Dell Data Security

Guía de integración de EnCase

Notas, precauciónes y advertencias

NOTA: Una NOTA señala información importante que lo ayuda a hacer un mejor uso de su producto.

PRECAUCIÓN: Una PRECAUCIÓN indica un potencial daño al hardware o pérdida de datos y le informa cómo evitar el problema.

ADVERTENCIA: Una señal de ADVERTENCIA indica la posibilidad de sufrir daño a la propiedad, heridas personales o la muerte.

Guía de integración de EnCase

2018 - 03

Rev. A01

Contenido

1 Introducción 4
Cómo ponerse en contacto con Dell ProSupport 4

2 Integración a EnCase 5
Activación de la API de EnCase 5
Instalación del adaptador de integración de EnCase 5

3 Uso de Dell Data Security con EnCase 6

4 Uso de EnCase con Dell Data Security 8
CEGetBundle 8

1

Introducción

Dell Data Security se integra con los productos forenses digitales de EnCase versión 6.15 de Guidance Software, Inc. para brindar asistencia a las investigaciones en línea de archivos cifrados de Dell. Con esta integración, los investigadores forenses pueden ver, exportar o buscar en los datos protegidos por Dell. Con las credenciales adecuadas de administrador forense, todos los datos protegidos por Dell, independientemente de las claves utilizadas para el cifrado, se descifran y se muestran al investigador sin ninguna interacción adicional. El almacenamiento seguro de EnCase guarda y almacena las credenciales de administrador forense con el caso para que no tenga que volver a ingresarlas.

La integración forense de EnCase versión 6.15 (32 bits) admite:

- Encryption Enterprise de Dell Data Security para Windows versión 7.0.x o posterior
- Dell Security Management Server versión 7.0.1 o posterior

NOTA: Encryption Enterprise de Dell Data Security para Mac no admite la investigación forense de EnCase.

Cómo ponerse en contacto con Dell ProSupport

Llame al 877-459-7304, extensión 4310039 para obtener soporte telefónico sobre su producto Dell 24 horas al día, 7 días a la semana.

De manera adicional, puede obtener soporte en línea para los productos Dell en dell.com/support. El soporte en línea incluye controladores, manuales, recomendaciones técnicas, P+F y posibles problemas.

Tenga su Código de servicio rápido o Etiqueta de servicio a mano cuando realice la llamada para asegúrese de ayudarnos a conectarle rápidamente con el experto técnico adecuado.

Para obtener los números de teléfono fuera de los Estados Unidos, consulte Números de teléfono internacionales de Dell ProSupport .

2

Integración a EnCase

Activación de la API de EnCase

NOTA: No utilice esta API con los Dell Device Server implementados en una DMZ. Utilice un Dell Device Server interno con acceso restringido para la integración de EnCase a fin de mantener la seguridad.

Security Management Server anterior a la versión 7.7

1 Abra **<Dirección de instalación de Dell>\Enterprise Edition\Device Server\conf\context.properties**.

2 Active la API de integración forense.

service.forensic.enable=true

3 Detenga y reinicie Dell Device Server desde el menú de inicio.

Para desactivar la integración forense, establezca el comando de la siguiente manera: service.forense.enable=false.

Security Management Server versión 7.7 y posteriores

- Este servicio se activa en Dell Server de manera predeterminada.
- Para desactivar la integración forense, establezca el comando de la siguiente manera: xapi.service.forensic.enable=false.

Detenga y reinicie Dell Device Server desde el menú de inicio.

Instalación del adaptador de integración de EnCase

1 En una computadora que ejecuta EnCase, haga doble clic en **CMGEnCaseIntegration.exe**.

2 Cuando el diálogo del instalador de la biblioteca aparezca, asegúrese de que la carpeta EnCase de destino es correcta.

3 Haga clic en **Finalizar** para extraer los archivos del adaptador de integración y CEGetBundle a \Archivos de programa\EnCase6\Lib \Credant Technologies\CMG

Uso de Dell Data Security con EnCase

Obtención de claves de cifrado

Utilice la interfaz de usuario de EnCase Enterprise para obtener las claves de cifrado de Dell Remote Management Console y descifrar todos los datos cifrados por Dell de esta computadora o archivo de evidencia.

1 Marque la casilla de verificación **En línea**.

2 Escriba el **nombre de usuario** del administrador forense.

3 Escriba la **contraseña** del administrador forense.

4 Escriba la dirección URL de Dell Server con la API de EnCase activada. Por ejemplo:

https://cred01.somedomain.com:8443/xapi/ (si la versión de Security Management Server es 7.7 o una posterior)

https://cred01.somedomain.com:8081/xapi (si la versión de Security Management Server es anterior a la 7.7)

Encuentre el URI de Dell Server en HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\CMGShield\Servlet

NOTA: Dell Server debe tener la API de EnCase activada para exportar claves. De manera opcional, puede implementar un Dell Device Server alternativo exclusivamente para la integración de EnCase.

5 Escriba la ID de máquina (también conocida como MCID e ID única) de la computadora o el archivo de evidencia de destino.

Encuentre la MCID en el registro de la computadora de destino en HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion \Winlogon\CMGShield

en Dell Remote Management Console, en el panel izquierdo, haga clic en **Poblaciones > Extremos**

- Haga clic en el ícono de Detalles del dispositivo correspondiente.
- En el menú superior, haga clic en **Detalles y acciones**.
- Ubique la ID única en el área *Detalles del extremo*.

6 Escriba la ID de Shield (también conocida como ID de dispositivo, DCID, ID de recuperación o SCID) de la computadora o el archivo de evidencia de destino.

Ubique la DCID en el registro de la computadora de destino en HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon \CMGShield

en Dell Remote Management Console, en el panel izquierdo, haga clic en **Poblaciones > Extremos**

- Haga clic en el ícono de **Detalles** del dispositivo correspondiente.
- En el menú superior, haga clic en **Detalles y acciones**.
- Ubique la ID de recuperación en el área de *Shield*.

NOTA: Especifique la MCID, la DCID o ambas. El caso importado contiene todos los materiales de claves para la ID de máquina, de Shield o ambas.

7 Haga clic en **Aceptar**.

El descifrado está en curso ahora.

Una vez que el descifrado se complete, los archivos son accesibles para realizar el análisis forense. Los archivos descifrados solo se pueden visualizar a través del módulo de EnCase, los archivos de origen iniciales permanecen sin cambios y cifrados.

Uso de EnCase con Dell Data Security

CEGetBundle

CEGetBundle es una utilidad que permite a los administradores forenses extraer el material de clave de un Dell Server. Esta utilidad está disponible a través de Dell ProSupport.

La tabla a continuación indica los parámetros disponibles para la instalación.

Parámetros
-L = modo heredado para exportar claves de un servidor CMG 5.3.x
URL = URL de Device Server (<securityserver.organization.com>)
AdminName = nombre de usuario del administrador
AdminPwd = contraseña del administrador
AdminDomain = dominio del administrador
MCID = ID de máquina para el dispositivo de destino (también conocida como la ID única o hostname)
SCID = ID de Shield Credant para el Shield de destino (también conocida como DCID o ID de recuperación)
Nombre de usuario = usuario seleccionado para la exportación del material de clave (solo en modo heredado)
OutputFile = nombre de archivo para el paquete de clave exportado
OutputPwd = contraseña para el paquete de clave exportado
-R = utiliza el modo de archivo de respaldo
BackupFile = archivo ejecutable que contiene las claves de respaldo
BackupPwd = contraseña del administrador que se utiliza para el archivo de respaldo

NOTA: El parámetro AdminDomain debe proporcionarse solo para exportar claves de servidores CMG Enterprise Edition 6.0 y posteriores configurados para admitir varios dominios.

NOTA: En el modo heredado, la MCID, la SCID y el nombre de usuario deben especificarse. El material de clave solo se agregará al archivo de salida para el usuario especificado. Debe ejecutar esta herramienta con el mismo nombre de archivo de salida para cada usuario en el dispositivo que se descifrará si los cifrados de usuario o de roaming de usuario están activados. Cada material de clave del usuario se agregará al archivo de salida.

Ejemplo de línea de comandos

- En el siguiente ejemplo se utilizan la MCID, la SCID o ambas. Todos los materiales de clave asociados a la máquina especificada (MCID) o SCID o ambas se guardarán en el archivo de salida que se sobrescribirá si ya existe.

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

- En el siguiente ejemplo se extrae el material de clave del archivo de respaldo exportado por el instalador.

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