Récupération d'Encryption

Encryption v10.0/Data Guardian v2.0

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.

Encryption v10.0/Data Guardian v2.0

2018 - 08

Rév. A01

Table des matières

1

Prise en main de la récupération

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

- 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 Security Management Server, 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.

Un support en ligne pour les produits Dell 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 numéro de service ou votre code de service express à portée de main lors de votre appel.

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

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

Une récupération est nécessaire lorsque l'ordinateur crypté ne démarre pas sur le système d'exploitation. Cela se produit lorsque le registre n'est pas correctement modifié ou que des modifications de matériel se sont produites sur un ordinateur crypté.

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 affiche un BSOD avec un code STOP de 0x6f ou 0x74.
- Un ordinateur sur lequel vous ne pouvez pas accéder aux données cryptées ni modifier des règles.
- Un serveur exécutant Dell 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.

REMARQUE : À partir de la version v8.9.3, l'accélérateur de cryptage matériel n'est pas pris en charge.

Présentation du processus de récupération

REMARQUE : La récupération nécessite un environnement 32 bits.

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 Obtenez 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 - Chiffrement basé sur des règles ou client de chiffrement FFE

Pour télécharger le fichier de récupération :

1 Téléchargez le module d'installation de Dell Encryption sur http://www.dell.com/support/home/us/en/19/product-support/product/dell-data-protection-encryption/drivers . Naviguez jusqu'au dossier **AdminUtilities** dans le module d'installation et ouvrez le fichier **CMGAd.exe**.
2 Dans le champ **Serveur Dell**, saisissez le serveur Security Management Server/Security Management Server Virtual sur lequel l'ordinateur a été activé.

3 Dans le champ **Admin Dell**, saisissez un nom de compte d'utilisateur disposant des privilèges de l'administrateur d'analyse.

4 Dans le champ **Mot de passe**, saisissez le mot de passe de l'administrateur d'analyse.

5 Dans le champ **MCID**, saisissez le nom de domaine complet (FQDN) du périphérique en cours de récupération.

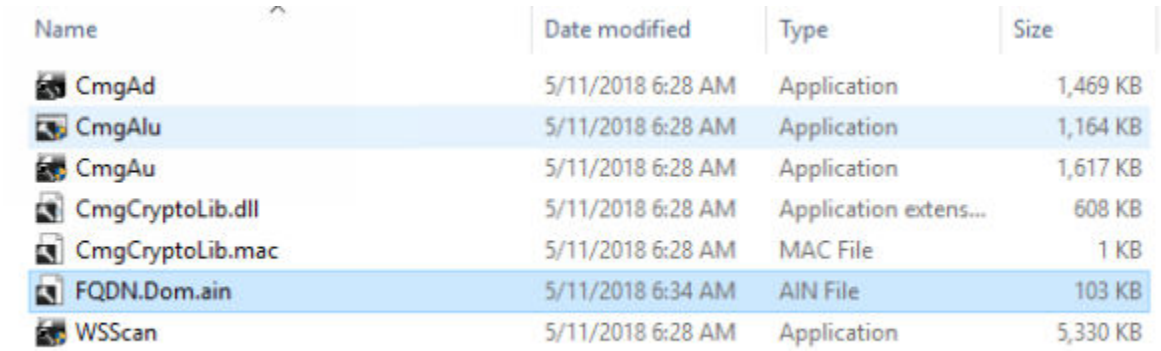
- Le champ **DCID** correspond à l'ID de récupération du périphérique en cours de récupération.

6 Sélectionnez **Suivant**.

7 Définissez, puis confirmez une **phrase de passe** pour le fichier de récupération. Cette phrase de passe est nécessaire pour effectuer la récupération.

8 Dans le champ **Téléchargement vers :**, saisissez un emplacement de destination pour le bundle de récupération, puis sélectionnez **Suivant**. Par défaut, il s'agit du répertoire à partir duquel le fichier CMGAd.exe a été exécuté.

9 Le bundle de récupération se télécharge dans le dossier spécifié dans **Télécharger vers :**.



10 Copiez le bundle de récupération à un emplacement accessible au démarrage dans WinPE.

Obtention du fichier de récupération : ordinateur géré en local

Pour obtenir le fichier de récupération Encryption Personal :

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 d'Encryption Personal.

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 précédemment, 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.

> **REMARQUE : Désactivez SecureBoot avant le processus de récupération. Lorsque vous avez terminé, réactivez SecureBoot.**

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 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 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 **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 Encryption Personal, 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 l'installation 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.

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 DCID/ID de récupération de huit caractères s'affiche après « Common ».

   b Ouvrez la console de gestion à distance et sélectionnez l'onglet **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 **Suivant**.
   Serveur : nom d'hôte complet du serveur, par exemple :

   Serveur de périphérique (avant les clients 8.x) : **https://<server.organization.com>:8081/xapi**

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

   Admin Dell : le nom du compte administrateur d'analyse approfondie (activé dans le Security Management Server/Security Management Server Virtual)

   Mot de passe de l'admin Dell : le mot de passe de compte de l'administrateur d'analyse approfondie (activé dans le Security Management Server/Security Management Server Virtual)

   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 **Non, effectuer un téléchargement à partir d'un serveur maintenant** et cliquez sur **Suivant**.

   REMARQUE :
   Si le client de chiffrement n'est pas installé, un message signale *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 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**.
   Une fois que vous avez cliqué sur Terminer, les fichiers chiffrés ne sont plus disponibles.

Récupération de l'accélérateur de cryptage matériel (Hardware Crypto Accelerator)

REMARQUE : À partir de la version v8.9.3, l'accélérateur de cryptage matériel n'est pas pris en charge.

À l'aide de la récupération Hardware Crypto Accelerator (HCA), vous pouvez récupérer 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 restauration (la restauration exige un environnement 32 bits)
- CD/DVD ou support USB amorçable

Présentation du processus de récupération

REMARQUE : La récupération nécessite un environnement 32 bits.

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 Obtenez le fichier de récupération.
3 Procéder à la récupération.

Procéder à la récupération de HCA

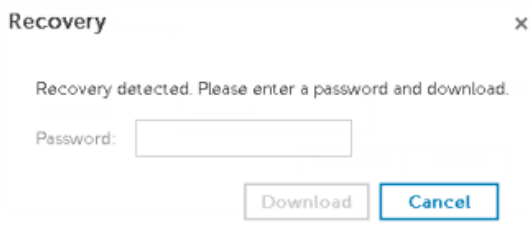
Suivez ces étapes pour effectuer une récupération de HCA.

Obtention du fichier de récupération : ordinateur géré à distance

Pour télécharger le fichier **<machinename_domain.com>.exe** généré à l'installation de Dell Encryption :

1 Ouvrez la console de gestion à distance et, dans le volet gauche, sélectionnez **Gestion** > **Récupérer le point de terminaison**.
2 Dans le champ de recherche, entrez le nom de domaine complet du point de terminaison et cliquez sur **Rechercher**.
3 Dans la fenêtre Récupération, saisissez 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 en local

Pour obtenir le fichier de récupération Encryption Personal :

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 d'Encryption Personal.

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 précédemment, 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.

REMARQUE : Désactivez SecureBoot avant le processus de récupération. Lorsque vous avez terminé, activez SecureBoot.

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 **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 ne fait pas l'objet d'un chiffrement HCA, la récupération échouera.

7 Saisissez votre mot de passe de récupération, puis cliquez sur **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 Récupération, cliquez sur **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 **Terminer**. L'ordinateur redémarre.

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

Récupération de lecteur auto-cryptable (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 l'authentification avant démarrage (PBA).
- 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

REMARQUE : La récupération nécessite un environnement 32 bits ou 64 bits en fonction du mode d'amorçage BIOS.

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. Obtenez 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 *<hostname>-sed-recovery.dat* généré à l'installation de Dell Data Security :

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

c Dans le champ SED, sélectionnez une option.
d Cliquez sur **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 a été généré et est accessible à partir de l'emplacement de sauvegarde que vous avez sélectionné lorsque Authentification avancée a été installée sur l'ordinateur. Le nom du fichier est *OpalSPkey<nom du système>.dat*.

Effectuer une récupération

1 À l'aide du support amorçable créé précédemment, 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.

REMARQUE : Désactivez SecureBoot avant le processus de récupération. Lorsque vous avez terminé, activez SecureBoot.

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 la 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.

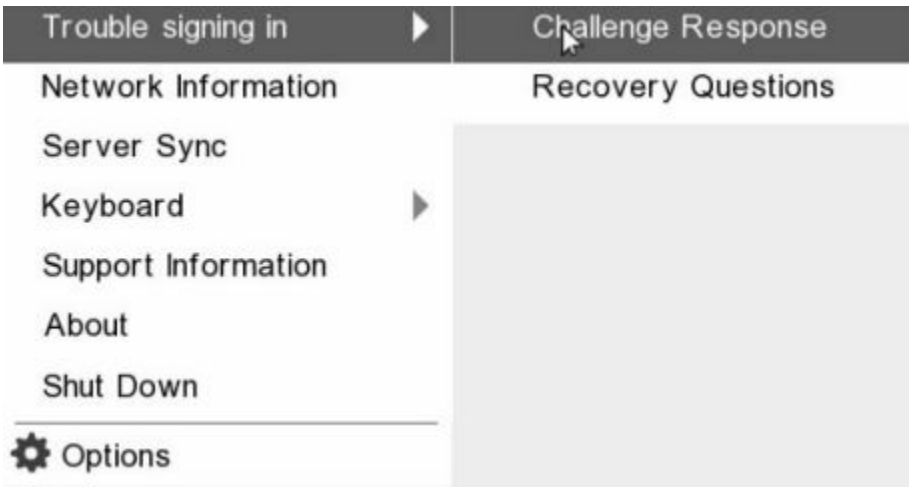
REMARQUE :
Veillez à bien retirer la clé USB ou le CD/DVD utilisé pour amorcer l'ordinateur. Si vous ne le faites pas, vous risquez de redémarrer dans l'environnement de récupération.

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

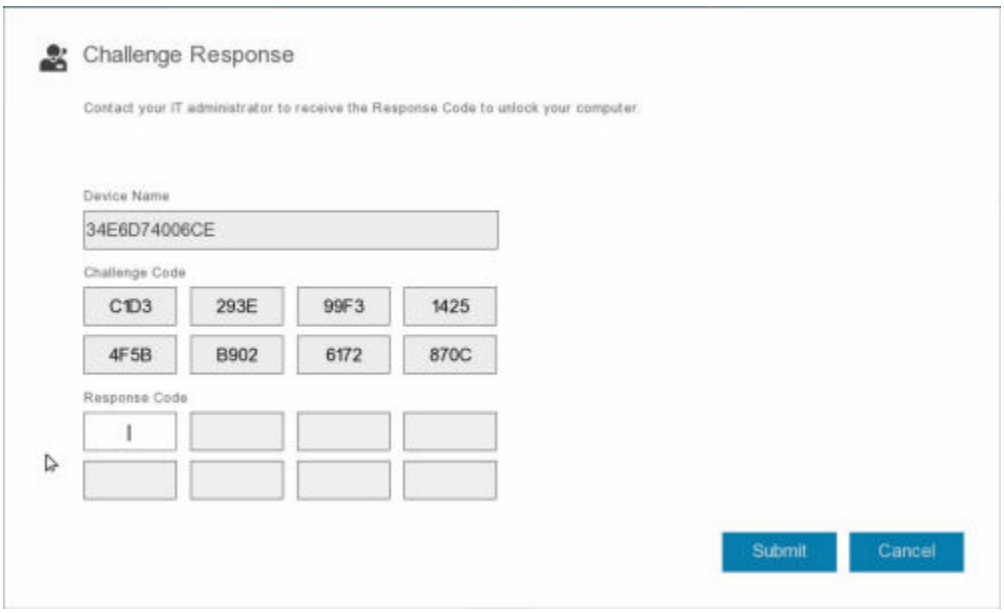
Restauration à la demande avec SED

Contourner l'environnement d'authentification avant démarrage

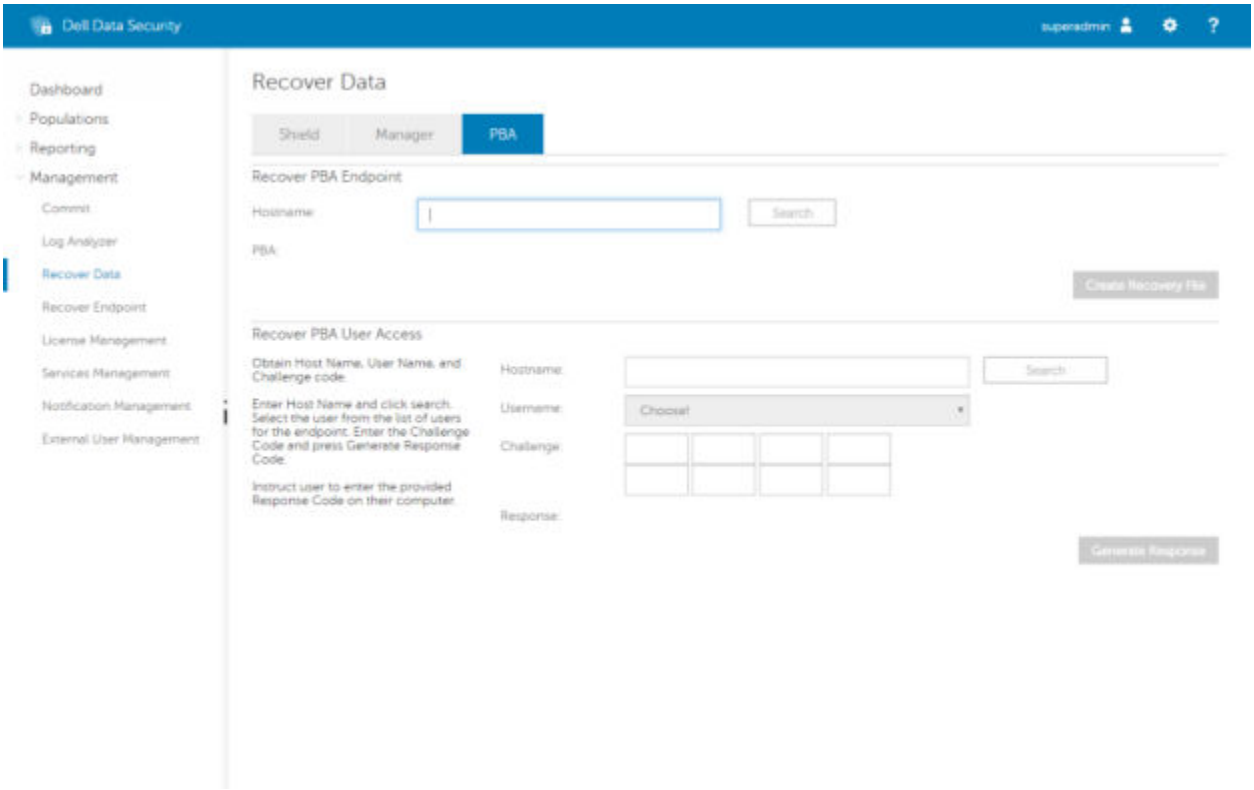
Les utilisateurs oublient leur mot de passe et appellent le centre d'assistance pour savoir comment se connecter à l'environnement PBA. Utilisez le mécanisme de question/réponse intégré à l'appareil. Il est défini pour chaque utilisateur et est basé sur un ensemble tournant de caractères alphanumériques. L'utilisateur doit entrer son nom dans le champ **Nom d'utilisateur**, puis sélectionner **Options > Question/réponse**.



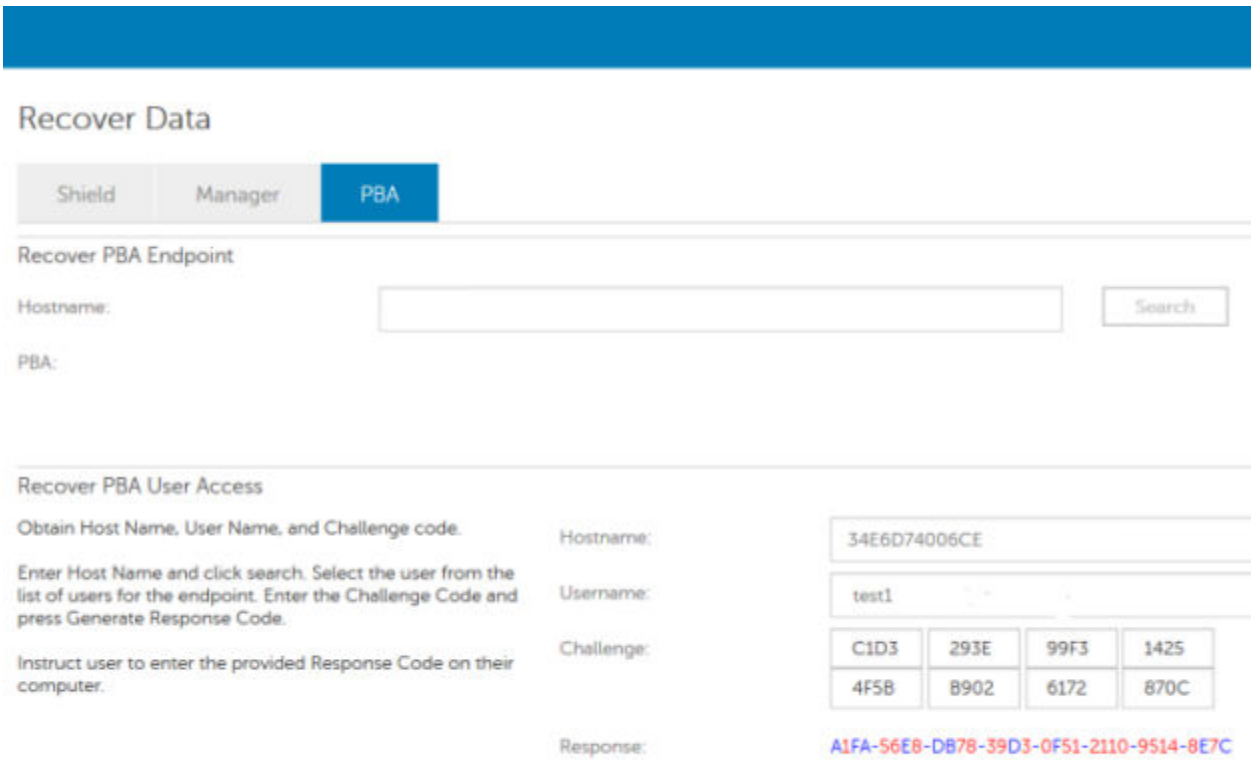
Les informations suivantes s'affichent après avoir sélectionné **Question/réponse**.



Le champ **Nom de l'appareil** est utilisé par le technicien du centre d'assistance dans la console de gestion à distance pour trouver le bon appareil, qui sélectionne ensuite un nom d'utilisateur. Il se trouve dans **Gestion > Récupérer des données** sous l'onglet **PBA**.

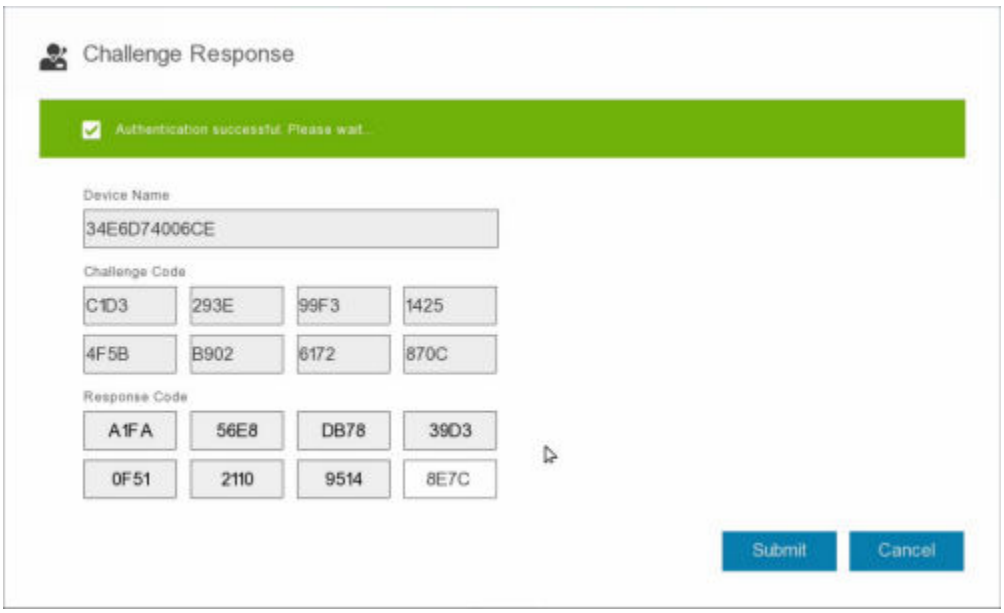


Le code de question est fourni au technicien du centre d'assistance qui entre les données, puis clique sur le bouton **Générer une réponse**.



Les données qui en résultent sont coordonnées par couleur pour vous aider à discerner les caractères numériques (en rouge) et alphabétiques (en bleu). Ces données sont lues à l'utilisateur final, qui les saisit dans l'environnement PBA, puis clique sur le bouton **Soumettre**, ce qui l'amène dans Windows.

Une fois l'authentification effectuée, le message suivant s'affiche :



La récupération à la demande est terminée.

5

Récupération de cryptage complet du disque

La récupération vous permet de récupérer un accès à des fichiers sur un lecteur crypté avec cryptage complet du disque.

REMARQUE : Un décryptage ne doit pas être interrompu. Si le décryptage est interrompu, vous risquez de perdre des données.

Configuration requise pour la récupération

Pour une récupération de cryptage complet du disque, vous avez besoin des éléments suivants :

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

Présentation du processus de récupération

REMARQUE : La récupération nécessite un environnement 64 bits.

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 Obtenez le fichier de récupération.
3 Procéder à la récupération.

Effectuer une récupération de cryptage complet du disque

Suivez ces étapes pour effectuer une récupération de cryptage complet du disque.

Obtention du fichier de récupération - Client de cryptage complet du disque

Obtenez le fichier de récupération.

Téléchargez le fichier de récupération à partir de la Console de gestion à distance. Pour télécharger le fichier *<hostname>-sed-recovery.dat* généré à l'installation de Dell Data Security :

a Ouvrez la console de gestion à distance et, dans le volet gauche, sélectionnez **Gestion > Récupérer les données**, puis sélectionnez l'onglet **PBA**.
b Dans l'écran Récupérer des données, dans le champ Nom d'hôte, entrez le nom de domaine complet du point de terminaison, puis cliquez sur **Rechercher**.
c Dans le champ SED, sélectionnez une option.
d Cliquez sur **Créer un fichier de récupération**.

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

Effectuer une récupération

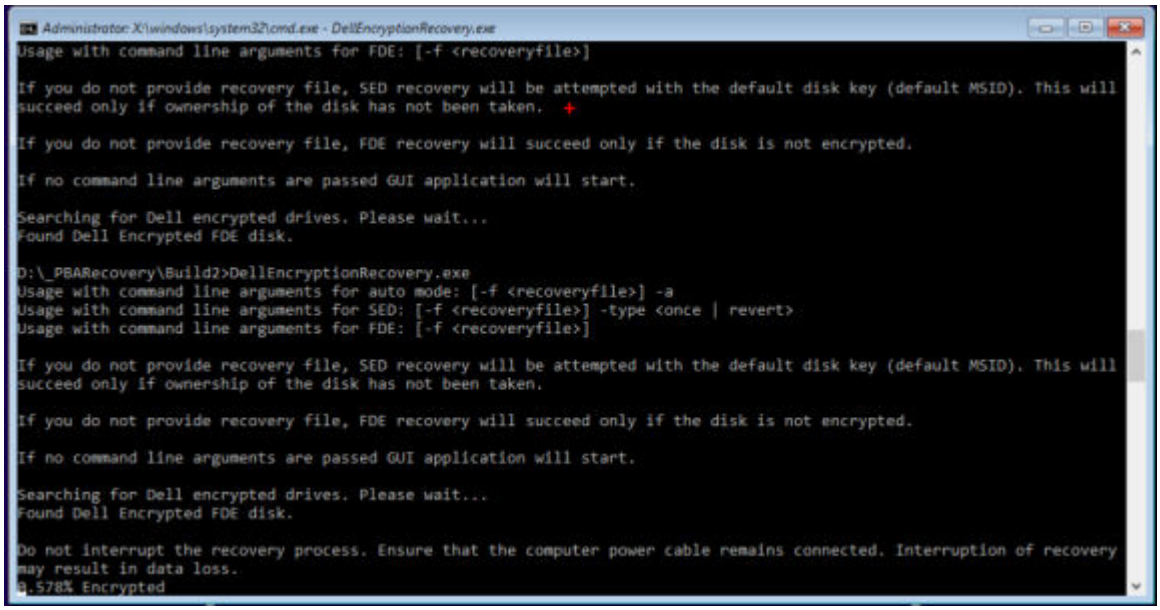
1 À l'aide du support amorçable créé précédemment, effectuez un amorçage sur ce support dans un système de récupération ou sur le périphérique qui contient le disque que vous tentez de récupérer. Un environnement WinPE s'ouvre avec l'application de récupération.

> **REMARQUE : Désactivez SecureBoot avant le processus de récupération. Lorsque vous avez terminé, réactivez SecureBoot.**

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

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

4 Cliquez sur **OK**.



.

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

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

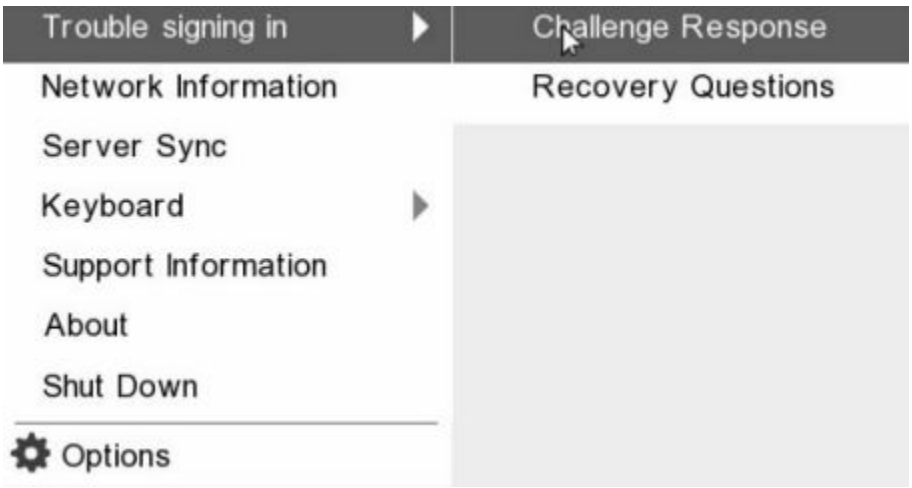
> **REMARQUE :**
> Veillez à bien retirer la clé USB ou le CD/DVD utilisé pour amorcer l'ordinateur. Si vous ne le faites pas, vous risquez de redémarrer dans l'environnement de récupération.

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

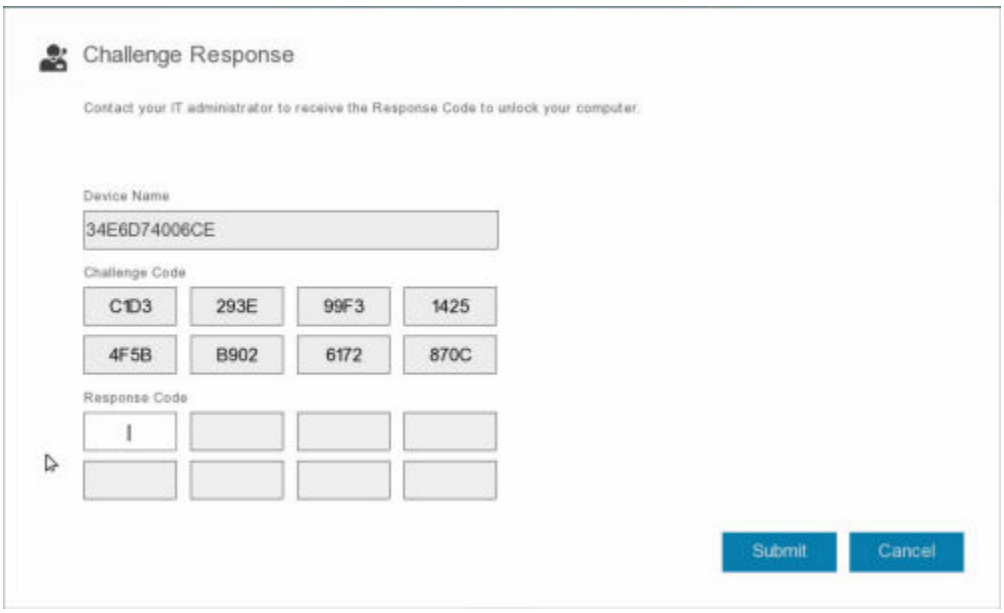
Récupération à la demande avec cryptage complet du disque

Contourner l'environnement d'authentification avant démarrage

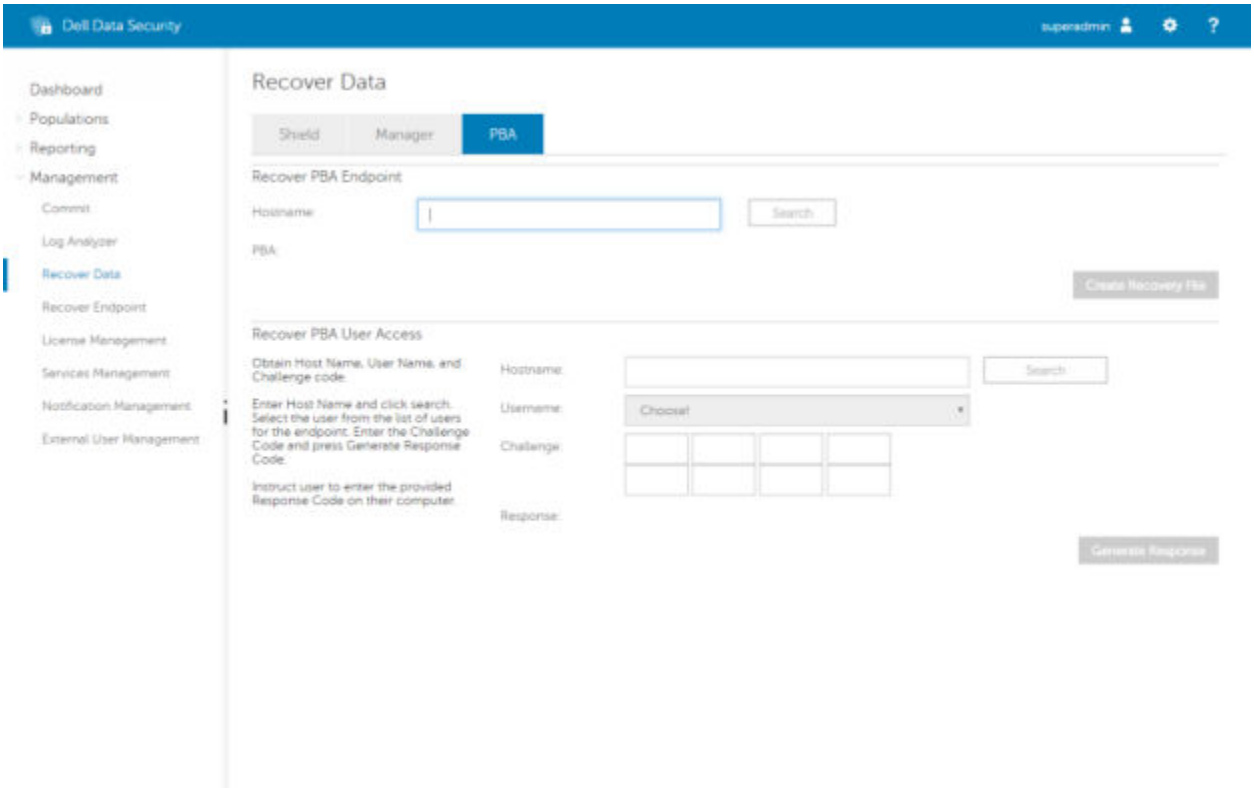
Les utilisateurs oublient leur mot de passe et appellent le centre d'assistance pour savoir comment se connecter à l'environnement PBA. Utilisez le mécanisme de question/réponse intégré à l'appareil. Il est défini pour chaque utilisateur et est basé sur un ensemble tournant de caractères alphanumériques. L'utilisateur doit entrer son nom dans le champ **Nom d'utilisateur**, puis sélectionner **Options > Question/réponse**.



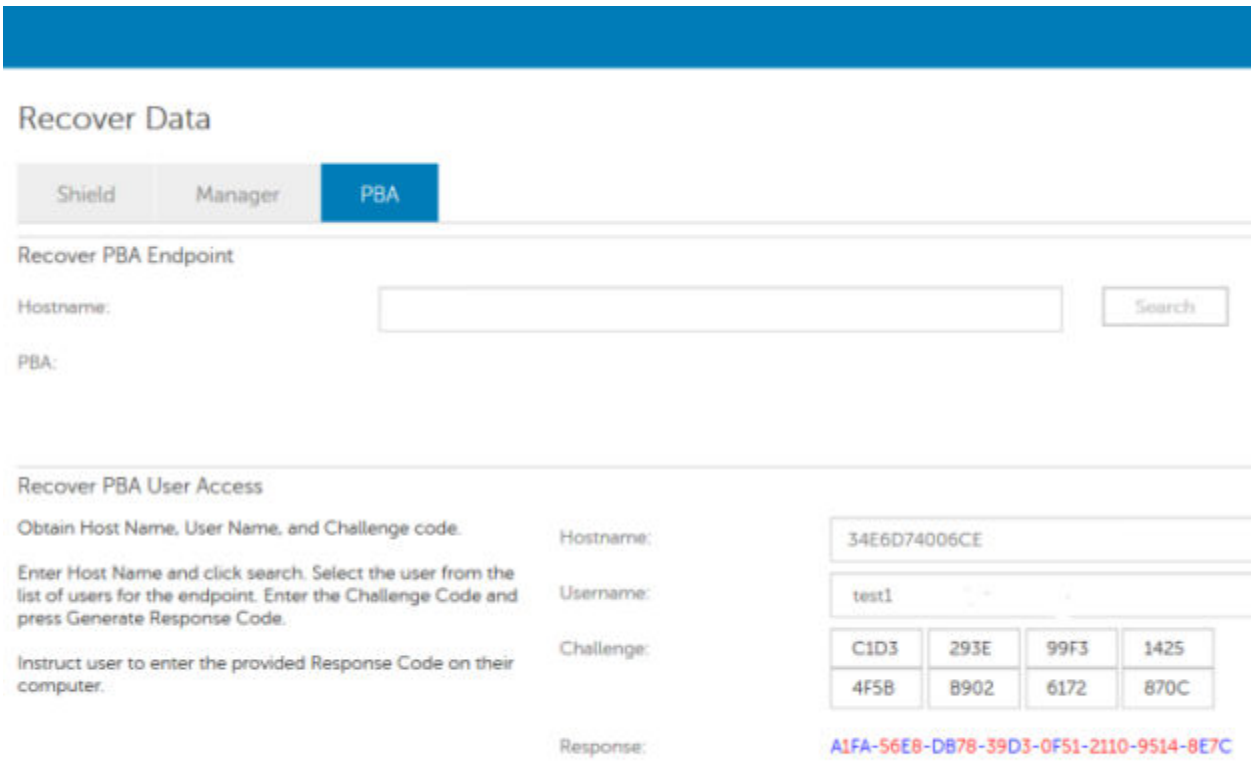
Les informations suivantes s'affichent après avoir sélectionné **Question/réponse**.



Le champ **Nom de l'appareil** est utilisé par le technicien du centre d'assistance dans la console de gestion à distance pour trouver le bon appareil, qui sélectionne ensuite un nom d'utilisateur. Il se trouve dans **Gestion > Récupérer des données** sous l'onglet **PBA**.

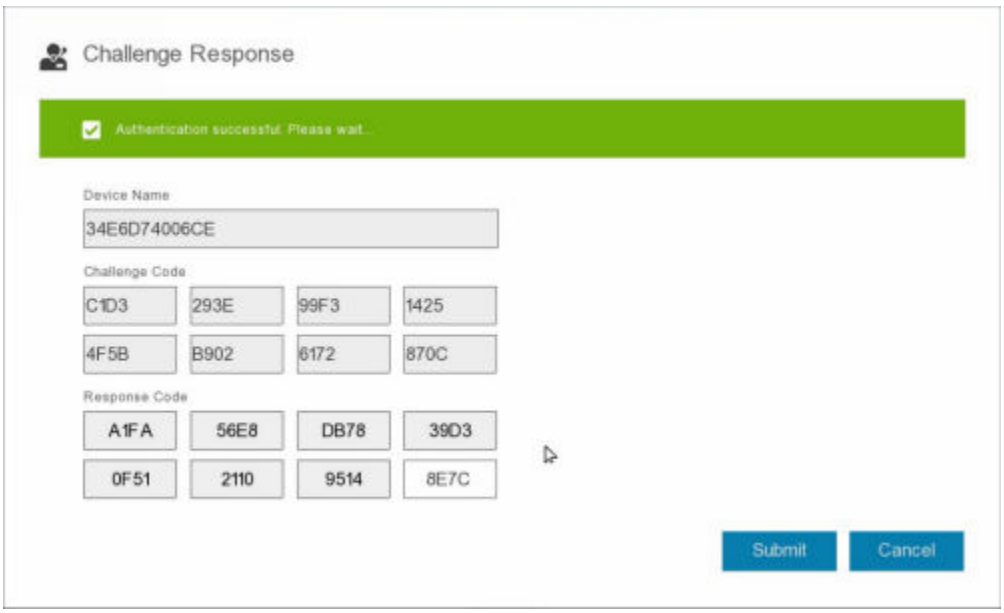


Le code de question est fourni au technicien du centre d'assistance qui entre les données, puis clique sur le bouton **Générer une réponse**.



Les données qui en résultent sont coordonnées par couleur pour vous aider à discerner les caractères numériques (en rouge) et alphabétiques (en bleu). Ces données sont lues à l'utilisateur final, qui les saisit dans l'environnement PBA, puis clique sur le bouton **Soumettre**, ce qui l'amène dans Windows.

Une fois l'authentification effectuée, le message suivant s'affiche :



La récupération à la demande est terminée.

6

Récupération de chiffrement complet du disque et de Dell Encryption

Ce chapitre détaille les étapes de récupération nécessaires pour récupérer l'accès aux fichiers protégés de Dell Encryption sur un disque protégé par un chiffrement complet de disque.

REMARQUE : Un décryptage ne doit pas être interrompu. Si le décryptage est interrompu, vous risquez de perdre des données.

Configuration requise pour la récupération

Pour la récupération de chiffrement complet du disque et de Dell Encryption, vous avez besoin des éléments suivants :

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

Présentation du processus de récupération

REMARQUE : La récupération nécessite un environnement 64 bits.

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 Procurez-vous les fichiers de récupération pour Dell Encryption et le chiffrement complet d'un disque.
3 Procéder à la récupération.

Récupération d'un disque complètement chiffré et d'un disque chiffré Dell

Pour effectuer la récupération d'un disque complètement chiffré et d'un disque chiffré Dell, procédez comme suit.

Obtention du fichier de récupération - Client de cryptage complet du disque

Obtenez le fichier de récupération.

Téléchargez le fichier de récupération à partir de la Console de gestion à distance. Pour télécharger le fichier *<hostname>-sed-recovery.dat* généré à l'installation de Dell Data Security :

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

d Cliquez sur **Créer un fichier de récupération**.
Le fichier **<nom d'hôte> -sed-recovery.dat** est téléchargé.

Obtention du fichier de récupération - Chiffrement basé sur des règles ou client de chiffrement FFE

Pour télécharger le fichier de récupération :

1 Téléchargez le module d'installation de Dell Encryption sur http://www.dell.com/support/home/us/en/19/product-support/product/dell-data-protection-encryption/drivers . Naviguez jusqu'au dossier **AdminUtilities** dans le module d'installation et ouvrez le fichier **CMGAd.exe**.

2 Dans le champ **Serveur Dell**, saisissez le serveur Security Management Server/Security Management Server Virtual sur lequel l'ordinateur a été activé.

3 Dans le champ **Admin Dell**, saisissez un nom de compte d'utilisateur disposant des privilèges de l'administrateur d'analyse.

4 Dans le champ **Mot de passe**, saisissez le mot de passe de l'administrateur d'analyse.

5 Dans le champ **MCID**, saisissez le nom de domaine complet (FQDN) du périphérique en cours de récupération.

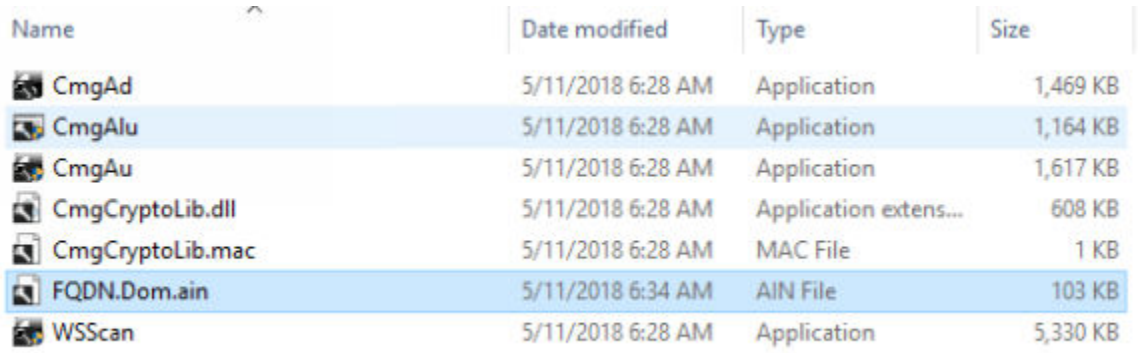
- Le champ **DCID** correspond à l'ID de récupération du périphérique en cours de récupération.

6 Sélectionnez **Suivant**.

7 Définissez, puis confirmez une **phrase de passe** pour le fichier de récupération. Cette phrase de passe est nécessaire pour effectuer la récupération.

8 Dans le champ **Téléchargement vers :**, saisissez un emplacement de destination pour le bundle de récupération, puis sélectionnez **Suivant**. Par défaut, il s'agit du répertoire à partir duquel le fichier CMGAd.exe a été exécuté.

9 Le bundle de récupération se télécharge dans le dossier spécifié dans **Télécharger vers :**.

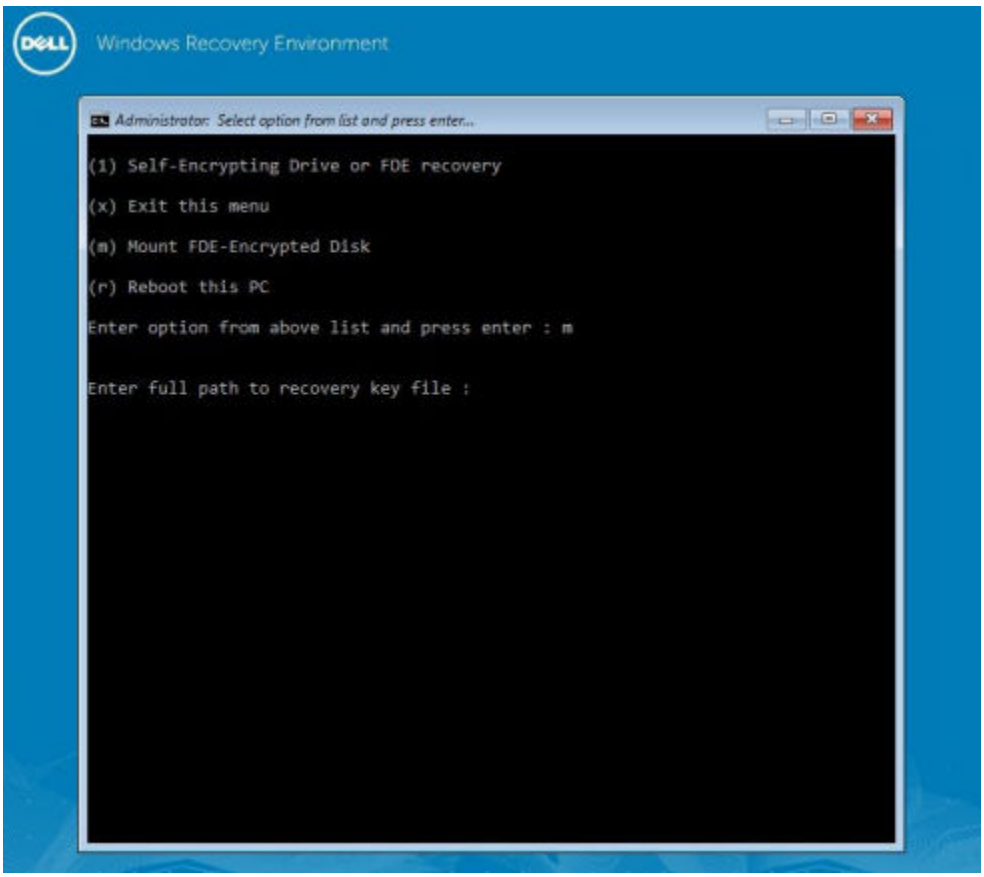


10 Copiez le bundle de récupération à un emplacement accessible au démarrage dans WinPE.

Effectuer une récupération

1 À l'aide du support amorçable créé précédemment, 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.

REMARQUE : Désactivez SecureBoot avant le processus de récupération. Lorsque vous avez terminé, réactivez SecureBoot.



2 Choisissez l'option 3 et appuyez sur **Entrée**.

3 Lorsque vous y êtes invité, saisissez le nom et l'emplacement du fichier récupération.

4 À l'aide de la clé de récupération, le disque complètement chiffré est monté.

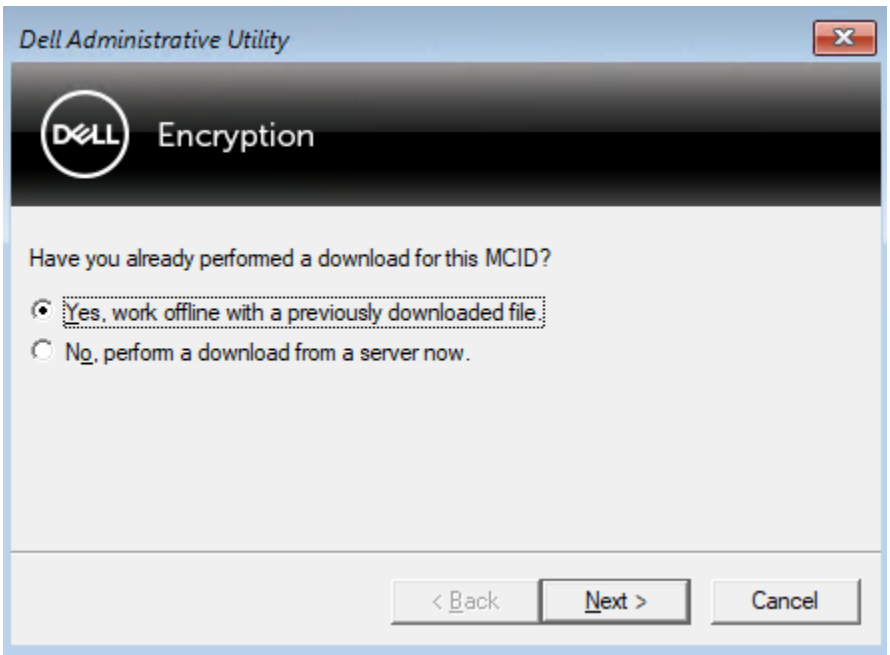
```
Enter option from above list and press enter : m


Enter the full path to the recovery key file: c:\recovery\opalSPKey.DESKTOP-XXYYZZ.recovery.dat


Recoveryfile loaded
====================   Disk 0   ====================
     Cylinders       = 15566
     Tracks/cylinder = 255
     Sectors/track   = 63
     Bytes/sector    = 512
     Disk size       = 128035676160 (Bytes)
                     = 119.24 GB
---> Disk 0, returned status...........: EDriverStatus_Success
====================   Disk 1   ====================
     Cylinders       = 973
     Tracks/cylinder = 255
     Sectors/track   = 63
     Bytes/sector    = 512
     Disk size       = 8004304896 (Bytes)
                     = 7.45 GB
---> Disk 0, returned status...........: EDriverStatus_DriveNotEncrypted
```

.

5 Naviguez jusqu'à l'utilitaire CMGAu.exe à l'aide de la commande suivante : `cd DDPEAdminUtilities\`

6 Lancez-le à l'aide de la commande suivante : `\DDPEAdminUtilities>CmgAu.exe`

Sélectionnez **Oui, travailler hors connexion avec un fichier téléchargé précédemment**.



7 Dans le champ **Fichier téléchargé :**, saisissez l'emplacement du **Bundle de récupération**, puis la **phrase de passe** de l'administrateur d'analyse et sélectionnez **Suivant**.

Une fois l'installation terminée, cliquez sur **Terminer**.

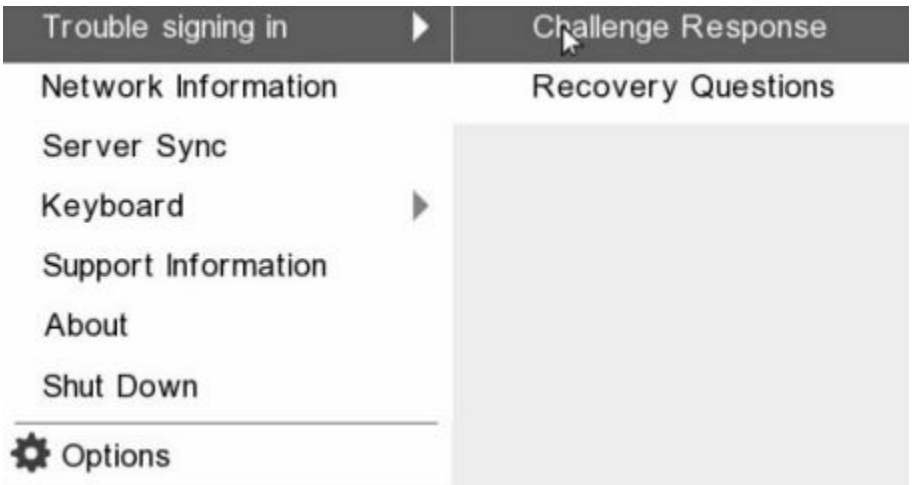
REMARQUE :
Veillez à bien retirer la clé USB ou le CD/DVD utilisé pour amorcer l'ordinateur. Si vous ne le faites pas, vous risquez de redémarrer dans l'environnement de récupération.

8 Après le redémarrage de l'ordinateur, vous devez pouvoir accéder aux fichiers chiffrés. Si le problème persiste, contactez Dell ProSupport.

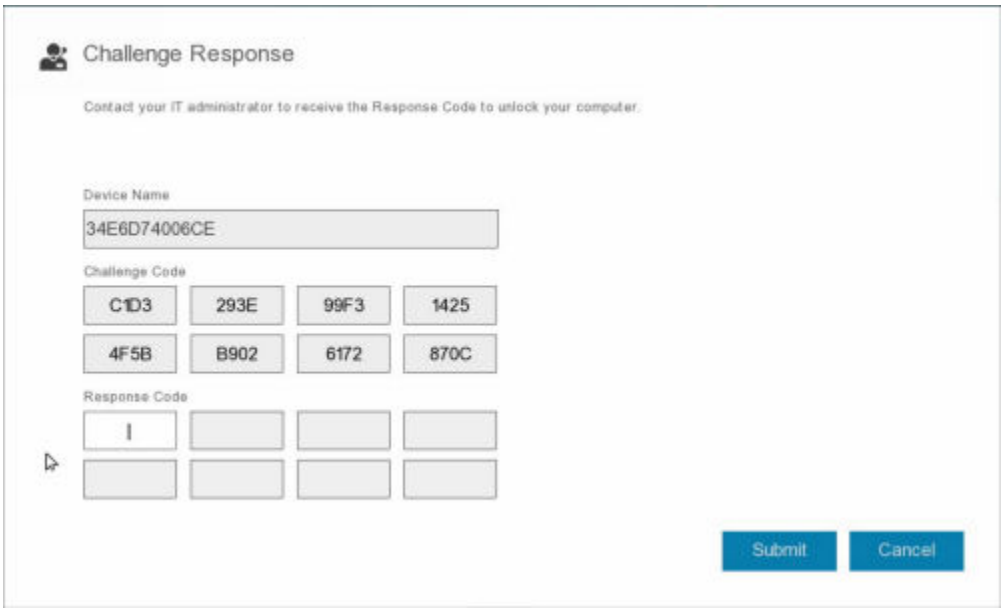
Récupération à la demande avec cryptage complet du disque

Contourner l'environnement d'authentification avant démarrage

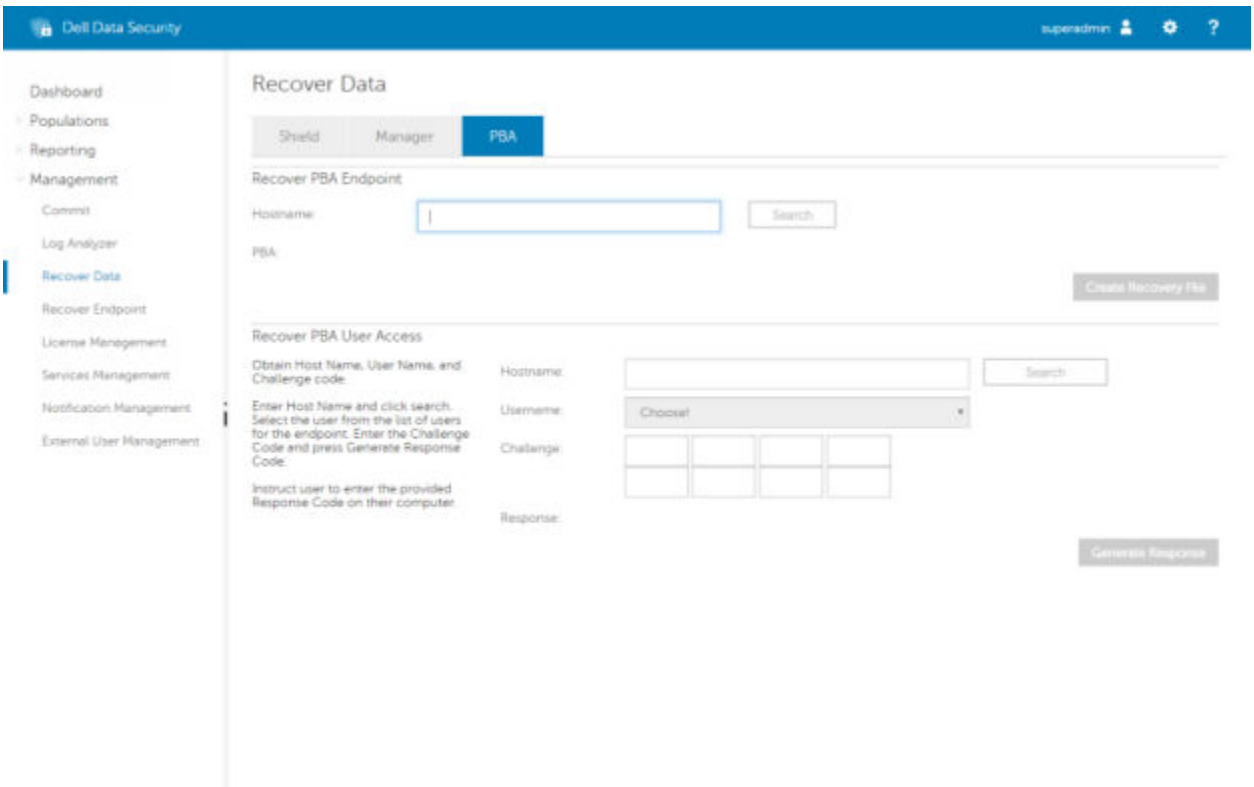
Les utilisateurs oublient leur mot de passe et appellent le centre d'assistance pour savoir comment se connecter à l'environnement PBA. Utilisez le mécanisme de question/réponse intégré à l'appareil. Il est défini pour chaque utilisateur et est basé sur un ensemble tournant de caractères alphanumériques. L'utilisateur doit entrer son nom dans le champ **Nom d'utilisateur**, puis sélectionner **Options > Question/réponse**.



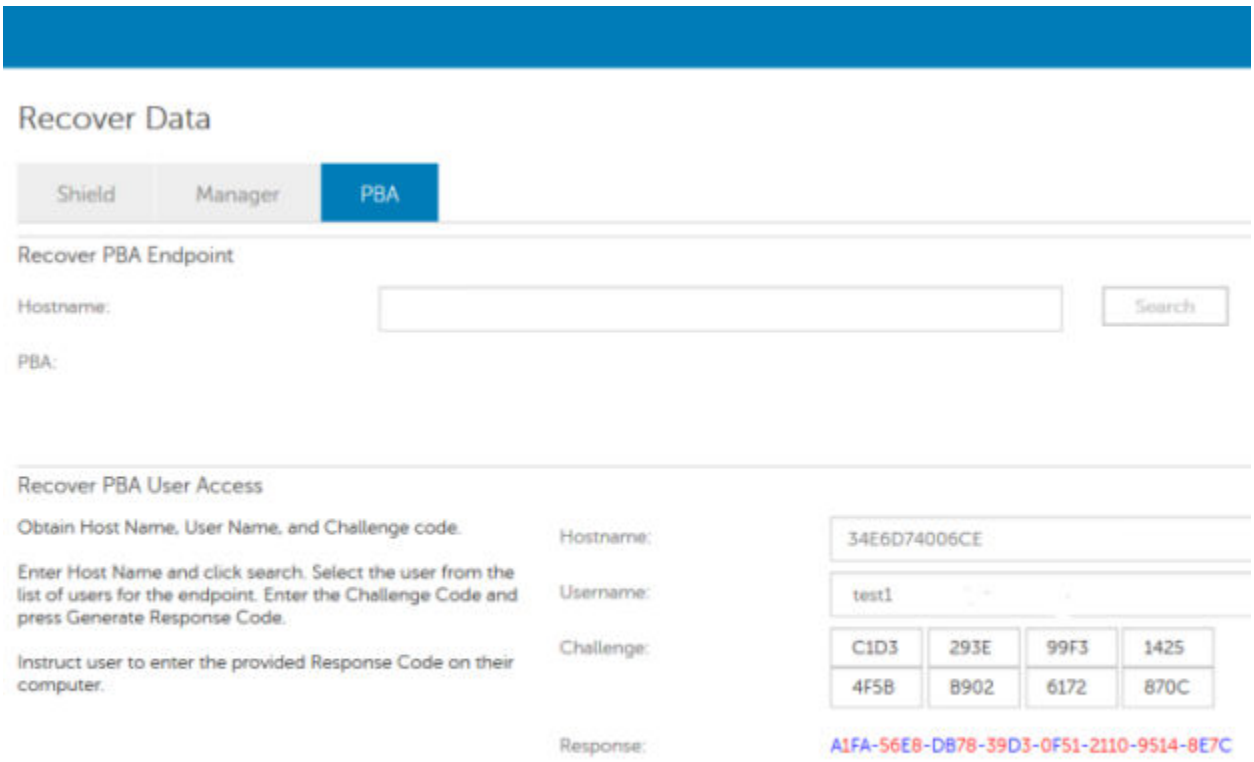
Les informations suivantes s'affichent après avoir sélectionné **Question/réponse**.



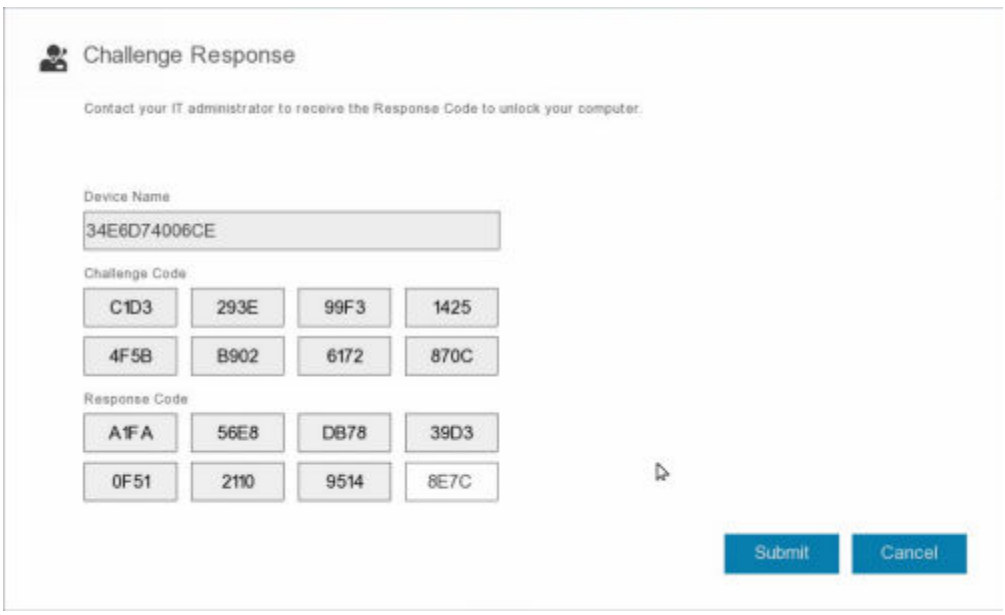
Le champ **Nom de l'appareil** est utilisé par le technicien du centre d'assistance dans la console de gestion à distance pour trouver le bon appareil, qui sélectionne ensuite un nom d'utilisateur. Il se trouve dans **Gestion > Récupérer des données** sous l'onglet **PBA**.



Le code de question est fourni au technicien du centre d'assistance qui entre les données, puis clique sur le bouton **Générer une réponse**.



Les données qui en résultent sont coordonnées par couleur pour vous aider à discerner les caractères numériques (en rouge) et alphabétiques (en bleu). Ces données sont lues à l'utilisateur final, qui les saisit dans l'environnement PBA, puis clique sur le bouton **Soumettre**, ce qui l'amène dans Windows.



Une fois l'authentification effectuée, le message suivant s'affiche :

La récupération à la demande est terminée.

7

Contrôle de périphériques PBA

Le contrôle de périphériques PBA s'applique aux points de terminaison cryptés avec SED ou un cryptage complet du disque.

Utiliser le contrôle de périphériques PBA

Les commandes PBA d'un point de terminaison spécifique sont effectuées dans la zone Contrôle de périphérique PBA. Chaque commande a un ordre de priorité. Les commandes de priorité élevée annulent les commandes de faible priorité figurant dans la file d'attente des commandes à appliquer. Pour obtenir une liste des classements de priorité des commandes, voir *AdminHelp,* disponible en cliquant sur l'icône ? dans la console de gestion à distance. Les contrôles de périphériques PBA sont disponibles sur la page Détails du point de terminaison sur la console de gestion à distance.

Les commandes suivantes sont disponibles dans le contrôle de périphérique PBA :

- **Verrouiller** : verrouille l'écran PBA et interdit à tout utilisateur de se connecter à l'ordinateur.
- **Déverrouiller** : déverrouille l'écran PBA après son verrouillage sur ce point de terminaison, soit par l'envoi d'une commande Verrouiller, soit parce que le nombre maximal de tentatives d'authentification par règle a été dépassé.
- **Supprimer des utilisateurs** : supprime tous les utilisateurs du PBA.
- **Éviter la connexion** : ignore l'écran PBA une seule fois pour donner à un utilisateur l'accès à l'ordinateur sans authentification. L'utilisateur devra quand même se connecter à Windows une fois l'écran PBA contourné.
- **Réinitialiser** : la commande d'effacement déclenche une « restauration de l'état d'usine » pour un lecteur crypté. Vous pouvez utiliser la commande d'effacement pour changer le mode d'utilisation d'un ordinateur ou, en cas d'urgence, pour effacer cet ordinateur afin de rendre les données définitivement irrécupérables. Assurez-vous que c'est bien ce que vous cherchez à faire avant d'exécuter cette commande. Pour un cryptage complet du disque, la commande d'effacement efface le lecteur de manière cryptographique et la PBA est supprimée. Pour SED, la commande d'effacement efface le lecteur de manière cryptographique et la PBA affiche « Appareil verrouillé ». Pour changer le mode d'utilisation du SED, supprimez la PBA avec la récupération du SED.

8

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 Dell.

Récupération de la GPK

Obtention du fichier de récupération

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

1. Ouvrez la console de gestion à distance et, dans le volet gauche, sélectionnez **Gestion** > **Récupérer le point de terminaison**.
2. Dans le champ de recherche, entrez le nom de domaine complet du point de terminaison et cliquez sur **Rechercher**.
3. Dans la fenêtre Récupération, saisissez 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 **<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.

   REMARQUE : Désactivez SecureBoot avant le processus de récupération. Lorsque vous avez terminé, activez SecureBoot.
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.

9

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.

Récupération de 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.

10

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.

Prérequis

- 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.

Récupération de mot de passe Encryption External Media

Encryption External Media 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 Dell 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 **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

Le lecteur doit être réinséré dans la machine qui l'a cryptée à l'origine pour que l'auto-récupération fonctionne. 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. Ce processus peut résoudre certains problèmes avec des supports partiellement corrompus.

1 Connectez-vous à un poste de travail chiffré par Dell Data Security 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.

12

Récupération de Dell Data Guardian

Cet outil de récupération offre les fonctionnalités suivantes :

- Le déchiffrement de :
  - Fichiers Office protégés avec n'importe quel format pris en charge. Les fichiers qui sont protégés par le chiffrement de document Office protégé de Data Guardian et la protection de son fournisseur de services Cloud peuvent être récupérés.
  - Formats de fichiers répertoriés dans la stratégie de protection de fichiers de base, si l'option est activée.
- Mise en dépôt manuelle 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

REMARQUE :
Vous pouvez utiliser l'outil de récupération Windows sur les fichiers créés sur Mac, sur un appareil mobile ou sur des plates-formes du portail Web.

Pré-requis

Les conditions préalables comprennent :

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

Récupération de Data Guardian

Procédez comme suit pour effectuer une récupération de documents Office protégés par Data Guardian. Vous pouvez récupérer un ordinateur à la fois.

IMPORTANT:
Afin d'éviter de perdre du contenu en cas de corruption, déchiffrez les copies de fichiers, non les fichiers originaux.

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

IMPORTANT:
En tant qu'administrateur, assurez-vous de ne copier que le fichier **RecoveryTools.exe** et non le programme d'installation. Le fichier **RecoveryTools.exe** fonctionne mieux si aucune analyse ni aucun déchiffrement n'est en cours d'exécution.

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

3 Dans la fenêtre Outil de récupération Data Guardian, sélectionnez **Connexion au domaine**.

REMARQUE :
L'option Connexion SaaS pour une solution hébergée sera disponible sur une version ultérieure.

4 Entrez le nom de domaine complet (FQDN) Serveur Dell au format suivant :
server.domain.com

REMARQUE :
Un préfixe et un suffixe sont automatiquement ajoutés au nom de domaine complet (FQDN).

5 Entrez le nom d'utilisateur et le mot de passe, puis cliquez sur **Connexion**.

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

REMARQUE :
Si vous n'êtes pas un administrateur d'analyse approfondie et que vous entrez des informations d'identification, un message s'affiche et vous indique que vous ne disposez pas des droits de connexion.

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

7 Sélectionnez **Source**.

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

8 Cliquez sur **Parcourir** pour sélectionner le dossier ou le lecteur à récupérer.

9 Cliquez sur **OK**.

10 Cliquez sur **Destination**, un dossier vide pour les fichiers déchiffrés ou récupérés.

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

12 Cliquez sur **OK**.

13 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 Dell Server. • 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.
Décrypter	Pointez l'outil de récupération vers un répertoire qui contient des documents Office protégés pour les déchiffrer. **REMARQUE :** Il est conseillé de déchiffrer les copies des fichiers, et non les originaux, en cas de corruption.

Options	Description
	Vous pouvez également, en cas d'altération, sélectionner l'une de ces options ou les deux (voir ci-dessous pour plus d'informations) : • **Vérification de l'altération** : vérifie les altérations potentielles des fichiers, sans les chiffrer. • **Vérification de l'altération** et **Déchiffrement forcé, même en cas d'altération** : vérifient si les fichiers et si 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 **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 ajoute un fichier texte avec une liste de tous les auteurs à un dossier *HiddenWatermark* dans les journaux.

14 Une fois les sélections terminées, cliquez sur **Analyser**.

La zone Log (Journal) affiche :

- Les dossiers identifiés et analysés dans la source sélectionnée
- Si un déchiffrement, par fichier, a réussi ou a échoué.
- Le nom du dernier auteur d'un fichier

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

Afficher des données d'une piste d'audit cachée

Pour Windows, si la stratégie de piste d'audit cachée pour les documents Office protégés est activée, les informations de l'utilisateur sont capturées dans les métadonnées du fichier. Pour afficher ces données, utilisez l'outil de récupération :

1 Lancez l'outil de récupération.
   - Pour la **source**, naviguez jusqu'à un dossier qui contient les documents Office protégés avec des données d'audit cachées. L'outil de récupération copie la structure du dossier et du sous-dossier, en décryptant les documents Office protégés qui contiennent des données d'audit cachées.
   - Avant de rechercher une **destination**, vous pouvez créer un dossier Fichiers décryptés, puis accéder à ce dernier.

2 Sélectionnez **Décrypter**.

3 Une fois les sélections terminées, cliquez sur **Analyser**.

Le dossier sélectionné comme destination contient un dossier *Fichiers récupérés* daté avec les éléments suivants :

- des fichiers Office protégés décryptés,
- un dossier *Piste d'audit*, créé par l'outil de récupération, avec un fichier .txt pour chaque fichier décrypté. Chaque fichier .txt possède un journal qui répertorie des informations du fichier déchiffré, notamment les auteurs, le dernier auteur, les horodatages.

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 une clé USB amorçable, suivez les instructions suivantes :

Amorçage hérité :

1 Connectez un lecteur USB au système.
2 Ouvrez une invite de commande d'administration.
3 Entrez dans l'utilitaire Diskpart en saisissant **diskpart**.
4 Trouvez le disque cible à modifier en saisissant **list disk**. Les disques seront désignés par numéro.
5 Sélectionnez le disque approprié à l'aide de la commande **select disk #**, où # est le numéro de disque du lecteur correspondant indiqué par l'étape précédente.
6 Effacez le disque en exécutant une commande **clean**. Cela purgera le lecteur des données en effaçant la table des fichiers.
7 Créez une partition pour accueillir l'image de démarrage.
   a La commande **create partition primary** génère une partition principale sur le lecteur.
   b La commande **select partition 1** sélectionne la nouvelle partition.
   c Utilisez la commande suivante pour formater rapidement le lecteur avec le système de fichiers NTFS : **format FS=NTFS quick**.
8 Le lecteur doit être marqué comme lecteur amorçable. Utilisez la commande **active** pour marquer le lecteur comme amorçable.
9 Pour déplacer des fichiers directement sur le disque, attribuez une lettre disponible au lecteur avec la commande **assign**.
10 Le lecteur sera monté automatiquement, et le contenu du fichier ISO pourra être copié à la racine du lecteur.

Une fois que le contenu du fichier ISO a été entièrement copié, le lecteur est amorçable et peut être utilisé pour la récupération.

Démarrage UEFI :

1 Connectez un lecteur USB au système.
2 Ouvrez une invite de commande d'administration.
3 Entrez dans l'utilitaire Diskpart en saisissant **diskpart**.
4 Trouvez le disque cible à modifier en saisissant **list disk**. Les disques seront désignés par numéro.

5 Sélectionnez le disque approprié à l'aide de la commande **select disk #**, où # est le numéro de disque du lecteur correspondant indiqué par l'étape précédente.

6 Effacez le disque en exécutant une commande **clean**. Cela purgera le lecteur des données en effaçant la table des fichiers.

7 Créez une partition pour accueillir l'image de démarrage.

   a La commande **create partition primary** génère une partition principale sur le lecteur.

   b La commande **select partition 1** sélectionne la nouvelle partition.

   c Utilisez la commande suivante pour formater rapidement le lecteur avec le système de fichiers FAT32 : **format FS=FAT32 quick**.

8 Le lecteur doit être marqué comme lecteur amorçable. Utilisez la commande **active** pour marquer le lecteur comme amorçable.

9 Pour déplacer des fichiers directement sur le disque, attribuez une lettre disponible au lecteur avec la commande **assign**.

10 Le lecteur sera monté automatiquement, et le contenu du fichier ISO pourra être copié à la racine du lecteur.

Une fois que le contenu du fichier ISO a été entièrement copié, le lecteur est amorçable et peut être utilisé pour la récupération.