Administración

Contenido

Administración

La administración es el conjunto de tareas con las que se prepara y supervisa el entorno de IBM Security Key Lifecycle Manager.

Las actividades de administración incluyen las siguientes tareas:

- Configuración y mantenimiento del sistema IBM Security Key Lifecycle Manager
- Configuración de los sistemas maestro y clon para la réplica
- Administración de los grupos, usuarios y roles
- Administración de dispositivos, objetos KMIP y Hardware Security Module
- Ejecución de tareas operativas, como copia de seguridad de los datos, restauración de los datos y exportación e importación de grupos de dispositivos
- Otras tareas administrativas

Antes de empezar, familiarícese con los conceptos y la terminología que se mencionan en esta sección. Consulte las secciones sobre visión general, planificación e instalación para ver información relacionada.

Especificación de certificados SSL o KMIP

Puede especificar el certificado autofirmado para ser utilizado como certificado de comunicación del servidor. Como alternativa, puede crear solicitudes de certificados y enviar manualmente la solicitud a una entidad emisora de certificados para firmar. Por ejemplo, puede utilizar certificados para añadir protección a la comunicación entre IBM Security Key Lifecycle Manager y una biblioteca de cintas. Los archivos de la solicitud de certificado generada residen en el directorio *<SKLM_HOME>*. Por ejemplo, una solicitud de certificado generada puede ser un archivo como `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\171029122037-sslcert001.csr`.

Acerca de esta tarea

Puede utilizar la página SSL/KMIP para el servicio de claves para especificar el tipo de certificados que utiliza IBM Security Key Lifecycle Manager. O bien, puede utilizar cualquiera de los siguientes mandatos de CLI o las interfaces REST:

- **tklmCertCreate** o **tklmCertGenRequest**
- **Servicio REST Generar solicitud de certificado** o el **Servicio REST Crear certificado**

Your role must have a permission to the configure action to create an SSL or KMIP certificate.

Antes de empezar, determine:

- Si puede utilizar los certificados autofirmados durante una fase en el proyecto como, por ejemplo, una fase de prueba.
- El intervalo de tiempo necesario para recibir un certificado emitido por una CA después de enviar una solicitud. Debe enviar manualmente una solicitud de certificado a la entidad emisora de certificados.
- Si el sitio requiere certificados de socio para su uso con business partners, proveedores o a efectos de recuperación tras desastre.
- El valor habitual en días para un intervalo de validez de certificado.

Procedimiento

1. Vaya al directorio o la página apropiada.
   - Interfaz gráfica de usuario:

     Inicie una sesión en la interfaz gráfica de usuario. Pulse **IBM Security Key Lifecycle Manager** > **Configuración** > **SSL/KMIP**.
   - Command-line interface
     a. Go to the <*WAS_HOME*>/bin directory. For example,

        Windows
        ```
        cd drive:\Program Files\IBM\WebSphere\AppServer\bin
        ```

        Linux
        ```
        cd /opt/IBM/WebSphere/AppServer/bin
        ```

     b. Start the **wsadmin** interface by using an authorized user ID, such as SKLMAdmin. For example,

        Windows
        ```
        wsadmin.bat -username SKLMAdmin -password mypwd -lang jython
        ```

        Linux
        ```
        ./wsadmin.sh -username SKLMAdmin -password mypwd -lang jython
        ```
   - Interfaz REST:
     – Abra un cliente REST.
2. Cree uno o varios certificados o solicitudes de certificado:
   - Interfaz gráfica de usuario

     Seleccione si desea generar un certificado autofirmado, o solicitar un certificado de un proveedor de terceros. También existe la opción de que el certificado utilice un certificado existente del almacén de claves. Complete los campos necesarios y opcionales y, a continuación, pulse **Aceptar**.
   - Interfaz de línea de mandatos

     Escriba el mandato **tklmCertCreate** en una línea. Por ejemplo, para crear un certificado autofirmado, escriba:
     ```
     print AdminTask.tklmCertCreate ('[-type selfsigned
      -alias sklmSSLCertificate -cn sklmssl -ou accounting -o myCompanyName
        -country US -keyStoreName defaultKeyStore
         -usage SSLSERVER -validity 999]')
     ```

     De manera alternativa, puede solicitar un certificado desde una entidad emisora de certificados. Por ejemplo, escriba:
     ```
     print AdminTask.tklmCertGenRequest('[-alias sklmSSLCertificate1
      -cn sklm -ou sales -o myCompanyName -locality myLocation
       -country US -validity 999 -keyStoreName defaultKeyStore
        -fileName mySSLCertRequest1.crt -usage SSLSERVER]')
     ```
   - Interfaz REST
     a. Obtenga un identificador de autenticación de usuario exclusivo para acceder a los servicios REST de IBM Security Key Lifecycle Manager. Para obtener más información sobre el proceso de autenticación, consulte Proceso de autenticación de los servicios REST.
     b. Para ejecutar **Servicio REST Generar solicitud de certificado**, envíe la solicitud HTTP POST. Pase el identificador de autenticación de usuario que ha obtenido en el Paso a junto con el mensaje de solicitud, como se muestra en el ejemplo siguiente.
        ```
        POST https://localhost:<puerto>/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 "  }
```

Enviar la siguiente solicitud HTTP para un certificado desde una entidad emisora de certificados:

```
POST https://localhost:<puerto>/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"}
```

Si selecciona una solicitud de certificado para un proveedor de terceros, se generará el archivo de solicitud de certificado en el formato `.csr` en el directorio `<SKLM_HOME>`, por ejemplo, `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\171029122037-sslcert001.csr`. Envíe manualmente la solicitud de certificado a una entidad emisora de certificados. A continuación, debe importar el certificado firmado a IBM Security Key Lifecycle Manager. Para ver los pasos sobre cómo enviar e importar el certificado, consulte Caso de ejemplo: solicitud de un certificado de terceros.

3. El indicador de éxito varía dependiendo de la interfaz.
   - Graphical user interface

     On the Success page, under Next Steps, click a related task that you want to carry out. If you create a self-signed certificate, you might restart the server and create a backup to ensure that you can restore this data.
   - Command-line interface

     A completion message indicates success.
   - REST interface

     The status code `200 OK` indicates success.

Qué hacer a continuación

Vaya a la página de Bienvenida y configure los tipos de unidad y las claves o certificados que su organización necesita.

Especificación de niveles de información de auditoría

En función de sus necesidades, puede cambiar el valor predeterminado que utiliza IBM Security Key Lifecycle Manager para recopilar información de auditoría.

Acerca de esta tarea

Puede utilizar la página Auditoría para cambiar los niveles (Bajo, Medio o Alto) de la información de auditoría que se graba en el registro de auditoría. O bien, puede utilizar los siguientes mandatos de CLI o las interfaces REST para enumerar o cambiar la propiedad **`Audit.event.types`** en el archivo `SKLMConfig.properties`:

- **`tklmConfigGetEntry`** y **`tklmConfigUpdateEntry`**
- **`Servicio REST Obtener propiedad de configuración única`** y **`Servicio REST Actualizar propiedad de configuración`**

Your role must have a permission to the configure action.

Procedimiento

1. Vaya a la página o el directorio correspondiente:
   - Interfaz gráfica de usuario:

     Inicie una sesión en la interfaz gráfica de usuario. Pulse **IBM Security Key Lifecycle Manager** > **Configuración** > **Auditoría y depuración**.
   - Command-line interface
     a. Go to the <*WAS_HOME*>/bin directory. For example,

        Windows
        ```
        cd drive:\Program Files\IBM\WebSphere\AppServer\bin
        ```

        Linux
        ```
        cd /opt/IBM/WebSphere/AppServer/bin
        ```

     b. Start the **wsadmin** interface by using an authorized user ID, such as SKLMAdmin. For example,

        Windows
        ```
        wsadmin.bat -username SKLMAdmin -password mypwd -lang jython
        ```

        Linux
        ```
        ./wsadmin.sh -username SKLMAdmin -password mypwd -lang jython
        ```
   - Interfaz REST:
     – Abra un cliente REST.
2. Cambie el valor del nivel de información de auditoría:
   - En la interfaz gráfica de usuario, seleccione un valor bajo, medio o alto para el valor Auditoría y, a continuación, pulse **Aceptar**.

     Bajo Almacena los registros de auditoría mínimos.

     La opción **Bajo** define los siguientes valores de propiedad del archivo SKLMConfig.properties:

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

     Medio (predeterminado)
     Almacena una cantidad intermedia de registros de auditoría.

     La opción **Medio** define los siguientes valores de propiedad del archivo SKLMConfig.properties:

     – `Audit.event.types = runtime, authorization, authorization_terminate, resource_management, key_management`
     – `Audit.event.outcome = success, failure`

     Alto Almacena la cantidad máxima de registros de auditoría.

     La opción **Alto** define los siguientes valores de propiedad del archivo SKLMConfig.properties:

     – `Audit.event.types = all`
     – `Audit.event.outcome = success, failure`
   - Interfaz de línea de mandatos:
     a. Escriba el mandato **tklmConfigGetEntry** en una línea para obtener el valor actual de la propiedad de destino en el archivo SKLMConfig.properties. Por ejemplo, para determinar qué tipos de sucesos se incluyen en el registro de auditoría, escriba en una línea:
     ```
     wsadmin>print AdminTask.tklmConfigGetEntry
      ('[-name Audit.event.types]')
     ```

Una respuesta de ejemplo puede ser:

```
All
```

b. Especifique el cambio necesario. Por ejemplo, para limitar la selección a dos tipos de sucesos para almacenarlos en el registro de auditoría, escriba en una línea:

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

- Interfaz REST:

a. Obtenga un identificador de autenticación de usuario exclusivo para acceder a los servicios REST de IBM Security Key Lifecycle Manager. Para obtener más información sobre el proceso de autenticación, consulte Proceso de autenticación de los servicios REST.

b. Para ejecutar el **Servicio REST Obtener propiedad de configuración única**, envíe la solicitud HTTP GET. Pase el identificador de autenticación de usuario que ha obtenido en el `Paso a` junto con el mensaje de solicitud, como se muestra en el ejemplo siguiente.

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

La respuesta satisfactoria puede ser:

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

c. Especifique el cambio necesario. Por ejemplo, puede utilizar el **Servicio REST Actualizar propiedad de configuración** para limitar la selección a dos tipos de sucesos para almacenar en el registro de auditoría enviando la siguiente solicitud HTTP:

```
PUT https://localhost:<puerto>/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. Reinicie el servidor. Para obtener instrucciones sobre cómo detener e iniciar el servidor, consulte el apartado “Reinicio de IBM Security Key Lifecycle Manager server” en la página 205.

Qué hacer a continuación

Puede volver a ejecutar una operación que anteriormente devolviera un error. A continuación, examine el registro de auditoría para obtener más información. Para obtener información detallada sobre los registros de auditoría, consulte el tema “Registros de auditoría en sistemas distribuidos” en la documentación IBM Security Key Lifecycle Manager.

Generación de registros de auditoría en formato de syslog

Puede utilizar la interfaz gráfica de usuario de IBM Security Key Lifecycle Manager para configurar y generar registros de auditoría en formato de syslog y enviarlos al servidor de syslog.

Acerca de esta tarea

Los mensajes del registro de auditoría se graban en un archivo de auditoría local configurado en formato de syslog cuando:

- El formato syslog está habilitado para los mensajes de auditoría.
- El formato syslog está habilitado y no se han especificado el nombre de host del servidor de syslog y el número de puerto.
- El formato de syslog está habilitado, se han especificado el nombre de host del servidor syslog y el número de puerto, sin embargo, no es posible acceder al nombre de host del servidor o al número de puerto.

Procedimiento

1. Inicie una sesión en la interfaz gráfica de usuario.
2. Pulse **IBM Security Key Lifecycle Manager** > **Configuración** > **Auditoría y depuración**.
3. Seleccione **Utilizar formato de syslog**.
4. Especifique el nombre de host del servidor o la dirección IP en **Host de servidor de syslog**.
5. Especifique el número de puerto en el que el servidor de syslog estará a la escucha de solicitudes en el **Puerto de servidor de syslog**.
6. Si necesita una transferencia segura de información de auditoría al servidor de syslog mediante el protocolo de transporte SSL/TLS, seleccione **Utilizar SSL/TLS**.
7. Pulse **Aceptar**.

Qué hacer a continuación

Después de habilitar el formato syslog para registros de auditoría con los parámetros necesarios, debe seguir los siguientes pasos únicamente si selecciona **Utilizar SSL/TLS**:

1. Si toda no se ha creado el certificado de servidor de SSL de IBM Security Key Lifecycle Manager, cree dicho certificado. Para crear el certificado, utilice la página SSL/KMIP para el servicio de claves en la interfaz gráfica, el **Servicio REST Crear certificado** o el mandato de CLI **tklmCertCreate**.
2. Exporte el certificado de servidor de SSL de IBM Security Key Lifecycle Manager a un archivo. Para exportar el certificado, puede utilizar el **Servicio REST Exportar certificado** o el mandato de CLI **tklmCertExport**.

   Para exportar el certificado de servidor, obtenga el alias del certificado de servidor del Paso 1 si todavía no se ha creado el certificado. Si el certificado ya está creado, desde la interfaz gráfica de usuario, vaya a **Configuración avanzada** > **Certificados del servidor**. El alias es el valor de la columna **Certificados** del certificado que está marcado como `En uso`.
3. Obtenga el certificado del servidor de syslog como un archivo, impórtelo y otorgue confianza al certificado de servidor de syslog en el servidor de IBM Security Key Lifecycle Manager. Utilice el mandato de CLI **tklmCertImport** o el **Servicio REST Importar certificado** para importar el certificado utilizado `SYSLOG`.
4. Importe el certificado de servidor de IBM Security Key Lifecycle Manager en el servidor de syslog. Utilice el archivo de certificado que se creó en el Paso 2.
5. Configure el alias del certificado del servidor de SSL de IBM Security Key Lifecycle Manager en el archivo de propiedades de configuración.

Nota: Este paso no es necesario si el certificado de servidor de SSL de IBM Security Key Lifecycle Manager se creó utilizando la interfaz gráfica de usuario. Por ejemplo,

Interfaz de línea de mandatos

```
 print AdminTask.tklmConfigUpdateEntry('[-name config.keystore.ssl.
certalias -value <alias del certificado de servidor que se
creó en el Paso 1>]')
```

Interfaz REST

```
PUT https://localhost:<puerto>/SKLM/rest/v1/configProperties
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth userAuthId=139aeh34567m
Accept-Language : en
{ "config.keystore.ssl.certalias" : "<alias del certificado de
servidor que se creó en el Paso 1>"}
```

6. Reinicie el servidor. Para obtener instrucciones sobre cómo detener e iniciar el servidor, consulte el apartado "Reinicio de IBM Security Key Lifecycle Manager server" en la página 205.

Especificación de valores para la información de depuración

Puede cambiar el valor predeterminado que utiliza IBM Security Key Lifecycle Manager para recopilar información de depuración. Los archivos de registro de depuración proporcionan información adicional para analizar y solucionar problemas de IBM Security Key Lifecycle Manager.

Acerca de esta tarea

Puede utilizar la sección Depuración de la página Auditoría para especificar los valores para generar información de depuración. O bien, puede utilizar los siguientes mandatos de CLI o las interfaces REST para listar o cambiar la propiedad **debug** en el archivo `SKLMConfig.properties`:

- **tklmConfigGetEntry** y **tklmConfigUpdateEntry**
- **Servicio REST Obtener propiedad de configuración única** y **Servicio REST Actualizar propiedad de configuración**

Your role must have a permission to the configure action.

Nota: Si se habilita el registro de depuración el rendimiento de IBM Security Key Lifecycle Manager puede disminuir. Solo habilite esta opción siguiendo las instrucciones del representante de soporte de IBM.

Procedimiento

1. Vaya a la página o el directorio correspondiente:
   - Interfaz gráfica de usuario:

     Inicie una sesión en la interfaz gráfica de usuario. Pulse **IBM Security Key Lifecycle Manager** > **Configuración** > **Auditoría y depuración**.
   - Command-line interface
     a. Go to the *<WAS_HOME>*`/bin` directory. For example,

        Windows

        ```
        cd drive:\Program Files\IBM\WebSphere\AppServer\bin
        ```

        Linux

        ```
        cd /opt/IBM/WebSphere/AppServer/bin
        ```

     b. Start the **wsadmin** interface by using an authorized user ID, such as `SKLMAdmin`. For example,

Windows

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

Linux

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

- Interfaz REST:
  - Abra un cliente REST.

2. Cambie los valores para generar información de depuración:
   - En la interfaz gráfica de usuario:
     a. Seleccione **Habilitar depuración** para establecer los valores de las propiedades siguientes en el archivo `SKLMConfig.properties`:

        ```
        debug=all
        ```

     b. Pulse **Aceptar**.
   - Interfaz de línea de mandatos:
     a. Escriba el mandato **`tklmConfigGetEntry`** en una línea para obtener el valor actual de la propiedad de destino en el archivo `SKLMConfig.properties`. Por ejemplo, para determinar el valor de `debug`, escriba en una sola línea:

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

        Una respuesta de ejemplo puede ser:

        ```
        none
        ```

     b. Especifique un valor nuevo para la propiedad. Por ejemplo, para especificar el valor `all` para generar registros de depuración, escriba en una línea:

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

   - Interfaz REST:
     a. Obtenga un identificador de autenticación de usuario exclusivo para acceder a los servicios REST de IBM Security Key Lifecycle Manager. Para obtener más información sobre el proceso de autenticación, consulte Proceso de autenticación de los servicios REST.
     b. Para ejecutar el **`Servicio REST Obtener propiedad de configuración única`**, envíe la solicitud HTTP GET. Pase el identificador de autenticación de usuario que ha obtenido en el `Paso a` junto con el mensaje de solicitud, como se muestra en el ejemplo siguiente.

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

        La respuesta satisfactoria puede ser:

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

     c. Especifique un valor nuevo para la propiedad. A continuación, envíe la siguiente solicitud HTTP:

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

3. El indicador de éxito varía dependiendo de la interfaz:

Especificación de los valores de puerto y tiempo de espera

Puede cambiar los valores de puerto y tiempo de espera predeterminados que proporciona IBM Security Key Lifecycle Manager.

Acerca de esta tarea

Puede utilizar la página Puertos de servicio de claves para cambiar los valores de puerto y tiempo de espera. O bien, puede utilizar los siguientes mandatos de CLI o los servicios REST para enumerar y cambiar las propiedades adecuadas en el archivo `SKLMConfig.properties`:

- **`tklmConfigGetEntry`** y **`tklmConfigUpdateEntry`**
- **`Servicio REST Obtener propiedad de configuración única`** y **`Servicio REST Actualizar propiedad de configuración`**

Antes de empezar, determine si hay conflictos de puerto o tiempo de espera en el sitio que impidan utilizar los valores predeterminados de IBM Security Key Lifecycle Manager. Your role must have a permission to the configure action.

Procedimiento

1. Vaya a la página o el directorio correspondiente:
   - Interfaz gráfica de usuario:

     Inicie una sesión en la interfaz gráfica de usuario. Pulse **IBM Security Key Lifecycle Manager** > **Configuration** > **Puertos de servicio de claves**.
   - Command-line interface
     a. Go to the `<WAS_HOME>/bin` directory. For example,

        Windows
        ```
        cd drive:\Program Files\IBM\WebSphere\AppServer\bin
        ```

        Linux
        ```
        cd /opt/IBM/WebSphere/AppServer/bin
        ```

     b. Start the **`wsadmin`** interface by using an authorized user ID, such as `SKLMAdmin`. For example,

        Windows
        ```
        wsadmin.bat -username SKLMAdmin -password mypwd -lang jython
        ```

        Linux
        ```
        ./wsadmin.sh -username SKLMAdmin -password mypwd -lang jython
        ```
   - Interfaz REST:
     – Abra un cliente REST.
2. Cambie los valores de puerto o tiempo de espera:
   - En la interfaz gráfica de usuario, cambie uno o varios de estos valores y pulse **Aceptar**:

     TCP port
     IBM Security Key Lifecycle Manager uses default port 3801. Values can range from 1 to 65535. The value that you set also changes the value of the **`TransportListener.tcp.port`** property in the `SKLMConfig.properties` file. You must ensure that the port is not already in use by another application.

     TCP timeout (in minutes)
     IBM Security Key Lifecycle Manager uses a default timeout value of 10 minutes. Values can range from 1 to 120. The value that you set

also changes the value of the **TransportListener.tcp.timeout** property in the SKLMConfig.properties file.

SSL port
IBM Security Key Lifecycle Manager uses default port 441. Values can range from 1 to 65535. The value that you set also changes the value of the **TransportListener.ssl.port** property in the SKLMConfig.properties file.

SSL timeout (in minutes)
IBM Security Key Lifecycle Manager uses a default timeout value of 10 minutes. Values can range from 1 to 120. This configuration parameter is associated with the value of the **TransportListener.ssl.timeout** property in the SKLMConfig.properties file.

KMIP SSL port
KMIP uses default port 5696.Values can range from 1 to 65535. This configuration parameter is associated with the value of the **KMIPListener.ssl.port** property in the SKLMConfig.properties file.

IBM Security Key Lifecycle Manager agent port
Agent uses default port 60015 to communicate with IBM Security Key Lifecycle Manager server. You can update the default agent port number only when the IBM Security Key Lifecycle Manager instance is not configured for multi-master setup.

- Interfaz de línea de mandatos:
  a. Escriba el mandato **tklmConfigGetEntry** en una línea para obtener el valor actual de la propiedad de destino en el archivo SKLMConfig.properties. Por ejemplo, escriba en una línea:

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

     Una respuesta de ejemplo puede ser:

     ```
     3801
     ```

  b. Especifique el cambio necesario. Por ejemplo, para especificar otro número de puerto TCP, escriba en una línea:

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

- Interfaz REST:
  a. Obtenga un identificador de autenticación de usuario exclusivo para acceder a los servicios REST de IBM Security Key Lifecycle Manager. Para obtener más información sobre el proceso de autenticación, consulte Proceso de autenticación de los servicios REST.
  b. Para ejecutar el **Servicio REST Obtener propiedad de configuración única**, envíe la solicitud HTTP GET. Pase el identificador de autenticación de usuario que ha obtenido en el Paso a junto con el mensaje de solicitud, como se muestra en el ejemplo siguiente.

     Solicitud de servicio

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

Respuesta satisfactoria

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

c. Especifique el cambio necesario. Por ejemplo, para especificar otro número de puerto TCP, envíe la siguiente solicitud de servicio:

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

Qué hacer a continuación

Para aplicar un cambio, por ejemplo, de número de puerto, reinicie el IBM Security Key Lifecycle Manager server.

Comprobación del número de puerto actual

Tras la instalación del IBM Security Key Lifecycle Manager server, quizás desee determinar los números de puerto seguros y no seguros para el IBM Security Key Lifecycle Manager server y para WebSphere Integrated Solutions Console.

Acerca de esta tarea

Los valores de los números de puerto se especifican en las propiedades **WC_adminhost_secure**, **WC_defaulthost** y **WC_defaulthost_secure**, en el archivo *WAS_HOME*/profiles/KLMProfile/properties/portdef.props. Por ejemplo, el archivo podría especificar estos valores:

```
WC_adminhost_secure=9083
WC_defaulthost=80
WC_defaulthost_secure=443
```

El valor de la propiedad **WC_adminhost_secure** corresponde al puerto seguro de WebSphere Integrated Solutions Console. El valor de la propiedad **WC_defaulthost** corresponde al puerto no seguro de IBM Security Key Lifecycle Manager server y **WC_defaulthost_secure** corresponde al puerto seguro.

Especificación de parámetros de servicio de claves

Puede cambiar los valores predeterminados de certificado que proporciona IBM Security Key Lifecycle Manager.

Acerca de esta tarea

Utilice la página Parámetros de servicio de claves para cambiar los valores de certificado. O bien, puede utilizar los siguientes mandatos de CLI o las interfaces REST para enumerar y cambiar las propiedades adecuadas en el archivo SKLMConfig.properties:

- **tklmConfigGetEntry** y **tklmConfigUpdateEntry**
- **Servicio REST Obtener propiedad de configuración única** y **Servicio REST Actualizar propiedad de configuración**

Your role must have a permission to the configure action.

Antes de empezar, determine si:

- Llevar a cabo la validación de la fecha del certificado antes de que se sirve una clave. La validación confirma que el certificado es válido y no ha caducado.
- Se van a identificar certificados utilizando el identificador de claves de sujeto que se almacena en el certificado.

Procedimiento

1. Vaya a la página o el directorio correspondiente:
   - Interfaz gráfica de usuario:

     Inicie una sesión en la interfaz gráfica de usuario. Pulse **IBM Security Key Lifecycle Manager** > **configuración** > **Parámetros de servicio de claves**.
   - Command-line interface
     a. Go to the <*WAS_HOME*>/bin directory. For example,

        Windows
        ```
        cd drive:\Program Files\IBM\WebSphere\AppServer\bin
        ```

        Linux
        ```
        cd /opt/IBM/WebSphere/AppServer/bin
        ```

     b. Start the **wsadmin** interface by using an authorized user ID, such as SKLMAdmin. For example,

        Windows
        ```
        wsadmin.bat -username SKLMAdmin -password mypwd -lang jython
        ```

        Linux
        ```
        ./wsadmin.sh -username SKLMAdmin -password mypwd -lang jython
        ```
   - Interfaz REST:
     – Abra un cliente REST.
2. Cambie el valor de uno o varios valores de certificado:
   - En la interfaz gráfica de usuario, cambie uno o varios de los siguientes valores y pulse **Aceptar**:

     Do not use expired certificates for write requests or data writes.
     Before you serve a key, validates that the expiration date is not passed for the certificate or certificates that wraps this key. Expired certificates are used only for read requests. When this setting is enabled, expired certificates are not used for write requests. Selecting this check box changes the value of the **cert.valiDATE** property to true in the SKLMConfig.properties file.

     Conservar certificados de comunicación de dispositivo cliente pendientes.
     Conservar los certificados de comunicación de dispositivo cliente pendientes hasta que acepte los certificados para su uso en la comunicación segura entre el dispositivo y el IBM Security Key Lifecycle Manager server. Si inhabilita este valor, debe importar manualmente los certificados de comunicación de dispositivo cliente pendientes. Este parámetro de configuración está asociado al valor de la propiedad **enableClientCertPush** de los dispositivos del cliente pendientes en el archivo SKLMConfig.properties.

     Identify certificates by certificate name.
     Identify certificates by using the certificate name that is stored in the certificate, rather than using a subject key identifier. You specify the certificate name when you create a certificate. This function is used when decrypting data that was written to a device.

     When disabled, the Subject Key Identifier is used to determine the certificate to be used when reading data on a cartridge or other

device. This configuration parameter is associated with the value of the **useSKIDefaultLabels** property in the SKLMConfig.properties file.

- Interfaz de línea de mandatos:
  a. Escriba el mandato **tklmConfigGetEntry** en una línea para obtener el valor actual de la propiedad de destino en el archivo SKLMConfig.properties. Por ejemplo, escriba:

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

     Una respuesta de ejemplo puede ser:

     ```
     False
     ```

  b. Especifique el cambio necesario. Por ejemplo, para cambiar el valor de la propiedad **zOSCompatibility** a true, escriba en una línea:

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

- Interfaz REST:
  a. Obtenga un identificador de autenticación de usuario exclusivo para acceder a los servicios REST de IBM Security Key Lifecycle Manager. Para obtener más información sobre el proceso de autenticación, consulte Proceso de autenticación de los servicios REST.
  b. Para ejecutar el **Servicio REST Obtener propiedad de configuración única**, envíe la solicitud HTTP GET. Pase el identificador de autenticación de usuario que ha obtenido en el Paso a junto con el mensaje de solicitud, como se muestra en el ejemplo siguiente.

     Solicitud de servicio

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

     Respuesta satisfactoria

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

  c. Especifique el cambio necesario. Por ejemplo, puede enviar la solicitud de servicio siguiente para cambiar el valor de la propiedad **zOSCompatibility** a true:

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

Qué hacer a continuación

Los cambios en los valores de certificado se realizan dinámicamente. A continuación, puede crear los certificados necesarios y asociarlos con dispositivos específicos.

Configuración del almacén de confianza

El almacén de confianza de IBM Security Key Lifecycle Manager almacena los certificados de confianza y los certificados raíz de dispositivos que se utilizan para la comunicación segura entre IBM Security Key Lifecycle Manager y los dispositivos.

La instalación de IBM Security Key Lifecycle Manager crea el archivo del almacén de confianza `tklmTruststore.jceks` en `<WAS_HOME>\products\sklm\keystore`.

Windows
`C:\Program Files\IBM\WebSphere\AppServer\products\sklm\keystore`

Linux `/opt/IBM/WebSphere/AppServer/products/sklm/keystore`

Puede añadir el certificado raíz del dispositivo a la lista de confianza añadiéndolo al almacén de confianza. Cuando el certificado raíz del dispositivo se añade al almacén de confianza, todos los dispositivos con certificados que están firmados por este certificado raíz se convierten automáticamente en de confianza. La adición del certificado raíz del dispositivo elimina la necesidad de importar el certificado del dispositivo en la lista de certificado de comunicación de dispositivo de cliente para establecer la comunicación de SSL/TLS con el servidor de IBM Security Key Lifecycle Manager.

Puede utilizar la interfaz gráfica de usuario, la interfaz de línea de mandatos y la interfaz REST de IBM Security Key Lifecycle Manager para gestionar certificados del almacén de confianza.

Puede realizar las siguientes acciones con los certificados:

- Añadir un certificado al almacén de confianza.
- Visualizar los certificados en el almacén de confianza.
- Suprimir certificados del almacén de confianza.

Adición de certificados al almacén de confianza

Es posible que tenga que añadir un certificado desde un archivo de certificado en formato `DER` o `base64` al almacén de confianza interno de IBM Security Key Lifecycle Manager. El certificado se utiliza para la comunicación entre IBM Security Key Lifecycle Manager y el dispositivo que se identifica a sí mismo con este certificado o el certificado raíz para este certificado.

Acerca de esta tarea

Utilice el diálogo Añadir certificado, el mandato **`tklmTrustStoreCertAdd`** o el **`Servicio REST Añadir certificado de almacén de confianza`** para añadir un certificado al almacén de confianza de IBM Security Key Lifecycle Manager. Su ID de usuario debe poseer el rol `klmSecurityOfficer`.

Procedimiento

1. Vaya al directorio o la página apropiada.
   - Interfaz gráfica de usuario
     a. Inicie una sesión en la interfaz gráfica de usuario.
     b. Pulse **IBM Security Key Lifecycle Manager** > **Configuración** > **Almacén de confianza**.
     c. En la página Almacén de confianza, pulse **Añadir**.

- Command-line interface
  a. Go to the <*WAS_HOME*>/bin directory. For example,

     Windows
     ```
     cd drive:\Program Files\IBM\WebSphere\AppServer\bin
     ```

     Linux
     ```
     cd /opt/IBM/WebSphere/AppServer/bin
     ```

  b. Start the **wsadmin** interface by using an authorized user ID, such as SKLMAdmin. For example,

     Windows
     ```
     wsadmin.bat -username SKLMAdmin -password mypwd -lang jython
     ```

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

- Interfaz REST
  – Abra un cliente REST.

2. Añada al almacén de confianza un certificado desde un archivo de certificado en formato DER o base64.
   - Interfaz gráfica de usuario
     a. En el campo **Alias de certificado**, especifique un nombre de alias para el certificado.
     b. Pulse **Examinar** para especificar la ubicación del archivo de certificado en el directorio <*SKLM_DATA*>, por ejemplo, C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data. Para ver la definición de <*SKLM_DATA*>, consulte Definiciones para *HOME* y otras variables de directorio.
     c. Seleccione el formato del certificado, DER o base64.
     d. Pulse **Añadir certificado**.
   - Interfaz de línea de mandatos

     Escriba **tklmTrustStoreCertAdd** para añadir un certificado al almacén de confianza. Por ejemplo, para añadir un archivo de certificado en formato DER, ejecute el siguiente mandato.

     ```
     print AdminTask.tklmTrustStoreCertAdd
      ('[-fileName d:\\mypath\\mycertfilename.der
       -format DER -alias myCertAlias]')
     ```

   - Interfaz REST

     Utilice el **Servicio REST Añadir certificado de almacén de confianza** para añadir un certificado. Por ejemplo, puede enviar la siguiente solicitud HTTP.

     ```
     PUT https://localhost:<puerto>/SKLM/rest/v2/trustStoreCertificates/addCertToTrustStore
     Content-Type: application/json
     Accept: application/json
     Authorization: SKLMAuth userAuthId=139aeh34567m
     {"certFile":"C:\\Program Files\\IBM\\WebSphere\\AppServer\\products\\sklm\\data\\clientsslce
     "certFormat":"DER","certAlias":"myCert"}
     ```

Supresión de un certificado del almacén de confianza

Podría tener la necesidad de suprimir un certificado en el almacén de confianza interno de IBM Security Key Lifecycle Manager. Por ejemplo, podría tener la necesidad de suprimir un certificado que ya no es necesario.

Acerca de esta tarea

Utilice el diálogo Suprimir, el mandato **tklmTrustStoreCertDelete** o el **Servicio REST Suprimir certificado de almacén de confianza** para suprimir un certificado

del almacén de confianza. Su ID de usuario debe poseer el rol klmSecurityOfficer.

Procedimiento

1. Vaya al directorio o la página apropiada.
   - Interfaz gráfica de usuario
     a. Inicie una sesión en la interfaz gráfica de usuario.
     b. Pulse **IBM Security Key Lifecycle Manager** > **Configuración** > **Almacén de confianza**.
     c. En la página Almacén de confianza, seleccione un certificado.
     d. Pulse **Suprimir**.
     e. O bien, pulse con el botón derecho del ratón en un certificado en la tabla y seleccione **Suprimir**.
   - Command-line interface
     a. Go to the <*WAS_HOME*>/bin directory. For example,

        Windows
        ```
        cd drive:\Program Files\IBM\WebSphere\AppServer\bin
        ```

        Linux
        ```
        cd /opt/IBM/WebSphere/AppServer/bin
        ```

     b. Start the **wsadmin** interface by using an authorized user ID, such as SKLMAdmin. For example,

        Windows
        ```
        wsadmin.bat -username SKLMAdmin -password mypwd -lang jython
        ```

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

   - Interfaz REST
     – Abra un cliente REST.
2. Suprima el certificado del almacén de confianza.
   - Interfaz gráfica de usuario

     En el diálogo Confirmar, lea el mensaje de confirmación antes de suprimir el certificado. Pulse **Aceptar**.
   - Interfaz de línea de mandatos

     Utilice el mandato tklmTrustStoreCertList para encontrar un certificado, y el mandato tklmTrustStoreCertDelete para suprimir un certificado del almacén de confianza. Ejecute el siguiente mandato para encontrar el certificado.
     ```
     print AdminTask.tklmTrustStoreCertList ('[-alias myCertAlias]')
     ```

     Ejecute el siguiente mandato para suprimir un certificado del almacén de confianza.
     ```
     print AdminTask.tklmTrustStoreCertDelete ('[-alias myCertAlias]')
     ```
   - Interfaz REST

     Utilice el Servicio REST Enumerar certificados de almacén de confianza para encontrar un certificado y el Servicio REST Suprimir certificado de almacén de confianza para suprimir un certificado del almacén de confianza. Por ejemplo, puede enviar las siguientes solicitudes HTTP utilizando un cliente REST.
     ```
     GET https://localhost:<puerto>/SKLM/rest/v1/trustStoreCertificates?alias=myCertAlias
     Content-Type: application/json
     Accept : application/json
     Authorization: SKLMAuth userAuthId=139aeh34567m
     ```

```
DELETE https://localhost:<puerto>/SKLM/rest/v2/trustStoreCertificates?alias=myCertAlias
Content-Type: application/json
Accept: application/json
Authorization: SKLMAuth userAuthId=139aeh34567m
```

Administración de grupos, usuarios y roles

Puede limitar el rango de actividades que los administradores pueden llevar a cabo de su organización.

Para garantizar la eficacia a largo plazo, se recomienda crear un grupo y asignarle roles y usuarios, en lugar de asignar los roles directamente a un usuario individual. De esta forma, será más fácil cambiar los roles de personas con tareas similares y evitar la repetición de trabajo si un usuario está asignado a otro departamento.

Por ejemplo, puede especificar este rango de actividades:

- No hay acceso disponible para algunos roles. Por ejemplo, la organización puede desear separar las tareas que hacen una copia de seguridad y restauran archivos.
- Algunas tareas están ocultas en WebSphere Integrated Solutions Console.
- La administración sólo puede realizarse en las LTO tape drives.

Asignación de permisos

Puede correlacionar un grupo administrativo con un conjunto limitado de permisos.

Acerca de esta tarea

Esta tarea utiliza el ID de usuario WASAdmin en la WebSphere Integrated Solutions Console para correlacionar un grupo con un conjunto limitado de acciones para administrar los DS5000 storage servers.

For more information about the commands that map groups to roles, see the IBM WebSphere Application Server documentation (http://www.ibm.com/support/knowledgecenter/en/SSAW57_9.0.0/com.ibm.websphere.nd.multiplatform.doc/ae/rxml_atauthorizationgroup.html).

Procedimiento

1. Inicie una sesión en WebSphere Integrated Solutions Console.
   - Interfaz gráfica de usuario:
     a. En la página de bienvenida del navegador, escriba un ID de usuario `WASAdmin` y un valor de contraseña como, por ejemplo, `wasadminpw`.
     b. En la interfaz gráfica de usuario, pulse **Usuarios y grupos** > **Roles de grupo administrativo**.
     c. Pulse **Añadir**.
   - Command-line interface
     a. Go to the *<WAS_HOME>*`/bin` directory. For example,

        Windows
        ```
        cd drive:\Program Files\IBM\WebSphere\AppServer\bin
        ```

        Linux `cd /opt/IBM/WebSphere/AppServer/bin`

     b. Start the **wsadmin** interface by using an authorized user ID, such as WASAdmin. For example,

Windows

```
wsadmin.bat -username WASAdmin -password wasadminpw -lang jython
```

Linux

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

2. Correlacione un conjunto limitado de roles con el grupo.
   - Interfaz gráfica de usuario:
     a. En la página Roles de grupo administrativo, bajo **Roles**, seleccione de la lista el subconjunto requerido de roles. Por ejemplo, siga estos pasos:
        - Bloquee el acceso a algunos roles. Por ejemplo, la organización puede desear separar las tareas que restauran archivos. En este caso, no seleccione el elemento `klmRestore` de la lista.
        - Determine si desea ocultar otras tareas en la WebSphere Integrated Solutions Console. Si desea ocultar tareas, seleccione **suppressmonitor** como rol.
        - Limite la administración sólo a los DS5000 storage servers. Por ejemplo, seleccione **DS5000**.

          O bien, si la tarea define actividades administrativas para un nuevo grupo de dispositivos como, por ejemplo, `myDS5000`, puede seleccionar `myDS5000`, que ha creado previamente.
        - Pulse la tecla Control y seleccione los roles que se aplican a IBM Security Key Lifecycle Manager:

          klmBackup
          Crear y suprimir una copia de seguridad de los datos.

          klmRestore
          Restaurar una copia de seguridad previa de los datos.

          klmConfigure
          Leer o cambiar las propiedades, o actuar en los certificados.

          klmAudit
          Ver datos de auditoría.

          klmView
          Ver objetos.

          klmCreate
          Crear objetos.

          klmModify
          Modificar objetos.

          klmDelete
          Suprimir objetos.

          klmGet
          Exportar una clave o un certificado.

          suppressmonitor
          Ocultar otras tareas en la WebSphere Integrated Solutions Console.

          DS5000
          Permite realizar acciones en los DS5000 storage servers.

     b. Seleccione **Correlacionar grupos como se especifica más abajo**.
     c. Escriba una serie de búsqueda en el campo **Buscar serie**. Por ejemplo, escriba `DS5000Admin`.

d. Pulse **Buscar**.
e. Desde la lista **Disponible**, seleccione el grupo.
f. Pulse en la flecha para mover el grupo seleccionado a la columna **Correlacionado con rol**.
g. Pulse **Aceptar**.
h. Pulse **Guardar** para guardar los cambios directamente en la configuración maestra.

- Interfaz de línea de mandatos:

  Escriba `mapGroupsToAdminRole` y especifique los valores necesarios para correlacionar el grupo con un rol administrativo específico. Por ejemplo, utilizando Jython para especificar más de un rol con un grupo, escriba una secuencia de mandatos, pulsando **Intro** después de cada mandato.

  – Especifique el primer rol del grupo:

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

  – Especifique el siguiente rol del grupo:

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

  – Especifique los restantes roles del grupo utilizando una sentencia aparte para cada rol:

  ```
  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]')
  ```

  donde:

  - authorizationGroupName
  El nombre del grupo de autorización. Si no especifica este parámetro, se da por supuesto el grupo de autorización a nivel de célula. (String, opcional)

  - roleName
  El nombre del rol administrativo. (String, necesario)

  - groupids
  La lista de ID de grupo que se correlacionan con el rol administrativo. (String[])

3. Guarde el trabajo.
   - Graphical user interface:

     Confirm completion of your task, by using the prompt that the graphical user interface provides.

   - Command-line interface:

     Save your configuration. For example, by using Jython, type:

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

4. Asegúrese de que los roles que ha guardado en el grupo estuvieran asignados.
   - Interfaz gráfica de usuario

     Salga y vuelva a entrar en la página Roles de grupo administrativo. Aparecen los roles adicionales.
   - Interfaz de línea de mandatos

     Utilizando la sintaxis Jython, escriba:

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

Qué hacer a continuación

A continuación, especifique los otros grupos que necesite su organización. Por ejemplo, especifique un grupo administrativo para realizar tareas de operador.

Creación de un usuario en un grupo

Cree un usuario y asigne la pertenencia del usuario a un grupo de administradores del sistema.

Acerca de esta tarea

Esta tarea utiliza el ID de usuario WASAdmin en la WebSphere Integrated Solutions Console para crear un usuario y añadirlo a un grupo.

Nota: Para acceder a una interfaz gráfica de usuario o interfaz de línea de mandatos de IBM Security Key Lifecycle Manager, el usuario debe estar asignado a este grupo: `klmGUICLIAccessGroup`

For more information about the commands that create groups and users, see the IBM WebSphere Application Server documentation (http://www.ibm.com/support/knowledgecenter/en/SSAW57_9.0.0/com.ibm.websphere.nd.multiplatform.doc/ae/rxml_atwimmgt.html).

Procedimiento

1. Inicie sesión en la consola WebSphere Integrated Solutions Console.
   - Interfaz gráfica de usuario:
     a. En la página de bienvenida del navegador, escriba un ID de usuario de `WASAdmin` y un valor de contraseña como por ejemplo, `wasadminpw`.
     b. En el árbol de navegación, pulse **Usuarios y grupos** > **Gestionar usuarios**.
   - Command-line interface
     a. Go to the <*WAS_HOME*>/bin directory. For example,

        Windows

        ```
        cd drive:\Program Files\IBM\WebSphere\AppServer\bin
        ```

        Linux

        ```
        cd /opt/IBM/WebSphere/AppServer/bin
        ```

     b. Start the **wsadmin** interface by using an authorized user ID, such as WASAdmin. For example,

        Windows

        ```
        wsadmin.bat -username WASAdmin -password wasadminpw -lang jython
        ```

        Linux

        ```
        ./wsadmin.sh -username WASAdmin -password wasadminpw -lang jython
        ```
2. Cree un usuario, especificando la pertenencia en el nuevo grupo.

- Interfaz gráfica de usuario:
  a. En la página Gestionar usuarios, pulse **Crear**.
  b. En la página Crear un usuario, especifique la información necesaria como, por ejemplo, el ID de usuario y la contraseña. Por ejemplo, escriba `myAdmin` como ID de usuario y `mypwd` como contraseña.
  c. Pulse **Crear**.
  d. Pulse el enlace al nuevo ID de usuario para mostrar las propiedades del usuario.
  e. En el diálogo Propiedades del usuario, pulse **Grupos**.
  f. Pulse **Añadir**.
  g. En el diálogo Añadir un usuario a grupos, pulse **Buscar**.
  h. En la tabla de grupos, seleccione el grupo que ha creado previamente y pulse **Añadir**.
  i. Lea el mensaje de confirmación que ha añadido el usuario al grupo y pulse **Cerrar**.
- Interfaz de línea de mandatos:
  a. Primero, cree el usuario. Escriba `createUser` y especifique los valores necesarios para crear un usuario. Por ejemplo, utilizando Jython, escriba:

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

     donde:

     -uid Especifica el ID exclusivo del usuario que desea crear. (String, necesario)

     -password
     Especifica la contraseña del usuario. (String, necesario)

     -confirmPassword
     Especifica la contraseña de nuevo para validar cómo se ha escrito para el parámetro de contraseña. (String, opcional)

     -cn Especifica el nombre o el nombre propio del usuario. (String, opcional)

     -sn Especifica el apellido o el nombre de familia del usuario. (String, opcional)
  b. Añada el usuario como miembro del grupo. Por ejemplo, en Jython, escriba:

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

     donde:

     memberUniqueName *uniqueName*
     Especifica el valor de nombre exclusivo para el usuario o el grupo que desea añadir al grupo especificado.

     groupUniqueName *uniqueName*
     Especifica el valor de nombre exclusivo para el grupo al que desea añadir el usuario.

3. Compruebe que el usuario sea miembro del grupo.
   - Interfaz gráfica de usuario:
     a. En el árbol de navegación, pulse **Usuarios y grupos** > **Gestionar usuarios**.

b. En la página Gestionar usuarios, en la columna **ID de usuario**, pulse en la entrada del nuevo ID de usuario.
c. En el diálogo Propiedades del usuario, pulse el separador **Grupos**. Compruebe que el usuario sea miembro del nuevo grupo.

- Interfaz de línea de mandatos:

  Por ejemplo, utilizando Jython, escriba:

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

4. Guarde el trabajo.
   - Graphical user interface:

     Confirm completion of your task, by using the prompt that the graphical user interface provides.
   - Command-line interface:

     Save your configuration. For example, by using Jython, type:

     ```
     print AdminConfig.save()
     ```
5. Si ha utilizado la interfaz de línea de mandatos para crear el usuario, ejecute los mandatos **stopServer** y **startServer** para reiniciar el IBM Security Key Lifecycle Manager server. A continuación, inicie sesión como nuevo usuario.

Qué hacer a continuación

A continuación, valide que el usuario pueda ejecutar tareas autorizadas. Finalice la sesión como WASAdmin. Inicie una sesión como el nuevo usuario y confirme que puede ejecutar las tareas utilizando IBM Security Key Lifecycle Manager.

Creación de un grupo

Puede crear un grupo y utilizarlo para especificar los límites de algunos administradores del sistema. Debe modelar el grupo después de los grupos predefinidos LTO.

Acerca de esta tarea

Esta tarea utiliza el ID de usuario WASAdmin en la WebSphere Integrated Solutions Console para crear un grupo administrativo.

Nota: Para acceder a una interfaz gráfica de usuario o interfaz de línea de mandatos de IBM Security Key Lifecycle Manager, el usuario debe estar asignado a este grupo: `klmGUICLIAccessGroup`

For more information about the commands that create groups and users, see the IBM WebSphere Application Server documentation (http://www.ibm.com/support/knowledgecenter/en/SSAW57_9.0.0/com.ibm.websphere.nd.multiplatform.doc/ae/rxml_atwimmgt.html).

You can use WebSphere Integrated Solutions Console to create child groups with different permissions within a parent group. However, IBM Security Key Lifecycle Manager recognizes the permissions of only the parent group, not the permissions of its child groups.

Procedimiento

1. Inicie sesión en WebSphere Integrated Solutions Console (`https://localhost:9083/ibm/console/logon.jsp`).
   - Interfaz gráfica de usuario:

a. En la página de bienvenida del navegador, escriba el ID de usuario `WASAdmin` y la contraseña de este administrador.
b. En el árbol de navegación, pulse **Usuarios y grupos** > **Gestionar grupos**.

- Command-line interface
  a. Go to the `<WAS_HOME>/bin` directory. For example,

     Windows
     ```
     cd drive:\Program Files\IBM\WebSphere\AppServer\bin
     ```

     Linux
     ```
     cd /opt/IBM/WebSphere/AppServer/bin
     ```

  b. Start the **wsadmin** interface by using an authorized user ID, such as WASAdmin. For example,

     Windows
     ```
     wsadmin.bat -username WASAdmin -password wasadminpw -lang jython
     ```

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

2. Cree un grupo:
   - Interfaz gráfica de usuario:
     a. En la página Gestionar grupos, pulse **Crear**.
     b. En el campo **Nombre de grupo**, especifique el nombre de grupo. Por ejemplo, escriba `DS5000Admin`.
     c. En el campo **Descripción**, especifique más información sobre el grupo que desea crear.
     d. Pulse **Crear**.
   - Interfaz de línea de mandatos:
     a. Cree un grupo de autorización.
     b. Cree un grupo.

     Escriba `createGroup` y especifique los valores necesarios para crear un grupo. Por ejemplo, utilizando Jython, escriba:
     ```
     print AdminTask.createGroup
       ('[-cn DS5000Admin -description DS5000_LocalAdmins]')
     ```
     donde:

     -cn Obligatorio (cadena). Especifica el nombre común del grupo que desea crear. Este parámetro se correlaciona con la propiedad **cn** en el gestor del miembro virtual.

     -description
     Opcional (cadena). Especifica más información sobre el grupo que desea crear.
3. Guarde el trabajo.
   - Graphical user interface:

     Confirm completion of your task, by using the prompt that the graphical user interface provides.
   - Command-line interface:

     Save your configuration. For example, by using Jython, type:
     ```
     print AdminConfig.save()
     ```

Qué hacer a continuación

A continuación, asigne uno o varios permisos o roles al grupo.

Validación de las tareas de usuario

Compruebe que un nuevo usuario en un grupo administrativo pueda realizar tareas.

Acerca de esta tarea

Esta tarea valida que un usuario de un grupo pueda ejecutar las tareas que proporciona la pertenencia al grupo. Por ejemplo, el usuario puede administrar DS5000 storage servers.

Nota: Para acceder a una interfaz gráfica de usuario o interfaz de línea de mandatos de IBM Security Key Lifecycle Manager, el usuario debe estar asignado a este grupo: `klmGUICLIAccessGroup`

For more information about the commands that map groups to roles, see the IBM WebSphere Application Server documentation (http://www.ibm.com/support/knowledgecenter/en/SSAW57_9.0.0/com.ibm.websphere.nd.multiplatform.doc/ae/rxml_atauthorizationgroup.html).

Procedimiento

Verifique que el usuario puede ejecutar un conjunto de tareas proporcionadas por la pertenencia al grupo.

- Interfaz gráfica de usuario:
  1. Finalice la sesión utilizando el ID de usuario WASAdmin.
  2. Inicie una sesión en la interfaz gráfica del usuario como el usuario autorizado en el grupo. Por ejemplo, inicie sesión como `myAdmin`.
  3. En la tabla Gestión de claves y dispositivos, compruebe que la única opción administrativa sea DS5000.

     O bien, si las tareas anteriores definían actividades administrativas para un nuevo grupo de dispositivos como, por ejemplo, `myDS5000`, compruebe que la única opción administrativa sea `myDS5000`.
  4. Seleccione el dispositivo y pulse **Ir a** > **Gestionar claves y dispositivos**.
  5. O bien, pulse con el botón derecho del ratón y seleccione **Gestionar claves y dispositivos**.
  6. En la página de gestión de DS5000, realice la tarea. Por ejemplo, añada un nuevo grupo de claves.
- Interfaz de línea de mandatos:
  1. Finalice la sesión de **wsadmin** como wasadmin.
  2. En el directorio *WAS_HOME*`/bin`, inicie una nueva sesión de **wsadmin** utilizando Jython. A continuación, inicie sesión en **wsadmin** con un ID de usuario autorizado, como por ejemplo, el nuevo ID de usuario `myAdmin` tal como se muestra en el ejemplo siguiente.
     - Vaya al directorio <*WAS_HOME*>`/bin`.

       Windows

       ```
       cd unidad:\Program Files\IBM\WebSphere\AppServer\bin
       ```

       Linux

       ```
       cd /opt/IBM/WebSphere/AppServer/bin
       ```
     - Inicie la interfaz **wsadmin** utilizando un ID de usuario autorizado.

       Windows

       ```
       wsadmin.bat -username myAdmin -password password -lang jython
       ```

Linux

```
./wsadmin.sh -username myAdmin -password password -lang jython
```

3. Añada un grupo de claves de ejemplo. Por ejemplo, escriba:

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

O bien, envíe la siguiente solicitud HTTP utilizando un cliente REST:

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

Qué hacer a continuación

A continuación, especifique los otros grupos que necesite su organización. Por ejemplo, especifique un grupo para realizar tareas de operador o auditor.

Política de contraseña para el usuario de IBM Security Key Lifecycle Manager

La política de contraseña que se aplica a la contraseña de un nuevo usuario de IBM Security Key Lifecycle Manager se especifica en el archivo *SKLM_DATA*/config/TKLMPasswordPolicy.xml.

La política no se aplica a las contraseñas iniciales que se crean para los usuarios predeterminados como, por ejemplo, SKLMAdmin. Estos usuarios predeterminados se crean durante la instalación de IBM Security Key Lifecycle Manager.

La política de contraseña se aplica a los cambios en las contraseñas de los usuarios predeterminados y a las contraseñas nuevas y modificadas de los nuevos usuarios. La comprobación de contraseñas sólo se hace cuando crea o cambia un perfil de usuario. Debe asignar un rol a un nuevo usuario antes de que el usuario intente iniciar una sesión en IBM Security Key Lifecycle Manager.

La política de contraseña está habilitada de forma predeterminada. Puede utilizar un editor XML o ASCII para cambiar este archivo. Para inhabilitar la política, cambie el valor del parámetro **enabled** en el archivo de política por `false`:

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

IBM Security Key Lifecycle Manager da soporte a estas reglas de contraseña:

Tabla 1. Reglas de contraseña

Regla	Valor predeterminado
Longitud mínima	6
Longitud máxima	20
Número mínimo de caracteres numéricos	2
Número mínimo de caracteres alfabéticos	3
Número máximo de apariciones consecutivas del mismo carácter	2
Caracteres en mayúsculas	Como mínimo 1
Caracteres en minúsculas	Como mínimo 1

Tabla 1. Reglas de contraseña (continuación)

Regla	Valor predeterminado
Caracteres especiales El requisito de carácter especial no está obligado cuando se utiliza la herramienta **imcl** para la instalación silenciosa. Para obtener más información sobre los caracteres especiales soportados, consulte "Caracteres especiales soportados en contraseñas".	Como mínimo 1
No permitir la presencia del ID* de usuario en la contraseña	Habilitado
No permitir la presencia del nombre* de usuario en la contraseña	Habilitado

* La detección de este valor es sensible a las mayúsculas y minúsculas.
Nota: Para especificar que el valor no sea sensible a las mayúsculas y minúsculas, edite la política de contraseña predeterminada y especifique `CaseInsensitive` para el ID y nombre de usuario:

```
<?xml version="1.0" encoding="UTF-8"?>
<PasswordPolicy enabled="true" name="Password policy for TKLM"
 uuid="" version="1.0">
 <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/>
         <NotUserName/>
     </PasswordRuleSet>
  ]]></PasswordRules>
</PasswordPolicy>
```

Caracteres especiales soportados en contraseñas

Los siguientes caracteres especiales están soportados en la contraseña del administrador de Db2, en la contraseña del administrador (WASadmin) de WebSphere Application Server y en la contraseña del administrador (SKLMAdmin) de IBM Security Key Lifecycle Manager.

Caracteres especiales soportados en contraseñas en sistemas Linux

En la siguiente tabla se proporciona la lista de caracteres especiales que están soportados en las contraseñas en sistemas Linux:

Nombre del carácter especial	Carácter especial
tilde	~
arroba	@
almohadilla	#
guión bajo	_
acento circunflejo	^
asterisco	*
signo de porcentaje	%

Nombre del carácter especial	Carácter especial
barra inclinada	/
punto	.
signo más	+
dos puntos	:
punto y coma	;
signo igual	=

Caracteres especiales soportados en contraseñas en sistemas Windows

En la siguiente tabla se proporciona la lista de caracteres especiales que están soportados en las contraseñas en sistemas Windows:

Nombre del carácter especial	Carácter especial
tilde	~
arroba	@
guión bajo	_
barra inclinada	/
signo más	+
dos puntos	:

Directrices para utilizar los caracteres especiales soportados en contraseñas

Tenga en cuenta las siguientes directrices cuando utilice los caracteres especiales soportados en contraseñas. Estas directrices no son aplicables cuando se especifican contraseñas en la interfaz gráfica de usuario.

- Cierre la contraseña entre comillas cuando utilice los shells del sistema operativo para conectar la interfaz wsadmin de WebSphere Application Server o la línea de mandatos de Db2 o para ejecutar una instalación de fixpack. Utilice comillas simples para Linux y comillas dobles para Windows. Por ejemplo:

  Linux

  ```
  [root@sklm bin]# ./wsadmin.sh -username sklmadmin -password '~@_ABc12/+:' -lang jython
  WASX7209I: Conectado para procesar "server1" en el nodo SKLMNode utilizando el conector de SOAP; El tipo de proceso es:
  WASX7031I: Para obtener ayuda, especifique: "print Help.help()"
  wsadmin>
  ```

  Windows

  ```
  C:\Program Files\IBM\WebSphere\AppServer\bin>wsadmin.bat -username sklmadmin -password "~@_ABc12/+:" -lang jython
  WASX7209I: Conectado para procesar "server1" en el nodo SKLMNode utilizando el conector de SOAP;
    El tipo de proceso es: UnManagedProcess
  WASX7031I: Para obtener ayuda, especifique: "print Help.help()"
  wsadmin>
  ```

- Añada contraseñas cifradas a elementos relevantes del archivo de respuestas cuando ejecute el proceso de instalación o actualización de IBM Security Key Lifecycle Manager (fix pack o release principal) en modalidad silenciosa.

  Para crear una contraseña cifrada, utilice el programa de utilidad `imcl`, como se muestra a continuación:

  Linux

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

Asegúrese de utilizar una barra inclinada invertida (\) como carácter de escape para los caracteres especiales en la contraseña. Por ejemplo:

```
cd /SKLM/disk1/im/tools
./imcl encryptString \~\@\_ABc12\/\+\:
```

Se devuelve la serie cifrada (por ejemplo, `pABm1rqy66jAykrhBtpM6Q==`).

Windows

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

Asegúrese de cerrar toda la contraseña completa entre comillas dobles. Por ejemplo:

```
cd C:\SKLM\disk1\im\tools
C:\SKLM301\disk1\im\tools>imcl.exe encryptString "~@_ABc12/+:"
```

Se devuelve la serie cifrada (por ejemplo, `pABm1rqy66jAykrhBtpM6Q==`).

Para obtener más información, consulte Contraseña cifrada para elementos del archivo de respuestas.

Cambio de la política de contraseña

Puede utilizar un editor para cambiar manualmente la política de contraseña que proporciona IBM Security Key Lifecycle Manager.

Acerca de esta tarea

Asegúrese de cambiar sólo los valores de elemento y atributo en la política de contraseña, no los propios nombres de elemento y atributo. La política de contraseña se aplica a los cambios en las contraseñas de los usuarios predeterminados y a las contraseñas nuevas y modificadas de los nuevos usuarios. La comprobación de contraseñas sólo se hace cuando crea o cambia un perfil de usuario.

Procedimiento

1. Antes de empezar, haga una copia de seguridad del archivo *SKLM_DATA*`/config/TKLMPasswordPolicy.xml` en una ubicación segura. Si una política de contraseña cambiada tiene problemas, puede volver a la copia de seguridad.
2. Edite el archivo `TKLMPasswordPolicy.xml` en un editor de texto, cambiando sólo los valores de los atributos y elementos XML en la política de contraseña.
3. Guarde el archivo modificado.

   El cambio de política se realiza inmediatamente. No es necesario reiniciar el IBM Security Key Lifecycle Manager server.
4. Para comprobar los cambios, inicie una sesión en WebSphere Application Server como WASAdmin y cree un perfil de usuario para un nuevo usuario.

   Confirme que se acepte una contraseña que cumpla la política y que se rechace una contraseña que infrinja la política. Cuando haya terminado, si es necesario, suprima el perfil de usuario de prueba.

Cambio de una contraseña de usuario

La contraseña cambiada debe cumplir la política de contraseña que proporciona IBM Security Key Lifecycle Manager.

Acerca de esta tarea

Esta tarea utiliza el ID de usuario WASAdmin en la WebSphere Integrated Solutions Console para cambiar la contraseña de un usuario, incluida la contraseña del ID de usuario SKLMAdmin.

For more information about the commands that create groups and users, see the IBM WebSphere Application Server documentation (http://www.ibm.com/support/knowledgecenter/en/SSAW57_9.0.0/com.ibm.websphere.nd.multiplatform.doc/ae/rxml_atwimmgt.html).

Procedimiento

1. Inicie sesión en la consola WebSphere Integrated Solutions Console.
   - Interfaz gráfica de usuario:
     a. En la página de bienvenida del navegador, escriba un ID de usuario de `WASAdmin` y un valor de contraseña como, por ejemplo, `wasadminpw`.
     b. En el árbol de navegación, pulse **Usuarios y grupos** > **Gestionar usuarios**.
   - Command-line interface
     a. Go to the `<WAS_HOME>/bin` directory. For example,

        Windows
        ```
        cd drive:\Program Files\IBM\WebSphere\AppServer\bin
        ```

        Linux
        ```
        cd /opt/IBM/WebSphere/AppServer/bin
        ```

     b. Start the **wsadmin** interface by using an authorized user ID, such as WASAdmin. For example,

        Windows
        ```
        wsadmin.bat -username WASAdmin -password wasadminpw -lang jython
        ```

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

2. Cambie la contraseña de un usuario.
   - Interfaz gráfica de usuario:
     a. En el diálogo **Gestionar usuarios** > **Buscar usuarios**, pulse **Buscar**.
     b. En la tabla de criterios de búsqueda, efectúe una doble pulsación en un ID de usuario seleccionado. Por ejemplo, efectúe una doble pulsación en `myAdmin` como ID de usuario.
     c. En el diálogo Propiedades de usuario, cambie el valor de los campos **Contraseña** y **Confirmar contraseña**.
     d. Pulse **Aceptar**.
   - Interfaz de línea de mandatos:
     a. Escriba `updateUser` y especifique los valores necesarios. Por ejemplo, utilizando Jython, escriba en una línea:

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

        Donde:

        -uniqueName
        Especifica el nombre exclusivo del usuario con una contraseña que desea crear. (String, necesario)

Puede utilizar el mandato **searchUsers** para comprobar que el nombre identifica correctamente al usuario antes de cambiar la contraseña.

-password
Especifica la contraseña del usuario. (String, necesario)

La nueva contraseña debe cumplir la política de contraseña que proporciona IBM Security Key Lifecycle Manager.

-confirmPassword
Especifica la contraseña de nuevo para validar cómo se ha escrito para el parámetro de contraseña. (String, opcional)

Qué hacer a continuación

A continuación, valide que el usuario pueda iniciar una sesión. Finalice la sesión como WASAdmin. Inicie una sesión como el usuario y confirme que se acepte la contraseña modificada.

Restablecimiento de una contraseña

Debe ser el administrador que poder restablecer una contraseña correspondiente a IBM Security Key Lifecycle Manager o WebSphere Application Server.

Acerca de esta tarea

Puede restablecer la contraseña en el sistema en el que se ejecuta IBM Security Key Lifecycle Manager. Utilice estos pasos sólo cuando la contraseña del usuario se haya perdido. En todos los demás casos, utilice la interfaz gráfica de usuario para actualizar la contraseña.

Procedimiento

1. Inicie sesión con el ID de usuario del administrador local.
2. Realice copia de seguridad del archivo *WAS_HOME*/profiles/KLMProfile/config/cells/SKLMCell/fileRegistry.xml. Si cambia el valor de la contraseña cambiará este archivo de propiedades.
3. Cambie la contraseña.
   - Windows
     a. Inicie una sesión de **wsadmin** utilizando la sintaxis Jython. Por ejemplo, escriba:

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

     b. Restablezca la contraseña para el ID de usuario de SKLMAdmin:

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

        Nota:
        - Sólo el ID de usuario de WASAdmin u otro ID de usuario con autoridad de administrador de WebSphere Application Server pueden cambiar contraseñas utilizando el mandato **AdminTask.changeFileRegistryAccountPassword**.
        - Las contraseñas que cree utilizando el mandato **AdminTask.changeFileRegistryAccountPassword** no se validan con la política de contraseña configurada que proporciona IBM Security Key Lifecycle Manager.

Tras el restablecimiento de una contraseña perdida, el usuario debe establecer la contraseña utilizando la interfaz gráfica de usuario.

c. Guarde el cambio y salga:

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

- Linux

a. Inicie una sesión de **wsadmin** utilizando la sintaxis Jython. Por ejemplo, escriba en una línea:

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

b. Restablezca la contraseña para el ID de usuario de SKLMAdmin:

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

Nota:

– Sólo el ID de usuario de WASAdmin u otro ID de usuario con autoridad de administrador de IBM Security Key Lifecycle Manager pueden cambiar contraseñas utilizando el mandato **AdminTask.changeFileRegistryAccountPassword**.

– Las contraseñas que cree utilizando el mandato **AdminTask.changeFileRegistryAccountPassword** no se validan con la política de contraseña configurada que proporciona IBM Security Key Lifecycle Manager.

Tras el restablecimiento de una contraseña perdida, el usuario debe establecer la contraseña utilizando la interfaz gráfica de usuario.

c. Guarde el cambio y salga:

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

4. Detenga e inicie el servidor.

- Detener

Windows

```
stopServer.bat server1
```

Linux

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

- Iniciar

Windows

```
startServer.bat server1
```

Linux

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

5. Verifique que puede iniciar sesión como administrador especificado con la nueva contraseña.

Cómo cambiar la contraseña de IBM Security Key Lifecycle Manager

Utilice el ID de usuario de la aplicación de IBM Security Key Lifecycle Manager para cambiar la contraseña del usuario. La contraseña cambiada debe cumplir la política de contraseña que proporciona IBM Security Key Lifecycle Manager.

Acerca de esta tarea

Para obtener más información sobre los mandatos para cambiar contraseña, consulte la documentación de IBM WebSphere Application Server (http://www.ibm.com/support/knowledgecenter/SSAW57_9.0.0/com.ibm.websphere.nd.multiplatform.doc/ae/rxml_atwimmgt.html).

Procedimiento

1. Navegue a la página o el directorio correspondiente:
   - Interfaz de línea de mandatos:
     - En el directorio *WAS_HOME*/bin, inicie una sesión de wsadmin utilizando Jython. Inicie una sesión en wsadmin con un ID de usuario autorizado.

       Windows

       Vaya al directorio C:\Program Files\IBM\WebSphere\AppServer\bin y escriba:

       ```
       wsadmin.bat -username <usuario_SKLM>
       -password <contraseña_usuario_SKLM> -lang jython
       ```

       AIX o Linux

       Vaya al directorio /opt/IBM/WebSphere/AppServer/bin y escriba:

       ```
       ./wsadmin.sh -username <usuario_SKLM>
       -password <contraseña_usuario_SKLM> -lang jython
       ```
   - Interfaz gráfica de usuario:
     - Inicie una sesión en la interfaz gráfica de usuario.
2. Cambie la contraseña de un usuario.
   - Interfaz de línea de mandatos:
     - Ejecute el siguiente mandato:

       ```
       AdminTask.changeMyPassword('[-oldPassword <valor_contraseña_anterior>
       -newPassword
       <valor_nueva_contraseña> -confirmNewPassword <valor_nueva_contraseña>]')
       ```

       Ejemplo:

       ```
       AdminTask.changeMyPassword('[-oldPassword sklmadmin -newPassword
       Ibm12one
       -confirmNewPassword Ibm12One]')
       ```
   - Interfaz gráfica de usuario:
     a. En la barra de la cabecera, pulse el enlace **<Usuario de SKLM>**.
     b. Pulse **Cambiar contraseña**.
     c. En el diálogo Cambiar contraseña, escriba su **Contraseña actual**.
     d. Escriba la **Nueva contraseña**.
     e. Vuelva a escribir la nueva contraseña en el campo **Confirmar nueva contraseña**.
     f. Pulse **Cambiar contraseña**.

Creación de un grupo de dispositivos

Dependiendo de los requisitos de la organización, puede crear un grupo de dispositivos para gestionar un subconjunto de dispositivos que tienen un uso empresarial restringido como, por ejemplo, las LTO tape drives que utiliza una división individual. También puede crear un rol con un nombre que coincida con el nombre del grupo de dispositivos, respetando las mayúsculas y minúsculas. La coincidencia de nombres es sensible a las mayúsculas y minúsculas.

Acerca de esta tarea

Esta tarea utiliza el ID de usuario SKLMAdmin y la interfaz de IBM Security Key Lifecycle Manager para crear un grupo de dispositivos extra.

Your user ID must have either:

- The `securityOfficer` role
- Permission to the administrative actions (**klmAdminDeviceGroup**)

  If you have the **klmAdminDeviceGroup** permission, you can create, view, and delete a device group. It is not required that you first define a role for the device group. However, your other actions are limited by the permissions that you have. For example, if you have only **klmAdminDeviceGroup** permission, you cannot update the attributes after you create the device group.

Procedimiento

1. Inicie una sesión en IBM Security Key Lifecycle Manager.
   - Interfaz gráfica de usuario:

     En la página de bienvenida del navegador, escriba un ID de usuario `SKLMAdmin` y un valor de contraseña como, por ejemplo, `mypassword`.
   - Command-line interface
     a. Go to the *<WAS_HOME>*`/bin` directory. For example,

        Windows
        ```
        cd drive:\Program Files\IBM\WebSphere\AppServer\bin
        ```

        Linux
        ```
        cd /opt/IBM/WebSphere/AppServer/bin
        ```

     b. Start the **wsadmin** interface by using an authorized user ID, such as `SKLMAdmin`. For example,

        Windows
        ```
        wsadmin.bat -username SKLMAdmin -password mypwd -lang jython
        ```

        Linux
        ```
        ./wsadmin.sh -username SKLMAdmin -password mypwd -lang jython
        ```
   - Interfaz REST:
     – Abra un cliente REST.
2. Navegue a la página o el directorio correspondiente:
   - Interfaz gráfica de usuario:

     Pulse **Configuración avanzada** > **Grupo de dispositivos**.
     a. En la tabla Grupo de dispositivos, pulse **Crear**.
     b. En el diálogo Crear grupo de dispositivos, rellene los campos necesarios y pulse **Crear**.
   - En la interfaz de línea de mandatos, escriba:
     ```
     AdminTask.tklmDeviceGroupCreate('[-name myLTO -deviceFamily LTO]')
     ```
   - Interfaz REST:
     a. Obtenga un identificador de autenticación de usuario exclusivo para acceder a los servicios REST de IBM Security Key Lifecycle Manager. Para obtener más información sobre el proceso de autenticación, consulte Proceso de autenticación de los servicios REST.
     b. Para invocar el **Servicio REST Crear grupo de dispositivos**, envíe solicitud HTTP POST. Pase el identificador de autenticación de usuario que ha obtenido en el `Paso a` junto con el mensaje de solicitud, como se muestra en el ejemplo siguiente.

```
POST https://localhost:<puerto>/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. Asegúrese de que el grupo de dispositivos exista.
   - Interfaz gráfica de usuario:

     En la página de gestión de grupos de dispositivos, explore la tabla de grupo de dispositivos para localizar el grupo de dispositivos.
   - En la interfaz de línea de mandatos, escriba:

     ```
     print AdminTask.tklmDeviceGroupList ('[-name myLTO -v y]')
     ```
   - Interfaz REST:

     Enviar la siguiente solicitud HTTP GET utilizando un cliente REST:

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

Qué hacer a continuación

Crear un rol con un nombre que coincide con el grupo de dispositivos.

Creación de un rol para un nuevo grupo de dispositivos

Cuando cree un nuevo grupo de dispositivos de IBM Security Key Lifecycle Manager, cree también un rol para el grupo de dispositivos. Especifique el mismo nombre para el grupo de dispositivos y el rol, incluidas las mayúsculas y minúsculas. La coincidencia de nombres es sensible a las mayúsculas y minúsculas.

Acerca de esta tarea

Puede añadir el rol de un grupo de dispositivos en el WebSphere Application Server editando el archivo de configuración `admin-authz.xml`.

Procedimiento

1. En el sistema operativo de Windows, edite el archivo *<WAS_HOME>*`/perfiles/KLMProfile/cofig/cells/SKLMCell/admin-authz.xml` añadiendo las líneas siguientes:

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

   Los valores de `roleId` y `roleAssignmentId` deben ser exclusivos en los roles y autorizaciones que existen en el archivo `admin-authz.xml`.

   Por ejemplo, debe añadir las líneas siguientes si se agrega un nuevo grupo de dispositivos, por ejemplo, `MyDS5K`:

   ```
   <roles xmi:id="MyDS5K_Role" roleName="MyDS5K"/>
   <authorizations xmi:id="MyDS5K_Role_Auth" role="MyDS5K_Role"/>
   ```
2. Reinicie WebSphere Application Server. Debe detener el servidor y, a continuación, volver a iniciarlo. Para obtener instrucciones sobre cómo detener e iniciar el servidor, consulte el apartado “Reinicio de IBM Security Key Lifecycle Manager server” en la página 205.

Qué hacer a continuación

A continuación, puede especificar que un grupo de usuarios tenga permisos en el nuevo grupo de dispositivos y las tareas administrativas necesarias como, por ejemplo, ver o configurar.

Administración de base de datos

El proceso de instalación proporciona un ID de usuario de administrador predeterminado con la contraseña y los permisos necesarios.

Debe garantizar que el ID de usuario permanezca activo y cumpla la política de seguridad que está activa en el sistema.

Movimiento de los archivos de registro de transacciones de Db2 para aumentar el rendimiento

Mueva periódicamente los registros transaccionales de Db2 antiguos que crea la base de datos de IBM Security Key Lifecycle Manager. De lo contrario, un gran número de registros transaccionales puede afectar al rendimiento.

Acerca de esta tarea

Los registros de transacciones de Db2 se encuentran en estos directorios:

Sistemas Windows:

INSTANCEHOME:\sklmdbarchive\sklmdb31\SKLMDB301\NODE0000\LOGSTREAM0000\C0000000

donde:

- *INSTANCEHOME* es la letra de unidad que ha especificado durante la instalación.
- sklmdb31 es el propietario de la instancia de base de datos.
- sklmdb31 es el nombre de la base de datos de IBM Security Key Lifecycle Manager.
- NODE0000, LOGSTREAM0000 y C0000000 pueden ser distintos en su sistema.

Sistemas como Linux o AIX:

~sklmdbarchive/sklmdb301/sklmdb31/NODE0000/LOGSTREAM0000/C0000000

donde:

- sklmdb31 es el propietario de la instancia de base de datos.
- sklmdb31 es el nombre de la base de datos de IBM Security Key Lifecycle Manager.
- NODE0000, LOGSTREAM0000 y C0000000 pueden ser distintos en su sistema.

Si IBM Security Key Lifecycle Manager gestiona un gran número de claves y la partición de disco que contiene el directorio sklmdbarchive tiene poco espacio de disco libre, mueva los registros de transacciones antiguos a otra partición de disco.

Nota: Cuando realice esta tarea, tenga cuidado de no mover el registro activo actual.

Siga estos pasos periódicamente:

Procedimiento

1. Cree una copia de seguridad IBM Security Key Lifecycle Manager mediante la interfaz gráfica de usuario, la interfaz de línea de mandatos o la interfaz REST. De lo contrario, la siguiente copia de seguridad puede fallar.
2. Inicie una sesión como el propietario de la instancia de base de datos en sistemas como Linux o AIX, o como el administrador de Db2 en los sistemas Windows.
3. Cree un directorio en otra partición que tenga suficiente espacio de disco, donde pueda mover los archivos de registro antiguos.
4. Identifique el primer registro activo. Escriba:

   Sistemas Windows:

   ```
   db2cmd
   SET DB2INSTANCE=sklmdb31
   db2 get db cfg for SKLMDB31
   ```

   Sistemas como Linux o AIX:

   ```
   db2 get db cfg for SKLMDB31
   ```

   El valor del parámetro de configuración `First active log file` identifica el primer registro activo.
5. Mueva los archivos de registro que se han modificado antes que el primer registro activo del directorio `sklmdbarchive` al nuevo directorio.

   Los registros se denominan S*nnnnnnn*`.LOG`. Normalmente, los registros con los números más bajos se han creado antes que los registros con los números más altos. La excepción es si la base de datos ya ha creado un registro denominado `S99999999.LOG`. En este caso, la numeración vuelve a empezar en `S0000000.LOG`.

   Nota: La ejecución de una operación de restauración elimina el directorio `sklmdbarchive` y crea un nuevo directorio.

Problemas de seguridad con la contraseña de Db2 en sistemas Windows

En sistemas Windows, el ID de usuario y la contraseña del administrador de Db2 están sujetos a la política de seguridad que esté activa en el sistema.

Si hay una restricción de caducidad de contraseña en vigor, deberá cambiar la contraseña de inicio de sesión y la contraseña de Db2 para el ID de usuario del administrador antes de la fecha de caducidad.

Además, la contraseña de inicio de sesión para el ID de usuario del administrador de Db2 y la contraseña del origen de datos de Db2 utilizadas por WebSphere Application Server deben ser la misma. Cuando se cambia una, deberá cambiar la otra.

Ejecute los pasos siguientes para cambiar la contraseña de la base de datos de Db2:

1. Detenga WebSphere Application Server y *todos* los servicios de Windows que estén relacionados con Db2.
2. Abra la herramienta de gestión de usuarios de Windows abriendo el Panel de control y pulsando **Herramientas administrativas** > **Administración de equipos** > **Usuarios y grupos locales** > **Usuarios**.
3. Cambie la contraseña del propietario de la base de datos de IBM Security Key Lifecycle Manager.

4. Abra la consola Servicios de Windows abriendo el Panel de control y pulsando **Herramientas administrativas > Administración de equipos**.
5. En los siguientes servicios, cambie la contraseña utilizando el separador **Inicio de sesión** del recuadro de diálogo **Propiedades**:
   - DB2 - DB2SKLMV301 - *sklminstance*

     Por ejemplo, con el nombre de instancia predeterminado, el valor de *sklminstance* es:

     DB2 - DBSKLMV301 - SKLMDB31

   Cuando haya cambiado las contraseñas de todos los servicios, reinicie los servicios.

   Los siguientes servicios se deben detener y reiniciar. El cambio de contraseña no es necesario:
   - Db2 License Server (DBSKLMV31)
   - Db2 Management Service (DBSKLMV31)
   - Db2 Governor (DBSKLMV31)
   - DB Remote Command Server (DBSKLMV31)
6. Inicie WebSphere Application Server.
7. Si utiliza la interfaz **wsadmin** que proporciona WebSphere Application Server, especifique la sintaxis Jython.

   Windows

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

   Linux

   ```
   ./wsadmin.sh -username WASAdmin -password mypwd -lang jython
   ```
8. Use the **wsadmin** command to change the password of the WebSphere Application Server data source:
   a. The following command lists JAASAuthData entries:

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

      The result might be:

      ```
      (cells/SKLMCell|security.xml#JAASAuthData_1379859888963)
      ```
   b. Identify the data source ID with the alias that matches the string sklm_db. Also, identify the data source ID with the alias that matches the string sklmdb:

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

      For example, type on one line:

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

      The result is:

      ```
      sklm_db
      ```
   c. Change the password of the sklm_db alias, entering this command on one line:

      ```
      print AdminConfig.modify('JAASAuthData_list_entry','[[password passw0rd]]')
      ```

      If you specify special characters in the password, use quotation marks as delimiters when you specify the password value.

      For example, type on one line:

      ```
      print AdminConfig.modify('(cells/SKLMCell|security.xml#JAASAuthData_1379859888963)','[[pass
      ```
   d. Save the changes:

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

e. Stop and restart the IBM Security Key Lifecycle Manager server by using the **stopServer** and **startServer** commands.

   Alternatively, stop and restart the IBM Security Key Lifecycle Manager server by using Windows Computer Management.

   1) Open the Control Panel and click **Administrative Tools** > **Computer Management** > **Services and Applications** > **Services**.
   2) Stop and start the IBM Security Key Lifecycle Manager server service, which has a name like `IBM WebSphere Application Server V9.0 - SKLM301Server`.

f. Verify that you can connect to the database by using the WebSphere Application Server data source.

   1) First, type:

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

      The result might be:

      ```
      "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) Test the connection on the first data source. For example, type:

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

      For example, type on one line:

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

   3) Test the connection on the remaining data source. For example, type:

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

   4) In both cases, you receive a message that the connection to the data source was successful. For example:

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

      Now you can run an IBM Security Key Lifecycle Manager operation.

Problemas de seguridad con la contraseña de Db2 en sistemas Linux o AIX

En sistemas Linux o AIX, es posible que desee cambiar la contraseña para el ID de usuario del administrador de Db2. La contraseña de inicio de sesión para el ID de usuario del administrador de Db2 y la contraseña de Db2 para el ID de usuario deben ser la misma.

El programa de instalación IBM Security Key Lifecycle Manager instala Db2 y solicita a la persona que realiza la instalación una contraseña para el usuario denominado `sklmdb31`. Además, la aplicación Db2 crea una entrada de usuario del sistema operativo denominada `sklmdb31`. Por ejemplo, la contraseña para este usuario podría caducar, lo que requerirá que vuelva a sincronizar la contraseña para ambos ID de usuario.

Antes de cambiar la contraseña para el ID de usuario del administrador de Db2, debe cambiar la contraseña del usuario a nivel de sistema operativo.

1. Inicie sesión en el IBM Security Key Lifecycle Manager server como usuario root.
2. Cambie el usuario a la entrada de usuario del sistema `sklmdb31`. Escriba:

   ```
   su sklmdb31
   ```

3. Cambie la contraseña. Escriba:

   ```
   passwd
   ```

   Especifique la nueva contraseña.
4. Salga para volver al usuario root.

   ```
   exit
   ```

5. En el directorio *WAS_HOME*/bin, utilice la interfaz **wsadmin** que proporciona WebSphere Application Server para especificar la sintaxis Jython.

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

6. Cambie la contraseña para el origen de datos de WebSphere Application Server:
   a. El siguiente mandato muestra las entradas de JAASAuthData:

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

      El resultado podría parecerse a este ejemplo:

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

   b. Escriba el mandato **AdminConfig.showall** de cada entrada para localizar el alias sklm_db. Por ejemplo, escriba en una línea:

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

      El resultado sería como el de este ejemplo:

      ```
      {alias sklm_db}
      {description "SKLM database user j2c authentication alias"}
      {password *****}
      {userId sklmdb31}
      ```

      Y también escriba en una línea:

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

      El resultado sería como el de este ejemplo:

      ```
      {alias sklmdb}
      {description "SKLM database user J2C authentication alias"}
      {password *****}
      {userId sklmdb31}
      ```

   c. Cambie la contraseña del alias sklm_db que tiene el identificador JAASAuthData_**1228871756187**:

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

      Por ejemplo, escriba en una línea:

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

   d. Cambie la contraseña del alias sklmdb que tiene el identificador JAASAuthData_**1228871757843**:

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

      Por ejemplo, escriba en una línea:

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

   e. Guarde los cambios:

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

f. Salga para volver al usuario root.

```
exit
```

g. En el directorio *WAS_HOME*/bin, detenga la aplicación WebSphere Application Server. Por ejemplo, como WASAdmin, escriba en una línea:

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

El resultado sería como el de este ejemplo:

```
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. Inicie la aplicación WebSphere Application Server. Como administrador de WebSphere Application Server, escriba en una línea:

```
startServer.sh server1
```

i. En el directorio *WAS_HOME*/bin, utilice la interfaz **wsadmin** que proporciona WebSphere Application Server para especificar la sintaxis Jython.

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

j. Compruebe que puede conectarse a la base de datos utilizando el origen de datos de WebSphere Application Server.

1) Primero, consulte una lista de los orígenes de datos. Escriba:

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

El resultado podría parecerse al del siguiente ejemplo:

```
"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) Escriba:

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

Por ejemplo, escriba en una línea:

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

3) Pruebe la conexión en el otro origen de datos. Por ejemplo, escriba:

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

4) En ambos casos, recibirá un mensaje informándole de que la conexión al origen de datos ha sido correcta. Por ejemplo:

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

Detención del Db2 server

Para detener el servidor de bases de datos, detenga el WebSphere Application Server y detenga el Db2 server.

Acerca de esta tarea

Debe ser el propietario de la instancia de la base de datos en sistemas AIX o Linux, o el administrador local en sistemas Windows.

Procedimiento

1. Inicie sesión como propietario de la instancia de la base de datos en sistemas como AIX o Linux, o inicie sesión como administrador local en sistemas Windows.
2. Detenga WebSphere Application Server. Escriba este mandato:

   Sistemas Windows

   ```
   cd C:\Program Files\IBM\WebSphere\AppServer\bin
   .\stopServer.bat server1 -username wasadmin
     -password micontraseñasecreta
   ```

   Sistemas AIX o Linux

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

3. Detenga Db2 server. Escriba estos mandatos.

   Sistemas Windows

   ```
   set DB2INSTANCE=sklmdb31
   db2stop
   ```

   Sistemas AIX o Linux

   ```
   su -sklmdb31
   db2stop
   ```

Cambio del nombre de host del Db2 server

Después de cambiar el nombre de host del sistema IBM Security Key Lifecycle Manager, debe cambiar el nombre de host del Db2 server.

Acerca de esta tarea

Encontrará los pasos a seguir para cambiar el nombre de host correspondiente a su nivel de Db2 server en la nota técnica de esta dirección web: 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

Cambio del nombre de host del WebSphere Application Server existente

Debe cambiar el nombre de host de WebSphere Application Server antes de cambiar el nombre de host del sistema.

Procedimiento

1. Cambie el nombre de host de WebSphere Application Server. Para obtener más información sobre cómo cambiar el nombre de host, consulte la documentación de IBM WebSphere Application Server (http://www.ibm.com/support/knowledgecenter/SSEQTP_9.0.0/com.ibm.websphere.base.doc/ae/tagt_hostname.html).
2. Cuando haya finalizado satisfactoriamente esta tarea, cambie el nombre de host del servidor DB2. Para obtener más información, consulte “Cambio del nombre de host del Db2 server”.

Gestión de una LTO tape drive

Puede gestionar las LTO tape drives utilizando IBM Security Key Lifecycle Manager.

Pasos guiados para crear grupos de claves y unidades

Cuando crea por primera vez grupos de claves y unidades, y posteriormente cuando añade grupos de claves y unidades adicionales, IBM Security Key Lifecycle Manager proporciona un conjunto guiado de pasos para completar la tarea.

Es posible que en las descripciones de algunos pasos se mencionen alternativas de línea de mandatos y de interfaz REST para la misma tarea. En un conjunto guiado de tareas, utilice la interfaz gráfica de usuario para completar las tareas.

Creación de un grupo de claves

Como primera actividad, cree claves y grupos de claves para IBM Security Key Lifecycle Manager. Antes de empezar, determine la cantidad de claves y el objetivo de los grupos de claves individuales que necesita la organización.

Acerca de esta tarea

Puede utilizar el diálogo Crear un grupo de claves. O bien, puede utilizar el mandato **tklmGroupCreate** o el **Servicio REST Crear grupo** para crear un grupo al que desea añadir claves. A continuación, utilice el mandato **tklmSecretKeyCreate** o el **Servicio REST Crear clave secreta** para crear una o más claves simétricas en el grupo existente. Your role must have a permission to the create action and a permission to the appropriate device group.

Procedimiento

1. Vaya a la página o el directorio correspondiente:
   - Interfaz gráfica de usuario:
     a. Inicie una sesión en la interfaz gráfica de usuario.
     b. En la sección clave y dispositivo sección Gestión de claves y dispositivos en la página de bienvenida, seleccione **LTO**.
     c. Pulse **Ir a** > **Creación guiada de claves y dispositivos**.
     d. O bien, pulse el botón derecho del ratón **LTO** y seleccione **Creación guiada de claves y dispositivos**.
   - Command-line interface
     a. Go to the <*WAS_HOME*>/bin directory. For example,

        Windows
        ```
        cd drive:\Program Files\IBM\WebSphere\AppServer\bin
        ```

        Linux
        ```
        cd /opt/IBM/WebSphere/AppServer/bin
        ```

     b. Start the **wsadmin** interface by using an authorized user ID, such as SKLMAdmin. For example,

        Windows
        ```
        wsadmin.bat -username SKLMAdmin -password mypwd -lang jython
        ```

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

   - Interfaz REST:
     – Abra un cliente REST.
2. Cree un grupo de claves:

- Interfaz gráfica de usuario:
  a. En la página Paso 1: crear grupos de claves, pulse **Crear** en la tabla **Grupo de claves**.
  b. En el diálogo Crear un grupo de claves, especifique valores para los parámetros necesarios y opcionales. Por ejemplo, puede crear un grupo de claves que contenga 100 claves.
  c. Pulse **Crear grupo de claves**.
- Interfaz de línea de mandatos:
  a. Primero, cree un grupo al que puede añadir claves.

     Escriba `tklmGroupCreate` para crear un grupo. Por ejemplo, escriba:

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

  b. A continuación, utilice el mandato **`tklmGroupList`** para obtener el valor de uuid del grupo que ha creado. Por ejemplo, escriba:

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

  c. A continuación, cree un grupo de claves y almacénelas en el grupo. Por ejemplo, escriba:

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

- Interfaz REST:
  a. Obtenga un identificador de autenticación de usuario exclusivo para acceder a los servicios REST de IBM Security Key Lifecycle Manager. Para obtener más información sobre el proceso de autenticación, consulte Proceso de autenticación de los servicios REST.
  b. Para ejecutar el **`Servicio REST Crear grupo`**, envíe la solicitud HTTP POST. Pase el identificador de autenticación de usuario que ha obtenido en el `Paso a` junto con el mensaje de solicitud, como se muestra en el ejemplo siguiente.

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

  c. Utilice el **`Servicio REST Enumerar grupos`** para obtener el valor de uuid del grupo que ha creado. Por ejemplo,

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

  d. A continuación, cree un grupo de claves y almacénelas en el grupo utilizando el **`Servicio REST Crear clave secreta`**. Por ejemplo, puede enviar la siguiente solicitud HTTP:

     ```
     POST https://localhost:<puerto>/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"}
     ```

Qué hacer a continuación

Realice una copia de seguridad de nuevas claves antes de que las claves se sirvan a los dispositivos. Puede ir al siguiente paso guiado para definir dispositivos específicos y asociar grupos de claves con los dispositivos. Seleccione **Paso 2: Identificar las unidades** o pulse **Ir al paso siguiente**.

Identificación de unidades

Identifique una LTO tape drive para utilizarla con IBM Security Key Lifecycle Manager.Antes de empezar, cree los grupos de claves que desee asociar con las unidades de cinta que ha identificado.

Acerca de esta tarea

Puede utilizar el diálogo Añadir unidad de cintas, el mandato **tklmDeviceAdd** o el **Servicio REST Añadir dispositivo** para añadir un dispositivo. Your role must have a permission to the create action and a permission to the appropriate device group.

Puede realizar cualquiera de las siguientes opciones para servir claves a dispositivos.

Only accept manually added devices for communication
All incoming devices are not added to the data store. You must manually specify key service to each device.

Hold new device requests pending my approval
All incoming devices of a valid device group are added to the device store, but are not automatically served keys upon request. You must accept or reject a device in the pending devices list before the device is served keys upon request.

Automatically accept all new device requests for communication
All new incoming devices of a valid device group are added to the data store and are automatically served keys upon request.

Nota: Do not use this setting if you intend to move the new device to another device group. Instead, select manual or pending approval mode to allow an opportunity to move the device into the appropriate device group before any keys are served.

Any setting is acceptable if there are no device groups. However, if device groups are specified:

Determine si desea que IBM Security Key Lifecycle Manager acepte automáticamente las solicitudes de todas las unidades. Para aumentar la seguridad, una vez descubiertas todas las unidades, puede desactivar esta opción para un entorno de producción.

Procedimiento

1. Vaya a la página o el directorio correspondiente:
   - Interfaz gráfica de usuario:
     a. Inicie una sesión en la interfaz gráfica de usuario.
     b. En la sección clave y dispositivo sección Gestión de claves y dispositivos en la página de bienvenida, seleccione **LTO**.
     c. Pulse **Ir a** > **Creación guiada de claves y dispositivos**.

d. O bien, pulse el botón derecho del ratón **LTO** y seleccione **Creación guiada de claves y dispositivos**.

- Command-line interface

a. Go to the *<WAS_HOME>*/bin directory. For example,

Windows

```
cd drive:\Program Files\IBM\WebSphere\AppServer\bin
```

Linux

```
cd /opt/IBM/WebSphere/AppServer/bin
```

b. Start the **wsadmin** interface by using an authorized user ID, such as SKLMAdmin. For example,

Windows

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

Linux

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

- Interfaz REST:
  - Abra un cliente REST.

2. Omita la página Crear grupos de claves. Pulse el enlace **Ir al paso siguiente** o pulse **Paso 2: Identificar las unidades**.
3. Puede especificar que IBM Security Key Lifecycle Manager retenga las nuevas solicitudes de dispositivo para su aprobación.
   - Interfaz gráfica de usuario:

     Seleccione **Retener las solicitudes de dispositivos nuevos pendientes de aprobación**.
   - Interfaz de línea de mandatos:

     Utilice el mandato **tklmDeviceGroupAttributeUpdate** o el **Servicio REST Actualizar atributos de grupo de dispositivos** para establecer el valor del atributo **device.AutoPendingAutoDiscovery**. Por ejemplo, escriba:

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

     For an LTO device group, use the **tklmDeviceGroupAttributeUpdate** command to specify a key group by using the **symmetricKeySet** attribute in the IBM Security Key Lifecycle Manager database.
   - Interfaz REST:

     a. Obtenga un identificador de autenticación de usuario exclusivo para acceder a los servicios REST de IBM Security Key Lifecycle Manager. Para obtener más información sobre el proceso de autenticación, consulte Proceso de autenticación de los servicios REST.

     b. Para ejecutar el **Servicio REST Actualizar atributos de grupo de dispositivos** y establecer el valor del atributo **device.AutoPendingAutoDiscovery**, envíe la solicitud HTTP PUT. Pase el identificador de autenticación de usuario que ha obtenido en el Paso a junto con el mensaje de solicitud, como se muestra en el ejemplo siguiente.

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

4. Añada un dispositivo:
   - Interfaz gráfica de usuario:

a. En la página Paso 2: Identificar las unidades, en la tabla **Dispositivos**, pulse **Añadir**.
b. En el diálogo Añadir unidad de cintas, escriba la información necesaria y opcional.
c. Pulse **Añadir unidad de cintas**.

- Interfaz de línea de mandatos:

  Escriba `tklmDeviceAdd` para añadir un dispositivo. Debe especificar el grupo de dispositivos y el número de serie. Por ejemplo, escriba:

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

- Interfaz REST:

  Puede utilizar el **Servicio REST Añadir dispositivo** para agregar un dispositivo. Por ejemplo, puede enviar la siguiente solicitud HTTP:

  ```
  POST https://localhost:<puerto>/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"}
  ```

Qué hacer a continuación

A continuación, puede utilizar la página Key and Device Management de LTO para ver todos los grupos de claves y dispositivos.

Gestión de claves, grupos de claves y unidades

Para administrar claves, grupos de claves y dispositivos, debe correlacionar grupos de claves con unidades. Puede añadir, modificar o suprimir claves específicas, grupos de claves o dispositivos.

Acerca de esta tarea

Utilice Key and Device Management de LTO para correlacionar grupos de claves con dispositivos. Puede añadir, modificar o suprimir claves específicas, grupos de claves o dispositivos. Your role must have a permission to the view action and a permission to the appropriate device group.

Para cambiar la visualización de la información, seleccione:

Visualizar grupos de claves y unidades
Visualice los nombres de los grupos de claves y los números de serie de las unidades. Asimismo, esta vista muestra el grupo de claves, la clave o el valor predeterminado del sistema que utiliza una unidad.

Visualizar claves, pertenencia a grupos de claves y unidades
Visualice las claves y la pertenencia de la clave en grupos de claves. Asimismo, esta vista muestra los números de serie de la unidad y el grupo de claves, la clave o el valor predeterminado del sistema que utiliza una unidad.

Antes de empezar, examine las columnas de la página, que proporciona botones para añadir, modificar o suprimir un elemento de tabla. Para ordenar la información, pulse una cabecera de columna.

La tabla está organizada en estas áreas:

- En las columnas de la izquierda, se incluye información sobre las claves o los grupos de claves.

  Para una clave, la información indica de qué grupo de claves es miembro la clave. Para un grupo de claves, la información indica si el grupo de claves se utiliza como valor predeterminado y el número de claves del grupo.
- En las columnas de la derecha, se incluye información sobre las unidades.

  La información indica el número de serie de la unidad, y el grupo de claves o la clave específica que utiliza la unidad. Por ejemplo, una unidad puede utilizar el grupo de claves Valor predeterminado del sistema.
- Los iconos indican el tipo de claves.

Tabla 2. Iconos y su significado

Icono	Descripción
	Una clave simétrica o una clave privada. Una clave privada es una clave asimétrica de un par de claves con una clave pública y una clave privada.
	Un grupo de claves

Procedimiento

1. Inicie una sesión en la interfaz gráfica de usuario:
   a. En la sección clave y dispositivo sección Gestión de claves y dispositivos en la página de bienvenida, seleccione **LTO**.
   b. Pulse **Ir a** > **Gestionar claves y dispositivos**.
   c. O bien, pulse con el botón del ratón derecho en **LTO** y seleccione **Gestionar claves y dispositivos**.

   Descriptions of some steps describe alternatives by using the graphical user interface, command-line interface, or the REST interface. For any one work session, do not switch between interfaces.

   Descriptions of some tasks might mention task-related properties in the `SKLMConfig.properties` file. Use the graphical user interface, command-line interface, or REST interface to change these properties.
2. En Key and Device Management de LTO, puede añadir, modificar o suprimir una clave, un grupo de claves o una unidad.

   Puede realizar las siguientes tareas administrativas:

   - Renovar la lista.

     Click the refresh icon  to refresh items in the table.
   - Añadir

     Pulse **Añadir**. De manera alternativa, puede seleccionar un proceso paso a paso para crear grupos de claves y unidades.

     – Grupo de claves

       En el diálogo **Crear un grupo de claves**, especifique la información necesaria como, por ejemplo, el nombre del grupo de claves. También puede especificar que este grupo sirva claves como el grupo de claves predeterminado. Sólo puede haber un grupo de claves predeterminado. A continuación, pulse **Crear un grupo de claves**. Your role must have a permission to the create action and a permission to the appropriate device group.

– Unidad de cintas

  En el diálogo Añadir unidad de cintas, escriba el número de serie de la unidad y otra información. A continuación, pulse **Añadir unidad de cintas**. Your role must have a permission to the create action and a permission to the appropriate device group.

– Utilizar el proceso paso a paso para la creación de grupos de claves, claves y unidades

  En las páginas Paso 1: Crear grupos de claves y Paso 2: Identificar unidades, especifique la información necesaria y pulse el botón correspondiente para completar la tarea.

El indicador de éxito varía, y muestra un grupo de claves o un dispositivo.

- Modificar

  Para cambiar un grupo de claves, una clave o una unidad, seleccione el grupo de claves, la clave o la unidad y pulse **Modificar**. O bien, pulse con el botón derecho del ratón en el grupo de claves, la clave o la unidad que haya seleccionado. A continuación, pulse **Modificar**.

  – Grupo de claves

    Especifique cambios en el diálogo Modificar grupo de claves. A continuación, pulse **Modificar grupo de claves**. Your role must have a permission to the modify action and a permission to the appropriate device group.

  – Clave

    Especifique cambios en el diálogo Modificar la pertenencia de la clave. A continuación, pulse **Modificar la pertenencia de la clave**. Your role must have a permission to the modify action and a permission to the appropriate device group.

  – Unidad de cintas

    Especifique cambios en el diálogo Modificar unidad de cintas. A continuación, pulse **Modificar unidad de cintas**. Your role must have a permission to the modify action and a permission to the appropriate device group.

  El indicador de éxito varía, y muestra un cambio en una columna para el grupo de claves, la clave o el dispositivo. Los cambios en la información opcional como, por ejemplo, el valor de una descripción de unidad puede que no se incluyan en la tabla.

- Suprimir

  Para suprimir un grupo de claves, una clave o una unidad, seleccione la clave, el grupo de claves o la unidad y pulse **Suprimir**. O bien, pulse con el botón derecho del ratón en el grupo de claves, la clave o la unidad que haya seleccionado. A continuación, pulse **Suprimir**.

  – Grupo de claves

    No puede suprimir un grupo de claves que esté asociado con un dispositivo, ni un grupo de claves que esté marcado como valor predeterminado. Al suprimir un grupo de claves lleno *también se suprimirán todas las claves* del grupo.

    Para confirmar la supresión, pulse **Aceptar**. Your role must have a permission to the delete action and a permission to the appropriate device group.

  – Clave

    La supresión de una clave la elimina de cualquier grupo de claves con el que esté asociada. Para confirmar la supresión, pulse **Aceptar**. No puede

suprimir una clave que esté asociada con una unidad. Your role must have a permission to the delete action and a permission to the appropriate device group.

– Unidad de cintas

Los metadatos de la unidad que suprime, por ejemplo, el número de serie de la unidad, se eliminan de la base de datos de IBM Security Key Lifecycle Manager. Para confirmar la supresión, pulse **Aceptar**. Your role must have a permission to the delete action and a permission to the appropriate device group.

El indicador de éxito es la supresión del grupo de claves, la clave o dispositivo de la tabla de gestión.

Adición de una clave o un grupo de claves

Puede añadir más claves o grupo de claves para su uso con IBM Security Key Lifecycle Manager.Antes de empezar, determine la política del sitio sobre los grupos de claves predeterminados y la denominación de los prefijos de clave.

Acerca de esta tarea

Puede utilizar el diálogo Crear un grupo de claves. O bien, puede utilizar primero el mandato **tklmGroupCreate** o el **Servicio REST Crear grupo** para crear un grupo al que añadir las claves y, a continuación, utilizar el mandato **tklmSecretKeyCreate** o el **Servicio REST Crear clave secreta** para crear una o varias claves simétricas en el grupo existente. Your role must have a permission to the create action and a permission to the appropriate device group.

Procedimiento

1. Vaya a la página o el directorio correspondiente:
   - Interfaz gráfica de usuario:
     a. Inicie una sesión en la interfaz gráfica de usuario.
     b. En la sección clave y dispositivo sección Gestión de claves y dispositivos en la página de bienvenida, seleccione **LTO**.
     c. Pulse **Ir a** > **Gestionar claves y dispositivos**.
     d. O bien, pulse con el botón del ratón derecho en **LTO** y seleccione **Gestionar claves y dispositivos**.
     e. En la página de gestión para LTO, pulse **Añadir**.
     f. Pulse **Grupo de claves**.
   - Command-line interface
     a. Go to the *<WAS_HOME>*/bin directory. For example,

        Windows
        ```
        cd drive:\Program Files\IBM\WebSphere\AppServer\bin
        ```

        Linux
        ```
        cd /opt/IBM/WebSphere/AppServer/bin
        ```

     b. Start the **wsadmin** interface by using an authorized user ID, such as SKLMAdmin. For example,

        Windows
        ```
        wsadmin.bat -username SKLMAdmin -password mypwd -lang jython
        ```

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

2. Cree una clave o un grupo de claves:
   - Interfaz gráfica de usuario

a. En el diálogo Crear un grupo de claves, especifique valores para los parámetros necesarios y opcionales. Por ejemplo, de manera opcional, puede especificar que este grupo de claves sea el valor predeterminado.
b. Pulse **Crear grupo de claves**.

- Interfaz de línea de mandatos:
  a. Primero, cree un grupo al que puede añadir claves.

     Escriba **tklmGroupCreate** para crear un grupo que tenga un tipo de grupo de claves. Por ejemplo, escriba:

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

  b. A continuación, utilice el mandato **tklmGroupList** para obtener el valor de uuid del grupo que ha creado. Por ejemplo, escriba:

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

  c. A continuación, cree un grupo de claves y almacénelas en el grupo. Por ejemplo, escriba:

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

- Interfaz REST:
  a. Cree un grupo al que puede añadir claves mediante el **Servicio REST Crear grupo**.

     Por ejemplo, puede enviar la siguiente solicitud HTTP utilizando un cliente REST:

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

  b. Utilice el **Servicio REST Enumerar grupos** para obtener el valor de uuid del grupo que ha creado. Por ejemplo, puede enviar la siguiente solicitud HTTP:

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

  c. Cree un grupo de claves y almacénelas en el grupo utilizando el **Servicio REST Crear clave secreta**. Por ejemplo, puede enviar la siguiente solicitud HTTP:

     ```
     POST https://localhost:<puerto>/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"}
     ```

Qué hacer a continuación

Realice una copia de seguridad de nuevas claves antes de que las claves se sirvan a los dispositivos. También puede asociar grupos de claves con dispositivos específicos.

Especificación de un grupo de claves de aplazamiento

Puede especificar un grupo de claves para uso futuro como valor predeterminado del sistema.

Acerca de esta tarea

Puede utilizar la interfaz gráfica de usuario, el mandato **tklmKeyGroupDefaultRolloverAdd** o el **Servicio REST Añadir el aplazamiento predeterminado de grupo de claves** para añadir un aplazamiento de grupo de claves predeterminado en una fecha específica para servir claves a un grupo de dispositivos. Your role must have a permission to the create action and a permission to the appropriate device group.

Procedimiento

1. Vaya a la página o el directorio correspondiente:
   - Interfaz gráfica de usuario:
     a. Inicie una sesión en la interfaz gráfica de usuario.
     b. En la sección clave y dispositivo sección Gestión de claves y dispositivos en la página de bienvenida, seleccione **LTO**.
     c. Pulse **Ir a** > **Gestionar aplazamiento predeterminado**.
     d. O bien, pulse con el botón del ratón derecho en **LTO** y seleccione **Gestionar aplazamiento predeterminado**.
   - Command-line interface
     a. Go to the <*WAS_HOME*>/bin directory. For example,

        Windows
        ```
        cd drive:\Program Files\IBM\WebSphere\AppServer\bin
        ```

        Linux
        ```
        cd /opt/IBM/WebSphere/AppServer/bin
        ```

     b. Start the **wsadmin** interface by using an authorized user ID, such as SKLMAdmin. For example,

        Windows
        ```
        wsadmin.bat -username SKLMAdmin -password mypwd -lang jython
        ```

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

2. Especifique un grupo de claves existente como valor predeterminado del sistema en el futuro.
   - Interfaz gráfica de usuario:
     a. En la página de gestión para LTO, pulse **Añadir**.
     b. En el diálogo Añadir valor predeterminado de escritura futuro, especifique la información.
     c. Pulse **Añadir valor predeterminado de escritura futuro**.

     Nota:
     - No especifique dos valores predeterminados para la misma fecha de aplazamiento.
     - Si un grupo de claves no existe en el momento del aplazamiento, IBM Security Key Lifecycle Manager continúa utilizando el grupo de claves predeterminado actual.
     - Puede añadir o suprimir entradas de tabla, pero no puede modificar una entrada.

- Interfaz de línea de mandatos:

  Añada un grupo de claves de aplazamiento. Por ejemplo, escriba:

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

3. El indicador de éxito varía dependiendo de la interfaz:
   - Interfaz gráfica de usuario:

     El grupo de claves aplazamiento aparece en la tabla de grupos de clave de aplazamiento en la página de gestión LTO.
   - Interfaz de línea de mandatos:

     Un mensaje de finalización indica que la operación se ha realizado correctamente.
4. Para suprimir un grupo de claves de la tabla de aplazamiento, su rol debe tener permiso para la acción de supresión.
   - Interfaz gráfica de usuario:

     Seleccione un grupo de claves y pulse **Suprimir**.
   - Interfaz de línea de mandatos:

     Utilice el mandato **tklmKeyGroupDefaultRolloverList** para ubicar el Universal Unique Identifier de un grupo de claves. Your role must have a permission to the view action and a permission to the appropriate device group. A continuación, utilice el mandato **tklmKeyGroupDefaultRolloverDelete** para eliminar el grupo de claves de la lista de aplazamiento. Your role must have a permission to the delete action and a permission to the appropriate device group.

     Por ejemplo, escriba:

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

Especificación de que las claves se utilicen sólo una vez

Puede especificar que las claves de un grupo de claves se utilicen sólo una vez. A efectos de seguridad, por ejemplo, puede evitar el uso adicional de las claves utilizadas previamente que se han definido para un grupo de claves.

Acerca de esta tarea

Utilice la interfaz de línea de mandatos o la interfaz REST para establecer la propiedad **stopRoundRobinKeyGrps** en el archivo SKLMConfig.properties. Your role must have a permission to the configure action.Esta propiedad no existe inicialmente en el archivo de propiedades a menos que establezca su valor en true.

Importante:

- Turning on this flag can cause key serving to stop if a key group is in use and the last key from the key group is served. Additional requests for a key from this group on a key serving write request cause an error and send an error code of 0xEE34 (NO_KEY_TO_SERVE) to the device. To enable successful processing of new key serving write requests, add new keys to the key group. Alternatively, you might specify use of a different key group that has available keys. Key serving read requests always succeed when the requested key exists.
- Use this property in an environment of strict government compliance and with FIPS 140. With the property on, you must actively monitor your key groups.

Ensure that a key group does not run out of keys, causing the server to stop serving keys and the tape write request to fail.

- If you turn on this flag, do not turn off the flag. For example, if you turn on the flag, a key group does not serve previously used keys. If you turn off the flag, the next key in the group is served. After the last key in the group is served, the next key to be served is the first key in the group.
- When this option is set, do not separately assign individual key aliases that belong to a key group to devices.

Procedimiento

1. Vaya al directorio apropiado:
   a. Go to the <*WAS_HOME*>/bin directory. For example,

      Windows

      ```
      cd drive:\Program Files\IBM\WebSphere\AppServer\bin
      ```

      Linux

      ```
      cd /opt/IBM/WebSphere/AppServer/bin
      ```

   b. Start the **wsadmin** interface by using an authorized user ID, such as SKLMAdmin. For example,

      Windows

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

      Linux

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

2. Primero, determine el estado actual de la propiedad en el archivo SKLMConfig.properties. Esta propiedad no existe inicialmente en el archivo de propiedades a menos que establezca su valor en true.
   - Interfaz de línea de mandatos:

     En el indicador de **wsadmin**, escriba este mandato en formato Jython:

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

   - Interfaz REST:

     Utilice el **Servicio REST Obtener propiedad de configuración única** para obtener el valor actual de la propiedad. Envíe la siguiente solicitud HTTP:

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

3. Cambie el estado de la propiedad **stopRoundRobinKeyGrps** en el valor de true en el archivo SKLMConfig.properties.
   - Interfaz de línea de mandatos:

     Escriba este mandato en formato Jython:

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

   - Interfaz REST:

     Envíe la siguiente solicitud HTTP:

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

4. Para determinar que se ha realizado correctamente, vuelva a escribir el mandato **tklmConfigGetEntry** o utilice el **Servicio REST Obtener propiedad de configuración única**.

   Asimismo, en la página de Bienvenida en la interfaz gráfica de usuario, puede aparecer un aviso en la sección Elementos de acción. Esta sección lista los grupos de claves con el 10 por ciento o menos de claves disponibles. Efectúe una doble pulsación en una entrada de esta tabla para acceder al diálogo Modificar grupos de claves, donde puede añadir claves adicionales para utilizarlas en el grupo.

   No hay ningún otro aviso. El aviso de recuento bajo de claves se aplica a todos los grupos de claves, incluido el grupo de claves especificado como predeterminado.

Modificación de un grupo de claves

Puede modificar información sobre los objetos de un grupo de claves en la base de datos de IBM Security Key Lifecycle Manager. Antes de empezar, determine la información modificada del grupo como, por ejemplo, el número de claves adicionales que desea añadir al grupo.

Acerca de esta tarea

Puede utilizar el diálogo Modificar grupo de claves. O bien, puede utilizar los siguientes mandatos o interfaces REST para modificar objetos en un grupo de claves en la base de datos IBM Security Key Lifecycle Manager.

- **tklmGroupEntryAdd** y **tklmGroupEntryDelete**
- **Servicio REST Añadir entrada de grupo** y **Servicio REST Suprimir entrada de grupo**

Your role must have a permission to the modify action and a permission to the appropriate device group.

Procedimiento

1. Vaya a la página o el directorio correspondiente:
   - Interfaz gráfica de usuario:
     a. Inicie una sesión en la interfaz gráfica de usuario.
     b. En la sección clave y dispositivo sección Gestión de claves y dispositivos en la página de bienvenida, seleccione **LTO**.
     c. Pulse **Ir a** > **Gestionar claves y dispositivos**.
     d. O bien, pulse con el botón del ratón derecho en **LTO** y seleccione **Gestionar claves y dispositivos**.
     e. En la página de gestión de LTO, seleccione un grupo de claves en la columna **Grupo de claves**.
     f. Pulse **Modificar**.
     g. O bien, pulse con el botón derecho del ratón en un grupo de claves y seleccione **Modificar**, o efectúe una doble pulsación en una entrada de grupo de claves.
   - Command-line interface
     a. Go to the <*WAS_HOME*>/bin directory. For example,

        Windows
        ```
        cd drive:\Program Files\IBM\WebSphere\AppServer\bin
        ```

        Linux
        ```
        cd /opt/IBM/WebSphere/AppServer/bin
        ```

b. Start the **wsadmin** interface by using an authorized user ID, such as SKLMAdmin. For example,

Windows

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

Linux

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

2. Modifique la información del grupo de claves:
   - Interfaz gráfica de usuario:
     a. En el diálogo Modificar grupo de claves, cambie los campos adecuados. Su rol debe tener permisos específicos para cada acción. Por ejemplo, para suprimir una clave del grupo, su rol debe tener capacidad de supresión y permiso al grupo de dispositivo en cuestión.
     b. Pulse **Modificar grupo de claves**.
   - Interfaz de línea de mandatos:

     Puede suprimir un objeto en un grupo o añadir un objeto a un grupo.
     - Suprima una clave del grupo. Your role must have a permission to the delete action and a permission to the appropriate device group. Por ejemplo, escriba:

       ```
       print AdminTask.tklmGroupEntryDelete ('[-entry "{type key}
        {uuid KEY-a3ce9230-bef9-42bd-86b7-6d208ec119cf}"
          -name GROUP-myKeyGroup -type keygroup]')
       ```
     - Vuelva a añadir la misma clave al grupo. Your role must have a permission to the modify action and a permission to the appropriate device group. Por ejemplo, escriba:

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

     Para suprimir una clave desde el grupo, puede enviar la siguiente solicitud HTTP:

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

     Para añadir la misma clave de nuevo en el grupo, puede enviar la siguiente solicitud HTTP:

     ```
     POST https://localhost:<puerto>/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. El indicador de éxito varía dependiendo de la interfaz:
   - Interfaz gráfica de usuario:

     Para los campos necesarios, una columna muestra los datos modificados. Para los campos opcionales, vuelva a abrir el diálogo Modificar grupo de claves para ver los valores modificados y, a continuación, pulse **Cancelar**.
   - Interfaz de línea de mandatos:

     Un mensaje de finalización indica que la operación se ha realizado correctamente.
   - Interfaz REST:

El código de estado `200 OK` indica que la operación ha sido satisfactoria.

Qué hacer a continuación

A continuación, puede utilizar la página Key and Device Management de LTO para asociar el grupo de claves con dispositivos específicos.

Supresión de una clave o un grupo de claves

Puede suprimir una clave o un grupo de claves seleccionado. No puede suprimir una clave o un grupo de claves que esté asociado a un dispositivo, o un grupo de claves que se haya marcado como el grupo de claves predeterminado.

Acerca de esta tarea

Delete keys only when the data protected by those keys is no longer needed. Deleting keys is like erasing the data. After keys are deleted, data that is protected by those keys is not retrievable.

Puede utilizar el elemento de menú **Suprimir**. O bien, puede utilizar los siguientes mandatos o servicios REST para suprimir una clave o suprimir el grupo de claves.

- **`tklmKeyDelete`** o el **`Servicio REST Suprimir clave`**
- **`tklmGroupDelete`** o el **`Servicio REST Suprimir grupo`**

Your role must have a permission to the delete action and a permission to the appropriate device group.

Antes de suprimir, lleve a cabo las siguientes comprobaciones:

- Clave

  Asegúrese de que exista una copia de seguridad del almacén de claves que contiene la clave que desea suprimir.
- Grupo de claves

  Si utiliza la interfaz de línea de mandatos, obtenga el uuid del grupo de claves que desea suprimir. Compruebe que el grupo de claves no esté asociado actualmente con un dispositivo y que no esté marcado como el grupo de claves predeterminado.

Procedimiento

1. Vaya a la página o el directorio correspondiente:
   - Interfaz gráfica de usuario:
     a. Inicie una sesión en la interfaz gráfica de usuario.
     b. En la sección clave y dispositivo sección Gestión de claves y dispositivos en la página de bienvenida, seleccione **LTO**.
     c. Pulse **Ir a** > **Gestionar claves y dispositivos**.
     d. O bien, pulse con el botón del ratón derecho en **LTO** y seleccione **Gestionar claves y dispositivos**.
     e. En la administración de `LTO`, seleccione una clave o grupo de claves en la columna adecuada.
     f. Pulse **Suprimir**.
     g. O bien, pulse con el botón derecho del ratón en una clave o un grupo de claves y seleccione **Suprimir**.
   - Command-line interface
     a. Go to the `<WAS_HOME>/bin` directory. For example,

Windows

```
cd drive:\Program Files\IBM\WebSphere\AppServer\bin
```

Linux

```
cd /opt/IBM/WebSphere/AppServer/bin
```

b. Start the **wsadmin** interface by using an authorized user ID, such as SKLMAdmin. For example,

Windows

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

Linux

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

2. Suprima la clave o el grupo de claves:
   - Interfaz gráfica de usuario:

     En el diálogo Confirmar, lea el mensaje de confirmación antes de suprimir la clave o el grupo de claves. Compruebe que se haya seleccionado la clave o el grupo de claves correcto. Por ejemplo, puede suprimir un grupo de claves vacío. Al suprimir un grupo de claves lleno *también se suprimirán todas las claves* del grupo. Si se suprime una clave que pertenece a un grupo de claves, también se suprime la clave del grupo. A continuación, pulse en **Aceptar**.
   - Interfaz de línea de mandatos:
     - Clave

       Escriba `tklmKeyDelete` para suprimir una clave. Por ejemplo, para suprimir una clave que no está asociada actualmente con un dispositivo, localice primero la clave. Puede utilizar el mandato **tklmKeyList** para buscar la clave que desea suprimir. Por ejemplo, escriba:

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

       A continuación, suprima la clave. Por ejemplo, escriba:

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

       Deleting a key deletes the key material from the database.
     - Grupo de claves

       Escriba `tklmGroupDelete` para suprimir un grupo de claves. Por ejemplo, puede suprimir un grupo de claves vacío. Al suprimir un grupo de claves lleno *también se suprimirán todas las claves* del grupo. Por ejemplo, para suprimir un grupo de claves que no está asociado actualmente con un dispositivo, escriba:

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

       Utilice el **Servicio REST Suprimir clave** para suprimir una clave. Utilice el **Servicio REST Enumerar clave** para buscar la clave que desea suprimir. Por ejemplo, puede enviar la siguiente solicitud HTTP:

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

       Envíe la siguiente solicitud HTTP para suprimir la clave:

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

– Grupo de claves

Utilice el **Servicio REST Suprimir grupo** para suprimir un grupo de claves. Por ejemplo, puede enviar la siguiente solicitud HTTP:

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

Qué hacer a continuación

Renueve la tabla para comprobar que se ha suprimido la clave o el grupo de claves. Haga una copia de seguridad del almacén de claves para reflejar correctamente el cambio en las claves. Haga una copia de seguridad de la base de datos para reflejar el cambio en los grupos de claves.

Adición de una unidad

Puede añadir un dispositivo como, por ejemplo, una unidad de cintas, a la base de datos de IBM Security Key Lifecycle Manager. Antes de empezar, cree las claves y los grupos de claves que desee asociar con los dispositivos que va a modificar. Asimismo, obtenga el número de serie de la unidad de cintas y otra información descriptiva. Determine si la unidad utiliza un grupo de claves específico o un grupo de claves predeterminado del sistema.

Acerca de esta tarea

Puede utilizar el diálogo Añadir unidad de cintas. O bien, puede utilizar el mandato **tklmDeviceAdd** o el **Servicio REST Añadir dispositivo** para agregar un dispositivo.Your role must have a permission to the create action and a permission to the appropriate device group.

Procedimiento

1. Vaya a la página o el directorio correspondiente:
   - Interfaz gráfica de usuario:
     a. Inicie una sesión en la interfaz gráfica de usuario.
     b. En la sección clave y dispositivo sección Gestión de claves y dispositivos en la página de bienvenida, seleccione **LTO**.
     c. Pulse **Ir a** > **Gestionar claves y dispositivos**.
     d. O bien, pulse con el botón del ratón derecho en **LTO** y seleccione **Gestionar claves y dispositivos**.
     e. En la página de gestión para LTO, pulse **Añadir**.
     f. Pulse **Unidad de cintas**.
   - Command-line interface
     a. Go to the <*WAS_HOME*>/bin directory. For example,

        Windows
        ```
        cd drive:\Program Files\IBM\WebSphere\AppServer\bin
        ```

        Linux
        ```
        cd /opt/IBM/WebSphere/AppServer/bin
        ```

     b. Start the **wsadmin** interface by using an authorized user ID, such as SKLMAdmin. For example,

        Windows
        ```
        wsadmin.bat -username SKLMAdmin -password mypwd -lang jython
        ```

Linux

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

2. Añada un dispositivo:
   - Interfaz gráfica de usuario:

     En el diálogo Añadir unidad de cintas, escriba la información necesaria y opcional. A continuación, pulse **Añadir unidad de cintas**.
   - Interfaz de línea de mandatos:

     Escriba `tklmDeviceAdd` para añadir un dispositivo. Debe especificar el grupo de dispositivos y el número de serie. Por ejemplo, escriba:

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

     Utilice el **Servicio REST Añadir dispositivo** para agregar un dispositivo. Por ejemplo, puede enviar la siguiente solicitud HTTP:

     ```
     POST https://localhost:<puerto>/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"}
     ```

Qué hacer a continuación

A continuación, verifique si la unidad que ha añadido aparece en la tabla Dispositivos.

Modificación de una unidad

Puede modificar información sobre un dispositivo como, por ejemplo, una unidad de cintas, en la base de datos de IBM Security Key Lifecycle Manager. Por ejemplo, puede actualizar la descripción de la unidad.

Acerca de esta tarea

Puede utilizar el diálogo Modificar unidad de cintas, el mandato **tklmDeviceUpdate** o el **Servicio REST Actualizar dispositivo** para actualizar un dispositivo. Your role must have a permission to the modify action and a permission to the appropriate device group.

Antes de empezar, cree las claves y los grupos de claves que desee asociar con los dispositivos que va a modificar. Si utiliza la interfaz de línea de mandatos o la interfaz REST, obtenga el valor del uuid del dispositivo que desea actualizar.

Procedimiento

1. Vaya al directorio o la página apropiada.
   - Interfaz gráfica de usuario:
     a. Inicie una sesión en la interfaz gráfica de usuario.
     b. En la sección clave y dispositivo sección Gestión de claves y dispositivos en la página de bienvenida, seleccione **LTO**.
     c. Pulse **Ir a** > **Gestionar claves y dispositivos**.
     d. O bien, pulse con el botón del ratón derecho en **LTO** y seleccione **Gestionar claves y dispositivos**.

e. En la página de gestión de LTO, seleccione un dispositivo en la columna **Unidades de cintas**.

f. Pulse **Modificar**.

g. O bien, pulse con el botón derecho del ratón en una unidad y seleccione **Modificar**, o efectúe una doble pulsación en una entrada de unidad.

- Command-line interface

a. Go to the <*WAS_HOME*>/bin directory. For example,

Windows

```
cd drive:\Program Files\IBM\WebSphere\AppServer\bin
```

Linux

```
cd /opt/IBM/WebSphere/AppServer/bin
```

b. Start the **wsadmin** interface by using an authorized user ID, such as SKLMAdmin. For example,

Windows

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

Linux

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

2. Modifique un dispositivo:

- Interfaz gráfica de usuario:

a. En el diálogo Modificar unidad de cintas, escriba la información necesaria y opcional.

b. Pulse **Modificar unidad de cintas**.

- Interfaz de línea de mandatos:

Escriba tklmDeviceUpdate para actualizar un dispositivo. Debe especificar el uuid del dispositivo y los atributos que cambian. Por ejemplo, escriba:

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

- Interfaz REST:

Utilice el **Servicio REST Actualizar dispositivo** para actualizar un dispositivo. Debe especificar el uuid del dispositivo y los atributos que cambian. Por ejemplo, puede enviar la siguiente solicitud HTTP:

```
GET https://localhost:<puerto>/SKLM/rest/v1/devices?type=LTO
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth userAuthId=139aeh34567m
Accept-Language : en
PUT https://localhost:<puerto>/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"}
```

Qué hacer a continuación

A continuación, compruebe que se han realizado los cambios. Para los campos opcionales como, por ejemplo, la descripción, es posible que deba ejecutar el mandato **tklmDeviceList** o el **Servicio REST Enumerar dispositivos** para determinar si el valor ha cambiado. O bien, vuelva a abrir el diálogo Modificar unidad de cintas.

Supresión de una unidad

Puede suprimir un dispositivo como, por ejemplo, una unidad de cintas. Los metadatos del dispositivo que suprime, por ejemplo, el número de serie de la unidad, se eliminan de la base de datos de IBM Security Key Lifecycle Manager.

Acerca de esta tarea

Antes de empezar, asegúrese de que exista una copia de seguridad actualizada de la base de datos de IBM Security Key Lifecycle Manager. Si utiliza la interfaz de línea de mandatos o la interfaz REST, obtenga el `uuid` del dispositivo que desea suprimir.

Puede utilizar el elemento de menú Suprimir o el mandato **tklmDeviceDelete** o el **Servicio REST Suprimir dispositivo** para suprimir un dispositivo. Your role must have a permission to the delete action and a permission to the appropriate device group.

Procedimiento

1. Vaya al directorio o la página apropiada.
   - Interfaz gráfica de usuario:
     a. Inicie una sesión en la interfaz gráfica de usuario.
     b. En la sección clave y dispositivo sección Gestión de claves y dispositivos en la página de bienvenida, seleccione **LTO**.
     c. Pulse **Ir a** > **Gestionar claves y dispositivos**.
     d. O bien, pulse con el botón del ratón derecho en **LTO** y seleccione **Gestionar claves y dispositivos**.
     e. En la página de gestión de `LTO`, seleccione un dispositivo.
     f. Pulse **Suprimir**.
     g. O bien, pulse con el botón derecho del ratón en una unidad y seleccione **Suprimir**.
   - Command-line interface
     a. Go to the *<WAS_HOME>*`/bin` directory. For example,

        Windows
        ```
        cd drive:\Program Files\IBM\WebSphere\AppServer\bin
        ```

        Linux
        ```
        cd /opt/IBM/WebSphere/AppServer/bin
        ```

     b. Start the **wsadmin** interface by using an authorized user ID, such as `SKLMAdmin`. For example,

        Windows
        ```
        wsadmin.bat -username SKLMAdmin -password mypwd -lang jython
        ```

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

2. Suprima el dispositivo.
   - Interfaz gráfica de usuario:

     En el diálogo Confirmar, lea el mensaje de confirmación antes de suprimir el dispositivo. Los metadatos del dispositivo que suprime, por ejemplo, el número de serie de la unidad, se eliminan de la base de datos de IBM Security Key Lifecycle Manager. Pulse **Aceptar**.
   - Interfaz de línea de mandatos:

     Escriba `tklmDeviceDelete` para suprimir un dispositivo. Debe especificar el uuid. Por ejemplo, escriba:

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

- Interfaz REST:

  Utilice el **Servicio REST Suprimir dispositivo** para suprimir un dispositivo. Debe especificar el uuid de dispositivo. Por ejemplo, puede enviar la siguiente solicitud HTTP utilizando un cliente REST:

```
GET https://localhost:<puerto>/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:<puerto>/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
```

Gestión de una 3592 tape drive

Puede gestionar las 3592 tape drives utilizando IBM Security Key Lifecycle Manager.

Descriptions of some steps describe alternatives by using the graphical user interface, command-line interface, or the REST interface. For any one work session, do not switch between interfaces.

Descriptions of some tasks might mention task-related properties in the `SKLMConfig.properties` file. Use the graphical user interface, command-line interface, or REST interface to change these properties.

Pasos guiados para crear certificados y unidades

Cuando crea por primera vez certificados y unidades, y posteriormente cuando añade certificados y unidades adicionales, IBM Security Key Lifecycle Manager proporciona un conjunto guiado de pasos para completar la tarea.

Las descripciones de algunos pasos pueden incluir alternativas de línea de mandatos o interfaz REST para realizar la misma tarea. En un conjunto guiado de tareas, utilice la interfaz gráfica de usuario para completar las tareas.

Creación de un certificado o una solicitud de certificado

Como primera actividad, cree certificados o solicitudes de certificado para IBM Security Key Lifecycle Manager. Antes de empezar, determine la política del sitio sobre el uso de certificados autofirmados y certificados emitidos por una entidad emisora de certificados (CA). Puede crear certificados autofirmados para la fase de prueba del proyecto. También puede solicitar por adelantado certificados a una entidad emisora de certificados para la fase de producción.

Acerca de esta tarea

Puede utilizar el diálogo Crear certificado. O bien, puede utilizar los mandatos siguientes o los servicios REST para crear certificados o solicitudes de certificado:

- **tklmCertCreate** o **tklmCertGenRequest**
- **Servicio REST Crear certificado** o el **Servicio REST Generar solicitud de certificado**

Your role must have a permission to the create action and permission to the appropriate device group. To make this certificate the default, your role must have permission to the modify action.

Si además desea especificar que un certificado se utilice como certificado predeterminado o de socio del sistema, puede utilizar los mandatos siguientes o los servicios REST:

- **tklmDeviceGroupAttributeList** and **tklmDeviceGroupAttributeUpdate**
- **Servicio REST Enumerar atributos de grupo de dispositivos** y **Servicio REST Actualizar atributos de grupo de dispositivos**

Estos valores se almacenaban anteriormente en las propiedades obsoletas **drive.default.alias1** (para el valor predeterminado del sistema) o **drive.default.alias2** (para el socio del sistema).

Procedimiento

1. Vaya al directorio o la página apropiada.
   - Interfaz gráfica de usuario:
     a. Inicie una sesión en la interfaz gráfica de usuario.
     b. En la sección clave y dispositivo sección Gestión de claves y dispositivos en la página de bienvenida, seleccione **3592**.
     c. Pulse **Ir a** > **Creación guiada de claves y dispositivos**.
     d. O bien, pulse el botón derecho del ratón **3592** y seleccione **Creación guiada de claves y dispositivos**.
   - Command-line interface
     a. Go to the *<WAS_HOME>*/bin directory. For example,

        Windows
        ```
        cd drive:\Program Files\IBM\WebSphere\AppServer\bin
        ```

        Linux
        ```
        cd /opt/IBM/WebSphere/AppServer/bin
        ```

     b. Start the **wsadmin** interface by using an authorized user ID, such as SKLMAdmin. For example,

        Windows
        ```
        wsadmin.bat -username SKLMAdmin -password mypwd -lang jython
        ```

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

   - Interfaz REST:
     – Abra un cliente REST.
2. Cree un certificado o solicite un certificado.
   - Interfaz gráfica de usuario:
     a. En la página Paso 1: crear certificados, pulse **Crear** en la tabla **Certificados**.
     b. En el diálogo Crear certificado, seleccione un certificado autofirmado o una solicitud de certificado de un proveedor de terceros.
     c. Especifique valores para los parámetros necesarios y opcionales. Por ejemplo, de manera opcional, puede especificar que el certificado sea el certificado predeterminado o de socio.
     d. Pulse **Crear certificado**.
   - Interfaz de línea de mandatos:
     – Certificado

Escriba tklmCertCreate para crear un certificado y un par de claves pública y privada, y almacene el certificado en un almacén de claves existente. Por ejemplo, escriba:

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

– Solicitud de certificado

Escriba tklmCertGenRequest para crear un archivo de solicitud de certificado PKCS #10. Por ejemplo, escriba:

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

- Interfaz REST:
  – Certificado
    a. Obtenga un identificador de autenticación de usuario exclusivo para acceder a los servicios REST de IBM Security Key Lifecycle Manager. Para obtener más información sobre el proceso de autenticación, consulte Proceso de autenticación de los servicios REST.
    b. Para ejecutar el **Servicio REST Crear certificado**, envíe la solicitud HTTP POST. Pase el identificador de autenticación de usuario que ha obtenido en el Paso a junto con el mensaje de solicitud, como se muestra en el ejemplo siguiente.

```
POST https://localhost:<puerto>/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 " }
```

  – Solicitud de certificado

    Utilice el **Servicio REST Generar solicitud de certificado** para crear un archivo de solicitud de certificado PKCS #10. Por ejemplo, puede enviar la siguiente solicitud HTTP:

```
POST https://localhost:<puerto>/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"}
```

Qué hacer a continuación

Realice una copia de seguridad de nuevos certificados antes de que los certificados se sirven como dispositivos. En el caso de una solicitud de certificado, el siguiente paso puede ser importar el certificado firmado. Puede ir al paso siguiente para definir dispositivos específicos y asociar certificados con dispositivos. Seleccione **Paso 2: Identificar las unidades** o pulse **Ir al paso siguiente**.

For a 3592 device group, also specify values for the system default and partner certificates in the IBM Security Key Lifecycle Manager database. Use the **tklmDeviceGroupAttributeUpdate** command or **Device Group Attribute Update REST Service** to set these values.

Identificación de unidades

Puede identificar una 3592 tape drive para utilizarla con IBM Security Key Lifecycle Manager. Antes de empezar, cree los certificados que desee asociar con los dispositivos que va a identificar.

Acerca de esta tarea

Puede utilizar el diálogo Añadir unidad de cintas, el mandato **tklmDeviceAdd** o el **Servicio REST Añadir dispositivo** para añadir un dispositivo. Your role must have a permission to the create action and a permission to the appropriate device group.

Puede realizar cualquiera de las siguientes opciones para servir claves a dispositivos.

Only accept manually added devices for communication
All incoming devices are not added to the data store. You must manually specify key service to each device.

Hold new device requests pending my approval
All incoming devices of a valid device group are added to the device store, but are not automatically served keys upon request. You must accept or reject a device in the pending devices list before the device is served keys upon request.

Automatically accept all new device requests for communication
All new incoming devices of a valid device group are added to the data store and are automatically served keys upon request.

Nota: Do not use this setting if you intend to move the new device to another device group. Instead, select manual or pending approval mode to allow an opportunity to move the device into the appropriate device group before any keys are served.

Procedimiento

1. Vaya al directorio o la página apropiada.
   - Interfaz gráfica de usuario:
     a. Inicie una sesión en la interfaz gráfica de usuario.
     b. En la sección clave y dispositivo sección Gestión de claves y dispositivos en la página de bienvenida, seleccione **3592**.
     c. Pulse **Ir a** > **Creación guiada de claves y dispositivos**.
     d. O bien, pulse el botón derecho del ratón **3592** y seleccione **Creación guiada de claves y dispositivos**.
   - Command-line interface
     a. Go to the *<WAS_HOME>*/bin directory. For example,

        Windows
        ```
        cd drive:\Program Files\IBM\WebSphere\AppServer\bin
        ```

        Linux
        ```
        cd /opt/IBM/WebSphere/AppServer/bin
        ```

     b. Start the **wsadmin** interface by using an authorized user ID, such as SKLMAdmin. For example,

        Windows
        ```
        wsadmin.bat -username SKLMAdmin -password mypwd -lang jython
        ```

Linux

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

- Interfaz REST:
  - Abra un cliente REST.

2. Omita el **Paso 1: Crear certificados**. Pulse el enlace **Ir al paso siguiente** o pulse **Paso 2: Identificar las unidades**.
3. Puede especificar que IBM Security Key Lifecycle Manager retenga las nuevas solicitudes de dispositivo para su aprobación. Your role must have a permission to the modify action and a permission to the appropriate device group.
   - Interfaz gráfica de usuario:

     Seleccione **Retener las solicitudes de dispositivos nuevos pendientes de aprobación**.
   - Interfaz de línea de mandatos:

     Utilice el mandato **tklmDeviceGroupAttributeUpdate** o el **Servicio REST Actualizar atributos de grupo de dispositivos** para establecer el valor del atributo **device.AutoPendingAutoDiscovery**. Por ejemplo, escriba:

     ```
     print AdminTask.tklmDeviceGroupAttributeUpdate ('[-name 3592
       -attributes "{device.AutoPendingAutoDiscovery 2}"]')
     ```
   - Interfaz REST:
     a. Obtenga un identificador de autenticación de usuario exclusivo para acceder a los servicios REST de IBM Security Key Lifecycle Manager. Para obtener más información sobre el proceso de autenticación, consulte Proceso de autenticación de los servicios REST.
     b. Para ejecutar el **Servicio REST Actualizar atributos de grupo de dispositivos** y establecer el valor del atributo **device.AutoPendingAutoDiscovery**, envíe la solicitud HTTP PUT. Pase el identificador de autenticación de usuario que ha obtenido en el Paso a junto con el mensaje de solicitud, como se muestra en el ejemplo siguiente.

        ```
        PUT https://localhost:<puerto>/SKLM/rest/v1/deviceGroupAttributes
        Content-Type: application/json
        Accept : application/json
        Authorization: SKLMAuth authId=139aeh34567m
        {"name":"3592","attributes":"device.AutoPendingAutoDiscovery 2"}
        ```
4. Añada un dispositivo.
   - Interfaz gráfica de usuario:
     a. En la página Paso 2: Identificar las unidades, en la tabla **Dispositivos**, pulse **Añadir**.
     b. En el diálogo Añadir unidad de cintas, escriba la información necesaria y opcional.
     c. Pulse **Añadir unidad de cintas**.
   - Interfaz de línea de mandatos:

     Escriba tklmDeviceAdd para añadir un dispositivo. Debe especificar el grupo de dispositivos y el número de serie. Por ejemplo, escriba:

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

     Puede utilizar el **Servicio REST Añadir dispositivo** para agregar un dispositivo. Por ejemplo, puede enviar la siguiente solicitud HTTP:

```
POST https://localhost:<puerto>/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"}
```

Qué hacer a continuación

A continuación, utilice la página Key and Device Management de 3592 para ver todos los certificados y dispositivos.

Administración de certificados y dispositivos

Para administrar certificados y dispositivos, deberá determinar su estado. Puede correlacionar su asociación o bien añadir, modificar o suprimir dispositivos y certificados específicos.

Acerca de esta tarea

Antes de empezar, examine las columnas de la página, que proporciona botones para añadir, modificar o suprimir un elemento de tabla. Para ordenar la información, pulse una cabecera de columna.

Utilice la página Key and Device Management de 3592 para correlacionar certificados con dispositivos y así determinar el estado de los elementos en la tabla. Puede añadir, modificar o suprimir certificados o dispositivos. Your role must have a permission to the view action and a permission to the appropriate device group.

La tabla está organizada en estas áreas:

- En las columnas de la izquierda, la información sobre los certificados indica el nombre de certificado, si el certificado se utiliza como valor predeterminado del sistema o como socio del sistema, la fecha de caducidad y el estado del certificado.
- En las columnas de la derecha, la información sobre las unidades indica el nombre de unidad y si la unidad utiliza un valor predeterminado del sistema como certificado predeterminado o de socio.
- Los iconos de estado indican el estado de un certificado.

Tabla 3. Iconos de estado y su significado

Icono	Descripción
	El certificado está activo.
	El certificado está comprometido.
	El certificado caduca pronto.
	El certificado ha caducado.
	Certificate valid from future date, for migrated certificates with a future use time stamp.
	IBM Security Key Lifecycle Manager tiene solicitudes de certificado de otro proveedor que están de pendientes de ser firmadas e importadas.

Procedimiento

1. Inicie una sesión en la interfaz gráfica de usuario:
   a. En la sección clave y dispositivo sección Gestión de claves y dispositivos en la página de bienvenida, seleccione **3592**.
   b. Pulse **Ir a** > **Gestionar claves y dispositivos**.
   c. O bien, pulse con el botón derecho del ratón en **3592** y seleccione **Gestionar claves y dispositivos**.

   Descriptions of some steps describe alternatives by using the graphical user interface, command-line interface, or the REST interface. For any one work session, do not switch between interfaces.

   Descriptions of some tasks might mention task-related properties in the `SKLMConfig.properties` file. Use the graphical user interface, command-line interface, or REST interface to change these properties.
2. En la página Key and Device Management de 3592, puede añadir, modificar o suprimir un certificado o una unidad. De manera adicional, puede supervisar el estado de los certificados.

   Puede realizar estas tareas administrativas:

   • Añadir

   Pulse **Añadir**. De manera alternativa, puede seleccionar un proceso paso a paso para crear certificados y unidades.

   – Certificado

   En el diálogo Crear certificado, seleccione el tipo de certificado como autofirmado o de un proveedor de terceros, y complete la información necesaria. A continuación, pulse **Crear certificado**. Your role must have a permission to the create action and permission to the appropriate device group. To make this certificate the default, your role must have permission to the modify action.

   – Unidad de cintas

   En el diálogo Añadir unidad de cintas, escriba la información de la unidad. A continuación, pulse **Añadir unidad de cintas**. Your role must have a permission to the create action and a permission to the appropriate device group.

   – Utilizar el proceso paso a paso para la creación de certificados y unidades

   En las páginas Paso 1: Crear certificados y Paso 2: Identificar unidades, especifique la información necesaria.

   El indicador de éxito varía, y muestra un cambio en una columna para el certificado o el dispositivo.

   • Modificar

   Para cambiar o suprimir un certificado o una unidad, seleccione el certificado o la unidad y pulse **Modificar**. O bien, pulse con el botón derecho del ratón en el certificado o la unidad que ha seleccionado. A continuación, pulse **Modificar** o efectúe una doble pulsación en una entrada de certificado o dispositivo en la lista.

   – Certificado

   Especifique cambios en el diálogo Modificar el certificado. A continuación, pulse **Modificar el certificado**. Your role must have a permission to the modify action and a permission to the appropriate device group.

   – Unidad de cintas

Especifique cambios en el diálogo Modificar unidad de cintas. A continuación, pulse **Modificar unidad de cintas**. Your role must have a permission to the modify action and a permission to the appropriate device group.

El indicador de éxito varía, y muestra un cambio en una columna para el certificado o el dispositivo. Los cambios de alguna información como, por ejemplo, los campos opcionales, puede que no se proporcionen en la tabla.

- Suprimir

  Para suprimir un certificado o una unidad, resalte la entrada en la tabla y pulse **Suprimir**. O bien, pulse con el botón derecho del ratón en el certificado o la unidad que ha seleccionado. A continuación, pulse **Suprimir**.

  – Certificado

    Asegúrese de que tiene una copia de seguridad actualizada del almacén de claves antes de suprimir un certificado. Una cinta grabada utilizando este certificado deja de ser legible después de suprimir el certificado. El certificado que se va a suprimir puede estar en cualquier estado, por ejemplo, activo. Independientemente del estado, no puede suprimir un certificado que esté asociado con un dispositivo. Tampoco puede suprimir un certificado que esté marcado como predeterminado o de socio. Your role must have a permission to the delete action and a permission to the appropriate device group.

    Deleting a certificate deletes the material from the database.

    Para confirmar la supresión, pulse **Aceptar**.

  – Unidad de cintas

    Los metadatos de la unidad que suprime, por ejemplo, el número de serie de la unidad, se eliminan de la base de datos de IBM Security Key Lifecycle Manager. Para confirmar la supresión, pulse **Aceptar**. Your role must have a permission to the delete action and a permission to the appropriate device group.

  El indicador de éxito es que el certificado o el dispositivo se elimina de la tabla de administración.

Adición de un certificado o una solicitud de certificado

Puede añadir más certificados o solicitudes de certificado para utilizarlos con IBM Security Key Lifecycle Manager.Antes de empezar, determine la política del sitio sobre el uso de certificados autofirmados y certificados de CA. Puede crear certificados autofirmados para la fase de prueba del proyecto. También puede solicitar por adelantado certificados a una entidad emisora de certificados para la fase de producción.

Acerca de esta tarea

Puede utilizar el diálogo Crear certificado. O bien, puede utilizar los mandatos siguientes o los servicios REST para crear certificados o solicitudes de certificado:

- **tklmCertCreate** o **tklmCertGenRequest**
- **Servicio REST Crear certificado** o el **Servicio REST Generar solicitud de certificado**

Your role must have a permission to the create action and permission to the appropriate device group. To make this certificate the default, your role must have permission to the modify action.

Antes de empezar, determine la política del sitio sobre el uso de certificados autofirmados y certificados de CA. Es posible que deba crear certificados

autofirmados para la fase de prueba del proyecto. También puede solicitar por adelantado certificados a una entidad emisora de certificados para la fase de producción.

Procedimiento

1. Vaya al directorio o la página apropiada.
   - Interfaz gráfica de usuario:
     a. Inicie una sesión en la interfaz gráfica de usuario.
     b. En la sección clave y dispositivo sección Gestión de claves y dispositivos en la página de bienvenida, seleccione **3592**.
     c. Pulse **Ir a** > **Gestionar claves y dispositivos**.
     d. O bien, pulse con el botón derecho del ratón en **3592** y seleccione **Gestionar claves y dispositivos**.
     e. En la página de gestión para 3592, pulse **Añadir**.
     f. Pulse **Certificado**.
   - Command-line interface
     a. Go to the <*WAS_HOME*>/bin directory. For example,

        Windows

        ```
        cd drive:\Program Files\IBM\WebSphere\AppServer\bin
        ```

        Linux

        ```
        cd /opt/IBM/WebSphere/AppServer/bin
        ```

     b. Start the **wsadmin** interface by using an authorized user ID, such as SKLMAdmin. For example,

        Windows

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

        Linux

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

2. Cree un certificado o solicite un certificado.
   - Interfaz gráfica de usuario:
     a. En el diálogo Crear certificado, seleccione un certificado autofirmado o una solicitud de certificado de un proveedor de terceros.
     b. Especifique valores para los parámetros necesarios y opcionales. Por ejemplo, de manera opcional, puede especificar que este certificado sea el certificado predeterminado o de socio. A continuación, pulse **Crear certificado**.
   - Interfaz de línea de mandatos:
     – Certificado:

       Escriba tklmCertCreate para crear un certificado y un par de claves pública y privada, y almacene el certificado en un almacén de claves existente. Por ejemplo, escriba:

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

     – Solicitud de certificado:

       Escriba tklmCertGenRequest para crear un archivo de solicitud de certificado PKCS #10. Por ejemplo, escriba:

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

- Interfaz REST:
  - Certificado

    Utilice el **Servicio REST Crear certificado** para crear un certificado y un par de claves pública y privada, y almacene el certificado en un almacén de claves existente. Por ejemplo, puede enviar la siguiente solicitud HTTP utilizando un cliente REST:

    ```
    POST https://localhost:<puerto>/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 " }
    ```

  - Solicitud de certificado

    Utilice el **Servicio REST Generar solicitud de certificado** para crear un archivo de solicitud de certificado PKCS #10. Por ejemplo, puede enviar la siguiente solicitud HTTP utilizando un cliente REST:

    ```
    POST https://localhost:<puerto>/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"}
    ```

Qué hacer a continuación

La próxima acción depende de si ha creado un certificado o una solicitud de certificado.

- Certificado:

  Realice una copia de seguridad de nuevos certificados antes de que los certificados se sirven como dispositivos. Puede asociar un certificado con un dispositivo específico.
- Solicitud de certificado:

  Envíe manualmente la solicitud de certificado a una entidad emisora de certificados. Cuando se devuelva el certificado firmado, impórtelo utilizando un elemento de acción pendiente en el panel de bienvenida o con el mandato **tklmCertImport** o el **Servicio REST Importar certificado**. Cuando finalice la importación, realice una copia de seguridad del certificado para habilitar el servicio del certificado a un dispositivo.

Especificación de un certificado de aplazamiento

Puede especificar un certificado para su uso futuro como certificado predeterminado del sistema o certificado de socio del sistema.

Acerca de esta tarea

Puede utilizar la interfaz gráfica de usuario, el mandato **tklmCertDefaultRolloverAdd** o el **Servicio REST Añadir el aplazamiento predeterminado de certificado** para añadir un aplazamiento de certificado predeterminado para una fecha determinada y el grupo de dispositivos. Your role must have a permission to the create action and a permission to the appropriate device group.

Procedimiento

1. Vaya al directorio o la página apropiada.
   - Interfaz gráfica de usuario:
     a. Inicie una sesión en la interfaz gráfica de usuario.
     b. En la sección clave y dispositivo sección Gestión de claves y dispositivos en la página de bienvenida, seleccione **3592**.
     c. Pulse **Ir a** > **Gestionar aplazamiento predeterminado**.
     d. O bien, pulse con el botón del ratón derecho en **3592** y seleccione **Gestionar aplazamiento predeterminado**.
   - Command-line interface
     a. Go to the *<WAS_HOME>*/bin directory. For example,

        Windows
        ```
        cd drive:\Program Files\IBM\WebSphere\AppServer\bin
        ```

        Linux
        ```
        cd /opt/IBM/WebSphere/AppServer/bin
        ```

     b. Start the **wsadmin** interface by using an authorized user ID, such as SKLMAdmin. For example,

        Windows
        ```
        wsadmin.bat -username SKLMAdmin -password mypwd -lang jython
        ```

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

2. Especifique un certificado existente para su uso futuro como certificado predeterminado del sistema o certificado de socio del sistema.
   - Interfaz gráfica de usuario:
     a. En la página de gestión para 3592, pulse **Añadir**.
     b. En el diálogo Añadir valor predeterminado de escritura futuro, especifique la información.
     c. Pulse **Añadir valor predeterminado de escritura futuro**.

     Nota:
     - No especifique dos valores predeterminados para la misma fecha de aplazamiento.
     - No se realiza ninguna validación si el certificado seleccionado ha caducado o caduca en el momento del aplazamiento.
     - Si un certificado no existe en el momento del aplazamiento, IBM Security Key Lifecycle Manager continúa utilizando el certificado predeterminado actual.
     - Puede añadir o suprimir entradas de tabla, pero no puede modificar una entrada.
   - Interfaz de línea de mandatos:

     Añada un certificado de aplazamiento. Por ejemplo, escriba:
     ```
     print AdminTask.tklmCertDefaultRolloverAdd
     ('[-usage 3592 -alias tklmcert1
          -certDefaultType 1 -effectiveDate 2010-05-30]')
     ```
3. El indicador de éxito varía dependiendo de la interfaz:
   - Interfaz gráfica de usuario:

     El certificado aparece en la tabla de certificados de aplazamiento en la página 3592.
   - Interfaz de línea de mandatos:

Un mensaje de finalización indica que la operación se ha realizado correctamente.

- Interfaz REST:

  El código de estado `200 OK` indica que la operación ha sido satisfactoria.

4. Para suprimir un certificado de la tabla de aplazamiento:
   - Interfaz gráfica de usuario:

     Seleccione un certificado y pulse **Suprimir**. Su rol debe tener permiso para la acción de supresión. Lea el mensaje de aviso. A continuación, pulse en **Aceptar**.

   - Interfaz de línea de mandatos:

     Utilice el mandato **`tklmCertDefaultRolloverList`** para ubicar el Universal Unique Identifier de un determinado certificado. Your role must have a permission to the view action and a permission to the appropriate device group. A continuación, utilice el mandato **`tklmCertDefaultRolloverDelete`** para eliminar el certificado de la lista de aplazamientos. Your role must have a permission to the delete action and a permission to the appropriate device group. Por ejemplo, escriba:

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

   El certificado se marca como certificado predeterminado o de socio del sistema, pero en cambio no se modifica ni suprime.

Modificación de un certificado

Puede modificar si un certificado se utiliza como certificado predeterminado del sistema o como certificado de socio del sistema. Antes de empezar, determine la información modificada del certificado como, por ejemplo, una descripción, o si desea que el certificado sea el certificado predeterminado del sistema o el certificado de socio del sistema. Si utiliza la interfaz de línea de mandatos, obtenga el valor del `uuid` del certificado.

Acerca de esta tarea

Puede utilizar el diálogo Modificar certificado para modificar un certificado. O bien, puede utilizar los siguientes mandatos o servicios REST:

- **`tklmCertUpdate`** o el **`Servicio REST Actualizar certificado`** para modificar el estado de los certificados como, por ejemplo, de confianza o comprometido, y modificar la información del certificado.
- **`tklmDeviceTypeAttributeUpdate`** o el **`Servicio REST Actualizar atributos de tipo de dispositivos`** para establecer el certificado como el certificado predeterminado del sistema o el certificado de socio del sistema.

Your role must have a permission to the modify action and a permission to the appropriate device group.

Procedimiento

1. Vaya al directorio o la página apropiada.
   - Interfaz gráfica de usuario:
     a. Inicie una sesión en la interfaz gráfica de usuario.
     b. En la sección clave y dispositivo sección Gestión de claves y dispositivos en la página de bienvenida, seleccione **3592**.
     c. Pulse **Ir a** > **Gestionar claves y dispositivos**.
     d. O bien, pulse con el botón derecho del ratón en **3592** y seleccione **Gestionar claves y dispositivos**.

e. En la página de gestión de 3592, seleccione un certificado en la columna **Certificados**.

f. Pulse **Modificar**.

g. O bien, pulse con el botón derecho del ratón en un certificado y seleccione **Modificar**, o efectúe una doble pulsación en una entrada de certificado.

- Command-line interface

a. Go to the <*WAS_HOME*>/bin directory. For example,

Windows

```
cd drive:\Program Files\IBM\WebSphere\AppServer\bin
```

Linux

```
cd /opt/IBM/WebSphere/AppServer/bin
```

b. Start the **wsadmin** interface by using an authorized user ID, such as SKLMAdmin. For example,

Windows

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

Linux

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

2. Modifique la información de certificados:

- Interfaz gráfica de usuario:

  En el diálogo Modificar el certificado, cambie los campos correspondientes. A continuación, pulse **Modificar el certificado**.

- Interfaz de línea de mandatos:

  Escriba tklmCertList para buscar un certificado y tklmCertUpdate para actualizar un certificado. Debe especificar el uuid del certificado y el atributo modificado. Por ejemplo, para cambiar la descripción, escriba:

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

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

- Interfaz REST:

  Utilice el **Servicio REST Enumerar certificado** para buscar un certificado. Por ejemplo, puede enviar la siguiente solicitud HTTP:

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

  Utilice el **Servicio REST Actualizar certificado** para actualizar un certificado. Por ejemplo, puede enviar la siguiente solicitud HTTP:

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

Qué hacer a continuación

A continuación, puede utilizar la página Key and Device Management de 3592 para asociar certificados con dispositivos específicos.

Supresión de un certificado

Puede suprimir un certificado seleccionado, que se puede encontrar en cualquier estado como, por ejemplo, activo. No puede suprimir un certificado que esté asociado a un dispositivo, ni un certificado que esté marcado como un certificado predeterminado o de socio. Por ejemplo, puede suprimir un certificado caducado.

Acerca de esta tarea

Antes de empezar, asegúrese de que exista una copia de seguridad del almacén de claves que contiene el certificado que desea suprimir. Compruebe que el certificado no esté asociado actualmente con un dispositivo y que no esté marcado como un certificado predeterminado o de socio. Determine el estado actual del certificado y asegúrese de que la supresión de un certificado en este estado cumple las políticas del sitio.

Delete certificates only when the data protected by those certificates is no longer needed. Deleting certificates is like erasing the data. After certificates are deleted, data that is protected by those certificates is not retrievable.

Puede utilizar el elemento de menú Suprimir o el mandato **tklmCertDelete** o el **Servicio REST Suprimir certificado** para suprimir un certificado. Your role must have a permission to the delete action and a permission to the appropriate device group.

Deleting a certificate deletes the material from the database.

Procedimiento

1. Vaya al directorio o la página apropiada.
   - Interfaz gráfica de usuario:
     a. Inicie una sesión en la interfaz gráfica de usuario.
     b. En la sección clave y dispositivo sección Gestión de claves y dispositivos en la página de bienvenida, seleccione **3592**.
     c. Pulse **Ir a** > **Gestionar claves y dispositivos**.
     d. O bien, pulse con el botón derecho del ratón en **3592** y seleccione **Gestionar claves y dispositivos**.
     e. En la página de gestión de 3592, seleccione un certificado en la columna **Certificados**.
     f. Pulse **Suprimir**.
     g. O bien, pulse con el botón derecho del ratón en un certificado y seleccione **Suprimir**.
   - Command-line interface
     a. Go to the <*WAS_HOME*>/bin directory. For example,

        Windows
        ```
        cd drive:\Program Files\IBM\WebSphere\AppServer\bin
        ```

        Linux
        ```
        cd /opt/IBM/WebSphere/AppServer/bin
        ```

     b. Start the **wsadmin** interface by using an authorized user ID, such as SKLMAdmin. For example,

        Windows
        ```
        wsadmin.bat -username SKLMAdmin -password mypwd -lang jython
        ```

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

2. Suprima el certificado.
   - Interfaz gráfica de usuario:

     En el diálogo Confirmar, lea el mensaje de confirmación para comprobar que ha seleccionado el certificado correcto antes de suprimirlo. A continuación, pulse en **Aceptar**.
   - Interfaz de línea de mandatos:

     Escriba `tklmCertList` para buscar un certificado y `tklmCertDelete` para suprimir un certificado. Debe especificar el alias de certificado y el nombre del almacén de claves. Por ejemplo, para suprimir un certificado caducado que no está asociado actualmente con un dispositivo, escriba:

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

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

     Utilice el **Servicio REST Enumerar certificado** para buscar un certificado y el **Servicio REST Suprimir certificado** para suprimir un certificado. Por ejemplo, puede enviar las siguientes solicitudes HTTP:

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

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

Qué hacer a continuación

A continuación, puede hacer otra copia de seguridad del almacén de claves para reflejar correctamente el cambio en los certificados.

Adición de una unidad

Puede añadir un dispositivo como, por ejemplo, una unidad de cintas, a la base de datos de IBM Security Key Lifecycle Manager. Antes de empezar, cree los certificados que desee asociar con los dispositivos que va a identificar. Asimismo, obtenga el número de serie de la unidad de cintas y otra información descriptiva. Determine si la unidad utiliza un certificado específico o un certificado predeterminado del sistema.

Acerca de esta tarea

el mandato **tklmDeviceAdd**

Puede utilizar el diálogo Añadir unidad de cintas. O bien, puede utilizar el mandato **tklmDeviceAdd** o el **Servicio REST Añadir dispositivo** para agregar un dispositivo.Your role must have a permission to the create action and a permission to the appropriate device group.

Procedimiento

1. Vaya al directorio o la página apropiada.
   - Interfaz gráfica de usuario:

a. Inicie una sesión en la interfaz gráfica de usuario.
b. En la sección clave y dispositivo sección Gestión de claves y dispositivos en la página de bienvenida, seleccione **3592**.
c. Pulse **Ir a** > **Gestionar claves y dispositivos**.
d. O bien, pulse con el botón derecho del ratón en **3592** y seleccione **Gestionar claves y dispositivos**.
e. En la página de gestión para 3592, pulse **Añadir**.
f. Pulse **Unidad de cintas**.

- Command-line interface
  a. Go to the *<WAS_HOME>*/bin directory. For example,

     Windows
     ```
     cd drive:\Program Files\IBM\WebSphere\AppServer\bin
     ```

     Linux
     ```
     cd /opt/IBM/WebSphere/AppServer/bin
     ```

  b. Start the **wsadmin** interface by using an authorized user ID, such as SKLMAdmin. For example,

     Windows
     ```
     wsadmin.bat -username SKLMAdmin -password mypwd -lang jython
     ```

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

2. Añada un dispositivo.
   - Interfaz gráfica de usuario:

     En el diálogo Añadir unidad de cintas, escriba la información necesaria y opcional. A continuación, pulse **Añadir unidad de cintas**.
   - Interfaz de línea de mandatos:

     Escriba tklmDeviceAdd para añadir un dispositivo. Debe especificar el grupo de dispositivos y el número de serie. Por ejemplo, escriba:
     ```
     print AdminTask.tklmDeviceAdd ('[-type 3592 -serialNumber CDA39403AQJF
       -attributes "{worldwideName ABCdeF1234567890}
       {description marketingDivisionDrive}
        {aliasOne encryption_cert}"]')
     ```
   - Interfaz REST:

     Utilice el **Servicio REST Añadir dispositivo** para agregar un dispositivo. Por ejemplo, puede enviar la siguiente solicitud HTTP:
     ```
     POST https://localhost:<puerto>/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"}
     ```

Qué hacer a continuación

A continuación, puede determinar el estado de la unidad que ha añadido.

Modificación de una unidad

Puede modificar información sobre un dispositivo como, por ejemplo, una unidad de cintas, en la base de datos de IBM Security Key Lifecycle Manager. Por ejemplo, puede actualizar la especificación de un certificado de socio que utiliza la unidad o especificar un grupo de dispositivos alternativo en la misma familia de dispositivos.

Acerca de esta tarea

Antes de empezar, cree los certificados que desee asociar con los dispositivos que va a modificar. Si utiliza la interfaz de línea de mandatos, obtenga el valor del uuid del dispositivo que desea actualizar. Asimismo, obtenga el alias de un certificado asociado con la unidad.

Puede utilizar el diálogo Modificar unidad de cintas. O bien, puede utilizar el mandato **tklmDeviceUpdate** o el **Servicio REST Actualizar dispositivo** para actualizar un dispositivo o especificar un grupo de dispositivos alternativo en la misma familia de dispositivos. Your role must have a permission to the modify action and a permission to the appropriate device group.

Procedimiento

1. Vaya al directorio o la página apropiada.
   - Interfaz gráfica de usuario:
     a. Inicie una sesión en la interfaz gráfica de usuario.
     b. En la sección clave y dispositivo sección Gestión de claves y dispositivos en la página de bienvenida, seleccione **3592**.
     c. Pulse **Ir a** > **Gestionar claves y dispositivos**.
     d. O bien, pulse con el botón derecho del ratón en **3592** y seleccione **Gestionar claves y dispositivos**.
     e. En la página de gestión de 3592, seleccione un dispositivo en la columna **Unidades de cintas**.
     f. Pulse **Modificar**.
     g. O bien, pulse con el botón derecho del ratón en una unidad y seleccione **Modificar**, o efectúe una doble pulsación en una entrada de unidad.
   - Command-line interface
     a. Go to the *<WAS_HOME>*/bin directory. For example,

        Windows
        ```
        cd drive:\Program Files\IBM\WebSphere\AppServer\bin
        ```

        Linux
        ```
        cd /opt/IBM/WebSphere/AppServer/bin
        ```

     b. Start the **wsadmin** interface by using an authorized user ID, such as SKLMAdmin. For example,

        Windows
        ```
        wsadmin.bat -username SKLMAdmin -password mypwd -lang jython
        ```

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

2. Modifique un dispositivo.
   - Interfaz gráfica de usuario:

     En el diálogo Modificar unidad de cintas, escriba la información necesaria y opcional. A continuación, pulse **Modificar unidad de cintas**.
   - Interfaz de línea de mandatos:

     Escriba tklmDeviceList para localizar un dispositivo y tklmDeviceUpdate para actualizar un dispositivo. Debe especificar el uuid del dispositivo y los atributos que cambian. Por ejemplo, escriba:

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

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

- Interfaz REST:

  Utilice el **Servicio REST Enumerar dispositivos** para ubicar un dispositivo y el **Servicio REST Actualizar dispositivo** para actualizar un dispositivo. Por ejemplo, puede enviar las siguientes solicitudes HTTP:

```
GET https://localhost:<puerto>/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:<puerto>/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"}
```

Qué hacer a continuación

A continuación, compruebe que se han realizado los cambios. Para los campos opcionales como, por ejemplo, la descripción, es posible que deba ejecutar el mandato **tklmDeviceList** o el **Servicio REST Enumerar dispositivos** para determinar si el valor ha cambiado. O bien, vuelva a abrir el diálogo Modificar unidad de cintas.

Supresión de una unidad

Puede suprimir un dispositivo como, por ejemplo, una unidad de cintas. Los metadatos de la unidad que suprime, por ejemplo, el número de serie de la unidad, se eliminan de la base de datos de IBM Security Key Lifecycle Manager.

Acerca de esta tarea

Antes de empezar, asegúrese de que exista una copia de seguridad actualizada de los certificados y los dispositivos en el sitio. Obtenga el uuid del dispositivo que desea suprimir.

Puede utilizar el elemento de menú Suprimir o el mandato **tklmDeviceDelete** o el **Servicio REST Suprimir dispositivo** para suprimir un dispositivo. Your role must have a permission to the delete action and a permission to the appropriate device group.

Procedimiento

1. Vaya al directorio o la página apropiada.
   - Interfaz gráfica de usuario:
     a. Inicie una sesión en la interfaz gráfica de usuario.
     b. En la sección clave y dispositivo sección Gestión de claves y dispositivos en la página de bienvenida, seleccione **3592**.
     c. Pulse **Ir a** > **Gestionar claves y dispositivos**.
     d. O bien, pulse con el botón derecho del ratón en **3592** y seleccione **Gestionar claves y dispositivos**.
     e. En la página de gestión de 3592, seleccione un dispositivo.
     f. Pulse **Suprimir**.
     g. O bien, pulse con el botón derecho del ratón en una unidad y seleccione **Suprimir**.
   - Command-line interface

a. Go to the <*WAS_HOME*>/bin directory. For example,

Windows

```
cd drive:\Program Files\IBM\WebSphere\AppServer\bin
```

Linux

```
cd /opt/IBM/WebSphere/AppServer/bin
```

b. Start the **wsadmin** interface by using an authorized user ID, such as SKLMAdmin. For example,

Windows

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

Linux

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

2. Suprima el dispositivo:
   - Interfaz gráfica de usuario:

     En el diálogo Confirmar, lea el mensaje de confirmación para comprobar que ha seleccionado el dispositivo correcto antes de suprimirlo. Los metadatos de la unidad que suprime, por ejemplo, el número de serie de la unidad, se eliminan de la base de datos de IBM Security Key Lifecycle Manager.

     A continuación, pulse en **Aceptar**.
   - Interfaz de línea de mandatos:

     Escriba tklmDeviceList para localizar un dispositivo y tklmDeviceDelete para suprimir un dispositivo. Debe especificar el uuid. Por ejemplo, escriba:

     ```
     print AdminTask.tklmDeviceList ('[-type 3592]')
     print AdminTask.tklmDeviceDelete
      ('[-uuid DEVICE-74386920-148c-47b2-a1e2-d19194b315cf]')
     ```
   - Interfaz REST:

     Utilice el **Servicio REST Enumerar dispositivos** para ubicar un dispositivo y el **Servicio REST Suprimir dispositivo** para suprimir un dispositivo. Por ejemplo, puede enviar las siguientes solicitudes HTTP:

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

Gestión de imágenes de almacenamiento de DS8000

Puede gestionar imágenes de almacenamiento de DS8000 utilizando IBM Security Key Lifecycle Manager.

Descriptions of some steps describe alternatives by using the graphical user interface, command-line interface, or the REST interface. For any one work session, do not switch between interfaces.

Descriptions of some tasks might mention task-related properties in the SKLMConfig.properties file. Use the graphical user interface, command-line interface, or REST interface to change these properties.

Pasos guiados para crear imágenes de almacenamiento y certificados de imagen

Cuando crea o añade imágenes de almacenamiento y certificados de imagen, IBM Security Key Lifecycle Manager proporciona un conjunto guiado de pasos para completar la tarea.

Las descripciones de algunos pasos pueden incluir alternativas de línea de mandatos para realizar la misma tarea. En un conjunto guiado de tareas, utilice la interfaz gráfica de usuario para completar las tareas.

Creación de un certificado de imagen o una solicitud de certificado

Como primera actividad, cree certificados de imagen o solicitudes de certificado para IBM Security Key Lifecycle Manager.

Acerca de esta tarea

Puede utilizar el diálogo Crear certificado. O bien, puede utilizar los mandatos siguientes o los servicios REST para crear certificados o solicitudes de certificado:

- **tklmCertCreate** o **tklmCertGenRequest**
- **Servicio REST Crear certificado** o el **Servicio REST Generar solicitud de certificado**

Your role must have a permission to the create action and permission to the appropriate device group. To make this certificate the default, your role must have permission to the modify action.

Procedimiento

1. Vaya al directorio o la página apropiada.
   - Interfaz gráfica de usuario:
     a. Inicie una sesión en la interfaz gráfica de usuario.
     b. En la sección clave y dispositivo sección Gestión de claves y dispositivos en la página de bienvenida, seleccione **DS8000**.
     c. Pulse **Ir a** > **Creación guiada de claves y dispositivos**.
     d. O bien, pulse el botón derecho del ratón **DS8000** y seleccione **Creación guiada de claves y dispositivos**.
   - Command-line interface
     a. Go to the *<WAS_HOME>*/bin directory. For example,

        Windows
        ```
        cd drive:\Program Files\IBM\WebSphere\AppServer\bin
        ```

        Linux
        ```
        cd /opt/IBM/WebSphere/AppServer/bin
        ```

     b. Start the **wsadmin** interface by using an authorized user ID, such as SKLMAdmin. For example,

        Windows
        ```
        wsadmin.bat -username SKLMAdmin -password mypwd -lang jython
        ```

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

   - Interfaz REST:
     – Abra un cliente REST.
2. Cree un certificado de imagen o solicite un certificado.

- Interfaz gráfica de usuario:
  a. En la página Paso 1: crear certificados, pulse **Crear** en la tabla **Certificados**.
  b. En el diálogo Crear certificado, seleccione un certificado autofirmado o una solicitud de certificado de un proveedor de terceros.
  c. Especifique valores para los parámetros necesarios y opcionales.
  d. Pulse **Crear certificado**.
- Interfaz de línea de mandatos:
  – Certificado

    Escriba `tklmCertCreate` para crear un certificado y un par de claves pública y privada, y almacene el certificado en un almacén de claves existente. Por ejemplo, escriba:

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

  – Solicitud de certificado

    Escriba `tklmCertGenRequest` para crear un archivo de solicitud de certificado `PKCS #10`. Por ejemplo, escriba:

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

- Interfaz REST:
  – Certificado
    a. Obtenga un identificador de autenticación de usuario exclusivo para acceder a los servicios REST de IBM Security Key Lifecycle Manager. Para obtener más información sobre el proceso de autenticación, consulte Proceso de autenticación de los servicios REST.
    b. Para invocar **`Tipo de lista de dispositivo servicio REST`**, envíe la solicitud HTTP POST. Pase el identificador de autenticación de usuario que ha obtenido en el `Paso a` junto con el mensaje de solicitud, como se muestra en el ejemplo siguiente.

    ```
    POST https://localhost:<puerto>/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 " }
    ```

  – Solicitud de certificado

    Utilice el **`Servicio REST Generar solicitud de certificado`** para crear un archivo de solicitud de certificado `PKCS #10`. Por ejemplo, puede enviar la siguiente solicitud HTTP utilizando un cliente REST:

    ```
    POST https://localhost:<puerto>/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"}
    ```

Qué hacer a continuación

A continuación, vaya al paso siguiente para definir imágenes de almacenamiento específicas y especificar certificados para las imágenes de almacenamiento. Seleccione **Paso 2: Identificar las imágenes** o pulse **Ir al paso siguiente**.

Identificación de imágenes de almacenamiento

Identifique una imagen de almacenamiento (dispositivo) para utilizarla con IBM Security Key Lifecycle Manager.Antes de empezar, cree los certificados de imagen que desee asociar con las imágenes de almacenamiento que va a identificar.

Acerca de esta tarea

Puede utilizar el diálogo Añadir imagen de almacenamiento. O bien, puede utilizar el mandato **tklmDeviceAdd** o el **Servicio REST Añadir dispositivo** para agregar una imagen de almacenamiento.

Puede realizar cualquiera de las siguientes opciones para servir claves a dispositivos.

Only accept manually added devices for communication
All incoming devices are not added to the data store. You must manually specify key service to each device.

Hold new device requests pending my approval
All incoming devices of a valid device group are added to the device store, but are not automatically served keys upon request. You must accept or reject a device in the pending devices list before the device is served keys upon request.

Automatically accept all new device requests for communication
All new incoming devices of a valid device group are added to the data store and are automatically served keys upon request.

Nota: Do not use this setting if you intend to move the new device to another device group. Instead, select manual or pending approval mode to allow an opportunity to move the device into the appropriate device group before any keys are served.

Procedimiento

1. Vaya al directorio o la página apropiada.
   - Interfaz gráfica de usuario:

     Inicie una sesión en la interfaz gráfica de usuario. From the navigation tree, click **IBM Security Key Lifecycle Manager > Welcome**. Scroll down the page to the key and device management section. In **Guided key and device creation**, select **DS8000**. Then, click **Go**.

     a. Inicie una sesión en la interfaz gráfica de usuario.
     b. En la sección clave y dispositivo sección Gestión de claves y dispositivos en la página de bienvenida, seleccione **DS8000**.
     c. Pulse **Ir a** > **Creación guiada de claves y dispositivos**.
     d. O bien, pulse el botón derecho del ratón **DS8000** y seleccione **Creación guiada de claves y dispositivos**.
   - Command-line interface
     a. Go to the *<WAS_HOME>*/bin directory. For example,

Windows

```
cd drive:\Program Files\IBM\WebSphere\AppServer\bin
```

Linux `cd /opt/IBM/WebSphere/AppServer/bin`

b. Start the **wsadmin** interface by using an authorized user ID, such as SKLMAdmin. For example,

Windows

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

Linux

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

- Interfaz REST:
  - Abra un cliente REST.

2. Omita el **Paso 1: Crear certificados**. Pulse el enlace **Ir al paso siguiente** o pulse **Paso 2: Identificar las unidades**.
3. Puede especificar que todos los dispositivos entrantes se añadan a una lista de pendientes, pero que no se les sirvan claves automáticamente cuando se solicite. Debe aceptar o rechazar un dispositivo de la lista de dispositivos pendientes antes de que IBM Security Key Lifecycle Manager sirva las claves al dispositivo cuando se solicite. Your role must have a permission to the modify action and a permission to the appropriate device group.
   - Interfaz gráfica de usuario:

     Seleccione **Retener las solicitudes de dispositivos nuevos pendientes de aprobación**.
   - Interfaz de línea de mandatos:

     Utilice el mandato **tklmDeviceGroupAttributeUpdate** o el **Servicio REST Actualizar atributos de grupo de dispositivos** para establecer el valor del atributo **device.AutoPendingAutoDiscovery**. Por ejemplo, escriba:

     ```
     print AdminTask.tklmDeviceGroupAttributeUpdate ('[-name DS8000
       -attributes "{device.AutoPendingAutoDiscovery 2}"]')
     ```
   - Interfaz REST:
     a. Obtenga un identificador de autenticación de usuario exclusivo para acceder a los servicios REST de IBM Security Key Lifecycle Manager. Para obtener más información sobre el proceso de autenticación, consulte Proceso de autenticación de los servicios REST.
     b. Para ejecutar el **Servicio REST Actualizar atributos de grupo de dispositivos** y establecer el valor del atributo **device.AutoPendingAutoDiscovery**, envíe la solicitud HTTP PUT. Pase el identificador de autenticación de usuario que ha obtenido en el Paso a junto con el mensaje de solicitud, como se muestra en el ejemplo siguiente.

     ```
     PUT https://localhost:<puerto>/SKLM/rest/v1/deviceGroupAttributes
     Content-Type: application/json
     Accept : application/json
     Authorization: SKLMAuth authId=139aeh34567m
     {"name":"DS8000","attributes":"device.AutoPendingAutoDiscovery 2"}
     ```
4. Añada una imagen de almacenamiento.
   - Interfaz gráfica de usuario:
     a. En la página Paso 2: Identificar las imágenes, en la tabla, pulse **Añadir**.
     b. En el diálogo Añadir imagen de almacenamiento, escriba la información necesaria y opcional.
     c. Pulse **Añadir imagen de almacenamiento**.
   - Interfaz de línea de mandatos:

Escriba `tklmDeviceAdd` para añadir una imagen de almacenamiento. Debe especificar el tipo de imagen de almacenamiento, el número de serie y un certificado de imagen. Por ejemplo, escriba:

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

- Interfaz REST:

  Puede utilizar el **Servicio REST Añadir dispositivo** para agregar una imagen de almacenamiento. Por ejemplo, puede enviar la siguiente solicitud HTTP utilizando un cliente REST:

```
POST https://localhost:<puerto>/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"}
```

Qué hacer a continuación

A continuación, puede importar el certificado firmado. O bien, utilice la página Key and Device Management para ver todas las imágenes de almacenamiento y los certificados de imagen.

Administración de las imágenes de almacenamiento y los certificados de imagen

Para administrar las imágenes de almacenamiento y los certificados de imagen, deberá determinar su estado. Puede correlacionar su asociación o bien añadir, modificar o suprimir imágenes de almacenamiento y certificados específicos.

Acerca de esta tarea

Antes de empezar, examine las columnas de la página, que proporciona botones para añadir, modificar o suprimir un elemento de tabla. Para ordenar la información, pulse una cabecera de columna.

Utilice la página Key and Device Management de DS8000 para correlacionar certificados de imagen con imágenes de almacenamiento y determinar el estado de los elementos en la tabla. Puede añadir, modificar o suprimir imágenes de almacenamiento o certificados de imagen. Your role must have a permission to the view action and a permission to the appropriate device group.

La tabla está organizada en estas áreas:

- En las columnas de la izquierda, la información sobre los certificados indica el nombre de certificado, la fecha de caducidad y el estado del certificado.
- En las columnas de la derecha, la información sobre las imágenes de almacenamiento indica el nombre de la imagen de almacenamiento y el certificado de imagen asociado.
- Los iconos de estado indican el estado de un certificado.

Tabla 4. Iconos de estado y su significado

Icono	Descripción
	El certificado está activo.
	El certificado está comprometido.
	El certificado caduca pronto.
	El certificado ha caducado.
	Certificate valid from future date, for migrated certificates with a future use time stamp.
	IBM Security Key Lifecycle Manager tiene solicitudes de certificado de otro proveedor que están de pendientes de ser firmadas e importadas.

Procedimiento

1. Inicie una sesión en la interfaz gráfica de usuario.
   a. En la sección clave y dispositivo sección Gestión de claves y dispositivos en la página de bienvenida, seleccione **DS8000**.
   b. Pulse **Ir a** > **Gestionar claves y dispositivos**.
   c. O bien, pulse con el botón del ratón derecho en **DS8000** y seleccione **Gestionar claves y dispositivos**.

   Descriptions of some steps describe alternatives by using the graphical user interface, command-line interface, or the REST interface. For any one work session, do not switch between interfaces.

   Descriptions of some tasks might mention task-related properties in the `SKLMConfig.properties` file. Use the graphical user interface, command-line interface, or REST interface to change these properties.
2. En la página Key and Device Management de DS8000, puede añadir, modificar o suprimir una imagen de almacenamiento o un certificado de imagen.

   Puede realizar las siguientes tareas administrativas:

   - Añadir

     Pulse **Añadir**. De manera alternativa, puede seleccionar un proceso paso a paso para crear certificados e imágenes de almacenamiento.

     – Certificado

       En la página Crear certificado, seleccione el tipo de certificado como autofirmado o una solicitud de un proveedor de terceros, y complete la información necesaria. A continuación, pulse **Crear certificado**. Your role must have a permission to the create action and permission to the appropriate device group. To make this certificate the default, your role must have permission to the modify action.

     – Imagen de almacenamiento

       En la página Añadir imagen de almacenamiento, escriba la información de la imagen de almacenamiento. A continuación, pulse **Añadir imagen de almacenamiento**. Your role must have a permission to the create action and a permission to the appropriate device group.

     – Utilizar el proceso paso a paso para la creación de certificados e imágenes de almacenamiento

En las páginas Paso 1: Crear certificados y Paso 2: Identificar imágenes, especifique la información necesaria.

El indicador de éxito varía, y muestra un cambio en una columna para el certificado o la imagen de almacenamiento.

- Modificar

  Para cambiar información sobre una imagen de almacenamiento o ver información sobre un certificado, seleccione el certificado o la imagen de almacenamiento y pulse **Modificar**. O bien, pulse con el botón derecho del ratón en el certificado o la imagen de almacenamiento que ha seleccionado. A continuación, pulse **Modificar** o efectúe una doble pulsación en la entrada del certificado o la imagen de almacenamiento.

  – Certificado

    Consulte la información de sólo lectura en la página Modificar el certificado. Your role must have a permission to the modify action and a permission to the appropriate device group.

  – Imagen de almacenamiento

    Especifique cambios en la página Modificar imagen de almacenamiento. A continuación, pulse **Modificar imagen de almacenamiento**. Your role must have a permission to the modify action and a permission to the appropriate device group.

  El indicador de éxito varía, y muestra un cambio en una columna para el certificado o la imagen de almacenamiento. Los cambios de alguna información como, por ejemplo, los campos opcionales, puede que no se proporcionen en la tabla.

- Suprimir

  Para suprimir un certificado o una imagen de almacenamiento, compruebe que se hayan seleccionado el certificado o la imagen de almacenamiento correctos. A continuación, pulse **Suprimir**. O bien, pulse con el botón derecho del ratón en el certificado o la imagen de almacenamiento que ha seleccionado. A continuación, pulse **Suprimir**.

  – Certificado

    Asegúrese de que tiene una copia de seguridad actualizada del almacén de claves antes de suprimir un certificado. Una imagen de almacenamiento grabada utilizando este certificado deja de ser legible después de suprimir el certificado. El certificado que se va a suprimir puede estar en cualquier estado, por ejemplo, activo. Independientemente del estado, no puede suprimir un certificado que esté:

    - Asociado con una imagen de almacenamiento.
    - Marcado por una DS8000 Turbo drive como un certificado primario de una imagen o un certificado secundario de una imagen.

    Deleting a certificate deletes the material from the database.

    Para confirmar la supresión, pulse **Aceptar**. Your role must have a permission to the delete action and a permission to the appropriate device group.

  – Imagen de almacenamiento

    Los metadatos de la imagen de almacenamiento que suprime, por ejemplo, el número de serie, se eliminan de la base de datos de IBM Security Key Lifecycle Manager. Para confirmar la supresión, pulse **Aceptar**. Your role must have a permission to the delete action and a permission to the appropriate device group.

El indicador de éxito es la supresión del certificado o la imagen de almacenamiento de la tabla de administración.

Adición de un certificado de imagen o una solicitud de certificado

Puede añadir más certificados de imagen o solicitudes de certificado para utilizarlos con IBM Security Key Lifecycle Manager. Antes de empezar, determine la política del sitio sobre el uso de certificados.

Acerca de esta tarea

Puede utilizar el diálogo Crear certificado. O bien, puede utilizar los mandatos siguientes o los servicios REST para crear certificados o solicitudes de certificado:

- **tklmCertCreate** o **tklmCertGenRequest**
- **Servicio REST Crear certificado** o el **Servicio REST Generar solicitud de certificado**

Your role must have a permission to the create action and permission to the appropriate device group. To make this certificate the default, your role must have permission to the modify action.

Procedimiento

1. Vaya al directorio o la página apropiada.
   - Interfaz gráfica de usuario:
     a. Inicie una sesión en la interfaz gráfica de usuario.
     b. En la sección clave y dispositivo sección Gestión de claves y dispositivos en la página de bienvenida, seleccione **DS8000**.
     c. Pulse **Ir a** > **Gestionar claves y dispositivos**.
     d. O bien, pulse con el botón del ratón derecho en **DS8000** y seleccione **Gestionar claves y dispositivos**.
     e. En la página de gestión para DS8000, pulse **Añadir**.
     f. Pulse **Certificado**.
   - Command-line interface
     a. Go to the <*WAS_HOME*>/bin directory. For example,

        Windows
        ```
        cd drive:\Program Files\IBM\WebSphere\AppServer\bin
        ```

        Linux
        ```
        cd /opt/IBM/WebSphere/AppServer/bin
        ```

     b. Start the **wsadmin** interface by using an authorized user ID, such as SKLMAdmin. For example,

        Windows
        ```
        wsadmin.bat -username SKLMAdmin -password mypwd -lang jython
        ```

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

2. Cree un certificado o solicite un certificado.
   - Interfaz gráfica de usuario:
     a. En la página Crear certificado, seleccione un certificado autofirmado o una solicitud de certificado de un proveedor de terceros.
     b. Especifique valores para los parámetros necesarios y opcionales. A continuación, pulse **Crear certificado**.
   - Interfaz de línea de mandatos:

– Certificado:

Escriba `tklmCertCreate` para crear un certificado y un par de claves pública y privada, y almacene el certificado en un almacén de claves existente. Por ejemplo, escriba:

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

– Solicitud de certificado:

Escriba `tklmCertGenRequest` para crear un archivo de solicitud de certificado `PKCS #10`. Por ejemplo, escriba:

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

- Interfaz REST:
  – Certificado

  Utilice el **Servicio REST Crear certificado** para crear un certificado y un par de claves pública y privada, y almacene el certificado en un almacén de claves existente. Por ejemplo, puede enviar la siguiente solicitud HTTP utilizando un cliente REST:

```
POST https://localhost:<puerto>/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 " }
```

  – Solicitud de certificado

  Utilice el **Servicio REST Generar solicitud de certificado** para crear un archivo de solicitud de certificado `PKCS #10`. Por ejemplo, puede enviar la siguiente solicitud HTTP utilizando un cliente REST:

```
POST https://localhost:<puerto>/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"}
```

Qué hacer a continuación

La próxima acción depende de si ha creado un certificado o una solicitud de certificado.

- Certificado:

  Puede asociar un certificado con una imagen de almacenamiento específica.

- Solicitud de certificado:

  Envíe manualmente la solicitud de certificado a una entidad emisora de certificados. Cuando se devuelva el certificado firmado, impórtelo utilizando un elemento de acción pendiente en el panel de bienvenida o con el mandato **tklmCertImport** o el **Servicio REST Importar certificado**.

Modificación de un certificado de imagen

Puede utilizar la interfaz gráfica de usuario para ver información de sólo lectura sobre un certificado de imagen en la base de datos de IBM Security Key Lifecycle

Manager. Utilizando la interfaz de línea de mandatos o la interfaz REST, puede cambiar un número limitado de atributos.

Acerca de esta tarea

Puede utilizar el diálogo Modificar certificado para modificar un certificado. O bien, puede utilizar los siguientes mandatos o servicios REST:

- **tklmCertUpdate** o el **Servicio REST Actualizar certificado** para modificar el estado de los certificados como, por ejemplo, de confianza o comprometido, y modificar la información del certificado.
- **tklmDeviceTypeAttributeUpdate** o el **Servicio REST Actualizar atributos de tipo de dispositivos** para establecer el certificado como el certificado primario o secundario.

Your role must have a permission to the modify action and a permission to the appropriate device group.

Nota: Los cambios en la base de datos de IBM Security Key Lifecycle Manager que realiza se configuran en la DS8000 Turbo drive cuando la unidad se pone en contacto con IBM Security Key Lifecycle Manager.

Procedimiento

1. Vaya al directorio o la página apropiada.
   - Interfaz gráfica de usuario:
     a. Inicie una sesión en la interfaz gráfica de usuario.
     b. En la sección clave y dispositivo sección Gestión de claves y dispositivos en la página de bienvenida, seleccione **DS8000**.
     c. Pulse **Ir a** > **Gestionar claves y dispositivos**.
     d. O bien, pulse con el botón del ratón derecho en **DS8000** y seleccione **Gestionar claves y dispositivos**.
     e. En la página de gestión de DS8000, seleccione un certificado en la columna **Certificados**.
     f. Pulse **Modificar**.
     g. O bien, pulse con el botón derecho del ratón en un certificado y seleccione **Modificar**, o efectúe una doble pulsación en una entrada de certificado.
   - Command-line interface
     a. Go to the <*WAS_HOME*>/bin directory. For example,

        Windows
        ```
        cd drive:\Program Files\IBM\WebSphere\AppServer\bin
        ```

        Linux
        ```
        cd /opt/IBM/WebSphere/AppServer/bin
        ```

     b. Start the **wsadmin** interface by using an authorized user ID, such as SKLMAdmin. For example,

        Windows
        ```
        wsadmin.bat -username SKLMAdmin -password mypwd -lang jython
        ```

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

2. Vea (interfaz gráfica de usuario) o modifique (interfaz de línea de mandatos) la información del certificado.
   - Interfaz gráfica de usuario:

En el diálogo Modificar el certificado, vea los campos de sólo lectura.

- Interfaz de línea de mandatos:

  Escriba `tklmCertList` para buscar un certificado y `tklmCertUpdate` para actualizar un certificado. Debe especificar el uuid del certificado y el atributo modificado. Por ejemplo, para cambiar la información, escriba:

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

- Interfaz REST:

  Utilice el **Servicio REST Enumerar certificado** para buscar un certificado. Por ejemplo, puede enviar la siguiente solicitud HTTP:

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

  Utilice el **Servicio REST Actualizar certificado** para actualizar un certificado. Por ejemplo, puede enviar la siguiente solicitud HTTP:

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

Qué hacer a continuación

A continuación, puede utilizar la página Key and Device Management de DS8000 para asociar certificados de imagen con imágenes de almacenamiento específicas.

Supresión de un certificado de imagen

Puede suprimir un certificado de imagen seleccionado, que se puede encontrar en cualquier estado como, por ejemplo, activo. No puede suprimir un certificado que esté asociado a una imagen de almacenamiento. Tampoco puede suprimir un certificado que esté identificado como el certificado primario de una imagen o un certificado secundario de una imagen. Por ejemplo, puede suprimir un certificado caducado.

Acerca de esta tarea

Antes de empezar, asegúrese de que exista una copia de seguridad del almacén de claves que contiene el certificado de imagen que desea suprimir. Compruebe que el certificado no esté asociado actualmente con una imagen de almacenamiento. Determine el estado actual del certificado y asegúrese de que la supresión de un certificado en este estado cumple las políticas del sitio.

Delete certificates only when the data protected by those certificates is no longer needed. Deleting certificates is like erasing the data. After certificates are deleted, data that is protected by those certificates is not retrievable.

Puede utilizar el elemento de menú Suprimir o el mandato **tklmCertDelete** o el **Servicio REST Suprimir certificado** para suprimir un certificado de imagen de

almacenamiento. Your role must have a permission to the delete action and a permission to the appropriate device group.

Deleting a certificate deletes the material from the database.

Procedimiento

1. Vaya al directorio o la página apropiada.
   - Interfaz gráfica de usuario:
     a. Inicie una sesión en la interfaz gráfica de usuario.
     b. En la sección clave y dispositivo sección Gestión de claves y dispositivos en la página de bienvenida, seleccione **DS8000**.
     c. Pulse **Ir a** > **Gestionar claves y dispositivos**.
     d. O bien, pulse con el botón del ratón derecho en **DS8000** y seleccione **Gestionar claves y dispositivos**.
     e. En la página de gestión de DS8000, seleccione un certificado en la columna **Certificados**.
     f. Pulse **Suprimir**.
     g. O bien, pulse con el botón derecho del ratón en un certificado y seleccione **Suprimir**.
   - Command-line interface
     a. Go to the <*WAS_HOME*>/bin directory. For example,

        Windows
        ```
        cd drive:\Program Files\IBM\WebSphere\AppServer\bin
        ```

        Linux
        ```
        cd /opt/IBM/WebSphere/AppServer/bin
        ```

     b. Start the **wsadmin** interface by using an authorized user ID, such as SKLMAdmin. For example,

        Windows
        ```
        wsadmin.bat -username SKLMAdmin -password mypwd -lang jython
        ```

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

2. Suprima el certificado.
   - Interfaz gráfica de usuario:

     En el diálogo Confirmar, lea el mensaje de confirmación para comprobar que ha seleccionado el certificado correcto antes de suprimirlo. A continuación, pulse en **Aceptar**.
   - Interfaz de línea de mandatos:

     Escriba tklmCertList para buscar un certificado y tklmCertDelete para suprimir un certificado. Debe especificar el alias de certificado y el nombre del almacén de claves. Por ejemplo, para suprimir un certificado caducado que no está asociado actualmente con una imagen de almacenamiento, escriba:

     ```
     print AdminTask.tklmCertList('[-usage DS8000 -v y]')
     print AdminTask.tklmCertDelete ('[-alias mycertalias
      -keyStoreName defaultKeyStore]')
     ```
   - Interfaz REST:

     Utilice el **Servicio REST Enumerar certificado** para buscar un certificado y el **Servicio REST Suprimir certificado** para suprimir un certificado. Por ejemplo, puede enviar las siguientes solicitudes HTTP:

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

Qué hacer a continuación

A continuación, puede hacer otra copia de seguridad del almacén de claves para reflejar correctamente el cambio en los certificados.

Adición de una imagen de almacenamiento

Puede añadir una imagen de almacenamiento a la base de datos de IBM Security Key Lifecycle Manager.Antes de empezar, cree los certificados que desee asociar con las imágenes de almacenamiento que va a identificar. Asimismo, obtenga el número de serie de la imagen de almacenamiento y otra información descriptiva.

Acerca de esta tarea

Puede utilizar el diálogo Añadir imagen de almacenamiento o puede utilizar el mandato **tklmDeviceAdd** o el **Servicio REST Añadir dispositivo** para añadir una imagen de almacenamiento. Your role must have a permission to the create action and a permission to the appropriate device group.

Procedimiento

1. Vaya al directorio o la página apropiada.
   - Interfaz gráfica de usuario:
     a. Inicie una sesión en la interfaz gráfica de usuario.
     b. En la sección clave y dispositivo sección Gestión de claves y dispositivos en la página de bienvenida, seleccione **DS8000**.
     c. Pulse **Ir a** > **Gestionar claves y dispositivos**.
     d. O bien, pulse con el botón del ratón derecho en **DS8000** y seleccione **Gestionar claves y dispositivos**.
     e. En la página de gestión para DS8000, pulse **Añadir**.
     f. Pulse **Imagen de almacenamiento**.
   - Command-line interface
     a. Go to the <*WAS_HOME*>/bin directory. For example,

        Windows
        ```
        cd drive:\Program Files\IBM\WebSphere\AppServer\bin
        ```

        Linux
        ```
        cd /opt/IBM/WebSphere/AppServer/bin
        ```

     b. Start the **wsadmin** interface by using an authorized user ID, such as SKLMAdmin. For example,

        Windows
        ```
        wsadmin.bat -username SKLMAdmin -password mypwd -lang jython
        ```

        Linux
        ```
        ./wsadmin.sh -username SKLMAdmin -password mypwd -lang jython
        ```
2. Añada una imagen de almacenamiento.

- Interfaz gráfica de usuario:

  En el diálogo Añadir imagen de almacenamiento, escriba la información necesaria y opcional. A continuación, pulse **Añadir imagen de almacenamiento**.
- Interfaz de línea de mandatos:

  Escriba `tklmDeviceAdd` para añadir una imagen de almacenamiento. Debe especificar el tipo de imagen de almacenamiento, el número de serie y un certificado de imagen. Por ejemplo, escriba:

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

  Utilice el **Servicio REST Añadir dispositivo** para agregar una imagen de almacenamiento. Por ejemplo, puede enviar la siguiente solicitud HTTP:

  ```
  POST https://localhost:<puerto>/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"}
  ```

Qué hacer a continuación

A continuación, puede determinar el estado de la imagen de almacenamiento que ha añadido.

Modificación de una imagen de almacenamiento

Puede modificar información sobre una imagen de almacenamiento en la base de datos de IBM Security Key Lifecycle Manager. Por ejemplo, puede actualizar la descripción de la imagen de almacenamiento.

Acerca de esta tarea

Antes de empezar, cree los certificados que desee asociar con las imágenes de almacenamiento que va a modificar. Si utiliza la interfaz de línea de mandatos, obtenga el valor del uuid de la imagen de almacenamiento que desea actualizar y el alias de los certificados asociados con la imagen de almacenamiento.

Puede utilizar el diálogo Modificar imagen de almacenamiento o puede utilizar el mandato **tklmDeviceUpdate** o el **Servicio REST Actualizar dispositivo** para actualizar una imagen de almacenamiento. Your role must have a permission to the modify action and a permission to the appropriate device group.

Procedimiento

1. Vaya al directorio o la página apropiada.
   - Interfaz gráfica de usuario:
     a. Inicie una sesión en la interfaz gráfica de usuario.
     b. En la sección clave y dispositivo sección Gestión de claves y dispositivos en la página de bienvenida, seleccione **DS8000**.
     c. Pulse **Ir a** > **Gestionar claves y dispositivos**.
     d. O bien, pulse con el botón del ratón derecho en **DS8000** y seleccione **Gestionar claves y dispositivos**.

e. En la página de gestión de DS8000, seleccione un dispositivo.
f. Pulse **Modificar**.
g. O bien, pulse con el botón derecho del ratón en una unidad y seleccione **Modificar**, o efectúe una doble pulsación en una entrada de unidad.

- Command-line interface
  a. Go to the *<WAS_HOME>*/bin directory. For example,

     Windows
     ```
     cd drive:\Program Files\IBM\WebSphere\AppServer\bin
     ```

     Linux
     ```
     cd /opt/IBM/WebSphere/AppServer/bin
     ```

  b. Start the **wsadmin** interface by using an authorized user ID, such as SKLMAdmin. For example,

     Windows
     ```
     wsadmin.bat -username SKLMAdmin -password mypwd -lang jython
     ```

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

2. Modifique una imagen de almacenamiento.
   - Interfaz gráfica de usuario:

     En el diálogo Modificar imagen de almacenamiento, escriba la información modificada. A continuación, pulse **Modificar imagen de almacenamiento**.
   - Interfaz de línea de mandatos:

     Escriba tklmDeviceUpdate para actualizar una imagen de almacenamiento. Debe especificar el uuid de la imagen de almacenamiento y los atributos que cambian. Por ejemplo, escriba:
     ```
     print AdminTask.tklmDeviceUpdate
      ('[-uuid DEVICE-15d499ad-3ad8-3333-8c84-64cb9e11d990
       -attributes "{description myDevice}"]')
     ```
   - Interfaz REST:

     Utilice el **Servicio REST Actualizar dispositivo** para actualizar una imagen de almacenamiento. Por ejemplo, puede enviar la siguiente solicitud HTTP:
     ```
     PUT https://localhost:<puerto>/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"}
     ```

Supresión de una imagen de almacenamiento

Puede suprimir una imagen de almacenamiento. Los metadatos de la imagen de almacenamiento que suprime, por ejemplo, el número de serie, se eliminan de la base de datos de IBM Security Key Lifecycle Manager.

Acerca de esta tarea

Antes de empezar, asegúrese de que exista una copia de seguridad actualizada de los certificados y las imágenes de almacenamiento en el sitio. Si utiliza la interfaz de línea de mandatos, obtenga el uuid de la imagen de almacenamiento que desea suprimir.

Puede utilizar el elemento de menú Suprimir o el mandato **tklmDeviceDelete** o el **Servicio REST Suprimir dispositivo** para suprimir una imagen de almacenamiento. Your role must have a permission to the delete action and a permission to the appropriate device group.

Procedimiento

1. Vaya al directorio o la página apropiada.
   - Interfaz gráfica de usuario:
     a. Inicie una sesión en la interfaz gráfica de usuario.
     b. En la sección clave y dispositivo sección Gestión de claves y dispositivos en la página de bienvenida, seleccione **DS8000**.
     c. Pulse **Ir a** > **Gestionar claves y dispositivos**.
     d. O bien, pulse con el botón del ratón derecho en **DS8000** y seleccione **Gestionar claves y dispositivos**.
     e. En la página de gestión de DS8000, seleccione un dispositivo.
     f. Pulse **Suprimir**.
     g. O bien, pulse con el botón derecho del ratón en una unidad y seleccione **Suprimir**.
   - Command-line interface
     a. Go to the <*WAS_HOME*>/bin directory. For example,

        Windows
        ```
        cd drive:\Program Files\IBM\WebSphere\AppServer\bin
        ```

        Linux
        ```
        cd /opt/IBM/WebSphere/AppServer/bin
        ```

     b. Start the **wsadmin** interface by using an authorized user ID, such as SKLMAdmin. For example,

        Windows
        ```
        wsadmin.bat -username SKLMAdmin -password mypwd -lang jython
        ```

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

2. Suprima la imagen de almacenamiento.
   - Interfaz gráfica de usuario:

     En la página Confirmar, lea el mensaje de confirmación para comprobar que ha seleccionado la imagen de almacenamiento correcta antes de suprimirla. Los metadatos de la imagen de almacenamiento que suprime, por ejemplo, el número de serie, se eliminan de la base de datos de IBM Security Key Lifecycle Manager.

     A continuación, pulse en **Aceptar**.
   - Interfaz de línea de mandatos:

     Escriba tklmDeviceList para localizar un dispositivo y tklmDeviceDelete para suprimir una imagen de almacenamiento. Debe especificar el uuid. Por ejemplo, escriba:

     ```
     print AdminTask.tklmDeviceList ('[-type DS8000]')
     print AdminTask.tklmDeviceDelete
      ('[-uuid DEVICE-74386920-148c-47b2-a1e2-d19194b315cf]')
     ```
   - Interfaz REST:

     Utilice el **Servicio REST Enumerar dispositivos** para ubicar un dispositivo y el **Servicio REST Suprimir dispositivo** para suprimir una imagen de almacenamiento. Por ejemplo, puede enviar las siguientes solicitudes HTTP:

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

Gestión de una DS5000

Puede gestionar las DS5000 storage servers utilizando IBM Security Key Lifecycle Manager.

Administración de dispositivos, claves y asociaciones de dispositivos

Para administrar los DS5000 storage servers, correlacione un dispositivo con claves o máquinas.

Acerca de esta tarea

Your role must have a permission to the view action and a permission to the appropriate device group. Utilice la página Key and Device Management de DS5000 para añadir, modificar o suprimir un dispositivo, clave o asociación. Estas acciones requieren más permisos.

Antes de empezar, examine las columnas de la página, que proporciona botones para añadir, modificar o suprimir un elemento de tabla. Para ordenar la información, pulse una cabecera de columna.

La tabla está organizada en las siguientes áreas de información:

- Dispositivos y las máquinas asociadas.
- Clave actual que utiliza el dispositivo y una descripción del mismo.

Procedimiento

1. Inicie una sesión en la interfaz gráfica de usuario.
   a. En la sección clave y dispositivo sección Gestión de claves y dispositivos en la página de bienvenida, seleccione **DS5000**.
   b. Pulse **Ir a** > **Gestionar claves y dispositivos**.
   c. O bien, pulse con el botón del ratón derecho en **DS5000** y seleccione **Gestionar claves y dispositivos**.

   Descriptions of some steps describe alternatives by using the graphical user interface, command-line interface, or the REST interface. For any one work session, do not switch between interfaces.

   Descriptions of some tasks might mention task-related properties in the `SKLMConfig.properties` file. Use the graphical user interface, command-line interface, or REST interface to change these properties.
2. Puede añadir, modificar o suprimir una clave, un dispositivo o una asociación de máquina.

   Puede realizar las siguientes tareas administrativas:

   - Renovar la lista.

     Click the refresh icon  to refresh items in the table.
   - Añadir

     Pulse **Añadir**.

     – Dispositivo

En el diálogo Añadir dispositivo, escriba el número de serie del dispositivo y otra información. A continuación, pulse **Añadir dispositivo**. Your role must have a permission to the create action and a permission to the appropriate device group.

– Más claves

Seleccione un dispositivo y, a continuación, seleccione **Añadir > Más claves**. En el diálogo Añadir clave, especifique la información necesaria como, por ejemplo, el número de claves que desea crear, hasta un máximo de 12. A continuación, pulse **Añadir > Más claves**. Your role must have a permission to the create action and a permission to the appropriate device group.

– Asociación

Cuando seleccione el recuadro de selección **Afinidad de la máquina** en la página Gestión de claves y dispositivos, el valor de la propiedad **`device.enableMachineAffinity`** se establece en true. Si utiliza la afinidad de la máquina, puede establecer el servicio de claves para combinaciones específicas de dispositivos y máquinas.

Si se habilita la afinidad de la máquina, utilice el diálogo Añadir asociación para especificar la información necesaria como, por ejemplo, el ID de máquina. A continuación, pulse **Añadir asociación**. Your role must have a permission to the create action and a permission to the appropriate device group.

El indicador de éxito varía y muestra la adición de un dispositivo, claves o una asociación.

• Modificar

Para cambiar un dispositivo o las claves, seleccione el dispositivo y, a continuación, pulse **Modificar**. O bien, pulse con el botón derecho del ratón en el dispositivo seleccionado. A continuación, pulse una de las opciones, por ejemplo, **Modificar dispositivo**.

– Dispositivo

Especifique cambios en el diálogo Modificar dispositivo. A continuación, pulse **Modificar dispositivo**.Your role must have a permission to the modify action and a permission to the appropriate device group.

– Claves

Seleccione una clave en el diálogo Modificar claves. A continuación, pulse **Suprimir**. Your role must have a permission to the delete action and a permission to the appropriate device group.

El indicador de éxito varía, y muestra un cambio en una columna para el dispositivo o la clave.

• Suprimir

Para suprimir un dispositivo, selecciónelo y pulse **Suprimir**. O bien, pulse con el botón derecho del ratón en el dispositivo seleccionado. A continuación, pulse **Suprimir**. Antes de suprimir el dispositivo, utilice el mandato **`tklmMachineDeviceDelete`** para eliminar la asociación de un dispositivo de un identificador de máquina existente en la base de datos de IBM Security Key Lifecycle Manager.

Los metadatos del dispositivo que suprime, por ejemplo, el número de serie del dispositivo, se eliminan de la base de datos de IBM Security Key Lifecycle Manager. Los datos de las claves también se eliminan. Para confirmar la supresión, pulse **Aceptar**. Your role must have a permission to the delete action and a permission to the appropriate device group.

El indicador de éxito es la supresión del dispositivo de la tabla.

Adición de un dispositivo

Puede añadir un dispositivo a la base de datos de IBM Security Key Lifecycle Manager.

Acerca de esta tarea

Si la afinidad de la máquina está habilitada, la adición de un dispositivo requiere también la adición de una relación entre un dispositivo y una máquina. De lo contrario, las claves no se sirven al dispositivo añadido. Si utiliza la afinidad de la máquina, puede establecer el servicio de claves para combinaciones específicas de dispositivos y máquinas.

Puede utilizar el diálogo Añadir dispositivo, el mandato **tklmDeviceAdd** o el **Servicio REST Añadir dispositivo** para añadir un dispositivo. Your role must have a permission to the create action and a permission to the appropriate device group.

Procedimiento

1. Vaya al directorio o la página apropiada.
   - Interfaz gráfica de usuario:
     a. Inicie una sesión en la interfaz gráfica de usuario.
     b. En la sección clave y dispositivo sección Gestión de claves y dispositivos en la página de bienvenida, seleccione **DS5000**.
     c. Pulse **Ir a** > **Gestionar claves y dispositivos**.
     d. O bien, pulse con el botón del ratón derecho en **DS5000** y seleccione **Gestionar claves y dispositivos**.
     e. En la página de gestión para DS5000, pulse **Añadir**.
     f. Pulse **Dispositivo**.
   - Command-line interface
     a. Go to the <*WAS_HOME*>/bin directory. For example,

        Windows
        ```
        cd drive:\Program Files\IBM\WebSphere\AppServer\bin
        ```

        Linux
        ```
        cd /opt/IBM/WebSphere/AppServer/bin
        ```

     b. Start the **wsadmin** interface by using an authorized user ID, such as SKLMAdmin. For example,

        Windows
        ```
        wsadmin.bat -username SKLMAdmin -password mypwd -lang jython
        ```

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

   - Interfaz REST:
     – Abra un cliente REST.
2. Añada un dispositivo.
   - Interfaz gráfica de usuario:

     En el diálogo Añadir dispositivo, escriba la información necesaria y opcional. A continuación, pulse **Añadir dispositivo**.
   - Interfaz de línea de mandatos:

     Escriba tklmDeviceAdd para añadir un dispositivo. Debe especificar el número de serie del dispositivo y el grupo de dispositivos. Por ejemplo, escriba:

```
print AdminTask.tklmDeviceAdd ('[-type DS5000 -serialNumber CDA39403AQJF
  -attributes "{worldwideName ABCdeF1234567890}
  {description marketingDivisionDrive}
  {keyPrefix AEF}
  {numberOfKeys 10}
  {deviceText abcdefghijklmnopqrst}
  {machineID 30423830303034370000000000000}"]')
```

- Interfaz REST:
  a. Obtenga un identificador de autenticación de usuario exclusivo para acceder a los servicios REST de IBM Security Key Lifecycle Manager. Para obtener más información sobre el proceso de autenticación, consulte Proceso de autenticación de los servicios REST.
  b. Para invocar el **Servicio REST Añadir dispositivo**, envíe la solicitud HTTP POST. Pase el identificador de autenticación de usuario que ha obtenido en el Paso a junto con el mensaje de solicitud, como se muestra en el ejemplo siguiente.

```
POST https://localhost:<puerto>/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"}
```

Qué hacer a continuación

A continuación, puede asociar el dispositivo con una máquina.

Modificación de un dispositivo

Puede modificar información sobre un dispositivo en la base de datos de IBM Security Key Lifecycle Manager. Por ejemplo, puede actualizar la descripción de la unidad.

Acerca de esta tarea

Puede utilizar el diálogo Modificar dispositivo. O bien, puede utilizar el mandato **tklmDeviceUpdate** o el **Servicio REST Actualizar dispositivo** para actualizar un dispositivo. Your role must have a permission to the modify action and a permission to the appropriate device group.

Antes de empezar, si utiliza la interfaz REST o de línea de mandatos, obtenga el valor del uuid del dispositivo que desea actualizar.

Procedimiento

1. Vaya al directorio o la página apropiada.
   - Interfaz gráfica de usuario:
     a. Inicie una sesión en la interfaz gráfica de usuario.
     b. En la sección clave y dispositivo sección Gestión de claves y dispositivos en la página de bienvenida, seleccione **DS5000**.
     c. Pulse **Ir a** > **Gestionar claves y dispositivos**.
     d. O bien, pulse con el botón del ratón derecho en **DS5000** y seleccione **Gestionar claves y dispositivos**.
     e. En la página de gestión de DS5000, seleccione un dispositivo en la columna **Número de serie del dispositivo**.
     f. Pulse **Modificar dispositivo**.

g. O bien, pulse con el botón derecho del ratón en una unidad y seleccione **Modificar dispositivo**, o efectúe una doble pulsación en una entrada de dispositivo.

- Command-line interface

a. Go to the <*WAS_HOME*>/bin directory. For example,

Windows

```
cd drive:\Program Files\IBM\WebSphere\AppServer\bin
```

Linux

```
cd /opt/IBM/WebSphere/AppServer/bin
```

b. Start the **wsadmin** interface by using an authorized user ID, such as SKLMAdmin. For example,

Windows

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

Linux

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

2. Modifique un dispositivo.

- Interfaz gráfica de usuario:

  En el diálogo Modificar dispositivo, escriba la información modificada. A continuación, pulse **Modificar dispositivo**.

- Interfaz de línea de mandatos:

  Escriba tklmDeviceUpdate para actualizar un dispositivo. Debe especificar el uuid del dispositivo y los atributos que cambian. Por ejemplo, escriba:

```
print AdminTask.tklmDeviceUpdate
 ('[-uuid DEVICE-15d499ad-3ad8-3333-8c84-64cb9e11d990
  -attributes "{description myDevice}"]')
```

- Interfaz REST:

  Utilice el **Servicio REST Actualizar dispositivo** para actualizar un dispositivo. Por ejemplo, envíe la siguiente solicitud HTTP:

```
PUT https://localhost:<puerto>/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"}
```

Qué hacer a continuación

A continuación, puede comprobar que se han realizado los cambios.

Supresión de un dispositivo

Puede suprimir un dispositivo como, por ejemplo, un DS5000 storage server. Al suprimir un dispositivo se eliminarán los datos del número de serie de dispositivo y de sus claves de la base de datos de IBM Security Key Lifecycle Manager.

Acerca de esta tarea

Si el dispositivo pertenece a la DS5000 device family y la afinidad de la máquina está habilitada, la supresión del dispositivo también suprime las relaciones entre un dispositivo y una máquina.

Puede utilizar el elemento de menú Suprimir o el mandato **tklmDeviceDelete** o el **Servicio REST Suprimir dispositivo** para suprimir un dispositivo. Your role must have a permission to the delete action and a permission to the appropriate device group.

Procedimiento

1. Vaya al directorio o la página apropiada.
   - Interfaz gráfica de usuario:
     a. Inicie una sesión en la interfaz gráfica de usuario.
     b. En la sección clave y dispositivo sección Gestión de claves y dispositivos en la página de bienvenida, seleccione **DS5000**.
     c. Pulse **Ir a** > **Gestionar claves y dispositivos**.
     d. O bien, pulse con el botón del ratón derecho en **DS5000** y seleccione **Gestionar claves y dispositivos**.
     e. En la página de gestión de DS5000, seleccione un dispositivo.
     f. Pulse **Suprimir**.
     g. O bien, pulse con el botón derecho del ratón en una unidad y seleccione **Suprimir**.
   - Command-line interface
     a. Go to the <*WAS_HOME*>/bin directory. For example,

        Windows
        ```
        cd drive:\Program Files\IBM\WebSphere\AppServer\bin
        ```

        Linux
        ```
        cd /opt/IBM/WebSphere/AppServer/bin
        ```

     b. Start the **wsadmin** interface by using an authorized user ID, such as SKLMAdmin. For example,

        Windows
        ```
        wsadmin.bat -username SKLMAdmin -password mypwd -lang jython
        ```

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

2. Utilizando la interfaz de línea de mandatos, ejecute el mandato **tklmMachineDeviceList** o utilice el **Servicio REST Enumerar dispositivos de máquina** para obtener el uuid del dispositivo que desea suprimir. Utilice el mandato **tklmMachineDeviceDelete** o el **Servicio REST Suprimir dispositivo de máquina** para suprimir las asociaciones que tiene el dispositivo con las máquinas.

   Por ejemplo, escriba:

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

   ```
   print AdminTask.tklmMachineDeviceDelete
   ('[-deviceUUID DEVICE-663b6d37-e6d5-4c9f-af90-e40e48d27f3c
    -machineID 30423830303034370000000000000]')
   ```

   Puede enviar las siguientes solicitudes HTTP:

   ```
   GET https://localhost:<puerto>/SKLM/rest/v1/machines/device?machineID=
   30423830303034370000000000000
   Content-Type: application/json
   Accept : application/json
   Authorization: SKLMAuth authId=139aeh34567m
   ```

   ```
   DELETE https://localhost:<puerto>/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. Suprima el dispositivo.
   - Interfaz gráfica de usuario:

En el diálogo Confirmar, lea el mensaje de confirmación antes de suprimir el dispositivo. Al suprimir un dispositivo se eliminarán los datos del número de serie de dispositivo y de sus claves de la base de datos de IBM Security Key Lifecycle Manager.

A continuación, pulse en **Aceptar**.

- Interfaz de línea de mandatos:

  Escriba `tklmDeviceDelete` para suprimir un dispositivo. Debe especificar el uuid. Por ejemplo, escriba:

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

- Interfaz REST:

  Utilice el **Servicio REST Suprimir dispositivo** para suprimir un dispositivo. Por ejemplo, puede enviar la siguiente solicitud HTTP:

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

Adición de claves

Puede añadir más claves para utilizarlas uso con DS5000 storage servers. Antes de empezar, determine la política del sitio para la denominación de prefijos de claves.

Acerca de esta tarea

Puede utilizar el diálogo Agregar clave, el mandato **tklmSecretKeyCreate** o el **Servicio REST Crear clave secreta** para crear una o más claves simétricas en el grupo existente. Your role must have a permission to the create action and a permission to the appropriate device group.

Procedimiento

1. Vaya al directorio o la página apropiada.
   - Interfaz gráfica de usuario:
     a. Inicie una sesión en la interfaz gráfica de usuario.
     b. En la sección clave y dispositivo sección Gestión de claves y dispositivos en la página de bienvenida, seleccione **DS5000**.
     c. Pulse **Ir a** > **Gestionar claves y dispositivos**.
     d. O bien, pulse con el botón del ratón derecho en **DS5000** y seleccione **Gestionar claves y dispositivos**.
     e. En la página de gestión para `DS5000`, pulse **Añadir**.
     f. Pulse **Más claves**.
   - Command-line interface
     a. Go to the *<WAS_HOME>*`/bin` directory. For example,

        Windows
        ```
        cd drive:\Program Files\IBM\WebSphere\AppServer\bin
        ```

        Linux `cd /opt/IBM/WebSphere/AppServer/bin`

     b. Start the **wsadmin** interface by using an authorized user ID, such as `SKLMAdmin`. For example,

        Windows
        ```
        wsadmin.bat -username SKLMAdmin -password mypwd -lang jython
        ```

Linux

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

- Interfaz REST:
  - Abra un cliente REST.

2. Cree claves.
   - Interfaz gráfica de usuario

     En el diálogo Añadir clave, especifique valores para los parámetros necesarios. A continuación, pulse **Añadir más claves**.
   - Interfaz de línea de mandatos:
     a. Utilice el mandato **tklmGroupList** para obtener el valor de uuid del grupo de claves. Por ejemplo, escriba:

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

     La salida será parecida a la de este ejemplo:

     ```
     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
     .
     . (Los elementos restantes no se muestran en este ejemplo).
     .
     ```

     b. Cree más claves y almacénelas en el grupo. Por ejemplo, escriba:

     ```
     print AdminTask.tklmSecretKeyCreate ('[-alias abc
      -keyStoreName defaultKeyStore -numOfKeys 10 -usage DS5000
       -keyGroupUuid KEYGROUP-9c97d9aa-b5f0-41a1-b65f-119756168211]')
     ```

   - Interfaz REST:
     a. Obtenga un identificador de autenticación de usuario exclusivo para acceder a los servicios REST de IBM Security Key Lifecycle Manager. Para obtener más información sobre el proceso de autenticación, consulte Proceso de autenticación de los servicios REST.
     b. Para invocar **Servicio REST Enumerar grupos**, envíe la solicitud HTTP GET. Pase el identificador de autenticación de usuario que ha obtenido en el Paso a junto con el mensaje de solicitud, como se muestra en el ejemplo siguiente.

     ```
     GET https://localhost:<puerto>/SKLM/rest/v1/keygroups
     Content-Type: application/json
     Accept : application/json
     Authorization: SKLMAuth authId=139aeh34567m
     Accept-Language : en
     ```

     La salida será parecida a la de este ejemplo:

     ```
     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. Utilice el **Servicio REST Crear clave secreta** para crear más claves y almacenarlas en el grupo. Por ejemplo, puede enviar la siguiente solicitud HTTP:

```
POST https://localhost:<puerto>/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. El indicador de éxito varía dependiendo de la interfaz:
   - Interfaz gráfica de usuario:

     Las claves adicionales están visibles en la tabla de claves en la página Modificar claves. Realice una copia de seguridad de nuevas claves antes de que las claves se sirvan a los dispositivos.
   - Interfaz de línea de mandatos:

     Los mensajes de finalización indican que la operación se ha realizado correctamente. Asimismo, vuelva a ejecutar el mandato **tklmGroupList** para comprobar que las claves que ha añadido aparecen ahora en el grupo de claves. Por ejemplo, escriba:

     ```
     print AdminTask.tklmGroupList ('[-type keygroup -v y]')
     ```
   - Interfaz REST:

     El código de estado `200 OK` indica que la operación ha sido satisfactoria.

Qué hacer a continuación

A continuación, puede asociar el dispositivo con una máquina.

Modificación (supresión) de claves

Puede modificar el número de claves que utiliza un DS5000 storage server suprimiendo una o varias claves. Antes de empezar, determine la información modificada como, por ejemplo, el número de claves que desea suprimir.

Acerca de esta tarea

Delete keys only when the data protected by those keys is no longer needed. Deleting keys is like erasing the data. After keys are deleted, data that is protected by those keys is not retrievable.

Puede utilizar el diálogo Modificar claves, el mandato **tklmKeyDelete** o el **Servicio REST Suprimir clave**. Your role must have a permission to the modify action and a permission to the appropriate device group.

Procedimiento

1. Vaya al directorio o la página apropiada.
   - Interfaz gráfica de usuario:
     a. Inicie una sesión en la interfaz gráfica de usuario.
     b. En la sección clave y dispositivo sección Gestión de claves y dispositivos en la página de bienvenida, seleccione **DS5000**.
     c. Pulse **Ir a** > **Gestionar claves y dispositivos**.
     d. O bien, pulse con el botón del ratón derecho en **DS5000** y seleccione **Gestionar claves y dispositivos**.
   - Command-line interface
     a. Go to the <*WAS_HOME*>/bin directory. For example,

        Windows
        ```
        cd drive:\Program Files\IBM\WebSphere\AppServer\bin
        ```

        Linux
        ```
        cd /opt/IBM/WebSphere/AppServer/bin
        ```

     b. Start the **wsadmin** interface by using an authorized user ID, such as SKLMAdmin. For example,

        Windows
        ```
        wsadmin.bat -username SKLMAdmin -password mypwd -lang jython
        ```

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

2. Modifique la información de claves.
   - Interfaz gráfica de usuario:

     En la página de gestión de DS5000, seleccione un dispositivo en la columna **Número de serie del dispositivo**.A continuación, pulse **Modificar > Claves**. O bien, pulse con el botón derecho del ratón en un dispositivo y seleccione **Modificar claves**.

     A continuación, en el diálogo Modificar claves, seleccione una clave y pulse **Suprimir**. Lea el mensaje de confirmación. A continuación, pulse en **Aceptar**.
   - Interfaz de línea de mandatos:

     Puede suprimir una clave. Your role must have a permission to the delete action and a permission to the appropriate device group. Por ejemplo, escriba:
     ```
     print AdminTask.tklmKeyDelete ('[-alias aaa000000000000000000
      -keyStoreName defaultKeyStore]')
     ```
   - Interfaz REST:

     Utilice el **Servicio REST Suprimir clave** para suprimir una clave. Por ejemplo, puede enviar la siguiente solicitud HTTP:
     ```
     DELETE https://localhost:<puerto>/SKLM/rest/v1/keys/aaa000000000000000000
     Content-Type: application/json
     Accept : application/json
     Authorization: SKLMAuth authId=139aeh34567m
     ```

Qué hacer a continuación

A continuación, puede asociar el dispositivo con una máquina.

Gestión de archivos GPFS (IBM Spectrum Scale)

Se puede utilizar el sistema de archivos GPFS para gestionar claves en IBM Security Key Lifecycle Manager.

GPFS (IBM Spectrum Scale) es una solución de gestión de archivos de disco compartido de alto rendimiento que proporciona un acceso fiable y rápido a los datos de varios nodos en un entorno de clúster. Las aplicaciones pueden fácilmente acceder a los archivos utilizando las interfaces de sistema de archivos, y al mismo archivo se puede acceder simultáneamente desde varios nodos.

GPFS proporciona soporte al cifrado de archivos lo que permite tanto un almacenamiento seguro como una supresión segura de los datos. GPFS gestiona el cifrado mediante la utilización de políticas de cifrado y claves de cifrado.

Consulte la documentación de GPFS para obtener más información http://www.ibm.com/support/knowledgecenter/SSFKCN/gpfs_welcome.html.

Administración de certificados y claves

La administración de certificados y claves incluye el añadir, modificar o suprimir sus nombres de nodo asociados. También se pueden añadir claves y un nombre que asocia con las claves.

Acerca de esta tarea

Your role must have a permission to the view action and a permission to the appropriate device group. Utilice la página de gestión para GPFS para añadir, modificar o suprimir un certificado o una clave.

Antes de empezar, examine las columnas de la página, que proporciona botones para añadir, modificar o suprimir un elemento de tabla.

La tabla está organizada en estas áreas de información:

- En las columnas de la izquierda, la información sobre los certificados indican el UUID del certificado, el nombre de certificado y el recuento de puntos finales. El recuento de puntos finales es el número de puntos finales que están utilizando este certificado.
- En las columnas de la derecha, la información sobre las claves indica el UUID de clave y el nombre de clave al que acceden los certificados en la izquierda.

Procedimiento

1. Inicie una sesión en la interfaz gráfica de usuario.
   a. En la sección Gestión de claves y dispositivos en la página Bienvenida, seleccione **GPFS**.
   b. Pulse **Ir a** > **Gestionar claves y dispositivos**.
   c. O bien, pulse con el botón del ratón derecho en **GPFS** y seleccione **Gestionar claves y dispositivos**.
2. Puede añadir, modificar o suprimir una clave o certificado.

   Puede realizar estas tareas administrativas:

   - Renovar la lista.

     Click the refresh icon  to refresh items in the table.
   - Añadir

     Pulse **Añadir**.

     – Certificado

       En el diálogo Añadir certificado, escriba un nombre, el nombre de archivo y la ubicación del certificado. A continuación, pulse **Añadir**.

– Clave

En el diálogo Añadir clave, especifique la información de acuerdo con sus requisitos como, por ejemplo, el número de claves a crear, hasta un máximo de 100 claves. A continuación, pulse **Añadir**.

El indicador de éxito varía, mostrando la adición de un certificado o clave.

- Modificar

  Para modificar el grupo de dispositivos al que pertenece un certificado o una clave, seleccione el certificado o la clave y, a continuación, pulse **Modificar**. O bien, pulse con el botón derecho del ratón en el certificado o la clave. A continuación, pulse **Modificar**.

  – Certificado

  Ver información de sólo lectura en la página Modificar el certificado. Your role must have a permission to the modify action and a permission to the appropriate device group.

  – Clave

  Ver información de sólo lectura en la página Modificar clave. Your role must have a permission to the delete action and a permission to the appropriate device group.

  El indicador de éxito varía, y muestra un cambio en una columna para el certificado o la clave.

- Suprimir

  Para suprimir un certificado o clave, seleccione dicho certificado o clave y, a continuación, pulse **Suprimir**. O bien, pulse con el botón derecho del ratón sobre el certificado seleccionado o la clave seleccionada y, a continuación, pulse **Suprimir**.

  Los metadatos para el certificado que suprime se eliminan de la base de datos de IBM Security Key Lifecycle Manager. Los datos de las claves también se eliminan. Para confirmar la supresión, pulse **Aceptar**. Your role must have a permission to the delete action and a permission to the appropriate device group.

  Si todo ha ido bien, verá que el certificado se ha suprimido de la tabla.

Adición de un certificado

Puede añadir más certificados para su uso con IBM Security Key Lifecycle Manager.

Acerca de esta tarea

Puede utilizar el diálogo Añadir certificado para añadir un certificado. Your role must have a permission to the create action and a permission to the appropriate device group.

Procedimiento

1. Inicie una sesión en la interfaz gráfica de usuario.
2. En la sección Gestión de claves y dispositivos en la página Bienvenida, seleccione **GPFS**.
3. Pulse **Ir a** > **Gestionar claves y dispositivos**.
4. O bien, pulse con el botón del ratón derecho en **GPFS** y seleccione **Gestionar claves y dispositivos**.
5. En la página de gestión para `GPFS`, pulse **Añadir**.
6. Pulse **Certificado**.

7. En el diálogo Añadir certificado, especifique la información de acuerdo con los requisitos.
8. Pulse **Añadir**.

   El certificado se añade a la tabla.

Modificación de un certificado

Puede modificar información sobre un dispositivo en la base de datos de IBM Security Key Lifecycle Manager.

Acerca de esta tarea

Puede utilizar el diálogo Modificar certificado para actualizar un certificado. Your role must have a permission to the modify action and a permission to the appropriate device group.

Procedimiento

1. Inicie una sesión en la interfaz gráfica de usuario.
2. En la sección Gestión de claves y dispositivos en la página Bienvenida, seleccione **GPFS**.
3. Pulse **Ir a** > **Gestionar claves y dispositivos**.
4. O bien, pulse con el botón del ratón derecho en **GPFS** y seleccione **Gestionar claves y dispositivos**.
5. En la página de gestión de `GPFS`, seleccione un certificado.
6. Pulse **Modificar**.
7. O bien, pulse con el botón derecho del ratón en un certificado y seleccione **Modificar**, o efectúe una doble pulsación en una entrada de certificado.
8. En el diálogo Modificar certificado, escriba la información que cambia.
9. Pulse **Modificar**.

   La información de la clave se modifica en la tabla.

Qué hacer a continuación

A continuación, puede comprobar que se han realizado los cambios.

Supresión de un certificado

Puede suprimir un certificado seleccionado, que se puede encontrar en cualquier estado como, por ejemplo, activo.

Acerca de esta tarea

Utilice el elemento de menú `Suprimir` para suprimir un certificado. Your role must have a permission to the delete action and a permission to the appropriate device group.

Procedimiento

1. Inicie una sesión en la interfaz gráfica de usuario.
2. En la sección Gestión de claves y dispositivos en la página Bienvenida, seleccione **GPFS**.
3. Pulse **Ir a** > **Gestionar claves y dispositivos**.
4. O bien, pulse con el botón del ratón derecho en **GPFS** y seleccione **Gestionar claves y dispositivos**.
5. En la página de gestión de `GPFS`, seleccione un certificado.

6. Pulse **Suprimir**.
7. O bien, pulse con el botón derecho del ratón en un certificado y seleccione **Suprimir**.
8. En el diálogo Confirmar, lea el mensaje de confirmación para comprobar que ha seleccionado el certificado correcto antes de suprimirlo. A continuación, pulse en **Aceptar**.

   Se elimina el certificado de la tabla.

Adición de claves

Puede añadir claves para utilizarlas con GPFS.

Acerca de esta tarea

Utilice el diálogo Añadir clave para crear una o varias claves en el grupo existente. Your role must have a permission to the create action and a permission to the appropriate device group.

Antes de empezar, determine la política del sitio para la denominación de prefijos de claves.

Procedimiento

1. Inicie una sesión en la interfaz gráfica de usuario.
2. En la sección Gestión de claves y dispositivos en la página Bienvenida, seleccione **GPFS**.
3. Pulse **Ir a** > **Gestionar claves y dispositivos**.
4. O bien, pulse con el botón del ratón derecho en **GPFS** y seleccione **Gestionar claves y dispositivos**.
5. En la página de gestión para GPFS, pulse **Añadir**.
6. Pulse **Clave**.
7. En el diálogo Añadir clave, especifique valores para los parámetros.
8. Pulse **Añadir**. Las claves que se añaden son visibles en la tabla de claves. Realice una copia de seguridad antes de que las claves se sirvan a los dispositivos.

Modificación de una clave

Puede modificar información sobre una clave en la base de datos de IBM Security Key Lifecycle Manager.

Acerca de esta tarea

Utilice el diálogo Modificar clave para modificar la información sobre una clave. Your role must have a permission to the modify action and a permission to the appropriate device group.

Procedimiento

1. Inicie una sesión en la interfaz gráfica de usuario.
2. En la sección Gestión de claves y dispositivos en la página Bienvenida, seleccione **GPFS**.
3. Pulse **Ir a** > **Gestionar claves y dispositivos**.
4. O bien, pulse con el botón del ratón derecho en **GPFS** y seleccione **Gestionar claves y dispositivos**.
5. En la página de gestión de GPFS, seleccione una clave.

6. Pulse **Modificar**.
7. O bien, pulse con el botón derecho del ratón en una clave y seleccione **Modificar**, o efectúe una doble pulsación en una entrada de clave.
8. En el diálogo Modificar clave, escriba la información que cambia. A continuación, pulse **Modificar**. La información de la clave se cambia en la tabla.

Supresión de una clave

Es posible que tenga que suprimir una entrada de clave de la base de datos de IBM Security Key Lifecycle Manager.

Acerca de esta tarea

Utilice el elemento de menú `Suprimir` para suprimir una clave. Your role must have a permission to the delete action and a permission to the appropriate device group.

Procedimiento

1. Inicie una sesión en la interfaz gráfica de usuario.
2. En la sección Gestión de claves y dispositivos en la página Bienvenida, seleccione **GPFS**.
3. Pulse **Ir a** > **Gestionar claves y dispositivos**.
4. O bien, pulse con el botón del ratón derecho en **GPFS** y seleccione **Gestionar claves y dispositivos**.
5. En la página de gestión de `GPFS`, seleccione una clave.
6. Pulse **Suprimir**.
7. Otra posibilidad es pulsar con el botón de la derecha sobre una clave y seleccionar **Suprimir**.
8. En el diálogo Confirmar, lea el mensaje de confirmación para comprobar que ha seleccionado la clave correcta antes de suprimirla. A continuación, pulse en **Aceptar**. La clave se elimina de la tabla.

Gestión de PEER_TO_PEER

El grupo de dispositivos PEER_TO_PEER sirve a los dispositivos que operan en el protocolo KMIP (Key Management Interoperability Protocol). Este grupo de dispositivos permite que un máximo de dos dispositivos compartan una o más claves simétricas.

Puede utilizar el grupo de dispositivos PEER_TO_PEER para gestionar las claves y los certificados de dispositivos en IBM Security Key Lifecycle Manager.

Administración de certificados y claves

La administración de certificados y claves incluye el añadir, modificar o suprimir sus nombres de nodo asociados. También se pueden añadir claves y un nombre que asocia con las claves.

Acerca de esta tarea

Your role must have a permission to the view action and a permission to the appropriate device group. Utilice la página de gestión para PEER_TO_PEER para añadir, modificar o suprimir un certificado o una clave.

Antes de empezar, examine las columnas de la página, que proporciona botones para añadir, modificar o suprimir un elemento de tabla.

La tabla está organizada en estas áreas de información:

- En las columnas de la izquierda, se muestra información sobre el dispositivo WWNN, el nombre de certificado del dispositivo y el tipo de dispositivo.
- En las columnas de la derecha, se muestra la información sobre las claves que indica el UUID de clave y el nombre de clave al que acceden los certificados en la izquierda.

Procedimiento

1. Inicie una sesión en la interfaz gráfica de usuario.
   a. En la sección Gestión de claves y dispositivos en la página Bienvenida, seleccione **PEER_TO_PEER**.
   b. Pulse **Ir a** > **Gestionar claves y dispositivos**.
   c. O bien, pulse con el botón derecho del ratón en **PEER_TO_PEER** y seleccione **Gestionar claves y dispositivos**.
2. Puede añadir, modificar o suprimir una clave o certificado de dispositivo.

Adición de un dispositivo

Puede añadir un dispositivo al grupo de dispositivos PEER_TO_PEER para utilizar con IBM Security Key Lifecycle Manager.

Acerca de esta tarea

Puede utilizar el cuadro de diálogo Añadir dispositivo para añadir un dispositivo. Your role must have a permission to the create action and a permission to the appropriate device group.

Procedimiento

1. Inicie una sesión en la interfaz gráfica de usuario.
2. En la sección clave y dispositivo sección Gestión de claves y dispositivos en la página de bienvenida, seleccione **PEER_TO_PEER**.
3. Pulse **Ir a** > **Gestionar claves y dispositivos**.
4. O bien, pulse con el botón derecho del ratón en **PEER_TO_PEER** y seleccione **Gestionar claves y dispositivos**.
5. En la página de gestión para `PEER_TO_PEER`, pulse **Añadir**.
6. Pulse **Dispositivo**.
7. En el cuadro de diálogo Añadir dispositivo, especifique el nombre y la ubicación del certificado del dispositivo, y el tipo de dispositivo. Puede añadir solo un dispositivo de cada tipo, y un máximo de dos dispositivos.
8. Pulse **Añadir**.

   El dispositivo se añade a la tabla PEER_TO_PEER.

Modificación de un dispositivo

Puede modificar un certificado de dispositivo en la base de datos de IBM Security Key Lifecycle Manager.

Acerca de esta tarea

Utilice el cuadro de diálogo Modificar certificado de dispositivo para actualizar un dispositivo.Your role must have a permission to the modify action and a

permission to the appropriate device group.

Procedimiento

1. Inicie una sesión en la interfaz gráfica de usuario.
2. En la sección Gestión de claves y dispositivos en la página Bienvenida, seleccione **PEER_TO_PEER**.
3. Pulse **Ir a** > **Gestionar claves y dispositivos**.
4. O bien, pulse con el botón derecho del ratón en **PEER_TO_PEER** y seleccione **Gestionar claves y dispositivos**.
5. En la página de gestión de PEER_TO_PEER, seleccione un dispositivo.
6. Pulse **Modificar**.
7. O bien, pulse con el botón derecho del ratón en un dispositivo y seleccione **Modificar**, o efectúe una doble pulsación en una entrada de dispositivo.
8. En el cuadro de diálogo Modificar certificado de dispositivo, seleccione un certificado que tenga el mismo WWNN que el certificado de dispositivo anterior.
9. Pulse **Modificar**.

   La información del dispositivo se modifica en la tabla.

Qué hacer a continuación

A continuación, puede comprobar que se han realizado los cambios.

Supresión de un dispositivo

Puede suprimir un dispositivo seleccionado y su correspondiente certificado de comunicación, que se puede encontrar en cualquier estado como, por ejemplo, activo. Tras la supresión, el dispositivo no puede comunicarse con los objetos del grupo PEER_TO_PEER.

Acerca de esta tarea

Utilice el elemento de menú Suprimir para suprimir un dispositivo. Your role must have a permission to the delete action and a permission to the appropriate device group.

Procedimiento

1. Inicie una sesión en la interfaz gráfica de usuario.
2. En la sección Gestión de claves y dispositivos en la página Bienvenida, seleccione **PEER_TO_PEER**.
3. Pulse **Ir a** > **Gestionar claves y dispositivos**.
4. O bien, pulse con el botón derecho del ratón en **PEER_TO_PEER** y seleccione **Gestionar claves y dispositivos**.
5. En la página de gestión de PEER_TO_PEER, seleccione un dispositivo.
6. Pulse **Suprimir**.
7. O bien, pulse con el botón derecho del ratón en un dispositivo y seleccione **Suprimir**.
8. En el diálogo Confirmar, lea el mensaje de confirmación. A continuación, pulse en **Aceptar**.

   El dispositivo se elimina de la tabla.

Adición de claves

Puede añadir claves para utilizarlas con PEER_TO_PEER.

Acerca de esta tarea

Utilice el cuadro diálogo Añadir clave para crear una o varias claves en el grupo existente. Your role must have a permission to the create action and a permission to the appropriate device group.

Antes de empezar, determine la política del sitio para la denominación de prefijos de claves.

Procedimiento

1. Inicie una sesión en la interfaz gráfica de usuario.
2. En la sección Gestión de claves y dispositivos en la página Bienvenida, seleccione **PEER_TO_PEER**.
3. Pulse **Ir a** > **Gestionar claves y dispositivos**.
4. O bien, pulse con el botón derecho del ratón en **PEER_TO_PEER** y seleccione **Gestionar claves y dispositivos**.
5. En la página de gestión para PEER_TO_PEER, pulse **Añadir**.
6. Pulse **Clave**.
7. En el diálogo Añadir clave, especifique valores para los parámetros.
8. Pulse **Añadir**. Las claves que se añaden son visibles en la tabla de claves. Realice una copia de seguridad antes de que las claves se sirvan a los dispositivos.

Modificación de una clave

Puede modificar información sobre una clave en la base de datos de IBM Security Key Lifecycle Manager.

Acerca de esta tarea

Utilice el cuadro de diálogo Modificar clave para modificar la información sobre una clave. Your role must have a permission to the modify action and a permission to the appropriate device group.

Procedimiento

1. Inicie una sesión en la interfaz gráfica de usuario.
2. En la sección Gestión de claves y dispositivos en la página Bienvenida, seleccione **PEER_TO_PEER**.
3. Pulse **Ir a** > **Gestionar claves y dispositivos**.
4. O bien, pulse con el botón derecho del ratón en **PEER_TO_PEER** y seleccione **Gestionar claves y dispositivos**.
5. En la página de gestión de PEER_TO_PEER, seleccione una clave.
6. Pulse **Modificar**.
7. O bien, pulse con el botón derecho del ratón en una clave y seleccione **Modificar**, o efectúe una doble pulsación en una entrada de clave.
8. En el cuadro de diálogo Modificar clave, escriba la información que cambia. A continuación, pulse **Modificar**. La información de la clave se cambia en la tabla.

Supresión de una clave

Es posible que tenga que suprimir una entrada de clave de la base de datos de IBM Security Key Lifecycle Manager.

Acerca de esta tarea

Utilice el elemento de menú `Suprimir` para suprimir una clave. Your role must have a permission to the delete action and a permission to the appropriate device group.

Procedimiento

1. Inicie una sesión en la interfaz gráfica de usuario.
2. En la sección clave y dispositivo sección Gestión de claves y dispositivos en la página de bienvenida, seleccione **PEER_TO_PEER**.
3. Pulse **Ir a** > **Gestionar claves y dispositivos**.
4. O bien, pulse con el botón derecho del ratón en **PEER_TO_PEER** y seleccione **Gestionar claves y dispositivos**.
5. En la página de gestión de `PEER_TO_PEER`, seleccione una clave.
6. Pulse **Suprimir**.
7. Otra posibilidad es pulsar con el botón de la derecha sobre una clave y seleccionar **Suprimir**.
8. En el diálogo Confirmar, lea el mensaje de confirmación para comprobar que ha seleccionado la clave correcta antes de suprimirla. A continuación, pulse en **Aceptar**. La clave se elimina de la tabla.

Exportación e importación de grupos de dispositivos

IBM Security Key Lifecycle Manager ofrece un conjunto de operaciones para exportar los grupos de dispositivos de una instancia de IBM Security Key Lifecycle Manager e importarlos en otra instancia que tenga la misma versión que la instancia de IBM Security Key Lifecycle Manager de origen entre sistema operativos. Los datos de los grupos de dispositivos se cifran y protegen mediante una contraseña.

Para obtener más información sobre la importación y exportación de grupos de dispositivos, consulte Visión general de la importación y exportación de grupos de dispositivos

Exportación de un grupo de dispositivos

Tiene la posibilidad de exportar los datos de un grupo de dispositivos seleccionado a un archivo de archivado cifrado. A continuación, puede importar los datos del grupo de dispositivos en otra instancia de IBM Security Key Lifecycle Manager en el mismo sistema operativo o en uno diferente.

Acerca de esta tarea

Utilice el diálogo Exportar grupo de dispositivos para exportar un grupo de dispositivos. De forma alternativa, puede utilizar el **`Servicio REST Exportación de grupo de dispositivos`**.

Su rol debe tener permiso para exportar grupos de dispositivos.

Nota: Durante la migración de datos de versiones anteriores de IBM Security Key Lifecycle Manager, algunos de los certificados podrían no estar asociados con el grupo de dispositivos correcto. Como resultado, es posible que algunos certificados se muestren equivocadamente (en la interfaz de usuario, los servicios REST o la interfaz de línea de mandatos) para un grupo de dispositivos como, como por ejemplo 3592 o DS8000, a pesar de que los certificados no pertenecen al grupo de dispositivos. Cuando exporte estos grupos de dispositivos, únicamente se exportarán los certificados del grupo de dispositivos. Los certificados que se muestran equivocadamente no se exportarán.

Procedimiento

1. Vaya al directorio o la página apropiada.

   Interfaz gráfica de usuario

   a. Inicie una sesión en la interfaz gráfica de usuario.
   b. En la sección Gestión de claves y dispositivos en la página de Bienvenida, seleccione un grupo de dispositivos.
   c. Pulse **Ir a** > **Exportar**.
   d. De forma alternativa, pulse con el botón derecho del ratón sobre el grupo de dispositivos seleccionado y seleccione **Exportar**.
   e. Como alternativa, en la página Bienvenida pulse **Administración** > **Exportar e Importar** > **Exportar**.

   Interfaz REST

   Abra un cliente REST.

2. Exporte los datos del grupo de dispositivos seleccionado al directorio que ha especificado.

   Interfaz gráfica de usuario

   a. En el diálogo Exportar grupo de dispositivos, el campo **Grupo de dispositivos** especifica el grupo de dispositivos seleccionado.
   b. Para cambiar el grupo de dispositivos, pulse **Seleccionar**.
   c. El campo **Ubicación del repositorio de exportación** muestra la vía de acceso del directorio *<SKLM_DATA>* predeterminada, donde se guardará el archivo exportado, por ejemplo, `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data`. Para ver la definición de *<SKLM_DATA>*, consulte Definiciones para *HOME* y otras variables de directorio. Pulse **Examinar** para especificar una ubicación del repositorio de exportación bajo el directorio *<SKLM_DATA>*.

      La vía de acceso del directorio en el campo **Ubicación de repositorio de exportación** cambia en base al valor que se establezca para la propiedad **`browse.root.dir`** en el archivo `SKLMConfig.properties`.
   d. En el campo **Contraseña**, especifique un valor para la contraseña de cifrado. Asegúrese de conservar la contraseña de cifrado para un uso futuro.
   e. En el campo **Vuelva a escribir la contraseña**, vuelva a escribir la contraseña que especificó en el campo **Contraseña**.
   f. En el campo **Descripción**, especifique la información adicional que indique el propósito del archivo de exportación del grupo de dispositivos.
   g. Pulse **Exportar**.

Interfaz REST

a. Obtenga un identificador de autenticación de usuario exclusivo para acceder a los servicios REST de IBM Security Key Lifecycle Manager. Para obtener más información sobre el proceso de autenticación, consulte Proceso de autenticación de los servicios REST.

b. Para ejecutar el **Servicio REST Exportar grupo de dispositivos**, envíe la solicitud HTTP POST. Pase el identificador de autenticación de usuario que ha obtenido en el `Paso a` junto con el mensaje de solicitud, como se muestra en el ejemplo siguiente.

```
POST https://localhost:<puerto>/SKLM/rest/v1/ckms/deviceGroupsExport
Content-Type: application/json
Accept: application/json
Authorization: SKLMAuth userAuthId=139aeh34567m
{"name": "3592", "exportDirectory": "/opt/IBM/WebSphere/AppServer/products/sklm/dat
"password":"mypassword"}
```

3. Cuando la exportación termina, se visualiza un recuadro de mensaje para indicar que se ha completado la operación de exportación.

Qué hacer a continuación

Asegúrese de conservar la contraseña para utilizarla cuando, más tarde, importe y descifre el archivo de exportación del grupo de dispositivos en otra instancia de IBM Security Key Lifecycle Manager. Revise el directorio que contiene el archivo de archivado de exportación para garantizar que existe el archivo de exportación. También puede verificar si el archivo de archivado aparece listado en la tabla en la página **IBM Security Key Lifecycle Manager** > **Administración** > **Exportar e Importar** > **Exportar/Importar**.

Importación de un grupo de dispositivos

Importe los datos de un grupo de dispositivos que se exportaron desde otra instancia de IBM Security Key Lifecycle Manager si desea mover datos entre instancias de IBM Security Key Lifecycle Manager.

Antes de empezar

Debe tener el archivo de exportación y asegurarse de que tiene la contraseña que se utilizó al crear el archivo de exportación. Guarde los archivos de exportación en el directorio <*SKLM_DATA*> predeterminado, por ejemplo, `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data`. Para ver la definición de <*SKLM_DATA*>, consulte Definiciones para *HOME* y otras variables de directorio.

La vía de acceso del directorio <*SKLM_DATA*> cambia en base al valor que se establece en la propiedad **browse.root.dir** en el archivo `SKLMConfig.properties`.

La versión de la instancia de IBM Security Key Lifecycle Manager en la que se importan los datos de exportación del grupo de dispositivos debe coincidir con la de la instancia de IBM Security Key Lifecycle Manager desde la que se han exportado los datos del grupo de dispositivos.

Acerca de esta tarea

A veces, los datos del grupo de dispositivos que se importa podrían entrar en conflicto con los datos existentes en la base de datos. Por ejemplo, una clave en el grupo de dispositivos importados podría ser una clave con el mismo nombre de

alias de un grupo de dispositivos en la instancia actual de IBM Security Key Lifecycle Manager en la que se están importando los datos. Cuando se producen conflictos, se deben resolver para que el proceso de importación pueda continuar.

Utilice la página Exportar e importar. De forma alternativa, puede utilizar el `Servicio REST Importación de grupo de dispositivos` para importar grupos de dispositivos.

Su rol debe tener permiso para importar grupos de dispositivos. Para obtener más información sobre la exportación de grupos de dispositivos y las operaciones de importación, consulte Visión general de la importación y exportación de grupos de dispositivos.

Procedimiento

1. Vaya al directorio o la página apropiada.

   Interfaz gráfica de usuario

   a. Inicie una sesión en la interfaz gráfica de usuario.
   b. En la página de Bienvenida, pulse **Administración** > **Exportar e importar**.

   Interfaz REST

   Abra un cliente REST.

2. Importe un archivo de exportación seleccionado. Únicamente es posible ejecutar al mismo tiempo una operación de importación o exportación. Si desea importar un archivo a una instancia de IBM Security Key Lifecycle Manager en un sistema operativo diferente, copie el archivo de exportación en dicho sistema utilizando un soporte como, por ejemplo, un disco o una transmisión electrónica.

   Interfaz gráfica de usuario

   a. Pulse **Examinar** para especificar la ubicación del archivo de exportación en el directorio <SKLM_DATA>, por ejemplo, `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data`.
   b. Pulse **Visualizar exportaciones** para visualizar los archivos de exportación.
   c. Seleccione un archivo de exportación en la tabla.
   d. Pulse en **Importar**.
   e. De forma alternativa, efectúe una doble pulsación o pulse con el botón derecho del ratón sobre el archivo de exportación y seleccione **Importar**.
   f. En el diálogo Importar desde archivador de exportación, especifique la contraseña de cifrado que se utilizó al crear el archivo de exportación.
   g. Pulse **Importar** para iniciar la operación de importación.

   Interfaz REST

   a. Obtenga un identificador de autenticación de usuario exclusivo para acceder a los servicios REST de IBM Security Key Lifecycle Manager. Para obtener más información sobre el proceso de autenticación, consulte Proceso de autenticación de los servicios REST.
   b. Para ejecutar el **`Servicio REST Importación de grupo de dispositivos`**, envíe la solicitud HTTP POST. Pase el identificador

de autenticación de usuario que ha obtenido en el Paso a junto con el mensaje de solicitud, como se muestra en el ejemplo siguiente.

```
POST https://localhost:<puerto>/SKLM/rest/v1/ckms/deviceGroupsImport
Content-Type: application/json
Accept: application/json
Authorization: SKLMAuth userAuthId=139aeh34567m
{"importFilePath": "C:\\Program Files\\IBM\\WebSphere\\AppServer\\products\\sklm\\c
"password": "passw0rd123"}
```

3. Si se presenta algún conflicto durante el proceso de importación, aparecerá el diálogo Conflictos durante la importación. Consulte el tema "Visualización de conflictos de importación" en la página 120 para obtener más información.
4. Si no se han producido conflictos de datos, se abre el recuadro de progreso. Cuando el proceso de importación termina, se visualiza un recuadro de mensaje que indica que se ha completado la operación de importación.
5. Pulse **Cerrar**.
6. Reinicie el servidor. Para obtener instrucciones sobre cómo detener e iniciar el servidor, consulte el apartado "Reinicio de IBM Security Key Lifecycle Manager server" en la página 205.

Supresión de un archivo de exportación de un grupo de dispositivo

Podría tener la necesidad de suprimir un archivo de exportación al dejar de existir la necesidad empresarial que lo originó. Utilice la interfaz gráfica de usuario o la interfaz REST para suprimir un archivo de exportación de un grupo de dispositivos.

Acerca de esta tarea

Puede utilizar la página Exportar/Importar o **Servicio REST Suprimir grupo de dispositivos** para suprimir un archivo de exportación.

Procedimiento

1. Vaya al directorio o la página apropiada.

   Interfaz gráfica de usuario

   a. Inicie una sesión en la interfaz gráfica de usuario.
   b. En la página de Bienvenida, pulse **Administración** > **Exportar e importar**.

   Interfaz REST

   Abra un cliente REST.

2. Suprima un archivo de exportación seleccionado.

   Interfaz gráfica de usuario

   a. Pulse **Examinar** para especificar la ubicación del archivo de exportación bajo el directorio <SKLM_DATA>. Para ver la definición de <SKLM_DATA>, consulte Definiciones para *HOME* y otras variables de directorio.
   b. Pulse **Visualizar exportaciones** para visualizar los archivos de exportación.
   c. Seleccione un archivo de exportación en la tabla.
   d. Pulse **Suprimir** para confirmar que desea suprimir el archivo.

e. Como alternativa, pulse con el botón derecho en el archivo de exportación y seleccione **Suprimir** para confirmar que desea suprimir el archivo.

Interfaz REST

a. Obtenga un identificador de autenticación de usuario exclusivo para acceder a los servicios REST de IBM Security Key Lifecycle Manager. Para obtener más información sobre el proceso de autenticación, consulte Proceso de autenticación de los servicios REST.

b. Para ejecutar el **Servicio REST Suprimir grupo de dispositivos**, envíe la solicitud HTTP DELETE. Pase el identificador de autenticación de usuario que ha obtenido en el `Paso a` junto con el mensaje de solicitud, como se muestra en el ejemplo siguiente.

```
DELETE https://localhost:<port>/SKLM/rest/v1/deviceGroups/newDevGrp
Content-Type: application/json
Accept: application/json
Authorization: SKLMAuth userAuthId=139aeh34567m
```

Qué hacer a continuación

Examine el directorio donde se almacenan los archivos de exportación para determinar si se ha suprimido el archivo especificado.

Visualización de conflictos de importación

Cuando se importan datos de un grupo de dispositivos desde un archivo de importación, su contenido se analiza para ver si hay conflictos con los datos almacenados en la base de datos de IBM Security Key Lifecycle Manager. Antes de poder importar los datos, es necesario resolver los conflictos. Puede ver una lista de conflictos para analizar y resolver los problemas.

Acerca de esta tarea

Los detalles de los conflictos de importación se abren en la ventana Conflictos durante la importación. Puede exportar los datos de los conflictos en un formato de valores separados por comas (CSV).

Procedimiento

1. Vaya al directorio o la página apropiada.

   Interfaz gráfica de usuario

   a. Inicie una sesión en la interfaz gráfica de usuario.

   b. En la página de Bienvenida, pulse **Administración** > **Exportar e importar**.

   Interfaz REST

   Abra un cliente REST.

2. Importe un archivo de exportación seleccionado. Únicamente es posible ejecutar al mismo tiempo una operación de importación o exportación. Si desea importar un archivo a una instancia de IBM Security Key Lifecycle Manager en un sistema operativo diferente, copie el archivo de exportación en dicho sistema utilizando un soporte como, por ejemplo, un disco o una transmisión electrónica.

   Interfaz gráfica de usuario

a. Pulse **Examinar** para especificar la ubicación del archivo de exportación en el directorio <SKLM_DATA>, por ejemplo, `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data`. Para ver la definición de `<SKLM_DATA>`, consulte Definiciones para *HOME* y otras variables de directorio.

b. Pulse **Visualizar exportaciones** para visualizar los archivos de exportación.

c. Seleccione un archivo de exportación en la tabla.

d. Pulse en **Importar**.

e. De forma alternativa, efectúe una doble pulsación o pulse con el botón derecho del ratón sobre el archivo de exportación y seleccione **Importar**.

f. En el diálogo Importar desde archivador de exportación, especifique la contraseña de cifrado que se utilizó al crear el archivo de exportación.

g. Pulse **Importar** para iniciar la operación de importación.

Interfaz REST

a. Obtenga un identificador de autenticación de usuario exclusivo para acceder a los servicios REST de IBM Security Key Lifecycle Manager. Para obtener más información sobre el proceso de autenticación, consulte Proceso de autenticación de los servicios REST.

b. Para ejecutar el **Servicio REST Importación de grupo de dispositivos**, envíe la solicitud HTTP POST. Pase el identificador de autenticación de usuario que ha obtenido en el `Paso a` junto con el mensaje de solicitud, como se muestra en el ejemplo siguiente.

```
POST https://localhost:<puerto>/SKLM/rest/v1/ckms/deviceGroupsImport
Content-Type: application/json
Accept: application/json
Authorization: SKLMAuth userAuthId=139aeh34567m
{"importFilePath": "C:\\Program Files\\IBM\\WebSphere\\AppServer\\products\\sklm\\c
"password": "passw0rd123"}
```

3. Si se detectan conflictos durante la operación de importación, podrá visualizar una lista de conflictos en la ventana Conflictos durante la importación.

4. También puede utilizar **Servicio REST Conflictos de importación de grupo de dispositivos** para ver una lista de conflictos de datos, si los hay, cuando los datos del grupo de dispositivos se importan de un archivo de exportación en una instancia de IBM Security Key Lifecycle Manager. Para ejecutar el **Servicio REST Conflictos de importación de grupo de dispositivos**, envíe la solicitud HTTP POST.

```
POST https://localhost:<port>/SKLM/rest/v1/ckms/deviceGroupsImport/importConflicts
Content-Type: application/json
Accept: application/json
Authorization: SKLMAuth userAuthId=139aeh34567m
{"importFilePath": "C:\\Program Files\\IBM\\WebSphere\\AppServer\\products\\sklm\\data\\sklm_v
"password": "passw0rd123"}
```

5. Para exportar los datos de los conflictos de importación a un archivo con formato de valores separados por comas (CSV) para un análisis posterior, pulse **Exportar informe de conflictos**.

Qué hacer a continuación

Debe resolver los conflictos antes de poder importar los datos. Puede utilizar los siguientes servicios REST para resolver conflictos de importación:

- **Servicio REST Cambiar nombre**
- **Servicio REST Cambiar alias de certificado**
- **Servicio REST Historial de cambios**
- **Servicio REST Renovar alias de clave**

Visualización del historial de exportación e importación de grupos de dispositivos

Utilice la página Historial para ver detalles de todas las operaciones de exportación e importación de grupos de dispositivos que se ejecuten en la instancia actual de IBM Security Key Lifecycle Manager.

Procedimiento

1. Inicie una sesión en la interfaz gráfica de usuario.
2. En la página de Bienvenida, pulse **Administración** > **Exportar e importar**.
3. En la página Exportar e importar, pulse **Historial**.

   Se muestra una lista de las operaciones de exportación e importación de grupos de dispositivos en la instancia actual de IBM Security Key Lifecycle Manager.
4. Seleccione una fila y realice una doble pulsación. Se muestran detalles resumidos de la operación de exportación o importación.

Visualización de información de resumen de exportación e importación de grupos de dispositivos

Utilice la página Resumen de exportación/importación para ver los detalles de un archivo de exportación seleccionado para comprender los datos del grupo de dispositivos y trabajar con los mismos. Puede ver los detalles de un archivo de exportación creado en la instancia actual de IBM Security Key Lifecycle Manager. También puede ver detalles de un archivo de exportación que desee importar en la instancia actual de IBM Security Key Lifecycle Manager.

Procedimiento

1. Inicie una sesión en la interfaz gráfica de usuario.
2. En la página de Bienvenida, pulse **Administración** > **Exportar e importar**.
3. Seleccione un archivo de exportación de grupo de dispositivos que aparezca listado en la tabla.
4. Pulse **Resumen**.
5. De forma alternativa, pulse con el botón derecho en el archivo de exportación y seleccione **Resumen**.

   En la tabla siguiente se proporciona la información de resumen.

ID	ID del archivo de exportación del grupo de dispositivos seleccionado.
Nombre de archivador	Nombre del archivo de exportación del grupo de dispositivos.
Hora de inicio	Hora a la que se ha iniciado la operación de exportación o importación.
Hora de finalización	Hora a la que ha finalizado la operación de exportación o importación.
Grupo de dispositivos	Nombre del grupo de dispositivos del que se exportan los datos al archivo.

<datos grupo dispositivos>	Muestra el número de certificados, grupos clave y otros detalles del archivo de exportación del grupo de dispositivos.

6. Pulse **Cancelar** para cerrar la página de resumen.

Copia de seguridad y restauración

IBM Security Key Lifecycle Manager proporciona un conjunto de operaciones para restaurar y hacer una copia de seguridad de los datos y los archivos activos actuales.

IBM Security Key Lifecycle Manager crea archivos de copia de seguridad entre plataformas, de modo independiente a los sistemas operativos y la estructura de directorios del servidor. Puede restaurar los archivos de copia de seguridad en un sistema operativo diferente del sistema desde el que ha realizado la copia de seguridad. Por ejemplo, puede restaurar un archivo de copia de seguridad realizado en un sistema Linux y restaurarlo en un sistema Windows.

Puede utilizar el programa de utilidad de copia de seguridad entre plataformas para ejecutar la operación de copia de seguridad en versiones anteriores de IBM Security Key Lifecycle Manager e IBM Tivoli Key Lifecycle Manager para realizar copias de seguridad de los datos críticos. Puede restaurar estos archivos de copia de seguridad en la versión actual de IBM Security Key Lifecycle Manager entre sistemas operativos.

Nota: En IBM Security Key Lifecycle Manager, Versión 3.0 y posterior, el sistema operativo Solaris no está soportado. Si utiliza IBM Security Key Lifecycle Manager en sistemas Solaris, utilice el programa de utilidad de copia de seguridad entre plataformas, para realizar la copia de seguridad de datos. A continuación, ejecute la operación de restauración para restaurar los datos de un sistema IBM Security Key Lifecycle Manager versión 3.0 o posterior desplegado en cualquier sistema operativo soportado, tal como Windows, Linux o AIX.

Los archivos de copia de seguridad incluyen los datos siguientes:

- Datos de las tablas de base de datos de IBM Security Key Lifecycle Manager
- Almacén de confianza y almacén de claves con la clave maestra
- Los archivos de configuración de IBM Security Key Lifecycle Manager

Your role must have permissions to back up or to restore files.

`Failure to back up your critical data properly might result in unrecoverable loss of all access to your encrypted data. Do not encrypt your backup file, or store a backup file on an encrypting device.` Failure to back up data might also result in a later inconsistency of the key manager and potential data loss on the storage device.

Las operaciones de copia de seguridad y restauración de IBM Security Key Lifecycle Manager permiten utilizar la longitud de claves AES de 256 bits para el cifrado o descifrado de datos, que se ajusta al estándar PCI DSS (Payment Card Industry Data Security Standard) que aumenta la seguridad de datos.

Métodos de cifrado para realizar copias de seguridad de datos de IBM Security Key Lifecycle Manager

IBM Security Key Lifecycle Manager da soporte a los siguientes métodos de cifrado para las copias de seguridad:

Cifrado basado en contraseña
Durante el proceso de copia de seguridad, se especifica una contraseña para cifrar la clave de la copia de seguridad. Se debe especificar la misma contraseña de cifrado para descifrar y restaurar los archivos de copia de seguridad.

Cifrado basado en HSM
Puede configurar a IBM Security Key Lifecycle Manager para utilizar HSM (Hardware Security Module) para almacenar la clave de cifrado maestra. Durante el proceso de copia de seguridad, la clave maestra cifra la clave de la copia de seguridad. La clave maestra se almacena en HSM. Durante el proceso de restauración, la clave maestra en HSM descifra la clave de la copia de seguridad. A continuación, se utiliza la clave de la copia de seguridad para restaurar el contenido de la copia de seguridad.

Copia de seguridad y restauración de alto rendimiento

La copia de seguridad y la restauración de alto rendimiento proporcionan copia de seguridad y restauración de grandes cantidades de claves de cifrado. Puede configurar IBM Security Key Lifecycle Manager para las operaciones de copia de seguridad y de restauración de alto rendimiento estableciendo el parámetro siguiente en el archivo de configuración `SKLMConfig.properties`.

```
enableHighScaleBackup=true
```

Cuando IBM Security Key Lifecycle Manager esté configurado para la copia de seguridad y la restauración de alto rendimiento, se utilizará la tecnología de copia de seguridad nativa de IBM DB2 para ejecutar la operación de copia de seguridad y de restauración para obtener más eficiencia. Sin embargo, con esta configuración, puede restaurar la copia de seguridad sólo en un entorno operativo idéntico. El sistema operativo, los componentes de middleware y las estructuras de directorios deben ser idénticos en ambos sistemas.

No es posible realizar un archivo de copia de seguridad compatible entre plataformas si se ha configurado a IBM Security Key Lifecycle Manager para actividades de copia se seguridad y restauración de alto rendimiento. Para obtener información sobre cómo realizar copias de seguridad de grandes cantidades de datos, consulte “Copia de seguridad de una cantidad grande de datos” en la página 132.

Requisitos de tiempo de ejecución de copia de seguridad y restauración

La copia de seguridad y la restauración de datos de archivos de copia de seguridad para IBM Security Key Lifecycle Manager tiene varios requisitos de tiempo de ejecución.

Puede evitar los errores de tiempo de espera si aumenta el intervalo de tiempo permitido para las transacciones de copia de seguridad y restauración cuando hay un gran número de claves. Especifique un valor mayor para **`totalTranLifetimeTimeout`** en este archivo:

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

Asimismo, deben cumplirse las siguientes condiciones:

- Asegúrese de que la tarea se realice en un intervalo de tiempo que permita una parada en la actividad de servicio de claves.
- Para una tarea de copia de seguridad, el IBM Security Key Lifecycle Manager server debe estar ejecutándose en un estado operativo normal. La instancia de base de datos de IBM Security Key Lifecycle Manager debe estar disponible.
- Para una tarea de restauración, la instancia de la base de datos de IBM Security Key Lifecycle Manager debe ser accesible a través del origen de datos de IBM Security Key Lifecycle Manager.

  Antes de iniciar una tarea de restauración para las copias de seguridad cifradas con contraseña, asegúrese de que tiene la contraseña que se ha utilizado al crear el archivo de copia de seguridad.
- Utilice las siguientes directrices para restaurar copias de seguridad cifradas basadas en HSM:
  - Asegúrese de que está presente la misma partición HSM con todas sus entradas de clave intactas en el sistema en el que se restaura el archivo de copia de seguridad.
  - También debe estar intacta la clave maestra que se utilizó para el cifrado de clave de copia de seguridad para poder restaurar el archivo de copia de seguridad. Si se renueva la clave maestra, todas las copias de seguridad antiguas serán inaccesibles o no se podrán utilizar.
  - Debe conectarse al mismo HSM y clave maestra para las operaciones de copia de seguridad y restauración independientemente de si ha utilizado cifrado basado en HSM o cifrado basado en contraseña.
- Asegúrese de que los directorios, que están asociados con la propiedad **tklm.backup.dir** existen. Asimismo, compruebe que exista acceso de lectura y escritura en dichos directorios para las cuentas de administrador de IBM Security Key Lifecycle Manager y el sistema con las que se ejecutan el IBM Security Key Lifecycle Manager server y el Db2 server.

Copias de seguridad de datos con cifrado basado en contraseña

Es necesario especificar una contraseña de cifrado para realizar copias de seguridad de datos de IBM Security Key Lifecycle Manager. Utilice la misma contraseña para descifrar y restaurar archivos de copia de seguridad.

Acerca de esta tarea

Puede utilizar la página Copia de seguridad y restauración. O bien, puede utilizar el mandato **tklmBackupRun** o el **Servicio REST Ejecutar copia de seguridad** para realizar la copia de seguridad de datos esenciales. Your role must have a permission to back up files.

IBM Security Key Lifecycle Manager crea archivos de copia de seguridad, de modo independiente en los sistemas operativos y en la estructura de directorios del servidor. Puede restaurar los archivos de copia de seguridad en un sistema operativo diferente del sistema desde el que ha realizado la copia de seguridad.

Nota: Backup success messages are system wide. Two administrators might run backup tasks that overlap in time. During this interval, the administrator who starts a second task that fails might see a false success message from the first backup task.

Procedimiento

1. Vaya al directorio o la página apropiada.

   Interfaz gráfica de usuario

   a. Inicie una sesión en la interfaz gráfica de usuario.
   b. En la página de Bienvenida, pulse **Administración** > **Copia de seguridad y restauración**.

   Interfaz de línea de mandatos

   a. Vaya al directorio `WAS_HOME/bin`. Por ejemplo,

      Windows

      ```
      cd unidad:\Program Files\IBM\WebSphere\AppServer\bin
      ```

      Linux

      ```
      cd /opt/IBM/WebSphere/AppServer/bin
      ```

   b. Inicie la interfaz **`wsadmin`** utilizando un ID de usuario autorizado, por ejemplo, `SKLMAdmin`. Por ejemplo,

      Windows

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

      Linux

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

   Interfaz REST

   Abra un cliente REST.

2. Cree un archivo de copia de seguridad. Sólo puede ejecutar una tarea de copia de seguridad o restauración a la vez.

   Interfaz gráfica de usuario

   a. En la tabla **Copia de seguridad y restauración**, el campo **Ubicación de repositorio de copia de seguridad** muestra la vía de acceso del directorio <*SKLM_DATA*> predeterminada, donde se guardará el archivo de copia de seguridad, por ejemplo, `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data`. Para ver la definición de <*SKLM_DATA*>, consulte Definiciones para *HOME* y otras variables de directorio. Pulse **Examinar** para especificar una ubicación del repositorio de copia de seguridad bajo el directorio <*SKLM_DATA*>.

      La vía de acceso al directorio en el campo **Ubicación de repositorio de copia de seguridad** cambia en base al valor que se establece en la propiedad **`tklm.backup.dir`** en el archivo `SKLMConfig.properties`.

   b. Pulse **Crear copia de seguridad**.
   c. En la página Crear copia de seguridad, especifique la información necesaria como, por ejemplo, un valor para la contraseña de cifrado y una descripción de la copia de seguridad. Se muestra una ubicación de archivo de copia de seguridad de solo lectura en el campo **Ubicación de la copia de seguridad**. Asegúrese de conservar la contraseña de cifrado para su uso futuro si desea restaurar la copia de seguridad.
   d. Pulse **Crear copia de seguridad**.

Interfaz de línea de mandatos

Escriba **tklmBackupRun**, la ubicación de la copia de seguridad, la contraseña de cifrado y toda la información necesaria para crear un archivo de copia de seguridad. Por ejemplo:

```
print AdminTask.tklmBackupRun ('[-backupDirectory C:\\sklmbackup1 -password myBackupPw
```

Interfaz REST

a. Obtenga un identificador de autenticación de usuario exclusivo para acceder a los servicios REST de IBM Security Key Lifecycle Manager. Para obtener más información sobre el proceso de autenticación, consulte Proceso de autenticación de los servicios REST.

b. Para ejecutar el **Servicio REST Ejecutar copia de seguridad**, envíe la solicitud HTTP POST. Pase el identificador de autenticación de usuario que ha obtenido en el Paso a junto con el mensaje de solicitud, como se muestra en el ejemplo siguiente.

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

3. Un mensaje indica que se ha creado el archivo de copia de seguridad o que la operación de copia de seguridad ha sido satisfactoria.

   The time stamp on a backup file has a Greenwich Mean Time (GMT) offset represented in RFC 822 format. The file name contains a *+hhmm* or *-hhmm* element to specify a timezone ahead of or behind GMT. For example, a file name might be sklm_v3.0.1.0_20170123144220**-0800**_backup.jar, where -0800 indicates that the timezone is eight hours behind GMT.

Qué hacer a continuación

Conserve la contraseña de cifrado para su uso futuro si desea restaurar la copia de seguridad. Revise el directorio que contiene los archivos de copia de seguridad para garantizar que existe el archivo de copia de seguridad. No edite un archivo en el archivo JAR de copia de seguridad. El archivo que intente editar se convertirá en no legible.

Copias de seguridad de datos con cifrado basado en contraseña cuando HSM está configurado

Se debe establecer la propiedad **enablePBEInHSM=true** en el archivo SKLMConfig.properties para realizar una copia de seguridad de los datos con cifrado basado en contraseña cuando HSM (Hardware Security Module) está configurado.

Antes de empezar

Asegúrese de que se ha configurado IBM Security Key Lifecycle Manager para que utilice HSM para almacenar la clave maestra siguiendo los pasos del tema "Configuración de los parámetros de HSM" en la página 210.

Acerca de esta tarea

Cuando se configura HSM, durante el proceso de copia de seguridad, la clave maestra en HSM cifra la clave de la copia de seguridad. El cifrado basado en HSM

es el método predeterminado para realizar copias de seguridad cuando se ha configurado a HSM para almacenar la clave maestra. Para obtener información sobre el cifrado basado en HSM, consulte Cifrado basado en HSM de copias de seguridad. Your role must have a permission to back up files.

Nota: Backup success messages are system wide. Two administrators might run backup tasks that overlap in time. During this interval, the administrator who starts a second task that fails might see a false success message from the first backup task.

Procedimiento

1. Establezca la propiedad **enablePBEInHSM=true** en el archivo *<SKLM_HOME>*/config/SKLMConfig.properties.

   Interfaz de línea de mandatos

   a. Vaya al directorio WAS_HOME/bin. Por ejemplo,

      Windows

      ```
      cd unidad:\Program Files\IBM\WebSphere\AppServer\bin
      ```

      Linux

      ```
      cd /opt/IBM/WebSphere/AppServer/bin
      ```

   b. Inicie la interfaz **wsadmin** utilizando un ID de usuario autorizado, por ejemplo, SKLMAdmin. Por ejemplo,

      Windows

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

      Linux

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

   c. Ejecute el mandato de interfaz de línea de mandatos **tklmConfigUpdateEntry** para establecer la propiedad **enablePBEInHSM** en el archivo de configuración SKLMConfig.properties.

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

   Interfaz REST

   a. Abra un cliente REST.

   b. Obtenga un identificador de autenticación de usuario exclusivo para acceder a los servicios REST de IBM Security Key Lifecycle Manager. Para obtener más información sobre el proceso de autenticación, consulte Proceso de autenticación de los servicios REST.

   c. Ejecute el **Servicio REST Actualizar propiedad de configuración** para establecer la propiedad **enablePBEInHSM** en el archivo de configuración SKLMConfig.properties. Pase el identificador de autenticación de usuario que ha obtenido en el Paso b junto con el mensaje de solicitud, como se muestra en el ejemplo siguiente.

      ```
      PUT https://localhost:<puerto>/SKLM/rest/v1/configProperties
      Content-Type: application/json
      Accept : application/json
      Authorization: SKLMAuth userAuthId=139aeh34567m
      Accept-Language : en
      { "enablePBEInHSM" : "true"}
      ```

2. Vaya al directorio o la página apropiada para realizar la copia de seguridad.

   Interfaz gráfica de usuario

   a. Inicie una sesión en la interfaz gráfica de usuario.

b. En la página de Bienvenida, pulse **Administración** > **Copia de seguridad y restauración**.

Interfaz de línea de mandatos

a. Vaya al directorio `WAS_HOME/bin`.
b. Inicie la interfaz **`wsadmin`** utilizando un ID de usuario autorizado, por ejemplo, `SKLMAdmin`.

Interfaz REST

Abra un cliente REST.

3. Cree un archivo de copia de seguridad. Sólo puede ejecutar una tarea de copia de seguridad o restauración a la vez.

Interfaz gráfica de usuario

a. En la tabla **Copia de seguridad y restauración**, el campo **Ubicación de repositorio de copia de seguridad** muestra la vía de acceso del directorio *<SKLM_DATA>* predeterminada, donde se guardará el archivo de copia de seguridad, por ejemplo, `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data`. Para ver la definición de *<SKLM_DATA>*, consulte Definiciones para *HOME* y otras variables de directorio.Pulse **Examinar** para especificar una ubicación del repositorio de copia de seguridad bajo el directorio *<SKLM_DATA>*.

   La vía de acceso al directorio en el campo **Ubicación de repositorio de copia de seguridad** cambia en base al valor que se establece en la propiedad **`tklm.backup.dir`** en el archivo `SKLMConfig.properties`.
b. Pulse **Crear copia de seguridad**.
c. En la página Crear copia de seguridad, especifique la información necesaria como, por ejemplo, un valor para la contraseña de cifrado y una descripción de la copia de seguridad. Se muestra una ubicación de archivo de copia de seguridad de solo lectura en el campo **Ubicación de la copia de seguridad**. Asegúrese de conservar la contraseña de cifrado para su uso futuro si desea restaurar la copia de seguridad.
d. Pulse **Crear copia de seguridad**.

Interfaz de línea de mandatos

Escriba **`tklmBackupRun`**, la ubicación de la copia de seguridad, la contraseña y cualquier otra información necesaria para crear un archivo de copia de seguridad tal como se muestra en el ejemplo siguiente.

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

Interfaz REST

Ejecute el **`Servicio REST Ejecutar copia de seguridad`** enviando la solicitud HTTP POST tal como se muestra en el ejemplo siguiente.

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

4. Un mensaje indica que se ha creado el archivo de copia de seguridad o que la operación de copia de seguridad ha sido satisfactoria.

   The time stamp on a backup file has a Greenwich Mean Time (GMT) offset represented in RFC 822 format. The file name contains a *+hhmm* or *-hhmm* element to specify a timezone ahead of or behind GMT. For example, a file

name might be sklm_v3.0.1.0_20170123144220**-0800**_backup.jar, where -0800 indicates that the timezone is eight hours behind GMT.

Qué hacer a continuación

No edite un archivo en el archivo JAR de copia de seguridad. El archivo que intente editar se convertirá en no legible. Debe conectarse al mismo HSM y clave maestra para las operaciones de copia de seguridad y restauración independientemente de si ha utilizado cifrado basado en HSM o cifrado basado en contraseña.

Copia de seguridad de datos con cifrado basado en HSM

Cuando se configura a IBM Security Key Lifecycle Manager con HSM (Hardware Security Module) para almacenar la clave de cifrado maestra, se puede utilizar el cifrado basado en HSM para la creación de copias de seguridad seguras.

Antes de empezar

Asegúrese de que se ha configurado IBM Security Key Lifecycle Manager para que utilice HSM para almacenar la clave maestra antes de crear copias de seguridad de datos con cifrado basado en HSM. Consulte "Configuración de los parámetros de HSM" en la página 210 para conocer los pasos de configuración.

Tenga en cuenta las siguientes directrices para el cifrado basado en HSM

- Debe estar presente la misma partición de HSM con todas sus entradas de clave en el sistema en el que se restaurará el archivo de copia de seguridad.
- También debe estar intacta la clave maestra que se utilizó para el cifrado de clave de copia de seguridad para poder restaurar el archivo de copia de seguridad. Si se renueva la clave maestra, todas las copias de seguridad antiguas serán inaccesibles o no se podrán utilizar.
- Debe conectarse al mismo HSM y clave maestra para las operaciones de copia de seguridad y restauración independientemente de si ha utilizado cifrado basado en HSM o cifrado basado en contraseña.

Acerca de esta tarea

Cuando se ejecuta una operación de copia de seguridad de IBM Security Key Lifecycle Manager, se crea un archivo de archivado de copia de seguridad. La clave de la copia de seguridad en el archivo de archivado cifra el contenido de la copia de seguridad. La clave maestra en HSM cifra la clave de la copia de seguridad. Durante el proceso de restauración, la clave maestra, que se almacena en HSM, descifra la clave de la copia de seguridad. A continuación, se utiliza la clave de la copia de seguridad para restaurar el contenido de la copia de seguridad. Para obtener información sobre el cifrado basado en HSM, consulte Cifrado basado en HSM de copias de seguridad. Your role must have a permission to back up files.

IBM Security Key Lifecycle Manager crea archivos de copia de seguridad, de modo independiente en los sistemas operativos y en la estructura de directorios del servidor. Puede restaurar los archivos de copia de seguridad en un sistema operativo diferente del sistema desde el que ha realizado la copia de seguridad.

Nota: Backup success messages are system wide. Two administrators might run backup tasks that overlap in time. During this interval, the administrator who starts a second task that fails might see a false success message from the first backup task.

Procedimiento

1. Vaya al directorio o la página apropiada.

   Interfaz gráfica de usuario

   a. Inicie una sesión en la interfaz gráfica de usuario.
   b. En la página de Bienvenida, pulse **Administración** > **Copia de seguridad y restauración**.

   Interfaz de línea de mandatos

   a. Vaya al directorio `WAS_HOME/bin`. Por ejemplo,

      Windows

      ```
      cd unidad:\Program Files (x86)\IBM\WebSphere\
      AppServer\bin
      ```

      Linux

      ```
      cd /opt/IBM/WebSphere/AppServer/bin
      ```

   b. Inicie la interfaz **`wsadmin`** utilizando un ID de usuario autorizado, por ejemplo, `SKLMAdmin`. Por ejemplo,

      Windows

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

      Linux

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

   Interfaz REST

   Abra un cliente REST.

2. Cree un archivo de copia de seguridad. Sólo puede ejecutar una tarea de copia de seguridad o restauración a la vez.

   Interfaz gráfica de usuario

   a. En la tabla **Copia de seguridad y restauración**, el campo **Ubicación de repositorio de copia de seguridad** muestra la vía de acceso del directorio <*SKLM_DATA*> predeterminada, donde se guardará el archivo de copia de seguridad, por ejemplo, `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data`. Para ver la definición de <*SKLM_DATA*>, consulte Definiciones para *HOME* y otras variables de directorio.Pulse **Examinar** para especificar una ubicación del repositorio de copia de seguridad bajo el directorio <*SKLM_DATA*>.

      La vía de acceso al directorio en el campo **Ubicación de repositorio de copia de seguridad** cambia en base al valor que se establece en la propiedad **`tklm.backup.dir`** en el archivo `SKLMConfig.properties`.

   b. Pulse **Crear copia de seguridad**.
   c. En la página Crear copia de seguridad, especifique una descripción. Se muestra una ubicación de archivo de copia de seguridad de solo lectura en el campo **Ubicación de la copia de seguridad**.
   d. Pulse **Crear copia de seguridad**.

   Interfaz de línea de mandatos

   Escriba **`tklmBackupRun`**, la ubicación de la copia de seguridad, y toda la información necesaria para crear un archivo de copia de seguridad. Por ejemplo:

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

   Interfaz REST

a. Obtenga un identificador de autenticación de usuario exclusivo para acceder a los servicios REST de IBM Security Key Lifecycle Manager. Para obtener más información sobre el proceso de autenticación, consulte Proceso de autenticación de los servicios REST.

b. Para ejecutar el **Servicio REST Ejecutar copia de seguridad**, envíe la solicitud HTTP POST. Pase el identificador de autenticación de usuario que ha obtenido en el `Paso a` junto con el mensaje de solicitud, como se muestra en el ejemplo siguiente.

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

3. Un mensaje indica que se ha creado el archivo de copia de seguridad o que la operación de copia de seguridad ha sido satisfactoria.

   The time stamp on a backup file has a Greenwich Mean Time (GMT) offset represented in RFC 822 format. The file name contains a *+hhmm* or *-hhmm* element to specify a timezone ahead of or behind GMT. For example, a file name might be `sklm_v3.0.1.0_20170123144220-0800_backup.jar`, where -0800 indicates that the timezone is eight hours behind GMT.

Qué hacer a continuación

No edite un archivo en el archivo JAR de copia de seguridad. El archivo que intente editar se convertirá en no legible. También debe estar intacta la clave maestra que se utilizó para el cifrado de clave de copia de seguridad para poder restaurar el archivo de copia de seguridad. Si se renueva la clave maestra, todas las copias de seguridad antiguas serán inaccesibles o no se podrán utilizar.

Copia de seguridad de una cantidad grande de datos

Debe establecer la propiedad **enableHighScaleBackup=true** en el archivo de configuración `SKLMConfig.properties` para realizar copias de seguridad de un gran número de claves de cifrado.

Acerca de esta tarea

La página Copia de seguridad y restauración sirve para realizar copias de seguridad de sus datos. O bien, puede utilizar el mandato **tklmBackupRun** o el **Servicio REST Ejecutar copia de seguridad**. Your role must have a permission to back up files.

Nota:

- No es posible realizar un archivo de copia de seguridad compatible entre plataformas si se ha configurado a IBM Security Key Lifecycle Manager para actividades de copia se seguridad y restauración de alto rendimiento. El archivo de copia de seguridad se puede utilizar para restaurar datos en un entorno operativo idéntico. El sistema operativo, los componentes de middleware y las estructuras de directorios deben ser idénticos en ambos sistemas.
- Durante el proceso de restauración el archivo `db2restore.log` únicamente se crea cuando se configura a IBM Security Key Lifecycle Manager para operaciones de copia de seguridad y restauración de alto rendimiento.

Procedimiento

1. Establezca la propiedad **enableHighScaleBackup=true** en el archivo <*SKLM_HOME*>/config/SKLMConfig.properties.

   Interfaz de línea de mandatos

   a. Vaya al directorio <*WAS_HOME*>/bin. Por ejemplo,

      Windows

      ```
      cd unidad:\Program Files (x86)\IBM\WebSphere\
      AppServer\bin
      ```

      Linux

      ```
      cd /opt/IBM/WebSphere/AppServer/bin
      ```

   b. Inicie la interfaz **wsadmin** utilizando un ID de usuario autorizado, por ejemplo, SKLMAdmin. Por ejemplo,

      Windows

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

      Linux

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

   c. Ejecute el mandato **tklmConfigUpdateEntry** para establecer la propiedad **enableHighScaleBackup** en el archivo de configuración SKLMConfig.properties.

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

   Interfaz REST

   a. Abra un cliente REST.

   b. Obtenga un identificador de autenticación de usuario exclusivo para acceder a los servicios REST de IBM Security Key Lifecycle Manager. Para obtener más información sobre el proceso de autenticación, consulte Proceso de autenticación de los servicios REST.

   c. Ejecute el **Servicio REST Actualizar propiedad de configuración** para establecer la propiedad **enableHighScaleBackup** en el archivo de configuración SKLMConfig.properties. Pase el identificador de autenticación de usuario que ha obtenido en el Paso b junto con el mensaje de solicitud, como se muestra en el ejemplo siguiente.

      ```
      PUT https://localhost:<puerto>/SKLM/rest/v1/configProperties
      Content-Type: application/json
      Accept : application/json
      Authorization: SKLMAuth userAuthId=139aeh34567m
      Accept-Language : en
      { "enableHighScaleBackup" : "true"}
      ```

2. Vaya al directorio o la página apropiada para realizar la copia de seguridad.

   Interfaz gráfica de usuario

   a. Inicie una sesión en la interfaz gráfica de usuario.

   b. En la página de Bienvenida, pulse **Administración** > **Copia de seguridad y restauración**.

   Interfaz de línea de mandatos

   a. Vaya al directorio <*WAS_HOME*>/bin.

   b. Inicie la interfaz **wsadmin** utilizando un ID de usuario autorizado, por ejemplo, SKLMAdmin.

   Interfaz REST

   Abra un cliente REST.

3. Cree un archivo de copia de seguridad. Sólo se puede ejecutar una tarea de copia de seguridad o restauración a la vez.

   Interfaz gráfica de usuario

   a. En la tabla **Copia de seguridad y restauración**, el campo **Ubicación de repositorio de copia de seguridad** muestra la vía de acceso del directorio <*SKLM_DATA*> predeterminada, donde se guardará el archivo de copia de seguridad, por ejemplo, `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data`. Para ver la definición de <*SKLM_DATA*>, consulte Definiciones para *HOME* y otras variables de directorio.Pulse **Examinar** para especificar una ubicación del repositorio de copia de seguridad bajo el directorio <*SKLM_DATA*>.

      La vía de acceso al directorio en el campo **Ubicación de repositorio de copia de seguridad** cambia en base al valor que se establece en la propiedad **`tklm.backup.dir`** en el archivo `SKLMConfig.properties`.

   b. Pulse **Crear copia de seguridad**.

   c. En la página Crear copia de seguridad, especifique la información necesaria como, por ejemplo, un valor para la contraseña de cifrado y una descripción de la copia de seguridad. Se muestra una ubicación de archivo de copia de seguridad de solo lectura en el campo **Ubicación de la copia de seguridad**. Asegúrese de conservar la contraseña de cifrado para su uso futuro si desea restaurar la copia de seguridad.

      Nota: Si para las copias de seguridad se está utilizando el cifrado basado en HSM, no es necesario especificar la contraseña.

   d. Pulse **Crear copia de seguridad**.

   Interfaz de línea de mandatos

   Escriba `tklmBackupRun` y especifique los valores necesarios para crear un archivo de copia de seguridad tal como se muestra en el ejemplo siguiente.

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

   Interfaz REST

   Ejecute el **`Servicio REST Ejecutar copia de seguridad`** enviando la solicitud HTTP POST tal como se muestra en el ejemplo siguiente.

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

4. Se visualiza un mensaje que indica que se ha creado el archivo de copia de seguridad, o que la operación de copia de seguridad ha sido satisfactoria.

   The time stamp on a backup file has a Greenwich Mean Time (GMT) offset represented in RFC 822 format. The file name contains a *+hhmm* or *-hhmm* element to specify a timezone ahead of or behind GMT. For example, a file name might be `sklm_v3.0.1.0_20170123144220`**`-0800`**`_backup.jar`, where -0800 indicates that the timezone is eight hours behind GMT.

   Nota: Backup success messages are system wide. Two administrators might run backup tasks that overlap in time. During this interval, the administrator who starts a second task that fails might see a false success message from the first backup task.

Qué hacer a continuación

Conserve la contraseña de cifrado para su uso futuro si desea restaurar la copia de seguridad. Revise el directorio que contiene los archivos de copia de seguridad para garantizar que existe el archivo de copia de seguridad. No edite un archivo en el archivo JAR de copia de seguridad. El archivo que intente editar se convertirá en no legible.

Restauración de un archivo de copia de seguridad

Una restauración devuelve el IBM Security Key Lifecycle Manager server a un estado conocido, utilizando datos de producción incluidos en la copia de seguridad como, por ejemplo, materiales de clave de IBM Security Key Lifecycle Manager y otra información crítica.

Antes de empezar

Tenga en cuenta las siguientes directrices antes de restaurar copias de seguridad cifradas basadas en HSM:

- Asegúrese de que está presente la misma partición HSM con todas sus entradas de clave intactas en el sistema en el que se restaura el archivo de copia de seguridad.
- También debe estar intacta la clave maestra que se utilizó para el cifrado de clave de copia de seguridad para poder restaurar el archivo de copia de seguridad. Si se renueva la clave maestra, todas las copias de seguridad antiguas serán inaccesibles o no se podrán utilizar.
- Debe conectarse al mismo HSM y clave maestra para las operaciones de copia de seguridad y restauración independientemente de si ha utilizado cifrado basado en HSM o cifrado basado en contraseña.

Cuando ejecuta la operación de copia de seguridad, se crea el archivo manifest junto con el archivo de archivado de copia de seguridad. Antes de restaurar los archivos de copia de seguridad, asegúrese de que el archivo manifest de copia de seguridad contenga todos los archivos de datos de IBM Security Key Lifecycle Manager de la copia archivada.

Acerca de esta tarea

Puede utilizar la página Copia de seguridad y restauración para restaurar un archivo de copia de seguridad.O bien, puede utilizar el mandato **tklmBackupRunRestore** o el **Servicio REST Ejecutar restauración de copia de seguridad** para restaurar el archivo. Your role must have a permission to restore files.. IBM Security Key Lifecycle Manager crea archivos de copia de seguridad de modo independiente a los sistemas operativos y la estructura de directorios del servidor. Puede restaurar los archivos de copia de seguridad en un sistema operativo diferente del sistema desde el que ha realizado la copia de seguridad.

Before you start a restore task, isolate the system for maintenance. Take a backup of the existing system. You can later use this backup to bring the system back to original state if any issues occur during the restore process. IBM Security Key Lifecycle Manager server automatically restarts after the restore process is complete. Verify the environment before you bring the IBM Security Key Lifecycle Manager server back into production.

Procedimiento

1. Vaya a la página o el directorio correspondiente:

   Interfaz gráfica de usuario

   a. Inicie una sesión en la interfaz gráfica de usuario.
   b. En la página de Bienvenida, pulse **Administración** > **Copia de seguridad y restauración**.

   Interfaz de línea de mandatos

   a. Vaya al directorio `WAS_HOME/bin`. Por ejemplo,

      Windows

      ```
      cd unidad:\Program Files\IBM\WebSphere\AppServer\bin
      ```

      Linux

      ```
      cd /opt/IBM/WebSphere/AppServer/bin
      ```

   b. Inicie la interfaz **wsadmin** utilizando un ID de usuario autorizado, por ejemplo, `SKLMAdmin`. Por ejemplo,

      Windows

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

      Linux

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

      Interfaz REST

      - Abra un cliente REST.

2. Restaure un archivo de copia de seguridad seleccionado. Sólo se puede ejecutar una tarea de copia de seguridad o restauración a la vez. Si restaura un archivo en un sistema de réplica, copie el archivo en el sistema utilizando un soporte como, por ejemplo, un disco o una transmisión electrónica.

   Interfaz gráfica de usuario

   a. En la tabla **Copia de seguridad y restauración**, seleccione un archivo de copia de seguridad que aparece en la tabla.
   b. Pulse **Restaurar desde copia de seguridad**.

      Nota:

      - Si ha aplicado un fixpack en los sistemas distribuidos, no intente restaurar los archivos de copia de seguridad que se han creado antes de la aplicación del fixpack.

   c. En la página Restaurar copia de seguridad, especifique la contraseña de cifrado que se ha utilizado para crear el archivo de copia de seguridad.

      Nota: Si para las copias de seguridad se está utilizando el cifrado basado en HSM, no es necesario especificar la contraseña.

   d. Pulse **Restaurar copia de seguridad**.

   Interfaz de línea de mandatos

   Escriba `tklmBackupRunRestore` y especifique la información necesaria como, por ejemplo, la vía de acceso y el nombre del archivo de copia de seguridad. Especifique la contraseña de cifrado que se ha utilizado para crear el archivo de copia de seguridad. Por ejemplo, escriba:

   ```
   print AdminTask.tklmBackupRunRestore
    ('[-backupFilePath /opt/mysklmbackups/sklm_v3.0.1.0_20170705235417-1200_backup
     -password myBackupPwd]')
   ```

Nota: Si para las copias de seguridad se está utilizando el cifrado basado en HSM, no es necesario especificar la contraseña.

Interfaz REST

a. Obtenga un identificador de autenticación de usuario exclusivo para acceder a los servicios REST de IBM Security Key Lifecycle Manager. Para obtener más información sobre el proceso de autenticación, consulte Proceso de autenticación de los servicios REST.

b. Para ejecutar el **Servicio REST Ejecutar restauración de copia de seguridad**, envíe la solicitud HTTP POST. Pase el identificador de autenticación de usuario que ha obtenido en el `Paso a` junto con el mensaje de solicitud, como se muestra en el ejemplo siguiente.

```
POST https://localhost:<puerto>/SKLM/rest/v1/ckms/restore
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth authId=139aeh34567m
Accept-Language : en
{"backupFilePath":"/opt/mysklmbackups/sklm_v2.7.0.0_20160705235417-1200_
backup.jar","password":"myBackupPwd"}
```

Nota: Si para las copias de seguridad se está utilizando el cifrado basado en HSM, no es necesario especificar la contraseña.

3. Un mensaje indica que la operación de restauración ha sido correcta.

Resultados

El servidor de IBM Security Key Lifecycle Manager se reinicia de forma automática una vez se haya restaurado un archivo de copia de seguridad cuando el valor de la propiedad **autoRestartAfterRestore** sea `true` (valor predeterminado) en el archivo `SKLMConfig.properties`.

Nota: Después del reinicio automático del servidor IBM Security Key Lifecycle Manager, el estado de servicio WebSphere Application Server de las ventanas no se renovará y se mostrará como detenido.

Qué hacer a continuación

Nota: After data restoration, ensure that the path for the properties in the `SKLMConfig.properties`, `datastore.properties`, and `ReplicationSKLMConfig.properties` files are correct before you proceed with your next task.

Determine si el servidor está en el estado esperado. Por ejemplo, puede examinar el almacén de claves para ver si un certificado generaba problemas antes de restaurar el archivo de seguridad está ahora disponible para su uso.

Supresión de un archivo de copia de seguridad

Utilice la interfaz gráfica de usuario o la interfaz de línea de mandatos para suprimir un archivo de copia de seguridad de IBM Security Key Lifecycle Manager. Por ejemplo, puede suprimir un archivo de copia de seguridad que ya no se necesita en la empresa.

Acerca de esta tarea

Puede utilizar la página Copia de seguridad y restauración para suprimir un archivo de copia de seguridad.

Your role must have a permission to back up files.

Procedimiento

1. Inicie una sesión en la interfaz gráfica de usuario.
2. En la página de Bienvenida, pulse **Administración** > **Copia de seguridad y restauración**.
3. En la tabla **Copia de seguridad y restauración**, seleccione un archivo de copia de seguridad que aparece en la tabla.
4. Pulse **Suprimir copia de seguridad** para confirmar que desea suprimir el archivo.

Qué hacer a continuación

Examine el directorio donde se almacenan los archivos de copia de seguridad para determinar si se ha suprimido el archivo especificado.

Ejecución de tareas de copia de seguridad y restauración en la interfaz REST o linea de mandatos

Puede utilizar la interfaz de línea de mandatos o la interfaz REST para más tareas de copia de seguridad y restauración que no están disponibles en la interfaz gráfica de usuario.

Acerca de esta tarea

Antes de empezar, obtenga la contraseña. Your role must have permissions to back up or to restore files.

Procedimiento

1. Vaya al directorio o la página apropiada.
   - Command-line interface
     a. Go to the <*WAS_HOME*>/bin directory. For example,

        Windows
        ```
        cd drive:\Program Files\IBM\WebSphere\AppServer\bin
        ```

        Linux
        ```
        cd /opt/IBM/WebSphere/AppServer/bin
        ```

     b. Start the **wsadmin** interface by using an authorized user ID, such as SKLMAdmin. For example,

        Windows
        ```
        wsadmin.bat -username SKLMAdmin -password mypwd -lang jython
        ```

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

   - Interfaz REST:
     – Abra un cliente REST.
2. Complete la tarea.
   - Interfaz de línea de mandatos:

     tklmBackupGetProgress

Escriba `tklmBackupGetProgress` para determinar la fase actual de una tarea de copia de seguridad que se está ejecutando. Por ejemplo, escriba:

```
print AdminTask.tklmBackupGetProgress()
```

tklmBackupGetRestoreProgress

Escriba `tklmBackupGetRestoreProgress` para determinar la fase actual de una tarea de restauración que se está ejecutando. Por ejemplo, escriba:

```
print AdminTask.tklmBackupGetRestoreProgress()
```

tklmBackupGetRestoreResult

Escriba `tklmBackupGetRestoreResult` para determinar si una tarea de restauración se ha ejecutado correctamente o no. Por ejemplo, escriba:

```
print AdminTask.tklmBackupGetRestoreResult()
```

tklmBackupGetResult

Escriba `tklmBackupGetResult` para determinar si una tarea de copia de seguridad se ha ejecutado correctamente o no. Por ejemplo, escriba:

```
print AdminTask.tklmBackupGetResult()
```

tklmBackupIsRestoreRunning

Escriba `tklmBackupIsRestoreRunning` para determinar si la tarea de restauración se está ejecutando. Por ejemplo, escriba:

```
print AdminTask.tklmBackupIsRestoreRunning()
```

tklmBackupIsRunning

Escriba `tklmBackupIsRunning` para determinar si la tarea de copia de seguridad se está ejecutando. Por ejemplo, escriba:

```
print AdminTask.sklmBackupIsRunning()
```

tklmBackupList

Escriba `tklmBackupList` para listar los archivos de copia de seguridad en un directorio. Por ejemplo, escriba:

```
print AdminTask.tklmBackupList
 ('[-backupDirectory C:\\sklmbackup1 -v y]')
```

- Interfaz REST:
  a. Obtenga un identificador de autenticación de usuario exclusivo para acceder a los servicios REST de IBM Security Key Lifecycle Manager. Para obtener más información sobre el proceso de autenticación, consulte Proceso de autenticación de los servicios REST.
  b. Para invocar el servicio REST, envíe la solicitud de HTTP. Pase el identificador de autenticación de usuario que ha obtenido en el `Paso a` junto con el mensaje de solicitud, como se muestra en el ejemplo siguiente.

Servicio REST Obtener progreso de copia de seguridad

Utilice el **Servicio REST Obtener progreso de copia de seguridad** para determinar la fase actual de una tarea de copia de seguridad que se esté ejecutando. Por ejemplo, puede enviar la siguiente solicitud HTTP:

```
GET https://localhost:<puerto>/SKLM/rest/v1/ckms/backups/progress
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth authId=139aeh34567m
Accept-Language : en
```

Servicio REST Obtener progreso de restauración de copia de seguridad

Utilice el **Servicio REST Obtener progreso de restauración de copia de seguridad** para determinar la fase actual de una tarea de restauración que se esté ejecutando. Por ejemplo, puede enviar la siguiente solicitud HTTP:

```
GET https://localhost:<puerto>/SKLM/rest/v1/ckms/restore/progress
Content-Type: application/json
Accept: application/json
Authorization: SKLMAuth authId=139aeh34567m
Accept-Language: en
```

Servicio REST Obtener resultado de restauración de copia de seguridad

Utilice el **Servicio REST Obtener resultado de restauración de copia de seguridad** para determinar si se ha completado la tarea de restauración de forma correcta o anómala. Por ejemplo, puede enviar la siguiente solicitud HTTP:

```
GET https://localhost:<puerto>/SKLM/rest/v1/ckms/restore/result
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth authId=139aeh34567m
Accept-Language : en
```

Servicio REST Obtener resultado de copia de seguridad

Utilice el **Servicio REST Obtener resultado de copia de seguridad** para determinar si se ha completado la tarea de copia de seguridad de forma correcta o anómala. Por ejemplo, puede enviar la siguiente solicitud HTTP:

```
GET https://localhost:<puerto>/SKLM/rest/v1/ckms/backups/result
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth authId=139aeh34567m
Accept-Language : en
```

Servicio REST Lista de copia de seguridad

Utilice el **Servicio REST Lista de copia de seguridad** para enumerar los archivos de copia de seguridad en un directorio. Por ejemplo, puede enviar la siguiente solicitud HTTP:

```
GET https://localhost:<puerto>/SKLM/rest/v1/ckms/backups?backupDirectory=
/sklmbackup
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth authId=139aeh34567m
Accept-Language : en
```

Operaciones de copia de seguridad y restauración para versiones anteriores de IBM Security Key Lifecycle Manager e IBM Tivoli Key Lifecycle Manager

Puede utilizar el programa de utilidad de copia de seguridad entre plataformas de la versión actual de IBM Security Key Lifecycle Manager para ejecutar la operación de copia de seguridad en las versiones anteriores de IBM Security Key Lifecycle Manager e IBM Tivoli Key Lifecycle Manager para realizar copias de seguridad de los datos críticos. Puede restaurar estos archivos de copia de seguridad en la

versión actual de IBM Security Key Lifecycle Manager entre sistemas operativos utilizando el programa de utilidad de restauración.

Nota: For greater security, change the IBM Security Key Lifecycle Manager User password soon after the data migration process.

Datos de migración cruzada de IBM Tivoli Key Lifecycle Manager, Versión 1.0

Utilice los programas de utilidad de copia de seguridad y restauración de IBM Security Key Lifecycle Manager para realizar una migración cruzada de los datos de IBM Tivoli Key Lifecycle Manager, Versión 1.0.

Acerca de esta tarea

La migración cruzada de los datos de IBM Tivoli Key Lifecycle Manager, Versión 1.0 a IBM Security Key Lifecycle Manager, Versión 3.0.1 está formada por las siguientes dos etapas:

1. Migración de los datos de IBM Tivoli Key Lifecycle Manager, Versión 1.0 a un sistema donde IBM Security Key Lifecycle Manager, Versión 2.7 esté instalado, siguiendo los pasos descritos en la documentación de IBM Security Key Lifecycle Manager, Versión 2.7.

   Copia de seguridad de los datos de IBM Tivoli Key Lifecycle Manager, Versión 1.0

   Restauración de archivos de copia de seguridad de IBM Tivoli Key Lifecycle Manager Versión 1.0
2. Migración de los datos de IBM Security Key Lifecycle Manager, Versión 2.7 a un sistema donde IBM Security Key Lifecycle Manager, Versión 3.0.1 esté instalado, siguiendo los pasos descritos en los siguientes temas.

   "Copia de seguridad de los datos de IBM Security Key Lifecycle Manager, Versión 2.7" en la página 161

   "Restauración de los archivos de copia de seguridad de IBM Security Key Lifecycle Manager, Versión 2.7" en la página 163

Datos de migración cruzada de IBM Tivoli Key Lifecycle Manager, Versión 2.0

Utilice los programas de utilidad de copia de seguridad y restauración de IBM Security Key Lifecycle Manager para realizar una migración cruzada de los datos de IBM Tivoli Key Lifecycle Manager, Versión 2.0.

Acerca de esta tarea

La migración cruzada de los datos de IBM Tivoli Key Lifecycle Manager, Versión 2.0 a IBM Security Key Lifecycle Manager, Versión 3.0.1 está formada por las siguientes dos etapas:

1. Migración de los datos de IBM Tivoli Key Lifecycle Manager, Versión 2.0 a un sistema donde IBM Security Key Lifecycle Manager, Versión 2.7 esté instalado, siguiendo los pasos descritos en la documentación de IBM Security Key Lifecycle Manager, Versión 2.7.

   Copia de seguridad de los datos de IBM Tivoli Key Lifecycle Manager, Versión 2.0

   Restauración de archivos de copia de seguridad de IBM Tivoli Key Lifecycle Manager Versión 2.0

2. Migración de los datos de IBM Security Key Lifecycle Manager, Versión 2.7 a un sistema donde IBM Security Key Lifecycle Manager, Versión 3.0.1 esté instalado, siguiendo los pasos descritos en los siguientes temas.

   "Copia de seguridad de los datos de IBM Security Key Lifecycle Manager, Versión 2.7" en la página 161

   "Restauración de los archivos de copia de seguridad de IBM Security Key Lifecycle Manager, Versión 2.7" en la página 163

Datos de migración cruzada de IBM Tivoli Key Lifecycle Manager, Versión 2.0.1

Utilice los programas de utilidad de copia de seguridad y restauración de IBM Security Key Lifecycle Manager para realizar una migración cruzada de los datos de IBM Tivoli Key Lifecycle Manager, Versión 2.0.1.

Acerca de esta tarea

La migración cruzada de los datos de IBM Tivoli Key Lifecycle Manager, Versión 2.0.1 a IBM Security Key Lifecycle Manager, Versión 3.0.1 está formada por las siguientes dos etapas:

1. Migración de los datos de IBM Tivoli Key Lifecycle Manager, Versión 2.0.1 a un sistema donde IBM Security Key Lifecycle Manager, Versión 2.7 esté instalado, siguiendo los pasos descritos en la documentación de IBM Security Key Lifecycle Manager, Versión 2.7.

   Copia de seguridad de los datos de IBM Tivoli Key Lifecycle Manager, Versión 2.0.1

   Restauración de archivos de copia de seguridad de IBM Tivoli Key Lifecycle Manager Versión 2.0.1
2. Migración de los datos de IBM Security Key Lifecycle Manager, Versión 2.7 a un sistema donde IBM Security Key Lifecycle Manager, Versión 3.0.1 esté instalado, siguiendo los pasos descritos en los siguientes temas.

   "Copia de seguridad de los datos de IBM Security Key Lifecycle Manager, Versión 2.7" en la página 161

   "Restauración de los archivos de copia de seguridad de IBM Security Key Lifecycle Manager, Versión 2.7" en la página 163

Copia de seguridad de los datos de Encryption Key Manager, Versión 2.1

Utilice el programa de utilidad de copia de seguridad de IBM Security Key Lifecycle Manager, Versión 3.0.1 para crear los archivos de copia de seguridad de Encryption Key Manager, Versión 2.1.

Antes de empezar

- Debe instalar IBM Security Key Lifecycle Manager, Versión 3.0.1 en un sistema.
- Asegúrese de que la carpeta Encryption Key Manager contiene el archivo de configuración, los archivos del almacén de claves y otros archivos de datos y carpetas que estén relacionadas con las tablas de unidades, grupos de claves y metadatos.

Acerca de esta tarea

Puede utilizar el programa de utilidad de copia de seguridad para crear archivos de copia de seguridad entre plataformas, de modo independiente a los sistemas

operativos y la estructura de directorios del servidor. Puede restaurar estos archivos de copia seguridad, compatibles entre plataformas, en un sistema con IBM Security Key Lifecycle Manager, Versión 3.0.1 en diferentes sistemas operativos.

Nota: For greater security, change the IBM Security Key Lifecycle Manager User password soon after the data migration process.

Procedimiento

1. Copie la carpeta Encryption Key Manager y todos los otros archivos necesarios en un sistema en el que esté instalado IBM Security Key Lifecycle Manager, Versión 3.0.1.
2. Asegúrese de que el archivo `KeyManagerConfig.properties` y los siguientes archivos que se mencionan en el archivo `KeyManagerConfig.properties` se copiarán.

   Nota: Edite el archivo de configuración `KeyManagerConfig.properties` de la carpeta Encryption Key Manager para especificar vías de acceso absolutas del almacén de claves y otros archivos de datos, como se muestra en el ejemplo siguiente.

   ```
   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. Localice la carpeta utilities de copia de seguridad en el sistema en el que está instalada la versión 3.0.1.

   Windows

   `<SKLM_INSTALL_HOME>\migration\utilities\ekm21`

   La ubicación predeterminada es `C:\Program Files\IBM\SKLMV301\migration\utilities\ekm21`.

   Linux `<SKLM_INSTALL_HOME>/migration/utilities/ekm21`

   La ubicación predeterminada es `/opt/IBM/SKLMV301/migration/utilities/ekm21`.

4. Edite `backup.properties` en la carpeta utilities para configurar las propiedades, como se muestra en el ejemplo siguiente. Debe establecer valores para todas las propiedades, excepto para la propiedad `BACKUP_DIR` (opcional).

   Si no especifica el valor para `BACKUP_DIR`, el archivo de copia de seguridad se crea en la subcarpeta `backup` en el mismo directorio desde donde se ejecuta la utilidad de copia de seguridad.

   Nota: On Windows operating system, the `backup.properties` file that you use for backup operations must not contain the property keys and values with leading or trailing spaces.

   Windows

   ```
   KLM_VERSION=2.1
   BACKUP_DIR=C:\\ekm_backup
   EKM_HOME=C:\\EKM21
   BACKUP_PASSWORD=passw0rd123
   JAVA_HOME=C:\\Program Files\\IBM\\WebSphere\\AppServer\\java\8.0
   ```

Linux

```
KLM_VERSION=2.1
BACKUP_DIR=/ekm_backup
EKM_HOME=/EKM21
BACKUP_PASSWORD=passw0rd123
JAVA_HOME=/opt/IBM/WebSphere/AppServer/java/8.0
```

Nota: En los sistemas Windows, cuando especifique la vía de acceso en el archivo de propiedades, utilice "/ " o "\\ " como separador de vías de acceso, como se muestra en el ejemplo siguiente.

```
C:\\ekm_backup
```

O

```
C:/ekm_backup
```

5. Abra una ventana del indicador de mandatos y ejecute el programa de utilidad de copia de seguridad.

Windows

Vaya al directorio <*SKLM_INSTALL_HOME*>\migration\utilities\ekm21 y ejecuta el siguiente mandato:

```
backupEKM21.bat
```

Linux

a. Vaya al directorio ekm21 (consulte el paso b).
b. Compruebe si el archivo backupEKM21.sh tiene permisos ejecutables. En caso de que no, otorgue permisos ejecutando el siguiente mandato:

   ```
   chmod 755 backupEKM21.sh
   ```

c. Ejecute el programa de utilidad de copia de seguridad:

   ```
   backupEKM21.sh
   ```

Qué hacer a continuación

- Review the directory that contains backup files to ensure that the backup file exists. The backup files are created in the location that you specified for BACKUP_DIR in the backup.properties file.
- Check the backup.log file for errors or exceptions. The backup.log file is created in the same directory where you run the backup utility. For a successful backup operation, ensure that there are no errors or exceptions in the log file.
- Retain the backup password for future use in case you restore the backup.
- Do not edit a file in the backup archive. The file that you attempt to edit becomes unreadable.

Restauración de los archivos de copia de seguridad de Encryption Key Manager, Versión 2.1

Puede restaurar los archivos de copia de seguridad entre plataformas de Encryption Key Manager, Versión 2.1 en un sistema con IBM Security Key Lifecycle Manager, Versión 3.0.1 utilizando la interfaz gráfica de usuario, la interfaz de línea de mandatos, la interfaz REST o el script de restauración de migración.

Antes de empezar

Instale IBM Security Key Lifecycle Manager, Versión 3.0.1 en un sistema. Debe tener el archivo de copia de seguridad de Encryption Key Manager y asegurarse de que tiene la contraseña que se ha utilizado al crear el archivo de copia de seguridad.

Nota: Debe tener el rol de usuario de IBM Security Key Lifecycle Manager para ejecutar operaciones de copia de seguridad y restauración.

Acerca de esta tarea

Puede restaurar los archivos de copia de seguridad compatibles entre plataformas de Encryption Key Manager en un sistema con IBM Security Key Lifecycle Manager, Versión 3.0.1 en diferentes sistemas operativos.

Before you start a restore task, isolate the system for maintenance. Take a backup of the existing system. You can later use this backup to bring the system back to original state if any issues occur during the restore process. IBM Security Key Lifecycle Manager server automatically restarts after the restore process is complete. Verify the environment before you bring the IBM Security Key Lifecycle Manager server back into production.

Nota: For greater security, change the IBM Security Key Lifecycle Manager User password soon after the data migration process.

Procedimiento

1. Inicie sesión en el sistema en el que está instalado IBM Security Key Lifecycle Manager, Versión 3.0.1.
2. Copie el archivo de copia de seguridad, por ejemplo `sklm_vEKM21_20170420113253+0530_backup.jar`, desde el sistema Encryption Key Manager, Versión 2.1 a una carpeta de su elección bajo el directorio <*SKLM_DATA*>, por ejemplo, `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data`. Para ver la definición de <*SKLM_DATA*>, consulte Definiciones para *HOME* y otras variables de directorio.
3. Restaure el archivo de copia de seguridad utilizando cualquiera de los métodos siguientes.

Interfaz gráfica de usuario	1. Inicie sesión en la interfaz gráfica de usuario como usuario autorizado, por ejemplo, `SKLMAdmin`. 2. En la página de Bienvenida, pulse **Administración** > **Copia de seguridad y restauración**. 3. Pulse **Examinar** para especificar la ubicación del archivo de copia de seguridad de Encryption Key Manager bajo el directorio <*SKLM_DATA*>. 4. Pulse **Visualizar copias de seguridad** para visualizar los archivos de copia de seguridad que desea restaurar. 5. En la tabla **Copia de seguridad y restauración**, seleccione un archivo de copia de seguridad. 6. Pulse **Restaurar desde copia de seguridad**. 7. En la página Restaurar copia de seguridad, especifique la contraseña de copia de seguridad que se ha utilizado para crear el archivo de copia de seguridad. 8. Pulse **Restaurar copia de seguridad**. 9. Reinicie el servidor de IBM Security Key Lifecycle Manager.

Interfaz de línea de mandatos	1. Vaya al directorio <*WAS_HOME*>/bin. Por ejemplo,
	Windows
	`cd unidad:\Program Files\IBM\WebSphere\AppServer\bin`
	Linux `cd /opt/IBM/WebSphere/AppServer/bin`
	2. Inicie la interfaz **wsadmin** utilizando un ID de usuario autorizado, por ejemplo, SKLMAdmin. Por ejemplo,
	Windows
	`wsadmin.bat -username SKLMAdmin -password mypwd -lang jython`
	Linux
	`./wsadmin.sh -username SKLMAdmin -password mypwd -lang jython`
	3. Ejecute el mandato de CLI **tklmBackupRunRestore** especificando los parámetros, por ejemplo, el nombre del archivo de copia de seguridad con su vía de acceso completa y la contraseña de copia de seguridad que ha utilizado para crear la copia de seguridad, como se muestra en el ejemplo siguiente.
	`print AdminTask.tklmBackupRunRestore ('[-backupFilePath <SKLM_DATA>/sklm_vEKM21_20170420113253+0530_backup.jar -password myBackupPwd]')`
	4. Reinicie el servidor de IBM Security Key Lifecycle Manager.

Interfaz REST	1. Abra un cliente REST.
	2. Obtenga un identificador de autenticación de usuario exclusivo para acceder a los servicios REST de IBM Security Key Lifecycle Manager. Para obtener más información sobre el proceso de autenticación, consulte Proceso de autenticación de los servicios REST.
	3. Para invocar el **Servicio REST Ejecutar restauración de copia de seguridad**, envíe la solicitud HTTP POST con el nombre de archivo de copia de seguridad y la vía de acceso completa y la contraseña de copia de seguridad como parámetros. Pase el identificador de autenticación de usuario que ha obtenido en el Paso b junto con el mensaje de solicitud, como se muestra en el ejemplo siguiente.
	`POST https://localhost:<puerto>/SKLM/rest/v1/ckms/restore`
	`Content-Type: application/json`
	`Accept: application/json`
	`Authorization: SKLMAuth authId=139aeh34567m`
	`Accept-Language: en`
	`{"backupFilePath":"<SKLM_DATA>/sklm_vEKM21_20170420113253+0530_backup.jar backup.jar","password":"myBackupPwd"}`
	4. Reinicie el servidor de IBM Security Key Lifecycle Manager.

Script de restauración de migración	1. Localice los programas de utilidad de IBM Security Key Lifecycle Manager. **Windows** <*SKLM_INSTALL_HOME*>\migration\utilities\ekm21 La ubicación predeterminada es C:\Program Files\IBM\SKLMV30\migration\utilities\ekm21. **Linux** <*SKLM_INSTALL_HOME*>/migration/utilities/ekm21 La ubicación predeterminada es /opt/IBM/SKLMV301/migration/utilities/ekm21. 2. Edite restore.properties en la carpeta ekm21 para configurar las propiedades, como se muestra en el ejemplo siguiente: **Nota:** On Windows operating system, the restore.properties file that you use for restore operations must not contain the property keys and values with leading or trailing spaces. **Windows** WAS_HOME=C:\\Program Files\\IBM\\WebSphere\\AppServer JAVA_HOME=C:\\Program Files\\IBM\\WebSphere\\AppServer\\java\8.0 BACKUP_PASSWORD=passw0rd123 DB_PASSWORD=db2_password RESTORE_FILE=<*SKLM_DATA*>\\sklm_vEKM21_20170424024117-0400_backup. WAS_USER_PWD=wasadmin_password RESTORE_USER_ROLES=n **Linux** WAS_HOME=/opt/IBM/WebSphere/AppServer JAVA_HOME=/opt/IBM/WebSphere/AppServer/java/8.0 BACKUP_PASSWORD=passw0rd123 DB_PASSWORD=db2_password RESTORE_FILE=<*SKLM_DATA*>/20170424024117-0400_backup.jar WAS_USER_PWD=wasadmin_password RESTORE_USER_ROLES=n Para iniciar una sesión en IBM Security Key Lifecycle Manager mediante la utilización de las credenciales especificadas durante la instalación del producto, establezca la propiedad **RESTORE_USER_ROLES** como “n”. Cuando la propiedad se establece en “n” se asegura que el ID de usuario y la contraseña no se sobrescriben con las credenciales de usuario de la versión antigua. **Nota:** En el sistema operativo de Windows, cuando especifique la vía de acceso en el archivo de propiedades, utilice “/ ” o “\\ ” como separador de vías de acceso, como se muestra en el ejemplo siguiente. C:\\ekm_restore O C:/ekm_restore 3. Abra una ventana del indicador de mandatos y especifique estos mandatos. **Windows** Vaya al directorio <*SKLM_INSTALL_HOME*>\migration\utilities\ekm21 y ejecuta el siguiente mandato: **restoreEKM21.bat** **Linux** a. Vaya al directorio <*SKLM_INSTALL_HOME*>/migration/utilities/ekm21. b. Compruebe si el archivo restoreEKM21.sh tiene permisos ejecutables. En caso de que no, otorgue permisos ejecutando el siguiente mandato: chmod 755 restoreEKM21.sh c. Ejecute el siguiente mandato: **restoreEKM21.sh**

Qué hacer a continuación

Nota: After data restoration, ensure that the path for the properties in the `SKLMConfig.properties`, `datastore.properties`, and `ReplicationSKLMConfig.properties` files are correct before you proceed with your next task.

Copia de seguridad de los datos de IBM Security Key Lifecycle Manager, Versión 2.5

Utilice el programa de utilidad de copia de seguridad de IBM Security Key Lifecycle Manager, Versión 3.0.1 para crear archivos de copia de seguridad de IBM Security Key Lifecycle Manager, Versión 2.5 entre plataformas.

Antes de empezar

Debe instalar IBM Security Key Lifecycle Manager, Versión 3.0.1 en un sistema.Asegúrese de que esté disponible el sistema con IBM Security Key Lifecycle Manager, versión 2.5 y el último fixpack 3.

Acerca de esta tarea

Puede utilizar el programa de utilidad de copia de seguridad para crear archivos de copia de seguridad entre plataformas, de modo independiente a los sistemas operativos y la estructura de directorios del servidor. Puede restaurar estos archivos de copia seguridad, compatibles entre plataformas, en un sistema con IBM Security Key Lifecycle Manager, Versión 3.0.1 en diferentes sistemas operativos.

Nota: For greater security, change the IBM Security Key Lifecycle Manager User password soon after the data migration process.

Procedimiento

Ejecute los pasos siguientes en los sistemas donde estén instalados IBM Security Key Lifecycle Manager versión 3.0.1 y versión 2.5.

IBM Security Key Lifecycle Manager, Versión3.0.1	1. Inicie sesión en el sistema con sus credenciales de usuario. 2. Localice la carpeta utilities de copia de seguridad. **Windows** `<SKLM_INSTALL_HOME>\migration\utilities\sklmv25` La ubicación predeterminada es `C:\Program Files\IBM\.SKLMV301\migration\utilities\sklmv25` **Linux** `<SKLM_INSTALL_HOME>/migration/utilities/sklmv25` La ubicación predeterminada es `/opt/IBM/SKLMV301/migration/utilities/sklmv25`.

IBM Security Key Lifecycle Manager, Versión 2.5	1. Inicie sesión en el sistema con sus credenciales de usuario.
	2. Copie la carpeta `sklmv25` desde el sistema en el que está instalado IBM Security Key Lifecycle Manager, Versión 3.0.1 al directorio local que desee.
	3. Edite `backup.properties` en la carpeta `sklmv25` para configurar las propiedades, como se muestra en el ejemplo siguiente. Debe establecer valores para todas las propiedades, excepto para la propiedad `BACKUP_DIR` (opcional).
	Si no especifica el valor para `BACKUP_DIR`, el archivo de copia de seguridad se crea en la subcarpeta `backup` en el mismo directorio desde donde se ejecuta la utilidad de copia de seguridad.
	Nota: On Windows operating system, the `backup.properties` file that you use for backup operations must not contain the property keys and values with leading or trailing spaces.
	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`
	Nota: En el sistema operativo de Windows, cuando especifique la vía de acceso en el archivo de propiedades, utilice "/ " o "\\ " como separador de vías de acceso, como se muestra en el ejemplo siguiente.
	`C:\\sklmv25_backup`
	O
	`C:/sklmv25_backup`
	4. Abra una ventana del indicador de mandatos y ejecute el programa de utilidad de copia de seguridad.
	Windows
	Vaya al directorio `sklmv25` (consulte el paso b) y ejecute el mandato siguiente:
	`backupV25.bat`
	Linux
	a. Vaya al directorio `sklmv25` (consulte el paso b).
	b. Compruebe si el archivo `backupV25.sh` tiene permisos ejecutables. En caso de que no, otorgue permisos ejecutando el siguiente mandato:
	`chmod 755 backupV25.sh`
	c. Ejecute el programa de utilidad de copia de seguridad:
	`backupV25.sh`

Qué hacer a continuación

- Review the directory that contains backup files to ensure that the backup file exists. The backup files are created in the location that you specified for `BACKUP_DIR` in the `backup.properties` file.

- Check the `backup.log` file for errors or exceptions. The `backup.log` file is created in the same directory where you run the backup utility. For a successful backup operation, ensure that there are no errors or exceptions in the log file.
- Retain the backup password for future use in case you restore the backup.
- Do not edit a file in the backup archive. The file that you attempt to edit becomes unreadable.

Restauración de los archivos de copia de seguridad de IBM Security Key Lifecycle Manager, Versión 2.5

Puede restaurar los archivos de copia de seguridad entre plataformas de IBM Security Key Lifecycle Manager Versión 2.5 en un sistema con IBM Security Key Lifecycle Manager, Versión 3.0.1 utilizando la interfaz gráfica de usuario, la interfaz de línea de mandatos, la interfaz REST o el script de restauración de migración.

Antes de empezar

Instale IBM Security Key Lifecycle Manager, Versión 3.0.1 en un sistema. Debe tener el archivo de copia de seguridad de la versión anterior y asegurarse de que tiene la contraseña que se ha utilizado al crear el archivo de copia de seguridad.

Nota: Debe tener el rol de usuario de IBM Security Key Lifecycle Manager para ejecutar operaciones de copia de seguridad y restauración.

Acerca de esta tarea

Puede restaurar archivos de copia de seguridad compatibles entre plataformas de IBM Security Key Lifecycle Manager, Versión 2.5 en un sistema con IBM Security Key Lifecycle Manager, Versión 3.0.1 en diferentes sistemas operativos.

Before you start a restore task, isolate the system for maintenance. Take a backup of the existing system. You can later use this backup to bring the system back to original state if any issues occur during the restore process. IBM Security Key Lifecycle Manager server automatically restarts after the restore process is complete. Verify the environment before you bring the IBM Security Key Lifecycle Manager server back into production.

Nota: For greater security, change the IBM Security Key Lifecycle Manager User password soon after the data migration process.

Procedimiento

1. Inicie sesión en el sistema en el que está instalado IBM Security Key Lifecycle Manager Versión 3.0.1.
2. Copie el archivo de copia de seguridad desde el sistema de versión 2.5 a una carpeta de su elección bajo el directorio <*SKLM_DATA*>, por ejemplo, `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data\sklm_v2.5.0.3_20170429013250-0400_migration_backup.jar`. Para ver la definición de <*SKLM_DATA*>, consulte Definiciones para *HOME* y otras variables de directorio.
3. Restaure el archivo de copia de seguridad utilizando cualquiera de los métodos siguientes.

Interfaz gráfica de usuario	1. Inicie sesión en la interfaz gráfica de usuario como usuario autorizado, por ejemplo, SKLMAdmin. 2. En la página de Bienvenida, pulse **Administración** > **Copia de seguridad y restauración**. 3. Pulse **Examinar** para especificar la ubicación del archivo de copia de seguridad de la versión 2.5 bajo el directorio <*SKLM_DATA*>. 4. Pulse **Visualizar copias de seguridad** para visualizar los archivos de copia de seguridad que desea restaurar. 5. En la tabla **Copia de seguridad y restauración**, seleccione un archivo de copia de seguridad. 6. Pulse **Restaurar desde copia de seguridad**. 7. En la página Restaurar copia de seguridad, especifique la contraseña de copia de seguridad que se ha utilizado para crear el archivo de copia de seguridad. 8. Pulse **Restaurar copia de seguridad**. 9. Reinicie el servidor de IBM Security Key Lifecycle Manager. **Nota:** Si utiliza la interfaz gráfica de usuario, no puede restaurar los roles, usuarios y grupos desde la copia de seguridad de IBM Security Key Lifecycle Manager Versión 2.5.

Interfaz de línea de mandatos	1. Vaya al directorio <*WAS_HOME*>/bin. Por ejemplo,
	Windows
	`cd unidad:\Program Files\IBM\WebSphere\AppServer\bin`
	Linux `cd /opt/IBM/WebSphere/AppServer/bin`
	2. Inicie la interfaz **wsadmin** utilizando un ID de usuario autorizado, por ejemplo, SKLMAdmin. Por ejemplo,
	Windows
	`wsadmin.bat -username SKLMAdmin -password mypwd -lang jython`
	Linux
	`./wsadmin.sh -username SKLMAdmin -password mypwd -lang jython`
	3. Ejecute el mandato de CLI **tklmBackupRunRestore** especificando los parámetros, por ejemplo, el nombre del archivo de copia de seguridad con su vía de acceso completa y la contraseña de copia de seguridad que ha utilizado para crear la copia de seguridad, como se muestra en el ejemplo siguiente.
	`print AdminTask.tklmBackupRunRestore ('[-backupFilePath <SKLM_DATA>/sklm_v2.5.0.3_20170429013250-0400_migration -password myBackupPwd]')`
	4. Reinicie el servidor de IBM Security Key Lifecycle Manager.
	Nota: Si utiliza la interfaz de línea de mandatos, no puede restaurar los roles, usuarios y grupos desde la copia de seguridad de IBM Security Key Lifecycle Manager Versión 2.5.

Interfaz REST	1. Abra un cliente REST.
	2. Obtenga un identificador de autenticación de usuario exclusivo para acceder a los servicios REST de IBM Security Key Lifecycle Manager. Para obtener más información sobre el proceso de autenticación, consulte Proceso de autenticación de los servicios REST.
	3. Para invocar el **Servicio REST Ejecutar restauración de copia de seguridad**, envíe la solicitud HTTP POST con el nombre de archivo de copia de seguridad y la vía de acceso completa y la contraseña de copia de seguridad como parámetros. Pase el identificador de autenticación de usuario que ha obtenido en el `Paso b` junto con el mensaje de solicitud, como se muestra en el ejemplo siguiente.
	`POST https://localhost:<puerto>/SKLM/rest/v1/ckms/restore`
	`Content-Type: application/json`
	`Accept: application/json`
	`Authorization: SKLMAuth authId=139aeh34567m`
	`Accept-Language: en`
	`{"backupFilePath":"<SKLM_DATA>/sklm_v2.5.0.3_20170429013250-0400_migration_bac`
	`"password":"myBackupPwd"}`
	4. Reinicie el servidor de IBM Security Key Lifecycle Manager.
	Nota: Si utiliza la interfaz REST, no puede restaurar los roles, usuarios y grupos desde la copia de seguridad de IBM Security Key Lifecycle Manager Versión 2.5.

Script de restauración de migración	1. Localice los programas de utilidad de IBM Security Key Lifecycle Manager. **Windows** <*SKLM_INSTALL_HOME*>\migration\utilities\sklmv25 La ubicación predeterminada es C:\Program Files\IBM\SKLMV301\migration\utilities\sklmv25. **Linux** <*SKLM_INSTALL_HOME*>/migration/utilities/sklmv25 La ubicación predeterminada es /opt/IBM/SKLMV301/migration/utilities/sklmv25. 2. Edite restore.properties en la carpeta sklmv25 para configurar las propiedades, como se muestra en el ejemplo siguiente. **Nota:** On Windows operating system, the restore.properties file that you use for restore operations must not contain the property keys and values with leading or trailing spaces. **Windows** WAS_HOME=C:\\Program Files\\IBM\\WebSphere\\AppServer JAVA_HOME=C:\\Program Files\\IBM\\WebSphere\\AppServer\\java\8.0 BACKUP_PASSWORD=passw0rd123 DB_PASSWORD=db2_password RESTORE_FILE=<*SKLM_DATA*>\\sklm_v2.5.0.3_20170429013250-0400_migratio WAS_USER_PWD=wasadmin_password RESTORE_USER_ROLES=y #pkcs11_config=C:\\luna.cfg **Linux** WAS_HOME=/opt/IBM/WebSphere/AppServer JAVA_HOME=/opt/IBM/WebSphere/AppServer/java/8.0 BACKUP_PASSWORD=passw0rd123 DB_PASSWORD=db2_password RESTORE_FILE=<*SKLM_DATA*>/sklm_v2.5.0.3_20170429013250-0400_migration WAS_USER_PWD=wasadmin_password RESTORE_USER_ROLES=y #pkcs11_config=/luna.cfg **Nota:** • Para iniciar una sesión en IBM Security Key Lifecycle Manager mediante la utilización de las credenciales especificadas durante la instalación del producto, establezca la propiedad **RESTORE_USER_ROLES** como “n”. Cuando la propiedad se establece en “n” se asegura que el ID de usuario y la contraseña no se sobrescriben con las credenciales de usuario de la versión antigua. • Si IBM Security Key Lifecycle Manager está configurado con HSM, elimine los comentarios de la propiedad **#pkcs11_config** y especifique la vía de acceso correcta del archivo luna.cfg como el valor. • En el sistema operativo de Windows, cuando especifique la vía de acceso en el archivo de propiedades, utilice “/ ” o “\\ ” como separador de vías de acceso, como se muestra en el ejemplo siguiente. C:\\sklmv25_restore O C:/sklmv25_restore 3. Abra una ventana del indicador de mandatos y especifique estos mandatos. **Windows** Vaya al directorio <*SKLM_INSTALL_HOME*>\migration\utilities\sklmv25 y ejecuta el siguiente mandato: **restoreV25.bat** **Linux** a. Vaya al directorio <*SKLM_INSTALL_HOME*>/migration/

Nota: Si desea configurar un clúster multimaestro en el servidor de IBM Security Key Lifecycle Manager restaurado, en el archivo `SKLMConfig.properties`, actualice la propiedad **`enableClientCertPush`** del siguiente modo:

```
enableClientCertPush=true
```

Puede utilizar Servicio REST Actualizar propiedad de configuración o el mandato de CLI de tklmConfigUpdateEntry para actualizar la propiedad.

A continuación, reinicie el servidor de IBM Security Key Lifecycle Manager.

Qué hacer a continuación

Nota: After data restoration, ensure that the path for the properties in the `SKLMConfig.properties`, `datastore.properties`, and `ReplicationSKLMConfig.properties` files are correct before you proceed with your next task.

Rollovers that are configured for LTO key groups and 3592 certificates are not automatically restored from the earlier versions of IBM Security Key Lifecycle Manager. You must manually set the rollover for certificates and key groups.

Para obtener más información, consulte Restauración de certificados de aplazamiento y grupos de claves.

Copia de seguridad de los datos de IBM Security Key Lifecycle Manager, Versión 2.6

Utilice el programa de utilidad de copia de seguridad de IBM Security Key Lifecycle Manager, Versión 3.0.1 para crear archivos de copia de seguridad de IBM Security Key Lifecycle Manager, Versión 2.6 entre plataformas.

Antes de empezar

Debe instalar IBM Security Key Lifecycle Manager, Versión 3.0.1 en un sistema.Asegúrese de que esté disponible el sistema con IBM Security Key Lifecycle Manager, versión 2.6 y el último fixpack 2.

Acerca de esta tarea

Puede utilizar el programa de utilidad de copia de seguridad para crear archivos de copia de seguridad entre plataformas, de modo independiente a los sistemas operativos y la estructura de directorios del servidor. Puede restaurar estos archivos de copia seguridad, compatibles entre plataformas, en un sistema con IBM Security Key Lifecycle Manager, Versión 3.0.1 en diferentes sistemas operativos.

Nota: For greater security, change the IBM Security Key Lifecycle Manager User password soon after the data migration process.

Procedimiento

Ejecute los pasos siguientes en los sistemas donde estén instalados IBM Security Key Lifecycle Manager versión 3.0.1 y versión 2.6.

IBM Security Key Lifecycle Manager, Versión3.0.1	1. Inicie sesión en el sistema con sus credenciales de usuario. 2. Localice la carpeta utilities de copia de seguridad. **Windows** <*SKLM_INSTALL_HOME*>\migration\utilities\sklmv26 La ubicación predeterminada es C:\Program Files\IBM\SKLMV301\migration\utilities\sklmv26. **Linux** <*SKLM_INSTALL_HOME*>/migration/utilities/sklmv26 La ubicación predeterminada es /opt/IBM/SKLMV301/migration/utilities/sklmv26.

IBM Security Key Lifecycle Manager, Versión 2.6	1. Inicie sesión en el sistema con sus credenciales de usuario.
	2. Copie la carpeta `sklmv26` desde el sistema en el que está instalado IBM Security Key Lifecycle Manager, Versión 3.0.1 al directorio local que desee.
	3. Edite `backup.properties` en la carpeta `sklmv26` para configurar las propiedades, como se muestra en el ejemplo siguiente. Debe establecer valores para todas las propiedades, excepto para la propiedad `BACKUP_DIR` (opcional).
	Si no especifica el valor para `BACKUP_DIR`, el archivo de copia de seguridad se crea en la subcarpeta `backup` en el mismo directorio desde donde se ejecuta la utilidad de copia de seguridad.
	Nota: On Windows operating system, the `backup.properties` file that you use for backup operations must not contain the property keys and values with leading or trailing spaces.
	Windows
	`WAS_HOME=C:\\Program Files (x86)\\IBM\\WebSphere\\AppServer`
	`BACKUP_PASSWORD=passw0rd123`
	`DB_PASSWORD=sklmdb2`
	`WAS_USER_PWD=wasadmin`
	`BACKUP_DIR=C:\\sklmv26_backup`
	Linux
	`WAS_HOME=/opt/IBM/WebSphere/AppServer`
	`BACKUP_PASSWORD=passw0rd123`
	`DB_PASSWORD=sklmdb2`
	`WAS_USER_PWD=wasadmin`
	`BACKUP_DIR=/sklmv26_backup`
	Nota: En el sistema operativo de Windows, cuando especifique la vía de acceso en el archivo de propiedades, utilice "/ " o "\\ " como separador de vías de acceso, como se muestra en el ejemplo siguiente.
	`C:\\sklmv26_backup`
	O
	`C:/sklmv26_backup`
	4. Abra una ventana del indicador de mandatos y ejecute el programa de utilidad de copia de seguridad.
	Windows
	Vaya al directorio `sklmv26` (consulte el paso b) y ejecute el mandato siguiente:
	`backupV26.bat`
	Linux
	a. Vaya al directorio `sklmv26` (consulte el paso b).
	b. Compruebe si el archivo `backupV26.sh` tiene permisos ejecutables. En caso de que no, otorgue permisos ejecutando el siguiente mandato:
	`chmod 755 backupV26.sh`
	c. Ejecute el programa de utilidad de copia de seguridad:
	`backupV26.sh`

Qué hacer a continuación

- Review the directory that contains backup files to ensure that the backup file exists. The backup files are created in the location that you specified for `BACKUP_DIR` in the `backup.properties` file.

- Check the `backup.log` file for errors or exceptions. The `backup.log` file is created in the same directory where you run the backup utility. For a successful backup operation, ensure that there are no errors or exceptions in the log file.
- Retain the backup password for future use in case you restore the backup.
- Do not edit a file in the backup archive. The file that you attempt to edit becomes unreadable.

Restauración de los archivos de copia de seguridad de IBM Security Key Lifecycle Manager, Versión 2.6

Puede restaurar los archivos de copia de seguridad entre plataformas de IBM Security Key Lifecycle Manager Versión 2.6 en un sistema con IBM Security Key Lifecycle Manager, Versión 3.0.1 utilizando la interfaz gráfica de usuario, la interfaz de línea de mandatos, la interfaz REST o el script de restauración de migración.

Antes de empezar

Instale IBM Security Key Lifecycle Manager, Versión 3.0.1 en un sistema. Debe tener el archivo de copia de seguridad de la versión anterior y asegurarse de que tiene la contraseña que se ha utilizado al crear el archivo de copia de seguridad.

Nota: Debe tener el rol de usuario de IBM Security Key Lifecycle Manager para ejecutar operaciones de copia de seguridad y restauración.

Acerca de esta tarea

Puede restaurar archivos de copia de seguridad compatibles entre plataformas de IBM Security Key Lifecycle Manager, Versión 2.6 en un sistema con IBM Security Key Lifecycle Manager, Versión 3.0.1 en diferentes sistemas operativos.

Before you start a restore task, isolate the system for maintenance. Take a backup of the existing system. You can later use this backup to bring the system back to original state if any issues occur during the restore process. IBM Security Key Lifecycle Manager server automatically restarts after the restore process is complete. Verify the environment before you bring the IBM Security Key Lifecycle Manager server back into production.

Nota: For greater security, change the IBM Security Key Lifecycle Manager User password soon after the data migration process.

Procedimiento

1. Inicie sesión en el sistema en el que está instalado IBM Security Key Lifecycle Manager, Versión 3.0.1.
2. Copie el archivo de copia de seguridad desde el sistema de versión 2.6 a una carpeta de su elección bajo el directorio <*SKLM_DATA*>, por ejemplo, `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data\sklm_v2.6.0.2_20170429013250-0400_migration_backup.jar`. Para ver la definición de <*SKLM_DATA*>, consulte Definiciones para *HOME* y otras variables de directorio.
3. Restaure el archivo de copia de seguridad utilizando cualquiera de los métodos siguientes.

Interfaz gráfica de usuario	1. Inicie sesión en la interfaz gráfica de usuario como usuario autorizado, por ejemplo, SKLMAdmin. 2. En la página de Bienvenida, pulse **Administración** > **Copia de seguridad y restauración**. 3. Pulse **Examinar** para especificar la ubicación del archivo de copia de seguridad de la versión 2.6 bajo el directorio <*SKLM_DATA*>. 4. Pulse **Visualizar copias de seguridad** para visualizar los archivos de copia de seguridad que desea restaurar. 5. En la tabla **Copia de seguridad y restauración**, seleccione un archivo de copia de seguridad. 6. Pulse **Restaurar desde copia de seguridad**. 7. En la página Restaurar copia de seguridad, especifique la contraseña de copia de seguridad que se ha utilizado para crear el archivo de copia de seguridad. 8. Pulse **Restaurar copia de seguridad**. 9. Reinicie el servidor de IBM Security Key Lifecycle Manager. **Nota:** Si utiliza la interfaz gráfica de usuario, no puede restaurar los roles, usuarios y grupos desde la copia de seguridad de IBM Security Key Lifecycle Manager Versión 2.6.

Interfaz de línea de mandatos	1. Vaya al directorio *WAS_HOME*/bin. Por ejemplo,
	Windows
	`cd unidad:\Program Files\IBM\WebSphere\AppServer\bin`
	Linux `cd /opt/IBM/WebSphere/AppServer/bin`
	2. Inicie la interfaz **wsadmin** utilizando un ID de usuario autorizado, por ejemplo, SKLMAdmin. Por ejemplo,
	Windows
	`wsadmin.bat -username SKLMAdmin -password mypwd -lang jython`
	Linux
	`./wsadmin.sh -username SKLMAdmin -password mypwd -lang jython`
	3. Ejecute el mandato de CLI **tklmBackupRunRestore** especificando los parámetros, por ejemplo, el nombre del archivo de copia de seguridad con su vía de acceso completa y la contraseña de copia de seguridad que ha utilizado para crear la copia de seguridad, como se muestra en el ejemplo siguiente.
	`print AdminTask.tklmBackupRunRestore ('[-backupFilePath <SKLM_DATA>/sklm_v2.6.0.2_20170429013250-0400_migration_ba -password myBackupPwd]')`
	4. Reinicie el servidor de IBM Security Key Lifecycle Manager.
	Nota: Si utiliza la interfaz de línea de mandatos, no puede restaurar los roles, usuarios y grupos desde la copia de seguridad de IBM Security Key Lifecycle Manager Versión 2.6.

Interfaz REST	1. Abra un cliente REST.
	2. Obtenga un identificador de autenticación de usuario exclusivo para acceder a los servicios REST de IBM Security Key Lifecycle Manager. Para obtener más información sobre el proceso de autenticación, consulte Proceso de autenticación de los servicios REST.
	3. Para invocar el **Servicio REST Ejecutar restauración de copia de seguridad**, envíe la solicitud HTTP POST con el nombre de archivo de copia de seguridad y la vía de acceso completa y la contraseña de copia de seguridad como parámetros. Pase el identificador de autenticación de usuario que ha obtenido en el `Paso b` junto con el mensaje de solicitud, como se muestra en el ejemplo siguiente.
	`POST https://localhost:<puerto>/SKLM/rest/v1/ckms/restore`
	`Content-Type: application/json`
	`Accept: application/json`
	`Authorization: SKLMAuth authId=139aeh34567m`
	`Accept-Language: en`
	`{"backupFilePath":"<SKLM_DATA>/sklm_v2.6.0.2_20170429013250-0400_migration_b`
	`"password":"myBackupPwd"}`
	4. Reinicie el servidor de IBM Security Key Lifecycle Manager.
	Nota: Si utiliza la interfaz REST, no puede restaurar los roles, usuarios y grupos desde la copia de seguridad de IBM Security Key Lifecycle Manager Versión 2.6.

Script de restauración de migración	1. Localice los programas de utilidad de IBM Security Key Lifecycle Manager. **Windows** <*SKLM_INSTALL_HOME*>\migration\utilities\sklmv26 La ubicación predeterminada es C:\Program Files\IBM\SKLMV301\migration\utilities\sklmv26. **Linux** <*SKLM_INSTALL_HOME*>/migration/utilities/sklmv26 La ubicación predeterminada es /opt/IBM/SKLMV301/migration/utilities/sklmv26. 2. Edite restore.properties en la carpeta sklmv26 para configurar las propiedades, como se muestra en el ejemplo siguiente. **Nota:** On Windows operating system, the restore.properties file that you use for restore operations must not contain the property keys and values with leading or trailing spaces. **Windows** WAS_HOME=C:\\Program Files\\IBM\\WebSphere\\AppServer JAVA_HOME=C:\\Program Files\\IBM\\WebSphere\\AppServer\\java\8.0 BACKUP_PASSWORD=passw0rd123 DB_PASSWORD=db2_password RESTORE_FILE=<*SKLM_DATA*>\\sklm_v2.6.0.2_20170429013250-0400_migration_ WAS_USER_PWD=wasadmin_password RESTORE_USER_ROLES=y #pkcs11_config=C:\\luna.cfg **Linux** WAS_HOME=/opt/IBM/WebSphere/AppServer JAVA_HOME=/opt/IBM/WebSphere/AppServer/java/8.0 BACKUP_PASSWORD=passw0rd123 DB_PASSWORD=db2_password RESTORE_FILE=<*SKLM_DATA*>/sklm_v2.6.0.2_20170429013250-0400_migration_b WAS_USER_PWD=wasadmin_password RESTORE_USER_ROLES=y #pkcs11_config=/luna.cfg **Nota:** • Para iniciar una sesión en IBM Security Key Lifecycle Manager mediante la utilización de las credenciales especificadas durante la instalación del producto, establezca la propiedad **RESTORE_USER_ROLES** como “n”. Cuando la propiedad se establece en “n” se asegura que el ID de usuario y la contraseña no se sobrescriben con las credenciales de usuario de la versión antigua. RESTORE_USER_ROLES=n • Si IBM Security Key Lifecycle Manager está configurado con HSM, elimine los comentarios de la propiedad **#pkcs11_config** y especifique la vía de acceso correcta del archivo luna.cfg como el valor. • En el sistema operativo de Windows, cuando especifique la vía de acceso en el archivo de propiedades, utilice “/ ” o “\\ ” como separador de vías de acceso, como se muestra en el ejemplo siguiente. C:\\sklmv26_restore O C:/sklmv26_restore 3. Abra una ventana del indicador de mandatos y especifique estos mandatos. **Windows** Vaya al directorio <*SKLM_INSTALL_HOME*>\migration\utilities\sklmv26 y ejecuta el siguiente mandato: **restoreV26.bat** **Linux**

Qué hacer a continuación

Nota: After data restoration, ensure that the path for the properties in the `SKLMConfig.properties`, `datastore.properties`, and `ReplicationSKLMConfig.properties` files are correct before you proceed with your next task.

Rollovers that are configured for LTO key groups and 3592 certificates are not automatically restored from the earlier versions of IBM Security Key Lifecycle Manager. You must manually set the rollover for certificates and key groups.

Para obtener más información, consulte "Restauración de grupos de claves y certificados de aplazamiento" en la página 173.

Copia de seguridad de los datos de IBM Security Key Lifecycle Manager, Versión 2.7

Utilice el programa de utilidad de copia de seguridad de IBM Security Key Lifecycle Manager, Versión 3.0.1 para crear archivos de copia de seguridad de IBM Security Key Lifecycle Manager, Versión 2.7 entre plataformas.

Antes de empezar

Debe instalar IBM Security Key Lifecycle Manager, Versión 3.0.1 en un sistema.Asegúrese de que esté disponible el sistema con IBM Security Key Lifecycle Manager, Versión 2.7 General Availability (GA).

Acerca de esta tarea

Puede utilizar el programa de utilidad de copia de seguridad para crear archivos de copia de seguridad entre plataformas, de modo independiente a los sistemas operativos y la estructura de directorios del servidor. Puede restaurar estos archivos de copia seguridad, compatibles entre plataformas, en un sistema con IBM Security Key Lifecycle Manager, Versión 3.0.1 en diferentes sistemas operativos.

Nota: For greater security, change the IBM Security Key Lifecycle Manager User password soon after the data migration process.

Procedimiento

Ejecute los pasos siguientes en los sistemas donde estén instalados IBM Security Key Lifecycle Manager versión 3.0.1 y versión 2.7.

IBM Security Key Lifecycle Manager, Versión3.0.1	1. Inicie sesión en el sistema con sus credenciales de usuario. 2. Localice la carpeta utilities de copia de seguridad. **Windows** `<SKLM_INSTALL_HOME>\migration\utilities\sklmv27` La ubicación predeterminada es `C:\Program Files\IBM\SKLMV301\migration\utilities\sklmv27`. **Linux** `<SKLM_INSTALL_HOME>/migration/utilities/sklmv27` La ubicación predeterminada es `/opt/IBM/SKLMV301/migration/utilities/sklmv27`.

IBM Security Key Lifecycle Manager, Versión 2.7	1. Inicie sesión en el sistema con sus credenciales de usuario.
	2. Copie la carpeta `sklmv27` desde el sistema en el que está instalado IBM Security Key Lifecycle Manager, Versión 3.0.1 al directorio local que desee.
	3. Edite `backup.properties` en la carpeta `sklmv27` para configurar las propiedades, como se muestra en el ejemplo siguiente. Debe establecer valores para todas las propiedades, excepto para la propiedad `BACKUP_DIR` (opcional).
	Si no especifica el valor para `BACKUP_DIR`, el archivo de copia de seguridad se crea en la subcarpeta `backup` en el mismo directorio desde donde se ejecuta la utilidad de copia de seguridad.
	Nota: On Windows operating system, the `backup.properties` file that you use for backup operations must not contain the property keys and values with leading or trailing spaces.
	Windows
	`WAS_HOME=C:\\Program Files\\IBM\\WebSphere\\AppServer`
	`JAVA_HOME=C:\\Program Files\\IBM\\WebSphere\\AppServer\\java\\8.0 (obli`
	`BACKUP_PASSWORD=passw0rd123`
	`DB_PASSWORD=sklmdb2`
	`WAS_USER_PWD=wasadmin`
	`MIGRATE_INSTANCE_ID=NO (opcional)`
	Linux
	`WAS_HOME=/opt/IBM/WebSphere/AppServer`
	`JAVA_HOME=/opt/IBM/WebSphere/AppServer/java/8.0`
	`BACKUP_PASSWORD=passw0rd123`
	`DB_PASSWORD=sklmdb2`
	`WAS_USER_PWD=wasadmin`
	`MIGRATE_INSTANCE_ID=NO (opcional)`
	Especifique `MIGRATE_INSTANCE_ID=YES` para migrar el ID de la instancia de IBM Security Key Lifecycle Manager. Si no especifica esta propiedad, el ID de la instancia no se migra a IBM Security Key Lifecycle Manager, Versión 3.0.1.
	Nota: En el sistema operativo de Windows, cuando especifique la vía de acceso en el archivo de propiedades, utilice "/ " o "\\ " como separador de vías de acceso, como se muestra en el ejemplo siguiente.
	`C:\\sklmv27_backup`
	O
	`C:/sklmv27_backup`
	4. Abra una ventana del indicador de mandatos y ejecute el programa de utilidad de copia de seguridad.
	Windows
	Vaya al directorio `sklmv27` (consulte el paso b) y ejecute el mandato siguiente:
	`backupV27.bat`
	Linux
	a. Vaya al directorio `sklmv27` (consulte el paso b).
	b. Compruebe si el archivo `backupV27.sh` tiene permisos ejecutables. En caso de que no, otorgue permisos ejecutando el siguiente mandato:
	`chmod 755 backupV27.sh`
	c. Ejecute el programa de utilidad de copia de seguridad:
	`backupV27.sh`

Qué hacer a continuación

- Review the directory that contains backup files to ensure that the backup file exists. The backup files are created in the location that you specified for `BACKUP_DIR` in the `backup.properties` file.
- Check the `backup.log` file for errors or exceptions. The `backup.log` file is created in the same directory where you run the backup utility. For a successful backup operation, ensure that there are no errors or exceptions in the log file.
- Retain the backup password for future use in case you restore the backup.
- Do not edit a file in the backup archive. The file that you attempt to edit becomes unreadable.

Restauración de los archivos de copia de seguridad de IBM Security Key Lifecycle Manager, Versión 2.7

Puede restaurar los archivos de copia de seguridad entre plataformas de IBM Security Key Lifecycle Manager Versión 2.7 en un sistema con IBM Security Key Lifecycle Manager, Versión 3.0.1 utilizando la interfaz gráfica de usuario, la interfaz de línea de mandatos, la interfaz REST o el script de restauración de migración.

Antes de empezar

Instale IBM Security Key Lifecycle Manager, Versión 3.0.1 en un sistema. Debe tener el archivo de copia de seguridad de la versión anterior y asegurarse de que tiene la contraseña que se ha utilizado al crear el archivo de copia de seguridad.

Nota: Debe tener el rol de usuario de IBM Security Key Lifecycle Manager para ejecutar operaciones de copia de seguridad y restauración.

Acerca de esta tarea

Puede restaurar archivos de copia de seguridad compatibles entre plataformas de IBM Security Key Lifecycle Manager, Versión 2.7 en un sistema con IBM Security Key Lifecycle Manager, Versión 3.0.1 en diferentes sistemas operativos.

Before you start a restore task, isolate the system for maintenance. Take a backup of the existing system. You can later use this backup to bring the system back to original state if any issues occur during the restore process. IBM Security Key Lifecycle Manager server automatically restarts after the restore process is complete. Verify the environment before you bring the IBM Security Key Lifecycle Manager server back into production.

Nota: For greater security, change the IBM Security Key Lifecycle Manager User password soon after the data migration process.

Procedimiento

1. Inicie sesión en el sistema en el que está instalado IBM Security Key Lifecycle Manager, Versión 3.0.1.
2. Copie el archivo de copia de seguridad desde el sistema de versión 2.7 a una carpeta de su elección bajo el directorio <*SKLM_DATA*>, por ejemplo, `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data\sklm_v2.7.0.0_20170429013250-0400_migration_backup.jar`. Para ver la definición de <*SKLM_DATA*>, consulte Definiciones para *HOME* y otras variables de directorio.
3. Restaure el archivo de copia de seguridad utilizando cualquiera de los métodos siguientes.

Interfaz gráfica de usuario	1. Inicie sesión en la interfaz gráfica de usuario como usuario autorizado, por ejemplo, SKLMAdmin. 2. En la página de Bienvenida, pulse **Administración** > **Copia de seguridad y restauración**. 3. Pulse **Examinar** para especificar la ubicación del archivo de copia de seguridad de la versión 2.7 bajo el directorio <*SKLM_DATA*>. 4. Pulse **Visualizar copias de seguridad** para visualizar los archivos de copia de seguridad que desea restaurar. 5. En la tabla **Copia de seguridad y restauración**, seleccione un archivo de copia de seguridad. 6. Pulse **Restaurar desde copia de seguridad**. 7. En la página Restaurar copia de seguridad, especifique la contraseña de copia de seguridad que se ha utilizado para crear el archivo de copia de seguridad. 8. Pulse **Restaurar copia de seguridad**. 9. Reinicie el servidor de IBM Security Key Lifecycle Manager. **Nota:** Si utiliza la interfaz gráfica de usuario, no puede restaurar los roles, usuarios y grupos desde la copia de seguridad de IBM Security Key Lifecycle Manager Versión 2.7.

Interfaz de línea de mandatos	1. Vaya al directorio *WAS_HOME*/bin. Por ejemplo,
	Windows
	`cd unidad:\Program Files\IBM\WebSphere\AppServer\bin`
	Linux `cd /opt/IBM/WebSphere/AppServer/bin`
	2. Inicie la interfaz **wsadmin** utilizando un ID de usuario autorizado, por ejemplo, SKLMAdmin. Por ejemplo,
	Windows
	`wsadmin.bat -username SKLMAdmin -password mypwd -lang jython`
	Linux
	`./wsadmin.sh -username SKLMAdmin -password mypwd -lang jython`
	3. Ejecute el mandato de CLI **tklmBackupRunRestore** especificando los parámetros, por ejemplo, el nombre del archivo de copia de seguridad con su vía de acceso completa y la contraseña de copia de seguridad que ha utilizado para crear la copia de seguridad, como se muestra en el ejemplo siguiente.
	`print AdminTask.tklmBackupRunRestore ('[-backupFilePath <SKLM_DATA>/sklm_v2.7.0.0_20170429013250-0400_migration_ba -password myBackupPwd]')`
	4. Reinicie el servidor de IBM Security Key Lifecycle Manager.
	Nota: Si utiliza la interfaz de línea de mandatos, no puede restaurar los roles, usuarios y grupos desde la copia de seguridad de IBM Security Key Lifecycle Manager Versión 2.7.

Interfaz REST	1. Abra un cliente REST.
	2. Obtenga un identificador de autenticación de usuario exclusivo para acceder a los servicios REST de IBM Security Key Lifecycle Manager. Para obtener más información sobre el proceso de autenticación, consulte Proceso de autenticación de los servicios REST.
	3. Para invocar el **Servicio REST Ejecutar restauración de copia de seguridad**, envíe la solicitud HTTP POST con el nombre de archivo de copia de seguridad y la vía de acceso completa y la contraseña de copia de seguridad como parámetros. Pase el identificador de autenticación de usuario que ha obtenido en el `Paso b` junto con el mensaje de solicitud, como se muestra en el ejemplo siguiente.
	`POST https://localhost:<puerto>/SKLM/rest/v1/ckms/restore`
	`Content-Type: application/json`
	`Accept: application/json`
	`Authorization: SKLMAuth authId=139aeh34567m`
	`Accept-Language: en`
	`{"backupFilePath":"<SKLM_DATA>/sklm_v2.7.0.0_20170429013250-0400_migration_b`
	`"password":"myBackupPwd"}`
	4. Reinicie el servidor de IBM Security Key Lifecycle Manager.
	Nota: Si utiliza la interfaz REST, no puede restaurar los roles, usuarios y grupos desde la copia de seguridad de IBM Security Key Lifecycle Manager Versión 2.7.

Script de restauración de migración	1. Localice los programas de utilidad de IBM Security Key Lifecycle Manager. **Windows** <*SKLM_INSTALL_HOME*>\migration\utilities\sklmv27 La ubicación predeterminada es C:\Program Files\IBM\SKLMV301\migration\utilities\sklmv27. **Linux** <*SKLM_INSTALL_HOME*>/migration/utilities/sklmv27 La ubicación predeterminada es /opt/IBM/SKLMV301/migration/utilities/sklmv27. 2. Edite restore.properties en la carpeta sklmv27 para configurar las propiedades, como se muestra en el ejemplo siguiente. **Nota:** On Windows operating system, the restore.properties file that you use for restore operations must not contain the property keys and values with leading or trailing spaces. **Windows** WAS_HOME=C:\\Program Files\\IBM\\WebSphere\\AppServer JAVA_HOME=C:\\Program Files\\IBM\\WebSphere\\AppServer\\java\8.0 BACKUP_PASSWORD=passw0rd123 DB_PASSWORD=db2_password RESTORE_FILE=<*SKLM_DATA*>\\sklm_v2.7.0.0_20170429013250-0400_migration_ WAS_USER_PWD=wasadmin_password RESTORE_USER_ROLES=y #pkcs11_config=C:\\luna.cfg **Linux** WAS_HOME=/opt/IBM/WebSphere/AppServer JAVA_HOME=/opt/IBM/WebSphere/AppServer/java/8.0 BACKUP_PASSWORD=passw0rd123 DB_PASSWORD=db2_password RESTORE_FILE=<*SKLM_DATA*>/sklm_v2.7.0.0_20170429013250-0400_migration_b WAS_USER_PWD=wasadmin_password RESTORE_USER_ROLES=y #pkcs11_config=/luna.cfg **Nota:** • Para iniciar una sesión en IBM Security Key Lifecycle Manager mediante la utilización de las credenciales especificadas durante la instalación del producto, establezca la propiedad **RESTORE_USER_ROLES** como “n”. Cuando la propiedad se establece en “n” se asegura que el ID de usuario y la contraseña no se sobrescriben con las credenciales de usuario de la versión antigua. RESTORE_USER_ROLES=n • Si IBM Security Key Lifecycle Manager está configurado con HSM, elimine los comentarios de la propiedad **#pkcs11_config** y especifique la vía de acceso correcta del archivo luna.cfg como el valor. • En el sistema operativo de Windows, cuando especifique la vía de acceso en el archivo de propiedades, utilice “/ ” o “\\ ” como separador de vías de acceso, como se muestra en el ejemplo siguiente. C:\\sklmv27_restore O C:/sklmv27_restore 3. Abra una ventana del indicador de mandatos y especifique estos mandatos. **Windows** Vaya al directorio <*SKLM_INSTALL_HOME*>\migration\utilities\sklmv27 y ejecute el siguiente mandato: **restoreV27.bat** **Linux**

Qué hacer a continuación

Nota: After data restoration, ensure that the path for the properties in the `SKLMConfig.properties`, `datastore.properties`, and `ReplicationSKLMConfig.properties` files are correct before you proceed with your next task.

Rollovers that are configured for LTO key groups and 3592 certificates are not automatically restored from the earlier versions of IBM Security Key Lifecycle Manager. You must manually set the rollover for certificates and key groups.

Para obtener más información, consulte "Restauración de grupos de claves y certificados de aplazamiento" en la página 173.

Copia de seguridad de los datos de IBM Security Key Lifecycle Manager, Versión 3.0

Utilice el programa de utilidad de copia de seguridad de IBM Security Key Lifecycle Manager, Versión 3.0.1 para crear archivos de copia de seguridad de IBM Security Key Lifecycle Manager, Versión 3.0 entre plataformas.

Antes de empezar

Debe instalar IBM Security Key Lifecycle Manager, Versión 3.0.1 en un sistema.Asegúrese de que esté disponible el sistema con IBM Security Key Lifecycle Manager, Versión 3.0 General Availability (GA).

Acerca de esta tarea

Puede utilizar el programa de utilidad de copia de seguridad para crear archivos de copia de seguridad entre plataformas, de modo independiente a los sistemas operativos y la estructura de directorios del servidor. Puede restaurar estos archivos de copia seguridad, compatibles entre plataformas, en un sistema con IBM Security Key Lifecycle Manager, Versión 3.0.1 en diferentes sistemas operativos.

Nota: For greater security, change the IBM Security Key Lifecycle Manager User password soon after the data migration process.

Procedimiento

Ejecute los pasos siguientes en los sistemas donde estén instalados IBM Security Key Lifecycle Manager versión 3.0.1 y versión 3.0.

IBM Security Key Lifecycle Manager, Versión 3.0.1	1. Inicie sesión en el sistema con sus credenciales de usuario. 2. Localice la carpeta utilities de copia de seguridad. **Windows** `<SKLM_INSTALL_HOME>\migration\utilities\sklmv30` La ubicación predeterminada es `C:\Program Files\IBM\SKLMV301\migration\utilities\sklmv30`. **Linux** `<SKLM_INSTALL_HOME>/migration/utilities/sklmv30` La ubicación predeterminada es `/opt/IBM/SKLMV301/migration/utilities/sklmv30`.

IBM Security Key Lifecycle Manager, Versión 3.0	1. Inicie sesión en el sistema con sus credenciales de usuario.
	2. Copie la carpeta `sklmv30` desde el sistema en el que está instalado IBM Security Key Lifecycle Manager, Versión 3.0.1 al directorio local que desee.
	3. Edite `backup.properties` en la carpeta `sklmv30` para configurar las propiedades, como se muestra en el ejemplo siguiente. Debe establecer valores para todas las propiedades, excepto para la propiedad `BACKUP_DIR` (opcional).
	Si no especifica el valor para `BACKUP_DIR`, el archivo de copia de seguridad se crea en la subcarpeta `backup` en el mismo directorio desde donde se ejecuta la utilidad de copia de seguridad.
	Nota: On Windows operating system, the `backup.properties` file that you use for backup operations must not contain the property keys and values with leading or trailing spaces.
	Windows
	`WAS_HOME=C:\\Program Files\\IBM\\WebSphere\\AppServer`
	`JAVA_HOME=C:\\Program Files\\IBM\\WebSphere\\AppServer\\java\\8.0 (obli`
	`BACKUP_PASSWORD=passw0rd123`
	`DB_PASSWORD=sklmdb2`
	`WAS_USER_PWD=wasadmin`
	`MIGRATE_INSTANCE_ID=NO (opcional)`
	Linux
	`WAS_HOME=/opt/IBM/WebSphere/AppServer`
	`JAVA_HOME=/opt/IBM/WebSphere/AppServer/java/8.0`
	`BACKUP_PASSWORD=passw0rd123`
	`DB_PASSWORD=sklmdb2`
	`WAS_USER_PWD=wasadmin`
	`MIGRATE_INSTANCE_ID=NO (opcional)`
	Especifique `MIGRATE_INSTANCE_ID=YES` para migrar el ID de la instancia de IBM Security Key Lifecycle Manager. Si no especifica esta propiedad, el ID de la instancia no se migra a IBM Security Key Lifecycle Manager, Versión 3.0.1.
	Nota: En el sistema operativo de Windows, cuando especifique la vía de acceso en el archivo de propiedades, utilice "/ " o "\\ " como separador de vías de acceso, como se muestra en el ejemplo siguiente.
	`C:\\sklmv30_backup`
	O
	`C:/sklmv30_backup`
	4. Abra una ventana del indicador de mandatos y ejecute el programa de utilidad de copia de seguridad.
	Windows
	Vaya al directorio `sklmv30` (consulte el paso b) y ejecute el mandato siguiente:
	`backupV30.bat`
	Linux
	a. Vaya al directorio `sklmv30` (consulte el paso b).
	b. Compruebe si el archivo `backupV30.sh` tiene permisos ejecutables. En caso de que no, otorgue permisos ejecutando el siguiente mandato:
	`chmod 755 backupV30.sh`
	c. Ejecute el programa de utilidad de copia de seguridad:
	`backupV30.sh`

Qué hacer a continuación

- Review the directory that contains backup files to ensure that the backup file exists. The backup files are created in the location that you specified for `BACKUP_DIR` in the `backup.properties` file.
- Check the `backup.log` file for errors or exceptions. The `backup.log` file is created in the same directory where you run the backup utility. For a successful backup operation, ensure that there are no errors or exceptions in the log file.
- Retain the backup password for future use in case you restore the backup.
- Do not edit a file in the backup archive. The file that you attempt to edit becomes unreadable.

Restauración de los archivos de copia de seguridad de IBM Security Key Lifecycle Manager, Versión 3.0

Puede restaurar los archivos de copia de seguridad entre plataformas de IBM Security Key Lifecycle Manager Versión 3.0 en un sistema con IBM Security Key Lifecycle Manager, Versión 3.0.1 utilizando la interfaz gráfica de usuario, la interfaz de línea de mandatos, la interfaz REST o el script de restauración de migración.

Antes de empezar

Instale IBM Security Key Lifecycle Manager, Versión 3.0.1 en un sistema. Debe tener el archivo de copia de seguridad de la versión anterior y asegurarse de que tiene la contraseña que se ha utilizado al crear el archivo de copia de seguridad.

Nota: Debe tener el rol de usuario de IBM Security Key Lifecycle Manager para ejecutar operaciones de copia de seguridad y restauración.

Acerca de esta tarea

Puede restaurar archivos de copia de seguridad compatibles entre plataformas de IBM Security Key Lifecycle Manager, Versión 3.0 en un sistema con IBM Security Key Lifecycle Manager, Versión 3.0.1 en diferentes sistemas operativos.

Before you start a restore task, isolate the system for maintenance. Take a backup of the existing system. You can later use this backup to bring the system back to original state if any issues occur during the restore process. IBM Security Key Lifecycle Manager server automatically restarts after the restore process is complete. Verify the environment before you bring the IBM Security Key Lifecycle Manager server back into production.

Nota: For greater security, change the IBM Security Key Lifecycle Manager User password soon after the data migration process.

Procedimiento

1. Inicie sesión en el sistema en el que está instalado IBM Security Key Lifecycle Manager, Versión 3.0.1.
2. Copie el archivo de copia de seguridad desde el sistema de versión 3.0 a una carpeta de su elección bajo el directorio <*SKLM_DATA*>, por ejemplo, `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data\sklm_v3.0.0.0_20170429013250-0400_migration_backup.jar`. Para ver la definición de <*SKLM_DATA*>, consulte Definiciones para *HOME* y otras variables de directorio.
3. Restaure el archivo de copia de seguridad utilizando cualquiera de los métodos siguientes.

Interfaz gráfica de usuario	1. Inicie sesión en la interfaz gráfica de usuario como usuario autorizado, por ejemplo, SKLMAdmin. 2. En la página de Bienvenida, pulse **Administración** > **Copia de seguridad y restauración**. 3. Pulse **Examinar** para especificar la ubicación del archivo de copia de seguridad de la versión 3.0 bajo el directorio <*SKLM_DATA*>. 4. Pulse **Visualizar copias de seguridad** para visualizar los archivos de copia de seguridad que desea restaurar. 5. En la tabla **Copia de seguridad y restauración**, seleccione un archivo de copia de seguridad. 6. Pulse **Restaurar desde copia de seguridad**. 7. En la página Restaurar copia de seguridad, especifique la contraseña de copia de seguridad que se ha utilizado para crear el archivo de copia de seguridad. 8. Pulse **Restaurar copia de seguridad**. 9. Reinicie el servidor de IBM Security Key Lifecycle Manager. **Nota:** Si utiliza la interfaz gráfica de usuario, no puede restaurar los roles, usuarios y grupos desde la copia de seguridad de IBM Security Key Lifecycle Manager Versión 3.0.

Interfaz de línea de mandatos	1. Vaya al directorio *WAS_HOME*/bin. Por ejemplo,
	Windows
	`cd unidad:\Program Files\IBM\WebSphere\AppServer\bin`
	Linux `cd /opt/IBM/WebSphere/AppServer/bin`
	2. Inicie la interfaz **wsadmin** utilizando un ID de usuario autorizado, por ejemplo, SKLMAdmin. Por ejemplo,
	Windows
	`wsadmin.bat -username SKLMAdmin -password mypwd -lang jython`
	Linux
	`./wsadmin.sh -username SKLMAdmin -password mypwd -lang jython`
	3. Ejecute el mandato de CLI **tklmBackupRunRestore** especificando los parámetros, por ejemplo, el nombre del archivo de copia de seguridad con su vía de acceso completa y la contraseña de copia de seguridad que ha utilizado para crear la copia de seguridad, como se muestra en el ejemplo siguiente.
	`print AdminTask.tklmBackupRunRestore ('[-backupFilePath <SKLM_DATA>/sklm_v3.0.0.0_20170429013250-0400_migration_ba -password myBackupPwd]')`
	4. Reinicie el servidor de IBM Security Key Lifecycle Manager.
	Nota: Si utiliza la interfaz de línea de mandatos, no puede restaurar los roles, usuarios y grupos desde la copia de seguridad de IBM Security Key Lifecycle Manager Versión 3.0.

Interfaz REST	1. Abra un cliente REST.
	2. Obtenga un identificador de autenticación de usuario exclusivo para acceder a los servicios REST de IBM Security Key Lifecycle Manager. Para obtener más información sobre el proceso de autenticación, consulte Proceso de autenticación de los servicios REST.
	3. Para invocar el **Servicio REST Ejecutar restauración de copia de seguridad**, envíe la solicitud HTTP POST con el nombre de archivo de copia de seguridad y la vía de acceso completa y la contraseña de copia de seguridad como parámetros. Pase el identificador de autenticación de usuario que ha obtenido en el `Paso b` junto con el mensaje de solicitud, como se muestra en el ejemplo siguiente.
	`POST https://localhost:<puerto>/SKLM/rest/v1/ckms/restore`
	`Content-Type: application/json`
	`Accept: application/json`
	`Authorization: SKLMAuth authId=139aeh34567m`
	`Accept-Language: en`
	`{"backupFilePath":"<SKLM_DATA>/sklm_v3.0.0.0_20170429013250-0400_migration_b`
	`"password":"myBackupPwd"}`
	4. Reinicie el servidor de IBM Security Key Lifecycle Manager.
	Nota: Si utiliza la interfaz REST, no puede restaurar los roles, usuarios y grupos desde la copia de seguridad de IBM Security Key Lifecycle Manager Versión 3.0.

Script de restauración de migración	1. Localice los programas de utilidad de IBM Security Key Lifecycle Manager. **Windows** <*SKLM_INSTALL_HOME*>\migration\utilities\sklmv30 La ubicación predeterminada es C:\Program Files\IBM\SKLMV301\migration\utilities\sklmv30. **Linux** <*SKLM_INSTALL_HOME*>/migration/utilities/sklmv30 La ubicación predeterminada es /opt/IBM/SKLMV301/migration/utilities/sklmv30. 2. Edite restore.properties en la carpeta sklmv30 para configurar las propiedades, como se muestra en el ejemplo siguiente. **Nota:** On Windows operating system, the restore.properties file that you use for restore operations must not contain the property keys and values with leading or trailing spaces. **Windows** WAS_HOME=C:\\Program Files\\IBM\\WebSphere\\AppServer JAVA_HOME=C:\\Program Files\\IBM\\WebSphere\\AppServer\\java\8.0 BACKUP_PASSWORD=passw0rd123 DB_PASSWORD=db2_password RESTORE_FILE=<*SKLM_DATA*>\\sklm_v3.0.0.0_20170429013250-0400_migration_ WAS_USER_PWD=wasadmin_password RESTORE_USER_ROLES=y #pkcs11_config=C:\\luna.cfg **Linux** WAS_HOME=/opt/IBM/WebSphere/AppServer JAVA_HOME=/opt/IBM/WebSphere/AppServer/java/8.0 BACKUP_PASSWORD=passw0rd123 DB_PASSWORD=db2_password RESTORE_FILE=<*SKLM_DATA*>/sklm_v3.0.0.0_20170429013250-0400_migration_b WAS_USER_PWD=wasadmin_password RESTORE_USER_ROLES=y #pkcs11_config=/luna.cfg **Nota:** • Para iniciar una sesión en IBM Security Key Lifecycle Manager mediante la utilización de las credenciales especificadas durante la instalación del producto, establezca la propiedad **RESTORE_USER_ROLES** como “n”. Cuando la propiedad se establece en “n” se asegura que el ID de usuario y la contraseña no se sobrescriben con las credenciales de usuario de la versión antigua. RESTORE_USER_ROLES=n • Si IBM Security Key Lifecycle Manager está configurado con HSM, elimine los comentarios de la propiedad **#pkcs11_config** y especifique la vía de acceso correcta del archivo luna.cfg como el valor. • En el sistema operativo de Windows, cuando especifique la vía de acceso en el archivo de propiedades, utilice “/ ” o “\\ ” como separador de vías de acceso, como se muestra en el ejemplo siguiente. C:\\sklmv30_restore O C:/sklmv30_restore 3. Abra una ventana del indicador de mandatos y especifique estos mandatos. **Windows** Vaya al directorio <*SKLM_INSTALL_HOME*>\migration\utilities\sklmv30 y ejecuta el siguiente mandato: **restoreV30.bat** **Linux**

Qué hacer a continuación

Nota: After data restoration, ensure that the path for the properties in the SKLMConfig.properties, datastore.properties, and ReplicationSKLMConfig.properties files are correct before you proceed with your next task.

Rollovers that are configured for LTO key groups and 3592 certificates are not automatically restored from the earlier versions of IBM Security Key Lifecycle Manager. You must manually set the rollover for certificates and key groups.

Para obtener más información, consulte "Restauración de grupos de claves y certificados de aplazamiento".

Restauración de grupos de claves y certificados de aplazamiento

Los aplazamientos configurados para grupos de claves LTO y certificados 3592 no se restauran automáticamente desde versiones anteriores. Para especificar dichos aplazamientos de modo manual en la versión 3.0.1, utilice el archivo de desplazamiento scheduledTasks.txt, que se ha creado en el directorio <WAS_HOME>/products/sklm/config durante el proceso de restauración.

Procedimiento

1. Abra un indicador de mandatos.
2. Vaya al siguiente directorio.

   Windows
   <*SKLM_INSTALL_HOME*>\migration\bin

   Linux <*SKLM_INSTALL_HOME*>/migration/bin
3. Ejecute el siguiente mandato.

   Windows
   Ejecute la utilidad **recreatetask.bat**.

   ```
   recreatetask.bat <WAS_HOME> <SKLMADMIN_USER> <SKLMADMIN_PASSWD>
   <SKLM_HOME>\config\scheduledTasks.txt <Logfile> <SKLM_INSTALL_HOME>
   ```

   Linux Ejecute la utilidad **recreatetask.sh**.

   ```
   ./recreatetask.sh <WAS_HOME> <SKLMADMIN_USER> <SKLMADMIN_PASSWD>
   <SKLM_HOME>/config/scheduledTasks.txt <Logfile> <SKLM_INSTALL_HOME>
   ```

   Donde <Logfile> es el nombre del archivo de registro al que se graba la información de registro, por ejemplo:

   ```
   C:\Program Files\IBM\WebSphere\AppServer\products\sklm\logs\rolloverlogs.txt
   ```

   <SKLMADMIN_USER> y <SKLMADMIN_PASSWD> son el ID de usuario y la contraseña del administrador de IBM Security Key Lifecycle Manager.

   Para las definiciones de <WAS_HOME>, <SKLM_HOME>, y <SKLM_INSTALL_HOME>, consulte Definiciones para *HOME* y otras variables de directorio.

   Nota: En sistemas operativos Windows, debe añadir una doble barra invertida en la vía de acceso y especificar la vía de acceso con delimitadores de comillas si la vía de acceso contiene espacios como, por ejemplo,

   ```
   recreatetask.bat "C:\\Program Files\\IBM\\WebSphere\\AppServer" SKLMAdmin SKLMAdminPwd
   "C:\\Program Files\\IBM\\WebSphere\\AppServer\\products\\sklm\\config\\scheduledTasks.txt"
   "C:\\Program Files\\IBM\\WebSphere\\AppServer\\products\\sklm\\logs\\rolloverlogs.txt" "C:\\Pr
   ```

Prevención de pérdida de claves

Para impedir la pérdida de datos de cifrado en claves y dispositivos de misión crítica, mantenga siempre un mínimo de dos instancias de IBM Security Key Lifecycle Manager. Asegúrese de que una de las instancias sea una réplica de los mismos dispositivos y claves. Puede proporcionar más de dos instancias redundantes.

IBM Security Key Lifecycle Manager proporciona soporte para los DS5000 storage servers que generan automáticamente una clave cuando se registra un nuevo dispositivo DS5000 en IBM Security Key Lifecycle Manager.

Do not use a setting of 1 (auto accept) for the DS5000 device family. This setting allows generation and serving of keys to DS5000 storage servers before you backup data. Para las demás familias de dispositivos, haga una copia de seguridad de las nuevas claves que se sirven.

Elimine los archivos de copia de seguridad del servidor y almacenar en una ubicación segura. Por ejemplo, copie los archivos de copia de seguridad para un CD/DVD y bloquéelos en un lugar seguro.

Nota: No copie los archivos en un almacenamiento cifrado que dependa de este producto. Si lo hace, puede provocar que la copia de seguridad no esté disponible porque el producto no está disponible.

IBM Security Key Lifecycle Manager también proporciona estas opciones de pérdida de claves:

backup.keycert.before.serving
Establezca esta propiedad en el archivo SKLMConfig.properties para que no se sirvan nuevas claves hasta que se haga una copia de seguridad de las claves.

Script de copia de seguridad automatizado
Utilice el script `autobackup.bat` para realizar de forma automática una copia de seguridad de los archivos. IBM Security Key Lifecycle Manager no sirve las claves o los certificados que no tienen una copia de seguridad si el valor de la propiedad **`backup.keycert.before.serving`** se establece en `true`, o, si no existe, en el archivo `SKLMConfig.properties`.

Configuración de script de copia de seguridad automáticas

Puede utilizar el script de copia de seguridad automatizado para hacer una copia de seguridad de los archivos.

Antes de empezar

Siga las siguientes directrices antes de restaurar copias de seguridad cifradas basadas en HSM:

- Asegúrese de que está presente la misma partición HSM con todas sus entradas de clave intactas en el sistema en el que se restaura el archivo de copia de seguridad.
- También debe estar intacta la clave maestra que se utilizó para el cifrado de clave de copia de seguridad para poder restaurar el archivo de copia de seguridad. Si se renueva la clave maestra, todas las copias de seguridad antiguas serán inaccesibles o no se podrán utilizar.

- Debe conectarse al mismo HSM y clave maestra para las operaciones de copia de seguridad y restauración independientemente de si ha utilizado cifrado basado en HSM o cifrado basado en contraseña.

Acerca de esta tarea

IBM Security Key Lifecycle Manager no sirve las claves o los certificados que no tienen una copia de seguridad si el valor de la propiedad **backup.keycert.before.serving** se establece en `true`, o, si no existe, en el archivo `SKLMConfig.properties`.

El script de copia de seguridad automatizado inicia una copia de seguridad invocando estos mandatos:

- **klmBackupIsRunning** para comprobar si se está ejecutando una operación de copia de seguridad.
- **tklmBackupIsNeeded** o el **Servicio REST Copia de seguridad necesaria** para determinar si existen nuevas clases o certificados, pero no se ha realizado todavía una copia de seguridad.
- **tklmBackupRun** o el **Servicio REST Ejecutar copia de seguridad** para ejecutar la tarea de copia de seguridad.

Antes de empezar, determine la contraseña que se utiliza para cifrar los datos del archivo de copia de seguridad.

Procedimiento

1. Ubique el script en este directorio:

   Windows

   unidad:\Program Files\IBM\SKLMV25\bin\samples\autobackup.bat

   Linux y AIX

   path/IBM/SKLMV25/bin/samples/autobackup.sh

2. Al principio del archivo `autobackup.bat` o `autobackup.sh`, ubique las líneas que cambian:

```
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. Cambie las líneas necesarias en el script:

tiphome
Necesario. El directorio de inicio de WebSphere Application Server.

Por ejemplo:

```
Set tiphome=C:/Progra~2/IBM/WebSphere/AppServer
```

username
Necesario. Un ID de usuario que tiene el permiso **klmBackup**. Utilice este ID de usuario para iniciar una sesión en IBM Security Key Lifecycle Manager. El ID de usuario también puede ser un ID de usuario existente como, por ejemplo, SKLMAdmin.

contraseña
Necesario. La contraseña del ID de usuario que tiene el permiso **klmBackup**.

backuppw
Necesario. Una contraseña que se utiliza para cifrar los datos del archivo de copia de seguridad. El valor puede tener de 6 caracteres como mínimo a un máximo de 32.

Nota: Si para las copias de seguridad se está utilizando el cifrado basado en HSM, no es necesario especificar la contraseña.

Puede utilizar una contraseña diferente para cada archivo de copia de seguridad. Al restaurar un archivo, debe poder suministrar la contraseña que se utilizó para cifrar los datos de dicho archivo durante la tarea de copia de seguridad.

backupdes
Opcional. Información adicional sobre el objetivo o el uso del archivo de copia de seguridad.

backupdir
Opcional. Un directorio que almacena los archivos JAR con datos de copia de seguridad para IBM Security Key Lifecycle Manager. Especifique la vía de acceso completa al directorio.

If the backup is successful, the value that you specify is written as the value of the **tklm.backup.dir** property in the `SKLMConfig.properties` file.

Nota:

- If you do not specify a value for this parameter and no successful backup was run before, the default is the *SKLM_DATA*`/backup` directory.
- If you specify a relative path (not suggested) such as `mybackupdir`, the backup is created in the *WAS_HOME*`/profiles/KLMProfile/`*mybackupdir* directory.
- IBM Security Key Lifecycle Manager can create a backup file in any directory for which the operating system superuser has permission to write the file. The superuser is `Administrator` on Windows systems or `root` on systems such as Linux or AIX.
- Do not create the backup file in the same directory that contains the database backup.

backupDBdir

Optional parameter. A directory in the IBM Security Key Lifecycle Manager database that contains temporary backup data for IBM Security Key Lifecycle Manager. If no parameter is specified, the

directory that is used is the value of the **tklm.backup.db2.dir** property in the datastore.properties file. The file is located in the *WAS_HOME*\products\sklm\config directory, or a temporary system directory if the directory specified by the **tklm.backup.db2.dir** property does not exist.

4. Para ejecutar el script:
   - Inmediatamente. Escriba:

     Windows

     unidad:\Program Files\IBM\SKLMV25\bin\samples\autobackup.bat

     Linux y AIX

     path/IBM/SKLMV25/bin/samples/autobackup.sh
   - De forma planificada.

     Dependiendo del sistema operativo, habilite el script en un trabajo cron o utilizando el planificador de Windows.

Configuración de las réplicas

Puede utilizar IBM Security Key Lifecycle Manager para replicar automáticamente sus materiales de claves, archivos de configuración y otra información importante desde un servidor maestro primario a un máximo de 20 servidores clon secundarios. La réplica automática garantiza la disponibilidad continuada de la clave y el certificado para los dispositivos de cifrado.

La réplica de datos permite crear clones de los entornos de IBM Security Key Lifecycle Manager en varios servidores, de un modo independiente de los sistemas operativos y la estructura de directorios del servidor.

La réplica automática garantiza la disponibilidad de un sistema de copia de seguridad cuando la instancia de IBM Security Key Lifecycle Manager primaria no está disponible. El sistema de copia de seguridad contiene todas las claves necesarias y datos asociados. Puede utilizar la interfaz gráfica de usuario, los mandatos de interfaz de línea de mandatos o las interfaces REST para configurar el proceso de réplica de clon automatizado de IBM Security Key Lifecycle Manager.

Configuración del servidor maestro

El servidor maestro es el sistema primario del que se crea la réplica. El proceso de réplica solo se desencadena cuando se añaden o modifican las nuevas claves y dispositivos en el servidor maestro. Puede realizar la réplica del servidor maestro con un máximo de 20 servidores clon. Cada servidor clon se identifica mediante una dirección IP o nombre de host y un número de puerto. El servidor utiliza las propiedades del archivo ReplicationSKLMConfig.properties para controlar el proceso de réplica.

También puede utilizar el programa de réplica de IBM Security Key Lifecycle Manager para planificar la operación de copia de seguridad automática. Solo debe configurar las propiedades del servidor maestro para realizar la copia de seguridad de datos en intervalos regulares.

Configuración del servidor clon

El proceso de réplica permite realizar clones de entornos de IBM Security Key Lifecycle Manager desde el servidor maestro para varios servidores clon. El servidor clon utiliza las propiedades del archivo

ReplicationSKLMConfig.properties para controlar el proceso de réplica. Cuando se activa el proceso de réplica, se realiza la réplica de los datos siguientes en el servidor clon:

- Datos de las tablas de base de datos de IBM Security Key Lifecycle Manager
- Almacén de confianza y almacén de claves con la clave maestra
- Los archivos de configuración de IBM Security Key Lifecycle Manager

Métodos de cifrado para realizar copias de seguridad de los datos para las actividades de réplica

IBM Security Key Lifecycle Manager da soporte a los siguientes métodos de cifrado para las copias de seguridad:

Cifrado basado en contraseña
Cuando se configura el servidor maestro para la creación de réplicas automatizadas, se especifica una contraseña para cifrar la clave de la copia de seguridad. Cuando se crea una réplica de los datos en el servidor clon, se utiliza la misma contraseña para descifrar y restaurar los archivos de copia de seguridad.

Cifrado basado en HSM
Puede configurar a IBM Security Key Lifecycle Manager para utilizar HSM (Hardware Security Module) para almacenar la clave de cifrado maestra en el servidor maestro y los servidores clon. Cuando se ejecuta el programa de réplica, se cifra la clave de la copia de seguridad en el servidor maestro con la clave maestra, que se almacena en HSM. Cuando se crea una réplica de los datos en el servidor clon, la clave maestra en HSM descifra la clave de la copia de seguridad. La clave de la copia de seguridad se utiliza para restaurar el contenido de la copia de seguridad.

Para obtener más información sobre los métodos de cifrado para las copias de seguridad y las réplicas, consulte Método de cifrado de copias de seguridad para las actividades de réplica.

Copia de seguridad y replicación de grandes cantidades de datos

Puede configurar IBM Security Key Lifecycle Manager para actividades de copia de seguridad y de réplica de alto rendimiento estableciendo el siguiente parámetro en el archivo de configuración SKLMConfig.properties del servidor maestro.

```
enableHighScaleBackup=true
```

Nota: Si establece el parámetro **enableHighScaleBackup=true** para realizar copias de seguridad y réplicas de una gran cantidad de claves, los servidores maestro y clon deben ser idénticos para que la réplica de los datos sea satisfactoria. El sistema operativo, las estructuras de directorios y el usuario administrador de DB2 debe ser iguales en los servidores maestro y clon.

Archivos de configuración de réplica

Puede ejecutar la réplica de IBM Security Key Lifecycle Manager como una tarea autónoma. Debe haber disponible un archivo de configuración de réplica válido para iniciar el proceso de réplica automática cuando se añaden claves nuevas.

IBM Security Key Lifecycle Manager utiliza las propiedades del archivo de configuración *<SKLM_HOME>*\config\ReplicationSKLMConfig.properties para controlar el proceso de réplica. Por ejemplo,

Windows
C:\Program Files\IBM\WebSphere\AppServer\products\sklm\config\
ReplicationSKLMConfig.properties

Linux /opt/IBM/WebSphere/AppServer/products/sklm/config/
ReplicationSKLMConfig.properties

Puede utilizar la interfaz gráfica de usuario de IBM Security Key Lifecycle Manager, la interfaz de línea de mandatos o la interfaz REST para cambiar las propiedades del archivo de configuración de réplica.

Puede clasificar cada sistema como:

- Maestro: el sistema primario que se está replicando.
- Clon: el sistema secundario en el que se realiza la copia.

El archivo de réplica del sistema maestro puede especificar hasta 20 clones. Cada sistema clon se identifica mediante una dirección IP o nombre de host y un número de puerto. Puede realizar la réplica de entornos de IBM Security Key Lifecycle Manager en varios servidores, de un modo independiente de los sistemas operativos y la estructura de directorios del servidor.

Notas:

- La réplica planificada solo se realiza cuando se añaden o modifican las nuevas claves y dispositivos en el sistema maestro.
- Solo puede haber un sistema maestro con un máximo de 20 clones. No se da soporte a varios maestros.

Puede utilizar el programa de réplica de IBM Security Key Lifecycle Manager para planificar la operación de copia de seguridad automática. Solo debe configurar las propiedades del servidor maestro para realizar la copia de seguridad de datos en intervalos regulares.

Ejemplo de archivo de configuración del maestro

```
replication.role=master
replication.auditLogName=replication.log
replication.MaxLogFileSize=1000
replication.MaxBackupNum=10
replication.MaxLogFileNum=3
replication.BackupDestDir=C:\\IBM\WebSphere\\AppServer\\products\\sklm\\restore
backup.ClientIP1=myhost1
backup.ClientPort1=2222
backup.EncryptionPassword=password
backup.ReleaseKeysOnSuccessfulBackup=false
backup.CheckFrequency=24
backup.TLSCertAlias=ssl_cert
replication.MasterListenPort=1111
```

- *master* es el rol de réplica predeterminado. Especifique el rol con el parámetro **replication.role**.
- Especifique al menos un clon con los parámetros **backup.ClientIPn** y **backup.ClientPortn** para replicar datos al servidor clon. Para realizar copias de seguridad de forma automática de los datos del servidor maestro a intervalos regulares, no necesita especificar la dirección y el puerto IP del clon.
- Asegúrese de que los puertos especificados están disponibles y de que IBM Security Key Lifecycle Manager, ni ningún otro proceso, los utiliza.
- Puede especificar un máximo de 20 sistemas clon.
- El parámetro **backup.TLSCertAlias** debe especificar un certificado que exista en el maestro y en todos los sistemas clon.

- Especifique una contraseña para cifrar y descifrar las copias de seguridad. Esta contraseña se enmascara en el archivo de configuración de réplica después de que IBM Security Key Lifecycle Manager la lea por primera vez.

Ejemplo de archivo de configuración del clon

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

- En el sistema clon, especifique el valor del parámetro `replication.role=clone`.
- El parámetro **`restore.ListenPort`** debe especificar el número de puerto que se especifica en el parámetro **`backup.ClientIPn`** del sistema maestro.

Para obtener información detallada sobre los parámetros de configuración de réplica disponibles, consulte Parámetros de configuración de réplica.

Comunicación entre servidores

El protocolo TLS (Transport Layer Security) se utiliza para la comunicación segura entre los sistemas maestro y clon.

Debe haber una clave privada existente disponible en el almacén de claves de IBM Security Key Lifecycle Manager del sistema maestro y de todos sus sistemas clon. El alias de esta clave en el sistema maestro se debe especificar en el parámetro **`backup.TLSCertAlias`** del archivo de configuración `ReplicationSKLMConfig.properties`. Si la misma clave no está disponible tanto en el sistema maestro como el clon, no puede iniciar la comunicación entre los sistemas para ejecutar la tarea de réplica. Puede utilizar la interfaz gráfica de usuario, la interfaz de línea de mandatos o la interfaz REST para cambiar las propiedades de la configuración de réplica.

Planificaciones de réplica

Configure las propiedades del archivo `ReplicationSKLMConfig.properties` para planificar el proceso automatizado de réplica.

Utilice la interfaz gráfica de usuario, la interfaz de línea de mandatos o la interfaz REST para configurar las propiedades del archivo de configuración de réplica para la planificación del proceso de réplica. La réplica planificada solo se realiza cuando se añaden o modifican las nuevas claves y dispositivos en el servidor maestro. También puede utilizar el programa de réplica de IBM Security Key Lifecycle Manager para planificar la operación de copia de seguridad automática. Solo debe configurar las propiedades del servidor maestro para realizar la copia de seguridad de datos en intervalos regulares.

Puede configurar la planificación de forma que IBM Security Key Lifecycle Manager compruebe periódicamente si la réplica es necesaria, e inicie el proceso si se realizan cambios. También puede especificar una hora del día para ejecutar una réplica cuando sea necesaria. Configure el parámetro **`backup.CheckFrequency`** de modo que especifique la frecuencia con que IBM Security Key Lifecycle Manager comprueba si hay actualizaciones en el sistema maestro.La réplica se desencadena cuando se realizan actualizaciones. El valor se establece en minutos, con 1440 como el valor predeterminado.

Para especificar una hora del día, configure el parámetro **backup.DailyStartReplicationBackupTime**. Debe especificar una hora en formato de 24 horas (HH:MM). La réplica se realiza solo cuando el sistema maestro haya cambiado desde la última réplica.

De forma predeterminada, el sistema clon restaura una copia de seguridad en cuanto se recibe desde el sistema maestro. Para especificar la hora de restauración, añada el parámetro **restore.DailyStartReplicationRestoreTime** en el archivo de configuración de réplica del sistema clon. Debe especificar una hora en formato de 24 horas (HH:MM).

Puede utilizar el mandato de CLI **tklmReplicationNow** o el **Servicio REST Réplica ahora** para forzar una réplica correspondiente en todos los clones definidos o una réplica específica.

Réplica de registros de auditoría

La réplica de IBM Security Key Lifecycle Manager registra información de auditoría en el archivo de registro de auditoría de IBM Security Key Lifecycle Manager.

El programa de réplica de IBM Security Key Lifecycle Manager proporciona un recurso para escribir registros de auditoría específicos de la réplica en sus propios archivos de registro de auditoría. El registro de auditoría de réplica registra todas las acciones relacionadas con el proceso de réplica. De forma predeterminada, la ubicación del archivo de registro de auditoría de réplica es *<SKLM_HOME>*\logs\replication\replication_audit.log.

Utilice la interfaz gráfica de usuario, la interfaz de línea de mandatos o la interfaz REST para establecer las propiedades de auditoría en el archivo ReplicationSKLMConfig.properties. En el archivo de configuración, puede configurar las propiedades de auditoría, tales como la ubicación del archivo de registro de auditoría, el nombre del archivo de registro, el tamaño del archivo de registro, el número máximo de archivos de registro que se ha de conservar o el número máximo de archivos de copia de seguridad que se ha de conservar.

Configuración de un servidor maestro con cifrado basado en contraseña para las copias de seguridad

Es posible cambiar los valores predeterminados del servidor maestro para la comunicación con el servidor clon para replicar datos de IBM Security Key Lifecycle Manager mediante la utilización del cifrado basado en contraseña para las copias de seguridad.

Acerca de esta tarea

Nota: Los datos se replican en los servidores clon en función de una planificación configurada sólo cuando se añaden objetos criptográficos nuevos al servidor maestro.

Utilice la interfaz gráfica de usuario, la interfaz de línea de mandatos o la interfaz REST para cambiar los valores en el archivo de configuración ReplicationSKLMConfig.properties de acuerdo con sus requisitos.

Para obtener información sobre los métodos de cifrado para las copias de seguridad y las réplicas, consulte Método de cifrado de copias de seguridad para las actividades de réplica.

Si desea configurar IBM Security Key Lifecycle Manager para actividades de copias de seguridad y réplicas de alto rendimiento, debe establecer el siguiente parámetro en el archivo de configuración *<SKLM_HOME>*/config/SKLMConfig.properties del servidor maestro, por ejemplo, C:\Program Files\IBM\WebSphere\AppServer\products\sklm\config\SKLMConfig.properties.

```
enableHighScaleBackup=true
```

Nota: Si establece el parámetro **enableHighScaleBackup=true** para realizar copias de seguridad y réplicas de una gran cantidad de claves, los sistemas maestro y clon deben ser idénticos para que la réplica de los datos sea satisfactoria. El sistema operativo, las estructuras de directorios y el usuario administrador de DB2 debe ser iguales en los servidores maestro y clon.

Procedimiento

1. Vaya a la página o el directorio correspondiente:

   Interfaz gráfica de usuario

   a. Inicie una sesión en la interfaz gráfica de usuario.
   b. Pulse **IBM Security Key Lifecycle Manager** > **Administración** > **Réplica**.

   Interfaz de línea de mandatos

   a. Vaya al directorio WAS_HOME/bin. Por ejemplo,

      Windows

      ```
      cd unidad:\Program Files (x86)\IBM\WebSphere\
      AppServer\bin
      ```

      Linux

      ```
      cd /opt/IBM/WebSphere/AppServer/bin
      ```

   b. Inicie la interfaz **wsadmin** utilizando un ID de usuario autorizado, por ejemplo, SKLMAdmin. Por ejemplo,

      Windows

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

      Linux

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

   Interfaz REST

   Abra un cliente REST.

2. Cambie el valor de uno o varios valores del servidor maestro:

   Interfaz gráfica de usuario

   a. Seleccione **Maestro**.
   b. Seleccione una opción de gestión de servidor de réplica.

      Iniciar servidor de réplica

      Pulse **Iniciar servidor de réplica** para iniciar el servidor de réplica para replicar los datos y los archivos activos de IBM Security Key Lifecycle Manager en los servidores de clonación en base a una planificación configurada.

      Detener servidor de réplica

      Pulse **Detener servidor de réplica** para detener el servidor de réplica de forma que los datos y los archivos activos de IBM Security Key Lifecycle Manager actuales no se repliquen en los servidores de clonación.

Replicar ahora

Pulse **Replicar ahora** para ejecutar de forma inmediata la tarea de réplica de IBM Security Key Lifecycle Manager y forzar el envío de una copia de seguridad a los clones configurados.

c. Configure los valores.

Propiedades básicas

Certificado del almacén de claves	Seleccione un certificado de la lista. Asegúrese de que existe un certificado SSL/TLS en el sistema maestro y en todos los sistemas clon que configura para la réplica.
Frase de contraseña para el cifrado de la copia de seguridad de réplica	La contraseña de cifrado del archivo de copia de seguridad garantiza la seguridad de los datos. El servidor clon utiliza la misma contraseña para descifrar y restaurar el archivo. **Nota:** Si para las copias de seguridad se está utilizando el cifrado basado en HSM, no es necesario especificar la contraseña.
Confirme la frase de contraseña para el cifrado de la copia de seguridad de réplica	Especifique la misma contraseña de nuevo para verificar la contraseña que ha especificado.
Puerto de escucha maestro	Número de puerto para las comunicaciones cuando se realizan réplicas no serializadas o con retardo. El puerto de escucha maestro predeterminado es 1111.
IP/Nombre de host de clon -1	Dirección IP o nombre de host de los servidores clon. Solo puede realizar la réplica de 1 servidor maestro con un máximo de 20 servidores clon. Pulse el enlace **Añadir clon** para configurar los valores de réplica para varios clones.
Puerto de clon -1	El número de puerto para enviar los archivos de copia de seguridad a los servidores clon. Cada servidor de clon se identifica mediante un número de puerto. El número de puerto predeterminado para el servidor clon es 2222.

Propiedades avanzadas

Directorio de destino de copia de seguridad de réplica	Ubicación en la que se almacenarán los archivos de copia de seguridad. El campo **Directorio de destino de copia de seguridad de réplica** muestra la vía de acceso del directorio <*SKLM_DATA*> predeterminada, donde se guardará el archivo de copia de seguridad, por ejemplo, `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data`. Para ver la definición de <*SKLM_DATA*>, consulte Definiciones para *HOME* y otras variables de directorio. Pulse **Examinar** para especificar una ubicación del repositorio de copia de seguridad bajo el directorio <*SKLM_DATA*>. La vía de acceso del directorio en el campo **Directorio de destino de copia de seguridad de réplica** cambia en función del valor establecido en la propiedad **`browse.root.dir`** en el archivo `SKLMConfig.properties`.
Número máximo de archivos de réplica que se han de conservar antes del aplazamiento	Número máximo de archivos de réplica que desea conservar. El valor debe ser un entero positivo entre 2 - 10. Cuando el número de archivos supera el límite especificado, se suprime el archivo más antiguo.

Frecuencia de réplica (en horas)	La frecuencia en la que se ha de comprobar si la operación de copia de seguridad es necesaria. El valor predeterminado se establece en 24 horas. Este parámetro se omite si está establecido el valor de **Hora de inicio de réplica diaria**.
Tiempo de réplica diaria (en formato HH:MM)	La hora en que se ha de ejecutar la tarea de réplica diaria con el formato `HH:MM`.
Nombre del archivo de registro de réplica:	El nombre y la ubicación del archivo de registro de réplica. El valor predeterminado de este parámetro es *<WAS_HOME>*`\products\sklm\logs\replication`.
Tamaño máximo del archivo de registro (en KB)	Tamaño máximo de un archivo de registro antes del aplazamiento. El valor predeterminado es 1000 KB (kilobytes). Cuando el archivo alcanza el tamaño máximo, se crea un nuevo archivo de registro.
Número máximo de archivos de registro que conservar	Número máximo de archivos de registro que desea conservar. De forma predeterminada, IBM Security Key Lifecycle Manager conserva los últimos 3 archivos de registro. Cuando el número de archivos supera el límite especificado, se suprime el archivo más antiguo.

d. Pulse **Aceptar**.

Interfaz de línea de mandatos

a. Escriba el mandato **`tklmReplicationConfigGetEntry`** en una línea para obtener el valor actual de la propiedad de destino en el archivo `ReplicationSKLMConfig.properties`. Por ejemplo, escriba

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

Una respuesta de ejemplo puede ser

```
none
```

b. Especifique los cambios. Por ejemplo, para cambiar el valor de la propiedad **`replication.role`** a `master`, escriba en una línea.

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

Interfaz REST

a. Obtenga un identificador de autenticación de usuario exclusivo para acceder a los servicios REST de IBM Security Key Lifecycle Manager. Para obtener más información sobre el proceso de autenticación, consulte Proceso de autenticación de los servicios REST.

b. Para ejecutar el **`Servicio REST Obtener propiedad de configuración única`**, envíe la solicitud HTTP GET. Pase el identificador de autenticación de usuario que ha obtenido en el `Paso a` junto con el mensaje de solicitud, como se muestra en el ejemplo siguiente.

Solicitud de servicio

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

Respuesta satisfactoria

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

c. Especifique los cambios. Por ejemplo, puede utilizar el **Servicio REST Actualizar propiedad de configuración de réplica** para enviar la siguiente solicitud de servicio para cambiar el valor de la propiedad **replication.role**.

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

Qué hacer a continuación

Es posible que desee cambiar los valores para los servidores clon para que reciban los archivos de copia de seguridad desde el servidor maestro.

Configuración de un servidor maestro con cifrado basado en contraseña cuando HSM está configurado

Es posible cambiar los valores predeterminados del servidor maestro para la comunicación con el servidor clon para replicar datos de IBM Security Key Lifecycle Manager utilizando el cifrado basado en contraseña para las copias de seguridad cuando HSM (Hardware Security Module) está configurado.

Antes de empezar

Asegúrese de que se ha configurado IBM Security Key Lifecycle Manager para que utilice HSM para almacenar la clave maestra antes de crear copias de seguridad y réplicas de datos con cifrado basado en HSM. Consulte “Configuración de los parámetros de HSM” en la página 210 para conocer los pasos de configuración.

Acerca de esta tarea

Nota: Los datos se replican en los servidores clon en función de una planificación configurada sólo cuando se añaden objetos criptográficos nuevos al servidor maestro.

Utilice la interfaz gráfica de usuario, la interfaz de línea de mandatos o la interfaz REST para cambiar los valores en el archivo de configuración `ReplicationSKLMConfig.properties` de acuerdo con sus requisitos.

Debe establecer la propiedad **enablePBEInHSM=true** en el archivo <*SKLM_HOME*>`/config/SKLMConfig.properties` para realizar copias de seguridad de datos con el cifrado basado en contraseña cuando HSM está configurado.

Para obtener información sobre los métodos de cifrado para las copias de seguridad y las réplicas, consulte Método de cifrado de copias de seguridad para las actividades de réplica.

Si desea configurar IBM Security Key Lifecycle Manager para actividades de copias de seguridad y réplicas de alto rendimiento, debe establecer el parámetro **enableHighScaleBackup=true** en el archivo de configuración <*SKLM_HOME*>`/config/SKLMConfig.properties` del servidor maestro.

Nota: Si establece el parámetro **enableHighScaleBackup=true** para realizar copias de seguridad y réplicas de una gran cantidad de claves, los sistemas maestro y clon deben ser idénticos para que la réplica de los datos sea satisfactoria. El sistema operativo, las estructuras de directorios y el usuario administrador de DB2 debe ser iguales en los servidores maestro y clon.

Procedimiento

1. Establezca la propiedad **enablePBEInHSM=true** en el archivo *<SKLM_HOME>*/config/SKLMConfig.properties.

   Interfaz de línea de mandatos

   a. Vaya al directorio WAS_HOME/bin. Por ejemplo,

      Windows

      ```
      cd unidad:\Program Files\IBM\WebSphere\AppServer\bin
      ```

      Linux

      ```
      cd /opt/IBM/WebSphere/AppServer/bin
      ```

   b. Inicie la interfaz **wsadmin** utilizando un ID de usuario autorizado, por ejemplo, SKLMAdmin. Por ejemplo,

      Windows

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

      Linux

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

   c. Ejecute el mandato **tklmConfigUpdateEntry** para establecer la propiedad **enablePBEInHSM** en el archivo de configuración SKLMConfig.properties.

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

   Interfaz REST

   a. Abra un cliente REST.

   b. Obtenga un identificador de autenticación de usuario exclusivo para acceder a los servicios REST de IBM Security Key Lifecycle Manager. Para obtener más información sobre el proceso de autenticación, consulte Proceso de autenticación de los servicios REST.

   c. Ejecute el **Servicio REST Actualizar propiedad de configuración** para establecer la propiedad **enablePBEInHSM** en el archivo de configuración SKLMConfig.properties. Pase el identificador de autenticación de usuario que ha obtenido en el Paso b junto con el mensaje de solicitud, como se muestra en el ejemplo siguiente.

      ```
      PUT https://localhost:<puerto>/SKLM/rest/v1/configProperties
      Content-Type: application/json
      Accept : application/json
      Authorization: SKLMAuth userAuthId=139aeh34567m
      Accept-Language : en
      { "enablePBEInHSM" : "true"}
      ```

2. Vaya a la página apropiada o al directorio apropiado para configurar los parámetros de réplica.

   Interfaz gráfica de usuario

   a. Inicie una sesión en la interfaz gráfica de usuario.

   b. Pulse **IBM Security Key Lifecycle Manager** > **Administración** > **Réplica**.

   Interfaz de línea de mandatos

a. Vaya al directorio WAS_HOME/bin.
b. Inicie la interfaz **wsadmin** utilizando un ID de usuario autorizado, por ejemplo, SKLMAdmin.

Interfaz REST
Abra un cliente REST.

3. Cambie el valor de uno o varios valores del servidor maestro.

Interfaz gráfica de usuario

a. Seleccione **Maestro**.
b. Seleccione una opción de gestión de servidor de réplica.

Iniciar servidor de réplica
Pulse **Iniciar servidor de réplica** para iniciar el servidor de réplica para replicar los datos y los archivos activos de IBM Security Key Lifecycle Manager en los servidores de clonación en base a una planificación configurada.

Detener servidor de réplica
Pulse **Detener servidor de réplica** para detener el servidor de réplica de forma que los datos y los archivos activos de IBM Security Key Lifecycle Manager actuales no se repliquen en los servidores de clonación.

Replicar ahora
Pulse **Replicar ahora** para ejecutar de forma inmediata la tarea de réplica de IBM Security Key Lifecycle Manager y forzar el envío de una copia de seguridad a los clones configurados.

c. Especifique los valores adecuados.

Propiedades básicas

Certificado del almacén de claves	Seleccione un certificado de la lista. Asegúrese de que existe un certificado SSL/TLS en el sistema maestro y en todos los sistemas clon que configura para la réplica.
Frase de contraseña para el cifrado de la copia de seguridad de réplica	La contraseña de cifrado del archivo de copia de seguridad garantiza la seguridad de los datos. El servidor clon utiliza la misma contraseña para descifrar y restaurar el archivo.
Confirme la frase de contraseña para el cifrado de la copia de seguridad de réplica	Especifique la misma contraseña de nuevo para verificar la contraseña que ha especificado.
Puerto de escucha maestro	Número de puerto para las comunicaciones cuando se realizan réplicas no serializadas o con retardo. El puerto de escucha maestro predeterminado es 1111.
Pulse el enlace **Añadir clon** en la sección **Detalles del clon** para configurar los valores de creación de réplicas para los clones.	
IP/Nombre de host de clon -1	Dirección IP o nombre de host de los servidores clon. Solo puede realizar la réplica de 1 servidor maestro con un máximo de 20 servidores clon.
Puerto de clon -1	El número de puerto para enviar los archivos de copia de seguridad a los servidores clon. Cada servidor de clon se identifica mediante un número de puerto. El número de puerto predeterminado para el servidor clon es 2222.

Propiedades avanzadas

Directorio de destino de copia de seguridad de réplica	Ubicación en la que se almacenarán los archivos de copia de seguridad. El campo **Directorio de destino de copia de seguridad de réplica** muestra la vía de acceso del directorio <*SKLM_DATA*> predeterminado, donde se guardará el archivo de copia de seguridad, por ejemplo, `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data`. Para ver la definición de <*SKLM_DATA*>, consulte Definiciones para *HOME* y otras variables de directorio.Pulse **Examinar** para especificar una ubicación del repositorio de copia de seguridad bajo el directorio <*SKLM_DATA*>. La vía de acceso del directorio en el campo **Directorio de destino de copia de seguridad de réplica** cambia en función del valor establecido en la propiedad **`browse.root.dir`** en el archivo `SKLMConfig.properties`.
Número máximo de archivos de réplica que se han de conservar antes del aplazamiento	Número máximo de archivos de réplica que desea conservar. El valor debe ser un entero positivo entre 2 - 10. Cuando el número de archivos supera el límite especificado, se suprime el archivo más antiguo.
Frecuencia de réplica (en horas)	La frecuencia en la que se ha de comprobar si la operación de copia de seguridad es necesaria. El valor predeterminado se establece en 24 horas. Este parámetro se omite si está establecido el valor de **Hora de inicio de réplica diaria**.
Tiempo de réplica diaria (en formato HH:MM)	La hora en que se ha de ejecutar la tarea de réplica diaria con el formato `HH:MM`.
Nombre del archivo de registro de réplica:	El nombre y la ubicación del archivo de registro de réplica. El valor predeterminado de este parámetro es `<WAS_HOME>\products\sklm\logs\replication`.
Tamaño máximo del archivo de registro (en KB)	Tamaño máximo de un archivo de registro antes del aplazamiento. El valor predeterminado es 1000 KB (kilobytes). Cuando el archivo alcanza el tamaño máximo, se crea un nuevo archivo de registro.
Número máximo de archivos de registro que conservar	Número máximo de archivos de registro que desea conservar. De forma predeterminada, IBM Security Key Lifecycle Manager conserva los últimos 3 archivos de registro. Cuando el número de archivos supera el límite especificado, se suprime el archivo más antiguo.

d. Pulse **Aceptar**.

Interfaz de línea de mandatos

a. Escriba el mandato `tklmReplicationConfigGetEntry` en una línea para obtener el valor actual de la propiedad de destino en el archivo `ReplicationSKLMConfig.properties` tal como se muestra en el ejemplo siguiente.

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

Una respuesta de ejemplo puede ser

```
none
```

b. Especifique los cambios. Por ejemplo, para cambiar el valor de la propiedad **`replication.role`** a `master`, escriba en una línea.

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

Para obtener información detallada sobre los parámetros de configuración de réplica disponibles, consulte Parámetros de configuración de réplica.

Interfaz REST

a. Ejecute el **Servicio REST Obtener propiedad de configuración única** enviando la solicitud HTTP GET tal como se muestra en el ejemplo siguiente.

Solicitud de servicio

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

Respuesta satisfactoria

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

b. Especifique los cambios. Por ejemplo, puede utilizar el **Servicio REST Actualizar propiedad de configuración de réplica** para enviar la siguiente solicitud de servicio para cambiar el valor de la propiedad **replication.role**.

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

Para obtener información detallada sobre los parámetros de configuración de réplica disponibles, consulte Parámetros de configuración de réplica.

Qué hacer a continuación

Es posible que desee cambiar los valores para los servidores clon para que reciban los archivos de copia de seguridad desde el servidor maestro.

Configuración de un servidor maestro con cifrado basado en HSM para las copias de seguridad

Es posible cambiar los valores predeterminados del servidor maestro para la comunicación con el servidor clon para replicar datos de IBM Security Key Lifecycle Manager mediante la utilización del cifrado basado en HSM para las copias de seguridad.

Antes de empezar

Asegúrese de que se ha configurado IBM Security Key Lifecycle Manager para que utilice HSM para almacenar la clave maestra antes de crear copias de seguridad y réplicas de datos con cifrado basado en HSM. Consulte “Configuración de los parámetros de HSM” en la página 210 para conocer los pasos de configuración.

Tenga en cuenta las siguientes directrices para utilizar el cifrado basado en HSM.

- La misma partición HSM debe estar presente con todas sus entradas de clave intactas en todos los servidores clon.

- La clave maestra que se utilizó para el cifrado de la clave de la copia de seguridad debe estar intacta para replicar el archivo de copia de seguridad en el servidor clon. Si se renueva la clave maestra, todas las copias de seguridad antiguas serán inaccesibles o no se podrán utilizar.
- Debe volverse a conectar al mismo HSM y la clave maestra para la réplica automatizada independientemente de si utilizó el cifrado basado en HSM o el cifrado basado en contraseña.

Acerca de esta tarea

Nota: Los datos se replican en los servidores clon en función de una planificación configurada sólo cuando se añaden objetos criptográficos nuevos al servidor maestro.

Utilice la interfaz gráfica de usuario, la interfaz de línea de mandatos o la interfaz REST para cambiar los valores en el archivo de configuración `ReplicationSKLMConfig.properties` de acuerdo con sus requisitos.

Para obtener información sobre los métodos de cifrado para las copias de seguridad y las réplicas, consulte Método de cifrado de copias de seguridad para las actividades de réplica.

Si desea configurar IBM Security Key Lifecycle Manager para actividades de copias de seguridad y réplicas de alto rendimiento, debe establecer el siguiente parámetro en el archivo de configuración *<SKLM_HOME>*`\config\SKLMConfig.properties` del servidor maestro, por ejemplo, `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\config\SKLMConfig.properties`.

```
enableHighScaleBackup=true
```

Nota: Si establece el parámetro **`enableHighScaleBackup=true`** para realizar copias de seguridad y réplicas de una gran cantidad de claves, los sistemas maestro y clon deben ser idénticos para que la réplica de los datos sea satisfactoria. El sistema operativo, las estructuras de directorios y el usuario administrador de DB2 debe ser iguales en los servidores maestro y clon.

Procedimiento

1. Vaya a la página o el directorio correspondiente:

   Interfaz gráfica de usuario

   a. Inicie una sesión en la interfaz gráfica de usuario.
   b. Pulse **IBM Security Key Lifecycle Manager** > **Administración** > **Réplica**.

   Interfaz de línea de mandatos

   a. Vaya al directorio `WAS_HOME/bin`. Por ejemplo,

      Windows

      ```
      cd unidad:\Program Files (x86)\IBM\WebSphere\
      AppServer\bin
      ```

      Linux

      ```
      cd /opt/IBM/WebSphere/AppServer/bin
      ```

   b. Inicie la interfaz **`wsadmin`** utilizando un ID de usuario autorizado, por ejemplo, `SKLMAdmin`. Por ejemplo,

      Windows

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

Linux

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

Interfaz REST

Abra un cliente REST.

2. Cambie el valor de uno o varios valores del servidor maestro:

Interfaz gráfica de usuario

a. Seleccione **Maestro**.

b. Seleccione una opción de gestión de servidor de réplica.

Iniciar servidor de réplica

Pulse **Iniciar servidor de réplica** para iniciar el servidor de réplica para replicar los datos y los archivos activos de IBM Security Key Lifecycle Manager en los servidores de clonación en base a una planificación configurada.

Detener servidor de réplica

Pulse **Detener servidor de réplica** para detener el servidor de réplica de forma que los datos y los archivos activos de IBM Security Key Lifecycle Manager actuales no se repliquen en los servidores de clonación.

Replicar ahora

Pulse **Replicar ahora** para ejecutar de forma inmediata la tarea de réplica de IBM Security Key Lifecycle Manager y forzar el envío de una copia de seguridad a los clones configurados.

c. Especifique los valores adecuados:

Propiedades básicas

Certificado del almacén de claves	Seleccione un certificado de la lista. Asegúrese de que existe un certificado SSL/TLS en el sistema maestro y en todos los sistemas clon que configura para la réplica.
Puerto de escucha maestro	Número de puerto para las comunicaciones cuando se realizan réplicas no serializadas o con retardo. El puerto de escucha maestro predeterminado es 1111.
Pulse el enlace **Añadir clon** en la sección **Detalles del clon** para configurar los valores de creación de réplicas para los clones.	
IP/Nombre de host de clon -1	Dirección IP o nombre de host de los servidores clon. Solo puede realizar la réplica de 1 servidor maestro con un máximo de 20 servidores clon. Pulse el enlace **Añadir clon** para configurar los valores de réplica para varios clones.
Puerto de clon -1	El número de puerto para enviar los archivos de copia de seguridad a los servidores clon. Cada servidor de clon se identifica mediante un número de puerto. El número de puerto predeterminado para el servidor clon es 2222.

Propiedades avanzadas

Directorio de destino de copia de seguridad de réplica	Ubicación en la que se almacenarán los archivos de copia de seguridad. El campo **Directorio de destino de copia de seguridad de réplica** muestra la vía de acceso del directorio <*SKLM_DATA*> predeterminado, donde se guardará el archivo de copia de seguridad, por ejemplo, `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data`. Para ver la definición de <*SKLM_DATA*>, consulte Definiciones para *HOME* y otras variables de directorio.Pulse **Examinar** para especificar una ubicación del repositorio de copia de seguridad bajo el directorio <*SKLM_DATA*>. La vía de acceso del directorio en el campo **Directorio de destino de copia de seguridad de réplica** cambia en función del valor establecido en la propiedad **`browse.root.dir`** en el archivo `SKLMConfig.properties`.
Número máximo de archivos de réplica que se han de conservar antes del aplazamiento	Número máximo de archivos de réplica que desea conservar. El valor debe ser un entero positivo entre 2 - 10. Cuando el número de archivos supera el límite especificado, se suprime el archivo más antiguo.
Frecuencia de réplica (en horas)	La frecuencia en la que se ha de comprobar si la operación de copia de seguridad es necesaria. El valor predeterminado se establece en 24 horas. Este parámetro se omite si está establecido el valor de **Hora de inicio de réplica diaria**.
Tiempo de réplica diaria (en formato HH:MM)	La hora en que se ha de ejecutar la tarea de réplica diaria con el formato `HH:MM`.
Nombre del archivo de registro de réplica:	El nombre y la ubicación del archivo de registro de réplica. El valor predeterminado de este parámetro es `<WAS_HOME>\products\sklm\logs\replication`.
Tamaño máximo del archivo de registro (en KB)	Tamaño máximo de un archivo de registro antes del aplazamiento. El valor predeterminado es 1000 KB (kilobytes). Cuando el archivo alcanza el tamaño máximo, se crea un nuevo archivo de registro.
Número máximo de archivos de registro que conservar	Número máximo de archivos de registro que desea conservar. De forma predeterminada, IBM Security Key Lifecycle Manager conserva los últimos 3 archivos de registro. Cuando el número de archivos supera el límite especificado, se suprime el archivo más antiguo.

d. Pulse **Aceptar**.

Interfaz de línea de mandatos

a. Escriba el mandato **`tklmReplicationConfigGetEntry`** en una línea para obtener el valor actual de la propiedad de destino en el archivo `ReplicationSKLMConfig.properties`. Por ejemplo, escriba

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

Una respuesta de ejemplo puede ser

```
none
```

b. Especifique los cambios. Por ejemplo, para cambiar el valor de la propiedad **`replication.role`** a `master`, escriba en una línea.

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

Para obtener información detallada sobre los parámetros de configuración de réplica disponibles, consulte Parámetros de configuración de réplica.

Interfaz REST

a. Obtenga un identificador de autenticación de usuario exclusivo para acceder a los servicios REST de IBM Security Key Lifecycle Manager. Para obtener más información sobre el proceso de autenticación, consulte Proceso de autenticación de los servicios REST.

b. Para ejecutar el **Servicio REST Obtener propiedad de configuración única**, envíe la solicitud HTTP GET. Pase el identificador de autenticación de usuario que ha obtenido en el `Paso a` junto con el mensaje de solicitud, como se muestra en el ejemplo siguiente.

   Solicitud de servicio

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

   Respuesta satisfactoria

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

c. Especifique los cambios. Por ejemplo, puede utilizar el **Servicio REST Actualizar propiedad de configuración de réplica** para enviar la siguiente solicitud de servicio para cambiar el valor de la propiedad **replication.role**.

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

   Para obtener información detallada sobre los parámetros de configuración de réplica disponibles, consulte Parámetros de configuración de réplica.

Qué hacer a continuación

Es posible que desee cambiar los valores para los servidores clon para que reciban los archivos de copia de seguridad desde el servidor maestro.

Especificar parámetros de réplica para un servidor clon

Los valores predeterminados de un servidor clon se pueden cambiar para recibir datos de IBM Security Key Lifecycle Manager desde el servidor maestro de acuerdo con una planificación configurada. Los datos se replican en los servidores clon únicamente cuando se añaden nuevos objetos criptográficos al servidor maestro.

Acerca de esta tarea

Utilice la página Configuración de la réplica de clon automatizada para cambiar los valores de la réplica. O bien, puede utilizar los siguientes mandatos de CLI o las interfaces REST para listar y cambiar las propiedades adecuadas en el archivo de configuración `ReplicationSKLMConfig.properties`:

- **tklmReplicationConfigGetEntry** y **tklmReplicationConfigUpdateEntry**

- **Servicio REST Obtener propiedad de configuración de réplica única** y **Servicio REST Actualizar propiedad de configuración de réplica**

Procedimiento

1. Navegue a la página o el directorio correspondiente:
   - Interfaz gráfica de usuario:
     a. Inicie una sesión en la interfaz gráfica de usuario.
     b. Pulse **IBM Security Key Lifecycle Manager** > **Administración** > **Réplica**.
   - Command-line interface
     a. Go to the <*WAS_HOME*>/bin directory. For example,

        Windows
        ```
        cd drive:\Program Files\IBM\WebSphere\AppServer\bin
        ```

        Linux
        ```
        cd /opt/IBM/WebSphere/AppServer/bin
        ```

     b. Start the **wsadmin** interface by using an authorized user ID, such as SKLMAdmin. For example,

        Windows
        ```
        wsadmin.bat -username SKLMAdmin -password mypwd -lang jython
        ```

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

   - Interfaz REST:
     – Abra un cliente REST.
2. Cambie el valor de uno o varios valores del servidor clon.
   - En la interfaz gráfica de usuario:
     a. Seleccione **Clon**.
     b. Seleccione una opción de gestión de servidor de réplica.

        Iniciar servidor de réplica
        Pulse **Iniciar servidor de réplica** para iniciar el servidor de réplica para la recepción de datos de IBM Security Key Lifecycle Manager desde el servidor maestro.

        Detener servidor de réplica
        Pulse **Detener servidor de réplica** para detener el servidor de réplica de forma que los servidores clon dejen de recibir datos de IBM Security Key Lifecycle Manager desde el servidor maestro.

     c. Especifique los valores adecuados:

        Propiedades básicas

Puerto de escucha clon	El número de puerto donde debe escuchar el servidor clon para recibir los archivos de copia de seguridad. El número de puerto predeterminado es 2222.
Puerto de escucha maestro	Número de puerto para las comunicaciones cuando se realizan réplicas no serializadas o con retardo. El puerto de escucha maestro predeterminado es 1111.

        Propiedades avanzadas

Número de reintentos en caso de error de restauración	El número máximo de reintentos permitidos después de que haya fallado la primera operación de restauración. El valor debe ser un entero positivo entre 0 - 2.

Nombre del archivo de registro de réplica:	El nombre y la ubicación del archivo de registro de réplica. El valor predeterminado de este parámetro es *<WAS_HOME>*\products\sklm\logs\replication.
Tamaño máximo del archivo de registro (en KB)	Tamaño máximo de un archivo de registro antes del aplazamiento. El valor predeterminado es 1000 KB (kilobytes). Cuando el archivo alcanza el tamaño máximo, se crea un nuevo archivo de registro.
Número máximo de archivos de registro que conservar	Número máximo de archivos de registro que desea conservar. De forma predeterminada, IBM Security Key Lifecycle Manager conserva los últimos 3 archivos de registro. Cuando el número de archivos supera el límite especificado, se suprime el archivo más antiguo.

d. Pulse **Aceptar**.

- Interfaz de línea de mandatos:
  a. Escriba el mandato **tklmReplicationConfigGetEntry** en una línea para obtener el valor actual de la propiedad de destino en el archivo ReplicationSKLMConfig.properties. Por ejemplo, escriba

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

     Una respuesta de ejemplo puede ser:

     ```
     none
     ```

  b. Especifique los cambios. Por ejemplo, para cambiar el valor de la propiedad **replication.role** a clone, escriba en una línea.

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

- Interfaz REST:
  a. Obtenga un identificador de autenticación de usuario exclusivo para acceder a los servicios REST de IBM Security Key Lifecycle Manager. Para obtener más información sobre el proceso de autenticación, consulte Proceso de autenticación de los servicios REST.
  b. Para invocar el **Servicio REST Obtener propiedad de configuración única**, envíe la solicitud HTTP GET. Pase el identificador de autenticación de usuario que ha obtenido en el Paso a junto con el mensaje de solicitud, como se muestra en el ejemplo siguiente.

     Solicitud de servicio

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

     Respuesta satisfactoria

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

  c. Especifique los cambios. Por ejemplo, puede utilizar el **Servicio REST Actualizar propiedad de configuración de réplica** para enviar la siguiente solicitud de servicio para cambiar el valor de la propiedad **replication.role**.

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

Qué hacer a continuación

Es posible que desee cambiar los valores para los otros servidores clon. Puede crear réplicas de datos de IBM Security Key Lifecycle Manager desde un servidor maestro primario para un máximo de 20 servidores clon secundarios.

Planificación de la operación de copia de seguridad automática

Puede configurar los valores de la réplica para que se ejecute automáticamente la operación de copia de seguridad y, de este modo, asegurarse de que se realiza la copia de seguridad de los datos críticos de IBM Security Key Lifecycle Manager en intervalos regulares.

Acerca de esta tarea

Puede utilizar el programa de réplica de IBM Security Key Lifecycle Manager para planificar la operación de copia de seguridad automática. Solo debe configurar las propiedades del servidor maestro para realizar la copia de seguridad de datos en intervalos regulares.

Utilice la interfaz gráfica de usuario, la interfaz de línea de mandatos o la interfaz REST para cambiar los valores en el archivo de configuración `ReplicationSKLMConfig.properties` de acuerdo con sus requisitos.

IBM Security Key Lifecycle Manager da soporte a los siguientes métodos de cifrado para las copias de seguridad:

Cifrado basado en contraseña
Cuando se configura el servidor maestro para la creación de réplicas automatizadas, se especifica una contraseña para cifrar la clave de la copia de seguridad. Cuando se crea una réplica de los datos en el servidor clon, se utiliza la misma contraseña para descifrar y restaurar los archivos de copia de seguridad.

Cifrado basado en HSM
Puede configurar a IBM Security Key Lifecycle Manager para utilizar HSM (Hardware Security Module) para almacenar la clave de cifrado maestra en el servidor maestro y los servidores clon. Cuando se ejecuta el programa de réplica, se cifra la clave de la copia de seguridad en el servidor maestro con la clave maestra, que se almacena en HSM. Cuando se crea una réplica de los datos en el servidor clon, la clave maestra en HSM descifra la clave de la copia de seguridad. La clave de la copia de seguridad se utiliza para restaurar el contenido de la copia de seguridad.

Para obtener información sobre la configuración del servidor maestro con el cifrado basado en HSM, consulte “Configuración de un servidor maestro con cifrado basado en HSM para las copias de seguridad” en la página 189. Para obtener información sobre la configuración del servidor maestro con el cifrado basado en

contraseña cuando HSM está configurado, consulte "Configuración de un servidor maestro con cifrado basado en contraseña cuando HSM está configurado" en la página 185.

El siguiente procedimiento describe cómo planificar una operación de copia de seguridad automática utilizando el cifrado basado en contraseña.

Procedimiento

1. Vaya a la página o el directorio correspondiente:

   Interfaz gráfica de usuario

   a. Inicie una sesión en la interfaz gráfica de usuario.
   b. Pulse **IBM Security Key Lifecycle Manager** > **Administración** > **Réplica**.

   Interfaz de línea de mandatos

   a. Vaya al directorio `WAS_HOME/bin`. Por ejemplo,

      Windows

      ```
      cd unidad:\Program Files\IBM\WebSphere\AppServer\bin
      ```

      Linux

      ```
      cd /opt/IBM/WebSphere/AppServer/bin
      ```

   b. Inicie la interfaz **wsadmin** utilizando un ID de usuario autorizado, por ejemplo, `SKLMAdmin`. Por ejemplo,

      Windows

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

      Linux

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

   Interfaz REST

   Abra un cliente REST.

2. Cambie el valor de uno o varios valores del servidor maestro:

   Interfaz gráfica de usuario

   a. Seleccione **Maestro**.
   b. Seleccione una opción de gestión de servidor de réplica.

      Iniciar servidor de réplica

      Pulse **Iniciar servidor de réplica** para iniciar el servidor de réplica para realizar una copia de seguridad de los datos de IBM Security Key Lifecycle Manager de acuerdo con una planificación configurada.

      Detener servidor de réplica

      Pulse **Detener servidor de réplica** para detener el servidor de réplica de forma que no se realicen copias de seguridad de los datos de IBM Security Key Lifecycle Manager.

      Replicar ahora

      Pulse **Replicar ahora** para ejecutar de forma inmediata la tarea de réplica de IBM Security Key Lifecycle Manager y de esta manera, forzar la creación de un archivo de copia de seguridad.

   c. Configure los valores.

      Propiedades básicas

Certificado del almacén de claves	Seleccione un certificado de la lista. Asegúrese de que existe un certificado SSL/TLS en el sistema maestro y en todos los sistemas clon que configura para la réplica.
Frase de contraseña para el cifrado de la copia de seguridad de réplica	La contraseña de cifrado del archivo de copia de seguridad garantiza la seguridad de los datos. Necesita la misma contraseña para descifrar y restaurar el archivo. **Nota:** Si para las copias de seguridad se está utilizando el cifrado basado en HSM, no es necesario especificar la contraseña.
Confirme la frase de contraseña para el cifrado de la copia de seguridad de réplica	Especifique la misma contraseña de nuevo para verificar la contraseña que ha especificado.
Puerto de escucha maestro	Número de puerto para las comunicaciones cuando se realizan réplicas no serializadas o con retardo. El puerto de escucha maestro predeterminado es 1111.

Propiedades avanzadas

Directorio de destino de copia de seguridad de réplica	Ubicación en la que se almacenarán los archivos de copia de seguridad. El campo **Directorio de destino de copia de seguridad de réplica** muestra la vía de acceso del directorio <*SKLM_DATA*> predeterminado, donde se guardará el archivo de copia de seguridad, por ejemplo, `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data`. Para ver la definición de <*SKLM_DATA*>, consulte Definiciones para *HOME* y otras variables de directorio.Pulse **Examinar** para especificar una ubicación del repositorio de copia de seguridad bajo el directorio <*SKLM_DATA*>.
Número máximo de archivos de réplica que se han de conservar antes del aplazamiento	Número máximo de archivos de réplica que desea conservar. El valor debe ser un entero positivo entre 2 - 10. Cuando el número de archivos supera el límite especificado, se suprime el archivo más antiguo.
Frecuencia de réplica (en horas)	La frecuencia en la que se ha de comprobar si la operación de copia de seguridad es necesaria. El valor predeterminado se establece en 1 hora. Este parámetro se omite si está establecido el valor de **Hora de inicio de réplica diaria**.
Tiempo de réplica diaria (en formato HH:MM)	La hora en que se ha de ejecutar la tarea de réplica diaria con el formato `HH:MM`.
Nombre del archivo de registro de réplica:	El nombre y la ubicación del archivo de registro de réplica. El valor predeterminado de este parámetro es `<WAS_HOME>\products\sklm\logs\replication`.
Tamaño máximo del archivo de registro (en KB)	Tamaño máximo de un archivo de registro antes del aplazamiento. El valor predeterminado es 1000 KB (kilobytes). Cuando el archivo alcanza el tamaño máximo, se crea un nuevo archivo de registro.
Número máximo de archivos de registro que conservar	Número máximo de archivos de registro que desea conservar. De forma predeterminada, IBM Security Key Lifecycle Manager conserva los últimos 3 archivos de registro. Cuando el número de archivos supera el límite especificado, se suprime el archivo más antiguo.

d. Pulse **Aceptar**.

Interfaz de línea de mandatos

a. Escriba el mandato **tklmReplicationConfigGetEntry** en una línea para obtener el valor actual de la propiedad de destino en el archivo ReplicationSKLMConfig.properties. Por ejemplo, escriba:

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

Una respuesta de ejemplo puede ser:

```
none
```

b. Especifique los cambios. Por ejemplo, para cambiar el valor de la propiedad **replication.role** a master, escriba en una línea.

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

Interfaz REST

a. Obtenga un identificador de autenticación de usuario exclusivo para acceder a los servicios REST de IBM Security Key Lifecycle Manager. Para obtener más información sobre el proceso de autenticación, consulte Proceso de autenticación de los servicios REST.

b. Para ejecutar el **Servicio REST Obtener propiedad de configuración única**, envíe la solicitud HTTP GET. Pase el identificador de autenticación de usuario que ha obtenido en el Paso a junto con el mensaje de solicitud, como se muestra en el ejemplo siguiente.

Solicitud de servicio

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

Respuesta satisfactoria

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

c. Especifique los cambios. Por ejemplo, puede utilizar el **Servicio REST Actualizar propiedad de configuración de réplica** para enviar la siguiente solicitud de servicio para cambiar el valor de la propiedad **replication.role**.

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

Configuración del proceso de réplica utilizando mandatos de la línea de interfaz de mandatos y los servicios REST

Debe configurar un entorno básico en IBM Security Key Lifecycle Manager para ejecutar el proceso de réplica.

Acerca de esta tarea

En este tema se describe cómo configurar el proceso de réplica mediante los mandatos de la interfaz de línea de mandatos y las interfaces REST de IBM Security Key Lifecycle Manager para la réplica.

Procedimiento

1. Configure el sistema maestro de IBM Security Key Lifecycle Manager.
2. Especifique un certificado de SSLSERVER para que la réplica funcione. El certificado se puede crear con la interfaz gráfica de usuario, la interfaz de línea de mandatos o la interfaz REST tal como se muestra en los siguientes ejemplos.

   Interfaz gráfica de usuario

   a. Inicie una sesión en la interfaz gráfica de usuario.
   b. Pulse **Configuración avanzada** > **Certificados del servidor**.

   Interfaz de línea de mandatos

   a. Vaya al directorio WAS_HOME/bin. Por ejemplo,

      Windows

      ```
      cd unidad:\Program Files\IBM\WebSphere\AppServer\bin
      ```

      Linux

      ```
      cd /opt/IBM/WebSphere/AppServer/bin
      ```

   b. Inicie la interfaz **wsadmin** utilizando un ID de usuario autorizado, por ejemplo, SKLMAdmin. Por ejemplo,

      Windows

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

      Linux

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

   c. Escriba el mandato **tklmCertCreate** en una línea. Por ejemplo, para crear un certificado autofirmado, escriba:

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

   Interfaz REST

   a. Abra un cliente REST.
   b. Obtenga un identificador de autenticación de usuario exclusivo para acceder a los servicios REST de IBM Security Key Lifecycle Manager. Para obtener más información sobre el proceso de autenticación, consulte Proceso de autenticación de los servicios REST.
   c. Para crear un certificado autofirmado, ejecute el **Servicio REST Generar solicitud de certificado** enviando la siguiente solicitud HTTP.

      ```
      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 "  }
      ```

3. Cree una copia de seguridad del IBM Security Key Lifecycle Manager maestro tal como se muestra en los siguientes ejemplos.

   Nota: No necesita especificar la contraseña cuando IBM Security Key Lifecycle Manager está configurado para utilizar HSM (Hardware Security Module) para almacenar la clave de cifrado maestra. Para obtener más información sobre los métodos de cifrado para realizar copias de seguridad de los datos, consulte Cifrado basado en HSM de copias de seguridad.

Interfaz gráfica de usuario

a. Inicie una sesión en la interfaz gráfica de usuario.
b. Pulse **Copia de seguridad y restauración**.

Interfaz de línea de mandatos

Escriba el mandato **tklmBackupRun**.

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

Interfaz REST

Para crear una copia de seguridad, ejecute el **Servicio REST Ejecutar copia de seguridad** enviando la siguiente solicitud HTTP.

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

Nota:

También existe la posibilidad de configurar a IBM Security Key Lifecycle Manager para actividades de copias de seguridad y restauración de alto rendimiento en el archivo de configuración `SKLMConfig.properties` del servidor maestro.

```
enableHighScaleBackup=true
```

Para realizar copias de seguridad y réplicas de grandes cantidades de claves, el servidor maestro y clon deben ser idénticos. El sistema operativo, las estructuras de directorios y el usuario administrador de DB2 deben ser iguales en ambos servidores.

Para obtener información sobre cómo realizar copias de seguridad de grandes cantidades de datos, consulte “Copia de seguridad de una cantidad grande de datos” en la página 132.

4. Tome la copia de seguridad que se creó en el Paso 3 y cópiela en sus sistemas clon de IBM Security Key Lifecycle Manager. Restaure esta copia de seguridad de cada uno de estos sistemas en los siguientes ejemplos:

Interfaz gráfica de usuario

a. Inicie una sesión en la interfaz gráfica de usuario.
b. Pulse **Copia de seguridad y restauración**.

Interfaz de línea de mandatos

Escriba el mandato **tklmBackupRestoreRun** en una línea:

```
print AdminTask.tklmBackupRunRestore
('[-backupFilePath /opt/sklmbackup/sklm_v2.7_20160412074433_backup.jar
  -password myBackupPwd]')
```

Interfaz REST

Para restaurar una copia de seguridad, ejecute el **Servicio REST Ejecutar restauración de copia de seguridad** enviando la siguiente solicitud HTTP.

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

5. Cree el archivo de configuración de réplica `ReplicationSKLMConfig.properties` en el sistema maestro. Este archivo de configuración debe ser un archivo de texto y encontrarse en el mismo directorio que el archivo de propiedades IBM Security Key Lifecycle Manager, por ejemplo `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\config\ReplicationSKLMConfig.properties`.

   Utilice la interfaz de línea de mandatos o los servicios REST para establecer las propiedades en el `ReplicationSKLMConfig.properties`.

   Interfaz de línea de mandatos

   Escriba el mandato **tklmReplicationConfigUpdateEntry** en una línea para establecer el valor de la propiedad **replication.role** en `master`.

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

   Interfaz REST

   Para establecer el valor, ejecute el **Servicio REST Actualizar propiedad de configuración de réplica** enviando la solicitud HTTP.

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

   Para obtener información detallada sobre los parámetros de configuración de réplica disponibles, consulte Parámetros de configuración de réplica.

   En el ejemplo siguiente se muestran los campos que son obligatorios en el maestro para permitir que la tarea de réplica empiece.

   - Establezca el rol en maestro.
   - Identifique el certificado del Paso 2 y proporcione al menos un servidor clon y un número de puerto.
   - Defina el puerto de escucha maestro y elija una contraseña.

     Nota: No necesita especificar la contraseña cuando IBM Security Key Lifecycle Manager está configurado para utilizar HSM (Hardware Security Module) para almacenar la clave de cifrado maestra. Para obtener información sobre los métodos de cifrado para realizar copias de seguridad de los datos para las actividades de réplica, consulte Método de cifrado de copias de seguridad para las actividades de réplica.

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

   La propiedad **backup.EncryptionPassword** puede contener caracteres, números o caracteres especiales. El producto enmascara esta propiedad cuando se ejecuta la réplica por primera vez. La propiedad **backup.TLSCertAlias** especifica el alias del certificado y la clave privada que se utiliza para comunicarse con el clon creado en el Paso 2.

   La propiedad **replication.MasterListenPort** especifica el puerto en el que el sistema maestro escucha de determinadas respuestas procedentes de los clones. Las propiedades **backup.ClientIP1** y **backup.ClientPort1** definen el clon. La propiedad **backup.ClientIP1** puede ser un nombre de host o una dirección IP. La propiedad **backup.ClientPort1** especifica el puerto en el que el cliente está a la escucha. Para definir otros clones, debe especificar las propiedades

backup.ClientIP* y **backup.ClientPort***, donde "*" es un número entre 2 y 20, al igual que hizo para el primer conjunto.

6. Cree el archivo de configuración de réplica `ReplicationSKLMConfig.properties` en el sistema clon. Este archivo de configuración debe ser un archivo que debe estar en el mismo directorio que el archivo de propiedades IBM Security Key Lifecycle Manager, por ejemplo, `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\config\ReplicationSKLMConfig.properties`.

   Utilice la interfaz de línea de mandatos o la interfaz REST para establecer las propiedades en el archivo de configuración de réplica tal como se describió en el Paso 5.

   En el ejemplo siguiente se muestran los campos que son obligatorios en el clon para permitir que la tarea de réplica empiece.

   - Establezca el rol en clon.
   - Defina un puerto de escucha maestro.
   - Defina un puerto de escucha de restauración. El puerto debe ser el mismo que el número de puerto que se codifica en el correspondiente parámetro **backup.ClientPort*** en el servidor maestro.

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

   Es obligatorio establecer la propiedad **replication.role** para los clones. De forma predeterminada, el valor de esta propiedad es `master`. La propiedad **backup.TLSCertAlias** se debe establecer en el certificado creado en el Paso 2. Esta propiedad se utiliza para enviar el estado del clon cuando se pospone la réplica a una hora posterior, o cuando el proceso de restauración toma más tiempo que el que espera el maestro por una respuesta.

   La propiedad **replication.MasterListenPort** especifica el puerto para enviar el estado cuando la réplica se pospone hasta más tarde o el proceso de restauración tarda más tiempo del que el maestro espera una respuesta. La última propiedad **restore.ListenPort** es el puerto en el que el clon escucha las solicitudes de réplica procedentes del maestro.

7. Puede ejecutar tareas de réplica ad hoc utilizando la interfaz de línea de mandatos **TKLMReplicationNow** o el **Servicio REST Réplica ahora**. También tiene la posibilidad de planificar una réplica. Utilice la propiedad **backup.DailyStartReplicationBackupTime** o **backup.CheckFrequency** en el archivo de configuración de réplica para planificar una tarea de copia de seguridad.

   La siguiente propiedad planifica la tarea de copia de seguridad a las 23:00 h cada día.

   ```
   backup.DailyStartReplicationBackupTime=23:00
   ```

   La siguiente propiedad comprueba si se necesita una copia de seguridad cada 24 horas y ejecuta la tarea si es necesario.

   ```
   backup.CheckFrequency=1440
   ```

8. Reinicie IBM Security Key Lifecycle Manager en los sistemas maestro y clon. Puede ver los siguientes mensajes en un sistema maestro y clon: utilice el mandato de CLI **tklmReplicationStatus** para asegurarse de que se esté ejecutando la tarea de réplica. Puede ver los siguientes mensajes en un sistema maestro y uno clon:

   Interfaz de línea de mandatos

   Puede utilizar el siguiente mandato de CLI para asegurarse de que se esté ejecutando la tarea de réplica:

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

Sistema maestro

```
CTGKM2215I The Security Key Lifecycle Manager Replication
task is UP. Role set to: MASTER
CTGKM2218I The last completed replication took place at
Thu Jun 19 14:50:59 WST 2017
CTGKM2217I The next scheduled replication is due at
Fri Jun 20 17:03:36 WST 2017
```

Sistema clon

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

Interfaz REST

Utilice el **Servicio REST Estado de réplica** para asegurarse de que se esté ejecutando la tarea de réplica. Envíe la siguiente solicitud HTTP utilizando un cliente REST:

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

Sistema maestro

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

]
```

Sistema clon

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

]
```

9. Ahora la réplica está configurada y la réplica comprueba si hay cambios cada 60 minutos. Puede cambiar este intervalo, configurar una hora específica cada día para que la réplica compruebe si hay cambios. También puede utilizar el mandato de CLI **tklmReplicationNow** o **Servicio REST Réplica ahora** para ejecutar una tarea de réplica inmediatamente.

Problemas de réplica y su resolución

Debe tener en cuenta los posibles problemas en los sistemas maestro y clon al ejecutar la tarea de réplica de IBM Security Key Lifecycle Manager.

Réplica incompleta

- Asegúrese de que el certificado TSL/SSL con la clave privada que se especifica en el parámetro **backup.TLSCertAlias** está disponible tanto en el servidor maestro como en el servidor clon.

- Asegúrese de que el número de puerto para el servidor maestro está libre. Los números de puerto de clon configurados en el servidor maestro deben estar libres en el servidor clon.
- Compruebe que los nombres de servidor o direcciones IP especificados en el archivo de configuración de réplica sean correctos y que el sistema maestro pueda acceder a los mismos.
- Compruebe si la tarea de réplica está activa en cada servidor ejecutando el mandato **tklmReplicationStatus**, el **Servicio REST Estado de réplica** o el estado en la sección **Réplica** de la página de bienvenida IBM Security Key Lifecycle Manager.
- Para la réplica de DB2, asegúrese de que la fecha/hora de los servidores maestro y clon esté sincronizada estrechamente. Si hay grandes discrepancias, es posible que falle la restauración.
- Compruebe el archivo de configuración de réplica para asegurarse de que se han definido los parámetros mínimos necesarios, sin errores tipográficos.
- Defina un máximo de 1 maestro y 20 clones asociados.
- Compruebe el archivo de auditoría de réplica para obtener más información sobre el error de réplica.

La réplica no se realiza a la hora planificada

- Las réplicas planificadas se realizan sólo cuando se han añadido o modificado nuevas claves y dispositivos en el servidor maestro.
- Cuando se ha establecido una hora de réplica específica y un intervalo de comprobación en el archivo de configuración de réplica maestro, la hora prevalece sobre el intervalo de comprobación.

Réplica de sistema de clon

- El clon del servidor IBM Security Key Lifecycle Manager se reinicia después de la réplica.
- Mantenga la disponibilidad de los servidores clon. Puede especificar una hora del día específica para realizar la réplica con el parámetro **restore.DailyStartReplicationRestoreTime**. Por ejemplo, para ejecutar restauraciones únicamente a las 23:00, independientemente de la hora en que se reciba el archivo de copia de seguridad, codifique la siguiente propiedad en el archivo de configuración:

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

Reinicio de IBM Security Key Lifecycle Manager server

Al reiniciar el servidor éste lee su configuración y acepta los cambios de configuración, si hay. Para reiniciar el servidor de IBM Security Key Lifecycle Manager, ejecute los scripts de reinicio del servidor, el servicio REST o utilice la interfaz gráfica de usuario.

Acerca de esta tarea

Para reiniciar el servidor, utilice el enlace <*Usuario de IBM Security Key Lifecycle Manager*> en la barra de la cabecera en la página de bienvenida, **Servicio REST Reiniciar servidor** o ejecute los scripts **stopServer** y **startServer**.

Procedimiento

1. Vaya al directorio o la página apropiada.

   Interfaz gráfica de usuario

   a. Inicie una sesión en la interfaz gráfica de usuario.

   b. En la barra de la cabecera de la página de bienvenida, pulse el enlace <*Usuario de IBM Security Key Lifecycle Manager*>. Por ejemplo, pulse el enlace **SKLMAdmin**.

   Scripts de reinicio del servidor

   a. Vaya al directorio <*WAS_HOME*>\bin.

      Windows

      ```
      C:\Program Files\IBM\WebSphere\AppServer\bin
      ```

      Linux

      ```
      /opt/IBM/WebSphere/AppServer/bin
      ```

   Interfaz REST

   Abra un cliente REST.

2. Reinicie el servidor.

   Interfaz gráfica de usuario

   a. Pulse **Reiniciar servidor**.

   b. Pulse **Aceptar**.

      Nota: El servidor de IBM Security Key Lifecycle Manager no está disponible durante unos minutos mientras se completa la operación de reinicio.

   Scripts de reinicio del servidor

   a. Detenga el servidor.

      Windows

      ```
      stopServer.bat server1
      ```

      Linux

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

      La seguridad global está habilitada de forma predeterminada. Especifique el ID de usuario y la contraseña del administrador de WebSphere Application Server como parámetros en el script `stopServer`. El script solicitará estos parámetros si se omiten, pero podrá especificarlos en la línea de mandatos:

      Windows

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

      Linux

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

   b. Inicie el servidor.

      Windows

      ```
      startServer.bat server1
      ```

      Linux

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

   Interfaz REST

   a. Obtenga un identificador de autenticación de usuario exclusivo para acceder a los servicios REST de IBM Security Key Lifecycle

Manager. Para obtener más información sobre el proceso de autenticación, consulte Proceso de autenticación de los servicios REST.

b. Para ejecutar **Servicio REST Reiniciar servidor**, envía la solicitud HTTP POST. Pase el identificador de autenticación de usuario que ha obtenido en el Paso a junto con el mensaje de solicitud, como se muestra en el ejemplo siguiente.

```
POST https://localhost:<puerto>/SKLM/rest/v1/ckms/servermanagement/restartServer
Content-Type: application/json
Accept: application/json
Authorization: SKLMAuth userAuthId=139aeh34567m
```

Qué hacer a continuación

Determine si IBM Security Key Lifecycle Manager está en ejecución. Por ejemplo, abra IBM Security Key Lifecycle Manager en un navegador web e inicie sesión en él.

Habilitación de la seguridad global

Pueden producirse condiciones en las que deba habilitar la seguridad global.

Acerca de esta tarea

No inhabilite la seguridad global cuando utilice IBM Security Key Lifecycle Manager.

Procedimiento

1. Para habilitar la seguridad global, inicie la sesión como el administrador de WebSphere Application Server WASAdmin.
2. En la barra de navegación, pulse **Seguridad** > **Seguridad global**.
3. Active el recuadro de selección **Habilitar seguridad administrativa**.

   Asegúrese de que **Habilitar seguridad de aplicación** también esté seleccionado y que **Utilizar seguridad Java 2 para restringir el acceso a los recursos locales** *no* esté seleccionado.
4. Pulse **Aplicar**.
5. Pulse **Guardar** en el recuadro Mensajes.
6. Pulse **Finalizar sesión**.
7. Detenga y reinicie el servidor.
8. Vuelva a cargar la página de inicio de sesión de IBM Security Key Lifecycle Manager. Verifique que la página requiera una contraseña.

Inhabilitación de la seguridad global

Pueden producirse condiciones en las que deba inhabilitar la seguridad global.

Acerca de esta tarea

No inhabilite la seguridad global cuando utilice IBM Security Key Lifecycle Manager.

Procedimiento

1. Para inhabilitar la seguridad global, inicie la sesión como el administrador de WebSphere Application Server WASAdmin.

2. En la barra de navegación, pulse **Seguridad** > **Seguridad global**.
3. Desactive el recuadro de selección **Habilitar seguridad administrativa**.
4. Pulse **Aplicar**.
5. Pulse **Guardar** en el recuadro Mensajes.
6. Pulse **Finalizar sesión**.
7. Detenga y reinicie el servidor.
8. Vuelva a cargar la página de inicio de sesión de IBM Security Key Lifecycle Manager. Verifique que la página *no* requiera contraseña.

Uso de Hardware Security Module en IBM Security Key Lifecycle Manager

Debe añadir los parámetros el archivo de configuración de IBM Security Key Lifecycle Manager para definir un Hardware Security Module (HSM).

Puede utilizar HSM para almacenar la clave maestra para proteger todas las contraseñas que se han almacenado en la base de datos IBM Security Key Lifecycle Manager. Puede habilitar esta funcionalidad para las nuevas instalaciones de IBM Security Key Lifecycle Manager.

IBM Security Key Lifecycle Manager da soporte a las siguientes tarjetas criptográficas:

- `SafeNet Luna SA 4.5`
- `SafeNet Luna SA 5.0`
- `SafeNet Luna SA 6.1`
- `nCipher nShield Connect 1500`
- `IBM 4765 PCIe Cryptographic Coprocessor`

Nota:

- Únicamente se pueden utilizar los dispositivos `SafeNet Luna SA 4.5`, `SafeNet Luna SA 5.0`, `SafeNet Luna SA 6.1` e `IBM 4765 PCIe Cryptographic Coprocessor` cuando el almacén de claves no está definido en IBM Security Key Lifecycle Manager. Estas tarjetas no permiten la importación de claves desde fuera.
- La tarjeta `IBM 4765 PCIe Cryptographic Coprocessor` sólo está soportada para las opciones siguientes de criptografía `PKCS#11`:
  - Convertir una clave de software de 128 bits o 256 bits de AES a una clave de hardware (`PKCS#11`) de AES
  - Generar una clave de 128 y 256 de bits de AES
  - Cifrar y descifrar datos utilizando una clave AES y un cifrado AES/ECB/NoPadding
  - Almacenar y recuperar una clave AES en o desde un almacén de claves `PKCS11IMPLKS` (`PKCS#11`)

Puede utilizar los siguientes parámetros de configuración para definir HSM:

- **`pkcs11.pin`**
- **`pkcs11.config`**
- **`useMasterKeyInHSM`**

Para obtener detalles de los parámetros de configuración de HSM, consulte los temas Referencia en la documentación de IBM Security Key Lifecycle Manager.

Archivos de configuración de HSM de ejemplo

Ejemplo de archivo de configuración de Sample HSM para SafeNet Luna SA 4.5, 5.0 y 6.1

```
#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
}
```

Nota: Para el parámetro **name**, siempre debe especificar el valor TKLM.

Archivo de configuración de HSM de ejemplo para nCipher nShield Connect 1500

```
# 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
}
```

Nota: Para el parámetro **name**, siempre debe especificar el valor TKLM.

Configuración de los parámetros de HSM

Debe utilizar los parámetros de configuración de **pkcs11.pin**, **pkcs11.config** y **useMasterKeyinHSM** para definir Hardware Security Module.

Procedimiento

1. Instale y configure el HSM según las instrucciones de los fabricantes de HSM.
2. Añada los parámetros **pkcs11.pin**, **pkcs11.config** y **useMasterKeyinHSM** al archivo de configuración de IBM Security Key Lifecycle Manager. Puede utilizar el siguiente mandato de CLI o interfaz REST para añadir el parámetro:

   Interfaz de línea de mandatos

   ```
   print AdminTask.tklmConfigUpdateEntry('[-name pkcs11.pin -value
   <hsm pin>]')

   print AdminTask.tklmConfigUpdateEntry('[-name pkcs11.config -value
   <hsm config file>]')

   print AdminTask.tklmConfigUpdateEntry('[-name useMasterKeyinHSM -value
   <true | false>]')
   ```

   Interfaz REST

   ```
   PUT https://localhost:<puerto>/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:<puerto>/SKLM/rest/v1/configProperties
   Content-Type: application/json
   Accept: application/json
   Authorization: SKLMAuth authId=139aeh34567m
   Accept-Language: en
   { "pkcs11.config" : "<hsm config file>"}

   PUT https://localhost:<puerto>/SKLM/rest/v1/configProperties
   Content-Type: application/json
   Accept: application/json
   Authorization: SKLMAuth authId=139aeh34567m
   Accept-Language: en
   { "useMasterKeyinHSM" : "<true | false>"}
   ```

   Nota: *<hsm pin>* es el PIN para HSM. *<archivo config hsm>* es la vía de acceso y nombre de archivo completos del archivo de configuración de HSM. Por ejemplo: C:\Program Files\IBM\WebSphere\AppServer\sklm\config\LunaSA.cfg.
3. Reinicie IBM Security Key Lifecycle Manager.

Requisitos de configuración para utilizar HSM

Debe validar la instalación de HSM con las herramientas que el cliente de HSM proporciona tras instalar HSM según las instrucciones del fabricante. IBM Security Key Lifecycle Manager da soporte al cliente de HSM de 64 bits.

- Siga los siguientes pasos para validar la instalación de HSM:
  - Cree una clave simétrica con **ckdemo** o **kSafe**.

kSafe es una herramienta incluida con la tarjeta nCipher nShield Connect 1500. **ckdemo** viene con la tarjeta SafeNet Luna SA 4.5, con la tarjeta SafeNet Luna SA 5.0 y con la tarjeta SafeNet Luna SA 6.1.

  - Liste la clave.
  - Suprima la clave.
- La tarjeta nCipher nShield Connect 1500 requiere que el archivo cknfastrc contenga la siguiente configuración:

  ```
  CKNFAST_OVERRIDE_SECURITY_ASSURANCES=import;
  ```

  Nota: Si el archivo cknfastrc no existe en el sistema, cree el archivo y configúrelo. Guarde este archivo en la ubicación mencionada en la documentación de HSM.
- La copia de seguridad o réplica de IBM Security Key Lifecycle Manager no realiza la copia de seguridad de la clave maestra cuando se encuentra en el HSM. Para realizar una copia de seguridad del HSM, siga las instrucciones de la documentación de HSM. Debe realizar la copia de seguridad del HSM porque la pérdida de la clave maestra puede resultar en la pérdida de todas las claves de IBM Security Key Lifecycle Manager.
- Utilice la tarjeta SafeNet Luna SA 4.5, la tarjeta SafeNet Luna SA 5.0 y la tarjeta SafeNet Luna SA 6.1 sólo cuando el almacén de claves no esté definido en IBM Security Key Lifecycle Manager. Estas tarjetas no permiten la importación de claves desde fuera.
- Para clonar IBM Security Key Lifecycle Manager, el HSM de los distintos sistemas deben utilizar la misma clave maestra. Si está utilizando un HSM conectado a la red, asegúrese de que todos los clientes para el HSM estén señalando a la misma área en la red de HSM.

Configuración de LDAP

Puede configurar los usuarios de IBM Security Key Lifecycle Manager en cualquier repositorio LDAP, tal como IBM Security Directory Server o Microsoft Active Directory, para acceder al servidor de IBM Security Key Lifecycle Manager.

Se debe añadir y configurar el repositorio de usuarios de LDAP en el repositorio federado de WebSphere Application Server. IBM Security Key Lifecycle Manager utiliza los grupos de aplicaciones como medio para imponer la autorización basada en roles para las funciones de IBM Security Key Lifecycle Manager. Para que un usuario de IBM Security Key Lifecycle Manager ejecute las funciones de IBM Security Key Lifecycle Manager en un repositorio de usuarios de LDAP, el usuario debe ser miembro de un grupo de aplicaciones de IBM Security Key Lifecycle Manager específico.

Cuando se instala IBM Security Key Lifecycle Manager, los usuarios y grupos de aplicaciones se crean en un repositorio basado en archivos predeterminado en el repositorio federado de WebSphere Application Server. Cuando se añade un repositorio de usuarios LDAP al repositorio federado de WebSphere Application Server, se debe hacer que los usuarios de LDAP sean miembros de los grupos de aplicaciones de IBM Security Key Lifecycle Manager.No es posible hacer que los usuarios de LDAP sean miembros de los grupos en el repositorio basado en archivos predeterminado.

Tampoco es posible la pertenencia a grupos de repositorios cruzados entre un repositorio basado en archivos y un repositorio LDAP. Sin embargo, es posible la pertenencia a grupos de repositorios cruzados entre un repositorio LDAP y un

repositorio basado en una base de datos. Por lo tanto, cree un repositorio basado en una base de datos y cree todos los grupos de aplicaciones de IBM Security Key Lifecycle Manager en este repositorio. Se eliminan los grupos de aplicaciones que existían en el repositorio basado en archivos.

Después de crear el repositorio basado en una base de datos y añadir a este repositorio los grupos de aplicaciones de IBM Security Key Lifecycle Manager, los usuarios del repositorio LDAP se pueden convertir en miembros de los grupos de aplicaciones de IBM Security Key Lifecycle Manager en el repositorio basado en la base de datos. A continuación, el usuario puede iniciar una sesión en la aplicación de IBM Security Key Lifecycle Manager y ejecutar las funciones de aplicación de IBM Security Key Lifecycle Manager.

Para integrar LDAP con IBM Security Key Lifecycle Manager, puede utilizar cualquiera de los siguientes métodos de configuración:

- mediante WebSphere Integrated Solutions Console. Para obtener más información, consulte Integración de LDAP mediante WebSphere Integrated Solutions Console.
- Mediante la ejecución de scripts de configuración de LDAP. Para obtener más información, consulte Ejecución de los scripts de configuración de LDAP.

Integración de LDAP mediante WebSphere Integrated Solutions Console

Antes de integrar LDAP con IBM Security Key Lifecycle Manager mediante WebSphere Integrated Solutions Console, debe ejecutar las tareas de copia de seguridad.

Requisitos previos para la integración de LDAP

Podría necesitar restaurar los siguientes datos al estado anterior a la ejecución de los mandatos de configuración de LDAP:

- Datos de configuración de WebSphere Application Server para IBM Security Key Lifecycle Manager
- Datos de aplicación de IBM Security Key Lifecycle Manager

Ejecute los siguientes pasos para realizar una copia de seguridad de los datos.

1. Haga una copia de seguridad del perfil de IBM Security Key Lifecycle Manager (KLMProfile) en WebSphere Application Server:
   a. En el directorio `WAS_HOME/bin`, detenga la aplicación WebSphere Application Server.
   b. Ejecute el siguiente mandato.

      Windows

      ```
      <WAS_HOME>\bin\manageProfiles.bat -backupProfile -profileName
      KLMProfile -backupFile <vía_a_archivo>
      ```

      ```
      C:\Program Files\IBM\WebSphere\AppServer\bin\manageProfiles.bat
      backupProfile -profileName KLMProfile -backupFile
      :\SKLM_WAS_ProfileBackup
      ```

      Linux

      ```
      <WAS_HOME>/bin/manageprofiles.sh -backupProfile -profileName
      KLMProfile -backupFile <vía_a_archivo>
      ```

      ```
      /opt/IBM/WebSphere/AppServer/bin/manageprofiles.sh -backupProfile
      profileName KLMProfile -backupFile /root/SKLM_WAS_ProfileBackup
      ```

   c. Inicie WebSphere Application Server.

2. Realice una copia de seguridad de los datos de la aplicación IBM Security Key Lifecycle Manager.

   Utilice la interfaz gráfica de usuario, la interfaz de línea de mandatos o la interfaz REST para realizar una copia de seguridad de los archivos más importantes de IBM Security Key Lifecycle Manager.

Para obtener más información sobre el mandato **manageprofiles**, consulte http://www.ibm.com/support/knowledgecenter/SSEQTP_9.0.0/com.ibm.websphere.base.doc/ae/rxml_manageprofiles.html.

Integración de LDAP mediante WebSphere Integrated Solutions Console

Los usuarios de IBM Security Key Lifecycle Manager se pueden configurar en cualquiera de los repositorios LDAP como, por ejemplo, IBM Security Directory Server o Microsoft Active Directory para acceder al servidor de IBM Security Key Lifecycle Manager y llamar a mandatos de CLI y API de servidor.

Antes de empezar

Consulte "Configuración de LDAP" en la página 211 para obtener información sobre los requisitos previos.

Procedimiento

1. Añada el repositorio LDAP al repositorio federado. Consulte "Adición de un repositorio de LDAP al repositorio federado" en la página 214 para obtener las instrucciones.
2. Cree la base de datos para la configuración de LDAP.
   a. Abra la ventana de mandatos de DB2.
   b. Ejecute el mandato siguiente para crear la base de datos.

      ```
      db2  create database USERDB31 using codeset UTF-8 territory US
      ```
3. Actualice el origen de datos desde la WebSphere Integrated Solutions Console con el nombre `jndi jdbc/wimXADS`. Consulte "Actualización de un origen de datos de WebSphere Integrated Solutions Console" en la página 215 para obtener las instrucciones.
4. Reinicie WebSphere Application Server.
5. Copie `db2jcc.jar and db2jcc_license_cu.jar` desde la carpeta `DB2SKLMV301` a la carpeta *WAS_HOME*`/lib`.

   Vía de acceso de `DB2SKLMV301`:

   Windows
   drive`:\Program Files\IBM\DB2SKLMV301\java`

   Linux *path*`/IBM/DB2SKLMV301/java`

   La definición predeterminada de la variable *WAS_HOME* habitualmente es:

   Windows
   `C:\Program Files\IBM\WebSphere\AppServer`

   Linux `/opt/IBM/WebSphere/AppServer`
6. Cree un repositorio basado en una base de datos para alojar todos los grupos de aplicaciones de IBM Security Key Lifecycle Manager. Consulte "Creación de un repositorio basado en una base de datos" en la página 215 para obtener las instrucciones.
7. Desde WebSphere Integrated Solutions Console añada correlaciones entre roles de seguridad y usuarios/grupos y correlacione el rol de administrador con

klmGUICLIAccessGroup. Consulte "Adición de roles de usuario de seguridad desde WebSphere Integrated Solutions Console" en la página 217 para obtener las instrucciones.

8. Reinicie WebSphere Application Server.
9. Añada usuarios de LDAP a los grupos de aplicaciones de IBM Security Key Lifecycle Manager. Consulte "Adición de usuarios de LDAP a grupos de aplicaciones de IBM Security Key Lifecycle Manager" en la página 218 para obtener las instrucciones.
10. Realice una copia de seguridad de la aplicación IBM Security Key Lifecycle Manager. También se realizará una copia una copia de seguridad de los datos en el repositorio basado en una base de datos.

Qué hacer a continuación

Después de que LDAP está configurado, se deben efectuar algunas tareas más. Para obtener más información, consulte "Tareas posteriores a la configuración de LDAP para dar soporte a la integración de LDAP" en la página 222

Adición de un repositorio de LDAP al repositorio federado:

Se debe añadir un repositorio LDAP al repositorio federado para configurar un repositorio LDAP como, por ejemplo IBM Security Directory Server o Microsoft Active Directory en el repositorio federado.

Acerca de esta tarea

Para obtener más información sobre la configuración de los valores de LDAP en una configuración de repositorio federada, consulte http://www-01.ibm.com/support/knowledgecenter/api/redirect/wasinfo/v8r5/topic/com.ibm.websphere.base.doc/ae/twim_ldap_settings.html.

Procedimiento

1. Inicie una sesión en WebSphere Integrated Solutions Console (`https://localhost:9093/ibm/console/logon.jsp`) como el usuario `wasadmin`.
2. En la barra de navegación, pulse **Seguridad** > **Seguridad global**.
3. Bajo Repositorio de cuentas de usuario, seleccione **Repositorios federados** en la lista desplegable de **Definiciones de reino disponibles**.
4. Pulse **Configurar**.
5. En la página **Seguridad global** > **Repositorios federados**, pulse **Añadir repositorios (LDAP, personalizado, etc...)**.
6. En la página **Seguridad global** > **Repositorios federados** > **Referencia de repositorio**, seleccione **Repositorio LDAP** de la lista desplegable **Nuevo repositorio**.
7. En la página **Seguridad global** > **Repositorios federados** > **Referencia de repositorio** > **Nuevo**, especifique el nombre del repositorio LDAP y otros detalles de acuerdo con sus requisitos.
8. Pulse **Aceptar**.
9. Pulse **Guardar** para guardar la configuración.
10. En la página **Seguridad global** > **Repositorios federados** > **Referencia de repositorio**, especifique el valor para **Nombre distinguido exclusivo de la entrada base (o padre) de los repositorios federados**.
11. Pulse **Aceptar**.

12. En la página **Seguridad global** > **Repositorios federados**, seleccione el enlace al repositorio LDAP que ha creado.
13. En la página **Seguridad global** > **Repositorios federados** > **<Nombre de repositorio de LDAP>**, bajo Propiedades adicionales, seleccione los tipos de entidad `Repositorios federados` para el enlace de correlación de clases de objeto de LDAP.

    En la página **Seguridad global** > **Repositorios federados** > **<Nombre de repositorio federado>** > **Correlación de tipos de entidad de repositorios federados con clases de objeto de LDAP**, asegúrese de que cada tipo de entidad que se lista se correlaciona con las clases de objeto correctas. Modifique los valores de acuerdo con sus requisitos.
14. En la página **Seguridad global** > **Repositorios federados**, seleccione el enlace al repositorio LDAP que ha creado. Bajo Propiedades adicionales, seleccione **Definición de atributo de grupo**.
15. En la página **Seguridad global** > **Repositorios federados** > **<Nombre de repositorio de LDAP>** > **Definición de atributo de grupo**, bajo Propiedades adicionales, seleccione **Atributos de miembro**.
16. En la página **Seguridad global** > **Repositorios federados** > **<Nombre de repositorio de LDAP>** > **Definición de atributos de grupo** > **Atributos de miembro**, asegúrese de que el atributo de miembro `uniqueMember` está correlacionado con la clase de objeto correcta. Si este atributo no está presente, cree un atributo y correlaciónelo con la clase de objeto correcta.

Qué hacer a continuación

Crear un origen de datos desde WebSphere Integrated Solutions Console.

Actualización de un origen de datos de WebSphere Integrated Solutions Console:

Debe actualizar el origen de datos para el repositorio basado en una base de datos para alojar los grupos de aplicaciones de IBM Security Key Lifecycle Manager. El repositorio basado en una base de datos utiliza las tablas que se crean en la base de datos de la aplicación de IBM Security Key Lifecycle Manager.

Procedimiento

1. Inicie sesión para actualizar el origen de datos desde WebSphere Integrated Solutions Console (`https://localhost:9093/ibm/console/logon.jsp`) como usuario `wasadmin`.
2. En la barra de navegación, pulse **Recursos** > **JDBC** > **Orígenes de datos**.
3. Pulse **Origen de datos WIM** para editar los valores de base de datos.
4. Actualice el nombre de base de datos con `USERDB31` en la sección **Propiedades de origen de datos comunes y necesarias**.
5. Pulse **Aceptar**.
6. Pulse **Guardar** para guardar la configuración.

Creación de un repositorio basado en una base de datos:

El repositorio basado en una base de datos se crea para alojar todos los grupos de aplicaciones de IBM Security Key Lifecycle Manager y para eliminar todos los grupos de aplicaciones de IBM Security Key Lifecycle Manager del repositorio basado en archivos. Debe añadir los grupos de aplicaciones de IBM Security Key

Lifecycle Manager al repositorio basado en una base de datos y actualizar el repositorio federado de WebSphere Application Server con un repositorio LDAP.

Procedimiento

1. Vaya a la carpeta <*SKLM_INSTALL_HOME*>\bin.

   Nota: Todos los scritps python .py se encuentran en el directorio <*SKLM_INSTALL_HOME*>\bin\LDAPIntegration.
   La vía <*SKLM_INSTALL_HOME*>, habitualmente es,

   Windows
   C:\Program Files\IBM\SKLMV301

   Linux opt/IBM/SKLMV301

2. Ejecute los siguientes mandatos:

   wsadmin.bat -user *usuario_wasadmin* -password *contraseña_wasadmin* -lang jython -f *SKLM_INSTALL_HOME*\bin\LDAPIntegration\createDBRepos.py *WAS_HOME LDAP_DBNAME SKLM_DBUSER SKLM_DBUSERPASSWD SKLM_DBPORT#*

   Notas: En plataformas Linux, utilice **wsadmin.sh** en lugar de **wsadmin.bat**

   Durante la instalación de IBM Security Key Lifecycle Manager, si utilizó los valores predeterminados,

   ```
   LDAP_DBNAME = USERDB31
   SKLM_DBUSER = SKLMDB31
   SKLM_DBPORT# = 50050
   ```

   SKLM_DBUSERPASSWD es la contraseña de la base de datos de IBM Security Key Lifecycle Manager que especificó durante la instalación.

3. Ejecute el siguiente mandato.

   wsadmin.bat -user <usuario_wasadmin> -password <contraseña_wasadmin> -lang jython -f <*SKLM_INSTALL_HOME*>\bin\LDAPIntegration\removeGroupsFromDefRepos.py

4. Desde WebSphere Integrated Solutions Console, modifique el Correlación de roles de seguridad con usuarios y grupos para eliminar la correlación del rol de administrador con klmGUICLIAccessGroup.
   a. Inicie una sesión en WebSphere Integrated Solutions Console (https://localhost:9093/ibm/console/logon.jsp).
   b. En la barra de navegación, pulse **Aplicaciones** > **Tipos de aplicación** > **Tipos de aplicación** > **Aplicaciones empresariales de WebSphere**.
   c. Pulse el enlace **sklm_kms**.
   d. En la página **Aplicaciones empresariales** > **sklm_kms**, bajo la sección Propiedades de detalle, pulse el enlace **Correlación de roles de seguridad con usuarios y grupos**.
   e. En la página **Aplicaciones empresariales** > **sklm_kms** > **Correlación de roles de seguridad con usuarios y grupos**, seleccione el rol **administrator**.
   f. Pulse **Correlacionar grupos**.
   g. Seleccione **klmGUICLIAccessGroup** en la lista y pulse el botón con la flecha hacia la izquierda para eliminar **klmGUICLIAccessGroup** de la lista.
   h. Pulse **Aceptar**.
   i. Pulse el enlace **Guardar** para guardar la configuración.
5. Reinicie WebSphere Application Server
6. Ejecute el siguiente mandato.

   wsadmin.bat -user <usuario_wasadmin> -password <contraseña_wasadmin> -lang jython -f <*SKLM_INSTALL_HOME*>\bin\LDAPIntegration\addGroupsToDBRepos.py

7. Ejecute el siguiente mandato.

```
wsadmin.bat -user <usuario_wasadmin> -password <contraseña_wasadmin> -lang jython
-f <SKLM_INSTALL_HOME>\bin\LDAPIntegration\updateLDAPReposConfig.py <Nombre_LDAPRepos
- nombre utilizado con anterioridad al crear el repositorio LDAP>
```

Qué hacer a continuación

Añadir correlaciones entre roles de seguridad y usuarios/grupos y correlacionar el rol de administrador con `klmGUICLIAccessGroup`.

Adición de roles de usuario de seguridad desde WebSphere Integrated Solutions Console:

Debe añadir una correlación rol de seguridad con usuarios y grupos, y correlacionar un rol de administrador con `klmGUICLIAccessGroup` para integrar IBM Security Key Lifecycle Manager con los repositorios de usuarios de LDAP.

Acerca de esta tarea

Procedimiento

1. Inicie una sesión en Integrated Solutions Console (`https://localhost:9083/ibm/console/logon.jsp`) como el usuario `wasadmin`.
2. En la barra de navegación, pulse **Aplicaciones** > **Tipos de aplicación** > **Tipos de aplicación** > **Aplicaciones empresariales de WebSphere**.
3. Pulse el enlace **sklm_kms**.
4. En la página **Aplicaciones empresariales** > **sklm_kms**, bajo la sección Propiedades de detalle, pulse el enlace **Correlación de roles de seguridad con usuarios y grupos**.
5. En la página **Aplicaciones empresariales** > **sklm_kms** > **Correlación de roles de seguridad con usuarios y grupos**, seleccione el rol **administrator**.
6. Pulse **Correlacionar grupos**.
7. En la página **Aplicaciones empresariales** > **sklm_kms** > **Correlación de roles de seguridad con usuarios y grupos** > **Correlacionar usuarios/grupos**:
   a. Bajo la sección Buscar y seleccionar grupos, en el recuadro de texto **Serie de búsqueda**, especifique `klmGUICLIAccessGroup`.
   b. Pulse **Buscar**.
   c. Seleccione `klmGUICLIAccessGroup` de la lista y pulse con el botón de flecha hacia la derecha.

      `klmGUICLIAccessGroup` se añadirá a la lista de **Seleccionado**.
   d. Pulse **Aceptar**.
   e. Pulse **Aceptar** en la página **Aplicaciones empresariales** > **sklm_kms** > **Correlación de roles de seguridad con usuarios y grupos**.
8. Pulse el enlace **Guardar** para guardar la información de configuración.

Qué hacer a continuación

Reinicie WebSphere Application Server.

Adición de usuarios de LDAP a grupos de aplicaciones de IBM Security Key Lifecycle Manager:

Debe añadir usuarios de LDAP a los grupos de aplicaciones de IBM Security Key Lifecycle Manager para integrar IBM Security Key Lifecycle Manager con repositorios de usuarios de LDAP.

Procedimiento

1. Vaya a la carpeta *<SKLM_INSTALL_HOME>*/bin.

   Nota: Todos los scritps python .py se encuentran en el directorio *<SKLM_INSTALL_HOME>*/bin/LDAPIntegration.
   La vía *<SKLM_INSTALL_HOME>*, habitualmente es,

   Windows
   C:\Program Files\IBM\SKLMV301

   Linux /opt/IBM/SKLMV301
2. Ejecute los siguientes mandatos:

   ```
   wsadmin.bat -user <usuario_wasadmin> -password <contraseña_waasadmin>  -lang jython -f
   addLDAPUserToGroup.py <nombre_exclusivo_usuario> <nombre_grupo>
   ```

   Notas: En plataformas Linux, utilice **wsadmin.sh** en lugar de **wsadmin.bat**

   El nombre exclusivo de usuario es el componente Nombre exclusivo en el registro LDAP. Por ejemplo:

   ```
   uid=001,c=in,ou=bluepages,o=ibm.com
   ```

   Para un usuario de LDAP que necesita acceso administrativo de IBM Security Key Lifecycle Manager, el usuario debe ser miembro de klmGUICLIAccessGroup y klmSecurityOfficerGroup. Ejecute el siguiente mandato:

   ```
   wsadmin.bat -user <usuario_wasadmin> -password <contraseña_wasadmin> -lang jython -f
   <SKLM_INSTALL_HOME>\bin\LDAPIntegration\addLDAPUserToGroup.py
   <nombre usuario único> klmGUICLIAccessGroup
   ```

Qué hacer a continuación

Realizar una copia de seguridad de la aplicación IBM Security Key Lifecycle Manager.

Ejecución de scripts de configuración de LDAP

Ejecute los scripts de configuración de LDAP para integrar fácilmente IBM Security Key Lifecycle Manager con LDAP para configurar usuarios de IBM Security Key Lifecycle Manager en cualquiera de los repositorios de LDAP, tales como IBM Security Directory Server o Microsoft Active Directory.

Acerca de esta tarea

Procedimiento

1. En las propiedades de config.py, actualice **ip**, **port**, **LDAP_server_type** y otras propiedades del entorno. Para ver una descripción de las propiedades de config.py, consulte Integración de LDAP mediante scripts de configuración.

   Windows
   SKLM_INSTALL_HOME\bin\LDAPIntegration\config.py

   C:\Program Files\IBM\SKLMV301\bin\LDAPIntegration\config.py

Linux *SKLM_INSTALL_HOME*/bin/LDAPIntegration/config.py

opt/IBM/SKLMV301/bin/LDAPIntegration/config.py

Nota: Para ejecutar los scripts con la configuración predeterminada, solo tiene que definir las propiedades **ip** y **port**.

2. Cree la base de datos para la configuración de LDAP.
   a. Abra la ventana de mandatos de DB2.
   b. Ejecute el mandato siguiente para crear la base de datos.

      ```
      db2  create database USERDB31 using codeset UTF-8 territory US
      ```

3. Actualice el origen de datos desde la WebSphere Integrated Solutions Console con el nombre jndi jdbc/wimXADS. Consulte "Actualización de un origen de datos de WebSphere Integrated Solutions Console" en la página 215 para obtener las instrucciones.
4. Cree un repositorio basado en una base de datos para alojar todos los grupos de aplicaciones de IBM Security Key Lifecycle Manager.
   a. Vaya a la carpeta <*WAS_HOME*>\bin.

      Windows
      C:\Program Files\IBM\WebSphere\AppServer\bin

      Linux /opt/IBM/WebSphere/AppServer/bin

   b. Abra un indicador de mandatos y ejecute los siguientes mandatos.

      ```
      wsadmin.bat -user <usuario_wasadmin> -password <contraseña_wasadmin> -lang jython -f
      <SKLM_INSTALL_HOME>\bin\LDAPIntegration\createDBRepos.py <WAS_HOME> <LDAP_DBNAME>
      <SKLM_DBUSER> <SKLM_DBUSERPASSWD> <SKLM_DBPORT#>
      ```

      Notas: En plataformas Linux, utilice **wsadmin.sh** en lugar de **wsadmin.bat**

      Durante la instalación de IBM Security Key Lifecycle Manager, si utilizó los valores predeterminados,

      ```
      LDAP_DBNAME = USERDB31
      SKLM_DBUSER = sklmdb31
      SKLM_DBPORT# = 50050
      ```

      SKLM_DBUSERPASSWD es la contraseña de la base de datos de IBM Security Key Lifecycle Manager que especificó durante la instalación.
5. Ejecute los scripts de configuración sklmLDAPConfigure y addLDAPUserToGroup.

   Windows
   Vaya al directorio *SKLM_INSTALL_HOME*\bin\LDAPIntegration y ejecute los siguientes scripts:

   ```
   sklmLDAPConfigure.bat WAS_HOME SKLM_INSTALL_HOME WAS_ADMIN WASAdmin_PASSWORD SKLM_ADMI
   addLDAPUserToGroup.bat WAS_HOME SKLM_INSTALL_HOME WAS_ADMIN WASADMIN_PASS USER_UNIQUE_
   ```

   Por ejemplo:

   ```
   sklmLDAPConfigure.bat "c:\Program Files\IBM\WebSphere\AppServer" "c:\Program Files\IBM
   addLDAPUserToGroup.bat "c:\Program Files\IBM\WebSphere\AppServer" "c:\Program Files\IB
   ```

   Linux Vaya al directorio *SKLM_INSTALL_HOME*/bin/LDAPIntegration y ejecute los siguientes scripts:

   ```
   sklmLDAPConfigure.sh WAS_HOME SKLM_INSTALL_HOME WAS_ADMIN WASAdmin_PASSWORD SKLM_ADMIN
   addLDAPUserToGroup.sh WAS_HOME SKLM_INSTALL_HOME WAS_ADMIN WASADMIN_PASS USER_UNIQUE_N
   ```

   Por ejemplo:

   ```
   sklmLDAPConfigure.sh "/opt/IBM/WebSphere/AppServer" "/opt/IBM/SKLMV301" wasadmin WAS@a
   addLDAPUserToGroup.sh "/opt/IBM/WebSphere/AppServer" "/opt/IBM/SKLMV301" wasadmin WAS@
   ```

WAS_HOME
El directorio en el que se ha instalado WebSphere Application Server para IBM Security Key Lifecycle Manager.

Windows
`unidad:\Program Files\IBM\WebSphere\AppServer`

Linux `path/IBM/WebSphere/AppServer`

SKLM_INSTALL_HOME
El directorio en el que se ha instalado IBM Security Key Lifecycle Manager.

Windows
drive`:\Program Files\IBM\SKLMV301`

Linux

WAS_ADMIN
Nombre de usuario de WebSphere Application Server para IBM Security Key Lifecycle Manager.

WAS_PASS
Contraseña de WebSphere Application Server para IBM Security Key Lifecycle Manager.

USER_UNIQUE_NAME
El usuario de LDAP al que desea asignar el rol de administrador de IBM Security Key Lifecycle Manager.

SKLM_ADMIN
Administrador de IBM Security Key Lifecycle Manager.

SKLM_ADMIN_PASS
Contraseña de IBM Security Key Lifecycle Manager administrator.

directorio_instalación_DB2
El directorio en el que está instalado DB2.

Windows
drive`:\Program Files\IBM\DB2SKLMV301`

Linux *path*`/IBM/DB2SKLMV301`

Para la instalación no root en Linux, la vía de acceso es: *<non_root_user_home _directory>*`/IBM/DB2SKLMV301`

Qué hacer a continuación

Después de la configuración de LDAP, se deben efectuar algunas tareas más. Consulte “Tareas posteriores a la configuración de LDAP para dar soporte a la integración de LDAP” en la página 222 para obtener más información.

Integración de LDAP mediante scripts de configuración

Puede ejecutar los scripts de configuración desde una línea de mandatos para integrar IBM Security Key Lifecycle Manager con LDAP mediante los valores predeterminados de configuración definidos en el archivo de propiedades `config.py`.

El ejemplo siguiente muestra las propiedades definidas en el archivo `config.py`.

```
serie de importación, sys
LDAP_server_type="IDS"
login_id="uid"
```

```
ip="9.x.x.x"
port="389"
gr_name="Group"
pr_name="PersonAccount"
gr_obj_class="groupOfUniqueNames"
pr_obj_class="person"
mem_name="uniqueMember"
mem_obj_class="groupOfUniqueNames"
base_entry="o=ibm.com"
scope="direct"
```

La tabla siguiente contiene una descripción de las propiedades del archivo `config.py`.

Propiedad	Descripción
LDAP_server_type	Tipo de servidor LDAP que se está utilizando. De forma predeterminada, se especifica IDS.
login_id	Nombre de la propiedad que se utiliza para el inicio de sesión. Por ejemplo, `uid` y `mail`.
ip	Dirección IP o nombre de host del servidor LDAP primario.
port	Número de puerto del servidor LDAP.
gr_name	Nombre del tipo de entidad.
pr_name	Nombre del tipo de entidad.
gr_obj_class	Clase de objeto del tipo de entidad.
pr_obj_class	Clase de objeto del tipo de entidad.
mem_name	Nombre del atributo de LDAP que se utiliza como atributo de miembro de grupo. Por ejemplo, `member` o `uniqueMember`.
mem_obj_class	Clase de objeto de grupo que contiene el atributo de miembro. Por ejemplo, `groupOfNames` o `groupOfUniqueNames`. Si no define este parámetro, el atributo de miembro se aplica a todas las clases del objeto de grupo.
scope	El ámbito del atributo de miembro. Especifique cualquiera de los siguientes valores para el parámetro. **direct** Atributo de miembro que solo contiene los miembros directos. Por lo tanto, este valor hace referencia al miembro contenido directamente en el grupo, no a los contenidos a través del grupo anidado. Por ejemplo, si `Group1` contiene `Group2` y `Group2` contiene `User1`, entonces `Group2` es un miembro directo de `Group1`, pero `User1` no es un miembro directo de `Group1`. Tanto `member` como `uniqueMember` son atributos de miembro directo. **nested** Atributo de miembro que contiene miembros directos y miembros anidados.

Si detecta problemas durante la integración de LDAP cuando se utilizan los scripts para ejecutar la tarea de configuración, quizás tenga que revisar los archivos de registro que se encuentran en *<SKLM_INSTALL_HOME>*`/bin/LDAPIntegration` para diagnosticar el problema.

- `sklmldapconf.log`
- `ldaplog.out`

Para obtener más información sobre cómo ejecutar los scripts de configuración, consulte el apartado Ejecución de los scripts de configuración de LDAP.

Tareas posteriores a la configuración de LDAP para dar soporte a la integración de LDAP

Después de configurar LDAP, podría tener que realizar tareas adicionales para asegurarse de que la integración de IBM Security Key Lifecycle Manager con los repositorios de usuarios de LDAP ha finalizado de forma satisfactoria.

Notas importantes después de configurar LDAP

1. Después de configurar LDAP, el usuario `sklmadmin` que existía en el repositorio de usuarios basado en archivos predeterminado no podrá acceder a la aplicación IBM Security Key Lifecycle Manager.
2. Después de configurar LDAP, se deben utilizar los mandatos **wsadmin** para crear grupos y asignar roles de IBM Security Key Lifecycle Manager. No se puede utilizar WebSphere Integrated Solutions Console. Ejecute los siguientes pasos para añadir grupos y asignar un rol a un grupo:
   a. Vaya a *<WAS_HOME>*/bin.
   b. Inicie una sesión en wsadmin utilizando el siguiente mandato:

      ```
      wsadmin.bat -user <usuario_wasadmin> -password <contraseña_wasadmin>
      -lang jython
      ```

   c. Ejecute el siguiente mandato para crear un grupo y asignar el rol:

      ```
      AdminTask.createGroup<'[-cn <nombre_grupo> -parent "o=sklmrepdb.ibm"]'>
      AdminTask.mapGroupsToAdminRole<'[-roleName <rol> -groupids
      <nombre_grupo>]'>
      ```

3. Después de configurar LDAP, podría desear restaurar la configuración de IBM Security Key Lifecycle Manager en WebSphere Application Server al estado que tenía con anterioridad a la configuración de LDAP. Para restaurar la configuración, siga estos pasos:
   a. Detenga WebSphere Application Server.
   b. Detenga, si hay, los procesos relacionados con WebSphere Application Server.
   c. Restaure la configuración del perfil de WebSphere Application Server que se tomó antes de la configuración de LDAP:
      1) Suprima de forma manual la carpeta `KLMProfile` en *<WAS_HOME>*/profiles/KLMProfile.
      2) Ejecute la opción **-validateAndUpdateRegistry** del mandato **manageProfiles**.

         Windows

         ```
         <WAS_HOME>\bin\manageProfiles.bat
         -validateAndUpdateRegistry
         ```

         Por ejemplo:

         ```
         C:\Program Files\IBM\WebSphere\AppServer\bin\
         manageProfiles.bat -validateAndUpdateRegistry
         ```

         Linux

         ```
         <WAS_HOME>/bin/manageprofiles.sh
         -validateAndUpdateRegistry
         ```

         Por ejemplo:

         ```
         /opt/IBM/WebSphere/AppServer/bin/
         manageprofiles.sh -validateAndUpdateRegistry
         ```

      3) Restaure el perfil:

Windows

<*WAS_HOME*>\bin\manageProfiles.bat -restoreProfile -backupFile <*vía_a_archivo_copia_seguridad_perfil*>

Por ejemplo: C:\Program Files\IBM\WebSphere\AppServer\bin\manageProfiles.bat -restoreProfile -backupFile C:\SKLM_WAS_ProfileBackup

Linux <*WAS_HOME*>/bin/manageprofiles.sh -restoreProfile -backupFile <*vía_a_archivo_copia_seguridad_perfil*>

Por ejemplo: /opt/IBM/WebSphere/AppServer/bin/manageprofiles.sh -restoreProfile -backupFile /root/SKLM_WAS_ProfileBackup

Para obtener información sobre el mandato **manageProfiles**, consulte http://www.ibm.com/support/knowledgecenter/SSEQTP_9.0.0/com.ibm.websphere.base.doc/ae/rxml_manageprofiles.html.

4) Inicie WebSphere Application Server.
5) Restaure la copia de seguridad de IBM Security Key Lifecycle Manager que se tomo con anterioridad a la configuración de LDAP, si es necesario.

4. No debe restaurar una copia de seguridad de la aplicación IBM Security Key Lifecycle Manager que se tomó con anterioridad a la configuración de LDAP una vez se haya realizado dicha configuración LDAP a no ser que se siga el Paso 3 en la sección **Notas importes después de la configuración de LDAP**.
5. Después de la configuración de LDAP, se crean las tablas en la base de datos de IBM Security Key Lifecycle Manager para el repositorio basado en un base de datos. Los grupos de IBM Security Key Lifecycle Manager se almacenan en estas tablas. Si el servidor de IBM Security Key Lifecycle Manager está configurado para réplica y la réplica se da en los clones configurados, también se replica el repositorio basado en una base de datos en el clon. Esto se debe a que las tablas de la base de datos del repositorio basado en una base de datos también se replican en los clones.
6. Si el servidor de IBM Security Key Lifecycle Manager (maestro) que está configurado para estregarse con los repositorios de LDAP tiene la característica de réplica habilitada, cuando la réplica se da en los clones configurados en los que LDAP no está configurado, puede configurar LDAP en el clon o no hacerlo. Si es necesario configurar LDAP en un clon, ejecute los siguientes pasos en el clon:
   a. Copie db2jcc.jar,db2jcc4.jar y db2jcc_license_cu.jar desde la carpeta DB2SKLMV301 a la carpeta <*WAS_HOME*>/lib.

      La definición predeterminada de la variable <*WAS_HOME*> habitualmente es:

      Windows

      C:\Program Files\IBM\WebSphere\AppServer

      Linux /opt/IBM/WebSphere/AppServer

   b. Vaya a <*WAS_HOME*>/bin.
      1) Inicie una sesión en wsadmin utilizando el siguiente mandato:

         ```
         wsadmin.bat -user <WASADMIN_USER> -password <WASADMIN_PASSWORD>
         -lang jython
         ```

      2) Ejecute el siguiente mandato:

```
AdminTask.deleteIdMgrDBTables<'[-schemaLocation "<WAS_HOME>/etc/wim/set
up" -databaseType db2 -dbURL "jdbc:db2://localhost:<SKLMDB_PORT>/
<LDAPDB_NAME>" -dbDriver com.ibm.db2.jcc.DB2Driver -dbAdminId
<SKLMDBADMIN_USER> -dbAdminPassword <SKLMDBADMIN_PASSWORD>
-reportSqlError true]'>
```

c. Siga el procedimiento para configurar la integración de LDAP tal como se hizo en el servidor de IBM Security Key Lifecycle Manager maestro. Consulte "Integración de LDAP mediante WebSphere Integrated Solutions Console" en la página 213 para obtener más información sobre los pasos de integración.

7. Después de que se complete la réplica entre un servidor de IBM Security Key Lifecycle Manager configurado para la integración de LDAP y un clon no configurado para la integración de LDAP, si de forma inadvertida ejecuta la integración de LDAP normal en el clon, fallará el Paso 5 en "Integración de LDAP mediante WebSphere Integrated Solutions Console" en la página 213. Debe ejecutar estos pasos:
   a. Vaya a *<WAS_HOME>*/bin.
      1) Inicie una sesión en wsadmin:

```
wsadmin.bat -user <usuario_wasadmin> -password <contraseña_wasadmin>
-lang
jython
```

      2) Ejecute el siguiente mandato:

```
AdminTask.deleteIdMgrDBTables<'[-schemaLocation "<WAS_HOME>/etc/wim/set
up" -databaseType db2 -dbURL "jdbc:db2://localhost:<SKLMDB_PORT>/
<LDAP_DBNAME>" -dbDriver com.ibm.db2.jcc.DB2Driver -dbAdminId
<SKLMDB2ADMINUSER> -dbAdminPassword <SKLMDB2ADMINUSER_PASSWORD>
-reportSqlError true]'>
```

   b. Ejecute los pasos 5 - 9 en "Integración de LDAP mediante WebSphere Integrated Solutions Console" en la página 213.

Cómo cambiar la contraseña del administrador de DB2 en servidores configurados con LDAP

Si hay en curso una restricción de caducidad de contraseña, debe cambiar la contraseña de DB2 del ID de usuario antes de que finalice el periodo de caducidad.

Acerca de esta tarea

Si el servidor IBM Security Key Lifecycle Manager está configurado con LDAP, se deben ejecutar los siguientes pasos para cambiar la contraseña del administrador de DB2.

Procedimiento

1. Asegúrese de seleccionar el recuadro de selección **Permitir operaciones si alguno de los repositorios están fuera de servicio**.
   a. Inicie sesión en la consola WebSphere Integrated Solutions Console.
   b. Pulse **Seguridad** > **Seguridad global**.
   c. En **Repositorio de cuentas de usuario** > **Definiciones de reino disponibles**, seleccione **Repositorios federados** en la lista desplegable.
   d. Pulse **Configurar**.
   e. Seleccione el recuadro de selección **Permitir operaciones si algunos de los repositorios están fuera de servicio**.

2. Ejecute los pasos que se describen en los siguientes temas para cambiar la contraseña del administrador de DB2.

   Windows
   Repita los pasos 3 - 5 en el tema "Problemas de seguridad con la contraseña de Db2 en sistemas Windows" en la página 36.

   Linux Ejecute los pasos 1 - 3 en el tema Problemas de seguridad de contraseña de Db2 en sistemas Linux o AIX.

3. Actualice los valores del repositorio federado para la conexión del repositorio de base de datos. Además, cambie la contraseña del administrador de DB2 con el mandato **updateIdMgrDBRepository AdminTask**.

   a. Si utiliza la interfaz **wsadmin** que proporciona WebSphere Application Server, especifique la sintaxis Jython.

      Windows
      ```
      wsadmin.bat -username WASAdmin -password mypwd -lang jython
      ```

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

   b. Ejecute, por ejemplo, el mandato:
      ```
      print AdminTask.updateIdMgrDBRepository ('[-id id_name -dbAdminPasswword new_password]')
      ```

      Donde id_name es SKLMDBRepos
      ```
      print AdminConfig.save()
      ```

   Para obtener más información, consulte https://www.ibm.com/support/knowledgecenter/SSAW57_9.0.0/com.ibm.websphere.nd.multiplatform.doc/ae/rxml_atidmgrrepositoryconfig.html#rxml_atidmgrrepositoryconfig__cmd46.

4. Ejecute los pasos que se describen en los siguientes temas para cambiar la contraseña del origen de datos de WebSphere Application Server.

   Windows
   Ejecute los pasos 7 - 8 en el tema "Problemas de seguridad con la contraseña de Db2 en sistemas Windows" en la página 36.

   Linux Ejecute los pasos 5 - 6 en el tema Problemas de seguridad de contraseña de Db2 en sistemas Linux o AIX.

5. Reinicie el servidor. Para obtener instrucciones sobre cómo detener e iniciar el servidor, consulte el apartado "Reinicio de IBM Security Key Lifecycle Manager server" en la página 205.

Configuraciones estándar de seguridad

Existe la posibilidad de configurar IBM Security Key Lifecycle Manager para que funcione con distintos estándares de seguridad para satisfacer los requisitos de seguridad especificados a nivel de cifrado.

Configuración del cumplimiento de FIPS en IBM Security Key Lifecycle Manager

Existe la posibilidad de activar FIPS para IBM Security Key Lifecycle Manager de forma que todas las operaciones criptográficas utilicen el proveedor IBMJCEFIPS que posee la certificación FIPS 140-2.

Procedimiento

1. Establezca la siguiente propiedad en el archivo *SKLM_HOME*/config/SKLMConfig.properties.

```
fips=on
```

Interfaz de línea de mandatos

a. Vaya al directorio <*WAS_HOME*>/bin. Por ejemplo,

Windows

```
cd unidad:\Program Files (x86)\IBM\WebSphere\
AppServer\bin
```

Linux

```
cd /opt/IBM/WebSphere/AppServer/bin
```

b. Inicie la interfaz **wsadmin** utilizando un ID de usuario autorizado, por ejemplo, SKLMAdmin. Por ejemplo,

Windows

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

Linux

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

c. Ejecute el mandato **tklmConfigUpdateEntry** para establecer la propiedad **fips** en el archivo de configuración SKLMConfig.properties.

```
print AdminTask.tklmConfigUpdateEntry ('[-name fips -value on]')
```

Interfaz REST

a. Abra un cliente REST.

b. Obtenga un identificador de autenticación de usuario exclusivo para acceder a los servicios REST de IBM Security Key Lifecycle Manager. Para obtener más información sobre el proceso de autenticación, consulte Proceso de autenticación de los servicios REST.

c. Ejecute el **Servicio REST Actualizar propiedad de configuración** para establecer la propiedad **fips** en el archivo de configuración SKLMConfig.properties. Pase el identificador de autenticación de usuario que ha obtenido en el Paso b junto con el mensaje de solicitud, como se muestra en el ejemplo siguiente.

```
PUT https://localhost:<puerto>/SKLM/rest/v1/configProperties
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth userAuthId=139aeh34567m
Accept-Language : en
{ "fips" : "on"}
```

2. Edite el archivo <*WAS_HOME*>/java_1.7.1_32/jre/lib/security/java.security y añada el proveedor IBMJCEFIPS a la lista de proveedores de seguridad tal como se muestra en el ejemplo siguiente.

Nota: Debe actualizar el archivo java.security para la versión de Java que el servidor de IBM Security Key Lifecycle Manager utiliza.

```
security.provider.1=com.ibm.crypto.fips.provider.IBMJCEFIPS
security.provider.2=com.ibm.crypto.provider.IBMJCE
security.provider.3=com.ibm.jsse.IBMJSSEProvider
security.provider.4=com.ibm.jsse2.IBMJSSEProvider2
security.provider.5=com.ibm.security.jgss.IBMJGSSProvider
security.provider.6=com.ibm.security.cert.IBMCertPath
security.provider.7=com.ibm.crypto.pkcs11.provider.IBMPKCS11
security.provider.8=com.ibm.security.cmskeystore.CMSProvider
security.provider.9=com.ibm.security.jgss.mech.spnego.IBMSPNEGO
```

Nota: Se cambia la numeración de los proveedores para añadir el proveedor IBMJCEFIPS al principio de la lista.

3. Guarde el archivo.
4. Reinicie el servidor de IBM Security Key Lifecycle Manager.

Configuración de IBM Security Key Lifecycle Manager para el cumplimiento de la Suite B

Se puede configurar a IBM Security Key Lifecycle Manager para que cumpla los estándares que la NSA (National Security Agency) de EE.UU. especifica para definir los requisitos de seguridad para el cifrado.

Acerca de esta tarea

Para habilitar el cumplimiento de la Suite B en IBM Security Key Lifecycle Manager, debe configurar el archivo de propiedades `SKLMConfig.properties` con la siguiente opción.

```
suiteB=128|192
```

Cuando configura **suiteB** con el valor 128 o 192, se añaden las siguientes propiedades al archivo de propiedades o se actualizan, si ya existen.

```
TransportListener.ssl.protocols=TLSv1.2
requireSHA2Signatures=true
autoScaleSignatureHash=true
useThisECKeySize=256(si suiteB es 128)|384(si suiteB es 192)
```

Procedimiento

1. Establezca la siguiente propiedad en el archivo *SKLM_HOME*/config/SKLMConfig.properties.

   ```
   suiteB=128|192
   ```

   - El valor 128 especifica el nivel mínimo de 128 bits de seguridad.
   - El valor 192 especifica el nivel mínimo de 192 bits de seguridad.

   Interfaz de línea de mandatos

   a. Vaya al directorio WAS_HOME/bin. Por ejemplo,

      Windows

      ```
      cd unidad:\Program Files\IBM\WebSphere\AppServer\bin
      ```

      Linux

      ```
      cd /opt/IBM/WebSphere/AppServer/bin
      ```

   b. Inicie la interfaz **wsadmin** utilizando un ID de usuario autorizado, por ejemplo, SKLMAdmin. Por ejemplo,

      Windows

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

      Linux

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

   c. Ejecute el mandato **tklmConfigUpdateEntry** para establecer la propiedad **suiteB** en el archivo de configuración SKLMConfig.properties.

      ```
      print AdminTask.tklmConfigUpdateEntry ('[-name suiteB -value 128|192]')
      ```

   Interfaz REST

   a. Abra un cliente REST.

   b. Obtenga un identificador de autenticación de usuario exclusivo para acceder a los servicios REST de IBM Security Key Lifecycle

Manager. Para obtener más información sobre el proceso de autenticación, consulte Proceso de autenticación de los servicios REST.

c. Ejecute el **Servicio REST Actualizar propiedad de configuración** para establecer la propiedad **suiteB** en el archivo de configuración SKLMConfig.properties. Pase el identificador de autenticación de usuario que ha obtenido en el Paso b junto con el mensaje de solicitud, como se muestra en el ejemplo siguiente.

```
PUT https://localhost:puerto/SKLM/rest/v1/configProperties
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth userAuthId=139aeh34567m
Accept-Language : en
{ "suiteB" : "128|192"}
```

2. Reinicie el servidor.

Qué hacer a continuación

Seleccione el certificado que utiliza el algoritmo ECDSA porque el cumplimiento de la Suite B requiere el certificado ECDSA para que la comunicación SSL funcione.

Si no hay disponible ningún certificado con el algoritmo ECDSA, cree un nuevo certificado. Para obtener más información, consulte "Especificación de certificados SSL o KMIP" en la página 1.

Configuración del cumplimiento de NIST SP 800-131A en IBM Security Key Lifecycle Manager

Configure a IBM Security Key Lifecycle Manager para que se comunique a través de sockets seguros de acuerdo conl estándar NIST SP 800-131A (National Institute of Standards and Technology (NIST) Special Publication (SP) 800-131A) en la modalidad estricta.

Acerca de esta tarea

El estándar NIST SP 800-131A especifica algoritmos para reforzar la seguridad y la fuerza del cifrado. En la modalidad estricta, todas las comunicaciones deben cumplir con la SP 800-131A.

Esta tarea utiliza el ID de usuario de WASAdmin en WebSphere Integrated Solutions Console para configurar el cumplimiento con el estándar NIST SP 800-131A en IBM Security Key Lifecycle Manager.

Para obtener información sobre cómo configurar WebSphere Application Server para la modalidad estricta del estándar SP800-131, consulte la documentación de IBM WebSphere Application Server (http://www.ibm.com/support/knowledgecenter/en/SSAW57_9.0.0/com.ibm.websphere.nd.multiplatform.doc/ae/tsec_config_strictsp300.html).

Procedimiento

1. Inicie sesión en WebSphere Integrated Solutions Console (`https://localhost:9083/ibm/console/logon.jsp`).
2. En la página de bienvenida del navegador, escriba el ID de usuario `WASAdmin` y la contraseña de este administrador.
3. Desde el panel de navegación izquierdo, pulse **Seguridad** > **Gestión de claves y certificados SSL**.

4. En la página Gestión de claves y certificados SSL, en **Elementos relacionados**, pulse **Configuraciones de SSL**.
5. Pulse **NodeDefaultSSLSettings**.
6. En la sección **Propiedades adicionales**, pulse **Valores de calidad de protección (QoP)**.
7. Desde la lista **Protocolo**, seleccione **TLSv1.2**, y en la sección **Valores de la suite Cipher**, en la sección **grupos de la suite cipher**, seleccione **Fuerte**, y pulse **Actualizar ciphers seleccionados**.
8. Pulse **Aceptar**.
9. Pulse **Guardar** para guardar la configuración.
10. Desde el panel de navegación izquierdo, pulse **Seguridad** > **Gestión de claves y certificados SSL** > **Gestionar FIPS**.

    Para trabajar en una modalidad SP800-131 estricta, todos los certificados que se utilizan para SSL en el servidor se deben convertir en certificados conformes con los requisitos de SP800-131.
11. Para convertir certificados, en **Elementos relacionados**, pulse **Convertir certificados**.
12. Seleccione **Estricta** y elija el algoritmo `SHA256withRSA` para utilizarlo con los nuevos certificados de la lista.
13. Seleccione el tamaño de `2048` bits para el certificado en la lista **Nuevo tamaño de clave de certificado**.

    Nota: Si elige un algoritmo de firma de curva elíptica, se necesitan tamaños específicos; no podrá especificar un tamaño. En su lugar, se utilizará el tamaño correcto.
14. Si no se visualizan certificados en el marco **Certificados que no se pueden convertir**, pulse **Aplicar** y **Acepar**.

    Si se visualizan certificados en el marco **Certificados que no se pueden convertir**, el servidor no es capaz de convertir esos certificados. Sustituya estos certificados con unos que satisfagan los requisitos de SP800-131. El servidor podría no convertir un certificado por las siguientes razones:
    - El certificado se ha creado mediante una Autoridad certificadora (CA)
    - El certificado está en un almacén de claves de sólo lectura.
15. Pulse **Gestión de claves y certificados SSL** > **Gestionar FIPS**.
16. Seleccione **Habilitar SP800-131**.
17. Seleccione **Estricto**.
18. Pulse **Aplicar** y, a continuación, **Aceptar**.
19. Pulse **Guardar** para guardar la configuración.
20. Detenga WebSphere Application Server.

    Para conocer los pasos para detener el servidor, consulte "Reinicio de IBM Security Key Lifecycle Manager server" en la página 205.
21. En el archivo `<SKLM_HOME>/config/SKLMConfig.properties`, establezca las propiedades,**`TransportListener.ssl.protocols`** y **`fips`** con estos valores.

    ```
    TransportListener.ssl.protocols=TLSv1.2
    fips=on
    ```

    Interfaz de línea de mandatos

    a. Vaya al directorio `WAS_HOME/bin`. Por ejemplo,

    Windows

    ```
    cd unidad:\Program Files\IBM\WebSphere\AppServer\bin
    ```

Linux `cd /opt/IBM/WebSphere/AppServer/bin`

b. Inicie la interfaz **wsadmin** utilizando un ID de usuario autorizado, por ejemplo, `SKLMAdmin`. Por ejemplo,

Windows

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

Linux

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

c. Ejecute el mandato **tklmConfigUpdateEntry**.

```
print AdminTask.tklmConfigUpdateEntry ('[-name TransportListener.ssl.protocols -valu
print AdminTask.tklmConfigUpdateEntry ('[-name fips -value on]')
```

Interfaz REST

a. Abra un cliente REST.

b. Obtenga un identificador de autenticación de usuario exclusivo para acceder a los servicios REST de IBM Security Key Lifecycle Manager. Para obtener más información sobre el proceso de autenticación, consulte Proceso de autenticación de los servicios REST.

c. Ejecute el **Servicio REST Actualizar propiedad de configuración**. Pase el identificador de autenticación de usuario que ha obtenido en el `Paso b` junto con el mensaje de solicitud, como se muestra en el ejemplo siguiente.

```
PUT https://localhost:<puerto>/SKLM/rest/v1/configProperties
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth userAuthId=139aeh34567m
Accept-Language : en
{ "TransportListener.ssl.protocols" : "TLSv1.2"}
```

```
PUT https://localhost:<puerto>/SKLM/rest/v1/configProperties
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth userAuthId=139aeh34567m
Accept-Language : en
{ "fips" : "on"}
```

22. En el archivo *<WAS_HOME>*`/profiles/KLMProfile/properties/ssl.client.props`, actualice las propiedades, como se muestra aquí.

```
com.ibm.ssl.protocol=TLSv1.2
com.ibm.security.useFIPS=true
com.ibm.websphere.security.FIPSLevel=SP800-131
```

23. Inicie WebSphere Application Server.

Para conocer los pasos para iniciar el servidor, consulte “Reinicio de IBM Security Key Lifecycle Manager server” en la página 205.

Gestión de claves maestras

Puede crear y actualizar las claves maestras de IBM Security Key Lifecycle Manager. También puede mover una clave maestra desde un almacén de claves Java a un módulo de seguridad de hardware (HSM) y viceversa.

Puede utilizar Servicio REST Clave maestra para realizar todas las operaciones de gestión de claves maestras.

Gestión de la clave maestra de IBM Security Key Lifecycle Manager en una configuración multimaestro

En este tema se indican los pasos para realizar las operaciones de gestión de claves maestras de IBM Security Key Lifecycle Manager en un clúster multimaestro. Todas las operaciones de gestión de claves maestras deben realizarse únicamente en el servidor maestro primario.

Procedimiento

1. Realice la copia de seguridad del servidor maestro primario. Para obtener instrucciones, consulte "Copia de seguridad y restauración" en la página 123.
2. Asegúrese de que todos los servidores maestro del clúster multimaestro estén conectados.
3. Realice las operaciones de gestión de claves maestras en el servidor maestro primario. Para obtener instrucciones, consulte Servicio REST Clave maestra.
4. En todos los servidores maestros, asegúrese de que el valor de la propiedad **useMasterKeyinHSM** del archivo `SKLMConfig.properties` esté configurado correctamente. Si el clúster multimaestro está configurado para utilizar HSM, el valor de la propiedad **useMasterKeyinHSM** deberá ser `true`.

Gestión de la clave maestra de IBM Security Key Lifecycle Manager en una configuración de réplica

En este tema se indican los pasos para realizar las operaciones de gestión de claves maestras en una configuración de réplica. Una vez completados estos pasos, podrá realizar la réplica del servidor maestro en los servidores clon.

Antes de empezar

Realice la copia de seguridad del servidor maestro de réplica. Para obtener más información, consulte "Copia de seguridad y restauración" en la página 123.

Procedimiento

1. Realice las operaciones de gestión de claves maestras en el servidor maestro de réplica. Para obtener instrucciones, consulte Servicio REST Clave maestra.
2. Realice la copia de seguridad del servidor maestro de réplica. Para obtener instrucciones, consulte "Copia de seguridad y restauración" en la página 123.
3. Copie el archivo JAR de copia de seguridad desde el servidor maestro a todos los servidores clon.
4. Si el servidor maestro de réplica está configurado para utilizar HSM para almacenar la clave maestra, asegúrese de que todos los servidores clon también estén configurados para utilizar el mismo HSM. Para obtener instrucciones, consulte "Configuración de los parámetros de HSM" en la página 210.
5. Restaure los archivos de copia de seguridad en todos los servidores clon. Para obtener instrucciones, consulte "Restauración de un archivo de copia de seguridad" en la página 135.
6. En todos los servidores clon, inicie sesión en la interfaz gráfica de usuario de IBM Security Key Lifecycle Manager como administrador de IBM Security Key Lifecycle Manager.
   a. Pulse **Administración** > **Réplica**.
   b. Seleccione el rol de réplica como **Clon**. El rol de réplica se ha cambiado a `Maestro` una vez restaurados los archivos de copia de seguridad en el servidor clon desde el servidor maestro.

7. Reinicie los servidores clon para los cuales ha cambiado los roles. Para obtener instrucciones, consulte Reinicio de IBM Security Key Lifecycle Manager server.

Configuración de multimaestro

La implementación de una solución de alta disponibilidad precisa de una configuración de maestros de IBM Security Key Lifecycle Manager en un clúster multimaestro. Todas las instancias de IBM Security Key Lifecycle Manager del clúster apuntan a una sola fuente de datos que se ha configurado para DB2 HADR (DB2 high availability disaster recovery) para garantizar la disponibilidad en tiempo real de los datos más recientes a todos los maestros del clúster.

Utilice la configuración de Multimaestro de IBM Security Key Lifecycle Manager para la transmisión de datos para lograr los siguientes objetivos:

- Asegurar una disponibilidad de datos continua y coherente de IBM Security Key Lifecycle Manager a lo largo de toda la organización.
- Evitar la existencia de un único punto de anomalía al utilizar la solución de alta disponibilidad.
- Los maestros se pueden ubicar varias ubicaciones físicas, esto es, distribuidos a través de la red.

La configuración de la recuperación ante desastres de alta disponibilidad de DB2 (DB2 HADR) se utiliza como único origen de datos para todos los maestros en el clúster Multimaestro de IBM Security Key Lifecycle Manager. HADR protege contra la pérdida de datos al transmitir cambios de datos desde una base de datos de origen, denominada primaria, a una base de datos de destino, denominada de en espera. DB2 HADR da soporte a varias bases de datos en espera en su configuración de multimaestro.

Características clave de la configuración de multimaestro de IBM Security Key Lifecycle Manager

- Las claves que se crean en un maestro de IBM Security Key Lifecycle Manager son accesibles a otros maestros de IBM Security Key Lifecycle Manager en el clúster.
- Los dispositivos IPP y los clientes KMIP registrados en un maestro de IBM Security Key Lifecycle Manager pueden acceder a claves en otro maestro en el clúster.
- Interfaz REST e interfaz gráfica de usuario (GUI) para configurar los servidores maestros de IBM Security Key Lifecycle Manager para la configuración de multimaestro.

Para obtener más información sobre los servicios REST multimaestros, consulte Servicios REST de configuración de multimaestro.

Arquitectura de despliegue de multimaestro

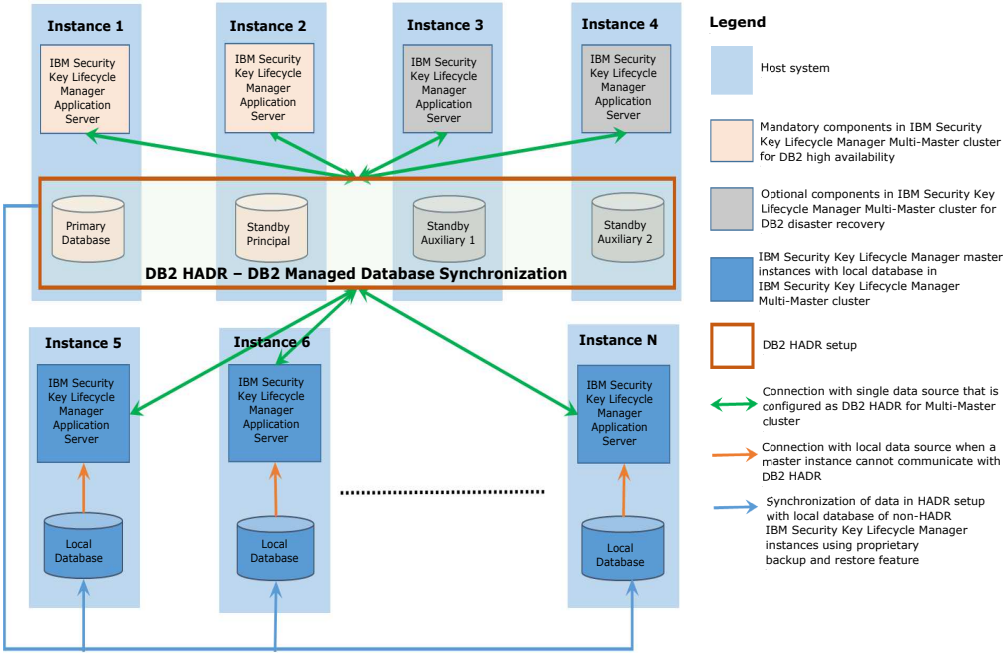
La arquitectura de multimaestro de IBM Security Key Lifecycle Manager se basa en la característica DB2 HADR (DB2 High Availability Disaster Recovery) para implementar una solución de alta disponibilidad.

Cada instancia de IBM Security Key Lifecycle Manager se instala con su instancia de DB2 que contiene todos los metadatos, datos de claves de objetos criptográficos gestionados y datos de auditoría. El clúster incluye varias instancias de IBM Security Key Lifecycle Manager, también denominadas como maestros. Todos los maestros en el clúster tienen los mismos privilegios. En el clúster multimaestro de

IBM Security Key Lifecycle Manager, cada uno de los maestros se conecta a una única base de datos denominada como la base de datos primaria. La base de datos primaria se conecta a otra base de datos de un maestro de IBM Security Key Lifecycle Manager denominada como la base de datos en espera. Con la configuración DB2 HADR, los datos se transmiten continuamente entre las dos bases de datos y se sincronizan. Cuando la base de datos primaria falla, una base de datos en espera toma el control automáticamente como la nueva base de datos primara para garantizar la disponibilidad de los datos más recientes a todos los maestros en el clúster.

Para configurar HADR (High Availability Disaster Recovery), los parámetros necesarios de DB2 se configuran en los maestros de IBM Security Key Lifecycle Manager con una base de datos primaria y una base de datos en espera. En los diagramas siguientes se muestra un despliegue simple de IBM Security Key Lifecycle Manager y DB2 HADR para un entorno multimaestro donde se han configurado cuatro instancias (maestros) de DB2 HADR y N instancias de IBM Security Key Lifecycle Manager.

Despliegue físico



WebSphere Application Server se configura con una base de datos DB2 habilitada para HADR para un direccionamiento de cliente automático. Cuando la base de datos HADR primaria falla, WebSphere Application Server restablece la conexión de forma automática a la base de datos HADR en espera principal.

DB2 HADR da soporte a varias bases de datos en espera en su configuración de multimaestro de IBM Security Key Lifecycle Manager. Puede tener un sistema en espera principal y hasta dos sistemas en espera auxiliares. Para obtener más información sobre varias bases de datos en espera, consulte Múltiples bases de datos en espera.

Requisitos previos de despliegue

- Tanto los servidores de base de datos DB2 primarias como en espera deben tener instalada la misma versión del sistema operativo.
- La versión de DB2 que se instala en los servidores maestros primario y en espera de IBM Security Key Lifecycle Manager deben coincidir.
- Se debe utilizar una red dedicada para las conexiones entre el primario y en espera de DB2 HADR.

Múltiples bases de datos en espera

La configuración de DB2 HADR (High Availability Disaster Recovery) se utiliza para proporcionar disponibilidad de datos de forma continua a todas las instancias de IBM Security Key Lifecycle Manager en un clúster multimaestro. HADR protege contra la pérdida de datos al transmitir cambios de datos desde una base de datos de origen, denominada primaria, a una base de datos de destino, denominada de en espera.

DB2 HADR admite hasta tres bases de datos en espera en su configuración de multimaestro, una en espera para la alta disponibilidad y las otras dos en espera para la recuperación ante desastres. Cuando la base de datos primaria está inactiva, el servicio de toma de control de HADR indica a la base de datos en espera a que asuma el rol de base de datos primaria. Para obtener más información sobre el servicio de toma de control de HADR, consulte Servicio de toma de control de HADR.

Las prioridades se asignan a cada base de datos en espera del clúster. La base de datos en espera con la prioridad más alta es la que asume el rol de base de datos primaria. Por ejemplo, si una base de datos primaria en el clúster de IBM Security Key Lifecycle Manager multimaestro falla, la base de datos en espera con un índice de prioridad 1 toma el rol de base de datos primaria.

Si desea añadir varios sistemas en espera al clúster, utilice la interfaz gráfica de usuario de IBM Security Key Lifecycle Manager o el Servicio REST Añadir maestro. Para obtener más información, consulte Adición de un maestro en espera a un clúster multimaestro.

Casos de ejemplo de toma de control de HADR

La tabla siguiente proporciona información sobre los casos de ejemplo de toma de control de DB2 HADR cuando se han configurado maestros de IBM Security Key Lifecycle Manager en un entorno multimaestro.

Agente de sistema host de la base de datos primaria	Base de datos primaria	Agente de sistema host de la base de datos en espera 1	Base de datos en espera 1	Agente de sistema host de la base de datos en espera 2	Base de datos en espera 2	Agente de sistema host de la base de datos en espera 3	Base de datos en espera 3	Acciones de agente	Servicio de claves de IBM Security Key Lifecycle Manager	Toma de control automática
Activo	Activo	Activo	Activo	Activo	Activo	Activo	Activo	Caso de ejemplo feliz.	Desde la base de datos primaria	N/D
Activo	Activo	Activo	Inactivo	Activo o inactivo	Activo o inactivo	Activo o inactivo	Activo o inactivo	-	Desde la base de datos primaria	N/D
Activo	Activo	Inactivo	Inactivo	Activo o inactivo	Activo o inactivo	Activo o inactivo	Activo o inactivo	-	Desde la base de datos primaria	N/D
Activo	Inactivo	Activo	Activo	Activo o inactivo	Activo o inactivo	Activo o inactivo	Activo o inactivo	El agente de primario envía la solicitud al agente del servidor en espera 1 para tomar el control como base de datos primaria.	Desde la base de datos en espera 1	Sí, si la base de datos primaria o en espera 1, sea cual sea la que esté disponible para la toma de control, y los agentes de ambos servidores deben estar en ejecución y se pueden comunicar entre sí. De lo contrario, No.
Inactivo	Inactivo	Activo	Activo	Activo o inactivo	Activo o inactivo	Activo o inactivo	Activo o inactivo	-	Desde la base de datos en espera 1	No

Agente de sistema host de la base de datos primaria	Base de datos primaria	Agente de sistema host de la base de datos en espera 1	Base de datos en espera 1	Agente de sistema host de la base de datos en espera 2	Base de datos en espera 2	Agente de sistema host de la base de datos en espera 3	Base de datos en espera 3	Acciones de agente	Servicio de claves de IBM Security Key Lifecycle Manager	Toma de control automática
Activo	Inactivo	Activo o inactivo	Inactivo	Activo	Activo	Activo o inactivo	Activo o inactivo	El agente de primario envía la solicitud al agente del servidor en espera 2 para tomar el control como base de datos primaria.	Desde base de datos en espera 2	Sí, si la base de datos primaria o en espera 2, sea cual sea la que esté disponible para la toma de control, y los agentes de ambos servidores deben estar en ejecución y se pueden comunicar entre sí. De lo contrario, No.
Inactivo	Inactivo	Activo o inactivo	Inactivo	Activo o inactivo	Activo	Activo o inactivo	Activo o inactivo	-	Desde la base de datos en espera 2 tras la toma de control manual	No
Inactivo	Inactivo	Inactivo	Inactivo	Activo o inactivo	Activo	Activo o inactivo	Activo o inactivo	-	Desde en espera 2 tras la toma de control manual	No

Agente de sistema host de la base de datos primaria	Base de datos primaria	Agente de sistema host de la base de datos en espera 1	Base de datos en espera 1	Agente de sistema host de la base de datos en espera 2	Base de datos en espera 2	Agente de sistema host de la base de datos en espera 3	Base de datos en espera 3	Acciones de agente	Servicio de claves de IBM Security Key Lifecycle Manager	Toma de control automática
Activo	Inactivo	Activo o inactivo	Inactivo	Activo o inactivo	Inactivo	Activo	Activo	El agente de primario envía la solicitud al agente del servidor en espera 3 para tomar el control como base de datos primaria.	Desde la base de datos en espera 3	Sí, si la base de datos primaria o en espera 3, sea cual sea la que esté disponible para la toma de control, y los agentes de ambos servidores deben estar en ejecución y se pueden comunicar entre sí. De lo contrario, No.
Activo	Inactivo	Activo o inactivo	Inactivo	Activo o inactivo	Inactivo	Activo o inactivo	Inactivo		Ninguno	No

Sistema de supervisión

En un clúster multimaestro, es esencial la supervisión del estado de salud de las instancias de IBM Security Key Lifecycle Manager y la rápida corrección de problemas antes de que afecten a las operaciones empresariales. IBM Security Key Lifecycle Manager incluye características de supervisión para supervisar el estado de salud de todos los servidores maestros de IBM Security Key Lifecycle Manager en el clúster.

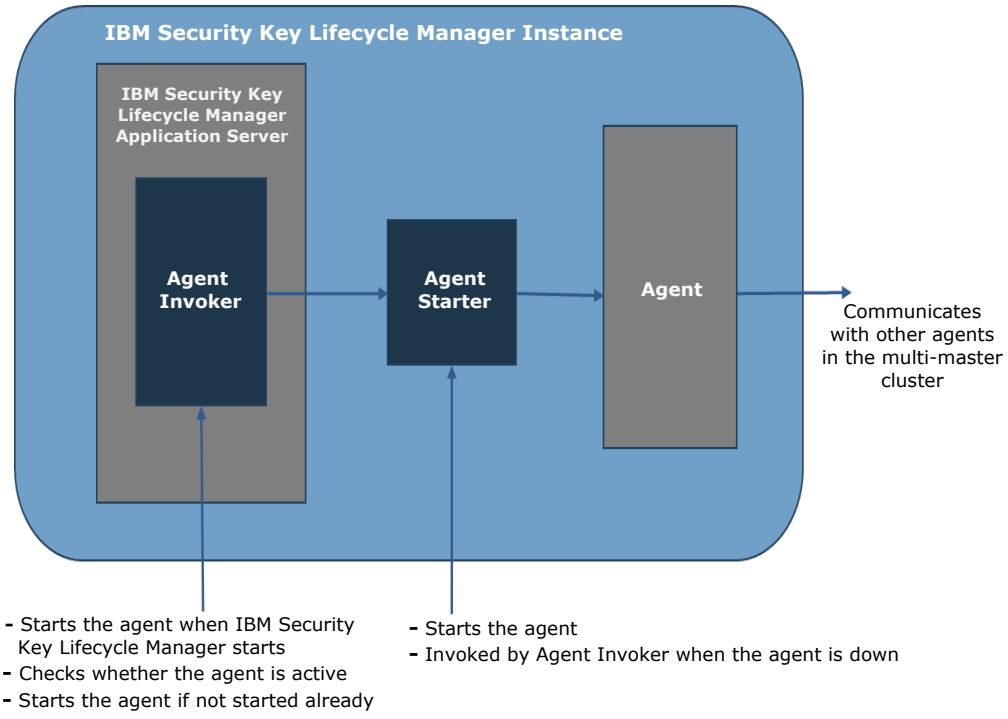
La supervisión es una parte integral de la configuración y el mantenimiento del entorno multimaestro. El sistema de supervisión de IBM Security Key Lifecycle Manager proporciona una imagen detallada de la configuración y la salud de su entorno multimaestro mediante la utilización de los siguientes componentes de supervisión.

Agente
Supervisa y recopila datos de estado de los servidores maestros de IBM Security Key Lifecycle Manager en el clúster en intervalos especificados. Para obtener más información, consulte Agente.

Iniciador de agente
Inicia el servicio del agente. Para obtener más información, consulte Iniciador de agente.

Invocador de agente
Supervisa el estado del servicio de agente a intervalos regulares. Para obtener más información, consulte Invocador de agente.

En el siguiente diagrama se muestran los componentes de supervisión en una instancia de IBM Security Key Lifecycle Manager (maestro) del clúster.

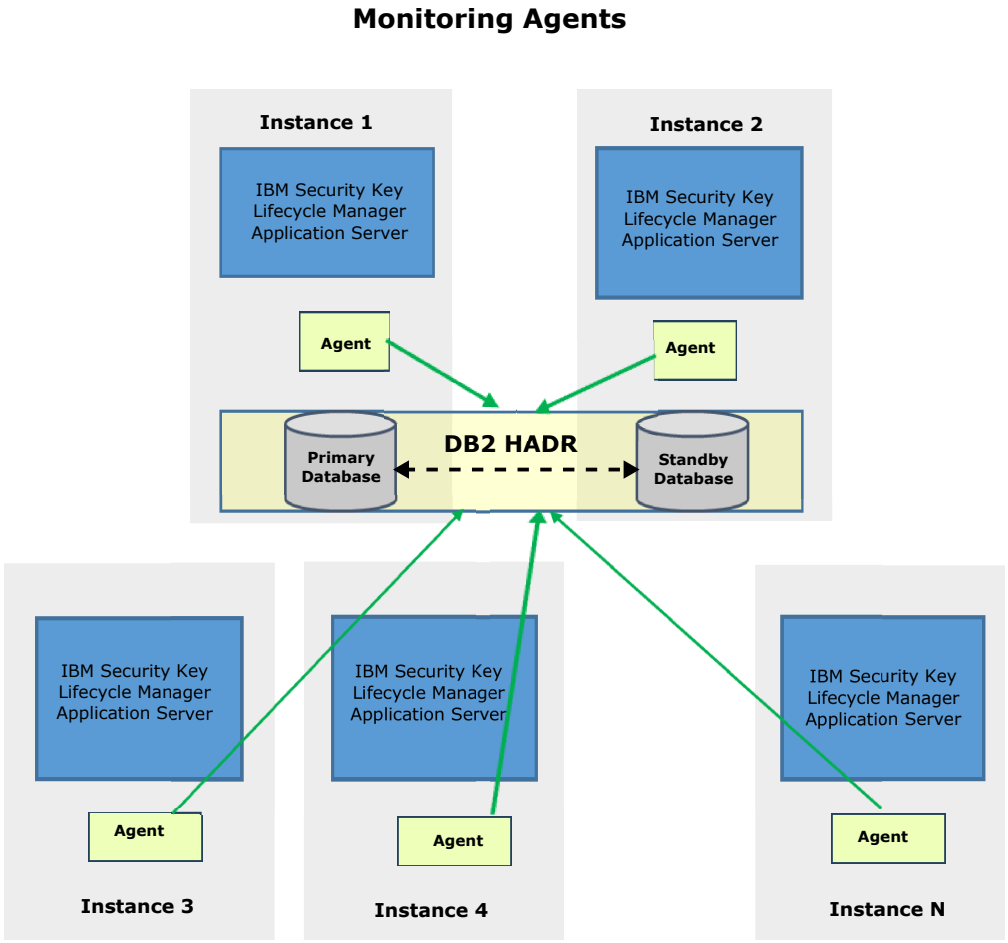


Agente

Utilice el servicio de agente de IBM Security Key Lifecycle Manager para supervisar el estado de salud y configure las instancias de IBM Security Key Lifecycle Manager en un clúster multimaestro.

Después de instalar una instancia de IBM Security Key Lifecycle Manager, el agente también se instala automáticamente en dicho servidor. El agente se inicia al iniciar IBM Security Key Lifecycle Manager. Cuando el servicio de agente está inactivo, el servicio Invocador de agente ejecuta el script Iniciador de agente `agentStarter` para reiniciar el servicio. El archivo `agentStarter.properties` contiene la información necesaria para ejecutar el script. Para obtener más información, consulte Invocador de agente e Iniciador de agente.

En el diagrama siguiente se muestra cómo los agentes de IBM Security Key Lifecycle Manager se despliegan en el entorno multimaestro. El agente en cada instancia de IBM Security Key Lifecycle Manager (maestro) captura el estado de la interfaz de usuario y los puertos KMIP e IPP. A continuación, se actualiza la información de estado en la base de datos con una indicación de fecha y hora.



El agente de IBM Security Key Lifecycle Manager proporciona los siguientes servicios para recopilar datos de supervisión y configurar instancias de IBM Security Key Lifecycle Manager en el clúster multimaestro.

Servicios planificados

Recopila datos de estado iniciando y manteniendo el siguiente conjunto de servicios a intervalos regulares.

- Servicio de Supervisión de agente
- Servicio de Supervisión de puertos
- Servicio de toma de control de HADR

Servicios de configuración

El agente proporciona varios servicios para establecer patrones para varios IBM Security Key Lifecycle Manager maestro de configuración. Los servicios de configuración se inician de forma automática al iniciar el agente.

- Servicios de configuración

Servicio de supervisión de agente:

El servicio de supervisión de agente comprueba de forma periódica si los agentes en otros servidores maestros de IBM Security Key Lifecycle Manager del clúster multimaestro están activos y ejecutándose.

Cuando se inicia el agente en un servidor maestro de IBM Security Key Lifecycle Manager, el servicio de supervisión de agente inicia de forma automática la supervisión del estado de los agentes a intervalos regulares si la instancia de IBM Security Key Lifecycle Manager no es el del tipo `Local`. El estado de disponibilidad se puede visualizar mediante la interfaz gráfica de usuario de IBM Security Key Lifecycle Manager o la interfaz REST. Para obtener más información sobre el servicio del agente, consulte Agentes.

Utilice la propiedad **`agent.monitoring.svc.interval`** del archivo `<SKLM_HOME>\config\SKLMConfig.properties`, por ejemplo, `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\config\SKLMConfig.properties`, para configurar el intervalo del servicio de supervisión del agente. Para obtener más información sobre la propiedad de configuración, consulte agent.monitoring.svc.interval.

Para obtener más información sobre la definición de <*SKLM_HOME*>, consulte Definiciones para *HOME* y otras variables de directorio.

Servicio de supervisión de puertos:

El servicio de supervisión de puertos comprueba periódicamente la disponibilidad de los puertos que un servidor maestro de IBM Security Key Lifecycle Manager necesita para la comunicación en el clúster multimaestro.

Cuando se inicia el servicio de agente en un maestro de IBM Security Key Lifecycle Manager, el servicio de supervisión de puertos empieza a supervisar automáticamente la disponibilidad de los puertos a intervalos regulares si la instancia de IBM Security Key Lifecycle Manager no es de tipo `Local`. El estado de disponibilidad se puede visualizar mediante la interfaz gráfica de usuario de IBM Security Key Lifecycle Manager o la interfaz REST. Para obtener más información sobre el servicio del agente, consulte Agentes.

Utilice la propiedad **`port.monitoring.svc.interval`** del archivo `<SKLM_HOME>\config\SKLMConfig.properties`, por ejemplo, `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\config\SKLMConfig.properties`, para configurar el intervalo de supervisión del puerto. Para obtener más información sobre la propiedad de configuración, consulte port.monitoring.svc.interval.

Para obtener más información sobre la definición de <*SKLM_HOME*>, consulte Definiciones para *HOME* y otras variables de directorio.

El servicio de supervisión de puertos comprueba si es posible acceder los puertos siguientes y si están en ejecución.

Puerto TCP
: Puerto en el que el servidor de IBM Security Key Lifecycle Manager está a la escucha de solicitudes de los dispositivos.

Puerto SSL
: Puerto en el que el servidor de IBM Security Key Lifecycle Manager está a la escucha de solicitudes de los dispositivos que se comunican mediante el protocolo SSL.

Puerto KMIP
: Puerto en el que el servidor de IBM Security Key Lifecycle Manager está a la escucha de solicitudes para comunicarse a través del socket SSL que utiliza el protocolo KMIP (Key Management Interoperability Protocol).

Puerto de DB2
Puerto en el que el servidor de IBM Security Key Lifecycle Manager está a la escucha de solicitudes de DB2.

Puerto HTTP
Puerto en el que IBM Security Key Lifecycle Manager está a la escucha de solicitudes HTTPS.

Puerto de administración
Puerto en el que el servidor de IBM Security Key Lifecycle Manager está a la escucha de solicitudes.

Puerto de HADR
Puerto para las bases de datos configuradas como de HADR para las comunicaciones de bases de datos.

Puerto de agente
Puerto en el que el agente está a la escucha de la comunicación desde IBM Security Key Lifecycle Manager.

Para obtener más información sobre los valores de puerto predeterminados, consulte Servicios, puertos y procesos.

Servicio de toma de control de HADR:

El servicio de toma de control de HADR es responsable de tomar el control de una base de datos primaria cuando se produce un problema de conexión entre el servidor maestro de IBM Security Key Lifecycle Manager y la base de datos primaria en el clúster. Cuando una base de datos primaria está inactiva, la operación de toma de control se inicia en una base de datos en espera de forma que las operaciones de usuario se continúan procesando durante la interrupción.

Configure la propiedad **agent.takeover.svc.interval** en el archivo *<SKLM_HOME>*/config/SKLMConfig.properties, por ejemplo, C:\Program Files\IBM\WebSphere\AppServer\products\sklm\config\SKLMConfig.properties, para ejecutar el servicio de toma de control de HADR. Para obtener más información sobre la propiedad de configuración, consulte agent.takeover.svc.interval.

DB2 HADR (DB2 High Availability Disaster Recovery) se utiliza en un clúster multimaestro de IBM Security Key Lifecycle Manager. DB2 HADR protege frente ante la pérdida de datos transmitiendo cambios de datos desde una base de datos primaria a bases de datos en espera. Bajo condiciones normales, DB2 HADR mantiene las bases de datos primaria y en espera DB2 HADR sincronizadas.

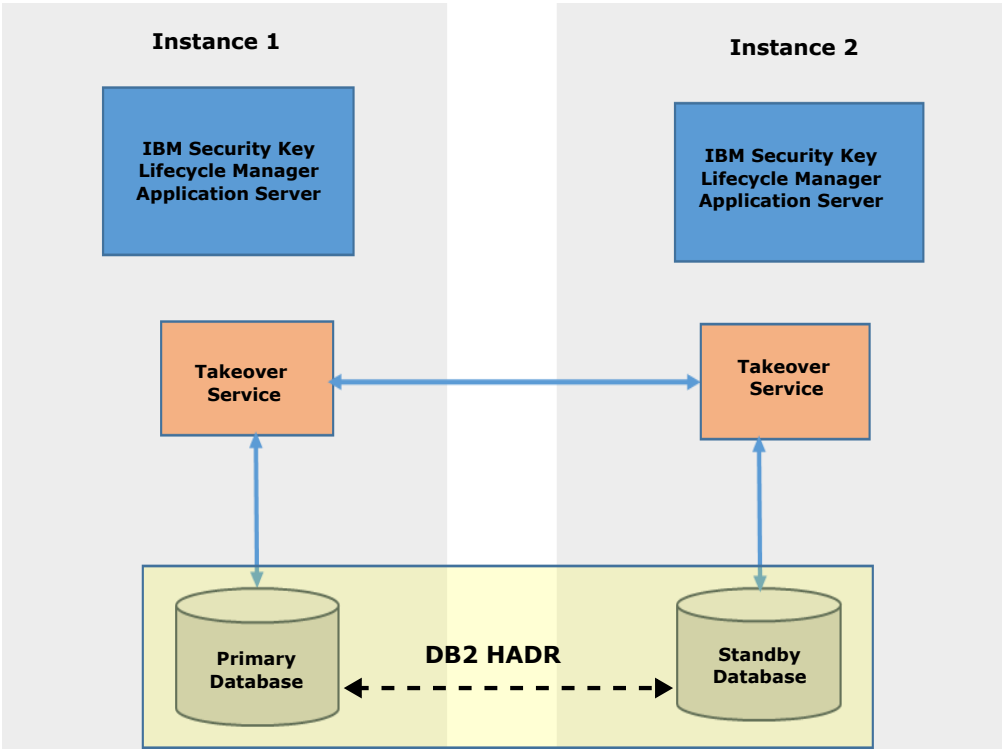
Los agentes se instalan en todos los servidores maestros del clúster. Los servicios del agente realizan un seguimiento de la disponibilidad de los puertos relacionados con IBM Security Key Lifecycle Manager. Si la base de datos primaria está inactiva, el servicio de toma de control indica a la base de datos en espera para que tome el control como la nueva base de datos primaria de HADR.

Para poder realizar la operación de toma de control, las bases de datos primaria y en espera se sincronizan de forma continua mediante un canal de comunicación seguro. Un conjunto de parámetros de configuración de WebSphere Application Server y DB2 HADR se actualizan de forma automática para la operación de toma de control mediante los servicios de configuración que ejecuta el agente. Para obtener más información sobre los distintos servicios de configuración, consulte Servicios de configuración.

DB2 HADR da soporte a hasta tres bases de datos en espera en su configuración de multimaestro. Puede tener un sistema en espera principal y hasta dos sistemas en espera auxiliares. Las prioridades se asignan a cada base de datos en espera del clúster. La base de datos en espera con la prioridad más alta es la que asume el rol de base de datos primaria. Por ejemplo, si una base de datos primaria en el clúster de IBM Security Key Lifecycle Manager multimaestro falla, la base de datos en espera con un índice de prioridad 1 toma el rol para actuar como base de datos primaria. Si la operación de toma de control en una base de datos en espera con un índice de prioridad 1 falla, la siguiente base de datos en espera con siguiente orden de prioridad (índice de prioridad 2) tomará el control para actuar como base de datos primaria.

Nota: Debe reiniciar manualmente WebSphere Application Server en todos los servidores en espera si un sistema en espera auxiliar asume el rol primario. No es necesario el reinicio de WebSphere Application Server cuando el sistema en espera principal asume el rol primario.

IBM Security Key Lifecycle Manager da soporte a la opción de recuperación tras error. Existe la posibilidad de configurar la base de datos primaria para tomar el rol primario cuando se active.



- El servicio de toma de control de la `Instancia 1` (servidor maestro primario) comprueba el estado de la base de datos (`Base de datos primaria`) mediante mandatos DB2.
- Si la `Base de datos primaria` está inactiva, la `Instancia 2` (servidor maestro en espera) recibe la solicitud de toma de control desde el servidor primario. La `Base de datos en espera` toma el control como la `Base de datos primaria`.
- El servidor maestro primario recibe un mensaje desde el sistema en espera que indica que la operación de toma de control ha sido satisfactoria. Cuando la operación de toma de control falla, el servicio de toma de control en el servidor

primario envía solicitudes de control al siguiente sistema en espera si el clúster multimaestro está configurado con varios servidores en espera.
- Cuando el servidor de base de datos primario antiguo está activo, el servicio de toma de control inicia HADR en él como en espera.

Para obtener más información sobre los requisitos previos para la configuración de DB2 HADR, consulte Configuración de la base de datos para HADR (high availability disaster recovery).

Cómo iniciar de forma manual la operación de toma de control

Cuando el servidor maestro primario de IBM Security Key Lifecycle Manager que contiene la base de datos primaria está inactivo, la operación de toma de control no se inicia de forma automática. En estos casos, la operación de toma de control se puede iniciar de forma manual ejecutando el script **sklmTakeoverHADR**.

Nota: Si falla el sistema operativo del servidor maestro primario de IBM Security Key Lifecycle Manager, utilice las instrucciones para iniciar manualmente la operación de toma de control que se da aquí: El sistema operativo del servidor maestro primario de IBM Security Key Lifecycle Manager falla.

1. Localice el script **sklmTakeoverHADR**.

   Windows
   <*SKLM_INSTALL_HOME*>\agent

   La ubicación predeterminada es C:\Program Files\IBM\SKLMV301\agent.

   Linux <*SKLM_INSTALL_HOME*>/agent

   La ubicación predeterminada es /opt/IBM/SKLMV301\agent.
2. Abra un indicador de mandatos y ejecute el script.

   Windows
   Vaya al directorio <*SKLM_INSTALL_HOME*>\agent y ejecute el siguiente mandato:

   ```
   sklmTakeoverHADR.bat <WAS_HOME> [NOMBREHOST_IP] [PUERTO_AGENTE]
   ```

   Por ejemplo,

   ```
   sklmTakeoverHADR.bat "C:\Program Files\IBM\WebSphere\AppServer" 9.113.37.10 60015
   ```

   Linux Vaya al directorio <*SKLM_INSTALL_HOME*>/agent y ejecute el siguiente mandato:

   ```
   sklmTakeoverHADR.sh <WAS_HOME> [NOMBREHOST_IP] [PUERTO_AGENTE]
   ```

   Por ejemplo,

   ```
   ./sklmTakeoverHADR.sh /opt/IBM/WebSphere/AppServer 9.113.37.10 60015
   ```

Servicios de configuración:

El agente proporciona varios servicios para establecer patrones para varios IBM Security Key Lifecycle Manager maestro de configuración.

Actualizar configuración de base de datos (Primaria)
Actualiza la base de datos primaria en un servidor maestro de IBM Security Key Lifecycle Manager en el clúster con las configuraciones necesarias para la configuración de multimaestro.

Actualizar configuración de base de datos HADR (Primaria/En espera)
Actualiza los parámetros de configuración en los servidores de base de datos primario y en espera para configurar DB2 HADR (DB2 High Availability Disaster Recovery).

Tomar y restaurar copias de seguridad
Realiza copias de seguridad de la base de datos desde el servidor primario y las restaura en el servidor en espera. En un clúster multimaestro con configuración DB2 HADR, el servidor de base de datos primario y el servidor de base de datos en espera deben estar sincronizados con los mismos datos.

Enviar y recibir copias de seguridad
Envía el archivo de copia de seguridad desde el servidor de bases de datos primario al servidor en espera utilizando un canal de comunicación seguro. En el servidor en espera, el archivo de copia de seguridad se almacena en la carpeta *<SKLM_DATA>*, por ejemplo, `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data`. Para ver la definición de *<SKLM_DATA>*, consulte Definiciones para *HOME* y otras variables de directorio.

Iniciar HADR (Primario/Secundario)
Inicia operaciones DB2 HADR en los servidores de base de datos primaria y en espera. Inicia DB2 HADR en el servidor en espera y, a continuación, en el servidor primario.

Actualizar configuración de WebSphere Application Server
Actualiza la configuración de WebSphere Application Server para especificar las propiedades de origen de datos de DB2 como, por ejemplo, los nombres y puertos de los servidores de base de datos en espera para dar soporte al redireccionamiento de cliente automático. Si la conexión con el servidor DB2 primario falla, WebSphere Application Server restablece la conexión automáticamente al servidor DB2 en espera.

Reiniciar WebSphere Application Server
Reinicia WebSphere Application Server en el servidor primario, servidor en espera y otras instancias de IBM Security Key Lifecycle Manager en el clúster para aplicar cambios de configuración de origen de datos de DB2 que se realizan para dar soporte a la redirección de cliente automático.

Obtener estado de configuración de WebSphere Application Server y DB2 HADR
Obtiene el estado de conexión de WebSphere Application Server y DB2 HADR. Para un entorno HADR operativo, debe asegurarse de que el DB2 HADR primario y el DB2 HADR en espera están conectados.

Servicio de sincronización de datos:

En el clúster multimaestro de IBM Security Key Lifecycle Manager, las bases de datos primarias y en espera se configuran con DB2 HADR para proporcionar alta disponibilidad. Bajo condiciones normales, DB2 HADR mantiene las bases de datos primaria y en espera sincronizadas. El servicio de sincronización de IBM Security Key Lifecycle Manager copia los archivos de copia de seguridad de DB2 desde el maestro primario a los otros nodos maestros en el clúster en un intervalo que se especifica. La sincronización de datos mantiene los datos en los nodos maestros actualizados con los datos en el servidor primario en el clúster.

Cuando se desconecta un servidor maestro del clúster debido a problemas de conectividad, puede establecer este servidor maestro en una modalidad de lectura-escritura. A continuación, puede restaurar los archivos de copia de

seguridad en el maestro de lectura-escritura para proporcionar claves a los dispositivos. Para obtener más información sobre cómo establecer el maestro aislado como un maestro de lectura-escritura, consulte “Configuración de un maestro aislado como maestro de lectura-escritura” en la página 262. Cuando se resuelvan los problemas de conectividad, podrá reincorporar el maestro al clúster. Para obtener más información sobre la reincorporación al clúster, consulte “Reincorporación de nuevo al clúster de un maestro de lectura-escritura aislado” en la página 264.

Ubicación del archivo de copia de seguridad

El archivo de copia de seguridad del servidor primario se copia en la carpeta *<WAS_HOME>*/products/sklm/data/synchronization en el nodo maestro. Se puede guardar un máximo de dos archivos de copia de seguridad.

Configuración de la sincronización de datos

Configure la propiedad **data.synchronizing.svc.interval** en el archivo <SKLM_HOME>/config/SKLMConfig.properties para establecer el intervalo de tiempo para la sincronización de datos. Para obtener más información sobre la propiedad de configuración, consulte data.synchronizing.svc.interval.

Establecimiento de contraseña para los archivos de copia de seguridad

Puede configurar la propiedad **data.synchronizing.backup.password** del archivo <SKLM_HOME>/config/SKLMConfig.properties para establecer la contraseña para los archivos de copia de seguridad generados por el servicio de sincronización de datos en el maestro primario o en espera. Estos archivos de copia de seguridad se copian en el resto de los nodos maestro del clúster multimaestro de IBM Security Key Lifecycle Manager en un intervalo especificado para la propiedad **data.synchronizing.svc.interval**.

A continuación, puede restaurar los archivos de copia de seguridad en el servidor maestro de lectura-escritura mediante la contraseña que ha establecido. Puede utilizar la interfaz gráfica de usuario, la interfaz de línea de mandatos o la interfaz REST para restaurar datos si ha establecido la contraseña en el archivo de configuración. Si el valor de la propiedad de configuración no está establecido, se generará una contraseña aleatoria y los datos se restaurarán automáticamente en el maestro de lectura-escritura. Debe reiniciar WebSphere Application Server y el servicio de agente después de establecer la contraseña. Para obtener más información sobre la propiedad de configuración, consulte data.synchronizing.backup.password.

Establecimiento del número máximo de archivos de copia de seguridad de DB2

Puede configurar la propiedad **data.synchronizing.svc.MaxBackupNum** en el archivo <SKLM_HOME>/config/SKLMConfig.properties para especificar el número máximo de archivos de copia de seguridad de DB2 a conservar en los maestros no HADR del clúster multimaestro. Debe reiniciar WebSphere Application Server y el servicio de agente después de establecer la contraseña. Para obtener más información sobre la propiedad de configuración, consulte data.synchronizing.svc.MaxBackupNum.

Reinicio del servicio de agente de IBM Security Key Lifecycle Manager:

El reinicio del servicio de agente de IBM Security Key Lifecycle Manager hace que el servidor lea su configuración y acepte los cambios de configuración, si los hay.

Procedimiento

1. Abra un indicador de mandatos.
2. Vaya al directorio *SKLM_INSTALL_HOME*\agent.

   Windows
   ```
   C:\Program Files\IBM\SKLMV301\agent
   ```

   Linux
   ```
   /opt/IBM/SKLMV301/agent
   ```
3. Detenga el servicio de agente ejecutando el mandato siguiente.

   Windows
   ```
   stopAgent.bat WAS_HOME
   stopAgent.bat "C:\Program Files\IBM\WebSphere\AppServer"
   ```

   Linux
   ```
   ./stopAgent.sh <WAS_HOME>
   ./stopAgent.sh /opt/IBM/WebSphere/AppServer
   ```
4. Inicie el servicio de agente ejecutando el mandato siguiente.

   Windows
   ```
   startAgent.bat WAS_HOME
   startAgent.bat "C:\Program Files\IBM\WebSphere\AppServer"
   ```

   Linux
   ```
   ./startAgent.sh WAS_HOME
   ./startAgent.sh /opt/IBM/WebSphere/AppServer
   ```

Iniciador de agente

El servicio Iniciador de agente en el clúster multimaestro de IBM Security Key Lifecycle Manager se utiliza para iniciar el agente de supervisión.

Cuando el agente en un maestro de IBM Security Key Lifecycle Manager está inactivo, el servicio Invocador de agente ejecuta el script Iniciador de agente `startAgent` para reiniciar el servicio. El archivo `agentStarter.properties` contiene la información necesaria para ejecutar el script.

Ubicación del script y del archivo de propiedades

El script `startAgent` y el archivo `agentStarter.properties` se encuentran en el directorio *SKLM_INSTALL_HOME*\`agent`. Por ejemplo,

Windows
```
C:\Program Files\IBM\SKLMV301\agent\startAgent.bat
C:\Program Files\IBM\SKLMV301\agent\agentStarter.properties
```

Linux
```
opt/IBM/SKLMV301/agent/startAgent.sh
opt/IBM/SKLMV301/agent/agentStarter.properties
```

Inicio del servicio de agente

Ejecute el siguiente mandato:

Windows
```
startAgent.bat WAS_HOME
startAgent.bat "C:\Program Files\IBM\WebSphere\AppServer"
```

Linux
```
./startAgent.sh WAS_HOME
./startAgent.sh /opt/IBM/WebSphere/AppServer
```

Ejemplo de archivo de propiedades del Iniciador de agente

```
SELF_DB_PASSWORD=75927941B378990404B33FBD35D3A433
PRIMARY_IP_HOSTNAME=civ3cez161
SERVICE=PortMonitoring,AgentMonitoring,TakeOverService
SELF_IP_HOSTNAME=civ3cez161
SELF_SSL_PORT=441
SELF_DB_NAME=sklmdb31
SELF_INSTANCE_ID=f39dba2
SELF_AGENT_PORT=60015
PRIMARY_DB_PORT=50050
PRIMARY_DB_IP=civ3cez161
SELF_NAME=f39dba2
SELF_SKLM_PASSWORD=A965C364C4DC71657A2A5B1013690045
STANDBY_INSTANCE_COUNT=0
PRIMARY_DB_PASSWORD=75927941B378990404B33FBD35D3A433
SELF_OWNER_EMAIL_ADDR2=
SELF_HTTP_PORT=443
SELF_OWNER_EMAIL_ADDR1=
SELF_WAS_PASSWORD=887A28DD992FC70B894C4BEE509B5876
SELF_SKLM_USERNAME=SKLMAdmin
SELF_HADR_TYPE=1
SELF_DB_PORT=50050
SELF_KEYSTORE_PASSWORD=EDB95C175FCC69347674702DB9C366BC
PRIMARY_DB_USERNAME=sklmdb31
SELF_DB_USERNAME=sklmdb31
SELF_DB_IP=civ3cez161
SELF_KMIP_PORT=5696
SELF_WAS_USERNAME=wasadmin
SELF_TCP_PORT=3801
PRIMARY_AGENT_PORT=60015
SELF_HADR_PORT=60025
NODE_INSTANCE_COUNT=0
PRIMARY_DB_NAME=SKLMDB31
PRIMARY_HADR_PORT=60025
SELF_ADMIN_PORT=9083
SELF_CLUSTER_NAME=multimaster
```

Los valores posibles para el parámetro **SERVICE** son `PortMonitoring`, `AgentMonitoring`, `TakeOverService` o `DataSynchronizeService`.

Invocador de agente

El servicio Invocador de agente en un maestro de IBM Security Key Lifecycle Manager supervisa el estado del agente a intervalos regulares.

El servicio Invocador de agente se ejecuta de forma automática en todos los maestros de IBM Security Key Lifecycle Manager de un clúster multimaestro. Cuando se inicia la aplicación de IBM Security Key Lifecycle Manager, el servicio Invocador de agente empieza comprobando si el servicio de agente se está ejecutando a intervalos regulares. Si el servicio de agente está inactivo, el servicio Invocador de agente inicia el agente mediante el servicio Iniciador de agente.

Utilice la propiedad **agent.invoker.polling.interval** del archivo *<SKLM_HOME>*`\config\SKLMConfig.properties`, por ejemplo, `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\config\SKLMConfig.properties`, para configurar el intervalo de supervisión del agente. Para obtener más información sobre la propiedad de configuración, consulte agent.invoker.polling.interval.

Detener agente

El servicio Detener agente en el clúster multimaestro de IBM Security Key Lifecycle Manager se utiliza para detener el agente de supervisión.

El agente detenido se reinicia automáticamente cuando se ejecuta el servicio Invocador de agente.

Ubicación del archivo de script `stopAgent`

El archivo de script `stopAgent` se encuentra en el directorio *SKLM_INSTALL_HOME*\`agent`. Por ejemplo,

Windows
```
C:\Program Files\IBM\SKLMV301\agent\stopAgent.bat
```

Linux `opt/IBM/SKLMV301/agent/stopAgent.sh`

Detención del servicio de agente

Ejecute el siguiente mandato:

Windows
```
stopAgent.bat WAS_HOME
stopAgent.bat "C:\Program Files\IBM\WebSphere\AppServer"
```

Linux
```
./stopAgent.sh WAS_HOME
./stopAgent.sh /opt/IBM/WebSphere/AppServer
```

Detención del agente de forma permanente

Puede detener un agente de forma permanente. Si se detiene de forma permanente, el agente no se reinicia automáticamente cuando se ejecuta el servicio Invocador de agente.

Para detener el agente de forma permanente:

1. En el archivo `SKLMConfig.properties`, actualice el valor de propiedad **`stopAgentInvocation`** a `true`.
   ```
   stopAgentInvocation=true
   ```
2. Detenga el agente. Consulte la sección “Detención del agente de forma permanente”.

Nota: No detenga el agente de forma permanente en una configuración multimaestro. Puede hacerlo en un servidor de IBM Security Key Lifecycle Manager autónomo o una configuración de réplica.

Para iniciar el agente que se ha detenido permanentemente:

1. En el archivo `SKLMConfig.properties`, actualice el valor de la propiedad **`stopAgentInvocation`** a `false`.
   ```
   stopAgentInvocation=false
   ```

   Puede utilizar el mandato de CLI de tklmConfigUpdateEntry o Servicio REST Actualizar propiedad de configuración para actualizar el archivo `SKLMConfig.properties`.
2. Reinicie WebSphere Application Server.

Requisitos y consideraciones para la configuración de multimaestro

Antes de configurar el entorno multimaestro de IBM Security Key Lifecycle Manager, revise los requisitos y consideraciones para garantizar una configuración satisfactoria.

- Asegúrese de que KMIP, SSL, TCP, y los puertos de agente no estén bloqueados para la comunicación antes de configurar los maestros de IBM Security Key Lifecycle Manager para la configuración multimaestra.
- Asegúrese de que el puerto del agente (60015) y el puerto HADR (60025) que se utilizan para la configuración multimaestra no estén bloqueados por el cortafuegos.

  El puerto de agente predeterminado es 60015, que puede actualizar a través de la interfaz de usuario. El puerto HADR predeterminado es 60025, que se asigna durante la configuración multimaestra, y que se puede configurar.
- La arquitectura de multimaestro de IBM Security Key Lifecycle Manager se basa en la tecnología Db2 HADR (Db2 High Availability Disaster Recovery) para implementar una solución de alta disponibilidad. Por lo tanto, todas las directrices y reglas de configuración Db2 HADR son aplicables a la configuración de multimaestro IBM Security Key Lifecycle Manager.
- Asegúrese de que los maestros de IBM Security Key Lifecycle Manager con sistemas host de base de datos Db2 HADR primaria y en espera tienen la misma versión de sistema operativo y niveles de fixpack.
- El nombre de usuario de Db2 y la contraseña deben ser los mismos en todos los maestros del clúster multimaestro de IBM Security Key Lifecycle Manager.
- La instancia de IBM Security Key Lifecycle Manager que desea añadir al clúster multimaestro no debe contener ningún dato. La adición del servidor maestro con datos da como resultado la pérdida de datos que se ha creado anteriormente.
  - Si desea añadir una instancia de IBM Security Key Lifecycle Manager existente en el clúster, utilice la característica de exportación e importación del grupo de dispositivos. Consulte “Adición de una instancia de IBM Security Key Lifecycle Manager existente con datos para el clúster multimaestro” en la página 255 para obtener más detalles.
- Debe estar disponible una interfaz TCP/IP entre los sistemas host de base de datos Db2 HADR primaria y en espera con una velocidad dedicada y alta y un ancho de banda de red de alta capacidad.
- Para el despliegue multimaestro de IBM Security Key Lifecycle Manager, el clúster debe contener un mínimo de un maestro primario y un maestro en espera. Cuando se configura un clúster multimaestro de IBM Security Key Lifecycle Manager, el servidor desde el que se añade al clúster un maestro o maestro en espera se convierte en el maestro primario. Debe añadir un sistema en espera al clúster antes de añadir otros maestros.
- El certificado de servidor se debe crear en una instancia de IBM Security Key Lifecycle Manager antes de añadirlo al clúster multimaestro como el maestro primario.
- El clúster multimaestro de IBM Security Key Lifecycle Manager da soporte a hasta tres maestros en espera. Cuando se añaden maestros en espera al clúster, el valor del índice de prioridad debe estar en el rango 1-3.
- Después de realizar una configuración de multimaestro de IBM Security Key Lifecycle Manager debe evitar ejecutar las operaciones de copia de seguridad y restauración manuales desde cualquiera de los maestros en el clúster.

- Ejecute las operaciones de configuración de multimaestro de IBM Security Key Lifecycle Manager sólo desde el maestro primario del clúster para evitar problemas.
- Antes de añadir un maestro al clúster multimaestro de IBM Security Key Lifecycle Manager en un sistema operativo Linux, los permisos para el directorio `/tmp` se deben establecer en 777, es decir, permisos de escritura, lectura y ejecución completos.
- Antes de añadir un servidor maestro al clúster, ejecute **Servicio REST Comprobar requisitos previos** para verificar si el maestro cumple todos los requisitos. Para obtener más información sobre el servicio REST, consulte Servicio REST Comprobar requisitos previos.
- Si desea configurar la configuración multimaestro de IBM Security Key Lifecycle Manager para utilizar HSM para almacenar la clave maestra, debe configurar todos los maestros del clúster para utilizar el mismo HSM.
- Antes de añadir un servidor maestro al clúster mediante el sistema migrado, debe modificar el nombre de usuario y la contraseña del administrador de IBM Security Key Lifecycle Manager en las siguientes situaciones:
  1. Cuando los usuarios y grupos se migran desde la versión anterior a la versión 3.0.1 a través del proceso de migración cruzada.
  2. El nombre de usuario y la contraseña del usuario administrador de IBM Security Key Lifecycle Manager son distintos de las credenciales especificadas durante la instalación de la versión 3.0.1.
- No es posible eliminar un servidor maestro o en espera de un clúster multimaestro si el servidor en espera está fuera de servicio.

Dirección IP para la correlación de nombre de host

Debe asegurarse de que el nombre de host del sistema esté configurado correctamente antes de configurar los maestros de IBM Security Key Lifecycle Manager para la configuración multimaestra. Puede resolver una dirección IP en un nombre de host editando el archivo `etc/hosts`.

Para la configuración de DB2 HADR, debe actualizar el archivo `etc/hosts` en los servidores maestros primarios y en espera del clúster para habilitar el nombre de host en la correlación de dirección IP.

Ubicación del archivo de host

Windows

```
C:\Windows\System32\Drivers\etc\
```

Linux `/etc/hosts`

El ejemplo siguiente muestra la dirección IP a la correlación del nombre de host en el archivo `etc/hosts`.

```
# 127.0.0.1 localhost
# ::1 localhost
9.199.138.209 sklmver3
```

Adición de un maestro en espera al clúster

En IBM Security Key Lifecycle Manager, la solución de alta disponibilidad se implementa utilizando la configuración de clúster multimaestro. Un clúster multimaestro de IBM Security Key Lifecycle Manager debe contener un maestro primario y un maestro en espera. Añada al clúster un maestro en espera para configurar un entorno multimaestro.

Antes de empezar

Antes de añadir un maestro en espera al clúster, revise las consideraciones y restricciones que se listan en el tema Requisitos y consideraciones para la configuración de multimaestro.

Ejecute Servicio REST Comprobar requisitos previos para asegurarse de que el maestro que desea añadir cumple con todos los requisitos y condiciones que se definen para la configuración de multimaestro de IBM Security Key Lifecycle Manager.

Acerca de esta tarea

Para proporcionar una disponibilidad de datos continuada a todas las instancias de IBM Security Key Lifecycle Manager en un clúster multimaestro, se utiliza la configuración de DB2 HADR (DB2 High Availability Disaster Recovery). DB2 HADR es una característica de réplica de base de datos que proporciona una solución de alta disponibilidad. HADR protege ante la pérdida de datos replicando cambios de datos desde una base de datos de origen, denominada primaria, a una base de datos de destino, denominada de en espera. DB2 HADR da soporte a hasta tres bases de datos en espera en su configuración de multimaestro.

Cuando se crea un clúster multimaestro de IBM Security Key Lifecycle Manager, el servidor desde el que se añade al clúster un maestro o maestro en espera se convierte en el maestro primario. Una vez que se crea un mínimo de un maestro primario y un maestro en espera, podrá añadir maestros al clúster desde cualquier maestro en el clúster. Utilice el diálogo Configuración de multimaestro - Añadir maestro o el **Servicio REST Añadir maestro** para añadir un maestro al clúster. Su rol debe tener un permiso para añadir un maestro en espera al clúster multimaestro de IBM Security Key Lifecycle Manager.

No puede añadir un maestro en espera al clúster utilizando la página Configuración de multimaestro - Añadir maestro cuando un servidor en espera o maestro del clúster está fuera de la red o no está accesible. Para añadir un maestro en espera en este caso de ejemplo, debe utilizar **Servicio REST Añadir maestro** con parámetros adicionales. Para obtener más información sobre el servicio REST, consulte Servicio REST para añadir un maestro cuando no se puede acceder a otro maestro del clúster.

Procedimiento

1. Vaya al directorio o la página apropiada.

   Interfaz gráfica de usuario

   a. Inicie una sesión en la interfaz gráfica de usuario.
   b. En la página de Bienvenida, pulse **Administración** > **Multimaestro** > **Maestros** > **Añadir maestro**.

   Interfaz REST

   Abra un cliente REST.

2. Añada un maestro en espera al clúster.

   Interfaz gráfica de usuario

   a. Pulse el separador **Propiedades básicas**.
   b. En el diálogo Propiedades básicas, especifique la información del maestro en espera que está añadiendo.

Nombre de host / Dirección IP	Especifique el nombre de host del maestro en espera de IBM Security Key Lifecycle Manager que se añade al clúster.
Nombre de usuario de IBM Security Key Lifecycle Manager	Especifique el nombre del administrador de IBM Security Key Lifecycle Manager. De forma predeterminada se visualiza el nombre del administrador.
Contraseña de IBM Security Key Lifecycle Manager	Especifique la contraseña del administrador del servidor de IBM Security Key Lifecycle Manager.
Nombre de usuario de WebSphere Application Server	Especifique el ID de usuario de inicio de sesión de WebSphere Application Server del perfil de administrador de servidor de IBM Security Key Lifecycle Manager. De forma predeterminada se visualizará el ID de inicio de sesión de WebSphere Application Server.
Contraseña de WebSphere Application Server	Especifique la contraseña del ID de usuario de inicio de sesión de WebSphere Application Server.
Puerto de interfaz de usuario	Especifique el puerto HTTPS para acceder a los servicios REST y a la interfaz gráfica de usuario de IBM Security Key Lifecycle Manager. Se visualiza el puerto predeterminado.

c. Pulse en el separador **Propiedades avanzadas**.

d. En el diálogo Propiedades avanzadas, especifique la información del maestro en espera que está añadiendo.

¿Desea establecer este maestro como base de datos en espera?	Seleccione **Sí** para añadir al clúster la instancia actual de IBM Security Key Lifecycle Manager como un maestro en espera.
Puerto de HADR	Especifique el número de puerto para la base de datos HADR en espera para comunicarse con la base de datos primaria HADR.
Índice de prioridad en espera	Especifique el valor de índice de prioridad para la base de datos en espera que tomará el control cuando la base de datos primaria esté caída. Puede establecer el índice de prioridad con cualquier valor en el rango 1-3. El servidor en espera con un nivel de índice de prioridad más elevado (número más bajo) tendrá la prioridad sobre las bases de datos con un nivel de prioridad más bajo.

e. Pulse **Conexión de prueba** para probar si la conexión entre el maestro en espera que está añadiendo y el maestro primario actual es satisfactoria. Para obtener más información, consulte Realizar una conexión de prueba.

f. Pulse **Añadir**.

Interfaz REST

a. Obtenga un identificador de autenticación de usuario exclusivo para acceder a los servicios REST de IBM Security Key Lifecycle Manager. Para obtener más información sobre el proceso de autenticación, consulte Proceso de autenticación de los servicios REST.

b. Para ejecutar el **`Servicio REST Añadir maestro`**, envíe la solicitud HTTP POST. Pase el identificador de autenticación de usuario que ha obtenido en el `Paso a` junto con el mensaje de solicitud, como se muestra en el ejemplo siguiente.

```
POST https://localhost:<puerto>/SKLM/rest/v1/ckms/config/nodes/addNodes
Content-Type: application/json
Accept: application/json
Authorization: SKLMAuth userAuthId=139aeh34567m
[
{
"clusterName" : "multimaster",
"hadrPort" : "60020"
},
{
"type" : "Standby",
"ipHostname" :  "cimkc2b151",
"httpPort" :  "443",
"sklmUsername" :  "sklmadmin",
"sklmPassword" :  "SKLM@admin123",
"wasUsername" :  "wasadmin",
"wasPassword" :  "WAS@admin123",
"standbyPriorityIndex" : "1",
"autoAccept" : "Yes"
}
]
```

Qué hacer a continuación

El maestro primario se reinicia, y está temporalmente no disponible durante este proceso después de añadir un maestro en espera al clúster. Verifique que se muestre el maestro en espera y la información de estado de salud en la tabla de Maestro y también en la página de bienvenida de IBM Security Key Lifecycle Manager.

Adición de un maestro al clúster

En IBM Security Key Lifecycle Manager, la solución de alta disponibilidad se implementa utilizando la configuración de clúster multimaestro. La adición de un maestro al clúster es parte de la configuración de un entorno multimaestro.

Antes de empezar

Complete las siguientes tareas:

- Revise las consideraciones y las restricciones que se listan en el tema Requisitos y consideraciones para la configuración de multimaestro.
- Ejecute Servicio REST Comprobar requisitos previos para asegurarse de que el maestro que desea añadir cumple con todos los requisitos y condiciones que se definen para la configuración de multimaestro de IBM Security Key Lifecycle Manager.
- Antes de añadir un maestro no HADR al clúster multimaestro, asegúrese de que se ha añadido al menos un maestro en espera en el clúster. Para obtener instrucciones sobre cómo añadir un maestro en espera, consulte “Adición de un maestro en espera al clúster” en la página 250.

Acerca de esta tarea

Cuando se crea un clúster multimaestro de IBM Security Key Lifecycle Manager, el servidor desde el que se añade al clúster un maestro o maestro en espera se convierte en el maestro primario. Una vez que se crea un mínimo de un maestro primario y un maestro en espera, podrá añadir maestros al clúster desde cualquier maestro en el clúster. Utilice la página Configuración de multimaestro - Añadir

maestro o **Servicio REST Añadir maestro** para añadir un maestro al clúster. Su rol debe tener un permiso para añadir un maestro al clúster multimaestro de IBM Security Key Lifecycle Manager.

No puede añadir un maestro al clúster utilizando la página Configuración de multimaestro - Añadir maestro cuando un servidor en espera o maestro del clúster está fuera de la red o no está accesible. Para añadir un maestro en este caso de ejemplo, debe utilizar **Servicio REST Añadir maestro** con parámetros adicionales. Para obtener más información sobre el servicio REST, consulte Servicio REST para añadir un maestro cuando no se puede acceder a otro maestro del clúster.

Procedimiento

1. Vaya al directorio o la página apropiada.

   Interfaz gráfica de usuario

   a. Inicie una sesión en la interfaz gráfica de usuario.
   b. En la página de Bienvenida, pulse **Administración** > **Multimaestro** > **Maestros** > **Añadir maestro**.

   Interfaz REST

   Abra un cliente REST.

2. Añada un maestro al clúster.

   Interfaz gráfica de usuario

   a. Pulse el separador **Propiedades básicas**.
   b. En el diálogo Propiedades básicas, especifique la información del maestro que está añadiendo.

Nombre de host / dirección IP	Especifique el nombre de host de la instancia de IBM Security Key Lifecycle Manager que se añade al clúster.
Nombre de usuario de IBM Security Key Lifecycle Manager	Especifique el nombre del administrador de IBM Security Key Lifecycle Manager. De forma predeterminada se visualiza el nombre del administrador.
Contraseña de IBM Security Key Lifecycle Manager	Especifique la contraseña del administrador del servidor de IBM Security Key Lifecycle Manager.
Nombre de usuario de WebSphere Application Server	Especifique el ID de usuario de inicio de sesión de WebSphere Application Server del perfil de administrador de servidor de IBM Security Key Lifecycle Manager. De forma predeterminada se visualizará el ID de inicio de sesión de WebSphere Application Server.
Contraseña de WebSphere Application Server	Especifique la contraseña del ID de usuario de inicio de sesión de WebSphere Application Server.
Puerto de interfaz de usuario	Especifique el puerto HTTPS para acceder a los servicios REST y a la interfaz gráfica de usuario de IBM Security Key Lifecycle Manager. Se visualiza el puerto predeterminado.

c. Pulse **Conexión de prueba** para probar si la conexión entre el maestro que está añadiendo y el servidor maestro primario actual es satisfactoria. Para obtener más información, consulte Realizar una conexión de prueba.

d. Pulse **Añadir**.

Interfaz REST

a. Obtenga un identificador de autenticación de usuario exclusivo para acceder a los servicios REST de IBM Security Key Lifecycle Manager. Para obtener más información sobre el proceso de autenticación, consulte Proceso de autenticación de los servicios REST.

b. Para ejecutar el **Servicio REST Añadir maestro**, envíe la solicitud HTTP POST. Pase el identificador de autenticación de usuario que ha obtenido en el Paso a junto con el mensaje de solicitud, como se muestra en el ejemplo siguiente.

```
POST https://localhost:<puerto>/SKLM/rest/v1/ckms/config/nodes/addNodes
Content-Type: application/json
Accept: application/json
Authorization: SKLMAuth userAuthId=139aeh34567m
[
{
"clusterName" : "multimaster",
"primaryHadrPort" : "60020"
},
{
"type" : "Node",
"ipHostname": "cimkc2b151",
"httpPort": "443",
"sklmUsername": "sklmadmin",
"sklmPassword": "SKLM@admin123",
"wasUsername": "wasadmin",
"wasPassword": "WAS@admin123",
"autoAccept": "Yes"
}
]
```

Qué hacer a continuación

El maestro primario se reinicia, y está temporalmente no disponible durante este proceso después de añadir un maestro al clúster. Verifique que se muestre el maestro y la información de estado de salud en la tabla de Maestro y también en la página de bienvenida de IBM Security Key Lifecycle Manager.

Adición de una instancia de IBM Security Key Lifecycle Manager existente con datos para el clúster multimaestro

Puede utilizar la característica de exportación e importación de IBM Security Key Lifecycle Manager para añadir datos de una instancia de IBM Security Key Lifecycle Manager existente al clúster multimaestro. Debe importar los datos que se exportan desde la instancia autónoma existente al servidor maestro primario que se ha configurado con DB2 HADR.

Acerca de esta tarea

No se puede añadir directamente una instancia autónoma existentes con los datos del clúster. Primero debe importar datos de la instancia existente de IBM Security Key Lifecycle Manager al maestro primario. A continuación, añada un servidor maestro al clúster por separado.

Cuando se importan datos, los datos están disponibles en todas las instancias del clúster. Decida usted si desea añadir un maestro por separado.

Procedimiento

1. Exporte datos del grupo de dispositivos desde la instancia existente de IBM Security Key Lifecycle Manager. Para obtener más información sobre cómo exportar datos del grupo de dispositivos, consulte "Exportación de un grupo de dispositivos" en la página 115.
2. Importe los datos que ha exportado desde la instancia autónoma existente al servidor maestro primario que se ha configurado con DB2 HADR. Para obtener más información sobre cómo importar datos del grupo de dispositivos, consulte "Importación de un grupo de dispositivos" en la página 117.
3. Después de importar los datos satisfactoriamente en el servidor primario, puede acceder a datos de todos los maestros en el clúster. Si necesita un maestro dedicado de IBM Security Key Lifecycle Manager para acceder a los datos importados, añada un maestro al clúster. Para obtener más información sobre cómo añadir un maestro, consulte "Adición de un maestro al clúster" en la página 253.

Qué hacer a continuación

Puede que desee dejar fuera de servicio la instancia autónoma existente de IBM Security Key Lifecycle Manager una vez que haya exportado correctamente los datos.

Modificación de los detalles de un clúster

Puede cambiar la configuración de multimaestro de IBM Security Key Lifecycle Manager, como por ejemplo modificando los detalles del servidor maestro para satisfacer sus requisitos. Por ejemplo, puede actualizar la contraseña del administrador de IBM Security Key Lifecycle Manager.

Antes de empezar

Antes de modificar los detalles de los maestros del clúster, revise las consideraciones y restricciones que se listan en el tema Requisitos y consideraciones para la configuración de multimaestro.

Acerca de esta tarea

Utilice el diálogo Configuración de multimaestro - Modificar maestro o el **Servicio REST Modificar maestro** para modificar los detalles del maestro.

Debe poseer un rol con permiso para modificar los detalles de un servidor maestro en el clúster multimaestro de IBM Security Key Lifecycle Manager.

Antes de añadir un servidor maestro al clúster mediante el sistema migrado, debe modificar el nombre de usuario y la contraseña del administrador de IBM Security Key Lifecycle Manager en las siguientes situaciones:

1. Cuando los usuarios y grupos se migran desde la versión anterior a la versión 3.0.1 a través del proceso de migración cruzada.
2. El nombre de usuario y la contraseña del usuario administrador de IBM Security Key Lifecycle Manager son distintos de las credenciales especificadas durante la instalación de la versión 3.0.1.

Procedimiento

1. Vaya al directorio o la página apropiada.

   Interfaz gráfica de usuario

   a. Inicie una sesión en la interfaz gráfica de usuario.
   b. En la página de Bienvenida, pulse **Administración** > **Multimaestro** > **Maestros**.

   Interfaz REST

   Abra un cliente REST.

2. Modifique los detalles del maestro.

   Interfaz gráfica de usuario

   a. Desde la tabla de **Maestros**, seleccione el maestro que desea modificar.
   b. Pulse el separador **Modificar maestro**. Como alternativa, efectúe una doble pulsación en la entrada del maestro seleccionado.
   c. En el diálogo Configuración de multimaestro - Modificar maestro, modifique los detalles del maestro según sea necesario.
   d. Pulse **Conexión de prueba** para probar que la comunicación entre el maestro que está modificando y el servidor primario actual es satisfactoria. Para obtener más información, consulte Realizar una conexión de prueba.
   e. Pulse **Actualizar**.

   Interfaz REST

   a. Obtenga un identificador de autenticación de usuario exclusivo para acceder a los servicios REST de IBM Security Key Lifecycle Manager. Para obtener más información sobre el proceso de autenticación, consulte Proceso de autenticación de los servicios REST.
   b. Para ejecutar el **Servicio REST Modificar maestro**, envíe la solicitud HTTP POST. Pase el identificador de autenticación de usuario que ha obtenido en el Paso a junto con el mensaje de solicitud, como se muestra en el ejemplo siguiente.

```
POST https://localhost:<puerto>/SKLM/rest/v1/ckms/config/nodes/updateMaster
Content-Type: application/json
Accept: application/json
Authorization: SKLMAuth userAuthId=139aeh34567m
{
"type" : "Standby",
"ipHostname": "cimkc2b151",
"httpPort": "443",
"sklmUsername": "sklmadmin",
"sklmPassword": "SKLM@admin123",
"wasUsername": "wasadmin",
"wasPassword": "WAS@admin123",
}
]
```

Qué hacer a continuación

Verifique la información del estado de salud del maestro que ha modificado en la tabla de Maestros y también en la página de bienvenida de IBM Security Key Lifecycle Manager.

Realizar una conexión de prueba

Después de definir los parámetros para añadir o modificar un maestro de IBM Security Key Lifecycle Manager, realice una conexión de prueba para asegurarse de que la información de conexión es correcta.

Para realizar una conexión de prueba, pulse **Probar conexión** en la página Configuración de multimaestro. Si **Probar conexión** devuelve un error, verifique los siguientes valores. A continuación, vuelva a probar la conexión.

- Verifique si es posible acceder al servidor maestro de IBM Security Key Lifecycle Manager.
- Verifique si el nombre de host del servidor maestro de IBM Security Key Lifecycle Manager es correcto.
- Verifique si las credenciales de usuario para el maestro de IBM Security Key Lifecycle Manager son correctas.
- Verifique si el puerto HTTP está habilitado.

Eliminación de un maestro de un clúster multimaestro

Una vez no sea necesario, puede eliminar un maestro del clúster multimaestro de IBM Security Key Lifecycle Manager.

Antes de empezar

Antes de suprimir un maestro del clúster, revise las consideraciones y restricciones que se listan en el tema Requisitos y consideraciones para la configuración de multimaestro.

Acerca de esta tarea

No puede suprimir un maestro primario del clúster. Un maestro en espera solo se puede suprimir cuando el clúster contiene varios maestros en espera. Un clúster multimaestro de IBM Security Key Lifecycle Manager da soporte a hasta tres maestros en espera.

Utilice la página Multimaestro de IBM Security Key Lifecycle Manager o el **`Servicio REST Eliminar maestro`** para suprimir un maestro.

Debe poseer un rol con permiso para suprimir maestros del clúster.

Procedimiento

1. Vaya al directorio o la página apropiada.

   Interfaz gráfica de usuario

   a. Inicie una sesión en la interfaz gráfica de usuario.
   b. En la página de Bienvenida, pulse **Administración** > **Multimaestro**.

   Interfaz REST

   Abra un cliente REST.

2. Suprima el maestro.

   Interfaz gráfica de usuario

   a. Desde la tabla de **Maestros**, seleccione el maestro que desea suprimir.
   b. Pulse **Suprimir maestro**.

c. En el diálogo Confirmar, lea el mensaje de confirmación antes de suprimir el maestro.
d. Pulse **Aceptar**.

Interfaz REST

a. Obtenga un identificador de autenticación de usuario exclusivo para acceder a los servicios REST de IBM Security Key Lifecycle Manager. Para obtener más información sobre el proceso de autenticación, consulte Proceso de autenticación de los servicios REST.
b. Para ejecutar el **Servicio REST Eliminar maestro**, envíe la solicitud HTTP POST. Pase el identificador de autenticación de usuario que ha obtenido en el Paso a junto con el mensaje de solicitud, como se muestra en el ejemplo siguiente.

```
POST https://localhost:<puerto>/SKLM/rest/v1/ckms/config/nodes/removeNode
Content-Type: application/json
Accept: application/json
Authorization: SKLMAuth userAuthId=139aeh34567m
[
{"clusterName": "multimaster"},
{"type": "Node",
"ipHostname" : "cimkc2b151",
"httpPort" : "443",
"sklmUsername" : "sklmadmin",
"sklmPassword" : "SKLM@admin123",
"wasUsername" : "wasadmin",
"wasPassword" : "WAS@admin123"}
]
```

3. Reinicie WebSphere Application Server para renovar la configuración.

Qué hacer a continuación

Verifique que el maestro que el maestro que ha eliminado no aparezca en la tabla de Maestros.

Promoción de un servidor en espera a servidor primario

Si un maestro primario en el clúster multimaestro de IBM Security Key Lifecycle Manager falla, podría querer promover un maestro en espera mientras se resuelve la anomalía.

Antes de empezar

Antes de promover un maestro de en espera al clúster, revise las consideraciones y restricciones que se listan en el tema Requisitos y consideraciones para la configuración de multimaestro.

Acerca de esta tarea

Si el maestro primario pasa a no estar disponible, utilice la página **Multimaestro de IBM Security Key Lifecycle Manager** > **Bases de datos HADR** o el **Servicio REST Promover maestro en espera** para cambiar un maestro en espera a maestro primario en el clúster.

Debe poseer un rol con permiso para cambiar maestros en espera a maestros primarios en el clúster multimaestro de IBM Security Key Lifecycle Manager.

Debe reiniciar manualmente WebSphere Application Server en todos los servidores en espera si un sistema en espera auxiliar se promociona como primario. No es necesario el reinicio de WebSphere Application Server cuando el sistema en espera principal se promociona como primario.

Procedimiento

1. Vaya al directorio o la página apropiada.

   Interfaz gráfica de usuario

   a. Inicie una sesión en la interfaz gráfica de usuario.
   b. En la página de Bienvenida, pulse **Administración** > **Multimaestro** > **Bases de datos de HADR**.

   Interfaz REST

   Abra un cliente REST.

2. Promocione el maestro en espera a servidor maestro primario.

   Interfaz gráfica de usuario

   a. En la tabla **Bases de datos de HADR**, seleccione el maestro en espera que desea promover.
   b. Pulse **Promover como primario**.
   c. En el diálogo Confirmar, lea el mensaje de confirmación antes de promover el maestro en espera.
   d. Pulse **Aceptar**.

   Interfaz REST

   a. Obtenga un identificador de autenticación de usuario exclusivo para acceder a los servicios REST de IBM Security Key Lifecycle Manager. Para obtener más información sobre el proceso de autenticación, consulte Proceso de autenticación de los servicios REST.
   b. Para ejecutar el **Servicio REST Promover maestro en espera**, envíe la solicitud HTTP POST. Pase el identificador de autenticación de usuario que ha obtenido en el `Paso a` junto con el mensaje de solicitud, como se muestra en el ejemplo siguiente.

```
POST https://localhost:<puerto>/SKLM/rest/v1/ckms/config/nodes/takeoverAsPrimary
Content-Type: application/json
Accept: application/json
Authorization: SKLMAuth userAuthId=139aeh34567m
[
{clusterName:"multimaster"},
{"ipHostname": "civ3cez160"}
]
```

Qué hacer a continuación

Verifique la información de estado de salud y el rol del maestro en espera que ha promocionado en la tabla Bases de datos HADR y también en la página de bienvenida de IBM Security Key Lifecycle Manager.

Visualización de la lista de servidores maestros y su estado de configuración

Puede ver la lista de servidores maestros de IBM Security Key Lifecycle Manager y su estado de salud en el clúster multimaestro para ayudarle a identificar problemas, si hay alguno, en los maestros. También puede ver el estado de configuración de DB2 HADR de los maestros primarios y en espera.

Acerca de esta tarea

En un clúster multimaestro, supervisar periódicamente el estado de salud de las instancias de IBM Security Key Lifecycle Manager es esencial para identificar y corregir rápidamente los problemas. Puede comprobar si es posible acceder a todos los puertos de comunicación y si están activos en cada servidor maestro en su despliegue de multimaestro.

Utilice la página Multimaestro de IBM Security Key Lifecycle Manager o el **Servicio REST Obtener estado de todos los maestros** para visualizar una lista de servidores y su estado.

También puede visualizar la lista de maestros y la información de estado en la página de bienvenida de IBM Security Key Lifecycle Manager.

Procedimiento

1. Vaya al directorio o la página apropiada.

   Interfaz gráfica de usuario

   a. Inicie una sesión en la interfaz gráfica de usuario.
   b. En la página de Bienvenida, pulse **Administración** > **Multimaestro**.

   Interfaz REST

   Abra un cliente REST.

2. Visualice la lista de servidores y su información de estado de salud para identificar cualquier problema, si es que lo hay.

   Interfaz gráfica de usuario

   El estado de configuración de DB2 HADR se visualiza en la página de Multimaestro de IBM Security Key Lifecycle Manager.

   a. Pulse el separador **Maestros** para ver la lista de maestros configurados para la réplica de multimaestro y su estado de configuración.
   b. Pulse el separador **Bases de datos de HADR** para ver la lista de maestros configurados con DB2 HADR y su estado de configuración.

   Interfaz REST

   a. Obtenga un identificador de autenticación de usuario exclusivo para acceder a los servicios REST de IBM Security Key Lifecycle Manager. Para obtener más información sobre el proceso de autenticación, consulte Proceso de autenticación de los servicios REST.
   b. Para ejecutar el **Servicio REST Obtener estado de todos los maestros**, envíe la solicitud HTTP POST. Pase el identificador de autenticación de usuario que ha obtenido en el `Paso a` junto con el mensaje de solicitud, como se muestra en el ejemplo siguiente.

      ```
      GET https://localhost:<puerto>/SKLM/rest/v1/ckms/nodes/allNodeStatus
      Content-Type: application/json
      Accept : application/json
      Authorization: SKLMAuth userAuthId=139aeh34567m
      Accept-Language : en
      ```

      Para obtener más información, consulte Servicio REST Obtener estado de todos los maestros.

Qué hacer a continuación

Utilice la información de estado en la tabla para investigar problemas, si hay alguno, y tomar las medidas necesarias.

Visualización de la información de resumen de un maestro

Utilice la página Detalles de maestro para ver los detalles de un servidor maestro seleccionado en el clúster multimaestro de IBM Security Key Lifecycle Manager para entender y trabajar con los datos de configuración.

Procedimiento

1. Inicie una sesión en la interfaz gráfica de usuario.
2. Pulse **Administración** > **Multimaestro** en la página de Bienvenida.
3. Seleccione un servidor maestro que esté en la lista de la tabla.
4. Pulse con el botón derecho del ratón sobre el servidor maestro y a continuación selecciones **Resumen** o efectúe una doble pulsación sobre la entrada maestra.

   En la tabla siguiente se proporciona la información de resumen.

IPP	Puerto en el que el servidor de IBM Security Key Lifecycle Manager está a la escucha de solicitudes de los dispositivos que se comunican mediante el protocolo IPP (IBM Proprietary Protocol).
SSL	Puerto en el que el servidor de IBM Security Key Lifecycle Manager está a la escucha de solicitudes de los dispositivos que se comunican mediante el protocolo SSL.
IU de administración	Puerto de WebSphere Application Server para el perfil de IBM Security Key Lifecycle Manager.
IU de aplicación	Puerto HTTPS para acceder a los servicios REST y a la interfaz gráfica de usuario de IBM Security Key Lifecycle Manager.
KMIP	Puerto en el que el servidor de IBM Security Key Lifecycle Manager está a la escucha de solicitudes para comunicarse a través del socket SSL que utiliza el protocolo KMIP (Key Management Interoperability Protocol).
Base de datos	Puerto en el que el servidor de IBM Security Key Lifecycle Manager está a la escucha de solicitudes de DB2.
Puerto de HADR	Puerto para las bases de datos configuradas como de HADR para las comunicaciones de bases de datos.
Agente	Puerto en el que el agente está a la escucha de la comunicación desde IBM Security Key Lifecycle Manager.

5. Pulse **Aceptar** para cerrar la página de resumen.

Configuración de un maestro aislado como maestro de lectura-escritura

Debido a problemas de conectividad/red, un servidor maestro podría no comunicarse con otros maestros en el clúster, por lo que quedaría aislado del clúster. Existe la posibilidad de configurar estos maestros aislados con su base de datos local en una modalidad de lectura-escritura. Después de la configuración en la modalidad de lectura-escritura, todos los dispositivos y clientes KMIP que

estuviesen registrados en el maestro aislado podrían comunicarse de forma transparente con el servidor, sin que fuese necesario realizar ningún cambio en los clientes/dispositivos.

Antes de empezar

Antes de configurar el maestro aislado como maestro de lectura-escritura, revise las consideraciones y restricciones que se listan en el tema Requisitos y consideraciones para la configuración de multimaestro.

Acerca de esta tarea

Después de la configuración en modalidad de lectura-escritura, puede añadir nuevos dispositivos y clientes KMIP al servidor, el maestro de lectura-escritura les seguirá dando servicio. Sin embargo, existen varias restricciones las funciones e interfaces del maestro de lectura-escritura aislado. Todas las operaciones de modificación y supresión en grupos de dispositivos, grupos de claves, cliente KMIP y objetos gestionados quedan inhabilitadas para mantener la coherencia de los datos en caso de que el maestro aislado se reincorpore de nuevo al clúster multimaestro. También ser restringen algunas funciones administrativas como, por ejemplo, la réplica, la configuración del multimaestro o la restauración de archivos de copia de seguridad.

Procedimiento

1. Vaya a la página apropiada.

   Interfaz gráfica de usuario

   a. Inicie una sesión en la interfaz gráfica de usuario del maestro aislado.

   Interfaz REST

   a. Abra un cliente REST.

2. Configure el maestro aislado como maestro de lectura-escritura.

   Interfaz gráfica de usuario

   a. Pulse el enlace **Unir de nuevo este maestro al clúster de lectura-escritura** en el área de notificación de la página Bienvenida de IBM Security Key Lifecycle Manager.

   b. En el diálogo Confirmación, lea el mensaje de confirmación antes de configurar el maestro aislado en la modalidad de lectura-escritura.

   c. Pulse **Aceptar**.

   Interfaz REST

   a. Obtenga un identificador de autenticación de usuario exclusivo para acceder a los servicios REST de IBM Security Key Lifecycle Manager. Para obtener más información sobre el proceso de autenticación, consulte Proceso de autenticación de los servicios REST.

   b. Para ejecutar el **`Servicio REST Configurar el maestro de lectura-escritura`**, envíe la solicitud HTTP GET. Pase el identificador de autenticación de usuario que ha obtenido en el `Paso a` junto con el mensaje de solicitud, como se muestra en el ejemplo siguiente.

```
GET https://localhost:<puerto>/SKLM/rest/v1/ckms/config/nodes/setupAsReadWriteMaster
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth userAuthId=139aeh34567m
Accept-Language : en
```

Reincorporación de nuevo al clúster de un maestro de lectura-escritura aislado

El servidor maestro, que se aisló del clúster multimaestro, y que se configuró como maestro de lectura-escritura, se puede reincorporar al clúster cuando se hayan resuelto los problemas de conectividad/red. Los datos del maestro de lectura-escritura aislado se fusionan en la base de datos primaria del clúster durante el proceso de reincorporación.

Antes de empezar

Antes de reincorporar un maestro de lectura-escritura al clúster, revise las consideraciones y restricciones que se listan en el tema Requisitos y consideraciones para la configuración de multimaestro.

Acerca de esta tarea

La operación de reincorporación comprueba posibles conflictos entre los datos del maestro de lectura-escritura aislado y el maestro primario del clúster. Se generará un informe de conflictos, si hay, para que los pueda ver. El maestro de lectura-escritura aislado únicamente se podrá reincorporar al clúster cuando se hayan resuelto todos los conflictos. Para obtener más información sobre cómo visualizar y resolver conflictos, consulte "Visualización del informe de conflictos" en la página 265.

Procedimiento

1. Vaya a la página apropiada.

   Interfaz gráfica de usuario

   a. Inicie una sesión en la interfaz gráfica de usuario del maestro aislado.
   b. Pulse el enlace **Unir de nuevo este maestro al clúster multimaestro** en el área de notificación en la página de bienvenida de IBM Security Key Lifecycle Manager.
   c. En el diálogo Confirmar, lea el mensaje de confirmación antes de reincorporar el maestro al clúster.
   d. Pulse **Aceptar** para iniciar el proceso de reincorporación.

   Interfaz REST

   a. Abra un cliente REST.
   b. Obtenga un identificador de autenticación de usuario exclusivo para acceder a los servicios REST de IBM Security Key Lifecycle Manager. Para obtener más información sobre el proceso de autenticación, consulte Proceso de autenticación de los servicios REST.
   c. Para ejecutar **`Servicio REST Unir de nuevo a clúster`**, envíe la solicitud HTTP GET. Pase el identificador de autenticación de usuario que ha obtenido en el `Paso b` junto con el mensaje de solicitud, como se muestra en el ejemplo siguiente.

```
GET https://localhost:<port>/SKLM/rest/v1/ckms/config/nodes/joinBackTheCluster
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth userAuthId=139aeh34567m
Accept-Language : en
```

2. Si aparecen conflictos durante el proceso de reincorporación, se visualizará la ventana "Conflictos con el clúster multimaestro". Consulte el tema "Visualización del informe de conflictos" para obtener más información.
3. Si no se han producido conflictos de datos, se abre el recuadro de progreso. Cuando el proceso se completa, se visualiza un recuadro de mensaje que indica que se ha completado la operación de reincorporación.
4. Pulse **Cerrar**.
5. Reinicie el servidor. Para obtener instrucciones sobre cómo detener e iniciar el servidor, consulte el apartado "Reinicio de IBM Security Key Lifecycle Manager server" en la página 205.

Visualización del informe de conflictos

Durante la reincorporación de un maestro de lectura-escritura al clúster, sus datos se analizan para ver si hay conflictos con los datos del maestro primario del clúster. Los conflictos se deben resolver antes de que los datos del maestro de lectura-escritura aislado se fusionen con la base de datos primaria. Puede ver una lista de conflictos para analizar y resolver los problemas. Puede exportar los datos de los conflictos en un formato de valores separados por comas (CSV).

Procedimiento

1. Vaya a la página apropiada.

   Interfaz gráfica de usuario

   a. Inicie una sesión en la interfaz gráfica de usuario del maestro de lectura-escritura aislado.
   b. Pulse el enlace **Unir de nuevo este maestro al clúster multimaestro** en el área de notificación en la página de bienvenida de IBM Security Key Lifecycle Manager.
   c. En el diálogo Confirmar, lea el mensaje de confirmación antes de reincorporar el maestro al clúster.
   d. Pulse **Aceptar** para ejecutar el proceso de reincorporación.

   Interfaz REST

   a. Abra un cliente REST.
   b. Obtenga un identificador de autenticación de usuario exclusivo para acceder a los servicios REST de IBM Security Key Lifecycle Manager. Para obtener más información sobre el proceso de autenticación, consulte Proceso de autenticación de los servicios REST.
   c. Para ejecutar **Servicio REST Unir de nuevo a clúster**, envíe la solicitud HTTP POST. Pase el identificador de autenticación de usuario que ha obtenido en el `Paso b` junto con el mensaje de solicitud, como se muestra en el ejemplo siguiente.

      ```
      GET https://localhost:<port>/SKLM/rest/v1/ckms/config/nodes/joinBackTheCluster
      Content-Type: application/json
      Accept : application/json
      Authorization: SKLMAuth userAuthId=139aeh34567m
      Accept-Language : en
      ```

2. Si aparecen conflictos durante el proceso de reincorporación, se visualizará una lista de conflictos en la ventana "Conflictos con el clúster multimaestro".
3. Para exportar los datos de los conflictos a un archivo con formato de valores separados por comas (CSV), pulse **Exportar informe de conflictos**.

Qué hacer a continuación

Debe resolver los conflictos antes de que se puedan fusionar los datos del maestro de lectura-escritura aislado en la base de datos primaria. Puede utilizar los siguientes servicios REST para resolver conflictos.

- **Servicio REST Cambiar nombre**
- **Servicio REST Cambiar alias de certificado**
- **Servicio REST Historial de cambios**
- **Servicio REST Renovar alias de clave**

Actualización de la contraseña de Db2 en el clúster multimaestro de IBM Security Key Lifecycle Manager

Cuando entra en vigor la restricción de caducidad de una contraseña, debe cambiar la contraseña antes de que pase el periodo de caducidad.

Antes de empezar

Asegúrese de que conoce la contraseña existente que desea cambiar.

Acerca de esta tarea

Debe ser el propietario de la instancia de la base de datos en sistemas AIX o Linux, o el administrador local en sistemas Windows. La contraseña de inicio de sesión para el ID de usuario administrador de Db2 y la contraseña del origen de datos de Db2 que utiliza WebSphere® Application Server debe ser la misma. Cuando se cambia una, deberá cambiar la otra.

Debe asegurarse de que el nombre de usuario y la contraseña de Db2 deben ser los mismos en todos los maestros del clúster multimaestro de IBM Security Key Lifecycle Manager.

Procedimiento

1. Detenga Db2 HADR en el maestro primario de IBM Security Key Lifecycle Manager con la base de datos primaria.

   Windows

   a. Pulse **Inicio** > **IBM DB2 DBSKLMV301 (Default)** > **Ventana de mandatos de DB2 - Administrador**.
   b. Escriba el siguiente mandato y pulse Intro.
      ```
      db2 stop hadr on database sklmdb31
      ```

   Linux

   a. En una ventana de terminal, escriba el mandato siguiente para cambiar el propietario de instancia de DB2.
      ```
      su -sklmdb31
      ```
   b. Ejecute el siguiente mandato.
      ```
      db2 stop hadr on database sklmdb31
      ```

2. Desactive la base de datos en espera en el maestro en espera de IBM Security Key Lifecycle Manager ejecutando el siguiente mandato.

   ```
   db2 deactivate db sklmdb31
   ```

3. Detenga Db2 HADR en el maestro en espera de IBM Security Key Lifecycle Manager con la base de datos en espera ejecutando el mandato siguiente.

   ```
   db2 stop hadr on database sklmdb31
   ```

4. Detenga WebSphere Application Server en todas las IBM Security Key Lifecycle Manager instancias del clúster multimaestro. Consulte el tema "Reinicio de IBM Security Key Lifecycle Manager server" en la página 205 para obtener los pasos.
5. Detenga el servicio de agente en todas las instancias de IBM Security Key Lifecycle Manager. Consulte el tema "Reinicio del servicio de agente de IBM Security Key Lifecycle Manager" en la página 245 para obtener los pasos.
6. Detenga Db2 en todos los servidores de IBM Security Key Lifecycle Manager del clúster ejecutando el siguiente mandato.

   ```
   db2stop force
   ```

7. Cambie la contraseña de origen de datos de Db2 en todos los servidores de IBM Security Key Lifecycle Manager. Consulte el tema siguiente para obtener los pasos.

   Windows
   Para cambiar la contraseña, ejecute los pasos 7 al 8 en el tema siguiente.

   Problemas de seguridad con la contraseña de Db2 en sistemas Windows

   Linux Para cambiar la contraseña, ejecute los pasos 5 al 6 en el tema siguiente.

   "Problemas de seguridad con la contraseña de Db2 en sistemas Linux o AIX" en la página 38
8. Inicie Db2 en todos los servidores de IBM Security Key Lifecycle Manager del clúster ejecutando el siguiente mandato.

   ```
   db2start
   ```

9. Inicie Db2 HADR en todos los servidores maestro en espera utilizando el siguiente mandato.

   ```
   db2 start hadr on database sklmdb31 as standby
   ```

10. Inicie Db2 HADR en el servidor maestro primario utilizando el siguiente mandato.

    ```
    db2 start hadr on database sklmdb31 as primary
    ```

11. Inicie WebSphere Application Server en el servidor maestro primario. Consulte el tema "Reinicio de IBM Security Key Lifecycle Manager server" en la página 205 para obtener los pasos.
12. Cambie la contraseña de origen de datos de Db2 en WebSphere Application Server en el servidor maestro primario utilizando **uno** de los siguientes métodos:
    - Complete los pasos que se indican en esta nota técnica: http://www.ibm.com/support/docview.wss?uid=ibm10788311

      o
    - Complete los pasos del siguiente modo:

Windows
Para cambiar la contraseña, ejecute los pasos 7 al 8 en el tema siguiente.

Problemas de seguridad con la contraseña de Db2 en sistemas Windows

Linux Para cambiar la contraseña, ejecute los pasos 5 al 6 en el tema siguiente.

"Problemas de seguridad con la contraseña de Db2 en sistemas Linux o AIX" en la página 38

13. Reinicie WebSphere Application Server en el servidor maestro primario.
14. Actualice la contraseña de Db2 en la tabla multimaestra ejecutando Servicio REST Actualizar contraseña de DB2 en todos los maestros.
15. Detenga el servicio de agente en todos los servidores maestro. Para obtener instrucciones, consulte "Detener agente" en la página 247.
16. Reinicie WebSphere Application Server en todos los servidores maestro que no sean primarios. Para obtener instrucciones, consulte "Reinicio de IBM Security Key Lifecycle Manager server" en la página 205.
17. Cambie la contraseña de origen de datos de Db2 en WebSphere Application Server en todos los servidores maestro que no sean primarios utilizando uno de los siguientes métodos:
    - Complete los pasos que se indican en esta nota técnica: http://www.ibm.com/support/docview.wss?uid=ibm10788311

      o
    - Complete los pasos del siguiente modo:

      Windows
      Para cambiar la contraseña, ejecute los pasos 7 al 8 en el tema siguiente.

      Problemas de seguridad con la contraseña de Db2 en sistemas Windows

      Linux Para cambiar la contraseña, ejecute los pasos 5 al 6 en el tema siguiente.

      "Problemas de seguridad con la contraseña de Db2 en sistemas Linux o AIX" en la página 38
18. Detenga el servicio de agente en todos los servidores maestro del clúster. Para obtener instrucciones, consulte "Detener agente" en la página 247.
19. Reinicie WebSphere Application Server en todos los servidores de IBM Security Key Lifecycle Manager del clúster. Para obtener instrucciones, consulte "Reinicio de IBM Security Key Lifecycle Manager server" en la página 205

Preguntas frecuentes sobre IBM Security Key Lifecycle Manager multimaestro

Las preguntas frecuentes (FAQ) sobre IBM Security Key Lifecycle Manager multimaestro pueden ayudarle a comprender mejor los procesos de configuración multimaestros.

P) Cuando los maestros de IBM Security Key Lifecycle Manager estén configurados para la configuración de multimaestro, el servicio de sincronización de datos copia automáticamente datos del servidor primario a los servidores maestros a intervalos regulares. ¿Por qué necesito utilizar la característica Copia

de seguridad y restauración de IBM Security Key Lifecycle Manager?

R) Como medida de precaución para evitar la posible pérdida de datos, utilice la característica Copia de seguridad y restauración para realizar copia de seguridad de los datos manualmente en intervalos regulares.

P) He añadido un maestro de IBM Security Key Lifecycle Manager no HADR al clúster multimaestro. ¿Por qué sigo viendo datos de la base de datos local en lugar de datos de la base de datos primaria?

R) El origen de datos de IBM Security Key Lifecycle Manager podría estar apuntando todavía a la base de datos local aún después de agregar satisfactoriamente el maestro al clúster. Después de añadir el maestro al clúster, el origen de datos de WebSphere Application Server debe apuntar a la base de datos primaria.

Puede actualizar manualmente los detalles del servidor en el origen de datos del servidor maestro que ha añadido ejecutando los pasos siguientes.

1. Inicie sesión en la WebSphere Integrated Solutions Console (https://localhost:9083/ibm/console/logon.jsp).
2. Pulse **Recursos** > **JDBC** > **Orígenes de datos** > **SKLM DataSource**.
3. En la página SKLM DataSource, verifique el valor del campo **Nombre de servidor** en la sección **Propiedades de origen de datos comunes y necesarias**. Si se muestra el nombre de host del servidor local, actualice el valor especificando el nombre de host del servidor primario.

   Si el valor del campo **Nombre de servidor** ya está actualizado con el nombre de host del servidor primario, reinicie WebSphere Application Server y cierre la página. De lo contrario, ejecute los pasos siguientes.
4. En la sección **Propiedades adicionales** de la página SKLM DataSource, pulse el enlace **Propiedades de origen de datos de WebSphere Application Server**.
5. En la sección **Características avanzadas de Db2**, compruebe los valores del campo **Nombre de servidor alternativo**.
6. Especifique el nombre de host de los servidores en espera como una lista separada por comas del campo **Nombres de servidor alternativos**.
7. Especifique el número de puerto de los servidores en espera como una lista separada por comas del campo **Números de puerto alternativos**.
8. Guarde los cambios.
9. Pulse **Recursos** > **JDBC** > **Orígenes de datos** > **SKLM scheduler XA Datasource**.
10. Repita los pasos del 3 al 8.
11. Reinicie WebSphere Application Server.

P) ¿Cómo puedo comprobar que la sincronización se está ejecutando entre los maestros primarios y en espera de IBM Security Key Lifecycle Manager?

A) Puede comprobar si se está ejecutando la sincronización entre los maestros primarios y en espera de IBM Security Key Lifecycle Manager verificando la diferencia horaria entre `PRIMARY_LOG_TIME` y `STANDBY_LOG_TIME` Ejecute el mandato siguiente desde la ventana de mandatos de Db2

```
#db2pd -d <SKLM_DBName> –hadr
```

Por ejemplo,

```
#db2pd -d sklmdb31 –hadr
```

Se muestra la salida siguiente.

```
Database Member 0 -- Database SKLMDB31 -- Active -- Up 1 days 21:27:01 -- Date 2018-11-09-20

                        HADR_ROLE = PRIMARY
                      REPLAY_TYPE = PHYSICAL
                        HADR_SYNCMODE = SYNC
                           STANDBY_ID = 1
                        LOG_STREAM_ID = 0
                           HADR_STATE = PEER
                           HADR_FLAGS = TCP_PROTOCOL
                  PRIMARY_MEMBER_HOST = WIN-DBA2ALEJOC8
                     PRIMARY_INSTANCE = SKLMDB31
                       PRIMARY_MEMBER = 0
                  STANDBY_MEMBER_HOST = WIN-VB479C09AG3
                     STANDBY_INSTANCE = SKLMDB31
                       STANDBY_MEMBER = 0
                  HADR_CONNECT_STATUS = CONNECTED
             HADR_CONNECT_STATUS_TIME = 11/08/2017 23:25:28.730219 (1510212328)
          HEARTBEAT_INTERVAL(seconds) = 30
                     HEARTBEAT_MISSED = 0
                   HEARTBEAT_EXPECTED = 2490
                HADR_TIMEOUT(seconds) = 120
        TIME_SINCE_LAST_RECV(seconds) = 3
             PEER_WAIT_LIMIT(seconds) = 0
           LOG_HADR_WAIT_CUR(seconds) = 0.000
    LOG_HADR_WAIT_RECENT_AVG(seconds) = 0.001541
   LOG_HADR_WAIT_ACCUMULATED(seconds) = 45.835
                  LOG_HADR_WAIT_COUNT = 19538
SOCK_SEND_BUF_REQUESTED,ACTUAL(bytes) = 0, 65536
SOCK_RECV_BUF_REQUESTED,ACTUAL(bytes) = 0, 65536
            PRIMARY_LOG_FILE,PAGE,POS = S0000003.LOG, 4891, 191226150
            STANDBY_LOG_FILE,PAGE,POS = S0000003.LOG, 4886, 191205494
                  HADR_LOG_GAP(bytes) = 0
     STANDBY_REPLAY_LOG_FILE,PAGE,POS = S0000003.LOG, 4886, 191205494
       STANDBY_RECV_REPLAY_GAP(bytes) = 0
                    PRIMARY_LOG_TIME = 11/09/2017 20:10:52.000000 (1510287052)
                    STANDBY_LOG_TIME = 11/09/2017 20:10:20.000000 (1510287020)
             STANDBY_REPLAY_LOG_TIME = 11/09/2017 20:10:20.000000 (1510287020)
          STANDBY_RECV_BUF_SIZE(pages) = 4298
              STANDBY_RECV_BUF_PERCENT = 0
            STANDBY_SPOOL_LIMIT(pages) = 380000
                 STANDBY_SPOOL_PERCENT = 0
                    STANDBY_ERROR_TIME = NULL
                  PEER_WINDOW(seconds) = 0
              READS_ON_STANDBY_ENABLED = N
```

En la salida, PRIMARY_LOG_TIME muestra el momento en el que se actualizan los registros de Db2 Transactional para el servidor primario. STANDBY_LOG_TIME muestra el momento en el que se actualizan los registros de Db2 Transactional para el servidor en espera. Puede pasar por alto la diferencia horaria en milisegundos.

P) ¿Cómo puedo ver el estado de los puertos en la configuración de multimaestro de IBM Security Key Lifecycle Manager?

R) La GUI de IBM Security Key Lifecycle Manager utiliza iconos para representar el estado del puerto en las páginas de multimaestro. La tabla siguiente muestra los iconos de estado de puerto y sus significados.

Tabla 5. Iconos de estado y su significado

Icono	Descripción
	Se puede acceder al puerto y a las solicitudes de servicio de acuerdo con las especificaciones.

Tabla 5. Iconos de estado y su significado (continuación)

Icono	Descripción
	No se puede acceder al puerto. El servicio en un puerto específico puede estar inactivo. Renueve el estado utilizando la opción Renovar de la página de la interfaz de usuario.

Q) ¿Cómo puedo ver el estado de Db2 HADR en la configuración de multimaestro de IBM Security Key Lifecycle Manager?

A) La GUI de IBM Security Key Lifecycle Manager utiliza iconos para representar el estado de Db2 HADR en las páginas de multimaestro. La tabla siguiente muestra los iconos de estado de Db2 HADR y sus significados.

Tabla 6. Iconos de estado y su significado

Icono	Descripción
	Db2 HADR está en estado de ejecución. Todos los maestros de HADR están conectados entre sí.
	Db2 HADR está en estado de ejecución, pero no se puede acceder al menos a uno de los maestros de HADR en espera.
	Db2 HADR está inactivo y no es funcional.

Exportación e importación de claves

Puede habilitar la transferencia de datos entre dos servidores de IBM Security Key Lifecycle Manager exportando las claves (simétricas o privadas) desde un servidor (origen) e importándolas al otro servidor (destino).

En función de la versión de IBM Security Key Lifecycle Manager de su servidor, puede utilizar uno de los siguientes métodos para exportar e importar claves:

Tabla 7. Métodos para exportar e importar claves

Método	Versión soportada de IBM Security Key Lifecycle Manager	Enlaces de procedimientos
Interfaz gráfica de usuario	3.0.1	• "Exportación de una clave utilizando la interfaz gráfica de usuario" en la página 272 • "Importación de una clave utilizando la interfaz gráfica de usuario" en la página 273
Servicio REST	Cualquier versión soportada	• Servicio REST Exportar clave • Servicio REST Importar clave
Mandato de CLI	Cualquier versión soportada	• tklmKeyExport • tklmKeyImport

Exportación de una clave utilizando la interfaz gráfica de usuario

Puede exportar claves simétricas y privadas a un archivo de almacén de claves cifrado en un servidor de IBM Security Key Lifecycle Manager. A continuación, puede importar las claves desde este archivo a otro servidor de IBM Security Key Lifecycle Manager para habilitar la transferencia de datos entre estos servidores.

Procedimiento

1. Vaya al directorio o la página apropiada.
   a. Inicie una sesión en la interfaz gráfica de usuario.
   b. Desde el menú principal, pulse **Buscar**.
   c. En el panel de búsqueda izquierdo, en **Tipo de objetos**, seleccione **Clave simétrica** o **Clave privada**, en función de las claves que desee buscar. Como alternativa, también puede buscar grupos de dispositivos cuyas claves desee exportar.
   d. Pulse **Buscar**. Las claves del tipo de clave seleccionado se listan en el panel de la derecha.
2. Exporte las claves a un archivo de almacén de claves.
   a. Desde la lista de claves en el panel derecho, seleccione las claves que desea exportar (Utilice la tecla CTRL para seleccionar varias claves), y pulse **Exportar**.
   b. En la ventana Exportar claves simétricas o Exportar claves privadas, especifique un nombre para el archivo de almacén de claves que se utiliza para almacenar las claves exportadas.
   c. Opcional: Especifique otra ubicación de archivo para guardar el archivo de almacén de claves. De forma predeterminada, el campo **Ubicación del archivo** muestra la vía de acceso del directorio *SKLM_DATA* predeterminada, donde se guarda el archivo de almacén de claves. Por ejemplo, `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data`. Para ver la definición de *SKLM_DATA*, consulte Definiciones para *HOME* y otras variables de directorio.
   d. Para el tipo de claves simétricas: Especifique un certificado como el alias de clave. El certificado es la entrada de clave pública que se utiliza para cifrar las claves simétricas. Solo el poseedor de la clave privada correspondiente podrá acceder a las claves.
   e. Para el tipo de claves privadas: Cree una contraseña de cifrado. Esta contraseña se utilizará para descifrar el archivo de almacén de claves al importar las claves a un servidor de IBM Security Key Lifecycle Manager.
   f. Pulse **Exportar**.

Qué hacer a continuación

Importe las claves al servidor de IBM Security Key Lifecycle Manager con el que desea habilitar la transferencia de datos.

Tareas relacionadas:

"Importación de una clave utilizando la interfaz gráfica de usuario" en la página 273

Puede importar claves privadas y simétricas a un servidor de IBM Security Key Lifecycle Manager para habilitar la transferencia de datos entre este servidor y el servidor desde el cual se han exportado las claves. Las claves que se van a importar deben estar almacenadas en un archivo de almacén de claves cifrado.

Referencia relacionada:

Servicio REST Exportar clave
Utilice el **Servicio REST Exportar clave** para exportar claves secretas o pares de claves públicas/privadas. Una clave secreta es una clave simétrica. Un par de claves públicas/privadas es un par de claves asimétricas con una clave pública y una clave privada.

Importación de una clave utilizando la interfaz gráfica de usuario

Puede importar claves privadas y simétricas a un servidor de IBM Security Key Lifecycle Manager para habilitar la transferencia de datos entre este servidor y el servidor desde el cual se han exportado las claves. Las claves que se van a importar deben estar almacenadas en un archivo de almacén de claves cifrado.

Antes de empezar

Copie el archivo de almacén de claves en la vía de acceso del directorio *SKLM_DATA* predeterminada en el servidor de IBM Security Key Lifecycle Manager donde desea importarlo. Por ejemplo, `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data`.Para ver la definición de *SKLM_DATA*, consulte Definiciones para *HOME* y otras variables de directorio.

Procedimiento

1. Vaya al directorio o la página apropiada.
   a. Inicie una sesión en la interfaz gráfica de usuario.
   b. En la página de Bienvenida, pulse **Administración** > **Exportar e importar** > **Importar claves**.
2. Importe una clave desde un archivo de almacén de claves. Puede importar una clave cada vez.
   a. Seleccione el tipo de clave.
   b. Pulse **Examinar** para seleccionar el archivo de almacén de claves que se va a importar.
   c. Para el tipo de clave simétrica: Seleccione el certificado que se utilizará para descifrar las claves en el archivo de almacén de claves. Asegúrese de que sea el mismo certificado que se utilizó cuando exportó la clave.
   d. Para claves privadas: Especifique la contraseña que se utilizará para descifrar las claves en el archivo de almacén de claves. Asegúrese de que sea la misma contraseña que se utilizó cuando exportó las claves.
   e. Especifique el alias de clave para la clave que se va a importar.
   f. Opcional: Para renombrar el alias de la clave que se importa, especifique un nuevo nombre de alias. Puede renombrar el alias si el alias de clave actual ya está siendo utilizado o si desea cambiarlo.
   g. Seleccione el grupo de dispositivos en el que se utilizará la clave importada.
   h. Pulse en **Importar**.
3. Para importar múltiples claves, repita el Paso 2 para cada clave.

Tareas relacionadas:

"Importación de una clave utilizando la interfaz gráfica de usuario"
Puede importar claves privadas y simétricas a un servidor de IBM Security Key Lifecycle Manager para habilitar la transferencia de datos entre este servidor y el servidor desde el cual se han exportado las claves. Las claves que se van a importar deben estar almacenadas en un archivo de almacén de claves cifrado.

Referencia relacionada:

Servicio REST Importar clave
Utilice el **Servicio REST Importar clave** para importar claves secretas o pares de claves públicas/privadas. Una clave secreta es una clave simétrica. Un par de claves públicas/privadas es un par de claves asimétricas que contienen una clave pública y una clave privada. El archivo de clave privada está en formato PKCS#12.

Formatos de indicación de fecha y hora

IBM Security Key Lifecycle Manager da soporte a la sintaxis de tiempo UTC (Universal Time).

A continuación se muestran ejemplos de la indicación de fecha y hora IST (hora estándar de la India) en formato UTC (GMT + 5:30).

Base de datos de IBM Security Key Lifecycle Manager
Las indicaciones de fecha y hora se almacenan en la base de datos de IBM Security Key Lifecycle Manager en formato UTC.

```
2018-03-22 05:52:07.0
```

Interfaz de usuario
Los valores de las indicaciones de fecha y hora se visualizan en la interfaz de usuario de IBM Security Key Lifecycle Manager utilizando el huso horario del navegador.

```
Last backup:Mar 22 2018, 05:51:24 AM IST (GMT+05:30)
```

Archivos de registro
Los valores de las indicaciones de fecha y hora en todos los archivos de registro se visualizan utilizando el huso horario del servidor con un desplazamiento de UTC. En el siguiente ejemplo, la indicación de fecha y hora para el huso horario IST.

```
Mar 22, 2018 11:31:40 AM +0500
```

Aceptación de dispositivos pendientes

Utilice la función de dispositivos pendientes para aceptar o rechazar un dispositivo que se pone en contacto con IBM Security Key Lifecycle Manager.

Acerca de esta tarea

Puede utilizar la página Solicitudes de dispositivo pendientes o puede utilizar varios mandatos para aceptar o rechazar un dispositivo que se pone en contacto con IBM Security Key Lifecycle Manager. Si el dispositivo pertenece a la DS5000 device family y la afinidad de la máquina está habilitada, también puede aceptar o rechazar la relación entre un dispositivo y una máquina. Si utiliza la afinidad de la máquina, puede restringir el servicio de claves a combinaciones específicas de dispositivos y máquinas.

Procedimiento

1. Las claves se generan automáticamente para un dispositivo en un DS5000 device group cuando llega una solicitud pendiente. Lleve a cabo una copia de seguridad antes de aceptar el dispositivo para garantizar que se realiza una copia de seguridad de las claves antes de servirse a un dispositivo. Para obtener más información, consulte los archivos de restauración y copia de seguridad de administración.
2. Vaya al directorio o la página apropiada.

- Interfaz gráfica de usuario:

  Inicie una sesión en la interfaz gráfica de usuario. En el árbol de navegación, pulse **IBM Security Key Lifecycle Manager**.
- Command-line interface
  a. Go to the <*WAS_HOME*>/bin directory. For example,

     Windows
     ```
     cd drive:\Program Files\IBM\WebSphere\AppServer\bin
     ```

     Linux
     ```
     cd /opt/IBM/WebSphere/AppServer/bin
     ```
  b. Start the **wsadmin** interface by using an authorized user ID, such as SKLMAdmin. For example,

     Windows
     ```
     wsadmin.bat -username SKLMAdmin -password mypwd -lang jython
     ```

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

3. Si no ha determinado previamente cómo aceptar los dispositivos pendientes, establezca el atributo **device.AutoPendingAutoDiscovery** en un valor que añada los dispositivos entrantes a la lista de dispositivos pendientes.

   Especifique un valor como, por ejemplo, 2 (pendientes automáticamente). All incoming devices are added to a pending list, but are not automatically served keys upon request. You must accept or reject a device in the pending devices list before the device is served keys upon request. Do not use a setting of 1 (auto accept) for the DS5000 device family. This setting allows generation and serving of keys to DS5000 storage servers before you backup data.
   - Interfaz gráfica de usuario:
     a. Navegue a la página Gestión de claves y dispositivos para el grupo de dispositivos de los dispositivos pendientes.
     b. En la lista desplegable de la parte inferior de la página, seleccione **Retener las solicitudes de dispositivos nuevos pendientes de aprobación**.
   - Interfaz de línea de mandatos:

     Por ejemplo, para un dispositivo DS5000, escriba:
     ```
     print AdminTask.tklmDeviceGroupAttributeUpdate ('[-name DS5000
       -attributes "{device.AutoPendingAutoDiscovery 2}"]')
     ```
4. Liste los dispositivos pendientes.
   - Interfaz gráfica de usuario:

     Vaya a la página de Bienvenida. En el área Elementos de acción, pulse el enlace de dispositivos pendientes.
   - Interfaz de línea de mandatos:

     Escriba:
     ```
     print AdminTask.tklmPendingDeviceList ('[-usage DS5000]')
     ```
5. Apruebe o rechace una solicitud de dispositivo pendiente.
   - Interfaz gráfica de usuario:

     En la tabla Solicitudes de dispositivo pendientes, seleccione un dispositivo pendiente y pulse **Aceptar** o **Rechazar**.

     Una solicitud pendiente aparece en la lista sólo una vez para un dispositivo DS5000 que también tenga una relación máquina-dispositivo. La solicitud aparece con la tabla con un valor para el ID de máquina. Si se acepta la solicitud de dispositivo pendiente, también se acepta la relación máquina-dispositivo.

En el diálogo Aceptar solicitud de dispositivo, pulse **Aceptar** o **Modificar y Aceptar**. Si elige modificar la información del dispositivo pendiente, realice los cambios necesarios y pulse **Aceptar**.

- Interfaz de línea de mandatos:
  - Puede utilizar un mandato para aceptar un dispositivo DS5000 pendiente y también la relación máquina-dispositivo pendiente. Por ejemplo, escriba:

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

  - De lo contrario, puede aceptar primero un dispositivo pendiente y asignarlo al grupo de dispositivos correspondiente. Por ejemplo, para aceptar un dispositivo DS5000 pendiente y aceptar posteriormente la relación máquina-dispositivo, siga estos pasos:
    a. Primero, escriba:

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

    b. Posteriormente, acepte o rechace las relaciones pendientes entre un dispositivo y una máquina.
       1) Liste todos los dispositivos pendientes que tengan una relación con un ID de máquina, o todos los dispositivos si no se especifica ningún ID de máquina. Por ejemplo, escriba:

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

       2) Acepte o rechace un dispositivo pendiente y la relación de máquina. Si acepta, se graban los datos de la relación en el almacén de datos de IBM Security Key Lifecycle Manager.

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

Qué hacer a continuación

Examine la lista de dispositivos aceptados. Utilice estos mandatos:

- **tklmDeviceList** para listar información sobre todos los dispositivos de un determinado tipo.
- **tklmMachineDeviceList** para listar todos los dispositivos que estén asociados con un ID de máquina específico, o todos los dispositivos si no se especifica ningún ID de máquina.

Movimiento de dispositivos entre grupos de dispositivos

Utilice la función de actualización de dispositivos para mover el dispositivo de un grupo de dispositivos existente a otro grupo de dispositivos existente. Por ejemplo, puede mover un dispositivo al grupo de dispositivos `MYDS5000`.

Acerca de esta tarea

Puede utilizar la página Modificar dispositivo, el mandato **`tklmDeviceUpdate`** o el **`Servicio REST Actualizar dispositivo`** para mover un dispositivo que contacte IBM Security Key Lifecycle Manager de un grupo de dispositivos a otro en la misma familia de dispositivos. Por ejemplo, puede mover un dispositivo al grupo de dispositivos `MYDS5000` dentro de la DS5000 device family.

Para obtener más información sobre cómo crear un grupo de dispositivos, consulte "Creación de un grupo de dispositivos" en la página 32.

Procedimiento

1. Navegue a la página o el directorio correspondiente:
   - Interfaz gráfica de usuario:
     a. Inicie una sesión en la interfaz gráfica de usuario.
     b. En la sección clave y dispositivo sección Gestión de claves y dispositivos en la página de bienvenida, seleccione **DS5000**.
     c. Pulse con el botón derecho del ratón **DS5000**.
     d. Pulse **Gestionar claves y dispositivos**.
   - Command-line interface
     a. Go to the *<WAS_HOME>*/bin directory. For example,

        Windows

        ```
        cd drive:\Program Files\IBM\WebSphere\AppServer\bin
        ```

        Linux

        ```
        cd /opt/IBM/WebSphere/AppServer/bin
        ```

     b. Start the **wsadmin** interface by using an authorized user ID, such as SKLMAdmin. For example,

        Windows

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

        Linux

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

   - Interfaz REST:
     – Abra un cliente REST.
2. Ubique el dispositivo que desea mover a otro grupo de dispositivos en una familia de dispositivos padre.
   - Interfaz gráfica de usuario:

     En la página Gestión de claves y dispositivos DS5000, ubique el dispositivo en la tabla de dispositivos. Por ejemplo, el dispositivo puede tener un número de serie como, por ejemplo, aaa123.
   - Interfaz de línea de mandatos:

     Escriba el mandato siguiente:

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

     En el indicador de mandatos, ubique el valor del uuid del dispositivo. Por ejemplo:

     ```
     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
     ```

   - Interfaz REST:
     a. Obtenga un identificador de autenticación de usuario exclusivo para acceder a los servicios REST de IBM Security Key Lifecycle Manager. Para obtener más información sobre el proceso de autenticación, consulte Proceso de autenticación de los servicios REST.

b. Para invocar el **Servicio REST Tipo de lista de dispositivos**, envíe la solicitud HTTP GET. Pase el identificador de autenticación de usuario que ha obtenido en el Paso a junto con el mensaje de solicitud, como se muestra en el ejemplo siguiente.

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

En la respuesta correcta, localice el valor del uuid de dispositivo. Por ejemplo:

```
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. Asegúrese de que el grupo de dispositivos de destino exista.
   - Interfaz gráfica de usuario:

     En la página Gestión de claves y dispositivos DS5000, en la tabla de dispositivos, seleccione el dispositivo y pulse **Modificar > Dispositivo**.

     En la página Modificar dispositivo, en el campo **Grupo de dispositivos asignado actualmente**, expanda la lista para determinar si el grupo de dispositivos **MYDS5000** está disponible.
   - Interfaz de línea de mandatos:

     Escriba el mandato siguiente:

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

     Ubique el grupo de dispositivos. Por ejemplo:

     ```
     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
     ```
   - Interfaz REST:

     Envíe la siguiente solicitud HTTP:

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

     Ubique el grupo de dispositivos. Por ejemplo:

     ```
     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. Actualice el dispositivo para especificar el nuevo grupo de dispositivos.
   - Interfaz gráfica de usuario:

     En la página Modificar dispositivo, en el campo **Grupo de dispositivos asignado actualmente**, seleccione el grupo de dispositivos **MYDS5000**.

     Pulse **Modificar dispositivo**.
   - Interfaz de línea de mandatos:

     Escriba el mandato siguiente:

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

     Envíe la siguiente solicitud HTTP:

     ```
     PUT https://localhost:<puerto>/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. Compruebe que el dispositivo esté en el nuevo grupo de dispositivos.
   - Interfaz gráfica de usuario:

     En la página Gestión de claves y dispositivos DS5000, el dispositivo ya no aparece en la tabla de dispositivos. Abra la página Gestión de claves y dispositivos MYDS5000 y compruebe que el dispositivo se enumera en la tabla de dispositivos.
   - Interfaz de línea de mandatos:

     Escriba el mandato siguiente:

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

     Por ejemplo, la salida contiene el valor de uuid del dispositivo y el nombre del nuevo grupo de dispositivos:

     ```
     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
     ```
   - Interfaz REST:

     Envíe la siguiente solicitud HTTP:

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

La respuesta satisfactoria contiene el valor de uuid del dispositivo y el nombre del nuevo grupo de dispositivos como se muestra en el ejemplo siguiente:

```
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"
},
]
```

Exportación de un certificado del servidor SSL/KMIP

Debe exportar el certificado del servidor SSL/KMIP IBM Security Key Lifecycle Manager en un archivo en un formato codificado para que el dispositivo de cliente lo pueda utilizar. El dispositivo de cliente importa este certificado para una comunicación segura con el servidor.

Acerca de esta tarea

Utilice el diálogo Exportar certificado, el mandato **tklmCertExport** o el **Servicio REST Exportar certificado** para exportar el certificador del servidor SSL/KMIP de IBM Security Key Lifecycle Manager en un archivo con formato codificado.

Procedimiento

1. Vaya al directorio o la página apropiada.
   - Interfaz gráfica de usuario:

     Inicie una sesión en la interfaz gráfica de usuario. Se muestra la página de Bienvenida.
   - Command-line interface
     a. Go to the <*WAS_HOME*>/bin directory. For example,

        Windows
        ```
        cd drive:\Program Files\IBM\WebSphere\AppServer\bin
        ```

        Linux
        ```
        cd /opt/IBM/WebSphere/AppServer/bin
        ```

     b. Start the **wsadmin** interface by using an authorized user ID, such as SKLMAdmin. For example,

        Windows
        ```
        wsadmin.bat -username SKLMAdmin -password mypwd -lang jython
        ```

        Linux
        ```
        ./wsadmin.sh -username SKLMAdmin -password mypwd -lang jython
        ```
   - Interfaz REST:
     – Abra un cliente REST.
2. Exporte un certificado.
   - Interfaz gráfica de usuario:
     a. Pulse **Configuración avanzada** > **Certificados del servidor**.
     b. En la tabla **Certificados**, seleccione el certificado adecuado.
     c. Pulse **Exportar**.

d. En el diálogo Exportar certificado, compruebe que el certificado que ha seleccionado en el `Paso b` se ha rellenado para el campo **Nombre de archivo**.

e. El campo **Ubicación de archivo** muestra la vía de acceso del directorio <*SKLM_DATA*> predeterminada, donde se exportará el certificado, por ejemplo, `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data`. Para ver la definición de <*SKLM_DATA*>, consulte Definiciones para *HOME* y otras variables de directorio. Pulse **Examinar** para especificar una ubicación bajo el directorio <SKLM_DATA>.

f. Seleccione el formato de archivo codificado **BASE64** (formato predeterminado) o **DER** (Distinguished Encoding Rules) para el certificado.

g. Pulse **Exportar certificado**.

- Interfaz de línea de mandatos:

  Escriba `tklmCertExport` para exportar un archivo de certificado. Por ejemplo:

  ```
  print AdminTask.tklmCertExport
   ('[-uuid CERTIFICATE-61f8e7ca-62aa-47d5-a915–8adbfbdca9de
    -format DER -fileName d:\\mypath\\mycertfilename.der]')
  ```

  Para obtener más información sobre el mandato **tklmCertExport**, consulte tklmCertExport.

- Interfaz REST:

  a. Obtenga un identificador de autenticación de usuario exclusivo para acceder a los servicios REST de IBM Security Key Lifecycle Manager. Para obtener más información sobre el proceso de autenticación, consulte Proceso de autenticación de los servicios REST.

  b. Para iniciar el **Servicio REST Exportar certificado**, envíe la solicitud HTTP PUT. Pase el identificador de autenticación de usuario que ha obtenido en el `Paso a` junto con el mensaje de solicitud, como se muestra en el ejemplo siguiente.

  ```
  PUT https://localhost:<puerto>/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"}
  ```

  Para obtener más información sobre el **Servicio REST Exportar certificado**, consulte Servicio REST Exportar certificado.

Cómo copiar un certificado entre los servidores IBM Security Key Lifecycle Manager

Puede utilizar la interfaz de línea de mandatos o la interfaz REST para copiar un certificado entre servidores IBM Security Key Lifecycle Manager con la clave pública y privada.

Acerca de esta tarea

Utilice los siguientes mandatos CLI o interfaces REST para copiar un certificado:

- **tklmKeyExport** y **tklmKeyImport**
- **Servicio REST Exportar clave** y **Servicio REST Importar clave**

Procedimiento

1. En el servidor IBM Security Key Lifecycle Manager donde se encuentra el certificado, ejecute el mandato **tklmKeyExport** o envíe la solicitud HTTP **Servicio REST Exportar clave**.

```
print AdminTask.tklmKeyExport ('[-alias sklmCertificate
   -fileName myprivatekeys -keyStoreName defaultKeyStore
    -type privatekey -password mypassword]')
```

```
PUT https://localhost:<puerto>/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. Copie el archivo mycert.p12 en el servidor IBM Security Key Lifecycle Manager de destino.
3. Ejecute el mandato **tklmKeyImport** o envíe la solicitud HTTP **Servicio REST Importar clave**.

```
print AdminTask.tklmKeyImport ('-type privatekey -fileName c:\\mycert.p12
-keyStoreName "Tivoli Key Lifecycle Manager Keystore" -usage 3592 -password
<password>]')
```

```
POST https://localhost:<puerto>/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"}
```

Resultados

Estos mandatos copian la clave pública y privada de lectura y escritura para cintas mediante el certificado.

Cambio del idioma de la interfaz del navegador

Puede cambiar el idioma que se muestra en la interfaz del navegador.

Acerca de esta tarea

Cambie la preferencia de idioma del navegador antes de iniciar una sesión en IBM Security Key Lifecycle Manager. Para cambiar la preferencia de idioma del navegador, siga estos pasos:

- Internet Explorer
  1. Seleccione **Herramientas > Opciones de Internet**.
  2. En el separador **General**, pulse **Idiomas**.
  3. Seleccione un idioma y pulse **Aceptar**.Es posible que primero deba añadir un idioma y subirlo al principio de la lista de idiomas.
  4. Reinicie el navegador.
- Firefox
  1. Seleccione **Herramientas > Opciones**.A continuación, pulse el icono Contenido.
  2. En el separador Contenido, en la sección Idiomas, pulse **Seleccionar**.
  3. Seleccione un idioma y pulse **Aceptar**.Es posible que primero deba añadir un idioma y subirlo al principio de la lista de idiomas.
  4. En el diálogo Opciones, pulse **Aceptar** otra vez.

5. Reinicie el navegador.

Avisos

Esta información se ha desarrollado para productos y servicios que se ofrecen en EE.UU. Puede que IBM no ofrezca en algunos países los productos, servicios o características que se explican en este documento. Póngase en contacto con el representante local de IBM para obtener información sobre los productos y servicios disponibles actualmente en su área. Las referencias a programas, productos o servicios de IBM no pretenden establecer ni implicar que sólo puedan utilizarse dichos productos, programas o servicios de IBM. En su lugar, se puede utilizar cualquier producto, programa o servicio funcionalmente equivalente que no infrinja ninguno de los derechos de propiedad intelectual de IBM. Sin embargo, es responsabilidad del cliente evaluar y verificar el funcionamiento de cualquier producto, programa o servicio que no sea de IBM.

IBM puede tener patentes o solicitudes de patentes pendientes que cubran el tema principal descrito en este documento. La posesión de este documento no confiere ninguna licencia sobre dichas patentes. Puede enviar consultas sobre licencias, por escrito, a:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
EE.UU.

Para formular consultas relacionadas con el juego de caracteres de doble byte (DBCS), póngase en contacto con el departamento de la propiedad intelectual de IBM de su país o envíe las consultas, por escrito, a la siguiente dirección:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japón

El párrafo siguiente no se aplica al Reino Unido ni a ningún otro país donde estas disposiciones sean incompatibles con la legislación vigente:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL" SIN GARANTÍAS DE NINGÚN TIPO NI EXPLÍCITAS NI IMPLÍCITAS, INCLUYENDO PERO NO LIMITÁNDOSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE NO VULNERACIÓN, COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO.

Algunas jurisdicciones no permiten la renuncia a las garantías explícitas o implícitas en determinadas transacciones; por lo tanto, es posible que esta declaración no sea aplicable en su caso.

Esta información puede incluir imprecisiones técnicas o errores tipográficos. Periódicamente se efectúan cambios en la información aquí contenida; estos cambios se incorporarán en nuevas ediciones de la publicación. IBM puede realizar en cualquier momento mejoras o cambios en los productos o programas descritos en esta publicación sin previo aviso.

Cualquier referencia incluida en esta información a sitios web que no sean de IBM sólo se proporciona para su comodidad y en ningún modo constituye una aprobación de dichos sitios web. Los materiales de dichos sitios web no forman parte de los materiales para este producto de IBM y el uso de dichos sitios web corre a cuenta y riesgo del Cliente.

IBM puede utilizar o distribuir cualquier información que se le proporcione en la forma que considere adecuada, sin incurrir por ello en ninguna obligación para con el remitente.

Los titulares de licencias de este programa que deseen obtener información sobre el mismo con el fin de permitir: (i) el intercambio de información entre programas creados independientemente y otros programas (incluido éste) y el uso mutuo de información que se haya intercambiado, deben ponerse en contacto con:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
EE.UU.

Dicha información puede estar disponible, sujeta a los términos y condiciones correspondientes, incluido en algunos casos el pago de una cuota.

El programa bajo licencia descrito en este documento y todos los materiales bajo licencia disponibles para el mismo los proporciona IBM bajo los términos del Acuerdo del Cliente de IBM y el Acuerdo Internacional de Programas Bajo Licencia de IBM.

Cualquier dato de rendimiento contenido en este documento se ha determinado en un entorno controlado. Por lo tanto, el resultado obtenido en otros entornos operativos puede variar significativamente. Es posible que algunas medidas se hayan tomado en sistemas de nivel de desarrollo y no hay ninguna garantía de que estas medidas sean las mismas en sistemas con mucha implantación. Además, algunas medidas se pueden haber estimado mediante extrapolación. Los resultados reales pueden variar. Los usuarios de este documento deben verificar los datos aplicables para su propio entorno.

La información relacionada con productos que no son de IBM se ha obtenido de los proveedores de dichos productos, de sus anuncios publicados o de otras fuentes de disponibilidad pública. IBM no ha comprobado estos productos y no puede confirmar la precisión de su rendimiento, compatibilidad ni contemplar ninguna otra reclamación relacionada con los productos que no son de IBM. Las preguntas relacionadas con las funciones de los productos que no son de IBM deberán dirigirse a los proveedores de estos productos.

Todas las declaraciones relacionadas con la dirección o intenciones futuras de IBM están sujetas a cambio o cancelación sin previo aviso, y únicamente representan objetivos.

Todos los precios de IBM que se muestran son precios de distribuidor recomendados por IBM, corresponden al momento actual y están sujetos a cambios sin aviso previo. Los precios de los distribuidores pueden variar.

Esta información se suministra meramente con fines de planificación. La información incluida en este documento puede cambiar antes de que los productos descritos estén disponibles.

Esta información contiene ejemplos de datos e informes que se utilizan en operaciones empresariales diarias. Para ilustrarlos de la forma más completa posible, los ejemplos incluyen nombres de particulares, empresas, marcas y productos. Todos estos nombres son ficticios y cualquier similitud con nombres y direcciones utilizados por una empresa real es mera coincidencia.

LICENCIA DE COPYRIGHT:

Esta información contiene programas de aplicación de ejemplo en lenguaje fuente que ilustran técnicas de programación en varias plataformas operativas. Puede copiar, modificar y distribuir dichos programas de ejemplo bajo cualquier forma y sin tener que pagar a IBM, con el objeto de desarrollar, utilizar, comercializar o distribuir programas de aplicación adaptados a la interfaz de programación de aplicaciones de la plataforma operativa para la que se han escrito los programas. Estos ejemplos no se han probado exhaustivamente bajo todas las condiciones. Por lo tanto, IBM no puede garantizar ni implicar la fiabilidad, capacidad de servicio o función de estos programas. Los programas de ejemplo se proporcionan "TAL CUAL", sin garantía de ningún tipo. IBM no se responsabiliza de ningún daño resultante de la utilización de los programas de ejemplo.

Cada copia o parte de estos programas de ejemplo, o todo trabajo derivado, debe incluir un aviso de copyright como este:

© (nombre de la empresa) (año). Las partes de este código se derivan de programas de ejemplo de IBM Corp. © Copyright IBM Corp. _escriba el año o años_.

Si está viendo esta información en copia software, es posible que no se visualicen las fotografías ni las ilustraciones de color.

Términos y condiciones para la documentación del producto

Los permisos para utilizar estas publicaciones se otorgan de acuerdo con los siguientes términos y condiciones.

Aplicabilidad

Estos términos y condiciones son adicionales a cualquier otro término de utilización del sitio web de IBM.

Uso personal

Estas publicaciones se pueden reproducir de acuerdo con un uso personal y no comercial siempre que se conserven todos los avisos de propiedad. No se permite distribuir, visualizar u obtener trabajos derivados de estas publicaciones o de cualquier parte de las mismas sin el consentimiento expreso de IBM.

Uso comercial

El usuario puede reproducir, distribuir y visualizar estas publicaciones únicamente dentro de su empresa siempre que se conserven todos los avisos de propiedad. No se permite obtener trabajos derivados de estas publicaciones, o reproducir, distribuir o visualizar estas publicaciones o de cualquier parte de las mismas fuera de su empresa sin el consentimiento expreso de IBM.

Derechos

Con la excepción de lo otorgado de forma expresa en este permiso, no se otorga ningún otro permiso, licencia o derecho, ya sea de forma explícita o implícita, para las publicaciones o para cualquier otra información, datos, software o propiedad intelectual que aquí se contienen.

IBM se reserva el derecho de retirar los permisos que aquí se otorgan siempre, que a su discreción, la utilización de las publicaciones sea perjudicial para sus intereses, o tal como IBM determine, si las anteriores instrucciones no se están siguiendo de forma adecuada.

No se puede descargar, exportar o volver a exportar esta información excepto cuando sea bajo un cumplimento estricto de todas las normas y leyes aplicables, incluidas todas las normas y leyes de exportación de los Estados Unidos.

IBM NO PROPORCIONA NINGUNA GARANTÍA SOBRE EL CONTENIDO DE ESTAS PUBLICACIONES. LAS PUBLICACIONES SE PROPORCIONAN "TAL CUAL" SIN NINGUNA GARANTÍA DE NINGÚN TIPO, EXPLÍCITA O IMPLÍCITA, INCLUYENDO, PERO SIN LIMITARSE A ELLAS, A LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN, DE NO VULNERACIÓN Y DE IDONEIDAD PARA UN FIN CONCRETO.

Marcas registradas

IBM, el logotipo de IBM e ibm.com son marcas registradas de International Business Machines Corp., registradas en muchas jurisdicciones en todo el mundo. Otros nombres de producto y servicio pueden ser marcas registradas de IBM o de otras empresas. Encontrará una lista de las marcas registradas disponibles de IBM en la página web http://www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, PostScript y todas las marcas registradas basadas en Adobe son marcas registradas de Adobe Systems Incorporated en Estados Unidos o en otros países.

IT Infrastructure Library es una marca registrada de la Central Computer and Telecommunications Agency, que ahora forma parte de la Office of Government Commerce.

Intel, el logotipo de Intel, Intel Inside, el logotipo de Intel Inside, Intel Centrino, el logotipo de Intel Centrino, Celeron, Intel Xeon, Intel SpeedStep, Itanium y Pentium son marcas registradas de Intel Corporation o sus subsidiarias en Estados Unidos y en otros países.

Linux es una marca registrada de Linus Torvalds en Estados Unidos o en otros países.

Microsoft, Windows, Windows NT y el logotipo de Windows son marcas registradas de Microsoft Corporation en Estados Unidos o en otros países.

ITIL es una marca registrada y una marca registrada comunitaria de la Office of Government Commerce, y está registrada en la Oficina de patentes y marcas de Estados Unidos.

UNIX es una marca registrada de The Open Group en Estados Unidos o en otros países.

Java y todas las marcas registradas y logotipos basados en Java son marcas registradas de Oracle y/o sus afiliados.

Cell Broadband Engine es una marca registrada de Sony Computer Entertainment, Inc., en Estados Unidos o en otros países, y se utiliza bajo su licencia.

Linear Tape-Open, LTO, el logotipo de LTO, Ultrium y el logotipo de Ultrium son marcas registradas de HP, IBM Corp. y Quantum en Estados Unidos y en otros países.

Índice

Caracteres Especiales

Números

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W