SOPHOS
Security made simple.

SafeGuard Enterprise
Guide des outils

Version du produit : 6.1
Date du document : février 2014

Table des matières

1 À propos de ce guide

Ce guide aborde l'utilisation des outils de chiffrement mis à disposition pour les ordinateurs d'extrémité protégés par SafeGuard Enterprise.

Retrouvez les outils dans le répertoire Tools de votre logiciel client SafeGuard Enterprise. Les outils suivants sont fournis :

- Outil SGNState : affiche l'état du système
- Outil SGNRollback : annule les installations en échec
- Outil de récupération de clé RecoverKeys.exe : récupère l'accès aux ordinateurs lorsque l'authentification au démarrage est corrompue
- Outil de récupération be_restore.exe : récupère les systèmes de chiffrement du disque SafeGuard sur Windows 7 (Master Boot Record)
- Outil de récupération BLCRBackupRestoren.exe : récupère les systèmes Bitlocker sur Windows 8 (sauvegarde du contenu ESP, récupération de la sauvegarde et réparation de l'ordre d'initialisation de NVRam)
- Outil de mise hors service beinvvol.exe : met hors service les volumes chiffrés
- Outil de mise hors service opalinvdisk.exe : met hors service les disques durs à auto-chiffrement et conformes à Opal

À qui s'adresse ce guide ?

Ce guide s'adresse aux administrateurs utilisant SafeGuard Enterprise et agissant en tant que responsables de la sécurité.

2 Affichage de l'état du système avec SGNState

SafeGuard Enterprise propose l'outil de ligne de commande SGNState pour afficher des informations sur l'état actuel (état du chiffrement et autres informations détaillées sur l'état) de l'installation SafeGuard Enterprise sur un ordinateur d'extrémité.

Rapports

`SGNState` peut également être utilisé comme suit :

- Le code renvoyé par **`SGNState`** peut être évalué sur le serveur à l'aide d'outils de gestion tiers.
- **`SGNState /LD`** renvoie un résultat formaté pour LANDesk pouvant être inscrit dans un fichier.

Paramètres

Vous pouvez appeler l'outil SGNState avec les paramètres suivants :

`SGNState [/?|H] [H/Type|Status] [/L] [/LD]`

- Le paramètre **`/?`** renvoie des informations d'aide sur les paramètres de ligne de commande SGNState disponibles.
- Le paramètre **`/H Type`** renvoie des informations d'aide sur les types de lecteur.
- Le paramètre **`/H Status`** renvoie des informations d'aide sur l'état des lecteurs.
- Le paramètre **`/L`** affiche les informations suivantes :

  Système d'exploitation
  Version installée de Sophos SafeGuard
  Type d'authentification au démarrage [SGN | Opal | BitLocker | C/R BitLocker | unknown or earlier version of SGN]
  Authentification au démarrage [yes | no | n/a]
  WOL (état de l'éveil par appel réseau) [yes | no | n/a]
  Nom du serveur
  Nom du second serveur
  Mode de connexion [SGN, no automatic logon | UID/PW | TOKEN/PIN | FINGERPRINT | BL (BitLocker)]
  État d'activation du client [ENTERPRISE | OFFLINE]
  Dernière réplication de données [date, time]
  Connexion au token par certificat appliquée à l'authentification au démarrage [yes | no | n/a]
  Code renvoyé [return code]
  Informations sur le volume :

Nom	Type	État	Algorithme

<nom>	[HD-Part | ...]	[encrypted | not encrypted | ...]	[<nom de l'algorithme> | n/a | ...]
	...	...	
	FLOPPY	inaccessible	
	REMOV.PART	interrompu en raison d'un échec	
	REM_PART	démarrage du chiffrement	
	HD-PART	chiffrement en cours	
	UNKNOWN	démarrage du déchiffrement	
		déchiffrement en cours	
		non préparé	

- Le paramètre **/LD** renvoie ces informations formatées pour LANDesk

  La sortie est semblable à la sortie **/L**, mais commence par :

  Sophos SafeGuard -
  différent format des informations sur le volume :
  Sophos SafeGuard - État du chiffrement <nom> = [encrypted | not encrypted | not prepared...]

- **Code renvoyé :**

  Bit 0 : il y a au moins un volume chiffré
  Bit 1 : le chiffrement/déchiffrement est en cours
  0 : aucun volume n'a été chiffré
  -1 : une erreur s'est produite (par exemple, aucun chiffrement de périphériques SGN n'est installé)

3 Annulation d'une installation en échec avec SGNRollback

Remarque : l'outil SGNRollback doit uniquement être utilisé avec Windows 7 sans BitLocker.

En cas d'échec d'installation de SafeGuard Enterprise sur un ordinateur d'extrémité, il se peut que l'ordinateur ne soit pas en mesure de démarrer et que son administration à distance soit impossible.

SGNRollback peut réparer une installation SafeGuard Enterprise infructueuse sur un ordinateur d'extrémité si les conditions suivantes s'appliquent :

- L'authentification au démarrage se bloque au premier démarrage et l'ordinateur ne peut plus être initialisé.
- Le disque dur n'est pas chiffré.

SGNRollback permet d'annuler automatiquement les effets de l'échec d'une installation de SafeGuard Enterprise en :

- Permettant l'initialisation de l'ordinateur bloqué
- Supprimant SafeGuard Enterprise
- Annulant les modifications des composants d'autres systèmes d'exploitation.

Démarrez SGNRollback à partir d'un système de récupération Windows (soit WindowsPE, soit BartPE).

3.1 Conditions préalables

L'utilisation de SGNRollback nécessite l'application des conditions préalables suivantes :

- SGNRollback fonctionne avec les systèmes de récupération WinPE et BartPE. Pour pouvoir utiliser SGNRollback à des fins de récupération, vous devez l'intégrer au système de récupération requis. Retrouvez plus d'informations dans la documentation du système de récupération correspondant.

  Si SGNRollback doit être exécuté par le programme de démarrage automatique, l'administrateur utilisant SGNRollback doit définir les paramètres correspondants dans WinPE (section Activation du programme de démarrage automatique de SGNRollback pour Windows PE à la page 7) ou dans BartPE (section Activation du programme de démarrage automatique de SGNRollback pour BartPE à la page 7).

- Le chiffrement intégral du disque de SafeGuard Enterprise est installé.

Remarque : la migration de SafeGuard Easy vers SafeGuard Enterprise n'est pas prise en charge.

3.2 Démarrage de SGNRollback dans le système de récupération

Vous pouvez démarrer SGNRollback manuellement ou l'ajouter au programme de démarrage automatique du système de récupération.

3.2.1 Activation du programme de démarrage automatique de SGNRollback pour Windows PE

Pour activer le programme de démarrage automatique de SGNRollback pour Windows PE, installez le kit d'installation automatisée (Windows AIK). Vous trouverez des informations sur la façon de concevoir un environnement Windows PE et d'exécuter automatiquement une application dans le guide de l'utilisateur de l'environnement de préinstallation Windows.

3.2.2 Activation du programme de démarrage automatique de SGNRollback pour BartPE

1. Utilisez la version 3.1.3 ou supérieure de BartPEBuilder pour créer une image PE. Retrouvez plus d'informations dans la documentation BartPE.
2. Dans BartPE Builder, ajoutez le dossier de l'outil de récupération dans le champ **Personnaliser**.
3. Créez l'image.
4. Copiez le fichier AutoRun0Recovery.cmd à partir du support SafeGuard Enterprise dans le dossier i386 de la version BartPE pour Windows.
5. Créez une commande AutoRun0Recovery.cmd à l'aide des deux lignes de texte suivantes :

   ```
   \Recovery\recovery.exe
   ```

   ```
   exit
   ```

6. Exécutez l'outil PEBuilder depuis la ligne de commande :

   ```
   Pebuilder -buildis
   ```

   Une nouvelle image iso est créée qui intègre le fichier de démarrage automatique.

7. Enregistrez l'image obtenue sur un support de récupération.

Au moment d'initialiser cette image, SGNRollback démarre automatiquement.

3.3 Paramètres

SGNRollback peut être démarré à l'aide du paramètre suivant :

`-drv WinDrive`	Indique la lettre du lecteur sur lequel l'installation SafeGuard Enterprise devant faire l'objet d'une réparation est installée. Ce paramètre ne peut être utilisé qu'en mode récupération. Il doit être utilisé

	dans des environnements à démarrage multiple pour signaler le bon lecteur.

3.4 Annulation d'une installation non réussie

Pour annuler les effets d'une installation non réussie de SafeGuard Enterprise sur un ordinateur d'extrémité, procédez comme suit :

1. Démarrez l'ordinateur à partir du support de récupération contenant le système de récupération, notamment SGNRollback.
2. Démarrez SGNRollback dans le système de récupération. Si le programme de démarrage automatique est présent, SGNRollback démarrera automatiquement. SGNRollback prépare le système d'exploitation pour la désinstallation de SafeGuard Enterprise.
3. Le système vous demande de retirer le support de récupération. Après avoir retiré le support, le système d'exploitation de l'ordinateur est réinitialisé en mode sans échec.

Toutes les modifications effectuées sont supprimées et SafeGuard Enterprise est désinstallé.

4 Récupération de l'accès aux ordinateurs à l'aide de l'outil KeyRecovery

L'outil KeyRecovery sert à récupérer l'accès à l'ordinateur dans des situations complexes de récupération d'urgence, par exemple lorsque l'authentification au démarrage est corrompue et que l'ordinateur doit être initialisé à partir du disque de récupération SafeGuard. L'outil est démarré dans le contexte d'une procédure de Challenge/Réponse.

Remarque : retrouvez une description détaillée de cet outil dans le *Manuel d'administration de SafeGuard Enterprise* à la section *Challenge/Réponse à l'aide de clients virtuels*.

5 Récupération des système de chiffrement intégral du disque SafeGuard avec be_restore.exe

Remarque : la description suivante se rapporte aux ordinateurs d'extrémité BIOS Windows protégés par le chiffrement intégral du disque SafeGuard Enterprise à l'aide de l'authentification au démarrage SafeGuard.

SafeGuard Enterprise chiffre les fichiers et les lecteurs de façon transparente. Les lecteurs d'initialisation peuvent également être chiffrés et les fonctions de déchiffrement telles que le code, les algorithmes de chiffrement et la clé de chiffrement doivent être disponibles très tôt au cours de la phase d'initialisation. C'est la raison pour laquelle les informations chiffrées ne sont pas accessibles si les modules essentiels de SafeGuard Enterprise ne sont pas disponibles ou ne fonctionnent pas.

5.1 Récupération d'un MBR corrompu

La fonction d'authentification au démarrage de SafeGuard Enterprise est chargée à partir du MBR du disque dur d'un ordinateur. Lorsque l'installation est terminée, SafeGuard Enterprise enregistre une copie de l'original (tel qu'il était avant l'installation de SafeGuard Enterprise) dans son noyau, et modifie le chargeur de PBR à partir de LBA 0. Dans son LBA 0, le MBR modifié contient l'adresse du premier secteur du noyau SafeGuard Enterprise et sa taille totale.

Les problèmes associés au MBR peuvent être résolus avec l'outil de récupération de SafeGuard Enterprise, **`be_restore.exe`**. Cet outil est une application Win32 qui doit être exécutée sous Windows et non sous DOS.

Un chargeur MBR défectueux signifie que le système ne peut pas être initialisé. Il existe deux manières de le récupérer :

- Récupération du MBR à partir d'une sauvegarde.
- Réparation du MBR.

Pour récupérer un MBR corrompu, procédez comme suit :

1. Nous vous conseillons de créer un CD-ROM d'initialisation Windows PE (environnement préinstallé).
2. Pour utiliser l'outil de récupération **`be_restore.exe`**, plusieurs fichiers supplémentaires sont nécessaires. L'outil et les fichiers nécessaires sont disponibles dans le répertoire **`Tools\KeyRecovery and restore`** de votre logiciel SafeGuard Enterprise. Copiez tous les fichiers de ce dossier sur une carte mémoire. Veillez à enregistrer tous les fichiers dans **le même** dossier sur votre carte mémoire. Cette condition est nécessaire au démarrage correct de l'outil de restauration.

   Remarque : pour démarrer **`be_restore.exe`** dans un environnement Windows PE, le fichier Windows OLEDLG.dll est requis. Ce fichier n'est pas inclus dans le dossier **`Tools\KeyRecovery and restore`**. Ajoutez ce fichier depuis une installation Windows dans le dossier des outils de récupération sur votre CD-ROM de récupération.

3. Si nécessaire, modifiez la séquence d'initialisation dans le BIOS et sélectionnez le CD-ROM en priorité.

Remarque : l'outil **`be_restore.exe`** peut uniquement récupérer ou réparer le MBR sur le disque 0. Si vous utilisez deux disques durs et que le système est démarré à partir de l'autre disque dur, le MBR ne pourra ni être récupéré ni être réparé. Cette condition s'applique également lors de l'utilisation d'un disque dur amovible.

5.1.1 Récupération d'une sauvegarde MBR précédemment enregistrée

Chaque ordinateur d'extrémité SafeGuard Enterprise enregistre le secteur de démarrage principal (MBR) SafeGuard Enterprise de son **propre ordinateur** (LBA 0 du disque dur d'initialisation après avoir été modifié par SafeGuard Enterprise) dans la base de données SafeGuard Enterprise. Il peut être exporté dans un fichier à partir de SafeGuard Management Center.

Pour récupérer une sauvegarde du secteur de démarrage principal (MBR) précédemment enregistrée :

1. Dans SafeGuard Management Center, cliquez sur **Utilisateurs et ordinateurs**, puis sélectionnez l'ordinateur approprié dans la zone de navigation.
2. Cliquez avec le bouton droit de la souris et sélectionnez **Propriétés** > **Paramètres machine** > **Sauvegarder** > **Exporter** pour exporter le secteur de démarrage principal (MBR). Cette action génère un fichier de 512 octets portant l'extension .BKN, qui contient le secteur de démarrage principal (MBR).
3. Copiez ce fichier dans le dossier de la carte mémoire dans lequel se trouvent les autres fichiers SafeGuard Enterprise.
4. Insérez maintenant le CD-ROM de démarrage Windows PE dans le lecteur, connectez la carte mémoire contenant les fichiers SafeGuard Enterprise et démarrez l'ordinateur à partir du CD.
5. Lorsque l'ordinateur est prêt, lancez cmd-box, naviguez jusqu'au répertoire de la carte mémoire contenant les fichiers SafeGuard Enterprise et exécutez **`be_restore.exe`**.
6. Sélectionnez **Restaurer le MBR** pour récupérer à partir d'une sauvegarde et sélectionnez le fichier .BKN.

L'outil vérifie à présent si le fichier .BKN sélectionné correspond à l'ordinateur, puis récupère le MBR sauvegardé.

5.1.2 Réparation du MBR sans sauvegarde

Même si aucun fichier de sauvegarde MBR n'est disponible localement, **`be_restore.exe`** peut réparer un chargeur MBR corrompu. **`be_restore.exe`** - **Réparer le MBR** recherche le noyau SafeGuard Enterprise sur le disque dur, utilise son adresse et recrée le chargeur MBR.

Cette procédure présente de très grands avantages, car aucun fichier de sauvegarde MBR spécifique à l'ordinateur n'a besoin d'être disponible en local. Toutefois, elle dure un peu plus longtemps en raison de la recherche effectuée sur le noyau SafeGuard Enterprise se trouvant sur le disque dur.

Pour utiliser la fonction de réparation, procédez selon les instructions, mais sélectionnez **Réparer le MBR** à l'exécution de **`be_restore.exe`**.

Si plusieurs noyaux existent, **`be_restore.exe`** – **Réparer le MBR** utilise celui dont l'estampille temporelle est la plus récente.

5.1.3 Table de partition

SafeGuard Enterprise permet de créer de nouvelles partitions principales ou étendues. Cette action modifie la table de partition du disque dur sur lequel se trouve la partition.

Lors de la restauration d'une sauvegarde MBR, l'outil sait si le MBR actuel contient des tables de partition différentes pour le LBA 0 et quel fichier de sauvegarde MBR (*.BKN) doit être récupéré. Dans une boîte de dialogue, vous pouvez sélectionner la procédure requise.

5.1.3.1 Réparation d'un MBR avec une table de partition corrompue

Une table de partition corrompue peut empêcher l'initialisation du système d'exploitation après une connexion d'authentification au démarrage réussie.

Vous pouvez résoudre ce problème en utilisant be_restore.exe pour récupérer un secteur de démarrage (MBR) précédemment enregistré ou réparer le MBR sans sauvegarde MBR.

Si vous avez une sauvegarde, procédez tel que décrit pour l'option **Restaurer le MBR**.

Si vous n'avez pas de sauvegarde, procédez comme suit :

1. Insérez le CD-ROM de démarrage Windows PE dans le lecteur, connectez la carte mémoire contenant les fichiers SafeGuard Enterprise et démarrez l'ordinateur à partir du CD-ROM.
2. Lorsque l'ordinateur est prêt, à partir de l'invite de commandes, naviguez jusqu'au répertoire de la carte mémoire contenant les fichiers SafeGuard Enterprise et exécutez **`be_restore.exe`**.
3. Sélectionnez **Réparer le MBR**. Si be_restore.exe détecte une différence entre la table de partition du MBR actuel et celle du MBR en miroir, une boîte de dialogue permettant de sélectionner la table de partition à utiliser s'affiche.

   Le MBR en miroir correspond au MBR Microsoft d'origine enregistré durant la configuration du client SafeGuard Enterprise afin de vous permettre de le restaurer, par exemple, en cas de désinstallation du client. La table de partition de ce MBR en miroir est mise à jour par SafeGuard Enterprise si un changement survient dans Windows au niveau de la partition.
4. Sélectionnez **À partir du MBR en miroir**.

   Remarque :

   Si vous sélectionnez **À partir du MBR actuel**, la table de partition du MBR actuel sera utilisée, (dans ce cas, une table de partition corrompue). Non seulement le système ne pourra toujours pas être initialisé, mais le MBR en miroir sera mis à jour et par conséquent corrompu.

5.1.4 Signature de disque Windows

Chaque fois que Windows crée un système de fichiers pour la première fois sur un disque dur, il l'associe à une signature. Cette signature est enregistrée dans le MBR du disque dur (offsets 0x01B – 0x01BB). Notez que, par exemple, les lettres d'unités logiques du disque dur dépendent de la signature de disque Windows.

Veuillez ne pas changer la signature du disque. Par exemple, en utilisant ("FDISK/MBR"). Autrement, Windows entrera dans un mode de contrôle du disque très long au prochain démarrage et récupérera la liste des lecteurs.

Chaque fois que cela se produit sous SafeGuard Enterprise, le pilote du filtre SafeGuard Enterprise "BEFLT.sys" n'est pas chargé. L'initialisation du système est ainsi impossible : l'ordinateur affiche un écran bleu « STOP 0xED "Unmountable Boot Volume" ».

Pour effectuer les réparations sous SafeGuard Enterprise, la signature de disque Windows originale doit être récupérée sur le secteur de démarrage principal (MBR) du disque dur.

L'utilitaire **`be_restore.exe`** effectue cette tâche.

Remarque : n'utilisez surtout pas d'autres outils pour réparer le secteur de démarrage principal (MBR). Par exemple, un ancien MS DOS FDISK.exe que vous utilisez pour réécrire le chargeur MBR («FDISK /MBR») peut créer un autre chargeur du secteur de démarrage principal (MBR) sans signature de disque Windows. De même que pour la suppression de la signature du disque Windows, le « nouveau » chargeur du secteur de démarrage principal (MBR) créé par un ancien outil ne sera probablement pas compatible avec les différentes tailles de disque dur généralement utilisées aujourd'hui. Utilisez toujours les versions les plus récentes des outils de réparation.

5.1.5 Secteur d'initialisation

Au cours du processus de chiffrement, le secteur d'initialisation d'un volume est remplacé par le secteur d'initialisation de SafeGuard Enterprise. Le secteur de démarrage de SafeGuard Enterprise contient des informations sur l'emplacement du KSA principal ou sa sauvegarde en clusters et sur les secteurs en rapport avec le démarrage de la partition et la taille du KSA. Même si le secteur d'initialisation de SafeGuard Enterprise est endommagé, les volumes chiffrés sont inaccessibles. L'utilitaire be_restore peut récupérer le secteur d'initialisation endommagé.

6 Récupération des systèmes de Challenge/Réponse Windows UEFI BitLocker avec BLCRBackupRestoren.exe

Pour récupérer les systèmes Windows UEFI BitLocker, Sophos met à disposition l'outil de récupération BLCRBackupRestoren.exe. Cet outil vous permet de :

- Sauvegarder les données Challenge/Réponse de BitLocker

  Remarque : cette opération est uniquement nécessaire en cas d'échec de la sauvegarde automatique (événement du journal 3071 : "La sauvegarde de clé n'a pas pu être enregistrée dans le partage réseau spécifié.")

- Récupérer manuellement une ancienne sauvegarde et réparer l'ordre d'initialisation de NVRAM.

  Remarque : cette opération s'avère uniquement nécessaire si vous pensez que les données Challenge/Réponse de BitLocker sont corrompues ou ont été supprimées.

  BLCRBackupRestoren.exe doit être redémarré à partir d'un environnement Windows PE. Il est disponible sur le CD-ROM du client virtuel Sophos.

6.1 Démarrage de l'outil de ligne de commande

Syntaxe

```
blcrbackuprestoren [-?] [-B [-T <Chemin du fichier>]] [-R [-K
<Nom du fichier>] [-S <Nom du fichier>]] [-I] [-D]
```

Options

- **`-?`**

  Afficher l'aide

- **`-B`**

  Sauvegarder

- **`-T <Chemin du fichier>`**

  Chemin cible existant en option

- **`-R`**

  Récupérer

- **`-K <Nom du fichier>`**

  Chemin\Nom du fichier de clé en option

  Le fichier de clé en option est le fichier .BKN qui doit être exporté à partir de SafeGuard Management Center.

Procédez à l'exportation de la manière suivante :

- Dans SafeGuard Management Center, cliquez sur **Utilisateurs et ordinateurs**, puis sélectionnez l'ordinateur approprié dans la zone de navigation.
- Cliquez avec le bouton droit de la souris et sélectionnez **Propriétés** > **Paramètres machine** > **Sauvegarder** > **Exporter**.

Si les données de Challenge/Réponse BitLocker ont été sauvegardées avec succès, l'utilisation de l'option **`-R`** est suffisante.

- **`-S <Nom du fichier>`**

  Chemin\Nom de fichier de la source en option

- **`-I`**

  Installer l'entrée d'initialisation.

- **`-D`**

  Supprimer l'entrée d'initialisation.

Exemples

- **Sauvegarder**
  - **`blcrbackuprestoren -b`** crée une archive à l'emplacement par défaut.
  - **`blcrbackuprestoren -b -T <USBStick:\Backup\`** met l'archive sur un lecteur externe.
- **Récupérer**
  - **`blcrbackuprestoren -r`** extrait une archive à l'emplacement par défaut.
  - **`blcrbackuprestoren -r -k X:\exemple\exemple.BKN`** extrait l'archive de l'emplacement par défaut et reconstruit le fichier de clé.

7 Mise hors service des volumes chiffrés avec beinvvol.exe

Pour les ordinateurs protégés par SafeGuard Enterprise, notre outil de ligne de commande **`beinvvol.exe`** peut être utilisé pour mettre hors service en toute sécurité les volumes chiffrés (disques durs, clés USB, etc.). Cet outil de ligne de commande est basé sur la norme DoD 5220.22-M et peut être utilisé pour supprimer des magasins de clés en toute sécurité. Cette norme comporte sept cycles de remplacement avec des modèles aléatoires et alternatifs.

Cet outil de ligne de commande est conçu pour être utilisé sur des ordinateurs sur lesquels s'appliquent les événements suivants :

- SafeGuard Enterprise est installé.
- Certains volumes de disque dur ont été chiffrés.

Vous devez exécuter cet outil au sein d'un système où le pilote de chiffrement SafeGuard Enterprise n'est pas actif. Ceci a pour but d'empêcher que des données soient mises hors service par accident. Sinon, l'outil ne fonctionne pas et un message d'erreur apparaît.

Remarque : nous vous conseillons de démarrer votre système à partir d'un support externe comme un CD-ROM Windows PE et d'utiliser l'outil en fonction des instructions disponibles dans l'aide de la ligne de commande.

Une fois que les volumes cibles correspondants ont été mis hors service, ils ne sont plus lisibles.

Conformément à la norme DoD 5220.22-M, l'outil de ligne de commande purge en permanence les secteurs de démarrage et les zones de stockage des clés de SafeGuard Enterprise (KSA d'origine et sauvegarde) de chaque volume chiffré en les remplaçant sept fois. Les clés de chiffrement de données (DEK) aléatoires de chaque volume n'étant pas sauvegardées dans la base de données centrale des clients SafeGuard Enterprise, les volumes sont alors parfaitement hermétiques. Même un responsable de sécurité ne peut y accéder.

L'outil de ligne de commande affiche également à l'écran des informations concernant les volumes disponibles. Ceci inclut, par exemple, le nom du volume, la taille du volume et les informations concernant les secteurs de démarrage et les KSA. Ces informations peuvent également être stockées dans un fichier. Le chemin de ce fichier doit, bien sûr, diriger vers un volume qui n'a pas été mis hors service.

Remarque : les données ne peuvent pas être récupérées après suppression.

7.1 Démarrage de l'outil de ligne de commande

Syntaxe

- **`xl[volume]`**

  Répertorier les informations du ou des volumes cibles. Répertorier les informations concernant tous les volumes si aucun volume cible n'est spécifié.

- **`xi<volume>`**

Invalider le(s) volume(s) cible(s), en cas de chiffrement SGN complet. Le <volume> cible doit être spécifié pour cette commande.

- **<volume>**

  Indiquer le volume cible = {a, b, c, ..., z, *}, <*> correspondant à l'ensemble des volumes.

Options

- **-g0**

  Désactiver le mécanisme de journalisation.

- **-ga[fichier]**

  Mode journalisation -append. Ajouter les entrées du journal à la fin du fichier journal cible ou le crée s'il n'existe pas.

- -**gt[fichier]**

  Mode journalisation -truncate. Tronquer le fichier journal cible s'il existe ou le créer s'il n'existe pas.

- **[fichier]**

  Indiquer le fichier journal cible. S'il n'est pas indiqué, le fichier journal cible par défaut est "BEInvVol.log" dans le chemin en cours. N'indiquez pas le fichier journal sur le volume qui va être invalidé !

- **-?, -h**

  Afficher l'aide.

Exemples

```
> beinvvol -h
> beinvvol xld
> beinvvol xle -ga"c:\sous-répert\fichier.log"
> beinvvol xl* -gt"c:\sous-répert\fichier.log"
> beinvvol xif -gt"c:\mon sous-répert\fichier.log"
> beinvvol xig -g0
> beinvvol xi*
```

8 Mise hors service de disques durs à chiffrement automatique compatibles Opal

Les disques durs à chiffrement automatique offrent un chiffrement de type matériel des données lorsqu'ils sont écrits sur le disque dur. Trusted Computing Group (TCG) a publié la norme Opal indépendante des fournisseurs pour les disques durs à chiffrement automatique. SafeGuard Enterprise prend en charge la norme Opal et permet la gestion des ordinateurs d'extrémité avec disques durs compatibles Opal à chiffrement automatique.

Retrouvez plus d'informations sur les disques durs compatibles Opal dans le *Manuel d'administration de SafeGuard Enterprise*, à la section *SafeGuard Enterprise et disques durs compatibles Opal à chiffrement automatique*.

Pour les ordinateurs protégés par SafeGuard Enterprise, nous mettons à votre disposition notre outil de ligne de commande **`opalinvdisk.exe`**.

8.1 Conditions préalables et conseils d'utilisation

Pour l'utilisation de **`opalinvdisk.exe`**, les conditions préalables et les conseils suivants s'appliquent :

- Avant d'utiliser **`opalinvdisk.exe`**, le disque dur compatible Opal doit être déchiffré avec la commande **Déchiffrer** de SafeGuard Enterprise disponible dans le menu contextuel de l'Explorateur Windows sur l'ordinateur d'extrémité. Retrouvez plus d'informations dans le *Manuel d'administration de SafeGuard Enterprise*, à la section *Autorisation de déverrouillage des disques durs compatibles Opal aux utilisateurs* et dans le *Manuel d'utilisation de SafeGuard Enterprise*, à la section *Extensions des icônes de la barre d'état et de l'Explorateur sur les ordinateurs d'extrémité avec disques durs compatibles Opal.*
- Vous avez besoin des droits d'administrateur.
- Nous vous conseillons d'utiliser **`opalinvdisk.exe`** dans un environnement Windows PE.
- L'outil **`opalinvdisk.exe`** lance le service facultatif **`RevertSP`** avec le paramètre **`KeepGlobalRangeKey`** défini sur **`False`**. La véritable procédure de mise hors service exécutée par **`RevertSP`** dépend du lecteur de disque dur spécifique. Retrouvez plus d'informations à la section 5.2.3 du document Opal standard TCG Storage Security Subsystem Class : Opal, Specification Version 1.00, Revision 3.00 sur www.trustedcomputinggroup.org.

8.2 Exécution de opalinvdisk.exe

1. Ouvrez une invite de commande et démarrez **`opalinvdisk.exe`** avec les droits administrateur.

   Des informations sur les outils et sur son utilisation apparaissent.

2. Sur la ligne de commande, saisissez **`opalinvdisk.exe <PériphériqueCible>`**.

   Par exemple : **`opalinvdisk.exe PhysicalDrive0`**

Si les conditions préalables nécessaires sont remplies, **`RevertSP`** est lancé sur le disque dur spécifié dans **`<PériphériqueCible>`**. Si les conditions préalables ne sont pas remplies ou si le disque dur ne prend pas en charge **`RevertSP`**, un message d'erreur apparaît.

9 Support technique

Vous bénéficiez du support technique des produits Sophos de l'une des manières suivantes :

- Rendez-vous sur le forum de la communauté SophosTalk en anglais sur http://community.sophos.com/ et recherchez d'autres utilisateurs rencontrant le même problème que le vôtre.
- Rendez-vous sur la base de connaissances du support de Sophos sur http://www.sophos.com/fr-fr/support.aspx/.
- Téléchargez la documentation des produits sur http://www.sophos.com/fr-fr/support/documentation.aspx/.
- Envoyez un e-mail à support@sophos.fr, y compris le(s) numéro(s) de version du logiciel Sophos, le(s) système(s) d'exploitation et le(s) niveau(x) de correctif ainsi que le texte de tous les messages d'erreur.

10 Mentions légales