The KEY to Protecting Your Data

By Dave Parry

Business today is creating data at unprecedented rates. Managing and protecting that data continues to challenge every organization. There are many technologies and methods for data centers to ensure the availability and integrity of information assets from snapshots and mirroring up to full disaster recovery solutions. Most of this is focused on protecting the systems and storage platforms. What happens when data needs to be transported outside of this protected environment?

On-line business data exchange is often protected via certificate based encryption or proprietary schemes to insure that data over the wire cannot be compromised. Wireless transmission adds an additional dimension to this.

What About Tape?

Tape continues to be the most economical and portable method to store off-line data. That portability is both a benefit and an area of risk. Encrypting the data on the tape would seem to be a simple solution. And it can be, but it is important to understand all aspects of this technology to insure you can access your data when you need to.

Data encryption involves modifying the data stream into seemingly random characters based on a unique character string or **key**. A similar key is required to read-back the data from the tape.

It is important to remember that if you lose the keys you lose the data. Forever.

This raises a number of challenges;

- how to generate, manage and protect the keys
- where in the data stream to perform the encryption
- how to transfer the keys to the tape drive
- how to read the tape in other environments

There are in-band encryption "appliances" from various manufacturers that encrypt the data stream before it gets to the device (disk or tape). A similar appliance (and key) is required at the remote site to be able to read the data. Encrypted data cannot be compressed. Therefore this process defeats the hardware compression on the drives, requiring more media. As your environment scales so too will the number of appliances required, adding yet one more layer of technology to manage.

There are software solutions such as Tivoli Storage Manager (TSM) that will encrypt the data on the server prior to writing out to tape. Bear in mind that the use of TSM, which is a very function-rich product, consumes some system resources and will have an impact on the efficiency of the backup process. The encryption key is stored in the TSM database and would need to be exported to a remote TSM server to be read, which means TSM must be in place on the remote server as well. This process also bypasses hardware compression on the tape devices.

Tivoli software

IBM has integrated hardware encryption into their **LTO-4** and **TS1120** tape drives using standard tape media. Since the encryption is done at the hardware level there is no performance overhead, and the data is compressed **prior** to encrypting on the drive, maintaining the write density.

There are a number of methods to move the keys to the drive, where it is stored in memory for each tape operation.

TSM (5.4) has been enhanced to directly manage encryption keys, generating and storing them in its database for each cartridge, tied to the unique tape label. TSM will pass the key string to the drive via the SAS or Fibre interface through standard SCSI commands.

For environments where TSM is not utilized, IBM provides a host-based key manager (EKM).

EKM is a java-based application that is small enough to be backed up to CD, and can be mirrored onto a number of servers in the enterprise—providing a primary and backup keystore for availability and protection.

With System-Managed encryption (AIX 5.x) EKM can transfer keys to the drive via the Atape system driver for directly connected tape drives

(SAS or Fibre). Encryption is configured at the tape drive level in this environment.

Dave Parry

Library-Managed encryption (AIX or i5/OS) transfers the keys from EKM via a LAN connection to the tape library. Encryption can be configured for individual cartridges in this environment, and is managed by policies configured in the library.

External data exchange requires similar tape technology at the remote location. The keystore will also need to be transferred securely (SSL/VPN) or via media (CD or tape) separate from the encrypted cartridges.

With current regulations such as PCI, HIPAA, SOX, Bill 189 and the like there is no question of the need to protect sensitive customer data. Just be clear about what you are trying to accomplish and why. If encryption is not absolutely necessary it may not be prudent to add this level of complexity to your environment. However, if this is a business requirement Mid-Range can help you determine the most efficient way to protect your information while insuring you can access it today and far into the future. M-R

Dave Parry *is a pre-sales technical specialist at Mid-Range, focusing on IBM System p and Storage solutions. His 22 years of IT experience includes field service, AIX and HPUX technical support, networking, high-availability, and solutions assurance. Dave has been directly supporting IBM opportunities for the past 10 years. He can be reached at dparry@midrange.ca.*

News and Rumours

► **AIX 6.1** is currently in beta and is planned to officially announce in Nov. Look for AIX v5.2 to be withdrawn in Q4 as IBM's policy is to support two O/S versions, the current release (AIX6.1) and one previous version (AIX 5.3).

► **Power 6 BladeServer** will be announced in November. Available initially as a 2-socket blade, supporting 4x P6 cores. Virtualization functionality will be supported via IVM. A follow-on single core P6 blade will be announced later in the quarter.

► **p6-P570.** This system currently has a single-bus 6-slot SAS backplane for internal disk in each 4-way node. IBM will announce in Nov an option to split this bus providing 2 controllers for bus-level mirroring or dual LPAR boot support. This option will also be available as an MES to installed P6-p570 servers.

► **AMD's new quad-core Opteron** is getting a lot of attention for outstanding performance results. IBM is planning a new BladeServer based on this new processor. Stay tuned.

► **New 8-core P6 server.** This will be the P6 follow-on to the current P5-550 server. Expected to announce in Q1.

► **SATA disk drives** from IBM include a 750GB drive offering. That will increase to 1TB drive modules early next year.

► **TS1120 Enterprise Tape** currently supports up to 700GB of uncompressed capacity. IBM is expected to announce a 1TB tape offering for this product early 2008. The advantage of the TS1120 architecture is the ability to reformat existing media to support the higher densities as the technology evolves.

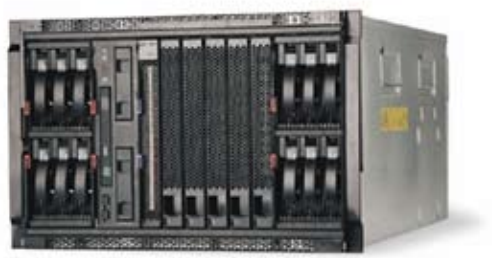
► **DS4000 RAID 6 support.** This will be a firmware update to existing DS4700 and DS4800's. Expected availability Feb/08.

► **DS3000 Mixed SATA and SAS** support drive support, as well as System P certification. (as well as System X and Blade). Expected availability Dec/07.

Recent Announcements:

IBM BladeCenter S Chassis

New SMB-focused chassis with Six BladeServer slots and 4x 3-drive hot-swap SAS or SATA disk bays. This lowers the entry point for IBM's BladeCenter and combined with the new P6 BladeServer provides attractive consolidation options for the SMB market. All current BladeServer and switch modules are supported in the new chassis. www-03.ibm.com/systems/bladecenter/tour/index.html.



IBM DS3300 — ISCSI Storage Susbsystem

New addition to the DS3000 SAS entry storage subsystem providing host connectivity options for SAS (DS3200), Fibre (DS3400), and now ISCSI. Scales up to 14TB. www-03.ibm.com/systems/storage/disk/ds3000/ds3300/.