniqueName ***uniqueName***
指定要添加到指定组的用户或组的唯一名称值。

groupUniqueName ***uniqueName***
指定要将用户添加到的组的唯一名称值。

3. 验证该用户是否是组的成员。
   - 图形用户界面:
     a. 在导航树中，单击**用户和组** > **管理用户**。
     b. 在“管理用户”页面上的**用户标识**列中，单击新用户标识的条目。
     c. 在“用户特性”对话框上，单击**组**选项卡。验证该用户是否是新组的成员。
   - 命令行界面:

     例如，使用 Jython 输入:

     ```
     print AdminTask.getMembersOfGroup('[-uniqueName
       cn=DS5000Admin,o=defaultWIMFileBasedRealm]')
     ```

4. 保存您的工作。
   - 图形用户界面:

     使用图形用户界面提供的提示来确认任务是否已完成。
   - 命令行界面:

     保存配置。 例如，使用 Jython 输入:

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

5. 如果您是使用命令行界面创建用户，请运行 **stopServer** 和 **startServer** 命令来重新启动 IBM Security Key Lifecycle Manager 服务器。然后，以新用户身份登录。

下一步做什么

接下来，验证该用户是否可以执行授权任务。以 WASAdmin 身份注销。以新用户身份登录并确认您能否使用 IBM Security Key Lifecycle Manager 执行任务。

验证用户任务

验证管理组中的新用户能否执行任务。

关于此任务

此任务用于验证组中的用户能否执行组成员资格提供的任务。 例如，用户可以管理 DS5000 存储服务器。

注: 要访问 IBM Security Key Lifecycle Manager 图形用户界面或命令行界面，必须将用户分配到以下组: `klmGUICLIAccessGroup`

有关用于将组映射到角色的命令的更多信息，请参阅 IBM WebSphere Application Server 文档 (http://www-01.ibm.com/support/knowledgecenter/SSAW57_8.5.5/com.ibm.websphere.nd.doc/ae/rxml_atauthorizationgroup.html)。

过程

验证用户能否执行组成员资格提供的一组任务。

- 图形用户界面:
  1. 从 WASAdmin 用户标识中注销。
  2. 以组中的授权用户身份登录图形用户界面。 例如，以 `myAdmin` 身份登录。
  3. 在“密钥和设备管理”表上，验证唯一的管理选项是否为 DS5000。

     或者，如果您先前的任务为新的设备组（例如 `myDS5000`）定义了管理活动，请验证唯一的管理选项是否为 `myDS5000`。
  4. 选择设备，然后单击**转至 > 管理密钥和设备**。
  5. 或者，右键单击设备，然后选择**管理密钥和设备**。
  6. 在 DS5000 的管理页面上，完成任务。 例如，添加新的密钥组。
- 命令行界面:
  1. 以 wasadmin 身份从 **wsadmin** 中注销。
  2. 在 *WAS_HOME*`/bin` 目录中，使用 Jython 启动新的 **wsadmin** 会话。 然后，使用授权用户标识（例如，新的 `myAdmin` 用户标识）登录 **wsadmin**。 例如，在 Windows 系统上，浏览至 *drive*`:\Program Files (x86)\IBM\WebSphere\AppServer\bin` 目录并输入以下命令:
     - Windows 系统:

       ```
       wsadmin -username myAdmin -password password -lang jython
       ```
     - AIX 或 Linux 等系统:

       ```
       ./wsadmin.sh -username myAdmin -password password -lang jython
       ```
  3. 添加示例密钥组。 例如，输入:

     ```
     print AdminTask.tklmGroupCreate
      ('[-name GROUP-DS5000-abcd2de9 -type keygroup -usage DS5000]')
     ```

或者，使用 REST 客户机发送以下 HTTP 请求:

```
POST https://localhost:9080/SKLM/rest/v1/keygroups/newGroup
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth authId=139aeh34567m
{"usage":"DS500"}
```

下一步做什么

接下来，指定您的组织可能需要的其他组。 例如，指定用于执行操作员或审计员任务的组。

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 1. 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

表 1. 密码规则 (续)

规则	缺省值

* 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"/>`
`<NotUserID`**`CaseInsensitive`**`/>`
`<NotUserName`**`CaseInsensitive`**`/>`
`</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. 浏览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**。

创建设备组

根据组织需求，您可以创建设备组来管理业务用途受限制的设备子集，例如单个部门所使用的 LTO 磁带机。 另外，您还必须创建名称与设备组的名称相匹配（包括大小写）的角色。 名称匹配区分大小写。

关于此任务

此任务使用 SKLMAdmin 用户标识和 IBM Security Key Lifecycle Manager 界面来创建额外的设备组。

您的用户标识必须具有:

- `securityOfficer` 角色
- 管理操作的许可权 (**klmAdminDeviceGroup**)

  如果您具有 **klmAdminDeviceGroup** 许可权，那么可以创建、查看和删除设备组。 您无需先为设备组定义一个角色。 但是，您具有的许可权会限制您的其他操作。 例如，如果您只具有 **klmAdminDeviceGroup** 许可权，那么无法在创建设备组之后更新属性。

过程

1. 登录 IBM Security Key Lifecycle Manager。
   - 图形用户界面:

     在浏览器的“欢迎”页面上，输入 `SKLMAdmin` 的用户标识和密码值，例如 `mypassword`。
   - 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. 浏览至相应的页面或目录:
   - 图形用户界面:

     单击**高级配置 > 设备组**。

     a. 在“设备组”表中，单击**创建**。

     b. 在“创建设备组”对话框中，填写必填字段并单击**创建**。

- 命令行界面，请输入:

  ```
  AdminTask.tklmDeviceGroupCreate('[-name myLTO -deviceFamily LTO]')
  ```

- REST 界面:

  a. 获取用于访问 IBM Security Key Lifecycle Manager REST 服务的唯一用户认证标识。 有关认证过程的更多信息，请参阅 REST 服务的验证流程。

  b. 要调用 **Device Group Create REST Service**，请发送 HTTP POST 请求。请将您在步骤 a 中获取的用户认证标识随请求消息一起传递，如以下示例所示。

  ```
  POST https://localhost:9080/SKLM/rest/v1/deviceGroups/newGroup
  Content-Type: application/json
  Accept : application/json
  Authorization: SKLMAuth authId=139aeh34567m
  {"deviceFamily":"LTO","shortName":"myLTO","longName":"my companyname
  LTO devices"}
  ```

3. 验证设备组是否存在。

   - 图形用户界面:

     在设备组管理页面上，浏览“设备组”表以找到设备组。

   - 命令行界面，请输入:

     ```
     print AdminTask.tklmDeviceGroupList ('[-deviceFamily myLTO -v y]')
     ```

   - REST 界面:

     请使用 REST 客户机发出以下 HTTP GET 请求:

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

下一步做什么

创建名称与设备组相匹配的角色。

为新设备组创建角色

创建新的 IBM Security Key Lifecycle Manager 设备组时，请还为该设备组创建角色。请对设备组和角色指定同一名称（包括大小写）。 名称匹配区分大小写。

关于此任务

您可以通过编辑 admin-authz.xml 配置文件来将设备组的角色添加到 WebSphere Application Server。

过程

1. 在 Windows 操作系统上，通过添加下列各行来编辑 *<WAS_HOME>*/profiles/KLMProfile/cofig/cells/SKLMCell/admin-authz.xml 文件:

   ```
   <roles xmi:id=<roleId> roleName=<deviceGroupName>/>
   <authorizations xmi:id=<roleAssignmentId> role=<roleId/>
   ```

   roleId 和 roleAssignmentId 的值必须在 admin-authz.xml 文件中存在的所有角色和授权中唯一。

   例如，如果添加了新的设备组（例如 MyDS5K），那么您必须添加下列各行:

```
<roles xmi:id="MyDS5K_Role" roleName="MyDS5K"/>
<authorizations xmi:id="MyDS5K_Role_Auth" role="MyDS5K_Role"/>
```

2. 重新启动 WebSphere Application Server。必须停止然后重新启动服务器。 有关如何停止和启动服务器的指示信息，请参阅第 122 页的『在分布式系统上启动和停止 IBM Security Key Lifecycle Manager 服务器』。

下一步做什么

接下来，您可以指定用户组对新的设备组和必需管理任务（例如查看或配置）具有许可权。

数据库管理

安装过程会提供具有必需许可权的缺省管理员用户标识和密码。

您必须确保用户标识保持活动状态，并且符合系统上的活动安全策略。

移动 DB2 事务日志文件以提高性能

请定期移动 IBM Security Key Lifecycle Manager 数据库创建的旧的 DB2® 事务日志。否则，大量的事务日志可能会影响性能。

关于此任务

DB2 事务日志存在于下列目录中:

Windows 系统:

INSTANCEHOME:\sklmdbarchive\SKLMDB26\SKLMDB26\NODE0000\LOGSTREAM0000\C0000000

其中:

- *INSTANCEHOME* 是您在安装期间指定的盘符。
- SKLMDB26 是数据库实例所有者。
- SKLMDB26 是 IBM Security Key Lifecycle Manager 数据库的名称。
- NODE0000、LOGSTREAM0000 和 C0000000 在您的系统上可能有所不同。

Linux 或 AIX 之类的系统:

~sklmdbarchive/sklmdb26/SKLMDB26/NODE0000/LOGSTREAM0000/C0000000

其中:

- sklmdb26 是数据库实例所有者。
- SKLMDB26 是 IBM Security Key Lifecycle Manager 数据库的名称。
- NODE0000、LOGSTREAM0000 和 C0000000 在您的系统上可能有所不同。

如果 IBM Security Key Lifecycle Manager 管理许多密钥，并且 sklmdbarchive 目录所在的磁盘分区具有较少的可用磁盘空间，请将旧的事务日志移到其他磁盘分区。

注: 执行此任务时，请注意不要移动当前活动日志。

请定期执行下列步骤:

过程

1. 使用图形用户界面、命令行界面或 REST 界面创建 IBM Security Key Lifecycle Manager 备份。 否则，下次备份可能会失败。
2. 以 Linux 或 AIX 之类的系统上的数据库实例所有者身份，或 Windows 系统上的 DB2 管理员身份登录。
3. 在另一个具有足够磁盘空间的分区上创建一个可以将旧的日志文件移到其中的目录。
4. 标识第一个活动日志。 输入:

   Windows 系统:

   ```
   db2cmd
   SET DB2INSTANCE=sklmdb26
   db2 get db cfg for SKLMDB26
   ```

   Linux 或 AIX 之类的系统:

   ```
   db2 get db cfg for SKLMDB26
   ```

   配置参数 `First active log file` 的值用于标识第一个活动日志。
5. 将修改时间早于第一个活动日志的日志文件从 `sklmdbarchive` 目录移到新目录。

   日志将命名为 S*nnnnnnn*.LOG。 通常，编号较小的日志的创建时间早于编号较大的日志。 异常情况是数据库已经创建了名为 S99999999.LOG 的日志。 在这种情况下，编号将从 S0000000.LOG 重新开始。

   注: 运行复原操作将除去 `sklmdbarchive` 目录并创建新目录。

Windows 系统上的 DB2 密码安全性问题

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

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

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

要更改 DB2 数据库密码，请执行以下步骤:

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

     例如，*sklminstance* 的值可能是:

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

     例如，使用缺省实例名称时，*sklminstance* 的值可能是:

     ```
     DB2 - DBSKLMV26 - SKLMDB26
     ```

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

所有服务的密码均已更改时，请重新启动这些服务。

必须停止并重新启动以下服务。无需更改密码:

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

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

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

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

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

      结果可能为:

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

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

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

      例如，在一行上输入:

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

      结果为:

      ```
      sklm_db
      ```

   c. 更改 sklm_db 别名的密码，并在一行上输入以下命令:

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

      如果在密码中指定特殊字符，请在指定密码值时使用引号作为定界符。

      例如，在一行上输入:

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

   d. 保存更改:

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

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

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

      1) 打开控制面板并单击**管理工具 > 计算机管理 > 服务和应用程序 > 服务**。

2) 停止然后启动其名称类似于 IBM WebSphere Application Server V8.5 - SKLM26Server 的 IBM Security Key Lifecycle Manager 服务器服务。

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

1) 首先，请输入:

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

结果可能为:

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

2) 在第一个数据源上测试连接。 例如，输入:

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

例如，在一行上输入:

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

3) 在其余的数据源上测试连接。例如，输入:

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

4) 在这两种情况下，您都会收到消息，表明与数据源的连接已成功。 例如:

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

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

诸如 Linux 或 AIX 等系统上的 DB2 密码安全性问题

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

IBM Security Key Lifecycle Manager 安装程序将安装 DB2，并提示安装人员输入名为 sklmdb26 的用户的密码。另外，DB2 应用程序将创建一个名为 sklmdb26 的操作系统用户条目。例如，此用户的密码可能到期，需要您对两个用户标识的密码都进行再同步。

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

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

```
su sklmdb26
```

3. 更改密码。 输入:

```
passwd
```

指定新密码。

4. 退回为 root 用户。

   ```
   exit
   ```

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

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

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

   a. 以下命令将列出 JAASAuthData 条目:

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

      结果可能类似于以下示例:

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

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

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

      结果类似于以下示例:

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

      同时在一行上输入:

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

      结果类似于以下示例:

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

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

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

      例如，在一行上输入:

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

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

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

      例如，在一行上输入:

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

   e. 保存更改:

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

f. 退回为 root 用户。

```
exit
```

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

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

结果类似于以下示例:

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

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

```
startServer.sh server1
```

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

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

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

1) 首先，查询数据源的列表。 输入:

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

结果可能类似于以下示例:

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

2) 输入:

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

例如，在一行上输入:

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

3) 在其余的数据源上测试连接。例如，输入:

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

4) 在这两种情况下，您都会收到消息，表明与数据源的连接已成功。 例如:

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

停止 DB2 服务器

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

关于此任务

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

要停止数据库服务器，请执行以下步骤:

过程

1. 以 AIX 或 Linux 等系统的数据库实例所有者或 Windows 系统的本地管理员的身份登录。
2. 停止 WebSphere Application Server。请输入此命令:

   Windows 系统:

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

   AIX 或 Linux 等系统:

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

3. 停止 DB2 服务器。 请输入以下命令:

   Windows 系统:

   ```
   set DB2INSTANCE=sklmdb2
   db2stop
   ```

   AIX 或 Linux 等系统:

   ```
   su -sklmdb2
   db2stop
   ```

更改 DB2 服务器 主机名

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

关于此任务

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

更改现有的 WebSphere Application Server 主机名

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

过程

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

接受暂挂设备

使用设备暂挂功能来接受或拒绝与 IBM Security Key Lifecycle Manager 联系的设备。

关于此任务

您可以使用“暂挂设备请求”页面或者使用一些命令来接受或拒绝与 IBM Security Key Lifecycle Manager 联系的设备。如果设备属于 DS5000 设备系列，并且启用了机器亲缘关系，那么您还可以接受或拒绝设备与机器之间的关系。 通过使用机器亲缘关系，您可以限制只有特定设备和机器组合可以使用密钥服务。

过程

1. 暂挂请求到达时，将针对 DS5000 设备组中的设备自动生成密钥。 请先执行备份，然后再接受设备，以确保密钥在提供给设备之前进行了备份。有关更多信息，请参阅“管理备份和复原文件”。
2. 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。在导航树中，单击 **IBM Security Key Lifecycle Manager**。
   - 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
       ```
3. 如果您先前尚未确定如何接受暂挂设备，请将 **device.AutoPendingAutoDiscovery** 属性设置为用于将入局设备添加到暂挂设备列表的值。

   指定一个设置，例如 2（自动暂挂）。 所有入局设备都会添加到暂挂列表，但不会在其提出请求时自动对其提供密钥。 必须先在暂挂设备列表中接受或拒绝设备，然后才可在该设备提出请求时对其提供密钥。 不要对 DS5000 设备系列使用设置 1（自动接受）。 此设置允许在备份数据之前生成密钥并将密钥提供给 DS5000 存储服务器。
   - 图形用户界面:
     a. 浏览到暂挂设备的设备组的“密钥和设备管理”页面。
     b. 在页面底部的下拉列表中，选择**保留正在等待我审核的新设备请求**。
   - 命令行界面:

     例如，对于 DS5000 设备，请输入以下命令:

     ```
     print AdminTask.tklmDeviceGroupAttributeUpdate ('[-name DS5000
       -attributes "{device.AutoPendingAutoDiscovery 2}"]')
     ```
4. 列出暂挂设备。

- 图形用户界面:

  浏览到“欢迎”页面。在“操作项”区域中，单击“暂挂设备”链接。

- 命令行界面:

  输入:

  ```
  print AdminTask.tklmPendingDeviceList ('[-usage DS5000]')
  ```

5. 核准或拒绝暂挂设备请求。
   - 图形用户界面:

     在“暂挂设备请求”表中，选择暂挂设备，然后单击**接受**或**拒绝**。

     对于还具有机器-设备关系的 DS5000 设备，暂挂请求将仅列出一次。 该请求与包含机器标识值的表一起显示。 接受暂挂设备请求还会接受机器-设备关系。

     在“接受设备请求”对话框中，单击**接受**或**修改并接受**。 如果您选择修改暂挂设备信息，请进行所需更改，然后单击**接受**。

   - 命令行界面:
     - 您可以使用一个命令来接受暂挂 DS5000 设备以及暂挂机器-设备关系。 例如，输入:

       ```
       print AdminTask.tklmPendingMachineDeviceAccept
       ('[-deviceUUID DEVICE-7d588437-e725-48bf-a836-00a47df64e78
       -machineID 30423830303034370000000000000]')
       ```

     - 另外，您还可以先接受暂挂设备，方法是将该设备分配给相应的设备组。 要接受暂挂 DS5000 设备然后接受机器-设备关系，例如

       a. 首先，请输入:

          ```
          print AdminTask.tklmPendingDeviceAccept
          ('[-deviceUUID DEVICE-7d588437-e725-48bf-a836-00a47df64e78
           -usage DS5000]')
          ```

       b. 然后，接受或拒绝设备与机器之间的暂挂关系。

          1) 列出所有与某个机器标识有关系的暂挂设备，或者列出所有设备（如果未指定机器标识）。 例如，输入:

             ```
             print AdminTask.tklmPendingMachineDeviceList
             ('[-machineID 30423830303034370000000000000]')
             ```

          2) 接受或拒绝暂挂设备和机器关系。 如果接受，那么关系数据将写入 IBM Security Key Lifecycle Manager 数据存储器。

             ```
             print AdminTask.tklmPendingMachineDeviceAccept
             ('[-deviceUUID DEVICE-7d588437-e725-48bf-a836-00a47df64e78
             -machineID 30423830303034370000000000000]')
             ```

6. 成功指示符会根据界面的不同而不同:
   - 图形用户界面:

     已接受的设备将在设备组的相应管理页面中列出。 例如，管理页面上的表列中显示了 LTO 磁带机的磁带机序列号。

   - 命令行界面:

     完成消息表示成功。

下一步做什么

检查已接受设备的列表。 请使用以下命令:

- **tklmDeviceList**，用于列出有关指定设备类型的所有设备的信息。
- **tklmMachineDeviceList**，用于列出所有与特定机器标识相关联的设备，或者列出所有设备（如果未指定机器标识）。

在设备组间移动设备

使用设备更新功能来将设备从一个现有设备组移到另一个现有设备组。 例如，您可能希望将某个设备移到 MYDS5000 设备组。

关于此任务

您可以使用“修改设备”页面、**tklmDeviceUpdate** 命令或 **Device Update REST Service**，将与 IBM Security Key Lifecycle Manager 联系的设备从一个设备组移到同一设备系列中的另一个设备组。 例如，您可能希望将某个设备移到 DS5000 设备系列中的 MYDS5000 设备组。

有关创建设备组的更多信息，请参阅第 33 页的『创建设备组』。

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”页面上的“密钥和设备管理”部分中，选择 **DS5000**。
     c. 右键单击 **DS5000**。
     d. 单击**管理密钥和设备**。
   - 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. 找到要移到父设备系列中的另一个设备组的设备。
   - 图形用户界面:

     在“密钥和设备管理 DS5000”页面上，在设备表中找到该设备。 例如，该设备可能具有 aaa123 之类的序列号。
   - 命令行界面:

输入以下命令:

```
print AdminTask.tklmDeviceList ('[-type DS5000]')
```

在命令输出中，找到设备 UUID 值。 例如:

```
Description = My long description
Serial Number = aaa123
Device uuid = DEVICE-b7678b4d-3898-4f8c-9557-dbb2f381fc8a
Device group = DS5000
Device Text =
World wide name =
Sym alias = DS5K-aaa123
```

- REST 界面:

  a. 获取用于访问 IBM Security Key Lifecycle Manager REST 服务的唯一用户认证标识。 有关认证过程的更多信息，请参阅 REST 服务的验证流程。

  b. 要调用 **Device List Type REST Service**，请发送 HTTP GET 请求。请将您在步骤 a 中获取的用户认证标识随请求消息一起传递，如以下示例所示。

  ```
  GET https:///localhost:9080/SKLM/rest/v1/devices?type=DS5000
  Content-Type: application/json
  Accept : application/json
  Authorization : SKLMAuth userAuthId=37ea1939-1374-4db7-84cd-14e399be2d20
  Accept-Language : en
  ```

  在成功响应中，找到设备 UUID 值。 例如:

  ```
  Status Code : 200 OK
  Content-Language: en
  [
  {
  "Description": "My long description",
  "Serial Number": "aaa123",
  "Device uuid": "DEVICE-b7678b4d-3898-4f8c-9557-dbb2f381fc8a",
  "Device group": "DS5000",
  "World wide name": "",
  "Sym alias": "DS5K-aaa123"
  },
  ]
  ```

3. 确保目标设备组存在。

   - 图形用户界面:

     在“密钥和设备管理 DS5000”页面上，在设备表中，选择该设备，然后单击**修改 > 设备**。

     在“修改设备”页面上，在**当前分配的设备组**字段中，展开列表以确定 **MYDS5000** 设备组是否可用。

   - 命令行界面:

     输入以下命令:

     ```
     print AdminTask.tklmDeviceGroupList ('[-deviceFamily DS5000 -v y]')
     ```

     找到该设备组。 例如:

     ```
     Device Group UUID               10000
     Device Group Name               MYDS5000
     Device Family                   DS5000
     symmetricKeySet                 null
     drive.default.alias1            null
     drive.default.alias2            null
     ```

```
shortName                          MYDS5000group
longName                           my companyname DS5000 devices
roleName                           MYDS5000
device.AutoPendingAutoDiscovery  0
enableKMIPDelete                   false
```

- REST 界面:

  发送以下 HTTP 请求:

  ```
  GET https://localhost:9080/SKLM/rest/v1/deviceGroups?deviceFamily=DS5000
  Content-Type: application/json
  Accept: application/json
  Authorization: SKLMAuth authId=139aeh34567m
  Accept-Language : en
  ```

  找到该设备组。 例如:

  ```
  Status Code : 200 OK
  Content-Language: en
  [
  {
  "Device Group UUID": "10000",
  "Device Group Name": "MYDS5000",
  "Device Family": "DS5000",
  "symmetricKeySet": null,
  "drive.default.alias1": null,
  "drive.default.alias2": null,
  "shortName": MYDS5000group,
  "longName": my companyname DS5000 devices,
  "roleName": "MYDS5000",
  "device.AutoPendingAutoDiscovery": "0",
  "enableKMIPDelete": "false"
  },
  ]
  ```

4. 更新该设备以指定新的设备组。
   - 图形用户界面:

     在“修改设备”页面上，在**当前分配的设备组**字段中，选择 **MYDS5000** 设备组。

     单击**修改设备**。
   - 命令行界面:

     输入以下命令:

     ```
     print AdminTask.tklmDeviceUpdate
     ('[-uuid DEVICE-b7678b4d-3898-4f8c-9557-dbb2f381fc8a -type MYDS5000]')
     ```
   - REST 界面:

     发送以下 HTTP 请求:

     ```
     PUT https://localhost:9080/SKLM/rest/v1/devices
     Content-Type: application/json
     Accept : application/json
     Authorization: SKLMAuth authId=139aeh34567m
     {"uuid":"DEVICE-b7678b4d-3898-4f8c-9557-dbb2f381fc8a","type":
     "MYDS5000"}
     ```
5. 验证该设备是否位于新的设备组中。
   - 图形用户界面:

     在“密钥和设备管理 DS5000”页面上，该设备不再在设备表中列出。 请打开“密钥和设备管理”的“MYDS5000”页面，并确保该设备在设备表中列出。

- 命令行界面:

  输入以下命令:

  ```
  print AdminTask.tklmDeviceList ('[-type MYDS5000]')
  ```

  例如，输出包含该设备的 UUID 值以及新设备组的名称:

  ```
  Description = My long description
  Serial Number = aaa123
  Device uuid = DEVICE-b7678b4d-3898-4f8c-9557-dbb2f381fc8a
  Device group = MYDS5000
  Device Text =
  World wide name =
  Sym alias = DS5K-aaa123
  ```

- REST 界面:

  发送以下 HTTP 请求:

  ```
  GET https:///localhost:9080/SKLM/rest/v1/devices?type=MYDS5000
  Content-Type: application/json
  Accept : application/json
  Authorization : SKLMAuth userAuthId=37ea1939-1374-4db7-84cd-14e399be2d20
  Accept-Language : en
  ```

  成功响应包含该设备的 UUID 值以及新设备组的名称，如以下示例所示:

  ```
  Status Code : 200 OK
  Content-Language: en
  [
  {
  "Description": "My long description",
  "Serial Number": "aaa123",
  "Device uuid": "DEVICE-b7678b4d-3898-4f8c-9557-dbb2f381fc8a",
  "Device group": "MYDS5000",
  "World wide name": "",
  "Sym alias": "DS5K-aaa123"
  },
  ]
  ```

LTO 磁带机管理

您可以使用 IBM Security Key Lifecycle Manager 来管理 LTO 磁带机。

创建密钥组和磁带机的指导步骤

首次创建密钥组和磁带机以及稍后添加更多密钥组或磁带机时，IBM Security Key Lifecycle Manager 会提供一组指导步骤来完成该任务。

对某些步骤的描述可能会提及用于执行同一任务的命令行替代方法。 在指导任务集中，请使用图形用户界面来完成这些任务。

创建密钥组

作为第一个活动，您可以创建用于 IBM Security Key Lifecycle Manager 的密钥和密钥组。

关于此任务

您可以使用“创建密钥组”对话框。另外，您还可以使用 **tklmGroupCreate** 命令或 **Group Create REST Service** 来创建要将密钥添加到的组。 然后，使用 **tklmSecretKeyCreate**

命令或 **Secret Key Create REST Service** 在现有组中创建一个或多个对称密钥。 您的角色必须具有执行创建操作和访问相应设备组的许可权。

开始之前，请确定密钥的数量以及组织需要的各个密钥组的用途。

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”页面上的“密钥和设备管理”部分中，选择 **LTO**。
     c. 单击**转至 > 根据指导创建密钥和设备**。
     d. 或者，右键单击 **LTO**，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. 创建密钥组:
   - 图形用户界面:
     a. 在“步骤 1: 创建密钥组”页面上，在**密钥组**表上单击**创建**。
     b. 在“创建密钥组”对话框上，为必需参数和可选参数指定值。 例如，您可以创建包含 100 个密钥的密钥组。
     c. 单击**创建密钥组**。
   - 命令行界面:
     a. 首先，创建可以将密钥添加到的组。

        输入 tklmGroupCreate 以创建组。 例如，输入:

        ```
        print AdminTask.tklmGroupCreate
         ('[-name GROUP-myKeyGroup -type keygroup -usage LTO]')
        ```

     b. 接下来，使用 **tklmGroupList** 命令获取所创建的组的 UUID 值。 例如，输入:

        ```
        print AdminTask.tklmGroupList
         ('[-name GROUP-myKeyGroup -type keygroup -v y]')
        ```

     c. 然后，创建一组密钥并将它们存储在组中。 例如，输入:

        ```
        print AdminTask.tklmSecretKeyCreate ('[-alias abc
        -keyStoreName defaultKeyStore
         -numOfKeys 10 -usage LTO
          -keyGroupUuid KEYGROUP-316408ac-f433-4c11-92bc-0de46d05bee9]')
        ```

- REST 界面:
  a. 获取用于访问 IBM Security Key Lifecycle Manager REST 服务的唯一用户认证标识。 有关认证过程的更多信息，请参阅 REST 服务的验证流程。
  b. 要调用 **Group Create REST Service**，请发送 HTTP POST 请求。请将您在步骤 a 中获取的用户认证标识随请求消息一起传递，如以下示例所示。

```
POST https://localhost:9080/SKLM/rest/v1/keygroups/newGroup
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth authId=139aeh34567m
{"usage":"LTO"}
```

  c. 使用 **Group List REST Service** 来获取所创建的组的 UUID 值。 例如:

```
GET https://localhost:9080/SKLM/rest/v1/keygroups?name=newGroup
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth authId=139aeh34567m
Accept-Language : en
```

  d. 然后，使用 **Secret Key Create REST Service** 创建一组密钥并将它们存储在组中。 例如，您可以发送以下 HTTP 请求:

```
POST https://localhost:9080/SKLM/rest/v1/keys
Content-Type: application/json
Accept: application/json
Authorization: SKLMAuth authId=139aeh34567m
{"alias":"abc","numOfKeys":"10","KEYGROUP-316408ac-f433-4c11-92bc-
0de46d05bee9","usage":"LTO"}
```

3. 成功指示符会根据界面的不同而不同:
   - 图形用户界面:

     该密钥组作为**密钥组**表中的项列出。
   - 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

请在将新密钥提供给设备之前备份这些密钥。 您还可以转至下一指导步骤以定义特定设备，并将密钥组与这些设备进行关联。 请选择**步骤 2: 识别磁带机**或单击**转至下一步**。

识别磁带机

您可以识别要用于 IBM Security Key Lifecycle Manager 的 LTO 磁带机。

关于此任务

您可以使用“添加磁带机”对话框、**tklmDeviceAdd** 命令或 **Device Add REST Service** 来添加设备。 您的角色必须具有执行创建操作和访问相应设备组的许可权。

开始之前，请创建要与所标识的磁带机相关联的密钥组。 另外，请确定您是否希望 IBM Security Key Lifecycle Manager 自动接受来自所有磁带机的请求。 为了提高安全性，在发现所有磁带机之后，您可以对生产环境关闭此选项。

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”页面上的“密钥和设备管理”部分中，选择 **LTO**。
     c. 单击**转至 > 根据指导创建密钥和设备**。
     d. 或者，右键单击 **LTO**，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. 跳过“创建密钥组”页面。 单击**转至下一步**链接，或者单击**步骤 2: 识别磁带机**。
3. 您可以指定 IBM Security Key Lifecycle Manager 存放新的设备请求以等待您的审核。
   - 图形用户界面:

     选择**保留正在等待我审核的新设备请求**。
   - 命令行界面:

     使用 **tklmDeviceGroupAttributeUpdate** 命令或 **Device Group Attribute Update REST Service** 来设置 **device.AutoPendingAutoDiscovery** 属性的值。例如，输入:

     ```
     print AdminTask.tklmDeviceGroupAttributeUpdate ('[-name LTO
       -attributes "{device.AutoPendingAutoDiscovery 2}"]')
     ```

     对于 LTO 设备组，使用 **tklmDeviceGroupAttributeUpdate** 命令通过 IBM Security Key Lifecycle Manager 数据库中 **symmetricKeySet** 属性指定密钥组。
   - REST 界面:
     a. 获取用于访问 IBM Security Key Lifecycle Manager REST 服务的唯一用户认证标识。 有关认证过程的更多信息，请参阅 REST 服务的验证流程。
     b. 要调用 **Device Group Attribute Update REST Service** 以及设置 **device.AutoPendingAutoDiscovery** 属性的值，请发送 HTTP PUT 请求。请将您在步骤 a 中获取的用户认证标识随请求消息一起传递，如以下示例所示。

        ```
        PUT https://localhost:9080/SKLM/rest/v1/deviceGroupAttributes
        Content-Type: application/json
        Accept : application/json
        Authorization: SKLMAuth authId=139aeh34567m
        {"name":"LTO","attributes":"device.AutoPendingAutoDiscovery 2"}
        ```

4. 添加设备:

- 图形用户界面:
  a. 在“步骤 2: 识别磁带机”页面上，在**设备**表中单击**添加**。
  b. 在“添加磁带机”对话框中，输入必需信息和可选信息。
  c. 单击**添加磁带机**。
- 命令行界面:

  输入 tklmDeviceAdd 以添加设备。 必须指定设备组和序列号。例如，输入:

```
print AdminTask.tklmDeviceAdd ('[-type LTO -serialNumber FAA49403AQJF
  -attributes "{worldwideName ABCdeF1234567890}
  {description salesDivisionDrive} {symAlias LTOKeyGroup1}"]')
```

- REST 界面:

  您可以使用 **Device Add REST Service** 来添加设备。 例如，您可以发送以下 HTTP 请求:

```
POST https://localhost:9080/SKLM/rest/v1/devices
Content-Type: application/json
Accept : application/json
Authorization : SKLMAuth userAuthId=37ea1939-1374-4db7-84cd-14e399be2d20
Accept-Language : en
{"type":"LTO","serialNumber":"FAA49403AQJF","attributes":"worldwideName
ABCdeF1234567890,description marketingDivisionDrive"}
```

5. 成功指示符会根据界面的不同而不同:
   - 图形用户界面:

     已将该设备添加到**设备**表。
   - 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

接下来，您可以使用 LTO“密钥和设备管理”页面来查看所有密钥组和设备。

管理密钥、密钥组和设备

要管理密钥、密钥组和设备，您需要将密钥组映射到磁带机。 您可以添加、修改或删除特定密钥、密钥组或设备。

关于此任务

使用 LTO“密钥和设备管理”来将密钥组映射到磁带机。 您可以添加、修改或删除特定密钥、密钥组或设备。 您的角色必须具有执行查看操作和访问相应设备组的许可权。

要更改信息的视图，请选择:

查看密钥组和磁带机

查看密钥组名称和磁带机序列号。 另外，此视图还会列出磁带机所使用的密钥组、密钥或系统缺省值。

查看密钥、密钥组成员资格和磁带机

查看密钥以及密钥组中的密钥成员资格。 另外，此视图还会列出磁带机序列号，以及磁带机所使用的密钥组、密钥或系统缺省值。

开始之前，先检查该页面上的列（页面上提供了用于添加、修改或删除表项的各个按钮）。 要对信息进行排序，请单击列标题。

表组织成下列区域:

- 在左侧列中，提供有关密钥或密钥组的信息。

  对于密钥，该信息指示该密钥所属的密钥组。对于密钥组，该信息指示该密钥组是否用作缺省密钥组以及组中的密钥数。
- 在右侧列中，提供有关磁带机的信息。

  该信息指示磁带机序列号以及磁带机所使用的密钥组或特定密钥。 例如，磁带机可以使用“系统缺省值”密钥组。
- 用于指示密钥类型的图标。

表 2. 图标及其含义

图标	描述
	对称密钥或专用密钥。 专用密钥是包含一个公用密钥和一个专用密钥的密钥对中的非对称密钥。
	密钥组

过程

1. 登录图形用户界面:
   a. 在“欢迎”页面上的“密钥和设备管理”部分中，选择 **LTO**。
   b. 单击**转至 > 管理密钥和设备**。
   c. 或者，右键单击 **LTO**，然后选择**管理密钥和设备**。

   某些步骤的描述提供了使用图形用户界面、命令行界面或 REST 界面而完成的备选步骤。 对于任何一个工作会话，都不要在界面之间进行切换。

   一些任务的描述可能会提及 `SKLMConfig.properties` 文件中与任务相关的属性。使用图形用户界面、命令行界面或 REST 界面可更改这些属性。
2. 在 LTO“密钥和设备管理”上，您可以添加、修改或删除密钥、密钥组或磁带机。

   您可以执行下列管理任务:
   - 刷新列表。

     单击“刷新”图标  可刷新表中的项。
   - 添加

     单击**添加**。 另外，您还可以选择用于创建密钥组和磁带机的逐步过程。
     – 密钥组

在**创建密钥组**对话框上，指定必需信息，例如密钥组名称。 您还可以指定此组作为缺省密钥组来提供密钥。只能有一个缺省密钥组。 然后单击**创建密钥组**。您的角色必须具有执行创建操作和访问相应设备组的许可权。

– 磁带机

在“添加磁带机”对话框中，输入磁带机序列号和其他信息。 然后单击**添加磁带机**。 您的角色必须具有执行创建操作和访问相应设备组的许可权。

– 使用逐步过程来创建密钥组、密钥和磁带机

在“步骤 1: 创建密钥组”和“步骤 2: 识别磁带机”页面上，输入必需信息，然后单击相应的按钮以完成该任务。

成功指示符各不相同，显示密钥组或设备。

- 修改

要更改密钥组、密钥或磁带机，请选择密钥组、密钥或磁带机，然后单击**修改**。或者，右键单击所选密钥组、密钥或磁带机。 然后单击**修改**。

– 密钥组

在“修改密钥组”对话框上指定更改。 然后单击**修改密钥组**。 您的角色必须具有执行修改操作和访问相应设备组的许可权。

– 密钥

在“修改密钥成员资格”对话框上指定更改。 然后单击**修改密钥成员资格**。 您的角色必须具有执行修改操作和访问相应设备组的许可权。

– 磁带机

在“修改磁带机”对话框上指定更改。然后单击**修改磁带机**。 您的角色必须具有执行修改操作和访问相应设备组的许可权。

成功指示符各不相同，显示密钥组、密钥或设备列中的更改。 表中可能不会提供对可选信息（例如磁带机描述值）进行的更改。

- 删除

要删除密钥组、密钥或磁带机，请选择密钥、密钥组或磁带机，然后单击**删除**。或者，右键单击所选密钥组、密钥或磁带机。然后单击**删除**。

– 密钥组

您无法删除与设备相关联的密钥组或标记为缺省密钥组的密钥组。 删除已填充的密钥组*还会删除该密钥组中的所有密钥*。

要确认删除，请单击**确定**。 您的角色必须具有执行删除操作和访问相应设备组的许可权。

– 密钥

删除密钥会将该密钥从与之相关联的所有密钥组中除去。 要确认删除，请单击**确定**。 您无法删除与磁带机相关联的密钥。 您的角色必须具有执行删除操作和访问相应设备组的许可权。

– 磁带机

所删除磁带机的元数据（例如磁带机序列号）将从 IBM Security Key Lifecycle Manager 数据库中除去。要确认删除，请单击**确定**。 您的角色必须具有执行删除操作和访问相应设备组的许可权。

成功指示符是已从管理表中删除密钥组、密钥或设备。

添加密钥或密钥组

您可以添加更多密钥或密钥组以用于 IBM Security Key Lifecycle Manager。

关于此任务

您可以使用“创建密钥组”对话框。另外，您还可以先使用 **tklmGroupCreate** 命令或 **Group Create REST Service** 创建要将密钥添加到的组，然后使用 **tklmSecretKeyCreate** 命令或 **Secret Key Create REST Service** 在现有组中创建一个或多个对称密钥。 您的角色必须具有执行创建操作和访问相应设备组的许可权。

开始之前，请确定有关缺省密钥组和命名密钥前缀的站点策略。

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”页面上的“密钥和设备管理”部分中，选择 **LTO**。
     c. 单击**转至 > 管理密钥和设备**。
     d. 或者，右键单击 **LTO**，然后选择**管理密钥和设备**。
     e. 在 LTO 的管理页面上，单击**添加**。
     f. 单击**密钥组**。
   - 命令行界面:

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

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

     – AIX 或 Linux 等系统:

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

2. 创建密钥或密钥组:
   - 图形用户界面
     a. 在“创建密钥组”对话框上，为必需参数和可选参数指定值。 例如，您可以选择指定此密钥组为缺省密钥组。
     b. 单击**创建密钥组**。
   - 命令行界面:
     a. 首先，创建可以将密钥添加到的组。

        输入 **tklmGroupCreate** 以创建密钥组类型的组。 例如，输入:

```
print AdminTask.tklmGroupCreate
 ('[-name GROUP-myKeyGroup -type keygroup -usage LTO]')
```

b. 接下来，使用 **tklmGroupList** 命令获取所创建的组的 UUID 值。 例如，输入：

```
print AdminTask.tklmGroupList
 ('[-name GROUP-myKeyGroup -type keygroup -v y]')
```

c. 然后，创建一组密钥并将它们存储在组中。 例如，输入：

```
print AdminTask.tklmSecretKeyCreate ('[-alias abc
-keyStoreName defaultKeyStore
 -numOfKeys 10 -usage LTO
  -keyGroupUuid KEYGROUP-316408ac-f433-4c11-92bc-0de46d05bee9]')
```

- REST 界面：

a. 使用 **Group Create REST Service** 来创建可以将密钥添加到的组。

例如，可以使用 REST 客户机发出以下 HTTP 请求：

```
POST https://localhost:9080/SKLM/rest/v1/keygroups/newGroup
Content-Type: application/json
Accept: application/json
Authorization: SKLMAuth authId=139aeh34567m
{"usage":"LTO"}
```

b. 使用 **Group List REST Service** 来获取所创建的组的 UUID 值。 例如，您可以发送以下 HTTP 请求：

```
GET https://localhost:9080/SKLM/rest/v1/keygroups?name=newGroup
Content-Type: application/json
Accept: application/json
Authorization: SKLMAuth authId=139aeh34567m
Accept-Language : en
```

c. 使用 **Secret Key Create REST Service** 创建一组密钥并将它们存储在组中。 例如，您可以发送以下 HTTP 请求：

```
POST https://localhost:9080/SKLM/rest/v1/keys
Content-Type: application/json
Accept: application/json
Authorization: SKLMAuth authId=139aeh34567m
{"alias":"abc","numOfKeys":"10","KEYGROUP-316408ac-f433-4c11-92bc-
0de46d05bee9","usage":"LTO"}
```

3. 成功指示符会根据界面的不同而不同：

- 图形用户界面：

该密钥组作为**密钥组**列中的项列出。

- 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

请在将新密钥提供给设备之前备份这些密钥。 您还可以将密钥组与特定设备进行关联。

指定回滚密钥组

您可以指定将来要用作系统缺省密钥组的密钥组。

关于此任务

您可以使用图形用户界面、**tklmKeyGroupDefaultRolloverAdd** 命令或 **Key Group Default Rollover Add REST Service** 在特定日期添加缺省密钥组回滚，以便为设备组提供密钥。您的角色必须具有执行创建操作和访问相应设备组的许可权。

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”页面上的“密钥和设备管理”部分中，选择 **LTO**。
     c. 单击**转至 > 管理缺省回滚**。
     d. 或者，右键单击 **LTO**，然后选择**管理缺省回滚**。
   - 命令行界面:

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

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

     – AIX 或 Linux 等系统:

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

2. 将现有密钥组指定为将来的系统缺省密钥组。
   - 图形用户界面:
     a. 在 LTO 的管理页面上，单击**添加**。
     b. 在“添加将来写缺省密钥组”对话框上，指定必需信息。
     c. 单击**添加将来写缺省密钥组**。

     注:
     – 请勿针对同一回滚日期指定两个缺省证书。
     – 如果回滚时不存在密钥组，那么 IBM Security Key Lifecycle Manager 将继续使用当前缺省密钥组。
     – 您可以添加或删除表条目，但无法修改条目。
   - 命令行界面:

     添加回滚密钥组。例如，输入:

     ```
     print AdminTask.tklmKeyGroupDefaultRolloverAdd
     ('[-usage LTO -keyGroupName myLTOkeygroup
          -effectiveDate 2010-04-30]')
     ```

3. 成功指示符会根据界面的不同而不同:
   - 图形用户界面:

     该回滚密钥组在 LTO 管理页面上的回滚密钥组表中列出。
   - 命令行界面:

完成消息表示成功。

4. 要从回滚表中删除密钥组，您的角色必须具有执行删除操作的许可权。
   - 图形用户界面:

     选择密钥组，然后单击**删除**。
   - 命令行界面:

     使用 **tklmKeyGroupDefaultRolloverList** 命令来查找密钥组的通用唯一标识。 您的角色必须具有执行查看操作和访问相应设备组的许可权。然后，使用 **tklmKeyGroupDefaultRolloverDelete** 命令将该密钥组从回滚列表中除去。 您的角色必须具有执行删除操作和访问相应设备组的许可权。

     例如，输入:

     ```
     print AdminTask.tklmKeyGroupDefaultRolloverList
     ('[-usage LTO]')

     print AdminTask.tklmKeyGroupDefaultRolloverDelete
     ('[-uuid 201]')
     ```

指定密钥仅使用一次

您可以指定密钥组中的密钥仅使用一次。 例如，为了确保安全，您可以阻止再次使用为密钥组定义的先前已使用过的密钥。

关于此任务

您可以使用命令行界面和 SKLMConfig.properties 文件中的 **stopRoundRobinKeyGrps** 特性。 您的角色必须具有执行配置操作的许可权。除非您将此特性的值设置为 true，否则此特性最初不会出现在特性文件中。 此特性只能通过使用命令行界面来设置。

要点:

- 如果密钥组在使用中并且已提供密钥组中的最后一个密钥，那么开启此标志会导致停止提供密钥。 在密钥提供写请求中，有对此组中密钥的其他请求会导致错误，并向设备发送错误代码 0xEE34 (NO_KEY_TO_SERVE)。 要能够成功处理新的密钥提供写请求，请将新的密钥添加到密钥组中。 或者，您可以指定使用具有可用密钥的其他密钥组。 只要所请求的密钥存在，密钥提供读请求始终会成功。
- 在严格遵守政府规范和 FIPS 140 的环境中使用此属性。 启用此属性时，必须主动监视密钥组。 确保密钥组不会用光密钥，从而导致服务器停止提供密钥以及磁带写请求失败。
- 如果已开启此标志，请不要将其关闭。 例如，如果您开启此标志，密钥组不会提供先前使用过的密钥。 如果关闭此标志，将提供组中的下一个密钥。 在提供组中的最后一个密钥之后，下一个提供的密钥将是组中的第一个密钥。
- 设置此选项时，不要单独将属于密钥组的各个密钥别名分配给设备。

过程

1. 浏览至相应的目录:

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

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

- AIX 或 Linux 等系统:

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

2. 首先，确定 SKLMConfig.properties 文件中此特性的当前状态。除非您将此特性的值设置为 true，否则此特性最初不会出现在特性文件中。
   - 命令行界面:

     在 **wsadmin** 提示符处，输入以下 Jython 格式化命令:

     ```
     print AdminTask.tklmConfigGetEntry
      ('[-name stopRoundRobinKeyGrps]')
     ```

   - REST 界面:

     使用 **Get Single Config Property REST Service** 来获取此特性的当前值。 发送以下 HTTP 请求:

     ```
     GET https://localhost:9080/SKLM/rest/v1/configProperties/
     stopRoundRobinKeyGrps
     Content-Type: application/json
     Accept : application/json
     Authorization: SKLMAuth userAuthId=139aeh34567m
     Accept-Language : en
     ```

3. 在 SKLMConfig.properties 文件中，将 **stopRoundRobinKeyGrps** 特性的状态更改为值 true。
   - 命令行界面:

     输入以下 Jython 格式化命令:

     ```
     print AdminTask.tklmConfigUpdateEntry ('[-name stopRoundRobinKeyGrps
      -value true]')
     ```

   - REST 界面:

     发送以下 HTTP 请求:

     ```
     PUT https://localhost:9080/SKLM/rest/v1/configProperties
     Content-Type: application/json
     Accept: application/json
     Authorization: SKLMAuth authId=139aeh34567m
     Accept-Language: en
     { "stopRoundRobinKeyGrps": "true"}
     ```

4. 要确定是否成功，请再次输入 **tklmConfigGetEntry** 命令或使用 **Get Single Config Property REST Service**。

   另外，在图形用户界面中的“欢迎”页面上，您可能会在“操作项”部分中看到一条警告。 此部分列出可用密钥百分比为 10% 或更少的密钥组。 双击此表中的条目可以访问“修改密钥组”对话框，您可以在此对话框中添加更多密钥以供组使用。

   不存在任何其他警告。低密钥计数警告适用于所有密钥组，包括指定为缺省密钥组的密钥组。

修改密钥组

您可以修改有关 IBM Security Key Lifecycle Manager 数据库中密钥组中的对象的信息。

关于此任务

您可以使用“修改密钥组”对话框。另外，您还可以使用下列命令或 REST 界面来修改 IBM Security Key Lifecycle Manager 数据库中密钥组中的对象。

- **tklmGroupEntryAdd** 和 **tklmGroupEntryDelete**
- **Group Entry Add REST Service** 和 **Group Entry Delete REST Service**

您的角色必须具有执行修改操作和访问相应设备组的许可权。

开始之前，请确定要对组更改的信息，例如要添加到组的更多密钥数。

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”页面上的“密钥和设备管理”部分中，选择 **LTO**。
     c. 单击**转至 > 管理密钥和设备**。
     d. 或者，右键单击 **LTO**，然后选择**管理密钥和设备**。
     e. 在 LTO 的管理页面上，在**密钥组**列中选择密钥组。
     f. 单击**修改**。
     g. 或者，右键单击密钥组，然后选择**修改**，或双击密钥组条目。
   - 命令行界面:

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

     – Windows 系统:

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

     – AIX 或 Linux 等系统:

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

2. 修改密钥组信息:
   - 图形用户界面:
     a. 在“修改密钥组”对话框上，更改相应的字段。 您的角色必须具有执行各项操作的特定许可权。 例如，要从组中删除密钥，您的角色必须具有执行删除操作和访问相应设备组的许可权。
     b. 单击**修改密钥组**。
   - 命令行界面:

     您可以删除组中的对象，也可以将对象添加到组。

     – 从组中删除密钥。 您的角色必须具有执行删除操作和访问相应设备组的许可权。例如，输入以下命令:

     ```
     print AdminTask.tklmGroupEntryDelete ('[-entry "{type key}
      {uuid KEY-a3ce9230-bef9-42bd-86b7-6d208ec119cf}"
        -name GROUP-myKeyGroup -type keygroup]')
     ```

– 将同一密钥再次添加回组。 您的角色必须具有执行修改操作和访问相应设备组的许可权。例如，输入以下命令:

```
print AdminTask.tklmGroupEntryAdd('[-name GROUP-myKeyGroup
 -type keygroup -entry "{type key}
  {alias aaa000000000000000000}
   {keyStoreName defaultKeyStore}"]')
```

- REST 界面:

  要从组中删除密钥，您可以发送以下 HTTP 请求:

```
DELETE https://localhost:9080/SKLM/rest/v1/keygroups/KEY-a3ce9230-bef9-
42bd-86b7-6d208ec119cf
Content-Type: application/json
Accept: application/json
Authorization: SKLMAuth userAuthId=139aeh34567m
```

  要将同一密钥再次添加回组，您可以发送以下 HTTP 请求:

```
POST https://localhost:9080/SKLM/rest/v1/keygroupentry
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth userAuthId=139aeh34567m
{"name":"GROUP-myKeyGroup", "entry": "KEY-a3ce9230-bef9-42bd-86b7-
6d208ec119cf"}
```

3. 成功指示符会根据界面的不同而不同:
   - 图形用户界面:

     对于必填字段，将显示一列，用于显示更改后的数据。 对于可选字段，您可能需要重新打开“修改密钥组”对话框以查看更改后的值，然后单击**取消**。
   - 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

接下来，您可以使用 LTO“密钥和设备管理”页面将密钥组与特定设备进行关联。

删除密钥或密钥组

您可以删除选中的密钥或密钥组。 您无法删除与设备相关联的密钥或密钥组，或标记为缺省密钥组的密钥组。

关于此任务

仅当不再需要密钥所保护的数据时，才能删除这些密钥。 删除密钥类似于擦除数据。 删除密钥后，无法对这些密钥保护的数据进行检索。

您可以使用**删除**菜单项。 另外，您还可以使用下列命令或 REST 服务来删除密钥或删除密钥组。

- **tklmKeyDelete** 或 **Delete Key REST Service**
- **tklmGroupDelete** 或 **Group Delete REST Service**

您的角色必须具有执行删除操作和访问相应设备组的许可权。

删除之前，请执行下列验证:

- 密钥

  请确保存在要删除的密钥所在密钥库的备份。

- 密钥组

  如果您使用命令行界面，请获取要删除的密钥组的 UUID。 请验证该密钥组当前是否未与设备相关联，并且是否未标记为缺省密钥组。

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”页面上的“密钥和设备管理”部分中，选择 **LTO**。
     c. 单击**转至 > 管理密钥和设备**。
     d. 或者，右键单击 **LTO**，然后选择**管理密钥和设备**。
     e. 在 LTO 的管理页面上，在相应的列中选择密钥或密钥组。
     f. 单击**删除**。
     g. 或者，右键单击密钥或密钥组，然后选择**删除**。
   - 命令行界面:

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

     – Windows 系统:

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

     – AIX 或 Linux 等系统:

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

2. 删除密钥或密钥组:
   - 图形用户界面:

     在“确认”对话框上，阅读确认消息，然后删除密钥或密钥组。 请验证是否选择了正确的密钥或密钥组。 例如，您可以删除空密钥组。 删除已填充的密钥组*还会删除该密钥组中的所有密钥*。 删除属于某个密钥组的密钥还会将该密钥从该组中除去。 然后单击**确定**。
   - 命令行界面:
     – 密钥

       输入 tklmKeyDelete 以删除密钥。 例如，要删除当前未与设备相关联的密钥，请先找到该密钥。 您可以使用 **tklmKeyList** 命令来找到要删除的密钥。 例如，输入:

       ```
       print AdminTask.tklmKeyList ('[-usage LTO
        -attributes "{state active}" -v y]')
       ```

       然后，删除该密钥。 例如，输入:

```
print AdminTask.tklmKeyDelete ('[-alias aaa000000000000000000
 -keyStoreName defaultKeyStore]')
```

删除密钥会从数据库中删除密钥数据。

– 密钥组

输入 tklmGroupDelete 以删除密钥组。 例如，您可以删除空密钥组。 删除已填充的密钥组*还会删除该密钥组中的所有密钥*。 例如，要删除当前未与设备相关联的密钥组，请输入以下命令:

```
print AdminTask.tklmGroupDelete
 ('[-uuid GROUP-7d588437-e725-48bf-a836-00a47df64e78]')
```

- REST 界面:
  – 密钥

使用 **Delete Key REST Service** 来删除密钥。 使用 **List Key REST Service** 来查找要删除的密钥。 例如，您可以发送以下 HTTP 请求:

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

发送以下 HTTP 请求以删除该密钥:

```
DELETE https://localhost:9080/SKLM/rest/v1/keys/aaa000000000000000000
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth userAuthId=139aeh34567m
```

– 密钥组

使用 **Group Delete REST Service** 来删除密钥组。 例如，您可以发送以下 HTTP 请求:

```
https://localhost:9080/SKLM/rest/v1/keygroups/GROUP-7d588437-e725-
48bf-a836-00a47df64e78
Content-Type: application/json
Accept: application/json
Authorization: SKLMAuth userAuthId=139aeh34567m
```

3. 成功指示符会根据界面的不同而不同:
   - 图形用户界面:

     已从表中除去该密钥或密钥组。 已从密钥库中删除密钥数据。
   - 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

刷新表以确保删除了密钥或密钥组。 请备份密钥库以准确地反映密钥更改。 备份数据库以反映密钥组更改。

添加磁带机

您可以将磁带机之类的设备添加到 IBM Security Key Lifecycle Manager 数据库。

关于此任务

您可以使用“添加磁带机”对话框。另外，您还可以使用 **tklmDeviceAdd** 命令或 **Device Add REST Service** 来添加设备。 您的角色必须具有执行创建操作和访问相应设备组的许可权。

开始之前，请创建要与将要识别的设备相关联的密钥和密钥组。 另外，请获取磁带机序列号和其他描述信息。 确定磁带机使用的是特定密钥组还是系统缺省密钥组。

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”页面上的“密钥和设备管理”部分中，选择 **LTO**。
     c. 单击**转至 > 管理密钥和设备**。
     d. 或者，右键单击 **LTO**，然后选择**管理密钥和设备**。
     e. 在 LTO 的管理页面上，单击**添加**。
     f. 单击**磁带机**。
   - 命令行界面:

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

     – Windows 系统:

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

     – AIX 或 Linux 等系统:

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

2. 添加设备:
   - 图形用户界面:

     在“添加磁带机”对话框中，输入必需信息和可选信息。 然后单击**添加磁带机**。
   - 命令行界面:

     输入 tklmDeviceAdd 以添加设备。 必须指定设备组和序列号。例如，输入:

     ```
     print AdminTask.tklmDeviceAdd ('[-type LTO -serialNumber FAA49403AQJF
       -attributes "{worldwideName ABCdeF1234567890}
       {description salesDivisionDrive} {symAlias LTOKeyGroup1}"]')
     ```

   - REST 界面:

     使用 **Device Add REST Service** 来添加设备。 例如，您可以发送以下 HTTP 请求:

```
POST https://localhost:9080/SKLM/rest/v1/devices
Content-Type: application/json
Accept : application/json
Authorization : SKLMAuth userAuthId=37ea1939-1374-4db7-84cd-14e399be2d20
Accept-Language : en
{"type":"LTO","serialNumber":"FAA49403AQJF","attributes":"worldwideName
ABCdeF1234567890,description salesDivisionDrive"}
```

3. 成功指示符会根据界面的不同而不同:
   - 图形用户界面:

     已将该设备添加到表。
   - 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

接下来，您可以确定所添加的磁带机的状态。

修改磁带机

您可以修改有关 IBM Security Key Lifecycle Manager 数据库中的设备（例如磁带机）的信息。例如，您可以更新对磁带机的描述。

关于此任务

您可以使用“修改磁带机”对话框、**tklmDeviceUpdate** 命令或 **Device Update REST Service** 来更新设备。 您的角色必须具有执行修改操作和访问相应设备组的许可权。

开始之前，请创建要与将要修改的设备相关联的密钥和密钥组。 如果您使用命令行界面，请获取要更新的设备的 UUID 值。

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”页面上的“密钥和设备管理”部分中，选择 **LTO**。
     c. 单击**转至 > 管理密钥和设备**。
     d. 或者，右键单击 **LTO**，然后选择**管理密钥和设备**。
     e. 在 LTO 的管理页面上，在**磁带机**列中选择磁带机。
     f. 单击**修改**。
     g. 或者，右键单击磁带机，然后选择**修改**，或双击磁带机条目。
   - 命令行界面:

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

– Windows 系统:

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

– AIX 或 Linux 等系统:

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

2. 修改设备:
   - 图形用户界面:
     a. 在“修改磁带机”对话框中，输入必需信息和可选信息。
     b. 单击**修改磁带机**。
   - 命令行界面:

     输入 tklmDeviceUpdate 以更新设备。 必须指定设备 UUID 以及发生了更改的属性。 例如，输入:

     ```
     print AdminTask.tklmDeviceList ('[-type lto]')
     ```

     ```
     print AdminTask.tklmDeviceUpdate
      ('[-uuid DEVICE-44b123ad-5ed8-4934-8c84-64cb9e11d990
       -attributes "{symAlias LTOKey000001} {description myLTOdrive}"]')
     ```

   - REST 界面:

     使用 **Device Update REST Service** 来更新设备。 必须指定设备 UUID 以及发生了更改的属性。 例如，您可以发送以下 HTTP 请求:

     ```
     GET https://localhost:9080/SKLM/rest/v1/devices?type=LTO
     Content-Type: application/json
     Accept : application/json
     Authorization: SKLMAuth userAuthId=139aeh34567m
     Accept-Language : en
     ```

     ```
     PUT https://localhost:9080/SKLM/rest/v1/devices
     Content-Type: application/json
     Accept : application/json
     Authorization: SKLMAuth userAuthId=139aeh34567m
     {"uuid":"DEVICE-44b123ad-5ed8-4934-8c84-64cb9e11d990","attributes":
     "symAlias LTOKey000001,description myLTOdrive"}
     ```

3. 成功指示符会根据界面的不同而不同:
   - 图形用户界面:

     已更改表中的设备信息。
   - 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

接下来，您可以验证是否进行了更改。 对于描述之类的可选字段，您可能希望运行 **tklmDeviceList** 命令或 **Device List REST Service** 来确定是否更改了值。或者，重新打开“修改磁带机”对话框。

删除磁带机

您可以删除磁带机之类的设备。 所删除设备的元数据（例如设备序列号）将从 IBM Security Key Lifecycle Manager 数据库中除去。

关于此任务

您可以使用“删除”菜单项、**tklmDeviceDelete** 命令或 **Device Delete REST Service** 来删除设备。 您的角色必须具有执行删除操作和访问相应设备组的许可权。

开始之前，请确保存在 IBM Security Key Lifecycle Manager 数据库的当前备份。如果您使用命令行界面或 REST 界面，请获取要删除的设备的 UUID。

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”页面上的“密钥和设备管理”部分中，选择 **LTO**。
     c. 单击**转至 > 管理密钥和设备**。
     d. 或者，右键单击 **LTO**，然后选择**管理密钥和设备**。
     e. 在 LTO 的管理页面上，选择设备。
     f. 单击**删除**。
     g. 或者，右键单击磁带机，然后选择**删除**。
   - 命令行界面:

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

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

     – AIX 或 Linux 等系统:

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

2. 删除设备:
   - 图形用户界面:

     在“确认”对话框上，阅读确认消息，然后删除设备。 所删除磁带机的元数据（例如设备序列号）将从 IBM Security Key Lifecycle Manager 数据库中除去。单击**确定**。
   - 命令行界面:

     输入 tklmDeviceDelete 以删除设备。 必须指定 UUID。 例如，输入:

     ```
     print AdminTask.tklmDeviceList ('[-type lto]')

     print AdminTask.tklmDeviceDelete
      ('[-uuid DEVICE-74386920-148c-47b2-a1e2-d19194b315cf]')
     ```

   - REST 界面:

使用 **Device Delete REST Service** 来删除设备。 必须指定设备 UUID。 例如，可以使用 REST 客户机发出以下 HTTP 请求:

```
GET https://localhost:9080/SKLM/rest/v1/devices?type=LTO
Content-Type: application/json
Accept : application/json
Authorization : SKLMAuth userAuthId=37ea1939-1374-4db7-84cd-14e399be2d20
Accept-Language : en

DELETE https://localhost:9080/SKLM/rest/v1/devices/DEVICE-74386920-148c-
47b2-a1e2-d19194b315cf
Content-Type: application/json
Accept : application/json
Authorization : SKLMAuth userAuthId=37ea1939-1374-4db7-84cd-14e399be2d20
```

3. 成功指示符会根据界面的不同而不同:
   - 图形用户界面:

     已从表中除去该设备。
   - 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。

3592 磁带机管理

您可以使用 IBM Security Key Lifecycle Manager 来管理 3592 磁带机。

某些步骤的描述提供了使用图形用户界面、命令行界面或 REST 界面而完成的备选步骤。 对于任何一个工作会话，都不要在界面之间进行切换。

一些任务的描述可能会提及 SKLMConfig.properties 文件中与任务相关的属性。使用图形用户界面、命令行界面或 REST 界面可更改这些属性。

创建证书和磁带机的指导步骤

首次创建证书和磁带机以及稍后添加更多证书或磁带机时，IBM Security Key Lifecycle Manager 会提供一组指导步骤来完成该任务。

对某些步骤的描述可能会提及用于执行同一任务的命令行或 REST 界面替代方法。 在指导任务集中，请使用图形用户界面来完成这些任务。

创建证书或证书请求

作为第一个活动，您可以创建用于 IBM Security Key Lifecycle Manager 的证书或证书请求。

关于此任务

您可以使用“创建证书”对话框。另外，您还可以使用下列任何命令或 REST 服务来创建证书或证书请求:

- **tklmCertCreate** 或 **tklmCertGenRequest**
- **Create Certificate REST Service** 或 **Certificate Generate Request REST Service**

您的角色必须具有执行创建操作和访问相应设备组的许可权。 要使此证书成为缺省证书，您的角色必须具有执行修改操作的许可权。

如果您还希望指定将证书用作系统缺省证书或合作伙伴证书，那么可以使用下列命令或 REST 服务:

- **tklmDeviceGroupAttributeList** 和 **tklmDeviceGroupAttributeUpdate**
- **Device Group Attribute List REST Service** 和 **Device Group Attribute Update REST Service**

这些值先前存储在过时的 **drive.default.alias1**（对于系统缺省证书）或 **drive.default.alias2**（对于系统合作伙伴证书）属性中。

开始之前，请确定有关使用自签名证书和认证中心 (CA) 发放的证书的站点策略。 您可能希望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。

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”页面上的“密钥和设备管理”部分中，选择 **3592**。
     c. 单击**转至 > 根据指导创建密钥和设备**。
     d. 或者，右键单击 **3592**，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. 创建证书或请求获取证书:
   - 图形用户界面:
     a. 在“步骤 1: 创建证书”页面上，在**证书**表上单击**创建**。
     b. 在“创建证书”对话框上，选择自签名证书或针对第三方提供者的证书请求。
     c. 指定必需和可选参数的值。 例如，您可以选择指定证书为缺省证书或合作伙伴证书。
     d. 单击**创建证书**。
   - 命令行界面:
     – 证书

输入 tklmCertCreate 以创建证书和公用/专用密钥对，并将证书存储在现有密钥库中。 例如，输入:

```
print AdminTask.tklmCertCreate ('[-type selfsigned
 -alias sklmCertificate -cn sklm -ou sales -o myCompanyName
   -usage 3592 -country US -keyStoreName defaultKeyStore
    -validity 999]')
```

– 证书请求

输入 tklmCertGenRequest 以创建 PKCS #10 证书请求文件。 例如，输入:

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

- REST 界面:
  – 证书
    a. 获取用于访问 IBM Security Key Lifecycle Manager REST 服务的唯一用户认证标识。 有关认证过程的更多信息，请参阅 REST 服务的验证流程。
    b. 要调用 **Create Certificate REST Service**，请发送 HTTP POST 请求。请将您在步骤 a 中获取的用户认证标识随请求消息一起传递，如以下示例所示。

```
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":"sklmCertificate1",
"cn":"sklm","ou":"sales",
"o":"myCompanyName","usage":"3592","country":"US",
"validity":"999", "
algorithm ": " RSA " }
```

  – 证书请求

使用 **Certificate Generate Request REST Service** 来创建 PKCS #10 证书请求文件。 例如，您可以发送以下 HTTP 请求:

```
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"}
```

3. 成功指示符会根据界面的不同而不同:
   - 图形用户界面:

     证书或证书请求作为**证书**表中的项列出。
   - 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

请在将新证书提供给设备之前备份这些证书。 对于证书请求，下一步可能是导入签名证书。 您可以转至下一步以定义特定设备，并将证书与这些设备进行关联。 请选择**步骤 2: 识别磁带机**或单击**转至下一步**。

对于 3592 设备组，也应为 IBM Security Key Lifecycle Manager 数据库中的系统缺省证书和合作伙伴证书指定值。使用 **tklmDeviceGroupAttributeUpdate** 命令或 **Device Group Attribute Update REST Service** 来设置这些值。

识别磁带机

您可以识别要用于 IBM Security Key Lifecycle Manager 的 3592 磁带机。

关于此任务

您可以使用“添加磁带机”对话框、**tklmDeviceAdd** 命令或 **Device Add REST Service** 来添加设备。 您的角色必须具有执行创建操作和访问相应设备组的许可权。

开始之前，请创建要与将要识别的设备相关联的证书。

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”页面上的“密钥和设备管理”部分中，选择 **3592**。
     c. 单击**转至 > 根据指导创建密钥和设备**。
     d. 或者，右键单击 **3592**，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. 跳过**步骤 1: 创建证书**。单击**转至下一步**链接，或者单击**步骤 2: 识别磁带机**。
3. 您可以指定 IBM Security Key Lifecycle Manager 存放新的设备请求以等待您的审核。 您的角色必须具有执行修改操作和访问相应设备组的许可权。
   - 图形用户界面:

     选择**保留正在等待我审核的新设备请求**。
   - 命令行界面:

使用 **tklmDeviceGroupAttributeUpdate** 命令或 **Device Group Attribute Update REST Service** 来设置 **device.AutoPendingAutoDiscovery** 属性的值。例如，输入:

```
print AdminTask.tklmDeviceGroupAttributeUpdate ('[-name 3592
  -attributes "{device.AutoPendingAutoDiscovery 2}"]')
```

- REST 界面:

  a. 获取用于访问 IBM Security Key Lifecycle Manager REST 服务的唯一用户认证标识。 有关认证过程的更多信息，请参阅 REST 服务的验证流程。

  b. 要调用 **Device Group Attribute Update REST Service** 以及设置 **device.AutoPendingAutoDiscovery** 属性的值，请发送 HTTP PUT 请求。请将您在步骤 a 中获取的用户认证标识随请求消息一起传递，如以下示例所示。

  ```
  PUT https://localhost:9080/SKLM/rest/v1/deviceGroupAttributes
  Content-Type: application/json
  Accept : application/json
  Authorization: SKLMAuth authId=139aeh34567m
  {"name":"3592","attributes":"device.AutoPendingAutoDiscovery 2"}
  ```

4. 添加设备:

   - 图形用户界面:

     a. 在“步骤 2: 识别磁带机”页面上，在**设备**表中单击**添加**。

     b. 在“添加磁带机”对话框中，输入必需信息和可选信息。

     c. 单击**添加磁带机**。

   - 命令行界面:

     输入 tklmDeviceAdd 以添加设备。 必须指定设备组和序列号。例如，输入:

     ```
     print AdminTask.tklmDeviceAdd ('[-type 3592 -serialNumber CDA39403AQJF
       -attributes "{worldwideName ABCdeF1234567890}
       {description marketingDivisionDrive}
        {aliasOne encryption_cert}"]')
     ```

   - REST 界面:

     您可以使用 **Device Add REST Service** 来添加设备。 例如，您可以发送以下 HTTP 请求:

     ```
     POST https://localhost:9080/SKLM/rest/v1/devices
     Content-Type: application/json
     Accept : application/json
     Authorization : SKLMAuth userAuthId=37ea1939-1374-4db7-84cd-14e399be2d20
     Accept-Language : en
     {"type":"3592","serialNumber":"CDA39403AQJF","attributes":"worldwideName
     ABCdeF1234567890,description marketingDivisionDrive"}
     ```

5. 成功指示符会根据界面的不同而不同:

   - 图形用户界面:

     已将该设备添加到**设备**表。

   - 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

接下来，您可以使用 3592“密钥和设备管理”页面来查看所有证书和设备。

管理证书和设备

要管理证书和设备，您可能希望确定其状态。 您可以映射其关联，或者添加、修改或删除特定证书或设备。

关于此任务

使用 3592“密钥和设备管理”页面来将证书映射到设备，以确定表中各项的状态。 您可以添加、修改或删除证书或设备。 您的角色必须具有执行查看操作和访问相应设备组的许可权。

开始之前，先检查该页面上的列（页面上提供了用于添加、修改或删除表项的各个按钮）。 要对信息进行排序，请单击列标题。

表组织成下列区域:

- 在左侧列中，有关证书的信息指示证书名称、证书是用作系统缺省证书还是系统合作伙伴证书、到期日期以及证书的状态。
- 在右侧列中，有关磁带机的信息指示磁带机名称，以及磁带机是使用系统缺省证书还是合作伙伴证书作为其缺省证书。
- “状态”图标指示证书的状态。

表 3. “状态”图标及其含义

图标	描述
	证书处于有效状态。
	证书处于已泄密状态。
	证书即将到期。
	证书处于到期状态。
	对于具有将来使用时间戳记的已迁移证书，证书从将来日期开始生效。
	IBM Security Key Lifecycle Manager 具有正在等待签名和导入的第三方证书请求。

过程

1. 登录图形用户界面:
   a. 在“欢迎”页面上的“密钥和设备管理”部分中，选择 **3592**。
   b. 单击**转至 > 管理密钥和设备**。
   c. 或者，右键单击 **3592**，然后选择**管理密钥和设备**。

   某些步骤的描述提供了使用图形用户界面、命令行界面或 REST 界面而完成的备选步骤。 对于任何一个工作会话，都不要在界面之间进行切换。

一些任务的描述可能会提及 SKLMConfig.properties 文件中与任务相关的属性。使用图形用户界面、命令行界面或 REST 界面可更改这些属性。

2. 在 3592“密钥和设备管理”页面上，您可以添加、修改或删除证书或磁带机。 另外，您还可以监视证书的状态。

   您可以执行下列管理任务:

   - 添加

     单击**添加**。 另外，您还可以选择用于创建证书和磁带机的逐步过程。

     – 证书

       在“创建证书”对话框上，选择自签名或来自第三方提供者作为证书类型，并填写必需信息。 然后单击**创建证书**。 您的角色必须具有执行创建操作和访问相应设备组的许可权。 要使此证书成为缺省证书，您的角色必须具有执行修改操作的许可权。

     – 磁带机

       在“添加磁带机”对话框中，输入磁带机信息。 然后单击**添加磁带机**。 您的角色必须具有执行创建操作和访问相应设备组的许可权。

     – 使用逐步过程来创建证书和磁带机

       在“步骤 1: 创建证书”和“步骤 2: 识别磁带机”页面上，输入必需信息。

     成功指示符各不相同，显示证书或设备列中的更改。

   - 修改

     要更改或删除证书或磁带机，请选择证书或磁带机，然后单击**修改**。或者，右键单击所选证书或磁带机。 然后单击**修改**，或者双击列表中的证书或设备条目。

     – 证书

       在“修改证书”对话框中指定更改。然后单击**修改证书**。 您的角色必须具有执行修改操作和访问相应设备组的许可权。

     – 磁带机

       在“修改磁带机”对话框中指定更改。然后单击**修改磁带机**。 您的角色必须具有执行修改操作和访问相应设备组的许可权。

     成功指示符各不相同，显示证书或设备列中的更改。 表中可能不会提供对某些信息（例如可选字段）的更改。

   - 删除

     要删除证书或磁带机，请在表中突出显示该条目，然后单击**删除**。 或者，右键单击所选证书或磁带机。 然后单击**删除**。

     – 证书

       删除证书之前，请确保您具有密钥库的当前备份。 任何使用此证书编写的磁带将在删除此证书后变得不可读。要删除的证书可以处于任何状态（例如“活动

”）。您无法删除与设备相关联的证书，而与其状态无关。 您也无法删除标记为缺省证书或合作伙伴证书的证书。 您的角色必须具有执行删除操作和访问相应设备组的许可权。

删除证书从数据库中删除数据。

要确认删除，请单击**确定**。

– 磁带机

所删除磁带机的元数据（例如磁带机序列号）将从 IBM Security Key Lifecycle Manager 数据库中除去。要确认删除，请单击**确定**。 您的角色必须具有执行删除操作和访问相应设备组的许可权。

成功指示符是已从管理表中除去证书或设备。

添加证书或证书请求

您可以添加更多证书或证书请求以用于 IBM Security Key Lifecycle Manager。

关于此任务

您可以使用“创建证书”对话框。另外，您还可以使用下列任何命令或 REST 服务来创建证书或证书请求:

- **tklmCertCreate** 或 **tklmCertGenRequest**
- **Create Certificate REST Service** 或 **Certificate Generate Request REST Service**

您的角色必须具有执行创建操作和访问相应设备组的许可权。 要使此证书成为缺省证书，您的角色必须具有执行修改操作的许可权。

开始之前，请确定有关使用自签名证书和 CA 证书的站点策略。 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。

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”页面上的“密钥和设备管理”部分中，选择 **3592**。
     c. 单击**转至 > 管理密钥和设备**。
     d. 或者，右键单击 **3592**，然后选择**管理密钥和设备**。
     e. 在 3592 的管理页面上，单击**添加**。
     f. 单击**证书**。
   - 命令行界面:

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

     – Windows 系统:

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

– AIX 或 Linux 等系统:

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

2. 创建证书或请求获取证书:

- 图形用户界面:
  a. 在“创建证书”对话框上，选择自签名证书或针对第三方提供者的证书请求。
  b. 指定必需和可选参数的值。 例如，您可以选择指定此证书为缺省证书或合作伙伴证书。 然后单击**创建证书**。
- 命令行界面:
  – 证书:

    输入 tklmCertCreate 以创建证书和公用/专用密钥对，并将证书存储在现有密钥库中。 例如，输入:

    ```
    print AdminTask.tklmCertCreate ('[-type selfsigned
     -alias sklmCertificate -cn sklm -ou sales -o myCompanyName
       -usage 3592 -country US -keyStoreName defaultKeyStore
        -validity 999]')
    ```

  – 证书请求:

    输入 tklmCertGenRequest 以创建 PKCS #10 证书请求文件。 例如，输入:

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

- REST 界面:
  – 证书

    使用 **Create Certificate REST Service** 来创建证书和公用/专用密钥对，并将证书存储在现有密钥库中。 例如，可以使用 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":"sklmCertificate1",
    "cn":"sklm","ou":
    "sales","o":"myCompanyName","usage":"3592",
    "country":"US","validity":
    "999", "algorithm ": " RSA " }
    ```

  – 证书请求

    使用 **Certificate Generate Request REST Service** 来创建 PKCS #10 证书请求文件。 例如，可以使用 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
    {"type":"certreq","alias":"sklmCertificate1",
    "cn":"sklm","ou":
    "sales","o":"myCompanyName","usage":"3592",
    "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**列表中的项。
   - 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

您的下一步操作取决于您已创建证书还是证书请求。

- 证书:

  请在将新证书提供给设备之前备份这些证书。 您可以将证书与特定设备进行关联。
- 证书请求:

  手动将证书请求发送到认证中心。 返回签名证书后，请使用“欢迎”面板上的暂挂操作项，或者使用 **tklmCertImport** 命令或 **Certificate Import REST Service** 导入该证书。 导入完成后，请备份该证书以启用向设备提供该证书。

指定回滚证书

您可以指定证书将来是用做系统缺省证书还是系统合作伙伴证书。

关于此任务

您可以使用图形用户界面、**tklmCertDefaultRolloverAdd** 命令或 **Cert Default Rollover Add REST Service** 来添加特定日期的缺省证书回滚以及设备组。 您的角色必须具有执行创建操作和访问相应设备组的许可权。

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”页面上的“密钥和设备管理”部分中，选择 **3592**。
     c. 单击**转至 > 管理缺省回滚**。
     d. 或者，右键单击 **3592**，然后选择**管理缺省回滚**。
   - 命令行界面:

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

       ```
       wsadmin -username SKLMAdmin -password mypwd -lang jython
       ```
     – AIX 或 Linux 等系统:

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

2. 指定现有证书将来是用做系统缺省证书还是系统合作伙伴证书。
   - 图形用户界面:
     a. 在 3592 的管理页面上，单击**添加**。
     b. 在“添加将来写缺省密钥组”对话框上，指定必需信息。
     c. 单击**添加将来写缺省密钥组**。

     注:
     – 请勿针对同一回滚日期指定两个缺省证书。
     – 不会验证所选证书已到期还是在回滚时到期。
     – 如果回滚时不存在证书，那么 IBM Security Key Lifecycle Manager 将继续使用当前缺省证书。
     – 您可以添加或删除表条目，但无法修改条目。
   - 命令行界面:

     添加回滚证书。例如，输入:

     ```
     print AdminTask.tklmCertDefaultRolloverAdd
     ('[-usage 3592 -alias tklmcert1
          -certDefaultType 1 -effectiveDate 2010-05-30]')
     ```
3. 成功指示符会根据界面的不同而不同:
   - 图形用户界面:

     该证书显示在“3592”页面上的回滚证书表中。
   - 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。
4. 要从回滚表中删除证书，您可以执行下列操作:
   - 图形用户界面:

     选择证书，然后单击**删除**。 您的角色必须具有执行删除操作的许可权。 请阅读警告消息。 然后单击**确定**。
   - 命令行界面:

     使用 **tklmCertDefaultRolloverList** 命令来查找证书的通用唯一标识。 您的角色必须具有执行查看操作和访问相应设备组的许可权。然后，使用 **tklmCertDefaultRolloverDelete** 命令将该证书从回滚列表中除去。 您的角色必须具有执行删除操作和访问相应设备组的许可权。例如，输入以下命令:

     ```
     print AdminTask.tklmCertDefaultRolloverDelete
     ('[-uuid 101]')
     ```

   该证书已取消标记为将来系统缺省证书或合作伙伴证书，但不会进行更改或删除。

修改证书

您可以修改证书是用作系统缺省证书还是系统合作伙伴证书。

关于此任务

您可以使用“修改证书”对话框来修改证书。 另外，您还可以使用下列命令或 REST 服务:

- **tklmCertUpdate** 或 **Certificate Update REST Service**，用于修改证书的状态（例如“受信任”或“已泄密”）以及修改证书信息。
- **tklmDeviceTypeAttributeUpdate** 或 **Device Type Attribute Update REST Service**，用于将证书设置为系统缺省证书或系统合作伙伴证书。

您的角色必须具有执行修改操作和访问相应设备组的许可权。

开始之前，请确定证书更改后的信息，例如描述，或您希望将证书用作系统缺省证书还是系统合作伙伴证书。如果您使用命令行界面，请获取证书的 UUID 值。

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”页面上的“密钥和设备管理”部分中，选择 **3592**。
     c. 单击**转至 > 管理密钥和设备**。
     d. 或者，右键单击 **3592**，然后选择**管理密钥和设备**。
     e. 在 3592 的管理页面上，在**证书**列中选择证书。
     f. 单击**修改**。
     g. 或者，右键单击证书，然后选择**修改**，或双击证书条目。
   - 命令行界面:

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

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

     – AIX 或 Linux 等系统:

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

2. 修改证书信息:
   - 图形用户界面:

     在“修改证书”对话框上，更改相应的字段。 然后单击**修改证书**。
   - 命令行界面:

     输入 tklmCertList 以查找证书，然后输入 tklmCertUpdate 以更新证书。 必须指定证书的 UUID 以及更改后的属性。 例如，要更改描述，请输入以下命令:

     ```
     print AdminTask.tklmCertList('[-usage 3592
      -attributes "{state active}" -v y]')

     print AdminTask.tklmCertUpdate
      ('[-uuid CERTIFICATE-99fc36a-4ab6a0e12343
        -usage 3592 -attributes "{information {new information}}"]')
     ```

- REST 界面:

  使用 **Certificate List REST Service** 来查找证书。 例如，您可以发送以下 HTTP 请求:

  ```
  GET https://localhost:9080/SKLM/rest/v1/certificates?attributes=
  state active
  Content-Type: application/json
  Accept: application/json
  Authorization : SKLMAuth userAuthId=37ea1939-1374-4db7-84cd-14e399be2d20
  Accept-Language : en
  ```

  使用 **Certificate Update REST Service** 来更新证书。 例如，您可以发送以下 HTTP 请求:

  ```
  PUT https://localhost:9080/SKLM/rest/v1/certificates
  Content-Type: application/json
  Accept: application/json
  Authorization: SKLMAuth authId=139aeh34567m
  {"uuid":"CERTIFICATE-99fc36a-4ab6a0e12343","usage":
  "3592","attributes":"information newinformation" }
  ```

3. 成功指示符会根据界面的不同而不同:
   - 图形用户界面:

     如果您修改了系统缺省设置或系统合作伙伴设置，那么**证书**表的“系统缺省/合作伙伴证书”列中会显示更改。
   - 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

接下来，您可以使用 3592“密钥和设备管理”页面将证书与特定设备进行关联。

删除证书

您可以删除已选中的证书，该证书可以处于任何状态（例如“活动”）。 您无法删除与设备相关联的证书，或者标记为缺省证书或合作伙伴证书的证书。 例如，您可以删除已到期的证书。

关于此任务

仅当不再需要证书所保护的数据时，才能删除这些证书。 删除证书类似于擦除数据。 删除证书后，无法对这些证书保护的数据进行检索。

您可以使用“删除”菜单项、**tklmCertDelete** 命令或 **Delete Certificate REST Service** 来删除证书。 您的角色必须具有执行删除操作和访问相应设备组的许可权。

开始之前，请确保存在要删除的证书所在的密钥库的备份。 请验证该证书当前是否未与设备相关联，并且该证书是否未标记为缺省证书或合作伙伴证书。 确定该证书的当前状态，并确保删除处于此状态的证书符合您的站点策略。

删除证书从数据库中删除数据。

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”页面上的“密钥和设备管理”部分中，选择 **3592**。
     c. 单击**转至 > 管理密钥和设备**。
     d. 或者，右键单击 **3592**，然后选择**管理密钥和设备**。
     e. 在 3592 的管理页面上，在**证书**列中选择证书。
     f. 单击**删除**。
     g. 或者，右键单击证书，然后选择**删除**。
   - 命令行界面:

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

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

     – AIX 或 Linux 等系统:

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

2. 删除证书:
   - 图形用户界面:

     删除证书之前，请在“确认”对话框上阅读确认消息以验证是否选择了正确的证书。 然后单击**确定**。
   - 命令行界面:

     输入 tklmCertList 以查找证书，然后输入 tklmCertDelete 以删除证书。 必须指定证书别名和密钥库名称。 例如，要删除当前未与设备相关联的已到期证书，请输入以下命令:

     ```
     print AdminTask.tklmCertList('[-usage 3592
      -attributes "{state active}" -v y]')

     print AdminTask.tklmCertDelete ('[-alias mycertalias
      -keyStoreName defaultKeyStore]')
     ```

   - REST 界面:

     使用 **Certificate List REST Service** 来查找证书，然后使用 **Delete Certificate REST Service** 来删除证书。 例如，您可以发送以下 HTTP 请求:

     ```
     GET https://localhost:9080/SKLM/rest/v1/certificates?attributes=
     state active
     Content-Type: application/json
     Accept: application/json
     Authorization : SKLMAuth userAuthId=37ea1939-1374-4db7-84cd-14e399be2d20
     Accept-Language : en
     ```

```
DELETE https://localhost:9080/SKLM/rest/v1/certificates/mycertalias
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth authId=139aeh34567m
Accept-Language : en
```

3. 成功指示符会根据界面的不同而不同:
   - 图形用户界面:

     已从“证书”表中除去该证书。
   - 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

接下来，您可以再次备份密钥库以准确地反映证书更改。

添加磁带机

您可以将磁带机之类的设备添加到 IBM Security Key Lifecycle Manager 数据库。

关于此任务

tklmDeviceAdd 命令

您可以使用“添加磁带机”对话框。 另外，您还可以使用 **tklmDeviceAdd** 命令或 **Device Add REST Service** 来添加设备。 您的角色必须具有执行创建操作和访问相应设备组的许可权。

开始之前，请创建要与将要识别的设备相关联的证书。 另外，请获取磁带机序列号和其他描述信息。 确定磁带机使用的是特定证书还是系统缺省证书。

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”页面上的“密钥和设备管理”部分中，选择 **3592**。
     c. 单击**转至 > 管理密钥和设备**。
     d. 或者，右键单击 **3592**，然后选择**管理密钥和设备**。
     e. 在 3592 的管理页面上，单击**添加**。
     f. 单击**磁带机**。
   - 命令行界面:

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

– Windows 系统:

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

– AIX 或 Linux 等系统:

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

2. 添加设备:
   - 图形用户界面:

     在“添加磁带机”对话框中，输入必需信息和可选信息。 然后单击**添加磁带机**。
   - 命令行界面:

     输入 tklmDeviceAdd 以添加设备。 必须指定设备组和序列号。例如，输入:

```
print AdminTask.tklmDeviceAdd ('[-type 3592 -serialNumber CDA39403AQJF
  -attributes "{worldwideName ABCdeF1234567890}
  {description marketingDivisionDrive}
   {aliasOne encryption_cert}"]')
```

   - REST 界面:

     使用 **Device Add REST Service** 来添加设备。 例如，您可以发送以下 HTTP 请求:

```
POST https://localhost:9080/SKLM/rest/v1/devices
Content-Type: application/json
Accept : application/json
Authorization : SKLMAuth userAuthId=37ea1939-1374-4db7-84cd-14e399be2d20
Accept-Language : en
{"type":"3592","serialNumber":"CDA39403AQJF","attributes":"worldwideName
ABCdeF1234567890,description salesDivisionDrive"}
```

3. 成功指示符会根据界面的不同而不同:
   - 图形用户界面:

     已将该设备添加到表。
   - 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

接下来，您可以确定所添加的磁带机的状态。

修改磁带机

您可以修改有关 IBM Security Key Lifecycle Manager 数据库中的设备（例如磁带机）的信息。例如，您可以更新磁带机所使用的合作伙伴证书的规范，或者指定同一设备系列中的备用设备组。

关于此任务

您可以使用“修改磁带机”对话框。另外，您还可以使用 **tklmDeviceUpdate** 命令或 **Device Update REST Service** 来更新设备，或者指定同一设备系列中的备用设备组。 您的角色必须具有执行修改操作和访问相应设备组的许可权。

开始之前，请创建要与将要修改的设备相关联的证书。 如果您使用命令行界面，请获取要更新的设备的 UUID 值。 另外，请还获取任何与该磁带机相关联的证书的别名。

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”页面上的“密钥和设备管理”部分中，选择 **3592**。
     c. 单击**转至 > 管理密钥和设备**。
     d. 或者，右键单击 **3592**，然后选择**管理密钥和设备**。
     e. 在 3592 的管理页面上，在**磁带机**列中选择磁带机。
     f. 单击**修改**。
     g. 或者，右键单击磁带机，然后选择**修改**，或双击磁带机条目。
   - 命令行界面:

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

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

     – AIX 或 Linux 等系统:

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

2. 修改设备:
   - 图形用户界面:

     在“修改磁带机”对话框中，输入必需信息和可选信息。 然后单击**修改磁带机**。
   - 命令行界面:

     输入 tklmDeviceList 以查找设备，然后输入 tklmDeviceUpdate 以更新设备。 必须指定设备 UUID 以及发生了更改的属性。例如，输入:

     ```
     print AdminTask.tklmDeviceList ('[-type 3592]')

     print AdminTask.tklmDeviceUpdate
      ('[-uuid DEVICE-64c588ad-5ed8-4934-8c84-64cb9e11d990
       -attributes "{aliasTwo myPartner99}"]')
     ```

   - REST 界面:

     使用 **Device List REST Service** 来查找设备，然后使用 **Device Update REST Service** 来更新设备。 例如，您可以发送以下 HTTP 请求:

     ```
     GET https://localhost:9080/SKLM/rest/v1/devices?type=3592
     Content-Type: application/json
     Accept : application/json
     Authorization : SKLMAuth userAuthId=37ea1939-1374-4db7-84cd-14e399be2d20
     Accept-Language : en
     ```

```
PUT https://localhost:9080/SKLM/rest/v1/devices
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth authId=139aeh34567m
{"uuid":"DEVICE-64c588ad-5ed8-4934-8c84-64cb9e11d990","attributes":
"aliasTwo myPartner99"}
```

3. 成功指示符会根据界面的不同而不同:
   - 图形用户界面:

     已更改表中的设备信息。
   - 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

接下来，您可以验证是否进行了更改。 对于描述之类的可选字段，您可能希望运行 **tklmDeviceList** 命令或 **Device List REST Service** 来确定是否更改了值。或者，重新打开“修改磁带机”对话框。

删除磁带机

您可以删除磁带机之类的设备。 所删除磁带机的元数据（例如磁带机序列号）将从 IBM Security Key Lifecycle Manager 数据库中除去。

关于此任务

您可以使用“删除”菜单项、**tklmDeviceDelete** 命令或 **Device Delete REST Service** 来删除设备。 您的角色必须具有执行删除操作和访问相应设备组的许可权。

开始之前，请确保站点中存在证书和设备的当前备份。 获取要删除的设备的 UUID。

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”页面上的“密钥和设备管理”部分中，选择 **3592**。
     c. 单击**转至 > 管理密钥和设备**。
     d. 或者，右键单击 **3592**，然后选择**管理密钥和设备**。
     e. 在 3592 的管理页面上，选择设备。
     f. 单击**删除**。
     g. 或者，右键单击磁带机，然后选择**删除**。
   - 命令行界面:

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

– Windows 系统:

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

– AIX 或 Linux 等系统:

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

2. 删除设备:

• 图形用户界面:

删除设备之前，请在“确认”对话框上阅读确认消息以验证是否选择了正确的设备。 所删除磁带机的元数据（例如磁带机序列号）将从 IBM Security Key Lifecycle Manager 数据库中除去。

然后单击**确定**。

• 命令行界面:

输入 tklmDeviceList 以查找设备，然后输入 tklmDeviceDelete 以删除设备。 必须指定 UUID。 例如，输入:

```
print AdminTask.tklmDeviceList ('[-type 3592]')

print AdminTask.tklmDeviceDelete
 ('[-uuid DEVICE-74386920-148c-47b2-a1e2-d19194b315cf]')
```

• REST 界面:

使用 **Device List REST Service** 来查找设备，然后使用 **Device Delete REST Service** 来删除设备。 例如，您可以发送以下 HTTP 请求:

```
GET https://localhost:9080/SKLM/rest/v1/devices?type=3592
Content-Type: application/json
Accept : application/json
Authorization : SKLMAuth userAuthId=37ea1939-1374-4db7-84cd-14e399be2d20
Accept-Language : en

DELETE https://localhost:9080/SKLM/rest/v1/devices/DEVICE-74386920-148c-
47b2-a1e2-d19194b315cf
Content-Type: application/json
Authorization: SKLMAuth authId=139aeh34567m
Accept : application/json
```

3. 成功指示符会根据界面的不同而不同:

• 图形用户界面:

已从表中除去该设备。

• 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。

DS8000 存储器映像管理

您可以使用 IBM Security Key Lifecycle Manager 来管理 DS8000 存储器映像。

某些步骤的描述提供了使用图形用户界面、命令行界面或 REST 界面而完成的备选步骤。 对于任何一个工作会话，都不要在界面之间进行切换。

一些任务的描述可能会提及 SKLMConfig.properties 文件中与任务相关的属性。使用图形用户界面、命令行界面或 REST 界面可更改这些属性。

创建存储器映像和映像证书的指导步骤

创建或添加存储器映像和映像证书时，IBM Security Key Lifecycle Manager 会提供一组指导步骤来完成该任务。

对某些步骤的描述可能会提及用于执行同一任务的命令行替代方法。 在指导任务集中，请使用图形用户界面来完成这些任务。

创建映像证书或证书请求

作为第一个活动，您可以创建用于 IBM Security Key Lifecycle Manager 的映像证书或证书请求。

关于此任务

您可以使用“创建证书”对话框。另外，您还可以使用下列任何命令或 REST 服务来创建证书或证书请求:

- **tklmCertCreate** 或 **tklmCertGenRequest**
- **Create Certificate REST Service** 或 **Certificate Generate Request REST Service**

您的角色必须具有执行创建操作和访问相应设备组的许可权。 要使此证书成为缺省证书，您的角色必须具有执行修改操作的许可权。

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”页面上的“密钥和设备管理”部分中，选择 **DS8000**。
     c. 单击**转至 > 根据指导创建密钥和设备**。
     d. 或者，右键单击 **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. 创建映像证书或请求获取证书:
   - 图形用户界面:
     a. 在“步骤 1: 创建证书”页面上，在**证书**表上单击**创建**。
     b. 在“创建证书”对话框上，选择自签名证书或针对第三方提供者的证书请求。
     c. 指定必需和可选参数的值。
     d. 单击**创建证书**。
   - 命令行界面:
     - 证书

       输入 tklmCertCreate 以创建证书和公用/专用密钥对，并将证书存储在现有密钥库中。 例如，输入:

       ```
       print AdminTask.tklmCertCreate ('[-type selfsigned
        -alias sklmCertificate -cn sklm -ou sales -o myCompanyName
          -usage DS8000 -country US -keyStoreName defaultKeyStore
           -validity 999]')
       ```

     - 证书请求

       输入 tklmCertGenRequest 以创建 PKCS #10 证书请求文件。 例如，输入:

       ```
       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:
     - 证书
       a. 获取用于访问 IBM Security Key Lifecycle Manager REST 服务的唯一用户认证标识。 有关认证过程的更多信息，请参阅 REST 服务的验证流程。
       b. 要调用 **Create Certificate REST Service**，请发送 HTTP POST 请求。请将您在步骤 a 中获取的用户认证标识随请求消息一起传递，如以下示例所示。

       ```
       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":"DS8000","country":"US",
       "validity":"999", "
       algorithm ": " RSA " }
       ```

     - 证书请求

       使用 **Certificate Generate Request REST Service** 来创建 PKCS #10 证书请求文件。 例如，可以使用 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
       ```

```
{"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。请在将新证书提供给设备之前备份这些证书。
   - 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

接下来，您可以转至下一步以定义特定存储器映像，并指定存储器映像证书。 请选择**步骤 2: 识别映像**或单击**转至下一步**。

识别存储器映像

您可以识别要用于 IBM Security Key Lifecycle Manager 的存储器映像（设备）。

关于此任务

您可以使用“添加存储器映像”对话框。另外，您还可以使用 **tklmDeviceAdd** 命令或 **Device Add REST Service** 来添加存储器映像。

开始之前，请创建要与将要识别的存储器映像相关联的映像证书。

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。 在导航树中，单击 **IBM Security Key Lifecycle Manager > 欢迎**。在该页面中下滚到密钥和设备管理部分。 在**根据指导创建密钥和设备**中，选择 **DS8000**。然后单击 **开始**。

     a. 登录图形用户界面。

     b. 在“欢迎”页面上的“密钥和设备管理”部分中，选择 **DS8000**。

     c. 单击**转至 > 根据指导创建密钥和设备**。

     d. 或者，右键单击 **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. 跳过**步骤 1: 创建证书**。单击**转至下一步**链接，或者单击**步骤 2: 识别磁带机**。
3. 您可以指定将所有入局设备添加到暂挂列表，但不会在其提出请求时自动对其提供密钥。您必须接受或拒绝暂挂设备列表中的设备之后，IBM Security Key Lifecycle Manager 才会在该设备提出请求时对其提供密钥。 您的角色必须具有执行修改操作和访问相应设备组的许可权。
   - 图形用户界面:

     选择**保留正在等待我审核的新设备请求**。
   - 命令行界面:

     使用 **tklmDeviceGroupAttributeUpdate** 命令或 **Device Group Attribute Update REST Service** 来设置 **device.AutoPendingAutoDiscovery** 属性的值。例如，输入:

     ```
     print AdminTask.tklmDeviceGroupAttributeUpdate ('[-name DS8000
       -attributes "{device.AutoPendingAutoDiscovery 2}"]')
     ```
   - REST 界面:
     a. 获取用于访问 IBM Security Key Lifecycle Manager REST 服务的唯一用户认证标识。 有关认证过程的更多信息，请参阅 REST 服务的验证流程。
     b. 要调用 **Device Group Attribute Update REST Service** 以及设置 **device.AutoPendingAutoDiscovery** 属性的值，请发送 HTTP PUT 请求。请将您在步骤 a 中获取的用户认证标识随请求消息一起传递，如以下示例所示。

     ```
     PUT https://localhost:9080/SKLM/rest/v1/deviceGroupAttributes
     Content-Type: application/json
     Accept : application/json
     Authorization: SKLMAuth authId=139aeh34567m
     {"name":"DS8000","attributes":"device.AutoPendingAutoDiscovery 2"}
     ```
4. 添加存储器映像:
   - 图形用户界面:
     a. 在“步骤 2: 识别映像”页面上，在表中单击**添加**。
     b. 在“添加存储器映像”对话框中，输入必需信息和可选信息。
     c. 单击**添加存储器映像**。
   - 命令行界面:

     输入 tklmDeviceAdd 以添加存储器映像。 必须指定存储器映像类型、序列号和映像证书。 例如，输入:

     ```
     print AdminTask.tklmDeviceAdd ('[-type DS8000 -serialNumber CCCB31403AFF
       -attributes "{worldwideName ABCdeF1234567890}
       {description salesDivisionDrive}
       {aliasOne myimagecertificate}"]')
     ```
   - REST 界面:

     您可以使用 **Device Add REST Service** 来添加存储器映像。 例如，可以使用 REST 客户机发出以下 HTTP 请求:

```
POST https://localhost:9080/SKLM/rest/v1/devices
Content-Type: application/json
Accept : application/json
Authorization : SKLMAuth userAuthId=37ea1939-1374-4db7-84cd-14e399be2d20
Accept-Language : en
{"type":"DS8000","serialNumber":"CCCB31403AFF","attributes":"worldwideName
ABCdeF1234567890,description marketingDivisionDrive"}
```

5. 成功指示符会根据界面的不同而不同:
   - 图形用户界面:

     已将该存储器映像添加到表。
   - 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

接下来，您可以导入签名证书。另外，还可以使用“密钥和设备管理”页面来查看所有存储器映像和映像证书。

管理存储器映像和映像证书

要管理存储器映像和映像证书，您可能希望确定其状态。 您可以映射其关联，或者添加、修改或删除特定证书或存储器映像。

关于此任务

使用 DS8000“密钥和设备管理”页面来将映像证书映射到存储器映像，以及确定表中各项的状态。 您可以添加、修改或删除映像证书或存储器映像。 您的角色必须具有执行查看操作和访问相应设备组的许可权。

开始之前，先检查该页面上的列（页面上提供了用于添加、修改或删除表项的各个按钮）。 要对信息进行排序，请单击列标题。

表组织成下列区域:

- 在左侧列中，有关证书的信息指示证书名称、到期日期和证书的状态。
- 在右侧列中，有关存储器映像的信息指示存储器映像名称以及相关联的映像证书。
- “状态”图标指示证书的状态。

表 4. “状态”图标及其含义

图标	描述
	证书处于有效状态。
	证书处于已泄密状态。
	证书即将到期。

表 4. “状态”图标及其含义 (续)

图标	描述
	证书处于到期状态。
	对于具有将来使用时间戳记的已迁移证书，证书从将来日期开始生效。
	IBM Security Key Lifecycle Manager 具有正在等待签名和导入的第三方证书请求。

过程

1. 登录图形用户界面。
   a. 在“欢迎”页面上的“密钥和设备管理”部分中，选择 **DS8000**。
   b. 单击**转至 > 管理密钥和设备**。
   c. 或者，右键单击 **DS8000**，然后选择**管理密钥和设备**。

   某些步骤的描述提供了使用图形用户界面、命令行界面或 REST 界面而完成的备选步骤。 对于任何一个工作会话，都不要在界面之间进行切换。

   一些任务的描述可能会提及 `SKLMConfig.properties` 文件中与任务相关的属性。使用图形用户界面、命令行界面或 REST 界面可更改这些属性。
2. 在 DS8000“密钥和设备管理”页面上，您可以添加、修改或删除存储器映像或映像证书。

   您可以执行下列管理任务:
   - 添加

     单击**添加**。 另外，您还可以选择用于创建证书和存储器映像的逐步过程。
     – 证书

       在“创建证书”页面上，选择自签名或来自第三方提供者的请求作为证书类型，并填写必需信息。然后单击**创建证书**。 您的角色必须具有执行创建操作和访问相应设备组的许可权。 要使此证书成为缺省证书，您的角色必须具有执行修改操作的许可权。
     – 存储器映像

       在“添加存储器映像”页面上，输入存储器映像信息。 然后单击**添加存储器映像**。 您的角色必须具有执行创建操作和访问相应设备组的许可权。
     – 使用逐步过程来创建证书和存储器映像

       在“步骤 1: 创建证书”和“步骤 2: 识别映像”页面上，输入必需信息。

     成功指示符各不相同，显示证书或存储器映像列中的更改。
   - 修改

     要更改有关存储器映像的信息或者查看有关证书的信息，请选择证书或存储器映像，然后单击**修改**。 或者，右键单击所选证书或存储器映像。 然后单击**修改**，或者双击证书或存储器映像条目。

– 证书

查看“修改证书”页面中的只读信息。 您的角色必须具有执行修改操作和访问相应设备组的许可权。

– 存储器映像

在“修改存储器映像”页面中指定更改。然后单击**修改存储器映像**。 您的角色必须具有执行修改操作和访问相应设备组的许可权。

成功指示符各不相同，显示证书或存储器映像列中的更改。 表中可能不会提供对某些信息（例如可选字段）的更改。

• 删除

要删除证书或存储器映像，请验证是否选择了正确的证书或存储器映像。 然后单击**删除**。 或者，右键单击所选证书或存储器映像。 然后单击**删除**。

– 证书

删除证书之前，请确保您具有密钥库的当前备份。 任何使用此证书编写的存储器映像将在删除此证书后变得不可读。 要删除的证书可以处于任何状态（例如“活动”）。 您无法删除满足下列条件的证书，而与其状态无关:

- 与存储器映像相关联。
- 被 DS8000 Turbo 磁带机标记为映像的主要证书或映像的辅助证书。

删除证书从数据库中删除数据。

要确认删除，请单击**确定**。 您的角色必须具有执行删除操作和访问相应设备组的许可权。

– 存储器映像

所删除存储器映像的元数据（例如序列号）将从 IBM Security Key Lifecycle Manager 数据库中除去。要确认删除，请单击**确定**。 您的角色必须具有执行删除操作和访问相应设备组的许可权。

成功指示符是已从管理表中删除证书或存储器映像。

添加映像证书或证书请求

您可以添加更多映像证书或证书请求以用于 IBM Security Key Lifecycle Manager。

关于此任务

您可以使用“创建证书”对话框。另外，您还可以使用下列任何命令或 REST 服务来创建证书或证书请求:

• **tklmCertCreate** 或 **tklmCertGenRequest**
• **Create Certificate REST Service** 或 **Certificate Generate Request REST Service**

您的角色必须具有执行创建操作和访问相应设备组的许可权。 要使此证书成为缺省证书，您的角色必须具有执行修改操作的许可权。

开始之前，请确定有关使用证书的站点策略。

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”页面上的“密钥和设备管理”部分中，选择 **DS8000**。
     c. 单击**转至 > 管理密钥和设备**。
     d. 或者，右键单击 **DS8000**，然后选择**管理密钥和设备**。
     e. 在 DS8000 的管理页面上，单击**添加**。
     f. 单击**证书**。
   - 命令行界面:

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

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

     – AIX 或 Linux 等系统:

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

2. 创建证书或请求获取证书:
   - 图形用户界面:
     a. 在“创建证书”页面上，选择自签名证书或针对第三方提供者的证书请求。
     b. 指定必需和可选参数的值。 然后单击**创建证书**。
   - 命令行界面:
     – 证书:

       输入 tklmCertCreate 以创建证书和公用/专用密钥对，并将证书存储在现有密钥库中。 例如，输入:

       ```
       print AdminTask.tklmCertCreate ('[-type selfsigned
        -alias sklmCertificate -cn sklm -ou sales -o myCompanyName
          -usage DS8000 -country US -keyStoreName defaultKeyStore
           -validity 999]')
       ```

     – 证书请求:

       输入 tklmCertGenRequest 以创建 PKCS #10 证书请求文件。 例如，输入:

       ```
       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:
     – 证书

       使用 **Create Certificate REST Service** 来创建证书和公用/专用密钥对，并将证书存储在现有密钥库中。 例如，可以使用 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":"DS8000",
"country":"US","validity":
"999", "algorithm ": " RSA " }
```

– 证书请求

使用 **Certificate Generate Request REST Service** 来创建 PKCS #10 证书请求文件。 例如，可以使用 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
{"type":"certreq","alias":"sklmCertificate3",
"cn":"sklm","ou":
"sales","o":"myCompanyName","usage":"DS8000",
"country":"US","validity":
"999","fileName":"myCertRequest3.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:

     证书或证书请求作为**证书**列表中的项列出。请在将新证书提供给设备之前备份这些证书。
   - 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

您的下一步操作取决于您已创建证书还是证书请求。

- 证书:

  您可以将证书与特定存储器映像进行关联。
- 证书请求:

  手动将证书请求发送到认证中心。 返回签名证书后，请使用“欢迎”面板上的暂挂操作项，或者使用 **tklmCertImport** 命令或 **Certificate Import REST Service** 导入该证书。

修改映像证书

您可以使用图形用户界面来查看有关 IBM Security Key Lifecycle Manager 数据库中的映像证书的只读信息。通过使用命令行界面或 REST 界面，您可以更改数目受限的属性。

关于此任务

您可以使用“修改证书”对话框来修改证书。 另外，您还可以使用下列命令或 REST 服务:

- **tklmCertUpdate** 或 **Certificate Update REST Service**，用于修改证书的状态（例如“受信任”或“已泄密”）以及修改证书信息。
- **tklmDeviceTypeAttributeUpdate** 或 **Device Type Attribute Update REST Service**，用于将证书设置为主要证书或辅助证书。

您的角色必须具有执行修改操作和访问相应设备组的许可权。

注: DS8000 Turbo 磁带机与 IBM Security Key Lifecycle Manager 联系时，您进行的 IBM Security Key Lifecycle Manager 数据库更改将在该磁带机上进行配置。

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”页面上的“密钥和设备管理”部分中，选择 **DS8000**。
     c. 单击**转至 > 管理密钥和设备**。
     d. 或者，右键单击 **DS8000**，然后选择**管理密钥和设备**。
     e. 在 DS8000 的管理页面上，在**证书**列中选择证书。
     f. 单击**修改**。
     g. 或者，右键单击证书，然后选择**修改**，或双击证书条目。
   - 命令行界面:

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

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

     – AIX 或 Linux 等系统:

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

2. 查看（图形用户界面）或修改（命令行界面）证书信息:
   - 图形用户界面:

     在“修改证书”对话框上，查看只读字段。
   - 命令行界面:

     输入 tklmCertList 以查找证书，然后输入 tklmCertUpdate 以更新证书。 必须指定证书的 UUID 以及更改后的属性。 例如，要更改信息，请输入以下命令:

     ```
     print AdminTask.tklmCertList('[-usage DS8000
       -attributes "{state active}" -v y]')

     print AdminTask.tklmCertUpdate
      ('[-uuid CERTIFICATE-33fc26e-5fb5a0e66143
        -usage DS8000 -attributes "{information {new information}}"]')
     ```

- REST 界面:

  使用 **Certificate List REST Service** 来查找证书。 例如，您可以发送以下 HTTP 请求:

  ```
  GET https://localhost:9080/SKLM/rest/v1/certificates?attributes=
  state active
  Content-Type: application/json
  Accept: application/json
  Authorization: SKLMAuth userAuthId=37ea1939-1374-4db7-84cd-14e399be2d20
  Accept-Language: en
  ```

  使用 **Certificate Update REST Service** 来更新证书。 例如，您可以发送以下 HTTP 请求:

  ```
  PUT https://localhost:9080/SKLM/rest/v1/certificates
  Content-Type: application/json
  Accept: application/json
  Authorization: SKLMAuth authId=139aeh34567m
  {"uuid":"CERTIFICATE-33fc26e-5fb5a0e66143","usage":
  "DS8000","attributes":"information {newinformation}" }
  ```

3. 成功指示符会根据界面的不同而不同:
   - 图形用户界面:

     显示一列，用于显示只读数据。
   - 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

接下来，您可以使用 DS8000“密钥和设备管理”页面将映像证书与特定存储器映像进行关联。

删除映像证书

您可以删除已选中的映像证书，该证书可以处于任何状态（例如“活动”）。 您无法删除与存储器映像相关联的证书。 另外，还不能删除识别为映像的主要证书或映像的辅助证书的证书。 例如，您可以删除已到期的证书。

关于此任务

仅当不再需要证书所保护的数据时，才能删除这些证书。 删除证书类似于擦除数据。 删除证书后，无法对这些证书保护的数据进行检索。

您可以使用“删除”菜单项，也可以使用 **tklmCertDelete** 命令或 **Delete Certificate REST Service** 来删除所选映像证书。 您的角色必须具有执行删除操作和访问相应设备组的许可权。

开始之前，请确保存在要删除的映像证书所在的密钥库的备份。 请验证该证书当前是否与存储器映像相关联。 确定该证书的当前状态，并确保删除处于此状态的证书符合您的站点策略。

删除证书从数据库中删除数据。

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”页面上的“密钥和设备管理”部分中，选择 **DS8000**。
     c. 单击**转至 > 管理密钥和设备**。
     d. 或者，右键单击 **DS8000**，然后选择**管理密钥和设备**。
     e. 在 DS8000 的管理页面上，在**证书**列中选择证书。
     f. 单击**删除**。
     g. 或者，右键单击证书，然后选择**删除**。
   - 命令行界面:

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

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

     – AIX 或 Linux 等系统:

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

2. 删除证书:
   - 图形用户界面:

     删除证书之前，请在“确认”对话框上阅读确认消息以验证是否选择了正确的证书。 然后单击**确定**。
   - 命令行界面:

     输入 tklmCertList 以查找证书，然后输入 tklmCertDelete 以删除证书。 必须指定证书别名和密钥库名称。 例如，要删除当前未与存储器映像相关联的已到期证书，请输入以下命令:

     ```
     print AdminTask.tklmCertList('[-usage DS8000 -v y]')

     print AdminTask.tklmCertDelete ('[-alias mycertalias
      -keyStoreName defaultKeyStore]')
     ```

   - REST 界面:

     使用 **Certificate List REST Service** 来查找证书，然后使用 **Delete Certificate REST Service** 来删除证书。 例如，您可以发送以下 HTTP 请求:

     ```
     GET https://localhost:9080/SKLM/rest/v1/certificates?usage=DS8000
     Content-Type: application/json
     Accept: application/json
     Authorization : SKLMAuth userAuthId=37ea1939-1374-4db7-84cd-14e399be2d20
     Accept-Language : en
     ```

```
DELETE https://localhost:9080/SKLM/rest/v1/certificates/mycertalias
Content-Type: application/json
Accept: application/json
Authorization: SKLMAuth authId=139aeh34567m
Accept-Language: en
```

3. 成功指示符会根据界面的不同而不同:
   - 图形用户界面:

     已从“证书”表中除去该证书。
   - 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

接下来，您可以再次备份密钥库以准确地反映证书更改。

添加存储器映像

您可以将存储器映像添加到 IBM Security Key Lifecycle Manager 数据库。

关于此任务

您可以使用“添加存储器映像”对话框，也可以使用 **tklmDeviceAdd** 命令或 **Device Add REST Service** 来添加存储器映像。 您的角色必须具有执行创建操作和访问相应设备组的许可权。

开始之前，请创建要与将要识别的存储器映像相关联的证书。 另外，请获取存储器映像序列号和其他描述信息。

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”页面上的“密钥和设备管理”部分中，选择 **DS8000**。
     c. 单击**转至 > 管理密钥和设备**。
     d. 或者，右键单击 **DS8000**，然后选择**管理密钥和设备**。
     e. 在 DS8000 的管理页面上，单击**添加**。
     f. 单击**存储器映像**。
   - 命令行界面:

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

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

– AIX 或 Linux 等系统:

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

2. 添加存储器映像:
   - 图形用户界面:

     在“添加存储器映像”对话框中，输入必需信息和可选信息。然后单击**添加存储器映像**。
   - 命令行界面:

     输入 tklmDeviceAdd 以添加存储器映像。 必须指定存储器映像类型、序列号和映像证书。 例如，输入:

     ```
     print AdminTask.tklmDeviceAdd ('[-type DS8000 -serialNumber CCCB31403AFF
       -attributes "{worldwideName ABCdeF1234567890}
       {description salesDivisionDrive}
       {aliasOne myimagecertificate}"]')
     ```
   - REST 界面:

     使用 **Device Add REST Service** 来添加存储器映像。 例如，您可以发送以下 HTTP 请求:

     ```
     POST https://localhost:9080/SKLM/rest/v1/devices
     Content-Type: application/json
     Accept : application/json
     Authorization : SKLMAuth userAuthId=37ea1939-1374-4db7-84cd-14e399be2d20
     Accept-Language : en
     {"type":"DS8000","serialNumber":"CCCB31403AFF","attributes":"worldwideName
     ABCdeF1234567890,description salesDivisionDrive"}
     ```
3. 成功指示符会根据界面的不同而不同:
   - 图形用户界面:

     已将该存储器映像添加到表。
   - 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

接下来，您可以确定所添加的存储器映像的状态。

修改存储器映像

您可以修改有关 IBM Security Key Lifecycle Manager 数据库中的存储器映像的信息。例如，您可以更新存储器映像描述。

关于此任务

您可以使用“修改存储器映像”对话框，也可以使用 **tklmDeviceUpdate** 命令或 **Device Update REST Service** 来更新存储器映像。 您的角色必须具有执行修改操作和访问相应设备组的许可权。

开始之前，请创建要与将要修改的存储器映像相关联的证书。 如果您使用命令行界面，请获取要更新的存储器映像的 UUID 值，以及任何与该存储器映像相关联的证书的别名。

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”页面上的“密钥和设备管理”部分中，选择 **DS8000**。
     c. 单击**转至 > 管理密钥和设备**。
     d. 或者，右键单击 **DS8000**，然后选择**管理密钥和设备**。
     e. 在 DS8000 的管理页面上，选择磁带机。
     f. 单击**修改**。
     g. 或者，右键单击磁带机，然后选择**修改**，或双击磁带机条目。
   - 命令行界面:

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

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

     – AIX 或 Linux 等系统:

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

2. 修改存储器映像:
   - 图形用户界面:

     在“修改存储器映像”对话框中，输入更改后的信息。 然后单击**修改存储器映像**。
   - 命令行界面:

     输入 tklmDeviceUpdate 以更新存储器映像。 必须指定存储器映像 UUID 以及发生了更改的属性。 例如，输入:

     ```
     print AdminTask.tklmDeviceUpdate
      ('[-uuid DEVICE-15d499ad-3ad8-3333-8c84-64cb9e11d990
       -attributes "{description myDevice}"]')
     ```

   - REST 界面:

     使用 **Device Update REST Service** 来更新存储器映像。 例如，您可以发送以下 HTTP 请求:

     ```
     PUT https://localhost:9080/SKLM/rest/v1/devices
     Content-Type: application/json
     Accept : application/json
     Authorization: SKLMAuth authId=139aeh34567m
     {"uuid":"DEVICE-15d499ad-3ad8-3333-8c84-64cb9e11d990","attributes":
     "description myDevice"}
     ```

3. 成功指示符会根据界面的不同而不同:
   - 图形用户界面:

已更改表中的存储器映像信息。

- 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。

删除存储器映像

您可以删除存储器映像。 所删除存储器映像的元数据（例如序列号）将从 IBM Security Key Lifecycle Manager 数据库中除去。

关于此任务

您可以使用“删除”菜单项，也可以使用 **tklmDeviceDelete** 命令或 **Device Delete REST Service** 来删除存储器映像。 您的角色必须具有执行删除操作和访问相应设备组的许可权。

开始之前，请确保站点中存在证书和存储器映像的当前备份。 如果您使用命令行界面，请获取要删除的存储器映像的 UUID。

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”页面上的“密钥和设备管理”部分中，选择 **DS8000**。
     c. 单击**转至 > 管理密钥和设备**。
     d. 或者，右键单击 **DS8000**，然后选择**管理密钥和设备**。
     e. 在 DS8000 的管理页面上，选择设备。
     f. 单击**删除**。
     g. 或者，右键单击磁带机，然后选择**删除**。
   - 命令行界面:

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

     – Windows 系统:

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

     – AIX 或 Linux 等系统:

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

2. 删除存储器映像:
   - 图形用户界面:

     删除存储器映像之前，请在“确认”页面上阅读确认消息以验证是否选择了正确的存储器映像。 所删除存储器映像的元数据（例如序列号）将从 IBM Security Key Lifecycle Manager 数据库中除去。

然后单击**确定**。

- 命令行界面:

  输入 tklmDeviceList 以查找设备，然后输入 tklmDeviceDelete 以删除存储器映像。 必须指定 UUID。 例如，输入:

  ```
  print AdminTask.tklmDeviceList ('[-type DS8000]')

  print AdminTask.tklmDeviceDelete
   ('[-uuid DEVICE-74386920-148c-47b2-a1e2-d19194b315cf]')
  ```

- REST 界面:

  使用 **Device List REST Service** 来查找设备，然后使用 **Device Delete REST Service** 来删除存储器映像。 例如，您可以发送以下 HTTP 请求:

  ```
  GET https://localhost:9080/SKLM/rest/v1/devices?type=DS8000
  Content-Type: application/json
  Accept : application/json
  Authorization : SKLMAuth userAuthId=37ea1939-1374-4db7-84cd-14e399be2d20
  Accept-Language : en

  DELETE https://localhost:9080/SKLM/rest/v1/devices/DEVICE-74386920-148c-
  47b2-a1e2-d19194b315cf
  Content-Type: application/json
  Accept : application/json
  Authorization: SKLMAuth authId=139aeh34567m
  ```

3. 成功指示符会根据界面的不同而不同:

   - 图形用户界面:

     已从表中除去该存储器映像。

   - 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。

DS5000 管理

您可以使用 IBM Security Key Lifecycle Manager 来管理 DS5000 存储服务器。

管理设备、密钥和设备关联

要管理 DS5000 存储服务器，您需要将设备映射到密钥或机器。

关于此任务

您的角色必须具有执行查看操作和访问相应设备组的许可权。使用 DS5000“密钥和设备管理”页面来添加、修改或删除设备、密钥或关联。 这些操作需要更多许可权。

开始之前，先检查该页面上的列（页面上提供了用于添加、修改或删除表项的各个按钮）。 要对信息进行排序，请单击列标题。

表组织成下列信息区域:

- 设备以及任何相关联的机器。
- 设备当前所使用的密钥以及对设备的描述。

过程

1. 登录图形用户界面。
   a. 在“欢迎”页面上的“密钥和设备管理”部分中，选择 **DS5000**。
   b. 单击**转至 > 管理密钥和设备**。
   c. 或者，右键单击 **DS5000**，然后选择**管理密钥和设备**。

   某些步骤的描述提供了使用图形用户界面、命令行界面或 REST 界面而完成的备选步骤。 对于任何一个工作会话，都不要在界面之间进行切换。

   一些任务的描述可能会提及 SKLMConfig.properties 文件中与任务相关的属性。使用图形用户界面、命令行界面或 REST 界面可更改这些属性。
2. 您可以添加、修改或删除密钥、设备或机器关联。

   您可以执行下列管理任务:
   - 刷新列表。

     单击“刷新”图标  可刷新表中的项。
   - 添加

     单击**添加**。
     – 设备

       在“添加设备”对话框中，输入设备序列号和其他信息。 然后单击**添加设备**。 您的角色必须具有执行创建操作和访问相应设备组的许可权。
     – 密钥

       选择设备，然后选择**添加 > 更多密钥**。 在“添加密钥”对话框中，指定必需信息，例如要创建的密钥数（最多可创建 12 个密钥）。 然后单击**添加 > 更多密钥**。 您的角色必须具有执行创建操作和访问相应设备组的许可权。
     – 关联

       如果通过 **device.enableMachineAffinity** 特性启用了机器亲缘关系，请使用“添加关联”对话框来指定机器标识之类的必需信息。 然后单击**添加关联**。 您的角色必须具有执行创建操作和访问相应设备组的许可权。

     成功指示符各不相同，显示添加设备、密钥或关联。
   - 修改

     要更改设备或密钥，请选择设备，然后单击**修改**。 或者，右键单击所选设备。 然后，单击其中一个选项，例如**修改设备**。
     – 设备

       在“修改设备”对话框上指定更改。 然后单击**修改设备**。 您的角色必须具有执行修改操作和访问相应设备组的许可权。
     – 密钥

       在“修改密钥”对话框上选择密钥。 然后单击**删除**。 您的角色必须具有执行删除操作和访问相应设备组的许可权。

成功指示符各不相同，显示设备或密钥列中的更改。

- 删除

  要删除设备，请选择设备，然后单击**删除**。 或者，右键单击所选设备。 然后单击**删除**。 删除设备之前，请使用 **tklmMachineDeviceDelete** 命令除去该设备与 IBM Security Key Lifecycle Manager 数据库中的现有机器标识的关联。

  所删除设备的元数据（例如设备序列号）将从 IBM Security Key Lifecycle Manager 数据库中除去。密钥数据也将被除去。 要确认删除，请单击**确定**。 您的角色必须具有执行删除操作和访问相应设备组的许可权。

  成功指示符是已从表中删除设备。

添加设备

您可以将设备添加到 IBM Security Key Lifecycle Manager 数据库。

关于此任务

如果启用了机器亲缘关系，那么添加设备还要求您添加设备与机器之间的关系。 否则，不会向添加的设备提供密钥。 通过使用机器亲缘关系，您可以针对特定设备和机器组合设置密钥提供。

您可以使用“添加设备”对话框、**tklmDeviceAdd** 命令或 **Device Add REST Service** 来添加设备。 您的角色必须具有执行创建操作和访问相应设备组的许可权。

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”页面上的“密钥和设备管理”部分中，选择 **DS5000**。
     c. 单击**转至 > 管理密钥和设备**。
     d. 或者，右键单击 **DS5000**，然后选择**管理密钥和设备**。
     e. 在 DS5000 的管理页面上，单击**添加**。
     f. 单击**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. 添加设备:

- 图形用户界面:

  在“添加设备”对话框中，输入必需信息和可选信息。 然后单击**添加设备**。

- 命令行界面:

  输入 tklmDeviceAdd 以添加设备。 必须指定设备序列号和设备组。 例如，输入:

  ```
  print AdminTask.tklmDeviceAdd ('[-type DS5000 -serialNumber CDA39403AQJF
    -attributes "{worldwideName ABCdeF1234567890}
    {description marketingDivisionDrive}
    {keyPrefix AEF}
    {numberOfKeys 10}
    {deviceText abcdefghijklmnopqrst}
    {machineID 3042383030303437000000000000}"]')
  ```

- REST 界面:

  a. 获取用于访问 IBM Security Key Lifecycle Manager REST 服务的唯一用户认证标识。 有关认证过程的更多信息，请参阅 REST 服务的验证流程。

  b. 要调用 **Device Add REST Service**，请发送 HTTP POST 请求。请将您在步骤 a 中获取的用户认证标识随请求消息一起传递，如以下示例所示。

  ```
  POST https://localhost:9080/SKLM/rest/v1/devices
  Content-Type: application/json
  Accept : application/json
  Authorization : SKLMAuth userAuthId=37ea1939-1374-4db7-84cd-14e399be2d20
  Accept-Language : en
  {"type":"DS5000","serialNumber":"CDA39403AQJF","attributes":"worldwideName
  ABCdeF1234567890,description marketingDivisionDrive"}
  ```

3. 成功指示符会根据界面的不同而不同:

   - 图形用户界面:

     已将该设备添加到表。

   - 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

接下来，您可以将设备与机器进行关联。

修改设备

您可以修改有关 IBM Security Key Lifecycle Manager 数据库中的设备的信息。例如，您可以更新对磁带机的描述。

关于此任务

您可以使用“修改设备”对话框。另外，您还可以使用 **tklmDeviceUpdate** 命令或 **Device Update REST Service** 来更新设备。 您的角色必须具有执行修改操作和访问相应设备组的许可权。

如果您使用命令行或 REST 界面，请在开始之前获取要更新的设备的 UUID 值。

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”页面上的“密钥和设备管理”部分中，选择 **DS5000**。
     c. 单击**转至 > 管理密钥和设备**。
     d. 或者，右键单击 **DS5000**，然后选择**管理密钥和设备**。
     e. 在 DS5000 的管理页面上，在**设备序列号**列中选择设备。
     f. 单击**修改设备**。
     g. 或者，右键单击磁带机，然后选择**修改设备**，或双击设备条目。
   - 命令行界面:

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

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

     – AIX 或 Linux 等系统:

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

2. 修改设备:
   - 图形用户界面:

     在“修改设备”对话框上，输入更改后的信息。 然后单击**修改设备**。
   - 命令行界面:

     输入 tklmDeviceUpdate 以更新设备。 必须指定设备 UUID 以及发生了更改的属性。 例如，输入:

     ```
     print AdminTask.tklmDeviceUpdate
      ('[-uuid DEVICE-15d499ad-3ad8-3333-8c84-64cb9e11d990
       -attributes "{description myDevice}"]')
     ```

   - REST 界面:

     使用 **Device Update REST Service** 来更新设备。 例如，发送以下 HTTP 请求:

     ```
     PUT https://localhost:9080/SKLM/rest/v1/devices
     Content-Type: application/json
     Accept : application/json
     Authorization: SKLMAuth authId=139aeh34567m
     {"uuid":"DEVICE-64c588ad-5ed8-4934-8c84-64cb9e11d990","attributes":
     "description myDevice"}
     ```

3. 成功指示符会根据界面的不同而不同:
   - 图形用户界面:

     已更改表中的设备信息。
   - 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

接下来，您可以验证是否进行了更改。

删除设备

您可以删除设备，例如 DS5000 存储服务器。 删除设备会从 IBM Security Key Lifecycle Manager 数据库中除去设备序列号及其密钥数据。

关于此任务

如果设备属于 DS5000 设备系列，并且启用了机器亲缘关系，那么删除设备还会删除设备与机器之间的所有关系。

您可以使用“删除”菜单项、**tklmDeviceDelete** 命令或 **Device Delete REST Service** 来删除设备。 您的角色必须具有执行删除操作和访问相应设备组的许可权。

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”页面上的“密钥和设备管理”部分中，选择 **DS5000**。
     c. 单击**转至 > 管理密钥和设备**。
     d. 或者，右键单击 **DS5000**，然后选择**管理密钥和设备**。
     e. 在 DS5000 的管理页面上，选择设备。
     f. 单击**删除**。
     g. 或者，右键单击磁带机，然后选择**删除**。
   - 命令行界面:

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

     – Windows 系统:

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

     – AIX 或 Linux 等系统:

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

2. 使用命令行界面运行 **tklmMachineDeviceList** 命令，或者使用 **Machine Device List REST Service** 来获取要删除的设备的 UUID。 使用 **tklmMachineDeviceDelete** 命令或 **Machine Device Delete REST Service** 来删除该设备与机器之间的所有关联。

   例如，输入:

   ```
   print AdminTask.tklmMachineDeviceList
   ('[-machineID 3042383030303437000000000000]')
   ```

```
print AdminTask.tklmMachineDeviceDelete
('[-deviceUUID DEVICE-663b6d37-e6d5-4c9f-af90-e40e48d27f3c
 -machineID 30423830303034370000000000000]')
```

您可以发送以下 HTTP 请求:

```
GET https://localhost:9080/SKLM/rest/v1/machines/device?machineID=
30423830303034370000000000000
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth authId=139aeh34567m
```

```
DELETE https://localhost:9080/SKLM/rest/v1/machines/device
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth authId=139aeh34567m
{"deviceUUID":"DEVICE-663b6d37-e6d5-4c9f-af90-e40e48d27f3c","machineID":
"30423830303034370000000000000"}
```

3. 删除设备:
   - 图形用户界面:

     在“确认”对话框上，阅读确认消息，然后删除设备。 删除设备会从 IBM Security Key Lifecycle Manager 数据库中除去设备序列号及其密钥数据。

     然后单击**确定**。
   - 命令行界面:

     输入 tklmDeviceDelete 以删除设备。 必须指定 UUID。 例如，输入:

     ```
     print AdminTask.tklmDeviceDelete
      ('[-uuid DEVICE-74386920-148c-47b2-a1e2-d19194b315cf]')
     ```
   - REST 界面:

     使用 **Device Delete REST Service** 来删除设备。 例如，您可以发送以下 HTTP 请求:

     ```
     DELETE https://localhost:9080/SKLM/rest/v1/devices/DEVICE-74386920-148c-
     47b2-a1e2-d19194b315cf
     Content-Type: application/json
     Accept : application/json
     Authorization: SKLMAuth authId=139aeh34567m
     ```
4. 成功指示符会根据界面的不同而不同:
   - 图形用户界面:

     已从表中除去该设备。
   - 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。

添加密钥

您可以添加更多密钥以用于 DS5000 存储服务器。

关于此任务

您可以使用“添加密钥”对话框、**tklmSecretKeyCreate** 命令或 **Secret Key Create REST Service** 在现有组中创建一个或多个对称密钥。 您的角色必须具有执行创建操作和访问相应设备组的许可权。

开始之前，请确定用于命名密钥前缀的站点策略。

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”页面上的“密钥和设备管理”部分中，选择 **DS5000**。
     c. 单击**转至 > 管理密钥和设备**。
     d. 或者，右键单击 **DS5000**，然后选择**管理密钥和设备**。
     e. 在 DS5000 的管理页面上，单击**添加**。
     f. 单击**更多密钥**。
   - 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. 创建密钥:
   - 图形用户界面

     在“添加密钥”对话框上，为必需参数指定值。 然后单击**添加更多密钥**。
   - 命令行界面:
     a. 使用 **tklmGroupList** 命令来获取密钥组的 UUID 值。 例如，输入:

        ```
        print AdminTask.tklmGroupList ('[-type keygroup -v y]')
        ```

        输出可能类似于以下示例:

        ```
        group name = DS5K-ds5kdevice
        group type = KEY
        group uuid = KEYGROUP-9c97d9aa-b5f0-41a1-b65f-119756168211
        initialization date = 6/4/10 12:00:00 AM GMT-12:00
        activation date = 6/4/10 12:00:00 AM GMT-12:00
        key[0]:
          uuid: KEY-66b0a3a2-3c52-4088-8772-0a1ddebf5803
          aliases: dsk000000000000000000
          keystore names: defaultKeyStore
        key[1]:
        ```

```
  uuid: KEY-3f1230fd-59ef-4c15-82e6-40d68ac5f2ab
  aliases: dsk000000000000000001
  keystore names: defaultKeyStore
.
. (Remaining elements not shown in this example.)
.
```

b. 创建更多密钥，并将它们存储在组中。 例如，输入:

```
print AdminTask.tklmSecretKeyCreate ('[-alias abc
 -keyStoreName defaultKeyStore -numOfKeys 10 -usage DS5000
  -keyGroupUuid KEYGROUP-9c97d9aa-b5f0-41a1-b65f-119756168211]')
```

- REST 界面:

a. 获取用于访问 IBM Security Key Lifecycle Manager REST 服务的唯一用户认证标识。 有关认证过程的更多信息，请参阅 REST 服务的验证流程。

b. 要调用 **Group List REST Service**，请发送 HTTP GET 请求。请将您在步骤 a 中获取的用户认证标识随请求消息一起传递，如以下示例所示。

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

输出可能类似于以下示例:

```
Status Code : 200 OK
Content-Language: en
[
 {
  "group name": "DS5K-ds5kdevice",
  "group type": "KEY",
  "group uuid": "KEYGROUP-9c97d9aa-b5f0-41a1-b65f-119756168211",
  "initialization date": "6/4/10 12:00:00 AM Central Standard Time",
  "activation date": "6/4/10 12:00:00 AM Central Standard Time",
 "keys":
[
 {
  "uuid": "KEY-66b0a3a2-3c52-4088-8772-0a1ddebf5803",
  "alias(es)": "dsk000000000000000000",
  "key store name(s)": "defaultKeyStore "
 },
 {
  "uuid": "KEY-3f1230fd-59ef-4c15-82e6-40d68ac5f2ab",
  "alias(es)": "dsk000000000000000001",
  "key store name(s)": "defaultKeyStore "
.
.
.
```

c. 使用 **Secret Key Create REST Service** 来创建更多密钥，并将它们存储在组中。 例如，您可以发送以下 HTTP 请求:

```
POST https://localhost:9080/SKLM/rest/v1/keys
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth authId=139aeh34567m
{"alias":"abc","numOfKeys":"10","keyGroupUuid":"KEYGROUP-9c97d9aa-
b5f0-41a1-b65f-119756168211",","usage":"DS5000"}
```

3. 成功指示符会根据界面的不同而不同:

- 图形用户界面:

“修改密钥”页面上的密钥表中显示了其他密钥。 请在将新密钥提供给设备之前备份这些密钥。

- 命令行界面:

  完成消息表示成功。另外，再次运行 **tklmGroupList** 命令可以验证您添加的密钥现在是否存在于密钥组中。 例如，输入:

  ```
  print AdminTask.tklmGroupList ('[-type keygroup -v y]')
  ```

- REST 界面:

  状态码 200 OK 表示成功。

下一步做什么

接下来，您可以将设备与机器进行关联。

修改（删除）密钥

您可以通过删除一个或多个密钥来修改 DS5000 存储服务器所使用的密钥数。

关于此任务

仅当不再需要密钥所保护的数据时，才能删除这些密钥。 删除密钥类似于擦除数据。 删除密钥后，无法对这些密钥保护的数据进行检索。

您可以使用“修改密钥”对话框、**tklmKeyDelete** 命令或 **Delete Key REST Service**。 您的角色必须具有执行修改操作和访问相应设备组的许可权。

开始之前，请确定要更改的信息，例如要删除的密钥数。

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”页面上的“密钥和设备管理”部分中，选择 **DS5000**。
     c. 单击**转至 > 管理密钥和设备**。
     d. 或者，右键单击 **DS5000**，然后选择**管理密钥和设备**。
   - 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
       ```

2. 修改密钥信息:
   - 图形用户界面:

在 DS5000 的管理页面上，在**设备序列号**列中选择设备。然后单击**修改 > 密钥**。或者，右键单击设备，然后选择**修改密钥**。

然后，在“修改密钥”对话框上，选择密钥并单击**删除**。阅读确认消息。 然后单击**确定**。

- 命令行界面:

  您可以删除密钥。 您的角色必须具有执行删除操作和访问相应设备组的许可权。例如，输入以下命令:

  ```
  print AdminTask.tklmKeyDelete ('[-alias aaa000000000000000000
   -keyStoreName defaultKeyStore]')
  ```

- REST 界面:

  使用 **Delete Key REST Service** 来删除密钥。 例如，您可以发送以下 HTTP 请求:

  ```
  DELETE https://localhost:9080/SKLM/rest/v1/keys/aaa000000000000000000
  Content-Type: application/json
  Accept : application/json
  Authorization: SKLMAuth authId=139aeh34567m
  ```

3. 成功指示符会根据界面的不同而不同:
   - 图形用户界面:

     显示一列，用于显示更改后的数据。 例如，已从“修改密钥”对话框中的密钥表中除去已删除的密钥。

   - 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

接下来，您可以将设备与机器进行关联。

IBM Spectrum Scale 文件管理

您可以使用 IBM Spectrum Scale 文件系统来管理 IBM Security Key Lifecycle Manager 中的密钥。

IBM Spectrum Scale（先前称为 GPFS）是一种高性能的共享磁盘文件管理解决方案，通过此解决方案，您可以从集群环境中的多个节点快速可靠地访问数据。应用程序可以使用标准文件系统接口轻松地访问文件，并且可以从多个节点同时访问同一文件。

IBM Spectrum Scale 提供文件加密支持，用于确保安全地存储和删除数据。IBM Spectrum Scale 通过使用加密密钥和加密策略来管理加密。

请参阅 IBM Spectrum Scale 文档以获取更多信息: http://www-01.ibm.com/support/knowledgecenter/SSFKCN_4.1.0/gpfs.v4r1_welcome.html。

管理证书和密钥

要管理证书和密钥，您可能希望添加、修改或删除其相关联节点名。 您还可以添加密钥以及与这些密钥相关联的名称。

关于此任务

您的角色必须具有执行查看操作和访问相应设备组的许可权。使用 IBM Spectrum Scale 的管理页面来添加、修改或删除证书或密钥。

开始之前，先检查该页面上的列（页面上提供了用于添加、修改或删除表项的各个按钮）。

表组织成下列信息区域:

- 在左侧列中，有关证书的信息指示证书 UUID、证书名称和端点计数。 端点计数是正在使用此证书的端点的数目。
- 在右侧列中，有关密钥的信息指示左侧证书对其具有访问权的密钥 UUID 和密钥名称。

过程

1. 登录图形用户界面。
   a. 在“欢迎”页面上的“密钥和设备管理”部分中，选择 **IBM Spectrum Scale**。
   b. 单击**转至 > 管理密钥和设备**。
   c. 或者，右键单击 **IBM Spectrum Scale**，然后选择**管理密钥和设备**。
2. 您可以添加、修改或删除密钥或证书。

   您可以执行下列管理任务:

   - 刷新列表。

     单击“刷新”图标  可刷新表中的项。
   - 添加

     单击**添加**。
     – 证书

       在“添加证书”对话框上，输入证书的名称以及文件名和位置。 然后单击**添加**。
     – 密钥

       在“添加密钥”对话框中，根据您的需求指定信息，例如要创建的密钥数（最多可创建 100 个密钥）。 然后单击**添加**。

     成功指示符各不相同，显示添加证书或密钥。
   - 修改

     要更改证书或密钥，请选择证书或密钥，然后单击**修改**。 或者，右键单击所选证书或密钥。 然后单击**修改**。
     – 证书

在“修改证书”对话框上指定更改。然后单击**修改**。 您的角色必须具有执行修改操作和访问相应设备组的许可权。

– 密钥

在“修改密钥”对话框上指定更改。然后单击**修改**。 您的角色必须具有执行删除操作和访问相应设备组的许可权。

成功指示符各不相同，显示证书或密钥列中的更改。

- 删除

要删除证书或密钥，请选择证书或密钥，然后单击**删除**。或者，右键单击所选证书或密钥，然后单击**删除**。

所删除证书的元数据将从 IBM Security Key Lifecycle Manager 数据库中除去。密钥数据也将被除去。 要确认删除，请单击**确定**。 您的角色必须具有执行删除操作和访问相应设备组的许可权。

成功指示符是已从表中删除证书。

添加证书

您可以添加更多证书以用于 IBM Security Key Lifecycle Manager。

关于此任务

您可以使用“添加证书”对话框来添加证书。 您的角色必须具有执行创建操作和访问相应设备组的许可权。

过程

1. 登录图形用户界面。
2. 在“欢迎”页面上的“密钥和设备管理”部分中，选择 **IBM Spectrum Scale**。
3. 单击**转至 > 管理密钥和设备**。
4. 或者，右键单击 **IBM Spectrum Scale**，然后选择**管理密钥和设备**。
5. 在 IBM Spectrum Scale 的管理页面上，单击**添加**。
6. 单击**证书**。
7. 在“添加证书”对话框上，根据您的需求指定信息。
8. 单击**添加**。

已将该证书添加到表。

修改证书

您可以修改有关 IBM Security Key Lifecycle Manager 数据库中的证书的信息。

关于此任务

您可以使用“修改证书”对话框来更新证书。 您的角色必须具有执行修改操作和访问相应设备组的许可权。

过程

1. 登录图形用户界面。
2. 在“欢迎”页面上的“密钥和设备管理”部分中，选择 **IBM Spectrum Scale**。
3. 单击**转至 > 管理密钥和设备**。
4. 或者，右键单击 **IBM Spectrum Scale**，然后选择**管理密钥和设备**。
5. 在 IBM Spectrum Scale 的管理页面上，选择证书。
6. 单击**修改**。
7. 或者，右键单击证书，然后选择**修改**，或双击证书条目。
8. 在“修改证书”对话框上，输入更改后的信息。
9. 单击**修改**。

   已更改表中的证书信息。

下一步做什么

接下来，您可以验证是否进行了更改。

删除证书

您可以删除已选中的证书，该证书可以处于任何状态（例如“活动”）。

关于此任务

您可以使用“删除”菜单项来删除证书。 您的角色必须具有执行删除操作和访问相应设备组的许可权。

过程

1. 登录图形用户界面。
2. 在“欢迎”页面上的“密钥和设备管理”部分中，选择 **IBM Spectrum Scale**。
3. 单击**转至 > 管理密钥和设备**。
4. 或者，右键单击 **IBM Spectrum Scale**，然后选择**管理密钥和设备**。
5. 在 IBM Spectrum Scale 的管理页面上，选择证书。
6. 单击**删除**。
7. 或者，右键单击证书，然后选择**删除**。
8. 删除证书之前，请在“确认”对话框上阅读确认消息以验证是否选择了正确的证书。 然后单击**确定**。

   已从表中除去该证书。

添加密钥

您可以添加密钥以用于 IBM Spectrum Scale。

关于此任务

您可以使用“添加密钥”对话框在现有组中创建一个或多个密钥。 您的角色必须具有执行创建操作和访问相应设备组的许可权。

开始之前，请确定用于命名密钥前缀的站点策略。

过程

1. 登录图形用户界面。
2. 在“欢迎”页面上的“密钥和设备管理”部分中，选择 **IBM Spectrum Scale**。
3. 单击**转至 > 管理密钥和设备**。
4. 或者，右键单击 **IBM Spectrum Scale**，然后选择**管理密钥和设备**。
5. 在 IBM Spectrum Scale 的管理页面上，单击**添加**。
6. 单击**密钥**。
7. 在“添加密钥”对话框上，为参数指定值。
8. 单击**添加**。 所添加的密钥将显示在密钥表中。 请在将密钥提供给设备之前备份这些密钥。

修改密钥

您可以修改有关 IBM Security Key Lifecycle Manager 数据库中的密钥的信息。

关于此任务

您可以使用“修改密钥”对话框来修改有关密钥的信息。 您的角色必须具有执行修改操作和访问相应设备组的许可权。

过程

1. 登录图形用户界面。
2. 在“欢迎”页面上的“密钥和设备管理”部分中，选择 **IBM Spectrum Scale**。
3. 单击**转至 > 管理密钥和设备**。
4. 或者，右键单击 **IBM Spectrum Scale**，然后选择**管理密钥和设备**。
5. 在 IBM Spectrum Scale 的管理页面上，选择一个密钥。
6. 单击**修改**。
7. 或者，右键单击密钥，然后选择**修改**，或双击密钥条目。
8. 在“修改密钥”对话框上，输入更改后的信息。 然后单击**修改**。 已更改表中的密钥信息。

删除密钥

您可以从 IBM Security Key Lifecycle Manager 数据库中删除密钥条目。

关于此任务

您可以使用“删除”菜单项来删除密钥。 您的角色必须具有执行删除操作和访问相应设备组的许可权。

过程

1. 登录图形用户界面。
2. 在“欢迎”页面上的“密钥和设备管理”部分中，选择 **IBM Spectrum Scale**。
3. 单击**转至 > 管理密钥和设备**。
4. 或者，右键单击 **IBM Spectrum Scale**，然后选择**管理密钥和设备**。
5. 在 IBM Spectrum Scale 的管理页面上，选择一个密钥。
6. 单击**删除**。

7. 或者，右键单击密钥，然后选择**删除**。
8. 删除密钥之前，请在“确认”对话框上阅读确认消息以验证是否选择了正确的密钥。然后单击**确定**。 已从表中除去该密钥信息。

备份和复原

IBM Security Key Lifecycle Manager 提供了一组操作，用于备份和复原当前处于活动状态的文件和数据。

IBM Security Key Lifecycle Manager 以独立于服务器的操作系统和目录结构的方式创建跨平台备份文件。 您可以将备份文件复原到与从中备份这些文件的操作系统不同的操作系统。 例如，可以在 Windows 系统上复原在 Linux 系统上备份的备份文件。

您可以使用跨平台备份实用程序在较低版本的 IBM Security Key Lifecycle Manager 上运行备份操作以备份关键数据。 您可以跨操作系统在当前版本的 IBM Security Key Lifecycle Manager 上复原这些备份文件。

注: 从 IBM Security Key Lifecycle Manager V2.6 发行版开始，不支持 Solaris 操作系统。 如果您是在 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。 然后，您可以运行复原操作，以便在任何受支持的操作系统（例如 Windows、Linux 或 AIX）上部署的 IBM Security Key Lifecycle Manager V2.6 系统上复原数据。

备份文件包含以下数据:

- IBM Security Key Lifecycle Manager 数据库表中的数据
- 信任库以及主密钥所在的密钥库
- IBM Security Key Lifecycle Manager 配置文件

您的角色必须具有备份或复原文件的许可权。

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。

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。

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。

通过针对大量密钥填充，增加其备份和复原事务允许使用的时间间隔，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:

- 确保任务发生时处于允许密钥服务活动停止的时间间隔期间。

- 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。
- 对于复原任务，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。

  在开始复原任务之前，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，恢复的文件必须写入副本计算机中。
- 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。

备份关键文件

使用图形用户界面、命令行界面或 REST 界面来备份 IBM Security Key Lifecycle Manager 的关键文件。

关于此任务

您可以使用“备份和复原”页面。另外，您还可以使用 **tklmBackupRun** 命令或 **Backup Run REST Service** 来备份关键数据。 您的角色必须具有备份文件的许可权。

IBM Security Key Lifecycle Manager 以独立于服务器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与从中备份这些文件的操作系统不同的操作系统。

注: 备份成功消息是系统范围的消息。 两个管理员可能会运行在时间上重叠的备份任务。在此时间间隔内，启动第二个任务失败的管理员可能会看到看到来自第一个备份任务的假成功消息。

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”页面上，单击**备份和复原**。
   - 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. 创建备份文件。 一次只能运行一项备份或复原任务。

- 图形用户界面:
  a. 在**备份和复原**表上，单击**浏览**并指定备份存储库位置，例如 C:\Program Files (x86)\IBM\WebSphere\AppServer\products\sklm\restore\backup\
  b. 单击**创建备份**。
  c. 在“创建备份”页面上，指定必需信息，例如加密密码值。 请确保保留加密密码以便将来复原备份时使用。
  d. 单击**创建备份**。
- 命令行界面:

  输入 tklmBackupRun 并指定创建备份文件所需的值。 例如，输入:

  ```
  print AdminTask.tklmBackupRun
   ('[-backupDirectory C:\\sklmbackup1 -password myBackupPwd]')
  ```
- REST 界面:
  a. 获取用于访问 IBM Security Key Lifecycle Manager REST 服务的唯一用户认证标识。 有关认证过程的更多信息，请参阅 REST 服务的验证流程。
  b. 要调用 **Backup Run REST Service**，请发送 HTTP POST 请求。请将您在步骤 a 中获取的用户认证标识随请求消息一起传递，如以下示例所示。

  ```
  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"}
  ```

3. 这将显示一条消息，指出已创建备份文件或备份操作已成功。

   备份文件的时间戳记中包含以 RFC 822 格式表示的格林威治标准时间 (GMT) 偏移量。 即文件名包含用于指定时区是早于还是晚于格林威治标准时间 (GMT) 的 *+hhmm* 或 *-hhmm* 元素。 例如，文件名可以是 sklm_v2.6.0.0_20100123144220-**0800**_backup.jar，其中 -0800 表示该时区比格林威治标准时间 (GMT) 晚 8 小时。

下一步做什么

保留加密密码以便将来复原备份时使用。 请查看备份文件所在的目录以确保该备份文件存在。 请勿编辑备份 JAR 文件中的文件。 您尝试编辑的文件将变得不可读。

复原备份文件

使用图形用户界面、命令行界面或 REST 界面来复原 IBM Security Key Lifecycle Manager 的备份文件。

关于此任务

您可以使用“备份和复原”页面来复原备份文件。 另外，您还可以使用 **tklmBackupRunRestore** 命令或 **Backup Run Restore REST Service** 来复原此文件。 您的角色必须具有复原文件的许可权。. 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与从中备份这些文件的操作系统不同的操作系统。

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。

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”页面上，单击**备份和复原**。
   - 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. 复原所选备份文件。 一次只能运行一项备份或复原任务。 如果您将某个文件复原到副本计算机，请使用磁盘之类的介质或电子传输将此文件复制到该计算机。
   - 图形用户界面:
     a. 单击**显示备份**以显示要复原的备份文件。
     b. 在**备份和复原**表上，选择该表中列出的备份文件。
     c. 单击**从备份复原**。

        注:
        – 如果您在分布式系统上应用了修订包，请勿尝试复原应用该修订包之前创建的备份文件。
     d. 在“复原备份”页面上，指定用于创建备份文件的加密密码。
     e. 单击**复原备份**。
   - 命令行界面:

     输入 tklmBackupRunRestore 并指定必需信息，例如路径和备份文件名。 指定用于创建备份文件的加密密码。 例如，输入:

     ```
     print AdminTask.tklmBackupRunRestore
      ('[-backupFilePath /opt/mysklmbackups/sklm_v2.6.0.0_20150705235417-1200_backup
       -password myBackupPwd]')
     ```

   - REST 界面:
     a. 获取用于访问 IBM Security Key Lifecycle Manager REST 服务的唯一用户认证标识。 有关认证过程的更多信息，请参阅 REST 服务的验证流程。
     b. 要调用 **Backup Run Restore REST Service**，请发送 HTTP POST 请求。请将您在步骤 a 中获取的用户认证标识随请求消息一起传递，如以下示例所示。

```
POST https://localhost:9080/SKLM/rest/v1/ckms/restore
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth authId=139aeh34567m
Accept-Language : en
{"backupFilePath":"/opt/mysklmbackups/sklm_v2.5.0.0_20130705235417-
1200_backup.jar","password":"myBackupPwd"}
```

3. 这将显示一条消息，指出复原操作已成功。

结果

当 SKLMConfig.properties 文件中的 **autoRestartAfterRestore** 属性值为 true（缺省值）时，复原备份文件后，IBM Security Key Lifecycle Manager 服务器会自动重新启动。

注: 自动重新启动 IBM Security Key Lifecycle Manager 服务器之后，Windows WebSphere Application Server 服务状态不会进行刷新并且会显示为“已停止”。

下一步做什么

然后，确定服务器是否处于期望的状态。 例如，您可以检查密钥库以确定在执行备份文件复原之前存在问题的证书现在是否可供使用。

安装 Java 密码术扩展无限制强度管辖区域策略文件

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。

关于此任务

注: 在当前版本中，安装 IBM Security Key Lifecycle Manager 之后，缺省情况下会生成 AES 256 位主密钥，并且将在服务器上安装 JCE 无限制强度管辖区域策略文件。

过程

1. 访问 ibm.com Web 站点 (https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk.)。
2. 指定 ibm.com Web 站点用户标识和密码。
3. 下载 unrestrictedpolicyfiles.zip 文件。
4. 停止 WebSphere Application Server。
5. 将压缩文件的内容解压缩到 <AppServer>\java\jre\lib\security 目录。 例如:

   Windows

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

   Linux `/opt/IBM/WebSphere/AppServer/java/jre/lib/security`

6. 重新启动 WebSphere Application Server。

在分布式系统上启动和停止 IBM Security Key Lifecycle Manager 服务器

可能想要使用 **startServer** 或 **stopServer** 命令启动或停止 IBM Security Key Lifecycle Manager 服务器。 例如，在复原任务完成之后，重新启动 IBM Security Key Lifecycle Manager 服务器。

关于此任务

当 SKLMConfig.properties 文件中的 **autoRestartAfterRestore** 属性值为 true（缺省值）时，复原备份文件后，IBM Security Key Lifecycle Manager 服务器会自动重新启动。

用于启动和停止 IBM Security Key Lifecycle Manager 服务器 的脚本在 *WAS_HOME*/bin 目录中。

过程

1. 导航至 *WAS_HOME*/bin 目录。
2. 启动或停止服务器。
   - 启动

     在 Windows 系统上:
     ```
     startServer.bat server1
     ```
     在诸如 Linux 或 AIX 的系统上:
     ```
     ./startServer.sh server1
     ```
   - 停止

     在 Windows 系统上:
     ```
     stopServer.bat server1
     ```
     在诸如 Linux 或 AIX 的系统上:
     ```
     ./stopServer.sh server1
     ```

   缺省情况下，将启用全局安全性。 请输入 WebSphere Application Server 管理员的用户标识和密码，作为 stopServer 的参数。 当省略这些参数时，脚本会提示您输入参数，但是可以在命令行上指定:

   在 Windows 系统上:
   ```
   stopServer.bat server1 -username wasadmin -password mypwd
   ```
   在诸如 Linux 或 AIX 的系统上:
   ```
   ./stopServer.sh server1  -username wasadmin -password mypwd
   ```

下一步做什么

确定 IBM Security Key Lifecycle Manager 是否正在运行。例如，在 Web 浏览器中打开 IBM Security Key Lifecycle Manager，然后登录。

启用全局安全性

可能发生必须启用全局安全性的情况。

关于此任务

当使用 IBM Security Key Lifecycle Manager 时，不要禁用全局安全性。

过程

1. 要启用全局安全性，请以 WebSphere Application Server 管理员 WASAdmin 的身份登录。
2. 在导航栏中，单击**安全性**。
3. 单击**保证管理、应用程序和基础结构的安全**。
4. 勾选**启用管理安全性**复选框。

   请确保也选择了**启用应用程序安全性**，并且未选择**使用 Java 2 安全性限制对本地资源的应用程序访问**。
5. 单击**应用**。
6. 在“消息”框中单击**保存**。 单击**注销**。
7. 停止并重新启动服务器。
8. 重新装入 IBM Security Key Lifecycle Manager 登录页面。验证该页面是否需要密码。

禁用全局安全性

可能发生必须禁用全局安全性的情况。

关于此任务

当使用 IBM Security Key Lifecycle Manager 时，不要禁用全局安全性。

过程

1. 要禁用全局安全性，请以 WebSphere Application Server 管理员 WASAdmin 的身份登录。
2. 在导航栏中，单击**安全性**。
3. 单击**保证管理、应用程序和基础结构的安全**。
4. 清除**启用管理安全性**复选框。
5. 单击**应用**。
6. 在“消息”框中单击**保存**。 单击**注销**。
7. 停止并重新启动服务器。
8. 重新装入 IBM Security Key Lifecycle Manager 登录页面。验证页面是否不需要密码。

删除备份文件

使用图形用户界面或命令行界面来删除 IBM Security Key Lifecycle Manager 的备份文件。 例如，您可以删除系统对其不再有业务需要的备份文件。

关于此任务

您可以使用“备份和复原”页面来删除备份文件。

您的角色必须具有备份文件的许可权。

过程

1. 登录图形用户界面。
2. 在“欢迎”页面上，单击**备份和复原**。
3. 在**备份和复原**表上，选择该表中列出的备份文件。
4. 单击**删除备份**，然后确认您要删除该文件。

下一步做什么

检查在其中存储备份文件的目录以确定是否删除了指定文件。

在命令行或 REST 界面上运行备份和复原任务

您可以使用命令行界面或 REST 界面来完成更多无法在图形用户界面上完成的备份和复原任务。

关于此任务

开始之前，请获取密码。 您的角色必须具有备份或复原文件的许可权。

过程

1. 浏览至相应的目录并登录:
   - 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（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. 完成该任务:
   - 命令行界面:

     tklmBackupGetProgress

     输入 tklmBackupGetProgress 以确定正在运行的备份任务的当前阶段。 例如，输入:

     ```
     print AdminTask.tklmBackupGetProgress()
     ```

     tklmBackupGetRestoreProgress

     输入 tklmBackupGetRestoreProgress 以确定正在运行的复原任务的当前阶段。 例如，输入:

     ```
     print AdminTask.tklmBackupGetRestoreProgress()
     ```

     tklmBackupGetRestoreResult

输入 tklmBackupGetRestoreResult 以确定复原任务已成功完成还是失败。例如，输入:

```
print AdminTask.tklmBackupGetRestoreResult()
```

tklmBackupGetResult

输入 tklmBackupGetResult 以确定备份任务已成功完成还是失败。 例如，输入:

```
print AdminTask.tklmBackupGetResult()
```

tklmBackupIsRestoreRunning

输入 tklmBackupIsRestoreRunning 以确定复原任务是否处于运行状态。例如，输入:

```
print AdminTask.tklmBackupIsRestoreRunning()
```

tklmBackupIsRunning

输入 tklmBackupIsRunning 以确定备份任务是否处于运行状态。 例如，输入:

```
print AdminTask.sklmBackupIsRunning()
```

tklmBackupList

输入 tklmBackupList 以列出目录中的备份文件。 例如，输入:

```
print AdminTask.tklmBackupList
 ('[-backupDirectory C:\\tipbak1\\tklmbackup1 -v y]')
```

- REST 界面:
  a. 获取用于访问 IBM Security Key Lifecycle Manager REST 服务的唯一用户认证标识。 有关认证过程的更多信息，请参阅 REST 服务的验证流程。
  b. 要调用 REST 服务，请发送 HTTP 请求。请将您在步骤 a 中获取的用户认证标识随请求消息一起传递，如以下示例所示。

Backup Get Progress REST Service

使用 **Backup Get Progress REST Service** 以确定正在运行的备份任务的当前阶段。 例如，您可以发送以下 HTTP 请求:

```
GET https://localhost:9080/SKLM/rest/v1/ckms/backups/progress
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth authId=139aeh34567m
Accept-Language : en
```

Backup Get Restore Progress REST Service

使用 **Backup Get Restore Progress REST Service** 以确定正在运行的复原任务的当前阶段。 例如，您可以发送以下 HTTP 请求:

```
GET https://localhost:9080/SKLM/rest/v1/ckms/restore/progress
Content-Type: application/json
Accept: application/json
Authorization: SKLMAuth authId=139aeh34567m
Accept-Language: en
```

Backup Get Restore Result REST Service

输入 **Backup Get Restore Result REST Service** 以确定复原任务已成功完成还是失败。 例如，您可以发送以下 HTTP 请求:

```
GET https://localhost:9080/SKLM/rest/v1/ckms/restore/result
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth authId=139aeh34567m
Accept-Language : en
```

Backup Get Result REST Service

输入 **Backup Get Result REST Service** 以确定备份任务已成功完成还是失败。 例如，您可以发送以下 HTTP 请求:

```
GET https://localhost:9080/SKLM/rest/v1/ckms/backups/result
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth authId=139aeh34567m
Accept-Language : en
```

Backup List REST Service

使用 **Backup List REST Service** 以列出目录中的备份文件。 例如，您可以发送以下 HTTP 请求:

```
GET https://localhost:9080/SKLM/rest/v1/ckms/backups?
backupDirectory=
/sklmbackup
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth authId=139aeh34567m
Accept-Language : en
```

完成消息表示成功。

- 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。

针对较低版本的 IBM Security Key Lifecycle Manager 的备份和复原操作

您可以使用当前版本的 IBM Security Key Lifecycle Manager 的跨平台备份实用程序在较低版本的 IBM Security Key Lifecycle Manager 上运行备份操作，以备份关键数据。您可以使用复原实用程序跨操作系统在当前版本的 IBM Security Key Lifecycle Manager 上复原这些备份文件。

备份 Encryption Key Manager V2.1 数据

使用 IBM Security Key Lifecycle Manager V2.6 备份实用程序来创建 Encryption Key Manager V2.1 备份文件。

开始之前

- 您必须在系统上安装 IBM Security Key Lifecycle Manager V2.6。
- 请确保 Encryption Key Manager 文件夹包含与磁带机表、密钥组和元数据相关的配置文件、密钥库文件、其他数据文件和文件夹。

关于此任务

您可以使用备份实用程序以独立于服务器的操作系统和目录结构的方式创建跨平台备份文件。 您可以跨操作系统在安装了 IBM Security Key Lifecycle Manager V2.6 的系统上复原这些跨平台兼容备份文件。

过程

1. 将 Encryption Key Manager 文件夹和所有其他必需文件复制到安装了 IBM Security Key Lifecycle Manager V2.6 的系统。
2. 确保复制 KeyManagerConfig.properties 文件和 KeyManagerConfig.properties 文件中提及的以下文件。

   注: 您必须编辑 Encryption Key Manager 文件夹中的 KeyManagerConfig.properties 配置文件以指定密钥库文件和其他数据文件的绝对路径，如以下示例中所示。

   ```
   Admin.ssl.keystore.name=C\:/EKM21/test.keys.ssl
   Admin.ssl.truststore.name=C\:/EKM21/test.keys.ssl
   TransportListener.ssl.truststore.name=C\:/EKM21/test.keys.ssl
   TransportListener.ssl.keystore.name=C\:/EKM21/test.keys.ssl
   config.keystore.file=C\:/EKM21/test.keys.jceks
   config.drivetable.file.url=FILE\:C\:/EKM21/filedrive.table
   Audit.handler.file.directory=C\:/audit
   Audit.metadata.file.name=C\:/EKM21/metadata/EKMData.xml
   config.keygroup.xml.file=FILE\:C\:/EKM21/KeyGroups.xml
   ```

3. 在安装了 V2.6 的系统上找到备份实用程序文件夹。

   Windows

   <SKLM_INSTALL_HOME>\migration\utilities\ekm21

   缺省位置为 C:\Program Files (x86)\IBM\SKLMV26\migration\utilities\ekm21。

   Linux <SKLM_INSTALL_HOME>/migration/utilities/ekm21

   缺省位置为 /opt/IBM/SKLMV26/migration/utilities/ekm21。

4. 编辑备份实用程序文件夹中的 backup.properties 以配置特性，如以下示例所示。您必须为除 BACKUP_DIR 特性（可选）以外的所有特性设置值。

   如果未指定 BACKUP_DIR 的值，那么将在运行备份实用程序的相同目录下的 backup 文件夹中创建备份文件。

   注: 在 Windows 操作系统上，用于备份操作的 backup.properties 文件不能包含首尾带有空格的属性关键字和值。

   Windows

   ```
   KLM_VERSION=2.1
   BACKUP_DIR=C:\\ekm_backup
   EKM_HOME=C:\\EKM21
   BACKUP_PASSWORD=passw0rd123
   JAVA_HOME=C:\\Program Files (x86)\\IBM\\WebSphere
   \\AppServer\\java
   ```

   Linux

   ```
   KLM_VERSION=2.1
   BACKUP_DIR=/ekm_backup
   EKM_HOME=/EKM21
   BACKUP_PASSWORD=passw0rd123
   JAVA_HOME=/opt/IBM/WebSphere/AppServer/java
   ```

注: 在 Windows 系统上，在属性文件中指定路径时，请使用“/”或“\\”作为路径分隔符，如以下示例所示。

```
C:\\ekm_backup
```

或

```
C:/ekm_backup
```

5. 打开命令提示符并运行备份实用程序。

Windows

转至 *<SKLM_INSTALL_HOME>*\migration\utilities\ekm21 目录并运行以下命令:

backupEKM21.bat

Linux 转至 *<SKLM_INSTALL_HOME>*/migration/utilities/ekm21 目录并运行以下命令:

backupEKM21.sh

下一步做什么

- 请复审包含备份文件的目录以确保备份文件存在。这些备份文件是在为 backup.properties 文件中的 BACKUP_DIR 指定的位置创建的。
- 请检查 backup.log 文件以找出错误或异常。backup.log 文件是在运行备份实用程序的目录中创建的。要成功执行备份操作，请确保该日志文件中没有错误或异常。
- 保留备份密码以供将来复原备份时使用。
- 请不要在备份归档中编辑文件。您尝试编辑的文件将会不可读。

复原 Encryption Key Manager V2.1 备份文件

通过使用图形用户界面、命令行界面、REST 界面或迁移复原脚本，您可以在安装有 IBM Security Key Lifecycle Manager V2.6 的系统上复原 Encryption Key Manager V2.1 跨平台备份文件。

开始之前

在系统上安装 IBM Security Key Lifecycle Manager V2.6。 您必须具有 Encryption Key Manager 备份文件，并确保具有创建该备份文件时所使用的密码。

注: 您的角色必须具有运行备份和复原操作的许可权。

关于此任务

您可以跨操作系统在安装了 IBM Security Key Lifecycle Manager V2.6 的系统上复原 Encryption Key Manager 跨平台兼容备份文件。

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。

过程

1. 登录安装了 IBM Security Key Lifecycle Manager V2.6 的系统。

2. 将备份文件（例如，sklm_vEKM21_20150820113253+0530_backup.jar）从 Encryption Key Manager V2.1 系统复制到选择的目录。
3. 使用下列任何方法复原备份文件。

图形用户界面	1. 以授权用户身份（例如，SKLMAdmin）登录图形用户界面。 2. 在“欢迎”页面上，单击**备份和复原**。 3. 在**备份存储库位置**字段中，指定 Encryption Key Manager 备份文件所在目录的完整路径。要找到该目录，请单击**浏览**。 4. 单击**显示备份**以显示要复原的备份文件。 5. 在**备份和复原**表中，选择备份文件。 6. 单击**从备份复原**。 7. 在“复原备份”页面上，指定创建备份文件时所使用的备份密码。 8. 单击**复原备份**。 9. 重新启动 IBM Security Key Lifecycle Manager 服务器。

命令行界面	1. 转至 WAS_HOME/bin 目录。 例如:
	Windows
	`cd drive:\Program Files (x86)\IBM\WebSphere\AppServer\bin`
	Linux `cd /opt/IBM/WebSphere/AppServer/bin`
	2. 使用授权用户标识（例如 SKLMAdmin）启动 **wsadmin** 界面。 例如:
	Windows
	`wsadmin -username SKLMAdmin -password mypwd -lang jython`
	Linux
	`./wsadmin.sh -username SKLMAdmin -password mypwd -lang jython`
	3. 通过指定参数（例如备份文件名及其完整路径，以及创建备份时所使用的备份密码）来运行 **tklmBackupRunRestore** CLI 命令，如以下示例所示。
	`print AdminTask.tklmBackupRunRestore ('[-backupFilePath /opt/mysklmbackups /sklm_vEKM21_20150820113253+0530_backup.jar -password myBackupPwd]')`
	4. 重新启动 IBM Security Key Lifecycle Manager 服务器。

REST 界面	1. 打开 REST 客户机。
	2. 获取用于访问 IBM Security Key Lifecycle Manager REST 服务的唯一用户认证标识。 有关认证过程的更多信息，请参阅 REST 服务的验证流程。
	3. 要调用 **Backup Run Restore REST Service**，请将备份文件名及其完整路径和备份密码指定为参数来发送 HTTP POST 请求。 请将您在步骤 b 中获取的用户认证标识随请求消息一起传递，如以下示例所示。
	`POST https://localhost:9080/SKLM/rest/v1/ckms/restore`
	`Content-Type: application/json`
	`Accept: application/json`
	`Authorization: SKLMAuth authId=139aeh34567m`
	`Accept-Language: en`
	`{"backupFilePath":"/opt/mysklmbackups`
	`/sklm_vEKM21_20150820113253+0530_backup.jar`
	`backup.jar","password":"myBackupPwd"}`
	4. 重新启动 IBM Security Key Lifecycle Manager 服务器。

迁移复原脚本	1. 找到 IBM Security Key Lifecycle Manager 复原实用程序。 **Windows** <*SKLM_INSTALL_HOME*>\migration\utilities\ekm21 缺省位置为 C:\Program Files (x86)\IBM\SKLMV26\migration\utilities\ekm21。 **Linux** <*SKLM_INSTALL_HOME*>/migration/utilities/ekm21 缺省位置为 /opt/IBM/SKLMV26/migration/utilities/ekm21。 2. 编辑 ekm21 文件夹中的 restore.properties 以配置属性，如以下示例所示: **注**: 在 Windows 操作系统上，用于复原操作的 restore.properties 文件不能包含首尾带有空格的属性关键字和值。 **Windows** WAS_HOME=C:\\Program Files (x86)\\IBM\\WebSphere \\AppServer BACKUP_PASSWORD=passw0rd123 DB_PASSWORD=sklmdb26 RESTORE_FILE=C:\\ekm_restore\ sklm_vEKM21_20150924024117-0400_backup.jar WAS_USER_PWD=wasadmin RESTORE_USER_ROLES=n **Linux** WAS_HOME=/opt/IBM/WebSphere/AppServer BACKUP_PASSWORD=passw0rd123 DB_PASSWORD=sklmdb26 RESTORE_FILE=/ekm_restore/sklm_vEKM21_ 20150820113253+0530_backup.jar WAS_USER_PWD=wasadmin RESTORE_USER_ROLES=n **注**: 在 Windows 操作系统上，在属性文件中指定路径时，请使用“/”或“\\”作为路径分隔符，如以下示例所示。 C:\\ekm_restore 或 C:/ekm_restore 3. 打开命令提示符并运行复原实用程序。 **Windows** 转至 <*SKLM_INSTALL_HOME*>\migration\utilities\ekm21 目录并运行以下命令: **restoreEKM21.bat** **Linux** 转至 <*SKLM_INSTALL_HOME*>/migration/utilities/ekm21 目录并运行以下命令: **restoreEKM21.sh** 4. 重新启动 IBM Security Key Lifecycle Manager 服务器。

备份 IBM Security Key Lifecycle Manager V1.0 (TKLM V1.0) 数据

使用 IBM Security Key Lifecycle Manager V2.6 备份实用程序来创建 IBM Security Key Lifecycle Manager V1.0（前身为 Tivoli Key Lifecycle Manager V1.0）跨平台备份文件。

开始之前

您必须在系统上安装 IBM Security Key Lifecycle Manager V2.6。 确保安装了 IBM Security Key Lifecycle Manager V1.0（具有最新 FP7）的系统可用。必须先配置密钥库，然后再运行备份操作。

关于此任务

您可以使用备份实用程序以独立于服务器的操作系统和目录结构的方式创建跨平台备份文件。 您可以跨操作系统在安装了 IBM Security Key Lifecycle Manager V2.6 的系统上复原这些跨平台兼容备份文件。

过程

在安装了 IBM Security Key Lifecycle Manager V2.6 和 V1.0 的系统上运行下列步骤。

IBM Security Key Lifecycle Manager V2.6	1. 使用用户凭证登录系统。 2. 找到备份实用程序文件夹。 **Windows** <*SKLM_INSTALL_HOME*>\migration\utilities\v1 缺省位置为 C:\Program Files (x86)\IBM\SKLMV26\migration\utilities\v1。 **Linux** <*SKLM_INSTALL_HOME*>/migration/utilities/v1 缺省位置为 /opt/IBM/SKLMV26/migration/utilities/v1。 3. 将 rt.jar 和 xml.jar 文件从 <WAS_HOME>/java/jre/lib 文件夹复制到步骤 b 中描述的备份实用程序文件夹。

IBM Security Key Lifecycle Manager V1.0	1. 使用用户凭证登录系统。
	2. 将 v1 文件夹从安装了 IBM Security Key Lifecycle Manager V2.6 的系统复制到您选择的本地目录。
	3. 编辑 v1 文件夹中的 backup.properties 以配置特性，如以下示例所示。您必须为除 BACKUP_DIR 特性（可选）以外的所有特性设置值。
	
	如果未指定 BACKUP_DIR 的值，那么将在运行备份实用程序的相同目录下的 backup 文件夹中创建备份文件。
	注: 在 Windows 操作系统上，用于备份操作的 backup.properties 文件不能包含首尾带有空格的属性关键字和值。
	
	Windows
	`TKLM_TIP_HOME=C:\\IBM\\tivoli\\tip`
	`DB_PASSWORD=tklmdb2`
	`KEYSTORE_PASSWORD=Passw0rd`
	`TIP_USER_PWD=tipadmin`
	`BACKUP_PASSWORD=passw0rd123`
	`BACKUP_DIR=C:\\tklmv1_backup`
	
	Linux
	`TKLM_TIP_HOME=/opt/IBM/tivoli/tip/`
	`DB_PASSWORD=tklmdb2`
	`KEYSTORE_PASSWORD=Passw0rd`
	`TIP_USER_PWD=tipadmin`
	`BACKUP_PASSWORD=passw0rd123`
	`BACKUP_DIR=/tklmv1_backup`
	注: 在 Windows 操作系统上，在属性文件中指定路径时，请使用“/”或“\\”作为路径分隔符，如以下示例所示。
	
	`C:\\tklmv1_backup`
	
	或
	
	`C:/tklmv1_backup`
	4. 打开命令提示符并运行备份实用程序。
	
	Windows
	转至 v1 目录（请参阅步骤 b）并运行以下命令:
	backupV1.bat
	Linux 转至 v1 目录（请参阅步骤 b）并运行以下命令:
	backupV1.sh

下一步做什么

- 请复审包含备份文件的目录以确保备份文件存在。这些备份文件是在为 backup.properties 文件中的 BACKUP_DIR 指定的位置创建的。
- 请检查 backup.log 文件以找出错误或异常。backup.log 文件是在运行备份实用程序的目录中创建的。要成功执行备份操作，请确保该日志文件中没有错误或异常。
- 保留备份密码以供将来复原备份时使用。
- 请不要在备份归档中编辑文件。您尝试编辑的文件将会不可读。

复原 IBM Security Key Lifecycle Manager V1.0 (TKLM V1.0) 备份文件

通过使用图形用户界面、命令行界面、REST 界面或迁移复原脚本，您可以在安装有 IBM Security Key Lifecycle Manager V2.6 的系统上复原 IBM Security Key Lifecycle Manager V1.0（前身为 Tivoli Key Lifecycle Manager V1.0）跨平台备份文件。

开始之前

在系统上安装 IBM Security Key Lifecycle Manager V2.6。 您必须具有来自较低版本的备份文件，并确保具有创建该备份文件时所使用的密码。

注: 您的角色必须具有运行备份和复原操作的许可权。

关于此任务

您可以跨操作系统在安装了 IBM Security Key Lifecycle Manager V2.6 的系统上复原 IBM Security Key Lifecycle Manager V1.0 跨平台兼容备份文件。

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。

过程

1. 登录安装了 IBM Security Key Lifecycle Manager V2.6 的系统。
2. 将备份文件（例如，`tklm_v1.0.0.7_20150729013250-0400_migration_backup.jar`）从 V1.0 系统复制到选择的目录。
3. 使用下列任何方法复原备份文件。

图形用户界面	1. 以授权用户身份（例如，`SKLMAdmin`）登录图形用户界面。 2. 在“欢迎”页面上，单击**备份和复原**。 3. 在**备份存储库位置**字段中，指定 V1.0 备份文件所在目录的完整路径。要找到该目录，请单击**浏览**。 4. 单击**显示备份**以显示要复原的备份文件。 5. 在**备份和复原**表中，选择备份文件。 6. 单击**从备份复原**。 7. 在“复原备份”页面上，指定创建备份文件时所使用的备份密码。 8. 单击**复原备份**。 9. 重新启动 IBM Security Key Lifecycle Manager 服务器。 **注:** 您无法使用图形用户界面从 IBM Security Key Lifecycle Manager V1.0 备份复原角色、用户和组。

命令行界面	1. 转至 WAS_HOME/bin 目录。 例如:
	
	Windows
	`cd drive:\Program Files (x86)\IBM\WebSphere\AppServer\bin`
	
	Linux `cd /opt/IBM/WebSphere/AppServer/bin`
	
	2. 使用授权用户标识（例如 SKLMAdmin）启动 **wsadmin** 界面。 例如:
	
	Windows
	`wsadmin -username SKLMAdmin -password mypwd -lang jython`
	
	Linux
	`./wsadmin.sh -username SKLMAdmin -password mypwd -lang jython`
	
	3. 通过指定参数（例如备份文件名及其完整路径，以及创建备份时所使用的备份密码）来运行 **tklmBackupRunRestore** CLI 命令，如以下示例所示。
	
	`print AdminTask.tklmBackupRunRestore ('[-backupFilePath /opt/mysklmbackups/tklm_v1.0.0.7_20150729013250-0400_migration_backup.jar -password myBackupPwd]')`
	
	4. 重新启动 IBM Security Key Lifecycle Manager 服务器。
	
	注: 您无法使用命令行界面从 IBM Security Key Lifecycle Manager V1.0 备份复原角色、用户和组。

REST 界面	1. 打开 REST 客户机。
	
	2. 获取用于访问 IBM Security Key Lifecycle Manager REST 服务的唯一用户认证标识。 有关认证过程的更多信息，请参阅 REST 服务的验证流程。
	
	3. 要调用 **Backup Run Restore REST Service**，请将备份文件名及其完整路径和备份密码指定为参数来发送 HTTP POST 请求。 请将您在步骤 b 中获取的用户认证标识随请求消息一起传递，如以下示例所示。
	
	`POST https://localhost:9080/SKLM/rest/v1/ckms/restore`
	`Content-Type: application/json`
	`Accept: application/json`
	`Authorization: SKLMAuth authId=139aeh34567m`
	`Accept-Language : en`
	`{"backupFilePath":"/opt/mysklmbackups/tklm_v1.0.0.7_20150729013250-0400_migration_backup.jar backup.jar","password":"myBackupPwd"}`
	
	4. 重新启动 IBM Security Key Lifecycle Manager 服务器。
	
	注: 您无法使用 REST 界面从 IBM Security Key Lifecycle Manager V1.0 备份复原角色、用户和组。

迁移复原脚本	1. 找到 IBM Security Key Lifecycle Manager 复原实用程序。 **Windows** <*SKLM_INSTALL_HOME*>\migration\utilities\v1 缺省位置为 C:\Program Files (x86)\IBM\SKLMV26\migration\utilities\v1。 **Linux** <*SKLM_INSTALL_HOME*>/migration/utilities/v1 缺省位置为 /opt/IBM/SKLMV26/migration/utilities/v1。 2. 编辑 v1 文件夹中的 restore.properties 以配置属性，如以下示例所示: **注**: 在 Windows 操作系统上，用于复原操作的 restore.properties 文件不能包含首尾带有空格的属性关键字和值。 **Windows** WAS_HOME=C:\\Program Files (x86)\\IBM\\WebSphere\\AppServer BACKUP_PASSWORD=passw0rd123 DB_PASSWORD=sklmdb26 RESTORE_FILE=C:\\tklmv1_restore\\tklm_v1.0.0.7_20150729013250-0400_migration_backup.jar WAS_USER_PWD=wasadmin RESTORE_USER_ROLES=y **Linux** WAS_HOME=/opt/IBM/WebSphere/AppServer BACKUP_PASSWORD=passw0rd123 DB_PASSWORD=sklmdb26 RESTORE_FILE=/tklmv1_restore/tklm_v1.0.0.7_20150729013250-0400_migration_backup.jar WAS_USER_PWD=wasadmin RESTORE_USER_ROLES=y **注**: 在 Windows 操作系统上，在属性文件中指定路径时，请使用“/”或“\\”作为路径分隔符，如以下示例所示。 C:\\tklmv1_restore 或 C:/tklmv1_restore 3. 打开命令提示符并运行复原实用程序。 **Windows** 转至 <*SKLM_INSTALL_HOME*>\migration\utilities\v1 目录并运行以下命令: **restoreV1.bat** **Linux** 转至 <*SKLM_INSTALL_HOME*>/migration/utilities/v1 目录并运行以下命令: **restoreV1.sh** 4. 重新启动 IBM Security Key Lifecycle Manager 服务器。 **注**: 您**可以**使用迁移复原脚本从 IBM Security Key Lifecycle Manager V1.0 备份复原角色、用户和组。

下一步做什么

为 LTO 密钥组和 3592 证书配置的回滚将不会自动从较低版本的 IBM Security Key Lifecycle Manager 中复原。您必须为证书和密钥组手动设置回滚。

有关更多信息，请参阅第 152 页的『复原回滚证书和密钥组』。

备份 IBM Security Key Lifecycle Manager V2.0 (TKLM V2.0) 数据

使用 IBM Security Key Lifecycle Manager V2.6 备份实用程序来创建 IBM Security Key Lifecycle Manager V2.0（前身为 Tivoli Key Lifecycle Manager V2.0）备份文件。

开始之前

您必须在系统上安装 IBM Security Key Lifecycle Manager V2.6。 确保安装了 IBM Security Key Lifecycle Manager V2.0（具有最新 FP6）的系统可用。必须先配置密钥库，然后再运行备份操作。

关于此任务

您可以使用备份实用程序以独立于服务器的操作系统和目录结构的方式创建跨平台备份文件。 您可以跨操作系统在安装了 IBM Security Key Lifecycle Manager V2.6 的系统上复原这些跨平台兼容备份文件。

过程

在安装了 IBM Security Key Lifecycle Manager V2.6 和 V2.0 的系统上运行下列步骤。

IBM Security Key Lifecycle Manager V2.6	1. 使用用户凭证登录系统。 2. 找到备份实用程序文件夹。 **Windows** <*SKLM_INSTALL_HOME*>\migration\utilities\v2 缺省位置为 C:\Program Files (x86)\IBM\SKLMV26\migration\utilities\v2。 **Linux** <*SKLM_INSTALL_HOME*>/migration/utilities/v2 缺省位置为 /opt/IBM/SKLMV26/migration/utilities/v2。 3. 将 rt.jar 和 xml.jar 文件从 <WAS_HOME>/java/jre/lib 文件夹复制到步骤 b 中描述的备份实用程序文件夹。

IBM Security Key Lifecycle Manager V2.0	1. 使用用户凭证登录系统。
	2. 将 v2 文件夹从安装了 IBM Security Key Lifecycle Manager V2.6 的系统复制到您选择的本地目录。
	3. 编辑 v2 文件夹中的 backup.properties 以配置属性，如以下示例所示。您必须为除 BACKUP_DIR 特性（可选）以外的所有特性设置值。
	
	如果未指定 BACKUP_DIR 的值，那么将在运行备份实用程序的相同目录下的 backup 文件夹中创建备份文件。
	注: 在 Windows 操作系统上，用于备份操作的 backup.properties 文件不能包含首尾带有空格的属性关键字和值。
	
	Windows
	`TKLM_TIP_HOME=C:\\IBM\\tivoli\\tiptklmV2`
	`DB_PASSWORD=tklmdb2`
	`KEYSTORE_PASSWORD=Passw0rd`
	`TIP_USER_PWD=tipadmin`
	`BACKUP_PASSWORD=passw0rd123`
	`BACKUP_DIR=C:\\tklmv2_backup`
	
	Linux
	`TKLM_TIP_HOME=/opt/IBM/tivoli/tiptklmV2/`
	`DB_PASSWORD=tklmdb2`
	`KEYSTORE_PASSWORD=Passw0rd`
	`TIP_USER_PWD=tipadmin`
	`BACKUP_PASSWORD=passw0rd123`
	`BACKUP_DIR=/tklmv2_backup`
	注: 在 Windows 操作系统上，在属性文件中指定路径时，请使用“/”或“\\”作为路径分隔符，如以下示例所示。
	`C:\\tklmv2_backup`
	
	或
	`C:/tklmv2_backup`
	4. 打开命令提示符并运行备份实用程序。
	
	Windows
	转至 v2 目录（请参阅步骤 b）并运行以下命令:
	backupV2.bat
	Linux 转至 v2 目录（请参阅步骤 b）并运行以下命令:
	backupV2.sh

下一步做什么

- 请复审包含备份文件的目录以确保备份文件存在。这些备份文件是在为 backup.properties 文件中的 BACKUP_DIR 指定的位置创建的。
- 请检查 backup.log 文件以找出错误或异常。backup.log 文件是在运行备份实用程序的目录中创建的。要成功执行备份操作，请确保该日志文件中没有错误或异常。
- 保留备份密码以供将来复原备份时使用。
- 请不要在备份归档中编辑文件。您尝试编辑的文件将会不可读。

复原 IBM Security Key Lifecycle Manager V2.0 (TKLM V2.0) 备份文件

通过使用图形用户界面、命令行界面、REST 界面或迁移复原脚本，您可以在安装有 IBM Security Key Lifecycle Manager V2.6 的系统上复原 IBM Security Key Lifecycle Manager V2.0（前身为 Tivoli Key Lifecycle Manager V2.0）跨平台备份文件。

开始之前

在系统上安装 IBM Security Key Lifecycle Manager V2.6。 您必须具有来自较低版本的备份文件，并确保具有创建该备份文件时所使用的密码。

注: 您的角色必须具有运行备份和复原操作的许可权。

关于此任务

您可以跨操作系统在安装了 IBM Security Key Lifecycle Manager V2.6 的系统上复原 IBM Security Key Lifecycle Manager V2.0 跨平台兼容备份文件。

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。

过程

1. 登录安装了 IBM Security Key Lifecycle Manager V2.6 的系统。
2. 将备份文件（例如，`tklm_v2.0.0.6_20150729013250-0400_migration_backup.jar`）从 V2.0 系统复制到选择的目录。
3. 使用下列任何方法复原备份文件。

图形用户界面	1. 以授权用户身份（例如，`SKLMAdmin`）登录图形用户界面。 2. 在“欢迎”页面上，单击**备份和复原**。 3. 在**备份存储库位置**字段中，指定 V2.0 备份文件所在目录的完整路径。要找到该目录，请单击**浏览**。 4. 单击**显示备份**以显示要复原的备份文件。 5. 在**备份和复原**表中，选择备份文件。 6. 单击**从备份复原**。 7. 在“复原备份”页面上，指定创建备份文件时所使用的备份密码。 8. 单击**复原备份**。 9. 重新启动 IBM Security Key Lifecycle Manager 服务器。 **注:** 您无法使用图形用户界面从 IBM Security Key Lifecycle Manager V2.0 备份复原角色、用户和组。

命令行界面	1. 转至 WAS_HOME/bin 目录。 例如:
	
	Windows
	`cd drive:\Program Files (x86)\IBM\WebSphere\AppServer\bin`
	
	Linux `cd /opt/IBM/WebSphere/AppServer/bin`
	
	2. 使用授权用户标识（例如 SKLMAdmin）启动 **wsadmin** 界面。 例如:
	
	Windows
	`wsadmin -username SKLMAdmin -password mypwd -lang jython`
	
	Linux
	`./wsadmin.sh -username SKLMAdmin -password mypwd -lang jython`
	
	3. 通过指定参数（例如备份文件名及其完整路径，以及创建备份时所使用的备份密码）来运行 **tklmBackupRunRestore** CLI 命令，如以下示例所示。
	
	`print AdminTask.tklmBackupRunRestore ('[-backupFilePath /opt/mysklmbackups/tklm_v2.0.0.6_20150729013250-0400_migration_backup.jar -password myBackupPwd]')`
	
	4. 重新启动 IBM Security Key Lifecycle Manager 服务器。
	
	注: 您无法使用命令行界面从 IBM Security Key Lifecycle Manager V2.0 备份复原角色、用户和组。

REST 界面	1. 打开 REST 客户机。
	
	2. 获取用于访问 IBM Security Key Lifecycle Manager REST 服务的唯一用户认证标识。 有关认证过程的更多信息，请参阅 REST 服务的验证流程。
	
	3. 要调用 **Backup Run Restore REST Service**，请将备份文件名及其完整路径和备份密码指定为参数来发送 HTTP POST 请求。 请将您在步骤 b 中获取的用户认证标识随请求消息一起传递，如以下示例所示。
	
	`POST https://localhost:9080/SKLM/rest/v1/ckms/restore`
	`Content-Type: application/json`
	`Accept: application/json`
	`Authorization: SKLMAuth authId=139aeh34567m`
	`Accept-Language: en`
	`{"backupFilePath":"/opt/mysklmbackups/tklm_v2.0.0.6_20150729013250-0400_migration_backup.jar backup.jar","password":"myBackupPwd"}`
	
	4. 重新启动 IBM Security Key Lifecycle Manager 服务器。
	
	注: 您无法使用 REST 界面从 IBM Security Key Lifecycle Manager V2.0 备份复原角色、用户和组。

迁移复原脚本	1. 找到 IBM Security Key Lifecycle Manager 复原实用程序。 **Windows** <*SKLM_INSTALL_HOME*>\migration\utilities\v2 缺省位置为 C:\Program Files (x86)\IBM\SKLMV26\migration\utilities\v2。 **Linux** <*SKLM_INSTALL_HOME*>/migration/utilities/v2 缺省位置为 /opt/IBM/SKLMV26/migration/utilities/v2。 2. 编辑 ekm21 文件夹中的 restore.properties 以配置属性，如以下示例所示: **注**: 在 Windows 操作系统上，用于复原操作的 restore.properties 文件不能包含首尾带有空格的属性关键字和值。 **Windows** WAS_HOME=C:\\Program Files (x86)\\IBM\\WebSphere \\AppServer BACKUP_PASSWORD=passw0rd123 DB_PASSWORD=sklmdb26 RESTORE_FILE=C:\\tklmv2_restore\\ tklm_v2.0.0.6_20150729013250-0400_migration _backup.jar WAS_USER_PWD=wasadmin RESTORE_USER_ROLES=y **Linux** WAS_HOME=/opt/IBM/WebSphere/AppServer BACKUP_PASSWORD=passw0rd123 DB_PASSWORD=sklmdb26 RESTORE_FILE=/tklmv2_restore/ tklm_v2.0.0.6_20150729013250-0400_migration _backup.jar WAS_USER_PWD=wasadmin RESTORE_USER_ROLES=y **注**: 在 Windows 系统上，在属性文件中指定路径时，请使用“/”或“\\”作为路径分隔符，如以下示例所示。 C:\\tklmv2_restore 或 C:/tklmv2_restore 3. 打开命令提示符并运行复原实用程序。 **Windows** 转至 <*SKLM_INSTALL_HOME*>\migration\utilities\v2 目录并运行以下命令: **restoreV2.bat** **Linux** 转至 <*SKLM_INSTALL_HOME*>/migration/utilities/v2 目录并运行以下命令: **restoreV2.sh** 4. 重新启动 IBM Security Key Lifecycle Manager 服务器。 **注**: 您**可以**使用迁移复原脚本从 IBM Security Key Lifecycle Manager V2.0 备份复原角色、用户和组。

下一步做什么

为 LTO 密钥组和 3592 证书配置的回滚将不会自动从较低版本的 IBM Security Key Lifecycle Manager 中复原。您必须为证书和密钥组手动设置回滚。

有关更多信息，请参阅第 152 页的『复原回滚证书和密钥组』。

备份 IBM Security Key Lifecycle Manager V2.0.1 (TKLM V2.0.1) 数据

使用 IBM Security Key Lifecycle Manager V2.6 备份实用程序来创建 IBM Security Key Lifecycle Manager V2.0.1（前身为 Tivoli Key Lifecycle Manager V2.0.1）备份文件。

开始之前

您必须在系统上安装 IBM Security Key Lifecycle Manager V2.6。 确保安装了 IBM Security Key Lifecycle Manager V2.0.1（具有最新 FP5）的系统可用。必须先配置密钥库，然后再运行备份操作。

关于此任务

您可以使用备份实用程序以独立于服务器的操作系统和目录结构的方式创建跨平台备份文件。 您可以跨操作系统在安装了 IBM Security Key Lifecycle Manager V2.6 的系统上复原这些跨平台兼容备份文件。

过程

在安装了 IBM Security Key Lifecycle Manager V2.6 和 V2.0.1 的系统上运行下列步骤。

IBM Security Key Lifecycle Manager V2.6	1. 使用用户凭证登录系统。 2. 找到备份实用程序文件夹。 **Windows** <*SKLM_INSTALL_HOME*>\migration\utilities\v2 缺省位置为 C:\Program Files (x86)\IBM\SKLMV26\migration\utilities\v2。 **Linux** <*SKLM_INSTALL_HOME*>/migration/utilities/v2 缺省位置为 /opt/IBM/SKLMV26/migration/utilities/v2。 3. 将 rt.jar 和 xml.jar 文件从 <WAS_HOME>/java/jre/lib 文件夹复制到步骤 b 中描述的备份实用程序文件夹。

IBM Security Key Lifecycle Manager V2.0.1	1. 使用用户凭证登录系统。
	2. 将 v2 文件夹从安装了 IBM Security Key Lifecycle Manager V2.6 的系统复制到您选择的本地目录。
	3. 编辑 v2 文件夹中的 backup.properties 以配置属性，如以下示例所示。您必须为除 BACKUP_DIR 特性（可选）以外的所有特性设置值。
	
	如果未指定 BACKUP_DIR 的值，那么将在运行备份实用程序的相同目录下的 backup 文件夹中创建备份文件。
	注: 在 Windows 操作系统上，用于备份操作的 backup.properties 文件不能包含首尾带有空格的属性关键字和值。
	
	Windows
	`TKLM_TIP_HOME=C:\\IBM\\tivoli\\tiptklmV2`
	`DB_PASSWORD=tklmdb2`
	`KEYSTORE_PASSWORD=Passw0rd`
	`TIP_USER_PWD=tipadmin`
	`BACKUP_PASSWORD=passw0rd123`
	`BACKUP_DIR=C:\\tklmv201_backup`
	
	Linux
	`TKLM_TIP_HOME=/opt/IBM/tivoli/tiptklmV2/`
	`DB_PASSWORD=tklmdb2`
	`KEYSTORE_PASSWORD=Passw0rd`
	`TIP_USER_PWD=tipadmin`
	`BACKUP_PASSWORD=passw0rd123`
	`BACKUP_DIR=/tklmv201_backup`
	注: 在 Windows 操作系统上，在属性文件中指定路径时，请使用“/”或“\\”作为路径分隔符，如以下示例所示。
	`C:\\tklmv201_backup`
	
	或
	`C:/tklmv201_backup`
	4. 打开命令提示符并运行备份实用程序。
	
	Windows
	转至 v2 目录（请参阅步骤 b）并运行以下命令:
	backupV2.bat
	
	Linux 转至 v2 目录（请参阅步骤 b）并运行以下命令:
	backupV2.sh

下一步做什么

- 请复审包含备份文件的目录以确保备份文件存在。这些备份文件是在为 backup.properties 文件中的 BACKUP_DIR 指定的位置创建的。
- 请检查 backup.log 文件以找出错误或异常。backup.log 文件是在运行备份实用程序的目录中创建的。要成功执行备份操作，请确保该日志文件中没有错误或异常。
- 保留备份密码以供将来复原备份时使用。
- 请不要在备份归档中编辑文件。您尝试编辑的文件将会不可读。

复原 IBM Security Key Lifecycle Manager V2.0.1 (TKLM V2.0.1) 备份文件

通过使用图形用户界面、命令行界面、REST 界面或迁移复原脚本，您可以在安装有 IBM Security Key Lifecycle Manager V2.6 的系统上复原 IBM Security Key Lifecycle Manager V2.0.1（前身为 Tivoli Key Lifecycle Manager V2.0.1）跨平台备份文件。

开始之前

在系统上安装 IBM Security Key Lifecycle Manager V2.6。 您必须具有来自较低版本的备份文件，并确保具有创建该备份文件时所使用的密码。

注: 您的角色必须具有运行备份和复原操作的许可权。

关于此任务

您可以跨操作系统在安装了 IBM Security Key Lifecycle Manager V2.6 的系统上复原 IBM Security Key Lifecycle Manager V2.0.1 跨平台兼容备份文件。

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。

过程

1. 登录安装了 IBM Security Key Lifecycle Manager V2.6 的系统。
2. 将备份文件（例如，`tklm_v2.0.1.5_20150729013250-0400_migration_backup.jar`）从 V2.0.1 系统复制到选择的目录。
3. 使用下列任何方法复原备份文件。

图形用户界面	1. 以授权用户身份（例如，`SKLMAdmin`）登录图形用户界面。 2. 在“欢迎”页面上，单击**备份和复原**。 3. 在**备份存储库位置**字段中，指定 V2.0.1 备份文件所在目录的完整路径。要找到该目录，请单击**浏览**。 4. 单击**显示备份**以显示要复原的备份文件。 5. 在**备份和复原**表中，选择备份文件。 6. 单击**从备份复原**。 7. 在“复原备份”页面上，指定创建备份文件时所使用的备份密码。 8. 单击**复原备份**。 9. 重新启动 IBM Security Key Lifecycle Manager 服务器。 **注:** 您无法使用图形用户界面从 IBM Security Key Lifecycle Manager V2.0.1 备份复原角色、用户和组。

命令行界面	1. 转至 WAS_HOME/bin 目录。 例如:
	
	Windows
	`cd drive:\Program Files (x86)\IBM\WebSphere\AppServer\bin`
	
	Linux `cd /opt/IBM/WebSphere/AppServer/bin`
	
	2. 使用授权用户标识（例如 SKLMAdmin）启动 **wsadmin** 界面。 例如:
	
	Windows
	`wsadmin -username SKLMAdmin -password mypwd -lang jython`
	
	Linux
	`./wsadmin.sh -username SKLMAdmin -password mypwd -lang jython`
	
	3. 通过指定参数（例如备份文件名及其完整路径，以及创建备份时所使用的备份密码）来运行 **tklmBackupRunRestore** CLI 命令，如以下示例所示。
	
	`print AdminTask.tklmBackupRunRestore ('[-backupFilePath /opt/mysklmbackups/tklm_v2.0.1.5_20150729013250-0400_migration_backup.jar -password myBackupPwd]')`
	
	4. 重新启动 IBM Security Key Lifecycle Manager 服务器。
	
	注: 您无法使用命令行界面从 IBM Security Key Lifecycle Manager V2.0.1 备份复原角色、用户和组。

REST 界面	1. 打开 REST 客户机。
	
	2. 获取用于访问 IBM Security Key Lifecycle Manager REST 服务的唯一用户认证标识。 有关认证过程的更多信息，请参阅 REST 服务的验证流程。
	
	3. 要调用 **Backup Run Restore REST Service**，请将备份文件名及其完整路径和备份密码指定为参数来发送 HTTP POST 请求。 请将您在步骤 b 中获取的用户认证标识随请求消息一起传递，如以下示例所示。
	
	`POST https://localhost:9080/SKLM/rest/v1/ckms/restore`
	`Content-Type: application/json`
	`Accept: application/json`
	`Authorization: SKLMAuth authId=139aeh34567m`
	`Accept-Language: en`
	`{"backupFilePath":"/opt/mysklmbackups/tklm_v2.0.1.5_20150729013250-0400_migration_backup.jar backup.jar","password":"myBackupPwd"}`
	
	4. 重新启动 IBM Security Key Lifecycle Manager 服务器。
	
	注: 您无法使用 REST 界面从 IBM Security Key Lifecycle Manager V2.0.1 备份复原角色、用户和组。

迁移复原脚本	1. 找到 IBM Security Key Lifecycle Manager 复原实用程序。 **Windows** <*SKLM_INSTALL_HOME*>\migration\utilities\v2 缺省位置为 C:\Program Files (x86)\IBM\SKLMV26\migration\utilities\v2。 **Linux** <*SKLM_INSTALL_HOME*>/migration/utilities/v2 缺省位置为 /opt/IBM/SKLMV26/migration/utilities/v2。 2. 编辑 ekm21 文件夹中的 restore.properties 以配置属性，如以下示例所示: **注**: 在 Windows 操作系统上，用于复原操作的 restore.properties 文件不能包含首尾带有空格的属性关键字和值。 **Windows** WAS_HOME=C:\\Program Files (x86)\\IBM\\WebSphere\\AppServer BACKUP_PASSWORD=passw0rd123 DB_PASSWORD=sklmdb26 RESTORE_FILE=C:\\tklmv201_restore\\tklm_v2.0.1.5_20150729013250-0400_migration_backup.jar WAS_USER_PWD=wasadmin RESTORE_USER_ROLES=y **Linux** WAS_HOME=/opt/IBM/WebSphere/AppServer BACKUP_PASSWORD=passw0rd123 DB_PASSWORD=sklmdb26 RESTORE_FILE=/tklmv201_restore/tklm_v2.0.1.5_20150729013250-0400_migration_backup.jar WAS_USER_PWD=wasadmin RESTORE_USER_ROLES=y **注**: 在 Windows 操作系统上，在属性文件中指定路径时，请使用“/”或“\\”作为路径分隔符，如以下示例所示。 C:\\tklmv201_restore 或 C:/tklmv201_restore 3. 打开命令提示符并运行复原实用程序。 **Windows** 转至 <*SKLM_INSTALL_HOME*>\migration\utilities\v2 目录并运行以下命令: **restoreV2.bat** **Linux** 转至 <*SKLM_INSTALL_HOME*>/migration/utilities/v2 目录并运行以下命令: **restoreV2.sh** 4. 重新启动 IBM Security Key Lifecycle Manager 服务器。 **注**: 您**可以**使用迁移复原脚本从 IBM Security Key Lifecycle Manager V2.0.1 备份复原角色、用户和组。

下一步做什么

为 LTO 密钥组和 3592 证书配置的回滚将不会自动从较低版本的 IBM Security Key Lifecycle Manager 中复原。您必须为证书和密钥组手动设置回滚。

有关更多信息，请参阅第 152 页的『复原回滚证书和密钥组』。

备份 IBM Security Key Lifecycle Manager V2.5 数据

使用 IBM Security Key Lifecycle Manager V2.6 备份实用程序来创建 IBM Security Key Lifecycle Manager V2.5 跨平台备份文件。

开始之前

您必须在系统上安装 IBM Security Key Lifecycle Manager V2.6。 确保安装了 IBM Security Key Lifecycle Manager V2.5（具有最新 FP3）的系统可用。

关于此任务

您可以使用备份实用程序以独立于服务器的操作系统和目录结构的方式创建跨平台备份文件。 您可以跨操作系统在安装了 IBM Security Key Lifecycle Manager V2.6 的系统上复原这些跨平台兼容备份文件。

过程

在安装了 IBM Security Key Lifecycle Manager V2.6 和 V2.5 的系统上运行下列步骤。

IBM Security Key Lifecycle Manager V2.6	1. 使用用户凭证登录系统。 2. 找到备份实用程序文件夹。 **Windows** <*SKLM_INSTALL_HOME*>\migration\utilities\sklmv25 缺省位置为 C:\Program Files (x86)\IBM\SKLMV26\migration\utilities\sklmv25。 **Linux** <*SKLM_INSTALL_HOME*>/migration/utilities/sklmv25 缺省位置为 /opt/IBM/SKLMV26/migration/utilities/sklmv25。 3. 将 rt.jar 和 xml.jar 文件从 <WAS_HOME>/java/jre/lib 文件夹复制到步骤 b 中描述的备份实用程序文件夹。

IBM Security Key Lifecycle Manager V2.5	1. 使用用户凭证登录系统。
	2. 将 sklmv25 文件夹从安装了 IBM Security Key Lifecycle Manager V2.6 的系统复制到您选择的本地目录。
	3. 编辑 sklmv25 文件夹中的 backup.properties 以配置特性，如以下示例所示。 您必须为除 BACKUP_DIR 特性（可选）以外的所有特性设置值。
	
	如果未指定 BACKUP_DIR 的值，那么将在运行备份实用程序的相同目录下的 backup 文件夹中创建备份文件。
	注: 在 Windows 操作系统上，用于备份操作的 backup.properties 文件不能包含首尾带有空格的属性关键字和值。
	Windows
	`WAS_HOME=C:\\Program Files (x86)\\IBM\\WebSphere \\AppServer`
	`BACKUP_PASSWORD=passw0rd123`
	`DB_PASSWORD=sklmdb2`
	`WAS_USER_PWD=wasadmin`
	`BACKUP_DIR=C:\\sklmv25_backup`
	Linux
	`WAS_HOME=/opt/IBM/WebSphere/AppServer`
	`BACKUP_PASSWORD=passw0rd123`
	`DB_PASSWORD=sklmdb2`
	`WAS_USER_PWD=wasadmin`
	`BACKUP_DIR=/sklmv25_backup`
	注: 在 Windows 操作系统上，在属性文件中指定路径时，请使用“/”或“\\”作为路径分隔符，如以下示例所示。
	`C:\\sklmv25_backup`
	
	或
	`C:/sklmv25_backup`
	4. 打开命令提示符并运行备份实用程序。
	Windows
	转至 sklmv25 目录（请参阅步骤 b）并运行以下命令:
	backupV25.bat
	Linux 转至 sklmv25 目录（请参阅步骤 b）并运行以下命令:
	backupV25.sh

下一步做什么

- 请复审包含备份文件的目录以确保备份文件存在。这些备份文件是在为 backup.properties 文件中的 BACKUP_DIR 指定的位置创建的。
- 请检查 backup.log 文件以找出错误或异常。backup.log 文件是在运行备份实用程序的目录中创建的。要成功执行备份操作，请确保该日志文件中没有错误或异常。
- 保留备份密码以供将来复原备份时使用。
- 请不要在备份归档中编辑文件。您尝试编辑的文件将会不可读。

复原 IBM Security Key Lifecycle Manager V2.5 备份文件

通过使用图形用户界面、命令行界面、REST 界面或迁移复原脚本，您可以在安装有 IBM Security Key Lifecycle Manager V2.6 的系统上复原 IBM Security Key Lifecycle Manager V2.5 跨平台备份文件。

开始之前

在系统上安装 IBM Security Key Lifecycle Manager V2.6。 您必须具有来自较低版本的备份文件，并确保具有创建该备份文件时所使用的密码。

注: 您的角色必须具有运行备份和复原操作的许可权。

关于此任务

您可以跨操作系统在安装了 IBM Security Key Lifecycle Manager V2.6 的系统上复原 IBM Security Key Lifecycle Manager V2.5 跨平台兼容备份文件。

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。

过程

1. 登录安装了 IBM Security Key Lifecycle Manager V2.6 的系统。
2. 将备份文件（例如，`sklm_v2.5.0.3_20150729013250-0400_migration_backup.jar`）从 V2.5 系统复制到选择的目录。
3. 使用下列任何方法复原备份文件。

图形用户界面	1. 以授权用户身份（例如，`SKLMAdmin`）登录图形用户界面。 2. 在“欢迎”页面上，单击**备份和复原**。 3. 在**备份存储库位置**字段中，指定 V2.5 备份文件所在目录的完整路径。要找到该目录，请单击**浏览**。 4. 单击**显示备份**以显示要复原的备份文件。 5. 在**备份和复原**表中，选择备份文件。 6. 单击**从备份复原**。 7. 在“复原备份”页面上，指定创建备份文件时所使用的备份密码。 8. 单击**复原备份**。 9. 重新启动 IBM Security Key Lifecycle Manager 服务器。 **注:** 您无法使用图形用户界面从 IBM Security Key Lifecycle Manager V2.5 备份复原角色、用户和组。

命令行界面	1. 转至 WAS_HOME/bin 目录。 例如:
	Windows
	`cd drive:\Program Files (x86)\IBM\WebSphere\AppServer\bin`
	Linux `cd /opt/IBM/WebSphere/AppServer/bin`
	2. 使用授权用户标识（例如 SKLMAdmin）启动 **wsadmin** 界面。 例如:
	Windows
	`wsadmin -username SKLMAdmin -password mypwd -lang jython`
	Linux
	`./wsadmin.sh -username SKLMAdmin -password mypwd -lang jython`
	3. 通过指定参数（例如备份文件名及其完整路径，以及创建备份时所使用的备份密码）来运行 **tklmBackupRunRestore** CLI 命令，如以下示例所示。
	`print AdminTask.tklmBackupRunRestore ('[-backupFilePath /opt/mysklmbackups/sklm_v2.5.0.3_20150729013250-0400_migration_backup.jar -password myBackupPwd]')`
	4. 重新启动 IBM Security Key Lifecycle Manager 服务器。
	注: 您无法使用命令行界面从 IBM Security Key Lifecycle Manager V2.5 备份复原角色、用户和组。

REST 界面	1. 打开 REST 客户机。
	2. 获取用于访问 IBM Security Key Lifecycle Manager REST 服务的唯一用户认证标识。 有关认证过程的更多信息，请参阅 REST 服务的验证流程。
	3. 要调用 **Backup Run Restore REST Service**，请将备份文件名及其完整路径和备份密码指定为参数来发送 HTTP POST 请求。 请将您在步骤 b 中获取的用户认证标识随请求消息一起传递，如以下示例所示。
	`POST https://localhost:9080/SKLM/rest/v1/ckms/restore`
	`Content-Type: application/json`
	`Accept: application/json`
	`Authorization: SKLMAuth authId=139aeh34567m`
	`Accept-Language: en`
	`{"backupFilePath":"/opt/mysklmbackups/sklm_v2.5.0.3_20150729013250-0400_migration_backup.jar backup.jar","password":"myBackupPwd"}`
	4. 重新启动 IBM Security Key Lifecycle Manager 服务器。
	注: 您无法使用 REST 界面从 IBM Security Key Lifecycle Manager V2.5 备份复原角色、用户和组。

迁移复原脚本	1. 找到 IBM Security Key Lifecycle Manager 复原实用程序。 **Windows** <*SKLM_INSTALL_HOME*>\migration\utilities\sklmv25 缺省位置为 C:\Program Files (x86)\IBM\SKLMV26\migration\utilities\sklmv25。 **Linux** <*SKLM_INSTALL_HOME*>/migration/utilities/sklmv25 缺省位置为 /opt/IBM/SKLMV26/migration/utilities/sklmv25。 2. 编辑 sklmv25 文件夹中的 restore.properties 以配置属性，如以下示例所示。 **注**: 在 Windows 操作系统上，用于复原操作的 restore.properties 文件不能包含首尾带有空格的属性关键字和值。 **Windows** WAS_HOME=C:\\Program Files (x86)\\IBM\\WebSphere \\AppServer BACKUP_PASSWORD=passw0rd123 DB_PASSWORD=sklmdb26 RESTORE_FILE=C:\\sklmv25_restore\\ sklm_v2.5.0.3_20150729013250-0400_migration_backup.jar WAS_USER_PWD=wasadmin **Linux** WAS_HOME=/opt/IBM/WebSphere/AppServer BACKUP_PASSWORD=passw0rd123 DB_PASSWORD=sklmdb26 RESTORE_FILE=/sklmv25_restore/ sklm_v2.5.0.3_20150729013250-0400_migration_backup.jar WAS_USER_PWD=wasadmin **注**: 在 Windows 操作系统上，在属性文件中指定路径时，请使用“/”或“\\”作为路径分隔符，如以下示例所示。 C:\\sklmv25_restore 或 C:/sklmv25_restore 3. 打开命令提示符并运行复原实用程序。 **Windows** 转至 <*SKLM_INSTALL_HOME*>\migration\utilities\sklmv25 目录并运行以下命令: **restoreV25.bat** **Linux** 转至 <*SKLM_INSTALL_HOME*>/migration/utilities/sklmv25 目录并运行以下命令: **restoreV25.sh** 4. 重新启动 IBM Security Key Lifecycle Manager 服务器。 **注**: 您**可以**使用迁移复原脚本从 IBM Security Key Lifecycle Manager V2.5 备份复原角色、用户和组。

复原回滚证书和密钥组

不会自动从先前版本的 IBM Security Key Lifecycle Manager 复原针对 LTO 密钥组和 3592 证书配置的回滚。要在 V2.6 中手动指定这些回滚，请使用复原过程中在 <WAS_HOME>/products/sklm/config 目录中创建的回滚文件 scheduledTasks.txt。

过程

1. 打开命令提示符。
2. 转至以下目录。

   Windows

   <*SKLM_INSTALL_HOME*>\migration\bin

   Linux <*SKLM_INSTALL_HOME*>/migration/bin
3. 运行以下命令。

   Windows

   运行 **recreatetask.bat** 实用程序。

   ```
   recreatetask.bat <WAS_HOME> <SKLMADMIN_USER> <SKLMADMIN_PASSWD>
   <SKLM_HOME>\config\scheduledTasks.txt <Logfile> <SKLM_INSTALL_HOME>
   ```

   Linux 运行 **recreatetask.sh** 实用程序。

   ```
   recreatetask.sh <WAS_HOME> <SKLMADMIN_USER> <SKLMADMIN_PASSWD>
   <SKLM_HOME>/config/scheduledTasks.txt <Logfile> <SKLM_INSTALL_HOME>
   ```

   其中，<Logfile> 是写入日志信息的日志文件名，例如:

   ```
   C:\Program Files (x86)\IBM\WebSphere\AppServer\products\sklm\logs\
   rolloverlogs.txt
   ```

   <SKLMADMIN_USER> 和 <SKLMADMIN_PASSWD> 是 IBM Security Key Lifecycle Manager 管理员用户标识密码。

   有关 <WAS_HOME>, <SKLM_HOME> 和 <SKLM_INSTALL_HOME> 的定义，请参阅*HOME* 和其他目录变量的定义。

预防密钥丢失

为了防止关键任务设备和密钥的加密数据丢失，请始终至少维护 IBM Security Key Lifecycle Manager 的两个实例。 请确保其中一个实例是相同设备和密钥的副本。您可以提供两个以上的冗余实例。

IBM Security Key Lifecycle Manager 针对 DS5000 存储服务器提供以下支持: 在 IBM Security Key Lifecycle Manager 中注册新的 DS5000 设备时，自动生成密钥。

不要对 DS5000 设备系列使用设置 1（自动接受）。 此设置允许在备份数据之前生成密钥并将密钥提供给 DS5000 存储服务器。对于所有其他设备系列，请备份提供的所有新密钥。

请从服务器中除去备份文件，并将其存储在安全的位置。例如，将备份文件复制到 CD/DVD 并锁定在安全的位置。

注: 请勿将文件复制到依赖于此产品的已加密存储器。 这可能会导致备份由于产品不可用而不可用。

IBM Security Key Lifecycle Manager 还提供了下列密钥丢失选项:

backup.keycert.before.serving
在 SKLMConfig.properties 文件中设置此特性可以防止在备份密钥之前提供新密钥。

自动备份脚本
使用 autobackup.bat 脚本可以自动备份文件。 如果 **backup.keycert.before.serving** 特性的值在 SKLMConfig.properties 文件中设置为 true 或者不存在，那么 IBM Security Key Lifecycle Manager 不会提供未备份的密钥或证书。

配置自动备份脚本

您可以使用自动备份脚本来备份文件。

关于此任务

如果 **backup.keycert.before.serving** 特性的值在 SKLMConfig.properties 文件中设置为 true 或者不存在，那么 IBM Security Key Lifecycle Manager 不会提供未备份的密钥或证书。

自动备份脚本通过呼叫下列命令来启动备份:

- **klmBackupIsRunning**，用于检查备份操作是否处于运行状态。
- **tklmBackupIsNeeded** 或 **Backup Is Needed REST Service**，用于确定是否存在新密钥或证书（但尚未运行备份）。
- **tklmBackupRun** 或 **Backup Run REST Service**，用于运行备份任务。

开始之前，请确定用于加密备份文件中的数据的密码。

过程

1. 在以下目录中查找该脚本:

   Windows
   drive:\Program Files (x86)\IBM\SKLMV25\bin\samples\autobackup.bat

   Linux 和 AIX®
   path/IBM/SKLMV25/bin/samples/autobackup.sh

2. 在 autobackup.bat 或 autobackup.sh 文件顶部，找到您要更改的行:

```
rem ########################################################
rem #
rem #       EDIT THE PARAMETER VALUE IN THIS SECTION
rem #
rem tiphome : required, home directory of Tivoli Integrated Portal
rem username : required, username of the Tivoli Key Lifecycle Manager
rem user with klmBackup permission
rem password : required, password for the Tivoli Key Lifecycle Manager
rem user to log in
rem backuppw : required, password used for backup operation
rem backupdes : optional, description of the Tivoli Key Lifecycle
rem Manager backup
rem backupdir : optional, full path to the directory, where the
rem backup jar file is stored
rem backupDBdir : optional, full path to the directory, where the
rem database backup is stored
Set tiphome=
```

```
Set username=
Set password=
Set backuppw=
Set backupdes=
Set backupdir=
Set backupDBdir=
rem ######################################################
```

3. 更改该脚本中的必需行:

tiphome

必需。 WebSphere Application Server 主目录。

例如:

```
Set tiphome=C:/Progra~2/IBM/WebSphere/AppServer
```

username

必需。 这是具有 **klmBackup** 许可权的用户标识。请使用此用户标识登录 IBM Security Key Lifecycle Manager。 此用户标识还可以是现有用户标识, 例如 SKLMAdmin。

password

必需。 这是具有 **klmBackup** 许可权的用户标识的密码。

backuppw

必需。 这是用于加密备份文件中的数据的密码。 值可以介于 6 个字符与 32 个字符之间。

您可以对每个备份文件使用不同的密码。 复原文件时, 您必须能够提供备份任务期间用于加密该文件中的数据的密码。

backupdes

可选。 这是关于备份文件的用途或用法的更多信息。

backupdir

可选。 这是一个目录, 用于存储 JAR 文件以及 IBM Security Key Lifecycle Manager 的备份数据。 请指定此目录的完整路径。

如果备份成功, 那么您指定的值将作为 **tklm.backup.dir** 属性的值写入 SKLMConfig.properties 文件中。

注:

- 如果没有为此参数指定值并且之前未成功运行备份, 那么缺省值为 *SKLM_HOME*/backup 目录。
- 如果您指定了不建议使用的相对路径（例如, mybackupdir）, 那么将在 *WAS_HOME*/profiles/KLMProfile/*mybackupdir* 目录中创建备份。
- IBM Security Key Lifecycle Manager 可在操作系统的超级用户有权编写备份文件的任何目录中创建备份文件。 超级用户在 Windows 系统上为 Administrator, 在 Linux 或 AIX 上为 root。
- 不要在包含数据库备份的同一目录中创建备份文件。

backupDBdir

可选。 包含 IBM Security Key Lifecycle Manager 临时备份数据的 IBM Security Key Lifecycle Manager 数据库中的目录。 如果未指定任何参数, 那么所使用的目录为 datastore.properties 文件中 **tklm.backup.db2.dir**

属性的值。该文件位于 *WAS_HOME*\products\sklm\config 目录或临时系统目录（如果 **tklm.backup.db2.dir** 属性指定的目录不存在）中。

4. 运行该脚本:
   - 立即运行。 输入:

     Windows

     drive:\Program Files (x86)\IBM\SKLMV25\bin\samples\autobackup.bat

     Linux 和 AIX

     path/IBM/SKLMV25/bin/samples/autobackup.sh
   - 根据安排运行。

     根据操作系统，在 cron 作业中或通过使用 Windows 计划程序启用该脚本。

KMIP 对象管理

IBM Security Key Lifecycle Manager 服务器支持与客户机设备进行密钥管理互操作性协议 (KMIP) 通信。您可以使用 IBM Security Key Lifecycle Manager 提供的一组操作来创建和管理加密对象。

您可以使用 IBM Security Key Lifecycle Manager 图形用户界面来完成下列加密对象管理活动:

- 向服务器注册客户机设备
- 针对注册的客户机设备创建和配置加密对象
- 查看注册的客户机设备的对象
- 通过添加更多对象或关联新证书修改客户机设备信息
- 从服务器中删除客户机设备和关联的对象
- 搜索服务器所管理的对象

注册符合 KMIP 的客户机设备

您必须向 IBM Security Key Lifecycle Manager 服务器注册符合 KMIP 的客户机设备，然后客户机才能与服务器进行密钥管理操作通信。

关于此任务

使用**客户机仪表板**来管理客户机设备及其对象。您可以使用仪表板来查看、注册、修改和删除客户机设备以及关联的加密对象。

将证书与客户机设备相关联以实现与服务器的安全通信。在注册客户机之前，确定以下哪个客户机设备证书将用于通信:

- 未在使用的现有客户机设备证书。
- 接受暂挂客户机设备证书。
- 导入客户机设备证书。

您还可以注册客户机设备而不使用关联的证书。在从暂挂证书列表选择证书之前，您可以稍后进行关联。单击仪表板上的**暂挂客户机注册请求**链接以选择证书。如果接受，那么会将证书导入数据库并标记为受信任。然后，可以使用证书以实现在客户机

设备和 IBM Security Key Lifecycle Manager 之间的安全通信。您还可以在修改客户机设备信息时关联证书。

过程

1. 使用凭证登到录图形用户界面。
2. 在“欢迎”页面上，单击**客户机和组**。
3. 在**客户机仪表板**上，单击**创建**。
4. 在**客户机名称**字段中，指定客户机的名称。
5. 选择客户机证书以实现与服务器的安全通信。

无	将向服务器注册客户机设备而不使用关联的客户机通信证书。
使用未在使用的现有客户机证书	使用数据库中任何其他客户机设备未在使用的现有客户机证书。从下拉列表中选择证书。
接受暂挂客户机证书	在从客户机设备推送到服务器但尚未接受的暂挂证书列表中，选择一个证书以用于与服务器的通信。在注册客户机设备时，使用以下步骤以接受客户机通信证书并将其标记为受信任: 1. 在**证书名称**字段中指定证书的名称。 2. 从下拉列表中选择证书。
导入客户机证书	将客户机设备证书导入 IBM Security Key Lifecycle Manager 以实现与注册的客户机的安全通信。 1. 在**证书名称**字段中指定证书的名称。 2. 单击**浏览**以选择文件并导入。

6. 单击**注册客户机**。

下一步做什么

将加密对象与注册的客户机相关联。请参阅『针对客户机设备创建加密对象』。

针对客户机设备创建加密对象

针对向 IBM Security Key Lifecycle Manager 注册的符合 KMIP 的客户机设备创建和配置加密对象。

关于此任务

使用**客户机仪表板**来管理客户机设备及其对象。您可以使用仪表板来查看、注册、修改和删除客户机设备以及关联的加密对象。

使用“对象与客户机”页面来为注册的客户机设备创建和配置以下对象:

- 对称密钥
- 密钥对

过程

1. 使用凭证登到录图形用户界面。
2. 在“欢迎”页面上，单击**客户机和组**。

3. 在**客户机仪表板**上，单击**创建**。
4. 使用**注册客户机**选项卡来创建和注册客户机设备。请参阅第 155 页的『注册符合 KMIP 的客户机设备』。
5. 在**添加对象**选项卡中，针对客户机设备添加和配置对象:

无	指示客户机设备未与任何对象相关联。
对称密钥	使用以下配置设置创建对称密钥: • 客户机设备的对称密钥的数量。 • 对象用于数据加密和解密的密码算法，例如，AES 或 3DES。 • 对称密钥对象的位长度。 • 密钥的前缀。您必须使用字母字符为密钥指定一个三字符值。 • 使用以下对象定义要执行的加密功能的加密用法掩码: Encrypt、Decrypt、Encrypt Decrypt、Sign、Sign Verify、Verify、Wrap、Unwrap 或 Wrap Unwrap。
密钥对	使用以下配置设置创建非对称密钥对对象: • 客户机设备的密钥对对象的数量。 • 对象用于数据加密和解密的密码算法，例如，RSA 或 DSA。 • 密钥的前缀。您必须使用字母字符为密钥指定一个三字符值。 • 使用以下对象定义要执行的加密功能的加密用法掩码: Encrypt、Decrypt、Encrypt Decrypt、Sign、Sign Verify、Verify、Wrap、Unwrap 或 Wrap Unwrap。

6. 单击**保存并退出**。要保存并添加更多对象，请单击**保存并添加更多对象**。

修改客户机设备信息

使用“修改客户机”页面来修改客户机设备信息以适合您的不断更改的需求。您可以添加更多对象并将证书与向 IBM Security Key Lifecycle Manager 注册的客户机设备相关联。

关于此任务

使用“客户机仪表板”页面来管理客户机设备及其对象。您可以使用仪表板来查看、注册、修改和删除客户机设备以及关联的加密对象。

您的角色必须具有执行修改操作的许可权。

过程

1. 使用凭证登到录图形用户界面。
2. 在“欢迎”页面上，单击**客户机和组**。
3. 从**客户机名称**列选择一个客户机设备。
4. 单击**修改**。
5. 或者，右键单击客户机名称，然后选择**修改**或双击客户机条目。

6. 在“修改客户机”对话框上，添加更多对象或将证书关联到客户机设备以适合您的需求。
7. 单击**保存并退出**。要保存并添加更多对象，请单击**保存并添加更多对象**。

删除客户机设备信息

您可以从 IBM Security Key Lifecycle Manager 数据库中删除客户机设备及其对象（如果不再需要）。

关于此任务

使用“客户机仪表板”页面来管理客户机设备及其对象。您可以使用仪表板来查看、注册、修改和删除客户机设备以及关联的加密对象。

您的角色必须具有执行删除操作的许可权。

开始之前，请确保存在 IBM Security Key Lifecycle Manager 数据库的当前备份。

过程

1. 使用凭证登到录图形用户界面。
2. 在“欢迎”页面上，单击**客户机和组**。
3. 从**客户机名称**列选择一个客户机设备。
4. 单击**删除**。
5. 或者，右键单击客户机名称，然后选择**删除**或双击客户机条目。
6. 在“确认”对话框上，阅读确认消息，然后删除客户机设备。单击**确定**。这将从 IBM Security Key Lifecycle Manager 数据库除去客户机设备及其对象。

IBM Security Key Lifecycle Manager 中硬件安全模块的使用

您必须将参数添加到 IBM Security Key Lifecycle Manager 配置文件来定义硬件安全模块 (HSM)。

您可以使用 HSM 来存储用于保护 IBM Security Key Lifecycle Manager 数据库中存储的所有密码的主密钥。您可以对具有现有数据的安装启用此功能，也可以对 IBM Security Key Lifecycle Manager 的新安装启用此功能。

IBM Security Key Lifecycle Manager 支持下列加密卡:

- SafeNet Luna SA 4.5
- SafeNet Luna SA 5.0
- nCipher nShield Connect 1500
- IBM 4765 PCIe Cryptographic Coprocessor

注:

- 仅当 IBM Security Key Lifecycle Manager 中未定义密钥库时，您才能使用 SafeNet Luna SA 4.5、SafeNet Luna SA 5.0 和 IBM 4765 PCIe Cryptographic Coprocessor。 这些卡不允许从外部导入密钥。
- 仅对于下列 PKCS#11 加密操作，才支持 IBM 4765 PCIe Cryptographic Coprocessor:

– 将 AES 128 位或 256 位软件密钥转换为 AES 硬件 (PKCS#11) 密钥
– 生成 AES 128 位或 256 位密钥
– 使用 AES 密钥和 AES/ECB/NoPadding 密码对数据进行加密和解密
– 在 PKCS11IMPLKS (PKCS#11) 密钥库中存储和检索 AES 密钥

您可以使用下列配置参数来定义 HSM:

- **pkcs11.pin**
- **pkcs11.pin.obfuscated**
- **pkcs11.config**

有关 HSM 配置参数详细信息，请参阅 IBM Security Key Lifecycle Manager 文档中的参考主题。

样本 HSM 配置文件

SafeNet Luna SA 4.5 和 SafeNet Luna SA 5.0 的样本 HSM 配置文件

```
#SafeNet Luna
name = TKLM
library=C:/Program Files/LunaSA/cryptoki.dll
description=Luna sample config


slotListIndex = 0

attributes (*, CKO_PRIVATE_KEY, *) = {
   CKA_SENSITIVE = true
}
attributes (GENERATE, CKO_SECRET_KEY, *) = {
   CKA_SENSITIVE = true
   CKA_ENCRYPT = true
   CKA_DECRYPT = true
}
attributes (IMPORT, CKO_PUBLIC_KEY, *) = {
   CKA_VERIFY = true
}
```

注: 对于 **name** 参数，必须始终指定值 TKLM。

nCipher nShield Connect 1500 的样本 HSM 配置文件

```
# nCipher nShield, nForce 4000 - Generation 2 cards
name = TKLM
library=C:/nCipher/nfast/cknfast.dll
description= nCipher sample config for TKLM

slotListIndex=1

attributes(*, CKO_SECRET_KEY, *) = {
  CKA_ENCRYPT=true
  CKA_DECRYPT=true
  CKA_SENSITIVE=true
  CKA_TOKEN=true
}

attributes(*, CKO_PRIVATE_KEY, *) = {
  CKA_SIGN=true
  CKA_SENSITIVE=false
#  CKA_DERIVE=true
# when using KeyAgreement CKA_DERIVE  should
# set to true and CKA_SIGN should set to false
}
```

```
attributes(GENERATE, CKO_PUBLIC_KEY, *) = {
  CKA_VERIFY=true
}

attributes(GENERATE, CKO_PRIVATE_KEY, CKK_RSA) = {
  CKA_DECRYPT=true
  CKA_UNWRAP=true
  CKA_EXTRACTABLE=true
}

attributes(*, CKO_PUBLIC_KEY, CKK_RSA) = {
  CKA_ENCRYPT=true
  CKA_WRAP=true
  CKA_VERIFY=true
}
attributes(IMPORT, CKO_PRIVATE_KEY, CKK_RSA) = {
  CKA_EXTRACTABLE=true
  CKA_DECRYPT=true
  CKA_UNWRAP=true
  CKA_DERIVE=true
}
```

注: 对于 **name** 参数，必须始终指定值 TKLM。

配置 HSM 参数

必须使用 **pkcs11.pin**、**pkcs11.pin.obfuscated** 和 **pkcs11.config** 配置参数来定义 HSM。

过程

1. 按照 HSM 制造商提供的指示信息设置和配置 HSM。
2. 将 **pkcs11.pin** 和 **pkcs11.config** 参数添加到 IBM Security Key Lifecycle Manager 配置文件。 您可以使用以下 CLI 命令或 REST 界面来添加参数:

   命令行界面

   ```
   print AdminTask.tklmConfigUpdateEntry('[-name pkcs11.pin -value
   <hsm pin>]')

   print AdminTask.tklmConfigUpdateEntry('[-name pkcs11.config -value
   <hsm config file>]')
   ```

   REST 界面

   ```
   PUT https://localhost:9080/SKLM/rest/v1/configProperties
   Content-Type: application/json
   Accept: application/json
   Authorization: SKLMAuth authId=139aeh34567m
   Accept-Language: en
   { "pkcs11.pin" : "<hsm pin>"}

   PUT https://localhost:9080/SKLM/rest/v1/configProperties
   Content-Type: application/json
   Accept: application/json
   Authorization: SKLMAuth authId=139aeh34567m
   Accept-Language: en
   { "pkcs11.config" : "<hsm config file>"}
   ```

   注: *<hsm pin>* 是 HSM 的 PIN 码。 *<hsm config file>* 是 HSM 配置文件的完整路径和文件名。 例如: C:\Program Files (x86)\IBM\WebSphere\AppServer\sklm\config\LunaSA.cfg
3. 重新启动 IBM Security Key Lifecycle Manager。

针对使用 HSM 的配置需求

按照制造商提供的指示信息安装 HSM 之后，您必须使用 HSM 客户机提供的工具来验证 HSM 安装。 仅支持 32 位 HSM 客户机。

- 要验证 HSM 安装，请执行下列步骤:
  - 使用 **ckdemo** 或 **kSafe** 创建一个对称密钥。

    kSafe 是 nCipher nShield Connect 1500 卡随附的工具。 **ckdemo** 随 SafeNet Luna SA 4.5 卡和 SafeNet Luna SA 5.0 卡一起提供。
  - 列出该密钥。
  - 删除该密钥。
- nCipher nShield Connect 1500 卡要求 cknfastrc 文件包含以下配置:

  ```
  CKNFAST_OVERRIDE_SECURITY_ASSURANCES=import;
  ```

  注: 如果 cknfastrc 文件在您的系统上不存在，请创建并配置此文件。 将此文件保存到 HSM 文档中提及的位置。
- 如果主密钥位于 HSM 中，那么 IBM Security Key Lifecycle Manager 备份或复制功能不会备份该主密钥。 要备份 HSM，请按照 HSM 文档中的指示信息执行操作。 您必须备份 HSM，这是因为任何主密钥丢失都可能会导致 IBM Security Key Lifecycle Manager 中的所有密钥丢失。
- 仅当 IBM Security Key Lifecycle Manager 中未定义密钥库时，才需要使用 SafeNet Luna SA 4.5 卡和 SafeNet Luna SA 5.0 卡。 这些卡不允许从外部导入密钥。
- 要克隆 IBM Security Key Lifecycle Manager，不同系统上的 HSM 必须使用同一主密钥。 如果您使用的是已连接网络的 HSM，请确保所有 HSM 客户机都指向 HSM 网络上的同一区域。

LDAP 配置

您可以配置任何 LDAP 存储库（例如 IBM Security Directory Server 或 Microsoft Active Directory）中的 IBM Security Key Lifecycle Manager 用户，使其访问 IBM Security Key Lifecycle Manager 服务器。

必须将 LDAP 用户存储库添加到 WebSphere Application Server 的联合存储库并进行配置。 IBM Security Key Lifecycle Manager 使用应用程序组对 IBM Security Key Lifecycle Manager 功能强制实施基于角色的授权。为使 IBM Security Key Lifecycle Manager 用户在 LDAP 用户存储库中运行 IBM Security Key Lifecycle Manager 功能，该用户必须是特定 IBM Security Key Lifecycle Manager 应用程序组的成员。

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

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

创建基于数据库的存储库并将 IBM Security Key Lifecycle Manager 应用程序组添加到此存储库后，即可使 LDAP 存储库中的用户成为基于数据库的存储库中 IBM Security Key Lifecycle Manager 应用程序组的成员。 然后，用户可以登录到 IBM Security Key Lifecycle Manager 应用程序并运行 IBM Security Key Lifecycle Manager 应用程序功能。

LDAP 集成的先决条件

您可能需要将以下数据复原到运行 LDAP 配置步骤之前的状态:

- IBM Security Key Lifecycle Manager 的 WebSphere Application Server 配置数据
- IBM Security Key Lifecycle Manager 应用程序数据

要备份数据，请运行下列步骤:

1. 在 WebSphere Application Server 中备份 IBM Security Key Lifecycle Manager 概要文件 (KLMProfile):
   a. 在 WAS_HOME/bin 目录中，停止 WebSphere Application Server 应用程序。
   b. 运行以下命令:

      Windows

      ```
      <WAS_HOME>\bin\manageProfiles.bat -backupProfile -profileName
      KLMProfile -backupFile <path to a file>
      ```

      ```
      C:\Program Files (x86)\IBM\WebSphere\AppServer\bin\manageProfiles.bat
      backupProfile -profileName KLMProfile -backupFile
      :\SKLM_WAS_ProfileBackup
      ```

      Linux

      ```
      <WAS_HOME>/bin/manageprofiles.sh -backupProfile -profileName
      KLMProfile -backupFile <path to a file>
      ```

      ```
      /opt/IBM/WebSphere/AppServer/bin/manageprofiles.sh -backupProfile
      profileName KLMProfile -backupFile /root/SKLM_WAS_ProfileBackup
      ```

   c. 启动 WebSphere Application Server。
2. 备份 IBM Security Key Lifecycle Manager 应用程序数据。

   使用图形用户界面、命令行界面或 REST 界面来备份 IBM Security Key Lifecycle Manager 的关键文件。

有关 **manageprofiles** 命令的更多信息，请参阅 http://www-01.ibm.com/support/knowledgecenter/SSEQTP_8.5.5/com.ibm.websphere.base.doc/ae/rxml_manageprofiles.html。

将 LDAP 与 IBM Security Key Lifecycle Manager 集成

您可以配置任何 LDAP 存储库（如 IBM Security Directory Server 或 Microsoft Active Directory）中的 IBM Security Key Lifecycle Manager 用户，以访问 IBM Security Key Lifecycle Manager 服务器并调用服务器 API 和 CLI。

开始之前

有关先决条件信息，请参阅 第 161 页的『LDAP 配置』

过程

1. 将 LDAP 存储库添加到联合存储库。 有关指示信息，请参阅『将 LDAP 存储库添加到联合存储库』。
2. 从 WebSphere Integrated Solutions Console 创建 jndi 名称为 jdbc/wimXADS 的数据源。有关指示信息，请参阅第 164 页的『从 WebSphere Integrated Solutions Console 创建数据源』。
3. 重新启动 WebSphere Application Server。
4. 将 db2jcc.jar and db2jcc_license_cu.jar 从 DB2SKLMV25 文件夹复制到 <WAS_HOME>/lib 文件夹。

   DB2SKLMV25 路径:

   Windows

   C:\Program Files (x86)\IBM\DB2SKLMV25\java

   Linux /opt/IBM/DB2SKLMV25/java

   通常，<*WAS_HOME*> 变量的缺省定义如下:

   Windows

   C:\Program Files (x86)\IBM\WebSphere\AppServer

   Linux /opt/IBM/WebSphere/AppServer
5. 创建基于数据库的存储库来存放所有 IBM Security Key Lifecycle Manager 应用程序组。 有关指示信息，请参阅第 166 页的『创建基于数据库的存储库』。
6. 从 WebSphere Integrated Solutions Console 添加“安全角色到用户/组映射”，并将管理员角色映射到 klmGUICLIAccessGroup。有关指示信息，请参阅第 167 页的『从 WebSphere Integrated Solutions Console 添加安全用户角色』。
7. 重新启动 WebSphere Application Server。
8. 将 LDAP 用户添加到 IBM Security Key Lifecycle Manager 应用程序组。 有关指示信息，请参阅第 168 页的『将 LDAP 用户添加到 IBM Security Key Lifecycle Manager 应用程序组』。
9. 执行 IBM Security Key Lifecycle Manager 应用程序备份。 基于数据库的存储库中的数据也会进行备份。

下一步做什么

配置 LDAP 之后，您必须运行后续任务。有关详细信息，请参阅第 168 页的『用于支持 LDAP 集成的 LDAP 配置后任务』。

将 LDAP 存储库添加到联合存储库

您必须将 LDAP 存储库添加到联合存储库以配置 LDAP 存储库，例如联合存储库中的 IBM Security Directory Server 或 Microsoft Active Directory。

关于此任务

有关在联合存储库配置中配置 LDAP 设置的更多信息，请参阅 http://www-01.ibm.com/support/knowledgecenter/api/redirect/wasinfo/v8r5/topic/com.ibm.websphere.base.doc/ae/twim_ldap_settings.html。

过程

1. 以 wasadmin 用户身份登录 WebSphere Integrated Solutions Console (https://localhost:9083/ ibm/console/logon.jsp)。
2. 在导航栏中，单击**安全性 > 全局安全性**。
3. 在“用户帐户存储库”下，从**可用的领域定义**下拉列表中选择**联合存储库**。
4. 单击**配置**。
5. 在**全局安全性 > 联合存储库**页面中，单击**添加存储库（LDAP、定制等）**。
6. 在**全局安全性 > 联合存储库 > 存储库引用**页面中，从**新存储库**下拉列表中选择**LDAP 存储库**。
7. 在**全局安全性 > 联合存储库 > 存储库引用 > 新建**页面中，根据您的需求指定 LDAP 存储库的名称和其他详细信息。
8. 单击**确定**。
9. 单击**保存**以保存配置。
10. 在**全局安全性 > 联合存储库 > 存储库引用**页面中，指定**联合存储库中基本（或父级）条目的唯一专有名称**值。
11. 单击**确定**。
12. 在**全局安全性 > 联合存储库**页面中，选择指向您创建的 LDAP 存储库的链接。
13. 在**全局安全性 > 联合存储库 > <LDAP 存储库名称>** 页面中，在“其他特性”下，选择“联合存储库实体类型到 LDAP 对象类映射”链接。

    在**全局安全性 > 联合存储库 > <LDAP 存储库名称> > 联合存储库实体类型到 LDAP 对象类映射**页面中，确保列出的每种实体类型都映射到正确的对象类。 请根据您的需求修改值。
14. 在**全局安全性 > 联合存储库**页面中，选择指向您创建的 LDAP 存储库的链接。 在“其他特性”下，选择**组属性定义**。
15. 在**全局安全性 > 联合存储库 > <LDAP 存储库名称> > 组属性定义**页面中，在“其他特性”下，选择**成员属性**。
16. 在**全局安全性 > 联合存储库 > <LDAP 存储库名称> > 组属性定义 > 成员属性**页面中，确保 uniqueMember 成员属性映射到正确的对象类。 如果此属性不存在，请创建属性并将其映射到正确的对象类。

下一步做什么

从 WebSphere Integrated Solutions Console 创建数据源。

从 WebSphere Integrated Solutions Console 创建数据源

您必须为基于数据库的存储库创建数据源来存放 IBM Security Key Lifecycle Manager 应用程序组。 基于数据库的存储库使用在 IBM Security Key Lifecycle Manager 应用程序数据库中创建的表。

过程

1. 以 wasadmin 用户身份从 WebSphere Integrated Solutions Console (https://localhost:9083/ ibm/console/logon.jsp) 登录以“创建数据源”。
2. 在导航栏中，单击**资源 > JDBC > 数据源**。
3. 从**选择**下拉列表中选择 **Node=SKLMNode, Server-server1**。

4. 单击**新建**。
5. 在“输入基本数据源信息”对话框中，指定值。

选项	描述
数据源名称	WIM Data Source
JNDI 名称	jdbc/wimXADS **注**: 不要更改此值。

6. 单击**下一步**。
7. 在“选择 JDBC 提供程序”对话框中，选择**选择现有 JDBC 提供程序 > SKLM XA DB2 JDBC 提供程序**。
8. 单击**下一步**。
9. 在“输入数据源的特定于数据库的特性”对话框中，指定下列值:

选项	描述
数据库名称	SKLMDB26 或 IBM Security Key Lifecycle Manager 安装期间使用的任何名称。
服务器名称	localhost
端口号	50020 或 IBM Security Key Lifecycle Manager 安装期间用于 DB2 的任何端口号。

10. 单击**下一步**。
11. 在“设置安全性别名”对话框中，从下拉列表中选择值:

选项	描述
用于 XA 复原的认证别名	sklm_db
组件管理的认证别名	sklm_db
映射配置别名	无
容器管理的认证别名	sklm_db

12. 单击**下一步**。
13. 在“摘要”页面中单击**完成**。
14. 在“数据源”页面中，单击**保存**以保存配置。
15. 在数据源列表中选择 **WIM 数据源**。
16. 单击**测试连接**以确保连接测试成功。
17. 在数据源列表中选择 **WIM 数据源**链接。
18. 在**数据源 > WIM 数据源**页面中，单击**定制特性**链接。
19. 浏览至页面以找到指向 **webSphereDefaultIsolationLevel** 特性的链接，然后单击此链接。
20. 在**数据源 > WIM 数据源 > 定制特性 > webSphereDefaultIsolationLevel** 页面中，在“常规特性”部分下的**值**字段中输入值 2。
21. 单击**确定**。
22. 单击**保存**以保存配置。

下一步做什么

重新启动 WebSphere Application Server。

创建基于数据库的存储库

创建基于数据库的存储库来存放所有 IBM Security Key Lifecycle Manager 应用程序组，以及从基于文件的存储库中除去所有 IBM Security Key Lifecycle Manager 应用程序组。您必须将 IBM Security Key Lifecycle Manager 应用程序组添加到基于数据库的存储库，并使用 LDAP 存储库更新 WebSphere Application Server 联合存储库。

过程

1. 转至 <WAS_HOME>/bin 文件夹。

   注: 所有 .py Python 脚本都存在于 <*SKLM_HOME*>/bin/LDAPIntegration 目录中。通常为 <*SKLM_HOME*> 路径。

   Windows

   C:\Program Files (x86)\IBM\SKLMV26

   Linux /opt/IBM/SKLMV26

2. 运行以下命令:

   ```
   wsadmin.bat -user <wasadmin user> -password <wasadmin passwd> -lang jython -f
   <SKLM_HOME>\bin\LDAPIntegration\createDBRepos.py <WAS_HOME> <SKLM_DBNAME>
   <SKLM_DBUSER> <SKLM_DBUSERPASSWD> <SKLM_DBPORT#>
   ```

   注释: 在 Linux 平台上，请使用 **wsadmin.sh**，而不是 **wsadmin.bat**

   在 IBM Security Key Lifecycle Manager 安装期间，如果您使用缺省值，

   ```
   SKLM_DBNAME = SKLMDB26
   SKLM_DBUSER = sklmdb26
   SKLM_DBPORT# = 50020
   ```

   SKLM_DBUSERPASSWD 是您在安装期间指定的 IBM Security Key Lifecycle Manager 数据库密码。

3. 运行以下命令。

   ```
   wsadmin.bat -user <wasadmin user> -password <wasadmin passwd> -lang jython -f
   <SKLM_HOME>\bin\LDAPIntegration\removeGroupsFromDefRepos.py
   ```

4. 从 WebSphere Integrated Solutions Console，修改安全角色到用户/组映射以除去到 klmGUICLIAccessGroup 的管理员角色映射。

   a. 登录 WebSphere Integrated Solutions Console (https://localhost:9083/ ibm/console/logon.jsp)。

   b. 在导航栏中，单击**应用程序** > **应用程序类型** > **应用程序类型** > **WebSphere 企业应用程序**。

   c. 单击 **sklm_kms** 链接。

   d. 在**企业应用程序** > **sklm_kms** 页面中，在“详细信息特性”部分下，单击**安全角色到用户/组映射**链接。

   e. 在**企业应用程序** > **sklm_kms** > **安全角色到用户/组映射**页面中，选择**管理员**角色。

   f. 单击**映射组**。

g. 从列表中选择 **klmGUICLIAccessGroup**，然后单击向左箭头按钮以便从列表中除去 **klmGUICLIAccessGroup**。

h. 单击**确定**。

i. 单击**保存**链接以保存配置。

5. 重新启动 WebSphere Application Server。
6. 运行以下命令。

```
wsadmin.bat -user <wasadmin user> -password <wasadmin passwd> -lang jython
-f <SKLM_HOME>\bin\LDAPIntegration\addGroupsToDBRepos.py
```

7. 运行以下命令。

```
wsadmin.bat -user <wasadmin user> -password <wasadmin passwd> -lang jython
-f <SKLM_HOME>\bin\LDAPIntegration\updateLDAPReposConfig.py <LDAPRepos Name
- name used earlier when LDAP repos was created>
```

下一步做什么

添加“安全角色到用户/组映射”，并将管理员角色映射到 klmGUICLIAccessGroup。

从 WebSphere Integrated Solutions Console 添加安全用户角色

您必须将安全角色添加到用户或组映射，并将管理员角色映射到 klmGUICLIAccessGroup，以便将 IBM Security Key Lifecycle Manager 与 LDAP 用户存储库集成。

关于此任务

过程

1. 以 wasadmin 用户身份登录 WebSphere Integrated Solutions Console (https://localhost:9083/ ibm/console/logon.jsp)。
2. 在导航栏中，单击**应用程序** > **应用程序类型** > **应用程序类型** > **WebSphere 企业应用程序**。
3. 单击 **sklm_kms** 链接。
4. 在**企业应用程序** > **sklm_kms** 页面中，在“详细信息特性”部分下，单击**安全角色到用户/组映射**链接。
5. 在**企业应用程序** > **sklm_kms** > **安全角色到用户/组映射**页面中，选择**管理员**角色。
6. 单击**映射组**。
7. 在**企业应用程序** > **sklm_kms** > **安全角色到用户/组映射** > **映射用户/组**页面中，执行下列操作:

   a. 在“搜索并选择组”部分下的**搜索字符串**文本框中，输入 klmGUICLIAccessGroup。

   b. 单击**搜索**。

   c. 从列表中选择 klmGUICLIAccessGroup，然后单击向右箭头按钮。

   klmGUICLIAccessGroup 将添加到**已选中**列表。

   d. 单击**确定**。

   e. 在**企业应用程序** > **sklm_kms** > **安全角色到用户/组映射**页面中，单击**确定**。
8. 单击**保存**链接以保存配置信息。

下一步做什么

重新启动 WebSphere Application Server。

将 LDAP 用户添加到 IBM Security Key Lifecycle Manager 应用程序组

您必须将 LDAP 用户添加到 IBM Security Key Lifecycle Manager 应用程序组，以便将 IBM Security Key Lifecycle Manager 与 LDAP 用户存储库集成。

过程

1. 转至 `<WAS_HOME>/bin` 文件夹。

   注: 所有 `.py` Python 脚本都存在于 `<SKLM_HOME>/bin/LDAPIntegration` 目录中。通常为 *<SKLM_HOME>* 路径。

   Windows

   ```
   C:\Program Files (x86)\IBM\SKLMV25
   ```

   Linux `/opt/IBM/SKLMV25`

2. 运行以下命令:

   ```
   wsadmin.bat -user <wasadmin user> -password <waasadmin passwd> -lang jython -f
   addLDAPUserToGroup.py <user uniqueName> <group name>
   ```

   注释: 在 Linux 平台上，请使用 **wsadmin.sh**，而不是 **wsadmin.bat**

   用户唯一名称是 LDAP 注册表中的“唯一名称”要素。 例如:

   ```
   uid=001,c=in,ou=bluepages,o=ibm.com
   ```

   对于需要 IBM Security Key Lifecycle Manager 管理员访问权的 LDAP 用户，必须使该用户成为 `klmGUICLIAccessGroup` 和 `klmSecurityOfficerGroup` 的成员。运行以下命令:

   ```
   wsadmin.bat -user <wasadmin user> -password <wasadmin passwd> -lang jython -f
   <SKLM_HOME>\bin\LDAPIntegration\addLDAPUserToGroup.py <user uniqueName>
   klmGUICLIAccessGroup
   ```

下一步做什么

执行 IBM Security Key Lifecycle Manager 应用程序备份。

用于支持 LDAP 集成的 LDAP 配置后任务

完成 LDAP 配置之后，您可能需要完成额外的任务，以确保 IBM Security Key Lifecycle Manager 与 LDAP 用户存储库的集成成功。

完成 LDAP 配置之后的重要说明

1. 完成 LDAP 配置之后，基于文件的缺省用户存储库中先前存在的 `sklmadmin` 用户无法访问 IBM Security Key Lifecycle Manager 应用程序。
2. 完成 LDAP 配置之后，您必须使用 **wsadmin** 命令创建组并分配 IBM Security Key Lifecycle Manager 角色。您无法使用 WebSphere Integrated Solutions Console。 请运行下列步骤以添加组并向该组分配角色:
   a. 转至 *<WAS_HOME>*`/bin`。
   b. 使用以下命令登录 `wsadmin`:

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

c. 要创建组并分配角色，请运行以下命令:

```
AdminTask.createGroup<'[-cn <groupname> -parent "o=sklmrepdb.ibm"]'>
AdminTask.mapGroupsToAdminRole<'[-roleName <role> -groupids
<groupname>]'>
```

3. 完成 LDAP 配置之后，您可能希望将 WebSphere Application Server 中的 IBM Security Key Lifecycle Manager 配置复原到执行 LDAP 配置之前的状态。 要复原此配置，请运行下列步骤:

   a. 停止 WebSphere Application Server。

   b. 停止与 WebSphere Application Server 相关的进程（如果有）。

   c. 复原执行 LDAP 配置之前所执行的 WebSphere Application Server 概要文件配置:

      1) 手动删除 *<WAS_HOME>*/profiles/KLMProfile 中的 KLMProfile 文件夹。

      2) 运行 **manageProfiles** 命令的 **-validateAndUpdateRegistry** 选项。

         Windows

         <WAS_HOME>\bin\manageProfiles.bat -validateAndUpdateRegistry

         例如: C:\Program Files (x86)\IBM\WebSphere\AppServer\bin\manageProfiles.bat -validateAndUpdateRegistry

         Linux *<WAS_HOME>*/bin/manageprofiles.sh -validateAndUpdateRegistry

         例如: /opt/IBM/WebSphere/AppServer/bin/manageprofiles.sh -validateAndUpdateRegistry

      3) 复原概要文件:

         Windows

         <WAS_HOME>\bin\manageProfiles.bat -restoreProfile -backupFile *<path to profile backup file>*

         例如: C:\Program Files (x86)\IBM\WebSphere\AppServer\bin\manageProfiles.bat -restoreProfile -backupFile C:\SKLM_WAS_ProfileBackup

         Linux *<WAS_HOME>*/bin/manageprofiles.sh -restoreProfile -backupFile *<path to profile backup file>*

         例如: /opt/IBM/WebSphere/AppServer/bin/manageprofiles.sh -restoreProfile -backupFile /root/SKLM_WAS_ProfileBackup

         有关 **manageProfiles** 命令的信息，请参阅 http://www-01.ibm.com/support/knowledgecenter/SSEQTP_8.5.5/com.ibm.websphere.base.doc/ae/rxml_manageprofiles.html。

      4) 启动 WebSphere Application Server。

      5) 复原进行 LDAP 配置之前所执行的 IBM Security Key Lifecycle Manager 备份（如果需要）。

4. 完成 LDAP 配置之后，除非执行了**完成 LDAP 配置之后的重要说明**部分中的步骤 3，否则您不得复原在进行 LDAP 配置之前执行的 IBM Security Key Lifecycle Manager 应用程序备份。

5. 完成 LDAP 配置之后，将在基于数据库的存储库的 IBM Security Key Lifecycle Manager 数据库中创建表。 IBM Security Key Lifecycle Manager 组将存储在这些表中。如果针对 IBM Security Key Lifecycle Manager 服务器配置了复制功能，并且对已配置的克隆执行了复制，那么基于数据库的存储库中的组也会在克隆上进行复制。这是因为基于数据库的存储库的数据库表也会复制到克隆。
6. 如果启用了配置为与 LDAP 存储库进行集成的 IBM Security Key Lifecycle Manager 服务器（主服务器）以及复制功能，那么对已配置的克隆（未在这些克隆中配置 LDAP）执行复制时，您可以在克隆上配置 LDAP，也可以不执行此配置。 如果必须在克隆上执行 LDAP 配置，请对该克隆运行下列步骤:
   a. 将 db2jcc.jar,db2jcc4.jar 和 db2jcc_license_cu.jar 从 DB2SKLMV25 文件夹复制到 *<WAS_HOME>*/lib 文件夹。

      通常，*<WAS_HOME>* 变量的缺省定义如下:

      Windows

      C:\Program Files (x86)\IBM\WebSphere\AppServer

      Linux /opt/IBM/WebSphere/AppServer
   b. 转至 *<WAS_HOME>*/bin。
      1) 使用以下命令登录 wsadmin:

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

      2) 运行以下命令:

```
AdminTask.deleteIdMgrDBTables<'[-schemaLocation "<WAS_HOME>/etc/wim/set
up" -databaseType db2 -dbURL "jdbc:db2://localhost:<sklmbport>/
<sklmdbname>" -dbDriver com.ibm.db2.jcc.DB2Driver -dbAdminId
<slmdb2adminuser> -dbAdminPassword <sklmb2adminuserPasswd>
-reportSqlError true]'>
```

   c. 按照在主 IBM Security Key Lifecycle Manager 服务器上完成的过程执行操作以设置/配置 LDAP 集成。要了解集成步骤，请参阅第 162 页的『将 LDAP 与 IBM Security Key Lifecycle Manager 集成』。
7. 完成已进行 LDAP 集成配置的 IBM Security Key Lifecycle Manager 服务器与未进行 LDAP 集成配置的克隆之间的复制之后，如果您在克隆上意外地运行常规 LDAP 集成配置，那么第 162 页的『将 LDAP 与 IBM Security Key Lifecycle Manager 集成』中的步骤 5 会失败。您必须运行下列步骤:
   a. 转至 *<WAS_HOME>*/bin。
      1) 登录 wsadmin:

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

      2) 运行以下命令:

```
AdminTask.deleteIdMgrDBTables<'[-schemaLocation "<WAS_HOME>/etc/wim/set
up" -databaseType db2 -dbURL "jdbc:db2://localhost:<sklmbport>/
<sklmdbname>" -dbDriver com.ibm.db2.jcc.DB2Driver -dbAdminId
<slmdb2adminuser> -dbAdminPassword <sklmb2adminuserPasswd>
-reportSqlError true]'>
```

   b. 运行第 162 页的『将 LDAP 与 IBM Security Key Lifecycle Manager 集成』中的步骤 5 - 9。

导出 SSL/KMIP 服务器证书

您必须以客户机设备使用的编码格式将 IBM Security Key Lifecycle Manager SSL/KMIP 服务器证书导出到文件。客户机设备导入此证书以实现与服务器的安全通信。

关于此任务

使用“导出证书”对话框、**tklmCertExport** 命令或 **Certificate Export REST Service** 将 IBM Security Key Lifecycle Manager SSL/KMIP 服务器证书导出到编码格式的文件。

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。这将显示“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. 导出证书。
   - 图形用户界面:
     a. 单击**高级配置** > **服务器证书**.
     b. 在**证书**表中，选择相应的证书。
     c. 单击**导出**。
     d. 在“导出证书”对话框中，将在**文件名**字段中填充在步骤 b 中选择的证书。
     e. 在**文件位置**字段中，输入证书文件的完整路径，或者单击**浏览**以指定位置。
     f. 为证书选择 **BASE64**（缺省格式）或 **DER**（特异编码规则）编码文件格式。
     g. 单击**导出证书**。
   - 命令行界面:

     输入 tklmCertExport 以导出证书文件。 例如:

     ```
     print AdminTask.tklmCertExport
      ('[-uuid CERTIFICATE-61f8e7ca-62aa-47d5-a915–8adbfbdca9de
       -format DER -fileName d:\\mypath\\mycertfilename.der]')
     ```

     有关 **tklmCertExport** 命令的更多信息，请参阅 tklmCertExport。
   - REST 界面:

a. 获取用于访问 IBM Security Key Lifecycle Manager REST 服务的唯一用户认证标识。 有关认证过程的更多信息，请参阅 REST 服务的验证流程。

b. 要启动 **Certificate Export REST Service**，请发送 HTTP PUT 请求。请将您在步骤 a 中获取的用户认证标识随请求消息一起传递，如以下示例所示。

```
PUT https://localhost:9080/SKLM/rest/v1/certificates/export
Content-Type: application/json
Accept: application/json
Authorization: SKLMAuth userAuthId=139aeh34567m
{"uuid":"CERTIFICATE-61f8e7ca-62aa-47d5-a915–8adbfbdca9de",
"format":"DER",
"fileName":"/mycertificate.der"}
```

有关 **Certificate Export REST Service** 的更多信息，请参阅 Certificate Export REST Service。

3. 成功指示符会根据界面的不同而不同:
   - 图形用户界面:

     已将证书文件保存在您指定的位置。
   - 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。

在 IBM Security Key Lifecycle Manager 服务器之间复制证书

您可以使用命令行界面或 REST 界面在 IBM Security Key Lifecycle Manager 服务器之间复制证书以及公用密钥和专用密钥。

关于此任务

使用下列 CLI 命令或 REST 界面来复制证书:

- **tklmKeyExport** 和 **tklmKeyImport**
- **Key Export REST Service** 和 **Key Import REST Service**

过程

1. 在证书所在的 IBM Security Key Lifecycle Manager 服务器上，运行 **tklmKeyExport** 命令或发送 **Key Export REST Service** HTTP 请求。

```
print AdminTask.tklmKeyExport ('[-alias sklmCertificate
   -fileName myprivatekeys -keyStoreName defaultKeyStore
    -type privatekey -password mypassword]')
```

```
PUT https://localhost:9080/SKLM/rest/v1/keys/export
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth authId=139aeh34567m
{"alias":"sklmCertificate","fileName":"myprivatekeys","type":"privatekey",
"password":"mypassword"}
```

2. 将 mycert.p12 文件复制到目标 IBM Security Key Lifecycle Manager 服务器。
3. 运行 **tklmKeyImport** 命令或发送 **Key Import REST Service** HTTP 请求。

```
print AdminTask.tklmKeyImport ('-type privatekey -fileName c:\\mycert.p12
-keyStoreName "Tivoli Key Lifecycle Manager Keystore" -usage 3592 -password
<password>]')
```

```
POST https://localhost:9080/SKLM/rest/v1/keys/import
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth authId=139aeh34567m
{"type":"privatekey","fileName":"mycert.p12","usage":"3592","password":
"mypassword","newAlias":"mykey"}
```

结果

这些命令通过使用证书来复制专用密钥和公用密钥以读写磁带。

更改浏览器界面的语言

您可以更改浏览器界面上显示的语言。

关于此任务

请先更改浏览器的语言首选项，然后再登录 IBM Security Key Lifecycle Manager。要更改浏览器的语言首选项，请完成下列步骤:

- Internet Explorer
  1. 选择**工具 > Internet 选项**。
  2. 在**常规**选项卡上，单击**语言**。
  3. 选择语言，然后单击**确定**。 您可能需要先添加语言，并将该语言上移到语言列表的顶部。
  4. 重新启动浏览器。
- Firefox
  1. 选择**工具 > 选项**。 然后，单击“内容”图标。
  2. 在“内容”选项卡上的“语言”部分中，单击**选择**。
  3. 选择语言，然后单击**确定**。 您可能需要先添加语言，并将该语言上移到语言列表的顶部。
  4. 在“选项”对话框中，再次单击**确定**。
  5. 重新启动浏览器。

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

[数字]

C

D

E

G

H

I

J

K

L

P

S

T

U

V

W