IBM z/VSE

Release Guide

Version 3 Release 1 Modification Level 3

SC33-8220-02

IBM z/VSE

Release Guide

Version 3 Release 1 Modification Level 3

SC33-8220-02

Note!

Before using this information and the product it supports, be sure to read the general information under "Notices" on page v.

This edition applies to Version 3 Release 1 Modification Level 3 of IBM z/Virtual Storage Extended (z/VSE), Program Number 5609-ZVS, and to all subsequent releases and modifications until otherwise indicated in new editions.

This edition replaces SC33–8220–01.

Order publications through your IBM representative or the IBM branch office serving your locality. Publications are not stocked at the addresses given below.

A form for readers' comments is provided at the back of this publication. If the form has been removed, address your comments to:

IBM Deutschland Entwicklung GmbH
Department 3248
Schoenaicher Strasse 220
D-71032 Boeblingen
Federal Republic of Germany

You may also send your comments by FAX or via the Internet:

Internet: s390id@de.ibm.com
FAX (Germany): 07031-16-3456
FAX (other countries): (+49)+7031-16-3456

When you send information to IBM, you grant IBM a non-exclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Contents

Notices

References in this publication to IBM products, programs, or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any of the intellectual property rights of IBM may be used instead of the IBM product, program, or service. The evaluation and verification of operation in conjunction with other products, except those expressly designated by IBM, are the responsibility of the user.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785, U.S.A.

Any pointers in this publication to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement. IBM accepts no responsibility for the content or use of non-IBM Web sites specifically mentioned in this publication or accessed through an IBM Web site that is mentioned in this publication.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Deutschland GmbH
Department 0790
Pascalstr. 100
70569 Stuttgart
Germany

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

Trademarks and Service Marks

The following terms are trademarks of International Business Machines Corporation in the United States, or other countries, or both:

Enterprise Storage Server
FICON
FlashCopy
IBM
The IBM logo
ibm.com
OS/390
System/390
System Storage
System z9
S/390
TotalStorage
VM/ESA
VSE/ESA
VTAM
zSeries
z/VM
z/VSE

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT and the Windows logo are trademarks of Microsoft Corporation in the United States, and/or other countries.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

SnapShot is a trademark of Storage Technology Corporation for a duplication product.

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

About This Book

This manual describes how you can encrypt tapes using the hardware-based encryption facilities provided by an *encryption-capable* tape device. Hardware-based tape encryption support has been implemented in IBM z/VSE Version 3, Release 1, Modification Level 3 (z/VSE 3.1.3).

It also briefly describes z/VSE 3.1.3's support for:

- The TS3400 Autoloader Tape Library
- DB2 Server for VSE Version 7 Release 5.

Who Should Use This Book

This manual is intended for those z/VSE users who need to be aware of the hardware-based tape encryption facilities provided with z/VSE Version 3 Release 1 Modification Level 3.

How to Use This Book

The book contains three chapters:

- Chapter 1, "Support for Hardware-Based Tape Encryption," on page 1
- Chapter 2, "Support for the TS3400 Autoloader," on page 11
- Chapter 3, "Support for DB2 Version 7 Release 5," on page 13

Where to Find More Information

Whenever appropriate, the book refers to other z/VSE manuals that provide further details on a specific topic.

The z/VSE home page provides additional z/VSE information:

z/VSE Home Page

z/VSE has a home page on the World Wide Web, which offers up-to-date information about VSE-related products and services, new z/VSE functions, and other items of interest to VSE users.

You can find the z/VSE home page at:

`http://www.ibm.com/servers/eserver/zseries/zvse/`

Chapter 1. Support for Hardware-Based Tape Encryption

> **Note!**
>
> Hardware-based tape encryption was first introduced with z/VSE Version 4 Release 1 (V4R1) and was described in detail in the manuals *supplied with z/VSE V4R1*. The implementation for z/VSE V3R1.3 is a "retrofit" of parts of the functionality that was first provided with z/VSE V4R1.

This chapter describes how you can encrypt tapes using the hardware-based encryption facilities provided by an *encryption-capable* tape drive. An example of an encryption-capable tape drive is the IBM System Storage TS1120[1].

This chapter contains these main topics:

- "Overview of Hardware-Based Tape Encryption" on page 2
- "Prerequisites for Using Hardware-Based Tape Encryption" on page 3
- "Restrictions When Using Hardware-Based Tape Encryption" on page 3
- "Tape Encryption When Running z/VSE as a Guest Under z/VM" on page 3
- "Support for the IBM System Storage TS1120 Tape Drive" on page 4
- "Obtaining and Installing the Encryption Key Manager" on page 4
- "Using a Job to Backup Data With Encryption" on page 4
- "Specifying KEKL Statements" on page 5
- "Specifying ASSGN Statements" on page 6
- "Using the Query Tape (QT) Command to Display Tape Information" on page 6
- "Reading the Contents of an Encrypted Tape" on page 7
- "Understanding Message 0P68I KEYXCHG ER" on page 7
- "Hints and Tips" on page 8

[1] The IBM System Storage TS1120 was previously referred to as the IBM TotalStorage 3592 Model E05.

Overview of Hardware-Based Tape Encryption

Figure 1 provides a simplified description of hardware-based tape encryption.

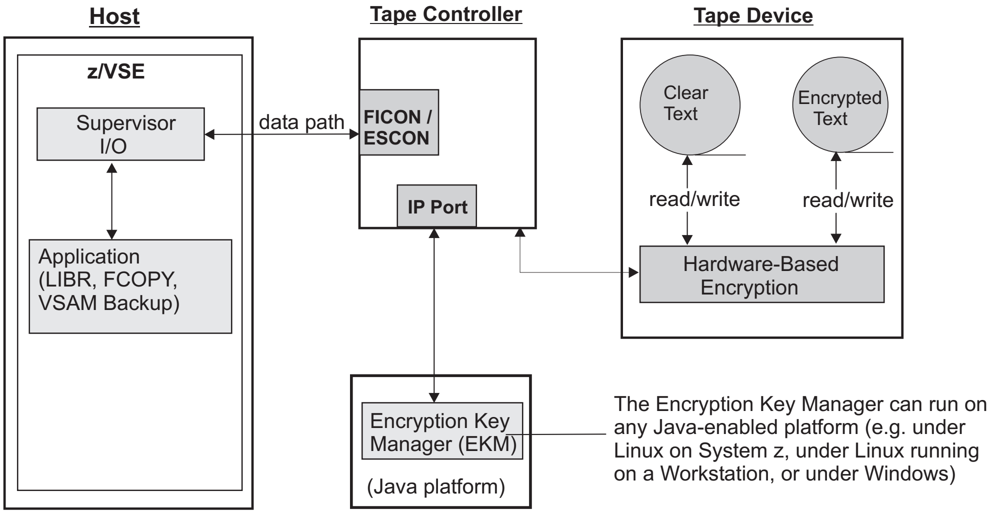
Host
z/VSE
Supervisor I/O
Application (LIBR, FCOPY, VSAM Backup)
data path
Tape Controller
FICON / ESCON
IP Port
Tape Device
Clear Text
Encrypted Text
read/write
read/write
Hardware-Based Encryption
Encryption Key Manager (EKM)
(Java platform)
The Encryption Key Manager can run on any Java-enabled platform (e.g. under Linux on System z, under Linux running on a Workstation, or under Windows)

Figure 1. Overview of Hardware-Based Tape Encryption

Here is an explanation of Figure 1:

1. A request is made for data to be backed-up to tape in *encrypted format*. This request can originate from a LIBR, FCOPY, or VSAM backup job running on the z/VSE host.

   An ASSGN statement (contained in the job or entered at the console) sets the Mode for the tape unit to 03, 0B, 2B, or 23 (all of which require encryption).

   A KEKL statement (contained in the job or entered at the console) containing one or two key-encryption-key labels informs z/VSE to associate a tape unit with one or two key-encryption-key labels.
2. The key-encryption-key labels are passed via the z/VSE Supervisor to the Encryption Key Manager (EKM).
3. "Key negotiation" takes place between the tape drive and the EKM, during which the EKM validates/supplies encryption keys with the tape drive. The tape drive and EKM communicate via the TCP/IP protocol.
4. If the key-verification process is successful, the data on the tape cartridge will be encrypted. If not, an error message is returned.

Prerequisites for Using Hardware-Based Tape Encryption

These are the prerequisites for using hardware-based tape encryption:

- The Encryption Key Manager must be running on a Java platform. For details, see “Obtaining and Installing the Encryption Key Manager” on page 4.
- You must have installed and configured an encryption-capable tape drive, such as the IBM System Storage TS1120 (IBM 3592 E05) and a tape controller.
- You must record your data using the *Encrypted Enterprise Format 2* (EEFMT2), which is the encrypted form of EFMT2. The EEFMT2 recording format is supported across all of the 3592 media types (MEDIA5 to MEDIA10).

Restrictions When Using Hardware-Based Tape Encryption

The following restrictions apply to the use of encrypted tapes:

- The use of the VSE/POWER POFFLOAD command to create encrypted tapes is **not** supported by the z/VSE Version 3 Release 1 Modification Level 3 implementation of hardware-based tape encryption.
- A tape cartridge cannot contain both encrypted and non-encrypted data.
- If the first file written to a tape is encrypted, all subsequent files written to that same tape cartridge will be encrypted using the *same key* (except for the volume label structure for the first file sequence).
- The DOSVSDMP utility is *not supported for encryption*. Therefore, a request to create an encrypted standalone dump tape using the DOSVSDMP utility will be rejected!

Tape Encryption When Running z/VSE as a Guest Under z/VM

The z/VSE and z/VM operating systems *both* support hardware-based tape encryption.

You are therefore recommended to use hardware-based tape encryption on *either* z/VSE or z/VM (*not* on both operating systems). Otherwise, there could be errors caused by different key labels being used. Below is a summary of the encryption possibilities that might be used with z/VM and z/VSE.

1. z/VM-Based Encryption IS Active (via an ATTACH or SET RDEV Command):

- If encryption *has not* been enabled in z/VSE via the *mode* setting of an ASSGN statement, encryption will be processed according to the encryption-settings *in z/VM*. However, although z/VSE is not “aware of” encryption, the QT (“Query Tape”) command *will* display the encryption-indication of the volume.
- If encryption *has* been enabled in z/VSE via the *mode* setting of an ASSGN statement, encryption will be handled according to the encryption-settings *in z/VSE*.

2. z/VM-Based Encryption IS NOT Active:

- If encryption *has* been enabled in z/VSE via the *mode* setting of an ASSGN statement, encryption will be handled according to the encryption-settings *in z/VSE*.

For further details about implementing hardware-based tape encryption under z/VM, refer to *z/VM CP Planning and Administration*, SC24-6083-04 or later.

Support for the IBM System Storage TS1120 Tape Drive

z/VSE V3R1.3 can be used with the IBM System Storage TS1120 (IBM 3592 E05) tape drive. This tape drive is designed to address the needs of applications for high capacity, fast access to data, and/or long term data retention.

The TS1120 offers these cartridges:
- 60 GB,
- 300 GB (up to 900 GB with 3:1 compression),
- 700 GB (up to 2.1 TB with 3:1 compression).

The above cartridge types are available in rewritable or WORM (Write Once Read Many) formats. WORM cartridges are designed to provide non-alterable, non-rewritable tape media for long-term records retention.

In addition to being used in standalone mode, a TS1120 tape drive can also be attached to an *IBM TotalStorage Enterprise Automated Tape Library 3494*. The TS1120 tape drive requires cartridges which are written in 512-track or 896-track formats.

Obtaining and Installing the Encryption Key Manager

The Encryption Key Manager (EKM) is a common-platform Java application that is used to generate and protect AES (Advanced Encryption Standard) keys. Upon request, the EKM generates AES keys to be used for encryption, and protects these keys using RSA key pairs.

To obtain a copy of the EKM from the Internet, you should:

1. Enter the following URL:

   ```
   http://www.ibm.com/support/us/
   ```

2. Search for “Encryption Key Manager” and locate the zipped file containing the EKM.
3. Download the zipped file containing the EKM to the directory where you want to install it.
4. Install and customize the EKM by following the instructions provided in the *IBM System Storage Tape Encryption Key Manager, Introduction, Planning and User Guide*, GA76-0418.

Using a Job to Backup Data With Encryption

Jobs for backing-up to tape with encryption (LIBR, FCOPY, VSAM Backup) *must* contain an ASSGN statement and *might* contain a KEKL statement. An example for a LIBR job is given below.

Example of a LIBR Job to Backup/Encrypt the Contents of a Library

The LIBR job below will backup to tape and encrypt the contents of library PRD2. It specifies *two* key-encryption-key labels (KEKL1 and KEKL2). The tape drive has a unit address (cuu) of 480.

```
// JOB ENCRYPT
// ID USER=user-ID,PWD=password
// ASSGN SYS005,480,03
// KEKL UNIT=480,KEKL1='HUSKEKL1',KEM1=L,KEKL2='HUSKEKL2',KEM2=L
```

```
// EXEC LIBR
BACKUP LIB=PRD2 TAPE=SYS005
/*
/&
```

Specifying KEKL Statements

Jobs for backing-up to tape with encryption (LIBR, FCOPY, VSAM backup) *might include* a KEKL statement.

If your job does *not contain* a KEKL statement, the EKM will *use the defaults* that you previously generated and stored in the EKM.

The KEKL statement has the following syntax:

```
// KEKL UNIT={cuu|SYSnnn},KEKL1='KEKL1',KEM1={L|H},KEKL2='KEKL2',KEM2={L|H}
// KEKL UNIT={cuu|SYSnnn},KEKL1='KEKL1',KEM1={L|H}
// KEKL UNIT={cuu|SYSnnn},CLEAR
```

where:

cuu Specifies the tape unit for which the key-encryption-key labels are to be used.

SYS*nnn*
Specifies the logical unit of the tape unit for which the key-encryption-key labels are to be used. *This logical unit must have been previously assigned*. The value of *nnn* can be:
- between 000 and 255
- LST
- PUN

KEKL1 Is the label for the first key-encryption-key to be used by the EKM to encrypt the data encryption key. Must be enclosed in single quotation marks.

KEKL2 Is the label for the second key-encryption-key to be used by the EKM to encrypt the data encryption key. Must be enclosed in single quotation marks.

L|H Specifies the “encoding mechanism” (KEM). The KEM specifies how the labels for the first key-encryption-key (KEKL1) and second key-encryption-key (KEKL2) is encoded by the EKM and stored on the tape cartridge. The values can be either:
L Encoded as the specified label.
H Encoded as a hash of the public key.

CLEAR
Indicates that the information previously established by a KEKL statement is cleared.

Note: You might need to reset the KEKL (the default KEKL, or the KEKL from a previous KEKL statement) on a previously-encrypted volume. To do so, you must issue a WRITE command (for example, writing a tape mark) from the Beginning-Of-the-Tape (BOT) with *encryption mode not active*.

Specifying ASSGN Statements

Jobs (LIBR, FCOPY, VSAM backup) that require hardware-based tape encryption must include an ASSGN statement as follows:

Method 1: Specify the Device Mode of the Encryption-Capable Tape Drive.

The syntax of the ASSGN statement is as follows:

```
// ASSGN SYSnnn,cuu,mode
```

where:

- *cuu* is the device address of the encryption-capable tape drive.
- *mode* is a 1-byte field that determines how the data on the tape should be written. These are the encryption-related modes you can use:

X'03'	Encryption Write Mode
X'0B'	Encryption and IDRC (compression) Write Mode
X'23'	Encryption with unbuffered Write Mode
X'2B'	Encryption and IDRC (compression) and unbuffered Write Mode

Note: IDRC is an abbreviation for Improved Data Recording Capability.

Method 2: Let z/VSE Find a Suitable Tape Drive

Here, you:

1. Specify that you require an encrypted write-format.
2. Let z/VSE locate a suitable tape drive.

The syntax of the ASSGN statement is as follows:

```
// ASSGN SYSnnn,device_class,mode
```

If the tape *device_class* is set to EEFMT2, z/VSE will search your system for an encryption-capable tape drive. The *mode* specifies any encryption mode.

Using the Query Tape (QT) Command to Display Tape Information

You can use the Attention Routine (AR) **QT** command to display the mode of a tape drive that is attached to your z/VSE system.

In the following example:

- CODE 5603 indicates:
  - A tape drive that uses the TPA is attached to z/VSE (the **56** part of 5603).
  - This tape drive is assigned to encryption mode (the **03** part of 5603).
- 3592-E05 is the device type for the IBM System Storage TS1120 (IBM 3592 E05) tape drive.
- KEY_LABEL_001 is the label for the first key-encryption-key to be used by the EKM to encrypt the data encryption key.
- KEY_LABEL_002 is the label for the second key-encryption-key to be used by the EKM to encrypt the data encryption key.

```
QT A83
AR 0015 CUU  CODE DEV.-TYP   VOLID  USAGE   MED-TYP   STATUS    POSITION
AR 0015 A83  5603 3592-E05   PAUL01 BG      CST5 /E   RESERVED  8 BLK
AR 0015      CU   3592-C06          LIB     3494-L10  (GALL88)
AR 0015                             FAST-ACC.SEG.=     0 MB    FILES = 2
AR 0015 KEKL1:KEY_LABEL_001
AR 0015 KEKL2:KEY_LABEL_002
AR 0015 1I40I  READY
```

Figure 2. Using the QT Command to Display the Details of an Encrypted Tape

Reading the Contents of an Encrypted Tape

Figure 3 is an example of how to read the contents of an encrypted tape *using the LIBR utility*:

- This job does *not* require KEKL statements to specify the encryption keys to be used.
- If KEKL statements are included in the job, they will be ignored.
- To read the encrypted data, the job uses the keys that are already stored on the tape.

However, these are the prerequisites for running this job:

- The z/VSE host where the job is to run must be connected to an EKM.
- The tape must have been previously encrypted using keys that are known by the currently-connected EKM.
- The encryption keys must not have been deleted from the currently-connected EKM.

```
* $$ JOB JNM=LIBSCAN,DISP=D,PRI=3,                                     C
* $$ NTFY=YES,                                                         C
* $$ LDEST=*,                                                          C
* $$ CLASS=0
// JOB LIBSCAN  SCAN VSE LIBRARY BACKUP TAPE
* THIS FUNCTION USES A TAPE FOR INPUT
* MOUNT TAPE BACKUP ON DEVICE 480
* THEN CONTINUE. IF NOT POSSIBLE CANCEL THIS JOB.
// PAUSE
// MTC REW,480
// ASSGN SYS004,480
// EXEC LIBR,PARM='MSHP'
   RESTORE *                         /* LIBRARY IDENTIFICATION */ -
          SCAN  = YES                /* SCAN SPECIFICATION     */ -
          TAPE = SYS004              /* TAPEADDRESS            */
/*
// MTC RUN,480
/&
* $$ EOJ
```

Figure 3. Using a LIBR Job to Read the Contents of an Encrypted Tape

Understanding Message 0P68I KEYXCHG ER

The EKM generates this message explanation:

```
0P68I Encryption key negotiation with the EKM failed
```

However, the *sense data* of the message contains additional useful information. For example:

```
804C08C022402751 0001FF0000000000 0005EE3100000092 2004E82061BA2111

CU=00 DRIVE=000000 EKM=EE31
```

In the above example (which starts at byte 0), bytes 4 and 5 might contains **2240**. This is the return code and reason-qualifier code (RC-RQC). It means that the required encryption-key exchange *has failed*. Furthermore:

1. Byte 8 contains the *CU reason code* (in the above example, **00**).
2. Bytes 13 ,14 and 15 contain the *sense key from the device* (in the above example, **000000**).
3. Bytes 18 and 19 contain the *sense key from the EKM*:
   - A value **0000** would mean that a failure has occurred whilst connecting to the EKM.
   - The value **EE31** (shown in the above example) means that an encryption configuration problem has occurred in which the error has something to do with the *key store*.

For further details of this and other EKM error messages, refer to the *IBM System Storage Tape Encryption Key Manager, Introduction Planning and User Guide*, GA76-0418.

Hints and Tips

This section contains various hints and tips that you might find useful.

Assigning System Logical Units

This problem-situation might arise:

1. The assignment of system logical units results in OPEN processing (during VOL1 and header-label checking). After OPEN processing:
   a. The tape (for labeled tapes) is positioned *behind* the VOL1 label.
   b. Previously-used KEKLs are still active.
2. A subsequent KEKL statement that is set *after* the ASSGN statement causes the job *to be cancelled*.

To overcome this problem, you can create the following job:

```
// ASSGN SYSnnn,cuu,mode
// MTC REW,cuu
// KEKL UNIT=cuu,KEKL1='TEST',KEM1=L
```

The *mode* must be one of the encryption modes (for example, **03**).

Positioning of the Tape When Using the ASSGN Statement

The syntax of the ASSGN statement is as follows:

```
ASSGN SYSnnn,cuu,mode
```

If the tape specified in the *cuu* device address is *at load point*, the new *mode* setting is *immediately effective*.

If the tape specified in the *cuu* device address is *not at load point*, the new *mode* setting will be effective *the next time a write occurs at load point*.

For *mode* set to encryption X'03':

- If the tape was *at load point*, the tape will be written *as encrypted*.

- If the tape was *not at load point*, the tape will continue writing *in the current mode*.

If the first file written to a tape is encrypted, all subsequent files written to that *same tape cartridge* will be encrypted using *the same data key*.

Handling Situations Where the EKM is not Available

If a tape contains encrypted data and is rewritten *without* encryption activated, the job might fail with a key-exchange error (described in "Understanding Message 0P68I KEYXCHG ER" on page 7).

This is because certain standalone utilities read the VOL1 label *before* starting the I/O process.

To overcome this problem, before you resubmit the job you should:

1. write a tape mark,
2. rewind the tape.

Running Standalone Utilities (FCOPY, ICKDSF, DITTO, LIBR)

The standalone utilities FCOPY, ICKDSF, DITTO, and LIBR can be called from an encrypted standalone backup tape.

Backups performed from any of these utilities will be in *unencrypted format* only.

Additional Considerations When Using LIBR Utility

A LIBR BACKUP job with RESTORE=STANDALONE can be written in encrypted format.

- If an IPL is made from an *unlabeled* tape, there might be a delay when the key-exchange occurs. You might be required to re-IPL the tape drive using the `IPL cuu` command.
- If an IPL is made from a *labeled* tape, you might have to enter the `IPL cuu` command approximately *four times*, until the tape marks at the beginning of the tape have been skipped. This problem can also occur without encryption.

Overwriting Encrypted Volumes

If an encrypted volume is processed but the key is unknown to the EKM, access might fail with the message "0P68I Key Exchange Error" (described in "Understanding Message 0P68I KEYXCHG ER" on page 7).

To overcome this error, you can write a tape mark at the Beginning-Of-the-Tape (BOT).

Multivolume File Processing

To process a multivolume file on an *alternate* volume, you must specify the *same KEKL* as was specified for the *original volume*.

Here is an example of how to process a multivolume file. In this example, the specified alternate tape must also be assigned to encryption mode.

```
// ASSGN SYS005,cuu1,3
// ASSGN SYS006,cuu2,3
// ASSGN SYS005,cuu2,ALT
// KEKL UNIT=cuu1,KEKL1='TEST',KEM1=L
// KEKL UNIT=cuu2,KEKL1='TEST',KEM1=L
```

Chapter 2. Support for the TS3400 Autoloader

From z/VSE Version 3 Release 1 Modification Level 2 onwards, z/VSE supports the TS3400 tape library as an *autoloader* operating in AUTO mode. In AUTO mode, as soon as a cartridge is unloaded from the drive, the next unused cartridge is loaded.

The TS3400 autoloader tape library supports up to **two** IBM System Storage TS1120 (3592 Model E05) tape drives. These are added in z/VSE as standalone TPA (Tape Products Architecture) devices.

The TS3400 contains two *cartridge magazines* that each hold up to nine tapes. The lower magazine can be configured to use up to three slots as *I/O slots*. This can be done using either the TS3400 Operator Panel, or using the Web Interface.

For details of how to:

- add TS1120 (3592 Model E05) tape drives as standalone TPA devices, refer to the chapter "Configuring Non-Communication Devices" in the *z/VSE Administration*.
- encrypt tapes using the hardware-based encryption facilities provided by an encryption-capable tape drive, see Chapter 1, "Support for Hardware-Based Tape Encryption," on page 1.
- setup and configure the TS3400 autoloader, refer to the technical article "Overview of IBM System Storage TS1120 Tape Controller Support for System Storage TS3400 Tape Library", which you can find in the "Documentation" section of the *z/VSE Homepage* (whose URL is given in "Where to Find More Information" on page vii).

Chapter 3. Support for DB2 Version 7 Release 5

The DB2 Server for VSE Version 7 Release 5 is shipped on the z/VSE Extended Base Tape.

The installation and Fast Service Upgrade (FSU) *Program Development dialogs* establish Version 7 Release 5 of the DB2 Server for VSE. This includes support for the *DB2 Client Edition for VSE*. For details, refer to the relevant DB2 documentation.

Index

Readers' Comments — We'd Like to Hear from You

IBM z/VSE
Release Guide
Version 3 Release 1 Modification Level 3

Publication No. SC33-8220-02

We appreciate your comments about this publication. Please comment on specific errors or omissions, accuracy, organization, subject matter, or completeness of this book. The comments you send should pertain to only the information in this manual or product and the way in which the information is presented.

For technical questions and information about products and prices, please contact your IBM branch office, your IBM business partner, or your authorized remarketer.

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you. IBM or any other organizations will only use the personal information that you supply to contact you about the issues that you state on this form.

Comments:

Thank you for your support.

Submit your comments using one of these channels:
- Send your comments to the address on the reverse side of this form.
- Send a fax to the following number: FAX (Germany): 07031+16-3456
  FAX (Other Countries): (+49)+7031-16-3456
- Send your comments via e-mail to: s390id@de.ibm.com

If you would like a response from IBM, please fill in the following information:

Name

Company or Organization

Phone No.

Address

E-mail address

Readers' Comments — We'd Like to Hear from You

SC33-8220-02

Cut or Fold
Along Line

Fold and Tape **Please do not staple** Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

IBM Deutschland Entwicklung GmbH
Department 3248
Schoenaicher Strasse 220
D-71032 Boeblingen
Federal Republic of Germany

Fold and Tape **Please do not staple** Fold and Tape

Cut or Fold
Along Line

File Number: S370/S390-34
Program Number: 5609–ZVS

Printed in USA

SC33-8220-02

Spine information:

IBM z/VSE

z/VSE V3R1.3 Release Guide

Version 3 Release 1
Modification Level 3

SC33-8220-02