Dell Data Security

Guida all'integrazione di EnCase

Messaggi di N.B., Attenzione e Avvertenza

N.B.: un messaggio N.B. (Nota Bene) indica informazioni importanti che contribuiscono a migliorare l'utilizzo del prodotto.

ATTENZIONE: Un messaggio di ATTENZIONE indica un danno potenziale all'hardware o la perdita di dati, e spiega come evitare il problema.

AVVERTENZA: Un messaggio di AVVERTENZA indica un rischio di danni materiali, lesioni personali o morte.

Guida all'integrazione di EnCase

2018 - 03

Rev. A01

Sommario

1

Introduzione

Dell Data Security si integra con i prodotti forensi digitali EnCase v6.15 di Guidance Software, Inc. per supportare le indagini online di file Dell crittografati. Grazie a questa integrazione, gli investigatori forensi possono visualizzare, esportare o effettuare ricerche all'interno di dati protetti Dell. Con le appropriate credenziali di amministratore forense, tutti i dati protetti Dell, indipendentemente dalle chiavi utilizzate per la crittografia, vengono decrittografati e presentati all'investigatore senza ulteriori interazioni. L'archiviazione protetta di EnCase salva e memorizza le credenziali di amministratore forense con la pratica, eliminando la necessità di immetterle nuovamente.

L'integrazione forense EnCase v6.15 (32 bit) supporta:

- Dell Data Security Encryption Enterprise per Windows v7.0.x o versioni successive
- Dell Security Management Server v7.0.1 o versioni successive

N.B.: Dell Data Security Encryption Enterprise per Mac non supporta l'investigazione forense di EnCase.

Contattare Dell ProSupport

Per assistenza telefonica sui prodotti Dell, chiamare il numero 877-459-7304, interno 4310039, 24h su 24, 7 giorni su 7.

Inoltre, il supporto online per i prodotti Dell è disponibile all'indirizzo dell.com/support. L'assistenza online comprende driver, manuali, consulenze tecniche, FAQ e problemi emergenti.

Assicurarsi di avere a portata di mano il codice di matricola o il codice di servizio rapido per essere messi rapidamente in contatto con l'esperto tecnico più adatto.

Per i numeri di telefono esterni agli Stati Uniti, controllare Numeri di telefono internazionali di Dell ProSupport.

2

Integrazione con EnCase

Abilitare l'API EnCase

N.B.: Non utilizzare questa API con Dell Device Server distribuiti in un DMZ. Per gestire la sicurezza utilizzare un Dell Device Server interno con accesso limitato per l'integrazione EnCase.

Security Management Server di versioni precedenti la v7.7

1 Aprire **<directory di installazione Dell>\Enterprise Edition\Device Server\conf\context.properties**.

2 Abilitare l'API di integrazione forense.

service.forensic.enable=true

3 Arrestare e riavviare Dell Device Server dal menu Start.

Per disabilitare l'integrazione forense, impostare service.forensic.enable=false.

Security Management Server v7.7 e versioni successive

- Questo servizio è abilitato in Dell Server per impostazione predefinita.
- Per disabilitare l'integrazione forense, impostare xapi.service.forensic.enable=false.

Arrestare e riavviare Dell Device Server dal menu Start.

Installare EnCase Integration Adapter

1 Su un computer su cui è in esecuzione EnCase, cliccare due volte su **CMGEnCaseIntegration.exe**.

2 Quando viene visualizzata la finestra di dialogo Library Installer (Programma di installazione librerie), accertarsi che la cartella di destinazione di EnCase sia corretta.

3 Cliccare su **Finish** (Fine) per estrarre i file di CEGetBundle e Integration Adapter su \Program Files\EnCase6\Lib\Credant Technologies\CMG

Utilizzare Dell Data Security con EnCase

Ottenere le chiavi di cifratura

Utilizzare l'interfaccia utente EnCase Enterprise per ottenere le chiavi di cifratura dalla Dell Remote Management Console e decifrare tutti i dati cifrati Dell per il computer o il file delle prove.

1 Selezionare la casella di controllo **Online**.

2 Digitare lo **Username** (nome utente) dell'amministratore forense.

3 Digitare la **Password** dell'amministratore forense.

4 Digitare l'URL del server con l'API EnCase abilitata. Per esempio:

https://cred01.somedomain.com:8443/xapi/ (se il Security Management Server è v7.7 o versione successiva)

https://cred01.somedomain.com:8081/xapi (se il Security Management Server è di una versione precedente alla v7.7)

Individuare l'URI del Dell Server in HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\Servlet

N.B.: Dell Server deve avere l'API EnCase abilitata per esportare le chiavi. Se si desidera, è possibile implementare un Dell Device Server alternativo esclusivamente per l'integrazione di EnCase.

5 Digitare l'ID macchina (noto anche come MCID e ID univoco) della macchina virtuale per il computer o il file delle prove di destinazione.

Individuare l'MCID nel registro di sistema del computer di destinazione in HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion \Winlogon\CMGShield

Da Dell Remote Management Console, nel riquadro di sinistra, cliccare su **Populations > Endpoints** (Popolazioni > Endpoint)

- Cliccare sull'icona Details (Dettagli) del dispositivo appropriato.
- Dal menu principale, cliccare su **Details & Actions** (Dettagli e azioni).
- Individuare l'ID univoco nell'area *Endpoint Detail* (Dettaglio endpoint).

6 Digitare l'ID Shield (noto anche come ID dispositivo, DCID, ID di ripristino o SCID) per il computer o il file delle prove di destinazione.

Individuare il DCID nel registro di sistema del computer di destinazione in HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion \Winlogon\CMGShield

Da Dell Remote Management Console, nel riquadro di sinistra, cliccare su **Populations > Endpoints** (Popolazioni > Endpoint)

- Cliccare sull'icona **Details** (Dettagli) del dispositivo appropriato.
- Dal menu principale, cliccare su **Details & Actions** (Dettagli e azioni).
- Individuare l'ID di ripristino nell'area *Shield*.

N.B.: Specificare MCID, DCID o entrambi gli ID. La pratica importata contiene tutto il materiale chiave per ID macchina, ID Shield o entrambi gli ID.

7 Fare clic su **OK**.

La decrittografia è ora in corso.

Una volta completata, i file sono accessibili per i controlli forensi. I file decrittografati sono visualizzabili solo attraverso il modulo EnCase; i file di origine iniziali rimangono inalterati e crittografati.

Utilizzare EnCase con Dell Data Security

CEGetBundle

CEGetBundle è una utility che consente agli amministratori forensi di estrarre materiale chiave da un Dell Server. Questa utility è disponibile tramite Dell ProSupport.

La tabella seguente descrive in dettaglio i parametri disponibili per l'installazione.

Parametri
-L=Modalità Legacy per esportare le chiavi da un Server CMG 5.3.x
URL=URL del Device Server (<securityserver.organization.com>)
AdminName=Nome utente amministratore
AdminPwd=Password amministratore
AdminDomain=Dominio amministratore
MCID=ID della macchina per il dispositivo di destinazione (noto anche come ID univoco o nome host)
SCID=ID Shield Credant per lo Shield di destinazione (noto anche come DCID o ID di ripristino)
Username=Utente previsto per l'esportazione del materiale chiave (solo modalità legacy)
OutputFile=Nome file per il bundle chiave esportato
OutputPwd =Password per il bundle chiave esportato
-R=Utilizzare la modalità di backup file
BackupFile=File eseguibile contenente i codici di backup
BackupPwd=Password amministratore utilizzata per il file di backup

N.B.: Il parametro AdminDomain deve essere fornito solo per esportare le chiavi da CMG Enterprise Edition 6.0 e server di versioni successive configurati per il supporto di più domini.

N.B.: In modalità legacy è necessario specificare MCID, SCID e nome utente. Al file di output verrà aggiunto solo il materiale chiave per l'utente specificato. È necessario eseguire questo strumento con lo stesso nome del file di output per ciascun utente sul dispositivo previsto per la decrittografia se sono abilitati l'utente o la crittografia roaming utente. Il materiale chiave di ogni utente verrà aggiunto al file di output.

Esempio di riga di comando

- L'esempio seguente utilizza MCID, SCID o entrambi. Tutti i materiali chiave associati alla macchina specificata (MCID) o SCID o entrambi verranno salvati nel file di output che sarà sovrascritto se già esistente.

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

- L'esempio seguente estrae materiale chiave dal file di backup esportato dal programma di installazione.

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