Dell Data Protection

Guide de récupération pour le cryptage de fichier/dossier, l'accélérateur de cryptage matériel, les lecteurs à auto-cryptage, et la clé universelle

v8.10

2016-07

Table des matières

1

Mise en route

Cette section détaille les éléments nécessaires pour créer l'environnement de récupération.

- Téléchargez une copie du logiciel d'environnement de récupération, stocké dans le dossier Kit de récupération Windows sur le support d'installation de Dell Data Protection.
- CD-R, DVD-R ou support USB formaté
  - Pour en savoir plus sur la façon de graver un CD ou un DVD, consultez la section Annexe A : Gravage de l'environnement de récupération
  - Pour en savoir plus sur l'utilisation d'un lecteur USB, consultez la section Annexe A : Gravage de l'environnement de récupération.
- Ensemble de récupération pour le périphérique en échec
  - Les instructions suivantes détaillent l'obtention d'un ensemble de récupération auprès de votre serveur Dell Data Protection, dans le cas des clients gérés à distance.
  - Dans le cas des clients gérés en local, le package d'ensemble de récupération est créé lors de l'installation, soit sur un lecteur réseau partagé, soit sur un support externe. Repérez ce package avant de continuer.

2

Récupération de cryptage de fichier/dossier

À l'aide de la récupération FFE (File/Folder Encryption, Cryptage de fichier/dossier), vous pouvez récupérer l'accès aux éléments suivants :

- Un ordinateur qui ne démarre pas et qui vous invite à procéder à une récupération de SDE.
- Un ordinateur sur lequel vous ne pouvez pas accéder aux données cryptées ni modifier des règles.
- Un serveur exécutant Dell Data Protection | Server Encryption qui répond à l'une des conditions précédentes.
- Un ordinateur dont la carte HCA (accélérateur de cryptage matériel) ou la carte mère/TPM doivent être remplacées.

Configuration requise pour la récupération

Pour la récupération du FFE, vous aurez besoin des éléments suivants :

- Kit de récupération Windows pour créer un disque d'amorçage spécial ; le kit contient des fichiers qui serviront à créer une image Windows PE (WinPE) et à la personnaliser à l'aide des pilotes et des logiciels Dell Data Protection. Le kit est situé dans le dossier Kit de récupération Windows dans le support d'installation de Dell Data Protection.

Présentation du processus de récupération

Pour récupérer un système défaillant :

1. Créez le fichier ISO de récupération puis gravez-le sur un CD/DVD ou créez un USB amorçable. Voir Annexe A : Gravage de l'environnement de récupération.
2. Obtention du fichier de récupération.
3. Procéder à la récupération.

Procéder à la récupération de FFE

Suivez ces étapes pour effectuer une récupération de FFE.

Obtention du fichier de récupération : ordinateur géré à distance

Pour télécharger le fichier **LSARecovery_<nommachine_domaine.com>.exe** :

1. Ouvrez la Console de gestion à distance et sélectionnez **Gestion > Récupérer le point final** dans le volet de gauche.
2. Dans le champ Nom d'hôte, entrez le nom de domaine entièrement qualifié de l'hôte du point final et cliquez sur **Rechercher**.
3. Dans la fenêtre Récupération avancée, entrez un mot de passe de récupération et cliquez sur **Télécharger**.

REMARQUE : Vous devez vous souvenir de ce mot de passe pour accéder aux clés de récupération.

4. Copiez le fichier **LSARecovery_<nommachine_domaine.com>.exe** à un emplacement accessible lors de l'amorçage du serveur dans l'environnement WinPE.

Obtention du fichier de récupération : ordinateur géré localement

Pour obtenir le fichier de récupération Personal Edition :

1. Localisez le fichier de récupération appelé **LSARecovery_<nomsystème>.exe**. Ce fichier a été stocké sur un disque réseau ou un périphérique de stockage amovible lorsque vous avez utilisé l'Assistant Configuration pendant l'installation de Personal Edition.
2. Copiez **LSARecovery_[nomhôte].exe** sur l'ordinateur cible (celui sur lequel récupérer les données).

Procéder à la récupération

1. À l'aide du support amorçable créé plus tôt, effectuez un démarrage sur ce support dans un système de récupération ou sur le périphérique qui contient le disque que vous tentez de récupérer. Un environnement WinPE s'ouvre.
2. Entrez **x** et appuyez sur **Entrée** pour ouvrir une invite de commande.
3. Naviguez jusqu'au fichier de récupération et lancez-le.
4. Sélectionnez une option :
   - Mon système ne démarre pas et affiche un message me demandant d'effectuer une récupération de SDE.

     Cela vous permet de reconstruire les contrôles matériels effectués par le client de cryptage lorsque vous amorcez le système dans le système d'exploitation.
   - Mon système ne me permet pas d'accéder à des données cryptées ni de modifier des règles ou est en cours de réinstallation.

     Utilisez cette option si vous devez remplacer la carte HCA (accélérateur de cryptage matériel) ou la carte mère/TPM.
5. Dans la boîte de dialogue Informations de sauvegarde et de récupération, confirmez que les informations sur l'ordinateur client à récupérer sont correctes et cliquez sur **Suivant.**

   Lors de la récupération d'ordinateurs non-Dell, les champs Numéro de série et Numéro d'inventaire sont vides.
6. Dans la boîte de dialogue qui répertorie les volumes de l'ordinateur, sélectionnez tous les lecteurs applicables et cliquez sur **Suivant**.

   Utilisez les combinaisons Maj-clic ou Ctrl-clic pour sélectionner plusieurs lecteurs.

   Si le lecteur sélectionné n'est pas crypté FFE, la récupération échoue.
7. Entrez votre mot de passe de récupération et appuyez sur **Suivant**.

   Avec un client géré à distance, il s'agit du mot de passe fourni dans étape 3 à la section Obtention du fichier de récupération : ordinateur géré à distance.

   Dans Personal Edition, il s'agit du mot de passe d'administrateur de cryptage défini pour le système au moment de la mise en séquestre des clés.
8. Dans la boîte de dialogue Récupération, cliquez sur **Récupérer**. Le processus de récupération démarre.
9. Une fois la récupération terminée, cliquez sur **Terminer**.

REMARQUE : Veillez à bien retirer la clé USB ou le CD/DVD utilisé pour amorcer la machine. Si vous ne le faites pas, vous risquez de redémarrer dans l'environnement de récupération.

10. Après le redémarrage de l'ordinateur, il devrait fonctionner parfaitement. Si le problème persiste, contactez Dell ProSupport.

3

Récupération de l'accélérateur de cryptage matériel

La fonction de récupération de l'accélérateur de cryptage matériel (HCA) de Dell Data Protection, vous pouvez rétablir l'accès aux éléments suivants :

- Les fichiers sur un lecteur crypté HCA : cette méthode décrypte le lecteur à l'aide des clés fournies. Vous pouvez sélectionner le lecteur spécifique à décrypter pendant le processus de récupération.
- Un lecteur crypté HCA après un remplacement de matériel : Cette méthode est utilisée lorsque vous avez dû remplacer la carte d'accélérateur de cryptage matériel (HCA) ou une carte mère/TPM. Vous pouvez exécuter une récupération pour regagner l'accès aux données cryptées sans décrypter le lecteur.

Configuration requise pour la récupération

Pour la récupération HCA, vous aurez besoin des éléments suivants :

- Accès à un fichier ISO d'environnement de récupération
- CD/DVD ou support USB amorçable

Présentation du processus de récupération

Pour récupérer un système défaillant :

1. Créez le fichier ISO de récupération et gravez-le sur un CD/DVD ou créez un USB amorçable. Voir Annexe A : Gravage de l'environnement de récupération.
2. Obtention du fichier de récupération.
3. Procéder à la récupération.

Procéder à la récupération de HCA

Suivez ces étapes pour effectuer une récupération de HCA.

Obtenez le fichier de récupération : Ordinateur géré à distance

Pour télécharger le fichier **LSARecovery_<nommachine_domaine.com>.exe** généré lors de l'installation de Dell Data Protection :

1. Ouvrez la Console de gestion à distance et sélectionnez **Gestion > Récupérer le point final** dans le volet de gauche.
2. Dans le champ Nom d'hôte, entrez le nom de domaine entièrement qualifié de l'hôte du point final et cliquez sur **Rechercher**.
3. Dans la fenêtre Récupération avancée, entrez un mot de passe de récupération et cliquez sur **Télécharger**.

REMARQUE : Vous devez vous souvenir de ce mot de passe pour accéder aux clés de récupération.

Le fichier **LSARecovery_<nommachine_domaine.com>.exe** est téléchargé.

Obtention du fichier de récupération : ordinateur géré localement

Pour obtenir le fichier de récupération Personal Edition :

1. Localisez le fichier de récupération appelé **LSARecovery_<nomsystème>.exe**. Ce fichier a été stocké sur un disque réseau ou un périphérique de stockage amovible lorsque vous avez utilisé l'Assistant Configuration au cours de l'installation de Personal Edition.
2. Copiez **LSARecovery_[nomhôte].exe** sur l'ordinateur cible (celui sur lequel récupérer les données).

Procéder à la récupération

1. À l'aide du support amorçable créé plus tôt, effectuez un démarrage sur ce support dans un système de récupération ou sur le périphérique qui contient le disque que vous tentez de récupérer.

   Un environnement WinPE s'ouvre.
2. Entrez **x** et appuyez sur **Entrée** pour ouvrir une invite de commande.
3. Accédez au fichier de récupération enregistré et lancez-le.
4. Sélectionnez une option :
   - Je veux décrypter le lecteur avec cryptage HCA.
   - Je veux restaurer l'accès au lecteur avec cryptage HCA.
5. Dans la boîte de dialogue Informations de sauvegarde et de récupération, vérifiez que le numéro de service et le numéro d'inventaire sont corrects, puis cliquez sur **Suivant**.
6. Dans la boîte de dialogue qui répertorie les volumes de l'ordinateur, sélectionnez tous les lecteurs applicables et cliquez sur **Suivant**.

   Utilisez les combinaisons Maj-clic ou Ctrl-clic pour sélectionner plusieurs lecteurs.

   Si le lecteur sélectionné n'est pas crypté HCA, la récupération échoue.
7. Entrez votre mot de passe de récupération et appuyez sur **Suivant**.

   Sur un ordinateur géré à distance, il s'agit du mot de passe fourni dans étape 3 dans Obtenez le fichier de récupération : Ordinateur géré à distance.

   Sur un ordinateur géré en local, ce mot de passe est le mot de passe d'administrateur de cryptage défini pour le système dans Personal Edition au moment de la mise en séquestre des clés.
8. Dans la boîte de dialogue Récupération, cliquez sur **Récupérer**. Le processus de récupération démarre.
9. À l'invite, naviguez jusqu'au fichier de récupération enregistré, puis cliquez sur **OK**.

   Si vous effectuez un décryptage complet, la boîte de dialogue suivante affiche l'état. Ce processus peut être assez long.
10. Lorsqu'un message s'affiche pour indiquer que la récupération a réussi, cliquez sur **Terminer**. L'ordinateur redémarre.

Après le redémarrage de l'ordinateur, il devrait fonctionner parfaitement. Si le problème persiste, contactez Dell ProSupport.

4

Récupération de lecteur à auto-cryptage (SED)

Avec la récupération de SED, vous pouvez récupérer l'accès aux fichiers situés sur un SED par les méthodes suivantes :

- Effectuer un déverrouillage ponctuel du lecteur afin de contourner et supprimer l'authentification avant démarrage (PBA).
  - Avec un client SED géré à distance, la PBA peut être réactivée ultérieurement via la console de gestion à distance.
  - Avec un client SED géré localement, la PBA peut être activée via la console administrateur de Security Tools.
- Déverrouiller, puis supprimer définitivement la PBA du lecteur. L'authentification unique ne fonctionnera pas en l'absence de PBA.
  - Avec un client SED géré à distance, la suppression de la PBA vous obligera à désactiver le produit à partir de la console de gestion à distance s'il est nécessaire de réactiver la PBA à l'avenir.
  - Avec un client SED géré localement, la suppression de la PBA vous obligera à désactiver le produit à l'intérieur du SE s'il est nécessaire de réactiver la PBA à l'avenir.

Configuration requise pour la récupération

Pour la récupération de SED, vous aurez besoin des éléments suivants :

- Accès au fichier ISO de l'environnement de récupération
- CD/DVD ou support USB amorçable

Présentation du processus de récupération

Pour récupérer un système défaillant :

1. Créez le fichier ISO de récupération puis gravez-le sur un CD/DVD ou créez un USB amorçable. Voir Annexe A : Gravage de l'environnement de récupération.
2. Obtenir le fichier de récupération.
3. Procéder à la récupération.

Procéder à la récupération d'un SED

Suivre ces étapes pour effectuer une récupération de SED.

Obtention du fichier de récupération : Client SED géré à distance

1 Obtention du fichier de récupération.

Le fichier de récupération peut être téléchargé à partir de la console de gestion à distance. Pour télécharger le fichier *<nomhôte>-sed-recovery.dat* généré lors de l'installation d'Enterprise Edition :

- **a** Ouvrez la Console de gestion à distance et sélectionnez **Gestion > Récupérer des données**, puis sélectionnez l'onglet **SED**.
- **b** Dans l'écran Récupérer des données, dans le champ Nom d'hôte, entrez le nom de domaine entièrement qualifié du point final, puis cliquez sur **Rechercher**.
- **c** Dans le champ SED, sélectionnez une option.
- **d** Cliquez sur **Créer un fichier de récupération**.

  Le fichier **<nomhôte>-sed-recovery.dat** est téléchargé.

Obtention du fichier de récupération : Client SED géré localement

1 Obtention du fichier de récupération.

Le fichier est généré et est accessible à partir du dossier de sauvegarde que vous avez sélectionné lors de l'installation de Dell Data Protection | Security Tool sur l'ordinateur. Le nom de fichier est *OpalSPkey<nomsystème>.dat*.

Effectuer une récupération

1 À l'aide du support amorçable que vous avez créé, effectuez un amorçage sur ce support dans un système de récupération ou sur le périphérique qui contient le disque que vous tentez de récupérer. Un environnement WinPE s'ouvre avec l'application de récupération.

2 Choisissez l'option 1 et appuyez sur **Entrée**.

3 Sélectionnez **Parcourir**, localisez le fichier de récupération, puis cliquez sur **Ouvrir**.

4 Sélectionnez une option, puis cliquez sur **OK**.

- **Déverrouillage ponctuel du lecteur** : Cette méthode contourne et supprime la PBA. Elle peut être réactivée ultérieurement via la console de gestion à distance (pour un client SED géré à distance) ou la console administrateur de Security Tools (pour un client SED géré localement).
- **Déverrouiller le lecteur et supprimer la PBA** : cette méthode déverrouille, puis supprime définitivement la PBA du lecteur. La suppression de la PBA vous obligera à désactiver le produit à partir de la console de gestion à distance (pour un client SED géré à distance) ou à l'intérieur du SE (pour un client SED géré localement) s'il est nécessaire de réactiver la PBA à l'avenir. L'authentification unique ne fonctionnera pas en l'absence de PBA.

5 La récupération est terminée. Appuyez sur n'importe quelle touche pour revenir au menu.

6 Appuyez sur **r** pour redémarrer l'ordinateur.

REMARQUE : Veillez à bien retirer la clé USB ou le CD/DVD utilisé pour amorcer l'ordinateur. Si vous ne le faites pas, vous risquez de redémarrer dans l'environnement de récupération.

7 Après le redémarrage de l'ordinateur, il devrait fonctionner parfaitement. Si le problème persiste, contactez Dell ProSupport.

5

Récupération de la clé universelle

La clé universelle (General Purpose Key – GPK) est utilisée pour crypter une partie du registre pour les utilisateurs de domaine. Cependant, au cours du processus de démarrage, celle-ci peut, dans de rares cas, être corrompue et ne pas parvenir à desceller. Dans ce cas, les erreurs suivantes s'affichent dans le fichier CMGShield.log sur l'ordinateur client :

```
[12.06.13 07:56:09:622 GeneralPurposeK: 268] GPK - Failure while unsealing data [error = 0xd]
[12.06.13 07:56:09:622 GeneralPurposeK: 631] GPK - Unseal failure
[12.06.13 07:56:09:622 GeneralPurposeK: 970] GPK - Failure to get keys for the registry driver
```

Si la GPK ne parvient pas à desceller, la GPK doit être récupérée en l'extrayant du bundle de récupération téléchargé à partir du serveur.

Récupération de la GPK

Obtention du fichier de récupération

Pour télécharger le fichier **LSARecovery_<nommachine_domaine.com>.exe** généré lors de l'installation de Dell Data Protection :

1. Ouvrez la Console de gestion à distance et sélectionnez **Gestion > Récupérer le point final** dans le volet de gauche.
2. Dans le champ Nom d'hôte, entrez le nom de domaine entièrement qualifié de l'hôte du point final et cliquez sur **Rechercher**.

3 Dans la fenêtre Récupération avancée, entrez un mot de passe de récupération et cliquez sur **Télécharger**.

REMARQUE : Vous devez mémoriser de ce mot de passe pour accéder aux clés de récupération.

Le fichier **LSARecovery_<nommachine_domaine.com>.exe** est téléchargé.

Procéder à la récupération

1 À l'aide du support amorçable créé à l'étape Annexe A : Gravage de l'environnement de récupération, amorcez le système sur ce support dans un système de récupération ou sur le périphérique qui contient le disque que vous tentez de récupérer.

Un environnement WinPE s'ouvre.

2 Entrez **x** et appuyez sur **Entrée** pour ouvrir une invite de commande.

3 Naviguez jusqu'au fichier de récupération et lancez-le.

La boîte de dialogue de diagnostic du client de cryptage s'ouvre et le fichier de récupération est généré en arrière-plan.

4 En réponse à l'invite de commande administrative, exécutez **LSARecovery_<nommachine_domaine.com>.exe –p <motdepasse> -gpk**

Il renvoie le fichier GPKRCVR.txt correspondant à votre ordinateur.

5 Copiez fichier **GPKRCVR.txt** sur la racine du lecteur du système d'exploitation de l'ordinateur.

6 Redémarrez l'ordinateur.

Le fichier GPKRCVR.txt sera consommé par le système d'exploitation et régénérera la GPK sur cet ordinateur.

7 Si vous y êtes invité, redémarrez de nouveau.

6

Récupération des données de lecteur crypté

Si l'ordinateur cible n'est pas amorçable et qu'il n'y a pas de panne matérielle, la récupération des données peut être réalisée sur l'ordinateur amorcé dans un environnement de récupération. Si l'ordinateur cible est amorçable et qu'il a une panne de matériel ou est un périphérique USB, la récupération des données peut être réalisée en démarrant sur un lecteur asservi. Lorsque vous asservissez un lecteur, vous pouvez voir le système de fichiers et parcourir les dossiers. Cependant, si vous tentez d'ouvrir ou de copier un fichier, une erreur *Accès refusé* se produit.

Récupérer des données de lecteur crypté

Pour récupérer des données de lecteur crypté :

1. Pour obtenir le DCID/ID de récupération de l'ordinateur, choisissez une option :
   a. Exécutez WSScan sur un dossier où les données cryptées « Common » sont stockées.
      Le code DCID/ID de récupération sur huit caractères s'affiche après la mention « Common ».
   b. Ouvrez la Console de gestion à distance et sélectionnez l'onglet **Détails et actions** du point final.
   c. Dans la section Détail de bouclier de l'écran Détail de point final, recherchez l'entrée DCID/ID de récupération.

2 Pour télécharger la clé du serveur, accédez à l'utilitaire Dell Administrative Unlock **(CMGAu)** et exécutez-le.

Vous pouvez obtenir l'utilitaire Dell Administrative Unlock auprès de Dell ProSupport.

3 Dans la boîte de dialogue de l'utilitaire Dell Administrative Unlock (CMGAu), entrez les informations suivantes (certains champs peuvent être prérenseignés) et cliquez sur **Suivant**.

Serveur :	Nom d'hôte complet du serveur, par exemple : Serveur de périphérique : **https://<entreprise.serveur.com>:8081/xapi** Serveur de sécurité : **https://<entreprise.serveur.com>:8443/xapi/**
Admin Dell :	le nom de compte de l'administrateur d'enquête (activé dans le serveur)
Mot de passe d'admin Dell :	le mot de passe de compte de l'administrateur d'enquête (activé dans le serveur)
MCID :	effacez le contenu du champ MCID
DCID :	DCID/ID de récupération que vous avez obtenu précédemment.

4 Dans la boîte de dialogue Dell Administrative Utility, sélectionnez **Non, effectuer un téléchargement depuis un serveur maintenant** et cliquez sur **Suivant**.

REMARQUE : Si le client de cryptage n'est pas installé, un message signale *Le déverrouillage a échoué*. Passez à un ordinateur où le client de cryptage est installé.

5 Une fois le téléchargement et le déverrouillage terminés, copiez les fichiers à récupérer à partir de ce lecteur. Tous les fichiers peuvent être lus. ***Ne cliquez pas sur Terminer tant que vous n'avez pas récupéré les fichiers***.

6 Après avoir récupéré les fichiers et lorsque vous êtes prêt à reverrouiller ces fichiers, cliquez sur **Terminer**.

Après que vous cliquez sur Terminer, les fichiers cryptés ne sont plus disponibles.

7

Récupération du gestionnaire BitLocker

Pour récupérer des données, vous pouvez obtenir un mot de passe de récupération ou un package de clés à partir de la Console de gestion à distance, ce qui vous permettra de déverrouiller les données sur l'ordinateur.

Récupérer des données

1. Dans la Console de gestion à distance, connectez-vous en tant qu'administrateur Dell.
2. Dans le volet de gauche, cliquez sur **Gestion > Récupérer des données**.
3. Cliquez sur l'onglet *Gestionnaire*.
4. Pour *BitLocker* :

   Entrez l'**ID de récupération** reçu de BitLocker. (Facultatif) Si vous indiquez le nom d'hôte et le volume, l'ID de récupération est entré automatiquement.

   Cliquez sur **Obtenir le mot de passe de récupération** ou **Créer un package de clés**.

   Selon la méthode de récupération souhaitée, vous allez utiliser le mot de passe de récupération ou le package de clés pour récupérer les données.

   Pour le *TPM* :

   entrez le **nom d'hôte**.

   Cliquez sur **Obtenir le mot de passe de récupération** ou **Créer un package de clés**.

   Selon la méthode de récupération souhaitée, vous allez utiliser le mot de passe de récupération ou le package de clés pour récupérer les données.
5. Pour terminer la récupération, voir la section Instructions Microsoft pour récupération.

REMARQUE : Si le gestionnaire BitLocker n'est pas « propriétaire » du TPM, le mot de passe TPM et le package de clés ne sont pas disponibles dans la base de données Dell. Dans ce cas, un message d'erreur indique que Dell ne peut pas trouver la clé, ce qui correspond au comportement prévu.

Pour récupérer un TPM dont une entité autre que le gestionnaire BitLocker est « propriétaire », vous devez suivre le processus de récupération du TPM à partir de ce « propriétaire » ou votre processus actuel de récupération du TPM.

A

Annexe A : Gravage de l'environnement de récupération

Gravage du fichier ISO d'environnement de récupération sur CD/DVD

Le lien suivant contient le processus à suivre pour utiliser Microsoft Windows 7/8/10 afin de créer un CD ou DVD amorçable pour l'environnement de récupération.

http://windows.microsoft.com/en-us/windows7/burn-a-cd-or-dvd-from-an-iso-file

Gravage du fichier ISO d'environnement de récupération sur support amovible

Pour créer un USB amorçable, suivez les instructions de cet article issu de Microsoft :

https://technet.microsoft.com/en-us/library/jj200124(v=ws.11).aspx


0XXXXXA0X