Dell™ PowerVault™ Encryption Key Manager

Guía de inicio rápido de LTO Ultrium 4 y LTO Ultrium 5

En esta guía empezará con una ***configuración básica*** para el cifrado de las unidades de cintas de LTO Gen 4 y LTO Gen 5. Visite **http://support.dell.com** para descargar el último firmware de controlador y biblioteca antes de instalar y configurar Dell PowerVault Encryption Key Manager para asegurarse de que no tenga problemas.

Dell PowerVault Encryption Key Manager (Encryption Key Manager de aquí en adelante) es un programa de software Java™ que permite que las unidades de cinta habilitadas para el cifrado generen, protejan, almacenen y mantengan claves de almacenamiento. Estas claves se utilizan para cifrar la información que se graba en un soporte de cinta LTO, así como para descifrarla cuando se lee desde dicho soporte. Encryption Key Manager funciona en Linux® y Windows® y está diseñado para que sea un recurso compartido desplegado en varias ubicaciones de una empresa.

Este documento muestra con qué rapidez puede instalar y configurar Encryption Key Manager utilizando la GUI (interfaz gráfica de usuario) o mandatos. En este documento se muestra cómo utilizar el tipo de almacén de claves JCEKS, ya que es el más sencillo y transferible de los almacenes de claves soportados. Si desea más información acerca de un paso en particular u otro tipo de almacén de claves soportado, consulte la publicación *Dell Encryption Key Manager User's Guide*, que puede encontrarse en: **http://support.dell.com** o en el soporte Dell Encryption Key Manager proporcionado con su producto.

Nota: IMPORTANTE Encryption Key Manager INFORMACIÓN DE CONFIGURACIÓN DEL SERVIDOR DE HOST: Es recomendable que aquellas máquinas que alojen el programa Dell Encryption Key Manager utilicen memoria ECC para minimizar el riesgo de pérdida de datos. Encryption Key Manager realiza la función de solicitar la generación de claves de cifrado y de pasar dichas claves a las unidades de cintas LTO-4 y LTO-5. El material de las claves, empaquetado (formato cifrado) reside en la memoria del sistema mientras es procesado por Encryption Key Manager. Tenga en cuenta que el material de las claves debe ser transferido sin errores a la unidad de cinta correspondiente para que los datos escritos en un cartucho puedan ser recuperados (descifrados). Si, por alguna razón, el material de las claves resulta dañado debido a un error en la memoria del sistema y dicho material de claves se utiliza para grabar datos en un cartucho, no será posible recuperar los datos grabados en dicho cartucho (es decir, descifrados posteriormente). Existen métodos para asegurarse de que dichos errores no se produzcan. Sin embargo, si la máquina que aloja Encryption Key Manager no está utilizando memoria ECC (código de corrección de errores), existe la posibilidad de que el material de las claves haya resultado dañado mientras se encontraba en la memoria del sistema y dichos daños pueden provocar la pérdida de los datos. La posibilidad de que esto suceda es pequeña, pero siempre es recomendable que las máquinas que alojan aplicaciones vitales (como Encryption Key Manager) utilicen memoria ECC.

Primer paso: instalar el software Encryption Key Manager

1. Inserte el CD de Dell Encryption Key Manager. Si la instalación no se inicia automáticamente en Windows, navegue a la unidad de CD y efectúe una doble pulsación en el archivo Install_Windows.bat.

   En Linux la instalación no se inicia automáticamente. Vaya al directorio raíz del CD y entre `Install_Linux.sh`.

   Se visualizará un acuerdo de licencia de usuario final. Debe aceptar este acuerdo de licencia para proseguir con la instalación.

   Durante el proceso de instalación se copia todo el contenido (documentación, archivos de GUI y los archivos de propiedades de la configuración), necesario para el sistema operativo, desde el CD a la

unidad de disco duro. Durante la instalación, se revisa el sistema para buscar el IBM Java Runtime Environment correcto. Si no se encuentra, se instala automáticamente.

Cuando la instalación se ha completado, se inicia la interfaz gráfica de usuario (GUI).

Método 1: configuración de Encryption Key Manager utilizando la GUI

Este procedimiento crea una configuración básica. Tras finalizar correctamente la configuración, el servidor Encryption Key Manager se inicia.

1. Si la GUI no se inicia, ábrala como se indica a continuación:

   En Windows
   Navegue a c:\ekm\gui y pulse en `LaunchEKMGui.bat`

   En plataformas Linux
   Navegue a /var/ekm/gui y entre `. ./LaunchEKMGui.sh`
   Nota: Especifique . ./ (punto espacio punto barra inclinada) antes del mandato shell de Linux para asegurarse de que el shell pueda encontrar el script.

2. En la página Configuration Server EKM (Figura 1) entre los datos en todos los campos necesarios (indicados por un asterisco *). Pulse el signo de interrogación que aparece a la derecha de cualquier campo de datos para obtener una descripción. Pulse **Next** para ir a la página EKM Server Certificate Configuration.

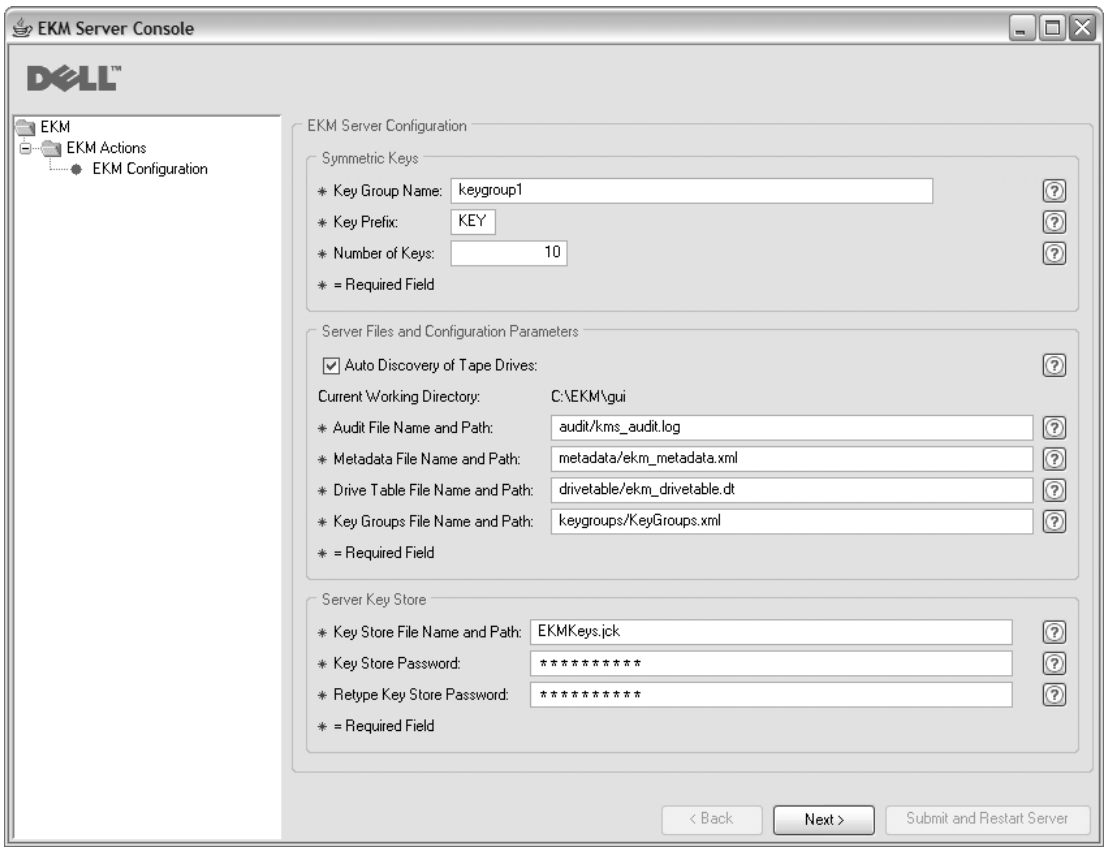

Figura 1. Página de configuración del servidor EKM

Notas:

a. Es necesario renovar el servidor Encryption Key Manager, utilizando para ello la GUI, después de haber añadido unidades mediante el descubrimiento automático, para garantizar que se almacenan en la tabla de controladores.

b. Una vez que haya establecido la contraseña del almacén de claves, **no la cambie**, salvo que su seguridad haya sido vulnerada. Las contraseñas se enmascaran para evitar cualquier riesgo de seguridad. Para cambiar la contraseña del almacén de claves tendrá que cambiar individualmente la contraseña de cada una de las claves del almacén de claves mediante el mandato **keytool**. Consulte el apartado "Changing Keystore Passwords" en la publicación *Dell Encryption Key Manager User's Guide*.

3. En la página EKM Server Certificate Configuration (Figura 2) entre el alias del almacén de claves y complete cualquier campo adicional que pueda servir para identificar el certificado y su finalidad. Pulse **Submit and Start Server**.

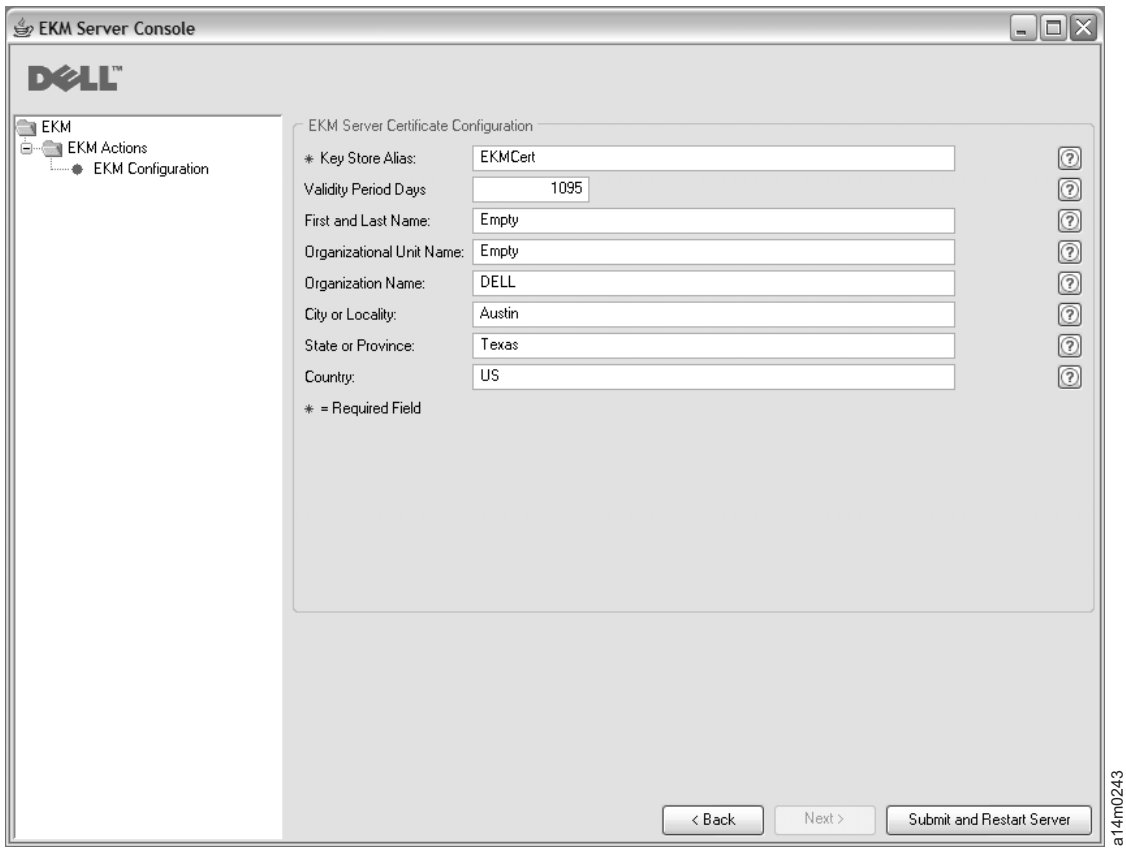

Figura 2. Página EKM Server Certificate Configuration

Nota: Detener la GUI de Encryption Key Manager durante la generación de claves hará que sea necesario reinstalar Encryption Key Manager.

El archivo de almacén de claves resultará dañado si detiene el proceso de generación de claves de Encryption Key Manager antes de que finalice. Para recuperarse de este suceso, siga estos pasos:

- Si se ha detenido Encryption Key Manager durante la instalación inicial, navegue hasta su directorio (por ejemplo, x:\ekm). Suprima este directorio y reinicie la instalación.
- Si Encryption Key Manager ha sido detenido mientras se estaba añadiendo un nuevo grupo de claves, detenga el servidor Encryption Key Manager y restaure su archivo de almacén de claves con la copia de seguridad más reciente del almacén de claves (este archivo se encuentra en la carpeta x:\ekm\gui\backupfiles). Tenga en cuenta que el archivo de copia de seguridad contiene la indicación de la fecha y hora como parte del nombre de archivo (por ejemplo, 2007_11_19_16_38_31_EKMKeys.jck). La indicación de la fecha y hora deberá eliminarse una vez se copie el archivo en el directorio x:\ekm\gui. Reinicie el servidor Encryption Key Manager y añada el grupo de claves interrumpido anteriormente.

4. Se abrirá una ventana de copia de seguridad (Figura 3) que le recordará que debe realizar una copia de sus archivos de datos de Encryption Key Manager. Entre la vía de acceso al directorio en el que desea guardar los datos de copia de seguridad. Pulse **Backup**.

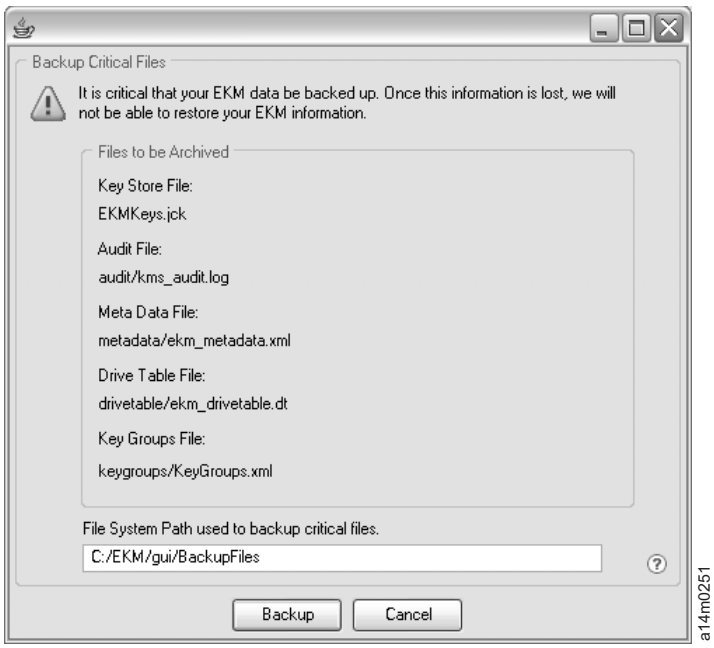

Figura 3. Backup Critical Files Window

5. Se visualizará la página de inicio de sesión del usuario. Entre el nombre de usuario predeterminado EKMAdmin y la contraseña predeterminada changeME. Pulse **Iniciar sesión**.

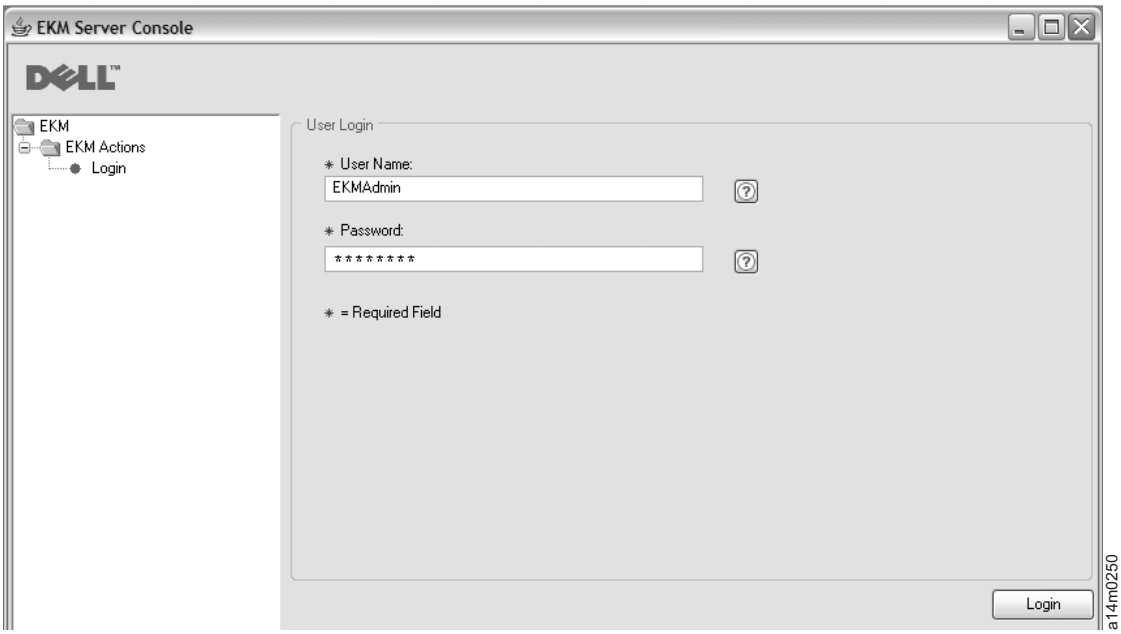

Figura 4. Página de inicio de sesión del usuario

El servidor Dell Encryption Key Manager se inicia en segundo plano.

6. Seleccione **Server Health Monitor** en el navegador de la GUI para verificar que el servidor Encryption Key Manager está activo.

Cómo encontrar la dirección IP del host correcta

Es posible que las limitaciones en la GUI actual de Encryption Key Manager impidan que aparezca la dirección IP del host de Encryption Key Manager en Server Health Monitor:

- Si el host está configurado con una dirección IPv6, la aplicación Encryption Key Manager no podrá mostrar la dirección IP.
- Si la aplicación Encryption Key Manager está instalada en un sistema Linux, la aplicación Encryption Key Manager mostrará la dirección del host local y no el puerto IP activo real.

a. Para recuperar la dirección IP real del sistema host, encuentre la dirección del puerto IP accediendo a la configuración de red.
   - En un sistema Windows, abra una ventana de mandatos y especifique `ipconfig`.
   - En linux, especifique `isconfig`.

Cómo identificar el puerto SSL de EKM

a. Inicie el servidor Encryption Key Manager utilizando la línea de mandatos.
   - En Windows, navegue a cd `c:\ekm` y pulse **startServer.bat**
   - En plataformas Linux, navegue a `/var/ekm` y escriba `startServer.sh`
   - Consulte el apartado "Starting, Refreshing, and Stopping the Key Manager Server" en la publicación *Dell Encryption Key Manager User's Guide* para obtener más información.
b. Inicie el cliente CLI utilizando la línea de mandatos.
   - En Windows, navegue a cd `c:\ekm` y pulse **startClient.bat**
   - En plataformas Linux, navegue a `/var/ekm` y escriba `startClient.sh`
   - Consulte el apartado "Starting the Command Line Interface Client" en la publicación *Dell Encryption Key Manager User's Guide* para obtener más información.
c. Inicie sesión en un cliente CLI en el servidor Encryption Key Manager utilizando el siguiente mandato:

   ```
   login –ekmuser ID_usuario –ekmpassword contraseña
   ```

   donde *ID_usuario* = EKMAdmin y *contraseña* = changeME (esta es la contraseña predeterminada. Si ha cambiado anteriormente la contraseña predeterminada, utilice la nueva contraseña.)

   Una vez haya iniciado correctamente la sesión, aparecerá el mensaje `User successfully logged in.`
d. Identifique el puerto SSL especificando el siguiente mandato:

   ```
   status
   ```

   La respuesta en pantalla debería ser similar a la siguiente: `server is running. TCP port: 3801, SSL port: 443.`

   Anote el puerto configurado SSL y compruebe que es el puerto utilizado para configurar los valores de cifrado gestionados por biblioteca.
e. Cierre la sesión de la línea de mandatos. Especifique el siguiente mandato:

   ```
   exit
   ```

   Cierre la ventana de mandatos.

Método 2: configuración de Encryption Key Manager utilizando mandatos

Paso 1. Cree un almacén de claves JCEKS

PRECAUCIÓN: es muy recomendable realizar una copia de Encryption Key Manager y de todos los archivos asociados de forma regular. Si las claves de cifrado de Encryption Key Manager se pierden o están dañadas, no hay ningún método para recuperar los datos cifrados.

Cree un almacén de claves y llénelo con una clave privada y un certificado. El certificado se utiliza para proteger las comunicaciones entre servidores Encryption Key Manager y con el cliente CLI de Encryption Key Manager. El mandato **keytool** crea un nuevo almacén de claves JCEKS denominado EKMKeys.jck y lo llena con una clave privada y certificada con el alias ekmcert. Este certificado es válido durante 5 años. Cuando este certificado caduca, es posible que las comunicaciones entre los servidores Encryption Key Manager y entre el cliente CLI de Encryption Key Manager y el servidor Encryption Key Manager dejen de funcionar. Elimine el antiguo certificado que ha caducado y cree uno nuevo, tal como se especifica en este paso.

```
keytool -keystore EKMKeys.jck -storetype jceks -genkey -alias ekmcert -keyAlg RSA -keysize 2048 –validity 1825
```

El mandato keytool le solicitará información para crear un certificado que permita su identificación Encryption Key Manager. Las solicitudes, con respuestas de muestra, se parecen a las siguientes:

```
¿Cuál es tu
nombre y apellidos? [Desconocido]:  ekmcert
¿Cuál es el nombre de su unidad organizativa?   [Desconocido]:  EKM
¿Cuál es el nombre de su organización?
[Desconocido]:  Dell
¿Cuál es el nombre de su ciudad o localidad?   [Desconocido]: Austin
¿Cuál es el nombre de su estado o provincia?   [Desconocido]:  TX
¿Cuál es el código de país para esta unidad? [Desconocido]:  US
¿Es CN=ekmcert, OU=EKM, O=Dell, L=Austin, ST=TX, C=US correcto? (escriba "sí"
o "no"):
```

Escriba `sí` y pulse Intro.

Paso 2. Genere claves de cifrado

Nota: Antes de utilizar por primera vez el mandato keytool en cualquier sesión, ejecute el script **updatePath** para establecer el entorno correcto.

En Windows
Navegue a `cd c:\ekm` y pulse updatePath.bat

En plataformas Linux
Navegue a /var/ekm y entre `. ./updatePath.sh`
Nota: Especifique . ./ (punto espacio punto barra inclinada) antes del mandato shell de Linux para asegurarse de que el shell pueda encontrar el script.

Para el cifrado LTO, Encryption Key Manager necesita que se pregenere y almacene en un almacén de claves un número de claves simétricas. El mandato **keytool** genera 32 claves AES de 256 bits y las almacena en el almacén de claves creado en el paso 3. Ejecute este mandato desde el directorio de Encryption Key Manager para crear el archivo del almacén de datos en dicho directorio. Las claves resultantes tendrán los nombres van desde key000000000000000000 hasta key00000000000000001f.

```
keytool –keystore EKMKeys.jck –storetype jceks –genseckey –keyAlg aes –keysize 256 –aliasrange key00-1f
```

Este mandato le solicita una contraseña del almacén de claves para acceder al almacén de claves. Entre la contraseña que quiera y pulse Intro. Pulse Intro de nuevo cuando se le solicite una contraseña de clave, ya que esa información no es necesaria. No escriba una contraseña nueva o diferente. Esto conllevará que la contraseña de la clave sea la misma que la contraseña del almacén de claves. Tenga en cuenta que deberá volver a escribir la contraseña del almacén de claves especificada aquí cuando inicie Encryption Key Manager posteriormente.

Nota: Una vez que haya establecido la contraseña del almacén de claves, no la cambie, salvo que su seguridad haya sido vulnerada. El cambio de contraseña del almacén de claves conlleva asimismo el cambio de todas las propiedades de contraseña en el archivo de configuración. Las contraseñas se enmascaran para evitar cualquier riesgo de seguridad.

Paso 3. Inicie el servidor Encryption Key Manager

Para iniciar el servidor Encryption Key Manager sin la GUI, inicie el script startServer:

En Windows
Navegue a `cd c:\ekm\ekmserver` y pulse startServer.bat

En plataformas Linux
Navegue a /var/ekm/ekmserver y entre `. ./startServer.sh`
Nota: Especifique . ./ (punto espacio punto barra inclinada) antes del mandato shell de Linux para asegurarse de que el shell pueda encontrar el script.

PRECAUCIÓN: es muy recomendable realizar una copia de Encryption Key Manager y de todos los archivos asociados de forma regular. Si las claves de cifrado de Encryption Key Manager se pierden o están dañadas, no hay ningún método para recuperar los datos cifrados.

Paso 4. Inicie el cliente de la interfaz de línea de mandatos de Encryption Key Manager

Para iniciar el cliente CLI de Encryption Key Manager, inicie el script startClient:

En Windows
Navegue a `cd c:\ekm\ekmclient` y pulse startClient.bat

En plataformas Linux
Navegue a /var/ekm\ekmclient y pulse `. ./startClient.sh`
Nota: Especifique . ./ (punto espacio punto barra inclinada) antes del mandato shell de Linux para asegurarse de que el shell pueda encontrar el script.

Una vez que el cliente de interfaz de línea de mandatos haya iniciado sesión satisfactoriamente en el servidor del gestor de claves, puede ejecutar cualquier mandato de interfaz de línea de mandatos. Utilice el mandato quit para cerrar el cliente de interfaz de línea de mandatos cuando haya finalizado. El cliente se cerrará automáticamente cuando esté 10 minutos sin utilizarse. Para obtener más información sobre mandatos de CLI, Consulte la publicación *Dell Encryption Key Manager User's Guide*, que puede encontrarse en: **http://support.dell.com** o en el soporte de Dell Encryption Key Manager proporcionado con su producto.

Para obtener más información

Consulte las siguientes publicaciones para obtener más información.

- *Dell Encryption Key Manager User's Guide* (incluida en su CE de Dell Encryption Key Manager CD y disponible en **http://support.dell.com**).
- En la documentación técnica *Library Managed Encryption for Tape* se ofrece métodos recomendados para el cifrado de cintas LTO (disponible en **http://www.dell.com**).