Dell Data Protection

Guide de récupération v8.13/v1.7/v1.4/v1.2

Remarques, précautions et avertissements

REMARQUE : Une REMARQUE indique des informations importantes qui peuvent vous aider à mieux utiliser votre produit.

PRÉCAUTION : Une PRÉCAUTION indique un risque d'endommagement du matériel ou de perte de données et vous indique comment éviter le problème.

AVERTISSEMENT : Un AVERTISSEMENT indique un risque d'endommagement du matériel, de blessures corporelles ou même de mort.

Guide de récupération Dell Data Protection

2017 - 04

Rév. A01

Table des matières

1

Prise en main de la récupération

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
  - En cas de gravure de CD ou DVD, consultez la section Gravure de l'image ISO de l'environnement de récupération sur CD/DVD pour en savoir plus.
  - Si vous utilisez un support USB, consultez Gravure de l'environnement de récupération sur un support amovible pour en savoir plus.
- 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.

Contacter Dell ProSupport

Appelez le 877-459-7304, poste 4310039, afin de recevoir 24h/24, 7j/7 une assistance téléphonique concernant votre produit Dell Data Protection.

Un support en ligne pour les produits Dell Data Protection est en outre disponible à l'adresse dell.com/support. Le support en ligne englobe les pilotes, les manuels, des conseils techniques et des réponses aux questions fréquentes et émergentes.

Aidez-nous à vous mettre rapidement en contact avec l'expert technique approprié en ayant votre Code de service à portée de main lors de votre appel.

Pour les numéros de téléphone en dehors des États-Unis, consultez Numéros de téléphone internationaux Dell ProSupport .

Récupération du chiffrement basé sur des règles ou de fichier/dossier

À l'aide de la récupération du chiffrement basé sur des règles ou FFE (File/Folder Encryption, chiffrement 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.

Présentation du processus de récupération

Pour récupérer un système défaillant :

1 Gravez l'environnement de restauration sur un CD/DVD ou créez une clé USB démarrable. Reportez-vous à l'Annexe A - Gravure de l'environnement de restauration.
2 Obtenir le fichier de récupération.
3 Procéder à la récupération.

Exécution du chiffrement basé sur des règles ou de fichier/dossier

Suivez ces étapes pour effectuer une récupération de chiffrement basé sur les règles ou FFE.

Obtention du fichier de récupération : ordinateur géré à distance

Pour télécharger le fichier **<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 **<nommachine_domaine.com** > **.exe** à un emplacement accessible au démarrage dans WinPE.

Obtention du fichier de récupération : ordinateur géré localement

Pour obtenir le fichier de récupération Personal Edition :

1 Localisez le fichier de restauration dénommé **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 lors de l'installation de Personal Edition.

2 Copiez **LSARecovery_<nomsystème> > .exe** sur l'ordinateur cible (où se trouvent les données à récupérer).

Effectuer une 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 Saisissez **x** et appuyez sur **Entrée** pour afficher une invite de commande.

3 Accédez 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 la carte HCA (accélérateur de cryptage matériel) ou la carte mère/TPM doivent être remplacées.

5 Dans la boîte de dialogue Backup and Recovery Information (Informations de sauvegarde et de récupération), confirmez que les informations sur l'ordinateur client à récupérer sont correctes et cliquez sur **Next** (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 **Next** (Suivant).

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

Si le lecteur sélectionné ne fait pas l'objet d'un chiffrement basé sur des règles ou de fichier/dossier (FFE), la récupération échouera.

7 Saisissez votre mot de passe de récupération, puis cliquez sur **Next** (Suivant).

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

Dans Personal Edition, il s'agit du mot de passe est le 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 Recover (Récupération), cliquez sur **Recover** (Récupérer). Le processus de récupération démarre.

9 Une fois l'installation terminée, cliquez sur **Finish** (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.

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 *Access denied* (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 DCID/ID de récupération de huit caractères s'affiche après « Common ».

   b Ouvrez la console de gestion à distance et sélectionnez l'onglet **Details & Actions** (Détails et actions) pour le point de terminaison.
   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 depuis le 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 **Next** (Suivant).
   Server (Serveur) : nom d'hôte complet du serveur, par exemple :

   Serveur de périphérique : **https://<server.organization.com>:8081/xapi**

   Serveur de sécurité : **https://<server.organization.com>:8443/xapi/**

   Dell Admin (Admin Dell) : le nom de compte de l'administrateur d'enquête (activé dans le serveur)

   Dell Admin Password (Mot de passe de l'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 : le DCID/ID de récupération que vous avez obtenu auparavant.

4 Dans la boîte de dialogue de l'utilitaire d'administration Dell, sélectionnez **No, perform a download from a server now** (Non, effectuer un téléchargement à partir d'un serveur maintenant) et cliquez sur **Next (Suivant)**.

> **REMARQUE :**
> Si le client de chiffrement n'est pas installé, un message signale *Unlock failed* (Échec du déverrouillage). 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 Finish (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 **Finish** (Terminer).
   Une fois que vous avez cliqué sur Finish (Terminer), les fichiers chiffrés ne sont plus disponibles.

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 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 Gravez l'environnement de restauration sur un CD/DVD ou créez une clé USB démarrable. Reportez-vous à l'Annexe A - Gravure de l'environnement de restauration.
2 Obtenir le fichier de récupération.
3 Procéder à la récupération.

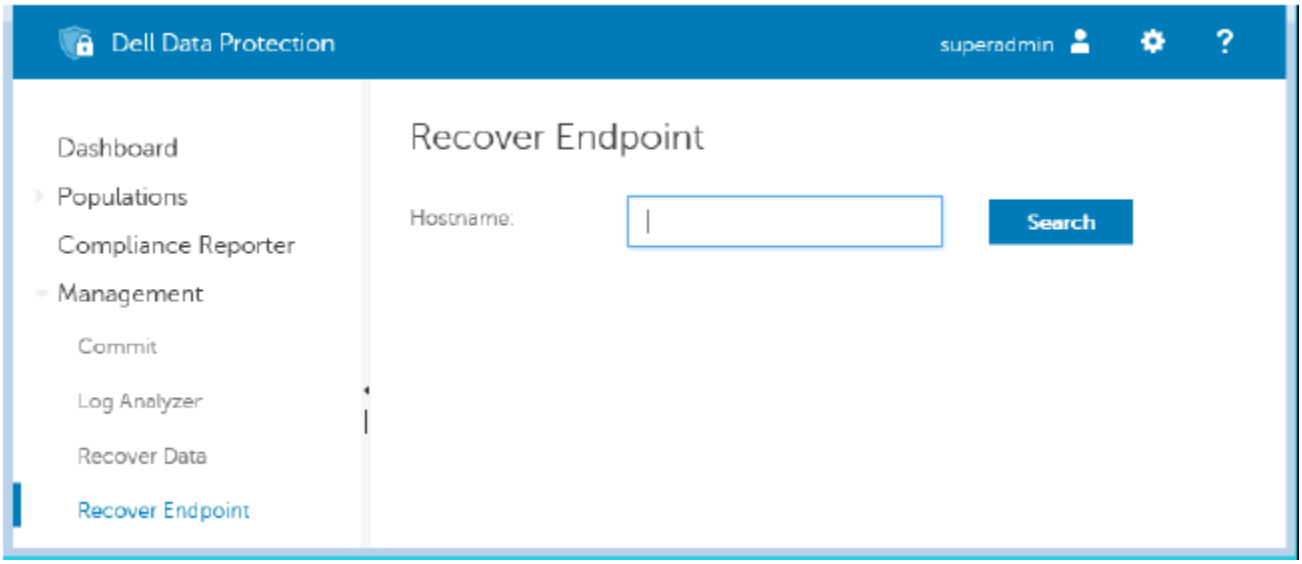
Procéder à la récupération de HCA

Suivez ces étapes pour effectuer une récupération de HCA.

Obtention du fichier de récupération : ordinateur géré à distance

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

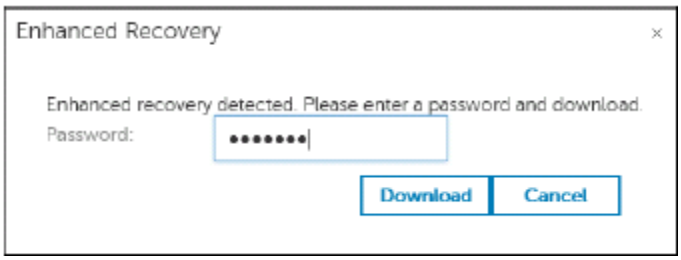
1 ouvrez la Console de gestion à distance et sélectionnez **Gestion** > **Récupérer le point final** dans le volet de gauche.



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.



Obtention du fichier de récupération : ordinateur géré localement

Pour obtenir le fichier de récupération Personal Edition :

1 Localisez le fichier de restauration dénommé **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 lors de l'installation de Personal Edition.

2 Copiez **LSARecovery_<nomsystème> > .exe** sur l'ordinateur cible (où se trouvent les données à récupérer).

Effectuer une 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 Saisissez **x** et appuyez sur **Entrée** pour afficher 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 **Next** (Suivant).

6 Dans la boîte de dialogue qui répertorie les volumes de l'ordinateur, sélectionnez tous les lecteurs applicables et cliquez sur **Next** (Suivant).

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

Si le lecteur sélectionné n'est pas crypté HCA, la récupération échouera.

7 Saisissez votre mot de passe de récupération, puis cliquez sur **Next** (Suivant).

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

Sur un ordinateur géré localement, le 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 Recover (Récupération), cliquez sur **Recover** (Récupérer). Le processus de récupération démarre.

9 À l'invite, accédez 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 prendre un certain temps.

10 Lorsqu'un message s'affiche pour indiquer que la récupération a réussi, cliquez sur **Finish** (Terminer). L'ordinateur redémarre.

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

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 Gravez l'environnement de restauration sur un CD/DVD ou créez une clé USB démarrable. Reportez-vous à l'Annexe A - Gravure de l'environnement de restauration.
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

Obtenez le fichier de récupération.

Le fichier de récupération peut être téléchargé à partir de la console de gestion à distance. Pour télécharger le fichier *<nom d'hôte> - sed-recovery.dat* généré à l'installation de Dell Data Protection :

a Ouvrez la console de gestion à distance et, dans le volet gauche, sélectionnez **Management > Recover Data** (Gestion > Récupérer les données), puis sélectionnez l'onglet **SED**.
b Dans l'écran Recover Data (Récupérer des données), dans le champ Hostname (Nom d'hôte), entrez le nom de domaine complet du point de terminaison, puis cliquez sur **Search** (Rechercher).

c Dans le champ SED, sélectionnez une option.

d Cliquez sur **Create Recovery File** (Créer un fichier de récupération).

Le fichier **<nom d'hôte> -sed-recovery.dat** est téléchargé.

Obtention du fichier de récupération - Client SED géré localement

Obtenez le 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 du fichier est *OpalSPkey<nom du système>.dat*.

Effectuer une 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 avec l'application de récupération.

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

3 Sélectionnez **Browse** (Parcourir), localisez le fichier de récupération, puis cliquez sur **Open** (Ouvrir).

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

- **One-time unlock of the drive** (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).
- **Unlock drive and remove PBA** (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 **<nommachine_domaine.com>.exe** généré à 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 Enhanced Recovery (Récupération avancée), saisissez un mot de passe de récupération et cliquez sur **Download** (Télécharger).

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

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

Effectuer une récupération

1 Créez un support amorçable de l'environnement de récupération. Pour obtenir des instructions, voir l'Annexe A - Gravure de l'environnement de restauration.

2 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.

3 Saisissez **x** et appuyez sur **Entrée** pour afficher une invite de commande.

4 Accédez 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.

5 À l'invite de commande d'administration, exécutez **<nommachine_domaine.com** > **.exe** > **-p <motdepasse** > **-gpk**

Il renvoie le GPKRCVR.txt correspondant à votre ordinateur.

6 Copiez le fichier **GPKRCVR.txt** à la racine du lecteur du système d'exploitation de l'ordinateur.

7 Redémarrez l'ordinateur.

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

8 Si vous y êtes invité, redémarrez de nouveau.

6

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 gauche, cliquez sur **Management** > **Recover Data** (Gestion > Récupérer des données).

3 Cliquez sur l'onglet **Manager** (Gestionnaire).

4 Pour *BitLocker* :

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

Cliquez sur **Get Recovery Password** (Obtenir le mot de passe de récupération) ou **Create Key Package** (Créer le 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 module *TPM* :

Saisissez le **Hostname** (nom d'hôte).

Cliquez sur **Get Recovery Password** (Obtenir le mot de passe de récupération) ou **Create Key Package** (Créer le 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 le processus de récupération, reportez-vous aux Instructions de récupération de Microsoft.

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.

Récupération du mot de passe

Les utilisateurs oublient couramment leur mot de passe. Heureusement, plusieurs méthodes sont à leur disposition pour retrouver l'accès à un ordinateur avec l'authentification avant démarrage, le cas échéant.

- La fonction Recovery Questions (Questions de récupération) offre une authentification basée sur des questions/réponses.
- Les codes de question/réponse permettent aux utilisateurs de retrouver l'accès à leur ordinateur en collaboration avec leur administrateur. Cette fonction est disponible uniquement pour les utilisateurs dont les ordinateurs sont gérés par leur entreprise.

Questions de récupération

La première fois qu'il se connecte à un ordinateur, l'utilisateur est invité à répondre à un ensemble standard de questions configurées par l'administrateur. Après avoir enregistré ses réponses à ces questions, au prochain oubli de son mot de passe, l'utilisateur est invité à les fournir. En supposant qu'il a répondu aux questions correctement, il est en mesure de se connecter et de retrouver l'accès à Windows.

Configuration requise

- Les questions de récupération doivent être configurées par l'administrateur.
- L'utilisateur doit enregistrer ses réponses aux questions.
- Avant de cliquer sur l'option de menu **Trouble Signing In** (Problème de connexion), l'utilisateur doit entrer un nom d'utilisateur et de domaine valides.

Pour accéder aux questions de récupération à partir de l'écran de connexion PBA :

1 Saisissez un nom de domaine et un nom d'utilisateur valides.
2 Dans le côté inférieur gauche de l'écran, cliquez sur **Options** > **Trouble Signing In** (Options > Problème de connexion).
3 Lorsque la boîte de dialogue de Q&R s'affiche, entrez les réponses indiquées à l'enregistrement des questions de récupération lors de votre première connexion.

Codes de question/réponse

La récupération de question/réponse peut être utilisée à des fins d'authentification via PBA pour accéder à Windows. La méthode de question/réponse peut être utilisée dans les scénarios suivants :

- Lorsqu'un utilisateur ne se rappelle pas des réponses fournies au moment de l'enregistrement des questions de récupération.
- L'administrateur n'a pas activé la fonction Recovery Questions (Questions de récupération).
- Un utilisateur est à distance avec aucune connectivité réseau et ne peut pas recevoir de commande de déverrouillage depuis le serveur de sécurité via le Contrôle de périphériques SED

Un utilisateur peut accéder à l'écran Challenge/Response (Question/réponse) en cliquant sur l'option **Trouble Signing In**(Problème de connexion) ou en saisissant un mot de passe erroné, en dépassant la limite de tentatives de mot de passe sans brancher de câble réseau. Si la fonctionnalité Recovery Questions (Questions de récupération) est désactivée, l'option **Trouble Signing In** (Problème de connexion) ouvre directement l'écran Challenge/Response (Question/réponse).

Requis

- La récupération par question/réponse est disponible uniquement sur les ordinateurs du domaine gérés à distance par votre organisation ou entreprise.

Configuration requise

- Déconnectez l'ordinateur du réseau avant de répondre à l'une des questions de récupération ou en saisissant des codes de question/réponse.
- Avant de cliquer sur Trouble Signing In (Problème de connexion), saisissez un nom d'utilisateur et de domaine valides.

Pour utiliser la récupération par question/réponse

1 L'utilisateur clique sur le lien **Options** pour afficher le menu.

2 L'utilisateur clique sur **Trouble Signing In** > **Challenge/Response** (Problème de connexion > Question/réponse).

> **REMARQUE :**
> L'option Challenge/Response (Question/réponse) est disponible uniquement sur les ordinateurs gérés par une entreprise. Si l'ordinateur ne fait pas partie du domaine, l'option Challenge/Response (Question/réponse) ne s'affiche pas dans le menu.

3 Lorsqu'il y est invité, l'utilisateur contacte le support technique et communique à l'administrateur le nom de périphérique (nom d'hôte) et le code de question.

4 L'administrateur ouvre la console de gestion à distance, clique sur **Management** > **Recover Data** (Gestion > Récupérer des données), puis clique sur **SED** dans le menu supérieur.

5 Sous Recover SED User Access (Récupérer l'accès utilisateur SED), l'administrateur saisit le **Host Name** (Nom d'hôte) obtenu auprès de l'utilisateur, puis clique sur **Search** (Rechercher).

6 L'administrateur sélectionne le nom d'utilisateur qui demande de l'aide :

7 Saisissez le code de périphérique obtenu auprès de l'utilisateur dans le champ **Challenge** (Question), puis cliquez sur **Generate Response** (Générer la réponse).

8 Communiquez le code de réponse généré à l'utilisateur.

> **REMARQUE :**
> Ces codes ne sont pas sensibles à la casse. Les chiffres s'affichent en rouge et les lettres en bleu.

9 L'utilisateur saisit le code de réponse dans les champs **Response code** (Code de réponse) dans l'écran d'authentification PBA. Voici un exemple de code de réponse saisi par l'utilisateur :

10 Cliquez sur la flèche droite pour continuer après authentification sur l'écran PBA.

11 Cliquez sur **Envoyer**.

Un utilisateur peut s'authentifier via PBA une seule fois à l'aide de la fonction Challenge/Response (Question/Réponse). Après un redémarrage de l'ordinateur, la couche PBA reprend la protection de l'ordinateur, en invitant l'utilisateur à s'identifier via l'écran PBA.

> **REMARQUE :**
> Une fois qu'il a affiché la boîte de dialogue Challenge/Response (Question/Réponse), l'utilisateur doit terminer la séquence pour accéder à nouveau au système. Si l'utilisateur éteint l'ordinateur et tente de se reconnecter, même avec le mot de passe correct, PBA réinvite l'utilisateur à utiliser la boîte de dialogue Challenge/Response (Question/réponse).

Récupération du mot de passe External Media Shield

External Media Shield (EMS) vous offre la possibilité de protéger les supports de stockage amovible dans et à l'extérieur de votre entreprise en permettant aux utilisateurs de chiffrer les clés USB et d'autres supports de stockage amovibles. L'utilisateur attribue un mot de passe à chaque périphérique de support amovible à protéger. Cette section décrit le processus de récupération de l'accès à un périphérique de stockage USB chiffré en cas d'oubli du mot de passe d'un périphérique par l'utilisateur.

Récupération de l'accès aux données

Lorsqu'un utilisateur ne parvient pas à saisir correctement son mot de passe après le nombre autorisé de tentatives, le périphérique USB est placé en mode d'authentification manuelle.

L'authentification manuelle consiste à fournir les codes à un administrateur connecté au serveur à partir du client.

Le mode d'authentification manuelle offre à l'utilisateur deux options de réinitialisation de mot de passe et de récupération de l'accès à ses données.

L'administrateur fournit un code d'accès pour le client, permettant ainsi à l'utilisateur de réinitialiser son mot de passe et de retrouver l'accès à ses données chiffrées.

1. Lorsque vous êtes invité à saisir votre mot de passe, cliquez sur le bouton **I Forgot** (J'ai oublié).

   La boîte de dialogue de confirmation s'affiche.
2. Cliquez sur **Yes** (Oui) pour confirmer. Après la confirmation, le périphérique passe en mode d'authentification manuelle.
3. Contactez l'administrateur du support technique et communiquez-lui les codes qui s'affichent dans la boîte de dialogue.
4. En tant qu'administrateur du support technique, ouvrez une session sur la console de gestion à distance. Le compte d'administrateur du support technique doit disposer des privilèges ad-hoc.
5. Naviguez jusqu'à l'option de menu **Recover Data** (Récupérer des données) dans le volet gauche.
6. Saisissez les codes fournis par l'utilisateur final.
7. Cliquez sur le bouton **Generate Response** (Générer une réponse) situé dans le coin inférieur droit de l'écran.
8. Communiquez le code d'accès à l'utilisateur.

   REMARQUE :

   Veuillez authentifier l'utilisateur manuellement avant de fournir un code d'accès. Par exemple, posez à l'utilisateur une série de questions au téléphone dont lui seul connaît les réponses, telles que « Quel est votre numéro d'ID d'employé ? ». Autre exemple : demandez à l'utilisateur de passer au support technique s'identifier, pour vous assurer qu'il est le propriétaire du support. Tout défaut d'authentification d'un utilisateur avant de fournir un code d'accès au téléphone permettrait à un attaquant d'avoir accès à un support amovible chiffré.
9. Réinitialisez le mot de passe de votre support chiffré.

   L'utilisateur est invité à réinitialiser le mot de passe du support chiffré.

Auto-récupération

L'auto-récupération est le processus de réinitialisation du mot de passe pour un périphérique de support amovible chiffré en insérant le lecteur dans une machine protégée à laquelle le propriétaire du support est connecté. Tant que le propriétaire du support est authentifié auprès du Mac ou du PC protégé, le client détecte la perte de clé matérielle et invite l'utilisateur à réinitialiser le périphérique. À ce stade, l'utilisateur peut réinitialiser son mot de passe et retrouver l'accès à ses données chiffrées.

1 Connectez-vous à un poste de travail chiffré par Dell Data Protection en tant que propriétaire de support.
2 Insérez le périphérique de stockage amovible chiffré.
3 Lorsque vous y êtes invité, saisissez un nouveau mot de passe pour réinitialiser le périphérique de stockage amovible.

   Si l'opération réussit, une petite notification s'affiche pour indiquer que le mot de passe a été accepté.
4 Accédez au périphérique de stockage et confirmez l'accès aux données.

9

Récupération Dell Data Guardian

Cet outil de récupération offre les fonctionnalités suivantes :

- Déchiffrement des fichiers Office protégés

  Ils incluent des fichiers offrant un triple chiffrement. En raison des multiples méthodes de chiffrement de fichiers, il arrive parfois qu'un fichier soit chiffré deux ou trois fois. Si l'utilisateur ouvre le fichier, un message d'erreur lui indique de contacter son administrateur pour les récupérer.
- Mise en dépôt de clé matérielle
- Possibilité de vérifier les fichiers altérés
- Possibilité de forcer le déchiffrement des documents Office protégés en cas d'altération du wrapper du fichier par un tiers, par exemple, la page de garde du fichier Office protégé dans le cloud ou sur un périphérique ne disposant pas de Data Guardian

Configuration requise pour la récupération

La configuration requise inclut :

- Microsoft .Net Framework 4.5.2 exécuté sur le point de terminaison à récupérer.
- Le rôle d'administrateur d'enquête doit être affecté dans la console de gestion à distance à l'administrateur effectuant la récupération.

Effectuer une récupération Data Guardian

Procédez comme suit pour effectuer une récupération de documents Office protégés par Data Guardian.

Exécution d'une récupération à partir de Windows, d'une clé USB ou d'un lecteur réseau

Pour effectuer une récupération :

1 À partir du support d'installation Dell, copiez **RecoveryTools.exe** à l'une des emplacements suivants :

   - Ordinateur : copiez le fichier .exe sur l'ordinateur sur lequel les documents Office doivent être récupérés.
   - USB : copiez le fichier .exe sur la clé USB et exécutez-le à partir de cette dernière.
   - Pilote réseau

2 Double-cliquez sur **RecoveryTools.exe** pour lancer l'outil de récupération.

3 Dans la fenêtre Data Guardian, saisissez l'URL du serveur Dell au format suivant :

   https://<server.domain.com>:8443/cloud

   REMARQUE :
   Remplacez <server.domain.com> par le nom d'hôte complet du serveur Dell qui gère Data Guardian sur ce point de terminaison. Pour localiser l'URL du serveur Dell, cliquez sur l'icône Data Guardian de la barre d'état système, puis cliquez sur **Details** (Détails). L'URL du serveur s'affiche dans le coin supérieur gauche de l'écran Details (Détails) :

4 Saisissez votre nom d'utilisateur et votre mot de passe, puis cliquez sur **Log in** (Connexion).

REMARQUE :
Ne décochez pas la case *Enable SSL Trust* (Activer la confiance SSL) sauf si votre administrateur vous y invite.

REMARQUE :
Si vous n'êtes pas un administrateur d'analyse et si vous saisissez les informations d'identification, un message s'affiche indiquant que vous ne disposez pas des droits de connexion.

Si vous êtes un administrateur d'analyse, l'outil de récupération s'ouvre.

5 Sélectionnez **Source**.

REMARQUE :
Vous devez accéder à une source et à une destination, mais vous pouvez les sélectionner dans n'importe quel ordre.

6 Cliquez sur **Browse** (Parcourir) pour sélectionner le dossier ou le lecteur à récupérer.

7 Cliquez sur **OK**.

8 Cliquez sur **Destination**

9 Cliquez sur **Browse** (Parcourir) pour sélectionner une destination, telle qu'un périphérique externe, un emplacement de répertoire ou le bureau.

10 Cliquez sur **OK**.

11 Sélectionnez une ou plusieurs cases en fonction des éléments que vous souhaitez récupérer.

Options	Description
Dépôt	• Récupérez les clés générées hors ligne qui n'ont pas pu être mises en dépôt sur le serveur Dell. • Si un disque dur tombe en panne alors que l'utilisateur est hors ligne, utilisez le lecteur asservi pour récupérer les données et les clés qui ne sont pas mises en dépôt à partir de l'ordinateur.
Décrypté	Pointez l'outil de récupération vers un répertoire qui contient des documents Office protégés pour les déchiffrer. Vous pouvez également, en cas d'altération, sélectionner l'une de ces options ou les deux (voir ci-dessous pour plus d'informations) : • **Tamper check** (Vérification de l'altération) : vérifie les altérations potentielles des fichiers, sans les chiffrer. • **Tamper check** (Vérification de l'altération) et **Force decrypt even if tampered** (Déchiffrement forcé, même en cas d'altération) : vérifie si les fichiers ou le wrapper d'un document Office protégé ont été altérés. Le cas échéant, Data Guardian répare le wrapper et déchiffre le document Office.
Vérification de l'altération	Détecte les fichiers qui ont été altérés et les journalise ou vous prévient. Journalise l'auteur qui a altéré le fichier. Elle ne déchiffre pas les fichiers.
Forcer le décryptage, même en cas d'altération	Pour sélectionner cette option, vous devez également sélectionner **Tamper check** (Vérification de l'altération). Si une personne non autorisée altère le wrapper d'un document Office protégé, tel que la page de garde, sur le cloud ou un périphérique ne disposant pas de Data Guardian, sélectionnez cette option pour réparer le wrapper et forcer le déchiffrement du fichier Office protégé. **Remarque :** si un utilisateur a altéré le fichier .xen Office chiffré du wrapper, le fichier n'est pas récupérable.

Chaque document Office protégé possède un filigrane masqué qui contient l'historique des utilisateurs d'origine et le nom de l'ordinateur, ainsi que tout autre nom d'ordinateur ayant modifié le fichier. Par défaut, l'outil de récupération vérifie les filigranes masqués et journalise les informations.

12 Une fois les sélections terminées, cliquez sur **Scan** (Analyser).

La zone Log (Journal) affiche :

- Les dossiers identifiés et analysés dans la source sélectionnée
- Si un déchiffrement a réussi ou échoué

L'outil de récupération ajoute les fichiers récupérés à la destination sélectionnée. Vous pouvez ouvrir et afficher les fichiers.

Annexe A - Gravure de l'environnement de restauration

Vous pouvez télécharger le programme d'installation Master Installer.

Gravure du fichier ISO de l'environnement de récupération sur CD/DVD

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

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

Gravure de l'environnement de récupération sur un 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