Installation, migration et configuration

Table des matières

Présentation de l'environnement

IBM Security Key Lifecycle Manager offre des fonctions simplifiées de gestion du cycle de vie des clés dans une solution facile à installer, à déployer et à gérer.

Ce document traite des tâches que vous devez effectuer pour installer et configurer IBM Security Key Lifecycle Manager.

Déploiement sur les systèmes Windows, Linux et AIX

Le déploiement d'IBM Security Key Lifecycle Manager comprend un processus d'installation qui permet de collecter des informations pour la préparation d'une base de données, la configuration d'ID utilisateur et la migration facultative de données depuis Encryption Key Manager.

Sur les systèmes Windows, Linux et AIX, le programme d'installation d'IBM Security Key Lifecycle Manager déploie le serveur IBM Security Key Lifecycle Manager et les composants middleware requis sur le même ordinateur. Vérifiez que l'ordinateur dispose de l'espace disque disponible, de la vitesse de processeur et de la mémoire nécessaires pour supporter la charge de travail.

IBM Security Key Lifecycle Manager peut être exécuté sur un serveur membre d'un environnement de contrôleurs de domaine, mais il n'est pas accepté sur un contrôleur de domaine principal ou de secours.

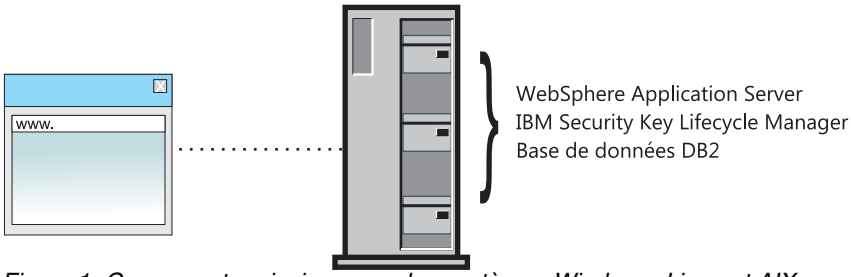

Figure 1. Composants principaux sur les systèmes Windows, Linux et AIX

Présentation de l'installation

L'installation d'IBM Security Key Lifecycle Manager implique de préparer le logiciel puis d'exécuter le programme d'installation.

L'installation d'IBM Security Key Lifecycle Manager inclut les principales étapes suivantes :

1. Planifiez votre installation et complétez les formulaires d'installation. Pour les détails, voir «Planification de l'installation», à la page 5 et «Feuilles de travail de préinstallation», à la page 39.
2. Installez et configurez IBM Security Key Lifecycle Manager. L'installation se compose de plusieurs phases :
   a. L'introduction qui comprend la fenêtre de présentation et de sélection de la langue, la fenêtre de sélection des packages d'installation, la fenêtre du contrat de licence, et la fenêtre d'information sur l'espace disque.

b. Installations de DB2, WebSphere Application Server, et IBM Security Key Lifecycle Manager qui comprennent des fenêtres pour la collecte d'informations. Une fois que vous avez saisi ces informations, le programme lance l'installation de DB2, WebSphere Application Server, et d'IBM Security Key Lifecycle Manager pendant cette phase.

3. Connectez-vous et vérifiez l'installation. Remédiez aux éventuels problèmes. Pour les détails, voir «URL de connexion», à la page 69 et «Vérification de l'installation», à la page 81.

Remarque : L'installation peut prendre plus d'une demi-heure.

Préparation du module d'installation

Le module d'installation est disponible sur DVD ou sous forme d'un ou de plusieurs fichiers compressés à télécharger.

Installation à partir d'un DVD

1. Insérez ou montez le DVD, selon le système d'exploitation utilisé.
2. Recherchez les scripts d'installation dans le répertoire racine du DVD.

Installation à partir des modules téléchargés

Les fichiers du module d'installation sont des fichiers archive contenant les fichiers utilisés lors de l'installation. Les modules libellés «eImage *<entier>*» doivent être assemblés dans un répertoire d'installation temporaire sur votre ordinateur. Par exemple, un module peut porter le libellé `eImage 1`. Les chemins d'accès aux répertoires d'installation temporaires ne peuvent pas contenir d'espaces ni de caractères spéciaux.

Pour effectuer l'installation à partir des fichiers eImage, effectuez les étapes d'assemblage suivantes :

1. Téléchargez les fichiers des modules eImage et placez-les dans un répertoire temporaire adéquat.
2. Décompressez tous les fichiers des modules eImage dans un répertoire temporaire différent du premier.

   Systèmes Windows

   Extrayez le premier module eImage dans un sous-répertoire temporaire correspondant au nom du premier module eImage. Extrayez les modules suivants dans le sous-répertoire correspondant au nom du premier module eImage (et non pas au nom du module suivant).

   Par exemple, si vous utilisez le répertoire temporaire `C:\mysklmV301download`, procédez comme suit :

   a. Extrayez tout d'abord le package eImage dans un sous-répertoire, par exemple `C:\mysklmV301download\`*`partNumberOfLatestBuild`*.
   b. Extrayez ensuite le package 2 dans le même sous-répertoire que celui du package 1 eImage, `C:\mysklmV301download\`*`partNumberOfLatestBuild`* dans le cas présent.
   c. Extrayez les packages suivants dans le sous-répertoire du package 1 eImage, `C:\mysklmV301download\`*`partNumberOfLatestBuild`* dans le cas présent.

   Systèmes Linux

   Sur les systèmes Linux, les fichiers compressés sont déployés

automatiquement dans le répertoire temporaire, sans qu'il soit nécessaire de spécifier les noms de package.

Systèmes AIX

Sur les systèmes AIX, les fichiers compressés sont déployés automatiquement dans le répertoire temporaire, sans qu'il soit ajouté le nom du module.

Vous devez utiliser un utilitaire `tar` GNU pour extraire les modules eImage. Effectuez les étapes suivantes :

a. Téléchargez et installez l'utilitaire `tar` GNU à partir de cette adresse :

   ftp://ftp.software.ibm.com/aix/freeSoftware/aixtoolbox/RPMS/ppc/tar/tar-1.22-1.aix6.1.ppc.rpm

b. Extrayez chaque module. Par exemple, pour extraire un premier fichier eImage nommé `CZJD7ML.tar`, exécutez cette commande :

   ```
   /usr/bin/gtar -xvf CZJD7ML.tar
   ```

c. Répétez cette commande en spécifiant le nom de chacun des autres fichiers eImage.

3. Localisez et exécutez les fichiers d'installation dans le répertoire temporaire où vous avez décompressé les modules d'installation. Par exemple, localisez :
   - Systèmes Windows : `launchpad.bat`
   - Autres systèmes : `launchpad.sh`

Pour effectuer une mise à niveau vers un groupe de correctifs, suivez les instructions du fichier Readme disponible sur le site Web IBM Fix Central à l'adresse : http://www.ibm.com/support/fixcentral. Pour accéder à ce site, effectuez les étapes suivantes :

1. Cliquez sur **Sélectionner un produit**.
2. Dans la liste déroulante **Groupe de produits**, sélectionnez `IBM Security`.
3. Dans la liste déroulante **Select from IBM Security**, sélectionnez `IBM Security Key Lifecycle Manager`.

Planification de l'installation

Avant d'installer IBM Security Key Lifecycle Manager, comprenez les prérequis et planifiez votre environnement en conséquence.

Avant d'installer IBM Security Key Lifecycle Manager, procédez comme suit :

- Utilisez la feuille de travail («Feuilles de travail de préinstallation», à la page 39) pour vous aider à effectuer les opérations de planification.
- Déterminez la topologie de IBM Security Key Lifecycle Manager, décrite à la rubrique «Déploiement sur les systèmes Windows, Linux et AIX», à la page 1.
- Vérifiez la configuration matérielle de votre système. Pour plus d'informations, voir «Configuration matérielle requise», à la page 7.
- Assurez-vous que vous disposez de la version appropriée du système d'exploitation et que tous les correctifs requis ont été installés. Pour plus d'informations sur les versions de système d'exploitation requises, voir «Configuration requise pour les systèmes d'exploitation», à la page 8.
- Vérifiez que les paramètres de noyau sont corrects pour les systèmes d'exploitation nécessitant une mise à jour. Pour plus de détails, voir «Paramètres de noyau Db2», à la page 14.
- Si vous souhaitez utiliser la version de Db2 installée sur votre système, vérifiez que vous disposez de la version logicielle requise pour Db2. Pour plus d'informations sur les versions de Db2 prises en charge, voir «Configuration logicielle requise», à la page 13.
- Déterminez si vous voulez procéder à la migration de la configuration provenant d'une version antérieure d'Encryption Key Manager. Pour plus d'informations sur la migration, voir «Planification de la migration», à la page 27.
- Choisissez le mode d'installation à utiliser pour IBM Security Key Lifecycle Manager : graphique ou silencieux. Pour une description des différents modes d'installation, voir «Types d'installation», à la page 23.

Définitions relatives à un répertoire *HOME* et d'autres variables de répertoire

Vous pouvez personnaliser le répertoire *HOME* (la racine) en fonction de votre propre implémentation. Remplacez la définition de la variable de répertoire de manière appropriée.

Le tableau ci-après contient des définitions par défaut permettant de représenter le niveau de répertoire *HOME* de plusieurs chemins d'installation du produit.

Tableau 1. Répertoire HOME et autres variables de répertoire

Variable de répertoire	Définition par défaut	Description
DB_HOME	**Systèmes Windows** *drive*:\Program Files\IBM\DB2SKLMV301 **Systèmes AIX et Linux** /opt/IBM/DB2SKLMV301	Répertoire contenant l'application Db2 pour IBM Security Key Lifecycle Manager.

Tableau 1. Répertoire HOME et autres variables de répertoire (suite)

Variable de répertoire	Définition par défaut	Description
DB_INSTANCE_HOME	**Windows** *unité**db2adminID* Par exemple, si la valeur d'*unité* est `C:` et que l'administrateur Db2 par défaut est `sklmdb31`, *DB_INSTANCE_HOME* est `C:\SKLMDB301`. **Linux et AIX** `/home/`*db2adminID*	Répertoire contenant l'instance de base de données Db2 pour IBM Security Key Lifecycle Manager.
RACINE_WAS	**Windows** *drive*`:\Program Files\IBM\WebSphere\AppServer` **Linux et AIX** *path*`/IBM/WebSphere/AppServer` Par exemple : `/opt/IBM/WebSphere/AppServer`	Répertoire de base de WebSphere Application Server.
SKLM_HOME	**Windows** *WAS_HOME*`\products\sklm` **Linux et AIX** *RACINE_WAS*`/products/sklm`	Répertoire de base d'IBM Security Key Lifecycle Manager.
SKLM_INSTALL_HOME	**Windows** *drive*`:\Program Files\IBM\SKLMV301` **Linux et AIX** *path*`/IBM/SKLMV301`	Répertoire contenant la licence et les fichiers de migration d'IBM Security Key Lifecycle Manager.

SKLM_DATA	**Windows**
	WAS_HOME`\products\sklm\data`
	`C:\Program Files\IBM\WebSphere\AppServer\products\sklm\data`
	Linux et AIX
	WAS_HOME`\products\sklm/data`
	`/opt/IBM/WebSphere/AppServer/products/sklm/data`
		Répertoire contenant les fichiers exportés à partir d'IBM Security Key Lifecycle Manager, tels que les fichiers de sauvegarde, les certificats exportés et les fichiers d'exportation de groupes d'unités. En outre, vous devez enregistrer les fichiers que vous souhaitez importer dans IBM Security Key Lifecycle Manager dans ce répertoire.

IM_INSTALL_DIR	**Windows** *unité*`:\Program Files\IBM\Installation Manager` **Linux et UNIX** `/opt/ibm/InstallationManager`	Répertoire dans lequel IBM Installation Manager est installé.

Tableau 1. Répertoire HOME et autres variables de répertoire (suite)

Variable de répertoire	Définition par défaut	Description
REP_DONNEES_IM	**Windows** *unité*:\ProgramData\IBM\Installation Manager **Linux et UNIX** /var/ibm/InstallationManager	Répertoire des données utilisé pour stocker des informations sur les produits qui sont installés avec Installation Manager. **Remarque :** ProgramData\ est un dossier masqué ; pour le voir, vous devez modifier les préférences d'affichage dans l'Explorateur pour afficher les dossiers et les fichiers masqués.

Configuration matérielle et logicielle requise

Votre environnement doit satisfaire aux conditions de configuration système minimale pour installer IBM Security Key Lifecycle Manager.

La configuration matérielle et logicielle requise publiée est exacte au moment de la publication.

Vous pouvez aussi consulter le document relatif à la configuration système requise à l'adresse http://www-969.ibm.com/software/reports/compatibility/clarity/softwareReqsForProduct.html.

1. Indiquez IBM Security Key Lifecycle Manager.
2. Sélectionnez la version du produit. Par exemple, 3.0.
3. Sélectionnez le système d'exploitation.
4. Cliquez sur **Envoyer**.

Configuration matérielle requise

Vérifiez que le système dispose de l'espace disque disponible, de la vitesse de processeur et de la mémoire nécessaires pour installer IBM Security Key Lifecycle Manager.

Tableau 2. Configuration matérielle requise

Composants système	Valeurs minimales	Valeurs recommandées
Mémoire système (RAM)	4 Go	8 Go
Vitesse du processeur	**Systèmes Linux et Windows** Monoprocesseur 1.0 GHz **Systèmes AIX** 1,5 GHz (2 voies)	**Systèmes Linux et Windows** Double processeur 3,0 GHz **Systèmes AIX** 1,5 GHz (4 voies)
Espace disque libre pour IBM Security Key Lifecycle Manager et les produits prérequis tels que Db2	16 Go	30 Go
Espace disque libre dans /tmp ou C:\temp	4 Go	4 Go

Tableau 2. Configuration matérielle requise (suite)

Composants système	Valeurs minimales	Valeurs recommandées
Espace disque libre Db2 dans le répertoire `/home` ou l'unité système pour Db2	7 Go	25 Go
Espace disque libre dans le répertoire `/var` pour Db2	1 Go sur les systèmes d'exploitation Linux et UNIX	1 Go sur les systèmes d'exploitation Linux et UNIX
Tous les systèmes de fichiers doivent être accessibles en écriture. * Valeurs minimales : ces valeurs permettent d'utiliser les fonctions de base d'IBM Security Key Lifecycle Manager. ** Valeurs recommandées : Vous devez utiliser des valeurs plus importantes, adaptées à votre environnement de production. La configuration requise critique est destinée à fournir une quantité adéquate de mémoire système et d'espace disque et d'échange libre. La vitesse du processeur est un facteur moins important. Sur les systèmes d'exploitation Linux et UNIX, vous devez installer votre produit Db2 dans un répertoire vide. Si le répertoire que vous spécifiez comme chemin d'installation contient des sous-répertoires ou des fichiers, l'installation de Db2 risque d'échouer. Sur les systèmes d'exploitation Linux et UNIX, vous devez disposer de 4 Go d'espace libre dans le répertoire «`$HOME`». Sur les systèmes d'exploitation Linux et UNIX, vous devez disposer d'au moins 16 Go d'espace libre dans les répertoires «/» et «`/opt`». L'installation sur des lecteurs réseau mappés ou des partitions montées n'est pas prise en charge. Si plusieurs composants du système sont installés sur le même lecteur Windows ou la même partition UNIX, l'espace total pour tous ces composants doit être disponible dans ce lecteur ou cette partition.		

Configuration requise pour les systèmes d'exploitation

IBM Security Key Lifecycle Manager est pris en charge sur plusieurs systèmes d'exploitation. Pour installer IBM Security Key Lifecycle Manager, assurez-vous que votre système répond aux exigences du système d'exploitation.

Tableau 3. Configuration requise pour les systèmes d'exploitation

Système d'exploitation	Utilisation de Db2 Advanced Workgroup Server Edition version 11.1.2.2
AIX versions 7.1 et 7.2 en mode 64 bits. Les serveurs basés sur un processeur POWER7 sont pris en charge. • Un noyau AIX 64 bits est requis. • Utilisez le niveau de technologie 4 d'AIX 7.1, Service Pack 6. Le niveau minimal d'exécution de XL C/C++ requiert les fichiers xlC.rte 12.1.2.0.	✓
Windows Server 2012 x86_64 bits pour : • Standard Edition	✓
Windows Server 2012 **R2** x86_64 bits pour : • Standard Edition	✓

Tableau 3. Configuration requise pour les systèmes d'exploitation (suite)

Système d'exploitation	**Utilisation de Db2 Advanced Workgroup Server Edition version 11.1.2.2**
Windows Server 2016 x86_64 bits pour : • Standard Edition	✓
Red Hat Enterprise Linux version 6.7 x86_64 bits	✓
Red Hat Enterprise Linux version 7.1 x86_64 bits	✓
Red Hat Enterprise Linux version 7.1 (IBM Z) x86_64 bits	✓
Red Hat Enterprise Linux version 7.1 (PowerPC Little Endian (LE)) x86_64 bits	✓
Ubuntu 16 x86_64 bits	✓
SuSE Linux Enterprise Server version 12 x86_64 bits	✓
SuSE Linux Enterprise Server version 12 (IBM Z) x86_64 bits	✓

N'installez pas IBM Security Key Lifecycle Manager sur des systèmes dotés d'un système d'exploitation renforcé.

Vérifiez que l'interpréteur de commandes bash est installé avant d'installer IBM Security Key Lifecycle Manager sur les systèmes d'exploitation AIX.

Vérifiez que l'interpréteur de commandes C (csh) est installé avant d'installer IBM Security Key Lifecycle Manager sur les systèmes d'exploitation Linux.

Avant d'installer IBM Security Key Lifecycle Manager sur un système d'exploitation Red Hat Enterprise Linux, vérifiez que les bibliothèques requises qui sont décrites dans la note technique suivante sont installées : https://www-304.ibm.com/support/docview.wss?uid=swg21459143

Avant d'installer IBM Security Key Lifecycle Manager sur un système d'exploitation AIX, vérifiez que les bibliothèques requises qui sont décrites dans la note technique suivante sont installées : http://www-01.ibm.com/support/docview.wss?uid=swg21631478

Conditions d'accès

Installez IBM Security Key Lifecycle Manager en tant qu'administrateur (utilisateur root).

Vous pouvez également installer IBM Security Key Lifecycle Manager en tant qu'utilisateur non root uniquement sur le système d'exploitation Linux.

Modules Linux

Sur les plateformes Linux, IBM Security Key Lifecycle Manager requiert le module `compat-libstdc++`, qui contient `libstdc++.so.6`. Il nécessite également le module `libaio`, qui contient la bibliothèque asynchrone requise pour les serveurs de base de données Db2.

- Module `libstdc`

  Pour déterminer si vous avez ce module, exécutez la commande suivante :

  ```
  rpm -qa  | grep -i "libstdc"
  ```

  Si le module n'est pas installé, recherchez le fichier `rpm` sur votre support d'installation d'origine et installez-le.

  ```
  find support_installation -name compat-libstdc++*
  rpm -ivh chemin_d'accès_complet_au_fichier_rpm_compat-libstdc++
  ```

- Module `libaio`

  Pour déterminer si vous avez ce module, exécutez la commande suivante :

  ```
  rpm -qa  | grep -i "libaio"
  ```

  Si le module n'est pas installé, recherchez le fichier `rpm` sur votre support d'installation d'origine et installez-le.

  ```
  find support_installation -name libaio*
  rpm -ivh chemin_d'accès_complet_au_fichier_rpm_libaio
  ```

Sur les systèmes Red Hat Enterprise Linux 64 bits, l'installation de Db2 requiert l'installation de deux packages `libaio` distincts avant l'exécution de **db2setup**. Ces packages s'appellent tous les deux `libaio`. Toutefois, il y a deux fichiers RPM distincts à installer : l'un est un fichier RPM i386 et l'autre, un fichier RPM x86_64.

Pour installer IBM Security Key Lifecycle Manager sur Red Hat Enterprise Linux 6.7, vous devez mettre à niveau la bibliothèque glibc 32 bits vers la version 7.3 ou supérieure.

1. Configurez le système avec Red Hat Enterprise Linux 6.7, pour obtenir les bibliothèques. Pour la procédure d'enregistrement et d'abonnement d'un système au portail client de Red Hat à l'aide du gestionnaire d'abonnements Red Hat, voir https://access.redhat.com/solutions/253273.
2. Mettez à niveau la bibliothèque glibc.

   ```
   yum install glibc-2.12-1.166.el6_7.3.i686
   ```

3. Exécutez l'installation d'IBM Security Key Lifecycle Manager.

Installation des bibliothèques requises sur des systèmes Red Hat Enterprise Linux :

Pour exécuter les commandes d'installation en mode graphique ou silencieux, vous devez au préalable avoir installé les bibliothèques requises sur les systèmes Red Hat Enterprise Linux.

Procédure

1. Montez le DVD de distribution Red Hat Enterprise Linux sur le système. Insérez le DVD dans le lecteur de DVD.
2. Sélectionnez l'option d'ouverture d'une fenêtre de terminal en tant que root.
3. Exécutez les commandes :

   ```
   [root@localhost]# mkdir /mnt/cdrom
   [root@localhost]# mount -o ro /dev/cdrom /mnt/cdrom
   ```

4. Créez le fichier texte `server.repo` dans le répertoire `/etc/yum.repos.d`.

Remarque : Pour utiliser `gedit` :

a. Exécutez la commande :

```
[root@localhost]# gedit /etc/yum.repos.d/server.repo
```

b. Ajoutez le texte suivant au fichier :

```
[server]
name=server
baseurl=file:///mnt/cdrom/Workstation
enabled=1
```

Où `baseurl` dépend du point de montage et de la distribution de Red Hat Enterprise Linux.

Dans l'exemple, le point de montage est `cdrom` et la distribution de Red Hat Enterprise Linux est `Workstation`, mais elle peut être `sever`.

5. Exécutez la commande :

```
[root@localhost]# yum clean all
```

6. Exécutez la commande pour importer les clés publiques associées :

```
[root@localhost]# rpm --import /mnt/cdrom/*GPG*
```

7. Exécutez les commandes pour installer les bibliothèques requises :

```
[root@localhost]# yum install gtk2.i686
[root@localhost]# yum install libXtst.i686
```

Si vous avez reçu le message ci-dessus à propos de l'absence de libstdc++, installez la bibliothèque libstdc++ :

```
[root@localhost]# yum install compat-libstdc++
```

Lors de l'installation, vous pouvez recevoir des invites similaires à celles de l'exemple. Répondez par `'y'` (oui).

Exemple :

```
Total download size: 15 M
Installed size: 47 M
Is this ok [y/N]: y
```

Remarque : L'extension de nom de package (.i686) peut changer dans la commande en fonction de la plate-forme matérielle que vous utilisez. Le tableau répertorie les valeurs valides pour l'extension du nom de package. Noms de package Red Hat Enterprise Linux 6.0 package sur différentes plate-formes :

Plate-forme	32 bits	64 bits
x86/x86_64	i686	x86_64
ppc/ppc64	ppc	ppc64
s390/s390x	s390	s390x

Configuration requise pour le système d'exploitation Linux sous System z

Avant d'installer IBM Security Key Lifecycle Manager sous Linux on System z, procédez comme suit :

1. Vérifiez que les bibliothèques suivantes sont présentes sur le système ; elles sont nécessaires pour l'installation de Db2.
   - libpam.so.0
   - libaio.so.1

- libstdc++.so.6.0.8
- libstdc++33
- ksh93

Si le système ne contient pas les bibliothèques nécessaires, exécutez la commande suivante.

```
yum install <library_name>
```

En cas de problème lié à une bibliothèque, utilisez la commande suivante pour supprimer la bibliothèque.

```
yum remove <library_name>
```

Pour plus d'informations, voir Db2 documentation http://www.ibm.com/support/knowledgecenter/en/SSEPGG_11.1.0/com.ibm.db2.luw.qb.server.doc/doc/r0008865.html.

2. For the following operating system versions, install the IBM XL/XL C++ runtime environment.
   - Red Hat Enterprise Linux 7.1 (RHEL 7.1)
   - Red Hat Enterprise Linux 7.2 (RHEL 7.2)
   - SUSE Linux Enterprise Server 11 Service Pack 3 (SLES 11 SP3)
   - SUSE Linux Enterprise Server 12 (SLES 12)
   - SUSE Linux Enterprise Server 12 Service Pack 1 (SLES 12 SP1)

   To install the IBM XL/XL C++ runtime environment:
   a. Extrayez le fichier d'installation.
   b. Exécutez **./install**.
   c. Exécutez la commande suivante si un message d'erreur s'affiche sur les bibliothèques manquantes.

      ```
      yum install <missing_lib_name>
      ```
3. Créez un lien entre les bibliothèques qui sont installées en exécutant les commandes suivantes :

   ```
   ln -s /opt/ibm/lib/* /usr/lib/
   ln -s /opt/ibm/lib64/* /usr/lib64/
   ```
4. Définissez LD_LIBRARY_PATH à l'aide de la commande suivante :

   ```
   LD_LIBRARY_PATH=/opt/ibm/lib:/opt/ibm/lib64:/usr/lib64;
   export LD_LIBRARY_PATH
   ```
5. Vérifiez que le répertoire /tmp dispose de toutes les autorisations. Pour fournir les autorisations, exécutez la commande suivante.

   ```
   chmod 777 /tmp
   ```

Configuration requise pour le système d'exploitation Linux on PowerPC

Avant d'installer IBM Security Key Lifecycle Manager sur le système d'exploitation PowerPC Little Endian (LE), vérifiez que la configuration requise est appliquée pour votre système.

1. Installez l'environnement IBM XL/XL C++.
   a. Extrayez le fichier d'installation dans un répertoire.

      ```
      tar -xvf <setup_name>
      ```
   b. Exécutez **./install**.
2. Après avoir installé le package, créez un lien entre les bibliothèques qui sont installées en exécutant les étapes suivantes.

   ```
   ln -s /opt/ibm/lib/* /usr/lib/
   ln -s /opt/ibm/lib64/* /usr/lib64/
   ```

3. Définissez LD_LIBRARY_PATH à l'aide de la commande suivante.

```
LD_LIBRARY_PATH=/opt/ibm/lib:/opt/ibm/lib64:/usr/lib64;
export LD_LIBRARY_PATH
```

4. Avant de commencer le processus d'installation, assurez-vous que le répertoire /tmp possède toutes les autorisations. Pour fournir les autorisations, exécutez la commande suivante.

```
chmod 777 /tmp
```

Désactivation de Security Enhanced Linux

IBM Security Key Lifecycle Manager sur les systèmes d'exploitation Linux peut rencontrer des problèmes fonctionnels lorsque le paramètre Security Enhanced Linux (SELINUX) est activé.

Pourquoi et quand exécuter cette tâche

Par exemple, un problème peut se produire au niveau des connexions TCP/IP sur les ports du serveur. Suivez les étapes fournies dans la documentation Linux pour désactiver Security Enhanced Linux.

Configuration logicielle requise

IBM Security Key Lifecycle Manager nécessite des programmes middleware et d'autres logiciels pour ses opérations. IBM Security Key Lifecycle Manager installe les programmes middleware tels que WebSphere Application Server, Java Runtime Environment (JRE) et DB2 et est livré avec le package IBM Security Key Lifecycle Manager.

Si Db2 est déjà installé sur le système, reportez-vous à la section «Exigences DB2», à la page 14.

Configuration requise pour WebSphere Application Server

IBM Security Key Lifecycle Manager requiert WebSphere Application Server 9.0 et tout groupe de correctifs ou correctif APAR applicable et requis.

IBM Security Key Lifecycle Manager inclut et installe WebSphere Application Server. Pendant l'installation, IBM Security Key Lifecycle Manager personnalise la configuration et les profils de WebSphere Application Server en fonction de ses opérations. Cette personnalisation peut provoquer des problèmes avec les produits qui utilisent le même serveur lorsque vous désinstallez IBM Security Key Lifecycle Manager. Par conséquent, vous devez prendre en considération les éléments suivants afin d'éviter les problèmes :

- N'installez pas IBM Security Key Lifecycle Manager dans une instance de WebSphere Application Server fournie par un autre produit.
- N'installez pas un autre produit dans l'instance de WebSphere Application Server fournie par IBM Security Key Lifecycle Manager.

Configuration requise pour un environnement Java Runtime Environment (JRE)

IBM Security Key Lifecycle Manager requiert Java Runtime Environment. IBM Java Runtime Environment est inclus avec WebSphere Application Server.

L'utilisation d'un kit de développement pour Java™ d'IBM® ou d'autres fournisseurs, installé de façon indépendante, n'est *pas* prise en charge. Pour plus d'informations, consultez le site http://www.ibm.com/support/knowledgecenter/SSEQTP_9.0.0/com.ibm.websphere.base.doc/ae/covr_javase8.html.

Exigences DB2

La base de données stocke les données d'IBM Security Key Lifecycle Manager. Avant d'installer IBM Security Key Lifecycle Manager, veillez à ce que les exigences de base de données soient respectées.

IBM Security Key Lifecycle Manager requiert Db2 Advanced Workgroup Server Edition, version 11.1.2.2 et les groupes de correctifs ultérieurs sur le même système où le serveur IBM Security Key Lifecycle Manager s'exécute.

Remarque :

- Vous devez utiliser IBM Security Key Lifecycle Manager pour gérer la base de données. Pour éviter tout problème de synchronisation des données, n'utilisez pas les outils de gestion fournis par l'application de base de données.
- Pour améliorer les performances de Db2 version 11.1.2.2 sous les systèmes AIX, veillez à installer et configurer le package de ports d'achèvement d'E-S (IOCP) décrit dans la documentation Db2 (http://www-01.ibm.com/support/knowledgecenter/SSEPGG_11.1.0/com.ibm.db2.luw.admin.perf.doc/doc/t0054518.html).
- Si une copie existante de Db2 Advanced Workgroup Server Edition a été installée en tant qu'utilisateur root au niveau de version correct pour le système d'exploitation, vous pouvez utiliser l'utiliser. Le programme d'installation d'IBM Security Key Lifecycle Manager ne détecte pas la présence de Db2. Vous devez indiquer le chemin d'installation de Db2.

Les systèmes SuSE Linux Enterprise Server Version 12 (System z) contiennent le package `libstdc++.6.so`. Mais, IBM Security Key Lifecycle Manager nécessite le package `libstdc++.5.so` pour l'installation de DB2.

Pour plus d'informations sur la configuration requise pour Db2, voir la documentation de DB2 (http://www-01.ibm.com/support/knowledgecenter/SSEPGG_11.1.0/com.ibm.db2.luw.admin.cmd.doc/doc/r0059710.html).

Paramètres de noyau Db2 :

Assurez-vous que les paramètres de noyau sont corrects pour le système d'exploitation pouvant nécessiter des mises à jour.

Systèmes AIX
Aucun paramètre requis.

Systèmes Linux
Pour plus d'informations sur les paramètre de noyau, voir la documentation DB2 http://www-01.ibm.com/support/knowledgecenter/SSEPGG_11.1.0/com.ibm.db2.luw.qb.server.doc/doc/t0008238.html.

Systèmes Windows
Aucun paramètre requis.

Exigences d'exécution XL C/C++ pour les systèmes Linux

IBM Security Key Lifecycle Manager requiert le module d'environnement d'exécution XL C/C++ pour les systèmes Linux.

Pour plus d'informations, voir :

http://www-01.ibm.com/support/docview.wss?uid=swg24041489

https://www.ibm.com/support/knowledgecenter/en/SSEPGG_11.1.0/com.ibm.db2.luw.apdv.gs.doc

Configuration requise pour le navigateur

Vous devez activer les cookies de session et Java Script dans le navigateur pour établir une session avec IBM Security Key Lifecycle Manager.

Les navigateurs pris en charge ne sont pas inclus dans l'installation du produit. Vous pouvez accéder à l'interface graphique utilisateur d'IBM Security Key Lifecycle Manager en utilisant l'un des navigateurs pris en charge (tout système confondu).

Tableau 4. Navigateurs pris en charge

Navigateur	Groupe de correctifs (Fix pack)	AIX	Windows Server 2012	Windows Server 2012 R2	Red Hat Enterprise Linux	SuSE Linux Enterprise Server
Microsoft Internet Explorer version 9.0	Aucun		✓	✓		
Microsoft Internet Explorer version 10.0	Aucun		✓	✓		
Microsoft Internet Explorer, version 11.0	Aucun		✓	✓		
Firefox ESR, version 24.0	Aucun	✓	✓	✓	✓	✓
Firefox ESR, version 31.0	Aucun	✓	✓	✓	✓	✓
Firefox ESR, version 38.0	Aucun	✓	✓	✓	✓	✓

ID utilisateur et mots de passe de l'administrateur

Les ID utilisateur de l'administrateur par défaut sont créés lorsque vous installez IBM Security Key Lifecycle Manager avec les droits d'accès requis pour l'administration du produit.

L'installation d'IBM Security Key Lifecycle Manager fournit les ID administrateur par défaut `WASAdmin`, `SKLMAdmin` et `sklmdb31`.

L'installation doit être effectuée par un ID administrateur local, qui est l'utilisateur root dans le cas des systèmes AIX ou Linux ou un membre du groupe Administrateurs pour les systèmes Windows. N'utilisez pas d'ID utilisateur du domaine pour installer IBM Security Key Lifecycle Manager.

Le tableau suivant présente les ID utilisateur.

Tableau 5. ID utilisateur et mots de passe de l'administrateur

Programme	ID utilisateur	Mot de passe
administrateur IBM Security Key Lifecycle Manager	**SKLMAdmin** En tant qu'administrateur principal disposant d'un plein accès à toutes les opérations, cet ID utilisateur a le rôle de superutilisateur `klmSecurityOfficer` dans le groupe nommé `klmSecurityOfficerGroup`. Cet ID utilisateur est insensible à la casse des caractères. Vous pouvez donc utiliser également `sklmadmin`. Utilisez l'ID `SKLMAdmin` pour administrer IBM Security Key Lifecycle Manager. Avec l'ID utilisateur `SKLMAdmin`, vous pouvez : • Afficher et utiliser l'interface IBM Security Key Lifecycle Manager. • Changer le mot de passe de l'administrateur d'IBM Security Key Lifecycle Manager. En revanche, vous ne pouvez pas : • Créer un ou plusieurs autres ID administrateur d'IBM Security Key Lifecycle Manager. • Effectuer des tâches d'administrateur de WebSphere Application Server telles que créer ou affecter un rôle. • Démarrez ou arrêtez le serveur.	Spécifiez un mot de passe durant l'installation et conservez-le en lieu sûr.

Tableau 5. ID utilisateur et mots de passe de l'administrateur (suite)

Programme	ID utilisateur	Mot de passe
administrateur WebSphere Application Server	**WASAdmin** Cet ID utilisateur est insensible à la casse des caractères. Vous pouvez donc utiliser également `wasadmin`, ou encore un ID utilisateur ayant été spécifié durant l'installation. N'utilisez pas : • L'ID utilisateur `SKLMAdmin` pour administrer WebSphere Application Server. • L'ID utilisateur `WASAdmin` pour administrer IBM Security Key Lifecycle Manager. L'ID utilisateur `WASAdmin` ne possède aucun rôle lui permettant d'utiliser IBM Security Key Lifecycle Manager. Cet ID administrateur est celui de l'administrateur de WebSphere Application Server. Avec l'ID utilisateur `wasadmin`, vous pouvez : • Afficher et utiliser l'interface de WebSphere Application Server. • Créer un ou plusieurs autres ID d'administrateur, groupes et rôles IBM Security Key Lifecycle Manager. • Réinitialiser le mot de passe de tout ID utilisateur d'IBM Security Key Lifecycle Manager, y compris celui de l'administrateur `SKLMAdmin`. • Démarrer et arrêter le serveur. En revanche, vous ne pouvez pas : • Utiliser IBM Security Key Lifecycle Manager pour effectuer des tâches qui lui sont propres. Par exemple, vous ne pouvez pas créer de groupes d'unités IBM Security Key Lifecycle Manager. • Effectuer d'autres tâches nécessitant un accès aux données de IBM Security Key Lifecycle Manager. L'ID utilisateur `wasadmin` n'a *pas* accès aux données d'IBM Security Key Lifecycle Manager en tant que superutilisateur.	Spécifiez un mot de passe durant l'installation et conservez-le en lieu sûr. Protégez l'ID utilisateur `WASAdmin` de la même manière que l'ID `SKLMAdmin`. L'ID utilisateur `WASAdmin` a le droit de réinitialiser le mot de passe de `SKLMAdmin`, de créer de nouveaux comptes d'utilisateur d'IBM Security Key Lifecycle Manager et de leur affecter des droits.
Base de données IBM Security Key Lifecycle Manager Db2		

Tableau 5. ID utilisateur et mots de passe de l'administrateur (suite)

Programme	ID utilisateur	Mot de passe
Propriétaire d'instance de la base de données	**Systèmes Windows, Linux ou AIX :** la valeur par défaut est `sklmdb31`. Vous pouvez spécifier une valeur différente durant l'installation. Cet ID est celui qui est utilisé par défaut, à l'installation, pour le propriétaire d'instance de la base de données. Ne spécifiez pas d'ID utilisateur de plus de huit caractères. Le nom de l'instance est également `sklmdb31`. Si Db2 est sur un système AIX ou Linux, votre ID utilisateur doit être dans le groupe bin ou root ou dans un groupe à part, dont root est membre. Si vous utilisez un ID utilisateur existant comme propriétaire d'instance de la base de données d'IBM Security Key Lifecycle Manager, il ne peut pas être propriétaire d'une autre instance de base de données. **Remarque :** N'utilisez pas de trait d'union (-) ni de caractère de soulignement (_) lorsque vous spécifiez un ID utilisateur pour une copie existante de Db2.	Spécifiez un mot de passe durant l'installation et conservez-le en lieu sûr. Il s'agit d'un mot de passe du système d'exploitation. Si vous en changez au niveau du système d'exploitation, vous devez ensuite le changer dans l'interface du produit. Pour plus d'informations, voir Réinitialisation d'un mot de passe..
Instance de base de données	L'ID administrateur `sklmdb31` dispose d'une instance Db2 nommée `sklmdb31`.	

Fichiers d'audit

IBM Security Key Lifecycle Manager possède un répertoire par défaut pour les données d'audit. L'emplacement du fichier dépend de la valeur de la propriété **`Audit.handler.file.name`** dans le fichier *SKLM_DATA*`/config/SKLMConfig.properties`.

La valeur par défaut est indiquée dans l'exemple ci-dessous.

```
Audit.handler.file.name=logs/audit/sklm_audit.log
```

Rôles utilisateur

IBM Security Key Lifecycle Manager fournit un rôle de superutilisateur (`klmSecurityOfficer` et `klmGUICLIAccessGroup`) et permet de spécifier des rôles d'administration aux pouvoirs plus limités afin de répondre aux besoins spécifiques de votre organisation. Par défaut, l'ID utilisateur `SKLMAdmin` a le rôle `klmSecurityOfficer`.

Pour les tâches de sauvegarde et de restauration, IBM Security Key Lifecycle Manager installe également le rôle `klmBackupRestoreGroup`, qui n'est initialement affecté à aucun ID utilisateur. L'installation d'IBM Security Key Lifecycle Manager crée des groupes prédéfinis d'administrateurs, d'opérateurs et d'auditeurs pour la gestion des unités de bande LTO.

L'ID utilisateur WASAdmin a le droit de créer et d'affecter ces rôles, ainsi que celui de changer le mot de passe de n'importe quel administrateur d'IBM Security Key Lifecycle Manager. Pour définir les limites d'administration d'IBM Security Key Lifecycle Manager, connectez-vous à la console WebSphere Integrated Solutions avec l'ID utilisateur WASAdmin et créez des rôles, des utilisateurs et des groupes. Affectez des rôles et des utilisateurs à un groupe. Par exemple, vous pouvez créer un groupe et lui affecter à la fois des utilisateurs et un rôle limitant les activités de ces utilisateurs à l'administration des unités de bande LTO. 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.

Avant de commencer, effectuez les tâches suivantes :

- Déterminez les limites exigées par votre organisation en matière d'administration des unités.

  Par exemple, il est possible qu'un groupe spécifique d'unités soit administré à part.
- Faites une estimation du nombre d'administrateurs nécessaires sur une période donnée. Pour plus de facilité, vous pouvez définir un groupe et un rôle déterminant les tâches auxquelles les utilisateurs de ce groupe auront accès.

  Par exemple, vous pouvez spécifier un groupe ayant des pouvoirs limités à la gestion des unités de bande 3592.

Droits disponibles

L'installation d'IBM Security Key Lifecycle Manager crée l'ID utilisateur SKLMAdmin, qui est le superutilisateur par défaut. A ce titre, il reçoit le rôle klmSecurityOfficer (responsable de la sécurité). Le processus d'installation déploie également des droits prédéfinis dans la liste de rôles d'administration de WebSphere Application Server.

Un *droit* accordé par IBM Security Key Lifecycle Manager autorise l'utilisation d'une action ou l'accès à un groupe d'unités. Une *rôle*, dans IBM Security Key Lifecycle Manager, représente un ou plusieurs droits. En revanche, dans l'interface graphique de WebSphere Application Server, le terme *rôle* désigne à la fois les droits et les rôles d'IBM Security Key Lifecycle Manager.

L'installation d'IBM Security Key Lifecycle Manager crée les groupes par défaut suivants.

klmSecurityOfficerGroup

L'installation affecte le rôle klmSecurityOfficer à ce groupe. Le rôle klmSecurityOfficer remplace l'ancien rôle klmApplicationRole dans le groupe qui a été nommé klmGroup. klmSecurityOfficerGroup remplace klmGroup.

Le rôle klmSecurityOfficer a :

- Un accès root à l'ensemble des droits et groupes d'unités décrits dans le tableau 6, à la page 20 et le tableau 7, à la page 21.
- Un droit d'accès à tout rôle ou groupe d'unités qui peut être créé.
- Le rôle suppressmonitor.

  WebSphere Application Server fournit le rôle suppressmonitor pour masquer dans le volet gauche de la console WebSphere Integrated Solutions des tâches qui ne sont pas utilisées par un administrateur IBM Security Key Lifecycle Manager. Les éléments masqués sont associés au serveur d'applications et comprennent les tâches d'administration de

WebSphere Application Server dans les dossiers `Sécurité`, `Identification et résolution des problèmes` et `Utilisateurs et groupes`.

klmBackupRestoreGroup
Permet de sauvegarder et de restaurer des données IBM Security Key Lifecycle Manager.

LTOAdmin
Permet d'administrer les unités dans la famille d'unités LTO avec des actions qui incluent la création, la visualisation, la modification, la suppression, l'obtention (exportation), la sauvegarde et la configuration.

LTOOperator
Permet de faire fonctionner les unités dans la famille d'unités LTO avec des actions qui incluent la création, la visualisation, la modification et la sauvegarde.

LTOAuditor
Permet d'auditer les unités dans la famille d'unités LTO avec des actions qui incluent la visualisation et l'audit.

klmGUICLIAccessGroup
Fournit aux utilisateurs un accès à l'interface graphique et à l'interface de ligne de commande d'IBM Security Key Lifecycle Manager. Chaque utilisateur du produit doit appartenir à ce groupe.

Remarque : En plus de cet accès au groupe, les utilisateurs doivent avoir d'autres accès pour être des utilisateurs opérationnels du produit.

Une utilisateur ayant l'un des droits décrits dans le tableau 6 peut voir :

- Les paramètres de configuration globale d'IBM Security Key Lifecycle Manager qui sont définis dans le fichier SKLMConfig.properties.
- Le statut du serveur de clés et la date de la dernière sauvegarde.

Tableau 6. Droits d'utilisation des actions

Droit	Actions autorisées	Sans lien avec les groupes d'unités	Associé aux groupes d'unités
`klmCreate`	Créer des objets, mais pas les visualiser ni les modifier ni les supprimer.		✓
`klmDelete`	Supprimer des objets, mais pas les visualiser, les modifier ni les créer.		✓
`klmGet`	Exporter une clé ou un certificat pour une unité client		✓
`klmModify`	Modifier des objets, mais pas les visualiser ni les créer ni les supprimer		✓

Tableau 6. Droits d'utilisation des actions (suite)

Droit	Actions autorisées	Sans lien avec les groupes d'unités	Associé aux groupes d'unités
`klmView`	Visualiser des objets, mais pas les créer ni les supprimer ni les modifier. Par exemple, vous devez avoir ce droit pour voir les tâches que vous voulez exécuter dans l'interface graphique.		✓
`klmAdminDeviceGroup`	Administrer. Créer un groupe d'unités, définir ses paramètres par défaut, visualiser, supprimer un groupe d'unités vides. Ce droit ne donne pas accès aux unités, aux clés et aux certificats.	✓	
`klmAudit`	Visualiser des données d'audit à l'aide de la commande **`tklmServedDataList`**.	✓	
`klmBackup`	Créer et supprimer une sauvegarde de données IBM Security Key Lifecycle Manager	✓	
`klmConfigure`	Lire et changer les propriétés de configuration d'IBM Security Key Lifecycle Manager ou agir sur un certificat SSL. Ajouter, visualiser, mettre à jour ou supprimer le magasin de clés.	✓	
`klmRestore`	Restaurer une copie de sauvegarde de données IBM Security Key Lifecycle Manager.	✓	

Le rôle `klmSecurityOfficer` a également un accès root aux droits qui s'exercent sur tous les groupes d'unités.

Tableau 7. Groupes d'unités

Droit	Actions autorisées sur ces objets
`LTO`	famille d'unités LTO
`TS3592`	famille d'unités 3592
`DS5000`	famille d'unités DS5000
`DS8000`	famille d'unités DS8000
`BRCD_ENCRYPTOR`	groupe d'unités BRCD_ENCRYPTOR
`ONESECURE`	groupe d'unités ONESECURE
`ETERNUS_DX`	Groupe d'unités ETERNUS_DX
`XIV`	Groupe d'unités XIV
`IBM_SYSTEM_X_SED`	Groupe d'unités IBM_SYSTEM_X_SED
`GPFS (IBM Spectrum Scale)`	Famille d'unités GPFS
`GENERIC`	Objets dans la famille d'unités GENERIC.

Tableau 7. Groupes d'unités (suite)

Droit	Actions autorisées sur ces objets
groupeunitésutilisateur	Instance définie par l'utilisateur, telle que `monLTO`, que vous créez manuellement à partir d'une famille d'unités prédéfinie telle que LTO.

Types d'installation

Vous pouvez installer IBM Security Key Lifecycle Manager dans une interface graphique ou en mode silencieux.

- Installation à l'aide d'une interface graphique via un assistant.
- Installation automatisée en mode silencieux à l'aide des fichiers de réponses des options de configuration.

Remarques :

- IBM Security Key Lifecycle Manager ne prend pas en charge l'installation en mode console.
- N'effectuez pas l'installation d'IBM Security Key Lifecycle Manager à partir d'une unité réseau ni d'une unité montée. Par exemple, ne spécifiez pas l'une de ces instructions **net use** comme emplacement de répertoire pour ensuite tenter une installation :

```
net use z: \\serveur\partage
net use \\serveur\partage
```

Installation en mode graphique

IBM Security Key Lifecycle Manager fournit un programme d'installation pour l'interface graphique. IBM Installation Manager est utilisé pour installer IBM Security Key Lifecycle Manager et ses composants. Il présente une série de panneaux qui demandent les informations nécessaires pour l'installation.

Exécutez les étapes suivantes pour installer IBM Security Key Lifecycle Manager en mode graphique.

- Lancez l'assistant d'installation.
- Renseignez les pages de l'assistant d'installation en entrant les options de configuration. Pour plus de détails, voir «Installation d'IBM Security Key Lifecycle Manager en mode graphique», à la page 44.
- Vérifiez que le serveur IBM Security Key Lifecycle Manager est opérationnel. Pour plus de détails, voir «Vérification de l'installation», à la page 81.

Panneaux d'installation et de migration

L'installation d'IBM Security Key Lifecycle Manager en mode graphique requiert de démarrer de l'assistant d'installation, de naviguer à travers une série de panneaux d'installation et de fournir les informations nécessaires.

Vous devez sélectionner l'environnement local à utiliser pour le processus d'installation. L'environnement local détermine la langue utilisée par le programme d'installation. Entrez le numéro s'affichant en regard de votre environnement local puis appuyez sur Entrée.

Les panneaux suivants peuvent s'afficher lors de l'installation :

1. Fenêtre d'Installation Manager avec les modules d'installation tels qu'IBM Installation Manager, IBM DB2, IBM WebSphere Application Server et IBM Security Key Lifecycle Manager
2. Contrat de licence du logiciel

3. Sélection du répertoire d'installation pour IBM Installation Manager et les autres modules d'installation.
4. Sélection de la langue pour la traduction du module
5. Sélection des fonctions du module à installer
6. Options de configuration de Db2
7. Options de configuration de IBM Security Key Lifecycle Manager
8. Sélection de la migration d'Encryption Key Manager
9. Aperçu du package d'installation
10. Progression de l'installation d'IBM Security Key Lifecycle Manager
11. Récapitulatif de l'installation

Remarques :

- Lorsque vous installez IBM Security Key Lifecycle Manager, conservez le chemin par défaut pour **Répertoire des ressources partagées** (Shared Resources Directory). IBM Installation Manager utilise cet emplacement pour télécharger des artefacts et pour stocker des informations sur les modules installés.
- Une fois l'installation terminée, une page affiche le statut de l'installation et la liste des modules qui sont installés. Vous devez sélectionner **Aucun** pour indiquer au programme d'installation de ne pas créer un profil, puis cliquer sur **Terminer**.

Les panneaux suivants peuvent s'afficher si une migration est effectuée lors de l'installation :

1. Introduction
2. Contrat de licence du logiciel
3. Répertoire de Db2
4. **Informations de migration**
5. **Récapitulatif de la migration**
6. Récapitulatif des prérequis
7. Progression de l'installation d'Db2
8. Début de l'installation d'IBM Security Key Lifecycle Manager
9. Répertoire d'installation d'IBM Security Key Lifecycle Manager et de WebSphere Application Server
10. Informations sur WebSphere Application Server
11. Mot de passe de SKLMAdmin
12. Récapitulatif de préinstallation
13. Progression de la migration d'IBM Security Key Lifecycle Manager
14. Récapitulatif de l'installation

Installation en mode silencieux

Une installation en mode silencieux est une installation non interactive pilotée par un fichier de réponses qui fournit les paramètres d'installation.

Lors d'une installation en mode silencieux, l'utilisateur n'a pas besoin d'entrer de données. Ce type d'installation est utile dans des environnements où IBM Security Key Lifecycle Manager doit être installé sur plusieurs systèmes identiques, par exemple dans un centre de données. Pour plus d'informations sur l'installation en mode silencieux d'IBM Security Key Lifecycle Manager, voir «Installation d'IBM Security Key Lifecycle Manager en mode silencieux», à la page 46.

Remarque : L'installation en mode silencieux utilise un fichier de réponses qui contient des informations sur les mots de passe. Pour plus de sécurité, supprimez le fichier de réponses immédiatement après avoir installé IBM Security Key Lifecycle Manager.

IBM Security Key Lifecycle Manager inclut des fichiers de réponses exemples que vous pouvez utiliser comme modèles pour créer vos propres fichiers de réponses. Avant d'utiliser un fichier exemple, vous devez le modifier en fonction des caractéristiques de votre environnement. Les exemples de fichiers de réponses se trouvent dans le répertoire où se trouve votre module d'installation. Pour plus d'informations, voir Exemples de fichier de réponses.

Planification de la migration

Avant d'installer IBM Security Key Lifecycle Manager dans cette version, vérifiez la version d'IBM Security Key Lifecycle Manager précédemment installée sur le système. IBM Security Key Lifecycle Manager prend en charge deux méthodes de migration de données, telles que la migration en ligne et la migration entre plateformes.

Migration en ligne

Lors de l'installation d'IBM Security Key Lifecycle Manager version 3.0.1, vous pouvez migrer des données à partir d'une version précédente d'IBM Security Key Lifecycle Manager, par exemple 2.5, 2.6, 2.7, 3.0 et Encryption Key Manager 2.1.

Migration multiplateforme

Après l'installation d'IBM Security Key Lifecycle Manager version 3.0.1, utilisez l'utilitaire de sauvegarde multiplateforme pour migrer des données provenant des versions antérieures suivantes :

- IBM Security Key Lifecycle Manager, version 2.5, 2.6 et 2.7
- Encryption Key Manager, version 2.1
- IBM Tivoli Key Lifecycle Manager, version 1.0, 2.0 et 2.0.1

  La migration croisée des données d'IBM Tivoli Key Lifecycle Manager versions 1.0, 2.0 et 2.0.1 vers IBM Security Key Lifecycle Manager version 3.0.1 s'effectue en deux étapes qui sont présentées ci-dessous :

  1. Migration des données IBM Tivoli Key Lifecycle Manager, version 1.0, 2.0 et 2.0.1 sur un système où IBM Security Key Lifecycle Manager, Version 2.7 est installé.
  2. Migration des données d'IBM Security Key Lifecycle Manager version 2.7 sur un système où IBM Security Key Lifecycle Manager version 3.0.1 est installé.

Pour plus d'informations, voir Opérations de sauvegarde et de restauration pour les versions précédentes d'IBM Security Key Lifecycle Manager et d'IBM Tivoli Key Lifecycle Manager.

Le tableau suivant répertorie la méthode de migration prise en charge pour les versions antérieures d'IBM Security Key Lifecycle Manager, IBM Tivoli Key Lifecycle Manager et Encryption Key Manager.

Version	Niveau minimal requis	Migration en ligne	Migration multiplateforme
Encryption Key Manager, version 2.1		✓	✓
IBM Tivoli Key Lifecycle Manager, version 1.0	Groupe de correctifs 7		✓
IBM Tivoli Key Lifecycle Manager, version 2.0	Groupe de correctifs 6		✓
IBM Tivoli Key Lifecycle Manager, version 2.0.1	Groupe de correctifs 5		✓

Version	Niveau minimal requis	Migration en ligne	Migration multiplateforme
IBM Security Key Lifecycle Manager version 2.5	Groupe de correctifs 3	✓	✓
IBM Security Key Lifecycle Manager version 2.6	Groupe de correctifs 2	✓	✓
IBM Security Key Lifecycle Manager version 2.7	Version 2.7 General Availability (GA)	✓	✓
IBM Security Key Lifecycle Manager version 3.0	Version 3.0 General Availability (GA)	✓	✓

Si la migration effectuée à partir du programme d'installation échoue, vous pouvez manuellement exécuter l'utilitaire de migration IBM Security Key Lifecycle Manager version 3.0.1 à partir du répertoire *SKLM_HOME*\migration\bin une fois que vous avez quitté l'installation.

- Exécutez **migrate.bat** ou **migrate.sh** pour migrer Encryption Key Manager, version 2.1 vers IBM Security Key Lifecycle Manager. Sur les systèmes Linux ou AIX, veillez à être connecté en tant qu'utilisateur root avant d'exécuter **migrate.sh**.
- Exécutez **migrateToSKLM.bat** ou **migrateToSKLM.sh** dans le répertoire <*SKLM_INSTALL_HOME*>\migration pour migrer une version antérieure d'IBM Security Key Lifecycle Manager vers la version 3.0.1. Sur les systèmes Linux ou AIX, veillez à être connecté en tant qu'utilisateur root avant d'exécuter **migrateToSKLM.sh**.

N'exécutez pas les autres utilitaires ***.bat** présents dans ce répertoire. Ils sont réservés à l'usage du processus d'installation automatique.

Avant la migration

Avant de commencer, vérifiez que votre entreprise autorise un arrêt temporaire de l'activité de service de clés.

Prévoyez également une période de test après la migration. Vous pourrez ainsi vérifier que le nouveau système IBM Security Key Lifecycle Manager contient les clés attendues et tous les attributs de configuration que vous aviez prévu de faire migrer.

Espace disque requis

Avant de migrer des données des versions antérieures vers IBM Security Key Lifecycle Manager version 3.0.1, assurez-vous que l'espace disque sur votre système est suffisant. Ces exigences d'espace disque s'ajoutent à celles du programme d'installation pour IBM Security Key Lifecycle Manager version 3.0.1 et ses logiciels requis.

De l'espace disque supplémentaire est requis pour que le programme de migration déplace les utilisateurs, les clés et les autres métadonnées se trouvant dans la base de données de l'ancien système vers IBM Security Key Lifecycle Manager version 3.0.1.

Conditions et limitations de la migration d'Encryption Key Manager

Vous devez suivre certaines règles et directives pour migrer d'Encryption Key Manager vers IBM Security Key Lifecycle Manager.

- IBM Security Key Lifecycle Manager prend en charge la migration d'Encryption Key Manager, version 2.1 uniquement.
- Copiez le fichier de configuration d'Encryption Key Manager et tous les autres fichiers nécessaires sur un système de destination sur lequel IBM Security Key Lifecycle Manager version 3.0.1 est installé.
- Editez le fichier de configuration d'Encryption Key Manager de manière à indiquer le chemin d'accès absolu et non relatif pour ces paramètres.
- Un serveur Encryption Key Manager ne doit migrer que vers un seul serveur IBM Security Key Lifecycle Manager. Pour migrer un second serveur Encryption Key Manager, utilisez un second serveur IBM Security Key Lifecycle Manager.
- Le serveur Encryption Key Manager et le serveur IBM Security Key Lifecycle Manager qui reçoit les données migrées doivent se trouver sur le même hôte. Après la migration, le serveur IBM Security Key Lifecycle Manager utilise le magasin de clés, le port TCP et le port SSL que le serveur Encryption Key Manager utilisait auparavant.
- Vous devez définir les deux propriétés suivantes :
  - **config.keystore.file**

    Chemin absolu du fichier de clés. Par exemple, `C:/EKM21/test.keys.jceks`.
  - **TransportListener.ssl.keystore.name**

    Nom du fichier de clés SSL d'Encryption Key Manager. Par exemple, `C:/EKM21/test.keys.ssl`.
- Si votre serveur Encryption Key Manager a été configuré avec des groupes de clés pour fonctionner avec des unités de bande LTO, et si vous souhaitez faire migrer ces groupes de clés, vérifiez que la propriété **config.keygroup.xml.file** existe dans le fichier de propriétés de Encryption Key Manager et que sa valeur est un chemin absolu.

  Il est possible que cette propriété ne se trouve pas dans le fichier de propriétés de Encryption Key Manager car ce dernier utilise peut-être le fichier d'un répertoire par défaut à partir duquel il a été démarré.
- Le composant Encryption Key Manager ne prend en charge que l'environnement local anglais. Par conséquent, vous devez effectuer la migration de Encryption Key Manager vers IBM Security Key Lifecycle Manager en environnement local anglais.

Migration d'Encryption Key Manager à partir d'un système IBM i

Vous devez déplacer Encryption Key Manager d'un système IBM i vers un système d'exploitation IBM Security Key Lifecycle Manager pris en charge avant de migrer Encryption Key Manager vers IBM Security Key Lifecycle Manager.

1. Sur un système IBM i, les clés doivent se trouver dans un magasin de clés JCEKS. Dans le cas contraire, vous devez d'abord les transférer dans un magasin JCEKS.
2. Déplacez le magasin de clés JCEKS et le fichier de propriétés Encryption Key Manager, que vous devez mettre à jour pour le nouveau système d'exploitation, du système IBM i vers un système pris en charge par IBM Security Key Lifecycle Manager version 3.0.1.

3. Utilisez le magasin de clés et le fichier de propriétés modifié que vous avez déplacés pour la configuration d'Encryption Key Manager sur le système pris en charge par IBM Security Key Lifecycle Manager version 3.0.1.
4. Assurez-vous que Encryption Key Manager est fonctionnel sur le nouveau système.
5. Effectuez une migration à partir de la nouvelle installation d'Encryption Key Manager vers IBM Security Key Lifecycle Manager version 3.0.1 lors de l'installation d'IBM Security Key Lifecycle Manager version 3.0.1. Pour connaître les étapes d'installation, voir Installation d'IBM Security Key Lifecycle Manager. La migration n'est possible qu'à partir de la version 2.1 de Encryption Key Manager.

Remarque : Pour obtenir Encryption Key Manager version 2.1, contactez le service de support logiciel IBM à l'adresse suivante : http://www.ibm.com/software/support

Restrictions de migration pour Encryption Key Manager

Seule la version 2.1 d'Encryption Key Manager peut être migrée vers IBM Security Key Lifecycle Manager version 3.0.1.

Si vous utilisez des versions antérieures d'Encryption Key Manager, effectuez une mise à niveau vers la version 2.1. Pour obtenir Encryption Key Manager version 2.1, contactez le service de support logiciel IBM à l'adresse suivante : http://www.ibm.com/software/support

Certaines restrictions s'appliquent sur ce vous pouvez migrer depuis Encryption Key Manager .

- La migration des magasins de clés (keystore) et des fichiers de clés certifiées (truststore) SSL de l'administrateur n'est pas prise en charge. Le serveur IBM Security Key Lifecycle Manager ne prévoit pas de capacité de synchronisation des comptes d'administrateur.
- La migration des magasins de clés (keystore) et des fichiers de clés certifiées (truststore) PKCS11Impl n'est pas prise en charge. Le serveur IBM Security Key Lifecycle Manager ne prend pas en charge les magasins de clés PKCS11Impl.
- IBM Security Key Lifecycle Manager ne prend pas en charge l'utilisation d'une clé au sein de plusieurs groupes, contrairement à Encryption Key Manager.

  Lors de la migration des données de clé du fichier `KeyGroup.xml` d'Encryption Key Manager vers IBM Security Key Lifecycle Manager, chaque clé est associée à un seul groupe. Une clé qui, auparavant, était membre de plusieurs groupes dans Encryption Key Manager ne dépend plus que d'un seul groupe dans IBM Security Key Lifecycle Manager.

  Le processus de migration consigne, dans le journal des événements, le fait que la clé n'est pas créée dans plusieurs groupes, puis il poursuit son traitement. Si la propriété **`symmetricKeySet`** spécifie une liste ou une plage de clés, et non pas un groupe, toutes les clés spécifiées par **`symmetricKeySet`** migrent dans un groupe de clés nommé **`DefaultMigrateGroup`**. Si les clés désignées par la propriété **`symmetricKeySet`** sont créées en tant que partie d'autres groupes et que le groupe de clés **`DefaultMigrateGroup`** est vide, IBM Security Key Lifecycle Manager ne crée pas le groupe **`DefaultMigrateGroup`** et ne migre pas la propriété **`symmetricKeySet`**.

  Pour contourner ce problème, utilisez l'interface graphique ou de ligne de commande d'IBM Security Key Lifecycle Manager pour définir un groupe de clés par défaut, par exemple, pour les unités de bande LTO.

Après la migration d'Encryption Key Manager

Après avoir migré Encryption Key Manager, vous devez valider les données de configuration et de protection.

- N'exécutez plus Encryption Key Manager. Après la migration, Encryption Key Manager conserve sa capacité à servir des clés.
- Résolvez les éventuels problèmes de certificats et de clés.

  Dans Encryption Key Manager, un certificat et ses clés peuvent être associés à n'importe quel groupe d'unités. Les certificats et les clés appartenant à plusieurs types d'unité portent la mention `CONFLICTED` (en conflit) après la migration vers IBM Security Key Lifecycle Manager, version 3.0.1. Vous ne pouvez pas les changer de groupe d'unités. IBM Security Key Lifecycle Manager peut utiliser un certificat ou une clé en conflit (`CONFLICTED`) pour les opérations de lecture et d'écriture.

  La migration peut aussi faire apparaître un certificat avec la mention `UNKNOWN` (inconnu) dans l'interface graphique d'IBM Security Key Lifecycle Manager.

  – Les certificats inconnus peuvent servir de certificats de remplacement. Une fois programmé comme remplaçant, le certificat inconnu peut être mis à jour pour être affecté au groupe d'unités spécifique du remplacement. Un certificat de serveur SSL avec une mise à jour `UNKNOWN` est mis à jour pour devenir un certificat SSL.

  – Les certificats en attente peuvent être répertoriés dans l'interface graphique avec un groupe d'unités ayant le statut `UNKNOWN` (inconnu). Acceptez tout d'abord le certificat en attente ayant le statut `UNKNOWN`. Ensuite, utilisez la commande **`tklmCertUpdate`** pour mettre à jour l'utilisation du certificat afin de l'associer à un groupe d'unités spécifique. Cette commande a pour effet de faire passer le certificat à un état tel que 'actif' (active).

  – Au terme de la migration, il est possible qu'une ou plusieurs unités soient associées au groupe d'unités `UNKNOWN` (inconnu). Vous pouvez affecter le groupe des unités inconnues à un nouveau groupe ou choisir de déterminer le groupe d'affectation lorsque les unités émettent leur première demande de clé.

  Utilisez la commande **`tklmCertList`** pour trouver les certificats marqués de la valeur `CONFLICTED` (en conflit) ou `UNKNOWN` (inconnu). Pour le paramètre **`-usage`**, ne spécifiez aucune valeur, ou alors indiquez la valeur 3592, DS8000 ou `SSLSERVER`. Par exemple, la commande suivante, au format Jython, obtient la liste de tous les certificats du groupe d'unités 3592 :

  ```
  print AdminTask.tklmCertList('[-usage 3592 -v y]')
  ```

- Vérifiez que la configuration qui vient de migrer depuis Encryption Key Manager est dans l'état attendu avant d'effectuer des mises à jour ou des modifications dans la configuration d'IBM Security Key Lifecycle Manager.

  Une fois la migration terminée, le magasin de clés de la configuration de Encryption Key Manager devient le magasin de clés d'IBM Security Key Lifecycle Manager. Vous ne pouvez pas faire migrer les données du serveur Encryption Key Manager une deuxième fois vers le même serveur IBM Security Key Lifecycle Manager.

  En cas d'échec de la migration, si vous choisissez de terminer le processus d'installation d'IBM Security Key Lifecycle Manager, vous pouvez utiliser un script autonome de reprise de la migration, mais à condition que vous n'ayez pas encore effectué de mise à jour ni apporté de modifications dans la configuration d'IBM Security Key Lifecycle Manager. Pour plus d'informations, voir «Récupération après un échec de migration», à la page 87.

Objets de données et propriétés migrant depuis Encryption Key Manager

Les objets de données et les propriétés sont également migrées depuis Encryption Key Manager.

Les propriétés qui doivent être dans le fichier de configuration de Encryption Key Manager sont les suivantes :

- **Audit.metadata.file.name**

  Le fichier désigné doit se trouver dans le même répertoire que le fichier de configuration lui-même et doit être accessible en lecture.
- **config.drivetable.file.url**

  Le fichier désigné doit se trouver dans le même répertoire que le fichier de configuration lui-même et doit être accessible en lecture.
- **config.keystore.file**

  Le fichier désigné doit se trouver dans le même répertoire que le fichier de configuration lui-même et doit être accessible en lecture et en écriture.
- **config.keystore.password.obfuscated**
- **config.keystore.type**

  Le type de magasin de clés ne doit pas être PKCS11IMPLKS.
- **TransportListener.ssl.keystore.name**

  Le fichier désigné doit se trouver dans le même répertoire que le fichier de configuration lui-même et doit être accessible en lecture.
- **TransportListener.ssl.keystore.password.obfuscated**
- **TransportListener.ssl.keystore.type**

  Le type de magasin de clés ne doit pas être PKCS11IMPLKS.
- **TransportListener.ssl.port**

  La valeur doit être un entier positif compris entre 1 et 65535, et ne doit pas être identique à celle de la propriété **TransportListener.tcp.port**.
- **TransportListener.ssl.truststore.type**

  Le fichier de clés certifiées ne doit pas être PKCS11IMPLKS.
- **TransportListener.tcp.port**

  La valeur doit être un entier positif compris entre 1 et 65535, et ne doit pas être identique à celle de la propriété **TransportListener.ssl.port**.

La migration inclut les objets de données suivants :

Magasins de clés

IBM Security Key Lifecycle Manager stocke l'ensemble des clés et des certificats dans la base de données. Lors de la migration, les clés et les certificats des deux magasins de clés du gestionnaire de clés de chiffrement de clés, Config et TransportListner, sont tous copiés dans la base de données d'IBM Security Key Lifecycle Manager. Les clés et les certificats sont copiés à partir du magasin de clés Config. Les certificats sont copiés à partir du fichier de clés certifiées TransportListner.

Un certificat provenant du magasin de clés TransportListener est désigné comme certificat SSL pour IBM Security Key Lifecycle Manager. La propriété **config.keystore.ssl.certalias** est mise à jour avec l'alias de ce certificat.

Les autres magasins de clés Encryption Key Manager ne sont pas utilisées.

Unités Toutes les informations se rapportant aux unités sont lues dans la table d'unités désignée par la propriété config.drivetable.file.url et sont entrées dans la base de données d'IBM Security Key Lifecycle Manager. Si la propriété symalias de l'unité est définie, le type d'unité a la valeur LTO. De plus, si des alias sont définis pour l'unité, le type d'unité a la valeur 3592. Le processus de migration attribue le type UNKNOWN (inconnu) à toute unité pour laquelle aucune de ces propriétés n'est définie et dont le type ne peut pas être déterminé.

Groupes de clés
Le fichier `keygroup.xml` désigné par la propriété **`config.keygroup.xml.file`** est analysé. Les informations de groupe de clés sont stockées dans une base de données IBM Security Key Lifecycle Manager. Tous les membres et les relations de groupes migrent également.

Si la propriété **`symmetricKeySet`** a une liste ou une série d'alias, un groupe de clés par défaut nommé `DefaultMigrationGroup` est créé et tous les alias sont désignés comme membres du groupe. Dans ce cas, la propriété **`symmetricKeySet`** a la valeur `DefaultMigrationGroup`. Si la propriété **`symmetricKeySet`** est déjà un alias de groupe, le groupe de migration par défaut n'est pas créé.

Métadonnées
Toutes les informations de métadonnées désignées par la propriété **`Audit.metadata.file.name`** sont migrées dans une base de données IBM Security Key Lifecycle Manager.

Les propriétés migrées depuis le fichier de configuration d'Encryption Key Manager vers le fichier SKLMConfig.properties peuvent inclure :

- **`Audit.eventQueue.max`**
- **`Audit.handler.file.size`**
- **`Audit.event.outcome`**
- **`Audit.event.types`**
- **`config.keystore.name`** (ayant la valeur `defaultKeyStore`)
- **`cert.valiDATE`**
- **`drive.acceptUnknownDrives`** est migré vers la base de données comme entrée par défaut dans le groupe d'unités indiqué.
- **`fips`**
- **`TransportListener.ssl.ciphersuites`**
- **`TransportListener.ssl.clientauthentication`**
- **`TransportListener.ssl.port`**
- **`TransportListener.ssl.protocols`**
- **`TransportListener.ssl.timeout`**
- **`TransportListener.tcp.port`**
- **`TransportListener.tcp.timeout`**
- **`useSKIDefaultLabels`**
- **`zOSCompatibility`**

Les propriétés suivantes **sont** migrées du fichier de configuration de Encryption Key Manager vers la base de données d'IBM Security Key Lifecycle Manager :

- **`drive.default.alias1`**
- **`drive.default.alias2`**

- **symmetricKeySet** (définie avec un alias de groupe déjà spécifié ; sinon, définie à **DefaultMigrationGroup**)

Restrictions et conditions requises pour la migration à partir d'une version antérieure d'IBM Security Key Lifecycle Manager

Avant de migrer votre ancienne version d'IBM Security Key Lifecycle Manager, par exemple la version 2.5, 2.6, 2.7 ou 3.0, vers la version 3.0.1, vous devez suivre certaines règles et directives.

- Vérifiez que le groupe de correctifs minimal requis est appliqué pour la version d'IBM Security Key Lifecycle Manager que vous migrez. Pour plus d'informations sur le niveau de groupe de correctifs requis minimal, voir Planification de la migration.
- Sauvegardez la version antérieure d'IBM Security Key Lifecycle Manager. Faites également une sauvegarde des serveurs secondaires. Si la migration échoue, restaurez IBM Security Key Lifecycle Manager à partir de la copie de sauvegarde.

  Remarque : Une fois la migration d'IBM Security Key Lifecycle Manager terminée, les fichiers de sauvegarde de la version précédente qui sont créés à l'aide de la commande de l'interface CLI, de l'interface graphique ou de l'interface REST ne peuvent pas être utilisés pour restaurer IBM Security Key Lifecycle Manager au niveau de la version 3.0.1.

  Vous pouvez utiliser l'utilitaire de sauvegarde d'IBM Security Key Lifecycle Manager version 3.0.1 pour créer les fichiers de sauvegarde multiplateformes compatibles pour les versions antérieures. Vous pouvez ensuite restaurer ces fichiers de sauvegarde à partir des versions antérieures sur un système IBM Security Key Lifecycle Manager version 3.0.1.
- La migration ne supprime pas la version antérieure d'IBM Security Key Lifecycle Manager. Pour la supprimer, suivez les instructions de désinstallation pour la version d'IBM Security Key Lifecycle Manager depuis laquelle vous avez migré.

  Remarque : Etant donné que les ports IP sont partagés entre les deux versions, n'exécutez pas les deux versions en même temps.
- Arrêtez IBM Security Key Lifecycle Manager et tout serveur secondaire (réplique). Le service de clés ne peut pas être actif durant la migration.
- Lors de la migration, examinez régulièrement le fichier *REP_DONNEES_IM*/logs/sklmLogs/migration.log pour déterminer la progression de la migration. Si la migration échoue, exécutez l'utilitaire de migration pour écrire des messages dans le fichier migration.log et les afficher dans l'interface de ligne de commande.
- Pour éviter toute erreur pendant le déroulement de la migration, vous ne devez pas démarrer ni arrêter le serveur Db2 ou le WebSphere Application Server en dehors du cadre normal du processus de migration. N'interrompez pas le processus de migration.
- Lorsque vous migrez IBM Security Key Lifecycle Manager en mode silencieux, vérifiez que le mot de passe administrateur correct est indiqué dans le fichier de réponses.
- Lorsqu'une version antérieure du système IBM Security Key Lifecycle Manager avec LDAP configuré est migrée vers la version 3.0.1, tous les utilisateurs LDAP du système de version antérieure ne sont pas migrés. Seul l'utilisateur LDAP qui est utilisé pour le rôle d'administrateur d'IBM Security Key Lifecycle Manager

pendant le processus d'installation est migré. Vous devez ajouter explicitement tous les autres utilisateurs LDAP après l'installation. Pour ajouter les utilisateurs, exécutez le script de configuration LDAP **addLDAPUserToGroup** comme décrit à l'**étape 3** de la rubrique Exécution des scripts de configuration LDAP.

Migration à partir de systèmes d'exploitation non pris en charge

Utilisez l'utilitaire de sauvegarde multiplateforme pour migrer les données d'IBM Security Key Lifecycle Manager, d'IBM Tivoli Key Lifecycle Manager et d'Encryption Key Manager exécutées sur les systèmes d'exploitation que la version 3.0.1 ne prend pas en charge.

Vous pouvez ensuite restaurer les fichiers de sauvegarde d'IBM Security Key Lifecycle Manager version 3.0.1 sur un système d'exploitation différent de celui sur lequel ils ont été créés. Pour plus d'informations, voir Opérations de sauvegarde et de restauration pour les versions précédentes d'IBM Security Key Lifecycle Manager et d'IBM Tivoli Key Lifecycle Manager.

Après la migration d'IBM Security Key Lifecycle Manager

Après avoir migré IBM Security Key Lifecycle Manager, vous devez valider la configuration et protéger les données.

- Immédiatement après l'installation d'IBM Security Key Lifecycle Manager version 3.0.1, exécutez l'opération de sauvegarde pour IBM Security Key Lifecycle Manager version 3.0.1.

  La migration vers la version 3.0.1 ne retire pas la version antérieure d'IBM Security Key Lifecycle Manager. Vous ne devez pas exécuter les deux versions simultanément pour éviter les conflits de port.

  En cas d'échec de la migration, si vous choisissez de terminer le processus d'installation d'IBM Security Key Lifecycle Manager, vous pouvez utiliser un script autonome de reprise de la migration, mais à condition que vous n'ayez pas encore effectué de mise à jour ni apporté de modifications dans la configuration d'IBM Security Key Lifecycle Manager. Pour plus d'informations, voir «Récupération après un échec de migration», à la page 87. Vous devez effectuer le processus de reprise de la migration avant de pouvoir utiliser IBM Security Key Lifecycle Manager version 3.0.1.
- Conservez une réplique de la version précédente d'IBM Security Key Lifecycle Manager, mais ne l'exécutez pas. Le maintien de la réplique de la version précédente garantit que vous disposez d'un environnement et de données dans le cas où la validation détermine qu'il existe un problème lié à la version 3.0.1.
- Résolvez les éventuels problèmes de certificats et de clés.

  Dans les versions antérieures 2.5, 2.6, 2.7 et 3.0 d'IBM Security Key Lifecycle Manager, un certificat et ses clés peuvent être associés à n'importe quel groupe d'unités. Les certificats et les clés qui appartiennent à plusieurs types d'unité dans les versions antérieures d'IBM Security Key Lifecycle Manager portent la mention `CONFLICTED` dans la version 3.0.1. Vous ne pouvez pas les changer de groupe d'unités. IBM Security Key Lifecycle Manager peut utiliser un certificat ou une clé en conflit (`CONFLICTED`) pour les opérations de lecture et d'écriture.
- Au terme de la migration, il est possible qu'une ou plusieurs unités soient associées au groupe d'unités `UNKNOWN` (inconnu). Vous pouvez affecter le groupe des unités inconnues à un nouveau groupe ou choisir de déterminer le groupe d'affectation lorsque les unités émettent leur première demande de clé.
- Une fois la migration de la version antérieure d'IBM Security Key Lifecycle Manager vers la version 3.0.1 effectuée, le programme de migration ne supprime

pas la version précédente. Pour la supprimer, suivez les instructions de désinstallation pour la version du produit depuis laquelle vous avez migré.

Remarque : Etant donné que les ports IP sont partagés entre les deux versions, n'exécutez pas les deux versions en même temps. Si ces étapes ne peuvent pas être réalisées dans leur intégralité, le processus de migration le signale dans un message d'avertissement qui conclut quand même à la réussite de l'opération. Recherchez des messages dans le fichier *<REP_DONNEES_IM>*/logs/sklmLogs/migration.log et effectuez les actions manuelles appropriées.

- Dans la version antérieure d'IBM Security Key Lifecycle Manager, un certificat peut avoir été marqué comme futur remplaçant pour l'administration d'unités 3592 ; de même, un groupe de clés peut avoir été marqué comme futur remplaçant pour l'administration d'unités LTO. Si la date prévue pour l'entrée en vigueur de remplaçants est antérieure à la date de la migration, cette dernière ajoute un message approprié au journal et ne fait pas migrer les entrées correspondantes. Une fois l'installation d'IBM Security Key Lifecycle Manager version 3.0.1 terminée, utilisez l'interface de ligne de commande ou l'interface graphique pour ajouter manuellement ces entrées de remplacement.
- Vous ne pouvez pas utiliser l'interface graphique pour supprimer une tâche de remplacement migrée que vous avez ajoutée via l'interface de ligne de commande (avec la commande **tklmCertDefaultRolloverAdd** ou **tklmKeyGroupDefaultRolloverAdd**). Utilisez l'interface de ligne de commande pour supprimer une tâche de remplacement migrée qui a été créée à l'aide de cette même interface.
- Après vous être assuré qu'IBM Security Key Lifecycle Manager version 3.0.1 est configuré et s'exécute correctement, sauvegardez le serveur IBM Security Key Lifecycle Manager version 3.0.1 et installez la sauvegarde sur un ordinateur réplique.
  - Assurez-vous que l'ordinateur réplique de la version 3.0.1 est configuré et s'exécute correctement.
  - Conservez une copie des fichiers de sauvegarde version 3.0.1 dans un emplacement différent du chemin du répertoire d'IBM Security Key Lifecycle Manager version 3.0.1. Vous êtes ainsi certain que les fichiers de sauvegarde ne pourront pas être supprimés par d'autres processus en cas de désinstallation de IBM Security Key Lifecycle Manager.

    Conservez également les fichiers *<REP_DONNEES_IM>*/logs/sklmLogs/migration.log afin de pouvoir vous y référer ultérieurement.

Pour la définition de *<REP_DONNEES_IM>*, voir «Définitions relatives à un répertoire *HOME* et d'autres variables de répertoire», à la page 5.

Objets de données et propriétés migrant depuis IBM Security Key Lifecycle Manager

Les objets de données et les propriétés sont également migrés à partir de versions antérieures d'IBM Security Key Lifecycle Manager telles que 2.5, 2.6, 2.7 et 3.0.

Magasin de clés
Le magasin de clés, y compris tous les certificats et toutes les métadonnées des versions antérieures, est ajouté à la base de données IBM Security Key Lifecycle Manager, Version 3.0.1. Le magasin de clés est identifié par la propriété **config.keystore.name** dans le fichier SKLMConfig.properties.

Unités Toutes les informations se rapportant aux unités sont lues dans la base de données de IBM Security Key Lifecycle Manager.

Groupes de clés

Les informations se rapportant aux groupes de clés sont lues dans la base de données de IBM Security Key Lifecycle Manager.

Certificats et groupes de clés de remplacement

Des certificats et des groupes de clés des versions antérieures peuvent être marqués pour l'administration future des lecteurs de bande d'3592. Le programme de migration détecte et marque ces remplacements pour l'administration future avec IBM Security Key Lifecycle Manager version 3.0.1.

Métadonnées

Toutes les informations de métadonnées sont migrées à partir d'une base de données de version antérieure et peuvent être utilisées par la base de données IBM Security Key Lifecycle Manager version 3.0.1.

Propriétés

Les propriétés dans le fichier SKLMConfig.properties migrent dans la base de données de IBM Security Key Lifecycle Manager. Le fichier `datastore.properties` est migré.

Ces propriétés sont remplacées dans le fichier 3.0.1 SKLMConfig.properties :

- **`ds8k.acceptUnknownDrives`**

  La propriété **`device.AutoPendingAutoDiscovery`** remplace cette propriété.

- **`drive.acceptUnknownDrives`**

  Cette propriété est remplacée par l'attribut **`device.AutoPendingAutoDiscovery`** dans la base de données IBM Security Key Lifecycle Manager.

Ces propriétés sont migrées du fichier SKLMConfig.properties version 3.0.1 vers la base de données IBM Security Key Lifecycle Manager :

- **`drive.default.alias1`**
- **`drive.default.alias2`**
- **`symmetricKeySet`** (supprimé du fichier SKLMConfig.properties et remplacé par une entrée pour le groupe d'unités dans la base de données d'IBM Security Key Lifecycle Manager)

Feuilles de travail de préinstallation

Avant d'effectuer l'installation et la configuration d'IBM Security Key Lifecycle Manager, vous pouvez compléter les feuilles de travail de préinstallation pour définir les paramètres de configuration requis pour effectuer l'installation d'IBM Security Key Lifecycle Manager.

Les feuilles de travail de préinstallation répertorient toutes les valeurs que vous devez spécifier au cours d'un processus d'installation d'IBM Security Key Lifecycle Manager. Remplir les feuilles de travail de préinstallation avant d'installer les composants peut vous aider à planifier votre installation, gagner du temps, et respecter la cohérence au cours du processus d'installation et de configuration.

Paramètres d'installation générale

Utilisez cette feuille de travail pour répertorier les paramètres de l'installation générale.

Tableau 8. Paramètres d'installation générale

Option	Description	Valeur par défaut ou d'exemple	Votre valeur
Mode d'installation	Mode d'exécution du programme d'installation.	`Interface (par défaut)` `silent`	
Etape importante : Vérifiez l'espace disque disponible.	Assurez-vous de disposer de suffisamment d'espace disque disponible	Pour connaître les valeurs possibles, voir «Configuration matérielle requise», à la page 7.	
Répertoire d'installation - IBM Installation Manager	Répertoire dans lequel IBM Installation Manager doit être installé.	**Windows** *drive*`:\Program Files\IBM\Installation Manager\eclipse` **AIX et Linux** `/opt/ibm/InstallationManager/eclipse`	
Répertoire d'installation - IBM DB2	Répertoire dans lequel IBM DB2 doit être installé.	**Windows** *drive*`:\Program Files\IBM\DB2SKLMV301` **AIX et Linux** `/opt/ibm/DB2SKLMV301`	

Tableau 8. Paramètres d'installation générale (suite)

Option	Description	Valeur par défaut ou d'exemple	Votre valeur
Répertoire d'installation - IBM WebSphere Application Server	Répertoire dans lequel WebSphere Application Server doit être installé.	**Windows** *drive*:\Program Files\IBM\WebSphere\AppServer **AIX et Linux** /opt/IBM/WebSphere/AppServer	
Répertoire d'installation - IBM Security Key Lifecycle Manager	Répertoire dans lequel IBM Security Key Lifecycle Manager doit être installé.	**Windows** *drive*:\Program Files\IBM\SKLMV301 **AIX et Linux** /opt/ibm/SKLMV301	

Paramètres de configuration de Db2

Utilisez cette feuille de travail pour répertorier les entrées relatives à l'installation et à la configuration de Db2.

Tableau 9. Paramètres de configuration de Db2

Nom de la zone	Description	Valeur par défaut ou d'exemple	Votre valeur
Répertoire d'installation de Db2	Répertoire dans lequel Db2 doit être installé.	**Windows** *drive*:\Program Files\IBM\DB2SKLMV301 **AIX et Linux** /opt/IBM/DB2SKLMV301	
Installer DB2 ou utiliser une installation existante de DB2	Indiquez si vous souhaitez utiliser une instance DB2 existante ou une nouvelle installation de DB2.	Si une instance DB2 existante est utilisée, vous devez spécifier l'emplacement d'installation de DB2 ainsi que d'autres détails.	
ID administrateur Db2	ID utilisateur de l'administrateur de la base de données d'IBM Security Key Lifecycle Manager (également appelé propriétaire de l'instance).	SKLMDB31	

Tableau 9. Paramètres de configuration de Db2 (suite)

Nom de la zone	Description	Valeur par défaut ou d'exemple	Votre valeur
Mot de passe administrateur Db2	Mot de passe de l'ID utilisateur de l'administrateur de la base de données.		
Nom de la base de données	Nom de la base de données IBM Security Key Lifecycle Manager.	`SKLMDB31`	
Port Db2	Port d'écoute du service Db2.	50050	

Répertoire de base de l'administrateur/ de la base de données	Répertoire dans lequel l'instance de base de données ainsi que les tables formatées sont créées.	**Windows**
		`C:`
		Linux et AIX
		`/home/sklmdb301`	

Groupe administrateur	Groupe d'utilisateurs du système d'exploitation dont est membre le propriétaire de l'instance de la base de données sur les systèmes Linux ou AIX.	Si Db2 est sur un système AIX ou Linux, votre ID utilisateur doit être dans le groupe bin ou root ou dans un groupe à part, dont root est membre.	

Paramètres de configuration de WebSphere Application Server et du serveur IBM Security Key Lifecycle Manager

Utilisez la feuille de travail de configuration pour enregistrer vos entrées pour l'installation et la configuration du serveur d'applications, qui est utilisé pour héberger votre serveur IBM Security Key Lifecycle Manager.

Tableau 10. Paramètres de configuration de WebSphere Application Server

Nom de la zone	Description	Valeur par défaut ou d'exemple	Votre valeur
Nom d'utilisateur	Indiquez l'ID utilisateur de connexion à WebSphere Application Server utilisé pour le profil d'administration de IBM Security Key Lifecycle Manager.	`wasadmin`	

Tableau 10. Paramètres de configuration de WebSphere Application Server (suite)

Nom de la zone	Description	Valeur par défaut ou d'exemple	Votre valeur
Mot de passe	Indiquez le mot de passe de l'ID de connexion à WebSphere Application Server utilisé pour le profil IBM Security Key Lifecycle Manager.		
Port d'administration HTTPS	Indiquez le port de connexion à WebSphere Application Server utilisé pour le profil IBM Security Key Lifecycle Manager.	`9083`	

Tableau 11. Paramètres de configuration de IBM Security Key Lifecycle Manager

Nom de la zone	Description	Valeur par défaut ou d'exemple	Votre valeur
Nom d'utilisateur	Spécifiez l'ID utilisateur pour administrer IBM Security Key Lifecycle Manager.	`SKLMAdmin`	
Mot de passe	Indiquez le mot de passe de l'administrateur IBM Security Key Lifecycle Manager.		
Numéro de port HTTPS	Indiquez le port sécurisé pour accéder à IBM Security Key Lifecycle Manager.	`443`	
Numéro de port HTTP	Indiquez le port non sécurisé pour accéder à IBM Security Key Lifecycle Manager.	`80`	

Installation et migration d'IBM Security Key Lifecycle Manager

Le programme d'installation IBM Security Key Lifecycle Manager peut fonctionner en deux modes, tels que le mode graphique et le mode silencieux. Sélectionnez le mode qui vous convient lorsque vous installez ou migrez IBM Security Key Lifecycle Manager.

Instructions d'installation

Pour une installation réussie, assurez-vous que vous comprenez et respectez les instructions et les recommandations pour installer IBM Security Key Lifecycle Manager.

- L'installation peut prendre plus d'une heure.
- N'effectuez pas l'installation à partir d'une unité réseau ni d'une unité montée.
- Veillez à sélectionner la langue correcte en réponse aux invites qui s'affichent durant l'installation. La correction d'une erreur de sélection de l'environnement local vous oblige à désinstaller puis à réinstaller IBM Security Key Lifecycle Manager et Db2.
- Lorsque vous installez IBM Security Key Lifecycle Manager, le mot de passe DB2 que vous spécifiez doit être conforme aux règles sur les mots de passe du système d'exploitation sous-jacent.
- Si vous utilisez un utilisateur existant en tant qu'administrateur DB2, vérifiez que le mot de passe est correctement spécifié.
- Lorsque vous installez IBM Security Key Lifecycle Manager sur Linux, certains changements apportés à la configuration d'Db2 lors de l'installation peuvent nécessiter un redémarrage du système. Fermez toutes les autres applications avant de redémarrer le système. Une fois le système redémarré, exécutez de nouveau le programme d'installation.
- Vérifiez que le nom d'hôte du système a été correctement défini.
- Pour tous les champs, les données entrées doivent se limiter aux caractères alphabétiques (A-Z et a-z), aux chiffres de 0 à 9 et au caractère de soulignement (_). La restriction s'applique également aux valeurs spécifiées dans le fichier de réponses utilisé pour les installations en mode silencieux.
- Vérifiez que le chemin d'installation ne contient pas de caractères Unicode.
- Vérifiez que le chemin d'installation ne contient pas de caractères non-ASCII.
- Lorsque vous installez IBM Security Key Lifecycle Manager, conservez le chemin par défaut pour **Répertoire des ressources partagées** (Shared Resources Directory). IBM Installation Manager utilise cet emplacement pour télécharger des artefacts et pour stocker des informations sur les modules installés.
- N'installez pas IBM Security Key Lifecycle Manager sur des systèmes dotés d'un système d'exploitation renforcé.

  Dans un système renforcé, vous pouvez avoir un accès restreint à des répertoires spécifiques ou vous pouvez ne pas faire partie du groupe d'administrateurs. Sous Windows, il est possible que vous n'ayez pas accès à certains répertoires du système même si vous faites partie du groupe d'administrateurs. Pour installer IBM Security Key Lifecycle Manager, vous devez avoir accès à tous les répertoires d'installation avec les autorisations de lecture, d'écriture et d'exécution.

- Vérifiez que l'interpréteur de commandes Bash est installé avant d'installer IBM Security Key Lifecycle Manager sur les systèmes d'exploitation UNIX.
- Si vous avez une version antérieure d'IBM Security Key Lifecycle Manager dans votre environnement, prenez en compte les instructions suivantes avant l'installation et la migration vers la version 3.0.1 :
  - Procurez-vous les mots de passe d'administration pour votre version antérieure d'IBM Security Key Lifecycle Manager.
  - Appliquez le groupe de correctifs le plus récent à votre version antérieure d'IBM Security Key Lifecycle Manager.
  - Sur les systèmes Windows, assurez-vous que le service IBM ADE est démarré.

    Sur un système Windows, ouvrez la console Services. Vérifiez que le service IBM ADE est démarré. S'il n'est pas démarré, sélectionnez-le et démarrez-le.

Images d'installation et groupes de correctifs

Procurez-vous les fichiers d'installation d'IBM Security Key Lifecycle Manager sur le site Web IBM Passport Advantage et les groupes de correctifs depuis Fix Central. Vous pouvez également obtenir les fichiers par d'autres moyens, par exemple sur un DVD fourni par votre ingénieur commercial IBM.

Le site Web Passport Advantage inclut des modules (appelés eAssemblies) pour différents produits IBM sur la page http://www-01.ibm.com/software/passportadvantage/pao_customer.html.

Vous pouvez utiliser Fix Central pour rechercher les correctifs fournis par le support IBM pour divers produits, y compris IBM Security Key Lifecycle Manager, sur la page https://www-945.ibm.com/support/fixcentral. Fix Central permet de rechercher, sélectionner, commander et télécharger des correctifs pour votre système et de choisir parmi différentes options de distribution. Un correctif de produit IBM Security Key Lifecycle Manager peut être disponible pour résoudre votre problème.

Installation d'IBM Security Key Lifecycle Manager en mode graphique

Utilisez l'assistant d'installation d'IBM Installation Manager pour installer IBM Security Key Lifecycle Manager et ses composants en mode d'interface utilisateur graphique.

Avant de commencer

- Téléchargez et extrayez les fichiers pour IBM Security Key Lifecycle Manager dans un répertoire. Ces fichiers peuvent être téléchargés depuis le site Web IBM Passport Advantage. Voir la rubrique Images d'installation et groupes de correctifs pour plus de détails.
- Consultez la rubrique Instructions d'installation pour connaître les considérations et les restrictions relatives à l'installation et la configuration d'IBM Security Key Lifecycle Manager.
- Consultez la rubrique Planification de l'installation pour comprendre les exigences.

Pourquoi et quand exécuter cette tâche

Lorsque vous démarrez le processus d'installation du programme Tableau de bord, IBM Installation Manager est automatiquement installé se il ne est pas déjà sur votre système. Lorsque la tâche d'installation est terminée, IBM Security Key

Lifecycle Manager est installé avec l'installation des composants middleware nécessaires, tels que WebSphere Application Server et DB2 sur le même système.

Procédure

1. Accédez au répertoire de votre package d'installation et ouvrez `disk1`. Par exemple : *chemin de téléchargement*`/disk1`
2. Démarrez le programme d'installation.

Système d'exploitation	Commande à exécuter
Windows	`launchpad.bat`
Linux ou AIX	`launchpad.sh`

3. Sélectionnez l'environnement local à utiliser pour le processus d'installation. L'environnement local détermine la langue utilisée par le programme d'installation. Entrez le numéro s'affichant en regard de votre environnement local puis appuyez sur Entrée. L'assistant Installation Manager s'affiche.
4. Dans la fenêtre Installer des packages, cliquez sur les packages du produit pour les mettre en évidence. La description du package est affichée dans la section **Détails** au bas de la fenêtre. Veillez à lire toutes les informations relatives au package avant de l'installer.
5. Sélectionnez les packages de produit à installer. Tous les paquets sont sélectionnés pour l'installation par défaut.
6. Cliquez sur **Suivant**. Les contrôles prérequis vérifient les conditions préalables d'installation suivantes :
7. Sélectionnez **I accept the terms in the license agreements** et cliquez sur **Next**.
8. Sélectionnez un emplacement pour le répertoire de ressources partagées et cliquez sur **Next**.

   Remarque : Conservez le chemin par défaut pour le répertoire des ressources partagées, par exemple, `C:\Program Files\IBM\IBMIMShared`. IBM Installation Manager utilise cet emplacement pour télécharger des artefacts et pour stocker des informations sur les modules installés.
9. La page Emplacement affiche l'emplacement du groupe de packages dans lequel chaque produit sera installé. Cliquez sur un produit pour voir l'emplacement de son groupe de packages. Cliquez sur **Suivant**.
10. Sur la page suivante, sélectionnez les des packages de traduction à installer et cliquez sur **Suivant**.
11. Sur la page Features, sélectionnez les fonctions de package que vous souhaitez installer.
    a. Pour afficher les relations de dépendance entre les fonctions, sélectionnez **Show dependencies**.
    b. Cliquez sur une fonction pour en afficher une brève description dans la section **Détails**.
    c. Après avoir sélectionné les fonctions, cliquez sur **Suivant**.
12. Sur la page Configuration for IBM DB2, spécifiez les informations de configuration de base de données et cliquez sur **Next**.

    Pour plus de détails sur la configuration de DB2, reportez-vous à Paramètres de configuration DB2 et Configuration de DB2 pendant l'installation.
13. Sur la page Configuration d'IBM Security Key Lifecycle Manager, spécifiez les informations de configuration pour IBM Security Key Lifecycle Manager et WebSphere Application Server. Cliquez ensuite sur **Next** (Suivant).

Pour plus de détails sur la configuration, voir Paramètres de configuration de WebSphere Application Server et du serveur IBM Security Key Lifecycle Manager et Configuration pendant l'installation.

14. Sur la page suivante, pour faire migrer une configuration existante Encryption Key Manager, sélectionnez **Faire migrer Encryption Key Manager** et spécifier l'emplacement du fichier de propriétés. Cliquez ensuite sur **Next** (Suivant).

    Pour plus d'informations et de directives concernant la configuration d'Encryption Key Manager, voir Migration de la configuration d'Encryption Key Manager.

15. Sur la page Summary, passez en revue vos choix avant de lancer l'installation du package. Pour modifier une sélection, cliquez sur **Précédent** pour revenir à vos sélections antérieures.
16. Pour commencer l'installation, cliquez sur **Install**.

    Un indicateur de progression affiche le pourcentage effectué de l'installation. Lorsque l'installation est terminée, un message vous en informe.

17. Cliquez sur **View Log File** pour ouvrir le fichier journal d'installation et vérifier que tous les composants ont été installés correctement.
18. Dans l'assistant d'installation de packages, sélectionnez **None** pour indiquer au programme d'installation de ne pas créer de profil.
19. Cliquez sur **Finish** pour compléter la tâche d'installation et fermer l'assistant.

Que faire ensuite

Avant d'utiliser IBM Security Key Lifecycle Manager, exécutez les tâches de post-installation décrites dans Etapes de post-installation.

Installation d'IBM Security Key Lifecycle Manager en mode silencieux

Vous pouvez installer IBM Security Key Lifecycle Manager en mode silencieux. Cette méthode d'installation est utile si vous voulez des configurations d'installation identiques sur plusieurs postes de travail. L'installation en mode silencieux requiert un fichier de réponses qui définit la configuration d'installation.

Avant de commencer

- Téléchargez et extrayez les fichiers pour IBM Security Key Lifecycle Manager dans un répertoire. Ces fichiers peuvent être téléchargés depuis le site Web IBM Passport Advantage. Voir la rubrique Images d'installation et groupes de correctifs pour plus de détails.
- Consultez la rubrique Instructions d'installation pour connaître les considérations et les restrictions relatives à l'installation et la configuration d'IBM Security Key Lifecycle Manager.
- Consultez la rubrique Planification de l'installation pour comprendre les exigences.
- IBM Security Key Lifecycle Manager inclut des fichiers de réponses exemples que vous pouvez utiliser comme modèles pour créer vos propres fichiers de réponses. Les exemples de fichiers de réponses se trouvent dans le répertoire où se trouve votre module d'installation. Avant d'utiliser un fichier exemple, vous devez le modifier en fonction des caractéristiques de votre environnement.

Pourquoi et quand exécuter cette tâche

Avant l'installation, vous devez également lire et accepter les dispositions du contrat de licence de ce produit. Vous trouverez les fichiers de réponse exemples,

ainsi que les fichiers des contrats de licence, dans le répertoire racine des images d'installation. Le sous-répertoire `/license` contient les fichiers de licence au format texte.

L'installation échoue sauf si vous effectuez ces étapes.

Dans le fichier de réponses, modifiez comme suit la ligne qui spécifie la licence :

- Mettez la valeur à `true` pour indiquer que vous acceptez les dispositions du contrat de licence.
- Supprimez la mise en commentaire de la ligne en ôtant le signe # au début de la ligne.

Procédure

1. Editez les informations d'emplacement du référentiel et d'autres détails dans le fichier de réponses. Les exemples de fichiers de réponses se trouvent dans le répertoire où se trouve votre module d'installation.

   Remarque : Si vous entrez une valeur non valide pour le paramètre **`chemin_complet_fichier_réponses`**, par exemple un chemin incomplet, le programme d'installation se ferme. Aucun message d'erreur ne s'affiche ou n'est consigné.

   Vous devez mettre à jour le fichier de réponses avec l'emplacement correct du référentiel. L'emplacement du référentiel est l'endroit où se trouve le package d'installation.

   ```
   <repository location='<emplacement de référentiel utilisateur>\im'/>
   <repository location='<emplacement de référentiel utilisateur>\'/>
   ```

   Si vous avez extrait le package d'installation dans `C:\sklm301`, mettez à jour l'emplacement du référentiel dans le fichier de réponses `SKLM_install_Win_Resp.xml` comme indiqué dans l'exemple ci-dessous.

   ```
   <repository location='<C:\sklm301\disk1\im'>\im'/>
   <repository location='<C:\sklm301\disk1\'/>
   ```

2. Pour ajouter les mots de passe chiffrés aux éléments pertinents du fichier de réponses, utilisez le programme IBM Installation Manager pour créer des mots de passe chiffrés.

   Pour plus d'informations sur la façon de chiffrer le mot de passe, consultez Mot de passe chiffré pour les éléments du fichier de réponses.

3. Ouvrez une invite de commande et exécutez la commande d'installation en mode silencieux.

   Windows
   Accédez au *<répertoire de package d'installation>*`\disk1` et exécutez la commande suivante.

   `silent_install.bat SKLM_Silent_Win_Resp.xml`

   Linux Accédez au *<répertoire de package d'installation>*`//disk1` et exécutez la commande suivante.

   `silent_install.sh SKLM_Silent_Linux_Resp.xml`

4. Vérifiez que l'installation a abouti en examinant les fichiers journaux. Vous pouvez afficher les journaux d'IBM Installation Manager dans les emplacements suivants.

   Windows
   `unité:\`*`<REP_DONNEES_IM>`*`\logs\native`.

   Par exemple, `C:\ProgramData\IBM\Installation Manager\logs\native`.

unité:\<*REP_DONNEES_IM*>\logs\sklmLogs\.
Par exemple, C:\ProgramData\IBM\Installation Manager\logs\sklmLogs\.

Linux /<*REP_DONNEES_IM*>/logs/native.

Par exemple, /var/ibm/installationmanager/logs/native.

/<*REP_DONNEES_IM*>/logs/sklmLogs/.
Par exemple, /var/ibm/InstallationManager/logs/sklmLogs/.

Pour la définition de <*REP_DONNEES_IM*>, voir «Définitions relatives à un répertoire *HOME* et d'autres variables de répertoire», à la page 5.

Que faire ensuite

Avant d'utiliser IBM Security Key Lifecycle Manager, exécutez les tâches de post-installation décrites dans Etapes de post-installation.

Mot de passe chiffré pour les éléments du fichier de réponses

Vous devez ajouter les mots de passe chiffrés aux éléments concernés du fichier de réponses. L'utilitaire IBM Installation Manager permet de créer des mots de passe chiffrés.

Vous devez ajouter les mots de passe chiffrés aux éléments concernés du fichier de réponses. L'utilitaire IBM Installation Manager permet de créer des mots de passe chiffrés.

Windows

Par exemple, si vous procédez à l'extraction de l'image du produit IBM Security Key Lifecycle Manager dans le répertoire C:\SKLM\disk1, exécutez la commande suivante pour créer un mot de passe chiffré :

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

Ajoutez le mot de passe chiffré dans le fichier de réponses comme illustré dans l'exemple ci-après.

```
<data key='user.DB2_ADMIN_PWD,com.ibm.sklm301.db2.win.ofng'
value='<mot_de_passe_chiffré>'/>
<data key='user.CONFIRM_PASSWORD,com.ibm.sklm301.db2.win.ofng'
value='<mot_de_passe_chiffré>'/>
...
<data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm301.win'
value='<mot_de_passe_chiffré>'/>
<data key='user.WAS_ADMIN_CONF_PWD,com.ibm.sklm301.win'
value='<mot_de_passe_chiffré>'/>
...
<data key='user.SKLM_ADMIN_PASSWORD,com.ibm.sklm301.win'
value='<mot_de_passe_chiffré>'/>
<data key='user.SKLM_ADMIN_CONF_PWD,com.ibm.sklm301.win'
value='<mot_de_passe_chiffré>'/>
```

Linux Par exemple, si vous procédez à l'extraction de l'image du produit IBM Security Key Lifecycle Manager dans le répertoire /SKLM/disk1, exécutez la commande suivante pour créer un mot de passe chiffré :

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

Ajoutez le mot de passe chiffré dans le fichier de réponses comme illustré dans l'exemple ci-après.

```
<data key='user.DB2_ADMIN_PWD,com.ibm.sklm301.db2.lin.ofng'
value='<mot_de_passe_chiffré>'/>
<data key='user.CONFIRM_PASSWORD,com.ibm.sklm301.db2.lin.ofng'
value='<mot_de_passe_chiffré>'/>
...
<data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm301.linux'
value='<mot_de_passe_chiffré>'/>
<data key='user.WAS_ADMIN_CONF_PWD,com.ibm.sklm301.linux'
value='<mot_de_passe_chiffré>'/>
...
<data key='user.SKLM_ADMIN_PASSWORD,com.ibm.sklm301.linux'
value='<mot_de_passe_chiffré>'/>
<data key='user.SKLM_ADMIN_CONF_PWD,com.ibm.sklm301.linux'
value='<mot_de_passe_chiffré>'/>
```

Vous pouvez créer un mot de passe chiffré différent pour chaque utilisateur.

Configuration de Db2 lors de l'installation

IBM Security Key Lifecycle Manager nécessite Db2 Advanced Workgroup Server Edition version 11.1.2.2.

Le programme d'installation effectue une des actions suivantes :

- Si un exemplaire de Db2 Advanced Workgroup Server Edition est déjà installé en tant que root, au niveau de version correct pour le système d'exploitation, vous pouvez l'utiliser. Le programme d'installation d'IBM Security Key Lifecycle Manager ne détecte pas la présence de Db2. Vous devez indiquer le chemin d'installation de Db2.

  Vous pouvez aussi installer un nouvel exemplaire de Db2 Advanced Workgroup Server Edition. L'exemplaire existant de Db2 doit être installé localement sur le système, et non sur une unité réseau ou partagée.

  Sur un système Windows, si un nouvel exemplaire de Db2 est installé, la variable `DB2_COPY_NAME` est définie sur `DBSKLMV31`.
- Si une version antérieure d'IBM Security Key Lifecycle Manager et de Db2 existent sur le système, le processus installe la version Db2 Advanced Workgroup Server Edition 11.1.2.2 qui dépend du système d'exploitation. Vous pouvez également utiliser une autre version existante de Db2 11.1.2.2 située à un niveau correct.

  Le processus fait également migrer les données de la version précédente d'IBM Security Key Lifecycle Manager vers la nouvelle version. Par exemple :
  - La nouvelle copie de Db2 Advanced Workgroup Server Edition utilise l'ID utilisateur et le mot de passe de `db2admin`.
  - Sur un système Windows, si un nouvel exemplaire de Db2 est installé, la variable `DB2_COPY_NAME` est définie sur `DBSKLMV31`.
- Si aucune instance d'IBM Security Key Lifecycle Manager, copie ou version antérieure d'Db2 n'est installée sur le système, le processus installe la version 11.1.2.2 liée au système d'exploitation.

  Aucun migration de Db2 n'a lieu.

Lors de la configuration de Db2, vous êtes invité à fournir les informations ci-dessous, qui peuvent varier à la fois en fonction du système d'exploitation utilisé et selon que Db2 est une instance installée par IBM Security Key Lifecycle Manager ou une copie existante :

Sélection de Db2
: Répertoire d'installation de Db2.

Sur les systèmes Linux ou AIX, l'entrée doit commencer au niveau du répertoire racine. Le premier caractère de l'entrée doit être une barre oblique "/".

Le processus d'installation fournit une valeur par défaut. Voir «Définitions relatives à un répertoire *HOME* et d'autres variables de répertoire», à la page 5.

ID administrateur Db2
ID d'administrateur local de Db2. Le processus d'installation fournit un ID d'administrateur par défaut, avec les droits nécessaires. N'utilisez pas d'ID utilisateur du domaine comme administrateur de Db2. Ne spécifiez pas d'ID utilisateur de plus de huit caractères.

Remarque : N'utilisez pas de trait d'union (-) ni de caractère de soulignement (_) lorsque vous spécifiez un ID utilisateur pour une copie existante de Db2.

Sous Windows, l'ID utilisateur de l'administrateur Db2 doit appartenir au groupe administrateur. L'ID utilisateur est soumis à la stratégie de sécurité en vigueur sur le système Windows.

Sur un système Linux ou AIX, l'ID utilisateur du propriétaire de l'instance IBM Security Key Lifecycle Manager Db2 doit appartenir à un groupe dont l'ID superutilisateur est également membre. Il est recommandé d'utiliser bin, si ce groupe est disponible. Si `bin` n'est pas disponible, demandez à l'administrateur système de vous fournir le nom d'un groupe à usage général.

Mot de passe administrateur Db2
Mot de passe de l'administrateur. La longueur maximale est de 20 caractères. Pour plus d'informations sur les caractères spéciaux pris en charge, voir Caractères spéciaux pris en charge dans les mots de passe.

Le mot de passe de l'administrateur Db2 est soumis à la stratégie de sécurité en vigueur sur le système. 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. Lorsque vous changez un mot de passe, veillez à ce que l'autre mot de passe soit également changé.

Remarque : Si vous utilisez un utilisateur existant en tant qu'administrateur Db2, assurez-vous que le mot de passe est correctement spécifié lors de l'installation.

Nom de la base de données
Nom de la base de données IBM Security Key Lifecycle Manager, `SKLMDB31`.

Port Db2
Port utilisé par Db2.

Groupe de l'administrateur
Groupe d'accès dans lequel figure l'ID utilisateur de l'administrateur. Si Db2 est sur un système AIX ou Linux, votre ID utilisateur doit être dans le groupe bin ou root ou dans un groupe à part, dont root est membre.

Répertoire de base de l'administrateur/de la base de données
Répertoire (systèmes AIX ou Linux) ou lecteur (systèmes Windows) dans lequel sont créées l'instance de la base de données et les tables formatées utilisées par IBM Security Key Lifecycle Manager.

Remarques :

- Pour tous les champs, les données entrées doivent se limiter aux caractères alphabétiques (A-Z et a-z), aux chiffres de 0 à 9 et au caractère de soulignement (_). La restriction s'applique également aux valeurs spécifiées dans le fichier de réponses utilisé pour les installations en mode silencieux.
- Les espaces ne sont pas autorisés dans les chemins de répertoire et les noms de fichier.
- Le nom de l'ordinateur sur lequel vous installez Db2 ne doit pas commencer par "ibm" ,"sql" ou "sys", que ce soit en minuscules ou en majuscules. Le nom de l'ordinateur ne doit pas non plus contenir de caractère de soulignement (_).
- Si vous utilisez un utilisateur existant en tant qu'administrateur Db2, assurez-vous que le mot de passe est correctement spécifié lors de l'installation.
- Le nom du groupe admin Db2 ne peut pas comporter plus de 8 caractères.

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 *RACINE_WAS*/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('JAASAuthData_list_entry','[[password passw0rd]]')
      ```

      Par exemple, entrez sur une seule ligne :

      ```
      print AdminConfig.modify
      ('(cells/SKLMCell|security.xml#JAASAuthData_1228871756187)','[[password passw0rd]]')
      ```

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

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

      Par exemple, entrez sur une seule ligne :

      ```
      print AdminConfig.modify
      ('(cells/SKLMCell|security.xml#JAASAuthData_1228871757843)','[[password passw0rd]]')
      ```

   e. Enregistrez les modifications :

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

   f. Reprenez l'ID superutilisateur.

      ```
      exit
      ```

   g. Dans le répertoire *RACINE_WAS*/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 *RACINE_WAS*/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.
```

Conditions et exigences pour l'ID utilisateur Db2

Vous devez vous assurer que l'administrateur Db2 respecte les conditions et exigences spécifiques.

- Il doit y avoir un groupe primaire autre que `invités`, `admins`, `utilisateurs` et `local`.
- Il peut contenir des lettres minuscules (a-z), des chiffres (0-9) et le caractère de soulignement (_).
- Il ne peut pas comporter plus de huit caractères.
- Ils ne peuvent pas commencer par `IBM`, `SYS`, `SQL`, ou un chiffre
- Vous ne pouvez pas utiliser de mot réservé DB2 (`USERS`, `ADMINS`, `GUESTS`, `PUBLIC` ou `LOCAL`) ou de mot réservé SQL

- Il ne peut pas utiliser des ID utilisateur avec des droits root pour l'ID de l'instance DB2, l'ID DAS ou l'ID isolé.
- Il ne peut pas comporter de caractères accentués.

Configuration de WebSphere Application Server et du serveur IBM Security Key Lifecycle Manager pendant l'installation

L'assistant d'installation recueille des informations de configuration pour IBM Security Key Lifecycle Manager et pour l'environnement d'exécution WebSphere Application Server.

Administration de serveur d'applications

Nom d'utilisateur
Indiquez l'ID utilisateur de connexion à WebSphere Application Server utilisé pour le profil d'administrateur d'IBM Security Key Lifecycle Manager.

Mot de passe
Indiquez le mot de passe de l'ID de connexion à WebSphere Application Server utilisé pour le profil IBM Security Key Lifecycle Manager. Pour plus d'informations sur les caractères spéciaux pris en charge, voir Caractères spéciaux pris en charge dans les mots de passe.

Port d'administration HTTPS
Indique le port HTTPS permettant d'accéder à WebSphere Integrated Solutions Console et au profil d'IBM Security Key Lifecycle Manager.

La valeur par défaut est 9083.

Administration d'application IBM Security Key Lifecycle Manager

Nom d'utilisateur
Spécifiez l'ID utilisateur pour administrer IBM Security Key Lifecycle Manager.

Mot de passe
Indiquez le mot de passe de l'administrateur IBM Security Key Lifecycle Manager. Pour plus d'informations sur les caractères spéciaux pris en charge, voir Caractères spéciaux pris en charge dans les mots de passe.

Numéro de port HTTPS
Indiquez le port sécurisé pour accéder à IBM Security Key Lifecycle Manager.

La valeur par défaut est 443.

Numéro de port HTTP
Indiquez le port non sécurisé pour accéder à IBM Security Key Lifecycle Manager.

La valeur par défaut est 80.

Remarque :

La chaîne **Nom d'utilisateur** ne doit pas contenir d'espace à gauche ou à droite ni les caractères suivants :

/ barre oblique
\ barre oblique inversée

* astérisque
, virgule
: deux-points
; point-virgule
= signe égal
+ signe plus
? point d'interrogation
| barre verticale
< signe inférieur à
> signe supérieur à
& perluète ("et" commercial)
% signe pour cent
' apostrophe
" guillemet
]]> (Deux crochets droits suivis du signe supérieur à)
. point (interdit comme premier caractère, mais autorisé ailleurs dans la chaîne)
# signe dièse
$ symbole du dollar
~ tilde
(parenthèse gauche
) parenthèse droite

Migration de la configuration d'Encryption Key Manager

Vous disposez d'une option permettant d'effectuer la migration d'une configuration existante d'Encryption Key Manager vers IBM Security Key Lifecycle Manager.

Avant de commencer, procurez-vous le mot de passe de connexion à serveur Encryption Key Manager.

Pour migrer une configuration existante, sélectionnez l'option suivante :

Migration de Encryption Key Manager
Cochez cette case si vous avez un ancien fichier de propriétés Encryption Key Manager à faire migrer vers IBM Security Key Lifecycle Manager. Si vous cochez cette case, vous devez spécifier le fichier de propriétés du système Encryption Key Manager précédent.

La migration est possible à partir de la version 2.1 de Encryption Key Manager.

Vous devez désactiver Encryption Key Manager lors de la migration. Pour arrêter un processus Encryption Key Manager en cours d'exécution, procédez comme suit :

1. Démarrez une session administrative. Dans la version 2.1, entrez la commande suivante :

   ```
   java com.ibm.keymanager.KMSAdminCmd KeyManagerConfig.properties -i
   ```

2. Une fois la session administrative démarrée, procédez comme suit :
   a. Authentifiez-vous sur le serveur Encryption Key Manager à l'aide de la commande login. Entrez :

      ```
      login -ekmuser EKMAdmin -password mot_de_passe
      ```

   b. Arrêtez le serveur. Entrez :

      ```
      stopekm
      ```

3. Quittez la session.

Pour les restrictions sur la migration, voir «Conditions et limitations de la migration d'Encryption Key Manager», à la page 29.

Sauvegardez le serveur sur lequel se trouvent les données de configuration à migrer. Les données migrées comprennent les fichiers suivants :

- Un fichier de propriétés de configuration
- Des clés et des certificats référencés par le fichier de propriétés de configuration
- Des tables d'unités
- Un fichier de métadonnées facultatif, vers lequel pointe le fichier de propriétés de configuration
- Un fichier de groupes de clés facultatif

Remarque : Vous pouvez également faire appel à l'utilitaire de sauvegarde multiplateforme pour exécuter l'opération de sauvegarde sur Encryption Key Manager 2.1 afin de sauvegarder les données critiques. Vous pouvez ensuite restaurer les fichiers de sauvegarde d'IBM Security Key Lifecycle Manager version 3.0 sur un système d'exploitation différent de celui sur lequel ils ont été créés. Pour plus d'informations, voir Opérations de sauvegarde et de restauration pour les versions précédentes d'IBM Security Key Lifecycle Manager et d'IBM Tivoli Key Lifecycle Manager.

Migration d'IBM Security Key Lifecycle Manager en mode en ligne silencieux

Le processus de migration d'IBM Security Key Lifecycle Manager en mode en ligne silencieux est similaire au processus d'installation du produit en mode silencieux. Avec ce type de migration, vous pouvez mettre à niveau IBM Security Key Lifecycle Manager sur le serveur et migrer des données de la version ACTUELLE (actuellement installée) vers la NOUVELLE version (la plus récente). Pour pouvoir migrer en mode en ligne silencieux, vous devez disposer d'un fichier de réponses qui définit la configuration de migration.

Avant de commencer

- Téléchargez et extrayez les fichiers pour IBM Security Key Lifecycle Manager dans un répertoire. Ces fichiers peuvent être téléchargés depuis le site Web IBM Passport Advantage. Voir la rubrique Images d'installation et groupes de correctifs pour plus de détails.
- Consultez la rubrique Instructions d'installation pour connaître les considérations et les restrictions relatives à l'installation et la configuration d'IBM Security Key Lifecycle Manager.
- Consultez la rubrique Planification de la migration pour comprendre les exigences.
- Lisez les dispositions du contrat de licence relatives à ce produit. Pour localiser les fichiers contenant ces informations, dans le répertoire principal dans lequel se trouve le module d'installation, accédez au sous-répertoire `disk1/im/license`. Le sous-répertoire `/license` contient les fichiers de licence au format texte.
- Sélectionnez l'exemple de fichier de réponses approprié.

  Utilisez le fichier de réponses `SKLM_Silent_`*`platform`*`_Mig_`*`version`*`_Resp.xml` dans lequel
  - *platform* correspond au système d'exploitation qui s'exécute sur le serveur.
  - *version* correspond à la version IBM Security Key Lifecycle Manager ACTUELLE.

IBM Security Key Lifecycle Manager inclut des exemples de fichiers de réponses spécifiques à la plateforme que vous pouvez utiliser comme modèles pour créer votre propre fichier de réponses. Ces exemples de fichiers de réponses se trouvent dans le répertoire dans lequel se trouve votre module d'installation.

Par exemple, si le serveur s'exécute sous Linux et que la version ACTUELLE d'IBM Security Key Lifecycle Manager est 3.0, utilisez le fichier de réponses `SKLM_Silent_Linux_Mig_30_Resp.xml`.

- Obtenez les valeurs chiffrées des mots de passe des administrateurs d'IBM Security Key Lifecycle Manager, de WebSphere Application Server et de la base de données ACTUELLE.

  Créez également un mot de passe chiffré pour l'administrateur de la NOUVELLE base de données, à savoir la nouvelle instance de base de données qui sera installée dans le cadre de la migration.

  Ces mots de passe sont utilisés dans la procédure de migration en ligne en mode silencieux.

  Pour créer le mot de passe chiffré, utilisez l'utilitaire IBM Installation Manager. Pour plus d'informations, voir Mot de passe chiffré pour les éléments du fichier de réponses.

Pourquoi et quand exécuter cette tâche

Pour migrer IBM Security Key Lifecycle Manager en mode en ligne silencieux, procédez comme suit :

Procédure

1. Ouvrez l'exemple de fichier de réponses en mode édition et mettez à jour les paramètres suivants :

   repository location
   Indiquez le chemin d'accès complet du répertoire dans lequel se trouve le module d'installation.

   Remarque : Si vous entrez une valeur non valide pour ce paramètre, le programme d'installation se ferme sans message d'erreur et l'erreur n'est pas consignée.

   Le fichier doit contenir deux instances de ce paramètre, et les deux doivent être mises à jour. Indiquez les valeurs comme suit :

   ```
   <repository location='myRepositoryLocation\im'/>
   <repository location='myRepositoryLocation\'/>
   ```

   où *myRepositoryLocation* correspond au chemin d'accès complet du répertoire du module d'installation.
   Par exemple, si le module d'installation se trouve dans le répertoire *C:\sklm301*, mettez à jour ce paramètre comme suit :

   ```
   <repository location='/SKLM301/disk1/im'/>
   <repository location='/SKLM301/disk1/'/>
   ```

   user.DB2_ADMIN_PWD,com.ibm.sklm301.db2.*platform*.ofng
   Indiquez le mot de passe chiffré pour le NOUVEL administrateur de base de données.

   Par exemple :

   ```
   <data key='user.DB2_ADMIN_PWD,com.ibm.sklm301.db2.linux.ofng' value='QTh/0AiFacssjhs9gnOYkGA=='/>
   ```

user.CONFIRM_PASSWORD,com.ibm.sklm301.db2.*platform*.ofng
Indiquez le même mot de passe que celui fourni dans le paramètre **user.DB2_ADMIN_PWD,com.ibm.sklm301.db2.*platform*.ofng**.

Par exemple :

```
<data key='user.CONFIRM_PASSWORD,com.ibm.sklm301.db2.linux.ofng' value='QTh/0AiFacssjhs9gnOYkGA=='/>
```

user.WAS_HOME,com.ibm.sklm301.*platform*
Indiquez le chemin du répertoire *WAS_HOME* pour le NOUVEAU WebSphere Application Server. Pour la définition de *WAS_HOME*, voir «Définitions relatives à un répertoire *HOME* et d'autres variables de répertoire», à la page 5.

Par exemple :

```
<data key='user.WAS_HOME,com.ibm.sklm301.linux' value='/opt/IBM/WebSphere/AppServer'/>
```

user.WAS_ADMIN_ID,com.ibm.sklm301.*platform*
Indiquez l'ID utilisateur de l'administrateur ACTUEL de WebSphere Application Server.

Par exemple :

```
<data key='user.WAS_ADMIN_ID,com.ibm.sklm301.linux' value='tipadmin'/>
```

user.WAS_ADMIN_PASSWORD,com.ibm.sklm301.*platform*
Indiquez le mot de passe chiffré de l'administrateur ACTUEL de WebSphere Application Server. Ce mot de passe sera utilisé pour le NOUVEL administrateur de WebSphere Application Server.

Par exemple :

```
<data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm301.linux' value='e9PjN93MeQxyzSs9VXJFMw==''/>
```

user.WAS_ADMIN_CONF_PWD,com.ibm.sklm301.*platform*
Indiquez le même mot de passe que celui fourni dans le paramètre **user.WAS_ADMIN_CONF_PWD,com.ibm.sklm301.***platform*.

Par exemple :

```
<data key='user.WAS_ADMIN_CONF_PWD,com.ibm.sklm301.linux' value='e9PjN93MeQxyzSs9VXJFMw==''/>
```

user.SKLM_ADMIN_USER,com.ibm.sklm301.*platform*
Indiquez l'ID utilisateur de l'administrateur ACTUEL de IBM Security Key Lifecycle Manager.

Par exemple :

```
<data key='user.SKLM_ADMIN_USER,com.ibm.sklm301.linux' value='TKLMAdmin'/>
```

user.SKLM_ADMIN_PASSWORD,com.ibm.sklm301.*platform*
Indiquez le mot de passe chiffré de l'administrateur ACTUEL de IBM Security Key Lifecycle Manager. Ce mot de passe s'appliquera au NOUVEL administrateur d'IBM Security Key Lifecycle Manager.

Par exemple :

```
<data key='user.SKLM_ADMIN_PASSWORD,com.ibm.sklm301.linux' value='9YTRJMRIydDSdfhaHPs1mn==''/>
```

user.SKLM_ADMIN_CONF_PWD,com.ibm.sklm301.*platform*
Indiquez le même mot de passe que celui fourni dans le paramètre **user.SKLM_ADMIN_PASSWORD,com.ibm.sklm301.***platform*.

Par exemple :

```
<data key='user.SKLM_ADMIN_CONF_PWD,com.ibm.sklm301.linux' value='9YTRJMRIydDSdfhaHPs1mn==''/>
```

user.TKLM_VERSION,com.ibm.sklm301.*platform*
Indiquez la version ACTUELLE d'IBM Security Key Lifecycle Manager.

Par exemple, si vous migrez à partir de la version 3.0 sur un serveur s'exécutant sous Linux, mettez à jour ce paramètre comme suit :

```
<data key='user.TKLM_VERSION,com.ibm.sklm301.linux' value='3.0.0.0'/>
```

user.TKLM_TIP_HOME,com.ibm.sklm301.*platform*
Pour IBM Security Key Lifecycle Manager 2.5 et versions ultérieures, indiquez le chemin du répertoire *WAS_HOME* pour l'instance ACTUELLE de WebSphere Application Server. Pour la définition de *WAS_HOME*, voir «Définitions relatives à un répertoire *HOME* et d'autres variables de répertoire», à la page 5.

Par exemple :

```
<data key='user.TKLM_TIP_HOME,com.ibm.sklm301.linux' value='/opt/IBM/WebSphere/AppServer'/>
```

Pour les versions d'IBM Security Key Lifecycle Manager antérieures à la version 2.5, vérifiez et indiquez le répertoire d'installation de WebSphere Application Server. Par exemple :

```
<data key='user.TKLM_TIP_HOME,com.ibm.sklm301.linux' value='/opt/IBM/tivoli/tiptklmV2'/>
```

user.TKLM_INSTALLED,com.ibm.sklm301.*platform*
Assurez-vous que la valeur est `true`, ce qui indique qu'une version antérieure d'IBM Security Key Lifecycle Manager est déjà installée sur le serveur.

Par exemple :

```
<data key='user.TKLM_INSTALLED,com.ibm.sklm301.linux' value='true'/>
```

user.TKLM_DB_PWD,com.ibm.sklm301.*platform*
Indiquez le mot de passe chiffré pour la base de données ACTUELLE.

Par exemple :

```
<data key='user.TKLM_DB_PWD,com.ibm.sklm301.linux' value='SwIhGBTDHcJok80Ux4Sb3g=='/>
```

user.SKLM_APP_PORT,com.ibm.sklm301.*platform*
Indiquez le numéro du port sur lequel le NOUVEAU serveur IBM Security Key Lifecycle Manager écoute les demandes HTTPS.

Par exemple :

```
<data key='user.SKLM_APP_PORT,com.ibm.sklm301.linux' value='8443'/>
```

user.WAS_ADMIN_PORT,com.ibm.sklm301.*platform*
Indiquez le numéro du port sur lequel la NOUVELLE instance de WebSphere Application Server écoute les demandes.

Par exemple :

```
<data key='user.WAS_ADMIN_PORT,com.ibm.sklm301.linux' value='8083'/>
```

user.SKLM_APP_NS_PORT,com.ibm.sklm301.*platform*
Indiquez le numéro du port sur lequel le NOUVEAU serveur IBM Security Key Lifecycle Manager écoute les demandes HTTP.

Par exemple :

```
<data key='user.SKLM_APP_NS_PORT,com.ibm.sklm301.linux' value='8080'/>
```

2. Enregistrez le fichier de réponses et fermez-le.
3. Assurez-vous que le fichier JAR Db2 `db2jcc.jar` existe dans le répertoire d'installation. Si ce n'est pas le cas, copiez le fichier du module d'installation dans le répertoire d'installation.

   Par exemple, copiez le fichier de `disk1/im/jre_7.0.9040.20160504_1613/jre/lib/ext` dans `/opt/IBM/InstallationManager/eclipse/jre_7.0.9040.20160504_1613/jre/lib/ext`.
4. Ouvrez une ligne de commande et exécutez la commande d'installation en mode silencieux, comme suit :

   ```
   ./silent_install.sh myResponseFile -acceptLicense
   ```

où *myResponseFile* correspond au fichier de réponses que vous souhaitez utiliser. Par exemple, `SKLM_Silent_Linux_30_Resp.xml`.

En indiquant le paramètre **-acceptLicense**, vous acceptez les dispositions du contrat de licence de ce produit.

5. Vérifiez que l'installation a abouti en examinant les fichiers journaux. Vous pouvez afficher les journaux IBM Installation Manager aux emplacements suivants.

   Windows

   `unité:\<REP_DONNEES_IM>\logs\native`.

   Par exemple, `C:\ProgramData\IBM\Installation Manager\logs\native`.

   `unité:\<REP_DONNEES_IM>\logs\sklmLogs\`.
   Par exemple, `C:\ProgramData\IBM\Installation Manager\logs\sklmLogs\`.

   Linux `/<REP_DONNEES_IM>/logs/native`.

   Par exemple, `/var/ibm/installationmanager/logs/native`.

   `/<REP_DONNEES_IM>/logs/sklmLogs/`.
   Par exemple, `/var/ibm/InstallationManager/logs/sklmLogs/`.

   Pour la définition de *<REP_DONNEES_IM>*, voir «Définitions relatives à un répertoire *HOME* et d'autres variables de répertoire», à la page 5.

Que faire ensuite

Avant d'utiliser IBM Security Key Lifecycle Manager, exécutez les tâches de post-installation décrites dans Etapes de post-installation.

Configuration d'un cluster multimaître sur un serveur IBM Security Key Lifecycle Manager version 3.0.1 ayant fait l'objet d'une migration croisée

Vous pouvez configurer un cluster multimaître sur un serveur IBM Security Key Lifecycle Manager version 3.0.1 qui fait l'objet d'une migration croisée à partir de l'une des versions antérieures.

Avant de commencer

Assurez-vous que le serveur IBM Security Key Lifecycle Manager sur lequel vous souhaitez configurer le cluster multimaître fait l'objet d'une migration croisée vers la version 3.0.1.

Procédure

1. Dans le fichier `SKLMConfig.properties`, mettez à jour la propriété **`TransportListener.ssl.protocols`** sur la valeur `TLSv1.2`.

   ```
   TransportListener.ssl.protocols=TLSv1.2
   ```

   Vous pouvez utiliser la commande de l'interface CLI Service REST Update Config Property ou tklmConfigUpdateEntry pour mettre à jour la propriété.
2. Arrêtez l'agent IBM Security Key Lifecycle Manager.
3. Redémarrez le serveur IBM Security Key Lifecycle Manager.

4. Lors du processus de restauration, si vous avez défini la propriété **RESTORE_USER_ROLES** sur RESTORE_USER_ROLES=y dans l'utilitaire restoreV*version* (par exemple, restoreV25.bat), actualisez les données d'identification de l'utilisateur sur le serveur IBM Security Key Lifecycle Manager :
   a. Connectez-vous à l'interface graphique IBM Security Key Lifecycle Manager.
   b. Cliquez sur **Administration** > **Multimaître**.
   c. Sur la page, cliquez sur le lien **Multimaître**, puis cliquez sur **OK** dans la boîte de dialogue Confirmer.
   d. Dans la table **Maîtres**, sélectionnez le serveur maître, puis cliquez sur **Modify Master**.
   e. Dans la fenêtre Configuration multimaître - Modifier un maître, indiquez les valeurs du mot de passe **IBM Security Key Lifecycle Manager** et du mot de passe **WebSphere Application Server**.
   f. Cliquez sur **Accepter automatiquement le certificat d'hôte**, puis sur **Mettre à jour**.
   g. Dans la boîte de dialogue contenant le message d'information Le maître a été modifié correctement, cliquez sur **Fermer**.
   h. Cliquez sur **Annuler**.

   Le serveur maître IBM Security Key Lifecycle Manager est configuré en tant que maître principal.

Que faire ensuite

Vous pouvez maintenant ajouter des serveurs maîtres de secours et non HADR au cluster. Pour plus d'informations, voir Ajout d'un maître de secours au cluster et Ajout d'un maître au cluster.

Erreurs survenant au cours de l'installation

Certaines erreurs devant être impérativement corrigées peuvent se produire lors de l'installation. La plupart des messages d'erreur contiennent suffisamment d'informations pour vous permettre de corriger la cause de l'erreur. Cependant, certaines conditions d'erreur requièrent des informations supplémentaires.

L'installation silencieuse peut se terminer prématurément sans afficher de message d'erreur, mais des erreurs sont consignées dans le fichier journal.

Si l'installation en mode silencieux se termine avec un code retour zéro, examinez également le fichier journal pour voir si des messages d'erreur y ont été consignés.

Windows

\<*IM_DATA_DIR*>\logs

Linux ou AIX

/<*IM_DATA_DIR*>/logs

Pour la définition de <*REP_DONNEES_IM*>, voir «Définitions relatives à un répertoire *HOME* et d'autres variables de répertoire», à la page 5.

Si vous recevez un message d'erreur concernant un disque ou un système de fichiers n'ayant pas suffisamment d'espace disque :

Supprimez des fichiers pour faire de la place sur le disque ou ajoutez de l'espace de stockage à votre système pour augmenter la taille du système de fichiers.

Ne corrigez pas ce problème pendant que le programme d'installation est en cours d'exécution. Quittez le programme d'installation avant d'effectuer les corrections et redémarrez-le une fois les corrections effectuées.

Pour plus d'informations sur l'espace disque et les configurations matérielles, voir «Configuration matérielle requise», à la page 7.

Si vous installez IBM Security Key Lifecycle Manager à l'aide d'un logiciel Exceed X Server sur une machine locale tout en exportant l'affichage depuis un système Linux, ne refusez pas le contrat de licence.

Si vous refusez le contrat de licence, le programme d'installation risque de ne plus répondre. Acceptez le contrat de licence ou bien utilisez un serveur Cygwin X Server ou une connexion VNC (Virtual Network Connection) à la place.

Si vous supprimez le compte d'administrateur `sklmdb31` à l'aide de l'outil Windows de gestion des utilisateurs et des groupes, vous devez également supprimer le sous-répertoire `sklmdb301` avant de réinstaller IBM Security Key Lifecycle Manager et Db2.

Lors de l'installation d'IBM Security Key Lifecycle Manager, un problème peut survenir si vous avez utilisé auparavant l'outil de gestion des groupes et des utilisateurs Windows pour supprimer en tant qu'administrateur Db2 l'ID utilisateur `sklmdb31`. A la réinstallation d'IBM Security Key Lifecycle Manager, le processus ne parvient pas à installer Db2.

Pour corriger le problème, effectuez les étapes suivantes :

1. Placez-vous dans le sous-répertoire approprié :
   - Windows Server 2012 : *`lecteur`*`:\Users`
2. Supprimez le sous-répertoire `sklmdb301`.
3. Réinstallez IBM Security Key Lifecycle Manager. Le sous-répertoire `sklmdb301` n'est pas automatiquement supprimé lorsque vous utilisez l'outil Windows de gestion des utilisateurs et des groupes pour supprimer le compte utilisateur `sklmdb301`.

Installation non root d'IBM Security Key Lifecycle Manager sur des systèmes Linux

Vous pouvez installer IBM Security Key Lifecycle Manager en tant qu'utilisateur non superutilisateur sur un système d'exploitation Linux.

Meilleures pratiques et instructions relatives à l'installation non root d'IBM Security Key Lifecycle Manager sur des systèmes Linux

Lorsque vous planifiez votre installation non root d'IBM Security Key Lifecycle Manager sur des systèmes Linux, vous pouvez appliquer un certain nombre de meilleures pratiques. Prenez-en connaissance avant de lancer l'installation.

- Vérifiez que l'utilisateur non superutilisateur appartient à un groupe principal non root. L'utilisateur non superutilisateur doit appartenir à un groupe principal autre que `guests`, `admins`, `users` ou `local`.
- Le répertoire de base de l'utilisateur non superutilisateur (`$HOME`) doit pointer vers l'emplacement approprié. Par exemple : `/home/<nom_utilisateur>`
- Vérifiez que l'installation précédente (le cas échéant) d'IBM Security Key Lifecycle Manager et de Db2 sur le système ont été intégralement supprimées.

- Lorsque vous installez IBM Security Key Lifecycle Manager, il se peut que le scanner de prérequis échoue pour l'installation non root. Assurez-vous que tous les prérequis sont remplis à l'exception des privilèges d'administrateur avant de poursuivre l'installation.

  Pour poursuivre l'installation, ignorez l'exécution du scanner de prérequis. Pour cela, créez le fichier `sklmInstall.properties` dans le répertoire `/tmp` à l'aide de la propriété suivante :

  ```
  SKIP_PREREQ=true
  ```
- Vérifiez que les paramètres de noyau au niveau du système d'exploitation sont corrects pour l'installation de Db2. Pour plus d'informations sur les paramètres de noyau Db2, voir la documentation Db2 à l'adresse : http://www.ibm.com/support/knowledgecenter/SSEPGG_11.1.0/com.ibm.db2.luw.qb.server.doc/doc/t0008238.html
- Pendant l'installation, l'ID administrateur de la base de données doit être le même que celui de l'utilisateur non superutilisateur qui est connecté au système pour exécuter le processus d'installation. Vérifiez que les exigences suivantes d'ID administrateur de base de données sont remplies :
  - La longueur maximale de l'ID administrateur de base de données est de 8 caractères.
  - Le mot de passe de l'ID administrateur de base de données est le même que celui de l'utilisateur non superutilisateur au niveau du système d'exploitation.
  - Le groupe administrateur de base de données est le même que le groupe principal de l'utilisateur non superutilisateur au niveau du système d'exploitation.
  - Le répertoire de base de la base de données doit pointer vers le répertoire de base de l'utilisateur non superutilisateur.
- Vous ne pouvez pas installer IBM Security Key Lifecycle Manager en tant qu'utilisateur non root en mode silencieux.
- La migration de versions antérieures d'IBM Security Key Lifecycle Manager (1.0, 2.0, 2.0.1, 2.5, 2.6, 2.7) et du composant Encryption Key Manager vers une installation non root de version 3.0.1 n'est pas prise en charge.
- Db2 risque de ne pas démarrer à l'amorçage du système lorsqu'il est installé en tant qu'utilisateur non superutilisateur. Corrigez le problème en démarrant Db2 avant WebSphere Application Server. Exécutez le script `nonrootconfig.sh` lorsque le programme d'installation a abouti.
- Le nom du groupe admin Db2 ne peut pas comporter plus de 8 caractères.
- Une fois la commande nonrootconfig.sh exécutée et WebSphere Application Server démarré, le message d'erreur `No DB connected` indiquant qu'aucune base de données n'est connectée peut s'afficher dans l'interface utilisateur d'IBM Security Key Lifecycle Manager. Pour résoudre ce problème, redémarrez Db2 et WebSphere Application Server.

Installation d'IBM Security Key Lifecycle Manager sur des systèmes Linux en tant qu'utilisateur non root

Vous pouvez installer IBM Security Key Lifecycle Manager en tant qu'utilisateur non root sur un système d'exploitation Linux. L'installation non root d'IBM Security Key Lifecycle Manager installe à la fois Db2 et WebSphere Application Server en tant qu'utilisateur non root.

Pourquoi et quand exécuter cette tâche

Avant d'installer IBM Security Key Lifecycle Manager sur des systèmes Linux en tant qu'utilisateur non root, prenez connaissance des meilleures pratiques décrites dans la rubrique «Installation non root d'IBM Security Key Lifecycle Manager sur des systèmes Linux», à la page 64.

Procédure

1. Assurez-vous que la configuration requise pour l'installation d'IBM Security Key Lifecycle Manager est respectée. Voir «Planification de l'installation», à la page 5.
2. Créez un ID utilisateur non root. Assurez-vous que l'ID utilisateur a un groupe principal autre que `invités`, `admins`, `utilisateurs` et `local`.
3. Ignorez l'exécution du scanner de prérequis en créant le fichier `sklmInstall.properties` dans le répertoire `/tmp` avec la propriété suivante.

   ```
   SKIP_PREREQ=true
   ```
4. Accédez au répertoire de votre package d'installation et ouvrez `disk1`. Exemple : *chemin_téléchargement*`/disk1`.
5. Ouvrez une fenêtre de ligne de commande et exécutez **launchpad.sh**.
6. Spécifiez les paramètres de configuration Db2. Voir «Configuration de Db2 lors de l'installation non root», à la page 67.
7. Spécifiez les paramètres de configuration WebSphere Application Server.
8. Une fois le processus d'installation d'IBM Security Key Lifecycle Manager terminé, ouvrez la fenêtre de ligne de commande.
9. Arrêtez WebSphere Application Server et Db2.

   Remarque : Veillez à exécuter cette étape en tant qu'utilisateur non superutilisateur créé à l'étape 2.

   Exécutez la commande suivante pour arrêter WebSphere Application Server :

   ```
   cd <RACINE_WAS>/bin
   ./stopServer.sh <nom_serveur> -username <ID administrateur WAS>
   -password <Mot de passe administrateur WAS>
   ```

   ```
   ./stopServer.sh server1 -username wasadmin -password wasadmin_pwd
   ```

   Exécutez la commande suivante pour arrêter Db2 :

   ```
   cd ~/sqllib/adm
   ./db2stop
   ```
10. Ouvrez un nouveau shell et exécutez la commande suivante sous `/home/username/sklm301properties/scripts`.

    L'installation non root de Db2 nécessite un accès root pour configurer l'instance Db2 avec un numéro de port et un nom de service spécifiques.

    ```
    sudo nonrootconfig.sh <DB_INST_HOME> <DB_INST_NAME> <PORT> <DB_USER>
     <DB_PASSWORD> <WAS_HOME> <WAS_USER> <WAS_PASSWORD>
    ```

    Par exemple, **sudo nonrootconfig.sh /home/testuser testuser 50050 testuser mydbpwd /home/testuser/IBM/WebSphere/AppServer wasadmin mypwd**. où

    <*DB_INST_HOME*> - Répertoire contenant l'instance de base de données Db2. Par exemple, `/home/testuser`.

    <*DB_INST_NAME*> - Nom de l'instance Db2. Par exemple, `testuser`.

    <*PORT*> - Port d'écoute du service Db2. Par exemple, 50050.

    <*DB_USER*> - Nom de l'utilisateur Db2. Par exemple, `testuser`.

<*DB_PASSWORD*> - Mot de passe Db2. Par exemple, `mydbpwd`.

<*WAS_HOME*> - Répertoire de base WebSphere Application Server. Par exemple, `/home/testuser/IBM/WebSphere/AppServer`.

<*WAS_USER*> - Nom de l'utilisateur WebSphere Application Server. Par exemple, `wasadmin`.

<*WAS_PASSWORD*> - Mot de passe WebSphere Application Server. Par exemple, `mypwd`.Lorsque vous exécutez le script, vous êtes invité à indiquer un mot de passe pour le nom d'utilisateur Db2 afin de poursuivre l'installation.

11. Redémarrez WebSphere Application Server.

    Remarque : Veillez à exécuter cette étape en tant qu'utilisateur non superutilisateur créé à l'étape 2.

    ```
    cd RACINE_WAS/bin
    ./startServer.sh nom_serveur
    ```

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

Que faire ensuite

- Dans le fichier *SKLM_HOME*`/config/SKLMConfig.properties`, mettez à jour le numéro de port SSL en indiquant une valeur supérieure à 1024 à l'aide de l'interface graphique, de l'interface de ligne de commande ou de l'interface REST. Par exemple :

  ```
  TransportListener.ssl.port=441
  ```

- Redémarrez le serveur IBM Security Key Lifecycle Manager.

  Une fois l'installation terminée, connectez-vous en tant qu'utilisateur non superutilisateur pour démarrer ou arrêter les serveurs IBM Security Key Lifecycle Manager et Db2.

Configuration de Db2 lors de l'installation non root

IBM Security Key Lifecycle Manager nécessite Db2 Advanced Workgroup Server Edition 11.1.2.2 qui dépend du système d'exploitation.

Lors de la configuration de Db2 , vous êtes invité à fournir les informations suivantes :

ID administrateur Db2
: ID d'administrateur local de Db2. Etant donné que l'utilisateur Db2 non root ne peut avoir qu'une seule instance, l'ID administrateur Db2 doit être identique à l'ID utilisateur qui est connecté sur le système. Assurez-vous que la longueur maximale de l'ID est de 8 caractères.

Mot de passe administrateur Db2
: Mot de passe de l'administrateur. Assurez-vous que la longueur maximale du mot de passe est de 20 caractères.

  Le mot de passe de l'administrateur Db2 est soumis à la stratégie de sécurité en vigueur sur le système. Le mot de passe de l'ID administrateur Db2 doit être identique au niveau du système d'exploitation à celui de l'utilisateur non superutilisateur connecté au système. Si vous modifiez l'un, vous devez faire de même pour l'autre.

Nom de la base de données
: Nom de la base de données IBM Security Key Lifecycle Manager, à savoir `SKLMDB31`.

Port Db2
: Port utilisé par Db2.

Groupe de l'administrateur
Groupe d'accès dans lequel figure l'ID utilisateur de l'administrateur. Le groupe administrateur de bases de données doit être identique à celui du groupe principal de l'utilisateur non superutilisateur au niveau du système d'exploitation.

Répertoire de base de l'administrateur/de la base de données
Le répertoire où sont créées l'instance de base de données et les tables formatées utilisées par IBM Security Key Lifecycle Manager sont créés. Le répertoire de base de la base de données doit pointer vers le répertoire de base de l'utilisateur non superutilisateur.

Remarques :

1. Pour tous les champs, les données entrées doivent se limiter aux caractères alphabétiques (A-Z et a-z), aux chiffres de 0 à 9 et au caractère de soulignement (_). La restriction s'applique également aux valeurs spécifiées dans le fichier de réponses utilisé pour les installations en mode silencieux.
2. Les espaces ne sont pas autorisés dans les chemins de répertoire et les noms de fichier.
3. Le nom de l'ordinateur sur lequel vous installez Db2 ne doit pas commencer par «ibm», «sql» ou «sys», que ce soit en minuscules ou en majuscules. Le nom de l'ordinateur ne doit pas non plus contenir de caractère de soulignement (_).
4. Le nom du groupe admin Db2 ne peut pas comporter plus de 8 caractères.

Pour plus d'informations sur la façon de modifier les paramètres du noyau et l'installation non root, voir la documentation de Db2.

- http://www-01.ibm.com/support/knowledgecenter/SSEPGG_11.1.0/com.ibm.db2.luw.qb.server.doc/doc/t0008238.html
- http://www-01.ibm.com/support/knowledgecenter/SSEPGG_11.1.0/com.ibm.db2.luw.qb.server.doc/doc/t0050571.html

Procédure de post-installation

Une fois IBM Security Key Lifecycle Manager installé, vérifiez que les services Db2 et WebSphere Application Server sont correctement configurés.

URL de connexion

Pour commencer à travailler après avoir installé IBM Security Key Lifecycle Manager, procurez-vous l'URL de connexion ainsi que l'ID utilisateur et le mot de passe initiaux de l'administrateur IBM Security Key Lifecycle Manager.

URL de connexion pour IBM Security Key Lifecycle Manager

Utilisez l'URL de connexion pour accéder à l'interface Web d'IBM Security Key Lifecycle Manager. L'URL de connexion à la console d'administration d'IBM Security Key Lifecycle Manager est la suivante :

`https://adresse_IP:port/ibm/SKLM/login.jsp`

La valeur d'*adresse-ip* correspond à une adresse IP ou DNS du serveur IBM Security Key Lifecycle Manager.

La valeur de *port* est le numéro du port sur lequel serveur IBM Security Key Lifecycle Manager écoute les demandes.

Par défaut, le serveur IBM Security Key Lifecycle Manager écoute le port non sécurisé (HTTP) 80 et le port sécurisé (HTTPS) 443 pour la communication. Pendant l'installation d'IBM Security Key Lifecycle Manager, vous pouvez modifier ces ports par défaut. Si vous utilisez le port par défaut pour HTTP ou HTTPS, le port est une partie optionnelle de l'URL. Exemple :

`https://adresse_IP/ibm/SKLM/login.jsp`

N'utilisez pas de valeur de port supérieure à 65520.

Sur les systèmes Windows, les informations équivalentes sont accessibles dans l'écran Démarrer :

1. Sur le bureau, placez le curseur de la souris dans l'angle inférieur gauche de l'écran, et cliquez lorsque la vignette de l'écran de démarrage apparaît.
2. Cliquez sur la flèche vers le bas dans le coin inférieur gauche de l'écran **Démarrer**.
3. Cliquez sur **IBM Security Key Lifecycle Manager** > **Lancement d'IBM Security Key Lifecycle Manager Application**.

URL de connexion abrégée pour IBM Security Key Lifecycle Manager

IBM Security Key Lifecycle Manager comporte une URL de connexion abrégée si bien que vous pouvez facilement vous en souvenir.

URL de connexion abrégée pour accéder à IBM Security Key Lifecycle Manager lorsque le port standard par défaut 80 (HTTP) et le port 443 (HTTPS) sont utilisés :

`https://adresse_IP/`

URL de connexion abrégée pour accéder à IBM Security Key Lifecycle Manager lorsque vous utilisez des ports personnalisés, au lieu des ports par défaut standard 80 et 443 :

`https://adresse_IP:port/`

URL de connexion pour WebSphere Application Server

L'URL de connexion à la console d'administration d'WebSphere Application Server :

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

La valeur d'*adresse-ip* correspond à une adresse IP ou DNS du WebSphere Application Server.

La valeur de *port* est le numéro du port sur lequel WebSphere Application Server écoute les demandes.

Le port par défaut affiché sur le panneau d'informations de WebSphere Application Server est 9093. Vous pouvez modifier le port par défaut lors de l'installation d'IBM Security Key Lifecycle Manager. Lors d'une migration ou si le port par défaut est en conflit avec un autre port, WebSphere Application Server sélectionne automatiquement un autre port libre.

Sur les systèmes Windows, ce numéro de port est repris dans le lien du menu Démarrer qui permet de se connecter à WebSphere Application Server.

Cliquez sur **IBM WebSphere** > **Console d'administration**.

Pour plus d'informations sur l'ID et le mot de passe de l'administrateur IBM Security Key Lifecycle Manager d'origine, voir ID utilisateur et mots de passe de l'administrateur.

Services, ports et processus

Après l'installation du serveur IBM Security Key Lifecycle Manager, vérifiez que les services, les ports et les processus requis sont bien lancés.

Windows

Services

Composant	Nom du service
WebSphere Application Server	`IBM WebSphere Application Server V9.0 - SKLM301Server`
Db2	`DB2SKLMV301 - SKLMDB31`

Ports Les ports suivants doivent être ouverts pour la communication et ne pas être utilisés par d'autres processus.

Description	Numéro de port
Port du gestionnaire FCM (Fast Communication Manager). Vous ne pouvez pas configurer ce port. Sa valeur est fixe. IBM Security Key Lifecycle Manager a besoin de ce port pour l'installation de Db2.	60050
Port HTTPS par défaut permettant d'accéder aux services REST et à l'interface graphique d'IBM Security Key Lifecycle Manager. Vous pouvez configurer ce port au moment de l'installation d'IBM Security Key Lifecycle Manager.	443
Port HTTP par défaut permettant d'accéder à l'interface graphique d'IBM Security Key Lifecycle Manager. Vous pouvez configurer ce port au moment de l'installation d'IBM Security Key Lifecycle Manager.	80
Port HTTPS par défaut permettant d'accéder à WebSphere Integrated Solutions Console. Vous pouvez configurer ce port au moment de l'installation d'IBM Security Key Lifecycle Manager.	9083
Port par défaut de Db2. Vous pouvez configurer ce port au moment de l'installation d'IBM Security Key Lifecycle Manager. Il peut s'agir d'un autre numéro de port, selon les paramètres d'installation. Il y a d'autres ports associés au numéro de port par défaut.	50050
Port SSL par défaut pour la phase d'installation, à l'écoute des messages KMIP.	5696
Port SSL pour les messages d'unité.	441
Port TCP pour les messages d'unité.	3801
L'installation de WebSphere Application Server requiert ces ports pour les différents services qu'il fournit.	9080 - 9099
Ports de réplication configurés par l'utilisateur dans le fichier de configuration de la réplication pour le serveur principal et les serveurs clones. Si un pare-feu est utilisé entre le serveur principal et les serveurs clones, il doit être configuré pour laisser passer Internet Control Message Protocol (ICMP).	-
Port par défaut de l'agent IBM Security Key Lifecycle Manager.	60015

Processus

Nom	Processus
IBM Security Key Lifecycle Manager	`WASService.exe` et `java.exe`
Db2	`db2fmp64.exe` et `db2syscs.exe`

Linux

Ports Les ports suivants doivent être ouverts pour la communication et ne pas être utilisés par d'autres processus.

Description	Numéro de port
Port du gestionnaire FCM (Fast Communication Manager). Vous ne pouvez pas configurer ce port. Sa valeur est fixe. IBM Security Key Lifecycle Manager a besoin de ce port pour l'installation de Db2.	60050
Port HTTPS par défaut permettant d'accéder aux services REST et à l'interface graphique d'IBM Security Key Lifecycle Manager. Vous pouvez configurer ce port au moment de l'installation d'IBM Security Key Lifecycle Manager.	443
Port HTTP par défaut permettant d'accéder à l'interface graphique d'IBM Security Key Lifecycle Manager. Vous pouvez configurer ce port au moment de l'installation d'IBM Security Key Lifecycle Manager.	80
Port HTTPS par défaut permettant d'accéder à WebSphere Integrated Solutions Console. Vous pouvez configurer ce port au moment de l'installation d'IBM Security Key Lifecycle Manager.	9083
Port par défaut de Db2. Vous pouvez configurer ce port au moment de l'installation d'IBM Security Key Lifecycle Manager. Il peut s'agir d'un autre numéro de port, selon les paramètres d'installation. Il y a d'autres ports associés au numéro de port par défaut.	50050
Port SSL par défaut pour la phase d'installation, à l'écoute des messages KMIP.	5696
Port SSL pour les messages d'unité.	441
Port TCP pour les messages d'unité.	3801
L'installation de WebSphere Application Server requiert ces ports pour les différents services qu'il fournit.	9080 - 9099
Ports de réplication configurés par l'utilisateur dans le fichier de configuration de la réplication pour le serveur principal et les serveurs clones. Si un pare-feu est utilisé entre le serveur principal et les serveurs clones, il doit être configuré pour laisser passer Internet Control Message Protocol (ICMP).	
Port par défaut de l'agent IBM Security Key Lifecycle Manager.	60015

Processus

Composant	Processus
IBM Security Key Lifecycle Manager	WebSphere Application Server et Java
Db2	`db2fmp64` et `db2syscs`

Sécurité post-installation

Après avoir installé IBM Security Key Lifecycle Manager, vous devez prendre plusieurs mesures pour faire reconnaître le certificat par votre navigateur et protéger les informations sensibles telles que les ID utilisateur et les mots de passe.

Spécification d'un certificat pour l'accès depuis un navigateur

Tous les navigateurs déclenchent une erreur relative au certificat, lequel doit être remplacé pour vous permettre d'accéder à WebSphere Application Server.

Pourquoi et quand exécuter cette tâche

L'erreur se produit parce que le propriétaire du certificat interne ne figure pas dans la liste des autorités signataires de confiance. Installez le certificat dans chaque navigateur que vous prévoyez d'utiliser pour accéder à IBM Security Key Lifecycle Manager. Vous pouvez utiliser l'interface utilisateur WebSphere Application Server pour remplacer le certificat.

Pour configurer le certificat, procédez comme suit :

Procédure

1. A l'aide de l'ID utilisateur WASAdmin, connectez-vous au serveur IBM Security Key Lifecycle Manager.
2. Sous l'onglet Sécurité, cliquez sur **Certificat SSL et gestion des clés**.
3. Sur la page Certificat SSL et gestion des clés, cliquez sur **Gérer les configurations de sécurité des noeuds finaux -> server1**. Il peut être nécessaire de cliquer sur **SKLMCell > noeuds > SKLMNode > serveurs > serveur1** pour développer l'arborescence de la topologie locale et situer serveur1 dans la branche sortante.
4. Pour définir la configuration SSL spécifique de ce noeud final, cliquez sur **Gérer les certificats**.
5. *Extrayez* le certificat.

   Le navigateur n'a besoin que du certificat. L'extraction récupère le certificat (la clé publique) et le stocke dans un fichier. N'exportez pas le certificat, car cette opération inclut à la fois la clé publique et la clé privée.
6. Importez le certificat dans votre navigateur.
   - Firefox
     a. Cliquez sur **Outils > Options > Avancé > Chiffrement**.
     b. Sélectionnez **Afficher les certificats > Importer**.
     c. Naviguez jusqu'au répertoire où se trouve le certificat à importer. Sélectionnez le certificat et cliquez sur **Ouvrir**.
     d. Dans la boîte de dialogue Gestionnaire de certificats, sélectionnez le certificat importé et cliquez sur **Modifier**.
     e. Dans la boîte de dialogue Edition des paramètres de confiance de l'autorité de certification (CA), sélectionnez **Faire confiance à l'authenticité de ce certificat** et cliquez sur **OK**.
     f. Dans la boîte de dialogue Gestionnaire de certificats, cliquez sur **OK**.
     g. Dans la boîte de dialogue Options, cliquez sur **OK**.
   - Internet Explorer
     a. Sélectionnez **Outils > Options Internet**.
     b. Sélectionnez l'onglet **Contenu** et cliquez sur le bouton **Certificats**.

c. Sélectionnez l'onglet **Autorités principales de confiance** et cliquez sur le bouton **Importer**.
d. Dans la fenêtre Assistant Importation de certificat, cliquez sur **Suivant**.
e. Localisez le certificat et cliquez sur **Suivant**.
f. Tapez le mot de passe du certificat et cliquez sur **Suivant**.
g. Effectuez les étapes restantes de l'assistant.
h. Lisez l'avertissement de sécurité qui s'affiche. Si vous êtes d'accord, cliquez sur **Oui**.

7. Dans la zone d'adresse du navigateur, entrez l'URL complète d'accès au serveur IBM Security Key Lifecycle Manager. Appuyez sur **Entrée**.

Changement du mot de passe des magasins de clés de WebSphere Application Server

Les certificats SSL du navigateur sont stockés dans les magasins de clés de WebSphere Application Server. Dans WebSphere Application Server, ces magasins de clés ont des mots de passe initialement connus de tous, qui doivent donc être changés.

Pourquoi et quand exécuter cette tâche

Lorsque vous installez le serveur d'applications, chaque serveur crée un magasin de clés (keystore) et un fichier de clés certifiées (truststore) pour sa configuration SSL par défaut, l'un et l'autre étant protégés par le même mot de passe par défaut, `WebAS`.

Procédure

1. Changez le mot de passe à l'aide de l'interface graphique :
   a. A l'aide de l'ID utilisateur WASAdmin, connectez-vous au WebSphere Integrated Solutions Console.
      `https://localhost:9083/ibm/console/logon.jsp`
   b. Sous l'onglet Sécurité, cliquez sur **Certificat SSL et gestion des clés**.
   c. Sur la page Certificat SSL et gestion des clés, cliquez sur **Magasins de clés et certificats -** > **NodeDefaultKeyStore**.
   d. Changez le mot de passe du magasin de clés.
   e. Sur la page Certificat SSL et gestion des clés, cliquez sur **Magasins de clés et certificats -** > **NodeDefaultTrustStore**.
   f. Changez le mot de passe du fichier de clés certifiées (truststore).
2. Sauvegardez le mot de passe dans un endroit sûr.

Sécurité de WebSphere Application Server

Vous devez prendre plusieurs mesures pour garantir la sécurité des informations sensibles dans WebSphere Application Server.

Le support technique peut déterminer qu'il est nécessaire d'activer le traçage pour déboguer un problème dans une fonction exécutée par la commande **WASService.exe**. L'activation du traçage de cette fonction a pour effet d'écrire des informations potentiellement sensibles dans le fichier `WASService.Trace`, dans le répertoire racine de Windows. Utilisez les mesures de protection appropriées à votre site pour protéger le fichier `WASService.Trace`.

Soyez également prudent lorsque vous exécutez la commande **stopServer**. N'inscrivez pas le mot de passe directement sur la ligne de commande. A la place, entrez le nom d'utilisateur et le mot de passe de l'administrateur de WebSphere Application Server lorsque vous y êtes invité.

Par exemple, pour arrêter tous les processus liés à *REP_BASE_WAS*, tapez :

```
stopServer server1
```

Entrez le nom d'utilisateur et le mot de passe lorsqu'ils vous sont demandés.

Evitez d'inclure l'ID utilisateur et le mot de passe dans la commande. Par exemple, ne tapez pas :

Windows

```
stopServer.bat server1 -username wasadmin -password mypwd
```

Linux ou AIX

```
./stopServer.sh server1  -username wasadmin -password mypwd
```

L'exécution postérieure de la commande **ps -aef** pour afficher des informations sur le processus actif peut faire apparaître le mot de passe de WebSphere Application Server.

Sauvegarde critique

Vous devez procéder à la sauvegarde des données critiques pour référence.

Pour sauvegarder les données, exécutez les tâches suivantes :

1. Sauvegardez les dossiers suivants et veillez à les stocker à un emplacement sécurisé :
   - *<WAS_HOME>*\configuration
     Exemple : C:\Program Files\IBM\WebSphere\AppServer\configuration
   - *<WAS_HOME>*\products
     Exemple : C:\Program Files\IBM\WebSphere\AppServer\products
2. Retirez les fichiers *.tss du dossier *<WAS_HOME>*\configuration.

Activation des services automatiques

Le processus d'installation d'IBM Security Key Lifecycle Manager démarre les services Db2 et WebSphere Application Server requis par IBM Security Key Lifecycle Manager. Le processus d'installation configure également ces services pour qu'ils démarrent automatiquement. Le démarrage automatique des services peut toutefois entraîner des erreurs, auquel cas vous devez les corriger.

Sous Windows

Sous Windows, vous devez utiliser la console des services Windows pour configurer les services afin qu'ils démarrent automatiquement.

Recherchez les services dans la liste ci-dessous. Pour chaque service de la liste, ouvrez la boîte de dialogue Propriétés du service et vérifiez que la zone **Type de démarrage** est définie sur Automatique. Si la zone **Etat du service** est définie sur la valeur Bloqué, cliquez sur **Démarrer** pour démarrer le service.

Db2 - *db2 copy name - SKLM_INSTANCE_OWNER*
Par exemple, **DB2 - DBSKLMV301 - SKLMDB31**

Db2 Governor (*nom de copie db2***)**
Par exemple, **Db2 Governor (DB2SKLMV301)**

Db2 License Server (*nom de copie db2***)**
Par exemple, **Db2 License Server (DB2SKLMV301)**

Db2 Management Service (*nom de copie db2***)**
Par exemple, **Db2 Management Service (DB2SKLMV301)**

Db2 Remote Command Server (*nom de copie db2***)**
Par exemple, **Db2 Remote Command Server (DB2SKLMV301)**

DB2DAS - *entrée_DB2DAS*
Par exemple, **DB2DAS - DB2DAS00**

Remarque : Désactivez Db2 Administration Server (DAS) uniquement si le service DAS est hébergé dans un service Windows.

WAS Service- IBM Security Key Lifecycle Manager
Par exemple, `IBM WebSphere Application Server V9.0 - SKLM301Server`

Systèmes Linux

Sur un système Linux, entrez les commandes suivantes pour configurer le démarrage automatique du propriétaire de l'instance Db2 d'IBM Security Key Lifecycle Manager :

```
<rép_base_BDD>/sqllib/db2profile
DB_HOME/instance/db2iauto -on sklmdb31
```

où `sklmdb31` correspond à l'ID utilisateur par défaut du propriétaire de l'instance. Si vous avez modifié cette valeur lors de l'installation, utilisez le nouvel ID utilisateur.

L'installation d'IBM Security Key Lifecycle Manager sur des systèmes Linux ajoute une commande de démarrage de WebSphere Application Server au fichier `/etc/inittab`. Sur les systèmes Linux, le programme d'installation crée le fichier `SecurityKeyLifecycleManager_was.init` dans `/etc/init.d`. Vous pouvez ajouter une commande similaire dans le fichier `/etc/initttab` :

```
slp:2345:wait:/bin/sleep 60
tt:23456789:wait:RACINE_WAS/bin/startServer.sh server1
```

Systèmes AIX

Sur un système AIX, entrez les commandes suivantes pour configurer le démarrage automatique du propriétaire de l'instance Db2 d'IBM Security Key Lifecycle Manager :

```
<rép_base_BDD>/sqllib/db2profile
DB_HOME/instance/db2iauto -on sklmdb31
```

où `sklmdb31` correspond à l'ID utilisateur par défaut du propriétaire de l'instance. Si vous avez modifié l'ID lors de l'installation, utilisez le nouvel ID.

L'installation d'IBM Security Key Lifecycle Manager sur des systèmes AIX ajoute des commandes de démarrage d'WebSphere Application Server au fichier `/etc/inittab`. Vous pouvez éditer ces commandes dans le fichier `/etc/inittab` :

```
sl:2345:wait:/bin/sleep 60
tt:23456:wait:RACINE_WAS/bin/startServer.sh server1
```

Pour configurer WebSphere Application Server pour qu'il démarre automatiquement, suivez les étapes décrites dans la section relative à la création d'une définition de service SMF, dans le document *IBM WebSphere Application Server V6.1 on the Solaris 10 Operating System* - Redbooks. Ce document est disponible à l'adresse suivante : http://www.redbooks.ibm.com/abstracts/sg247584.html.

Adaptez les informations figurant sur la page Web avec des valeurs dépendant de votre installation d'IBM Security Key Lifecycle Manager. Par exemple, utilisez les répertoires de votre système dans le script :

```
WAS_DIR="//opt/IBM/WebSphere/AppServer/profiles/KLMProfile"
```

Sur certains systèmes, il peut être nécessaire d'augmenter la valeur du délai d'attente de 60 à 300 dans le fichier manifeste.

Définition du délai d'expiration de la session

La session de l'interface utilisateur IBM Security Key Lifecycle Manager peut être configurée pour expirer au bout de 30 minutes (par défaut) d'inactivité ou pour rester active indéfiniment.

Procédure

1. Vous pouvez définir l'intervalle de délai d'attente de session à l'aide de l'interface graphique :
   a. A l'aide de l'ID utilisateur `WASAdmin`, connectez-vous au WebSphere Integrated Solutions Console.
      ```
      https://localhost:9083/ibm/console/logon.jsp
      ```
   b. Dans l'onglet **Applications**, cliquez sur **Types d'application** > **Applications d'entreprise WebSphere**.
   c. Sur la page Applications d'entreprise, cliquez sur **sklm_kms**.
   d. Dans la section Propriétés du module Web, cliquez sur **Gestion de session**.
   e. Dans la section Propriétés générales, sélectionnez **Remplacer la gestion de session** .
   f. Dans la section Délai d'attente de session, sélectionnez **Aucun délai d'expiration** pour conserver la session sans délai d'expiration.
   g. Pour définir le délai d'inactivité en minutes, sélectionnez **Définir le délai d'expiration** et spécifiez la valeur du délai d'inactivité souhaité.
2. Cliquez sur **Appliquer**.
3. Cliquez sur **OK**.

Définition du délai maximal imparti aux transactions

La valeur du délai d'expiration total de transaction est définie à 600 secondes par défaut. Dans IBM Security Key Lifecycle Manager, certaines opérations à exécution longue peuvent nécessiter plus de temps et échouer.

Pourquoi et quand exécuter cette tâche

Dans IBM Security Key Lifecycle Manager, les opérations à exécution longue peuvent manquer de temps et échouer avec un message d'erreur tel que le suivant :

```
[10/21/08 14:28:41:693 CDT] 00000020 TimeoutManage I
WTRN0006W: Transaction 00000110001 en dépassement de délai après xxx secondes.
```

Pour configurer un délai plus long, procédez comme suit :

Procédure

1. Arrêtez le serveur.
   - Systèmes Windows :

     Dans le répertoire *RACINE_WAS*\bin, tapez :

     ```
     stopServer.bat server1
     ```
   - Systèmes AIX et Linux :

     Dans le répertoire *RACINE_WAS*/bin, tapez :

     ```
     ./stopServer.sh server1
     ```
2. Editez le fichier :

   ```
   ..\profiles\KLMProfile\config\cells\SKLMCell\nodes\SKLMNode\
     servers\server1\server.xml
   ```
3. Changez le paramètre **propogatedOrBMTTranLifetimeTimeout** pour une valeur plus grande.
4. Enregistrez le fichier.
5. Démarrez le serveur.
   - Systèmes Windows :

     Dans le répertoire *RACINE_WAS*\bin, tapez :

     ```
     startServer.bat server1
     ```
   - Systèmes AIX et Linux :

     Dans le répertoire *RACINE_WAS*/bin, tapez :

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

Changement de nom d'hôte du système IBM Security Key Lifecycle Manager

Vous devez modifier le nom d'hôte de WebSphere Application Server et de Db2 lorsque le nom d'hôte du système d'IBM Security Key Lifecycle Manager est modifié.

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», à la page 78.

Arrêt du serveur Db2

Certaines procédures opérationnelles peuvent vous obliger à arrêter le serveur serveur Db2. Vous devez arrêter WebSphere Application Server avant d'arrêter le serveur 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 AIX ou Linux, ou connectez-vous en tant qu'administrateur local sur les systèmes Windows.
2. Exécutez la commande suivante pour arrêter WebSphere Application Server :

   Windows

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

   AIX ou Linux

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

3. Exécutez la commande suivante pour arrêter le serveur Db2.

   Windows

   ```
   set DB2INSTANCE=sklmdb31
   db2stop
   ```

   AIX ou Linux

   ```
   su - sklmdb31
   db2stop
   ```

Configuration de SSL

Après l'installation d'IBM Security Key Lifecycle Manager, vous pouvez configurer une communication sécurisée via SSL.

Pourquoi et quand exécuter cette tâche

Cette option est contrôlée par la propriété **config.keystore.ssl.certalias** dans le fichier *SKLM_DATA*/config/SKLMConfig.properties.

Si des ports de transport sont spécifiés, cet alias pointe vers un certificat existant qui est utilisé pour l'authentification SSL dans la communication sécurisée entre une unité et le serveur IBM Security Key Lifecycle Manager.

Si vous faites migrer des données d'Encryption Key Manager, tous les certificats du fichier de clés certifiées (truststore) TransportListener sont importés dans le magasin de clés d'IBM Security Key Lifecycle Manager.

Un certificat provenant du *magasin de clés* TransportListener est désigné comme certificat SSL pour IBM Security Key Lifecycle Manager. La propriété **config.keystore.ssl.certalias** est mise à jour avec l'alias de ce certificat.

Pour configurer SSL en vue de sécuriser la communication, suivez ces étapes :

Procédure

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

     Connectez-vous à l'interface graphique. Vous pouvez sélectionner l'un ou l'autre des chemins suivants :
     - Cliquez sur **IBM Security Key Lifecycle Manager > Configuration > SSL/KMIP**.
     - **IBM Security Key Lifecycle Manager > Configuration avancée > Certificats de serveur**.
   - 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 le certificat utilisé pour la communication sécurisée par SSL.
   - Interface graphique :

     Spécifiez un certificat comme certificat SSL :
     - Sur la page SSL/KMIP pour le service de clés, sélectionnez l'option d'utilisation d'un certificat existant du magasin de clés comme certificat SSL. Sélectionnez un certificat et cliquez sur **OK**.
     - Vous pouvez aussi sélectionner un certificat existant et cliquez sur **Modifier** sur la page Administrer les certificats de serveur. Spécifiez que le certificat est celui qui est actuellement utilisé et cliquez sur **Modifier un certificat**.
   - Interface de ligne de commande :

– Pour déterminer la valeur de la propriété, utilisez la commande **tklmConfigGetEntry**. Vous pouvez, par exemple, souhaiter vérifier qu'un certificat ayant migré est bien désigné comme le certificat SSL.

  Cette commande au format Jython permet d'obtenir la valeur actuelle de la propriété **config.keystore.ssl.certalias**.

  ```
  wsadmin>print AdminTask.tklmConfigGetEntry
   ('[-name config.keystore.ssl.certalias]')
  ```

– Pour changer la valeur de la propriété, utilisez la commande **tklmConfigUpdateEntry** et spécifiez le certificat utilisé par le serveur IBM Security Key Lifecycle Manager.

Par exemple, cette commande au format Jython permet de changer la valeur de la propriété **config.keystore.ssl.certalias**.

```
print AdminTask.tklmConfigUpdateEntry
  ('[-name config.keystore.ssl.certalias
   -value moncertif]')
```

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

     Sur la page intitulée L'opération a abouti, sous Etapes suivantes, cliquez sur une tâche associée à effectuer.
   - Interface de ligne de commande :

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

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 *RACINE_WAS*/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.

Vérification de l'installation

Après avoir effectué l'installation, vérifiez qu'IBM Security Key Lifecycle Manager a été correctement installé.

1. Démarrez et arrêtez le serveur. Pour plus de détails, voir «Serveur IBM Security Key Lifecycle Manager - Redémarrage», à la page 83.
2. Ouvrez IBM Security Key Lifecycle Manager dans un navigateur Web.
   a. Utilisez l'URL de connexion pour accéder à l'interface Web d'IBM Security Key Lifecycle Manager.

      https://*adresse-ip*:*port*/ibm/SKLM/login.jsp

La valeur d'*adresse-ip* correspond à une adresse IP ou DNS du serveur IBM Security Key Lifecycle Manager.

La valeur de *port* est le numéro du port sur lequel serveur IBM Security Key Lifecycle Manager écoute les demandes.

Par défaut, le serveur IBM Security Key Lifecycle Manager écoute le port non sécurisé (HTTP) 80 et le port sécurisé (HTTPS) 443 pour la communication. Pendant l'installation d'IBM Security Key Lifecycle Manager, vous pouvez modifier ces ports par défaut. Si vous utilisez le port par défaut pour HTTP ou HTTPS, le port est une partie optionnelle de l'URL. Par exemple :

```
https://adresse_IP/ibm/SKLM/login.jsp
```

IBM Security Key Lifecycle Manager comporte une URL de connexion abrégée si bien que vous pouvez facilement vous en souvenir. L'URL de connexion abrégée pour accéder à IBM Security Key Lifecycle Manager lorsque des ports par défaut sont utilisés est :

```
https://adresse_IP/
```

Sur les systèmes Windows, les informations équivalentes sont accessibles dans l'écran Démarrer :

1) Sur le bureau, placez le curseur de la souris dans l'angle inférieur gauche de l'écran, et cliquez lorsque la vignette de l'écran de démarrage apparaît.
2) Cliquez sur la flèche vers le bas dans le coin inférieur gauche de l'écran **Démarrer**.
3) Cliquez sur **IBM Security Key Lifecycle Manager 3.0.1** > **Lancement d'IBM Security Key Lifecycle Manager**.

b. Connectez-vous avec vos données d'identification et vérifiez que la page d'accueil d'IBM Security Key Lifecycle Manager s'affiche.

3. Utilisez l'interface de ligne de commande pour répertorier le groupe de commandes d'IBM Security Key Lifecycle Manager. Par exemple, à partir de *RACINE_WAS*/bin, entrez :

```
./wsadmin.sh -username <sklmadmin id> -password <sklmadmin passwd> -lang jython
```

Lorsque l'outil **wsadmin** vous y invite, entrez la commande suivante :

```
wsadmin>print AdminTask.help("-commandGroups")
```

Les groupes de commandes IBM Security Key Lifecycle Manager s'affichent. Par exemple, la liste contient les commandes de sauvegarde et d'autres groupes de commandes :

```
TKLMBackupCommands - Commandes de sauvegarde/restauration IBM Security Key Lifecycle Manager
```

Activation des paramètres de scriptage pour Internet Explorer versions 9.0, 10 et 11

Vérifiez que les paramètres de scriptage sont activés pour Internet Explorer version 9.0, 10 et 11.

Pourquoi et quand exécuter cette tâche

Si certains paramètres de scriptage ne sont pas activés pour Internet Explorer, versions 9.0, 10 et 11.0, vous risquez de ne pas pouvoir créer d'utilisateur IBM Security Key Lifecycle Manager.

Assurez-vous que les options suivantes du navigateur sont activées :

- Autoriser les mises à jour de la barre d'état via des scripts
- Active Scripting (Autoriser les scripts actifs)
- Script des applets Java

Procédure

1. Ouvrez le navigateur et cliquez sur **Outils** > **Options Internet** > **Sécurité**.
2. Faites défiler la liste des paramètres de sécurité jusqu'à atteindre les options de la catégorie Script et vérifiez que les options suivantes sont activées :
   - Autoriser les mises à jour de la barre d'état via des scripts
   - Active Scripting (Autoriser les scripts actifs)
   - Script des applets Java
3. Cliquez sur **OK**.

Serveur IBM Security Key Lifecycle Manager - Redémarrage

Une fois le serveur redémarré, ce dernier 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.

Récupération après un échec de migration

Pendant le processus de migration en ligne pour les versions antérieures d'Encryption Key Manager ou d'IBM Security Key Lifecycle Manager vers la version 3.0.1, la migration peut échouer. Vous pouvez exécuter les étapes de reprise de la migration en cas d'échec de la migration.

Récupération d'Encryption Key Manager après l'échec de la migration

Pendant le processus de migration en ligne pour Encryption Key Manager, vous risquez de rencontrer un échec de migration. Si l'échec de migration se produit, exécutez les étapes de reprise de la migration.

Le processus d'installation exécute la phase d'installation d'IBM Security Key Lifecycle Manager, puis il démarre un processus de migration pour faire migrer les données d'Encryption Key Manager vers IBM Security Key Lifecycle Manager.

- Lorsque le processus de migration démarre, une erreur peut se produire pendant que le programme d'installation valide les valeurs dans le fichier de propriétés d'Encryption Key Manager dans les conditions suivantes :
  - Le fichier de propriétés ne peut pas être lu en raison d'autorisations d'accès inadéquates.
  - Une propriété obligatoire n'existe pas ou ne possède pas de valeur.
  - La valeur d'une propriété est syntaxiquement incorrecte.
  - Le fichier vers lequel pointe une propriété n'existe pas ou ne peut pas être lu car les autorisations d'accès sont inadéquates.
- Une erreur peut se produire plus tard, alors que la migration est déjà bien avancée. Dans ce cas, vérifiez le fichier journal des erreurs :

  Windows

  `<REP_DONNEES_IM>\logs\sklmLogs\migration.log`

  AIX et Linux

  `<REP_DONNEES_IM>/logs/sklmLogs/migration.log`

En cas d'échec de la migration d'Encryption Key Manager, si vous choisissez de terminer le reste du processus de migration, vous pouvez démarrer un script autonome de reprise de la migration, mais à condition que vous n'ayez pas encore effectué de mise à jour ni apporté de modifications dans la configuration du serveur IBM Security Key Lifecycle Manager. Pour plus d'informations sur la façon d'exécuter le script, consultez Script de reprise de la migration d'Encryption Key Manager.

Si la migration d'Encryption Key Manager échoue et qu'aucune donnée n'a été migrée, supprimez le fichier `tklmKeystore.jceks` pour démarrer à nouveau le processus de migration. Le fichier est disponible dans le répertoire `<WAS_HOME>\products\sklm\keystore`.

Pour la définition de <*REP_DONNEES_IM*> et <*WAS_HOME*>, voir «Définitions relatives à un répertoire *HOME* et d'autres variables de répertoire», à la page 5.

Script de reprise de la migration d'Encryption Key Manager

Vous pouvez démarrer un script de récupération pour Encryption Key Manager si vous ne faites pas modifications ou si vous ne configurez pas autrement le serveur IBM Security Key Lifecycle Manager avant d'exécuter le script. Par exemple, l'espace disque disponible sur le système ne doit pas changer significativement.

Le script de migration se trouve dans le répertoire *<SKLM_INSTALL_HOME>*\migration\bin. Voici les commandes permettant d'exécuter le script :

Systèmes Windows :

```
cd <RACINE_INSTALL_SKLM>\migration\bin
.\migrate.bat motdepasse_propriétaire_instance_sklm
```

Systèmes Linux et AIX :

```
cd <RACINE_INSTALL_SKLM>/migration/bin
./migrate.sh motdepasse_propriétaire_instance_sklm
```

Sur les systèmes Linux ou AIX, veillez à être connecté en tant qu'utilisateur root avant d'exécuter migrate.sh.

Où le paramètre *motdepasse_propriétaire_instance_sklm* correspond au mot de passe du propriétaire de l'instance Db2 du serveur IBM Security Key Lifecycle Manager.

Le paramètre *<SKLM_INSTALL_HOME>* est utilisé uniquement sous Windows et doit être entouré de guillemets.

Systèmes Windows :

```
cd "C:\Program Files\IBM\SKLMV301\migration\bin"
.\bin\migrate.bat motdepasse
echo %ERRORLEVEL%
```

Remarque :

- Omettez le mot de passe si vous ne voulez pas qu'il apparaisse en clair sur la ligne de commande. Il vous sera demandé par le script de récupération. Il ne sera pas affiché en clair. Par exemple :

  ```
  migrate.bat
  echo $?
  ```

- Durant son exécution, le script de reprise de la migration crée un fichier migration.log.
- Si migrate.bat ou migrate.sh n'est pas disponible :
  1. Copiez migrate.bat.template ou migrate.sh.template vers migrate.bat ou migrate.sh.
  2. Spécifiez les paramètres requis.
  3. Exécutez le fichier.

Systèmes Linux et AIX :

```
cd /opt/IBM/SKLMV301/migration/bin
./bin/migrate.sh motdepasse
echo $?
```

Sur les systèmes Linux ou AIX, veillez à être connecté en tant qu'utilisateur root avant d'exécuter migrate.sh.

Récupération après un échec de migration pour IBM Security Key Lifecycle Manager

Les scénarios d'erreur suivants peuvent se produire pendant la migration d'IBM Security Key Lifecycle Manager :

- Au démarrage de la migration, un message d'erreur peut être émis si une ou plusieurs des conditions suivantes sont rencontrées :
  - Des autorisations d'accès inadéquates empêchent la lecture des fichiers requis, ou bien des propriétés ou des fichiers sont manquants.
  - D'autres applications utilisent un fichier requis.
  - Durant la migration du serveur Db2, le WebSphere Application Server est arrêté d'une manière inattendue.
- Une erreur peut survenir plus tard, lorsque la migration est terminée ou qu'elle est bien avancée.

  Le programme d'installation affiche un message d'erreur. Dans ce cas, vérifiez le fichier journal des erreurs :

  Systèmes Windows :
  <REP_DONNEES_IM>\logs\sklmLogs\migration.log

  Systèmes AIX et Linux :
  <REP_DONNEES_IM>/logs/sklmLogs/migration.log

  En cas d'échec répété du programme de migration, si vous choisissez de revenir à la version antérieure, effectuez les étapes suivantes pour une nouvelle version de Db2 :
  - Désinstallez la version antérieure d'IBM Security Key Lifecycle Manager. Sur les systèmes AIX ou Linux, accédez au répertoire de base du propriétaire d'instance, par exemple /home/SKLMDB301. Si le répertoire sqllib_v91 existe, supprimez-le.
  - Redémarrez l'ordinateur.
  - Réinstallez la version antérieure d'IBM Security Key Lifecycle Manager et restaurez la sauvegarde la plus récente. Appliquez le groupe de correctifs le plus récent.

Script de reprise de la migration d'IBM Security Key Lifecycle Manager

Vous pouvez démarrer un script de récupération pour IBM Security Key Lifecycle Manager si vous ne faites pas modifications ou si vous ne configurez pas autrement le serveur IBM Security Key Lifecycle Manager avant d'exécuter le script. Par exemple, l'espace disque disponible sur le système ne doit pas changer significativement.

L'utilitaire de migration crée un fichier migration.log dans le répertoire *<REP_DONNEES_IM>\logs\sklmLogs*.

Le script de migration se trouve dans le répertoire *<SKLM_INSTALL_HOME>*\migration. Avant d'exécuter le script de migration, veillez à ce que JAVA_HOME soit correctement défini. L'exemple suivant indique le chemin de JAVA_HOME :

Systèmes Windows
C:\Program Files\IBM\WebSphere\AppServer\java\jre

Systèmes Linux et AIX
/opt/IBM/WebSphere/AppServer/java/jre

Commandes d'exécution des scripts de migration

Systèmes Windows

```
cd <RACINE_INSTALL_SKLM>\migration
.\migrateToSKLM.bat
```

Par exemple :

```
cd "C:\Program Files\IBM\SKLMV27\migration"
.\migrateToSKLM.bat
```

Vous devez spécifier une valeur pour les paramètres de migration dans le fichier `migration.properties`, qui se trouve dans le répertoire `<SKLM_INSTALL_HOME>\migration`.

Systèmes Linux et AIX

Remarque : Sur les systèmes Linux ou AIX, veillez à être connecté en tant qu'utilisateur root avant d'exécuter **migrateToSKLM.sh**.

```
cd <RACINE_INSTALL_SKLM>/migration
./migrateToSKLM.sh
```

Par exemple :

```
cd /opt/IBM/SKLMV301/migration
./migrateToSKLM.sh
```

Vous devez spécifier une valeur pour les paramètres de migration dans le fichier `migration.properties`, qui se trouve dans le répertoire `<SKLM_INSTALL_HOME>/migration`.

Après avoir exécuté le script de reprise de la migration, redémarrez le serveur IBM Security Key Lifecycle Manager. Pour plus d'informations sur le mode de redémarrage du serveur, voir «Serveur IBM Security Key Lifecycle Manager - Redémarrage», à la page 83.

Pour la définition de *<REP_DONNEES_IM>* et *<SKLM_INSTALL_HOME>*, voir «Définitions relatives à un répertoire *HOME* et d'autres variables de répertoire», à la page 5.

Paramètres du fichier `migration.properties`

WAS_HOME
Répertoire dans lequel WebSphere Application Server for IBM Security Key Lifecycle Manager, Version 3.0.1 est installé.

TKLM_TIP_HOME
Ce paramètre permet de définir `<WAS_HOME>` pour les versions précédentes, telles que 2.5, 26 et 2.7.

WAS_ADMIN_ID
Nom d'utilisateur de l'administrateur WebSphere Application Server pour la version antérieure.

WAS_ADMIN_PASSWORD
Mot de passe pour le nom d'utilisateur de l'administrateur WebSphere Application Server.

SKLM_INSTALL_PATH
Répertoire dans lequel IBM Security Key Lifecycle Manager est installé.

SKLM_ADMIN_USER
Nom d'utilisateur de l'administrateur pour la version antérieure d'IBM Security Key Lifecycle Manager. Le nom d'utilisateur doit être `SKLMAdmin`.

SKLM_ADMIN_USER_PASSWORD
Mot de passe pour le nom d'utilisateur de l'administrateur IBM Security Key Lifecycle Manager.

MIG_LOG_PATH
Chemin d'accès où le fichier `migration.log` est stocké.

TKLM_VERSION
Numéro de version d'IBM Security Key Lifecycle Manager installé sur le système.

TKLM_DB_PWD
Mot de passe de l'administrateur Db2 pour IBM Security Key Lifecycle Manager.

KEYSTORE_PWD
ce paramètre n'est pas requis pour les versions 2.5, 2.6 et 2.7.

IM_INSTALL_DIR
Répertoire dans lequel IBM Installation Manager est installé.

Remarque : Toutes les valeurs sauf les mots de passe sont préremplies dans le fichier de propriétés. Ne modifiez aucune valeur, sauf pour les zones qui sont vides.

Fichier `migration.properties` exemple

```
WAS_HOME=C:\Program Files\IBM\WebSphere\AppServer_1
TKLM_TIP_HOME=C:\Program Files\IBM\WebSphere\AppServer
WAS_ADMIN_ID=wasadmin
WAS_ADMIN_PASSWORD=WAS@admin123
SKLM_INSTALL_PATH=C:\Program Files\IBM\SKLMV301
SKLM_ADMIN_USER=SKLMAdmin
SKLM_ADMIN_USER_PASSWORD=SKLM@admin123
MIG_LOG_PATH=C:\Program Files\IBM\SKLMV301\migration\migration.log
TKLM_VERSION=2.7.0.0
TKLM_DB_PWD=SKLM@db2
KEYSTORE_PWD=none
IM_INSTALL_DIR=C:\Program Files\IBM\Installation Manager\eclipse
```

Lancement automatique de Db2

Si la migration a échoué en cours de traitement et que, pour terminer les étapes restantes, vous l'avez reprise en exécutant le script de migration en mode récupération, vous devez configurer les services Db2 afin qu'ils démarrent automatiquement au démarrage de l'ordinateur.

Sous Windows

Sur un système Windows, effectuez les étapes suivantes pour configurer le démarrage automatique des services Db2 :

1. Cliquez sur **Démarrer** > **Panneau de configuration** > **Outils d'administration** > **Services**.
2. Cliquez avec le bouton droit de la souris sur le service **DB2 - DBSKLMV301 - SKLMDB31**, puis cliquez avec le bouton droit de la souris sur **Propriétés**.
3. Dans la boîte de dialogue Propriétés, sous l'onglet **Général**, sélectionnez **Automatique** pour le paramètre **Type de démarrage** et cliquez sur **Appliquer**.

4. Redémarrez le système pour vérifier que le serveur de base de données démarre automatiquement.

Systèmes AIX et Linux

Si vous avez activé `crontab` dans IBM Security Key Lifecycle Manager, tapez cette commande pour activer le démarrage automatique de Db2 :

```
. <rép_base_BDD>/sqllib/db2profile
DB_HOME/instance/db2iauto -on sklmdb31
```

où `sklmdb31` correspond à l'ID utilisateur par défaut du propriétaire de l'instance. Si vous avez modifié cette valeur lors de l'installation, utilisez le nouvel ID utilisateur.

Fichier de propriétés du statut de migration

L'utilitaire de migration du serveur IBM Security Key Lifecycle Manager tient à jour un fichier *<SKLM_INSTALL_HOME>*`\migration\migratestatus.properties` pour conserver une trace des tâches accomplies.

Si la migration échoue, le fichier de propriétés est conservé pour aider au débogage. L'utilitaire de migration utilise également ce fichier pour déterminer à quel stade reprendre un nouveau processus de migration. C'est également grâce à ce fichier qu'il peut déterminer que la migration a déjà été exécutée jusqu'à son terme et qu'elle a réussi, si vous la relancez accidentellement.

Désinstallation d'IBM Security Key Lifecycle Manager

Vous devez tenir compte de quelques facteurs pour désinstaller correctement IBM Security Key Lifecycle Manager.

- Le mode de désinstallation par défaut est identique à celui utilisé pour installer IBM Security Key Lifecycle Manager.
- La désinstallation d'IBM Security Key Lifecycle Manager ne désinstalle pas Db2 s'il a été installé avant l'installation d'IBM Security Key Lifecycle Manager. Cette tâche est une étape distincte et facultative. Pour plus d'informations, voir «Désinstallation de Db2», à la page 101.

  En outre, bien que la désinstallation d'IBM Security Key Lifecycle Manager dissocie l'instance de base de données Db2 de l'ID utilisateur servant au propriétaire de l'instance Db2 d'IBM Security Key Lifecycle Manager, la suppression de cet ID utilisateur constitue une étape distincte. Pour plus d'informations, voir «Suppression de l'ID utilisateur du propriétaire de l'instance Db2», à la page 104.

  Un échec de la désinstallation peut indiquer la nécessité de revenir à un état connu d'IBM Security Key Lifecycle Manager, voir «Réinstallation de la version antérieure en cas d'échecs répétés de la migration», à la page 100.
- Sur les systèmes Linux, lorsque vous désinstallez IBM Security Key Lifecycle Manager, l'utilisateur DB2, par exemple `sklmdb31`, n'est pas supprimé. Les utilisateurs créés par le programme d'installation d'IBM Security Key Lifecycle Manager ou les utilisateurs existants ne sont pas retirés par le programme de désinstallation. Si nécessaire, vous pouvez les retirer manuellement.

  Toutefois, `klmfcuser` est retiré au cours de la désinstallation d'IBM Security Key Lifecycle Manager.
- Pour une désinstallation en mode graphique, si WebSphere Application Server n'est pas arrêté avant la désinstallation d'IBM Security Key Lifecycle Manager, le message erroné suivant s'affiche.

  ```
  Des processus en cours d'exécution, susceptibles d'interférer avec l'opération
  en cours, ont été détectés. Arrêtez tous les processus WebSphere et apparentés
  avant de continuer.
  ```

  Cliquez sur **Revérifier l'état** pour passer à la tâche de désinstallation.

Désinstallation sur des systèmes Windows

Désinstallez IBM Security Key Lifecycle Manager et ses composants lorsque vous n'en avez plus besoin sur vos systèmes Windows.

Désinstallation en mode graphique

Désinstallez IBM Security Key Lifecycle Manager et ses composants lorsque vous n'en avez plus besoin sur vos systèmes Windows en mode graphique.

Procédure

1. Depuis l'invite de commande, accédez au répertoire `disk1` de votre module d'installation. Exemple : *chemin_téléchargement*`/disk1`.
2. Exécutez la commande suivante :

   ```
   uninstallSKLM.bat IM_INSTALL_LOCATION WAS_INSTALL_LOCATION SKLM_INSTALL_HOME
   WAS_ADMIN WAS_PASSWORD
   ```

IM_INSTALL_LOCATION - Répertoire d'Installation Manager pour IBM Security Key Lifecycle Manager.

WAS_INSTALL_LOCATION - Répertoire de WebSphere Application Server pour IBM Security Key Lifecycle Manager.

SKLM_INSTALL_HOME - Répertoire d'installation d'IBM Security Key Lifecycle Manager.

WAS_ADMIN - Nom d'utilisateur de WebSphere Application Server pour IBM Security Key Lifecycle Manager.

WAS_PASSWORD - Mot de passe correspondant au nom d'utilisateur WebSphere Application Server.

Par exemple :

```
uninstallSKLM.bat "C:\Program Files\IBM\Installation Manager"
"C:\Program Files\IBM\WebSphere\AppServer"
"C:\Program Files\IBM\SKLMV301" wasadmin WAS@admin123
```

3. Dans IBM Installation Manager, cliquez sur **Désinstaller**.
4. Sélectionnez les cases à cocher pour désinstaller IBM Security Key Lifecycle Manager, Db2 et WebSphere Application Server.

   Remarque : Si WebSphere Application Server n'est pas arrêté avant la désinstallation d'IBM Security Key Lifecycle Manager, le message d'erreur suivant s'affiche.

   ```
   Des processus en cours d'exécution, susceptibles d'interférer avec l'opération
   en cours, ont été détectés. Arrêtez tous les processus WebSphere et apparentés
   avant de continuer.
   ```

   Cliquez sur **Revérifier l'état** pour passer à la tâche de désinstallation.
5. Cliquez sur **Suivant**. Entrez l'ID utilisateur et le mot de passe d'administrateur de WebSphere Application Server.
6. Cliquez sur **Suivant**. La fenêtre Panneau Récapitulatif s'ouvre.
7. Vérifiez les progiciels à désinstaller et leurs répertoires d'installation.
8. Cliquez sur **Désinstaller**.

   Une fois IBM Security Key Lifecycle Manager désinstallé, si des services Db2 sont encore en cours d'exécution, désinstallez manuellement Db2 et ses composants. Pour plus d'informations sur la désinstallation de Db2, voir http://www-01.ibm.com/support/docview.wss?uid=swg21104569.

Que faire ensuite

Consultez le récapitulatif de désinstallation et les fichiers journaux dans `C:\ProgramData\IBM\InstallationManager\logs\sklmLogs\`.

Après avoir désinstallé IBM Security Key Lifecycle Manager, supprimez les répertoires `C:\Program Files\IBM\WebSphere` et `C:\Program Files\DB2SKLMV301`, le cas échéant.

Désinstallation en mode silencieux

Désinstallez IBM Security Key Lifecycle Manager et ses composants lorsque vous n'en avez plus besoin sur vos systèmes Windows en mode silencieux.

Procédure

1. Editez le fichier de réponses afin d'ajouter des mots de passe chiffrés aux éléments concernés du fichier. Les exemples de fichiers de réponses se trouvent dans le répertoire où se trouve votre module d'installation.

L'utilitaire IBM Installation Manager permet de créer des mots de passe chiffrés. Pour plus d'informations sur la façon de chiffrer le mot de passe, consultez Mot de passe chiffré pour les éléments du fichier de réponses.

2. Depuis l'invite de commande, accédez au répertoire `disk1` de votre module d'installation. Exemple : *chemin_téléchargement*`/disk1`.
3. Exécutez la commande suivante :

   ```
   silent_uninstallSKLM.bat IM_INSTALL_LOCATION WAS_INSTALL_LOCATION SKLM_INSTALL_HOME
   WAS_ADMIN WAS_PASSWORD
   ```

   IM_INSTALL_LOCATION - Répertoire d'Installation Manager pour IBM Security Key Lifecycle Manager.

   WAS_INSTALL_LOCATION - Répertoire de WebSphere Application Server pour IBM Security Key Lifecycle Manager.

   SKLM_INSTALL_HOME - Répertoire d'installation d'IBM Security Key Lifecycle Manager.

   WAS_ADMIN - Nom d'utilisateur de WebSphere Application Server pour IBM Security Key Lifecycle Manager.

   WAS_PASSWORD - Mot de passe correspondant au nom d'utilisateur WebSphere Application Server.

   Exemple :

   ```
   silent_uninstallSKLM.bat "C:\Program Files\IBM\Installation Manager"
   "C:\Program Files\IBM\WebSphere\AppServer"
   "C:\Program Files\IBM\SKLMV301" wasadmin WAS@admin123
   ```

   Une fois IBM Security Key Lifecycle Manager désinstallé, si des services Db2 sont encore en cours d'exécution, désinstallez manuellement Db2 et ses composants. Pour plus d'informations sur la désinstallation de Db2, voir http://www-01.ibm.com/support/docview.wss?uid=swg21104569.

Que faire ensuite

Consultez le récapitulatif de désinstallation et les fichiers journaux dans `C:\ProgramData\IBM\InstallationManager\logs\sklmLogs\`.

Après avoir désinstallé IBM Security Key Lifecycle Manager, supprimez les répertoires `C:\Program Files\IBM\WebSphere` et `C:\Program Files\DB2SKLMV301`, le cas échéant.

Récupération après une désinstallation manquée sur un système Windows

Vous devez effectuer une récupération après un échec de désinstallation d'IBM Security Key Lifecycle Manager sur un système Windows.

Pourquoi et quand exécuter cette tâche

Cette tâche suppose que le programme de désinstallation ne s'est pas terminé correctement. Effectuez les étapes de récupération suivantes :

Procédure

1. Arrêtez le service WebSphere Application Server.
   a. Ouvrez la console de services de Windows en accédant au Panneau de configuration et en cliquant sur **Outils d'administration** > **Services**.
   b. Recherchez le service WebSphere Application Server.

Exemple : `IBM WebSphere Application Server V9.0 - SKLM301Server`

c. Ouvrez la boîte de dialogue **Propriétés** pour le service. Si l'**état du service** n'est pas `Arrêté`, cliquez sur **Arrêter**.

d. Cliquez sur **OK** pour fermer la boîte de dialogue et quittez la console des services Windows.

Si vous ne parvenez pas à arrêter le service depuis la console Services de Windows, ouvrez une fenêtre d'invite de commande et entrez les commandes suivantes pour arrêter le service manuellement :

```
cd RACINE_WAS\bin
WASService -stop SKLMServer
```

2. Supprimez le service WebSphere Application Server s'il n'est pas déjà supprimé. Ouvrez une fenêtre d'invite de commande, puis entrez les commandes suivantes :

```
cd RACINE_WAS\bin
WASService -remove SKLMServer
```

3. Désinstallez WebSphere Application Server, s'il existe et s'il n'est utilisé par aucun autre produit.

Pour obtenir les instructions de désinstallation, voir les liens suivants :

Interface graphique
http://www.ibm.com/support/knowledgecenter/SSAW57_9.0.0/com.ibm.websphere.installation.nd.doc/ae/tins_uninstallation_dist_gui.html

Interface de ligne de commande
http://www.ibm.com/support/knowledgecenter/SSAW57_9.0.0/com.ibm.websphere.installation.nd.doc/ae/tins_uninstallation_cl.html

Si les répertoires *WAS_HOME* ou *WAS_HOME*`\bin` ont déjà été retirés, ignorez les étapes 1, 2 et 3.

4. Désinstallez Db2, s'il existe et s'il n'est utilisé par aucun autre produit.

Pour les instructions de désinstallation, voir «Suppression facultative de Db2», à la page 101.

5. Ouvrez le fichier `C:\ProgramData\IBM\Installation Manager\installRegistry.xml` dans un éditeur de texte.

Remarque : Faites une copie de sauvegarde du fichier `installRegistry.xml`.

6. Retirez les entrées *uniquement* liées à IBM Security Key Lifecycle Manager. Par exemple :

```
<profile id='IBM Security Key Lifecycle Manager v2.7' kind='product'>
  ....
</profile>
```

7. Supprimez les fichiers journaux d'installation du répertoire suivant :

`\<`*IM App Data Dir*`>\logs`

8. Supprimez **Panneau de configuration** > **Ajouter ou supprimer des programmes** > **IBM Installation Manager**.

9. Supprimez les dossiers suivants, s'ils existent :
   - `C:\Program Files\IBM\DB2SKLMV301`
   - `C:\Program Files\IBM\WebSphere`
   - `C:\Program Files\IBM\SKLMV301`
   - `C:\Program Files\IBM\Installation Manager`
   - `C:\Program Files\IBM\IBMIMShared`

10. Redémarrez l'ordinateur.

Désinstallation sur les systèmes Linux et AIX

Désinstallez IBM Security Key Lifecycle Manager et ses composants lorsque vous n'en avez plus besoin sur vos systèmes Linux ou AIX.

Désinstallation en mode graphique

Désinstallez IBM Security Key Lifecycle Manager et ses composants lorsque vous n'en avez plus besoin sur vos systèmes Linux ou AIX en mode graphique.

Procédure

1. Ouvrez une fenêtre de terminal.
2. Accédez au répertoire `disk1` de votre module d'installation. Exemple : *chemin_téléchargement*`/disk1`.
3. Exécutez la commande suivante :

   `uninstallSKLM_linux.sh` *IM_INSTALL_LOCATION WAS_INSTALL_LOCATION SKLM_INSTALL_HOME WAS_ADMIN WAS_PASSWORD*

   IM_INSTALL_LOCATION - Répertoire d'Installation Manager pour IBM Security Key Lifecycle Manager.

   WAS_INSTALL_LOCATION - Répertoire de WebSphere Application Server pour IBM Security Key Lifecycle Manager.

   SKLM_INSTALL_HOME - Répertoire d'installation d'IBM Security Key Lifecycle Manager.

   WAS_ADMIN - Nom d'utilisateur de WebSphere Application Server pour IBM Security Key Lifecycle Manager.

   WAS_PASSWORD - Mot de passe correspondant au nom d'utilisateur WebSphere Application Server.

   Par exemple :

   ```
   uninstallSKLM_linux.sh /opt/IBM/Installation Manager /opt/IBM/WebSphere/AppServer
   /opt/IBM/SKLMV301 wasadmin WAS@admin123
   ```
4. Dans l'assistant IBM Installation Manager, cliquez sur **Désinstaller**.
5. Sélectionnez les packages à désinstaller, IBM Security Key Lifecycle Manager, Db2 et WebSphere Application Server.

   Remarque : Si WebSphere Application Server n'est pas arrêté avant la désinstallation d'IBM Security Key Lifecycle Manager, le message d'erreur suivant s'affiche.

   ```
   Des processus en cours d'exécution, susceptibles d'interférer avec l'opération
   en cours, ont été détectés. Arrêtez tous les processus WebSphere et apparentés
   avant de continuer.
   ```

   Cliquez sur **Revérifier l'état** pour passer à la tâche de désinstallation.
6. Cliquez sur **Suivant**.
7. Entrez l'ID utilisateur et le mot de passe d'administrateur de WebSphere Application Server.
8. Cliquez sur **Suivant**.
9. Vérifiez les progiciels à désinstaller et leurs répertoires d'installation.
10. Cliquez sur **Désinstaller**.

Que faire ensuite

Consultez le récapitulatif de désinstallation et les fichiers journaux dans `/var/ibm/InstallationManager/logs/sklmLogs/`.

Après avoir désinstallé IBM Security Key Lifecycle Manager, supprimez les répertoires /opt/IBM/WebSphere et /opt/DB2SKLMV301, le cas échéant.

Désinstallation en mode silencieux

Désinstallez IBM Security Key Lifecycle Manager et ses composants lorsque vous n'en avez plus besoin sur vos systèmes Linux et AIX en mode silencieux.

Procédure

1. Editez le fichier de réponses afin d'ajouter des mots de passe chiffrés aux éléments concernés du fichier. Les exemples de fichiers de réponses se trouvent dans le répertoire où se trouve votre module d'installation.

   L'utilitaire IBM Installation Manager permet de créer des mots de passe chiffrés. Pour plus d'informations sur la façon de chiffrer le mot de passe, consultez Mot de passe chiffré pour les éléments du fichier de réponses.
2. Depuis le fenêtre de terminal, accédez au répertoire disk1 de votre module d'installation. Exemple : *chemin_téléchargement*/disk1.
3. Exécutez la commande suivante :

   Linux

   ```
   silent_uninstallSKLM_linux.sh IM_INSTALL_LOCATION WAS_INSTALL_LOCATION
   SKLM_INSTALL_HOME WAS_ADMIN WAS_PASSWORD
   ```

   ```
   silent_uninstallSKLM_linux.sh /opt/IBM/InstallationManager
   /opt/IBM/WebSphere/AppServer /opt/IBM/SKLMV301 wasadmin WAS@admin123
   ```

   AIX

   ```
   silent_uninstallSKLM_AIX.sh IM_INSTALL_LOCATION WAS_INSTALL_LOCATION
   SKLM_INSTALL_HOME WAS_ADMIN WAS_PASSWORD
   ```

   ```
   silent_uninstallSKLM_AIX.sh /opt/IBM/InstallationManager
   /opt/IBM/WebSphere/AppServer /opt/IBM/SKLMV301 wasadmin WAS@admin123
   ```

   IM_INSTALL_LOCATION - Répertoire d'Installation Manager pour IBM Security Key Lifecycle Manager.

   WAS_INSTALL_LOCATION - Répertoire de WebSphere Application Server pour IBM Security Key Lifecycle Manager.

   SKLM_INSTALL_HOME - Répertoire d'installation d'IBM Security Key Lifecycle Manager.

   WAS_ADMIN - Nom d'utilisateur de WebSphere Application Server pour IBM Security Key Lifecycle Manager.

   WAS_PASSWORD - Mot de passe correspondant au nom d'utilisateur WebSphere Application Server.

Que faire ensuite

Consultez le récapitulatif de désinstallation et les fichiers journaux dans /var/ibm/InstallationManager/logs/sklmLogs/.

Après avoir désinstallé IBM Security Key Lifecycle Manager, supprimez les répertoires /opt/IBM/WebSphere et /opt/DB2SKLMV301, le cas échéant.

Récupération après une désinstallation manquée sur un système Linux ou AIX

Vous souhaiterez peut-être effectuer une récupération après l'échec d'une tentative de désinstallation d'IBM Security Key Lifecycle Manager sur les systèmes Linux ou AIX.

Pourquoi et quand exécuter cette tâche

Cette tâche suppose que le programme de désinstallation ne s'est pas terminé correctement. Effectuez les étapes de récupération suivantes :

Procédure

1. Connectez-vous en tant qu'utilisateur root.
2. Arrêtez les processus WebSphere Application Server, le cas échéant.

   ```
   cd RACINE_WAS/profiles/KLMProfile/bin
   ./stopServer.sh server1
   ```
3. Désinstallez WebSphere Application Server, s'il existe et s'il n'est utilisé par aucun autre produit.

   Pour obtenir les instructions de désinstallation, voir les liens suivants :

   Interface graphique
   http://www.ibm.com/support/knowledgecenter/SSAW57_9.0.0/com.ibm.websphere.installation.nd.doc/ae/tins_uninstallation_dist_gui.html

   Interface de ligne de commande
   http://www.ibm.com/support/knowledgecenter/SSAW57_9.0.0/com.ibm.websphere.installation.nd.doc/ae/tins_uninstallation_cl.html

   Si les répertoires *WAS_HOME* ou *WAS_HOME*/bin ont déjà été retirés, ignorez les étapes 2 et 3.
4. Désinstallez Db2, s'il existe et s'il n'est utilisé par aucun autre produit.

   Pour les instructions de désinstallation, voir «Suppression facultative de Db2», à la page 101.
5. Ouvrez le fichier /var/ibm/InstallationManager/installRegistry.xml.

   Remarque : Faites une copie de sauvegarde du fichier installRegistry.xml.
6. Retirez les entrées **uniquement** liées à IBM Security Key Lifecycle Manager. Par exemple :

   ```
   <profile id='IBM Security Key Lifecycle Manager v3.0' kind='product'>
     ....
   </profile>
   ```
7. Supprimez les fichiers journaux d'installation du répertoire /var/ibm/InstallationManager/logs à l'aide de la commande suivante :

   ```
   rm -rf /var/ibm/InstallationManager/logs
   ```
8. Désinstallez IBM Installation Manager.
9. Supprimez les dossiers suivants, s'ils existent :
   - opt/IBM/DB2SKLMV301
   - opt/IBM/WebSphere
   - opt/IBM/SKLMV301
   - opt/IBM/Installation Manager
   - opt/IBM/IBMIMShared
10. Redémarrez l'ordinateur.

Mot de passe chiffré pour les éléments du fichier de réponses

Vous devez ajouter les mots de passe chiffrés aux éléments concernés du fichier de réponses. L'utilitaire IBM Installation Manager permet de créer des mots de passe chiffrés.

Windows

Par exemple, si vous procédez à l'extraction de l'image du produit IBM Security Key Lifecycle Manager dans le répertoire `C:\SKLM\disk1`, exécutez la commande suivante pour créer un mot de passe chiffré :

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

Ajoutez le mot de passe chiffré dans le fichier de réponses comme illustré dans l'exemple ci-après.

```
<data key='user.WAS_ADMIN_ID,com.ibm.sklm301.win' value='wasadmin'/>
<data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm301.win' value='e9PjN93MeQxwnSs9VXJFMw==/>
```

Linux Par exemple, si vous procédez à l'extraction de l'image du produit IBM Security Key Lifecycle Manager dans le répertoire `/SKLM/disk1`, exécutez la commande suivante pour créer un mot de passe chiffré :

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

Ajoutez le mot de passe chiffré dans le fichier de réponses comme illustré dans l'exemple ci-après.

```
<data key='user.WAS_ADMIN_ID,com.ibm.sklm301.linux' value='wasadmin'/>
<data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm301.linux' value='e9PjN93MeQxwnSs9VXJFMw==/>
```

Réinstallation de la version antérieure en cas d'échecs répétés de la migration

Le processus de migration n'affecte pas la version antérieure d'IBM Security Key Lifecycle Manager. Si la migration échoue de nouveau, désinstallez IBM Security Key Lifecycle Manager version 3.0.1 et continuez d'exécuter la version précédente.

Remarque : Sur la plateforme Windows, après la migration de la version antérieure d'IBM Security Key Lifecycle Manager vers la version 3.0.1, le programme DB2 associé à la version antérieure peut ne pas démarrer si vous désinstallez IBM Security Key Lifecycle Manager version 3.0.1 avant de désinstaller la version antérieure.

Vous pouvez désinstaller IBM Security Key Lifecycle Manager version 3.0.1 en suivant la procédure décrite dans «Désinstallation d'IBM Security Key Lifecycle Manager», à la page 93.

Suppression facultative de Db2

Après avoir désinstallé IBM Security Key Lifecycle Manager, vous pouvez choisir de désinstaller ou non Db2.

La désinstallation d'IBM Security Key Lifecycle Manager ne désinstalle pas DB2 s'il a été installé avant l'installation d'IBM Security Key Lifecycle Manager. DB2 est désinstallé lorsque vous désinstallez IBM Security Key Lifecycle Manager s'il a été installé par le programme d'installation d'IBM Security Key Lifecycle Manager. Vous pouvez aussi désactiver les services associés pour les empêcher de démarrer automatiquement.

Désinstallation de Db2

Après avoir désinstallé IBM Security Key Lifecycle Manager, vous pouvez choisir de désinstaller ou non Db2.

Si vous choisissez de ne pas désinstaller Db2, vous pouvez conserver ou supprimer le propriétaire de l'instance IBM Security Key Lifecycle Manager Db2. A moins d'avoir une raison spécifique de conserver le propriétaire de l'instance (pour conserver une connexion vers une base de données, par exemple), vous devez dissocier l'ID utilisateur de l'instance de base de données Db2. Pour plus d'informations, voir «Dissociation d'un ID utilisateur de l'instance Db2», à la page 103.

Si vous choisissez de désinstaller Db2, procédez comme suit :

Windows

Ouvrez le Panneau de configuration.

Windows Server 2012 : cliquez sur **Programmes et fonctionnalités**. Trouvez l'entrée Db2, puis cliquez sur **Supprimer** pour désinstaller le programme.

Remarque : Après avoir désinstallé Db2, vous pouvez être amené à effectuer des étapes supplémentaires afin de terminer la suppression des artefacts Db2.

1. Pour supprimer l'ID utilisateur qui a été utilisé pour le propriétaire de l'instance IBM Security Key Lifecycle Manager Db2, ouvrez Gestionnaire de serveurs et cliquez sur **Outils > Gestion de l'ordinateur > Utilisateurs et groupes locaux > Utilisateurs**.

   Consultez la liste des ID utilisateur. Si l'ID du propriétaire de l'instance IBM Security Key Lifecycle Manager Db2 existe toujours, supprimez-le.

   Fermez la console de gestion de l'ordinateur.
2. Examinez les entrées et vérifiez que celles correspondant aux ports Db2 sont supprimées du fichier `C:\WINDOWS\system32\drivers\etc\services`. Editez le fichier et recherchez les numéros de port utilisés par Db2. Si vous en trouvez, supprimez les entrées correspondantes dans le fichier.
3. Ouvrez Gestionnaire de serveurs et cliquez sur **Outils > Services**. Consultez la liste des services et vérifiez que les entrées de service associées à Db2 sont supprimées. Une fois que vous avez terminé, fermez la console des services.

4. Supprimez le répertoire d'installation de Db2 si cela n'a pas déjà été fait.

Pour plus d'informations sur la désinstallation de Db2 sur les systèmes Windows, voir la documentation de Db2 (http://www-01.ibm.com/support/knowledgecenter/SSEPGG_11.1.0/com.ibm.db2.luw.qb.server.doc/doc/t0007436.html).

AIX et Linux

1. Connectez-vous en tant que superutilisateur.
2. Supprimez l'ID utilisateur du propriétaire de l'instance IBM Security Key Lifecycle Manager Db2 :
   a. Employez l'ID utilisateur du propriétaire de l'instance Db2 d'IBM Security Key Lifecycle Manager, exécutez la commande **db2stop** pour l'ID utilisateur du propriétaire de l'instance puis reconnectez-vous avec l'ID root :

      ```
      su - ID_util_propriétaire_instance_sklm

      cd RACINE_BDD/instance
      ./db2stop sklm_instance_owner_userid /home/sklm_instance_owner_userid

      exit
      ```

   b. Exécutez la commande **db2idrop** sur l'ID utilisateur du propriétaire de l'instance :

      ```
      cd RACINE_BDD/instance
      ./db2idrop ID_util_propriétaire_instance_sklm
      ```

   c. Supprimez l'ID utilisateur du système :

      ```
      userdel -r ID_util_propriétaire_instance_sklm
      ```

3. Supprimez Db2 du système :

   ```
   cd REP_BASE_BDD/install/
   ./db2_deinstall -a
   ```

4. Editez le fichier de services :

   ```
   vi /etc/services
   ```

   Recherchez les numéros de port qui sont utilisés par Db2 et retirez les entrées du fichier.
5. Supprimez le répertoire d'installation de Db2 s'il n'est pas supprimé.

Pour plus d'informations sur la désinstallation de Db2 sur les systèmes Linux et AIX, voir la documentation de Db2 (http://www-01.ibm.com/support/knowledgecenter/SSEPGG_11.1.0/com.ibm.db2.luw.qb.server.doc/doc/t0007439.html).

L'exemple suivant présente la procédure résultant de l'utilisation de l'ID utilisateur correspondant au propriétaire de l'instance Db2 par défaut, `sklmdb31` et du répertoire Db2 par défaut, `/opt/IBM/DB2SKLMV301`.

Démarrez en tant que superutilisateur et entrez les commandes suivantes :

```
su - sklmdb31
cd /opt/IBM/DB2SKLMV301/instance
./db2stop sklmdb301/home/sklmdb301
exit
# Reprenez l'ID superutilisateur.
cd /opt/IBM/DB2SKLMV301/instance
./db2idrop sklmdb31
userdel -r sklmdb31
cd /opt/IBM/DB2SKLMV301/install
```

```
./db2_deinstall -a
vi /etc/services
# Locate and remove the Db2 port entries in the services file.
rm -rf /opt/IBM/DB2SKLMV301
```

Dissociation d'un ID utilisateur de l'instance Db2

Vous pouvez dissocier un ID utilisateur de l'instance Db2 d'IBM Security Key Lifecycle Manager.

Si l'ID utilisateur est déjà dissocié de l'instance Db2, il se peut qu'à un moment de la procédure, vous receviez un message indiquant que l'utilisateur est introuvable. Si vous recevez ce message, passez à l'étape suivante.

- **Sous Windows :**
  1. Ouvrez la console des services Windows et arrêtez le service Db2 pour le propriétaire de l'instance d'IBM Security Key Lifecycle Manager.

     Pour localiser le service de l'instance Db2, consultez la liste des services et recherchez ceux dont le nom commence par "Db2". Le service de l'instance doit contenir l'ID utilisateur du propriétaire de l'instance Db2 d'IBM Security Key Lifecycle Manager dans son nom. Par exemple, **DB2 - DBSKLMV301 - SKLMDB31**.

     Ouvrez la boîte de dialogue des propriétés du service et définissez les zones **Statut du service** sur `Arrêté` et **Type de démarrage** sur `Manuel`.
  2. Cliquez sur **Démarrer** > **Programmes** > **IBM Db2 >** *propriétaire_instance* > **Outils ligne de commande** > **Fenêtre de commande** pour ouvrir la fenêtre de commande Db2, puis entrez :

     ```
     db2idrop db nombasededonnées
     db2idrop ID_util_propriétaire_instance_sklm
     ```
  3. Si le répertoire C:*ID_util_propriétaire_instance_sklm* existe encore, supprimez-le :

     ```
     del /s /q  C:\ID_util_propriétaire_instance_sklm
     ```
- **Sous AIX et Linux :**

  Connectez-vous en tant que superutilisateur et procédez comme suit.
  1. Employez l'ID utilisateur du propriétaire de l'instance Db2 d'IBM Security Key Lifecycle Manager, exécutez la commande **db2stop** pour l'ID utilisateur du propriétaire de l'instance puis reconnectez-vous avec l'ID root :

     ```
     su - ID_util_propriétaire_instance_sklm

     cd RACINE_BDD/instance
     ./db2stop sklm_instance_owner_userid /home/sklm_instance_owner_userid

     exit
     ```
  2. Exécutez la commande **db2idrop** sur l'ID utilisateur du propriétaire de l'instance :

     ```
     cd DB_HOME/instance
     ./db2idrop ID_util_propriétaire_instance_sklm
     ```
  3. Si le répertoire *ID_util_propriétaire_instance_sklm*`/sqllib` existe encore, supprimez-le :

     ```
     rm -rf ID_util_propriétaire_instance_sklm/sqllib
     ```

Suppression de l'ID utilisateur du propriétaire de l'instance Db2

Pour supprimer l'ID utilisateur utilisé en tant que propriétaire de l'instance d'IBM Security Key Lifecycle Manager Db2, employez les utilitaires de gestion d'utilisateurs du système d'exploitation pour supprimer l'ID utilisateur.

Avant de supprimer un ID utilisateur utilisé comme propriétaire d'instance pour les bases de données d'IBM Security Key Lifecycle Manager, assurez-vous qu'il n'est plus associé à l'instance Db2.

Suivez les étapes de la section «Dissociation d'un ID utilisateur de l'instance Db2», à la page 103. Si l'ID utilisateur est déjà dissocié de l'instance Db2, il se peut qu'à un moment de la procédure, vous receviez un message indiquant que l'utilisateur est introuvable. Dans ce cas, passez à l'étape suivante.

Après avoir vérifié que l'ID utilisateur n'est plus associé à l'instance de base de données Db2, suivez ces étapes pour le supprimer du système :

- **Sous Windows :**

  Utilisez l'outil de gestion des utilisateurs disponible dans votre version de Windows pour supprimer l'administrateur Db2 du système. Par exemple, sur certaines versions de Windows, effectuez les étapes suivantes :

  1. Ouvrez le Panneau de configuration.
  2. Cliquez sur **Outils d'administration > Gestion de l'ordinateur > Utilisateurs et groupes locaux > Utilisateurs**.
  3. Supprimez l'utilisateur du système.
- **Sous AIX et Linux :**

  Connectez-vous en tant que superutilisateur et entrez la commande suivante pour supprimer l'ID utilisateur :

  ```
  userdel -r id_utilisateur_propriétaire_instance_sklm
  ```

Désactivation des services automatiques

Le processus de désinstallation d'IBM Security Key Lifecycle Manager désactive les services Db2 et WebSphere Application Server associés à IBM Security Key Lifecycle Manager. Pour remédier à certaines erreurs, vous pouvez vérifier que ces services sont effectivement désactivés.

Systèmes Windows

Sur les systèmes Windows, utilisez la console des services Windows pour empêcher les services Db2 et WebSphere Application Server associés à IBM Security Key Lifecycle Manager de démarrer automatiquement.

Ouvrez la console des services Windows et recherchez les services dans la liste suivante. Pour chaque service de la liste, ouvrez la boîte de dialogue Propriétés du service et vérifiez que la zone **Type de démarrage** est définie sur `Désactivé` et que la zone **Statut du service** est définie sur `Arrêté`.

Db2 - *db2 copy name - SKLM_INSTANCE_OWNER*
Par exemple, **DB2 - DBSKLMV301 - SKLMDB31**

Db2 Governor (*nom de copie db2***)**
Par exemple, **Db2 Governor (DB2SKLMV301)**

Db2 License Server (*nom de copie db2***)**
Par exemple, **Db2 License Server (DB2SKLMV301)**

Db2 Management Service (*nom de copie db2***)**
Par exemple, **Db2 Management Service (DB2SKLMV301)**

Db2 Remote Command Server (*nom de copie db2***)**
Par exemple, **Db2 Remote Command Server (DB2SKLMV301)**

DB2DAS - *entrée_DB2DAS*
Par exemple, **DB2DAS - DB2DAS00**

Remarque : Désactivez Db2 Administration Server (DAS) uniquement si le service DAS est hébergé dans un service Windows.

Systèmes AIX et Linux

Sur un système AIX ou Linux, entrez les commandes suivantes pour configurer le propriétaire de l'instance Db2 d'IBM Security Key Lifecycle Manager de sorte qu'il ne démarre pas automatiquement :

```
. ~sklmdb2/sqllib/db2profile
DB_HOME/instance/db2iauto -off sklmdb31
```

où `sklmdb2` correspond à l'ID utilisateur du propriétaire de l'instance par défaut. Si vous avez modifié l'ID lors de l'installation, utilisez le nouvel ID.

Editez ensuite le fichier `/etc/inittab` et supprimez l'entrée qui active le démarrage automatique du serveur WebSphere Application Server :

```
/opt/IBM/WebSphere/AppServer/bin/startServer.sh server1
```

Fichiers journaux d'installation et de migration

Si une erreur inattendue se produit lors de l'installation ou de la migration, utilisez les fichiers journaux pour déterminer la cause du problème.

Informations de base

Le programme d'installation utilise plusieurs sous-programmes, composants et sous-systèmes lors de l'installation. Plusieurs conditions d'erreur surviennent en raison de l'échec d'un sous-programme.

Sous-programmes, composants et systèmes utilisés lors de l'installation

Les fichiers journaux peuvent contenir les abréviations et noms suivants :

- Db2
- IBM Installation Manager

Phases d'installation

Les conditions d'erreur et la disponibilité des fichiers journaux dépendent du stade auquel l'erreur est survenue :

1. Présentation qui comprend des panneaux pour la sélection de la langue, des détails sur les packages à installer et le contrat de licence. Le programme d'installation gère également un système vérification des prérequis pour vérifier la configuration requise d'installation du produit.
2. La phase d'installation de Db2 qui inclut les panneaux permettant de recueillir des informations pour l'installation de Db2. Une fois que vous avez entré ces informations, le programme lance l'installation de Db2.
3. La phase d'installation du middleware qui inclut les panneaux de collecte des informations pour installer le middleware WebSphere Application Server. Une fois ces informations saisies, le programme lance l'installation du middleware.

   IBM Security Key Lifecycle Manager est installé au cours de cette phase.

Fichiers journaux importants et emplacements

L'installation d'IBM Security Key Lifecycle Manager et de ses composants génère des fichiers journaux que vous pouvez lire pour veiller à ce que l'installation ait abouti. Les journaux d'erreurs d'installation fournissent des informations critiques.

Le tableau suivant répertorie les fichiers journaux et les emplacements de fichiers générés lorsque vous utilisez les paramètres d'installation par défaut.

Tableau 12. Emplacement des fichiers journaux d'installation

Fichier journal	Description	Emplacement

`db2_install.log`	Fichier journal d'installation de Db2.	**Systèmes Windows**
		`unité:\<REP_DONNEES_IM>\logs\sklmLogs\`
		`C:\ProgramData\IBM\Installation Manager\logs\sklmLogs\`
		Systèmes Linux
		`/<REP_DONNEES_IM>/logs/sklmLogs/`
		`/var/ibm/InstallationManager/logs/sklmLogs/`

`db_config.log`	Contient des informations sur la création de la base de données et la création des tables d'IBM Security Key Lifecycle Manager.	**Systèmes Windows**
		`unité:\<REP_DONNEES_IM>\logs\sklmLogs\`
		`C:\ProgramData\IBM\Installation Manager\logs\sklmLogs\`
		Systèmes Linux
		`/<REP_DONNEES_IM>/logs/sklmLogs/`
		`/var/ibm/InstallationManager/logs/sklmLogs/`

Différents fichiers `*.xml` et `*.log`	Fichiers journaux d'installation d'IBM Security Key Lifecycle Manager
	Vous pouvez vérifier l'installation, la modification ou la désinstallation d'IBM Security Key Lifecycle Manager en consultant le fichier journal créé par IBM Installation Manager.
		Systèmes Windows
		`unité:\<REP_DONNEES_IM>\logs\`
		`C:\ProgramData\IBM\Installation Manager\logs\`
		Systèmes Linux
		`/<REP_DONNEES_IM>/logs/`
		`/var/ibm/InstallationManager/logs/`

Plusieurs fichiers `*.out` et `*.err`	Fichiers STDOUT et STDERR générés au cours de l'installation.
	La taille d'un fichier **.err** est de zéro octet si l'opération correspondante a réussi. Examinez les fichiers d'erreur dont la taille est supérieure à zéro.
		Windows
		`RACINE_WAS\logs\`
		`C:\Program Files\IBM\WebSphere\AppServer\logs\`
		Linux `RACINE_WAS/logs/`
		`/opt/IBM/WebSphere/AppServer/log/`

Tableau 12. Emplacement des fichiers journaux d'installation (suite)

Fichier journal	Description	Emplacement

`migration.log`	Après avoir migré les données existantes (version antérieure) dans la nouvelle installation, vous pouvez consulter le fichier journal de migration pour vérifier si le processus a abouti, ou à des fins de traitement des problèmes.	**Systèmes Windows**
		`unité:\<REP_DONNEES_IM>\logs\sklmLogs\`
		`C:\ProgramData\IBM\Installation Manager\logs\sklmLogs\`
		Systèmes Linux
		`/<REP_DONNEES_IM>/logs/sklmLogs/`
		`/var/ibm/InstallationManager/logs/sklmLogs/`

`sklmInstall*.log`	Fichiers journaux du programme d'installation d'IBM Security Key Lifecycle Manager. Les fichiers journaux sont créées quand chaque étape de l'installation est exécutée. Vous pouvez lire ces fichiers journaux pour vérifier si le produit est installé correctement.	**Windows** `%temp%/sklmInstaller*.log*` **Linux** `${TMPDIR}/sklmInstaller*.log`
Fichiers journaux dans `sklmPRS`	Le fichier `sklmPRS` contient des fichiers journaux pour la sortie détaillée de l'activité d'analyse prérequise (`precheck.log`) et pour les résultats de l'analyse (`results.txt`).	**Windows** `%temp%/sklmPRS/` **Linux** `${TMPDIR}/PRS/`

Fichiers journaux pour la résolution des problèmes

Le moment où se produit une erreur peut vous donner une idée du fichier journal à consulter en priorité. Les deux moments où une erreur peut se produire sont juste après la phase Db2 et juste après la phase middleware. Utilisez la liste ci-dessous pour savoir par où commencer.

Pendant ou immédiatement après la phase d'installation de Db2

1. Si l'erreur se produit assez tôt, vous pouvez vérifier les fichiers`db2_install.log`, `prsResults.xml` et `sklmInstaller*.log`.
2. Si l'erreur se produit ultérieurement au cours de cette phase, il est possible que le répertoire `sklm301properties` contienne les résultats d'une partie de la configuration de Db2, ou d'autres sous-programmes exécutés pendant la même phase.
3. L'emplacement du fichier journal des erreurs varie selon que l'erreur survient au cours ou à la fin de la phase Db2.

A la fin de la phase Db2, les fichiers journaux sont copiés du répertoire `sklm301properties` vers le répertoire `<IM_DATA_DIR>\logs\sklmLogs`. Voir tableau 12, à la page 108 pour connaître l'emplacement des fichiers.

Pendant ou immédiatement après la phase d'installation de WebSphere Application Server

Les fichiers journaux permettant d'examiner les erreurs sont les fichiers `db_config.log` et `sklmInstaller*.log`.

Nom et emplacement des fichiers journaux de migration

Durant le processus de migration, le programme de migration crée des fichiers journaux lorsqu'il appelle d'autres programmes ou outils.

Après avoir mis à niveau IBM Security Key Lifecycle Manager et avoir migré vos données existantes dans la nouvelle installation, vous pouvez consulter le fichier `migration.log` pour vérifier si le processus a abouti, ou à des fins de résolution des problèmes.

Systèmes Windows

`unité:\<REP_DONNEES_IM>\logs\sklmLogs`

Par exemple : `C:\ProgramData\IBM\Installation Manager\logs\sklmLogs\migration.log`

Systèmes Linux

`/<REP_DONNEES_IM>/logs/sklmLogs`

Par exemple : `/var/ibm/InstallationManager/logs/sklmLogs/migration.log`

Etude d'un fichier journal des erreurs

IBM Security Key Lifecycle Manager génère plusieurs fichiers journaux que vous pouvez utiliser pour résoudre les problèmes qui se produisent lorsque vous installez et configurez IBM Security Key Lifecycle Manager.

Procédure

1. Consultez la liste des fichiers journaux. Le fichier journal à examiner en premier dépend du système d'exploitation utilisé et de la phase d'installation concernée par l'erreur. La liste «Fichiers journaux pour la résolution des problèmes», à la page 109 peut fournir un point de départ. Vous devrez peut-être passer en revue plusieurs fichiers journaux avant de trouver le fichier contenant les messages d'erreur.
2. Accédez au répertoire contenant le fichier journal, puis ouvrez-le avec un éditeur de texte. Sous Windows, utilisez un éditeur de texte capable d'interpréter les sauts de lignes de style UNIX ; par exemple, Microsoft WordPad.
3. Les entrées de journal les plus récentes se trouvent à la fin du fichier. Examinez chaque entrée en commençant par la dernière entrée du fichier journal. Prenez note du programme impliqué et de l'horodatage de l'entrée (le cas échéant).

   Une fois que vous avez examiné la dernière entrée, examinez l'entrée qui la précède. Vérifiez cette entrée comme vous l'avez fait pour l'entrée précédente. Recherchez tout élément commun aux deux entrées, comme des noms de fichier ou des conditions d'erreur.

Répétez l'étape précédente, en remontant dans le fichier journal. Il se peut que plusieurs entrées contiennent des informations relatives à la condition d'erreur. Si les informations figurant dans ce fichier journal sont insuffisantes, recherchez des informations supplémentaires dans un autre fichier journal.

S'il n'existe aucun message relatif à une erreur, passez à un autre fichier journal.

Autres informations à collecter

Vous devez effectuer plusieurs actions qui peuvent fournir davantage d'informations pour vérifier l'installation.

- Vérifiez l'espace disque disponible. Pour connaître l'espace minimum requis, voir «Configuration matérielle requise», à la page 7.
- Pour valider l'installation de Db2, vérifiez que l'instance de Db2 est créée.

  Pour vérifier que l'instance Db2 a été créée, connectez-vous en tant que propriétaire de l'instance IBM Security Key Lifecycle Manager Db2, accédez au répertoire *DB_INSTANCE_HOME*, puis exécutez :

  ```
  db2ilist
  ```

  Une liste des instances configurées s'affiche. Le nom d'instance pour IBM Security Key Lifecycle Manager, par exemple `sklmdb31`, figure généralement dans la liste.
- Pour valider la création de la base de données, démarrez et arrêtez le serveur de base de données IBM Security Key Lifecycle Manager à l'aide de l'ID utilisateur du propriétaire d'instance.

  Pour démarrer et arrêter la base de données, connectez-vous en tant que propriétaire de l'instance IBM Security Key Lifecycle Manager Db2, accédez au répertoire *DB_INSTANCE_HOME*, puis exécutez les commandes **db2start** et **db2stop** sur la base de données.
- Pour valider le processus DDL (Dynamic Data Language), affichez la liste des tables dans la base de données Db2.

  Pour afficher la liste des tables, connectez-vous en tant que propriétaire de l'instance IBM Security Key Lifecycle Manager Db2, accédez au répertoire *DB_INSTANCE_HOME*, puis exécutez les commandes suivantes :

  ```
  db2 connect to base_de_données_sklm user ID_util_propriétaire_instance_sklm \
  using mot_de_passe_propriétaire_instance_sklm

  db2 list tables

  db2 describe table nom_table
  ```
- Détermine si le processus Java pour WebSphere Application Server est en cours d'exécution. Un processus en cours d'exécution valide l'installation du WebSphere Application Server.

  Pour déterminer si le processus Java est en cours d'exécution, accédez au répertoire *WAS_HOME*`/bin`, puis arrêtez et redémarrez le serveur en exécutant les commandes suivantes :

  ```
  stopServer.sh server1
  startServer.sh server1
  ```

  Si la sécurité globale est activée, ajoutez ces paramètres aux commandes d'arrêt et de redémarrage du serveur :

  ```
  -username id_admin_was -password mot_de_passe_admin_was
  ```

  Sur des systèmes Windows, vous pouvez également ouvrir la console des services Windows et vérifier que le service pour `KLMProfile` est démarré.

- Démarrez l'application IBM Security Key Lifecycle Manager pour valider l'installation d'IBM Security Key Lifecycle Manager ainsi que l'installation dans son ensemble.

  Pour démarrer l'application IBM Security Key Lifecycle Manager, démarrez WebSphere Application Server et recherchez la tâche IBM Security Key Lifecycle Manager.

Messages d'erreur liés à l'installation

Les messages indiquent les événements qui peuvent se produire lors du fonctionnement du système. En fonction du résultat d'une opération, IBM Security Key Lifecycle Manager fournit un message d'information, d'avertissement ou d'erreur.

Format des messages

Les messages qui sont consignés par IBM Security Key Lifecycle Manager respectent la norme des messages Tivoli. Chaque message comprend un ID message et un texte de message.

Les messages utilisent la syntaxe suivante :

`CTG`*`UUXXXXZ`*

où :

CTG Identifie le produit IBM Security Key Lifecycle Manager.

UU Identifie le composant ou le sous-système d'IBM Security Key Lifecycle Manager. Par exemple :

- **KM** Messages du serveur IBM Security Key Lifecycle Manager.
- **KO** Messages liés aux règles sur les mots de passe.
- **KS** Messages de serveur de clés IBM Security Key Lifecycle Manager

XXXX Indique le numéro de série ou du message, par exemple 0001.

Z Code de type sur un caractère, indiquant la gravité du message :

- `I` pour un message d'information
- `W` pour un message d'avertissement
- `E` pour un message d'erreur

Par exemple :

```
CTGKM0545E : Une erreur s'est produite lors de l'exportation d'un certificat.
```

Messages d'erreur et d'avertissement

IBM Security Key Lifecycle Manager génère des messages d'erreur et d'avertissement qui sont basées sur l'action que vous effectuez.

CTGKM9002E L'ID administrateur doit inclure 8 caractères au maximum.

Explication : L'ID utilisateur doit comporter huit caractères au maximum.

Réaction du système : Vous devez corriger l'erreur pour pouvoir poursuivre l'installation.

Action de l'utilisateur : Sélectionnez un autre ID utilisateur comportant huit caractères au maximum.

CTGKM9003E L'ID administrateur doit commencer par un caractère alphabétique.

Explication : L'ID utilisateur doit commencer par une lettre.

Par ailleurs, l'ID utilisateur peut uniquement contenir des caractères alphabétiques, des caractères numériques et le caractère de soulignement (A-Z, a-z, 0–9, et _).

Réaction du système : Vous devez corriger l'erreur pour pouvoir poursuivre l'installation.

Action de l'utilisateur : Sélectionnez un autre ID utilisateur commençant par une lettre.

CTGKM9004E L'ID administrateur ne peut pas commencer par ibm, sql ou sys.

Explication : L'ID administrateur ne peut pas commencer par ibm, sql ou sys.

Réaction du système : Vous devez corriger l'erreur pour pouvoir poursuivre l'installation.

Action de l'utilisateur : Sélectionnez un autre ID utilisateur, ne commençant pas par l'une des chaînes restreintes.

CTGKM9005E L'ID administrateur ne peut pas être db2, users, admins, guests, public, private, properties, local ou root.

Explication : Les mots clés cités dans le message sont réservés à Db2 et ne peuvent pas être utilisés comme ID utilisateur de l'administrateur.

Réaction du système : Vous devez corriger l'erreur pour pouvoir poursuivre l'installation.

Action de l'utilisateur : Sélectionnez un ID utilisateur différent, qui ne soit pas un mot clé Db2.

CTGKM9006E L'ID administrateur est obligatoire.

Explication : Vous devez indiquer un ID administrateur.

Réaction du système : Impossible de poursuivre l'installation tant que la zone n'est pas renseignée.

Action de l'utilisateur : Entrez un ID utilisateur dans la zone correspondante.

CTGKM9007E Le mot de passe est obligatoire.

Explication : Vous devez indiquer un mot de passe.

Réaction du système : Impossible de poursuivre l'installation tant que la zone n'est pas renseignée.

Action de l'utilisateur : Entrez un mot de passe associé à l'ID utilisateur.

CTGKM9010E La confirmation du mot de passe est obligatoire.

Explication : Vous devez indiquer un mot de passe.

Réaction du système : Impossible de poursuivre l'installation tant que la zone n'est pas renseignée.

Action de l'utilisateur : Entrez un mot de passe associé à l'ID utilisateur.

CTGKM9011E Le répertoire de base de la base de données est obligatoire.

Explication : Vous devez indiquer le répertoire de base de la base de données.

Réaction du système : Impossible de poursuivre l'installation tant que la zone n'est pas renseignée.

Action de l'utilisateur : Indiquez le répertoire dans lequel stocker les fichiers de base de données.

CTGKM9012E Le nom de la base de données est obligatoire.

Explication : Vous devez entrer un nom pour la base de données.

Réaction du système : Impossible de poursuivre l'installation tant que la zone n'est pas renseignée.

Action de l'utilisateur : Entrez un nom pour la base de données.

CTGKM9037E Le numéro de port doit être 443 ou 80 ou être un entier positif compris entre 1024 et 65536.

Réaction du système : Vous devez corriger l'erreur pour pouvoir poursuivre l'installation.

Action de l'utilisateur : Entrez un numéro de port 443, 80 ou compris entre 1024 et 65536.

CTGKM9038E Le port est obligatoire.

Explication : Vous devez spécifier un port.

Réaction du système : Impossible de poursuivre l'installation tant que la zone n'est pas renseignée.

Action de l'utilisateur : Entrez un numéro de port.

CTGKM9041E Le mot de passe et le mot de passe de confirmation ne correspondent pas. Entrez de nouveau des mots de passe correspondants dans les deux zones.

Explication : Les mots de passe indiqués dans les deux zones doivent concorder.

Réaction du système : Vous devez corriger l'erreur pour pouvoir poursuivre l'installation.

Action de l'utilisateur : Renseignez à nouveau les deux zones.

CTGKM9042I Les mots de passe ne doivent pas comporter d'espaces.

Explication : Les mots de passe doivent uniquement inclure des caractères alphanumériques et le caractère de soulignement (a-z, A-Z, 0–9 et _).

Réaction du système : Vous devez corriger l'erreur

pour pouvoir poursuivre l'installation.

Action de l'utilisateur : Entrez un autre mot de passe, qui sera conforme aux règles.

CTGKM9044I L'ID administrateur ne peut pas être un mot réservé SQL.

Explication : L'ID administrateur ne peut pas être un mot réservé SQL.

Réaction du système : Vous devez corriger l'erreur pour pouvoir poursuivre l'installation.

Action de l'utilisateur : Entrez un autre ID administrateur.

CTGKM9049I Sous Windows, la zone du répertoire de base de la base de données Db2 doit contenir une lettre de lecteur [A à Z] suivie du signe deux-points.

Explication : Sous Windows, vous devez sélectionner l'unité sur laquelle vous allez installer la base de données d'IBM Security Key Lifecycle Manager. L'identificateur d'unité Windows est une lettre suivie du signe deux-points (:). Par exemple, C:.

Réaction du système : Vous devez corriger l'erreur pour pouvoir poursuivre l'installation.

Action de l'utilisateur : Entrez un identificateur d'unité au format correct.

CTGKM9050E Le nom de la base de données doit comporter au plus 8 caractères.

Explication : Le nom de la base de données doit comporter au plus 8 caractères.

Réaction du système : Vous devez corriger l'erreur pour pouvoir poursuivre l'installation.

Action de l'utilisateur : Sélectionnez un autre nom.

CTGKM9050I Sous Windows, la zone du répertoire de base de la base de données Db2 doit désigner une unité qui soit accessible en écriture.

Explication : L'unité doit être accessible en écriture pour que l'installation puisse continuer.

Réaction du système : Vous devez corriger l'erreur pour pouvoir poursuivre l'installation.

Action de l'utilisateur : Exécutez les utilitaires du système d'exploitation pour rendre l'unité accessible en écriture, ou bien sélectionnez une autre unité.

CTGKM9051E Le nom de la base de données ne peut pas contenir de caractères spéciaux.

Explication : Le mot de passe contient un ou plusieurs caractères incorrects.

Action de l'utilisateur : Entrez à nouveau le nom et recommencez.

CTGKM9052E Le nom de la base de données doit commencer par un caractère alphabétique.

Explication : Le nom de la base de données peut uniquement contenir des caractères alphabétiques, des caractères numériques et le caractère de soulignement (A-Z, a-z, 0–9, et _).

Réaction du système : Vous devez corriger l'erreur pour pouvoir poursuivre l'installation.

Action de l'utilisateur : Sélectionnez un autre nom.

CTGKM9053E La version DB2 actuellement sélectionnée pour utilisation n'est pas supportée. Seules les versions 11.1 et ultérieures sont prises en charge.

Explication : IBM Security Key Lifecycle Manager requiert une version prise en charge de Db2.

Réaction du système : La tâche d'installation échoue.

Action de l'utilisateur : Procurez-vous une version prise en charge de Db2. Recommencez.

CTGKM9054E L'emplacement spécifié n'est pas un répertoire d'installation DB2 valide.

Explication : Le répertoire spécifié ne contient pas l'installation existante de DB2.

Action de l'utilisateur : Sélectionnez un répertoire d'installation DB2 valide.

CTGKM9055E Les zones de nom d'utilisateur/mot de passe ne peuvent pas comporter plus de {0} caractères.

Explication : La valeur que vous avez spécifiée dépasse la longueur maximale.

Réaction du système : Vous devez corriger l'erreur pour pouvoir poursuivre l'installation.

Action de l'utilisateur : Spécifiez une valeur qui ne dépasse pas la limite. Recommencez ensuite l'opération.

CTGKM9056E Le mot de passe et le mot de passe de confirmation ne correspondent pas pour {0}.

Explication : Les zones Mot de passe et Confirmer le mot de passe doivent avoir la même valeur.

Réaction du système : Vous devez corriger l'erreur pour pouvoir poursuivre l'installation.

Action de l'utilisateur : Spécifiez la même valeur pour les zones Mot de passe et Confirmer le mot de passe, puis tentez à nouveau l'opération.

CTGKM9057E La zone de confirmation du mot de passe de l'administrateur Application Server est vide.

Explication : L'utilisateur n'a pas spécifié la valeur de confirmation du mot de passe.

Réaction du système : Vous devez corriger l'erreur pour pouvoir poursuivre l'installation.

Action de l'utilisateur : Entrez une valeur dans la zone Confirmer le mot de passe. Recommencez.

CTGKM9058E La zone de nom d'utilisateur de l'administrateur Application Server est vide.

Explication : Ce message s'affiche lorsque la zone de nom d'utilisateur de l'administrateur du serveur d'applications est vide ou ne contient pas une valeur valide.

Réaction du système : Vous devez corriger l'erreur pour pouvoir poursuivre l'installation.

Action de l'utilisateur : Spécifiez une valeur correcte et réessayez.

CTGKM9059E La zone de nom d'utilisateur de l'administrateur IBM Security Key Lifecycle Manager est vide.

Explication : Ce message s'affiche lorsque la zone de nom d'utilisateur de l'administrateur d'IBM Security Key Lifecycle Manager est vide ou ne contient pas une valeur valide.

Réaction du système : Vous devez corriger l'erreur pour pouvoir poursuivre l'installation.

Action de l'utilisateur : Spécifiez une valeur correcte et réessayez.

CTGKM9060E La zone de nom d'utilisateur ne peut pas contenir de caractères spéciaux.

Explication : Le nom d'utilisateur contient un ou plusieurs caractères incorrects.

Réaction du système : Vous devez corriger l'erreur pour pouvoir poursuivre l'installation.

Action de l'utilisateur : Entrez à nouveau le nom d'utilisateur avec des caractères valides et réessayez.

CTGKM9061E Le port spécifié est déjà utilisé.

Explication : Le numéro de port entré doit être disponible pour l'utilisation. Le numéro de port est déjà utilisé.

Réaction du système : Vous devez corriger l'erreur pour pouvoir poursuivre l'installation.

Action de l'utilisateur : Sélectionnez un autre numéro de port. Assurez-vous que le numéro de port spécifié est disponible.

CTGKM9062E La zone du mot de passe de l'administrateur IBM Security Key Lifecycle Manager est vide.

Explication : Ce message s'affiche lorsque la zone de mot de passe de l'administrateur d'IBM Security Key Lifecycle Manager est vide ou ne contient pas une valeur valide.

Réaction du système : Vous devez corriger l'erreur pour pouvoir poursuivre l'installation.

Action de l'utilisateur : Spécifiez une valeur correcte et réessayez.

CTGKM9063E La zone du mot de passe de l'administrateur Application Server est vide.

Explication : Ce message s'affiche lorsque la zone de mot de passe de l'administrateur du serveur d'applications est vide ou ne contient pas une valeur valide.

Réaction du système : Vous devez corriger l'erreur pour pouvoir poursuivre l'installation.

Action de l'utilisateur : Spécifiez une valeur correcte et réessayez.

CTGKM9064E La zone Fichier de propriétés Encryption Key Manager est vide.

Explication : Ce message est affiché lorsque la zone Fichier de propriétés Encryption Key Manager est vide.

Réaction du système : Vous devez corriger l'erreur pour pouvoir poursuivre l'installation.

Action de l'utilisateur : Spécifiez une valeur.

CTGKM9065E La zone de confirmation du mot de passe de l'administrateur IBM Security Key Lifecycle Manager est vide.

Explication : L'utilisateur n'a pas spécifié la valeur de confirmation du mot de passe.

Réaction du système : Vous devez corriger l'erreur pour pouvoir poursuivre l'installation.

Action de l'utilisateur : Spécifiez une valeur et recommencez.

CTGKM9066E La zone du numéro de port de l'application IBM Security Key Lifecycle Manager est vide.

Explication : Ce message est affiché lorsque la zone du numéro de port de l'application IBM Security Key Lifecycle Manager est vide.

Réaction du système : Vous devez corriger l'erreur pour pouvoir poursuivre l'installation.

Action de l'utilisateur : Spécifiez une valeur et recommencez.

CTGKM9067E La zone de mot de passe de l'administrateur de base de données est vide.

Explication : Ce message est affiché lorsque la zone de mot de passe de l'administrateur de base de données est vide.

Réaction du système : Vous devez corriger l'erreur pour pouvoir poursuivre l'installation.

Action de l'utilisateur : Spécifiez une valeur et recommencez.

CTGKM9068E Le mot de passe du magasin de clés est vide.

Explication : Vous devez spécifier un mot de passe pour le magasin de clés.

Action de l'utilisateur : Spécifiez un mot de passe pour le magasin de clés et recommencez.

CTGKM9069E Le nom d'utilisateur {0} ou le mot de passe ne sont pas valides.

Explication : L'opération requiert un nom d'utilisateur et un mot de passe valides.

Réaction du système : L'opération échoue.

Action de l'utilisateur : Spécifiez un nom d'utilisateur et un mot de passe valides, puis recommencez.

CTGKM9070E Les données d'identification n'ont pas pu être validées.

Explication : Les données d'identification spécifiées sont peut-être incorrectes.

Réaction du système : Vous devez corriger l'erreur pour pouvoir poursuivre l'installation.

Action de l'utilisateur : Consultez les journaux de WebSphere Application Server pour plus d'informations et corrigez le problème.

CTGKM9071E L'instance WebSphere Application Server n'a pas pu être démarrée.

Explication : L'instance WebSphere Application Server n'a pas pu être démarrée.

Réaction du système : Vous devez corriger l'erreur pour pouvoir poursuivre l'installation.

Action de l'utilisateur : Consultez les journaux de WebSphere Application Server pour plus d'informations et corrigez le problème.

CTGKM9072E Le fichier de détails d'installation DB2 {0} est introuvable.

Explication : Le fichier de données d'instance Db2 est introuvable.

Réaction du système : Vous devez corriger l'erreur pour pouvoir poursuivre l'installation.

Action de l'utilisateur : Vérifiez que les fichiers suivants existent.

Systèmes Windows

Le fichier `db2srcit.txt` dans les répertoires suivants :

- `C:\sklmtemp`
- `C:\sklm301properties`

Systèmes Linux et AIX

Recherchez les propriétés manquantes dans le fichier `db2unix.srcit` dans les répertoires suivants :

- `/sklmtemp`
- `/root/sklm301properties`

CTGKM9073E DB2InstallResponseUpdater requiert un minimum de {0} paramètres. Seuls {1} paramètres ont été spécifiés.

Explication : Le programme d'installation ne passe pas les paramètres appropriés pour un binaire qui tente de s'exécuter. Il s'agit d'une erreur interne qui ne peut pas être corrigée par Installation Manager.

Réaction du système : L'installation échoue.

Action de l'utilisateur : Identifiez le package qui a ce problème en consultant l'historique d'installation. Dans Installation Manager, cliquez sur **Fichier** > **Historique d'installation**. En mode console, entrez S dans le menu principal pour sélectionner «Afficher l'historique d'installation». Contactez le support client IBM.

CTGKM9074E Le fichier {0} n'existe pas.

Explication : Un binaire exécuté par le programme d'installation tente d'accéder à un fichier qui n'existe pas. Il s'agit d'une erreur interne qui ne peut pas être corrigée par Installation Manager.

Réaction du système : L'installation échoue.

Action de l'utilisateur : Identifiez le package qui a ce problème en consultant l'historique d'installation. Dans Installation Manager, cliquez sur **Fichier** > **Historique d'installation**. En mode console, entrez S dans le menu principal pour sélectionner «Afficher l'historique d'installation». Contactez le support client IBM.

CTGKM9075E Le fichier {0} n'est pas inscriptible.

Explication : Un binaire exécuté par le programme d'installation tente de modifier un fichier en lecture seule. Il s'agit d'une erreur interne qui ne peut pas être corrigée par Installation Manager.

Réaction du système : L'installation échoue.

Action de l'utilisateur : Identifiez le package qui a ce problème en consultant l'historique d'installation. Dans Installation Manager, cliquez sur **Fichier** > **Historique d'installation**. En mode console, entrez S dans le menu principal pour sélectionner «Afficher l'historique d'installation». Contactez le support client IBM.

CTGKM9076E Le chemin spécifié pour l'installation DB2 existante n'est pas valide.

Explication : Le chemin spécifié pour l'installation DB2 existante est incorrect.

Réaction du système : Vous devez corriger l'erreur pour pouvoir poursuivre l'installation.

Action de l'utilisateur : Spécifiez le chemin correct, puis recommencez.

CTGKM9077E L'objet fichier de réponses est Null.

Explication : Vous devez spécifier le fichier de réponses.

Action de l'utilisateur : Spécifiez une valeur, puis recommencez.

CTGKM9078E {0} requiert {1} paramètres. Seuls {1} paramètres ont été spécifiés.

Explication : Le programme d'installation ne passe pas les paramètres appropriés pour un binaire qui tente de s'exécuter. Il s'agit d'une erreur interne qui ne peut pas être corrigée par Installation Manager.

Réaction du système : L'installation échoue.

Action de l'utilisateur : Identifiez le package qui a ce problème en consultant l'historique d'installation. Dans Installation Manager, cliquez sur **Fichier** > **Historique d'installation**. En mode console, entrez S dans le menu principal pour sélectionner «Afficher l'historique d'installation». Contactez le support client IBM.

CTGKM9079E Le fichier/dossier spécifié par le chemin {0} n'existe pas dans le système de fichiers.

Explication : Un binaire exécuté par le programme d'installation tente d'accéder à un fichier qui n'existe pas. Il s'agit d'une erreur interne qui ne peut pas être corrigée par Installation Manager.

Réaction du système : L'installation échoue.

Action de l'utilisateur : Identifiez le package qui a ce problème en consultant l'historique d'installation. Dans Installation Manager, cliquez sur **Fichier** > **Historique d'installation**. En mode console, entrez S dans le menu principal pour sélectionner «Afficher l'historique d'installation». Contactez le support client IBM.

CTGKM9080E La version {0} du serveur IBM Tivoli Key Lifecycle Manager a été détectée sur le système. Cette version ne peut pas être mise à niveau vers la version 2.6. Pour poursuivre l'installation, mettez à niveau IBM Tivoli Key Lifecycle Manager vers la version {1}.

Explication : L'installation échoue.

Réaction du système : Vous devez corriger l'erreur pour pouvoir poursuivre l'installation.

Action de l'utilisateur : Mettez à niveau IBM Tivoli Key Lifecycle Manager vers la version prise en charge.

CTGKM9081E Erreur lors de l'exécution de la commande {0}

Explication : Un problème est survenu lors de l'exécution de la commande spécifiée.

Réaction du système : L'installation échoue.

Action de l'utilisateur : Consultez les fichiers journaux d'Installation Manager et effectuez les actions correctives requises, puis recommencez.

CTGKM9082E Impossible de trouver un processus actif pour le serveur.

Explication : Un problème s'est produit lors de la tentative d'arrêt de WebSphere Application Server.

Réaction du système : L'installation échoue.

Action de l'utilisateur : Démarrez manuellement le serveur et recommencez.

CTGKM9083E Impossible de déterminer l'emplacement d'installation pour WebSphere Application Server v9.

Explication : Le programme d'installation n'a pas pu identifier l'emplacement de WebSphere Application Server version 9.0.

Réaction du système : L'installation échoue.

Action de l'utilisateur : Désinstallez Installation Manager et recommencez le processus d'installation.

CTGKM9084E Fichier de détails d'installation DB2 non valide. Impossible de trouver une entrée pour {0}.

Explication : Les informations présentes dans le fichier de données de l'instance Db2 sont incorrectes.

Réaction du système : L'installation échoue.

Action de l'utilisateur :

Sous Windows
Recherchez les propriétés manquantes dans le fichier `db2srcit.txt` dans les répertoires suivants :
- `C:\sklmtemp`
- `C:\sklm301properties`

Systèmes Linux et AIX
Recherchez les propriétés manquantes dans le fichier `db2unix.srcit` dans les répertoires suivants :
- `/sklmtemp`
- `/root/sklm301properties`

CTGKM9085E Le fichier de détails d'installation DB2 {0} est introuvable.

Explication : Le fichier de données d'instance DB2 est introuvable.

Réaction du système : Vous devez corriger l'erreur pour pouvoir poursuivre l'installation.

Action de l'utilisateur : Vérifiez que les fichiers suivants existent.

Systèmes Windows
Le fichier `db2srcit.txt` dans les répertoires suivants :
- `C:\sklmtemp`
- `C:\sklm301properties`

Systèmes Linux et AIX
Recherchez les propriétés manquantes dans le fichier `db2unix.srcit` dans les répertoires suivants :
- `/sklmtemp`
- `/root/sklm301properties`

CTGKM9086E Aucune installation WebSphere Application Server n'a été trouvée dans le registre.

Explication : Aucune instance de WebSphere Application Server version 8.5 n'a été trouvée dans le registre d'installation.

Réaction du système : Vous devez corriger l'erreur pour pouvoir poursuivre l'installation.

Action de l'utilisateur : Désinstallez Installation Manager et réexécutez le programme d'installation.

CTGKM9087E Impossible de charger les données du fichier de définition de ports {0}.

Explication : Le fichier de définition des ports pour WebSphere Application Server n'a pas pu être lu.

Réaction du système : Vous devez corriger l'erreur pour pouvoir poursuivre l'installation.

Action de l'utilisateur : Nettoyez toute installation existante et relancez le programme d'installation.

CTGKM9088E Le fichier de définition de ports {0} ne contient pas les clés requises - {1}.

Explication : Des informations du fichier de définition de ports sont incorrectes.

Réaction du système : Vous devez corriger l'erreur pour pouvoir poursuivre l'installation.

Action de l'utilisateur : Nettoyez toute installation existante et relancez le programme d'installation.

CTGKM9089E Impossible d'obtenir l'emplacement du fichier du magasin de clés.

Explication : L'emplacement du magasin de clés est introuvable.

Réaction du système : Echec de l'installation.

Action de l'utilisateur : Vérifiez que la base de données Tivoli Key Lifecycle Manager est active et en cours d'exécution, puis relancez le programme d'installation.

CTGKM9090E Les offres IBM DB2 et IBM WebSphere Application Server doivent être sélectionnées pour que l'installation d'IBM Security Key Lifecycle Manager puisse se poursuivre. Retournez à l'écran précédent et sélectionnez les offres IBM DB2 V11.1 et IBM WebSphere Application Server V9.0.

Explication : Les informations que vous avez spécifiées ne sont pas correctes.

Action de l'utilisateur : Spécifiez les valeurs correctes.

CTGKM9091E Les offres IBM DB2 et IBM WebSphere Application Server associées à IBM Security Key Lifecycle Manager doivent être sélectionnées pour que la désinstallation d'IBM Security Key Lifecycle Manager puisse se poursuivre. Retournez à l'écran précédent et sélectionnez les offres IBM DB2 V11.1 et IBM WebSphere Application Server V9.0.

Explication : Les informations que vous avez spécifiées ne sont pas correctes.

Réaction du système : Vous devez corriger l'erreur pour pouvoir poursuivre la désinstallation.

Action de l'utilisateur : Spécifiez les valeurs correctes.

CTGKM9092E Un ou plusieurs prérequis ne remplissent pas les conditions. Le rapport est fourni ci-après.

Explication : Les conditions prérequises pour l'installation ne sont pas remplies. Toutes les conditions prérequises doivent être remplies pour l'installation.

Réaction du système : Vous devez corriger l'erreur pour pouvoir poursuivre l'installation.

Action de l'utilisateur : Prenez les mesures correctives pour satisfaire aux conditions requises, puis recommencez.

CTGKM9093E Aucun des lecteurs sur le système n'a l'espace requis ({0}) pour l'installation du produit.

Explication : L'espace minimal pour installer le produit n'est pas disponible dans le système.

Réaction du système : Vous devez corriger l'erreur pour pouvoir poursuivre l'installation.

Action de l'utilisateur : Augmentez la quantité d'espace disponible sur l'unité spécifiée de façon à atteindre le minimum requis, puis recommencez.

CTGKM9094E Impossible de lire les résultats du scanner de prérequis.

Explication : Le fichier de sortie requis est introuvable après l'exécution du scanner de prérequis.

Réaction du système : Vous devez corriger l'erreur pour pouvoir poursuivre l'installation.

Action de l'utilisateur : Réexécutez l'installation sans supprimer aucun fichier du système.

CTGKM9095E Le mot de passe ne respecte pas les exigences de règles sur les mots de passe du système d'exploitation. Vérifiez la longueur minimale du mot de passe et les exigences de complexité du mot de passe.

Explication : Le mot de passe spécifié ne respecte pas les règles de mot de passe.

Réaction du système : Le mot de passe n'est pas mis à jour sur le serveur.

Action de l'utilisateur : Vérifiez la longueur de mot de passe minimale, la complexité du mot de passe et l'historique des critères de mots de passe.

CTGKM9096E Les données d'identification fournies pour l'administrateur de WebSphere Application Server ne sont pas valides.

Explication : Des données d'identification incorrectes sont spécifiées pour l'administrateur de WebSphere Application Server.

Réaction du système : Vous devez corriger l'erreur pour pouvoir poursuivre l'installation.

Action de l'utilisateur : Spécifiez le nom d'utilisateur et le mot de passe corrects pour l'administrateur WebSphere Application Server, puis recommencez.

CTGKM9099E Les données d'identification de l'administrateur WebSphere sont requises pour la désinstallation.

Explication : Le nom d'utilisateur ou le mot de passe pour WebSphere Application Server n'est pas spécifié ou est incorrect.

Action de l'utilisateur : Spécifiez le nom d'utilisateur et le mot de passe corrects pour l'administrateur WebSphere Application Server, puis réessayez.

CTGKM9100E Le fichier de détails d'installation DB2 {0} est introuvable.

Explication : Le fichier de données d'instance Db2 est introuvable.

Réaction du système : Vous devez corriger l'erreur pour pouvoir poursuivre l'installation.

Action de l'utilisateur : Vérifiez que les fichiers suivants existent.

Systèmes Windows

Le fichier `db2srcit.txt` dans les répertoires suivants :

- `C:\sklmtemp`
- `C:\sklm301properties`

Systèmes Linux et AIX

Recherchez les propriétés manquantes dans le fichier `db2unix.srcit` dans les répertoires suivants :

- `/sklmtemp`
- `/root/sklm301properties`

CTGKM9101E Le chemin "<Variable formatSpec="{0}">VALUE_0</Variable>" est sur un système de fichiers réseau ou n'est pas accessible en écriture. Sélectionnez un chemin du système de fichiers local pour l'installation.

Explication : L'installation est tentée à un emplacement qui n'est pas sur le disque dur local du système.

Réaction du système : Vous devez corriger l'erreur pour pouvoir poursuivre l'installation.

Action de l'utilisateur : Changez le chemin d'installation et indiquez un chemin d'accès local sur le système.

CTGKM9102E Le chemin "<Variable formatSpec="{0}">VALUE_0</Variable>" est sur un lecteur réseau ou n'est pas accessible en écriture. Sélectionnez un lecteur local pour l'installation.

Explication : L'installation est tentée à un emplacement qui n'est pas sur le disque dur local du système.

Réaction du système : Vous devez corriger l'erreur pour pouvoir poursuivre l'installation.

Action de l'utilisateur : Changez le chemin d'installation et indiquez un chemin d'accès local sur le système.

CTGKM9103E Impossible de trouver l'emplacement de l'outil scanner de prérequis.

Explication : L'emplacement de l'outil scanner de prérequis est introuvable.

Réaction du système : Vous devez corriger l'erreur pour pouvoir poursuivre l'installation.

Action de l'utilisateur : Réexécutez l'installation sans supprimer aucun fichier du système.

CTGKM9104E Les droits requis ne sont pas disponibles dans {0} pour effectuer l'installation.

Explication : Vous pourriez ne pas disposer des droits de lecture, écriture et exécution sur les répertoires d'installation.

Réaction du système : Vous devez corriger l'erreur pour pouvoir poursuivre l'installation.

Action de l'utilisateur : Vérifiez les droits sur les répertoires d'installation pour effectuer l'installation de chaque composant d'IBM Security Key Lifecycle Manager et tentez à nouveau l'installation.

CTGKM9105E L'emplacement TEMP Java et l'emplacement TEMP de variable d'environnement sont différents. Les chemins d'emplacement doivent être identiques.

Explication : L'emplacement du répertoire temporaire Java et l'emplacement de la variable d'environnement TEMP, peuvent ne pas être identiques.

Réaction du système : Vous devez corriger l'erreur pour pouvoir poursuivre l'installation.

Action de l'utilisateur : Assurez-vous que les chemins d'emplacement pour le répertoire temporaire Java et la variable d'environnement TEMP sont identiques.

CTGKM9106E Erreur lors de la désinstallation d'IBM Security Key Lifecycle Manager. Consultez les fichiers journaux du programme d'installation pour plus d'informations.

Réaction du système : Vous ne pouvez pas procéder à la désinstallation tant que vous n'avez pas corrigé l'erreur.

Action de l'utilisateur : Corrigez l'erreur et réessayez.

CTGKM9107E La variable d'environnement {0} n'est pas définie OU est NULL. Définissez la variable d'environnement pour continuer.

Explication : La variable d'environnement `TEMP` (Windows) ou `TMPDIR` (Linux) n'est pas définie ou est vide.

Réaction du système : Vous devez corriger l'erreur pour pouvoir poursuivre l'installation.

Action de l'utilisateur : Assurez-vous que la valeur de la variable d'environnement est définie vers un répertoire temporaire valide, par exemple `TMPDIR=/tmp`.

CTGKM9108E Le port FCM_PORT_NUMBER {0} requis pour l'installation de DB2 est déjà utilisé. Libérez ce port pour poursuivre l'installation.

Réaction du système : Vous devez corriger l'erreur pour pouvoir poursuivre l'installation.

Action de l'utilisateur : Libérez le port en arrêtant l'application qui l'utilise. Ensuite, tentez de nouveau l'installation.

CTGKM9109E Le numéro de port {0} est en conflit avec la valeur FCM_PORT_NUMBER. Choisissez un autre port puis faites une nouvelle tentative.

Réaction du système : Vous devez corriger l'erreur pour pouvoir poursuivre l'installation.

Action de l'utilisateur : Spécifiez un port valide, qui ne provoque pas de conflit de port. Ensuite, tentez de nouveau l'installation.

CTGKM9110W IBM Security Key Lifecycle Manager est en cours d'installation sur un système d'exploitation non pris en charge.

Action de l'utilisateur : Assurez-vous que la commande est exécutée sur un système d'exploitation pris en charge. Pour une liste des systèmes d'exploitation pris en charge, consultez la documentation du produit IBM Security Key Lifecycle Manager dans IBM Knowledge Center.

CTGKM9111W Le programme d'installation du produit ne peut pas détecter le système d'exploitation sur l'hôte.

Action de l'utilisateur : Assurez-vous que la commande est exécutée sur un système d'exploitation pris en charge. Pour une liste des systèmes d'exploitation pris en charge, consultez la documentation du produit IBM Security Key Lifecycle Manager dans IBM Knowledge Center.

CTGKM9112E Vous devez indiquer des numéros de port différents.

Explication : Les numéros de ports qui sont mentionnés sur le formulaire ne doit pas être identiques.

Réaction du système : Vous devez corriger l'erreur pour pouvoir poursuivre l'installation.

Action de l'utilisateur : Assurez-vous que les numéros de port sont différents et tentez à nouveau l'installation.

CTGKM9113E Le port {0} est en conflit avec le port DB2. Choisissez un autre port pour poursuivre l'installation.

Explication : La valeur sélectionnée pour le port est en conflit avec le port DB2.

Réaction du système : Vous devez corriger l'erreur pour pouvoir poursuivre l'installation.

Action de l'utilisateur : Indiquez un port libre et relancez l'installation.

CTGKM9114E Les ports 441, 5696, 3801 sont réservés pour d'autres services. Indiquez un autre port pour poursuivre l'installation.

Explication : La valeur sélectionnée pour le port est réservée pour un autre service.

Réaction du système : Vous devez corriger l'erreur pour pouvoir poursuivre l'installation.

Action de l'utilisateur : Assurez-vous que la valeur du port n'est pas réservée pour tous les autres services.

CTGKM9115E Impossible de créer le fichier de propriétés pour la définition de port.

Explication : Impossible de modifier le fichier `portsDef.props` avec les paramètres de numéro de port pour la création du profil de WebSphere Application Server.

Réaction du système : Vous devez corriger l'erreur pour pouvoir poursuivre l'installation.

Action de l'utilisateur : Vérifiez les informations suivantes et essayez l'installation :

- Vérifiez que vous disposez des droits de lecture, d'écriture et d'exécution à l'emplacement `TEMP` (Windows) et `$HOME` (Linux).
- Assurez-vous qu'aucun fichier de propriétés ne porte le même nom.
- Assurez-vous que le fichier n'est pas utilisé par un autre programme.

CTGKM9116E Le mot de passe doit être différent du nom d'utilisateur. Indiquez un autre mot de passe.

Explication : Un mot de passe ne peut pas être identique à votre nom d'utilisateur ou ID utilisateur.

Réaction du système : Vous devez corriger l'erreur pour pouvoir poursuivre l'installation.

Action de l'utilisateur : Entrez un mot de passe différent conforme aux règles et faites une nouvelle tentative.

CTGKM9117E La version détectée n'est pas prise en charge pour la migration en ligne d'IBM Security Key Lifecycle Manager.

Action de l'utilisateur : Assurez-vous que vous migrez une version prise en charge. Pour la liste des versions prises en charge pour la migration en ligne, voir la documentation du produit IBM Security Key Lifecycle Manager dans l'IBM Knowledge Center.

Exemples de fichier de réponses

Vous pouvez utiliser les fichiers de réponses exemples pour des systèmes Windows et d'autres systèmes. Avant l'installation, vous devez également lire et accepter les dispositions du contrat de licence de ce produit. Vous trouverez les fichiers de réponse exemples, ainsi que les fichiers des contrats de licence, dans le répertoire racine des images d'installation. Le sous-répertoire `/license` contient les fichiers de licence au format texte.

L'installation échoue sauf si vous effectuez ces étapes.

Dans le fichier de réponses, modifiez comme suit la ligne qui spécifie la licence :

- Mettez la valeur à `true` pour indiquer que vous acceptez les dispositions du contrat de licence.
- Supprimez la mise en commentaire de la ligne en ôtant le signe # au début de la ligne.

Nouvelle installation de la version 3.0.1 sur des systèmes Windows

L'exemple de fichier de réponses contient les réponses nécessaires à l'installation d'IBM Security Key Lifecycle Manager version 3.0.1 sur un système Windows ou à une installation s'accompagnant d'une migration de Encryption Key Manager.

```
<?xml version='1.0' encoding='UTF-8'?>
<agent-input clean='true' >
  <server>
    <repository location='C:\disk1\im'/>
 <repository location='C:\disk1\'/>
  </server>
  <profile id='IBM Installation Manager' installLocation='C:\Program Files\IBM\Installation Manager\eclipse' kind='self'>
    <data key='eclipseLocation' value='C:\Program Files\IBM\Installation Manager\eclipse'/>
    <data key='user.import.profile' value='false'/>
    <data key='cic.selector.os' value='win32'/>
    <data key='cic.selector.arch' value='x86_64'/>
    <data key='cic.selector.ws' value='win32'/>
  </profile>
  <install modify='false'>
    <offering profile='IBM Installation Manager' id='com.ibm.cic.agent' features='agent_core,agent_jre,agent_web' installFixes='none'
    <offering profile='IBM DB2 SKLM301' id='com.ibm.sklm301.db2.win.ofng' features='main.feature' installFixes='none'/>
    <offering profile='IBM WebSphere Application Server V9.0' id='com.ibm.websphere.BASE.v90' features='core.feature,ejbdeploy,thincl
    <offering profile='IBM WebSphere Application Server V9.0' id='com.ibm.java.jdk.v8' features='com.ibm.sdk.8' installFixes='none'/>
    <offering profile='IBM Security Key Lifecycle Manager v3.0.1' id='com.ibm.sklm301.win' features='main.feature' installFixes='none
  </install>
  <profile id='IBM DB2 SKLM301' installLocation='C:\Program Files\IBM\DB2SKLMV301'>
    <data key='eclipseLocation' value='C:\Program Files\IBM\DB2SKLMV301'/>
    <data key='user.import.profile' value='false'/>
    <data key='cic.selector.os' value='win32'/>
    <data key='cic.selector.arch' value='x86_64'/>
    <data key='cic.selector.ws' value='win32'/>
    <data key='user.DB2_ADMIN_ID,com.ibm.sklm301.db2.win.ofng' value='sklmdb31'/>
    <data key='user.DB2_ADMIN_PWD,com.ibm.sklm301.db2.win.ofng' value='QTh/0AiFvrljhs9gnOYkGA=='/>
    <data key='user.CONFIRM_PASSWORD,com.ibm.sklm301.db2.win.ofng' value='QTh/0AiFvrljhs9gnOYkGA=='/>
    <data key='user.DB2_DB_HOME,com.ibm.sklm301.db2.win.ofng' value='C:'/>
    <data key='user.DB2_DB_NAME,com.ibm.sklm301.db2.win.ofng' value='SKLMDB31'/>
    <data key='user.DB2_DB_PORT,com.ibm.sklm301.db2.win.ofng' value='50050'/>
    <data key='user.DB2_EXISTS,com.ibm.sklm301.db2.win.ofng' value='false'/>
    <data key='user.DB2_LOCATION,com.ibm.sklm301.db2.win.ofng' value='C:\\Program Files\\IBM\\DB2SKLMV301'/>
    <data key='cic.selector.nl' value='en'/>
  </profile>

  <profile id='IBM WebSphere Application Server V9.0' installLocation='C:\Program Files\IBM\WebSphere\AppServer'>
    <data key='eclipseLocation' value='C:\Program Files\IBM\WebSphere\AppServer'/>
    <data key='user.import.profile' value='false'/>
    <data key='cic.selector.os' value='win32'/>
    <data key='cic.selector.arch' value='x86_64'/>
    <data key='cic.selector.ws' value='win32'/>
    <data key='cic.selector.nl' value='en'/>
  </profile>
  <profile id='IBM Security Key Lifecycle Manager v3.0.1' installLocation='C:\Program Files\IBM\SKLMV301'>
    <data key='eclipseLocation' value='C:\Program Files\IBM\SKLMV301'/>
    <data key='user.import.profile' value='false'/>
    <data key='cic.selector.os' value='win32'/>
```

```
    <data key='cic.selector.arch' value='x86_64'/>
    <data key='cic.selector.ws' value='win32'/>
    <data key='user.IS_SILENT_MODE,com.ibm.sklm301.win' value='false'/>
    <data key='user.EKM_PROPFILE,com.ibm.sklm301.win' value='C:\KeyManagerConfig.properties'/>
    <data key='user.EKM_MIGRATION,com.ibm.sklm301.win' value='false'/>
    <data key='user.PROFILE_NAME,com.ibm.sklm301.win' value='KLMProfile'/>
    <data key='user.WAS_ADMIN_ID,com.ibm.sklm301.win' value='wasadmin'/>
    <data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm301.win' value='e9PjN93MeQxwnSs9VXJFMw==''/>
    <data key='user.WAS_ADMIN_CONF_PWD,com.ibm.sklm301.win' value='e9PjN93MeQxwnSs9VXJFMw==''/>
    <data key='user.SKLM_ADMIN_USER,com.ibm.sklm301.win' value='SKLMAdmin'/>
    <data key='user.SKLM_ADMIN_PASSWORD,com.ibm.sklm301.win' value='9YTRJMRIydDSdfhaHPs1ag==''/>
    <data key='user.SKLM_ADMIN_CONF_PWD,com.ibm.sklm301.win' value='9YTRJMRIydDSdfhaHPs1ag==''/>
    <data key='user.SKLM_APP_PORT,com.ibm.sklm301.win' value='443'/>
  <data key='user.WAS_ADMIN_PORT,com.ibm.sklm301.win' value='9083'/>
  <data key='user.SKLM_APP_NS_PORT,com.ibm.sklm301.win' value='80'/>
    <data key='cic.selector.nl' value='en'/>
  </profile>

  <preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='C:\Program Files (x86)\IBM\IBMIMShared'/>
  <preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30'/>
  <preference name='com.ibm.cic.common.core.preferences.readTimeout' value='45'/>
  <preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0'/>
  <preference name='offering.service.repositories.areUsed' value='true'/>
  <preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false'/>
  <preference name='com.ibm.cic.common.core.preferences.http.disablePreemptiveAuthentication' value='false'/>
  <preference name='http.ntlm.auth.kind' value='NTLM'/>
  <preference name='http.ntlm.auth.enableIntegrated.win32' value='true'/>
  <preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true'/>
  <preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false'/>
  <preference name='PassportAdvantageIsEnabled' value='false'/>
  <preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false'/>
  <preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false'/>
  <preference name='com.ibm.cic.common.sharedUI.showErrorLog' value='true'/>
  <preference name='com.ibm.cic.common.sharedUI.showWarningLog' value='true'/>
  <preference name='com.ibm.cic.common.sharedUI.showNoteLog' value='true'/>
</agent-input>
```

Nouvelle installation de la version 3.0.1 sur des systèmes Linux

L'exemple de fichier de réponses contient des réponses pour une installation d'IBM Security Key Lifecycle Manager version 3.0.1 sur un système tel que Linux, ou pour une installation dans laquelle la migration d'Encryption Key Manager se produit.

```
<?xml version='1.0' encoding='UTF-8'?>
<agent-input clean='true' >
  <server>
    <repository location='/disk1/im'/>
    <repository location='/disk1/'/>
  </server>
  <profile id='IBM Installation Manager' installLocation='/opt/IBM/InstallationManager/eclipse' kind='self'>
    <data key='eclipseLocation' value='/opt/IBM/InstallationManager/eclipse'/>
    <data key='user.import.profile' value='false'/>
    <data key='cic.selector.os' value='linux'/>
    <data key='cic.selector.arch' value='x86_64'/>
    <data key='cic.selector.ws' value='gtk'/>
  </profile>
  <install modify='false'>
    <offering profile='IBM Installation Manager' id='com.ibm.cic.agent' features='agent_core,agent_jre,agent_web' installFixes='none'/>
 <offering profile='IBM DB2 SKLM301' id='com.ibm.sklm301.db2.lin.ofng' features='main.feature' installFixes='none'/>
 <offering profile='IBM WebSphere Application Server V9.0' id='com.ibm.websphere.BASE.v90' features='core.feature,ejbdeploy,thinclient,e
 <offering profile='IBM WebSphere Application Server V9.0' id='com.ibm.java.jdk.v8' features='com.ibm.sdk.8' installFixes='none'/>
 <offering profile='IBM Security Key Lifecycle Manager v3.0.1' id='com.ibm.sklm301.linux' features='main.feature' installFixes='none'/>
  </install>
  <profile id='IBM DB2 SKLM301' installLocation='/opt/IBM/DB2SKLMV301'>
    <data key='eclipseLocation' value='/opt/IBM/DB2SKLMV301'/>
    <data key='user.import.profile' value='false'/>
    <data key='cic.selector.os' value='linux'/>
    <data key='cic.selector.arch' value='x86_64'/>
    <data key='cic.selector.ws' value='gtk'/>
    <data key='user.DB2_ADMIN_ID,com.ibm.sklm301.db2.lin.ofng' value='sklmdb31'/>
    <data key='user.DB2_ADMIN_PWD,com.ibm.sklm301.db2.lin.ofng' value='QTh/0AiFvrljhs9gnOYkGA==''/>
    <data key='user.CONFIRM_PASSWORD,com.ibm.sklm301.db2.lin.ofng' value='QTh/0AiFvrljhs9gnOYkGA==''/>
    <data key='user.DB2_DB_HOME,com.ibm.sklm301.db2.lin.ofng' value='/home/sklmdb31'/>
    <data key='user.DB2_DB_NAME,com.ibm.sklm301.db2.lin.ofng' value='SKLMDB31'/>
    <data key='user.DB2_DB_PORT,com.ibm.sklm301.db2.lin.ofng' value='50050'/>
    <data key='user.DB2_EXISTS,com.ibm.sklm301.db2.lin.ofng' value='false'/>
    <data key='user.DB2_LOCATION,com.ibm.sklm301.db2.lin.ofng' value='/opt/IBM/DB2SKLMV301'/>
    <data key='user.DB2_DB_LHOME,com.ibm.sklm301.db2.lin.ofng' value='/home/sklmdb31'/>
    <!--The DB2 Group name should not be more than 8 characters -->
    <data key='user.DB2_ADMIN_GRP,com.ibm.sklm301.db2.lin.ofng' value='sklmdb31'/>
    <data key='cic.selector.nl' value='en'/>
  </profile>
  <profile id='IBM WebSphere Application Server V9.0' installLocation='/opt/IBM/WebSphere/AppServer'>
    <data key='eclipseLocation' value='/opt/IBM/WebSphere/AppServer'/>
    <data key='user.import.profile' value='false'/>
    <data key='cic.selector.os' value='linux'/>
```

```
    <data key='cic.selector.arch' value='x86_64'/>
    <data key='cic.selector.ws' value='gtk'/>
    <data key='cic.selector.nl' value='en'/>
  </profile>
  <profile id='IBM Security Key Lifecycle Manager v3.0.1' installLocation='/opt/IBM/SKLMV301'>
    <data key='eclipseLocation' value='/opt/IBM/SKLMV301'/>
    <data key='user.import.profile' value='false'/>
    <data key='cic.selector.os' value='linux'/>
    <data key='cic.selector.arch' value='x86_64'/>
    <data key='cic.selector.ws' value='gtk'/>
    <data key='user.IS_SILENT_MODE,com.ibm.sklm301.linux' value='false'/>
    <data key='user.EKM_PROPFILE,com.ibm.sklm301.linux' value='/opt/IBM/KeyManagerConfig.properties'/>
    <data key='user.EKM_MIGRATION,com.ibm.sklm301.linux' value='false'/>
    <data key='user.PROFILE_NAME,com.ibm.sklm301.linux' value='KLMProfile'/>
    <data key='user.WAS_ADMIN_ID,com.ibm.sklm301.linux' value='wasadmin'/>
    <data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm301.linux' value='e9PjN93MeQxwnSs9VXJFMw==' />
    <data key='user.WAS_ADMIN_CONF_PWD,com.ibm.sklm301.linux' value='e9PjN93MeQxwnSs9VXJFMw==' />
    <data key='user.SKLM_ADMIN_USER,com.ibm.sklm301.linux' value='SKLMAdmin'/>
    <data key='user.SKLM_ADMIN_PASSWORD,com.ibm.sklm301.linux' value='9YTRJMRIydDSdfhaHPs1ag==' />
    <data key='user.SKLM_ADMIN_CONF_PWD,com.ibm.sklm301.linux' value='9YTRJMRIydDSdfhaHPs1ag==' />
    <data key='user.SKLM_APP_PORT,com.ibm.sklm301.linux' value='443'/>
  <data key='user.WAS_ADMIN_PORT,com.ibm.sklm301.linux' value='9083'/>
  <data key='user.SKLM_APP_NS_PORT,com.ibm.sklm301.linux' value='80'/>
    <data key='cic.selector.nl' value='en'/>
  </profile>
  <preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='/opt/IBM/IBMIMShared'/>
  <preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30'/>
  <preference name='com.ibm.cic.common.core.preferences.readTimeout' value='45'/>
  <preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0'/>
  <preference name='offering.service.repositories.areUsed' value='true'/>
  <preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false'/>
  <preference name='com.ibm.cic.common.core.preferences.http.disablePreemptiveAuthentication' value='false'/>
  <preference name='http.ntlm.auth.kind' value='NTLM'/>
  <preference name='http.ntlm.auth.enableIntegrated.win32' value='true'/>
  <preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true'/>
  <preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false'/>
  <preference name='PassportAdvantageIsEnabled' value='false'/>
  <preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false'/>
  <preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false'/>
  <preference name='com.ibm.cic.common.sharedUI.showErrorLog' value='true'/>
  <preference name='com.ibm.cic.common.sharedUI.showWarningLog' value='true'/>
  <preference name='com.ibm.cic.common.sharedUI.showNoteLog' value='true'/>
</agent-input>
```

Nouvelle installation de la version 3.0.1 sur Linux for System z

L'exemple de fichier de réponses contient des réponses pour une installation d'IBM Security Key Lifecycle Manager version 3.0.1 sur Linux for System z ou une installation dans laquelle la migration d'Encryption Key Manager se produit.

```
<?xml version="1.0" encoding="UTF-8"?>
<!--L'attribut "acceptLicense" est obsolète. La ligne de commande "-acceptLicense" permet d'accepter les contrats de licence.-->
<agent-input clean='true' >
 <server>
  <repository location='/disk1/im'/>
  <repository location='/disk1/'/>
 </server>
 <profile id='IBM Installation Manager' installLocation='/opt/IBM/InstallationManager/eclipse' kind='self'>
  <data key='eclipseLocation' value='/opt/IBM/InstallationManager/eclipse'/>
  <data key='user.import.profile' value='false'/>
  <data key='cic.selector.os' value='linux'/>
  <data key='cic.selector.arch' value='s390x'/>
  <data key='cic.selector.ws' value='gtk'/>
 </profile>
 <install modify='false'>
  <offering id='com.ibm.cic.agent'  profile='IBM Installation Manager' features='agent_core,agent_jre' installFixes='none'/>
  <offering id='com.ibm.sklm301.db2.lin.ofng'  profile='IBM DB2 SKLM301' features='main.feature' installFixes='none'/>
  <offering id='com.ibm.websphere.BASE.v90'  profile='IBM WebSphere Application Server V9.0'  features='core.feature,ejbdeploy,thincl
  <offering id='com.ibm.java.jdk.v8' profile='IBM WebSphere Application Server V9.0'  features='com.ibm.sdk.8' installFixes='none'/>
  <offering id='com.ibm.sklm301.linux'  profile='IBM Security Key Lifecycle Manager v3.0.1' features='main.feature' installFixes='nor
 </install>
 <profile id='IBM DB2 SKLM301' installLocation='/opt/IBM/DB2SKLMV301'>
  <data key='eclipseLocation' value='/opt/IBM/DB2SKLMV301'/>
  <data key='user.import.profile' value='false'/>
  <data key='cic.selector.os' value='linux'/>
  <data key='cic.selector.arch' value='s390x'/>
  <data key='cic.selector.ws' value='gtk'/>
  <data key='user.DB2_ADMIN_ID,com.ibm.sklm301.db2.lin.ofng' value='sklmdb31'/>
  <!--The DB2 Group name should not be more than 8 characters -->
  <data key='user.DB2_ADMIN_GRP,com.ibm.sklm301.db2.lin.ofng' value='sklmdb31'/>
  <data key='user.DB2_ADMIN_PWD,com.ibm.sklm301.db2.lin.ofng' value='QTh/0AiFvrljhs9gnOYkGA==' />
  <data key='user.CONFIRM_PASSWORD,com.ibm.sklm301.db2.lin.ofng' value='QTh/0AiFvrljhs9gnOYkGA==' />
  <data key='user.DB2_DB_HOME,com.ibm.sklm301.db2.lin.ofng' value='/home/sklmdb31'/>
  <data key='user.DB2_DB_LHOME,com.ibm.sklm301.db2.lin.ofng' value='/home/sklmdb31'/>
  <data key='user.DB2_DB_NAME,com.ibm.sklm301.db2.lin.ofng' value='SKLMDB31'/>
  <data key='user.DB2_DB_PORT,com.ibm.sklm301.db2.lin.ofng' value='50050'/>
  <data key='user.DB2_EXISTS,com.ibm.sklm301.db2.lin.ofng' value='false'/>
  <data key='user.DB2_LOCATION,com.ibm.sklm301.db2.lin.ofng' value='/opt/IBM/DB2SKLMV301'/>
```

```
 <data key='cic.selector.nl' value='en'/>
</profile>
<profile id='IBM WebSphere Application Server V9.0' installLocation='/opt/IBM/WebSphere/AppServer'>
 <data key='eclipseLocation' value='/opt/IBM/WebSphere/AppServer'/>
 <data key='user.import.profile' value='false'/>
 <data key='cic.selector.os' value='linux'/>
 <data key='cic.selector.arch' value='s390x'/>
 <data key='cic.selector.ws' value='gtk'/>
 <data key='cic.selector.nl' value='en'/>
</profile>
<profile id='IBM Security Key Lifecycle Manager v3.0.1' installLocation='/opt/IBM/SKLMV301'>
 <data key='eclipseLocation' value='/opt/IBM/SKLMV301'/>
 <data key='user.import.profile' value='false'/>
 <data key='cic.selector.os' value='linux'/>
 <data key='cic.selector.arch' value='s390x'/>
 <data key='cic.selector.ws' value='gtk'/>
 <data key='user.IS_SILENT_MODE,com.ibm.sklm301.linux' value='false'/>
 <data key='user.EKM_PROPFILE,com.ibm.sklm301.linux' value='/opt/IBM/KeyManagerConfig.properties'/>
 <data key='user.EKM_MIGRATION,com.ibm.sklm301.linux' value='false'/>
 <data key='user.PROFILE_NAME,com.ibm.sklm301.linux' value='KLMProfile'/>
 <data key='user.WAS_ADMIN_ID,com.ibm.sklm301.linux' value='wasadmin'/>
 <data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm301.linux' value='e9PjN93MeQxwnSs9VXJFMw=='/>
 <data key='user.WAS_ADMIN_CONF_PWD,com.ibm.sklm301.linux' value='e9PjN93MeQxwnSs9VXJFMw=='/>
 <data key='user.SKLM_ADMIN_USER,com.ibm.sklm301.linux' value='SKLMAdmin'/>
 <data key='user.SKLM_ADMIN_PASSWORD,com.ibm.sklm301.linux' value='9YTRJMRIydDSdfhaHPs1ag=='/>
 <data key='user.SKLM_ADMIN_CONF_PWD,com.ibm.sklm301.linux' value='9YTRJMRIydDSdfhaHPs1ag=='/>
 <data key='user.SKLM_APP_PORT,com.ibm.sklm301.linux' value='443'/>
 <data key='user.WAS_ADMIN_PORT,com.ibm.sklm301.linux' value='9083'/>
 <data key='user.SKLM_APP_NS_PORT,com.ibm.sklm301.linux' value='80'/>
 <data key='cic.selector.nl' value='en'/>
</profile>
<preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='/opt/IBM/IBMIMShared'/>
<preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30'/>
<preference name='com.ibm.cic.common.core.preferences.readTimeout' value='45'/>
<preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0'/>
<preference name='offering.service.repositories.areUsed' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.http.disablePreemptiveAuthentication' value='false'/>
<preference name='http.ntlm.auth.kind' value='NTLM'/>
<preference name='http.ntlm.auth.enableIntegrated.win32' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false'/>
<preference name='PassportAdvantageIsEnabled' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false'/>
<preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false'/>
<preference name='com.ibm.cic.common.sharedUI.showErrorLog' value='true'/>
<preference name='com.ibm.cic.common.sharedUI.showWarningLog' value='true'/>
<preference name='com.ibm.cic.common.sharedUI.showNoteLog' value='true'/>
</agent-input>
```

Nouvelle installation de la version 3.0.1 sur des systèmes Linux PPC

L'exemple de fichier de réponses contient des réponses pour une installation d'IBM Security Key Lifecycle Manager version 3.0.1 sur un système tel que Linux PPC, ou pour une installation dans laquelle la migration d'Encryption Key Manager se produit.

```
<?xml version="1.0" encoding="UTF-8"?>
<!--L'attribut "acceptLicense" est obsolète. La ligne de commande "-acceptLicense" permet d'accepter les contrats de licence.-->
<agent-input clean='true' >
 <server>
  <repository location='/disk1/im'/>
  <repository location='/disk1/'/>
 </server>
 <profile id='IBM Installation Manager' installLocation='/opt/IBM/InstallationManager/eclipse' kind='self'>
  <data key='eclipseLocation' value='/opt/IBM/InstallationManager/eclipse'/>
  <data key='user.import.profile' value='false'/>
  <data key='cic.selector.os' value='linux'/>
  <data key='cic.selector.arch' value='ppc64le'/>
  <data key='cic.selector.ws' value='gtk'/>
 </profile>
 <install modify='false'>
  <offering id='com.ibm.cic.agent'  profile='IBM Installation Manager' features='agent_core,agent_jre' installFixes='none'/>
  <offering id='com.ibm.sklm301.db2.lin.ofng'  profile='IBM DB2 SKLM301' features='main.feature' installFixes='none'/>
  <offering id='com.ibm.websphere.BASE.v90'  profile='IBM WebSphere Application Server V9.0'  features='core.feature,ejbdeploy,thinclien
  <offering id='com.ibm.java.jdk.v8' profile='IBM WebSphere Application Server V9.0'  features='com.ibm.sdk.8' installFixes='none'/>
  <offering id='com.ibm.sklm301.linux'  profile='IBM Security Key Lifecycle Manager v3.0.1' features='main.feature' installFixes='none'/
 </install>
 <profile id='IBM DB2 SKLM301' installLocation='/opt/IBM/DB2SKLMV301'>
  <data key='eclipseLocation' value='/opt/IBM/DB2SKLMV301'/>
  <data key='user.import.profile' value='false'/>
  <data key='cic.selector.os' value='linux'/>
  <data key='cic.selector.arch' value='ppc64le'/>
  <data key='cic.selector.ws' value='gtk'/>
  <data key='user.DB2_ADMIN_ID,com.ibm.sklm301.db2.lin.ofng' value='sklmdb31'/>
  <!--The DB2 Group name should not be more than 8 characters -->
  <data key='user.DB2_ADMIN_GRP,com.ibm.sklm301.db2.lin.ofng' value='sklmdb31'/>
```

```
 <data key='user.DB2_ADMIN_PWD,com.ibm.sklm301.db2.lin.ofng' value='QTh/0AiFvrljhs9gnOYkGA=='/>
 <data key='user.CONFIRM_PASSWORD,com.ibm.sklm301.db2.lin.ofng' value='QTh/0AiFvrljhs9gnOYkGA=='/>
 <data key='user.DB2_DB_HOME,com.ibm.sklm301.db2.lin.ofng' value='/home/sklmdb31'/>
 <data key='user.DB2_DB_LHOME,com.ibm.sklm301.db2.lin.ofng' value='/home/sklmdb31'/>
 <data key='user.DB2_DB_NAME,com.ibm.sklm301.db2.lin.ofng' value='SKLMDB31'/>
 <data key='user.DB2_DB_PORT,com.ibm.sklm301.db2.lin.ofng' value='50050'/>
 <data key='user.DB2_EXISTS,com.ibm.sklm301.db2.lin.ofng' value='false'/>
 <data key='user.DB2_LOCATION,com.ibm.sklm301.db2.lin.ofng' value='/opt/IBM/DB2SKLMV301'/>
 <data key='cic.selector.nl' value='en'/>
</profile>
<profile id='IBM WebSphere Application Server V9.0' installLocation='/opt/IBM/WebSphere/AppServer'>
 <data key='eclipseLocation' value='/opt/IBM/WebSphere/AppServer'/>
 <data key='user.import.profile' value='false'/>
 <data key='cic.selector.os' value='linux'/>
 <data key='cic.selector.arch' value='ppc64le'/>
 <data key='cic.selector.ws' value='gtk'/>
 <data key='cic.selector.nl' value='en'/>
</profile>
<profile id='IBM Security Key Lifecycle Manager v3.0.1' installLocation='/opt/IBM/SKLMV301'>
 <data key='eclipseLocation' value='/opt/IBM/SKLMV301'/>
 <data key='user.import.profile' value='false'/>
 <data key='cic.selector.os' value='linux'/>
 <data key='cic.selector.arch' value='ppc64le'/>
 <data key='cic.selector.ws' value='gtk'/>
 <data key='user.IS_SILENT_MODE,com.ibm.sklm301.linux' value='false'/>
 <data key='user.EKM_PROPFILE,com.ibm.sklm301.linux' value='/opt/IBM/KeyManagerConfig.properties'/>
 <data key='user.EKM_MIGRATION,com.ibm.sklm301.linux' value='false'/>
 <data key='user.PROFILE_NAME,com.ibm.sklm301.linux' value='KLMProfile'/>
 <data key='user.WAS_ADMIN_ID,com.ibm.sklm301.linux' value='wasadmin'/>
 <data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm301.linux' value='e9PjN93MeQxwnSs9VXJFMw=='/>
 <data key='user.WAS_ADMIN_CONF_PWD,com.ibm.sklm301.linux' value='e9PjN93MeQxwnSs9VXJFMw=='/>
 <data key='user.SKLM_ADMIN_USER,com.ibm.sklm301.linux' value='SKLMAdmin'/>
 <data key='user.SKLM_ADMIN_PASSWORD,com.ibm.sklm301.linux' value='9YTRJMRIydDSdfhaHPs1ag=='/>
 <data key='user.SKLM_ADMIN_CONF_PWD,com.ibm.sklm301.linux' value='9YTRJMRIydDSdfhaHPs1ag=='/>
 <data key='user.SKLM_APP_PORT,com.ibm.sklm301.linux' value='443'/>
 <data key='user.WAS_ADMIN_PORT,com.ibm.sklm301.linux' value='9083'/>
 <data key='user.SKLM_APP_NS_PORT,com.ibm.sklm301.linux' value='80'/>
 <data key='cic.selector.nl' value='en'/>
</profile>
<preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='/opt/IBM/IBMIMShared'/>
<preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30'/>
<preference name='com.ibm.cic.common.core.preferences.readTimeout' value='45'/>
<preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0'/>
<preference name='offering.service.repositories.areUsed' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.http.disablePreemptiveAuthentication' value='false'/>
<preference name='http.ntlm.auth.kind' value='NTLM'/>
<preference name='http.ntlm.auth.enableIntegrated.win32' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false'/>
<preference name='PassportAdvantageIsEnabled' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false'/>
<preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false'/>
<preference name='com.ibm.cic.common.sharedUI.showErrorLog' value='true'/>
<preference name='com.ibm.cic.common.sharedUI.showWarningLog' value='true'/>
<preference name='com.ibm.cic.common.sharedUI.showNoteLog' value='true'/>
</agent-input>
```

Nouvelle installation de la version 3.0.1 sur des systèmes AIX

L'exemple de fichier de réponses contient des réponses pour une installation d'IBM Security Key Lifecycle Manager version 3.0.1 sur des systèmes AIX ou une installation dans laquelle la migration d'Encryption Key Manager se produit.

```
<?xml version="1.0" encoding="UTF-8"?>
<!--L'attribut "acceptLicense" est obsolète. La ligne de commande "-acceptLicense" permet d'accepter les contrats de licence.-->
<agent-input clean='true' >
<server>
 <repository location='/disk1/im'/>
 <repository location='/disk1/'/>
</server>
<profile id='IBM Installation Manager' installLocation='/opt/IBM/InstallationManager/eclipse' kind='self'>
 <data key='eclipseLocation' value='/opt/IBM/InstallationManager/eclipse'/>
 <data key='user.import.profile' value='false'/>
 <data key='cic.selector.os' value='aix'/>
 <data key='cic.selector.arch' value='ppc'/>
 <data key='cic.selector.ws' value='gtk'/>
</profile>
<install modify='false'>
<offering id='com.ibm.cic.agent'  profile='IBM Installation Manager' features='agent_core,agent_jre' installFixes='none'/>
<offering id='com.ibm.sklm301.db2.aix.ofng'  profile='IBM DB2 SKLM301' features='main.feature' installFixes='none'/>
<offering id='com.ibm.websphere.BASE.v90'  profile='IBM WebSphere Application Server V9.0' features='core.feature,ejbdeploy,thinclier
<offering id='com.ibm.java.jdk.v8' profile='IBM WebSphere Application Server V9.0' features='com.ibm.sdk.8' installFixes='none'/>
<offering id='com.ibm.sklm301.aix' profile='IBM Security Key Lifecycle Manager v3.0.1' features='main.feature' installFixes='none'/>
</install>
<profile id='IBM DB2 SKLM301' installLocation='/opt/IBM/DB2SKLMV301'>
<data key='eclipseLocation' value='/opt/IBM/DB2SKLMV301'/>
<data key='user.import.profile' value='false'/>
```

```
<data key='cic.selector.os' value='aix'/>
<data key='cic.selector.arch' value='ppc64'/>
<data key='cic.selector.ws' value='gtk'/>
<data key='user.DB2_ADMIN_ID,com.ibm.sklm301.db2.aix.ofng' value='sklmdb31'/>
<!--The DB2 Group name should not be more than 8 characters -->
<data key='user.DB2_ADMIN_GRP,com.ibm.sklm301.db2.aix.ofng' value='bin'/>
<data key='user.DB2_ADMIN_PWD,com.ibm.sklm301.db2.aix.ofng' value='QTh/0AiFvrljhs9gnOYkGA=='/>
<data key='user.CONFIRM_PASSWORD,com.ibm.sklm301.db2.aix.ofng' value='QTh/0AiFvrljhs9gnOYkGA=='/>
<data key='user.DB2_DB_HOME,com.ibm.sklm301.db2.aix.ofng' value='/home/sklmdb31'/>
<data key='user.DB2_DB_NAME,com.ibm.sklm301.db2.aix.ofng' value='SKLMDB31'/>
<data key='user.DB2_DB_PORT,com.ibm.sklm301.db2.aix.ofng' value='50050'/>
<data key='user.DB2_EXISTS,com.ibm.sklm301.db2.aix.ofng' value='false'/>
<data key='user.DB2_LOCATION,com.ibm.sklm301.db2.aix.ofng' value='/opt/IBM/DB2SKLMV301'/>
<data key='cic.selector.nl' value='en'/>
</profile>
<profile id='IBM WebSphere Application Server V9.0' installLocation='/usr/IBM/WebSphere/AppServer'>
<data key='eclipseLocation' value='/usr/IBM/WebSphere/AppServer'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='aix'/>
<data key='cic.selector.arch' value='ppc64'/>
<data key='cic.selector.ws' value='gtk'/>
<data key='cic.selector.nl' value='en'/>
</profile>
<profile id='IBM Security Key Lifecycle Manager v3.0.1' installLocation='/opt/IBM/SKLMV301'>
<data key='eclipseLocation' value='/opt/IBM/SKLMV301'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='aix'/>
<data key='cic.selector.arch' value='ppc64'/>
<data key='cic.selector.ws' value='gtk'/>
<data key='user.IS_SILENT_MODE,com.ibm.sklm301.linux' value='false'/>
<data key='user.EKM_PROPFILE,com.ibm.sklm301.aix' value='/opt/IBM/KeyManagerConfig.properties'/>
<data key='user.EKM_MIGRATION,com.ibm.sklm301.aix' value='false'/>
<data key='user.PROFILE_NAME,com.ibm.sklm301.aix' value='KLMProfile'/>
<data key='user.WAS_ADMIN_ID,com.ibm.sklm301.aix' value='wasadmin'/>
<data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm301.aix' value='e9PjN93MeQxwnSs9VXJFMw=='/>
<data key='user.WAS_ADMIN_CONF_PWD,com.ibm.sklm301.aix' value='e9PjN93MeQxwnSs9VXJFMw=='/>
<data key='user.SKLM_ADMIN_USER,com.ibm.sklm301.aix' value='SKLMAdmin'/>
<data key='user.SKLM_ADMIN_PASSWORD,com.ibm.sklm301.aix' value='9YTRJMRIydDSdfhaHPs1ag=='/>
<data key='user.SKLM_ADMIN_CONF_PWD,com.ibm.sklm301.aix' value='9YTRJMRIydDSdfhaHPs1ag=='/>
<data key='user.SKLM_APP_PORT,com.ibm.sklm301.aix' value='443'/>
<data key='user.WAS_ADMIN_PORT,com.ibm.sklm301.aix' value='9083'/>
<data key='user.SKLM_APP_NS_PORT,com.ibm.sklm301.aix' value='80'/>
 <data key='cic.selector.nl' value='en'/>
</profile>
<preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='/opt/IBM/IBMIMShared'/>
<preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30'/>
<preference name='com.ibm.cic.common.core.preferences.readTimeout' value='45'/>
<preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0'/>
<preference name='offering.service.repositories.areUsed' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.http.disablePreemptiveAuthentication' value='false'/>
<preference name='http.ntlm.auth.kind' value='NTLM'/>
<preference name='http.ntlm.auth.enableIntegrated.win32' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false'/>
<preference name='PassportAdvantageIsEnabled' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false'/>
<preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false'/>
<preference name='com.ibm.cic.common.sharedUI.showErrorLog' value='true'/>
<preference name='com.ibm.cic.common.sharedUI.showWarningLog' value='true'/>
<preference name='com.ibm.cic.common.sharedUI.showNoteLog' value='true'/>
</agent-input>
```

Migration des versions antérieures 2.5, 2.6, 2.7 et 3.0 vers la version 3.0.1 sur des systèmes Windows

Les exemples de fichiers de réponses contiennent des réponses pour une installation sur un système Windows sur lequel la migration des versions antérieures 2.5, 2.6, 2.7 et 3.0 d'IBM Security Key Lifecycle Manager vers la version 3.0.1 est effectuée.

Remarque : Pour déterminer s'il existe une installation d'IBM Security Key Lifecycle Manager d'une version antérieure nécessitant une migration, utilisez la commande **tklmVersionInfo**. Par exemple, entrez la commande suivante dans une session Jython :

```
print AdminTask.tklmVersionInfo<>
```

Migration de la version 2.5 vers la version 3.0.1

```
<agent-input clean='true' >
  <server>
    <repository location='C:\disk1'/>
    <repository location='C:\disk1\im'/>
  </server>
    <install modify='false'>
  <offering profile='IBM Installation Manager' id='com.ibm.cic.agent' features='agent_core,agent_jre,agent_web'
   installFixes='none'/>
    <offering profile='IBM DB2 SKLM30' id='com.ibm.sklm30.db2.win.ofng' version='11.1.2.2' features='main.feature'
   installFixes='none'/>
    <offering profile='IBM WebSphere Application Server V9.0' id='com.ibm.websphere.BASE.v90'
    features='core.feature,ejbdeploy,thinclient,embeddablecontainer' installFixes='none'/>
    <offering profile='IBM WebSphere Application Server V9.0' id='com.ibm.java.jdk.v8'
    features='com.ibm.sdk.8' installFixes='none'/>
    <offering profile='IBM Security Key Lifecycle Manager v3.0' id='com.ibm.sklm30.win' version='3.0.0.0'
    features='main.feature' installFixes='none'/>
  </install>
  <profile id='IBM DB2 SKLM30' installLocation='C:\Program Files\IBM\DB2SKLMV30'>
    <data key='eclipseLocation' value='C:\Program Files\IBM\DB2SKLMV30'/>
    <data key='user.import.profile' value='false'/>
    <data key='cic.selector.os' value='win32'/>
    <data key='cic.selector.arch' value='x86_64'/>
    <data key='cic.selector.ws' value='win32'/>
    <data key='cic.selector.nl' value='en'/>
    <data key='user.DB2_ADMIN_ID,com.ibm.sklm30.db2.win.ofng' value='sklmdb30'/>
    <data key='user.DB2_ADMIN_PWD,com.ibm.sklm30.db2.win.ofng' value='QTh/0AiFvrljhs9gnOYkGA=='/>
    <data key='user.CONFIRM_PASSWORD,com.ibm.sklm30.db2.win.ofng' value='QTh/0AiFvrljhs9gnOYkGA=='/>
    <data key='user.DB2_DB_HOME,com.ibm.sklm30.db2.win.ofng' value='C:'/>
    <data key='user.DB2_DB_NAME,com.ibm.sklm30.db2.win.ofng' value='SKLMDB30'/>
    <data key='user.DB2_DB_PORT,com.ibm.sklm30.db2.win.ofng' value='50040'/>
    <data key='user.DB2_EXISTS,com.ibm.sklm30.db2.win.ofng' value='false'/>
    <data key='user.DB2_LOCATION,com.ibm.sklm30.db2.win.ofng' value='C:\\Program Files\\IBM\\DB2SKLMV30'/>
  </profile>
  <profile id='IBM WebSphere Application Server V9.0' installLocation='C:\Program Files\IBM\WebSphere30\AppServer'>
    <data key='eclipseLocation' value='C:\Program Files\IBM\WebSphere30\AppServer'/>
    <data key='user.import.profile' value='false'/>
    <data key='cic.selector.os' value='win32'/>
    <data key='cic.selector.arch' value='x86_64'/>
    <data key='cic.selector.ws' value='win32'/>
    <data key='cic.selector.nl' value='en'/>
  </profile>

  <profile id='IBM Security Key Lifecycle Manager v3.0' installLocation='C:\Program Files\IBM\SKLMV30'>
    <data key='eclipseLocation' value='C:\Program Files\IBM\SKLMV30'/>
    <data key='user.import.profile' value='false'/>
    <data key='cic.selector.os' value='win32'/>
    <data key='cic.selector.arch' value='x86_64'/>
    <data key='cic.selector.ws' value='win32'/>
 <data key='user.EKM_PROPFILE,com.ibm.sklm30.win' value='C:\KeyManagerConfig.properties'/>
 <data key='user.EKM_MIGRATION,com.ibm.sklm30.win' value='false'/>
    <data key='user.IS_SILENT_MODE,com.ibm.sklm30.win' value='false'/>
    <data key='cic.selector.nl' value='en'/>
    <data key='user.PROFILE_NAME,com.ibm.sklm30.win' value='KLMProfile'/>
    <data key='user.WAS_HOME,com.ibm.sklm30.win' value='C:\Program Files\IBM\WebSphere30\AppServer'/>
    <data key='user.WAS_ADMIN_ID,com.ibm.sklm30.win' value='wasadmin'/>
    <data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm30.win' value='e9PjN93MeQxwnSs9VXJFMw=='/>
    <data key='user.WAS_ADMIN_CONF_PWD,com.ibm.sklm30.win' value='e9PjN93MeQxwnSs9VXJFMw=='/>
    <data key='user.SKLM_ADMIN_USER,com.ibm.sklm30.win' value='SKLMAdmin'/>
    <data key='user.SKLM_ADMIN_PASSWORD,com.ibm.sklm30.win' value='9YTRJMRIydDSdfhaHPs1ag=='/>
    <data key='user.SKLM_ADMIN_CONF_PWD,com.ibm.sklm30.win' value='9YTRJMRIydDSdfhaHPs1ag=='/>
    <data key='user.TKLM_VERSION,com.ibm.sklm30.win' value='2.5.0.4'/>
    <data key='user.TKLM_TIP_HOME,com.ibm.sklm30.win' value='C:\Program Files (x86)\IBM\WebSphere\AppServer'/>
    <data key='user.TKLM_INSTALLED,com.ibm.sklm30.win' value='true'/>
    <data key='user.TKLM_DB_PWD,com.ibm.sklm30.win' value='SwIhGBTDHcJok80Ux4Sb3g=='/>
 <data key='user.TKLM_KEYSTORE_PWD,com.ibm.sklm30.win' value='fufgZbY47EfxLYarBAIxeQ=='/>
 <data key='user.SKLM_APP_PORT,com.ibm.sklm30.win' value='443'/>
 <data key='user.WAS_ADMIN_PORT,com.ibm.sklm30.win' value='9083'/>
 <data key='user.SKLM_APP_NS_PORT,com.ibm.sklm30.win' value='80'/>
  </profile>

  <preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='C:\Program Files (x86)\IBM\IBMIMShared'/>
  <preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30'/>
  <preference name='com.ibm.cic.common.core.preferences.readTimeout' value='45'/>
  <preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0'/>
  <preference name='offering.service.repositories.areUsed' value='true'/>
  <preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false'/>
  <preference name='com.ibm.cic.common.core.preferences.http.disablePreemptiveAuthentication' value='false'/>
  <preference name='http.ntlm.auth.kind' value='NTLM'/>
  <preference name='http.ntlm.auth.enableIntegrated.win32' value='true'/>
  <preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true'/>
  <preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false'/>
  <preference name='PassportAdvantageIsEnabled' value='false'/>
  <preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false'/>
  <preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false'/>
  <preference name='com.ibm.cic.common.sharedUI.showErrorLog' value='true'/>
  <preference name='com.ibm.cic.common.sharedUI.showWarningLog' value='true'/>
  <preference name='com.ibm.cic.common.sharedUI.showNoteLog' value='true'/>
</agent-input>
```

Migration de la version 2.6 vers la version 3.0.1

```
<!-- insta -->
<agent-input clean='true' >
  <server>
    <repository location='C:\disk1'/>
    <repository location='C:\disk1\im'/>
  </server>
    <install modify='false'>
  <offering profile='IBM Installation Manager' id='com.ibm.cic.agent' features='agent_core,agent_jre,agent_web' installFixes='none'/>
    <offering profile='IBM DB2 SKLM301' id='com.ibm.sklm301.db2.win.ofng' version='11.1.2.2' features='main.feature' installFixes='none'
    <offering profile='IBM WebSphere Application Server V9.0' id='com.ibm.websphere.BASE.v90'  features='core.feature,ejbdeploy,thinclie
    <offering profile='IBM WebSphere Application Server V9.0' id='com.ibm.java.jdk.v8' features='com.ibm.sdk.8' installFixes='none'/>
    <offering profile='IBM Security Key Lifecycle Manager v3.0.1' id='com.ibm.sklm301.win' version='3.0.1000.00' features='main.feature'
  </install>
  <profile id='IBM DB2 SKLM301' installLocation='C:\Program Files\IBM\DB2SKLMV301'>
    <data key='eclipseLocation' value='C:\Program Files\IBM\DB2SKLMV301'/>
    <data key='user.import.profile' value='false'/>
    <data key='cic.selector.os' value='win32'/>
    <data key='cic.selector.arch' value='x86_64'/>
    <data key='cic.selector.ws' value='win32'/>
    <data key='cic.selector.nl' value='en'/>
    <data key='user.DB2_ADMIN_ID,com.ibm.sklm301.db2.win.ofng' value='sklmdb31'/>
    <data key='user.DB2_ADMIN_PWD,com.ibm.sklm301.db2.win.ofng' value='QTh/0AiFvrljhs9gnOYkGA=='/>
    <data key='user.CONFIRM_PASSWORD,com.ibm.sklm301.db2.win.ofng' value='QTh/0AiFvrljhs9gnOYkGA=='/>
    <data key='user.DB2_DB_HOME,com.ibm.sklm301.db2.win.ofng' value='C:'/>
    <data key='user.DB2_DB_NAME,com.ibm.sklm301.db2.win.ofng' value='SKLMDB31'/>
    <data key='user.DB2_DB_PORT,com.ibm.sklm301.db2.win.ofng' value='50050'/>
    <data key='user.DB2_EXISTS,com.ibm.sklm301.db2.win.ofng' value='false'/>
    <data key='user.DB2_LOCATION,com.ibm.sklm301.db2.win.ofng' value='C:\\Program Files\\IBM\\DB2SKLMV301'/>
  </profile>
  <profile id='IBM WebSphere Application Server V9.0' installLocation='C:\Program Files\IBM\WebSphere30\AppServer'>
    <data key='eclipseLocation' value='C:\Program Files\IBM\WebSphere30\AppServer'/>
    <data key='user.import.profile' value='false'/>
    <data key='cic.selector.os' value='win32'/>
    <data key='cic.selector.arch' value='x86_64'/>
    <data key='cic.selector.ws' value='win32'/>
    <data key='cic.selector.nl' value='en'/>
  </profile>

  <profile id='IBM Security Key Lifecycle Manager v3.0.1' installLocation='C:\Program Files\IBM\SKLMV301'>
    <data key='eclipseLocation' value='C:\Program Files\IBM\SKLMV301'/>
    <data key='user.import.profile' value='false'/>
    <data key='cic.selector.os' value='win32'/>
    <data key='cic.selector.arch' value='x86_64'/>
    <data key='cic.selector.ws' value='win32'/>
 <data key='user.EKM_PROPFILE,com.ibm.sklm301.win' value='C:\KeyManagerConfig.properties'/>
 <data key='user.EKM_MIGRATION,com.ibm.sklm301.win' value='false'/>
    <data key='user.IS_SILENT_MODE,com.ibm.sklm301.win' value='false'/>
    <data key='cic.selector.nl' value='en'/>
    <data key='user.PROFILE_NAME,com.ibm.sklm301.win' value='KLMProfile'/>
    <data key='user.WAS_HOME,com.ibm.sklm301.win' value='C:\Program Files\IBM\WebSphere30\AppServer'/>
    <data key='user.WAS_ADMIN_ID,com.ibm.sklm301.win' value='wasadmin'/>
    <data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm301.win' value='e9PjN93MeQxwnSs9VXJFMw=='/>
    <data key='user.WAS_ADMIN_CONF_PWD,com.ibm.sklm301.win' value='e9PjN93MeQxwnSs9VXJFMw=='/>
    <data key='user.SKLM_ADMIN_USER,com.ibm.sklm301.win' value='SKLMAdmin'/>
    <data key='user.SKLM_ADMIN_PASSWORD,com.ibm.sklm301.win' value='9YTRJMRIydDSdfhaHPs1ag=='/>
    <data key='user.SKLM_ADMIN_CONF_PWD,com.ibm.sklm301.win' value='9YTRJMRIydDSdfhaHPs1ag=='/>
    <data key='user.TKLM_VERSION,com.ibm.sklm301.win' value='2.6.0.2'/>
    <data key='user.TKLM_TIP_HOME,com.ibm.sklm301.win' value='C:\Program Files (x86)\IBM\WebSphere\AppServer'/>
    <data key='user.TKLM_INSTALLED,com.ibm.sklm301.win' value='true'/>
    <data key='user.TKLM_DB_PWD,com.ibm.sklm301.win' value='Fr4dMn3eZtW5WgCojtMXrg==/>
 <data key='user.TKLM_KEYSTORE_PWD,com.ibm.sklm301.win' value='fufgZbY47EfxLYarBAIxeQ==/>
 <data key='user.SKLM_APP_PORT,com.ibm.sklm301.win' value='443'/>
 <data key='user.WAS_ADMIN_PORT,com.ibm.sklm301.win' value='9083'/>
 <data key='user.SKLM_APP_NS_PORT,com.ibm.sklm301.win' value='80'/>
  </profile>

  <preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='C:\Program Files (x86)\IBM\IBMIMShared'/>
  <preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30'/>
  <preference name='com.ibm.cic.common.core.preferences.readTimeout' value='45'/>
  <preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0'/>
  <preference name='offering.service.repositories.areUsed' value='true'/>
  <preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false'/>
  <preference name='com.ibm.cic.common.core.preferences.http.disablePreemptiveAuthentication' value='false'/>
  <preference name='http.ntlm.auth.kind' value='NTLM'/>
  <preference name='http.ntlm.auth.enableIntegrated.win32' value='true'/>
  <preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true'/>
  <preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false'/>
  <preference name='PassportAdvantageIsEnabled' value='false'/>
  <preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false'/>
  <preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false'/>
  <preference name='com.ibm.cic.common.sharedUI.showErrorLog' value='true'/>
  <preference name='com.ibm.cic.common.sharedUI.showWarningLog' value='true'/>
  <preference name='com.ibm.cic.common.sharedUI.showNoteLog' value='true'/>
</agent-input>
```

Migration de la version 2.7 vers la version 3.0.1

```
<!-- insta -->
<agent-input clean='true' >
  <server>
    <repository location='C:\disk1'/>
    <repository location='C:\disk1\im'/>
  </server>
    <install modify='false'>
  <offering profile='IBM Installation Manager' id='com.ibm.cic.agent' features='agent_core,agent_jre,agent_web' installFixes='none'/>
    <offering profile='IBM DB2 SKLM301' id='com.ibm.sklm301.db2.win.ofng' version='11.1.2.2' features='main.feature' installFixes='no
    <offering profile='IBM WebSphere Application Server V9.0_1' id='com.ibm.websphere.BASE.v90'  features='core.feature,ejbdeploy,thi
    <offering profile='IBM WebSphere Application Server V9.0_1' id='com.ibm.java.jdk.v8' features='com.ibm.sdk.8' installFixes='none'
    <offering profile='IBM Security Key Lifecycle Manager v3.0.1' id='com.ibm.sklm301.win' version='3.0.1000.00' features='main.featu
  </install>
  <profile id='IBM DB2 SKLM301' installLocation='C:\Program Files\IBM\DB2SKLMV301'>
    <data key='eclipseLocation' value='C:\Program Files\IBM\DB2SKLMV301'/>
    <data key='user.import.profile' value='false'/>
    <data key='cic.selector.os' value='win32'/>
    <data key='cic.selector.arch' value='x86_64'/>
    <data key='cic.selector.ws' value='win32'/>
    <data key='cic.selector.nl' value='en'/>
    <data key='user.DB2_ADMIN_ID,com.ibm.sklm301.db2.win.ofng' value='sklmdb31'/>
    <data key='user.DB2_ADMIN_PWD,com.ibm.sklm301.db2.win.ofng' value='QTh/0AiFvrljhs9gnOYkGA=='/>
    <data key='user.CONFIRM_PASSWORD,com.ibm.sklm301.db2.win.ofng' value='QTh/0AiFvrljhs9gnOYkGA=='/>
    <data key='user.DB2_DB_HOME,com.ibm.sklm301.db2.win.ofng' value='C:'/>
    <data key='user.DB2_DB_NAME,com.ibm.sklm301.db2.win.ofng' value='SKLMDB31'/>
    <data key='user.DB2_DB_PORT,com.ibm.sklm301.db2.win.ofng' value='50050'/>
    <data key='user.DB2_EXISTS,com.ibm.sklm301.db2.win.ofng' value='false'/>
    <data key='user.DB2_LOCATION,com.ibm.sklm301.db2.win.ofng' value='C:\\Program Files\\IBM\\DB2SKLMV301'/>
  </profile>
  <profile id='IBM WebSphere Application Server V9.0_1' installLocation='C:\Program Files\IBM\WebSphere30\AppServer'>
    <data key='eclipseLocation' value='C:\Program Files\IBM\WebSphere30\AppServer'/>
    <data key='user.import.profile' value='false'/>
    <data key='cic.selector.os' value='win32'/>
    <data key='cic.selector.arch' value='x86_64'/>
    <data key='cic.selector.ws' value='win32'/>
    <data key='cic.selector.nl' value='en'/>
  </profile>

  <profile id='IBM Security Key Lifecycle Manager v3.0.1' installLocation='C:\Program Files\IBM\SKLMV301'>
    <data key='eclipseLocation' value='C:\Program Files\IBM\SKLMV301'/>
    <data key='user.import.profile' value='false'/>
    <data key='cic.selector.os' value='win32'/>
    <data key='cic.selector.arch' value='x86_64'/>
    <data key='cic.selector.ws' value='win32'/>
 <data key='user.EKM_PROPFILE,com.ibm.sklm301.win' value='C:\KeyManagerConfig.properties'/>
 <data key='user.EKM_MIGRATION,com.ibm.sklm301.win' value='false'/>
    <data key='user.IS_SILENT_MODE,com.ibm.sklm301.win' value='false'/>
    <data key='cic.selector.nl' value='en'/>
    <data key='user.PROFILE_NAME,com.ibm.sklm301.win' value='KLMProfile'/>
    <data key='user.WAS_HOME,com.ibm.sklm301.win' value='C:\Program Files\IBM\WebSphere30\AppServer'/>
    <data key='user.WAS_ADMIN_ID,com.ibm.sklm301.win' value='wasadmin'/>
    <data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm301.win' value='e9PjN93MeQxwnSs9VXJFMw=='/>
    <data key='user.WAS_ADMIN_CONF_PWD,com.ibm.sklm301.win' value='e9PjN93MeQxwnSs9VXJFMw=='/>
    <data key='user.SKLM_ADMIN_USER,com.ibm.sklm301.win' value='SKLMAdmin'/>
    <data key='user.SKLM_ADMIN_PASSWORD,com.ibm.sklm301.win' value='9YTRJMRIydDSdfhaHPs1ag=='/>
    <data key='user.SKLM_ADMIN_CONF_PWD,com.ibm.sklm301.win' value='9YTRJMRIydDSdfhaHPs1ag=='/>
    <data key='user.TKLM_VERSION,com.ibm.sklm301.win' value='2.7.0.0'/>
    <data key='user.TKLM_TIP_HOME,com.ibm.sklm301.win' value='C:\Program Files\IBM\WebSphere\AppServer'/>
    <data key='user.TKLM_INSTALLED,com.ibm.sklm301.win' value='true'/>
    <data key='user.TKLM_DB_PWD,com.ibm.sklm301.win' value='SwIhGBTDHcJok80Ux4Sb3g=='/>
 <data key='user.TKLM_KEYSTORE_PWD,com.ibm.sklm301.win' value='m4oQ5vWqvwGUwOgZaAiFqg=='/>
 <data key='user.SKLM_APP_PORT,com.ibm.sklm301.win' value='443'/>
 <data key='user.WAS_ADMIN_PORT,com.ibm.sklm301.win' value='9083'/>
 <data key='user.SKLM_APP_NS_PORT,com.ibm.sklm301.win' value='80'/>
  </profile>

  <preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='C:\Program Files\IBM\IBMIMShared'/>
  <preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30'/>
  <preference name='com.ibm.cic.common.core.preferences.readTimeout' value='45'/>
  <preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0'/>
  <preference name='offering.service.repositories.areUsed' value='true'/>
  <preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false'/>
  <preference name='com.ibm.cic.common.core.preferences.http.disablePreemptiveAuthentication' value='false'/>
  <preference name='http.ntlm.auth.kind' value='NTLM'/>
  <preference name='http.ntlm.auth.enableIntegrated.win32' value='true'/>
  <preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true'/>
  <preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false'/>
  <preference name='PassportAdvantageIsEnabled' value='false'/>
  <preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false'/>
  <preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false'/>
  <preference name='com.ibm.cic.common.sharedUI.showErrorLog' value='true'/>
  <preference name='com.ibm.cic.common.sharedUI.showWarningLog' value='true'/>
  <preference name='com.ibm.cic.common.sharedUI.showNoteLog' value='true'/>
</agent-input>
```

Migration de la version 3.0 vers la version 3.0.1

```
<!-- insta -->
<agent-input clean='true' >
  <server>
    <repository location='C:\disk1'/>
    <repository location='C:\disk1\im'/>
  </server>
    <install modify='false'>
  <offering profile='IBM Installation Manager' id='com.ibm.cic.agent' features='agent_core,agent_jre,agent_web' installFixes='none'/>
    <offering profile='IBM DB2 SKLM301' id='com.ibm.sklm301.db2.win.ofng' version='11.1.2.2' features='main.feature' installFixes='none'
    <offering profile='IBM WebSphere Application Server V9.0_1' id='com.ibm.websphere.BASE.v90'  features='core.feature,ejbdeploy,thincl
    <offering profile='IBM WebSphere Application Server V9.0_1' id='com.ibm.java.jdk.v8' features='com.ibm.sdk.8' installFixes='none'/>
    <offering profile='IBM Security Key Lifecycle Manager v3.0.1' id='com.ibm.sklm301.win' version='3.0.1000.00' features='main.feature'
  </install>
  <profile id='IBM DB2 SKLM301' installLocation='C:\Program Files\IBM\DB2SKLMV301'>
    <data key='eclipseLocation' value='C:\Program Files\IBM\DB2SKLMV301'/>
    <data key='user.import.profile' value='false'/>
    <data key='cic.selector.os' value='win32'/>
    <data key='cic.selector.arch' value='x86_64'/>
    <data key='cic.selector.ws' value='win32'/>
    <data key='cic.selector.nl' value='en'/>
    <data key='user.DB2_ADMIN_ID,com.ibm.sklm301.db2.win.ofng' value='sklmdb31'/>
    <data key='user.DB2_ADMIN_PWD,com.ibm.sklm301.db2.win.ofng' value='QTh/0AiFvrljhs9gnOYkGA=='/>
    <data key='user.CONFIRM_PASSWORD,com.ibm.sklm301.db2.win.ofng' value='QTh/0AiFvrljhs9gnOYkGA=='/>
    <data key='user.DB2_DB_HOME,com.ibm.sklm301.db2.win.ofng' value='C:'/>
    <data key='user.DB2_DB_NAME,com.ibm.sklm301.db2.win.ofng' value='SKLMDB31'/>
    <data key='user.DB2_DB_PORT,com.ibm.sklm301.db2.win.ofng' value='50050'/>
    <data key='user.DB2_EXISTS,com.ibm.sklm301.db2.win.ofng' value='false'/>
    <data key='user.DB2_LOCATION,com.ibm.sklm301.db2.win.ofng' value='C:\\Program Files\\IBM\\DB2SKLMV301'/>
  </profile>
  <profile id='IBM WebSphere Application Server V9.0_1' installLocation='C:\Program Files\IBM\WebSphere30\AppServer'>
    <data key='eclipseLocation' value='C:\Program Files\IBM\WebSphere30\AppServer'/>
    <data key='user.import.profile' value='false'/>
    <data key='cic.selector.os' value='win32'/>
    <data key='cic.selector.arch' value='x86_64'/>
    <data key='cic.selector.ws' value='win32'/>
    <data key='cic.selector.nl' value='en'/>
  </profile>

  <profile id='IBM Security Key Lifecycle Manager v3.0.1' installLocation='C:\Program Files\IBM\SKLMV301'>
    <data key='eclipseLocation' value='C:\Program Files\IBM\SKLMV301'/>
    <data key='user.import.profile' value='false'/>
    <data key='cic.selector.os' value='win32'/>
    <data key='cic.selector.arch' value='x86_64'/>
    <data key='cic.selector.ws' value='win32'/>
 <data key='user.EKM_PROPFILE,com.ibm.sklm301.win' value='C:\KeyManagerConfig.properties'/>
 <data key='user.EKM_MIGRATION,com.ibm.sklm301.win' value='false'/>
    <data key='user.IS_SILENT_MODE,com.ibm.sklm301.win' value='false'/>
    <data key='cic.selector.nl' value='en'/>
    <data key='user.PROFILE_NAME,com.ibm.sklm301.win' value='KLMProfile'/>
    <data key='user.WAS_HOME,com.ibm.sklm301.win' value='C:\Program Files\IBM\WebSphere30\AppServer'/>
    <data key='user.WAS_ADMIN_ID,com.ibm.sklm301.win' value='wasadmin'/>
    <data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm301.win' value='e9PjN93MeQxwnSs9VXJFMw=='/>
    <data key='user.WAS_ADMIN_CONF_PWD,com.ibm.sklm301.win' value='e9PjN93MeQxwnSs9VXJFMw=='/>
    <data key='user.SKLM_ADMIN_USER,com.ibm.sklm301.win' value='SKLMAdmin'/>
    <data key='user.SKLM_ADMIN_PASSWORD,com.ibm.sklm301.win' value='9YTRJMRIydDSdfhaHPs1ag=='/>
    <data key='user.SKLM_ADMIN_CONF_PWD,com.ibm.sklm301.win' value='9YTRJMRIydDSdfhaHPs1ag=='/>
    <data key='user.TKLM_VERSION,com.ibm.sklm301.win' value='3.0.0.0'/>
    <data key='user.TKLM_TIP_HOME,com.ibm.sklm301.win' value='C:\Program Files\IBM\WebSphere\AppServer'/>
    <data key='user.TKLM_INSTALLED,com.ibm.sklm301.win' value='true'/>
    <data key='user.INSTALL_AS_FP,com.ibm.sklm301.win' value='false'/>
    <data key='user.TKLM_DB_PWD,com.ibm.sklm301.win' value='SwIhGBTDHcJok80Ux4Sb3g=='/>
 <data key='user.TKLM_KEYSTORE_PWD,com.ibm.sklm301.win' value='m4oQ5vWqvwGUwOgZaAiFqg=='/>
 <data key='user.SKLM_APP_PORT,com.ibm.sklm301.win' value='443'/>
 <data key='user.WAS_ADMIN_PORT,com.ibm.sklm301.win' value='9083'/>
 <data key='user.SKLM_APP_NS_PORT,com.ibm.sklm301.win' value='80'/>
  </profile>

  <preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='C:\Program Files\IBM\IBMIMShared'/>
  <preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30'/>
  <preference name='com.ibm.cic.common.core.preferences.readTimeout' value='45'/>
  <preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0'/>
  <preference name='offering.service.repositories.areUsed' value='true'/>
  <preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false'/>
  <preference name='com.ibm.cic.common.core.preferences.http.disablePreemptiveAuthentication' value='false'/>
  <preference name='http.ntlm.auth.kind' value='NTLM'/>
  <preference name='http.ntlm.auth.enableIntegrated.win32' value='true'/>
  <preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true'/>
  <preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false'/>
  <preference name='PassportAdvantageIsEnabled' value='false'/>
  <preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false'/>
  <preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false'/>
  <preference name='com.ibm.cic.common.sharedUI.showErrorLog' value='true'/>
  <preference name='com.ibm.cic.common.sharedUI.showWarningLog' value='true'/>
  <preference name='com.ibm.cic.common.sharedUI.showNoteLog' value='true'/>
</agent-input>
```

Migration des versions 2.5, 2.6, 2.7 et 3.0 vers la version 3.0.1 sur des systèmes Linux

Les exemples de fichiers de réponses contiennent des réponses pour une installation sur un système Linux sur lequel la migration d'une version 2.5, 2.6, 2.7 et 3.0 précédente d'IBM Security Key Lifecycle Manager vers la version 3.0.1 est effectuée.

Remarque : Pour déterminer s'il existe une installation d'IBM Security Key Lifecycle Manager d'une version antérieure nécessitant une migration, utilisez la commande **tklmVersionInfo**. Par exemple, entrez la commande suivante dans une session Jython :

```
print AdminTask.tklmVersionInfo<>
```

Migration de la version 2.5 vers la version 3.0.1

```
<?xml version='1.0' encoding='UTF-8'?>
<agent-input clean='true' >
  <server>
    <repository location='/disk1'/>
    <repository location='/disk1/im'/>
  </server>
   <install modify='false'>
 <offering profile='IBM Installation Manager'  id='com.ibm.cic.agent'  features='agent_core,agent_jre,agent_web' installFixes='none'/
    <offering profile='IBM WebSphere Application Server V9.0' id='com.ibm.websphere.BASE.v90' features='core.feature,ejbdeploy,thincl
    <offering profile='IBM WebSphere Application Server V9.0' id='com.ibm.java.jdk.v8' features='com.ibm.sdk.8' installFixes='none'/>
    <offering profile='IBM DB2 SKLM301' id='com.ibm.sklm301.db2.lin.ofng' version='11.1.2.2' features='main.feature' installFixes='no
    <offering profile='IBM Security Key Lifecycle Manager v3.0.1' id='com.ibm.sklm301.linux' version='3.0.1000.00' features='main.fea
  </install>
  <profile id='IBM DB2 SKLM301' installLocation='/opt/IBM/DB2SKLMV301'>
    <data key='eclipseLocation' value='/opt/IBM/DB2SKLMV301'/>
    <data key='user.import.profile' value='false'/>
    <data key='cic.selector.os' value='linux'/>
    <data key='cic.selector.arch' value='x86_64'/>
    <data key='cic.selector.ws' value='gtk'/>
    <data key='cic.selector.nl' value='en'/>
    <data key='user.DB2_ADMIN_ID,com.ibm.sklm301.db2.lin.ofng' value='sklmdb31'/>
    <data key='user.DB2_ADMIN_PWD,com.ibm.sklm301.db2.lin.ofng' value='QTh/0AiFvrljhs9gnOYkGA=='/>
    <data key='user.CONFIRM_PASSWORD,com.ibm.sklm301.db2.lin.ofng' value='QTh/0AiFvrljhs9gnOYkGA=='/>
    <data key='user.DB2_DB_HOME,com.ibm.sklm301.db2.lin.ofng' value='/home/sklmdb31'/>
    <data key='user.DB2_DB_NAME,com.ibm.sklm301.db2.lin.ofng' value='SKLMDB31'/>
    <data key='user.DB2_DB_PORT,com.ibm.sklm301.db2.lin.ofng' value='50050'/>
    <data key='user.DB2_EXISTS,com.ibm.sklm301.db2.lin.ofng' value='false'/>
    <data key='user.DB2_LOCATION,com.ibm.sklm301.db2.lin.ofng' value='/opt/IBM/DB2SKLMV301'/>
    <data key='user.DB2_DB_LHOME,com.ibm.sklm301.db2.lin.ofng' value='/home/sklmdb31'/>
    <!--The DB2 Group name should not be more than 8 characters -->
    <data key='user.DB2_ADMIN_GRP,com.ibm.sklm301.db2.lin.ofng' value='sklmdb31'/>
  </profile>
  <profile id='IBM Installation Manager' installLocation='/opt/IBM/InstallationManager/eclipse' kind='self'>
 <data key='eclipseLocation' value='/opt/IBM/InstallationManager/eclipse'/>
 <data key='user.import.profile' value='false'/>
 <data key='cic.selector.os' value='linux'/>
 <data key='cic.selector.arch' value='x86_64'/>
 <data key='cic.selector.ws' value='gtk'/>
</profile>
  <profile id='IBM WebSphere Application Server V9.0' installLocation='/opt/IBM/WebSphere30/AppServer'>
    <data key='eclipseLocation' value='/opt/IBM/WebSphere30/AppServer'/>
    <data key='user.import.profile' value='false'/>
    <data key='cic.selector.os' value='linux'/>
    <data key='cic.selector.arch' value='x86_64'/>
    <data key='cic.selector.ws' value='gtk'/>
    <data key='cic.selector.nl' value='en'/>
  </profile>

  <profile id='IBM Security Key Lifecycle Manager v3.0.1' installLocation='/opt/IBM/SKLMV301'>
    <data key='eclipseLocation' value='/opt/IBM/SKLMV301'/>
    <data key='user.import.profile' value='false'/>
    <data key='cic.selector.os' value='linux'/>
    <data key='cic.selector.arch' value='x86_64'/>
    <data key='cic.selector.ws' value='gtk'/>
    <data key='user.IS_SILENT_MODE,com.ibm.sklm301.linux' value='false'/>
    <data key='cic.selector.nl' value='en'/>
    <data key='user.PROFILE_NAME,com.ibm.sklm301.linux' value='KLMProfile'/>
    <data key='user.WAS_ADMIN_ID,com.ibm.sklm301.linux' value='wasadmin'/>
    <data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm301.linux' value='e9PjN93MeQxwnSs9VXJFMw=='/>
    <data key='user.WAS_ADMIN_CONF_PWD,com.ibm.sklm301.linux' value='e9PjN93MeQxwnSs9VXJFMw=='/>
    <data key='user.SKLM_ADMIN_USER,com.ibm.sklm301.linux' value='SKLMAdmin'/>
    <data key='user.SKLM_ADMIN_PASSWORD,com.ibm.sklm301.linux' value='9YTRJMRIydDSdfhaHPs1ag=='/>
    <data key='user.SKLM_ADMIN_CONF_PWD,com.ibm.sklm301.linux' value='9YTRJMRIydDSdfhaHPs1ag=='/>
    <data key='user.TKLM_VERSION,com.ibm.sklm301.linux' value='2.5.0.4'/>
    <data key='user.TKLM_TIP_HOME,com.ibm.sklm301.linux' value='/opt/IBM/WebSphere/AppServer'/>
```

```
    <data key='user.TKLM_INSTALLED,com.ibm.sklm301.linux' value='true'/>
    <data key='user.TKLM_DB_PWD,com.ibm.sklm301.linux' value='SwIhGBTDHcJok80Ux4Sb3g=='/>
    <data key='user.SKLM_APP_PORT,com.ibm.sklm301.linux' value='443'/>
 <data key='user.WAS_ADMIN_PORT,com.ibm.sklm301.linux' value='9083'/>
 <data key='user.SKLM_APP_NS_PORT,com.ibm.sklm301.linux' value='80'/>
  </profile>

  <preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='/opt/IBM/IBMIMShared'/>
  <preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30'/>
  <preference name='com.ibm.cic.common.core.preferences.readTimeout' value='45'/>
  <preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0'/>
  <preference name='offering.service.repositories.areUsed' value='true'/>
  <preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false'/>
  <preference name='com.ibm.cic.common.core.preferences.http.disablePreemptiveAuthentication' value='false'/>
  <preference name='http.ntlm.auth.kind' value='NTLM'/>
  <preference name='http.ntlm.auth.enableIntegrated.win32' value='true'/>
  <preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true'/>
  <preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false'/>
  <preference name='PassportAdvantageIsEnabled' value='false'/>
  <preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false'/>
  <preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false'/>
  <preference name='com.ibm.cic.common.sharedUI.showErrorLog' value='true'/>
  <preference name='com.ibm.cic.common.sharedUI.showWarningLog' value='true'/>
  <preference name='com.ibm.cic.common.sharedUI.showNoteLog' value='true'/>
</agent-input>
```

Migration de la version 2.6 vers la version 3.0.1

```
<?xml version='1.0' encoding='UTF-8'?>
<agent-input clean='true' >
  <server>
    <repository location='/disk1'/>
    <repository location='/disk1/im'/>
  </server>
   <install modify='false'>
 <offering profile='IBM Installation Manager'  id='com.ibm.cic.agent'  features='agent_core,agent_jre,agent_web' installFixes='none'/>
    <offering profile='IBM WebSphere Application Server V9.0' id='com.ibm.websphere.BASE.v90' features='core.feature,ejbdeploy,thinclien
    <offering profile='IBM WebSphere Application Server V9.0' id='com.ibm.java.jdk.v8' features='com.ibm.sdk.8' installFixes='none'/>
    <offering profile='IBM DB2 SKLM301' id='com.ibm.sklm301.db2.lin.ofng' version='11.1.2.2' features='main.feature' installFixes='none'
    <offering profile='IBM Security Key Lifecycle Manager v3.0.1' id='com.ibm.sklm301.linux' version='3.0.1000.00' features='main.featur
  </install>
  <profile id='IBM DB2 SKLM301' installLocation='/opt/IBM/DB2SKLMV301'>
    <data key='eclipseLocation' value='/opt/IBM/DB2SKLMV301'/>
    <data key='user.import.profile' value='false'/>
    <data key='cic.selector.os' value='linux'/>
    <data key='cic.selector.arch' value='x86_64'/>
    <data key='cic.selector.ws' value='gtk'/>
    <data key='cic.selector.nl' value='en'/>
    <data key='user.DB2_ADMIN_ID,com.ibm.sklm301.db2.lin.ofng' value='sklmdb31'/>
    <data key='user.DB2_ADMIN_PWD,com.ibm.sklm301.db2.lin.ofng' value='QTh/0AiFvrljhs9gnOYkGA=='/>
    <data key='user.CONFIRM_PASSWORD,com.ibm.sklm301.db2.lin.ofng' value='QTh/0AiFvrljhs9gnOYkGA=='/>
    <data key='user.DB2_DB_HOME,com.ibm.sklm301.db2.lin.ofng' value='/home/sklmdb31'/>
    <data key='user.DB2_DB_NAME,com.ibm.sklm301.db2.lin.ofng' value='SKLMDB31'/>
    <data key='user.DB2_DB_PORT,com.ibm.sklm301.db2.lin.ofng' value='50050'/>
    <data key='user.DB2_EXISTS,com.ibm.sklm301.db2.lin.ofng' value='false'/>
    <data key='user.DB2_LOCATION,com.ibm.sklm301.db2.lin.ofng' value='/opt/IBM/DB2SKLMV301'/>
    <data key='user.DB2_DB_LHOME,com.ibm.sklm301.db2.lin.ofng' value='/home/sklmdb31'/>
    <!--The DB2 Group name should not be more than 8 characters -->
    <data key='user.DB2_ADMIN_GRP,com.ibm.sklm301.db2.lin.ofng' value='sklmdb31'/>
  </profile>
  <profile id='IBM Installation Manager' installLocation='/opt/IBM/InstallationManager/eclipse' kind='self'>
 <data key='eclipseLocation' value='/opt/IBM/InstallationManager/eclipse'/>
 <data key='user.import.profile' value='false'/>
 <data key='cic.selector.os' value='linux'/>
 <data key='cic.selector.arch' value='x86_64'/>
 <data key='cic.selector.ws' value='gtk'/>
</profile>
  <profile id='IBM WebSphere Application Server V9.0' installLocation='/opt/IBM/WebSphere30/AppServer'>
    <data key='eclipseLocation' value='/opt/IBM/WebSphere30/AppServer'/>
    <data key='user.import.profile' value='false'/>
    <data key='cic.selector.os' value='linux'/>
    <data key='cic.selector.arch' value='x86_64'/>
    <data key='cic.selector.ws' value='gtk'/>
    <data key='cic.selector.nl' value='en'/>
  </profile>

  <profile id='IBM Security Key Lifecycle Manager v3.0.1' installLocation='/opt/IBM/SKLMV301'>
    <data key='eclipseLocation' value='/opt/IBM/SKLMV301'/>
    <data key='user.import.profile' value='false'/>
    <data key='cic.selector.os' value='linux'/>
    <data key='cic.selector.arch' value='x86_64'/>
    <data key='cic.selector.ws' value='gtk'/>
    <data key='user.IS_SILENT_MODE,com.ibm.sklm301.linux' value='false'/>
    <data key='cic.selector.nl' value='en'/>
    <data key='user.PROFILE_NAME,com.ibm.sklm301.linux' value='KLMProfile'/>
    <data key='user.WAS_ADMIN_ID,com.ibm.sklm301.linux' value='wasadmin'/>
    <data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm301.linux' value='e9PjN93MeQxwnSs9VXJFMw=='/>
    <data key='user.WAS_ADMIN_CONF_PWD,com.ibm.sklm301.linux' value='e9PjN93MeQxwnSs9VXJFMw=='/>
    <data key='user.SKLM_ADMIN_USER,com.ibm.sklm301.linux' value='SKLMAdmin'/>
    <data key='user.SKLM_ADMIN_PASSWORD,com.ibm.sklm301.linux' value='9YTRJMRIydDSdfhaHPs1ag==''/>
```

```
    <data key='user.SKLM_ADMIN_CONF_PWD,com.ibm.sklm301.linux' value='9YTRJMRIydDSdfhaHPs1ag==' />
    <data key='user.TKLM_VERSION,com.ibm.sklm301.linux' value='2.5.0.4' />
    <data key='user.TKLM_TIP_HOME,com.ibm.sklm301.linux' value='/opt/IBM/WebSphere/AppServer' />
    <data key='user.TKLM_INSTALLED,com.ibm.sklm301.linux' value='true' />
    <data key='user.TKLM_DB_PWD,com.ibm.sklm301.linux' value='SwIhGBTDHcJok80Ux4Sb3g==' />
    <data key='user.SKLM_APP_PORT,com.ibm.sklm301.linux' value='443' />
 <data key='user.WAS_ADMIN_PORT,com.ibm.sklm301.linux' value='9083' />
 <data key='user.SKLM_APP_NS_PORT,com.ibm.sklm301.linux' value='80' />
  </profile>

  <preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='/opt/IBM/IBMIMShared' />
  <preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30' />
  <preference name='com.ibm.cic.common.core.preferences.readTimeout' value='45' />
  <preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0' />
  <preference name='offering.service.repositories.areUsed' value='true' />
  <preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false' />
  <preference name='com.ibm.cic.common.core.preferences.http.disablePreemptiveAuthentication' value='false' />
  <preference name='http.ntlm.auth.kind' value='NTLM' />
  <preference name='http.ntlm.auth.enableIntegrated.win32' value='true' />
  <preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true' />
  <preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false' />
  <preference name='PassportAdvantageIsEnabled' value='false' />
  <preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false' />
  <preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false' />
  <preference name='com.ibm.cic.common.sharedUI.showErrorLog' value='true' />
  <preference name='com.ibm.cic.common.sharedUI.showWarningLog' value='true' />
  <preference name='com.ibm.cic.common.sharedUI.showNoteLog' value='true' />
</agent-input>
```

Migration de la version 2.7 vers la version 3.0.1

```
<?xml version='1.0' encoding='UTF-8'?>
<agent-input clean='true' >
  <server>
    <repository location='/disk1' />
    <repository location='/disk1/im' />
  </server>
   <install modify='false'>
 <offering profile='IBM Installation Manager'  id='com.ibm.cic.agent'  features='agent_core,agent_jre,agent_web' installFixes='none'/
    <offering profile='IBM WebSphere Application Server V9.0_1' id='com.ibm.websphere.BASE.v90'  features='core.feature,ejbdeploy,thi
    <offering profile='IBM WebSphere Application Server V9.0_1' id='com.ibm.java.jdk.v8' features='com.ibm.sdk.8' installFixes='none'
    <offering profile='IBM DB2 SKLM301' id='com.ibm.sklm301.db2.lin.ofng' version='11.1.2.2' features='main.feature' installFixes='no
    <offering profile='IBM Security Key Lifecycle Manager v3.0.1' id='com.ibm.sklm301.linux' version='3.0.1000.00' features='main.fea
  </install>
  <profile id='IBM DB2 SKLM301' installLocation='/opt/IBM/DB2SKLMV301'>
    <data key='eclipseLocation' value='/opt/IBM/DB2SKLMV301' />
    <data key='user.import.profile' value='false' />
    <data key='cic.selector.os' value='linux' />
    <data key='cic.selector.arch' value='x86_64' />
    <data key='cic.selector.ws' value='gtk' />
    <data key='cic.selector.nl' value='en' />
    <data key='user.DB2_ADMIN_ID,com.ibm.sklm301.db2.lin.ofng' value='sklmdb31' />
    <data key='user.DB2_ADMIN_PWD,com.ibm.sklm301.db2.lin.ofng' value='QTh/0AiFvrljhs9gnOYkGA==' />
    <data key='user.CONFIRM_PASSWORD,com.ibm.sklm301.db2.lin.ofng' value='QTh/0AiFvrljhs9gnOYkGA==' />
    <data key='user.DB2_DB_HOME,com.ibm.sklm301.db2.lin.ofng' value='/home/sklmdb31' />
    <data key='user.DB2_DB_NAME,com.ibm.sklm301.db2.lin.ofng' value='SKLMDB31' />
    <data key='user.DB2_DB_PORT,com.ibm.sklm301.db2.lin.ofng' value='50050' />
    <data key='user.DB2_EXISTS,com.ibm.sklm301.db2.lin.ofng' value='false' />
    <data key='user.DB2_LOCATION,com.ibm.sklm301.db2.lin.ofng' value='/opt/IBM/DB2SKLMV301' />
    <data key='user.DB2_DB_LHOME,com.ibm.sklm301.db2.lin.ofng' value='/home/sklmdb31' />
    <!--The DB2 Group name should not be more than 8 characters -->
    <data key='user.DB2_ADMIN_GRP,com.ibm.sklm301.db2.lin.ofng' value='sklmdb31' />
  </profile>
  <profile id='IBM Installation Manager' installLocation='/opt/IBM/InstallationManager/eclipse' kind='self'>
 <data key='eclipseLocation' value='/opt/IBM/InstallationManager/eclipse' />
 <data key='user.import.profile' value='false' />
 <data key='cic.selector.os' value='linux' />
 <data key='cic.selector.arch' value='x86_64' />
 <data key='cic.selector.ws' value='gtk' />
</profile>
  <profile id='IBM WebSphere Application Server V9.0' installLocation='/opt/IBM/WebSphere30/AppServer'>
    <data key='eclipseLocation' value='/opt/IBM/WebSphere30/AppServer' />
    <data key='user.import.profile' value='false' />
    <data key='cic.selector.os' value='linux' />
    <data key='cic.selector.arch' value='x86_64' />
    <data key='cic.selector.ws' value='gtk' />
    <data key='cic.selector.nl' value='en' />
  </profile>

  <profile id='IBM Security Key Lifecycle Manager v3.0.1' installLocation='/opt/IBM/SKLMV301'>
    <data key='eclipseLocation' value='/opt/IBM/SKLMV301' />
    <data key='user.import.profile' value='false' />
    <data key='cic.selector.os' value='linux' />
    <data key='cic.selector.arch' value='x86_64' />
    <data key='cic.selector.ws' value='gtk' />
    <data key='user.IS_SILENT_MODE,com.ibm.sklm301.linux' value='false' />
    <data key='cic.selector.nl' value='en' />
    <data key='user.PROFILE_NAME,com.ibm.sklm301.linux' value='KLMProfile' />
    <data key='user.WAS_ADMIN_ID,com.ibm.sklm301.linux' value='wasadmin' />
    <data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm301.linux' value='e9PjN93MeQxwnSs9VXJFMw==' />
```

```
    <data key='user.WAS_ADMIN_CONF_PWD,com.ibm.sklm301.linux' value='e9PjN93MeQxwnSs9VXJFMw=='/>
    <data key='user.SKLM_ADMIN_USER,com.ibm.sklm301.linux' value='SKLMAdmin'/>
    <data key='user.SKLM_ADMIN_PASSWORD,com.ibm.sklm301.linux' value='9YTRJMRIydDSdfhaHPs1ag=='/>
    <data key='user.SKLM_ADMIN_CONF_PWD,com.ibm.sklm301.linux' value='9YTRJMRIydDSdfhaHPs1ag=='/>
    <data key='user.TKLM_VERSION,com.ibm.sklm301.linux' value='2.5.0.4'/>
    <data key='user.TKLM_TIP_HOME,com.ibm.sklm301.linux' value='/opt/IBM/WebSphere/AppServer'/>
    <data key='user.TKLM_INSTALLED,com.ibm.sklm301.linux' value='true'/>
    <data key='user.TKLM_DB_PWD,com.ibm.sklm301.linux' value='SwIhGBTDHcJok80Ux4Sb3g=='/>
    <data key='user.SKLM_APP_PORT,com.ibm.sklm301.linux' value='443'/>
 <data key='user.WAS_ADMIN_PORT,com.ibm.sklm301.linux' value='9083'/>
 <data key='user.SKLM_APP_NS_PORT,com.ibm.sklm301.linux' value='80'/>
  </profile>

  <preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='/opt/IBM/IBMIMShared'/>
  <preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30'/>
  <preference name='com.ibm.cic.common.core.preferences.readTimeout' value='45'/>
  <preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0'/>
  <preference name='offering.service.repositories.areUsed' value='true'/>
  <preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false'/>
  <preference name='com.ibm.cic.common.core.preferences.http.disablePreemptiveAuthentication' value='false'/>
  <preference name='http.ntlm.auth.kind' value='NTLM'/>
  <preference name='http.ntlm.auth.enableIntegrated.win32' value='true'/>
  <preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true'/>
  <preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false'/>
  <preference name='PassportAdvantageIsEnabled' value='false'/>
  <preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false'/>
  <preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false'/>
  <preference name='com.ibm.cic.common.sharedUI.showErrorLog' value='true'/>
  <preference name='com.ibm.cic.common.sharedUI.showWarningLog' value='true'/>
  <preference name='com.ibm.cic.common.sharedUI.showNoteLog' value='true'/>
</agent-input>
```

Migration de la version 3.0 vers la version 3.0.1

```
<?xml version='1.0' encoding='UTF-8'?>
<agent-input clean='true' >
  <server>
    <repository location='/disk1'/>
    <repository location='/disk1/im'/>
  </server>
   <install modify='false'>
 <offering profile='IBM Installation Manager'  id='com.ibm.cic.agent'  features='agent_core,agent_jre,agent_web' installFixes='none'/>
    <offering profile='IBM WebSphere Application Server V9.0_2' id='com.ibm.websphere.BASE.v90'  features='core.feature,ejbdeploy,thincl
    <offering profile='IBM WebSphere Application Server V9.0_2' id='com.ibm.java.jdk.v8' features='com.ibm.sdk.8' installFixes='none'/>
    <offering profile='IBM DB2 SKLM301' id='com.ibm.sklm301.db2.lin.ofng' version='11.1.2.2' features='main.feature' installFixes='none'
    <offering profile='IBM Security Key Lifecycle Manager v3.0.1' id='com.ibm.sklm301.linux' version='3.0.1000.00' features='main.featur
  </install>
  <profile id='IBM DB2 SKLM301' installLocation='/opt/IBM/DB2SKLMV301'>
    <data key='eclipseLocation' value='/opt/IBM/DB2SKLMV301'/>
    <data key='user.import.profile' value='false'/>
    <data key='cic.selector.os' value='linux'/>
    <data key='cic.selector.arch' value='x86_64'/>
    <data key='cic.selector.ws' value='gtk'/>
    <data key='cic.selector.nl' value='en'/>
    <data key='user.DB2_ADMIN_ID,com.ibm.sklm301.db2.lin.ofng' value='sklmdb31'/>
    <data key='user.DB2_ADMIN_PWD,com.ibm.sklm301.db2.lin.ofng' value='QTh/0AiFvrljhs9gnOYkGA=='/>
    <data key='user.CONFIRM_PASSWORD,com.ibm.sklm301.db2.lin.ofng' value='QTh/0AiFvrljhs9gnOYkGA=='/>
    <data key='user.DB2_DB_HOME,com.ibm.sklm301.db2.lin.ofng' value='/home/sklmdb31'/>
    <data key='user.DB2_DB_NAME,com.ibm.sklm301.db2.lin.ofng' value='SKLMDB31'/>
    <data key='user.DB2_DB_PORT,com.ibm.sklm301.db2.lin.ofng' value='50050'/>
    <data key='user.DB2_EXISTS,com.ibm.sklm301.db2.lin.ofng' value='false'/>
    <data key='user.DB2_LOCATION,com.ibm.sklm301.db2.lin.ofng' value='/opt/IBM/DB2SKLMV301'/>
    <data key='user.DB2_DB_LHOME,com.ibm.sklm301.db2.lin.ofng' value='/home/sklmdb31'/>
    <!--The DB2 Group name should not be more than 8 characters -->
    <data key='user.DB2_ADMIN_GRP,com.ibm.sklm301.db2.lin.ofng' value='sklmdb31'/>
  </profile>
  <profile id='IBM Installation Manager' installLocation='/opt/IBM/InstallationManager/eclipse' kind='self'>
 <data key='eclipseLocation' value='/opt/IBM/InstallationManager/eclipse'/>
 <data key='user.import.profile' value='false'/>
 <data key='cic.selector.os' value='linux'/>
 <data key='cic.selector.arch' value='x86_64'/>
 <data key='cic.selector.ws' value='gtk'/>
</profile>
  <profile id='IBM WebSphere Application Server V9.0_2' installLocation='/opt/IBM/WebSphere30/AppServer'>
    <data key='eclipseLocation' value='/opt/IBM/WebSphere30/AppServer'/>
    <data key='user.import.profile' value='false'/>
    <data key='cic.selector.os' value='linux'/>
    <data key='cic.selector.arch' value='x86_64'/>
    <data key='cic.selector.ws' value='gtk'/>
    <data key='cic.selector.nl' value='en'/>
  </profile>
  <profile id='IBM Security Key Lifecycle Manager v3.0.1' installLocation='/opt/IBM/SKLMV301'>
    <data key='eclipseLocation' value='/opt/IBM/SKLMV301'/>
    <data key='user.import.profile' value='false'/>
    <data key='cic.selector.os' value='linux'/>
    <data key='cic.selector.arch' value='x86_64'/>
    <data key='cic.selector.ws' value='gtk'/>
    <data key='user.IS_SILENT_MODE,com.ibm.sklm301.linux' value='false'/>
    <data key='cic.selector.nl' value='en'/>
    <data key='user.PROFILE_NAME,com.ibm.sklm301.linux' value='KLMProfile'/>
```

```
    <data key='user.WAS_ADMIN_ID,com.ibm.sklm301.linux' value='wasadmin'/>
    <data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm301.linux' value='e9PjN93MeQxwnSs9VXJFMw=='/>
    <data key='user.WAS_ADMIN_CONF_PWD,com.ibm.sklm301.linux' value='e9PjN93MeQxwnSs9VXJFMw=='/>
    <data key='user.SKLM_ADMIN_USER,com.ibm.sklm301.linux' value='SKLMAdmin'/>
    <data key='user.SKLM_ADMIN_PASSWORD,com.ibm.sklm301.linux' value='9YTRJMRIydDSdfhaHPs1ag=='/>
    <data key='user.SKLM_ADMIN_CONF_PWD,com.ibm.sklm301.linux' value='9YTRJMRIydDSdfhaHPs1ag=='/>
    <data key='user.TKLM_VERSION,com.ibm.sklm301.linux' value='3.0.0.0'/>
    <data key='user.TKLM_TIP_HOME,com.ibm.sklm301.linux' value='/opt/IBM/WebSphere/AppServer'/>
    <data key='user.TKLM_INSTALLED,com.ibm.sklm301.linux' value='true'/>
    <data key='user.INSTALL_AS_FP,com.ibm.sklm301.linux' value='false'/>
    <data key='user.TKLM_DB_PWD,com.ibm.sklm301.linux' value='SwIhGBTDHcJok80Ux4Sb3g=='/>
    <data key='user.SKLM_APP_PORT,com.ibm.sklm301.linux' value='443'/>
    <data key='user.WAS_ADMIN_PORT,com.ibm.sklm301.linux' value='9083'/>
    <data key='user.SKLM_APP_NS_PORT,com.ibm.sklm301.linux' value='80'/>
  </profile>
  <preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='/opt/IBM/IBMIMShared'/>
  <preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30'/>
  <preference name='com.ibm.cic.common.core.preferences.readTimeout' value='45'/>
  <preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0'/>
  <preference name='offering.service.repositories.areUsed' value='true'/>
  <preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false'/>
  <preference name='com.ibm.cic.common.core.preferences.http.disablePreemptiveAuthentication' value='false'/>
  <preference name='http.ntlm.auth.kind' value='NTLM'/>
  <preference name='http.ntlm.auth.enableIntegrated.win32' value='true'/>
  <preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true'/>
  <preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false'/>
  <preference name='PassportAdvantageIsEnabled' value='false'/>
  <preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false'/>
  <preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false'/>
  <preference name='com.ibm.cic.common.sharedUI.showErrorLog' value='true'/>
  <preference name='com.ibm.cic.common.sharedUI.showWarningLog' value='true'/>
  <preference name='com.ibm.cic.common.sharedUI.showNoteLog' value='true'/>
</agent-input>
```

Migration des versions 2.5, 2.6, 2.7 et 3.0 vers la version 3.0.1 sur Linux for System z

L'exemple de fichiers de réponses contient des réponses pour une installation Linux for System z dans laquelle la migration d'une version 2.5, 2.6, 2.7 et 3.0 précédente d'IBM Security Key Lifecycle Manager vers la version 3.0.1 est effectuée.

Remarque : Pour déterminer s'il existe une installation d'IBM Security Key Lifecycle Manager d'une version antérieure nécessitant une migration, utilisez la commande **tklmVersionInfo**. Par exemple, entrez la commande suivante dans une session Jython :

```
print AdminTask.tklmVersionInfo<>
```

Migration de la version 2.5 vers la version 3.0.1

```
<?xml version="1.0" encoding="UTF-8"?>
<!--L'attribut "acceptLicense" est obsolète. La ligne de commande "-acceptLicense" permet d'accepter les contrats de licence.-->
<agent-input clean='true' >

<server>
<repository location='/disk1/im'/>
<repository location='/disk1/'/>
</server>

<install modify='false'>
<offering profile='IBM Installation Manager' id='com.ibm.cic.agent' features='agent_core,agent_jre' installFixes='none'/>
<offering profile='IBM DB2 SKLM301' id='com.ibm.sklm301.db2.lin.ofng' features='main.feature' installFixes='none'/>
<offering profile='IBM WebSphere Application Server V9.0' id='com.ibm.websphere.BASE.v90' features='core.feature,ejbdeploy,thinclient
<offering profile='IBM WebSphere Application Server V9.0' id='com.ibm.java.jdk.v8' features='com.ibm.sdk.8' installFixes='none'/>
<offering profile='IBM Security Key Lifecycle Manager v3.0.1' id='com.ibm.sklm301.linux' features='main.feature' installFixes='none'/
</install>

<profile id='IBM DB2 SKLM301' installLocation='/opt/IBM/DB2SKLMV301'>
<data key='eclipseLocation' value='/opt/IBM/DB2SKLMV301'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='linux'/>
<data key='cic.selector.arch' value='s390x'/>
<data key='cic.selector.ws' value='gtk'/>
<data key='user.DB2_ADMIN_ID,com.ibm.sklm301.db2.lin.ofng' value='sklmdb31'/>
<!--The DB2 Group name should not be more than 8 characters -->
<data key='user.DB2_ADMIN_GRP,com.ibm.sklm301.db2.lin.ofng' value='sklmdb31'/>
<data key='user.DB2_ADMIN_PWD,com.ibm.sklm301.db2.lin.ofng' value='QTh/0AiFvrljhs9gnOYkGA=='/>
<data key='user.CONFIRM_PASSWORD,com.ibm.sklm301.db2.lin.ofng' value='QTh/0AiFvrljhs9gnOYkGA=='/>
<data key='user.DB2_DB_LHOME,com.ibm.sklm301.db2.lin.ofng' value='/home/sklmdb31'/>
<data key='user.DB2_DB_NAME,com.ibm.sklm301.db2.lin.ofng' value='SKLMDB31'/>
```

```
<data key='user.DB2_DB_PORT,com.ibm.sklm301.db2.lin.ofng' value='50050'/>
<data key='user.DB2_EXISTS,com.ibm.sklm301.db2.lin.ofng' value='false'/>
<data key='user.DB2_LOCATION,com.ibm.sklm301.db2.lin.ofng' value='/opt/IBM/DB2SKLMV301'/>
<data key='cic.selector.nl' value='en'/>
</profile>
<profile id='IBM Installation Manager' installLocation='/opt/IBM/InstallationManager/eclipse' kind='self'>
<data key='eclipseLocation' value='/opt/IBM/InstallationManager/eclipse'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='linux'/>
<data key='cic.selector.arch' value='s390x'/>
<data key='cic.selector.ws' value='gtk'/>
</profile>
<profile id='IBM WebSphere Application Server V9.0' installLocation='/opt/IBM/WebSphere30/AppServer'>
<data key='eclipseLocation' value='/opt/IBM/WebSphere30/AppServer'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='linux'/>
<data key='cic.selector.arch' value='s390x'/>
<data key='cic.selector.ws' value='gtk'/>
<data key='cic.selector.nl' value='en'/>
</profile>
<profile id='IBM Security Key Lifecycle Manager v3.0.1' installLocation='/opt/IBM/SKLMV301'>
<data key='eclipseLocation' value='/opt/IBM/SKLMV301'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='linux'/>
<data key='cic.selector.arch' value='s390x'/>
<data key='cic.selector.ws' value='gtk'/>
<data key='user.EKM_PROPFILE,com.ibm.sklm301.linux' value='/opt/IBM/KeyManagerConfig.properties'/>
<data key='user.EKM_MIGRATION,com.ibm.sklm301.linux' value='false'/>
<data key='user.PROFILE_NAME,com.ibm.sklm301.linux' value='KLMProfile'/>
<data key='user.WAS_ADMIN_ID,com.ibm.sklm301.linux' value='tipadmin'/>
<data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm301.linux' value='e9PjN93MeQxwnSs9VXJFMw=='/>
<data key='user.WAS_ADMIN_CONF_PWD,com.ibm.sklm301.linux' value='e9PjN93MeQxwnSs9VXJFMw=='/>
<data key='user.SKLM_ADMIN_USER,com.ibm.sklm301.linux' value='TKLMAdmin'/>
<data key='user.SKLM_ADMIN_PASSWORD,com.ibm.sklm301.linux' value='9YTRJMRIydDSdfhaHPs1ag=='/>
<data key='user.SKLM_ADMIN_CONF_PWD,com.ibm.sklm301.linux' value='9YTRJMRIydDSdfhaHPs1ag=='/>
<data key='user.TKLM_VERSION,com.ibm.sklm301.linux' value='2.0.1'/>
<data key='user.TKLM_TIP_HOME,com.ibm.sklm301.linux' value='/opt/IBM/tivoli/tiptklmV2/'/>
<data key='user.TKLM_INSTALLED,com.ibm.sklm301.linux' value='true'/>
<data key='user.TKLM_DB_PWD,com.ibm.sklm301.linux' value='/6vJK3fcU3QxHY+RVfCFVw=='/>
<data key='user.TKLM_KEYSTORE_PWD,com.ibm.sklm301.linux' value='fufgZbY47EfxLYarBAIxeQ=='/>
<data key='user.SKLM_APP_PORT,com.ibm.sklm301.linux' value='443'/>
<data key='user.WAS_ADMIN_PORT,com.ibm.sklm301.linux' value='9083'/>
<data key='user.SKLM_APP_NS_PORT,com.ibm.sklm301.linux' value='80'/>
<data key='cic.selector.nl' value='en'/>
</profile>
<preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='/opt/IBM/IBMIMShared'/>
<preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30'/>
<preference name='com.ibm.cic.common.core.preferences.readTimeout' value='45'/>
<preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0'/>
<preference name='offering.service.repositories.areUsed' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.http.disablePreemptiveAuthentication' value='false'/>
<preference name='http.ntlm.auth.kind' value='NTLM'/>
<preference name='http.ntlm.auth.enableIntegrated.win32' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false'/>
<preference name='PassportAdvantageIsEnabled' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false'/>
<preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false'/>
<preference name='com.ibm.cic.common.sharedUI.showErrorLog' value='true'/>
<preference name='com.ibm.cic.common.sharedUI.showWarningLog' value='true'/>
<preference name='com.ibm.cic.common.sharedUI.showNoteLog' value='true'/>
</agent-input>
```

Migration de la version 2.6 vers la version 3.0.1

```
<?xml version="1.0" encoding="UTF-8"?>
<!--L'attribut "acceptLicense" est obsolète. La ligne de commande "-acceptLicense" permet d'accepter les contrats de licence.-->
<agent-input clean='true' >

<server>
<repository location='/disk1/im'/>
<repository location='/disk1/'/>
</server>

<install modify='false'>
<offering profile='IBM Installation Manager' id='com.ibm.cic.agent' features='agent_core,agent_jre' installFixes='none'/>
<offering profile='IBM DB2 SKLM301' id='com.ibm.sklm301.db2.lin.ofng' features='main.feature' installFixes='none'/>
<offering profile='IBM WebSphere Application Server V9.0' id='com.ibm.websphere.BASE.v90' features='core.feature,ejbdeploy,thinclient,em
<offering profile='IBM WebSphere Application Server V9.0' id='com.ibm.java.jdk.v8' features='com.ibm.sdk.8' installFixes='none'/>
<offering profile='IBM Security Key Lifecycle Manager v3.0.1' id='com.ibm.sklm301.linux' features='main.feature' installFixes='none'/>
</install>

<profile id='IBM DB2 SKLM301' installLocation='/opt/IBM/DB2SKLMV301'>
<data key='eclipseLocation' value='/opt/IBM/DB2SKLMV301'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='linux'/>
<data key='cic.selector.arch' value='s390x'/>
<data key='cic.selector.ws' value='gtk'/>
<data key='user.DB2_ADMIN_ID,com.ibm.sklm301.db2.lin.ofng' value='sklmdb31'/>
```

```
<!--The DB2 Group name should not be more than 8 characters -->
<data key='user.DB2_ADMIN_GRP,com.ibm.sklm301.db2.lin.ofng' value='sklmdb31'/>
<data key='user.DB2_ADMIN_PWD,com.ibm.sklm301.db2.lin.ofng' value='QTh/0AiFvrljhs9gnOYkGA=='/>
<data key='user.CONFIRM_PASSWORD,com.ibm.sklm301.db2.lin.ofng' value='QTh/0AiFvrljhs9gnOYkGA=='/>
<data key='user.DB2_DB_LHOME,com.ibm.sklm301.db2.lin.ofng' value='/home/sklmdb31'/>
<data key='user.DB2_DB_NAME,com.ibm.sklm301.db2.lin.ofng' value='SKLMDB31'/>
<data key='user.DB2_DB_PORT,com.ibm.sklm301.db2.lin.ofng' value='50050'/>
<data key='user.DB2_EXISTS,com.ibm.sklm301.db2.lin.ofng' value='false'/>
<data key='user.DB2_LOCATION,com.ibm.sklm301.db2.lin.ofng' value='/opt/IBM/DB2SKLMV301'/>
<data key='cic.selector.nl' value='en'/>
</profile>
<profile id='IBM Installation Manager' installLocation='/opt/IBM/InstallationManager/eclipse' kind='self'>
<data key='eclipseLocation' value='/opt/IBM/InstallationManager/eclipse'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='linux'/>
<data key='cic.selector.arch' value='s390x'/>
<data key='cic.selector.ws' value='gtk'/>
</profile>
<profile id='IBM WebSphere Application Server V9.0' installLocation='/opt/IBM/WebSphere30/AppServer'>
<data key='eclipseLocation' value='/opt/IBM/WebSphere30/AppServer'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='linux'/>
<data key='cic.selector.arch' value='s390x'/>
<data key='cic.selector.ws' value='gtk'/>
<data key='cic.selector.nl' value='en'/>
</profile>
<profile id='IBM Security Key Lifecycle Manager v3.0.1' installLocation='/opt/IBM/SKLMV301'>
<data key='eclipseLocation' value='/opt/IBM/SKLMV301'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='linux'/>
<data key='cic.selector.arch' value='s390x'/>
<data key='cic.selector.ws' value='gtk'/>
<data key='user.EKM_PROPFILE,com.ibm.sklm301.linux' value='/opt/IBM/KeyManagerConfig.properties'/>
<data key='user.EKM_MIGRATION,com.ibm.sklm301.linux' value='false'/>
<data key='user.PROFILE_NAME,com.ibm.sklm301.linux' value='KLMProfile'/>
<data key='user.WAS_ADMIN_ID,com.ibm.sklm301.linux' value='tipadmin'/>
<data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm301.linux' value='e9PjN93MeQxwnSs9VXJFMw=='/>
<data key='user.WAS_ADMIN_CONF_PWD,com.ibm.sklm301.linux' value='e9PjN93MeQxwnSs9VXJFMw=='/>
<data key='user.SKLM_ADMIN_USER,com.ibm.sklm301.linux' value='TKLMAdmin'/>
<data key='user.SKLM_ADMIN_PASSWORD,com.ibm.sklm301.linux' value='9YTRJMRIydDSdfhaHPs1ag=='/>
<data key='user.SKLM_ADMIN_CONF_PWD,com.ibm.sklm301.linux' value='9YTRJMRIydDSdfhaHPs1ag=='/>
<data key='user.TKLM_VERSION,com.ibm.sklm301.linux' value='2.0.1'/>
<data key='user.TKLM_TIP_HOME,com.ibm.sklm301.linux' value='/opt/IBM/tivoli/tiptklmV2/'/>
<data key='user.TKLM_INSTALLED,com.ibm.sklm301.linux' value='true'/>
<data key='user.TKLM_DB_PWD,com.ibm.sklm301.linux' value='/6vJK3fcU3QxHY+RVfCFVw=='/>
<data key='user.TKLM_KEYSTORE_PWD,com.ibm.sklm301.linux' value='fufgZbY47EfxLYarBAIxeQ=='/>
<data key='user.SKLM_APP_PORT,com.ibm.sklm301.linux' value='443'/>
<data key='user.WAS_ADMIN_PORT,com.ibm.sklm301.linux' value='9083'/>
<data key='user.SKLM_APP_NS_PORT,com.ibm.sklm301.linux' value='80'/>
<data key='cic.selector.nl' value='en'/>
</profile>
<preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='/opt/IBM/IBMIMShared'/>
<preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30'/>
<preference name='com.ibm.cic.common.core.preferences.readTimeout' value='45'/>
<preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0'/>
<preference name='offering.service.repositories.areUsed' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.http.disablePreemptiveAuthentication' value='false'/>
<preference name='http.ntlm.auth.kind' value='NTLM'/>
<preference name='http.ntlm.auth.enableIntegrated.win32' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false'/>
<preference name='PassportAdvantageIsEnabled' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false'/>
<preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false'/>
<preference name='com.ibm.cic.common.sharedUI.showErrorLog' value='true'/>
<preference name='com.ibm.cic.common.sharedUI.showWarningLog' value='true'/>
<preference name='com.ibm.cic.common.sharedUI.showNoteLog' value='true'/>
</agent-input>
```

Migration de la version 2.7 vers la version 3.0.1

```
<?xml version="1.0" encoding="UTF-8"?>
<!--L'attribut "acceptLicense" est obsolète. La ligne de commande "-acceptLicense" permet d'accepter les contrats de licence.-->
<agent-input clean='true' >

<server>
<repository location='/disk1/im'/>
<repository location='/disk1/'/>
</server>

<install modify='false'>
<offering profile='IBM Installation Manager' id='com.ibm.cic.agent' features='agent_core,agent_jre' installFixes='none'/>
<offering profile='IBM DB2 SKLM301' id='com.ibm.sklm301.db2.lin.ofng' features='main.feature' installFixes='none'/>
<offering profile='IBM WebSphere Application Server V9.0_1' id='com.ibm.websphere.BASE.v90'  features='core.feature,ejbdeploy,thincli
<offering profile='IBM WebSphere Application Server V9.0_1' id='com.ibm.java.jdk.v8' features='com.ibm.sdk.8' installFixes='none'/>
<offering profile='IBM Security Key Lifecycle Manager v3.0.1' id='com.ibm.sklm301.linux' features='main.feature' installFixes='none'/
</install>

<profile id='IBM DB2 SKLM301' installLocation='/opt/IBM/DB2SKLMV301'>
```

```
<data key='eclipseLocation' value='/opt/IBM/DB2SKLMV301'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='linux'/>
<data key='cic.selector.arch' value='s390x'/>
<data key='cic.selector.ws' value='gtk'/>
<data key='user.DB2_ADMIN_ID,com.ibm.sklm301.db2.lin.ofng' value='sklmdb31'/>
<!--The DB2 Group name should not be more than 8 characters -->
<data key='user.DB2_ADMIN_GRP,com.ibm.sklm301.db2.lin.ofng' value='sklmdb31'/>
<data key='user.DB2_ADMIN_PWD,com.ibm.sklm301.db2.lin.ofng' value='QTh/0AiFvrljhs9gnOYkGA=='/>
<data key='user.CONFIRM_PASSWORD,com.ibm.sklm301.db2.lin.ofng' value='QTh/0AiFvrljhs9gnOYkGA=='/>
<data key='user.DB2_DB_LHOME,com.ibm.sklm301.db2.lin.ofng' value='/home/sklmdb31'/>
<data key='user.DB2_DB_NAME,com.ibm.sklm301.db2.lin.ofng' value='SKLMDB31'/>
<data key='user.DB2_DB_PORT,com.ibm.sklm301.db2.lin.ofng' value='50050'/>
<data key='user.DB2_EXISTS,com.ibm.sklm301.db2.lin.ofng' value='false'/>
<data key='user.DB2_LOCATION,com.ibm.sklm301.db2.lin.ofng' value='/opt/IBM/DB2SKLMV301'/>
<data key='cic.selector.nl' value='en'/>
</profile>
<profile id='IBM Installation Manager' installLocation='/opt/IBM/InstallationManager/eclipse' kind='self'>
<data key='eclipseLocation' value='/opt/IBM/InstallationManager/eclipse'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='linux'/>
<data key='cic.selector.arch' value='s390x'/>
<data key='cic.selector.ws' value='gtk'/>
</profile>
<profile id='IBM WebSphere Application Server V9.0' installLocation='/opt/IBM/WebSphere30/AppServer'>
<data key='eclipseLocation' value='/opt/IBM/WebSphere30/AppServer'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='linux'/>
<data key='cic.selector.arch' value='s390x'/>
<data key='cic.selector.ws' value='gtk'/>
<data key='cic.selector.nl' value='en'/>
</profile>
<profile id='IBM Security Key Lifecycle Manager v3.0.1' installLocation='/opt/IBM/SKLMV301'>
<data key='eclipseLocation' value='/opt/IBM/SKLMV301'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='linux'/>
<data key='cic.selector.arch' value='s390x'/>
<data key='cic.selector.ws' value='gtk'/>
<data key='user.EKM_PROPFILE,com.ibm.sklm301.linux' value='/opt/IBM/KeyManagerConfig.properties'/>
<data key='user.EKM_MIGRATION,com.ibm.sklm301.linux' value='false'/>
<data key='user.PROFILE_NAME,com.ibm.sklm301.linux' value='KLMProfile'/>
<data key='user.WAS_ADMIN_ID,com.ibm.sklm301.linux' value='tipadmin'/>
<data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm301.linux' value='e9PjN93MeQxwnSs9VXJFMw=='/>
<data key='user.WAS_ADMIN_CONF_PWD,com.ibm.sklm301.linux' value='e9PjN93MeQxwnSs9VXJFMw=='/>
<data key='user.SKLM_ADMIN_USER,com.ibm.sklm301.linux' value='TKLMAdmin'/>
<data key='user.SKLM_ADMIN_PASSWORD,com.ibm.sklm301.linux' value='9YTRJMRIydDSdfhaHPs1ag=='/>
<data key='user.SKLM_ADMIN_CONF_PWD,com.ibm.sklm301.linux' value='9YTRJMRIydDSdfhaHPs1ag=='/>
<data key='user.TKLM_VERSION,com.ibm.sklm301.linux' value='2.0.1'/>
<data key='user.TKLM_TIP_HOME,com.ibm.sklm301.linux' value='/opt/IBM/tivoli/tiptklmV2/'/>
<data key='user.TKLM_INSTALLED,com.ibm.sklm301.linux' value='true'/>
<data key='user.TKLM_DB_PWD,com.ibm.sklm301.linux' value='/6vJK3fcU3QxHY+RVfCFVw=='/>
<data key='user.TKLM_KEYSTORE_PWD,com.ibm.sklm301.linux' value='fufgZbY47EfxLYarBAIxeQ=='/>
<data key='user.SKLM_APP_PORT,com.ibm.sklm301.linux' value='443'/>
<data key='user.WAS_ADMIN_PORT,com.ibm.sklm301.linux' value='9083'/>
<data key='user.SKLM_APP_NS_PORT,com.ibm.sklm301.linux' value='80'/>
<data key='cic.selector.nl' value='en'/>
</profile>
<preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='/opt/IBM/IBMIMShared'/>
<preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30'/>
<preference name='com.ibm.cic.common.core.preferences.readTimeout' value='45'/>
<preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0'/>
<preference name='offering.service.repositories.areUsed' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.http.disablePreemptiveAuthentication' value='false'/>
<preference name='http.ntlm.auth.kind' value='NTLM'/>
<preference name='http.ntlm.auth.enableIntegrated.win32' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false'/>
<preference name='PassportAdvantageIsEnabled' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false'/>
<preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false'/>
<preference name='com.ibm.cic.common.sharedUI.showErrorLog' value='true'/>
<preference name='com.ibm.cic.common.sharedUI.showWarningLog' value='true'/>
<preference name='com.ibm.cic.common.sharedUI.showNoteLog' value='true'/>
</agent-input>
```

Migration de la version 3.0 vers la version 3.0.1

```
<?xml version="1.0" encoding="UTF-8"?>
<!--L'attribut "acceptLicense" est obsolète. La ligne de commande "-acceptLicense" permet d'accepter les contrats de licence.-->
<agent-input clean='true' >

<server>
<repository location='/disk1/im'/>
<repository location='/disk1/'/>
</server>

<install modify='false'>
<offering profile='IBM Installation Manager' id='com.ibm.cic.agent' features='agent_core,agent_jre' installFixes='none'/>
<offering profile='IBM DB2 SKLM301' id='com.ibm.sklm301.db2.lin.ofng' features='main.feature' installFixes='none'/>
```

```
<offering profile='IBM WebSphere Application Server V9.0_1' id='com.ibm.websphere.BASE.v90'  features='core.feature,ejbdeploy,thincli
<offering profile='IBM WebSphere Application Server V9.0_1' id='com.ibm.java.jdk.v8' features='com.ibm.sdk.8' installFixes='none'/>
<offering profile='IBM Security Key Lifecycle Manager v3.0.1' id='com.ibm.sklm301.linux' features='main.feature' installFixes='none'/
</install>

<profile id='IBM DB2 SKLM301' installLocation='/opt/IBM/DB2SKLMV301'>
<data key='eclipseLocation' value='/opt/IBM/DB2SKLMV301'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='linux'/>
<data key='cic.selector.arch' value='s390x'/>
<data key='cic.selector.ws' value='gtk'/>
<data key='user.DB2_ADMIN_ID,com.ibm.sklm301.db2.lin.ofng' value='sklmdb31'/>
<!--The DB2 Group name should not be more than 8 characters -->
<data key='user.DB2_ADMIN_GRP,com.ibm.sklm301.db2.lin.ofng' value='sklmdb31'/>
<data key='user.DB2_ADMIN_PWD,com.ibm.sklm301.db2.lin.ofng' value='QTh/0AiFvrljhs9gnOYkGA=='/>
<data key='user.CONFIRM_PASSWORD,com.ibm.sklm301.db2.lin.ofng' value='QTh/0AiFvrljhs9gnOYkGA=='/>
<data key='user.DB2_DB_LHOME,com.ibm.sklm301.db2.lin.ofng' value='/home/sklmdb31'/>
<data key='user.DB2_DB_HOME,com.ibm.sklm301.db2.lin.ofng' value='/home/sklmdb31'/>
<data key='user.DB2_DB_NAME,com.ibm.sklm301.db2.lin.ofng' value='SKLMDB31'/>
<data key='user.DB2_DB_PORT,com.ibm.sklm301.db2.lin.ofng' value='50050'/>
<data key='user.DB2_EXISTS,com.ibm.sklm301.db2.lin.ofng' value='false'/>
<data key='user.DB2_LOCATION,com.ibm.sklm301.db2.lin.ofng' value='/opt/IBM/DB2SKLMV301'/>
<data key='cic.selector.nl' value='en'/>
</profile>
<profile id='IBM Installation Manager' installLocation='/opt/IBM/InstallationManager/eclipse' kind='self'>
<data key='eclipseLocation' value='/opt/IBM/InstallationManager/eclipse'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='linux'/>
<data key='cic.selector.arch' value='s390x'/>
<data key='cic.selector.ws' value='gtk'/>
</profile>
<profile id='IBM WebSphere Application Server V9.0_1' installLocation='/opt/IBM/WebSphere30/AppServer'>
<data key='eclipseLocation' value='/opt/IBM/WebSphere30/AppServer'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='linux'/>
<data key='cic.selector.arch' value='s390x'/>
<data key='cic.selector.ws' value='gtk'/>
<data key='cic.selector.nl' value='en'/>
</profile>
<profile id='IBM Security Key Lifecycle Manager v3.0.1' installLocation='/opt/IBM/SKLMV301'>
<data key='eclipseLocation' value='/opt/IBM/SKLMV301'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='linux'/>
<data key='cic.selector.arch' value='s390x'/>
<data key='cic.selector.ws' value='gtk'/>
<data key='user.EKM_PROPFILE,com.ibm.sklm301.linux' value='/opt/IBM/KeyManagerConfig.properties'/>
<data key='user.EKM_MIGRATION,com.ibm.sklm301.linux' value='false'/>
<data key='user.PROFILE_NAME,com.ibm.sklm301.linux' value='KLMProfile'/>
<data key='user.WAS_ADMIN_ID,com.ibm.sklm301.linux' value='tipadmin'/>
<data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm301.linux' value='e9PjN93MeQxwnSs9VXJFMw=='/>
<data key='user.WAS_ADMIN_CONF_PWD,com.ibm.sklm301.linux' value='e9PjN93MeQxwnSs9VXJFMw=='/>
<data key='user.SKLM_ADMIN_USER,com.ibm.sklm301.linux' value='TKLMAdmin'/>
<data key='user.SKLM_ADMIN_PASSWORD,com.ibm.sklm301.linux' value='9YTRJMRIydDSdfhaHPs1ag=='/>
<data key='user.SKLM_ADMIN_CONF_PWD,com.ibm.sklm301.linux' value='9YTRJMRIydDSdfhaHPs1ag=='/>
<data key='user.TKLM_VERSION,com.ibm.sklm301.linux' value='3.0.0.0'/>
<data key='user.TKLM_TIP_HOME,com.ibm.sklm301.linux' value='/opt/IBM/WebSphere/AppServer/'/>
<data key='user.TKLM_INSTALLED,com.ibm.sklm301.linux' value='true'/>
<data key='user.INSTALL_AS_FP,com.ibm.sklm301.linux' value='false'/>
<data key='user.TKLM_DB_PWD,com.ibm.sklm301.linux' value='/6vJK3fcU3QxHY+RVfCFVw=='/>
<data key='user.TKLM_KEYSTORE_PWD,com.ibm.sklm301.linux' value='fufgZbY47EfxLYarBAIxeQ=='/>
<data key='user.SKLM_APP_PORT,com.ibm.sklm301.linux' value='443'/>
<data key='user.WAS_ADMIN_PORT,com.ibm.sklm301.linux' value='9083'/>
<data key='user.SKLM_APP_NS_PORT,com.ibm.sklm301.linux' value='80'/>
<data key='cic.selector.nl' value='en'/>
</profile>
<preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='/opt/IBM/IBMIMShared'/>
<preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30'/>
<preference name='com.ibm.cic.common.core.preferences.readTimeout' value='45'/>
<preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0'/>
<preference name='offering.service.repositories.areUsed' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.http.disablePreemptiveAuthentication' value='false'/>
<preference name='http.ntlm.auth.kind' value='NTLM'/>
<preference name='http.ntlm.auth.enableIntegrated.win32' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false'/>
<preference name='PassportAdvantageIsEnabled' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false'/>
<preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false'/>
<preference name='com.ibm.cic.common.sharedUI.showErrorLog' value='true'/>
<preference name='com.ibm.cic.common.sharedUI.showWarningLog' value='true'/>
<preference name='com.ibm.cic.common.sharedUI.showNoteLog' value='true'/>
</agent-input>
```

Migration des versions antérieures 2.5, 2.6, 2.7 et 3.0 vers la version 3.0.1 sur des systèmes AIX

Les exemples de fichiers de réponses contiennent des réponses pour une installation sur un système AIX sur lequel la migration d'une version 2.5, 2.6, 2.7 et 3.0 précédente d'IBM Security Key Lifecycle Manager vers la version 3.0.1 est effectuée.

Remarque : Pour déterminer s'il existe une installation d'IBM Security Key Lifecycle Manager d'une version antérieure nécessitant une migration, utilisez la commande **tklmVersionInfo**. Par exemple, entrez la commande suivante dans une session Jython :

```
print AdminTask.tklmVersionInfo<>
```

Migration de la version 2.5 vers la version 3.0.1

```
<?xml version="1.0" encoding="UTF-8"?>
<!--L'attribut "acceptLicense" est obsolète. La ligne de commande "-acceptLicense" permet d'accepter les contrats de licence.-->
<agent-input clean='true'>
<server>
<repository location='/disk1/im'/>
<repository location='/disk1/'/>
</server>
<install modify='false'>
<offering profile='IBM Installation Manager' id='com.ibm.cic.agent' features='agent_core,agent_jre' installFixes='none'/>
<offering profile='IBM DB2 SKLM301' id='com.ibm.sklm301.db2.aix.ofng' features='main.feature' installFixes='none'/>
<offering profile='IBM WebSphere Application Server V9.0' id='com.ibm.websphere.BASE.v90' features='core.feature,ejbdeploy,thinclient,em
<offering profile='IBM WebSphere Application Server V9.0' id='com.ibm.java.jdk.v8' features='com.ibm.sdk.8' installFixes='none'/>
<offering profile='IBM Security Key Lifecycle Manager v3.0.1' id='com.ibm.sklm301.aix' features='main.feature' installFixes='none'/>
</install>
<profile id='IBM DB2 SKLM301' installLocation='/opt/IBM/DB2SKLMV301'>
<data key='eclipseLocation' value='/opt/IBM/DB2SKLMV301'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='aix'/>
<data key='cic.selector.arch' value='ppc64'/>
<data key='cic.selector.ws' value='gtk'/>
<data key='user.DB2_ADMIN_ID,com.ibm.sklm301.db2.aix.ofng' value='sklmdb31'/>
<!--The DB2 Group name should not be more than 8 characters -->
<data key='user.DB2_ADMIN_GRP,com.ibm.sklm301.db2.aix.ofng' value='bin'/>
<data key='user.DB2_ADMIN_PWD,com.ibm.sklm301.db2.aix.ofng' value='QTh/0AiFvrljhs9gnOYkGA=='/>
<data key='user.CONFIRM_PASSWORD,com.ibm.sklm301.db2.aix.ofng' value='QTh/0AiFvrljhs9gnOYkGA=='/>
<data key='user.DB2_DB_HOME,com.ibm.sklm301.db2.aix.ofng' value='/home/sklmdb31'/>
<data key='user.DB2_DB_NAME,com.ibm.sklm301.db2.aix.ofng' value='SKLMDB31'/>
<data key='user.DB2_DB_PORT,com.ibm.sklm301.db2.aix.ofng' value='50050'/>
<data key='user.DB2_EXISTS,com.ibm.sklm301.db2.aix.ofng' value='false'/>
<data key='user.DB2_LOCATION,com.ibm.sklm301.db2.aix.ofng' value='/opt/IBM/DB2SKLMV301'/>
<data key='cic.selector.nl' value='en'/>
</profile>
<profile id='IBM Installation Manager' installLocation='/opt/IBM/InstallationManager/eclipse' kind='self'>
<data key='eclipseLocation' value='/opt/IBM/InstallationManager/eclipse'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='aix'/>
<data key='cic.selector.arch' value='ppc'/>
<data key='cic.selector.ws' value='gtk'/>
</profile>
<profile id='IBM WebSphere Application Server V9.0' installLocation='/usr/IBM/WebSphere30/AppServer'>
<data key='eclipseLocation' value='/usr/IBM/WebSphere30/AppServer'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='aix'/>
<data key='cic.selector.arch' value='ppc64'/>
<data key='cic.selector.ws' value='gtk'/>
<data key='cic.selector.nl' value='en'/>
</profile>
<profile id='IBM Security Key Lifecycle Manager v3.0.1' installLocation='/opt/IBM/SKLMV301'>
<data key='eclipseLocation' value='/opt/IBM/SKLMV301'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='aix'/>
<data key='cic.selector.arch' value='ppc64'/>
<data key='cic.selector.ws' value='gtk'/>
<data key='user.EKM_PROPFILE,com.ibm.sklm301.aix' value='/opt/IBM/KeyManagerConfig.properties'/>
<data key='user.EKM_MIGRATION,com.ibm.sklm301.aix' value='false'/>
<data key='user.PROFILE_NAME,com.ibm.sklm301.aix' value='KLMProfile'/>
<data key='user.WAS_ADMIN_ID,com.ibm.sklm301.aix' value='tipadmin'/>
<data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm301.aix' value='e9PjN93MeQxwnSs9VXJFMw=='/>
<data key='user.WAS_ADMIN_CONF_PWD,com.ibm.sklm301.aix' value='e9PjN93MeQxwnSs9VXJFMw=='/>
<data key='user.SKLM_ADMIN_USER,com.ibm.sklm301.aix' value='TKLMAdmin'/>
<data key='user.SKLM_ADMIN_PASSWORD,com.ibm.sklm301.aix' value='9YTRJMRIydDSdfhaHPs1ag=='/>
<data key='user.SKLM_ADMIN_CONF_PWD,com.ibm.sklm301.aix' value='9YTRJMRIydDSdfhaHPs1ag=='/>
<data key='user.TKLM_VERSION,com.ibm.sklm301.aix' value='2.0.1'/>
<data key='user.TKLM_TIP_HOME,com.ibm.sklm301.aix' value='/opt/IBM/tivoli/tiptklmV2/'/>
<data key='user.TKLM_INSTALLED,com.ibm.sklm301.aix' value='true'/>
```

```
<data key='user.TKLM_DB_PWD,com.ibm.sklm301.aix' value='/6vJK3fcU3QxHY+RVfCFVw==' />
<data key='user.TKLM_KEYSTORE_PWD,com.ibm.sklm301.aix' value='fufgZbY47EfxLYarBAIxeQ==' />
<data key='user.SKLM_APP_PORT,com.ibm.sklm301.aix' value='443' />
<data key='user.WAS_ADMIN_PORT,com.ibm.sklm301.aix' value='9083' />
<data key='user.SKLM_APP_NS_PORT,com.ibm.sklm301.aix' value='80' />
<data key='cic.selector.nl' value='en' />
</profile>
<preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='/opt/IBM/IBMIMShared' />
<preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30' />
<preference name='com.ibm.cic.common.core.preferences.readTimeout' value='45' />
<preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0' />
<preference name='offering.service.repositories.areUsed' value='true' />
<preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false' />
<preference name='com.ibm.cic.common.core.preferences.http.disablePreemptiveAuthentication' value='false' />
<preference name='http.ntlm.auth.kind' value='NTLM' />
<preference name='http.ntlm.auth.enableIntegrated.win32' value='true' />
<preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true' />
<preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false' />
<preference name='PassportAdvantageIsEnabled' value='false' />
<preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false' />
<preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false' />
<preference name='com.ibm.cic.common.sharedUI.showErrorLog' value='true' />
<preference name='com.ibm.cic.common.sharedUI.showWarningLog' value='true' />
<preference name='com.ibm.cic.common.sharedUI.showNoteLog' value='true' />
</agent-input>
```

Migration de la version 2.6 vers la version 3.0.1

```
<?xml version="1.0" encoding="UTF-8"?>
<!--L'attribut "acceptLicense" est obsolète. La ligne de commande "-acceptLicense" permet d'accepter les contrats de licence.-->
<agent-input clean='true'>
<server>
<repository location='/disk1/im' />
<repository location='/disk1/' />
</server>
<install modify='false'>
<offering profile='IBM Installation Manager' id='com.ibm.cic.agent' features='agent_core,agent_jre' installFixes='none' />
<offering profile='IBM DB2 SKLM301' id='com.ibm.sklm301.db2.aix.ofng' features='main.feature' installFixes='none' />
<offering profile='IBM WebSphere Application Server V9.0' id='com.ibm.websphere.BASE.v90' features='core.feature,ejbdeploy,thinclient
<offering profile='IBM WebSphere Application Server V9.0' id='com.ibm.java.jdk.v8' features='com.ibm.sdk.8' installFixes='none' />
<offering profile='IBM Security Key Lifecycle Manager v3.0.1' id='com.ibm.sklm301.aix' features='main.feature' installFixes='none' />
</install>
<profile id='IBM DB2 SKLM301' installLocation='/opt/IBM/DB2SKLMV301'>
<data key='eclipseLocation' value='/opt/IBM/DB2SKLMV301' />
<data key='user.import.profile' value='false' />
<data key='cic.selector.os' value='aix' />
<data key='cic.selector.arch' value='ppc64' />
<data key='cic.selector.ws' value='gtk' />
<data key='user.DB2_ADMIN_ID,com.ibm.sklm301.db2.aix.ofng' value='sklmdb31' />
<!--The DB2 Group name should not be more than 8 characters -->
<data key='user.DB2_ADMIN_GRP,com.ibm.sklm301.db2.aix.ofng' value='bin' />
<data key='user.DB2_ADMIN_PWD,com.ibm.sklm301.db2.aix.ofng' value='QTh/0AiFvrljhs9gnOYkGA==' />
<data key='user.CONFIRM_PASSWORD,com.ibm.sklm301.db2.aix.ofng' value='QTh/0AiFvrljhs9gnOYkGA==' />
<data key='user.DB2_DB_HOME,com.ibm.sklm301.db2.aix.ofng' value='/home/sklmdb31' />
<data key='user.DB2_DB_NAME,com.ibm.sklm301.db2.aix.ofng' value='SKLMDB31' />
<data key='user.DB2_DB_PORT,com.ibm.sklm301.db2.aix.ofng' value='50050' />
<data key='user.DB2_EXISTS,com.ibm.sklm301.db2.aix.ofng' value='false' />
<data key='user.DB2_LOCATION,com.ibm.sklm301.db2.aix.ofng' value='/opt/IBM/DB2SKLMV301' />
<data key='cic.selector.nl' value='en' />
</profile>
<profile id='IBM Installation Manager' installLocation='/opt/IBM/InstallationManager/eclipse' kind='self'>
<data key='eclipseLocation' value='/opt/IBM/InstallationManager/eclipse' />
<data key='user.import.profile' value='false' />
<data key='cic.selector.os' value='aix' />
<data key='cic.selector.arch' value='ppc' />
<data key='cic.selector.ws' value='gtk' />
</profile>
<profile id='IBM WebSphere Application Server V9.0' installLocation='/usr/IBM/WebSphere30/AppServer'>
<data key='eclipseLocation' value='/usr/IBM/WebSphere30/AppServer' />
<data key='user.import.profile' value='false' />
<data key='cic.selector.os' value='aix' />
<data key='cic.selector.arch' value='ppc64' />
<data key='cic.selector.ws' value='gtk' />
<data key='cic.selector.nl' value='en' />
</profile>
<profile id='IBM Security Key Lifecycle Manager v3.0.1' installLocation='/opt/IBM/SKLMV301'>
<data key='eclipseLocation' value='/opt/IBM/SKLMV301' />
<data key='user.import.profile' value='false' />
<data key='cic.selector.os' value='aix' />
<data key='cic.selector.arch' value='ppc64' />
<data key='cic.selector.ws' value='gtk' />
<data key='user.EKM_PROPFILE,com.ibm.sklm301.aix' value='/opt/IBM/KeyManagerConfig.properties' />
<data key='user.EKM_MIGRATION,com.ibm.sklm301.aix' value='false' />
<data key='user.PROFILE_NAME,com.ibm.sklm301.aix' value='KLMProfile' />
<data key='user.WAS_ADMIN_ID,com.ibm.sklm301.aix' value='tipadmin' />
<data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm301.aix' value='e9PjN93MeQxwnSs9VXJFMw==' />
<data key='user.WAS_ADMIN_CONF_PWD,com.ibm.sklm301.aix' value='e9PjN93MeQxwnSs9VXJFMw==' />
<data key='user.SKLM_ADMIN_USER,com.ibm.sklm301.aix' value='TKLMAdmin' />
<data key='user.SKLM_ADMIN_PASSWORD,com.ibm.sklm301.aix' value='9YTRJMRIydDSdfhaHPs1ag==' />
<data key='user.SKLM_ADMIN_CONF_PWD,com.ibm.sklm301.aix' value='9YTRJMRIydDSdfhaHPs1ag==' />
```

```
<data key='user.TKLM_VERSION,com.ibm.sklm301.aix' value='2.0.1'/>
<data key='user.TKLM_TIP_HOME,com.ibm.sklm301.aix' value='/opt/IBM/tivoli/tiptklmV2/'/>
<data key='user.TKLM_INSTALLED,com.ibm.sklm301.aix' value='true'/>
<data key='user.TKLM_DB_PWD,com.ibm.sklm301.aix' value='/6vJK3fcU3QxHY+RVfCFVw=='/>
<data key='user.TKLM_KEYSTORE_PWD,com.ibm.sklm301.aix' value='fufgZbY47EfxLYarBAIxeQ=='/>
<data key='user.SKLM_APP_PORT,com.ibm.sklm301.aix' value='443'/>
<data key='user.WAS_ADMIN_PORT,com.ibm.sklm301.aix' value='9083'/>
<data key='user.SKLM_APP_NS_PORT,com.ibm.sklm301.aix' value='80'/>
<data key='cic.selector.nl' value='en'/>
</profile>
<preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='/opt/IBM/IBMIMShared'/>
<preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30'/>
<preference name='com.ibm.cic.common.core.preferences.readTimeout' value='45'/>
<preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0'/>
<preference name='offering.service.repositories.areUsed' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.http.disablePreemptiveAuthentication' value='false'/>
<preference name='http.ntlm.auth.kind' value='NTLM'/>
<preference name='http.ntlm.auth.enableIntegrated.win32' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false'/>
<preference name='PassportAdvantageIsEnabled' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false'/>
<preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false'/>
<preference name='com.ibm.cic.common.sharedUI.showErrorLog' value='true'/>
<preference name='com.ibm.cic.common.sharedUI.showWarningLog' value='true'/>
<preference name='com.ibm.cic.common.sharedUI.showNoteLog' value='true'/>
</agent-input>
```

Migration de la version 2.7 vers la version 3.0.1

```
<?xml version="1.0" encoding="UTF-8"?>
<!--L'attribut "acceptLicense" est obsolète. La ligne de commande "-acceptLicense" permet d'accepter les contrats de licence.-->
<agent-input clean='true'>
<server>
<repository location='/disk1/im'/>
<repository location='/disk1/'/>
</server>
<install modify='false'>
<offering profile='IBM Installation Manager' id='com.ibm.cic.agent' features='agent_core,agent_jre' installFixes='none'/>
<offering profile='IBM DB2 SKLM301' id='com.ibm.sklm301.db2.aix.ofng' features='main.feature' installFixes='none'/>
<offering profile='IBM WebSphere Application Server V9.0_1' id='com.ibm.websphere.BASE.v90'  features='core.feature,ejbdeploy,thinclient
<offering profile='IBM WebSphere Application Server V9.0_1' id='com.ibm.java.jdk.v8' features='com.ibm.sdk.8' installFixes='none'/>
<offering profile='IBM Security Key Lifecycle Manager v3.0.1' id='com.ibm.sklm301.aix' features='main.feature' installFixes='none'/>
</install>
<profile id='IBM DB2 SKLM301' installLocation='/opt/IBM/DB2SKLMV301'>
<data key='eclipseLocation' value='/opt/IBM/DB2SKLMV301'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='aix'/>
<data key='cic.selector.arch' value='ppc64'/>
<data key='cic.selector.ws' value='gtk'/>
<data key='user.DB2_ADMIN_ID,com.ibm.sklm301.db2.aix.ofng' value='sklmdb31'/>
<!--The DB2 Group name should not be more than 8 characters -->
<data key='user.DB2_ADMIN_GRP,com.ibm.sklm301.db2.aix.ofng' value='bin'/>
<data key='user.DB2_ADMIN_PWD,com.ibm.sklm301.db2.aix.ofng' value='QTh/0AiFvrljhs9gnOYkGA=='/>
<data key='user.CONFIRM_PASSWORD,com.ibm.sklm301.db2.aix.ofng' value='QTh/0AiFvrljhs9gnOYkGA=='/>
<data key='user.DB2_DB_HOME,com.ibm.sklm301.db2.aix.ofng' value='/home/sklmdb31'/>
<data key='user.DB2_DB_NAME,com.ibm.sklm301.db2.aix.ofng' value='SKLMDB31'/>
<data key='user.DB2_DB_PORT,com.ibm.sklm301.db2.aix.ofng' value='50050'/>
<data key='user.DB2_EXISTS,com.ibm.sklm301.db2.aix.ofng' value='false'/>
<data key='user.DB2_LOCATION,com.ibm.sklm301.db2.aix.ofng' value='/opt/IBM/DB2SKLMV301'/>
<data key='cic.selector.nl' value='en'/>
</profile>
<profile id='IBM Installation Manager' installLocation='/opt/IBM/InstallationManager/eclipse' kind='self'>
<data key='eclipseLocation' value='/opt/IBM/InstallationManager/eclipse'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='aix'/>
<data key='cic.selector.arch' value='ppc'/>
<data key='cic.selector.ws' value='gtk'/>
</profile>
<profile id='IBM WebSphere Application Server V9.0' installLocation='/usr/IBM/WebSphere30/AppServer'>
<data key='eclipseLocation' value='/usr/IBM/WebSphere30/AppServer'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='aix'/>
<data key='cic.selector.arch' value='ppc64'/>
<data key='cic.selector.ws' value='gtk'/>
<data key='cic.selector.nl' value='en'/>
</profile>
<profile id='IBM Security Key Lifecycle Manager v3.0.1' installLocation='/opt/IBM/SKLMV301'>
<data key='eclipseLocation' value='/opt/IBM/SKLMV301'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='aix'/>
<data key='cic.selector.arch' value='ppc64'/>
<data key='cic.selector.ws' value='gtk'/>
<data key='user.EKM_PROPFILE,com.ibm.sklm301.aix' value='/opt/IBM/KeyManagerConfig.properties'/>
<data key='user.EKM_MIGRATION,com.ibm.sklm301.aix' value='false'/>
<data key='user.PROFILE_NAME,com.ibm.sklm301.aix' value='KLMProfile'/>
<data key='user.WAS_ADMIN_ID,com.ibm.sklm301.aix' value='tipadmin'/>
<data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm301.aix' value='e9PjN93MeQxwnSs9VXJFMw=='/>
<data key='user.WAS_ADMIN_CONF_PWD,com.ibm.sklm301.aix' value='e9PjN93MeQxwnSs9VXJFMw=='/>
```

```
<data key='user.SKLM_ADMIN_USER,com.ibm.sklm301.aix' value='TKLMAdmin'/>
<data key='user.SKLM_ADMIN_PASSWORD,com.ibm.sklm301.aix' value='9YTRJMRIydDSdfhaHPs1ag=='/>
<data key='user.SKLM_ADMIN_CONF_PWD,com.ibm.sklm301.aix' value='9YTRJMRIydDSdfhaHPs1ag=='/>
<data key='user.TKLM_VERSION,com.ibm.sklm301.aix' value='2.0.1'/>
<data key='user.TKLM_TIP_HOME,com.ibm.sklm301.aix' value='/opt/IBM/tivoli/tiptklmV2/'/>
<data key='user.TKLM_INSTALLED,com.ibm.sklm301.aix' value='true'/>
<data key='user.TKLM_DB_PWD,com.ibm.sklm301.aix' value='/6vJK3fcU3QxHY+RVfCFVw=='/>
<data key='user.TKLM_KEYSTORE_PWD,com.ibm.sklm301.aix' value='fufgZbY47EfxLYarBAIxeQ=='/>
<data key='user.SKLM_APP_PORT,com.ibm.sklm301.aix' value='443'/>
<data key='user.WAS_ADMIN_PORT,com.ibm.sklm301.aix' value='9083'/>
<data key='user.SKLM_APP_NS_PORT,com.ibm.sklm301.aix' value='80'/>
<data key='cic.selector.nl' value='en'/>
</profile>
<preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='/opt/IBM/IBMIMShared'/>
<preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30'/>
<preference name='com.ibm.cic.common.core.preferences.readTimeout' value='45'/>
<preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0'/>
<preference name='offering.service.repositories.areUsed' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.http.disablePreemptiveAuthentication' value='false'/>
<preference name='http.ntlm.auth.kind' value='NTLM'/>
<preference name='http.ntlm.auth.enableIntegrated.win32' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false'/>
<preference name='PassportAdvantageIsEnabled' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false'/>
<preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false'/>
<preference name='com.ibm.cic.common.sharedUI.showErrorLog' value='true'/>
<preference name='com.ibm.cic.common.sharedUI.showWarningLog' value='true'/>
<preference name='com.ibm.cic.common.sharedUI.showNoteLog' value='true'/>
</agent-input>
```

Migration de la version 3.0 vers la version 3.0.1

```
<?xml version="1.0" encoding="UTF-8"?>
<!--L'attribut "acceptLicense" est obsolète. La ligne de commande "-acceptLicense" permet d'accepter les contrats de licence.-->
<agent-input clean='true'>
<server>
<repository location='/disk1/im'/>
<repository location='/disk1/'/>
</server>
<install modify='false'>
<offering profile='IBM Installation Manager' id='com.ibm.cic.agent' features='agent_core,agent_jre' installFixes='none'/>
<offering profile='IBM DB2 SKLM301' id='com.ibm.sklm301.db2.aix.ofng' features='main.feature' installFixes='none'/>
<offering profile='IBM WebSphere Application Server V9.0_1' id='com.ibm.websphere.BASE.v90'  features='core.feature,ejbdeploy,thincli
<offering profile='IBM WebSphere Application Server V9.0_1' id='com.ibm.java.jdk.v8' features='com.ibm.sdk.8' installFixes='none'/>
<offering profile='IBM Security Key Lifecycle Manager v3.0.1' id='com.ibm.sklm301.aix' features='main.feature' installFixes='none'/>
</install>
<profile id='IBM DB2 SKLM301' installLocation='/opt/IBM/DB2SKLMV301'>
<data key='eclipseLocation' value='/opt/IBM/DB2SKLMV301'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='aix'/>
<data key='cic.selector.arch' value='ppc64'/>
<data key='cic.selector.ws' value='gtk'/>
<data key='user.DB2_ADMIN_ID,com.ibm.sklm301.db2.aix.ofng' value='sklmdb31'/>
<!--The DB2 Group name should not be more than 8 characters -->
<data key='user.DB2_ADMIN_GRP,com.ibm.sklm301.db2.aix.ofng' value='bin'/>
<data key='user.DB2_ADMIN_PWD,com.ibm.sklm301.db2.aix.ofng' value='QTh/0AiFvrljhs9gnOYkGA=='/>
<data key='user.CONFIRM_PASSWORD,com.ibm.sklm301.db2.aix.ofng' value='QTh/0AiFvrljhs9gnOYkGA=='/>
<data key='user.DB2_DB_HOME,com.ibm.sklm301.db2.aix.ofng' value='/home/sklmdb31'/>
<data key='user.DB2_DB_NAME,com.ibm.sklm301.db2.aix.ofng' value='SKLMDB31'/>
<data key='user.DB2_DB_PORT,com.ibm.sklm301.db2.aix.ofng' value='50050'/>
<data key='user.DB2_EXISTS,com.ibm.sklm301.db2.aix.ofng' value='false'/>
<data key='user.DB2_LOCATION,com.ibm.sklm301.db2.aix.ofng' value='/opt/IBM/DB2SKLMV301'/>
<data key='cic.selector.nl' value='en'/>
</profile>
<profile id='IBM Installation Manager' installLocation='/opt/IBM/InstallationManager/eclipse' kind='self'>
<data key='eclipseLocation' value='/opt/IBM/InstallationManager/eclipse'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='aix'/>
<data key='cic.selector.arch' value='ppc'/>
<data key='cic.selector.ws' value='gtk'/>
</profile>
<profile id='IBM WebSphere Application Server V9.0_1' installLocation='/usr/IBM/WebSphere30/AppServer'>
<data key='eclipseLocation' value='/usr/IBM/WebSphere30/AppServer'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='aix'/>
<data key='cic.selector.arch' value='ppc64'/>
<data key='cic.selector.ws' value='gtk'/>
<data key='cic.selector.nl' value='en'/>
</profile>
<profile id='IBM Security Key Lifecycle Manager v3.0.1' installLocation='/opt/IBM/SKLMV301'>
<data key='eclipseLocation' value='/opt/IBM/SKLMV301'/>
<data key='user.import.profile' value='false'/>
<data key='cic.selector.os' value='aix'/>
<data key='cic.selector.arch' value='ppc64'/>
<data key='cic.selector.ws' value='gtk'/>
<data key='user.EKM_PROPFILE,com.ibm.sklm301.aix' value='/opt/IBM/KeyManagerConfig.properties'/>
<data key='user.EKM_MIGRATION,com.ibm.sklm301.aix' value='false'/>
<data key='user.PROFILE_NAME,com.ibm.sklm301.aix' value='KLMProfile'/>
```

```
<data key='user.WAS_ADMIN_ID,com.ibm.sklm301.aix' value='tipadmin'/>
<data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm301.aix' value='e9PjN93MeQxwnSs9VXJFMw==/>
<data key='user.WAS_ADMIN_CONF_PWD,com.ibm.sklm301.aix' value='e9PjN93MeQxwnSs9VXJFMw==/>
<data key='user.SKLM_ADMIN_USER,com.ibm.sklm301.aix' value='TKLMAdmin'/>
<data key='user.SKLM_ADMIN_PASSWORD,com.ibm.sklm301.aix' value='9YTRJMRIydDSdfhaHPs1ag==/>
<data key='user.SKLM_ADMIN_CONF_PWD,com.ibm.sklm301.aix' value='9YTRJMRIydDSdfhaHPs1ag==/>
<data key='user.TKLM_VERSION,com.ibm.sklm301.aix' value='3.0.0.0'/>
<data key='user.TKLM_TIP_HOME,com.ibm.sklm301.aix' value='/opt/IBM/WebSphere/AppServer'/>
<data key='user.TKLM_INSTALLED,com.ibm.sklm301.aix' value='true'/>
<data key='user.INSTALL_AS_FP,com.ibm.sklm301.aix' value='false'/>
<data key='user.TKLM_DB_PWD,com.ibm.sklm301.aix' value='/6vJK3fcU3QxHY+RVfCFVw==/>
<data key='user.TKLM_KEYSTORE_PWD,com.ibm.sklm301.aix' value='fufgZbY47EfxLYarBAIxeQ==/>
<data key='user.SKLM_APP_PORT,com.ibm.sklm301.aix' value='443'/>
<data key='user.WAS_ADMIN_PORT,com.ibm.sklm301.aix' value='9083'/>
<data key='user.SKLM_APP_NS_PORT,com.ibm.sklm301.aix' value='80'/>
<data key='cic.selector.nl' value='en'/>
</profile>
<preference name='com.ibm.cic.common.core.preferences.eclipseCache' value='/opt/IBM/IBMIMShared'/>
<preference name='com.ibm.cic.common.core.preferences.connectTimeout' value='30'/>
<preference name='com.ibm.cic.common.core.preferences.readTimeout' value='45'/>
<preference name='com.ibm.cic.common.core.preferences.downloadAutoRetryCount' value='0'/>
<preference name='offering.service.repositories.areUsed' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.ssl.nonsecureMode' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.http.disablePreemptiveAuthentication' value='false'/>
<preference name='http.ntlm.auth.kind' value='NTLM'/>
<preference name='http.ntlm.auth.enableIntegrated.win32' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.preserveDownloadedArtifacts' value='true'/>
<preference name='com.ibm.cic.common.core.preferences.keepFetchedFiles' value='false'/>
<preference name='PassportAdvantageIsEnabled' value='false'/>
<preference name='com.ibm.cic.common.core.preferences.searchForUpdates' value='false'/>
<preference name='com.ibm.cic.agent.ui.displayInternalVersion' value='false'/>
<preference name='com.ibm.cic.common.sharedUI.showErrorLog' value='true'/>
<preference name='com.ibm.cic.common.sharedUI.showWarningLog' value='true'/>
<preference name='com.ibm.cic.common.sharedUI.showNoteLog' value='true'/>
</agent-input>
```

Désinstallation sur des systèmes Windows

L'exemple de fichier de réponses contient des réponses pour la désinstallation sur un système Windows.

```
<?xml version="1.0" encoding="UTF-8"?>
<agent-input clean='true' >
<profile id='IBM Security Key Lifecycle Manager v3.0.1'>
<data key='user.WAS_ADMIN_ID,com.ibm.sklm301.win' value='wasadmin'/>
<data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm301.win' value='e9PjN93MeQxwnSs9VXJFMw==/>
</profile>
<uninstall modify='false'>
<offering id='com.ibm.sklm301.win'  profile='IBM Security Key Lifecycle Manager v3.0.1'  features='main.feature'/>
<offering id='com.ibm.websphere.BASE.v90'  profile='IBM WebSphere Application Server V9.0' features='core.feature,ejbdeploy,thinclient,e
<offering id='com.ibm.java.jdk.v8' profile='IBM WebSphere Application Server V9.0' features='com.ibm.sdk.8'/>
<offering id='com.ibm.sklm301.db2.win.ofng'  profile='IBM DB2 SKLM301' features='main.feature'/>
</uninstall>
</agent-input>
```

Désinstallation sur des systèmes Linux

Le fichier de réponses exemple contient des réponses pour la désinstallation sur un système Linux.

```
<?xml version="1.0" encoding="UTF-8"?>
<agent-input clean='true' >
<profile id='IBM Security Key Lifecycle Manager v3.0.1'>
<data key='user.WAS_ADMIN_ID,com.ibm.sklm301.linux' value='wasadmin'/>
<data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm301.linux' value='e9PjN93MeQxwnSs9VXJFMw==/>
</profile>
<uninstall modify='false'>
<offering id='com.ibm.sklm301.linux'  profile='IBM Security Key Lifecycle Manager v3.0.1' features='main.feature'/>
<offering id='com.ibm.websphere.BASE.v90'  profile='IBM WebSphere Application Server V9.0' features='core.feature,ejbdeploy,thinclient,e
<offering id='com.ibm.java.jdk.v8' profile='IBM WebSphere Application Server V9.0' features='com.ibm.sdk.8'/>
<offering id='com.ibm.sklm301.db2.lin.ofng'  profile='IBM DB2 SKLM301' features='main.feature'/>
</uninstall>
</agent-input>
```

Désinstallation sur des systèmes Linux for System z

Le fichier de réponses exemple contient des réponses pour la désinstallation sur un système Linux for System z.

```
<?xml version="1.0" encoding="UTF-8"?>
<agent-input clean='true' >
<profile id='IBM Security Key Lifecycle Manager v3.0.1'>
<data key='user.WAS_ADMIN_ID,com.ibm.sklm301.linux' value='wasadmin'/>
```

```
<data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm301.linux' value='e9PjN93MeQxwnSs9VXJFMw==’/>
</profile>
<uninstall modify='false'>
<offering id='com.ibm.sklm301.linux'  profile='IBM Security Key Lifecycle Manager v3.0.1' features='main.feature'/>
<offering id='com.ibm.websphere.BASE.v90'  profile='IBM WebSphere Application Server V9.0' features='core.feature,ejbdeploy,thinclien
<offering id='com.ibm.java.jdk.v8' profile='IBM WebSphere Application Server V9.0' features='com.ibm.sdk.8'/>
<offering id='com.ibm.sklm301.db2.lin.ofng'  profile='IBM DB2 SKLM301' features='main.feature'/>
</uninstall>
</agent-input>
```

Désinstallation sur des systèmes Linux PPC

Le fichier de réponses exemple contient des réponses pour la désinstallation sur un système Linux PPC.

```
<?xml version="1.0" encoding="UTF-8"?>
<agent-input clean='true' >
<profile id='IBM Security Key Lifecycle Manager v3.0.1'>
<data key='user.WAS_ADMIN_ID,com.ibm.sklm301.linux' value='wasadmin'/>
<data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm301.linux' value='e9PjN93MeQxwnSs9VXJFMw==’/>
</profile>
<uninstall modify='false'>
<offering id='com.ibm.sklm301.linux'  profile='IBM Security Key Lifecycle Manager v3.0.1' features='main.feature'/>
<offering id='com.ibm.websphere.BASE.v90'  profile='IBM WebSphere Application Server V9.0' features='core.feature,ejbdeploy,thinclien
<offering id='com.ibm.java.jdk.v8' profile='IBM WebSphere Application Server V9.0' features='com.ibm.sdk.8'/>
<offering id='com.ibm.sklm301.db2.lin.ofng'  profile='IBM DB2 SKLM301' features='main.feature'/>
</uninstall>
</agent-input>
```

Désinstallation sur des systèmes AIX

Le fichier de réponses exemple contient des réponses pour la désinstallation sur un système AIX.

```
<?xml version="1.0" encoding="UTF-8"?>
<agent-input clean='true' >
<profile id='IBM Security Key Lifecycle Manager v3.0.1'>
<data key='user.WAS_ADMIN_ID,com.ibm.sklm301.aix' value='wasadmin'/>
<data key='user.WAS_ADMIN_PASSWORD,com.ibm.sklm301.aix' value='e9PjN93MeQxwnSs9VXJFMw==’/>
</profile>
<uninstall modify='false'>
<offering id='com.ibm.sklm301.aix'  profile='IBM Security Key Lifecycle Manager v3.0.1' features='main.feature'/>
<offering id='com.ibm.websphere.BASE.v90'  profile='IBM WebSphere Application Server V9.0' features='core.feature,ejbdeploy,thinclien
<offering id='com.ibm.java.jdk.v8' profile='IBM WebSphere Application Server V9.0' features='com.ibm.sdk.8'/>
<offering id='com.ibm.sklm301.db2.aix.ofng'  profile='IBM DB2 SKLM301' features='main.feature'/>
</uninstall>
</agent-input>
```

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

Nombres

A

B

C

D

E

F

G

I

J

K

L

M

N

P

R

S

T

U

V

W

X