Administration

Table des matières

Administration

L'administration représente l'ensemble des tâches via lesquelles vous préparez, puis surveillez l'environnement IBM Security Key Lifecycle Manager.

Les activités administratives comprennent les tâches suivantes :

- Configuration et maintenance du système IBM Security Key Lifecycle Manager
- Configuration du système principal et des clones pour la réplication
- Administration des groupes, des utilisateurs et des rôles
- Administration des unités, des objets KMIP et du module de sécurité matérielle
- Exécution de tâches opérationnelles telles que la sauvegarde de données, la restauration de données et l'exportation/importation de groupes d'unités
- Autres tâches administratives diverses

Avant de commencer, familiarisez-vous avec les concepts et la terminologie qui sont mentionnés dans cette section. Reportez-vous aux sections Présentation, Planification et Installation et configuration pour des informations associées.

Spécification de certificats SSL ou KMIP

Vous pouvez spécifier le certificat autosigné à utiliser comme certificat de communication serveur. Vous pouvez également créer des demandes de certificats et les envoyer manuellement à une autorité de certification pour approbation. Par exemple, vous pouvez utiliser des certificats pour protéger la communication entre IBM Security Key Lifecycle Manager et une bandothèque. Les fichiers générés sont stockés dans le répertoire <*SKLM_INSTALL_HOME*>. Par exemple, un certificat généré peut être un fichier tel que `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\171029122037-sslcert001.csr`.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser la page SSL/KMIP pour le service de clés pour spécifier le type de certificat utilisé par IBM Security Key Lifecycle Manager. Vous pouvez également utiliser l'une des commandes CLI ou interfaces REST suivantes :

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

Votre rôle doit avoir le droit d'utiliser l'action de configuration afin que vous puissiez créer un certificat SSL ou KMIP.

Avant de commencer, déterminez les points suivants :

- Si vous pouvez utiliser des certificats autosignés lors d'une phase de votre projet, la phase de test par exemple.
- L'intervalle de temps nécessaire pour la réception d'un certificat délivré par une autorité de certification après l'envoi d'une demande. Vous devez envoyer manuellement une demande de certificat à l'autorité concernée.
- Si votre site requiert des certificats partenaires à utiliser avec les partenaires commerciaux, les fournisseurs ou pour la reprise après incident.
- La configuration habituelle en jours pour l'intervalle de validité de certificat.

Procédure

1. Accédez à la page ou au répertoire approprié.
   - Interface graphique :

     Connectez-vous à l'interface graphique. Cliquez sur **IBM Security Key Lifecycle Manager** > **Configuration** > **SSL/KMIP**.
   - Interface de ligne de commande
     a. Accédez au répertoire <*WAS_HOME*>/bin. Exemple :

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

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

     b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme SKLMAdmin. Exemple :

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

        Linux
        ```
        ./wsadmin.sh -username SKLMAdmin
        -password mypwd -lang jython
        ```
   - Interface REST :
     – Ouvrez un client REST.
2. Créez un ou plusieurs certificats ou demandes de certificat :
   - Interface graphique

     Permet de générer un certificat autosigné ou d'effectuer une demande de certificat auprès d'un fournisseur tiers. Une option est également disponible, qui permet au certificat de s'appuyer sur un certificat existant du magasin de clés. Renseignez les zones requises et facultatives, puis cliquez sur **OK**.
   - Interface de ligne de commande

     Entrez la commande **tklmCertCreate** sur une seule ligne. Par exemple, pour créer un certificat autosigné, entrez :
     ```
     print AdminTask.tklmCertCreate ('[-type selfsigned
      -alias sklmSSLCertificate -cn sklmssl -ou accounting -o myCompanyName
        -country US -keyStoreName defaultKeyStore
         -usage SSLSERVER -validity 999]')
     ```

     Vous pouvez également effectuer une demande de certificat auprès d'une autorité de certification. Par exemple, entrez :
     ```
     print AdminTask.tklmCertGenRequest('[-alias sklmSSLCertificate1
      -cn sklm -ou sales -o myCompanyName -locality myLocation
       -country US -validity 999 -keyStoreName defaultKeyStore
        -fileName mySSLCertRequest1.crt -usage SSLSERVER]')
     ```
   - Interface REST
     a. Obtenez un identificateur d'authentification utilisateur unique pour accéder aux services REST d'IBM Security Key Lifecycle Manager. Pour plus d'informations sur le processus d'authentification, voir Processus d'authentification pour les services REST.
     b. Pour exécuter le **service REST Certificate Generate Request**, envoyez la demande HTTP POST. Transmettez l'identificateur d'authentification utilisateur que vous avez obtenu à l'étape a avec le message de demande, conformément à l'exemple suivant :
        ```
        POST https://localhost:<port>/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 "  }
```

Envoyez la demande HTTP suivante pour obtenir un certificat auprès d'une autorité de certification :

```
POST https://localhost:<port>/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 vous sélectionnez une demande de certificat pour un fournisseur tiers, le fichier de demande de certificat au format `.csr` est généré dans le répertoire `<SKLM_HOME>`, par exemple `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\171029122037-sslcert001.csr`. Envoyez manuellement la demande de certificat à une autorité de certification. Ensuite, importez le certificat signé dans IBM Security Key Lifecycle Manager. Pour la procédure à suivre pour envoyer et importer le certificat, voir Scénario : Demande d'un certificat de fournisseur tiers.

3. L'indicateur de réussite varie en fonction de l'interface.
   - Interface graphique

     Sur la page Opération achevée avec succès, sous Etapes suivantes, cliquez sur une tâche associée à effectuer. Si vous créez un certificat autosigné, il est prudent de redémarrer le serveur et de créer une copie de sauvegarde afin de pouvoir restaurer ces données en cas de besoin.
   - Interface de ligne de commande

     Un message d'achèvement indique la réussite de l'opération.
   - Interface REST

     Le code de statut `200 OK` indique la réussite de l'opération.

Que faire ensuite

Accédez à la page Bienvenue et configurez les types d'unité, ainsi que les clés ou certificats requis par votre organisation.

Définition des niveaux d'informations d'audit

Vous serez peut-être amené à modifier le paramètre par défaut utilisé par IBM Security Key Lifecycle Manager pour collecter des informations d'audit.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser la page Audit pour modifier les niveaux d'informations d'audit (Faible, Moyen ou Elevé) inscrits dans le journal d'audit. Vous pouvez également utiliser les commandes CLI ou les interfaces REST suivantes pour répertorier ou modifier la propriété **Audit.event.types** dans le fichier `SKLMConfig.properties` :

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

Votre rôle doit avoir un droit d'utilisation de l'action de configuration.

Procédure

1. Accédez à la page ou au répertoire approprié(e) :
   - Interface graphique :

     Connectez-vous à l'interface graphique. Cliquez sur **IBM Security Key Lifecycle Manager** > **Configuration** > **Audit et débogage**.
   - Interface de ligne de commande
     a. Accédez au répertoire <*WAS_HOME*>/bin. Exemple :

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

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

     b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme SKLMAdmin. Exemple :

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

        Linux
        ```
        ./wsadmin.sh -username SKLMAdmin
        -password mypwd -lang jython
        ```
   - Interface REST :
     – Ouvrez un client REST.
2. Modifiez la valeur du niveau d'informations d'audit :
   - Dans l'interface graphique, sélectionnez un niveau faible, moyen ou élevé pour le paramètre Audit, puis cliquez sur **OK**.

     Faible Stocke un volume minimal d'enregistrements d'audit.

     La sélection du niveau **Faible** définit les valeurs de propriété suivantes dans le fichier SKLMConfig.properties :
     – `Audit.event.types = runtime, authorization, authorization_terminate, resource_management, key_management`
     – `Audit.event.outcome = failure`

     Moyen (valeur par défaut)
     Stocke un nombre intermédiaire d'enregistrements d'audit.

     La sélection du niveau **Moyen** définit les valeurs de propriété suivantes dans le fichier SKLMConfig.properties :
     – `Audit.event.types = runtime,authorization, authorization_terminate,resource_management,key_management`
     – `Audit.event.outcome = success,failure`

     Elevé Stocke le nombre maximal d'enregistrements d'audit.

     La sélection du niveau **Elevé** définit les valeurs de propriété suivantes dans le fichier SKLMConfig.properties :
     – `Audit.event.types = all`
     – `Audit.event.outcome = success,failure`
   - Interface de ligne de commande :
     a. Entrez la commande **tklmConfigGetEntry** sur une ligne pour obtenir la valeur en cours de la propriété cible dans le fichier SKLMConfig.properties. Par exemple, pour déterminer les types d'événements inclus dans le journal d'audit, entrez la commande suivante sur une seule ligne :

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

Voici un exemple de réponse :

```
All
```

b. Indiquez la modification demandée. Par exemple, pour limiter la sélection à deux types d'événements à stocker dans le journal d'audit, entrez la commande suivante sur une seule ligne :

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

- Interface REST :

a. Obtenez un identificateur d'authentification utilisateur unique pour accéder aux services REST d'IBM Security Key Lifecycle Manager. Pour plus d'informations sur le processus d'authentification, voir Processus d'authentification pour les services REST.

b. Pour exécuter le **service REST Get Single Config Property**, envoyez la demande HTTP GET. Transmettez l'identificateur d'authentification utilisateur que vous avez obtenu à l'étape a avec le message de demande, conformément à l'exemple suivant :

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

Le message indiquant que l'opération a abouti peut se présenter comme suit :

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

c. Indiquez la modification demandée. Par exemple, vous pouvez utiliser le **service REST Update Config Property** pour limiter la sélection à deux types d'événements à stocker dans le journal d'audit, en envoyant la demande HTTP suivante :

```
PUT https://localhost:<port>/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. Redémarrez le serveur. Pour des instructions sur la façon d'arrêter et de démarrer le serveur, voir «Serveur IBM Security Key Lifecycle Manager - Redémarrage», à la page 211.

Que faire ensuite

Vous pouvez réexécuter une opération ayant précédemment renvoyé une erreur. Examinez ensuite le journal d'audit pour obtenir davantage d'informations. Pour des informations détaillées sur les enregistrements d'audit, voir la rubrique «Enregistrements d'audit sur des systèmes répartis» dans la documentation d'IBM Security Key Lifecycle Manager.

Génération d'enregistrements d'audit au format syslog

Vous pouvez utiliser l'interface graphique d'IBM Security Key Lifecycle Manager pour configurer et générer les enregistrements d'audit au format syslog et les envoyer à un serveur syslog.

Pourquoi et quand exécuter cette tâche

Les messages de journal d'audit sont enregistrés dans un fichier d'audit local configuré au format syslog pour les raisons suivantes :

- Le format syslog est activé pour les messages d'audit.
- Le format syslog est activé et le nom d'hôte et le numéro de port de serveur syslog ne sont pas spécifiés.
- Le format syslog est activé, le nom d'hôte et le numéro de port de serveur syslog sont spécifiés, mais le nom d'hôte ou le numéro de port sont inaccessibles.

Procédure

1. Connectez-vous à l'interface graphique.
2. Cliquez sur **IBM Security Key Lifecycle Manager** > **Configuration** > **Audit et débogage**.
3. Sélectionnez **Utiliser le format syslog**.
4. Spécifiez le nom d'hôte ou l'adresse IP du serveur dans **Hôte de serveur syslog**.
5. Spécifiez le numéro de port sur lequel le serveur syslog écoute les demandes dans **Port de serveur syslog**.
6. Si vous avez besoin du transfert sécurisé des informations d'audit vers le serveur syslog à l'aide du protocole de transport SSL/TLS, sélectionnez **Utiliser SSL/TLS**.
7. Cliquez sur **OK**.

Que faire ensuite

Après avoir activé le format syslog pour les enregistrements d'audit à l'aide des paramètres requis, vous devez exécuter les étapes suivantes uniquement si vous sélectionnez **Utiliser SSL/TLS** :

1. Si le certificat de serveur SSL d'IBM Security Key Lifecycle Manager n'a pas encore été créé, créez-le. Pour créer le certificat, vous pouvez utiliser la page SSL/KMIP pour le service de clés sur l'interface graphique, le **service REST Create Certificate** ou la commande CLI **tklmCertCreate**.
2. Exportez le certificat de serveur SSL d'IBM Security Key Lifecycle Manager dans un fichier. Pour exporter le certificat, vous pouvez utiliser le **service REST Certificate Export** ou la commande CLI **tklmCertExport**.

   Pour exporter le certificat de serveur, procurez-vous l'alias du certificat de serveur à partir de l'étape 1 si le certificat n'a pas encore été créé. Si le certificat a déjà été créé, à partir de l'interface graphique, accédez à **Configuration avancée** > **Certificats de serveur**. L'alias correspond au certificat pour lequel la valeur `En cours d'utilisation` est spécifiée dans la colonne **Certificats**.
3. Procurez-vous le certificat de serveur syslog en tant que fichier, importez-le et marquez-le comme certificat de serveur syslog de confiance dans le serveur IBM Security Key Lifecycle Manager. Utilisez la commande CLI **tklmCertImport** ou le **service REST Certificate Import** pour importer le certificat à l'aide de `SYSLOG`.
4. Importez le certificat de serveur IBM Security Key Lifecycle Manager sur le serveur syslog. Utilisez le fichier de certificat qui a été créé à l'étape 2.
5. Définissez l'alias de certificat de serveur SSL d'IBM Security Key Lifecycle Manager dans le fichier de propriétés de configuration.

Remarque : Cette étape n'est pas obligatoire si le certificat de serveur SSL d'IBM Security Key Lifecycle Manager est créé à l'aide de l'interface graphique. Par exemple,

Interface de ligne de commande

```
 print AdminTask.tklmConfigUpdateEntry('[-name config.keystore.ssl.
certalias -value <alias du certificat de serveur qui a été
créé à l'étape 1>]')
```

Interface REST

```
PUT https://localhost:<port>/SKLM/rest/v1/configProperties
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth userAuthId=139aeh34567m
Accept-Language : en
{ "config.keystore.ssl.certalias" : "<alias du certificat de
serveur qui a été créé à l'étape 1>"}
```

6. Redémarrez le serveur. Pour des instructions sur la façon d'arrêter et de démarrer le serveur, voir «Serveur IBM Security Key Lifecycle Manager - Redémarrage», à la page 211.

Spécification des paramètres pour les informations de débogage

Vous pouvez changer le paramètre par défaut qu'IBM Security Key Lifecycle Manager utilise pour collecter les informations de débogage. Les fichiers du journal de débogage fournissent des informations supplémentaires permettant d'analyser et de traiter les problèmes liés à IBM Security Key Lifecycle Manager.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser la section Débogage de la page Audit pour spécifier les paramètres de génération des informations de débogage. Vous pouvez également utiliser les commandes de l'interface CLI ou les interfaces REST suivantes pour répertorier ou modifier la propriété **debug** dans le fichier `SKLMConfig.properties` :

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

Votre rôle doit avoir un droit d'utilisation de l'action de configuration.

Remarque : L'activation de la journalisation de débogage peut avoir un impact sur les performances d'IBM Security Key Lifecycle Manager. N'activez cette option que sous la direction de votre support IBM.

Procédure

1. Accédez à la page ou au répertoire approprié(e) :
   - Interface graphique :

     Connectez-vous à l'interface graphique. Cliquez sur **IBM Security Key Lifecycle Manager** > **Configuration** > **Audit et débogage**.
   - Interface de ligne de commande
     a. Accédez au répertoire <*WAS_HOME*>/bin. Exemple :

     Windows

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

     Linux

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

b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme SKLMAdmin. Exemple :

Windows

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

Linux

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

- Interface REST :
  - Ouvrez un client REST.

2. Modifiez les paramètres de génération des informations de débogage :
   - Dans l'interface graphique :
     a. Sélectionnez **Activer le débogage** pour définir les valeurs de propriété suivantes dans le fichier SKLMConfig.properties :

     ```
     debug=all
     ```

     b. Cliquez sur **OK**.
   - Interface de ligne de commande :
     a. Entrez la commande **tklmConfigGetEntry** sur une ligne pour obtenir la valeur en cours de la propriété cible dans le fichier SKLMConfig.properties. Par exemple, pour déterminer la valeur de debug, entrez sur une seule ligne :

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

     Voici un exemple de réponse :

     ```
     none
     ```

     b. Spécifiez une nouvelle valeur pour la propriété. Par exemple, pour spécifier la valeur all pour la génération des journaux de débogage, entrez sur une seule ligne :

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

   - Interface REST :
     a. Obtenez un identificateur d'authentification utilisateur unique pour accéder aux services REST d'IBM Security Key Lifecycle Manager. Pour plus d'informations sur le processus d'authentification, voir Processus d'authentification pour les services REST.
     b. Pour exécuter le **service REST Get Single Config Property**, envoyez la demande HTTP GET. Transmettez l'identificateur d'authentification utilisateur que vous avez obtenu à l'étape a avec le message de demande, conformément à l'exemple suivant :

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

     Le message indiquant que l'opération a abouti peut se présenter comme suit :

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

     c. Spécifiez une nouvelle valeur pour la propriété. Envoyez ensuite la demande HTTP suivante :

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

3. L'indicateur de réussite varie, selon l'interface :

Définition des paramètres de port et de délai d'attente

Vous pouvez modifier les paramètres de port et de délai d'attente par défaut fournis par IBM Security Key Lifecycle Manager.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser la page Ports de service de clés pour changer les valeurs de port et de délai d'attente. Vous pouvez également utiliser les commandes CLI ou les services REST suivants pour répertorier et modifier les propriétés appropriées dans le fichier `SKLMConfig.properties` :

- **`tklmConfigGetEntry`** et **`tklmConfigUpdateEntry`**
- **`Service REST Get Single Config Property`** et **`Service REST Update Config Property`**

Avant de commencer, déterminez s'il existe des conflits de ports ou de délais d'attente sur votre site, empêchant l'utilisation des valeurs par défaut d'IBM Security Key Lifecycle Manager. Votre rôle doit avoir un droit d'utilisation de l'action de configuration.

Procédure

1. Accédez à la page ou au répertoire approprié(e) :
   - Interface graphique :

     Connectez-vous à l'interface graphique. Cliquez sur **IBM Security Key Lifecycle Manager** > **Configuration** > **Ports de service de clés**.
   - Interface de ligne de commande
     a. Accédez au répertoire <*WAS_HOME*>/bin. Exemple :

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

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

     b. Démarrez l'interface **`wsadmin`** en utilisant un ID utilisateur autorisé, comme `SKLMAdmin`. Exemple :

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

        Linux
        ```
        ./wsadmin.sh -username SKLMAdmin
        -password mypwd -lang jython
        ```
   - Interface REST :
     – Ouvrez un client REST.
2. Modifiez la valeur des paramètres de port ou de délai d'attente :
   - Dans l'interface graphique, modifiez un ou plusieurs des paramètres suivants avant de cliquer sur **OK** :

Port TCP
Par défaut, IBM Security Key Lifecycle Manager utilise le port 3801. Les valeurs s'étendent de 1 à 65535. La valeur que vous définissez change aussi la valeur de la propriété **TransportListener.tcp.port** dans le fichier SKLMConfig.properties. Assurez-vous que le port choisi n'est pas déjà utilisé par une autre application.

Délai d'attente TCP (en minutes)
IBM Security Key Lifecycle Manager utilise une valeur de délai d'attente par défaut de 10 minutes. Les valeurs peuvent aller de 1 à 120. La valeur que vous définissez change aussi la valeur de la propriété **TransportListener.tcp.timeout** dans le fichier SKLMConfig.properties.

Port SSL
Par défaut, IBM Security Key Lifecycle Manager utilise le port 441. Les valeurs s'étendent de 1 à 65535. La valeur que vous définissez change aussi la valeur de la propriété **TransportListener.ssl.port** dans le fichier SKLMConfig.properties.

Délai d'attente SSL (en minutes)
IBM Security Key Lifecycle Manager utilise une valeur de délai d'attente par défaut de 10 minutes. Les valeurs peuvent aller de 1 à 120. Ce paramètre de configuration est associé à la valeur de la propriété **TransportListener.ssl.timeout** dans le fichier SKLMConfig.properties.

Port SSL KMIP
KMIP utilise le port par défaut 5696. Les valeurs admises vont de 1 à 65535. Ce paramètre de configuration est associé à la valeur de la propriété **KMIPListener.ssl.port** dans le fichier SKLMConfig.properties.

Port d'agent IBM Security Key Lifecycle Manager
L'agent utilise le port par défaut 60015 pour communiquer avec le serveur IBM Security Key Lifecycle Manager. Vous pouvez mettre à jour le numéro de port de l'agent par défaut uniquement lorsque l'instance d'IBM Security Key Lifecycle Manager n'est pas configurée pour une configuration multimaître.

- Interface de ligne de commande :
  a. Entrez la commande **tklmConfigGetEntry** sur une ligne pour obtenir la valeur en cours de la propriété cible dans le fichier SKLMConfig.properties. Par exemple, entrez sur une seule ligne :

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

     Voici un exemple de réponse :

     ```
     3801
     ```

  b. Indiquez la modification demandée. Par exemple, pour définir un autre numéro de port TCP, entrez sur une seule ligne :

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

- Interface REST :
  a. Obtenez un identificateur d'authentification utilisateur unique pour accéder aux services REST d'IBM Security Key Lifecycle Manager. Pour plus d'informations sur le processus d'authentification, voir Processus d'authentification pour les services REST.

b. Pour exécuter le **service REST Get Single Config Property**, envoyez la demande HTTP GET. Transmettez l'identificateur d'authentification utilisateur que vous avez obtenu à l'étape a avec le message de demande, conformément à l'exemple suivant :

Demandes de service

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

Réponse positive

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

c. Indiquez la modification demandée. Par exemple, pour définir un autre numéro de port TCP, envoyez la demande de service suivante :

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

Que faire ensuite

Pour qu'une modification (changement de numéro de port par exemple) prenne effet, redémarrez le serveur IBM Security Key Lifecycle Manager.

Vérification du numéro de port actuel

Après l'installation du serveur IBM Security Key Lifecycle Manager, vous pouvez déterminer les numéros de port sécurisés et non sécurisés pour le serveur IBM Security Key Lifecycle Manager et pour WebSphere Integrated Solutions Console.

Pourquoi et quand exécuter cette tâche

La valeur des numéros de port est spécifiée par la propriété **WC_adminhost_secure**, **WC_defaulthost**, et **WC_defaulthost_secure**, dans le fichier *WAS_HOMEWAS*/profiles/KLMProfile/properties/portdef.props. Par exemple, le fichier peut spécifier les valeurs suivantes :

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

La valeur de propriété **WC_adminhost_secure** correspond au port sécurisé de WebSphere Integrated Solutions Console. La valeur de propriété **WC_defaulthost** correspond au port non sécurisé serveur IBM Security Key Lifecycle Manager et **WC_defaulthost_secure** correspond au port sécurisé.

Spécification des paramètres de service de clés

Vous pouvez modifier les paramètres de certificat par défaut fournis par IBM Security Key Lifecycle Manager.

Pourquoi et quand exécuter cette tâche

Utilisez la page Paramètres de service de clés pour changer les valeurs de certificats. Vous pouvez également utiliser les commandes CLI ou les interfaces REST suivantes pour répertorier ou modifier les propriétés appropriées dans le fichier `SKLMConfig.properties` :

- **`tklmConfigGetEntry`** et **`tklmConfigUpdateEntry`**
- **`Service REST Get Single Config Property`** et **`Service REST Update Config Property`**

Votre rôle doit avoir un droit d'utilisation de l'action de configuration.

Avant de commencer, déterminez si :

- Vous devez valider la date du certificat avant qu'une clé soit servie. La validation confirme que le certificat est valide et qu'il n'est pas arrivé à expiration.
- Des certificats doivent être identifiés à l'aide de l'identificateur de clé d'objet stocké dans le certificat.

Procédure

1. Accédez à la page ou au répertoire approprié(e) :
   - Interface graphique :

     Connectez-vous à l'interface graphique. Cliquez sur **IBM Security Key Lifecycle Manager** > **Configuration** > **Paramètres de service de clés**.
   - Interface de ligne de commande
     a. Accédez au répertoire `<WAS_HOME>/bin`. Exemple :

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

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

     b. Démarrez l'interface **`wsadmin`** en utilisant un ID utilisateur autorisé, comme `SKLMAdmin`. Exemple :

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

        Linux
        ```
        ./wsadmin.sh -username SKLMAdmin
        -password mypwd -lang jython
        ```
   - Interface REST :
     – Ouvrez un client REST.
2. Modifiez la valeur d'un ou de plusieurs paramètres de certificat :
   - Dans l'interface graphique, modifiez un ou plusieurs des paramètres suivants avant de cliquer sur **OK** :

     Ne pas utiliser de certificats arrivés à expiration pour les demandes d'écriture ou les écritures de données

     Avant de servir une clé, vérifie que la date d'expiration du ou des certificats qui encapsulent cette clé n'est pas passée. Les certificats arrivés à expiration sont utilisés uniquement pour les demandes de lecture. Lorsque cette option est sélectionnée, les certificats arrivés à expiration ne sont pas utilisés pour l'écriture de données. La sélection de cette case à cocher fait passer à `true` la propriété **`cert.valiDATE`** dans le fichier `SKLMConfig.properties`.

Maintenir en attente les certificats de communication des unités client
Permet de maintenir en attente les certificats de communication des unités client jusqu'à ce que vous les acceptiez comme certificats de confiance pour sécuriser la communication entre les unités en question et le serveur IBM Security Key Lifecycle Manager. Si cette option est désactivée, vous devrez importer manuellement les certificats de communication des unités client. Ce paramètre de configuration est associé à la propriété **enableClientCertPush** dans le fichier SKLMConfig.properties.

Identifier les certificats par leur nom.
Identifiez les certificats à l'aide du nom de certificat stocké dans le certificat, plutôt qu'à l'aide d'un identificateur de clé du sujet. Vous définissez le nom du certificat au moment de sa création. Cette fonction est utilisée lors du déchiffrement des données écrites sur une unité.

Si cette option n'est pas sélectionnée, l'identificateur de clé de sujet (SKI) est utilisé pour déterminer le certificat à employer lors de la lecture de données sur une cartouche ou une autre unité. Ce paramètre de configuration est associé à la valeur de la propriété **useSKIDefaultLabels** dans le fichier SKLMConfig.properties.

- Interface de ligne de commande :
  a. Entrez la commande **tklmConfigGetEntry** sur une ligne pour obtenir la valeur en cours de la propriété cible dans le fichier SKLMConfig.properties. Par exemple, entrez :

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

     Voici un exemple de réponse :

     ```
     False
     ```

  b. Indiquez la modification demandée. Par exemple, pour faire passer à true la propriété **zOSCompatibility**, tapez sur une seule ligne :

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

- Interface REST :
  a. Obtenez un identificateur d'authentification utilisateur unique pour accéder aux services REST d'IBM Security Key Lifecycle Manager. Pour plus d'informations sur le processus d'authentification, voir Processus d'authentification pour les services REST.
  b. Pour exécuter le **service REST Get Single Config Property**, envoyez la demande HTTP GET. Transmettez l'identificateur d'authentification utilisateur que vous avez obtenu à l'étape a avec le message de demande, conformément à l'exemple suivant :

     Demandes de service

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

     Réponse positive

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

c. Indiquez la modification demandée. Par exemple, vous pouvez envoyer la demande de service suivante pour modifier la valeur de la propriété **zOSCompatibility** en `true` :

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

Que faire ensuite

Les modifications apportées aux paramètres de certificat se produisent de manière dynamique. Vous pouvez ensuite créer les certificats nécessaires et les associer à des unités spécifiques.

Configuration du fichier de clés certifiées

Le fichier de clés certifiées IBM Security Key Lifecycle Manager stocke les certificats de confiance et les certificats racine d'unité qui sont utilisés pour la communication sécurisée entre IBM Security Manager Key Lifecycle et les unités.

L'installation d'IBM Security Key Lifecycle Manager crée le fichier de clés certifiées `tklmTruststore.jceks` dans `<WAS_HOME>\products\sklm\keystore`.

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

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

Vous pouvez ajouter le certificat racine de l'unité à la liste de confiance en l'ajoutant dans le fichier de clés certifiées. Une fois que le certificat racine de l'unité est ajouté au fichier de clés certifiées, toutes les unités possédant des certificats signés par ce certificat racine deviennent automatiquement dignes de confiance. L'ajout d'un certificat racine d'unité évite d'avoir à importer le certificat d'unité dans la liste des certificats de communication d'unité client pour établir la communication SSL/TLS avec le serveur IBM Security Key Lifecycle Manager.

Vous pouvez utiliser l'interface graphique d'IBM Security Key Lifecycle Manager, l'interface de ligne de commande et l'interface REST pour gérer les certificats dans le fichier de clés certifiées.

Vous pouvez exécuter les actions suivantes sur les certificats :

- Ajouter un certificat au fichier de clés certifiées
- Afficher les certificats dans le fichier de clés certifiées
- Supprimer des certificats du fichier de clés certifiées

Ajout d'un certificat au fichier de clés certifiées

Vous pouvez ajouter un certificat à partir d'un fichier de certificat qui est au format `DER` ou `base64` au fichier de clés certifiées interne d'IBM Security Key Lifecycle Manager. Le certificat permet la communication entre IBM Security Key Lifecycle Manager et l'unité qui s'identifie elle-même à l'aide de ce certificat ou du certificat racine associé.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser la boîte de dialogue Ajouter un certificat, la commande **tklmTrustStoreCertAdd** ou le **Truststore Certificate Add REST Service** pour ajouter un certificat au fichier de clés certifiées d'IBM Security Key Lifecycle Manager. Votre ID utilisateur doit avoir le rôle `klmSecurityOfficer`.

Procédure

1. Accédez à la page ou au répertoire approprié.
   - Interface graphique
     a. Connectez-vous à l'interface graphique.
     b. Cliquez sur **IBM Security Key Lifecycle Manager** > **Configuration** > **Fichier de clés certifiées**.
     c. Sur la page Fichier de clés certifiées, cliquez sur **Ajouter**.
   - Interface de ligne de commande
     a. Accédez au répertoire <*WAS_HOME*>/bin. Exemple :

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

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

     b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme `SKLMAdmin`. Exemple :

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

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

   - Interface REST
     – Ouvrez un client REST.
2. Ajoutez un certificat à partir d'un fichier de certificat qui est au format `DER` ou `base64` au fichier de clés certifiées.
   - Interface graphique
     a. Dans la zone **Alias de certificat**, indiquez le nom d'alias pour le certificat.
     b. Cliquez sur **Parcourir** pour spécifier l'emplacement du fichier certificat sous le répertoire <*SKLM_DATA*>, par exemple `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data`. Pour la définition de <*SKLM_DATA*>, voir Définitions relatives à un répertoire *HOME* et d'autres variables de répertoire.
     c. Sélectionnez le fichier de certificat comme par exemple `DER` ou `base64`.
     d. Cliquez sur **Ajouter un certificat**.
   - Interface de ligne de commande

     Entrez **tklmTrustStoreCertAdd** pour ajouter un fichier certificat au fichier de clés certifiées. Par exemple, pour ajouter un fichier certificat au format `DER`, exécutez la commande suivante.
     ```
     print AdminTask.tklmTrustStoreCertAdd
      ('[-fileName d:\\mypath\\mycertfilename.der
       -format DER -alias myCertAlias]')
     ```
   - Interface REST

     Utilisez le **service REST Truststore Certificate Add** pour ajouter un certificat. Par exemple, vous pouvez envoyer la demande HTTP ci-dessous.

```
PUT https://localhost:<port>/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\\clientsslcert
"certFormat":"DER","certAlias":"myCert"}
```

Suppression d'un certificat du fichier de clés certifiées

Vous pouvez supprimer un certificat qui se trouve dans le fichier de clés certifiées interne d'IBM Security Key Lifecycle Manager. Par exemple, vous pouvez supprimer un certificat si celui-ci n'a plus de raison d'être.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser la boîte de dialogue Supprimer, la commande **tklmTrustStoreCertDelete** ou le **Service REST Truststore Certificate Delete** pour supprimer un certificat du fichier de clés certifiées. Votre ID utilisateur doit avoir le rôle klmSecurityOfficer.

Procédure

1. Accédez à la page ou au répertoire approprié.
   - Interface graphique
     a. Connectez-vous à l'interface graphique.
     b. Cliquez sur **IBM Security Key Lifecycle Manager** > **Configuration** > **Fichier de clés certifiées**.
     c. Sur la page Fichier de clés certifiées, sélectionnez un certificat.
     d. Cliquez sur **Supprimer**.
     e. Vous pouvez également faire un clic droit sur un certificat dans le tableau, puis sélectionner **Supprimer**.
   - Interface de ligne de commande
     a. Accédez au répertoire <*WAS_HOME*>/bin. Exemple :

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

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

     b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme SKLMAdmin. Exemple :

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

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

   - Interface REST
     – Ouvrez un client REST.
2. Supprimez le certificat du fichier de clés certifiées.
   - Interface graphique

     Dans la boîte de dialogue Confirmer, lisez le message avant de supprimer le certificat. Cliquez sur **OK**.
   - Interface de ligne de commande

Utilisez la commande `tklmTrustStoreCertList` pour rechercher un certificat, et la commande `tklmTrustStoreCertDelete` pour supprimer un certificat dans le fichier de clés certifiées. Pour rechercher le certificat, exécutez la commande suivante.

```
print AdminTask.tklmTrustStoreCertList ('[-alias myCertAlias]')
```

Pour supprimer un certificat du fichier de clés certifiées, exécutez la commande suivante.

```
print AdminTask.tklmTrustStoreCertDelete ('[-alias myCertAlias]')
```

- Interface REST

  Utilisez le `Service REST Truststore Certificate List` pour rechercher un certificat et le `Service REST Truststore Certificate Delete` pour supprimer un certificat du fichier de clés certifiées. Par exemple, vous pouvez envoyer les demandes HTTP suivantes à l'aide d'un client REST.

```
GET https://localhost:<port>/SKLM/rest/v1/trustStoreCertificates?alias=myCertAlias
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth userAuthId=139aeh34567m
```

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

Administration des groupes, des utilisateurs et des rôles

Vous pouvez limiter la gamme d'activités que les administrateurs peuvent effectuer dans votre organisation.

Pour plus d'efficacité à long terme, créez un groupe et associez-lui des rôles et des utilisateurs plutôt que d'affecter directement un ensemble déterminé de rôles à chaque utilisateur. Vous aurez plus de facilité à définir ou changer les rôles des personnes accomplissant le même travail et vous éviterez d'avoir à tout reprendre si des utilisateurs sont mutés dans d'autres services.

Par exemple, vous pouvez spécifier les gammes d'activités suivantes :

- Aucun accès n'est disponible pour certains rôles. Par exemple, votre organisation peut souhaiter séparer les activités de sauvegarde et de restauration des fichiers.
- Certaines tâches sont masquées dans WebSphere Integrated Solutions Console.
- L'administration est limitée aux unités de bande LTO.

Affectation de droits

Vous pouvez associer un groupe d'administration a un ensemble limité de droits.

Pourquoi et quand exécuter cette tâche

Cette tâche fait appel à l'ID utilisateur WASAdmin dans WebSphere Integrated Solutions Console. Son but est d'associer un groupe à un ensemble limité d'actions d'administration des serveurs de stockage DS5000.

Pour plus d'informations sur les commandes qui servent à mapper des groupes aux rôles, voir la documentation IBM WebSphere Application Server (http://www.ibm.com/support/knowledgecenter/en/SSAW57_9.0.0/com.ibm.websphere.nd.multiplatform.doc/ae/rxml_atauthorizationgroup.html).

Procédure

1. Connectez-vous à la WebSphere Integrated Solutions Console.
   - Interface graphique :
     a. Sur la page d'accueil du navigateur, tapez l'ID utilisateur `WASAdmin` et un mot de passe tel que `wasadminpw`.
     b. Dans l'interface graphique, cliquez sur **Utilisateurs et groupes** > **Rôles du groupe d'administration**.
     c. Cliquez sur **Ajouter**.
   - Interface de ligne de commande
     a. Accédez au répertoire `<WAS_HOME>/bin`. Exemple :

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

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

     b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme WASAdmin. Exemple :

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

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

2. Associez un ensemble limité de rôles au groupe.
   - Interface graphique :
     a. Dans la page Rôles du groupe d'administration, sous **Rôle(s)**, sélectionnez le sous-ensemble nécessaire des rôles dans la liste. Par exemple, effectuez les étapes suivantes :
        – Bloquez l'accès à certains rôles. Par exemple, votre organisation peut souhaiter séparer les activités de restauration des fichiers. Dans ce cas, ne sélectionnez pas l'entrée `klmRestore` dans la liste.
        – Déterminez s'il est nécessaire de masquer d'autres tâches dans WebSphere Integrated Solutions Console. Dans l'affirmative, sélectionnez le rôle **suppressmonitor**.
        – Limitez l'administration aux serveurs de stockage DS5000. Par exemple, sélectionnez **DS5000**.

          Autrement, si votre travail est d'administrer un nouveau groupe d'unités tel que `monDS5000`, sélectionnez `monDS5000` (groupe qui doit avoir été préalablement créé).
        – Maintenez la touche Ctrl enfoncée et sélectionnez les rôles qui s'appliquent à IBM Security Key Lifecycle Manager :

          klmBackup
          Créer et supprimer une sauvegarde de données.

          klmRestore
          Restaurer une copie de sauvegarde de données.

          klmConfigure
          Lire ou changer des propriétés, ou agir sur des certificats.

          klmAudit
          Visualiser des données d'audit.

          klmView
          Visualiser des objets.

klmCreate
Créer des objets.

klmModify
Modifier des objets.

klmDelete
Supprimer des objets.

klmGet
Exporter une clé ou un certificat.

suppressmonitor
Masquer les autres tâches dans la WebSphere Integrated Solutions Console.

DS5000
Actions sur les serveurs de stockage DS5000.

b. Sélectionnez **Mapper les groupes comme indiqué ci-dessous**.
c. Entrez une chaîne de recherche dans la zone **Chaîne de recherche**. Par exemple, entrez `DS5000Admin`.
d. Cliquez sur **Rechercher**.
e. Dans la liste **Disponible**, sélectionnez le groupe.
f. Cliquez sur la flèche pour déplacer le groupe sélectionné vers la colonne **Mappé sur le rôle**.
g. Cliquez sur **OK**.
h. Cliquez sur **Sauvegarder** pour enregistrer directement les modifications dans la configuration maîtresse.

- Interface de ligne de commande :

  Tapez `mapGroupsToAdminRole` et spécifiez les valeurs requises pour associer le groupe à un rôle d'administration spécifique. Par exemple, pour associer plusieurs rôles à un groupe, tapez la série de commandes Jython correspondantes, en appuyant sur **Entrée** après chacune d'elles.

  – Spécifiez le premier rôle du groupe :

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

  – Spécifiez le rôle suivant du groupe :

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

  – Spécifiez les rôles restants du groupe, en utilisant une commande distincte pour chacun d'eux :

  ```
  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]')
  ```

  où :

- authorizationGroupName
Nom du groupe d'autorisation. Si vous ne spécifiez pas ce paramètre, le groupe d'autorisations de niveau cellule est utilisé. (Chaîne, facultative)

- roleName
Nom du rôle d'administration. (Chaîne, requise)

- groupids
Liste d'ID de groupe associés au rôle d'administration. (String[])

3. Enregistrez votre travail.
   - Interface graphique :

     Confirmez l'achèvement de la tâche en répondant à l'invite affichée par l'interface graphique.
   - Interface de ligne de commande :

     Enregistrez votre configuration. Par exemple, à l'aide de Jython, tapez :

     ```
     print AdminConfig.save()
     ```
4. Vérifiez que les rôles sauvegardés ont bien été affectés au groupe.
   - Interface graphique

     Fermez et rouvrez la page Rôles du groupe d'administration. Les rôles supplémentaires apparaissent.
   - Interface de ligne de commande

     En utilisant la syntaxe Jython, tapez :

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

Que faire ensuite

Spécifiez ensuite les autres groupes requis par votre organisation. Par exemple, spécifiez un groupe d'administration en charge des tâches d'exploitation (opérateurs).

Création d'un utilisateur dans un groupe

Créez un utilisateur et affectez-le à un groupe d'administrateurs du système afin qu'il devienne membre de ce groupe.

Pourquoi et quand exécuter cette tâche

Cette tâche utilise l'ID utilisateur WASAdmin dans WebSphere Integrated Solutions Console pour créer un utilisateur et l'ajouter à un groupe.

Remarque : Pour accéder à l'interface graphique ou à l'interface de ligne de commande d'IBM Security Key Lifecycle Manager, l'utilisateur doit être affecté à ce groupe : `klmGUICLIAccessGroup`

Pour plus d'informations sur les commandes qui servent à créer des groupes et des utilisateurs, voir la documentation IBM WebSphere Application Server (http://www.ibm.com/support/knowledgecenter/en/SSAW57_9.0.0/com.ibm.websphere.nd.multiplatform.doc/ae/rxml_atwimmgt.html).

Procédure

1. Connectez-vous à WebSphere Integrated Solutions Console.
   - Interface graphique :

a. Sur la page d'accueil du navigateur, tapez l'ID utilisateur `WASAdmin` et un mot de passe tel que `wasadminpw`.
b. Dans l'arborescence de navigation, cliquez sur **Utilisateurs et groupes** > **Gérer utilisateurs**.

- Interface de ligne de commande
  a. Accédez au répertoire *<WAS_HOME>*`/bin`. Exemple :

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

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

  b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme WASAdmin. Exemple :

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

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

2. Créez un utilisateur et spécifiez son appartenance au nouveau groupe.
   - Interface graphique :
     a. Sur la page Gérer les utilisateurs, cliquez sur **Créer**.
     b. Sur la page Créer un utilisateur, spécifiez les informations requises telles que l'ID utilisateur et le mot de passe. Par exemple, entrez `monAdmin` comme ID utilisateur et `monmdp` comme mot de passe.
     c. Cliquez sur **Créer**.
     d. Cliquez sur le lien au nouvel ID utilisateur pour afficher les propriétés de cet utilisateur.
     e. Dans la boîte de dialogue Propriétés utilisateur, cliquez sur **Groupes**.
     f. Cliquez sur **Ajouter**.
     g. Dans la boîte de dialogue Ajouter un utilisateur aux groupes, cliquez sur **Rechercher**.
     h. Dans la table des groupes, sélectionnez le groupe que vous avez créé précédemment, puis cliquez sur **Ajouter**.
     i. Lisez le message confirmant que l'utilisateur a été ajouté au groupé, puis cliquez sur **Fermer**.
   - Interface de ligne de commande :
     a. Créez d'abord l'utilisateur. Tapez `createUser` et spécifiez les valeurs nécessaires à la création d'un utilisateur. Par exemple, à l'aide de Jython, tapez :
     ```
     print AdminTask.createUser ('[-uid monAdmin -password tempPass
       -confirmPassword tempPass -cn monAdmin -sn JDoe]')
     ```
     où :

     -uid ID unique de l'utilisateur que vous voulez créer. (Chaîne, requise)

     -password
     Spécifie le mot de passe de l'utilisateur. (Chaîne, requise)

     -confirmPassword
     Nouvelle saisie du même mot de passe pour vérifier sa concordance avec la première saisie (paramètre password). (Chaîne, facultative)

     -cn Prénom de l'utilisateur. (Chaîne, facultative)

-sn Nom de famille de l'utilisateur. (Chaîne, facultative)

b. Ajoutez l'utilisateur comme membre du groupe. Par exemple, en utilisant le format Jython, tapez :

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

où :

memberUniqueName *nomUnique*
Nom unique de l'utilisateur que vous voulez ajouter au groupe spécifié.

groupUniqueName *nomUnique*
Nom unique du groupe auquel vous souhaitez ajouter l'utilisateur.

3. Vérifiez que l'utilisateur est devenu membre du groupe.
   - Interface graphique :
     a. Dans l'arborescence de navigation, cliquez sur **Utilisateurs et groupes** > **Gérer les utilisateurs**.
     b. Sur la page Gérer les utilisateurs, dans la colonne **ID utilisateur**, cliquez sur l'entrée correspondant au nouvel ID utilisateur.
     c. Dans la boîte de dialogue Propriétés utilisateur, cliquez sur l'onglet **Groupes**. Vérifiez que l'utilisateur est un membre du nouveau groupe.
   - Interface de ligne de commande :

     Par exemple, à l'aide de Jython, tapez :

     ```
     print AdminTask.getMembersOfGroup('[-uniqueName
       cn=DS5000Admin,o=defaultWIMFileBasedRealm]')
     ```
4. Enregistrez votre travail.
   - Interface graphique :

     Confirmez l'achèvement de la tâche en répondant à l'invite affichée par l'interface graphique.
   - Interface de ligne de commande :

     Enregistrez votre configuration. Par exemple, à l'aide de Jython, tapez :

     ```
     print AdminConfig.save()
     ```
5. Si vous avez utilisé l'interface de ligne de commande pour créer l'utilisateur, exécutez successivement les commandes **stopServer** et **startServer** pour redémarrer le serveur IBM Security Key Lifecycle Manager. Connectez-vous ensuite à l'aide du nouvel ID utilisateur.

Que faire ensuite

Vérifiez ensuite que l'utilisateur peut exécuter les tâches autorisées. Fermez la session ouverte avec WASAdmin. Connectez-vous en tant que nouvel utilisateur et vérifiez que vous pouvez effectuer des tâches à l'aide d'IBM Security Key Lifecycle Manager.

Création d'un groupe

Vous pouvez créer un groupe afin de spécifier des limites pour certains administrateurs du système. Vous devez modéliser le groupe d'après les groupes LTO prédéfinis.

Pourquoi et quand exécuter cette tâche

Cette tâche utilise l'ID utilisateur WASAdmin dans la WebSphere Integrated Solutions Console pour créer un groupe d'administration.

Remarque : Pour accéder à l'interface graphique ou à l'interface de ligne de commande d'IBM Security Key Lifecycle Manager, l'utilisateur doit être affecté à ce groupe : `klmGUICLIAccessGroup`

Pour plus d'informations sur les commandes qui servent à créer des groupes et des utilisateurs, voir la documentation IBM WebSphere Application Server (http://www.ibm.com/support/knowledgecenter/en/SSAW57_9.0.0/com.ibm.websphere.nd.multiplatform.doc/ae/rxml_atwimmgt.html).

Vous pouvez utiliser WebSphere Integrated Solutions Console pour créer des groupes enfants avec des droits différents au sein d'un groupe parent. Cependant, sachez que IBM Security Key Lifecycle Manager reconnaît seulement les droits du groupe parent, et non ceux des groupes enfants.

Procédure

1. Connectez-vous à WebSphere Integrated Solutions Console (`https://localhost:9083/ibm/console/logon.jsp`).
   - Interface graphique :
     a. Sur la page d'accueil du navigateur, tapez l'ID utilisateur `WASAdmin` et le mot de passe de cet administrateur.
     b. Dans l'arborescence de navigation, cliquez sur **Utilisateurs et groupes** > **Gérer les groupes**.
   - Interface de ligne de commande
     a. Accédez au répertoire `<WAS_HOME>/bin`. Exemple :

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

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

     b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme WASAdmin. Exemple :

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

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

2. Créez un groupe :
   - Interface graphique :
     a. Sur la page Gérer les groupes, cliquez sur **Créer**.
     b. Dans la zone **Nom du groupe**, spécifiez le nom du groupe. Par exemple, entrez `DS5000Admin`.
     c. Dans la zone **Description**, spécifiez davantage d'informations sur le groupe que vous voulez créer.
     d. Cliquez sur **Créer**.
   - Interface de ligne de commande :
     a. Créez un groupe d'autorisation.
     b. Créez un groupe.

Tapez `createGroup` et spécifiez les valeurs nécessaires à la création d'un groupe. Par exemple, à l'aide de Jython, tapez :

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

où :

-cn Obligatoire (chaîne). Nom usuel du groupe que vous voulez créer. Ce paramètre est mappé à la propriété **cn** dans le gestionnaire de membre virtuel (Virtual Member Manager).

-description
Facultatif (chaîne). Spécifie plus d'informations sur le groupe que vous voulez créer.

3. Enregistrez votre travail.
   - Interface graphique :

     Confirmez l'achèvement de la tâche en répondant à l'invite affichée par l'interface graphique.
   - Interface de ligne de commande :

     Enregistrez votre configuration. Par exemple, à l'aide de Jython, tapez :

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

Que faire ensuite

Affectez ensuite un ou plusieurs droits ou rôles au groupe.

Vérification des tâches accessibles à un utilisateur

Vérifiez qu'un nouvel utilisateur ajouté à un groupe d'administration peut exécuter les tâches prévues.

Pourquoi et quand exécuter cette tâche

Cette tâche permet de vérifier qu'un utilisateur membre d'un groupe donné peut exécuter les tâches qui lui sont autorisées du fait de son appartenance à ce groupe. Par exemple, l'utilisateur peut administrer des serveurs de stockage DS5000.

Remarque : Pour accéder à l'interface graphique ou à l'interface de ligne de commande d'IBM Security Key Lifecycle Manager, l'utilisateur doit être affecté à ce groupe : `klmGUICLIAccessGroup`

Pour plus d'informations sur les commandes qui servent à mapper des groupes aux rôles, voir la documentation IBM WebSphere Application Server (http://www.ibm.com/support/knowledgecenter/en/SSAW57_9.0.0/com.ibm.websphere.nd.multiplatform.doc/ae/rxml_atauthorizationgroup.html).

Procédure

Vérifiez que l'utilisateur peut effectuer les tâches que lui autorise son appartenance au groupe.

- Interface graphique :
  1. Fermez la session ouverte avec l'ID utilisateur WASAdmin.
  2. Connectez-vous à l'interface graphique en tant qu'utilisateur autorisé dans le groupe. Par exemple, utilisez `monAdmin`.
  3. Dans la table Gestion des clés et des unités, vérifiez que le seul choix administratif disponible est DS5000.

Autrement, si une tâche exécutée antérieurement a défini des activités administratives pour la gestion d'un nouveau groupe d'unités tel que monDS5000, vérifiez que le seul choix administratif disponible est monDS5000.

4. Sélectionnez l'unité et cliquez sur **Aller à** > **Gestion des clés et des unités**.
5. Vous pouvez aussi cliquer avec le bouton droit sur l'unité et sélectionner **Gestion des clés et des unités**.
6. Sur la page de gestion pour DS5000, effectuez une tâche. Par exemple, ajoutez un nouveau groupe de clés.

- Interface de ligne de commande :
  1. Fermez la session **wsadmin** ouverte avec wasadmin.
  2. Dans le répertoire *WAS_HOME*WAS/bin, démarrez une nouvelle session **wsadmin** en utilisant Jython. Ensuite, connectez-vous à **wsadmin** avec un ID utilisateur autorisé, tel que le nouvel ID monAdmin comme indiqué dans l'exemple ci-dessous.
     – Accédez au répertoire <*WAS_HOME*>/bin.

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

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

     – Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé.

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

       Linux
       ```
       ./wsadmin.sh -username monAdmin -password password -lang jython
       ```

  3. Ajoutez un groupe de clés exemple. Par exemple, entrez :
     ```
     print AdminTask.tklmGroupCreate
      ('[-name GROUP-DS5000-abcd2de9 -type keygroup -usage DS5000]')
     ```
     Vous pouvez également envoyer la demande HTTP suivante à l'aide d'un client REST :
     ```
     POST https://localhost:<port>/SKLM/rest/v1/keygroups/newGroup
     Content-Type: application/json
     Accept : application/json
     Authorization: SKLMAuth authId=139aeh34567m
     {"usage":"DS500"}
     ```

Que faire ensuite

Spécifiez ensuite les autres groupes requis par votre organisation. Par exemple, définissez un groupe réservé au tâches d'opérateur et d'auditeur.

Règles sur les mots de passe pour l'utilisateur IBM Security Key Lifecycle Manager

Les règles s'appliquant au mot de passe d'un nouvel utilisateur d'IBM Security Key Lifecycle Manager sont spécifiées par le fichier *SKLM_DATA*/config/TKLMPasswordPolicy.xml.

Les règles ne s'appliquent pas aux mots de passe créés initialement pour les utilisateurs par défaut tels que SKLMAdmin. Ces utilisateurs par défaut sont eux-mêmes créés durant l'installation d'IBM Security Key Lifecycle Manager.

Les règles sur les mots de passe s'appliquent en revanche aux changements des mots de passe des utilisateurs par défaut, ainsi qu'aux mots de passe des nouveaux

utilisateurs et à leurs changements futurs. Le contrôle du respect de ces règles n'est effectué que lorsque vous créez ou changez un profil d'utilisateur. Lorsque vous créez un nouvel utilisateur, vous devez lui affecter un rôle avant qu'il ne tente de se connecter à IBM Security Key Lifecycle Manager.

La stratégie globale (ensemble de règles sur les mots de passe) est activée par défaut. Vous pouvez utiliser un éditeur XML ou ASCII pour modifier ce fichier. Pour désactiver la stratégie dans son ensemble, faites passer à `false` le paramètre **`enabled`** :

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

Les règles sur les mots de passe reconnues et appliquées par IBM Security Key Lifecycle Manager sont les suivantes :

Tableau 1. Règles sur les mots de passe

Règle	**Valeur par défaut**
Longueur minimale	6
Longueur maximale	20
Nombre minimum de caractères numériques	2
Nombre minimum de caractères alphabétiques	3
Nombre maximal d'occurrences consécutives du même caractère	2
Caractères majuscules	1 au minimum
Caractères minuscules	1 au minimum
Caractères spéciaux Cette exigence de caractère spécial ne s'applique pas lorsque l'outil **`imcl`** est utilisé pour l'installation en mode silencieux. Pour plus d'informations sur les caractères spéciaux pris en charge, voir «Caractères spéciaux pris en charge dans les mots de passe», à la page 27.	1 au minimum
Interdire la présence de l'ID utilisateur* dans le mot de passe	Activée
Interdire la présence du nom de l'utilisateur* dans le mot de passe	Activée

* La détection de cette valeur tient compte de la casse des caractères.
Remarque : Pour spécifier que la valeur est indépendante de la casse, éditez le fichier de règles par défaut et spécifiez `CaseInsensitive` pour l'ID et le nom d'utilisateur :

```
<?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>
```

Caractères spéciaux pris en charge dans les mots de passe

Les caractères spéciaux suivants sont pris en charge dans le mot de passe administrateur Db2, le mot de passe administrateur WebSphere Application Server (WASadmin) et le mot de passe administrateur IBM Security Key Lifecycle Manager (SKLMAdmin).

Caractères spéciaux pris en charge dans les mots de passe sur les systèmes Linux

Le tableau suivant fournit la liste des caractères spéciaux pris en charge dans les mots de passe sur les systèmes Linux :

Nom du caractère spécial	Caractère spécial
tilde	~
arobase	@
dièse	#
trait de soulignement	_
accent circonflexe	^
astérisque	*
signe pourcentage	%
barre oblique	/
point	.
signe plus	+
deux-points	:
point-virgule	;
signe égal	=

Caractères spéciaux pris en charge dans les mots de passe sur les systèmes Windows

Le tableau suivant fournit la liste des caractères spéciaux pris en charge dans les mots de passe sur les systèmes Windows :

Nom du caractère spécial	Caractère spécial
tilde	~
arobase	@
trait de soulignement	_
barre oblique	/
signe plus	+
deux-points	:

Instructions d'utilisation des caractères spéciaux pris en charge dans les mots de passe

Tenez compte des instructions suivantes lorsque vous utilisez des caractères spéciaux pris en charge dans les mots de passe. Ces instructions ne sont pas applicables lorsque vous indiquez des mots de passe dans l'interface graphique.

- Placez le mot de passe entre guillemets lorsque vous utilisez les shells du système d'exploitation pour vous connecter à l'interface wsadmin WebSphere Application Server ou à la ligne de commande Db2 ou pour exécuter une installation de groupe de correctifs. Utilisez des guillemets simples pour Linux et des guillemets doubles pour Windows. Par exemple :

  Linux

  ```
  [root@sklm bin]# ./wsadmin.sh -username sklmadmin -password '~@_ABc12/+:' -lang jython
  WASX7209I: Connected to process "server1" on node SKLMNode using SOAP connector; The type of process is: UnManagedProcess
  WASX7031I: For help, enter: "print Help.help()"
  wsadmin>
  ```

  Windows

  ```
  C:\Program Files\IBM\WebSphere\AppServer\bin>wsadmin.bat -username sklmadmin -password "~@_ABc12/+:" -lang jython
  WASX7209I: Connected to process "server1" on node SKLMNode using SOAP connector;
    The type of process is: UnManagedProcess
  WASX7031I: For help, enter: "print Help.help()"
  wsadmin>
  ```

- Ajoutez des mots de passe chiffrés aux éléments appropriés du fichier de réponses lorsque vous exécutez le processus d'installation ou de mise à niveau d'IBM Security Key Lifecycle Manager (groupe de correctifs ou édition principale) en mode silencieux.

  Pour créer un mot de passe chiffré, utilisez l'utilitaire `imcl` comme suit :

  Linux

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

  Veillez à utiliser une barre oblique inversée (\) comme caractère d'échappement pour les caractères spéciaux du mot de passe. Par exemple :

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

  La chaîne chiffrée (par exemple, `pABm1rqy66jAykrhBtpM6Q==`) est renvoyée.

  Windows

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

  Veillez à placer le mot de passe complet entre guillemets doubles. Par exemple :

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

  La chaîne chiffrée (par exemple, `pABm1rqy66jAykrhBtpM6Q==`) est renvoyée.

Pour plus d'informations, voir Mot de passe chiffré pour les éléments du fichier de réponses.

Changement des règles sur les mots de passe

Utilisez un éditeur pour changer manuellement les règles sur les mots de passe fournies par IBM Security Key Lifecycle Manager.

Pourquoi et quand exécuter cette tâche

Veillez à changer uniquement les valeurs des éléments et des attributs dans les règles sur les mots de passe, et non les noms des éléments et des attributs eux-mêmes. Les règles sur les mots de passe s'appliquent aux changements des mots de passe des utilisateurs par défaut, ainsi qu'aux mots de passe des nouveaux utilisateurs et à leurs changements futurs. Le contrôle du respect de ces règles n'est effectué que lorsque vous créez ou changez un profil d'utilisateur.

Procédure

1. Avant tout, faites une copie de sauvegarde du fichier *SKLM_DATA*/config/TKLMPasswordPolicy.xml et conservez-la dans un endroit sûr. Si vous rencontrez des problèmes avec les règles sur les mots de passe qui ont été modifiées, vous pouvez restaurer la copie de sauvegarde.
2. Editez le fichier TKLMPasswordPolicy.xml dans un éditeur de texte en veillant à changer uniquement les valeurs des éléments et des attributs XML.
3. Enregistrez le fichier modifié.

   La modification des règles prend effet immédiatement. Vous n'avez pas besoin de redémarrer le serveur IBM Security Key Lifecycle Manager.
4. Pour tester les modifications, connectez-vous à WebSphere Application Server en tant qu'utilisateur WASAdmin et créez un profil pour un nouvel utilisateur.

   Vérifiez qu'un mot de passe obéissant aux nouvelles règles est accepté et qu'un autre qui les enfreint est refusé. Après quoi, si vous n'avez plus l'utilité du profil d'utilisateur ayant servi aux tests, supprimez-le.

Changement du mot de passe d'un utilisateur

Le mot de passe modifié d'un utilisateur doit obéir aux règles de mot de passe fournies par IBM Security Key Lifecycle Manager.

Pourquoi et quand exécuter cette tâche

Cette tâche fait appel à l'ID utilisateur WASAdmin dans la WebSphere Integrated Solutions Console. Son but est de changer le mot de passe d'un utilisateur, y compris lorsqu'il s'agit de l'ID utilisateur SKLMAdmin.

Pour plus d'informations sur les commandes qui servent à créer des groupes et des utilisateurs, voir la documentation IBM WebSphere Application Server (http://www.ibm.com/support/knowledgecenter/en/SSAW57_9.0.0/com.ibm.websphere.nd.multiplatform.doc/ae/rxml_atwimmgt.html).

Procédure

1. Connectez-vous à WebSphere Integrated Solutions Console.
   - Interface graphique :
     a. Sur la page d'accueil du navigateur, tapez l'ID utilisateur de WASAdmin et un mot de passe tel que wasadminpw.
     b. Dans l'arborescence de navigation, cliquez sur **Utilisateurs et groupes** > **Gestion des utilisateurs**.
   - Interface de ligne de commande

a. Accédez au répertoire <*WAS_HOME*>/bin. Exemple :

Windows

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

Linux

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

b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme WASAdmin. Exemple :

Windows

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

Linux

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

2. Changez le mot de passe de l'utilisateur.
   - Interface graphique :
     a. Sur la boîte de dialogue **Gérer les utilisateurs** > **Rechercher des utilisateurs**, cliquez sur **Rechercher**.
     b. Dans la table de critères de recherche, faites un double clic sur un ID utilisateur préalablement sélectionné. Par exemple, double-cliquez sur `myAdmin` comme ID utilisateur.
     c. Dans la boîte de dialogue Propriétés utilisateur, changez la valeur des zones **Mot de passe** et **Confirmer le mot de passe**.
     d. Cliquez sur **OK**.
   - Interface de ligne de commande :
     a. Tapez `updateUser` et spécifiez les valeurs requises. Par exemple, en utilisant Jython, entrez sur une seule ligne :

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

où

-uniqueName
Spécifie le nom unique de l'utilisateur dont vous souhaitez créer le mot de passe. (Chaîne, requise)

Vous pouvez utiliser la commande **searchUsers** pour vérifier que le nom identifie correctement l'utilisateur avant de changer son mot de passe.

-password
Spécifie le mot de passe de l'utilisateur. (Chaîne, requise)

Le nouveau mot de passe doit obéir aux règles fournies par IBM Security Key Lifecycle Manager.

-confirmPassword
Nouvelle saisie du même mot de passe pour vérifier sa concordance avec la première saisie (paramètre password). (Chaîne, facultative)

Que faire ensuite

Vérifiez ensuite que l'utilisateur peut se connecter. Fermez la session ouverte avec WASAdmin. Ouvrez une nouvelle session avec l'ID utilisateur dont vous venez de changer le mot de passe et vérifiez que le nouveau mot de passe est accepté.

Réinitialisation d'un mot de passe

Vous devez être l'administrateur pour réinitialiser un mot de passe pour IBM Security Key Lifecycle Manager ou pour WebSphere Application Server.

Pourquoi et quand exécuter cette tâche

Vous pouvez réinitialiser le mot de passe sur l'ordinateur où IBM Security Key Lifecycle Manager s'exécute. Appliquez cette procédure uniquement en cas de perte du mot de passe de l'utilisateur. Dans tous les autres cas, changez le mot de passe via l'interface utilisateur.

Procédure

1. Connectez-vous en utilisant l'ID de l'administrateur local.
2. Sauvegardez le fichier *WAS_HOMEWAS*/profiles/KLMProfile/config/cells/SKLMCell/fileRegistry.xml. Le fait de changer le mot de passe change également ce fichier de registre.
3. Changez le mot de passe.
   - Windows
     a. Démarrez une session **wsadmin** en utilisant la syntaxe Jython. Par exemple, entrez :

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

     b. Réinitialisez le mot de passe de l'utilisateur SKLMAdmin :

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

        Remarque :

        – Seul l'ID utilisateur WASAdmin ou un autre ID ayant des droits d'administrateur de WebSphere Application Server peut changer les mots de passe à l'aide de la commande **AdminTask.changeFileRegistryAccountPassword**.

        – Les mots de passe que vous créez à l'aide de la commande **AdminTask.changeFileRegistryAccountPassword** ne sont pas validés par rapport aux règles sur les mots de passe configurées fournies par IBM Security Key Lifecycle Manager.

          Après la réinitialisation d'un mot de passe perdu, l'utilisateur doit définir son nouveau mot de passe via l'interface graphique.

     c. Enregistrez les changements et quittez la session :

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

   - Linux
     a. Démarrez une session **wsadmin** en utilisant la syntaxe Jython. Par exemple, entrez sur une seule ligne :

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

     b. Réinitialisez le mot de passe de l'utilisateur SKLMAdmin :

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

        Remarque :

        – Seul l'ID utilisateur WASAdmin ou un autre ID ayant des droits d'administrateur de IBM Security Key Lifecycle Manager peut changer

les mots de passe à l'aide de la commande **AdminTask.changeFileRegistryAccountPassword**.

– Les mots de passe que vous créez à l'aide de la commande **AdminTask.changeFileRegistryAccountPassword** ne sont pas validés par rapport aux règles sur les mots de passe configurées fournies par IBM Security Key Lifecycle Manager.

Après la réinitialisation d'un mot de passe perdu, l'utilisateur doit définir son nouveau mot de passe via l'interface graphique.

c. Enregistrez les changements et quittez la session :

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

4. Arrêtez puis redémarrez le serveur.
   - Arrêt

     Windows

     ```
     stopServer.bat server1
     ```

     Linux

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

   - Démarrage

     Windows

     ```
     startServer.bat server1
     ```

     Linux

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

5. Vérifiez que vous pouvez ouvrir une session avec l'ID de l'administrateur spécifié en utilisant le nouveau mot de passe.

Changement du mot de passe d'un utilisateur IBM Security Key Lifecycle Manager

Vous pouvez utiliser l'ID utilisateur de l'application IBM Security Key Lifecycle Manager pour changer le mot de passe d'un utilisateur. Le mot de passe modifié doit obéir aux règles sur les mots de passe fournies par IBM Security Key Lifecycle Manager.

Pourquoi et quand exécuter cette tâche

Pour plus d'informations sur les commandes qui permettent de changer les mots de passe, voir la documentation IBM WebSphere Application Server (http://www.ibm.com/support/knowledgecenter/SSAW57_9.0.0/com.ibm.websphere.nd.multiplatform.doc/ae/rxml_atwimmgt.html).

Procédure

1. Accédez à la page ou au répertoire approprié(e) :
   - Interface de ligne de commande :
     – Dans le répertoire *WAS_HOME*/bin, démarrez une session wsadmin à l'aide de Jython. Connectez-vous à wsadmin avec un ID utilisateur autorisé.

       Windows

       Accédez au répertoire C: \Program Files\IBM\WebSphere\AppServer\bin et tapez :

       ```
       wsadmin.bat -username <utilisateur SKLM> -password <mot de passe utilisateur SKLM>
       -lang jython
       ```

AIX ou Linux

Accédez au répertoire /opt/IBM/WebSphere/AppServer/bin et tapez :

```
./wsadmin.sh -username <utilisateur SKLM> -password <mot de passe utilisateur SKL
-lang jython
```

- Interface graphique :
  - Connectez-vous à l'interface graphique.

2. Changez le mot de passe de l'utilisateur.
   - Interface de ligne de commande :
     - Exécutez la commande suivante :

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

       Exemple :

       ```
       AdminTask.changeMyPassword('[-oldPassword sklmadmin -newPassword
       Ibm12one
       -confirmNewPassword Ibm12One]')
       ```
   - Interface graphique :
     a. Sur la barre d'en-tête, cliquez sur le lien **<Utilisateur SKLM>**.
     b. Cliquez sur l'option de **changement de mot de passe**.
     c. Dans la boîte de dialogue de changement de mot de passe, entrez votre **mot de passe en cours**.
     d. Entrez le **nouveau mot de passe**.
     e. Entrez le nouveau mot de passe dans la zone **Confirmation du nouveau mot de passe**.
     f. Cliquez sur l'option de **changement de mot de passe**.

Création d'un groupe d'unités

Vous pouvez créer un groupe d'unités afin de gérer un sous-ensemble d'unités ayant un usage restreint dans l'entreprise ; il peut s'agir par exemple d'unités de bande LTO réservées exclusivement à une division spécifique de l'organisation. Vous devez également créer un rôle et lui donner exactement le même nom (casse comprise) que celui du groupe d'unités. La concordance des noms tient compte de la casse des caractères.

Pourquoi et quand exécuter cette tâche

Cette tâche utilise l'ID utilisateur SKLMAdmin et l'interface IBM Security Key Lifecycle Manager pour créer un groupe d'unités supplémentaire.

Votre ID utilisateur doit avoir l'une des caractéristiques suivantes :

- Le rôle `securityOfficer` (responsable de la sécurité)
- Le droit d'utiliser les actions d'administration (**klmAdminDeviceGroup**)

  Si vous avez le droit **klmAdminDeviceGroup**, vous pouvez créer, visualiser et supprimer un groupe d'unités. Il n'est pas indispensable que vous définissiez d'abord un rôle pour le groupe d'unités. Cependant, les autres actions auxquelles vous avez accès sont limitées par les droits que vous avez. Par exemple, si vous avez seulement le droit **klmAdminDeviceGroup**, vous ne pouvez pas mettre à jour les attributs après avoir créé le groupe d'unités.

Procédure

1. Connectez-vous à IBM Security Key Lifecycle Manager.
   - Interface graphique :

     Sur la page d'accueil du navigateur, tapez l'ID utilisateur `SKLMAdmin` et un mot de passe tel que `monmotdepasse`.
   - Interface de ligne de commande
     a. Accédez au répertoire `<WAS_HOME>/bin`. Exemple :

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

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

     b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme `SKLMAdmin`. Exemple :

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

        Linux
        ```
        ./wsadmin.sh -username SKLMAdmin
        -password mypwd -lang jython
        ```
   - Interface REST :
     – Ouvrez un client REST.
2. Accédez à la page ou au répertoire approprié :
   - Interface graphique :

     Cliquez sur **Configuration avancée** > **Groupe d'unités**.
     a. Dans la table Groupes d'unités, cliquez sur **Créer**.
     b. Dans la boîte de dialogue Créer un groupe d'unités, remplissez les zones requises et cliquez sur **Créer**.
   - Interface de ligne de commande : tapez :
     ```
     AdminTask.tklmDeviceGroupCreate('[-name myLTO -deviceFamily LTO]')
     ```
   - Interface REST :
     a. Obtenez un identificateur d'authentification utilisateur unique pour accéder aux services REST d'IBM Security Key Lifecycle Manager. Pour plus d'informations sur le processus d'authentification, voir Processus d'authentification pour les services REST.
     b. Pour appeler le **service REST Device Group Create**, envoyez la demande HTTP POST. Transmettez l'identificateur d'authentification utilisateur que vous avez obtenu à l'étape a avec le message de demande, conformément à l'exemple suivant :
     ```
     POST https://localhost:<port>/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. Vérifiez que le groupe d'unités existe.
   - Interface graphique :

     Sur la page de gestion des groupes d'unités, dans la table Groupes d'unités, recherchez le groupe d'unités.
   - Interface de ligne de commande : tapez :
     ```
     print AdminTask.tklmDeviceGroupList ('[-name myLTO -v y]')
     ```
   - Interface REST :

Envoyez la demande HTTP GET suivante à l'aide d'un client REST :

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

Que faire ensuite

Créez un rôle en lui affectant un nom correspondant au groupe d'unités.

Création d'un rôle pour un nouveau groupe d'unités

Lorsque vous créez un nouveau groupe d'unités dans la base de données de IBM Security Key Lifecycle Manager, vous devez également créer un rôle correspondant. Spécifiez le même nom pour le groupe d'unités et pour le rôle. La concordance des noms tient compte de la casse des caractères.

Pourquoi et quand exécuter cette tâche

Vous pouvez ajouter le rôle pour un groupe d'unités à WebSphere Application Server en éditant le fichier de configuration `admin-authz.xml`.

Procédure

1. Sur le système d'exploitation Windows, modifiez le fichier *<WAS_HOME>*`/profiles/KLMProfile/cofig/cells/SKLMCell/admin-authz.xml` en ajoutant les lignes suivantes :

   ```
   <roles xmi:id=<ID_rôle> roleName=<nom_groupe_unités>/>
   <authorizations xmi:id=<ID_affectation_rôle> role=<ID_rôle/>
   ```

   Les valeurs pour `ID_rôle` et `ID_affectation_rôle` doivent être uniques dans les rôles et les autorisations existant dans le fichier `admin-authz.xml`.

   Par exemple, vous devez ajouter les lignes suivantes si un nouveau groupe d'unités `MonDS5K` est ajouté :

   ```
   <roles xmi:id="rôle_MonDS5K" roleName="MonDS5K"/>
   <authorizations xmi:id="Aut_rôle_MonDS5K" role="rôle_MonDS5K"/>
   ```

2. Redémarrez WebSphere Application Server. Vous devez arrêter le serveur puis le redémarrer. Pour des instructions sur la façon d'arrêter et de démarrer le serveur, voir «Serveur IBM Security Key Lifecycle Manager - Redémarrage», à la page 211.

Que faire ensuite

Vous pouvez ensuite spécifier quel groupe d'utilisateurs a accès au nouveau groupe d'unités et quelles tâches d'administration il peut exécuter (par exemple, les actions de consultation et de configuration).

Administration de la base de données

Le processus d'installation fournit un ID utilisateur d'administrateur par défaut, avec les droits et le mot de passe nécessaires.

Vous devez veiller à ce que l'ID utilisateur demeure actif et soit en conformité avec la politique de sécurité en vigueur sur le système.

Déplacement des journaux de transactions de Db2 pour conserver de bonnes performances

Périodiquement, les journaux de transactions Db2 créés par la base de données de IBM Security Key Lifecycle Manager doivent être transférés ailleurs. Trop nombreux, ils risqueraient d'affecter les performances du système.

Pourquoi et quand exécuter cette tâche

Les journaux de transactions de Db2 se trouvent dans les répertoires suivants :

Systèmes Windows :

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

où :

- *INSTANCEHOME* est la lettre de lecteur que vous avez spécifiée lors de l'installation.
- sklmdb31 est le propriétaire de l'instance de base de données.
- sklmdb31 est le nom de la base de données IBM Security Key Lifecycle Manager.
- NODE0000, LOGSTREAM0000 et C0000000 peuvent être des répertoires différents sur votre système.

Systèmes tels que Linux ou AIX :

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

où :

- sklmdb31 est le propriétaire de l'instance de base de données.
- sklmdb31 est le nom de la base de données IBM Security Key Lifecycle Manager.
- NODE0000, LOGSTREAM0000 et C0000000 peuvent être des répertoires différents sur votre système.

Si IBM Security Key Lifecycle Manager gère un grand nombre de clés et si la partition de disque contenant le répertoire sklmdbarchive a peu d'espace libre, transférez les anciens journaux de transactions sur une autre partition de disque.

Remarque : En exécutant cette tâche, veillez à ne pas déplacer le journal actuellement actif.

Effectuez ces étapes périodiquement :

Procédure

1. Créez une copie de sauvegarde d'IBM Security Key Lifecycle Manager à l'aide de l'interface graphique, l'interface de ligne de commande ou l'interface REST. La prochaine sauvegarde risquerait sinon d'échouer.
2. Connectez-vous en tant que propriétaire de l'instance de base de données sur un système tel que Linux ou AIX ou en tant qu'administrateur Db2 sur un système Windows.
3. Créez un répertoire sur une autre partition ayant suffisamment d'espace libre pour accueillir les anciens fichiers journaux.
4. Identifiez le premier journal actif. Entrez :

Systèmes Windows :

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

Systèmes tels que Linux ou AIX :

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

La valeur du paramètre de configuration `Premier fichier journal actif` identifie le premier journal actif.

5. Transférez, du répertoire `sklmdbarchive` vers le nouveau répertoire, les fichiers journaux dont la date de dernière modification est antérieure à celle du premier journal actif.

   Les journaux portent des noms de la forme S*nnnnnnn*`.LOG`. Généralement, plus ils ont un petit numéro, plus ils sont anciens. Il se peut toutefois que la base de données ait déjà créé un journal nommé `S99999999.LOG`. Dans ce cas, la numérotation reprend à `S0000000.LOG`.

   Remarque : L'exécution d'une opération de restauration supprime le répertoire `sklmdbarchive` et crée un nouveau répertoire.

Problèmes liés à la sécurité des mots de passe Db2 sous Windows

Sous Windows, le mot de passe et l'ID utilisateur de l'administrateur Db2 sont soumis à la stratégie de sécurité activée sur le système.

Si une règle d'expiration des mots de passe est en vigueur, vous devez changer le mot de passe de connexion et le mot de passe Db2 de l'ID utilisateur de l'administrateur avant la date d'expiration.

En outre, le mot de passe de connexion de l'ID utilisateur de l'administrateur Db2 et le mot de passe de la source de données Db2 qui est utilisé par WebSphere Application Server doivent être identiques. Si vous modifiez l'un, vous devez faire de même pour l'autre.

Exécutez les étapes suivantes pour modifier le mot de passe de la base de données Db2.

1. Arrêtez WebSphere Application Server et *tous* les services Windows liés à Db2.
2. Sous Windows, ouvrez l'outil de gestion des utilisateurs. Pour ce faire, accédez au panneau de configuration et choisissez **Outils d'administration** > **Gestion de l'ordinateur** > **Utilisateurs et groupes locaux** > **Utilisateurs**.
3. Changez le mot de passe du propriétaire de la base de données de IBM Security Key Lifecycle Manager.
4. Ouvrez la console de services Windows en accédant au panneau de configuration et en choisissant **Outils d'administration > Gestion de l'ordinateur**.
5. Modifiez le mot de passe de tous les services suivants en utilisant l'onglet **Connexion** de la boîte de dialogue **Propriétés** :
   - DB2 - `DB2SKLMV301` - *sklminstance*

     Par exemple, avec le nom d'instance par défaut, la valeur de *instance_sklm* est :

     `DB2 - DBSKLMV301 - SKLMDB31`

Une fois les mots de passe changés pour tous les services, redémarrez les services.

Les services suivants doivent être arrêtés puis redémarrés. La modification du mot de passe n'est pas obligatoire :

- Db2 License Server (DBSKLMV31)
- Db2 Management Service (DBSKLMV31)
- Db2 Governor (DBSKLMV31)
- DB Remote Command Server (DBSKLMV31)

6. Démarrez WebSphere Application Server.
7. A l'aide de l'interface **wsadmin** intégrée à WebSphere Application Server, entrez la syntaxe Jython suivante :

   Windows

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

   Linux

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

8. Utilisez la commande **wsadmin** pour changer le mot de passe de la source de données WebSphere Application Server :
   a. La commande suivante fournit la liste des entrées JAASAuthData :

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

      Le résultat obtenu peut être similaire au suivant :

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

   b. Déterminez l'ID de source de données avec un alias correspondant à la chaîne sklm_db. Déterminez également l'ID de source de données avec l'alias correspondant à la chaîne sklmdb :

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

      Par exemple, entrez sur une seule ligne :

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

      Le résultat est :

      ```
      sklm_db
      ```

   c. Changez le mot de passe de l'alias sklm_db en entrant la commande suivante sur une seule ligne :

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

      Si le mot de passe contient des caractères spéciaux, délimitez-le avec des guillemets.

      Par exemple, entrez sur une seule ligne :

      ```
      print AdminConfig.modify
      ('(cells/SKLMCell|security.xml#JAASAuthData_1379859888963)','[[password passw0rd]]')
      ```

   d. Enregistrez les modifications :

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

   e. Arrêtez et redémarrez le serveur IBM Security Key Lifecycle Manager à l'aide des commandes **stopServer** et **startServer**.

      Vous pouvez également arrêter et démarrer le serveur IBM Security Key Lifecycle Manager en utilisant l'outil Gestion de l'ordinateur de Windows.

      1) Ouvrez le panneau de configuration et cliquez sur **Outils d'administration** > **Gestion de l'ordinateur** > **Services et applications** > **Services**.

2) Redémarrez le service serveur IBM Security Key Lifecycle Manager, qui a un nom similaire à `IBM WebSphere Application Server V9.0 - SKLM301Server`.

f. Vérifiez que vous pouvez vous connecter à la base de données en utilisant la source de données WebSphere Application Server.

1) Entrez d'abord :

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

Le résultat obtenu peut être similaire au suivant :

```
"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) Testez la connexion sur la première source de données. Par exemple, entrez :

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

Par exemple, entrez sur une seule ligne :

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

3) Testez la connexion sur la source de données restante. Par exemple, entrez :

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

4) Dans les deux cas, vous devez recevoir un message indiquant que la connexion à la source de données a réussi. Exemple :

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

A présent, vous devez être en mesure d'effectuer une opération IBM Security Key Lifecycle Manager.

Problèmes liés à la sécurité des mots de passe Db2 sur les systèmes Linux ou AIX

Sur les systèmes Linux ou AIX, vous pouvez modifier le mot de passe de l'ID utilisateur de l'administrateur Db2. En outre, le mot de passe de connexion de l'ID utilisateur de l'administrateur Db2 et le mot de passe Db2 de l'ID utilisateur doivent être identiques.

Le programme d'installation d'IBM Security Key Lifecycle Manager installe Db2 et invite la personne qui effectue l'installation à entrer le mot de passe de l'utilisateur nommé `sklmdb31`. En outre, l'application Db2 crée une entrée utilisateur du système d'exploitation nommée `sklmdb31`. Ainsi, lorsque le mot de passe de cet utilisateur arrive à expiration, vous devez resynchroniser le mot de passe de ces deux ID utilisateur.

Avant de modifier le mot de passe de l'ID utilisateur de l'administrateur Db2, vous devez au préalable modifier le mot de passe de l'utilisateur au niveau du système d'exploitation.

1. Connectez-vous au serveur IBM Security Key Lifecycle Manager en tant que superutilisateur.

2. Changez d'utilisateur pour utiliser l'entrée utilisateur système sklmdb31. Entrez :

   ```
   su sklmdb31
   ```

3. Changez le mot de passe. Entrez :

   ```
   passwd
   ```

   Spécifiez le nouveau mot de passe.

4. Reprenez l'ID superutilisateur.

   ```
   exit
   ```

5. Dans le répertoire *WAS_HOMEWAS*/bin, utilisez l'interface **wsadmin** fournie par WebSphere Application Server pour spécifier la syntaxe Jython.

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

6. Changez le mot de passe de la source de données WebSphere Application Server :

   a. La commande suivante répertorie les entrées JAASAuthData :

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

      Le résultat obtenu devrait ressembler à l'exemple suivant :

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

   b. Entrez la commande **AdminConfig.showall** pour chaque entrée afin de localiser l'alias sklm_db. Par exemple, entrez sur une seule ligne :

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

      Le résultat obtenu devrait ressembler à l'exemple suivant :

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

      Entrez également sur une seule ligne :

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

      Le résultat obtenu devrait ressembler à l'exemple suivant :

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

   c. Changez le mot de passe de l'alias sklm_db dont l'identificateur est JAASAuthData_**1228871756187** :

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

      Par exemple, entrez sur une seule ligne :

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

   d. Changez le mot de passe de l'alias sklmdb dont l'identificateur est JAASAuthData_**1228871757843** :

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

      Par exemple, entrez sur une seule ligne :

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

   e. Enregistrez les modifications :

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

f. Reprenez l'ID superutilisateur.

```
exit
```

g. Dans le répertoire *WAS_HOMEWAS*/bin, arrêtez l'application WebSphere Application Server. Par exemple, en tant que WASAdmin, entrez sur une seule ligne :

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

Le résultat obtenu devrait ressembler à l'exemple suivant :

```
ADMU0116I: Les informations sur les outils sont journalisées dans le fichier
//opt/IBM/WebSphere/AppServer/profiles/KLMProfile/logs/server1/stopServer.log
ADMU0128I : Démarrage de l'outil à l'aide du profil WASProfile
ADMU3100I: Lecture de la configuration du serveur : server1
ADMU3201I: Une demande d'arrêt du serveur a été émise. Attente de l'état d'arrêt.
ADMU4000I: Le serveur server1 est arrêté.
```

h. Démarrez l'application WebSphere Application Server. En tant qu'administrateur WebSphere Application Server, entrez sur une seule ligne :

```
startServer.sh server1
```

i. Dans le répertoire *WAS_HOMEWAS*/bin, utilisez l'interface **wsadmin** fournie par WebSphere Application Server pour spécifier la syntaxe Jython.

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

j. Vérifiez que vous pouvez vous connecter à la base de données en utilisant la source de données WebSphere Application Server.

1) Recherchez d'abord une liste de source de données. Entrez :

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

Le résultat obtenu devrait ressembler à l'exemple suivant :

```
"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) Entrez :

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

Par exemple, entrez sur une seule ligne :

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

3) Testez la connexion sur la source de données restante. Par exemple, entrez :

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

4) Dans les deux cas, vous devez recevoir un message indiquant que la connexion à la source de données a réussi. Par exemple :

```
WASX7217I: La connexion à la source de données indiquée a abouti.
```

Arrêt du serveur Db2

Pour arrêter le serveur de base de données, arrêtez d'abord le WebSphere Application Server. Après quoi, vous pouvez arrêter le serveur Db2.

Pourquoi et quand exécuter cette tâche

Vous devez être le propriétaire de l'instance de base de données sur un système Linux ou AIX ou l'administrateur local sur un système Windows.

Procédure

1. Connectez-vous en tant que propriétaire de l'instance de base de données sur un système tel que Linux ou AIX ou en tant qu'administrateur local sur un système Windows.
2. Arrêtez le serveur WebSphere Application Server. Tapez cette commande :

   Systèmes Windows

   ```
   cd C:\Program Files\IBM\WebSphere\AppServer\bin
   .\stopServer.bat serveur1 -username admin_was -password monmdpsecret
   ```

   Systèmes AIX ou Linux

   ```
   /opt/IBM/WebSphere/AppServer/bin/stopServer.sh serveur1 -username admin_was
    -password mysecretpwd
   ```

3. Arrêtez le serveur Db2. Entrez les commandes suivantes :

   Systèmes Windows

   ```
   set DB2INSTANCE=sklmdb31
   db2stop
   ```

   Systèmes AIX ou Linux

   ```
   su - sklmdb31
   db2stop
   ```

Changement du nom d'hôte du serveur Db2

Après avoir modifié le nom d'hôte d'IBM Security Key Lifecycle Manager, vous pouvez également changer le nom d'hôte du serveur Db2.

Pourquoi et quand exécuter cette tâche

Vous pouvez obtenir la liste des étapes actuelles pour changer le nom d'hôte pour votre niveau du serveur Db2 dans la note technique disponible à cette adresse 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

Changement du nom d'hôte d'un serveur WebSphere Application Server existant

Vous devez modifier le nom d'hôte de WebSphere Application Server avant de modifier le nom d'hôte du système.

Procédure

1. Changez le nom d'hôte de WebSphere Application Server. Pour plus d'informations sur la façon de changer le nom d'hôte, voir la documentation d'IBM WebSphere Application Server (http://www.ibm.com/support/knowledgecenter/SSEQTP_9.0.0/com.ibm.websphere.base.doc/ae/tagt_hostname.html).
2. Une fois cette tâche accomplie, changez le nom d'hôte du serveur DB2. Pour plus d'informations, voir «Changement du nom d'hôte du serveur Db2».

Gestion d'unité de bande LTO

Vous pouvez gérer des unités de bande LTO à l'aide d'IBM Security Key Lifecycle Manager.

Etapes guidées pour la création de groupes de clés et d'unités

Lorsque vous créez des groupes de clés et des unités, puis que vous ajoutez d'autres groupes de clés et unités ultérieurement, IBM Security Key Lifecycle Manager fournit un ensemble d'étapes détaillées permettant d'effectuer la tâche.

La description de certaines étapes mentionne parfois la possibilité d'accomplir la même tâche en utilisant l'interface de ligne de commande et l'interface REST. Dans un ensemble de tâches détaillées, utilisez l'interface utilisateur graphique pour effectuer les tâches.

Création d'un groupe de clés

Créez en premier lieu des clés et des groupes de clés pour IBM Security Key Lifecycle Manager. Avant de commencer, déterminez le nombre de clés, ainsi que l'usage des groupes de clés individuels requis par votre organisation.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser la boîte de dialogue Créer un groupe de clés. Vous pouvez également utiliser la commande **tklmGroupCreate** ou **Service REST Group Create** pour créer un groupe auquel vous prévoyez d'ajouter des clés. Utilisez ensuite la commande **tklmSecretKeyCreate** ou **Service REST Secret Key Create** pour créer une ou plusieurs clés symétriques dans le groupe existant. Votre rôle doit avoir un droit d'utilisation de l'action de création, ainsi qu'un droit d'accès au groupe d'unités approprié.

Procédure

1. Accédez à la page ou au répertoire approprié(e) :
   - Interface graphique :
     a. Connectez-vous à l'interface graphique.
     b. Dans la section Gestion des clés et des unités de la page de bienvenue, sélectionnez **Unité LTO**.
     c. Cliquez sur **Aller à** > **Création de clés et d'unités en mode guidé**.
     d. Vous pouvez aussi cliquer avec le bouton droit sur **LTO** et sélectionner **Création de clés et d'unités en mode guidé**.
   - Interface de ligne de commande
     a. Accédez au répertoire *<WAS_HOME>*/bin. Exemple :

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

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

     b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme SKLMAdmin. Exemple :

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

Linux

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

- Interface REST :
  - Ouvrez un client REST.

2. Créez un groupe de clés :
   - Interface graphique :
     a. Sur la page Etape 1 : Créer des groupes de clés, cliquez sur **Créer** dans la table **Groupe de clés**.
     b. Dans la boîte de dialogue Créer un groupe de clés, indiquez des valeurs pour les paramètres obligatoires et facultatifs. Vous pouvez par exemple créer un groupe de clés contenant 100 clés.
     c. Cliquez sur **Créer un groupe de clés**.
   - Interface de ligne de commande :
     a. D'abord, créez un groupe auquel ajouter des clés.

        Entrez la commande `tklmGroupCreate` pour créer un groupe. Par exemple, entrez :

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

     b. Utilisez ensuite la commande **`tklmGroupList`** pour obtenir la valeur de l'identificateur unique universel (UUID) du groupe que vous avez créé. Par exemple, entrez :

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

     c. Ensuite, créez un groupe de clés et stockez les clés dans le groupe. Par exemple, entrez :

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

   - Interface REST :
     a. Obtenez un identificateur d'authentification utilisateur unique pour accéder aux services REST d'IBM Security Key Lifecycle Manager. Pour plus d'informations sur le processus d'authentification, voir Processus d'authentification pour les services REST.
     b. Pour exécuter le **`service REST Group Create`**, envoyez la demande HTTP POST. Transmettez l'identificateur d'authentification utilisateur que vous avez obtenu à l'`étape a` avec le message de demande, conformément à l'exemple suivant :

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

     c. Utilisez le **`service REST Group List`** pour obtenir la valeur de l'identificateur unique universel (UUID) du groupe que vous avez créé. Exemple :

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

d. Créez ensuite des clés et stockez-les dans un groupe à l'aide du **service REST Secret Key Create**. Par exemple, vous pouvez envoyer la demande HTTP suivante :

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

Que faire ensuite

Faites une sauvegarde des nouvelles clés avant qu'elles ne commencent à être servies aux unités. Vous pouvez passer à l'étape guidée suivante pour définir des unités spécifiques et leur associer des groupes de clés. Sélectionnez **Etape 2 : Identifier les unités** ou cliquez sur **Passer à l'étape suivante**.

Identification des unités

Identifiez une unité de bande LTO à utiliser avec IBM Security Key Lifecycle Manager. Avant de commencer, créez le groupe de clés à associer aux lecteurs de bande que vous identifiez.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser la boîte de dialogue Ajouter un lecteur de bande, la commande **tklmDeviceAdd** ou **Service REST Device Add** pour ajouter une unité. Votre rôle doit avoir un droit d'utilisation de l'action de création, ainsi qu'un droit d'accès au groupe d'unités approprié.

Vous pouvez effectuer les choix suivants pour fournir des clés à des unités :

Accepter uniquement les unités ajoutées manuellement pour la communication
Les unités entrantes ne sont pas systématiquement ajoutées au magasin de données. Vous devez spécifier manuellement, pour chaque unité, si des clés lui seront servies ou non.

Retenir les demandes des nouvelles unités en attente de mon approbation
Toutes les unités entrantes d'un groupe d'unités valide sont ajoutées au magasin de données, mais lorsqu'elles demandent des clés, celles-ci ne leur sont pas servies automatiquement. Vous devez accepter ou rejeter chaque unité dans la liste des unités en attente, en fonction de quoi des clés lui sont servies ou non lorsqu'elle en fait la demande.

Accepter automatiquement toutes les demandes des nouvelles unités pour la communication
Toutes les nouvelles unités entrantes d'un groupe d'unités valide sont ajoutées au magasin de données et, lorsqu'elles demandent des clés, celles-ci leur sont servies automatiquement.

Remarque : N'utilisez pas cette option si vous comptez déplacer la nouvelle unité vers un autre groupe d'unités. Sélectionnez plutôt le mode d'approbation manuel ou avec mise en attente pour que l'occasion vous soit donnée de transférer l'unité dans le groupe approprié avant que des clés ne lui soient servies.

Chacune de ces options est acceptable à condition qu'il n'y ait pas de groupe d'unités défini. Car si des groupes d'unités sont définis :

Déterminez si IBM Security Key Lifecycle Manager devra accepter automatiquement les demandes de toutes les unités. Pour garantir une sécurité optimale, une fois toutes les unités reconnues, vous pouvez désactiver cette option dans l'environnement de production.

Procédure

1. Accédez à la page ou au répertoire approprié :
   - Interface graphique :
     a. Connectez-vous à l'interface graphique.
     b. Dans la section Gestion des clés et des unités de la page de bienvenue, sélectionnez **Unité LTO**.
     c. Cliquez sur **Aller à** > **Création de clés et d'unités en mode guidé**.
     d. Vous pouvez aussi cliquer avec le bouton droit sur **LTO** et sélectionner **Création de clés et d'unités en mode guidé**.
   - Interface de ligne de commande
     a. Accédez au répertoire <*WAS_HOME*>/bin. Exemple :

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

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

     b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme SKLMAdmin. Exemple :

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

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

   - Interface REST :
     – Ouvrez un client REST.
2. Ignorez la page Créer des groupes de clés. Cliquez sur **Passer à l'étape suivante** ou sur **Etape 2 : Identifier les unités**.
3. Vous pouvez demander qu'IBM Security Key Lifecycle Manager mette en attente les demandes des nouvelles unités afin que vous puissiez ensuite les accepter ou les rejeter.
   - Interface graphique :

     Sélectionnez **Retenir les demandes des nouvelles unités en attente de mon approbation**.
   - Interface de ligne de commande :

     Utilisez la commande **tklmDeviceGroupAttributeUpdate** ou le **service REST Device Group Attribute Update** pour définir la valeur de l'attribut **device.AutoPendingAutoDiscovery**. Par exemple, entrez :
     ```
     print AdminTask.tklmDeviceGroupAttributeUpdate ('[-name LTO
       -attributes "{device.AutoPendingAutoDiscovery 2}"]')
     ```
     Pour un groupe d'unités LTO, utilisez la commande **tklmDeviceGroupAttributeUpdate** afin de spécifier un groupe de clés à l'aide de l'attribut **symmetricKeySet** dans la base de données d'IBM Security Key Lifecycle Manager.
   - Interface REST :
     a. Obtenez un identificateur d'authentification utilisateur unique pour accéder aux services REST d'IBM Security Key Lifecycle Manager. Pour

plus d'informations sur le processus d'authentification, voir Processus d'authentification pour les services REST.

b. Pour exécuter le **service REST Device Group Attribute Update** et définir la valeur de l'attribut **device.AutoPendingAutoDiscovery**, envoyez la demande HTTP PUT. Transmettez l'identificateur d'authentification utilisateur que vous avez obtenu à l'étape a avec le message de demande, conformément à l'exemple suivant :

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

4. Ajoutez une unité :
   - Interface graphique :
     a. Sur la page Etape 2 : Identifier les unités, dans la table **Unités**, cliquez sur **Ajouter**.
     b. Entrez les informations obligatoires et facultatives dans la boîte de dialogue Ajouter un lecteur de bande.
     c. Cliquez sur **Ajouter un lecteur de bande**.
   - Interface de ligne de commande :

     Entrez `tklmDeviceAdd` pour ajouter une unité. Vous devez indiquer le groupe d'unités et le numéro de série. Par exemple, entrez :

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

   - Interface REST :

     Vous pouvez utiliser le **service REST Device Add** pour ajouter une unité. Par exemple, vous pouvez envoyer la demande HTTP suivante :

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

Que faire ensuite

Ensuite, vous pouvez utiliser la page Gestion des clés et des unités LTO pour afficher tous les groupes de clés et toutes les unités.

Gestion de clés, de groupes de clés et d'unités

Pour administrer des clés, des groupes de clés et des unités, vous établissez le lien entre groupes de clés et unités. Vous pouvez ajouter, modifier ou supprimer des clés, des groupes de clés ou des unités spécifiques.

Pourquoi et quand exécuter cette tâche

Utilisez la page Gestion des clés et des unités LTO pour mapper des groupes de clés à des unités. Vous pouvez ajouter, modifier ou supprimer des clés, des groupes de clés ou des unités spécifiques. Votre rôle doit avoir un droit d'utilisation de l'action de visualisation, ainsi qu'un droit d'accès au groupe d'unités approprié.

Pour modifier l'affichage des informations, sélectionnez :

Afficher les groupes de clés et les unités
Affichez les noms des groupes de clés et les numéros de série des unités. Cette vue indique également le groupe de clés, la clé ou la valeur système par défaut utilisés par une unité.

Afficher les clés, l'appartenance au groupe de clés et les unités
Affichez les clés et l'appartenance aux groupes de clés. En outre, cette vue indique les numéros de série des unités, ainsi que le groupe de clés, la clé ou la valeur système par défaut utilisé par une unité.

Avant de commencer, examinez les colonnes de la page, qui comprend des boutons permettant d'ajouter, de modifier ou de supprimer un élément de la table. Pour trier les informations, cliquez sur un en-tête de colonne.

La table se présente comme suit :

- Dans les colonnes de gauche, informations sur les clés ou les groupes de clés.

  Dans le cas d'une clé, ces informations indiquent le groupe de clés auquel appartient la clé. Dans le cas d'un groupe de clés, ces informations indiquent si le groupe de clés est utilisé par défaut, ainsi que le nombre de clés qu'il contient.
- Dans les colonnes de droite, informations sur les unités.

  Ces informations indiquent, pour chaque unité, son numéro de série et le groupe de clés ou la clé spécifique qu'elle utilise. Par exemple, une unité peut utiliser le groupe de clés par défaut du système.
- Icônes indiquant le type des clés.

Tableau 2. Icônes et signification

Icône	Description
	Une clé symétrique ou une clé privée. Une clé privée est une clé asymétrique figurant dans une paire de clés contenant une clé publique et une clé privée.
	Un groupe de clés

Procédure

1. Connectez-vous à l'interface graphique :
   a. Dans la section Gestion des clés et des unités de la page de bienvenue, sélectionnez **Unité LTO**.
   b. Cliquez sur **Aller à** > **Gestion des clés et des unités**.
   c. Vous pouvez aussi cliquer avec le bouton droit sur **LTO** et sélectionner **Gestion des clés et des unités**.

   Les descriptions de certaines étapes proposent d'utiliser l'interface graphique, l'interface de ligne de commande ou l'interface REST. Veillez à ne pas changer d'interface au cours d'une même session de travail.

   Les descriptions de certaines tâches peuvent mentionner des propriétés contenues dans le fichier `SKLMConfig.properties`. Utilisez l'interface graphique, l'interface de ligne de commande ou l'interface REST pour modifier ces propriétés.
2. Sur la page Gestion des clés et des unités LTO, vous pouvez ajouter, modifier ou supprimer une clé, un groupe de clés ou une unité.

   Vous pouvez effectuer les tâches administratives suivantes :

- Actualiser la liste

  Cliquez sur l'icône de régénération  pour actualiser les éléments de la table.

- Ajouter

  Cliquez sur **Ajouter**. Vous pouvez également sélectionner une procédure pas à pas pour créer des groupes de clés et des unités.

  – Groupe de clés

    Dans la boîte de dialogue **Créer un groupe de clés**, indiquez les informations requises telles que le nom du groupe de clés. Vous pouvez aussi spécifier que ce groupe sert des clés en tant que groupe de clés par défaut. Il n'existe qu'un seul groupe de clés par défaut. Cliquez ensuite sur **Créer un groupe de clés**. Votre rôle doit avoir un droit d'utilisation de l'action de création, ainsi qu'un droit d'accès au groupe d'unités approprié.

  – Lecteur de bande

    Dans la boîte de dialogue Ajouter un lecteur de bande, entrez le numéro de série de l'unité et d'autres informations. Cliquez ensuite sur **Ajouter un lecteur de bande**. Votre rôle doit avoir un droit d'utilisation de l'action de création, ainsi qu'un droit d'accès au groupe d'unités approprié.

  – Utilisez la procédure pas à pas pour créer des groupes de clés, des clés et des unités.

    Entrez les informations nécessaires dans les pages Etape 1 : Créer des groupes de clés et Etape 2 : Identifier les unités, puis cliquez sur le bouton approprié pour terminer la tâche.

  L'indication de réussite varie, montrant l'objet (groupe de clés ou unité) qui vient d'être créé.

- Modifier

  Pour modifier un groupe de clés, une clé ou une unité, sélectionnez l'élément souhaité, puis cliquez sur **Modifier**. Vous pouvez également cliquer avec le bouton droit de la souris sur le groupe de clés, la clé ou l'unité sélectionnée, Cliquez ensuite sur **Modifier**.

  – Groupe de clés

    Apportez des modifications dans la boîte de dialogue Modifier un groupe de clés. Cliquez ensuite sur **Modifier un groupe de clés**. Votre rôle doit avoir un droit d'utilisation de l'action de modification, ainsi qu'un droit d'accès au groupe d'unités approprié.

  – Clé

    Apportez des modifications dans la boîte de dialogue Modifier l'appartenance de la clé. Cliquez ensuite sur **Modifier l'appartenance de la clé**. Votre rôle doit avoir un droit d'utilisation de l'action de modification, ainsi qu'un droit d'accès au groupe d'unités approprié.

  – Lecteur de bande

    Apportez des modifications dans la boîte de dialogue Modifier un lecteur de bande. Cliquez ensuite sur **Modifier un lecteur de bande**. Votre rôle doit avoir un droit d'utilisation de l'action de modification, ainsi qu'un droit d'accès au groupe d'unités approprié.

  L'indication de réussite varie, reflétant le changement dans la colonne dédiée au groupe de clés, à la clé ou à l'unité. Il se peut que les modifications apportées aux informations facultatives, telles que la valeur de la description d'une unité, ne figurent pas dans la table.

- Supprimer

Pour supprimer un groupe de clés, une clé ou une unité, sélectionnez l'élément souhaité, puis cliquez sur **Supprimer**. Vous pouvez également cliquer avec le bouton droit de la souris sur le groupe de clés, la clé ou l'unité sélectionnée, Cliquez ensuite sur **Supprimer**.

– Groupe de clés

  Il n'est pas possible de supprimer un groupe de clés associé à une unité ou un groupe de clés marqué comme élément par défaut. La suppression d'un groupe de clés entraîne *la suppression de toutes les clés* contenues dans le groupe.

  Pour confirmer la suppression, cliquez sur **OK**. Votre rôle doit avoir un droit d'utilisation de l'action de suppression, ainsi qu'un droit d'accès au groupe d'unités approprié.

– Clé

  Si vous supprimez une clé, elle est supprimée de tous les groupes de clés auxquels elle est associée. Pour confirmer la suppression, cliquez sur **OK**. Vous ne pouvez pas supprimer une clé associée à une unité. Votre rôle doit avoir un droit d'utilisation de l'action de suppression, ainsi qu'un droit d'accès au groupe d'unités approprié.

– Lecteur de bande

  Les métadonnées relatives à l'unité que vous supprimez, telles que son numéro de série, sont supprimées de la base de données IBM Security Key Lifecycle Manager. Pour confirmer la suppression, cliquez sur **OK**. Votre rôle doit avoir un droit d'utilisation de l'action de suppression, ainsi qu'un droit d'accès au groupe d'unités approprié.

La réussite de l'opération est reflétée par la suppression du groupe de clés, de la clé ou de l'unité dans la table de gestion.

Ajout d'une clé ou d'un groupe de clés

Vous pouvez ajouter des clés ou des groupes de clés supplémentaires à utiliser avec IBM Security Key Lifecycle Manager. Avant de commencer, déterminez la stratégie de votre site concernant les groupes de clés par défaut et la définition des préfixes de clés.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser la boîte de dialogue Créer un groupe de clés. Vous pouvez également utiliser la commande **tklmGroupCreate** ou **Service REST Group Create** pour créer un groupe auquel ajouter des clés, puis utiliser la commande **tklmSecretKeyCreate** ou **Service REST Secret Key Create** pour créer une ou plusieurs clés symétriques dans le groupe existant. Votre rôle doit avoir un droit d'utilisation de l'action de création, ainsi qu'un droit d'accès au groupe d'unités approprié.

Procédure

1. Accédez à la page ou au répertoire approprié(e) :
   - Interface graphique :
     a. Connectez-vous à l'interface graphique.
     b. Dans la section Gestion des clés et des unités de la page de bienvenue, sélectionnez **Unité LTO**.
     c. Cliquez sur **Aller à** > **Gestion des clés et des unités**.
     d. Vous pouvez aussi cliquer avec le bouton droit sur **LTO** et sélectionner **Gestion des clés et des unités**.

e. Sur la page de gestion pour LTO, cliquez sur **Ajouter**.

f. Cliquez sur **Groupe de clés**.

- Interface de ligne de commande

a. Accédez au répertoire <*WAS_HOME*>/bin. Exemple :

Windows

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

Linux

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

b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme SKLMAdmin. Exemple :

Windows

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

Linux

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

2. Créez une clé ou un groupe de clés :

- Interface graphique

a. Dans la boîte de dialogue Créer un groupe de clés, indiquez des valeurs pour les paramètres obligatoires et facultatifs. Vous pouvez, par exemple, indiquer qu'il s'agit du groupe de clés par défaut.

b. Cliquez sur **Créer un groupe de clés**.

- Interface de ligne de commande :

a. Vous devez d'abord créer un groupe dans lequel vous pouvez ajouter des clés.

Entrez la commande **tklmGroupCreate** pour créer un groupe de type groupe de clés. Par exemple, entrez :

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

b. Utilisez ensuite la commande **tklmGroupList** pour obtenir la valeur de l'identificateur unique universel (UUID) du groupe que vous avez créé. Par exemple, entrez :

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

c. Créez ensuite des clés et stockez-les dans le groupe. Par exemple, entrez :

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

- Interface REST :

a. Créez un groupe dans lequel vous pouvez ajouter des clés à l'aide de **Service REST Group Create**.

Par exemple, vous pouvez envoyer la demande HTTP suivante à l'aide d'un client REST :

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

b. Utilisez **Service REST Group List** pour obtenir la valeur de l'identificateur unique universel (UUID) du groupe que vous avez créé. Par exemple, vous pouvez envoyer la demande HTTP suivante :

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

c. Créez des clés et stockez-les dans un groupe à l'aide de **Service REST Secret Key Create**. Par exemple, vous pouvez envoyer la demande HTTP suivante :

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

Que faire ensuite

Faites une sauvegarde des nouvelles clés avant qu'elles ne commencent à être servies aux unités. Vous pouvez ensuite associer des groupes de clés à des unités spécifiques.

Spécification d'un groupe de clés de remplacement

Vous pouvez spécifier un groupe de clés à utiliser ultérieurement comme valeur par défaut du système.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser l'interface graphique, la commande **tklmKeyGroupDefaultRolloverAdd** ou **Service REST Key Group Default Rollover Add** pour ajouter un remplacement de groupe de clés par défaut, programmé à une date ultérieure pour servir des clés à un groupe d'unités. Votre rôle doit avoir un droit d'utilisation de l'action de création, ainsi qu'un droit d'accès au groupe d'unités approprié.

Procédure

1. Accédez à la page ou au répertoire approprié(e) :
   - Interface graphique :
     a. Connectez-vous à l'interface graphique.
     b. Dans la section Gestion des clés et des unités de la page de bienvenue, sélectionnez **Unité LTO**.
     c. Cliquez sur **Aller à** > **Gestion des remplacements de valeurs par défaut**.
     d. Vous pouvez aussi cliquer avec le bouton droit sur **LTO** et sélectionner **Gestion des remplacements de valeurs par défaut**.
   - Interface de ligne de commande
     a. Accédez au répertoire <*WAS_HOME*>/bin. Exemple :

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

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

     b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme SKLMAdmin. Exemple :

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

Linux

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

2. Spécifiez un groupe de clés existant, qui sera utilisé comme valeur par défaut du système à une date ultérieure.
   - Interface graphique :
     a. Sur la page de gestion pour LTO, cliquez sur **Ajouter**.
     b. Dans la boîte de dialogue Ajouter une future valeur par défaut, spécifiez les informations requises.
     c. Cliquez sur **Ajouter une future valeur par défaut**.

     Remarque :
     - Veillez à ne pas indiquer deux valeurs par défaut pour la même date de remplacement.
     - Si aucun groupe de clés n'existe à la date du remplacement, IBM Security Key Lifecycle Manager continue à utiliser le groupe de clés par défaut du moment.
     - Vous pouvez ajouter ou supprimer des entrées de la table, mais il n'est pas possible de les modifier.
   - Interface de ligne de commande :

     Ajoutez un groupe de clés de remplacement. Par exemple, entrez :

     ```
     print AdminTask.tklmKeyGroupDefaultRolloverAdd
     ('[-usage LTO -keyGroupName myLTOkeygroup
          -effectiveDate 2010-04-30]')
     ```
3. L'indication de réussite varie en fonction de l'interface :
   - Interface graphique :

     Le groupe de clés est répertorié dans la table des groupes de clés de remplacement, sur la page de gestion LTO.
   - Interface de ligne de commande :

     Un message d'achèvement indique la réussite de l'opération.
4. Pour supprimer un groupe de clés de la table des remplacements, votre rôle doit avoir le droit d'utiliser l'action de suppression.
   - Interface graphique :

     Sélectionnez un groupe de clés et cliquez sur **Supprimer**.
   - Interface de ligne de commande :

     Utilisez la commande **tklmKeyGroupDefaultRolloverList** pour afficher l'UUID d'un groupe de clés. Votre rôle doit avoir un droit d'utilisation de l'action de visualisation, ainsi qu'un droit d'accès au groupe d'unités approprié. Utilisez ensuite la commande **tklmKeyGroupDefaultRolloverDelete** pour supprimer le groupe de clés de la liste des groupes de remplacement. Votre rôle doit avoir un droit d'utilisation de l'action de suppression, ainsi qu'un droit d'accès au groupe d'unités approprié.

     Par exemple, entrez :

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

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

Interdiction de la réutilisation de clés

Vous pouvez demander que les clés d'un groupe de clés particulier soient à usage unique. Pour des raisons de sécurité, par exemple, vous pouvez interdire la réutilisation de clés ayant déjà servi.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser l'interface de ligne de commande ou l'interface REST pour définir la propriété **stopRoundRobinKeyGrps** dans le fichier `SKLMConfig.properties`. Votre rôle doit avoir un droit d'utilisation de l'action de configuration. A l'origine, cette propriété n'est pas présente dans le fichier de propriétés ; elle n'y apparaît que si vous lui attribuez explicitement la valeur `true`.

Important :

- Si vous activez cet indicateur, la mise à disposition des clés risque d'être interrompue si un groupe de clés est en cours d'utilisation et si la dernière clé de ce groupe est mise à disposition. En effet, dans cette situation, si une unité demande une clé de groupe pour écrire des données chiffrées, elle recevra un code d'erreur `0xEE34 (NO_KEY_TO_SERVE)`. Pour permettre le traitement des demandes d'écriture par mise à disposition de clés, ajoutez de nouvelles clés au groupe de clés. Vous pouvez également définir l'utilisation d'un groupe de clés différent disposant de clés disponibles. Les demandes adressées au service de clés dans le but de lire des données aboutissent toujours lorsque la clé demandée existe.
- Utilisez cette propriété dans un environnement respectant scrupuleusement la conformité aux normes gouvernementales et en conjonction avec les normes `FIPS` 140. Lorsque cette propriété est activée, vous devez surveiller activement vos groupes de clé. Assurez-vous qu'aucun d'eux n'est à court de clés, car cela entraînerait l'arrêt du service de clés par le serveur et l'échec des demandes d'écriture sur bande.
- Dès lors que vous activez cette option, ne la désactivez plus. Par exemple, si vous l'activez, un groupe de clés ne sert plus les clés ayant déjà été utilisées. Si vous la désactivez ensuite, la prochaine clé disponible dans le groupe est servie. Une fois la dernière clé du groupe servie, la prochaine à l'être est la première clé du groupe.
- Lorsque cette option est définie, n'affectez pas des alias de clé individuels appartenant à un groupe de clés à des unités.

Procédure

1. Accédez au répertoire approprié :
   a. Accédez au répertoire <*WAS_HOME*>`/bin`. Exemple :

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

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

   b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme `SKLMAdmin`. Exemple :

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

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

2. Dans un premier temps, déterminez l'état actuel de la propriété dans le fichier SKLMConfig.properties. Cette propriété ne figure pas dans le fichier de propriétés à l'origine, sauf si vous avez défini sa valeur sur true.
   - Interface de ligne de commande :

     A l'invite **wsadmin**, entrez la commande au format Jython suivante :

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

     Utilisez **Service REST Get Single Config Property** pour obtenir la valeur en cours de la propriété. Envoyez la demande HTTP suivante :

     ```
     GET https://localhost:<port>/SKLM/rest/v1/configProperties/
     stopRoundRobinKeyGrps
     Content-Type: application/json
     Accept : application/json
     Authorization: SKLMAuth userAuthId=139aeh34567m
     Accept-Language : en
     ```
3. Faites passer à true la propriété **stopRoundRobinKeyGrps** dans le fichier SKLMConfig.properties.
   - Interface de ligne de commande :

     Entrez la commande au format Jython suivante :

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

     Envoyez la demande HTTP suivante :

     ```
     PUT https://localhost:<port>/SKLM/rest/v1/configProperties
     Content-Type: application/json
     Accept : application/json
     Authorization: SKLMAuth authId=139aeh34567m
     Accept-Language: en
     { "stopRoundRobinKeyGrps": "true"}
     ```
4. Pour vérifier si l'opération a réussi, entrez de nouveau la commande **tklmConfigGetEntry** ou utilisez **Service REST Get Single Config Property**.

   Il est possible qu'un avertissement apparaisse dans la section Actions de la page Bienvenue de l'interface graphique. Cette section répertorie les groupes de clés comportant 10 % ou moins de clés disponibles. Cliquez deux fois sur une entrée de cette table pour accéder à la boîte de dialogue Modifier un groupe de clés, dans laquelle vous pouvez ajouter des clés supplémentaires que le groupe peut utiliser.

   Il n'existe aucun autre avertissement. La table signalant un nombre de clés faible s'applique à tous les groupes de clés, y compris le groupe de clés spécifié par défaut.

Modification d'un groupe de clés

Vous pouvez modifier les informations relatives aux objets d'un groupe de clés dans la base de données d'IBM Security Key Lifecycle Manager. Avant de commencer, déterminez les changements à apporter au groupe, par exemple le nombre de clés supplémentaires à ajouter.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser la boîte de dialogue Modifier un groupe de clés. Vous pouvez également utiliser les commandes ou interfaces REST suivantes pour modifier des objets dans un groupe de clés dans la base de données d'IBM Security Key Lifecycle Manager.

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

Votre rôle doit avoir un droit d'utilisation de l'action de modification, ainsi qu'un droit d'accès au groupe d'unités approprié.

Procédure

1. Accédez à la page ou au répertoire approprié(e) :
   - Interface graphique :
     a. Connectez-vous à l'interface graphique.
     b. Dans la section Gestion des clés et des unités de la page de bienvenue, sélectionnez **Unité LTO**.
     c. Cliquez sur **Aller à** > **Gestion des clés et des unités**.
     d. Vous pouvez aussi cliquer avec le bouton droit sur **LTO** et sélectionner **Gestion des clés et des unités**.
     e. Sur la page de gestion pour LTO, sélectionnez un groupe de clés dans la colonne **Groupe de clés**.
     f. Cliquez sur **Modifier**.
     g. Vous pouvez également faire un clic droit sur un groupe de clés et sélectionner **Modifier**, ou bien faire un double clic sur une entrée de groupe de clés.
   - Interface de ligne de commande
     a. Accédez au répertoire *<WAS_HOME>*/bin. Exemple :

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

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

     b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme SKLMAdmin. Exemple :

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

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

2. Modifiez les informations relatives au groupe de clés :
   - Interface graphique :
     a. Dans la boîte de dialogue Modifier un groupe de clés, modifiez les champs appropriés. Votre rôle doit vous autoriser à utiliser l'action voulue. Par exemple, pour supprimer une clé du groupe, votre rôle doit avoir un droit d'utilisation de l'action de suppression, ainsi qu'un droit d'accès au groupe d'unités approprié.
     b. Cliquez sur **Modifier un groupe de clés**.
   - Interface de ligne de commande :

     Vous pouvez ajouter ou supprimer un objet d'un groupe.
     – Supprimez une clé du groupe. Votre rôle doit avoir un droit d'utilisation de l'action de suppression, ainsi qu'un droit d'accès au groupe d'unités approprié. Par exemple, entrez :

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

– Rajoutez la même clé dans le groupe. Votre rôle doit avoir un droit d'utilisation de l'action de modification, ainsi qu'un droit d'accès au groupe d'unités approprié. Par exemple, entrez :

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

- Interface REST :

  Pour supprimer une clé du groupe, vous pouvez envoyer la demande HTTP suivante :

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

  Pour ajouter de nouveau la même clé au groupe, vous pouvez envoyer la demande HTTP suivante :

```
POST https://localhost:<port>/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. L'indication de réussite varie en fonction de l'interface :
   - Interface graphique :

     Pour les zones obligatoires, une colonne affiche les données modifiées. Pour les zones facultatives, vous devrez peut-être rouvrir la boîte de dialogue Modifier un groupe de clés pour afficher les modifications. Cliquez ensuite sur **Annuler**.
   - Interface de ligne de commande :

     Un message d'achèvement indique la réussite de l'opération.
   - Interface REST :

     Le code de statut `200 OK` indique un succès.

Que faire ensuite

Vous pouvez ensuite utiliser la page Gestion des clés et des unités LTO pour associer le groupe de clés à des unités spécifiques.

Suppression d'une clé ou d'un groupe de clés

Vous pouvez supprimer une clé ou un groupe de clés sélectionné. Vous ne pouvez pas supprimer une clé ou un groupe de clés s'il est associés à une unité ou à un groupe de clés par défaut.

Pourquoi et quand exécuter cette tâche

Ne supprimez des clés que lorsque les données qu'elles protègent ne sont plus utiles. Leur suppression a en effet les mêmes conséquences que l'effacement des données en question. Une fois les clés supprimées, les données protégées ne sont plus récupérables.

Vous pouvez utiliser l'option de menu **Supprimer**. Vous pouvez également utiliser les commandes ou les services REST suivants pour supprimer une clé ou un groupe de clés.

- **tklmKeyDelete** ou **Service REST Delete Key**

- **tklmGroupDelete** ou **Service REST Group Delete**

Votre rôle doit avoir un droit d'utilisation de l'action de suppression, ainsi qu'un droit d'accès au groupe d'unités approprié.

Avant d'effectuer la suppression, exécutez les vérifications suivantes :

- Clé

  Vérifiez que vous disposez d'une sauvegarde du magasin de clés contenant la clé à supprimer.
- Groupe de clés

  Si vous utilisez l'interface de ligne de commande, procurez-vous l'identificateur unique universel (UUID) du groupe de clés que vous comptez supprimer. Vérifiez que le groupe de clés n'est pas associé à une unité et qu'il ne correspond pas à un groupe de clés par défaut.

Procédure

1. Accédez à la page ou au répertoire approprié(e) :
   - Interface graphique :
     a. Connectez-vous à l'interface graphique.
     b. Dans la section Gestion des clés et des unités de la page de bienvenue, sélectionnez **Unité LTO**.
     c. Cliquez sur **Aller à** > **Gestion des clés et des unités**.
     d. Vous pouvez aussi cliquer avec le bouton droit sur **LTO** et sélectionner **Gestion des clés et des unités**.
     e. Sur la page de gestion pour LTO, sélectionnez une clé ou un groupe de clés dans la colonne appropriée.
     f. Cliquez sur **Supprimer**.
     g. Vous pouvez également faire un clic droit sur une clé ou un groupe de clés, puis sélectionner **Supprimer**.
   - Interface de ligne de commande
     a. Accédez au répertoire *<WAS_HOME>*/bin. Exemple :

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

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

     b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme SKLMAdmin. Exemple :

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

        Linux
        ```
        ./wsadmin.sh -username SKLMAdmin
        -password mypwd -lang jython
        ```
2. Supprimez la clé ou le groupe de clés :
   - Interface graphique :

     Dans la boîte de dialogue de confirmation, lisez le message de mise en garde avant de supprimer la clé ou le groupe de clés. Vérifiez que la clé ou le groupe de clés sélectionnés sont bien ceux que vous comptez supprimer. Vous pouvez, par exemple, supprimer un groupe de clés vide. La suppression d'un groupe de clés entraîne *la suppression de toutes les clés* qu'il contient. La suppression d'une clé membre d'un groupe de clés la supprime également de ce groupe. Cliquez ensuite sur **OK**.

- Interface de ligne de commande :
  - Clé

    Pour supprimer une clé, entrez la commande `tklmKeyDelete`. Par exemple, pour supprimer une clé non associée à une unité, vous devez d'abord localiser la clé. La commande **`tklmKeyList`** permet de trouver la clé à supprimer. Par exemple, tapez :

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

    Ensuite, supprimez la clé. Par exemple, tapez :

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

    La suppression d'une clé entraîne la suppression des éléments associés dans la base de données.
  - Groupe de clés

    Pour supprimer un groupe de clés, entrez la commande `tklmGroupDelete`. Vous pouvez, par exemple, supprimer un groupe de clés vide. La suppression d'un groupe de clés entraîne *la suppression de toutes les clés* qu'il contient. Par exemple, pour supprimer un groupe de clés non associé à une unité, entrez :

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

    Utilisez **`Service REST Delete Key`** pour supprimer une clé. Utilisez **`Service REST List Key`** pour trouver la clé à supprimer. Par exemple, vous pouvez envoyer la demande HTTP suivante :

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

    Envoyez la demande HTTP suivante pour supprimer la clé :

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

    Utilisez **`Service REST Group Delete`** pour supprimer un groupe de clés. Par exemple, vous pouvez envoyer la demande HTTP suivante :

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

Que faire ensuite

Actualisez la table pour vérifier que la clé ou le groupe de clés a bien été supprimé. Sauvegardez le magasin de clés afin de refléter précisément le changement de clés. Sauvegardez la base de données afin de refléter le changement de groupes de clés.

Ajout d'une unité

Vous pouvez ajouter une unité, telle qu'un lecteur de bande, à la base de données IBM Security Key Lifecycle Manager. Avant de commencer, créez les clés et groupes de clés à associer aux unités que vous allez identifier. Procurez-vous également le numéro de série du lecteur de bande, ainsi que d'autres informations descriptives. Déterminez si l'unité doit utiliser un groupe de clés spécifique ou le groupe par défaut du système.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser la boîte de dialogue Ajouter un lecteur de bande. Une unité peut également être ajoutée à l'aide de la commande **tklmDeviceAdd** ou du **service REST Device Add**. Votre rôle doit avoir un droit d'utilisation de l'action de création, ainsi qu'un droit d'accès au groupe d'unités approprié.

Procédure

1. Accédez à la page ou au répertoire approprié(e) :
   - Interface graphique :
     a. Connectez-vous à l'interface graphique.
     b. Dans la section Gestion des clés et des unités de la page de bienvenue, sélectionnez **Unité LTO**.
     c. Cliquez sur **Aller à** > **Gestion des clés et des unités**.
     d. Vous pouvez aussi cliquer avec le bouton droit sur **LTO** et sélectionner **Gestion des clés et des unités**.
     e. Sur la page de gestion pour LTO, cliquez sur **Ajouter**.
     f. Cliquez sur **Lecteur de bande**.
   - Interface de ligne de commande
     a. Accédez au répertoire <*WAS_HOME*>/bin. Exemple :

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

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

     b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme SKLMAdmin. Exemple :

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

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

2. Ajoutez une unité :
   - Interface graphique :

     Entrez les informations obligatoires et facultatives dans la boîte de dialogue Ajouter un lecteur de bande. Cliquez ensuite sur **Ajouter un lecteur de bande**.
   - Interface de ligne de commande :

     Entrez tklmDeviceAdd pour ajouter une unité. Vous devez indiquer le groupe d'unités et le numéro de série. Par exemple, entrez :

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

Utilisez **Service REST Device Add** pour ajouter une unité. Par exemple, vous pouvez envoyer la demande HTTP suivante :

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

Que faire ensuite

Ensuite, vérifiez que l'unité que vous avez ajoutée est répertoriée dans la table Unités.

Modification d'une unité

Vous pouvez modifier les informations relatives à une unité (par exemple, un lecteur de bande) dans la base de données d'IBM Security Key Lifecycle Manager. Vous pouvez par exemple mettre à jour la description de l'unité.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser la boîte de dialogue Modifier un lecteur de bande, la commande **tklmDeviceUpdate** ou **Service REST Device Update** pour mettre à jour une unité. Votre rôle doit avoir un droit d'utilisation de l'action de modification, ainsi qu'un droit d'accès au groupe d'unités approprié.

Avant de commencer, créez les clés et les groupes de clés à associer aux unités que vous allez modifier. Si vous utilisez l'interface de ligne de commande ou l'interface REST, obtenez la valeur de l'identificateur unique universel (UUID) de l'unité que vous souhaitez mettre à jour.

Procédure

1. Accédez à la page ou au répertoire approprié.
   - Interface graphique :
     a. Connectez-vous à l'interface graphique.
     b. Dans la section Gestion des clés et des unités de la page de bienvenue, sélectionnez **Unité LTO**.
     c. Cliquez sur **Aller à** > **Gestion des clés et des unités**.
     d. Vous pouvez aussi cliquer avec le bouton droit sur **LTO** et sélectionner **Gestion des clés et des unités**.
     e. Sur la page de gestion pour LTO, sélectionnez une unité dans la colonne **Lecteurs de bande**.
     f. Cliquez sur **Modifier**.
     g. Vous pouvez également faire un clic droit sur une unité et sélectionner **Modifier**, ou bien faire un double clic sur une entrée d'unité.
   - Interface de ligne de commande
     a. Accédez au répertoire *<WAS_HOME>*/bin. Exemple :

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

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

     b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme SKLMAdmin. Exemple :

Windows

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

Linux

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

2. Modifiez une unité :
   - Interface graphique :
     a. Entrez les informations obligatoires et facultatives dans la boîte de dialogue Modifier un lecteur de bande.
     b. Cliquez sur **Modifier un lecteur de bande**.
   - Interface de ligne de commande :

     Entrez la commande `tklmDeviceUpdate` pour mettre à jour une unité. Vous devez spécifier l'identificateur unique universel de l'unité, ainsi que les attributs à modifier. Par exemple, entrez :

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

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

   - Interface REST :

     Utilisez **Service REST Device Update** pour mettre à jour une unité. Vous devez spécifier l'identificateur unique universel de l'unité, ainsi que les attributs à modifier. Par exemple, vous pouvez envoyer la demande HTTP suivante :

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

     ```
     PUT https://localhost:<port>/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 monUnitéLTO"}
     ```

Que faire ensuite

Vous pouvez ensuite vérifier les modifications apportées. Pour les champs optionnels tels que la description, vous voudrez peut-être exécuter la commande **tklmDeviceList** ou **Service REST Device List** pour déterminer si leur valeur a été modifiée. Vous pouvez également rouvrir la boîte de dialogue Modifier un lecteur de bande.

Suppression d'une unité

Vous pouvez supprimer une unité, telle qu'un lecteur de bande. Les métadonnées de l'unité que vous supprimez, telles que son numéro de série, sont supprimées de la base de données de IBM Security Key Lifecycle Manager.

Pourquoi et quand exécuter cette tâche

Avant de commencer, assurez-vous qu'il existe une sauvegarde à jour de la base de données IBM Security Key Lifecycle Manager. Si vous utilisez l'interface de ligne de commande ou l'interface REST, procurez-vous l'identificateur unique universel (`uuid`) de l'unité que vous comptez supprimer.

Vous pouvez utiliser l'option de menu Supprimer, la commande **tklmDeviceDelete** ou le **Service REST Device Delete** pour supprimer une unité. Votre rôle doit avoir un droit d'utilisation de l'action de suppression, ainsi qu'un droit d'accès au groupe d'unités approprié.

Procédure

1. Accédez à la page ou au répertoire approprié.
   - Interface graphique :
     a. Connectez-vous à l'interface graphique.
     b. Dans la section Gestion des clés et des unités de la page de bienvenue, sélectionnez **Unité LTO**.
     c. Cliquez sur **Aller à** > **Gestion des clés et des unités**.
     d. Vous pouvez aussi cliquer avec le bouton droit sur **LTO** et sélectionner **Gestion des clés et des unités**.
     e. Sur la page de gestion pour LTO, sélectionnez une unité.
     f. Cliquez sur **Supprimer**.
     g. Vous pouvez également cliquer avec le bouton droit de la souris sur une unité, puis sélectionner **Supprimer**.
   - Interface de ligne de commande
     a. Accédez au répertoire <*WAS_HOME*>/bin. Exemple :

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

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

     b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme SKLMAdmin. Exemple :

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

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

2. Supprimez l'unité.
   - Interface graphique :

     Dans la boîte de dialogue de confirmation, lisez le message de confirmation avant de supprimer l'unité. Les métadonnées de l'unité que vous supprimez, telles que son numéro de série, sont supprimées de la base de données de IBM Security Key Lifecycle Manager. Cliquez sur **OK**.
   - Interface de ligne de commande :

     Entrez tklmDeviceDelete pour supprimer une unité. Vous devez indiquer son identificateur unique universel (UUID). Par exemple, entrez :

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

     Utilisez **Service REST Device Delete** pour supprimer une unité. Vous devez indiquer l'identificateur unique universel (UUID) de l'unité. Par exemple, vous pouvez envoyer la demande HTTP suivante à l'aide d'un client REST :

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

Gestion d'unité de bande 3592

Vous pouvez gérer des unités de bande 3592 à l'aide d'IBM Security Key Lifecycle Manager.

Les descriptions de certaines étapes proposent d'utiliser l'interface graphique, l'interface de ligne de commande ou l'interface REST. Veillez à ne pas changer d'interface au cours d'une même session de travail.

Les descriptions de certaines tâches peuvent mentionner des propriétés contenues dans le fichier `SKLMConfig.properties`. Utilisez l'interface graphique, l'interface de ligne de commande ou l'interface REST pour modifier ces propriétés.

Etapes guidées pour la création de certificats et d'unités

Lorsque vous créez des certificats et des unités, puis que vous ajoutez d'autres certificats et unités ultérieurement, IBM Security Key Lifecycle Manager fournit un ensemble d'étapes détaillées permettant d'effectuer la tâche.

La description de certaines étapes mentionne parfois la possibilité d'accomplir la même tâche en utilisant l'interface de ligne de commande ou l'interface REST. Dans un ensemble de tâches détaillées, utilisez l'interface utilisateur graphique pour effectuer les tâches.

Création d'un certificat ou d'une demande de certificat

Dans un premier temps, créez des certificats ou des demandes de certificat pour IBM Security Key Lifecycle Manager. Avant de commencer, déterminez la politique de votre site concernant l'utilisation de certificats autosignés et de certificats émis par une autorité de certification. Vous pouvez créer des certificats autosignés pour la phase de test de votre projet. Vous pouvez également adresser sans tarder vos demandes de certificats à une autorité de certification afin de les recevoir à temps pour l'entrée en production de votre projet.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser la boîte de dialogue Créer un certificat. Vous pouvez également utiliser l'une des commandes ou des services REST suivants pour créer des certificats ou des demandes de certificat :

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

Votre rôle doit avoir un droit d'utilisation de l'action de création, ainsi qu'un droit d'accès au groupe d'unités approprié. Pour désigner ce certificat comme certificat par défaut, vous devez également avoir accès à l'action de modification.

Si vous souhaitez également indiquer qu'un certificat est utilisé comme certificat par défaut ou comme certificat partenaire, vous pouvez utiliser les commandes ou services REST suivants :

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

Ces valeurs étaient auparavant stockées dans les propriétés **drive.default.alias1** (pour le certificat par défaut) et **drive.default.alias2** (pour le certificat partenaire). Ces propriétés sont obsolètes dans la nouvelle version du produit.

Procédure

1. Accédez à la page ou au répertoire approprié.
   - Interface graphique :
     a. Connectez-vous à l'interface graphique.
     b. Dans la section Gestion des clés et des unités de la page de bienvenue, sélectionnez **3592**.
     c. Cliquez sur **Aller à** > **Création de clés et d'unités en mode guidé**.
     d. Vous pouvez aussi cliquer avec le bouton droit sur **3592** et sélectionner **Création de clés et d'unités en mode guidé**.
   - Interface de ligne de commande
     a. Accédez au répertoire <*WAS_HOME*>/bin. Exemple :

        Windows

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

        Linux

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

     b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme SKLMAdmin. Exemple :

        Windows

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

        Linux

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

   - Interface REST :
     – Ouvrez un client REST.
2. Créez ou demandez un certificat.
   - Interface graphique :
     a. Sur la page Etape 1 : Créer des certificats, cliquez sur **Créer** dans la table **Certificats**.
     b. Dans la boîte de dialogue Créer un certificat, sélectionnez un certificat autosigné ou une demande de certificat pour un fournisseur tiers.
     c. Indiquez des valeurs pour les paramètres obligatoires et facultatifs. Vous pouvez, par exemple, indiquer qu'il s'agit du certificat par défaut ou du certificat partenaire.
     d. Cliquez sur **Créer un certificat**.
   - Interface de ligne de commande :
     – Certificat

       Entrez tklmCertCreate pour créer un certificat et une paire de clés publique et privée, et stockez le certificat dans un fichier de clés existant. Par exemple, entrez :

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

– Demande de certificat

Entrez `tklmCertGenRequest` pour créer un fichier de demande de certificat PKCS #10. Par exemple, entrez :

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

- Interface REST :
  – Certificat
    a. Obtenez un identificateur d'authentification utilisateur unique pour accéder aux services REST d'IBM Security Key Lifecycle Manager. Pour plus d'informations sur le processus d'authentification, voir Processus d'authentification pour les services REST.
    b. Pour exécuter le **service REST Create Certificate**, envoyez la demande HTTP POST. Transmettez l'identificateur d'authentification utilisateur que vous avez obtenu à l'étape a avec le message de demande, conformément à l'exemple suivant :

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

  – Demande de certificat

Utilisez le **service REST Certificate Generate Request** pour créer un fichier de demande de certificat PKCS #10. Par exemple, vous pouvez envoyer la demande HTTP suivante :

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

Que faire ensuite

Faites une sauvegarde des nouveaux certificats avant qu'ils ne commencent à être servis aux unités. Pour une demande de certificat, l'étape suivante consiste à importer le certificat signé. Vous pouvez ensuite passer à l'étape guidée suivante pour définir des unités spécifiques et leur associer des certificats. Sélectionnez **Etape 2 : Identifier les unités** ou cliquez sur **Passer à l'étape suivante**.

Pour un groupe d'unités 3592, spécifiez également des valeurs pour les certificats par défaut et partenaire dans la base de données d'IBM Security Key Lifecycle Manager. Utilisez la commande **tklmDeviceGroupAttributeUpdate** ou le **service REST Device Group Attribute Update** pour définir ces valeurs.

Identification d'unités

Vous pouvez identifier une unité de bande 3592 à utiliser avec IBM Security Key Lifecycle Manager. Avant de commencer, créez les certificats à associer aux unités que vous allez identifier.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser la boîte de dialogue Ajouter un lecteur de bande, la commande **tklmDeviceAdd** ou **Service REST Device Add** pour ajouter une unité. Votre rôle doit avoir un droit d'utilisation de l'action de création, ainsi qu'un droit d'accès au groupe d'unités approprié.

Vous pouvez effectuer les choix suivants pour fournir des clés à des unités :

Accepter uniquement les unités ajoutées manuellement pour la communication
Les unités entrantes ne sont pas systématiquement ajoutées au magasin de données. Vous devez spécifier manuellement, pour chaque unité, si des clés lui seront servies ou non.

Retenir les demandes des nouvelles unités en attente de mon approbation
Toutes les unités entrantes d'un groupe d'unités valide sont ajoutées au magasin de données, mais lorsqu'elles demandent des clés, celles-ci ne leur sont pas servies automatiquement. Vous devez accepter ou rejeter chaque unité dans la liste des unités en attente, en fonction de quoi des clés lui sont servies ou non lorsqu'elle en fait la demande.

Accepter automatiquement toutes les demandes des nouvelles unités pour la communication
Toutes les nouvelles unités entrantes d'un groupe d'unités valide sont ajoutées au magasin de données et, lorsqu'elles demandent des clés, celles-ci leur sont servies automatiquement.

Remarque : N'utilisez pas cette option si vous comptez déplacer la nouvelle unité vers un autre groupe d'unités. Sélectionnez plutôt le mode d'approbation manuel ou avec mise en attente pour que l'occasion vous soit donnée de transférer l'unité dans le groupe approprié avant que des clés ne lui soient servies.

Procédure

1. Accédez à la page ou au répertoire approprié.
   - Interface graphique :
     a. Connectez-vous à l'interface graphique.
     b. Dans la section Gestion des clés et des unités de la page de bienvenue, sélectionnez **3592**.
     c. Cliquez sur **Aller à** > **Création de clés et d'unités en mode guidé**.
     d. Vous pouvez aussi cliquer avec le bouton droit sur **3592** et sélectionner **Création de clés et d'unités en mode guidé**.
   - Interface de ligne de commande
     a. Accédez au répertoire *<WAS_HOME>*/bin. Exemple :

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

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

     b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme SKLMAdmin. Exemple :

Windows

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

Linux

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

- Interface REST :
  - Ouvrez un client REST.

2. Ignorez la page **Etape 1 : Créer des certificats**. Cliquez sur **Passer à l'étape suivante** ou sur **Etape 2 : Identifier les unités**.
3. Vous pouvez demander que IBM Security Key Lifecycle Manager mette en attente les demandes des nouvelles unités afin que vous puissiez ensuite les accepter ou les rejeter. Votre rôle doit avoir un droit d'utilisation de l'action de modification, ainsi qu'un droit d'accès au groupe d'unités approprié.
   - Interface graphique :

     Sélectionnez **Retenir les demandes des nouvelles unités en attente de mon approbation**.
   - Interface de ligne de commande :

     Utilisez la commande **tklmDeviceGroupAttributeUpdate** ou le **service REST Device Group Attribute Update** pour définir la valeur de l'attribut **device.AutoPendingAutoDiscovery**. Par exemple, entrez :

     ```
     print AdminTask.tklmDeviceGroupAttributeUpdate ('[-name 3592
       -attributes "{device.AutoPendingAutoDiscovery 2}"]')
     ```
   - Interface REST :
     a. Obtenez un identificateur d'authentification utilisateur unique pour accéder aux services REST d'IBM Security Key Lifecycle Manager. Pour plus d'informations sur le processus d'authentification, voir Processus d'authentification pour les services REST.
     b. Pour exécuter le **service REST Device Group Attribute Update** et définir la valeur de l'attribut **device.AutoPendingAutoDiscovery**, envoyez la demande HTTP PUT. Transmettez l'identificateur d'authentification utilisateur que vous avez obtenu à l'étape a avec le message de demande, conformément à l'exemple suivant :

     ```
     PUT https://localhost:<port>/SKLM/rest/v1/deviceGroupAttributes
     Content-Type: application/json
     Accept : application/json
     Authorization: SKLMAuth authId=139aeh34567m
     {"name":"3592","attributes":"device.AutoPendingAutoDiscovery 2"}
     ```
4. Ajoutez une unité.
   - Interface graphique :
     a. Sur la page Etape 2 : Identifier les unités, dans la table **Unités**, cliquez sur **Ajouter**.
     b. Entrez les informations obligatoires et facultatives dans la boîte de dialogue Ajouter un lecteur de bande.
     c. Cliquez sur **Ajouter un lecteur de bande**.
   - Interface de ligne de commande :

     Entrez tklmDeviceAdd pour ajouter une unité. Vous devez indiquer le groupe d'unités et le numéro de série. Par exemple, entrez :

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

Vous pouvez utiliser le **service REST Device Add** pour ajouter une unité. Par exemple, vous pouvez envoyer la demande HTTP suivante :

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

Que faire ensuite

Vous pouvez ensuite utiliser la page Gestion des clés et des unités 3592 pour afficher tous les certificats et toutes les unités.

Administration de certificats et d'unités

Pour administrer des certificats et des unités, vous voudrez peut-être déterminer leur statut actuel. Vous pouvez mapper leur association ou ajouter, modifier ou supprimer des certificats ou des unités spécifiques.

Pourquoi et quand exécuter cette tâche

Avant de commencer, examinez les colonnes de la page, qui comprend des boutons permettant d'ajouter, de modifier ou de supprimer un élément de la table. Pour trier les informations, cliquez sur un en-tête de colonne.

Utilisez la page Gestion des clés et des unités 3592 pour mapper des certificats à des unités afin de déterminer le statut des éléments dans la table. Vous pouvez ajouter, modifier ou supprimer des certificats ou des unités spécifiques. Votre rôle doit avoir un droit d'utilisation de l'action de visualisation, ainsi qu'un droit d'accès au groupe d'unités approprié.

La table est organisée selon les zones suivantes :

- Dans les colonnes de gauche, informations sur les certificats indiquant le nom, la date d'expiration et le statut actuel de chaque certificat. Il est également précisé si le certificat est utilisé comme certificat par défaut ou comme certificat partenaire.
- Dans les colonnes de droite, informations indiquant le nom de chaque unité et précisant si celle-ci utilise une valeur par défaut du système comme son certificat par défaut ou son certificat partenaire.
- Icônes de statut indiquant le statut de chaque certificat.

Tableau 3. Icônes de statut et signification

Icône	Description
	Le certificat est actif.
	Le certificat est dans un état compromis.
	Le certificat arrive bientôt à expiration.
	Le certificat est arrivé à expiration.

Tableau 3. Icônes de statut et signification (suite)

Icône	Description
	Certificat valide à une date ultérieure ; concerne les certificats migrés dont l'horodatage spécifie une date d'utilisation à venir.
	IBM Security Key Lifecycle Manager a des demandes de certificat de fournisseur tiers en attente de signature et d'importation.

Procédure

1. Connectez-vous à l'interface graphique :
   a. Dans la section Gestion des clés et des unités de la page de bienvenue, sélectionnez **3592**.
   b. Cliquez sur **Aller à** > **Gestion des clés et des unités**.
   c. Vous pouvez aussi cliquer avec le bouton droit sur **3592** et sélectionner **Gestion des clés et des unités**.

   Les descriptions de certaines étapes proposent d'utiliser l'interface graphique, l'interface de ligne de commande ou l'interface REST. Veillez à ne pas changer d'interface au cours d'une même session de travail.

   Les descriptions de certaines tâches peuvent mentionner des propriétés contenues dans le fichier `SKLMConfig.properties`. Utilisez l'interface graphique, l'interface de ligne de commande ou l'interface REST pour modifier ces propriétés.
2. Sur la page Gestion des clés et des unités 3592, vous pouvez ajouter, modifier ou supprimer un certificat ou une unité. Vous pouvez également contrôler l'état des certificats.

   Vous pouvez exécuter les tâches d'administration suivantes :

   - Ajouter

     Cliquez sur **Ajouter**. Vous pouvez également sélectionner un processus pas à pas pour créer des certificats et des unités.

     – Certificat

       Dans la boîte de dialogue Créer un certificat, sélectionnez un type de certificat autosigné ou issu d'un fournisseur tiers, et renseignez les informations requises. Cliquez ensuite sur **Créer un certificat**. Votre rôle doit avoir un droit d'utilisation de l'action de création, ainsi qu'un droit d'accès au groupe d'unités approprié. Pour désigner ce certificat comme certificat par défaut, vous devez également avoir accès à l'action de modification.

     – Lecteur de bande

       Entrez les informations sur l'unité dans la boîte de dialogue Ajouter un lecteur de bande. Cliquez ensuite sur **Ajouter un lecteur de bande**. Votre rôle doit avoir un droit d'utilisation de l'action de création, ainsi qu'un droit d'accès au groupe d'unités approprié.

     – Utilisez le processus pas à pas pour la création de certificats et d'unités

       Entrez les informations requises sur les pages Etape 1 : Créer des certificats et Etape 2 : Identifier les unités.

     L'indication de réussite varie, reflétant le changement dans la colonne dédiée au certificat ou à l'unité.

   - Modifier

Pour modifier ou supprimer un certificat ou une unité, sélectionnez l'élément approprié, puis cliquez sur **Modifier**. Vous pouvez également cliquer avec le bouton droit de la souris sur l'unité ou le certificat sélectionné. Cliquez ensuite sur **Modifier** ou cliquez deux fois sur une entrée d'unité ou de certificat dans la liste.

– Certificat

  Indiquez les modifications dans la boîte de dialogue Modifier un certificat. Cliquez ensuite sur **Modifier un certificat**. Votre rôle doit avoir un droit d'utilisation de l'action de modification, ainsi qu'un droit d'accès au groupe d'unités approprié.

– Lecteur de bande

  Indiquez les modifications dans la boîte de dialogue Modifier un lecteur de bande. Cliquez ensuite sur **Modifier un lecteur de bande**. Votre rôle doit avoir un droit d'utilisation de l'action de modification, ainsi qu'un droit d'accès au groupe d'unités approprié.

L'indication de réussite varie, reflétant le changement dans la colonne dédiée au certificat ou à l'unité. Il se peut que des modifications relatives à certaines informations, telles que des zones facultatives, ne figurent pas dans la table.

- Supprimer

  Pour supprimer un certificat ou une unité, mettez l'entrée en évidence dans la table, puis cliquez sur **Supprimer**. Vous pouvez également cliquer avec le bouton droit de la souris sur l'unité ou le certificat sélectionné. Cliquez ensuite sur **Supprimer**.

  – Certificat

    Vérifiez que vous disposez d'une sauvegarde actualisée du magasin de clés avant de supprimer un certificat. Toutes les bandes écrites à l'aide de ce certificat deviennent illisibles après sa suppression. Le certificat à supprimer peut présenter n'importe quel statut, il peut par exemple être actif. Quel que soit le statut, vous ne pouvez pas supprimer un certificat qui est associé à une unité. Vous ne pouvez pas non plus supprimer un certificat marqué comme certificat par défaut ou certificat partenaire. Votre rôle doit avoir un droit d'utilisation de l'action de suppression, ainsi qu'un droit d'accès au groupe d'unités approprié.

    La suppression d'un certificat entraîne la suppression des éléments associés dans la base de données.

    Pour confirmer la suppression, cliquez sur **OK**.

  – Lecteur de bande

    Les métadonnées relatives à l'unité que vous supprimez, telles que son numéro de série, sont supprimées de la base de données IBM Security Key Lifecycle Manager. Pour confirmer la suppression, cliquez sur **OK**. Votre rôle doit avoir un droit d'utilisation de l'action de suppression, ainsi qu'un droit d'accès au groupe d'unités approprié.

  L'indicateur de réussite indique que le certificat ou l'unité est supprimé de la table d'administration.

Ajout d'un certificat ou d'une demande de certificat

Vous pouvez ajouter d'autres certificats ou demandes de certificat à utiliser avec IBM Security Key Lifecycle Manager. Avant de commencer, déterminez la stratégie de votre site concernant l'utilisation de certificats autosignés et d'une autorité de certification. Vous pouvez créer des certificats autosignés pour la phase de test de votre projet. Vous pouvez également adresser sans tarder vos demandes de certificats à une autorité de certification afin de les recevoir à temps pour l'entrée en production de votre projet.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser la boîte de dialogue Créer un certificat. Vous pouvez également utiliser l'une des commandes ou des services REST suivants pour créer des certificats ou des demandes de certificat :

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

Votre rôle doit avoir un droit d'utilisation de l'action de création, ainsi qu'un droit d'accès au groupe d'unités approprié. Pour désigner ce certificat comme certificat par défaut, vous devez également avoir accès à l'action de modification.

Avant de commencer, déterminez la stratégie de votre site concernant l'utilisation de certificats autosignés et d'une autorité de certification. Vous pouvez être amené à créer des certificats autosignés pour la phase de test de votre projet. Vous pouvez également adresser sans tarder vos demandes de certificats à une autorité de certification afin de les recevoir à temps pour l'entrée en production de votre projet.

Procédure

1. Accédez à la page ou au répertoire approprié.
   - Interface graphique :
     a. Connectez-vous à l'interface graphique.
     b. Dans la section Gestion des clés et des unités de la page de bienvenue, sélectionnez **3592**.
     c. Cliquez sur **Aller à** > **Gestion des clés et des unités**.
     d. Vous pouvez aussi cliquer avec le bouton droit sur **3592** et sélectionner **Gestion des clés et des unités**.
     e. Sur la page de gestion pour 3592, cliquez sur **Ajouter**.
     f. Cliquez sur **Certificat**.
   - Interface de ligne de commande
     a. Accédez au répertoire <*WAS_HOME*>/bin. Exemple :

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

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

     b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme SKLMAdmin. Exemple :

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

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

2. Créez ou demandez un certificat.
   - Interface graphique :
     a. Dans la boîte de dialogue Créer un certificat, sélectionnez un certificat autosigné ou une demande de certificat auprès d'un fournisseur tiers.
     b. Indiquez des valeurs pour les paramètres obligatoires et facultatifs. Vous pouvez, par exemple, indiquer qu'il s'agit du certificat par défaut ou du certificat partenaire. Cliquez ensuite sur **Créer un certificat**.

- Interface de ligne de commande :
  - Certificat :

    Entrez `tklmCertCreate` pour créer un certificat ainsi qu'une paire de clés publiques et privées, puis stockez le certificat dans un magasin de clés existant. Par exemple, tapez :

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

  - Demande de certificat :

    Entrez `tklmCertGenRequest` pour créer un fichier de demande de certificat PKCS #10. Par exemple, tapez :

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

- Interface REST :
  - Certificat

    Utilisez **Service REST Create Certificate** pour créer un certificat et une paire de clés publique et privée, puis stockez le certificat dans un magasin de clés existant. Par exemple, vous pouvez envoyer la demande HTTP suivante à l'aide d'un client REST :

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

  - Demande de certificat

    Utilisez **Service REST Certificate Generate Request** pour créer un fichier de demande de certificat PKCS #10. Par exemple, vous pouvez envoyer la demande HTTP suivante à l'aide d'un client REST :

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

Que faire ensuite

La prochaine action varie selon que vous avez créé ou non un certificat ou une demande de certificat.

- Certificat :

  Faites une sauvegarde des nouveaux certificats avant qu'ils ne commencent à être servis aux unités. Vous pouvez associer un certificat à une unité spécifique.

- Demande de certificat :

  Envoyez manuellement la demande de certificat à une autorité de certification. Au retour du certificat signé, importez-le à l'aide d'un élément d'action en attente sur le panneau d'accueil ou à l'aide de la commande **tklmCertImport** ou de **Service REST Certificate Import**. Après quoi, faites une sauvegarde du certificat afin qu'il puisse être servi à une unité.

Spécification d'un certificat de remplacement

Vous pouvez spécifier un certificat à utiliser ultérieurement comme certificat par défaut ou certificat partenaire du système.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser l'interface graphique, la commande **tklmCertDefaultRolloverAdd** ou **Service REST Cert Default Rollover Add** pour ajouter un remplacement de certificat par défaut pour une date et un groupe d'unités spécifiques. Votre rôle doit avoir un droit d'utilisation de l'action de création, ainsi qu'un droit d'accès au groupe d'unités approprié.

Procédure

1. Accédez à la page ou au répertoire approprié.
   - Interface graphique :
     a. Connectez-vous à l'interface graphique.
     b. Dans la section Gestion des clés et des unités de la page de bienvenue, sélectionnez **3592**.
     c. Cliquez sur **Aller à** > **Gestion des remplacements de valeurs par défaut**.
     d. Vous pouvez aussi cliquer avec le bouton droit sur **3592** et sélectionner **Gestion des remplacements de valeurs par défaut**.
   - Interface de ligne de commande
     a. Accédez au répertoire <*WAS_HOME*>/bin. Exemple :

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

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

     b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme SKLMAdmin. Exemple :

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

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

2. Spécifiez un certificat existant à utiliser ultérieurement comme certificat par défaut ou certificat partenaire du système.
   - Interface graphique :
     a. Sur la page de gestion pour 3592, cliquez sur **Ajouter**.
     b. Dans la boîte de dialogue Ajouter une future valeur par défaut, spécifiez les informations requises.
     c. Cliquez sur **Ajouter une future valeur par défaut**.

     Remarque :
     - Veillez à ne pas indiquer deux valeurs par défaut pour la même date de remplacement.
     - Le système ne vérifie pas si le certificat sélectionné a déjà expiré ou aura expiré à la date prévue pour le remplacement.
     - Si aucun certificat n'existe à la date du remplacement, IBM Security Key Lifecycle Manager continue à utiliser le certificat par défaut du moment.
     - Vous pouvez ajouter ou supprimer des entrées dans la table, mais il n'est pas possible de les modifier.

- Interface de ligne de commande :

  Ajoutez un certificat de remplacement. Par exemple, entrez :

  ```
  print AdminTask.tklmCertDefaultRolloverAdd
  ('[-usage 3592 -alias tklmcert1
       -certDefaultType 1 -effectiveDate 2010-05-30]')
  ```

3. L'indication de réussite varie en fonction de l'interface :
   - Interface graphique :

     Le certificat apparaît dans la table des certificats de remplacement, sur la page 3592.
   - Interface de ligne de commande :

     Un message d'achèvement indique la réussite de l'opération.
   - Interface REST :

     Le code de statut `200 OK` indique un succès.
4. Pour supprimer un certificat de la table des remplacements :
   - Interface graphique :

     Sélectionnez un certificat et cliquez sur **Supprimer**. Votre rôle doit avoir un droit d'utilisation de l'action de suppression. Lisez le message d'avertissement. Cliquez ensuite sur **OK**.
   - Interface de ligne de commande :

     Utilisez la commande **tklmCertDefaultRolloverList** pour afficher l'UUID d'un certificat. Votre rôle doit avoir un droit d'utilisation de l'action de visualisation, ainsi qu'un droit d'accès au groupe d'unités approprié. Utilisez ensuite la commande **tklmCertDefaultRolloverDelete** pour supprimer le certificat de la liste des certificats de remplacement. Votre rôle doit avoir un droit d'utilisation de l'action de suppression, ainsi qu'un droit d'accès au groupe d'unités approprié. Par exemple, entrez :

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

   Le certificat n'est plus considéré comme futur certificat par défaut ou partenaire du système, mais il n'est pas modifié ni supprimé.

Modification d'un certificat

Vous pouvez modifier un certificat de façon à ce que ce dernier soit utilisé en tant que certificat par défaut ou certificat partenaire. Avant de commencer, déterminez la nature des modifications apportées au certificat. Il peut s'agir de changer sa description ou de le désigner comme certificat par défaut ou certificat partenaire. Si vous utilisez l'interface de ligne de commande, obtenez la valeur de l'identificateur unique universel (`uuid`) du certificat.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser la boîte de dialogue Modifier un certificat pour modifier un certificat. Vous pouvez également utiliser les commandes ou services REST suivants :

- **tklmCertUpdate** ou **Service REST Certificate Update** pour modifier l'état d'un certificat (par exemple, le désigner comme certificat de confiance ou compromis) et pour modifier les informations d'un certificat.
- **tklmDeviceTypeAttributeUpdate** ou **Service REST Device Type Attribute Update** pour désigner un certificat comme certificat par défaut ou certificat partenaire.

Votre rôle doit avoir un droit d'utilisation de l'action de modification, ainsi qu'un droit d'accès au groupe d'unités approprié.

Procédure

1. Accédez à la page ou au répertoire approprié.
   - Interface graphique :
     a. Connectez-vous à l'interface graphique.
     b. Dans la section Gestion des clés et des unités de la page de bienvenue, sélectionnez **3592**.
     c. Cliquez sur **Aller à** > **Gestion des clés et des unités**.
     d. Vous pouvez aussi cliquer avec le bouton droit sur **3592** et sélectionner **Gestion des clés et des unités**.
     e. Sur la page de gestion pour 3592, sélectionnez un certificat dans la colonne **Certificats**.
     f. Cliquez sur **Modifier**.
     g. Vous pouvez également faire un clic droit sur un certificat et sélectionner **Modifier**, ou bien faire un double clic sur une entrée de certificat.
   - Interface de ligne de commande
     a. Accédez au répertoire <*WAS_HOME*>/bin. Exemple :

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

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

     b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme SKLMAdmin. Exemple :

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

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

2. Modifiez les informations relatives au certificat :
   - Interface graphique :

     Dans la boîte de dialogue Modifier un certificat, modifiez les zones appropriées. Cliquez ensuite sur **Modifier un certificat**.
   - Interface de ligne de commande :

     Tapez tklmCertList pour rechercher un certificat et tklmCertUpdate pour mettre à jour un certificat. Vous devez indiquer l'identificateur unique universel (UUID) du certificat, ainsi que l'attribut modifié. Par exemple, pour modifier une description, entrez :

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

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

     Utilisez **Service REST Certificate List** pour rechercher un certificat. Par exemple, vous pouvez envoyer la demande HTTP suivante :

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

Utilisez **Service REST Certificate Update** pour mettre à jour un certificat. Par exemple, vous pouvez envoyer la demande HTTP suivante :

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

Que faire ensuite

Vous pouvez utiliser la page Gestion des clés et des unités 3592 pour associer des certificats à des unités spécifiques.

Suppression d'un certificat

Vous pouvez être amené à supprimer un certificat sélectionné, lequel peut avoir n'importe quel statut, par exemple actif. Vous ne pouvez pas supprimer un certificat associé à une unité ou un certificat marqué en tant que certificat par défaut ou certificat partenaire. Vous pouvez, par exemple, supprimer un certificat arrivé à expiration.

Pourquoi et quand exécuter cette tâche

Avant de commencer, assurez-vous que vous disposez d'une sauvegarde du magasin de clés contenant le certificat à supprimer. Vérifiez que le certificat n'est pas actuellement associé à une unité et qu'il n'est pas marqué en tant que certificat par défaut ou certificat partenaire. Déterminez l'état actuel du certificat et assurez-vous que la suppression d'un certificat dans cet état est conforme à la politique de votre site.

Ne supprimez des certificats que lorsque les données qu'ils protègent ne sont plus utiles. Leur suppression a en effet les mêmes conséquences que l'effacement des données en question. Une fois les certificats supprimés, les données protégées ne sont plus récupérables.

Vous pouvez utiliser l'option de menu Supprimer, la commande **tklmCertDelete** ou **Service REST Delete Certificate** pour supprimer un certificat. Votre rôle doit avoir un droit d'utilisation de l'action de suppression, ainsi qu'un droit d'accès au groupe d'unités approprié.

La suppression d'un certificat entraîne la suppression des éléments associés dans la base de données.

Procédure

1. Accédez à la page ou au répertoire approprié.
   - Interface graphique :
     a. Connectez-vous à l'interface graphique.
     b. Dans la section Gestion des clés et des unités de la page de bienvenue, sélectionnez **3592**.
     c. Cliquez sur **Aller à** > **Gestion des clés et des unités**.
     d. Vous pouvez aussi cliquer avec le bouton droit sur **3592** et sélectionner **Gestion des clés et des unités**.
     e. Sur la page de gestion pour 3592, sélectionnez un certificat dans la colonne **Certificats**.
     f. Cliquez sur **Supprimer**.

g. Vous pouvez également cliquer avec le bouton droit de la souris sur un certificat, puis sélectionner **Supprimer**.

- Interface de ligne de commande

a. Accédez au répertoire *<WAS_HOME>*/bin. Exemple :

Windows

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

Linux

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

b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme SKLMAdmin. Exemple :

Windows

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

Linux

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

2. Supprimez le certificat.

- Interface graphique :

  Lisez le message de confirmation dans la boîte de dialogue correspondante afin de vérifier que vous avez sélectionné le certificat approprié avant de le supprimer. Cliquez ensuite sur **OK**.

- Interface de ligne de commande :

  Tapez tklmCertList pour rechercher un certificat et tklmCertDelete pour supprimer un certificat. Vous devez spécifier l'alias du certificat, ainsi que le nom du magasin de clés. Par exemple, pour supprimer un certificat arrivé à expiration et qui n'est actuellement pas associé à une unité, entrez :

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

- Interface REST :

  Utilisez **Service REST Certificate List** et **Service REST Delete Certificate** respectivement pour rechercher et supprimer un certificat. Par exemple, vous pouvez envoyer les demandes HTTP suivantes :

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

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

Que faire ensuite

Vous pouvez ensuite être amené à sauvegarder de nouveau le magasin de clés afin de refléter précisément les modifications apportées aux certificats.

Ajout d'une unité

Vous pouvez ajouter une unité, telle qu'un lecteur de bande, à la base de données IBM Security Key Lifecycle Manager. Avant de commencer, créez les certificats à associer aux unités que vous allez identifier. Procurez-vous également le numéro

de série du lecteur de bande, ainsi que d'autres informations descriptives. Déterminez si l'unité doit utiliser un certificat spécifique ou un certificat par défaut.

Pourquoi et quand exécuter cette tâche

commande **tklmDeviceAdd**

Vous pouvez utiliser la boîte de dialogue Ajouter un lecteur de bande. Une unité peut également être ajoutée à l'aide de la commande **tklmDeviceAdd** ou de **Service REST Device Add**. Votre rôle doit avoir un droit d'utilisation de l'action de création, ainsi qu'un droit d'accès au groupe d'unités approprié.

Procédure

1. Accédez à la page ou au répertoire approprié.
   - Interface graphique :
     a. Connectez-vous à l'interface graphique.
     b. Dans la section Gestion des clés et des unités de la page de bienvenue, sélectionnez **3592**.
     c. Cliquez sur **Aller à** > **Gestion des clés et des unités**.
     d. Vous pouvez aussi cliquer avec le bouton droit sur **3592** et sélectionner **Gestion des clés et des unités**.
     e. Sur la page de gestion pour 3592, cliquez sur **Ajouter**.
     f. Cliquez sur **Lecteur de bande**.
   - Interface de ligne de commande
     a. Accédez au répertoire <*WAS_HOME*>/bin. Exemple :

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

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

     b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme SKLMAdmin. Exemple :

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

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

2. Ajoutez une unité.
   - Interface graphique :

     Entrez les informations obligatoires et facultatives dans la boîte de dialogue Ajouter un lecteur de bande. Cliquez ensuite sur **Ajouter un lecteur de bande**.
   - Interface de ligne de commande :

     Entrez tklmDeviceAdd pour ajouter une unité. Vous devez indiquer le groupe d'unités et le numéro de série. Par exemple, entrez :

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

Utilisez le **Service REST Device Add** pour ajouter une unité. Par exemple, vous pouvez envoyer la demande HTTP suivante :

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

Que faire ensuite

Vous pouvez ensuite déterminer le statut actuel de l'unité que vous avez ajoutée.

Modification d'une unité

Vous pouvez modifier les informations relatives à une unité (par exemple, un lecteur de bande) dans la base de données d'IBM Security Key Lifecycle Manager. Par exemple, vous pouvez mettre à jour la spécification pour un certificat partenaire que l'unité utilise ou spécifier un autre groupe d'unités au sein de la même famille d'unités.

Pourquoi et quand exécuter cette tâche

Avant de commencer, créez les certificats à associer aux unités que vous allez modifier. Si vous utilisez l'interface de ligne de commande, obtenez la valeur de l'identificateur unique universel (UUID) de l'unité que vous souhaitez mettre à jour. Procurez-vous aussi l'alias de tout certificat associé à l'unité.

Vous pouvez utiliser la boîte de dialogue Modifier un lecteur de bande. Vous pouvez également utiliser la commande **tklmDeviceUpdate** ou **Service REST Device Update** pour mettre à jour une unité ou spécifier un autre groupe d'unités au sein de la même famille d'unités. Votre rôle doit avoir un droit d'utilisation de l'action de modification, ainsi qu'un droit d'accès au groupe d'unités approprié.

Procédure

1. Accédez à la page ou au répertoire approprié.
   - Interface graphique :
     a. Connectez-vous à l'interface graphique.
     b. Dans la section Gestion des clés et des unités de la page de bienvenue, sélectionnez **3592**.
     c. Cliquez sur **Aller à** > **Gestion des clés et des unités**.
     d. Vous pouvez aussi cliquer avec le bouton droit sur **3592** et sélectionner **Gestion des clés et des unités**.
     e. Sur la page de gestion pour 3592, sélectionnez une unité dans la colonne **Lecteurs de bande**.
     f. Cliquez sur **Modifier**.
     g. Vous pouvez également faire un clic droit sur une unité et sélectionner **Modifier**, ou bien faire un double clic sur une entrée d'unité.
   - Interface de ligne de commande
     a. Accédez au répertoire *<WAS_HOME>*/bin. Exemple :

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

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

b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme SKLMAdmin. Exemple :

Windows

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

Linux

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

2. Modifiez une unité.
   - Interface graphique :

     Dans la boîte de dialogue Modifier un lecteur de bande, entrez les informations obligatoires et facultatives. Cliquez ensuite sur **Modifier un lecteur de bande**.
   - Interface de ligne de commande :

     Tapez tklmDeviceList pour localiser une unité et tklmDeviceUpdate pour mettre à jour une unité. Vous devez indiquer l'identificateur unique universel (UUID) de l'unité, ainsi que les attributs modifiés. Par exemple, entrez :

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

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

     Utilisez **Service REST Device List** et **Service REST Device Update** respectivement pour rechercher et mettre à jour une unité. Par exemple, vous pouvez envoyer les demandes HTTP suivantes :

     ```
     GET https://localhost:<port>/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:<port>/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"}
     ```

Que faire ensuite

Vous pouvez ensuite vérifier les modifications apportées. Pour les champs optionnels tels que la description, vous voudrez peut-être exécuter la commande **tklmDeviceList** ou **Service REST Device List** pour déterminer si leur valeur a été modifiée. Vous pouvez également rouvrir la boîte de dialogue Modifier un lecteur de bande.

Suppression d'une unité

Vous pouvez supprimer une unité, telle qu'un lecteur de bande. Les métadonnées relatives à l'unité que vous supprimez, telles que son numéro de série, sont supprimées de la base de données IBM Security Key Lifecycle Manager.

Pourquoi et quand exécuter cette tâche

Avant de commencer, assurez-vous que vous disposez d'une sauvegarde actualisée des certificats et des unités sur le site. Procurez-vous l'identificateur unique universel (UUID) de l'unité à supprimer.

Vous pouvez utiliser l'option de menu Supprimer, la commande **tklmDeviceDelete** ou **Service REST Device Delete** pour supprimer une unité. Votre rôle doit avoir un droit d'utilisation de l'action de suppression, ainsi qu'un droit d'accès au groupe d'unités approprié.

Procédure

1. Accédez à la page ou au répertoire approprié.
   - Interface graphique :
     a. Connectez-vous à l'interface graphique.
     b. Dans la section Gestion des clés et des unités de la page de bienvenue, sélectionnez **3592**.
     c. Cliquez sur **Aller à** > **Gestion des clés et des unités**.
     d. Vous pouvez aussi cliquer avec le bouton droit sur **3592** et sélectionner **Gestion des clés et des unités**.
     e. Sur la page de gestion pour 3592, sélectionnez une unité.
     f. Cliquez sur **Supprimer**.
     g. Vous pouvez également cliquer avec le bouton droit de la souris sur une unité, puis sélectionner **Supprimer**.
   - Interface de ligne de commande
     a. Accédez au répertoire <*WAS_HOME*>/bin. Exemple :

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

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

     b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme SKLMAdmin. Exemple :

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

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

2. Supprimez l'unité :
   - Interface graphique :

     Lisez le message de confirmation de la boîte de dialogue correspondante pour vérifier que vous avez sélectionné l'unité appropriée avant de la supprimer. Les métadonnées relatives à l'unité que vous supprimez, telles que son numéro de série, sont supprimées de la base de données IBM Security Key Lifecycle Manager.

     Cliquez ensuite sur **OK**.
   - Interface de ligne de commande :

     Tapez tklmDeviceList pour localiser une unité et tklmDeviceDelete pour supprimer une unité. Vous devez indiquer l'identificateur unique universel (UUID). Par exemple, entrez :

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

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

     Utilisez **Service REST Device List** et **Service REST Device Delete** respectivement pour rechercher et supprimer une unité. Par exemple, vous pouvez envoyer les demandes HTTP suivantes :

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

Gestion d'images de stockage DS8000

Vous pouvez gérer des images de stockage DS8000 à l'aide d'IBM Security Key Lifecycle Manager.

Les descriptions de certaines étapes proposent d'utiliser l'interface graphique, l'interface de ligne de commande ou l'interface REST. Veillez à ne pas changer d'interface au cours d'une même session de travail.

Les descriptions de certaines tâches peuvent mentionner des propriétés contenues dans le fichier `SKLMConfig.properties`. Utilisez l'interface graphique, l'interface de ligne de commande ou l'interface REST pour modifier ces propriétés.

Etapes guidées pour la création d'images de stockage et de certificats d'images

Lorsque vous créez ou ajoutez des images de stockage et des certificats d'images, IBM Security Key Lifecycle Manager fournit à chaque fois un ensemble d'étapes guidées pour vous aider à accomplir la tâche.

La description de certaines étapes mentionne parfois la possibilité d'accomplir la même tâche en utilisant l'interface de ligne de commande. Dans un ensemble de tâches détaillées, utilisez l'interface utilisateur graphique pour effectuer les tâches.

Création d'un certificat d'image ou d'une demande de certificat

Dans un premier temps, créez des certificats d'image ou des demandes de certificat pour IBM Security Key Lifecycle Manager.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser la boîte de dialogue Créer un certificat. Vous pouvez également utiliser l'une des commandes ou des services REST suivants pour créer des certificats ou des demandes de certificat :

- **`tklmCertCreate`** ou **`tklmCertGenRequest`**
- **`Service REST Create Certificate`** ou **`Service REST Certificate Generate Request`**

Votre rôle doit avoir un droit d'utilisation de l'action de création, ainsi qu'un droit d'accès au groupe d'unités approprié. Pour désigner ce certificat comme certificat par défaut, vous devez également avoir accès à l'action de modification.

Procédure

1. Accédez à la page ou au répertoire approprié.
   - Interface graphique :
     a. Connectez-vous à l'interface graphique.

b. Dans la section Gestion des clés et des unités de la page de bienvenue, sélectionnez **DS8000**.
c. Cliquez sur **Aller à** > **Création de clés et d'unités en mode guidé**.
d. Vous pouvez aussi cliquer avec le bouton droit sur **DS8000** et sélectionner **Création de clés et d'unités en mode guidé**.

- Interface de ligne de commande
  a. Accédez au répertoire <*WAS_HOME*>/bin. Exemple :

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

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

  b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme SKLMAdmin. Exemple :

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

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

- Interface REST :
  – Ouvrez un client REST.

2. Créez un certificat d'image ou demandez un certificat.
   - Interface graphique :
     a. Sur la page Etape 1 : Créer des certificats, cliquez sur **Créer** dans la table **Certificats**.
     b. Dans la boîte de dialogue Créer un certificat, sélectionnez un certificat autosigné ou une demande de certificat pour un fournisseur tiers.
     c. Indiquez des valeurs pour les paramètres obligatoires et facultatifs.
     d. Cliquez sur **Créer un certificat**.
   - Interface de ligne de commande :
     – Certificat

       Entrez tklmCertCreate pour créer un certificat et une paire de clés publique et privée, et stockez le certificat dans un fichier de clés existant. Par exemple, entrez :

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

     – Demande de certificat

       Entrez tklmCertGenRequest pour créer un fichier de demande de certificat PKCS #10. Par exemple, entrez :

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

   - Interface REST :
     – Certificat
       a. Obtenez un identificateur d'authentification utilisateur unique pour accéder aux services REST d'IBM Security Key Lifecycle Manager. Pour plus d'informations sur le processus d'authentification, voir Processus d'authentification pour les services REST.

b. Pour appeler le **service REST Create Certificate**, envoyez la demande HTTP POST. Transmettez l'identificateur d'authentification utilisateur que vous avez obtenu à l'étape a avec le message de demande, conformément à l'exemple suivant :

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

– Demande de certificat

Utilisez le **service REST Certificate Generate Request** pour créer un fichier de demande de certificat PKCS #10. Par exemple, vous pouvez envoyer la demande HTTP suivante à l'aide d'un client REST :

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

Que faire ensuite

Passez à l'étape suivante pour définir des images de stockage spécifiques et leur associer des certificats. Sélectionnez **Etape 2 : Identifier les images** ou cliquez sur **Passer à l'étape suivante**.

Identification des images de stockage

Identifiez une image de stockage (unité) afin de l'utiliser avec IBM Security Key Lifecycle Manager. Avant de commencer, créez les certificats d'image à associer aux images de stockage que vous allez identifier.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser la boîte de dialogue Ajouter une image de stockage. Une image de stockage peut également être ajoutée à l'aide de la commande **tklmDeviceAdd** ou de **Service REST Device Add**.

Vous pouvez effectuer les choix suivants pour fournir des clés à des unités :

Accepter uniquement les unités ajoutées manuellement pour la communication
Les unités entrantes ne sont pas systématiquement ajoutées au magasin de données. Vous devez spécifier manuellement, pour chaque unité, si des clés lui seront servies ou non.

Retenir les demandes des nouvelles unités en attente de mon approbation
Toutes les unités entrantes d'un groupe d'unités valide sont ajoutées au magasin de données, mais lorsqu'elles demandent des clés, celles-ci ne leur sont pas servies automatiquement. Vous devez accepter ou rejeter chaque unité dans la liste des unités en attente, en fonction de quoi des clés lui sont servies ou non lorsqu'elle en fait la demande.

Accepter automatiquement toutes les demandes des nouvelles unités pour la communication
Toutes les nouvelles unités entrantes d'un groupe d'unités valide sont

ajoutées au magasin de données et, lorsqu'elles demandent des clés, celles-ci leur sont servies automatiquement.

Remarque : N'utilisez pas cette option si vous comptez déplacer la nouvelle unité vers un autre groupe d'unités. Sélectionnez plutôt le mode d'approbation manuel ou avec mise en attente pour que l'occasion vous soit donnée de transférer l'unité dans le groupe approprié avant que des clés ne lui soient servies.

Procédure

1. Accédez à la page ou au répertoire approprié.
   - Interface graphique :

     Connectez-vous à l'interface graphique. Dans l'arborescence de navigation, cliquez sur **IBM Security Key Lifecycle Manager >Bienvenue**. Faites défiler la page jusqu'à la section de gestion des clés et des unités. Dans **Création de clés et d'unités en mode guidé**, sélectionnez **DS8000**. Cliquez ensuite sur **Aller**.

     a. Connectez-vous à l'interface graphique.
     b. Dans la section Gestion des clés et des unités de la page de bienvenue, sélectionnez **DS8000**.
     c. Cliquez sur **Aller à** > **Création de clés et d'unités en mode guidé**.
     d. Vous pouvez aussi cliquer avec le bouton droit sur **DS8000** et sélectionner **Création de clés et d'unités en mode guidé**.
   - Interface de ligne de commande

     a. Accédez au répertoire *<WAS_HOME>*/bin. Exemple :

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

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

     b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme SKLMAdmin. Exemple :

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

        Linux
        ```
        ./wsadmin.sh -username SKLMAdmin
        -password mypwd -lang jython
        ```
   - Interface REST :
     – Ouvrez un client REST.
2. Ignorez la page **Etape 1 : Créer des certificats**. Cliquez sur **Passer à l'étape suivante** ou sur **Etape 2 : Identifier les unités**.
3. Vous pouvez demander que toutes les unités entrantes soient ajoutées à une liste d'attente et que des clés ne leur soient pas servies automatiquement lorsqu'elles en font la demande. Vous devez accepter ou rejeter chaque unité dans la liste des unités en attente avant que IBM Security Key Lifecycle Manager ne commence à lui servir des clés lorsqu'elle en fait la demande. Votre rôle doit avoir un droit d'utilisation de l'action de modification, ainsi qu'un droit d'accès au groupe d'unités approprié.
   - Interface graphique :

     Sélectionnez **Retenir les demandes des nouvelles unités en attente de mon approbation**.
   - Interface de ligne de commande :

Utilisez la commande **tklmDeviceGroupAttributeUpdate** ou le **service REST Device Group Attribute Update** pour définir la valeur de l'attribut **device.AutoPendingAutoDiscovery**. Par exemple, entrez :

```
print AdminTask.tklmDeviceGroupAttributeUpdate ('[-name DS8000
  -attributes "{device.AutoPendingAutoDiscovery 2}"]')
```

- Interface REST :
  a. Obtenez un identificateur d'authentification utilisateur unique pour accéder aux services REST d'IBM Security Key Lifecycle Manager. Pour plus d'informations sur le processus d'authentification, voir Processus d'authentification pour les services REST.
  b. Pour exécuter le **service REST Device Group Attribute Update** et définir la valeur de l'attribut **device.AutoPendingAutoDiscovery**, envoyez la demande HTTP PUT. Transmettez l'identificateur d'authentification utilisateur que vous avez obtenu à l'étape a avec le message de demande, conformément à l'exemple suivant :

```
PUT https://localhost:<port>/SKLM/rest/v1/deviceGroupAttributes
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth authId=139aeh34567m
{"name":"DS8000","attributes":"device.AutoPendingAutoDiscovery 2"}
```

4. Ajoutez une image de stockage.
   - Interface graphique :
     a. Dans la page Etape 2 : Identifier les images de stockage de la table, cliquez sur **Ajouter**.
     b. Dans la boîte de dialogue Ajouter une image de stockage, entrez les informations obligatoires et facultatives.
     c. Cliquez sur **Ajouter une image de stockage**.
   - Interface de ligne de commande :

     Entrez tklmDeviceAdd pour ajouter une image de stockage. Vous devez spécifier le type d'image de stockage, le numéro de série et un certificat d'image. Par exemple, entrez :

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

   - Interface REST :

     Vous pouvez utiliser le **service REST Device Add** pour ajouter une image de stockage. Par exemple, vous pouvez envoyer la demande HTTP suivante à l'aide d'un client REST :

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

Que faire ensuite

Vous pouvez ensuite importer le certificat signé. Sinon, utilisez la page Gestion des clés et des unités pour voir toutes les images de stockage et tous les certificats d'image.

Administration d'images de stockage et de certificats d'images

Pour administrer des images de stockage et des certificats d'image, vous voudrez peut-être déterminer leur statut actuel. Vous pouvez mapper leur association ou ajouter, modifier ou supprimer des certificats ou des images de stockage spécifiques.

Pourquoi et quand exécuter cette tâche

Avant de commencer, examinez les colonnes de la page, qui comprend des boutons permettant d'ajouter, de modifier ou de supprimer un élément de la table. Pour trier les informations, cliquez sur un en-tête de colonne.

Utilisez la page Gestion des clés et des unités DS8000 pour mapper des certificats d'image à des images de stockage et pour déterminer le statut des éléments contenus dans la table. Vous pouvez ajouter, modifier ou supprimer des certificats ou des images de stockage spécifiques. Votre rôle doit avoir un droit d'utilisation de l'action de visualisation, ainsi qu'un droit d'accès au groupe d'unités approprié.

La table est organisée selon les zones suivantes :

- Dans les colonnes de gauche, informations sur les certificats indiquant le nom, la date d'expiration et le statut actuel de chaque certificat.
- Dans les colonnes de droite, informations sur les images de stockage indiquant le nom de chaque image et le certificat d'image associé.
- Icônes de statut indiquant le statut de chaque certificat.

Tableau 4. Icônes de statut et signification

Icône	Description
	Le certificat est actif.
	Le certificat est dans un état compromis.
	Le certificat arrive bientôt à expiration.
	Le certificat est arrivé à expiration.
	Certificat valide à une date ultérieure ; concerne les certificats migrés dont l'horodatage spécifie une date d'utilisation à venir.
	IBM Security Key Lifecycle Manager a des demandes de certificat de fournisseur tiers en attente de signature et d'importation.

Procédure

1. Connectez-vous à l'interface graphique.
   a. Dans la section Gestion des clés et des unités de la page de bienvenue, sélectionnez **DS8000**.
   b. Cliquez sur **Aller à** > **Gestion des clés et des unités**.
   c. Vous pouvez aussi cliquer avec le bouton droit sur **DS8000** et sélectionner **Gestion des clés et des unités**.

Les descriptions de certaines étapes proposent d'utiliser l'interface graphique, l'interface de ligne de commande ou l'interface REST. Veillez à ne pas changer d'interface au cours d'une même session de travail.

Les descriptions de certaines tâches peuvent mentionner des propriétés contenues dans le fichier `SKLMConfig.properties`. Utilisez l'interface graphique, l'interface de ligne de commande ou l'interface REST pour modifier ces propriétés.

2. Sur la page Gestion des clés et des unités DS8000, vous pouvez ajouter, modifier ou supprimer une image de stockage ou un certificat d'image.

   Vous pouvez effectuer les tâches administratives suivantes :

   - Ajouter

     Cliquez sur **Ajouter**. Vous pouvez également sélectionner un processus pas à pas pour créer des certificats et des images de stockage.

     – Certificat

       Sur la page Créer un certificat, sélectionnez le type de certificat (autosigné ou demande envoyée par un fournisseur tiers) et renseignez les informations requises. Cliquez ensuite sur **Créer un certificat**. Votre rôle doit avoir un droit d'utilisation de l'action de création, ainsi qu'un droit d'accès au groupe d'unités approprié. Pour désigner ce certificat comme certificat par défaut, vous devez également avoir accès à l'action de modification.

     – Image mémoire

       Entrez les informations relatives à l'image de stockage sur la page Ajouter une image de stockage. Cliquez ensuite sur **Ajouter une image de stockage**. Votre rôle doit avoir un droit d'utilisation de l'action de création, ainsi qu'un droit d'accès au groupe d'unités approprié.

     – Créez des certificats et images de stockage à l'aide du processus pas à pas

       Entrez les informations requises sur les pages Etape 1 : Créer des certificats et Etape 2 : Identifier les images.

     L'indication de réussite varie, reflétant le changement dans la colonne dédiée au certificat ou à l'image de stockage.

   - Modifier

     Pour modifier les informations relatives à une image de stockage ou afficher celles relatives à un certificat, sélectionnez un certificat ou une image de stockage, puis cliquez sur **Modifier**. Vous pouvez également cliquer avec le bouton droit de la souris sur l'image de stockage ou le certificat sélectionné. Cliquez ensuite sur **Modifier** ou cliquez deux fois sur l'entrée de l'image de stockage ou du certificat.

     – Certificat

       Affichez des informations en lecture seule dans la page Modifier un certificat. Votre rôle doit avoir un droit d'utilisation de l'action de modification, ainsi qu'un droit d'accès au groupe d'unités approprié.

     – Image mémoire

       Spécifiez les modifications effectuées dans la page Modifier une image de stockage. Cliquez ensuite sur **Modifier une image de stockage**. Votre rôle doit avoir un droit d'utilisation de l'action de modification, ainsi qu'un droit d'accès au groupe d'unités approprié.

     L'indication de réussite varie, reflétant le changement dans la colonne dédiée au certificat ou à l'image de stockage. Il se peut que les modifications apportées à certaines informations, telles que les zones facultatives, ne figurent pas dans la table.

- Supprimer

  Pour supprimer un certificat ou une image de stockage, assurez-vous de sélectionner le certificat ou l'image de stockage approprié. Cliquez ensuite sur **Supprimer**. Vous pouvez également cliquer avec le bouton droit de la souris sur l'image de stockage ou le certificat sélectionné. Cliquez ensuite sur **Supprimer**.

  – Certificat

    Vérifiez que vous disposez d'une sauvegarde actualisée du magasin de clés avant de supprimer un certificat. Une fois le certificat supprimé, toute image de stockage écrite à l'aide de ce certificat deviendra illisible. Le certificat à supprimer peut présenter n'importe quel statut ; il peut, par exemple, être actif. Quel que soit le statut, vous ne pouvez pas supprimer un certificat qui est :

    - Associé à une image de stockage.
    - Marqué par une unité DS8000 Turbo comme certificat principal ou secondaire d'une image.

    La suppression d'un certificat entraîne la suppression des éléments associés dans la base de données.

    Pour confirmer la suppression, cliquez sur **OK**. Votre rôle doit avoir un droit d'utilisation de l'action de suppression, ainsi qu'un droit d'accès au groupe d'unités approprié.

  – Image mémoire

    Les métadonnées relatives à l'image de stockage que vous supprimez, telles que le numéro de série, sont supprimées de la base de données IBM Security Key Lifecycle Manager. Pour confirmer la suppression, cliquez sur **OK**. Votre rôle doit avoir un droit d'utilisation de l'action de suppression, ainsi qu'un droit d'accès au groupe d'unités approprié.

  Pour savoir si l'opération a réussi, vérifiez que le certificat ou l'image de stockage a été supprimé de la table d'administration.

Ajout d'un certificat d'image ou d'une demande de certificat

Vous pouvez ajouter d'autres certificats d'image ou demandes de certificat à utiliser avec IBM Security Key Lifecycle Manager. Avant de commencer, déterminez la stratégie de votre site concernant l'utilisation des certificats.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser la boîte de dialogue Créer un certificat. Vous pouvez également utiliser l'une des commandes ou des services REST suivants pour créer des certificats ou des demandes de certificat :

- **`tklmCertCreate`** ou **`tklmCertGenRequest`**
- **`Service REST Create Certificate`** ou **`Service REST Certificate Generate Request`**

Votre rôle doit avoir un droit d'utilisation de l'action de création, ainsi qu'un droit d'accès au groupe d'unités approprié. Pour désigner ce certificat comme certificat par défaut, vous devez également avoir accès à l'action de modification.

Procédure

1. Accédez à la page ou au répertoire approprié.
   - Interface graphique :
     a. Connectez-vous à l'interface graphique.

b. Dans la section Gestion des clés et des unités de la page de bienvenue, sélectionnez **DS8000**.
c. Cliquez sur **Aller à** > **Gestion des clés et des unités**.
d. Vous pouvez aussi cliquer avec le bouton droit sur **DS8000** et sélectionner **Gestion des clés et des unités**.
e. Sur la page de gestion pour DS8000, cliquez sur **Ajouter**.
f. Cliquez sur **Certificat**.

- Interface de ligne de commande
  a. Accédez au répertoire <*WAS_HOME*>/bin. Exemple :

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

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

  b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme SKLMAdmin. Exemple :

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

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

2. Créez ou demandez un certificat.
   - Interface graphique :
     a. Sur la page Créer un certificat, sélectionnez un certificat autosigné ou une demande de certificat associée à un fournisseur tiers.
     b. Indiquez des valeurs pour les paramètres obligatoires et facultatifs. Cliquez ensuite sur **Créer un certificat**.
   - Interface de ligne de commande :
     – Certificat :

       Entrez la commande tklmCertCreate pour créer un certificat et une paire de clés publique et privée, puis stockez le certificat dans un magasin de clés existant. Par exemple, entrez :

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

     – Demande de certificat :

       Entrez tklmCertGenRequest pour créer un fichier de demande de certificat PKCS #10. Par exemple, entrez :

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

   - Interface REST :
     – Certificat

       Utilisez **Service REST Create Certificate** pour créer un certificat et une paire de clés publique et privée, puis stockez le certificat dans un magasin de clés existant. Par exemple, vous pouvez envoyer la demande HTTP suivante à l'aide d'un client REST :

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

– Demande de certificat

Utilisez **Service REST Certificate Generate Request** pour créer un fichier de demande de certificat PKCS #10. Par exemple, vous pouvez envoyer la demande HTTP suivante à l'aide d'un client REST :

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

Que faire ensuite

La prochaine action varie selon que vous avez créé un certificat ou une demande de certificat.

- Certificat :

  Vous pouvez associer un certificat à une image de stockage spécifique.

- Demande de certificat :

  Envoyez manuellement la demande de certificat à une autorité de certification. Au retour du certificat signé, importez-le à l'aide d'un élément d'action en attente sur le panneau d'accueil ou à l'aide de la commande **tklmCertImport** ou de **Service REST Certificate Import**.

Modification d'un certificat d'image

Vous pouvez utiliser l'interface graphique pour consulter, sans possibilité de les modifier, les informations relatives à un certificat d'image dans la base de données d'IBM Security Key Lifecycle Manager. En utilisant l'interface de ligne de commande ou l'interface REST, vous pouvez consulter ces informations, mais aussi modifier certains de leurs attributs.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser la boîte de dialogue Modifier un certificat pour modifier un certificat. Vous pouvez également utiliser les commandes ou services REST suivants :

- **tklmCertUpdate** ou **Service REST Certificate Update** pour modifier l'état d'un certificat (par exemple, le désigner comme certificat de confiance ou compromis) et pour modifier les informations d'un certificat.
- **tklmDeviceTypeAttributeUpdate** ou **Service REST Device Type Attribute Update** pour désigner un certificat comme certificat principal ou secondaire.

Votre rôle doit avoir un droit d'utilisation de l'action de modification, ainsi qu'un droit d'accès au groupe d'unités approprié.

Remarque : Les changements que vous apportez à la base de données d'IBM Security Key Lifecycle Manager sont configurés sur l'unité DS8000 Turbo lorsque celle-ci contacte IBM Security Key Lifecycle Manager.

Procédure

1. Accédez à la page ou au répertoire approprié.
   - Interface graphique :
     a. Connectez-vous à l'interface graphique.
     b. Dans la section Gestion des clés et des unités de la page de bienvenue, sélectionnez **DS8000**.
     c. Cliquez sur **Aller à** > **Gestion des clés et des unités**.
     d. Vous pouvez aussi cliquer avec le bouton droit sur **DS8000** et sélectionner **Gestion des clés et des unités**.
     e. Sur la page de gestion pour DS8000, sélectionnez un certificat dans la colonne **Certificats**.
     f. Cliquez sur **Modifier**.
     g. Vous pouvez également faire un clic droit sur un certificat et sélectionner **Modifier**, ou bien faire un double clic sur une entrée de certificat.
   - Interface de ligne de commande
     a. Accédez au répertoire *<WAS_HOME>*/bin. Exemple :

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

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

     b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme SKLMAdmin. Exemple :

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

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

2. Affichez (interface graphique) ou modifiez (interface de ligne de commande) les informations de certificat.
   - Interface graphique :

     Dans la boîte de dialogue Modifier un certificat, affichez les zones en lecture seule.
   - Interface de ligne de commande :

     Tapez tklmCertList pour rechercher un certificat et tklmCertUpdate pour mettre à jour un certificat. Vous devez indiquer l'identificateur unique universel (UUID) du certificat, ainsi que l'attribut modifié. Par exemple, pour modifier les informations, entrez :

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

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

     Utilisez **Service REST Certificate List** pour rechercher un certificat. Par exemple, vous pouvez envoyer la demande HTTP suivante :

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

Utilisez **Service REST Certificate Update** pour mettre à jour un certificat. Par exemple, vous pouvez envoyer la demande HTTP suivante :

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

Que faire ensuite

Vous pouvez ensuite utiliser la page Gestion des clés et des unités DS8000 pour associer des certificats d'image à des images de stockage spécifiques.

Suppression d'un certificat d'image

Vous pouvez être amené à supprimer un certificat d'image sélectionné, lequel peut avoir n'importe quel statut (actif, par exemple). Vous ne pouvez pas supprimer un certificat associé à une image de stockage. Vous ne pouvez pas non plus supprimer un certificat qui est identifié comme certificat principal ou secondaire d'une image. Vous pouvez, par exemple, supprimer un certificat arrivé à expiration.

Pourquoi et quand exécuter cette tâche

Avant de commencer, assurez-vous que vous disposez d'une sauvegarde du magasin de clés contenant le certificat d'image à supprimer. Vérifiez que le certificat n'est associé à aucune image de stockage. Déterminez l'état actuel du certificat et assurez-vous que la suppression d'un certificat dans cet état est conforme à la politique de votre site.

Ne supprimez des certificats que lorsque les données qu'ils protègent ne sont plus utiles. Leur suppression a en effet les mêmes conséquences que l'effacement des données en question. Une fois les certificats supprimés, les données protégées ne sont plus récupérables.

Vous pouvez utiliser l'option de menu Supprimer, la commande **tklmCertDelete** ou **Service REST Delete Certificate** pour supprimer le certificat d'image sélectionné. Votre rôle doit avoir un droit d'utilisation de l'action de suppression, ainsi qu'un droit d'accès au groupe d'unités approprié.

La suppression d'un certificat entraîne la suppression des éléments associés dans la base de données.

Procédure

1. Accédez à la page ou au répertoire approprié.
   - Interface graphique :
     a. Connectez-vous à l'interface graphique.
     b. Dans la section Gestion des clés et des unités de la page de bienvenue, sélectionnez **DS8000**.
     c. Cliquez sur **Aller à** > **Gestion des clés et des unités**.
     d. Vous pouvez aussi cliquer avec le bouton droit sur **DS8000** et sélectionner **Gestion des clés et des unités**.
     e. Sur la page de gestion pour DS8000, sélectionnez un certificat dans la colonne **Certificats**.
     f. Cliquez sur **Supprimer**.

g. Vous pouvez également cliquer avec le bouton droit de la souris sur un certificat, puis sélectionner **Supprimer**.

- Interface de ligne de commande

a. Accédez au répertoire *<WAS_HOME>*/bin. Exemple :

Windows

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

Linux

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

b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme SKLMAdmin. Exemple :

Windows

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

Linux

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

2. Supprimez le certificat.

- Interface graphique :

  Lisez le message de confirmation dans la boîte de dialogue correspondante afin de vérifier que vous avez sélectionné le certificat approprié avant de le supprimer. Cliquez ensuite sur **OK**.

- Interface de ligne de commande :

  Tapez tklmCertList pour rechercher un certificat et tklmCertDelete pour supprimer un certificat. Vous devez spécifier l'alias du certificat, ainsi que le nom du magasin de clés. Par exemple, pour supprimer un certificat arrivé à expiration et qui n'est associé à aucune image de stockage, entrez :

```
print AdminTask.tklmCertList('[-usage DS8000 -v y]')
```

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

- Interface REST :

  Utilisez **Service REST Certificate List** et **Service REST Delete Certificate** respectivement pour rechercher et supprimer un certificat. Par exemple, vous pouvez envoyer les demandes HTTP suivantes :

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

Que faire ensuite

Vous pouvez ensuite être amené à sauvegarder de nouveau le magasin de clés afin de refléter précisément les modifications apportées aux certificats.

Ajout d'une image de stockage

Vous pouvez ajouter une image de stockage à la base de données IBM Security Key Lifecycle Manager. Avant de commencer, créez les certificats à associer aux images de stockage que vous allez identifier. Procurez-vous également le numéro de série de l'image de stockage, ainsi que d'autres informations descriptives.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser la boîte de dialogue Ajouter une image de stockage, la commande **tklmDeviceAdd** ou **Service REST Device Add** pour ajouter une image de stockage. Votre rôle doit avoir un droit d'utilisation de l'action de création, ainsi qu'un droit d'accès au groupe d'unités approprié.

Procédure

1. Accédez à la page ou au répertoire approprié.
   - Interface graphique :
     a. Connectez-vous à l'interface graphique.
     b. Dans la section Gestion des clés et des unités de la page de bienvenue, sélectionnez **DS8000**.
     c. Cliquez sur **Aller à** > **Gestion des clés et des unités**.
     d. Vous pouvez aussi cliquer avec le bouton droit sur **DS8000** et sélectionner **Gestion des clés et des unités**.
     e. Sur la page de gestion pour DS8000, cliquez sur **Ajouter**.
     f. Cliquez sur **Image de stockage**.
   - Interface de ligne de commande
     a. Accédez au répertoire <*WAS_HOME*>/bin. Exemple :

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

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

     b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme SKLMAdmin. Exemple :

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

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

2. Ajoutez une image de stockage.
   - Interface graphique :

     Dans la boîte de dialogue Ajouter une image de stockage, entrez les informations obligatoires et facultatives. Cliquez ensuite sur **Ajouter une image de stockage**.
   - Interface de ligne de commande :

     Entrez la commande tklmDeviceAdd pour ajouter une image de stockage. Vous devez indiquer le type d'image de stockage, le numéro de série et un certificat d'image. Par exemple, entrez :

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

     Utilisez **Service REST Device Add** pour ajouter une image de stockage. Par exemple, vous pouvez envoyer la demande HTTP suivante :

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

Que faire ensuite

Vous pouvez ensuite déterminer le statut actuel de l'image de stockage que vous avez ajoutée.

Modification d'une image de stockage

Vous pouvez modifier les informations concernant une image de stockage dans la base de données d'IBM Security Key Lifecycle Manager. Vous pouvez, par exemple, mettre à jour la description de l'image de stockage.

Pourquoi et quand exécuter cette tâche

Avant de commencer, créez les certificats à associer aux images de stockage que vous allez modifier. Si vous utilisez l'interface de ligne de commande, obtenez la valeur de l'identificateur unique universel (UUID) de l'image de stockage que vous souhaitez mettre à jour et l'alias du certificat qui lui est associé.

Vous pouvez utiliser la boîte de dialogue Modifier une image de stockage, la commande **tklmDeviceUpdate** ou **Service REST Device Update** pour mettre à jour une image de stockage. Votre rôle doit avoir un droit d'utilisation de l'action de modification, ainsi qu'un droit d'accès au groupe d'unités approprié.

Procédure

1. Accédez à la page ou au répertoire approprié.
   - Interface graphique :
     a. Connectez-vous à l'interface graphique.
     b. Dans la section Gestion des clés et des unités de la page de bienvenue, sélectionnez **DS8000**.
     c. Cliquez sur **Aller à** > **Gestion des clés et des unités**.
     d. Vous pouvez aussi cliquer avec le bouton droit sur **DS8000** et sélectionner **Gestion des clés et des unités**.
     e. Sur la page de gestion pour DS8000, sélectionnez une unité.
     f. Cliquez sur **Modifier**.
     g. Vous pouvez également faire un clic droit sur une unité et sélectionner **Modifier**, ou bien faire un double clic sur une entrée d'unité.
   - Interface de ligne de commande
     a. Accédez au répertoire <*WAS_HOME*>/bin. Exemple :

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

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

     b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme SKLMAdmin. Exemple :

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

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

2. Modifiez une image de stockage.

- Interface graphique :

  Dans la boîte de dialogue Modifier une image de stockage, entrez les changements voulus. Cliquez ensuite sur **Modifier une image de stockage**.
- Interface de ligne de commande :

  Entrez `tklmDeviceUpdate` pour mettre à jour une image de stockage. Vous devez indiquer l'identificateur unique universel (UUID) de l'image de stockage, ainsi que les attributs à modifier. Par exemple, entrez :

  ```
  print AdminTask.tklmDeviceUpdate
   ('[-uuid DEVICE-15d499ad-3ad8-3333-8c84-64cb9e11d990
    -attributes "{description myDevice}"]')
  ```
- Interface REST :

  Utilisez **Service REST Device Update** pour mettre à jour une image de stockage. Par exemple, vous pouvez envoyer la demande HTTP suivante :

  ```
  PUT https://localhost:<port>/SKLM/rest/v1/devices
  Content-Type: application/json
  Accept : application/json
  Authorization: SKLMAuth authId=139aeh34567m
  {"uuid":"DEVICE-15d499ad-3ad8-3333-8c84-64cb9e11d990","attributes":
  "description monUnité"}
  ```

Suppression d'une image de stockage

Vous pouvez supprimer une image de stockage. Les métadonnées de l'image de stockage que vous supprimez, telles que son numéro de série, sont supprimées de la base de données de IBM Security Key Lifecycle Manager.

Pourquoi et quand exécuter cette tâche

Avant de commencer, assurez-vous que vous disposez d'une sauvegarde actualisée des certificats et images de stockage sur le site. Si vous utilisez l'interface de ligne de commande, procurez-vous l'identificateur unique universel (UUID) de l'image de stockage à supprimer.

Vous pouvez utiliser l'option de menu Supprimer, la commande **tklmDeviceDelete** ou **Service REST Device Delete** pour supprimer une image de stockage. Votre rôle doit avoir un droit d'utilisation de l'action de suppression, ainsi qu'un droit d'accès au groupe d'unités approprié.

Procédure

1. Accédez à la page ou au répertoire approprié.
   - Interface graphique :
     a. Connectez-vous à l'interface graphique.
     b. Dans la section Gestion des clés et des unités de la page de bienvenue, sélectionnez **DS8000**.
     c. Cliquez sur **Aller à** > **Gestion des clés et des unités**.
     d. Vous pouvez aussi cliquer avec le bouton droit sur **DS8000** et sélectionner **Gestion des clés et des unités**.
     e. Sur la page de gestion pour `DS8000`, sélectionnez une unité.
     f. Cliquez sur **Supprimer**.
     g. Vous pouvez également cliquer avec le bouton droit de la souris sur une unité, puis sélectionner **Supprimer**.
   - Interface de ligne de commande
     a. Accédez au répertoire *<WAS_HOME>*`/bin`. Exemple :

Windows

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

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

b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme SKLMAdmin. Exemple :

Windows

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

Linux

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

2. Supprimez l'image de stockage.
   - Interface graphique :

     Dans la page de confirmation, lisez le message de confirmation afin de vous assurer d'avoir sélectionné l'image de stockage appropriée avant de la supprimer. Les métadonnées relatives à l'image de stockage que vous supprimez, telles que le numéro de série, sont supprimées de la base de données IBM Security Key Lifecycle Manager.

     Cliquez ensuite sur **OK**.
   - Interface de ligne de commande :

     Tapez tklmDeviceList pour localiser une unité et tklmDeviceDelete pour supprimer une image de stockage. Vous devez indiquer son identificateur unique universel (UUID). Par exemple, entrez :

     ```
     print AdminTask.tklmDeviceList ('[-type DS8000]')
     ```

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

     Utilisez **Service REST Device List** pour localiser une unité et **Service REST Device Delete** pour supprimer une image de stockage. Par exemple, vous pouvez envoyer les demandes HTTP suivantes :

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

Gestion de DS5000

Vous pouvez gérer des serveurs de stockage DS5000 à l'aide d'IBM Security Key Lifecycle Manager.

Administration d'unités, de clés et d'associations d'unités

Pour administrer les serveurs de stockage DS5000, vous mappez une unité à des clés ou des machines.

Pourquoi et quand exécuter cette tâche

Votre rôle doit avoir un droit d'utilisation de l'action de visualisation, ainsi qu'un droit d'accès au groupe d'unités approprié. Utilisez la page Gestion des clés et des

unités DS5000 pour ajouter, modifier ou supprimer une unité, une clé ou une association. Ces actions requièrent des droits supplémentaires.

Avant de commencer, examinez les colonnes de la page, qui comprend des boutons permettant d'ajouter, de modifier ou de supprimer un élément de la table. Pour trier les informations, cliquez sur un en-tête de colonne.

La table est organisée selon les zones d'informations suivantes :

- Les unités et les éventuelles machines associées.
- La clé actuellement utilisée par l'unité et une description de l'unité.

Procédure

1. Connectez-vous à l'interface graphique.
   a. Dans la section Gestion des clés et des unités de la page de bienvenue, sélectionnez **DS5000**.
   b. Cliquez sur **Aller à** > **Gestion des clés et des unités**.
   c. Vous pouvez aussi cliquer avec le bouton droit sur **DS5000** et sélectionner **Gestion des clés et des unités**.

   Les descriptions de certaines étapes proposent d'utiliser l'interface graphique, l'interface de ligne de commande ou l'interface REST. Veillez à ne pas changer d'interface au cours d'une même session de travail.

   Les descriptions de certaines tâches peuvent mentionner des propriétés contenues dans le fichier `SKLMConfig.properties`. Utilisez l'interface graphique, l'interface de ligne de commande ou l'interface REST pour modifier ces propriétés.
2. Vous pouvez ajouter, modifier ou supprimer une unité, une clé ou une association de machine.

   Vous pouvez effectuer les tâches administratives suivantes :

   - Actualiser la liste

     Cliquez sur l'icône de régénération  pour actualiser les éléments de la table.
   - Ajouter

     Cliquez sur **Ajouter**.
     – Unité

       Dans la boîte de dialogue Ajouter une unité, entrez le numéro de série de l'unité et d'autres informations. Cliquez ensuite sur **Ajouter une unité**. Votre rôle doit avoir un droit d'utilisation de l'action de création, ainsi qu'un droit d'accès au groupe d'unités approprié.
     – Ajouter des clés

       Sélectionnez une unité, puis choisissez **Ajouter > Ajouter des clés**. Dans la boîte de dialogue Ajouter une clé, indiquez les informations nécessaires, telles que le nombre de clés à créer, sans dépasser 12. Cliquez ensuite sur **Ajouter > Ajouter des clés**. Votre rôle doit avoir un droit d'utilisation de l'action de création, ainsi qu'un droit d'accès au groupe d'unités approprié.
     – Association

       Lorsque vous sélectionnez la case à cocher **Affinité machine** dans la page Gestion des clés et des unités, la propriété **`device.enableMachineAffinity`** a pour valeur true. L'utilisation de l'affinité machine vous permet de limiter le service de clés à des combinaisons spécifiques d'unités et de machines.

Lorsque l'affinité machine est activée, utilisez la boîte de dialogue Ajouter une association pour spécifier les informations nécessaires telles que l'ID machine. Cliquez ensuite sur **Ajouter une association**. Votre rôle doit avoir un droit d'utilisation de l'action de création, ainsi qu'un droit d'accès au groupe d'unités approprié.

L'indication de réussite de l'opération varie selon que vous ajoutez une unité, des clés ou une association.

- Modifier

  Pour changer une unité ou des clés, sélectionnez l'unité et cliquez sur **Modifier**. Vous pouvez également faire un clic droit sur l'unité préalablement sélectionnée. Après quoi, cliquez sur l'un des choix proposés, tels que **Modifier une unité**.

  – Unité

    Spécifiez les changements à apporter dans la boîte de dialogue Modifier une unité. Cliquez ensuite sur **Modifier une unité**. Votre rôle doit avoir un droit d'utilisation de l'action de modification, ainsi qu'un droit d'accès au groupe d'unités approprié.

  – Clés

    Sélectionnez une clé dans la boîte de dialogue Modifier des clés. Cliquez ensuite sur **Supprimer**. Votre rôle doit avoir un droit d'utilisation de l'action de suppression, ainsi qu'un droit d'accès au groupe d'unités approprié.

  L'indication de réussite varie, reflétant le changement dans la colonne dédiée à l'unité ou à la clé.

- Supprimer

  Pour supprimer une unité, sélectionnez-la et cliquez sur **Supprimer**. Vous pouvez également faire un clic droit sur l'unité préalablement sélectionnée. Cliquez ensuite sur **Supprimer**. Avant de supprimer l'unité, si elle est associée à une machine existante dans la base de données d'IBM Security Key Lifecycle Manager, utilisez la commande **tklmMachineDeviceDelete** pour supprimer cette association.

  Les métadonnées de l'unité que vous supprimez, telles que son numéro de série, sont supprimées de la base de données de IBM Security Key Lifecycle Manager. Les données de clé sont également supprimées. Pour confirmer la suppression, cliquez sur **OK**. Votre rôle doit avoir un droit d'utilisation de l'action de suppression, ainsi qu'un droit d'accès au groupe d'unités approprié.

  La réussite de l'opération est indiquée par la suppression de l'unité dans la table.

Ajout d'une unité

Vous pouvez ajouter une unité à la base de données IBM Security Key Lifecycle Manager.

Pourquoi et quand exécuter cette tâche

Si l'affinité machine est activée, l'ajout d'une unité vous impose d'ajouter également une relation entre l'unité et une machine. Sinon, aucune clé ne sera jamais servie à l'unité ajoutée. L'utilisation de l'affinité machine vous permet de limiter le service de clés à des combinaisons spécifiques d'unités et de machines.

Vous pouvez utiliser la boîte de dialogue Ajouter une unité, la commande **tklmDeviceAdd** ou **Service REST Device Add** pour ajouter une unité. Votre rôle doit

avoir un droit d'utilisation de l'action de création, ainsi qu'un droit d'accès au groupe d'unités approprié.

Procédure

1. Accédez à la page ou au répertoire approprié.
   - Interface graphique :
     a. Connectez-vous à l'interface graphique.
     b. Dans la section Gestion des clés et des unités de la page de bienvenue, sélectionnez **DS5000**.
     c. Cliquez sur **Aller à** > **Gestion des clés et des unités**.
     d. Vous pouvez aussi cliquer avec le bouton droit sur **DS5000** et sélectionner **Gestion des clés et des unités**.
     e. Sur la page de gestion pour DS5000, cliquez sur **Ajouter**.
     f. Cliquez sur **Unité**.
   - Interface de ligne de commande
     a. Accédez au répertoire *<WAS_HOME>*/bin. Exemple :

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

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

     b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme SKLMAdmin. Exemple :

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

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

   - Interface REST :
     – Ouvrez un client REST.
2. Ajoutez une unité.
   - Interface graphique :

     Dans la boîte de dialogue Ajouter une unité, entrez les informations obligatoires et optionnelles. Cliquez ensuite sur **Ajouter une unité**.
   - Interface de ligne de commande :

     Entrez tklmDeviceAdd pour ajouter une unité. Vous devez spécifier le numéro de série de l'unité ainsi que le groupe d'unités. Par exemple, entrez :

     ```
     print AdminTask.tklmDeviceAdd ('[-type DS5000 -serialNumber CDA39403AQJF
       -attributes "{worldwideName ABCdeF1234567890}
       {description marketingDivisionDrive}
       {keyPrefix AEF}
       {numberOfKeys 10}
       {deviceText abcdefghijklmnopqrst}
       {machineID 30423830303034370000000000000}"]')
     ```

   - Interface REST :
     a. Obtenez un identificateur d'authentification utilisateur unique pour accéder aux services REST d'IBM Security Key Lifecycle Manager. Pour plus d'informations sur le processus d'authentification, voir Processus d'authentification pour les services REST.

b. Pour appeler le **service Device Add**, envoyez la demande HTTP POST. Transmettez l'identificateur d'authentification utilisateur que vous avez obtenu à l'étape a avec le message de demande, conformément à l'exemple suivant :

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

Que faire ensuite

Vous pouvez associer l'unité à une machine.

Modification d'une unité

Vous pouvez modifier les informations relatives à une unité dans la base de données d'IBM Security Key Lifecycle Manager. Vous pouvez, par exemple, mettre à jour la description de l'unité.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser la boîte de dialogue Modifier une unité. Une unité peut également être mise à jour à l'aide de la commande **tklmDeviceUpdate** ou de **Service REST Device Update**. Votre rôle doit avoir un droit d'utilisation de l'action de modification, ainsi qu'un droit d'accès au groupe d'unités approprié.

Avant de commencer, si vous utilisez l'interface de ligne de commande ou l'interface REST, obtenez la valeur de l'identificateur unique universel (UUID) de l'unité que vous souhaitez mettre à jour.

Procédure

1. Accédez à la page ou au répertoire approprié.
   - Interface graphique :
     a. Connectez-vous à l'interface graphique.
     b. Dans la section Gestion des clés et des unités de la page de bienvenue, sélectionnez **DS5000**.
     c. Cliquez sur **Aller à** > **Gestion des clés et des unités**.
     d. Vous pouvez aussi cliquer avec le bouton droit sur **DS5000** et sélectionner **Gestion des clés et des unités**.
     e. Sur la page de gestion pour DS5000, sélectionnez une unité dans la colonne **Numéro de série de l'unité**.
     f. Cliquez sur **Modifier une unité**.
     g. Vous pouvez également cliquer sur une unité à l'aide du bouton droit de la souris, puis sélectionner **Modifier une unité**, ou bien cliquer deux fois sur une entrée d'unité.
   - Interface de ligne de commande
     a. Accédez au répertoire <*WAS_HOME*>/bin. Exemple :

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

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

b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme SKLMAdmin. Exemple :

Windows

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

Linux

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

2. Modifiez une unité.
   - Interface graphique :

     Dans la boîte de dialogue Modifier une unité, entrez les changements voulus. Cliquez ensuite sur **Modifier une unité**.
   - Interface de ligne de commande :

     Entrez la commande tklmDeviceUpdate pour mettre à jour une unité. Vous devez spécifier l'identificateur unique universel de l'unité (UUID), ainsi que les attributs à modifier. Par exemple, entrez :

     ```
     print AdminTask.tklmDeviceUpdate
      ('[-uuid DEVICE-15d499ad-3ad8-3333-8c84-64cb9e11d990
       -attributes "{description myDevice}"]')
     ```
   - Interface REST :

     Utilisez le **service REST Device Update** pour mettre à jour une unité. Par exemple, envoyez la demande HTTP suivante :

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

Que faire ensuite

Vous pouvez ensuite vérifier que les changements sont effectifs.

Suppression d'une unité

Vous pouvez supprimer une unité, telle qu'un serveur de stockage DS5000. La suppression de l'unité revient à supprimer son numéro de série d'unité ainsi que ses données de clé de la base de données de IBM Security Key Lifecycle Manager.

Pourquoi et quand exécuter cette tâche

Si l'unité appartient à la famille d'unités DS5000 et si l'affinité machine est activée, la suppression de l'unité supprime également la relation qui peut exister entre une unité et une machine.

Vous pouvez utiliser l'option de menu Supprimer, la commande **tklmDeviceDelete** ou **Service REST Device Delete** pour supprimer une unité. Votre rôle doit avoir un droit d'utilisation de l'action de suppression, ainsi qu'un droit d'accès au groupe d'unités approprié.

Procédure

1. Accédez à la page ou au répertoire approprié.
   - Interface graphique :
     a. Connectez-vous à l'interface graphique.

b. Dans la section Gestion des clés et des unités de la page de bienvenue, sélectionnez **DS5000**.

c. Cliquez sur **Aller à** > **Gestion des clés et des unités**.

d. Vous pouvez aussi cliquer avec le bouton droit sur **DS5000** et sélectionner **Gestion des clés et des unités**.

e. Sur la page de gestion pour DS5000, sélectionnez une unité.

f. Cliquez sur **Supprimer**.

g. Vous pouvez également cliquer avec le bouton droit de la souris sur une unité, puis sélectionner **Supprimer**.

- Interface de ligne de commande

  a. Accédez au répertoire <*WAS_HOME*>/bin. Exemple :

  Windows

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

  Linux

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

  b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme SKLMAdmin. Exemple :

  Windows

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

  Linux

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

2. A partir de l'interface de ligne de commande, exécutez la commande **tklmMachineDeviceList** ou utilisez le **service REST Machine Device List** pour vous procurer l'identificateur unique universel (uuid) de l'unité à supprimer. Utilisez la commande **tklmMachineDeviceDelete** ou **Service REST Machine Device Delete** pour supprimer toute association entre l'unité et une machine.

   Par exemple, entrez :

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

   ```
   print AdminTask.tklmMachineDeviceDelete
   ('[-deviceUUID DEVICE-663b6d37-e6d5-4c9f-af90-e40e48d27f3c
    -machineID 30423830303034370000000000000]')
   ```

   Vous pouvez envoyer les demandes HTTP suivantes :

   ```
   GET https://localhost:<port>/SKLM/rest/v1/machines/device?machineID=
   30423830303034370000000000000
   Content-Type: application/json
   Accept : application/json
   Authorization: SKLMAuth authId=139aeh34567m
   ```

   ```
   DELETE https://localhost:<port>/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. Supprimez l'unité.

   - Interface graphique :

     Dans la boîte de dialogue de confirmation, lisez le message de confirmation avant de supprimer l'unité. La suppression de l'unité entraîne celle de son numéro de série et de ses clés dans la base de données d'IBM Security Key Lifecycle Manager.

     Cliquez ensuite sur **OK**.

- Interface de ligne de commande :

  Entrez `tklmDeviceDelete` pour supprimer une unité. Vous devez indiquer son identificateur unique universel (UUID). Par exemple, entrez :

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

- Interface REST :

  Utilisez le **service REST Device Delete** pour supprimer une unité. Par exemple, vous pouvez envoyer la demande HTTP suivante :

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

Ajout de clés

Vous pouvez ajouter des clés supplémentaires à utiliser avec les serveurs de stockage DS5000. Avant de commencer, déterminez la stratégie de votre site concernant la définition des préfixes de clés.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser la boîte de dialogue Ajouter une clé, la commande **tklmSecretKeyCreate** ou **Service REST Secret Key Create** pour créer une ou plusieurs clés symétriques dans le groupe existant. Votre rôle doit avoir un droit d'utilisation de l'action de création, ainsi qu'un droit d'accès au groupe d'unités approprié.

Procédure

1. Accédez à la page ou au répertoire approprié.
   - Interface graphique :
     a. Connectez-vous à l'interface graphique.
     b. Dans la section Gestion des clés et des unités de la page de bienvenue, sélectionnez **DS5000**.
     c. Cliquez sur **Aller à** > **Gestion des clés et des unités**.
     d. Vous pouvez aussi cliquer avec le bouton droit sur **DS5000** et sélectionner **Gestion des clés et des unités**.
     e. Sur la page de gestion pour DS5000, cliquez sur **Ajouter**.
     f. Cliquez sur **Ajouter des clés**.
   - Interface de ligne de commande
     a. Accédez au répertoire <*WAS_HOME*>/bin. Exemple :

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

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

     b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme SKLMAdmin. Exemple :

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

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

   - Interface REST :

– Ouvrez un client REST.

2. Créez des clés.
   - Interface graphique

     Dans la boîte de dialogue Ajouter une clé, spécifiez des valeurs pour les paramètres requis. Cliquez ensuite sur **Ajouter des clés**.
   - Interface de ligne de commande :
     a. Utilisez la commande **tklmGroupList** pour obtenir la valeur de l'identificateur unique universel (UUID) du groupe de clés. Par exemple, entrez :

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

     Le résultat obtenu devrait ressembler à l'exemple suivant :

     ```
     nom de groupe = DS5K-ds5kdevice
     type de groupe = KEY
     UUID de groupe = KEYGROUP-9c97d9aa-b5f0-41a1-b65f-119756168211
     date d'initialisation = 6/4/10 12:00:00 AM GMT-12:00
     date d'activation = 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
     .
     . (Eléments restants non représentés dans cet exemple.)
     .
     ```

     b. Créez des clés supplémentaires et stockez-les dans le groupe. Par exemple, entrez :

     ```
     print AdminTask.tklmSecretKeyCreate ('[-alias abc
      -keyStoreName defaultKeyStore -numOfKeys 10 -usage DS5000
       -keyGroupUuid KEYGROUP-9c97d9aa-b5f0-41a1-b65f-119756168211]')
     ```

   - Interface REST :
     a. Obtenez un identificateur d'authentification utilisateur unique pour accéder aux services REST d'IBM Security Key Lifecycle Manager. Pour plus d'informations sur le processus d'authentification, voir Processus d'authentification pour les services REST.
     b. Pour appeler le **service REST Group List**, envoyez la demande HTTP GET. Transmettez l'identificateur d'authentification utilisateur que vous avez obtenu à l'étape a avec le message de demande, conformément à l'exemple suivant :

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

     Le résultat obtenu devrait ressembler à l'exemple suivant :

     ```
     Code de statut :200 OK
     Content-Language: en
     [
      {
       "nom de groupe" : "DS5K-ds5kdevice",
       "type de groupe" : "KEY",
       "UUID de groupe" : "KEYGROUP-9c97d9aa-b5f0-41a1-b65f-119756168211",
       "date d'initialisation" : "6/4/10 12:00:00 AM Central Standard Time",
       "date d'activation" : "6/4/10 12:00:00 AM Central Standard Time",
      "clés" :
      [
     ```

```
{
 "uuid" : "KEY-66b0a3a2-3c52-4088-8772-0a1ddebf5803",
 "alias" : "dsk000000000000000000",
 "nom(s) de magasin de clés" : "defaultKeyStore "
},
{
 "uuid" : "KEY-3f1230fd-59ef-4c15-82e6-40d68ac5f2ab",
 "alias" : "dsk000000000000000001",
 "nom(s) de magasin de clés" : "defaultKeyStore "
.
.
.
```

c. Utilisez le **service REST Secret Key Create** pour créer des clés supplémentaires et les stocker dans le groupe. Par exemple, vous pouvez envoyer la demande HTTP suivante :

```
POST https://localhost:<port>/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. L'indicateur de réussite varie, selon l'interface :
   - Interface graphique :

     Les clés ajoutées sont visibles dans la table de clés, sur la page Modifier des clés. Faites une sauvegarde des nouvelles clés avant qu'elles ne commencent à être servies aux unités.
   - Interface de ligne de commande :

     Des messages d'achèvement indiquent la réussite de l'opération. Exécutez également la commande **tklmGroupList** pour vérifier que les clés ajoutées existent à présent dans le groupe de clés. Par exemple, entrez :

     ```
     print AdminTask.tklmGroupList ('[-type keygroup -v y]')
     ```
   - Interface REST :

     Le code de statut `200 OK` indique la réussite de l'opération.

Que faire ensuite

Vous pouvez associer l'unité à une machine.

Modification (suppression) de clés

Vous pouvez modifier le nombre de clés utilisées par un serveur de stockage DS5000 en supprimant une ou plusieurs d'entre elles. Avant de commencer, déterminez les changements à apporter, par exemple le nombre de clés à supprimer.

Pourquoi et quand exécuter cette tâche

Ne supprimez des clés que lorsque les données qu'elles protègent ne sont plus utiles. Leur suppression a en effet les mêmes conséquences que l'effacement des données en question. Une fois les clés supprimées, les données protégées ne sont plus récupérables.

Vous pouvez utiliser la boîte de dialogue Modifier des clés, la commande **tklmKeyDelete** ou **Service REST Delete Key**. Votre rôle doit avoir un droit d'utilisation de l'action de modification, ainsi qu'un droit d'accès au groupe d'unités approprié.

Procédure

1. Accédez à la page ou au répertoire approprié.
   - Interface graphique :
     a. Connectez-vous à l'interface graphique.
     b. Dans la section Gestion des clés et des unités de la page de bienvenue, sélectionnez **DS5000**.
     c. Cliquez sur **Aller à** > **Gestion des clés et des unités**.
     d. Vous pouvez aussi cliquer avec le bouton droit sur **DS5000** et sélectionner **Gestion des clés et des unités**.
   - Interface de ligne de commande
     a. Accédez au répertoire *<WAS_HOME>*/bin. Exemple :

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

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

     b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme SKLMAdmin. Exemple :

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

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

2. Modifiez les informations relatives aux clés.
   - Interface graphique :

     Sur la page de gestion pour DS5000, sélectionnez une unité dans la colonne **Numéro de série de l'unité**. Cliquez ensuite sur **Modifier > Clés**. Vous pouvez également faire un clic droit sur une unité, puis sélectionner **Modifier des clés**.

     Dans la boîte de dialogue Modifier des clés, sélectionnez une clé et cliquez sur **Supprimer**. Lisez le message de confirmation. Cliquez ensuite sur **OK**.
   - Interface de ligne de commande :

     Vous pouvez supprimer une clé. Votre rôle doit avoir un droit d'utilisation de l'action de suppression, ainsi qu'un droit d'accès au groupe d'unités approprié. Par exemple, entrez :
     ```
     print AdminTask.tklmKeyDelete ('[-alias aaa000000000000000000
      -keyStoreName defaultKeyStore]')
     ```
   - Interface REST :

     Utilisez **Service REST Delete Key** pour supprimer une clé. Par exemple, vous pouvez envoyer la demande HTTP suivante :
     ```
     DELETE https://localhost:<port>/SKLM/rest/v1/keys/aaa000000000000000000
     Content-Type: application/json
     Accept : application/json
     Authorization: SKLMAuth authId=139aeh34567m
     ```

Que faire ensuite

Vous pouvez associer l'unité à une machine.

Gestion de fichiers GPFS (IBM Spectrum Scale)

Vous pouvez utiliser le système de fichiers GPFS pour gérer les clés dans IBM Security Key Lifecycle Manager.

GPFS (IBM Spectrum Scale) est une solution de gestion de fichiers de disque partagé hautes performances qui permet d'accéder à des données de façon rapide et fiable à partir de plusieurs noeuds dans un environnement de cluster. Les applications peuvent facilement accéder aux fichiers à l'aide d'interfaces de système de fichiers standard, et il est possible d'accéder au même fichier simultanément depuis plusieurs noeuds.

GPFS fournit la prise en charge du chiffrement de fichiers afin de permettre le stockage et la suppression sécurisés des données. GPFS gère le chiffrement via des clés de chiffrement et des règles de chiffrement.

Voir la documentation GPFS pour plus d'informations http://www.ibm.com/support/knowledgecenter/SSFKCN/gpfs_welcome.html.

Administration de certificats et de clés

Pour administrer des certificats et des clés, vous souhaiterez peut-être ajouter, modifier ou supprimer les noms de noeud qui leur sont associés. Vous pouvez également ajouter des clés et un nom qui leur est associé.

Pourquoi et quand exécuter cette tâche

Votre rôle doit avoir un droit d'utilisation de l'action de visualisation, ainsi qu'un droit d'accès au groupe d'unités approprié. Utilisez la page de gestion pour GPFS pour ajouter, modifier ou supprimer un certificat ou une clé.

Avant de commencer, examinez les colonnes de la page, qui comprend des boutons permettant d'ajouter, de modifier ou de supprimer un élément de la table.

La table est organisée selon les zones d'informations suivantes :

- Dans les colonnes de gauche, les informations sur les certificats indiquent l'identificateur unique universel du certificat, le nom du certificat et le nombre de noeuds finaux. Il s'agit du nombre de noeuds finaux qui utilisent ce certificat.
- Dans les colonnes de droite, les informations sur les clés indiquent l'identificateur unique universel de la clé et le nom de la clé à laquelle les certificats situés à gauche ont accès.

Procédure

1. Connectez-vous à l'interface graphique.
   a. Dans la section Gestion des clés et des unités de la page Bienvenue, sélectionnez **GPFS**.
   b. Cliquez sur **Aller à** > **Gestion des clés et des unités**.
   c. Vous pouvez aussi cliquer avec le bouton droit sur **GPFS** et sélectionner **Gestion des clés et des unités**.
2. Vous pouvez ajouter, modifier ou supprimer une clé ou un certificat.
   Vous pouvez exécuter les tâches d'administration suivantes :
   - Actualiser la liste

     Cliquez sur l'icône de régénération  pour actualiser les éléments de la table.

- Ajouter

  Cliquez sur **Ajouter**.

  – Certificat

    Dans la boîte de dialogue Ajouter un certificat, tapez le nom et le nom de fichier et l'emplacement d'un certificat. Cliquez ensuite sur **Ajouter**.

  – Clé

    Dans la boîte de dialogue Ajouter une clé, spécifiez les informations correspondant à vos besoins, telles que le nombre de clés à créer, sans dépasser 100. Cliquez ensuite sur **Ajouter**.

  L'indicateur de réussite varie selon que vous ajoutez un certificat ou des clés.

- Modifier

  Pour modifier le groupe d'unités auquel un certificat ou une clé appartient, sélectionnez le certificat ou la clé, puis cliquez sur **Modifier**. Vous pouvez aussi cliquer avec le bouton droit de la souris sur le certificat ou la clé sélectionnés. Cliquez ensuite sur **Modifier**.

  – Certificat

    Affichez des informations en lecture seule dans la page Modifier un certificat. Votre rôle doit avoir un droit d'utilisation de l'action de modification, ainsi qu'un droit d'accès au groupe d'unités approprié.

  – Clé

    Affichez des informations en lecture seule dans la page Modifier une clé. Votre rôle doit avoir un droit d'utilisation de l'action de suppression, ainsi qu'un droit d'accès au groupe d'unités approprié.

  L'indicateur de réussite varie selon que le changement est apporté à une colonne dédiée au certificat ou à la clé.

- Supprimer

  Pour supprimer un certificat ou une clé, sélectionnez le certificat ou la clé, puis cliquez sur **Supprimer**. Vous pouvez aussi cliquer avec le bouton droit de la souris sur le certificat ou la clé sélectionnés, puis cliquez sur **Supprimer**.

  Les métadonnées relatives au certificat que vous supprimez sont retirées de la base de données IBM Security Key Lifecycle Manager. Les données de clé sont également supprimées. Pour confirmer la suppression, cliquez sur **OK**. Votre rôle doit avoir un droit d'utilisation de l'action de suppression, ainsi qu'un droit d'accès au groupe d'unités approprié.

  Un indicateur de réussite indique la suppression du certificat dans la table.

Ajout d'un certificat

Vous pouvez ajouter d'autres certificats à utiliser avec IBM Security Key Lifecycle Manager.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser la boîte de dialogue Ajout un certificat pour ajouter un certificat. Votre rôle doit avoir un droit d'utilisation de l'action de création, ainsi qu'un droit d'accès au groupe d'unités approprié.

Procédure

1. Connectez-vous à l'interface graphique.
2. Dans la section Gestion des clés et des unités de la page de bienvenue, sélectionnez **GPFS**.

3. Cliquez sur **Aller à** > **Gestion des clés et des unités**.
4. Vous pouvez aussi cliquer avec le bouton droit sur **GPFS** et sélectionner **Gestion des clés et des unités**.
5. Sur la page de gestion pour GPFS, cliquez sur **Ajouter**.
6. Cliquez sur **Certificat**.
7. Dans la boîte de dialogue Ajouter un certificat, spécifiez les informations correspondant à vos besoins.
8. Cliquez sur **Ajouter**.

   Le certificat est ajouté à la table.

Modification d'un certificat

Vous pouvez modifier les informations relatives à un certificat dans la base de données d'IBM Security Key Lifecycle Manager.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser la boîte de dialogue Modifier un certificat pour mettre à jour un certificat. Votre rôle doit avoir un droit d'utilisation de l'action de modification, ainsi qu'un droit d'accès au groupe d'unités approprié.

Procédure

1. Connectez-vous à l'interface graphique.
2. Dans la section Gestion des clés et des unités de la page Bienvenue, sélectionnez **GPFS**.
3. Cliquez sur **Aller à** > **Gestion des clés et des unités**.
4. Vous pouvez aussi cliquer avec le bouton droit sur **GPFS** et sélectionner **Gestion des clés et des unités**.
5. Sur la page de gestion pour GPFS, sélectionnez un certificat.
6. Cliquez sur **Modifier**.
7. Vous pouvez également faire un clic droit sur un certificat et sélectionner **Modifier**, ou bien faire un double clic sur une entrée de certificat.
8. Dans la boîte de dialogue Modifier un certificat, entrez les informations modifiées.
9. Cliquez sur **Modifier**.

   Les informations relatives au certificat sont modifiées dans la table.

Que faire ensuite

Vous pouvez ensuite vérifier que les changements sont effectifs.

Suppression d'un certificat

Vous pouvez être amené à supprimer un certificat sélectionné, lequel peut avoir n'importe quel statut, par exemple actif.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser l'option de menu Supprimer pour supprimer un certificat. Votre rôle doit avoir un droit d'utilisation de l'action de suppression, ainsi qu'un droit d'accès au groupe d'unités approprié.

Procédure

1. Connectez-vous à l'interface graphique.

2. Dans la section Gestion des clés et des unités de la page Bienvenue, sélectionnez **GPFS**.
3. Cliquez sur **Aller à** > **Gestion des clés et des unités**.
4. Vous pouvez aussi cliquer avec le bouton droit sur **GPFS** et sélectionner **Gestion des clés et des unités**.
5. Sur la page de gestion pour GPFS, sélectionnez un certificat.
6. Cliquez sur **Supprimer**.
7. Vous pouvez également cliquer avec le bouton droit de la souris sur un certificat, puis sélectionner **Supprimer**.
8. Lisez le message de confirmation dans la boîte de dialogue correspondante afin de vérifier que vous avez sélectionné le certificat approprié avant de le supprimer. Cliquez ensuite sur **OK**.

   Le certificat est retiré de la table.

Ajout de clés

Vous pouvez ajouter des clés à utiliser avec GPFS.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser la boîte de dialogue Ajouter une clé pour créer une ou plusieurs clés dans le groupe existant. Votre rôle doit avoir un droit d'utilisation de l'action de création, ainsi qu'un droit d'accès au groupe d'unités approprié.

Avant de commencer, déterminez la stratégie de votre site concernant la définition des préfixes de clés.

Procédure

1. Connectez-vous à l'interface graphique.
2. Dans la section Gestion des clés et des unités de la page Bienvenue, sélectionnez **GPFS**.
3. Cliquez sur **Aller à** > **Gestion des clés et des unités**.
4. Vous pouvez aussi cliquer avec le bouton droit sur **GPFS** et sélectionner **Gestion des clés et des unités**.
5. Sur la page de gestion pour GPFS, cliquez sur **Ajouter**.
6. Cliquez sur **Clé**.
7. Dans la boîte de dialogue Ajouter une clé, spécifiez des valeurs pour les paramètres.
8. Cliquez sur **Ajouter**. Les clés que vous avez ajoutées sont visibles dans la table de clés. Sauvegardez les clés avant qu'elles ne commencent à être servies aux unités.

Modification d'une clé

Vous pouvez modifier les informations relatives à une clé dans la base de données d'IBM Security Key Lifecycle Manager.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser la boîte de dialogue Modifier une clé pour modifier les informations relatives à une clé. Votre rôle doit avoir un droit d'utilisation de l'action de modification, ainsi qu'un droit d'accès au groupe d'unités approprié.

Procédure

1. Connectez-vous à l'interface graphique.
2. Dans la section Gestion des clés et des unités de la page Bienvenue, sélectionnez **GPFS**.
3. Cliquez sur **Aller à** > **Gestion des clés et des unités**.
4. Vous pouvez aussi cliquer avec le bouton droit sur **GPFS** et sélectionner **Gestion des clés et des unités**.
5. Sur la page de gestion pour GPFS, sélectionnez une clé.
6. Cliquez sur **Modifier**.
7. Vous pouvez également cliquer avec le bouton droit de la souris sur une clé, puis sélectionner **Modifier** ou cliquer deux fois sur une entrée de clé.
8. Dans la boîte de dialogue Modifier une clé, entrez les informations modifiées. Cliquez ensuite sur **Modifier**. Les informations relatives à la clé sont modifiées dans la table.

Suppression d'une clé

Vous pouvez supprimer une entrée de clé de la base de données d'IBM Security Key Lifecycle Manager.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser l'option de menu Supprimer pour supprimer une clé. Votre rôle doit avoir un droit d'utilisation de l'action de suppression, ainsi qu'un droit d'accès au groupe d'unités approprié.

Procédure

1. Connectez-vous à l'interface graphique.
2. Dans la section Gestion des clés et des unités de la page de bienvenue, sélectionnez **GPFS**.
3. Cliquez sur **Aller à** > **Gestion des clés et des unités**.
4. Vous pouvez aussi cliquer avec le bouton droit sur **GPFS** et sélectionner **Gestion des clés et des unités**.
5. Sur la page de gestion pour GPFS, sélectionnez une clé.
6. Cliquez sur **Supprimer**.
7. Vous pouvez également cliquer avec le bouton droit de la souris sur une clé et sélectionner **Supprimer**.
8. Lisez le message de confirmation de la boîte de dialogue correspondante pour vérifier que vous avez sélectionné la clé appropriée avant de la supprimer. Cliquez ensuite sur **OK**. Les informations de clé sont retirées de la table.

Gestion d'un groupe d'unités PEER_TO_PEER

Le groupe d'unités PEER_TO_PEER met à disposition les unités qui fonctionnent sur le protocole KMIP (Key Management Interoperability Protocol). Avec ce type de groupe d'unités, jusqu'à deux unités peuvent partager une ou plusieurs clés symétriques.

Vous pouvez utiliser le groupe d'unités PEER_TO_PEER pour gérer des clés et des certificats d'unité dans IBM Security Key Lifecycle Manager.

Administration de certificats et de clés

Pour administrer des certificats et des clés, vous souhaiterez peut-être ajouter, modifier ou supprimer les noms de noeud qui leur sont associés. Vous pouvez également ajouter des clés et un nom qui leur est associé.

Pourquoi et quand exécuter cette tâche

Votre rôle doit avoir un droit d'utilisation de l'action de visualisation, ainsi qu'un droit d'accès au groupe d'unités approprié. Utilisez la page de gestion pour PEER_TO_PEER pour ajouter, modifier ou supprimer un certificat ou une clé.

Avant de commencer, examinez les colonnes de la page, qui comprend des boutons permettant d'ajouter, de modifier ou de supprimer un élément de la table.

La table est organisée selon les zones d'informations suivantes :

- Dans les colonnes de gauche, les informations indiquent le nom WWNN, le nom du certificat de l'unité et le type d'unité.
- Dans les colonnes de droite, les informations sur les clés indiquent l'identificateur unique universel et le nom de la clé à laquelle les certificats situés à gauche ont accès.

Procédure

1. Connectez-vous à l'interface graphique.
   a. Dans la section Gestion des clés et des unités de la page Bienvenue, sélectionnez **PEER_TO_PEER**.
   b. Cliquez sur **Aller à** > **Gestion des clés et des unités**.
   c. Vous pouvez aussi cliquer avec le bouton droit de la souris sur **PEER_TO_PEER** et sélectionner **Gestion des clés et des unités**.
2. Vous pouvez ajouter, modifier ou supprimer un certificat de clé ou d'unité.

Ajout d'une unité

Vous pouvez ajouter une unité au groupe d'unités PEER_TO_PEER pour l'utiliser avec IBM Security Key Lifecycle Manager.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser la boîte de dialogue Ajouter une unité pour ajouter une unité. Votre rôle doit avoir un droit d'utilisation de l'action de création, ainsi qu'un droit d'accès au groupe d'unités approprié.

Procédure

1. Connectez-vous à l'interface graphique.
2. Dans la section Gestion des clés et des unités de la page de bienvenue, sélectionnez **PEER_TO_PEER**.
3. Cliquez sur **Aller à** > **Gestion des clés et des unités**.
4. Vous pouvez aussi cliquer avec le bouton droit de la souris sur **PEER_TO_PEER** et sélectionner **Gestion des clés et des unités**.
5. Sur la page de gestion pour PEER_TO_PEER, cliquez sur **Ajouter**.
6. Cliquez sur **Unité**.
7. Dans la boîte de dialogue Ajouter une unité, indiquez le nom du certificat, l'emplacement, puis le type d'unité. Vous ne pouvez ajouter qu'une seule unité de chaque type et un maximum de deux unités.

8. Cliquez sur **Ajouter**.
   L'unité est ajoutée à la table PEER_TO_PEER.

Modification d'une unité

Vous pouvez modifier un certificat d'unité dans la base de données IBM Security Key Lifecycle Manager.

Pourquoi et quand exécuter cette tâche

Utilisez la boîte de dialogue Modifier le certificat d'unité pour mettre à jour une unité. Votre rôle doit avoir un droit d'utilisation de l'action de modification, ainsi qu'un droit d'accès au groupe d'unités approprié.

Procédure

1. Connectez-vous à l'interface graphique.
2. Dans la section Gestion des clés et des unités de la page Bienvenue, sélectionnez **PEER_TO_PEER**.
3. Cliquez sur **Aller à** > **Gestion des clés et des unités**.
4. Vous pouvez aussi cliquer avec le bouton droit de la souris sur **PEER_TO_PEER** et sélectionner **Gestion des clés et des unités**.
5. Sur la page de gestion pour `PEER_TO_PEER`, sélectionnez une unité.
6. Cliquez sur **Modifier**.
7. Vous pouvez également cliquer avec le bouton droit de la souris sur une unité, puis sélectionner **Modifier**, ou bien cliquer deux fois sur une entrée d'unité.
8. Dans la boîte de dialogue Modifier le certificat d'unité, sélectionnez un certificat ayant la même valeur WWNN que le précédent certificat d'unité.
9. Cliquez sur **Modifier**.
   Les informations relatives à l'unité sont modifiées dans la table.

Que faire ensuite

Vous pouvez ensuite vérifier que les changements sont effectifs.

Suppression d'une unité

Vous pouvez être amené à supprimer une unité sélectionnée ainsi que son certificat de communication correspondant, lequel peut avoir n'importe quel statut, par exemple actif. Après la suppression, cette unité ne peut plus communiquer avec les objets du groupe PEER_TO_PEER.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser l'élément de menu `Supprimer` pour supprimer une unité. Votre rôle doit avoir un droit d'utilisation de l'action de suppression, ainsi qu'un droit d'accès au groupe d'unités approprié.

Procédure

1. Connectez-vous à l'interface graphique.
2. Dans la section Gestion des clés et des unités de la page Bienvenue, sélectionnez **PEER_TO_PEER**.
3. Cliquez sur **Aller à** > **Gestion des clés et des unités**.
4. Vous pouvez aussi cliquer avec le bouton droit de la souris sur **PEER_TO_PEER** et sélectionner **Gestion des clés et des unités**.

5. Sur la page de gestion pour PEER_TO_PEER, sélectionnez une unité.
6. Cliquez sur **Supprimer**.
7. Sinon, cliquez avec le bouton droit de la souris sur une unité, puis sélectionnez **Supprimer**.
8. Dans la boîte de dialogue de confirmation, lisez le message de confirmation. Cliquez ensuite sur **OK**.

   L'unité est supprimée de la table.

Ajout de clés

Vous pouvez ajouter des clés à utiliser avec PEER_TO_PEER.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser la boîte de dialogue Ajouter une clé pour créer une ou plusieurs clés dans le groupe existant. Votre rôle doit avoir un droit d'utilisation de l'action de création, ainsi qu'un droit d'accès au groupe d'unités approprié.

Avant de commencer, déterminez la stratégie de votre site concernant la définition des préfixes de clés.

Procédure

1. Connectez-vous à l'interface graphique.
2. Dans la section Gestion des clés et des unités de la page Bienvenue, sélectionnez **PEER_TO_PEER**.
3. Cliquez sur **Aller à** > **Gestion des clés et des unités**.
4. Vous pouvez aussi cliquer avec le bouton droit de la souris sur **PEER_TO_PEER** et sélectionner **Gestion des clés et des unités**.
5. Sur la page de gestion pour PEER_TO_PEER, cliquez sur **Ajouter**.
6. Cliquez sur **Clé**.
7. Dans la boîte de dialogue Ajouter une clé, spécifiez des valeurs pour les paramètres.
8. Cliquez sur **Ajouter**. Les clés que vous avez ajoutées sont visibles dans la table de clés. Sauvegardez les clés avant qu'elles ne commencent à être servies aux unités.

Modification d'une clé

Vous pouvez modifier les informations relatives à une clé dans la base de données d'IBM Security Key Lifecycle Manager.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser la boîte de dialogue Modifier une clé pour modifier des informations relatives à la clé. Votre rôle doit avoir un droit d'utilisation de l'action de modification, ainsi qu'un droit d'accès au groupe d'unités approprié.

Procédure

1. Connectez-vous à l'interface graphique.
2. Dans la section Gestion des clés et des unités de la page Bienvenue, sélectionnez **PEER_TO_PEER**.
3. Cliquez sur **Aller à** > **Gestion des clés et des unités**.
4. Vous pouvez aussi cliquer avec le bouton droit de la souris sur **PEER_TO_PEER** et sélectionner **Gestion des clés et des unités**.

5. Sur la page de gestion pour PEER_TO_PEER, sélectionnez une clé.
6. Cliquez sur **Modifier**.
7. Vous pouvez également cliquer avec le bouton droit de la souris sur une clé, puis sélectionner **Modifier** ou cliquer deux fois sur une entrée de clé.
8. Dans la boîte de dialogue Modifier une clé, entrez les informations modifiées. Cliquez ensuite sur **Modifier**. Les informations relatives à la clé sont modifiées dans la table.

Suppression d'une clé

Vous pouvez supprimer une entrée de clé de la base de données d'IBM Security Key Lifecycle Manager.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser l'option de menu Supprimer pour supprimer une clé. Votre rôle doit avoir un droit d'utilisation de l'action de suppression, ainsi qu'un droit d'accès au groupe d'unités approprié.

Procédure

1. Connectez-vous à l'interface graphique.
2. Dans la section Gestion des clés et des unités de la page de bienvenue, sélectionnez **PEER_TO_PEER**.
3. Cliquez sur **Aller à** > **Gestion des clés et des unités**.
4. Vous pouvez aussi cliquer avec le bouton droit de la souris sur **PEER_TO_PEER** et sélectionner **Gestion des clés et des unités**.
5. Sur la page de gestion pour PEER_TO_PEER, sélectionnez une clé.
6. Cliquez sur **Supprimer**.
7. Vous pouvez également cliquer avec le bouton droit de la souris sur une clé et sélectionner **Supprimer**.
8. Lisez le message de confirmation de la boîte de dialogue correspondante pour vérifier que vous avez sélectionné la clé appropriée avant de la supprimer. Cliquez ensuite sur **OK**. Les informations de clé sont retirées de la table.

Exportation et importation de groupes d'unités

IBM Security Key Lifecycle Manager fournit un ensemble d'opérations pour exporter les groupes d'unités d'une instance d'IBM Security Key Lifecycle Manager et les importer dans une autre instance ayant la même version que l'instance source d'IBM Security Key Lifecycle Manager à travers les systèmes d'exploitation. Les données des groupes d'unités exportés sont chiffrées et protégées par un mot de passe.

Pour plus d'informations sur l'importation et l'exportation du groupe d'unités, voir Présentation de l'importation et de l'exportation d'un groupe d'unités

Exportation d'un groupe d'unités

Vous pouvez exporter des données de groupe d'unités pour le groupe d'unités sélectionné vers une archive chiffrée. Ensuite, vous pouvez importer ces données de groupe d'unités dans une autre instance d'IBM Security Key Lifecycle Manager à travers les systèmes d'exploitation.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser la boîte de dialogue Exporter le groupe d'unités pour exporter un groupe d'unités. Vous pouvez aussi utiliser le **service REST Device Group Export**.

Votre rôle doit disposer d'un droit d'exporter des groupes d'unités.

Remarque : Au cours de la migration des données à partir des versions précédentes d'IBM Security Key Lifecycle Manager, certains des certificats peuvent ne pas être associés au groupe d'unités correct. En conséquence, il est possible que quelques certificats soient faussement présentés (dans l'interface utilisateur, REST ou l'interface CLI) pour un groupe d'unités, par exemple 3592 ou DS8000, même si les certificats ne font pas partie du groupe d'unités. Lorsque vous exportez ces groupes d'unités, seuls les certificats du groupe d'unités sont exportés. Les certificats faussement présentés ne sont pas exportés.

Procédure

1. Accédez à la page ou au répertoire approprié.

   Interface graphique

   a. Connectez-vous à l'interface graphique.
   b. Dans la section Gestion des clés et des unités de la page Bienvenue, sélectionnez un groupe d'unités.
   c. Cliquez sur **Aller à** > **Exportation**.
   d. Vous pouvez également faire un clic droit sur le groupe d'unités sélectionné et choisir **Exporter**.
   e. Vous pouvez également à partir de la page Bienvenue cliquer sur **Administration** > **Exporter et importer** > **Exporter**.

   Interface REST

   Ouvrez un client REST.

2. Exportez les données du groupe d'unités correspondant au groupe sélectionné dans le répertoire que vous avez spécifié.

   Interface graphique

   a. Dans la boîte de dialogue Exporter le groupe d'unités, la zone **Groupe d'unités** indique le groupe d'unités sélectionné.
   b. Pour modifier le groupe, cliquez sur **Sélectionner**.
   c. La zone **Emplacement du référentiel d'exportation** affiche le chemin de répertoire <*SKLM_DATA*> par défaut dans lequel le fichier d'exportation est sauvegardé, par exemple `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data`. Pour la définition de <*SKLM_DATA*>, voir Définitions relatives à un répertoire *HOME* et d'autres variables de répertoire. Cliquez sur **Parcourir** pour spécifier l'emplacement du référentiel d'exportation sous le répertoire <*SKLM_DATA*>.

      Le chemin de répertoire dans la zone **Emplacement du référentiel d'exportation** change en fonction de la valeur définie pour la propriété **browse.root.dir** dans le fichier `SKLMConfig.properties`.
   d. Dans la zone **Mot de passe**, indiquez une valeur pour le mot de passe de chiffrement. Retenez bien ce mot de passe pour une utilisation ultérieure.

e. Dans la zone **Confirmer le mot de passe**, saisissez de nouveau le mot de passe que vous avez entré dans la zone **Mot de passe**.

f. Dans la zone **Description**, spécifiez des informations supplémentaires qui indiquent l'objet du fichier d'exportation du groupes d'unités.

g. Cliquez sur **Exporter**.

Interface REST

a. Obtenez un identificateur d'authentification utilisateur unique pour accéder aux services REST d'IBM Security Key Lifecycle Manager. Pour plus d'informations sur le processus d'authentification, voir Processus d'authentification pour les services REST.

b. Pour exécuter le **service REST Device Group Export**, envoyez la demande POST HTTP. Transmettez l'identificateur d'authentification utilisateur que vous avez obtenu à l'étape a avec le message de demande, conformément à l'exemple suivant :

```
POST https://localhost:<port>/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/data/
"password":"mypassword"}
```

3. Lorsque l'exportation est terminée, une boîte de message apparaît pour indiquer que l'opération d'exportation est terminée.

Que faire ensuite

Mémorisez ce mot de passe car il sera utile lors des opérations d'importation et de déchiffrement ultérieures du fichier d'exportation de groupe d'unités dans une autre instance d' IBM Security Key Lifecycle Manager. Examinez le répertoire contenant l'archive d'exportation pour vérifier que le fichier d'exportation y figure. Vous pouvez également vérifier si l'archive est répertoriée dans le tableau sur la page **IBM Security Key Lifecycle Manager** > **Administration** > **Exporter et importer** > **Récapitulatif d'exportation/importation**.

Importation d'un groupe d'unités

Vous pouvez importer des données de groupe d'unités qui ont été exportées d'une autre instance d'IBM Security Key Lifecycle Manager si vous souhaitez déplacer les données entre les instances IBM Security Key Lifecycle Manager.

Avant de commencer

Vous devez disposer du fichier d'exportation et vous rappeler le mot de passe que vous avez utilisé lors de la création du fichier d'exportation. Sauvegardez les fichiers d'exportation dans le répertoire *<SKLM_DATA>* par défaut, par exemple `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data`. Pour la définition de *<SKLM_DATA>*, voir Définitions relatives à un répertoire *HOME* et d'autres variables de répertoire.

Le chemin de répertoire *<SKLM_DATA>* change en fonction de la valeur définie pour la propriété **browse.root.dir** dans le fichier `SKLMConfig.properties`.

La version de l'instance d'IBM Security Key Lifecycle Manager dans laquelle les données d'exportation du groupe d'unités sont importées doit être identique à

l'instance d'IBM Security Key Lifecycle Manager à partir de laquelle les données du groupe d'unités ont été exportées.

Pourquoi et quand exécuter cette tâche

Parfois, les données du groupe d'unités qui sont importées peuvent entrer en conflit avec des données existantes dans la base de données. Par exemple, une clé dans le groupe d'unités importé peut être une clé associée au même nom d'alias que celui d'un groupe d'unités dans l'instance en cours d'IBM Security Key Lifecycle Manager dans laquelle les données sont importées. En cas de conflit, celui-ci doit être résolu pour que le processus d'importation puisse continuer.

Vous pouvez utiliser la page Exporter et importer. Vous pouvez aussi utiliser le `Service REST Device Group Import` pour importer des groupes d'unités.

Votre rôle doit disposer d'un droit d'importer des groupes d'unités. Pour plus d'informations sur l'importation et l'exportation du groupe d'unités, voir Présentation de l'importation et de l'exportation d'un groupe d'unités.

Procédure

1. Accédez à la page ou au répertoire approprié.

   Interface graphique

   a. Connectez-vous à l'interface graphique.
   b. Sur la page Bienvenue, cliquez sur **Administration** > **Exporter et importer**.

   Interface REST

   Ouvrez un client REST.

2. Importez un fichier d'exportation sélectionné. Une seule tâche d'exportation ou d'importation peut s'exécuter à la fois. Si vous souhaitez importer un fichier vers une instance IBM Security Key Lifecycle Manager sur un autre système, copiez le fichier d'exportation sur ce système en utilisant un support tel qu'un disque, ou par transmission électronique.

   Interface graphique

   a. Cliquez sur **Parcourir** pour spécifier l'emplacement du fichier d'exportation sous le répertoire <SKLM_DATA>, par exemple `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data`.
   b. Cliquez sur **Afficher les exportations** pour afficher les fichiers d'exportation.
   c. Dans le tableau, sélectionnez un fichier d'exportation.
   d. Cliquez sur **Importer**.
   e. Vous pouvez également cliquer deux fois ou faire un clic droit sur le fichier d'exportation et sélectionner **Importer**.
   f. Sur la boîte de dialogue Importer à partir de l'archive d'exportation, indiquez le mot de passe de chiffrement que vous avez utilisé pour créer le fichier d'exportation.
   g. Cliquez sur **Importer** pour démarrer l'opération d'importation.

   Interface REST

   a. Obtenez un identificateur d'authentification utilisateur unique pour accéder aux services REST d'IBM Security Key Lifecycle Manager. Pour plus d'informations sur le processus d'authentification, voir Processus d'authentification pour les services REST.

b. Pour exécuter le **service REST Device Group Import**, envoyez la demande POST HTTP. Transmettez l'identificateur d'authentification utilisateur que vous avez obtenu à l'étape a avec le message de demande, conformément à l'exemple suivant :

```
POST https://localhost:<port>/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\\data
"password": "passw0rd123"}
```

3. Si des conflits surgissent au cours du processus d'importation, la boîte de dialogue Conflits lors de l'importation apparaît. Pour plus d'informations, voir la rubrique «Affichage des conflits d'importation», à la page 123.
4. Si aucune donnée n'est en conflit, la boîte de dialogue de progression apparaît. Lorsque l'importation est terminée, une boîte de message apparaît pour indiquer que l'opération d'importation est terminée.
5. Cliquez sur **Fermer**.
6. Redémarrez le serveur. Pour des instructions sur la façon d'arrêter et de démarrer le serveur, voir «Serveur IBM Security Key Lifecycle Manager - Redémarrage», à la page 211.

Suppression d'un fichier d'exportation de groupes d'unités

Vous pouvez supprimer un fichier d'exportation dont une entreprise n'a plus besoin. Utilisez l'interface utilisateur graphique ou l'interface REST pour supprimer un fichier d'exportation de groupes d'unités.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser la page Exportation/Importation ou le **service REST Device Group Delete** pour supprimer un fichier d'exportation.

Procédure

1. Accédez à la page ou au répertoire approprié.

   Interface graphique

   a. Connectez-vous à l'interface graphique.
   b. Sur la page Bienvenue, cliquez sur **Administration** > **Exporter et importer**.

   Interface REST

   Ouvrez un client REST.

2. Supprimez le fichier d'exportation sélectionné.

   Interface graphique

   a. Cliquez sur **Parcourir** pour spécifier l'emplacement du fichier d'exportation sous le répertoire <SKLM_DATA>. Pour la définition de <SKLM_DATA>, voir Définitions relatives à un répertoire *HOME* et d'autres variables de répertoire.
   b. Cliquez sur **Afficher les exportations** pour afficher les fichiers d'exportation.
   c. Dans le tableau, sélectionnez un fichier d'exportation.
   d. Cliquez sur **Supprimer** et confirmez la suppression du fichier.

e. Sinon, cliquez avec le bouton droit de la souris sur le fichier d'exportation et sélectionnez **Supprimer** et confirmez que vous souhaitez supprimer le fichier.

Interface REST

a. Obtenez un identificateur d'authentification utilisateur unique pour accéder aux services REST d'IBM Security Key Lifecycle Manager. Pour plus d'informations sur le processus d'authentification, voir Processus d'authentification pour les services REST.

b. Pour exécuter le **Service REST Device Group Delete**, envoyez la demande HTTP DELETE. Transmettez l'identificateur d'authentification utilisateur que vous avez obtenu à l'étape a avec le message de demande, conformément à l'exemple suivant :

```
DELETE https://localhost:<port>/SKLM/rest/v1/deviceGroups/newDevGrp
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth userAuthId=139aeh34567m
```

Que faire ensuite

Examinez le répertoire dans lequel les fichiers d'exportation sont stockés afin de déterminer si le fichier spécifié a été supprimé.

Affichage des conflits d'importation

Lorsque les données de groupe d'unités sont importées à partir d'un fichier d'exportation, leur contenu est analysé pour déterminer les conflits avec les données qui sont stockées dans la base de données IBM Security Key Lifecycle Manager. Les conflits doivent être résolus pour que les données puissent être importées. Vous pouvez afficher la liste des conflits pour analyser et résoudre les problèmes.

Pourquoi et quand exécuter cette tâche

Les détails de conflit d'importation sont ouverts dans la fenêtre Conflits lors de l'importation. Vous pouvez exporter les données de conflits au format de valeurs séparées par des virgules (CSV).

Procédure

1. Accédez à la page ou au répertoire approprié.

   Interface graphique

   a. Connectez-vous à l'interface graphique.

   b. Sur la page Bienvenue, cliquez sur **Administration** > **Exporter et importer**.

   Interface REST

   Ouvrez un client REST.

2. Importez un fichier d'exportation sélectionné. Une seule tâche d'exportation ou d'importation peut s'exécuter à la fois. Si vous souhaitez importer un fichier vers une instance IBM Security Key Lifecycle Manager sur un autre système, copiez le fichier d'exportation sur ce système en utilisant un support tel qu'un disque, ou par transmission électronique.

   Interface graphique

   a. Cliquez sur **Parcourir** pour spécifier l'emplacement du fichier d'exportation sous le répertoire <SKLM_DATA>, par exemple

C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data. Pour la définition de <SKLM_DATA>, voir Définitions relatives à un répertoire *HOME* et d'autres variables de répertoire.

b. Cliquez sur **Afficher les exportations** pour afficher les fichiers d'exportation.

c. Dans le tableau, sélectionnez un fichier d'exportation.

d. Cliquez sur **Importer**.

e. Vous pouvez également cliquer deux fois ou faire un clic droit sur le fichier d'exportation et sélectionner **Importer**.

f. Sur la boîte de dialogue Importer à partir de l'archive d'exportation, indiquez le mot de passe de chiffrement que vous avez utilisé pour créer le fichier d'exportation.

g. Cliquez sur **Importer** pour démarrer l'opération d'importation.

Interface REST

a. Obtenez un identificateur d'authentification utilisateur unique pour accéder aux services REST d'IBM Security Key Lifecycle Manager. Pour plus d'informations sur le processus d'authentification, voir Processus d'authentification pour les services REST.

b. Pour exécuter le **service REST Device Group Import**, envoyez la demande POST HTTP. Transmettez l'identificateur d'authentification utilisateur que vous avez obtenu à l'étape a avec le message de demande, conformément à l'exemple suivant :

```
POST https://localhost:<port>/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\\data
"password": "passw0rd123"}
```

3. Si les conflits sont détectés lors de l'opération d'importation, vous pouvez afficher la liste des conflits dans la fenêtre Conflits lors de l'importation.

4. Le **Service REST de conflits d'importation de groupe d'unités** énumère les conflits de données, le cas échéant, lorsque les données de groupe d'unités sont importées à partir d'un fichier d'exportation dans une instance d'IBM Security Key Lifecycle Manager. Pour exécuter le **Service REST Device Group Import**, envoyez la demande POST HTTP.

```
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_v2.7
"password": "passw0rd123"}
```

5. Pour exporter les données de conflits d'importation dans un fichier de valeurs séparées par des virgules (format CSV) pour une analyse ultérieure, cliquez sur **Exporter le rapport des conflits**.

Que faire ensuite

Vous devez résoudre les conflits pour que les données puissent être importées. Vous pouvez utiliser les services REST suivants pour résoudre les conflits d'importation :

- **Service REST Change Name**
- **Service REST Change Certificate Alias**
- **Service REST Change History**

- **Service REST Renew Key Alias**

Affichage de l'historique d'importation et d'exportation d'un groupe d'unités

La page Historique inclut les détails de toutes les opérations d'exportation et d'importation de groupe d'unités s'exécutant sur l'instance en cours d'IBM Security Key Lifecycle Manager.

Procédure

1. Connectez-vous à l'interface graphique.
2. Sur la page Bienvenue, cliquez sur **Administration** > **Exporter et importer**.
3. Dans la page Exporter et importer, cliquez sur **Historique**.

   Une liste des opérations d'exportation et d'importation de groupes d'unités exécutées sur l'instance actuelle d'IBM Security Key Lifecycle Manager s'affiche.
4. Sélectionnez une ligne et cliquez deux fois. Les détails récapitulatifs de l'opération d'exportation ou d'importation sont affichés.

Affichage des informations récapitulatives d'exportation et d'importation d'un groupe d'unités

La page Récapitulatif d'exportation/d'importation présente les informations détaillées d'un fichier d'exportation sélectionné permettant de comprendre et d'utiliser les données du groupe d'unités. Vous pouvez également consulter les informations détaillées d'un fichier d'exportation créé dans l'instance en cours d'IBM Security Key Lifecycle Manager. Vous pouvez également consulter les informations détaillées d'un fichier d'exportation que vous souhaitez importer dans l'instance en cours d'IBM Security Key Lifecycle Manager.

Procédure

1. Connectez-vous à l'interface graphique.
2. Sur la page Bienvenue, cliquez sur **Administration** > **Exporter et importer**.
3. Sélectionnez un fichier d'exportation de groupes d'unités répertorié dans le tableau.
4. Cliquez sur **Récapitulatif**.
5. Vous pouvez également faire un clic droit sur le fichier d'exportation et sélectionner **Récapitulatif**.

   Le tableau suivant fournit les informations récapitulatives.

ID	ID du fichier d'exportation de groupe d'unités sélectionné.
Nom de l'archive	Nom du fichier d'exportation du groupe d'unités.
Heure de début	Heure de début de l'opération d'exportation ou d'importation.
Heure de fin	Heure de fin de l'opération d'exportation ou d'importation.
Groupe d'unités	Nom du groupe d'unités à partir duquel les données sont exportées vers le fichier.
<données groupe unités>	Affiche le nombre de certificats, de groupes de clés ainsi que d'autres détails du fichier d'exportation de groupe d'unités.

6. Cliquez sur **Annuler** pour fermer la page de récapitulatif.

Sauvegarde et restauration

IBM Security Key Lifecycle Manager fournit un ensemble d'opérations permettant de sauvegarder et de restaurer les fichiers et les données en cours et actifs.

IBM Security Key Lifecycle Manager crée des fichiers de sauvegarde multiplateformes indépendamment des systèmes d'exploitation et de l'arborescence du serveur. Vous pouvez restaurer les fichiers de sauvegarde sur un système d'exploitation différent de celui à partir duquel ils ont été créés. Par exemple, vous pouvez restaurer un fichier de sauvegarde qui a été créé sur un système Linux sur un système Windows.

Vous pouvez vous servir de l'utilitaire de sauvegarde multiplateforme afin d'effectuer une opération de sauvegarde de versions précédentes d'IBM Security Key Lifecycle Manager et d'IBM Tivoli Key Lifecycle Manager en vue de sauvegarder les données critiques. Vous pouvez restaurer ces fichiers de sauvegarde dans la version actuelle d'IBM Security Key Lifecycle Manager sur divers systèmes d'exploitation.

Remarque : Dans IBM Security Key Lifecycle Manager version 3.0 et ultérieure, le système d'exploitation Solaris n'est pas pris en charge. Si vous utilisez IBM Security Key Lifecycle Manager sur des systèmes Solaris, servez-vous de l'utilitaire de sauvegarde multiplateforme pour sauvegarder les données. Vous pouvez ensuite exécuter l'opération de restauration afin de restaurer les données sur un système IBM Security Key Lifecycle Manager version 3.0 ou ultérieure déployé sur l'un des systèmes d'exploitation pris en charge, par exemple Windows, Linux ou AIX.

Les fichiers sauvegardés incluent les données suivantes :

- Les données dans les tables de base de données IBM Security Key Lifecycle Manager
- Le fichier de clés certifiées et le magasin de clés avec la clé principale
- Les fichiers de configuration d'IBM Security Key Lifecycle Manager

Votre rôle doit avoir les droits d'utilisation des actions de sauvegarde et de restauration de fichiers.

Si vous ne sauvegardez pas correctement vos données sensibles, vous risquez de perdre définitivement et totalement l'accès à vos données chiffrées, sans possibilité de récupération. Ne chiffrez pas votre fichier de sauvegarde et ne le stockez pas sur une unité chiffrée. A défaut de sauvegarder vos données, vous risquez également d'être confronté ultérieurement à une incohérence du gestionnaire de clés, ainsi qu'à des pertes de données sur l'unité de stockage.

Les opérations de sauvegarde et de restauration d'IBM Security Key Lifecycle Manager prennent en charge l'utilisation d'une longueur de clé AES de 256 bits pour le chiffrement/déchiffrement des données, conformément aux standards PCI-DSS (Payment Card Industry Data Security Standard), afin d'améliorer la sécurité des données.

Méthodes de chiffrement pour sauvegarder les données IBM Security Key Lifecycle Manager

IBM Security Key Lifecycle Manager prend en charge les méthodes de chiffrement suivantes pour les sauvegardes :

Chiffrement par mot de passe
Pendant le processus de sauvegarde, un mot de passe est spécifié pour chiffrer la clé de sauvegarde et vous devez spécifier le même mot de passe de chiffrement pour déchiffrer et restaurer les fichiers de sauvegarde.

Chiffrement basé sur HSM
Vous pouvez configurer IBM Security Key Lifecycle Manager pour utiliser Hardware Security Module (HSM) afin de stocker la clé de chiffrement principale. Pendant le processus de sauvegarde, la clé de sauvegarde est chiffrée par la clé principale, qui est stockée dans HSM. Pendant le processus de restauration, la clé principale dans HSM déchiffre la clé de sauvegarde. Ensuite, la clé de sauvegarde est utilisée pour restaurer le contenu de sauvegarde.

Sauvegarde et restauration de haute performance

La sauvegarde et la restauration de haute performance permettent de sauvegarder et de restaurer de grandes quantités de clés de chiffrement. Vous pouvez configurer IBM Security Key Lifecycle Manager pour des opérations de sauvegarde et de restauration de haute performance en définissant le paramètre suivant dans le fichier de configuration `SKLMConfig.properties` :

```
enableHighScaleBackup=true
```

Lorsqu'IBM Security Key Lifecycle Manager est configuré pour la sauvegarde et la restauration de haute performance, la technologie de sauvegarde native d'IBM Db2 est utilisée pour exécuter l'opération de sauvegarde et de restauration pour plus d'efficacité. Toutefois, dans cette configuration, vous ne pouvez restaurer la sauvegarde que dans un environnement d'exploitation identique. Le système d'exploitation, les composants middleware, et les structures de répertoires doivent être identiques sur les deux systèmes.

Vous ne pouvez pas créer de fichier de sauvegarde compatible sur plusieurs plateformes si IBM Security Key Lifecycle Manager est configuré pour des activités de sauvegarde et de restauration de haute performance. Pour plus d'informations sur la façon de sauvegarder une quantité importante de données, consultez «Sauvegarde de grande quantité de données», à la page 135.

Configurations requises pour l'exécution de la sauvegarde et de la restauration

Il existe plusieurs configurations requises pour l'exécution de la sauvegarde et de la restauration de données à partir des fichiers de sauvegarde d'IBM Security Key Lifecycle Manager.

Evitez les défaillances dues à des dépassements de délai en augmentant le délai imparti aux transactions de sauvegarde et de restauration pour le remplissage de grandes quantités de clés. Spécifiez une valeur plus élevée pour le paramètre **totalTranLifetimeTimeout** dans ce fichier :

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

En outre, les conditions suivantes doivent être vérifiées :

- Veillez à ce que la tâche soit exécutée au cours d'une période se prêtant à un arrêt temporaire de l'activité de service de clés.
- Pour une tâche de sauvegarde, le serveur IBM Security Key Lifecycle Manager doit être dans un état fonctionnel normal. L'instance de la base de données d'IBM Security Key Lifecycle Manager doit être disponible.
- Pour une tâche de restauration, l'instance de la base de données d'IBM Security Key Lifecycle Manager doit être accessible par l'intermédiaire de la source de données IBM Security Key Lifecycle Manager.

  Avant de commencer une tâche de restauration pour les sauvegardes de chiffrement par mot de passe, vérifiez que vous disposez du mot de passe utilisé lors de la création du fichier de sauvegarde.
- Utilisez les instructions suivantes pour restaurer les sauvegardes de chiffrement basé sur HSM :
  - Assurez-vous que la même partition HSM se trouve avec toutes ses entrées clés intactes sur le système où le fichier de sauvegarde est restauré.
  - La clé principale qui a été utilisée pour le chiffrement de la clé de sauvegarde doit être intacte pour restaurer le fichier de sauvegarde. Si la clé principale est rafraîchie, toutes les anciennes sauvegardes sont inaccessibles ou inutilisables.
  - Vous devez vous connecter aux mêmes instance HSM et clé principale pour les opérations de sauvegarde et de restauration, indépendamment du fait que vous utilisez le chiffrement basé sur HSM ou le chiffrement par mot de passe.
- Vérifiez que les répertoires associés à la propriété **tklm.backup.dir** existent. Assurez-vous également que ces répertoires sont accessibles en lecture et en écriture, tant pour le système que pour les comptes d'administrateur IBM Security Key Lifecycle Manager avec lesquels sont exécutés le serveur IBM Security Key Lifecycle Manager et le serveur Db2.

Sauvegarde des données avec chiffrement par mot de passe

Vous devez spécifier un mot de passe de chiffrement pour sauvegarder les données IBM Security Key Lifecycle Manager. Utilisez le même mot de passe pour déchiffrer et restaurer les fichiers de sauvegarde.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser la page Sauvegarde et restauration. Les données critiques peuvent aussi être sauvegardées à l'aide de la commande **tklmBackupRun** ou de **Service REST Backup Run**. Votre rôle doit avoir un droit d'utilisation de l'action de sauvegarde de fichiers.

IBM Security Key Lifecycle Manager crée des fichiers de sauvegarde indépendamment des systèmes d'exploitation et de l'arborescence du serveur. Vous pouvez restaurer les fichiers de sauvegarde sur un système d'exploitation différent de celui à partir duquel ils ont été créés.

Remarque : La diffusion d'un message signalant la réussite d'une opération de sauvegarde se fait à l'échelle du système. Or, deux administrateurs peuvent exécuter chacun de leur côté des tâches de sauvegarde qui se chevauchent dans le temps. Pendant cette période de chevauchement, si la tâche lancée en deuxième échoue, l'administrateur qui en est à l'origine peut très bien voir s'afficher le message de réussite de la première tâche et penser, à tort, qu'il s'agit de la sienne.

Procédure

1. Accédez à la page ou au répertoire approprié.

   Interface graphique

   a. Connectez-vous à l'interface graphique.

   b. Sur la page Bienvenue, cliquez sur **Administration** > **Sauvegarde et restauration**.

   Interface de ligne de commande

   a. Accédez au répertoire `WAS_HOME/bin`. Par exemple,

      Windows

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

      Linux

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

   b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme `SKLMAdmin`. Par exemple,

      Windows

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

      Linux

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

   Interface REST

   Ouvrez un client REST.

2. Créez un fichier de sauvegarde. Vous ne pouvez exécuter qu'une tâche de sauvegarde ou de restauration à un moment donné.

   Interface graphique

   a. Dans la table **Sauvegarde et restauration**, la zone **Emplacement du référentiel de sauvegarde** affiche le chemin de répertoire <*SKLM_DATA*> par défaut dans lequel le fichier de sauvegarde est stocké, par exemple `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data`. Pour la définition de <*SKLM_DATA*>, voir Définitions relatives à un répertoire *HOME* et d'autres variables de répertoire. Cliquez sur **Parcourir** pour spécifier l'emplacement du référentiel de sauvegarde sous le répertoire <*SKLM_DATA*>.

      Le chemin de répertoire dans la zone **Emplacement du référentiel de sauvegarde** change en fonction de la valeur définie pour la propriété **tklm.backup.dir** dans le fichier `SKLMConfig.properties`.

   b. Cliquez sur **Créer une sauvegarde**.

   c. Dans la page Créer une sauvegarde, indiquez les informations, notamment une valeur pour le mot de passe de chiffrement et la description de sauvegarde. Un emplacement de fichier de sauvegarde en lecture seule est affiché dans la zone **Emplacement de la sauvegarde**. Retenez le mot de passe de chiffrement car vous en aurez besoin si vous devez restaurer des données à partir de cette sauvegarde.

   d. Cliquez sur **Créer une sauvegarde**.

   Interface de ligne de commande

   Tapez **tklmBackupRun**, l'emplacement de la sauvegarde, le mot de passe de chiffrement et toute autre information nécessaire pour créer un fichier de sauvegarde. Par exemple :

   ```
   print AdminTask.tklmBackupRun ('[-backupDirectory C:\\sklmbackup1 -password myBackupPw
   ```

Interface REST

a. Obtenez un identificateur d'authentification utilisateur unique pour accéder aux services REST d'IBM Security Key Lifecycle Manager. Pour plus d'informations sur le processus d'authentification, voir Processus d'authentification pour les services REST.

b. Pour exécuter le **service REST Backup Run**, envoyez la demande HTTP POST. Transmettez l'identificateur d'authentification utilisateur que vous avez obtenu à l'étape a avec le message de demande, conformément à l'exemple suivant :

```
POST https://localhost:<port>/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 message indique que le fichier de sauvegarde a été créé ou que l'opération de sauvegarde a réussi.

   L'horodatage d'un fichier de sauvegarde présente un décalage par rapport à l'heure GMT qui est représenté au format RFC 822. Le nom de fichier contient un élément *+hhmm* ou *-hhmm* pour spécifier un fuseau horaire en avance ou en retard par rapport à l'heure GMT. Par exemple, un nom de fichier peut être sklm_v3.0.1.0_20170123144220**-0800**_backup.jar, où -0800 indique que le fuseau horaire a 8 h de retard par rapport à l'heure GMT.

Que faire ensuite

Retenez le mot de passe de chiffrement car vous en aurez besoin si vous devez restaurer des données à partir de cette sauvegarde. Examinez le répertoire dans lequel les fichiers de sauvegarde sont stockés pour vérifier que le fichier de sauvegarde que vous venez de créer y figure. Ne modifiez pas les fichiers qui se trouvent dans le fichier JAR de sauvegarde. Sinon, ils deviennent illisibles.

Sauvegarde des données avec un chiffrement par mot de passe lorsque HSM est configuré

Vous devez définir la propriété **enablePBEInHSM=true** dans le fichier SKLMConfig.properties pour sauvegarder des données avec le chiffrement par mot de passe lorsque HSM est configuré.

Avant de commencer

Assurez-vous que IBM Security Key Lifecycle Manager est configuré pour utiliser HSM pour stocker la clé principale, à l'aide des étapes de la rubrique «Configuration de paramètres HSM», à la page 215.

Pourquoi et quand exécuter cette tâche

Lorsque HSM est configuré, au cours du processus de sauvegarde, la clé principale dans HSM chiffre la clé de sauvegarde. Le chiffrement basé sur HSM est la méthode par défaut pour les sauvegardes lorsque HSM est configuré pour stocker la clé principale. Pour plus d'informations sur le chiffrement basé sur HSM, voir Chiffrement basé sur HSM pour les sauvegardes. Votre rôle doit avoir un droit d'utilisation de l'action de sauvegarde de fichiers.

Remarque : La diffusion d'un message signalant la réussite d'une opération de sauvegarde se fait à l'échelle du système. Or, deux administrateurs peuvent

exécuter chacun de leur côté des tâches de sauvegarde qui se chevauchent dans le temps. Pendant cette période de chevauchement, si la tâche lancée en deuxième échoue, l'administrateur qui en est à l'origine peut très bien voir s'afficher le message de réussite de la première tâche et penser, à tort, qu'il s'agit de la sienne.

Procédure

1. Définissez la propriété **enablePBEInHSM=true** dans le fichier *<SKLM_HOME>*/config/SKLMConfig.properties.

   Interface de ligne de commande

   a. Accédez au répertoire WAS_HOME/bin. Par exemple,

      Windows

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

      Linux

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

   b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme SKLMAdmin. Par exemple,

      Windows

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

      Linux

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

   c. Exécutez la commande CLI **tklmConfigUpdateEntry** pour définir la propriété **enablePBEInHSM** dans le fichier de configuration SKLMConfig.properties.

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

   Interface REST

   a. Ouvrez un client REST.

   b. Obtenez un identificateur d'authentification utilisateur unique pour accéder aux services REST d'IBM Security Key Lifecycle Manager. Pour plus d'informations sur le processus d'authentification, voir Processus d'authentification pour les services REST.

   c. Exécutez le **service REST Update Config Property** pour définir la propriété **enablePBEInHSM** dans le fichier de configuration SKLMConfig.properties. Transmettez l'identificateur d'authentification utilisateur que vous avez obtenu à l'étape b avec le message de demande, conformément à l'exemple suivant :

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

2. Accédez à la page ou au répertoire approprié pour sauvegarder les données.

   Interface graphique

   a. Connectez-vous à l'interface graphique.

   b. Sur la page Bienvenue, cliquez sur **Administration** > **Sauvegarde et restauration**.

   Interface de ligne de commande

   a. Accédez au répertoire WAS_HOME/bin.

b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme SKLMAdmin.

Interface REST

Ouvrez un client REST.

3. Créez un fichier de sauvegarde. Vous ne pouvez exécuter qu'une tâche de sauvegarde ou de restauration à un moment donné.

Interface graphique

a. Dans la table **Sauvegarde et restauration**, la zone **Emplacement du référentiel de sauvegarde** affiche le chemin de répertoire <*SKLM_DATA*> par défaut dans lequel le fichier de sauvegarde est stocké, par exemple C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data. Pour la définition de <*SKLM_DATA*>, voir Définitions relatives à un répertoire *HOME* et d'autres variables de répertoire. Cliquez sur **Parcourir** pour spécifier l'emplacement du référentiel de sauvegarde sous le répertoire <*SKLM_DATA*>.

Le chemin de répertoire dans la zone **Emplacement du référentiel de sauvegarde** change en fonction de la valeur définie pour la propriété **tklm.backup.dir** dans le fichier SKLMConfig.properties.

b. Cliquez sur **Créer une sauvegarde**.

c. Dans la page Créer une sauvegarde, indiquez les informations, notamment une valeur pour le mot de passe de chiffrement et la description de sauvegarde. Un emplacement de fichier de sauvegarde en lecture seule est affiché dans la zone **Emplacement de la sauvegarde**. Retenez le mot de passe de chiffrement car vous en aurez besoin si vous devez restaurer des données à partir de cette sauvegarde.

d. Cliquez sur **Créer une sauvegarde**.

Interface de ligne de commande

Tapez **tklmBackupRun**, l'emplacement de la sauvegarde, le mot de passe et toute autre information nécessaire pour créer un fichier de sauvegarde, comme indiqué dans l'exemple ci-dessous.

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

Interface REST

Exécutez le **service REST Backup Run** en envoyant la demande HTTP POST, comme illustré dans l'exemple suivant :

```
POST https://localhost:<port>/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 message indique que le fichier de sauvegarde a été créé ou que l'opération de sauvegarde a réussi.

L'horodatage d'un fichier de sauvegarde présente un décalage par rapport à l'heure GMT qui est représenté au format RFC 822. Le nom de fichier contient un élément *+hhmm* ou *-hhmm* pour spécifier un fuseau horaire en avance ou en retard par rapport à l'heure GMT. Par exemple, un nom de fichier peut être sklm_v3.0.1.0_20170123144220**-0800**_backup.jar, où -0800 indique que le fuseau horaire a 8 h de retard par rapport à l'heure GMT.

Que faire ensuite

Ne modifiez pas les fichiers qui se trouvent dans le fichier JAR de sauvegarde. Sinon, ils deviennent illisibles. Vous devez vous connecter aux mêmes instance HSM et clé principale pour les opérations de sauvegarde et de restauration, indépendamment du fait que vous utilisez le chiffrement basé sur HSM ou le chiffrement par mot de passe.

Sauvegarde des données avec chiffrement basé sur HSM

Lorsque IBM Security Key Lifecycle Manager est configuré avec le module de sécurité matériel (HSM) pour stocker la clé de chiffrement principale, vous pouvez utiliser le chiffrement basé sur HSM pour la création de sauvegardes sécurisées.

Avant de commencer

Assurez-vous que IBM Security Key Lifecycle Manager est configuré pour utiliser HSM pour stocker la clé principale avant de sauvegarder les données avec un chiffrement basé sur HSM. Pour connaître les étapes de configuration, voir «Configuration de paramètres HSM», à la page 215.

Vous devez tenir compte des directives suivantes pour le chiffrement HSM

- La même partition HSM doit se trouver avec toutes ses entrées clés sur le système où le fichier de sauvegarde est restauré.
- La clé principale que vous avez utilisée pour le chiffrement de la clé de sauvegarde doit être intacte pour restaurer le fichier de sauvegarde. Si la clé principale est rafraîchie, toutes les anciennes sauvegardes sont inaccessibles ou inutilisables.
- Vous devez vous connecter aux mêmes instance HSM et clé principale pour les opérations de sauvegarde et de restauration, indépendamment du fait que vous utilisez le chiffrement basé sur HSM ou le chiffrement par mot de passe.

Pourquoi et quand exécuter cette tâche

Lorsque vous exécutez l'opération de sauvegarde d'IBM Security Key Lifecycle Manager, une archive de sauvegarde est créée. La clé de sauvegarde dans l'archive chiffre le contenu de sauvegarde. La clé principale dans HSM chiffre la clé de sauvegarde. Pendant le processus de restauration, la clé principale, qui est stockée dans HSM, déchiffre la clé de sauvegarde. Ensuite, la clé de sauvegarde est utilisée pour restaurer le contenu de sauvegarde. Pour plus d'informations sur le chiffrement basé sur HSM, voir Chiffrement basé sur HSM pour les sauvegardes. Votre rôle doit avoir un droit d'utilisation de l'action de sauvegarde de fichiers.

IBM Security Key Lifecycle Manager crée des fichiers de sauvegarde indépendamment des systèmes d'exploitation et de l'arborescence du serveur. Vous pouvez restaurer les fichiers de sauvegarde sur un système d'exploitation différent de celui à partir duquel ils ont été créés.

Remarque : La diffusion d'un message signalant la réussite d'une opération de sauvegarde se fait à l'échelle du système. Or, deux administrateurs peuvent exécuter chacun de leur côté des tâches de sauvegarde qui se chevauchent dans le temps. Pendant cette période de chevauchement, si la tâche lancée en deuxième échoue, l'administrateur qui en est à l'origine peut très bien voir s'afficher le message de réussite de la première tâche et penser, à tort, qu'il s'agit de la sienne.

Procédure

1. Accédez à la page ou au répertoire approprié.

   Interface graphique

   a. Connectez-vous à l'interface graphique.

   b. Sur la page Bienvenue, cliquez sur **Administration** > **Sauvegarde et restauration**.

   Interface de ligne de commande

   a. Accédez au répertoire `WAS_HOME/bin`. Par exemple,

      Windows

      ```
      cd unité:\Program Files (x86)\IBM\WebSphere\AppServer\
      bin
      ```

      Linux

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

   b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme `SKLMAdmin`. Par exemple,

      Windows

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

      Linux

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

   Interface REST

   Ouvrez un client REST.

2. Créez un fichier de sauvegarde. Vous ne pouvez exécuter qu'une tâche de sauvegarde ou de restauration à un moment donné.

   Interface graphique

   a. Dans la table **Sauvegarde et restauration**, la zone **Emplacement du référentiel de sauvegarde** affiche le chemin de répertoire *<SKLM_DATA>* par défaut dans lequel le fichier de sauvegarde est stocké, par exemple `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data`. Pour la définition de *<SKLM_DATA>*, voir Définitions relatives à un répertoire *HOME* et d'autres variables de répertoire. Cliquez sur **Parcourir** pour spécifier l'emplacement du référentiel de sauvegarde sous le répertoire *<SKLM_DATA>*.

      Le chemin de répertoire dans la zone **Emplacement du référentiel de sauvegarde** change en fonction de la valeur définie pour la propriété **tklm.backup.dir** dans le fichier `SKLMConfig.properties`.

   b. Cliquez sur **Créer une sauvegarde**.

   c. Sur la page Créer une sauvegarde, spécifiez une description. Un emplacement de fichier de sauvegarde en lecture seule est affiché dans la zone **Emplacement de la sauvegarde**.

   d. Cliquez sur **Créer une sauvegarde**.

   Interface de ligne de commande

   Tapez **tklmBackupRun**, l'emplacement de la sauvegarde, et toute autre information nécessaire pour créer un fichier de sauvegarde. Par exemple :

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

   Interface REST

a. Obtenez un identificateur d'authentification utilisateur unique pour accéder aux services REST d'IBM Security Key Lifecycle Manager. Pour plus d'informations sur le processus d'authentification, voir Processus d'authentification pour les services REST.

b. Pour exécuter le **service REST Backup Run**, envoyez la demande HTTP POST. Transmettez l'identificateur d'authentification utilisateur que vous avez obtenu à l'étape a avec le message de demande, conformément à l'exemple suivant :

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

3. Un message indique que le fichier de sauvegarde a été créé ou que l'opération de sauvegarde a réussi.

   L'horodatage d'un fichier de sauvegarde présente un décalage par rapport à l'heure GMT qui est représenté au format RFC 822. Le nom de fichier contient un élément *+hhmm* ou *-hhmm* pour spécifier un fuseau horaire en avance ou en retard par rapport à l'heure GMT. Par exemple, un nom de fichier peut être sklm_v3.0.1.0_20170123144220**-0800**_backup.jar, où -0800 indique que le fuseau horaire a 8 h de retard par rapport à l'heure GMT.

Que faire ensuite

Ne modifiez pas les fichiers qui se trouvent dans le fichier JAR de sauvegarde. Sinon, ils deviennent illisibles. La clé principale qui a été utilisée pour le chiffrement de la clé de sauvegarde doit être intacte pour restaurer le fichier de sauvegarde. Si la clé principale est rafraîchie, toutes les anciennes sauvegardes sont inaccessibles ou inutilisables.

Sauvegarde de grande quantité de données

Vous devez définir la propriété **enableHighScaleBackup=true** dans le fichier de configuration SKLMConfig.properties pour sauvegarder un grand nombre de clés de chiffrement.

Pourquoi et quand exécuter cette tâche

La page Sauvegarde et restauration permet de sauvegarder des données. Les données peuvent aussi être sauvegardées à l'aide de la commande **tklmBackupRun** ou du **service REST Backup Run**. Votre rôle doit avoir un droit d'utilisation de l'action de sauvegarde de fichiers.

Remarque :

- Vous ne pouvez pas créer un fichier de sauvegarde compatible multiplateforme si IBM Security Key Lifecycle Manager est configuré pour des activités de sauvegarde et de restauration de haute performance. Vous pouvez utiliser le fichier de sauvegarde pour restaurer des données dans un environnement d'exploitation identique. Le système d'exploitation, les composants middleware, et les structures de répertoires doivent être identiques sur les deux systèmes.
- Le fichier db2restore.log est créé pendant le processus de restauration uniquement lorsque IBM Security Key Lifecycle Manager est configuré pour des opérations de sauvegarde et de restauration de haute performance.

Procédure

1. Définissez la propriété **enableHighScaleBackup=true** dans le fichier <*SKLM_HOME*>/config/SKLMConfig.properties.

   Interface de ligne de commande

   a. Accédez au répertoire <*WAS_HOME*>/bin. Par exemple,

      Windows

      ```
      cd unité:\Program Files (x86)\IBM\WebSphere\AppServer\
      bin
      ```

      Linux

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

   b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme SKLMAdmin. Par exemple,

      Windows

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

      Linux

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

   c. Exécutez la commande **tklmConfigUpdateEntry** pour définir la propriété **enableHighScaleBackup** dans le fichier de configuration SKLMConfig.properties.

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

   Interface REST

   a. Ouvrez un client REST.

   b. Obtenez un identificateur d'authentification utilisateur unique pour accéder aux services REST d'IBM Security Key Lifecycle Manager. Pour plus d'informations sur le processus d'authentification, voir Processus d'authentification pour les services REST.

   c. Exécutez le **service REST Update Config Property** pour définir la propriété **enableHighScaleBackup** dans le fichier de configuration SKLMConfig.properties. Transmettez l'identificateur d'authentification utilisateur que vous avez obtenu à l'étape b avec le message de demande, conformément à l'exemple suivant :

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

2. Accédez à la page ou au répertoire approprié pour sauvegarder les données.

   Interface graphique

   a. Connectez-vous à l'interface graphique.

   b. Sur la page Bienvenue, cliquez sur **Administration** > **Sauvegarde et restauration**.

   Interface de ligne de commande

   a. Accédez au répertoire <*WAS_HOME*>/bin.

   b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme SKLMAdmin.

   Interface REST

   Ouvrez un client REST.

3. Créez un fichier de sauvegarde. Une seule tâche de sauvegarde ou de restauration peut être exécutée à un moment donné.

   Interface graphique

   a. Dans la table **Sauvegarde et restauration**, la zone **Emplacement du référentiel de sauvegarde** affiche le chemin de répertoire <*SKLM_DATA*> par défaut dans lequel le fichier de sauvegarde est stocké, par exemple `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data`. Pour la définition de <*SKLM_DATA*>, voir Définitions relatives à un répertoire *HOME* et d'autres variables de répertoire. Cliquez sur **Parcourir** pour spécifier l'emplacement du référentiel de sauvegarde sous le répertoire <*SKLM_DATA*>.

      Le chemin de répertoire dans la zone **Emplacement du référentiel de sauvegarde** change en fonction de la valeur définie pour la propriété **`tklm.backup.dir`** dans le fichier `SKLMConfig.properties`.

   b. Cliquez sur **Créer une sauvegarde**.

   c. Dans la page Créer une sauvegarde, indiquez les informations, notamment une valeur pour le mot de passe de chiffrement et la description de sauvegarde. Un emplacement de fichier de sauvegarde en lecture seule est affiché dans la zone **Emplacement de la sauvegarde**. Retenez le mot de passe de chiffrement car vous en aurez besoin si vous devez restaurer des données à partir de cette sauvegarde.

      Remarque : Si le chiffrement basé sur HSM est utilisé pour les sauvegardes, vous ne devez pas spécifier le mot de passe.

   d. Cliquez sur **Créer une sauvegarde**.

   Interface de ligne de commande

   Entrez `tklmBackupRun` et spécifiez les valeurs nécessaires à la création d'un fichier de sauvegarde comme indiqué dans l'exemple ci-dessous.

   ```
   print AdminTask.tklmBackupRun ('[-backupDirectory C:\\sklmbackup1 -password myBackupPw
   ```

   Interface REST

   Exécutez le **`service REST Backup Run`** en envoyant la demande HTTP POST, comme illustré dans l'exemple suivant :

   ```
   POST https://localhost:<port>/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 message indique que le fichier de sauvegarde a été créé ou que l'opération de sauvegarde a réussi.

   L'horodatage d'un fichier de sauvegarde présente un décalage par rapport à l'heure GMT qui est représenté au format RFC 822. Le nom de fichier contient un élément *+hhmm* ou *-hhmm* pour spécifier un fuseau horaire en avance ou en retard par rapport à l'heure GMT. Par exemple, un nom de fichier peut être `sklm_v3.0.1.0_20170123144220-0800_backup.jar`, où -0800 indique que le fuseau horaire a 8 h de retard par rapport à l'heure GMT.

   Remarque : La diffusion d'un message signalant la réussite d'une opération de sauvegarde se fait à l'échelle du système. Or, deux administrateurs peuvent exécuter chacun de leur côté des tâches de sauvegarde qui se chevauchent dans le temps. Pendant cette période de chevauchement, si la tâche lancée en

deuxième échoue, l'administrateur qui en est à l'origine peut très bien voir s'afficher le message de réussite de la première tâche et penser, à tort, qu'il s'agit de la sienne.

Que faire ensuite

Retenez le mot de passe de chiffrement car vous en aurez besoin si vous devez restaurer des données à partir de cette sauvegarde. Examinez le répertoire dans lequel les fichiers de sauvegarde sont stockés pour vérifier que le fichier de sauvegarde que vous venez de créer y figure. Ne modifiez pas les fichiers qui se trouvent dans le fichier JAR de sauvegarde. Sinon, ils deviennent illisibles.

Restauration d'un fichier de sauvegarde

Une restauration permet de faire repasser le serveur IBM Security Key Lifecycle Manager à un état connu à l'aide des données de production sauvegardées, telles que les éléments de clés IBM Security Key Lifecycle Manager et d'autres informations critiques.

Avant de commencer

Utilisez les instructions suivantes pour restaurer les sauvegardes de chiffrement basé sur HSM :

- Assurez-vous que la même partition HSM se trouve avec toutes ses entrées clés intactes sur le système où le fichier de sauvegarde est restauré.
- La clé principale qui a été utilisée pour le chiffrement de la clé de sauvegarde doit être intacte pour restaurer le fichier de sauvegarde. Si la clé principale est rafraîchie, toutes les anciennes sauvegardes sont inaccessibles ou inutilisables.
- Vous devez vous connecter aux mêmes instance HSM et clé principale pour les opérations de sauvegarde et de restauration, indépendamment du fait que vous utilisez le chiffrement basé sur HSM ou le chiffrement par mot de passe.

Lorsque vous exécutez une opération de sauvegarde, le fichier de manifeste est créé en même temps que l'archive de sauvegarde. Avant de restaurer les fichiers de sauvegarde, vérifiez que le fichier de manifeste de sauvegarde répertorie tous les fichiers de données IBM Security Key Lifecycle Manager de l'archive.

Pourquoi et quand exécuter cette tâche

La page Sauvegarder et restaurer vous permet de supprimer un fichier de sauvegarde. Le fichier peut également être restauré à l'aide de la commande **tklmBackupRunRestore** ou de **Service REST Backup Run Restore**. Votre rôle doit avoir un droit d'utilisation de l'action de restauration de fichiers.. IBM Security Key Lifecycle Manager crée des fichiers de sauvegarde indépendamment des systèmes d'exploitation et de l'arborescence de l'application. Vous pouvez restaurer les fichiers de sauvegarde sur un système d'exploitation différent de celui à partir duquel ils ont été créés.

Avant de lancer une tâche de restauration, isolez le système en vue de sa maintenance. Faites une copie de sauvegarde du système existant. Vous pourrez l'utiliser ultérieurement pour rétablir l'état d'origine du système en cas de problème pendant le processus de restauration. Le serveur IBM Security Key Lifecycle Manager redémarre automatiquement après le processus de restauration. Vérifiez l'environnement avant de remettre en service le serveur IBM Security Key Lifecycle Manager.

Procédure

1. Accédez à la page ou au répertoire approprié(e) :

   Interface graphique

   a. Connectez-vous à l'interface graphique.

   b. Sur la page Bienvenue, cliquez sur **Administration** > **Sauvegarde et restauration**.

   Interface de ligne de commande

   a. Accédez au répertoire `WAS_HOME/bin`. Par exemple,

      Windows

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

      Linux

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

   b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme `SKLMAdmin`. Par exemple,

      Windows

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

      Linux

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

      Interface REST

      - Ouvrez un client REST.

2. Restaurez un fichier de sauvegarde sélectionné. Une seule tâche de sauvegarde ou de restauration peut être exécutée à un moment donné. Pour restaurer un fichier sur l'ordinateur secondaire, copiez-le sur cet ordinateur via un disque ou une transmission électronique.

   Interface graphique

   a. Sélectionnez un fichier de sauvegarde dans la table **Sauvegarder et restaurer**.

   b. Cliquez sur **Restaurer à partir d'une sauvegarde**.

      Remarque :

      - Si vous avez appliqué un groupe de correctifs sur des systèmes répartis, n'essayez pas de restaurer les fichiers de sauvegarde qui ont été créés avant l'application du groupe de correctifs.

   c. Dans la page Restaurer une sauvegarde, indiquez le mot de passe de chiffrement utilisé pour créer le fichier de sauvegarde.

      Remarque : Si le chiffrement basé sur HSM est utilisé pour les sauvegardes, vous ne devez pas spécifier le mot de passe.

   d. Cliquez sur **Restaurer une sauvegarde**.

   Interface de ligne de commande

   Entrez la commande `tklmBackupRunRestore` et indiquez les informations nécessaires, telles que le chemin et le nom du fichier de sauvegarde. Indiquez le mot de passe de chiffrement utilisé pour créer le fichier de sauvegarde. Par exemple, entrez :

   ```
   print AdminTask.tklmBackupRunRestore
    ('[-backupFilePath /opt/mysklmbackups/sklm_v3.0.1.0_20170705235417-1200_backup
     -password myBackupPwd]')
   ```

Remarque : Si le chiffrement basé sur HSM est utilisé pour les sauvegardes, vous ne devez pas spécifier le mot de passe.

Interface REST

a. Obtenez un identificateur d'authentification utilisateur unique pour accéder aux services REST d'IBM Security Key Lifecycle Manager. Pour plus d'informations sur le processus d'authentification, voir Processus d'authentification pour les services REST.

b. Pour exécuter le **service REST Backup Run Restore**, envoyez la demande HTTP POST. Transmettez l'identificateur d'authentification utilisateur que vous avez obtenu à l'étape a avec le message de demande, conformément à l'exemple suivant :

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

Remarque : Si le chiffrement basé sur HSM est utilisé pour les sauvegardes, vous ne devez pas spécifier le mot de passe.

3. Un message indique que l'opération de restauration a réussi.

Résultats

Le serveur IBM Security Key Lifecycle Manager redémarre automatiquement après qu'un fichier de sauvegarde est restauré lorsque la valeur de la propriété **autoRestartAfterRestore** est `true` (valeur par défaut) dans le fichier `SKLMConfig.properties`.

Remarque : Après le redémarrage automatique du serveur IBM Security Key Lifecycle Manager, la fenêtre d'état du service WebSphere Application Server n'est pas actualisée et celui-ci apparaît comme étant arrêté.

Que faire ensuite

Remarque : Après la restauration des données, assurez-vous que le chemin des propriétés dans les fichiers `SKLMConfig.properties`, `datastore.properties` et `ReplicationSKLMConfig.properties` est correct avant de procéder à votre prochaine tâche.

Vérifiez que l'état du serveur est celui attendu. Vous pouvez, par exemple, examiner le magasin de clés afin de déterminer s'il est désormais possible d'utiliser un certificat qui n'était pas disponible avant la restauration du fichier de sauvegarde.

Suppression d'un fichier de sauvegarde

Utilisez l'interface graphique ou l'interface de ligne de commande pour supprimer un fichier de sauvegarde de IBM Security Key Lifecycle Manager. Par exemple, vous pouvez souhaiter supprimer un fichier de sauvegarde si celui-ci n'a plus de raison d'être.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser la page Sauvegarde et restauration pour supprimer un fichier de sauvegarde.

Votre rôle doit avoir un droit d'utilisation de l'action de sauvegarde de fichiers.

Procédure

1. Connectez-vous à l'interface graphique.
2. Sur la page Bienvenue, cliquez sur **Administration** > **Sauvegarde et restauration**.
3. Sélectionnez un fichier de sauvegarde dans la table **Sauvegarder et restaurer**.
4. Cliquez sur **Supprimer une sauvegarde** et confirmez la suppression du fichier.

Que faire ensuite

Examinez le répertoire dans lequel les fichiers de sauvegarde sont stockés afin de déterminer si le fichier spécifié a été supprimé.

Exécution de tâches de sauvegarde et de restauration via l'interface de ligne de commande ou l'interface REST

Vous pouvez utiliser l'interface de ligne de commande ou l'interface REST pour effectuer d'autres tâches de sauvegarde et de restauration qui ne sont pas disponibles dans l'interface graphique.

Pourquoi et quand exécuter cette tâche

Avant de commencer, procurez-vous le mot de passe. Votre rôle doit avoir les droits d'utilisation des actions de sauvegarde et de restauration de fichiers.

Procédure

1. Accédez à la page ou au répertoire approprié.
   - Interface de ligne de commande
     a. Accédez au répertoire *<WAS_HOME>*/bin. Exemple :

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

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

     b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme SKLMAdmin. Exemple :

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

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

   - Interface REST :
     – Ouvrez un client REST.
2. Effectuez la tâche.
   - Interface de ligne de commande :

     tklmBackupGetProgress

Entrez la commande `tklmBackupGetProgress` pour déterminer la phase actuelle d'une tâche de sauvegarde en cours d'exécution. Par exemple, entrez :

```
print AdminTask.tklmBackupGetProgress ()
```

tklmBackupGetRestoreProgress

Entrez la commande `tklmBackupGetRestoreProgress` pour déterminer la phase actuelle d'une tâche de restauration en cours d'exécution. Par exemple, entrez :

```
print AdminTask.tklmBackupGetRestoreProgress ()
```

tklmBackupGetRestoreResult

Entrez la commande `tklmBackupGetRestoreResult` pour déterminer si une opération de restauration s'est terminée avec succès ou a échoué. Par exemple, entrez :

```
print AdminTask.tklmBackupGetRestoreResult ()
```

tklmBackupGetResult

Entrez la commande `tklmBackupGetResult` pour déterminer si une opération de sauvegarde s'est terminée avec succès ou a échoué. Par exemple, entrez :

```
print AdminTask.tklmBackupGetResult ()
```

tklmBackupIsRestoreRunning

Entrez la commande `tklmBackupIsRestoreRunning` pour déterminer si la tâche de restauration est en cours d'exécution. Par exemple, entrez :

```
print AdminTask.tklmBackupIsRestoreRunning ()
```

tklmBackupIsRunning

Entrez la commande `tklmBackupIsRunning` pour déterminer si la tâche de sauvegarde est en cours d'exécution. Par exemple, entrez :

```
print AdminTask.sklmBackupIsRunning()
```

tklmBackupList

Entrez la commande `tklmBackupList` pour répertorier les fichiers de sauvegarde figurant dans un répertoire. Par exemple, entrez :

```
print AdminTask.tklmBackupList
 ('[-backupDirectory C:\\sklmbackup1 -v y]')
```

- Interface REST :
  a. Obtenez un identificateur d'authentification utilisateur unique pour accéder aux services REST d'IBM Security Key Lifecycle Manager. Pour plus d'informations sur le processus d'authentification, voir Processus d'authentification pour les services REST.
  b. Pour appeler le service REST, envoyez la demande HTTP. Transmettez l'identificateur d'authentification utilisateur que vous avez obtenu à l'étape a avec le message de demande, conformément à l'exemple suivant :

Service REST Backup Get Progress

Utilisez le **service REST Backup Get Progress** pour déterminer la phase actuelle d'une tâche de sauvegarde en cours d'exécution. Par exemple, vous pouvez envoyer la demande HTTP suivante :

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

Service REST Backup Get Restore Progress

Utilisez le **service REST Backup Get Restore Progress** pour déterminer la phase actuelle d'une tâche de restauration en cours d'exécution. Par exemple, vous pouvez envoyer la demande HTTP suivante :

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

Service REST Backup Get Restore Result

Utilisez le **service REST Backup Get Restore Result** pour déterminer si une opération de restauration s'est terminée avec succès ou a échoué. Par exemple, vous pouvez envoyer la demande HTTP suivante :

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

Service REST Backup Get Result

Utilisez le **service REST Backup Get Result** pour déterminer si une opération de sauvegarde s'est terminée avec succès ou a échoué. Par exemple, vous pouvez envoyer la demande HTTP suivante :

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

Service REST Backup List

Utilisez le **service REST Backup List** pour répertorier les fichiers de sauvegarde figurant dans un répertoire. Par exemple, vous pouvez envoyer la demande HTTP suivante :

```
GET https://localhost:<port>/SKLM/rest/v1/ckms/backups?backupDirectory=
/sklmbackup
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth authId=139aeh34567m
Accept-Language : en
```

Opérations de sauvegarde et de restauration pour les versions précédentes d'IBM Security Key Lifecycle Manager et d'IBM Tivoli Key Lifecycle Manager

Vous pouvez vous servir de l'utilitaire de sauvegarde multiplateforme de la version actuelle d'IBM Security Key Lifecycle Manager afin d'effectuer une opération de sauvegarde de versions précédentes d'IBM Security Key Lifecycle Manager et d'IBM Tivoli Key Lifecycle Manager en vue de sauvegarder les données critiques. Vous pouvez restaurer ces fichiers de sauvegarde dans la version actuelle d'IBM Security Key Lifecycle Manager sur divers systèmes d'exploitation à l'aide de l'utilitaire de restauration.

Remarque : Pour plus de sécurité, modifiez le mot de passe utilisateur d'IBM Security Key Lifecycle Manager peu de temps après le processus de migration des données.

Migration croisée des données IBM Tivoli Key Lifecycle Manager, Version 1.0

Les utilitaires de sauvegarde et de restauration d'IBM Security Key Lifecycle Manager permettent d'effectuer la migration croisée des données IBM Tivoli Key Lifecycle Manager, version 1.0.

Pourquoi et quand exécuter cette tâche

La migration croisée des données IBM Tivoli Key Lifecycle Manager version 1.0 vers IBM Security Key Lifecycle Manager version 3.0.1 s'effectue en deux étapes qui sont présentées ci-dessous :

1. La migration des données IBM Tivoli Key Lifecycle Manager, version 1.0 vers un système où IBM Security Key Lifecycle Manager, version 2.7 est installé s'effectue en appliquant les étapes suivantes décrites dans la documentation IBM Security Key Lifecycle Manager, version 2.7.

   Sauvegarde des données d'IBM Tivoli Key Lifecycle Manager, version 1.0

   Restauration des fichiers de sauvegarde d'IBM Tivoli Key Lifecycle Manager, version 1.0
2. La migration des données d'IBM Security Key Lifecycle Manager version 2.7 sur un système sur lequel IBM Security Key Lifecycle Manager version 3.0.1 est installé s'effectue en appliquant les étapes décrites dans les rubriques suivantes.

   «Sauvegarde des données d'IBM Security Key Lifecycle Manager, version 2.7», à la page 164

   «Restauration des fichiers de sauvegarde d'IBM Security Key Lifecycle Manager, version 2.7», à la page 167

Migration croisée des données IBM Tivoli Key Lifecycle Manager, Version 2.0

Les utilitaires de sauvegarde et de restauration d'IBM Security Key Lifecycle Manager permettent d'effectuer la migration croisée des données IBM Tivoli Key Lifecycle Manager, version 2.0.

Pourquoi et quand exécuter cette tâche

La migration croisée des données IBM Tivoli Key Lifecycle Manager version 2.0 vers IBM Security Key Lifecycle Manager version 3.0.1 s'effectue en deux étapes qui sont présentées ci-dessous :

1. La migration des données IBM Tivoli Key Lifecycle Manager, version 2.0 vers un système où IBM Security Key Lifecycle Manager, version 2.7 est installé s'effectue en appliquant les étapes suivantes décrites dans la documentation IBM Security Key Lifecycle Manager, version 2.7.

   Sauvegarde des données d'IBM Tivoli Key Lifecycle Manager, version 2.0

   Restauration des fichiers de sauvegarde d'IBM Tivoli Key Lifecycle Manager, version 2.0

2. La migration des données d'IBM Security Key Lifecycle Manager version 2.7 sur un système sur lequel IBM Security Key Lifecycle Manager version 3.0.1 est installé s'effectue en appliquant les étapes décrites dans les rubriques suivantes.

   «Sauvegarde des données d'IBM Security Key Lifecycle Manager, version 2.7», à la page 164

   «Restauration des fichiers de sauvegarde d'IBM Security Key Lifecycle Manager, version 2.7», à la page 167

Migration croisée des données IBM Tivoli Key Lifecycle Manager, version 2.0.1

Les utilitaires de sauvegarde et de restauration d'IBM Security Key Lifecycle Manager permettent d'effectuer la migration croisée des données IBM Tivoli Key Lifecycle Manager, version 2.0.1.

Pourquoi et quand exécuter cette tâche

La migration croisée des données IBM Tivoli Key Lifecycle Manager version 2.0.1 vers IBM Security Key Lifecycle Manager version 3.0.1 s'effectue en deux étapes qui sont présentées ci-dessous :

1. La migration des données IBM Tivoli Key Lifecycle Manager, version 2.0.1 vers un système où IBM Security Key Lifecycle Manager, version 2.7 est installé s'effectue en appliquant les étapes suivantes décrites dans la documentation IBM Security Key Lifecycle Manager, version 2.7.

   Sauvegarde des données d'IBM Tivoli Key Lifecycle Manager, version 2.0.1

   Restauration des fichiers de sauvegarde d'IBM Tivoli Key Lifecycle Manager, version 2.0.1
2. La migration des données d'IBM Security Key Lifecycle Manager version 2.7 sur un système sur lequel IBM Security Key Lifecycle Manager version 3.0.1 est installé s'effectue en appliquant les étapes décrites dans les rubriques suivantes.

   «Sauvegarde des données d'IBM Security Key Lifecycle Manager, version 2.7», à la page 164

   «Restauration des fichiers de sauvegarde d'IBM Security Key Lifecycle Manager, version 2.7», à la page 167

Sauvegarde des données d'Encryption Key Manager, version 2.1

Utilisez l'utilitaire de sauvegarde d'IBM Security Key Lifecycle Manager version 3.0.1 pour créer des fichiers de sauvegarde d'Encryption Key Manager version 2.1.

Avant de commencer

- Vous devez installer IBM Security Key Lifecycle Manager version 3.0.1 sur un système.
- Vérifiez que le dossier Encryption Key Manager contient le fichier de configuration, le fichier du magasin de clés et d'autres fichiers de données et dossiers associés aux tables d'unité, aux groupes de clés et aux métadonnées.

Pourquoi et quand exécuter cette tâche

Vous pouvez vous servir de l'utilitaire de sauvegarde pour créer des fichiers de sauvegarde multiplateformes indépendamment des systèmes d'exploitation et de l'arborescence du serveur. Vous pouvez restaurer ces fichiers de sauvegarde

multiplateformes compatibles sur un système sur lequel est installé IBM Security Key Lifecycle Manager version 3.0.1, quel que soit le système d'exploitation.

Remarque : Pour plus de sécurité, modifiez le mot de passe utilisateur d'IBM Security Key Lifecycle Manager peu de temps après le processus de migration des données.

Procédure

1. Copiez le dossier Encryption Key Manager et tous les autres fichiers nécessaires sur un système sur lequel IBM Security Key Lifecycle Manager version 3.0.1 est installé.
2. Assurez-vous que le fichier `KeyManagerConfig.properties` et les fichiers figurant dans le fichier `KeyManagerConfig.properties` sont copiés.

   Remarque : Editez le fichier de configuration `KeyManagerConfig.properties` qui se trouve dans le dossier Encryption Key Manager afin de spécifier des chemins d'accès absolus au fichier du magasin de clés et aux autres fichiers de données, comme indiqué ci-dessous.

   ```
   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. Localisez le dossier des utilitaires de sauvegarde sur le système sur lequel la version 3.0.1 est installée.

   Windows

   `<SKLM_INSTALL_HOME>\migration\utilities\ekm21`

   L'emplacement par défaut est `C:\Program Files\IBM\SKLMV301\migration\utilities\ekm21`.

   Linux `<SKLM_INSTALL_HOME>/migration/utilities/ekm21`

   L'emplacement par défaut est `/opt/IBM/SKLMV301/migration/utilities/ekm21`.
4. Editez le fichier `backup.properties` qui se trouve dans le dossier des utilitaires de sauvegarde afin de configurer des propriétés conformément à l'exemple ci-dessous. Vous devez définir des valeurs pour toutes les propriétés, sauf pour la propriété `BACKUP_DIR` (facultative).

   Si vous n'indiquez pas de valeur pour `BACKUP_DIR`, le fichier de sauvegarde est créé dans le sous-dossier `backup` à partir duquel vous exécutez l'utilitaire de sauvegarde.

   Remarque : Sous Windows, le fichier `backup.properties` que vous utilisez pour les opérations de sauvegarde ne doit pas contenir d'espace avant ni après les valeurs et clés de propriété.

   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
```

Remarque : Sous Windows, lorsque vous spécifiez un chemin dans le fichier de propriétés, utilisez «/ » ou «\\ » comme séparateur de chemin, conformément à l'exemple suivant :

```
C:\\ekm_backup
```

ou

```
C:/ekm_backup
```

5. Ouvrez une invite de commande et exécutez l'utilitaire de sauvegarde.

   Windows

   Accédez au répertoire <*SKLM_INSTALL_HOME*>\migration\utilities\ekm21 et exécutez la commande suivante :

   backupEKM21.bat

   Linux

   a. Accédez au répertoire ekm21 (voir l'étape b).
   b. Vérifiez que le fichier backupEKM21.sh dispose de droits d'exécution. Si ce n'est pas le cas, accordez des droits en exécutant la commande suivante :

      ```
      chmod 755 backupEKM21.sh
      ```

   c. Exécutez l'utilitaire de sauvegarde :

      backupEKM21.sh

Que faire ensuite

- Examinez le répertoire dans lequel les fichiers de sauvegarde sont stockés pour vérifier que le fichier de sauvegarde que vous venez de créer y figure. Les fichiers de sauvegarde sont créés à l'emplacement que vous avez défini pour le paramètre BACKUP_DIR dans le fichier backup.properties.
- Vérifiez si le fichier backup.log contient des erreurs ou des exceptions. Ce fichier est créé dans le même répertoire que celui dans lequel vous avez exécuté l'utilitaire de sauvegarde. Pour que l'opération de sauvegarde aboutisse, assurez-vous que le fichier journal ne contient aucune erreur ni exception.
- Retenez le mot de passe de sauvegarde car vous en aurez besoin si vous devez restaurer des données à partir de cette sauvegarde.
- N'éditez pas les fichiers figurant dans l'archive de sauvegarde. Sinon, ils deviennent illisibles.

Restauration des fichiers de sauvegarde d'Encryption Key Manager, version 2.1

Vous pouvez restaurer les fichiers de sauvegarde multiplateformes d'Encryption Key Manager version 2.1 sur un système où est installé IBM Security Key Lifecycle Manager version 3.0.1 à l'aide de l'interface graphique, de l'interface de ligne de commande, de l'interface REST ou du script de restauration de migration.

Avant de commencer

Installez IBM Security Key Lifecycle Manager version 3.0.1 sur un système. Vous devez disposer du fichier de sauvegarde d'Encryption Key Manager et vous rappeler du mot de passe que vous avez utilisé lors de la création du fichier de sauvegarde.

Remarque : Vous devez disposer du rôle utilisateur IBM Security Key Lifecycle Manager pour exécuter les opérations de sauvegarde et de restauration.

Pourquoi et quand exécuter cette tâche

Vous pouvez restaurer les fichiers de sauvegarde multiplateformes compatibles avec Encryption Key Manager sur un système où est installé IBM Security Key Lifecycle Manager version 3.0.1, quel que soit le système d'exploitation.

Avant de lancer une tâche de restauration, isolez le système en vue de sa maintenance. Faites une copie de sauvegarde du système existant. Vous pourrez l'utiliser ultérieurement pour rétablir l'état d'origine du système en cas de problème pendant le processus de restauration. Le serveur IBM Security Key Lifecycle Manager redémarre automatiquement après le processus de restauration. Vérifiez l'environnement avant de remettre en service le serveur IBM Security Key Lifecycle Manager.

Remarque : Pour plus de sécurité, modifiez le mot de passe utilisateur d'IBM Security Key Lifecycle Manager peu de temps après le processus de migration des données.

Procédure

1. Connectez-vous au système sur lequel IBM Security Key Lifecycle Manager Version 3.0.1 est installé.
2. Copiez le fichier de sauvegarde, par exemple `sklm_vEKM21_20170420113253+0530_backup.jar`, depuis le système Encryption Key Manager version 2.1 vers un dossier de votre choix sous le répertoire *<SKLM_DATA>*, par exemple `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data`. Pour la définition de *<SKLM_DATA>*, voir Définitions relatives à un répertoire *HOME* et d'autres variables de répertoire.
3. Restaurez le fichier de sauvegarde en suivant l'une des méthodes ci-après.

Interface graphique	1. Connectez-vous à l'interface graphique en tant qu'utilisateur autorisé, par exemple `SKLMAdmin`. 2. Sur la page Bienvenue, cliquez sur **Administration** > **Sauvegarde et restauration**. 3. Cliquez sur **Parcourir** pour spécifier l'emplacement du fichier de sauvegarde Encryption Key Manager sous le répertoire *<SKLM_DATA>*. 4. Cliquez sur **Afficher les sauvegardes** pour afficher les fichiers de sauvegarde à restaurer. 5. Dans la table **Sauvegarde et restauration**, sélectionnez un fichier de sauvegarde. 6. Cliquez sur **Restaurer à partir d'une sauvegarde**. 7. Dans la page Restaurer une sauvegarde, spécifiez le mot de passe de sauvegarde que vous avez utilisé pour créer le fichier de sauvegarde. 8. Cliquez sur **Restaurer une sauvegarde**. 9. Redémarrez le serveur IBM Security Key Lifecycle Manager.

Interface de ligne de commande	1. Accédez au répertoire *<WAS_HOME>*/bin. Par exemple :
	Windows
	`cd unité:\Program Files\IBM\WebSphere\AppServer\bin`
	Linux `cd /opt/IBM/WebSphere/AppServer/bin`
	2. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme SKLMAdmin. Par exemple :
	Windows
	`wsadmin.bat -username SKLMAdmin -password mypwd -lang jython`
	Linux
	`./wsadmin.sh -username SKLMAdmin -password mypwd -lang jython`
	3. Exécutez la commande d'interface de ligne de commande **tklmBackupRunRestore** en spécifiant les paramètres tels que le nom du fichier de sauvegarde ainsi que son chemin d'accès complet et le mot de passe de sauvegarde que vous avez utilisé pour créer la sauvegarde, conformément à l'exemple suivant :
	`print AdminTask.tklmBackupRunRestore ('[-backupFilePath <SKLM_DATA>/sklm_vEKM21_20170420113253+0530_backup.jar -password myBackupPwd]')`
	4. Redémarrez le serveur IBM Security Key Lifecycle Manager.

Interface REST	1. Ouvrez un client REST.
	2. Obtenez un identificateur d'authentification utilisateur unique pour accéder aux services REST d'IBM Security Key Lifecycle Manager. Pour plus d'informations sur le processus d'authentification, voir Processus d'authentification pour les services REST.
	3. Pour appeler le **service REST Backup Run Restore**, envoyez la demande HTTP POST avec le nom du fichier de sauvegarde ainsi que son chemin d'accès complet et le mot de passe de sauvegarde sous forme de paramètres. Transmettez l'identificateur d'authentification utilisateur que vous avez obtenu à l'étape b avec le message de demande, conformément à l'exemple suivant :
	`POST https://localhost:<port>/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. Redémarrez le serveur IBM Security Key Lifecycle Manager.

Script de restauration de migration	1. Localisez les utilitaires de restauration d'IBM Security Key Lifecycle Manager. **Windows** <*SKLM_INSTALL_HOME*>\migration\utilities\ekm21 L'emplacement par défaut est C:\Program Files\IBM\SKLMV30\migration\utilities\ekm21. **Linux** <*SKLM_INSTALL_HOME*>/migration/utilities/ekm21 L'emplacement par défaut est /opt/IBM/SKLMV301/migration/utilities/ekm21. 2. Editez le fichier restore.properties dans le dossier ekm21 afin de configurer les propriétés, conformément à l'exemple ci-dessous : **Remarque :** Sous Windows, le fichier restore.properties que vous utilisez pour les opérations de restauration ne doit pas contenir d'espace avant ni après les valeurs et clés de propriété. **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.jar 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 Pour vous connecter à IBM Security Key Lifecycle Manager en utilisant les données d'identification utilisateur définies lors de l'installation du produit, attribuez la valeur «n» à la propriété **RESTORE_USER_ROLES**. Le fait d'attribuer la valeur «n» à cette propriété permet de garantir que l'ID utilisateur et le mot de passe ne sont pas remplacés par les données d'identification de l'ancienne version. **Remarque :** Sous Windows, lorsque vous spécifiez un chemin dans le fichier de propriétés, utilisez «/ » ou «\\ » comme séparateur de chemin, conformément à l'exemple suivant : C:\\ekm_restore ou C:/ekm_restore 3. Ouvrez une invite de commande et exécutez l'utilitaire de restauration. **Windows** Accédez au répertoire <*SKLM_INSTALL_HOME*>\migration\utilities\ekm21 et exécutez la commande suivante : **restoreEKM21.bat** **Linux** a. Accédez au répertoire <*SKLM_INSTALL_HOME*>/migration/utilities/ekm21. b. Vérifiez si le fichier restoreEKM21.sh dispose de droits d'exécution. Si ce n'est pas le cas, accordez des droits en exécutant la commande suivante : chmod 755 restoreEKM21.sh c. Exécutez la commande suivante : **restoreEKM21.sh** 4. Redémarrez le serveur IBM Security Key Lifecycle Manager.

Que faire ensuite

Remarque : Après la restauration des données, assurez-vous que le chemin des propriétés dans les fichiers `SKLMConfig.properties`, `datastore.properties` et `ReplicationSKLMConfig.properties` est correct avant de procéder à votre prochaine tâche.

Sauvegarde des données d'IBM Security Key Lifecycle Manager, version 2.5

Utilisez l'utilitaire de sauvegarde d'IBM Security Key Lifecycle Manager version 3.0.1 pour créer des fichiers de sauvegarde multiplateformes d'IBM Security Key Lifecycle Manager version 2.5.

Avant de commencer

Vous devez installer IBM Security Key Lifecycle Manager version 3.0.1 sur un système. Assurez-vous que le système sur lequel sont installés IBM Security Key Lifecycle Manager version 2.5 et le groupe de correctifs 3 est disponible.

Pourquoi et quand exécuter cette tâche

Vous pouvez vous servir de l'utilitaire de sauvegarde pour créer des fichiers de sauvegarde multiplateformes indépendamment des systèmes d'exploitation et de l'arborescence du serveur. Vous pouvez restaurer ces fichiers de sauvegarde multiplateformes compatibles sur un système sur lequel est installé IBM Security Key Lifecycle Manager version 3.0.1, quel que soit le système d'exploitation.

Remarque : Pour plus de sécurité, modifiez le mot de passe utilisateur d'IBM Security Key Lifecycle Manager peu de temps après le processus de migration des données.

Procédure

Procédez comme suit sur les systèmes où les versions 3.0.1 et 2.5 d'IBM Security Key Lifecycle Manager sont installées.

IBM Security Key Lifecycle Manager version3.0.1	1. Connectez-vous au système avec vos données d'identification utilisateur. 2. Localisez le dossier des utilitaires de sauvegarde. **Windows** `<SKLM_INSTALL_HOME>\migration\utilities\sklmv25` L'emplacement par défaut est `C:\Program Files\IBM\.SKLMV301\migration\utilities\sklmv25` **Linux** `<SKLM_INSTALL_HOME>/migration/utilities/sklmv25` L'emplacement par défaut est `/opt/IBM/SKLMV301/migration/utilities/sklmv25`.

IBM Security Key Lifecycle Manager version 2.5	1. Connectez-vous au système avec vos données d'identification utilisateur.
	2. Copiez le dossier `sklmv25` du système sur lequel IBM Security Key Lifecycle Manager version 3.0.1 est installé dans un répertoire local de votre choix.
	3. Editez `backup.properties` dans le dossier `sklmv25` afin de configurer les propriétés, conformément à l'exemple suivant : Vous devez définir des valeurs pour toutes les propriétés, sauf pour la propriété `BACKUP_DIR` (facultative).
	Si vous n'indiquez pas de valeur pour `BACKUP_DIR`, le fichier de sauvegarde est créé dans le sous-dossier `backup` à partir duquel vous exécutez l'utilitaire de sauvegarde.
	Remarque : Sous Windows, le fichier `backup.properties` que vous utilisez pour les opérations de sauvegarde ne doit pas contenir d'espace avant ni après les valeurs et clés de propriété.
	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`
	Remarque : Sous Windows, lorsque vous spécifiez un chemin dans le fichier de propriétés, utilisez «/ » ou «\\ » comme séparateur de chemin, conformément à l'exemple suivant :
	`C:\\sklmv25_backup`
	ou
	`C:/sklmv25_backup`
	4. Ouvrez une invite de commande et exécutez l'utilitaire de sauvegarde.
	Windows
	Accédez au répertoire `sklmv25` (voir étape b) et exécutez la commande suivante :
	`backupV25.bat`
	Linux
	a. Accédez au répertoire `sklmv25` (voir l'étape b).
	b. Vérifiez que le fichier `backupV25.sh` dispose de droits d'exécution. Si ce n'est pas le cas, accordez des droits en exécutant la commande suivante :
	`chmod 755 backupV25.sh`
	c. Exécutez l'utilitaire de sauvegarde :
	`backupV25.sh`

Que faire ensuite

- Examinez le répertoire dans lequel les fichiers de sauvegarde sont stockés pour vérifier que le fichier de sauvegarde que vous venez de créer y figure. Les

fichiers de sauvegarde sont créés à l'emplacement que vous avez défini pour le paramètre BACKUP_DIR dans le fichier backup.properties.

- Vérifiez si le fichier backup.log contient des erreurs ou des exceptions. Ce fichier est créé dans le même répertoire que celui dans lequel vous avez exécuté l'utilitaire de sauvegarde. Pour que l'opération de sauvegarde aboutisse, assurez-vous que le fichier journal ne contient aucune erreur ni exception.
- Retenez le mot de passe de sauvegarde car vous en aurez besoin si vous devez restaurer des données à partir de cette sauvegarde.
- N'éditez pas les fichiers figurant dans l'archive de sauvegarde. Sinon, ils deviennent illisibles.

Restauration des fichiers de sauvegarde d'IBM Security Key Lifecycle Manager, version 2.5

Vous pouvez restaurer les fichiers de sauvegarde multiplateformes d'IBM Security Key Lifecycle Manager version 2.5 sur un système sur lequel est installé IBM Security Key Lifecycle Manager version 3.0.1 à l'aide de l'interface graphique, de l'interface de ligne de commande, de l'interface REST ou du script de restauration de migration.

Avant de commencer

Installez IBM Security Key Lifecycle Manager version 3.0.1 sur un système. Vous devez disposer du fichier de sauvegarde de la version précédente et vous rappeler du mot de passe que vous avez utilisé lors de la création du fichier de sauvegarde.

Remarque : Vous devez disposer du rôle utilisateur IBM Security Key Lifecycle Manager pour exécuter les opérations de sauvegarde et de restauration.

Pourquoi et quand exécuter cette tâche

Vous pouvez restaurer les fichiers de sauvegarde multiplateformes compatibles avec IBM Security Key Lifecycle Manager version 2.5 sur un système sur lequel est installé IBM Security Key Lifecycle Manager version 3.0.1, quel que soit le système d'exploitation.

Avant de lancer une tâche de restauration, isolez le système en vue de sa maintenance. Faites une copie de sauvegarde du système existant. Vous pourrez l'utiliser ultérieurement pour rétablir l'état d'origine du système en cas de problème pendant le processus de restauration. Le serveur IBM Security Key Lifecycle Manager redémarre automatiquement après le processus de restauration. Vérifiez l'environnement avant de remettre en service le serveur IBM Security Key Lifecycle Manager.

Remarque : Pour plus de sécurité, modifiez le mot de passe utilisateur d'IBM Security Key Lifecycle Manager peu de temps après le processus de migration des données.

Procédure

1. Connectez-vous au système sur lequel IBM Security Key Lifecycle Manager version 3.0.1 est installé.
2. Copiez le fichier de sauvegarde du système version 2.5 dans un dossier de votre choix sous *<SKLM_DATA>*, par exemple `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data\sklm_v2.5.0.3_20170429013250-0400_migration_backup.jar`. Pour la définition de *<SKLM_DATA>*, voir Définitions relatives à un répertoire *HOME* et d'autres variables de répertoire.

3. Restaurez le fichier de sauvegarde en suivant l'une des méthodes ci-après.

Interface graphique	1. Connectez-vous à l'interface graphique en tant qu'utilisateur autorisé, par exemple SKLMAdmin. 2. Sur la page Bienvenue, cliquez sur **Administration** > **Sauvegarde et restauration**. 3. Cliquez sur **Parcourir** pour spécifier l'emplacement du fichier de sauvegarde version 2.5 sous le répertoire <*SKLM_DATA*>. 4. Cliquez sur **Afficher les sauvegardes** pour afficher les fichiers de sauvegarde à restaurer. 5. Dans la table **Sauvegarde et restauration**, sélectionnez un fichier de sauvegarde. 6. Cliquez sur **Restaurer à partir d'une sauvegarde**. 7. Dans la page Restaurer une sauvegarde, spécifiez le mot de passe de sauvegarde que vous avez utilisé pour créer le fichier de sauvegarde. 8. Cliquez sur **Restaurer une sauvegarde**. 9. Redémarrez le serveur IBM Security Key Lifecycle Manager. **Remarque :** Si vous utilisez l'interface graphique, vous ne pouvez pas restaurer les rôles, les utilisateurs et les groupes à partir de la sauvegarde d'IBM Security Key Lifecycle Manager version 2.5.

Interface de ligne de commande	1. Accédez au répertoire <*WAS_HOME*>/bin. Exemple :
	Windows
	`cd unité:\Program Files\IBM\WebSphere\AppServer\bin`
	Linux `cd /opt/IBM/WebSphere/AppServer/bin`
	2. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme SKLMAdmin. Exemple :
	Windows
	`wsadmin.bat -username SKLMAdmin -password mypwd -lang jython`
	Linux
	`./wsadmin.sh -username SKLMAdmin -password mypwd -lang jython`
	3. Exécutez la commande d'interface de ligne de commande **tklmBackupRunRestore** en spécifiant les paramètres tels que le nom du fichier de sauvegarde ainsi que son chemin d'accès complet et le mot de passe de sauvegarde que vous avez utilisé pour créer la sauvegarde, conformément à l'exemple suivant :
	`print AdminTask.tklmBackupRunRestore ('[-backupFilePath <SKLM_DATA>/sklm_v2.5.0.3_20170429013250-0400_migration_ba -password myBackupPwd]')`
	4. Redémarrez le serveur IBM Security Key Lifecycle Manager.
	Remarque : Si vous utilisez l'interface de ligne de commande, vous ne pouvez pas restaurer les rôles, les utilisateurs et les groupes à partir de la sauvegarde d'IBM Security Key Lifecycle Manager version 2.5.

Interface REST	1. Ouvrez un client REST.
	2. Obtenez un identificateur d'authentification utilisateur unique pour accéder aux services REST d'IBM Security Key Lifecycle Manager. Pour plus d'informations sur le processus d'authentification, voir Processus d'authentification pour les services REST.
	3. Pour appeler le **service REST Backup Run Restore**, envoyez la demande HTTP POST avec le nom du fichier de sauvegarde ainsi que son chemin d'accès complet et le mot de passe de sauvegarde sous forme de paramètres. Transmettez l'identificateur d'authentification utilisateur que vous avez obtenu à l'étape b avec le message de demande, conformément à l'exemple suivant :
	`POST https://localhost:<port>/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_b`
	`"password":"myBackupPwd"}`
	4. Redémarrez le serveur IBM Security Key Lifecycle Manager.
	Remarque : Si vous utilisez l'interface REST, vous ne pouvez pas restaurer les rôles, les utilisateurs et les groupes à partir de la sauvegarde d'IBM Security Key Lifecycle Manager version 2.5.

Script de restauration de migration	1. Localisez les utilitaires de restauration d'IBM Security Key Lifecycle Manager. **Windows** <*SKLM_INSTALL_HOME*>\migration\utilities\sklmv25 L'emplacement par défaut est C:\Program Files\IBM\SKLMV301\migration\utilities\sklmv25. **Linux** <*SKLM_INSTALL_HOME*>/migration/utilities/sklmv25 L'emplacement par défaut est /opt/IBM/SKLMV301/migration/utilities/sklmv25. 2. Editez le fichier restore.properties dans le dossier sklmv25 afin de configurer les propriétés, conformément à l'exemple ci-dessous. **Remarque :** Sous Windows, le fichier restore.properties que vous utilisez pour les opérations de restauration ne doit pas contenir d'espace avant ni après les valeurs et clés de propriété. **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_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_v2.5.0.3_20170429013250-0400_migration_b WAS_USER_PWD=wasadmin_password RESTORE_USER_ROLES=y #pkcs11_config=/luna.cfg **Remarque :** • Pour vous connecter à IBM Security Key Lifecycle Manager en utilisant les données d'identification utilisateur définies lors de l'installation du produit, attribuez la valeur «n» à la propriété **RESTORE_USER_ROLES**. Le fait d'attribuer la valeur «n» à cette propriété permet de garantir que l'ID utilisateur et le mot de passe ne sont pas remplacés par les données d'identification de l'ancienne version. • Si IBM Security Key Lifecycle Manager est configuré avec HSM, ne commentez pas la propriété **#pkcs11_config** et indiquez le chemin correct du fichier luna.cfg comme valeur. • Sous Windows, lorsque vous spécifiez un chemin dans le fichier de propriétés, utilisez «/ » ou «\\ » comme séparateur de chemin, conformément à l'exemple suivant : C:\\sklmv25_restore Ou C:/sklmv25_restore 3. Ouvrez une invite de commande et exécutez l'utilitaire de restauration. **Windows** Accédez au répertoire <*SKLM_INSTALL_HOME*>\migration\utilities\sklmv25 et exécutez la commande suivante : **restoreV25.bat** **Linux** a. Accédez au répertoire <*SKLM_INSTALL_HOME*>/migration/utilities/sklmv25. b. Vérifiez que le fichier restoreV25.sh dispose de droits

Remarque : Si vous souhaitez configurer un cluster multimaître sur le serveur IBM Security Key Lifecycle Manager restauré, dans le fichier `SKLMConfig.properties`, mettez à jour la propriété **`enableClientCertPush`** comme suit :

```
enableClientCertPush=true
```

Vous pouvez utiliser la commande de l'interface CLI Service REST Update Config Property ou tklmConfigUpdateEntry pour mettre à jour la propriété.

Redémarrez ensuite le serveur IBM Security Key Lifecycle Manager.

Que faire ensuite

Remarque : Après la restauration des données, assurez-vous que le chemin des propriétés dans les fichiers `SKLMConfig.properties`, `datastore.properties` et `ReplicationSKLMConfig.properties` est correct avant de procéder à votre prochaine tâche.

Les remplacements configurés pour les groupes de clés LTO et les certificats 3592 ne sont pas automatiquement restaurés à partir des versions antérieures d'IBM Security Key Lifecycle Manager. Vous devez configurer manuellement le remplacement des certificats et des groupes de clés.

Pour plus d'informations, voir Restauration des certificats et groupes de clés de remplacement

Sauvegarde des données d'IBM Security Key Lifecycle Manager, version 2.6

Utilisez l'utilitaire de sauvegarde IBM Security Key Lifecycle Manager version 3.0.1 pour créer des fichiers de sauvegarde multiplateformes IBM Security Key Lifecycle Manager version 2.6.

Avant de commencer

Vous devez installer IBM Security Key Lifecycle Manager version 3.0.1 sur un système. Assurez-vous que le système sur lequel sont installés IBM Security Key Lifecycle Manager version 2.6 et le groupe de correctifs 2 est disponible.

Pourquoi et quand exécuter cette tâche

Vous pouvez vous servir de l'utilitaire de sauvegarde pour créer des fichiers de sauvegarde multiplateformes indépendamment des systèmes d'exploitation et de l'arborescence du serveur. Vous pouvez restaurer ces fichiers de sauvegarde multiplateformes compatibles sur un système sur lequel est installé IBM Security Key Lifecycle Manager version 3.0.1, quel que soit le système d'exploitation.

Remarque : Pour plus de sécurité, modifiez le mot de passe utilisateur d'IBM Security Key Lifecycle Manager peu de temps après le processus de migration des données.

Procédure

Procédez comme suit sur les systèmes sur lesquels les versions 3.0.1 et 2.6 d'IBM Security Key Lifecycle Manager sont installées.

IBM Security Key Lifecycle Manager version3.0.1	1. Connectez-vous au système avec vos données d'identification utilisateur. 2. Localisez le dossier des utilitaires de sauvegarde. **Windows** <*SKLM_INSTALL_HOME*>\migration\utilities\sklmv26 L'emplacement par défaut est C:\Program Files\IBM\SKLMV301\migration\utilities\sklmv26. **Linux** <*SKLM_INSTALL_HOME*>/migration/utilities/sklmv26 L'emplacement par défaut est /opt/IBM/SKLMV301/migration/utilities/sklmv26.

IBM Security Key Lifecycle Manager version 2.6	1. Connectez-vous au système avec vos données d'identification utilisateur.
	2. Copiez le dossier `sklmv26` du système sur lequel IBM Security Key Lifecycle Manager version 3.0.1 est installé dans un répertoire local de votre choix.
	3. Editez `backup.properties` dans le dossier `sklmv26` afin de configurer les propriétés, conformément à l'exemple suivant : Vous devez définir des valeurs pour toutes les propriétés, sauf pour la propriété `BACKUP_DIR` (facultative).
	Si vous n'indiquez pas de valeur pour `BACKUP_DIR`, le fichier de sauvegarde est créé dans le sous-dossier `backup` à partir duquel vous exécutez l'utilitaire de sauvegarde.
	Remarque : Sous Windows, le fichier `backup.properties` que vous utilisez pour les opérations de sauvegarde ne doit pas contenir d'espace avant ni après les valeurs et clés de propriété.
	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`
	Remarque : Sous Windows, lorsque vous spécifiez un chemin dans le fichier de propriétés, utilisez «/ » ou «\\ » comme séparateur de chemin, conformément à l'exemple suivant :
	`C:\\sklmv26_backup`
	ou
	`C:/sklmv26_backup`
	4. Ouvrez une invite de commande et exécutez l'utilitaire de sauvegarde.
	Windows
	Accédez au répertoire `sklmv26` (voir étape b) et exécutez la commande suivante :
	`backupV26.bat`
	Linux
	a. Accédez au répertoire `sklmv26` (voir l'étape b).
	b. Vérifiez que le fichier `backupV26.sh` dispose de droits d'exécution. Si ce n'est pas le cas, accordez des droits en exécutant la commande suivante :
	`chmod 755 backupV26.sh`
	c. Exécutez l'utilitaire de sauvegarde :
	`backupV26.sh`

Que faire ensuite

- Examinez le répertoire dans lequel les fichiers de sauvegarde sont stockés pour vérifier que le fichier de sauvegarde que vous venez de créer y figure. Les

fichiers de sauvegarde sont créés à l'emplacement que vous avez défini pour le paramètre `BACKUP_DIR` dans le fichier `backup.properties`.

- Vérifiez si le fichier `backup.log` contient des erreurs ou des exceptions. Ce fichier est créé dans le même répertoire que celui dans lequel vous avez exécuté l'utilitaire de sauvegarde. Pour que l'opération de sauvegarde aboutisse, assurez-vous que le fichier journal ne contient aucune erreur ni exception.
- Retenez le mot de passe de sauvegarde car vous en aurez besoin si vous devez restaurer des données à partir de cette sauvegarde.
- N'éditez pas les fichiers figurant dans l'archive de sauvegarde. Sinon, ils deviennent illisibles.

Restauration des fichiers de sauvegarde d'IBM Security Key Lifecycle Manager, version 2.6

Vous pouvez restaurer les fichiers de sauvegarde multiplateformes d'IBM Security Key Lifecycle Manager version 2.6 sur un système sur lequel est installé IBM Security Key Lifecycle Manager version 3.0.1 à l'aide de l'interface graphique, de l'interface de ligne de commande, de l'interface REST ou du script de restauration de migration.

Avant de commencer

Installez IBM Security Key Lifecycle Manager version 3.0.1 sur un système. Vous devez disposer du fichier de sauvegarde de la version précédente et vous rappeler du mot de passe que vous avez utilisé lors de la création du fichier de sauvegarde.

Remarque : Vous devez disposer du rôle utilisateur IBM Security Key Lifecycle Manager pour exécuter les opérations de sauvegarde et de restauration.

Pourquoi et quand exécuter cette tâche

Vous pouvez restaurer les fichiers de sauvegarde multiplateformes compatibles avec IBM Security Key Lifecycle Manager version 2.6 sur un système sur lequel est installé IBM Security Key Lifecycle Manager version 3.0.1 quel que soit le système d'exploitation.

Avant de lancer une tâche de restauration, isolez le système en vue de sa maintenance. Faites une copie de sauvegarde du système existant. Vous pourrez l'utiliser ultérieurement pour rétablir l'état d'origine du système en cas de problème pendant le processus de restauration. Le serveur IBM Security Key Lifecycle Manager redémarre automatiquement après le processus de restauration. Vérifiez l'environnement avant de remettre en service le serveur IBM Security Key Lifecycle Manager.

Remarque : Pour plus de sécurité, modifiez le mot de passe utilisateur d'IBM Security Key Lifecycle Manager peu de temps après le processus de migration des données.

Procédure

1. Connectez-vous au système sur lequel IBM Security Key Lifecycle Manager Version 3.0.1 est installé.
2. Copiez le fichier de sauvegarde du système version 2.6 dans un dossier de votre choix sous le répertoire <*SKLM_DATA*>, par exemple `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data\`

sklm_v2.6.0.2_20170429013250-0400_migration_backup.jar. Pour la définition de <*SKLM_DATA*>, voir Définitions relatives à un répertoire *HOME* et d'autres variables de répertoire.

3. Restaurez le fichier de sauvegarde en suivant l'une des méthodes ci-après.

Interface graphique	1. Connectez-vous à l'interface graphique en tant qu'utilisateur autorisé, par exemple SKLMAdmin. 2. Sur la page Bienvenue, cliquez sur **Administration** > **Sauvegarde et restauration**. 3. Cliquez sur **Parcourir** pour spécifier l'emplacement du fichier de sauvegarde version 2.6 sous le répertoire <*SKLM_DATA*>. 4. Cliquez sur **Afficher les sauvegardes** pour afficher les fichiers de sauvegarde à restaurer. 5. Dans la table **Sauvegarde et restauration**, sélectionnez un fichier de sauvegarde. 6. Cliquez sur **Restaurer à partir d'une sauvegarde**. 7. Dans la page Restaurer une sauvegarde, spécifiez le mot de passe de sauvegarde que vous avez utilisé pour créer le fichier de sauvegarde. 8. Cliquez sur **Restaurer une sauvegarde**. 9. Redémarrez le serveur IBM Security Key Lifecycle Manager. **Remarque :** Si vous utilisez l'interface graphique, vous ne pouvez pas restaurer les rôles, les utilisateurs et les groupes à partir de la sauvegarde d'IBM Security Key Lifecycle Manager version 2.6.

Interface de ligne de commande	1. Accédez au répertoire *WAS_HOME*/bin. Par exemple,
	Windows
	`cd unité:\Program Files\IBM\WebSphere\AppServer\bin`
	Linux `cd /opt/IBM/WebSphere/AppServer/bin`
	2. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme SKLMAdmin. Par exemple,
	Windows
	`wsadmin.bat -username SKLMAdmin -password mypwd -lang jython`
	Linux
	`./wsadmin.sh -username SKLMAdmin -password mypwd -lang jython`
	3. Exécutez la commande d'interface de ligne de commande **tklmBackupRunRestore** en spécifiant les paramètres tels que le nom du fichier de sauvegarde ainsi que son chemin d'accès complet et le mot de passe de sauvegarde que vous avez utilisé pour créer la sauvegarde, conformément à l'exemple suivant :
	`print AdminTask.tklmBackupRunRestore ('[-backupFilePath <SKLM_DATA>/sklm_v2.6.0.2_20170429013250-0400_migration -password myBackupPwd]')`
	4. Redémarrez le serveur IBM Security Key Lifecycle Manager.
	Remarque : Si vous utilisez l'interface de ligne de commande, vous ne pouvez pas restaurer les rôles, les utilisateurs et les groupes à partir de la sauvegarde d'IBM Security Key Lifecycle Manager version 2.6.

Interface REST	1. Ouvrez un client REST.
	2. Obtenez un identificateur d'authentification utilisateur unique pour accéder aux services REST d'IBM Security Key Lifecycle Manager. Pour plus d'informations sur le processus d'authentification, voir Processus d'authentification pour les services REST.
	3. Pour appeler le **service REST Backup Run Restore**, envoyez la demande HTTP POST avec le nom du fichier de sauvegarde ainsi que son chemin d'accès complet et le mot de passe de sauvegarde sous forme de paramètres. Transmettez l'identificateur d'authentification utilisateur que vous avez obtenu à l'étape b avec le message de demande, conformément à l'exemple suivant :
	`POST https://localhost:<port>/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_bac`
	`"password":"myBackupPwd"}`
	4. Redémarrez le serveur IBM Security Key Lifecycle Manager.
	Remarque : Si vous utilisez l'interface REST, vous ne pouvez pas restaurer les rôles, les utilisateurs et les groupes à partir de la sauvegarde d'IBM Security Key Lifecycle Manager version 2.6.

Script de restauration de migration	1. Localisez les utilitaires de restauration d'IBM Security Key Lifecycle Manager. **Windows** <*SKLM_INSTALL_HOME*>\migration\utilities\sklmv26 L'emplacement par défaut est C:\Program Files\IBM\SKLMV301\migration\utilities\sklmv26. **Linux** <*SKLM_INSTALL_HOME*>/migration/utilities/sklmv26 L'emplacement par défaut est /opt/IBM/SKLMV301/migration/utilities/sklmv26. 2. Editez le fichier restore.properties dans le dossier sklmv26 afin de configurer les propriétés, conformément à l'exemple ci-dessous. **Remarque :** Sous Windows, le fichier restore.properties que vous utilisez pour les opérations de restauration ne doit pas contenir d'espace avant ni après les valeurs et clés de propriété. **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_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_v2.6.0.2_20170429013250-0400_migration WAS_USER_PWD=wasadmin_password RESTORE_USER_ROLES=y #pkcs11_config=/luna.cfg **Remarque :** • Pour vous connecter à IBM Security Key Lifecycle Manager en utilisant les données d'identification utilisateur définies lors de l'installation du produit, attribuez la valeur «n» à la propriété **RESTORE_USER_ROLES**. Le fait d'attribuer la valeur «n» à cette propriété permet de garantir que l'ID utilisateur et le mot de passe ne sont pas remplacés par les données d'identification de l'ancienne version. RESTORE_USER_ROLES=n • Si IBM Security Key Lifecycle Manager est configuré avec HSM, ne commentez pas la propriété **#pkcs11_config** et indiquez le chemin correct du fichier luna.cfg comme valeur. • Sous Windows, lorsque vous spécifiez un chemin dans le fichier de propriétés, utilisez «/ » ou «\\ » comme séparateur de chemin, conformément à l'exemple suivant : C:\\sklmv26_restore Ou C:/sklmv26_restore 3. Ouvrez une invite de commande et exécutez l'utilitaire de restauration. **Windows** Accédez au répertoire <*SKLM_INSTALL_HOME*>\migration\utilities\sklmv26 et exécutez la commande suivante : **restoreV26.bat** **Linux** a. Accédez au répertoire <*SKLM_INSTALL_HOME*>/migration/utilities/sklmv26.

Que faire ensuite

Remarque : Après la restauration des données, assurez-vous que le chemin des propriétés dans les fichiers `SKLMConfig.properties`, `datastore.properties` et `ReplicationSKLMConfig.properties` est correct avant de procéder à votre prochaine tâche.

Les remplacements configurés pour les groupes de clés LTO et les certificats 3592 ne sont pas automatiquement restaurés à partir des versions antérieures d'IBM Security Key Lifecycle Manager. Vous devez configurer manuellement le remplacement des certificats et des groupes de clés.

Pour plus d'informations, voir «Restauration des certificats et groupes de clés de remplacement», à la page 178.

Sauvegarde des données d'IBM Security Key Lifecycle Manager, version 2.7

Utilisez l'utilitaire de sauvegarde d'IBM Security Key Lifecycle Manager version 3.0.1 pour créer des fichiers de sauvegarde multiplateformes IBM Security Key Lifecycle Manager version 2.7.

Avant de commencer

Vous devez installer IBM Security Key Lifecycle Manager version 3.0.1 sur un système. Vérifiez que le système sur lequel est installé IBM Security Key Lifecycle Manager, Version 2.7 General Availability (GA) est disponible.

Pourquoi et quand exécuter cette tâche

Vous pouvez vous servir de l'utilitaire de sauvegarde pour créer des fichiers de sauvegarde multiplateformes indépendamment des systèmes d'exploitation et de l'arborescence du serveur. Vous pouvez restaurer ces fichiers de sauvegarde multiplateformes compatibles sur un système sur lequel est installé IBM Security Key Lifecycle Manager version 3.0.1, quel que soit le système d'exploitation.

Remarque : Pour plus de sécurité, modifiez le mot de passe utilisateur d'IBM Security Key Lifecycle Manager peu de temps après le processus de migration des données.

Procédure

Procédez comme suit sur les systèmes sur lesquels les versions 3.0.1 et 2.7 d'IBM Security Key Lifecycle Manager sont installées.

IBM Security Key Lifecycle Manager version3.0.1	1. Connectez-vous au système avec vos données d'identification utilisateur. 2. Localisez le dossier des utilitaires de sauvegarde. **Windows** `<SKLM_INSTALL_HOME>\migration\utilities\sklmv27` L'emplacement par défaut est `C:\Program Files\IBM\SKLMV301\migration\utilities\sklmv27`. **Linux** `<SKLM_INSTALL_HOME>/migration/utilities/sklmv27` L'emplacement par défaut est `/opt/IBM/SKLMV301/migration/utilities/sklmv27`.

IBM Security Key Lifecycle Manager version 2.7	1. Connectez-vous au système avec vos données d'identification utilisateur.
	2. Copiez le dossier `sklmv27` du système sur lequel IBM Security Key Lifecycle Manager version 3.0.1 est installé dans un répertoire local de votre choix.
	3. Modifiez le fichier `backup.properties` se trouvant dans le dossier `sklmv27` afin de configurer les propriétés, comme cela est présenté dans l'exemple suivant : Vous devez définir des valeurs pour toutes les propriétés, sauf pour la propriété `BACKUP_DIR` (facultative).
	Si vous n'indiquez pas de valeur pour `BACKUP_DIR`, le fichier de sauvegarde est créé dans le sous-dossier `backup` à partir duquel vous exécutez l'utilitaire de sauvegarde.
	Remarque : Sous Windows, le fichier `backup.properties` que vous utilisez pour les opérations de sauvegarde ne doit pas contenir d'espace avant ni après les valeurs et clés de propriété.
	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 (facultatif)`
	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 (facultatif)`
	Indiquez `MIGRATE_INSTANCE_ID=YES` pour migrer l'ID d'instance IBM Security Key Lifecycle Manager. Si vous ne spécifiez pas cette propriété, l'ID d'instance n'est pas migré vers IBM Security Key Lifecycle Manager version 3.0.1.
	Remarque : Sous Windows, lorsque vous spécifiez un chemin dans le fichier de propriétés, utilisez «/ » ou «\\ » comme séparateur de chemin, conformément à l'exemple suivant :
	`C:\\sklmv27_backup`
	ou
	`C:/sklmv27_backup`
	4. Ouvrez une invite de commande et exécutez l'utilitaire de sauvegarde.
	Windows
	Accédez au répertoire `sklmv27` (voir étape b) et exécutez la commande suivante :
	`backupV27.bat`
	Linux
	a. Accédez au répertoire `sklmv27` (voir l'étape b).
	b. Vérifiez que le fichier `backupV27.sh` dispose de droits d'exécution. Si ce n'est pas le cas, accordez des droits en exécutant la commande suivante :
	`chmod 755 backupV27.sh`
	c. Exécutez l'utilitaire de sauvegarde :
	`backupV27.sh`

Que faire ensuite

- Examinez le répertoire dans lequel les fichiers de sauvegarde sont stockés pour vérifier que le fichier de sauvegarde que vous venez de créer y figure. Les fichiers de sauvegarde sont créés à l'emplacement que vous avez défini pour le paramètre `BACKUP_DIR` dans le fichier `backup.properties`.
- Vérifiez si le fichier `backup.log` contient des erreurs ou des exceptions. Ce fichier est créé dans le même répertoire que celui dans lequel vous avez exécuté l'utilitaire de sauvegarde. Pour que l'opération de sauvegarde aboutisse, assurez-vous que le fichier journal ne contient aucune erreur ni exception.
- Retenez le mot de passe de sauvegarde car vous en aurez besoin si vous devez restaurer des données à partir de cette sauvegarde.
- N'éditez pas les fichiers figurant dans l'archive de sauvegarde. Sinon, ils deviennent illisibles.

Restauration des fichiers de sauvegarde d'IBM Security Key Lifecycle Manager, version 2.7

Vous pouvez restaurer les fichiers de sauvegarde multiplateformes d'IBM Security Key Lifecycle Manager version 2.7 sur un système sur lequel est installé IBM Security Key Lifecycle Manager version 3.0.1 à l'aide de l'interface graphique, de l'interface de ligne de commande, de l'interface REST ou du script de restauration de migration.

Avant de commencer

Installez IBM Security Key Lifecycle Manager version 3.0.1 sur un système. Vous devez disposer du fichier de sauvegarde de la version précédente et vous rappeler du mot de passe que vous avez utilisé lors de la création du fichier de sauvegarde.

Remarque : Vous devez disposer du rôle utilisateur IBM Security Key Lifecycle Manager pour exécuter les opérations de sauvegarde et de restauration.

Pourquoi et quand exécuter cette tâche

Vous pouvez restaurer les fichiers de sauvegarde multiplateformes compatibles avec IBM Security Key Lifecycle Manager version 2.7 sur un système sur lequel est installé IBM Security Key Lifecycle Manager version 3.0.1, quel que soit le système d'exploitation.

Avant de lancer une tâche de restauration, isolez le système en vue de sa maintenance. Faites une copie de sauvegarde du système existant. Vous pourrez l'utiliser ultérieurement pour rétablir l'état d'origine du système en cas de problème pendant le processus de restauration. Le serveur IBM Security Key Lifecycle Manager redémarre automatiquement après le processus de restauration. Vérifiez l'environnement avant de remettre en service le serveur IBM Security Key Lifecycle Manager.

Remarque : Pour plus de sécurité, modifiez le mot de passe utilisateur d'IBM Security Key Lifecycle Manager peu de temps après le processus de migration des données.

Procédure

1. Connectez-vous au système sur lequel IBM Security Key Lifecycle Manager Version 3.0.1 est installé.
2. Copiez le fichier de sauvegarde du système version 2.7 dans un dossier de votre choix sous *<SKLM_DATA>*, par exemple `C:\Program Files\IBM\`

WebSphere\AppServer\products\sklm\data\sklm_v2.7.0.0_20170429013250-0400_migration_backup.jar. Pour la définition de <*SKLM_DATA*>, voir Définitions relatives à un répertoire *HOME* et d'autres variables de répertoire.

3. Restaurez le fichier de sauvegarde en suivant l'une des méthodes ci-après.

Interface graphique	1. Connectez-vous à l'interface graphique en tant qu'utilisateur autorisé, par exemple SKLMAdmin. 2. Sur la page Bienvenue, cliquez sur **Administration** > **Sauvegarde et restauration**. 3. Cliquez sur **Parcourir** pour spécifier l'emplacement du fichier de sauvegarde version 2.7 sous le répertoire <*SKLM_DATA*>. 4. Cliquez sur **Afficher les sauvegardes** pour afficher les fichiers de sauvegarde à restaurer. 5. Dans la table **Sauvegarde et restauration**, sélectionnez un fichier de sauvegarde. 6. Cliquez sur **Restaurer à partir d'une sauvegarde**. 7. Dans la page Restaurer une sauvegarde, spécifiez le mot de passe de sauvegarde que vous avez utilisé pour créer le fichier de sauvegarde. 8. Cliquez sur **Restaurer une sauvegarde**. 9. Redémarrez le serveur IBM Security Key Lifecycle Manager. **Remarque :** Si vous utilisez l'interface graphique, vous ne pouvez pas restaurer les rôles, les utilisateurs et les groupes à partir de la sauvegarde d'IBM Security Key Lifecycle Manager version 2.7.

Interface de ligne de commande	1. Accédez au répertoire *WAS_HOME*/bin. Par exemple :
	Windows
	`cd unité:\Program Files\IBM\WebSphere\AppServer\bin`
	Linux `cd /opt/IBM/WebSphere/AppServer/bin`
	2. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme SKLMAdmin. Par exemple :
	Windows
	`wsadmin.bat -username SKLMAdmin -password mypwd -lang jython`
	Linux
	`./wsadmin.sh -username SKLMAdmin -password mypwd -lang jython`
	3. Exécutez la commande d'interface de ligne de commande **tklmBackupRunRestore** en spécifiant les paramètres tels que le nom du fichier de sauvegarde ainsi que son chemin d'accès complet et le mot de passe de sauvegarde que vous avez utilisé pour créer la sauvegarde, conformément à l'exemple suivant :
	`print AdminTask.tklmBackupRunRestore ('[-backupFilePath <SKLM_DATA>/sklm_v2.7.0.0_20170429013250-0400_migration_ba -password myBackupPwd]')`
	4. Redémarrez le serveur IBM Security Key Lifecycle Manager.
	Remarque : Si vous utilisez l'interface de ligne de commande, vous ne pouvez pas restaurer les rôles, les utilisateurs et les groupes à partir de la sauvegarde d'IBM Security Key Lifecycle Manager version 2.7.

Interface REST	1. Ouvrez un client REST.
	2. Obtenez un identificateur d'authentification utilisateur unique pour accéder aux services REST d'IBM Security Key Lifecycle Manager. Pour plus d'informations sur le processus d'authentification, voir Processus d'authentification pour les services REST.
	3. Pour appeler le **service REST Backup Run Restore**, envoyez la demande HTTP POST avec le nom du fichier de sauvegarde ainsi que son chemin d'accès complet et le mot de passe de sauvegarde sous forme de paramètres. Transmettez l'identificateur d'authentification utilisateur que vous avez obtenu à l'étape b avec le message de demande, conformément à l'exemple suivant :
	`POST https://localhost:<port>/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. Redémarrez le serveur IBM Security Key Lifecycle Manager.
	Remarque : Si vous utilisez l'interface REST, vous ne pouvez pas restaurer les rôles, les utilisateurs et les groupes à partir de la sauvegarde d'IBM Security Key Lifecycle Manager version 2.7.

Script de restauration de migration	1. Localisez les utilitaires de restauration d'IBM Security Key Lifecycle Manager. **Windows** <*SKLM_INSTALL_HOME*>\migration\utilities\sklmv27 L'emplacement par défaut est C:\Program Files\IBM\SKLMV301\migration\utilities\sklmv27. **Linux** <*SKLM_INSTALL_HOME*>/migration/utilities/sklmv27 L'emplacement par défaut est /opt/IBM/SKLMV301/migration/utilities/sklmv27. 2. Editez restore.properties dans le dossier sklmv27 afin de configurer les propriétés, conformément à l'exemple suivant : **Remarque :** Sous Windows, le fichier restore.properties que vous utilisez pour les opérations de restauration ne doit pas contenir d'espace avant ni après les valeurs et clés de propriété. **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 **Remarque :** • Pour vous connecter à IBM Security Key Lifecycle Manager en utilisant les données d'identification utilisateur définies lors de l'installation du produit, attribuez la valeur «n» à la propriété **RESTORE_USER_ROLES**. Le fait d'attribuer la valeur «n» à cette propriété permet de garantir que l'ID utilisateur et le mot de passe ne sont pas remplacés par les données d'identification de l'ancienne version. RESTORE_USER_ROLES=n • Si IBM Security Key Lifecycle Manager est configuré avec HSM, ne commentez pas la propriété **#pkcs11_config** et indiquez le chemin correct du fichier luna.cfg comme valeur. • Sous Windows, lorsque vous spécifiez un chemin dans le fichier de propriétés, utilisez «/ » ou «\\ » comme séparateur de chemin, conformément à l'exemple suivant : C:\\sklmv27_restore Ou C:/sklmv27_restore 3. Ouvrez une invite de commande et exécutez l'utilitaire de restauration. **Windows** Accédez au répertoire <*SKLM_INSTALL_HOME*>\migration\utilities\sklmv27 et exécutez la commande suivante : **restoreV27.bat** **Linux** a. Accédez au répertoire <*SKLM_INSTALL_HOME*>/migration/utilities/sklmv27.

Que faire ensuite

Remarque : Après la restauration des données, assurez-vous que le chemin des propriétés dans les fichiers `SKLMConfig.properties`, `datastore.properties` et `ReplicationSKLMConfig.properties` est correct avant de procéder à votre prochaine tâche.

Les remplacements configurés pour les groupes de clés LTO et les certificats 3592 ne sont pas automatiquement restaurés à partir des versions antérieures d'IBM Security Key Lifecycle Manager. Vous devez configurer manuellement le remplacement des certificats et des groupes de clés.

Pour plus d'informations, voir «Restauration des certificats et groupes de clés de remplacement», à la page 178.

Sauvegarde des données d'IBM Security Key Lifecycle Manager version 3.0

Utilisez l'utilitaire de sauvegarde d'IBM Security Key Lifecycle Manager version 3.0.1 pour créer des fichiers de sauvegarde multiplateformes IBM Security Key Lifecycle Manager version 3.0.

Avant de commencer

Vous devez installer IBM Security Key Lifecycle Manager version 3.0.1 sur un système. Vérifiez que le système sur lequel est installé IBM Security Key Lifecycle Manager version 3.0 General Availability (GA) est disponible.

Pourquoi et quand exécuter cette tâche

Vous pouvez vous servir de l'utilitaire de sauvegarde pour créer des fichiers de sauvegarde multiplateformes indépendamment des systèmes d'exploitation et de l'arborescence du serveur. Vous pouvez restaurer ces fichiers de sauvegarde multiplateformes compatibles sur un système sur lequel est installé IBM Security Key Lifecycle Manager version 3.0.1, quel que soit le système d'exploitation.

Remarque : Pour plus de sécurité, modifiez le mot de passe utilisateur d'IBM Security Key Lifecycle Manager peu de temps après le processus de migration des données.

Procédure

Procédez comme suit sur les systèmes sur lesquels les versions 3.0.1 et 3.0 d'IBM Security Key Lifecycle Manager sont installées.

IBM Security Key Lifecycle Manager version 3.0.1	1. Connectez-vous au système avec vos données d'identification utilisateur. 2. Localisez le dossier des utilitaires de sauvegarde. **Windows** <*SKLM_INSTALL_HOME*>\migration\utilities\sklmv30 L'emplacement par défaut est C:\Program Files\IBM\SKLMV301\migration\utilities\sklmv30. **Linux** <*SKLM_INSTALL_HOME*>/migration/utilities/sklmv30 L'emplacement par défaut est /opt/IBM/SKLMV301/migration/utilities/sklmv30.

IBM Security Key Lifecycle Manager version 3.0	1. Connectez-vous au système avec vos données d'identification utilisateur.
	2. Copiez le dossier `sklmv30` du système sur lequel IBM Security Key Lifecycle Manager version 3.0.1 est installé dans un répertoire local de votre choix.
	3. Editez `backup.properties` dans le dossier `sklmv30` afin de configurer les propriétés, conformément à l'exemple suivant. Vous devez définir des valeurs pour toutes les propriétés, sauf pour la propriété `BACKUP_DIR` (facultative).
	Si vous n'indiquez pas de valeur pour `BACKUP_DIR`, le fichier de sauvegarde est créé dans le sous-dossier `backup` à partir duquel vous exécutez l'utilitaire de sauvegarde.
	Remarque : Sous Windows, le fichier `backup.properties` que vous utilisez pour les opérations de sauvegarde ne doit pas contenir d'espace avant ni après les valeurs et clés de propriété.
	Windows
	`WAS_HOME=C:\\Program Files\\IBM\\WebSphere\\AppServer`
	`JAVA_HOME=C:\\Program Files\\IBM\\WebSphere\\AppServer\\java\\8.0 (o`
	`BACKUP_PASSWORD=passw0rd123`
	`DB_PASSWORD=sklmdb2`
	`WAS_USER_PWD=wasadmin`
	`MIGRATE_INSTANCE_ID=NO (facultatif)`
	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 (facultatif)`
	Indiquez `MIGRATE_INSTANCE_ID=YES` pour migrer l'ID d'instance IBM Security Key Lifecycle Manager. Si vous ne spécifiez pas cette propriété, l'ID d'instance n'est pas migré vers IBM Security Key Lifecycle Manager version 3.0.1.
	Remarque : Sous Windows, lorsque vous spécifiez un chemin dans le fichier de propriétés, utilisez «/ » ou «\\ » comme séparateur de chemin, conformément à l'exemple suivant :
	`C:\\sklmv30_backup`
	ou
	`C:/sklmv30_backup`
	4. Ouvrez une invite de commande et exécutez l'utilitaire de sauvegarde.
	Windows
	Accédez au répertoire `sklmv30` (voir l'étape b) et exécutez la commande suivante :
	`backupV30.bat`
	Linux
	a. Accédez au répertoire `sklmv30` (voir l'étape b).
	b. Vérifiez que le fichier `backupV30.sh` dispose des droits d'exécution. Si ce n'est pas le cas, accordez des droits en exécutant la commande suivante :
	`chmod 755 backupV30.sh`
	c. Exécutez l'utilitaire de sauvegarde :
	`backupV30.sh`

Que faire ensuite

- Examinez le répertoire dans lequel les fichiers de sauvegarde sont stockés pour vérifier que le fichier de sauvegarde que vous venez de créer y figure. Les fichiers de sauvegarde sont créés à l'emplacement que vous avez défini pour le paramètre `BACKUP_DIR` dans le fichier `backup.properties`.
- Vérifiez si le fichier `backup.log` contient des erreurs ou des exceptions. Ce fichier est créé dans le même répertoire que celui dans lequel vous avez exécuté l'utilitaire de sauvegarde. Pour que l'opération de sauvegarde aboutisse, assurez-vous que le fichier journal ne contient aucune erreur ni exception.
- Retenez le mot de passe de sauvegarde car vous en aurez besoin si vous devez restaurer des données à partir de cette sauvegarde.
- N'éditez pas les fichiers figurant dans l'archive de sauvegarde. Sinon, ils deviennent illisibles.

Restauration des fichiers de sauvegarde d'IBM Security Key Lifecycle Manager version 3.0

Vous pouvez restaurer les fichiers de sauvegarde multiplateformes d'IBM Security Key Lifecycle Manager version 3.0 sur un système sur lequel est installé IBM Security Key Lifecycle Manager version 3.0.1 à l'aide de l'interface graphique, de l'interface de ligne de commande, de l'interface REST ou du script de restauration de migration.

Avant de commencer

Installez IBM Security Key Lifecycle Manager version 3.0.1 sur un système. Vous devez disposer du fichier de sauvegarde de la version précédente et vous rappeler du mot de passe que vous avez utilisé lors de la création du fichier de sauvegarde.

Remarque : Vous devez disposer du rôle utilisateur IBM Security Key Lifecycle Manager pour exécuter les opérations de sauvegarde et de restauration.

Pourquoi et quand exécuter cette tâche

Vous pouvez restaurer les fichiers de sauvegarde multiplateformes compatibles avec IBM Security Key Lifecycle Manager version 3.0 sur un système sur lequel est installé IBM Security Key Lifecycle Manager version 3.0.1 quel que soit le système d'exploitation.

Avant de lancer une tâche de restauration, isolez le système en vue de sa maintenance. Faites une copie de sauvegarde du système existant. Vous pourrez l'utiliser ultérieurement pour rétablir l'état d'origine du système en cas de problème pendant le processus de restauration. Le serveur IBM Security Key Lifecycle Manager redémarre automatiquement après le processus de restauration. Vérifiez l'environnement avant de remettre en service le serveur IBM Security Key Lifecycle Manager.

Remarque : Pour plus de sécurité, modifiez le mot de passe utilisateur d'IBM Security Key Lifecycle Manager peu de temps après le processus de migration des données.

Procédure

1. Connectez-vous au système sur lequel IBM Security Key Lifecycle Manager Version 3.0.1 est installé.
2. Copiez le fichier de sauvegarde du système version 3.0 dans un dossier de votre choix sous le répertoire <*SKLM_DATA*>, par exemple `C:\Program`

`Files\IBM\WebSphere\AppServer\products\sklm\data\sklm_v3.0.0.0_20170429013250-0400_migration_backup.jar`. Pour la définition de <*SKLM_DATA*>, voir Définitions relatives à un répertoire *HOME* et d'autres variables de répertoire.

3. Restaurez le fichier de sauvegarde en suivant l'une des méthodes ci-après.

Interface graphique	1. Connectez-vous à l'interface graphique en tant qu'utilisateur autorisé, par exemple `SKLMAdmin`. 2. Sur la page Bienvenue, cliquez sur **Administration** > **Sauvegarde et restauration**. 3. Cliquez sur **Parcourir** pour spécifier l'emplacement du fichier de sauvegarde version 3.0 sous le répertoire <*SKLM_DATA*>. 4. Cliquez sur **Afficher les sauvegardes** pour afficher les fichiers de sauvegarde à restaurer. 5. Dans la table **Sauvegarde et restauration**, sélectionnez un fichier de sauvegarde. 6. Cliquez sur **Restaurer à partir d'une sauvegarde**. 7. Dans la page Restaurer une sauvegarde, spécifiez le mot de passe de sauvegarde que vous avez utilisé pour créer le fichier de sauvegarde. 8. Cliquez sur **Restaurer une sauvegarde**. 9. Redémarrez le serveur IBM Security Key Lifecycle Manager. **Remarque :** Si vous utilisez l'interface graphique, vous ne pouvez pas restaurer les rôles, les utilisateurs et les groupes à partir de la sauvegarde d'IBM Security Key Lifecycle Manager version 3.0.

Interface de ligne de commande	1. Accédez au répertoire *WAS_HOME*`/bin`. Par exemple :
	Windows
	`cd unité:\Program Files\IBM\WebSphere\AppServer\bin`
	Linux `cd /opt/IBM/WebSphere/AppServer/bin`
	2. Démarrez l'interface **`wsadmin`** en utilisant un ID utilisateur autorisé, comme `SKLMAdmin`. Par exemple :
	Windows
	`wsadmin.bat -username SKLMAdmin -password mypwd -lang jython`
	Linux
	`./wsadmin.sh -username SKLMAdmin -password mypwd -lang jython`
	3. Exécutez la commande d'interface de ligne de commande **`tklmBackupRunRestore`** en spécifiant les paramètres tels que le nom du fichier de sauvegarde ainsi que son chemin d'accès complet et le mot de passe de sauvegarde que vous avez utilisé pour créer la sauvegarde, conformément à l'exemple suivant :
	`print AdminTask.tklmBackupRunRestore ('[-backupFilePath <SKLM_DATA>/sklm_v3.0.0.0_20170429013250-0400_migration -password myBackupPwd]')`
	4. Redémarrez le serveur IBM Security Key Lifecycle Manager.
	Remarque : Si vous utilisez l'interface de ligne de commande, vous ne pouvez pas restaurer les rôles, les utilisateurs et les groupes à partir de la sauvegarde d'IBM Security Key Lifecycle Manager version 3.0.

Interface REST	1. Ouvrez un client REST.
	2. Obtenez un identificateur d'authentification utilisateur unique pour accéder aux services REST d'IBM Security Key Lifecycle Manager. Pour plus d'informations sur le processus d'authentification, voir Processus d'authentification pour les services REST.
	3. Pour appeler le **service REST Backup Run Restore**, envoyez la demande HTTP POST avec le nom du fichier de sauvegarde ainsi que son chemin d'accès complet et le mot de passe de sauvegarde sous forme de paramètres. Transmettez l'identificateur d'authentification utilisateur que vous avez obtenu à l'étape b avec le message de demande, conformément à l'exemple suivant :
	`POST https://localhost:<port>/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_bac`
	`"password":"myBackupPwd"}`
	4. Redémarrez le serveur IBM Security Key Lifecycle Manager.
	Remarque : Si vous utilisez l'interface REST, vous ne pouvez pas restaurer les rôles, les utilisateurs et les groupes à partir de la sauvegarde d'IBM Security Key Lifecycle Manager version 3.0.

Script de restauration de migration	1. Localisez les utilitaires de restauration d'IBM Security Key Lifecycle Manager. **Windows** <*SKLM_INSTALL_HOME*>\migration\utilities\sklmv30 L'emplacement par défaut est C:\Program Files\IBM\SKLMV301\migration\utilities\sklmv30. **Linux** <*SKLM_INSTALL_HOME*>/migration/utilities/sklmv30 L'emplacement par défaut est /opt/IBM/SKLMV301/migration/utilities/sklmv30. 2. Editez restore.properties dans le dossier sklmv30 afin de configurer les propriétés, conformément à l'exemple suivant. **Remarque :** Sous Windows, le fichier restore.properties que vous utilisez pour les opérations de restauration ne doit pas contenir d'espace avant ni après les valeurs et clés de propriété. **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_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_v3.0.0.0_20170429013250-0400_migration WAS_USER_PWD=wasadmin_password RESTORE_USER_ROLES=y #pkcs11_config=/luna.cfg **Remarque :** • Pour vous connecter à IBM Security Key Lifecycle Manager en utilisant les données d'identification utilisateur définies lors de l'installation du produit, attribuez la valeur «n» à la propriété **RESTORE_USER_ROLES**. Le fait d'attribuer la valeur «n» à cette propriété permet de garantir que l'ID utilisateur et le mot de passe ne sont pas remplacés par les données d'identification de l'ancienne version. RESTORE_USER_ROLES=n • Si IBM Security Key Lifecycle Manager est configuré avec HSM, ne commentez pas la propriété **#pkcs11_config** et indiquez le chemin correct du fichier luna.cfg comme valeur. • Sous Windows, lorsque vous spécifiez un chemin dans le fichier de propriétés, utilisez «/ » ou «\\ » comme séparateur de chemin, conformément à l'exemple suivant : C:\\sklmv30_restore Ou C:/sklmv30_restore 3. Ouvrez une invite de commande et exécutez l'utilitaire de restauration. **Windows** Accédez au répertoire <*SKLM_INSTALL_HOME*>\migration\utilities\sklmv30 et exécutez la commande suivante : **restoreV30.bat** **Linux** a. Accédez au répertoire <*SKLM_INSTALL_HOME*>/migration/utilities/sklmv30.

Que faire ensuite

Remarque : Après la restauration des données, assurez-vous que le chemin des propriétés dans les fichiers SKLMConfig.properties, datastore.properties et ReplicationSKLMConfig.properties est correct avant de procéder à votre prochaine tâche.

Les remplacements configurés pour les groupes de clés LTO et les certificats 3592 ne sont pas automatiquement restaurés à partir des versions antérieures d'IBM Security Key Lifecycle Manager. Vous devez configurer manuellement le remplacement des certificats et des groupes de clés.

Pour plus d'informations, voir «Restauration des certificats et groupes de clés de remplacement».

Restauration des certificats et groupes de clés de remplacement

Les remplacements configurés pour les groupes de clés LTO et les certificats 3592 ne sont pas automatiquement restaurés à partir des versions antérieures. Pour les spécifier manuellement dans la version 3.0.1, utilisez le fichier de remplacement scheduledTasks.txt, qui est créé dans le répertoire <WAS_HOME>/products/sklm/config au moment de la restauration.

Procédure

1. Ouvrez une invite de commande.
2. Accédez au répertoire ci-dessous.

   Windows
   <*SKLM_INSTALL_HOME*>\migration\bin

   Linux <*SKLM_INSTALL_HOME*>/migration/bin
3. Exécutez la commande suivante :

   Windows
   Exécutez l'utilitaire **recreatetask.bat**.

   ```
   recreatetask.bat
   <WAS_HOME> <SKLMADMIN_USER> <SKLMADMIN_PASSWD>
   <SKLM_HOME>\config\scheduledTasks.txt <fichier_journal>
   <SKLM_INSTALL_HOME>
   ```

   Linux Exécutez l'utilitaire **recreatetask.sh**.

   ```
   ./recreatetask.sh <WAS_HOME> <SKLMADMIN_USER> <SKLMADMIN_PASSWD>
   <SKLM_HOME>/config/scheduledTasks.txt <fichier_journal>
   <SKLM_INSTALL_HOME>
   ```

   Où <fichier_journal> désigne le fichier journal dans lequel sont consignées les informations, par exemple :

   ```
   C:\Program Files\IBM\WebSphere\AppServer\products\sklm\logs\rolloverlogs.txt
   ```

   <SKLMADMIN_USER> et <SKLMADMIN_PASSWD> correspondent à l'ID utilisateur et au mot de passe de l'administrateur IBM Security Key Lifecycle Manager.

   Pour obtenir une définition des répertoires <WAS_HOME>, <SKLM_HOME> et <SKLM_INSTALL_HOME>, voir Définitions relatives à un répertoire *HOME* et d'autres variables de répertoire.

Remarque : Sur les systèmes d'exploitation Windows, vous devez ajouter une double barre oblique dans le chemin d'accès et indiquer le chemin entre guillemets s'il contient des espaces, par exemple,

```
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:\\Program Files\\IBM\\SKLMV301"
```

Prévention de la perte de clés

Pour prévenir la perte de données de chiffrement vitales, veillez à toujours disposer d'un minimum de deux instances d'IBM Security Key Lifecycle Manager. Assurez-vous que l'une des instances contient une réplique exacte des données de gestion d'unités et de clés tenues à jour par l'autre instance. Vous pouvez aussi gérer plus de deux instances redondantes.

IBM Security Key Lifecycle Manager fournit un support particulier aux serveurs de stockage DS5000, qui consiste à générer automatiquement des clés lorsqu'une nouvelle unité DS5000 est enregistrée dans IBM Security Key Lifecycle Manager.

N'utilisez pas la valeur 1 (acceptation automatique) pour la famille d'unités DS5000. Sinon, des clés pourraient être générées et servies aux serveurs de stockage DS5000 avant même que vous puissiez effectuer une sauvegarde. Pour toutes les autres familles d'unités, faites une sauvegarde des nouvelles clés servies.

Supprimez les fichiers de sauvegarde du serveur et stockez-les à un emplacement sécurisé. Par exemple, copiez les fichiers de sauvegarde sur un CD/DVD et placez-le dans un endroit sûr.

Remarque : Ne copiez pas les fichiers sur un stockage chiffré dépendant de ce produit. Procéder ainsi rendrait la sauvegarde indisponible dès lors que le produit est indisponible.

IBM Security Key Lifecycle Manager fournit également les options suivantes pour limiter les conséquences d'une perte de clés:

backup.keycert.before.serving
: Définissez cette propriété dans le fichier SKLMConfig.properties pour empêcher que de nouvelles clés ne soient servies tant qu'elles n'ont pas été sauvegardées.

Script de sauvegarde automatisée
: Utilisez le script `autobackup.bat` pour automatiser la sauvegarde des fichiers. IBM Security Key Lifecycle Manager ne sert pas de clés ou de certificats qui n'ont pas été préalablement sauvegardés si la propriété **`backup.keycert.before.serving`** a la valeur `true` ou n'est pas présente dans le fichier `SKLMConfig.properties`.

Configuration du script de sauvegarde automatisée

Vous pouvez utiliser le script de sauvegarde automatisé pour sauvegarder des fichiers.

Avant de commencer

Vous devez suivre ces instructions avant de restaurer des sauvegardes de chiffrement basé sur HSM :

- Assurez-vous que la même partition HSM se trouve avec toutes ses entrées clés intactes sur le système où le fichier de sauvegarde est restauré.
- La clé principale qui a été utilisée pour le chiffrement de la clé de sauvegarde doit être intacte pour restaurer le fichier de sauvegarde. Si la clé principale est rafraîchie, toutes les anciennes sauvegardes sont inaccessibles ou inutilisables.
- Vous devez vous connecter aux mêmes instance HSM et clé principale pour les opérations de sauvegarde et de restauration, indépendamment du fait que vous utilisez le chiffrement basé sur HSM ou le chiffrement par mot de passe.

Pourquoi et quand exécuter cette tâche

IBM Security Key Lifecycle Manager ne sert pas de clés ou de certificats qui n'ont pas été préalablement sauvegardés si la propriété **backup.keycert.before.serving** a la valeur `true` ou n'est pas présente dans le fichier `SKLMConfig.properties`.

Le script de sauvegarde automatisée déclenche une sauvegarde en appelant les commandes suivantes :

- **klmBackupIsRunning** pour vérifier si une opération de sauvegarde est en cours.
- **tklmBackupIsNeeded** ou **Service REST Backup Is Needed** pour déterminer si de nouvelles clés ou de nouveaux certificats n'ont encore jamais été sauvegardés.
- **tklmBackupRun** ou **Service REST Backup Run** pour exécuter la tâche de sauvegarde proprement dite.

Avant de commencer, déterminez le mot de passe utilisé pour chiffrer les données dans le fichier de sauvegarde.

Procédure

1. Localisez le script dans le répertoire suivant :

   Windows

   unité:\Program Files\IBM\SKLMV25\bin\samples\autobackup.bat

   Linux et AIX

   chemin/IBM/SKLMV25/bin/samples/autobackup.sh

2. Au début du fichier `autobackup.bat` ou `autobackup.sh`, localisez les lignes à changer :

```
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. Changez les lignes requises dans le script :

tiphome
Obligatoire. Répertoire de base de WebSphere Application Server.

Par exemple :

```
Set tiphome=C:/Progra~2/IBM/WebSphere/AppServer
```

username
Obligatoire. ID utilisateur ayant le droit **klmBackup**. Utilisez cet ID pour vous connecter à IBM Security Key Lifecycle Manager. Il peut également s'agir d'un ID utilisateur existant, tel que SKLMAdmin.

password
Obligatoire. Mot de passe de l'ID utilisateur ayant le droit **klmBackup**.

backuppw
Obligatoire. Le mot de passe utilisé pour chiffrer les données contenues dans le fichier de sauvegarde. La valeur doit être comprise entre 6 et 32 caractères.

Remarque : Si le chiffrement basé sur HSM est utilisé pour les sauvegardes, vous ne devez pas spécifier le mot de passe.

Vous pouvez utiliser un mot de passe différent pour chaque fichier de sauvegarde. Lorsque vous restaurez un fichier, vous devez disposer du mot de passe utilisé pour chiffrer les données qu'il contient lors de la tâche de sauvegarde.

backupdes
Facultatif. Il s'agit d'informations supplémentaires relatives à l'utilisation du fichier de sauvegarde.

backupdir
Facultatif. Répertoire de stockage des fichiers JAR qui contiennent les données de sauvegarde d'IBM Security Key Lifecycle Manager. Spécifiez un chemin complet.

Si la sauvegarde réussit, la valeur que vous spécifiez est écrite comme valeur de la propriété **tklm.backup.dir** dans le fichier SKLMConfig.properties.

Remarque :

- Si vous n'indiquez pas de valeur pour ce paramètre, et si aucune sauvegarde réussie n'a encore jamais été exécutée, la valeur par défaut est le répertoire *SKLM_DATA*/backup.
- Si, bien que cela soit déconseillé, vous spécifiez un chemin relatif tel que monrepbackup, la sauvegarde est créée dans le répertoire *WAS_HOMEWAS*/profiles/KLMProfile/*monrepbackup*.
- IBM Security Key Lifecycle Manager peut créer un fichier de sauvegarde partout où le superutilisateur du système d'exploitation a le droit d'écrire. Le superutilisateur est Administrateur sur les systèmes Windows ou root sur les systèmes tels que Linux ou AIX.
- Ne créez pas le fichier de sauvegarde dans le répertoire qui contient la sauvegarde de la base de données.

backupDBdir

Paramètre obligatoire. Il s'agit d'un répertoire de la base de données de IBM Security Key Lifecycle Manager, qui contient des données de sauvegarde temporaires de IBM Security Key Lifecycle Manager. Si aucun paramètre n'est spécifié, le répertoire utilisé correspond à la valeur de la propriété **tklm.backup.db2.dir** contenue dans le fichier `datastore.properties`. Le fichier est situé dans le répertoire *WAS_HOMEWAS*`\products\sklm\config` ou dans un répertoire temporaire du système si le répertoire spécifié par la propriété **tklm.backup.db2.dir** n'existe pas.

4. Exécutez le script :
   - Immédiatement. Entrez :

     Windows

     unité`:\Program Files\IBM\SKLMV25\bin\samples\autobackup.bat`

     Linux et AIX

     chemin`/IBM/SKLMV25/bin/samples/autobackup.sh`
   - A intervalles réguliers.

     Selon le système d'exploitation, programmez l'exécution du script dans un travail cron ou à l'aide du planificateur Windows.

Configuration de la réplication

Vous pouvez utiliser IBM Security Key Lifecycle Manager pour répliquer automatiquement vos éléments de clé, vos fichiers de configuration et d'autres informations critiques d'un serveur maître principal vers un maximum de 20 serveurs clone secondaires. La réplication automatique garantit une disponibilité continue des clés et des certificats pour les unités de chiffrement.

La réplication de données permet le clonage d'environnements IBM Security Key Lifecycle Manager sur plusieurs serveurs indépendamment des systèmes d'exploitation et de l'arborescence du serveur.

La réplication automatique garantit la disponibilité d'un système de sauvegarde lorsque l'instance IBM Security Key Lifecycle Manager principale n'est pas disponible. Le système de secours contient toutes les clés requises et les données qui y sont associées. Vous pouvez utiliser l'interface graphique, les commandes CLI ou les interfaces REST pour configurer le processus de réplication de clone automatisé d'IBM Security Key Lifecycle Manager.

Configuration du serveur maître

Le serveur maître est le système principal qui est répliqué. Le processus de réplication est déclenché uniquement lorsque de nouvelles clés et des unités sont ajoutées ou modifiées sur le serveur maître. Vous pouvez répliquer le serveur maître avec 20 serveurs clones maximum. Chaque serveur clone est identifié par une adresse IP ou un nom d'hôte, et un numéro de port. Le serveur utilise des propriétés dans le fichier `ReplicationSKLMConfig.properties` pour contrôler le processus de réplication.

Vous pouvez aussi utiliser le programme de réplication d'IBM Security Key Lifecycle Manager pour planifier une opération de sauvegarde automatique. Vous ne devez configurer les propriétés que pour le serveur maître afin de sauvegarder les données à intervalles réguliers.

Configuration du serveur clone

Le processus de réplication permet le clonage d'environnements IBM Security Key Lifecycle Manager depuis le serveur maître sur plusieurs serveurs clones. Le serveur clone utilise des propriétés du fichier `ReplicationSKLMConfig.properties` pour contrôler le processus de réplication. Lorsque la procédure de réplication est déclenchée, les données ci-dessous sont répliquées sur le serveur clone :

- Les données dans les tables de base de données IBM Security Key Lifecycle Manager
- Le fichier de clés certifiées et le magasin de clés avec la clé principale
- Les fichiers de configuration d'IBM Security Key Lifecycle Manager

Méthodes de chiffrement pour sauvegarder les données pour les activités de réplication

IBM Security Key Lifecycle Manager prend en charge les méthodes de chiffrement suivantes pour les sauvegardes :

Chiffrement par mot de passe
Lorsque vous configurez le serveur maître pour la réplication automatisée, un mot de passe est spécifié pour chiffrer la clé de sauvegarde. Lorsque les données sont répliquées sur le serveur clone, le même mot de passe de chiffrement est utilisé pour déchiffrer et restaurer les fichiers de sauvegarde.

Chiffrement basé sur HSM
Vous pouvez configurer IBM Security Key Lifecycle Manager pour utiliser Hardware Security Module (HSM) afin de stocker la clé de chiffrement principale sur les serveurs maîtres et clones. Lorsque vous exécutez le programme de réplication, la clé de sauvegarde sur le serveur maître est chiffrée par la clé principale, qui est stockée dans HSM. Lorsque les données sont reproduites sur le serveur clone, la clé principale stockée dans HSM déchiffre la clé de sauvegarde. La clé de sauvegarde est utilisée pour restaurer le contenu de la sauvegarde.

Pour plus d'informations sur les méthodes de chiffrement pour la sauvegarde et la réplication, consultez Méthodes de chiffrement de sauvegarde pour activités de réplication.

Sauvegarde et la réplication d'une grande quantité de données

Vous pouvez configurer IBM Security Key Lifecycle Manager pour des activités de sauvegarde et de réplication de haute performance en définissant le paramètre suivant dans le fichier de configuration `SKLMConfig.properties` sur le serveur maître :

```
enableHighScaleBackup=true
```

Remarque : Si vous définissez le paramètre **`enableHighScaleBackup=true`** pour la sauvegarde et la réplication de grandes quantités de clés, les serveurs maîtres et clones doivent être identiques pour que la réplication des données aboutisse. Le système d'exploitation, les structures de répertoire et l'administrateur Db2 doivent être identiques sur les serveurs maîtres et clones.

Fichiers de configuration de réplication

Vous pouvez exécuter la réplication IBM Security Key Lifecycle Manager comme une tâche autonome. Un fichier de configuration de réplication valide doit être disponible pour démarrer le processus de réplication automatisée lorsque de nouvelles clés sont ajoutées.

IBM Security Key Lifecycle Manager utilise des propriétés dans le fichier de configuration *<SKLM_HOME>*\config\ReplicationSKLMConfig.properties pour contrôler le processus de réplication. Par exemple,

Windows
```
C:\Program Files\IBM\WebSphere\AppServer\products\sklm\config\
ReplicationSKLMConfig.properties
```

Linux
```
/opt/IBM/WebSphere/AppServer/products/sklm/config/
ReplicationSKLMConfig.properties
```

Vous pouvez utiliser l'interface graphique d'IBM Security Key Lifecycle Manager, l'interface de ligne de commande ou l'interface REST pour modifier les propriétés dans le fichier de configuration de réplication.

Vous pouvez classifier chaque système comme suit :

- Principal - système principal qui est répliqué.
- Clone - système secondaire qui est la cible de la copie.

Le fichier de réplication du système principal peut spécifier jusqu'à 20 clones. Chaque système clone est identifié via une adresse IP ou un nom d'hôte, et un numéro de port. Vous pouvez répliquer des environnements IBM Security Key Lifecycle Manager sur plusieurs serveurs clones indépendamment des systèmes d'exploitation et de l'arborescence du serveur.

Remarques :

- La réplication planifiée a lieu uniquement lorsque de nouvelles clés et des unités sont ajoutées ou modifiées sur le système maître.
- Il ne peut exister qu'un seul système principal avec un maximum de 20 clones. Il ne peut pas y avoir plusieurs systèmes principaux.

Vous pouvez utiliser le programme de réplication d'IBM Security Key Lifecycle Manager afin de planifier une opération de sauvegarde automatique. Vous ne devez configurer les propriétés que pour le serveur maître afin de sauvegarder les données à intervalles réguliers.

Exemple de fichier de configuration principale

```
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* désigne le rôle de réplication par défaut. Spécifiez le rôle en utilisant le paramètre **replication.role**.

- Indiquez au moins un clone avec les paramètres **backup.ClientIPn** et **backup.ClientPortn** pour répliquer les données vers le serveur clone. Pour sauvegarder automatiquement les données du serveur maître à intervalles réguliers, vous n'avez pas à spécifier l'adresse IP et du port du clone.
- Assurez-vous que les ports spécifiés sont disponibles et ne sont pas actuellement utilisés par IBM Security Key Lifecycle Manager ou par tout autre processus.
- Vous pouvez spécifier un maximum de 20 systèmes clones.
- Le paramètre **backup.TLSCertAlias** doit indiquer un certificat qui existe sur le système principal et tous les clones.
- Indiquez un mot de passe pour chiffrer et déchiffrer les sauvegardes. Ce mot de passe devient impénétrable dans le fichier de configuration de la réplication une fois qu'IBM Security Key Lifecycle Manager l'a lu pour la première fois.

Exemple de fichier de configuration de clone

```
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
```

- Sur le système clone, spécifiez la valeur de paramètre `replication.role=clone`.
- Le paramètre **restore.ListenPort** doit spécifier le numéro de port spécifié dans le paramètre **backup.ClientIPn** sur le système principal.

Pour plus de détails sur tous les paramètres de configuration de réplication disponibles, voir Paramètres de configuration de réplication.

Communication interserveur

Le protocole TLS (Transport Layer Security) permet de sécuriser les communications entre le système maître et ses clones.

Une clé privée existante doit être disponible dans le magasin de clés IBM Security Key Lifecycle Manager du système principal et de tous les systèmes clones associés. Vous devez définir l'alias de cette clé sur le système maître dans le paramètre **backup.TLSCertAlias** du fichier de configuration `ReplicationSKLMConfig.properties`. Si la même clé n'est pas disponible à la fois sur le système principal et sur les clones, vous ne pouvez pas lancer la communication entre les systèmes pour effectuer la tâche de réplication. Vous pouvez utiliser l'interface graphique, l'interface de ligne de commande ou l'interface REST pour changer les propriétés du fichier de configuration.

Planifications de réplication

Configurez les propriétés du fichier `ReplicationSKLMConfig.properties` pour planifier le processus de réplication automatisé.

Utilisez l'interface graphique, l'interface de ligne de commande ou l'interface REST afin de configurer les propriétés du fichier de configuration de réplication pour la planification du processus de réplication. La réplication planifiée a lieu uniquement lorsque de nouvelles clés et des unités sont ajoutées ou modifiées sur le serveur maître. Vous pouvez aussi utiliser le programme de réplication d'IBM Security Key Lifecycle Manager pour planifier une opération de sauvegarde automatique. Vous ne devez configurer les propriétés que pour le serveur maître afin de sauvegarder les données à intervalles réguliers.

Vous pouvez configurer la planification de telle sorte qu'IBM Security Key Lifecycle Manager vérifie régulièrement si la réplication est requise et démarre le processus lorsque des modifications ont été effectuées. Vous pouvez également spécifier une heure de la journée pour exécuter une réplication, si nécessaire. Configurez le paramètre **backup.CheckFrequency** pour définir la fréquence à laquelle IBM Security Key Lifecycle Manager vérifie si des mises à jour ont été effectuées sur le système maître. La réplication se déclenche lorsque des mises à jour se produisent. La valeur est définie en minutes et il s'agit de 1440 par défaut.

Pour définir une heure du jour, configurez le paramètre **backup.DailyStartReplicationBackupTime**. L'heure doit être indiquée au format 24 heures (HH:MM). La réplication a lieu uniquement lorsque le système principal est modifié depuis la dernière réplication.

Par défaut, le système clone restaure une sauvegarde dès qu'elle est reçue du système principal. Pour indiquer l'heure de la restauration, ajoutez le paramètre **restore.DailyStartReplicationRestoreTime** dans le fichier de configuration de la réplication sur le système clone. L'heure doit être indiquée au format 24 heures (HH:MM).

Vous pouvez utiliser la commande CLI **tklmReplicationNow** ou le **service REST Replication Now** pour forcer une réplication ad hoc sur tous les clones définis, ou une réplication spécifique.

Enregistrements d'audit de réplication

La réplication d'IBM Security Key Lifecycle Manager enregistre des informations d'audit dans le fichier journal d'audit d'IBM Security Key Lifecycle Manager.

Le programme de réplication d'IBM Security Key Lifecycle Manager inclut une fonction permettant de placer les enregistrements d'audit spécifiques à la réplication dans un fichier de journal d'audit séparé. Le journal d'audit de réplication enregistre toutes les actions liées au processus de réplication. Par défaut, ce fichier se trouve dans `<SKLM_HOME>\logs\replication\replication_audit.log`.

Utilisez l'interface graphique, l'interface de ligne de commande ou l'interface REST pour définir les propriétés d'audit dans le fichier `ReplicationSKLMConfig.properties`. Dans le fichier de configuration, vous pouvez configurer les propriétés d'audit, telles l'emplacement du fichier journal d'audit, le nom du fichier journal, la taille du fichier journal, le nombre maximal de fichiers journaux à conserver ou le nombre maximal de fichiers de sauvegarde à conserver.

Configuration d'un serveur maître avec chiffrement par mot de passe pour les sauvegardes

Vous pouvez changer les paramètres par défaut d'un serveur maître pour la communication avec le serveur clone afin de répliquer des données d'IBM Security Key Lifecycle Manager en utilisant le chiffrement par mot de passe pour les sauvegardes.

Pourquoi et quand exécuter cette tâche

Remarque : Les données sont répliquées sur les serveurs clones selon un calendrier planifié uniquement lorsque de nouveaux objets cryptographiques sont ajoutés au serveur maître.

Utilisez l'interface graphique, l'interface de ligne de commande ou l'interface REST pour modifier les paramètres dans le fichier de configuration `ReplicationSKLMConfig.properties` en fonction de vos besoins.

Pour plus d'informations sur les méthodes de chiffrement pour les sauvegardes et la réplication, consultez Méthodes de chiffrement de sauvegarde pour activités de réplication.

Si vous voulez configurer IBM Security Key Lifecycle Manager pour les activités de sauvegarde et de réplication de haute performance, vous devez définir le paramètre suivant dans le fichier de configuration *<SKLM_HOME>*`/config/SKLMConfig.properties` du serveur maître, par exemple `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\config\SKLMConfig.properties` :

```
enableHighScaleBackup=true
```

Remarque : Si vous définissez le paramètre **`enableHighScaleBackup=true`** pour la sauvegarde et la réplication de grandes quantités de clés, les systèmes maître et clone doivent être identiques pour que la réplication des données aboutisse. Le système d'exploitation, les structures de répertoire et l'administrateur Db2 doivent être identiques sur les serveurs maîtres et clones.

Procédure

1. Accédez à la page ou au répertoire approprié(e) :

   Interface graphique

   a. Connectez-vous à l'interface graphique.

   b. Cliquez sur **IBM Security Key Lifecycle Manager** > **Administration** > **Réplication**.

   Interface de ligne de commande

   a. Accédez au répertoire `WAS_HOME/bin`. Par exemple,

      Windows

      ```
      cd unité:\Program Files (x86)\IBM\WebSphere\AppServer\
      bin
      ```

      Linux

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

   b. Démarrez l'interface **`wsadmin`** en utilisant un ID utilisateur autorisé, comme `SKLMAdmin`. Par exemple,

      Windows

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

      Linux

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

   Interface REST

   Ouvrez un client REST.

2. Modifiez la valeur d'un ou de plusieurs paramètres du serveur maître :

   Interface graphique

   a. Sélectionnez **Maître**.

   b. Sélectionnez une option de gestion de serveur de réplication.

      Démarrage du serveur de réplication

      Cliquez sur **Démarrer le serveur de réplication** afin de démarrer le serveur de réplication pour la réplication des

données et des fichiers actifs IBM Security Key Lifecycle Manager sur les serveurs clones en fonction d'un calendrier configuré.

Arrêt du serveur de réplication
Cliquez sur **Arrêter le serveur de réplication** pour arrêter le serveur de réplication, de telle sorte que les données et les fichiers actifs IBM Security Key Lifecycle Manager ne soient pas répliqués sur les serveurs clones.

Réplication immédiate
Cliquez sur **Répliquer maintenant** pour exécuter immédiatement la tâche de réplication IBM Security Key Lifecycle Manager et pour faire en sorte qu'une sauvegarde soit envoyée aux clones configurés.

c. Configurez les paramètres.

Propriétés de base

Certificat du magasin de clés	Sélectionnez un certificat dans la liste. Assurez-vous que le certificat SSL/TLS existe sur le maître et sur tous les systèmes clones que vous configurez pour la réplication.
Phrase de passe de chiffrement de la sauvegarde de la réplication	Mot de passe de chiffrement du fichier de sauvegarde pour s'assurer de la sécurité des données. Le serveur clone utilise le même mot de passe pour déchiffrer et restaurer le fichier. **Remarque :** Si le chiffrement basé sur HSM est utilisé pour les sauvegardes, vous ne devez pas spécifier le mot de passe.
Confirmer la phrase de passe de chiffrement de la sauvegarde de la réplication	Spécifiez de nouveau le même mot de passe pour vérifier le mot de passe que vous avez spécifié.
Port d'écoute maître	Numéro de port pour la communication lorsque des réplications non sérialisées ou retardées ont lieu. Le port d'écoute maître par défaut est 1111.
Adresse IP ou nom d'hôte du clone -1	Adresse IP ou nom d'hôte des serveurs clones. Vous ne pouvez répliquer qu'un seul serveur maître avec 20 serveurs clones maximum. Cliquez sur le lien **Ajouter des clones** pour configurer les paramètres de réplication pour plusieurs clones.
Port du clone -1	Numéro de port pour l'envoi des fichiers de sauvegarde sur les serveurs clones. Chaque serveur clone est identifié par un numéro de port. Le numéro de port par défaut pour le serveur clone est 2222.

Propriétés avancées

Répertoire de destination de la sauvegarde de la réplication	Emplacement de stockage des fichiers de sauvegarde. La zone **Répertoire de destination de la sauvegarde de la réplication** affiche le chemin de répertoire *<SKLM_DATA>* par défaut dans lequel le fichier de sauvegarde est stocké, par exemple `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data`. Pour la définition de *<SKLM_DATA>*, voir Définitions relatives à un répertoire *HOME* et d'autres variables de répertoire. Cliquez sur **Parcourir** pour spécifier l'emplacement du référentiel de sauvegarde sous le répertoire *<SKLM_DATA>*. Le chemin de répertoire dans la zone **Répertoire de destination de sauvegarde de la réplication** change en fonction de la valeur définie pour la propriété **`browse.root.dir`** dans le fichier `SKLMConfig.properties`.
Nombre maximal de fichiers de réplication à conserver avant le remplacement	Nombre maximal de fichiers de réplication que vous souhaitez conserver. La valeur doit être un entier positif compris entre 2 et 10. Lorsque le nombre de fichiers dépasse la limite spécifiée, le fichier le plus ancien est supprimé.
Fréquence de réplication (en heures)	Fréquence à laquelle vérifier si l'opération de sauvegarde est nécessaire. La valeur par défaut est définie sur 24 heures. Ce paramètre est ignoré si la valeur de **Heure de début de réplication quotidienne** est définie.
Heure de réplication quotidienne (au format HH:MM)	Heure au format `HH:MM` à laquelle la tâche de réplication est exécuté tous les jours.
Nom du fichier journal de réplication	Nom et emplacement du fichier journal de réplication. La valeur par défaut ce de paramètre est `<WAS_HOME>\products\sklm\logs\replication`.
Taille maximale du fichier journal (en Ko)	Taille maximale d'un fichier journal avant que le remplacement n'ait lieu. La valeur par défaut est 1 000 Ko. Lorsque le fichier atteint la taille maximale, un nouveau fichier journal est créé.
Nombre maximal de fichiers journaux à conserver	Nombre maximal de fichiers journaux que vous souhaitez conserver. Par défaut, IBM Security Key Lifecycle Manager conserve les trois derniers fichiers journaux. Lorsque le nombre de fichiers dépasse la limite spécifiée, le fichier le plus ancien est supprimé.

d. Cliquez sur **OK**.

Interface de ligne de commande

a. Entrez la commande **`tklmReplicationConfigGetEntry`** sur une seule ligne pour obtenir la valeur en cours de la propriété cible dans le fichier `ReplicationSKLMConfig.properties`. Par exemple, entrez :

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

Voici un exemple de réponse :

```
none
```

b. Spécifiez les modifications. Par exemple, pour remplacer la valeur de la propriété **`replication.role`** par `master`, entrez sur une seule ligne :

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

Interface REST

a. Obtenez un identificateur d'authentification utilisateur unique pour accéder aux services REST d'IBM Security Key Lifecycle Manager. Pour plus d'informations sur le processus d'authentification, voir Processus d'authentification pour les services REST.

b. Pour exécuter le **service REST Get Single Config Property**, envoyez la demande HTTP GET. Transmettez l'identificateur d'authentification utilisateur que vous avez obtenu à l'étape a avec le message de demande, conformément à l'exemple suivant :

Demandes de service

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

Réponse positive

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

c. Spécifiez les modifications. Par exemple, vous pouvez utiliser le **service REST Update Replication Config Property** pour envoyer la demande de service suivante afin de changer la valeur de la propriété **replication.role** :

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

Que faire ensuite

Vous pouvez changer les paramètres des serveurs clones en vue de la réception des fichiers de sauvegarde du serveur maître.

Configuration d'un serveur maître avec chiffrement par mot de passe lorsque HSM est configuré

Vous pouvez changer les paramètres par défaut d'un serveur maître pour la communication avec le serveur clone afin de répliquer des données d'IBM Security Key Lifecycle Manager en utilisant le chiffrement par mot de passe pour les sauvegardes quand Hardware Security Module (HSM) est configuré.

Avant de commencer

Assurez-vous que IBM Security Key Lifecycle Manager est configuré pour utiliser HSM pour stocker la clé principale avant de sauvegarder et de répliquer les données avec un chiffrement basé sur HSM. Pour connaître les étapes de configuration, voir «Configuration de paramètres HSM», à la page 215.

Pourquoi et quand exécuter cette tâche

Remarque : Les données sont répliquées sur les serveurs clones en fonction d'un calendrier planifié uniquement lorsque de nouveaux objets cryptographiques sont ajoutés au serveur maître.

Utilisez l'interface graphique, l'interface de ligne de commande ou l'interface REST pour modifier les paramètres dans le fichier de configuration ReplicationSKLMConfig.properties en fonction de vos besoins.

Vous devez définir la propriété **enablePBEInHSM=true** dans le fichier <*SKLM_HOME*>/config/SKLMConfig.properties pour sauvegarder des données avec le chiffrement par mot de passe lorsque HSM est configuré.

Pour plus d'informations sur les méthodes de chiffrement pour les sauvegardes et la réplication, consultez Méthodes de chiffrement de sauvegarde pour activités de réplication.

Si vous souhaitez configurer IBM Security Key Lifecycle Manager pour les activités de sauvegarde et de réplication haute performance, vous devez définir le paramètre **enableHighScaleBackup=true** dans le fichier de configuration <*SKLM_HOME*>/config/SKLMConfig.properties file du serveur maître.

Remarque : Si vous définissez le paramètre **enableHighScaleBackup=true** pour la sauvegarde et la réplication de grandes quantités de clés, les systèmes maître et clone doivent être identiques pour que la réplication des données aboutisse. Le système d'exploitation, les structures de répertoire et l'administrateur Db2 doivent être identiques sur les serveurs maîtres et clones.

Procédure

1. Définissez la propriété **enablePBEInHSM=true** dans le fichier <*SKLM_HOME*>/config/SKLMConfig.properties.

   Interface de ligne de commande

   a. Accédez au répertoire WAS_HOME/bin. Par exemple,

      Windows

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

      Linux

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

   b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme SKLMAdmin. Par exemple,

      Windows

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

      Linux

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

   c. Exécutez la commande **tklmConfigUpdateEntry** pour définir la propriété **enablePBEInHSM** dans le fichier de configuration SKLMConfig.properties.

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

   Interface REST

   a. Ouvrez un client REST.

   b. Obtenez un identificateur d'authentification utilisateur unique pour accéder aux services REST d'IBM Security Key Lifecycle Manager. Pour plus d'informations sur le processus d'authentification, voir Processus d'authentification pour les services REST.

   c. Exécutez **Update Config Property REST Service** pour définir la propriété **enablePBEInHSM** dans le fichier de configuration SKLMConfig.properties. Transmettez l'identificateur

d'authentification utilisateur que vous avez obtenu à l'étape b avec le message de demande, conformément à l'exemple suivant :

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

2. Accédez à la page ou au répertoire approprié pour configurer des paramètres de réplication.

   Interface graphique

   a. Connectez-vous à l'interface graphique.
   b. Cliquez sur **IBM Security Key Lifecycle Manager** > **Administration** > **Réplication**.

   Interface de ligne de commande

   a. Accédez au répertoire WAS_HOME/bin.
   b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme SKLMAdmin.

   Interface REST

   Ouvrez un client REST.

3. Modifiez la valeur d'un ou de plusieurs paramètres du serveur maître .

   Interface graphique

   a. Sélectionnez **Maître**.
   b. Sélectionnez une option de gestion de serveur de réplication.

      Démarrage du serveur de réplication

      Cliquez sur **Démarrer le serveur de réplication** afin de démarrer le serveur de réplication pour la réplication des données et des fichiers actifs IBM Security Key Lifecycle Manager sur les serveurs clones en fonction d'un calendrier configuré.

      Arrêt du serveur de réplication

      Cliquez sur **Arrêter le serveur de réplication** pour arrêter le serveur de réplication, de telle sorte que les données et les fichiers actifs IBM Security Key Lifecycle Manager ne soient pas répliqués sur les serveurs clones.

      Réplication immédiate

      Cliquez sur **Répliquer maintenant** pour exécuter immédiatement la tâche de réplication IBM Security Key Lifecycle Manager et pour faire en sorte qu'une sauvegarde soit envoyée aux clones configurés.

   c. Indiquez les paramètres appropriés.

      Propriétés de base

Certificat du magasin de clés	Sélectionnez un certificat dans la liste. Assurez-vous que le certificat SSL/TLS existe sur le maître et sur tous les systèmes clones que vous configurez pour la réplication.
Phrase de passe de chiffrement de la sauvegarde de la réplication	Mot de passe de chiffrement du fichier de sauvegarde pour s'assurer de la sécurité des données. Le serveur clone utilise le même mot de passe pour déchiffrer et restaurer le fichier.

Confirmer la phrase de passe de chiffrement de la sauvegarde de la réplication	Spécifiez de nouveau le même mot de passe pour vérifier le mot de passe que vous avez spécifié.
Port d'écoute maître	Numéro de port pour la communication lorsque des réplications non sérialisées ou retardées ont lieu. Le port d'écoute maître par défaut est 1111.
Cliquez sur le lien **Ajouter un clone** dans la section **Détails du clone** pour configurer les paramètres de réplication pour les clones.	
Adresse IP ou nom d'hôte du clone -1	Adresse IP ou nom d'hôte des serveurs clones. Vous ne pouvez répliquer qu'un seul serveur maître avec 20 serveurs clones maximum.
Port du clone -1	Numéro de port pour l'envoi des fichiers de sauvegarde sur les serveurs clones. Chaque serveur clone est identifié par un numéro de port. Le numéro de port par défaut pour le serveur clone est 2222.

Propriétés avancées

Répertoire de destination de la sauvegarde de la réplication	Emplacement de stockage des fichiers de sauvegarde. La zone **Répertoire de destination de la sauvegarde de la réplication** affiche le chemin de répertoire *<SKLM_DATA>* par défaut dans lequel le fichier de sauvegarde est stocké, par exemple `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data`. Pour la définition de *<SKLM_DATA>*, voir Définitions relatives à un répertoire *HOME* et d'autres variables de répertoire. Cliquez sur **Parcourir** pour spécifier l'emplacement du référentiel de sauvegarde sous le répertoire *<SKLM_DATA>*. Le chemin de répertoire dans la zone **Répertoire de destination de sauvegarde de la réplication** change en fonction de la valeur définie pour la propriété **`browse.root.dir`** dans le fichier `SKLMConfig.properties`.
Nombre maximal de fichiers de réplication à conserver avant le remplacement	Nombre maximal de fichiers de réplication que vous souhaitez conserver. La valeur doit être un entier positif compris entre 2 et 10. Lorsque le nombre de fichiers dépasse la limite spécifiée, le fichier le plus ancien est supprimé.
Fréquence de réplication (en heures)	Fréquence à laquelle vérifier si l'opération de sauvegarde est nécessaire. La valeur par défaut est définie sur 24 heures. Ce paramètre est ignoré si la valeur de **Heure de début de réplication quotidienne** est définie.
Heure de réplication quotidienne (au format HH:MM)	Heure au format `HH:MM` à laquelle la tâche de réplication est exécuté tous les jours.
Nom du fichier journal de réplication	Nom et emplacement du fichier journal de réplication. La valeur par défaut ce de paramètre est *<WAS_HOME>*`\products\sklm\logs\replication`.
Taille maximale du fichier journal (en Ko)	Taille maximale d'un fichier journal avant que le remplacement n'ait lieu. La valeur par défaut est 1 000 Ko. Lorsque le fichier atteint la taille maximale, un nouveau fichier journal est créé.

Nombre maximal de fichiers journaux à conserver	Nombre maximal de fichiers journaux que vous souhaitez conserver. Par défaut, IBM Security Key Lifecycle Manager conserve les trois derniers fichiers journaux. Lorsque le nombre de fichiers dépasse la limite spécifiée, le fichier le plus ancien est supprimé.

d. Cliquez sur **OK**.

Interface de ligne de commande

a. Entrez la commande `tklmReplicationConfigGetEntry` sur une seule ligne pour obtenir la valeur en cours de la propriété cible dans le fichier `ReplicationSKLMConfig.properties` comme indiqué dans l'exemple ci-dessous.

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

Voici un exemple de réponse :

```
none
```

b. Spécifiez les modifications. Par exemple, pour remplacer la valeur de la propriété **replication.role** par `master`, entrez sur une seule ligne :

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

Pour plus de détails sur tous les paramètres de configuration de réplication disponibles, voir Paramètres de configuration de réplication.

Interface REST

a. Exécutez le **service REST Get Single Config Property** en envoyant la demande HTTP GET, comme illustré dans l'exemple suivant :

Demandes de service

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

Réponse positive

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

b. Spécifiez les modifications. Par exemple, vous pouvez utiliser le **service REST Update Replication Config Property** pour envoyer la demande de service suivante afin de changer la valeur de la propriété **replication.role** :

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

Pour plus de détails sur tous les paramètres de configuration de réplication disponibles, voir Paramètres de configuration de réplication.

Que faire ensuite

Vous pouvez changer les paramètres des serveurs clones en vue de la réception des fichiers de sauvegarde du serveur maître.

Configuration d'un serveur maître avec chiffrement basé sur HSM pour les sauvegardes

Vous pouvez changer les paramètres par défaut d'un serveur maître pour la communication avec le serveur clone afin de répliquer des données d'IBM Security Key Lifecycle Manager en utilisant le chiffrement basé sur HSM pour les sauvegardes.

Avant de commencer

Assurez-vous que IBM Security Key Lifecycle Manager est configuré pour utiliser HSM pour stocker la clé principale avant de sauvegarder et de répliquer les données avec un chiffrement basé sur HSM. Pour connaître les étapes de configuration, voir «Configuration de paramètres HSM», à la page 215.

Appliquez les directives suivantes pour l'utilisation du chiffrement HSM.

- La même partition HSM doit se trouver avec toutes ses entrées clés intactes sur tous les serveurs clones.
- La clé principale que vous avez utilisée pour le chiffrement de la clé de sauvegarde doit être intacte pour répliquer le fichier de sauvegarde sur le serveur clone. Si la clé principale est rafraîchie, toutes les anciennes sauvegardes sont inaccessibles ou inutilisables.
- Vous devez vous connecter aux mêmes instance HSM et clé principale pour la réplication automatisée, indépendamment du fait que vous utilisez le chiffrement basé sur HSM ou le chiffrement par mot de passe.

Pourquoi et quand exécuter cette tâche

Remarque : Les données sont répliquées sur les serveurs clones en fonction d'un calendrier planifié uniquement lorsque de nouveaux objets cryptographiques sont ajoutés au serveur maître.

Utilisez l'interface graphique, l'interface de ligne de commande ou l'interface REST pour modifier les paramètres dans le fichier de configuration `ReplicationSKLMConfig.properties` en fonction de vos besoins.

Pour plus d'informations sur les méthodes de chiffrement pour les sauvegardes et la réplication, consultez Méthodes de chiffrement de sauvegarde pour activités de réplication.

Si vous voulez configurer IBM Security Key Lifecycle Manager pour les activités de sauvegarde et de réplication de haute performance, vous devez définir le paramètre suivant dans le fichier de configuration *<SKLM_HOME>*`\config\SKLMConfig.properties` du serveur maître, par exemple `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\config\SKLMConfig.properties` :

```
enableHighScaleBackup=true
```

Remarque : Si vous définissez le paramètre **`enableHighScaleBackup=true`** pour la sauvegarde et la réplication de grandes quantités de clés, les systèmes maître et clone doivent être identiques pour que la réplication des données aboutisse. Le

système d'exploitation, les structures de répertoire et l'administrateur Db2 doivent être identiques sur les serveurs maîtres et clones.

Procédure

1. Accédez à la page ou au répertoire approprié(e) :

   Interface graphique

   a. Connectez-vous à l'interface graphique.
   b. Cliquez sur **IBM Security Key Lifecycle Manager** > **Administration** > **Réplication**.

   Interface de ligne de commande

   a. Accédez au répertoire `WAS_HOME/bin`. Par exemple,

      Windows

      ```
      cd unité:\Program Files (x86)\IBM\WebSphere\AppServer\
      bin
      ```

      Linux

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

   b. Démarrez l'interface **`wsadmin`** en utilisant un ID utilisateur autorisé, comme `SKLMAdmin`. Par exemple,

      Windows

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

      Linux

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

   Interface REST

   Ouvrez un client REST.

2. Modifiez la valeur d'un ou de plusieurs paramètres du serveur maître :

   Interface graphique

   a. Sélectionnez **Maître**.
   b. Sélectionnez une option de gestion de serveur de réplication.

      Démarrez le serveur de réplication

      Cliquez sur **Démarrer le serveur de réplication** afin de démarrer le serveur de réplication pour la réplication des données et des fichiers actifs IBM Security Key Lifecycle Manager sur les serveurs clones en fonction d'un calendrier configuré.

      Arrêt du serveur de réplication

      Cliquez sur **Arrêter le serveur de réplication** pour arrêter le serveur de réplication, de telle sorte que les données et les fichiers actifs IBM Security Key Lifecycle Manager ne soient pas répliqués sur les serveurs clones.

      Réplication immédiate

      Cliquez sur **Répliquer maintenant** pour exécuter immédiatement la tâche de réplication IBM Security Key Lifecycle Manager et pour faire en sorte qu'une sauvegarde soit envoyée aux clones configurés.

   c. Spécifiez les paramètres appropriés :

      Propriétés de base

Certificat du magasin de clés	Sélectionnez un certificat dans la liste. Assurez-vous que le certificat SSL/TLS existe sur le maître et sur tous les systèmes clones que vous configurez pour la réplication.
Port d'écoute maître	Numéro de port pour la communication lorsque des réplications non sérialisées ou retardées ont lieu. Le port d'écoute maître par défaut est 1111.
Cliquez sur le lien **Ajouter un clone** dans la section **Détails du clone** pour configurer les paramètres de réplication pour les clones.	
Adresse IP ou nom d'hôte du clone -1	Adresse IP ou nom d'hôte des serveurs clones. Vous ne pouvez répliquer qu'un seul serveur maître avec 20 serveurs clones maximum. Cliquez sur le lien **Ajouter des clones** pour configurer les paramètres de réplication pour plusieurs clones.
Port du clone -1	Numéro de port pour l'envoi des fichiers de sauvegarde sur les serveurs clones. Chaque serveur clone est identifié par un numéro de port. Le numéro de port par défaut pour le serveur clone est 2222.

Propriétés avancées

Répertoire de destination de la sauvegarde de la réplication	Emplacement de stockage des fichiers de sauvegarde. La zone **Répertoire de destination de la sauvegarde de la réplication** affiche le chemin de répertoire *<SKLM_DATA>* par défaut dans lequel le fichier de sauvegarde est stocké, par exemple `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data`. Pour la définition de *<SKLM_DATA>*, voir Définitions relatives à un répertoire *HOME* et d'autres variables de répertoire. Cliquez sur **Parcourir** pour spécifier l'emplacement du référentiel de sauvegarde sous le répertoire *<SKLM_DATA>*. Le chemin de répertoire dans la zone **Répertoire de destination de sauvegarde de la réplication** change en fonction de la valeur définie pour la propriété **`browse.root.dir`** dans le fichier `SKLMConfig.properties`.
Nombre maximal de fichiers de réplication à conserver avant le remplacement	Nombre maximal de fichiers de réplication que vous souhaitez conserver. La valeur doit être un entier positif compris entre 2 et 10. Lorsque le nombre de fichiers dépasse la limite spécifiée, le fichier le plus ancien est supprimé.
Fréquence de réplication (en heures)	Fréquence à laquelle vérifier si l'opération de sauvegarde est nécessaire. La valeur par défaut est définie sur 24 heures. Ce paramètre est ignoré si la valeur de **Heure de début de réplication quotidienne** est définie.
Heure de réplication quotidienne (au format HH:MM)	Heure au format `HH:MM` à laquelle la tâche de réplication est exécuté tous les jours.
Nom du fichier journal de réplication	Nom et emplacement du fichier journal de réplication. La valeur par défaut ce de paramètre est *<WAS_HOME>*`\products\sklm\logs\replication`.
Taille maximale du fichier journal (en Ko)	Taille maximale d'un fichier journal avant que le remplacement n'ait lieu. La valeur par défaut est 1 000 Ko. Lorsque le fichier atteint la taille maximale, un nouveau fichier journal est créé.

Nombre maximal de fichiers journaux à conserver	Nombre maximal de fichiers journaux que vous souhaitez conserver. Par défaut, IBM Security Key Lifecycle Manager conserve les trois derniers fichiers journaux. Lorsque le nombre de fichiers dépasse la limite spécifiée, le fichier le plus ancien est supprimé.

d. Cliquez sur **OK**.

Interface de ligne de commande

a. Entrez la commande **tklmReplicationConfigGetEntry** sur une seule ligne pour obtenir la valeur en cours de la propriété cible dans le fichier ReplicationSKLMConfig.properties. Par exemple, entrez

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

Voici un exemple de réponse :

```
none
```

b. Spécifiez les modifications. Par exemple, pour remplacer la valeur de la propriété **replication.role** par master, entrez sur une seule ligne :

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

Pour plus de détails sur tous les paramètres de configuration de réplication disponibles, voir Paramètres de configuration de réplication.

Interface REST

a. Obtenez un identificateur d'authentification utilisateur unique pour accéder aux services REST d'IBM Security Key Lifecycle Manager. Pour plus d'informations sur le processus d'authentification, voir Processus d'authentification pour les services REST.

b. Pour exécuter le **service REST Get Single Config Property**, envoyez la demande HTTP GET. Transmettez l'identificateur d'authentification utilisateur que vous avez obtenu à l'étape a avec le message de demande, conformément à l'exemple suivant :

Demandes de service

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

Réponse positive

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

c. Spécifiez les modifications. Par exemple, vous pouvez utiliser le **service REST Update Replication Config Property** pour envoyer la demande de service suivante afin de changer la valeur de la propriété **replication.role** :

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

Pour plus de détails sur tous les paramètres de configuration de réplication disponibles, voir Paramètres de configuration de réplication.

Que faire ensuite

Vous pouvez changer les paramètres des serveurs clones en vue de la réception des fichiers de sauvegarde du serveur maître.

Spécification des paramètres de réplication pour un serveur clone

Vous pouvez changer les paramètres par défaut d'un serveur clone afin de recevoir les données IBM Security Key Lifecycle Manager du serveur maître en fonction d'un calendrier configuré. Les données sont répliquées sur les serveurs clones uniquement lorsque de nouveaux objets cryptographiques sont ajoutés au serveur maître.

Pourquoi et quand exécuter cette tâche

Utilisez la page Configuration de réplication automatisée du clone pour modifier les paramètres de réplication. Vous pouvez également utiliser les commandes de l'interface CLI ou les interfaces REST suivantes pour répertorier ou modifier les propriétés appropriées dans le fichier de configuration `ReplicationSKLMConfig.properties` :

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

Procédure

1. Accédez à la page ou au répertoire approprié :
   - Interface graphique :
     a. Connectez-vous à l'interface graphique.
     b. Cliquez sur **IBM Security Key Lifecycle Manager** > **Administration** > **Réplication**.
   - Interface de ligne de commande
     a. Accédez au répertoire <*WAS_HOME*>/bin. Exemple :

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

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

     b. Démarrez l'interface **`wsadmin`** en utilisant un ID utilisateur autorisé, comme `SKLMAdmin`. Exemple :

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

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

   - Interface REST :
     – Ouvrez un client REST.
2. Modifiez la valeur d'un ou de plusieurs paramètres du serveur clone.
   - Dans l'interface graphique :
     a. Sélectionnez **Clone**.

b. Sélectionnez une option de gestion de serveur de réplication.

Démarrez le serveur de réplication
Cliquez sur **Démarrer le serveur de réplication** afin de démarrer le serveur de réplication pour la réception des données IBM Security Key Lifecycle Manager à partir du serveur maître.

Arrêt du serveur de réplication
Cliquez sur **Arrêter le serveur de réplication** pour arrêter le serveur de réplication afin que les données IBM Security Key Lifecycle Manager du serveur maître ne soient pas reçues par les serveurs clones.

c. Spécifiez les paramètres appropriés :

Propriétés de base

Port d'écoute du clone	Numéro de port sur lequel le serveur clone doit être à l'écoute pour recevoir les fichiers de sauvegarde. Le numéro de port par défaut est 2222.
Port d'écoute maître	Numéro de port pour la communication lorsque des réplications non sérialisées ou retardées ont lieu. Le port d'écoute maître par défaut est 1111.

Propriétés avancées

Nombre de tentatives en cas d'échec de la restauration	Nombre maximal de tentatives autorisées après l'échec de la première opération de restauration. La valeur doit être un entier positif compris entre 0 et 2.
Nom du fichier journal de réplication	Nom et emplacement du fichier journal de réplication. La valeur par défaut ce de paramètre est *<WAS_HOME>*\products\sklm\logs\replication.
Taille maximale du fichier journal (en Ko)	Taille maximale d'un fichier journal avant que le remplacement n'ait lieu. La valeur par défaut est 1 000 Ko. Lorsque le fichier atteint la taille maximale, un nouveau fichier journal est créé.
Nombre maximal de fichiers journaux à conserver	Nombre maximal de fichiers journaux que vous souhaitez conserver. Par défaut, IBM Security Key Lifecycle Manager conserve les trois derniers fichiers journaux. Lorsque le nombre de fichiers dépasse la limite spécifiée, le fichier le plus ancien est supprimé.

d. Cliquez sur **OK**.

- Interface de ligne de commande :
  a. Entrez la commande **tklmReplicationConfigGetEntry** sur une seule ligne pour obtenir la valeur en cours de la propriété cible dans le fichier ReplicationSKLMConfig.properties. Par exemple, entrez

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

  Voici un exemple de réponse :

```
none
```

  b. Spécifiez les modifications. Par exemple, pour remplacer la valeur de la propriété **replication.role** par clone, entrez sur une seule ligne :

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

- Interface REST :

a. Obtenez un identificateur d'authentification utilisateur unique pour accéder aux services REST d'IBM Security Key Lifecycle Manager. Pour plus d'informations sur le processus d'authentification, voir Processus d'authentification pour les services REST.

b. Pour appeler le **service REST Get Single Config Property**, envoyez la demande HTTP GET. Transmettez l'identificateur d'authentification utilisateur que vous avez obtenu à l'étape a avec le message de demande, conformément à l'exemple suivant :

Demandes de service

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

Réponse positive

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

c. Spécifiez les modifications. Par exemple, vous pouvez utiliser le **service REST Update Replication Config Property** pour envoyer la demande de service suivante afin de changer la valeur de la propriété **replication.role** :

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

Que faire ensuite

Vous pouvez changer les paramètres pour d'autres serveurs de clone. Vous pouvez répliquer des données d'IBM Security Key Lifecycle Manager depuis un serveur maître principal sur 20 serveurs clones secondaires maximum.

Planification d'une opération de sauvegarde automatique

Vous pouvez configurer des paramètres de réplication afin d'exécuter automatiquement l'opération de sauvegarde pour vous assurer que les données critiques d'IBM Security Key Lifecycle Manager sont sauvegardées à intervalles réguliers.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser le programme de réplication d'IBM Security Key Lifecycle Manager afin de planifier une opération de sauvegarde automatique. Vous ne devez configurer les propriétés que pour le serveur maître afin de sauvegarder les données à intervalles réguliers.

Utilisez l'interface graphique, l'interface de ligne de commande ou l'interface REST pour modifier les paramètres dans le fichier de configuration `ReplicationSKLMConfig.properties` en fonction de vos besoins.

IBM Security Key Lifecycle Manager prend en charge les méthodes de chiffrement suivantes pour les sauvegardes :

Chiffrement par mot de passe
Lorsque vous configurez le serveur maître pour la réplication automatisée, un mot de passe est spécifié pour chiffrer la clé de sauvegarde. Lorsque les données sont répliquées sur le serveur clone, le même mot de passe de chiffrement est utilisé pour déchiffrer et restaurer les fichiers de sauvegarde.

Chiffrement basé sur HSM
Vous pouvez configurer IBM Security Key Lifecycle Manager pour utiliser Hardware Security Module (HSM) afin de stocker la clé de chiffrement principale sur les serveurs maîtres et clones. Lorsque vous exécutez le programme de réplication, la clé de sauvegarde sur le serveur maître est chiffrée par la clé principale, qui est stockée dans HSM. Lorsque les données sont reproduites sur le serveur clone, la clé principale stockée dans HSM déchiffre la clé de sauvegarde. La clé de sauvegarde est utilisée pour restaurer le contenu de la sauvegarde.

Pour plus d'informations sur la façon de configurer le serveur maître avec le chiffrement basé sur HSM, voir «Configuration d'un serveur maître avec chiffrement basé sur HSM pour les sauvegardes», à la page 195. Pour plus d'informations sur la façon de configurer le serveur maître avec le chiffrement par mot de passe lorsque HSM est configuré, voir «Configuration d'un serveur maître avec chiffrement par mot de passe lorsque HSM est configuré», à la page 190.

La procédure suivante décrit comment planifier une opération de sauvegarde automatique en utilisant le chiffrement par mot de passe.

Procédure

1. Accédez à la page ou au répertoire approprié(e) :

   Interface graphique
   a. Connectez-vous à l'interface graphique.
   b. Cliquez sur **IBM Security Key Lifecycle Manager** > **Administration** > **Réplication**.

   Interface de ligne de commande
   a. Accédez au répertoire `WAS_HOME/bin`. Par exemple,

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

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

   b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme `SKLMAdmin`. Par exemple,

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

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

   Interface REST
   Ouvrez un client REST.

2. Modifiez la valeur d'un ou de plusieurs paramètres du serveur maître :

   Interface graphique
   a. Sélectionnez **Maître**.
   b. Sélectionnez une option de gestion de serveur de réplication.

Démarrage du serveur de réplication
Cliquez sur **Démarrer le serveur de réplication** pour que le serveur de réplication commence la sauvegarde des données IBM Security Key Lifecycle Manager en fonction d'un calendrier configuré.

Arrêt du serveur de réplication
Cliquez sur **Arrêter le serveur de réplication** pour arrêter le serveur de réplication de telle sorte que les données IBM Security Key Lifecycle Manager ne soient pas sauvegardées.

Réplication immédiate
Cliquez sur **Répliquer maintenant** pour exécuter immédiatement la tâche de réplication IBM Security Key Lifecycle Manager et pour provoquer la création d'un fichier de sauvegarde.

c. Configurez les paramètres.

Propriétés de base

Certificat du magasin de clés	Sélectionnez un certificat dans la liste. Assurez-vous que le certificat SSL/TLS existe sur le maître et sur tous les systèmes clones que vous configurez pour la réplication.
Phrase de passe de chiffrement de la sauvegarde de la réplication	Mot de passe de chiffrement du fichier de sauvegarde pour s'assurer de la sécurité des données. Vous devez utiliser le même mot de passe pour déchiffrer et restaurer le fichier. **Remarque :** Si le chiffrement basé sur HSM est utilisé pour les sauvegardes, vous ne devez pas spécifier le mot de passe.
Confirmer la phrase de passe de chiffrement de la sauvegarde de la réplication	Spécifiez de nouveau le même mot de passe pour vérifier le mot de passe que vous avez spécifié.
Port d'écoute maître	Numéro de port pour la communication lorsque des réplications non sérialisées ou retardées ont lieu. Le port d'écoute maître par défaut est 1111.

Propriétés avancées

Répertoire de destination de la sauvegarde de la réplication	Emplacement de stockage des fichiers de sauvegarde. La zone **Répertoire de destination de la sauvegarde de la réplication** affiche le chemin de répertoire *<SKLM_DATA>* par défaut dans lequel le fichier de sauvegarde est stocké, par exemple `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data`. Pour la définition de *<SKLM_DATA>*, voir Définitions relatives à un répertoire *HOME* et d'autres variables de répertoire. Cliquez sur **Parcourir** pour spécifier l'emplacement du référentiel de sauvegarde sous le répertoire *<SKLM_DATA>*.
Nombre maximal de fichiers de réplication à conserver avant la réinitialisation	Nombre maximal de fichiers de réplication que vous souhaitez conserver. La valeur doit être un entier positif compris entre 2 et 10. Lorsque le nombre de fichiers dépasse la limite spécifiée, le fichier le plus ancien est supprimé.
Fréquence de réplication (en heures)	Fréquence à laquelle vérifier si l'opération de sauvegarde est nécessaire. La valeur par défaut est définie sur 1 heure. Ce paramètre est ignoré si la valeur de **Heure de début de réplication quotidienne** est définie.

Heure de réplication quotidienne (au format HH:MM)	Heure au format `HH:MM` à laquelle la tâche de réplication est exécuté tous les jours.
Nom du fichier journal de réplication	Nom et emplacement du fichier journal de réplication. La valeur par défaut ce de paramètre est *<WAS_HOME>*`\products\sklm\logs\replication`.
Taille maximale du fichier journal (en Ko)	Taille maximale d'un fichier journal avant que le remplacement n'ait lieu. La valeur par défaut est 1 000 Ko. Lorsque le fichier atteint la taille maximale, un nouveau fichier journal est créé.
Nombre maximal de fichiers journaux à conserver	Nombre maximal de fichiers journaux que vous souhaitez conserver. Par défaut, IBM Security Key Lifecycle Manager conserve les trois derniers fichiers journaux. Lorsque le nombre de fichiers dépasse la limite spécifiée, le fichier le plus ancien est supprimé.

d. Cliquez sur **OK**.

Interface de ligne de commande

a. Entrez la commande **tklmReplicationConfigGetEntry** sur une seule ligne pour obtenir la valeur en cours de la propriété cible dans le fichier `ReplicationSKLMConfig.properties`. Par exemple, entrez :

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

Voici un exemple de réponse :

```
none
```

b. Spécifiez les modifications. Par exemple, pour remplacer la valeur de la propriété **replication.role** par `master`, entrez sur une seule ligne :

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

Interface REST

a. Obtenez un identificateur d'authentification utilisateur unique pour accéder aux services REST d'IBM Security Key Lifecycle Manager. Pour plus d'informations sur le processus d'authentification, voir Processus d'authentification pour les services REST.

b. Pour exécuter le **service REST Get Single Config Property**, envoyez la demande HTTP GET. Transmettez l'identificateur d'authentification utilisateur que vous avez obtenu à l'`étape a` avec le message de demande, conformément à l'exemple suivant :

Demandes de service

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

Réponse positive

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

c. Spécifiez les modifications. Par exemple, vous pouvez utiliser le **service REST Update Replication Config Property** pour envoyer la demande de service suivante afin de changer la valeur de la propriété **replication.role** :

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

Mise en place d'un processus de réplication en utilisant les commandes CLI et les services REST

Vous devez configurer un environnement de base dans IBM Security Key Lifecycle Manager pour exécuter le processus de réplication.

Pourquoi et quand exécuter cette tâche

Cette rubrique décrit comment configurer le processus de réplication en utilisant les commandes de l'interface de ligne de commande IBM Security Key Lifecycle Manager et les interfaces REST pour la réplication.

Procédure

1. Configurez le système principal d'IBM Security Key Lifecycle Manager.
2. Spécifiez un certificat SSLSERVER pour que la réplication fonctionne. Vous pouvez créer le certificat en utilisant l'interface utilisateur graphique, l'interface de ligne de commande, ou l'interface REST comme le montrent les exemples suivants.

   Interface graphique

   a. Connectez-vous à l'interface graphique.
   b. Cliquez sur **Configuration avancée** > **Certificats de serveur**.

   Interface de ligne de commande

   a. Accédez au répertoire WAS_HOME/bin. Par exemple,

      Windows

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

      Linux

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

   b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme SKLMAdmin. Par exemple,

      Windows

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

      Linux

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

   c. Entrez la commande **tklmCertCreate** sur une seule ligne. Par exemple, pour créer un certificat autosigné, entrez :

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

   Interface REST

a. Ouvrez un client REST.
b. Obtenez un identificateur d'authentification utilisateur unique pour accéder aux services REST d'IBM Security Key Lifecycle Manager. Pour plus d'informations sur le processus d'authentification, voir Processus d'authentification pour les services REST.
c. Pour créer un certificat autosigné, exécutez le service **Certificate Generate Request REST Service** en envoyant la demande HTTP suivante.

```
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. Créez une sauvegarde du serveur IBM Security Key Lifecycle Manager maître comme indiqué dans les exemples suivants.

Remarque : Vous n'avez pas à spécifier le mot de passe lorsque IBM Security Key Lifecycle Manager est configuré pour utiliser Hardware Security Module (HSM) afin de stocker la clé de chiffrement principale. Pour plus d'informations sur les méthodes de chiffrement pour la sauvegarde des données, voir Chiffrement basé sur HSM pour les sauvegardes.

Interface graphique

a. Connectez-vous à l'interface graphique.
b. Cliquez sur **Sauvegarde et restauration**.

Interface de ligne de commande

Entrez la commande **tklmBackupRun**.

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

Interface REST

Pour créer une sauvegarde, exécutez le **Service REST Backup Run** en envoyant la demande HTTP suivante.

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

Remarque :

Vous pouvez configurer IBM Security Key Lifecycle Manager pour des activités de sauvegarde et de réplication de haute performance en définissant le paramètre suivant dans le fichier de configuration `SKLMConfig.properties` sur le serveur maître.

```
enableHighScaleBackup=true
```

Pour sauvegarder et répliquer de grandes quantités de données, les serveurs maîtres et clones doivent être identiques. Le système d'exploitation, les structures de répertoire et l'administrateur Db2 doivent être identiques sur les serveurs.

Pour plus d'informations sur la façon de sauvegarder une quantité importante de données, consultez «Sauvegarde de grande quantité de données», à la page 135.

4. Copiez la sauvegarde créée à l'étape 3 sur chacun des systèmes clones d'IBM Security Key Lifecycle Manager. Restaurez cette sauvegarde sur chacun de ces systèmes comme dans les exemples suivants :

   Interface graphique

   a. Connectez-vous à l'interface graphique.
   b. Cliquez sur **Sauvegarde et restauration**.

   Interface de ligne de commande

   Entrez la commande **tklmBackupRestoreRun** sur une seule ligne :

   ```
   print AdminTask.tklmBackupRunRestore
   ('[-backupFilePath /opt/sklmbackup/sklm_v2.7_20160412074433_backup.jar
     -password myBackupPwd]')
   ```

   Interface REST

   Pour restaurer une sauvegarde, exécutez le **Service REST Backup Run Restore** en envoyant la demande HTTP suivante.

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

5. Créez le fichier de configuration de la réplication `ReplicationSKLMConfig.properties` sur le système principal. Ce fichier de configuration doit être un fichier texte que vous devez placer dans le même répertoire que le fichier de propriétés IBM Security Key Lifecycle Manager, par exemple, `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\config\ReplicationSKLMConfig.properties`.

   Utilisez l'interface de ligne de commande ou les services REST pour définir les propriétés dans le fichier `ReplicationSKLMConfig.properties`.

   Interface de ligne de commande

   Entrez la commande **tklmReplicationConfigUpdateEntry** sur une seule ligne pour définir la valeur en cours de la propriété **replication.role** sur `master`.

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

   Interface REST

   Pour définir la valeur, exécutez le **Service REST Update Replication Config Property** en envoyant la demande HTTP suivante.

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

   Pour plus de détails sur tous les paramètres de configuration de réplication disponibles, voir Paramètres de configuration de réplication.

   L'exemple suivant indique les zones obligatoires sur le système principal pour permettre le démarrage de la tâche de réplication.

   - Définir le rôle principal.

- Identifier le certificat à partir de l'étape 2 et fournir au moins un serveur clone et un numéro de port.
- Définir un port d'écoute principal et choisir un mot de passe.

  Remarque : Vous n'avez pas à spécifier le mot de passe lorsque IBM Security Key Lifecycle Manager est configuré pour utiliser Hardware Security Module (HSM) afin de stocker la clé de chiffrement principale. Pour plus d'informations sur les méthodes de chiffrement pour la sauvegarde des données dans le cadre des activités de réplication, voir Méthodes de chiffrement de sauvegarde pour activités de réplication.

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

La propriété **backup.EncryptionPassword** peut contenir des caractères, des chiffres ou des caractères spéciaux. Le produit rend impénétrable cette propriété lors de la première exécution de la réplication. La propriété **backup.TLSCertAlias** indique l'alias du certificat et la clé privée utilisée pour communiquer avec le clone créé à l'étape 2.

La propriété **replication.MasterListenPort** spécifie le port d'écoute du système principal pour certaines réponses des clones. Les propriétés **backup.ClientIP1** et **backup.ClientPort1** définissent le clone. La propriété **backup.ClientIP1** peut être un nom d'hôte ou une adresse IP. La propriété **backup.ClientPort1** indique le port d'écoute du client. Pour définir d'autres clones, vous devez spécifier les propriétés **backup.ClientIP*** et **backup.ClientPort***, où «*» est un nombre compris entre 2 et 20, comme vous l'avez fait lors de la première configuration.

6. Créez le fichier de configuration de la réplication `ReplicationSKLMConfig.properties` sur le système clone. Ce fichier de configuration doit être un fichier texte que vous devez placer dans le même répertoire que le fichier de propriétés IBM Security Key Lifecycle Manager, par exemple, `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\config\ReplicationSKLMConfig.properties`.

   Utilisez l'interface de ligne de commande ou l'interface REST pour définir les propriétés dans le fichier de configuration de la réplication comme décrit à l'étape 5.

   L'exemple suivant indique les zones obligatoires sur le système clone pour permettre le démarrage de la tâche de réplication.

   - Définir le rôle clone.
   - Définir un port d'écoute principal.
   - Définir un port d'écoute pour la restauration. Ce port doit avoir le même numéro de port codé dans le paramètre **backup.ClientPort*** correspondant sur le serveur principal.

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

   Définir la propriété **replication.role** est obligatoire pour les clones. Par défaut, la valeur de cette propriété est `master` (principal). La propriété **backup.TLSCertAlias** doit définir le certificat créé à l'étape 2. Cette propriété permet d'envoyer l'état du clone lorsque la réplication est retardée ou lorsque le processus de restauration dure plus longtemps que la durée pendant laquelle le système principal attend une réponse.

La propriété **replication.MasterListenPort** indique le port d'envoi de l'état lorsque la réplication est retardée ou lorsque le processus de restauration dure plus longtemps que la durée pendant laquelle le système principal attend une réponse. La dernière propriété **restore.ListenPort** est le port d'écoute du clone pour les demandes de réplication provenant du système principal.

7. Vous pouvez exécuter la tâche de réplication ad-hoc en utilisant la commande CLI **TKLMReplicationNow** ou le **Service REST Replication Now**. Ou, vous pouvez configurer une réplication planifiée. Vous pouvez planifier une tâche de sauvegarde à l'aide de la propriété **backup.DailyStartReplicationBackupTime** ou **backup.CheckFrequency** dans le fichier de configuration de la réplication.

   La propriété suivante planifie la tâche de sauvegarde à 23 h tous les jours.

   ```
   backup.DailyStartReplicationBackupTime=23:00
   ```

   La propriété suivante vérifie si une sauvegarde est nécessaire toutes les 24 heures et exécute la tâche si nécessaire.

   ```
   backup.CheckFrequency=1440
   ```

8. Redémarrez IBM Security Key Lifecycle Manager sur le système principal et sur le système clone. Utilisez la commande **tklmReplicationStatus** pour garantir l'exécution de la tâche de réplication. Vous pouvez voir les messages suivants sur un système clone et un système principal :

   Interface de ligne de commande

   Vous pouvez utiliser la commande CLI suivante pour vérifier que la tâche de réplication est en cours d'exécution :

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

   Système maître

   ```
   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
   ```

   Système clone

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

   Interface REST

   Utilisez **Service REST Replication Status** pour vérifier que la tâche de réplication est en cours d'exécution. Envoyez la demande HTTP suivante en utilisant un client REST :

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

   Système maître

   ```
   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." }

   ]
   ```

Système clone

```
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. La réplication est maintenant configurée et recherche les modifications toutes les 60 minutes. Vous pouvez modifier cet intervalle, défini pour que la réplication recherche chaque jour les modifications. Vous pouvez aussi utiliser la commande CLI **tklmReplicationNow** ou **Service REST Replication Now** pour exécuter une tâche de réplication immédiatement.

Résolution des problèmes liés à la réplication

Il convient de prendre en compte d'éventuels problèmes pouvant survenir sur les systèmes clones et sur le système principal lorsque vous exécutez la tâche de réplication d'IBM Security Key Lifecycle Manager.

Réplication incomplète

- Vérifiez que le certificat TSL/SSL et que la clé privée spécifiée dans le paramètre **backup.TLSCertAlias** sont disponibles sur les serveurs maîtres et clones.
- Assurez-vous que le numéro de port pour le serveur maître est libre. Les numéros de port de clone qui sont configurés sur le serveur maître doivent être libres sur le serveur clone.
- Contrôlez que les noms de serveur ou les adresses IP qui figurent dans le fichier de configuration de réplication sont corrects et accessibles depuis le serveur principal.
- Vérifiez si la tâche de réplication est active sur chaque serveur en exécutant la commande **tklmReplicationStatus**, le **service REST Replication Status** ou le statut de la section **Réplication** sur la page de bienvenue IBM Security Key Lifecycle Manager.
- En ce qui concerne la réplication Db2, assurez-vous que la date et l'heure du serveur principal et des serveurs clones sont bien synchronisées. Des différences importantes peuvent aboutir à un échec de la restauration.
- Vérifiez dans le fichier de configuration de la réplication que les paramètres minimaux requis sont définis sans erreur typographique.
- Définissez au maximum un élément maître et jusqu'à 20 clones associés.
- Consultez le fichier d'audit de la réplication pour obtenir plus d'informations sur l'échec de la réplication.

La réplication ne s'exécute pas au moment planifié

- Les réplications planifiées ont lieu uniquement lorsque de nouvelles clés et des unités sont ajoutées ou modifiées sur le serveur maître.
- Lorsqu'une heure de réplication spécifique et un intervalle de vérification sont définis dans le fichier de configuration de la réplication principale, l'heure remplace l'intervalle de vérification.

Réplication des systèmes clones

- Le serveur IBM Security Key Lifecycle Manager clone redémarre après la réplication.

- Les serveurs clones doivent être maintenus disponibles. Vous pouvez spécifier une heure précise pour terminer la réplication à l'aide du paramètre **restore.DailyStartReplicationRestoreTime**. Par exemple, pour exécuter des restaurations uniquement à 23h00, quelle que soit l'heure de réception du fichier de sauvegarde, codez la propriété suivante dans le fichier de configuration :

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

Serveur IBM Security Key Lifecycle Manager - Redémarrage

Suite au redémarrage du serveur, le serveur lit sa configuration et accepte les modifications de configuration, s'il en existe. Pour redémarrer le serveur IBM Security Key Lifecycle Manager, vous pouvez exécuter les scripts de redémarrage de serveur, le service REST ou utiliser l'interface graphique utilisateur.

Pourquoi et quand exécuter cette tâche

Pour redémarrer le serveur, utilisez le lien *<Utilisateur IBM Security Key Lifecycle Manager>* dans la barre d'en-tête de la page d'accueil (**service REST Restart Server**) ou exécutez les scripts **stopServer** et **startServer**.

Procédure

1. Accédez à la page ou au répertoire approprié.

   Interface graphique

   a. Connectez-vous à l'interface graphique.

   b. Sur la barre d'en-tête de la page d'accueil, cliquez sur le lien *<Utilisateur IBM Security Key Lifecycle Manager>*. Par exemple, cliquez sur le lien **SKLMAdmin**.

   Scripts de redémarrage de serveur

   a. Accédez au répertoire *<WAS_HOME>*\bin.

      Windows

      ```
      C:\Program Files\IBM\WebSphere\AppServer\bin
      ```

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

   Interface REST

   Ouvrez un client REST.

2. Redémarrez le serveur.

   Interface graphique

   a. Cliquez sur **Redémarrer le serveur**.

   b. Cliquez sur **OK**.

   Remarque : Le serveur IBM Security Key Lifecycle Manager est indisponible pendant quelques minutes lorsque l'opération de redémarrage est en cours.

   Scripts de redémarrage de serveur

   a. Arrêtez le serveur.

      Windows

      ```
      stopServer.bat server1
      ```

      Linux

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

La sécurité globale est activée par défaut. Entrez l'ID utilisateur et le mot de passe de l'administrateur WebSphere Application Server en tant que paramètres du script `stopServer`. Le script vous demande ces paramètres s'ils ont été omis, mais vous pouvez les spécifier sur la ligne de commande :

Windows

```
stopServer.bat server1 -username wasadmin -password mypwd
```

Linux

```
./stopServer.sh server1  -username wasadmin -password mypwd
```

b. Démarrez le serveur.

Windows

```
startServer.bat server1
```

Linux

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

Interface REST

a. Obtenez un identificateur d'authentification utilisateur unique pour accéder aux services REST d'IBM Security Key Lifecycle Manager. Pour plus d'informations sur le processus d'authentification, voir Processus d'authentification pour les services REST.

b. Pour exécuter le **service REST Restart Server**, envoyez la demande HTTP POST. Transmettez l'identificateur d'authentification utilisateur que vous avez obtenu à l'étape a avec le message de demande, conformément à l'exemple suivant :

```
POST https://localhost:<port>/SKLM/rest/v1/ckms/servermanagement/restartServer
Content-Type: application/json
Accept: application/json
Authorization: SKLMAuth userAuthId=139aeh34567m
```

Que faire ensuite

Déterminez si IBM Security Key Lifecycle Manager est en cours d'exécution. Par exemple, ouvrez IBM Security Key Lifecycle Manager dans un navigateur Web et connectez-vous.

Activation de la sécurité globale

Certaines conditions peuvent vous obliger à activer la sécurité globale.

Pourquoi et quand exécuter cette tâche

Ne désactivez pas la sécurité globale lorsque vous utilisez IBM Security Key Lifecycle Manager.

Procédure

1. Pour activer la sécurité globale, connectez-vous en tant qu'administrateur de WebSphere Application Server, avec l'ID WASAdmin.
2. Dans la barre de navigation, cliquez sur **Sécurité** > **Sécurité globale**.
3. Cochez la case **Activer la sécurité administrative**.

   Vérifiez que l'option **Activer la sécurité des applications** est également sélectionnée et que l'option **Utiliser la sécurité Java 2 pour limiter l'accès aux applications par les ressources locales** ne l'est *pas*.
4. Cliquez sur **Appliquer**.

5. Cliquez sur **Sauvegarder** dans la boîte de message.
6. Cliquez sur **Déconnexion**.
7. Arrêtez et redémarrez le serveur.
8. Rechargez la page de connexion à IBM Security Key Lifecycle Manager. Vérifiez que la page exige à présent un mot de passe.

Désactivation de la sécurité globale

Certaines conditions peuvent vous obliger à désactiver la sécurité globale.

Pourquoi et quand exécuter cette tâche

Ne désactivez pas la sécurité globale lorsque vous utilisez IBM Security Key Lifecycle Manager.

Procédure

1. Pour désactiver la sécurité globale, connectez-vous en tant qu'administrateur de WebSphere Application Server, avec l'ID WASAdmin.
2. Dans la barre de navigation, cliquez sur **Sécurité** > **Sécurité globale**.
3. Décochez la case **Activer la sécurité administrative**.
4. Cliquez sur **Appliquer**.
5. Cliquez sur **Sauvegarder** dans la boîte de message.
6. Cliquez sur **Déconnexion**.
7. Arrêtez et redémarrez le serveur.
8. Rechargez la page de connexion à IBM Security Key Lifecycle Manager. Vérifiez que la page ne demande *pas* de mot de passe.

Utilisation du module matériel de sécurité dans IBM Security Key Lifecycle Manager

Vous devez ajouter les paramètres au fichier de configuration d'IBM Security Key Lifecycle Manager pour définir un module matériel de sécurité (HSM).

Vous pouvez utiliser le module HSM pour stocker la clé principale qui permet de protéger tous les mots de passe contenus dans la base de données IBM Security Key Lifecycle Manager. Vous pouvez activer cette fonction pour les nouvelles installations d'IBM Security Key Lifecycle Manager.

IBM Security Key Lifecycle Manager prend en charge les cartes cryptographiques suivantes :

- `SafeNet Luna SA 4.5`
- `SafeNet Luna SA 5.0`
- `SafeNet Luna SA 6.1`
- `nCipher nShield Connect 1500`
- `IBM 4765 PCIe Cryptographic Coprocessor`

Remarque :

- Vous pouvez utiliser les cartes `SafeNe Luna SA 4.5`, `SafeNet Luna SA 5.0`, `SafeNet Luna SA 6.1` et `IBM 4765 PCIe Cryptographic Coprocessor` uniquement lorsque le magasin de clés n'est pas défini dans IBM Security Key Lifecycle Manager. Ces cartes ne permettent pas d'importer des clés de l'extérieur.

- IBM 4765 PCIe Cryptographic Coprocessor est pris en charge seulement pour les opérations de chiffrement PKCS#11 suivantes :
  - Convertir une clé logicielle AES 128 bits ou 256 bits en clé matérielle AES (PKCS#11)
  - Générer une clé AES 128 bits ou 256 bits
  - Chiffrer et déchiffrer des données à l'aide d'une clé AES et d'un chiffrement AES/ECB/NoPadding
  - Stocker et récupérer une clé AES vers/depuis un magasin de clés PKCS11IMPLKS (PKCS#11)

Vous pouvez utiliser les paramètres de configurations suivantes pour définir HSM :

- **pkcs11.pin**
- **pkcs11.config**
- **useMasterKeyInHSM**

Pour plus de détails sur les paramètres de configuration HSM, consultez les rubriques Référence dans la documentation IBM Security Key Lifecycle Manager.

Exemple de fichiers de configuration HSM

Exemple de fichier de configuration HSM pour SafeNet Luna SA 4.5, 5.0 et 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
}
```

Remarque : Pour le paramètre **name**, vous devez toujours indiquer la valeur TKLM.

Exemple de fichier de configuration HSM pour 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
}
```

Remarque : Pour le paramètre **name**, vous devez toujours indiquer la valeur TKLM.

Configuration de paramètres HSM

Vous devez utiliser les paramètres de configuration **pkcs11.pin**, **pkcs11.config** et **useMasterKeyinHSM** pour définir module matériel de sécurité.

Procédure

1. Définissez et configurez le module HSM en suivant les instructions des fabricants de module HSM.
2. Ajoutez les paramètres **pkcs11.pin**, **pkcs11.config** et **useMasterKeyinHSM** au fichier de configuration IBM Security Key Lifecycle Manager. Vous pouvez utiliser la commande CLI ou l'interface REST suivante pour ajouter le paramètre :

   Interface de ligne de commande

   ```
   print AdminTask.tklmConfigUpdateEntry('[-name pkcs11.pin -value
   <pin_hsm>]')

   print AdminTask.tklmConfigUpdateEntry('[-name pkcs11.config -value
   <fichier_config_hsm>]')

   print AdminTask.tklmConfigUpdateEntry('[-name useMasterKeyinHSM -value
   <true | false>]')
   ```

   Interface REST

   ```
   PUT https://localhost:<port>/SKLM/rest/v1/configProperties
   Content-Type: application/json
   Accept : application/json
   Authorization: SKLMAuth authId=139aeh34567m
   Accept-Language: en
   { "pkcs11.pin" : "<pin_hsm>"}

   PUT https://localhost:<port>/SKLM/rest/v1/configProperties
   Content-Type: application/json
   Accept : application/json
   ```

```
Authorization: SKLMAuth authId=139aeh34567m
Accept-Language: en
{ "pkcs11.config" : "<fichier_config_hsm>"}
PUT https://localhost:<port>/SKLM/rest/v1/configProperties
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth authId=139aeh34567m
Accept-Language: en
{ "useMasterKeyinHSM" : "<true | false>"}
```

Remarque : *<hsm pin>* est le code confidentiel PIN du module HSM. *<fichier_config_hsm>* est le chemin d'accès complet et le nom du fichier de configuration HSM. Par exemple : `C:\Program Files\IBM\WebSphere\AppServer\sklm\config\LunaSA.cfg`.

3. Redémarrez IBM Security Key Lifecycle Manager.

Configuration requise pour l'utilisation d'un module HSM

Vous devez valider l'installation du module HSM à l'aide des outils fournis par le client HSM après l'installation du module selon les instructions des fabricants. IBM Security Key Lifecycle Manager prend en charge le client HSM 64 bits.

- Pour valider l'installation du module HSM, procédez comme suit :
  - Créez une clé symétrique avec **ckdemo** ou **kSafe**.

    kSafe est un outil fourni avec la carte `nCipher nShield Connect 1500`. **ckdemo** est fourni avec les cartes `SafeNet Luna SA 4.5`, `SafeNet Luna SA 5.0` et `SafeNet Luna SA 6.1`.
  - Répertoriez la clé.
  - Supprimez la clé.
- La carte `nCipher nShield Connect 1500` nécessite que le fichier `cknfastrc` contienne la configuration suivante :

  ```
  CKNFAST_OVERRIDE_SECURITY_ASSURANCES=import;
  ```

  Remarque : Si le fichier `cknfastrc` n'existe pas sur le système, créez-le et configurez-le. Enregistrez ce fichier dans l'emplacement indiqué dans la documentation HSM.
- La sauvegarde ou la réplication d'IBM Security Key Lifecycle Manager n'enregistre pas la clé principale lorsqu'elle est placée dans le module HSM. Pour enregistrer le module HSM, suivez les instructions contenues dans la documentation HSM. Vous devez sauvegarder le module HSM car la perte de la clé principale risque d'entraîner la perte de toutes les clés dans IBM Security Key Lifecycle Manager.
- Utilisez les cartes `SafeNet Luna SA 4.5`, `SafeNet Luna SA 5.0` et `SafeNet Luna SA 6.1` uniquement si le magasin de clés n'est pas défini dans IBM Security Key Lifecycle Manager. Ces cartes ne permettent pas d'importer des clés de l'extérieur.
- Pour cloner IBM Security Key Lifecycle Manager, le module HSM contenu sur les différents systèmes doit utiliser la même clé principale. Si vous utilisez un module HSM connecté au réseau, assurez-vous que tous les clients du module HSM pointent sur la même zone du réseau HSM.

Configuration LDAP

Vous pouvez configurer des utilisateurs IBM Security Key Lifecycle Manager dans n'importe quel référentiel LDAP, par exemple IBM Security Directory Server ou Microsoft Active Directory, pour l'accès au serveur IBM Security Key Lifecycle Manager.

Vous devez ajouter et configurer un référentiel d'utilisateurs LDAP pour le référentiel fédéré de WebSphere Application Server. IBM Security Key Lifecycle Manager utilise des groupes d'applications afin d'imposer l'autorisation par rôle pour les fonctions IBM Security Key Lifecycle Manager. Pour qu'un utilisateur IBM Security Key Lifecycle Manager puisse exécuter des fonctions IBM Security Key Lifecycle Manager dans un référentiel d'utilisateurs LDAP, il doit être membre d'un groupe d'applications IBM Security Key Lifecycle Manager spécifique.

Lorsque vous installez IBM Security Key Lifecycle Manager, les groupes d'applications et les utilisateurs sont créés dans un référentiel de type fichier par défaut dans le référentiel fédéré de WebSphere Application Server. Lorsqu'un référentiel d'utilisateurs LDAP est ajouté au référentiel fédéré de WebSphere Application Server, vous devez définir l'utilisateur LDAP comme membre des groupes d'applications IBM Security Key Lifecycle Manager. Vous ne pouvez pas définir des utilisateurs LDAP comme membres des groupes présents dans le référentiel de type fichier par défaut.

L'appartenance à un groupe de référentiels n'est pas possible entre un référentiel de type fichier et un référentiel LDAP. En revanche, l'appartenance entre plusieurs groupes de référentiels est possible entre un référentiel LDAP et un référentiel de type base de données. Par conséquent, créez un référentiel de type base de données et créez tous les groupes d'applications IBM Security Key Lifecycle Manager dans ce référentiel. Les groupes d'applications qui existaient dans le référentiel de type fichier sont retirés.

Lorsque le référentiel reposant sur une base de données est créé et que des groupes d'applications IBM Security Key Lifecycle Manager sont ajoutés à ce référentiel, l'utilisateur d'un référentiel LDAP peut devenir membre des groupes d'applications IBM Security Key Lifecycle Manager dans le référentiel reposant sur une base de données. Les utilisateurs peuvent ensuite se connecter à l'application IBM Security Key Lifecycle Manager et exécuter les fonctions correspondantes.

Pour intégrer LDAP à IBM Security Key Lifecycle Manager, vous pouvez utiliser l'une des méthodes de configuration suivantes :

- A l'aide de WebSphere Integrated Solutions Console. Pour plus d'informations, voir Intégration de LDAP à l'aide de WebSphere Integrated Solutions Console.
- En exécutant les scripts de configuration LDAP. Pour plus d'informations, voir Exécution des scripts de configuration LDAP.

Intégration de LDAP à l'aide de WebSphere Integrated Solutions Console

Avant d'intégrer LDAP à IBM Security Key Lifecycle Manager à l'aide de WebSphere Integrated Solutions Console, vous devez exécuter les tâches de sauvegarde.

Prérequis pour l'intégration LDAP

Vous devrez peut-être restaurer les données suivantes telles qu'elles existaient avant la configuration de LDAP :

- Données de configuration de WebSphere Application Server pour IBM Security Key Lifecycle Manager
- Données d'application IBM Security Key Lifecycle Manager

Exécutez les étapes suivantes pour sauvegarder les données.

1. Sauvegardez le profil IBM Security Key Lifecycle Manager (KLMProfile) dansWebSphere Application Server :
   a. Dans le répertoire WAS_HOME/bin, arrêtez l'application WebSphere Application Server.
   b. Exécutez la commande suivante.

      Windows

      ```
      <WAS_HOME>\bin\manageProfiles.bat -backupProfile -profileName
      KLMProfile -backupFile <chemin d'accès à un fichier>
      ```

      ```
      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 <chemin d'accès à un fichier>
      ```

      ```
      /opt/IBM/WebSphere/AppServer/bin/manageprofiles.sh -backupProfile
      profileName KLMProfile -backupFile /root/SKLM_WAS_ProfileBackup
      ```

   c. Démarrez WebSphere Application Server.
2. Sauvegardez les données d'application IBM Security Key Lifecycle Manager

   Utilisez l'interface graphique, l'interface de ligne de commande ou l'interface REST pour sauvegarder les fichiers critiques d'IBM Security Key Lifecycle Manager.

Pour plus d'informations sur la commande **manageprofiles**, voir http://www.ibm.com/support/knowledgecenter/SSEQTP_9.0.0/com.ibm.websphere.base.doc/ae/rxml_manageprofiles.html.

Intégration de LDAP à l'aide de WebSphere Integrated Solutions Console

Vous pouvez configurer les utilisateurs IBM Security Key Lifecycle Manager dans n'importe quel annuaire LDAP, tels qu'IBM Security Directory Server ou Microsoft Active Directory, pour accéder au serveur IBM Security Key Lifecycle Manager et appeler les API et les CLI de serveur.

Avant de commencer

Pour plus d'informations sur les prérequis, voir «Configuration LDAP», à la page 217.

Procédure

1. Ajoutez un référentiel LDAP au référentiel fédéré. Pour obtenir les instructions correspondantes, voir «Ajout d'un référentiel LDAP au référentiel fédéré», à la page 219.
2. Créez la base de données pour la configuration LDAP.
   a. Ouvrez la fenêtre de commande Db2.

b. Exécutez la commande suivante pour créer la base de données :

```
db2  create database USERDB31 using codeset UTF-8 territory US
```

3. Mettez à jour la source de données à partir de WebSphere Integrated Solutions Console à l'aide du nom `jndi jdbc/wimXADS`. Pour obtenir les instructions correspondantes, voir «Mise à jour d'une source de données depuis WebSphere Integrated Solutions Console», à la page 221.
4. Redémarrez WebSphere Application Server.
5. Copiez `db2jcc.jar` et `db2jcc_license_cu.jar` du dossier `DB2SKLMV301` dans le dossier *WAS_HOME*`/lib`.

   Chemin de `DB2SKLMV301` :

   Windows
   drive`:\Program Files\IBM\DB2SKLMV301\java`

   Linux *path*`/IBM/DB2SKLMV301/java`

   La valeur définition par défaut de la variable *WAS_HOME* se présente généralement comme suit :

   Windows
   `C:\Program Files\IBM\WebSphere\AppServer`

   Linux `/opt/IBM/WebSphere/AppServer`
6. Créez un référentiel de type base de données afin de stocker tous les groupes d'applications IBM Security Key Lifecycle Manager. Pour obtenir les instructions correspondantes, voir «Création d'un référentiel de type base de données», à la page 221.
7. A partir de WebSphere Integrated Solutions Console, ajoutez un rôle de sécurité au mappage utilisateur/groupe et mappez le rôle administrateur à `klmGUICLIAccessGroup`. Pour obtenir les instructions correspondantes, voir «Ajout de rôles de sécurité à un utilisateur à partir de WebSphere Integrated Solutions Console», à la page 222.
8. Redémarrez WebSphere Application Server.
9. Ajoutez des utilisateurs LDAP aux groupes d'applications IBM Security Key Lifecycle Manager. Pour obtenir les instructions correspondantes, voir «Ajout d'utilisateurs LDAP aux groupes d'applications IBM Security Key Lifecycle Manager», à la page 223
10. Effectuez la sauvegarde de l'application IBM Security Key Lifecycle Manager. Les données du référentiel de type base de données sont également sauvegardées.

Que faire ensuite

Une fois LDAP configuré, vous devez exécuter les tâches suivantes. Pour plus d'informations, voir «Tâches à effectuer après la configuration de LDAP pour permettre la prise en charge de l'intégration LDAP», à la page 227

Ajout d'un référentiel LDAP au référentiel fédéré :

Vous devez ajouter un référentiel LDAP au référentiel fédéré pour configurer un référentiel LDAP, tel qu'IBM Security Directory Server ou Microsoft Active Directory, dans le référentiel fédéré.

Pourquoi et quand exécuter cette tâche

Pour plus d'informations sur la configuration des paramètres LDAP dans une configuration de référentiel fédéré, voir http://www-01.ibm.com/support/knowledgecenter/api/redirect/wasinfo/v8r5/topic/com.ibm.websphere.base.doc/ae/twim_ldap_settings.html.

Procédure

1. Connectez-vous à WebSphere Integrated Solutions Console (`https://localhost:9093/ibm/console/logon.jsp`) en tant qu'utilisateur `wasadmin`.
2. Dans la barre de navigation, cliquez sur **Sécurité** > **Sécurité globale**.
3. Sous Référentiel de comptes utilisateur, sélectionnez **Référentiels fédérés** dans la liste déroulante **Définitions de superdomaines disponibles**.
4. Cliquez sur **Configurer**.
5. Sur la page **Sécurité globale** > **Référentiels fédérés**, cliquez sur **Ajouter des référentiels (LDAP, personnalisé, etc...)**.
6. Sur la page **Sécurité globale** > **Référentiels fédérés** > **Référence du référentiel**, sélectionnez **Référentiel LDAP** dans la liste déroulante **Nouveau référentiel**.
7. Sur la page **Sécurité globale** > **Référentiels fédérés** > **Référence du référentiel** > **Nouveau**, spécifiez le nom du référentiel LDAP et d'autres informations en fonction de vos besoins.
8. Cliquez sur **OK**.
9. Cliquez sur **Enregistrer** pour enregistrer la configuration.
10. Sur la page **Sécurité globale** > **Référentiels fédérés** > **Référence du référentiel**, spécifiez une valeur pour **Nom distinctif unique de l'entrée de base (ou parent) dans les référentiels fédérés**.
11. Cliquez sur **OK**.
12. Sur la page **Sécurité globale** > **Référentiels fédérés**, sélectionnez le lien vers le référentiel LDAP que vous avez créé.
13. Sur la page **Sécurité globale** > **Référentiels fédérés** > **<Nom du référentiel LDAP>**, sous Propriétés supplémentaires, sélectionnez le lien Mappage entre types d'entité des référentiels fédérés et classes d'objet LDAP.

    Sur la page **Sécurité globale** > **Référentiels fédérés** > **<Nom du référentiel LDAP>** > **Mappage entre types d'entité des référentiels fédérés et classes d'objet LDAP**, vérifiez que chaque type d'entité répertorié est mappé aux classes d'objet appropriées. Modifiez les valeurs en fonction de vos besoins.
14. Sur la page **Sécurité globale** > **Référentiels fédérés**, sélectionnez le lien vers le référentiel LDAP que vous avez créé. Sous Propriétés supplémentaires, sélectionnez **Définition des attributs de groupe**.
15. Sur la page **Sécurité globale** > **Référentiels fédérés** > **<Nom du référentiel LDAP>** > **Définition des attributs de groupe**, sous Propriétés supplémentaires, sélectionnez **Attributs des membres**.
16. Sur la page **Sécurité globale** > **Référentiels fédérés** > **<Nom du référentiel LDAP>** > **Définition des attributs de groupe** > **Attributs des membres**, vérifiez que l'attribut de membre `uniqueMember` est mappé à la classe d'objet appropriée. Si cet attribut est manquant, créez un attribut et mappez-le à la classe d'objet appropriée.

Que faire ensuite

Créez une source de données à partir de WebSphere Integrated Solutions Console.

Mise à jour d'une source de données depuis WebSphere Integrated Solutions Console :

Vous devez mettre à jour la source de données pour le référentiel de type base de données pour le stockage des groupes d'applications d'IBM Security Key Lifecycle Manager. Le référentiel de type base de données utilise les tables qui sont créées dans la base de données de l'application IBM Security Key Lifecycle Manager.

Procédure

1. Connectez-vous pour créer la source de données depuis WebSphere Integrated Solutions Console (`https://localhost:9093/ibm/console/logon.jsp`) en tant qu'utilisateur `wasadmin`.
2. Dans la barre de navigation, cliquez sur **Ressources** > **JDBC** > **Sources de données**.
3. Cliquez sur **Source de données WIM** pour éditer les valeurs de base de données.
4. Mettez à jour le nom de base de données `USERDB31` dans la section **Propriétés communes et obligatoires des sources de données**.
5. Cliquez sur **OK**.
6. Cliquez sur **Sauvegarder** pour enregistrer la configuration.

Création d'un référentiel de type base de données :

Créez un référentiel de type base de données afin de stocker tous les groupes d'applications IBM Security Key Lifecycle Manager et de retirer tous les groupes d'applications IBM Security Key Lifecycle Manager d'un référentiel de type fichier. Vous devez ajouter les groupes d'applications IBM Security Key Lifecycle Manager à un référentiel de type base de données et mettre à jour le référentiel fédéré de WebSphere Application Server avec le référentiel LDAP.

Procédure

1. Accédez au dossier <*SKLM_INSTALL_HOME*>\bin.

   Remarque : Tous les scripts Python `.py` sont présents dans le répertoire <*SKLM_INSTALL_HOME*>\bin\LDAPIntegration.
   Le chemin <*SKLM_INSTALL_HOME*> est généralement le suivant :

   Windows
   `C:\Program Files\IBM\SKLMV301`

   Linux `opt/IBM/SKLMV301`
2. Exécutez les commandes suivantes :

   ```
   wsadmin.bat -user wasadmin user -password wasadmin passwd -lang jython -f
   SKLM_INSTALL_HOME\bin\LDAPIntegration\createDBRepos.py WAS_HOME LDAP_DBNAME
   SKLM_DBUSER SKLM_DBUSERPASSWD SKLM_DBPORT#
   ```

   Remarques : Sur les plateformes Linux, utilisez **`wsadmin.sh`** au lieu de **`wsadmin.bat`**

   Lors de l'installation d'IBM Security Key Lifecycle Manager, si vous utilisez les paramètres par défaut,

```
LDAP_DBNAME = USERDB31
SKLM_DBUSER = SKLMDB31
SKLM_DBPORT# = 50050
```

SKLM_DBUSERPASSWD correspond au mot de passe de la base de données d'IBM Security Key Lifecycle Manager que vous avez spécifié lors de l'installation.

3. Exécutez la commande suivante.

   ```
   wsadmin.bat -user <wasadmin user> -password <wasadmin passwd> -lang jython -f
   <SKLM_INSTALL_HOME>\bin\LDAPIntegration\removeGroupsFromDefRepos.py
   ```

4. A partir de WebSphere Integrated Solutions Console, modifiez la valeur de Mappage d'un rôle de sécurité à un utilisateur/groupe pour retirer le mappage de rôle d'administrateur à klmGUICLIAccessGroup.
   a. Connectez-vous à WebSphere Integrated Solutions Console (https://localhost:9093/ibm/console/logon.jsp).
   b. Dans la barre de navigation, cliquez sur **Applications** > **Types d'application** > **Types d'application** > **Applications d'entreprise WebSphere**.
   c. Cliquez sur le lien **sklm_kms**.
   d. Sur la page **Applications d'entreprise** > **sklm_kms**, sous la section Propriétés du détail, cliquez sur le lien **Mappage d'un rôle de sécurité à des utilisateurs ou des groupes**.
   e. Sur la page **Applications d'entreprise** > **sklm_kms** > **Mappage d'un rôle de sécurité à des utilisateurs ou des groupes**, sélectionnez le rôle **administrateur**.
   f. Cliquez sur **Mapper des groupes**.
   g. Sélectionnez **klmGUICLIAccessGroup** dans la liste, puis cliquez sur le bouton représentant une flèche vers la gauche pour retirer **klmGUICLIAccessGroup** de la liste.
   h. Cliquez sur **OK**.
   i. Cliquez sur **Enregistrer** pour enregistrer la configuration.
5. Redémarrez WebSphere Application Server
6. Exécutez la commande suivante.

   ```
   wsadmin.bat -user <wasadmin user> -password <wasadmin passwd> -lang jython
   -f <SKLM_INSTALL_HOME>\bin\LDAPIntegration\addGroupsToDBRepos.py
   ```

7. Exécutez la commande suivante.

   ```
   wsadmin.bat -user <wasadmin user> -password <wasadmin passwd> -lang jython
   -f <SKLM_INSTALL_HOME>\bin\LDAPIntegration\updateLDAPReposConfig.py <LDAPRepos Name
   - name used earlier when LDAP repos was created>
   ```

Que faire ensuite

Ajoutez un rôle de sécurité au mappage utilisateur/groupe et mappez un rôle d'administrateur à klmGUICLIAccessGroup.

Ajout de rôles de sécurité à un utilisateur à partir de WebSphere Integrated Solutions Console :

Vous devez ajouter un mappage de rôle de sécurité à des utilisateurs ou des groupes et mapper un rôle d'administrateur à klmGUICLIAccessGroup pour l'intégration d'IBM Security Key Lifecycle Manager aux référentiels d'utilisateurs LDAP.

Pourquoi et quand exécuter cette tâche

Procédure

1. Connectez-vous à WebSphere Integrated Solutions Console (`https://localhost:9083/ibm/console/logon.jsp`) en tant qu'utilisateur `wasadmin`.
2. Dans la barre de navigation, cliquez sur **Applications** > **Types d'application** > **Types d'application** > **Applications d'entreprise WebSphere**.
3. Cliquez sur le lien **sklm_kms**.
4. Sur la page **Applications d'entreprise** > **sklm_kms**, sous la section Propriétés du détail, cliquez sur le lien **Mappage d'un rôle de sécurité à des utilisateurs ou des groupes**.
5. Sur la page **Applications d'entreprise** > **sklm_kms** > **Mappage d'un rôle de sécurité à des utilisateurs ou des groupes**, sélectionnez le rôle **administrateur**.
6. Cliquez sur **Mapper des groupes**.
7. Sur la page **Applications d'entreprise** > **sklm_kms** > **Mappage d'un rôle de sécurité à des utilisateurs ou des groupes** > **Mappage des utilisateurs/groupes** :
   a. Sous la section Rechercher et sélectionner des groupes, dans la zone de texte **Chaîne de recherche**, entrez `klmGUICLIAccessGroup`.
   b. Cliquez sur **Rechercher**.
   c. Sélectionnez `klmGUICLIAccessGroup` dans la liste, puis cliquez sur le bouton représentant une flèche vers la droite.

      `klmGUICLIAccessGroup` est ajouté à la liste **Sélectionné(e)**.
   d. Cliquez sur **OK**.
   e. Cliquez sur **OK** sur la page **Applications d'entreprise** > **sklm_kms** > **Mappage d'un rôle de sécurité à des utilisateurs ou des groupes**.
8. Cliquez sur le lien **Enregistrer** pour enregistrer les informations de configuration.

Que faire ensuite

Redémarrez WebSphere Application Server.

Ajout d'utilisateurs LDAP aux groupes d'applications IBM Security Key Lifecycle Manager :

Vous devez ajouter des utilisateurs LDAP aux groupes d'applications IBM Security Key Lifecycle Manager afin d'intégrer IBM Security Key Lifecycle Manager à des référentiels d'utilisateurs LDAP.

Procédure

1. Accédez au dossier <*SKLM_INSTALL_HOME*>/bin.

   Remarque : Tous les scripts Python `.py` sont présents dans le répertoire <*SKLM_INSTALL_HOME*>/bin/LDAPIntegration.
   Le chemin <*SKLM_INSTALL_HOME*> est généralement le suivant :

   Windows
   `C:\Program Files\IBM\SKLMV301`

   Linux `/opt/IBM/SKLMV301`
2. Exécutez les commandes suivantes :

```
wsadmin.bat -user <wasadmin user> -password <wasadmin passwd> -lang jython -f
addLDAPUserToGroup.py <nom unique utilisateur> <nom groupe>
```

Remarques : Sur les plateformes Linux, utilisez **wsadmin.sh** au lieu de **wsadmin.bat**

Le nom unique d'utilisateur correspond au composant Nom unique dans le registre LDAP. Par exemple :

```
uid=001,c=in,ou=bluepages,o=ibm.com
```

Un utilisateur LDAP qui a besoin de disposer d'un accès administrateur à IBM Security Key Lifecycle Manager doit être défini en tant que membre de klmGUICLIAccessGroup et klmSecurityOfficerGroup. Exécutez la commande suivante :

```
wsadmin.bat -user <wasadmin user> -password <wasadmin passwd> -lang jython -f
<SKLM_INSTALL_HOME>\bin\LDAPIntegration\addLDAPUserToGroup.py
<user uniqueName> klmGUICLIAccessGroup
```

Que faire ensuite

Effectuez la sauvegarde de l'application IBM Security Key Lifecycle Manager.

Exécution des scripts de configuration LDAP

Exécutez les scripts de configuration LDAP pour intégrer facilement IBM Security Key Lifecycle Manager à LDAP afin de configurer les utilisateurs d'IBM Security Key Lifecycle Manager dans tous les référentiels LDAP, comme IBM Security Directory Server ou Microsoft Active Directory.

Pourquoi et quand exécuter cette tâche

Procédure

1. Dans les propriétés config.py, mettez à jour **ip**, **port**, **LDAP_server_type** et d'autres propriétés de votre environnement. Pour la description des propriétés dans le fichier config.py, voir Intégration de LDAP à l'aide de scripts de configuration.

   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

   Remarque : Pour exécuter les scripts avec la configuration par défaut, il suffit de définir les propriétés **ip** et **port**.
2. Créez la base de données pour la configuration LDAP.
   a. Ouvrez la fenêtre de commande Db2.
   b. Exécutez la commande suivante pour créer la base de données :
      ```
      db2  create database USERDB31 using codeset UTF-8 territory US
      ```
3. Mettez à jour la source de données à partir de WebSphere Integrated Solutions Console à l'aide du nom jndi jdbc/wimXADS. Pour obtenir les instructions correspondantes, voir «Mise à jour d'une source de données depuis WebSphere Integrated Solutions Console», à la page 221.
4. Créez un référentiel de type base de données afin de stocker tous les groupes d'applications IBM Security Key Lifecycle Manager.

a. Accédez au dossier <*WAS_HOME*>\bin.

Windows
C:\Program Files\IBM\WebSphere\AppServer\bin

Linux /opt/IBM/WebSphere/AppServer/bin

b. Ouvrez une invite de commande et exécutez les commandes suivantes.

```
wsadmin.bat -user <wasadmin user> -password <wasadmin passwd> -lang jython -f
<SKLM_INSTALL_HOME>\bin\LDAPIntegration\createDBRepos.py <WAS_HOME> <LDAP_DBNAME>
<SKLM_DBUSER> <SKLM_DBUSERPASSWD> <SKLM_DBPORT#>
```

Remarques : Sur les plateformes Linux, utilisez **wsadmin.sh** au lieu de **wsadmin.bat**

Lors de l'installation d'IBM Security Key Lifecycle Manager, si vous utilisez les paramètres par défaut,

```
LDAP_DBNAME = USERDB31
SKLM_DBUSER = sklmdb31
SKLM_DBPORT# = 50050
```

SKLM_DBUSERPASSWD correspond au mot de passe de la base de données d'IBM Security Key Lifecycle Manager que vous avez spécifié lors de l'installation.

5. Exécuter les scripts de configuration sklmLDAPConfigure et addLDAPUserToGroup.

Windows
Accédez au répertoire *SKLM_INSTALL_HOME*\bin\LDAPIntegration et exécutez les scripts suivants :

```
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_
```

Par exemple :

```
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 Accédez au répertoire *SKLM_INSTALL_HOME*/bin/LDAPIntegration et exécutez les scripts suivants :

```
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
```

Par exemple :

```
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
Répertoire dans lequel WebSphere Application Server pour IBM Security Key Lifecycle Manager est installé.

Windows
unité:\Program Files\IBM\WebSphere\AppServer

Linux chemin/IBM/WebSphere/AppServer

SKLM_INSTALL_HOME
Répertoire dans lequel IBM Security Key Lifecycle Manager est installé.

Windows
drive:\Program Files\IBM\SKLMV301

Linux

ADMIN_WAS
Nom d'utilisateur de WebSphere Application Server pour IBM Security Key Lifecycle Manager.

MDP_WAS
Mot de passe de WebSphere Application Server pour IBM Security Key Lifecycle Manager.

USER_UNIQUE_NAME
Utilisateur LDAP auquel vous souhaitez attribuer le rôle d'administrateur IBM Security Key Lifecycle Manager.

ADMIN_SKLM
Administrateur d'IBM Security Key Lifecycle Manager.

MDP_ADMIN_SKLM
Mot de passe de l'administrateur d'IBM Security Key Lifecycle Manager.

rép_install_Db2
Le répertoire dans lequel Db2 est installé.

Windows
drive:\Program Files\IBM\DB2SKLMV301

Linux *path*/IBM/DB2SKLMV301

Pour les installations non root sous Linux, le chemin d'accès est le suivant : *<non_root_user_home _directory>*/IBM/DB2SKLMV301

Que faire ensuite

Une fois LDAP configuré, vous devez exécuter les tâches suivantes. Pour plus d'informations, voir «Tâches à effectuer après la configuration de LDAP pour permettre la prise en charge de l'intégration LDAP», à la page 227

Intégration de LDAP à l'aide de scripts de configuration

Vous pouvez exécuter les scripts de configuration à partir d'une ligne de commande pour intégrer IBM Security Key Lifecycle Manager à LDAP en utilisant les paramètres de configuration par défaut définis dans le fichier de propriétés `config.py`.

L'exemple suivant montre les propriétés définies dans le fichier `config.py`.

```
import string, 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"
```

Le tableau suivant décrit les propriétés du fichier `config.py`.

Propriété	Description
LDAP_server_type	Type du serveur LDAP utilisé. Par défaut, IDS est spécifié.

Propriété	Description
login_id	Nom de propriété utilisé pour la connexion. Par exemple, `uid` et `mail`.
ip	Adresse IP ou nom d'hôte du serveur LDAP principal.
port	Numéro de port du serveur LDAP.
gr_name	Nom du type d'entité.
pr_name	Nom du type d'entité.
gr_obj_class	Classe d'objet du type d'entité.
pr_obj_class	Classe d'objet du type d'entité.
mem_name	Nom de l'attribut LDAP utilisé comme attribut de membre du groupe. Par exemple, `member` ou `uniqueMember`.
mem_obj_class	Classe d'objet de groupe qui contient l'attribut membre. Par exemple, `groupOfNames` ou `groupOfUniqueNames`. Si vous ne définissez pas ce paramètre, l'attribut de membre s'applique à toutes les classes d'objets de groupe.
scope	Portée de l'attribut de membre. Spécifiez l'une des valeurs suivantes pour le paramètre. **direct** Attribut de membre qui ne contient que les membres directs. Par conséquent, cette valeur se réfère aux membres directement contenus par le groupe et non contenus par le groupe imbriqué. Si, par exemple, `Group1` contient `Group2` et `Group2` contient `User1`, alors `Group2` est un membre direct de `Group1` mais `User1` n'est pas un membre direct de `Group1`. `member` et `uniqueMember` sont tous deux des attributs de membre direct. **nested** Attribut de membre qui contient les membres directs et les membres imbriqués.

Si vous découvrez des problèmes lors de l'intégration LDAP lorsque les scripts sont utilisés pour exécuter la tâche de configuration, vous devrez peut-être consulter les fichiers journaux suivants qui se trouvent dans *<SKLM_INSTALL_HOME>*`/bin/LDAPIntegration` pour diagnostiquer les problèmes.

- `sklmldapconf.log`
- `ldaplog.out`

Pour plus d'informations sur l'exécution des scripts de configuration, voir Exécution des scripts de configuration LDAP.

Tâches à effectuer après la configuration de LDAP pour permettre la prise en charge de l'intégration LDAP

Après la configuration de LDAP, vous devrez peut-être effectuer d'autres tâches pour que l'intégration d'IBM Security Key Lifecycle Manager aux référentiels d'utilisateurs LDAP aboutisse.

Remarques importantes sur les tâches à effectuer après la configuration de LDAP

1. Après la configuration de LDAP, l'utilisateur `sklmadmin` qui figurait dans le référentiel d'utilisateurs à base de fichier par défaut ne peut plus accéder à l'application IBM Security Key Lifecycle Manager.

2. Après la configuration de LDAP, vous devez utiliser des commandes **wsadmin** pour créer des groupes et affecter des rôles IBM Security Key Lifecycle Manager. Vous ne pouvez pas utiliser WebSphere Integrated Solutions Console. Exécutez les étapes suivantes pour ajouter un groupe et affecter un rôle à ce groupe :
   a. Accédez à *<WAS_HOME>*/bin.
   b. Connectez-vous à wsadmin à l'aide de la commande suivante :

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

   c. Pour créer un groupe et affecter le rôle, exécutez la commande suivante :

      ```
      AdminTask.createGroup<'[-cn <groupname> -parent "o=sklmrepdb.ibm"]'>
      AdminTask.mapGroupsToAdminRole<'[-roleName <rôle> -groupids
      <nom de groupe>]'>
      ```

3. Après la configuration de LDAP, vous devrez peut-être restaurer la configuration d'IBM Security Key Lifecycle Manager dans WebSphere Application Server telle qu'elle existait avant la configuration de LDAP. Pour restaurer la configuration, procédez comme suit :
   a. Arrêtez WebSphere Application Server.
   b. Arrêtez les éventuels processus liés à WebSphere Application Server.
   c. Restaurez la configuration de profil WebSphere Application Server effectuée avant la configuration de LDAP :
      1) Supprimez manuellement le dossier KLMProfile dans *<WAS_HOME>*/profiles/KLMProfile.
      2) Exécutez l'option **-validateAndUpdateRegistry** de la commande **manageProfiles**.

         Windows

         ```
         <WAS_HOME>\bin\manageProfiles.bat
         -validateAndUpdateRegistry
         ```

         Par exemple : C:\Program Files\IBM\WebSphere\AppServer\bin\manageProfiles.bat-validateAndUpdateRegistry

         Linux

         ```
         <WAS_HOME>/bin/manageprofiles.sh
         -validateAndUpdateRegistry
         ```

         Par exemple : /opt/IBM/WebSphere/AppServer/bin/manageprofiles.sh -validateAndUpdateRegistry

      3) Restaurez le profil :

         Windows

         ```
         <WAS_HOME>\bin\manageProfiles.bat -restoreProfile
         -backupFile <chemin d'accès à un fichier de sauvegarde de
         profil>
         ```

         Par exemple : C:\Program Files\IBM\WebSphere\AppServer\bin\manageProfiles.bat -restoreProfile -backupFile C:\SKLM_WAS_ProfileBackup

         Linux

         ```
         <WAS_HOME>/bin/manageprofiles.sh -restoreProfile
         -backupFile <chemin d'accès à un fichier de sauvegarde de
         profil>
         ```

         Par exemple : /opt/IBM/WebSphere/AppServer/bin/manageprofiles.sh -restoreProfile -backupFile /root/SKLM_WAS_ProfileBackup

Pour plus d'informations sur la commande **manageProfiles**, voir http://www.ibm.com/support/knowledgecenter/SSEQTP_9.0.0/com.ibm.websphere.base.doc/ae/rxml_manageprofiles.html.

4) Démarrez WebSphere Application Server.
5) Restaurez la sauvegarde d'IBM Security Key Lifecycle Manager effectuée avant la configuration de LDAP, si besoin est.

4. Vous ne devez pas restaurer la sauvegarde de l'application IBM Security Key Lifecycle Manager effectuée avant la configuration de LDAP une fois la configuration de LDAP terminée sauf si vous suivez l'étape 3 de la section **Remarques importantes sur les tâches à effectuer après la configuration de LDAP**.
5. Après la configuration de LDAP, les tables sont créées dans la base de données d'IBM Security Key Lifecycle Manager pour le référentiel de type base de données. Les groupes IBM Security Key Lifecycle Manager sont stockés dans ces tables. Si le serveur IBM Security Key Lifecycle Manager est configuré pour la réplication et si celle-ci se produit sur les clones configurés, les groupes présents dans le référentiel de type de base de données sont également répliqués sur le clone. Cela est dû au fait que les tables de base de données du référentiel de type base de données sont également répliquées sur les clones.
6. Si le serveur IBM Security Key Lifecycle Manager (maître) est configuré pour s'intégrer aux référentiels LDAP et si la réplication est activée, lorsque celle-ci se produit sur les clones LDAP où LDAP n'est pas configuré, vous pouvez configurer ou non LDAP sur les clones. Si la configuration de LDAP doit être effectuée sur le clone, exécutez les étapes suivantes sur celui-ci :
   a. Copiez les fichiers `db2jcc.jar`,`db2jcc4.jar` et `db2jcc_license_cu.jar` du dossier `DB2SKLMV301` dans le dossier `<WAS_HOME>/lib`.

      La valeur définition par défaut de la variable <*WAS_HOME*> se présente généralement comme suit :

      Windows
      `C:\Program Files\IBM\WebSphere\AppServer`

      Linux `/opt/IBM/WebSphere/AppServer`
   b. Accédez à `<WAS_HOME>/bin`.
      1) Connectez-vous à `wsadmin` à l'aide de la commande suivante :

         ```
         wsadmin.bat -user <WASADMIN_USER> -password <WASADMIN_PASSWORD>
         -lang jython
         ```
      2) Exécutez la commande suivante :

         ```
         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. Effectuez la même procédure de configuration de l'intégration LDAP que celle qui a été utilisée sur le serveur IBM Security Key Lifecycle Manager maître. Pour connaître les étapes de la procédure d'intégration, voir «Intégration de LDAP à l'aide de WebSphere Integrated Solutions Console», à la page 218.
7. Après la réplication entre un serveur IBM Security Key Lifecycle Manager qui est configuré pour l'intégration LDAP et un clone qui n'est pas configuré pour l'intégration LDAP, si par inadvertance vous exécutez la configuration de l'intégration LDAP normale sur le clone, l'étape 5 décrite à la section

«Intégration de LDAP à l'aide de WebSphere Integrated Solutions Console», à la page 218 échoue. Vous devez exécuter les étapes suivantes :

a. Accédez à *<WAS_HOME>*/bin.

   1) Connectez-vous à wsadmin :

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

   2) Exécutez la commande suivante :

      ```
      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. Exécutez les étapes 5 à 9 décrites à la section «Intégration de LDAP à l'aide de WebSphere Integrated Solutions Console», à la page 218.

Changement du mot de passe d'administrateur Db2 sur les serveurs configurés LDAP

Si une règle d'expiration de mot de passe est en vigueur, vous devez changer le mot de passe Db2 de l'ID utilisateur avant la fin de la période d'expiration.

Pourquoi et quand exécuter cette tâche

Si le serveur IBM Security Key Lifecycle Manager est configuré avec LDAP, vous devez procéder comme suit pour changer le mot de passe de l'administrateur Db2.

Procédure

1. Vérifiez que la case à cocher **Autoriser des opérations si certains référentiels sont arrêtés** est sélectionnée.
   a. Connectez-vous à WebSphere Integrated Solutions Console.
   b. Cliquez sur **Sécurité** > **Sécurité globale**.
   c. Dans **Référentiel de comptes utilisateur** > **Définitions de superdomaines disponibles**, sélectionnez **Référentiels fédérés** dans la liste déroulante.
   d. Cliquez sur **Configurer**.
   e. Sélectionnez la case à cocher **Autoriser des opérations si certains référentiels sont arrêtés**.
2. Exécutez les étapes décrites dans les rubriques suivantes pour changer le mot de passe de l'administrateur Db2.

   Windows
   Exécutez les étapes 3 à 5 de la rubrique «Problèmes liés à la sécurité des mots de passe Db2 sous Windows», à la page 37.

   Linux Exécutez les étapes 1 à 3 de la rubrique Problèmes liés à la sécurité des mots de passe Db2 sur les systèmes Linux ou AIX.
3. Mettez à jour les paramètres de référentiel fédéré pour la connexion à un référentiel de base de données. Changez également le mot de passe de l'administrateur Db2 en utilisant la commande **updateIdMgrDBRepository AdminTask**.
   a. A l'aide de l'interface **wsadmin** intégrée à WebSphere Application Server, entrez la syntaxe Jython suivante :

      Windows

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

Linux

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

b. Exécutez la commande, par exemple :

```
print AdminTask.updateIdMgrDBRepository ('[-id id_name -dbAdminPasswword new_password]')
```

où `id_name` est `SKLMDBRepos`

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

Pour plus d'informations, voir https://www.ibm.com/support/knowledgecenter/SSAW57_9.0.0/com.ibm.websphere.nd.multiplatform.doc/ae/rxml_atidmgrrepositoryconfig.html#rxml_atidmgrrepositoryconfig__cmd46.

4. Exécutez les étapes décrites dans les rubriques suivantes pour changer le mot de passe de la source de données WebSphere Application Server.

Windows
Exécutez les étapes 7 et 8 de la rubrique «Problèmes liés à la sécurité des mots de passe Db2 sous Windows», à la page 37.

Linux Exécutez les étapes 5 et 6 de la rubrique Problèmes liés à la sécurité des mots de passe Db2 sur les systèmes Linux ou AIX.

5. Redémarrez le serveur. Pour des instructions sur la façon d'arrêter et de démarrer le serveur, voir «Serveur IBM Security Key Lifecycle Manager - Redémarrage», à la page 211.

Configurations standard de sécurité

Vous configurez IBM Security Key Lifecycle Manager pour travailler avec différentes normes de sécurité afin de répondre aux exigences de sécurité spécifiées pour le chiffrement.

Configuration de la conformité FIPS dans IBM Security Key Lifecycle Manager

Vous pouvez activer FIPS pour IBM Security Key Lifecycle Manager de telle sorte que toutes les opérations de chiffrement utilisent le fournisseur `IBMJCEFIPS` qui est certifié FIPS 140-2.

Procédure

1. Définissez la propriété suivante dans le fichier *SKLM_HOME*`/config/SKLMConfig.properties`.

```
fips=on
```

Interface de ligne de commande

a. Accédez au répertoire <*WAS_HOME*>`/bin`. Par exemple,

Windows

```
cd unité:\Program Files (x86)\IBM\WebSphere\AppServer\bin
```

Linux

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

b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme `SKLMAdmin`. Par exemple,

Windows

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

Linux

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

c. Exécutez la commande **tklmConfigUpdateEntry** pour définir la propriété **fips** dans le fichier de configuration SKLMConfig.properties.

```
print AdminTask.tklmConfigUpdateEntry ('[-name fips -value on]')
```

Interface REST

a. Ouvrez un client REST.

b. Obtenez un identificateur d'authentification utilisateur unique pour accéder aux services REST d'IBM Security Key Lifecycle Manager. Pour plus d'informations sur le processus d'authentification, voir Processus d'authentification pour les services REST.

c. Exécutez **Update Config Property REST Service** pour définir la propriété **fips** dans le fichier de configuration SKLMConfig.properties. Transmettez l'identificateur d'authentification utilisateur que vous avez obtenu à l'étape b avec le message de demande, conformément à l'exemple suivant :

```
PUT https://localhost:<port>/SKLM/rest/v1/configProperties
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth userAuthId=139aeh34567m
Accept-Language : en
{ "fips" : "on"}
```

2. Editez le fichier *<WAS_HOME>*/java_1.7.1_32/jre/lib/security/java.security et ajoutez le fournisseur IBMJCEFIPS à la liste des fournisseurs de sécurité, comme indiqué dans l'exemple ci-dessous.

   Remarque : Vous devez mettre à jour le fichier java.security pour le code Java qui est utilisé par le serveur IBM Security Key Lifecycle Manager.

```
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
```

   Remarque : Les fournisseurs sont renumérotés pour ajouter le fournisseur IBMJCEFIPS en début de liste.

3. Enregistrez le fichier.
4. Redémarrez le serveur IBM Security Key Lifecycle Manager.

Configuration d'IBM Security Key Lifecycle Manager pour la conformité Suite B

Vous pouvez configurer IBM Security Key Lifecycle Manager afin qu'il soit conforme aux normes spécifiées par l'agence NSA (National Security Agency), agence américaine qui définit les exigences de sécurité en matière de chiffrement.

Pourquoi et quand exécuter cette tâche

Pour activer la conformité Suite B dans IBM Security Key Lifecycle Manager, vous devez configurer le fichier de propriétés SKLMConfig.properties avec l'option suivante.

```
suiteB=128|192
```

Lorsque vous configurez **suiteB** avec la valeur 128 ou 192, les propriétés suivantes sont ajoutées au fichier de propriétés, ou mises à jour si elles existent déjà.

```
TransportListener.ssl.protocols=TLSv1.2
requireSHA2Signatures=true
autoScaleSignatureHash=true
useThisECKeySize=256(if suiteB is 128)|384(if suiteB is 192)
```

Procédure

1. Définissez la propriété suivante dans le fichier *SKLM_HOME*/config/SKLMConfig.properties.

   ```
   suiteB=128|192
   ```

   - La valeur 128 définit le niveau minimal 128 bits de sécurité.
   - La valeur 192 définit le niveau minimal 192 bits de sécurité.

   Interface de ligne de commande

   a. Accédez au répertoire WAS_HOME/bin. Par exemple,

      Windows

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

      Linux

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

   b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme SKLMAdmin. Par exemple,

      Windows

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

      Linux

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

   c. Exécutez la commande **tklmConfigUpdateEntry** pour définir la propriété **suiteB** dans le fichier de configuration SKLMConfig.properties.

      ```
      print AdminTask.tklmConfigUpdateEntry ('[-name suiteB -value 128|192]')
      ```

   Interface REST

   a. Ouvrez un client REST.

   b. Obtenez un identificateur d'authentification utilisateur unique pour accéder aux services REST d'IBM Security Key Lifecycle Manager. Pour plus d'informations sur le processus d'authentification, voir Processus d'authentification pour les services REST.

   c. Exécutez le **Service REST Update Config Property** pour définir la propriété **suiteB** dans le fichier de configuration SKLMConfig.properties. Transmettez l'identificateur d'authentification utilisateur que vous avez obtenu à l'étape b avec le message de demande, conformément à l'exemple suivant :

```
PUT https://localhost:port/SKLM/rest/v1/configProperties
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth userAuthId=139aeh34567m
Accept-Language : en
{ "suiteB" : "128|192"}
```

2. Redémarrez le serveur.

Que faire ensuite

Sélectionnez un certificat qui utilise l'algorithme ECDSA, car la conformité Suite B nécessite que le certificat ECDSA pour la communication SSL fonctionne.

Si aucun certificat avec l'algorithme ECDSA n'est disponible, créez-en un nouveau. Pour plus d'informations, voir «Spécification de certificats SSL ou KMIP», à la page 1.

Configuration de la conformité NIST SP 800-131A dans IBM Security Key Lifecycle Manager

Configurez IBM Security Key Lifecycle Manager pour communiquer sur des connexions sécurisées, conformes à la norme National Institute of Standards and Technology (NIST) Special Publication (SP) 800-131A en mode strict.

Pourquoi et quand exécuter cette tâche

La norme NIST SP 800-131A spécifie des algorithmes à utiliser pour renforcer la sécurité et le chiffrement. En mode strict, toutes les communications doivent se conformer à la norme SP 800-131A.

Cette tâche utilise l'ID utilisateur WASAdmin dans la WebSphere Integrated Solutions Console pour configurer la conformité à NIST SP 800-131A dans IBM Security Key Lifecycle Manager.

Pour plus d'informations sur la configuration de WebSphere Application Server pour le mode strict de la norme SP800 131, consultez la documentation d'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).

Procédure

1. Connectez-vous à WebSphere Integrated Solutions Console (`https://localhost:9083/ibm/console/logon.jsp`).
2. Sur la page d'accueil du navigateur, tapez l'ID utilisateur `WASAdmin` et le mot de passe de cet administrateur.
3. Dans le panneau de navigation de gauche, cliquez sur **Sécurité** > **Certificat SSL et gestion des clés**.
4. Sur la page Certificat SSL et gestion des clés, sous **Articles liés**, cliquez sur **SSL configurations**.
5. Cliquez sur **NodeDefaultSSLSettings**.
6. Dans la section **Propriétés supplémentaires**, cliquez sur **Quality of protection (QoP) settings**.
7. Dans la liste **Protocol**, sélectionnez **TLSv1.2**, et dans la section **Cipher suite settings**, section **cipher suite groups**, sélectionnez **Strong**, puis cliquez sur **Update selected ciphers**.

8. Cliquez sur **OK**.
9. Cliquez sur **Enregistrer** pour enregistrer la configuration.
10. Dans le panneau de navigation de gauche, cliquez sur **Sécurité** > **Certificat SSL et gestion des clés** > **Gérer la norme FIPS**.

    Pour une exécution en mode SP800-131 strict, tous les certificats qui sont utilisés pour SSL sur le serveur doivent être convertis en certificats conformes aux exigences de SP800-131.
11. Pour convertir des certificats, sous **Articles liés**, cliquez sur **Convertir les certificats**.
12. Sélectionnez **Strict**, et choisissez l'algorithme `SHA256withRSA` à utiliser pour les nouveaux certificats à partir de la liste.
13. Sélectionnez la taille `2048` bits pour le certificat de la liste **New certificate key size**.

    Remarque : Si vous choisissez un algorithme de signature à courbe elliptique, ceux-ci utilisent des tailles spécifiques et vous ne pouvez pas indiquer de taille vous-même. La taille appropriée est utilisée automatiquement.
14. Si aucun certificat n'est affiché dans le cadre **Certificates that can not be converted**, cliquez sur **Appliquer** et **OK**.

    Si les certificats sont affichés dans le cadre **Certificates that can not be converted**, le serveur est incapable de les convertir. Remplacez ces certificats par ceux qui répondent aux exigences de la norme SP800-131. Le serveur peut ne pas convertir un certificat pour les raisons suivantes :
    - Le certificat a été créé par une autorité de certification (CA).
    - Le certificat se trouve dans un fichier de clés en lecture seule.
15. Cliquez sur **Certificat SSL et gestion de clés** > **Gérer la norme FIPS**.
16. Sélectionnez **Activer SP800-131**.
17. Sélectionnez **Strict**.
18. Cliquez sur **Appliquer**, puis sur **OK**.
19. Cliquez sur **Enregistrer** pour enregistrer la configuration.
20. Arrêtez WebSphere Application Server.

    Pour connaître la procédure d'arrêt du serveur, voir «Serveur IBM Security Key Lifecycle Manager - Redémarrage», à la page 211.
21. Dans le fichier `<SKLM_HOME>/config/SKLMConfig.properties`, définissez les propriétés **`TransportListener.ssl.protocols`** et **`fips`** par ces valeurs.

    ```
    TransportListener.ssl.protocols=TLSv1.2
    fips=on
    ```

    Interface de ligne de commande

    a. Accédez au répertoire `WAS_HOME/bin`. Par exemple,

       Windows

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

       Linux

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

    b. Démarrez l'interface **`wsadmin`** en utilisant un ID utilisateur autorisé, comme `SKLMAdmin`. Par exemple,

       Windows

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

       Linux

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

c. Exécutez la commande **tklmConfigUpdateEntry**.

```
print AdminTask.tklmConfigUpdateEntry ('[-name TransportListener.ssl.protocols -valu
print AdminTask.tklmConfigUpdateEntry ('[-name fips -value on]')
```

Interface REST

a. Ouvrez un client REST.

b. Obtenez un identificateur d'authentification utilisateur unique pour accéder aux services REST d'IBM Security Key Lifecycle Manager. Pour plus d'informations sur le processus d'authentification, voir Processus d'authentification pour les services REST.

c. Exécutez **Update Config Property REST Service**. Transmettez l'identificateur d'authentification utilisateur que vous avez obtenu à l'étape b avec le message de demande, conformément à l'exemple suivant :

```
PUT https://localhost:<port>/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:<port>/SKLM/rest/v1/configProperties
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth userAuthId=139aeh34567m
Accept-Language : en
{ "fips" : "on"}
```

22. Dans le fichier *<WAS_HOME>*/profiles/KLMProfile/properties/ssl.client.props, mettez à jour les propriétés comme suit :

```
com.ibm.ssl.protocol=TLSv1.2
com.ibm.security.useFIPS=true
com.ibm.websphere.security.FIPSLevel=SP800-131
```

23. Démarrez WebSphere Application Server.

Pour connaître la procédure de démarrage du serveur, voir «Serveur IBM Security Key Lifecycle Manager - Redémarrage», à la page 211.

Gestion de la clé principale

Vous pouvez créer et actualiser des clés principales IBM Security Key Lifecycle Manager. Vous pouvez également déplacer une clé principale du magasin de clés Java vers Hardware Security Module (HSM), et inversement.

Vous pouvez utiliser le Service REST Master Key pour exécuter toutes les opérations de gestion de la clé principale.

Gestion de la clé principale IBM Security Key Lifecycle Manager dans une configuration multimaître

Cette rubrique explique les étapes à suivre pour effectuer les opérations de gestion de la clé principale IBM Security Key Lifecycle Manager dans un cluster multimaître. Toutes les opérations de gestion des clés principales doivent être effectuées sur le serveur maître principal uniquement.

Procédure

1. Sauvegardez le serveur maître principal. Pour obtenir des instructions, voir «Sauvegarde et restauration», à la page 126.

2. Assurez-vous que tous les serveurs maîtres du cluster multimaître sont connectés.
3. Exécutez les opérations de gestion de la clé principale sur le serveur maître principal. Pour obtenir des instructions, voir Service REST Master Key.
4. Sur tous les serveurs maîtres, vérifiez que la valeur de la propriété **useMasterKeyinHSM** dans le fichier `SKLMConfig.properties` est correctement configurée. Si le cluster multimaître est configuré pour utiliser le client HSM, la valeur de la propriété **useMasterKeyinHSM** doit être `true`.

Gestion de la clé principale IBM Security Key Lifecycle Manager dans une configuration de réplication

Cette rubrique explique les étapes à suivre pour effectuer les opérations de gestion de la clé principale dans une configuration de réplication. Une fois ces étapes exécutées, vous pouvez effectuer la réplication du serveur maître sur les serveurs clones.

Avant de commencer

Faites une copie de sauvegarde du serveur maître de réplication. Pour plus d'informations, voir «Sauvegarde et restauration», à la page 126.

Procédure

1. Exécutez les opérations de gestion des clés principales sur le serveur maître de réplication. Pour obtenir des instructions, voir Service REST Master Key.
2. Faites une copie de sauvegarde du serveur maître de réplication. Pour obtenir des instructions, voir «Sauvegarde et restauration», à la page 126.
3. Copiez le fichier JAR de sauvegarde du serveur maître sur tous les serveurs clones.
4. Si le serveur maître de réplication est configuré pour utiliser HSM pour stocker la clé principale, assurez-vous que tous les serveurs clones sont également configurés pour utiliser le même client HSM. Pour obtenir des instructions, voir «Configuration de paramètres HSM», à la page 215.
5. Restaurez les fichiers de sauvegarde sur tous les serveurs clones. Pour obtenir des instructions, voir «Restauration d'un fichier de sauvegarde», à la page 138.
6. Sur tous les serveurs clones, connectez-vous à l'interface graphique d'IBM Security Key Lifecycle Manager en tant qu'administrateur IBM Security Key Lifecycle Manager.
   a. Cliquez sur **Administration** > **Réplication**.
   b. Sélectionnez le rôle de réplication en tant que **Clone**. Le rôle de réplication a été changé en `Master` après la restauration des fichiers de sauvegarde sur le serveur clone à partir du serveur maître.
7. Redémarrez les serveurs clones pour lesquels vous avez modifié les rôles. Pour obtenir des instructions, voir Serveur IBM Security Key Lifecycle Manager - Redémarrage.

Configuration multimaître

L'implémentation de la solution à haute disponibilité requiert la configuration de maîtres IBM Security Key Lifecycle Manager dans une configuration multimaître. Toutes les instances d'IBM Security Key Lifecycle Manager dans le cluster pointent vers une source de données unique qui est configurée pour la fonction de reprise à

haute disponibilité après incident (HADR) de Db2 afin d'assurer la disponibilité en temps réel des données les plus récentes pour tous les maîtres dans le cluster.

Vous pouvez utiliser la configuration multimaître d'IBM Security Key Lifecycle Manager pour la transmission de données dans l'optique suivante :

- Assurer la disponibilité des données cohérente et continue d'IBM Security Key Lifecycle Manager dans l'ensemble de l'organisation.
- Eviter un point de défaillance unique en utilisant la solution à haute disponibilité.
- Les maîtres peuvent se trouver sur plusieurs sites physiques, autrement dit être répartis sur le réseau.

La configuration Db2 HADR est utilisée comme source de données unique pour tous les maîtres dans le cluster multimaître d'IBM Security Key Lifecycle Manager. HADR vous protège contre la perte de données en transmettant les modifications d'une base de données source (principale) à une base de données cible (de secours). Db2 HADR prend en charge plusieurs bases de données de secours dans votre configuration multimaître.

Principales fonctions de la configuration multimaître d'IBM Security Key Lifecycle Manager

- D'autres maîtres IBM Security Key Lifecycle Manager dans le cluster multimaître peuvent accéder aux clés créées sur un maître IBM Security Key Lifecycle Manager.
- Les unités IPP et les clients KMIP enregistrés sur un maître IBM Security Key Lifecycle Manager peuvent accéder aux clés se trouvant sur un autre maître du cluster multimaître.
- Utilisation de l'interface graphique et de l'interface REST pour configurer les serveurs maîtres IBM Security Key Lifecycle Manager pour la configuration multimaître.

Pour plus d'informations sur les services REST multimaîtres, voir Services REST de configuration multimaître.

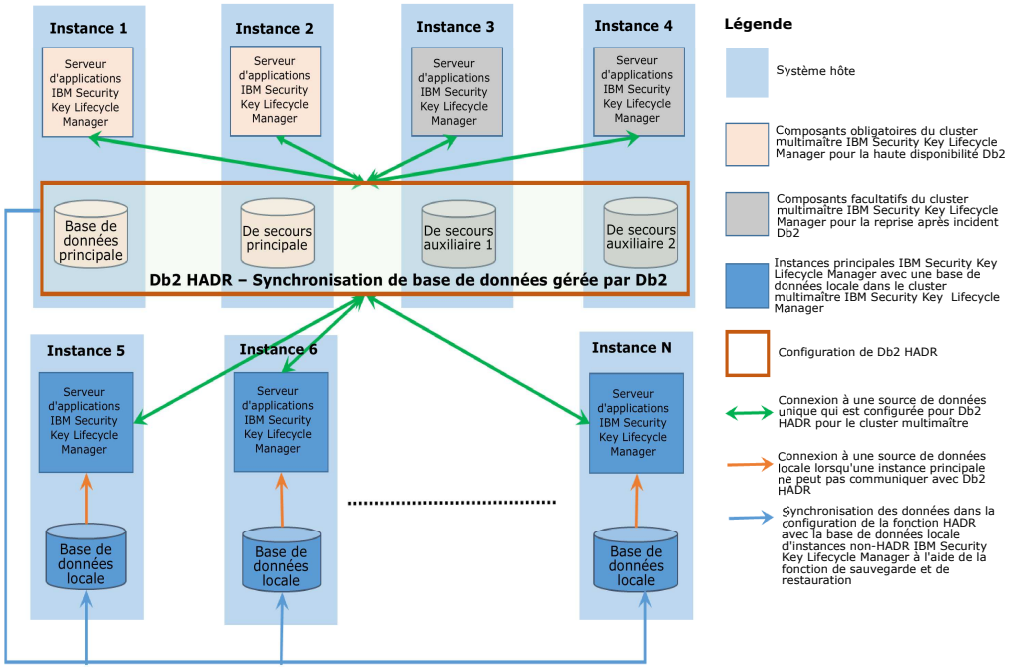
Architecture de déploiement multimaître

L'architecture multimaître d'IBM Security Key Lifecycle Manager s'appuie sur la fonction HADR (fonction de reprise à haute disponibilité après incident) de Db2 pour implémenter une solution à haute disponibilité.

Chaque instance d'IBM Security Key Lifecycle Manager est installée avec son instance Db2 qui contient toutes les métadonnées, les données clés des objets cryptographiques gérés et les données d'audit. Le cluster inclut plusieurs instances d'IBM Security Key Lifecycle Manager appelées maîtres. Tous les maîtres du cluster ont les mêmes privilèges. Dans le cluster multimaître d'IBM Security Key Lifecycle Manager, chaque maître se connecte à une seule base de données, appelée base de données principale. Cette dernière se connecte à une autre base de données d'un maître IBM Security Key Lifecycle Manager, également appelée base de données de secours. Avec la configuration Db2 HADR, les données sont transmises de manière continue entre les deux bases de données et sont synchronisées. En cas d'échec de la base de données principale, une base de données prend automatiquement le relais en tant qu'élément principal et garantit la disponibilité des dernières données pour tous les maîtres du cluster.

Pour la configuration de la fonction HADR (reprise à haute disponibilité après incident), les paramètres Db2 requis sont configurés sur les maîtres IBM Security Key Lifecycle Manager avec une base de données principale et une base de données de secours. Le diagramme ci-dessous représente un déploiement simple d'IBM Security Key Lifecycle Manager et de Db2 HADR pour un environnement multimaître dans lequel quatre instances (maîtres) de Db2 HADR et N instances d'IBM Security Key Lifecycle Manager sont configurées.

Déploiement physique



WebSphere Application Server est configuré avec la base de données Db2 activée HADR pour la redirection automatique du client. En cas de défaillance de la base de données HADR principale, WebSphere Application Server rétablit automatiquement la connexion à la base de données HADR de secours principale.

Db2 HADR prend en charge plusieurs bases de données de secours dans la configuration multimaître d'IBM Security Key Lifecycle Manager. Vous pouvez disposer d'une base de données de secours principale et de deux bases de données de secours auxiliaires. Pour plus d'informations sur les cas de bases de données de secours multiples, voir Bases de données de secours multiples.

Conditions requises pour le déploiement

- Les serveurs de base de données Db2, qu'ils soient principaux ou de secours, doivent être installés sur la même version du système d'exploitation.
- La version Db2 installée sur les différents serveurs maîtres IBM Security Key Lifecycle Manager doit être la même.
- Vous devez utiliser un réseau dédié pour les connexions de secours et principale Db2 HADR.

Bases de données de secours multiples

La configuration de la fonction de reprise à haute disponibilité après incident (HADR) de Db2 garantit la disponibilité continue des données pour toutes les

instances d'IBM Security Key Lifecycle Manager d'un cluster multimaître. HADR vous protège contre la perte de données en transmettant les modifications d'une base de données source (principale) à une base de données cible (de secours).

Db2 HADR prend en charge trois bases de données de secours dans votre configuration multimaître : une base de données de secours pour la haute disponibilité et deux autres pour la reprise après incident. Lorsque la base de données principale est arrêtée, le service de reprise HADR demande à la base de données de prendre le relais en tant que nouvelle base de données principale HADR. Pour plus d'informations sur le service de reprise HADR, voir Service de reprise HADR.

Des priorités sont affectées à chaque base de données de secours dans le cluster. Celle ayant la priorité la plus élevée est celle qui a le rôle de base de données principale. Par exemple, si une base de données principale du cluster multimaître IBM Security Key Lifecycle Manager est défaillante, la base de données de secours ayant l'index de priorité 1 devient la base de données principale.

Pour ajouter plusieurs bases de données de secours au cluster multimaître, vous pouvez utiliser l'interface graphique d'IBM Security Key Lifecycle Manager ou le service REST Add Master. Pour plus d'informations, voir Ajout d'un maître de secours au cluster multimaître.

Scénarios de reprise HADR

Le tableau ci-dessous contient des informations sur les scénarios de reprise Db2 HADR lorsque des maîtres IBM Security Key Lifecycle Manager sont configurés dans un environnement multimaître.

Agent du système hôte de la base de données principale	**Base de données principale**	**Agent du système hôte de la base de données 1 de secours**	**Base de données 1 de secours**	**Agent du système hôte de la base de données 2 de secours**	**Base de données 2 de secours**	**Agent du système hôte de la base de données 3 de secours**	**Base de données 3 de secours**	**Actions de l'agent**	**Service de clés IBM Security Key Lifecycle Manager**	**Reprise automatique**
Démarré	Démarrée	Démarré	Démarrée	Démarré	Démarrée	Démarré	Démarrée	Scénario satisfaisant.	De la base de données principale	Non disponible
Démarré	Démarrée	Démarré	Arrêtée	Démarré ou arrêté	Démarrée ou arrêtée	Démarré ou arrêté	Démarrée ou arrêtée		De la base de données principale	Non disponible
Démarré	Démarrée	Arrêté	Arrêtée	Démarré ou arrêté	Démarrée ou arrêtée	Démarré ou arrêté	Démarrée ou arrêtée		De la base de données principale	Non disponible

Agent du système hôte de la base de données principale	Base de données principale	Agent du système hôte de la base de données 1 de secours	Base de données 1 de secours	Agent du système hôte de la base de données 2 de secours	Base de données 2 de secours	Agent du système hôte de la base de données 3 de secours	Base de données 3 de secours	Actions de l'agent	Service de clés IBM Security Key Lifecycle Manager	Reprise automatique
Démarré	Arrêtée	Démarré	Démarrée	Démarré ou arrêté	Démarrée ou arrêtée	Démarré ou arrêté	Démarrée ou arrêtée	L'agent sur le serveur principal envoie une demande à l'agent sur le serveur de secours 1 pour qu'il procède à la reprise en tant que base de données principale.	De la base de données 1 de secours	Oui, si la base de données principale ou si la base de données 1 de secours (celle qui est disponible pour la reprise) et les agents sur les deux serveurs doivent être démarrés et peuvent communiquer les uns avec les autres. Sinon, non.
Arrêté	Arrêtée	Démarré	Démarrée	Démarré ou arrêté	Démarrée ou arrêtée	Démarré ou arrêté	Démarrée ou arrêtée		De la base de données 1 de secours	Non
Démarré	Arrêtée	Démarré ou arrêté	Arrêtée	Démarré	Démarrée	Démarré ou arrêté	Démarrée ou arrêtée	L'agent sur le serveur principal envoie une demande à l'agent sur le serveur de secours 2 pour qu'il procède à la reprise en tant que base de données principale.	De la base de données 2 de secours	Oui, si la base de données principale ou si la base de données 2 de secours (celle qui est disponible pour la reprise) et les agents sur les deux serveurs doivent être démarrés et peuvent communiquer les uns avec les autres. Sinon, non.
Arrêté	Arrêtée	Démarré ou arrêté	Arrêtée	Démarré ou arrêté	Démarrée	Démarré ou arrêté	Démarrée ou arrêtée		De la base de données 2 de secours après une reprise manuelle	Non
Arrêté	Arrêtée	Arrêté	Arrêtée	Démarré ou arrêté	Démarrée	Démarré ou arrêté	Démarrée ou arrêtée		De la base de données 2 de secours après une reprise manuelle	Non

Agent du système hôte de la base de données principale	Base de données principale	Agent du système hôte de la base de données 1 de secours	Base de données 1 de secours	Agent du système hôte de la base de données 2 de secours	Base de données 2 de secours	Agent du système hôte de la base de données 3 de secours	Base de données 3 de secours	Actions de l'agent	Service de clés IBM Security Key Lifecycle Manager	Reprise automatique
Démarré	Arrêtée	Démarré ou arrêté	Arrêtée	Démarré ou arrêté	Arrêtée	Démarré	Démarrée	L'agent sur le serveur principal envoie une demande à l'agent sur le serveur de secours 3 pour qu'il procède à la reprise en tant que base de données principale.	De la base de données 3 de secours	Oui, si la base de données principale ou si la base de données 3 de secours (celle qui est disponible pour la reprise) et les agents sur les deux serveurs doivent être démarrés et peuvent communiquer les uns avec les autres. Sinon, non.
Démarré	Arrêtée	Démarré ou arrêté	Arrêtée	Démarré ou arrêté	Arrêtée	Démarré ou arrêté	Arrêtée	-	Aucun	Non

Système de surveillance

Dans un cluster multimaître, la surveillance de l'état de santé des instances d'IBM Security Key Lifecycle Manager et la correction rapide des problèmes avant qu'ils n'impactent les opérations métier constituent des étapes essentielles. IBM Security Key Lifecycle Manager inclut la fonction de surveillance qui permet de surveiller l'état de santé de tous les serveurs maîtres IBM Security Key Lifecycle Manager du cluster.

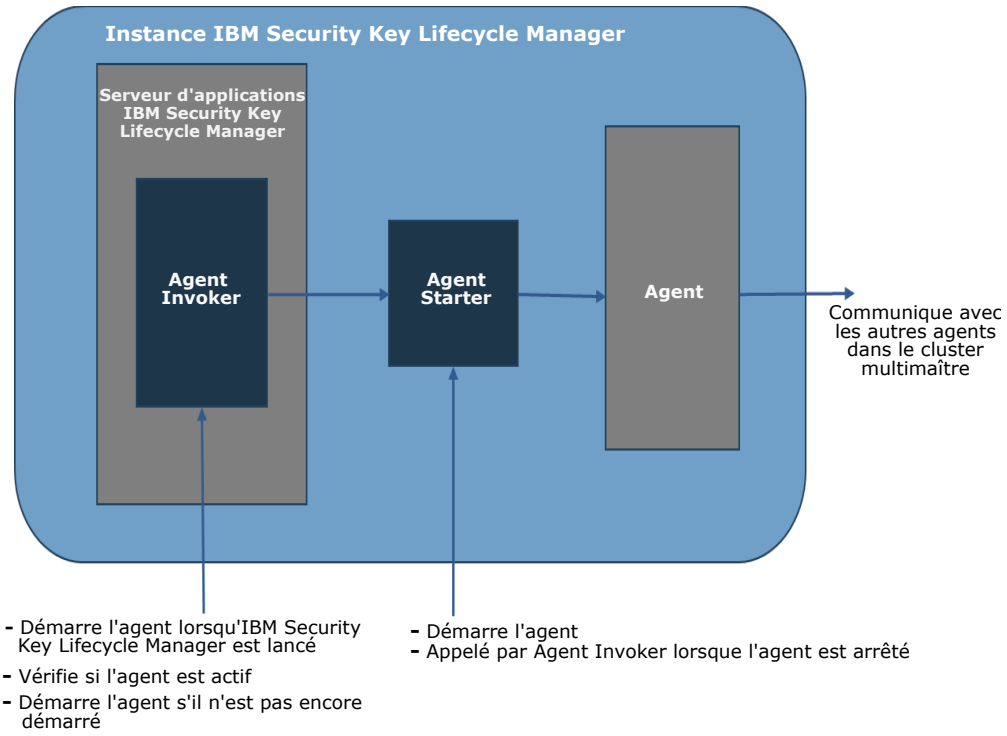
La surveillance est une partie intégrante de la configuration et de la gestion de votre environnement multimaître. Le système de surveillance d'IBM Security Key Lifecycle Manager fournit une vue détaillée de la configuration et de l'état de votre environnement multimaître en utilisant les composants de surveillance ci-après.

Agent Surveille et collecte les données de statut pour les serveurs maîtres IBM Security Key Lifecycle Manager dans le cluster selon une fréquence définie. Pour plus d'informations, voir Agent.

Agent Starter
Démarre le service d'agent. Pour plus d'informations, voir Agent Starter.

Agent Invoker
Surveille le statut du service d'agent à intervalles réguliers. Pour plus d'informations, voir Agent Invoker.

Le diagramme ci-dessous représente les composants de surveillance dans une instance (maître) d'IBM Security Key Lifecycle Manager du cluster.



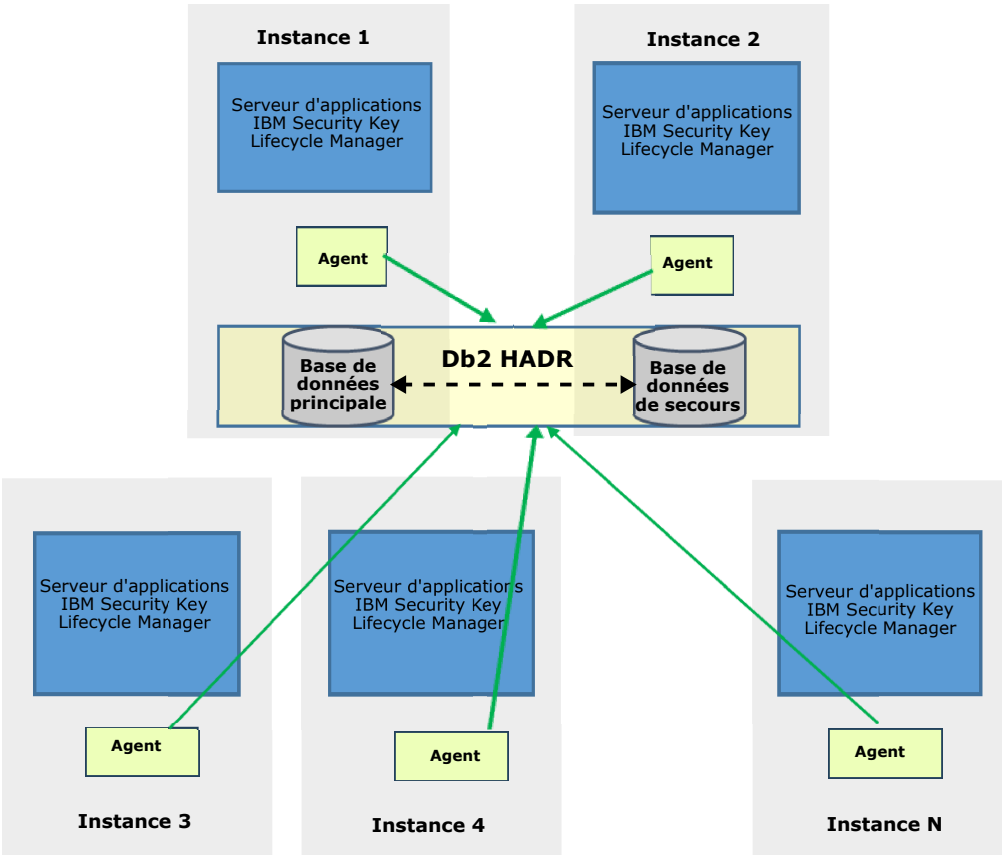
Agent

Le service d'agent d'IBM Security Key Lifecycle Manager permet de surveiller l'état de santé et de configurer les instances d'IBM Security Key Lifecycle Manager d'un cluster multimaître.

Après l'installation d'une instance IBM Security Key Lifecycle Manager, l'agent est également automatiquement installé dans ce serveur. L'agent démarre lorsque vous démarrez IBM Security Key Lifecycle Manager. Lorsque le service d'agent est arrêté, le service Agent Invoker exécute le script Agent Starter `agentStarter` pour redémarrer le service. Le fichier `agentStarter.properties` contient les informations nécessaires à l'exécution du script. Pour plus d'informations, voir Agent Invoker et Agent Starter.

Le diagramme ci-dessous présente la façon dont les agents IBM Security Key Lifecycle Manager sont déployés dans l'environnement multimaître. L'agent sur chaque instance (maître) IBM Security Key Lifecycle Manager capture le statut de l'interface utilisateur, de KMIP et des ports IP. Puis, les informations de statut sont mises à jour dans la base de données avec les données d'horodatage.

Agents de surveillance



L'agent IBM Security Key Lifecycle Manager fournit les services ci-après pour collecter des données de surveillance et configurer les instances IBM Security Key Lifecycle Manager dans le cluster multimaître.

Services planifiés

Rassemble des données de statut en démarrant et en gérant l'ensemble suivant de services à des intervalles réguliers.

- Service de surveillance d'agent
- Service de surveillance de port
- Service de reprise HADR

Services de configuration

L'agent fournit plusieurs services permettant de configurer des maîtres IBM Security Key Lifecycle Manager pour la configuration multimaître. Les services de configuration sont automatiquement démarrés en même temps que l'agent.

- Services de configuration

Service de surveillance d'agent :

Le service de surveillance d'agent vérifie régulièrement si les agents sur les autres serveurs maîtres IBM Security Key Lifecycle Manager du cluster multimaître sont opérationnels.

Lorsque l'agent d'un serveur maître IBM Security Key Lifecycle Manager est démarré, le service de surveillance d'agent démarre automatiquement la surveillance du statut des agents à des intervalles réguliers si l'instance IBM Security Key Lifecycle Manager n'est pas de type `Local`. Vous pouvez afficher le statut de disponibilité en utilisant l'interface REST ou l'interface utilisateur graphique IBM Security Key Lifecycle Manager. Pour plus d'informations sur le service d'agent, voir Agents.

Vous pouvez utiliser la propriété **agent.monitoring.svc.interval** dans le fichier *<SKLM_HOME>*`\config\SKLMConfig.properties`, par exemple `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\config\SKLMConfig.properties`, pour configurer la fréquence d'exécution du service de surveillance de l'agent. Pour plus d'informations sur la propriété de configuration, voir agent.monitoring.svc.interval.

Pour la définition de *<SKLM_HOME>*, voir Définitions relatives à un répertoire *HOME* et d'autres variables de répertoire.

Service de surveillance de port :

Le service de surveillance de port vérifie régulièrement la disponibilité des ports requis par un serveur maître IBM Security Key Lifecycle Manager pour la communication dans le cluster multimaître.

Lorsque le service d'agent d'un maître IBM Security Key Lifecycle Manager est démarré, le service de surveillance de port commence automatiquement la surveillance de la disponibilité des ports à intervalles réguliers si l'instance IBM Security Key Lifecycle Manager n'est pas de type `Local`. Vous pouvez afficher le statut de disponibilité en utilisant l'interface REST ou l'interface utilisateur graphique IBM Security Key Lifecycle Manager. Pour plus d'informations sur le service d'agent, voir Agents.

Vous pouvez utiliser la propriété **port.monitoring.svc.interval** dans le fichier *<SKLM_HOME>*`\config\SKLMConfig.properties`, par exemple `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\config\SKLMConfig.properties`, pour configurer la fréquence d'exécution du service de surveillance de port. Pour plus d'informations sur la propriété de configuration, voir port.monitoring.svc.interval.

Pour la définition de *<SKLM_HOME>*, voir Définitions relatives à un répertoire *HOME* et d'autres variables de répertoire.

Le service de surveillance de port vérifie si les ports suivants sont en cours d'exécution et accessibles.

Port TCP
: Port sur lequel le serveur IBM Security Key Lifecycle Manager écoute les demandes des unités.

Port SSL
: Port sur lequel le serveur IBM Security Key Lifecycle Manager écoute les demandes des unités qui communiquent via le protocole SSL.

Port KMIP
: Port sur lequel le serveur IBM Security Key Lifecycle Manager écoute les demandes pour communiquer via le socket SSL qui utilise le protocole KMIP (Key Management Interoperability Protocol).

Port Db2
Port sur lequel le serveur IBM Security Key Lifecycle Manager écoute les demandes provenant de Db2.

Port HTTP
Port sur lequel IBM Security Key Lifecycle Manager écoute les demandes HTTPS.

Port d'administration
Port sur lequel le serveur IBM Security Key Lifecycle Manager écoute les demandes.

Port HADR
Port des bases de données configurées en tant qu'élément HADR pour les communications de base de données.

Port d'agent
Port sur lequel l'agent écoute les communications d'IBM Security Key Lifecycle Manager.

Pour plus d'informations sur les valeurs de port par défaut, voir Services, ports et processus.

Service de reprise HADR :

Le service de reprise HADR assure la reprise depuis une base de données principale lorsqu'un problème de connexion survient entre le serveur maître IBM Security Key Lifecycle Manager et la base de données principale dans le cluster multimaître. Lorsque la base de données principale est arrêtée, l'opération de reprise est lancée sur une base de données de secours pour que les opérations des utilisateur ne soient pas bloquées lors de l'indisponibilité.

Vous pouvez configurer la propriété **agent.takeover.svc.interval** dans le fichier *<SKLM_HOME>*/config/SKLMConfig.properties, par exemple C:\Program Files\IBM\WebSphere\AppServer\products\sklm\config\SKLMConfig.properties pour définir la fréquence d'exécution du service de reprise HADR. Pour plus d'informations sur la propriété de configuration, voir agent.takeover.svc.interval.

La fonction HADR (reprise à haute disponibilité après incident) de Db2 est utilisée dans le cluster multimaître d'IBM Security Key Lifecycle Manager. La configuration de Db2 HADR vous protège contre la perte de données en transmettant les modifications d'une base de données principale aux bases de données de secours. Dans des conditions normales, la synchronisation des bases de données principales et de secours Db2 HADR est assurée par Db2 HADR.

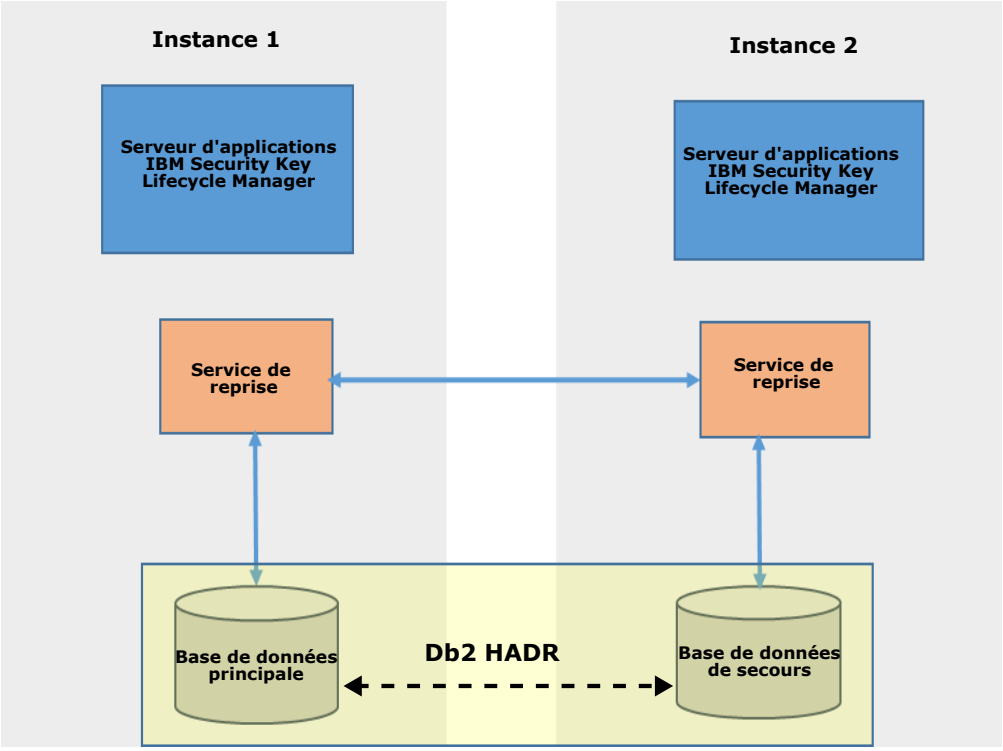
Les agents sont installés sur tous les serveurs maîtres d'un cluster multimaître. Les services d'agent effectuent le suivi de la disponibilité des ports liés IBM Security Key Lifecycle Manager. Si la base de données principale est arrêtée, le service de reprise demande à la base de données de secours HADR de prendre le relais en tant que nouvelle base de données principale HADR.

Pour l'opération de reprise, les bases de données principales et de secours sont synchronisées en permanence en utilisant un canal de communication sécurisé. Des paramètres de configuration Db2 HADR et WebSphere Application Server sont automatiquement mis à jour pour l'opération de reprise en utilisant les services de configuration exécutés par l'agent. Pour plus d'informations sur les différents services de configuration, voir Services de configuration.

Db2 HADR prend en charge jusqu'à trois bases de données de secours dans votre configuration multimaître. Vous pouvez disposer d'une base de données de secours principale et de deux bases de données de secours auxiliaires. Des priorités sont affectées à chaque base de données de secours dans le cluster. Celle ayant la priorité la plus élevée est celle qui a le rôle de base de données principale. Par exemple, si une base de données principale du cluster multimaître IBM Security Key Lifecycle Manager est défaillante, la base de données de secours ayant l'index de priorité 1 devient la base de données principale. Si l'opération de reprise sur la base de données de secours ayant l'index de priorité 1 échoue, l'élément de secours avec l'index de priorité suivant (index de priorité 2) prend alors le relais en tant que base de données principale.

Remarque : Vous devez redémarrer WebSphere Application Server manuellement sur tous les serveurs de secours si une base de données de secours auxiliaire devient la base de données principale. Il n'est pas nécessaire de redémarrer WebSphere Application Server lorsque la base de données de secours principal devient la base de données principale.

IBM Security Key Lifecycle Manager prend en charge l'option de reprise par restauration. Vous pouvez configurer la base de données principale de telle sorte qu'elle ait à nouveau le rôle principal dès qu'elle redémarre.



- Le service de reprise d'`Instance 1` (serveur maître principal) vérifie le statut de la base de données (`Base de données principale`) en utilisant des commandes Db2.
- Si la `base de données principale` est arrêtée, l'`Instance 2` (serveur maître de secours) reçoit une demande de reprise du serveur principal. Le `serveur de secours` prend le relais en tant que `base de données principale`.
- Le serveur maître principal reçoit un message du serveur de secours indiquant si l'opération de reprise a abouti. Lorsque l'opération de reprise échoue, le service

de reprise sur le serveur principal envoie des demandes de reprise au serveur de secours suivant si le cluster est configuré avec plusieurs serveurs de secours.
- Lorsque l'ancien serveur de base de données principal est à nouveau opérationnel, le service de reprise démarre HADR sur ce serveur comme élément de secours.

Pour plus d'informations sur la configuration requise pour Db2 HADR, voir Database configuration for high availability disaster recovery (HADR).

Lancement manuel d'une opération de reprise

Lorsque le serveur maître principal IBM Security Key Lifecycle Manager contenant la base de données principale est arrêté, l'opération de reprise n'est pas lancée automatiquement. Vous pouvez alors démarrer manuellement l'opération de reprise en exécutant le script **sklmTakeoverHADR**.

Remarque : Si le système d'exploitation du serveur maître principal IBM Security Key Lifecycle Manager échoue, suivez les instructions de lancement manuel de l'opération de reprise présentées ici : Echec du démarrage du système d'exploitation du serveur maître principal IBM Security Key Lifecycle Manager.

1. Recherchez le script **sklmTakeoverHADR**.

   Windows
   <*SKLM_INSTALL_HOME*>\agent

   L'emplacement par défaut est C:\Program Files\IBM\SKLMV301\agent.

   Linux <*SKLM_INSTALL_HOME*>/agent

   L'emplacement par défaut est /opt/IBM/SKLMV301\agent.
2. Ouvrez une invite de commande et exécutez le script.

   Windows
   Accédez au répertoire <*SKLM_INSTALL_HOME*>\agent et exécutez la commande suivante :

   ```
   sklmTakeoverHADR.bat <WAS_HOME> [IP_HOSTNAME] [AGENT_PORT]
   ```

   Par exemple :

   ```
   sklmTakeoverHADR.bat "C:\Program Files\IBM\WebSphere\AppServer" 9.113.37.10 60015
   ```

   Linux Accédez au répertoire <*SKLM_INSTALL_HOME*>/agent et exécutez la commande suivante :

   ```
   sklmTakeoverHADR.sh <WAS_HOME> [IP_HOSTNAME] [AGENT_PORT]
   ```

   Par exemple :

   ```
   ./sklmTakeoverHADR.sh /opt/IBM/WebSphere/AppServer 9.113.37.10 60015
   ```

Services de configuration :

L'agent fournit plusieurs services permettant de configurer des maîtres IBM Security Key Lifecycle Manager pour la configuration multimaître.

Mise à jour de la configuration de la base de données (principale)
Met à jour la base de données principale sur un serveur maître IBM Security Key Lifecycle Manager dans le cluster avec la configuration requise pour une configuration multimaître.

Mise à jour de la configuration de la base de données HADR (principale et de secours)
Met à jour les paramètres de configuration sur les serveurs de base de données principal et de secours pour la configuration de la fonction de reprise à haute disponibilité après incident (HADR) de Db2.

Exécution et restauration de sauvegarde
Sauvegarde la base de données à partir du serveur principal et la restaure sur le serveur de secours. Dans un cluster multimaître avec une configuration Db2 HADR, le serveur de base de données principal et le serveur de base de données de secours doivent être synchronisés avec les mêmes données.

Envoi et réception de sauvegarde
Envoie le fichier de sauvegarde du serveur de base de données principal au serveur de secours en utilisant un canal de communication sécurisé. Sur le serveur de secours, le fichier de sauvegarde se trouve dans le dossier *<SKLM_DATA>*, par exemple `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data`. Pour la définition de *<SKLM_DATA>*, voir Définitions relatives à un répertoire *HOME* et d'autres variables de répertoire.

Démarrage de la fonction HADR (principal/de secours)
Démarre les opérations Db2 HADR sur les serveurs de base de données principaux et de secours. Démarre Db2 HADR sur le serveur de secours puis sur le serveur principal.

Mise à jour de la configuration WebSphere Application Server
Met à jour la configuration WebSphere Application Server afin de spécifier les propriétés de la source de données Db2, telles les noms et les ports des serveurs de base de données de secours pour la prise en charge de la redirection automatique de client. Si la connexion au serveur Db2 échoue, WebSphere Application Server rétablit automatiquement la connexion au serveur Db2 de secours.

Redémarrage de WebSphere Application Server
Redémarre WebSphere Application Server sur le serveur principal, le serveur de secours et d'autres instances d'IBM Security Key Lifecycle Manager dans le cluster multimaître afin d'appliquer les modifications de configuration de source de données Db2 effectuées pour la prise en charge de la redirection automatique de client.

Obtention du statut de configuration Db2 HADR et WebSphere Application Server
Obtient le statut de connexion Db2 HADR et WebSphere Application Server. Pour un environnement HADR, vous devez vous assurer que le système Db2 HADR principal et le système Db2 HADR de secours sont connectés.

Service de synchronisation des données :

Dans le cluster multimaître IBM Security Key Lifecycle Manager, les bases de données principale et de secours sont configurées avec Db2 HADR pour garantir la haute disponibilité. Dans des conditions normales, la synchronisation des bases de données principales et de secours est assurée par Db2 HADR. Le service de synchronisation des données IBM Security Key Lifecycle Manager copie les fichiers de sauvegarde Db2 du maître principal dans les autres noeuds maîtres du cluster à une fréquence définie. La synchronisation des données permet que les données des noeuds principaux soient identiques à celles du serveur principal du cluster.

Lorsqu'un serveur maître est déconnecté du cluster en raison de problèmes de connectivité, vous pouvez définir ce serveur de telle sorte qu'il soit en mode lecture/écriture. Vous pouvez ensuite restaurer les fichiers de sauvegarde sur ce serveur maître afin de servir les clés se trouvant sur les unités. Pour plus d'informations sur la définition du maître isolé en mode lecture/écriture, voir «Configuration d'un maître isolé en tant que maître en lecture/écriture», à la page 267. Une fois les problèmes de connectivité résolus, vous pouvez ajouter le serveur maître au cluster multimaître. Pour plus d'informations sur l'ajout au cluster, voir «Intégration du maître en lecture/écriture au cluster», à la page 268.

Emplacement du fichier de sauvegarde

Le fichier de sauvegarde du serveur principal est copié dans le dossier *<WAS_HOME>*/products/sklm/data/synchronization sur le noeud maître. Vous pouvez conserver jusqu'à deux fichiers de sauvegarde.

Configuration de la fréquence de synchronisation des données

Vous pouvez configurer la propriété **data.synchronizing.svc.interval** dans le fichier <SKLM_HOME>/config/SKLMConfig.properties afin de définir la fréquence de synchronisation des données. Pour plus d'informations sur la propriété de configuration, voir data.synchronizing.svc.interval.

Définition du mot de passe pour les fichiers de sauvegarde

Vous pouvez configurer la propriété **data.synchronizing.backup.password** dans le fichier <SKLM_HOME>/config/SKLMConfig.properties afin de définir le mot de passe pour les fichiers de sauvegarde qui sont générés par le service de synchronisation des données sur le maître principal ou de secours. Ces fichiers de sauvegarde sont copiés sur les autres noeuds maîtres dans le cluster multimaître d'IBM Security Key Lifecycle Manager à la fréquence que vous avez spécifiée dans la propriété à **data.synchronizing.svc.interval**.

Vous pouvez ensuite restaurer les fichiers de sauvegarde sur le serveur maître en lecture/écriture en utilisant le mot de passe que vous avez défini. Vous pouvez utiliser l'interface graphique, l'interface de ligne de commande ou l'interface REST pour restaurer les données si vous avez défini le mot de passe dans le fichier de configuration. Si la valeur de la propriété de configuration n'est pas définie, un mot de passe aléatoire est généré et les données sont automatiquement restaurées sur le maître en lecture/écriture. Vous devez redémarrer WebSphere Application Server et le service d'agent après avoir défini le mot de passe. Pour plus d'informations sur la propriété de configuration, voir data.synchronizing.backup.password.

Définition du nombre maximal de fichiers de sauvegarde Db2

Vous pouvez configurer la propriété **data.synchronizing.svc.MaxBackupNum** dans le fichier <SKLM_HOME>/config/SKLMConfig.properties pour spécifier le nombre maximal de fichiers de sauvegarde Db2 à conserver sur les maîtres non HADR du cluster multimaître. Vous devez redémarrer WebSphere Application Server et le service d'agent après avoir défini le mot de passe. Pour plus d'informations sur la propriété de configuration, voir data.synchronizing.svc.MaxBackupNum.

Redémarrage du service d'agent IBM Security Key Lifecycle Manager :

Lorsque le service d'agent IBM Security Key Lifecycle Manager redémarre, le serveur lit sa configuration et accepte les modifications de configuration, le cas échéant.

Procédure

1. Ouvrez une invite de commande.
2. Accédez au répertoire *SKLM_INSTALL_HOME*\agent.

   Windows
   `C:\Program Files\IBM\SKLMV301\agent`

   Linux `/opt/IBM/SKLMV301/agent`
3. Arrêtez le service d'agent avec la commande suivante :

   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. Démarrez le service d'agent avec la commande suivante :

   Windows
   `startAgent.bat WAS_HOME`
   `startAgent.bat "C:\Program Files\IBM\WebSphere\AppServer"`

   Linux
   `./startAgent.sh WAS_HOME`
   `./startAgent.sh /opt/IBM/WebSphere/AppServer`

Agent Starter

Le service Agent Starter dans le cluster multimaître d'IBM Security Key Lifecycle Manager permet de démarrer l'agent de surveillance.

Lorsque l'agent dans un maître IBM Security Key Lifecycle Manager est arrêté, le service Agent Invoker exécute le script Agent Starter `startAgent` pour redémarrer le service. Le fichier `agentStarter.properties` contient les informations nécessaires à l'exécution du script.

Emplacement du script et du fichier de propriétés

Le script `startAgent` et le fichier `agentStarter.properties` se trouvent dans le répertoire *SKLM_INSTALL_HOME*\agent. Par exemple,

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`

Démarrage du service d'agent

Exécutez la commande suivante :

Windows

```
startAgent.bat WAS_HOME
startAgent.bat "C:\Program Files\IBM\WebSphere\AppServer"
```

Linux

```
./startAgent.sh WAS_HOME
./startAgent.sh /opt/IBM/WebSphere/AppServer
```

Exemple de fichier de propriétés Agent Starter

```
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
```

Les valeurs possibles pour le paramètre **SERVICE** sont `PortMonitoring`, `AgentMonitoring`, `TakeOverService` ou `DataSynchronizeService`.

Agent Invoker

Le service Agent Invoker au sein d'un maître IBM Security Key Lifecycle Manager surveille le statut de l'agent à intervalles réguliers.

Le service Agent Invoker s'exécute automatiquement sur tous les maîtres IBM Security Key Lifecycle Manager du cluster multimaître. Lorsque l'application IBM Security Key Lifecycle Manager est démarrée, le service Agent Invoker vérifie si le service s'exécute à intervalles réguliers. Si le service Agent est arrêté, le service Agent Invoker redémarre l'agent en utilisant le service Agent Starter.

Vous pouvez utiliser la propriété **agent.invoker.polling.interval** dans le fichier <*SKLM_HOME*>\config\SKLMConfig.properties, par exemple C:\Program Files\IBM\WebSphere\AppServer\products\sklm\config\SKLMConfig.properties,

pour configurer la fréquence d'exécution du service de surveillance de l'agent. Pour plus d'informations sur la propriété de configuration, voir agent.invoker.polling.interval.

Stop Agent

Le service Stop Agent se trouvant dans le cluster multimaître IBM Security Key Lifecycle Manager est utilisé pour arrêter l'agent de surveillance.

L'agent arrêté redémarre automatiquement lorsque le service Agent Invoker est en cours d'exécution.

Emplacement du fichier script `stopAgent`

Le fichier script `stopAgent` se trouve dans le répertoire *SKLM_INSTALL_HOME*`\agent`. Par exemple,

Windows

```
C:\Program Files\IBM\SKLMV301\agent\stopAgent.bat
```

Linux `opt/IBM/SKLMV301/agent/stopAgent.sh`

Arrêt du service d'agent

Exécutez la commande suivante :

Windows

```
stopAgent.bat WAS_HOME
stopAgent.bat "C:\Program Files\IBM\WebSphere\AppServer"
```

Linux

```
./stopAgent.sh WAS_HOME
./stopAgent.sh /opt/IBM/WebSphere/AppServer
```

Arrêt permanent de l'agent

Vous pouvez arrêter un agent de manière permanente. Lorsqu'un agent est arrêté de manière permanente, il ne redémarre pas automatiquement lorsque le service Agent Invoker s'exécute.

Pour arrêter l'agent de manière permanente, procédez comme suit :

1. Dans le fichier `SKLMConfig.properties`, mettez à jour la propriété **`stopAgentInvocation`** sur la valeur `true`.

   ```
   stopAgentInvocation=true
   ```

2. Arrêtez l'agent. Voir la section «Arrêt permanent de l'agent».

Remarque : N'arrêtez pas l'agent de manière permanente dans une configuration multimaître. Vous pouvez le faire sur un serveur IBM Security Key Lifecycle Manager autonome ou dans une configuration de réplication.

Pour démarrer un agent qui a été arrêté de manière permanente, procédez comme suit :

1. Dans le fichier `SKLMConfig.properties`, mettez à jour la propriété **`stopAgentInvocation`** sur la valeur `false`.

   ```
   stopAgentInvocation=false
   ```

Vous pouvez utiliser la commande CLI tklmConfigUpdateEntry ou Service REST Update Config Property pour mettre à jour le fichier `SKLMConfig.properties`.

2. Redémarrez WebSphere Application Server.

Exigences et remarques relatives à la configuration multimaître

Avant de configurer l'environnement multimaître d'IBM Security Key Lifecycle Manager, prenez connaissances des exigences et des remarques ci-après pour garantir la réussite de l'opération.

- Assurez-vous que les ports KMIP, SSL, TCP et de l'agent ne sont pas bloqués pour la communication avant de configurer des serveurs maîtres IBM Security Key Lifecycle Manager pour la configuration multimaître.
- Assurez-vous que le port de l'agent (60015) et le port HADR (60025) qui sont utilisés pour la configuration multimaître ne sont pas bloqués par le pare-feu.

  Le port de l'agent par défaut est 60015, et vous pouvez le mettre à jour dans l'interface utilisateur. Le port HADR par défaut est 60025 ; il est affecté au cours de la configuration multimaître et peut être configuré.
- L'architecture multimaître d'IBM Security Key Lifecycle Manager s'appuie sur la technologie HADR (fonction de reprise à haute disponibilité après incident de DB2) pour implémenter une solution à haute disponibilité. Par conséquent, toutes les règles et instructions de configuration de la fonction DB2 HADR s'appliquent à la configuration multimaître d'IBM Security Key Lifecycle Manager.
- Vérifiez que les maîtres IBM Security Key Lifecycle Manager utilisant des systèmes hôte pour les bases de données DB2 HADR principale et de secours possèdent les mêmes niveaux de système d'exploitation et de groupe de correctifs.
- Le nom d'utilisateur et le mot de passe DB2 doivent être les mêmes sur tous les maîtres du cluster multimaître IBM Security Key Lifecycle Manager.
- L'instance IBM Security Key Lifecycle Manager que vous souhaitez ajouter au cluster multimaître ne doit pas contenir de données. L'ajout d'un serveur maître contenant des données entraîne la perte des données qui ont été créées précédemment.
  - Si vous voulez ajouter une instance IBM Security Key Lifecycle Manager existante dans le cluster, utilisez la fonction d'exportation et d'importation de groupe d'unités. Voir «Ajout d'une instance d'IBM Security Key Lifecycle Manager existante contenant des données dans le cluster multimaître», à la page 260 pour plus de détails.
- Une interface TCP/IP doit être disponible entre les systèmes hôte des bases de données DB2 HADR principale et de secours, avec une bande passante du réseau dédiée, à vitesse et à capacité élevées.
- Pour le déploiement multimaître IBM Security Key Lifecycle Manager, le cluster doit inclure au moins un maître principal et un maître de secours. Lorsque vous configurez un cluster multimaître IBM Security Key Lifecycle Manager, le serveur à partir duquel vous ajoutez un noeud maître ou de secours au cluster devient le maître principal. Vous devez ajouter un noeud de secours au cluster avant d'ajouter d'autres maîtres.
- Un certificat serveur doit être créé dans une instance IBM Security Key Lifecycle Manager pour que celle-ci puisse être ajoutée au cluster en tant que maître principal.

- Le cluster multimaître IBM Security Key Lifecycle Manager prend en charge jusqu'à trois maîtres de secours. Lorsque vous ajoutez des noeuds de secours au cluster, la valeur d'index de priorité doit être comprise entre 1 et 3.
- Après la configuration multimaître IBM Security Key Lifecycle Manager, vous devez éviter d'exécuter des opérations de sauvegarde manuelle et de restauration à partir d'un des maîtres du cluster.
- Exécutez les opérations de configuration multimaître IBM Security Key Lifecycle Manager uniquement à partir du maître principal du cluster afin d'éviter tout problème.
- Pour que vous puissiez ajouter un maître au cluster multimaître IBM Security Key Lifecycle Manager sur un système d'exploitation Linux, les droits du répertoire `/tmp` doivent être 277, ce qui correspond aux droits complets d'exécution, de lecture et d'écriture.
- Avant d'ajouter un serveur maître au cluster, exécutez **Check Prerequisites REST Service** pour vérifier si le maître répond à toutes les exigences. Pour plus d'informations sur le service REST, voir Service REST Check Prerequisites.
- Si vous voulez définir la configuration multimaître IBM Security Key Lifecycle Manager en vue de l'utilisation de l'outil HSM (Hardware Security Module) pour stocker la clé principale, vous devez configurer tous les maîtres dans le cluster afin d'utiliser le même outil HSM.
- Avant d'ajouter un serveur maître au cluster via le système migré, vous devez modifier le nom d'utilisateur et le mot de passe de l'administrateur d'IBM Security Key Lifecycle Manager dans les cas suivants :
  1. Lorsque les utilisateurs et les groupes sont migrés depuis une version précédente vers la version 3.0.1 via le processus de migration croisée.
  2. Lorsque le nom et le mot de passe de l'administrateur d'IBM Security Key Lifecycle Manager sont différents de ceux des données d'identification spécifiées au cours de l'installation de la version 3.0.1.
- Vous ne pouvez pas retirer de serveur de secours ou maître du cluster multimaître lorsqu'un serveur de secours est arrêté.

Mappage d'adresse IP et de nom d'hôte

Vous devez vous assurer que le nom d'hôte de votre ordinateur est configuré correctement avant de configurer des maîtres IBM Security Key Lifecycle Manager pour la configuration multimaître. Vous pouvez résoudre une adresse IP en nom d'hôte en éditant le fichier `etc/hosts`.

Pour la configuration Db2 HADR, vous devez mettre à jour le fichier `etc/hosts` sur les serveurs des maîtres principal et de secours du cluster afin de permettre le mappage du nom d'hôte à une adresse IP.

Emplacement du fichier hôte

Windows

```
C:\Windows\System32\Drivers\etc\
```

Linux `/etc/hosts`

L'exemple suivant illustre le mappage de l'adresse IP à un nom d'hôte dans le fichier `etc/hosts` :

```
# 127.0.0.1 localhost
# ::1 localhost
9.199.138.209 sklmver3
```

Ajout d'un maître de secours au cluster

Dans IBM Security Key Lifecycle Manager, la solution à haute disponibilité est implémentée à l'aide d'une configuration de cluster multimaître. Le cluster multimaître d'IBM Security Key Lifecycle Manager doit inclure un maître principal et un maître de secours. Ajoutez un maître de secours au cluster pour la configuration d'un environnement multimaître.

Avant de commencer

Avant d'ajouter un maître de secours au cluster, consultez les remarques et les restrictions répertoriées dans la rubrique Exigences et remarques relatives à la configuration multimaître.

Exécutez le Service REST Check Prerequisites pour vérifier si le maître à ajouter satisfait les exigences et remplit les conditions qui sont définies pour la configuration multimaître d'IBM Security Key Lifecycle Manager.

Pourquoi et quand exécuter cette tâche

La configuration de la fonction de reprise à haute disponibilité après incident (HADR) de Db2 est utilisée pour garantir la disponibilité continue des données pour toutes les instances d'IBM Security Key Lifecycle Manager dans un cluster multimaître. Db2 HADR est une fonction de réplication de base de données qui offre une solution à haute disponibilité. HADR vous protège contre la perte de données en répliquant les modifications d'une base de données source (principale) dans une base de données cible (de secours). Db2 HADR prend en charge jusqu'à trois bases de données de secours dans votre configuration multimaître.

Lorsque vous créez un cluster multimaître IBM Security Key Lifecycle Manager, le serveur à partir duquel vous ajoutez un noeud maître ou de secours au cluster devient le maître principal. Une fois que le cluster est créé avec au moins un maître principal et un maître de secours, vous pouvez ajouter des maîtres au cluster à partir d'un des maîtres du cluster. Utilisez la boîte de dialogue Configuration multimaître - Ajouter un maître ou le **`service REST Add Master`** pour ajouter un maître au cluster. Votre rôle doit disposer du droit permettant d'ajouter un maître de secours au cluster multimaître d'IBM Security Key Lifecycle Manager.

Vous ne pouvez pas ajouter un maître de secours au cluster depuis la page Configuration multimaître - Ajouter un maître lorsqu'un serveur de secours ou maître est hors du réseau ou inaccessible. Pour ajouter un maître de secours dans ce scénario, vous devez utiliser le **`service REST Add Master`** avec des paramètres supplémentaires. Pour plus d'informations sur le service REST, voir Service REST pour l'ajout d'un maître lorsqu'un autre maître dans le cluster n'est pas accessible.

Procédure

1. Accédez à la page ou au répertoire approprié.

   Interface graphique

   a. Connectez-vous à l'interface graphique.
   b. Sur la page Bienvenue, cliquez sur **Administration** > **Multimaître** > **Maîtres** > **Ajouter un maître**.

   Interface REST

   Ouvrez un client REST.

2. Ajoutez un maître de secours au cluster.

Interface graphique

a. Cliquez sur l'onglet **Propriétés de base**.

b. Dans la boîte de dialogue Propriétés de base, indiquez des informations sur le maître de secours que vous ajoutez.

Adresse IP/Nom d'hôte	Indiquez le nom d'hôte de l'instance IBM Security Key Lifecycle Manager ajoutée au cluster.
Nom d'utilisateur IBM Security Key Lifecycle Manager	Indiquez le nom de l'administrateur IBM Security Key Lifecycle Manager. Le nom de l'administrateur s'affiche par défaut.
Mot de passe IBM Security Key Lifecycle Manager	Indiquez le mot de passe de l'administrateur du serveur IBM Security Key Lifecycle Manager.
Nom d'utilisateur WebSphere Application Server	Indiquez l'ID utilisateur de connexion WebSphere Application Server pour le profil de l'administrateur de serveur IBM Security Key Lifecycle Manager. L'ID de connexion WebSphere Application Server s'affiche par défaut.
Mot de passe WebSphere Application Server	Indiquez le mot de passe de l'ID utilisateur de connexion WebSphere Application Server.
Port d'interface utilisateur	Indiquez le port HTTPS pour accéder aux services REST et à l'interface utilisateur graphique IBM Security Key Lifecycle Manager. Le numéro de port s'affiche par défaut.

c. Cliquez sur l'onglet **Propriétés avancées**.

d. Dans la boîte de dialogue Propriétés avancées, indiquez les informations pour le maître de secours que vous ajoutez.

Voulez-vous définir ce maître comme base de données de secours ?	Sélectionnez **Oui** pour ajouter au cluster l'instance en cours d'IBM Security Key Lifecycle Manager comme maître de secours.
Port HADR	Indiquez le numéro de port pour la base de données HADR de secours afin de communiquer avec la base de données HADR principale.
Index de priorité de secours	Indiquez la valeur de l'index de priorité pour que la base de données de secours prenne le relais lorsque la base de données principale est arrêtée. Vous pouvez attribuer une valeur comprise entre 1 et 3 pour l'index de priorité. Le serveur de secours avec un niveau d'index de priorité plus élevé (nombre plus faible) est prioritaire par rapport aux bases de données de priorité inférieure.

e. Cliquez sur **Test de connexion** pour tester la communication entre le maître que vous ajoutez et le maître principal en cours. Pour plus d'informations, voir Exécution d'un test de connexion.

f. Cliquez sur **Ajouter**.

Interface REST

a. Obtenez un identificateur d'authentification utilisateur unique pour accéder aux services REST d'IBM Security Key Lifecycle Manager. Pour plus d'informations sur le processus d'authentification, voir Processus d'authentification pour les services REST.

b. Pour exécuter le **`service REST Add Master`**, envoyez la demande HTTP POST. Transmettez l'identificateur d'authentification utilisateur que vous avez obtenu à l'`étape a` avec le message de demande, conformément à l'exemple suivant :

```
POST https://localhost:<port>/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"
}
]
```

Que faire ensuite

Le maître principal redémarre et est temporairement indisponible au cours du processus après l'ajout du maître de secours au cluster. Vérifiez que le maître de secours avec ses informations d'état de santé est répertorié dans la table Maîtres ainsi que sur la page d'accueil d'IBM Security Key Lifecycle Manager.

Ajout d'un maître au cluster

Dans IBM Security Key Lifecycle Manager, la solution à haute disponibilité est implémentée à l'aide d'une configuration de cluster multimaître. L'ajout d'un maître au cluster fait partie du processus de configuration d'un environnement multimaître.

Avant de commencer

Procédez comme suit :

- Consultez les remarques et les restrictions répertoriées dans la rubrique Exigences et remarques relatives à la configuration multimaître.
- Exécutez le Service REST Check Prerequisites pour vérifier si le maître à ajouter satisfait les exigences et remplit les conditions qui sont définies pour la configuration multimaître d'IBM Security Key Lifecycle Manager.
- Avant d'ajouter un serveur maître non HADR au cluster multimaître, assurez-vous qu'au moins un maître de secours est ajouté au cluster. Pour obtenir des instructions sur l'ajout d'un maître de secours, voir «Ajout d'un maître de secours au cluster», à la page 256.

Pourquoi et quand exécuter cette tâche

Lorsque vous créez un cluster multimaître IBM Security Key Lifecycle Manager, le serveur à partir duquel vous ajoutez un noeud maître ou de secours au cluster devient le maître principal. Une fois que le cluster est créé avec au moins un maître principal et un maître de secours, vous pouvez ajouter des maîtres au cluster à partir d'un des maîtres du cluster. Utilisez la page Configuration multimaître - Ajouter un maître ou le **service REST Add Master** pour ajouter un maître au cluster. Votre rôle doit disposer du droit permettant d'ajouter un maître au cluster multimaître d'IBM Security Key Lifecycle Manager.

Vous ne pouvez pas ajouter un maître au cluster depuis la page Configuration multimaître - Ajouter un maître lorsqu'un serveur de secours ou maître est hors du réseau ou inaccessible. Pour ajouter un maître dans ce scénario, vous devez utiliser le **service REST Add Master** avec des paramètres supplémentaires. Pour plus d'informations sur le service REST, voir Service REST pour l'ajout d'un maître lorsqu'un autre maître dans le cluster n'est pas accessible.

Procédure

1. Accédez à la page ou au répertoire approprié.

   Interface graphique

   a. Connectez-vous à l'interface graphique.

   b. Sur la page Bienvenue, cliquez sur **Administration** > **Multimaître** > **Maîtres** > **Ajouter un maître**.

   Interface REST

   Ouvrez un client REST.

2. Ajoutez un maître au cluster.

   Interface graphique

   a. Cliquez sur l'onglet **Propriétés de base**.

   b. Dans la boîte de dialogue Propriétés de base, indiquez des informations sur le maître que vous ajoutez.

Adresse IP/Nom d'hôte	Indiquez le nom d'hôte de l'instance IBM Security Key Lifecycle Manager ajoutée au cluster.
Nom d'utilisateur IBM Security Key Lifecycle Manager	Indiquez le nom de l'administrateur IBM Security Key Lifecycle Manager. Le nom de l'administrateur s'affiche par défaut.
Mot de passe IBM Security Key Lifecycle Manager	Indiquez le mot de passe de l'administrateur du serveur IBM Security Key Lifecycle Manager.
Nom d'utilisateur WebSphere Application Server	Indiquez l'ID utilisateur de connexion WebSphere Application Server pour le profil de l'administrateur de serveur IBM Security Key Lifecycle Manager. L'ID de connexion WebSphere Application Server s'affiche par défaut.
Mot de passe WebSphere Application Server	Indiquez le mot de passe de l'ID utilisateur de connexion WebSphere Application Server.
Port d'interface utilisateur	Indiquez le port HTTPS pour accéder aux services REST et à l'interface utilisateur graphique IBM Security Key Lifecycle Manager. Le numéro de port s'affiche par défaut.

   c. Cliquez sur **Test de connexion** pour tester la communication entre le maître que vous ajoutez et le serveur maître principal. Pour plus d'informations, voir Exécution d'un test de connexion.

   d. Cliquez sur **Ajouter**.

   Interface REST

   a. Obtenez un identificateur d'authentification utilisateur unique pour accéder aux services REST d'IBM Security Key Lifecycle Manager.

Pour plus d'informations sur le processus d'authentification, voir Processus d'authentification pour les services REST.

b. Pour exécuter le **service REST Add Master**, envoyez la demande HTTP POST. Transmettez l'identificateur d'authentification utilisateur que vous avez obtenu à l'étape a avec le message de demande, conformément à l'exemple suivant :

```
POST https://localhost:<port>/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"
}
]
```

Que faire ensuite

Le maître principal redémarre et est temporairement indisponible au cours du processus après l'ajout du maître au cluster. Vérifiez que le maître avec ses informations d'état de santé est répertorié dans la table Maîtres ainsi que sur la page d'accueil d'IBM Security Key Lifecycle Manager.

Ajout d'une instance d'IBM Security Key Lifecycle Manager existante contenant des données dans le cluster multimaître

Vous pouvez utiliser la fonction d'exportation et d'importation d'IBM Security Key Lifecycle Manager pour ajouter des données depuis une instance d'IBM Security Key Lifecycle Manager existante dans le cluster multimaître. Vous devez importer les données qui ont été exportées depuis l'instance autonome existante sur le serveur maître principal qui est configuré avec Db2 HADR.

Pourquoi et quand exécuter cette tâche

Vous ne pouvez pas ajouter directement une instance autonome existante contenant des données dans le cluster. Vous devez d'abord importer les données depuis l'instance d'IBM Security Key Lifecycle Manager existante sur le maître principal. Ensuite, ajoutez un serveur maître dans le cluster séparément.

Une fois les données importées, elles sont disponibles sur toutes les instances dans le cluster. C'est à vous de décider s'il est nécessaire d'ajouter un maître séparément.

Procédure

1. Exportez les données du groupe d'unités depuis l'instance d'IBM Security Key Lifecycle Manager existante. Pour plus d'informations sur l'exportation des données de groupe d'unités, voir «Exportation d'un groupe d'unités», à la page 118.

2. Importez les données qui ont été exportées depuis l'instance autonome existante sur le serveur maître principal qui est configuré avec Db2 HADR. Pour plus d'informations sur l'importation des données de groupe d'unités, voir «Importation d'un groupe d'unités», à la page 120.
3. Une fois les données importées sur le serveur principal, vous pouvez y accéder depuis tous les maîtres dans le cluster. Si vous avez besoin d'un maître IBM Security Key Lifecycle Manager dédié pour accéder aux données importées, ajoutez un maître au cluster. Pour plus d'informations sur l'ajout d'un maître, voir «Ajout d'un maître au cluster», à la page 258.

Que faire ensuite

Vous pouvez mettre hors service l'instance d'IBM Security Key Lifecycle Manager autonome existante une fois les données exportées.

Modification des détails du maître d'un cluster

Vous pouvez changer la configuration multimaître d'IBM Security Key Lifecycle Manager en fonction de vos besoins (modification des détails du serveur maître, par exemple). Par exemple, vous pouvez mettre à jour le mot de passe de l'administrateur d'IBM Security Key Lifecycle Manager.

Avant de commencer

Avant de modifier les détails du maître dans le cluster, consultez les remarques et les restrictions répertoriées dans la rubrique Exigences et remarques relatives à la configuration multimaître.

Pourquoi et quand exécuter cette tâche

Utilisez la boîte de dialogue Configuration multimaître - Modifier un maître ou le **`service REST Modify Master`** pour modifier les détails du maître.

Votre rôle doit disposer du droit permettant de modifier les détails d'un serveur maître dans le cluster multimaître IBM Security Key Lifecycle Manager.

Avant d'ajouter un serveur maître au cluster via le système migré, vous devez modifier le nom d'utilisateur et le mot de passe de l'administrateur d'IBM Security Key Lifecycle Manager dans les cas suivants :

1. Lorsque des utilisateurs et des groupes sont migrés depuis une version précédente vers la version 3.0.1 via le processus de migration croisée.
2. Lorsque le nom et le mot de passe de l'administrateur d'IBM Security Key Lifecycle Manager sont différents de ceux des données d'identification spécifiées au cours de l'installation de la version 3.0.1.

Procédure

1. Accédez à la page ou au répertoire approprié.

   Interface graphique

   a. Connectez-vous à l'interface graphique.
   b. Sur la page Bienvenue, cliquez sur **Administration** > **Multimaître** > **Maîtres**.

   Interface REST

   Ouvrez un client REST.
2. Modifiez les détails du maître.

Interface graphique

a. Dans la table **Maîtres**, sélectionnez le maître à modifier.
b. Cliquez sur l'onglet **Modifier le maître**. Vous pouvez également cliquer deux fois sur l'entrée de maître sélectionnée.
c. Dans la boîte de dialogue Configuration multimaître - Modifier un maître, modifiez les détails du maître, lorsque cela est nécessaire.
d. Cliquez sur **Test de connexion** pour tester la communication entre le maître que vous modifiez et le serveur principal actuel. Pour plus d'informations, voir Exécution d'un test de connexion.
e. Cliquez sur **Mettre à jour**.

Interface REST

a. Obtenez un identificateur d'authentification utilisateur unique pour accéder aux services REST d'IBM Security Key Lifecycle Manager. Pour plus d'informations sur le processus d'authentification, voir Processus d'authentification pour les services REST.
b. Pour exécuter le **service REST Modify Master**, envoyez la demande HTTP POST. Transmettez l'identificateur d'authentification utilisateur que vous avez obtenu à l'étape a avec le message de demande, conformément à l'exemple suivant :

```
POST https://localhost:<port>/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",
}
]
```

Que faire ensuite

Vérifiez les informations d'état de santé du maître modifié dans la table Maîtres ainsi que sur la page d'accueil d'IBM Security Key Lifecycle Manager.

Exécution d'un test de connexion

Une fois que vous avez défini les paramètres d'ajout ou de modification d'un maître IBM Security Key Lifecycle Manager, effectuez un test de connexion afin de vérifier que les informations de connexion sont correctes.

Pour effectuer un test de connexion, cliquez sur **Test de connexion** sur la page Configuration multimaître. Si une erreur est alors générée, vérifiez les paramètres suivants. Testez ensuite à nouveau la connexion.

- Vérifiez si le serveur maître IBM Security Key Lifecycle Manager est accessible.
- Vérifiez si le nom d'hôte du serveur maître IBM Security Key Lifecycle Manager est correct.
- Vérifiez si les données d'identification utilisateur pour le maître IBM Security Key Lifecycle Manager sont correctes.
- Vérifiez si le port HTTP est activé.

Retrait d'un maître du cluster multimaître

Vous pouvez retirer un maître qui n'est plus requis dans le cluster multimaître d'IBM Security Key Lifecycle Manager.

Avant de commencer

Avant de supprimer les détails du maître dans le cluster, consultez les remarques et les restrictions répertoriées dans la rubrique Exigences et remarques relatives à la configuration multimaître.

Pourquoi et quand exécuter cette tâche

Vous ne pouvez pas supprimer un maître principal du cluster. Vous pouvez supprimer un maître de secours uniquement lorsque le cluster contient plusieurs éléments de secours. Le cluster multimaître d'IBM Security Key Lifecycle Manager prend en charge jusqu'à trois éléments de secours.

Utilisez la page IBM Security Key Lifecycle Manager - Multimaître ou le **service REST Remove Master** pour supprimer un maître.

Votre rôle doit disposer du droit permettant de supprimer un maître du cluster.

Procédure

1. Accédez à la page ou au répertoire approprié.

   Interface graphique

   a. Connectez-vous à l'interface graphique.
   b. Sur la page Bienvenue, cliquez sur **Administration** > **Multimaître**.

   Interface REST

   Ouvrez un client REST.

2. Supprimez les détails du maître.

   Interface graphique

   a. Dans la table **Maîtres**, sélectionnez le maître à supprimer.
   b. Cliquez sur **Supprimer le maître**.
   c. Dans la boîte de dialogue Confirmer, lisez le message de confirmation avant de supprimer le maître.
   d. Cliquez sur **OK**.

   Interface REST

   a. Obtenez un identificateur d'authentification utilisateur unique pour accéder aux services REST d'IBM Security Key Lifecycle Manager. Pour plus d'informations sur le processus d'authentification, voir Processus d'authentification pour les services REST.
   b. Pour exécuter le **service REST Remove Master**, envoyez la demande HTTP POST. Transmettez l'identificateur d'authentification utilisateur que vous avez obtenu à l'étape a avec le message de demande, conformément à l'exemple suivant :

```
POST https://localhost:<port>/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. Redémarrez WebSphere Application Server pour actualiser la configuration.

Que faire ensuite

Vérifiez que le maître que vous avez supprimé ne se trouve plus dans la table Maîtres.

Promotion du serveur de secours en serveur principal

Si un maître principal du cluster multimaître IBM Security Key Lifecycle Manager est défaillant, vous pouvez souhaiter promouvoir un maître de secours pendant que vous résolvez le problème.

Avant de commencer

Avant de promouvoir un maître de secours dans le cluster, consultez les remarques et les restrictions répertoriées dans la rubrique Exigences et remarques relatives à la configuration multimaître.

Pourquoi et quand exécuter cette tâche

Si le maître principal devient indisponible, utilisez la page **IBM Security Key Lifecycle Manager - Multimaître** > **Bases de données HADR** ou le **service REST Promote Standby** pour faire en sorte qu'un maître de secours devienne le maître principal dans le cluster.

Votre rôle doit disposer du droit permettant de changer un maître de secours en maître principal dans le cluster multimaître IBM Security Key Lifecycle Manager.

Vous devez redémarrer WebSphere Application Server manuellement sur tous les serveurs de secours si une base de données de secours auxiliaire devient la base de données principale. Il n'est pas nécessaire de redémarrer WebSphere Application Server lorsque la base de données de secours principal devient la base de données principale.

Procédure

1. Accédez à la page ou au répertoire approprié.

   Interface graphique

   a. Connectez-vous à l'interface graphique.
   b. Sur la page Bienvenue, cliquez sur **Administration** > **Multimaître** > **Bases de données HADR**.

   Interface REST

   Ouvrez un client REST.

2. Effectuez la promotion du maître de secours en serveur maître principal.

   Interface graphique

   a. Dans la table **Bases de données HADR**, sélectionnez le maître de secours à promouvoir.

b. Cliquez sur **Promouvoir comme principal**.
c. Dans la boîte de dialogue Confirmer, lisez le message de confirmation avant de promouvoir le maître de secours.
d. Cliquez sur **OK**.

Interface REST

a. Obtenez un identificateur d'authentification utilisateur unique pour accéder aux services REST d'IBM Security Key Lifecycle Manager. Pour plus d'informations sur le processus d'authentification, voir Processus d'authentification pour les services REST.
b. Pour exécuter le **service REST Promote Standby**, envoyez la demande HTTP POST. Transmettez l'identificateur d'authentification utilisateur que vous avez obtenu à l'étape a avec le message de demande, conformément à l'exemple suivant :

```
POST https://localhost:<port>/SKLM/rest/v1/ckms/config/nodes/takeoverAsPrimary
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth userAuthId=139aeh34567m
[
{clusterName:"multimaster"},
{"ipHostname": "civ3cez160"}
]
```

Que faire ensuite

Vérifiez les informations de rôle et d'état de santé du maître de secours promu dans la table Bases de données HADR ainsi que sur la page d'accueil IBM Security Key Lifecycle Manager.

Affichage de la liste des serveurs maîtres et de leur statut de configuration

Vous pouvez afficher la liste des serveurs maîtres IBM Security Key Lifecycle Manager ainsi que leur état de santé dans le cluster multimaître afin d'identifier plus facilement les problèmes éventuels dans les maîtres. Vous pouvez également afficher le statut de configuration Db2 HADR des maîtres, qu'ils soient principaux ou de secours.

Pourquoi et quand exécuter cette tâche

Dans un cluster multimaître, la surveillance régulière de l'état de santé des instances IBM Security Key Lifecycle Manager est essentielle pour pouvoir identifier rapidement les problèmes et les résoudre. Vous pouvez vérifier si tous les ports de communication sont actifs et accessibles sur chaque serveur maître de votre déploiement multimaître.

Utilisez la page Multimaître d'IBM Security Key Lifecycle Manager ou le **service REST Get All Masters Status** pour afficher la liste des serveurs et leur statut.

Vous pouvez également afficher la liste des maîtres et les informations de statut sur la page d'accueil d'IBM Security Key Lifecycle Manager.

Procédure

1. Accédez à la page ou au répertoire approprié.

   Interface graphique

   a. Connectez-vous à l'interface graphique.

b. Sur la page Bienvenue, cliquez sur **Administration** > **Multimaître**.

Interface REST

Ouvrez un client REST.

2. Affichez la liste des serveurs et les informations de statut pour identifier les problèmes, s'il en existe.

Interface graphique

Le statut de configuration Db2 HADR s'affiche sur la page Multimaître d'IBM Security Key Lifecycle Manager.

a. Cliquez sur l'onglet **Maîtres** pour afficher la liste des maîtres configurés pour la réplication multimaître ainsi que leur statut de configuration.

b. Cliquez sur l'onglet **Bases de données HADR** pour afficher la liste des maîtres configurés avec Db2 HADR et leur statut de configuration.

Interface REST

a. Obtenez un identificateur d'authentification utilisateur unique pour accéder aux services REST d'IBM Security Key Lifecycle Manager. Pour plus d'informations sur le processus d'authentification, voir Processus d'authentification pour les services REST.

b. Pour exécuter le **service REST Get All Masters Status**, envoyez la demande HTTP POST. Transmettez l'identificateur d'authentification utilisateur que vous avez obtenu à l'étape a avec le message de demande, conformément à l'exemple suivant :

```
GET https://localhost:<port>/SKLM/rest/v1/ckms/nodes/allNodeStatus
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth userAuthId=139aeh34567m
Accept-Language : en
```

Pour plus d'informations, voir Service REST Get All Masters Status.

Que faire ensuite

Utilisez les informations de statut de la table afin d'examiner les problèmes, s'il en existe, et d'effectuer les actions nécessaires.

Affichage des informations récapitulatives d'un maître

Utilisez la page Détails du maître pour afficher les détails d'un serveur maître sélectionné dans le cluster multimaître IBM Security Key Lifecycle Manager afin de pouvoir mieux comprendre et utiliser les données de configuration.

Procédure

1. Connectez-vous à l'interface graphique.
2. Cliquez sur **Administration** > **Multimaître** sur la page Bienvenue.
3. Sélectionnez un serveur maître répertorié.
4. Cliquez avec le bouton droit de la souris sur le serveur maître puis sélectionnez **Récapitulatif** ou cliquez deux fois sur l'entrée du maître.

   Le tableau suivant fournit les informations récapitulatives.

IPP	Port sur lequel le serveur IBM Security Key Lifecycle Manager écoute les demandes des unités qui communiquent via le protocole IPP (IBM Proprietary Protocol).

SSL	Port sur lequel le serveur IBM Security Key Lifecycle Manager écoute les demandes des unités qui communiquent via le protocole SSL.
Interface utilisateur d'administration	Port WebSphere Application Server pour le profil IBM Security Key Lifecycle Manager.
Interface utilisateur de l'application	Port HTTPS permettant d'accéder aux services REST et à l'interface utilisateur graphique IBM Security Key Lifecycle Manager.
KMIP	Port sur lequel le serveur IBM Security Key Lifecycle Manager écoute les demandes pour communiquer via le socket SSL qui utilise le protocole KMIP (Key Management Interoperability Protocol).
Base de données	Port sur lequel le serveur IBM Security Key Lifecycle Manager écoute les demandes provenant de Db2.
Port HADR	Port des bases de données configurées en tant qu'élément HADR pour les communications de base de données.
Agent	Port sur lequel l'agent écoute les communications d'IBM Security Key Lifecycle Manager.

5. Cliquez sur **OK** pour fermer la page Récapitulatif.

Configuration d'un maître isolé en tant que maître en lecture/écriture

En raison de problèmes de connectivité/réseau, un serveur maître n'arrive pas à communiquer avec les autres maîtres du cluster et est isolé de ce dernier. Vous pouvez alors configurer ce maître isolé avec sa base de données locale en mode lecture/écriture. Une fois cette configuration effectuée, toutes les unités et les clients KMIP enregistrés sur le maître isolé peuvent communiquer en toute transparence avec le serveur sans qu'il soit nécessaire de changer leur configuration.

Avant de commencer

Avant de définir un maître isolé de telle sorte qu'il soit en lecture/écriture, consultez les remarques et les restrictions répertoriées dans la rubrique Exigences et remarques relatives à la configuration multimaître.

Pourquoi et quand exécuter cette tâche

Une fois la configuration en mode lecture/écriture effectuée, vous pouvez ajouter de nouveaux unités et clients KMIP au serveur et le maître en lecture/écriture peut alors les servir. Toutefois, un ensemble de restrictions s'applique aux fonctions et aux interfaces du maître en lecture/écriture isolé. Toutes les opérations de suppression et de modification sur les groupes d'unités, les groupes de clés, les clients KMIP et les objets gérés sont désactivées afin de garantir la cohérence des données au cas où le maître isolé serait à nouveau intégré au cluster multimaître. Les fonctions administratives, telles que la réplication, la configuration multimaître et la restauration des fichiers de sauvegarde, sont également restreintes.

Procédure

1. Accédez à la page appropriée.

   Interface graphique

   a. Connectez-vous à l'interface graphique utilisateur du maître isolé.

Interface REST

a. Ouvrez un client REST.

2. Configurez le maître isolé en tant que maître en lecture/écriture.

Interface graphique

a. Cliquez sur le lien permettant de définir ce maître en lecture/écriture dans la zone de notification de la page Bienvenue d'IBM Security Key Lifecycle Manager.

b. Dans la boîte de dialogue Confirmer, lisez le message de confirmation avant de configurer le maître isolé en mode lecture/écriture.

c. Cliquez sur **OK**.

Interface REST

a. Obtenez un identificateur d'authentification utilisateur unique pour accéder aux services REST d'IBM Security Key Lifecycle Manager. Pour plus d'informations sur le processus d'authentification, voir Processus d'authentification pour les services REST.

b. Pour exécuter le **service REST Set Up Read-Write Master**, envoyez la demande HTTP GET. Transmettez l'identificateur d'authentification utilisateur que vous avez obtenu à l'étape a avec le message de demande, conformément à l'exemple suivant :

```
GET https://localhost:<port>/SKLM/rest/v1/ckms/config/nodes/setupAsReadWriteMaster
Content-Type: application/json
Accept : application/json
Authorization: SKLMAuth userAuthId=139aeh34567m
Accept-Language : en
```

Intégration du maître en lecture/écriture au cluster

Le serveur maître qui était isolé du cluster multimaître, et configuré comme maître en lecture/écriture, peut rejoindre le cluster une fois les problèmes de connectivité/réseau résolus. Les données du maître en lecture/écriture isolé sont fusionnées dans la base de données principale du cluster lors de ce processus.

Avant de commencer

Avant d'intégrer le maître en lecture/écriture isolé au cluster, prenez connaissance des remarques et des restrictions répertoriées dans la rubrique Exigences et remarques relatives à la configuration multimaître.

Pourquoi et quand exécuter cette tâche

L'opération d'intégration recherche les conflits possibles entre les données du maître en lecture/écriture isolé et le maître principal du cluster. Un rapport de conflit présentant les éventuels conflits est généré. Le maître en lecture/écriture isolé peut intégrer le cluster uniquement lorsque tous les conflits ont été résolus. Pour plus d'informations sur l'affichage et la résolution des conflits, voir «Affichage du rapport de conflits», à la page 269.

Procédure

1. Accédez à la page appropriée.

Interface graphique

a. Connectez-vous à l'interface graphique utilisateur du maître isolé.

b. Cliquez sur le lien **Associer à nouveau ce maître au cluster multimaître** dans la zone de notification de la page d'accueil d'IBM Security Key Lifecycle Manager.
c. Dans la boîte de dialogue Confirmer, lisez le message de confirmation avant d'intégrer le maître au cluster.
d. Cliquez sur **OK** pour lancer le processus d'intégration.

Interface REST

a. Ouvrez un client REST.
b. Obtenez un identificateur d'authentification utilisateur unique pour accéder aux services REST d'IBM Security Key Lifecycle Manager. Pour plus d'informations sur le processus d'authentification, voir Processus d'authentification pour les services REST.
c. Pour exécuter le **service REST Join Back Cluster**, envoyez la demande HTTP GET. Transmettez l'identificateur d'authentification utilisateur que vous avez obtenu à l'étape b avec le message de demande, conformément à l'exemple suivant :

```
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 des conflits surviennent lors du processus d'intégration, la fenêtre «Conflicts with MM Cluster» s'affiche. Pour plus d'informations, voir la rubrique «Affichage du rapport de conflits».
3. Si aucune donnée n'est en conflit, la boîte de dialogue de progression apparaît. Une fois le processus terminé, un message s'affiche indiquant que l'opération d'intégration est terminée.
4. Cliquez sur **Fermer**.
5. Redémarrez le serveur. Pour des instructions sur la façon d'arrêter et de démarrer le serveur, voir «Serveur IBM Security Key Lifecycle Manager - Redémarrage», à la page 211.

Affichage du rapport de conflits

Lors de l'intégration au cluster du maître en lecture/écriture isolé, une recherche est effectuée dans ce maître afin de détecter des conflits éventuels avec les données du maître principal du cluster. Il est nécessaire de résoudre les conflits pour que les données du maître en lecture/écriture isolé soient fusionnées avec la base de données principale. Vous pouvez afficher la liste des conflits pour analyser et résoudre les problèmes. Vous pouvez exporter les données de conflits au format de valeurs séparées par des virgules (CSV).

Procédure

1. Accédez à la page appropriée.

Interface graphique

a. Connectez-vous à l'interface graphique utilisateur du maître en lecture/écriture isolé.
b. Cliquez sur le lien **Associer à nouveau ce maître au cluster multimaître** dans la zone de notification de la page d'accueil d'IBM Security Key Lifecycle Manager.
c. Dans la boîte de dialogue Confirmer, lisez le message de confirmation avant d'intégrer le maître au cluster.

d. Cliquez sur **OK** pour exécuter le processus d'intégration.

Interface REST

a. Ouvrez un client REST.

b. Obtenez un identificateur d'authentification utilisateur unique pour accéder aux services REST d'IBM Security Key Lifecycle Manager. Pour plus d'informations sur le processus d'authentification, voir Processus d'authentification pour les services REST.

c. Pour exécuter le **service REST Join Back Cluster**, envoyez la demande HTTP POST. Transmettez l'identificateur d'authentification utilisateur que vous avez obtenu à l'étape b avec le message de demande, conformément à l'exemple suivant :

```
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 des conflits surviennent lors du processus d'intégration, ils s'affichent dans la fenêtre «Conflicts with MM Cluster».
3. Pour exporter les données des conflits dans un fichier de valeurs séparées par des virgules (format CSV), cliquez sur **Exporter le rapport des conflits**.

Que faire ensuite

Vous devez résoudre les conflits pour que les données du maître en lecture/écriture isolé soient fusionnées avec la base de données principale. Vous pouvez utiliser les services REST suivants pour résoudre les conflits.

- **Service REST Change Name**
- **Service REST Change Certificate Alias**
- **Service REST Change History**
- **Service REST Renew Key Alias**

Mise à jour du mot de passe Db2 dans le cluster multimaître d'IBM Security Key Lifecycle Manager

Si une règle d'expiration de mot de passe est appliquée, vous devez changer le mot de passe avant qu'il n'expire.

Avant de commencer

Assurez-vous de connaître le mot de passe existant à changer.

Pourquoi et quand exécuter cette tâche

Vous devez être le propriétaire de l'instance de base de données sur un système Linux ou AIX ou l'administrateur local sur un système Windows. Le mot de passe de connexion correspondant à l'ID utilisateur de l'administrateur Db2 et le mot de passe de la source de données Db2 qui est utilisé par WebSphere® Application Server doivent être identiques. Si vous modifiez l'un, vous devez faire de même pour l'autre.

Vous devez vous assurer que le nom d'utilisateur et le mot de passe Db2 sont identiques sur tous les maîtres du cluster multimaître IBM Security Key Lifecycle Manager.

Procédure

1. Arrêtez Db2 HADR sur le maître principal IBM Security Key Lifecycle Manager sur lequel se trouve la base de données principale.

   Windows

   a. Cliquez sur **Démarrer** > **IBM DB2 DBSKLMV301 (Default)** > **DB2 Command Window - Administrator**.

   b. Entrez la commande suivante et appuyez sur Entrée :

   ```
   db2 stop hadr on database sklmdb31
   ```

   Linux

   a. Dans une fenêtre de terminal, entrez la commande suivante pour changer le propriétaire de l'instance Db2 :

   ```
   su -sklmdb31
   ```

   b. Exécutez la commande suivante :

   ```
   db2 stop hadr on database sklmdb31
   ```

2. Désactivez la base de données de secours sur le maître de secours IBM Security Key Lifecycle Manager avec la commande suivante :

   ```
   db2 deactivate db sklmdb31
   ```

3. Arrêtez Db2 HADR sur le maître de secours IBM Security Key Lifecycle Manager sur lequel se trouve la base de données de secours à l'aide de la commande suivante :

   ```
   db2 stop hadr on database sklmdb31
   ```

4. Arrêtez WebSphere Application Server sur toutes les instances d'IBM Security Key Lifecycle Manager du cluster multimaître. Voir la rubrique «Serveur IBM Security Key Lifecycle Manager - Redémarrage», à la page 211 pour la procédure à suivre.

5. Arrêtez le service d'agent sur toutes les instances d'IBM Security Key Lifecycle Manager. Voir la rubrique «Redémarrage du service d'agent IBM Security Key Lifecycle Manager», à la page 251 pour la procédure à suivre.

6. Arrêtez Db2 sur tous les serveurs IBM Security Key Lifecycle Manager du cluster en exécutant la commande suivante :

   ```
   db2stop force
   ```

7. Modifiez le mot de passe pour la source de données Db2 sur tous les serveurs IBM Security Key Lifecycle Manager. Voir la rubrique suivante pour la procédure à suivre.

   Windows

   Pour changer le mot de passe, exécutez les étapes 7 à 8 décrites dans la rubrique suivante :

   Problèmes liés à la sécurité des mots de passe Db2 sous Windows

   Linux Pour changer le mot de passe, exécutez les étapes 5 à 6 décrites dans la rubrique suivante :

   «Problèmes liés à la sécurité des mots de passe Db2 sur les systèmes Linux ou AIX», à la page 39

8. Démarrez Db2 sur tous les serveurs IBM Security Key Lifecycle Manager du cluster en exécutant la commande suivante :

   ```
   db2start
   ```

9. Démarrez Db2 HADR sur tous les serveurs maîtres de secours en exécutant la commande suivante :

   ```
   db2 start hadr on database sklmdb31 as standby
   ```

10. Démarrez Db2 HADR sur le serveur maître principal en exécutant la commande suivante :

    ```
    db2 start hadr on database sklmdb31 as primary
    ```

11. Démarrez WebSphere Application Server sur le serveur maître principal. Voir la rubrique «Serveur IBM Security Key Lifecycle Manager - Redémarrage», à la page 211 pour la procédure à suivre.
12. Modifiez le mot de passe pour la source de données Db2 dans WebSphere Application Server sur le serveur maître principal de l'**une** des manières suivantes :
    - Suivez les étapes indiquées dans la note technique suivante : http://www.ibm.com/support/docview.wss?uid=ibm10788311

      ou
    - Procédez comme suit :

      Windows
      Pour changer le mot de passe, exécutez les étapes 7 à 8 décrites dans la rubrique suivante :

      Problèmes liés à la sécurité des mots de passe Db2 sous Windows

      Linux Pour changer le mot de passe, exécutez les étapes 5 à 6 décrites dans la rubrique suivante :

      «Problèmes liés à la sécurité des mots de passe Db2 sur les systèmes Linux ou AIX», à la page 39
13. Redémarrez WebSphere Application Server sur le serveur maître principal.
14. Mettez à jour le mot de passe Db2 dans la table multimaître en exécutant Service REST Update DB2 Password On All Masters.
15. Arrêtez le service d'agent sur tous les serveurs maîtres. Pour obtenir des instructions, voir la rubrique «Stop Agent», à la page 253.
16. Redémarrez WebSphere Application Server sur tous les serveurs maîtres non principaux. Pour obtenir des instructions, voir la rubrique «Serveur IBM Security Key Lifecycle Manager - Redémarrage», à la page 211.
17. Modifiez le mot de passe pour la source de données Db2 dans WebSphere Application Server sur tous les serveurs maîtres non principaux de l'une des manières suivantes :
    - Suivez les étapes indiquées dans la note technique suivante : http://www.ibm.com/support/docview.wss?uid=ibm10788311

      ou
    - Procédez comme suit :

      Windows
      Pour changer le mot de passe, exécutez les étapes 7 à 8 décrites dans la rubrique suivante :

      Problèmes liés à la sécurité des mots de passe Db2 sous Windows

      Linux Pour changer le mot de passe, exécutez les étapes 5 à 6 décrites dans la rubrique suivante :

      «Problèmes liés à la sécurité des mots de passe Db2 sur les systèmes Linux ou AIX», à la page 39
18. Arrêtez le service d'agent sur tous les serveurs maîtres du cluster. Pour obtenir des instructions, voir «Stop Agent», à la page 253.

19. Redémarrez WebSphere Application Server sur tous les serveurs IBM Security Key Lifecycle Manager du cluster. Pour obtenir des instructions, voir «Serveur IBM Security Key Lifecycle Manager - Redémarrage», à la page 211

Foire aux questions concernant la configuration multimaître d'IBM Security Key Lifecycle Manager

La foire aux questions (FAQ) concernant la configuration multimaître d'IBM Security Key Lifecycle Manager peut vous aider à mieux comprendre les processus de configuration multimaître.

Q) Lorsque des maîtres IBM Security Key Lifecycle Manager sont configurés pour la configuration multimaître, le service de synchronisation des données copie automatiquement les données du serveur principal sur les serveurs maîtres à intervalles réguliers. Pourquoi dois-je utiliser la fonction Sauvegarde et restauration d'IBM Security Key Lifecycle Manager ?

R) A titre préventif afin d'éviter toute perte de données, utilisez la fonction Sauvegarde et restauration pour sauvegarder les données manuellement à intervalles réguliers.

Q) J'ai ajouté un maître IBM Security Key Lifecycle Manager non HADR au cluster multimaître. Pourquoi les données de la base de données locale continuent-elles d'apparaître au lieu des données de la base de données principale ?

R) Il se peut que la source de données d'IBM Security Key Lifecycle Manager continue de pointer vers la base de données locale, même si l'ajout du maître au cluster a abouti. Après l'ajout du maître au cluster, la source de données dans WebSphere Application Server doit pointer vers la base de données principale.

Vous pouvez mettre à jour manuellement les détails du serveur dans la source de données du serveur maître que vous avez ajouté en procédant comme suit :

1. Connectez-vous à WebSphere Integrated Solutions Console (https://localhost:9083/ibm/console/logon.jsp).
2. Cliquez sur **Ressources** > **JDBC** > **Sources de données** > **Source de données SKLM**.
3. Dans la page Source de données SKLM, vérifiez la valeur de la zone **Nom du serveur** dans la section **Propriétés communes et obligatoires des sources de données**. Si le nom d'hôte du serveur local est affiché, mettez à jour la valeur en spécifiant le nom d'hôte du serveur principal.

   Si la valeur dans la zone **Nom du serveur** a déjà été mise à jour avec le nom d'hôte du serveur principal, redémarrez WebSphere Application Server et fermez la page. Sinon, effectuez les opérations suivantes :
4. Dans la section **Propriétés supplémentaires** de la page Source de données SKLM, cliquez sur le lien **Propriétés de la source de données WebSphere Application Server**.
5. Dans la section **Fonctions Db2 avancées**, vérifiez les valeurs dans la zone **Autres noms de serveur**.
6. Spécifiez le nom d'hôte des serveurs de secours dans une liste en les séparant par une virgule dans la zone **Autres noms de serveur**.
7. Spécifiez les numéros de port des serveurs de secours dans une liste en les séparant par une virgule dans la zone **Autres numéros de port**.

8. Sauvegardez les modifications.
9. Cliquez sur **Ressources** > **JDBC** > **Sources de données** > **SKLM scheduler XA Datasource**.
10. Répétez les étapes 3 à 8.
11. Redémarrez WebSphere Application Server.

Q) Comment puis-je vérifier que la synchronisation est exécutée entre les maîtres principal et de secours d'IBM Security Key Lifecycle Manager ?

A) Vous pouvez vérifier que la synchronisation s'exécute entre les maîtres principal et de secours d'IBM Security Key Lifecycle Manager en vérifiant l'écart de temps entre PRIMARY_LOG_TIME et STANDBY_LOG_TIME. Exécutez la commande suivante depuis une fenêtre de commande Db2 :

```
#db2pd -d <SKLM_DBName> –hadr
```

Par exemple :

```
#db2pd -d sklmdb31 –hadr
```

La sortie suivante s'affiche :

```
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
```

Dans la sortie, PRIMARY_LOG_TIME affiche la date et l'heure de mise à jour des journaux de transactions Db2 pour le serveur principal. STANDBY_LOG_TIME affiche la date et l'heure de mise à jour des journaux de transactions Db2 pour le serveur de secours. Vous pouvez ignorer l'écart de temps s'il se compte en millisecondes.

Q) Comment puis-je afficher le statut des ports dans la configuration multimaître d'IBM Security Key Lifecycle Manager ?

R) L'interface graphique d'IBM Security Key Lifecycle Manager utilise des icônes pour représenter le statut du port dans les pages de configuration multimaître. Le tableau ci-dessous présente les icônes de statut de port et leur signification.

Tableau 5. Icônes de statut et signification

Icône	Description
	Le port est accessible et gère les demandes conformément aux spécifications.
	Le port n'est pas accessible. Il se peut que le service soit arrêté sur un port spécifique. Actualisez le statut avec l'option Actualiser dans la page de l'interface utilisateur.

Q) Comment puis-je afficher le statut Db2 HADR dans la configuration multimaître d'IBM Security Key Lifecycle Manager ?

A) L'interface graphique d'IBM Security Key Lifecycle Manager utilise des icônes pour représenter le statut Db2 HADR dans les pages de configuration multimaître. Le tableau suivant présente les icônes de statut Db2 HADR et leur signification.

Tableau 6. Icônes de statut et signification

Icône	Description
	Db2 HADR est en cours d'exécution. Tous les maîtres HADR sont connectés entre eux.
	Db2 HADR est en cours d'exécution mais au moins l'un des maîtres HADR de secours n'est pas accessible.
	Db2 HADR est arrêté et n'est pas opérationnel.

Exportation et importation de clés

Vous pouvez autoriser le transfert de données entre deux serveurs IBM Security Key Lifecycle Manager en exportant les clés (symétriques ou privées) d'un serveur (source) et en les important sur un autre serveur (cible).

Selon la version d'IBM Security Key Lifecycle Manager installée sur votre serveur, vous pouvez utiliser l'une des méthodes suivantes pour exporter et importer des clés :

Tableau 7. Méthodes d'exportation et d'importation de clés

Méthode	Version IBM Security Key Lifecycle Manager prise en charge	Liens pratiques
Interface graphique	3.0.1	• «Exportation d'une clé à l'aide de l'interface graphique» • «Importation d'une clé à l'aide de l'interface graphique», à la page 277
service REST	Aucune version prise en charge.	• Service REST Key Export • Service REST Key Import
Commande CLI	Aucune version prise en charge.	• tklmKeyExport • tklmKeyImport

Exportation d'une clé à l'aide de l'interface graphique

Vous pouvez exporter des clés symétriques et privées dans un fichier de clés chiffré sur un serveur IBM Security Key Lifecycle Manager. Vous pouvez ensuite importer les clés de ce fichier sur un autre serveur IBM Security Key Lifecycle Manager pour permettre le transfert des données entre ces serveurs.

Procédure

1. Accédez à la page ou au répertoire approprié.
   a. Connectez-vous à l'interface graphique.
   b. Dans le menu principal, cliquez sur **Rechercher**.
   c. Dans le volet Rechercher de gauche, dans **Type d'objet**, sélectionnez **Clé symétrique** ou **Clé privée**, selon les clés que vous souhaitez rechercher. Vous pouvez également rechercher des groupes d'unités pour lesquels vous souhaitez exporter des clés.
   d. Cliquez sur **Rechercher**. Les clés du type de clé sélectionné sont répertoriées dans le volet de droite.
2. Exportez les clés dans un fichier de clés.
   a. Dans la liste de clés du volet de droite, sélectionnez les clés que vous souhaitez exporter (utilisez la touche CTRL pour sélectionner plusieurs clés), puis cliquez sur **Exporter**.
   b. Dans la fenêtre Exporter les clés symétriques ou Exporter les clés privées, indiquez un nom pour le fichier de clés qui est utilisé pour stocker les clés exportées.
   c. Facultatif : Indiquez un emplacement de fichier différent pour enregistrer le fichier de clés. Par défaut, la zone **Emplacement du fichier** affiche le chemin du répertoire *SKLM_DATA* par défaut dans lequel le fichier de clés est enregistré. Par exemple, `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data`. Pour la définition de *SKLM_DATA*, voir Définitions relatives à un répertoire *HOME* et d'autres variables de répertoire.
   d. Pour le type de clé symétrique, indiquez un certificat comme alias de clé. Le certificat est l'entrée de clé publique dans le magasin de clés qui est utilisée pour déchiffrer les clés symétriques. Seule la personne possédant la clé privée correspondante peut accéder aux clés.

e. Pour le type de clé privée, créez un mot de passe de chiffrement. Ce mot de passe sera utilisé pour déchiffrer le fichier de clés lors de l'importation des clés sur un serveur IBM Security Key Lifecycle Manager.

f. Cliquez sur **Exporter**.

Que faire ensuite

Importez les clés sur le serveur IBM Security Key Lifecycle Manager sur lequel vous souhaitez activer le transfert de données.

Tâches associées:

«Importation d'une clé à l'aide de l'interface graphique»
Vous pouvez importer des clés symétriques et privées sur un serveur IBM Security Key Lifecycle Manager pour permettre le transfert de données entre ce serveur et le serveur à partir duquel les clés ont été exportées. Les clés à importer doivent être stockées dans un fichier de clés chiffré.

Référence associée:

Service REST Key Export
Le **service REST Key Export** permet d'exporter des clés secrètes ou des paires clé privée - clé publique. Une clé secrète est une clé symétrique. Une paire clé privée - clé publique est une paire de clés asymétriques contenant une clé publique et une clé privée.

Importation d'une clé à l'aide de l'interface graphique

Vous pouvez importer des clés symétriques et privées sur un serveur IBM Security Key Lifecycle Manager pour permettre le transfert de données entre ce serveur et le serveur à partir duquel les clés ont été exportées. Les clés à importer doivent être stockées dans un fichier de clés chiffré.

Avant de commencer

Copiez le fichier de clés dans le chemin de répertoire *SKLM_DATA* par défaut sur le serveur IBM Security Key Lifecycle Manager sur lequel vous souhaitez l'importer. Par exemple, `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data`. Pour la définition de *SKLM_DATA*, voir Définitions relatives à un répertoire *HOME* et d'autres variables de répertoire.

Procédure

1. Accédez à la page ou au répertoire approprié.
   a. Connectez-vous à l'interface graphique.
   b. Sur la page Bienvenue, cliquez sur **Administration** > **Exporter et importer** > **Importer des clés**.
2. Importez une clé à partir d'un fichier de clés. Vous ne pouvez importer qu'une seule clé à la fois.
   a. Sélectionnez le type de clé.
   b. Cliquez sur **Parcourir** pour sélectionner le fichier de clés à importer.
   c. Pour les clés symétriques, sélectionnez le certificat à utiliser pour déchiffrer les clés dans le fichier de clés. Assurez-vous qu'il s'agit du même certificat que celui utilisé lors de l'exportation de la clé.
   d. Pour les clés privées, indiquez le mot de passe à utiliser pour déchiffrer les clés dans le fichier de clés. Assurez-vous qu'il s'agit du même mot de passe que celui utilisé lors de l'exportation des clés.
   e. Indiquez l'alias de la clé à importer.

f. Facultatif : Pour renommer l'alias de la clé importée, indiquez un nouveau nom d'alias. Vous pouvez renommer l'alias si l'alias de clé actuel est déjà utilisé ou si vous souhaitez le modifier.

g. Sélectionnez le groupe d'unités dans lequel la clé importée doit être utilisée.

h. Cliquez sur **Importer**.

3. Pour importer plusieurs clés, répétez l'étape 2 pour chaque clé.

Tâches associées:

«Importation d'une clé à l'aide de l'interface graphique», à la page 277
Vous pouvez importer des clés symétriques et privées sur un serveur IBM Security Key Lifecycle Manager pour permettre le transfert de données entre ce serveur et le serveur à partir duquel les clés ont été exportées. Les clés à importer doivent être stockées dans un fichier de clés chiffré.

Référence associée:

Service REST Key Import
Le **service REST Key Import** permet d'importer des clés secrètes ou des paires clé privée - clé publique. Une clé secrète est une clé symétrique. Une paire clé privée - clé publique est une clé asymétrique qui contient une clé publique et une clé privée. Le magasin de clés privées est au format PKCS#12.

Formats d'horodatage

IBM Security Key Lifecycle Manager prend en charge le format UTC (temps universel coordonné).

Les exemples suivants présentent l'horodatage IST au format UTC (GMT + 5:30).

La base de données IBM Security Key Lifecycle Manager
Les horodatages sont stockés dans la base de données IBM Security Key Lifecycle Manager au format UTC.

```
2018-03-22 05:52:07.0
```

Interface utilisateur
Les valeurs d'horodatage s'affichent dans l'interface utilisateur d'IBM Security Key Lifecycle Manager en fonction du fuseau horaire du navigateur.

```
Last backup:Mar 22 2018, 05:51:24 AM IST (GMT+05:30)
```

Fichiers journaux
Les valeurs d'horodatage de tous les fichiers journaux s'affichent en fonction du fuseau horaire du serveur avec le décalage UTC. Dans l'exemple suivant, l'horodatage s'affiche pour le fuseau horaire IST.

```
Mar 22, 2018 11:31:40 AM +0500
```

Acceptation des unités en attente

Utilisez la fonction de mise en attente d'unités pour accepter ou rejeter une unité qui contacte IBM Security Key Lifecycle Manager.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser la page Demandes d'unités en attente de l'interface graphique ou plusieurs commandes équivalentes dans l'interface de ligne de commande pour accepter ou rejeter une unité qui contacte IBM Security Key Lifecycle Manager. Si l'unité appartient à la famille d'unités DS5000 et si l'affinité machine est activée, vous pouvez accepter ou rejeter une relation entre une unité et une machine.

L'utilisation de l'affinité machine vous permet de limiter le service de clés à des combinaisons spécifiques d'unités et de machines.

Procédure

1. Des clés sont générées automatiquement pour une unité d'un groupe d'unités DS5000 lorsqu'une demande en attente arrive. Effectuez une sauvegarde avant d'accepter l'unité. Vous êtes ainsi certain de sauvegarder les clés avant qu'elles ne commencent à être servies à une unité. Pour plus d'informations, consultez la section traitant de l'administration des fichiers de sauvegarde et de restauration.
2. Accédez à la page ou au répertoire approprié.
   - Interface graphique :

     Connectez-vous à l'interface graphique. Dans l'arborescence de navigation, cliquez sur **IBM Security Key Lifecycle Manager**.
   - Interface de ligne de commande
     a. Accédez au répertoire <*WAS_HOME*>/bin. Exemple :

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

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

     b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme SKLMAdmin. Exemple :

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

        Linux
        ```
        ./wsadmin.sh -username SKLMAdmin
        -password mypwd -lang jython
        ```
3. Si vous n'avez pas encore déterminé comment accepter les unités en attente, réglez l'attribut **device.AutoPendingAutoDiscovery** sur une valeur qui ajoute les unités entrantes à la liste des unités en attente.

   Spécifiez une valeur telle que 2 (mise en attente automatique). Toutes les unités entrantes sont ajoutées à une liste d'attente, mais lorsqu'elles demandent des clés, celles-ci ne leur sont pas servies automatiquement. Vous devez accepter ou rejeter chaque unité dans la liste des unités en attente, en fonction de quoi des clés lui sont servies ou non lorsqu'elle en fait la demande. N'utilisez pas la valeur 1 (acceptation automatique) pour la famille d'unités DS5000. Sinon, des clés pourraient être générées et servies aux serveurs de stockage DS5000 avant même que vous puissiez effectuer une sauvegarde.
   - Interface graphique :
     a. Naviguez jusqu'à la page Gestion des clés et des unités du groupe d'unités auquel appartiennent les unités en attente.
     b. Dans la liste déroulante en bas de page, sélectionnez **Retenir les demandes des nouvelles unités en attente de mon approbation**.
   - Interface de ligne de commande :

     Par exemple, pour une unité DS5000, tapez :
     ```
     print AdminTask.tklmDeviceGroupAttributeUpdate ('[-name DS5000
       -attributes "{device.AutoPendingAutoDiscovery 2}"]')
     ```
4. Affichez la liste des unités en attente.
   - Interface graphique :

     Accédez à la page Bienvenue. Dans la zone Actions, cliquez sur le lien des unités en attente.

- Interface de ligne de commande :

  Entrez :

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

5. Approuvez ou rejetez une demande d'unité en attente.
   - Interface graphique :

     Dans la table Demandes d'unités en attente, sélectionnez une unité en attente et cliquez sur **Accepter** ou **Rejeter**.

     Une demande en attente n'est listée qu'une seule fois dans le cas d'une unité DS5000 ayant également une relation machine-unité. La demande apparaît dans la table avec la valeur de l'ID machine. Le fait d'accepter la demande de l'unité en attente accepte également la relation machine-unité.

     Dans la boîte de dialogue Accepter la demande de l'unité, cliquez sur **Accepter** ou **Modifier et accepter**. Si vous choisissez de modifier les informations de l'unité en attente, apportez les changements nécessaires, puis cliquez sur **Accepter**.
   - Interface de ligne de commande :
     - Vous pouvez utiliser une seule et même commande pour accepter une unité DS5000 en attente ainsi que la relation machine-unité en attente. Par exemple, entrez :

       ```
       print AdminTask.tklmPendingMachineDeviceAccept
       ('[-deviceUUID DEVICE-7d588437-e725-48bf-a836-00a47df64e78
       -machineID 30423830303034370000000000000]')
       ```
     - Sinon, vous pouvez d'abord accepter une unité en attente et l'affecter au groupe d'unités approprié. Pour accepter une unité DS5000 en attente et accepter ultérieurement une relation machine-unité :
       a. Entrez d'abord :

          ```
          print AdminTask.tklmPendingDeviceAccept
          ('[-deviceUUID DEVICE-7d588437-e725-48bf-a836-00a47df64e78
           -usage DS5000]')
          ```
       b. Plus tard, acceptez ou rejetez les relations en attente entre une unité et une machine.
          1) Listez toutes les unités en attente qui ont une relation avec un ID machine précis, ou bien toutes les unités si aucun ID machine n'est spécifié. Par exemple, entrez :

             ```
             print AdminTask.tklmPendingMachineDeviceList
             ('[-machineID 30423830303034370000000000000]')
             ```
          2) Acceptez ou rejetez une relation machine-unité en attente. L'acceptation a pour effet d'écrire les données de relation dans le magasin de données d'IBM Security Key Lifecycle Manager.

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

Que faire ensuite

Examinez la liste des unités acceptées. Utilisez les commandes suivantes :

- **tklmDeviceList** pour lister les informations relatives à toutes les unités du type indiqué.
- **tklmMachineDeviceList** pour lister toutes les unités qui sont associées à un ID machine précis, ou bien toutes les unités si aucun ID machine n'est spécifié.

Déplacement d'unités entre groupes d'unités

Utilisez la fonction de mise à jour d'unité pour déplacer une unité d'un groupe d'unités existant vers un autre groupe existant. Par exemple, vous pourriez déplacer une unité vers le groupe MONDS5000.

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser la page Modifier une unité, la commande **tklmDeviceUpdate** ou **Service REST Device Update** pour déplacer une unité qui contacte IBM Security Key Lifecycle Manager entre deux groupes d'unités de la même famille. Par exemple, vous pourriez déplacer une unité vers le groupe MYDS5000 de la famille d'unités DS5000.

Pour plus d'informations sur la création d'un groupe d'unités, voir «Création d'un groupe d'unités», à la page 33.

Procédure

1. Accédez à la page ou au répertoire approprié :
   - Interface graphique :
     a. Connectez-vous à l'interface graphique.
     b. Dans la section Gestion des clés et des unités de la page de bienvenue, sélectionnez **DS5000**.
     c. Cliquez sur **DS5000** à l'aide du bouton droit de la souris.
     d. Cliquez sur **Gestion des clés et des unités**.
   - Interface de ligne de commande
     a. Accédez au répertoire <*WAS_HOME*>/bin. Exemple :

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

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

     b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme SKLMAdmin. Exemple :

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

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

   - Interface REST :
     – Ouvrez un client REST.
2. Localisez l'unité à déplacer dans un autre groupe d'unités au sein d'une famille d'unités parent.
   - Interface graphique :

     Sur la page Gestion des clés et des unités DS5000, localisez l'unité dans la table d'unités. Par exemple, supposons que le numéro de série de l'unité est aaa123.
   - Interface de ligne de commande :

     Entrez la commande suivante :

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

     Dans la sortie de la commande, recherchez la valeur de l'identificateur unique universel (UUID) de l'unité. Exemple :

```
Description = Ma description longue
Numéro de série = aaa123
UUID d'unité = DEVICE-b7678b4d-3898-4f8c-9557-dbb2f381fc8a
Groupe d'unités = DS5000
Libellé de l'unité =
Nom WWN =
Alias de clé symétrique = DS5K-aaa123
```

- Interface REST :
  a. Obtenez un identificateur d'authentification utilisateur unique pour accéder aux services REST d'IBM Security Key Lifecycle Manager. Pour plus d'informations sur le processus d'authentification, voir Processus d'authentification pour les services REST.
  b. Pour appeler le **service REST Device List Type**, envoyez la demande HTTP GET. Transmettez l'identificateur d'authentification utilisateur que vous avez obtenu à l'étape a avec le message de demande, conformément à l'exemple suivant :

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

  Dans le message indiquant la réussite de l'opération, recherchez la valeur de l'identificateur unique universel (UUID) de l'unité. Exemple :

```
Code de statut :200 OK
Content-Language: en
[
{
"Description" : "Ma description longue",
"Numéro de série" : "aaa123",
"UUID d'unité" : "DEVICE-b7678b4d-3898-4f8c-9557-dbb2f381fc8a",
"Groupe d'unités" : "DS5000",
"Nom WWN" : "",
"Alias de clé symétrique" : "DS5K-aaa123"
},
]
```

3. Vérifiez que le groupe d'unités cible existe.
   - Interface graphique :

     Sur la page Gestion des clés et des unités DS5000, dans la table d'unités, sélectionnez l'unité et cliquez sur **Modifier > Unité**.

     Sur la page Modifier une unité, dans la zone **Groupe d'unités actuellement affecté**, développez la liste pour déterminer si le groupe d'unités **MONDS5000** est disponible.
   - Interface de ligne de commande :

     Entrez la commande suivante :

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

     Localisez le groupe d'unités. Exemple :

```
UUID du groupe d'unités          10000
Nom du groupe d'unités           MONDS5000
Famille d'unités                 DS5000
symmetricKeySet                  null
drive.default.alias1             null
drive.default.alias2             null
shortName                        MONGroupeDS5000
longName                         Unités DS5000 de ma société
roleName                         MONDS5000
device.AutoPendingAutoDiscovery  0
enableKMIPDelete                 false
```

- Interface REST :

  Envoyez la demande HTTP suivante :

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

  Localisez le groupe d'unités. Exemple :

  ```
  Code de statut :200 OK
  Content-Language: en
  [
  {
  "UUID du groupe d'unités" : "10000",
  "Nom du groupe d'unités" : "MONDS5000",
  "Famille d'unités" : "DS5000",
  "symmetricKeySet" : null,
  "drive.default.alias1" : null,
  "drive.default.alias2" : null,
  "shortName" : MONGroupeDS5000,
  "longName" : Unités DS5000 de ma société,
  "roleName" : "MONDS5000",
  "device.AutoPendingAutoDiscovery" : "0",
  "enableKMIPDelete" : "false"
  },
  ]
  ```

4. Mettez à jour l'unité afin de spécifier le nouveau groupe d'unités.
   - Interface graphique :

     Sur la page Modifier une unité, dans la zone **Groupe d'unités actuellement affecté**, sélectionnez le groupe d'unités **MONDS5000**.

     Cliquez sur **Modifier une unité**.
   - Interface de ligne de commande :

     Entrez la commande suivante :

     ```
     print AdminTask.tklmDeviceUpdate
     ('[-uuid DEVICE-b7678b4d-3898-4f8c-9557-dbb2f381fc8a -type MONDS5000]')
     ```
   - Interface REST :

     Envoyez la demande HTTP suivante :

     ```
     PUT https://localhost:<port>/SKLM/rest/v1/devices
     Content-Type: application/json
     Accept : application/json
     Authorization: SKLMAuth authId=139aeh34567m
     {"uuid" :"DEVICE-b7678b4d-3898-4f8c-9557-dbb2f381fc8a","type" :
     "MONDS5000"}
     ```
5. Vérifiez que l'unité se trouve dans le nouveau groupe d'unités.
   - Interface graphique :

     Sur la page Gestion des clés et des unités DS5000, l'unité ne figure plus dans la table d'unités. Ouvrez la page Gestion des clés et des unités MONDS5000 et vérifiez que l'unité est répertoriée dans la table d'unités.
   - Interface de ligne de commande :

     Entrez la commande suivante :

     ```
     print AdminTask.tklmDeviceList ('[-type MONDS5000]')
     ```

     Par exemple, la sortie de la commande contient la valeur de l'identificateur unique universel de l'unité et le nom du nouveau groupe d'unités.

     ```
     Description = Ma description longue
     Numéro de série = aaa123
     UUID d'unité = DEVICE-b7678b4d-3898-4f8c-9557-dbb2f381fc8a
     ```

```
Groupe d'unités = MONDS5000
Libellé de l'unité =
Nom WWN =
Alias de clé symétrique = DS5K-aaa123
```

- Interface REST :

  Envoyez la demande HTTP suivante :

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

  Le message indiquant la réussite de l'opération contient la valeur de l'identificateur unique universel de l'unité et le nom du nouveau groupe d'unités comme indiqué dans l'exemple suivant :

```
Code de statut :200 OK
Content-Language: en
[
{
"Description" : "Ma description longue",
"Numéro de série" : "aaa123",
"UUID d'unité" : "DEVICE-b7678b4d-3898-4f8c-9557-dbb2f381fc8a",
"Groupe d'unités" : "MONDS5000",
"Nom WWN" : "",
"Alias de clé symétrique" : "DS5K-aaa123"
},
]
```

Exportation d'un certificat de serveur SSL/KMIP

Exportez le certificat de serveur SSL/KMIP d'IBM Security Key Lifecycle Manager dans un fichier au format encodé à des fins d'utilisation par l'unité client. Ce dernier importe le certificat pour établir une communication sécurisée avec le serveur.

Pourquoi et quand exécuter cette tâche

Utilisez la boîte de dialogue Exportation d'un certificat, la commande **tklmCertExport** ou le **service REST Certificate Export** pour exporter le certificat de serveur SSL/KMIP d'IBM Security Key Lifecycle Manager dans un fichier dans un format codé.

Procédure

1. Accédez à la page ou au répertoire approprié.
   - Interface graphique :

     Connectez-vous à l'interface graphique. La page Bienvenue s'affiche.
   - Interface de ligne de commande
     a. Accédez au répertoire <*WAS_HOME*>/bin. Exemple :

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

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

     b. Démarrez l'interface **wsadmin** en utilisant un ID utilisateur autorisé, comme SKLMAdmin. Exemple :

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

Linux

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

- Interface REST :
  - Ouvrez un client REST.

2. Exportez un certificat.
   - Interface graphique :
     a. Cliquez sur **Configuration avancée** > **Certificats de serveur**.
     b. Dans la table **Certificats**, sélectionnez le certificat approprié.
     c. Cliquez sur **Exporter**.
     d. Dans la boîte de dialogue Exporter un certificat, le certificat que vous avez sélectionné à l'étape b est renseigné dans la zone **Nom de fichier**.
     e. La zone **Emplacement du fichier** affiche le chemin de répertoire <*SKLM_DATA*> par défaut dans lequel le certificat est exporté, par exemple `C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data`. Pour la définition de <*SKLM_DATA*>, voir Définitions relatives à un répertoire *HOME* et d'autres variables de répertoire. Cliquez sur **Parcourir** pour spécifier un emplacement sous le répertoire <SKLM_DATA>.
     f. Sélectionnez le format de fichier codé **BASE64** (format par défaut) ou **DER** (fichier de règles de codage distinctif) pour le certificat.
     g. Cliquez sur **Exporter un certificat**.
   - Interface de ligne de commande :

     Entrez `tklmCertExport` pour exporter un fichier de certificat. Exemple :

     ```
     print AdminTask.tklmCertExport
      ('[-uuid CERTIFICATE-61f8e7ca-62aa-47d5-a915–8adbfbdca9de
       -format DER -fileName d:\\mypath\\mycertfilename.der]')
     ```

     Pour plus d'informations sur la commande **tklmCertExport**, voir tklmCertExport.
   - Interface REST :
     a. Obtenez un identificateur d'authentification utilisateur unique pour accéder aux services REST d'IBM Security Key Lifecycle Manager. Pour plus d'informations sur le processus d'authentification, voir Processus d'authentification pour les services REST.
     b. Pour démarrer le **service REST Certificate Export**, envoyez la demande HTTP PUT. Transmettez l'identificateur d'authentification utilisateur que vous avez obtenu à l'étape a avec le message de demande, conformément à l'exemple suivant :

        ```
        PUT https://localhost:<port>/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"}
        ```

        Pour plus d'informations sur le **service REST Certificate Export**, voir service REST Certificate Export.

Copie d'un certificat entre des serveurs IBM Security Key Lifecycle Manager

Vous pouvez utiliser l'interface de ligne de commande ou l'interface REST pour copier un certificat entre des serveurs IBM Security Key Lifecycle Manager à l'aide de la clé publique et de la clé privée.

Pourquoi et quand exécuter cette tâche

Utilisez les commandes CLI ou les interfaces REST suivantes pour copier un certificat :

- **tklmKeyExport** et **tklmKeyImport**
- **Service REST Key Export** et **Service REST Key Import**

Procédure

1. Sur le serveur IBM Security Key Lifecycle Manager sur lequel le certificat est installé, exécutez la commande **tklmKeyExport** ou envoyez la demande HTTP **Service REST Key Export**.

```
print AdminTask.tklmKeyExport ('[-alias sklmCertificate
   -fileName myprivatekeys -keyStoreName defaultKeyStore
    -type privatekey -password mypassword]')
```

```
PUT https://localhost:<port>/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. Copiez le fichier mycert.p12 sur le serveur IBM Security Key Lifecycle Manager de destination.
3. Exécutez la commande **tklmKeyImport** ou envoyez la demande HTTP **Service REST Key Import**.

```
print AdminTask.tklmKeyImport ('-type privatekey -fileName c:\\mycert.p12
-keyStoreName "Tivoli Key Lifecycle Manager Keystore" -usage 3592 -password
<password>]')
```

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

Résultats

Ces commandes permettent de copier les clés privées et publiques sur les bandes accessibles en lecture et en écriture à l'aide du certificat.

Changement de la langue de l'interface du navigateur

Vous pouvez changer la langue dans l'interface du navigateur.

Pourquoi et quand exécuter cette tâche

Modifiez la langue d'affichage de votre navigateur avant de vous connecter à IBM Security Key Lifecycle Manager. Pour changer la langue d'affichage préférée dans votre navigateur, procédez comme suit :

- Internet Explorer

1. Sélectionnez **Outils > Options Internet**.
2. Dans l'onglet **Général**, cliquez sur **Langues**.
3. Sélectionnez une langue et cliquez sur **OK**. Il est possible que vous deviez d'abord ajouter une langue et la placer en première position dans la liste des langues.
4. Redémarrez le navigateur.

- Firefox
  1. Sélectionnez **Outils > Options**. Cliquez ensuite sur l'icône Contenu.
  2. Sous l'onglet Contenu, dans la section Langues, cliquez sur **Choisir**.
  3. Sélectionnez une langue et cliquez sur **OK**. Vous devrez peut-être dans un premier temps ajouter une langue et la placer en première position dans la liste des langues.
  4. Dans la boîte de dialogue Options, cliquez à nouveau sur **OK**.
  5. Redémarrez le navigateur.

Remarques

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM non annoncés dans ce pays. Pour plus de détails, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial IBM. Toute référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit d'IBM. Il est de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, logiciels ou services non expressément référencés par IBM.

IBM peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous donne aucun droit de licence sur ces brevets ou demandes de brevet. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
U.S.A.

Pour le Canada, veuillez adresser votre courrier à :

IBM Director of Commercial Relations
IBM Canada Ltd.
3600 Steeles Avenue East
Markham, Ontario
L3R 9Z7 Canada

Les informations sur les licences concernant les produits utilisant un jeu de caractères double octet peuvent être obtenues par écrit à l'adresse suivante :

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

Le paragraphe suivant ne s'applique ni au Royaume-Uni, ni dans aucun pays dans lequel il serait contraire aux lois locales.

LE PRESENT DOCUMENT EST LIVRE EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFACON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE.

Certaines juridictions n'autorisent pas l'exclusion des garanties implicites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Le présent document peut contenir des inexactitudes ou des coquilles. Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. IBM peut, à tout moment et sans préavis, modifier les produits et logiciels décrits dans ce document.

Les références à des sites Web non IBM sont fournies à titre d'information uniquement et n'impliquent en aucun cas une adhésion aux données qu'ils contiennent. Les éléments figurant sur ces sites Web ne font pas partie des éléments du présent produit IBM et l'utilisation de ces sites relève de votre seule responsabilité.

IBM pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie des informations qui lui seront fournies.

Les licenciés souhaitant obtenir des informations permettant : (i) l'échange des données entre des logiciels créés de façon indépendante et d'autres logiciels (dont celui-ci), et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à :

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
U.S.A.

Ces informations peuvent être soumises à des conditions particulières, prévoyant notamment le paiement d'une redevance.

Le logiciel sous licence décrit dans ce document et tous les éléments sous licence disponibles s'y rapportant sont fournis par IBM conformément aux dispositions de l'ICA, des Conditions internationales d'utilisation des logiciels IBM ou de tout autre accord équivalent.

Les données de performance indiquées dans ce document ont été déterminées dans un environnement contrôlé. Par conséquent, les résultats peuvent varier de manière significative selon l'environnement d'exploitation utilisé. Certaines mesures évaluées sur des systèmes en cours de développement ne sont pas garanties sur tous les systèmes disponibles. En outre, elles peuvent résulter d'extrapolations. Les résultats peuvent donc varier. Il incombe aux utilisateurs de ce document de vérifier si ces données sont applicables à leur environnement d'exploitation.

Les informations concernant des produits non IBM ont été obtenues auprès des fournisseurs de ces produits, par l'intermédiaire d'annonces publiques ou via d'autres sources disponibles. IBM n'a pas testé ces produits et ne peut confirmer l'exactitude de leurs performances ni leur compatibilité. Elle ne peut recevoir aucune réclamation concernant des produits non IBM. Toute question concernant les performances de produits non IBM doit être adressée aux fournisseurs de ces produits.

Toute instruction relative aux intentions d'IBM pour ses opérations à venir est susceptible d'être modifiée ou annulée sans préavis, et doit être considérée uniquement comme un objectif.

Tous les tarifs indiqués sont les prix de vente actuels suggérés par IBM et sont susceptibles d'être modifiés sans préavis. Les tarifs appliqués peuvent varier selon les revendeurs.

Ces informations sont fournies uniquement à titre de planification. Elles sont susceptibles d'être modifiées avant la mise à disposition des produits décrits.

Le présent document peut contenir des exemples de données et de rapports utilisés couramment dans l'environnement professionnel. Ces exemples mentionnent des noms fictifs de personnes, de sociétés, de marques ou de produits à des fins illustratives ou explicatives uniquement. Toute ressemblance avec des noms de personnes, de sociétés ou des données réelles serait purement fortuite.

LICENCE DE COPYRIGHT :

Le présent logiciel contient des exemples de programmes d'application en langage source destinés à illustrer les techniques de programmation sur différentes plateformes d'exploitation. Vous avez le droit de copier, de modifier et de distribuer ces exemples de programmes sous quelque forme que ce soit et sans paiement d'aucune redevance à IBM, à des fins de développement, d'utilisation, de vente ou de distribution de programmes d'application conformes aux interfaces de programmation des plateformes pour lesquels ils ont été écrits ou aux interfaces de programmation IBM. Ces exemples de programmes n'ont pas été rigoureusement testés dans toutes les conditions. Par conséquent, IBM ne peut garantir expressément ou implicitement la fiabilité, la maintenabilité ou le fonctionnement de ces programmes. Ces exemples de programmes sont fournis "en l'état", sans garantie d'aucune sorte. IBM n'est en aucun cas responsable des dommages liés à l'utilisation de ces exemples de programmes.

Toute copie totale ou partielle de ces programmes exemples et des oeuvres qui en sont dérivées doit comprendre une notice de copyright, libellée comme suit :

© (nom de votre société) (année). Des segments de code sont dérivés des Programmes exemples d'IBM Corp. © Copyright IBM Corp. _année ou années_.

Si vous visualisez ces informations en ligne, il se peut que les photographies et illustrations en couleur n'apparaissent pas à l'écran.

Dispositions relatives à la documentation du produit

Les droits d'utilisation relatifs à ces publications sont soumis aux dispositions suivantes.

Domaine d'application
Ces dispositions viennent s'ajouter aux éventuelles conditions d'utilisation du site Web IBM.

Usage personnel
Vous pouvez reproduire ces publications pour votre usage personnel, non commercial, sous réserve que toutes les mentions de propriété soient conservées. Vous ne pouvez distribuer ou publier tout ou partie de ces publications ou en faire des oeuvres dérivées sans le consentement exprès d'IBM.

Usage commercial
Vous pouvez reproduire, distribuer et afficher ces publications uniquement au sein de votre entreprise, sous réserve que toutes les mentions de

propriété soient conservées. Vous ne pouvez pas procéder à des travaux dérivés de ces publications, ni les reproduire, les distribuer ou les afficher en totalité ou partiellement en dehors de votre entreprise sans le consentement exprès d'IBM.

Droits Sauf autorisation expresse, aucun autre droit, autorisation ou licence n'est accordé de façon explicite ou implicite aux publications ou à toute information, donnée ou tout logiciel ou autre propriété intellectuelle contenu dans ces publications.

IBM se réserve le droit de retirer les autorisations accordées ici si, à sa discrétion, l'utilisation des publications s'avère préjudiciable à ses intérêts ou que, selon son appréciation, les instructions susmentionnées n'ont pas été respectées.

Vous ne pouvez télécharger, exporter ou réexporter ces informations qu'en total accord avec toutes les lois et règlements applicables dans votre pays, y compris les lois et règlements américains relatifs à l'exportation.

IBM N'OCTROIE AUCUNE GARANTIE SUR LE CONTENU DE CES PUBLICATIONS. LES PUBLICATIONS SONT LIVREES EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES PUBLICATIONS EN CAS DE CONTREFAÇON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE.

Marques

IBM, le logo IBM et ibm.com sont des marques d'International Business Machines Corp. aux Etats-Unis et/ou dans certains autres pays. Les autres noms de produits et de services peuvent appartenir à IBM ou à des tiers. La liste actualisée de toutes les marques d'IBM est disponible sur la page Web "Copyright and trademark information" à l'adresse http://www.ibm.com/legal/copytrade.shtml (www.ibm.com/legal/copytrade.shtml).

Adobe, Acrobat, PostScript et toutes les marques incluant Adobe sont des marques d'Adobe Systems Incorporated aux Etats-Unis et/ou dans certains autres pays.

IT Infrastructure Library est une marque de The Central Computer and Telecommunications Agency qui fait désormais partie de The Office of Government Commerce.

Intel, le logo Intel, Intel Inside, le logo Intel Inside, Intel Centrino, le logo Intel Centrino, Celeron, Intel Xeon, Intel SpeedStep, Itanium, et Pentium sont des marques d'Intel Corporation ou de ses filiales aux Etats-Unis et dans certains autres pays.

Linux est une marque de Linus Torvalds aux Etats-Unis et/ou dans certains autres pays.

Microsoft, Windows, Windows NT et le logo Windows sont des marques de Microsoft Corporation aux Etats-Unis et/ou dans certains autres pays.

ITIL est une marque de The Office of Government Commerce et est enregistrée au bureau américain Patent and Trademark Office.

UNIX est une marque enregistrée de The Open Group aux Etats-Unis et/ou dans certains autres pays.

Java ainsi que tous les logos et toutes les marques incluant Java sont des marques d'Oracle et/ou de ses sociétés affiliées.

Cell Broadband Engine est une marque de Sony Computer Entertainment, Inc. aux Etats-Unis et/ou dans certains autres pays, et sont utilisées sous licence.

Linear Tape-Open, LTO, le logo LTO, Ultrium et le logo Ultrium sont des marques de HP, IBM Corp. et Quantum aux Etats-Unis et/ou dans certains autres pays.

Index

Caractères spéciaux

Nombres

A

B

C

D

E

F

G

H

I

K

L

M

N

P

R

S

T

U

V

W