Dell Data Protection

Guía de recuperación para el Cifrado de archivo/carpeta, Hardware Crypto Accelerator, Unidades de cifrado automático y Clave de propósito general v8.10

© 2016 Dell Inc.

Marcas comerciales y marcas comerciales registradas utilizadas en el conjunto de documentos de Dell Data Protection | Encryption, Dell Data Protection | Endpoint Security Suite, Dell Data Protection | Endpoint Security Suite Enterprise, Dell Data Protection | Security Tools y Dell Data Protection | Cloud Edition: Dell™ y el logotipo de Dell, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS®, y KACE™ son marcas comerciales de Dell Inc. Cylance® y el logotipo de Cylance son marcas comerciales registradas de Cylance, Inc. en los EE. UU. y en otros países. McAfee® y el logotipo de McAfee son marcas comerciales o marcas comerciales registradas de McAfee, Inc. en los EE. UU. y en otros países. Intel®, Pentium®, Intel Core Inside Duo®, Itanium® y Xeon® son marcas comerciales registradas de Intel Corporation en los EE. UU. y en otros países. Adobe®, Acrobat® y Flash® son marcas comerciales registradas de Adobe Systems Incorporated. Authen Tec® y Eikon® son marcas comerciales registradas de Authen Tec. AMD® es una marca comercial registrada de Advanced Micro Devices, Inc. Microsoft®, Windows® y Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista®, MSN®, ActiveX®, Active Directory®, Access®, ActiveSync®, BitLocker®, BitLocker To Go®, Excel®, Hyper-V®, Silverlight®, Outlook®, PowerPoint®, OneDrive®, SQL Server® y Visual C++® son marcas comerciales o marcas comerciales registradas de Microsoft Corporation en los Estados Unidos y/o en otros países. VMware® es una marca comercial o una marca comercial registrada de VMware, Inc. en los Estados Unidos o en otros países. Box® es una marca comercial registrada de Box. Dropbox℠ es una marca de servicio de Dropbox, Inc. Google™, Android™, Google™ Chrome™, Gmail™, YouTube® y Google™ Play son marcas comerciales o marcas comerciales registradas de Google Inc. en los Estados Unidos y en otros países. Apple®, Aperture®, App Store℠, Apple Remote Desktop™, Apple TV®, Boot Camp™, FileVault™, iCloud®℠, iPad®, iPhone®, iPhoto®, iTunes Music Store®, Macintosh®, Safari® y Siri® son marcas de servicio, marcas comerciales o marcas comerciales registradas de Apple, Inc. en los Estados Unidos y/o en otros países. GO ID®, RSA® y SecurID® son marcas comerciales registradas de EMC Corporation. EnCase™ y Guidance Software® son marcas comerciales o marcas comerciales registradas de Guidance Software. Entrust® es una marca comercial registrada de Entrust®, Inc. en los Estados Unidos y en otros países. InstallShield® es una marca comercial registrada de Flexera Software en Estados Unidos, China, Unión Europea, Hong Kong, Japón, Taiwán y Reino Unido. Micron® y RealSSD® son marcas comerciales registradas de Micron Technology, Inc. en los Estados Unidos y en otros países. Mozilla® Firefox® es una marca comercial registrada de Mozilla Foundation en los Estados Unidos y/o en otros países. iOS® es una marca comercial o una marca comercial registrada de Cisco Systems, Inc. en los Estados Unidos y en determinados países y se utiliza bajo licencia. Oracle® y Java® son marcas comerciales registradas de Oracle y/o sus afiliados. Los demás nombres utilizados pueden ser marcas comerciales de sus respectivos propietarios. SAMSUNG™ es una marca comercial de SAMSUNG en los Estados Unidos o en otros países. Seagate® es una marca comercial registrada de Seagate Technology LLC en los Estados Unidos y/o en otros países. Travelstar® es una marca comercial registrada de HGST, Inc. en los Estados Unidos y en otros países. UNIX® es una marca comercial registrada de The Open Group. VALIDITY™ es una marca comercial de Validity Sensors, Inc. en los Estados Unidos y en otros países. VeriSign® y otras marcas relacionadas son las marcas comerciales o marcas comerciales registradas de VeriSign, Inc. o sus afiliados o filiales en los Estados Unidos y en otros países y han otorgado la licencia a Symantec Corporation. KVM on IP® es una marca comercial registrada de Video Products. Yahoo!® es una marca comercial registrada de Yahoo! Inc.

Este producto utiliza partes del programa 7-Zip. El código fuente se encuentra disponible en www.7-zip.org. La concesión de licencia está bajo la licencia de GNU LGPL + restricciones de unRAR (www.7-zip.org/license.txt).

07/2016

Protegido por una o más patentes de EE. UU., incluidas las siguientes: Número 7665125; Número 7437752; y Número 7665118;

La información en este documento está sujeta a cambios sin aviso previo.

Contenido

1

Introducción

En esta sección se describe lo necesario para crear un entorno de recuperación.

- Una copia descargada del software del entorno de recuperación ubicada en la carpeta Kit de recuperación de Windows en los medios de instalación de Dell Data Protection.
- Medios CD-R, DVD-R o medios USB formateados
  - Si desea grabar un CD o DVD, revise Apéndice A - Grabación del entorno de recuperación para obtener más detalles.
  - Si utiliza medios USB, revise Apéndice A - Grabación del entorno de recuperación para obtener más detalles.
- Paquete de recuperación para dispositivos en error
  - Para clientes administrados remotamente, las instrucciones siguientes explican cómo recuperar un paquete de recuperación desde su Dell Data Protection Server.
  - Para clientes administrados localmente, el paquete de recuperación se creó durante la configuración en una unidad de red compartida o en un medio externo. Localice este paquete antes de continuar.

2

Recuperación de cifrado de archivo/carpeta

Con la recuperación de Cifrado de archivo/carpeta (FFE), puede recuperar el acceso a lo siguiente:

- A un equipo que no se inicia y que muestra una petición para realizar recuperación de SDE.
- A un equipo en el que no se pueden editar políticas ni acceder a los datos cifrados.
- A un servidor que ejecuta Dell Data Protection | Server Encryption que cumple con las condiciones anteriores.
- A un equipo en el que se debe sustituir la tarjeta de Hardware Crypto Accelerator o la placa base/TPM.

Requisitos de recuperación

Para la recuperación de FFE necesita lo siguiente:

- Kit de recuperación de Windows para crear un disco de reinicio especial: el kit contiene archivos que se utilizarán para crear una imagen de Windows PE (WinPE) y personalizarla con software y controladores de Dell Data Protection. El kit se ubica en la carpeta Kit de recuperación de Windows en los medios de instalación de Dell Data Protection.

Descripción general del proceso de recuperación

Para recuperar un sistema defectuoso:

1. Cree la ISO de recuperación y grábela en un CD/DVD o cree un USB de arranque. Consulte Apéndice A - Grabación del entorno de recuperación.
2. Obtenga el archivo de recuperación.
3. Realice la recuperación.

Realizar la recuperación de FFE

Siga estos pasos para realizar la recuperación de FFE.

Obtener el archivo de recuperación - Equipo administrado remotamente

Para descargar el archivo **LSARecovery_<nombremáquina_dominio.com>.exe**:

1. Abra la Remote Management Console y, desde el panel izquierdo, seleccione **Administración > Recuperar extremo**.
2. En el campo Nombre de host, introduzca el nombre de dominio completo del extremo y haga clic en **Buscar**.
3. En la ventana Recuperación mejorada, introduzca una Contraseña de recuperación y haga clic en **Descargar**.

NOTA: Debe recordar esta contraseña para acceder a las claves de recuperación.

4. Copie el archivo **LSARecovery_<nombremáquina_dominio.com>.exe** en una ubicación a la que pueda accederse cuando se inicie en WinPE.

Obtener el archivo de recuperación - Equipo administrado localmente

Para obtener el archivo de recuperación de Personal Edition:

1. Busque el archivo de recuperación **LSARecovery_<nombresistema>.exe**. Este archivo fue almacenado en una unidad de red o unidad de almacenamiento extraíble al hacerse la instalación de Personal Edition por medio del asistente de configuración.
2. Copie **LSARecovery_<nombresistema>.exe** al equipo de destino (el equipo que tiene la información que desea recuperar).

Realizar una recuperación

1. Con los medios de arranque creados anteriormente, realice el inicio con dichos medios en un sistema de recuperación o en el dispositivo con la unidad que está intentando recuperar. Se abre un entorno WinPE.
2. Introduzca **x** y presione **Intro** para obtener una solicitud de comandos.
3. Vaya al archivo de recuperación e inícielo.
4. Seleccione una opción:
   - Mi sistema no se inicia y muestra un mensaje que me pide que ejecute la recuperación SDE.

     Esto le permitirá volver a crear las comprobaciones de hardware que realiza el cliente Encryption cuando lo inicia en el SO.
   - Mi sistema no me permite el acceso a la información cifrada, ni modificar las políticas, o se está reinstalando.

     Utilícelo si se debe sustituir la tarjeta de Hardware Crypto Accelerator o la placa base/TPM.
5. En el cuadro de diálogo Información de recuperación y copia de seguridad, confirme que es correcta la información acerca del equipo cliente que se debe recuperar y haga clic en **Siguiente**.

   Al recuperar equipos que no sean de Dell, los campos Número de serie y Etiqueta de activos se dejarán en blanco.
6. En el cuadro de diálogo que muestra los volúmenes del equipo, seleccione todas las unidades correspondientes y haga clic en **Siguiente**.

   Haga clic en Mayús o Ctrl para resaltar varias unidades.

   Si la unidad seleccionada no está cifrada con FFE, no se realizará la recuperación.
7. Introduzca su contraseña de recuperación y haga clic en **Siguiente**.

   Con un cliente administrado remotamente, esta es la contraseña proporcionada en el paso 3 en Obtener el archivo de recuperación - Equipo administrado remotamente.

   En Personal Edition, la contraseña es la Contraseña del administrador de cifrado que estableció el sistema al custodiar las claves.
8. En el cuadro de diálogo Recuperar, haga clic en **Recuperar**. Se inicia el proceso de recuperación.
9. Una vez completada la recuperación, haga clic en **Finalizar**.

NOTA: Asegúrese de extraer cualquier medio USB o CD\DVD que utilizó para iniciar la máquina. Si no hace esto, es posible que se vuelva a iniciar al entorno de recuperación.

10. Después de reiniciar el equipo, debe tener un equipo en pleno funcionamiento. Si los problemas continúan, póngase en contacto con Dell ProSupport.

3

Recuperación de Hardware Crypto Accelerator

Con la recuperación de Hardware Crypto Accelerator (HCA) de Dell Data Protection, puede recuperar el acceso a lo siguiente:

- Archivos en una unidad cifrada de HCA: este método descifra la unidad mediante las claves proporcionadas. Puede seleccionar la unidad específica que necesita descifrar durante el procesado de recuperación.
- Una unidad cifrada de HCA después de la sustitución del hardware: este método se utiliza después de sustituir la tarjeta de Hardware Crypto Accelerator o la placa base/TPM. Puede ejecutar una recuperación para volver a tener acceso a los datos cifrados sin tener que descifrar la unidad.

Requisitos de recuperación

Para la recuperación de HCA, necesita lo siguiente:

- Acceso a una ISO de entorno de recuperación
- CD\DVD o medios USB de arranque

Descripción general del proceso de recuperación

Para recuperar un sistema defectuoso:

1. Cree la ISO de recuperación y grábela en un CD/DVD o cree un USB de arranque. Consulte Apéndice A - Grabación del entorno de recuperación.
2. Obtenga el archivo de recuperación.
3. Realice la recuperación.

Realizar la recuperación de HCA

Siga estos pasos para realizar la recuperación de HCA.

Obtener el archivo de recuperación - Equipo administrado remotamente

Para descargar el archivo **LSARecovery_<nombremáquina_dominio.com>.exe** que se generó al instalar Dell Data Protection:

1. Abra la Remote Management Console y, desde el panel izquierdo, seleccione **Administración > Recuperar extremo**.
2. En el campo Nombre de host, introduzca el nombre de dominio completo del extremo y haga clic en **Buscar**.
3. En la ventana Recuperación mejorada, introduzca una Contraseña de recuperación y haga clic en **Descargar**.

NOTA: Debe recordar esta contraseña para acceder a las claves de recuperación.

Se ha descargado el archivo **LSARecovery_<nombremáquina_dominio.com>.exe**.

Obtener el archivo de recuperación - Equipo administrado localmente

Para obtener el archivo de recuperación de Personal Edition:

1. Busque el archivo de recuperación **LSARecovery_<nombresistema>.exe**. Este archivo fue almacenado en una unidad de red o unidad de almacenamiento extraíble al hacerse la instalación de Personal Edition por medio del asistente de configuración.
2. Copie **LSARecovery_<nombresistema>.exe** al equipo de destino (el equipo que tiene la información que desea recuperar).

Realizar una recuperación

1. Con los medios de arranque creados anteriormente, realice el inicio con dichos medios en un sistema de recuperación o en el dispositivo con la unidad que está intentando recuperar.

   Se abre un entorno WinPE.
2. Escriba **x** y presione **Intro** para obtener una solicitud de comandos.
3. Vaya al archivo de recuperación guardado e inícielo.
4. Seleccione una opción:
   - Deseo descifrar mi unidad HCA cifrada.
   - Deseo restaurar el acceso a mi unidad HCA cifrada.
5. En el cuadro de diálogo Información de recuperación y copia de seguridad, confirme que el Número de activo o la Etiqueta de servicio son correctos y haga clic en **Siguiente**.
6. En el cuadro de diálogo que muestra los volúmenes del equipo, seleccione todas las unidades correspondientes y haga clic en **Siguiente**.

   Haga clic en Mayús o Ctrl para resaltar varias unidades.

   Si la unidad seleccionada no está cifrada con HCA, no se realizará la recuperación.
7. Introduzca su contraseña de recuperación y haga clic en **Siguiente**.

   En un equipo administrado remotamente, esta es la contraseña proporcionada en el paso 3 en Obtener el archivo de recuperación - Equipo administrado remotamente.

   En un equipo administrado localmente, la contraseña es la Contraseña del administrador de cifrado que estableció el sistema en Personal Edition al custodiar las claves.
8. En el cuadro de diálogo Recuperar, haga clic en **Recuperar**. Se inicia el proceso de recuperación.
9. Cuando se le solicite, vaya al archivo de recuperación guardado y haga clic en **Aceptar**.

   Si está realizando un descifrado completo, el siguiente cuadro de diálogo mostrará el estado. Este proceso puede tardar un poco.
10. Cuando se muestre el mensaje para indicar que la recuperación ha finalizado correctamente, haga clic en **Finalizar**. Se reinicia el equipo.

Después de reiniciar el equipo, debe tener un equipo en pleno funcionamiento. Si los problemas continúan, póngase en contacto con Dell ProSupport.

4

Recuperación de la unidad de cifrado automático (SED)

Con la recuperación de SED, puede recuperar el acceso a los archivos en una SED mediante los siguientes métodos:

- Realice un desbloqueo de una sola vez de la unidad para omitir y quitar la Autenticación previa al inicio (PBA).
  - En un cliente SED administrado remotamente, la PBA se puede volver a habilitar más tarde mediante la Remote Management Console.
  - En un cliente SED administrado localmente, la PBA se puede volver a habilitar mediante la Consola del administrador de Security Tools.
- Desbloquéela y, a continuación, quite de forma permanente la PBA de la unidad. El inicio de sesión único no funcionará con la PBA quitada.
  - En un cliente SED administrado remotamente, para quitar la PBA, tendrá que desactivar el producto desde la Remote Management Console si es necesario para volver a habilitar la PBA en un futuro.
  - En un cliente SED administrado localmente, para quitar la PBA, tendrá que desactivar el producto del SO si es necesario para volver a habilitar la PBA en un futuro.

Requisitos de recuperación

Para la recuperación de SED, necesita lo siguiente:

- Acceso a una ISO de entorno de recuperación
- CD\DVD o medios USB de arranque

Descripción general del proceso de recuperación

Para recuperar un sistema defectuoso:

1. Cree la ISO de recuperación y grábela en un CD/DVD o cree un USB de arranque. Consulte Apéndice A - Grabación del entorno de recuperación.
2. Obtenga el archivo de recuperación.
3. Realice la recuperación.

Realizar la recuperación de SED

Siga estos pasos para realizar la recuperación de SED.

Obtener el archivo de recuperación - Cliente SED administrado remotamente

1 Obtenga el archivo de recuperación.

El archivo de recuperación se puede descargar desde la Remote Management Console. Para descargar el archivo *<nombrehost>-sed-recovery.dat* que se generó al instalar Dell Data Protection:

- **a** Abra la Remote Management Console y, desde el panel izquierdo, seleccione **Administración > Recuperar datos** y, a continuación, seleccione la pestaña **SED**.
- **b** En la pantalla Recuperar datos, en el campo Nombre de host, introduzca el nombre de dominio completo del extremo y, a continuación, haga clic en **Buscar**.
- **c** En el campo SED, seleccione una opción.
- **d** Haga clic en **Crear archivo de recuperación**.

  Se ha descargado el archivo **<nombrehost>-sed-recovery.dat**.

Obtener el archivo de recuperación - Cliente SED administrado localmente

1 Obtenga el archivo de recuperación.

Se ha generado el archivo y se puede acceder a él desde la ubicación de la copia de seguridad que seleccionó al instalar Dell Data Protection | Security Tools en el equipo. El nombre del archivo es *OpalSPkey<nombresistema>.dat*.

Realizar una recuperación

1 Mediante los medios de arranque creados, realice el inicio con dichos medios en un sistema de recuperación o en el dispositivo con la unidad que está intentando recuperar. Se abre un entorno de WinPE con la aplicación de recuperación.

2 Elija una opción y presione **Intro**.

3 Seleccione **Examinar**, busque el archivo de recuperación y, a continuación, haga clic en **Abrir**.

4 Seleccione una opción y haga clic en **Aceptar**.

- **Desbloqueo de una sola vez de la unidad**: este método omite y quita la PBA. Después, se puede volver a habilitar a través de la Remote Management Console (para un cliente SED administrado remotamente) o a través de la Consola del administrador de Security Tools (para un cliente SED administrado localmente).
- **Desbloquear unidad y quitar PBA**: este método desbloquea y, a continuación, quita la PBA de la unidad de manera permanente. Si quiere quitar la PBA tendrá que desactivar el producto desde la Remote Management Console (para un cliente SED administrado remotamente) o en el SO (para un cliente SED administrado localmente) si es necesario para volver a habilitar la PBA en el futuro. El inicio de sesión único no funcionará con la PBA quitada.

5 La recuperación está ahora completada. Presione cualquier tecla para volver al menú.

6 Presione **r** para reiniciar el equipo.

NOTA: Asegúrese de extraer cualquier medio USB o CD\DVD que utilizó para iniciar el equipo. Si no hace esto, es posible que se vuelva a iniciar al entorno de recuperación.

7 Después de reiniciar el equipo, debe tener un equipo en pleno funcionamiento. Si los problemas continúan, póngase en contacto con Dell ProSupport.

5

Recuperación de la clave de propósito general

Se utiliza la Clave de propósito general (GPK) para cifrar una parte del registro para los usuarios de dominio. Sin embargo, raras veces, durante el proceso de inicio se vuelve inutilizable y no se puede abrir. Si ocurre esto, se muestran los siguientes errores en el archivo CMGShield.log en el equipo cliente:

```
[12.06.13 07:56:09:622 GeneralPurposeK: 268] GPK - Failure while unsealing data [error = 0xd]
[12.06.13 07:56:09:622 GeneralPurposeK: 631] GPK - Unseal failure
[12.06.13 07:56:09:622 GeneralPurposeK: 970] GPK - Failure to get keys for the registry driver
```

Si no se puede abrir la GPK, ésta se debe recuperar. Para ello, extráigala del paquete de recuperación que se ha descargado del servidor.

Recuperar la GPK

Obtener el archivo de recuperación

Para descargar el archivo **LSARecovery_<nombremáquina_dominio.com>.exe** que se generó al instalar Dell Data Protection:

1. Abra la Remote Management Console y, desde el panel izquierdo, seleccione **Administración > Recuperar extremo**.
2. En el campo Nombre de host, introduzca el nombre de dominio completo del extremo y haga clic en **Buscar**.

3 En la ventana Recuperación mejorada, introduzca una Contraseña de recuperación y haga clic en **Descargar**.

NOTA: Debe recordar esta contraseña para acceder a las claves de recuperación.

Se ha descargado el archivo **LSARecovery_<nombremáquina_dominio.com>.exe**.

Realizar una recuperación

1 Mediante los medios de arranque creados en Apéndice A - Grabación del entorno de recuperación, realice el inicio con dichos medios en un sistema de recuperación o en el dispositivo con la unidad que está intentando recuperar.

Se abre un entorno WinPE.

2 Escriba **x** y presione **Intro** para obtener una solicitud de comandos.

3 Vaya al archivo de recuperación e inícielo.

Se abre el cuadro de diálogo de diagnóstico del cliente Encryption y se genera el archivo de recuperación en segundo plano.

4 En un símbolo del sistema administrativo, ejecute **LSARecovery_<nombremáquina_dominio.com>.exe –p <contraseña> -gpk**

Devuelve el archivo GPKRCVR.txt para su equipo.

5 Copie el archivo **GPKRCVR.txt** en la raíz de la unidad del SO del equipo.

6 Reinicie el equipo.

El sistema operativo consumirá el archivo GPKRCVR.txt y volverá a generar la GPK en ese equipo.

7 Si se le solicita, reinicie de nuevo.

6

Recuperación de datos con unidad de cifrado

Si el equipo de destino no puede iniciarse y no hay ningún error de hardware, la recuperación de datos se puede realizar en un equipo iniciado en un entorno de recuperación. Si el equipo de destino no puede iniciarse y ha fallado el hardware o es un dispositivo USB, la recuperación de datos se puede realizar iniciando en una unidad secundaria. Cuando utiliza una unidad, verá el sistema de archivos y podrá navegar por los directorios. Sin embargo, si intenta abrir o copiar un archivo, se producirá un error de *Acceso denegado*.

Recuperar datos con unidad de cifrado

Para recuperar datos con unidad de cifrado:

1. Para obtener la Id. de recuperación/DCID del equipo, seleccione una opción:
   a. Ejecute WSScan en cualquier carpeta donde se almacenan los datos cifrados comunes.
      Se muestra la Id. de recuperación/DCID de ocho caracteres después de “Común”.
   b. Abra la Remote Management Console y seleccione la pestaña **Detalles y acciones** para el extremo.
   c. En la sección Detalle de Shield de la pantalla Detalles de extremo, localice la Id. de recuperación/DCID.

2 Para descargar la clave desde el servidor, vaya a la utilidad Dell Administrative Unlock (**CMGAu**) y ejecútela.

La utilidad Dell Administrative Unlock se puede obtener desde Dell ProSupport.

3 En el cuadro de diálogo Dell Administrative Utility (CMGAu), introduzca la siguiente información (algunos campos se rellenan previamente) y haga clic en **Siguiente**.

Servidor:	Nombre del host completo del servidor, por ejemplo: Device Server: **https://<server.organization.com>:8081/xapi** Security Server: **https://<server.organization.com>:8443/xapi/**
Administrador de Dell:	El nombre de la cuenta del Administrador forense (habilitado en el servidor)
Contraseña del administrador de Dell:	La contraseña de la cuenta del Administrador forense (habilitado en el servidor)
MCID:	Borre el campo MCID
DCID:	La Id. de recuperación/DCID que ha obtenido antes.

4 En el cuadro de diálogo Dell Administrative Utility, seleccione **No, realizar ahora una descarga desde un servidor** y haga clic en **Siguiente**.

NOTA: Si no tiene instalado el cliente Encryption, se muestra el mensaje *Error al desbloquear*. Muévalo a un equipo que tenga instalado cliente Encryption.

5 Cuando la descarga y el desbloqueo se hayan completado, copie los archivos que necesite recuperar de esta unidad. Se pueden leer todos los archivos. ***No haga clic en Finalizar hasta que no haya recuperado los archivos***.

6 Cuando haya recuperado los archivos y ya pueda volver a bloquearlos, haga clic en **Finalizar**.

Después de hacer clic en Finalizar, los archivos cifrados ya no estarán disponibles.

7

Recuperación de BitLocker Manager

Para recuperar datos, obtenga una contraseña de recuperación o paquete de claves de la Remote Management Console, que le permitan desbloquear los datos en el equipo.

Recuperar datos

1. Inicie sesión como administrador de Dell en la Remote Management Console.
2. En el panel izquierdo, haga clic en **Administración** > **Recuperar datos**.
3. Haga clic en la pestaña *Manager*.
4. Para *BitLocker*:

   Introduzca la **Id. de recuperación** recibida de BitLocker. De manera opcional, si introduce el Nombre de host y el Volumen, se completará la Id. de recuperación.

   Haga clic en **Obtener contraseña de recuperación** o **Crear paquete de claves**.

   En función de la manera en que desee realizar la recuperación, utilizará la contraseña de recuperación o el paquete de claves para recuperar datos.

   Para el *TPM*:

   Introduzca el **Nombre de host**.

   Haga clic en **Obtener contraseña de recuperación** o **Crear paquete de claves**.

   En función de la manera en que desee realizar la recuperación, utilizará la contraseña de recuperación o el paquete de claves para recuperar datos.
5. Para completar la recuperación, consulte las Instrucciones de Microsoft para recuperación.

NOTA: Si BitLocker Manager no es "propietario" de TPM, la contraseña y el paquete de claves de TPM no estarán disponibles en la base de datos de Dell. Recibirá un mensaje de error indicando que Dell no puede encontrar la clave, que es el comportamiento esperado.

Para recuperar un TPM "con propietario" de una entidad distinta de BitLocker Manager, deberá seguir el proceso de recuperación del TPM de ese propietario específico o seguir su propio proceso existente para la recuperación del TPM.

A

Apéndice A - Grabación del entorno de recuperación

Grabación de la ISO del entorno de recuperación en un CD\DVD

El siguiente enlace contiene el proceso necesario para utilizar Microsoft Windows 7/8/10 para crear un CD o DVD de arranque para el entorno de recuperación.

http://windows.microsoft.com/en-us/windows7/burn-a-cd-or-dvd-from-an-iso-file

Grabación del entorno de recuperación en medios extraíbles

Para crear un USB de arranque, siga las instrucciones de este artículo de Microsoft:

https://technet.microsoft.com/en-us/library/jj200124(v=ws.11).aspx


0XXXXXA0X