STORServer

WHITE PAPER ›

DATA ENCRYPTION – STORSERVER/TSM

WHITE PAPER

Prepared by:
Jarrett F. Potts, Director of Marketing, STORServer, Inc.

storserver.com
(800) 550-5121

How Encryption Works with STORServer and IBM® Tivoli® Storage Manager

IBM encryption technology is a feature that is available within IBM's Tivoli Storage Manager (TSM) software (the driving force within all STORServer Appliances). IBM encryption technology ensures that data is secure by requiring a 256-bit Advanced Encryption Standard (AES). To encrypt and decrypt data, encryption keys pass to the media source by a key manager. There are several approaches to data encryption through TSM including Application, Library, System and Drive methods.

Application Encryption

When securing applications, encryption keys are managed by each application. Tivoli Storage Manager generates and stores the keys in the application server's database. Data is encrypted during "WRITE" operations, when the encryption key is passed from the server to the media source. Data is decrypted to allow only "READ" operations.

When using application encryption, you must take extra care to secure database backups. Encryption keys that are used to encrypt and decrypt data are stored in the server's database. In order to restore data, the correct database backup and corresponding encryption key are required. Databases should be backed up frequently and the backup media should be carefully safeguarded.

Note: Use application-managed encryption for storage pool volumes only. Other volumes such as backup-set tapes, export volumes, and database backups are not encrypted using the application method.

Library encryption

When securing data using the "Library" encryption method, encryption keys are managed through the library. Keys are stored in an encryption key manager and provided to the media drive. To execute library encryption, set the "DRIVEENCRYPTION" parameter in the device class definition to "ALLOW."

Note: Not all IBM libraries support IBM LTO-4 library encryption.

System Encryption

System encryption is available on AIX platforms only. When securing systems, encryption keys are managed by the device driver or operating system and are stored in an encryption key manager. To execute system encryption, set the "DRIVEENCRYPTION" parameter in the device class definition to "ALLOW."

Drive Encryption

Drive encryption is set through the hardware configuration. TSM cannot control or change which encryption method is used in the hardware configuration. If the hardware is set up for the application encryption method, TSM can turn encryption on or off depending on the "DRIVEENCRYPTION" value on the device class.

Choosing an Encryption Method

Choosing which encryption method depends on the backup strategy. If storage pool volumes are the target for encryption, the Application method should be enabled.

If all data should be encrypted, not just storage pool volumes, the System or Library method can be used.

Library managed encryption allows control over which volumes are encrypted through the use of the volume's serial number. At this level, you can specify a range or set of volumes to encrypt. You can also use storage pool hierarchies and policies to manage the way that data is encrypted.

Both Library and System methods of encryption can share the same encryption key manager, which allows the two modes to be interchanged. This can only occur, however, if the encryption key manager is set up to share keys.

To determine whether or not a volume is encrypted and which method was used, execute the "QUERY VOLUME" command with "FORMAT=DETAILED."

For more information on data encryption using the backup-archive client, see the Backup-Archive Clients Installation and User's Guide by browsing to: http://publib.boulder.ibm.com/tividd/td/TSMC/GC32-0789-04/en_US/HTML/ans5000002.htm

Changing Your Encryption Method and Hardware Configuration

To change the encryption method for a given set of volumes, each volume needs to be returned to "scratch" status. Updating the parameter value will only affect empty volumes. For example, if "Application" managed encryption is enabled and is subsequently changed to "disabled," only empty volumes will be impacted by the change. Filling volumes will continue to be encrypted while new volumes will not.

To turn off encryption on currently encrypted "filling" volumes, the volume status should be changed to "READONLY." This will ensure that TSM does not append any more encrypted data to the volumes. Use the "MOVE DATA" command to transfer data to a new volume following the update of the "DRIVEENCRYPTION" parameter. The data will then be available in an unencrypted format.

When migrating from one hardware configuration to another, data should be moved from the old volumes to new volumes, generating new encryption keys and key managers. To do this, set up two logical libraries and storage pools (each with a different encryption method). Next, migrate data from the old volumes to the new volumes. This approach will eliminate volumes that were encrypted using the original method.

Note: It is not possible to migrate from the "Library" method to "Application" method as TSM does not have access to library encryption keys.

For more information on data encryption using IBM Tivoli Storage Manager, contact your Authorized STORServer Reseller or call 1-800-550-5121 to speak to a STORServer representative.

ABOUT STORSERVER

STORServer is a leading provider of data protection solutions and offers the only enterprise data backup appliance that is built to order. Each backup appliance solution is tailored to the customer's unique environment to simplify management of complex backup, archive and disaster recovery needs. STORServer's appliances feature enterprise class data backup, archive and disaster recovery software, hardware, services and U.S.-based customer support. Companies of all sizes trust in STORServer's proven appliances to solve their most complex data protection problems. For more information on STORServer, please visit storserver.com.

storserver.com
(800) 550-5121

STORServer