Dell Data Security

Guide d'intégration EnCase

Remarques, précautions et avertissements

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

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

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

Guide d'intégration EnCase

2018 - 03

Rév. A01

Table des matières

1

Introduction

Dell Data Security s'intègre aux produits d'analyses approfondies numériques EnCase 6.15 de Guidance Software, Inc. pour prendre en charge les analyses en ligne de fichiers cryptés par Dell. Grâce à cette intégration, les enquêteurs judiciaires peuvent consulter, exporter ou effectuer des recherches au sein de données sécurisées par Dell. À l'aide d'informations d'identification d'administrateur d'analyse approfondie, toutes les données sécurisées par Dell, quelles que soient les clés utilisées pour les crypter, sont décryptées et présentées à l'enquêteur sans interaction supplémentaire. La fonction de stockage sécurisé de EnCase permet d'enregistrer et de stocker les informations d'identification d'administrateur d'analyse approfondie avec le cas concerné, évitant ainsi de devoir les saisir à nouveau.

L'intégration des analyses approfondies de EnCase 6.15 (32 bits) prend en charge ce qui suit :

- Dell Data Security Encryption Enterprise pour Windows 7.0.x ou version ultérieure
- Dell Security Management Server 7.0.1 ou version ultérieure

REMARQUE : Dell Data Security Encryption Enterprise pour Mac ne prend pas en charge les analyses approfondies EnCase.

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 Numéros de téléphone internationaux Dell ProSupport.

2

Intégration à EnCase

Activation de l'API EnCase

REMARQUE : N'utilisez pas cette API avec des serveurs Dell Device Server déployés dans un DMZ. Utilisez un Dell Device Server interne avec un accès restreint pour l'intégration EnCase afin de maintenir la sécurité.

Avant la version 7.7 de Security Management Server

1 Ouvrez **<Dell install dir>\Enterprise Edition\Device Server\conf\context.properties**.

2 Activez l'API d'intégration des analyses approfondies.

service.forensic.enable=true

3 Arrêtez et redémarrez le Dell Device Server à partir du menu Démarrer.

Pour désactiver l'intégration des analyses approfondies, procédez à la configuration suivante : service.forensic.enable=false.

À partir de la version 7.7 de Security Management Server

- Ce service est activé sur le Dell Server par défaut.
- Pour désactiver l'intégration des analyses approfondies, procédez à la configuration suivante : xapi.service.forensic.enable=false.

Arrêtez et redémarrez le Dell Device Server à partir du menu Démarrer.

Installation de l'adaptateur d'intégration EnCase

1 Sur un ordinateur exécutant EnCase, double-cliquez sur **CMGEnCaseIntegration.exe**.

2 Lorsque la boîte de dialogue du programme d'installation de la bibliothèque s'affiche, vérifiez que le dossier EnCase cible est correct.

3 Cliquez sur **Terminer** pour extraire les fichiers de CEGetBundle et de l'adaptateur d'intégration à l'emplacement suivant : \Program Files\EnCase6\Lib\Credant Technologies\CMG

Utilisation de Dell Data Security avec EnCase

Obtention des clés de cryptage

Via l'interface utilisateur d'Enterprise EnCase, obtenez des clés de cryptage à partir de la console de gestion à distance Dell et décryptez toutes les données cryptées par Dell pour cet ordinateur ou ce fichier de preuve.

1 Cochez la case **En ligne**.

2 Saisissez le **Nom d'utilisateur** de l'administrateur d'analyse approfondie.

3 Saisissez le **Mot de passe** de l'administrateur d'analyse approfondie.

4 Saisissez l'URL du Dell Server avec l'API EnCase activée. Par exemple :

https://cred01.somedomain.com:8443/xapi/ (si vous disposez de la version 7.7 ou ultérieure de Security Management Server)

https://cred01.somedomain.com:8081/xapi (si vous disposez de la version 7.7 ou antérieure de Security Management Server)

Localisez l'URI du Dell Server sous HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\Servlet

REMARQUE : L'API EnCase du Dell Server doit être activée pour permettre l'exportation de clés. Vous pouvez éventuellement déployer un autre Dell Device Server exclusivement pour l'intégration EnCase.

5 Saisissez l'ID de machine (également appelé MCID et ID unique) pour l'ordinateur cible ou le fichier de preuve.

Localisez le MCID dans le registre de l'ordinateur cible sous HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon \CMGShield

Depuis la console de gestion à distance Dell, dans le volet gauche, cliquez sur **Populations > Points de terminaison**

- Cliquez sur l'icône Détails du périphérique approprié.
- Dans le menu supérieur, cliquez sur **Détails et actions**.
- Localisez l'ID unique dans la zone *Détails de point de terminaison*.

6 Saisissez l'ID de bouclier (également appelé ID de périphérique, DCID, ID de récupération ou SCID) utilisé pour l'ordinateur cible ou le fichier de preuve.

Localisez le DCID dans le registre de l'ordinateur cible sous HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon \CMGShield

Depuis la console de gestion à distance Dell, dans le volet gauche, cliquez sur **Populations > Points de terminaison**

- Cliquez sur l'icône **Détails** du périphérique approprié.
- Dans le menu supérieur, cliquez sur **Détails et actions**.
- Localisez l'ID de récupération dans la zone *Bouclier*.

REMARQUE : Indiquez le MCID, le DCID ou les deux ID. L'importation contient tout le matériel clé de l'ID de machine, de l'ID de bouclier ou des deux ID.

7 Cliquez sur **OK**.

Le décryptage est en cours.

Une fois le décryptage terminé, les fichiers sont accessibles pour analyse approfondie. Seul le module EnCase permet de consulter les fichiers décryptés ; les fichiers source d'origine restent inchangés et cryptés.

Utilisation de EnCase avec Dell Data Security

CEGetBundle

CEGetBundle est un utilitaire qui permet aux administrateurs d'analyse approfondie d'extraire le matériel clé d'un Dell Server. Cet utilitaire est disponible via Dell ProSupport.

Le tableau suivant indique les paramètres disponibles dans le cadre de l'installation.

Paramètres
-L = mode hérité pour l'exportation de clés à partir d'un serveur CMG 5.3.x
URL = URL du serveur de périphérique (<securityserver.organization.com>)
AdminName = nom d'utilisateur de l'administrateur
AdminPwd = mot de passe de l'administrateur
AdminDomain = administrateur du domaine
MCID = (Machine ID) ID de machine utilisé pour le périphérique cible (également appelé ID unique ou hostname)
SCID = (Shield Credant ID) ID utilisé pour le bouclier cible (également appelé DCID ou ID de récupération)
Username = utilisateur cible de l'exportation de matériel clé (mode hérité seulement)
OutputFile = nom de fichier utilisé pour l'ensemble de clés exporté
OutputPwd = mot de passe utilisé pour l'ensemble de clés exporté
-R = utilisation du mode fichier de sauvegarde
BackupFile = fichier exécutable contenant les clés de sauvegarde
BackupPwd = mot de passe d'administrateur utilisé pour le fichier de sauvegarde

REMARQUE : Le paramètre AdminDomain doit être fourni uniquement pour l'exportation de clés à partir de serveurs CMG Enterprise éditions 6.0 et ultérieures configurés pour prendre en charge plusieurs domaines.

REMARQUE : En mode hérité, le MCID, le SCID et le nom d'utilisateur doivent être indiqués. Le matériel clé pour l'utilisateur spécifié uniquement sera ajouté au fichier de sortie. Si le cryptage d'utilisateur ou le cryptage d'itinérance d'utilisateur est activé, vous devez exécuter cet outil avec le même nom de fichier de sortie pour chaque utilisateur sur le périphérique concerné par le décryptage. Le matériel clé de chaque utilisateur est alors ajouté au fichier de sortie.

Exemples de ligne de commande

- L'exemple suivant utilise le MCID, le SCID ou les deux. Tout le matériel clé associé à l'ID de machine (MCID) précisé, au SCID ou aux deux est enregistré dans le fichier de sortie qui est écrasé s'il existe déjà.

```
CEGetBundle [-L] -XURL -aAdminName -AAdminPwd [-DAdminDomain] [-dMCID] [-sSCID] [-uUsername] -
oOutputFile -iOutputPwd
```

- L'exemple suivant extrait le matériel clé à partir du fichier de sauvegarde exporté par le programme d'installation.

```
CEGetBundle -R -bBackupFile -ABackupPwd -oOutputFile -iOutputPwd
```