November 2019

IBM® Virtualization Engine TS7700 Series Encryption Overview Version 2.0

By: Wayne Carlson
Duke Lee
Jeffrey Pilch
IBM Senior Engineer
Tucson, Arizona

Introduction

The IBM Virtualization Engine TS7700 Series is the latest in the line of tape virtualization products that has revolutionized the way mainframe customers utilize their tape resources. Security of the information stored on the backstore tape cartridges has become important to many customers. The IBM System Storage TS1120 Tape Drive Model E05 was enhanced to support data encryption in September 2006. All subsequent IBM System Storage TS11xx tape drive models support data encryption. This white paper describes the use of data encryption on these tape drives when attached to the TS7700 Virtualization Engine (VE).

Summary of Changes

Version 1.1 – April 2007 This is the initial version of this document.

Version 2.0 – November 2019 Updated with the support for TLS 1.2

Overview

The importance of data protection has become increasingly apparent with news reports of security breaches, loss and theft of personal and financial information, and government regulation. Encryption of backstore tapes helps control the risks of unauthorized data access without excessive security management burden or subsystem performance issues.

The encryption solution for tape virtualization consists of several components.

IBM's tape encryption solutions all use an Encryption Key Manager (EKM) as a central point from which all encryption key information is managed and served to the various subsystems. The EKM communicates with the TS7700 Virtualization Engine as well as tape libraries, control units, and open-systems device drivers.

The TS11xx model encryption-enabled tape drive, as the other common component to the various data encryption solutions, provides hardware that performs the cryptography function without reducing the data-transfer rate.

The TS7700 Virtualization Engine provides the means to manage the use of encryption and what keys are used on a storage-pool basis. It also acts as a proxy between the tape drives and the EKMs, using ethernet to communicate with the EKMs and Fibre Channel connections with the drives. Encryption support is enabled with Feature Code 9900.

Code Requirements

This function was introduced with the TS7700 Virtualization Engine microcode version 8.2.0.19 in March 2007. Although there are no library manager code changes to support the function, there are other functions of the TS7700 Virtualization Engine that require a compatible level of library manager code. There are no host software updates required for this function.

Encryption Keys

Data Keys

Tapes encrypted in the TS7700 backstore use a "wrapped key" model. Each cartridge is encrypted with a random (so, likely to be unique) 256-bit Advanced Encryption Stardard (AES-256) Data Key (DK). The Data Key is stored on the cartridge in an encrypted, or "wrapped", form. Two of these wrapped keys are stored on each cartridge.

Key Encryption Keys

The keys used to encrypt the data key are called Key Encryption Keys or KEKs. KEKs are stored in one of several types of keystore supported by the EKM[1]. KEKs are Rivest-Shamir-Adleman (RSA) key pairs, typically generated and kept in the keystore as a certificate. The public half of the key pair is used to encrypt the DK and store it into an Externally Encrypted Data

[1] EKM supports the following IBM keystores: JCEKS, JCE4758KS/JCECAAKS, JCE4785RACFKS/JCECCARACFKS, JCERACFKS, PKCS11IMPLKS, and IBMi5OSKeyStore.

Key (EEDK) which is stored in the cartridge memory as well as several places on the tape media. The private half of the key pair is needed to decrypt (or "unwrap") the DK from the EEDK.

A KEK may be created that contains only the public half of the key pair. This is useful for setting up main processing and disaster recovery sites without requiring sharing of private keys between sites. Each site need have the private half of only one KEK used for each tape in order to read data from encrypted tapes, yet can create EEDKs that can be used by both sites.

Key Labels

KEKs may be tagged with user-friendly labels. These 64-character fields are relatively free-form and are not case-sensitive. For example, a KEK certificate may be labeled "Finance Dept GL Key 1". When configuring TS7740 storage pools to use this KEK, the label would be entered on the web panel. From the TS7700 web panel, there is also an option to enable the storage pool to use default keys if the Encryption Key Server have been configured to use default keys.

Key Modes

Note, however, that the same certificate may be in one keystore with one label, and be imported into another keystore with a different label. Such a situation may occur between main processing and disaster-recovery sites. The main site may have keys labeled "June 2007 Key" and "June 2007 DR Site Key" while the disaster-recovery site calls these same keys "June 2007 Main Site Key" and "June 2007 Key" respectively. Cartridges that are written using the "Clear Label" mode for the EEDKs will not decrypt at the disaster-recovery site since the labels are not consistent.

To avoid problems with key label inconsistency, you may want to select the "Hash Label" mode when setting up the encryption settings for storage pools. Since the hashes are generated from the KEK certificate itself, they will be consistent between locations. The trade-off is that since labels will no longer be stored as part of the EEDK, there isn't a good way to determine what key is required to decrypt a cartridge if it has been removed from the keystore..

Encryption Key Manger

The Encryption Key Manager (EKM) communicates with the VE over an ethernet TCP/IP interface. It is set up to access one of the supported keystores.

When the EKM receives a key request from the VE, it uses commands, requests, and responses defined in its proprietary protocol to verify authorization of the drive that needs a DK, get EEDK information from the cartridge, and send an encrypted copy of the DK to the VE. At no point is the Data Key sent in an unencrypted form.

Generation of new DKs, decryption of EEDKs, and encryption of EEDKs and other encrypted DK forms is performed by a crypto services function in conjunction with the attached keystore.

Administrative access to the EKM and keystore must be well-secured as part of a secure encryption implementation.

If you plan on using Transport Layer Security (TLS)for secure network communications, the Encryption Key Server must be running the IBM Security Key Lifecycle Manager that supports TLS 1.2.

Virtualization Engine

Encryption operations in the TS7700 VE environment are performed on the backstore physical tape cartridges. This protects the data at rest. Loss or theft of the cartridges does not expose the contained data since reading the tapes requires deciphering of the Data Key in the cartridge's EEDKs. Such deciphering requires use of KEKs which are contained and accessed by the secured EKMs and keystores.

Prerequisites

While the feature for encryption support is customer-installable, some of the prerequisites may require additional hardware installation or configuration by an IBM Service representative.

Tape Drives

Since data encryption is performed on the tape drives themselves, TS11xx Model encryption-capable tape drives must be attached to the TS7700 VE. For TS1120 Model E05 tape drives, they also must be running in native (E05) mode rather than J1A emulation mode.

If you have 3592 Model J1A drives attached to the VE, they should be detached. The VE does not allow a mixture of drive types to be used. The J1A drives may be redeployed in other subsystems or used as direct-attached drives for open-systems hosts. If you have a mixture of J1A and E05 drives attached to your VE and cannot detach the J1A drives right away, you may proceed as long as you have a minimum of 4 encryption-capable E05 drives attached. Be aware, though, that the J1A drives will not be used by the VE once the E05 drives are put into native mode.

All TS1120 Tape Drives with Feature Code 5592 or 9592 are encryption-capable.

TS7700 Virtualization Engine

The Virtualization Engine (VE) must be running microcode level 8.2.0.19 or higher. Feature code 9900 must be installed to access the encryption settings.

The VE must not be configured to force the TS1120 drives into "J1A" mode. This setting may only be changed by your service representative. If you need to update the microcode level, be sure the service representative checks and changes this setting if needed.

Encryption Key Manager

Your EKMs should be installed, configured, and operational before installing the encryption feature on the TS7700 VE. You should also create the KEK certificates you plan to use for encrypting your backstore tape cartridges.

Although you may run with a single EKM, it is strongly suggested that you have two EKMs for use by the VE. Each EKM should have all the required KEKs in their respective keystores (or share a single highly-available keystore). The EKMs should have independent power and network connections to maximize the chances that at least one of them is reachable from the VE when needed. If the VE is unable to contact either EKM when required, you may temporarily lose access to migrated logical volumes and will not be able to move logical volumes in encryption-enabled storage pools out of cache.

See the **IBM Encryption Key Manager component for the Java platform Introduction, Planning, and User's Guide** (GA76-0418) for details on installing and configuring your EKMs.

Since the VE maintains TCP/IP connections with the EKMs at all times, it is recommended that the EKM configuration file have the following setting to prevent the EKM from timing out on these always-on connections:

TransportListener.tcp.timeout = 0

Installation

Feature code 9900 provides explicit instructions on setting up the drives and activating the feature on the VE. These illustrated instructions are not repeated in this paper. Briefly, the installation steps are:

- Determine which TS11xx drives are attached to the TS7700 VE.
- Verify the tape drives are encryption-capable.
- Configure the drives to be encryption-enabled by specifying the "System Managed" Encryption Method.
- Install the Feature Code 9900 License Key.
- Set up the EKM IP address and port information (See below).
- Verify connection to the EKMs.

It is essential that you configure the tape drives for System Managed encryption. The TS7700 uses the drives in this mode only and does not support Library Managed or Application Managed encryption.

Once the TS7700 is using drives for encrypted physical tape volumes, it will put drives that are not properly enabled for encryption offline to the subsystem. TS3500 library operators should be made aware to leave TS7700-attached drives in System Managed encryption mode at all times so drives are not taken offline.

TS7700 VE Configuration

Encryption Key Manager Addresses

This is the EKM address configuration panel through which the feature installation instructions guide you.

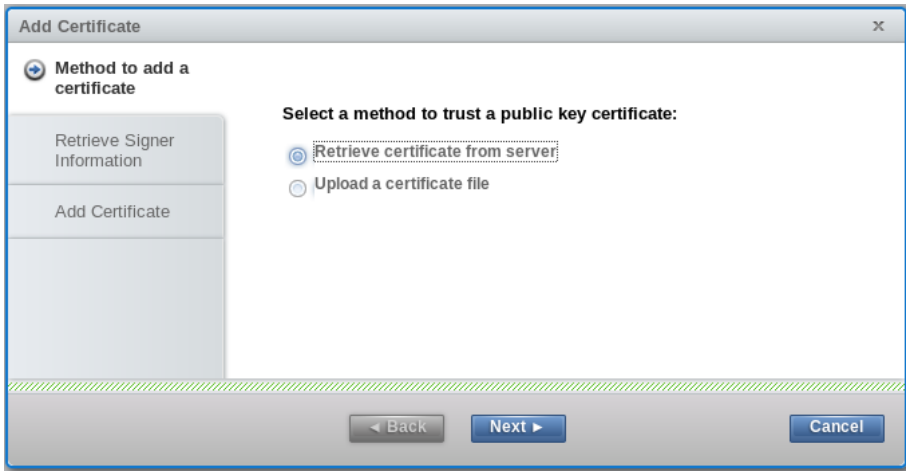
The secondary key manager address is optional on the panel. It's recommended that you always set up and configure for two EKMs. To maintain continuous access to your data it is critical to take advantage of all possible redundancies in the subsystem.

Your network and/or EKM administrator should be able to provide you with the two EKM IP addresses.

The standard (and default) EKM port for non-TLS communication is 3801, but your EKM administrator may have selected a different port number for the EKM configuration file due to conflicts on the system on which the EKM runs.

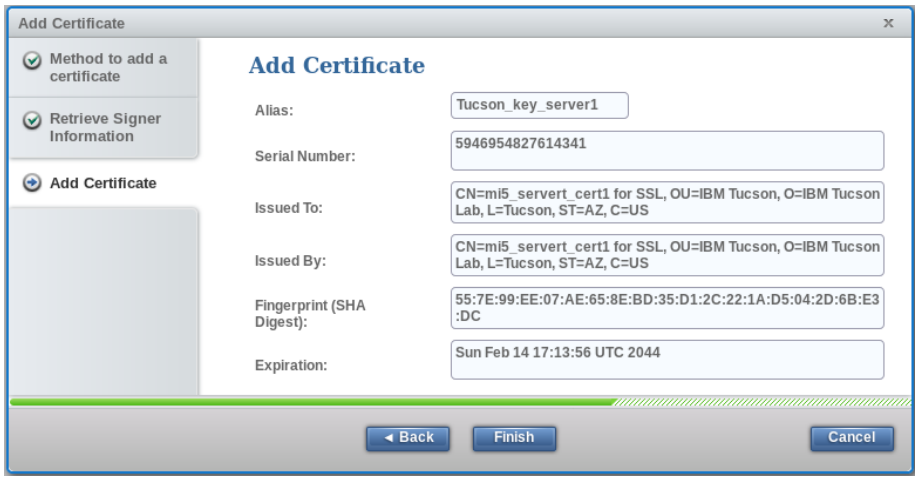
Starting with the TS7700 5.0 Code Release, the support for TLS Version 1.2 was added. The use of TLS ensures the entire conversation is encrypted between the TS7700 and the Encryption Key Server. When using TLS 1.2, be sure to import the public digital certificate of each Encryption Key Server that has a self-signed certificated installed. The default TS7700 certificate used for secure communications is the "Iwiks" certificate. Normally, the default TLS port 441 is used by the Encryption Key Server for TLS network communication.

When configuring the TS7700 to use TLS 1.2 to communicate with a key server, use the TS7700 SSL Certificates function on the Management Interface to add a new certificate. After clicking on the "+ New Certificate" tab, select "Retrieve certificate from server" from the popup screen.



Click "Next" to enter the key server IP and TLS port number that is configured at the key server. The TLS port number is normally 441.

Click "Next" and provide an alias for storing the key server's certificate. Click "Finish" to complete the process. Remember to repeat these steps to import the second key server's certificate.



Encryption by Storage Pool

Encryption on the TS7700 VE is controlled on a storage pool basis. "Storage Group" and "Management Class" DFSMS constructs specified for logical tape volumes determine, through mapping in the Enterprise Library Controller (ELC), which

storage pools are used for the primary and backup (if used) copies of the logical volumes. The storage pools, originally created for management of physical media, have been enhanced to include encryption characteristics.

z/OS DFSMS

For information on setting DFSMS policy constructs, see publication SC35-0427-04, ***DFSMS Object Access Method Planning, Installation, and Storage Administration Guide for Tape Libraries***.

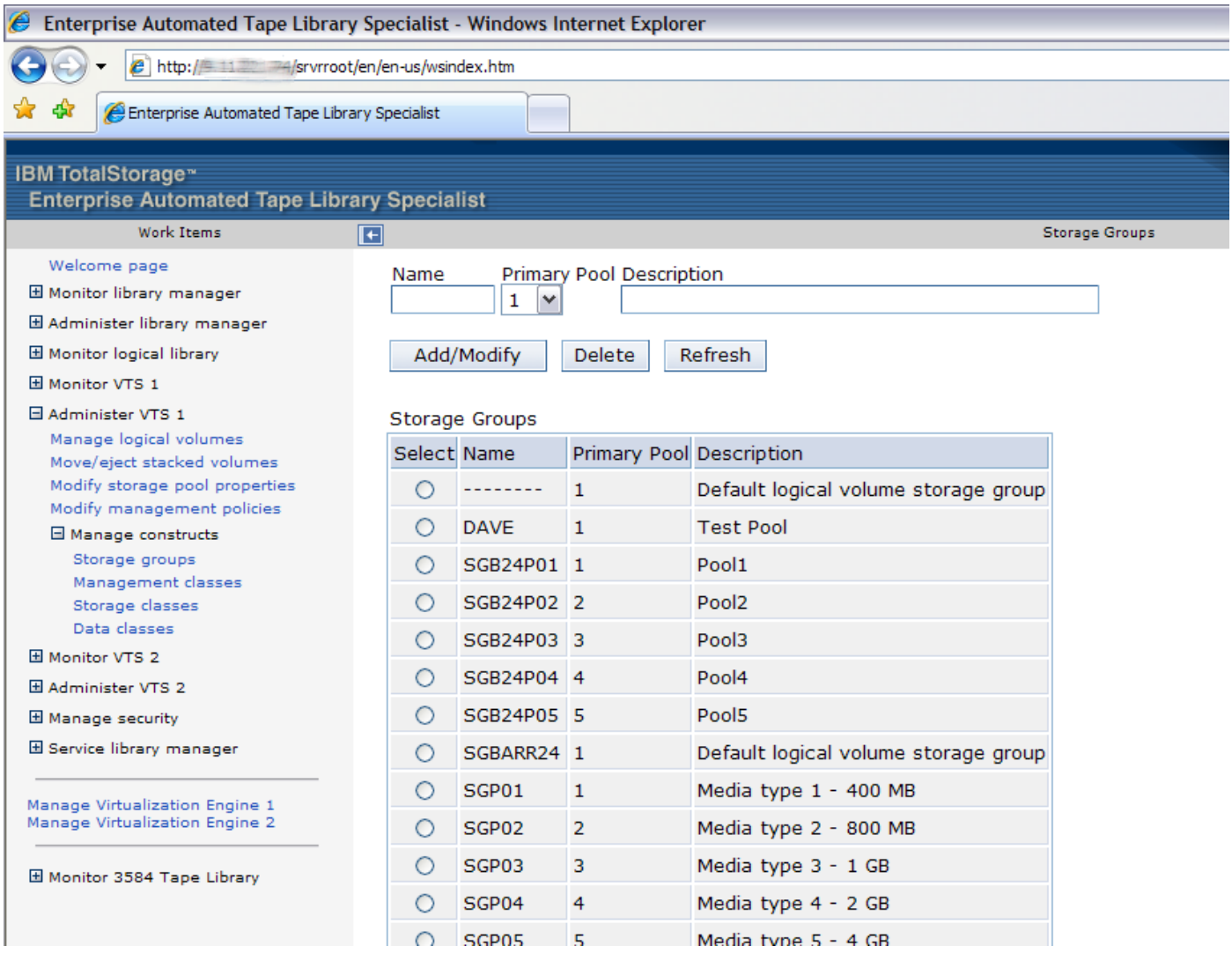
Non-DFSMS

If you are not running z/OS or are running z/OS without DFSMS, logical volumes will be assigned default constructs. The primary copy of the logical volumes on physical tape are assigned to storage pool 1 and backup copies are not assigned to a storage pool (no copy) by default. You may change the default storage pool assignments on ELC panels.

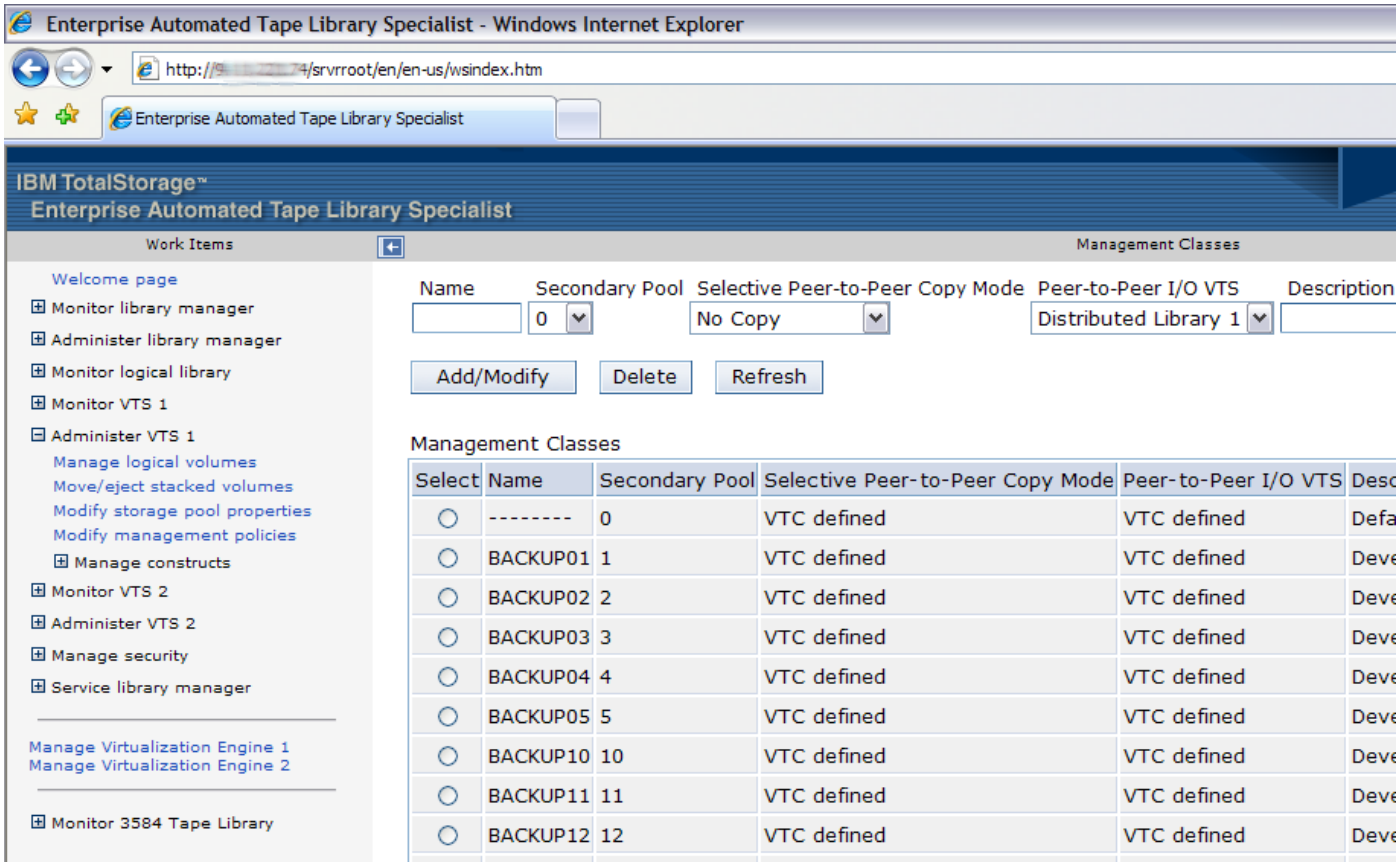
Enterprise Library Controller

The Tape Library Specialist (web interface) menu selections for managing the constructs are under the "Administer VTS n" (n is 1 or 2 depending on the VE subsystem to be managed), then "Manage constructs" selections.

An example "Storage groups" screen is shown below. It associates Storage Group names with storage pools (called "Primary Pool" on this screen). Multiple storage groups may be associated with any given storage pool.

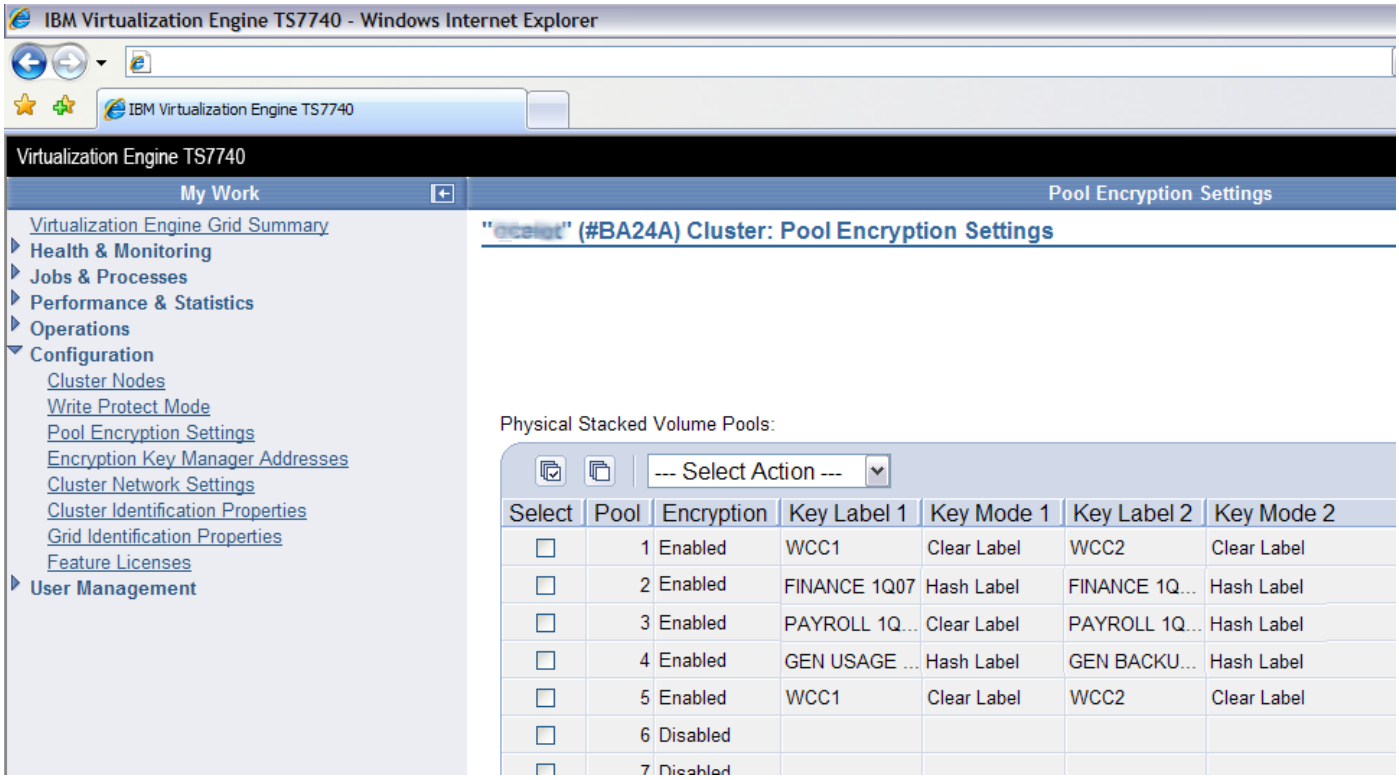


An example "Management classes" screen is shown below. It associates Management Class construct names with storage pools (called "Secondary Pool" on this screen). Multiple management classes may be associated with any given storage pool.



Pool Encryption Settings

The Maintenance Interface (MI) web interface for the TS7700 VE "Pool Encryption Settings" panel (in the "Configuration" group) allows you to specify the key labels and modes to use for each storage pool. An example screen is shown below.



Be sure to define all key labels are known by the keystores associated with your EKMs ***before*** they will be used by the system. The safest way to ensure this is to set up the certificates in the keystores before entering the key labels on this screen.

The key modes are also entered here. See Key Modes on page 3 for more information.

The pool settings for each TS7700 VE node are independent of the settings for other nodes. Encryption enablement, key labels, and key modes may all vary between nodes. If you want your nodes to use the same settings, you must configure each with the settings.

Note that EKM address setup is also independent on a per-node basis. You may want to use local EKMs for geographically separated nodes. The EKMs must recognize the key labels for VEs that are configured to use them. If you are sharing keys (KEKs) across different EKMs, be sure to import the necessary certificates into their corresponding keystores. Do not create separate certificates with the same key labels.

Operations

Writing Physical Tapes

When a physical volume is mounted to be written from the beginning of tape (BOT), the VE checks the encryption settings for the storage pool to which the physical volume is assigned. If encryption is enabled for the storage pool, the VE configures the drive to use encryption and sets the encryption key labels and modes to be used for the cartridge. The drive and EKM interact through the VE to get the drive set up properly for the encrypted write operations.

This is the sequence of events for a write from BOT:

1) Mount the physical volume selected from the storage pool associated with logical volumes to be written to tape
2) If the storage pool has encryption enabled
    a) The VE sets the drive into encryption mode, sends the key labels configured for the storage pool to the drive, and start writing logical volume data.
    b) The write operations require that a Data Key (DK) be loaded into the drive encryption hardware, so a request for a DK is set to the EKM.
    c) A series of commands, requests, and responses are exchanged with the EKM through the TCP/IP interface.
    d) During this exchange, an encrypted version of the DK is sent to the drive. The drive decrypts the DK and set the AES-256 Data Key into the encryption hardware.
    e) The VE continues writing logical volume data at full data-transfer speed
3) If the pool has encryption disabled
    a) The VE turns off encryption mode at the drive
    b) The VE writes logical volume data to the drive. This completes just as it does with a non-encryption-enabled VE.
4) The physical volume is demounted, freeing the drive for other VE operations

When a physical volume is mounted so logical volume data can be appended to it (ie, it is not being written from BOT), the current encryption characteristics of the volume are used.

This is the sequence of events when appending a physical volume:

1) Mount the physical volume selected from the storage pool associated with logical volumes to be written to tape
2) If the cartridge is encrypted
    a) The drive is in encryption mode because the cartridge is recognized as having been written in encryption format.
    b) The tape is positioned to the append point.
    c) The write operations require that a Data Key (DK) be loaded into the drive encryption hardware, so a request for a DK is set to the EKM.
    d) A series of commands, requests, and responses are exchanged with the EKM through the TCP/IP interface.
    e) During this exchange, the EKM extracts the DK from one of the EEDKs contained in the cartridge. An encrypted version of this DK is sent to the drive. The drive decrypts the DK and set the AES-256 Data Key into the encryption hardware.
    f) The VE writes logical volume data at full data-transfer speed
3) If the cartridge is not encrypted
    a) The drive remains in non-encryption mode
    b) The VE positions tape and writes logical volume data to the drive. This completes just as it does with a non-encryption-enabled VE.
4) The physical volume is demounted, freeing the drive for other VE operations

Reading Physical Tapes

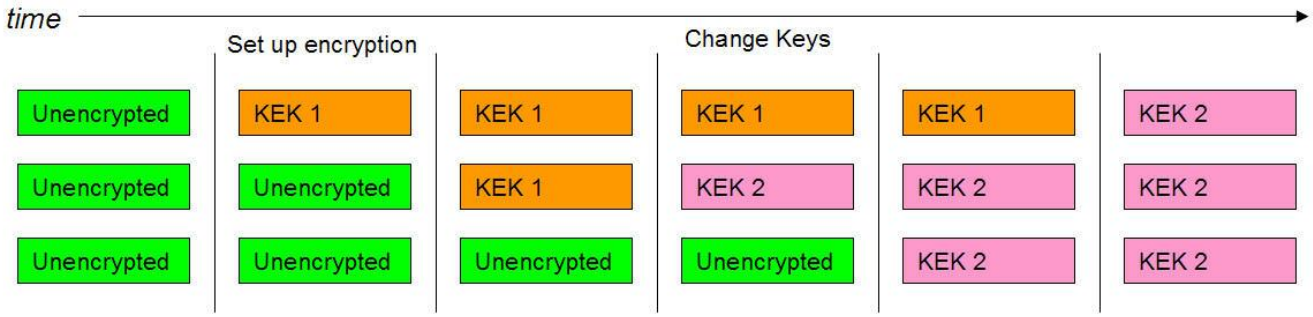
Encrypted tapes are written in a unique format, so the drive detects if tapes are encrypted or not. The tape cartridges contain encrypted data key information which the EKM can decipher. Once the key exchange has completed, the drive is set up to decrypt the data on tape and processing continues.

1) Mount the physical volume containing the required logical volume data
2) If the physical volume is encrypted
    a) The drive is in encryption mode because the cartridge is recognized as having been written in encryption format.
    b) The read operations require that a Data Key (DK) be loaded into the drive encryption hardware, so a request for a DK is set to the EKM.
    c) A series of commands, requests, and responses are exchanged with the EKM through the TCP/IP interface.
    d) During this exchange, the EKM extracts the DK from one of the EEDKs contained in the cartridge. An encrypted version of this DK is sent to the drive. The drive decrypts the DK and set the AES-256 Data Key into the encryption hardware.
    e) The VE reads logical volume data at full data-transfer speed
3) If physical volume is not encrypted
    a) The VE reads logical volume data from the drive just as it does with a non-encryption-enabled VE.
4) The physical volume is demounted, freeing the drive for other VE operations

Changing Storage Pool Encryption Settings

Storage pool encryption settings may be changed at any time. Keep in mind that these settings are applied only when the physical volume is written from beginning of tape. As a result, there may be a mix of encryption usage and/or key use on physical volumes in a given storage pool until volumes are reclaimed and reused.

The figure below illustrates a simple example of physical volumes in a storage pool over time. In the beginning, encryption is not enabled for the storage pool, so all physical volumes are unencrypted. Encryption is then enabled for the pool using key label "KEK 1". As unencrypted physical volumes are rewritten from the beginning of tape, they will be encrypted using that key label.



When the pool is reconfigured to use key label "KEK 2" instead of "KEK 1", there will still be physical tapes that are encrypted with the old key label. The certificate must be maintained in the EKMs long enough for all the volumes to be rewritten with the new "KEK 2" key label.

The transition from unencrypted tapes to encrypted, as well as that from one set of KEKs to another occur naturally at the pace the tapes are reused by the VE. In the meantime, the physical volumes in the storage pool may be a mix of unencrypted tapes and encrypted tapes with different KEKs.

Progress of the migration of data from unencrypted media to encrypted can be monitored by using a new storage pool for encryption rather than modifying the current pool. The Tape Library Specialist "Search Database" function can then be used to see remaining volumes in the old unencrypting storage pool.

Moving Data to Encrypted Storage Pools

There are several means of expediting movement of data onto encrypted tapes. All of these methods begin with the same configuration changes:

1) Change the storage pool associated with a storage group construct to a new (empty) pool with encryption enabled.
2) Change the properties of the old storage pool to specify the new encryption-enabled storage pool as its reclaim pool.
3) Change the properties of the old storage pool to specify that borrowed volumes be returned to the scratch pool.

Once this change is made, all new data associated with the storage group will migrate to encrypted media, old data recalled to cache will migrate to encrypted media, and other old data will migrate to encrypted media as tapes are reclaimed. The migration may be accelerated by using one or more of the methods below.

If the dual copy function is used, the secondary pools should be changed in a similar manner.

Note: If a migration to new media is planned for the same timeframe as encryption implementation, the new storage pool can be set up for the new media type and encryption attributes and the migrations combined to one.

Recall Data Method

Once the changes have been made, old data is automatically migrated as it is accessed (recalled). To force this to occur with selected logical volumes, a job may be run that causes them to be recalled. When they are subsequently unloaded and demounted, the TS7700 VE will see that the pool now associated with the volumes is different than the one the last time they were copied from the cache and it will copy them to the new pool. This method, combined with directing all new allocations as described above, is probably sufficient if the time period allowed for migration is long enough such that most of the old data has expired or recalled as part of normal job processing, leaving a relatively small amount of data to migrate by forcing a recall. If there are a large number of volumes to migrate, the effort to set up the host jobs to force the recalls becomes cumbersome and cache space will be taken up by the recalled volumes.

Note: If there are a large number of volumes to migrate and this method is desired, the efficiency for recalling the data from tape can be improved by using a map of the logical volumes on them. Rather than randomly recalling the logical volumes, the map can be used to structure the recall job such that the volumes are requested in the order they are located on the tape. The Bulk Volume Information Retrieval (BVIR) function can provide the physical volume to logical volume mapping information. Refer to the 3494 ***Bulk Volume Information Retrieval Function User's Guide*** for details on how to use the function.

Note: If a logical volume is in cache at the time its primary pool assignment is changed, the pool assignment will not affect where the data will be copied until the volume is subsequently unloaded and demounted. It is during the rewind/unload command processing time that the primary pool destination for a logical volume is determined.

Move Logical Volumes Method

With this method, the valid logical volumes on one or more physical volumes are moved to a target pool that with encryption specified. This is accomplished by using the move stacked volume function of the library. Through that function, the logical volumes resident on a range of stacked volumes are moved to a target pool immediately or as each stacked volume becomes eligible for reclaim. This method is a better alternative than the force recall method to move a small number of logical volumes. The VE manages the migration internally and no host jobs need be run. Data is moved from tape to tape so no cache space is needed.

Reclamation Processing Method

This method uses reclamation policies to affect how quickly the old data is moved to encrypted volumes due to reclamation.

The following policies are supported:

Reclaim Percentage Threshold

A physical volume is eligible for reclaim when the amount of active data on the volume falls below the threshold defined for the pool. A value of 5 to 95 percent can be specified for this field. This is the default policy.

Days Since Last Accessed

A physical volume is eligible for reclaim when the number of days defined in the *days without access* field has elapsed since any data on the volume has been accessed because of a recall. A value from 1 to 365 days can be specified as a criteria for reclaim. A value of 0 disables this criteria for reclaim.

Days Since Last Written

A physical volume is eligible for reclaim when the number of days defined in the *age of last data written* field has elapsed since any data was written to the volume. A value from 1 to 365 days can be specified as a criteria for reclaim. A value of 0 disables this criteria for reclaim.

Days Since Last Data Inactivation

A physical volume is eligible for reclaim when the number of days defined in the *days without data inactivation* field has elapsed since any data was invalidated on the volume and the amount of active data on the volume falls below the threshold defined in the maximum active data field. A value from 1 to 365 days can be specified as a criteria for reclaim. A value of 0 disables this criteria for reclaim. A value of 5 to 95 percent can be specified for the maximum active data field.

Note: The maximum active data field is only used in conjunction with the days since last data inactivation policy. It is independent of the reclaim percentage threshold field.

Note: A portion of the data on a physical volume is invalidated when the logical volume it represents has been modified/rewritten or deleted (as part of the delete expired volume data function). The remaining data on the physical volume is considered active data.

When reclaim is allowed, the VE examines the physical volumes that have been filled and takes into account all of the policies specified for a pool independently when determining the physical volumes in the pool that are eligible for reclamation. Each pool can have a different set of reclamation policies. During reclamation processing, the VE will prefer eligible physical volumes that have the least amount of active data to move, considering all pools. This means that although a pool may have volumes that meet one or more of the reclamation policies for that pool, If another pool has physical volumes with less active data to move, it will get preference during reclaim. Physical volumes that have not yet been filled are not considered for reclamation.

Note: The reclamation workload for a VTS will increase while the migration of old data is taking place. The impact of that increased workload should be monitored and if it is impacting production use of the VTS, the inhibit reclamation policy setting for the VTS should be used to minimize that impact during peak production demand times.

If the dual copy function is used, the reclamation policies need to be set up for both the primary and secondary pools.

Clean-up

After all of the previously full volumes in a pool have been migrated (and assuming you redefined the pool to return scratch volumes), a few physical volumes will be left in the pool. Those volumes are ones that were partially filled when the migration began and are not considered for reclamation. You will need to use the move stacked volume method to complete the migration of the data from the pool.

Once you have completed the migration, you may redefine the old storage pools for other uses.

EKM Connections

The VE tries to maintain TCP/IP connections with all configured EKMs at all times. When contact is lost with a configured EKM, an operator intervention is raised at the Enterprise Library Controller (ELC). This is displayed on the user interface and web panels for the ELC. In addition, the host are notified of the degraded mode which is displayed on z/OS host consoles. When contact is regained, the intervention is cleared and the hosts are notified.

Operators should be trained to recognize and respond to EKM communications loss as loss of the second EKM will cause a temporary loss of access to encrypted data.

The VE will always perform key exchanges with the primary EKM when it can. If EKMs differ in host or network performance or reliability, the best choice should be specified as the primary EKM.

If communications with no EKMs are established when a key exchange is required, or if contact with EKMs is lost during the exchange, a call-home is generated to alert IBM service of the problem. Loss of communications with both EKMs will prevent you from accessing encrypted data, so is treated as a serious issue, even though the fault may lay in the network or host on which the EKMs are installed rather than the TS7700 VE.

Tracking Encryption Usage

If new storage pools are configured for use with encryption, database queries and statistics records gave give an indication of the amount of data being encrypted on the system.

The Library Manager specialist or user interface panels may then be used to query tape volumes in the encryption storage pools. This is most useful when you configure the pools to borrow and return tapes from the common scratch pool.

The TS7700 statistics records may also be used to gather information regarding storage pools used for encrypted data. See the ***IBM Virtualization Engine TS7700 Series Statistical Data Format White Paper*** for information on these statistics.

Messages for the host console are sent whenever a tape has been filled and a database backup has been written to it. For unencrypted tapes, the message is “Database Backup written to Physical Tape XXXXXX” while for encrypted tapes, the message is of the form "Database Backup written to Encrypted Physical Tape XXXXXX".

References

IBM Encryption Key Manager component for the Java platform Introduction, Planning, and User's Guide, GA76-0418

DFSMS Object Access Method Planning, Installation, and Storage Administration Guide for Tape Libraries, SC35-0427-04

IBM System Storage TS3500 Tape Library Operator Guide, GA32-0560

DFSMS: Using Magnetic Tapes , SC26-7412-01

DFSMSdfp Utilities, SC26-7414-02

z/OS V1R8.0 DFSMS Storage Administration Reference, SC26-7402-06

TS7700 Virtualization Engine Information Center, http://publib.boulder.ibm.com/infocenter/ts7700ic/v1r0/index.jsp

IBM TotalStorage Virtual Tape Server – Using 3592 In a VTS – Version 5,
http://www.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP100488

IBM TotalStorage Enterprise Automated Tape Library (3494) Operator Guide, GA32-0449

IBM White Paper - 3494 Bulk Volume Information Retrieval Function User's Guide,
http://www.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP100430

IBM Virtualization Engine TS7700 Series Statistical Data Format White Paper,
http://03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP100829

Disclaimers:

Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. This information could include technical inaccuracies or typographical errors. IBM may make improvements and/or changes in the product(s) and/or programs(s) at any time without notice.

References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business. Any reference to an IBM Program Product in this document is not intended to state or imply that only that program product may be used. Any functionally equivalent program, that does not infringe IBM's intellectually property rights, may be used instead. It is the user's responsibility to evaluate and verify the operation of any non-IBM product, program or service.

The information provided in this document is distributed "AS IS" without any warranty, either express or implied. IBM EXPRESSLY DISCLAIMS any warranties of merchantability, fitness for a particular purpose OR NON INFRINGEMENT. IBM shall have no responsibility to update this information. IBM products are warranted according to the terms and conditions of the agreements (*e.g*., IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) under which they are provided. IBM is not responsible for the performance or interpretability of any non-IBM products discussed herein. The customer is responsible for the implementation of these techniques in its environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. Unless otherwise noted, IBM has not tested those products in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

The provision of the information contained herein is not intended to, and does not grant any right or license under any IBM patents or copyrights. Inquiries regarding patent or copyright licenses should be made, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Trademarks

The following are trademarks or registered trademarks of International Business Machines in the United States, other countries, or both.

IBM, TotalStorage, DFSMS/MVS, S/390, z/OS, and zSeries.

Other company, product, or service names may be the trademarks or service marks of others.

