Library-Managed Encryption for Tape

Libby McTeer

Dell Product Group| Storage Engineering

December 2011| Rev 1.0

Contents

Tables

Figures

Abstract

Increased security for data at rest is available via library-managed LTO4 and LTO5 hardware encryption on the Dell ™ PowerVault ™ TL2000, TL4000, and ML6000 tape automation libraries.

What is Encryption?

Encryption is the process of taking clear text data and converting it to data unreadable by anyone not possessing the decrypting key. The strength of the algorithm, i.e. how long it would take someone to break the encryption, is based on the algorithm used and the length of the encrypting key. Longer encryption keys provide greater security.

Why Should I Use Encryption?

New laws in many states require protection of personally identifiable customer data, not just notification after a security breach. Due to the proliferation of personally identifiable data like credit card numbers, businesses from self-employed service providers to large enterprise companies need to take measures to be in compliance.

Federal privacy regulations such as HIPAA covering health information and the Gramm-Leach-Bliley Act covering financial data are in the news due to data breaches. Federal privacy laws also cover the safeguard of customer data in areas such as the cable and telecommunications industry, the US census, the department of motor vehicles, and even DVD rentals.

These regulations require that companies disclose to the public when data is compromised. These disclosures cost millions of dollars in lost sales and lost reputation. LTO4 and LTO5 hardware encryption addresses the threat model of lost or stolen tapes. If sensitive data is encrypted on the tape media, the data cannot be compromised even if the tape is lost or stolen.

Encryption Method Overview

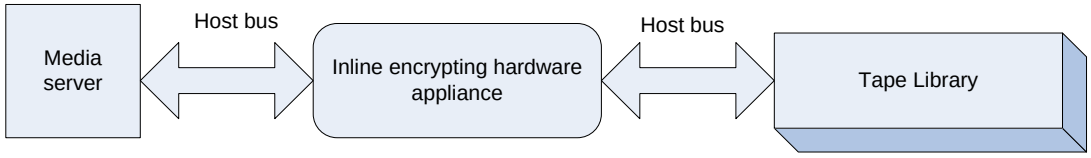
There are 3 basic ways to encrypt data stored on tape media:

- Software encryption
- Encryption via inline hardware appliance
- Hardware encryption

Software encryption is performed by the tape backup software application prior to sending the data to the tape drive. Software encryption can be CPU-intensive and can cause performance degradation on the host server depending on the type and size of the data to be encrypted. Software encryption is transparent to the tape drive/library as the data is encrypted prior to reaching the hardware.

When using an inline hardware appliance, the data is sent from the media server to the tape device through the appliance. The appliance encrypts the data before passing the data to the tape device. Encryption via inline appliance is transparent to the tape backup software and the tape device. This method of encryption often requires expensive third party hardware for policy and key management. Higher levels of Federal Information Processing (FIPS) certification require the use of appliances for encryption to safeguard the keys used to encrypt the data. Figure 1 shows the system configuration using an inline hardware appliance.

Figure 1. Inline Hardware Appliance Configuration



When using hardware encryption, the encryption engine in the LTO4 or LTO5 drive is used to encrypt the data using a key provided by the tape backup software or another external source. Hardware encryption is efficient due to the encryption function being offloaded to the drive from the CPU with little or no performance impact. Hardware encryption is also cost effective as it does not require expensive third party hardware.

LTO Encryption Basics

LTO drive-based encryption was announced by the LTO consortium in January 2007. LTO4 and LTO5 drives use a standard Advanced Encryption Standard (AES) Galois Counter Mode (GCM) algorithm with 256-bit encrypting keys to encrypt and decrypt data on the LTO4 and LTO5 media. This algorithm is a National Institute of Standards and Technology (NIST) approved AES-256 block cipher. More details on the GCM algorithm can be found by searching for "Galois Counter Mode" at http://csrc.nist.gov/publications.

If compression is enabled, the drive will encrypt the data after it is compressed. The data is then reformatted to the Ultrium format before it is written to the media. Encryption can cause a slight performance degradation due to authentication/key passing overhead and the encryption algorithm itself but should not increase the backup window. Some capacity loss on the media may be experienced if small block sizes are used or if there are frequent key changes.

Encryption Management Layers

On the Dell PowerVault TL2000, TL4000, and ML6000 tape libraries, the data encryption and decryption is performed by the LTO4 and/or LTO5 drives in the library. The drive alone cannot identify whether the data it receives should be encrypted or generate the encryption key. An encryption management layer is used to determine what data will be encrypted (referred to as policy) and provides the encryption key to the drive. There are two LTO encryption management methods:

- Application-managed encryption (AME)
- Library-managed encryption (LME)

Application-Managed Encryption

The PowerVault tape libraries support application-managed encryption with a tape backup software application that supports LTO encryption. CommVault® Simpana® (v7.0 SP1 and higher) and Symantec™ Backup Exec™ (12 and higher) support LTO application-managed encryption.

In the case of application-managed encryption, the tape backup software determines what data will be encrypted and provides the key to the drive over the host bus. In addition to providing the keys to the drive, the tape backup software is responsible for generating, storing, and managing the keys.

Encryption is transparent to the library when using AME. AME can provide greater granularity in what data is encrypted as data can be encrypted on a job basis. If application-managed encryption is selected as part of the library encryption configuration, only the tape backup software will be allowed to provide keys to the drive. A library-managed encryption activation license key is not required for use of application-managed encryption on Dell tape libraries.

Library-Managed Encryption

In the case of library-managed encryption in PowerVault tape libraries, there is very limited policy for data encryption. All data written to LTO drives in a library-managed encryption enabled partition will be encrypted. The only exception is data written to media not initially encrypted from beginning of tape (BOT).

The library serves as the proxy to provide keys to the drive from the key store in the Dell Encryption Key Manager (EKM) application.

How do I Choose?

Security

Security concerns should be considered when selecting between AME and LME. When AME is used, the keys may be passed in the clear i.e. not encrypted between the media server and the drive over the host bus. Depending on the physical security of the datacenter, this may not be a concern for direct attach devices but the concern may be much greater in a Fibre Channel SAN environment where the connection medium is shared between multiple hosts. The T10 specification now provides a method of wrapping (encrypting) of encryption keys during transmission over the host bus. Please refer to your tape backup software documentation to determine if your application supports encryption key wrapping for transmission. Keys are never passed in the clear when using LME on PowerVault tape libraries.

Encryption Policy Granularity

AME can provide finer granularity in determining what data will be encrypted. Customers can select which backup jobs to encrypt or not encrypt using the same LTO drive. To achieve a similar level of granularity with LME, multiple library partitions would be required as well as more administration to direct backup jobs to the appropriate partition (encrypted or unencrypted).

Key Management

Key management or the process of providing keys to the drive for encryption should be considered when choosing between AME and LME. AME provides centralized key management within a single tape backup software application instance (e.g. Symantec™ Media Server and CommVault® CommServe™), but there may be limits on encryption key migration. LME provides centralized key management as the Dell Encryption Key Manager application can provide keys to multiple libraries and multiple library types e.g. TL2000/TL4000 and ML6000 simultaneously. This allows for greater interchange and migration of tapes between libraries – tapes can be interchanged between PowerVault libraries as long as the libraries can access the same EKM or key store. Maintaining the EKM application does require additional responsibility for the system administrator.

Table 1 summarizes the advantages and disadvantages of application-managed and library-managed encryption.

Table 1. AME and LME Comparison

Management Layer	Policy Granularity	Advantages	Disadvantages
Application-managed	May be more than one key per tape May be key per data chunk or backup job	Finer policy granularity Less new responsibility for storage admin	Key may be passed in the clear to drive Limited centralized key management Limited interchange/migration
Library-managed	One key per tape Encryption enabled at partition level	Key encrypted when passed to drive Centralized key management Application agnostic	Limited policy More responsibility for storage admin

Dell's Library-Managed Encryption Solution

For Dell's library-managed encryption best practices, please refer to the Read This First documentation on the EKM 3.0 installation media or at http://support.dell.com/manuals. Navigate to **Systems Management -> Encryption Key Management**.

The library-managed encryption configuration differs from a normal tape library backup configuration in that a Dell Encryption Key Manager (EKM) server is required to provide the encrypting keys to the drive via the library Ethernet management interface. In the Dell solution, the EKM server is separate from the tape library. Dell recommends installing EKM 3.0 on a dedicated physical server that is not used for any other services. This will ensure EKM 3.0's performance and response time is not affected by any other applications running on the same physical server. The library and EKM server can communicate over IPv4 and IPv6 networks.

Library-managed encryption on the library is configured at the partition level. An encryption-enabled partition must contain at least one LTO4 or LTO5 drive. Only encryption-capable drives can be used in an encryption enabled partition i.e. LTO3 drives are not supported in an encryption-enabled partition. All LTO4 and LTO5 media assigned to the encryption-enabled partition will be encrypted. The only exception is data written to media not initially encrypted from beginning of tape (BOT). Non-LTO4 and non-LTO5 media will not be encrypted even if assigned to an encryption-enabled partition.

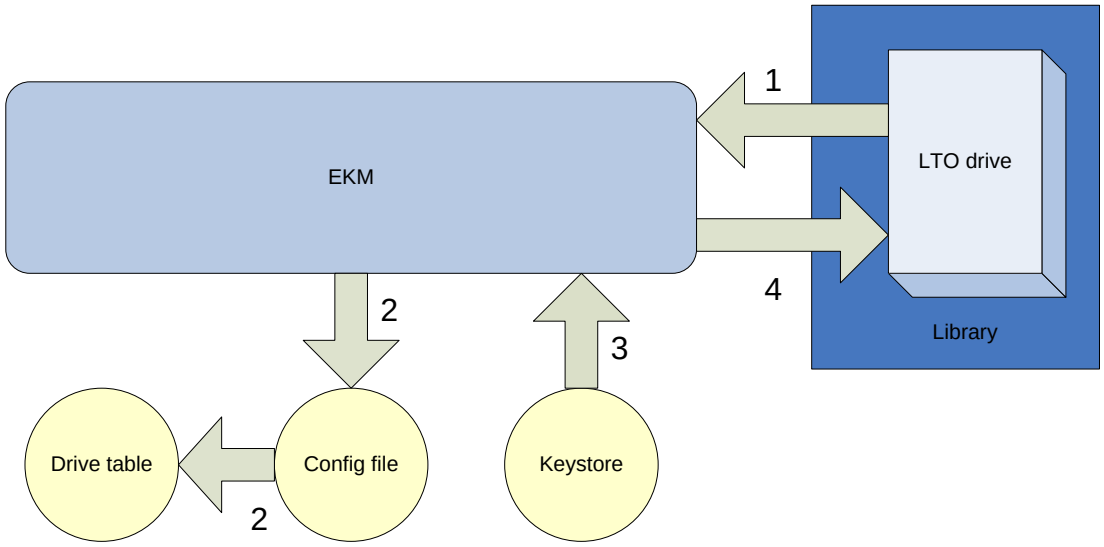
To prevent possible data loss due to an EKM 3.0 server failure, Dell recommends using a primary and secondary EKM 3.0 server setup. This configuration provides redundancy in the event that the primary EKM server is down or unavailable. Each encryption-enabled partition in the library can be configured for up to two EKM servers. The EKM server configuration must be identical in order to allow uninterrupted access to the data on the media. The Dell Encryption Key Manager 3.0 Deployment Guide covers the necessary steps to configure a primary and secondary server pair. The deployment guide can be found at http://support.dell.com/manuals. Navigate to **Systems Management -> Encryption Key Management**.

The EKM application consists of a drive table, configuration file, and a key store. The drive table maintains a list of drives that have been authenticated to the EKM. The configuration file is used to configure the EKM server settings such as auto discovery of drives. The key store is a DB2 database containing all of the keys that have been generated for that key store. The keys are obfuscated in the database and are never visible in the clear. The EKM GUI is used to make most configuration file changes and for EKM server maintenance. A command line interface can also be utilized for functions not offered in the GUI.

The process of EKM providing the encrypting key to the drive is outlined below and illustrated in Figure 2.

1. When the encrypted tape is mounted into the drive in an encryption-enabled partition, the drive will request a key from the EKM via the library. The library will pass the key request to the EKM server over the Ethernet management interface.
2. The EKM authenticates the requesting drive via a private key associated with the digital certificate on the drive. The drive and the EKM establish a public/private session key used to wrap the key for transit.
3. The key (DK) is fetched from the key store.
4. The encryption key is provided to the library wrapped in the session key for security. The library provides the wrapped key to the drive via the library control port on the drive. The encryption key is never passed in the clear between the EKM server and the library. The key is never stored on the media.
5. The drive unwraps the encryption key using the session key and uses the encryption key to encrypt or decrypt the data as needed.
6. The clear text data key identifier (DKi) provided by the EKM is written to the tape so the encryption key can be identified later for appends or restores. The relationship between the encryption key and the DKi is stored in an encrypted format in the EKM server.

Figure 2. EKM Data flow



The drive will retain the encryption key until the current media is unmounted or until power is removed from the drive. This is to ensure the security of the encryption key when it is outside of the encrypted key store.

Only one encryption key is used per tape when using library-managed encryption on PowerVault tape libraries. Depending on how many keys are in the EKM key store and how the EKM key store is configured, a key may be used for more than one tape.

Please refer to the 'Privacy Regulation Compliance with Dell ™ PowerVault ™ Tape Libraries' and the 'Dell Encryption Key Manager' white papers for library-managed encryption reference architectures for small to medium business customers and large enterprise customers.