May 22, 2007

Product Note: Encryption with LTO-4 tape drives

One of tape's chief advantages over other storage mediums is portability. Sending large amounts of data on tape to another location for disaster protection or simply as an economical transfer method is used by almost all large organizations. Recent events have highlighted the impact of losing control of the data on tapes that are lost through misadventure or outright theft. LTO 4 tape drives incorporate strong encryption to eliminate the risk that the data on missing tapes could be used in a malicious manner.

Is encryption an extra-cost option?
No. Encryption is a standard feature of all LTO-4 drives sold by Qualstar.

Does encryption require special media?
No. Any LTO 4 media can be used with encryption.

Does using drive encryption preclude using drive data compression?
No, the two functions are not related. Encrypted data will compress in the same manner as the unencrypted version.

How much does encryption impact data transfer rates?
Very little: ~1% slower reading or writing

Who/what controls encryption and decryption?
Your data protection backup and recovery software program controls the encryption/decryption process. This is called Application Managed Encryption, or AME.

Do all data protection applications include drive-based encryption support?
Not as yet. Some do already, some are about to release full support and some are planning to release basic support with a plan to enhance their support over the next few months. You should check with your software vendor for current availability and the schedule for the release that includes drive-based encryption support.

How does the data protection application control encryption/decryption?
When the application wants to write an encrypted tape, it sends a special command to the tape drive telling it to start encrypting. That command also includes a mathematical key to be used to encrypt the data. When the application wants to read that data back, it sends the decrypt command along with that same key to the drive to decrypt and read the data.

What is this "key"?
The key is a string of bits i.e. numbers, letters, and other characters, which is used in a complex mathematical formula to encrypt the data.

Do I need to make up a fancy key to make sure my data is safe?
No. The key is composed by the key manager software within the data protection application. The encryption engine within the drive will ensure that your data is safely encrypted. It is important to keep all of the keys confidential and secure, because losing a key is tantamount to losing the data.

If I do not have the key, can I—or anyone else—decrypt the data?
No. Without the key the data is unrecoverable by any means.

Can I have encrypted and non-encrypted data on the same tape cartridge?
Yes. In fact, you can have multiple files encrypted with different keys on the same tape cartridge.

Could multiple cartridges be written with the same key?
Yes. The drive can handle as many or as few keys as are needed to fit your security and encryption needs.

What is the overhead cost for encrypting data, both in speed and in tape capacity loss?
IBM's studies show an overhead of less than 1% in transfer loss and capacity loss. If the user wants many key changes, overhead will go up, though, both for the drive and for the application software to manage all of the keys.

Why not just have the library encrypt all of my tapes?
library based encryption does work, but the main disadvantage is in transporting tapes to other libraries at other locations, such as a Disaster Recovery (DR) site. Then there needs to be a mechanism to securely transmit and load the appropriate keys at the DR site.

With AME, what happens when I need to read that tape cartridge somewhere else— say, another library at another location?
The key must to be sent to that other library. The key needs to be kept secure, so must not accompany the tape cartridge unless it is also encrypted with a key that is known at the other site. The safest way to do this is to keep the keys updated via a separate means, such as a secure VPN, and send them encrypted to the other site where the other site knows the key to decrypt them. Rule number one in sending secure data is to separate the key(s) from the encrypted data.

Is it more efficient to use a separate encryption appliance than trying to cram all of this functionality into the drive? Isn't a separate encryption appliance more efficient than doing the encryption/decryption on the drive?
No. There is a dedicated hardware-based encryption engine in the drive which works closely with the compression engine, data buffering algorithms, error correction/detection code engine, and other drive functions. Thus, by controlling all of the processes of receiving data from the external interface through writing to tape, the drive optimizes the writing and reading processes. An external encryption appliance could never be as efficient as the hardware within the drive, both for reading and writing, since the drive has to then do much of that work again to generate the patterns for the data reading from or writing to the tape.

I just use TAR to write my tapes. How can I tell the drive to encrypt that tape for the write, then decrypt for the read?
This is not yet available. A version of the IBM LTO tape driver that supports encryption is being developed by IBM.

I am a software developer who writes applications for reading and writing tapes. How do I find out specifically what the commands are for encrypt and decrypt?
The LTO encryption specification is available from the T10 committee.