

Dell Encryption Key Manager 3.0

Guide de déploiement



Remarques, précautions et avertissements

-  **REMARQUE:** une REMARQUE indique des informations importantes qui peuvent vous aider à mieux utiliser l'ordinateur.
-  **PRÉCAUTION:** une PRÉCAUTION vous avertit d'un risque d'endommagement du matériel ou de perte de données si les consignes ne sont pas respectées.
-  **AVERTISSEMENT:** un AVERTISSEMENT signale un risque d'endommagement du matériel, de blessure corporelle, voire de mort.

Les informations que contient cette publication sont sujettes à modification sans préavis.

© 2011 Dell Inc. Tous droits réservés. Imprimé aux États-Unis

La reproduction de ce document, de quelque manière que ce soit, sans l'autorisation écrite de Dell Inc. est strictement interdite.

Marques commerciales utilisées dans ce document : Dell™, le logo Dell, Dell Precision™, OptiPlex™, Latitude™, PowerEdge™, PowerVault™, PowerConnect™, OpenManage™, EqualLogic™, Compellent™, KACE™, FlexAddress™ et Vostro™ sont des marques commerciales de Dell Inc. Intel®, Pentium®, Xeon®, Core® et Celeron® sont des marques déposées d'Intel Corporation aux États-Unis et dans d'autres pays. AMD® est une marque déposée, et AMD Opteron™, AMD Phenom™ et AMD Sempron™ sont des marques commerciales d'Advanced Micro Devices, Inc. Microsoft®, Windows®, Windows Server®, Internet Explorer®, MS-DOS® et Windows Vista® sont des marques commerciales ou déposées de Microsoft Corporation aux États-Unis et/ou dans d'autres pays. Red Hat® et Red Hat® Enterprise Linux® sont des marques déposées de Red Hat, Inc. aux États-Unis et/ou d'autres pays. Novell® et SUSE® sont des marques déposées de Novell Inc. aux États-Unis et dans d'autres pays. Oracle® est une marque déposée d'Oracle Corporation et/ou de ses filiales. Citrix®, Xen®, XenServer® et XenMotion® sont des marques commerciales ou déposées de Citrix Systems, Inc. aux États-Unis et/ou dans d'autres pays. VMware®, Virtual SMP®, vMotion®, vCenter® et vSphere® sont des marques commerciales ou déposées de VMware, Inc. aux États-Unis ou dans d'autres pays. IBM® est une marque déposée d'International Business Machines Corporation.

D'autres marques et noms commerciaux peuvent être utilisés dans cette publication pour faire référence aux entités se réclamant de ces marques et noms ou à leurs produits Dell Inc. rejette tout intérêt exclusif dans les marques et noms ne lui appartenant pas.

2011 – 12

Rev. A00

Table des matières

Remarques, précautions et avertissements.....	2
Chapitre 1: Présentation.....	5
Configuration matérielle et logicielle requise.....	6
Configuration matérielle requise pour le serveur.....	6
Configuration requise pour le navigateur.....	6
Configuration requise pour le système d'exploitation.....	6
Chapitre 2: Installation d'EKM 3.0.....	7
Préparation de l'installation d'EKM 3.0 sous Microsoft Windows.....	7
Préparation de l'installation d'EKM 3.0 sous Red Hat Enterprise Linux.....	8
Préparation de l'installation d'EKM 3.0 sous SUSE Linux Enterprise Server.....	8
Exécution de la procédure d'installation d'EKM 3.0.....	9
Chapitre 3: Configuration des serveurs EKM 3.0 principal et secondaire.....	13
Installation d'EKM 3.0 sur le serveur principal.....	13
Utilisation d'EKM 3.0 sur le serveur principal.....	13
Installation d'EKM 3.0 sur le serveur secondaire.....	13
Utilisation d'EKM 3.0 sur le serveur secondaire.....	14
Désinstallation d'EKM 3.0 sur les serveurs principal et secondaire.....	14
Chapitre 4: Exécution de sauvegardes et restauration à partir d'une sauvegarde.....	15
Création d'une sauvegarde du magasin de clés.....	15
Restauration à partir d'une sauvegarde.....	16
Chapitre 5: Utilisation d'EKM 3.0.....	17
Connexion au portail Encryption Key Manager 3.0.....	17
Création du magasin de clés maître.....	18
Activation du pare-feu sur le serveur EKM 3.0.....	18
Configuration d'EKM 3.0 pour accepter les périphériques qui le contactent pour obtenir des clés.....	19
Création d'un groupe de périphériques.....	20
Création de groupes de clés pour des groupes de périphériques.....	20
Ajout d'un périphérique à un groupe de périphériques.....	21
Ajout et suppression de clés dans des groupes de clés.....	22
Suppression de groupes de clés.....	23
Vérification du certificat de serveur.....	23
Affichage des détails du certificat de serveur.....	24
Connexion au serveur WebSphere.....	24

Démarrage et arrêt du serveur EKM 3.0 sous Windows	25
Démarrage et arrêt du serveur EKM 3.0 sous Linux.....	25
Chapitre 6: Migration et fusion.....	27
Migration d'une installation Encryption Key Manager (EKM) 2.X lors de l'installation d'EKM 3.0.....	29
Procédure de migration d'EKM 2.X vers EKM 3.0.....	29
Fusion d'Encryption Key Manager (EKM) 2.X dans EKM 3.0 après l'installation d'EKM 3.0.....	31
Prérequis de l'outil de fusion.....	33
Procédure de fusion entre EKM 2.X et EKM 3.0.....	33
Vérification de la fusion ou de la migration d'EKM 2.X vers EKM 3.0.....	37
Échec de la fusion.....	38
Fusion d'installations EKM 2.X supplémentaires dans EKM 3.0.....	38
Suppression du certificat ekmcert, des clés et des groupes de clés, et changement du nom des périphériques.....	39
Chapitre 7: Désinstallation d'EKM 3.0.....	45
Désinstallation d'EKM 3.0 sous Windows.....	45
Désinstallation d'EKM 3.0 sous Linux.....	46
Chapitre 8: Dépannage.....	47
Contacter Dell.....	47
Vérifications des prérequis système.....	49
Codes d'erreur.....	51
Fichiers de référence Windows.....	53
Fichiers de référence Linux.....	55
Désinstallation manuelle d'EKM 3.0.....	57
Désinstallation manuelle d'EKM 3.0 sous Windows.....	57
Désinstallation manuelle d'EKM 3.0 sous Linux.....	58
Réinstallation d'EKM 3.0.....	59
Questions fréquemment posées.....	59
Problèmes connus et solutions.....	62
Installation de la bibliothèque compat-libstdc+.....	65

Présentation

Dell Encryption Key Manager (EKM) 3.0 est un utilitaire de cryptage qui sécurise les données stockées sur des cartouches à bande LTO en gérant des clés de cryptage pour les solutions d'automatisation des bandes Dell, y compris les gammes ML et TL PowerVault. EKM 3.0 gère le cycle de vie des clés de cryptage des bandes : génération, distribution, administration et suppression.

Ce guide explique comment installer et configurer Dell Encryption Key Manager 3.0 (EKM 3.0), et y exécuter des opérations de base. Dell vous recommande de lire attentivement ce document avant d'installer EKM 3.0.

Ce guide fournit des informations sur les éléments suivants :

- Configuration matérielle et logicielle requise pour EKM 3.0
- Installation et désinstallation d'EKM 3.0 sous Windows et sous Linux
- Configuration d'EKM 3.0
- Opérations de base dans EKM 3.0
- Migration d'EKM 2.X pendant l'installation d'EKM 3.0 et fusion d'EKM 2.X dans une installation EKM 3.0 configurée
- Questions fréquemment posées, informations de débogage, messages d'erreur courants et coordonnées du support technique



REMARQUE: EKM 3.0 est basé sur IBM Tivoli Key Lifecycle Manager (TKLM) V2 FixPack 2, mais il a été personnalisé pour prendre en charge les environnements de bibliothèque de bandes Dell : nous avons sélectionné les fonctions de TKLM propres aux bandes.

Pour consulter des informations d'utilisation d'EKM 3.0 absentes du présent guide, consultez la documentation de TKLM, notamment les documents suivants :

- IBM Tivoli Key Manager 2,0 *Quick Start Guide* (Guide de démarrage d'IBM Tivoli Key Manager 2.0)
- IBM Tivoli Key Manager 2,0 *Installation and Configuration Guide* (Guide d'installation et de configuration d'IBM Tivoli Key Manager 2.0)
- IBM Tivoli Key Manager 2,0 *Product Overview/Scenario Guide* (Guide de présentation des produits/scénarios d'IBM Tivoli Key Manager 2.0)

Pour savoir comment accéder à la documentation TKLM, consultez la section **Documentation and Reference Materials** (Documentation et informations de référence) du fichier **ReadThisFirst.txt** sur le support d'installation d'EKM 3.0.

Certains écrans et fonctions présentés dans la documentation d'IBM TKLM ne sont pas activés dans Dell EKM 3.0. Ce dernier contient uniquement le sous-ensemble de fonctions nécessaire pour prendre en charge les bibliothèques de bandes Dell PowerVault.



REMARQUE: Pour connaître l'utilisation et la configuration recommandées pour Dell EKM 3.0, consultez la section **Best Practices** (Meilleures pratiques) du fichier **ReadThisFirst.txt** sur le support d'installation d'EKM 3.0.



REMARQUE: Pour consulter les informations les plus récentes, notamment les améliorations et corrections de bug apportées au produit, consultez les Notes de mise à jour, à l'adresse suivante : support.dell.com/manuals. Accédez à **Software** → **Systems Management** → **Dell Encryption Key Manager**. (Logiciel > Systems Management > Dell Encryption Key Manager)

Configuration matérielle et logicielle requise

Configuration matérielle requise pour le serveur

La configuration matérielle minimale requise pour le serveur de gestion des clés (matériel sur lequel vous allez installer EKM 3.0) est la suivante :

- UC : 2,3 GHz
- Mémoire : 4 Go de mémoire ECC
- Espace disque disponible (pour l'installation d'EKM 3.0 et le stockage standard des clés) : 5 Go

 **REMARQUE:** Si le système où vous installez EKM 3.0 comporte 24 UC ou plus, reportez-vous aux Notes de mise à jour d'EKM 3.0 pour en savoir plus sur la mise à jour d'EKM 3.0 après l'installation. Pour accéder aux Notes de mise à jour d'EKM 3.0, reportez-vous à support.dell.com/manuals, puis naviguez vers **Software** → **Systems Management** → **Dell Encryption Key Manager** (Logiciel > Systems Management > Dell Encryption Key Manager).

Configuration requise pour le navigateur

EKM 3.0 prend en charge les navigateurs suivants :

- Microsoft Internet Explorer Version 7.0
- Microsoft Internet Explorer Version 8.0, mode Affichage de compatibilité
- Firefox Version 3.0.x (EKM 3.0 ne prend pas en charge Firefox Version 3.5 et supérieure.)

 **REMARQUE:** JavaScript doit être activé pour que toutes les fonctions d'EKM 3.0 soient opérationnelles. Reportez-vous à la documentation de votre navigateur pour savoir comment activer JavaScript.

Configuration requise pour le système d'exploitation

EKM 3.0 prend en charge les systèmes d'exploitation suivants :

- Windows Server 2003 R2 avec Service Pack 2, versions 32 et 64 bits, éditions Standard et Enterprise
- Windows Server 2008 avec Service Pack 2, versions 32 et 64 bits, éditions Standard et Enterprise
- Windows Server 2008 R2, éditions Standard et Enterprise
- Red Hat Enterprise Linux (RHEL) 4.X, Advanced Server (AS), version 32 bits
- Red Hat Enterprise Linux (RHEL) 5.X, versions 32 et 64 bits
- SUSE Linux Enterprise Server (SLES) 10 avec Service Pack 4, version 64 bits
- SUSE Linux Enterprise Server (SLES) 11 avec Service Pack 1, version 64 bits

 **REMARQUE:** EKM 3.0 ne prend pas en charge VMware ni Microsoft Hyper-V Server.

 **REMARQUE:** Pour en savoir plus sur la configuration requise et les limitations applicables à une configuration avec serveurs principal et secondaire, reportez-vous à [Setting up Primary and Secondary EKM 3.0 Servers](#) (Configuration des serveurs EKM 3.0 principal et secondaire).

 **REMARQUE:** EKM 3.0 vérifie la configuration système requise avant l'installation. Pour en savoir plus, reportez-vous à [System Prerequisite Checks](#) (Vérifications des prérequis système).

Installation d'EKM 3.0

Ce chapitre explique comment installer EKM 3.0 sous Windows et Linux.

-  **REMARQUE:** Si vous utilisez actuellement EKM 2.X, Dell vous recommande de conserver votre infrastructure actuelle (serveurs, systèmes d'exploitation, bibliothèques de bandes, etc. protégés par EKM 2.X), sauf en cas de problème.
EKM 3.0 ne prend pas en charge l'utilisation de machines virtuelles comme hôtes. Si vous utilisez une machine virtuelle comme hôte EKM 2.X, vous devez conserver votre installation EKM 2.X ou migrer vers un serveur physique.
-  **REMARQUE:** Si vous prévoyez de migrer votre installation EKM 2.X vers EKM 3.0, reportez-vous à [Migrating an Encryption Key Manager \(EKM\) 2.X Version during the EKM 3.0 Installation](#) (Migration d'une installation Encryption Key Manager (EKM) 2.X lors de l'installation d'EKM 3.0) avant de commencer l'installation d'EKM 3.0.
-  **REMARQUE:** Dell vous recommande d'installer EKM 3.0 sur un serveur physique dédié qui n'est utilisé pour aucun autre service. Cela garantit que les performances et les temps de réponse d'EKM 3.0 ne sont pas affectés par d'autres applications exécutées sur le même serveur physique.
-  **PRÉCAUTION:** EKM 3.0 prend uniquement en charge l'installation directe depuis le support EKM 3.0. Ne copiez pas le contenu du support EKM 3.0 sur votre disque dur.
-  **REMARQUE:** Les procédures de ce chapitre nécessitent des connaissances d'administrateur système.

Préparation de l'installation d'EKM 3.0 sous Microsoft Windows

Ce chapitre décrit les étapes de préinstallation de Dell Encryption Key Manager 3.0 sous Microsoft Windows.

-  **REMARQUE:** La procédure d'installation prend environ 45 minutes. N'éteignez pas le système tant que l'installation n'est pas terminée.
 -  **REMARQUE:** Vous devez être connecté en tant qu'**administrateur** pour installer EKM 3.0.
 -  **REMARQUE:** Si vous ne souhaitez pas utiliser un mot de passe complexe pour la base de données, désactivez l'option **Le mot de passe doit respecter des exigences de complexité** dans le système d'exploitation avant d'insérer le support d'installation d'EKM 3.0 dans le lecteur.
1. Insérez le disque d'installation d'EKM 3.0 pour Microsoft Windows dans le lecteur du système où vous souhaitez installer EKM 3.0.
 2. Si votre système est configuré pour exécuter autorun à l'insertion d'un DVD, patientez un moment pour que le programme d'installation apparaisse. Si votre système n'est pas configuré pour exécuter autorun, accédez au lecteur DVD et double-cliquez dessus, ou sur **install.exe**, à la racine du lecteur de DVD.
L'écran **Welcome** (Bienvenue) de l'Assistant d'installation EKM 3.0 s'affiche.
-  **REMARQUE:** Si vous souhaitez installer EKM 3.0 sur un partage réseau n'utilisez pas de chemin au format `\<adresse_IP>\partage_EKM_3.0`. À la place, adressez le partage sur une lettre de lecteur. Dans l'Explorateur Windows, utilisez **Tools** → **Map Network Drive** (Outils > Connecter un lecteur réseau) pour créer le chemin d'installation `<lettre_lecteur_partagé>:\<support_EKM_3.0>`.

Passez à l'étape [Performing the EKM 3.0 Installation Procedure](#) (Exécution de la procédure d'installation d'EKM 3.0).

Préparation de l'installation d'EKM 3.0 sous Red Hat Enterprise Linux

Ce chapitre décrit les étapes de préinstallation de Dell Encryption Key Manager 3.0 sous Red Hat Enterprise Linux.

 **REMARQUE:** La procédure d'installation prend environ 45 minutes. N'éteignez pas le système tant que l'installation n'est pas terminée.

Pour préparer l'installation d'EKM 3.0, procédez comme suit :

1. Insérez le disque d'installation d'EKM 3.0 correspondant à votre système d'exploitation dans le lecteur du système où vous souhaitez installer EKM 3.0.
2. Si votre système est configuré pour exécuter autorun à l'insertion d'un DVD, patientez un moment pour que le programme d'installation apparaisse. Si votre système n'est pas configuré pour exécuter autorun, ouvrez une session de terminal avec accès root et accédez au dossier où le DVD EKM 3.0 est monté. Saisissez `./autorun.sh` et appuyez sur **Entrée**.

 **REMARQUE:** Si SELinux est installé et activé, désactivez-le avant de lancer l'installation. Reportez-vous à [System Prerequisite Checks](#) (Vérifications des prérequis système).

 **REMARQUE:** Les systèmes d'exploitation Red Hat comportent souvent une configuration où le bit **noexec** désactive l'exécution des fichiers binaires sur les systèmes de fichiers montés. Si le bit **noexec** du DVD-ROM monté est **disabled** (désactivé), le programme d'installation d'EKM 3.0 ne démarre pas sur le DVD. Pour le lancer, procédez comme suit :

- a) Ouvrez une session de terminal avec accès root.
- b) Démontez le DVD EKM 3.0.
- c) Remontez le DVD EKM 3.0 **en lecture seule** avec l'option **noexec** désactivée, à l'aide des commandes suivantes :

```
mkdir /media/dellmedia mount /dev/<périphérique EKM 3.0><espace>/media/dellmedia cd /media/dellmedia
```

- d) Pour exécuter le programme d'installation, saisissez `./autorun.sh` et appuyez sur **Entrée**.

L'écran **Bienvenue** de l'Assistant d'installation EKM 3.0 s'affiche.

Passez à l'étape [Performing the EKM 3.0 Installation Procedure](#) (Exécution de la procédure d'installation d'EKM 3.0).

Préparation de l'installation d'EKM 3.0 sous SUSE Linux Enterprise Server

Ce chapitre décrit les étapes de préinstallation de Dell Encryption Key Manager 3.0 sous SUSE Linux Enterprise Server (SLES).

 **REMARQUE:** La procédure d'installation prend environ 45 minutes. N'éteignez pas le système tant que l'installation n'est pas terminée.

Pour préparer l'installation d'EKM 3.0, procédez comme suit :

1. Insérez le disque d'installation d'EKM 3.0 correspondant à votre système d'exploitation dans le lecteur de la machine où vous souhaitez installer EKM 3.0.
2. Si votre système est configuré pour exécuter autorun à l'insertion d'un DVD, patientez un moment pour que le programme d'installation apparaisse. Si votre système n'est pas configuré pour exécuter autorun, ouvrez une session de terminal avec accès root et accédez au dossier où le DVD EKM 3.0 est monté. Saisissez `./autorun.sh` et appuyez sur **Entrée**.

L'écran **Welcome** (Bienvenue) de l'Assistant d'installation EKM 3.0 s'affiche.

 **REMARQUE:** Si SELinux est installé et activé, désactivez-le avant de lancer l'installation.

3. Ouvrez le port 50000. Pour ce faire, procédez comme suit :
 - a) Accédez à **Computer (Ordinateur)** → **Places (Emplacements)** → **File System (Système de fichiers)**.
 - b) Double-cliquez sur **etc**.
 - c) Double-cliquez sur **Services**.
 - d) Dans le fichier **Services**, remplacez **50000/tcp** et **50000/udp** par **50100/tcp** et **50100/udp**.
 - e) Cliquez sur **Save** (Enregistrer).

Passez à l'étape « [Exécution de la procédure d'installation d'EKM 3.0](#) ».

Exécution de la procédure d'installation d'EKM 3.0

Ce chapitre explique comment installer EKM 3.0.

 **REMARQUE:** La procédure d'installation prend environ 45 minutes. N'éteignez pas le système tant que l'installation n'est pas terminée.

 **REMARQUE:** Si vous installez EKM 3.0 sur un serveur destiné à jouer le rôle de serveur secondaire EKM 3.0, les mots de passe doivent être identiques à ceux utilisés pour l'installation du serveur principal EKM 3.0.

1. Dans l'écran **Welcome** (Bienvenue) de l'Assistant d'installation EKM 3.0, cliquez sur **Next** (Suivant).
La fenêtre **License Agreement** (Contrat de licence) s'affiche.
2. Cliquez sur le bouton radio approprié pour accepter les termes du contrat de licence.
3. Cliquez sur **Next** (Suivant).

 **REMARQUE:** Le programme d'installation d'EKM 3.0 exécute les vérifications de prérequis système. Il vérifie que le système répond à la configuration minimale requise, puis configure EKM 3.0 pour votre système.

Si un message d'erreur s'affiche, reportez-vous à « [Vérifications des prérequis système](#) ».

L'écran **Reuse Installation Profile** (Réutiliser le profil d'installation) apparaît.

4. *Si vous installez EKM 3.0 pour la première fois*, désélectionnez la case à cocher **Reuse an EKM 3.0 installation profile** (Réutiliser un profil d'installation EKM 3.0).

Si vous réinstallez EKM 3.0 ou que vous installez EKM 3.0 sur le serveur secondaire, et si vous voulez utiliser un profil d'installation enregistré au cours d'une installation précédente, procédez comme suit :

- a) Cochez la case **Reuse an EKM 3.0 installation profile** (Réutiliser un profil d'installation EKM 3.0). La sélection de cette option active le champ **File Location** (Emplacement du fichier).
- b) Cliquez sur **Choose** (Choisir) et accédez au profil d'installation créé lors de la session précédente de configuration et d'installation d'EKM 3.0 (par exemple, **E:\EKM_config.txt** sous Windows ou **/tmp/ekm_config** sous Linux).

Vous pouvez utiliser un lecteur amovible ou un partage réseau pour transférer le profil d'installation depuis l'emplacement où vous l'avez enregistré.

 **REMARQUE:** Le profil d'installation remplit tous les champs de saisie (à l'exception des mots de passe) dans l'interface GUI d'installation, à l'aide des informations utilisées pour l'installation précédente. Si vous utilisez un profil d'installation, vous devez entrer de nouveau tous les mots de passe.

 **REMARQUE:** Si vous installez EKM 3.0 sur un serveur secondaire, vous devez réutiliser le profil d'installation du serveur principal afin de garantir que les paramètres entrés sont les mêmes.

5. Cliquez sur **Next** (Suivant).

L'écran **Database** (Base de données) s'affiche. Cet écran vous permet de créer le compte d'administrateur de la base de données DB2 EKM.

 **REMARQUE:** Cet écran et les deux suivants permettent de créer un compte différent. Prenez note de tous les noms d'utilisateur et mots de passe que vous créez pour ces comptes.

6. Le champ **Database Location** (Emplacement de la base de données) indique par défaut un emplacement prédéfini. Dell vous recommande de conserver cet emplacement par défaut. Il s'agit de l'emplacement où le programme d'installation va placer le logiciel DB2 d'EKM 3.0.
7. Dans le champ **Database User Name** (Nom d'utilisateur de la base de données), entrez un nom d'utilisateur conforme aux critères suivants :
 - Peut uniquement inclure des lettres minuscules (a–z), des chiffres (0–9) et le caractère souligné (_)
 - Ne peut pas dépasser 8 caractères
 - Ne peut pas commencer par « ibm », « sys » ou « sql », ni par un chiffre
 - Ne peut pas commencer ni finir par le caractère souligné (_)
 - Ne peut pas être un mot réservé DB2, comme « users » (utilisateurs), « admins », « guests » (invités), « public » ou « local », ni par un mot réservé SQL
 - Ne peut pas être le nom d'un utilisateur existant déjà dans le système

Il s'agit de l'ID du compte d'administrateur de base de données DB2 EKM 3.0. EKM 3.0 crée sur votre système un compte d'utilisateur local portant ce nom d'utilisateur.

8. Dans le champ **Database Password** (Mot de passe de base de données), attribuez un mot de passe au compte d'administrateur de base de données DB2 EKM. Dans le champ **Confirm Database Password** (Confirmer le mot de passe de base de données), entrez de nouveau le mot de passe.

 **REMARQUE:** Tous les mots de passe sont sensibles à la casse.

 **REMARQUE:** Dell vous recommande d'utiliser des mots de passe forts pour tous les comptes d'utilisateur EKM 3.0.

9. Dans le champ **Database Data Drive** (Lecteur de données de base de données), entrez l'emplacement du lecteur de base de données. Il s'agit de l'emplacement où seront stockées les données DB2 d'EKM 3.0. Sous Windows, indiquez une lettre de lecteur et le caractère deux-points (:). Sous Linux, indiquez un dossier, comme **/home/ekmdb2**.
10. Dans le champ **Database Name** (Nom de base de données), entrez le nom de la base de données DB2 EKM 3.0.
11. Le champ **Database Port** (Port de base de données) affiche par défaut **50010** sous Windows et **50000** sous Linux. Tous les ports utilisés par EKM 3.0 et configurés pendant l'installation d'EKM 3.0 sont prédéfinis sur les adresses de port recommandées. Dell vous recommande fortement d'utiliser ces adresses de port recommandées. Si vous prévoyez d'utiliser un serveur secondaire et que vous modifiez une adresse de port pendant l'installation d'EKM 3.0, cette adresse de port doit être identique pour les serveurs EKM 3.0 principal et secondaire.

 **REMARQUE:** Tous les ports utilisés pendant l'installation doivent être ouverts pour que vous puissiez installer EKM 3.0. Vérifiez qu'ils sont ouverts :

Pour vérifier que les ports sont ouverts sous Windows :

- a. Accédez à **<root>:\Windows\System32\drivers\etc**.
- b. Ouvrez le fichier texte **Services**.
- c. Passez le fichier en revue et assurez-vous que le numéro de port que vous souhaitez utiliser dans le champ **Database Port** (Port de base de données) est disponible. Si tel est le cas, il n'est pas répertorié.

Pour vérifier que les ports sont ouverts sous Linux :

- a. Ouvrez le fichier **/etc/services**.
- b. Passez le fichier en revue et assurez-vous que le numéro de port que vous souhaitez utiliser dans le champ **Database Port** (Port de base de données) est disponible. Si tel est le cas, il n'est pas répertorié.

12. Cliquez sur **Next** (Suivant).

L'écran **EKM Administrator** (Administrateur EKM) s'affiche. Cet écran vous permet de créer l'administrateur (superutilisateur) EKM 3.0. Ce compte sert à créer de nouveaux utilisateurs et de nouveaux groupes, et à leur affecter des permissions.

13. Dans le champ **Administrator Username** (Nom d'utilisateur de l'administrateur), entrez le nom d'utilisateur d'un administrateur EKM 3.0. (Il peut s'agir du nom de votre choix, à l'exception de **tkladmin**.)
14. Dans le champ **Password** (Mot de passe), attribuez un mot de passe au compte d'administrateur EKM 3.0. Dans le champ **Confirm Password** (Confirmer le mot de passe), entrez de nouveau le mot de passe.
15. Cliquez sur **Next** (Suivant).
L'écran **Encryption Manager** (Gestionnaire de cryptage) s'affiche. Vous utilisez cet écran pour créer le compte de gestionnaire de cryptage EKM 3.0 (TKLMAdmin). Il s'agit du compte d'utilisateur standard. Vous l'utilisez pour la gestion quotidienne des clés. Le champ **TKLMAdmin Username** (Nom d'utilisateur TKLMAdmin) est prérempli avec le nom **tkladmin**. Il s'agit du nom de gestionnaire de cryptage EKM requis.
16. Dans le champ **TKLMAdmin Password** (Mot de passe TKLMAdmin), attribuez un mot de passe au compte de gestionnaire de cryptage EKM 3.0. Dans le champ **TKLMAdmin Confirm Password** (Confirmer le mot de passe TKLMAdmin), entrez de nouveau le mot de passe.
17. Le champ **EKM Port** (Port EKM) affiche par défaut la valeur **16310** sous Windows et Linux. Il s'agit du port recommandé. Cliquez sur **Next** (Suivant).

 **REMARQUE:** Si le port fourni est utilisé par un autre service, le programme d'installation d'EKM 3.0 vous invite à sélectionner un autre port. Utilisez la commande **netstat** pour déterminer les ports utilisés, puis sélectionnez un port disponible. Enregistrez le numéro de port. Vous utiliserez ce port pour accéder au portail EKM 3.0.

L'écran **Migration** apparaît. Vous utilisez cet écran pour migrer d'EKM 2.X à EKM 3.0.

Si vous disposez d'une version d'EKM 2.X que vous souhaitez migrer vers EKM 3.0, vous devez effectuer la migration immédiatement. Reportez-vous à « [Migration d'une installation Encryption Key Manager \(EKM\) 2.X lors de l'installation d'EKM 3.0](#) ».

 **REMARQUE:** Vous ne pouvez migrer qu'une installation EKM 2.X ayant servi à créer des clés.

Si vous n'avez aucune installation EKM 2.X à migrer vers EKM 3.0.

- a) Laissez la case à cocher **Migrer d'EKM 2.X vers EKM 3.0** non sélectionnée et cliquez sur **Next** (Suivant). Une fenêtre pop-up de vérification s'affiche.
- b) Si vous avez choisi de ne pas migrer d'installation EKM 2.X, cliquez sur **Yes** (Oui) dans la fenêtre pop-up pour confirmer que vous ne migrez pas de version EKM 2.X.
L'écran **Configuration Summary** (Récapitulatif de la configuration) s'affiche.

18. Dans l'écran **Configuration Summary** (Récapitulatif de la configuration), cochez la case **Save profile** (Enregistrer le profil).

Le champ **File Directory** (Répertoire des fichiers) devient actif.

 **REMARQUE:** Dell vous recommande d'enregistrer le profil d'installation, au cas où vous deviez réinstaller EKM 3.0 dans le cadre d'une récupération après sinistre. Vous devez disposer d'un profil d'installation enregistré pour créer un serveur secondaire EKM 3.0.

 **REMARQUE:** Dell vous recommande d'utiliser pour cela un lecteur amovible. Dans ce cas, vous devez insérer ce lecteur dans votre système avant de cliquer sur **Next** (Suivant). Vous devez laisser le lecteur amovible en place jusqu'à la fin de l'installation. Si vous le souhaitez, vous pouvez enregistrer le fichier dans un dossier du lecteur local et copier ultérieurement ce fichier sur le lecteur amovible.

 **REMARQUE:** Le chemin entré dans ce champ doit inclure un nom de fichier. Le nom du dossier ne suffit pas. De plus, le chemin indiqué doit exister jusqu'au nom du dossier, mais le fichier portant le nom indiqué ne doit pas exister.

19. Dans le champ **File Directory** (Répertoire des fichiers), indiquez l'emplacement et le nom de fichier du profil d'installation que vous créez, ou cliquez sur **Choose** (Choisir) pour sélectionner un emplacement, puis entrez un nom de fichier.

Il s'agit de l'emplacement où vous souhaitez enregistrer le profil d'installation et du nom à attribuer au fichier enregistré.

EKM 3.0 enregistre le profil d'installation à la fin de l'installation d'EKM 3.0. Si vous utilisez une configuration avec serveurs principal et secondaire, vous devez utiliser le profil d'installation du serveur EKM 3.0 principal pendant l'installation du serveur secondaire afin de remplir automatiquement les champs de saisie de l'installation.

(Facultatif) Si vous effectuez une réinstallation sur le même serveur et que vous souhaitez utiliser les mêmes champs, vous pouvez utiliser ce profil d'installation pour remplir automatiquement les champs de saisie de l'installation.

-  **REMARQUE:** Dell vous recommande de capturer ou d'imprimer le **Configuration Summary** (Récapitulatif de la configuration) pour référence.
20. Dans l'écran **Configuration Summary** (Récapitulatif de la configuration), cliquez sur **Next** (Suivant).
L'écran **Installation Summary** (Récapitulatif de l'installation) apparaît.
 21. Passez en revue les informations de l'écran **Installation Summary** (Récapitulatif de l'installation).
 22. Cliquez sur **Install** (Installer).
-  **REMARQUE:** L'installation du logiciel prend environ 45 minutes. N'éteignez pas le système tant que l'installation n'est pas terminée.
 -  **REMARQUE:** Si vous prévoyez de configurer un serveur EKM 3.0 secondaire, ne commencez pas l'installation du serveur secondaire tant que l'installation du serveur EKM 3.0 principal n'est pas terminée.
23. Une fois l'installation terminée, cliquez sur **Done** (Terminer).
-  **REMARQUE:** Si vous avez migré une installation EKM 2.X vers la nouvelle installation EKM 3.0, Dell vous recommande fortement de créer une sauvegarde d'EKM 3.0 pour éviter que les nouvelles clés soient perdues. Reportez-vous à « [Création d'une sauvegarde du magasin de clés](#) ».
 -  **REMARQUE:** Si vous réinstallez EKM 3.0 et que l'installation échoue en raison d'une désinstallation incomplète, effectuez la désinstallation manuellement. Reportez-vous à « [Désinstallation manuelle d'EKM 3.0 sous Windows](#) ».

Configuration des serveurs EKM 3.0 principal et secondaire

Ce chapitre explique comment installer, utiliser et désinstaller EKM 3.0 sur les serveurs principal et secondaire.

 **PRÉCAUTION:** Pour éviter les pertes de données en cas de défaillance d'un serveur EKM 3.0, Dell vous recommande d'utiliser une configuration de serveurs EKM 3.0 comprenant un serveur principal et un serveur secondaire. Cette configuration offre une redondance, en cas de panne ou d'indisponibilité du serveur principal EKM 3.0.

 **REMARQUE:** Attention, il n'est pas possible d'utiliser un serveur principal EKM 3.0 avec un serveur secondaire EKM 2.X ou inversement.

Installation d'EKM 3.0 sur le serveur principal

Pendant l'installation d'EKM 3.0 sur le serveur principal, vous devez sélectionner l'option d'enregistrement du profil d'installation. Une fois l'installation d'EKM 3.0 terminée sur le serveur principal, copiez le profil d'installation enregistré sur un lecteur amovible ou dans un partage réseau. Reportez-vous à [Installing EKM 3.0](#) (Installation d'EKM 3.0).

Utilisation d'EKM 3.0 sur le serveur principal

Le serveur EKM 3.0 principal est l'emplacement où vous effectuez toutes les tâches de gestion des clés de cryptage. Par défaut, le serveur EKM 3.0 principal est configuré sur l'option **Automatically accept all new device requests for communication** (Accepter automatiquement toutes les demandes de communication des nouveaux périphériques). Reportez-vous à « [Configuration d'EKM 3.0 pour accepter les périphériques qui contactent EKM 3.0 pour obtenir des clés](#) » afin d'en savoir plus sur l'affichage ou la configuration de ce paramètre. Dell vous recommande d'effectuer des sauvegardes régulières du serveur EKM 3.0 principal. Reportez-vous à « [Exécution de sauvegardes et restauration à partir d'une sauvegarde](#) ».

Si vous devez remplacer le serveur EKM 3.0 principal, quelle qu'en soit la raison, installez EKM 3.0 sur un autre serveur physique à l'aide du profil d'installation qui a servi à installer le serveur EKM 3.0 principal d'origine. Restaurez les données de ce nouveau serveur principal à l'aide de la sauvegarde la plus récente, puis mettez à jour tous les périphériques pour qu'ils communiquent avec le nouveau serveur EKM 3.0 pour leurs demandes de clés. Reportez-vous au manuel d'utilisation de votre bandothèque pour en savoir plus sur la modification de l'adresse IP du serveur EKM 3.0 utilisé pour les demandes de clés. Pour trouver le manuel d'utilisation de la bandothèque, consultez la section « Documentation et informations de référence » du fichier **ReadThisFirst.txt** sur le support d'installation d'EKM 3.0.

Installation d'EKM 3.0 sur le serveur secondaire

 **REMARQUE:** Ne commencez pas l'installation du serveur EKM 3.0 secondaire tant que l'installation du serveur EKM 3.0 principal n'est pas terminée.

Le système sur lequel vous installez EKM 3.0 en tant que serveur secondaire doit posséder la même version de système d'exploitation que celle installée sur le serveur principal. EKM 3.0 ne prend pas en charge les paires serveur principal/serveur secondaire avec des systèmes d'exploitation mixtes.

Installez EKM 3.0 sur le serveur secondaire en suivant la procédure [Installing EKM 3.0](#) (Installation d'EKM 3.0). Utilisez le profil d'installation enregistré lors de l'installation d'EKM 3.0 sur le serveur principal. Vous devez entrer manuellement les mêmes mots de passe que ceux utilisés pour installer EKM 3.0 sur le serveur principal.

Utilisation d'EKM 3.0 sur le serveur secondaire

Le serveur EKM 3.0 secondaire est utilisé pour la redondance, lorsque le serveur EKM 3.0 principal est en panne ou non disponible.

Utilisez la sauvegarde créée sur le serveur EKM 3.0 principal pour effectuer à intervalle régulier une opération de restauration sur le serveur EKM 3.0 secondaire, afin de maintenir la synchronisation entre les serveurs EKM 3.0 principal et secondaire. Reportez-vous à « [Exécution de sauvegardes et restauration à partir d'une sauvegarde](#) ».

Par défaut, le serveur EKM 3.0 secondaire est également configuré sur l'option **Automatically accept all new device requests for communication** (Accepter automatiquement toutes les demandes de communication des nouveaux périphériques). Dell vous recommande de configurer ce paramètre sur **Only accept manually added devices for communication** (Accepter uniquement les périphériques ajoutés manuellement pour la communication) après chaque opération de restauration. Cela empêche le serveur EKM 3.0 secondaire de fournir des clés aux nouveaux périphériques que vous n'avez pas ajoutés au serveur EKM 3.0 principal. Reportez-vous à « [Configuration d'EKM 3.0 pour accepter les périphériques qui contactent EKM 3.0 pour obtenir des clés](#) » afin d'en savoir plus sur l'affichage ou la configuration de ce paramètre.

Si le serveur EKM 3.0 principal est temporairement en panne ou indisponible, vous devez effectuer une opération de restauration sur le serveur EKM 3.0 secondaire à l'aide de la toute dernière sauvegarde créée sur le serveur EKM 3.0 principal.

 **REMARQUE:** Si le serveur EKM 3.0 principal est en panne ou indisponible, et que vous utilisez le serveur EKM 3.0 secondaire pour prendre en charge les demandes de clés des périphériques, Dell vous recommande de n'effectuer aucune tâche opérationnelle ou de gestion sur le serveur EKM 3.0 secondaire.

Désinstallation d'EKM 3.0 sur les serveurs principal et secondaire

Pour savoir comment désinstaller EKM 3.0 des serveurs principal et secondaire, reportez-vous à « [Désinstallation d'EKM 3.0](#) ».

Exécution de sauvegardes et restauration à partir d'une sauvegarde

Vous pouvez exécuter une sauvegarde à tout moment. Cette opération crée un fichier de sauvegarde contenant le magasin de clés (ensemble de périphériques et de clés).

Les sauvegardes ne stockent pas les groupes de périphériques, les utilisateurs ni les groupes d'utilisateurs. Ces éléments sont stockés dans la base de données DB2.

Vous pouvez à tout moment restaurer les données depuis une sauvegarde.

 **REMARQUE:** Si certaines clés ne sont pas sauvegardées, le serveur ne les fournit pas. Dans ce cas, les tâches de sauvegarde cryptée échouent.

Création d'une sauvegarde du magasin de clés

Ce chapitre explique comment sauvegarder le magasin de clés.

1. Connectez-vous au portail EKM 3.0. Reportez-vous à « [Connexion au portail Encryption Key Manager 3.0](#) ». L'écran **Welcome to Dell Encryption Key Manager** (Bienvenue dans Dell Encryption Key Manager) s'affiche.
2. Dans le volet de navigation, accédez à **Dell Encryption Key Manager** → **Backup and Restore** (Sauvegarde et restauration). L'écran **Backup and Restore** (Sauvegarde et restauration) s'affiche.
3. Cliquez sur **Browse** (Parcourir), en regard du champ **Backup repository location** (Emplacement du référentiel de sauvegarde) et accédez au dossier où le fichier de sauvegarde doit être stocké (par exemple, **C:\EKM_Backup** sous Windows ou **/root/EKM_Backup** sous Linux).

 **REMARQUE:** Ce dossier doit exister avant le démarrage de la sauvegarde, sinon cette dernière échoue. Pour utiliser un autre dossier, créez-le avant de tenter de créer la sauvegarde.

4. Cliquez sur **Select** (Sélectionner) dans la fenêtre pop-up **Browse Directory** (Rechercher le dossier) afin de revenir à la fenêtre **Backup and Restore** (Sauvegarde et Restauration).
5. Cliquez sur **Create Backup** (Créer une sauvegarde). L'écran **Create Backup** (Créer une sauvegarde) apparaît.
6. Dans le champ **Create password** (Créer un mot de passe), créez un mot de passe pour la sauvegarde. Il doit comporter au moins six caractères.

 **REMARQUE:** Dell vous recommande d'utiliser des mots de passe forts pour toutes les activités liées à EKM 3.0.

7. Dans le champ **Retype Password** (Resaisissez le mot de passe), entrez de nouveau le mot de passe.
8. (Facultatif) Dans le champ **Backup description** (Description de la sauvegarde), entrez la description du fichier de sauvegarde. Si vous ne le faites pas, une description par défaut est ajoutée au fichier de sauvegarde.

 **REMARQUE:** Dans certaines versions de navigateur, le champ de description par défaut est en lecture seule. Pour en savoir plus, reportez-vous à « [Problèmes connus et solutions](#) ».

9. Cliquez sur **Create Backup** (Créer une sauvegarde). Une fenêtre pop-up de confirmation s'affiche.
10. Dans la fenêtre pop-up de confirmation, cliquez sur **OK**. Le processus de sauvegarde est exécuté.

 **REMARQUE:** N'utilisez pas le système pendant la sauvegarde. Si le contenu d'EKM 3.0 est grisé sur une longue période, cliquez sur le bouton d'actualisation du navigateur Web.

11. Une fois le fichier de sauvegarde créé, la fenêtre pop-up **Informations** s'affiche et confirme la réussite de la création du fichier. Dans cette fenêtre, cliquez sur **OK**. Le fichier de sauvegarde créé s'affiche dans la table de l'écran **Backup and Restore** (Sauvegarde et restauration).

12. Cliquez sur **Return home** (Retour à l'accueil), au bas de l'écran.

L'écran **Welcome to Dell Encryption Key Manager** (Bienvenue dans Dell Encryption Key Manager) s'affiche.

Restauration à partir d'une sauvegarde

Vous pouvez effectuer une restauration depuis une sauvegarde. Vous pouvez utiliser une sauvegarde pour créer des serveurs de clés secondaires, ainsi que pour recréer le serveur EKM 3.0 dans le cadre d'une récupération après sinistre.

 **PRÉCAUTION:** Vous ne devez effectuer la restauration que depuis une sauvegarde créée sur le même système ou sur un autre serveur EKM 3.0 installé avec le même profil d'installation. Vous ne pouvez pas effectuer la restauration depuis une sauvegarde créée sur un autre système avec des détails d'installation différents.

1. Connectez-vous au portail EKM 3.0. Reportez-vous à « [Connexion au portail Encryption Key Manager 3.0](#) ».
L'écran **Welcome to Dell Encryption Key Manager** (Bienvenue dans Dell Encryption Key Manager) s'affiche.

2. Dans le volet de navigation, accédez à **Dell Encryption Key Manager** → **Backup and Restore** (Sauvegarde et restauration).

L'écran **Backup and Restore** (Sauvegarde et restauration) s'affiche.

3. Sélectionnez la sauvegarde à restaurer.

4. Cliquez sur **Restore From Backup** (Restaurer depuis la sauvegarde), en haut de la table.

La sous-fenêtre **Restore From Backup** (Restaurer depuis la sauvegarde) apparaît.

5. Entrez le mot de passe du fichier de sauvegarde.

6. Cliquez sur **Restore Backup** (Restaurer la sauvegarde).

Une fenêtre pop-up de confirmation s'affiche.

 **PRÉCAUTION:** Toutes les clés créées après la création de la sauvegarde sont perdues, ainsi que l'accès aux données cryptées à l'aide de ces clés. Il est totalement impossible de récupérer les clés perdues ou supprimées.

7. Dans la fenêtre pop-up de confirmation, cliquez sur **OK**.

8. Après restauration de la sauvegarde, vous devez manuellement arrêter le serveur EKM 3.0 et le redémarrer. Reportez-vous à « [Démarrage et arrêt du serveur EKM 3.0 sous Windows](#) » ou « [Démarrage et arrêt du serveur EKM 3.0 sous Linux](#) ».

Utilisation d'EKM 3.0

Ce chapitre décrit les opérations de base réalisées dans EKM 3.0.

 **REMARQUE:** EKM 3.0 est basé sur IBM Tivoli Key Lifecycle Manager (TKLM) V2 FixPack 2, mais il a été personnalisé pour prendre en charge les environnements de bibliothèque de bandes Dell : nous avons sélectionné les fonctions de TKLM propres aux bandes.

Pour consulter des informations d'utilisation d'EKM 3.0 absentes du présent guide, consultez la documentation de TKLM, notamment les documents suivants :

- IBM Tivoli Key Manager 2,0 *Quick Start Guide* (Guide de démarrage d'IBM Tivoli Key Manager 2.0)
- IBM Tivoli Key Manager 2,0 *Installation and Configuration Guide* (Guide d'installation et de configuration d'IBM Tivoli Key Manager 2.0)
- IBM Tivoli Key Manager 2,0 *Product Overview/Scenario Guide* (Guide de présentation des produits/scénarios d'IBM Tivoli Key Manager 2.0)

Pour savoir comment accéder à la documentation TKLM, consultez la section Documentation and Reference Materials (Documentation et informations de référence) du fichier **ReadThisFirst.txt** sur le support d'installation d'EKM 3.0.

Certains écrans et fonctions présentés dans la documentation d'IBM TKLM ne sont pas activés dans Dell EKM 3.0. Ce dernier contient uniquement le sous-ensemble de fonctions nécessaire pour prendre en charge les bibliothèques de bandes Dell PowerVault.

Connexion au portail Encryption Key Manager 3.0

Procédez comme suit pour vous connecter au portail Encryption Key Manager 3.0 :

1. Ouvrez un navigateur et entrez l'URL suivante pour ouvrir le portail EKM 3.0 :

http://<adresse_IP_serveur_EKM_3.0>:<numéro_port_EKM_3.0>

 **REMARQUE:** Le numéro de port indiqué est celui que vous avez fourni lors de l'installation d'EKM 3.0. La valeur par défaut est **16310**.

Si vous ne connaissez pas le numéro de port, reportez-vous aux éléments suivants :

Sous Windows Consultez la valeur de la propriété **WC_defaulthost** dans le fichier suivant : **<racine>\Dell\EKM\profiles\TIPProfile\properties\portdef.props**.

Sous Linux Consultez la valeur de la propriété **WC_defaulthost** dans le fichier suivant : **/opt/dell/ekm/profiles/TIPProfile/properties/portdef.props**.

 **REMARQUE:** Si un message d'erreur s'affiche et vous signale que la page est introuvable, c'est que le service EKM 3.0 n'est pas démarré. Reportez-vous à « [Démarrage et arrêt du serveur EKM 3.0 sous Windows](#) » ou « [Démarrage et arrêt du serveur EKM 3.0 sous Linux](#) ».

La fenêtre de connexion à EKM 3.0 s'affiche.

2. Connectez-vous à EKM 3.0 à l'aide de votre nom d'utilisateur EKM 3.0 Encryption Manager (**tkladmin**) et du mot de passe EKM 3.0 Encryption Manager défini lors de l'installation d'EKM 3.0.

L'écran **Welcome to Dell Encryption Key Manager** (Bienvenue dans Dell Encryption Key Manager) s'affiche.

Création du magasin de clés maître

Ce chapitre explique comment créer le magasin de clés maître (master keystore). Vous devez le créer lors de votre première connexion à EKM 3.0.

 **REMARQUE:** Si vous avez migré un magasin de clés EKM 2.X pendant l'installation d'EKM 3.0, un magasin de clés a déjà été créé et cette procédure ne s'applique pas.

 **REMARQUE:** Ultérieurement, si vous souhaitez créer des clés et/ou des groupes de clés supplémentaires, reportez-vous à [Creating Key Groups for the Device Group](#) (Création de groupes de clés pour des groupes de périphériques).

Pour créer le magasin de clés maître, procédez comme suit :

1. Dans l'écran **Welcome to Dell Encryption Key Manager** (Bienvenue dans Dell Encryption Key Manager), utilisez le lien **click here to create the master keystore** (cliquez ici pour créer le magasin de clés maître).
L'écran **Keystore** (Magasin de clés) apparaît.
2. Conservez les valeurs par défaut pour les options **Keystore type** (Type de magasin de clés), **Keystore path** (Chemin du magasin de clés) et **Keystore name** (Nom du magasin de clés).
Les valeurs par défaut sont les suivantes : **Keystore type** = JCEKS et **Keystore name** = defaultKeyStore. Le **Keystore path** par défaut sous Windows est : `<racine>:\Dell\EKM\products\tklm\keystore`. Sous Linux, la valeur par défaut pour **Keystore path** est : `/opt/dell/ekm/products/tklm/keystore`.
3. Dans le champ **Password** (Mot de passe), créez un mot de passe pour le magasin de clés par défaut. Il doit comporter au moins six caractères.
4. Dans le champ **Retype Password** (Resaisissez le mot de passe), entrez de nouveau le mot de passe.
5. Cliquez sur **OK**.
L'écran **Keystore** confirme que le magasin de clés a été créé avec succès.
6. Créez une sauvegarde du magasin de clés. Reportez-vous à [Performing Backups and Restoring from a Backup](#) (Exécution de sauvegardes et restauration à partir d'une sauvegarde).

Activation du pare-feu sur le serveur EKM 3.0

 **REMARQUE:** Reportez-vous à la documentation de votre système d'exploitation pour savoir comment configurer le pare-feu.

EKM 3.0 communique avec la bibliothèque de bandes sur le réseau. Si le pare-feu du système où EKM 3.0 est installé est activé mais que les ports requis ne sont pas ouverts, la communication entre EKM 3.0 et la bibliothèque de bandes échoue. Si vous devez activer le pare-feu sur le système où EKM 3.0 est installé, procédez comme suit pour permettre la communication entre EKM 3.0 et la bibliothèque de bandes :

 **REMARQUE:** Voici les ports par défaut utilisés par EKM 3.0. Si votre bibliothèque de bandes est configurée pour utiliser d'autres ports, vérifiez que ces numéros de port sont utilisés dans les paramètres de pare-feu et dans la configuration d'EKM 3.0.

 **REMARQUE:** Si vous utilisez une configuration avec serveurs principal et secondaire pour EKM 3.0, répétez cette procédure sur le serveur secondaire.

1. Ouvrez les ports suivants, en fonction du protocole voulu :
 - TCP : 3801

2. Si votre pare-feu est configuré pour autoriser uniquement des adresses IP et/ou masques de sous-réseau spécifiques à communiquer avec les ports ci-dessus, veillez à inclure l'adresse IP et/ou le masque de sous-réseau de la bibliothèque de bandes dans la liste des éléments autorisés.

Pour accéder à la configuration réseau de la bibliothèque de bandes, connectez-vous à l'unité de gestion à distance (RMU) de la bibliothèque et accédez aux paramètres réseau. Pour en savoir plus, consultez le guide d'utilisation de la bibliothèque de bandes. Pour le trouver, consultez la section « Documentation et informations de référence » du fichier **ReadThisFirst.txt** sur le support d'installation d'EKM 3.0.

3. Si vous souhaitez ultérieurement modifier les paramètres de port intervenant dans la communication entre EKM 3.0 et la bibliothèque de bandes, veillez à modifier ces ports dans les paramètres de la bibliothèque de bandes, dans EKM 3.0 et dans le pare-feu du système où EKM 3.0 est installé.

Configuration d'EKM 3.0 pour accepter les périphériques qui le contactent pour obtenir des clés

Ce chapitre explique comment configurer le comportement d'EKM 3.0 concernant la gestion des périphériques qui tentent de se connecter à EKM 3.0 pour demander des clés. Reportez-vous au guide d'utilisation de votre périphérique pour en savoir plus sur la connexion à EKM 3.0 en vue de demander des clés.

1. Connectez-vous au portail EKM 3.0. Reportez-vous à [Logging into the Encryption Key Manager 3.0 Portal](#) (Connexion au portail Encryption Key Manager 3.0).
L'écran **Welcome to Dell Encryption Key Manager** (Bienvenue dans Dell Encryption Key Manager) s'affiche.
2. Dans le volet de navigation, accédez à **Dell Encryption Key Manager** → **Key and Device Management** (Gestion des clés et des périphériques).
L'écran **Key and Device Management** s'ouvre.
3. Dans le menu déroulant **Manage keys and device** (Gérer les clés et les périphériques) sélectionnez **LTO**, puis cliquez sur **Go** (OK).

 **REMARQUE:** Reportez-vous à la documentation TKLM pour en savoir plus sur ces périphériques. Pour savoir comment accéder à cette documentation, consultez la section Documentation and Reference Materials (Documentation et informations de référence) du fichier **ReadThisFirst.txt** sur le support d'installation d'EKM 3.0.

4. Dans le menu déroulant au bas de la table, sélectionnez l'une des options suivantes :

Automatically accept all new device requests for communication (Accepter automatiquement toutes les demandes de communication des nouveaux périphériques)

Les clés sont automatiquement transmises aux nouveaux périphériques. Il s'agit du paramètre par défaut pour EKM 3.0. Dell vous recommande de conserver ce paramètre pour le serveur EKM 3.0 principal, mais pas pour le serveur secondaire si vous en avez configuré un.

Only accept manually added devices for communication (Accepter uniquement les périphériques ajoutés manuellement pour la communication)

Les clés ne sont transmises aux périphériques que si ces derniers sont ajoutés manuellement. Si vous configurez le serveur EKM 3.0 secondaire, Dell vous recommande d'utiliser ce paramètre afin que le serveur secondaire ne transmette pas automatiquement les clés aux nouveaux périphériques.

Hold new device requests pending my approval (Stocker les nouvelles demandes des périphériques en attente de mon approbation)

Les périphériques qui contactent EKM 3.0 sont ajoutés à une file d'attente.

Création d'un groupe de périphériques

Cette procédure permet de créer un groupe de périphériques. Si vous utilisez un groupe de périphériques par défaut, sautez cette section.

Les groupes de périphériques servent à gérer les clés destinées à un ou plusieurs périphériques. Dell vous recommande d'utiliser des groupes de périphériques pour gérer un sous-ensemble de vos périphériques en fonction des besoins de votre organisation.

Pour créer un nouveau groupe de périphériques, procédez comme suit :

1. Connectez-vous au portail EKM 3.0. Reportez-vous à [Logging into the Encryption Key Manager 3.0 Portal](#) (Connexion au portail Encryption Key Manager 3.0).
L'écran **Welcome to Dell Encryption Key Manager** (Bienvenue dans Dell Encryption Key Manager) s'affiche.
2. Dans le volet de navigation, accédez à **Dell Encryption Key Manager** → **Advanced Configuration** → **Device Group** (Dell Encryption Key Manager > Configuration avancée > Groupe de périphériques).
L'écran **Manage Device Groups** (Gérer les groupes de périphériques) apparaît.
3. Cliquez sur **Create** (Créer) en haut de la table.
La sous-fenêtre **Create Device Group** (Créer un groupe de périphériques) s'affiche.
4. Sous **Device family** (Gamme de périphériques), sélectionnez le bouton radio **LTO**.
5. Dans le champ **Device group name** (Nom du groupe de périphériques), entrez le nom approprié. Dell vous recommande de saisir un nom reflétant l'utilisation de ce groupe de périphériques, par exemple **Accounting** (Comptabilité).
6. Cliquez sur **Create** (Créer).
La fenêtre pop-up **Information** vous présente les paramètres de gamme de périphériques.
7. Dans la fenêtre pop-up **Information**, cliquez sur **OK**.
Le groupe de périphériques est créé. Ce nouveau groupe apparaît dans l'écran **Manage Device Groups** (Gérer les groupes de périphériques).

Création de groupes de clés pour des groupes de périphériques

Les groupes de clés regroupent des clés propres à un périphérique donné. Ce chapitre explique comment créer et configurer des groupes de clés pour un périphérique particulier. Les groupes de clés configurés pour un périphérique ne peuvent pas être utilisés avec un autre.

Pour créer des groupes de clés pour un groupe de périphériques, procédez comme suit :

1. Connectez-vous au portail EKM 3.0. Reportez-vous à [Logging into the Encryption Key Manager 3.0 Portal](#) (Connexion au portail Encryption Key Manager 3.0).
L'écran **Welcome to Dell Encryption Key Manager** (Bienvenue dans Dell Encryption Key Manager) s'affiche.
2. Dans le volet de navigation, accédez à **Dell Encryption Key Manager** → **Key and Device Management** (Gestion des clés et des périphériques).
L'écran **Key and Device Management** (Gestion des clés et des périphériques) s'ouvre.
3. Dans le menu déroulant **Key and Device Management** (Gérer les clés et les périphériques), sélectionnez le nom du groupe de périphériques auquel ajouter le groupe de clés.
4. En regard de **Key and Device Management** (Gestion des clés et des périphériques), cliquez sur **OK**.
Dans l'utilitaire **Key and Device Management**, vous voyez s'afficher la page correspondant au groupe de périphériques sélectionné. Cette page répertorie tous les groupes de clés et tous les périphériques appartenant à ce groupe de périphériques.

5. Dans la table, cliquez sur **Add** (Ajouter), puis sur **Key Group** (Groupe de clés).
La sous-fenêtre **Create Key Group** (Créer un groupe de clés) s'affiche.
 6. Dans le champ **Key group name** (Nom du groupe de clés), entrez le nom approprié.
 7. Dans le champ **Number of keys to create** (Nombre de clés à créer), entrez le nombre de votre choix.
 8. Dans le champ **First three letters of key name** (Trois premières lettres du nom de la clé), entrez les caractères qui doivent constituer le préfixe de la clé.
 9. Pour que ce groupe de clés devienne le groupe de clés par défaut, cochez la case **Make this the default key group** (Désigner comme groupe de clés par défaut).
 10. Cliquez sur **Create Key Group** (Créer un groupe de clés).
Une fenêtre pop-up **Warning** (Avertissement) s'affiche.
 11. Pour créer une sauvegarde, cliquez sur le lien bleu dans la fenêtre pop-up **Warning** afin d'accéder à l'écran **Backup and Restore** (Sauvegarde et Restauration). Reportez-vous à [Performing Backups and Restoring from a Backup](#) (Exécution de sauvegardes et restauration à partir d'une sauvegarde). Après avoir créé la sauvegarde, revenez à l'écran **Key and Device Management** (Gestion des clés et des périphériques). Si vous ne souhaitez pas créer de sauvegarde à ce stade, passez à l'étape suivante.
-  **REMARQUE:** Dell vous recommande de créer une sauvegarde chaque fois que vous modifiez des clés, des groupes de clés ou des groupes de périphériques.
12. Cliquez sur **OK** dans la fenêtre pop-up **Warning**.
Le groupe de clés est créé. L'écran **Key and Device Management** (Gestion des clés et des périphériques) affiche les groupes de clés.
 13. Cette étape est facultative. Vérifiez que les clés ont été créées en procédant comme suit dans l'écran **Key and Device Management** :
 - a) Dans le menu déroulant en haut de la table, sélectionnez **View Keys, Key Group Membership and Drives** (Afficher les clés, l'appartenance aux groupes de clés et les lecteurs).
Les clés s'affichent dans la table.
 - b) Faites défiler l'affichage pour trouver les nouvelles clés.

Ajout d'un périphérique à un groupe de périphériques

Ce chapitre explique comment ajouter un périphérique à un groupe de périphériques existant.

-  **REMARQUE:** Les groupes de périphériques par défaut d'EKM 3.0 sont **FUTURE_DEVICES** et **LTO**.
-  **REMARQUE:** Pour ajouter automatiquement un périphérique à un groupe de périphériques, vous devez créer un groupe de clés et une sauvegarde. Sinon, les diagnostics de chemin de clés de la bibliothèque de bandes échouent et le périphérique n'est pas ajouté. Reportez-vous à [Creating Key Groups for a Device Group](#) (Création de groupes de clés pour des groupes de périphériques) et à [Creating a Backup of the Keystore](#) (Création d'une sauvegarde du magasin de clés) pour en savoir plus.
1. Connectez-vous au portail EKM 3.0. Reportez-vous à [Logging into the Encryption Key Manager 3.0](#) (Portail Connexion au portail Encryption Key Manager 3.0).
L'écran **Welcome to Dell Encryption Key Manager** (Bienvenue dans Dell Encryption Key Manager) s'affiche.
 2. Sélectionnez le groupe de périphériques à utiliser sous **Key and Device Management** (Gestion des clés et des périphériques), dans le menu déroulant **Manage keys and devices** (Gérer les clés et les périphériques).
 3. Cliquez sur **Go** (OK).
Dans l'utilitaire **Key and Device Management**, vous voyez s'afficher la page correspondant au groupe de périphériques sélectionné. Cette page répertorie tous les groupes de clés et tous les périphériques appartenant à ce groupe de périphériques.

4. Dans le menu déroulant au bas de la page, sélectionnez **Automatically accept all new device requests for communication** (Accepter automatiquement toutes les demandes de communication des nouveaux périphériques).
5. Configurez la bibliothèque de bandes pour qu'elle se connecte au serveur EKM 3.0.
Pour en savoir plus, consultez le guide d'utilisation de la bibliothèque de bandes. Pour savoir comment accéder à ce guide, consultez la section Documentation and Reference Materials (Documentation et informations de référence) du fichier **ReadThisFirst.txt** sur le support d'installation d'EKM 3.0.
6. Exécutez les diagnostics de chemin de clés dans l'unité de gestion à distance (RMU) de la bibliothèque de bandes.
Pour en savoir plus, consultez le guide d'utilisation de la bibliothèque de bandes.
Le nouveau périphérique apparaît dans l'écran **Key and Device Management** (Gestion des clés et des périphériques).

 **REMARQUE:** Pour ajouter manuellement un périphérique, reportez-vous à la documentation TKLM. Pour savoir comment accéder à cette documentation, consultez la section Documentation and Reference Materials (Documentation et informations de référence) du fichier **ReadThisFirst.txt** sur le support d'installation d'EKM 3.0.

Ajout et suppression de clés dans des groupes de clés

Ce chapitre explique comment ajouter et supprimer des clés dans des groupes de clés.

 **REMARQUE:** La suppression d'une clé d'un groupe de clés ne détruit pas cette clé ; elle est simplement retirée du groupe de clés. Pour supprimer une seule clé, reportez-vous à [Deleting a Specific Key](#) (Suppression d'une clé spécifique).

 **REMARQUE:** Pour savoir comment accéder à l'écran **Key and Device Management** (Gestion des clés et des périphériques), reportez-vous à [Creating Key Groups for the Device Group](#) (Création de groupes de clés pour des groupes de périphériques).

1. Connectez-vous au portail EKM 3.0. Reportez-vous à [Logging into the Encryption Key Manager 3.0 Portal](#) (Connexion au portail Encryption Key Manager 3.0).
L'écran **Welcome to Dell Encryption Key Manager** (Bienvenue dans Dell Encryption Key Manager) s'affiche.
2. Dans le volet de navigation, accédez à **Dell Encryption Key Manager** → **Key and Device Management**.
L'écran **Key and Device Management** s'ouvre.
3. Dans le menu déroulant **Manage keys and devices** (Gérer les clés et les périphériques), sélectionnez le nom du groupe de périphériques auquel ajouter le groupe de clés.
4. En regard de **Key and Device Management**, cliquez sur **Go**.
Dans l'utilitaire **Key and Device Management**, vous voyez s'afficher la page correspondant au groupe de périphériques sélectionné. Cette page répertorie tous les groupes de clés et tous les périphériques appartenant à ce groupe de périphériques.
5. Sélectionnez le groupe de clés à modifier.
6. Cliquez sur **Modify** (Modifier) en haut de la table.
La sous-fenêtre **Modify Key Group** (Modifier le groupe de clés) s'affiche.
7. Dans la sous-fenêtre **Modify Key Group**, sélectionnez le bouton radio approprié.
Si vous sélectionnez le bouton radio **Create additional keys in key group** (Créer des clés supplémentaires dans le groupe de clés), entrez le nombre de clés à ajouter au groupe de clés dans le champ **Number of keys to create** (Nombre de clés à créer). Dans le champ **First three letters of key name** (Trois premières lettres du nom de la clé), entrez trois lettres, qui serviront de préfixe aux nouvelles clés.
Si vous sélectionnez le champ **Delete key from key group** (Supprimer une clé du groupe de clés), entrez l'alias de clé dans le champ de texte.
8. Sélectionnez **Modify Key Group** (Modifier le groupe de clés).

Le groupe de clés est modifié pour refléter ces modifications.

Suppression de groupes de clés

Ce chapitre explique comment supprimer un groupe de clés.

 **PRÉCAUTION:** La suppression d'un groupe de clés supprime toutes les clés de ce groupe. La suppression d'une clé revient à supprimer toutes les données protégées par cette clé, puisqu'elles deviennent inaccessibles. Il est totalement impossible de récupérer les clés supprimées, par quelque moyen que ce soit, pour des raisons de sécurité.

 **REMARQUE:** Vous ne pouvez pas supprimer le groupe de clés par défaut d'un groupe de périphériques.

Pour supprimer un groupe de clés, procédez comme suit :

1. Connectez-vous au portail EKM 3.0. Reportez-vous à [Logging into the Encryption Key Manager 3.0 Portal](#) (Connexion au portail Encryption Key Manager 3.0).
L'écran **Welcome to Dell Encryption Key Manager** s'affiche.
2. Dans le volet de navigation, accédez à **Dell Encryption Key Manager** → **Key and Device Management** (Dell Encryption Manager > Gestion des clés et des périphériques).
L'écran **Key and Device Management** s'ouvre.
3. Dans le menu déroulant **Manage keys and devices** (Gérer les clés et les périphériques), sélectionnez le nom du groupe de périphériques auquel ajouter le groupe de clés.
4. En regard de **Key and Device Management**, cliquez sur **Go**.
Dans l'utilitaire **Key and Device Management**, vous voyez s'afficher la page correspondant au groupe de périphériques sélectionné. Cette page répertorie tous les groupes de clés et tous les périphériques appartenant à ce groupe de périphériques.
5. Vérifiez que le groupe de clés à supprimer n'est pas le groupe de clés par défaut. Si c'est le cas, modifiez le groupe de clés afin qu'il ne soit plus désigné comme groupe de clés par défaut :
 - a) Dans la table **Key Group** (Groupe de clés), effectuez un clic droit sur le groupe de clés à supprimer.
Un menu contextuel apparaît.
 - b) Dans le menu contextuel, sélectionnez **Modify** (Modifier).
La sous-fenêtre **Modify Key Group** (Modifier le groupe de clés) s'affiche.
 - c) Désélectionnez la case à cocher **Make this the default key group** (Désigner comme groupe de clés par défaut).
 - d) Cliquez sur **Modify Key Group**.
L'écran **Key and Device Management** s'ouvre.
6. Sélectionnez le groupe de clés à supprimer pour le mettre en surbrillance, puis cliquez sur **Delete** (Supprimer).
Une fenêtre contextuelle de confirmation s'affiche.
7. Cliquez sur **OK** dans la fenêtre contextuelle de confirmation.
Le groupe de clés et toutes les clés associées à ce groupe sont supprimés.

Vérification du certificat de serveur

Ce chapitre explique comment vérifier que le certificat de serveur que vous souhaitez employer est bien celui qui est en cours d'utilisation. Pour ce faire, procédez comme suit :

1. Connectez-vous au portail EKM 3.0. Reportez-vous à [Logging into the Encryption Key Manager 3.0 Portal](#) (Connexion au portail Encryption Key Manager 3.0).

L'écran **Welcome to Dell Encryption Key Manager** (Bienvenue dans Dell Encryption Key Manager) s'affiche.

2. Dans le volet de navigation, accédez à **Dell Encryption Key Manager** → **Advanced Configuration** → **Server Certificates** (Dell Encryption Key Manager Configuration avancée Certificats de serveur).
L'écran **Administer Server Certificates** (Administrer les certificats de serveur) s'affiche.
3. Vérifiez qu'il y a une coche dans la colonne **In Use** (En cours d'utilisation) pour le certificat à utiliser.
*Si la colonne **In Use** du certificat voulu comporte une coche, cette procédure est terminée.*
*Si la colonne **In Use** du certificat que vous souhaitez utiliser ne comporte aucune coche, procédez comme suit :*
 - a) Cliquez sur le certificat à utiliser pour le mettre en surbrillance.
 - b) Cliquez sur **Modify** (Modifier) en haut de la table.
La sous-fenêtre **Modify SSL/KMIP** (Modifier SSL/KMIP) s'affiche.
 - c) Cochez la case **Current certificate in use** (Certificat actuel utilisé).
 - d) Cliquez sur **Modify Certificate** (Modifier le certificat).
Une fenêtre pop-up **Warning** (Avertissement) s'affiche.
 - e) Cliquez sur **OK** dans la fenêtre pop-up **Warning**.
 - f) Arrêtez le serveur et redémarrez-le. Reportez-vous à [Starting and Stopping the EKM 3.0 Server in Windows](#) (Démarrage et arrêt du serveur EKM 3.0 sous Windows) ou à [Starting and Stopping the EKM 3.0 Server in Linux](#) (Démarrage et arrêt du serveur EKM 3.0 sous Linux).

 **REMARQUE:** Vous ne pouvez pas modifier les certificats, à part les marquer comme **In Use**.

Affichage des détails du certificat de serveur

Pour afficher les détails du certificat, procédez comme suit :

1. Cliquez sur le certificat pour le mettre en surbrillance.
2. Cliquez sur **Modify** (Modifier) en haut de la table.
La sous-fenêtre **Modify SSL/KMIP Certificate** s'affiche.
3. Affichez les détails du certificat. Vous pouvez également cliquer sur **Optional Certificate Parameters** (Paramètres facultatifs du certificat) pour afficher les paramètres en option.

Connexion au serveur WebSphere

Certaines procédures dans ce guide exigent que vous vous connectiez au serveur WebSphere. Ce chapitre explique comment vous connecter au serveur WebSphere sous Windows et Linux. Vous n'avez besoin de vous connecter directement au serveur WebSphere que si une autre procédure vous le demande.

Pour vous connecter au serveur WebSphere avec la commande **wsadmin** :

1. *Sous Windows*, ouvrez une invite de commandes et accédez à **<root>:\Dell\EKM\bin**. *Sous Linux*, ouvrez une session de terminal, accédez à **/opt/dell/ekm/bin**.
2. *Sous Windows*, entrez la commande suivante :

```
wsadmin -username tklmadmin -password <mot de passe tklm> -lang jython
```

Sous Linux, entrez la commande suivante :

```
./wsadmin.sh -username tklmadmin -password <mot de passe tklm> -lang jython
```

Appuyez sur **Entrée**. La commande s'exécute un bref instant et l'invite de commandes **wsadmin** s'affiche.

 **REMARQUE:** Les commandes sont sensibles à la casse. Il n'y a aucun espace autour des parenthèses ou des crochets. N'entrez pas les symboles supérieur ou inférieur (< >) autour des variables.

 **REMARQUE:** Pour vous déconnecter du serveur WebSphere, entrez **Exit** (Quit) et appuyez sur **Entrée**.

Démarrage et arrêt du serveur EKM 3.0 sous Windows

Ce chapitre explique comment démarrer et arrêter le serveur EKM 3.0 sous Windows.

1. Ouvrez une invite de commandes et accédez à *<racine>\Dell\EKM\bin*.

2. Pour démarrer le serveur, entrez la commande suivante :

```
startserver server1
```

Pour arrêter le serveur, entrez la commande suivante :

```
stopserver server1
```

3. Appuyez sur **Entrée**.

La commande s'exécute et l'invite de commandes affiche le message de confirmation :

```
Serveur server1 ouvert pour l'e-business
```

ou

```
Arrêt du serveur server1 terminé
```

Démarrage et arrêt du serveur EKM 3.0 sous Linux

Ce chapitre explique comment démarrer et arrêter le serveur EKM 3.0 sous Linux.

 **REMARQUE:** Vous devez vous connecter en tant qu'utilisateur root pour démarrer et arrêter le serveur.

1. Ouvrez une session de terminal et accédez à */opt/dell/ekm/bin*.

2. Pour démarrer le serveur, entrez la commande suivante :

```
./startserver.sh server1
```

Pour arrêter le serveur, entrez la commande suivante :

```
./stopserver.sh server1
```

 **REMARQUE:** Vous êtes invité à entrer le nom de connexion et le mot de passe de l'administrateur EKM 3.0 pour arrêter le serveur.

3. Appuyez sur **Entrée**.

La commande s'exécute et la session de terminal affiche le message de confirmation :

```
Serveur server1 ouvert pour l'e-business
```

ou

```
Arrêt du serveur server1 terminé
```


Migration et fusion

Pendant l'installation d'EKM 3.0, vous pouvez migrer EKM 2.X dans EKM 3.0.

Après l'installation d'EKM 3.0, vous pouvez fusionner EKM 2.X dans EKM 3.0.

Ce chapitre décrit les procédures de fusion et de migration.

 **REMARQUE:** Vous ne pouvez migrer ou fusionner qu'une installation EKM 2.X ayant servi à créer des clés.

Migration d'une installation Encryption Key Manager (EKM) 2.X lors de l'installation d'EKM 3.0

Exécutez cette procédure uniquement pour configurer l'écran **Migration** pendant l'installation d'EKM 3.0. L'écran **Migration** permet de migrer une installation Encryption Key Manager (EKM) 2.X dans EKM 3.0.

-  **REMARQUE:** Si vous utilisez actuellement EKM 2.X, Dell vous recommande de conserver votre infrastructure actuelle (serveurs, systèmes d'exploitation, bibliothèques, etc. protégés par EKM 2.X), sauf en cas de problème. Si vous devez migrer une installation EKM 2.X vers EKM 3.0, Dell vous recommande de le faire à ce stade.
-  **REMARQUE:** Si vous utilisez EKM 2.X avec une machine virtuelle comme hôte EKM 2.X, vous devez rester dans EKM 2.X ou migrer vers un serveur physique. EKM 3.0 ne prend pas en charge l'utilisation de machines virtuelles comme hôtes.
-  **REMARQUE:** Pendant l'installation d'EKM 3.0, vous ne pouvez migrer qu'une seule installation EKM 2.X. Si vous possédez plusieurs installations EKM 2.X à porter dans EKM 3.0, migrez la première en appliquant cette procédure, puis, une fois l'installation terminée, reportez-vous à « [Fusion d'installations EKM 2.X supplémentaires dans EKM 3.0](#) » pour fusionner les autres installations.
Il est possible de *fusionner* l'installation EKM 2.X dans EKM 3.0 une fois l'installation d'EKM 3.0 terminée, à l'aide de l'outil de fusion d'EKM 2.X dans EKM 3.0, mais Dell vous recommande fortement d'effectuer la migration à ce stade.
-  **REMARQUE:** Si vous utilisez une configuration EKM 3.0 avec serveurs principal et secondaire, vous devez effectuer la migration uniquement sur le serveur EKM 3.0 principal.
Une fois la migration terminée, sauvegardez le serveur EKM 3.0 principal et utilisez la sauvegarde pour restaurer le serveur EKM 3.0 secondaire pour qu'il soit identique au serveur principal.

Pour migrer le système depuis EKM 2.X pendant l'installation d'EKM 3.0, passez à l'étape « [Procédure de migration d'EKM 2.X vers EKM 3.0](#) ».

Procédure de migration d'EKM 2.X vers EKM 3.0

Pour migrer une installation EKM 2.X vers EKM 3.0 depuis l'écran **Migration** pendant l'installation d'EKM 3.0, procédez comme suit :

1. Connectez-vous à la console EKM 2.X, sauvegardez le magasin de clés EKM 2.X, arrêtez le serveur EKM 2.X et quittez la console EKM 2.X. Pour en savoir plus, reportez-vous au guide d'utilisation d'EKM 2.X.
 2. Copiez le dossier EKM 2.X :
*Si votre serveur EKM 2.X est installé sur une machine différente de celle de l'installation EKM 3.0 cible, copiez le dossier EKM 2.X du serveur EKM 2.X vers un dossier temporaire sur le serveur EKM 3.0 (par exemple, **C:\temp\MyEKM2** sous Windows ou **/opt/myekm2** sous Linux).*
Si votre serveur EKM 2.X est installé sur la même machine que l'installation EKM 3.0 cible, vous devez quand même copier le dossier EKM 2.X sur cette machine.
 3. Dans l'écran **Migration** du programme d'installation d'EKM 3.0, cochez la case **Migrer d'EKM 2.X vers EKM 3.0**.
 4. Cliquez sur **Choose** (Choisir) et activez au répertoire où vous avez [précédemment](#) copié le dossier EKM 2.X. Ne sélectionnez aucun élément sous ce dossier.
-  **PRÉCAUTION:** Si votre serveur EKM 2.X est installé sur la même machine que l'installation EKM 3.0 cible, n'accédez pas au dossier où EKM 2.X est installé, car le programme d'installation d'EKM 3.0 supprime le dossier utilisé pour la migration. Accédez à la copie du répertoire EKM 2.X créé [précédemment](#).
5. Cliquez sur **Next** (Suivant).

L'écran **Configuration Summary** (Récapitulatif de la configuration) s'affiche.



REMARQUE: Si un message d'erreur apparaît, vérifiez le chemin du répertoire EKM 2.X.

6. Continuez l'installation d'EKM 3.0. Reportez-vous à [Performing the EKM 3.0 Installation Procedure](#) (Exécution de la procédure d'installation d'EKM 3.0).



REMARQUE: Le mot de passe du nouveau magasin de clés EKM 3.0 est identique à celui associé au magasin de clés EKM 2.X utilisé pour la migration.



PRÉCAUTION: N'exécutez pas EKM 2.X après avoir migré ses clés dans EKM 3.0. Si vous le souhaitez, vous pouvez désinstaller EKM 2.X après migration d'EKM 2.X vers EKM 3.0. Dell vous recommande de sauvegarder les fichiers EKM 2.X avant de désinstaller EKM 2.X.

Fusion d'Encryption Key Manager (EKM) 2.X dans EKM 3.0 après l'installation d'EKM 3.0

Ce chapitre décrit la procédure de fusion d'EKM 2.X dans EKM 3.0 après l'installation sous Windows et Linux. Cette procédure utilise l'outil de fusion d'EKM 2.X dans EKM 3.0.

Utilisez cette procédure si EKM 3.0 est déjà installé et configuré, et que vous souhaitez fusionner EKM 2.X dans EKM 3.0.

 **REMARQUE:** Si vous utilisez une configuration EKM 3.0 avec serveurs principal et secondaire, vous devez exécuter la procédure de fusion uniquement sur le serveur EKM 3.0 principal. Une fois la fusion terminée sur le serveur principal, suivez la procédure de sauvegarde, puis restaurez le fichier de sauvegarde sur le serveur EKM 3.0 secondaire. Reportez-vous à « [Exécution de sauvegardes et restauration à partir d'une sauvegarde](#) ».

 **REMARQUE:** Si EKM 3.0 n'est pas encore installé, Dell vous recommande de migrer EKM 2.X vers EKM 3.0 pendant l'installation d'EKM 3.0. Reportez-vous à « [Exécution de la procédure d'installation d'EKM 3.0](#) ».

Les exemples du présent document utilisent des chemins Windows standard (par exemple, **C:\<nom_dossier>**). Remplissez les chemins indiqués par la lettre de lecteur racine ou le chemin Linux correspondant à votre système.

Prérequis de l'outil de fusion

Avant d'exécuter l'outil de fusion, vérifiez que la configuration requise suivante est respectée :

- EKM 3.0 doit être installé et vous devez créer le magasin de clés maître ; sinon, la procédure échoue. Reportez-vous à [Creating a Master Keystore](#) (Création du magasin de clés maître).
- Lorsque vous fusionnez EKM 2.X dans EKM 3.0, EKM 2.X et EKM 3.0 doivent être installés sous la même version du système d'exploitation.
- Si vous avez précédemment fusionné ou migré EKM 2.X dans EKM 3.0, le certificat **ekmcert** issu de la fusion/migration précédente existe toujours sur le serveur EKM 3.0, parfois même si vous avez effectué une restauration depuis une sauvegarde précédente. Vous devez supprimer le certificat **ekmcert** du serveur EKM 3.0 avant de lancer la procédure de fusion. Reportez-vous à [Deleting the ekmcert Certificate, Keys, and Key Groups, and Renaming Devices](#) (Suppression du certificat ekmcert, des clés et des groupes de clés, et changement du nom des périphériques).
- Vous devez renommer les clés, groupes de clés et périphériques en double dans EKM 2.X avant la fusion dans EKM 3.0. Reportez-vous au guide d'utilisation d'EKM 2.X.
 - Il ne doit pas exister d'alias/noms de clés en double entre l'installation EKM 2.X source et l'installation EKM 3.0 cible. Chaque clé entrante doit avoir un alias/nom unique ; sinon, la procédure de fusion échoue.
 - Il ne doit pas exister d'alias/noms de *groupe* de clés en double entre l'installation EKM 2.X source et l'installation EKM 3.0 cible. Chaque groupe de clés entrant doit avoir un alias/nom unique ; sinon, la procédure de fusion échoue.
 - Il ne doit pas exister de périphérique en double entre l'installation EKM 2.X source et l'installation EKM 3.0 cible ; sinon, la procédure de fusion échoue.

Procédure de fusion entre EKM 2.X et EKM 3.0

Procédez comme suit pour exécuter l'outil de fusion :

1. Connectez-vous au portail EKM 3.0. Reportez-vous à [Logging into the Encryption Key Manager 3.0 Portal](#) (Connexion au portail Encryption Key Manager 3.0).
L'écran **Welcome to Dell Encryption Key Manager** (Bienvenue dans Dell Encryption Key Manager) s'affiche.
2. Sur le serveur EKM 3.0, créez une sauvegarde d'EKM 3.0. Reportez-vous à [Performing Backups and Restoring from a Backup](#) (Exécution de sauvegardes et restauration à partir d'une sauvegarde) pour savoir comment créer des sauvegardes.
Si l'outil de fusion échoue ou endommage des données EKM 3.0, vous pourrez alors utiliser la sauvegarde pour récupérer les informations perdues.
3. Déconnectez-vous d'EKM 3.0.
4. Arrêtez le serveur EKM 3.0 avant d'exécuter l'outil de fusion. Reportez-vous à [Starting and Stopping the EKM 3.0 Server in Windows](#) (Démarrage et arrêt du serveur EKM 3.0 sous Windows) ou [Starting and Stopping the EKM 3.0 Server in Linux](#) (Démarrage et arrêt du serveur EKM 3.0 sous Linux).
5. À la racine du serveur EKM 3.0, créez le dossier approprié (par exemple, **C:\EKM_Files** sous Windows ou **/opt/EKM_Files** sous Linux).
6. Connectez-vous à la console EKM 2.X, sauvegardez le serveur EKM 2.X, arrêtez-le et quittez la console EKM 2.X. Reportez-vous au guide d'utilisation d'EKM 2.X.
7. Depuis l'emplacement où EKM 2.X est installé, copiez les fichiers suivants vers le dossier créé sur le serveur EKM 3.0 à l'étape précédente. Si EKM 2.X est installé sur un système physique différent, utilisez un lecteur amovible ou un partage réseau utilisant le même système d'exploitation.
 - Sous Windows, depuis le dossier **<racine>\ekm\gui**, copiez **EKMKeys.jck**. Sous Linux, ce fichier est stocké dans **/var/ekm/gui**.

- Sous Windows, depuis le dossier `<racine>\ekm\gui\`, copiez **KeyManagerConfig.properties** (fichier de configuration d'EKM). Sous Linux, ce fichier se trouve dans `/var/ekm/gui`.
- Sous Windows, depuis le dossier `<racine>\ekm\gui\keygroups\`, copiez **keygroup.xml**. Sous Linux, ce fichier se trouve dans `/var/ekm/gui/keygroups`.
- Sous Windows, depuis le dossier `<racine>\ekm\gui\drivetable\`, copiez **ekm_drivetable.dt**. Sous Linux, ce fichier se trouve dans `/var/ekm/gui/drivetable`.

 **PRÉCAUTION:** Sous Windows, utilisez le Bloc-notes pour créer ou modifier les fichiers texte. Si vous utilisez Wordpad, la procédure échoue.

8. Éditez le fichier **KeyManagerConfig.properties** pour qu'il contienne uniquement les propriétés suivantes :

- **config.keygroup.xml.file**
- **config.keystore.password.obfuscated**
- **config.keystore.file**
- **config.drivetable.file.url**

Supprimez les autres lignes. Pour consulter un exemple, reportez-vous à la section [Code Example](#) (Exemple de code) de la présente procédure.

9. Ajoutez les options DB2 suivantes au fichier **KeyManagerConfig.properties** :

- `jdbcURL = jdbc:db2://localhost:<port de base de données DB2 EKM 3.0>|<nom de la base de données DB2 EKM 3.0>`
- ou
- `jdbcURL = jdbc:db2://<adresse IPM du serveur EKM 3.0>:<port de base de données DB2 EKM 3.0>|<nom de la base de données DB2 EKM 3.0>`
- `jdbcUID = <nom de l'utilisateur administrateur DB2>`
- `jdbcPW = <mot de passe de l'administrateur DB2>`
- `dbType = DB2`

Pour consulter un exemple, reportez-vous à la section [Code Example](#) de la présente procédure.

 **REMARQUE:** Les variables sont des paramètres que vous définissez lors de l'installation d'EKM 3.0. N'entrez pas les symboles supérieur ou inférieur (< >) autour des variables. Les variables, noms d'utilisateur et mots de passe sont sensibles à la casse.

10. Ajoutez l'entrée de mot de passe correspondant au magasin de clés EKM 3.0 par défaut au fichier **KeyManagerConfig.properties**. Cette entrée est la suivante :

`tklm.encryption.password = <mot de passe du magasin de clés EKM 3.0>`.

Le fichier **KeyManagerConfig.properties** mis à jour doit ressembler à l'exemple suivant :

Exemple de code pour Windows

```
config.keygroup.xml.file = File:c:\\<EKM_Files>\\KeyGroups.xml
config.keystore.password.obfuscated = 38087C9DA4A4696A6B6C
config.keystore.file = c:\\<EKM_Files>\\EKMKeys.jck
config.drivetable.file.url = File:c:\\<EKM_Files>\\
\ekm_drivetable.dt jdbcURL = jdbc:db2://localhost:50010/
ekm_dell jdbcUID = ekmdell1 jdbcPW = Dell1234 dbType = DB2
tklm.encryption.password = Dell1234
```

Où `EKM_Files` est le dossier que vous avez créé [plus haut](#).

Exemple de code pour Linux

```
config.keygroup.xml.file = File:/opt/<EKM_Files>/KeyGroups.xml
config.keystore.password.obfuscated = 38087C9DA4A4696A6B6C
config.keystore.file = /opt/<EKM_Files>/EKMKeys.jck
config.drivetable.file.url = File:/opt/<EKM_Files>/
```

```
ekm_drivetable.dt jdbcURL = jdbc:db2://localhost:50010/ekm_dell
jdbcUID = ekmdell1 jdbcPW = Dell1234 dbType = DB2
tklm.encryption.password = Dell1234
```

Où *EKM_Files* est le dossier que vous avez créé [plus haut](#).

11. Accédez au dossier **EKM2DKMMerge** sur le support d'installation d'EKM 3.0. Depuis ce dossier, copiez le fichier **EKM2DKMMerge.jar** vers le dossier que vous avez créé plus tôt dans cette procédure (par exemple, [C:\EKM_Files](#) sous Windows ou [/opt/EKM_Files](#) sous Linux).

 **REMARQUE:** Vous devez utiliser la même invite de commandes ou la même session de terminal pour toutes les étapes qui suivent. Si vous changez de fenêtre d'invite de commandes ou de terminal, la variable CLASSPATH que vous définissez n'est pas automatiquement appliquée aux autres invites de commandes ou sessions de terminal.

12. Sur le serveur EKM 3.0, configurez les chemins WAS et TIP dont l'outil de fusion a besoin.

Sous Windows :

- a. Ouvrez une invite de commandes et accédez à *<racine>\Dell\EKM\bin*.
- b. Entrez la commande suivante pour exécuter le script de ligne de commande :

```
setupCmdLine.bat
```

Exemple :

```
C:\Dell\EKM\bin\setupCmdLine.bat
```

- c. Appuyez sur **Entrée**. La commande s'exécute et le système affiche le texte suivant sur la dernière ligne :

```
goto :EOF
```

Sous Linux :

- a. Ouvrez une session de terminal et accédez à */opt/dell/ekm/bin*.
 - b. Entrez la commande suivante :
- ```
. setupCmdLine.sh
```
- c. La commande s'exécute. Une fois l'opération réussie sous Linux, une invite vide apparaît. Elle ne donne aucune indication de la réussite de la commande.

 **REMARQUE:** Le script **setupCmdLine.sh** doit disposer de l'autorisation Exécuter.

13. Créez un fichier séquentiel d'invite de commande (.bat ou .sh sous Linux) pour alimenter les fichiers .jar nécessaires à l'outil de fusion et définir des paramètres supplémentaires pour la variable CLASSPATH :

  - a) Copiez la configuration CLASSPATH temporaire suivante dans un fichier texte et nommez-la *<nom\_fichier>.bat* ou, sous Linux, *<nom\_fichier>.sh* (par exemple, **configclasspath.bat** sous Windows ou **configclasspath.sh** sous Linux).
  - b) Enregistrez le fichier .bat/.sh dans le dossier créé plus tôt dans cette procédure, par exemple [C:\EKM\\_Files](#) ou [/opt/EKM\\_Files](#).

 **PRÉCAUTION:** Sous Windows, utilisez le Bloc-notes pour créer ou modifier les fichiers texte. Si vous utilisez Wordpad, la procédure échoue.

- c) Éditez le fichier séquentiel :

Sous Windows, ouvrez le fichier séquentiel et remplacez *c:\EKM\Needed* par le chemin où vous avez placé le fichier **EKM2DKMMerge.jar**, par exemple *c:\EKM\_Files*.

Sous Linux, éditez le script shell pour remplacer [/opt/EKM\\_Files](#) par le chemin où vous avez placé le fichier **EKM2DKMMerge.jar**.

**Configuration CLASSPATH temporaire pour Windows**

```
set JAVA_HOME=%WAS_HOME%\java set PATH=%JAVA_HOME%\bin;%JAVA_HOME%\jre
\bin;%PATH% set CLASSPATH=c:\EKM\Needed\EKM2DKMMerge.jar;%CLASSPATH% set
CLASSPATH=.;%WAS_HOME%\plugins\com.ibm.icu_3.4.5.jar;%WAS_HOME%\products
\tklm\migration\j2ee.jar;%WAS_HOME%\plugins\com.ibm.tklm.commands.jar;
```

```
%WAS_HOME%\products\tklm\migration\com.ibm.tklm.kmip.adapter.jar;%WAS_HOME%
%\profiles\TIPProfile\installedApps\TIPCell\tklm_kms.ear
\com.ibm.tklm.kmip.jar;"C:\Program Files\Dell\db2dkm\java\db2jcc.jar";"C:
\Program Files\Dell\db2dkm\java\db2jcc_license_cu.jar";%WAS_HOME%\profiles
\TIPProfile\installedApps\TIPCell\tklm_kms.ear\com.ibm.tklm.keyserver.jar;
%WAS_HOME%\profiles\TIPProfile\installedApps\TIPCell\tklm_kms.ear
\com.ibm.tklm.server.api.jar;%WAS_HOME%\profiles\TIPProfile\installedApps
\TIPCell\tklm_kms.ear\com.ibm.tklm.server.db.ejb.jar;%CLASSPATH%
```

 **REMARQUE:** Remplacez les lettres de lecteur si nécessaire.

 **REMARQUE:** Si vous utilisez Windows 64 bits, éditez le fichier séquentiel pour remplacer **Program Files**, dans le chemin CLASSPATH ci-dessus, par **Program Files (x86)**.

#### Configuration CLASSPATH temporaire pour Linux

```
export JAVA_HOME=$WAS_HOME/java export PATH=${JAVA_HOME}/bin:${JAVA_HOME}
$/jre/bin:$PATH export CLASSPATH=/opt/EKM_Files/EKM2DKMMerge.jar:
$CLASSPATH export CLASSPATH=.:$WAS_HOME/plugins/com.ibm.icu_3.4.5.jar:
$WAS_HOME/products/tklm/migration/j2ee.jar:$WAS_HOME/plugins/
com.ibm.tklm.commands.jar:$WAS_HOME/products/tklm/migration/
com.ibm.tklm.kmip.adapter.jar:$WAS_HOME/profiles/TIPProfile/installedApps/
TIPCell/tklm_kms.ear/com.ibm.tklm.kmip.jar:/opt/dell/db2ekm/java/
db2jcc.jar:/opt/dell/db2ekm/java/db2jcc_license_cu.jar:$WAS_HOME/profiles/
TIPProfile/installedApps/TIPCell/tklm_kms.ear/com.ibm.tklm.keyserver.jar:
$WAS_HOME/profiles/TIPProfile/installedApps/TIPCell/tklm_kms.ear/
com.ibm.tklm.server.api.jar:$WAS_HOME/profiles/TIPProfile/installedApps/
TIPCell/tklm_kms.ear/com.ibm.tklm.server.db.ejb.jar:$CLASSPATH
```

14. Exécutez le fichier séquentiel que vous venez de créer. Dans la même fenêtre d'invite de commandes ou de terminal sur le serveur EKM 3.0, accédez au dossier créé plus tôt dans cette procédure (par exemple, [C:\EKM\\_Files](#) sous Windows ou [/opt/EKM\\_Files](#) sous Linux), puis exécutez le fichier séquentiel créé à l'étape précédente. Sous Linux, utilisez le fichier que vous avez créé plus haut, par exemple, [.setupclasspath.sh](#).

15. Dans la même fenêtre d'invite de commandes ou de terminal sur le serveur EKM 3.0, exécutez la commande Java suivante :

```
java<espace>com.ibm.tklm.ekm2tklm.MergeEKM2KLM<espace>KeyManagerConfig.prope
rties
```

 **REMARQUE:** Les commandes sont sensibles à la casse. N'entrez pas les symboles supérieur ou inférieur (<>) autour des variables.

Le fichier **KeyManagerConfig.properties** est celui que vous avez déjà utilisé plus tôt dans cette procédure.

Cette commande fusionne EKM 2.X dans EKM 3.0.

Une fois le traitement achevé avec succès, le message suivant s'affiche :

```
Version TKLM : 2.0.0.0 201007241325 Démarrage d'EKM dans KLM
MergeKMSDebug.init, nom de fichier de sortie de débogage non spécifié :
utilisation de la valeur par défaut CTGKS0250I : magasins de clés,
certificats et clés Encryption Key Manager migrés avec succès. CTGKS0251I :
groupes de clés Encryption Key Manager migrés avec succès. CTGKS0249I :
périphériques Encryption Key Manager migrés avec succès. Migration terminée.
```

 **REMARQUE:** Si des erreurs apparaissent, consultez le journal de débogage pour en connaître la cause. Si vous le souhaitez, vous pouvez enregistrer ce journal à un autre endroit ou le renommer pour qu'il devienne statique. Sinon, l'outil de fusion d'EKM 2.X dans EKM 3.0 ajoute des données à la fin de ce fichier. Sous Windows, le journal de débogage se trouve dans le dossier suivant sur le serveur EKM 3.0 : **<racine>:\Dell\EKM\bin\products\tklm\logs\debug.log**. Sous Linux, le journal de débogage se trouve dans le dossier suivant sur le serveur EKM 3.0 : **/opt/dell/ekm/bin/products/tklm/logs/debug.log**.

 **REMARQUE:** Si l'erreur suivante s'affiche, vous tentez d'effectuer la migration alors qu'il existe un élément en double (qui existe à la fois sur le serveur EKM 2.X et le serveur EKM 3.0).

Doublon d'<élément> = Échec de la migration d'<élément>. Consultez le fichier de débogage pour en savoir plus.

Reportez-vous à [Deleting the ekmcert Certificate, Keys, and Key Groups, and Renaming Devices](#) (Suppression du certificat ekmcert, des clés et des groupes de clés, et changement du nom des périphériques).

Si l'erreur suivante se produit et que vous souhaitez supprimer la clé au lieu de la renommer, ne fermez pas la fenêtre d'invite de commande ou de terminal. Vous allez devoir copier l'alias de clé depuis cette fenêtre.

Doublon d'alias de clé = <alias de clé>

Reportez-vous à [Deleting the ekmcert Certificate, Keys, and Key Groups, and Renaming Devices](#) (Suppression du certificat ekmcert, des clés et des groupes de clés, et changement du nom des périphériques).

 **PRÉCAUTION:** La suppression d'une clé revient à supprimer toutes les données protégées par cette clé, puisqu'elles deviennent inaccessibles. Il est totalement impossible de récupérer les clés supprimées, par quelque moyen que ce soit, pour des raisons de sécurité.

16. Démarrez le serveur EKM 3.0 à l'aide de la commande **startserver**. Reportez-vous à [Starting and Stopping the EKM 3.0 Server in Windows](#) (Démarrage et arrêt du serveur EKM 3.0 sous Windows) ou à [Starting and Stopping the EKM 3.0 Server in Linux](#) (Démarrage et arrêt du serveur EKM 3.0 sous Linux).

17. Vérifiez que les groupes de clés, clés et périphériques EKM 2.X ont été migrés vers EKM 3.0. Reportez-vous à [Verifying the EKM 2.X to EKM 3.0 Merge or Migration](#) (Vérification de la fusion ou de la migration d'EKM 2.X vers EKM 3.0). Si la procédure de fusion réussit, vous avez terminé. Si vous souhaitez fusionner des installations EKM 2.X supplémentaires dans EKM 3.0, reportez-vous à [Merging Additional EKM 2.X Versions into EKM 3.0](#) (Fusion d'installations EKM 2.X supplémentaires dans EKM 3.0). Si la procédure de fusion échoue, reportez-vous à [Merge Failure](#) (Échec de la fusion).

 **PRÉCAUTION:** N'exécutez pas EKM 2.X après avoir fusionné ses clés dans EKM 3.0. Si vous le souhaitez, vous pouvez désinstaller EKM 2.X après fusion d'EKM 2.X dans EKM 3.0. Dell vous recommande de sauvegarder les fichiers EKM 2.X avant de désinstaller EKM 2.X.

## Vérification de la fusion ou de la migration d'EKM 2.X vers EKM 3.0

Ce chapitre explique comment vérifier que la procédure de fusion ou de migration d'EKM 2.X dans EKM 3.0 a réussi, et que les bibliothèques de bandes sont opérationnelles.

Pour vérifier que l'installation EKM 2.X a été fusionnée ou migrée avec succès dans EKM 3.0, procédez comme suit :

1. Connectez-vous au portail EKM 3.0. Reportez-vous à [Logging into the Encryption Key Manager 3.0 Portal](#) (Connexion au portail Encryption Key Manager 3.0).  
L'écran **Welcome to Dell Encryption Key Manager** (Bienvenue dans Dell Encryption Key Manager) s'affiche.
2. Dans le volet de navigation, accédez à **Dell Encryption Key Manager** → **Key and Device Management** (Gestion des clés et des périphériques).  
L'écran **Key and Device Management** (Gestion des clés et des périphériques) s'ouvre.
3. Dans le menu déroulant **Manage keys and devices** (Gérer les clés et les périphériques), sélectionnez **LTO**, puis cliquez sur **OK**.  
L'écran **Key and Device Management** affiche le ou les groupes de clés EKM migrés et le nombre de clés dans chaque groupe.
4. Dans le menu déroulant en haut de la table, sélectionnez **View Keys, Key Group Membership and Drives** (Afficher les clés, l'appartenance aux groupes de clés et les lecteurs). Si des clés apparaissent à gauche de la table, la fusion a réussi.

5. La migration n'importe pas les périphériques configurés dans EKM 2.X. Vous devez configurer les périphériques EKM 2.X. Reportez-vous à [Adding a Device to a Device Group](#) (Ajout d'un périphérique à un groupe de périphériques).
6. Dans le portail EKM 3.0, vérifiez qu'EKM 3.0 est configuré pour accepter automatiquement les demandes des périphériques. Le paramètre sélectionné dans l'écran **Key and Device Management** doit être **Automatically accept all new device requests for communication** (Accepter automatiquement toutes les demandes de communication des nouveaux périphériques).
7. Vérifiez les périphériques dans votre bibliothèque :
  - a) Vérifiez que le port SSL et le port TCP sont correctement configurés dans votre bibliothèque.
  - b) Exécutez les diagnostics de chemins de clés dans votre bibliothèque de bandes pour vérifier la configuration de cette dernière.

 **REMARQUE:** Pour en savoir plus, consultez le guide d'utilisation de la bibliothèque de bandes. Pour savoir comment accéder à ce guide, consultez la section Documentation and Reference Materials (Documentation et informations de référence) du fichier **ReadThisFirst.txt** sur le support d'installation d'EKM 3.0.

## Échec de la fusion

Si la fusion échoue, procédez comme suit :

1. Vérifiez que le serveur EKM 3.0 est démarré. Si tel n'est pas le cas, démarrez-le à l'aide de la commande **startserver**. Reportez-vous à « [Démarrage et arrêt du serveur EKM 3.0 sous Windows](#) » ou à « [Démarrage et arrêt du serveur EKM 3.0 sous Linux](#) ».
2. Fermez l'invite de commandes.
3. Capturez le journal de débogage en l'enregistrant à un autre emplacement ou en le renommant.  
Le journal de débogage se trouve dans le dossier suivant : `<root>:\Dell\EKM\bin\products\tklm\logs\debug.log` sous Windows ou `/opt/dell/ekm/bin/products/tklm/logs/debug.log` sous Linux.
4. Restaurez EKM 3.0 (via le portail EKM 3.0) depuis la sauvegarde créée à la première étape de la [procédure de fusion entre EKM 2.X et EKM 3.0](#). Pour en savoir plus sur la restauration depuis une sauvegarde, reportez-vous à « [Restauration à partir d'une sauvegarde](#) ».
5. Répétez la procédure de fusion. Reportez-vous à « [Procédure de fusion entre EKM 2.X et EKM 3.0](#) ».

## Fusion d'installations EKM 2.X supplémentaires dans EKM 3.0

Appliquez cette procédure si vous avez migré ou fusionné une installation EKM 2.X dans EKM 3.0, et que vous voulez fusionner des installations EKM 2.X supplémentaires dans EKM 3.0.

1. Supprimez le certificat **ekmcert** d'EKM 3.0. Reportez-vous à « [Suppression du certificat ekmcert, des clés et des groupes de clés, et changement du nom des périphériques](#) ».
2. Appliquez la procédure de fusion à chacune des installations EKM 2.X supplémentaires à fusionner. Reportez-vous à « [Procédure de fusion entre EKM 2.X et EKM 3.0](#) ».

## Suppression du certificat ekmcert, des clés et des groupes de clés, et changement du nom des périphériques

Lors d'une fusion entre EKM 2.X et EKM 3.0, il ne peut pas exister de certificat **ekmcert**, d'alias de clé, d'alias de groupe de clés ou de périphériques en double dans EKM 2.X et sur le serveur EKM 3.0.

 **REMARQUE:** S'il existe des clés ou groupes de clés en double, Dell vous recommande de renommer les doublons dans EKM 2.X avant la fusion vers EKM 3.0. Reportez-vous au guide d'utilisation d'EKM 2.X pour en savoir plus. Si les clés ou groupes de clés en double sont obsolètes, vous pouvez les supprimer dans EKM 2.X. Toutefois, la suppression d'une clé revient à supprimer toutes les données protégées par cette clé, puisqu'elles deviennent inaccessibles. Il est totalement impossible de récupérer les clés supprimées, par quelque moyen que ce soit, pour des raisons de sécurité.

Si vous possédez des périphériques en double, vous devez supprimer un périphérique dans EKM 2.X.

Si l'erreur suivante apparaît lorsque vous effectuez la fusion, supprimez l'élément approprié selon les informations du message d'erreur.

Duplicate <item> = <item> Migration failed. Please refer to the debug file for more information. (Doublon d'<élément> = Échec de la migration d'<élément>. Consultez le fichier de débogage pour en savoir plus.)

Reportez-vous à la section appropriée :

- [Suppression du certificat ekmcert](#)
- [Suppression d'une clé spécifique](#)
- [Suppression d'un périphérique](#)



## Suppression du certificat **ekmcert**

Chaque installation EKM 2.X comporte un seul certificat **ekmcert**. Si vous fusionnez ou migrez plusieurs installations EKM 2.X vers EKM 3.0, vous devez supprimer le certificat **ekmcert** d'EKM 3.0 avant de tenter de fusionner une nouvelle installation EKM 2.X.

Comme **ekmcert** est un certificat et non une clé, il n'appartient à aucun groupe de clés sur le serveur EKM 3.0. Par conséquent, si vous avez fusionné une installation EKM 2.X dans EKM 3.0, puis supprimé les groupes de clés EKM 2.X d'EKM 3.0, le certificat **ekmcert** issu de la fusion existera toujours sur le serveur EKM 3.0, parfois même si vous restaurez les données à partir d'une sauvegarde précédente. Comme l'outil de fusion tente de nouveau d'ajouter le certificat **ekmcert**, la fusion échoue.

Vous devez supprimer le certificat **ekmcert** du serveur EKM 3.0 dans les situations suivantes :

- Vous avez migré une installation EKM 2.X vers EKM 3.0 pendant l'installation d'EKM 3.0.
- Ce n'est pas la première fusion que vous effectuez entre EKM 2.X et EKM 3.0.
- Vous devez supprimer une version d'EKM 2.X précédemment fusionnée ou migrée.
- L'erreur suivante s'affiche lorsque vous tentez la fusion. Cette erreur indique que le certificat **ekmcert** se trouve déjà dans EKM 3.0 :

Duplicate Key Alias = ekmcert Migration failed. Please refer to the debug file for more information. (Doublon d'alias de clé = Échec de la migration d'ekmcert. Consultez le fichier de débogage pour en savoir plus.)

Pour supprimer le certificat **ekmcert**, reportez-vous à « [Suppression du certificat ekmcert](#) ».

### **Suppression du certificat ekmcert**

Pour vérifier que le certificat **ekmcert** se trouve dans EKM 3.0 et pour le supprimer, procédez comme suit :

1. Connectez-vous au portail EKM 3.0. Reportez-vous à « [Connexion au portail Encryption Key Manager 3.0](#) ».  
L'écran **Bienvenue dans Dell Encryption Key Manager** s'affiche.
2. Dans le volet de navigation, accédez à **Dell Encryption Key Manager** → **Advanced Configuration (Configuration avancée)** → **Server Certificates (Certificats de serveur)**.  
L'écran **Administer Server Certificates** (Administrer les certificats de serveur) s'affiche.
3. Dans l'écran **Administer Server Certificates** (Administrer les certificats de serveur), vérifiez que le certificat **ekmcert** apparaît dans la liste et qu'il n'est pas en cours d'utilisation.  
Si le certificat **ekmcert** n'est pas en cours d'utilisation, passez à l'[étape suivante](#). Si le certificat **ekmcert** est en cours d'utilisation, procédez comme suit :
  - a) Sélectionnez le certificat **ekmcert**.
  - b) Cliquez sur **Modify** (Modifier).
  - c) Désélectionnez la case à cocher **Current Certificate In Use** (Certificat actuel utilisé).
  - d) Cliquez sur **Modify Certificate** (Modifier le certificat).  
L'écran **Administer Server Certificates** (Administrer les certificats de serveur) apparaît. Le certificat est marqué comme n'étant pas en cours d'utilisation.
4. Sélectionnez de nouveau le certificat **ekmcert**.
5. Cliquez sur **Delete** (Supprimer) en haut de la table.  
Une fenêtre de confirmation s'affiche.
6. Cliquez sur **OK** pour supprimer le certificat.  
Le certificat est supprimé de la liste.

### **Suppression d'une clé spécifique**

Ce chapitre explique comment supprimer une seule clé. Vous ne pouvez pas supprimer une clé associée à un périphérique.



**PRÉCAUTION:** La suppression d'une clé revient à supprimer toutes les données protégées par cette clé, puisqu'elles deviennent inaccessibles. Il est totalement impossible de récupérer les clés supprimées, par quelque moyen que ce soit, pour des raisons de sécurité.



**REMARQUE:** Si un message d'erreur vous indique qu'il existe une clé en double pendant la fusion entre EKM 2.X et EKM 3.0, Dell vous recommande de renommer le doublon dans EKM 2.X. Pour en savoir plus, consultez le guide d'installation d'EKM 2.X.

1. Connectez-vous au portail EKM 3.0. Reportez-vous à [Logging into the Encryption Key Manager 3.0 Portal](#) (Connexion au portail Encryption Key Manager 3.0).  
L'écran **Welcome to Dell Encryption Key Manager** (Bienvenue dans Dell Encryption Key Manager) s'affiche.
2. Dans le volet de navigation, accédez à **Dell Encryption Key Manager** → **Key and Device Management** (Gestion des clés et des périphériques).  
L'écran **Key and Device Management** s'ouvre.
3. Dans le menu déroulant **Manage keys and devices** (Gérer les clés et les périphériques), sélectionnez **LTO**, puis cliquez sur **OK**.  
L'écran **Key and Device Management** s'ouvre.
4. Dans le menu déroulant en haut de la table, sélectionnez **View Keys, Key Group Membership and Drives** (Afficher les clés, l'appartenance aux groupes de clés et les lecteurs).  
Les clés s'affichent dans la table.
5. Cliquez sur la clé à supprimer pour la mettre en surbrillance.
6. Cliquez sur **Delete** (Supprimer) en haut de la table.  
Une fenêtre pop-up de confirmation s'affiche.
7. Si vous êtes certain de vouloir supprimer la clé sélectionnée, cliquez sur **OK**.  
La clé est supprimée.

### Suppression d'un périphérique

Ce chapitre explique comment supprimer un périphérique. On appelle périphérique chacun des lecteurs distincts installés dans la bibliothèque de bandes. Le numéro de série est affiché sur la droite du lecteur de bande.



**REMARQUE:** Si un message d'erreur vous indique qu'il existe un périphérique en double pendant la fusion entre EKM 2.X et EKM 3.0, Dell vous recommande de supprimer le périphérique dans EKM 2.X. Pour en savoir plus, consultez le guide d'installation d'EKM 2.X.

Pour supprimer le périphérique d'EKM 3.0, procédez comme suit :

1. Connectez-vous au portail EKM 3.0. Reportez-vous à [Logging into the Encryption Key Manager 3.0 Portal](#) (Connexion au portail Encryption Key Manager 3.0).  
L'écran **Welcome to Dell Encryption Key Manager** (Bienvenue dans Dell Encryption Key Manager) s'affiche.
2. Dans le volet de navigation, accédez à **Dell Encryption Key Manager** → **Key and Device Management** (Gestion des clés et des périphériques).  
L'écran **Key and Device Management** s'ouvre.
3. Dans le menu déroulant **Manage keys and devices** (Gérer les clés et les périphériques), sélectionnez le nom du groupe de périphériques qui contient le périphérique à supprimer.
4. Cliquez sur **Go** (OK).  
Les périphériques qui appartiennent au groupe de périphériques sont affichés.
5. Cliquez sur le périphérique à supprimer pour le mettre en surbrillance.
6. Cliquez sur **Delete** (Supprimer) en haut de la table.  
Une fenêtre contextuelle de confirmation s'affiche.

7. Cliquez sur **OK** dans la fenêtre contextuelle.  
Le périphérique est supprimé.

### Vérification de la suppression de la bibliothèque de magasins de clés EKM 2.X depuis EKM 3.0

Cette procédure est facultative. Ce chapitre explique comment vérifier que toutes les entrées de magasin de clés EKM 2.X (certificat **ekmcert** et clés dans le magasin de clés EKM 2.X) ont été supprimées du serveur EKM 3.0. Pour ce faire, procédez comme suit :

1. Ouvrez une invite de commandes ou une session de terminal sur le serveur EKM 3.0, accédez au dossier créé lors de la [procédure de fusion entre EKM 2.X et EKM 3.0](#) (par exemple, **C:\EKM\_Files** sous Windows ou **/opt/EKM\_Files** sous Linux).

2. Vérifiez que l'outil **keytool** de Java SDK est disponible sur le chemin de la ligne de commande.

3. Répertoriez le contenu du magasin de clés EKM 2.X à l'aide de la commande suivante :

```
keytool -list -keystore <nom_magasin_clés_EKM_2.X> -storetype JCEKS
```

Où *<nom\_magasin\_clés\_EKM\_2.X>* est le nom du magasin de clés EKM 2.X que vous importez.

Par exemple :

```
keytool -list -keystore EKMKeys.jck -storetype JCEKS
```

Le système vous invite à saisir un mot de passe.

4. Entrez le mot de passe du magasin de clés EKM 2.X et appuyez sur **Entrée**.

Le type du magasin de clés EKM 2.X, le certificat **ekmcert**, le fournisseur du magasin de clés et les clés du magasin de clés EKM 2.X sont affichés. Vous utilisez la liste de clés pour effectuer une comparaison avec le magasin de clés EKM 3.0 afin de vérifier que ces clés ne sont pas dans le magasin EKM 3.0.

 **REMARQUE:** Maintenez l'invite de commandes ouverte. À l'une des étapes ultérieures, vous allez rechercher ces clés et/ou le certificat **ekmcert** dans le magasin de clés EKM 3.0 pour vérifier qu'ils ont été supprimés d'EKM 3.0.

5. Démarrez le serveur EKM 3.0 à l'aide de la commande **startserver**. Reportez-vous à « [Démarrage et arrêt du serveur EKM 3.0 sous Windows](#) » ou à « [Démarrage et arrêt du serveur EKM 3.0 sous Linux](#) ».

6. Ouvrez une invite de commandes Windows et accédez à **<root>:\Dell\EKM\bin**. Sous Linux, accédez à **/opt/dell/ekm/bin**.

7. Connectez-vous au serveur WebSphere à l'aide de la commande **wsadmin**. Reportez-vous à « [Connexion au serveur WebSphere](#) ».

8. À l'invite **wsadmin**, utilisez l'alias de clé obtenu précédemment pour envoyer l'une des commandes suivantes, qui répertorient une clé ou un certificat spécifique sur le serveur EKM 3.0 :

Pour les clés :

```
print AdminTask.tklmKeyList('[-alias <alias de clé>]')
```

Pour le certificat **ekmcert** :

```
print AdminTask.tklmKeyList('[-alias ekmcert]')
```

 **REMARQUE:** Vous avez obtenu les alias de clé lors d'une étape précédente. Sous Windows, vous pouvez copier les alias à l'aide de la barre d'outils de la fenêtre d'invite de commandes.

 **REMARQUE:** Pour comparer visuellement les alias de clé, vous pouvez lister toutes les clés du serveur EKM 3.0 avec la commande suivante :

```
print AdminTask.tklmKeyList('[-alias]')
```

9. Appuyez sur **Entrée**.

La commande est exécutée.

Si le double de la clé ne se trouve pas dans EKM 3.0, le message suivant apparaît :

```
0 clé trouvée.
```

Si la clé ou le certificat existe dans EKM 3.0, l'écran affiche l'UUID, et l'alias de la clé ou du certificat.

Si la clé ou le certificat existe dans EKM 3.0, supprimez cet élément d'EKM 3.0. Reportez-vous à « [Suppression d'une clé spécifique](#) ».

Répétez [cette étape](#) pour chaque double de clé répertorié [précédemment](#).

# Désinstallation d'EKM 3.0

Ce chapitre explique comment désinstaller EKM 3.0 sous Windows et Linux.

 **PRÉCAUTION:** La désinstallation d'EKM 3.0 rend illisibles toutes les données cryptées écrites dans la bande de Dell PowerVault par cryptage géré par la bibliothèque (LME). Vérifiez que toutes les données critiques ont été restaurées avant de désinstaller EKM 3.0. Si vous pensez être amené à réinstaller EKM 3.0 à l'avenir, créez une sauvegarde avant de désinstaller EKM 3.0. Copiez la sauvegarde EKM 3.0 et le profil d'installation (si vous en avez enregistré un) sur un lecteur externe avant de désinstaller EKM 3.0. Ultérieurement, pour réinstaller EKM 3.0, utilisez ce fichier de sauvegarde pour exécuter une opération de restauration. Reportez-vous à « [Exécution de sauvegardes et restauration à partir d'une sauvegarde](#) ».

 **REMARQUE:** La procédure de désinstallation prend environ 35 minutes. N'éteignez pas le système tant que la désinstallation n'est pas terminée.

 **REMARQUE:** La désinstallation d'EKM 3.0 désinstalle également WebSphere et DB2. Si vous utilisez DB2 pour d'autres applications, Dell vous recommande de ne pas désinstaller EKM 3.0. Il est recommandé, à la place, d'arrêter le service EKM 3.0. Pour plus d'informations sur l'arrêt du service EKM 3.0, reportez-vous à « [Démarrage et arrêt du serveur EKM 3.0 sous Windows](#) » ou à « [Démarrage et arrêt du serveur EKM 3.0 sous Linux](#) ».

 **REMARQUE:** Si vous utilisez une configuration avec serveurs principal et secondaire, vous devez également effectuer l'opération de désinstallation sur le serveur EKM 3.0 secondaire.

 **REMARQUE:** Si vous souhaitez réinstaller EKM 3.0, reportez-vous à « [Réinstallation d'EKM 3.0](#) ».

## Désinstallation d'EKM 3.0 sous Windows

Cette procédure utilise le programme de désinstallation d'EKM 3.0 pour Windows.

 **REMARQUE:** La procédure de désinstallation prend environ 35 minutes. N'éteignez pas le système tant que la désinstallation n'est pas terminée.

1. Sous Windows 2008, ouvrez le **Panneau de configuration**, puis accédez à **Programmes et fonctionnalités**.  
Sous Windows Server 2003 R2 avec Service Pack 2, ouvrez le **Panneau de configuration**, puis accédez à **Ajouter ou supprimer des programmes**.
2. Cliquez avec le bouton droit sur **EKM 3.0** et sélectionnez **Désinstaller**.
3. Suivez les instructions affichées à l'écran.  
Une fois la désinstallation terminée, vous voyez s'afficher la fenêtre **Désinstallation terminée**.
4. Dans l'écran **Désinstallation terminée**, cliquez sur **Terminé**.  
Une boîte de dialogue s'affiche, signalant que le système va redémarrer.
5. Cliquez sur **Terminé** dans cette boîte de dialogue. (Même si vous ne le faites pas, Windows redémarre après environ une minute.)

 **REMARQUE:** Si Windows ne redémarre pas, redémarrez manuellement la machine.

 **REMARQUE:** En cas d'erreur pendant la désinstallation, vous pouvez consulter le journal d'installation principal stocké dans le répertoire de travail, sous `<racine>\Utilisateurs\Administrateur`. Le fichier journal d'installation principal s'appelle `IA-TIPxxx`. Faites défiler l'affichage pour aller à la fin de ce journal, afin de déterminer l'endroit où le processus s'est arrêté ou l'endroit où la dernière erreur s'est produite. Vous pouvez aussi afficher les fichiers journaux sous `<racine>\tklmv2properties` pour en savoir plus.

 **REMARQUE:** Si vous réinstallez EKM 3.0 et que l'installation échoue en raison d'une désinstallation incomplète, effectuez la désinstallation manuellement. Reportez-vous à [Manually Uninstalling EKM 3.0 in Windows](#) (Désinstallation manuelle d'EKM 3.0 sous Windows).

## Désinstallation d'EKM 3.0 sous Linux

Cette procédure utilise le programme de désinstallation d'EKM 3.0 pour Linux.

 **REMARQUE:** La procédure de désinstallation prend environ 35 minutes. N'éteignez pas le système tant que la désinstallation n'est pas terminée.

1. Ouvrez une session de terminal et accédez à `/opt/dell/ekm/Uninstall_EKM`.
2. Exécutez la **désinstallation d'EKM** à l'aide de la commande suivante :  

```
./Uninstall EKM
```

Une fenêtre pop-up s'affiche.
3. Cliquez sur **Run** (Exécuter) dans la fenêtre pop-up.  
La fenêtre **Uninstall EKM** (Désinstaller EKM) s'affiche.
4. Cliquez sur **Désinstaller** (Désinstaller).  
Le processus de désinstallation démarre.
5. Une fois la désinstallation terminée, vous voyez s'afficher la fenêtre **Uninstall Complete** (Désinstallation terminée). Cliquez sur **Done** (Terminé).  
Le système redémarre.

 **REMARQUE:** Si vous réinstallez EKM 3.0 et que l'installation échoue en raison d'une désinstallation incomplète, effectuez la désinstallation manuellement. Reportez-vous à « [Désinstallation manuelle d'EKM 3.0 sous Linux](#) ».

# Dépannage

Ce chapitre fournit des informations sur le dépannage, détaille les questions fréquemment posées, présente les messages d'erreur courants et indique les coordonnées du support technique.

 **REMARQUE:** Si votre problème n'est pas présenté dans ce chapitre, reportez-vous au guide de dépannage de TKLM. Pour savoir comment accéder à cette documentation, consultez la section Documentation and Reference Materials (Documentation et informations de référence) du fichier **ReadThisFirst.txt** sur le support d'installation d'EKM 3.0.

## Contacteur Dell

 **REMARQUE:** Si vous ne disposez pas d'une connexion Internet, les informations de contact figurent sur la facture d'achat, le bordereau de colisage, la facture le catalogue des produits Dell.

Dell propose diverses options d'assistance et de maintenance en ligne et téléphonique. Ces options varient en fonction du pays et du produit et certains services peuvent ne pas être disponibles dans votre région. Pour contacter le service commercial, technique ou client de Dell :

1. Visitez le site **support.dell.com**.
2. Sélectionnez la catégorie d'assistance.
3. Si vous ne résidez pas aux États-Unis, sélectionnez le code pays au bas de la page ou sélectionnez **Tout** pour afficher d'autres choix.
4. Sélectionnez le lien de service ou d'assistance approprié.



## Vérifications des prérequis système

EKM 3.0 vérifie les prérequis système avant l'installation. Si un message d'erreur s'affiche après l'écran **License Agreement** (Contrat de licence), suivez les instructions de ce message. Pour les erreurs les plus courantes, vous trouverez des instructions ci-dessous.

### Configuration système minimale non conforme

Si vous voyez apparaître l'erreur **Minimum System Requirements Failed** (Configuration système minimale non conforme), cliquez sur **Cancel and Exit** (Annuler et quitter), puis vérifiez que votre système répond à la configuration minimale requise. Pour connaître la configuration système requise, reportez-vous à [Hardware and Software Requirements](#) (Configuration matérielle et logicielle requise).

### L'utilisateur n'est pas administrateur de ce système.

Vous devez être utilisateur root sous Linux ou administrateur sous Windows pour installer EKM 3.0.

### SELinux doit être désactivé.

Si SELinux est installé et activé, désactivez-le avant de lancer l'installation.

Pour désactiver SELinux sous RHEL5, procédez comme suit :

1. Utilisez la barre d'outils supérieure du bureau pour accéder à **System** → **Administration** → **Security Level and Firewall** (Système > Administration < Niveau de sécurité et pare-feu).  
La fenêtre **Security Level Configuration** (Configuration du niveau de sécurité) s'affiche.
2. Cliquez sur l'onglet **SELinux**. Dans la zone **SELinux Setting** (Paramètre SELinux), cliquez sur les flèches et sélectionnez **Disabled** (Désactivé).
3. Cliquez sur **Apply** (Appliquer).
4. Cliquez sur **OK**.
5. Redémarrez le système pour que les modifications prennent effet.

Pour désactiver SELinux sous RHEL4, procédez comme suit :

1. Accédez à **Applications** → **System Settings** → **Security Level** (Applications > Paramètres système > Niveau de sécurité).  
Une fenêtre contextuelle s'affiche.
2. Dans la fenêtre contextuelle, sélectionnez l'onglet **SELinux**.
3. Dans le menu déroulant, sélectionnez **Disable** (Désactiver).
4. Redémarrez le système.

### compat-libstdc++ Not Installed (compat-libstdc++ non installé)

Si un message d'erreur signale que compat-libstdc++ n'est pas installé, reportez-vous à [Installing the compat-libstdc++ Library](#) (Installation de la bibliothèque compat-libstdc++).

### Limites minimales de mémoire partagée requises non conformes.

Lors de l'installation d'EKM 3.0 sous Linux, l'erreur suivante apparaît :

```
The system did not meet the minimum shared memory requirements needed for the installation. Make sure your system meets the minimum requirements before attempting this installation. (Le système ne répond pas à la configuration minimale de mémoire partagée nécessaire à l'installation. Assurez-vous que votre système répond à la configuration requise avant de tenter d'effectuer cette installation.)
```

Pour résoudre ce problème, effectuez les étapes suivantes :

1. Pour augmenter la mémoire partagée afin d'atteindre la taille requise et de la rendre temporaire (persistente), ouvrez une session de terminal et saisissez la commande suivante :

```
echo "kernel.msgmni = 1024" >> /etc/sysctl.conf echo "kernel.msgmax = 65536" >> /etc/sysctl.conf echo "kernel.msgmnb = 65536" >> /etc/sysctl.conf echo "kernel.sem = 250 256000 32 1024" >> /etc/sysctl.conf echo "kernel.shmmax = 1268435456" >> /etc/sysctl.conf
```

 **REMARQUE:** Il s'agit des valeurs minimales requises pour l'installation d'EKM 3.0 sous Linux. EKM 3.0 peut avoir besoin de davantage de mémoire partagée (kernel.shmmax) pour que l'installation réussisse. Si l'installation échoue, désinstallez EKM 3.0, augmentez kernel.shmmax d'environ 25 %, puis réinstallez EKM 3.0. Pour désinstaller EKM 3.0, reportez-vous à [Uninstalling EKM 3.0](#) (Désinstallation d'EKM 3.0).

2. Utilisez la commande suivante pour que le système utilise immédiatement la nouvelle taille de mémoire partagée (sinon, vous devez redémarrer l'ordinateur) :

```
sysctl -p
```

#### **L'utilisateur DB2 existe déjà comme utilisateur standard.**

Le nom d'utilisateur entré dans le champ **DB2 User Name** (Nom d'utilisateur DB2) existe déjà en tant qu'utilisateur sur le système. Choisissez un autre nom d'utilisateur.

#### **Installation TKLM ou EKM 3.0 existante sur le même système.**

TKLM ou EKM 3.0 est déjà installé. Désinstallez l'instance existante ou installez EKM 3.0 sur un autre système.

#### **Installation DB2 existante sur le même système.**

DB2 est déjà installé. Désinstallez DB2 ou installez EKM 3.0 sur un autre système.

#### **ksh non installé.**

Le programme d'installation d'EKM 3.0 a besoin de **ksh**. Installez **ksh**, puis EKM 3.0. Reportez-vous à la documentation de votre système d'exploitation.

#### **Le nom d'hôte contient des caractères spéciaux.**

Le nom d'hôte de l'ordinateur où vous installez EKM 3.0 ne doit contenir ni espaces, ni caractères spéciaux tels que les tirets (-) ou traits de soulignement (\_). EKM 3.0 prend en charge uniquement les caractères alphanumériques dans le nom d'hôte.

#### **Nom de domaine.**

Le nom de domaine de l'ordinateur où vous installez EKM 3.0 ne doit contenir ni espaces, ni caractères spéciaux tels que les tirets (-) ou traits de soulignement (\_). EKM 3.0 prend en charge uniquement les caractères alphanumériques dans le nom de domaine.

#### **Fichier /etc/hosts non valide.**

Le fichier **/etc/hosts** doit contenir une entrée valide correspondant à l'adresse IPv4 de boucle de rappel. Cette entrée doit être au format suivant :

```
<Adresse IPv4 de boucle de rappel><espace><nom d'hôte entièrement qualifié><espace><nom d'hôte abrégé>
```

Où *<espace>* indique un espace.

## Codes d'erreur

Pour accéder à la liste des codes d'erreur avec leur description, consultez la section Documentation and Reference Materials (Documentation et informations de référence du fichier **ReadThisFirst.txt** sur le support d'installation d'EKM 3.0.



## Fichiers de référence Windows

Vous pouvez utiliser les fichiers journaux et fichiers d'erreurs suivants pour dépanner l'installation d'EKM 3.0 sous Windows :

- **C:\tkm\_install.stderr** (fichier journal d'erreurs standard)
- **C:\tkmV2properties\\*.log** (journaux d'installation de DB2)
- **C:\Users\Administrator\IA-TIPInstall-00.txt** (journal d'installation d'EKM 3.0)

 **REMARQUE:** Ce chemin s'applique aux installations sous Windows Server 2008. Pour Windows Server 2003 R2 avec Service Pack 2, le journal d'installation d'EKM 3.0 se trouve dans **C:\Documents and Settings\Administrator\IA-TIPInstall-00.txt**.

- **C:\Dell\EKM\products\tkm\logs\audit\tkm\_audit.txt** (fichier d'audit). (Ce fichier peut aussi servir à dépanner les problèmes d'utilisation, en plus des incidents d'installation.)

 **REMARQUE:** Les chemins indiqués ici supposent que C: est votre lecteur racine. Remplacez **C:** par la lettre de votre lecteur racine.



## Fichiers de référence Linux

Vous pouvez utiliser les fichiers journaux et fichiers d'erreurs suivants pour dépanner l'installation d'EKM 3.0 sous Linux :

- **/root/IA-TipInstall\_\*.log**
- **/tklm\_install.stderr** (fichier journal d'erreurs standard)
- **/tklmV2properties/\*.log**
- **/opt/dell/ekm/products/tklm/logs/audit/tklm\_audit.log**



# Désinstallation manuelle d'EKM 3.0

Pour désinstaller EKM 3.0, commencez par utiliser la procédure de désinstallation automatique. Reportez-vous à « [Désinstallation d'EKM 3.0](#) ». Si la désinstallation automatique échoue, désinstallez EKM 3.0 manuellement.

## Désinstallation manuelle d'EKM 3.0 sous Windows

Si vous réinstallez EKM 3.0 et que l'installation échoue en raison d'une désinstallation incomplète, effectuez la désinstallation manuellement. Si l'un des éléments cités est déjà désinstallé, sautez l'étape correspondante.

-  **REMARQUE:** Si vous avez la possibilité de réinstaller le système d'exploitation de votre serveur, Dell vous recommande de le faire, puis d'installer EKM 3.0.
  -  **REMARQUE:** Les chemins indiqués dans cette procédure correspondent à Windows Server 2008. Sous Windows Server 2003 R2 avec Service Pack 2, vous devez, si la procédure l'exige, accéder à **Démarrer** → **Panneau de configuration** → **Ajouter ou supprimer des programmes**.
1. Accédez à **Démarrer** → **Panneau de configuration** → **Programmes (ou Programmes et fonctionnalités)** → **Désinstaller un programme**. Désinstallez IBM DB2 (DB2 Workgroup Server Edition - DB2TKLMV2).
  2. Accédez à **Démarrer** → **Panneau de configuration** → **Programmes (ou Programmes et fonctionnalités)** → **Désinstaller un programme**.
  3. Cliquez sur **EKM**.
  4. Cliquez sur **Désinstaller/Modifier**.  
L'Assistant Désinstallation d'EKM 3.0 s'affiche.
  5. Suivez les instructions de l'Assistant Désinstallation.  
Une fois EKM 3.0 désinstallé, le système redémarre automatiquement.
  6. Accédez à **Démarrer** → **Panneau de configuration** → **Programmes** → **Désinstaller un programme**. Désinstallez **IBM Update Installer for WebSphere software V7.0**.
  7. Exécutez l'Éditeur du Registre Windows (Regedit). Accédez à l'entrée **HKEY\_CURRENT\_USER** → **Software** → **IBM** → **DB2** → **InstalledCopies**. Supprimez le dossier **DB2TKLMV2**.
-  **PRÉCAUTION:** Soyez prudent lorsque vous modifiez le registre. Une modification inappropriée peut rendre votre système instable.
8. Dans l'Explorateur Windows, accédez à **<root>:\Dell**, si ce dossier existe (par exemple, **C:\Dell**). Supprimez le dossier **EKM** (s'il existe) et tous ses sous-dossiers (**<root>:\Dell\EKM**).
  9. Sur le lecteur root (par exemple, **C:\**), supprimez le dossier **tklmV2properties** (**<root>:\tklmV2properties**).
  10. Sur le lecteur root, supprimez le dossier **tklmbarchive**. (**<root>:\tklmbarchive**).
  11. Sur le lecteur root, supprimez le dossier portant le nom de l'utilisateur DB2.
  12. Sur le lecteur root, supprimez le fichier **tklm\_install.stderr** (**<root>:\tklm\_install.stderr**).
  13. Dans l'Explorateur Windows, accédez à **<root>:\Program Files (x86)\dell**. Supprimez le répertoire d'installation de DB2 (**<root>:\Program Files (x86)\dell\db2dkm**).
-  **REMARQUE:** Pour cette étape et les trois suivantes, si vous utilisez un système d'exploitation 32 bits, remplacez le chemin « Program Files (x86) » par « Program Files ».
14. Dans l'Explorateur Windows, accédez à **<root>:\Program Files (x86)\ibm**. Supprimez le dossier **Common** (**<root>:\Program Files (x86)\ibm\Common**).
  15. Dans l'Explorateur Windows, accédez à **<root>:\Program Files (x86)\ibm**. Supprimez le dossier **gsk8** (**<root>:\Program Files (x86)\ibm\gsk8**).

16. Accédez à **Démarrer** → **Outils d'administration** → **Gestion de l'ordinateur**. Dans le volet de gauche, accédez à **Utilisateurs et groupes locaux** → **Utilisateurs**. Dans le volet de droite, supprimez le ou les comptes d'administrateur DB2.
17. Accédez à **Démarrer** → **Outils d'administration** → **Gestion de l'ordinateur**. Dans le volet de gauche, accédez à **Utilisateurs et groupes locaux** → **Groupes**. Dans le volet de droite, supprimez les groupes d'administrateurs DB2 (**DB2ADMINS** et **DB2USERS**).
18. Dans l'Explorateur Windows, accédez à **<root>:\Users**. Supprimez le dossier portant le nom de l'utilisateur DB2.
19. Dans l'Explorateur Windows, accédez à **<root>:\Users\Administrator**. Supprimez le fichier texte **IA-TIPInstall-xx log**.
20. Arrêtez les services Windows EKM 3.0 suivants s'ils sont installés et supprimez-les. Pour ce faire, utilisez les commandes suivantes dans une invite de commandes sur le lecteur root (par exemple, **C:**). Si le service concerné est déjà arrêté, vous pouvez sauter l'étape d'arrêt (commande stop).

 **REMARQUE:** Si nécessaire, vous pouvez arrêter et supprimer ces services depuis l'utilitaire Services de Windows.

```
sc stop "DBTKLM20" sc delete "DBTKLM20" sc stop "<nom d'utilisateur DB2>"
sc delete "<nom d'utilisateur DB2>" sc stop "DB2GOVERNOR_DB2TKLMV2" sc
delete "DB2GOVERNOR_DB2TKLMV2" sc stop "DB2LICD_DB2TKLMV2" sc delete
"DB2LICD_DB2TKLMV2" sc stop "DB2MGMTSVC_DB2TKLMV2" sc delete
"DB2MGMTSVC_DB2TKLMV2" sc stop "DB2REMO TECMD_DB2TKLMV2" sc delete
"DB2REMO TECMD_DB2TKLMV2" sc stop "DB2DAS00" sc delete "DB2DAS00"
```

 **REMARQUE:** Le service suivant est affiché en tant que **Tivoli Integrated Portal - TIPProfile\_Port\_<numéro de port DB2>** dans l'utilitaire Services de Windows.

```
sc stop "IBM WAS61Service - TIPProfile_Port_<numéro de port DB2>" sc delete
"IBM WAS61Service - TIPProfile_Port_<numéro de port DB2>"
```

 **REMARQUE:** Le numéro de port DB2 par défaut est 16310.

21. Ouvrez une invite de commandes sur le lecteur root (par exemple, **C:**) et utilisez les commandes suivantes :
 

```
reg delete HKEY_LOCAL_MACHINE\software\classes\installer\Products
\907E425044C581845A83FCBED0CD5771 /f reg delete HKEY_LOCAL_MACHINE\software
\classes\installer\Features\907E425044C581845A83FCBED0CD5771 /f
```
22. Redémarrez le système.
23. Pour réinstaller EKM 3.0, reportez-vous à « [Exécution de la procédure d'installation d'EKM 3.0](#) ».

## Désinstallation manuelle d'EKM 3.0 sous Linux

Si vous réinstallez EKM 3.0 et que l'installation échoue en raison d'une désinstallation incomplète, effectuez la désinstallation manuellement. Si l'un des éléments cités est déjà désinstallé, sautez l'étape correspondante.

 **REMARQUE:** Si vous avez la possibilité de réinstaller le système d'exploitation de votre serveur, Dell vous recommande de le faire, puis d'installer EKM 3.0.

Dans la procédure suivante, remplacez les variables indiquées (*<variable>*) par votre propre chemin d'installation ou nom d'élément.

- *<DB2\_INSTALL\_DIR>* : répertoire sélectionné pour l'installation de la base de données.
- *<DB2\_ADMIN>* : ID de l'administrateur DB2 (par exemple, **ekm\_dell1**).
- *<DB2\_ADMIN\_HOME>* : répertoire de travail de la base de données (également appelé emplacement des données de la base de données).
- *<DB2\_DB\_NAME>* : nom de la base de données.

1. Ouvrez une session de terminal.
2. Supprimez l'instance DB2 à l'aide des commandes suivantes :
 

```
cd /opt/dell/ekm/products/tklm/_uninst ./removeDB2Inst.sh
<DB2_INSTALL_DIR> ./removeDB2Inst.sh <DB2_ADMIN> ./removeDB2Inst.sh
<DB2_ADMIN_HOME> ./removeDB2Inst.sh <DB2_DB_NAME>
```

Par exemple :

```
./removeDB2Inst.sh /opt/dell/db2ekm ./removeDB2Inst.sh /ekm_dell1 ./
removeDB2Inst.sh /home/db2ekm ./removeDB2Inst.sh /db2ekm
```
3. Exécutez l'installation à l'arrière-plan de TKLM avec fichier de réponses, à l'aide des commandes suivantes :
 

```
/opt/dell/ekm/_uninst/TIPInstall/uninstall -i silent -f /opt/dell/ekm/
Uninstall_EKM/dkm_uninstall_response.txt
```
4. Supprimez les fichiers journaux à l'aide des commandes suivantes :
 

```
rm -rf /tklmV2properties cd /opt/dell/ekm/ rm tklm_install.stderr rm IA-
TIPIn*.log rm EKM_Install*.log
```
5. Supprimez l'ID d'utilisateur DB2 du système à l'aide de la commande suivante :
 

```
userdel -r $DB2_ADMIN$
```

Par exemple :

```
userdel -r ekm_dell1
```
6. Supprimez DB2 du système à l'aide des commandes suivantes :
 

```
cd /opt/dell/ekm/install ./db2_deinstall -a
```
7. Supprimez le répertoire parent utilisé pour la fusion/migration d'EKM 2.X et l'installation d'EKM 3.0.
 

```
rm -rf /opt/dell/ekm
```
8. Redémarrez la machine.
9. Pour réinstaller EKM 3.0, reportez-vous à « [Exécution de la procédure d'installation d'EKM 3.0](#) ».

## Réinstallation d'EKM 3.0

Pour réinstaller EKM 3.0, procédez comme suit :

1. Désinstallez EKM 3.0 en suivant la procédure appropriée. Reportez-vous à [Uninstalling EKM 3.0](#) (Désinstallation d'EKM 3.0).
-  **REMARQUE:** Si la machine n'a pas redémarré automatiquement lorsque vous avez désinstallé EKM 3.0, redémarrez-la.
2. Réinstallez EKM 3.0 en appliquant la procédure d'installation. Reportez-vous à [Performing the EKM 3.0 Installation Procedure](#) (Exécution de la procédure d'installation d'EKM 3.0).
-  **REMARQUE:** Si vous avez enregistré un profil d'installation pendant l'installation d'origine d'EKM 3.0, vous pouvez l'utiliser pour réinstaller EKM 3.0. Toutefois, si vous utilisez une configuration avec serveurs principal et secondaire, et si le profil d'installation appartient au serveur EKM 3.0 secondaire, ne l'utilisez pas pour réinstaller EKM 3.0 sur le serveur principal.

## Questions fréquemment posées

**Puis-je installer EKM 3.0 sous un système d'exploitation qui n'est pas répertorié dans le chapitre « [Configuration matérielle et logicielle requise](#) » ?**

Non. EKM 3.0 prend uniquement en charge les systèmes d'exploitation, versions, éditions, niveaux de Service Pack et versions (32 ou 64 bits) répertoriés sous « [Configuration matérielle et logicielle requise](#) ».

### Puis-je copier les fichiers du programme d'installation d'EKM 3.0 sur le disque dur de mon système et effectuer l'installation depuis le système local ?

Non. EKM 3.0 prend uniquement en charge l'installation depuis le support EKM 3.0. Reportez-vous à « [Installation d'EKM 3.0](#) ».

### Pendant l'installation d'EKM 3.0, que faire si un message d'erreur me signale que l'installation en arrière-plan a échoué ?

Reportez-vous au fichier `tklm_install.stderr` (fichier journal d'erreur standard) pour en savoir plus. *Sous Windows*, ce fichier se trouve dans `<racine>\tklm_install.stderr`. *Sous Linux*, vous le trouverez dans `/tklm_install.stderr`. Si un code d'erreur code figure dans ce fichier, reportez-vous à « [Codes d'erreur](#) ».

Une fois que vous avez corrigé l'erreur signalée par le code d'erreur, effectuez une désinstallation manuelle. Reportez-vous à « [Désinstallation manuelle d'EKM 3.0 sous Windows](#) ». Redémarrez le système après avoir désinstallé manuellement EKM 3.0, puis réinstallez EKM 3.0.

### Pendant la réinstallation d'EKM 3.0, que faire si un message d'erreur me signale que l'installation a échoué ?

Effectuez une désinstallation manuelle. Reportez-vous à « [Désinstallation manuelle d'EKM 3.0 sous Windows](#) ». Redémarrez le système après avoir désinstallé manuellement EKM 3.0, puis réinstallez EKM 3.0.

### Pendant l'installation d'EKM 3.0, que faire si un message d'erreur me signale que Windows Server 2003 R2 SP2 n'est pas installé ?

Pour connaître la liste des systèmes d'exploitation pris en charge, reportez-vous à « [Configuration matérielle et logicielle requise](#) ». Après avoir installé le deuxième CD de Windows Server 2003 R2, redémarrez le système avant d'installer EKM 3.0.



**PRÉCAUTION:** Cette opération écrase les données figurant sur le lecteur de bande. Une fois écrasées, ces données ne sont plus accessibles.

### Comment réutiliser un support crypté en tant que support non crypté ou en tant que support crypté avec une autre clé ?

La réutilisation d'un support précédemment crypté nécessite une configuration EKM 3.0 opérationnelle contenant les clés des bandes à réutiliser, ainsi qu'un PowerVault TL2000 ou TL4000.

Vous ne pouvez pas écraser de bandes de cette façon avec PowerVault ML6000. Vous pouvez migrer des bandes de ML6000 vers TL2000 ou TL4000 dans ce but. Vous devez alors faire pointer le TL2000 ou le TL4000 vers le serveur EKM 3.0 approprié.

Pour réutiliser un support précédemment crypté, procédez comme suit :

1. Vérifiez que le serveur EKM 3.0 est en cours d'exécution et correctement configuré.
2. Connectez-vous à l'interface GUI RMU du TL2000/TL4000 (vous devez vous connecter avec administrateur/service).
3. Accédez à la section **Configure Library** (Configurer la bibliothèque).
4. Accédez à **Encryption** (Cryptage).
5. Modifiez le paramètre **Encryption Policy** (Stratégie de cryptage) afin d'utiliser **Internal Label – Selective Encryption** (Étiquette interne – Cryptage sélectif).
6. Soumettez une tâche d'écriture (exemple : effacement rapide, effacement long ou sauvegarde) sur le support à réutiliser.

Pour vérifier que le cryptage a été écrasé, procédez comme suit :

1. Connectez-vous à l'interface GUI RMU du TL2000/TL4000.
2. Accédez à **Monitor Library** (Surveiller la bibliothèque), puis à **Inventory** (Inventaire).
3. Cliquez sur le menu déroulant correspondant au magasin approprié.
4. Vérifiez que la section **Comment** (Commentaire) indique **Not Encrypted** (Non crypté).

Vous ne pouvez supprimer ou désinstaller EKM 3.0 qu'après avoir écrasé tous les supports voulus. Dell vous recommande de sauvegarder les fichiers critiques de l'interface GUI d'EKM 3.0 et de stocker cette sauvegarde sur une source externe, comme un lecteur amovible. Cela vous permet de restaurer EKM 3.0 si vous devez écraser des bandes supplémentaires.

### **J'ai des difficultés avec ma nouvelle installation EKM 3.0 et je dois réinstaller le produit. Comment déterminer si EKM 3.0 a déjà fourni des clés ?**

1. Ouvrez une invite de commandes et accédez au répertoire du journal d'audit.  
*Sous Windows*, le journal d'audit se trouve dans `<root>\Dell\EKM\products\tklm\logs\audit\tklm_audit.txt`.  
*Sous Linux*, le journal d'audit est stocké dans : `/opt/dell/ekm/products/tklm/logs/audit/tklm_audit.log`.
2. Copiez le journal d'audit actuel vers un dossier temporaire pour pouvoir l'ouvrir. En effet, il est actif et vous ne pouvez pas l'ouvrir pendant sa mise à jour.
3. Ouvrez la copie temporaire dans un éditeur de texte (comme WordPad). Recherchez le **Drive Serial Number** (numéro de série du lecteur). Si cette entrée comporte une valeur, une clé a été fournie. Si l'entrée **volser** est vide, il s'agit du résultat d'un diagnostic de chemin de clé et vous devez rechercher dans le fichier les autres entrées associées au numéro de série du lecteur, pour être sûr du résultat.

 **PRÉCAUTION: Si des clés ont été fournies, vous devez décrypter les données sur le support concerné avant de désinstaller EKM 3.0.**

### **Quel est l'impact sur mon application de sauvegarde lorsque je configure ma bandothèque pour un cryptage géré par la bibliothèque ?**

Si vous avez activé le cryptage géré par la bibliothèque dans la bandothèque et configuré les partitions avec cryptage, les paramètres du ou des lecteurs figurant dans ces partitions sont modifiés. Vous devez arrêter et redémarrer les services d'application de sauvegarde après la configuration des partitions avec cryptage afin de garantir que l'application de sauvegarde reconnaît le paramètre de cryptage du ou des lecteurs.

 **REMARQUE:** L'application de sauvegarde sur bande n'indique pas que le cryptage est **enabled** (activé) si vous utilisez le cryptage géré par la bibliothèque. La bandothèque affiche les partitions comme étant **encryption enabled** (avec cryptage). Le cryptage géré par la bibliothèque est transparent pour l'application de sauvegarde sur bande, qui affiche uniquement la mention de cryptage **enabled** (activé) si cette application elle-même (Symantec, CommVault, etc.) fournit les clés de cryptage aux lecteurs.

### **Comment EKM 3.0 gère-t-il l'ajout de nouveaux lecteurs ou le remplacement d'un lecteur défectueux ?**

Vous pouvez ajouter des lecteurs nouveaux ou de remplacement au serveur EKM 3.0 manuellement ou par détection automatique. Pour ajouter des lecteurs par détection automatique, reportez-vous à « [Ajout d'un périphérique à un groupe de périphériques](#) ».

Dell vous recommande d'utiliser la détection automatique car il faut entrer le numéro de série du lecteur, sur 12 caractères (numéro de série sur 10 chiffres, précédé de deux zéros) pour ajouter le lecteur manuellement. Si vous êtes soucieux de la sécurité, activez la détection automatique, et exécutez des sauvegardes de test ou des diagnostics de chemin de clés dans la bandothèque pour ajouter les lecteurs nécessaires à la table des lecteurs. Vous pouvez ensuite désactiver la découverte automatique pour éviter que les nouveaux lecteurs obtiennent des clés. Tant qu'EKM 3.0 peut authentifier la signature numérique attribuée au lecteur en usine, il accepte la demande de clés. Les clés forment des groupes dans le magasin de clés et vous pouvez associer des groupes de clés aux nouveaux lecteurs/lecteurs de remplacement après leur ajout.

 **REMARQUE:** Pour ajouter manuellement un périphérique, reportez-vous à la documentation TKLM. Pour savoir comment accéder à cette documentation, consultez la section « Documentation et informations de référence » du fichier **ReadThisFirst.txt** sur le support d'installation d'EKM 3.0.

### **Comment EKM 3.0 gère-t-il l'ajout d'une nouvelle bandothèque ou le remplacement d'une bandothèque défectueuse ?**

Avec le cryptage géré par la bibliothèque, la bandothèque n'est qu'un proxy. Vous pouvez ajouter ou remplacer des bandothèques, et fournir des clés, tant qu'EKM 3.0 peut authentifier la signature numérique du lecteur. La bandothèque

de remplacement devra posséder une licence de cryptage géré par la bibliothèque et être configurée pour utilisation avec le système EKM 3.0 existant.

#### **Quel est l'impact du cryptage sur la compression et inversement ?**

Les données sont compressées avant leur cryptage car les données cryptées sont généralement incompressibles. Par conséquent, la compression n'a aucun effet sur le cryptage et inversement.

#### **Le cryptage a-t-il un impact sur les performances ?**

Le cryptage peut avoir un très léger impact sur les performances, mais cela ne devrait pas augmenter la fenêtre de sauvegarde.

#### **Comment demander et utiliser un certificat tiers ?**

Créez une demande de certificat dans EKM 3.0. Envoyez-la à l'autorité de certification (CA). Vous pouvez importer le certificat renvoyé par l'autorité de certification dans EKM 3.0 et l'utiliser pour protéger les données d'un périphérique où le cryptage est activé ou pour la communication SSL. Consultez la documentation TKLM pour en savoir plus sur la génération d'une demande de certificat, l'importation du certificat reçu et son utilisation pour le cryptage. Pour en savoir plus sur l'accès à la documentation TKLM, consultez la section « Documentation et informations de référence » du fichier **ReadThisFirst.txt** sur le support d'installation d'EKM 3.0.

## **Problèmes connus et solutions**

### **Problème : je ne peux pas créer de sauvegarde.**

#### **Description**

Utilisez Internet Explorer pour tenter de créer une sauvegarde du magasin de clés. Si vous spécifiez un emplacement de sauvegarde qui n'existe pas, la sauvegarde n'est pas créée.

#### **Solution :**

Effectuez l'une des opérations suivantes. Si l'action choisie ne fonctionne pas, appliquez la solution suivante :

- Activez JavaScript dans votre navigateur. Si vous utilisez Internet Explorer V8, activez le mode Compatibility View (Affichage de compatibilité).
- Utilisez un autre navigateur pris en charge. Reportez-vous à [Hardware and Software Requirements](#) (Configuration matérielle et logicielle requise) pour en savoir plus.
- Spécifiez un dossier qui existe. Si vous souhaitez spécifier un autre dossier, créez-le avant de lancer la sauvegarde.

### **Problème : plusieurs sauvegardes sont créées simultanément.**

#### **Description**

Lorsque vous tentez de sauvegarder le magasin de clés, plusieurs fichiers de sauvegarde sont créés simultanément. Ce dysfonctionnement est très rare.

#### **Solution :**

Tous les fichiers de sauvegarde ont le même contenu. Vous pouvez utiliser le fichier de votre choix pour l'opération de restauration.

### **Problème : je dois entrer deux fois mes informations de connexion.**

#### **Description**

Après l'expiration du délai d'EKM 3.0 (après environ 30 minutes d'inactivité), la première tentative de reconnexion à EKM 3.0 est rejetée et vous devez vous connecter une deuxième fois.

#### **Solution :**

Entrez vos informations de connexion à EKM 3.0 les deux fois.

**Problème : le volet de droite est partiellement masqué par le volet de navigation.**

**Description**

Vous utilisez Internet Explorer. Vous accédez à l'écran **Gestion des clés et des périphériques** d'EKM 3.0. Vous sélectionnez le groupe de clés ou un lecteur de bandes. Le volet de droite est partiellement masqué par le volet de navigation.

**Solution :**

Effectuez l'une des opérations suivantes :

- Actualisez l'écran.
- Agrandissez le navigateur.
- Utilisez un autre navigateur pris en charge. Reportez-vous à [Hardware and Software Requirements](#) (Configuration matérielle et logicielle requise) pour en savoir plus.

**Problème : le message « Erreur de certificat » apparaît en haut du navigateur.**

**Description**

Vous utilisez Internet Explorer 8 en mode Affichage de compatibilité. Vous importez un certificat d'autorité de certification avec succès, mais le message **Certificate Error** (Erreur de certificat) apparaît en haut de l'écran, près de la barre d'URL.

**Solution :**

Effectuez l'une des opérations suivantes :

- Ignorez cette erreur, elle n'a pas d'impact sur les performances d'EKM 3.0.
- Utilisez un autre navigateur pris en charge (par exemple, Internet Explorer 6.X ou Firefox). Reportez-vous à [Hardware and Software Requirements](#).

**Problème : je ne peux pas trier les informations des tables.**

**Description**

L'utilisation des champs Filter (Filtrer), en haut des tables des écrans **Administer Server Certificates** (Administrer les certificats de serveur), **Backup and Restore** (Sauvegarde et Restauration) et **Credential Store** (Banque de références) ne trie pas les éléments des tables.

**Solution :**

Cliquez sur la ligne d'en-tête de chaque colonne pour trier les éléments.

**Problème : je ne peux pas entrer la description de la sauvegarde que j'ai créée.**

**Description**

Lorsque vous utilisez Firefox sous Windows, vous générez une sauvegarde. Vous ne pouvez pas entrer la description de cette sauvegarde ; la description est utilisée par défaut.

**Solution :**

Utilisez une version prise en charge d'Internet Explorer. Reportez-vous à [Hardware and Software Requirements](#) pour en savoir plus.

**Problème : certaines actions effectuées dans l'interface GUI d'EKM 3.0 provoquent des erreurs de script, affichées dans des fenêtres contextuelles dans le navigateur.**

**Description**

Des erreurs de script s'affichent dans le navigateur et l'action demandée n'est pas exécutée.

**Solution :**

Effectuez l'une des opérations suivantes. Si l'action choisie ne fonctionne pas, appliquez-en une autre :

- Activez JavaScript dans votre navigateur. Si vous utilisez Internet Explorer V8, activez le mode Affichage de compatibilité.



**REMARQUE:** Vous devez activer le mode Affichage de compatibilité après vous être connecté à EKM 3.0.

- Utilisez un autre navigateur pris en charge. Reportez-vous à [Hardware and Software Requirements](#) pour en savoir plus.

**Problème : pendant la désinstallation, la barre de progression n'affiche pas l'avancement réel.**

#### Description

La barre de progression de la désinstallation n'affiche pas l'avancement réel. Elle passe directement à 30 % au début de la désinstallation et y reste pendant toute la durée de l'opération. À la fin du traitement, elle saute à 100 %.

#### Solution :

Il s'agit d'un problème connu. Cela n'indique aucun dysfonctionnement dans la désinstallation.



**PRÉCAUTION:** Ne redémarrez pas le système et ne quittez pas le programme de désinstallation.

**Problème : les paramètres de l'écran Key and Device Management (Gestion des clés et des périphériques) ne sont pas appliqués.**

#### Description

Dans l'écran Gestion des clés et des périphériques, lorsque je modifie les paramètres de communication avec les lecteurs, le changement n'est pas appliqué.

#### Solution :

Après modification du paramètre de communication des lecteurs, arrêtez et redémarrez le serveur EKM 3.0. Les modifications seront appliquées. Pour en savoir plus, reportez-vous à [Starting and Stopping the EKM 3.0 Server in Windows démarrage et arrêt du serveur EKM 3.0 sous Windows](#) (Démarrage et arrêt du serveur EKM 3.0 sous Windows) ou à [Starting and Stopping the EKM 3.0 Server in Linux](#) (Démarrage et arrêt du serveur EKM 3.0 sous Linux).

**Problème : sur un serveur Windows Server 2008, après l'installation d'EKM 3.0, la barre d'état système affiche une icône verte associée à la procédure d'installation.**

#### Description

La barre d'état système affiche une icône verte.

#### Solution :

Il s'agit d'un problème connu, qui n'affecte ni le fonctionnement, ni la fiabilité d'EKM 3.0. Lorsque vous vous déconnectez du système et que vous vous reconnectez, l'icône n'est plus visible.

**Problème : lors de la configuration de l'installation d'EKM 3.0, certains champs affichent zéro (0).**

#### Description

Lors de la configuration de l'installation d'EKM 3.0, certains champs affichent zéro (0). Cela se produit lorsque vous utilisez un profil d'installation lors de l'installation d'EKM 3.0, et que ce profil d'installation est non valide ou comporte des champs manquants.

#### Solution :

Vérifiez que vous utilisez un profil d'installation valide.



**REMARQUE:** Si vous remplissez manuellement les champs, vous devez garantir que les données correspondent exactement à celles de l'installation d'origine. Sinon, le deuxième serveur ne peut pas être utilisé pour la sauvegarde du premier serveur.

**Problème : lors de la création d'une sauvegarde, le message d'erreur « software exception » (« Exception logicielle ») s'affiche.**

#### Description

Lorsque vous créez une sauvegarde, un message d'erreur vous signale une exception logicielle.

**Solution :**

EKM 3.0 comporte une limitation connue concernant les serveurs dotés de 24 UC ou plus. Vous devez installer le tout dernier correctif (fixpack) universel pour DB2 afin de résoudre le problème.



**REMARQUE:** Pour en savoir plus, consultez les Notes de mise à jour, à l'adresse suivante : [support.dell.com/manuals](http://support.dell.com/manuals). Accédez à **Software** → **Systems Management** → **Dell Encryption Key Manager** (Logiciel > Systems Management > Dell Encryption Key Manager).

**Problème : je ne peux pas ajouter de rôle à un utilisateur nouvellement créé si j'utilise Internet Explorer V8.**

**Description**

Lorsque vous vous connectez en tant qu'administrateur EKM 3.0, que vous créez un nouvel utilisateur, puis que vous tentez d'ajouter un rôle à cet utilisateur, une erreur JavaScript apparaît et le rôle n'est pas ajouté.

**Solution :**

Créez d'abord l'utilisateur, puis ajoutez-lui des rôles dans l'écran **Administrative User Roles** (Rôles des utilisateurs administratifs). Pour accéder à cet écran, ouvrez le volet de navigation et accédez à **Users and Groups** → **Administrative User Roles** (Utilisateurs et groupes > Rôles des utilisateurs administratifs). Vous pouvez également résoudre le problème en utilisant une version prise en charge de Firefox.

**Problème : lors de la désinstallation d'EKM 3.0, l'erreur Java « stack overflow exception » (« exception de dépassement de pile ») apparaît.**

**Description**

Une erreur Java apparaît lorsque vous désinstallez EKM 3.0.

**Solution :**

Désinstallez manuellement EKM 3.0. Reportez-vous à [Manually Uninstalling EKM 3.0](#) (Désinstallation manuelle d'EKM 3.0) pour en savoir plus.

**Problème : le processus de désinstallation d'EKM 3.0 s'exécute pendant plusieurs heures sans s'achever.**

**Description**

Lorsque vous tentez de désinstaller EKM 3.0, l'opération ne s'achève pas.

**Solution :**

Désinstallez manuellement EKM 3.0. Reportez-vous à [Manually Uninstalling EKM 3.0](#) (Désinstallation manuelle d'EKM 3.0) pour en savoir plus.

## Installation de la bibliothèque compat-libstdc++

Vous devez installer la bibliothèque **compat-libstdc++-33-3.2.3-61** ou version ultérieure avant d'installer EKM 3.0 sous Linux.

Si l'erreur suivante s'affiche pendant l'installation d'EKM 3.0 sous Linux, vous devez installer **compat-libstdc++** :

« Le paquet compat-libstdc++ n'est pas installé sur votre système d'exploitation. »

Pour installer **compat-libstdc++** :

1. Ouvrez une session de terminal, accédez au fichier RPM **compat-libstdc++** stocké dans le dossier **EKMPREQLIBS** du support d'installation d'EKM 3.0 en émettant la commande suivante :

```
cd /<chemin_du_DVD_d'installation_EKM_3.0>/EKMPREQLIBS
```

2. Installez **compat-libstdc++** en émettant la commande suivante :

```
rpm -ivh compat-libstdc++*.rpm
```

 **REMARQUE:** Si un message d'erreur apparaît, indiquant que le RPM **compat-libstdc++** que vous tentez d'installer est en conflit avec le fichier **libstdc++-33** déjà installé, procédez comme suit :

a. Utilisez la commande suivante :

```
rpm -e libstdc++-33
```

b. Utilisez la commande suivante :

```
rpm -ivh compat-libstdc++*.rpm
```