Dell Data Security

Guia de integração do EnCase

Notas, avisos e advertências

NOTA: Uma NOTA indica informações importantes que ajudam a melhorar a utilização do produto.

AVISO: Um AVISO indica potenciais danos do hardware ou a perda de dados e explica como evitar o problema.

ADVERTÊNCIA: Uma ADVERTÊNCIA indica potenciais danos no equipamento, lesões pessoais ou mesmo morte.

Guia de integração do EnCase

2018 - 03

Rev. A01

Índice

1

Introdução

O Dell Data Security integra-se nos produtos forenses digitais do EnCase v6.15 a partir do Guidance Software, Inc. para apoiar investigações online de ficheiros encriptados da Dell. Com esta integração, os investigadores forenses podem ver, exportar ou pesquisar os dados protegidos da Dell. Com as devidas credenciais de administrador forense, todos os dados protegidos da Dell, independentemente das chaves de encriptação utilizadas, são desencriptados e apresentados ao investigador sem interação adicional. O armazenamento protegido do EnCase grava e armazena as credenciais do administrador forense juntamente com o caso, eliminando a necessidade de os voltar a introduzir.

A integração forense do EnCase v6.15 (32 bits) é compatível com::

- Dell Data Security Encryption Enterprise para Windows v7.0.x ou posterior
- Dell Security Management Server v7.0.1 ou posterior

NOTA: O Dell Data Security Encryption Enterprise para Mac não é compatível com a investigação forense EnCase.

Contacte o Dell ProSupport

Contacte o número 877-459-7304, extensão 4310039 para obter suporte telefónico permanente (24 x 7) para o seu produto Dell.

Adicionalmente, o suporte online para os produtos Dell encontra-se disponível em dell.com/support. O suporte online inclui controladores, manuais, conselhos técnicos, FAQ e problemas emergentes.

Ajude-nos a garantir que o direcionamos rapidamente para o especialista técnico mais indicado para si tendo o seu Código de serviço ou Código de serviço expresso disponível quando nos contactar.

Para números de telefone fora dos Estados Unidos, consulte Números de telefone internacionais do Dell ProSupport.

2

Integração com o EnCase

Ativação da API do EnCase

NOTA: Não utilize esta API com Dell Device Servers implementados num DMZ. Utilize um Dell Device Server interno com acesso restrito para a integração do EnCase de forma a manter a segurança.

Security Management Server anterior a v7.7

1 Aceda a **<Diretório de instalação Dell>\Enterprise Edition\Device Server\conf\context.properties**.

2 Ative a API de integração forense.

service.forensic.enable=true

3 Pare e reinicie o Dell Device Server a partir do menu Iniciar.

Para desativar a integração forense, defina service.forensic.enable=false.

Security Management Server v7.7 e posteriores

- Este serviço está ativado no Dell Server por predefinição.
- Para desativar a integração forense, defina xapi.service.forensic.enable=false.

Pare e reinicie o Dell Device Server a partir do menu Iniciar.

Instalação do adaptador de integração do EnCase

1 Num computador a executar o EnCase, faça duplo clique em **CMGEnCaseIntegration.exe**.

2 Quando for apresentada uma caixa de diálogo do Library Installer, certifique-se de que a pasta de destino do EnCase está correta.

3 Clique em **Concluir** para extrair o CEGetBundle e os ficheiros do adaptador de integração para \Program Files\EnCase6\Lib\Credant Technologies\CMG

Utilização do Dell Data Security com o EnCase

Obter chaves de encriptação

Utilize a interface de utilizador do EnCase Enterprise para obter chaves de encriptação da Remote Management Console da Dell e desencripte todos os dados encriptados da Dell para este computador ou para um ficheiro de provas.

1 Assinale a caixa de verificação **Online**.

2 Introduza o **Nome de utilizador** do administrador forense

3 Introduza a **Palavra-passe** do administrador forense.

4 Introduza o URL do Dell Server com a API do EnCase ativada. Por exemplo:

https://cred01.somedomain.com:8443/xapi/ (se tiver o Security Management Server, versão v7.7 ou posterior)

https://cred01.somedomain.com:8081/xapi (se tiver o Security Management Server, versão anterior à v7.7)

Localize o URI do Dell Server em HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\Servlet

NOTA: O Dell Server tem de ter a API do EnCase ativada para exportar as chaves. Pode, em alternativa, implementar um Dell Device Server alternativo exclusivamente para a integração do EnCase.

5 Introduza a ID do computador (também conhecida como MCID e ID exclusivo) para o computador de destino ou para um ficheiro de provas.

Localize a MCID no registo do computador de destino em HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon \CMGShield

a partir da Dell Remote Management Console, no painel esquerdo, e clique em **Populações > Endpoints**

- Clique no ícone Detalhes do dispositivo adequado.
- No menu superior, clique em **Detalhes e ações**.
- Localize a ID exclusiva na secção *Detalhes do Endpoint*.

6 Introduza a ID Shield (também conhecida como ID do dispositivo, ID de recuperação e SCID) para o computador de destino ou para um ficheiro de provas.

Localize o DCID no registo do computador de destino em HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon \CMGShield

a partir da Dell Remote Management Console, no painel esquerdo, e clique em **Populações > Endpoints**

- Clique no ícone **Detalhes** do dispositivo adequado.
- No menu superior, clique em **Detalhes e ações**.
- Localize a ID de recuperação na secção *Shield*.

NOTA: Especifique a MCID, a DCID ou as duas ID. A pasta importada contém todos os materiais de chave para a ID do computador especificado, ID Shield ou para as duas ID.

7 Clique em **OK**.

A desencriptação está agora em curso.

Assim que a desencriptação estiver concluída, os ficheiros estão disponíveis para avaliação forense. Os ficheiros desencriptados apenas são visíveis através do módulo do EnCase, os ficheiros de origem permanecem inalterados e encriptados.

Utilização do Encase com o Dell Data Security

CEGetBundle

O CEGetBundle é um utilitário que permite que os administradores forenses retirem material de chave a partir de um Dell Server. Este utilitário está disponível através do Dell ProSupport.

A tabela seguinte descreve os parâmetros disponíveis para a instalação.

Parâmetros
-L = modo legacy para exportar chaves de um servidor CMG 5.3.x
URL = URL do Device Server (<securityserver.organization.com>)
AdminName = nome de utilizador de administrador
AdminPwd = palavra-passe de administrador
AdminDomain = administrador de domínio
MCID = ID do computador para o dispositivo de destino (também conhecida como ID exclusiva ou nome do anfitrião)
SCID = ID Shield Credant para o Shield de destino (também conhecida como DCID ou ID de recuperação)
Username = utilizador pretendido para exportação de material de chave (apenas em modo legacy)
OutputFile = nome do ficheiro para a chave de encriptação exportada
OutputPwd = palavra-passe para a chave de encriptação exportada
-R = utiliza o modo de ficheiro de cópia de segurança
BackupFile = ficheiro executável que contém as chaves de cópia de segurança
BackupPwd = a palavra-passe de administrador utilizada para o ficheiro de cópia de segurança

NOTA: O parâmetro AdminDomain deve ser fornecido apenas para exportar chaves de servidores configurados para suportar vários domínios do CMG Enterprise Edition 6.0 ou de versões posteriores.

NOTA: No modo legacy, o MCID, o SCID e o nome de utilizador devem ser especificados. O material de chave apenas para o utilizador especificado será anexado ao ficheiro de saída. Tem de executar esta ferramenta com o mesmo nome de ficheiro de saída para cada utilizador no dispositivo pretendido para a desencriptação, se a encriptação do utilizador ou do roaming de utilizador estiver ativada. Cada material de chave de utilizador será anexada ao ficheiro de saída.

Exemplo de linha de comandos

- O exemplo que se segue utiliza o MCID, o SCID ou ambos. Todos os materiais de chave associados aos computadores especificados (MCID, SCID ou ambos) serão guardados no ficheiro de saída que será substituído, se este existir.

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

- O exemplo que se segue extrai material de chave do ficheiro de cópia de segurança exportado pelo instalador.

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