Directory Maintenance VM/ESA

General Information

Release 5.0

GC20-1836-07

Directory Maintenance VM/ESA

General Information

Release 5.0

GC20-1836-07

Note:

Before using this information and the product it supports, read the general information under “Notices” on page 31.

| **Eighth Edition (February 2001)**

| This edition applies to Version 1, Release 5, Modification 0 of IBM® Directory Maintenance (DirMaint VM/ESA®) (product number
| 5748-XE4) and to all subsequent releases and modifications until otherwise indicated in new editions.

| This edition replaces GC20-1836-06.

Contents

Preface

This publication provides information about Release 5.0 for the IBM Directory Maintenance VM/ESA, Program Number 5748-XE4. This program product provides efficient and secure interactive facilities for maintenance of your VM system directory. You should have a knowledge of VM; in particular you should have knowledge of the purpose, structure, and contents of the system directory. You should also be familiar with the system directory information provided in *z/VM: Planning and Administration*.

How to Send Your Comments to IBM

Your feedback is important in helping us to provide the most accurate and high-quality information. If you have comments about this book or any other VM documentation, send your comments to us using one of the following methods. Be sure to include the name of the book, the form number (including the suffix), and the page, section title, or topic you are commenting on.

- Visit the DirMaint web site at:

  `http://www.vm.ibm.com/related/dirmaint`

  There you will find the feedback page where you can enter and submit your comments.

- Send your comments by electronic mail to one of the following addresses:

  Internet: pubrcf@vnet.ibm.com

  IBMLink™: GDLVME(PUBRCF)

- Fill out the Readers' Comments form at the back of this book and return it using one of the following methods:
  - Mail it to the address printed on the form (no postage required in the USA).
  - Fax it to 1-607-752-2327.
  - Give it to an IBM representative.

Introduction to IBM Directory Maintenance VM/ESA

IBM Directory Maintenance VM/ESA (DirMaint) is a Conversational Monitor System (CMS) application that helps you manage your VM directory. Directory management is simplified by DirMaint's command interface and automated facilities. DirMaint's directory statement-like commands are used to initiate directory transactions. DirMaint's error checking ensures that only valid changes are made to the directory, and that only authorized personnel are able to make the requested changes. Any transaction requiring the allocation or deallocation of minidisk extents can be handled automatically. All user initiated transactions can be password controlled and can be recorded for auditing purposes.

The DirMaint functions are accomplished by two disconnected virtual machines equipped with an automatic restart facility. The DIRMAINT virtual machine owns and manages the directory, and the DATAMOVE virtual machine performs the copying and formatting of CMS minidisks. Users invoke DirMaint functions by submitting commands to the DIRMAINT virtual machine. Large systems may have multiple DATAMOVE machines.

The use of virtual machines to provide services for directory maintenance functions takes advantage of the inherent reliability, availability, and serviceability characteristics of the system architecture. The automatic re-initial program load (re-IPL) feature ensures against loss of availability and removes the dependency upon human intervention in the event of a directory virtual machine programming failure. The likelihood of a system-wide directory lockout caused by erroneous directory maintenance, such as human or input/output (I/O) errors, is significantly reduced.

DirMaint provides a command for every VM directory statement, plus additional commands for managing DirMaint itself. These commands mimic the format of the system directory entries, so familiarity with one makes learning the other easier. Online HELP is available for every command, as well as every message.

Command authorization is controlled by use of command sets. Users can be authorized to use multiple command sets. DirMaint comes with 9 command sets already defined. Commands sets can be changed, or additional ones created during or after installation. Up to 36 command sets are supported.

Numerous user exit routines provide support for centralized directory maintenance of distributed systems and the ability for DirMaint to communicate with other products, including external security managers such as IBM Resource Access Control Facility (RACF®).

DirMaint Release 5.0 uses VMSES/E to simplify installation and service. DirMaint Release 5.0 can run in 370, XA, ESA, or XC mode, and is supported on with VM releases:

- VM/ESA (370 Feature) Release 1.5
- VM/ESA Version 1 Release 2.1
- VM/ESA Version 1 Release 2.2
- VM/ESA Version 2 Release 1.0
- VM/ESA Version 2 Release 2.0
- VM/ESA Version 2 Release 3.0

- VM/ESA Version 2 Release 4.0
- z/VM Version 3 Release 1.0

as well as any future releases of VM, until otherwise announced.

Program Highlights

DirMaint provides efficient, easy-to-use, and secure interactive facilities for maintaining the system directory. The nuisances resulting from manually maintaining a system directory are virtually eliminated by using DirMaint.

The highlights of the DirMaint product are summarized below.

- DirMaint operates as a CMS application on a VM/ESA operating system. It can run in 370, XA, ESA, or XC mode. It uses CMS interfaces for CMS and control program services. As a CMS application, DirMaint is not dependent on specific hardware. DirMaint does verify that the device types specified in DirMaint command operands are only those supported by the host control program.
- DirMaint has a corresponding command for every VM/ESA directory statement, including cross system extension (CSE) cluster directory statements. All directory transactions are done by issuing commands to the DIRMAINT service machine, therefore taking advantage of DirMaint's automated DASD management, error checking, and auditing facilities. With a few exceptions, the syntax of the DirMaint directory commands and the system directory statements are the same. This eases the transition from manual directory maintenance to using DirMaint's automated method.
- Command authorization is controlled by assigning DirMaint commands to privileged command sets. Users may be authorized to issue commands from multiple DirMaint command sets. This allows for delegation of certain types of directory tasks to specific support personnel. Also, general users can be given authorization to manage their portion of the directory not related to resource allocation. This capability provides for timely directory modifications and can relieve the system administrator from making all directory changes.
- DirMaint supports up to 36 privilege command sets. All of these sets can be customized by the installation. By default, DirMaint provides 9 predefined privileged command sets at installation. They are:
  - system administrator
  - DASD management administrator
  - general user
  - help desk
  - password control and monitoring
  - system operator
  - automated DASD management programs
  - support programmer
  - internal use (DIRMAINT, DATAMOVE, DIRMSAT*x* service machines)
- DirMaint provides numerous user exit routines that enable centralized directory maintenance of remote systems, while still allowing the delegation of certain types of directory maintenance tasks to personnel located at these remote sites. Some exit routines also enable DirMaint to interact with other products such as RACF and OfficeVision/VM™.
- DirMaint Release 5.0's open command structure allows you to replace any and all commands with your own user-written commands.

- DirMaint Release 5.0 maintains compatibility with DirMaint Release 4.0 user-written programs. You have the choice of running DirMaint in two command levels: 140A or 150A. Using the 140A command level, commands are invoked for DirMaint Release 5.0 using the same syntax as used in DirMaint Release 4.0. Few new commands, and minimal new function is provided using the 140A level. The 150A command level allows for use of all new commands and function provided with DirMaint Release 5.0. You can use the 140A command level until you have converted your user-written programs to be compatible with the 150A level.
- DirMaint minimizes the possibility of human error through an automated process for copying CMS minidisk files. This process optionally formats the old (source) minidisk before returning it to the available minidisk pool.
- DirMaint ensures the integrity of CMS files by preventing new minidisk space from being inadvertently allocated over existing extents.
- DirMaint improves overall system efficiency by minimizing the number of DIRECT or DIRECTXA utility runs required. The update-in-place facility (DIAGNOSE X'84') can be used to place many of the changes online immediately.
- DirMaint ensures the integrity of the directory through the ownership of strictly-controlled service virtual machines that use automatic backup/restore and auditing of all service machine transactions.
- System security is enhanced by providing the ability to enforce regular password changes. A user is required to enter the new password twice when changing it to guard against typographical errors.
- An additional level of security can be implemented by requiring that a password be entered for every user transaction. This is the default. For more information on password authorization strategy, see *Directory Maintenance VM/ESA: Tailoring and Administration Guide*.
- DirMaint can be installed as either interpretive REXX or compiled REXX. Interpretive REXX provides the flexibility to easily modify and write new user exits, while compiled REXX provides better performance. If the REXX compiler is installed, an installation can achieve both flexibility and performance.
- A menu is displayed for the most complex DirMaint commands if the command name is specified without any parameters.
- HELP abbreviations are the same as the DirMaint command abbreviations. Generally, the minimum abbreviation is 3 characters. In some cases, more than 3 characters may be required to make the abbreviation unique.
- The DirMaint service machines can run disconnected and unattended in a stand-alone processor, or in a cross system extension (CSE) cluster.
- DirMaint's installation and service is simplified by using VMSES/E.
- Online HELP is available for every DirMaint command and message.
- DirMaint provides national language support for translation of error messages and responses. DirMaint Release 5.0 is available in mixed case American English, uppercase English, and Japanese Kanji.

Release 5.0 Enhancements

DirMaint Release 5.0 provides many new features and functions that make directory maintenance as simple and painless as possible. Complete support for VM/ESA Version 2 Release 1.0 system directory statements, additional commands that extend DirMaint's control, support for additional options on existing commands, more command authorization sets, many new exit routines, DASD management improvements, installation and service using VMSES/E, plus many more miscellaneous enhancements make DirMaint Release 5.0 an excellent choice for directory maintenance.

Complete Directory Statement Support

DirMaint Release 5.0 provides support for every VM/ESA directory statement, including CSE cluster directory statements. In addition to the directory statements previously supported in DirMaint Release 4.0, DirMaint Release 5.0 now supports these additional directory statements:

ACIGROUP	IUCV	PRIORITY
CLASS	LOGONBY	SHARE
CRYPTO	POOL	SPOOL
DATEFORMAT	POSIXFSROOT	SPECIAL
DEDICATE	POSIXGROUP	STDEVOPT
DIRECTORY	POSIXINFO	SYSAFFIN
D8ONECMD	POSIXIUPGM	XAUTOLOG
GLOBALOPTS	POSIXIWDIR	
INCLUDE	POSIXOPT	

Note: POSIXIUPGM, POSIXIWDIR, and POSIXFSROOT are not directory statements, but are DirMaint commands that manipulate the IUPGM, IWDIR, and FSROOT fields on the POSIXINFO statement.

Additional Commands to Control DirMaint Operations

These commands were added to support the operation and usability of the DirMaint Release 5.0 program:

ACNTADD	CHECK	EXECLOAD
ACNTDEL	DEFAULTS	GLOBALV
AUTHBY	DROPBY	SECUSER*
AUTHFOR	DROPFOR	SETACNT*
AUTHLINK	DROPSCIF	SETCLASS*
AUTHSCIF	EXECDROP	SETPRIOR*

Note: The SECUSER, SETACNT, SETCLASS, and SETPRIOR are not commands used to control DirMaint, but are used to manipulate fields on the CONSOLE, ACCOUNT, CLASS, and USER directory statements respectively.

Additional Link Mode Support for Existing DirMaint Commands

These commands that existed in DirMaint Release 4.0 now support all of the link modes supported by VM/ESA Version 2 Release 1.0, as well as some additional DirMaint-specific options:

These commands now accept all link modes supported by CP:

Command	New Options
AMDISK	SR, ER, SW, EW, SM,

Command	New Options
LINK	RS, RE, WS, WE, MS, ME, MWS, RRS, RRE, WRS, WRE, MRS, MRE
MDISK	SR, ER, SW, EW, SM

These DirMaint commands have additional options for maintaining and moving links during minidisk and user ID manipulation:

Command	New Options
CHNGID	KEEPLINKS, MOVELINKS
CHVADDR	KEEPLINKS, MOVELINKS
DMDISK	KEEPLINKS
PURGE	KEEPLINKS
USEROPTN	LINKS EXCLUDE
TMDISK	KEEPLINKS

More Flexible Authorization Control through Command Sets

With DirMaint Release 5.0 you can have up to 36 tailorable DirMaint command sets. A user ID cannot issue commands in a command set unless authorized to do so. However, user IDs can be authorized to act on behalf of other user IDs, and may be authorized to use the command sets of the user ID they are acting on behalf of. This allows for delegation of administrative authority. For example, administrative authority could be delegated to class instructors over student user IDs, or to department supervisors over user IDs within their department.

By default, DirMaint Release 5.0 provides these nine command sets at installation:

- A - system administrator
- D - DASD management administrator
- G - general user
- H - HELPDESK team
- M - password monitor and control
- O - system operator
- P - automated DASD management programs, such as DFSMS/VM®
- S - support programmer
- Z - internal use (DIRMAINT, DATAMOVE, DIRMSAT service machines)

By comparison, DirMaint Release 4.0 provided only six command sets with membership in those command sets fixed at installation. The relationship between the Release 4.0 and Release 5.0 command sets is as follows:

Release 4.0	Release 5.0 equivalent
DIRM_STAFF	G A D H P
DIRM_SUB_STAFF	G H
OPERATOR	G O
PWMON	G M
OWNER	G S
not listed	G

Greater Flexibility through Additional Exit Routines

The availability of new exit routines provided by DirMaint Release 5.0 allows you great flexibility in tailoring DirMaint to meet your needs. DirMaint Release 4.0 provided only nine exit routines for the DIRMAINT service machine and no user exits. DirMaint Release 5.0 provides additional exit routines that allow you to tailor DirMaint functions, or if you wish, even write your own command routines. Where appropriate, the DirMaint exit routines are enabled for handshaking between DirMaint and other programs, such as RACF, OVVM, or products that facilitate distributed processing. Some exit routines may require tailoring for use with RACF or other external security managers. Most supplied exit routines are written in the REXX programming language for easy tailoring.

The DirMaint Release 4.0 exits have been replaced with new exits that perform comparable function, but have been enhanced for system affinity support. The Release 4.0 exit routines and their corresponding Release 5.0 replacement exit routines are:

Release 4	Release 5.0
DVHUA1	DVHXRB
DVHUA2	DVHXRA
DVHACCT	DVHXAV
DVHACCTM	DVHXAV
DVHPWX	DVHPXV
DVHMPW	DVHXMP
DVHLOCAL	DVHXPROF
DVHDATLC	DVHXPROF
DVHSATLC	DVHXPROF

There are three types of IBM supplied exits for Release 5.0: User Exits, DIRMAINT Service Machine Exits, and DATAMOVE Service Machine Exits. Any of these exits may be modified or replaced by a user-written exit, or be called by a user-written command (see “User-Written Command Handlers using SDI Routines” on page 9).

Release 5.0 User Exits

COMMAND_BEFORE_PARSING_USER_EXIT (DVHCXC EXEC)
: Command exit, before parsing. IBM supplies a sample.

COMMAND_BEFORE_PROCESSING_USER_EXIT (DVHCXB EXEC)
: Command exit, after parsing, before processing. No sample is provided.

COMMAND_AFTER_PROCESSING_USER_EXIT (DVHCXA EXEC)
: Command exit, after processing. IBM supplies a sample.

PASSWORD_RANDOM_GENERATOR_USER_EXIT (DVHPXR EXEC)
: User's logon password exit, random generator. IBM supplies a sample.

PASSWORD_SYNTAX_CHECKING_USER_EXIT (DVHPXV EXEC)
: User's logon password exit, syntax verification. IBM supplies a sample.

PASSWORD_NOTIFICATION_USER_EXIT (DVHPXA EXEC)
: User's logon password exit, after transmission to DIRMAINT. IBM supplies a sample.

Release 5.0 DIRMAINT Service Machine Exits

ESM_PASSWORD_AUTHENTICATION_EXIT (DVHDA0 MODULE)
: Exit for password verification by a call to an external security manager (ESM). The IBM supplied routine uses DIAGNOSE X'A0' subcode 4 to call RACF.

ESM_LOG_RECORDING_EXIT (DVHESMLR EXEC)
: Exit for recording a message in an ESM audit log. The IBM supplied routine uses RACROUTE to call RACF.

PW_REUSE_HASHING_EXIT (DVHHASH MODULE)
: Routine hashes the user's password for storage in the password history file. The file type may be either EXEC or MODULE. The IBM supplied default is DVHHASH MODULE. If not specified, the passwords will be stored in the history file as hexadecimal digits.

PASSWORD_RANDOM_GENERATOR_EXIT (DVHPXR EXEC)
: Exit for random logon password generation. Allows the installation to customize the format of passwords generated by PWGEN. The IBM supplied default is alphanumeric, with the length specified by the issuer of the PWGEN command. (This is the same routine as the user exit.) IBM supplies a sample.

PASSWORD_SYNTAX_CHECKING_EXIT (DVHPXV EXEC)
: Exit for logon password syntax verification. The passed parameters are enhanced for networking support. The exit will now make ALL decisions regarding password acceptability for the PW and TESTPW , as well as the ADD, SETPW, and CHNGID commands; including when and whether to accept or reject passwords of AUTOONLY, LBYONLY, NOLOG, NOPASS, or a password equal to the user ID. (This is the same routine as the user exit.) IBM supplies a sample.

ACCOUNT_NUMBER_NOTIFICATION_EXIT (DVHXAN EXEC)
: Exit for user account number notification. This exit may be used to notify other service machines of changes to a user's account number. It will be called whenever an account number change is successful. No sample is provided.

ACCOUNT_NUMBER_VERIFICATION_EXIT (DVHXAV EXEC)
: Exit for user account number verification. The passed parameters are enhanced for networking support. The exit will not only be called for the ACCOUNT command, but also for ADD, CHNGID, PURGE, and SETACNT. IBM supplies a sample.

CHECK_USER_PRIVILEGE_EXIT (DVHXCP EXEC)
: Exit for checking user privilege. This exit may be used to determine whether a given user ID is *privileged*. This determines which password change interval rule applies. No sample is provided.

DASD_AUTHORIZATION_CHECKING_EXIT (DVHXDA EXEC)
: Exit for DASD authorization checking. This exit routine determines whether the originator is authorized to allocate space for the target user ID on the requested DASD volume. This supports distributed (departmental) administration and centralized (networking) administration. This exit will be called for all AMDISK, CMDISK, RMDISK, and ADD, commands. No sample is provided.

DASD_OWNERSHIP_NOTIFICATION_EXIT (DVHXDN EXEC)
: Exit for DASD notification. This exit may be used to notify other service machines of new, deleted, or transferred minidisks. It will be called

whenever the ADD, REPLACE, CHNGID, PURGE, AMDISK, DMDISK, CHVADDR, or TMDISK commands have added, deleted, or changed ownership of a minidisk. No sample is provided.

FOR_AUTHORIZATION_CHECKING_EXIT (DVHXFA EXEC)
: Exit for FOR authorization checking. This exit routine determines whether the originator is authorized to issue commands FOR the target user ID, and if so the command sets authorized. This supports distributed (departmental) administration and centralized (networking) administration. No sample is provided.

LINK_AUTHORIZATION_EXIT (DVHXLA EXEC)
: Exit for link authorization checking. This exit may be used to perform alternative checking for LINK authorization. It will be called whenever a LINK command is issued, other than a LINK DELETE. It will also be called for ADD (ADD generates LINK requests indirectly), REPLACE, and CHNGID. No sample is provided.

ESM_LOG_FILTER_EXIT (DVHXLF EXEC)
MESSAGE_LOGGING_FILTER_EXIT (DVHXLF EXEC)
: Exit for log record filtering. By default, all commands received by the DIRMAINT machine are auditable, and all messages sent by the DIRMAINT machine are auditable. This exit routine may selectively reduce the quantity of data logged. IBM supplies a sample.

LINK_NOTIFICATION_EXIT (DVHXLN EXEC)
: Exit for notification to used for notifying other service machines of changes to directory LINKs. It will be called whenever a LINK command is issued, including a LINK DELETE. It will also be called for ADD (ADD generates LINK requests indirectly), REPLACE, CHNGID, and PURGE. No sample is provided.

(DVHXLVL EXEC)
: Pre-profile exit for linking alternate disks or other environmental modifications. This exit is common for the DIRMAINT, DATAMOVE, and DIRMSAT service machines. This exit name is not tailorable.

MINIDISK_PASSWORD_NOTIFICATION_EXIT (DVHXMN EXEC)
: Exit for minidisk password change notification. This exit may be used to notify other service machines of changes to a user's minidisk password. It will be called whenever a minidisk password change is successful. IBM supplies a sample.

MINIDISK_PASSWORD_CHECKING_EXIT (DVHXMP EXEC)
: Exit for minidisk password syntax verification. The passed parameters are enhanced for networking support. This exit will be called for the ADD, AMDISK, CHNGID, CHVADDR, and TMDISK commands as well as for the MDISK command. No sample is provided.

MULTI_USER_VERIFICATION_EXIT (DVHXMU EXEC)
: MULTIUSER authorization checking exit screens all attempts to use the MULTIUSER prefix operand. This exit must approve any use of this prefix operand. No sample is provided.

PASSWORD_CHANGE_NOTIFICATION_EXIT (DVHXPN EXEC)
: Exit for user password change notification. This exit may be used to notify other service machines of changes to a user's logon password. It will be called whenever a password change is successful. The IBM supplied sample maintains a history of recently used passwords in the

DVHPWUSE DATADVH file. The passwords are obscured using the PW_REUSE_HASHING_EXIT .

(DVHXPROF EXEC)
Post-profile exit for the DirMaint service machines. Typically a router to call DVHLOCAL for DIRMAINT, DVHDATLC for DATAMOVE, or DVHSATLC for DIRMSAT. The exit name, DVHXPROF, must **not** be renamed. IBM supplies a sample.

PW_NOTICE_PRT_EXIT (DVHXPP EXEC)
Exit for printing password notices. This exit may be used to forward printed password notices to a network printer for those systems that do not have a local printer. IBM supplies a sample.

REQUEST_AFTER_PROCESSING_EXIT (DVHXRA EXEC)
Request exit, after processing. The passed parameters are enhanced for networking support. No sample is provided.

REQUEST_BEFORE_PARSING_EXIT (DVHXRC EXEC)
Request exit, before parsing. No sample is provided.

REQUEST_BEFORE_PROCESSING_EXIT (DVHXRB EXEC)
Request exit, after parsing, before processing. The passed parameters are enhanced for networking support, and additional return codes are recognized. No sample is provided.

LOCAL_STAG_AUTHORIZATION_EXIT (DVHXTA EXEC)
Local STAG authorization exit controls authorization allowing manipulation of locally defined *Star Tags*, or STAGs. No sample is provided.

BACKUP_TAPE_MOUNT_EXIT (DVHXTP EXEC)
Backup tape mount exit may be used to mount backup tape using AMMR, VMTAPE, and other tape library management programs. IBM supplies a sample.

USER_CHANGE_NOTIFICATION_EXIT (DVHXUN EXEC)
Exit for user notification. This exit may be used to notify other service machines of new, deleted, or changed user IDs. It will be called whenever the ADD, CHNGID, PURGE, or POSIXGROUP commands have added, changed, or deleted a user ID, profile, or posix group. No sample is provided.

Release 5.0 DATAMOVE Service Machine Exit:

DATAMOVE_NONCMS_COPYING_EXIT (DVHDXP EXEC)
Data Move exit to process non-CMS minidisk copy requests. No sample is provided.

User-Written Command Handlers using SDI Routines

Additional exits, called Source Directory Interface Routines (SDI Routines), provide a common interface for user-written programs to modify the directory source. The routines are broken into these categories:

- Initialization
- Internal Manipulation
- Update and Merge

The Initialization routines obtain a copy of the target directory entry for one or more user IDs, and create an *internal* format filectory. This internal directory contains

control information that allows other SDI routines to manipulate it. The Internal Manipulation routines modify the internal format directory. The Update and Merge routines convert the internal format directory to an external format. This new directory replaces the existing source directory entry for the user ID being changed and the new directory is placed online. A Cleanup routine removes the internal format directory.

The names and functions of the supplied SDI routines are as follows:

Initialization

DVHBBINI Converts a directory entry into DirMaint's internal format.

Internal Manipulation

DVHBBLGT Given a set of search parameters, returns a record from the internal directory that matches the search.

DVHBBLDE Given a list of parameters, deletes the specified record from the internal directory.

DVHBBLPT Given a token count and the new record to be inserted, or given a token count and a list of parameters, replaces the specified record with the new record if the record existed. Inserts the record if it did not exist.

Update and Merge

DVHBBIUP Converts the internal format directory back to its original format, updates the appropriate source directory disks, lets any satellite machines know that a source change has been made and places the new source directory online.

DASD Management Improvements

To improve the efficiency and usability of DirMaint Release 5.0 DASD management, these changes have been made:

- Limitations for DASD groups, volumes, and allocatable regions have been removed.

  The DirMaint Release 4.0 limitation of 10 DASD groups with a maximum of 32 volumes per group and 16 allocatable regions per volume have been removed. The slot-size allocation method is replaced by named regions within a volume, which does not need to be aligned on a slot-size boundary. Entries within a DASD group can refer to one or more named regions within a DASD volume.

  The AMDISK and CMDISK commands have been enhanced to allow automatic allocation of space within a named region of a volume, as well as within a group, or on a volume. The RMDISK command has been enhanced to allow automatic allocation within either groups, named regions, or on a volume.

- BLKSIZE and LABEL parameters have been added to the AMDISK and CMDISK commands.

  AMDISK will optionally format the newly allocated space before making it available to the user. Both AMDISK and CMDISK allow optional specification of a blocksize with which the new minidisk should be formatted, the label that should be used for the new minidisk, or both.

- CMDISK and RMDISK commands were redefined to make them function more rationally. The CMDISK command is now used for operations that require data movement, and RMDISK is used for operations that do not. The V-DISK and T-DISK parameters are dropped from the CMDISK command and added to the RMDISK command.
- There is no automatic allocation of DASD space beginning at cylinder or block zero.

  DirMaint Release 5.0 does not format any space being allocated or de-allocated if that space overlaps another minidisk extent. In most cases, space allocated starting at cylinder or block zero (most often a full volume minidisk) will not be formatted. Note that full volume minidisks may still be formatted as a result of CMDISK, DMDISK, or PURGE processing if CLEANUP is specified, unless they overlap another minidisk extent or they are defined as a DEVNO minidisk.

  This new entry has been added to the DIRMAINT DATA file to allow you some control over whether a disk gets formatted starting at block or cylinder zero:

  ```
  CYL0/BLK0_CLEANUP= NO | YES
  ```

  If NO is specified, DirMaint will NEVER clean any minidisk beginning at cylinder or block 0; even if it doesn't overlap any other minidisk. If YES is specified, DirMaint will conditionally clean minidisks starting on cylinder or block zero provided it doesn't overlap any other minidisk as described above.

Miscellaneous Operational Enhancements

These miscellaneous enhancements were made to DirMaint Release 5.0 as a result of customer feedback and observations during usage of DirMaint Release 4.0.

- Initialization processing, ADD processing, and REPLACE processing now leave directory information in mixed case except for the directory statement names, which are the first token on each statement. While most DirMaint commands will be converted to all uppercase during parsing, the parsing control files can be customized to leave any desired data parameter or parameters in mixed case.
- Minidisk space that is allocated but excluded is shown in the FREEXT listings with a notation that it is excluded space. Similar space is also shown in the USEDEXT listings with a notation that it is excluded space.
- DirMaint will automatically map and reserve PAGE, SPOOL, and T-DISK space if given the necessary CP privilege class.
- When the DATAMOVE service machine is unable to complete CMDISK processing, the original extent will be returned to the original owner until arrangements are made with the system administration staff for another try. (The DATAMOVE machine will hold the lock if the condition is transient, such as a non-zero return code from a CP LINK command.)
- DirMaint Release 5.0 supports alternate object directories and alternate source directories.

  To enable alternate source directory support, you must simply allocate a 2DF minidisk (or an equivalent SFS directory) for the DIRMAINT virtual machine and any satellite service machines.
- The base CONFIG DATADVH file is created during installation by specifying the SAMP option on the IN2PROD install invocation. There is a significant

number of new entries in this file that are needed by general users, with system-wide defaults being tailorable by the system administrator. General users may copy the installed CONFIG DATADVH file to their own disk or SFS directory as file CONFIG* DATADVH, and supplement or override the system defaults contained in it. The CONFIG files are searched in reverse EBCDIC order (for example, CONFIG99 ... CONFIG0 ... CONFIGZZ ... CONFIGA ... CONFIG).

Information contained in the CONFIG DATADVH file that is not needed by general users, and that the installation considers sensitive, may be removed from the system-wide CONFIG DATADVH file and moved to a separate CONFIG* DATADVH file on the DIRMAINT machine's 191 disk (or an equivalent SFS directory) where it is not accessible to the general user community.

However, most of the sensitive information formerly contained in the DIRMAINT DATA file has been moved to other files, the:

- `DIRM_MONITOR_BROADCAST=` list is now in a DVHNAMES DATADVH file.
- `DIRM_STAFF=` list and `DIRM_SUBSTAFF=` list are now contained in the AUTHFOR CONTROL file which is contained on the source directory minidisk (or equivalent SFS directory).
- `WPW=` list is now contained in the source directory itself. By default, password authentication is required for most commands. Password authentication is not required for the PW? command, or commands that are not sent to the DIRMAINT virtual machine and are executed in the user's virtual machine. These commands are CHECK, EXECDROP, EXECLOAD, GLOBALV, and HELP. The system default is controlled by an entry in the CONFIG DATADVH file.

None of these files are accessible to general users.

- Password warning notice distribution is controlled by these entries in the CONFIG DATADVH file:

  ```
  PW_NOTICE_RDR_CLASS= A|class_letter|NONE
  PW_NOTICE_PRT_CLASS= A|class_letter|NONE
  PW_NOTICE_PRT_EXIT=  DVHXPP EXEC
  ```

  Unless `RDR_CLASS= NONE` is specified, reader notices are generated daily until the password is changed. Also, unless `PRT_CLASS=NONE` is specified, printer notices are generated daily until the password is changed. Before sending a printer or reader notice, a CP TRANSFER command is used to get back and purge the previous notice.

  Note: Use of any RDR or PRT class other than A or NONE requires the use of VM/ESA Release 2.2 or later.

  If the `PW_NOTICE_PRT_EXIT=` routine is specified, it will be called to handle the routing of the printed notices. This allows printed notices to be sent to another system for printing.

- All device statements may be kept in statement type and device address order by this new entry in the CONFIG DATADVH file:

  ```
  SORT_BY_DEVICE_ADDRESS= NO | YES
  ```

  The device statements are maintained in this order:

  1. CONSOLE

2. SPOOL
3. SPECIAL
4. DEDICATE
5. LINK
6. MDISK

- Selective logging and log file filtering can be established by using the DVHXLF exit routine. Refer to page 8 for a description of this routine.
- All of the password interval specifications are changed to a consistent format to eliminate the need for mental arithmetic. You can specify a default for the number of days a password is valid until it expires by modifying these entries in the CONFIG DATADVH file.

```
PW_INTERVAL_FOR_GEN=  83|nnn 97|nnn
PW_INTERVAL_FOR_PRIV= 28|nnn 35|nnn
PW_INTERVAL_FOR_SET=   4|nnn  3|nnn
```

  The first value is the number of days after change before generating warning notices, the second value is the number of days after change before the password expires. A password can only be changed using the PW command. A password is set by using the ADD, CHNGID, REPLACE, and SETPW commands. A privileged user is one for whom the DVHXCP EXEC returns a non-zero return code. For more information on the DVHXCP exit, see 7.

  The SETPW command has been modified to include the DAYS parameter as:

  EXEC DIRMaint FOR *targetid* SETPW *newpass* [*nnn* DAYS]

  Where:

  nnn **DAYS**
  Specifies to set the password expiration date *nnn* days in the future, and use the entries in the CONFIG DATADVH file to calculate the age necessary to give the required effect.

- Passwords on *MDISK directory statements are masked in the same manner as those on ordinary MDISK statements.
- Any customization of objects, such as product files or tables, can be customized by the system administrator at the central site and then distributed to the remote sites through NetView Distribution Manager (NetView DM).
- A DirMaint user will never have to make a note of message responses provided by the product. All important information is logged by the system.
- Customization and administration tasks, as well as installation and service, can be performed from a single user ID (for example, logged onto user ID P748XE4M, rather than MAINT).
- Audit trail information can be accumulated in up to three places, the:
  - DIRMAINT service machine's console spool file(s)
  - DIRMAINT service machine's DIRMAINT TRANSLOG file
  - External Security Manager (ESM) service machine's audit data set, if an ESM (such as RACF/VM) is installed.

An administrator may select which of the last two are active, and may select the retention characteristics of the first two. (The console spool file is always active and no information is filtered as in previous releases. The retention in the ESM audit trail is under control of the ESM).

- DirMaint user is not required to create or manipulate files on his or her private disk space, although the use of certain options may require such files. Any required configuration parameters are maintained in the user's LASTING GLOBALV file using the DIRMAINT GLOBALV command.

Compatibility

DirMaint Release 5.0 maintains compatibility with DirMaint Release 4.0 by providing a choice of operating modes: 140A compatibility mode, and 150A mode. 150A is the normal mode of operation and enables all new command support and DirMaint Release 5.0 function. 140A compatibility mode allows DirMaint to accept commands using the same syntax as used in DirMaint Release 4.0. In this mode minimal new function is enabled. If you are upgrading from DirMaint Release 4.0 to DirMaint Release 5.0 you may choose to run DirMaint in the 140A compatibility mode until you convert your user-written programs to work with the 150A level.

Some of the differences and similarities between DirMaint Release 4.0 and DirMaint Release 5.0, as well as between 140A mode and 150A mode are worth noting here.

- In 140A mode DirMaint accepts all valid DirMaint Release 4.0 commands.
- In 140A mode DirMaint accepts all valid DirMaint Release 4.0 SMSGs.
- Message prefixes are expanded from 10 character fixed length identifiers to variable length 10 to 13 character identifiers. However, message identification (routine names and message numbers) are tailorable to allow increased compatibility if desired.
- When running DirMaint Release 5.0 in 140A command level mode, the CONSOLE command performs the same function as it did with DirMaint Release 4.0. When running in 150A command level mode, the function provided by the CONSOLE command is invoked by using the GETCONS command.
- When running with command level 140A, the SETOPTN command will perform the same function as it did in DirMaint Release 4.0. When running with command level 150A, that function is now performed by the USEROPTN command.

  When running with command level 150A, the SETOPTN command lets a privileged administrator add option keywords to a user's OPTION directory statement. This is consistent with the user or the SET prefix for other commands where both the user and the administrator may manipulate the same directory statement.
- These commands work differently than in DirMaint Release 4.0, even in 140A compatibility mode:

Command	DirMaint Release 4.0	Dirmaint Release 5.0 CMDLEVEL 140A
BATCH	Required no parameters. Used to enter an XEDIT session to build the enters an XEDIT session file.	Requires no parameters. If none are provided, to build the file. Optionally, the file name and file type of a pre-built file may be specified.
GLOBALV	Command did not exist.	Command is supported.
MDPW	Allowed a maximum of one disk address	Allows multiple disk addresses.
NEEDPASS	Command did not exist.	Command is supported.
PW	Did not allow a password to be specified directly on on the command. Also, no provision for generating a random password.	Allows specification of a password directly the command. Also, accepts the RANDOM keyword for generating a random password that the user may accept or reject.
TESTPW	Same as PW, above.	Same as PW, above.
USEROPTN	Command did not exist.	Command is supported.

- The new DIRM NEEDPASS command can now be used to waive a password.
- General users no longer need access to the list of DIRM_STAFF or WPW users. Checking in the user's machine is based on GLOBALV settings. The DIRMAINT service machine still checks the real authorization list.
- An empty DIRMAINT TESTONLY file is no longer required for testing. A GLOBALV setting controls this.

Migration

When migrating from a prior release of VM on which DirMaint Release 5.0 is not supported (VM/ESA 1.2.0 or earlier) to a newer release of VM on which DirMaint 1.4.0 (or whatever other directory management product you have been using) is not supported (VM/ESA 2.1.0 or later), we recommend that you use your existing directory management methods to create the directory entries needed for the new DirMaint service machines and allocate the required DASD space. Then quiesce your old manager, install the new level of CP and CMS, then install your new DirMaint Release 5.0, and tailor as necessary. Other migration sequences may give unpredictable results. When migrating from one VM release to another VM release where DirMaint Release 4.0 and DirMaint Release 5.0 are both supported on both VM releases (VM/ESA 1.1.5, 1.2.1, 1.2.2), you may migrate VM and DirMaint in either order.

Migration from DirMaint Release 4.0 to DirMaint Release 5.0 does not require changes to customer programs that issue DirMaint commands using the DIRMAINT EXEC, unless they are dependent upon specific return codes or message responses.

The migration of DirMaint Release 4.0 to DirMaint Release 5.0 does not require changes to customer programs that issue DirMaint commands using SMSG directly to the DIRMAINT service machine, unless the command involves the transmission of a spool file or the command is dependent upon specific message responses.

Migration utilities are available to assist the customer in converting the following DirMaint 1.4.0 customer tailorable files to DirMaint Release 5.0 format:

ASSIGN FILE
DIRMAINT DATA
EXTENT CONTROL
LINKS EXCLUDE
LINKS FILE
PWMON CONTROL

National Language Support Considerations

Online information for the DirMaint Release 5.0 base feature only includes American English. You can convert to uppercase English by following the directions supplied in the program directory.

The message repositories are shipped with the base product. Messages are available in mixed case American English, uppercase English, and Japanese Kanji.

Installation Considerations

Before you begin the installation of DirMaint, you will need to do the following:

- Ensure that your source directory satisfies DirMaint restrictions. Review "Restrictions" on page 18.
- Define the required user IDs and allocate the necessary minidisk space for installation and use of the product. See the DirMaint Program Directory.
- Identify the configuration of a multiple system cluster or network, and identify the user IDs that will have authority to issue the privileged commands, and the user IDs that are to be defined in the event of significant events.

Note: User IDs defined for DirMaint must be made up of only the characters that are valid for CMS file names.

The planning documentation is available in two forms:

- The Program Directory in printed form
- The 5748XE4M PLANINFO file which is created during installation and placed on the file mode A minidisk.

Installation Using VMSES/E

VMFINS is used to install DirMaint Release 5.0. VMFINS is an installation aid supplied as part of VMSES/E to make installation of VM products consistent.

For more information on the VMFINS installation, see *z/VM: VMSES/E Introduction and Reference*.

VMSES/E Installation Process Overview

The overview will give a brief description of the main steps in installing DirMaint using VMSES/E. For more information see, *DirMaint Program Directory* and *Directory Maintenance VM/ESA: Tailoring and Administration Guide*.

- Planning

Use the PLAN function of VMSES/E to generate a PLANINFO file listing all the user ID requirements, required products, and minidisk space requirements for installing DirMaint. Use the planning information in the 5748XE4M PLANINFO file to create the required user IDs and minidisks.

- Installing

  To install DirMaint issue the VMFINS INSTALL command without the PLAN option while logged onto the P748XE4M user ID, the default user ID for DirMaint. This will install all base files required to run and rebuild DirMaint. Source files can also be loaded from the product tape. An SFS directory can be substituted for some of the product disks.

  You can select a PPF override for installing DirMaint Release 5.0 based on whether you wish to use the compiled execs or interpretive execs. DIRM will be used for interpretive, and DIRMC will be used for compiled.

- Tailoring

  Once DirMaint is installed, you can customize tailorable files, then test the new installation. Once you are satisfied with a test environment, place DirMaint into production by doing the following from the P748XE4M user ID.

  1. Copy the DIRMAINT EXEC and ACCESS DATADVH files onto the MAINT 19E Y-disk from the 29E test disk. No other DirMaint product files are to be installed to this disk. The DIRMAINT EXEC file is the only product file referenced by general users that does not contain the DVH component id as part of the file name or file type.
  2. Use the IN2PROD exec to copy files from the 492 to the 491 minidisk and the 41F to the 11F minidisk.

     The remaining files needed by general users for submitting transactions to the DIRMAINT service machine will be located on the 41F test and 11F production minidisks. This is equivalent to the 1A5 disk used in DirMaint Release 4.0.

     Note: If a different disk other than the 11F minidisk is used as the production minidisk, the ACCESS DATADVH file must be tailored to identify the location used for these files on each node in a multiple system cluster. The same ACCESS DATADVH file may be shared by all nodes in a multiple system cluster or throughout a corporate wide network. If the default 11F production minidisk is chosen, tailoring is not required.

     If the compiled EXECs are used for production, either the $EXEC source or the interpretive EXEC for the five user exit routines should be made available to the user community.
  3. All files needed by the DirMaint service machines (DIRMAINT, one or more optional DATAMOVE machines, and the optional DIRMSAT cluster satellite server machines) will be located on the 492 test and 491 production minidisks. The DIRMSAT and DATAMOVE service machines will have a read-only link to the 491 minidisk as their 191 minidisk. The DIRMAINT service machine will have a read-write link to the 491 minidisk.

     Note: If a different disk other than the 491 minidisk is used as the production disk, the directory entry for each server must be tailored to identify the location used for these files.

4. Copy the DirMaint Release 5.0 general user HELP files from the 29D minidisk to MAINT's 19D minidisk. Alternatively, these files may be placed on the same disk or directory as the command interface files.
5. Re-save the NSS (Named Saved System) or DCSS (Discontiguous Saved Segments) to pick up the changes to the YSTAT resulting from DirMaint's installation.

Service Considerations

DirMaint is installed using VMSES/E. Corrective service PTFs will be available when necessary and also installed using VMSES/E. Cumulative preventive service will be available following the VM Recommended Service Upgrade (RSU) process, and will be installed using VMSES/E. Periodic DirMaint refreshes will be available using the System Delivery Offering (SDO).

Restrictions

These restrictions apply to DirMaint Release 5.0:

- User IDs defined for DirMaint must conform to the CMS file naming convention. Each profile name and user ID must be unique. The names $DIRCTL$ and $DIRGRP$ are reserved for DirMaint's use. Names in the form $DIR*xxx*$ should be avoided because they are reserved for any future use by DirMaint.
- The display of menus requires a 3270 compatible terminal with a minimum of 24 lines and at least an 80 column line length.
- Exits may require tailoring for use with RACF or other external security managers.
- Although minimal, there are some changes that are made to the system directory as a side effect of using SDI routines.
  - All addresses are expanded to four digits (if not already so) when the source directory is converted to internal format. When the internal format is converted back to the external format, the four digit address expansion is maintained.
  - When converted to the internal format, most directory statements are uppercased and excessive blanks are removed between the statement operands. When the internal format is converted back to the external format, the uppercasing and single spacing is maintained. Comments, POSIX, and optionally the ACCOUNT statements are excluded from this process.
  - Only one copy of NOPDATA per System Affinity group is retained. If multiple copies of NOPDATA exist in the user's directory, the SDI routines strip out the excessive copies during initialization.
- DirMaint does not allow the use of &SYSRES for a volume identification on an MDISK directory statement. The value of +VMRES is supported, with some restrictions. The use of +VMRES is reserved by CP and should not be used as the real volume label of a physical DASD volume. The value of the synonym may be changed by including the &SYSRES parameter on the DIRECTXA_OPTIONS entry in the CONFIG* DATADVH file(s). For example,

DIRECTXA_OPTIONS= MIXED NOMIXMSG &SYSRES VM:RES tells DirMaint, DIRECTXA, and CP to use VM:RES as the synonym rather than +VMRES.

Object Code Maintained Parts

The DVHCRC, DVHWAKE, and DVHWAKE3 modules are shipped as Object Code Maintained (OCM) parts; base source code and source updates are not available through the DirMaint product, but are available to licensees of other IBM products. The DVHHASH module is shipped as an Object Code Only (OCO) part; source code is not available.

System Integrity Statement

DirMaint Release 5.0 supports the VM/ESA System Integrity statement. *IBM will accept APARs that describe exposures to system integrity or that describe problems encountered when a program running in a virtual machine not authorized by a mechanism under the customer's control introduces an exposure to system integrity*.

Standard VM system facilities are used to:

- Protect the DirMaint service machines (DIRMAINT, DATAMOVE, DIRMSATs) from subversion
- Protect files from outside interference or contamination
- Isolate users both from each other and from the system
- Exploit hardware protection mechanisms
- Identify the originating user ID (and node ID), for all incoming requests
- Record auditable information

DirMaint runs as a CMS application program, written primarily in the REXX language.

The DIRMAINT service machine requires CP privilege class B to use diagnoses X'84', X'A0', X'3C', X'D4', and the CP MSGNOH command. The optional DIRMSAT service machines used in a multiple system cluster require CP privilege class B to use diagnose X'84' and diagnose X'3C'. The DIRMAINT service machine requires CP privilege class D in order to issue the CP QUERY ALLOC command to determine system owned space. Both DIRMAINT and the DIRMSAT machines benefit from use of the OPTION D84NOPAS directory statement, and security is enhanced somewhat with the D8ONECMD FAIL LOCK directory statement.

Note: The D8ONECMD statement and the D84NOPAS option are not supported by the VM/ESA (370 Feature) Release 1.5. DirMaint can use CP class D of VM/ESA Version 1 Release 2.2 or later to use the CP QUERY ALLOC command to automatically map system PAGE, SPOOL, and T-DISK space (not valid on a VM/ESA (370 Feature) Release 1.5, and not useful in a CSE cluster).

Security Strategy

DirMaint Release 5.0 supports the VM/ESA Security strategy:

- Access to user IDs is password controlled. DirMaint maintains user passwords, with customer choice of administration control or user control. DirMaint also supports the use of an External Security Manager (ESM), such as RACF for password control.
- Access to minidisks is controlled by either passwords or explicit link authorization, as determined by the minidisk owner. Minidisk passwords are now optional for controlling minidisk directory links. DirMaint also supports control of minidisk links by an ESM.
- In a VM Trusted Computing Base (TCB) environment, all DirMaint service machines must run with SECLEVEL=SYSHIGH in order to receive requests from all users, and must be trusted servers in order to respond to these. For more information about TCB systems, see Appendix A, “Trusted Computing Base Security Support” on page 21.
- VM system services are used to identify the originating user ID (and node ID) for all requests, whether local or remote. By default, all requests must be authenticated by providing the correct logon password for each DirMaint transaction. Unless prohibited by the system administrator, users may request suspension of authentication for requests made from their user ID within the scope of a multiple system cluster. Remote requests never require authentication, and surrogate requests always require authentication.
- DirMaint does not provide nor use cryptographic services.
- All DirMaint commands involving the DirMaint service machines (DIRMAINT, DATAMOVE, DIRMSATs) are auditable. A few DirMaint commands (CHECK, DEFAULTS, EXECDROP, EXECLOAD, GLOBALV, HELP) are completely processed in the user's virtual machine, and are therefore not auditable.

  All messages generated by the DirMaint service machines are auditable.

  An exit routine will allow customer tailorable filtering of unnecessary audit details.

Appendix A. Trusted Computing Base Security Support

The IBM Directory Maintenance VM/ESA Licensed Program (DirMaint) is designed to meet the Trusted Computer System Evaluation Criteria (TCSEC) established by the U.S. Department of Defense (DoD) National Computer Security Center (NCSC), for classes C2 and B1, as documented in DoD publication 5200.28-STD dated December 1985. This allows DirMaint (release 4 and later) to serve as one of the trusted components of the VM/ESA C2/B1 Trusted Computing Base (TCB), along with the Resource Access Control Facility (RACF) and other components.

Some or all of the capability provided by this support may be of interest to you even if your system is not an officially evaluated TCB system.

TCB Function Provided by DirMaint

DirMaint satisfies the Trusted facility Manual (TFM) requirements of a TCB system by:

- Notifying more than one person in the DVHNAMES DATADVH for any events that require attention, with the intent being to minimize reaction time to the event.

  This capability is supported on any level of VM/ESA operating system with or without RACF installed.

- Recording transactions and messages in the RACF *single audit log file*. This allows all audit information to be placed in a single file called the RACF SMF DATA file, where it can not be tampered with by the DirMaint user.

  This capability requires the use of RACF 1.9.0 or higher running on VM/ESA. This capability is a requirement for both class C2 and class B1 TCB operation. For either class C2 or class B1 TCB operation, at a minimum, RACF 1.9.2 on VM/ESA 1.2.0 or higher is required.

- Sends all spool files (except dumps) with a SECLABEL of SYSLOW (or other SECLABEL value chosen by the system administrator) when mandatory access control (MAC) is active. This allows all users to read the files sent to them by DirMaint. While this DIRMAINT SECLABEL support is not required for class B1 TCB operation, it does make MAC more usable, and MAC is required for class B1 TCB operation.

  This capability requires the use of VM/ESA 1.2.0 or higher and RACF 1.9.2 or higher.

  Note: The SECLABEL function is not supported in a Cross System Extension (CSE) environment.

These functions are disabled by default. For more information, see *Directory Maintenance VM/ESA: Tailoring and Administration Guide*.

DirMaint and the TCSEC

The Trusted Computer System Evaluation Criteria (TCSEC) established by the U.S. Department of Defense (DoD) National Computer Security Center (NCSC), as documented in DoD publication 5200.28-STD, dated December 1985, defines 4 divisions or major levels of trust for computer security:

1. Division D: Minimal Protection
2. Division C: Discretionary Protection
3. Division B: Mandatory Protection
4. Division A: Verified Protection

and further refines each division (except D) into classes:

1. Class C1: Discretionary Security Protection

   The primary feature of interest for this class is that access is granted at the discretion of an authorized resource user, typically via password protection. The primary drawback to this is that any user who knows the password can authorize other users by disclosing the password.

2. Class C2: Controlled Access Protection

   The primary feature of interest for this class is that access is granted at the discretion of the resource owner, typically by means of an access control list to prevent propagation of access privileges. Also, an audit trail of security-relevant events is maintained.

3. Class B1: Labeled Security Protection

   The primary feature of interest for this class is that access is granted at the discretion of the resource owner, typically by means of an access control list to prevent propagation of access privileges; with the additional requirement for a verified need-to-know. Again, an audit trail of security-relevant events is kept.

4. Class B2: Structured Protection
5. Class B3: Security Domains
6. Class A1: Verified Design

Each class addresses a common set of trust-related topics, with the requirements getting progressively more stringent in each class. The topics include:

1. Audit (C2, B1)
2. Configuration Management (nr)
3. Covert Channel Analysis (nr)
4. Design Documentation (C1, C2, B1)
5. Design Specification and Verification (B1)
6. Device Labels (nr)
7. Discretionary Access Control (C1, C2, B1)
8. Exportation of Labeled Information (B1,na)
9. Exportation to Multilevel Devices (B1,na)
10. Exportation to Single Level Devices (B1,na)
11. Identification and Authentication (C1, C2, B1)
12. Label Integrity (B1,na)
13. Labeling and Human-Readable Output (B1,na)
14. Labels (B1)
15. Mandatory Access Control (B1)
16. Object Reuse (C2, B1)

17. Security Features User's Guide (C1, C2, B1)
18. Security Testing (C1, C2, B1)
19. Subject Sensitivity Labels (nr)
20. System Architecture (C1, C2, B1)
21. System Integrity (C1, C2, B1)
22. Test Documentation (C1, C2, B1)
23. Trusted Distribution (nr)
24. Trusted Facility Management (nr)
25. Trusted Facility Manual (C1, C2, B1)
26. Trusted Path (nr)
27. Trusted Recovery (nr)

Those topics identified with *(nr)* above have no requirements for the C1, C2, or B1 classes. DirMaint is not involved with the exportation of labeled information to any external device, label integrity, or human-readable labels; therefore, the topics marked with *na* above are not applicable to DirMaint. Each of the remaining topics will be addressed as they pertain to DirMaint.

Note: DirMaint is only one component of the VM TCB. Each component of the TCB, and the TCB as a whole, must address each of these topics. The information in this publication is concerned only with how these topics apply to DirMaint.

Audit (C2, B1)

There are two requirements here. First, all security-relevant events should be recorded in a single audit trail. These security-relevant events include all commands (transactions) received by the DIRMAINT virtual machine, and all messages (responses) generated by the DIRMAINT virtual machine. Second, the system must protect this audit trail from unauthorized access or modification. The DIRMAINT TRANSLOG file kept on the DIRMAINT machine's disks do not satisfy this requirement. DirMaint transactions and responses must be recorded in the RACF SMF Data Set or *single audit log file*.

This audit capability is not provided by default. For more information, see *Directory Maintenance VM/ESA: Tailoring and Administration Guide*.

Design Documentation (C1, C2, B1)

The DirMaint library satisfies the design documentation requirement. For more information, see *Directory Maintenance VM/ESA: Tailoring and Administration Guide* and *Directory Maintenance VM/ESA: Diagnosis Reference*.

Design Specification and Verification (B1)

The DIRMAINT library satisfies the design specification and verification requirement. For more information, see *Directory Maintenance VM/ESA: Command Reference* and *Directory Maintenance VM/ESA: Tailoring and Administration Guide*.

Discretionary Access Control (C1, C2, B1)

DIRMAINT supports class C1 DAC capability by default. RACF supplements and largely supersedes this capability for classes C2 and B1. For more information, see *Directory Maintenance VM/ESA: Command Reference* and *Directory Maintenance VM/ESA: Tailoring and Administration Guide*.

Identification and Authentication (C1, C2, B1)

The CP component of the VM system obtains the user ID when the user first logs on to the computer system. This user ID is authenticated by an associated password. On a non-RACF system, the authentication is performed solely by the CP component of VM. On a system with RACF installed and operational, CP and RACF are both involved in the authentication of the user ID/password pair.

DirMaint uses CP facilities to obtain the user ID of the originator of a command or transaction. DirMaint usually requires the originator to supply his or her logon password for authentication of each DirMaint command or transaction. A user may waive the requirement to authenticate each command; however, this waiver may be prevented by the system administrator.

For more information, see *Directory Maintenance VM/ESA: Command Reference* and *Directory Maintenance VM/ESA: Tailoring and Administration Guide*.

Labels (B1)

DirMaint is not directly involved with labels, but will coexist in a system that provides this support. As a key component of the TCB, the DIRMAINT and DATAMOVE service machines are usually assigned a label of SYSHIGH. This makes spool files that the DIRMAINT machine sends to users generally unusable. As a trusted service machine, DirMaint can send these spool files to users with a more useful label, usually SYSLOW.

This spool file label support is not provided by default. For more information, see *Directory Maintenance VM/ESA: Tailoring and Administration Guide*.

Mandatory Access Controls (B1)

DIRMAINT is not directly involved with mandatory access control, but will coexist in a system which provides this support. For more information, see *Directory Maintenance VM/ESA: Tailoring and Administration Guide*.

Object Reuse (C2, B1)

The critical requirement here is that a resource object (DASD space) that was previously allocated to one subject (user) must not contain any residual data after it has been de-allocated and made available for reallocation to another subject (user).

This object reuse support is not provided by default. For more information, see *Directory Maintenance VM/ESA: Tailoring and Administration Guide* and comply with the rules given in *Directory Maintenance VM/ESA: Command Reference* to enable this support.

Security Features User's Guide (C1, C2, B1)

This publication in combination with *Directory Maintenance VM/ESA: Command Reference* satisfies the Security Features User's Guide (SFUG) requirement for the DirMaint component of the TCB.

Security Testing (C1, C2, B1)

The security testing done by IBM satisfies this requirement. The customer is responsible for testing the system to satisfy their own requirement.

System Architecture (C1, C2, B1)

The hardware architecture on which the VM operating systems run satisfies this requirement.

System Integrity (C1, C2, B1)

Tests performed by the Customer Engineer satisfy this requirement. This does not involve DirMaint.

Test Documentation (C1, C2, B1)

IBM's test documentation satisfies this requirement. The customer is responsible for documenting their own testing, and the results of those tests.

Trusted Facility Manual (C1, C2, B1)

A combination of this publication, *Directory Maintenance VM/ESA: Command Reference* and *Directory Maintenance VM/ESA: Tailoring and Administration Guide* satisfies the Trusted Facility Manual (TFM) requirement for the DirMaint component of the TCB.

Appendix B. Library Guide

The following describes the design and appearance of the DirMaint Release 5.0 library. It identifies the publications and the major tasks that they support. In addition, information for ordering publications is provided.

Library Structure

The DirMaint Release 5.0 library is organized according to the main tasks that computer users perform. The main tasks are:

Task	Definition
Evaluation	The evaluation task is performed by system managers, system analysts, and system programmers. This task consists of evaluating DirMaint to determine its applicability and advantages in maintaining the system directory.
Planning/installation	The planning/installation task is performed by system programmers. This task consists of the preinstallation planning and installation of DirMaint. It includes the tailoring of DirMaint to the requirements of an installation's system operation.
Administration/operation	The administration/operation task is performed by the system administrator. The system administrator is provided with a set of DirMaint command operands for performing the privileged directory maintenance operations. These operands provide an efficient and accurate method of performing the minidisk management and space allocation tasks.
End use	The end use task is performed by the general user and the system administrator. The general user is provided with a set of DirMaint command operands for modifying options in the user's directory entry on an interactive basis. These modifications are limited to those that do not require administrative authorization.
Diagnosis/Maintenance	The diagnosis/maintenance task is performed by the system programmer. These tasks include: • Tailoring DirMaint to accommodate changes in the system operation and resources • Problem source identification • Assisting the system administrator with tailoring DirMaint for optimum system performance.

Abstracts of Books in the Directory Maintenance VM/ESA Base Library

These abstracts describe the contents of the books in the DirMaint VM/ESA base library. The title of the book is followed by its form number.

Evaluation: Deciding if DirMaint Meets Your Needs

Directory Maintenance VM/ESA: Licensed Program Specifications, GC20-1837

This document provides information on the warranted functions of DirMaint, the specified operating environment, and the supplemental terms.

Directory Maintenance VM/ESA: General Information, GC20-1836

This book provides general information about DirMaint. It contains:

- An introduction to Directory Maintenance VM/ESA
- An overview of the functions that are new or changed for the current release
- Hardware and software requirements and packaging information
- Descriptions of the DirMaint, components, additional facilities supplied with DirMaint
- A library guide that explains the structure and content of the DirMaint publications library
- A list of the IBM processors that DirMaint supports
- A list of the IBM operating systems supported as guests of VM
- A list of the IBM devices that VM supports

Readers should have a background in VM in particular, some knowledge of the purpose, structure and content of the VM directory.

Planning/Installation: Generating, Maintaining and Making Decisions for DirMaint

Directory Maintenance VM/ESA: Tailoring and Administration, SC23-0533

This publication contains information intended for system programmers and system administrators. This publication provides the user with the information necessary for using DirMaint's programming interfaces (for example, user exits), tailoring DirMaint's files to accommodate the installation's needs, and administering user IDs and DirMaint's facilities.

This book is the primary source of information about the system configuration of DirMaint.

Directory Maintenance VM/ESA: Program Directory

This publication is sent with the product tape.

End Use: Performing DirMaint User Tasks

Directory Maintenance VM/ESA: Command Reference, SC20-1839

This publication contains information intended for System Administrators, System Programmers, and and DirMaint general users. This publication describes the command functions and syntax diagrams.

Diagnosis: Identifying, Describing, Reporting, and Correcting Problems

Directory Maintenance VM/ESA: Messages, SC20-1839

This publication contains information intended for system programmers, system administrators, and DirMaint general users. This publication provides the user with explanations, failing component names, and suggested corrective actions for messages issued by DirMaint.

Directory Maintenance VM/ESA: Diagnosis Reference, SC24-5883

This book provides diagnostic guidance information to help you identify, report, solve, and collect information about problems in DirMaint.

This book is intended for system programmers, system programmers, system analysts, and others that do diagnosis activities.

Ordering Publications

Online books are available in two formats: Adobe Portable Document Format (PDF) and IBM BookManager®.

Portable Document Format (PDF)

The Adobe Acrobat Reader is required to open and view PDF books on your workstation. You can also use the Adobe Acrobat Reader to print PDF books or sections of PDF books. The Adobe Acrobat Reader is available free from the Adobe home page (http://www.adobe.com).

IBM BookManager

IBM BookManager READ/VM (5684-062) Release 3 or later is required to view BookManager books loaded on the z/VM system. This program has the following prerequisite licensed programs:

- GDDM/VMXA Version 2 (5684-007) Release 3 or later
- C/370 Library Version 2 (5688-188) Release 2 or later
- IBM Compiler and Library for REXX/370 (5695-013) or IBM Library for REXX/370 (5695-014)

BookManager APAR GC05366 is required for READ/VM Public Library to run in a non-370 mode virtual machine.

Special versions of the BookManager READ programs for Windows, OS/2, and DOS are included on the *IBM Online Library Omnibus Edition: VM Collection* CD-ROM. Also included is the IBM Bookshelf Upload Program, which allows you to upload books to a VM, OS/390, or MVS® host.

Note: The IBM Library Reader™ programs for Windows, OS/2, and DOS have been revised to read all books in BookManager format (IBM and non-IBM). The BookManager files supplied with z/VM will work only with the new readers. Library Reader programs provided prior to VM/ESA 2.4.0 will not read these BookManager files. To read these files using a Library Reader program on your workstation, you must use one of the Library Reader programs provided on the July 1999 or later CD-ROM or download the revised program from the IBM BookManager Web site (http://booksrv1.raleigh.ibm.com/homepage/ilrserv.html).

Notices

IBM may not offer the products, services, or features discussed in this document in all countries. Consult your local IBM representative for information on the products and services currently available in your area. 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 IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described 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:

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

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:
INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes to the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

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 Corporation
Mail Station P300,
522 South Road
Poughkeepsie, NY 12601-5400
U.S.A.
Attention: Information Request

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

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

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

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information may contain examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information may contain sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to IBM's application programming interfaces. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

Trademarks

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

- BookManager
- DFSMS/VM
- Enterprise Systems Architecture/370
- Enterprise Systems Architecture/390
- IBM
- IBMLink
- Library Reader
- OfficeVision/VM
- RACF
- System/370
- VM/ESA
- z/VM

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

Index

U

V

Communicating Your Comments to IBM

Directory Maintenance VM/ESA
General Information
Release 5.0

Publication No. GC20-1836-07

If you especially like or dislike anything about this book, please use one of the methods listed below to send your comments to IBM. Whichever method you choose, make sure you send your name, address, and telephone number if you would like a reply.

Feel free to comment on specific errors or omissions, accuracy, organization, subject matter, or completeness of this book. However, the comments you send should pertain to only the information in this manual and the way in which the information is presented. To request additional publications, or to ask questions or make comments about the functions of IBM products or systems, you should talk to your IBM representative or to your IBM 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.

If you are mailing a readers' comment form (RCF) from a country other than the United States, you can give the RCF to the local IBM branch office or IBM representative for postage-paid mailing.

- If you prefer to send comments by mail, use the RCF at the back of this book.
- If you prefer to send comments by FAX, use this number:

  1-607-752-2327 (US and Canada)
- If you prefer to send comments electronically, use this network ID:
  - pubrcf@vnet.ibm.com
  - USIB2L8Z@IBMMAIL

Make sure to include the following in your note:

- Title and publication number of this book
- Page number or topic to which your comment applies.

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

Directory Maintenance VM/ESA
General Information
Release 5.0

Publication No. GC20-1836-07

Overall, how satisfied are you with the information in this book?

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Overall satisfaction	□	□	□	□	□

How satisfied are you that the information in this book is:

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Accurate	□	□	□	□	□
Complete	□	□	□	□	□
Easy to find	□	□	□	□	□
Easy to understand	□	□	□	□	□
Well organized	□	□	□	□	□
Applicable to your tasks	□	□	□	□	□

Please tell us how we can improve this book:

Thank you for your responses. May we contact you? □ Yes □ No

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.

Name

Address

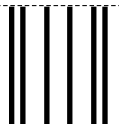
Company or Organization

Phone No.

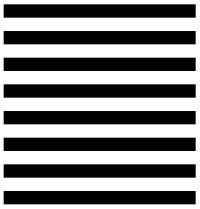
Readers' Comments — We'd Like to Hear from You
GC20-1836-07

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 Corporation
Information Development
Department G60G
1701 North Street
Endicott, New York 13760-5553

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

Cut or Fold
Along Line

File Number: S370/S390-34
Program Number: 5748-XE4

Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.

GC20-1836-07

Spine information:

IBM Directory Maintenance VM/ESA General Information *Release 5.0*