Dell PowerVault Encryption Key Manager

Guide de démarrage rapide pour LTO Ultrium 4 et LTO Ultrium 5

Le présent guide est destiné à vous aider dans la ***configuration de base*** du chiffrement d'unités de bande LTO de 4ème et de 5ème génération. Visitez le site Web **http://support.dell.com** pour télécharger les dernières versions de microprogramme d'unité et de bandothèque avant d'installer et de configurer Dell PowerVault Encryption Key Manager.

Dell PowerVault Encryption Key Manager (appelé Encryption Key Manager dans le reste du texte) est un programme informatique Java™ destiné à aider les unités de bande activées pour le chiffrement dans la génération, la protection, le stockage et la gestion des clés de chiffrement. Ces clés sont utilisées pour chiffrer les informations écrites sur, et déchiffrer les informations lues à partir d'un support de bande LTO. Encryption Key Manager fonctionne sous Linux® et Windows® ; il s'agit d'une ressource partagée déployée à plusieurs emplacements au sein d'une entreprise.

Ce document explique de manière concise l'installation et la configuration d'Encryption Key Manager à l'aide de l'interface graphique ou de commandes. Il indique également comment utiliser le type de magasin de clés JCEKS : il s'agit du type de magasin de clés le plus facile et le plus transportable de tous les magasins de clés pris en charge. Pour plus d'informations sur une étape particulière ou un autre type de magasin de clés pris en charge, voir le document *Dell Encryption Key Manager - Guide d'utilisation*, disponible à l'adresse suivante : **http://support.dell.com** ou sur le support Dell Encryption Key Manager fourni avec votre produit.

Remarque : INFORMATIONS IMPORTANTES CONCERNANT LA CONFIGURATION DU SERVEUR D'HOTE Encryption Key Manager : Il est recommandé que les machines hébergeant le programme Dell Encryption Key Manager utilisent la mémoire ECC afin de minimiser les risques de perte de données. Encryption Key Manager exécute la fonction de demande de création de clés de chiffrement et communique ces clés aux unités de bande LTO-4 et LTO-5. Le matériel de clé encapsulé (format chiffré) réside dans la mémoire système lors de son traitement par Encryption Key Manager. Notez que le matériel de clé doit être correctement transféré vers l'unité de bande appropriée de sorte que les données écrites sur une cartouche puissent être récupérées (déchiffrées). Si, pour une raison ou une autre, le matériel de clé est corrompu à cause d'une erreur de bit dans la mémoire système, et que ce matériel de clé est utilisé pour écrire dans une cartouche, alors les données écrites dans cette cartouche ne seront pas récupérables (c'est-à-dire déchiffrées à une date ultérieure). Des dispositifs de protection sont mis en place pour éviter que de telles erreurs de données se produisent. Toutefois, si la machine hébergeant Encryption Key Manager n'utilise pas la mémoire Error Correction Code (ECC), il se peut que le matériel de clé soit corrompu au sein de la mémoire système et que cette corruption provoque une perte des données. Cette éventualité est rare, mais il est toujours recommandé que les machines hébergeant les applications vitales (telles que Encryption Key Manager) utilisent la mémoire ECC.

Première étape : Installation du logiciel Encryption Key Manager

1. Insérez votre CD-ROM Dell Encryption Key Manager. Si l'installation ne démarre pas automatiquement sous Windows, naviguez vers le CD-ROM et cliquez deux fois sur Install_Windows.bat.

   Sous Linux, l'installation ne démarre pas automatiquement. Accédez au répertoire principal du CD-ROM et entrez `Install_Linux.sh`.

   Un contrat de licence utilisateur final s'affiche. Vous devez accepter ce contrat de licence afin de poursuivre l'installation.

   L'installation copie les éléments (documentation, fichiers d'interface graphique et fichiers de propriété de configuration) appropriés à votre système d'exploitation sur le CD-ROM et les colle sur votre disque dur. Au cours de l'installation, le programme vérifie si l'environnement IBM Java Runtime Environment correct est installé sur votre système. S'il ne le trouve pas, il est automatiquement installé.

   Une fois l'installation terminée, l'interface graphique est lancée.

Méthode 1 : Configuration d'Encryption Key Manager à l'aide de l'interface graphique

Cette procédure crée une configuration de base. Une fois terminée, le serveur Encryption Key Manager est démarré.

1. Si l'interface graphique n'est pas démarrée, ouvrez-la comme suit :

   Sous Windows
   Naviguez vers c:\ekm\gui et cliquez sur `LaunchEKMGui.bat`

   Sous Linux
   Naviguez vers /var/ekm/gui et entrez `. ./LaunchEKMGui.sh`
   Remarque : indiquez . ./ (point espace point barre oblique) avant la commande de shell Linux pour vous assurer que le shell puisse trouver le script.

2. Sur la page Configuration d'EKM (figure 1), entrez les données dans les zones requises (signalées par un astérisque *). Cliquez sur le point d'interrogation situé à droite de n'importe quelle zone pour obtenir sa description. Cliquez sur **Suivant** pour accéder à la page Configuration du certificat.

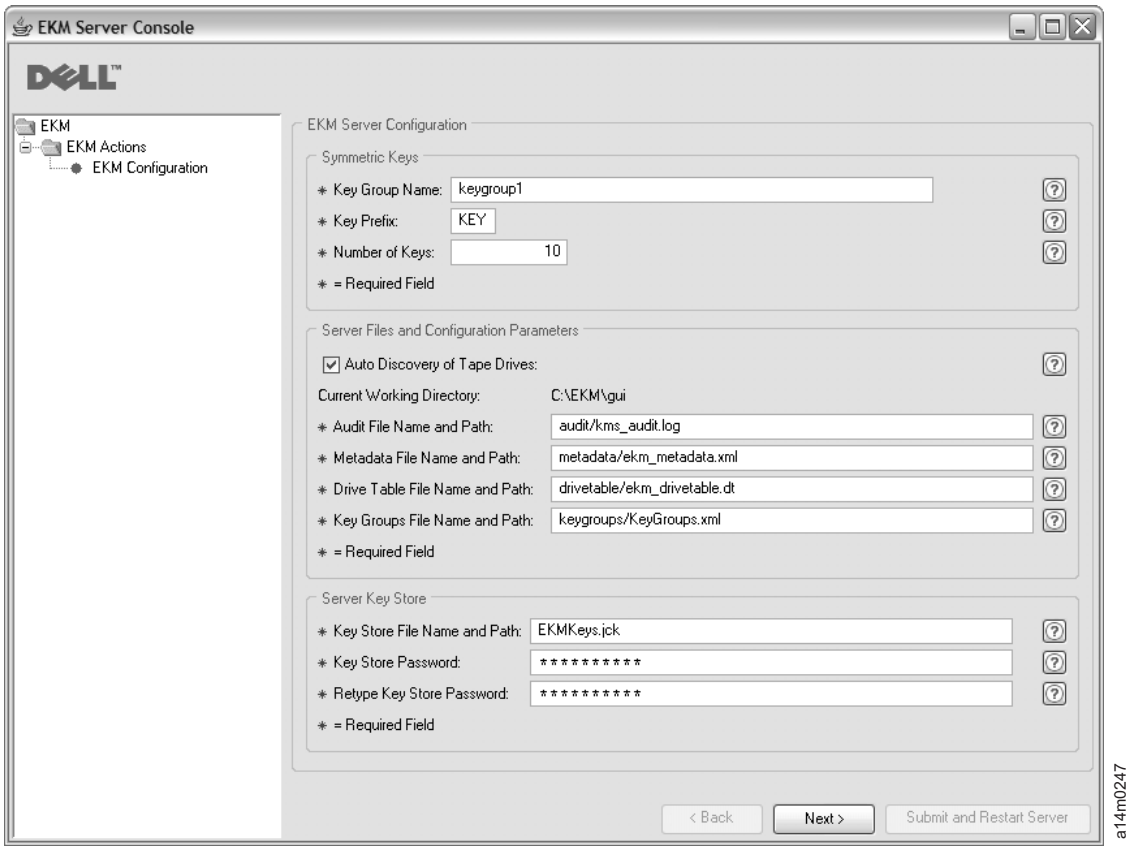

Figure 1. Page Configuration du serveur EKM

Remarques :

a. Le serveur Encryption Key Manager doit être actualisé à l'aide de l'interface graphique une fois les unités ajoutées via la reconnaissance automatique, de sorte à vérifier qu'elles sont stockées dans la table des unités.

b. Une fois le mot de passe du magasin de clés défini, **ne le modifiez pas** à moins que sa sécurité n'ait été violée. Les mots de passe sont chiffrés de sorte à éliminer tout risque potentiel de sécurité. La modification du mot de passe du magasin de clés nécessite que le mot de passe de chaque clé

du magasin de clés soit modifiée individuellement à l'aide de la commande **keytool**. Voir la section «Modification des mots de passe du magasin de clés» du manuel *Dell Encryption Key Manager - Guide d'utilisation*.

3. Sur la page Configuration du certificat de serveur EKM, (figure 2) entrez l'alias du magasin de clés et renseignez toute zone supplémentaire pouvant servir à identifier le certificat et son objectif. Cliquez sur **Valider et démarrer le serveur**.

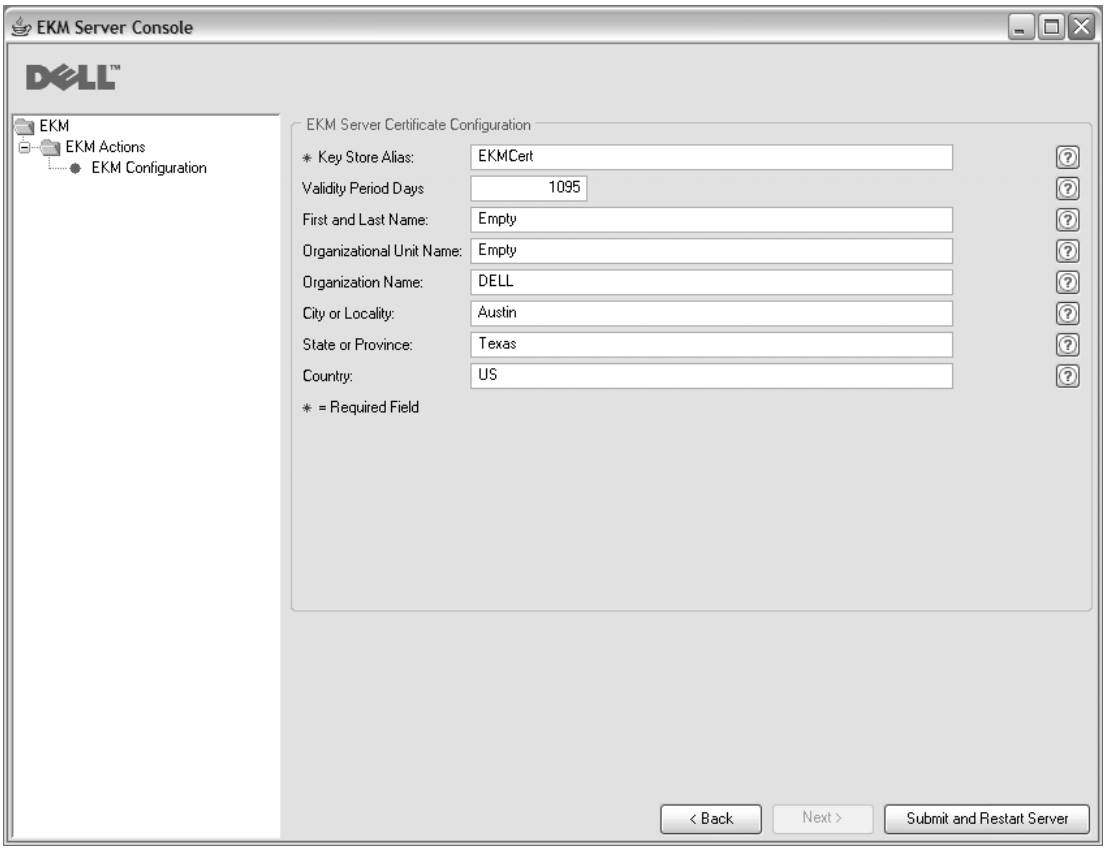

Figure 2. Page Configuration du certificat de serveur EKM

Remarque : Si vous arrêtez l'interface graphique de Encryption Key Manager au cours de la génération de clé, vous devez réinstaller Encryption Key Manager.

La corruption d'un fichier de magasin de clés se produit si vous arrêtez le processus de génération de clé Encryption Key Manager avant qu'il soit terminé. Pour se remettre de cet événement, procédez comme suit :

- Si Encryption Key Manager a été arrêté au cours de l'installation initiale, accédez au répertoire de EKM (exemple x:\ekm). Supprimez le répertoire et redémarrez l'installation.
- Si Encryption Key Manager a été arrêté au cours de l'ajout d'un nouveau groupe de clés, arrêtez votre serveur Encryption Key Manager, restaurez votre fichier de magasin de clés à l'aide de la dernière sauvegarde en date du magasin de clés (ce fichier se trouve dans le dossier x:\ekm\gui\backupfiles). Notez que le nom du fichier de sauvegarde contient la date et l'horodatage (par exemple, 2007_11_19_16_38_31_EKMKeys.jck). La date et l'horodatage doivent être supprimés une fois le fichier copié dans le répertoire x:\ekm\gui. Redémarrez le serveur Encryption Key Manager et ajoutez le groupe de clés précédemment arrêté.

4. Une fenêtre de sauvegarde (figure 3) s'affiche et vous rappelle de sauvegarder vos fichiers de données Encryption Key Manager. Entrez le chemin de sauvegarde des données. Cliquez sur **Sauvegarde**.

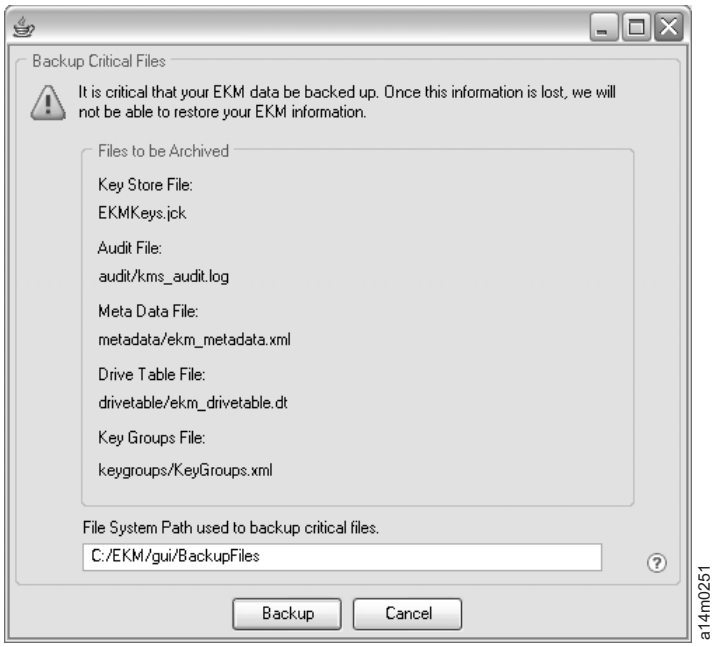

Figure 3. Fenêtre Sauvegarde des fichiers critiques

5. La page Connexion utilisateur s'affiche. Entrez le nom d'utilisateur par défaut EKMAdmin et le mot de passe par défaut changeME. Cliquez sur **Connexion**.

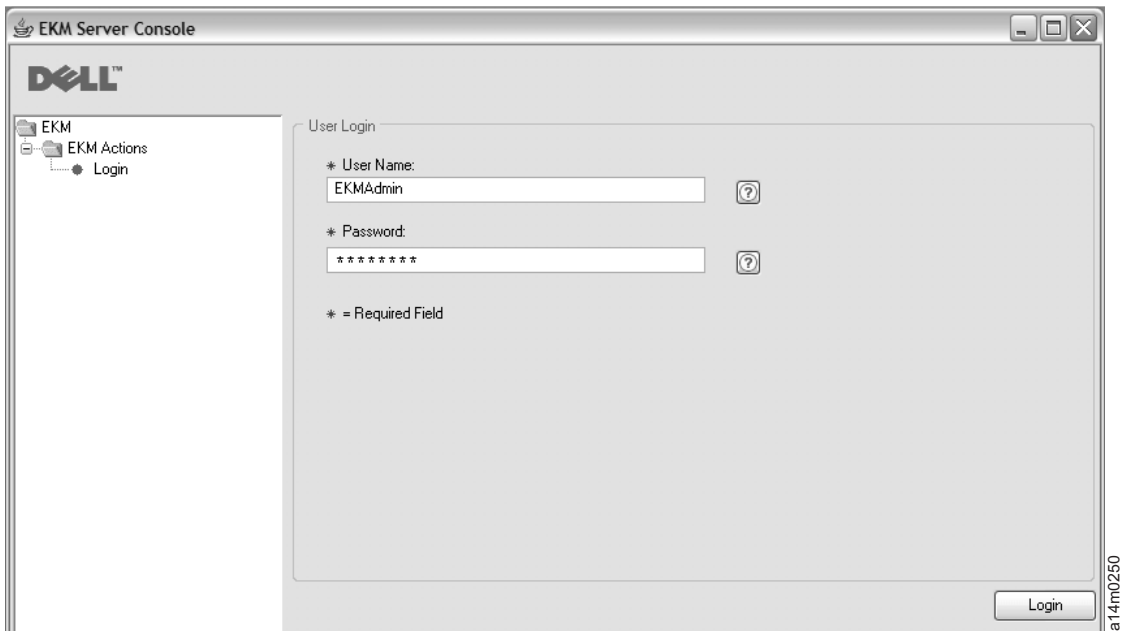

Figure 4. Page Connexion utilisateur

Le serveur Dell Encryption Key Manager est lancé en arrière-plan.

6. Sélectionnez **Moniteur d'état du serveur** dans le navigateur de l'interface graphique pour vérifier que le serveur Encryption Key Manager est en fonctionnement.

Comment localiser l'adresse IP correcte de l'hôte

Les limitations de l'interface graphique Encryption Key Manager actuelle peuvent empêcher d'afficher l'adresse IP de l'hôte Encryption Key Manager dans le moniteur d'état du serveur :

- Si l'hôte est configuré avec une adresse IPv6, l'application Encryption Key Manager ne pourra pas afficher l'adresse IP.
- Si l'application Encryption Key Manager est installée sur un système Linux, l'application Encryption Key Manager affiche l'adresse localhost et non le port IP actif en cours.

a. Pour récupérer l'adresse IP actuelle du système hôte, localisez l'adresse du port IP en accédant à la configuration du réseau.
   - Sous Windows, ouvrez une fenêtre de commande et entrez `ipconfig`.
   - Sous Linux, entrez `isconfig`.

Comment identifier le port SSL de EKM

a. Démarrez le serveur Encryption Key Manager à l'aide de la ligne de commande.
   - Sous Windows, accédez à cd `c:\ekm` et cliquez sur **startServer.bat**
   - Sous Linux, accédez à `/var/ekm` et entrez `startServer.sh`
   - Pour plus d'informations, voir la section «Démarrage, régénération et arrêt du serveur du gestionnaire de clés» du manuel *Dell Encryption Key Manager - Guide d'utilisation*.

b. Démarrez le client CLI à l'aide de la ligne de commande.
   - Sous Windows, accédez à cd `c:\ekm` et cliquez sur **startClient.bat**
   - Sous Linux, accédez à `/var/ekm` et entrez `startClient.sh`
   - Pour plus d'informations, voir la section «Démarrage du client d'interface de ligne de commande» du manuel *Dell Encryption Key Manager - Guide d'utilisation*.

c. Connectez-vous à un client CLI sur le serveur Encryption Key Manager à l'aide de la commande suivante :

   ```
   login –ekmuser ID utilisateur –ekmpassword mot de passe
   ```

   où *ID utilisateur* = EKMAdmin et *mot de passe* = changeME (Mot de passe par défaut. Si vous avez modifié le mot de passe par défaut, utilisez votre nouveau mot de passe.)

   Une fois connecté, le message `User successfully logged in` s'affiche.

d. Identifiez le port SSL en entrant la commande suivante :

   ```
   status
   ```

   La réponse qui s'affiche doit être identique à ce qui suit : `server is running. TCP port: 3801, SSL port: 443`.

   Notez le numéro du port SSL configuré et vérifiez qu'il s'agit du port utilisé pour configurer vos paramètres de chiffrement gérés par la bibliothèque.

e. Déconnectez-vous de la ligne de commande. Entrez la commande suivante :

   ```
   exit
   ```

   Fermez la fenêtre de commande .

Méthode 2 : Configuration d'Encryption Key Manager à l'aide de commandes

Etape 1. Création d'un magasin de clés JCEKS

ATTENTION : il est fortement recommandé qu'une copie de Encryption Key Manager et de tous les fichiers associés soit effectuée de manière fréquente. Si les clés de chiffrement Encryption Key Manager sont perdues ou corrompues, il n'existe aucune méthode de restauration des données chiffrées.

Créez un magasin de clés et remplissez-le avec un certificat et une clé privée. Le certificat permet de sécuriser les communications entre les serveurs Encryption Key Manager et celles du client CLI Encryption Key Manager. Cette commande **keytool** crée un magasin de clés JCEKS appelé EKMKeys.jck, puis le remplit avec un certificat et intègre à la clé privée l'alias d'ekmcert. Ce certificat est valide pendant 5 ans. Lorsque ce certificat arrive à expiration, les communications entre les serveurs Encryption Key Manager et entre le client CLI Encryption Key Manager et le serveur Encryption Key Manager peuvent ne plus fonctionner. Supprimez l'ancien certificat expiré et créez-en un autre, comme indiqué dans cette étape.

```
keytool -keystore EKMKeys.jck -storetype jceks -genkey -alias ekmcert -keyAlg RSA -keysize 2048 –validity 1825
```

La commande keytool affiche les information utilisées pour créer un certificat autorisant votre identification Encryption Key Manager. Les invites, avec leurs exemples de réponses, ressemblent à ce qui suit :

```
What is your first and last name? [Unknown]:  ekmcert
What is the name of your organizational unit?   [Unknown]:  EKM
What is the name of your organization? [Unknown]:  Dell
What is the name of your City or Locality?   [Unknown]: Austin
What is the name of your State or Province?   [Unknown]:  TX
What is the two-letter country code for this unit? [Unknown]:  US
Is CN=ekmcert, OU=EKM, O=Dell, L=Austin, ST=TX, C=US correct?(type "yes" or "no"):
```

Entrez yes et appuyez sur Entrée.

Etape 2. Génération de clés de chiffrement

Remarque : Avant d'utiliser la commande keytool pour la première fois dans une session, exécutez le script **updatePath** pour définir l'environnement approprié.

Sous Windows
Naviguez vers `cd c:\ekm` et cliquez sur updatePath.bat

Sous Linux
Naviguez vers /var/ekm et entrez `. ./updatePath.sh`
Remarque : indiquez . ./ (point espace point barre oblique) avant la commande de shell Linux pour vous assurer que le shell puisse trouver le script.

Pour le chiffrement LTO, Encryption Key Manager nécessite un nombre défini de clés symétriques à pré-générer et stocker dans un magasin de clés. Cette commande **keytool** génère des clés AES 32 256 bits et les stocke dans le magasin de clés créé à l'étape 3. Exécutez cette commande à partir du répertoire Encryption Key Manager pour que le fichier du magasin de clés soit créé dans ce répertoire. Les clés créées portent les noms key0000000000000000 à key0000000000000001f.

```
keytool –keystore EKMKeys.jck –storetype jceks –genseckey –keyAlg aes –keysize 256 –aliasrange key00-1f
```

Cette commande vous invite à entrer un mot de passe de magasin de clés de sorte à y accéder. Entrez le mot de passe de votre choix, puis appuyez sur Entrée. Appuyez de nouveau sur Entrée lorsque vous êtes invité à entrer un mot de passe de clé, car ces informations ne sont pas nécessaires. N'entrez pas un mot de passe nouveau ou différent. De cette manière, le mot de passe de clé devient identique à celui du

magasin de clé. Notez le mot de passe du magasin de clés entré ici car vous en aurez besoin ultérieurement lors du démarrage de Encryption Key Manager.

Remarque : Une fois le mot de passe du magasin de clés défini, ne le modifiez pas à moins que sa sécurité n'ait été violée. La modification du mot de passe du magasin de clés nécessite que toutes les propriétés de mot de passe du fichier de configuration soient également modifiées. Les mots de passe sont chiffrés de sorte à éliminer tout risque potentiel de sécurité.

Etape 3. Démarrage du serveur Encryption Key Manager

Pour démarrer le serveur Encryption Key Manager sans interface graphique, exécutez le script startServer :

Sous Windows

Naviguez vers `cd c:\ekm\ekmserver` et cliquez sur startServer.bat

Sous Linux

Naviguez vers /var/ekm/ekmserver et entrez `. ./startServer.sh`
Remarque : indiquez . ./ (point espace point barre oblique) avant la commande de shell Linux pour vous assurer que le shell puisse trouver le script.

ATTENTION : il est fortement recommandé qu'une copie de Encryption Key Manager et de tous les fichiers associés soit effectuée de manière fréquente. Si les clés de chiffrement Encryption Key Manager sont perdues ou corrompues, il n'existe aucune méthode de restauration des données chiffrées.

Etape 4. Démarrage du client d'interface de ligne de commande Encryption Key Manager

Pour démarrer le client CLI Encryption Key Manager, lancez le script startClient :

Sous Windows

Naviguez vers `cd c:\ekm\ekmclient` et cliquez sur startClient.bat

Sous Linux

Naviguez vers /var/ekm\ekmclient et entrez `. ./startClient.sh`
Remarque : indiquez . ./ (point espace point barre oblique) avant la commande de shell Linux pour vous assurer que le shell puisse trouver le script.

Une fois le client CLI connecté au serveur du gestionnaire de clés, vous pouvez exécuter n'importe quelle commande CLI. Utilisez la commande quit pour arrêter le client CLI. Le client s'arrête automatiquement après 10 minutes d'inutilisation. Pour plus d'informations sur la commande LCI, consultez le manuel *Dell Encryption Key Manager - Guide d'utilisation*, disponible à l'adresse : **http://support.dell.com** ou sur le support Dell Encryption Key Manager fournit avec votre produit.

Informations supplémentaires

Consultez les publications suivantes pour plus d'informations.

- *Dell Encryption Key Manager - Guide d'utilisation* (disponible sur votre CD-ROM Dell Encryption Key Manager et sur le site Web **http://support.dell.com**).
- Livre blanc *Library Managed Encryption for Tape* indiquant les meilleures méthodes de chiffrement des bandes LTO (disponible à l'adresse **http://www.dell.com**).