Library-Managed Encryption for Tape

Cifrado de hardware de LTO administrado por biblioteca en bibliotecas de automatización cintas Dell™ PowerVault™.

Grupo de productos Dell | Ingeniería de almacenamiento
Marzo de 2016

Notas técnicas de Dell

Revisiones

Fecha	Descripción
Enero de 2015	Revisión 2.0
Noviembre de 2015	Revisión 3.0
Marzo de 2016	Revisión 4.0

Reconocimientos

Este documento fue producido por el equipo de Ingeniería de almacenamiento.

Autor: Libby McTeer, ingeniero principal de almacenamiento

Este documento solo tiene propósitos informativos y puede contener errores tipográficos e imprecisiones técnicas. El contenido se proporciona “tal cual”, sin garantías expresas ni implícitas de ningún tipo.

© 2016 Dell Inc. Todos los derechos reservados. Queda estrictamente prohibida la reproducción de este material de cualquier forma sin la expresa autorización por escrito de Dell Inc. Para obtener más información, comuníquese con Dell. Dell, el logotipo de DELL y el distintivo de DELL son marcas registradas de Dell Inc. Es posible que en este documento se utilicen otras designaciones o marcas comerciales para hacer referencia a las entidades titulares de las marcas y designaciones o a sus productos. Dell niega todo derecho de propiedad sobre las marcas y designaciones de terceros.

Tabla de contenido

TOC

Tablas

TOC

Figuras

TOC

Resumen

Una mayor seguridad para los datos en reposo está disponible a través de un cifrado de hardware de unidades de cintas LTO administrado por biblioteca en las bibliotecas de automatización de cintas TL1000, TL2000, TL4000 y ML6000 Dell PowerVault.

¿Qué es el cifrado?

El cifrado es el proceso de tomar datos de texto claro y convertirlos en datos ilegibles para cualquiera que no tenga la clave de descifrado. La solidez de un algoritmo, o cuánto le tomaría a alguien averiguar el cifrado, se basa en el algoritmo utilizado y en la longitud de la clave de cifrado. Las claves de cifrado más largas proporcionan mayor seguridad.

¿Por qué debería usar el cifrado?

Las leyes en muchos estados requieren protección de los datos de identificación personal del cliente, no solo una notificación después de una violación de seguridad. Debido a la proliferación de datos de identificación personal como números de tarjetas de crédito, los negocios de proveedores de servicio autónomos hasta las empresas grandes deben tomar medidas para cumplir con las leyes.

Las reglamentaciones federales de privacidad tales como HIPAA, que cubre la información de la salud, y la Ley Gramm-Leach-Bliley, que cubre los datos financieros, están en las noticias debido a la violación de datos. Las leyes federales de privacidad también cubren la protección de datos del cliente en áreas tales como la industria del cable y de las telecomunicaciones, el censo de los Estados Unidos y el departamento de vehículos automotores.

Estas reglamentaciones requieren que las empresas divulguen al público cuando estos datos se vean comprometidos. Estas divulgaciones cuestan millones de dólares en ventas perdidas y en reputación perdida. El cifrado de hardware de unidades de cinta LTO trata el modelo de amenaza de las cintas perdidas o robadas. Si hay datos sensibles cifrados en los medios de cinta, los datos no pueden estar comprometidos incluso si la cinta se pierde o se roba.

Descripción general del método de cifrado

Existen tres maneras básicas de cifrar los datos almacenados en los medios de cinta:

- Cifrado"de"software
- Cifrado"a"través"de"un"dispositivo"de"hardware"en"línea
- Cifrado"de"hardware

El cifrado de software se realiza mediante la aplicación de software de respaldo en cinta antes de enviar los datos a la unidad de cinta. El cifrado de software puede ser de uso intensivo de CPU y puede provocar una degradación del rendimiento en el servidor host según el tipo y el tamaño de los datos a cifrar. El

cifrado de software es transparente para la unidad de cinta/biblioteca ya que los datos se cifran antes de llegar al hardware.

Al utilizar un dispositivo de hardware en línea, los datos se envían desde el servidor de medios hasta el dispositivo de cinta a través del dispositivo. El dispositivo cifra los datos antes de transmitir los datos al dispositivo de cinta. El cifrado a través del dispositivo en línea es transparente para el software de respaldo en cinta y el dispositivo de cinta. A menudo, este método de cifrado requiere un hardware costoso de terceros para la administración de políticas y claves. Los niveles más elevados del certificado de procesamiento de información federal (FIPS, Federal Information Processing) requieren el uso de dispositivos de cifrado para respaldar las claves utilizadas para cifrar los datos. La Figure 1 muestra la configuración del sistema que utiliza un dispositivo de hardware en línea.

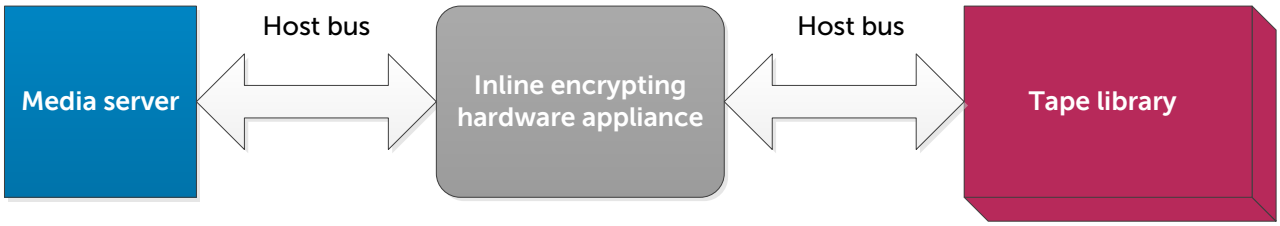

Figure 1 Configuración del dispositivo de hardware en línea

Al utilizar un cifrado de hardware, el motor de cifrado en LTO-4 y en unidades de cinta de generaciones posteriores se utiliza para cifrar los datos utilizando una clave provista por el software de respaldo en cinta o por un servidor de administración de claves de cifrado externo. El cifrado de hardware es eficiente debido a que la función de cifrado se descarga a la unidad desde la CPU afectando muy poco el rendimiento o sin afectarlo. El cifrado de hardware también es rentable, ya que no requiere un hardware costoso de terceros.

Aspectos básicos del cifrado LTO

El cifrado basado en unidades LTO se anunció por el consorcio LTO en 2007. LTO-4 y las unidades de cinta de generaciones posteriores utilizan un algoritmo Galois Counter Mode (GCM) de estándar Advanced Encryption Standard (AES) con claves de cifrado de 256 bits para cifrar y descifrar datos en LTO-4 y medios de generaciones posteriores. Este algoritmo es un cifrado de bloque AES-256 aprobado por el Instituto Nacional de Estándares y Tecnología (NIST, National Institute of Standards and Technology). Para obtener más detalles sobre el algoritmo GCM, visite http://csrc.nist.gov/publications y busque “Galois Counter Mode”.

Si la compresión se encuentra habilitada, la unidad cifrará los datos después de que se realice la compresión. A continuación, los datos se reformatean al formato Ultrium antes de que se escriban en los medios. El cifrado puede causar una ligera degradación del rendimiento debido a la autenticación/sobrecarga de la transmisión de claves y el algoritmo de cifrado mismo, pero no debería incrementar la ventana de respaldo. Se puede experimentar cierta pérdida de capacidad en los medios si se utilizan tamaños de bloque pequeños o si hay cambios frecuentes en las claves.

Capas de administración de cifrado

En las bibliotecas de cintas TL1000, TL2000, TL4000 y ML6000 de Dell PowerVault, el LTO-4 y las unidades de cinta de generaciones posteriores cifran y descifran los datos. La unidad sola no puede identificar si los datos que recibe deberían estar cifrados o si deberían generar la clave de cifrado. Se utiliza una capa de administración de cifrado para determinar qué datos se cifrarán (conocidos como política) y proporciona la clave de cifrado a la unidad. Hay dos métodos de administración de cifrado LTO:

- Cifrado"administrado"por"la"aplicación"(AME,"application-managed"encryption).
- Cifrado"administrado"por"la"biblioteca"(LME,"library-managed"encryption).

Cifrado administrado por la aplicación

Las bibliotecas de cintas PowerVault admiten AME con una aplicación de software de respaldo en cinta que admite el cifrado LTO. Consulte la documentación para el software de respaldo en cinta para determinar si se admite el cifrado de hardware basado en LTO.

En el caso del cifrado administrado por la aplicación, el software de respaldo en cinta determina qué datos se cifrarán y proporciona la clave para la unidad sobre el bus de host. Además de proporcionar las claves para la unidad, el software de respaldo en cinta es responsable de generar, almacenar y administrar las claves.

El cifrado es transparente para la biblioteca cuando se utiliza AME. AME puede ofrecer una mayor granularidad en la que los datos se cifran, ya que los datos se pueden cifrar trabajo por trabajo si el software de respaldo en cinta lo admite. Si el cifrado administrado por la aplicación se selecciona como parte de la configuración del cifrado de biblioteca, solo el software de respaldo en cinta tendrá permitido proporcionar claves a la unidad. No se requiere una clave de licencia de activación de cifrado administrado por la biblioteca para utilizar el cifrado administrado por la aplicación en las bibliotecas de cintas de Dell.

Cifrado administrado por la biblioteca

En caso de un cifrado administrado por la biblioteca en las bibliotecas de cintas de PowerVault, existe una política muy limitada para el cifrado de datos. Todos los datos escritos para las unidades LTO en una partición habilitada para el cifrado administrado por la biblioteca estarán cifrados. La única excepción son los datos escritos en los medios que no están inicialmente cifrados desde el comienzo de la cinta (BOT, beginning of tape). En este caso, los datos escritos en los medios no se cifrarán.

La biblioteca sirve como el proxy para proporcionar claves a la unidad desde la tienda de claves en la aplicación Security Key Lifecycle Manager (SKLM) de IBM®. Consulte la sección “

How to purchase IBM SKLM software" para conocer más detalles sobre cómo obtener la aplicación.

¿Cómo elijo?

Seguridad

Las preocupaciones de seguridad se deberían considerar al realizar la selección entre AME y LME. Cuando se utiliza AME, las claves se pueden transmitir sin protección y no se cifran entre el servidor de medios y la unidad en el bus de host. De acuerdo con la seguridad física en el centro de datos, es posible que esto no sea una preocupación por los dispositivos de ataque directo, pero la preocupación puede ser mucho mayor en un entorno de canal de fibra SAN en donde el medio de conexión se comparta entre varios hosts. La especificación T10 ahora proporciona un método de empaquetado (cifrado) de las claves de cifrado durante la transmisión por los bus de host. Consulte la documentación del software de respaldo en cinta para determinar si su aplicación admite el empaquetado de clave de cifrado para la transmisión. Las claves nunca se transmiten sin protección al utilizar LME en las bibliotecas de cintas PowerVault.

Granularidad de la política de cifrado

AME puede ofrecer una granularidad más fina en la determinación de qué datos se cifrarán. Se puede seleccionar qué trabajos de respaldo cifrar o no cifrar utilizando la misma unidad LTO. Para lograr un nivel similar de granularidad con LME, se requerirían varias particiones de biblioteca así como una mayor administración para dirigir los trabajos de respaldo a la partición adecuada (cifrada o descifrada).

Administración de claves

Considere la administración de claves, el proceso de proporcionar claves a la unidad para el cifrado, cuando tenga que escoger entre AME y LME. AME ofrece una administración de claves centralizada dentro de una instancia única de aplicación de software de respaldo en cinta, pero puede haber límites en la migración de la clave de cifrado. LME ofrece una administración de claves centralizada que, como la aplicación SKLM de IBM, puede proporcionar claves a varias bibliotecas y a varios tipos de bibliotecas como TL1000, TL2000, TL4000 y ML6000 simultáneamente. Esto permite un mayor intercambio y migración de cintas entre las bibliotecas; las cintas se pueden intercambiar entre las bibliotecas de PowerVault siempre que las bibliotecas puedan acceder a la misma tienda de claves SKLM de IBM. Mantener la aplicación SKLM de IBM no requiere responsabilidad adicional para el administrador del sistema.

La Table 1 resume las ventajas y desventajas del cifrado administrado por la aplicación y administrado por la biblioteca.

Table 1 Comparación entre AME y LME

Capa de administración	Granularidad de la política	Ventajas	Desventajas
Administrado por la aplicación	Puede haber más de una clave por cinta.	Granularidad de la política más fina.	La clave se puede transmitir sin protección a la unidad.

	Puede haber una clave por fragmento de datos o trabajo de respaldo.	Menos nueva responsabilidad para el administrador del almacenamiento.	Administración centralizada de claves limitada. Intercambio/migración limitada.
Administrado por la biblioteca	Una clave por cinta. Cifrado habilitado a nivel de la partición.	Clave cifrada al transmitirse a la unidad. Administración centralizada de claves. Independiente de la aplicación.	Política limitada. Más responsabilidad para el administrador del almacenamiento.

Solución de cifrado administrado por la biblioteca de Dell

La configuración de cifrado administrado por la biblioteca difiere de una configuración normal de respaldo en cintas por biblioteca en que un servidor que ejecuta la aplicación SKLM de IBM se requiere para proporcionar claves de cifrado a la unidad a través de la interfaz Ethernet de administración de biblioteca. En la solución de Dell, el servidor de claves está separado de la biblioteca de cintas. Debe asegurarse de que el rendimiento y el tiempo de respuesta del servidor de claves no se vean afectados por otras aplicaciones que se ejecuten en el mismo servidor físico para garantizar que las claves estén disponibles para los respaldos programados. La biblioteca y el servidor de claves se pueden comunicar a través de las redes IPv4 e IPv6.

El cifrado administrado por la biblioteca en la biblioteca está configurado a nivel de la partición. Una partición que tiene el cifrado habilitado debe contar con al menos una unidad de cinta de generación posterior o LTO-4. Sólo las unidades capaces de realizar el cifrado se pueden utilizar en una partición que tenga cifrado habilitado; las unidades LTO-3 no se admiten en la partición con cifrado habilitado. Todos los medios LTO-4 y de generaciones posteriores asignados a la partición con cifrado habilitado se cifrarán. La única excepción son los datos escritos en los medios que no están inicialmente cifrados desde el comienzo de la cinta (BOT). Los medios LTO-1, LTO-2 y/o LTO-3 no se cifrarán incluso si se asignan a una partición con cifrado habilitado.

Para evitar una posible pérdida de datos debido a una falla en el servidor de claves, Dell recomienda utilizar una configuración del servidor SKLM de IBM primario y secundario. Esta configuración proporciona redundancia en el caso de que el servidor primario de claves esté caído o no se encuentre disponible. Cada partición con cifrado habilitado en la biblioteca se pueden configurar para hasta dos servidores de claves. Las configuraciones del servidor SKLM deben ser idénticas para permitir el acceso ininterrumpido a los datos en los medios. Security Key Lifecycle Manager Information Center de IBM proporciona la documentación necesaria para instalar y configurar los servidores de clave primarios y secundarios. Para obtener más información, visite http://www-

01.ibm.com/support/knowledgecenter/#!/SSWPVP_2.5.0/com.ibm.sklm.doc_2.5/welcome.htm (para otros idiomas, cambie la selección del país en la parte superior de la página).

La aplicación SKLM de IBM consta de una tabla de unidades, un archivo de configuración y una tienda de claves. La tabla de unidades mantiene una lista de unidades que se han autenticado para el servidor de claves. El archivo de configuración se utiliza para establecer las configuraciones del servidor de claves tales como la detección automática de unidades. La tienda de claves es una base de datos DB2 que contiene todas las claves que se han generado para esa tienda de claves. Las claves están disimuladas en la base de datos y nunca están visibles libremente.

Los siguientes pasos detallan el proceso para proporcionar la clave de cifrado a la unidad. Consulte también la Figure 2 para obtener una representación ilustrada del proceso.

1. Cuando la cinta cifrada se coloca en la unidad en una partición que permite el cifrado, la unidad solicitará una clave desde el servidor de claves a través de la biblioteca. La biblioteca transmitirá la solicitud de clave al servidor de claves por la interfaz Ethernet de administración.
2. El servidor de claves autentica la unidad que realiza la solicitud a través de una clave privada asociada con el certificado digital en la unidad. La unidad y el servidor de claves establecen una clave de sesión pública/privada utilizada para proteger la clave para el tránsito.
3. La clave (DK) se trae desde la tienda de claves.
4. El servidor de claves entrega la clave de cifrado a la biblioteca protegida en la clave de sesión para seguridad. La biblioteca proporciona la clave protegida a la unidad a través del puerto de control de la biblioteca en la unidad. La clave de cifrado nunca se transmite sin protección entre el servidor de claves y la biblioteca. La clave nunca se almacena en los medios.
5. La unidad quita la protección de la clave de cifrado mediante el uso de la clave de sesión y utiliza la clave de cifrado para cifrar o descifrar los datos según sea necesario.
6. El identificador de clave de datos de texto claro (DKi, data key identifier) proporcionado por el servidor de claves se escribe para la cinta de modo que la clave de cifrado se pueda identificar más adelante para adiciones o restauraciones. La relación entre la clave de cifrado y el DKi se almacena en un formato cifrado en el servidor de claves.

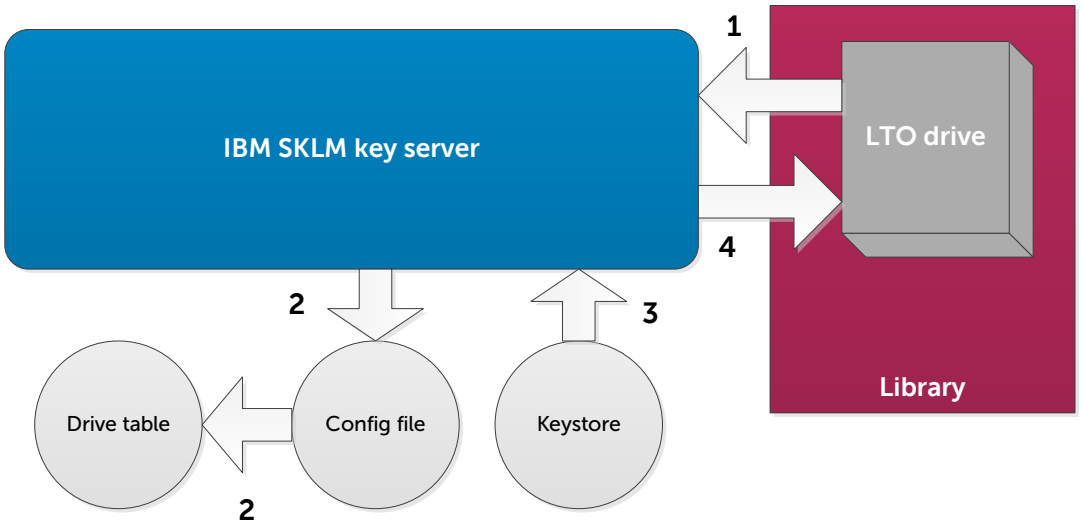

Figure 2 Flujo de datos del servidor de claves.

La unidad conservará la clave de cifrado hasta que los medios actuales se desmonten o hasta que se retire la alimentación de la unidad. Esto es para garantizar la seguridad de la clave de cifrado cuando esté fuera de la tienda de claves cifradas.

Solo se utiliza una clave de cifrado por cinta al utilizar el cifrado administrado por la biblioteca en las bibliotecas de cintas PowerVault. Según cuántas claves haya en la tienda de claves y cómo esté configurada la tienda de claves, una clave se puede utilizar para más de una cinta.

Consulte las notas técnicas de "Cumplimiento de la reglamentación de privacidad de las bibliotecas de cintas Dell ™ PowerVault ™" para las arquitecturas de referencia de cifrado administrado por la biblioteca para clientes de pequeñas y medianas empresas y clientes de empresas grandes.

Cómo adquirir el software SKLM de IBM

Los clientes de Dell pueden adquirir el software SKLM de IBM directamente desde IBM. Para adquirir el software dentro de Estados Unidos, visite http://www-03.ibm.com/software/products/en/key-lifecycle-manager-dell. Para adquirir el software en otro país, cambie la selección de país en la parte superior de la página. Estas páginas solamente enumeran los requisitos de adquisición para los clientes de Dell que utilizan bibliotecas de cintas PowerVault. Los clientes de Dell con relaciones de ventas de IBM existentes pueden aprovechar esas relaciones para la adquisición. Las licencias de unidades SKLM y el mantenimiento de software después del primer año se pueden adquirir por parte de IBM.

La vida de ventas del software Dell Encryption Key Manager 3.0 ha finalizado. Los clientes que adquieran licencias de cifrado administrado por la biblioteca para sus bibliotecas de cintas PowerVault deberán adquirir el software de Security Key Lifecycle Manager de IBM desde IBM.

Los clientes de Dell que actualmente utilizan el Dell Encryption Key Manager 3.0 (EKM 3.0) pueden utilizar el software hasta el fin de la vida de soporte de las bibliotecas de cintas TL2000, TL4000 y ML6000 PowerVault. Sin embargo, ninguna actualización ni arreglo del hardware ni del sistema operativo estará disponible para el software EKM 3.0. Los clientes que necesiten actualizaciones del sistema operativo como Microsoft Windows 2012 o actualizaciones de hardware como LTO-7 y TL1000 deberán adquirir el software SKLM de IBM.

Cómo adquirir el cifrado administrado por la biblioteca en TL1000 PowerVault

Las bibliotecas de cintas TL1000 de PowerVault que admiten el cifrado administrado por la biblioteca se pueden adquirir solamente en el punto de venta. El cifrado administrado por la biblioteca no se puede habilitar en las bibliotecas de cintas TL1000 existentes, y esta función no se puede adquirir después del punto de venta como sucede con otras bibliotecas de cintas de PowerVault.

El cifrado administrado por la biblioteca solamente está disponible en bibliotecas de cintas TL1000 LTO-6 y de generaciones posteriores. Los clientes que actualmente estén utilizando medios cifrados LTO-4 deberán adquirir la configuración LTO-6 debido a la limitación de lectura de la compatibilidad con versiones anteriores n-2 de los medios y las unidades LTO.